

Integrations

Alert Rules

V5.4.12

CONTENTS

1	Alert Rules	2
2	MITRE ATT&CK Analytics	3
2.1	LP_Unsigned DLLs loaded by RunDLL32 or RegSvr32	3
2.2	LP_Terminal Service Configuration Modified	3
2.3	LP_System Service Reconnaissance through WMI	4
2.4	LP_Suspicious Msiexec Child Process	4
2.5	LP_Process Reconnaissance through WMI	5
2.6	LP_Process Created through WMI	5
2.7	LP_Local Users Reconnaissance through WMI	6
2.8	LP_Installed Software Updates Reconnaissance through WMI	6
2.9	LP_Application uninstall via WMIC	7
2.10	LP_Applnit DLLs Detected	7
2.11	LP_High Severity EPP Alert	8
2.12	LP_Host Generating Multiple Medium Severity EPP Alert	8
2.13	LP_Host Generating Multiple High Severity EPP Alert	8
2.14	LP_Medium Severity EPP Alert	9
2.15	LP_Windows Service Stop or Delete	9
2.16	LP_Suspicious Hack Tools Execution	10
2.17	LP_Suspicious Execution of XORDump Utility for LSASS Memory Dump	10
2.18	LP_Suspicious Execution of Createdump Utility for Memory Dump	11
2.19	LP_Suspicious DsInternals Get-ADReplAccount Activities	11
2.20	LP_Suspicious Activities Associated with NTDS Exfiltration	12
2.21	LP_Possible LSASS Memory Dump Via Windows Task Manager	12
2.22	LP_Possible LSASS Dump Via SilentProcessExit Technique	13
2.23	LP_NTDS or SAM Database Copy Operation	13
2.24	LP_Microsoft IIS Service Account Password Dumped	14
2.25	LP_Dumpert Process Dumper Execution	14
2.26	LP_Credential Dump Via NPPSpy	15
2.27	LP_Malicious PowerShell Commandlets Detected	15
2.28	LP_Code Execution Via Diskshadow Detected	16
2.29	LP_Image Mount Indicator in Recent Files	16
2.30	LP_Disk Image File Created	17

2.31	LP_PowerShell Execution via DLL Detected	17
2.32	LP_Suspicious Windows Defender Registry keys Modification	18
2.33	LP_Executable Files Created and Executed by Office Applications	18
2.34	LP_WMI Backdoor in Exchange Transport Agent	19
2.35	LP_Suspicious Msiexec Usage Detected	19
2.36	LP_Suspicious Usage of Advanced IP Scanner	20
2.37	LP_Persistence through Port Monitor Registry modification	20
2.38	LP_File Dropped in Suspicious Location	21
2.39	LP_Alternate PowerShell Hosts via Powershell Module	21
2.40	LP_Suspicious Usage of Where Binary	22
2.41	LP_MSHTA - Activity Detected	22
2.42	LP_Alternate PowerShell Hosts via Named Pipe	23
2.43	LP_Suspicious File Execution Using Wcript or Cscript	23
2.44	LP_Suspicious Child Process Spawned by Microsoft Office Product	24
2.45	LP_Windows Login Attempt on Disabled Account	24
2.46	LP_RClone Utility Execution	25
2.47	LP_UAC Bypass via SDCLT	25
2.48	LP_Suspicious Binary Execution in User Directory	26
2.49	LP_Suspicious WMIC Child Process	26
2.50	LP_Suspicious File Execution Using Wscript or Cscript	27
2.51	LP_BCDEdit Safe Mode Command Execution	27
2.52	LP_Suspicious Encoded PowerShell Command Line	28
2.53	LP_Persistence Attack through Accessibility Process Feature	28
2.54	LP_Firewall Rule Addition via Netsh Detected	29
2.55	LP_MSHTA Spawned by SVCHOST Detected	29
2.56	LP_Exploitation of CVE-2019-1388 Detected	30
2.57	LP_Sophos EPP Registry Modification	30
2.58	LP_Office365 Inbox Rule with Special Characters Created	31
2.59	LP_Suspicious WerFault Process Creation	31
2.60	LP_Suspicious WerFault File Creation	31
2.61	LP_Snake Malware Covert Store Registry Key Detected	32
2.62	LP_Suspicious WerFault Service Creation	32
2.63	LP_Suspicious Named Pipe Connection to Azure AD Connect Database	33
2.64	LP_Suspicious Driver Loaded	33
2.65	LP_AADInternals PowerShell Cmdlet Execution	34
2.66	LP_Suspicious Scheduled Task Creation via Masqueraded XML File	34
2.67	LP_Suspicious Microsoft Equation Editor Child Process	35
2.68	LP_Windows Error Process Masquerading	35
2.69	LP_Bypass UAC via CMSTP Detected	35
2.70	LP_Application Whitelisting Bypass via Dxcap Detected	36
2.71	LP_Suspicious WMIC XSL Script Execution	36
2.72	LP_Suspicious File Execution via MSHTA	37
2.73	LP_Regsvr32 Anomalous Activity Detected	37
2.74	LP_Remote File Execution via MSIEXEC	38
2.75	LP_Execution of Trojanized 3CX Application	38

2.76	LP_Msbuild Spawned by Unusual Parent Process	39
2.77	LP_Suspicious Files Designated as System Files Detected	39
2.78	LP_Bypass User Account Control using Registry	40
2.79	LP_Unsigned Image Loaded Into LSASS Process	40
2.80	LP_Usage of Sysinternals Tools Detected	40
2.81	LP_Microsoft SharePoint Remote Code Execution Detected	41
2.82	LP_DenyAllWAF SQL Injection Attack	41
2.83	LP_Windows CryptoAPI Spoofing Vulnerability Detected	42
2.84	LP_Malicious use of Scriptrunner Detected	42
2.85	LP_Suspicious process related to Rundll32 Detected	43
2.86	LP_Javascript conversion to executable Detected	43
2.87	LP_Suspicious Execution of Gpscript Detected	44
2.88	LP_Proxy Execution via Desktop Setting Control Panel	44
2.89	LP_Xwizard DLL Side Loading Detected	44
2.90	LP_DLL Side Loading Via Microsoft Defender	45
2.91	LP_ZIP File Creation or Extraction via Printer Migration CLI Tool	45
2.92	LP_Credentials Capture via Rcping Detected	46
2.93	LP_Suspicious ConfigSecurityPolicy Execution Detected	46
2.94	LP_C-Sharp Code Compilation Using Ilasm Detected	47
2.95	LP_Process Dump via Resource Leak Diagnostic Tool	47
2.96	LP_Suspicious DLL execution via Register-Cimprovider	47
2.97	Accessibility features - Process	48
2.98	LP_Accessibility Features-Registry	48
2.99	LP_Active Directory DLLs Loaded By Office Applications	49
2.100	LP_DCSync detected	49
2.101	LP_Active Directory Replication User Backdoor	50
2.102	LP_Activity Related to NTDS Domain Hash Retrieval	50
2.103	LP_AD Object WriteDAC Access Detected	51
2.104	LP_AD Privileged Users or Groups Reconnaissance Detected	51
2.105	LP_Addition of SID History to Active Directory Object	52
2.106	LP_Admin User Remote Logon Detected	52
2.107	LP_Adwind RAT JRAT Detected	52
2.108	LP_Apache Struts 2 Remote Code Execution Detected	53
2.109	LP_AppCert DLLs Detected	53
2.110	LP_Application Shimming - File Access Detected	54
2.111	LP_Application Whitelisting Bypass via Dnx Detected	54
2.112	LP_Audio Capture Detected	55
2.113	LP_Authentication Package Detected	55
2.114	LP_Autorun Keys Modification Detected	56
2.115	LP_Bloodhound and Sharphound Hack Tool Detected	56
2.116	LP_BlueMashroom DLL Load Detected	57
2.117	LP_Remote Thread Creation via Cactustorch	57
2.118	LP_Call to a Privileged Service Failed	58
2.119	LP_Capture a Network Trace with netsh	58
2.120	LP_CEO Fraud - Possible Fraudulent Email Behavior	58

2.121LP_Certutil Encode Detected	59
2.122LP_Change of Default File Association Detected	59
2.123LP_Citrix ADC VPN Directory Traversal Detected	60
2.124LP_Clear Command History	60
2.125LP_Clearing of PowerShell Logs Detected	61
2.126LP_Clipboard Data Access Detected	61
2.127LP_Cmdkey Cached Credentials Recon Detected	62
2.128LP_CMSTP Detected	62
2.129LP_CMSTP Execution Detected	62
2.130LP_CMSTP UAC Bypass via COM Object Access	63
2.131LP_CobaltStrike Process Injection Detected	63
2.132LP_Windows Command Line Execution with Suspicious URL and AppData Strings	64
2.133LP_Compiled HTML File Detected	64
2.134LP_Console History Discovery Detected	65
2.135LP_Control Panel Items - Registry Detected	65
2.136LP_Copy from Admin Share Detected	66
2.137LP_Copying Sensitive Files with Credential Data	66
2.138LP_Copyright Violation Email	67
2.139LP_CreateMiniDump Hacktool Detected	67
2.140LP_CreateRemoteThread API and LoadLibrary	67
2.141LP_Command Obfuscation via Character Insertion	68
2.142LP_Command Obfuscation via Environment Variable Concatenation Reassembly	68
2.143LP_Credential Access via Input Prompt Detected	69
2.144LP_Credential Dump Tools Dropped Files Detected	69
2.145LP_Credential Dumping with ImageLoad Detected	70
2.146LP_Credentials Access in Files Detected	70
2.147LP_Registry Enumeration for credentials Detected	70
2.148LP_Default Account privilege elevation followed by restoration of previous account state	71
2.149LP_Default Blocked Inbound Traffic followed by Allowed Event	71
2.150LP_Default Blocked Outbound Traffic followed by Allowed Event	72
2.151LP_Default Brute Force Attack Successful	72
2.152LP_Default Connection Attempts on Closed Port	73
2.153LP_Default CPU Usage Status	73
2.154LP_Default Device Stopped Sending Logs for Half an Hour	74
2.155LP_Default DNS Tunneling Detection - Query Size	74
2.156LP_Default Excessive Blocked Connections	75
2.157LP_Default File Association Changed	75
2.158LP_Default Guest Account Added to Administrative Group	75
2.159LP_Default Inbound Connection with Non-Whitelist Country	76
2.160LP_Default Inbound RDP Connection	76
2.161LP_Default Inbound SMB Connection	77
2.162LP_Default Inbound SMTP Connection	77

2.163LP_Default Inbound SSH Connection	78
2.164LP_Default IRC connection	78
2.165LP_Default Malware Detected	78
2.166LP_Default Malware not Cleaned	79
2.167LP_Default Malware Removed	79
2.168LP_Default Memory Usage Status	80
2.169LP_Default Network Configuration Change on Network Device	80
2.170LP_Default Outbound Connection with Non-Whitelist Country	81
2.171LP_Default Outbound Traffic from Unusual Source	81
2.172LP_Default Port Scan Detected	81
2.173LP_Default Possible Cross Site Scripting Attack Detected	82
2.174LP_Default Possible Network Performance Degradation Detected	82
2.175LP_Default Possible Non-PCI Compliant Inbound Network Traffic Detected	83
2.176LP_Default Possible Spamming Zombie	83
2.177LP_Default Possible SQL Injection Attack	84
2.178LP_Default Possible System Instability State Detected	84
2.179LP_Default PowerSploit and Empire Schtasks Persistence	84
2.180LP_Default Successful Login outside Normal Hour	85
2.181LP_Default Successful Login Using a Default Account	85
2.182LP_Default System Time Change	86
2.183LP_Default TCP Probable SynFlood Attack	86
2.184LP_Default Unapproved Port Activity Detected	87
2.185LP_Default Unusual Number of Failed Vendor User Login	87
2.186LP_HandleKatz Duplicating LSASS Handle	88
2.187LP_PowerShell Execution Policy Modification Detected	88
2.188LP_Devtoolslauncher Executes Specified Binary	89
2.189LP_DHCP Callout DLL Installation Detected	89
2.190LP_DHCP Server Error Failed Loading the CallOut DLL	90
2.191LP_DHCP Server Loaded the CallOut DLL	90
2.192LP_Direct Autorun Keys Modification Detected	90
2.193LP_Disable of ETW Trace Detected	91
2.194LP_MiniNt Registry Key Addition	92
2.195LP_Discovery via Discovery via PowerSploit Recon Module Detected	92
2.196LP_DLL Load via LSASS Detected	93
2.197LP_DNS Server Error Failed Loading the ServerLevelPluginDLL	93
2.198LP_DNS ServerLevelPluginDll Install	94
2.199LP_Domain Trust Discovery Detected	94
2.200LP_dotNET DLL Loaded Via Office Applications	95
2.201LP_DPAPI Domain Backup Key Extraction Detected	95
2.202LP_DPAPI Domain Master Key Backup Attempt	95
2.203LP_Dridex Process Pattern Detected	96
2.204LP_Droppers Exploiting CVE-2017-11882 Detected	96
2.205LP_Drupal Arbitrary Code Execution Detected	97
2.206LP_Elevated Command Prompt Activity by Non-Admin User Detected	97
2.207LP EMC Possible Ransomware Detection	97

2.208LP_Empire PowerShell Launch Parameters	98
2.209LP_Empire PowerShell UAC Bypass Detected	98
2.210LP_Enabled User Right in AD to Control User Objects	99
2.211LP_PowerShell Encoded FromBase64String Detected	99
2.212LP_Encoded IEX Detected	100
2.213LP_Encoded PowerShell Command Detected	100
2.214LP_Eventlog Cleared Detected	101
2.215LP_Executables Stored in OneDrive	101
2.216LP_Execution in Non-Executable Folder Detected	101
2.217LP_Execution in Outlook Temp Folder Detected	102
2.218LP_Execution in Webserver Root Folder Detected	102
2.219LP_Execution of Renamed PaExec Detected	103
2.220LP_Execution via Control Panel Items	103
2.221LP_Execution via HTA using IE JavaScript Engine Detected	104
2.222LP_Execution via Squiblydoo Technique Detected	104
2.223LP_Execution via Windows Scripting Host Component Detected	105
2.224LP_Exim MTA Remote Code Execution Vulnerability Detected	105
2.225LP_Exim Remote Command Execution Detected	105
2.226LP_Existing Service Modification Detected	106
2.227LP_External Disk Drive or USB Storage Device Detected	106
2.228LP_Fail2ban IP Banned	107
2.229LP_File Creation by PowerShell Detected	107
2.230LP_File Deletion Detected	107
2.231LP_File or Folder Permissions Modifications	108
2.232LP_File System Permissions Weakness	108
2.233LP_Firewall Configuration Modification Detected	109
2.234LP_Firewall Disabled via Netsh Detected	109
2.235LP_First Time Seen Remote Named Pipe	110
2.236LP_FirstClass Failed Login Attempt	110
2.237LP_FirstClass Failed Password Change Attempt	111
2.238LP_Formbook Process Creation Detected	111
2.239LP_FortiGate Admin Login Disable	111
2.240LP_FortiGate Anomaly	112
2.241LP_FortiGate Antivirus Botnet Warning	112
2.242LP_FortiGate Antivirus Scan Engine Load Failed	112
2.243LP_FortiGate Attack	113
2.244LP_FortiGate Critical Events	113
2.245LP_FortiGate Data Leak Protection	113
2.246LP_FortiGate IPS Events	114
2.247LP_FortiGate Malicious URL Attack	114
2.248LP_FortiGate Virus	114
2.249LP_FortiGate VPN SSL User Login Failed	115
2.250LP_FromBase64String Command Line Detected	115
2.251LP_FSecure File Infection	116
2.252LP_FSecure Virus Detection	116

2.253LP_Fsutil Suspicious Invocation Detected	116
2.254LP_GAC DLL Loaded Via Office Applications Detected	117
2.255LP_Generic Password Dumper Activity on LSASS Detected	117
2.256LP_Grabbing Sensitive Hives via Reg Utility	117
2.257LP_Hacktool Ruler Detected	118
2.258LP_HH Execution Detected	118
2.259LP_Hidden Files and Directories Detected	119
2.260LP_Hiding Files with Attrib Detected	119
2.261LP_IIS Native-Code Module Command Line Installation	120
2.262LP_In-memory PowerShell Detected	120
2.263LP_Indicator Blocking - Driver Unloaded	121
2.264LP_Indicator Blocking - Sysmon Registry Edited	121
2.265LP_Install Root Certificate	122
2.266LP_Suspicious InstallUtil Execution	122
2.267LP_Invocation of Active Directory Diagnostic Tool Detected	123
2.268LP_Java Running with Remote Debugging	123
2.269LP_Judgement Panda Exfil Activity	123
2.270LP_JunOS Attack	124
2.271LP_JunOS Authentication Failed	124
2.272LP_JunOS Policy Violation	125
2.273LP_JunOS Security Log Clear	125
2.274LP_Kaspersky Antivirus - Outbreak Detection	125
2.275LP_Kaspersky Antivirus - Update Fail	126
2.276LP_Kaspersky Antivirus Extremely Out of Date Event	126
2.277LP_Kaspersky Antivirus Outbreak Detection by Source	127
2.278LP_Kaspersky Antivirus Outbreak Detection by Virus	127
2.279LP_Kaspersky Antivirus Threat Affecting Multiple Host	128
2.280LP_Kerberoasting via PowerShell Detected	128
2.281LP_Kernel Firewall Connection Denied	128
2.282LP_Koadic Execution Detected	129
2.283LP_Large ICMP Traffic	129
2.284LP_Local Account Creation on Workstation Detected	130
2.285LP_LockCrypt Ransomware	130
2.286LP_Log Files Creation of Dot-Net-to-JS Detected	131
2.287LP_LSASS Access from Non System Account Detected	131
2.288LP_LSASS Memory Dump Detected	131
2.289LP_LSASS Memory Dump File Creation	132
2.290LP_LSSAS Memory Dump with MiniDumpWriteDump API Detected . . .	132
2.291LP_Macro file Creation Detected	133
2.292LP_Malicious Base64 Encoded PowerShell Keywords in Command Lines Detected	133
2.293LP_Malicious File Execution Detected	134
2.294LP_Malicious Service Installations Detected	135
2.295LP_Malware Shellcode in Verclsid Target Process	135
2.296LP_Malware Threat Connection from Malicious Source	136

2.297LP_Malware Threat Connection to Malicious Destination	136
2.298LP_Malware Threat Connection to Malicious URLs	136
2.299LP_Malware Threat Emails Sent to Attacker	137
2.300LP_Meltdown and Spectre Vulnerabilities	137
2.301LP_Meterpreter or Cobalt Strike Getsystem Service Start Detected . . .	138
2.302LP_Microsoft ActiveX Control Code Execution Vulnerability Detected . .	138
2.303LP_Microsoft DotNET Framework Remote Code Execution Detected . .	139
2.304LP_Microsoft Office Memory Corruption Vulnerability CVE-2015-1641 Detected	139
2.305LP_Microsoft Office Memory Corruption Vulnerability CVE-2017-0199 Detected	139
2.306LP_Microsoft Office Memory Corruption Vulnerability CVE-2017-11882 Detected	140
2.307LP_Mimikatz Command Line Detected	140
2.308LP_Mitre Discovery Using Query Registry Detected	141
2.309LP_Mitre Discovery Using System Network Configuration Discovery Detected	141
2.310LP_Mitre Persistence via Winlogon Helper DLL Detected	142
2.311LP_MMC Spawning Windows Shell Detected	142
2.312LP_Most Exploitable Vulnerabilities Detected	143
2.313LP_Mshta JavaScript Execution Detected	143
2.314LP_MSHTA Spawning Windows Shell Detected	143
2.315LP_MSHTA Suspicious Execution Detected	144
2.316LP_MsiExec Web Install Detected	144
2.317LP_MSTSC Shadowing Detected	145
2.318LP_Multiple Failed Login Followed by Successful Login Followed by Logoff	145
2.319LP_Named Pipe added to Null Session Detected	146
2.320LP_Narrators Feedback-Hub Persistence Detected	146
2.321LP_Net exe Execution Detected	146
2.322LP_NetNTLM Downgrade Attack Detected	147
2.323LP_Netsh Port Forwarding Detected	147
2.324LP_Netsh RDP Port Forwarding Detected	148
2.325LP_Network Share Connection Removed	148
2.326LP_Network Share Discovery	149
2.327LP_Network Sniffing Detected	149
2.328LP_New Firewall Port Opening Detected	150
2.329LP_New RUN Key Pointing to Suspicious Folder Detected	150
2.330LP_New Service Creation	151
2.331LP_Non Interactive PowerShell Execution	151
2.332LP_NoPowerShell Tool Activity Detected	152
2.333LP_NotPetya Ransomware Activity Detected	152
2.334LP_Office365 Multiple Failed Login from Different Host by Single User .	153
2.335LP_Office365 Multiple Failed Login from Same Host	153
2.336LP_Office365 Multiple Successful Login from Different Country by Single User	154

2.337LP_Office365 Multiple Successful Login From Different Host by Single User	154
2.338LP_Office365 Password Resets	155
2.339LP_OpenWith Execution of Specified Binary Detected	155
2.340LP_Password Change on DSRM Account Detected	155
2.341LP_Password Dumper Remote Thread in LSASS	156
2.342LP_Password Spraying Attack Detected	156
2.343LP_Persistence and Execution at Scale via GPO Scheduled Task	157
2.344LP_Possible Access to ADMIN Share	157
2.345LP_Possible Account Misuse-Privilege Escalation	158
2.346LP_Possible Applocker Bypass Detected	158
2.347LP_Possible Bitsadmin Download Detected	159
2.348LP_Possible Botnet Connection-DNS Server Modified	159
2.349LP_Possible Botnet Connection-IRC Port	160
2.350LP_Possible Botnet Connection-Outbound DDOS	160
2.351LP_Possible Botnet Connection-Outbound Spam	160
2.352LP_Possible CLR DLL Loaded Via Office Applications	161
2.353LP_Possible Credential Dump-Tools Named Pipes Detected	161
2.354LP_Possible Data Breach	162
2.355LP_Possible Data Breach-Off Hour Transfer	162
2.356LP_Possible DDOS Attack	163
2.357LP_Possible Detection of SafetyKatz	163
2.358LP_Possible DNS Rebinding Detected	163
2.359LP_Possible Empire Monkey Detected	164
2.360LP_Possible Impacket Lateral Movement Detected	164
2.361LP_Possible Impacket SecretDump Remote Activity	165
2.362LP_Possible Inbound Spamming Detected	165
2.363LP_Possible Insider Threat	166
2.364LP_Malicious Payload Download via Office Binaries	166
2.365LP_Possible Malware Detected	167
2.366LP_Possible Modification of Boot Configuration	167
2.367LP_Possible Outbound Spamming Detected	168
2.368LP_Possible Pass the Hash Activity Detected	168
2.369LP_Possible Privilege Escalation via Weak Service Permissions	169
2.370LP_Possible Process Hollowing Image Loading	169
2.371LP_Possible SPN Enumeration Detected	169
2.372LP_Possible SquiblyTwo Detected	170
2.373LP_Possible Taskmgr run as LOCAL_SYSTEM Detected	170
2.374LP_Powershell AMSI Bypass via dotNET Reflection	171
2.375LP_PowerShell Base64 Encoded Shellcode Detected	171
2.376LP_PowerShell Network Connections Detected	172
2.377LP_PowerShell Profile Modification	172
2.378LP_PowerShell Rundll32 Remote Thread Creation Detected	173
2.379LP_PowerShell Script Run in AppData Detected	173
2.380LP_PowerShell Version Downgrade Detected	173
2.381LP_Process Dump via Comsvcs DLL Detected	174

2.382LP_Process Dump via Rundll32 and Comsvcs Detected	174
2.383LP_Process Hollowing Detected	175
2.384LP_Process Injection Detected	175
2.385LP_Protected Storage Service Access Detected	176
2.386LP_PsExec Tool Execution Detected	176
2.387LP_Psr Capture Screenshots Detected	177
2.388LP_Pulse Secure Arbitrary File Reading Detected	177
2.389LP_Query Registry Network	177
2.390LP_Rare Scheduled Task Creations Detected	178
2.391LP_RDP Login from Localhost Detected	178
2.392LP_RDP Over Reverse SSH Tunnel Detected	179
2.393LP_RDP Registry Modification	179
2.394LP_RDP Sensitive Settings Changed	179
2.395LP_Reconnaissance Activity with Net Command	180
2.396LP_RedSocks Backdoor Connection	180
2.397LP_RedSocks Bad Neighborhood Detection	181
2.398LP_RedSocks Blacklist URL Detection	181
2.399LP_RedSocks FileSharing	182
2.400LP_RedSocks Ransomware Connection	182
2.401LP_RedSocks Sinkhole Detection	182
2.402LP_RedSocks Tor Connection	183
2.403LP_RedSocks Trojan Connection	183
2.404LP_Register new Logon Process by Rubeus	184
2.405LP_Registry Persistence Mechanisms Detected	184
2.406LP_Regsvcs-Regasm Detected	185
2.407LP_Remote PowerShell Session	185
2.408LP_Remote System Discovery	185
2.409LP_Renamed Binary Detected	186
2.410LP_Renamed PsExec Detected	186
2.411LP_Rogue Access Point Detected	187
2.412LP_RSA SecurID Account Lockout	187
2.413LP_RSA SecurID Account Lockout	188
2.414LP_Rubeus Hack Tool Detected	188
2.415LP_Run PowerShell Script from ADS Detected	188
2.416LP_Rundll32 Internet Connection Detected	189
2.417LP_Scheduled Task Creation Detected	189
2.418LP_SCM Database Handle Failure Detected	190
2.419LP_SCM Database Privileged Operation Detected	190
2.420LP_Screensaver Activities Detected	191
2.421LP_Secure Deletion with SDelete	191
2.422LP_SecurityXploded Tool Detected	191
2.423LP_smbexec Service Installation Detected	192
2.424LP_SolarisLDAP Group Remove from LDAP Detected	192
2.425LP_SolarisLDAP Password Spraying Attack Detected	193
2.426LP_SolarisLDAP Possible Bruteforce Attack Detected	193

2.427LP_SolarisLDAP Successful Bruteforce Attack Detected	194
2.428LP_SolarisLDAP User Account Lockout Detected	194
2.429LP_Sophos XG Firewall - Inbound Attack Detected by IDP	195
2.430LP_Sophos XG Firewall - Outbound Attack Detected by IDP	195
2.431LP_SophosUTM Policy Violation	196
2.432LP_SSHD Connection Denied	196
2.433LP_Stealthy Scheduled Task Creation via VBA Macro Detected	197
2.434LP_Sticky Key Like Backdoor Usage Detected	197
2.435LP_Stop Windows Service Detected	198
2.436LP_Successful Lateral Movement to Administrator via Pass the Hash using Mimikatz Detected	198
2.437LP_Successful Overpass the Hash Attempt	199
2.438LP_Suspect Svchost Activity Detected	199
2.439LP_Suspect Svchost Memory Access	200
2.440LP_Suspicious Access to Sensitive File Extensions	200
2.441LP_Suspicious Calculator Usage Detected	200
2.442LP_Suspicious Call by Ordinal Detected	201
2.443LP_Suspicious Code Page Switch Detected	201
2.444LP_Suspicious Commandline Escape Detected	202
2.445LP_Suspicious Compression Tool Parameters	202
2.446LP_Suspicious Control Panel DLL Load Detected	203
2.447LP_Suspicious Csc Source File Folder Detected	203
2.448LP_Suspicious Debugger Registration Detected	204
2.449LP_Suspicious Double Extension Detected	204
2.450LP_Suspicious Driver Load from Temp	205
2.451LP_Suspicious Eventlog Clear or Configuration Using Wevtutil Detected .	205
2.452LP_Suspicious Execution from Outlook	206
2.453LP_Suspicious GUP Usage Detected	206
2.454LP_Suspicious HWP Sub Processes Detected	206
2.455LP_Suspicious In-Memory Module Execution Detected	207
2.456LP_Suspicious Kerberos RC4 Ticket Encryption	207
2.457LP_Suspicious MsiExec Directory Detected	208
2.458LP_Suspicious Named Pipes Detected	208
2.459LP_Suspicious Outbound Kerberos Connection	209
2.460LP_Suspicious Outbound RDP Connections Detected	209
2.461LP_Suspicious Parent of Csc Detected	210
2.462LP_Suspicious PowerShell Invocation Based on Parent Process	210
2.463LP_Suspicious PowerShell Parameter Substring Detected	211
2.464LP_Suspicious Process Start Locations Detected	211
2.465LP_Suspicious Program Location with Network Connections	212
2.466LP_Suspicious PsExec Execution Detected	212
2.467LP_Suspicious RDP Redirect Using TSCON Detected	212
2.468LP_Suspicious Remote Thread Created	213
2.469LP_Suspicious RUN Key from Download Detected	214
2.470LP_Suspicious Rundll32 Activity Detected	214

2.471LP_Suspicious Scripting in a WMI Consumer	215
2.472LP_Suspicious Service Path Modification Detected	215
2.473LP_Suspicious Svchost Process Detected	216
2.474LP_Suspicious TSCON Start	216
2.475LP_Suspicious Typical Malware Back Connect Ports Detected	217
2.476LP_Suspicious CSharp or FSharp Interactive Console Execution	217
2.477LP_Suspicious Userinit Child Process	218
2.478LP_Suspicious Windows ANONYMOUS LOGON Local Account Creation	218
2.479LP_Suspicious WMI Execution Detected	218
2.480LP_Svchost DLL Search Order Hijack Detected	219
2.481LP_SysKey Registry Keys Access	220
2.482LP_Sysmon Configuration Modification Detected	220
2.483LP_Sysmon Driver Unload Detected	220
2.484LP_Sysmon Error Event Detected	221
2.485LP_System File Execution Location Anomaly Detected	221
2.486LP_System Service Discovery	222
2.487LP_Tap Driver Installation Detected	222
2.488LP_Tasks Folder Evasion Detected	223
2.489LP_Terminal Service Process Spawn Detected	223
2.490LP_Threat Intel Allowed Connections from Suspicious Sources	224
2.491LP_Threat Intel Connections with Suspicious Domains	224
2.492LP_Time-Stomping of Users Directory Files Detected	225
2.493LP_Transferring Files with Credential Data via Network Shares	225
2.494LP_TrendMicroDeepSecurity Virus Quarantined	226
2.495LP_UAC Bypass via Event Viewer Detected	226
2.496LP_Unix Possible Bruteforce Attack	227
2.497LP_Unix User Deleted	227
2.498LP_Unsigned Driver Loading Detected	227
2.499LP_Possible Ursnif Registry Activity	228
2.500LP_VBA DLL Loaded by Office	228
2.501LP_VM - High Risk Vulnerability on High Impact Assets	229
2.502LP_VM - High Risk Vulnerability on Low Impact Assets	229
2.503LP_VM - High Risk Vulnerability on Medium Impact Assets	229
2.504LP_VM - Medium Risk Vulnerability on High Impact Assets	230
2.505LP_VM - Medium Risk Vulnerability on Low Impact Assets	230
2.506LP_VM - Medium Risk Vulnerability on Medium Impact Assets	231
2.507LP_WannaCry MS17-010 Vulnerable Sources	231
2.508LP_WannaCry Sources in Connections to Sinkhole Domain	232
2.509LP_WCE wceaux dll Access Detected	232
2.510LP_Wdigest Registry Modification	232
2.511LP_Weak Encryption Enabled for User	233
2.512LP_Potential Webshell Activity Detected	233
2.513LP_Windows Audit Logs Cleared	234
2.514LP_Windows Data Copied to Removable Device	234
2.515LP_Windows Defender Antivirus Disable via Registry Modification	235

2.516LP_Shadow Copy Deletion Using OS Utilities Detected	235
2.517LP_Windows Defender Exclusion Set Detected	236
2.518LP_Windows Excessive Amount of Files Copied to Removable Device . .	236
2.519LP_Windows Failed Login Attempt Using Service Account	237
2.520LP_Windows Failed Login Followed by Lockout Event	238
2.521LP_Windows Local User Management	238
2.522LP_WMI DLL Loaded by Office	239
2.523LP_Windows Processes Suspicious Parent Directory Detected	239
2.524LP_Windows Registry Persistence COM Key Linking Detected	240
2.525LP_Windows Shell Spawning Suspicious Program	240
2.526LP_Windows Suspicious Creation of User Accounts	241
2.527LP_Windows User Account Created via Command Line	241
2.528LP_Windows User Account Change to End with Dollar Sign	242
2.529LP_Windows Webshell Creation Detected	242
2.530LP_Winlogon Helper DLL	242
2.531LP_WMI Backdoor Exchange Transport Agent	243
2.532LP_WMI Modules Loaded by Suspicious Process	243
2.533LP_WMI Persistence - Script Event Consumer Detected	244
2.534LP_WMI Persistence - Script Event Consumer File Write	245
2.535LP_WMI Spawning Windows Shell	245
2.536LP_WMIExec VBS Script Detected	245
2.537LP_Wmiprvse Spawning Process	246
2.538LP_WScript or CScript Dropper Detected	246
2.539LP_Wsreset UAC Bypass Detected	247
2.540LP_XSL Script Processing Detected	247
2.541LP_ZOHO Dctask64 Process Injection Detected	248
2.542LP_APT 34 Initial Access Using Spearphishing Link Detected	248
2.543LP_Suspicious File Deletion Detected	249
2.544LP_Security Software Discovery Process Detected	249
2.545LP_System Network Configuration Discovery	250
2.546LP_System Network Connections Discovery	250
2.547LP_Exfiltration over Cloud Application Detected	251
2.548LP_Remote File Copy Detected	251
2.549LP_Privilege Escalation - Bypassing User Account Control Detected . . .	251
2.550LP_Process Execution from Suspicious Location	252
2.551LP_Active Directory Enumeration via ADFind	252
2.552LP_Possible Command Prompt Process Hollowing	253
2.553LP_Suspicious Taskkill Activity	253
2.554LP_Suspicious File or Directory Permission Modification	254
2.555LP_Ryuk Wake-On-LAN Activity	254
2.556LP_EXE or DLL Dropped in Perflogs Folder	255
2.557LP_Credential Access via LaZagne	255
2.558LP_RDP Connection Initiated from Domain Controller	255
2.559LP_Active Directory Module Load in PowerShell	256
2.560LP_Possible Active Directory Enumeration via AD Module	256

2.561LP_Microsoft Defender Disabling Attempt via PowerShell	257
2.562LP_Possible Kerberoasting via Rubeus	257
2.563LP_Suspicious Scheduled Task Creation	258
2.564LP_RDP Connection Initiated from Suspicious Country	258
2.565LP_Scheduled Task Deletion	259
2.566LP_Possible GootKit WScript Execution	259
2.567LP_Exchange Remote Code Execution CVE-2020-0688 Attempt	259
2.568LP_BlueKeep Vulnerability CVE-2019-0708 Exploitation	260
2.569LP_ZoHo ManageEngine Pre-Auth File Upload CVE-2019-8394 Exploitation Attempt	260
2.570LP_ZoHo ManageEngine Desktop Central CVE-2020-10189 Exploitation Attempt	261
2.571LP_Fortinet Pre-Auth File Read CVE-2018-13379 Exploitation Attempt	261
2.572LP_Adobe ColdFusion Remote Code Execution CVE-2018-15961 Attempt	262
2.573LP_Default Hard disk Usage Status	262
2.574LP_Default License Grace State	262
2.575LP_Default License Invalid	263
2.576LP_Microsoft Build Engine Loading Credential Libraries	263
2.577LP_Microsoft Build Engine started by Office	264
2.578LP_Potential Phishing Attack Detected	264
2.579LP_Safe DLL Search Mode Disabled	264
2.580LP_Potential Intrusion Detected	265
2.581LP_Windows Crash Dump Disabled	265
2.582LP_Suspicious Shells Spawn by SQL Server	266
2.583LP_Suspicious Microsoft SQL Server PowerShell Module Use Detected	266
2.584LP_HermeticWiper Driver Load	267
2.585LP_UltraVNC Execution via Command Line	267
2.586LP_Office Security Settings Changed	267
2.587LP_Actinium IoC Domains Detected	268
2.588LP_Suspicious VMToolsd Child Process	268
2.589LP_Impacket PsExec Execution	269
2.590LP_Oracle WebLogic CVE-2021-2109 Exploitation	269
2.591LP_Possible JSP Webshell Detected	269
2.592LP_PowerShell ADRecon Execution	270
2.593LP_PowerView PowerShell Commandlets	270
2.594LP_PowerView PowerShell Commandlets	271
2.595LP_Stealthy VSTO Persistence	272
2.596LP_Suspicious DLL or VBS Files being created in ProgramData	272
2.597LP_Suspicious VMToolsd Child Process	273
2.598LP_Suspicious WMPRVSE Child Process	273
2.599LP_TerraMaster TOS CVE-2020-28188 Exploitation	274
2.600LP_VMware VSphere CVE-2021-21972 Exploitation	274
2.601LP_VMware View Planner CVE-2021-21978 Exploitation	274
2.602LP_Zoho ManageEngine ADSelfService Plus CVE-2021-40539 Exploitation	275
2.603LP_Possible Access to ADMIN Share	275

2.604LP_PsExec Tool Execution Detected	276
2.605LP_Screensaver Activities Detected	276
2.606LP_Suspect Svchost Activity Detected	277
2.607LP_Time-Stomping of Users Directory Files Detected	277
2.608LP_Windows Defender Exclusion Set Detected	278
2.609LP_Suspicious Netsh DLL Persistence Detected	278
2.610LP_Usage of Procdump Detected	278
2.611LP_Conhost Spawning Suspicious Processes	279
2.612LP_Proxy Execution via Explorer	279
2.613LP_Wlrmldr Lolbin Use as Launcher	280
2.614LP_Suspicious Process Execution via Pester Detected	280
2.615LP_Root Certificate Installation Detected	280
2.616LP_Suspicious process spawned by FTP	281
2.617LP_Chromeloder Cross-Process Injection to Load Extention	281
2.618LP_Proxy Execution via Explorer	282
2.619LP_Suspicious Root Certificate installation Detected	282
2.620LP_Windows Logon Reminder Usage as Launcher	283
2.621LP_Suspicious File Transfer Using Replace	283
2.622LP_Proxy Execution via Program Compatibility Wizard	284
2.623LP_Suspicious Driver Installation via PnPUtil	284
2.624LP_Application Whitelisting Bypass via PresentationHost	285
2.625LP_Suspicious File Extraction via Expand Detected	285
2.626LP_Suspicious Use of Extrac32 Detected	286
2.627LP_Shell spawn via HTML Help Detected	286
2.628LP_DLL Injection with Tracker Detected	286
2.629LP_Powershell Code Execution via SyncAppvPublishingServer	287
2.630LP_Malicious PE Execution by Microsoft Visual Studio Debugger	287
2.631LP_Suspicious Atbroker Registry Change Detected	288
2.632LP_DLL loaded Via Certoc Binary Detected	288
2.633LP_Suspicious Remote Binary Usage Detected	289
2.634LP_Suspicious ASP NET Compiler Execution Detected	289
2.635LP_Suspicious LoadAssembly PowerShell Diagnostic Script Execution	290
2.636LP_Suspicious Invocation PowerShell Diagnostic Script Execution	290
2.637LP_Registry Configured RunOnce Task Execution	291
2.638LP_RunOnce Registry Key Configuration Change	291
2.639LP_Suspicious WSL Bash Execution	292
2.640LP_WSL Execution Detected	292
2.641LP_Supsicious Usage of Csharp or Roslyn Csharp Interactive Console	292
2.642LP_Possible Commandline Obfuscation Detected	293
2.643LP_Possible Emotet Activity Detected	293
2.644LP_Suspicious Use of Control Panel Items	294
2.645LP_Suspicious Use of CSharp Interactive Console Detected	294
2.646LP_Suspicious Use of Colorcpl Detected	295
2.647LP_Suspicious File Download via Certreq	295
2.648LP_Process Dump via Rundll32 and Comsvcs	296

2.649LP_Registry Key Import Detected	296
2.650LP_Suspicious MachineGUID Query Detected	297
2.651LP_Process Injection Via Mavinject Detected	297
2.652Possible File Transfer Using Finger Detected	298
2.653LP_Suspicious Use of Findstr Detected	298
2.654LP_Suspicious File Overwrite Using extrac32 Detected	298
2.655LP_Suspicious Sysmon Driver Unload Detected	299
2.656LP_Suspicious Execution via IE per User Utility	299
2.657LP_Proxy Execution via xWizard	300
2.658LP_Suspicious MSHTA Process Pattern	300
2.659LP_COM Object Execution via Shell Extension CLSID Verification Host	301
2.660LP_Suspicious Setup Information File Invoked via DefaultInstall	301
2.661LP_Creation of Alternate Data Stream	302
2.662LP_Alternate Data Stream Created using Findstr	302
2.663LP_Suspicious Download Using Diantz	303
2.664LP_Ngrok RDP Tunnel Detected	303
2.665LP_Ngrok Execution	304
2.666LP_Windows Defender Uninstall via PowerShell	304
2.667LP_Hijacked Binary Execution via Settings Synchronizer	305
2.668LP_Suspicious Execution of Dump64	305
2.669LP_Code Compilation via Visual Basic Command Line Compiler	306
2.670LP_File Downloaded from Suspicious URL Using GfxDownloadWrapper	306
2.671LP_Suspicious CLR Logs File Creation	307
2.672LP_CLR DLL Loaded via Scripting Application	307
2.673LP_Obfuscation Script Usage via MSHTA to Execute Vbscript	308
2.674LP_Microsoft Defender Logging Disabled	308
2.675LP_UAC Bypass via CMLUA or CMSTPLUA	309
2.676LP_High Number of Service Stop or Task Kill in Short Span	309
2.677LP_LSA Protected Process Light Disabled	310
2.678LP_Suspicious Invocation of Microsoft Workflow Compiler	310
2.679LP_Process Dump via Sqldumper Detected	311
2.680LP_Suspicious Usage of SQLToolsPS Detected	311
2.681LP_Proxy Execution of Malicious Payload via Pubprn	312
2.682LP_File Download via IMEWDBLD	312
2.683LP_Memory Dump via Adplus	312
2.684LP_Remote Thread Created via Ttdinject	313
2.685LP_Proxy Download via OneDriveStandaloneUpdater	313
2.686LP_Suspicious WMIC ActiveScriptEventConsumer Created	314
2.687LP_Remote Connection Established via Msbuild	314
2.688LP_Executables Started in Suspicious Folder	315
2.689LP_Windows RDP Port Modified	315
2.690LP_Curl Silent Mode Execution Detected	316
2.691LP_High Volume of File Modification or Deletion in Short Span	316
2.692LP_Non-Existent User Login Attempt Detected	317
2.693LP_Execution of Temporary Files Via Office Application	317

2.694LP_Execution of Temporary Files Via Office Application	317
2.695LP_Malicious Image Loaded Via Excel	318
2.696LP_Malicious Chrome Extension Detected	318
2.697LP_Chrome Extension Installed Outside of the Webstore	319
2.698LP_Chrome Extension Installed with DevTools Permission	319
2.699LP_Suspicious WMIC Process Creation	320
2.700LP_Browser Credential Files Accessed	320
2.701LP_Windows Defender Antivirus Definitions Removal Detected	321
2.702LP_Exchange ProxyShell Pattern Detected	321
2.703LP_Successful Exchange ProxyShell Attack	322
2.704LP_Malicious Base64 Encoded PowerShell Keywords in Command Lines Detected	322
2.705LP_DLL Loaded Via AllocConsole and RunDLL32	323
2.706LP_Active Directory Database Dump Attempt	324
2.707LP_Suspicious Child Process Creation via OneNote	324
2.708LP_Usage of Web Request Command	325
2.709LP_Reconnaissance Activity with Nltest	326
2.710LP_Regsvr32 Network Activity Detected	326
2.711LP_Possible Reconnaissance Activity	327
2.712LP_Privilege Escalation via Kerberos KrbRelayUp	327
2.713LP_Suspicious Execution of LNK File	328
2.714LP_Insecure Policy Set via Set-ExecutionPolicy	328
2.715LP_Network Connection to Suspicious Server	329
3 NON-MITRE ATT&CK Analytics	330
3.1 LP_Windows Login Attempt on Disabled Account	330
3.2 LP_VMware Link Up	330
3.3 LP_VMware Link Down	331
3.4 LP_LogPoint License Expiry Status	331
3.5 LP_Mitre Initial Access Using Spearphishing link Detected	331
3.6 LP_Mitre Command and Control Using Standard Application Layer Protocol Detected	332
3.7 LP_Endpoint Protect Threat Content Detected	332
3.8 LP_Endpoint Protect Device Disconnect	333
3.9 LP_Endpoint Protect File Delete	333
3.10 LP_Endpoint Protect File Copied To USB Device	333
3.11 LP_System Owner or User Discovery Process Detected	334
3.12 LP_System Services Discovery Detected	334
3.13 LP_SolarisLDAP Password Spraying Attack Detected	335
3.14 LP_Microsoft Defender AMSI Trigger	335
3.15 LP_Petitpotam - Anonymous RPC and File Share	336
3.16 LP_RDP Sensitive Settings Changed	336
3.17 LP_Secure Deletion with SDelete	336
3.18 LP_Suspicious Keyboard Layout Load Detected	337
3.19 LP_Remote Code Execution using WMI Win32_Process Class over WinRM	337

3.20	LP_Remote Code Execution using WMI Win32_Service Class over WinRM	338
3.21	LP_Suspicious Microsoft SQL Server PowerShell Module Use Detected	338
3.22	LP_Shadow Copy Deletion Using OS Utilities Detected	339
3.23	LP_Child Process Spawned via Diskshadow Detected	339
3.24	LP_Code Execution Via Diskshadow Detected	340
3.25	LP_Process Pattern Match For CVE-2021-40444 Exploitation	340
3.26	LP_Suspicious Extexport Execution Detected	341
3.27	LP_Proxy Execution via Workfolders	341
3.28	LP_Proxy Execution via Windows Update Client	342
3.29	LP_Suspicious DLL Execution Using Windows Address Book	342
3.30	LP_Suspicious Use of Dotnet Detected	343
3.31	LP_Execution of Arbitrary Executable Using Storddiag	343
3.32	LP_Process Creation via Time Travel Tracer	344
3.33	LP_Time Travel Debugging Utility DLL Loaded	344
3.34	LP_File Execution via Msdeploy	344
3.35	LP_CVE-2022-40684 Exploitation Detected	345
3.36	LP_Possible Proxy Execution of Malicious Code	345
3.37	LP_Suspicious Usage of BitLocker Management Script	346
3.38	LP_Proxy Execution of Payloads via Microsoft Signed Script	346
3.39	LP_Execution of Windows Defender Offline Shell from Suspicious Folder	347
3.40	LP_DLL Loaded Via AccCheckConsole	347
3.41	LP_Proxy Execution via Appvlp	348
3.42	LP_Proxy DLL Execution via UtilityFunctions	348
3.43	LP_Suspicious Usage of Squirrel Binary	348
3.44	LP_Suspicious File Share Permission	349
3.45	LP_Legitimate Application Dropping Script File	349
4	Alert Rules Dashboards	351
4.1	LP_Mitre Attack Analytics Overview	351
4.2	Adding the Alert Rules Dashboard	351
5	KB-Lists	355

s.. Logpoint Documentation documentation master file, created by
sphinx-quickstart on Wed Aug 3 14:33:36 2011.

ALERT RULES

Alert Rules consists of alert packages, the *LP_Mitre Attack Analytics Overview* dashboard package and *Knowledge Base (KB) Lists* for analytics integrated into Logpoint. It provides a compliance and triage dashboard, enabling you to analyze trends and behaviors of entities and users within the organization and perform defensive gap assessment with MITRE ATT&CK. The alerts triggered by Logpoint are categorized based on the [MITRE ATT&CK](#) framework and are the starting point to build various detection techniques. When Logpoint identifies threats within your environment, it triggers security alerts based on predetermined rules, allowing you to detect the malicious activity, advanced malware and their Techniques, Tactics and Procedures (TTPs) early, so you can take corrective actions against them. You can customize dashboards and alerts to suit your needs and perform in-depth analysis with customized data and searches.

Logpoint's [ATT&CK navigator](#) shows the coverage of the ATT&CK framework in Logpoint. You can use the navigator to match Logpoint alerts with the relevant ATT&CK techniques and tactics. Read more about MITRE ATT&CK techniques and tactics in addition to their integration in Logpoint on the [Logpoint website](#).

Alert Rules Component

1. Alert Packages

- [MITRE ATT&CK Analytics](#)
- [NON-MITRE ATT&CK Analytics](#).

Required Log Source

MITRE ATT&CK Analytics

- Windows Security Audit
- Windows Sysmon

Default Alert Rules

- All applicable log sources

MITRE ATT&CK ANALYTICS

The MITRE ATT&CK alerts available in Alert Rules are:

2.1 LP_Unsigned DLLs loaded by RunDLL32 or RegSvr32

- **Trigger Condition:** Injection of unsigned dynamic-link library (DLL), a common tactic attackers use to execute arbitrary code on Windows systems. Adversaries often leverage Windows builtin tools like RunDLL32 or RegSvr32 to execute the malicious code through unsigned or untrusted DLLs.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Regsvr32, Rundll32
- **ATT&CK ID:** T1218.010, T1218.011
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label=Image label=Load "process" IN ["*\regsvr32.exe", "*\rundll32.exe"] (-is_signed=  
→ "true" OR status IN ["errorChaining", "errorCode_endpoint*", "errorExpired", "trusted  
→ "])
```

2.2 LP_Terminal Service Configuration Modified

- **Trigger Condition:** Modifying settings related to terminal services. Adversaries can use this technique to bypass authentication requirements or bypass security settings.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Modify Registry

- **ATT&CK ID:** T1112
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
(label="Registry" label=Set target_object IN ["*Software\Microsoft\Terminal Server Client*",
↳ "*Software\Policies\Microsoft\Windows NT\Terminal Services\"]) target_object IN [
↳ "*AuthenticationLevelOverride*", "*DisableRemoteDesktopAntiAlias*",
↳ "*DisableSeucirtySettings*"]) OR (label="Process" label=Create "process"="*\reg.exe"
↳ command="*add*" command IN ["*Software\Microsoft\Terminal Server Client*",
↳ "*Software\Policies\Microsoft\Windows NT\Terminal Services\"]) command IN [
↳ "*AuthenticationLevelOverride*", "*DisableRemoteDesktopAntiAlias*",
↳ "*DisableSeucirtySettings*"])
```

2.3 LP_System Service Reconnaissance through WMI

- **Trigger Condition:** Usage of WMI for service reconnaissance is detected. Adversaries might use WMI to check if a specific service is running on a host to gather reconnaissance information, identify potential vulnerabilities, plan further actions and maintain persistence within the target network.
- **ATT&CK Category:** Execution, Discovery
- **ATT&CK Tag:** System Service Discovery, Windows Management Instrumentation
- **ATT&CK ID:** T1007, T1047
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create ("process"="*\wmic.exe" OR file="wmic.exe") command=
↳ "*service*" -command IN ["*assoc*", "*call*", "*create*", "*delete*"]
```

2.4 LP_Suspicious Msiexec Child Process

- **Trigger Condition:** Suspicious child processes spawned via Msiexec. Adversaries often use MSI files for initial access due to their legitimate appearance, making them less likely to raise suspicion when delivered through phishing or other social engineering tactics.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Msiexec

- **ATT&CK ID:** T1218.007
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "parent_process"="*\msiexec.exe" "process" IN ["*\cmd.
↪exe", "powershell.exe", "icacls.exe", "expand.exe", "rundll32.exe"]
```

2.5 LP_Process Reconnaissance through WMI

- **Trigger Condition:** Usage of WMI for listing processes running on the compromised host. Adversaries might use WMI to list all the running processes on the host to bypass security measures.
- **ATT&CK Category:** Execution, Discovery
- **ATT&CK Tag:** Windows Management Instrumentation, System Service Discovery
- **ATT&CK ID:** T1047, T1007
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create("process"="*\wmic.exe" OR file="wmic.exe") command=
↪"*process*" -command IN ["*assoc*", "*call*", "*create*", "*delete*"]
```

2.6 LP_Process Created through WMI

- **Trigger Condition:** Usage of WMI to spawn new processes either on local or remote hosts. Adversaries use WMI to spawn new processes because it provides them with a stealthy, persistent and flexible means of executing malicious code, bypassing security controls and maintaining control over compromised systems.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Windows Management Instrumentation
- **ATT&CK ID:** T1047
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create ("process"="*\wmic.exe" OR file="wmic.exe") command=
↳ "*process*" command="*call*" command="*create*"
```

2.7 LP_Local Users Reconnaissance through WMI

- **Trigger Condition:** Usage of Windows Management Instrumentation (WMI) to list all local user accounts. Adversaries might use WMI to list all local user accounts rather than a straightforward command like net user for defense evasion.
- **ATT&CK Category:** Execution, Discovery
- **ATT&CK Tag:** Windows Management Instrumentation, Local Account
- **ATT&CK ID:** T1047, T1087.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create ("process"="*\wmic.exe" OR file="wmic.exe") command=
↳ "*useraccount*"
```

2.8 LP_Installed Software Updates Reconnaissance through WMI

- **Trigger Condition:** Usage of Windows Management Instrumentation (WMI) to list installed software hotfixes and patches. Adversaries might use WMI to gather information about target systems, identify vulnerabilities and plan attack strategies.
- **ATT&CK Category:** Execution, Discovery
- **ATT&CK Tag:** Windows Management Instrumentation, Software Discovery
- **ATT&CK ID:** T1047, T1518
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create ("process"="*\wmic.exe" OR file="wmic.exe") command=
↳ "*qfe*"
```

2.9 LP_Application uninstall via WMIC

- **Trigger Condition:** Uninstallation of applications on a system using the Windows Management Instrumentation Command-line (WMIC) tool is detected. This uninstallation method is commonly observed in Advanced Persistent Threat (APT) activities, where adversaries aim to remove security products installed on target systems to evade detection and maintain persistence.
- **ATT&CK Category:** Execution, Defense Evasion
- **ATT&CK Tag:** Windows Management Instrumentation, Disable or Modify Tools
- **ATT&CK ID:** T1047, T1562.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create ("process"="*\wmic.exe" OR file="wmic.exe") command=
↳ "*product*" command="*call*" command="*uninstall*"
```

2.10 LP_Applnit DLLs Detected

- **Trigger Condition:** Adversaries establish persistence and/or elevate privileges by executing malicious content triggered by Applnit DLLs loaded into processes.
- **ATT&CK Category:** Persistence, Privilege Escalation
- **ATT&CK Tag:** Event Triggered Execution, Applnit DLLs
- **ATT&CK ID:** T1546, T1546.010
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon (event_id=12 or event_id=13 or event_id=14) (target_object=
↳ "*\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\Appinit_Dlls\*" or
↳ target_object="*\SOFTWARE\Wow6432Node\Microsoft\Windows
↳ NT\CurrentVersion\Windows\Appinit_Dlls\*") -user IN EXCLUDED_USERS
```

2.11 LP_High Severity EPP Alert

- **Trigger Condition:** High or critical severity alert is generated by any endpoint protection platform like CrowdStrike and Microsoft Defender for Endpoint.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** CrowdStrikeEPO, Microsoft Defender ATP
- **Query:**

```
norm_id=* device_category=EPP log_level IN [ "High", "Critical"]
```

2.12 LP_Host Generating Multiple Medium Severity EPP Alert

- **Trigger Condition:** Multiple medium severity alerts are generated by endpoint protection platforms like CrowdStrike and Microsoft Defender for Endpoint.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** CrowdStrikeEPO, Microsoft Defender ATP
- **Query:**

```
norm_id=* device_category=EPP log_level="Medium" | chart distinct_count(detection_↪id) as DC by host_id | search DC > 1
```

2.13 LP_Host Generating Multiple High Severity EPP Alert

- **Trigger Condition:** Multiple high or critical severity alerts are generated by endpoint protection platforms like CrowdStrike and Microsoft Defender for Endpoint.
- **ATT&CK Category:** -

- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** CrowdStrikeEPO, Microsoft Defender ATP
- **Query:**

```
norm_id=* device_category=EPP log_level IN ["high", "critical"] | chart distinct_
↪ count(detection_id) as DC by host_id | search DC > 1
```

2.14 LP_Medium Severity EPP Alert

- **Trigger Condition:** Medium severity alert is generated by any endpoint protection platform like Crowdstrike and Microsoft Defender for Endpoint.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** CrowdStrikeEPO, Microsoft Defender ATP
- **Query:**

```
norm_id=* device_category=EPP log_level="Medium"
```

2.15 LP_Windows Service Stop or Delete

- **Trigger Condition:** Windows service or process being stopped, deleted or disabled via system binaries is detected. `sc.exe`, `net.exe` and `net1.exe` are Microsoft Windows system internal binaries that adversaries can use to stop or delete services and processes to render those services unavailable to legitimate users or to avoid hindrances in their attack chain.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Service Stop
- **ATT&CK ID:** T1489
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create ("process" IN ["*\sc.exe", ".*\net.exe", ".*\net1.exe"]  
↪ command="*stop*") OR ("process"="*\sc.exe" command IN ["*delete*", ".*disabled*  
↪"]) -user IN EXCLUDED_USERS
```

2.16 LP_Suspicious Hack Tools Execution

- **Trigger Condition:** Execution of different Windows-based hack tools via their import hash (imphash) is detected, even if the files have been renamed. The MALICIOUS_TOOLS_IMPHASH list must be imported before activating this alert.
- **ATT&CK Category:** Credential Access, Resource Development
- **ATT&CK Tag:** OS Credential Dumping, Tool
- **ATT&CK ID:** T1003, T1588.002
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 hash_import IN MALICIOUS_TOOLS_IMPHASH
```

2.17 LP_Suspicious Execution of XORDump Utility for LSASS Memory Dump

- **Trigger Condition:** Suspicious execution of XORDump Utility, commonly used for LSASS Memory Dump, is detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** LSASS Memory
- **ATT&CK ID:** T1003.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create "process"="*\xordump.exe" OR command IN ["* -process  
↪ lsass.exe *", ".* -m comsvcs *", ".* -m dbghelp *", ".* -m dbgcore *"]
```

2.18 LP_Suspicious Execution of Createdump Utility for Memory Dump

- **Trigger Condition:** Usage of the *createdump.exe* LOLOBIN utility to dump process memory is detected. Adversaries often seek to dump the *lsass.exe* process memory because it contains sensitive information, such as user credentials and authentication tokens.
- **ATT&CK Category:** Credential Access, Defense Evasion
- **ATT&CK Tag:** LSASS Memory, Masquerading
- **ATT&CK ID:** T1003.001, T1036
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create "process"="*\createdump.exe" OR file="FX_VER_
↪INTERNALNAME_STR" command IN ["* -u *", "* -full *", "* -f *", "* --name *", "*.dmp*
↪"]
```

2.19 LP_Suspicious DsInternals Get-ADReplAccount Activities

- **Trigger Condition:** Suspicious activities related to Get-ADReplAccount from the DsInternals PowerShell Module are detected. Adversaries may use this tool to maliciously access Domain Controllers' credentials. For event id 4104, Powershell Script Block logging is required.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** DCSync
- **ATT&CK ID:** T1003.006
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
(label="process" label=create command="*Get-ADReplAccount*" command="*-All*"
↪command="*Server*") OR (norm_id=WinServer event_id=4104 script_block="*Get-
↪ADReplAccount*" script_block="*-All*" script_block="*Server*")
```

2.20 LP_Suspicious Activities Associated with NTDS Exfiltration

- **Trigger Condition:** Suspicious activities related to the Active Directory Domain Database (ntds.dit) are detected. Adversaries may attempt to access or create a copy of the Active Directory domain database to steal credential information and obtain information about domain members, such as devices, users and access rights.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** NTDS
- **ATT&CK ID:** T1003.003
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create ("process" IN ["*\\NTDSDump.exe", "*\\NTDSDumpEx.exe"
↪"]) OR (command="*ntds.dit*" command="*system.hive*") OR (command=
↪"*NTDSgrab.ps1*") OR (command="*ac i ntds*" command="*create full*") OR
↪(command="*/c copy*" command="*\\windows\\ntds\\ntds.dit*") OR (command=
↪"*activate instance ntds*" command="*create full*") OR (command="*powershell*"
↪command="*ntds.dit*") OR (command="*ntds.dit*" (parent_process IN ["*\\apache*",
↪"*\\tomcat*", "*\\AppData*", "*\\Temp\\*", "*\\Public\\*", "*\\PerfLogs\\*"] OR "process" IN [
↪"*\\apache*", "*\\tomcat*", "*\\AppData*", "*\\Temp\\*", "*\\Public\\*", "*\\PerfLogs\\*"])))
```

2.21 LP_Possible LSASS Memory Dump Via Windows Task Manager

- **Trigger Condition:** Creation of a *lsass.dmp* file by the taskmgr process is detected. Adversaries often seek to dump the *lsass.exe* process memory because it contains sensitive information, such as user credentials and authentication tokens.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** LSASS Memory
- **ATT&CK ID:** T1003.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=11 "process"="*\taskmgr.exe" path=
↳ "\Appdata\local\*" file="lsass*.dmp"
```

2.22 LP_Possible LSASS Dump Via SilentProcessExit Technique

- **Trigger Condition:** Dumping of a possible LSASS via the SilentProcessExit Technique is detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** LSASS Memory
- **ATT&CK ID:** T1003.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id IN [12,13,14] target_object="*Microsoft\Windows
↳ NT\CurrentVersion\SilentProcessExit\lsass.exe"
```

2.23 LP_NTDS or SAM Database Copy Operation

- **Trigger Condition:** Copy operation of Active Directory Domain Database (ntds.dit) or Security Account Manager (SAM) files is detected. Adversaries may attempt to access or create a copy of the Active Directory domain database or SAM database to steal credential information and obtain other information about domain members, such as devices, users and access rights.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** OS Credential Dumping, Security Account Manager, NTDS
- **ATT&CK ID:** T1003, T1003.002, T1003.003
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create (command IN ["*copy*", "*xcopy*", "*Copy-Item*",
↳ "*move*", "*cp*", "*mv*"] OR "process"="*\esentutl.exe" command IN ["*/y*", "*/vss*
↳ ", "*/d*"]) command IN ["*\NTDS.dit",
↳ "*\\GLOBALROOT\\Device\\HarddiskVolumeShadowCopy*", "*\\SYSTEM*",
↳ "*\\SECURITY*", "*C:\\tmp\\log*", "**\\config\\SAM", "*/system32/config/SAM*"]
```

2.24 LP_Microsoft IIS Service Account Password Dumped

- **Trigger Condition:** Execution of Information Services (IIS) command-line tool AppCmd to list passwords is detected. An attacker with IIS web server access via a web shell can decrypt and dump the IIS AppPool service account password using AppCmd.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** OS Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create ("process" = "*\appcmd.exe" or file=appcmd.exe)
↪ command="*list*" (command IN ["*/config*", "*/xml*", "*/-config*", "*/-xml*"]) OR
↪ (command IN ["*/@t'", "*/text*", "*/show*", "*/-@t'", "*/-text*", "*/-show*",
↪ "*/password*", "*/.*"])
```

2.25 LP_Dumpert Process Dumper Execution

- **Trigger Condition:** Dumping of a possible credential via a tool called NPPSpy is detected. NPPSpy is a Network Provider/Credential Manager DLL that extracts credentials and stores them in plain text. This alert monitors file creation, registry manipulation and process creation events that indicate a potential credential dump via NPPSpy.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** LSASS Memory
- **ATT&CK ID:** T1003.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 hash_import=
↪ "09D278F9DE118EF09163C6140255C690" or command="*Dumpert.dll*"
```

2.26 LP_Credential Dump Via NPPSpy

- **Trigger Condition:** Dumping of a possible credential via a tool called NPPSpy is detected. NPPSpy is a Network Provider/Credential Manager DLL that extracts credentials and stores them in plain text. This alert monitors file creation, registry manipulation and process creation events that indicate a potential credential dump via NPPSpy.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** OS Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
(label=Registry label=Set target_object IN ["*\System\CurrentControlSet\Services\*",
↪ "*CurrentControlSet\Control\*" ] target_object="*\NetworkProvider*" -(target_object
↪ IN ["*\System\CurrentControlSet\Services\WebClient\NetworkProvider*",
↪ "*\System\CurrentControlSet\Services\LanmanWorkstation\NetworkProvider*",
↪ "*\System\CurrentControlSet\Services\RDPNP\NetworkProvider*"] OR "process"=
↪ "C:\Windows\System32\poqexec.exe")) OR (label=file label=create file IN ["NPPSpy.txt",
↪ "NPPSpy.dll"]) OR (label="process" label=create command=
↪ "*\System\CurrentControlSet\Services\*" command="*\NetworkProvider*" )
```

2.27 LP_Malicious PowerShell Commandlets Detected

- **Trigger Condition:** Commandlet names from well-known Command and Scripting Interpreter, PowerShell exploitation frameworks are detected. The MALICIOUS_POWERSHELL_COMMANDLET_NAMES list must be imported for this alert to work correctly.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** PowerShell
- **ATT&CK ID:** T1059.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
command IN MALICIOUS_POWERSHELL_COMMANDLET_NAMES -command="*Get-
↪ SystemDriveInfo*" OR script_block IN MALICIOUS_POWERSHELL_COMMANDLET_
↪ NAMES -script_block="*Get-SystemDriveInfo"
```

2.28 LP_Code Execution Via Diskshadow Detected

- **Trigger Condition:** Usage of diskshadow binary to execute code from a file is detected. Adversaries can use diskshadow with -s or /s tag to execute a command from a file and bypass detection.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*\diskshadow.exe" command IN ["*/s *", "*-s *
↪ "]
```

2.29 LP_Image Mount Indicator in Recent Files

- **Trigger Condition:** Recent element files pointing to .iso, .img, .vhd or .vhdx files are detected. These image files are used in phishing attacks to deliver malware and circumvent the Mark of the Web (MotW) in Windows to execute malicious commands. It is a false positive on server systems, but on workstations, users rarely mount .iso or .img files.
- **ATT&CK Category:** Initial Access, Defense Evasion
- **ATT&CK Tag:** Mark-of-the-Web Bypass, Spearphishing Attachment
- **ATT&CK ID:** T1553.005, T1566.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id="WindowsSysmon" event_id=11 path="*\Microsoft\Windows\Recent\*" file IN [
↪ "*.iso.lnk", "*.img.lnk", "*.vhd.lnk", "*.vhdx.lnk"]
```

2.30 LP_Disk Image File Created

- **Trigger Condition:** Image files with extensions like .iso, .vhd, and .vhdx are downloaded from the internet into a user's download or temporary folder. Adversaries often deliver their malware payloads through a .iso file format to bypass the Mark of the Web (MotW) in Windows and execute their payload successfully.
- **ATT&CK Category:** Initial Access, Defense Evasion
- **ATT&CK Tag:** Mark-of-the-Web Bypass, Spearphishing Attachment
- **ATT&CK ID:** T1553.005, T1566.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id="WindowsSysmon" event_id=11 (path="*Users*" path="*Downloads*") OR
↪(path="*Appdata*") file IN ["*.iso", "*.vhd", "*.vhdx", "*.img"]
```

