LOGPOINT

Integrations

Alert Rules

*V*6.0.0

CONTENTS

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

CHAPTER

ONE

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 Logoint. 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*.
2. **Dashboard Package**
   - LP_Mitre Attack Analytics Overview
3. **Search Template**
   - LP_Mitre Attack Analytics Overview

Required Log Source

MITRE ATT&CK Analytics

- Windows Security Audit
- Windows Sysmon

Default Alert Rules

- All applicable log sources

CHAPTER

TWO

MITRE ATT&CK ANALYTICS

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

- **Trigger Condition:** User agents associated with known reconnaissance tools like AADInternals and AzureHound, presented during successful logins to Microsoft 365.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Permission Groups Discovery, Cloud Account, Cloud Service Discovery
- **ATT&CK ID:** T1069, T1087.004, T1526
- **Minimum Log Source Requirement:** Office365
- **Query:**

```
norm_id=office365 label=User label=Login label=Successful user_agent IN ["AadInternals",
↪"azurehound*"]
```

2.1 LP_Multiple Exchange Mailboxes Accessed via API in Short Span

- **Trigger Condition:** High number of mailboxes accessed via an API, such as Microsoft Graph API or Exchange Web Services, within a short period.
- **ATT&CK Category:** Collection
- **ATT&CK Tag:** Remote Email Collection
- **ATT&CK ID:** T1114.002
- **Minimum Log Source Requirement:** Office365

- **Query:**

```
norm_id="Office365" action="MailItemsAccessed" user_type="Application" | process eval(
↪"match=like(client_information, 'Client=WebServices;ExchangeWebServices%')") | process
↪eval("search_result=if(match) {return 1} else-if(target_application=='Microsoft Graph') {return
↪1} else {return 0}") | filter search_result=1 | timechart distinct_count(upn) as user_mailbox_
↪count, distinct_list(user) as user_list, distinct_list(source_address) as source_address by target_
↪application every 10 minutes | filter user_mailbox_count > 5
```

2.2 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.
- **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
```

2.3 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="Process" label=Create (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*"))
```

2.4 LP_Remote Thread Creation via Cactustorch

- **Trigger Condition:** This alert is triggered whenever it detects remote thread creation from CACTUSTORCH.
- **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
```

2.5 LP_Call to a Privileged Service Failed

- **Trigger Condition:** This alert is triggered whenever 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()"
keyword="0x8010000000000000" -user IN EXCLUDED_USERS
```

2.6 LP_CEO Fraud - Possible Fraudulent Email Behavior

- **Trigger Condition:** An email received from a threat source in the internal network exhibits fraudulent behavior.
- **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
```

2.7 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
```

2.8 LP_Change of Default File Association Detected

- **Trigger Condition:** This alert is triggered whenever a registry value is set to change the file association.
- **ATT&CK Category:** Persistence, Privilege Escalation
- **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*"]
```

2.9 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*"]
```

2.10 LP_Clearing of PowerShell Logs Detected

- **Trigger Condition:** Erasing PowerShell's console history logs. Console history logs are records of commands executed in the PowerShell console. Adversaries can use this technique to remove traces of executed PowerShell commands to cover their malicious activity.
- **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"))
```

2.11 LP_Clipboard Data Access Detected

- **Trigger Condition:** This alert is triggered whenever data collection from clipboard using Windows utilities are 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 file="clip.exe"))
OR
(script_block="*Get-Clipboard*" OR command="*Get-Clipboard*")
```

2.12 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.
- **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
```

2.13 LP_CMSTP Execution Detected

- **Trigger Condition:** Loading and execution of local or remote payloads using CMSTP.
- **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")
```

2.14 LP_CMSTP UAC Bypass via COM Object Access

- **Trigger Condition:** Loading and execution of local or remote payloads using CMSTP is detected.
- **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"]
```

2.15 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:** Dynamic-link Library Injection
- **ATT&CK ID:** T1055.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

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

2.16 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:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter
- **ATT&CK ID:** T1059
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
norm_id=WindowsSysmon event_id=1 command IN ["cmd.exe /c *http://*%AppData%", "cmd.
↪exe /c *https://*%AppData%"] -user IN EXCLUDED_USERS
```

2.17 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
```

2.18 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*"]
```

2.19 LP_Copy from Admin Share Detected

- **Trigger Condition:** Copying of file from a remote C$ or ADMIN$ share via copy command. Adversaries abuse these shares to gain unauthorized access to sensitive data on a network.
- **ATT&CK Category:** Lateral Movement, Command, Exfiltration
- **ATT&CK Tag:** SMB/Windows Admin Shares, Data from Network Shared Drive, Exfiltration Over Alternative Protocol
- **ATT&CK ID:** T1021.002, T1039, T1048
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

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

2.20 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>
```

2.21 LP_CreateMiniDump Hacktool Detected

- **Trigger Condition:** Usage of the CreateMiniDump hack tool to dump memory in Windows. Adversaries use the tool to dump LSASS without Mimikatz, reducing the chances of getting flagged by antivirus software.
- **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"="*\CreateMiniDump.exe" OR hash_import=
↪"4a07f944a83e8a7c2525efa35dd30e2f"
```

2.22 LP_CreateRemoteThread API and LoadLibrary

- **Trigger Condition:** Usage of CreateRemoteThread API and LoadLibrary functions to inject DLL into a process.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Dynamic-link Library Injection
- **ATT&CK ID:** T1055.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

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

2.23 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]'>
| filter command_match=*
```

2.24 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
```

2.25 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.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** LSASS Memory, Security Account Manager, NTDS, LSA Secrets, Cached Domain Credentials
- **ATT&CK ID:** T1003.001, T1003.002, T1003.003, T1003.004, T1003.005
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

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

2.26 LP_Credential Dumping with ImageLoad Detected

- **Trigger Condition:** This alert is triggered whenever 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\samlib.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
```

2.27 LP_Registry Enumeration for credentials Detected

- **Trigger Condition:** This alert is triggered whenever adversaries search the registry of compromised systems to find and obtain insecurely stored credentials.
- **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*"]))
```

2.28 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
```

2.29 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
```

2.30 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
```

2.31 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
```

2.32 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
```

2.33 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, Web Server, DNS Server
- **Query:**

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

2.34 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]
```

2.35 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
```

2.36 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
```

2.37 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, Web Server
- **Query:**

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

2.38 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
```

2.39 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
```

2.40 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=*
```

2.41 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
```

2.42 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)
```

2.43 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
```

2.44 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, Web Server
- **Query:**

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

2.45 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
```

2.46 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, Web Server
- **Query:**

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

2.47 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]
```

2.48 LP_Default PowerSploit and Empire Schtasks Persistence

- **Trigger Condition:** Creation of a *schtask* via PowerSploit or Empire default configuration.
- **ATT&CK Category:** Execution, Persistence, Privilege Escalation
- **ATT&CK Tag:** Scheduled Task, PowerShell
- **ATT&CK ID:** T1053.005, T1059.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

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

2.49 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
```

2.50 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
```

2.51 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")
```

2.52 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]
```

2.53 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
```

2.54 LP_HandleKatz Duplicating LSASS Handle

- **Trigger Condition:** 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="*)"
```

2.55 LP_PowerShell Execution Policy Modification Detected

- **Trigger Condition:** 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:**

```
label=Registry label=Set label=Value target_object IN ["*\ShellIds\Microsoft.
↪PowerShell\ExecutionPolicy*","*\Policies\Microsoft\Windows\PowerShell\ExecutionPolicy*"]
↪detail IN ["*Bypass*","*RemoteSigned'*","*Unrestricted*"] -"process" IN [
↪"C:\Windows\System32\*","C:\Windows\SysWOW64\*"]
```

2.56 LP_Devtoolslauncher Executes Specified Binary

- **Trigger Condition:** Usage of devtoolslauncher to execute other binaries. Adversaries attempt to bypass process or signature-based defences 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
```

2.57 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\DHCPServer\Parameters\CalloutDlls",
↪"*\Services\DHCPServer\Parameters\CalloutEnabled"] -user IN EXCLUDED_USERS
```

2.58 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
```

2.59 LP_DHCP Server Loaded the CallOut DLL

- **Trigger Condition:** Specified Callout DLL in the registry loaded by the DHCP server. Adversaries attempt to run their specified DLL through the DHCP server to achieve their objectives.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** DLL Side-Loading
- **ATT&CK ID:** T1574.002
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=1033 event_source="Microsoft-Windows-DHCP-Server" -user IN
↪EXCLUDED_USERS
```

2.60 LP_Disable of ETW Trace

- **Trigger Condition:** Usage of a command that clears or disables any Event Tracing for Windows (ETW) trace log. Adversaries can temporarily or permanently cease logging flow without generating any additional event-clear log entries from this tactic.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Indicator Blocking, Indicator Removal
- **ATT&CK ID:** T1562.006, T1070
- **Minimum Log Source Requirement:** Windows Sysmon, Windows, PowerShell
- **Query:**

```
(label="Process" label=Create
((command="*cl*" command="*/Trace*")
OR (command="*clear-log*" command="*/Trace*")
OR (command="*sl*" command="*/e:false*")
OR (command="*set-log*" command="*/e:false*")
OR (command="*logman*" command="*update*" command="*trace*" command="*--p*"
↪command="*-ets*")
OR command="*Remove-EtwTraceProvider*"
OR (command="*Set-EtwTraceProvider*" command="*0x11*"))
)
OR
(norm_id=WinServer event_id=4104
(script_block="*Remove-EtwTraceProvider *" OR (script_block="*Set-EtwTraceProvider *"
↪script_block="*0x11*"))
)
```

2.61 LP_Execution of Base64 Encoded Command Using IEX

- **Trigger Condition:** This alert detects the usage of the "IEX" (Invoke-Expression) cmdlet to execute encoded PowerShell commands.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** PowerShell
- **ATT&CK ID:** T1059.001

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

```
label="Process" label=Create command IN ["*SUVYIChb*", "*lFWCAoW*", "*JRVggKF*",
↪"*aWV4IChb*", "*lleCAoW*", "*pZXggKF*", "*aWV4IChOZXcn*", "*lleCAoTmV3J*",
↪"*pZXggKE5ldy*", "*SUVYIChOZX*", "*lFWCAoTmV3*", "*JRVggKE5ld*", "*SUVYKF*",
↪"*lFWChb*", "*JRVgoW*", "*aWV4KF*", "*lleChb*", "*pZXgoW*", "*aWV4KE5ld*",
↪"*lleChOZX*", "*pZXgoTmV3*", "*SUVYKE5ld*", "*lFWChOZX*", "*JRVgoTmV3*",
↪"*SUVYKCgn*", "*lFWCgoJ*", "*JRVgoKC*", "*aWV4KCgn*", "*lleCgoJ*", "*pZXgoKC*"]
↪command IN ["*SQBFAFgAIAAoAFsA*","*kARQBYACAAKABbA*","*JAEUAWAAgACgAWw*
↪","*aQBlAHgAIAAoAFsA*","*kAZQB4ACAAKABbA*","*pAGUAeAAgACgAWw*",
↪"*aQBlAHgAIAAoAE4AZQB3A*","*kAZQB4ACAAKABOAGUAdw*",
↪"*pAGUAeAAgACgATgBlAHcA*","*SQBFAFgAIAAoAE4AZQB3A*",
↪"*kARQBYACAAKABOAGUAdw*","*JAEUAWAAgACgATgBlAHcA*"]
```

2.62 LP_Discovery via PowerSploit Recon Module

- **Trigger Condition:** This alert is triggered whenever execution via PowerSploit Reconnaissance module is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** PowerShell
- **ATT&CK ID:** T1059.001
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id="WinServer" event_source="Microsoft-Windows-PowerShell" event_id=4104 script_
↪block IN POWERSPLOIT_RECON_MODULES
```

2.63 LP_DLL Load via LSASS Detected

- **Trigger Condition:** A DLL loaded through an undocumented Registry key via the LSASS process.
- **ATT&CK Category:** Persistence
- **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*"] -("process"=
↪"C:\Windows\system32\lsass.exe" detail IN ["%%systemroot%%\system32\ntdsa.dll", "%
↪%systemroot%%\system32\lsadb.dll"])
```

2.64 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 connot 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"]
```

2.65 LP_DNS ServerLevelPluginDll Install

- **Trigger Condition:** This alert is triggered whenever it detects the installation of a plugin DLL via ServerLevelPluginDll parameter in Registry,which can be used to execute code in context of the Application Layer Protocol, DNS server. A restart is required to have the change in effect.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Modify Registry, DLL Side-Loading
- **ATT&CK ID:** T1112, 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 *")
```

2.66 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.
- **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
```

2.67 LP_dotNET DLL Loaded Via Office Applications

- **Trigger Condition:** Assembly of DLL loaded by the Office Product.
- **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 ["*\excel.exe", "*\mspub.exe", "*\onenote.exe", "*\onenoteim.exe", "*\outlook.
↪exe", "*\powerpnt.exe", "*\winword.exe"]
image="*C:\Windows\assembly\*"
```

2.68 LP_DPAPI Domain Backup Key Extraction Detected

- **Trigger Condition:** Tools extracting the LSA secret DPAPI domain backup key from domain controllers.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** LSA Secrets
- **ATT&CK ID:** T1003.004
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
(norm_id=WinServer event_id=4662 object_type="SecretObject" access="0x2" object_name=
↪"*BCKUPKEY*")
```

2.69 LP_DPAPI Domain Master Key Backup Attempt

- **Trigger Condition:** An attempt to backup Data Protection API (DPAPI) master key is detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** LSA Secrets
- **ATT&CK ID:** T1003.004
- **Minimum Log Source Requirement:** Windows
- **Query:**

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

2.70 LP_Dridex Process Pattern Detected

- **Trigger Condition:** A typical dridex process patterns are detected.
- **ATT&CK Category:** Defense Evasion, Privilege , Discovery
- **ATT&CK Tag:** Process Injection, System Owner/User Discovery, Network Share Discovery

- **ATT&CK ID:** T1055, T1033, T1135
- **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
```

2.71 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
```

2.72 LP_Drupal Arbitrary Code Execution Detected

- **Trigger Condition:** This alert is triggered whenever 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, Web Server
- **Query:**

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

2.73 LP_Elevated Command Prompt Activity by Non-Admin User Detected

- **Trigger Condition:** Execution of an elevated command prompt by a non-admin user. Adversaries use this technique to execute commands or scripts that require a higher privilege than the regular users.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter
- **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
```

2.74 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
```

2.75 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 -NonI -W Hidden -Enc *", "* -noP -sta -w 1 -enc *", "* -NoP -NonI -
↪W Hidden -enc *","* -enc  SQB*","* -nop -exec bypass -EncodedCommand*"]
-user IN EXCLUDED_USERS
```

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

```
norm_id=WinServer event_id=4704 message="*SeEnableDelegationPrivilege*"
```