2.31 LP_PowerShell Execution via DLL Detected

- **Trigger Condition:** Execution of PowerShell via DLL instead of powershell.exe is detected. Powershell is a command-line shell used in Windows. Adversaries can execute PowerShell for malicious activities even if powershell.exe is blocked and no strict application whitelisting is implemented.
- **ATT&CK Category:** Execution, Defense Evasion
- **ATT&CK Tag:** PowerShell, Rundll32
- **ATT&CK ID:** T1059.001, T1218.011
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create ("process" IN ["*\\rundll32.exe", "*\\regsvcs.exe",
↪"*\\InstallUtil.exe", "*\\regasm.exe"] OR file in ["RUNDLL32.EXE", "RegSvcs.exe", "InstallUtil.
↪exe", "RegAsm.exe"]) command IN ["*Default.GetString*", "*FromBase64String*",
↪"*Invoke-Expression*", "*IEX *", "*Invoke-Command*", "*ICM *", "*DownloadString*"]
```

2.32 LP_Suspicious Windows Defender Registry keys Modification

- **Trigger Condition:** Changes in the Windows Defender registry settings to disable Windows Defender functionalities. Adversaries try to alter Windows Defender-associated registries to disable protection and detection features.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Disable or Modify Tools
- **ATT&CK ID:** T1562.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label=registry label=set target_object IN ["*\SOFTWARE\Microsoft\Windows Defender*",
↪  "\SOFTWARE\Policies\Microsoft\Windows Defender"] ( detail="DWORD(
↪  0x00000001)" target_object IN ["*\DisableAntiSpyware", "\DisableAntiVirus",
↪  "\DisableBehaviorMonitoring", "\DisableIntrusionPreventionSystem",
↪  "\DisableIOAVProtection", "\DisableOnAccessProtection",
↪  "\DisableRealtimeMonitoring", "\DisableScanOnRealtimeEnable",
↪  "\DisableScriptScanning", "\DisableEnhancedNotifications",
↪  "\DisableBlockAtFirstSeen"] ) OR ( detail="DWORD(0x00000000)" target_object IN [
↪  "\App and Browser protection\DisallowExploitProtectionOverride",
↪  "\Features\TamperProtection", "\MpEngine\MpEnablePus", "\PUAProtection",
↪  "\Signature Update\ForceUpdateFromMU", "\SpyNet\SpynetReporting",
↪  "\SpyNet\SubmitSamplesConsent", "\Windows Defender Exploit Guard\Controlled
↪  Folder Access\EnableControlledFolderAccess"] )
```

2.33 LP_Executable Files Created and Executed by Office Applications

- **Trigger Condition:** When the executable file dropped or modified via office applications and executed within a specific time range is detected.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** Phishing, Spearphishing Attachment
- **ATT&CK ID:** T1566, T1566.001
- **Minimum Log Source Requirement:** Windows Sysmon

- **Query:**

```
[norm_id=WindowsSysmon event_id=11 "process" IN ["*\WINWORD.EXE", ".*\EXCEL.EXE", ".*\POWERPNT.EXE", ".*\MSACCESS.EXE"] file IN [".*.exe", ".*.com", ".*bat", ".*.cmd"]]]?
→ as s1 followed by [norm_id=WindowsSysmon event_id=1] as s2 within 2 minute on s1.
→ path=s2.path and s1.file=s2.file | rename s1.host as host, s1.user as user, s1.domain as?
→ domain, s1.process as "process", s1.file as file, s1.path as path
```

2.34 LP_WMI Backdoor in Exchange Transport Agent

- **Trigger Condition:** A WMI backdoor in Exchange Transport Agents (ETA) via WMI event filters is detected.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Event Triggered Execution, Windows Management Instrumentation Event Subscription
- **ATT&CK ID:** T1546, T1546.003
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create (parent_process="*\EdgeTransport.exe" -("process"=
→ "C:\Windows\System32\conhost.exe" OR ("process"="C:\Program?
→ Files\Microsoft\Exchange Server\*" "process"="*\Bin\OleConverter.exe")) -user IN?
→ EXCLUDED_USERS
```

2.35 LP_Suspicious Msiexec Usage Detected

- **Trigger Condition:** A .msi file executed from publicly writable folder and a command prompt or powershell spawned by msiexec.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Msiexec
- **ATT&CK ID:** T1218.007
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create ("process"="*\msiexec.exe" command IN
["*\ProgramData*", " *\AppData\Local*", " *\AppData\Roaming*", " *\Users\Public*"]
command IN [ "*.msi *", "*.msi" ]) OR
(parent_process="*\msiexec.exe" "process" IN
["*\cmd.exe", " *\powershell.exe", " *\pwsh.exe" ])
```

2.36 LP_Suspicious Usage of Advanced IP Scanner

- **Trigger Condition:** Suspicious usage of Advanced IP Scanner is detected.
- **ATT&CK Category:** Reconnaissance, Discovery
- **ATT&CK Tag:** Network Service Discovery, Network Share Discovery, Gather Victim Network Information
- **ATT&CK ID:** T1046, T1135, T1590
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create ("process"="*\advanced_ip_scanner*" OR file="*\advanced_
↪ ip_scanner*" ) OR (description="*\Advanced IP Scanner*" ) OR (command="*/portable*"
↪ command="*/Ing*")
```

2.37 LP_Persistence through Port Monitor Registry modification

- **Trigger Condition:** A new entry in the printer monitor registry is detected.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Boot or Logon Autostart Execution, Port Monitors
- **ATT&CK ID:** T1547, T1547.010
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=13 target_object=
↪ "HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors\*" detail="*.dll" -(("process
↪ " = "C:\Windows\System32\spoolsv.exe" target_object=
↪ " *\System\CurrentControlSet\Control\Print\Monitors\CutePDF Writer Monitor v4.
↪ 0\Driver*" detail="cpwmon64_v40.dll" user IN [ " *\AUTHOR*", " *\AUTOR*" ]) OR (target_
↪ object=" *\Control\Print\Monitors\MONVNC\Driver*" ) OR (target_object=
↪ " *\Control\Print\Environments\*" target_object=" *\Drivers\*" target_object=" *\VNC
↪ Printer*")
```

(continued from previous page)

2.38 LP_File Dropped in Suspicious Location

- **Trigger Condition:** Dropping a file in a suspicious system location is detected.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Ingress Tool Transfer
- **ATT&CK ID:** T1105
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=11 path IN ["C:\ProgramData*", "*\AppData\Local*",
↪ "*\AppData\Roaming*", "C:\Users\Public*"] - "process" IN ["*\Microsoft Visual[?]
↪ Studio\Installer*\BackgroundDownload.exe", "C:\Windows\system32\cleanmgr.exe",
↪ "*\Microsoft\Windows Defender*\MsMpEng.exe",
↪ "C:\Windows\SysWOW64\OneDriveSetup.exe", "*\AppData\Local\Microsoft\OneDrive*
↪ ", "*\Microsoft\Windows Defender\platform*\MpCmdRun.exe",
↪ "*\AppData\Local\Temp\mpam-*.exe"] -file IN ["vs_setup_bootstrapper.exe",
↪ "DismHost.exe", "*_PSScriptPolicyTest*.ps1"]
```

2.39 LP_Alternate PowerShell Hosts via Powershell Module

- **Trigger Condition:** Alternate Command and Scripting Interpreter and PowerShell hosts are detected. Adversaries might use this technique to bypass detections looking for *powershell.exe*. PowerShell commands/scripts can also be executed without directly invoking the *powershell.exe* binary. Powershell module logging is needed for log source.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, PowerShell
- **ATT&CK ID:** T1059, T1059.001
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4103 host_application IN ["*= powershell*", "*=?
↪ C:\Windows\System32\WindowsPowerShell\v1.0\powershell*", "*=?
↪ C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell*", "*= C:/Windows/
↪ System32/WindowsPowerShell/v1.0/powershell*", "*= C:/Windows/SysWOW64/
↪ WindowsPowerShell/v1.0/powershell*"] -(host_application IN ["*=?
↪ C:\WINDOWS\System32\sdiagnhost.exe -Embedding*", "*ConfigSyncRun.exe*",
↪ "*C:\Windows\system32\dsac.exe*", "*C:\Windows\system32\wsmprovhost.exe -
↪ Embedding*"] OR payload IN ["*Update-Help*", "*Failed to update Help for the?
↪ module*"])
```

2.40 LP_Suspicious Usage of Where Binary

- **Trigger Condition:** An enumeration attempt on browser bookmarks to learn more about compromised hosts is detected.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Browser Bookmark Discovery
- **ATT&CK ID:** T1217
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label="Process" label=Create "process"="*\where.exe" command in ["*places.sqlite*",
↪ "*cookies.sqlite*", "*formhistory.sqlite*", "*logins.json*", "*key4.db*", "*key3.db*",
↪ "*sessionstore.jsonlz4*", "*History*", "*Bookmarks*", "*Cookies*", "*Login Data*"]
```

2.41 LP_MSHTA - Activity Detected

- **Trigger Condition:** Network connection events initiated by *mshta.exe* are detected. Adversaries abuse *mshta.exe* for proxy execution of malicious .hta files, and Javascript or VBScript through a trusted Windows utility.
- **ATT&CK Category:** Defense Evasion, Execution
- **ATT&CK Tag:** Signed Binary Proxy Execution, Mshta
- **ATT&CK ID:** T1218, T1218.005
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=3 (command="*mshta.exe" or parent_command=
↳ "*mshta.exe") -user IN EXCLUDED_USERS
```

2.42 LP_Alternate PowerShell Hosts via Named Pipe

- **Trigger Condition:** Alternate Command and Scripting Interpreter and PowerShell hosts are detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, PowerShell
- **ATT&CK ID:** T1059, T1059.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=17 pipe="\PSHost*" source_image=* -source_image
↳ IN ["*\powershell.exe", ".*\powershell_ise.exe", ".*\WINDOWS\System32\sdiagnhost.exe",
↳ ".*\WINDOWS\System32\wsmprovhost.exe", ".*\Windows\system32\dsac.exe",
↳ ".*\Windows\system32\wbem\wmiprvse.exe", ".*\ForefrontActiveDirectoryConnector.exe",
↳ ".*c:\windows\system32\inetsrv\w3wp.exe", "C:\Program Files\Citrix\*", "C:\Program
↳ Files\Microsoft\Exchange Server\*", "C:\Windows\system32\ServerManager.exe",
↳ "C:\Program Files\PowerShell\7\pwsh.exe", ".*\Program Files\Microsoft SQL
↳ Server\*\Tools\Binn\SQLPS.exe"]
```

2.43 LP_Suspicious File Execution Using Wcript or Cscript

- **Trigger Condition:** Process create events for the *fltmc.exe* utility and the specific command line used to unload minifilter drivers is detected. An adversary may attempt to block indicators or events captured by sensors from being gathered and analyzed.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Impair Defenses, Indicator Blocking
- **ATT&CK ID:** T1562, T1562.006
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="Process" label=Create ("process" = "*\fltmc.exe" OR command = "*fltmc*unload*") -
  ↳ user IN EXCLUDED_USERS
```

2.44 LP_Suspicious Child Process Spawned by Microsoft Office Product

- **Trigger Condition:** Suspicious child process spawned by Microsoft Office Products such as Excel, Powerpoint, Onenote or Visio are detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, PowerShell, Windows Command Shell, Malicious File
- **ATT&CK ID:** T1059, T1059.001, T1059.003, T1204.002
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="Process" label=Create parent_process IN ["*\WINWORD.EXE", ".*\EXCEL.EXE",
  ↳ ".*\POWERPNT.exe", ".*\MSPUB.exe", ".*\VISIO.exe", ".*\OUTLOOK.EXE",
  ↳ ".*\MSACCESS.EXE", ".*\EQNEDT32.EXE", ".*\Onenote.exe", ".*\wordview.exe",
  ↳ ".*\outlook.exe"] ("process" IN ["\AppVLP.exe", ".*\bash.exe", ".*\bitsadmin.exe",
  ↳ ".*\certoc.exe", ".*\certutil.exe", ".*\cmd.exe", ".*\cmstp.exe", ".*\control.exe", ".*\cscript.exe",
  ↳ ".*\curl.exe", ".*\forfiles.exe", ".*\hh.exe", ".*\ieexec.exe", ".*\installutil.exe", ".*\javaw.exe",
  ↳ ".*\mftrace.exe", ".*\Microsoft.Workflow.Compiler.exe", ".*\msbuild.exe", ".*\msdt.exe",
  ↳ ".*\mshta.exe", ".*\msidb.exe", ".*\msiexec.exe", ".*\msxsl.exe", ".*\odbcconf.exe",
  ↳ ".*\pcalua.exe", ".*\powershell.exe", ".*\pwsh.exe", ".*\regasm.exe", ".*\regsvcs.exe",
  ↳ ".*\regsvr32.exe", ".*\rundll32.exe", ".*\schtasks.exe", ".*\scrcons.exe", ".*\scriptrunner.exe",
  ↳ ".*\sh.exe", ".*\svchost.exe", ".*\verclsid.exe", ".*\wmic.exe", ".*\workfolders.exe", ".*\wscript.
  ↳ exe", ".*\AppData\*", ".*\Users\Public\*", ".*\ProgramData\*", ".*\Windows\Tasks\*",
  ↳ ".*\Windows\Temp\*", ".*\Windows\System32\Tasks\*"] OR file in ["bitsadmin.exe",
  ↳ "CertOC.exe", "CertUtil.exe", "Cmd.Exe", "CMSTP.EXE", "cscript.exe", "curl.exe", "HH.
  ↳ exe", "IEExec.exe", "InstallUtil.exe", "javaw.exe", "Microsoft.Workflow.Compiler.exe",
  ↳ "msdt.exe", "MSHTA.EXE", "msiexec.exe", "Msxsl.exe", "odbcconf.exe", "pcalua.exe",
  ↳ "PowerShell.EXE", "RegAsm.exe", "RegSvc.exe", "REGSVR32.exe", "RUNDLL32.exe",
  ↳ "schtasks.exe", "ScriptRunner.exe", "wmic.exe", "WorkFolders.exe", "wscript.exe"])
```

2.45 LP_Windows Login Attempt on Disabled Account

- **Trigger Condition:** Login attempt on disabled account is detected.

- **ATT&CK Category:** Initial Access, Persistence, Privilege Escalation, Defense Evasion
- **ATT&CK Tag:** Valid Accounts
- **ATT&CK ID:** T1078
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer* label=User label>Login label=Fail sub_status_code="0xC0000072" -
↪target_user=*$ -user=*$ -user IN EXCLUDED_USERS | rename user as target_user,
↪domain as target_domain, reason as failure_reason
```

2.46 LP_RClone Utility Execution

- **Trigger Condition:** Execution of the RClone tool or command line option used in the tool is detected.
- **ATT&CK Category:** Exfiltration
- **ATT&CK Tag:** Exfiltration Over Web Service, Exfiltration to Cloud Storage
- **ATT&CK ID:** T1567, T1567.002
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create (command="*--config*" command="*--no-check-
↪certificate*" command="*copy*") OR (("process"="*\rclone.exe" OR description=
↪"Rsync for cloud storage") command IN ["*pass*", "*user*", "*copy*", "*sync*", "*config*",
↪"*lsd*", "*remote*", "*ls*", "*mega*", "*pcloud*", "*ftp*", "*ignore-existing*", "*auto-
↪confirm*", "*transfers*", "*multi-thread-streams*", "*no-check-certificate*"])
```

2.47 LP_UAC Bypass via SDCLT

- **Trigger Condition:** User Account Control (UAC) bypass attempt via SDCLT.exe is detected or it detects modification to registry keys HKCU:\Software\Classes\exefile\shell\runas\command\isolatedCommand and HKCU:\Software\Classes\Folder\shell\open\command which can indicate UAC bypass using registry key manipulation of sdclt.exe.
- **ATT&CK Category:** Privilege Escalation

- **ATT&CK Tag:** Abuse Elevation Control Mechanism, Bypass User Account Control
- **ATT&CK ID:** T1548, T1548.002
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
(norm_id=WindowsSysmon event_id=1 parent_process="*\sdclt.exe" parent_command=
↪ "*/kickoffelev*" integrity_level=High -"process" IN ["C:\Windows\SysWOW64\sdclt.exe",
↪ "C:\Windows\System32\sdclt.exe", "C:\Windows\SysWOW64\control.exe",
↪ "C:\Windows\System32\control.exe", "C:\Windows\System32\WerFault.exe",
↪ "C:\Windows\SysWOW64\WerFault.exe", "C:\Windows\System32\wermgr.exe",
↪ "C:\Windows\SysWOW64\wermgr.exe"]) OR (norm_id=WindowsSysmon event_id="13"
↪ target_object IN ["*\Classes\exefile\shell\runas\command\isolatedCommand*",
↪ "*/Classes\Folder\shell\open\command*"])
```

2.48 LP_Suspicious Binary Execution in User Directory

- **Trigger condition:** An executable in the users directory started from Microsoft Word, Excel, Powerpoint, Publisher or Visio is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Malicious File
- **ATT&CK ID:** T1204.002
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create parent_process IN ["*\WINWORD.EXE", "*/EXCEL.EXE",
↪ "*/POWERPNT.exe", "*/MSPUB.exe", "*/VISIO.exe", "*/MSACCESS.exe",
↪ "*/EQNEDT32.exe"] "process"="C:\users\*.exe" - "process"="*/Teams.exe"
```

2.49 LP_Suspicious WMIC Child Process

- **Trigger condition:** Suspicious child process of WMIC is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Windows Management Instrumentation
- **ATT&CK ID:** T1047

- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create parent_process="*\wmic.exe" - "process" IN [
↪ "C:\Windows\System32\conhost.exe", "C:\Windows\system32\wbem\WMIC.exe",
↪ "C:\Windows\syswow64\wbem\WMIC.exe", "C:\Windows\system32\WerFault.exe",
↪ "C:\Windows\SysWOW64\WerFault.exe"]
```

2.50 LP_Suspicious File Execution Using Wscript or Cscript

- **Trigger condition:** File with extensions of .jse, .vbe, .js and .vba is executed using wscript or cscript is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Visual Basic, JavaScript
- **ATT&CK ID:** T1059.005, T1059.007
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Create" label="Process" "process" IN ["*\wscript.exe", "*\cscript.exe"] -
↪ command="*.json*" command IN ["*.jse*", "*.vbe*", "*.js*", "*.vba*"]
```

2.51 LP_BCDEdit Safe Mode Command Execution

- **Trigger condition:** Spawning of Boot Configuration Data Edit (BCDEdit) from suspicious processes, to configure a reboot into safe mode, is detected.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Inhibit System Recovery
- **ATT&CK ID:** T1490
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*\bcdedit.exe" command IN ["*minimal*",
↪ "*network*", "*safebootalternateshell*"] parent_process IN ["*\WINWORD.EXE",
↪ "*\EXCEL.EXE", "*\POWERPNT.EXE", "*\MSACCESS.EXE", "*\MSPUB.EXE",
↪ "*\OUTLOOK.EXE", "*\ftldr.exe", "*\cscript.exe", "*\powershell.exe", "*\pwsh.exe",
↪ "*\wscript.exe", "*\cmd.exe", "*\rundll32.exe", "*\regsvr32.exe", "*\vsshlta.exe",
↪ "*\msbuild.exe"] (continues on next page)
```

(continued from previous page)

2.52 LP_Suspicious Encoded PowerShell Command Line

- **Trigger condition:** A suspicious PowerShell base64 encoded command is detected. Adversaries can use this technique to evade defense mechanisms by encoding and decoding payload.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, PowerShell
- **ATT&CK ID:** T1059, T1059.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label= "Process" label>Create command IN ["*-e JAB*", "* -e JAB*", "*-e JAB*", "-e ?  
↪JAB*", "** -e JAB*", "** -e JAB*", "** -en JAB*", "** -enc JAB*", "-enc* JAB*", "-w? ↪hidden  
↪-e* JAB*", "** BA^J e-", "** -e SUVYI*", "** -e aWV4l*", "** -e SQBFAFgA*", "-e[ ↪aQBIAHgA*",  
↪"-enc SUVYI*", "-enc aWV4l*", "-enc SQBFAFgA*", "-end?" ↪aQBIAHgA*"] -command="*" -ExecutionPolicy remotesigned "*" -user IN EXCLUDED_  
↪USERS
```

2.53 LP_Persistence Attack through Accessibility Process Feature

- **Trigger condition:** Accessibility features used to execute a command prompt or other backdoors are detected.
- **ATT&CK Category:** Persistence, Privilege Escalation
- **ATT&CK Tag:** Event Triggered Execution, Accessibility Features
- **ATT&CK ID:** T1546, T1546.008
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 user="SYSTEM" parent_process IN ["*\Utilman.exe",
→ ".*\winlogon.exe"] "process" IN ["*\osk.exe", ".*\Magnify.exe", ".*\Narrator.exe",
→ ".*\sethc.exe", ".*\utilman.exe", ".*\ATBroker.exe", ".*\DisplaySwitch.exe"] -file IN ["osk.
→ exe", "sethc.exe", "utilman2.exe", "DisplaySwitch.exe", "ATBroker.exe", "ScreenMagnifier
→ exe", "SR.exe", "Narrator.exe", "magnify.exe"]
```

(continues on next page)

(continues on next page)

(continued from previous page)

2.54 LP_Firewall Rule Addition via Netsh Detected

- **Trigger condition:** A connection allowed by a port or application on the Windows firewall is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Impair Defenses, Disable or Modify System Firewall
- **ATT&CK ID:** T1562, T1562.004
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create command IN ["*netsh* firewall add*"] -user IN EXCLUDED_
↪ USERS
```

2.55 LP_MSHTA Spawned by SVCHOST Detected

- **Trigger condition:** Microsoft HTML Application Host (MSHTA) binary spawned by the Svchost process is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Mshta
- **ATT&CK ID:** T1218.005
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create parent_process="*\svchost.exe" "process"="*\mshta.exe" -
↪ user IN EXCLUDED_USERS
```

2.56 LP_Exploitation of CVE-2019-1388 Detected

- **Trigger condition:** An exploitation attempt of CVE-2019-1388 in which the UAC consent dialogue used to invoke a Windows process running as LOCAL_SYSTEM is detected. CVE-2019-1388 is an elevation of privilege vulnerability in the Windows Certificate Dialog.
- **ATT&CK Category:** Privilege Escalation
- **ATT&CK Tag:** Exploitation for Privilege Escalation
- **ATT&CK ID:** T1068
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create parent_process="*\consent.exe" "process"="*\iexplore.exe"
↪ "command"="* http*" (integrity_level="System" OR user IN ["SYSTEM","*AUTHORI*",
↪ "*AUTORI*", "*AUKTORI*"])
```

2.57 LP_Sophos EPP Registry Modification

- **Trigger condition:** Modifying Sophos EPP Tamper Protection registry keys to turn off services is detected. Sophos EPP Tamper Protection is the service offered by the EPP that constantly checks if a malware or adversary or rogue employee turns off the AV services to avoid detection.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Modify Registry
- **ATT&CK ID:** T1112
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label=Registry label=Set label=value target_object IN [
↪ "*\CurrentControlSet\Services\Sophos Endpoint*\SEDEnabled",
↪ "*\CurrentControlSet\Services\Sophos Endpoint*\SAVEEnabled "] detail="DWORD"
↪ (0x00000000)"
```

2.58 LP_Office365 Inbox Rule with Special Characters Created

- **Trigger condition:** A new inbox rule created on Office365 with a suspicious name made of only special characters is detected.
- **ATT&CK Category:** Collection
- **ATT&CK Tag:** Email Forwarding Rule
- **ATT&CK ID:** T1114.003
- **Minimum Log Source Requirement:** Office365
- **Query:**

```
norm_id=Office365 action="New-InboxRule" name=* | process regex("(?P<match>^[^a-zA-Z0-9]*$)", "name") | search match=*
```

2.59 LP_Suspicious WerFault Process Creation

- **Trigger condition:** A *services.exe* spawns *werfault.exe* process from non-default paths is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Masquerading
- **ATT&CK ID:** T1036
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*\WerFault.exe" ("process"=
↪ "C:\Windows\WinSxS\*" OR -"process" IN ["C:\Windows\System32\*",
↪ "C:\Windows\SysWOW64\*"])
```

2.60 LP_Suspicious WerFault File Creation

- **Trigger condition:** A non-system process drops the *WerFault.exe* binary inside the *C:\Windows\WinSxS* folder is detected.
- **ATT&CK Category:** Defense Evasion

- **ATT&CK Tag:** Masquerading
- **ATT&CK ID:** T1036
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label=File label=Create path="C:\Windows\WinSxS\*" file="WerFault.exe" - "process"
↪ IN ["C:\Windows\System32\*", "C:\Windows\SysWOW64\*", "*C:\Windows\WinSxS\*"]
```

2.61 LP_Snake Malware Covert Store Registry Key Detected

- **Trigger condition:** A registry operation for the key `SECURITYPolicySecretsn` is detected. Snake Malware utilizes the registry key to store the encryption key.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Modify Registry
- **ATT&CK ID:** T1112
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
(norm_id=WindowsSysmon event_id IN [12,13,14] target_object=
↪ "*SECURITY\Policy\Secrets\n") OR (norm_id=Winserver event_id=4657 path=
↪ "*SECURITY\Policy\Secrets\n")
```

2.62 LP_Suspicious WerFault Service Creation

- **Trigger condition:** A new service installed using the `WerFault.exe` file is detected. `WerFault.exe` is a system component that plays a crucial role in Windows operating systems. It manages system error reporting.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Masquerading
- **ATT&CK ID:** T1036
- **Minimum Log Source Requirement:** Windows Sysmon, Windows

- **Query:**

```
norm_id=WinServer event_id IN [4697,7045] (file="WerFault.exe" OR path="*WerFault.
↪exe") (path="C:\Windows\WinSxS\*" OR -path IN ["C:\Windows\System32*",
↪ "C:\Windows\SysWOW64*"])
```

2.63 LP_Suspicious Named Pipe Connection to Azure AD Connect Database

- **Trigger condition:** Named pipe connection to Azure AD Connect database from suspicious processes coming from command shells like PowerShell, which may indicate attackers attempting to dump plaintext credentials of AD and Azure AD connector account using tools such as AADInternals is detected.
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon label=Pipe label=Connect pipe="*\tsql\query" -image IN [
↪ "\Program Files\Microsoft Azure AD Sync\Bin\miiserver.exe", "\Tools\Binn\SqlCmd.exe
↪"]
```

2.64 LP_Suspicious Driver Loaded

- **Trigger condition:** Misuse of known drivers by adversaries for malicious purposes is detected. The driver itself are not malicious but are misused by threat actors. For this alert to trigger SUSPICIOUS_DRIVER list is required.
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label=Image label=Load image IN SUSPICIOUS_DRIVER
```

2.65 LP_AADInternals PowerShell Cmdlet Execution

- **Trigger condition:** The execution of *AADInternals* commandlets is detected. AADInternals (S0677) toolkit is a PowerShell module containing tools for administering and hacking Azure AD and Office 365. Adversaries use *AADInternals* to extract the credentials from the system where the AAD Connect server was installed and compromise the AAD environment.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, PowerShell
- **ATT&CK ID:** T1059, T1059.001
- **Minimum Log Source Requirement:** Windows, PowerShell
- **Query:**

```
norm_id=WinServer event_source="Microsoft-Windows-PowerShell" event_id=4104
↪script_block IN AADINTERNALS_CMDLETS
```

2.66 LP_Suspicious Scheduled Task Creation via Masqueraded XML File

- **Trigger condition:** The creation of a suspicious scheduled task using an XML file with a masqueraded extension is detected.
- **ATT&CK Category:** Persistence, Defense Evasion
- **ATT&CK Tag:** Masquerading, Match Legitimate Name or Location, Scheduled Task/Job and Scheduled Task
- **ATT&CK ID:** T1036, T1036.005, T1053 and T1053.005
- **Minimum Log Source Requirement:** Windows Sysmon, Windows

```
label=create label="process" "process"="*\schtasks.exe" command IN ["*/create*", "*-
↪create*"] command IN ["*/xml*", "*-xml*"] (-integrity_level=system OR -integrity_
↪label=*system*) -command = *.xml* ((-parent_process IN [
↪"*.\\ProgramData\\OEM\\UpgradeTool\\CareCenter_*\\BUnzip\\Setup_msi.exe",
↪"*.\\Program Files\\Axis Communications\\AXIS Camera Station\\SetupActions.exe",
↪"*.\\Program Files\\Axis Communications\\AXIS Device Manager\\AdmSetupActions.exe",
↪"*.\\Program Files (x86)\\Zemana\\AntiMalware\\AntiMalware.exe", ".*\\Program
↪Files\\Dell\\SupportAssist\\pcdrcui.exe" ]) OR (-parent_process = ".*\\rundll32.exe"
↪command = ".*\\WINDOWS\\Installer\\MSI*.tmp,
↪zzzzInvokeManagedCustomActionOutOfProc" ))
```

2.67 LP_Suspicious Microsoft Equation Editor Child Process

- **Trigger condition:** A suspicious child process of Microsoft's equation editor is detected as a sign of possible exploitation of CVE-2017-11882. CVE-2017-11882 is a vulnerability in Microsoft Office's Equation Editor component.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Exploitation for Client Execution
- **ATT&CK ID:** T1203
- **Minimum Log Source Requirement:** Windows Sysmon, Windows

```
label="Process" label=Create parent_process="*\EQNEDT32.exe" - "process" IN [
  ↳ "C:\Windows\System32\WerFault.exe", "C:\Windows\SysWOW64\WerFault.exe"]
```

2.68 LP_Windows Error Process Masquerading

- **Trigger condition:** Suspicious Windows error reporting process behavior, where network connections are made after execution is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Masquerading
- **ATT&CK ID:** T1036
- **Minimum Log Source Requirement:** Windows Sysmon

```
[norm_id=WindowsSysmon event_id=1 "process" IN ["*\WerMgr.exe", "\WerFault.exe"]][?]
↳ as s1 followed by [norm_id=WindowsSysmon event_id=3 "process" IN ["*\WerMgr.exe",
↳ "\WerFault.exe"]] as s2 within 1 minute on s1.process_guid=s2.process_guid | rename[?]
↳ s1.host as host, s1.user as user, s1.domain as domain, s1.image as image, s2.destination_
↳ address as destination_address, s2.destination_port as destination_port
```

2.69 LP_Bypass UAC via CMSTP Detected

- **Trigger condition:** Child processes of automatically elevated instances of Microsoft Connection Manager Profile Installer (cmstp.exe) are detected.
- **ATT&CK Category:** Privilege Escalation, Defense Evasion

- **ATT&CK Tag:** CMSTP, Abuse Elevation Control Mechanism, Bypass User Account Control
- **ATT&CK ID:** T1218.003, T1548, T1548.002
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*\cmstp.exe" command IN ["*/s*", "*/au*", "*/
↪ni*", "*/s*", "*/au*", "*/ni*"] -user IN EXCLUDED_USERS
```

2.70 LP_Application Whitelisting Bypass via Dxcap Detected

- **Trigger condition:** Adversaries bypass process and/or signature-based defenses by execution of *Dxcap.exe* is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Trusted Developer Utilities Proxy Execution
- **ATT&CK ID:** T1127
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*\dxcap.exe" command="*/-c*" command="*/.
↪exe*" -user IN EXCLUDED_USERS
```

2.71 LP_Suspicious WMIC XSL Script Execution

- **Trigger condition:** Loading of a Windows Script module through wmic by Microsoft Core XML Services (MSXML) process is detected to bypass application whitelisting.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** XSL Script Processing
- **ATT&CK ID:** T1220
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
[norm_id=WindowsSysmon event_id=1 file="wmic.exe" command IN ["*format*:*", "*/
↪format*:*", "*-format*:*"] -command IN ["*format:list*", "*format:table*",
↪"*format:htable", "*format:texttablesys*", "*format:texttable*", "*format:textvaluelist*",
↪"*format:TEXTVALUELIST*", "*format:csv*", "*format:value*"]]] as s1 followed by [?]
↪[norm_id=WindowsSysmon event_id=7 image IN ["*jscript.dll", "*vbscript.dll"]] as s2 [?]
↪within 2 minute on s1.process_guid=s2.process_guid | rename s1.process as "process", [?]
↪s1.host as host, s1.domain as domain, s1.command as command, s2.image as loaded_
↪image
```

2.72 LP_Suspicious File Execution via MSHTA

- **Trigger condition:** Execution of javascript or VBScript files and other abnormal extension files executed via mshta binary is detected.
- **ATT&CK Category:** Execution, Defense Evasion
- **ATT&CK Tag:** JavaScript, Deobfuscate/Decode Files or Information, Mshta
- **ATT&CK ID:** T1059.007, T1140, T1218.005
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label="create" "process"="*\mshta.exe" command IN ["*javascript*",
↪"*vbscript*", "*.jpg*", "*.png*", "*.lnk*", "*.xls*", "*.doc*", "*.zip*"] -user IN [?]
↪EXCLUDED_USERS
```

2.73 LP_Regsvr32 Anomalous Activity Detected

- **Trigger condition:** Various anomalies concerning regsvr32.exe are detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Signed Binary Proxy Execution, Regsvr32
- **ATT&CK ID:** T1218, T1218.010
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 ((image="*\regsvr32.exe" command="*\Temp\*") [?]
↪OR (image="*\regsvr32.exe" parent_image="*\powershell.exe") OR (image=
↪"**\regsvr32.exe" parent_image="*\cmd.exe") OR (image="*\regsvr32.exe" command [?]
↪IN ["*/i:http*scrobj.dll", "*/i:ftp*scrobj.dll"]) OR (image="*\wscript.exe" parent_image=
↪"**\regsvr32.exe") OR (image="*\EXCEL.EXE" command="*..\..\.. (continues on next page)
↪\Windows\System32\regsvr32.exe *")) -user IN EXCLUDED_USERS
```

(continued from previous page)

2.74 LP_Remote File Execution via MSIEXEC

- **Trigger condition:** Suspicious use of *msiexec.exe* to install remote Microsoft Software Installer (MSI) files is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Msiexec
- **ATT&CK ID:** T1218.007
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create "process"="/msiexec.exe" command="*http*" command
↪ IN ["*/i*", "*/j*"] ((command IN ["*/q*", "*/quiet*", "*/qn*", "*/-q*", "*/-quiet*", "*/-qn*
↪ ") OR (command IN ["*/-Q-", "*/-I-Q*", "*/q-i*", "*/-q/i*", "*/q/i*"] )) -(parent_image=
↪ "*/setup*") -integrity_level=SYSTEM
```

2.75 LP_Execution of Trojanized 3CX Application

- **Trigger Condition:** Execution of the trojanized version of the 3CX Desktop is detected. 3CX Desktop versions 18.12.407 and 18.12.416 are known to be trojanized by the Lazarus Group and are also signed using the 3CX signature.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Masqueradings
- **ATT&CK ID:** T1036
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 file="3CXDesktopApp.exe" product IN ["*3CX Ltd*
↪ ", "*3CX Desktop App*"] file_version IN ["*18.12.407*", "18.12.416*"]
```

2.76 LP_Msbuild Spawned by Unusual Parent Process

- **Trigger condition:** Suspicious use of *msbuild.exe* by an uncommon parent process is detected. *msbuild.exe* is a legitimate Microsoft tool used for building and deploying software applications.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Trusted Developer Utilities Proxy Execution, MSBuild
- **ATT&CK ID:** T1127, T1127.001
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label=Create label="Process" "process"="*\MSBuild.exe" -parent_process in ["*\devenv.exe",
↪ "\cmd.exe", "\msbuild.exe", "\python.exe", "\explorer.exe", "\nuget.exe"]
```

2.77 LP_Suspicious Files Designated as System Files Detected

- **Trigger condition:** The execution of the **+s** option of the **attrib** command is detected to designate scripts or executable files in suspicious locations as system files, hiding them from users and making them difficult to detect or remove. *attrib.exe* is a Windows command-line utility that allows users to adjust file or folder attributes such as read-only, hidden and system.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Hide Artifacts, Hidden Files and Directories
- **ATT&CK ID:** T1564, T1564.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label=Create label="Process" "process"="*\attrib.exe" command = "*" +s "*" command in [
↪ "*" %*", "\Users\Public\*", "\AppData\Local\*", "\ProgramData\*",
↪ "\Windows\Temp\*"] command in ["*.bat*", "*.dll*", "*.exe*", "*.hta*", "*.ps1*", "*.
↪ vbe*", "*.vbs*"] -command="*\Windows\TEMP\*.exe"
```

2.78 LP_Bypass User Account Control using Registry

- **Trigger condition:** Bypass of User Account Control (UAC) is detected. Adversaries bypass UAC mechanisms to elevate process privileges on the system. The alert queries for `*\mscfile\shell\open\command\*` or `*\ms-settings\shell\open\command\*`.
- **ATT&CK Category:** Defense Evasion, Privilege Escalation
- **ATT&CK Tag:** Abuse Elevation Control Mechanism, Bypass User Account Control
- **ATT&CK ID:** T1548, T1548.002
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon ((event_id=12 event_type=*Create*) OR (event_id=13 event_
↪ type=SetValue)) target_object IN ["*\mscfile\shell\open\command\*", "*\ms-
↪ settings\shell\open\command\*"]
```

2.79 LP_Unsigned Image Loaded Into LSASS Process

- **Trigger condition:** Loading of unsigned images like DLL or EXE into the LSASS process is detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** OS Credential Dumping, LSASS Memory
- **ATT&CK ID:** T1003, T1003.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=7 image="*\lsass.exe" signed="false" -user IN[
↪ EXCLUDED_USERS]
```

2.80 LP_Usage of Sysinternals Tools Detected

- **Trigger condition:** The use of Sysinternals tools due to the addition of *accepteula* key to a registry is detected.

- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Masquerading
- **ATT&CK ID:** T1036
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
(label=Registry label=Set target_object="*\EulaAccepted") or (label=Create label=
↪ "Process" command IN ["* -accepteula*", "* /accepteula*"])
```

2.81 LP_Microsoft SharePoint Remote Code Execution Detected

- **Trigger condition:** The execution of a remote code in Microsoft SharePoint (CVE-2019-19781).
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** Exploit Public-Facing Application
- **ATT&CK ID:** T1190
- **Minimum Log Source Requirement:** Firewall, IDS/IPS, Web server
- **Query:**

```
request_method=POST (url='*_layouts/15/Picker.aspx*WebControls.ItemPickerDialog*'
↪ OR resource='*_layouts/15/Picker.aspx*WebControls.ItemPickerDialog*')
```

2.82 LP_DenyAllWAF SQL Injection Attack

- **Trigger condition:** DenyALLWAF detects SQL injection attack.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** Exploit Public-Facing Application
- **ATT&CK ID:** T1190
- **Minimum Log Source Requirement:** DenyAll WAF
- **Query:**

```
norm_id=DenyAllWAF label=SQL label=Injection
```

2.83 LP_Windows CryptoAPI Spoofing Vulnerability Detected

- **Trigger condition:** Vulnerability related to CVE-2020-0601 is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Subvert Trust Controls, Code Signing
- **ATT&CK ID:** T1553, T1553.002
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer label=CVE label=Exploit label=Detect cve_id="CVE-2020-0601" -
↪ user IN EXCLUDED_USERS
```

2.84 LP_Malicious use of Scriptrunner Detected

- **Trigger condition:** The malicious use of *Scriptrunner.exe* is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Signed Binary Proxy Execution
- **ATT&CK ID:** T1218
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="create" label="process" ("process"="*\ScriptRunner.exe" OR file="ScriptRunner.
↪ exe") command="* -appvscript *
```

2.85 LP_Suspicious process related to Rundll32 Detected

- **Trigger condition:** A suspicious process related to *RunDLL32.exe* is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Rundll32
- **ATT&CK ID:** T1218.011
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="create" label="process" (command IN ["*javascript:*", "*.RegisterXLL*"] OR
↪ (command="*url.dll*" command="*OpenURL*") OR (command="*url.dll*" command=
↪ "*OpenURLA*") OR (command="*url.dll*" command="*FileProtocolHandler*") OR
↪ (command="*zipfldr.dll*" command="*RouteTheCall*") OR (command="*shell32.dll*"
↪ command="*Control_RunDLL*") OR (command="*shell32.dll*" command="*ShellExec_
↪ RunDLL*") OR (command="*mshtml.dll*" command="*PrintHTML*") OR (command=
↪ "*advpack.dll*" command="*LaunchINFSection*") OR (command="*advpack.dll*"
↪ command="*RegisterOCX*") OR (command="*ieadvpack.dll*" command=
↪ "*LaunchINFSection*") OR (command="*ieadvpack.dll*" command="*RegisterOCX*")
↪ OR (command="*ieframe.dll*" command="*OpenURL*") OR (command="*shdocvw.dll*
↪ " command="*OpenURL*") OR (command="*syssetup.dll*" command=
↪ "*SetupInfObjectInstallAction*") OR (command="*setupapi.dll*" command=
↪ "*InstallHinfSection*") OR (command="*pcwutl.dll*" command="*LaunchApplication*
↪ ") OR (command="*dfshim.dll*" command="*ShOpenVerbApplication*"))
```

2.86 LP_Javascript conversion to executable Detected

- **Trigger condition:** A windows executable *jsc.exe* is used to convert javascript files to craft malicious executables.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Trusted Developer Utilities Proxy Execution
- **ATT&CK ID:** TT1127
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="create" label="process" "process"="*\\jsc.exe" command="*.js"
```

2.87 LP_Suspicious Execution of Gpscript Detected

- **Trigger condition:** A group policy script *gpscript.exe* is used to execute logon or startup scripts configured in Group Policy.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Signed Binary Proxy Execution
- **ATT&CK ID:** T1218
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="create" label="process" "process"="*\gpscript.exe" command IN ["*/logon*", "*/startup*"]
```

2.88 LP_Proxy Execution via Desktop Setting Control Panel

- **Trigger condition:** A windows internal binary *rundll32* with *desk.cpl* is used to execute spoof binary with ".cpl" extension.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Rundll32
- **ATT&CK ID:** T1218.011
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label="Create" "process"="*\rundll32.exe" command="*desk.cpl*InstallScreenSaver*.scr"
```

2.89 LP_Xwizard DLL Side Loading Detected

- **Trigger condition:** The use of *xwizard* binary from the non-default directory is detected.
- **ATT&CK Category:** Defense Evasion

- **ATT&CK Tag:** DLL Side-Loading
- **ATT&CK ID:** T1574.002
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*\xwizard.exe" - "process"=
↪ "C:\Windows\System32\*"
```

2.90 LP_DLL Side Loading Via Microsoft Defender

- **Trigger condition:** An execution of *mpcmdrun* binary from non default path is detected.
- **ATT&CK Category:** Persistence, Defense Evasion
- **ATT&CK Tag:** DLL Side-Loading
- **ATT&CK ID:** T1574.002
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label=Image label=Load "process" IN ["*\MpCmdRun.exe", "*\NisSrv.exe"] - "process" IN [
↪ "C:\Program Files\Windows Defender\*", "C:\ProgramData\Microsoft\Windows
↪ Defender\Platform\*"] image="*\mpclient.dll"
```

2.91 LP_ZIP File Creation or Extraction via Printer Migration CLI Tool

- **Trigger condition:** The creation or extraction of .zip file via *printbrm* utility is detected.
- **ATT&CK Category:** Defense Evasion, Command and Control
- **ATT&CK Tag:** Ingress Tool Transfer, NTFS File Attributes
- **ATT&CK ID:** T1105, T1564.004
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label="Create" "process"="*\printbrm.exe" command="*f*" command=
↳ "*.zip"
```

2.92 LP_Credentials Capture via Rcping Detected

- **Trigger condition:** The creation of Remote Procedure Call (RPC) via Rcping binary is detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** OS Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label="Create" "process"="*\rcping.exe" command="*s*" (
↳ (command="*u*" command="*NTLM*") OR (command="*t*" command="*ncacn_np*"
↳ ))
```

2.93 LP_Suspicious ConfigSecurityPolicy Execution Detected

- **Trigger condition:** A local file upload via ConfigSecurityPolicy binary to attack the control server is detected.
- **ATT&CK Category:** Exfiltration
- **ATT&CK Tag:** Exfiltration Over Web Service
- **ATT&CK ID:** T1567
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label="Create" "process"="*\ConfigSecurityPolicy.exe" command IN [
↳ "*https://*", "*http://*", "*ftp://*"]
```

2.94 LP_C-Sharp Code Compilation Using Ilasm Detected

- **Trigger condition:** C# code is either compiled into executables or into DLL using Ilasm utility.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Trusted Developer Utilities Proxy Execution
- **ATT&CK ID:** T1127
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label="Process" label="Create" ("process"="*\ilasm.exe" OR file="ilasm.exe")
```

2.95 LP_Process Dump via Resource Leak Diagnostic Tool

- **Trigger condition:** A process dump is detected using a Microsoft Windows native tool *rdrleakdiag.exe*.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** LSASS Memory
- **ATT&CK ID:** T1003.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create ("process"="*\RdrLeakDiag.exe" or file="RdrLeakDiag.exe  
↪") command="*fullmemdump"
```

2.96 LP_Suspicious DLL execution via Register-Cimprovider

- **Trigger condition:** A dll file load/execution is detected using a Microsoft Windows native tool *Register-Cimprovider.exe*.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Hijack Execution Flow
- **ATT&CK ID:** TT1574

- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label="create" "process"="*\register-cimprovider.exe" command="*-
↳path*" command="*dll*"
```

2.97 Accessibility features - Process

- **Trigger condition:** Adversaries establish persistence and/or elevate privileges by executing malicious content by process features.
- **ATT&CK Category:** Persistence, Privilege Escalation
- **ATT&CK Tag:** Event Triggered Execution, Accessibility Features
- **ATT&CK ID:** T1546,T1546.008
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 parent_image="*winlogon.exe" (image="*sethc.
↳exe" or image="*utilman.exe" or image="*osk.exe" or image="*magnify.exe" or
↳image="*displayswitch.exe" or image="*narrator.exe" or image="*atbroker.exe") -
↳user IN EXCLUDED_USERS
```

2.98 LP_Accessibility Features-Registry

- **Trigger condition:** An adversary establish persistence and/or elevates privileges by executing malicious content, replacing accessibility feature binaries, pointers, or references to these binaries in the registry.
- **ATT&CK Category:** Persistence, Privilege Escalation
- **ATT&CK Tag:** Event Triggered Execution, Accessibility Features
- **ATT&CK ID:** T1546,T1546.008
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon (event_id=12 or event_id=13 or event_id=14) target_object=
↳ "*HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution"
↳ Options\*" -user IN EXCLUDED_USERS
```

2.99 LP_Active Directory DLLs Loaded By Office Applications

- **Trigger condition:** Kerberos DLL or DSParse DLL loaded by the Office products like WinWord, Microsoft PowerPoint, Microsoft Excel or Microsoft Outlook is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Malicious File
- **ATT&CK ID:** T1204.002
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=7 "process" IN ["*\winword.exe*", "*\powerpnt.exe*",
↳ "*\excel.exe*", "*\outlook.exe*"] image IN ["*\kerberos.dll*", "*\c.dll*"] -user IN
↳ EXCLUDED_USERS
```

2.100 LP_DCSync detected

- **Trigger condition:** The abuse of Active Directory Replication Service (ADRS) detected from a non-machine account to request credentials or DC Sync by creating a new SPN.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** OS Credential Dumping, DCSync
- **ATT&CK ID:** T1003,T1003.006
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
((norm_id=WinServer event_id=4662 access_mask="0x100" properties IN ["*1131f6aa-
↳ 9c07-11d1-f79f-00c04fc2dcd2*", "*1131f6ad-9c07-11d1-f79f-00c04fc2dcd2*",
↳ "*89e95b76-444d-4c62-991a-0facbeda640c*", "*Replicating Directory Changes All*"] -
↳ user= "$" -user= "MSOL_*") or (norm_id=WinServer event_id=4742 service= "GC/*"))-
↳ user IN EXCLUDED_USERS
```

2.101 LP_Active Directory Replication User Backdoor

- **Trigger condition:** Modification of the security descriptor of a domain object for granting Active Directory replication permissions to a user.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** File and Directory Permissions Modification, Windows File and Directory Permissions Modification
- **ATT&CK ID:** T1222,T1222.001
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=5136 ldap_display="ntsecuritydescriptor" attribute_value?
↪ IN ["*1131f6aa-9c07-11d1-f79f-00c04fc2dcd2*", "*1131f6ad-9c07-11d1-f79f-
↪ 00c04fc2dcd2*", "*89e95b76-444d-4c62-991a-0facbeda640c*"] -user IN EXCLUDED_
↪ USERS
```

2.102 LP_Activity Related to NTDS Domain Hash Retrieval

- **Trigger condition:** Copying of *ntds.dit* file is detected. *NTDS.dit* file is a database that stores the Active Directory data (including users, groups, security descriptors and password hashes).
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** OS Credential Dumping, NTDS
- **ATT&CK ID:** T1003, T1003.003
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create command IN [ "*vssadmin.exe Delete Shadows*",
↪ "*vssadmin create shadow /for=C:*", "*copy \\?
↪ \GLOBALROOT\Device\*\windows\ntds\ntds.dit*", "*copy \\?
↪ \GLOBALROOT\Device\*\config\SAM*", "*vssadmin delete shadows /for=C:*", "*reg?
↪ SAVE HKLM\SYSTEM*", "*esentutl.exe /y /vss *\ntds.dit*", "*esentutl.exe /y /vss *\SAM*
↪ ", "*esentutl.exe /y /vss *\SYSTEM*" ]
```

2.103 LP_AD Object WriteDAC Access Detected

- **Trigger condition:** WRITE_DAC, which can modify the discretionary access-control list (DACL) in the object security descriptor, is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** File and Directory Permissions Modification
- **ATT&CK ID:** T1222
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4662 object_server="DS" access_mask=0x40000 object_
↪ type IN ["19195a5b-6da0-11d0-afd3-00c04fd930c9", "domainDNS"] -user IN
↪ EXCLUDED_USERS
```

2.104 LP_AD Privileged Users or Groups Reconnaissance Detected

- **Trigger condition:** *priv* users or groups recon based on 4661 event ID and privileged users or groups SIDs are detected. The object names must be; domain admin, KDC service account, admin account, enterprise admin, group policy creators and owners, backup operator, or remote desktop users.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Account Discovery, Local Account, Domain Account
- **ATT&CK ID:** T1087,T1087.001,T1087.002
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4661 object_type IN ["SAM_USER", "SAM_GROUP"]
↪ object_name IN ["*-512", "*-502", "*-500", "*-505", "*-519", "*-520", "*-544", "*-551",
↪ "*-555", "*admin*"] -user IN EXCLUDED_USERS
```

2.105 LP_Addition of SID History to Active Directory Object

- **Trigger condition:** Addition of SID History to Active Directory Object is detected. An attacker can use the SID history attribute to gain additional privileges.
- **ATT&CK Category:** Persistence, Privilege Escalation
- **ATT&CK Tag:** Access Token Manipulation, SID-History Injection
- **ATT&CK ID:** T1134,T1134.005
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer (event_id IN ["4765", "4766"] OR (event_id=4738 -sid_history="%  
↪%1793" sid_history=*)) -user IN EXCLUDED_USERS
```

2.106 LP_Admin User Remote Logon Detected

- **Trigger condition:** Successful remote login by the administrator depending on the internal pattern is detected.
- **ATT&CK Category:** Defense Evasion, Persistence, Privilege Escalation, Initial Access
- **ATT&CK Tag:** Valid Accounts
- **ATT&CK ID:** T1078
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4624 logon_type="10" (authentication_package=  
↪ "Negotiate" OR package="Negotiate") user="Admin-*" -user IN EXCLUDED_USERS |  
↪ rename package as authentication_package
```

2.107 LP_Adwind RAT JRAT Detected

- **Trigger condition:** The applications like javaw.exe, cscript in the AppData folder, or set values of Windows Run* register used by Adwind or JRAT are detected.

- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, Visual Basic, JavaScript/JScript, Windows Command Shell, PowerShell
- **ATT&CK ID:** T1059, T1059.001, T1059.003, T1059.005, T1059.007
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
(event_id=1 command IN ["*\AppData\Roaming\Oracle*\java*.exe ", "*cscript.exe",
↳ *Retrive*.vbs *"]) OR (event_id=11 file IN ["*\AppData\Roaming\Oracle\bin\java*.exe ",
↳ "*\Retrive*.vbs"]) OR (event_id=13 target_object=
↳ "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*" detail="%AppData
↳ %\Roaming\Oracle\bin\*")
```

2.108 LP_Apache Struts 2 Remote Code Execution Detected

- **Trigger condition:** A remote code execution vulnerability (CVE-2017-5638) in Apache Struts 2 is detected.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** Exploit Public-Facing Application
- **ATT&CK ID:** T1190
- **Minimum Log Source Requirement:** ApacheTomcat
- **Query:**

```
norm_id=ApacheTomcatServer label=Content label=Invalid label=Type | norm on content_
↳ type #cmd=<command:quoted>
```

2.109 LP_AppCert DLLs Detected

- **Trigger condition:** Adversaries establish persistence and/or elevate privileges by executing malicious content triggered by AppCert DLLs loaded into processes.
- **ATT&CK Category:** Persistence, Privilege Escalation
- **ATT&CK Tag:** Event Triggered Execution, AppCert DLLs

- **ATT&CK ID:** T1546, T1546.009
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon (event_id=12 or event_id=13 or event_id=14) target_object=
↳ "*\System\CurrentControlSet\Control\Session Manager\AppCertDlls\*" -user IN EXCLUDED_USERS
```

2.110 LP_Application Shimming - File Access Detected

- **Trigger condition:** Adversaries establish persistence or elevate privileges by executing malicious content initiated by application shims is detected.
- **ATT&CK Category:** Persistence, Privilege Escalation
- **ATT&CK Tag:** Event Triggered Execution, Application Shimming
- **ATT&CK ID:** T1546, T1546.011
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon ((event_id=11 file="*C:\Windows\AppPatch\Custom\*" or
↳ (event_id=1 "process"="*\sdbinst.exe") or (event_id IN [12,13,14] target_object=
↳ "*\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\InstalledSDB\*"
↳ ")) -user IN EXCLUDED_USERS
```

2.111 LP_Application Whitelisting Bypass via Dnx Detected

- **Trigger condition:** Execution of Dnx binary with ConsoleApp commandline argument is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Compile After Delivery, Signed Binary Proxy Execution
- **ATT&CK ID:** T1027.004, T1218
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*\dnx.exe" command="*ConsoleApp*" -user
↪ IN EXCLUDED_USERS
```

2.112 LP_Audio Capture Detected

- **Trigger condition:** The use of Powershell, sound recorder application, or command to get the audio device is detected. Adversaries attempt to leverage peripheral devices or applications to obtain audio recordings for sensitive conversations.
- **ATT&CK Category:** Collection
- **ATT&CK Tag:** Audio Capture
- **ATT&CK ID:** T1123
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 ((image="*SoundRecorder.exe" and command="*/
↪ FILE*") or command="*Get-AudioDevice*" or command="*WindowsAudioDevice-
↪ Powershell-Cmdlet*") -user IN EXCLUDED_USERS
```

2.113 LP_Authentication Package Detected

- **Trigger Condition:** The LSA process loaded by services other than lsass, svchost, msixec and services is detected. Windows authentication package DLLs are loaded by the Local Security Authority (LSA) process at the system start. Adversaries may abuse authentication packages to execute DLLs when the system boots.
- **ATT&CK Category:** Persistence, Privilege Escalation
- **ATT&CK Tag:** Authentication Package, Security Support Provider
- **ATT&CK ID:** T1547.002, T1547.005
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id IN [12,13,14] -event_type=INFO (target_object=
↪ "*\SYSTEM\CurrentControlSet\Control\Lsa\*" ) -"process" in [
↪ "*C:\WINDOWS\system32\lsass.exe", "*C:\Windows\system32\svchost.exe",
↪ "*C:\Windows\system32\services.exe", "C:\Windows\system32\msiexec.exe"]
```

2.114 LP_Autorun Keys Modification Detected

- **Trigger Condition:** Modification of autostart extensibility point (ASEP) in the registry is detected. ASEP allows a particular program to run automatically when a user logs into the system. Adversaries may achieve persistence by adding a program to a startup folder or referencing it with a Registry run key.
- **ATT&CK Category:** Persistence, Privilege Escalation
- **ATT&CK Tag:** Boot or Logon Autostart Execution, Registry Run Keys / Startup Folder
- **ATT&CK ID:** T1547, T1547.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label=Registry label=Set label=Value -event_type=info target_object IN [
  ↳ "\\software\\Microsoft\\Windows\\CurrentVersion\\Run*", "\\software\\Microsoft\\Windows
  ↳ NT\\CurrentVersion\\Winlogon\\Userinit*", "\\software\\Microsoft\\Windows
  ↳ NT\\CurrentVersion\\Winlogon\\Shell*",
  ↳ "\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\Run",
  ↳ "\\software\\Microsoft\\Windows NT\\CurrentVersion\\Windows*",
  ↳ "\\software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\User Shell Folders*"] detail IN [
  ↳ "*C:\\Windows\\Temp\\*", "*C:\\$Recycle.bin\\*", "*C:\\Temp\\*", "*C:\\Users\\Public\\*",
  ↳ "*C:\\ProgramData\\*", "*C:\\Users\\Default\\*", "*C:\\Users\\Desktop\\*",
  ↳ "*\\AppData\\Local\\*", "*Public\\*", "*wscript*", "*cscript*", "*powershell.exe*"] -detail=
  ↳ "*\\AppData\\Local\\Microsoft\\Teams\\Update.exe *"
```

2.115 LP_Bloodhound and Sharphound Hack Tool Detected

- **Trigger Condition:** Command-line parameters used by Bloodhound and Sharphound hack tools are detected.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Account Discovery
- **ATT&CK ID:** T1087
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label="Process" label=Create (("process" IN ["*\Bloodhound.exe*", "*\SharpHound.exe*"
↪"]) OR (command IN ["*-CollectionMethod All *", "*--CollectionMethods Session *", "*-
↪-Loop --Loopduration *", "*--PortScanTimeout *", "*.exe -c All -d *", "*Invoke-
↪Bloodhound*", "*Get-BloodHoundData*"]) OR (command="*-JsonFolder *"
↪command="*-ZipFileName *") OR (command="* DCOOnly *" command="*-
↪NoSaveCache *") OR (application="*SharpHound*" description="*SharpHound*"
↪vendor IN ["*SpecterOps*", "*evil corp*"])))
```

2.116 LP_BlueMashroom DLL Load Detected

- **Trigger Condition:** Suspicious dynamic-link libraries (DLLs) loading from the AppData Local path are detected. Adversaries can inject DLLs from AppData into processes to evade process-based defenses and elevate privileges.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Regsvr32, DLL Side-Loading
- **ATT&CK ID:** T1218.010, T1574.002
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
norm_id=WindowsSysmon event_id=1 command IN ["*\regsvr32*\AppData\Local\*",
↪ "\AppData\Local\*, DllEntry*"] -user IN EXCLUDED_USERS
```

2.117 LP_Remote Thread Creation via Cactustorch

- **Trigger Condition:** Creation of a remote thread from CACTUSTORCH is detected.
- **ATT&CK Category:** Execution, Defense Evasion
- **ATT&CK Tag:** Process Hollowing, Visual Basic, JavaScript, Mshta
- **ATT&CK ID:** T1055.012, T1059.005, T1059.007, T1218.005
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Remote" label="Thread" label="Create" "process" IN ["*\System32\cscript.exe",
↪ "\System32\wscript.exe", "*\System32\mshta.exe", "*\winword.exe", "*\excel.exe"]
↪ image="*\SysWOW64\*" -start_module=* -user IN EXCLUDED_USERS
```

2.118 LP_Call to a Privileged Service Failed

- **Trigger Condition:** The privileged service call using *LsaRegisterLogonProcess* fails.
- **ATT&CK Category:** Privilege Escalation
- **ATT&CK Tag:** Valid Account
- **ATT&CK ID:** T1078
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4673 service="LsaRegisterLogonProcess()" event_type=
↪ "*Failure*" -user IN EXCLUDED_USERS
```

2.119 LP_Capture a Network Trace with netsh

- **Trigger Condition:** Network trace capture via *netsh.exe* trace functionality is detected. *netsh.exe* is a command-line utility in Windows for configuring and displaying the network configuration on the system. Adversaries may abuse its functionality to sniff network traffic to capture information about an environment, including the authentication with credentials information.
- **ATT&CK Category:** Discovery, Credential Access
- **ATT&CK Tag:** Network Sniffing
- **ATT&CK ID:** T1040
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create "process"="*\netsh.exe" command="*trace*" command=
↪ "*start*"
```

2.120 LP_CEO Fraud - Possible Fraudulent Email Behavior

- **Trigger Condition:** An email received from a threat source in the internal network exhibits fraudulent behavior. For this alert to work, you must update the following:
 - HOME_DOMAIN, which is the list of selected domain names. For example, logpoint.com

- MANAGERS, which is the list of selected managers and executives. For example, *Alice*
- SERVER_ADDRESS, which is the list of trusted clients or servers from where the emails are received.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** Phishing
- **ATT&CK ID:** T1566, T1566.001
- **Minimum Log Source Requirement:** Exchange MT
- **Query:**

```
norm_id=ExchangeMT event_id=receive sender=* receiver IN HOME_DOMAIN original_
↪ client_address=* -original_client_address IN SERVER_ADDRESS | norm on sender
↪ <target_manager:all>@<domain:string> |
norm on message_id @<original_domain:'.*'><:'\>'> | search target_manager IN
↪ MANAGERS
```

2.121 LP_Certutil Encode Detected

- **Trigger Condition:** The *certutil* command, sometimes used for data exfiltration, is used to encode files.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Obfuscated Files or Information
- **ATT&CK ID:** T1027
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 command IN ["certutil -f -encode *", "certutil.exe -
↪ f -encode *", "certutil -encode -f *", "certutil.exe -encode -f *"] -user IN EXCLUDED_
↪ USERS
```

2.122 LP_Change of Default File Association Detected

- **Trigger Condition:** A registry value is set to change the file association. Adversaries establish persistence by executing malicious content triggered by a file type association.

- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Event Triggered Execution, Change Default File Association
- **ATT&CK ID:** T1546, T1546.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon label=Registry label=Set label=Value target_object="*HKEY_
↳ CLASSES_ROOT\mscfile*" detail in ["*powershell*", "*.exe*", "*.dat*"] -user IN
↳ EXCLUDED_USERS
```

2.123 LP_Citrix ADC VPN Directory Traversal Detected

- **Trigger Condition:** The exploitation of directory traversal vulnerability (CVE-2019-19781) in Citrix ADC is detected.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** External Remote Services
- **ATT&CK ID:** T1133
- **Minimum Log Source Requirement:** Webserver, Firewall
- **Query:**

```
norm_id=*(url="*/../vpns/*" OR resource="*/../vpns/*")
```

2.124 LP_Clear Command History

- **Trigger Condition:** Command line arguments to delete console history are detected. Adversaries can use this technique to remove the traces of their executed commands.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Clear Command History
- **ATT&CK ID:** T1070.003
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create command IN ["*rm (Get-PSReadlineOption).
↪ HistorySavePath*", "*del (Get-PSReadlineOption).HistorySavePath*", "*Set-
↪ PSReadlineOption -HistorySaveStyle SaveNothing*", "*Remove-Item (Get-
↪ PSReadlineOption).HistorySavePath*"]
```

2.125 LP_Clearing of PowerShell Logs Detected

- **Trigger Condition:** A console history logs clear is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Indicator Removal
- **ATT&CK ID:** T1070
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
(norm_id=WinServer event_id=4103 command="Remove-Item" payload=
↪ "*consolehost*history*") OR (label=File label=Delete (object="ConsoleHost_history.txt
↪ " OR file="ConsoleHost_history.txt"))
```

2.126 LP_Clipboard Data Access Detected

- **Trigger Condition:** Adversaries collect data stored on a clipboard from users copying information within or between applications is detected.
- **ATT&CK Category:** Collection
- **ATT&CK Tag:** Clipboard Data
- **ATT&CK ID:** T1115
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label="process" label=create ("process"="*\clip.exe" OR command="*Get-Clipboard*") -
↪ user IN EXCLUDED_USERS
```

2.127 LP_Cmdkey Cached Credentials Recon Detected

- **Trigger Condition:** The usage of *cmdkey* to detect cached credentials.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 image="*\cmdkey.exe" command="*/list *" -user IN EXCLUDED_USERS
```

2.128 LP_CMSTP Detected

- **Trigger Condition:** Adversaries abuse CMSTP for proxy execution of malicious code. *CMSTP.exe* accepts an installation information file (INF) as a parameter and installs a service profile leveraged for remote access connections. Also, the adversary supplies *CMSTP.exe* with INF files infected with malicious commands.
- **ATT&CK Category:** Defense Evasion, Execution
- **ATT&CK Tag:** Signed Binary Proxy Execution, CMSTP
- **ATT&CK ID:** T1218, T1218.003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 image="*CMSTP.exe" -user IN EXCLUDED_USERS
```

2.129 LP_CMSTP Execution Detected

- **Trigger Condition:** Loading and execution of local or remote payloads using CMSTP. Adversaries abuse *CMSTP.exe* to load and execute DLLs and/or COM scriptlets (SCT) from remote servers. The execution bypasses AppLocker and other safe listing defenses since *CMSTP.exe* is a legitimate and signed Microsoft application.