2.77 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")
```

2.78 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 IN ["104","1102","1100","1104"] event_source="Microsoft-
↪Windows-Eventlog"
```

2.79 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
```

2.80 LP_Execution in Non-Executable Folder Detected

- **Trigger Condition:** Process creation from an uncommon directory.
- **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"
```

2.81 LP_Execution in Webserver Root Folder Detected

- **Trigger Condition:** Execution of a suspicious program in a web service root folder (filter out false positives).
- **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"
```

2.82 LP_Execution of Renamed PaExec Detected

- **Trigger Condition:** Execution of renamed *paexec* via imphash and executable product string.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Indirect Command Execution
- **ATT&CK ID:** T1202
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id="WindowsSysmon" event_id=1 (description="PAExec Application" OR file="PAExec.
↪exe" OR application="*PAExec*" OR hash_import IN [
↪"11D40A7B7876288F919AB819CC2D9802", "6444f8a34e99b8f7d9647de66aabe516",
↪"dfd6aa3f7b2b1035b76b718f1ddc689f", "1a6cca4d5460b1710a12dea39e4a592c"]) -"process
↪" IN ["*\paexec.exe", "C:\Windows\PAExec-*"]
```

2.83 LP_Execution via Control Panel Items

- **Trigger Condition:** Execution of binary via Signed Binary Proxy Execution, Control Panel items.
- **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"="*\control.exe" command="*control*" command=
↪"*cpl*"
```

2.84 LP_Execution via HTA using IE JavaScript Engine Detected

- **Trigger Condition:** Execution of an HTA (HTML Application) file using the Internet Explorer JavaScript engine.
- **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"
```

2.85 LP_Suspicious Fsutil Invocation

- **Trigger Condition:** Execution of Fsutil with Createjournal, Deletejournal or setZeroData command-line argument.
- **ATT&CK Category:** Defense Evasion, Impact
- **ATT&CK Tag:** Indicator Removal, Data Destruction
- **ATT&CK ID:** T1070, T1485
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

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

2.86 LP_High Number of Process Termination

- **Trigger Condition:** When more than ten processes are terminated. In Microsoft Windows, processes can be terminated using task kill, service stop, and service delete. Adversaries can use this technique to kill, stop, or delete services or processes that could prevent payload execution.

- **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"="*\taskkill.exe" OR file="taskkill.exe") command =
↪"*/f*" command IN ["* /pid*", "* /im*", "* /t*"]) OR ("process" IN ["*\sc.exe", "*\net.exe",
↪"*\net1.exe"] command IN ["*delete*", "*disabled*", "*pause*", "*stop*"])) | chart count()
↪as occurrence by user, host, domain, "process", parent_process | search occurrence > 10
```

2.87 LP_Execution via Windows Scripting Host Component Detected

- **Trigger Condition:** Execution of a script using a system's Windows Scripting Host (WSH) component. WSH is a Microsoft technology that allows users to run scripts and automate tasks on Windows systems.
- **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"]
```

2.88 LP_Exim MTA Remote Code Execution Vulnerability Detected

- **Trigger Condition:** Remote code execution vulnerability in Exim MTA is detected.
- **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*"
```

2.89 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*"
```

2.90 LP_Existing Service Modification Detected

- **Trigger Condition:** A modification of an existing service via the *sc.exe* system utility is detected.
- **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="Process" label=Create "process" IN ["*sc.exe", "*powershell.exe", "*cmd.exe"]
↪command="*sc*" command="*config*" command="*binpath*" -user IN EXCLUDED_USERS
```

2.91 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
```

2.92 LP_File Creation by PowerShell Detected

- **Trigger Condition:** Creation of a new file using PowerShell on a system. Adversaries may use PowerShell to create new files, as a way to drop and execute malicious payloads, or to store data for later retrieval.
- **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"] -file IN ["*.mui"]
```

2.93 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
```

2.94 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.
- **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:\ProgramData\dynatrace\gateway\config\connectivity.history /reset" OR (command=
↪"*ICACLS C:\ProgramData\dynatrace\gateway\config\config.properties /grant :r *"
↪command="*S-1-5-19:F*")OR (command="*\AppData\Local\Programs\Microsoft VS Code*"
↪OR parent_process="*\Microsoft VS Code\Code.exe")) -user IN EXCLUDED_USERS
```

2.95 LP_File System Permissions Weakness

- **Trigger Condition:** A weakness in the file system permissions on a system is detected.
- **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
```

2.96 LP_Firewall Disabled via Netsh Detected

- **Trigger Condition:** *netsh* commands that turn off the Windows firewall are detected. Adversaries disable the firewall through *netsh* to bypass restrictions allowing connections with C&C servers.
- **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" OR file="netsh.exe") command=
↪"*set*" command="*firewall*"(( command="*opmode*" command="*disable*")
OR (command="*state*" command="*off*"))
```

2.97 LP_First Time Seen Remote Named Pipe

- **Trigger Condition:** The alert rule excludes the named pipes accessible remotely and notifies on new cases.
- **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
```

2.98 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
```

2.99 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
```

2.100 LP_Formbook Process Creation Detected

- **Trigger Condition:** This alert is triggered whenever it detects Formbook like process executions that inject code into a set of files in the System32 folder, which executes a special command line to delete the dropper from the AppData Temp folder.
- **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"]  parent_command="*.exe"
(command="*c*" command="*:\Users\*"
((command="*del*" command IN ["*\AppData\Local\Temp\*", "*\Desktop\*"]) OR (command=
↪"*type nul >*" command="*\Desktop\*")))
command="*.exe"
```

2.101 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=*
```

2.102 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
```

2.103 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
```

2.104 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
```

2.105 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
```

2.106 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
```

2.107 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
```

2.108 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
```

2.109 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
```

2.110 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 geoip(source_address) as
↪source_country | process geoip(destination_address) as destination_country
```

2.111 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=*
```

2.112 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
```

2.113 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=*
```

2.114 LP_GAC DLL Loaded Via Office Applications Detected

- **Trigger Condition:** GAC DLL loaded by an Office Product 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*", "*\mspub.exe","*\onenote.exe","*\onenoteim.exe"]
image IN ["*C:\Windows\Microsoft.NET\assembly\GAC_MSIL*"]
```

2.115 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
```

2.116 LP_Grabbing Sensitive Hives via Reg Utility

- **Trigger Condition:** This alert is triggered whenever sensitive Windows hives (SYSTEM, SAM, SECURITY) is accessed via Reg utility.
- **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 *", "*
↪ave *", "* e port *"] command IN ["*hklm*", "*hk m*", "*hkey_local_machine*", "*hkey_
↪ocal_machine*", "*hkey_loca _machine*", "*hkey_ oca _machine*"] command IN [
↪"*\system*", "*\sam*", "*\security*", "*\ystem*", "*\sy tem*", "*\y tem*", "*\ am*",
↪"*\ ecurity*"]
```

2.117 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
```

2.118 LP_HH Execution Detected

- **Trigger Condition:** Use of *hh.exe* to execute local Compiled HTML Help (CHM) or remote CHM files.
- **ATT&CK Category:** Defense Evasion, Initial Access
- **ATT&CK Tag:** Compiled HTML File, Spearphishing Attachment
- **ATT&CK ID:** T1218.001, T1566.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create ("process"="*\hh.exe" OR file="hh.exe")
command IN ["*.chm*", "*http*", "*.application*", "*\AppData\Local\*", "*\Content.Outlook\*
↪", "*\Downloads\*", "*\Users\Public\*", "*\Temp\*"]
```

2.119 LP_Hiding Files with Attrib Detected

- **Trigger Condition:** Use of *attrib.exe* to hide files from users.
- **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" OR FIle="ATTRIB.EXE") command =
↪"* +h *"
-(command = "*\desktop.ini*" OR (parent_process = "*\cmd.exe" command = "*+R +H +S +A
↪\*.cui*" parent_command = "*C:\WINDOWS\system32\*.bat*"))
```