- **ATT&CK Category:** Defense Evasion, Execution
- **ATT&CK Tag:** CMSTP, Component Object Model
- **ATT&CK ID:** T1218.003, T1559.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
(norm_id="WindowsSysmon" ((event_id IN [12, 13] target_object="*\cmmgr32.exe*") OR
↪ (event_id=10 call_trace="*cmlua.dll*") OR (event_id=3 "process"="*\cmstp.exe" is_
↪ initiated="true")))) OR (label="Process" label=Create parent_process="*\cmstp.exe")
```

2.130 LP_CMSTP UAC Bypass via COM Object Access

- **Trigger Condition:** Loading and execution of local or remote payloads using CMSTP is detected. Adversaries abuse CMSTP.exe to bypass User Account Control and execute arbitrary commands from a malicious INF through an auto-elevated COM interface.
- **ATT&CK Category:** Defense Evasion, Privilege Escalation
- **ATT&CK Tag:** Bypass User Access Control, CMSTP
- **ATT&CK ID:** T1548.002, T1218.003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 parent_process="*\DllHost.exe" parent_
↪ command IN ["*/Processid:{3E5FC7F9-9A51-4367-9063-A120244FBEC7}*","*/Processid:
↪ {3E000D72-A845-4CD9-BD83-80C07C3B881F}*","*/Processid:{BD54C901-076B-434E-
↪ B6C7-17C531F4AB41}*","*/Processid:{D2E7041B-2927-42FB-8E9F-7CE93B6DC937}*","
↪ "*/Processid:{E9495B87-D950-4AB5-87A5-FF6D70BF3E90}*"] integrity_level IN ["High",
↪ "System"]
```

2.131 LP_CobaltStrike Process Injection Detected

- **Trigger Condition:** Creation of remote threat with specific characteristics that are typical for Cobalt Strike beacons.
- **ATT&CK Category:** Defense Evasion

- **ATT&CK Tag:** Process Injection
- **ATT&CK ID:** T1055
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=8 start_address IN ["*0B80", "*0C7C", "*0C88"] -  
↪ user IN EXCLUDED_USERS
```

2.132 LP_Windows Command Line Execution with Suspicious URL and AppData Strings

- **Trigger Condition:** Execution of Windows command line with command line parameters URL and AppData string used by droppers.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Process Injection
- **ATT&CK ID:** T1055
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=8 start_address IN ["*0B80", "*0C7C", "*0C88"] -  
↪ user IN EXCLUDED_USERS
```

2.133 LP_Compiled HTML File Detected

- **Trigger Condition:** Adversaries abuse Compiled HTML files (.chm) to conceal malicious code.
- **ATT&CK Category:** Defense Evasion, Execution
- **ATT&CK Tag:** Signed Binary Proxy Execution, Compiled HTML File
- **ATT&CK ID:** T1218, T1218.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 image="*hh.exe" -user IN EXCLUDED_USERS
```

2.134 LP_Console History Discovery Detected

- **Trigger Condition:** Adversaries attempt to get detailed information about the console history discovery is detected.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** System Information Discovery
- **ATT&CK ID:** T1082
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create command IN ["*Get-History*", "*PSReadline\ConsoleHost_
↪ history.txt*", "(Get-PSReadlineOption).HistorySavePath*"]
```

2.135 LP_Control Panel Items - Registry Detected

- **Trigger Condition:** Adversaries abuse *control.exe* for proxy execution of malicious payloads.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Signed Binary Proxy Execution, Control Panel Items
- **ATT&CK ID:** T1218, T1218.002
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon (event_id=12 or event_id=13 or event_id=14) (target_object=
↪ "*\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ControlPanel\NameSpace*"
↪ " or target_object="*\Software\Microsoft\Windows\CurrentVersion\Controls
↪ Folder\*\ShellEx\PropertySheetHandlers\*" or target_object=
↪ "*\Software\Microsoft\Windows\CurrentVersion\Control Panel\*" ) -user IN EXCLUDED_
↪ USERS
```

2.136 LP_Copy from Admin Share Detected

- **Trigger Condition:** Copying of file from a remote C\$ or ADMIN\$ share via copy command is detected.
- **ATT&CK Category:** Lateral Movement, Command, Exfiltration
- **ATT&CK Tag:** Remote Services, SMB/Windows Admin Shares, Ingress Tool Transfer, Data from Network Shared Drive
- **ATT&CK ID:** T1021,T1021.002, T1105, T1039
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create (command="*\\\\" command="*$") OR (command=
↳ "*\Sysvol\"") ("process" IN
["*\robocopy.exe", "*\xcopy.exe"]) OR ("process"="*\cmd.exe" command="*copy")
↳ OR ("process" IN
["*\powershell.exe", "*\pwsh.exe"] command IN
["*copy-item", "*copy*", "*cp*", "* cp *", "*move *", "*move-item*", "* mi *", "* mv *"]
↳ ))
```

2.137 LP_Copying Sensitive Files with Credential Data

- **Trigger Condition:** Copying of sensitive files with credential data is detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** OS Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label=Create label="Process" (("process"="*\esentutl.exe" OR file="esentutl.exe"
↳ command IN ["*vss*", "* /m *", "* /y *"]) OR command IN ["*\windows\ntds\ntds.dit",
↳ "*\config\sam*", "*\config\security*", "*\config\system *", "*\repair\sam*",
↳ "*\repair\system*", "*\repair\security*", "*\config\RegBack\sam*",
↳ "*\config\RegBack\system*", "*\config\RegBack\security*"])
```

2.138 LP_Copyright Violation Email

- **Trigger Condition:** An email with copyright or infringement contents as message subject is received. For this alert to work, the list KNOWN_SERVER_HOST must be updated known mail servers.
- **ATT&CK Category:** Collection
- **ATT&CK Tag:** Email Collection
- **ATT&CK ID:** T1114
- **Minimum Log Source Requirement:** ExchangeMT
- **Query:**

```
device_category=Email* sender=* receiver=* -source_host IN KNOWN_SERVER_HOST
↪ subject IN ["*copyright*", "*infringement*"] | norm on receiver <user:all>@
↪ <domain:string>
```

2.139 LP_CreateMiniDump Hacktool Detected

- **Trigger Condition:** The use of the *CreateMiniDump* hack tool to dump the LSASS process memory for credential extraction on the attacker's machine is detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Credential Dumping, LSASS Memory
- **ATT&CK ID:** T1003, T1003.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
(event_id=1 (image="*\CreateMiniDump.exe*" OR hash=
↪ "4a07f944a83e8a7c2525efa35dd30e2f")) OR (event_id=11 file="*\lsass.dmp*")
```

2.140 LP_CreateRemoteThread API and LoadLibrary

- **Trigger Condition:** The use of CreateRemoteThread API and LoadLibrary function to inject DLL into a process is detected.
- **ATT&CK Category:** Defense Evasion

- **ATT&CK Tag:** Process Injection
- **ATT&CK ID:** T1055
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=8 start_module="*\kernel32.dll" start_function=
↪ "LoadLibraryA" -user IN EXCLUDED_USERS
```

2.141 LP_Command Obfuscation via Character Insertion

- **Trigger Condition:** Command obfuscation of command prompt by character insertion is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, Windows Command Shell
- **ATT&CK ID:** T1059, T1059.003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label="Process" label=Create parent_process='*\cmd.exe' parent_command="cmd*/c*" [?]
↪ norm on parent_command <command_match:'[^\w](s\^+e\^*t|s\^*e\^+t)[^\w]'\> [?]
↪ search command_match=*
```

2.142 LP_Command Obfuscation via Environment Variable Concatenation Reassembly

- **Trigger Condition:** Command obfuscation in command prompt by environment variable concatenation reassembly is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, Windows Command Shell
- **ATT&CK ID:** T1059, T1059.003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label="Process" label=Create "parent_process"='*cmd.exe' command='cmd*/c*' | norm
→ on command <command_match:'%[^%]+%{4}'> | rename command as changed_
→ command, command_match as command | search command=*
```

2.143 LP_Credential Access via Input Prompt Detected

- **Trigger Condition:** A command executed to capture user input to obtain the credentials is detected.
- **ATT&CK Category:** Credential Access, Collection
- **ATT&CK Tag:** Input Capture, GUI Input Capture
- **ATT&CK ID:** T1056, T1056.002
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
((label="Process" label=Create command="*UI.promptforcredential*" command=
→ "*getnetworkcredential*") OR (norm_id=WinServer event_id=4104 script_block="*UI.
→ promptforcredential*" script_block="*getnetworkcredential*")) | rename script_block as
→ command
```

2.144 LP_Credential Dump Tools Dropped Files Detected

- **Trigger Condition:** Creation of files with a well-known filename, or parts of credential dump software or files produced by them is detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=11 file IN ["*\\pwdump*", "*\\kirbi*", "*\\pwhashes*",
→ "*\\wce_ccache*", "*\\wce_krbtkts*", "*\\fgdump-log*", "*\\test.pwd", "*\\lsremora64.dll",
→ "*\\lsremora.dll", "*\\fgexec.exe", "*\\wceaux.dll", "*\\SAM.out", "*\\SECURITY.out",
→ "*\\SYSTEM.out", "*\\NTDS.out", "*\\DumpExt.dll", "*\\DumpSvc.exe", "*\\cachedump64.
→ exe", "*\\cachedump.exe", "*\\pstgdump.exe", "*\\servpw.exe", "*\\servpw64.exe",
→ "*\\pwdump.exe", "*\\procdump64.exe"] -user IN EXCLUDED_USERS
```

2.145 LP_Credential Dumping with ImageLoad Detected

- **Trigger Condition:** Attempts by adversaries to dump credentials using DLL images are detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** OS Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Image" label="Load" image IN ["*C:\Windows\System32\saml.dll*",
↪ "*C:\Windows\System32\WinSCard.dll*", "*C:\Windows\System32\cryptdll.dll*",
↪ "*C:\Windows\System32\hid.dll*", "*C:\Windows\System32\vaultcli.dll*"] - "process" IN [
↪ "*\Sysmon.exe", "*\svchost.exe", "*\logonui.exe"] -user IN EXCLUDED_USERS
```

2.146 LP_Credentials Access in Files Detected

- **Trigger Condition:** Command line arguments containing pattern to search pass in files are detected. Adversaries can use this technique to search for local file systems and remote file shares to discover files containing insecurely stored credentials.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Unsecured Credentials, Credentials in Files
- **ATT&CK ID:** T1552, T1552.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create command IN ["*findstr* /si pass*", "*select-string -Pattern*
↪ pass*", "*|list vdir*/text:password*"]
```

2.147 LP_Registry Enumeration for credentials Detected

- **Trigger Condition:** Search of the compromised system's registry to find and obtain insecurely stored credentials is detected. Adversaries can inspect the Windows Registry on compromised systems for insecurely stored credentials and passwords, as the registry contains configuration data used by the system and software.

- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Unsecured Credentials, Credentials in Registry
- **ATT&CK ID:** T1552, T1552.002
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create "process"="*\reg.exe" command="*query*" command="*/
↪t*" command="*REG_SZ*" command="*/s*" (command=
↪"*HKCU\Software\SimonTatham\PuTTY\Sessions*" OR (command="*/f*" command IN [
↪"*HKLM*", "*HKCU*"])))
```

2.148 LP_Default Account privilege elevation followed by restoration of previous account state

- **Trigger Condition:** A user is added to a group or assigned privilege followed by restoration or removal from those rights.
- **ATT&CK Category:** Persistence, Privilege Escalation
- **ATT&CK Tag:** Account Manipulation, Exploitation for Privilege Escalation
- **ATT&CK ID:** T1098, T1068
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
[label=User label=Group label=Management label=Add | rename target_user as
↪account] as s1 followed by [ label=User label=Group (label=Remove or label=Delete) -
↪target_user=*$ | rename target_user as account] as s2 on s1.account=s2.account |
↪rename s1.log_ts as ElevationTime_ts, s2.log_ts as RestorationTime_ts, s1.user as
↪UserElevation, s2.user as UserRestoration, s1.account as Account, s1.message as
↪PrivilegeElevation, s2.message as PrivilegeRestoration
```

2.149 LP_Default Blocked Inbound Traffic followed by Allowed Event

- **Trigger Condition:** Blocked inbound traffic followed by allowed traffic is detected.
- **ATT&CK Category:** Command and Control

- **ATT&CK Tag:** Proxy
- **ATT&CK ID:** T1090
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

```
[norm_id=*firewall or norm_id=*IDS label=Block or label=Deny label=Connection -source_
↪address IN HOMENET destination_address IN HOMENET] as s1 followed by [norm_
↪id=*firewall label=Allow label=Connection -source_address IN HOMENET destination_
↪address IN HOMENET] as s2 on s1.source_address=s2.source_address | rename s1.
↪source_address as source
```

2.150 LP_Default Blocked Outbound Traffic followed by Allowed Event

- **Trigger Condition:** Blocked outbound traffic followed by allowed traffic is detected.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Proxy
- **ATT&CK ID:** T1090
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

```
[norm_id=*firewall or norm_id=*IDS label=Block or label=Deny label=Connection source_
↪address IN HOMENET -destination_address IN HOMENET] as s1 followed by [norm_
↪id=*firewall label=Allow label=Connection source_address IN HOMENET -destination_
↪address IN HOMENET]
as s2 on s1.source_address=s2.source_address | rename s1.source_address as source
```

2.151 LP_Default Brute Force Attack Successful

- **Trigger Condition:** Five failed users login attempts followed by a successful login from the same user within five minutes is detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Brute Force

- **ATT&CK ID:** T1110
- **Minimum Log Source Requirement:** Windows, AWS, Firewall, WAF, Unix
- **Query:**

```
[label=User label=Login label=Fail -user=*$ | chart count() as cnt by user | search cnt > 5 ]
↪ as s1 followed by [label=User label=Login label=Successful] as s2 on s1.user = s2.user
↪ rename s2.user as user
```

2.152 LP_Default Connection Attempts on Closed Port

- **Trigger Condition:** A connection is established on closed ports. For the alert to work, you must update the list ALERT_OPEN_PORTS, which includes a list of open ports.
- **ATT&CK Category:** Command And Control, Persistence, Privilege Escalation
- **ATT&CK Tag:** Traffic Signaling, Port Knocking
- **ATT&CK ID:** T1205, T1205.001
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

```
label=Connection -destination_port IN ALERT_OPEN_PORTS source_address=*
↪ destination_port=*
```

2.153 LP_Default CPU Usage Status

- **Trigger Condition:** The use of CPU exceeds 90%.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Logpoint
- **Query:**

```
label=Metrics label=CPU label=Usage use>90
```

2.154 LP_Default Device Stopped Sending Logs for Half an Hour

- **Trigger Condition:** A device that has not sent logs for half an hour or more is detected.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Service Stop
- **ATT&CK ID:** T1489
- **Minimum Log Source Requirement:** Firewall, IDS, IPS, Proxy Server, Windows, Unix
- **Query:**

```
| chart max(col_ts) as max_time_ts by device_ip | process current_time(a) as time | chart
↪ max(time-max_time_ts) as elapsed_time by max_time_ts, device_ip | search elapsed_
↪ time>1800
```

2.155 LP_Default DNS Tunneling Detection - Query Size

- **Trigger Condition:** Traffic with more than 64 characters in Application Layer Protocol and DNS is detected.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Application Layer Protocol, DNS, Dynamic Resolution, Domain Generation Algorithms
- **ATT&CK ID:** T1071,T1071.004,T1568,T1568.002
- **Minimum Log Source Requirement:** Firewall, IDS/IPS, Webserver, DNS Server
- **Query:**

```
norm_id=* "DNS" qname=* | process count_char(qname) as charCount | search
↪ charCount>64
```

2.156 LP_Default Excessive Blocked Connections

- **Trigger Condition:** 50 blocked or denied connections are observed from the same source within a minute.
- **ATT&CK Category:** Impact, Command and Control
- **ATT&CK Tag:** Network Denial of Service, Endpoint Denial of Service, Proxy
- **ATT&CK ID:** T1498, T1499, T1090
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

```
[50 label=Connection (label=Deny OR label=Block) source_address=* having same source_
↪address within 1 minute]
```

2.157 LP_Default File Association Changed

- **Trigger Condition:** Adversaries establish persistence and/or elevate privileges by executing malicious content triggered by a file type association.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Event Triggered Execution, Change Default File Association
- **ATT&CK ID:** T1546, T1546.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon (event_id=12 or event_id=13 or event_id=14) (target_object=
↪"*\\SOFTWARE\\Classes\\*" or target_object=
↪"*\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Explorer\\GlobalAssocChangedCounter*"
↪) -user IN EXCLUDED_USERS
```

2.158 LP_Default Guest Account Added to Administrative Group

- **Trigger Condition:** A guest account is added to security group management.

- **ATT&CK Category:** Credential Access, Persistence, Privilege Escalation, Defense Evasion, Initial Access
- **ATT&CK Tag:** Account Manipulation, Abuse Elevation Control Mechanism, Bypass User Access Control, Valid Accounts
- **ATT&CK ID:** T1098, T1548, T1548.002, T1078
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
label=Security label=Group label=Management label=Add (member_sid="S-1-5-21-*501
↪ " OR target_id="S-1-5-21-*501") | rename target_user as member, group as group_
↪ name
```

2.159 LP_Default Inbound Connection with Non-Whitelist Country

- **Trigger Condition:** An inbound connection established with a non-whitelisted country is detected. For this alert to work, you must update the list WHITELIST_COUNTRY.
- **ATT&CK Category:** Command And Control
- **ATT&CK Tag:** Proxy
- **ATT&CK ID:** T1090
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

```
-source_address IN HOMENET destination_address IN HOMENET | process geoip(source_
↪ address) as country | search -country IN WHITELIST_COUNTRY
```

2.160 LP_Default Inbound RDP Connection

- **Trigger Condition:** Inbound RDP traffic events on destination port 3389 is detected.
- **ATT&CK Category:** Lateral Movement, Command And Control
- **ATT&CK Tag:** Remote Services, Application Layer Protocol

- **ATT&CK ID:** T1021, T1071
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

```
label=Connection -source_address IN HOMENET destination_address in HOMENET  
↪ destination_port=3389
```

2.161 LP_Default Inbound SMB Connection

- **Trigger Condition:** Inbound SMB traffic events on destination port 445 is detected.
- **ATT&CK Category:** Lateral Movement, Command And Control
- **ATT&CK Tag:** Application Layer Protocol
- **ATT&CK ID:** T1071
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

```
label=Connection -source_address IN HOMENET destination_address in HOMENET  
↪ destination_port=445
```

2.162 LP_Default Inbound SMTP Connection

- **Trigger Condition:** Inbound SMTP traffic event on destination ports 25, 456, 587, 2525, and 2526 is detected.
- **ATT&CK Category:** Command And Control
- **ATT&CK Tag:** Application Layer Protocol
- **ATT&CK ID:** T1071
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

```
label=Connection -source_address IN HOMENET destination_address in HOMENET  
↪ destination_port in [25,456,587,2525,2526]
```

2.163 LP_Default Inbound SSH Connection

- **Trigger Condition:** Inbound Remote Services SSH traffic event on destination port 22 is detected.
- **ATT&CK Category:** Lateral Movement, Command and Control
- **ATT&CK Tag:** Remote Services, Application Layer Protocol
- **ATT&CK ID:** T1021, T1071
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

```
label=Connection -source_address IN HOMENET destination_address in HOMENET
↔ destination_port=22
```

2.164 LP_Default IRC connection

- **Trigger Condition:** The IRC connection is detected. For this alert to work, you must update ALERT_IRC_PORT list with possible IRC ports.
- **ATT&CK Category:** Command and Control, Discovery
- **ATT&CK Tag:** Proxy, Network Service Scanning
- **ATT&CK ID:** T1090, T1046
- **Minimum Log Source Requirement:** Firewall, IDS/IPS, Webserver
- **Query:**

```
(destination_port IN ALERT_IRC_PORT OR destination_port=6667)
```

2.165 LP_Default Malware Detected

- **Trigger Condition:** A malware or a virus is detected in the system.
- **ATT&CK Category:** Resource Development
- **ATT&CK Tag:** Develop Capabilities, Malware
- **ATT&CK ID:** T1587, T1587.001

- **Minimum Log Source Requirement:** Antivirus
- **Query:**

```
(label=Virus OR label=Malware ) (label=Detect OR label=Find) (virus=* OR malware=* OR
↪ file=* OR path=*) | rename malware as virus
```

2.166 LP_Default Malware not Cleaned

- **Trigger Condition:** A malware clean events including deletion, removal, and quarantine, is followed by detecting the same malware in the same host.
- **ATT&CK Category:** Discovery, Defense Evasion
- **ATT&CK Tag:** Network Service Scanning,Exploitation for Defense Evasion,Software Discovery, Security Software Discovery
- **ATT&CK ID:** T1046, T1211, T1518, T1518.001
- **Minimum Log Source Requirement:** Antivirus
- **Query:**

```
norm_id=* malware=* action IN ["*delete*", "*remove*", "*quarantine*"] as s1 followed
↪ by [norm_id=* malware=* source_address=] as s2 on s1.malware=s2.malware | process
↪ compare(s1.source_address, s2.source_address) as match | search match=true | rename
↪ s1.source_address as source_address, s1.malware as malware
```

2.167 LP_Default Malware Removed

- **Trigger Condition:** Removal of malware or a virus from the system is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Indicator Removal on Host, Obfuscated Files or Information, Indicator Removal from Tools
- **ATT&CK ID:** T1070, T1027, T1027.005
- **Minimum Log Source Requirement:** Antivirus
- **Query:**

```
(label=Virus OR label=Malware ) (label=Remove OR label=Clean OR label=Delete) -label=
↪ "Not" -label=Error | rename malware as virus | search virus=*
```

2.168 LP_Default Memory Usage Status

- **Trigger Condition:** Physical memory usage exceeds 90% of the total memory available is detected.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Logpoint
- **Query:**

```
label=Metrics label=Memory label=Usage object="Physical Memory" use>90
```

2.169 LP_Default Network Configuration Change on Network Device

- **Trigger Condition:** A change in the core network event source, such as a router or switch, is detected.
- **ATT&CK Category:** Persistence, Credential Access, Defense Evasion, Privilege Escalation
- **ATT&CK Tag:** Modify Existing Service, Account Manipulation, Abuse Elevation Control Mechanism, Bypass User Access Control, Impair Defenses, Indicator Blocking, Modify Registry, Exploitation for Privilege Escalation
- **ATT&CK ID:** T1098, T1548, T1562, T1562.006, T1112, T1068
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

```
label=Network label=Configuration (label=Change OR label=Modify OR label=Reset OR
↪ label=Enable OR label=Disable OR label=Add or label=Delete or label=Undelete)
```

2.170 LP_Default Outbound Connection with Non-Whitelist Country

- **Trigger Condition:** Outbound connections with non-whitelisted countries are detected. For this alert to work, you must update the list WHITELIST_COUNTRY.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Proxy
- **ATT&CK ID:** T1090
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

```
source_address IN HOMENET -destination_address IN HOMENET | process
↳ geoip(destination_address) as country | search -country IN WHITELIST_COUNTRY
```

2.171 LP_Default Outbound Traffic from Unusual Source

- **Trigger Condition:** Outbound traffic is detected from an unusual source. For this alert to work, you must update the list ALERT_UNUSUAL_SOURCE with source addresses from which outbound connections are not established.
- **ATT&CK Category:** Command and Control, Exfiltration
- **ATT&CK Tag:** Proxy, Automated Exfiltration, Exfiltration Over C2 Channel
- **ATT&CK ID:** T1090, T1020, T1041
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

```
source_address IN ALERT_UNUSUAL_SOURCE source_address IN HOMENET
↳ (label=Traffic OR label=Connection) -destination_address IN HOMENET
```

2.172 LP_Default Port Scan Detected

- **Trigger Condition:** Connection from multiple ports of a public IP address to a destination address is detected.
- **ATT&CK Category:** -

- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Firewall, IDS, IPS, Webserver
- **Query:**

```
-source_address IN HOMENET destination_port=* | chart distinct_count(destination_
↪port) as CNT by source_address, destination_address | search CNT>50
```

2.173 LP_Default Possible Cross Site Scripting Attack Detected

- **Trigger Condition:** The script tag indicating the XSS attack is detected in the URL.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** Exploiting Public-Facing Application
- **ATT&CK ID:** T1190
- **Minimum Log Source Requirement:** Firewall, IDS/IPS, Webserver
- **Query:**

```
norm_id=* url IN ["*<script>*", "%3c%73%63%72%69%70%74%3e*", "%3cscript%3e*"]2
↪or resource IN ["*<script>*", "%3c%73%63%72%69%70%74%3e*", "%3cscript%3e*"]2
↪| rename resource as url
```

2.174 LP_Default Possible Network Performance Degradation Detected

- **Trigger Condition:** 100 or more network-related errors are detected in security devices within five minutes.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Network Denial of Service
- **ATT&CK ID:** T1498
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

```
norm_id=* ((label=Connection (label=Error or label=Fail or label=Deny or label=Drop)) or
↪(label="Limit" label=Exceed) or (label=Packet label=Drop) or (label=Protocol
↪label=Deny)) | chart count() as Event by device_ip, norm_id | search Event>1000
```

2.175 LP_Default Possible Non-PCI Compliant Inbound Network Traffic Detected

- **Trigger Condition:** An inbound connection is detected in secure devices over non-compliant ports as specified by PCI compliance practices. For this alert to work, you must update the list NON_PCI_COMPLIANT_PORT.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Proxy
- **ATT&CK ID:** T1090
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

```
label=Inbound label=Connection destination_port IN NON_PCI_COMPLIANT_PORT -
↪source_address IN HOMENET
```

2.176 LP_Default Possible Spamming Zombie

- **Trigger Condition:** Systems other than mail servers attempt to establish an outbound SMTP connection is detected. For this alert to work, you must update the list MAIL_SERVERS with possible mail servers to remove false positives. For example, *exchange*, *postfix*, and so on.
- **ATT&CK Category:** Command and Control, Impact
- **ATT&CK Tag:** Proxy, Application Layer Protocol, Network Denial of Service
- **ATT&CK ID:** T1090, T1071, T1498
- **Minimum Log Source Requirement:** All except Mail Server
- **Query:**

```
-norm_id IN MAIL_SERVERS destination_port IN ["25", "587"]
```

2.177 LP_Default Possible SQL Injection Attack

- **Trigger Condition:** SQL character injection in the input field of a web application is detected.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** Exploit Public-Facing Application
- **ATT&CK ID:** T1190
- **Minimum Log Source Requirement:** Firewall, IDS/IPS, Webserver
- **Query:**

```
norm_id=* url IN SQL_INJECTION_CHARACTER or resource IN SQL_INJECTION_
↳ CHARACTER | rename resource as url
```

2.178 LP_Default Possible System Instability State Detected

- **Trigger Condition:** The instability of a system is detected. For example, a system shut down or restarts more than five times within ten minutes. A correlation rule is designed to detect if a system has become unstable.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** System Shutdown/Reboot
- **ATT&CK ID:** T1529
- **Minimum Log Source Requirement:** OS
- **Query:**

```
[5 (-label=Require -label=Request -label=Reply) (label=Restart OR label=Shutdown OR
↳ label=Boot) having same device_ip within 10 minutes]
```

2.179 LP_Default PowerSploit and Empire Schtasks Persistence

- **Trigger Condition:** Creation of a *schtask* via PowerSploit or Empire Default Configuration is detected.

- **ATT&CK Category:** Execution, Persistence, Privilege Escalation
- **ATT&CK Tag:** Scheduled Task/Job, Scheduled Task, Command and Scripting Interpreter, PowerShell + **ATT&CK ID:** T1053, T1053.005, T1059, T1059.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create parent_process="*\powershell.exe" "process"="*\schtasks.
↪exe" command = "*/Create*" command = "*/SC*" (command in ["*ONLOGON*",
↪"*DAILY*", "*ONIDLE*", "*Updater*"] command = "*/TN*" command = "*Updater*"
↪command = "*/TR*" command = "*powershell*")
```

2.180 LP_Default Successful Login outside Normal Hour

- **Trigger Condition:** Successful user login beyond regular office hour is detected. You can adjust the regular work hour according to your company.
- **ATT&CK Category:** Defense Evasion, Persistence, Privilege Escalation, Initial Access
- **ATT&CK Tag:** Valid Accounts
- **ATT&CK ID:** T1078
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
label=Login label=Successful target_user=* ((day_of_week(log_ts)=2 OR day_of_week(log_
↪ts)=3 OR day_of_week(log_ts)=4 OR day_of_week(log_ts)=5 OR day_of_week(log_ts)=6)
↪(hour(log_ts)>0 hour(log_ts)<9) OR hour(log_ts)>17) OR (day_of_week(log_ts) IN [1, 7])
↪rename target_user as user
```

2.181 LP_Default Successful Login Using a Default Account

- **Trigger Condition:** Successful login attempts using a vendor default account is detected. The alert is essential for those organizations employing Payment Card Industry (PCI) Compliance.
- **ATT&CK Category:** Defense Evasion, Persistence, Privilege Escalation, Initial Access

- **ATT&CK Tag:** Valid Accounts, Default Accounts
- **ATT&CK ID:** T1078, T1078.001
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
label=User label=Login label=Successful (target_user=* OR user=*) (target_user IN
↪ DEFAULT_USERS OR user IN DEFAULT_USERS) | rename target_user as user
```

2.182 LP_Default System Time Change

- **Trigger Condition:** The system time is changed or when Logpoint command `/opt/immune/installed/system/root_actions/*_ntp.sh` is executed.
- **ATT&CK Category:** Persistence, Impact
- **ATT&CK Tag:** Modify Existing Service, Data Destruction
- **ATT&CK ID:** T1485
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
(label=System label=Time label=Change) OR (label=Execute label=Command command=
↪ "/opt/immune/installed/system/root_actions/*_ntp.sh")
```

2.183 LP_Default TCP Probable SynFlood Attack

- **Trigger Condition:** Security devices detect ten TCP Syn flood events within a minute.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Endpoint Denial of Service
- **ATT&CK ID:** T1499
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

[10 TCP SYN having same source_address within 1 minute]

2.184 LP_Default Unapproved Port Activity Detected

- **Trigger Condition:** A user uses unapproved ports.
- **ATT&CK Category:** Defense Evasion, Persistence, Command And Control
- **ATT&CK Tag:** Boot or Logon Autostart Execution, Port Monitors, Traffic Signaling, Port Knocking
- **ATT&CK ID:** T1547, T1547.01, T1205, T1205.001
- **Minimum Log Source Requirement:** Firewall, IDS/IPS, Webserver
- **Query:**

```
norm_id=* source_port IN UNAPPROVED_PORT or destination_port IN UNAPPROVED_
↳ PORT or port IN UNAPPROVED_PORT | rename source_port as port, destination_port
↳ as port
```

2.185 LP_Default Unusual Number of Failed Vendor User Login

- **Trigger Condition:** Failed user logins using default credentials for more than 10 times are detected. For this alert to work, you must update the list DEFAULT_USERS with default vendor user names.
- **ATT&CK Category:** Defense Evasion, Persistence, Privilege Escalation, Initial Access
- **ATT&CK Tag:** Valid Accounts, Default Accounts
- **ATT&CK ID:** T1078, T1078.001
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
label=User label=Login label=Fail (target_user=* OR user=*) (target_user IN DEFAULT_
↳ USERS OR user IN DEFAULT_USERS) | rename target_user as user | chart count() as
↳ Event by user, source_address | search Event>10
```

2.186 LP_HandleKatz Duplicating LSASS Handle

- **Trigger Condition:** The HandleKatz tool directly opening LSASS process to duplicate its handle is detected.
- **ATT&CK Category:** Execution, Credential Access
- **ATT&CK Tag:** LSASS Memory, Native API
- **ATT&CK ID:** T1003.001, T1106
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=10 access="0x1440" "image"="*\lsass.exe" call_
↪ trace="C:\Windows\System32\ntdll.dll+*" call_trace="*|UNKNOWN(*" call_trace="*)"
```

2.187 LP_PowerShell Execution Policy Modification Detected

- **Trigger Condition:** The registry value for the PowerShell execution policy is changed.
- **ATT&CK Category:** Execution, Defense Evasion
- **ATT&CK Tag:** PowerShell, Modify Registry
- **ATT&CK ID:** T1059.001, T1112
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
::S
```

```
norm_id=WindowsSysmon      event_id=13      event_type=setvalue
target_object IN ["ShellIdsMicrosoft.PowerShellExecutionPolicy","PoliciesMicrosoftWindows
detail IN ["Bypass","RemoteSigned","Unrestricted"] -image IN
["C:\Windows\System32*","C:\Windows\SysWOW64*"]
```

2.188 LP_Devtoolslauncher Executes Specified Binary

- **Trigger Condition:** The use of *devtoolslauncher* to execute other binaries is detected. Devtoolslauncher is a Microsoft Windows executable, a part of VS/VSCode installation, that enables the use of developer tools by other applications. Adversaries attempt to bypass process or signature-based defenses by proxying the execution of malicious content with signed binaries using *devtoolslauncher* and *LaunchForDeploy* commands.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** System Binary Proxy Execution
- **ATT&CK ID:** T1218
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*\devtoolslauncher.exe" command=
↳ "*LaunchForDeploy*" -user IN EXCLUDED_USERS
```

2.189 LP_DHCP Callout DLL Installation Detected

- **Trigger Condition:** Installation of a *Callout DLL* via *CalloutDlls* and *CalloutEnabled* parameters in the registry, used to execute code in the context of the DHCP server is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Hijack Execution Flow, DLL Side-Loading, Modify Registry
- **ATT&CK ID:** T1574, T1574.002, T1112
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=13 target_object IN [
↳ "*\Services\DHCP\Parameters\CalloutDlls",
↳ "*\Services\DHCP\Parameters\CalloutEnabled"] -user IN EXCLUDED_USERS
```

2.190 LP_DHCP Server Error Failed Loading the CallOut DLL

- **Trigger Condition:** DHCP server error in which a specified Callout DLL in registry cannot be loaded.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Hijack Execution Flow, DLL Side-Loading
- **ATT&CK ID:** T1574, T1574.002
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WinServer event_id IN ["1031", "1032", "1034"] event_source="Microsoft-  
↪ Windows-DHCP-Server" -user IN EXCLUDED_USERS
```

2.191 LP_DHCP Server Loaded the CallOut DLL

- **Trigger Condition:** A DHCP server loads callout DLL in the registry. The alert has been translated from its corresponding sigma rule. For more information, you can check the sigma rule.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Hijack Execution Flow, DLL Side-Loading
- **ATT&CK ID:** T1574, T1574.002
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=1033 -user IN EXCLUDED_USERS
```

2.192 LP_Direct Autorun Keys Modification Detected

- **Trigger Condition:** A modification to the direct autorun keys on a system (ASEP) in the registry using *reg.exe* is detected. These keys are used to run programs or scripts automatically when a specific event occurs, such as when the system starts up or when a user logs in. Adversaries may use this technique to establish

persistence on a system and ensure that their malware or other malicious programs are launched automatically whenever the system is restarted. They may also use it to evade detection by disguising their malware as a legitimate program automatically launched by the system. This alert requires registry auditing to be enabled. When an admin user modifies the keys, false positive alerts may be triggered.

- **ATT&CK Category:** Persistence, Privilege Escalation
- **ATT&CK Tag:** Boot or Logon Autostart Execution, Registry Run Keys/Startup Folder
- **ATT&CK ID:** T1547, T1547.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*\reg.exe" command="*add*"
↪ command IN ["*\software\Microsoft\Windows\CurrentVersion\Run*",
↪ "*\software\Microsoft\Windows\CurrentVersion\RunOnce*",
↪ "*\software\Microsoft\Windows\CurrentVersion\RunOnceEx*",
↪ "*\software\Microsoft\Windows\CurrentVersion\RunServices*",
↪ "*\software\Microsoft\Windows\CurrentVersion\RunServicesOnce*",
↪ "*\software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit*",
↪ "*\software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell*",
↪ "*\software\Microsoft\Windows NT\CurrentVersion\Windows*",
↪ "*\software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders*",
↪ "*\system\CurrentControlSet\Control\SafeBoot\AlternateShell*"] -user IN
↪ EXCLUDED_USERS
```

2.193 LP_Disable of ETW Trace Detected

- **Trigger Condition:** A command that clears or disables the ETW trace log, indicating a logging evasion attempt by adversaries. Adversaries can cease the flow of logging temporarily or permanently without generating any additional event clear log entries from this method.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Impair Defenses, Indicator Blocking
- **ATT&CK ID:** T1562, T1562.006
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label=Create label="process" ((command="* cl */Trace*" ) OR (command="* clear-log */
↳ Trace*" ) OR (command="* sl* /e:false*" ) OR (command="* set-log* /e:false*" ) OR
↳ (command="* Remove-EtwTraceProvider*" command="* EventLog-Microsoft-Windows-
↳ WMI-Activity-Trace*" command="* {1418ef04-b0b4-4623-bf7e-d74ab47bbdaa}*") OR
↳ (command="* Set-EtwTraceProvider*" command="* {1418ef04-b0b4-4623-bf7e-
↳ d74ab47bbdaa}*") command="* EventLog-Microsoft-Windows-WMI-Activity-Trace*"
↳ command="* 0x11*" ) OR (command="* logman update trace*" command="* --p *")
↳ command="* -ets *")) -user IN EXCLUDED_USERS
```

2.194 LP_MiniNt Registry Key Addition

- **Trigger Condition:** The addition of a key *MiniNt* to the registry is detected. Windows Event Log service will stop the write events after reboot.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Impair Defenses, Disable or Modify Tools
- **ATT&CK ID:** T1562, T1562.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon label=Registry label=Set label=Value target_object=
↳ "HKLM\SYSTEM\CurrentControlSet\Control\MiniNt" -user IN EXCLUDED_USERS
```

2.195 LP_Discovery via Discovery via PowerSploit Recon Module Detected

- **Trigger Condition:** Adversaries abuse Command and Script Interpreters to execute scripts via the PowerSploitReconnaissance module. For this alert to work, you must update the list POWERSPLOIT_RECON_MODULES.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, PowerShell
- **ATT&CK ID:** T1059, T1059.001
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4104 (scriptblocktext in POWERSPLOIT_RECON_
↳ MODULES OR script_block in POWERSPLOIT_RECON_MODULES) -user IN EXCLUDED_
↳ USERS | rename scriptblocktext as script_block
```

2.196 LP_DLL Load via LSASS Detected

- **Trigger Condition:** A method to load DLL via the LSASS process using an undocumented registry key is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Boot or Logon Autostart Execution, LSASS Driver
- **ATT&CK ID:** T1547, T1547.008
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id IN ["12", "13"] target_object IN [
↳ "*\CurrentControlSet\Services\NTDS\DirectoryServiceExtPt*",
↳ "*\CurrentControlSet\Services\NTDS\LsaDbExtPt*"]
```

2.197 LP_DNS Server Error Failed Loading the ServerLevelPluginDLL

- **Trigger Condition:** Application Layer Protocol and DNS server error where a specified plugin DLL in the registry cannot be loaded.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Hijack Execution Flow, DLL Side-Loading
- **ATT&CK ID:** T1574, T1574.002
- **Minimum Log Source Requirement:** DNS Server
- **Query:**

```
event_source="DNS Server" event_id IN ["150", "770"]
```

2.198 LP_DNS ServerLevelPluginDll Install

- **Trigger Condition:** Installation of a plugin DLL via the ServerLevelPluginDll parameter in the registry used to execute code in Application Layer Protocol and DNS server.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Hijack Execution Flow, DLL Side-Loading
- **ATT&CK ID:** T1574, T1574.002
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon (event_id=13 target_object=
↪ "*\services\DNS\Parameters\ServerLevelPluginDll") OR (event_id=1 command=
↪ "dnscmd.exe /config /serverlevelpluginDll *") -user IN EXCLUDED_USERS
```

2.199 LP_Domain Trust Discovery Detected

- **Trigger Condition:** Adversaries attempt to gather information on domain trust relationships is detected. Domain trust is a relationship between two domains that allows users in one domain to be authenticated in the other domain. It enables users to access resources in a trusted domain as if they were local. Adversaries may attempt to establish domain trusts to access additional resources or move laterally within an organization's network. They may also use domain trusts to hide their activities or to evade detection.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Domain Trust Discovery
- **ATT&CK ID:** T1482
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create (("process"="*\dsquery.exe" command="*-filter*"
↪ command="*trustedDomain*") OR ("process"="*\nltest.exe" command="*domain_
↪ trusts*")) -user IN EXCLUDED_USERS
```

2.200 LP_dotNET DLL Loaded Via Office Applications

- **Trigger Condition:** Assembly of DLL loaded by the Office Product is detected.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** Phishing, Spearphishing Attachment
- **ATT&CK ID:** T1566, T1566.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=7 "process" IN ["*\winword.exe*", "*\powerpnt.exe*",
↪ "\excel.exe*", "*\outlook.exe*"] image="*C:\Windows\assembly\*" -user IN [?]
↪ EXCLUDED_USERS
```

2.201 LP_DPAPI Domain Backup Key Extraction Detected

- **Trigger Condition:** Tools extracting the LSA secret DPAPI domain backup key from Domain Controllers are detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
(norm_id=WinServer event_id=4662 object_type="SecretObject" access_mask="0x2" [?]
↪ object_name="*BCKUPKEY") -user IN EXCLUDED_USERS
```

2.202 LP_DPAPI Domain Master Key Backup Attempt

- **Trigger Condition:** An attempt to backup DPAPI master key is detected. The event is generated on the source and not on the Domain Controller.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Credential Dumping

- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4692 -user IN EXCLUDED_USERS
```

2.203 LP_Dridex Process Pattern Detected

- **Trigger Condition:** A typical dridex process patterns are detected.
- **ATT&CK Category:** Defense Evasion, Privilege Escalation
- **ATT&CK Tag:** Process Injection
- **ATT&CK ID:** T1055
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create (("process"="*\svchost.exe" command="*C:\Users\*"
↪ command="*\Desktop\*" -parent_process="C:\Windows\System32\*" ) OR (parent_
↪ process="*\excel.exe" "process"="*\regsvr32.exe" command IN ["*-s *",
↪ "*\AppData\Local\Temp\*" ] -command="*.dll*") OR (parent_process="*\svchost.exe" ((
↪ "process"="*\whoami.exe" command="*/all*") OR ("process" IN ["*\net.exe", "*\net1.
↪ exe"] command="* view*")))) -user IN EXCLUDED_USERS
```

2.204 LP_Droppers Exploiting CVE-2017-11882 Detected

- **Trigger Condition:** The exploitation using CVE-2017-11882 to start EQNEDT32.EXE and other sub-processes like mshta.exe are detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Exploitation for Defense Evasion
- **ATT&CK ID:** T1211
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 parent_image="*\EQNEDT32.EXE" -user IN 
↪ EXCLUDED_USERS
```

2.205 LP_Drupal Arbitrary Code Execution Detected

- **Trigger Condition:** The exploitation of arbitrary code execution vulnerability (CVE-2018-7600) in Drupal, is detected.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** Exploit Public-Facing Application
- **ATT&CK ID:** T1190
- **Minimum Log Source Requirement:** Firewall, IDS/IPS, Webserver
- **Query:**

```
norm_id=* label=Access request_method=POST resource='ajax_form*drupal*ajax'
```

2.206 LP_Elevated Command Prompt Activity by Non-Admin User Detected

- **Trigger Condition:** The execution of an elevated command prompt by a non-admin user.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command-Line Interface
- **ATT&CK ID:** T1059
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4688 -user IN ADMINS "process"="cmd.exe"
token_elevation_type="*(2)" -user IN EXCLUDED_USERS
```

2.207 LP EMC Possible Ransomware Detection

- **Trigger Condition:** Suspicious data activity affecting more than 200 files or in-house baseline is detected.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Data Encrypted for Impact, Data Destruction, Proxy
- **ATT&CK ID:** T1486, T1485, T1090
- **Minimum Log Source Requirement:** EMC

- **Query:**

```
label=EMC -"bytesWritten"="0" -"bytesWritten"="0x0" event="0x80"
flag=0x2 userSid=*| chart count() as handle by userSid, clientIP | search
handle>200
```

2.208 LP_Empire PowerShell Launch Parameters

- **Trigger Condition:** Suspicious PowerShell command line parameters used in Empire are detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, PowerShell
- **ATT&CK ID:** T1059, T1059.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create command IN ["*-NoP -sta -Nonl -W Hidden -Enc *", "* -
↳noP -sta -w 1 -enc *", "*-NoP -Nonl -W Hidden -enc *", "* -enc SQB*", "* -nop -exed
↳bypass -EncodedCommand*"] -user IN EXCLUDED_USERS
```

2.209 LP_Empire PowerShell UAC Bypass Detected

- **Trigger Condition:** Empire Command and Scripting Interpreter and PowerShell UAC bypass methods are detected.
- **ATT&CK Category:** Defense Evasion, Privilege Escalation
- **ATT&CK Tag:** Abuse Elevation Control Mechanism, Bypass User Access Control
- **ATT&CK ID:** T1548
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 command IN ["*-NoP -Nonl -w Hidden -c x=((gp
↳HKCU:Software\Microsoft\Windows Update).Update)*", "*-NoP -Nonl -c x=((gp
↳HKCU:Software\Microsoft\Windows Update).Update)*"] -user IN EXCLUDED_USERS
```

2.210 LP_Enabled User Right in AD to Control User Objects

- **Trigger Condition:** Logpoint detects a scenario where if a user is assigned the *SeEnableDelegation Privilege* right in Active Directory, they will be allowed to control other Active Directory user's objects.
- **ATT&CK Category:** Privilege Escalation
- **ATT&CK Tag:** Valid Accounts
- **ATT&CK ID:** T1078
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4704 message="*SeEnableDelegationPrivilege*" -user IN[?]
↪ EXCLUDED_USERS
```

2.211 LP_PowerShell Encoded FromBase64String Detected

- **Trigger Condition:** The .NET method *FromBase64String* decodes a Base64-encoded string is detected. Base64 is a widely used encoding scheme representing binary data in an ASCII string format.
- **ATT&CK Category:** Execution, Defense Evasion
- **ATT&CK Tag:** Command and Scripting Interpreter, PowerShell, Deobfuscate/Decode Files or Information
- **ATT&CK ID:** T1059, T1059.001, T1140
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create command IN [
↪ "*OgA6AEYAcgBvAG0AQgBhAHMAZQA2ADQAUwB0AHIAaQBuAGcA*",
↪ "*oAOgBGAHIAbwBtAEIAYQBzAGUANgA0AFMAAdABYAGkAbgBnA*",
↪ "*6ADoARgByAG8AbQBCAGEAcwBIADYANABTAHQAcgBpAG4AZw*" ]
```

2.212 LP_Encoded IEX Detected

- **Trigger Condition:** The use of the "IEX" (Invoke-Expression) cmdlet to execute encoded PowerShell commands is detected. "IEX" is a built-in cmdlet in PowerShell that allows users to run scripts or commands stored in a string. Adversaries may use encoding to conceal the contents of their scripts or commands, making it more difficult for defenders to detect and analyze their activities. Adversaries may use the "IEX" cmdlet to execute encoded PowerShell commands as part of their attack. They may also use encoding to hide their activities' true nature or evade detection. False Positive: Some legitimate processes might use encoded commands.
- **ATT&CK Category:** Execution, Defense Evasion
- **ATT&CK Tag:** Command and Scripting Interpreter, PowerShell, Deobfuscate/Decode Files or Information
- **ATT&CK ID:** T1059, T1059.001, T1140
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label="process" label=create command IN ["*SUVYIChb*", "*|FWCAoW*", "*JRVggKF*",
↳ "*aWV4IChb*", "*|leCAoW*", "*pZXggKF*", "*aWV4IChOZX*", "*|leCAoTmV3*",
↳ "*pZXggKE5ld*", "*SUVYIChOZX*", "*|FWCAoTmV3*", "*JRVggKE5ld*"] -user IN [
↳ EXCLUDED_USERS]
```

2.213 LP_Encoded PowerShell Command Detected

- **Trigger Condition:** Execution of encoded Command and Scripting Interpreter and PowerShell commands are detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** PowerShell
- **ATT&CK ID:** T1059.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*\powershell.exe" command IN ["*-e *", "*-
↳ enc *", "*-ec *", "*-en *", "*-enco *"] -command="* -Encoding * -{\"parent_process
↳ \"= \"C:\\Packages\\Plugins\\Microsoft.GuestConfiguration.ConfigurationforWindows\\*\"
↳ parent_process=\"*\\gc_worker.exe\"})
```

2.214 LP_Eventlog Cleared Detected

- **Trigger Condition:** One of the Windows Event logs been cleared is detected. Adversaries can use this technique to remove the traces of intrusion.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Clear Windows Event Logs
- **ATT&CK ID:** T1070.001
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=104 event_source="Microsoft-Windows-Eventlog" -user IN EXCLUDED_USERS
```

2.215 LP_Executables Stored in OneDrive

- **Trigger Condition:** A user stores files that are executable in OneDrive.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Masquerading
- **ATT&CK ID:** T1036
- **Minimum Log Source Requirement:** Office365
- **Query:**

```
event_source=OneDrive source_file_extension IN EXECUTABLES | chart  
count() by user_id, source_address, source_file, source_file_extension,  
source_relative_url
```

2.216 LP_Execution in Non-Executable Folder Detected

- **Trigger Condition:** Process creation from an uncommon directory is detected. Adversaries may drop and execute payloads from such Windows locations to evade detection and gain persistence.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Masquerading
- **ATT&CK ID:** T1036

- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process" IN SUSPICIOUS_FOLDER_EXE_EXECUTION - "process"
↪ " = "*" \servicing\TrustedInstaller.exe "
```

2.217 LP_Execution in Outlook Temp Folder Detected

- **Trigger Condition:** Execution of a suspicious program in the Outlook's temp folder is detected.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** Phishing, Spearphishing Attachment
- **ATT&CK ID:** T1566, T1566.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process" = "*" \Temporary Internet Files\Content.Outlook\*" -
↪ user IN EXCLUDED_USERS
```

2.218 LP_Execution in Webserver Root Folder Detected

- **Trigger Condition:** A suspicious program execution in a web service root folder (filter out false positives) is detected. Attackers use this common tactic to achieve persistence in web servers by placing their malicious files in the web service root directory. False positives could be various applications and tools, including ping or nslookup command invocations.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Server Software Component, Web Shell
- **ATT&CK ID:** T1505, T1505.003
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process" IN ["*\\wwwroot\\*", "*\\wmpub\\*", "*\\htdocs\\*"] -
↪ "process" IN ["*\\bin\\*", "*\\Tools\\*", "*\\SMSComponent\\*"] parent_process="*\\services.
↪ exe" -user IN EXCLUDED_USERS
```

2.219 LP_Execution of Renamed PaExec Detected

- **Trigger Condition:** Execution of renamed paexec via imphash and executable product string is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Masquerading
- **ATT&CK ID:** T1036
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 product IN ["*PAExec*"] hash_imphash IN [
↪ "11D40A7B7876288F919AB819CC2D9802", "6444f8a34e99b8f7d9647de66aabe516",
↪ "dfd6aa3f7b2b1035b76b718f1ddc689f", "1a6cca4d5460b1710a12dea39e4a592c"] -
↪ image="*paexec*" -user IN EXCLUDED_USERS
```

2.220 LP_Execution via Control Panel Items

- **Trigger Condition:** Execution of binary via Signed Binary Proxy Execution, Control Panel items are detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Control Panel Items
- **ATT&CK ID:** T1218.002
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*\\control.exe" command="*control*"
↪ command="*cp|*" -user IN EXCLUDED_USERS
```

2.221 LP_Execution via HTA using IE JavaScript Engine Detected

- **Trigger Condition:** The execution of an HTA (HTML Application) file using the Internet Explorer JavaScript engine. HTAs are standalone applications written in HTML and can execute scripts, such as JavaScript or VBScript, on a system. Adversaries may use HTAs as a delivery mechanism for their payloads or execute arbitrary code on a system. Adversaries may use HTAs as a way to bypass security controls or to evade detection. They may also use them to execute arbitrary code on a system, potentially allowing them to access sensitive information or compromise the system.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Mshta
- **ATT&CK ID:** T1218.005
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=7 "process"="*mshta.exe" image="*jscript9.dll" -
↪user IN EXCLUDED_USERS
```

2.222 LP_Execution via Squiblydoo Technique Detected

- **Trigger Condition:** Execution of the Squiblydoo technique is detected. Squiblydoo runs payloads or scripts by leveraging the Windows Script Host (WSH) and its default file associations. Adversaries may use Squiblydoo to bypass security controls or to evade detection. Adversaries may use the Squiblydoo technique to execute arbitrary code on a system, potentially allowing them to access sensitive information or compromise the system. They may also use it to hide their activities' true nature or evade detection.
- **ATT&CK Category:** Execution, Defense Evasion
- **ATT&CK Tag:** Signed Binary Proxy Execution, Regsvr32
- **ATT&CK ID:** T1218, T1218.01
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=7 image="*scrobj.dll" -user IN
EXCLUDED_USERS
```

2.223 LP_Execution via Windows Scripting Host Component Detected

- **Trigger Condition:** This alert detects the execution of a script using the Windows Scripting Host (WSH) component on a system. WSH is a Microsoft technology that allows users to run scripts and automate tasks on Windows systems. Adversaries may use the WSH component to execute arbitrary code on a system, potentially allowing them to access sensitive information or compromise the system. They may also use it to hide their activities' true nature or evade detection.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter
- **ATT&CK ID:** T1059
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=7 image in ["*wshom.ocs", "*scrrun.dll",
"*vbscript.dll"] -user IN EXCLUDED_USERS
```

2.224 LP_Exim MTA Remote Code Execution Vulnerability Detected

- **Trigger Condition:** Remote code execution vulnerability in Exim MTA is detected. The U.S. National Security Agency (NSA) reported that Russian military cyber actors, also known as Sandworm Team, have been actively exploiting a critical vulnerability in Exim MTA since August 2019.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Network Service Scanning, Software Discovery, Security Software Discovery
- **ATT&CK ID:** T1046, T1518, T1518.001
- **Minimum Log Source Requirement:** Vulnerability Management
- **Query:**

```
norm_id=VulnerabilityManagement cve_id="CVE-2019-10149"
```

2.225 LP_Exim Remote Command Execution Detected

- **Trigger Condition:** Remote command execution in Exim is detected (CVE-2019-10149 is detected).

- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Exploitation for Client Execution
- **ATT&CK ID:** T1203
- **Minimum Log Source Requirement:** Mail Server
- **Query:**

```
norm_id=* receiver="{run"
```

2.226 LP_Existing Service Modification Detected

- **Trigger Condition:** A modification of an existing service via the sc.exe system utility is detected. Adversaries abuses the Windows Service Control Manager to execute malicious commands or payloads without creating new services.
- **ATT&CK Category:** Persistence, Privilege Escalation
- **ATT&CK Tag:** Create or Modify System Process, Windows Service
- **ATT&CK ID:** T1543, T1543.003
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Create" label="Process" "process" IN ["*sc.exe", "*powershell.exe", "*cmd.exe"]  
↪ command="*sc*" command="*config*" command="*binpath*" -user IN EXCLUDED_  
↪ USERS
```

2.227 LP_External Disk Drive or USB Storage Device Detected

- **Trigger Condition:** External disk drives or plugged in USB devices are detected.
- **ATT&CK Category:** Lateral Movement, Initial Access
- **ATT&CK Tag:** Replication Through Removable Media, Hardware Additions
- **ATT&CK ID:** T1091, T1200
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer ((event_id IN ["6416"] class="DiskDrive") OR  
message="USB Mass Storage Device") -user IN EXCLUDED_USERS
```

2.228 LP_Fail2ban IP Banned

- **Trigger Condition:** A client's IP address is banned after exceeding the limit for failed authentications.
- **ATT&CK Category:** Credential Access, Persistence
- **ATT&CK Tag:** Brute Force, Valid Accounts, Account Manipulation
- **ATT&CK ID:** T1110, T1078, T1098
- **Minimum Log Source Requirement:** Fail2ban
- **Query:**

```
norm_id=Fail2ban label=IP label=Block | process geoip(source_address) as country
```

2.229 LP_File Creation by PowerShell Detected

- **Trigger Condition:** The creation of a new file using PowerShell on a system. PowerShell is a powerful scripting language that is built into Windows and can be used to automate a wide variety of tasks. Adversaries may use PowerShell to create new files, drop and execute malicious payloads or store data for later retrieval. False positive Notice: Administrative tasks and genuine processes might cause the alert to trigger as well. Proper analysis and whitelisting are recommended.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** PowerShell
- **ATT&CK ID:** T1059.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=11 file=* "process"="*powershell.exe" -file IN ["__
↪ PSScriptPolicyTest_*. ", "PowerShell_transcript.*", "powershell.exe.log",
↪ "StartupProfileData*", "ModuleAnalysisCache"] -user IN EXCLUDED_USERS -file IN ["*.
↪ mui"]
```

2.230 LP_File Deletion Detected

- **Trigger Condition:** Adversaries delete files to erase the traces of the intrusion.
- **ATT&CK Category:** Defense Evasion

- **ATT&CK Tag:** Indicator Removal on Host, File Deletion
- **ATT&CK ID:** T1070, T1070.004
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon      event_id=1      (command="remove-item"
or      command="vssadmin*Delete      Shadows      /All      /Q"      or
command="wmic*shadowcopy delete"      or command="wbdadmin delete
catalog -q*"      or command="bcdedit*bootstatuspolicy ignoreallfailures"      or
command="bcdedit*recoveryenabled no") -user IN EXCLUDED_USERS
```

2.231 LP_File or Folder Permissions Modifications

- **Trigger Condition:** Modifications to file or folder permissions are detected. Permissions control access to files and directories and determine which users and processes can read, write, or execute them. Adversaries may attempt to modify these permissions to gain unauthorized access to sensitive files or to execute arbitrary code on a system. They can also use these modifications to escalate system privileges or move laterally within an organization's network.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Windows File and Directory Permissions Modification
- **ATT&CK ID:** T1222.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process"      label=Create      (("process"      IN      ["cacls.exe",
"icacls.exe",      "net.exe",      "net1.exe"]      command      IN      ["/grant",
"/setowner",      "/inheritance:r"])      OR      ("process"      =      "attrib.exe"
command="-r*")      OR      "process"="takeown.exe")      -(command="*ICACLS
C:ProgramDatadynatracegatewayconfigconnectivity.history /reset"      OR
(command="*ICACLS C:ProgramDatadynatracegatewayconfigconfig.properties
/grant :r *"      command="*S-1-5-19:F")      OR      (command="AppDataLocalProgramsMicrosoft
VS Code"      OR      parent_process="*Microsoft VS CodeCode.exe")) -user IN
EXCLUDED_USERS
```

2.232 LP_File System Permissions Weakness

- **Trigger Condition:** A weakness in the file system permissions on a system is detected. File system permissions control access to files and directories and determine which users and processes can read, write, or execute

them. Adversaries may exploit weaknesses in file system permissions to gain unauthorized access to sensitive files or execute arbitrary code on a system.

- **ATT&CK Category:** Persistence, Privilege Escalation, Defense Evasion
- **ATT&CK Tag:** Hijack Execution Flow, Services File Permissions Weakness
- **ATT&CK ID:** T1574,T1574.010
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon      event_id=7      (image="Temp*"      or
image="*C:Users*" or status!="*Valid") -user IN EXCLUDED_USERS
```

2.233 LP_Firewall Configuration Modification Detected

- **Trigger Condition:** When there is a change or modification to the Windows firewall configuration on a system. This could indicate malicious activity, as an adversary may be attempting to disable or bypass the firewall to gain unauthorized access to the system or network. False Positive Notice: Legitimate system maintenance or system administration tasks may involve the modification of firewall configurations, and these could potentially trigger the alert. It is essential to carefully review and investigate any instances of this alert before taking action to ensure that the activity detected is genuinely malicious.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Non-Standard Port
- **ATT&CK ID:** T1571
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4946 rule=* -user IN EXCLUDED_USERS
```

2.234 LP_Firewall Disabled via Netsh Detected

- **Trigger Condition:** *netsh* command turns off the Windows firewall is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Disable or Modify System Firewall
- **ATT&CK ID:** T1562.004
- **Minimum Log Source Requirement:** Windows Sysmon, Windows

- **Query:**

```
label="process" label=Create "process"="*\netsh.exe" command="*set*" command=
↪ "*firewall*"((command="*opmode*" command="*disable*") OR (command="*state*"
↪ command="*off*"))
```

2.235 LP_First Time Seen Remote Named Pipe

- **Trigger Condition:** The alert rule excludes the named pipes accessible remotely and notifies on new cases. Also, it helps to detect lateral movement and remote execution using named pipes.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Remote Services
- **ATT&CK ID:** T1021
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=5145 share_name="IPC$" -relative_target
IN ["atsvc", "samr", "lsarpc", "winreg", "netlogon", "srvsvc",
"protected_storage", "wkssvc", "browser", "netdfs", "svcctl", "spoolss",
"ntsvcs", "LSM_API_service", "HydraLsPipe", "TermSrv_API_service",
"MsFteWds"] -user IN EXCLUDED_USERS
```

2.236 LP_FirstClass Failed Login Attempt

- **Trigger Condition:** A user or a gateway attempts to log in with an incorrect password.
- **ATT&CK Category:** Defense Evasion, Persistence, Privilege Escalation, Initial Access
- **ATT&CK Tag:** Exploitation for Credential Access, Exploitation for Privilege Escalation, Brute Force
- **ATT&CK ID:** T1212, T1068, T1110
- **Minimum Log Source Requirement:** Firstclass
- **Query:**

```
norm_id=FirstClass label=Login label=Fail
```

2.237 LP_FirstClass Failed Password Change Attempt

- **Trigger Condition:** A user fails to change their password.
- **ATT&CK Category:** Credential Access, Persistence
- **ATT&CK Tag:** Account Manipulation, Exploitation for Credential Access, Exploitation for Privilege Escalation
- **ATT&CK ID:** T1098, T1212, T1068
- **Minimum Log Source Requirement:** Firstclass
- **Query:**

norm_id=FirstClass label=Password label=Change label=Fail

2.238 LP_Formbook Process Creation Detected

- **Trigger Condition:** Formbook like process executions injecting code into a set of files in the System32 folder, which executes a unique command line to delete the dropper from the AppData Temp folder is detected.
- **ATT&CK Category:** Resource Development
- **ATT&CK Tag:** Malware
- **ATT&CK ID:** T1587.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create parent_process IN ["*:\Windows\System32*.exe",
↪ "*:\Windows\SysWOW64*.exe"] (command="*c*" command="*\Users\*" ((command=
↪ "*del*" command in ["*\AppData\Local\Temp*", "*\Desktop*"]) OR (command=
↪ "*type nul >*" command="*\Desktop*")))) command="*.exe"
```

2.239 LP_FortiGate Admin Login Disable

- **Trigger Condition:** The administrator login is disabled in the system.
- **ATT&CK Category:** Impact, Credential Access, Persistence
- **ATT&CK Tag:** Account Access Removal, Account Manipulation
- **ATT&CK ID:** T1531, T1098
- **Minimum Log Source Requirement:** Fortigate

- **Query:**

```
norm_id=Forti*      event_category=event      sub_category=system
message_id=32021 user=*
```

2.240 LP_FortiGate Anomaly

- **Trigger Condition:** An anomaly in the system is detected.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Network Service Scanning
- **ATT&CK ID:** T1046
- **Minimum Log Source Requirement:** Fortigate
- **Query:**

```
norm_id=Forti*      event_category=anomaly      sub_category=anomaly
log_level=alert attack=* | process geoip(source_address) as source_country |
process geoip(destination_address) as destination_country
```

2.241 LP_FortiGate Antivirus Botnet Warning

- **Trigger Condition:** A botnet warning from antivirus is detected.
- **ATT&CK Category:** Command and Control, Impact
- **ATT&CK Tag:** Proxy, Network Denial of Service
- **ATT&CK ID:** T1090, T1498
- **Minimum Log Source Requirement:** Fortigate
- **Query:**

```
norm_id=Forti*      (event_category=av      OR      event_category=antivirus)
sub_category=botnet message_id=9248 | process geoip(source_address) as
source_country | process geoip(destination_address) as destination_country
```

2.242 LP_FortiGate Antivirus Scan Engine Load Failed

- **Trigger Condition:** *Antivirus Scan Engine Load Failure* is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Impair Defenses, Impair Defenses, Disable or Modify Tools
- **ATT&CK ID:** T1562, T1562.001
- **Minimum Log Source Requirement:** Fortigate

- **Query:**

```
norm_id=Forti*          event_category=av          sub_category=scanerror
message_id=8974 | process geoip(source_address) as source_location |
process geoip(destination_address) as destination_location
```

2.243 LP_FortiGate Attack

- **Trigger Condition:** An attack in the system is detected.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Network Denial of Service
- **ATT&CK ID:** T1498
- **Minimum Log Source Requirement:** Fortigate
- **Query:**

```
norm_id=Forti* attack=* | process geoip(source_address) as source_country |
process geoip(destination_address) as destination_country
```

2.244 LP_FortiGate Critical Events

- **Trigger Condition:** Critical events in the system are detected.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Network Service Scanning
- **ATT&CK ID:** T1046
- **Minimum Log Source Requirement:** Fortigate
- **Query:**

```
norm_id=Forti*          event_category=event          sub_category=system
log_level=critical
```

2.245 LP_FortiGate Data Leak Protection

- **Trigger Condition:** An attempt to data leak is detected.
- **ATT&CK Category:** Exfiltration
- **ATT&CK Tag:** Automated Exfiltration
- **ATT&CK ID:** T1020
- **Minimum Log Source Requirement:** Fortigate

- **Query:**

```
norm_id=Forti* event_category=utm sub_category=dlp file=* | process
geoip(source_address) as source_country | process geoip(destination_address)
as destination_country
```

2.246 LP_FortiGate IPS Events

- **Trigger Condition:** An intrusion attempt is detected in the system.
- **ATT&CK Category:** Discovery, Defense Evasion
- **ATT&CK Tag:** Network Service Scanning, Exploitation for Defense Evasion
- **ATT&CK ID:** T1046, T1211
- **Minimum Log Source Requirement:** Fortigate
- **Query:**

```
norm_id=Forti* event_category=utm sub_category=ips user=* | process
geoip(source_address) as source_country | process geoip(destination_address)
as destination_country
```

2.247 LP_FortiGate Malicious URL Attack

- **Trigger Condition:** A malicious attack in a system is detected. This alert rule is valid only for FortiOS V6.0.4.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** Phishing, Spearphishing Link
- **ATT&CK ID:** T1566, T1566.002
- **Minimum Log Source Requirement:** Fortigate
- **Query:**

```
norm_id=Forti* event_category=ips sub_category="malicious-url"
message_id=16399 | process geoip(source_address) as source_country |
process geoip(destination_address) as destination_country
```

2.248 LP_FortiGate Virus

- **Trigger Condition:** A virus attack is detected.
- **ATT&CK Category:** Discovery, Defense Evasion
- **ATT&CK Tag:** Network Service Scanning, Exploitation for Defense Evasion
- **ATT&CK ID:** T1046, T1211

- **Minimum Log Source Requirement:** Fortigate
- **Query:**

```
norm_id=Forti* event_category=utm sub_category=virus | process
geop(source_address) as source_country | process geop(destination_address)
as destination_country
```

2.249 LP_FortiGate VPN SSL User Login Failed

- **Trigger Condition:** A VPN SSL login failure is detected.
- **ATT&CK Category:** Initial Access, Credential Access
- **ATT&CK Tag:** Valid Accounts, Brute Force
- **ATT&CK ID:** T1078, T1110
- **Minimum Log Source Requirement:** Fortigate
- **Query:**

```
norm_id=Forti* event_category=event sub_category=vpn
message_id=39426 user=*
```

2.250 LP_FromBase64String Command Line Detected

- **Trigger Condition:** When the *FromBase64String* command used in a command line interface on a system is detected. This command decodes a string that was encoded using base64 encoding.
- **ATT&CK Category:** Defense Evasion, Execution
- **ATT&CK Tag:** PowerShell, Obfuscated Files or Information, Deobfuscate/Decode Files or Information
- **ATT&CK ID:** T1059.001, T1027, T1140
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create command="*FromBase64String*" -user IN EXCLUDED_
↳ USERS
```

2.251 LP_FSecure File Infection

- **Trigger Condition:** An infected file is detected.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Network Service Scanning, File and Directory Discovery
- **ATT&CK ID:** T1046, T1083
- **Minimum Log Source Requirement:** Fsecure Gatekeeper
- **Query:**

norm_id=FSecureGatekeeper label=Infection label=File label=Attack

2.252 LP_FSecure Virus Detection

- **Trigger Condition:** Virus alert is detected while scanning.
- **ATT&CK Category:** Discovery, Defense Evasion
- **ATT&CK Tag:** Network Service Scanning, Exploitation for Defense Evasion
- **ATT&CK ID:** T1046, T1211
- **Minimum Log Source Requirement:** Fsecure
- **Query:**

norm_id=FSecure* label=Detect label=Malware malware=*

2.253 LP_Fsutil Suspicious Invocation Detected

- **Trigger Condition:** Execution of Fsutil with *Createjournal* or *Deletejournal* command line argument is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Indicator Removal
- **ATT&CK ID:** T1070
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create ("process"="*\fsutil.exe" OR file="fsutil.exe") command IN [
  ↳ "*deletejournal*", "*createjournal*"] -user IN EXCLUDED_USERS
```

2.254 LP_GAC DLL Loaded Via Office Applications Detected

- **Trigger Condition:** GAC DLL loaded by an Office Product is detected.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** Phishing, Spearphishing Attachment
- **ATT&CK ID:** T1566, T1566.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=7 "process" IN ["*\winword.exe*", ".*\powerpnt.exe*
↪", ".*\excel.exe*", ".*\outlook.exe*"] image IN ["*C:\Windows\Microsoft.
↪NET\assembly\GAC_MSIL*"] -user IN EXCLUDED_USERS
```

2.255 LP_Generic Password Dumper Activity on LSASS Detected

- **Trigger Condition:** Process handle on LSASS process with access mask is detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer (event_id=4656 OR event_id="4663")
object_name="lsass.exe" access_mask IN ["*0x40", "0x1400", "0x1000",
"0x100000", "0x1410", "0x1010", "0x1438", "0x143a", "0x1418", "0x1f0fff",
"0x1f1fff", "0x1f2fff", "0x1f3fff"] -user IN EXCLUDED_USERS
```

2.256 LP_Grabbing Sensitive Hives via Reg Utility

- **Trigger Condition:** Grabbing of Sensitive Hives via Reg Utility is detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** LSA Secrets, Cached Domain Credentials, Credentials in Registry

- **ATT&CK ID:** T1003.004, T1003.005, T1552.002
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*\reg.exe" command IN ["*save*", "*export*"]
↪ command IN ["*hklm*", "*hkey_local_machine*"] command IN ["*\system", "*\sam",
↪ "*\security"] -user IN EXCLUDED_USERS
```

2.257 LP_Hacktool Ruler Detected

- **Trigger Condition:** Sensepost uses a Hacktool ruler.
- **ATT&CK Category:** Discovery, Execution
- **ATT&CK Tag:** Account Discovery, Use Alternate Authentication Material, Pass the Hash, Email Collection, Command-Line Interface + **ATT&CK ID:** T1087, T1550, T1550.002, T1114, T1059
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id IN ["4776", "4624", "4625"]
workstation="RULER" -user IN EXCLUDED_USERS
```

2.258 LP_HH Execution Detected

- **Trigger Condition:** The *hh.exe* process running on a system is detected. *HH.exe* is a legitimate process associated with the Windows HTML Help feature and is used to display compiled help files (.chm) on a system. While the execution of *hh.exe* in itself is not necessarily malicious, an adversary may use this process as part of a more significant attack. For example, they may embed malicious code in a compiled help file and use *hh.exe* to execute it on a target system. False Positive Note: Legitimate applications or system processes may use *hh.exe* to display help files, which could trigger the alert. It is essential to carefully review and investigate any instances of this alert before taking action to ensure that the detected activity is genuinely malicious.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Compiled HTML File
- **ATT&CK ID:** T1218.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows

- **Query:**

```
label="Process" label=Create ("process"="hh.exe" OR file="hh.exe")
command IN [".chm*", "http", ".application", "AppDataLocal*",
"Content.Outlook*", "Downloads*", "UsersPublic*", "*Temp*"] -user IN
EXCLUDED_USERS
```

2.259 LP_Hidden Files and Directories Detected

- **Trigger Condition:** When the presence of hidden files and directories on a system is detected. Adversaries may use hidden files and directories to conceal malicious files or activities from the victim. They may also use these files to store command and control information or to persist on a system after an initial compromise. By hiding their files and directories, adversaries can make it more difficult for defenders to detect and respond to their activities.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Hide Artifacts, Hidden Files and Directories
- **ATT&CK ID:** T1564, T1564.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*attrib.exe" command IN ["*+h*", "*+s*"] -
↪ user IN EXCLUDED_USERS
```

2.260 LP_Hiding Files with Attrib Detected

- **Trigger Condition:** The use of *attrib.exe* to hide files from users is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Hide Artifacts, Hidden Files and Directories
- **ATT&CK ID:** T1564, T1564.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label=Create label="Process" "process"="*\attrib.exe" command = "*+h*" - (command
↪ = "*\desktop.ini*" OR (parent_process = "*\cmd.exe" command = "*+R +H +S +A \*.
↪ cui*" parent_command = "*C:\WINDOWS\system32\*.bat*"))
```

2.261 LP_IIS Native-Code Module Command Line Installation

- **Trigger Condition:** Logpoint detects suspicious IIS native-code module installations via the command line.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Server Software Component, Web Shell
- **ATT&CK ID:** T1505, T1505.003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 command IN ["*\APPCMD.EXE install module /
↪name:*"] -user IN EXCLUDED_USERS
```

2.262 LP_In-memory PowerShell Detected

- **Trigger Condition:** Loading of *System.Management.Automation.dll* by other processes than PowerShell is detected. Adversaries can use this technique to evade defenses by loading the DLL and executing Powershell commands without the need of executing *powershell.exe* binary.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, PowerShell
- **ATT&CK ID:** T1059, T1059.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label=Image label=load image IN ["*\System.Management.Automation.Dll", ".*\System.
↪Management.Automation.ni.Dll"] -"process" IN [ ".*\Altaro.SubAgent.exe", ".*\AppV_
↪Manage.exe", ".*\azureadconnect.exe", ".*\CcmExec.exe", ".*\configsyncrun.exe",
↪ ".*\choco.exe", ".*\ctxappvservice.exe", ".*\DVLS.Console.exe", ".*\edgetransport.exe",
↪ ".*\exsetup.exe", ".*\forefrontactivedirectoryconnector.exe", ".*\InstallUtil.exe",
↪ ".*\JenkinsOnDesktop.exe", ".*\Microsoft.EnterpriseManagement.ServiceManager.UI.
↪Console.exe", ".*\mmc.exe", ".*\mscorsvw.exe", ".*\msexchangedelivery.exe",
↪ ".*\msexchangefrontendtransport.exe", ".*\msexchangehmworker.exe",
↪ ".*\msexchangesubmission.exe", ".*\msiexec.exe", ".*\MsiExec.exe", ".*\noderunner.exe",
↪ ".*\NServiceBus.Host.exe", ".*\NServiceBus.Host32.exe", ".*\NServiceBus.Hosting.Azure.
↪HostProcess.exe", ".*\OuiGui.WPF.exe", ".*\powershell.exe", ".*\powershell_ise.exe",
↪ ".*\pwsh.exe", ".*\SCCMcliCtrWPF.exe", ".*\ScriptEditor.exe", ".*\ScriptRunner.exe",
↪ ".*\sdiaghost.exe", ".*\servermanager.exe", ".*\setup100.exe", ".*\ServiceHub.
↪VSDetectedHost.exe", ".*\SPCAFRClient.exe", ".*\SPCAF.SettingsEditor.exe", ".*\SQLPS.
↪exe", ".*\telemetryservice.exe", ".*\UMWorkerProcess.exe", ".*\w3wp.exe",
↪ ".*\wsmprovhost.exe", ".*\dsac.exe", ".*\RemoteFXvGPUDisablement.exe",
↪ ".*\runscripthelper.exe", ".*\SyncAppvPublishingServer.exe", ".*\winrshost.exe"
```

(continues on next page)

(continued from previous page)

2.263 LP_Indicator Blocking - Driver Unloaded

- **Trigger Condition:** Adversaries blocks indicators or events captured by sensors from being gathered and analyzed.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Impair Defenses, Indicator Blocking
- **ATT&CK ID:** T1562, T1562.006
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 (image="*fltmc.exe" or command="*fltmc*unload*  
↪") -user IN EXCLUDED_USERS
```

2.264 LP_Indicator Blocking - Sysmon Registry Edited

- **Trigger Condition:** An indicator blocking via registry editing is detected. Adversaries might block indicators or events typically captured by sensors from being gathered and analyzed to evade detection.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Impair Defenses, Indicator Blocking
- **ATT&CK ID:** T1562, T1562.006
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id IN [12,13,14] target_object in [  
↪ "*HKLM\System\CurrentControlSet\Services\SysmonDrv*",  
↪ "*HKLM\System\CurrentControlSet\Services\Sysmon*",  
↪ "*HKLM\System\CurrentControlSet\Services\Sysmon64*" ] - "process" IN ["*\Sysmon64.  
↪ exe", "*\Sysmon.exe"] -event_type=INFO -user IN EXCLUDED_USERS
```

2.265 LP_Install Root Certificate

- **Trigger Condition:** Undermine security controls by adversaries that warn users of untrusted activity or prevent the execution of untrusted programs detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Subvert Trust Controls, Install Root Certificate
- **ATT&CK ID:** T1553, T1553.004
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id IN ["12", "13", "14"] "process"!="*svchost.exe"
↪target_object IN ["*\SOFTWARE\Microsoft\EnterpriseCertificates\Root\Certificates\*",
↪"*\Microsoft\SystemCertificates\Root\Certificates\*"] -user IN EXCLUDED_USERS
```

2.266 LP_Suspicious InstallUtil Execution

- **Trigger Condition:** Use of *InstallUtil* for proxy execution of code through a trusted Windows utility is detected. *InstallUtil* is a command-line utility that allows installation and uninstallation of resources by executing specific installer components specified in .NET binaries. Typically, adversaries utilize the most commonly found way to invoke via the InstallUtil Uninstall method.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Signed Binary Proxy Execution, InstallUtil
- **ATT&CK ID:** T1218, T1218.004
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create ( "process"="*Microsoft.NET\Framework*" "process"=
↪"*\InstallUtil.exe" command="* /logfile=*" command="*/LogToConsole=false*")
```

2.267 LP_Invocation of Active Directory Diagnostic Tool Detected

- **Trigger Condition:** Execution of `ntdsutil.exe` used for various attacks against the OS Credential Dumping, NTDS database (OS Credential Dumping, NTDS.DIT) is detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** OS Credential Dumping, NTDS
- **ATT&CK ID:** T1003, T1003.003
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
'label="Process" label=Create "process"="*\ntdsutil.exe" -user IN EXCLUDED_USERS'
```

2.268 LP_Java Running with Remote Debugging

- **Trigger Condition:** A JAVA process running with remote debugging allowing more than just localhost to connect, is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Exploitation for Client Execution
- **ATT&CK ID:** T1203
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label=create label="process" command="*transport=dt_socket,address=*" command IN [
↪ "*jre1.*", "*jdk1.*"] -command IN ["*address=127.0.0.*", "*address=localhost*"]
```

2.269 LP_Judgement Panda Exfil Activity

- **Trigger Condition:** Russian group activity as described in Global Threat Report 2019 by CrowdStrike is detected.
- **ATT&CK Category:** Credential Access

- **ATT&CK Tag:** OS Credential Dumping, Unsecured Credentials, Credentials In Files
- **ATT&CK ID:** T1552, T1552.001, T1003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 ((image="*\xcopy.exe" command="* /S /E /C /Q /
↪ H *") OR (image="*\adexplorer.exe" command="* -snapshot * c:\users\*")) -user IN
↪ EXCLUDED_USERS
```

2.270 LP_JunOS Attack

- **Trigger Condition:** Logpoint detects an attack pattern.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Network Denial of Service, Endpoint Denial of Service
- **ATT&CK ID:** T1498, T1499
- **Minimum Log Source Requirement:** JunOS
- **Query:**

```
norm_id=JunOS (label=Application OR label=appddos OR threat=*dos*) label=Attack
↪ (label=Warning OR label=Successful)
```

2.271 LP_JunOS Authentication Failed

- **Trigger Condition:** Failure of an authentication.
- **ATT&CK Category:** Defense Evasion, Persistence, Privilege Escalation, Initial Access
- **ATT&CK Tag:** Valid Accounts, Brute Force
- **ATT&CK ID:** T1078, T1110
- **Minimum Log Source Requirement:** JunOS
- **Query:**

```
norm_id=JunOS label=User (label=Authentication OR Login) label=Fail
```

2.272 LP_JunOS Policy Violation

- **Trigger Condition:** A policy violation is detected.
- **ATT&CK Category:** Defense Evasion, Privilege Escalation, Credential Access
- **ATT&CK Tag:** Bypass User Access Control, Exploitation for Credential Access, Exploitation for Privilege Escalation
- **ATT&CK ID:** T1548, T1212, T1068
- **Minimum Log Source Requirement:** JunOS
- **Query:**

```
norm_id=JunOS label=Policy (label=Violation OR label=Error)
```

2.273 LP_JunOS Security Log Clear

- **Trigger Condition:** An administrator has cleared one or more audit logs.
- **ATT&CK Category:** Defense Evasion, Impact
- **ATT&CK Tag:** Indicator Removal on Host, Data Destruction, Indicator Removal on Host, File Deletion
- **ATT&CK ID:** T1070, T1485, T1070, T1070.004
- **Minimum Log Source Requirement:** JunOS
- **Query:**

```
norm_id=JunOS label=Log label=Clear
```

2.274 LP_Kaspersky Antivirus - Outbreak Detection

- **Trigger Condition:** This alert rule is triggered whenever a threat is detected.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Software Discovery, Security Software Discovery

- **ATT&CK ID:** T1518, T1518.001
- **Minimum Log Source Requirement:** Kaspersky
- **Query:**

```
norm_id=KasperskyAntivirus event_type="*threat*detected" | rename wstrPar5 as virus |  
↪ chart distinct_count(win_name) as CNT by virus, event_type
```

2.275 LP_Kaspersky Antivirus - Update Fail

- **Trigger Condition:** Automatic updates are disabled, not all the components are updated, or there is a network error.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Impair Defenses, Impair Defenses, Disable or Modify Tools
- **ATT&CK ID:** T1562, T1562.001
- **Minimum Log Source Requirement:** Kaspersky
- **Query:**

```
norm_id=KasperskyAntivirus (event_type="Automatic updates are disabled" OR event_  
↪ type="Not all components were updated" OR event_type="Network update error" OR  
↪ event_type="Error updating component"  
OR description="Error downloading update files" OR description="Update files are  
↪ corrupted") | rename event_type as reason, description as reason
```

2.276 LP_Kaspersky Antivirus Extremely Out of Date Event

- **Trigger Condition:** Outdated events are detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Impair Defenses, Indicator Blocking
- **ATT&CK ID:** T1562, T1562.006
- **Minimum Log Source Requirement:** Kaspersky
- **Query:**

```
norm_id=KasperskyAntivirus event_type="*extremely out of date*"
```

2.277 LP_Kaspersky Antivirus Outbreak Detection by Source

- **Trigger Condition:** More than one source is affected by the same virus.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Software Discovery, Security Software Discovery
- **ATT&CK ID:** T1518, T1518.001
- **Minimum Log Source Requirement:** Kaspersky
- **Query:**

```
norm_id=KasperskyAntivirus "event_type"="Threats have been detected" | chart distinct_
↪count(win_name) as DC | search DC>1
```

2.278 LP_Kaspersky Antivirus Outbreak Detection by Virus

- **Trigger Condition:** More than ten viruses are detected in the system.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Software Discovery, Security Software Discovery
- **ATT&CK ID:** T1518, T1518.001
- **Minimum Log Source Requirement:** Kaspersky
- **Query:**

```
norm_id=KasperskyAntivirus "event_type"="Threats have been detected" | chart distinct_
↪count(wstrPar5) as DC | search DC>10
```

2.279 LP_Kaspersky Antivirus Threat Affecting Multiple Host

- **Trigger Condition:** The same threat is detected in multiple hosts.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Impair Defenses, Indicator Blocking
- **ATT&CK ID:** T1562, T1562.006
- **Minimum Log Source Requirement:** Kaspersky
- **Query:**

```
norm_id=KasperskyAntivirus event_type="*threat*detected" | chart distinct_count(win_
↪ name) as HostCount by event_type | process quantile(HostCount) | chart count() by
↪ event_type, quantile, HostCount
```

2.280 LP_Kerberoasting via PowerShell Detected

- **Trigger Condition:** Steal or forge Kerberos tickets, Kerberoasting via Command and Scripting Interpreter, and PowerShell is detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Steal or Forge Kerberos Tickets, Kerberoasting
- **ATT&CK ID:** T1558, T1558.003
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4103 (command_name="Invoke-Kerberoast" OR command=
↪ "Invoke-Kerberoast") -user IN EXCLUDED_USERS | rename command_name as
↪ command
```

2.281 LP_Kernel Firewall Connection Denied

- **Trigger Condition:** Ten firewall connections are denied from the same source to the same destination in a minute.
- **ATT&CK Category:** Impact, Command and Control

- **ATT&CK Tag:** Network Denial of Service, Endpoint Denial of Service, Proxy
- **ATT&CK ID:** T1498, T1499, T1090
- **Minimum Log Source Requirement:** Kernel
- **Query:**

```
[10 norm_id=Kernel label=Firewall label=Connection label=Deny having same source_
↪address, destination_address within 1 minute]
```

2.282 LP_Koadic Execution Detected

- **Trigger Condition:** The use of command line parameters associated with the Koadic hack tool during process creation events in Windows systems is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** - Windows Command Shell, Visual Basic, JavaScript
- **ATT&CK ID:** T1059.003, T1059.005, T1059.007
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*\cmd.exe" command="*/q*/c*chcp*" -user?
↪IN EXCLUDED_USERS
```

2.283 LP_Large ICMP Traffic

- **Trigger Condition:** ICMP datagrams with a size greater than 1024 bytes are received.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Network Service Scanning
- **ATT&CK ID:** T1046
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

```
((label=Receive label=Packet) or label=Illegal label=Receive label=Packet) (packet_length>
↪ 1024 or fragment_length>1024)
```

2.284 LP_Local Account Creation on Workstation Detected

- **Trigger Condition:** Creation of a local account on a domain workstation that is not Windows Domain Controller (DC).
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Create Account
- **ATT&CK ID:** T1136
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer label=User label=Account label=Create -target_user="*$" target_
↪ user=* -host in WINDOWS_DC -user IN EXCLUDED_USERS
```

2.285 LP_LockCrypt Ransomware

- **Trigger Condition:** LockCrypt ransomware encrypts a file.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Disk Wipe, Disk Content Wipe, Data Encrypted for Impact, Data Destruction
- **ATT&CK ID:** T1561, T1561.001, T1486, T1485
- **Minimum Log Source Requirement:** Integrity Scanner
- **Query:**

```
norm_id=IntegrityScanner label = File label="Rename" new_file=*.lock | norm on new_
↪ file <path:.*><:'\''><EncryptedFileName:.*> | norm on file_path <:.*><:'\''>
↪ <OriginalFileName:.*> | rename hostname as host | chart count() by log_ts, host, path,
↪ OriginalFileName, EncryptedFileName order by count() desc limit 10
```

2.286 LP_Log Files Creation of Dot-Net-to-JS Detected

- **Trigger Condition:** Creation of log files of Dot-Net-to-JavaScript.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter
- **ATT&CK ID:** T1059
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=11 path="*UsageLogs*" file in ["*cscript.exe.log",
↪ "*wscript.exe.log", "*wmic.exe.log", "*mshta.exe.log", "*svchost.exe.log", "*regsvr32.
↪ exe.log", "*rundll32.exe.log"] -user IN EXCLUDED_USERS
```

2.287 LP_LSASS Access from Non System Account Detected

- **Trigger Condition:** Potential mimikatz-like tools accessing LSASS from non system account is detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** OS Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id IN ["4663", "4656"] object_type="Process" object_name=
↪ "*\\lsass.exe" -user="*$" -user IN EXCLUDED_USERS
```

2.288 LP_LSASS Memory Dump Detected

- **Trigger Condition:** Process access to lsass.exe with access rights 0x1ffff is detected.
- **ATT&CK Category:** Credential Access

- **ATT&CK Tag:** LSASS Memory
- **ATT&CK ID:** T1003.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=10 "image"="C:\windows\system32\lsass.exe"
↪ access="0x1ffff" call_trace IN ["*dbghelp.dll*", "*dbgcore.dll*"] -user IN EXCLUDED_
↪ USERS
```

2.289 LP_LSASS Memory Dump File Creation

- **Trigger Condition:** LSASS memory dump creation using operating systems utilities is detected. *Procdump* uses process name in the output file if no name is specified.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=11 file="*lsass*dmp" -user IN EXCLUDED_USERS
```

2.290 LP_LSSAS Memory Dump with MiniDumpWriteDump API Detected

- **Trigger Condition:** The use of *MiniDumpWrite Dump* API for dumping *lsass.exe* memory in a stealth way is detected. Tools like *ProcessHacker* and some attacker *tradecraft* use this API found in *dbghelp.dll* or *dbgcore.dll*. For example, *SilentTrynity C2 Framework* has a module that leverages this API to dump the contents of *Lsass.exe* and transfer it over the network back to the attacker's machine.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** OS Credential Dumping
- **ATT&CK ID:** T1003

- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
(norm_id=WindowsSysmon event_id=7 image IN ["*\dbgghelp.dll", "*\dbgcore.dll"]
↪ "process" IN ["*\msbuild.exe", "*\cmd.exe", "*\svchost.exe", "*\rundll32.exe",
↪ "*\powershell.exe", "*\word.exe", "*\excel.exe", "*\powerpnt.exe", "*\outlook.exe",
↪ "*\monitoringhost.exe", "*\wmic.exe", "*\msiexec.exe", "*\bash.exe", "*\wscript.exe",
↪ "*\cscript.exe", "*\mshta.exe", "*\regsvr32.exe", "*\schtasks.exe", "*\dnx.exe",
↪ "*\regsvcs.exe", "*\sc.exe", "*\scriptrunner.exe"] - "process" = "*Visual Studio*") OR
↪ (event_id=7 image IN ["*\dbgghelp.dll", "*\dbgcore.dll"] Signed="FALSE" - "process" =
↪ "*Visual Studio*") -user IN EXCLUDED_USERS
```

2.291 LP_Macro file Creation Detected

- **Trigger Condition:** Creation of a macro file is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, Visual Basic
- **ATT&CK ID:** T1059, T1059.005
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=11 file in ["*.docm", "*.pptm", "*.xlsm", "*.xlm", "*.
↪ dotm", "*.xltm", "*.potm", "*.ppsm", "*.sldm", "*.xlam", "*.xla"]
```

2.292 LP_Malicious Base64 Encoded PowerShell Keywords in Command Lines Detected

- **Trigger Condition:** When base64 encoded strings are used in hidden malicious Command and Scripting Interpreter, PowerShell command lines. Adversaries hides their activities by encoding commands to bypass detection with this technique.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, PowerShell
- **ATT&CK ID:** T1059, T1059.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows

- **Query:**

```
norm_id=WindowsSysmon event_id=1 image="*\powershell.exe" command IN [
  ↳ hidden *, "*AGkAdABzAGEAZABtAGkAbgAgAC8AdABYAGEAbgBzAGYAZQByA*",
  ↳ "*aXRzYWRtaW4gL3RyYW5zMVY*",
  ↳ "*IAaQB0AHMAYQBkAG0AaQBuACAALwB0AHIAyQBuAHMAZgBIAHIA*",
  ↳ "*JpdHnHZG1pbiAvdHJhbnNmZX*",
  ↳ "*YgBpAHQAcwBhAGQAbQBpAG4AIAAvAHQAcgBhAG4AcwBmAGUAcg*",
  ↳ "*Yml0c2FkbWluc90cmFuc2Zlc*",
  ↳ "*AGMAaAB1AG4AawBfAHMAaQB6AGUA*", "*JABjAGgAdQBuAGsAXwBzAGkAegBIA*",
  ↳ ", "*JGNodW5rX3Npem*", "*QAYwBoAHUAbgBrAF8AcwBpAHoAZQ*",
  ↳ "*RjaHVua19zaXpl*", "*Y2h1bmtfc2l6Z*",
  ↳ "*AE8ALgBDAG8AbQBwAHIAZQBzAHMAaQBvAG4A*",
  ↳ "*kATwAuAEMAbwBtAHAACgBIAHMAcwbPAG8Abg*", "*IPLkNvbXByZXNzaW9u*",
  ↳ "*SQBPAC4AQwBvAG0AcABYAGUAcwBzAGkAbwBuA*", "*SU8uQ29tcHJlc3Npb2*",
  ↳ "*Ty5Db21wcmVzc2lvb*", "*AE8ALgBNAGUAbQBvAHIAeQBTAHQAcgBIAGEAbQ*",
  ↳ "*kATwAuAE0AZQBtAG8AcgB5AFMAAdABYAGUAYQBtA*",
  ↳ "*IPLk1lbW9yeVN0cmVhb*", "*SQBPAC4ATQBIAg0AbwByAHkAUwB0AHIAZQBhAG0A*",
  ↳ ", "*SU8uTWVtb3J5U3RyZWZt*", "*Ty5NZW1vcnltDhJlYW*",
  ↳ "*4ARwBIAHQAcwBoAHUAbgBrA*", "*5HZXRDaHVua*",
  ↳ "*AEcAZQB0AEMAaAB1AG4Aaw*",
  ↳ "*LgBHAGUAdABDAGgAdQBuAGsA*", "*LkdldENodW5r*", "*R2V0Q2h1bm*",
  ↳ "*AEgAUgBFAEEARABfAEkATgBGAE8ANgA0A*",
  ↳ "*QASABSAEUAAQQBEAF8ASQBOAEYATwA2ADQA*", "*RIUkVBRf9JTkZPNj*",
  ↳ "*SFJFQURfSU5GTzY0*", "*VABIAFIARQBBAEQAXwBJAE4ARgBPADYANA*",
  ↳ ", "*VEhSRUFEX0lORk82N*",
  ↳ "*AHIAZQBhAHQAZQBSAGUAbQBvAHQAZQBUAGgAcgBIAGEAZA*",
  ↳ ", "*cmVhdGVSZW1vdGVUaHJlYW*",
  ↳ ", "*MAcgBIAGEAdABIAFIAZQBtAG8AdABIAFQAaABYAGUAYQBkA*",
  ↳ ", "*NyZWFOZVJlbW90ZVRocmVhZ*", "*Q3JlYXRIUmVtb3RlVGhyZWZk*",
  ↳ ", "*QwByAGUAYQB0AGUAAUgBIAg0ABwB0AGUAVAB0AHIAZQBhAGQA*",
  ↳ ", "*0AZQBtAG0AbwB2AGUA*", "*1lbW1vdm*", "*AGUAbQBtAG8AdgBIA*",
  ↳ ", "*bQBIAG0AbQBvAHYAZQ*", "*bWVtbW92Z*", "*ZW1tb3Zl"] -user IN EXCLUDED_
  ↳ USERS
```

2.293 LP_Malicious File Execution Detected

- **Trigger Condition:** Execution of a suspicious file by wscript and cscript.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter
- **ATT&CK ID:** T1059
- **Minimum Log Source Requirement:** Windows Sysmon

- **Query:**

```
norm_id=WindowsSysmon event_id=1 image IN ["*\\wscript.exe", "*\\cscript.exe"]  
↪ command IN ["*.jse", "*.vbe", "*.js", "*.vba"] -user IN EXCLUDED_USERS
```

2.294 LP_Malicious Service Installations Detected

- **Trigger Condition:** Malicious service installs appearing in lateral movement, credential dumping, and other suspicious activity are detected.
- **ATT&CK Category:** Persistence, Privilege Escalation
- **ATT&CK Tag:** Credential Dumping, System Services, Service Execution, New Service
- **ATT&CK ID:** T1003, T1569, T1569.002, T1543
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=7045 service in ["*\\PAExec*", "mssecsvc2.0", "*net user*",  
↪ "WCESERVICE", "WCE SERVICE", "winexesvc.exe*", "*\\DumpSvc.exe", "pwdump*",  
↪ "gsecdump*", "cachedump*"] -user IN EXCLUDED_USERS
```

2.295 LP_Malware Shellcode in Verclsid Target Process

- **Trigger Condition:** A process accessing verclsid.exe that injects shellcode from a Microsoft Office application or VBA macro is detected.
- **ATT&CK Category:** Defense Evasion, Privilege Escalation
- **ATT&CK Tag:** Process Injection, Verclsid
- **ATT&CK ID:** T1055, T1218.012
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=10 image="*\\verclsid.exe" access="0x1FFFFFF" (call_  
↪ trace="*|UNKNOWN(*VBE7.DLL*" OR ("process"="*\\Microsoft Office\\*" call_trace=  
↪ "*|UNKNOWN*")) -user IN EXCLUDED_USERS
```

2.296 LP_Malware Threat Connection from Malicious Source

- **Trigger Condition:** Inbound connection from malicious sources is detected.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Proxy
- **ATT&CK ID:** T1090
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

```
(source_address=* OR destination_address=*) source_address in MALWARE_IP?  
↪ destination_address IN HOMENET | process geoip(source_address) as country
```

2.297 LP_Malware Threat Connection to Malicious Destination

- **Trigger Condition:** Hosts make an outbound connection to malicious sources.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Proxy
- **ATT&CK ID:** T1090
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

```
(source_address=* OR destination_address=*) destination_address in MALWARE_IP?  
↪ source_address IN HOMENET | process geoip(destination_address) as country
```

2.298 LP_Malware Threat Connection to Malicious URLs

- **Trigger Condition:** A connection to a malicious URL is detected.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Proxy

- **ATT&CK ID:** T1090
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

```
url=* source_address=* | process domain(url) as domain | search domain in MALWARE_URL
```

2.299 LP_Malware Threat Emails Sent to Attacker

- **Trigger Condition:** Email is sent to malware listed emails.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Proxy, Exfiltration Over C2 Channel, Automated Exfiltration, Email Collection
- **ATT&CK ID:** T1090, T1041, T1020, T1114
- **Minimum Log Source Requirement:** Mail Server
- **Query:**

```
(receiver in MALWARE_EMAILS OR sender in MALWARE_EMAILS) sender=* receiver=?  
↪ (host=* OR source_host=*) | rename source_host as host
```

2.300 LP_Meltdown and Spectre Vulnerabilities

- **Trigger Condition:** Meltdown and Spectre vulnerabilities are detected in the system.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Software Discovery, Security Software Discovery
- **ATT&CK ID:** T1518, T1518.001
- **Minimum Log Source Requirement:** Vulnerability Management
- **Query:**

```
title=*spectre* or title=*meltdown* source_address=* | rename host as source_address |  
↪ chart count() by source_address, severity, cve_id, solution order by count() desc
```

2.301 LP_Meterpreter or Cobalt Strike Getsystem Service Start Detected

- **Trigger Condition:** The use of getsystem Meterpreter or Cobalt Strike command to obtain SYSTEM privileges by detecting a specific service starting.
- **ATT&CK Category:** Privilege Escalation, Defense Evasion
- **ATT&CK Tag:** Access Token Manipulation
- **ATT&CK ID:** T1134
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create parent_process="*\services.exe" command IN ['*cmd* /c *  
↪ echo *\pipe\*', '*%COMPSEC%* /c * echo *\pipe\*', '*rundll32*.dll,a*/p:*'] -command=  
↪ "*MpCmdRun*" -user IN EXCLUDED_USERS
```

2.302 LP_Microsoft ActiveX Control Code Execution Vulnerability Detected

- **Trigger Condition:** Remote code execution in Microsoft ActiveX Control (CVE-2012-0158) is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Exploitation for Client Execution
- **ATT&CK ID:** T1203
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon label=Key label="Map" label=Registry target_object=  
↪ '*Software\Microsoft\Office*Resiliency' -user IN EXCLUDED_USERS
```

2.303 LP_Microsoft DotNET Framework Remote Code Execution Detected

- **Trigger Condition:** Remote code execution vulnerability (CVE-2017-8759) in Microsoft .NET Framework is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** User Execution, Malicious File
- **ATT&CK ID:** T1204, T1204.002
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 parent_process='*WINWORD.exe' parent_
↪command='*.rtf*' "process"='*\csc.exe' -user IN EXCLUDED_USERS
```

2.304 LP_Microsoft Office Memory Corruption Vulnerability CVE-2015-1641 Detected

- **Trigger Condition:** The exploitation of memory corruption vulnerability (CVE-2015-1641) in Microsoft Office is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** User Execution
- **ATT&CK ID:** T1204
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon label=Image label=Load "process" IN ['*WINWORD.exe',
↪'*EXCEL.exe'] image='*MSVCR71.DLL' -user IN EXCLUDED_USERS
```

2.305 LP_Microsoft Office Memory Corruption Vulnerability CVE-2017-0199 Detected

- **Trigger Condition:** The exploitation of memory corruption vulnerability (CVE-2017-0199) in Microsoft Office is detected.

- **ATT&CK Category:** Execution
- **ATT&CK Tag:** User Execution
- **ATT&CK ID:** T1204
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon label=Network label=Connection image='*WINWORD.exe'
↪ destination_address IN MOST_EXPLOITABLE_IPS -user IN EXCLUDED_USERS
```

2.306 LP_Microsoft Office Memory Corruption Vulnerability CVE-2017-11882 Detected

- **Trigger Condition:** The exploitation of memory corruption vulnerability (CVE-2017-11882) in Microsoft Office is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** User Execution
- **ATT&CK ID:** T1204
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon label="Process" label=Create parent_image='*EQNEDT32.EXE'
↪ 'parent_command='*EQNEDT32.EXE*-Embedding' image='*.exe' -user IN EXCLUDED_
↪ USERS
```

2.307 LP_Mimikatz Command Line Detected

- **Trigger Condition:** *mimikatz* command line arguments are detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** OS Credential Dumping, LSASS Memory, Security Account Manager, LSA Secrets, Cached Domain Credentials, DCSync
- **ATT&CK ID:** T1003, T1003.001, T1003.002, T1003.003, T1003.004, T1003.005, T1003.006

- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create command IN ["*DumpCreds*", "*mimikatz*", "*::aadcookie*",
↳ "*::detours*", "*::memssp*", "*::mflt*", "*::ncroutemon*", "*::ngcsign*",
↳ "*::printrnightmare*", "*::skeleton*", "*::preshutdown*", "*::mstsc*", "*::multirdp*",
↳ "*rpc:*", "*token:*", "*crypto:*", "*dpapi:*", "*sekurlsa:*", "*kerberos:*",
↳ "*lsadump:*", "*privilege:*", "*process:*", "*vault:*", "*crypto:*", "*misc:*", "*event:*",
↳ "*ILS::AppHost*", "*net:*", "*sid:*", "*standard:*", "*vault:*"]
```

2.308 LP_Mitre Discovery Using Query Registry Detected

- **Trigger Condition:** Discovery uses the attack technique Query Registry.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Query Registry
- **ATT&CK ID:** T1012
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer label="Process" label=Create commandline="*reg query*" -user IN[
↳ EXCLUDED_USERS | process eval("attack_class='Discovery'") | process eval("technique=
↳ 'Query Registry'") | rename commandline as command | chart count() by user, host,
↳ domain, log_ts, command, attack_class, technique order by count() desc limit 10
```

2.309 LP_Mitre Discovery Using System Network Configuration Discovery Detected

- **Trigger Condition:** Discovery uses the attack technique System Network Configuration Discovery.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** System Network Configuration Discovery
- **ATT&CK ID:** T1016
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer label="Process" label=Create (commandline="*ipconfig.exe*" OR
↪ commandline="*route.exe*" OR commandline="*netsh advfirewall*" OR commandline=
↪ "*arp.exe*" OR commandline="*nbtstat.exe*" OR commandline="*netsh.exe*interface
↪ show" OR commandline="*net*config") -user IN EXCLUDED_USERS | process eval(
↪ "attack_class='Discovery'") | process eval("technique='System Network Configuration
↪ Discovery'") | rename commandline as command | chart count() by user, host, domain,
↪ log_ts, command, attack_class, technique order by count() desc limit 10
```

2.310 LP_Mitre Persistence via Winlogon Helper DLL Detected

- **Trigger Condition:** Modifications in Winlogon registry keys are detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Boot or Logon Autostart Execution, Winlogon Helper DLL
- **ATT&CK ID:** T1547, T1547.004
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4657 object=Winlogon event_category=Registry path=
↪ "*Windows NT\CurrentVersion*" new_value=* -user IN EXCLUDED_USERS
```

2.311 LP_MMC Spawning Windows Shell Detected

- **Trigger Condition:** Windows command line executable starting from MMC is detected.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Distributed Component Object Model
- **ATT&CK ID:** T1021.003
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create parent_process="*\\mmc.exe" ("process" IN ["*\\cmd.exe",
↪ "*\\powershell.exe", "*\\pwsh.exe", "*\\wscript.exe", "*\\cscript.exe", "*\\sh.exe", "*\\bash.
↪ exe", "*\\reg.exe", "*\\regsvr32.exe"] OR "process"="*\\BITSADMIN*") -user IN
↪ EXCLUDED_USERS
```

2.312 LP_Most Exploitable Vulnerabilities Detected

- **Trigger Condition:** The most exploitable vulnerabilities from 2015 are detected in a network. For this alert to work, MOST_EXPLOITABLE_CVE must be updated with the list of exploitable vulnerabilities.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Network Service Scanning, Software Discovery, Security Software Discovery
- **ATT&CK ID:** T1046, T1518, T1518.001
- **Minimum Log Source Requirement:** Vulnerability Management
- **Query:**

```
norm_id=VulnerabilityManagement cve_id IN MOST_EXPLOITABLE_CVE
```

2.313 LP_Mshta JavaScript Execution Detected

- **Trigger Condition:** The *mshta.exe* command is detected.
- **ATT&CK Category:** Defense Evasion, Execution
- **ATT&CK Tag:** Signed Binary Proxy Execution, Mshta
- **ATT&CK ID:** T1218, T1218.005
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 image="*\mshta.exe" command="*javascript*" -  
↪ user IN EXCLUDED_USERS
```

2.314 LP_MSHTA Spawning Windows Shell Detected

- **Trigger Condition:** Windows command line executable started from MSHTA is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Mshta

- **ATT&CK ID:** T1218.005
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create parent_process="*\mshta.exe" "process" IN ["*\cmd.exe",
↪ "powershell.exe", "wscript.exe", "cscript.exe", "sh.exe", "bash.exe", "reg.
↪ exe", "regsvr32.exe", "bitsadmin.exe"]
```

2.315 LP_MSHTA Suspicious Execution Detected

- **Trigger Condition:** *mshta.exe* suspicious execution patterns sometimes involving file polyglotism is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Deobfuscate/Decode Files or Information
- **ATT&CK ID:** T1140
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
event_id=1 image="*\mshta.exe" command IN ["*vbscript*", "*.jpg*", "*.png*", "*.lnk*",
↪ "*.xls*", "*.doc*", "*.zip*"] -user IN EXCLUDED_USERS
```

2.316 LP_MsiExec Web Install Detected

- **Trigger Condition:** When the *msiexec* process starts with the web address as a parameter is detected.
- **ATT&CK Category:** Defense Evasion, Command and Control
- **ATT&CK Tag:** Ingress Tool Transfer, Msiexec
- **ATT&CK ID:** T1105, T1218.007
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label=create label="process" command="*msiexec*" command="*://*"
```

2.317 LP_MSTSC Shadowing Detected

- **Trigger Condition:** Hijacking of Remote Desktop Protocol (RDP) session using Microsoft Terminal Services Client (MSTSC) shadowing is detected.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Remote Service Session Hijacking, RDP Hijacking
- **ATT&CK ID:** T1563, T1563.002
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label=Create label="Process" command="*noconsentprompt*" command="*shadow:*" -
↪ user IN EXCLUDED_USERS
```

2.318 LP_Multiple Failed Login Followed by Successful Login Followed by Logoff

- **Trigger Condition:** Multiple failed login attempts are followed by successful login, and then by log off from the same user are detected.
- **ATT&CK Category:** Defense Evasion, Persistence, Privilege Escalation, Initial Access, Credential Access
- **ATT&CK Tag:** Valid Accounts, Brute Force
- **ATT&CK ID:** T1078, T1110
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
[incident_name="Multiple Failed User Login Followed by Successful Login" incident_
↪ user=*] as FirstAlert followed by [norm_id=WinServer* label=User label=Logoff user=* -
↪ user IN EXCLUDED_USERS] as Logoff on FirstAlert.incident_user=Logoff.user | rename
↪ Logoff.user as User, FirstAlert.incident_address as SourceAddress
```

2.319 LP_Named Pipe added to Null Session Detected

- **Trigger Condition:** A new value set for the NullSessionPipe registry key is detected.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Remote Services
- **ATT&CK ID:** T1021
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=13 "process"="*\reg.exe" target_object=
↳ "\lanmanserver\NullSessionPipes" -user IN EXCLUDED_USERS
```

2.320 LP_Narrators Feedback-Hub Persistence Detected

- **Trigger Condition:** Abusing Windows 10 Narrator's Feedback-Hub is detected.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Boot or Logon Autostart Execution, Registry Run Keys/Startup Folder
- **ATT&CK ID:** T1547, T1547.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
(event_id=12 event_type="DeleteValue" target_object=
↳ "\AppXypsaf9f1qserqevf0sww76dx4k9a5206\Shell\open\command\DelegateExecute")
↳ OR (event_id=13 target_object=
↳ "\AppXypsaf9f1qserqevf0sww76dx4k9a5206\Shell\open\command\{Default}")
```

2.321 LP_Net exe Execution Detected

- **Trigger Condition:** The execution of Net.exe, which can be suspicious or benign, is detected.
- **ATT&CK Category:** Lateral Movement, Discovery, Defense Evasion

- **ATT&CK Tag:** Obfuscated Files or Information, System Network Connections Discovery, Remote Services, Network Share Discovery
- **ATT&CK ID:** T1027, T1049, T1021, T1135
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 image IN ["*\net.exe", "*\net1.exe"] command IN [
↪ "* group*", "* localgroup*", "* user*", "* view*", "* share", "* accounts*", "* use*", "*[?]
↪ stop *"] -user IN EXCLUDED_USERS
```

2.322 LP_NetNTLM Downgrade Attack Detected

- **Trigger Condition:** When post-exploitation using NetNTLM downgrade attacks are detected. NetNTLM is a proprietary authentication protocol used by Microsoft Windows. Adversaries may use a downgrade attack to force the use of a weaker version of the protocol, allowing them to intercept and crack the password hashes used for authentication. This can allow the adversary to gain unauthorized access to the system.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Impair Defenses, Disable or Modify Tools, Modify Registry
- **ATT&CK ID:** T1562, T1562.001, T1112
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
(event_id=13 target_object IN ["*SYSTEM*\ControlSet*\Control\Lsa\Imcompatibilitylevel",
↪ "*SYSTEM*\ControlSet*\Control\Lsa\NtlmMinClientSec",
↪ "*SYSTEM*\ControlSet*\Control\Lsa\RestrictSendingNTLMTraffic"]) OR (norm_
↪ id=WinServer event_id=4657 object_name=
↪ "\REGISTRY\MACHINE\SYSTEM*\ControlSet*\Control\Lsa" object_value IN [
↪ "LmCompatibilityLevel", "NtlmMinClientSec", "RestrictSendingNTLMTraffic"]) -user IN[?]
↪ EXCLUDED_USERS
```

2.323 LP_Netsh Port Forwarding Detected

- **Trigger Condition:** The *netsh* command used in the configuration of port forwarding is detected. Port forwarding is a pivoting technique that redirects traffic from one port to another.

- **ATT&CK Category:** Lateral Movement, Command and Control
- **ATT&CK Tag:** Proxy, Exploitation of Remote Services
- **ATT&CK ID:** T1090, T1210
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="create" label="process" "process"="*\netsh.exe" command in ["*interface*  
↪portproxy add v4tov4 *", "*i p a v*"] -user IN EXCLUDED_USERS
```

2.324 LP_Netsh RDP Port Forwarding Detected

- **Trigger Condition:** The *netsh* command used in the configuration of port forwarding of port 3389 for RDP is detected.
- **ATT&CK Category:** Lateral Movement, Command and Control
- **ATT&CK Tag:** Remote Services, Proxy
- **ATT&CK ID:** T1021, T1090
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create command IN ["netsh i* p*=3389 c*"] -user IN EXCLUDED_  
↪USERS
```

2.325 LP_Network Share Connection Removed

- **Trigger Condition:** The removal of a share connection is detected. Adversaries removes share connections that are no longer useful to clean traces of their operation.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Network Share Connection Removal
- **ATT&CK ID:** T1070.005
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="create" label="process" "process" in ["*\net.exe", " *\net1.exe"] command =
↳ "*share*" command="*delete*"
```

2.326 LP_Network Share Discovery

- **Trigger Condition:** The net utility used to query a system for available shared drives using net view or net share command is detected. Adversaries look for folders and drive shared on remote systems to identify sources of information to gather as a precursor for collecting and identifying potential systems of interest for Lateral Movement.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Network Share Discovery
- **ATT&CK ID:** T1135
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create ("process" IN ["*\net.exe", " *\net1.exe"] command="*net*
↳ " (command="*view*" command="*\") OR (command="*share*")) OR (command IN [
↳ "*get-smbshare*", "*Find-DomainShare*", "*Invoke-ShareFinder*",
↳ "*shareenumeration*")) OR (command="*dir*" command="*\") command IN ["*c$",
↳ "*admin$", "*IPC$"])
```

2.327 LP_Network Sniffing Detected

- **Trigger Condition:** When the execution of network sniffing tools is detected. Adversaries may use network sniffing to intercept sensitive information, such as passwords or confidential data, as it is transmitted over the network. They may also use sniffing to gain visibility into network traffic and identify vulnerabilities or weaknesses.
- **ATT&CK Category:** Credential Access, Discovery
- **ATT&CK Tag:** Network Sniffing
- **ATT&CK ID:** T1040
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
'label="Process" label=create "process" IN ["*tshark.exe", "*windump.exe", "*logman.exe"
↪ ", "*tcpdump.exe", "*wprui.exe", "*wpr.exe"] -user IN EXCLUDED_USERS'
```

2.328 LP_New Firewall Port Opening Detected

- **Trigger Condition:** An opening of a new port in a firewall is detected.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Non-Standard Port
- **ATT&CK ID:** T1571
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4657 object=FirewallRules event_category=Registry object_
↪ name= "*ControlSet*FirewallPolicy\FirewallRules" new_value=* -user IN EXCLUDED_
↪ USERS | norm on new_value <:all>Action=<action:word><:all>Active=<active:word>
↪ <:all>Dir=<direction:word><:all>Protocol=<proto:int><:all>Port=<port:int><:all>
↪ Name=<rule:string><:'\|'> | process eval("protocol = if(proto == 6) {return 'TCP'} else
↪ {return 'UDP'}")
```

2.329 LP_New RUN Key Pointing to Suspicious Folder Detected

- **Trigger Condition:** A new suspicious RUN key element pointing to an executable in a folder is detected.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Boot or Logon Autostart Execution, Registry Run Keys/Startup Folder
- **ATT&CK ID:** T1547, T1547.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
event_id=13 target_object IN ["*\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\*",
↪ "*\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\RunOnce\\*"] detail IN [
↪ "*C:\\Windows\\Temp\\*", "*\\AppData\\*", "%AppData%\\*", "*C:\\$Recycle.bin\\*",
↪ "*C:\\Temp\\*", "*C:\\Users\\Public\\*", "%Public%\\*", "*C:\\Users\\Default\\*",
↪ "*C:\\Users\\Desktop\\*", "wscript*", "cscript*"] -detail IN [ (continues on next page)
↪ "*\\AppData\\Local\\Microsoft\\OneDrive\\*"] -user IN EXCLUDED_USERS
```

(continued from previous page)

2.330 LP_New Service Creation

- **Trigger Condition:** The creation of a new service is detected. Windows Services can allow the creation and management of long-running processes. It can start automatically and keep running for a long time after the user logs off. Adversaries might leverage this functionality to maintain persistence and escalate their privilege.
- **ATT&CK Category:** Persistence, Privilege Escalation
- **ATT&CK Tag:** Create or Modify System Process, Windows Service
- **ATT&CK ID:** T1543, T1543.003
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Create" label="Process" "process" IN ["*sc.exe", "*powershell.exe", "*cmd.exe"][2]
↪ command IN [ "*Get-WmiObject*Win32_Service*create*", "*create*binPath=*", "*New-Service*-BinaryPathName*", "*powershell*", "*mshta*", "*wscript*", "*cscript*",
↪ "*svchost*", "*dllhost*", "*cmd *", "*cmd.exe /c*", "*cmd.exe /k*", "*cmd.exe /r*",
↪ "*rundll32*", "*C:\Users\Public*", "*\Downloads\*", "*\Desktop\*",
↪ "*\Microsoft\Windows\Start Menu\Programs\Startup\*", "*C:\Windows\TEMP\*",
↪ "*\AppData\Local\Temp*" ] -user IN EXCLUDED_USERS
```

2.331 LP_Non Interactive PowerShell Execution

- **Trigger Condition:** Non-interactive Command and Scripting Interpreter and PowerShell activity by looking at *powershell.exe* with no *explorer.exe* as a parent is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, PowerShell
- **ATT&CK ID:** T1059, T1059.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
'label="Create" label="Process" ("Process" IN ["*\powershell.exe", ".*\pwsh.exe"] OR
↪(file IN ["PowerShell.EXE", "pwsh.dll"])) -(parent_process IN ["*C:\Windows\explorer.exe
↪", "*C:\Windows\System32\CompatTelRunner.exe", "*C:\Windows\SysWOW64\explorer.
↪exe", "C:\$WINDOWS.~BT\Sources\SetupHost.exe"]) -(parent_process="C:\Users\*
↪parent_process="*\AppData\Local\Programs\Microsoft VS Code\Code.exe" parent_
↪command="* --ms-enable-electron-run-as-node *") -user IN EXCLUDED_USERS'
```

2.332 LP_NoPowerShell Tool Activity Detected

- **Trigger Condition:** Execution of NoCommand and Scripting Interpreter and PowerShell tool.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Shared Modules
- **ATT&CK ID:** T1129
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=11 -file in ["*cscript.exe.log", "*wscript.exe.log",
↪"*wmic.exe.log", "*mshta.exe.log", "*svchost.exe.log", "*regsvr32.exe.log", "*rundll32.
↪exe.log"] file="*.exe.log" -user IN EXCLUDED_USERS
```

2.333 LP_NotPetya Ransomware Activity Detected

- **Trigger Condition:** NotPetya ransomware activity in which the extracted passwords are passed back to the main module via named pipe is detected. The file system journal of drive C is deleted, and window event logs are cleared using wevtutil.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Signed Binary Proxy Execution, Rundll32, Indicator Removal on Host
- **ATT&CK ID:** T1218, T1218.011, T1070
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 (command="*\AppData\Local\Temp\*\.pipe\*"
↪OR (image="*\rundll32.exe" command="*.dat, #1")) -user IN EXCLUDED_USERS
```

2.334 LP_Office365 Multiple Failed Login from Different Host by Single User

- **Trigger Condition:** A user attempts multiple failed logins from distinct hosts with a count greater than one.
- **ATT&CK Category:** Credential Access, Persistence, Defense Evasion, Privilege Escalation, Initial Access
- **ATT&CK Tag:** Brute Force, Valid Accounts
- **ATT&CK ID:** T1110, T1078
- **Minimum Log Source Requirement:** Office365
- **Query:**

```
norm_id="Office365" source_address=* label=User label=Login label=Fail | chart distinct_
↪count(source_address) as DC by user | search DC>1
```

2.335 LP_Office365 Multiple Failed Login from Same Host

- **Trigger Condition:** Multiple failed logins from the same host with a count greater than five.
- **ATT&CK Category:** Credential Access, Persistence, Defense Evasion, Privilege Escalation, Initial Access
- **ATT&CK Tag:** Brute Force, Valid Accounts
- **ATT&CK ID:** T1110, T1078
- **Minimum Log Source Requirement:** Office365
- **Query:**

```
norm_id="Office365" source_address=* label=User label=Login label=Fail | chart count()
↪as "Cnt" by user, source_address | search Cnt > 5
```

2.336 LP_Office365 Multiple Successful Login from Different Country by Single User

- **Trigger Condition:** A user attempts multiple failed logins from different countries with a count greater than one.
- **ATT&CK Category:** Defense Evasion, Persistence, Privilege Escalation, Initial Access
- **ATT&CK Tag:** Valid Accounts
- **ATT&CK ID:** T1078
- **Minimum Log Source Requirement:** Office365
- **Query:**

```
norm_id="Office365" label=User label=login label=Successful source_address=* |  
↪ process geoip(source_address) as country | chart distinct_count(country) as DC by user |  
↪ search DC >1
```

2.337 LP_Office365 Multiple Successful Login From Different Host by Single User

- **Trigger Condition:** A user attempts multiple successful logins from a distinct host with a count greater than one.
- **ATT&CK Category:** Defense Evasion, Persistence, Privilege Escalation, Initial Access
- **ATT&CK Tag:** Valid Accounts
- **ATT&CK ID:** T1078
- **Minimum Log Source Requirement:** Office365
- **Query:**

```
norm_id="Office365" label=User label=login label=Successful source_address=* | chart  
↪ distinct_count(source_address) as DC by user | search DC >1
```

2.338 LP_Office365 Password Resets

- **Trigger Condition:** A user's password is reset.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Account Manipulation
- **ATT&CK ID:** T1098
- **Minimum Log Source Requirement:** Office365
- **Query:**

```
norm_id="Office365" label=Password label=Reset user=*
```

2.339 LP_OpenWith Execution of Specified Binary Detected

- **Trigger Condition:** The execution of *OpenWith.exe* with command line argument "-c" or "/c" is detected.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label="Process" label=Create "process"="*\OpenWith.exe" command IN ["/c*", "-c*"] -  
↪ user IN EXCLUDED_USERS
```

2.340 LP_Password Change on DSRM Account Detected

- **Trigger Condition:** Password change in Directory Service Restore Mode (DSRM) account is detected.
- **ATT&CK Category:** Persistence, Privilege Escalation
- **ATT&CK Tag:** Account Manipulation

- **ATT&CK ID:** T1098
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4794 -user IN EXCLUDED_USERS
```

2.341 LP_Password Dumper Remote Thread in LSASS

- **Trigger Condition:** Password dumper activity by monitoring remote thread creation event ID 8 in combination with the lsass.exe process as *TargetImage* is detected. The process in the field *Process* is a malicious program and a single execution can lead to hundreds of events.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** OS Credential Dumping, LSASS Memory
- **ATT&CK ID:** T1003, T1003.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
'label="Remote" label="Thread" label="Create" image="*\lsass.exe" start_module="" -  
↪user IN EXCLUDED_USERS'
```

2.342 LP_Password Spraying Attack Detected

- **Trigger Condition:** Multiple login fail attempts on a host by various users are detected. Adversaries can use a list of commonly used passwords against different versions to attempt to obtain valid account credentials.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Password Spraying
- **ATT&CK ID:** T1110.003
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4625 | chart distinct_count(user) as UserCount, distinct_
↪ list(user) as Users by host | search UserCount > 5
```

2.343 LP_Persistence and Execution at Scale via GPO Scheduled Task

- **Trigger Condition:** Lateral movement using GPO scheduled task used to deploy ransomware at scale is detected.
- **ATT&CK Category:** Persistence, Lateral Movement, Execution, Privilege Escalation
- **ATT&CK Tag:** Scheduled Task/Job, Scheduled Task
- **ATT&CK ID:** T1053, T1053.005
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=5145 share_name="\*\SYSVOL" relative_target=
↪ "\*ScheduledTasks.xml" access="\*WriteData*" -user IN EXCLUDED_USERS
```

2.344 LP_Possible Access to ADMIN Share

- **Trigger Condition:** Access to \$ADMIN share is detected, which may help to detect lateral movement attempts. Since Windows Admin Share activity is so common, it provides adversaries with a powerful, discreet way to move laterally within an environment.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Remote Services
- **ATT&CK ID:** T1021
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=5140 share_name="Admin$" -user="\*$" -user IN
↪ EXCLUDED_USERS
```

2.345 LP_Possible Account Misuse-Privilege Escalation

- **Trigger Condition:** The non-admin users are assigned privileged access. The event maps to event ID of 4648 and 4672 in Windows.
- **ATT&CK Category:** Privilege Escalation, Persistence, Defense Evasion
- **ATT&CK Tag:** Account Manipulation, Abuse Elevation Control Mechanism, Bypass User Account Control
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
((label=Privilege label=Assign) or (label>Login label=Explicit label=Credential) user=* -
↪ user in ADMINS) OR (label=User label=Add label=Group user=* group=*admin*)
```

2.346 LP_Possible Applocker Bypass Detected

- **Trigger Condition:** The execution of executables like msdt, installutil, regsvcs, regasm or msbuild.ieexec is detected, which is used to bypass Applocker whitelisting is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Signed Binary Proxy Execution, Mshta, InstallUtil, Regsvcs/Regasm, Trusted Developer Utilities, MSBuild
- **ATT&CK ID:** T1218, T1218.004, T1218.009, T1127, T1218.005, T1127.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Create" label="Process" command IN ["*\msdt.exe*", "*\installutil.exe*",
↪ "*\regsvcs.exe*", "*\regasm.exe*", "*\msbuild.exe*", "*\ieexec.exe*"] -user IN
↪ EXCLUDED_USERS
```

2.347 LP_Possible Bitsadmin Download Detected

- **Trigger Condition:** The use of *bitsadmin* downloading a file is detected.
- **ATT&CK Category:** Defense Evasion, Persistence
- **ATT&CK Tag:** BITS Jobs
- **ATT&CK ID:** T1197
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
'label="Process" label=Create ("process"="*\bitsadmin.exe" (command IN ["*/create *", "*/
↪addfile *"] command="*http*")OR (7104command="*/transfer *")) OR (command="*copy
↪bitsadmin.exe*") -user IN EXCLUDED_USERS'
```

2.348 LP_Possible Botnet Connection-DNS Server Modified

- **Trigger Condition:** An unauthorized default Application Layer Protocol and DNS server modification are detected in Unix or Windows Server.
- **ATT&CK Category:** Impact, Command and Control, Defense Evasion
- **ATT&CK Tag:** Network Denial of Service, Proxy, Exploitation for Defense Evasion
- **ATT&CK ID:** T1498, T1090, T1211
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
((norm_id=Unix action="RUN" (file="etc/resolv.conf" or file="*\etc\host")) or (norm_
↪id=WinServer* (label=File (label=Write or label=Modify) path=
↪"C:\Windows\System32\Drivers\etc" object="hosts") or (label=DNS label=Update
↪(label=Successful or label=Request OR label=Fail)) (host=* or source_address=*)) -user
↪IN EXCLUDED_USERS
```

2.349 LP_Possible Botnet Connection-IRC Port

- **Trigger Condition:** The connection through the IRC port is detected. For this alert to work, you must update the list IRC_PORTS, including commonly used ports 6660 to 6669 and 6700.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Firewall, IDS/IPS, Webserver
- **Query:**

```
source_address=* destination_address=* destination_port in IRC_PORTS
```

2.350 LP_Possible Botnet Connection-Outbound DDOS

- **Trigger Condition:** Multiple hosts connecting to the same destination address is detected.
- **ATT&CK Category:** Impact, Command and Control, Defense Evasion
- **ATT&CK Tag:** Network Denial of Service, Proxy, Exploitation for Defense Evasion
- **ATT&CK ID:** T1498, T1090, T1211
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

```
label=Connection source_address in HOMENET destination_address=* | chart distinct_
↪count(source_address) as source by destination_address| search source>100
```

2.351 LP_Possible Botnet Connection-Outbound Spam

- **Trigger Condition:** An unauthorized email sent through an open relay is detected.
- **ATT&CK Category:** Command and Control, Defense Evasion, Impact
- **ATT&CK Tag:** Proxy, Exploitation for Defense Evasion, Network Denial of Service
- **ATT&CK ID:** T1090, T1211, T1498

- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

```
(source_address=* or host=* method="HELO" or method="EHLO") or
↪(label=Connection destination_port="25" source_address=* or host=*) | search -source_
↪address IN MAIL_SERVER_IP
```

2.352 LP_Possible CLR DLL Loaded Via Office Applications

- **Trigger Condition:** CLR DLL loaded by an Office Product like WinWord, PowerPoint Excel or Outlook is detected.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** Phishing, Spearphishing Attachment
- **ATT&CK ID:** T1566, T1566.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=7 "process" IN ["*\winword.exe", "*\powerpnt.exe",
↪"*\excel.exe", "*\outlook.exe"] image IN ["*\clr.dll*"] -user IN EXCLUDED_USERS
```

2.353 LP_Possible Credential Dump-Tools Named Pipes Detected

- **Trigger Condition:** A well-known credential dumping tool execution via specifically named pipes like lsadump, cachedump, or wceservicepipe is detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** OS Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=17 pipe IN ["*\lsadump*", "*\cachedump*",
↪"*\wceservicepipe*"] -user IN EXCLUDED_USERS
```

2.354 LP_Possible Data Breach

- **Trigger Condition:** Unauthorized transfer of sensitive data is detected using mail applications, cloud applications, or other sources. For the alert to work, you must update the lists RESIGNED_EMPLOYEES, KNOWN_DOMAINS, and CLOUD_APPLICATIONS.
- **ATT&CK Category:** Exfiltration
- **ATT&CK Tag:** Exfiltration Over Web Service, Exfiltration to Cloud Storage
- **ATT&CK ID:** T1567, T1567.002
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

```
(label=Mail object="*attachment*" sender in RESIGNED_EMPLOYEES -receiver in
KNOWN_DOMAINS) or (label=Object label=Access (label=Write or label=Modify)
event_category="*Removable*" user in RESIGNED_EMPLOYEES) or (label=Access
label=Object (label=Write or label=Modify) path IN CLOUD_APPLICATIONS user in
RESIGNED_EMPLOYEES) or (label=Data label=Transfer label=Sensitive source_
address=* destination_address=*)
```

2.355 LP_Possible Data Breach-Off Hour Transfer

- **Trigger Condition:** Unauthorized transfer of sensitive data during off-hours is detected.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

```
(norm_id=*Firewall or norm_id=*IDS) label=Connection source_address=* destination_
address=* destination_port=* sent_datasize=* ((day_of_week(log_ts) IN ["Monday",
Tuesday", "Wednesday", "Thursday", "Friday"]) and (hour(log_ts)<9 or hour(log_ts)>
17)) or (day_of_week(log_ts) IN ["Saturday", "Sunday"]) | chart sum((sent_datasize)/1024/
1024) as TotalSentMB by user | search TotalSentMB>20
```

2.356 LP_Possible DDOS Attack

- **Trigger Condition:** A considerable number of inbound traffic within a short period is detected.
- **ATT&CK Category:** Initial Access, Impact
- **ATT&CK Tag:** Exploit Public-Facing Application, Network Denial of Service
- **ATT&CK ID:** T1190, T1498
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

```
label=Deny ((protocol=icmp or application="icmp" or service=icmp) or (protocol=http or
↪ protocol=https) or (protocol=udp or 'dns reply' or 'SYN') source_address=* destination_
↪ address=*) | chart count(source_address) as ddos_source by destination_address | search
↪ ddos_source>2000
```

2.357 LP_Possible Detection of SafetyKatz

- **Trigger Condition:** SafetyKatz behavior where a temp file *debug.bin* is created in temp folder to dump credentials using *lsass*.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** OS Credential Dumping, LSASS Memory
- **ATT&CK ID:** T1003, T1003.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=11 path="*\Temp" file="debug.bin" -user IN
↪ EXCLUDED_USERS
```

2.358 LP_Possible DNS Rebinding Detected

- **Trigger Condition:** Different DNS answers by one domain with IPs from internal and external networks are detected. Typically, DNS-answer contains TTL greater than 100. Application Layer Protocol and DNS-record are saved in the host cache during TTL.

- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
event_id=22 query="*" status_code="0" query_result IN [ "(:ffff:)?10.*", "(:ffff:)?192.168.*",
→ "(:ffff:)?172.16.*", "(:ffff:)?172.17.*", "(:ffff:)?172.18.*", "(:ffff:)?172.19.*", "(:ffff:)?172.20.*",
→ "(:ffff:)?172.21.*", "(:ffff:)?172.22.*", "(:ffff:)?172.23.*", "(:ffff:)?172.24.*", "(:ffff:)?172.25.*",
→ "(:ffff:)?172.26.*", "(:ffff:)?172.27.*", "(:ffff:)?172.28.*", "(:ffff:)?172.29.*", "(:ffff:)?172.30.*",
→ "(:ffff:)?172.31.*", "(:ffff:)?127.*" ] -user IN EXCLUDED_USERS | chart
→ count(QueryName) as val by host | search val > 3
```

2.359 LP_Possible Empire Monkey Detected

- **Trigger Condition:** The execution of a specific command line sequence using the `cutil.exe` or `regsvr32.exe` tool is detected.
- **ATT&CK Category:** Execution, Defense Evasion
- **ATT&CK Tag:** PowerShell, Regsvr32
- **ATT&CK ID:** T1059.001, T1218.010
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create (command="*/i:%APPDATA%\logs.txt scrobj.dll" ("process
→ " = "*" \cutil.exe" OR description = "Microsoft(C) Registerserver")) -user IN EXCLUDED_
→ USERS
```

2.360 LP_Possible Impacket Lateral Movement Detected

- **Trigger Condition:** Instances of lateral movement using the Impacket framework, specifically when utilizing the `wmiexec`, `dcomexec`, `atexec` and `smbexec` tools are detected.
- **ATT&CK Category:** Lateral Movement, Execution

- **ATT&CK Tag:** Windows Management Instrumentation, Inter-Process Communication, Distributed Component Object Model, Remote Services, Component Object Model, Component Object Model
- **ATT&CK ID:** T1047, T1559, T1021.003, T1021, T1559.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create command="*cmd.exe*" command="*/c*" command="*&1
↪*" (parent_process IN ["*\wmiprvse.exe", "*\mmc.exe", "*\explorer.exe", "*\services.
↪exe"] command="*/Q*" command="*\\127.0.0.1\\*" ) OR (parent_command IN [
↪"*svchost.exe -k netsvcs*", "*taskeng.exe*"] command="*Windows\Temp\*" ) host.exe -
↪k netsvcs", "taskeng.exe*"] command IN ["cmd.exe /C *Windows\Temp\*&1" ])) -user IN
↪EXCLUDED_USERS'
```

2.361 LP_Possible Impacket SecretDump Remote Activity

- **Trigger Condition:** Logpoint detects *share_nameAD* credential dumping using *impacket secretdump HKTL*.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** OS Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=5145 share_name="*\ADMIN$" relative_target=
↪"SYSTEM32\*.tmp" -user IN EXCLUDED_USERS
```

2.362 LP_Possible Inbound Spamming Detected

- **Trigger Condition:** Logpoint detects possible inbound spam.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Mail Server

- **Query:**

```
(sender=* receiver=* -sender in KNOWN_DOMAINS) | chart distinct_count(receiver) as ?
↪ spam_receiver by sender | search spam_receiver > 100
```

2.363 LP_Possible Insider Threat

- **Trigger Condition:** Logpoint detects alerts like privilege escalation, unauthorized access, and data breach for the same user.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Logpoint
- **Query:**

```
event_type="Possible Insider Threat" incident_user=* -incident_user in EXCLUDED_
↪ USERS | rename incident_user as user | chart distinct_count(incident_name) as ?
↪ AlertCount by user | search AlertCount > 2
```

2.364 LP_Malicious Payload Download via Office Binaries

- **Trigger Condition:** An arbitrary file downloaded using Microsoft Office binaries is detected.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Ingress Tool Transfer
- **ATT&CK ID:** T1105
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create ("process" IN ["*\powerpnt.exe", "*\winword.exe", "*\excel.
↪ exe"] OR file IN ["powerpnt.exe", "winword.exe", "excel.exe"]) command= "*http*" -
↪ user IN EXCLUDED_USERS
```

2.365 LP_Possible Malware Detected

- **Trigger Condition:** A file or software is detected as worm, virus, trojan, or malware.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Antivirus
- **Query:**

```
(label=Malware or label=Threat or label=Virus or label=Quarantine or label=Risk)
↪ (malware=* OR risk=* OR virus=*) (file=* or application=* or url=*)
```

2.366 LP_Possible Modification of Boot Configuration

- **Trigger Condition:** When the use of the bcdedit command to delete or modify Boot Configuration Data is detected. Boot Configuration Data (BCD) files provide a store that describes boot applications and application settings. Boot configuration data edit (bcdedit) allows manipulating BCD. This tactic is used by malware or attackers as a destructive technique to prevent system recovery. Legitimate usage can trigger this alert. We recommend including the legitimate user in the EXCLUDED_USERS list.
- **ATT&CK Category:** Impact, Defense Evasion, Persistence
- **ATT&CK Tag:** Inhibit System Recovery, Pre-OS Boot, Bootkit
- **ATT&CK ID:** T1490, T1542, T1542.003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 ((image="*\bcdedit.exe" command IN ["*delete*",
↪ "*import*", "set"]) OR ((command="*bootstatuspolicy*" command="*ignoreallfailures*"
↪ ") OR (command="*recoveryenabled*" command="*no*"))) -user IN EXCLUDED_USERS
```

2.367 LP_Possible Outbound Spamming Detected

- **Trigger Condition:** Mail received or sent to domains not included in the KNOWN_DOMAINS list is detected. The KNOWN_DOMAINS lists need to be updated with the domains known to communicate to and from the organization.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Mail Server
- **Query:**

```
(sender=* receiver=* -receiver in KNOWN_DOMAINS sender in KNOWN_DOMAINS) |  
↪ chart distinct_count(receiver) as spam_receiver by sender | search spam_receiver>100
```

2.368 LP_Possible Pass the Hash Activity Detected

- **Trigger Condition:** When the attack technique passes the hash, which is used to move laterally inside the network. Pass the hash is a method of authenticating to a system using a password hash rather than the actual password. Adversaries may use this technique to gain unauthorized access to a system, bypassing normal authentication controls. Pass the hash attacks can be challenging to detect and prevent, as they do not involve using a clear-text password.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Use Alternate Authentication Material, Pass the Hash
- **ATT&CK ID:** T1550, T1550.002
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4624 ((caller_id="S-1-0-0" logon_type="3" logon_process=  
↪ "NtLmSsp" key_length="0") OR (logon_type="9" logon_process="seclogo")) -user=  
↪ "ANONYMOUS LOGON" -user IN EXCLUDED_USERS
```

2.369 LP_Possible Privilege Escalation via Weak Service Permissions

- **Trigger Condition:** The `sc.exe` utility spawning by a user with medium integrity level to change the service `ImagePath` or `FailureCommand` is detected.
- **ATT&CK Category:** Privilege Escalation, Defense Evasion
- **ATT&CK Tag:** Access Token Manipulation
- **ATT&CK ID:** T1134
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label="Process" label=Create "process"="*\sc.exe" integrity_level="Medium" command
↪ IN ["*config*binPath*", "*failure*command*"] -user IN EXCLUDED_USERS
```

2.370 LP_Possible Process Hollowing Image Loading

- **Trigger Condition:** Loading of `saml.dll` or `WinSCard.dll` from untypical process is detected. For example, through process hollowing by Mimikatz.
- **ATT&CK Category:** Defense Evasion, Privilege Escalation
- **ATT&CK Tag:** Hijack Execution Flow, DLL Side-Loading, Process Injection, Process Hollowing
- **ATT&CK ID:** T1574, T1574.002, T1055, T1055.012
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=7 "process" IN ["*\notepad.exe"] image IN [
↪ "*\saml.dll", "*\WinSCard.dll"] -user IN EXCLUDED_USERS
```

2.371 LP_Possible SPN Enumeration Detected

- **Trigger Condition:** *Service Principal Name Enumeration* used for Steal or Forge Kerberos Tickets and Kerberoasting is detected.
- **ATT&CK Category:** Credential Access

- **ATT&CK Tag:** Steal or Forge Kerberos Tickets, Kerberoasting
- **ATT&CK ID:** T1558, T1558.003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label="Process" label=Create command="*-q*" "process"="*\setspn.exe" -user IN [
  ↳ EXCLUDED_USERS
```

2.372 LP_Possible SquiblyTwo Detected

- **Trigger Condition:** WMI SquiblyTwo Attack with possible renamed WMI seeking for imphash is detected.
- **ATT&CK Category:** Defense Evasion, Execution
- **ATT&CK Tag:** Windows Management Instrumentation, Visual Basic, JavaScript, XSL Script Processing
- **ATT&CK ID:** T1047, T1059.005, T1059.007, T1220
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 file="wmic.exe" hash_imphash IN [
  ↳ "1B1A3F43BF37B5BFE60751F2EE2F326E", "37777A96245A3C74EB217308F3546F4C",
  ↳ "9D87C9D67CE724033C0B40CC4CA1B206"] command="*format:*" command="*http*"
```

2.373 LP_Possible Taskmgr run as LOCAL_SYSTEM Detected

- **Trigger Condition:** Creation of a *taskmgr.exe* process in the context of LOCAL_SYSTEM is detected. *Taskmgr.exe* is the executable file for Windows Task Manager.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Masquerading
- **ATT&CK ID:** T1036
- **Minimum Log Source Requirement:** Windows Sysmon, Windows

- **Query:**

```
label="Process" label=Create "process"="*\taskmgr.exe" user in ["*AUTHORI*",
↳ "*AUTORI*"]
```

2.374 LP_Powershell AMSI Bypass via dotNET Reflection

- **Trigger Condition:** Request to *amsiInitFailed* used to disable AMSI Scanning is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, PowerShell
- **ATT&CK ID:** T1059, T1059.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
'label="Process" label=Create command IN ["*System.Management.Automation.AmsiUtils*"]
↳ command IN ["*amsiInitFailed*"] -user IN EXCLUDED_USERS'
```

2.375 LP_PowerShell Base64 Encoded Shellcode Detected

- **Trigger Condition:** Potential Base64 encoded shellcode for PowerShell memory injection is detected.
- **ATT&CK Category:** Defense Evasion, Privilege Escalation
- **ATT&CK Tag:** Process Injection
- **ATT&CK ID:** T1055
- **Minimum Log Source Requirement:** Windows, PowerShell
- **Query:**

```
norm_id=WinServer event_id=4104 script_block="*AAAAYInIM*" script_block IN [
↳ "*OiCAAAAYInIM*", "*OiJAAAAYInIM*"]
```

2.376 LP_PowerShell Network Connections Detected

- **Trigger Condition:** Logpoint detects a Command and Scripting Interpreter and PowerShell process that opens network connections. We recommend you check suspicious target ports and systems, and adjust them according to your environment. For example, extend filters with the company's IP range.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, PowerShell
- **ATT&CK ID:** T1059, T1059.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=3 image="*\powershell.exe" initiated="true" -
↪ destination_address IN HOMENET -user="NT AUTHORITY\SYSTEM" -user IN ?
↪ EXCLUDED_USERS
```

2.377 LP_PowerShell Profile Modification

- **Trigger Condition:** Modification of Command and Scripting Interpreter and PowerShell profile is detected.
- **ATT&CK Category:** Persistence, Privilege Escalation, Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, Event Triggered Execution, PowerShell Profile, Powershell
- **ATT&CK ID:** T1546, T1546.013, T1059, T1059.001
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4103 command in ["Write-Output", "Add-Content"] ?
↪ payload= "*powershell_profile*" -user IN EXCLUDED_USERS
```

2.378 LP_PowerShell Rundll32 Remote Thread Creation Detected

- **Trigger Condition:** The creation of a remote thread from a Powershell process in a rundll32 process is detected.
- **ATT&CK Category:** Defense Evasion, Execution
- **ATT&CK Tag:** PowerShell, Rundll32
- **ATT&CK ID:** T1059.001, T1218.011
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Remote" label="Thread" label="Create" "process" IN ["*\powershell.exe", "pwsh.
↪exe"] image="*\rundll32.exe" -user IN EXCLUDED_USERS
```

2.379 LP_PowerShell Script Run in AppData Detected

- **Trigger Condition:** A suspicious command line execution that invokes Command and Scripting Interpreter and PowerShell concerning an AppData folder is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** PowerShell
- **ATT&CK ID:** T1059.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Create" label="Process" command IN ["*\powershell.exe*", "*\powershell*",
↪ "*\pwsh*", "*\pwsh.exe*"] command="*/c *" command="*\AppData\*" command IN [
↪ "*\Local*", "*\Roaming\*"]
```

2.380 LP_PowerShell Version Downgrade Detected

- **Trigger Condition:** The execution of legacy PowerShell version 2 is detected.
- **ATT&CK Category:** Execution, Defense Evasion

- **ATT&CK Tag:** Command and Scripting Interpreter, PowerShell, Downgrade Attack
- **ATT&CK ID:** T1059, T1059.001, T1562.010
- **Minimum Log Source Requirement:** Windows, PowerShell
- **Query:**

```
norm_id=WinServer event_source="Powershell" event_id IN [400, 403, 600] host_version=
↪ "2.0" OR engine_version="2.0"
```

2.381 LP_Process Dump via Comsvcs DLL Detected

- **Trigger Condition:** Process memory dump via *comsvcs.dll* and *rundll32* is detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** OS Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 (image="*\rundll32.exe" OR file="RUNDLL32.EXE
↪ ") command IN ["*comsvcs*MiniDump*full*", "*comsvcs*MiniDumpW*full*"] -user IN [
↪ EXCLUDED_USERS
```

2.382 LP_Process Dump via Rundll32 and Comsvcs Detected

- **Trigger Condition:** Process memory dump performed via ordinal function 24 in *comsvcs.dll* is detected.
- **ATT&CK Category:** Defense Evasion, Credential Access
- **ATT&CK Tag:** Masquerading, OS Credential Dumping, LSASS Memory
- **ATT&CK ID:** T1036, T1003, T1003.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 command IN ["*comsvcs.dll, #24*", "*comsvcs.dll,
↳ MiniDump*"] -user IN EXCLUDED_USERS
```

2.383 LP_Process Hollowing Detected

- **Trigger Condition:** Adversaries attempts to inject malicious code into suspended and hollowed processes to evade process-based defenses.
- **ATT&CK Category:** Defense Evasion, Privilege Escalation
- **ATT&CK Tag:** Process Injection, Process Hollowing
- **ATT&CK ID:** T1055, T1055.012
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 (image="*smss.exe" parent_command!="*smss.
↳ exe") or (image="*csrss.exe" (parent_command!="*smss.exe" and parent_command!=
↳ "*svchost.exe")) or (image="*wininit.exe" parent_command!="*smss.exe") or (image=
↳ "*winlogon.exe" parent_command!="*smss.exe") or (image="*lsass.exe" parent_
↳ command!="*wininit.exe") or (image="*LogonUI.exe" (parent_command!="*winlogon.
↳ exe" and parent_command!="*wininit.exe")) or (image="*services.exe" parent_
↳ command!="*wininit.exe") or (image="*spoolsv.exe" parent_command!="*services.exe
↳ ") or (image="*taskhost.exe" (parent_command!="*services.exe" and parent_command!
↳ ="*svchost.exe")) or (image="*taskhostw.exe" (parent_command!="*services.exe" and
↳ parent_command!="*svchost.exe")) or (image="*userinit.exe" (parent_command!=
↳ "*dwm.exe" and parent_command!="*winlogon.exe")) -user IN EXCLUDED_USERS
```

2.384 LP_Process Injection Detected

- **Trigger Condition:** Adversaries injects code into processes to evade process-based defenses and possibly elevate privileges using commands like Invoke-DllInjection.
- **ATT&CK Category:** Defense Evasion, Privilege Escalation
- **ATT&CK Tag:** Process Injection
- **ATT&CK ID:** T1055
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 (command="*Invoke-DllInjection*" or command=
↪ "*C:\windows\syste\native\*" ) -user IN EXCLUDED_USERS
```

2.385 LP_Protected Storage Service Access Detected

- **Trigger Condition:** An access to a *protected_storage* service over the network is detected. The potential abuse of DPAPI to extract domain backup keys from Domain Controllers.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Remote Services
- **ATT&CK ID:** T1021
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=5145 share_name="*IPC*" relative_target="protected_
↪ storage" -user IN EXCLUDED_USERS
```

2.386 LP_PsExec Tool Execution Detected

- **Trigger Condition:** PsExec service installation and execution event (Service and Sysmon) is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** System Services, Service Execution
- **ATT&CK ID:** T1569, T1569.002
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
((norm_id=WinServer service="PSEXESVC" event_id IN [7045, 7036]) OR (norm_
↪ id=WindowsSysmon event_id=1 "process"="*\PSEXESVC.exe" user="*SYSTEM*")) -
↪ user IN EXCLUDED_USERS
```

2.387 LP_Psr Capture Screenshots Detected

- **Trigger Condition:** The psr utility adversaries use to take screen captures of the desktop to gather information throughout an operation is detected. The `psr.exe` utility is a legitimate Windows application that captures desktop screenshots.
- **ATT&CK Category:** Collection
- **ATT&CK Tag:** Screen Capture
- **ATT&CK ID:** T1113
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*\Psr.exe" command="*/start*" -user IN EXCLUDED_USERS
```

2.388 LP_Pulse Secure Arbitrary File Reading Detected

- **Trigger Condition:** The exploitation of arbitrary file reading vulnerability (CVE-2019-11510) in Pulse Secure is detected.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** External Remote Services
- **ATT&CK ID:** T1113
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

```
norm_id=* url IN ['*dana*guacamole*', '*lmbd*data.mdb*', '*data*mtmp/system*']
```

2.389 LP_Query Registry Network

- **Trigger Condition:** Adversaries uses `reg.exe` component for network connection and interact with the Windows Registry to gather information about the system, configuration, and installed software.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Query Registry

- **ATT&CK ID:** T1012
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=3 image="*reg.exe" command="*reg query*" -user
↪ IN EXCLUDED_USERS
```

2.390 LP_Rare Scheduled Task Creations Detected

- **Trigger Condition:** Rare scheduled task creations are detected. A software gets installed on multiple systems. The aggregation and count function selects tasks with rare names.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Scheduled Task/Job, Scheduled Task
- **ATT&CK ID:** T1053, T1053.005
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id="106" | chart count() as val by task | search val < 5
```

2.391 LP_RDP Login from Localhost Detected

- **Trigger Condition:** RDP login with a localhost source address that may be a tunneled login is detected.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Remote Services, Remote Desktop Protocol
- **ATT&CK ID:** T1021, T1021.001
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4624 logon_type="10" source_address IN ["::1", "127.0.0.1
↪ "] -user IN EXCLUDED_USERS
```

2.392 LP_RDP Over Reverse SSH Tunnel Detected

- **Trigger Condition:** *svchost* hosting RDP *termsvcs* communicating with the loopback address and on TCP port 3389 is detected.
- **ATT&CK Category:** Lateral Movement, Command and Control
- **ATT&CK Tag:** Remote Services, Remote Desktop Protocol, Protocol Tunneling
- **ATT&CK ID:** T1021, T1021.001, T1572
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=3 "process"="*\svchost.exe" is_initiated="true"
↪source_port="3389" destination_address IN ["127.*", "::1"] -user IN EXCLUDED_USERS
```

2.393 LP_RDP Registry Modification

- **Trigger Condition:** Potential malicious modification of the property value of *fDenyTS Connections* and *UserAuthentication* to enable remote desktop connections is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Modify Registry
- **ATT&CK ID:** T1112
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=13 target_object IN [
↪"*\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\UserAuthentication
↪", "\CurrentControlSet\Control\Terminal Server\fDenyTSConnections"] details=
↪"DWORD (0x00000000)" -user IN EXCLUDED_USERS
```

2.394 LP_RDP Sensitive Settings Changed

- **Trigger Condition:** Changes registry keys related to RDP terminal service are detected.
- **ATT&CK Category:** Defense Evasion

- **ATT&CK Tag:** Modify Registry
- **ATT&CK ID:** T1112
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=13 target_object IN [
  ↳ "*\services\TermService\Parameters\ServiceDll*", "*\Control\Terminal
  ↳ Server\SingleSessionPerUser*", "*\Control\Terminal Server\DenyTSConnections*" ] -
  ↳ user IN EXCLUDED_USERS
```

2.395 LP_Reconnaissance Activity with Net Command

- **Trigger Condition:** A set of commands often used in recon stages by different attack groups to discover the victim's information, systems, or network are detected.
- **ATT&CK Category:** Discovery, Reconnaissance
- **ATT&CK Tag:** Account Discovery, System Information Discovery, Gather Victim Host Information, Gather Victim Identity Information
- **ATT&CK ID:** T1087, T1082, T1589, T1592
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 command IN ["tasklist", "net time", "systeminfo",
  ↳ "whoami", "nbtstat", "net start", "*\net1 start", "qprocess", "nslookup", "hostname.exe
  ↳ ", "*\net1 user /domain", "*\net1 group /domain", "*\net1 group *domain admins* /
  ↳ domain", "*\net1 group *Exchange Trusted Subsystem* /domain", "*\net1 accounts /
  ↳ domain", "*\net1 user net localgroup administrators", "netstat -an"]
  ↳ -user IN EXCLUDED_USERS | chart count() as val by command | search val > 4
```

2.396 LP_RedSocks Backdoor Connection

- **Trigger Condition:** A backdoor event is detected. Adversaries develops malware and malware components as backdoors, which are used during targeting.
- **ATT&CK Category:** Resource Development
- **ATT&CK Tag:** Develop Capabilities, Malware

- **ATT&CK ID:** T1587, T1587.001
- **Minimum Log Source Requirement:** Redsocks
- **Query:**

```
norm_id=RedSocks description="*backdoor*" | process geoip(destination_address) as?
↪ country
```

2.397 LP_RedSocks Bad Neighborhood Detection

- **Trigger Condition:** A bad neighborhood is detected where adversaries use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a Command and Control server to avoid direct connections to their infrastructure.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Proxy
- **ATT&CK ID:** T1090
- **Minimum Log Source Requirement:** Redsocks
- **Query:**

```
norm_id=RedSocks category="bad hood" | process geoip(destination_address) as? country
```

2.398 LP_RedSocks Blacklist URL Detection

- **Trigger Condition:** Blacklist URLs are detected.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Redsocks
- **Query:**

```
norm_id=RedSocks category="URL blacklist" | process geoip(destination_address) as?
↪ country
```

2.399 LP_RedSocks FileSharing

- **Trigger Condition:** Filesharing using an alternate platform like 4Shared, FileHippo, Torrent, Picofile, or WeTransfer is detected.
- **ATT&CK Category:** Exfiltration
- **ATT&CK Tag:** Exfiltration over Alternative Protocol
- **ATT&CK ID:** T1048
- **Minimum Log Source Requirement:** Redsocks
- **Query:**

```
norm_id=RedSocks category="Filesharing" description in ["*4share*", "*torrent*",
↪ "*FileHippo*", "*picofile*", "*wetransfer*"] | process geoip(destination_address) as?
↪ country
```

2.400 LP_RedSocks Ransomware Connection

- **Trigger Condition:** A ransomware event is detected.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Disk Wipe, Disk Content Wipe, Data Encrypted for Impact, Data Destruction, Proxy
- **ATT&CK ID:** T1561, T1561.001, T1486, T1485, T1090
- **Minimum Log Source Requirement:** Redsocks
- **Query:**

```
norm_id=RedSocks description="*ransomware*" | process geoip(destination_address) as?
↪ country
```

2.401 LP_RedSocks Sinkhole Detection

- **Trigger Condition:** Sinkhole is detected.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** -

- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Redsocks
- **Query:**

```
norm_id=RedSocks category="Sinkhole" | process geoip(destination_address) as country
```

2.402 LP_RedSocks Tor Connection

- **Trigger Condition:** A Tor connection is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Proxy
- **ATT&CK ID:** T1090
- **Minimum Log Source Requirement:** Redsocks
- **Query:**

```
norm_id=RedSocks category="tor" | process geoip(destination_address) as country
```

2.403 LP_RedSocks Trojan Connection

- **Trigger Condition:** A trojan event is detected.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Redsocks
- **Query:**

```
norm_id=RedSocks description="*trojan*" | process geoip(destination_address) as country
```

2.404 LP_Register new Logon Process by Rubeus

- **Trigger Condition:** Potential use of Rubeus via registered new trusted logon process is detected. Adversaries abuses a valid Kerberos ticket-granting ticket (TGT) or sniff network traffic to obtain a ticket-granting service (TGS) ticket that may be vulnerable to Brute Force.
- **ATT&CK Category:** Lateral Movement, Privilege Escalation
- **ATT&CK Tag:** Steal or Forge Kerberos Tickets, Kerberoasting
- **ATT&CK ID:** T1558, T1558.003
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4611 logon_process="User32LogonProcess" -user IN EXCLUDED_USERS
```

2.405 LP_Registry Persistence Mechanisms Detected

- **Trigger Condition:** Persistence registry keys at the current version folder for registry keys are detected. Adversaries establish persistence and/or elevate privileges by executing malicious content triggered by Image File Execution Options (IFEO) debuggers.
- **ATT&CK Category:** Privilege Escalation, Persistence
- **ATT&CK Tag:** Event Triggered Execution, Image File Execution Options Injection
- **ATT&CK ID:** T1546, T1546.012
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
event_id=13 target_object IN ["*\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\*\\GlobalFlag",
"*\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\SilentProcessExit\\*\\ReportingMode",
"*\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\SilentProcessExit\\*\\MonitorProcess"] event_type="SetValue" -user IN EXCLUDED_USERS
```

2.406 LP_Regsvcs-Regasm Detected

- **Trigger Condition:** Adversaries abuses trusted Windows command line utilities *regsvcs* and *regasm* for proxy execution of code.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Signed Binary Proxy Execution, Regsvcs/Regasm
- **ATT&CK ID:** T1218, T1218.009
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=3 (image="*regsvcs.exe" or image="*regasm.exe")
```

2.407 LP_Remote PowerShell Session

- **Trigger Condition:** Remote PowerShell sessions on endpoints are detected. Powershell allows functionality to execute code on a remote system without using RDP.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, PowerShell
- **ATT&CK ID:** T1059, T1059.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
(norm_id=WinServer event_id IN ["4103", "400"] execution_host="ServerRemoteHost" host_
↪ application="*wsmprovhost.exe*")OR (label="Process" label=Create ("process"=
↪ "*wsmprovhost.exe" OR parent_process="*\wsmprovhost.exe"))
```

2.408 LP_Remote System Discovery

- **Trigger Condition:** The components like *net.exe* and *ping.exe* are used to list other systems by IP address, hostname, or other logical identifiers on a network used for Lateral Movement from the current system.
- **ATT&CK Category:** Discovery

- **ATT&CK Tag:** Remote System Discovery
- **ATT&CK ID:** T1018
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon (image="*net.exe" or image="*ping.exe") (command="*view*"
↪ " or command="*ping*") -user IN EXCLUDED_USERS
```

2.409 LP_Renamed Binary Detected

- **Trigger Condition:** The execution of a renamed binary is detected. Renamed binaries are executable files disguised in a different name or file extension to evade detection by security measures.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Rename System Utilities
- **ATT&CK ID:** T1036.003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label="Process" label=Create (application = "Sysinternals PsExec" OR description IN
["Windows PowerShell*", "pwsh*", "Execute processes remotely"] OR file IN
["powershell.exe", "pwsh.dll", "powershell_ise.exe", "psexec.exe", "psexec.c", "psexesvc.
↪ exe", "cscript.exe", "wscript.exe",
"mshta.exe", "regsvr32.exe", "wmic.exe", "certutil.exe", "rundll32.exe", "cmstp.exe",
↪ "msiexec.exe", "reg.exe"])
- "process" IN ["*\powershell.exe", ".*\pwsh.exe", ".*\powershell_ise.exe", ".*\psexec.exe",
↪ ".*\psexec64.exe", ".*\PSEXESVC.exe", ".*\cscript.exe", ".*\wscript.exe", ".*\mshta.exe",
↪ ".*\regsvr32.exe", ".*\wmic.exe", ".*\certutil.exe", ".*\rundll32.exe", ".*\cmstp.exe",
↪ ".*\msiexec.exe", ".*\reg.exe"]) -user IN EXCLUDED_USERS
```

2.410 LP_Renamed PsExec Detected

- **Trigger Condition:** Execution of a renamed PsExec used by attackers or malware.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Masquerading

- **ATT&CK ID:** T1036
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon message="Execute processes remotely" product=
↪ "Sysinternals PsExec" -image IN ["*\PsExec.exe", "*\PsExec64.exe"]
```

2.411 LP_Rogue Access Point Detected

- **Trigger Condition:** Rouge access point is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Exploitation for Defense Evasion, Exploitation for Defense Evasion, Software Discovery, Security Software Discovery
- **ATT&CK ID:** T1211, T1211, T1518, T1518.001
- **Minimum Log Source Requirement:** Firewall, IDS/IPS (ArubaOS, Cisco Controller)
- **Query:**

```
label=Accesspoint label=Rogue -label=Clear access_point=*
```

2.412 LP_RSA SecurID Account Lockout

- **Trigger Condition:** User's account is locked after entering the wrong passcode multiple times in a row.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Brute Force
- **ATT&CK ID:** T1110
- **Minimum Log Source Requirement:** RSA Secure ID
- **Query:**

```
norm_id=RSA_SecurID type=Runtime action=AUTHN_LOCKOUT_EVENT
```

2.413 LP_RSA SecurID Account Lockout

- **Trigger Condition:** User's account is locked after entering the wrong passcode multiple times in a row.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Brute Force
- **ATT&CK ID:** T1110
- **Minimum Log Source Requirement:** RSA Secure ID
- **Query:**

```
norm_id=RSA_SecurID type=Runtime action=AUTHN_LOCKOUT_EVENT
```

2.414 LP_Rubeus Hack Tool Detected

- **Trigger Condition:** The Command line parameters like asreproast, dump, impersonate user, harvest and other commands used by the Rubeus hack tool are detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** OS Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label="Process" label=Create command IN ["* asreproast *", "* dump /service:krbtgt *",  
→ "* kerberoast *", "* createnetenonly /program:*", "* ptt /ticket:*", "* /impersonateuser:*",  
→ "* renew /ticket:*", "* asktgt /user:*", "* harvest /interval:*"] -user IN EXCLUDED_USERS
```

2.415 LP_Run PowerShell Script from ADS Detected

- **Trigger Condition:** PowerShell script execution from Alternate Data Stream (ADS) is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Hide Artifacts, NTFS File Attributes

- **ATT&CK ID:** T1564, T1564.004
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create parent_process IN ["*\powershell.exe", ".*\pwsh.exe"]
↪ "process" IN ["*\powershell.exe", ".*\pwsh.exe"] command="*Get-Content*"
↪ command="*Stream*" -user IN EXCLUDED_USERS
```

2.416 LP_Rundll32 Internet Connection Detected

- **Trigger Condition:** A rundll32 that communicates with public IP addresses is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Rundll32
- **ATT&CK ID:** T1218.011
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=3 "process"="*\rundll32.exe" is_initiated="true" -
↪ (((destination_address IN HOMENET) OR destination_address IN ["127.*", "20.*", "51.
↪ 103.*", "51.104.*", "51.105.*"] OR (command="*PcaSvc.dll,PcaPatchSdbTask*" OR
↪ source_host="*.internal.cloudapp.net"))) OR (parent_process=
↪ "C:\Windows\System32\svchost.exe" destination_port="443")) -user IN EXCLUDED_
↪ USERS
```

2.417 LP_Scheduled Task Creation Detected

- **Trigger Condition:** The creation of scheduled task is detected. Schtasks is a windows internal binary that allows us to schedule tasks.
- **ATT&CK Category:** Execution, Persistence, Privilege Escalation
- **ATT&CK Tag:** Scheduled Task/Job, Scheduled Task
- **ATT&CK ID:** T1053, T1053.005
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
(label="Process" label=Create "process"="*\schtasks.exe" command="* /create *" -user
↪ IN EXCLUDED_USERS) OR (label="Registry" label="Key" label="Map" "target_object
↪ "="*\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\*" -
↪ target_object IN ["*\SOFTWARE\Microsoft\Windows
↪ NT\CurrentVersion\Schedule\TaskCache\Tree\Microsoft\Windows\UpdateOrchestrator*
↪ "] event_type=CreateKey) OR (norm_id=WinServer event_id=4698 (-command IN [
↪ "*MpCmdRun.exe", "*msfeedssync.exe", "*usoclient.exe"] OR (-task=
↪ "\CreateExplorerShellUnelevatedTask" command="*explorer.exe"))))
```

2.418 LP_SCM Database Handle Failure Detected

- **Trigger Condition:** Non-system user fails to get a handle of the SCM database.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Endpoint Denial of Service
- **ATT&CK ID:** T1499
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4656 object_type="SC_MANAGER OBJECT" object_name=
↪ "servicesactive" event_type="Audit Failure" logon_id="0x3e4" -user IN EXCLUDED_
↪ USERS
```

2.419 LP_SCM Database Privileged Operation Detected

- **Trigger Condition:** Non-system user performs privileged operation on the SCM database.
- **ATT&CK Category:** Privilege Escalation
- **ATT&CK Tag:** Abuse Elevation Control Mechanism, Bypass User Account Control
- **ATT&CK ID:** T1548, T1548.002
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4674 object_type="SC_MANAGER OBJECT" object_name=
↪ "servicesactive" privilege="SeTakeOwnershipPrivilege" logon_id="0x3e4" -user IN
↪ EXCLUDED_USERS
```

2.420 LP_Screensaver Activities Detected

- **Trigger Condition:** Screensaver registry key modified via *rundll32.exe* is detected.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Screensaver
- **ATT&CK ID:** T1546.002
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
norm_id=WindowsSysmon (event_id=12 or event_id=13 or event_id=14) (target_object=
↪ "*\Control Panel\Desktop\SCRNSAVE.exe") (parent_command!="*explorer.exe" or
↪ image!="*rundll32.exe" or command!="*shell32.dll, Control_RunDLL desk.cpl,
↪ ScreenSaver, *") -user IN EXCLUDED_USERS
```

2.421 LP_Secure Deletion with SDelete

- **Trigger Condition:** Logpoint detects renaming of a file during deletion using SDelete tool.
- **ATT&CK Category:** Defense Evasion, Impact
- **ATT&CK Tag:** Indicator Removal on Host, File Deletion, Obfuscated Files or Information, Indicator Removal from Tools, Data Destruction, Subvert Trust Controls, Code Signing
- **ATT&CK ID:** T1070, T1070.004, T1027, T1027.005, T1485, T1553, T1553.002
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id IN ["4656", "4663", "4658"] object_name IN ["*.AAA", "*.ZZZ
↪ "] -user IN EXCLUDED_USERS
```

2.422 LP_SecurityXploded Tool Detected

- **Trigger Condition:** Execution of the SecurityXploded tools is detected.
- **ATT&CK Category:** Credential Access

- **ATT&CK Tag:** Credentials from Password Stores
- **ATT&CK ID:** T1555
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create (vendor="SecurityXploded" OR "process"=
↪ "*PasswordDump.exe" OR file="*PasswordDump.exe") -user IN EXCLUDED_USERS
```

2.423 LP_smbexec Service Installation Detected

- **Trigger Condition:** smbexec.py tool is detected by identifying a specific service installation.
- **ATT&CK Category:** Lateral Movement, Execution
- **ATT&CK Tag:** Remote Services, System Services, Service Execution
- **ATT&CK ID:** T1021, T1569, T1569.002
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=7045 service="BTOBTO" service="*\execute.bat" -user IN
↪ EXCLUDED_USERS
```

2.424 LP_SolarisLDAP Group Remove from LDAP Detected

- **Trigger Condition:** The removal of a group from LDAP is detected.
- **ATT&CK Category:** Credential Access, Persistence, Impact, Defense Evasion
- **ATT&CK Tag:** Account Manipulation, Account Access Removal
- **ATT&CK ID:** T1098, T1531
- **Minimum Log Source Requirement:** Solaris LDAP
- **Query:**

```
norm_id=SolarisLDAP label=Remove label=Member label=Management label=Group
```

2.425 LP_SolarisLDAP Password Spraying Attack Detected

- **Trigger Condition:** Multiple login or authentication fail attempts on a SOLARISLDAP by various users are detected. Adversaries can use a list of commonly used passwords against different accounts to attempt to obtain valid account credentials.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Solaris LDAP
- **Query:**

```
norm_id=SolarisLDAP label=User (label=Login OR label=Authentication) label=Fail | chart↵
↵distinct_count(user) as UserCount, distinct_list(user) as Users | search UserCount > 5
```

2.426 LP_SolarisLDAP Possible Bruteforce Attack Detected

- **Trigger Condition:** Five failed Solaris LDAP user login or authentication attempts from a user are detected. Adversaries can perform brute force attacks to find the valid credentials of a user. The fail count number needs to be adjusted to the environment.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Brute Force
- **ATT&CK ID:** T1110
- **Minimum Log Source Requirement:** Solaris LDAP
- **Query:**

```
norm_id=SolarisLDAP label=User (label=Login OR label=Authentication) label=Fail | chart
↪ count() as cnt by user | search cnt > 5
```

2.427 LP_SolarisLDAP Successful Bruteforce Attack Detected

- **Trigger Condition:** Successful login event after multiple failed login counts is detected as defined in the query. Adversaries perform brute-force attacks to discover and validate credentials and gain access to the system and network. The fail count needs to be adjusted according to the environment.
- **ATT&CK Category:** Initial Access, Persistence, Privilege Escalation, Defense Evasion, Credential Access
- **ATT&CK Tag:** Valid Accounts, Account Manipulation, Brute Force, Forced Authentication
- **ATT&CK ID:** T1078, T1098, T1110, T1187
- **Minimum Log Source Requirement:** Solaris LDAP
- **Query:**

```
[norm_id=SolarisLDAP label=User (label=Login OR label=Authentication) label=Fail |
↪ chart count() as cnt by user | search cnt > 10 ] as s1 followed by [norm_id=SolarisLDAP
↪ label=User (label=Login OR label=Authentication) label=Successful] as s2 on s1.user =
↪ s2.user
```

2.428 LP_SolarisLDAP User Account Lockout Detected

- **Trigger Condition:** A locked user account is detected.
- **ATT&CK Category:** Defense Evasion, Persistence, Privilege Escalation, Initial Access
- **ATT&CK Tag:** Valid Accounts, Abuse Elevation Control Mechanism, Bypass User Access Control
- **ATT&CK ID:** T1078, T1548
- **Minimum Log Source Requirement:** Solaris LDAP
- **Query:**

```
norm_id=SolarisLDAP label=User label=Account label=Lock
```

2.429 LP_Sophos XG Firewall - Inbound Attack Detected by IDP

- **Trigger Condition:** An inbound attack defined in IDP policy is detected.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Network Denial of Service, Endpoint Denial of Service
- **ATT&CK ID:** T1498, T1499
- **Minimum Log Source Requirement:** Sophos XG Firewall
- **Query:**

```
norm_id=SophosXGFirewall label=Attack label=Detect label=IDP destination_address=* -
↪source_address in HOMENET | process geoip(source_address) as country
```

2.430 LP_Sophos XG Firewall - Outbound Attack Detected by IDP

- **Trigger Condition:** An outbound attack defined in IDP policy is detected.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Network Denial of Service, Endpoint Denial of Service
- **ATT&CK ID:** T1498, T1499
- **Minimum Log Source Requirement:** Sophos XG Firewall
- **Query:**

```
norm_id=SophosXGFirewall label=Attack label=Detect label=IDP destination_address=* -
↪destination_address in HOMENET | process geoip(destination_address) as country
```

2.431 LP_SophosUTM Policy Violation

- **Trigger Condition:** Different policy violation from a source is detected. For this alert to work, the following list must be updated;
 - EXTREMIST _CONTENT, for example, weapons.
 - CONCERNED _CONTENT, for example, alcohol, tobacco, gambling, and so on.
 - CRIMINAL _CONTENT, for example, hacking, drugs, and so on.
 - VULNERABLE _CONTENT, for example, abuse, and so on.
- **ATT&CK Category:** Defense Evasion, Privilege Escalation, Credential Access
- **ATT&CK Tag:** Abuse Elevation Control Mechanism, Bypass User Access Control, Group Policy Modification, Exploitation for Credential Access, Exploitation for Privilege Escalation
- **ATT&CK ID:** T1548, T1484, T1212, T1068
- **Minimum Log Source Requirement:** Sophos UTM
- **Query:**

```
norm_id=SophosUTM category_name=* source_address=* | chart count(category_name
↪ IN EXTREMIST_CONTENT) as Extremist, count(category_name IN CONCERNED_
↪ CONTENT) as Concerning, count(category_name IN CRIMINAL_CONTENT) as Criminal,
↪ count(category_name IN VULNERABLE_CONTENT) as Vulnerable by source_address,
↪ user | chart sum(Extremist+Concerning+Criminal+Vulnerable) as Violation by Extremist,
↪ Concerning, Criminal, Vulnerable, source_address,
user order by Violation | search Violation>1
```

2.432 LP_SSHD Connection Denied

- **Trigger Condition:** Ten denied connections are detected from the same source.
- **ATT&CK Category:** Lateral Movement, Command and Control, Impact
- **ATT&CK Tag:** Remote Services, Commonly Used Port, Network Denial of Service, Endpoint Denial of Service
- **ATT&CK ID:** T1021, T1498, T1499
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

```
[10 norm_id=Unix label=Connection label=Deny having same source_address within 10↵
↵seconds]
```

2.433 LP_Stealthy Scheduled Task Creation via VBA Macro Detected

- **Trigger Condition:** Office products such as Word, Excel, PowerPoint and Outlook.exe load *taskschd.dll* is detected.
- **ATT&CK Category:** Execution, Persistence, Privilege Escalation
- **ATT&CK Tag:** Scheduled Task/Job, Scheduled Task
- **ATT&CK ID:** T1053, T1053.005
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=7 image="*\taskschd.dll" "process" IN ["*\winword.
↵exe", " *\excel.exe", " *\powerpnt.exe", " *\outlook.exe"] -user IN EXCLUDED_USERS
```

2.434 LP_Sticky Key Like Backdoor Usage Detected

- **Trigger Condition:** The use and installation of a backdoor that uses an option to register a malicious debugger for built-in tools that are accessible on the login screen. Sticky keys are a Windows accessibility feature that allows a user to press a modifier key (For example, Shift, Ctrl, Alt) and remain active until another key is pressed. Adversaries may use a sticky key-like backdoor to gain unauthorized access to a system by pressing a specific combination of keys. This can allow them to execute malicious code or bypass security controls.
- **ATT&CK Category:** Privilege Escalation, Persistence
- **ATT&CK Tag:** Event Triggered Execution, Accessibility Features
- **ATT&CK ID:** T1546, T1546.008
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
(norm_id=WindowsSysmon event_id=13 target_object IN [
  ↳ "*\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution
  ↳ Options\\*\\Debugger"] event_type="SetValue") OR (label="Process" label=Create
  ↳ parent_process="*\\winlogon.exe" command IN ["*cmd.exe sethc.exe *", "*cmd.exe
  ↳ utilman.exe *", "*cmd.exe osk.exe *", "*cmd.exe Magnify.exe *", "*cmd.exe Narrator.
  ↳ exe *", "*cmd.exe DisplaySwitch.exe *"])
```

2.435 LP_Stop Windows Service Detected

- **Trigger Condition:** Windows Service stops.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Service Stop
- **ATT&CK ID:** T1489
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 image IN ["*\\sc.exe", "*\\net.exe", "*\\net1.exe"]
↳ command= "*stop*" -user IN EXCLUDED_USERS
```

2.436 LP_Successful Lateral Movement to Administrator via Pass the Hash using Mimikatz Detected

- **Trigger Condition:** Lateral Movement is successful in compromising the admin account via Pass the Hash method.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Use Alternate Authentication Material, Pass the Hash
- **ATT&CK ID:** T1550, T1550.002
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
[norm_id=WinServer event_id=4624 logon_type=9 logon_process=seclogo
↪package=Negotiate label=User label=Login label=Successful -user IN EXCLUDED_
↪USERS] as s1
followed by [norm_id=WinServer event_id=4672 label=Privilege label=Assign] as s2 on s1.
↪user=s2.user | rename s1.log_ts
as log_ts, s1.user as user, s1.domain as domain, s1.user_id as user_id, s1.host as host
```

2.437 LP_Successful Overpass the Hash Attempt

- **Trigger Condition:** Successful logon with logon type 9 (NewCredentials), which matches the Overpass the Hash behavior of Mimikatz's sekurlsa::pth module is detected.
- **ATT&CK Category:** Lateral Movement, Defense Evasion
- **ATT&CK Tag:** T1550 - Use Alternate Authentication Material (2), T1550.002 - Pass the Hash (2)
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4624 logon_type="9" logon_process="seclogo" package=
↪"Negotiate" -user IN EXCLUDED_USERS
```

2.438 LP_Suspect Svchost Activity Detected

- **Trigger Condition:** A suspicious Svchost activity is detected. It is abnormal for svchost.exe to spawn without any CLI arguments and is observed when a malicious process spawns the process and injects code into the process memory space.
- **ATT&CK Category:** Defense Evasion, Privilege Escalation
- **ATT&CK Tag:** Process Injection
- **ATT&CK ID:** T1055
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 image="*svchost.exe" parent_image=* -parent_
↪image IN ["*rpcnet.exe", "*rpcnetp.exe", "*svchost.exe", "*Mrt.exe", "*MsMpEng.
↪exe"] command=* command="*svchost.exe" -user IN EXCLUDED_USERS
```

2.439 LP_Suspect Svchost Memory Access

- **Trigger Condition:** When access to svchost process memory such as that used by Invoke-Phantom to kill the winRM windows event logging service is detected. The "svchost.exe" process is a legitimate system that hosts multiple Windows services. However, adversaries may use this process to execute malicious code or gain unauthorized system access.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Impair Defenses, Disable or Modify Tools
- **ATT&CK ID:** T1562, T1562.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=10 image="*\windows\system32\svchost.exe"
↪access="0x1f3fff" call_trace="*unknown*" -user IN EXCLUDED_USERS
```

2.440 LP_Suspicious Access to Sensitive File Extensions

- **Trigger Condition:** Sensitive file extensions are detected.
- **ATT&CK Category:** Collection
- **ATT&CK Tag:** Data Staged
- **ATT&CK ID:** T1074
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=5145 relative_target IN ["*.pst", "*.ost", "*.msg", "*.nst", "*.
↪oab", "*.edb", "*.nsf",
"*.bak", "*.dmp", "*.kirbi", "*\groups.xml", "*.rdp"] -user IN EXCLUDED_USERS
```

2.441 LP_Suspicious Calculator Usage Detected

- **Trigger Condition:** The use of calc.exe with command line parameters or in a suspicious directory, which is likely caused by some PoC or detection evasion, is detected.

- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Masquerading
- **ATT&CK ID:** T1036
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 (command="*\calc.exe *" OR (event_id=1 image=
↪ "\calc.exe" -image="*\Windows\Sys*")) -user IN EXCLUDED_USERS
```

2.442 LP_Suspicious Call by Ordinal Detected

- **Trigger Condition:** When suspicious calls of DLLs through RUNDLL32 via ordinal. This search looks for executing scripts with rundll32. Adversaries may abuse rundll32.exe to proxy the execution of malicious code. Using rundll32.exe, vice executing directly, may avoid triggering security tools that may not monitor the execution of the rundll32.exe process because of allowlists or false positives from normal operations.
- **ATT&CK Category:** Defense Evasion, Execution
- **ATT&CK Tag:** Signed Binary Proxy Execution, Rundll32
- **ATT&CK ID:** T1218, T1218.011
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WinServer event_id=4688 "process"="*\rundll32.exe" command IN ["*,#*", "*",
↪ #*", "*.dll #*", "*.ocx #*"] -command IN ["*EDGEHTML.DLL*", "*#141*"] -user IN
↪ EXCLUDED_USERS
```

2.443 LP_Suspicious Code Page Switch Detected

- **Trigger Condition:** Code page switch in a command line or batch scripts to a rare language is detected.
- **ATT&CK Category:** Defense Evasion, Discovery
- **ATT&CK Tag:** Masquerading, System Language Discovery

- **ATT&CK ID:** T1036, T1614.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*\chcp.com" command IN ["* 936", "* 1258"] -
↪ user IN EXCLUDED_USERS
```

2.444 LP_Suspicious Commandline Escape Detected

- **Trigger Condition:** Suspicious processes that use escape characters are detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Deobfuscate/Decode Files or Information
- **ATT&CK ID:** T1140
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label=create label="process" command IN ["*h^t^t^p*", "*h\t\t\p*"]
```

2.445 LP_Suspicious Compression Tool Parameters

- **Trigger Condition:** Suspicious command line arguments of common data compression tools, such as 7z and Rar are detected.
- **ATT&CK Category:** Collection, Exfiltration
- **ATT&CK Tag:** Automated Exfiltration, Archive Collected Data
- **ATT&CK ID:** T1020, T1560
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create ((file IN ["7z*.exe", "*.rar.exe", "*Command*Line*RAR*"]
↪ OR "process" IN ["*\7z*.exe", "*\rar.exe"]) command IN ["* -p*", "* -ta*", "* -tb*", "* -
↪ sdel*", "* -dw*", "* -hp*"]) OR (((("process"="*/powershell.exe" OR file="powershell.exe
↪ ") command="*-Recurse Compress-Archive*") OR ((("process"="*/rar.exe" OR file IN [
↪ "*rar.exe", "*Command*Line*RAR*"]) command="*rar* a*") -parent_process=
↪ "C:\Program*")
```

2.446 LP_Suspicious Control Panel DLL Load Detected

- **Trigger Condition:** Execution of a suspicious Signed Binary Proxy Execution or Rundll32 from *control.exe* used by Equation Group and Exploit Kits is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Rundll32
- **ATT&CK ID:** T1218.011
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create parent_process="*\System32\control.exe" command=
↳ "\rundll32.exe *" -command="*Shell32.dll*
```

2.447 LP_Suspicious Csc Source File Folder Detected

- **Trigger Condition:** Execution of *csc.exe* that uses a source in a suspicious folder is detected. For example, AppData.
- **ATT&CK Category:** Execution, Defense Evasion
- **ATT&CK Tag:** Obfuscated Files or Information, Compile After Delivery, User Execution, Native API
- **ATT&CK ID:** T1027, T1027.004, T1204, T1106
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create "process"="*\csc.exe" command IN ["*\AppData\*",
↳ "\Windows\Temp\*"] -(parent_process="*\Program Files*" OR parent_process in [
↳ "\sdiagnhost.exe", "\w3wp.exe", "\choco.exe"]) OR parent_command=
↳ "\ProgramData\Microsoft\Windows Defender Advanced Threat Protection*") -user IN
↳ EXCLUDED_USERS
```

2.448 LP_Suspicious Debugger Registration Detected

- **Trigger Condition:** Registration of a debugger for a program available in the logon screen (sticky key backdoor) is detected.
- **ATT&CK Category:** Persistence, Privilege Escalation
- **ATT&CK Tag:** Event Triggered Execution, Accessibility Features
- **ATT&CK ID:** T1546, T1546.008
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create command IN ["*\CurrentVersion\Image File Execution↗
↪Options\sethc.exe*", " *\CurrentVersion\Image File Execution Options\utilman.exe*",
↪ " *\CurrentVersion\Image File Execution Options\osk.exe*", " *\CurrentVersion\Image↗
↪File Execution Options\magnify.exe*", " *\CurrentVersion\Image File Execution↗
↪Options\narrator.exe*", " *\CurrentVersion\Image File Execution Options\displayswitch.
↪exe*", " *\CurrentVersion\Image File Execution Options\atbroker.exe*"]
```

2.449 LP_Suspicious Double Extension Detected

- **Trigger Condition:** Double extension of a file is detected. Adversaries use double extensions to mask the real file extension and evade detection by security software or bypass whitelisting.
- **ATT&CK Category:** Initial Access, Defense Evasion
- **ATT&CK Tag:** Double File Extension, Spearphishing Attachment, Masquerading
- **ATT&CK ID:** T1036.007, T1566.001, T1036
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create ("process" IN ["*.doc.exe", "*.docx.exe", "*.doc.lnk", "*.
↪docx.lnk", "*.xls.lnk", "xlsx.lnk", "*.ppt.lnk", "*.pptx.lnk", "*.rtf.lnk", "*.pdf.lnk", "*.txt.lnk
↪", "*.doc.js", "*.docx.js", "*.xls.js", "*.xlsx.js", "*.ppt.js", "*.pptx.js", "*.rtf.js", "*.pdf.js",
↪ "*.txt.js", "*.tmp.bat", "*.xls.exe", "*.bat.exe", "*.xlsx.exe", "*.ppt.exe", "*.pptx.exe", "*.
↪rtf.exe", "*.pdf.exe", "*.bat.exe", "*.txt.exe", "*.exe", "*_____.exe"] OR command IN [
↪ "*.doc.exe*", "*.docx.exe*", "*.doc.lnk*", "*.docx.lnk*", "*.xls.lnk*", "*.xlsx.lnk*", "*.ppt.
↪lnk*", "*.pptx.lnk*", "*.rtf.lnk*", "*.pdf.lnk*", "*.txt.lnk*", "*.doc.js*", "*.docx.js*", "*.xls.
↪js*", "*.xlsx.js*", "*.ppt.js*", "*.pptx.js*", "*.rtf.js*", "*.pdf.js*", "*.txt.js*", "*.tmp.bat*",
↪ "*.xls.exe*", "*.bat.exe*", "*.xlsx.exe*", "*.ppt.exe*", "*.pptx.exe*", "*.rtf.exe*", "*.pdf.
↪exe*", "*.bat.exe*", "*.txt.exe*", "*.exe*", "*_____.exe*"] ) (continues on next page)
```

(continued from previous page)

2.450 LP_Suspicious Driver Load from Temp

- **Trigger Condition:** Driver load from a temporary directory is detected.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** New Service
- **ATT&CK ID:** T1543
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=6 image="*\Temp\*" -user IN EXCLUDED_USERS
```

2.451 LP_Suspicious Eventlog Clear or Configuration Using Wevtutil Detected

- **Trigger Condition:** Clearing or configuration of eventlogs using wevtutil, PowerShell and wmic is detected. It is used by ransomware during the attack as seen by NotPetya and others.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Indicator Removal on Host
- **ATT&CK ID:** T1070
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label="Process" label=Create (((("process" IN ["*\powershell.exe", "*\pwsh.exe"]  
↪ command IN ["*Clear-EventLog*", "*Remove-EventLog*", "*Limit-EventLog*", "*Clear-  
↪ WinEvent*"]) OR ("process"="*\wmic.exe" command="* ClearEventLog *")) OR (  
↪ "process"="*\wevtutil.exe" command IN ["*clear-log*", "*cl *", "*set-log*", "*sl *"]))) -  
↪ user IN EXCLUDED_USERS
```

2.452 LP_Suspicious Execution from Outlook

- **Trigger Condition:** *EnableUnsafeClient MailRules* used for Script Execution from Outlook is detected.
- **ATT&CK Category:** Execution, Defense Evasion
- **ATT&CK Tag:** Command and Scripting Interpreter, Indirect Command Execution
- **ATT&CK ID:** T1059, T1202
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create (command="*EnableUnsafeClientMailRules*" OR (parent_
↪process="*\outlook.exe" command="\\*\*.exe")) -user IN EXCLUDED_USERS
```

2.453 LP_Suspicious GUP Usage Detected

- **Trigger Condition:** Execution of the Notepad++ updater in a suspicious directory used in DLL side-loading attacks is detected.
- **ATT&CK Category:** Defense Evasion, Persistence, Privilege Escalation
- **ATT&CK Tag:** Hijack Execution Flow, DLL Side-Loading
- **ATT&CK ID:** T1574, T1574.002
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*\GUP.exe" -(("process" IN ["*\Program
↪Files\Notepad++\updater\GUP.exe", "*\Program Files (x86)\Notepad++\updater\GUP.
↪exe"]) OR ("process"="*\Users\*" "process" IN [
↪"*\AppData\Local\Notepad++\updater\GUP.exe",
↪"*\AppData\Roaming\Notepad++\updater\GUP.exe"])))
```

2.454 LP_Suspicious HWP Sub Processes Detected

- **Trigger Condition:** Hangul Word Processor (Hanword) sub-processes that could indicate exploitation are detected.
- **ATT&CK Category:** Execution, Initial Access

- **ATT&CK Tag:** Windows Command Shell, Exploitation for Client Execution, Spearphishing Attachment
- **ATT&CK ID:** T1059.003, T1203, T1566.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create parent_process="*\Hwp.exe" "process"="*\gbb.exe" -
↪ user IN EXCLUDED_USERS
```

2.455 LP_Suspicious In-Memory Module Execution Detected

- **Trigger Condition:** An access to processes by other suspicious processes that have reflectively loaded libraries in their memory space are detected.
- **ATT&CK Category:** Privilege Escalation
- **ATT&CK Tag:** Process Injection
- **ATT&CK ID:** T1055
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=10 (call_trace IN ["C:\Windows\SYSTEM32\ntdll.dll+*"
↪ ", "C:\Windows\System32\KERNELBASE.dll+*", "*UNKNOWN(*)"] OR (call_trace=
↪ "*UNKNOWN*" access IN ["0x1F0FFF", "0x1F1FFF", "0x143A", "0x1410", "0x1010",
↪ "0x1F2FFF", "0x1F3FFF", "0x1FFFFF"])) -user IN EXCLUDED_USERS
```

2.456 LP_Suspicious Kerberos RC4 Ticket Encryption

- **Trigger Condition:** Service ticket requests using the RC4 encryption type are detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Steal or Forge Kerberos Tickets, Kerberoasting
- **ATT&CK ID:** T1558, T1558.003
- **Minimum Log Source Requirement:** Windows

- **Query:**

```
norm_id=WinServer event_id=4769 ticket_option="0x40810000" Encryption_type="0x17" -
↪ service="$*" -user IN EXCLUDED_USERS
```

2.457 LP_Suspicious MsiExec Directory Detected

- **Trigger Condition:** Suspicious *msiexec* process starting in an uncommon directory is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Masquerading
- **ATT&CK ID:** T1036
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*\msiexec.exe" -"process" IN [
↪ "C:\Windows\System32\*", "C:\Windows\SysWOW64\*", "C:\Windows\WinSxS\*"]
```

2.458 LP_Suspicious Named Pipes Detected

- **Trigger Condition:** Suspicious named pipes commonly used by threat actors are detected.
- **ATT&CK Category:** Defense Evasion, Privilege Escalation, Lateral Movement
- **ATT&CK Tag:** Process Injection, Lateral Tool Transfer
- **ATT&CK ID:** T1055, T1570
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id IN ["17", "18"] pipe IN ["\isapi_http", "\isapi_dg",
↪ "\isapi_dg2", "\sdlrpc", "\ahexec", "\winsession", "\lsassw",
↪ "\46a676ab7f179e511e30dd2dc41bd388", "\9f81f59bc58452127884ce513865ed20",
↪ "\e710f28d59aa529d6792ca6ff0ca1b34", "\rpchlp_3", "\NamePipe_MoreWindows",
↪ "\pcheap_reuse", "\msagent_", "\gruntsvc", "\PSEXESVC*",
↪ "\PowerShellISEPipeName_", "\csexec", "\paexec", "\remcom", "\lsadump",
↪ "\cachedump", "\wcservicepipe", "\psexec", "\mojo.5688.8052.183894939787088877",
↪ "\mojo.5688.8052.35780273329370473", "\mypipe-f", "\mypipe-h", "\ntsvcs_",
↪ "\scerpc_", "\DserNamePipe", "\srvsvc_", "\status_", "\MSSE-", "(continues on next page)",
↪ "\winsock", "\win_svc", "\dce_86"]
```

(continued from previous page)

2.459 LP_Suspicious Outbound Kerberos Connection

- **Trigger Condition:** Suspicious outbound network activity via kerberos is detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Steal or Forge Kerberos Tickets, Kerberoasting
- **ATT&CK ID:** T1558, T1558.003
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
norm_id=Windows* (event_id=3 OR event_id=5156) destination_port="88" is_initiated=
↪ "true" - "process" IN ["C:\Windows\System32\lsass.exe", "C:\Program
↪ Files\Google\Chrome\Application\chrome.exe", "C:\Program Files\Mozilla
↪ Firefox\firefox.exe"] -user IN EXCLUDED_USERS
```

2.460 LP_Suspicious Outbound RDP Connections Detected

- **Trigger Condition:** Non-Standard tools connecting to TCP port 3389 indicating possible Lateral Movement are detected.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Exploitation of Remote Services
- **ATT&CK ID:** T1210
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=3 destination_port="3389" initiated="true" -image
↪ IN ["*\mstsc.exe", ".*\RTSApp.exe", ".*\RTS2App.exe", ".*\RDCMan.exe", ".*\ws_
↪ TunnelService.exe", ".*\RSSensor.exe",
↪ ".*\RemoteDesktopManagerFree.exe", ".*\RemoteDesktopManager.exe",
↪ ".*\RemoteDesktopManager64.exe", ".*\mRemoteNG.exe", ".*\mRemote.exe",
↪ ".*\Terminals.exe", ".*\spiceworks-finder.exe", ".*\FSDiscovery.exe", ".*\FSAssessment.exe
↪ ", ".*\MobaRTE.exe", ".*\chrome.exe", ".*\thor.exe", ".*\thor64.exe"] -user IN
↪ EXCLUDED_USERS
```

2.461 LP_Suspicious Parent of Csc Detected

- **Trigger Condition:** Suspicious parent of csc.exe is detected. It is an executable file part of the Microsoft .NET framework.
- **ATT&CK Category:** Defense Evasion, Execution
- **ATT&CK Tag:** Compile After Delivery, Visual Basic, JavaScript, Mshta
- **ATT&CK ID:** T1027.004, T1059.005, T1059.007, T1218.005
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*\csc.exe*" parent_process IN ["*\wscript.exe",
↪ ".*\cscript.exe", ".*\mshta.exe"] -user IN EXCLUDED_USERS
```

2.462 LP_Suspicious PowerShell Invocation Based on Parent Process

- **Trigger Condition:** Suspicious PowerShell invocations from interpreters or unusual programs like wscript or IIS worker process(w3wp.exe) are detected. Admins can add other suspicious parent processes to increase visibility.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, PowerShell
- **ATT&CK ID:** T1059, T1059.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create parent_process IN [".*\mshta.exe", ".*\wscript.exe",
↪ ".*\cscript.exe", ".*\rundll32.exe", ".*\regsvr32.exe", ".*\services.exe", ".*\winword.exe",
↪ ".*\wmiprvse.exe", ".*\powerpnt.exe", ".*\excel.exe", ".*\msaccess.exe", ".*\mspub.exe",
↪ ".*\visio.exe", ".*\outlook.exe", ".*\amigo.exe", ".*\chrome.exe", ".*\firefox.exe",
↪ ".*\iexplore.exe", ".*\microsoftedgecp.exe", ".*\microsoftedge.exe", ".*\browser.exe",
↪ ".*\vivaldi.exe", ".*\safari.exe", ".*\sqlagent.exe", ".*\sqlserver.exe", ".*\sqlservr.exe",
↪ ".*\w3wp.exe", ".*\httpd.exe", ".*\nginx.exe", ".*\php-cgi.exe", ".*\jbossvc.exe",
↪ ".*\MicrosoftEdgeSH.exe", ".*\tomcat*"] "process"=".*\powershell.exe" -path=".*\Health[?]
↪ Service State\*"
```

2.463 LP_Suspicious PowerShell Parameter Substring Detected

- **Trigger Condition:** PowerShell invocation with a suspicious parameter substring is detected. PowerShell offers a commandline shell and a scripting language for automating and managing tasks.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, PowerShell
- **ATT&CK ID:** T1059, T1059.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label=create label="process" "process"="*\powershell.exe" command IN ["*-en*", "*-
↪ec*", "*-noni*", "*-nop*", "*-exe* bypass*", "*-ep bypass*", "*-win* hid*", "*-w hid*
↪", "*-sta*", "*FromBase64String*"]
```

2.464 LP_Suspicious Process Start Locations Detected

- **Trigger Condition:** Execution of suspicious processes from unusual locations like Recycle bin or Fonts folder is detected. Adversaries often run malicious scripts or applications from unusual locations like temporary folders or recycle bin folders.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Masquerading
- **ATT&CK ID:** T1036
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create "process" IN ["*:\RECYCLER\*",
↪ "*:\SystemVolumeInformation\*", "C:\Windows\Tasks\*", "C:\Windows\debug\*",
↪ "C:\Windows\fonts\*", "C:\Windows\help\*", "C:\Windows\drivers\*",
↪ "C:\Windows\addins\*", "C:\Windows\cursors\*", "C:\Windows\system32\tasks\*",
↪ "*\Windows\IME\*", "C:\Perflogs\*"] -user IN EXCLUDED_USERS
```

2.465 LP_Suspicious Program Location with Network Connections

- **Trigger Condition:** Network connections run in suspicious file system locations.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Masquerading
- **ATT&CK ID:** T1036
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=3 "process" IN ["*\\$Recycle.bin", "*\\Users\\All Users\\*",
↪ "*\\Users\\Default\\*", "*\\Users\\Public\\*", "*\\Users\\Contacts\\*", "*\\Users\\Searches\\*",
↪ "C:\\Perflogs\\*", "*\\config\\systemprofile\\*", "*\\Windows\\Fonts\\*", "*\\Windows\\IME\\*",
↪ "*\\Windows\\addins\\*"] -user IN EXCLUDED_USERS
```

2.466 LP_Suspicious PsExec Execution Detected

- **Trigger Condition:** Execution of *psexec* or *paexec* with the renamed service name. This rule helps filter out the noise if *psexec* is used for legitimate purposes or if an attacker uses a different *psexec* client other than *sysinternal* one.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Remote Services
- **ATT&CK ID:** T1021
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=5145 share_name="IPC$" relative_target IN ["*-stdin", "*-
↪ stdout", "*-stderr"] -relative_target="PSEXESVC*" -user IN EXCLUDED_USERS
```

2.467 LP_Suspicious RDP Redirect Using TSCON Detected

- **Trigger Condition:** A suspicious Remote Desktop Protocol (RDP) session redirect using *tscon.exe* is detected.

- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Remote Services, Remote Desktop Protocol
- **ATT&CK ID:** T1021, T1021.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 command="*/dest:rdp-tcp:*" -user IN EXCLUDED_
↳ USERS
```

2.468 LP_Suspicious Remote Thread Created

- **Trigger Condition:** The suspicious processes (like word.exe or outlook.exe) create remote threads on other processes. This technique is used by malware to inject code and hide in other processes. The event indicates the source and target process. It gives information on the code that will run in the new thread: StartAddress, StartModule and StartFunction.
- **ATT&CK Category:** Privilege Escalation
- **ATT&CK Tag:** Process Injection
- **ATT&CK ID:** T1055
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=8 "process" IN ["*\bash.exe", "*/cvtres.exe",
↳ "*/defrag.exe", "*/dnx.exe", "*/esentutl.exe", "*/excel.exe", "*/expand.exe",
↳ "*/explorer.exe", "*/find.exe", "*/findstr.exe", "*/forfiles.exe", "*/git.exe", "*/gpupdate.
↳ exe", "*/hh.exe", "*/iexplore.exe", "*/installutil.exe", "*/lync.exe", "*/makecab.exe",
↳ "*/mDNSResponder.exe", "*/monitoringhost.exe", "*/msbuild.exe", "*/mshta.exe",
↳ "*/msiexec.exe", "*/mspaint.exe", "*/outlook.exe", "*/ping.exe", "*/powerpnt.exe",
↳ "*/powershell.exe", "*/provtool.exe", "*/python.exe", "*/regsvr32.exe", "*/robocopy.
↳ exe", "*/runonce.exe", "*/sapcimc.exe", "*/schtasks.exe", "*/smartscreen.exe",
↳ "*/spoolsv.exe", "*/tstheme.exe", "*/userinit.exe", "*/vssadmin.exe", "*/vssvc.exe",
↳ "*/w3wp.exe", "*/winlogon.exe", "*/winscp.exe", "*/wmic.exe", "*/word.exe",
↳ "*/wscript.exe"] - "process"="*/Visual Studio*" -user IN EXCLUDED_USERS
```

2.469 LP_Suspicious RUN Key from Download Detected

- **Trigger Condition:** A suspicious RUN keys created by software located in the Download or temporary Outlook/Internet Explorer directories.
- **ATT&CK Category:** Persistence, Privilege Escalation
- **ATT&CK Tag:** Boot or Logon Autostart Execution, Registry Run Keys/Startup Folder
- **ATT&CK ID:** T1547, T1547.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=13 "process" IN ["*\Downloads\*", ".*\Temporary
↪Internet Files\Content.Outlook\*", ".*\Local Settings\Temporary Internet Files\*"] target_
↪object=".*\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\*" -user IN EXCLUDED_
↪USERS
```

2.470 LP_Suspicious Rundll32 Activity Detected

- **Trigger Condition:** Suspicious processes related to the RunDLL32 binary based on its command-line arguments are detected. Adversaries may abuse RunDLL32 to proxy code executions and avoid triggering security tools that may not monitor the execution of the *rundll32.exe* process because of allowlists or false positives from normal operations. Whitelisting is required due to the inherent RunDLL32 noise.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Rundll32
- **ATT&CK ID:** T1218.011
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create ("process"=".*\rundll32.exe" OR file="rundll32.exe")
↪((command=".*javascript:.*" command=".*.RegisterXLL*") OR (command=".*url.dll*")
↪(command=".*OpenURL*" OR command=".*FileProtocolHandler*")) OR (command=
↪".*shell32.dll*" (command=".*Control_RunDLL*" OR command=".*ShellExec_RunDLL*"
↪))OR (command=".*mshtml.dll*" command=".*PrintHTML*") OR (command=".*advpack.
↪dll*" (command=".*LaunchINFSection*" OR command=".*RegisterOCX*")) OR
↪((command=".*ieframe.dll*" OR command=".*shdocvw.dll*") command=".*OpenURL*")
↪OR (command=".*syssetup.dll*" command=".*SetupInfObjectInstal(continues on next page)
↪(command=".*setupapi.dll*" command=".*InstallHinfSection*") OR (command=".*pcwutl.
↪dll*" command=".*LaunchApplication*") OR (command=".*dfshim.dll*" (command="
↪".*ShOpenVerbApplication*" OR command=".*ShOpenVerbShortcut*")) OR ((command=
↪".*scrobj.dll*" command=".*GenerateTypeLib*") OR (command=".*shimgvw.dll*"
↪command=".*ImageView_Fullscreen*") command=".*http*" OR (command=".*comsvcs.
```

(continued from previous page)

2.471 LP_Suspicious Scripting in a WMI Consumer

- **Trigger Condition:** Suspicious scripting in the WMI Event Consumers.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, PowerShell
- **ATT&CK ID:** T1059, T1059.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=20 destination IN ["*new-object .webclient).
↳ downloadstring("*", "*new-object .webclient).downloadfile("*", "*new-object net.
↳ webclient).downloadstring("*", "*new-object net.webclient).downloadfile("*", "* iex("*",
↳ "*WScript.shell*", "* -nop *", "* -noprofile *", "* -decode *", "* -enc *"] -user IN EXCLUDED_USERS
```

2.472 LP_Suspicious Service Path Modification Detected

- **Trigger Condition:** Modification of service path to powershell/cmd is detected.
- **ATT&CK Category:** Persistence, Privilege Escalation
- **ATT&CK Tag:** Windows Service
- **ATT&CK ID:** T1543.003
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create "process"="*\.sc.exe" command="*config*" command=
↳ "*binpath*" command In ["*powershell*", "*cmd*", "*mshta*", "*wscript*", "*cscript*",
↳ "*rundll32*", "*svchost*", "*dllhost*", "*cmd.exe /c*", "*cmd.exe /k*", "*cmd.exe /r*",
↳ "*cmd /c*", "*cmd /k*", "*cmd /r*", "*C:\Users\Public*", "*\Downloads\*",
↳ "*\Desktop\*", "*\Microsoft\Windows\Start Menu\Programs\Startup\*",
↳ "*C:\Windows\TEMP\*", "\AppData\Local\Temp"]
```

2.473 LP_Suspicious Svchost Process Detected

- **Trigger Condition:** Any suspicious svchost process creation is detected. Svchost is essential in implementing shared service processes, where a number of services can share a process to reduce resource consumption.
- **ATT&CK Category:** Defense Evasion, Privilege Escalation
- **ATT&CK Tag:** Masquerading, Match Legitimate Name or Location, Process Injection
- **ATT&CK ID:** T1036, T1036.005, T1055
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create "process"="*\svchost.exe" -parent_process IN [
  ↳ "*\MsMpEng.exe", "*\Mrt.exe", "*\rpcnet.exe", "C:\Windows\System32\svchost.exe"] (-
  ↳ parent_process="*\services.exe" -command="* -k *") parent_process=* -user IN [
  ↳ EXCLUDED_USERS
```

2.474 LP_Suspicious TSCON Start

- **Trigger Condition:** tscon.exe process execution as LOCAL SYSTEM is detected. If tscon.exe run as SYSTEM, users can gain access to the currently logged-in session without credential.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Remote Access Software
- **ATT&CK ID:** T1219
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create user IN ["SYSTEM", "*AUTHOR*", "*AUTOR*"] "process"=
  ↳ "*\tscon.exe" -user IN EXCLUDED_USERS
```

2.475 LP_Suspicious Typical Malware Back Connect Ports Detected

- **Trigger Condition:** Programs connecting to a typical malware back connect ports based on statistical analysis from two different sandbox system databases are detected.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Non-Standard Port
- **ATT&CK ID:** T1571
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
destination_port IN ["4443", "2448", "8143", "1777", "1443", "243", "65535", "13506",
↪ "3360", "200", "198", "49180", "13507", "6625", "4444", "4438", "1904", "13505",
↪ "13504", "12102", "9631", "5445",
"2443", "777", "13394", "13145", "12103", "5552", "3939", "3675", "666", "473", "5649",
↪ "4455", "4433", "1817", "100", "65520", "1960", "1515", "743", "700", "14154", "14103",
↪ "14102", "12322", "10101", "7210", "4040", "9943"] -image="*\Program Files*"
-destination_address IN HOMENET -user IN EXCLUDED_USERS
```

2.476 LP_Suspicious CSharp or FSharp Interactive Console Execution

- **Trigger Condition:** Execution of CSharp or FSharp interactive console by scripting utilities like WScript or PowerShell is detected. The alert warns you of the use of the .NET framework by attackers for offensive purposes.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Trusted Developer Utilities Proxy Execution
- **ATT&CK ID:** T1127
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process" IN ["*\csi.exe", "*\fsi.exe"] parent_process IN [
↪ "*\cmd.exe", "*\powershell.exe", "*\wscript.exe", "*\cscript.exe"] -user IN EXCLUDED_
↪ USERS
```

2.477 LP_Suspicious Userinit Child Process

- **Trigger Condition:** Suspicious process spawned by *Userinit* is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Process Injection
- **ATT&CK ID:** T1055
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label="Create" (parent_process="*\userinit.exe" -(command=
↪ "*\netlogon\*" OR ("process"="*\explorer.exe" OR file="explorer.exe")) -user IN❗
↪ EXCLUDED_USERS
```

2.478 LP_Suspicious Windows ANONYMOUS LOGON Local Account Creation

- **Trigger Condition:** Creation of suspicious accounts similar to ANONYMOUS LOGON like using additional spaces, is detected. It is created to catch the exclusion of Logon Type 3 from ANONYMOUS LOGON accounts.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Create Account
- **ATT&CK ID:** T1136
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4720 user="*ANONYMOUS*LOGON*" -user IN❗
↪ EXCLUDED_USERS
```

2.479 LP_Suspicious WMI Execution Detected

- **Trigger Condition:** When WMI executing suspicious commands, including but not limited to AV product enumeration and remote process creation, are detected. WMIC.exe is a built-in Microsoft program that allows command-line access to the

Windows Management Instrumentation. Adversaries can use this technique to create remote or local processes, get details about antivirus and firewalls, delete shadow copies and modify defender configurations.

- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Windows Management Instrumentation
- **ATT&CK ID:** T1047
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create command="*process*" command="*call*" command=
↳ "*create*" command IN ["*rundll32*", "*bitsadmin*", "*regsvr32*", "*cmd.exe /c*",
↳ "*cmd.exe /k*", "*cmd.exe /r*", "*cmd /c*", "*cmd /k*", "*cmd /r*", "*powershell*",
↳ "*pwsh*", "*certutil*", "*cscript*", "*wscript*", "*mshta*", "*\Users\Public\*",
↳ "*\Windows\Temp\*", "*\AppData\Local\*", "*%temp%*", "*%tmp%*",
```

2.480 LP_Svchost DLL Search Order Hijack Detected

- **Trigger Condition:** Svchost DLL Search Order Hijack is detected. By default, IKEEXT and SessionEnv service call LoadLibrary on files that does not exist within C:/Windows/System 32/. An attacker can place their malicious logic within the PROCESS_ATTACH block of their library and restart the services mentioned above svchost.exe -k netsvcs to gain code execution on a remote machine.
- **ATT&CK Category:** Persistence, Privilege Escalation, Defense Evasion
- **ATT&CK Tag:** Hijack Execution Flow, DLL Side-Loading, DLL Search Order Hijacking
- **ATT&CK ID:** T1574, T1574.002, T1574.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=7 "process" IN ["*svchost.exe"] image IN [
↳ "*tsmsisrv.dll", "*tsvipsrv.dll", "*wlbsctrl.dll"] -image IN ["C:\Windows\WinSxS\*"] -
↳ user IN EXCLUDED_USERS
```

2.481 LP_SysKey Registry Keys Access

- **Trigger Condition:** Requests and access operations to specific registry keys to calculate the SysKey are detected. Adversaries use a tool (like Mimikatz) or a script (like Invoke-PowerDump) to get the SysKey to decrypt Security Account Manager (SAM) database entries from registry or hive and get NTLM and LM hashes of local accounts passwords.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Query Registry
- **ATT&CK ID:** T1012
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id IN [4656, 4663] object_type="key" object_name IN ["*lsa\JD
↪", "*lsa\GBG", "*lsa\Skew1", "*lsa\Data"]
-user IN EXCLUDED_USERS
```

2.482 LP_Sysmon Configuration Modification Detected

- **Trigger Condition:** Modification in Sysmon configuration.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Impair Defenses, Indicator Blocking
- **ATT&CK ID:** T1562, T1562.006
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon label=Sysmon label=Config label=Change -user IN ↪
↪ EXCLUDED_USERS
```

2.483 LP_Sysmon Driver Unload Detected

- **Trigger Condition:** Unloading of Sysmon driver is detected. After error events are logged, logs will not be collected and parsed by Sysmon.

- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Impair Defenses, Disable or Modify Tools
- **ATT&CK ID:** T1562, T1562.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=255 id="DriverCommunication" -user IN EXCLUDED_
↪USERS
```

2.484 LP_Sysmon Error Event Detected

- **Trigger Condition:** Sysmon error event is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Impair Defenses, Disable or Modify Tools
- **ATT&CK ID:** T1562, T1562.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=255 -user IN EXCLUDED_USERS
```

2.485 LP_System File Execution Location Anomaly Detected

- **Trigger Condition:** Starting a Windows program executable in a suspicious folder is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Masquerading
- **ATT&CK ID:** T1036
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create
"process" IN ["*\\svchost.exe", "*\\rundll32.exe", "*\\services.exe", "*\\powershell.exe",
↪ "*\\powershell_ise.exe", "*\\pwsh.exe", "*\\regsvr32.exe", "*\\spoolsv.exe", "*\\lsass.exe",
↪ "*\\smss.exe", "*\\csrss.exe", "*\\conhost.exe", "*\\wininit.exe", "*\\lsmd.exe", "*\\winlogon.
↪ exe", "*\\explorer.exe", "*\\taskhost.exe", "*\\Taskmgr.exe", "*\\sihost.exe",
↪ "*\\RuntimeBroker.exe", "*\\smartscreen.exe", "*\\dllhost.exe", "*\\audiodg.exe",
↪ "*\\wlanext.exe", "*\\dashost.exe", "*\\schtasks.exe", "*\\cscript.exe", "*\\wscript.exe",
↪ "*\\wsl.exe", "*\\bitsadmin.exe", "*\\atbroker.exe", "*\\bcdedit.exe", "*\\certutil.exe",
↪ "*\\certreq.exe", "*\\cmstp.exe", "*\\consent.exe", "*\\defrag.exe", "*\\dism.exe",
↪ "*\\dllhst3g.exe", "*\\eventvwr.exe", "*\\msiexec.exe", "*\\runonce.exe", "*\\winver.exe",
↪ "*\\logonui.exe", "*\\userinit.exe", "*\\dwm.exe", "*\\lsalso.exe", "*\\ntoskrnl.exe",
↪ "*\\wsmprovhost.exe", "*\\dfrgui.exe"]
- ("process" IN ["C:\\Windows\\System32\\*", "C:\\Windows\\SysWOW64\\*",
↪ "C:\\Windows\\WinSxS\\*", "*\\SystemRoot\\System32\\*", "C:\\Windows\\explorer.exe",
↪ "C:\\Program Files\\PowerShell\\7\\pwsh.exe", "C:\\Program
↪ Files\\WindowsApps\\MicrosoftCorporationII.WindowsSubsystemForLinux*\\wsl.exe"])
```

2.486 LP_System Service Discovery

- **Trigger Condition:** When an adversary attempts to get information about registered services is detected.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** System Service Discovery
- **ATT&CK ID:** T1007
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process" IN ["*\\net.exe", "*\\tasklist.exe", "*\\sc.exe",
↪ "*\\wmic.exe"] command IN ["*\\net.exe* start*", "*\\tasklist.exe* /SVC", "*\\sc.exe* query*",
↪ "*\\wmic.exe* service where*"]
```

2.487 LP_Tap Driver Installation Detected

- **Trigger Condition:** Installation of TAP software. It indicates possible preparation for data exfiltration using tunneling techniques.
- **ATT&CK Category:** Exfiltration
- **ATT&CK Tag:** Exfiltration Over Alternative Protocol

- **ATT&CK ID:** T1048
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
((norm_id=WindowsSysmon event_id=6) OR (norm_id=WinServer (event_id=7045 OR
↪ event_id=4697))) (path="*tap0901*" OR file="*tap0901*") -user IN EXCLUDED_USERS
```

2.488 LP_Tasks Folder Evasion Detected

- **Trigger Condition:** Evasion of task folder is detected. Task folder in system32 and syswow64 are globally writable paths. Adversaries can load or influence script hosts, or any .NET application in task to load and execute a custom assembly into cscript, wscript, regsvr32, mshta, and eventvwr.
- **ATT&CK Category:** Persistence, Privilege Escalation, Defense Evasion
- **ATT&CK Tag:** Hijack Execution Flow, DLL Side-Loading
- **ATT&CK ID:** T1574, T1574.002
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WinServer event_id=4688 command IN ["*echo *", "*copy *", "*type *", "*file
↪ createnew*"] command IN ["* C:\Windows\System32\Tasks\*", "*
↪ C:\Windows\SysWow64\Tasks\*"]
```

2.489 LP_Terminal Service Process Spawn Detected

- **Trigger Condition:** Process spawned by the terminal service server process is detected. It can be used as an indicator for the exploitation of CVE-2019-0708.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Exploitation of Remote Services
- **ATT&CK ID:** T1210
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create parent_command="*\svchost.exe*termsvcs"- "process" IN [
  ↳ "\*\\rdpclip.exe", "\*\\Windows\\System32\\csrss.exe*", "\*\\Windows\\System32\\wininit.exe",
  ↳ "\*\\Windows\\System32\\winlogon.exe"]
```

2.490 LP_Threat Intel Allowed Connections from Suspicious Sources

- **Trigger Condition:** A connection from suspicious sources are detected.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Proxy
- **ATT&CK ID:** T1090
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

```
norm_id=* label=Allow label=Connection -source_address in HOMENET destination_
  ↳ address in HOMENET | process ti(source_address) | rename et_ip_address as
  ↳ SourceAddress, cs_ip_address as SourceAddress, et_category as Category,
  cs_category as Category, rf_ip_address as SourceAddress, rf_category as Category, et_
  ↳ score as Score, cs_score as Score, rf_score as Score, destination_port as Port | fields
  ↳ Category, SourceAddress, Score, Port
```

2.491 LP_Threat Intel Connections with Suspicious Domains

- **Trigger Condition:** A connection is established with a suspicious domain.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

```
label=Connection (url=* OR domain=*) | process domain(url) as domain | process
  ↳ ti(domain) | rename et_category as Category, cs_category as Category, rf_category as
  ↳ Category, et_score as Score, cs_score as Score, rf_score as Score, rf_domain as Domain,
  ↳ et_domain as Domain, cs_domain as Domain
```

(continues on next page)

(continued from previous page)

2.492 LP_Time-Stomping of Users Directory Files Detected

- **Trigger Condition:** Time-stomping of user directory file is detected. Sysmon can only detect a change of CreationTime and not LastWriteTime and LastAccessTime. Therefore, we recommend that whitelist legitimate noisy processes like browsers, slack, or teams to reduce false positives.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Indicator Removal on Host, Timestomp
- **ATT&CK ID:** T1070, T1070.006
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=2 path="C:\Users*" -source_image IN ["*iexplore.exe"
↳, "*cortana*", "*\StartMenuExperienceHost.exe", "C:\Windows\system32\cleanmgr.exe"
↳, "C:\Windows\Explorer.EXE", "*\LocalBridge.exe", "*\svchost.exe",
"*\RuntimeBroker.exe", "*\msedge.exe"]-path=
↳ "*\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations" -user IN ?
↳ EXCLUDED_USERS
```

2.493 LP_Transferring Files with Credential Data via Network Shares

- **Trigger Condition:** Transfer of sensitive files with credential data using a network share.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=5145 relative_target IN ["*\mimidrv*", "*\lsass*",
↪ "*\windows\minidump*", "*\hiberfil*", "*\sqlmgr*", "*\sam*", "*\ntds.dit*",
↪ "*\security*"] -user IN EXCLUDED_USERS
```

2.494 LP_TrendMicroDeepSecurity Virus Quarantined

- **Trigger Condition:** A virus-infected file is quarantined.
- **ATT&CK Category:** Defense Evasion, Discovery
- **ATT&CK Tag:** Obfuscated Files or Information, Indicator Removal from Tools, Network Service Scanning
- **ATT&CK ID:** T1027, T1027.005, T1046
- **Minimum Log Source Requirement:** Trend Micro Deep Security
- **Query:**

```
norm_id=TrendMicroDeepSecurity label=Virus OR label=Malware label=File🔗
↪ label=Quarantine
```

2.495 LP_UAC Bypass via Event Viewer Detected

- **Trigger Condition:** UAC bypass method using the Windows Event Viewer is detected.
- **ATT&CK Category:** Defense Evasion, Privilege Escalation
- **ATT&CK Tag:** Abuse Elevation Control Mechanism, Bypass User Access Control
- **ATT&CK ID:** T1548, T1548.002
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
(label="Process" label=Create parent_process="*\eventvwr.exe" - "process"="*\mmc.exe
↪ ") OR (norm_id = WindowsSysmon event_id=13 target_object=
↪ "HKCU*\mscfile\shell\open\command")
```

2.496 LP_Unix Possible Bruteforce Attack

- **Trigger Condition:** An account is not present but is used repeatedly to login. This may be a brute force attack by a bot, malware, or threat agent.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Brute Force
- **ATT&CK ID:** T1110
- **Minimum Log Source Requirement:** Unix
- **Query:**

```
norm_id=Unix ((label=Account label=Absent) OR (label=User label=Authentication
↪label=Fail)) user=* | chart count() as cnt by user | search cnt>10
```

2.497 LP_Unix User Deleted

- **Trigger Condition:** Deletion of a user account.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Account Access Removal
- **ATT&CK ID:** T1531
- **Minimum Log Source Requirement:** Unix
- **Query:**

```
norm_id=Unix label=User label=Account label=Management label=Delete label=Remove
↪user=*
```

2.498 LP_Unsigned Driver Loading Detected

- **Trigger Condition:** Loading of an unsigned driver is detected.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -

- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=6 is_sign=False image=* -user IN EXCLUDED_USERS
```

2.499 LP_Possible Ursnif Registry Activity

- **Trigger Condition:** A new registry key under *AppDataLowSoftwareMicrosoft* is detected, which was used by Ursnif malware.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Modify Registry
- **ATT&CK ID:** T1112
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=13 target_object=
↳ "*\Software\AppDataLow\Software\Microsoft\*" -user IN EXCLUDED_USERS
```

2.500 LP_VBA DLL Loaded by Office

- **Trigger Condition:** Loading of DLL related to VBA macros by Office products id detected. To reduce false positives, we recommend you filter the use of the legitimate macro.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** Phishing, Spearphishing Attachment
- **ATT&CK ID:** T1566, T1566.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=7 source_image IN ["*\winword.exe*", "*\powerpnt.
↳ exe*", "*\excel.exe*", "*\outlook.exe*"] image IN ["*\VBE7.DLL*", "*\VBEUI.DLL*",
↳ "*\VBE7INTL.DLL*"] -user IN EXCLUDED_USERS
```

2.501 LP_VM - High Risk Vulnerability on High Impact Assets

- **Trigger Condition:** High-risk vulnerability is detected in high impact assets.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Network Service Scanning
- **ATT&CK ID:** T1046
- **Minimum Log Source Requirement:** Qualys, Vulnerability Management
- **Query:**

```
(col_type=qualys* or col_type=Nessus or norm_id=VulnerabilityManagement) (severity=4[?]
↪ or severity=5) source_address IN HIGH_IMPACT_ASSETS
```

2.502 LP_VM - High Risk Vulnerability on Low Impact Assets

- **Trigger Condition:** High-risk vulnerability is detected in low impact assets.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Network Service Scanning
- **ATT&CK ID:** T1046
- **Minimum Log Source Requirement:** Qualys, Vulnerability Management
- **Query:**

```
(col_type=qualys* or col_type=Nessus or norm_id=VulnerabilityManagement) (severity=4[?]
↪ OR severity=5) source_address IN LOW_IMPACT_ASSETS
```

2.503 LP_VM - High Risk Vulnerability on Medium Impact Assets

- **Trigger Condition:** High-risk vulnerability is detected in medium impact assets.
- **ATT&CK Category:** Discovery

- **ATT&CK Tag:** Network Service Scanning
- **ATT&CK ID:** T1046
- **Minimum Log Source Requirement:** Qualys, Vulnerability Management
- **Query:**

```
(col_type=qualys* or col_type=Nessus or norm_id=VulnerabilityManagement) (severity=4 or severity=5) source_address IN MEDIUM_IMPACT_ASSETS
```

2.504 LP_VM - Medium Risk Vulnerability on High Impact Assets

- **Trigger Condition:** Medium-risk vulnerability is detected in high impact assets.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Network Service Scanning
- **ATT&CK ID:** T1046
- **Minimum Log Source Requirement:** Qualys, Vulnerability Management
- **Query:**

```
(col_type=qualys* or col_type=Nessus or norm_id=VulnerabilityManagement) (severity=2 or severity=3) source_address IN HIGH_IMPACT_ASSETS
```

2.505 LP_VM - Medium Risk Vulnerability on Low Impact Assets

- **Trigger Condition:** Medium-risk vulnerability is detected in low impact assets.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Network Service Scanning
- **ATT&CK ID:** T1046
- **Minimum Log Source Requirement:** Qualys, Vulnerability Management
- **Query:**

```
(col_type=qualys* or col_type=Nessus or norm_id=VulnerabilityManagement) (severity=2?)  
↪ OR severity=3) source_address IN LOW_IMPACT_ASSETS
```

2.506 LP_VM - Medium Risk Vulnerability on Medium Impact Assets

- **Trigger Condition:** Medium-risk vulnerability is detected in medium impact assets.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Network Service Scanning
- **ATT&CK ID:** T1046
- **Minimum Log Source Requirement:** Qualys, Vulnerability Management
- **Query:**

```
(col_type=qualys* or col_type=Nessus or norm_id=VulnerabilityManagement) (severity=2?)  
↪ OR severity=3) source_address IN MEDIUM_IMPACT_ASSETS
```

2.507 LP_WannaCry MS17-010 Vulnerable Sources

- **Trigger Condition:** MS17-010 vulnerability is detected.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Qualys, Vulnerability Management
- **Query:**

```
col_type=qualys* qualys_id IN [91345, 91357, 91359, 91360, 70077, 91360, 91345]
```

2.508 LP_WannaCry Sources in Connections to Sinkhole Domain

- **Trigger Condition:** A source tries to connect to the WannaCry sinkhole domain.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Proxy
- **ATT&CK ID:** T1090
- **Minimum Log Source Requirement:** Firewall, IDS/IPS, Webserver
- **Query:**

```
norm_id=* url IN WANNACRY_DOMAIN or domain IN WANNACRY_DOMAIN
```

2.509 LP_WCE wceaux.dll Access Detected

- **Trigger Condition:** *wceaux.dll* access during Windows Credential Editor (WCE) pass-the-hash remote command execution on the source host is detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id IN ["4656", "4658", "4660", "4663"] object_name=
↳ "*"wceaux.dll" -user IN EXCLUDED_USERS
```

2.510 LP_Wdigest Registry Modification

- **Trigger Condition:** Modification of the wdigest registry value is detected. Wdigest is an windows authentication protocol which stores credential in plain text. Adversaries can enable wdigest authentication and retrieve plain text credential of users.
- **ATT&CK Category:** Defense Evasion

- **ATT&CK Tag:** Modify Registry
- **ATT&CK ID:** T1112
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label=Registry label=Value label=Set target_object="*WDigest\LogonCredential"
```

2.511 LP_Weak Encryption Enabled for User

- **Trigger Condition:** Weak encryption is enabled for a user profile, which is later used for hash or password cracking.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Modify Registry
- **ATT&CK ID:** T1112
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WinServer event_id=4738 user_account_control IN ["*DES*", "*Preauth*",  
↪ "*Encrypted*"] user_account_control="*Enabled*" -user IN EXCLUDED_USERS
```

2.512 LP_Potential Webshell Activity Detected

- **Trigger Condition:** Specific command line parameters, commonly associated with reconnaissance activities via web shells, are detected.
- **ATT&CK Category:** Discovery, Persistence
- **ATT&CK Tag:** Remote System Discovery, System Owner/User Discovery, Account Discovery, Web Shell
- **ATT&CK ID:** T1018, T1033, T1087, T1505.003
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label="Create" ((parent_process IN ["*\\w3wp.exe", "*\\php-cgi.exe",
↪ "*\\nginx.exe", "*\\httpd.exe", "*\\caddy.exe", "*\\ws_tomcat-service.exe"] OR (parent_
↪ process IN ["*\\java.exe", "*\\javaw.exe"] (parent_process IN ["*-tomcat-*", "*\\tomcat*"]
↪ OR command IN ["*catalina.jar*", "*CATALINA_HOME*"]))) (((file IN ["net.exe", "net1.
↪ exe"] command IN ["* user *", "* use *", "* group *"]) OR (file = "ping.exe" command
↪ = "* -n *") OR command IN ["*&cd&echo*", "*cd /d *"] OR (file = "wmic.exe"
↪ command = "* /node:*") OR ("process" IN ["*\\whoami.exe", "*\\systeminfo.exe",
↪ "*\\quser.exe", "*\\ipconfig.exe", "*\\pathping.exe", "*\\tracert.exe", "*\\netstat.exe",
↪ "*\\schtasks.exe", "*\\vssadmin.exe", "*\\wevtutil.exe", "*\\tasklist.exe"] OR file IN [
↪ "whoami.exe", "sysinfo.exe", "quser.exe", "ipconfig.exe", "pathping.exe", "tracert.exe",
↪ "netstat.exe", "schtasks.exe", "VSSADMIN.EXE", "wevtutil.exe", "tasklist.exe"]) OR
↪ command IN ["* Test-NetConnection *", "*dir \\*"]))) -user IN EXCLUDED_USERS
```

2.513 LP_Windows Audit Logs Cleared

- **Trigger Condition:** The Windows Security audit log is cleared.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Clear Windows Event Logs
- **ATT&CK ID:** T1070.001
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer label=Audit label=Log label=Clear -user IN EXCLUDED_USERS
```

2.514 LP_Windows Data Copied to Removable Device

- **Trigger Condition:** A file is copied to removable storage. For this alert to work, you must update the list CRITICAL_HOSTS, which includes hosts where admin monitors file copy across removable storage.
- **ATT&CK Category:** Exfiltration
- **ATT&CK Tag:** Exfiltration Over Physical Medium, Exfiltration over USB
- **ATT&CK ID:** T1052, T1052.001
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer* event_id=4663 event_category="Removable Storage" access=
↪ "WriteData*" or access="*AppendData*" host IN CRITICAL_HOSTS -user IN
↪ EXCLUDED_USERS
```

2.515 LP_Windows Defender Antivirus Disable via Registry Modification

- **Trigger Condition:** Windows Defender Antivirus registry values added or modified to set it to a disabled state are detected. Windows Defender Antivirus is a native anti-malware component of Microsoft Windows. Adversaries generally attempt to turn off anti-virus components of any system to inhibit detection.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Disable or Modify Tools
- **ATT&CK ID:** T1562.001
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="process" label="create" "process"="*\reg.exe" command=
↪ "*HKLM\Software\Policies\Microsoft\Windows Defender*" command="*add*1*"
↪ command IN ["*DisableAntiSpyware*", "*DisableAntiVirus*", "*MpEnablePus*",
↪ "*DisableBehaviorMonitoring*", "*DisableIOAVProtection*",
↪ "*DisableOnAccessProtection*", "*DisableRealtimeMonitoring*",
↪ "*DisableScanOnRealtimeEnable*", "*DisableEnhancedNotifications*",
↪ "*DisableBlockAtFirstSeen*"]
```

2.516 LP_Shadow Copy Deletion Using OS Utilities Detected

- **Trigger Condition:** Windows Defender Antivirus registry values added or modified to set it to a disabled state are detected. Windows Defender Antivirus is a native anti-malware component of Microsoft Windows. Adversaries generally attempt to turn off anti-virus components of any system to inhibit detection.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Inhibit System Recovery
- **ATT&CK ID:** T1490

- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="Process" label="Create" ("process" IN ["*\powershell.exe", ".*\wmic.exe",
↪ ".*\vssadmin.exe", ".*\diskshadow.exe"] command=".*shadow*" command=".*delete*")
↪ OR ("process" = ".*\wbadmin.exe" command=".*delete*")
↪ (command=".*systemstatebackup*" OR (command=".*catalog*" command=".*quiet*"))
↪ OR ("process" = ".*\vssadmin.exe" command=".*resize*" command=".*shadowstorage*")
↪ command IN [".*unbounded*", ".*MaxSize=*"]) OR (command IN [".*Get-WmiObject*",
↪ ".*gwmi*", ".*Get-CimInstance*", ".*gcim*"] command=".*Win32_Shadowcopy*"
↪ "command IN [".*Delete()*", ".*Remove-WmiObject*", ".*rwm*", ".*Remove-
↪ CimInstance*", ".*rcim*"])
```

2.517 LP_Windows Defender Exclusion Set Detected

- **Trigger Condition:** Events where a Windows Defender antivirus exclusion was added. Adversaries can abuse the file exclusion feature in Windows Defender to evade detection of their malicious binaries by excluding the file type or file from being scanned.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Impair Defenses, Disable or Modify Tools
- **ATT&CK ID:** T1562, T1562.001
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
(norm_id=WinServer event_source="Microsoft-Windows-Windows Defender" event_
↪ id=5007 new_value=".*\Microsoft\Windows Defender\Exclusions\*") OR (norm_
↪ id=WindowsSysmon event_id=13 target_object = ".*\Microsoft\Windows
↪ Defender\Exclusions*" event_type=setvalue)
```

2.518 LP_Windows Excessive Amount of Files Copied to Removable Device

- **Trigger Condition:** One hundred or more files the user copied to the removable storage device are detected. Threat actors generally attempt to exfiltrate as much data as possible through removable storage devices from the victim organizations. Setting the threshold value according to the organization's behavior or risk appetite

is recommended. It is recommended to enable this alert only if the organizational policy explicitly disallows this behavior.

- **ATT&CK Category:** Exfiltration
- **ATT&CK Tag:** Exfiltration Over Physical Medium, Exfiltration over USB
- **ATT&CK ID:** T1052, T1052.001
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer* event_id=4663 event_category="Removable Storage" access=
↪ "WriteData*" or access="*AppendData*" -user IN EXCLUDED_USERS | chart distinct_
↪ count(object) as DataCopied by user | search DataCopied>100
```

2.519 LP_Windows Failed Login Attempt Using Service Account

- **Trigger Condition:** A user fails to log in using a service account. Generally, failed logon events with logon type 5 indicate the password change without updating the service; however, a possibility of malicious users at work exists. Conversely, the existence of malicious users is less likely to happen as creating a new service or editing an existing service by default requires membership in Administrators or Server Operators. Also, malicious users will already have the authority to perpetuate their desired goal.
- **ATT&CK Category:** Defense Evasion, Persistence, Privilege Escalation, Initial Access
- **ATT&CK Tag:** Valid Accounts
- **ATT&CK ID:** T1078
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer* label=User label=Login label=Fail target_user=*ORuser=?logon_
↪ type = 5 -user IN EXCLUDED_USERS | rename target_user as user, target_domain as?
↪ domain
```

2.520 LP_Windows Failed Login Followed by Lockout Event

- **Trigger Condition:** A failed login attempt followed by account lockout is detected.
- **ATT&CK Category:** Defense Evasion, Persistence, Privilege Escalation, Initial Access
- **ATT&CK Tag:** Valid Accounts, Exploitation for Credential Access, Exploitation for Privilege Escalation, Exploitation for Defense Evasion, Brute Force
- **ATT&CK ID:** T1078, T1212, T1068, T1211 ,T1110
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
[norm_id=WinServer label=User label=Login label=Fail -user IN EXCLUDED_USERS] as s1
↪ followed by [norm_id=WinServer label=User label=Account label=Lock user=*) as s2 on
↪ s1.user=s2.user | rename s1.user as User, s1.source_address as SourceAddress, s2.
↪ workstation as ComputerName, s2.caller_domain as Domain, s1.log_ts as
↪ LastFailedLogin_ts, s2.log_ts as LockedOut_ts
```

2.521 LP_Windows Local User Management

- **Trigger Condition:** A user is created on a non-domain controller. For the alert to work, you must update the list DOMAIN with domain controllers.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Create Account, Local Account
- **ATT&CK ID:** T1136, T1136.001
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer* label=User label=Create -target_user=*-user= -target_domain IN
↪ DOMAIN -domain IN DOMAIN -user IN EXCLUDED_USERS
```

2.522 LP_WMI DLL Loaded by Office

- **Trigger Condition:** Loading of DLLs related to WMI by Office products signaling VBA macros executing WMI Commands.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** User Execution, Malicious File
- **ATT&CK ID:** T1204, T1204.002
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=7 source_image IN ["*\winword.exe", ".*\powerpnt.
↪exe", ".*\excel.exe", ".*\outlook.exe"] image IN ["*\wmiutils.dll", ".*\wbemcomn.dll",
↪ ".*\wbemprox.dll", ".*\wbemdisp.dll", ".*\wbemsvc.dll"]
-user IN EXCLUDED_USERS
```

2.523 LP_Windows Processes Suspicious Parent Directory Detected

- **Trigger Condition:** Suspicious parent processes of Windows processes are detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Rename System Utilities, Match Legitimate Name or Location
- **ATT&CK ID:** T1036.003, T1036.005
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process" IN ["*\svchost.exe", ".*\taskhost.exe", ".*\sm.exe
↪", ".*\lsass.exe", ".*\services.exe", ".*\lsaiso.exe", ".*\csrss.exe", ".*\wininit.exe",
↪ ".*\winlogon.exe"] -((parent_process IN ["*\SavService.exe", ".*\ngen.exe"] parent_
↪ process IN ["*\System32\*", ".*\SysWOW64\*"]) OR (parent_process IN ["*\Windows
↪ Defender\*", ".*\Microsoft Security Client\*"] parent_process=".*\MsMpEng.exe*") OR
↪ (parent_process="-"))
```

2.524 LP_Windows Registry Persistence COM Key Linking Detected

- **Trigger Condition:** COM object hijacking via TreatAs subkey is detected. It is rare, but there are some cases where system utilities use linking keys for backward compatibility.
- **ATT&CK Category:** Privilege Escalation, Persistence
- **ATT&CK Tag:** Event Triggered Execution, Component Object Model Hijacking
- **ATT&CK ID:** T1546, T1546.015
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=12 target_object="HKU\*_Classes\CLSID\*\TreatAs" -
↪ user IN EXCLUDED_USERS
```

2.525 LP_Windows Shell Spawning Suspicious Program

- **Trigger Condition:** A suspicious child process of Windows Shell and scripting processes such as Wscript, Rundll32, Regsvr32, powershell and Mshta is detected.
- **ATT&CK Category:** Execution, Defense Evasion
- **ATT&CK Tag:** PowerShell, Visual Basic, System Binary Proxy Execution
- **ATT&CK ID:** T1059.001, T1059.005, T1218
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create parent_process IN ["*\mshta.exe", "powershell.exe",
↪ "rundll32.exe", "cscript.exe", "wscript.exe", "wmiprvse.exe", "pwsh.exe",
↪ "regsvr32.exe"] "process" IN ["schtasks.exe", "nslookup.exe", "certutil.exe",
↪ "bitsadmin.exe", "mshta.exe"] -(path="ccmcache\*" OR (parent_process=
↪ "mshta.exe" "process"="mshta.exe" parent_command="C:\MEM_Configmgr_*"
↪ parent_command="*\splash.hta*" parent_command= "{1E460BD7-F1C3-4B2E-88BF-
↪ 4E770A288AF5}" command= "C:\MEM_Configmgr_*" command=
↪ "SMSSETUP\BIN\*" command= "autorun.hta*" command= "{1E460BD7-F1C3-
↪ 4B2E-88BF-4E770A288AF5}*" OR command="*\nessus_*" OR (parent_command=
↪ "Program Files\Amazon\WorkSpacesConfig\Scripts\setup-scheduledtask.ps1*" parent_
↪ command="*\Program Files\Amazon\WorkSpacesConfig\Scripts\set-selfhealing.ps1*"
↪ parent_command="*\Program Files\Amazon\WorkSpacesConfig\Scripts\check-
↪ workspacehealth.ps1*"))
```

(continues on next page)

(continued from previous page)

2.526 LP_Windows Suspicious Creation of User Accounts

- **Trigger Condition:** Creation of an account, followed by its deletion in a day is detected.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Account Create
- **ATT&CK ID:** T1136
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
[norm_id=WinServer* label=User label=Create -target_user=*-calleruser=?-calleruser=? -
↪ user=*$ -user IN EXCLUDED_USERS | rename target_user as Account, caller_user as ?
↪ user] as s1 followed by [norm_id=WinServer* label=User (label=Delete or ?
↪ label=Remove) | rename target_user as Account, caller_user as user]
as s2 on s1.Account=s2.Account | rename s1.col_ts as CreatedTime_ts, s2.col_ts as ?
↪ DeletedTime_ts, s1.user as CreatedUser, s2.user as DeletedUser, s1.Account as Account
```

2.527 LP_Windows User Account Created via Command Line

- **Trigger Condition:** Creation of a user account via CLI like PowerShell or net utility is detected.
- **ATT&CK Category:** Execution, Persistence
- **ATT&CK Tag:** Create Account, PowerShell, Local Account
- **ATT&CK ID:** T1136, T1059.001, T1136.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label="create" (command="*New-LocalUser*" or command="*net user?
↪ add*")
```

2.528 LP_Windows User Account Change to End with Dollar Sign

- **Trigger Condition:** A user account is changed to end with the dollar sign (\$).
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Account Manipulation
- **ATT&CK ID:** T1098
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer* label=User label=Account label=Change label=Name new_user=*$ -
↪ user IN EXCLUDED_USERS | rename caller_user as user, caller_domain as domain
```

2.529 LP_Windows Webshell Creation Detected

- **Trigger Condition:** Creation of WebShell file on a static web site. The alert has been directly translated from sigma rule.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Server Software Component, Web Shell
- **ATT&CK ID:** T1505, T1505.003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=11 ((path="*\inetpub\wwwroot*" file IN ["*.asp", "*.
↪ ashx", "*.ph"]) OR (path IN ["*\www\*", "*\htdocs\*", "*\html\*"] file="*.ph") OR (file=
↪ "*.jsp" path="*\cgi-bin\*" path="*.p/*"))
-path IN ["*\AppData\Local\Temp*", "*\Windows\Temp*"]
```

2.530 LP_Winlogon Helper DLL

- **Trigger Condition:** Modification of registry entries related to winlogon.exe to load and execute possible malicious DLLs and/or executables is detected.
- **ATT&CK Category:** Persistence

- **ATT&CK Tag:** Boot or Logon Autostart Execution, Winlogon Helper DLL
- **ATT&CK ID:** T1547, T1547.004
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon (event_id=12 or event_id=13 or event_id=14) (target_object=
↳ "*\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\user_nameinit\*" or
↳ target_object="*\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell\*"
↳ " or target_object="*\SOFTWARE\Microsoft\Windows
↳ NT\CurrentVersion\Winlogon\Notify\*")
-user IN EXCLUDED_USERS
```

2.531 LP_WMI Backdoor Exchange Transport Agent

- **Trigger Condition:** WMI backdoor in Exchange Server Software Component and Transport Agents via WMI event filters is detected.
- **ATT&CK Category:** Privilege Escalation, Persistence
- **ATT&CK Tag:** Event Triggered Execution, Windows Management Instrumentation Event Subscription
- **ATT&CK ID:** T1546, T1546.003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 parent_image="*\EdgeTransport.exe" -user IN
↳ EXCLUDED_USERS
```

2.532 LP_WMI Modules Loaded by Suspicious Process

- **Trigger Condition:** Loading of WMI modules by suspicious processes like a binary from ProgramData is detected. Legitimate system processes and third-party utilities extensively use WMI. We recommend you whitelist to reduce false-positive flooding. Also, do not monitor C:Windows* as extensive whitelisting is required, which may hamper query's performance.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Windows Management Instrumentation

- **ATT&CK ID:** T1047
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label=Image label=Load image IN ["*wmicnt.dll", "*WmiApRpl.dll", "*wmiprov.dll",
↪ "*wmiutils.dll", "*wbemcomn.dll", "*wbemprox.dll", "*WMINet_Utils.dll", "*wbemsvc.dll",
↪ "*fastprox.dll"] - "process" IN ["C:\Program Files\*", "C:\Program Files (x86)\*",
↪ "*\WmiPrvSE.exe", "*\WmiApSrv.exe", "*\svchost.exe", "*\DeviceCensus.exe",
↪ "*\CompatTelRunner.exe", "*\sdiaghost.exe", "*\SIHClient.exe", "*\ngentask.exe",
↪ "*\windows\system32\taskhostw.exe", "*\windows\system32\MoUsocoreWorker.exe",
↪ "*\windows\system32\wbem\WMIADAP.exe", "C:\Windows\Sysmon64.exe",
↪ "C:\Windows\Sysmon.exe", "C:\Windows\System32\wbem\unsecapp.exe", "*\logman.
↪ exe", "*\systeminfo.exe", "*\nvcontainer.exe", "C:\Windows\System32\wbem\WMIC.
↪ exe", "*\explorer.exe", "*\opera_autoupdate.exe", "*\MsMpEng.exe", "*\thor64.exe",
↪ "*\thor.exe", "*\WaAppAgent.exe", "*\WindowsAzureGuestAgent.exe",
↪ "*\Microsoft\Teams\Update.exe", "*\Microsoft\Teams\current\Teams.exe",
↪ "*\Windows\System32\ServerManager.exe", "*\Windows\System32\vds.exe",
↪ "*\Windows\System32\dfsrs.exe", "*\Windows\System32\SecurityHealthService.exe",
↪ "*\Windows\System32\dxdiag.exe", "*\Windows\System32\dispdiag.exe",
↪ "*\Windows\System32\gpreresult.exe", "*\Windows\System32\tasklist.exe"]
```

2.533 LP_WMI Persistence - Script Event Consumer Detected

- **Trigger Condition:** Windows Management Instrumentation (WMI) script event consumers are detected. Attackers leverage WMI ActiveScriptEventConsumers remotely to move laterally in the network.
- **ATT&CK Category:** Privilege Escalation, Persistence
- **ATT&CK Tag:** Event Triggered Execution, Windows Management Instrumentation Event Subscription
- **ATT&CK ID:** T1546, T1546.003
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*:\WINDOWS\system32\wbem\scrcons.exe"
↪ parent_process="*:\Windows\System32\svchost.exe" -user IN EXCLUDED_USERS
```

2.534 LP_WMI Persistence - Script Event Consumer File Write

- **Trigger Condition:** File writes of WMI script event consumer are detected.
- **ATT&CK Category:** Privilege Escalation
- **ATT&CK Tag:** Event Triggered Execution, Windows Management Instrumentation Event Subscription
- **ATT&CK ID:** T1546, T1546.003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=11 source_image=  
↪ "C:\WINDOWS\system32\wbem\scrcons.exe" -user IN EXCLUDED_USERS
```

2.535 LP_WMI Spawning Windows Shell

- **Trigger Condition:** WMI spawning Command and Scripting Interpreter and PowerShell are detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, PowerShell, Windows Management Instrumentation
- **ATT&CK ID:** T1059, T1059.001, T1047
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 parent_image="*\wmiprvse.exe" image=  
↪ ".*\powershell.exe" -user IN EXCLUDED_USERS
```

2.536 LP_WMIExec VBS Script Detected

- **Trigger Condition:** WSF/JSE/JS/VBA/VBE File Execution execution by cscript or wscript is detected. Adversaries can utilize wscript and cscript to run suspicious files on a victim's workstation, such as malicious scripts or programs.

- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, Visual Basic, JavaScript
- **ATT&CK ID:** T1059, T1059.005, T1059.007
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label=Create label="process" "process" IN ["*\cscript.exe", "*\wscript.exe"] command in [
↪ "*.js*", "*.jse*", "*.vba*", "*.vbe*", "*.vbs*"]
```

2.537 LP_Wmiprvse Spawning Process

- **Trigger Condition:** *wmiprvse* spawning unusual processes are detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Windows Management Instrumentation
- **ATT&CK ID:** T1047
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
label="Process" label=Create "process"="*\WmiPrvSe.exe" -target_logon_id="0x3e7" -
↪ logon_id="0x3e7" -user IN EXCLUDED_USERS
```

2.538 LP_WScript or CScript Dropper Detected

- **Trigger Condition:** Execution of *wscript* or *cscript* scripts in user directories is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, Visual Basic, JavaScript
- **ATT&CK ID:** T1059.007, T1059.005, T1059
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process" IN ["*\\wscript.exe", "*\\cscript.exe"] command IN [
↪ "*\\AppData\\Local\\*", "*\\ProgramData\\*", "*\\Temp\\*"] command IN ["*.jse", "*.vbe", "*.
↪ js", "*.vba", "*.vbs"] -parent_process = "*\\winzip*"
```

2.539 LP_Wsreset UAC Bypass Detected

- **Trigger Condition:** A method that uses the Wsreset.exe tool to reset the Windows Store bypassing UAC is detected.
- **ATT&CK Category:** Privilege Escalation, Defense Evasion
- **ATT&CK Tag:** Abuse Elevation Control Mechanism, Bypass User Access Control
- **ATT&CK ID:** T1548, T1548.002
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create parent_process="*\\WSreset.exe" (-"process" = "*\\conhost.
↪ exe" OR integrity_level IN [High,System])
```

2.540 LP_XSL Script Processing Detected

- **Trigger Condition:** Application control bypass attempt via execution of embedded scripts inside Extensible Stylesheet Language (XSL) files is detected. The alert detects another variation of this technique, dubbed *Squiblytwo*, that utilizes WMI to invoke JScript or VBScript within an XSL file. Legitimate invocations of *msxsl* employ the *-o* command-line argument should be whitelisted to reduce false positives.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** XSL Script Processing
- **ATT&CK ID:** T1220
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create (((("process" = "*\\wmic.exe" command IN ["* format*:*", "* /
↪ format*:*", "*-format*:*"] ) -command in ["*Format:List", "*Format:htable",
↪ "*Format:hform", "*Format:table", "*Format:mof", "*Format:value", "*Format:rawxml",
↪ "*Format:xml", "*Format:csv"] ) OR ("process" = "*\\msxsl.exe" -command = "* -o *") -
↪ user IN EXCLUDED_USERS
```

(continues on next page)

(continued from previous page)

2.541 LP_ZOHO Dctask64 Process Injection Detected

- **Trigger Condition:** Process injection using ZOHO's dctask64.exe is detected.
- **ATT&CK Category:** Defense Evasion, Privilege Escalation
- **ATT&CK Tag:** Process Injection
- **ATT&CK ID:** T1055
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*\dctask64.exe" -command="*DesktopCentral_
↪Agent\agent*" -user IN EXCLUDED_USERS
```

2.542 LP_APT 34 Initial Access Using Spearphishing Link Detected

- **Trigger Condition:** Entry vectors try to gain their initial foothold within a network using Spearphishing link with IOCs' attacks related to APT34. For the alert to work, it uses lists; IRANIAN_SPEARPHISHING_DOMAINS and IRANIAN_SPEARPHISHING_IP.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** Spearphishing Link
- **ATT&CK ID:** T1566
- **Minimum Log Source Requirement:** EmailServer
- **Query:**

```
norm_id=* label=Detect label=Malicious label=URL (source_address in IRANIAN_
↪SPEARPHISHING_IP OR domain in IRANIAN_SPEARPHISHING_DOMAINS) -user IN
↪EXCLUDED_USERS
```

2.543 LP_Suspicious File Deletion Detected

- **Trigger Condition:** Adversaries removes trail files for an intrusion to keep their footprint low or remove them at the end as part of the post-intrusion cleanup process. For the alert to work, you must configure ACLs on paths and extensions you want to monitor for deletion operations.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Indicator Removal on Host, File Deletion
- **ATT&CK ID:** T1070, T1070.004
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer label=Object label=Access access="*delete*" (relative_target="*.exe
↪ " OR relative_target="*.bat" OR relative_target="*.ps1" OR relative_target="*.cmd") -
↪ user IN EXCLUDED_USERS | rename relative_target as file
```

2.544 LP_Security Software Discovery Process Detected

- **Trigger Condition:** Adversaries attempts to get a listing of security software, configurations, defensive tools, and sensors that are installed on the system.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Security Software Discovery
- **ATT&CK ID:** T1518
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer label="Process" label=Create (command="*findstr.exe*virus" OR
↪ command="*findstr.exe*cylance" OR command="*findstr.exe*defender" OR
↪ command="*findstr.exe*cb" ) -user IN EXCLUDED_US
```

2.545 LP_System Network Configuration Discovery

- **Trigger Condition:** Discovery of network configuration via system utilities like ipconfig, route, or netsh is detected.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** System Network Configuration Discovery
- **ATT&CK ID:** T1016
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer label="Process" label=Create (command="*ipconfig.exe*" OR
↪ command="*route.exe*" OR command="*netsh advfirewall*" OR command="*arp.exe*"
↪ " OR command="*nbtstat.exe*" OR command="*netsh.exe*interface show" OR
↪ command="*net*config" ) -user IN EXCLUDED_USERS | rename commandline as
↪ command
```

2.546 LP_System Network Connections Discovery

- **Trigger Condition:** Discovery of network connections via system utilities like netstat or net is detected.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** System Network Connections Discovery
- **ATT&CK ID:** T1049
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create ("process" IN ["*net.exe", "*netstat.exe"] command IN [
↪ "*net* use*", "*net* sessions*", "*net* file*", "*netstat*"]) OR command="*Get-
↪ NetTCPConnection*" -user IN EXCLUDED_USERS
```

2.547 LP_Exfiltration over Cloud Application Detected

- **Trigger Condition:** Adversaries performs data exfiltration with a different protocol from the main Command and Control protocol or channel.
- **ATT&CK Category:** Exfiltration
- **ATT&CK Tag:** Exfiltration Over Alternative Protocol
- **ATT&CK ID:** T1048
- **Minimum Log Source Requirement:** ProxyServer
- **Query:**

```
norm_id=*Proxy* source_address=* destination_address=* destination_address IN ?
↪ CLOUD_APPLICATION_IP -user IN EXCLUDED_USERS
```

2.548 LP_Remote File Copy Detected

- **Trigger Condition:** Files are copied from one system to another to stage adversary tools or other files throughout an operation.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Remote File Copy
- **ATT&CK ID:** T1105
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer label=Object label=Access access=* (relative_target="*.exe" OR ?
↪ relative_target="*.bat") -user IN EXCLUDED_USERS | rename relative_target as file
```

2.549 LP_Privilege Escalation - Bypassing User Account Control Detected

- **Trigger Condition:** Adversaries uses techniques to elevate a user's privileges manipulating UAC to administer if the target process is unprotected.
- **ATT&CK Category:** Privilege Escalation

- **ATT&CK Tag:** Bypass User Account Control
- **ATT&CK ID:** T1548
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
(norm_id=WindowsSysmon OR ((command=* OR commandline=*) norm_id=WinServer))
↪ label="Process" label=Create (command="*eventvwr.exe*" OR commandline=
↪ "*eventvwr.exe*" OR command="*wscript.exe*" OR commandline="*wscript.exe*" OR
↪ token_elevation_type="TokenElevationTypeLimited*")
-user IN EXCLUDED_USERS | rename commandline as command
```

2.550 LP_Process Execution from Suspicious Location

- **Trigger Condition:** Execution of a process from suspicious location is detected.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4688 "process" IN ["C:\ProgramData\*.exe",
↪ "*\AppData\Local\*.exe", "*\AppData\Roaming\*.exe", "C:\Users\Public\*"] -"process
↪ " IN ["*\Teams.exe", "*\Teams\Update.exe", "*\Temp\*\dismhost.exe",
↪ "*\Microsoft\OneDrive\*\FileCoAuth.exe", "C:\ProgramData\Microsoft\*\MpCmdRun.exe
↪ ", "*\Local\Temp\*\BackgroundDownload.exe", "*\Microsoft\Windows
↪ Defender\*\NisSrv.exe", "C:\ProgramData\Microsoft\*\MsMpEng.exe"]
```

2.551 LP_Active Directory Enumeration via ADFind

- **Trigger Condition:** When enumeration of Active Directory using the ADfind tool is detected. AdFind is a CLI-based utility that can be used for gathering information from Active Directory like organizational units, users, computers, and groups. Adversaries can use this utility to gather information related to the Active Directory.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** T1059 - Command and Scripting Interpreter, T1059.001 - PowerShell

- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="Process" label=Create "process"="*.exe" command IN ["*-f *objectcategory=*",
↪ "-sc trustdmp*", "*lockoutduration*", "*lockoutthreshold",
↪ "*lockoutobservationwindow*", "*maxpwdage*", "*minpwdage*", "*minpwdlength*",
↪ "*pwdhistorylength*", "*pwdproperties*", "-sc admincountdmp*", "-sc?",
↪ exchaddresses*"]
```

2.552 LP_Possible Command Prompt Process Hollowing

- **Trigger Condition:** Possible process hollowing of the command prompt is detected using applications like net.exe, nltest.exe or ipfconfig. Adversaries injects malicious code into suspended and hollowed processes to evade process-based defenses.
- **ATT&CK Category:** Defense Evasion, Privilege Escalation
- **ATT&CK Tag:** Process Injection, Process Hollowing
- **ATT&CK ID:** T1055, T1055.012
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WindowsSysmon event_id=1 parent_image="*cmd.exe" image IN ["*\net.exe",
↪ "*\net1.exe", "*\nltest.exe", "*\ipconfig.exe"] -parent_command IN ["*/c *", "*/k *"]
```

2.553 LP_Suspicious Taskkill Activity

- **Trigger Condition:** More than two processes terminated in a short time via task kill command that may signal malicious activity like ransomware are detected.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Service Stop
- **ATT&CK ID:** T1489
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4688 "process"="*\taskkill.exe" | chart count() as cnt by host,
↪ "process" | search cnt > 2
```

2.554 LP_Suspicious File or Directory Permission Modification

- **Trigger Condition:** Permission modification of suspicious file or directory is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** File and Directory Permissions Modification, Windows File and Directory Permissions Modification
- **ATT&CK ID:** T1222.001
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4688 "process"="*\icacls.exe" command="icacls*:*/*grant
↪ everyone*"
```

2.555 LP_Ryuk Wake-On-LAN Activity

- **Trigger Condition:** Ryuks Wake-On-LAN activity is detected.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4688 "process"="*.exe" command="* 8 LAN *"
```

2.556 LP_EXE or DLL Dropped in Perflogs Folder

- **Trigger Condition:** The EXE or DLL file is dropped in Windows's Perflog directory.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=11 file IN ["*.dll", "*.exe"] path="C:\Perflogs"
```

2.557 LP_Credential Access via LaZagne

- **Trigger Condition:** Credential access via the popular open-source LaZagne tool is detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** OS Credential Dumping, LSASS Memory
- **ATT&CK ID:** T1003,T1003.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=10 call_trace="*C:\Windows\SYSTEM32\ntdll.  
↪dll+*[C:\Windows\System32\KERNELBASE.dll+*_ctypes.pyd+*python27.dll+*"
```

2.558 LP_RDP Connection Initiated from Domain Controller

- **Trigger Condition:** Initiation of RDP connection from a domain controller is detected.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Remote Services, Remote Desktop Protocol

- **ATT&CK ID:** T1021, T1021.001
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_source="Microsoft-Windows-TerminalServices-
↳ RemoteConnectionManager" event_id=1149 |
rename eventxml.param3 as source_address | search source_address IN WINDOWS_DC
```

2.559 LP_Active Directory Module Load in PowerShell

- **Trigger Condition:** Active Directory module loading in PowerShell is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, PowerShell
- **ATT&CK ID:** T1059, T1059.001
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4103 command="Import-Module" payload=
↳ "*ActiveDirectory*"
```

2.560 LP_Possible Active Directory Enumeration via AD Module

- **Trigger Condition:** Command related to retrieving the last logon date of a computer in an Active Directory (AD) is detected.
- **ATT&CK Category:** Execution, Discovery
- **ATT&CK Tag:** Remote System Discovery, Command and Scripting Interpreter, PowerShell
- **ATT&CK ID:** T1018, T1059, T1059.001
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4103 command="Get-ADComputer" payload=
↪ "*DNSHostName*LastLogonDate*"
```

2.561 LP_Microsoft Defender Disabling Attempt via PowerShell

- **Trigger Condition:** An attempt to disable Microsoft Defender via PowerShell is detected.
- **ATT&CK Category:** Defense Evasion, Execution
- **ATT&CK Tag:** Impair Defenses, Disable or Modify Tools, Command and Scripting Interpreter, PowerShell
- **ATT&CK ID:** T1562, T1562.001, T1059, T1059.001
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4104 script_block="Set-MpPreference -
↪ DisableRealtimeMonitoring $true"
```

2.562 LP_Possible Kerberoasting via Rubeus

- **Trigger Condition:** Kerberoasting attack via popular open-source tool Rubeus is detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Steal or Forge Kerberos Tickets, Kerberoasting
- **ATT&CK ID:** T1558, T1558.003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=7 -"process"="C:\Windows\System32\*" image IN [
↪ "*\clr.dll", "*\kerberos.dll", "*\cryptdll.dll", "*\dsparse.dll"] | chart distinct_
↪ count(image) as dc, distinct_list(image) as images | search dc=4
```

2.563 LP_Suspicious Scheduled Task Creation

- **Trigger Condition:** When a suspicious scheduled task creation is detected in a Windows endpoint. The suspicious task here refers to tasks running scripts or programs from temp directories or insecure locations (writable by any user). Adversaries may abuse the Windows Task Scheduler to perform task scheduling for the initial or recurring execution of malicious code to achieve persistence, lateral movement, execution, detection evasion, and privilege escalation. Also, it is prevalent among ransomware to use public directories for scheduled task creation.
- **ATT&CK Category:** Execution, Persistence, Privilege Escalation
- **ATT&CK Tag:** Scheduled Task/Job, Scheduled Task
- **ATT&CK ID:** T1053, T1053.005
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer label=Schedule label=Task label=Create command IN ["*C:\Users\*",
↪ "*C:\Windows\Temp\*", "*C:\ProgramData\*"] -command=
↪ "C:\ProgramData\Microsoft\Windows Defender\Platform\*"
```

2.564 LP_RDP Connection Initiated from Suspicious Country

- **Trigger Condition:** Initiation of RDP connection from a domain controller is detected.
- **ATT&CK Category:** Defense Evasion, Persistence, Privilege Escalation, Initial Access
- **ATT&CK Tag:** Valid Accounts, Domain Accounts
- **ATT&CK ID:** T1078, T1078.002
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_source="Microsoft-Windows-TerminalServices-
↪ RemoteConnectionManager" event_id=1149 -eventxml.param3 IN HOMENET | rename?
↪ eventxml.param3 as source_address
| process geoip(source_address) as country | search country IN SUSPICIOUS_COUNTRY
```

2.565 LP_Scheduled Task Deletion

- **Trigger Condition:** Deletion of a scheduled task using *schtasks* utility with *delete* command is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Scheduled Task
- **ATT&CK ID:** T1053.005
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
(label="process" label="create" "process"="*\schtasks.exe" command="*delete*") OR
↪(norm_id=WinServer event_id=4699 -task="*\Microsoft\Windows\RemovalTools\MRT_
↪ERROR_HB")
```

2.566 LP_Possible GootKit WScript Execution

- **Trigger Condition:** GootKit banking trojan's WScript execution activity is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, Visual Basic
- **ATT&CK ID:** T1059, T1059.003
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4688 "process"="*\wscript.exe" command="*\APPDATA\*.
↪js"
```

2.567 LP_Exchange Remote Code Execution CVE-2020-0688 Attempt

- **Trigger Condition:** A remote code execution attempt via CVE-2020-0688 in Microsoft Exchange is detected.
- **ATT&CK Category:** Initial Access

- **ATT&CK Tag:** External Remote Services
- **ATT&CK ID:** T1133
- **Minimum Log Source Requirement:** Firewall, Proxy Server
- **Query:**

```
norm_id=* (url="*/ecp/default.aspx*__VIEWSTATEGENERATOR*VIEWSTATE=*" OR
↪resource="*__VIEWSTATEGENERATOR*VIEWSTATE=*" )
```

2.568 LP_BlueKeep Vulnerability CVE-2019-0708 Exploitation

- **Trigger Condition:** The exploitation of BlueKeep, a remote desktop services remote code execution vulnerability, also known as CVE-2019-0708 is detected.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Exploitation of Remote Services
- **ATT&CK ID:** T1210
- **Minimum Log Source Requirement:** IDS/IPS
- **Query:**

```
(norm_id=Short OR norm_id=SuricataIDS) message="*Windows RDP MS_T120*"
```

2.569 LP_ZoHo ManageEngine Pre-Auth File Upload CVE-2019-8394 Exploitation Attempt

- **Trigger Condition:** A pre-auth file upload vulnerability CVE-2019-8394 in ZoHo ManageEngine ServiceDesk Plus is detected.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** Exploit Public-Facing Application
- **ATT&CK ID:** T1190
- **Minimum Log Source Requirement:** Firewall, Proxy Server
- **Query:**

```
norm_id=* request_method=POST (url='*/common/FileAttachment.jsp?
↪module=CustomLogin*' OR resource='*/common/FileAttachment.jsp?
↪module=CustomLogin*')
```

2.570 LP_ZoHo ManageEngine Desktop Central CVE-2020-10189 Exploitation Attempt

- **Trigger Condition:** A remote code execution attempt via CVE-2019-11580 in ZoHo ManageEngine Desktop Central is detected.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** Exploit Public-Facing Application
- **ATT&CK ID:** T1190
- **Minimum Log Source Requirement:** Firewall, Proxy Server
- **Query:**

```
norm_id=* request_method=POST (url='*/mdm/client/v1/mdmLogUploader*webapps*_
↪chart*' OR resource='*/mdm/client/v1/mdmLogUploader*webapps*_chart*')
```

2.571 LP_Fortinet Pre-Auth File Read CVE-2018-13379 Exploitation Attempt

- **Trigger Condition:** The exploitation of pre-auth file read vulnerability (2018-13379) in Fortinet FortiOS is detected.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** External Remote Services
- **ATT&CK ID:** T1133
- **Minimum Log Source Requirement:** Firewall, Proxy Server
- **Query:**

```
norm_id=* (url='*|lang=../../dev/cmdb/sslvpn_websession*' OR resource='*|lang=../../dev/cmdb/sslvpn_websession*')
```

2.572 LP_Adobe ColdFusion Remote Code Execution CVE-2018-15961 Attempt

- **Trigger Condition:** The exploitation of arbitrary file upload vulnerability (CVE-2018-15961) to upload JSP webshell for remote code execution in Adobe ColdFusion is detected.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** Exploit Public-Facing Application
- **ATT&CK ID:** T1190
- **Minimum Log Source Requirement:** Firewall, Proxy Server
- **Query:**

```
norm_id=* request_method=POST (url='*/cf_scripts/*/upload.cfm*' OR resource='*/cf_
↳scripts/*/upload.cfm*')
```

2.573 LP_Default Hard disk Usage Status

- **Trigger Condition:** The hard disk uses storage greater than or equal to 80%.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Logpoint
- **Query:**

```
label=Harddisk label=Usage label=Metrics use>=80
```

2.574 LP_Default License Grace State

- **Trigger Condition:** Logpoint's license has expired and is operating in grace state.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -

- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Logpoint
- **Query:**

```
norm_id=Logpoint label=Audit label=License label=Grace
```

2.575 LP_Default License Invalid

- **Trigger Condition:** 's license is no longer valid.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:**
- **Query:**

```
norm_id=LogPoint label=Audit label=License label=Invalid
```

2.576 LP_Microsoft Build Engine Loading Credential Libraries

- **Trigger Condition:** Loading of credential libraries such as *vaultcli.dll* and *SAMLib.dll* by MS Build engine is detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** OS Credential Dumping, Security Account Manager
- **ATT&CK ID:** T1003, T1003.002
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=7 "process"='*\msbuild.exe' image IN ['*\vaultcli.dll',  
↪ '\SAMLib.DLL']
```

2.577 LP_Microsoft Build Engine started by Office

- **Trigger Condition:** Execution of Microsoft Build engine by Office products is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** MSBuild
- **ATT&CK ID:** T1127.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"='*msbuild.exe' parent_process IN ['*\eqnedt32.
↪exe', '*\excel.exe', '*\ftldr.exe', '*\msaccess.exe', '*\winword.exe', '*\mspub.exe',
↪ '*\outlook.exe', '*\powerpnt.exe']
```

2.578 LP_Potential Phishing Attack Detected

- **Trigger Condition:** Phishing attack is detected
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** Phishing, Spearphishing Attachment
- **ATT&CK ID:** T1566, T1566.001
- **Minimum Log Source Requirement:** MailServer
- **Query:**

```
label=Detect label=Malicious label=File file=* sender=* receiver=* hash=*
```

2.579 LP_Safe DLL Search Mode Disabled

- **Trigger Condition:** Safe DLL search mode is disabled.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Impair Defenses, Indicator Blocking
- **ATT&CK ID:** T1562, T1562.001

- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WindowSysmon event_id=13 target_object=
↳ '*\CurrentControlSet\Control\Session Manager\SafeDllSearchMode' detail="DWORD"
↳ (0x00000000)"
```

2.580 LP_Potential Intrusion Detected

- **Trigger Condition:** An intrusion by IDS or IPS devices is detected.
- **ATT&CK Category:** Command and Control, Defense Evasion
- **ATT&CK Tag:** Proxy, Exploitation for Defense Evasion
- **ATT&CK ID:** T1090, T1211
- **Minimum Log Source Requirement:** -
- **Query:**

```
label=Intrusion label=Detect source_address=* destination_address=*
```

2.581 LP_Windows Crash Dump Disabled

- **Trigger Condition:** Windows's crash dump registry setting is disabled.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Modify Registry
- **ATT&CK ID:** T1112
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=13 target_object=
↳ "HKLM\System\CurrentControlSet\Control\CrashControl\CrashDumpEnabled" detail=
↳ "DWORD (0x00000000)"
```

2.582 LP_Suspicious Shells Spawn by SQL Server

- **Trigger Condition:** A suspicious shell process is spawned by the SQL Server process which may indicate exploitation of a vulnerability.
- **ATT&CK Category:** Initial Access, Execution
- **ATT&CK Tag:** Exploit Public-Facing Application, PowerShell
- **ATT&CK ID:** T1190, T1059.001
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4688 parent_process="*\sqlservr.exe" "process" IN [
  ↳ "\cmd.exe", "\powershell.exe", "\bash.exe", "\sh.exe", "\bitsadmin.exe"] -(parent_
  ↳ process IN ["C:\Program Files\Microsoft SQL Server\*", "*DATEV_
  ↳ DBENGINE\MSSQL\Binn\sqlservr.exe"] "process"="C:\Windows\System32\cmd.exe" ?)
  ↳ command="'C:\Windows\system32\cmd.exe" *)
```

2.583 LP_Suspicious Microsoft SQL Server PowerShell Module Use Detected

- **Trigger Condition:** A PowerShell code through the `sqlps.exe` utility, which is included in the standard set of utilities supplied with the MSSQL Server is detected.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label=Create label="Process"("process"="*\sqlps.exe" OR parent_process="*\sqlps.exe
  ↳ " OR file="*\sqlps.exe" ) -(parent_process="*\sqlagent.exe")
```

2.584 LP_HermeticWiper Driver Load

- **Trigger Condition:** When loading of HermeticWiper's driver IoC hashes is detected.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=6 (hash IN HERMETIC_WIPER_DRIVER_HASHES OR
↳ hash_sha1 IN HERMETIC_WIPER_DRIVER_HASHES OR hash_sha256 IN HERMETIC_
↳ WIPER_DRIVER_HASHES) | rename hash as ioc, hash_sha1 as ioc, hash_sha256 as ioc
```