2.120 LP_In-memory PowerShell Detected

- **Trigger Condition:** Loading of *System.Management.Automation.dll* by other processes than PowerShell.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** PowerShell
- **ATT&CK ID:** 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",
```

(continues on next page)

(continued from previous page)

```
"*\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", "*\sdiagnhost.exe",
 "*\servermanager.exe", "*\setup100.exe","*\ServiceHub.VSDetouredHost.exe",
 "*\SPCAF.Client.exe", "*\SPCAF.SettingsEditor.exe", "*\SQLPS.exe",
"*telemetryservice.exe", "*\UMWorkerProcess.exe", "*\w3wp.exe",
"*\wsmprovhost.exe","*\dsac.exe","*\RemoteFXvGPUDisablement.exe","*\runscripthelper.exe
↪",
"*\SyncAppvPublishingServer.exe","*\winrshost.exe","*\Windows\Microsoft.NET\Framework*
↪"] -user="NT AUTHORITY\SYSTEM"
```

2.121 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
```

2.122 LP_Indicator Blocking - Sysmon Registry Edited

- **Trigger Condition:** An indicator blocking via registry editing is detected.
- **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
```

2.123 LP_Suspicious InstallUtil Execution

- **Trigger Condition:** Manipulation of *InstallUtil* to execute proxy code via a trusted Windows utility. *InstallUtil* is a command-line utility that allows resource installation and uninstallation by executing specific installer components specified in .NET binaries.
- **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*")
```

2.124 LP_Java Running with Remote Debugging

- **Trigger Condition:** Operation of a JAVA process with remote debugging, allowing more than one local host to connect. Adversaries may abuse its functionality to execute arbitrary code on remote systems.
- **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*"]
```

2.125 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)
```

2.126 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
```

2.127 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)
```

2.128 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
```

2.129 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
```

2.130 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
```

2.131 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*"
```

2.132 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
```

2.133 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
```

2.134 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
```

2.135 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]
```

2.136 LP_Koadic Execution Detected

- **Trigger Condition:** Use of command line parameters associated with the Koadic hack tool during process creation events in Windows systems.
- **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
```

2.137 LP_Local Account Creation on Workstation Detected

- **Trigger Condition:** This alert is triggered whenever a local account creation on a domain workstation that is not a DC is detected.
- **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
```

2.138 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
```

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

- **Trigger Condition:** This alert is triggered whenever creation of log files of Dot-Net-to-JavaScript is detected.
- **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 ["*cmstp.exe.log",
↪"*cscript.exe.log", "*wscript.exe.log", "*wmic.exe.log", "*mshta.exe.log", "*msxsl.exe.log",
↪"*svchost.exe.log", "*regsvr32.exe.log", "*rundll32.exe.log"]
```

2.140 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*",
↪"*aXRzYWRtaW4gL3RyYW5zZmVy*",
"*IAaQB0AHMAYQBkAG0AaQBuACAALwB0AHIAYQBuAHMAZgBlAHIA*",
↪"*JpdHNhZG1pbiAvdHJhbnNmZX*",
↪"*YgBpAHQAcwBhAGQAbQBpAG4AIAAvAHQAcgBhAG4AcwBmAGUAcg*",
↪"*Yml0c2FkbWluIC90cmFuc2Zlc*",
"*AGMAaAB1AG4AawBfAHMAaQB6AGUA*", "*JABjAGgAdQBuAGsAXwBzAGkAegBlA*",
↪"*JGNodW5rX3Npem*","*QAYwBoAHUAbgBrAF8AcwBpAHoAZQ*", "*RjaHVua19zaXpl*",
↪"*Y2h1bmtfc2l6Z*",
"*AE8ALgBDAG8AbQBwAHIAZQBzAHMAaQBvAG4A*",
↪"*kATwAuAEMAbwBtAHAAcgBlAHMAcwBpAG8Abg*", "*lPLkNvbXByZXNzaW9u*",
"*SQBPAC4AQwBvAG0AcAByAGUAcwBzAGkAbwBuA*", "*SU8uQ29tcHJlc3Npb2*",
↪"*Ty5Db21wcmVzc2lvb*", "*AE8ALgBNAGUAbQBvAHIAeQBTAHQAcgBlAGEAbQ*",
↪"*kATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtA*",
"*lPLk1lbW9yeVN0cmVhb*","*SQBPAC4ATQBlAG0AbwByAHkAUwB0AHIAZQBhAG0A*",
↪"*SU8uTWVtb3J5U3RyZWFt*", "*Ty5NZW1vcnlTdHJlYW*",
↪"*4ARwBlAHQAQwBoAHUAbgBrA*", "*5HZXRDaHVua*","*AEcAZQB0AEMAaAB1AG4Aaw*
↪",
"*LgBHAGUAdABDAGgAdQBuAGsA*", "*LkdldENodW5r*","*R2V0Q2h1bm*",
↪"*AEgAUgBFAEEARABfAEkATgBGAE8ANgA0A*",
↪"*QASABSAEUAQQBEAF8ASQBOAEYATwA2ADQA*", "*RlUkVBRF9JTkZPNj*",
"*SFJFQURfSU5GTzY0*", "*VABlAFIARQBBAEQAXwBJAE4ARgBPADYANA*",
↪"*VEhSRUFEX0lORk82N*",
"*AHIAZQBhAHQAZQBSAGUAbQBvAHQAZQBUAGgAcgBlAGEAZA*",
↪"*cmVhdGVSZW1vdGVUaHJlYW*",
↪"*MAcgBlAGEAdABlAFIAZQBtAG8AdABlAFQAaAByAGUAYQBkA*",
↪"*NyZWF0ZVJlbW90ZVRocmVhZ*", "*Q3JlYXRlUmVtb3RlVGhyZWFk*",
"*QwByAGUAYQB0AGUAUgBlAG0AbwB0AGUAVABoAHIAZQBhAGQA*",
↪"*0AZQBtAG0AbwB2AGUA*", "*1lbW1vdm*", "*AGUAbQBtAG8AdgBlA*",
↪"*bQBlAG0AbQBvAHYAZQ*", "*bWVtbW92Z*", "*ZW1tb3Zl*"] -user IN EXCLUDED_USERS
```

2.141 LP_Malicious Service Installations Detected

- **Trigger Condition:** Installation of malicious services. Adversaries install such services for lateral movement, credential dumping, and other suspicious activity.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Service Execution
- **ATT&CK ID:** T1569.002
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="Install" label="Service" service IN ["*\PAExec*", "mssecsvc2.0", "*net user*",
↪"WCESERVICE", "WCE SERVICE", "winexesvc.exe*", "*\DumpSvc.exe", "pwdump*",
↪"gsecdump*", "cachedump*"]
```

2.142 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
```

2.143 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
```

2.144 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
```

2.145 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
```

2.146 LP_Meterpreter or Cobalt Strike Getsystem Service Start Detected

- **Trigger Condition:** This alert is triggered whenever it detects the use of getsystem Meterpreter/Cobalt Strike command to obtain SYSTEM privileges by detecting a specific service starting.

- **ATT&CK Category:** Privilege Escalation
- **ATT&CK Tag:** Token Impersonation/Theft, Create Process with Token
- **ATT&CK ID:** T1134.001, T1134.002
- **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*"
```

2.147 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
```

2.148 LP_Mimikatz Command Line Detected

- **Trigger Condition:** This alert is triggered whenever well-known 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*", "*::printnightmare*",
↪ "*::skeleton*", "*::preshutdown*", "*::mstsc*", "*::multirdp*", "*rpc::*", "*token::*",
↪"*crypto::*", "*dpapi::*", "*sekurlsa::*", "*kerberos::*", "*lsadump::*", "*privilege::*",
↪"*process::*", "*vault::*","*crypto::*","*misc::*","*event::*","*IIS::AppHost*","*net::*","*sid::*
↪","*standard::*","*vault::*"]
```

2.149 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
```

2.150 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
```

2.151 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
```

2.152 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","*\BITSADMIN*", "*\mshta.exe"]
```

2.153 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
```

2.154 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
```

2.155 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"]
```

2.156 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
```

2.157 LP_MSTSC Shadowing Detected

- **Trigger Condition:** This alert is triggered whenever it detects RDP session hijacking by using MSTSC (Microsoft Terminal Services Client) shadowing.
- **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="Process" label=Create command="*noconsentprompt*" command="*shadow:*"
```

2.158 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
```

2.159 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"
```

2.160 LP_Narrators Feedback-Hub Persistence Detected

- **Trigger Condition:** Attempt made to abuse Windows 10 Narrator's Feedback-Hub.
- **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:**

```
(event_id=12 event_type="DeleteValue" target_object=
↪"*\AppXypsaf9f1qserqevf0sws76dx4k9a5206\Shell\open\command\DelegateExecute") OR
↪(event_id=13 target_object=
↪"*\AppXypsaf9f1qserqevf0sws76dx4k9a5206\Shell\open\command\(Default)")
```

2.161 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
```

2.162 LP_NetNTLM Downgrade Attack Detected

- **Trigger Condition:** Post exploitation using NetNTLM downgrade attacks.
- **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:**

```
norm_id="WindowsSysmon" (event_id=13 target_object IN [
↪"*SYSTEM\*ControlSet*\Control\Lsa\lmcompatibilitylevel",
↪"*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"])
```

2.163 LP_Network Share Connection Removed

- **Trigger Condition:** This alert is triggered whenever it detects the removal of the share connection. A network share is a shared folder or directory on a network that allows multiple users to access and share files or resources. Adversaries may use network shares to gain unauthorized access to sensitive data or resources on a network or distribute their malware. After finishing their operation, they may remove share connections that are no longer useful in order to clean up 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*"
```

2.164 LP_Network Sniffing Detected

- **Trigger Condition:** This alert is triggered whenever the execution of network sniffing tools is detected.
- **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
```

2.165 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'}")
```

2.166 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 ["*\AppData\Local\Microsoft\OneDrive\\*"] -user IN
↪EXCLUDED_USERS
```

2.167 LP_New Service Creation

- **Trigger Condition:** This alert is triggered whenever it detects creation of a new service. Windows Services can allow creation and management of long running processes.
- **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="Process" label=Create "process" IN ["*sc.exe", "*powershell.exe", "*cmd.exe"]
↪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
```

2.168 LP_NoPowerShell Tool Activity Detected

- **Trigger Condition:** This alert is triggered whenever execution of NoCommand and Scripting Interpreter, PowerShell tool is detected.
- **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"
```

2.169 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
```

2.170 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
```

2.171 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
```

2.172 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
```

2.173 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=*
```

2.174 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
```

2.175 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
```

2.176 LP_Password Dumper Remote Thread in LSASS

- **Trigger Condition:** This alert is triggered whenever it detects password dumper activity in LSASS.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** LSASS Memory
- **ATT&CK ID:** T1003.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label=Remote label=Thread label=Create image="*\lsass.exe" start_module=""
```

2.177 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
```

2.178 LP_Persistence and Execution at Scale via GPO Scheduled Task

- **Trigger Condition:** Attempt to access the SYSVOL share, explicitly targeting the *ScheduleTasks.xml* file with writeData permissions. SYSVOL is a critical directory on Windows domain controllers that stores domain-wide data, including Group Policy objects.
- **ATT&CK Category:** Persistence, 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*"
```

2.179 LP_Possible Account Misuse-Privilege Escalation

- **Trigger Condition:** 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*)
```

2.180 LP_Possible Applocker Bypass Detected

- **Trigger Condition:** This alert is triggered whenever it detects the execution of potentially suspicious executables capable of bypassing AppLocker whitelisting.
- **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="Process" label=Create command IN ["*\msdt.exe*", "*\installutil.exe*", "*\regsvcs.exe*
↪", "*\regasm.exe*", "*\msbuild.exe*", "*\ieexec.exe*"]
```

2.181 LP_File Download via Bitsadmin Detected

- **Trigger Condition:** Use of *bitsadmin* to download a file.
- **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 (command="* /transfer *")) OR (command="*copy bitsadmin.exe*")
```

2.182 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
```

2.183 LP_Possible CLR DLL Loaded Via Office Applications

- **Trigger Condition:** This alert is triggered whenever it detects CLR DLL being loaded by an Office Product like Winword, PowerPoint, Excel, or Outlook.
- **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", "*\onenote.exe", "*\onenoteim.exe"] image IN ["*\clr.dll*"]
```

2.184 LP_Credential Dumping Tools Named Pipes Detected

- **Trigger Condition:** This alert is triggered whenever it detects well-known credential dumping tools execution via specific named pipes like lsadump,cachedump,wceservicepipe,etc.
- **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*"]
```

2.185 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
```

2.186 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
```

2.187 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
```

2.188 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
```

2.189 LP_Possible Empire Monkey Detected

- **Trigger Condition:** This alert is triggered whenever it detects the execution of a specific command line sequence using the cutil.exe or regsvr32.exe tools. Empire Monkey is an advanced persistent threat (APT) group that has been involved in cyber espionage activities.
- **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"))
```

2.190 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
```

2.191 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
```

2.192 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
```

2.193 LP_Malicious Payload Download via Office Binaries

- **Trigger Condition:** This alert is triggered whenever an arbitrary file is downloaded using Microsoft Office binaries.
- **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
```

2.194 LP_PowerShell Script Execution from Suspicious Location

- **Trigger Condition:** Suspicious command line that invokes PowerShell from a suspicious location.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** PowerShell
- **ATT&CK ID:** T1059.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows, PowerShell
- **Query:**

```
label="Process" label=Create command IN ["*powershell*", "*pwsh*"] command="*-c *"
↪command IN ["*\AppData*", "*\ProgramData*", "*\Users\Public*", "*\PerfLogs*",
↪"*\Windows\Temp*", "*\Windows\Tracing*"]
```

2.195 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=*)
```

2.196 LP_Possible Modification of Boot Configuration

- **Trigger Condition:** Use of the bcdedit command to delete or modify Boot Configuration Data. Boot Configuration Data (BCD) files provide a store that describes boot applications and application settings. Boot configuration data edit (bcdedit) allows manipulation of BCD. This tactic is used by malware or attackers to prevent system recovery. Legitimate usage can trigger this alert. We recommend including legitimate users 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, Windows
- **Query:**

```
label="Process" label="Create" (("process"="*\bcdedit.exe" command IN ["*deletevalue*",
↪"*delete*", "*import*","*set*"]) OR ((command="*bootstatuspolicy*" command=
↪"*ignoreallfailures*") OR (command="*recoveryenabled*" command="*no*")))
```

2.197 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
```