2.585 LP_UltraVNC Execution via Command Line

- **Trigger Condition:** When UltraVNC execution via the command line is detected. Gamaredon is known to use this technique for gaining remote access.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Remote Access Software
- **ATT&CK ID:** T1219
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
norm_id=WinServer event_id=4688 command="*-autoreconnect *" command="*-
↳ connect *" command="*-id:*
```

2.586 LP_Office Security Settings Changed

- **Trigger Condition:** When modification of Microsoft Office security settings in the registry is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Modify Registry

- **ATT&CK ID:** T1112
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=13 target_object In ["*\\Security\\Trusted?
↪Documents\\TrustRecords*", "*\\Security\\AccessVBOM*", "*\\Security\\VBAWarnings*"]
```

2.587 LP_Actinium IoC Domains Detected

- **Trigger Condition:** When any Actinium IoC domain match is found. IoC Reference: Hashes are latest up to Feb 2022.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** IDS, IPS, Firewall
- **Query:**

```
domain IN ACTINIUM_DOMAINS
```

2.588 LP_Suspicious VMToolsd Child Process

- **Trigger Condition:** Creation of a suspicious child process of the VMware Tools process that may indicate persistence set up by attackers.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** T1059 - Command and Scripting Interpreter
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4688 parent_process="*\\vmtoolsd.exe" image IN ["*\\cmd.
↪exe", "*\\powershell.exe", "*\\wscript.exe", "*\\cscript.exe", "*\\rundll32.exe", "*\\regsvr32.
↪exe"] -command IN ["*\\VMware\\VMware Tools\\poweron-vm-default.bat*",
↪"*\\VMware\\VMware Tools\\poweroff-vm-default.bat*", "*\\VMware\\VMware Tools\\resume-
↪vm-default.bat*", "*\\VMware\\VMware Tools\\suspend-vm-default.bat*"]
```

2.589 LP_Impacket PsExec Execution

- **Trigger Condition:** Execution of Impacket's PsExec utility is detected. Impacket is a collection of Python classes for working with network protocols. Impacket focuses on providing low-level programmatic access to the packets and is commonly used in PoCs.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** T1570 - Lateral Tool Transfer
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=5145 share_name="IPC$" relative_target IN ["*RemCom_
↳ stdout*", "*RemCom_stdoutt*", "*RemCom_stderrt*"] -user IN EXCLUDED_USERS
```

2.590 LP_Oracle WebLogic CVE-2021-2109 Exploitation

- **Trigger Condition:** Possible exploitation of the Oracle WebLogic server vulnerability CVE-2021-2109 is detected. This vulnerability allows a high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** T1190 - Exploit Public-Facing Application
- **Minimum Log Source Requirement:** Firewall, Proxy Server
- **Query:**

```
norm_id=* request_method=GET url="*com.bea.console.handles.JndiBindingHandle*"
↳ url="*|dap://*" url="*AdminServer"
```

2.591 LP_Possible JSP Webshell Detected

- **Trigger Condition:** JSP Webshell is detected in the URL. This may indicate springshell is being exploited. However, if .jsp and .class files are commonly used in the network, the result may be false positives.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** T1505.003 - Web Shell

- **Minimum Log Source Requirement:** -
- **Query:**

```
status_code=200 request_method IN ["POST", "GET"] url in ["*.jsp*", "*.class*"]
```

2.592 LP_PowerShell ADRecon Execution

- **Trigger Condition:** Execution of the ADRecon PowerShell script for AD reconnaissance is detected. The script is reported to be actively used by FIN7. For the alert to work, the Script block logging must be enabled.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, PowerShell
- **ATT&CK ID:** T1059, T1059.001
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4104 script_block IN ["*Function Get-ADRExcelComOb*",  
↪ "*ADRecon-Report.xlsx*", "*Get-ADRGPO*", "*Get-ADRDdomainController*"]
```

2.593 LP_PowerView PowerShell Commandlets

- **Trigger Condition:** Execution of PowerShell commandlets of the popular PowerView module of the PowerSploit framework is detected. For the alert to work, the script block logging must be enabled.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** T1059 - Command and Scripting Interpreter, T1059.001 - PowerShell
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4104 script_block IN ["Export-PowerViewCSV", "Get-  
↪ IPAddress", "Resolve-IPAddress", "Convert-NameToSid", "ConvertTo-SID", "Convert-  
↪ ADName", "ConvertFrom-UACValue", "Add-RemoteConnection", "Remove-  
↪ RemoteConnection", "Invoke-UserImpersonation", "Invoke-RevertToSelf", "Request-  
↪ SPNTicket", "Get-DomainSPNTicket", "Invoke-Kerberoast", "Get-PathAcl", "Get-  
↪ DNSZone", "Get-DomainDNSZone", "Get-DNSRecord", "Get-DomainDNSRecord",  
↪ "Get-NetDomain", "Get-Domain", "Get-NetDomainController", "Get-DomainController  
↪ ", "Get-NetForest", "Get-Forest", "Get-NetForestDomain", "Get-ForestDomain", "Get-  
↪ NetForestCatalog", "Get-ForestGlobalCatalog", "Find-DomainObjectPropertyOutlier",  
↪ "Get-NetUser", "Get-DomainUser", "New-DomainUser", "Set-DomainUserPassword", "Get-  
↪ "Get-UserEvent", "Get-DomainUserEvent", "Get-NetComputer", "Get-  
↪ DomainComputer", "Get-ADObject", "Get-DomainObject", "Set-ADObject", "Set-  
↪ DomainObject", "Get-ObjectAcl", "Get-DomainObjectAcl", "Add-ObjectAcl", "Add-
```

(continued from previous page)

2.594 LP_PowerView PowerShell Commandlets

- **Trigger Condition:** Execution of PowerShell commandlets of the popular PowerView module of the PowerSploit framework is detected. For the alert to work, the script block logging must be enabled.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** T1059 - Command and Scripting Interpreter, T1059.001 - PowerShell
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4104 script_block IN ["Export-PowerViewCSV", "Get-
↪IPAddress", "Resolve-IPAddress", "Convert-NameToSid", "ConvertTo-SID", "Convert-
↪ADName", "ConvertFrom-UACValue", "Add-RemoteConnection", "Remove-
↪RemoteConnection", "Invoke-UserImpersonation", "Invoke-RevertToSelf", "Request-
↪SPNNTicket", "Get-DomainSPNNTicket", "Invoke-Kerberoast", "Get-PathAcl", "Get-
↪DNSZone", "Get-DomainDNSZone", "Get-DNSRecord", "Get-DomainDNSRecord",
↪"Get-NetDomain", "Get-Domain", "Get-NetDomainController", "Get-DomainController
↪", "Get-NetForest", "Get-Forest", "Get-NetForestDomain", "Get-ForestDomain", "Get-
↪NetForestCatalog", "Get-ForestGlobalCatalog", "Find-DomainObjectPropertyOutlier",
↪"Get-NetUser", "Get-DomainUser", "New-DomainUser", "Set-DomainUserPassword",
↪"Get-UserEvent", "Get-DomainUserEvent", "Get-NetComputer", "Get-
↪DomainComputer", "Get-ADObject", "Get-DomainObject", "Set-ADObject", "Set-
↪DomainObject", "Get-ObjectAcl", "Get-DomainObjectAcl", "Add-ObjectAcl", "Add-
↪DomainObjectAcl", "Invoke-ACLScanner", "Find-InterestingDomainAcl", "Get-NetOU",
↪"Get-DomainOU", "Get-NetSite", "Get-DomainSite", "Get-NetSubnet", "Get-
↪DomainSubnet", "Get-DomainSID", "Get-NetGroup", "Get-DomainGroup", "New-
↪DomainGroup", "Find-ManagedSecurityGroups", "Get-DomainManagedSecurityGroup
↪", "Get-NetGroupMember", "Get-DomainGroupMember", "Add-DomainGroupMember
↪", "Get-NetFileServer", "Get-DomainFileServer", "Get-DFSshare", "Get-
↪DomainDFSshare", "Get-NetGPO", "Get-DomainGPO", "Get-NetGPOGroup", "Get-
↪DomainGPOLocalGroup", "Find-GPOLocation", "Get-
↪DomainGPOUserLocalGroupMapping", "Find-GPOComputerAdmin", "Get-
↪DomainGPOComputerLocalGroupMapping", "Get-DomainPolicy", "Get-NetLocalGroup
↪", "Get-NetLocalGroupMember", "Get-NetShare", "Get-NetLoggedon", "Get-
↪NetSession", "Get-LoggedOnLocal", "Get-RegLoggedOn", "Get-NetRDPSession",
↪"Invoke-CheckLocalAdminAccess", "Test-AdminAccess", "Get-SiteName", "Get-
↪NetComputerSiteName", "Get-Proxy", "Get-WMIRegProxy", "Get-LastLoggedOn",
↪"Get-WMIRegLastLoggedOn", "Get-CachedRDPConnection", "Get-
↪WMIRegCachedRDPConnection", "Get-RegistryMountedDrive", "Get-
↪WMIRegMountedDrive", "Get-NetProcess", "Get-WMIProcess", (continues on next page)
↪"Invoke-UserHunter", "Find-DomainUserLocation", "Invoke-ProcessHunter", "Find-
↪DomainProcess", "Invoke-EventHunter", "Find-DomainUserEvent", "Invoke-ShareFinder",
↪"Find-DomainShare", "Invoke-FileFinder", "Find-InterestingDomainShareFile", "Find-
↪LocalAdminAccess", "Invoke-EnumerateLocalAdmin", "Find-DomainLocalGroupMember
↪", "Get-NetDomainTrust", "Get-DomainTrust", "Get-NetForestTrust", "Get-ForestTrust",
↪"Find-LocalAdmin", "Get-DomainLocalAdmin", "Find-LocalAdminGroup", "Get-
```

(continued from previous page)

2.595 LP_Stealthy VSTO Persistence

- **Trigger Condition:** Persistence via Visual Studio Tools for Office (VSTO) add-ins in Office application is detected.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Add-ins, Office Application Startup
- **ATT&CK ID:** T1137.006, T1137
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label=Registry label=Set target_object IN ["*\\Software\\Microsoft\\Office\\Outlook\\Addins\\*",
↪ ", "*\\Software\\Microsoft\\Office\\Word\\Addins\\*",
↪ "*\\Software\\Microsoft\\Office\\Excel\\Addins\\*",
↪ "*\\Software\\Microsoft\\Office\\Powerpoint\\Addins\\*",
↪ "*\\Software\\Microsoft\\VSTO\\Security\\Inclusion\\*" ] - "process" IN ["*\\msiexec.exe",
↪ "*\\regsvr32.exe", "*\\winword.exe", "*\\integrator.exe", "*\\OfficeClickToRun.exe",
↪ "*\\teams.exe", "C:\\Program Files\\AVG\\Antivirus\\RegSvr.exe"]
```

2.596 LP_Suspicious DLL or VBS Files being created in ProgramData

- **Trigger Condition:** When a file is created with .dll or vbs extension to the ProgramData folder. A DLL is a library containing code and data that can be used by multiple programs simultaneously. VBScript is an interpreted script language from Microsoft that is a subset of its Visual Basic programming language designed for interpretation by Microsoft's Internet Explorer web browser. Attackers use these techniques for the execution of malicious payloads. This method is predominantly used in Bumblebee attacks.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** T1204.002 - Malicious File
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=11 file IN ["*.dll", "*.vbs"] path="C:\ProgramData"
```

2.597 LP_Suspicious VMToolsd Child Process

- **Trigger Condition:** Creation of suspicious child process VMware Tools process, which may indicate persistence set up by attackers.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** T1059 - Command and Scripting Interpreter
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WinServer event_id=4688 parent_process="*\vmtoolsd.exe" image IN ["*\cmd.exe",
↪ "\powershell.exe", "\wscript.exe", "\cscript.exe", "\rundll32.exe", "\regsvr32.exe"]
↪ -command IN ["*\VMware\VMware Tools\poweron-vm-default.bat",
↪ "\VMware\VMware Tools\poweroff-vm-default.bat", "\VMware\VMware Tools\resume-vm-default.bat",
↪ "\VMware\VMware Tools\suspend-vm-default.bat"]
```

2.598 LP_Suspicious WMPRVSE Child Process

- **Trigger Condition:** A suspicious child process of WMIC is detected.
- **ATT&CK Category:** Execution, Defense Evasion
- **ATT&CK Tag:** Windows Management Instrumentation, Malicious File, Regsvr32
- **ATT&CK ID:** T1047, T1204.002, T1218.010
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create (parent_process="*\wmprvse.exe" ("process" IN [
↪ "\certutil.exe", "\cscript.exe", "\mshta.exe", "\msiexec.exe", "\regsvr32.exe",
↪ "\rundll32.exe", "\verclsid.exe", "\wscript.exe"]) OR ("process"="\cmd.exe"
↪ command IN ["*cscript*", "*mshta*", "*powershell*", "*pwsh*", "*regsvr32*", "*rundll32*",
↪ "*wscript*"])-"process" IN ["*\conhost.exe", "\WMIC.exe", "\WerFault.exe",
↪ "\wmprvse.exe"])
```

2.599 LP_TerraMaster TOS CVE-2020-28188 Exploitation

- **Trigger Condition:** The exploitation of the TerraMaster TOS vulnerability CVE-2020-28188 is detected. CVE-2020-28188 is a remote command execution (RCE) vulnerability in TerraMaster TOS <= v4.2.06 that allows remote unauthenticated attackers to inject OS commands.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** T1190 - Exploit Public-Facing Application
- **Minimum Log Source Requirement:** Firewall, Proxy Server
- **Query:**

```
norm_id=* request_method=GET url="*/include/makecvs.php*" url="**?Event=*" url IN [
  ↳ "*/curl*", "*/wget*", "*/.py*", "*/.sh*", "*/chmod*", "*/_GET*"]
```

2.600 LP_VMware VSphere CVE-2021-21972 Exploitation

- **Trigger Condition:** The exploitation of VSphere Remote Code Execution vulnerability CVE-2021-21972 is detected.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** T1190 - Exploit Public-Facing Application
- **Minimum Log Source Requirement:** Firewall, Proxy Server
- **Query:**

```
norm_id=* request_method=POST url="*/ui/vropspluginui/rest/services/uploadova*"
```

2.601 LP_VMware View Planner CVE-2021-21978 Exploitation

- **Trigger Condition:** The exploitation of the VMware View Planner vulnerability CVE-2021-21978 is detected. CVE-2021-21978 is a flaw due to proper input validation and lack of authorization leading to arbitrary file upload in Log Upload web applications.
- **ATT&CK Category:** Initial Access

- **ATT&CK Tag:** T1190 - Exploit Public-Facing Application
- **Minimum Log Source Requirement:** Firewall, Proxy Server
- **Query:**

```
norm_id=* request_method=POST url="*logupload*" url="*logMetaData*" url="*wsgi_
↳log_upload.py"
```

2.602 LP_Zoho ManageEngine ADSelfService Plus CVE-2021-40539 Exploitation

- **Trigger Condition:** The REST API authentication bypass vulnerability (CVE-2021-40539) in Zoho ManageEngine ADSelfService Plus (v6113 and prior) is detected. For the detection to work, Administrators must fetch logs from the `\ManageEngine\ADSelfService Plus\logs` path.
- **ATT&CK Category:** Initial Access, Persistence
- **ATT&CK Tag:** T1190 - Exploit Public-Facing Application, T1505.003 - Web Shell
- **Minimum Log Source Requirement:** Web Server
- **Query:**

```
url=* url IN ["*/help/admin-guide/Reports/ReportGenerate.jsp*", "*/RestAPI/
↳LogonCustomization*", "*/RestAPI/Connection*"]
```

2.603 LP_Possible Access to ADMIN Share

- **Trigger Condition:** Access to \$ADMIN share that may help detect lateral movement attempts is detected. Since Windows Admin Share activity is so common, it provides adversaries with a powerful, discreet way to move laterally within an environment. Self-propagating ransomware and cryptocurrency miners, both rapidly emerging threats, rely on Windows Admin Shares. Suppose an adversary can obtain legitimate Windows credentials. The hidden shares (C\$, ADMIN\$, and IPC\$) can be accessed remotely via server message block (SMB) or the Net utility to transfer files and execute code. Windows Admin Shares are often used in conjunction with behaviors relating to Remote File Copy (T1105)—because adversaries commonly use the technique to copy files remotely—and Network Share Discovery (T1135). It can also occur with New Service (T1050) and Service Execution (T1035) because tools like PsExec deploys their receiver executable to admin shares, scheduling a service to execute it. Legitimate administrative activities may generate false positives and will require whitelisting.

- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** T1021.002 - SMB/Windows Admin Shares
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=5140 share_name="Admin$" -user="*$" -user IN EXCLUDED_USERS
```

2.604 LP_PsExec Tool Execution Detected

- **Trigger Condition:** PsExec service installation and execution events (service and Sysmon) are detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** System Services, Service Execution
- **ATT&CK ID:** T1569, T1569.002
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
(norm_id=WinServer service="PSEXESVC" (event_id=7045 event_source="Service Control Manager" file="PSEXESVC.exe")
OR (event_id=7036)) OR (label=file label=create file=PSEXESVC.exe) OR (event_id IN [17, 18] pipe="\PSEXESVC*")
```

2.605 LP_Screensaver Activities Detected

- **Trigger Condition:** Adversaries's modification of registry key containing the path to binary used as screensaver executable is detected to establish persistence.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** T1546 - Event Triggered Execution, T1546.002 - Screensaver
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon (event_id=12 or event_id=13 or event_id=14) (target_object=
↳ "*\\Control Panel\\Desktop\\SCRNSAVE.exe") (parent_command!="*explorer.exe" or
↳ image!="*rundll32.exe" or command!="*shell32.dll, Control_RunDLL desk.cpl,
↳ ScreenSaver, *") -user IN EXCLUDED_USERS
```

2.606 LP_Suspect Svchost Activity Detected

- **Trigger Condition:** Svchost activity is detected. It is abnormal for svchost.exe to spawn without any CLI arguments and is normally observed when a malicious process spawns the process and injects code into the process memory space.
- **ATT&CK Category:** Privilege Escalation, Defense Evasion
- **ATT&CK Tag:** T1055 - Process Injection
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 image="*\\svchost.exe" parent_image=* -parent_
↳ image IN ["*\\rpcnet.exe", "*\\rpcnetp.exe", "*\\svchost.exe", "*\\Mrt.exe", "*\\MsMpEng.
↳ exe"] command=* command="*\\svchost.exe" -user IN EXCLUDED_USERS
```

2.607 LP_Time-Stomping of Users Directory Files Detected

- **Trigger Condition:** Time-stomping of user directory file is detected. Sysmon can only detect a change of CreationTime and not LastWriteTime and LastAccessTime. Whitelisting legitimate noisy processes like browsers, Slack, or Teams are required to reduce false positives.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1070 - Indicator Removal on Host, T1070.006 - Timestomp
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=2 path="C:\\Users*" -source_image IN ["*\\iexplore.exe
↳ ", "*\\cortana*", "*\\StartMenuExperienceHost.exe", "C:\\Windows\\system32\\cleanmgr.exe
↳ ", "C:\\Windows\\Explorer.EXE", "*\\LocalBridge.exe", "*\\svchost.exe", "*\\RuntimeBroker.
↳ exe", "*\\msedge.exe", "*\\SearchApp.exe", "C:\\Windows\\system32\\ServerManager.exe
↳ ", "*\\ServiceHub.RoslynCodeAnalysisService32.exe"] -path=
↳ "*\\AppData\\Roaming\\Microsoft\\Windows\\Recent\\CustomDestinations\\*.*" (continues on next page)
↳ EXCLUDED_USERS
```

(continued from previous page)

2.608 LP_Windows Defender Exclusion Set Detected

- **Trigger Condition:** Added Windows Defender exclusion in the registry where an entity bypasses antivirus scanning from Windows Defender.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1562 - Impair Defenses, T1562.001 - Disable or Modify Tools
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_source="Microsoft-Windows-Windows Defender" event_  
↪ id=5007 new_value="HKLM\\SOFTWARE\\Microsoft\\Windows Defender\\Exclusions\\*"
```

2.609 LP_Suspicious Netsh DLL Persistence Detected

- **Trigger Condition:** Detects persistence via Netsh Helper.
- **ATT&CK Category:** Privilege Escalation
- **ATT&CK Tag:** Netsh Helper DLL
- **ATT&CK ID:** T1546.007
- **Minimum Log Source Requirement:** Window Sysmon, Windows
- **Query:**

```
(label=Registry label=Set label=Value target_object="*\\SOFTWARE\\Microsoft\\Netsh\\*")  
↪ OR (label="process" label=create "process"="*\\netsh.exe" command="*add*"  
↪ command="*helper*")
```

2.610 LP_Usage of Procdump Detected

- **Trigger Condition:** Suspicious use of the SysInternals ProcDump utility tool is detected.
- **ATT&CK Category:** Credential Access

- **ATT&CK Tag:** OS Credential Dumping, LSASS Memory
- **ATT&CK ID:** T1003, T1003.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Create" label="Process" "process" IN ["*\procdump.exe", "*\procdump64.exe"]  
↪ command IN ["* -ma*", "* /ma*"]
```

2.611 LP_Conhost Spawning Suspicious Processes

- **Trigger Condition:** *conhost.exe* spawns other processes.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1202 - Indirect Command Execution
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
label="Process" label="Create" "parent_process"="*\conhost.exe" "process"=*
```

2.612 LP_Proxy Execution via Explorer

- **Trigger Condition:** *explorer.exe* is used in *cmd.exe* to proxy execution.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1202 - Indirect Command Execution
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
label="process" label="Create" "parent_process"="*\cmd.exe" "process"="*\explorer.exe"  
↪ "command"="*explorer*"
```

2.613 LP_Wlrmldr Lolbin Use as Launcher

- **Trigger Condition:** *wlrmldr.exe* is used to proxy launch other executables.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1202 - Indirect Command Execution
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
label="process" "process"="*\wlrmldr.exe" - "parent_process"="*\winlogon.exe"
↪ command IN ['*-s *', '*-f *', '*-t *', '*-m *', '*-a *', '*-u *']
```

2.614 LP_Suspicious Process Execution via Pester Detected

- **Trigger Condition:** Detects code execution via *Pester.bat* (Pester - Powershell Module for testing).
- **ATT&CK Category:** Defense Evasion, Execution
- **ATT&CK Tag:** T1059.001 - PowerShell, T1216 - Signed Script Proxy Execution
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label="create" label="process" event_source="Microsoft-Windows-Sysmon" (
↪ "process"="*\powershell.exe" command="*Pester*Get-Help*") OR ("process"=
↪ "C:\Windows\System32\cmd.exe" command="*pester*;" command IN ["*help*",
↪ "*?*"])
```

2.615 LP_Root Certificate Installation Detected

- **Trigger Condition:** Adversaries may install a root certificate on a compromised system to avoid warnings when connecting to adversary-controlled web servers. This alert can detect the installation of a root certificate.
- **ATT&CK Category:** Defense Evasion

- **ATT&CK Tag:** T1553.004 - Install Root Certificate
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label="Create" label="Process" event_source="Microsoft-Windows-Sysmon"
↪ command="*root*" ("process"="C:\Windows\System32\certutil.exe" command=
↪ "*-addstore*") OR ("process"="*CertMgr.exe" command="*/add*") | norm on
↪ command <certificate:'\S+.cer'>
```

2.616 LP_Suspicious process spawned by FTP

- **Trigger Condition:** *ftp.exe* is used to file transfer, but it can be abused by spawning a new process using *ftp.exe*. The alert detects; renamed *ftp.exe*, *ftp.exe* script execution, and child processes run by *ftp.exe*.
- **ATT&CK Category:** Execution, Defense Evasion
- **ATT&CK Tag:** T1059 - Command and Scripting Interpreter, T1202 - Indirect Command Execution
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label="create" label="process" event_source="Microsoft-Windows-Sysmon"
↪ (command="*-s.*" ("process"="C:\Windows\System32\ftp.exe" OR file="*ftp.exe*
↪ ")) OR (file="*ftp.exe*" - "process"="C:\Windows\System32\ftp.exe") OR parent_
↪ process="C:\Windows\System32\ftp.exe"
```

2.617 LP_Chromeloader Cross-Process Injection to Load Extension

- **Trigger Condition:** Chromeloader uses process injection using PowerShell and loads the malicious extension in Chrome.
- **ATT&CK Category:** Execution, Persistence, Privilege Escalation
- **ATT&CK Tag:** T1055 - Process Injection, T1059.001 - PowerShell, T1176 - Browser Extensions

- **Minimum Log Source Requirement:** -
- **Query:**

```
label="Process" label=Create parent_process="*powershell" parent_command = "*-exe* byp*  

↳ -win* hid* -e* JAB*" command IN ["*--load-extension=*", "*Appdata\\local\\chrome*"]  

↳ "process" = "*chrome"
```

2.618 LP_Proxy Execution via Explorer

- **Trigger Condition:** When Explorer is used to proxy execution. Explorer is a Microsoft Windows GUI shell used for task-based file management systems. Adversaries uses Explorer to proxy the execution of other commands or processes, evading defense mechanisms.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1202 - Indirect Command Execution
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="process" label=Create "process"="*\explorer.exe" "command"="*explorer*"
```

2.619 LP_Suspicious Root Certificate installation Detected

- **Trigger Condition:** Installation of a root certificate is detected. Adversaries may install a root certificate on a compromised system to avoid warnings when connecting to adversary-controlled web servers. However, sometimes Help Desk or IT may need to add a corporate Root CA on occasion manually. So they need to test if the GPO push doesn't trigger a False Positive.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1553.004 - Install Root Certificate
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="create" label="process" (command="*root*" (("process"="*\certutil.exe" command=
↪ "*-addstore*") OR ("process"="*\CertMgr.exe" command="*/add*"))))
```

2.620 LP_Windows Logon Reminder Usage as Launcher

- **Trigger Condition:** When *Wlrmldr* is used to proxy launch other executables. *Wlrmldr* (Windows Logon Reminder) is a Microsoft Windows Binary used by Microsoft to display messages at login. Adversaries uses *Wlrmldr* to pass parameters to *ShellExecute*.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1202 - Indirect Command Execution
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="process" label=create "process"="*\wlrmldr.exe" -"parent_process"="*\winlogon.exe" ⓘ
↪ command IN ['*-s *', '*-f *', '*-t *', '*-m *', '*-a *', '*-u *']
```

2.621 LP_Suspicious File Transfer Using Replace

- **Trigger Condition:** *Replace* is used to transfer (copy or download files) files. *Replace.exe* is a Microsoft Windows executable that allows replacing existing or adding new files in a directory if used with the */a* option. Adversaries uses the *replace* process to silently download or copy files in the target system.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1105 - Ingress Tool Transfer
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="process" label=create "process"="*\replace.exe" command IN ["*/a*", "*-a*"]
```

2.622 LP_Proxy Execution via Program Compatibility Wizard

- **Trigger Condition:** Pcwrn process is used to initiate a proxy execution. Pcwrn is a Microsoft Windows Operating System file used to invoke Program Compatibility Troubleshooter/Wizard. Adversaries uses pcwrn to proxy the execution of other commands, processes, or executables in order to evade defense mechanisms. However, the specific focus needs to be on outlier events, for example unique counts, instead of commonly seen artifacts to prevent false positives.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1218 - Signed Binary Proxy Execution
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label=create label="process" parent_process="*\pcwrn.exe"
```

2.623 LP_Suspicious Driver Installation via PnPUtl

- **Trigger Condition:** Pnputil process is used to install or add drivers. PnPUtl is a Microsoft Windows process that lets an administrator perform actions on driver packages. Adversaries uses pnputil to install or add malicious drivers. Anyone who uses pnputil.exe who is not a system administrator should be investigated, even when they have system change permissions.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** T1547 - Boot or Logon Autostart Execution, T1547.006 - Kernel Modules and Extensions
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="process" label=create "process"="*\pnputil.exe" command IN ["*-i*", "*/install*", "*/add-driver*", "*/inf*"]
```

2.624 LP_Application Whitelisting Bypass via PresentationHost

- **Trigger Condition:** Presentationhost process is used to execute browser applications. Presesntationhost is a Microsoft Windows application that enables the hosting of WPF applications in compatible browsers (including Microsoft Internet Explorer 6 and later). Adversaries uses presentationhost.exe to evade application whitelisting and execute malicious XAML Browser Application (XBAP) files.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1218 - Signed Binary Proxy Execution
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="process" label=create "process"="*\presentationhost.exe" command="*.xbap"
```

2.625 LP_Suspicious File Extraction via Expand Detected

- **Trigger Condition:** Expand process is used for file transfer (copy or download files). Expand is a Microsoft Windows binary file provided by Microsoft that can extract one or more compressed files and retrieve them from distribution disks. Adversaries uses expand to silently download or copy files into the target system or location.
- **ATT&CK Category:** Defense Evasion, Command and Control
- **ATT&CK Tag:** T1105 - Ingress Tool Transfer, T1218 - Signed Binary Proxy Execution
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="process" label=create "process"="*\expand.exe" command IN ["*.cab*", "*/F:*", "*/F:*  
↪", "*/C:\ProgramData\*", "*/C:\Public\*", "*/AppData\Local\Temp\*",  
↪ "*/AppData\Roaming\Temp\*"]
```

2.626 LP_Suspicious Use of Extrac32 Detected

- **Trigger Condition:** Suspicious file overwrite using `extrac32.exe` is detected.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Ingress Tool Transfer
- **ATT&CK ID:** T1105
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="Create" label="Process" "process"="*\extrac32.exe" command="*\extrac32*"
↪command IN ["*/C*", "*/Y*", "*/\\*"]
```

2.627 LP_Shell spawn via HTML Help Detected

- **Trigger Condition:** *Hh* (HTML Help) spawns shell processes. *Hh.exe* is a Microsoft Windows executable program that allows developers to compile .chm file(s) with expanding tables of contents, shortcuts, keyword search, and pop-up topics. Adversaries uses *Hh* as a target for overwriting and executing their malicious commands, spawning other processes.
- **ATT&CK Category:** Execution, Defense Evasion
- **ATT&CK Tag:** T1047 - Windows Management Instrumentation, T1218.001 - Compiled HTML File
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="process" label=create parent_process="*\hh.exe" "process" IN ["*\cmd.exe",
↪ "*/powershell.exe", "*/wscript.exe", "*/cscript.exe", "*/regsvr32.exe", "*/wmic.exe",
↪ "*/rundll32.exe"]
```

2.628 LP_DLL Injection with Tracker Detected

- **Trigger Condition:** DLL injection with the tracker process is detected. *Tracker.exe* is a legitimate internal Windows binary file required to incrementally generate resources like building on a 64-bit OS using 32-bit MSBuild. Adversaries can use it

to bypass application whitelisting solutions by proxy execution of an arbitrary DLL into another process.

- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1055.001 - Dynamic-link Library Injection
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="create" label="process" (("process"="*\tracker.exe" OR description="Tracker")  
↪command="*/d*" command="*/c*")
```

2.629 LP_Powershell Code Execution via SyncAppvPublishingServer

- **Trigger Condition:** Arbitrary Powershell command is executed via SyncAppvPublishingServer. VBScript files, such as SyncAppvPublishingServer.vbs, are trusted scripts, often signed with certificates. Adversaries can use SyncAppvPublishingServer.vbs to proxy execute PowerShell code.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1216 - Signed Script Proxy Execution, T1218 - Signed Binary Proxy Execution
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label='create' label='process' command='*\SyncAppvPublishingServer.vbs*' command='*,*'
```

2.630 LP_Malicious PE Execution by Microsoft Visual Studio Debugger

- **Trigger Condition:** Arbitrary Powershell command is executed via SyncAppvPublishingServer. VBScript files, such as SyncAppvPublishingServer.vbs, are trusted scripts, often signed with certificates. Adversaries can use SyncAppvPublishingServer.vbs to proxy execute PowerShell code.
- **ATT&CK Category:** Defense Evasion

- **ATT&CK Tag:** T1218 - Signed Binary Proxy Execution
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="Create" label="Process"(parent_process="*\vsjitdebugger.exe" -(("process"=
↪ ".*\vsimmersiveactivatehelper*.exe" OR "process"=".*\devenv.exe")))
```

2.631 LP_Suspicious Atbroker Registry Change Detected

- **Trigger Condition:** Creation or modification of Assistive Technology (AT) registry value is detected. Atbroker is a Windows internal helper binary that provides accessibility tools like screen readers, speech input and text readers, people with disabilities use to accomplish tasks. Adversaries can modify the assistive technology registry value and include their malicious application to maintain persistence.
- **ATT&CK Category:** Persistence, Defense Evasion
- **ATT&CK Tag:** T1218 - Signed Binary Proxy Execution, T1547 - Boot or Logon Autostart Execution
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon label=Registry label=Set target_object IN [
↪ ".*\Software\Microsoft\Windows NT\CurrentVersion\Accessibility\ATs*",
↪ ".*\Software\Microsoft\Windows NT\CurrentVersion\Accessibility\Configuration*"]
```

2.632 LP_DLL loaded Via Certoc Binary Detected

- **Trigger Condition:** DLL loading is detected using certoc binary. Certoc is Windows internal binary used to install certificates, but it also has a feature to load a DLL by LoadDll tag. Adversaries can use certoc binary to load their malicious DLL even when they don't have the relevant access rights.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1218 - Signed Binary Proxy Execution
- **Minimum Log Source Requirement:** Windows, Windows Sysmon

- **Query:**

```
label="Process" label=Create command="*certoc.exe*" command IN ["* -LoadDll *", "* /
↳ LoadDll *"] command="*.dll*"
```

2.633 LP_Suspicious Remote Binary Usage Detected

- **Trigger Condition:** remote.exe binary is used to bypass application whitelisting and execute or run a local or remote file. Remote.exe is a Windows binary server/client tool that allows users to run command-line programs on remote computers. Adversaries can use the remote.exe binary to spawn a new Powershell session, AWL bypass, and execute other commands.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1127 - Trusted Developer Utilities Proxy Execution
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="Process" label="Create" "process"="*\remote.exe" command="*/s *"
```

2.634 LP_Suspicious ASP NET Compiler Execution Detected

- **Trigger Condition:** A file with the extension .jse, .vbe, .js, or .vba is executed using wscript or cscript. Wscript and cscript are Windows binaries that provide an environment in which users can execute scripts in various languages or start a script to run in a command-line environment. Adversaries can code malicious scripts in .jse, .vbe, .js, or .vba files and execute them using wscript or cscript and bypass detection.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1127 - Trusted Developer Utilities Proxy Execution
- **Minimum Log Source Requirement:** -
- **Query:**

```
label=Create label="Process" "process" = "C:\Windows\Microsoft.NET\Framework*" "process"
↳ "*"aspnet_compiler.exe"
```

2.635 LP_Suspicious LoadAssembly PowerShell Diagnostic Script Execution

- **Trigger Condition:** Microsoft signed script is used to execute commands and bypass AppLocker. CL_LoadAssembly.ps1, a windows native diagnostic script, provides two functions (LoadAssemblyFromNS and LoadAssemblyFromPath) for loading .NET/C# assemblies (DLLs/EXEs). An attacker can bypass Constrained Language mode by invoking PowerShell version 2 (Note: this must be enabled) and bypass AppLocker by loading an assembly through CL_LoadAssembly.ps1.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1216 - Signed Script Proxy Execution
- **Minimum Log Source Requirement:** -
- **Query:**

```
command IN ["*\CL_LoadAssembly.ps1", "*LoadAssemblyFromPath*"] "Process" =
↳ "*"powershell.exe"
```

2.636 LP_Suspicious Invocation PowerShell Diagnostic Script Execution

- **Trigger Condition:** The execution of malicious payloads via SyncInvoke in CL_Invocation.ps1 module is detected. CL_Invocation is a PowerShell Diagnostic script, but an attacker can import it and then call SyncInvoke to launch a malicious executable.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1216 - Signed Script Proxy Execution
- **Minimum Log Source Requirement:** -
- **Query:**

```
command IN ["*\CL_Invocation.ps1 ", "*SynclInvoke*"] "Process"="*\powershell.exe"
```

2.637 LP_Registry Configured RunOnce Task Execution

- **Trigger Condition:** The RunOnce task executes as configured in the registry. Runonce.exe is a Microsoft Windows Operating System component called the *Run Once Wrapper Utility* that allows the installation program to reboot after initial start up to enable the user to make further configurations. Adversaries uses the runonce executable to evade defense mechanisms while running their programs/code through registry entries in the host machine.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1112 - Modify Registry
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="process" label=create "process"="*\runonce.exe" command="* /AlternateShellStartup*
↪ "
```

2.638 LP_RunOnce Registry Key Configuration Change

- **Trigger Condition:** When the configuration of Run Once registry key is changed. Runonce.exe is a Microsoft Windows Operating System component called the *Run Once Wrapper Utility* that allows the installation program to reboot after initial start up to enable the user to make further configurations. Adversaries uses/changes the runonce registry key values to evade defense mechanisms while running their programs/code in the host machine.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1112 - Modify Registry
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label="process" label=create "process"="*\runonce.exe" command="* /AlternateShellStartup*
↪ "
```

2.639 LP_Suspicious WSL Bash Execution

- **Trigger Condition:** When bash is used to execute the Linux command. Bash is a Unix shell and command language. Adversaries can use bash to execute a specified file or commands in the Windows subsystem for Linux and can be used as a defensive evasion mechanism. Executing programs using bash can trigger this alert, so alerts must be further analyzed to determine legitimate or illegitimate use.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1202 - Indirect Command Execution
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Create" label="Process" command="*bash* -c *
```

2.640 LP_WSL Execution Detected

- **Trigger Condition:** When Windows subsystem for Linux (WSL) binary is used to execute Linux commands. WSL is a compatibility layer that allows running Linux binaries in Windows. Adversaries can use the wsl binary to execute Windows and Linux binaries, execute arbitrary Linux commands as root without a password or download files.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1202 - Indirect Command Execution
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Create" label="Process" "process"="*\wsl.exe" command in ["*-e *", "--exec *"]
```

2.641 LP_Suspicious Usage of Csharp or Roslyn Csharp Interactive Console

- **Trigger Condition:** When the use of csi and rcsi binary are detected. Csi.exe is a Microsoft signed binary that provides C# interactive capabilities. Rcsi.exe is a Microsoft signed binary that can execute C# code. Adversaries can use these binaries to execute their malicious C# code.

- ```
label="Create" label="Process" ("process" IN ["*\csi.exe", "*\rcsi.exe"]) OR (file in ["csi.exe",
↪ "rcsi.exe"])
```

- **Trigger Condition:** Suspicious characters in the command indicating possible command obfuscation is detected. Adversaries leverage this technique by using multiple Unicode characters to obfuscate the command they are executing to bypass signature-based detections.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Obfuscated Files or Information
- **ATT&CK ID:** T1027
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create ((parent_process="*\cmd.exe" parent_command IN ["**^/^/^/^/^/^
→ ", "**set*=call*%*%", 's^e^t*"]) OR (command IN [{"?}*","?*?", "?*", "*/", "*/*", "?*",
→ "*_*", "*â*", "*€*", "*£*", "*~*", "*®*", "*μ*", "*¶*"])))
```

- **Trigger Condition:** Process events related to emotet is created.
- **ATT&CK Category:** Defense Evasion, Execution
- **ATT&CK Tag:** Obfuscated Files or Information, PowerShell
- **ATT&CK ID:** T1027, T1059.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create (command IN ["* -e* PAA*",
↪ "*JABIAG4AdgA6AHUAacwBIAHIAcABYAG8AZgBpAGwAZQ*",
↪ "*QAZQBuAHYAogB1AHMAZQByAHAAcgbvAGYAaQBsaGUA*",
↪ "*kAGUAbgB2ADoAdQBzAGUAcgBwAHIAbwBmAGkAbABIA*",
↪ "*IgAoACcAKgAnACkAOwAkA*", "*IAKAAnACoAJwApADsAJA*",
↪ "*iACgAJwAqACcAKQA7ACQA*", "*JABGAGwAeABYAGgAYwBmAGQ*"]) (-command IN [
↪ "fAAgAEMAbwBuAHYAZQByAHQAVABvAC0ASgBzAG8AbgAgAC0ARQByAHIAbwByAEEAYwB0AGkAbwBu",
↪ ",
↪ "wAIBDAG8AbgB2AGUAcgB0AFQAbwAtAEoAcwBvAG4AIAAtAEUAcgByAG8AcgBBAGMAdABpAG8Abg",
↪ ",
↪ "8ACAAQwBvAG4AdgBIAHIAdABUAG8ALQBKAHMABwBuACAALQBFAHIAcgbvAHIAQQBjAHQAaQBvAG",
↪ "]) -user IN EXCLUDED_USERS
```

## 2.644 LP\_Suspicious Use of Control Panel Items

- **Trigger Condition:** Malicious use of a control panel item is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Control Panel
- **ATT&CK ID:** T1218.002
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create (((("process"="*\reg.exe" OR file="reg.exe") command="*add*"
↪ command="*CurrentVersion\Control Panel\CPLs*") OR (command="*.cpl" -(command IN [
↪ "*\System32*", "%System%*"]) OR (command="*regsvr32 *" command="*/s *" command=
↪ "*igfxCPL.cpl*")))))
```

## 2.645 LP\_Suspicious Use of CSharp Interactive Console Detected

- **Trigger Condition:** The execution of the CSharp interactive console by using PowerShell is detected. Adversaries can run CSharp interactive console from PowerShell and execute their malicious code.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1127 - Trusted Developer Utilities Proxy Execution

- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label="Create" "process"="*\csi.exe" file="csi.exe" parent_process=
↳ ".*\powershell.exe"
```

## 2.646 LP\_Suspicious Use of Colorcpl Detected

- **Trigger Condition:** Suspicious usage of colorcpl binary such as execution from non default path and creation of unusual files are detected.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** T1574.001 - DLL Search Order Hijacking
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
(label="Process" label="Create" -"process"="C:\Windows\System32\colorcpl.exe" "process"=
↳ ".*\colorcpl.exe") OR (norm_id=WindowsSysmon event_id=11 image=".*\colorcpl.exe" file In [
↳ ".*.icm", ".*.gmmp", ".*.cdmp", ".*.camp"])
```

## 2.647 LP\_Suspicious File Download via Certreq

- **Trigger Condition:** When a file is downloaded using certreq binary. Certreq is a Windows binary used to manage and request a certificate from the certificate authority. Adversaries can use certreq to download payload from their C2 server.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** T1105 - Ingress Tool Transfer
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label="Create" "process"="*\certreq.exe" command=".*certreq*" command
↳ IN ["* -Post *", " /Post *"] command IN ["* -config *", " /config *"] command=".* http*"
↳ command=".* C:\windows\win.ini *
```

## 2.648 LP\_Process Dump via Rundll32 and Comsvcs

- **Trigger Condition:** When LSASS dump using Rundll32 with Comsvcs DLL is detected. *Rundll32.exe* is a Windows binary that loads and runs 32-bit dynamic-link libraries. *comsvcs.dll* is a DLL file used by COM+ Services created by Microsoft. Adversaries can use the binary and DLL to dump the LSASS process.
- **ATT&CK Category:** Defense Evasion, Credential Access
- **ATT&CK Tag:** LSASS Memory, Rundll32
- **ATT&CK ID:** T1003.001, T1218.011
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create ("process"="*\rundll32.exe" or file="RUNDLL32.EXE")
↪command="*comsvcs*" command="*full*" command IN ["*#-*", "*#+*", "*#24*", "*24 *",
↪"*MiniDump*"]
```

## 2.649 LP\_Registry Key Import Detected

- **Trigger Condition:** When registry key import is detected via regedit.exe. Regedit is a Windows binary to access and manipulate the Windows registry. This hierarchical database stores low-level settings for the Microsoft Windows operating system and applications that opt to use the registry. A registry key is an organizational unit in the Windows registry. Adversaries can use Regedit to import their malicious registry key to achieve persistence.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1112 - Modify Registry
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="Process" label="Create" "process"="*\regedit.exe" OR file="regedit.exe" command
↪IN ["*/i *", "*/j *"] command="*.reg*" -command IN ["*/e *", "*/a *", "*/c *", "*/-e *", "*/-a *", "*/-
↪c *"]
```

## 2.650 LP\_Suspicious MachineGUID Query Detected

- **Trigger Condition:** When reg.exe is used to detect query machine GUID. Reg.exe is a Windows binary that performs operations on registry subkey information and values in registry entries. MachineGUID is a unique identifier for a machine. Adversaries can use this technique to get MachineGuid information. Also, ransomware abuses this technique to keep track of infected systems using a unique ID.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** T1082 - System Information Discovery
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="Process" label="Create" "process"="*reg.exe" command="* query *" command=
↳ "*SOFTWARE\Microsoft\Cryptography*" command IN ["*/v *", "*-v *"] command=
↳ "*MachineGuid*"
```

## 2.651 LP\_Process Injection Via Mavinject Detected

- **Trigger Condition:** When DLL is injected into a running process. Microsoft Application Virtualization Injector (Mavinject) is a Windows utility that can inject code into external processes as part of Microsoft Application Virtualization (App-V). Adversaries can use mavinject to inject malicious DLL to obtain arbitrary code execution.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1218.013 - Mavinject
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="Process" label="Create" "process"="*\mavinject.exe" command IN ["* /injectrunning*",
↳ "* -injectrunning*", "*.dll*"]
```

## 2.652 Possible File Transfer Using Finger Detected

- **Trigger Condition:** When the execution of Finger.exe is detected. It is a simple Windows binary that displays user information on a specified remote computer running the Finger service or daemon. It can be abused as a data transfer tool and makeshift C2 channel. However, general administrative use can trigger false positives, but it is still unclear why they use finger.exe.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** T1105 - Ingress Tool Transfer
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="process" label="create" "process"="*\finger.exe"
```

## 2.653 LP\_Suspicious Use of Findstr Detected

- **Trigger Condition:** When suspicious actions such as credential access, file download, or creation of alternate data stream using findstr are detected. Generally, it is used to search for strings in files or to filter command line output. Adversaries can exploit it for defense evasion. However, general administrative use of findstr can trigger false positives.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1218 - Signed Binary Proxy Execution
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="create" label="process" "process"="*\findstr.exe" command="*findstr*" ((command=
↪ "*/V*" command="*/L*") OR (command="*/S*" command="*/I*"))
```

## 2.654 LP\_Suspicious File Overwrite Using extrac32 Detected

- **Trigger Condition:** When suspicious actions such as credential access, file download, or creation of alternate data stream using findstr are detected.

Generally, it is used to search for strings in files or to filter command line output. Adversaries can exploit it for defense evasion. However, general administrative use of findstr can trigger false positives.

- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1218 - Signed Binary Proxy Execution
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="create" label="process" "process"="*\findstr.exe" command="*findstr*" ((command=
↪ "*/V*" command="*/L*") OR (command="*/S*" command="*/I*"))
```

## 2.655 LP\_Suspicious Sysmon Driver Unload Detected

- **Trigger Condition:** When suspicious unload of SysmonDrv Filter Driver is detected. Fltmc.exe program is a system-supplied command line utility for mini-filter driver management operations. Adversaries can abuse its functionality to unload the filter driver, which can affect sysmon and stop from collecting the data.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1070 - Indicator Removal on Host, T1562 - Impair Defenses, T1562.002 - Disable Windows Event Logging
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="process" label="create" "process"="*\fltmc.exe" command="*unload*" command =
↪ "*sys*"
```

## 2.656 LP\_Suspicious Execution via IE per User Utility

- **Trigger Condition:** When ie4uinit is executed from unusual file directories. ie4uinit.exe (Internet Explorer (for) Each User Initialization) file is a software component of Internet Explorer by Microsoft Corporation. Adversaries generally abuse ie4uinit.exe to overwrite malicious programs on it and spread them via the internet to execute them on target machines as legitimate processes.
- **ATT&CK Category:** Defense Evasion

- **ATT&CK Tag:** T1218 - Signed Binary Proxy Execution
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="process" label="create" ("process"="*\ie4unit.exe" OR file="ie4unit.exe") -(path IN [
↪ "C:\Windows\System32\","C:\Windows\SysWOW64\"])
```

## 2.657 LP\_Proxy Execution via xWizard

- **Trigger Condition:** When the execution of the xWizard tool with runwizard and CLSID arguments are utilized to achieve proxy execution. xWizard is Windows internal binary used to run the Windows component object model (COM). COM is operated to enable inter-process communication. Class ID (CLSID) is a unique number representing a single application component in windows. Adversaries can bypasses the defense mechanism by proxying the execution of malicious content via xWizard.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1218 - System Binary Proxy Execution
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*\xwizard.exe" | process regex("(?P<new_
↪command>{\w{8}-\w{4}-\w{4}-\w{4}-\w{12}})",command) | filter new_command=*
```

## 2.658 LP\_Suspicious MSHTA Process Pattern

- **Trigger Condition:** When suspicious *mshta.exe* process patterns, such as binary run from a non-default path, *mshta.exe* binary masquerading as different binary, and execution of HTML application (HTA) masquerading as non-HTA file are detected. *Mshta.exe* is a utility that executes HTA files. HTAs are standalone applications based on HTML and VBScript that can access local system resources, run scripts and display dynamic content. Adversaries may abuse *mshta.exe* to evade defense by proxy, executing malicious files and Javascript or VBScript through a trusted Windows utility.
- **ATT&CK Category:** Defense Evasion, Execution

- **ATT&CK Tag:** Mshta, Native API
- **ATT&CK ID:** T1218.005, T1106
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create "process"="*\mshta.exe"
((parent_process IN ["*\cmd.exe", "powershell.exe"] OR command IN ["*\AppData\Local*",
↪ "C:\Windows\Temp*", "C:\Users\Public*"]) OR (-"process" IN ["C:\Windows\System32*",
↪ "C:\Windows\SysWOW64*"]) OR (-command IN ["*\mshta.exe", "mshta"] -command IN ["*.
↪ htm*", "*.hta*"]))
```

## 2.659 LP\_COM Object Execution via Shell Extension CLSID Verification Host

- **Trigger Condition:** When verclsid.exe is used to run COM object via GUID. Verclsid.exe (Verify COM Shell Extension CLSID) is a Microsoft Windows Native Shell Extension CLSID (Class ID) verification host responsible for verifying each shell extension before Windows Explorer or the Windows Shell uses them. Adversaries may abuse verclsid.exe to execute malicious payloads-COM Scriptlets, by running verclsid.exe and referencing files by Class ID (CLSID), a unique identification number used to identify COM objects.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label="create" "process"="*\verclsid.exe" command="*/C*" command="*/S*"
↪ "
```

## 2.660 LP\_Suspicious Setup Information File Invoked via DefaultInstall

- **Trigger Condition:** When InfDefaultInstall.exe is used to install an INF file. InfDefaultInstall.exe is a Microsoft Windows native tool invoked when an INF (Setup Information) file is selected to install. Adversaries uses InfDefaultInstall to install on the target system through maliciously crafted INF files.

- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1562.001 - Disable or Modify Tools
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label="create" "process"="*\InfDefaultInstall.exe" command=
↪ "InfDefaultInstall*" command="*.inf"
```

## 2.661 LP\_Creation of Alternate Data Stream

- **Trigger Condition:** When an alternate data stream is created. Alternate Data Stream (ADS) is the ability of an NTFS file system to store different streams of data, in addition to the default stream, which is used for a file. Attackers can leverage a little-known compatibility feature to hide hacking tools, keyloggers, and other malware on a compromised system and subsequently execute them undetected. Also, it can be used for data exfiltration. The alert requires the ADS\_FILE\_EXTENSIONS list to work.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1564.004 - NTFS File Attributes
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
(label="create" label="process" command IN ADS_FILE_EXTENSIONS ((command="*type *"
↪ command="* > *") OR (command="*makecab*" command="*.cab*") OR (command="*reg
↪ *" command="* export *") OR (command="*diantz.exe*" command="*.cab*") OR
↪ (command="*regedit*" command="*/E *") OR (command="*print*" command IN ["/D:*",
↪ "*/d:*"]) OR (command="*expand*") OR (command="*extrac32*" command="*.cab*") OR
↪ (command="*curl*" command IN ["*--output*", "*-o*"]) OR (command="*certutil*"
↪ command="*-urlcache*") OR (command="*esentutl*" command="*/y*" command="*/d*")
↪ OR (command="*esentutl*" command="*/y*" command="*/d*" command="*/o *"))
↪ OR (label="create" label="file" file in ADS_FILE_EXTENSIONS)
```

## 2.662 LP\_Alternate Data Stream Created using Findstr

- **Trigger Condition:** When findstr is used to create an alternate data stream. Findstr is generally used to search for strings in files or to filter command line output. Adversaries can exploit it to create an alternate data stream for defense evasion. For this alert to work, the ADS\_FILE\_EXTENSIONS list is required.

- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1564.004 - NTFS File Attributes
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
[label="create" label="process" "process"="*\findstr.exe" command="*\findstr*" ((command=
↪ "*/V*" command="*/L*") OR (command="*/S*" command="*/I*"))] as s1 followed by [label=
↪ "Create" label="File" file in ADS_FILE_EXTENSIONS] as s2 on s1.process_id=s2.process_id [?]
↪ rename s1.process as "process", s1.log_ts as log_ts, s1.command as command, s1.host as host,
↪ s1.user as user, s1.parent_process as parent_process
```

## 2.663 LP\_Suspicious Download Using Diantz

- **Trigger Condition:** When a remote file is downloaded using diantz.exe and stored by compressing it into a .cab file on a local machine. It performs a similar function as makecab.exe, which compresses a file into a smaller file with a .cab file extension. Adversaries can use diantz.exe for ingress tool transfer to evade the defenses and establish a c2 connection.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** T1105 - Ingress Tool Transfer
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Create" label="Process" command="*\diantz.exe*" command="**" command="*.*.
↪ cab"
```

## 2.664 LP\_Ngrok RDP Tunnel Detected

- **Trigger Condition:** When it detects the execution of Ngrok utility for tunneling RDP connection. Threat actors often use Ngrok to expose internal services to the internet, like making RDP publicly accessible. 16777216 artifact gets logged when an incoming RDP connection is established via ngrok.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** T1572 - Protocol Tunneling

- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer ((event_source IN ["Microsoft-Windows-TerminalServices-
↪ LocalSessionManager", "Microsoft-Windows-TerminalServices-RemoteConnectionManager
↪"]) OR (channel=Security event_id=4779)) (source_address="::%16777216" OR eventxml.
↪address="::%16777216") | rename eventxml.address as source_address
```

## 2.665 LP\_Ngrok Execution

- **Trigger Condition:** When it detects the execution of the Ngrok utility used for port forwarding and protocol tunneling. Threat actors often use Ngrok to expose internal services to the internet, like making RDP publicly accessible.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** T1572 - Protocol Tunneling
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="Process" label=Create (("process"="*\ngrok.exe" command IN ["* tcp *", "* http *", "*?
↪ authtoken *"]) OR (command="* start *" command="*--all*" command="*.yaml*" command=
↪ "*--config*") OR (command IN ["* tcp 139*", "* tcp 445*", "* tcp 3389*", "* tcp 5985*", "*?
↪ tcp 5986*"])))
```

## 2.666 LP\_Windows Defender Uninstall via PowerShell

- **Trigger Condition:** When PowerShell is used to uninstall Windows Defender. PowerShell is a Microsoft task automation and configuration management program consisting of a command-line shell with its scripting language. Microsoft Defender Antivirus is an anti-malware component of Microsoft Windows. Adversaries can use this technique to avoid the detection of their malware.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1562 - Impair Defenses
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*\powershell.exe" command="*Uninstall-
↳ WindowsFeature*Name*Windows-Defender*"
```

## 2.667 LP\_Hijacked Binary Execution via Settings Synchronizer

- **Trigger Condition:** When SettingSyncHost is used to run hijacked binaries. SettingSyncHost is a Microsoft Windows host process that synchronizes system settings with other devices, including Internet Explorer, a mail application, OneDrive, Xbox and other application settings. Adversaries can exploit SettingSyncHost to run hijacked binaries and other specified files.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1574.008 - Path Interception by Search Order Hijacking
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label="create" - "process" IN ["C:\Windows\System32*",
↳ "C:\Windows\SysWOW64*"] parent_command IN ["*cmd.exe /c*", "*cmd /c*"] parent_
↳ command="*RoamDiag.cmd*" parent_command="*-outputpath*"
```

## 2.668 LP\_Suspicious Execution of Dump64

- **Trigger Condition:** When suspicious use of dump64.exe is detected. dump64.exe is a memory dump tool bundled with Microsoft Visual Studio. Adversaries can leverage it to create a memory dump and parse it offline to retrieve credentials. Adversaries can bypass Microsoft Defender by renaming a tool to dump64.exe and placing it in a Visual Studio folder, for example, procdump.exe. It can trigger false positives if dump64.exe is executed from any folder other than excluded one, even for a legitimate purpose.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** T1003.001 - LSASS Memory
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label="create" "process"="*\dump64.exe" (-("process"=
↪ " *\Installer\Feeback\dump64.exe*") OR command IN ["*-ma *", "*accpeteula*"])
```

## 2.669 LP\_Code Compilation via Visual Basic Command Line Compiler

- **Trigger Condition:** When a successful compilation of code using Visual Basic Command Line Compiler is detected. vbc.exe is Microsoft's Visual Basic compiler used to compile programs within the Visual Studio integrated development environment (IDE). Adversaries can leverage it to collect malicious code on the system to bypass defensive countermeasures. The legitimate use of this tool can trigger false positives, but it is barely used in enterprise environments, so the detection of service is suspicious.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1027.004 - Compile After Delivery
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Create" label="Process" parent_process="*\vbc.exe" "process"="*\cvtres.exe"
```

## 2.670 LP\_File Downloaded from Suspicious URL Using GfxDownloadWrapper

- **Trigger Condition:** When downloading files from suspicious (non-standard) URLs using GfxDownloadWrapper.exe is detected. Intel Graphics Executable Download Wrapper (GfxDownloadWrapper) is an application file that allows you to update your graphics card module. It downloads JSON files from <https://gameplayapi.intel.com>. Adversaries can leverage its functionality to download files from other non-standard URLs.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** T1105 - Ingress Tool Transfer
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Create" label="Process" "process"="*\GfxDownloadWrapper.exe" - command=
↪ "*gameplayapi.intel.com*" - parent_process="*\GfxDownloadWrapper.exe"
```

## 2.671 LP\_Suspicious CLR Logs File Creation

- **Trigger Condition:** When .NET code is executed via applications, such as mshta, cscript, wscript, regsvr32 and wmic. .NET is a developer platform with tools and libraries for building applications, including web, mobile, desktop, games, IoT, cloud, and microservices. Common Language Runtime in a .NET environment runs code and provides services to make the development process more manageable. The binaries included in the query are Windows internal binary which adversaries can use to execute their malicious scripts.
- **ATT&CK Category:** Privilege Escalation
- **ATT&CK Tag:** T1055 - Process Injection
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label=File label=Create label=Overwrite path="*\AppData\Local\Microsoft\CLR*\UsageLogs*"
↪ " file IN ["mshta*", "cscript*", "wscript*", "regsvr32*", "wmic*"]
```

## 2.672 LP\_CLR DLL Loaded via Scripting Application

- **Trigger Condition:** When Common Language Runtime (CLR) DLL is loaded via scripting applications. mshta.exe, wscript.exe and cscript.exe are Windows internal binary. Common Language Runtime works in the .NET environment, which runs the code and provides services that make the development process more manageable. Adversaries can use this technique to execute malicious scripts.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1218.005 - Mshta
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label=image label=load source_image IN ["*\wscript.exe", "cscript.exe", "mshta.exe"] ⓘ
↪ image IN ["*\clr.dll", "mscorlib.dll", "mscorlib.dll"]
```

## 2.673 LP\_Obfuscation Script Usage via MSHTA to Execute Vbscript

- **Trigger Condition:** When execution of invoke-obfuscation PowerShell script with mshta to execute vbscript is detected. mshta.exe file is a software component of Windows Internet Explorer that runs HTML application(HTA) files. Invoke Obfuscation is a PowerShell command and script obfuscation framework. VBScript is an Active Scripting language developed by Microsoft modeled on Visual Basic. Adversaries can use this technique to bypass defensive mechanisms.
- **ATT&CK Category:** Defense Evasion, Execution
- **ATT&CK Tag:** T1027 - Obfuscated Files or Information, T1059.001 - PowerShell
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create command=* | process regex("(?P<new_command>(?!).*(&&
↪).*(mshta).*(vbscript:createobject).*(\\.run).*(\\window\\.close\\.)*",command) | filter new_
↪command=*
```

## 2.674 LP\_Microsoft Defender Logging Disabled

- **Trigger Condition:** When Windows Defender Registry key is modified to disable Windows Defender's logging. Windows Defender is an anti-malware component of Microsoft Windows. Adversaries use this technique to disable logs generated from Windows Defender and avoid detection.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1562 - Impair Defenses
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label=Registry label=Value label=Set target_object=
↪"*\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\WINEVT\\Channels\\Microsoft-Windows-
↪Windows Defender\\Operational\\Enabled" detail="DWORD (0x00000000)"
```

## 2.675 LP\_UAC Bypass via CMLUA or CMSTPLUA

- **Trigger Condition:** When user CMLUA OR CMSTPLUA DLL is loaded to perform user account control (UAC) bypass.
- **ATT&CK Category:** Privilege Escalation
- **ATT&CK Tag:** T1548.002 - Bypass User Account Control
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id="WindowsSysmon" label=Image label=Load image IN ["*\cmlua.dll", "*\cmstplua.dll",
↪ "\cmluautil.dll"] - "process" IN ["*\cmstp.exe", "*\cmmgr32.exe"] - "process" IN [
↪ "\windows*", "*\program files*"]
```

## 2.676 LP\_High Number of Service Stop or Task Kill in Short Span

- **Trigger Condition:** Over ten task kill, service stop or delete events are detected. Adversaries can use this technique to kill, stop or delete services or processes that might otherwise hinder their payload execution. Ransomware is seen as deleting or blocking processes or services before starting the encryption process.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Service Stop
- **ATT&CK ID:** T1489
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="process" label=create (("process" = "\taskkill.exe" (command= "f" command="im *
↪ ") OR command="IM ") OR ("process" IN ["\sc.exe", "\net.exe", "\net1.exe"]
↪ command="stop") OR ("process" = "\sc.exe" command IN ["delete", "disabled"])) -
↪ user IN EXCLUDED_USERS | chart count() as occurrence by user,host,domain,"process",
↪ parent_process | search occurrence > 10
```

## 2.677 LP\_LSA Protected Process Light Disabled

- **Trigger Condition:** When modification of the registry value of Protection Process Light (PPL) to disable, it is detected. Protected Process can be accessed by executables that are digitally signed with a unique Windows Media, with administrator privilege. Protected Process Light is an extension of a protected process where a process can be assigned a different level of protection. Adversaries can use this technique to access the LSASS process and dump it to retrieve credentials.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1112 - Modify Registry
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label=Registry label=Set label=Value target_object=
→ "*\\System\\CurrentControlSet\\Control\\Lsa\\RunAsPPL " detail="DWORD (0x00000000) "
```

## 2.678 LP\_Suspicious Invocation of Microsoft Workflow Compiler

- **Trigger Condition:** When the use of Microsoft Workflow Compiler is detected. Microsoft Workflow Compiler is a utility included by default in the .NET framework, capable of compiling and executing arbitrary, unsigned C# or VB.net code. Adversaries can leverage it for the proxy execution of executables to evade detection. The use of MWC in an enterprise environment is highly unlikely. However, legitimate use can trigger false positives.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1127 - Trusted Developer Utilities Proxy Execution
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label="create" ("process"="*\\Microsoft.Workflow.Compiler.exe" OR (file=
→ "Microsoft.Workflow.Compiler.exe" command="*.xml*"))
```

## 2.679 LP\_Process Dump via Sqldumper Detected

- **Trigger Condition:** When a process dump via Sqldumper.exe is detected. The Sqldumper.exe is a debugging utility, included with Microsoft SQL Server, which generates memory dumps of SQL Server and of related processes for debugging purposes. Adversaries can leverage its functionality to dump processes like LSASS. Legitimate MSSQL Server actions can trigger false positives.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** T1003 - OS Credential Dumping, T1003.001 - LSASS Memory
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label="create" "process"="*\sqldumper.exe" command IN ["*0x0110*",
↪ "*0x01100:40*"]
```

## 2.680 LP\_Suspicious Usage of SQLToolsPS Detected

- **Trigger Condition:** When the proxy execution of PowerShell code through the SQLToolsPS.exe is detected. SQLToolsPS.exe is a utility shipped along with Microsoft SQL Server Management Studio that loads SQL Server cmdlts. Adversaries can leverage its functionality to execute malicious powershell codes and bypass the detection methods. Direct execution of PowerShell codes via SQLToolsPS.exe are uncommon. However, the child process sqltoolsps.exe spawned by smss.exe is a legitimate action.
- **ATT&CK Category:** Execution, Defense Evasion
- **ATT&CK Tag:** T1059.001 - PowerShell, T1127 - Trusted Developer Utilities Proxy Execution
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label="create" (("process"="*\sqltoolsps.exe" OR parent_process=
↪ "*\sqltoolsps.exe") OR (file="*\sqltoolsps.exe" -(parent_process="*\smss.exe")))
```

## 2.681 LP\_Proxy Execution of Malicious Payload via Pubprn

- **Trigger Condition:** When proxy execution of malicious payloads via PubPrn.bs is detected. PubPrn.vbs is a signed Visual Basic script that publishes a printer to Active Directory Domain Services. Adversaries can abuse PubPrn to execute malicious payloads hosted on remote sites.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1216.001 - PubPrn
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label="create" command="*\pubprn.vbs*" command="*script:*
```

## 2.682 LP\_File Download via IMEWDBLD

- **Trigger Condition:** When a network connection is detected via the IMEWDBLD.exe binary. IMEWDBLD.EXE is a part of Microsoft Input Method Editor (IME). IME is a software component that enables a user to enter text in a language that can't easily be typed using a standard keyboard. Adversaries can use this technique to download remote system payload.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** T1105 - Ingress Tool Transfer
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label=Connection label=Network label=Detect "process"="*\IMEWDBLD.exe" is_initiated=true
```

## 2.683 LP\_Memory Dump via Adplus

- **Trigger Condition:** When LSASS process dump via adplus.exe is detected. Local Security Authority Server Service (LSASS) is a process in Microsoft Windows operating systems that is responsible for enforcing the security policy on the system and handles authentication, password change and tokens. ADPlus is a console-based Visual Basic script included with Microsoft Debugging Tools for Windows installation. Adversaries may attempt to access credentials stored in the process memory of the LSASS.

- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** T1003.001 - LSASS Memory
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create "process"="*\adplus.exe" command IN ["*-hang *", "*-pn *",
↳ "*-pmn *", "*-p *", "*-po *", "*-c *", "*-sc *"]
```

## 2.684 LP\_Remote Thread Created via Ttdinject

- **Trigger Condition:** When a remote thread is created by ttdinject binary. Ttdinject is a binary that is a part of the Time Travel Debugging utility, which is used in Windows 10 v1809. Time Travel Debugging is a tool that captures a process trace as it executes and allows to replay it later. Adversaries can use this technique to proxy execute malicious payloads.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1127 - Trusted Developer Utilities Proxy Execution
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create ("process"="*\ttdinject.exe" OR file="TTDInject.exe")
```

## 2.685 LP\_Proxy Download via OneDriveStandaloneUpdater

- **Trigger Condition:** When OneDriveStandaloneUpdater registry value is modified. OneDriveStandaloneUpdater.exe is a binary that belongs to the Standalone Updater process and comes with Microsoft OneDrive. Adversaries can use this technique for transferring tools or other files to the victim system from a URL that is set in the OneDriveStandaloneUpdater registry. Registry auditing must be enabled and permission must be allowed for auditing the OneDriveStandaloneUpdater registry.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** T1105 - Ingress Tool Transfer
- **Minimum Log Source Requirement:** Windows Sysmon

- **Query:**

```
label=registry label=value label=set target_object=
↪ "*"SOFTWARE\Microsoft\OneDrive\UpdateOfficeConfig\UpdateRingSettingURLFromOC*"
```

## 2.686 LP\_Suspicious WMIC ActiveScriptEventConsumer Created

- **Trigger Condition:** When WMIC is executed to create an event consumer. ActiveScriptEventConsumer is a class that runs a predefined script in an arbitrary scripting language when an event is delivered to it. Adversaries may establish persistence and elevate privileges by executing malicious content triggered by a Windows Management Instrumentation (WMI) event subscription.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** T1546.003 - Windows Management Instrumentation Event Subscription
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create command="*ActiveScriptEventConsumer*" command="*?
↪ CREATE *"
```

## 2.687 LP\_Remote Connection Established via Msbuild

- **Trigger Condition:** When a network connection is initiated via MSBuild while building an application is detected. Microsoft Build (MSBuild) Engine is a platform for building applications. Adversaries can use this technique to build their payload and establish a network connection to their controlled server.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** MSBuild
- **ATT&CK ID:** T1127.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=windowssysmon "process"="*\msbuild.exe" event_id=3 destination_port IN ["80",
↪ "443"]
```

## 2.688 LP\_Executables Started in Suspicious Folder

- **Trigger Condition:** When the execution of binaries from a suspicious folder is detected. Paths mentioned in lists are not Windows default paths from where native and internal binaries are executed. Adversaries may attempt to masquerade their payload as legitimate binaries and execute from non-default paths to avoid detection. Legitimate binaries executed from those paths can trigger an alert, so include those binaries in the excluded process list.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1036 - Masquerading
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label="process" label=create "process" IN SUSPICIOUS_FOLDER_EXE_EXECUTION
-"process" IN ["*SpeechUXWiz.exe", "*SystemSettings.exe", "*TrustedInstaller.exe",
↪ "*PrintDialog.exe",
"*MpSigStub.exe", "*LMS.exe", "*mpam-*.exe"]
```

## 2.689 LP\_Windows RDP Port Modified

- **Trigger Condition:** When remote desktop protocol (RDP) for Windows protocol is modified. RDP is a protocol that allows users to have GUI access to a remote desktop. Adversaries can modify the RDP port to evade the defense mechanism used to detect connections in the default RDP port.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** T1021.001 - Remote Desktop Protocol
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label=Registry label=Value label=Set target_object=
↪ "*\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\PortNumber"
```

## 2.690 LP\_Curl Silent Mode Execution Detected

- **Trigger Condition:** When curl is run in silent mode. Client URL (curl) is a command line tool that is used to transfer data to and from a server. Adversaries can use this technique to prevent showing file transfer progress and redirect output to a file.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** T1105 - Ingress Tool Transfer
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create command="*curl*" ((command="*-s*" command="*-o*") OR
↪ command="*-s*")
```

## 2.691 LP\_High Volume of File Modification or Deletion in Short Span

- **Trigger Condition:** When 30 file modifications or deletions are detected within a single minute. A large number of file modifications and deletions is an indicator of ransomware. Based on requirements and the number of detected false positives, a user can modify the number of events needed or the time frame. To generate logs, enable the auditing policy of the relevant folders. When a user/software modifies a large number of files this can result in a false positive. To reduce the number of false positives events exclude the process in the query.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** T1565 - Data Manipulation
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
[30 label=File label=Object label=Storage access IN ["Delete*", "writedata*"] - "process" IN [
↪ "*\tiworker.exe", "*\poqexec.exe", "*\msiexec.exe"] having same host,domain,user, "process
↪ " within 1 minutes]
```

## 2.692 LP\_Non-Existent User Login Attempt Detected

- **Trigger Condition:** When eight non-existent user login attempts on SSH service are detected within a minute. Secure Shell (SSH) is a protocol that provides a secure way to access a computer over a network. Adversaries can perform username brute force to find a valid username. Based on the requirement and false positive, the user can modify the number of invalid login attempts and time frame.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** T1110 - Brute Force
- **Minimum Log Source Requirement:** Unix
- **Query:**

```
[8 label=Invalid label=User "process"=sshd having same source_address within 1 minutes]
```

## 2.693 LP\_Execution of Temporary Files Via Office Application

- **Trigger Condition:** When Office applications creates a child process that executes a file with .tmp extension. Adversaries uses this technique to avoid detection by using the legit application to run a payload that is masquerading as a temporary file.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1036 - Masquerading
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label="Create" "parent_process" IN ["*\winword.exe", "*\powerpnt.exe",
↪ "*\excel.exe"] "process"="*.tmp"
```

## 2.694 LP\_Execution of Temporary Files Via Office Application

- **Trigger Condition:** When Office applications creates a child process that executes a file with .tmp extension. Adversaries use this technique to avoid detection by

using the legit application to run a payload that is masquerading as a temporary file.

- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1036 - Masquerading
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label="Create" "parent_process" IN ["*\winword.exe", "\powerpnt.exe",
↪ "\excel.exe"] "process"="*.tmp"
```

## 2.695 LP\_Malicious Image Loaded Via Excel

- **Trigger Condition:** When an unsigned image is loaded via Excel. An XLL file is an add-in used by Microsoft Excel. It contains extra functions, templates, or other tools that enhance the capabilities of Excel. Examples of add-ins include custom chart generators and template managers. Adversaries can use this technique to load their malicious unsigned add-ins to execute their payload or download malware from a remote server.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** T1137 - Office Application Startup, T1137.001 - Office Template Macros
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label=Image label=Load "process"="*\excel.exe" file IN ["*.xlam ", "*.xla ", "*.xll "] is_sign=false
```

## 2.696 LP\_Malicious Chrome Extension Detected

- **Trigger Condition:** When malicious Chrome extension IDs are detected by Osquery. This analytic relies on chrome\_extensions table and requires analysts to keep an up-to-date list of malicious chrome extension IDs.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** T1176 - Browser Extensions

- **Minimum Log Source Requirement:** -
- **Query:**

```
event_source=OSQuery event_type=chrome_extension* columns_identifier IN MALICIOUS_
↳ CHROME_EXTENSIONS
```

## 2.697 LP\_Chrome Extension Installed Outside of the Webstore

- **Trigger Condition:** When malicious chrome extensions are installed from outside the official Chrome webstore. Adversaries can manually install the browser extension via their batch, PowerShell or VBS scripts. Analysts need to make sure they place the correct event types in the query.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** T1176 - Browser Extensions
- **Minimum Log Source Requirement:** -
- **Query:**

```
event_source=OSQuery event_type="chrome_extension*" columns_from_webstore=false
```

## 2.698 LP\_Chrome Extension Installed with DevTools Permission

- **Trigger Condition:** When OSQuery detects the chrome extension installed with devtools permission. Analyst must check for unusual extensions installed with this permission and also check if the extensions were installed from the webstore.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** T1176 - Browser Extensions
- **Minimum Log Source Requirement:** -
- **Query:**

```
event_source=OSQuery event_type="chrome_extension*" columns_permission="*devtools*"
```

## 2.699 LP\_Suspicious WMIC Process Creation

- **Trigger Condition:** When WMIC executes "Process Call Create," suspicious calls to processes such as, rundll32, regsrv32, mshta. The WMI command-line (WMIC) utility provides a command-line interface for Windows Management Instrumentation (WMI). WMI is a Microsoft technology that provides a common framework for managing and monitoring Windows-based systems. Adversaries can use this technique to proxy execute their malicious files and payloads via wmic.exe.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** T1047 - Windows Management Instrumentation
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create command="process" command=call command=create
command IN ["*rundll32*", "*bitsadmin*", "*regsvr32*", "*cmd.exe /c *", "*cmd.exe /k *", "*cmd.
↪ exe /r *", "*cmd /c *", "*cmd /k *",
"*cmd /r *", "*powershell*", "*pwsh*", "*certutil*", "*cscript*", "*wscript*", "*mshta*",
↪ "*\Users\Public*", "*\Windows\Temp*", "*\AppData\Local*", "*%temp%*", "*%tmp%*", "*
↪ %ProgramData%*", "*%appdata%*", "*%comspec%*", "*%localappdata%"]
```

## 2.700 LP\_Browser Credential Files Accessed

- **Trigger Condition:** When access to a browser (Chrome, Edge & Firefox) using stored credential is detected. When a user saves any credentials in the browser, those credentials are stored in files that are included in the query. Adversaries can access those files in an attempt to retrieve the stored credentials.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1202 - Indirect Command Execution
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label=File label=Access ((path IN ["*\\AppData\\Local\\Google\\Chrome\\User
↪Data\\Default\\Network\\Cookies*", "*\\Appdata\\Local\\Chrome\\User Data\\Default\\Login Data*",
↪"*\\AppData\\Local\\Google\\Chrome\\User Data\\Local State*"] object_name IN [
↪"*\\Appdata\\Local\\Microsoft\\Windows\\WebCache\\WebCacheV01.dat", "*\\cookies.sqlite"])
OR object_name IN ["*\\Microsoft\\Edge\\User Data\\Default\\Web Data", "*\\Firefox*release\\logins.
↪json", "*\\firefox*release\\key3.db", "*\\firefox*release\\key4.db"])
- "process" IN ["*\\firefox.exe", "*\\chrome.exe", "C:\\Program Files*", "C:\\Program Files (x86)*",
↪"C:\\WINDOWS\\system32*", "*\\MsMpEng.exe", "*\\MpCopyAccelerator.exe", "*\\thor64.exe",
↪"*\\thor.exe"] -parent_process IN ["C:\\Windows\\System32\\msiexec.exe"] -("process"=system
↪parent_process=idle) "access"="ReadData"
```

## 2.701 LP\_Windows Defender Antivirus Definitions Removal Detected

- **Trigger Condition:** When Microsoft Defender Antivirus signature definitions are removed from the system. Microsoft Defender Antivirus (formerly Windows Defender) offers protection against all threats on Windows devices. The Malware Protection Command Line Utility (MpCmdRun) is a Microsoft Windows internal command-line tool dedicated to automating and managing Microsoft Defender Antivirus operations on Windows devices. Adversaries leverages this method to remove Antivirus definitions and ultimately avoid detection.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1562.001 - Disable or Modify Tools
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create "process"="*\\MpCmdRun.exe" command="*RemoveDefinitions*
↪"
```

## 2.702 LP\_Exchange ProxyShell Pattern Detected

- **Trigger Condition:** When a URL pattern associated with ProxyShell exploitation attempts (both successful and failure) against Exchange servers is detected. ProxyShell is an attack chain that exploits three known vulnerabilities in Microsoft Exchange: CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207. Adversaries may exploits these vulnerabilities to perform remote code execution.
- **ATT&CK Category:** Initial Access

- **ATT&CK Tag:** T1190 - Exploit Public-Facing Application
- **Minimum Log Source Requirement:** Webserver
- **Query:**

```
norm_id=* ((url="*/autodiscover.json*" url IN ["/powershell*", "*/mapi/nsapi*", "*/EWS*", "X-
↪ Rps-CAT*"]) OR url IN ["*/autodiscover.json?*", "*/autodiscover.json%3f@*", "*/%3f@foo.com*
↪ ", "*/Email=autodiscover/autodiscover.json*", "*/json?@foo.com*"])
```

## 2.703 LP\_Successful Exchange ProxyShell Attack

- **Trigger Condition:** When a URL pattern and status code associated with a successful ProxyShell exploitation attack against Exchange servers are detected. ProxyShell is an attack chain that exploits three known vulnerabilities in Microsoft Exchange: CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207. Adversaries may exploit these vulnerabilities to perform remote code execution.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** T1190 - Exploit Public-Facing Application
- **Minimum Log Source Requirement:** Webserver
- **Query:**

```
norm_id=* (url="*/autodiscover.json*" url IN ["/powershell*", "*/mapi/nsapi*", "*/EWS*", "X-
↪ Rps-CAT*"] status_code IN [200, 301])
```

## 2.704 LP\_Malicious Base64 Encoded PowerShell Keywords in Command Lines Detected

- **Trigger Condition:** When base64 encoded strings are used in hidden malicious Command and Scripting Interpreter and PowerShell command lines. Adversaries hides their activities by encoding commands to bypass detection with this technique.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** T1059 - Command and Scripting Interpreter, T1059.001 - PowerShell
- **Minimum Log Source Requirement:** Windows Sysmon, Windows

- **Query:**

```
label="process" label=create "process"="*\powershell.exe" command IN ["* hidden *",
↳ "*AGkAdABzAGEAZABtAGkAbgAgAC8AdABYAGEAbgBzAGYAZQByA*",
↳ "*aXRzYWRtaW4gL3RyYW5zMVY*",
↳ "*IAaQB0AHMAYQBkAG0AaQBuACAALwB0AHIAyQBuaHMAZgBIAHIA*",
↳ "*JpdHNhZG1pbIAvdHJhbnNmZX*",
↳ "*YgBpAHQAacwBhAGQAbQBpAG4AIAAvAHQAacgBhAG4AcwBmAGUAacg*",
↳ "*Yml0c2FkbWlucC90cmFuc2Zlc*", "*AGMAaAB1AG4AawBfAHMAaQB6AGUA*",
↳ "*JABjAGgAdQBuaGsAXwBzAGkAegBIA*", "*JGNodW5rX3Npem*",
↳ "*QAYwBoAHUAbgBrAF8AcwBpAHoAZQ*", "*RjaHVua19zaXpI*", "*Y2h1bmtfc2l6Z*",
↳ "*AE8ALgBDAG8AbQBwAHIAZQBzAHMAaQBvAG4A*",
↳ "*kATwAuAEMAbwBtAHAacgBIAHMAcwbPAG8Abg*", "*IPLkNvbXByZXNzaW9u*",
↳ "*SQBPAC4AQwBvAG0AcABYAGUAacwBzAGkAbwBuA*", "*SU8uQ29tcHJlc3Npb2*",
↳ "*Ty5Db21wcmVzc2lvc*", "*AE8ALgBNAGUAbQBvAHIAeQBTahQAacgBIAgEAbQ*",
↳ "*kATwAuAE0AZQBtAG8AcgB5AFMAcABYAGUAYQBtA*", "*IPLk1lbW9yeVN0cmVhb*",
↳ "*SQBPAC4ATQBIAG0AbwByAHkAUwB0AHIAZQBhAG0A*", "*SU8uTWVtb3J5U3RyZWFT*",
↳ "*Ty5NZW1vcnltDhJiYW*", "*4ARwBIAHQAQwBoAHUAbgBrA*", "*5HZXRDaHVua*",
↳ "*AEcAZQB0AEMAaAB1AG4Aaw*", "*LgBHAGUAdABDAGgAdQBuaGsA*",
↳ "*LkdldENodW5r*", "*R2V0Q2h1bm*", "*AEgAUgBFAEEARABfAEkATgBGAE8ANgA0A*",
↳ "*QASABSAEUAAQQBEAF8ASQBOAEYATwA2ADQA*", "*RIUkVBRF9JTkZPNj*",
↳ "*SFJFQURfSU5GTzY0*", "*VABIAFIARQBBAEQAXwBJAE4ARgBPADYANA*",
↳ "*VEhSRUFEX0lOrk82N*",
↳ "*AHIAZQBhAHQAQZQBSAGUAbQBvAHQAQZQBUAGgAcgBIAgEAZA*",
↳ "*cmVhdGVhZGVzZW1vdGVUaHJiYW*",
↳ "*MAcGBlAGEAdABIAFIAZQBtAG8AdABIAFQAaABYAGUAYQBkA*",
↳ "*NyZWFOZVJlbW90ZVRocmVhZ*", "*Q3JIYXRlUmVtb3RlVGHYzWFk*",
↳ "*QwByAGUAYQB0AGUAUgBIAg0AbwB0AGUAUVABoAHIAZQBhAGQA*",
↳ "*0AZQBtAG0AbwB2AGUA*", "*1lbW1vdm*", "*AGUAbQBtAG8AdgBIA*",
↳ "*bQBIAG0AbQBvAHYAZQ*", "*bWVtbW92Z*", "*ZW1tb3Zl"] -user IN EXCLUDED_USERS
```

## 2.705 LP\_DLL Loaded Via AllocConsole and RunDLL32

- **Trigger Condition:** When DLL loading through allocconsole function and rundll32. AllocConsole is a Windows internal function that allocates a new console for the calling process. Rundll32.exe is a Windows internal binary that loads and runs 32-bit dynamic-link libraries (DLLs). Adversaries can use this technique to execute their payload using rundll32 to load a malicious DLL by invoking the AllocConsole function.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1218.011 - Rundll32
- **Minimum Log Source Requirement:** Windows Sysmon, Windows

- **Query:**

```
label="process" label=create "process" = "*\\rundll32.exe" command="*.dll*" command=
↳ "*allocconsole*"
```

## 2.706 LP\_Active Directory Database Dump Attempt

- **Trigger Condition:** When an attempt to dump the *ntds.dit* file is detected. *NTDS.dit* file is a database that stores the Active Directory data (including users, groups, security descriptors and password hashes). Adversaries can use this technique to retrieve credentials and obtain other domain information.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** T1003.003 - NTDS
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create(("process" IN ["*\\NTDSDump.exe", "*\\NTDSDumpEx.exe"]) OR
(command="*ntds.dit*" command="*system.hiv*") OR (command="*NTDSgrab.ps1*")) OR
↳ (command="*ac i ntds*"
command="*create full*") OR (command="*/c copy *" command="*\\windows\\ntds\\ntds.dit*")
↳ OR
(command="*activate instance ntds*" command="*create full*") OR (command="*powershell*"
↳ " command="*ntds.dit*") OR
(command="*ntds.dit*" "process" IN
["*\\apache*", "*\\tomcat*", "*\\AppData*", "*\\Temp*", "*\\Public*", "*\\PerfLogs*"] OR
↳ "parent_process" IN
["*\\apache*", "*\\tomcat*", "*\\AppData*", "*\\Temp*", "*\\Public*", "*\\PerfLogs*"])
```

## 2.707 LP\_Suspicious Child Process Creation via OneNote

- **Trigger Condition:** When the creation of suspicious child processes, execution of binaries from non-default paths and script file execution through OneNote are detected. Adversaries can use malicious OneNote files to social engineer users to execute it and drop their malicious payload or execute commands in the victim system.
- **ATT&CK Category:** Initial Access, Execution
- **ATT&CK Tag:** T1204.002 - Malicious File, T1566.001 - Spearphishing Attachment

- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 parent_image="*\onenote.exe"
(file IN ["RUNDLL32.exe", "REGSVR32.exe", "bitsadmin.exe", "CertUtil.exe", "InstallUtil.exe",
↪ "schtasks.exe", "wmic.exe", "cscript.exe", "wscript.exe", "CMSTP.EXE", "Microsoft.Workflow.
↪ Compiler.exe", "RegAsm.exe", "RegSvcs.exe", "MSHTA.EXE", "Msxsl.exe", "IEExec.exe", "Cmd.
↪ Exe", "PowerShell.EXE", "HH.exe", "javaw.exe", "pcalua.exe", "curl.exe", "ScriptRunner.exe",
↪ "CertOC.exe", "WorkFolders.exe", "odbcconf.exe", "msiexec.exe", "msdt.exe"] OR
(image="*\explorer.exe" command IN ["*.hta*", "*.vb*", "*.wsh*", "*.js*", "*.ps*", "*.scr*", "*.pif*",
↪ " ", "*.bat", "*.cmd*"]) OR image IN ["*\AppData*", "*\Users\Public*", "*\ProgramData*",
↪ "*\Windows\Tasks*", "*\Windows\Temp*", "*\Windows\System32\Tasks*"])
```

## 2.708 LP\_Usage of Web Request Command

- **Trigger Condition:** Various web request commands used with command line tools and Windows PowerShell cmdlets (including aliases) via CommandLine are detected. Adversaries use this technique to download malicious payloads. However, the Usage of Get-Command and Get-Help modules referencing Invoke-WebRequest and Start-BitsTransfer might trigger false positives. Script Block Logging must be enabled for this alert rule to work.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** PowerShell
- **ATT&CK ID:** T1059.001
- **Minimum Log Source Requirement:** Windows, Windows Sysmon, PowerShell
- **Query:**

```
(label="Create" label="Process" command IN ["*Invoke-WebRequest*", "*iwr*", "*wget*",
↪ "*curl*", "*Net.WebClient*", "*Start-BitsTransfer*", "*Resume-BitsTransfer*", "*[System.Net.
↪ WebRequest]::create*", "*Invoke-RestMethod*", "*WinHttp.WinHttpRequest*", "*new-
↪ object system.net.webclient).downloadstring*", "*new-object system.net.webclient).
↪ downloadfile*", "*new-object net.webclient).downloadstring*", "*new-object net.webclient).
↪ downloadfile*", "*.Download*", "*Net.WebClient*"] -user IN EXCLUDED_USERS) OR (norm_
↪ id=WinServer event_id= 4104 script_block IN ["*Invoke-WebRequest*", "*iwr*", "*wget*",
↪ "*curl*", "*Net.WebClient*", "*Start-BitsTransfer*", "*Resume-BitsTransfer*", "*[System.Net.
↪ WebRequest]::create*", "*Invoke-RestMethod*", "*WinHttp.WinHttpRequest*", "*new-object
↪ system.net.webclient).downloadstring*", "*new-object system.net.webclient).downloadfile*",
↪ "*new-object net.webclient).downloadstring*", "*new-object net.webclient).downloadfile*",
↪ "*.Download*", "*Net.WebClient*"] -path="C:\Packages\Plugins\Microsoft.
↪ GuestConfiguration.ConfigurationforWindows*")
```

## 2.709 LP\_Reconnaissance Activity with Nltest

- **Trigger Condition:** When possible reconnaissance activity via nltest binary is detected. Nltest is a Windows command-line utility that comes with a Windows Server, which is used to list domain controllers and enumerate domain trusts. The binary is available if you have installed the AD DS or the AD LDS server role. It is also available if you install the Active Directory Domain Services Tools that are part of the Remote Server Administration Tools (RSAT). Adversaries can use this technique to discover domain controllers, users and query the domain trust relationship.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** T1016 - System Network Configuration Discovery, T1482 - Domain Trust Discovery
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*\nltest.exe" file="nltestrk.exe" ((command = "*/
↪server*" command="*/query*") OR command IN ["*/dclist:*", "*/domain_trusts*", "*/trusted_
↪domains*", "*/user*", "*/parentdomain*"])
```

## 2.710 LP\_Regsvr32 Network Activity Detected

- **Trigger Condition:** When network connections and Application Layer Protocol, DNS queries initiated via regsvr32 binary are detected. Regsvr32 is a command-line utility to register and unregister the Windows Registry's OLE controls, such as DLLs and ActiveX controls. Adversaries utilized regsvr32 to run their malicious DLL, which downloads their other stager payload.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Regsvr32
- **ATT&CK ID:** T1218.010
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon "process"="*\regsvr32.exe" event_id IN ["3", "22"]
```

## 2.711 LP\_Possible Reconnaissance Activity

- **Trigger Condition:** Possible reconnaissance activity via nltest binary is detected. Nltest is a Windows command-line utility with a Windows server that lists domain controllers and enumerates domain trusts. Adversaries use this technique to discover the OS, user, network, subnets, file shares and domain trust, which will be used for further actions.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** System Network Configuration Discovery, Domain Trust Discovery
- **ATT&CK ID:** T1016, T1482
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create " process="*\nltest.exe" file="nltestrk.exe" ((command="*/
↪server*" command="*/query*") OR command IN ["*/dclist:*", "*/domain_trusts*", "*/trusted_
↪domains*", "*/user*", "*/parentdomain*"])
```

## 2.712 LP\_Privilege Escalation via Kerberos KrbRelayUp

- **Trigger Condition:** KrbRelayUp performs a universal no-fix local privilege escalation in Windows domain environments where LDAP signing is not enforced. KrbRelayUp is a wrapper that can streamline the use of some features in Rubeus, KrbRelay, SCMUACBypass, PowerMad/SharpMad, Whisker and ADCSPwn tools in attacks.
- **ATT&CK Category:** Credential Access, Lateral Movement
- **ATT&CK Tag:** Pass the Ticket, Kerberoasting
- **ATT&CK ID:** T1550.003, T1558.003
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create
(parent_image="KrbRelayUp.exe" OR image="KrbRelayUp.exe" OR
(command=" relay " AND command=" -Domain " AND command=" -ComputerName ") OR
(command=" krbscm " AND command=" -sc ") OR
(command=" spawn " AND command=" -d " AND command=" -cn " AND command=" -cp *"))
```

## 2.713 LP\_Suspicious Execution of LNK File

- **Trigger Condition:** When the execution of suspicious LNK files that either spawns Powershell or command prompt and has high entropy in the command field is detected. A LNK file is a Windows Shortcut that is a pointer to open a file, folder or application. Adversaries can utilize LNK files to embed their malicious scripts and commands and lure victims into executing the payload to gain initial access and evade defense. For this alert to work, an entropy plugin is required. Analysts can set the entropy value depending on the environment to filter out false positives. In our environment, legitimate use entropy was below five, so we used an entropy value greater than five to filter out false positives. The baseline time for using the process entropy command to detect such events is 90 days.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** T1204.002 - Malicious File
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create parent_process="*\explorer.exe" "process" IN ["*\cmd.exe",
↪ " *\powershell.exe"]
| process entropy(command) as command_entropy
| search command_entropy > 5
```

## 2.714 LP\_Insecure Policy Set via Set-ExecutionPolicy

- **Trigger Condition:** Set-ExecutionPolicy command utilized to set insecure policies such as Unrestricted, bypass and RemoteSigned is detected. Adversaries can utilize this technique to change the execution policy in order to execute their choice of malicious powershell scripts.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** PowerShell
- **ATT&CK ID:** T1059.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WinServer event_id=4104 script_block="*Set-ExecutionPolicy*" script_block IN [
↪ "*Unrestricted*", "*bypass*", "*RemoteSigned*"] -script_block IN [
↪ "*\AppData\Roaming\Code*"]
```

## 2.715 LP\_Network Connection to Suspicious Server

- **Trigger Condition:** Communication between hosts and domains mentioned in the query's list is detected. The query will search for logs generated from the Windows system or proxies and firewalls. The mentioned sites are either file storing or hosting sites. Adversaries have utilized such sites in many campaigns to upload and download data.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Ingress Tool Transfer
- **ATT&CK ID:** T1105
- **Minimum Log Source Requirement:** Windows Sysmon, Firewall, Proxy Server, WAF
- **Query:**

```
(norm_id=WindowsSysmon event_id=3 "image" IN ["C:\Windows*", "C:\Users\Public*"]?
↪ destination_host IN ["*dl.dropboxusercontent.com*", "*.pastebin.com*", "*.githubusercontent.
↪ com*", "*.cdn.discordapp.com/attachments*", "*.mediafire.com*", "*.mega.nz*", "*.ddns.net*",
↪ "*.paste.ee*", "*.hastebin.com/raw/*", "*.ghostbin.co/*", "*.ufile.io*", "*.anonfiles.com*",
↪ "*send.exploit.in*", "*.transfer.sh*", "*.privatlab.net*", "*.privatlab.com*", "*.sendspace.com*",
↪ "*pastetext.net*", "*.pastebin.pl*", "*.paste.ee*", "*.api.telegram.org*"]) OR (device_category?
↪ IN ["Firewall", "ProxyServer"] url IN ["*dl.dropboxusercontent.com*", "*.pastebin.com*", "*.
↪ githubusercontent.com*", "*.cdn.discordapp.com/attachments*", "*.mediafire.com*", "*.mega.
↪ nz*", "*.ddns.net*", "*.paste.ee*", "*.hastebin.com/raw/*", "*.ghostbin.co/*", "*.ufile.io*",
↪ "*anonfiles.com*", "*send.exploit.in*", "*.transfer.sh*", "*.privatlab.net*", "*.privatlab.com*",
↪ "*sendspace.com*", "*pastetext.net*", "*.pastebin.pl*", "*.paste.ee*", "*.api.telegram.org*"])
```

## NON-MITRE ATT&CK ANALYTICS

The NON-MITRE ATT&CK alerts available in Alert Rules are:

### 3.1 LP\_Windows Login Attempt on Disabled Account

- **Trigger condition:** A user attempts to log in using a disabled account.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer* label=User label=Login label=Fail sub_status_code= "0xC0000072" -
↪ target_user=*-user = ?-user IN EXCLUDED_USERS | rename user as target_user,?
↪ domain as target_domain,reason as failure_reason
```

### 3.2 LP\_VMware Link Up

- **Trigger condition:** VMware connection is up.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** VMware
- **Query:**

```
norm_id=VmwareESX label = Link label=Up | chart count() by log_ts, host, switch, port_
↪group, network_adapter
```

### 3.3 LP\_VMware Link Down

- **Trigger condition:** VMware's connection is down.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** VMware
- **Query:**

```
norm_id=VmwareESX label = Link label=Down | chart count() by log_ts, host, switch, port_
↪group, network_adapter
```

### 3.4 LP\_LogPoint License Expiry Status

- **Trigger condition:** Logpoint license is about to expire.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Logpoint
- **Query:**

```
norm_id=LogPoint label=Audit object='License checker' days_remaining=*
```

### 3.5 LP\_Mitre Initial Access Using Spearphishing link Detected

- **Trigger condition:** Malicious URL is detected.
- **ATT&CK Category:** N/A

- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Mimecast
- **Query:**

```
norm_id=Mimecast label=Detect label=Malicious label=URL | process eval("attack_class=
↪ 'Initial Access'") | process eval("technique='Spearphishing Link'")
```

### 3.6 LP\_Mitre Command and Control Using Standard Application Layer Protocol Detected

- **Trigger condition:** Command and control activity using standard application layer protocol is detected.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Proxy server
- **Query:**

```
norm_id=*proxy source_address=* destination_address=* destination_port IN[?]
↪ STANDARD_APPLICATION_PORTS | process ti(destination_address) | rename et_
↪ category as ti_category | process eval("attack_class='Command and Control'") | process[?]
↪ eval("technique='Standard Application Layer Protocol'") | search ti_category=
↪ "*Command and Control*"
```

### 3.7 LP\_Endpoint Protect Threat Content Detected

- **Trigger condition:** Threat content is detected.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Endpoint Protector

- **Query:**

```
norm_id=EndPointProtector label=Threat label=Content (label=Detect OR label=Block)
↪ file=* user=*
```

## 3.8 LP\_Endpoint Protect Device Disconnect

- **Trigger condition:** A USB device is disconnected.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Endpoint Protector
- **Query:**

```
norm_id = EndPointProtector label=disconnect user=* device_type="USB Storage Device"
```

## 3.9 LP\_Endpoint Protect File Delete

- **Trigger condition:** A file is deleted.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Endpoint Protector
- **Query:**

```
norm_id=EndPointProtector label=File label=Delete file=* user=*
```

## 3.10 LP\_Endpoint Protect File Copied To USB Device

- **Trigger condition:** A file is copied to external USB drive.
- **ATT&CK Category:** N/A

- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Endpoint Protector
- **Query:**

```
norm_id=EndPointProtector label=File label=Copy device_type="USB Storage Device"
↪ file=* user=*
```

### 3.11 LP\_System Owner or User Discovery Process Detected

- **Trigger condition:** An attack *Discovery* is performed using the attack technique *System Owner or User Discovery*.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer label="Process" label=Create (commandline="*whoami*" OR
↪ commandline="*quser*" OR commandline="*wmic.exe*useraccount get*" OR
↪ command="*whoami*" OR command="*quser*" OR command="*wmic.
↪ exe*useraccount get*") -user IN EXCLUDED_USERS | rename commandline as command
```

### 3.12 LP\_System Services Discovery Detected

- **Trigger condition:** An attack *Discovery* is performed using the attack technique *System Service Discovery*.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows

- **Query:**

```
norm_id=WinServer label="Process" label=Create (commandline="*net.exe*start*" OR
↪ commandline="*tasklist.exe*" OR command="*net.exe*start*" OR command="*tasklist.
↪ exe*") -user IN EXCLUDED_USERS | rename commandline as command
```

### 3.13 LP\_SolarisLDAP Password Spraying Attack Detected

- **Trigger condition:** Password spraying attack is detected.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Solaris LDAP
- **Query:**

```
norm_id=SolarisLDAP label=User (label=Login OR label=Authentication) label=Fail | chart
↪ distinct_count(user) as UserCount, distinct_list(user) as Users | search UserCount > 5
```

### 3.14 LP\_Microsoft Defender AMSI Trigger

- **Trigger Condition:** Logpoint detects Microsoft Defender with AMSI as the detection source. The Windows Antimalware Scan Interface (AMSI) is a versatile interface standard that allows your applications and services to integrate with any antimalware product on a machine.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=1116 source_name=AMSI event_source="Microsoft-
↪ Windows-Windows Defender"
```

### 3.15 LP\_Petitpotam - Anonymous RPC and File Share

- **Trigger Condition:** Events related to Petitpotam are logged.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
[event_id=4624 package="NTLM*" (user="ANONYMOUS LOGON" or -workstation=*)]
↪ as stream1 join [event_id=5145 share_name=IPC$ access="*ReadData (or ListDirectory)
↪ WriteData (or AddFile)*" relative_target IN ["lsarpc", "efsrpc", "lsass", "samr",
↪ "netlogon"]] as stream2 on stream1.source_address = stream2.source_address and
↪ stream1.host = stream2.host | rename stream1.user as user, stream1.host as host,
↪ stream1.domain as domain, stream2.source_address as source_address, stream2.share_
↪ name as share_name, stream2.access as access, stream2.log_ts as log_ts
```

### 3.16 LP\_RDP Sensitive Settings Changed

- **Trigger Condition:** Changes to RDP terminal service sensitive settings are detected.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WindowsSysmon event_id=13 target_object IN [
↪ "*\services\TermService\Parameters\ServiceDll*", "*\Control\Terminal
↪ Server\SingleSessionPerUser*", "*\Control\Terminal Server\DenyTSConnections*"] -
↪ user IN EXCLUDED_USERS
```

### 3.17 LP\_Secure Deletion with SDelete

- **Trigger Condition:** Renamed a file while deleting it with the SDelete tool. Adversaries use various tools to clean traces left after their intrusion activity.
- **ATT&CK Category:** -

- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id IN ["4656", "4663", "4658"] object_name IN ["*.AAA", "*.ZZZ",
↪ "] -user IN EXCLUDED_USERS
```

### 3.18 LP\_Suspicious Keyboard Layout Load Detected

- **Trigger Condition:** The keyboard preload installation with a suspicious keyboard layout, for example, Chinese, Iranian, or Vietnamese layout, loads in user sessions on systems that is maintained by US staff only.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=13 target_object IN ["*\Keyboard Layout\Preload*",
↪ "\Keyboard Layout\Substitutes*"] detail IN ["00000804", "00000c04", "00000404",
↪ "00001004", "00001404", "00000429", "00050429", "0000042a", "00000401", "00010401",
↪ "00020401"] -user IN EXCLUDED_USERS
```

### 3.19 LP\_Remote Code Execution using WMI Win32\_Process Class over WinRM

- **Trigger Condition:** When an attempt to execute code or create a service on a remote host via winrm.vbs is detected. WinRM is a windows native script used to manage Windows RM settings. The functionality of the WinRM command is provided through a Visual Basic Script, winrm.vbs. This script can be abused to create a process leading to remote code execution and lateral movement. False positives are uncommon, but legitimate use for administrative purposes such as remote PowerShell execution can trigger this alert.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows Sysmon, Windows

- **Query:**

```
label=Create label="Process" command="*winrm*" command="*invoke Create wmicimv2/
↳ Win32_*" command="*-r:http*"
```

## 3.20 LP\_Remote Code Execution using WMI Win32\_Service Class over WinRM

- **Trigger Condition:** Application Whitelisting Bypass and Arbitrary Unsigned Code Execution Technique is attempted using winrm.vbs. It detects the execution of attacker-controlled WsmPty.xml or WsmTxt.xml via winrm.vbs and copied cscript.exe (can be renamed). winrm.vbs (a Windows-signed script) can consume and execute attacker-controlled XSL, which is not subject to enlightened script host restrictions, resulting in the execution of arbitrary, unsigned code execution.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label=Create label="Process" command="*winrm*" command IN ['*format:pretty*', '*format:
↳ "pretty"*', '*format:"text"*', '*format:text*'] -(image IN ["C:\Windows\System32*",
↳ "C:\Windows\SysWOW64*"])
```

## 3.21 LP\_Suspicious Microsoft SQL Server PowerShell Module Use Detected

- **Trigger Condition:** The execution of a PowerShell code by the sqlps.exe utility, which is included in the standard set of utilities supplied with the MSSQL Server is detected. Script blocks are not logged in this case, so this utility helps to bypass protection mechanisms based on the analysis of these logs. As this attack requires sqlps.exe bundled with MSSQL installation, any device without it is not vulnerable. Also, child process sqlps.exe spawned by sqlagent.exe is a legitimate action. Direct PS command execution through SQLPS.exe is rare, but if it occurs, it results in a false positive.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -

- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label=Create label="Process" ("process"="*\sqlps.exe" OR parent_process="*\sqlps.exe" OR
↪file="*\sqlps.exe") -(parent_process="*\sqlagent.exe")
```

## 3.22 LP\_Shadow Copy Deletion Using OS Utilities Detected

- **Trigger Condition:** When shadow copies are deleted using operating systems utilities. Shadow copy is a Microsoft technology that can create backup copies or snapshots of computer files or volumes. Windows internal binaries are PowerShell, wmic, vssadmin, diskshadow, wbadmin, and vssadmin. Adversaries can utilize these binaries to delete shadow copies from the system so that the data recovery and reverting the system to a saved state is impossible after dropping malware.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label="Create" ("process" IN ["*\powershell.exe", ".*\wmic.exe", ".*\vssadmin.
↪exe", ".*\diskshadow.exe"] command=".* shadow*" command=".*delete*") OR ("process"=
↪".*\wbadmin.exe" command=".*delete*" command=".*catalog*" command=".*quiet*") OR (
↪"process"=".*\vssadmin.exe" command=".*resize*" command=".*shadowstorage*"
↪command=".*unbounded*")
```

## 3.23 LP\_Child Process Spawned via Diskshadow Detected

- **Trigger Condition:** When child processes are created using the diskshadow binary. DiskShadow.exe is a Windows internal binary that exposes the functionality offered by the Volume Shadow Copy Service. Volume shadow copy service is a Windows framework that backs up a volume by creating a copy of it. Adversaries can use diskshadow binary's interactive mode and execute other binaries using the exec command to bypass defensive countermeasures.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -

- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "parent_process"="*\diskshadow.exe" -command="*conhost.
↪exe"
```

## 3.24 LP\_Code Execution Via Diskshadow Detected

- **Trigger Condition:** When diskshadow binary is used to execute code from a file. DiskShadow.exe is Windows internal binary that exposes the functionality offered by the Volume Shadow Copy Service. Volume shadow copy service is a framework in Windows that provides the function to backup a volume by creating a copy of it. Adversaries can use diskshadow with -s or /s tag to execute a command from a file and bypass detection.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*\diskshadow.exe" command IN ["*/s *", "*-s *"]
```

## 3.25 LP\_Process Pattern Match For CVE-2021-40444 Exploitation

- **Trigger Condition:** The process pattern for CVE-2021-40444 is detected. CVE-2021-40444 is a remote code execution vulnerability in MSHTML, which is Microsoft's proprietary browser engine for Internet Explorer. Control.exe is a Windows internal binary to access the control panel. Adversaries can rename their malware or payload to control.exe and execute it to escape detection.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*\control.exe" parent_process IN ["*\winword.exe",
↪ " *\excel.exe", " *\powerpnt.exe"] -command="*\control.exe input.dll"
```

## 3.26 LP\_Suspicious Extexport Execution Detected

- **Trigger Condition:** When a service is created by loading a DLL using the ExtExport service in IE. ExtExport is a module that serves to import/export data from other programs, for example, favorites or bookmarks from other browsers. Attackers can use Extexport.exe to load any DLL using the built-in tool ExtExport.exe which can be found inside the Internet Explorer directory.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label=Create label="Process" command IN ["*ExtExport*", "extexport"]
```

## 3.27 LP\_Proxy Execution via Workfolders

- **Trigger Condition:** When Logpoint detects the use of workfolders binary to execute other process. Workfolders is a Windows internal binary that provides a consistent way for users to access their work files from their PCs and devices. Adversaries can use this technique to evade defensive countermeasures or to hide as a persistence mechanism.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "parent_process"="*\workfolders.exe" "process"="*\control.exe
↪ " "process"="C:\Windows\System32\control.exe"
```

## 3.28 LP\_Proxy Execution via Windows Update Client

- **Trigger Condition:** When wuauctl.exe is used to proxy execute codes. Wuauctl.exe (Windows Update Auto Update Client) is a Microsoft Windows native AutoUpdate Client used to check for available updates from Microsoft Update. Adversaries may abuse wuauctl.exe to camouflage and execute malicious codes.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label="create" ("process"="*\wuauctl.exe" OR file="wuauctl.exe")
↪(command="*UpdateDeploymentProvider*" command="*.dll*" command=
↪"*RunHandlerComServer*")
- (command IN ["* /UpdateDeploymentProvider UpdateDeploymentProvider.dll *", "* wuaueng.
↪dll *"])
```

## 3.29 LP\_Suspicious DLL Execution Using Windows Address Book

- **Trigger Condition:** When a suspicious DLL is executed using wab.exe. Windows Address Book stores addresses, contact details, and e-mail addresses by programs like Outlook. When wab.exe executes, it tries to load DLL pointed by the registry key. But adversaries leverage this functionality to load their custom malicious DLL from a path other than the default by modifying the path pointed by the registry key.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1564.004 - NTFS File Attributes
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="registry" label="set" target_object="*\Software\Microsoft\WAB\DLLPath*" - detail="
↪%CommonProgramFiles%\System\wab32.dll"
```

### 3.30 LP\_Suspicious Use of Dotnet Detected

- **Trigger Condition:** When the execution of either suspicious DLL or unsigned code using dotnet.exe is detected. dotnet.exe is a command line tool for managing .NET source codes and binaries. Adversaries can use it to execute DLL or some unsigned code and can bypass default AppLocker rules. dotnet.exe might trigger false positives if used for penetrating testing or system administration.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="create" label="process" command IN ["*.dll", "*.csproj"] "process"="*\dotnet.exe"
```

### 3.31 LP\_Execution of Arbitrary Executable Using Storddiag

- **Trigger Condition:** When a renamed arbitrary executable is executed using storddiag.exe. storddiag.exe collects storage and file system diagnostic logs and outputs to a folder. Generally, storddiag.exe performs schtasks.exe, systeminfo.exe and fltmc.exe after it is executed. Adversaries can abuse its functionality by copying it into a random folder, renaming the malicious executables as schtasks.exe, systeminfo.exe and fltmc.exe, and running them. It might trigger false positives for legitimate use of storddiag.exe.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Create" label="Process" parent_process="*\storddiag.exe" "process" IN ["*\schtasks.exe",
↪ "\systeminfo.exe", "\fltmc.exe"] - parent_process IN ["C:\windows\system32*",
↪ "C:\windows\syswow64*"]
```

### 3.32 LP\_Process Creation via Time Travel Tracer

- **Trigger Condition:** When a new child process is spawned via tttracer.exe. Microsoft Time Travel Tracing Tool (Tttracer) is a diagnostic tool to collect time travel traces of given processes. Later, traces are analyzed by Microsoft Support for troubleshooting purposes. Adversaries can use this binary to launch their malicious binary and create a dump of a process.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create "parent_process"="*\tttracer.exe"
```

### 3.33 LP\_Time Travel Debugging Utility DLL Loaded

- **Trigger Condition:** When loading of time travel debugging utility DLLs are detected. Ttdrecord.dll, ttdwriter.dll and ttdloader.dll are part of a time travel debugging utility. Time Travel Debugging is a tool that captures a trace of a process as it executes and replays it later, forward and backward. DLL adversaries can run other binaries or dump a process by loading.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label=image label=load image IN ["*\ttdrecord.dll", "*\ttdwriter.dll", "*\ttdloader.dll"]
```

### 3.34 LP\_File Execution via Msdeploy

- **Trigger Condition:** When MSDeploy is used to execute files. Microsoft Deploy (MSDeploy) is a binary that allows users to deploy Web Applications. Adversaries can use this technique to bypass application whitelisting.
- **ATT&CK Category:** -

- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create "process"="*\msdeploy.exe" command="*verb:sync*"
↪ command="*-source:RunCommand*" command="*-dest:runCommand"
```

### 3.35 LP\_CVE-2022-40684 Exploitation Detected

- **Trigger Condition:** When an exploitation attempt of CVE-2022-40684 is detected. CVE-2022-40684 is an authentication bypass using an alternate path or channel vulnerability [CWE-288] in FortiOS, FortiProxy and FortiSwitchManager that may allow an unauthenticated attacker to perform operations on the administrative interface via specially crafted HTTP or HTTPS requests. Adversaries can use this technique to gain remote access to a system. The affected versions are: FortiOS v7.2.0-7.2.1, FortiOS v7.0.0-7.0.6, FortiProxy v7.2.0, FortiProxy v7.0.0-7.0.6, FortiSwitchManager v7.2.0 and FortiSwitchManager v7.0.0.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Firewall, Proxy Server, Web Server
- **Query:**

```
(url="*/api/v2/cmdb/system/admin/*" OR resource="*/api/v2/cmdb/system/admin/*") user_
↪ agent IN ["report runner", "Node.js"]
```

### 3.36 LP\_Possible Proxy Execution of Malicious Code

- **Trigger Condition:** When the possible use of TE.exe for proxy execution of malicious scripts is detected. TE.exe is a testing tool included with Microsoft Test Authoring and Execution Framework (TAEF). TAEF allows users to run automation by executing test files written in different languages (C, C#, Microsoft COM Scripting interfaces). Adversaries can leverage its functionality to execute malicious codes (such as WSC files with VBScript or DLL) directly by running te.exe. It is not unusual to use te.exe directly to execute legal TAEF tests, so legitimate use can trigger false positives.
- **ATT&CK Category:** -

- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="process" label="create" "process"="*\te.exe" OR parent_process="*\te.exe" OR file=
↪ "\te.exe"
```

### 3.37 LP\_Suspicious Usage of BitLocker Management Script

- **Trigger Condition:** When proxy execution of malicious payloads via Manage-bde.wsf is detected. Manage-bde.wsf is a BitLocker management script file that is generally used to turn BitLocker, specify unlock mechanisms, update recovery methods and unlock BitLocker-protected data drives. Adversaries can use it for the proxy execution of malicious payloads.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="process" label="create" command="*cscript*" command="*manage-bde.wsf"
```

### 3.38 LP\_Proxy Execution of Payloads via Microsoft Signed Script

- **Trigger Condition:** When proxy execution of PowerShell code via Microsoft signed script CL\_Mutexverifiers.ps1 is detected. Adversaries can execute payloads via runAfterCancelProcess in CL\_Mutexverifiers.ps1 module. Script block logging must have been enabled for the alert to work.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id="WinServer" event_id=4104 script_block IN ["*\CL_Mutexverifiers.ps1*",
↪ "*runAfterCancelProcess *"]
```

### 3.39 LP\_Execution of Windows Defender Offline Shell from Suspicious Folder

- **Trigger Condition:** When OfflineScannerShell.exe is executed from a folder other than the default. Microsoft Defender Offline is an antimalware scanning tool that lets you boot and run a scan from a trusted environment. Adversaries can use OfflineScannerShell.exe to execute the mpclient.dll library in the current working directory and execute arbitrary codes.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
label="create" label="process" ("process"="*\OfflineScannerShell.exe" -((path="C:\Program
↪ Files\Windows Defender\Offline\") OR (-path=*))
```

### 3.40 LP\_DLL Loaded Via AccCheckConsole

- **Trigger Condition:** When DLL loading through AccCheckConsole binary is detected. AccCheckConsole is a command-line tool for verifying the accessibility implementation of your application's UI. Adversaries can use this technique to load their malicious DLL.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create "process"="*\AccCheckConsole.exe" command="*-window*.dll*"
↪ "
```

### 3.41 LP\_Proxy Execution via Appvlp

- **Trigger Condition:** When proxy execution of binaries via appvlp.exe is detected. Appvlp, also known as Application Virtualization Utility, is included with Microsoft Office 2016, which makes applications available to end-user computers without having to install applications directly on those computers. Adversaries can use this technique to bypass process or signature-based defenses by proxying the execution of malicious content with signed or otherwise trusted binaries.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create "process"="*\appvlp.exe" command IN ["*cmd.exe",
↪ "*powershell.exe*"] command IN ["*.sh*", "*.exe*", "*.dll*", "*.bin*", "*.bat*", "*.cmd*", "*.js*",
↪ "*.msh*", "*.reg*", "*.scr*", "*.ps*", "*.vb*", "*.jar*", "*.pl*", "*.inf*"]
```

### 3.42 LP\_Proxy DLL Execution via UtilityFunctions

- **Trigger Condition:** When the use of UtilityFunctions script to execute a managed DLL is detected. UtilityFunctions is one of several powershell scripts from Microsoft for diagnostic and maintenance work. Adversaries can use this technique to proxy execute malicious files.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create command IN ["*UtilityFunctions.ps1*", "*RegSnapin*"]
```

### 3.43 LP\_Suspicious Usage of Squirrel Binary

- **Trigger Condition:** When squirrel.exe is run via using arguments download, update and updateRollback arguments. Squirrel.exe is a binary to update the existing

installed NuGet or squirrel package. NuGet is a package manager designed to enable developers to share reusable code. Adversaries can use this technique to download and execute malicious NuGet package.

- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label="create" "process"="*\Squirrel.exe" command IN ["*download*",
↪ "*update*"]
```

### 3.44 LP\_Suspicious File Share Permission

- **Trigger Condition:** When the execution of binaries from a suspicious folder is detected. Paths mentioned in the lists are not Windows default paths from where native and internal binaries are executed. Adversaries may attempt to masquerade their payload as legitimate binaries and execute from non-default paths to avoid detection. Legitimate binaries executed from those paths can trigger an alert, so include those binaries in the excluded process list.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create "process"="*\net.exe" command="* share *grant:*FULL"
```

### 3.45 LP\_Legitimate Application Dropping Script File

- **Trigger Condition:** When the creation of a new script file by those applications which should not create one such as office applications, Wordpad. Script files contain a set of instructions or commands and are executed by a script interpreter or runtime environment. Adversaries can use this technique to drop their payload in the system and execute it.
- **ATT&CK Category:** -

- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=11 file IN ["*.ps1", "*.bat", "*.vbs", "*.scf", "*.wsf", "*.wsh"]
↪ "process" IN ["*\\onenote.exe", "*\\winword.exe", "*\\excel.exe", "*\\powerpnt.exe",
↪ "*\\msaccess.exe", "*\\mspub.exe", "*\\eqnedt32.exe", "*\\visio.exe", "*\\wordpad.exe",
↪ "*\\wordview.exe", "*\\certutil.exe", "*\\certoc.exe", "*\\CertReq.exe", "*\\Desktopimgdownldr.exe",
↪ "*\\esentutl.exe", "*\\finger.exe", "*\\AcroRd32.exe", "*\\RdrCEF.exe", "*\\mshta.exe", "*\\hh.exe",
↪ "]"
```

## ALERT RULES DASHBOARDS

### 4.1 LP\_Mitre Attack Analytics Overview

This dashboard consists of the following widgets:

| Widget Name                          | Description                                                                                                                                                                                                                                                                   |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Triggered Attack Tactics             | The count of tactics that the attacker may use to perform an attack. The tactics are Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration and Impact. |
| Triggered Attack Tactics - Timetrend | A time trend for the attack tactics that the attacker used to perform an attack.                                                                                                                                                                                              |
| Mitre Att&ck Matrix                  | An ATT&CK chart, a heatmap describing the attacks carried out in a system in the form of attack tactics, techniques and procedures defined by MITRE.                                                                                                                          |
| Top Recurring Attacks                | The most recurring attacks, their attack category and the count of attacks. For example, Console History Discover Detected is an attack, Collection is its attack category and the attack occurred three times.                                                               |
| Top Users by Attack Tactics          | The top users based on attack tactics.                                                                                                                                                                                                                                        |
| Top Hosts in Attack                  | The count of top hosts by attack category.                                                                                                                                                                                                                                    |

### 4.2 Adding the Alert Rules Dashboard

1. Go to *Settings >> Knowledge Base* from the navigation bar and click **Dashboards**.
2. Select **VENDOR DASHBOARD** from the drop-down.
3. Click **Add** from **Actions**.

The screenshot shows the LogPoint Vendor Dashboard interface. At the top, there's a navigation bar with 'LOGPOINT', 'DASHBOARD', 'SEARCH', 'REPORT', 'INCIDENT', and 'SETTINGS'. Below this is the 'Vendor Dashboard' header. The main content area displays a table of widgets. The first widget is 'LP\_Mitre Attack Analytics Overview'. Its details are shown in a modal or expanded view, including a description, a complex query, and repository settings. The 'Used' column for this widget is 'NO' and the 'Version' is '2'. A red arrow points to a plus icon in the 'Actions' column, indicating the option to add or modify repositories.

Fig. 1: Adding the Alert Rules Dashboard

#### 4. Click **Choose Repos.**

The screenshot shows the 'ASK REPOS' dialog box. It has a title bar with a close button. Below the title bar is a table with columns 'S.N.', 'Dashboard', and 'Repos'. The first row is '1 LP\_Mitre Attack Analytics Overview'. A red box highlights the 'Choose Repos' button in the top right corner. Below the table, there is a yellow note: 'Note: Using all repos in all the widgets of all dashboards may hit on performance'. At the bottom right, there are 'Ok' and 'Cancel' buttons.

Fig. 2: Selecting Repos

#### 5. Select the repo and click **Done.**

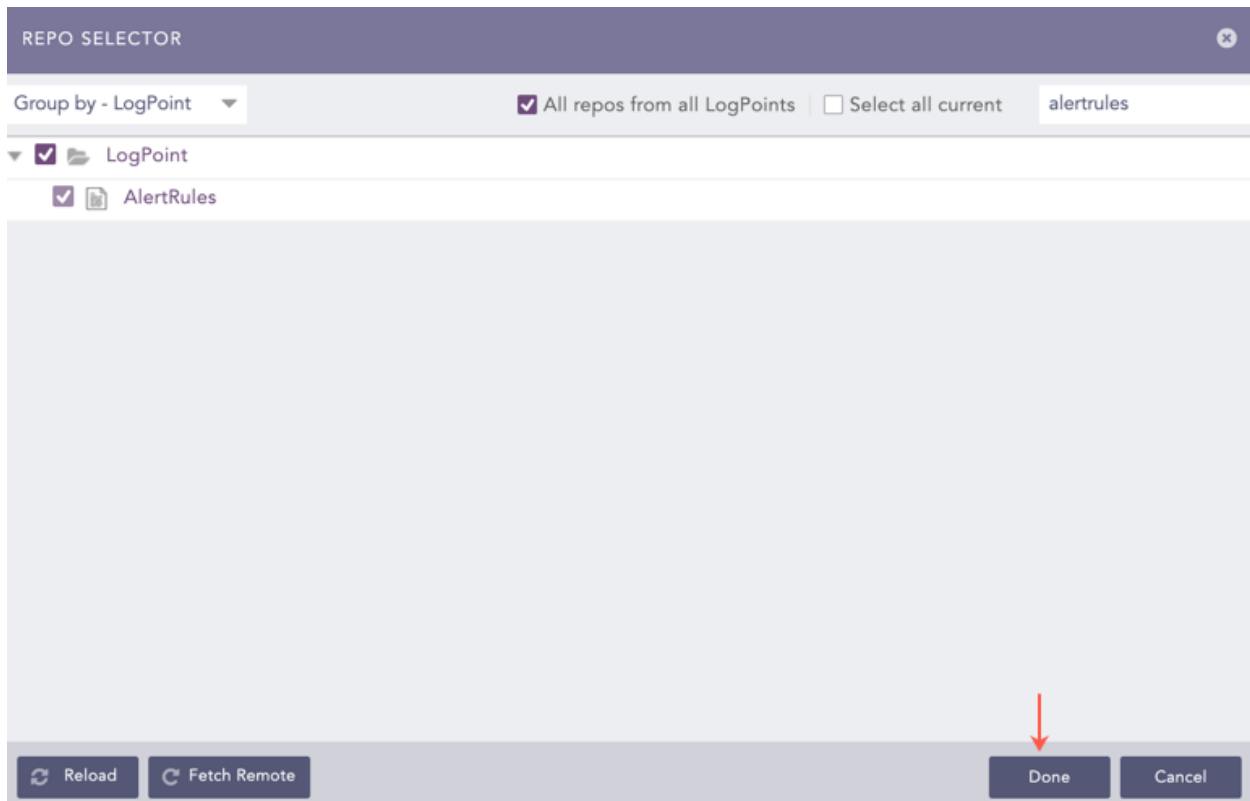


Fig. 3: Selecting Repos

6. Click **Ok**.

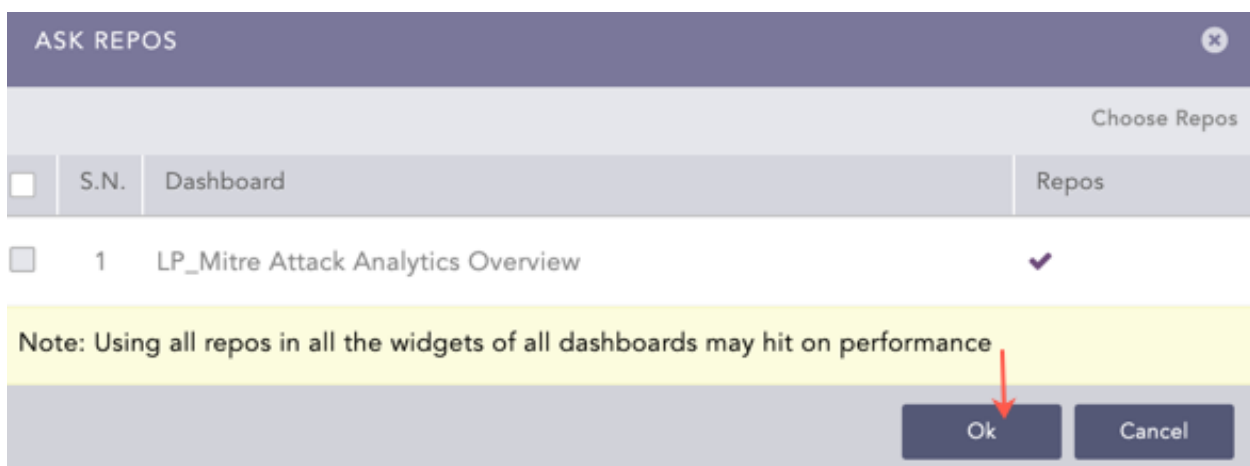


Fig. 4: Confirmation for Repo

You can find the Alert Rules dashboard under **Dashboards**.

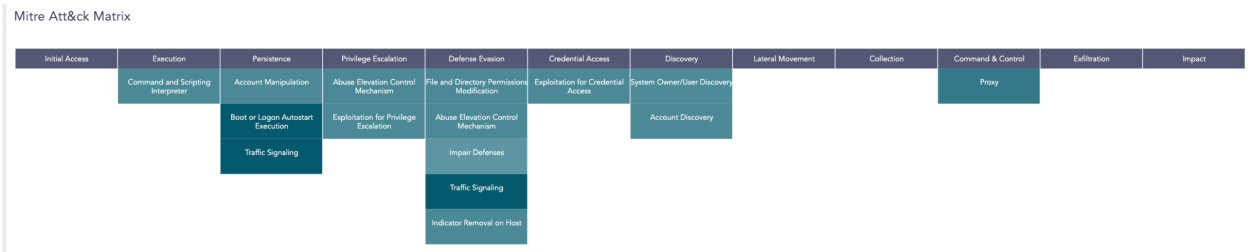


Fig. 5: Alert Rules Dashboard

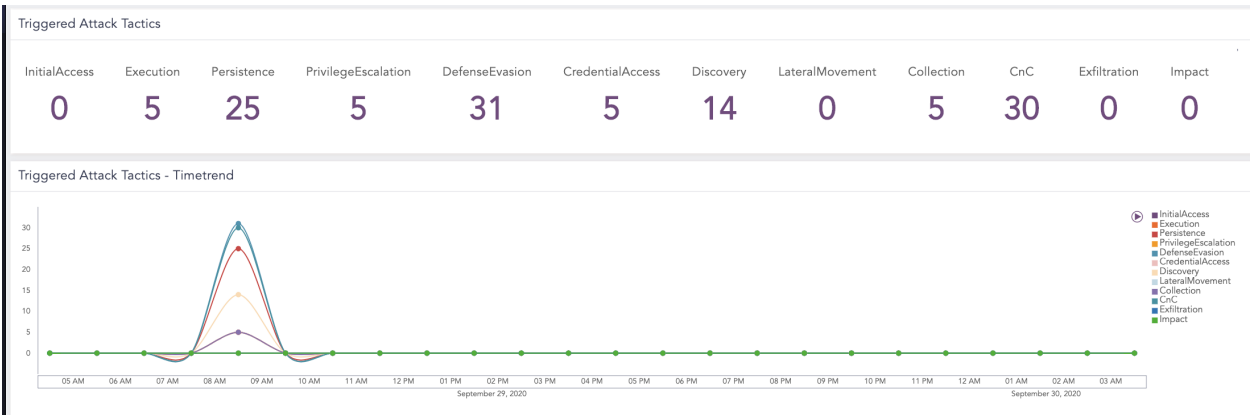


Fig. 6: Alert Rules Dashboard

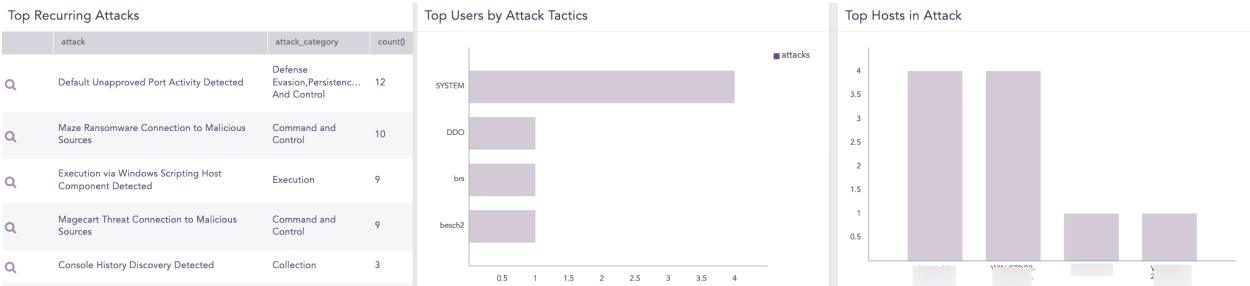


Fig. 7: Alert Rules Dashboard

## **KB-LISTS**

- ABNORMAL\_FILES
- ACTINIUM\_DOMAINS
- ADMIN\_GROUPS
- ADMIN\_SOURCES
- ADMINS
- ALERT\_IRC\_PORT
- ALERT\_OPEN\_PORTS
- ALERT\_PRESENT\_EMPLOYEES
- ALERT\_UNUSUAL\_SOURCE
- ALLOWED\_PORTS
- ATTACK\_COMMANDS
- BAD\_RABBIT\_FILE
- BAD\_RABBIT\_HASH
- BLACKLIST\_IPS
- BLACKLISTED\_DOMAIN
- BLACKLISTED\_IP
- BLACKLISTED\_PORTS
- BLOCKED\_APPLICATION
- CLOUD\_APP
- CLOUD\_APPLICATION\_IP

- CLOUD\_APPLICATIONS
- CONCERNED\_CONTENT
- CRIMINAL\_CONTENT
- CRITICAL\_FILE
- CRITICAL\_FILES
- CRITICAL\_FOLDER
- DEFAULT\_USERS
- DOMAIN
- DOPPELPAYMER\_RANSOMWARE\_CVE
- DRAGONFLY\_CNC\_REQUEST
- DYNAMIC\_CATEGORIES
- EXCLUDED\_USERS
- EXECUTABLES
- EXISTING\_USERS
- EXTREMIST\_CONTENT
- GHOSTWRITER\_IPS
- HERMETIC\_WIPER\_DRIVER\_HASHES
- HIDDEN\_COBRA\_FILE
- HIDDEN\_COBRA\_HASH
- HIDDEN\_COBRA\_IP
- HOME\_DIR
- HOME\_DOMAIN
- HOME\_FOLDER
- HOMENET
- HTTP\_ERROR
- INACTIVE\_USERS
- INVISIMOLE\_MALWARE\_HASHES

- KASPERSKY\_DETECTED\_MALWARE\_HASHES
- KASPERSKY\_UPDATE\_FAILURES
- KNOWN\_APPLICATIONS
- KNOWN\_DOMAINS
- KNOWN\_FILE
- KNOWN\_SERVER\_HOST
- LOCKERGOGA\_FILES
- MAGECART\_DOMAINS
- MAIL\_SERVER\_IP
- MAIL\_SERVERS
- MALICIOUS\_POWERSHELL\_COMMANDLET\_NAMES
- MALICIOUS\_TOOLS\_IMPHASH
- MALWARE\_EMAILS
- MALWARE\_FILES
- MALWARE\_HASH
- MALWARE\_IP
- MATRIX\_FILE
- MAZE\_RANSOMWARE\_DOMAINS
- MAZE\_RANSOMWARE\_EMAILS
- MOST\_EXPLOITABLE\_CVE
- MOST\_EXPLOITABLE\_DOMAINS
- MOST\_EXPLOITABLE\_EMAILS
- MOST\_EXPLOITABLE\_HASHES
- MOST\_EXPLOITABLE\_IPS
- NEFILIM\_RANSOMWARE\_EMAILS
- NEFILIM\_RANSOMWARE\_HASHES
- NON\_EXISTING\_USERS

- NON\_PCI\_COMPLIANT\_PORT
- POWERSPLOIT\_RECON\_MODULES
- PRIVILEGED\_USER
- PROWLI\_CVE
- PROWLI\_DOMAIN
- PROWLI\_EMAIL
- PROWLI\_FILE
- PROWLI\_HASH
- SERVER\_ADDRESS
- SQL\_INJECTION\_CHARACTER
- SQL\_INJECTION\_CHARACTERS
- SUSPICIOUS\_COUNTRY
- UNAPPROVED\_PORT
- VULNERABLE\_CONTENT
- VULNERABLE\_WORKSTATIONS
- WANNACRY\_DOMAIN
- WANNACRY\_EXTENSION
- WEBSERVER\_SYSTEMS
- WINADMINS
- WINDOWS\_DC
- XSS\_TAG
- YOUTUBE

For more details on Lists, go to the [Lists](#) section in the *Logpoint Data Integration guide*.