2.198 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
```

2.199 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
```

2.200 LP_Possible Process Hollowing Image Loading

- **Trigger Condition:** Loading of *samlib.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 ["*\samlib.dll", "*\WinSCard.dll"] -user IN EXCLUDED_USERS
```

2.201 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, Windows
- **Query:**

```
label="Process" label=Create
("process"="*\setspn.exe" OR
(description="*Query or reset the computer's SPN attribute" file=setspn.exe) )
command IN ["* -q *","* /q *"]
```

2.202 LP_Possible Taskmgr run as LOCAL_SYSTEM Detected

- **Trigger Condition:** This alert is triggered whenever it detects the creation of taskmgr.exe process in the context of LOCAL_SYSTEM.
- **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*"]
```

2.203 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="*AAAAYInlM*" script_block IN [
↪"*OiCAAAAYInlM*", "*OiJAAAAYInlM*"]
```

2.204 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
```

2.205 LP_PowerShell Profile Modification

- **Trigger Condition:** Modification of a PowerShell profile using the Write-Output or Add-Content command.
- **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, PowerShell
- **Query:**

```
norm_id=WinServer event_id=4103 command in ["*Write-Output*", "*Add-Content*"]
↪payload= "*powershell_profile*"
```

2.206 LP_PowerShell Version Downgrade Detected

- **Trigger Condition:** Execution of legacy PowerShell version 2.
- **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_id=400 event_source="Powershell" host_version="*2*" -engine_
↪version="*2*")
OR (label="Process" label="Create"  "process"="*\powershell.exe"  (command IN ["*-version
↪2*",  "*-versio 2*", "*-versi 2*",  "*-vers 2*", "*-ver 2*","*-ve 2*", "*-v 2*"]))
```

2.207 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
```

2.208 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
```

2.209 LP_Process Hollowing Detected

- **Trigger Condition:** This alert is triggered whenever process hollowing is detected.
- **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, Windows
- **Query:**

```
label="Create" label="Process" ("process"="*smss.exe" parent_command!="*smss.exe") or (
↪"process"="*csrss.exe" (parent_command!="*smss.exe" and parent_command!="*svchost.
↪exe")) or ("process"="*wininit.exe" parent_command!="*smss.exe") or ("process"=
↪"*winlogon.exe" parent_command!="*smss.exe") or ("process"="*lsass.exe" parent_
↪command!="*wininit.exe") or ("process"="*LogonUI.exe" (parent_command!="*winlogon.
↪exe" and parent_command!="*wininit.exe")) or ("process"="*services.exe" parent_
↪command!="*wininit.exe") or ("process"="*spoolsv.exe" parent_command!="*services.exe
↪") or ("process"="*taskhost.exe" (parent_command!="*services.exe" and parent_command!
↪="*svchost.exe")) or ("process"="*taskhostw.exe" (parent_command!="*services.exe" and
↪parent_command!="*svchost.exe")) or ("process"="*userinit.exe" (parent_command!=
↪"*dwm.exe" and parent_command!="*winlogon.exe")) -user IN EXCLUDED_USERS
```

2.210 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\sysnative\*") -user IN EXCLUDED_USERS
```

2.211 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
```

2.212 LP_Psr Capture Screenshots Detected

- **Trigger Condition:** This alert is triggered when psr utility is used by adversaries to take screen captures of the desktop to gather information over the course of an operation.
- **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
```

2.213 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
```

2.214 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
```

2.215 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
```

2.216 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
```

2.217 LP_RDP Registry Modification

- **Trigger Condition:** This alert is triggered whenever remote desktop protocol (RDP) registry keys are modify to enable RDP.
- **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 IN ["*\CurrentControlSet\Control\Terminal
↪Server\WinStations\RDP-Tcp\UserAuthentication",
"*\CurrentControlSet\Control\Terminal Server\fDenyTSConnections"]
detail="DWORD (0x00000000)" -user IN EXCLUDED_USERS
```

2.218 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\fSingleSessionPerUser*", "*\Control\Terminal Server\fDenyTSConnections*"] -user IN
↪EXCLUDED_USERS
```

2.219 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
```

2.220 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
```

2.221 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
```

2.222 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
```

2.223 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
```

2.224 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
```

2.225 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
```

2.226 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
```

2.227 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
```

2.228 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="User32LogonProcesss" -user IN
↪EXCLUDED_USERS
```

2.229 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
```

2.230 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")
```

2.231 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"))
```

2.232 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
```

2.233 LP_Renamed Binary Detected

- **Trigger Condition:** This alert is triggered whenever it detects the execution of a renamed binary.
- **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
```

2.234 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"]
```

2.235 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
- **Query:**

```
label=Accesspoint label=Rogue -label=Clear access_point=*
```

2.236 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
```

2.237 LP_Rubeus Hack Tool Detected

- **Trigger Condition:** This alert is triggered whenever it detects command line parameters like asreproast, dump, impersonate user, harvest, and other commands used by the Rubeus hack tool. The Rubeus hack tool is a popular command-line tool used by attackers to perform various attacks related to credential access such as Kerberoasting in Windows environments.
- **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 command IN ["*asreproast *", "*dump /service:krbtgt *",
↪"*dump /luid:0x*", "*kerberoast *", "*createnetonly /program:*", "*ptt /ticket:*", "*/
↪impersonateuser:*", "*renew /ticket:*", "*asktgt /user:*", "*harvest /interval:*", "*s4u /user:*",
↪ "*s4u /ticket:*", "*hash /password:*", "*golden /aes256:*", "*silver /user:*"] ("process"=
↪"*\Rubeus.exe" OR file="Rubeus.exe" OR description="Rubeus")
```

2.238 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
```

2.239 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
```

2.240 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
```

2.241 LP_SecurityXploded Tool Detected

- **Trigger Condition:** Execution of the SecurityXploded tools. Adversaries abuse these tools for credential access or other malicious purposes.
- **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
```

2.242 LP_smbexec Service Installation Detected

- **Trigger Condition:** Usage of the *smbexec.py* tool to identify a specific service installation.
- **ATT&CK Category:** Lateral Movement, Execution
- **ATT&CK Tag:** SMB/Windows Admin Shares, Service Execution
- **ATT&CK ID:** T1021.002, T1569.002
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=7045 (provider="Service Control Manager" or event_source=
↪"Service Control Manager") (service="BTOBTO" OR path IN ["*.bat & del *","*__output 2^>
↪^&1 >*"]) -user IN EXCLUDED_USERS
```

2.243 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
```

2.244 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
```

2.245 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
```

2.246 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
```

2.247 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
```

2.248 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
```

2.249 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
```

2.250 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
```

2.251 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]
```

2.252 LP_Stealthy Scheduled Task Creation via VBA Macro Detected

- **Trigger Condition:** Office products such as Word, Excel, PowerPoint and Outlook.exe load *taskschd.dll*.
- **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"]
```

2.253 LP_Sticky Key Like Backdoor Usage Detected

- **Trigger Condition:** This alert is triggered upon detecting the utilization and installation of a backdoor employing a method to register a malicious debugger for native tools accessible from the login screen.
- **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:**

```
(
label=Registry label=Set label=Value event_type="SetValue"
target_object IN ["*\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
↪Options\sethc.exe\Debugger",
"*\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\utilman.
↪exe\Debugger",
"*\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\osk.
↪exe\Debugger",
"*\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Magnify.
↪exe\Debugger",
"*\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Narrator.
↪exe\Debugger",
"*\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
↪Options\DisplaySwitch.exe\Debugger",
"*\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\atbroker.
↪exe\Debugger",
"*\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\HelpPane.
↪exe\Debugger"]
)
OR
(
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*",
"*\CurrentVersion\Image File Execution Options\HelpPane.exe*"]
)
OR
(
label="Process" label=Create
"process" IN ["*\cmd.exe","*\cscript.exe","*\mshta.exe","*\powershell.exe","*\pwsh.exe",
↪"*\regsvr32.exe", "*\rundll32.exe","*\wscript.exe","*\wt.exe"]
command IN ["*sethc.exe*", "*utilman.exe*", "*osk.exe*", "*Magnify.exe*", "*Narrator.exe*",
↪"*DisplaySwitch.exe*"]
)
```

2.254 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
```

2.255 LP_Successful Lateral Movement to Administrator via Pass the Hash using Mimikatz Detected

- **Trigger Condition:** This alert is triggered whenever 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
```

2.256 LP_Successful Overpass the Hash Attempt

- **Trigger Condition:** Successful Overpass-the-Hash Attempt is detected. This attack involves exploiting both pass-the-hash and pass-the-ticket techniques. Adversaries use this technique when obtaining a cleartext password is impossible, but Kerberos authentication can be used to access the target system.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Pass the Hash

- **ATT&CK ID:** T1550.002
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4624 logon_type="9" logon_process="seclogo" package=
↪"Negotiate" -user IN EXCLUDED_USERS
```

2.257 LP_Suspect Svchost Memory Access

- **Trigger Condition:** Suspicious access to svchost process memory such as that used by Invoke-Phantom, to kill the WinRM Windows event logging service. The *svchost.exe* process is a legitimate system that hosts multiple Windows services. 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*"
```

2.258 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
```

2.259 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
```

2.260 LP_Suspicious Call by Ordinal Detected

- **Trigger Condition:** Suspicious execution of exported functions in DLLs through RunDLL32 via ordinal (16-bit integer).
- **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 IN ["*,#*", "*, #*", "*.dll #*", "*.ocx #*"]
-command="*EDGEHTML.DLL*#141*"
-(parent_process IN ["*\Msbuild\Current\Bin\*", "*\VC\Tools\MSVC\*", "*\Tracker.exe"]
command IN ["*\FileTracker32.dll,#1*", '*\FileTracker32.dll",#1*', "*\FileTracker64.dll,#1*",
↪'*\FileTracker64.dll",#1*'])
```

2.261 LP_Suspicious Compression Tool Parameters

- **Trigger Condition:** Suspicious command line arguments of standard data compression tools such as 7z and Rar are detected. Adversaries can utilize these techniques to compress data to exfiltrate those data.
- **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", "WinRAR.exe"] OR description="Command
↪line RAR") OR "process" IN ["*\7z.exe","*\rar.exe"] ) command IN ["* -p*", "* -ta*", "* -tb*",
↪"* -sdel*", "* -dw*", "* -hp*"] -(parent_process="*:\Program Files*" OR parent_process=
↪"*:\Program Files (x86)*") ) OR ("process"="*\rar.exe" command="* a *")
```

2.262 LP_Suspicious Control Panel DLL Load Detected

- **Trigger Condition:** Suspicious execution of Rundll32 from *control.exe*. Adversaries may use this technique to proxy execute their malicious applications through signed binary without being noticed by the security controls.
- **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" ("process"=
↪"*\rundll32.exe" OR file="RUNDLL32.EXE") -command="*Shell32.dll*" )
```

2.263 LP_Suspicious Csc Source File Folder Detected

- **Trigger Condition:** Suspicious execution of *csc.exe* that uses a source in a suspicious folder like AppData. Adversaries often download their source code and compile it in the victim's computer using the functionality of *csc.exe*.
- **ATT&CK Category:** Execution, Defense Evasion
- **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" OR file="csc.exe")
(
(command IN ["*:\Perflogs\*", "*:\Users\Public\*", "*\AppData\Local\Temp\*", "*\Temporary
↪Internet", "*\Windows\Temp\*" ])
OR
(parent_command IN ["*\cscript.exe", "*\excel.exe", "*\mshta.exe", "*\onenote.exe",
↪"*\outlook.exe", "*\powerpnt.exe", "*\winword.exe", "*\wscript.exe"])
OR
(parent_command IN ["*\powershell.exe", "*\pwsh.exe"] parent_command IN ["*-Encoded*",
↪"*FromBase64String*"])
OR
(command="*:\Users\*" command IN ["*\Favorites\*", "*\Favourites\*", "*\Contacts\*",
↪"*\Pictures\*"])
OR
(command IN ["*ProgramData\*", "*%LocalAppData%\*", "*%AppData%\*",
↪"*\AppData\Local\*", "*\AppData\LocalLow\*", "*Roaming\*"])
)
(
-(parent_process IN ["C:\Program Files (x86)\*", "C:\Program Files\*"]  OR parent_process=
↪"C:\Windows\System32\sdiagnhost.exe" OR parent_process=
↪"C:\Windows\System32\inetsrv\w3wp.exe")
)
(
-(parent_process IN ["C:\ProgramData\chocolatey\choco.exe",
↪"C:\ProgramData\chocolatey\tools\shimgen.exe"] OR parent_command=
↪"*\ProgramData\Microsoft\Windows Defender Advanced Threat Protection*"
OR parent_command IN [
↪"*JwB7ACIAZgBhAGkAbABlAGQAIgA6AHQAcgB1AGUALAAiAG0AcwBnACIAOgAiAEEAbgBzAGkAYgBsAG
↪",
↪"*cAewAiAGYAYQBpAGwAZQBkACIAOgB0AHIAdQBlACwAIgBtAHMAZwAiADoAIgBBAG4AcwBpAGIAbAB
↪",
↪"*nAHsAIgBmAGEAaQBsAGUAZAAiADoAdAByAHUAZQAsACIAbQBzAGcAIgA6ACIAQQBuAHMAaQBiAGw
↪"])
```

(continues on next page)

(continued from previous page)

```
)
```

2.264 LP_Suspicious Double Extension Detected

- **Trigger Condition:** This alert is triggered whenever it detects a double extension of a file.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** Spearphishing Attachment
- **ATT&CK ID:** T1566.001
- **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"]) (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*" ])
```

2.265 LP_Suspicious Driver Load from Temp

- **Trigger Condition:** Driver loaded from a temporary directory.
- **ATT&CK Category:** Persistence, Privilege Escalation
- **ATT&CK Tag:** Windows Service
- **ATT&CK ID:** T1543.003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=6 file="*\Temp\*" -user IN EXCLUDED_USERS
```

2.266 LP_Suspicious Eventlog Clear or Configuration Using Wevtutil Detected

- **Trigger Condition:** Clearing or configuration of eventlogs uwing wevtutil, PowerShell and wmic. Adversaries use this technique to delete the logs and hide their traces.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Clear Windows Event Logs, Disable Windows Event Logging
- **ATT&CK ID:** T1070.001, T1562.002
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **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 *","*lfn: "])
)
-(parent_process IN ["C:\Windows\SysWOW64\msiexec.exe","C:\Windows\System32\msiexec.
↪exe"] command="* sl *")
```

2.267 LP_Suspicious GUP Usage Detected

- **Trigger Condition:** This alert is triggered whenever it detects execution of the Notepad++ updater in a suspicious directory, which is often used in DLL side-loading attacks.
- **ATT&CK Category:** Defense Evasion, Persistence, Privilege Escalation
- **ATT&CK Tag:** DLL Side-Loading
- **ATT&CK ID:** 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"]))
```

2.268 LP_Suspicious Kerberos RC4 Ticket Encryption

- **Trigger Condition:** This alert is triggered whenever it detects service ticket requests using RC4 encryption type.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Kerberoasting
- **ATT&CK ID:** T1558.003
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4769 ticket_option="0x40810000" Encryption_type="0x17" -
↪service="*$"
```

2.269 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", "\wceservicepipe", "\psexec", "\mojo.5688.8052.183894939787088877",
↪"\mojo.5688.8052.35780273329370473", "\mypipe-f", "\mypipe-h", "\ntsvcs_", "\scerpc_",
↪"\DserNamePipe", "\srvsvc_", "\status_", "\MSSE-", "\postex_", "\spoolss_", "\winsock",
↪"\win_svc", "\dce_86" ]
```

(continues on next page)

(continued from previous page)

2.270 LP_Suspicious Outbound Kerberos Connection

- **Trigger Condition:** This alert is triggered whenever it detects suspicious outbound network activity via kerberos.
- **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
```

2.271 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
```

2.272 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*). Adversaries 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", "*\jbosssvc.exe", "*MicrosoftEdgeSH.exe", "*tomcat*"]
("process"IN ["*\powershell.exe", "*\pwsh.exe"] OR command IN ["*/c powershell*", "*/c
↪pwsh*"])
-path="*\Health Service State\*"
```

2.273 LP_Suspicious Process Start Locations Detected

- **Trigger Condition:** This alert is triggered whenever it detects the execution of suspicious processes from unusual locations like Recycle bin, Fonts folder, etc.
- **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\*
↪"]
```

2.274 LP_Suspicious Program Location with Network Connections

- **Trigger Condition:** Programs with network connections executed 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
```

2.275 LP_Suspicious PsExec Execution Detected

- **Trigger Condition:** This alert is triggered whenever it detects execution of psexec or paexec with renamed service name, this rule helps to filter out the noise if psexec is used for legit purposes or if attacker uses a different psexec client other than sysinternal one.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Lateral Tool Transfer
- **ATT&CK ID:** T1570
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=5145 share_path="*\*" share_path="*\IPC$*" relative_target IN [
↪"*-stdin", "*-stdout", "*-stderr"]
-relative_target="PSEXESVC*"
```

2.276 LP_Suspicious Remote Thread Created

- **Trigger Condition:** This alert is triggered to detect suspicious processes (those we would not expect to behave in this way like word.exe or outlook.exe) creating 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 be run in the new thread: StartAddress, StartModule and StartFunction.
- **ATT&CK Category:** Privilege Escalation, Defense Evasion
- **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", "*\cscript.exe", "*\cvtres.
↪exe", "*\defrag.exe", "*\dnx.exe",
"*\esentutl.exe", "*\excel.exe", "*\expand.exe", "*\find.exe", "*\findstr.exe", "*\forfiles.exe",
↪"*\gpupdate.exe", "*\hh.exe",
"*\installutil.exe", "*\lync.exe", "*\makecab.exe", "*\mDNSResponder.exe", "*\monitoringhost.
↪exe", "*\msbuild.exe",
"*\mshta.exe", "*\mspaint.exe", "*\outlook.exe", "*\ping.exe", "*\provtool.exe", "*\python.exe
↪", "*\regsvr32.exe",
"*\robocopy.exe", "*\runonce.exe", "*\sapcimc.exe", "*\smartscreen.exe", "*\spoolsv.exe",
↪"*\tstheme.exe",
"*\userinit.exe", "*\vssadmin.exe", "*\vssvc.exe", "*\w3wp.exe", "*\winscp.exe", "*\winword.
↪exe", "*\wmic.exe", "*\wscript.exe"] -"process"="*Visual Studio*"
```

2.277 LP_Suspicious RUN Key from Download Detected

- **Trigger Condition:** Suspicious RUN keys created by software located in the Download or temporary Outlook/Internet Explorer directories that may signal malicious activity.
- **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
```

2.278 LP_Suspicious Rundll32 Activity Detected

- **Trigger Condition:** This alert is triggered whenever it detects suspicious processes related to the RunDLL32 system binary based on its command line arguments.
- **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="*zipfldr.dll*" command="*RouteTheCall*")
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="*SetupInfObjectInstallAction*")
OR (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*")
```

(continues on next page)

(continued from previous page)

```
OR (command="*comsvcs.dll*" command="*MiniDump*")
OR (command="*\\*\*,*")
)
-(
(command="*shell32.dll,Control_RunDLL desk.cpl,screensaver,@screensaver*")
OR (parent_process="C:\Windows\System32\control.exe" parent_command="*.cpl*"
(command="*.cpl*" command="*Shell32.dll*" command="*Control_RunDLL*"))
OR (command="*rundll32*Shell32.dll,Control_RunDLL*C:\Windows\System32\*" parent_
↪process="C:\Windows\System32\control.exe"
command='.cpl", ')
)
```

2.279 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="*binpath*" command=
↪"*config*"
 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*"]
```

2.280 LP_Suspicious TSCON Start

- **Trigger Condition:** Execution of *tscon.exe* process as local system. If *tscon.exe* run as system, adversaries can gain access to the currently logged-in session without credentials.
- **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","*AUTHORI*", "*AUTORI*"] "process"=
↪"*\tscon.exe"
```

2.281 LP_Potential Suspicious Malware Callback Communication

- **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 ["100", "198", "200", "243", "473", "666", "700", "743", "777", "1443",
↪"1515", "1777", "1817", "1904", "1960", "2443", "2448", "3360", "3675", "3939", "4040",
↪"4433", "4438", "4443", "4444", "4455", "5445", "5552", "5649", "6625", "7210", "7777",
↪"8143", "8843", "9631", "9943", "10101", "12102", "12103", "12322", "13145", "13394",
↪"13504", "13505", "13506", "13507", "14102", "14103", "14154", "49180", "65520", "65535"] -
↪image="*\Program Files*" -destination_address IN HOMENET -user IN EXCLUDED_USERS
```

2.282 LP_Suspicious Userinit Child Process

- **Trigger Condition:** This alert is triggered whenever it detects a suspicious process spawned by Userinit.
- **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")))
```

2.283 LP_Suspicious Windows ANONYMOUS LOGON Local Account Creation

- **Trigger Condition:** Creation of suspicious accounts similar to ANONYMOUS LOGON, like using additional spaces. This rule catches 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
```

2.284 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%*", "*%ProgramData%*", "*%appdata%*", "*%comspec%*", "*%localappdata%" ]
```

2.285 LP_SysKey Registry Keys Access

- **Trigger Condition:** Handle requests and access operations to specific registry keys to calculate the SysKey. Adversaries use a tool like Mimikatz or a script like Invoke-PowerDump to get the SysKey, decrypt Security Account Manager (SAM) database entries from the registry or hive, and get NTLM and LM hashes of local account 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
```

2.286 LP_Sysmon Configuration Modification Detected

- **Trigger Condition:** This alert is triggered whenever modification of Sysmon(System Monitor) Configuration is detected.
- **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
```

2.287 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
```

2.288 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
```

2.289 LP_System Service Discovery

- **Trigger Condition:** This alert is triggered when binaries that can be used to retrieve Windows service information are 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*"]
```

2.290 LP_Tap Driver Installation Detected

- **Trigger Condition:** Installation of TAP software. It indicates possible preparation for data exfiltration using tunnelling 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
```

2.291 LP_Tasks Folder Evasion Detected

- **Trigger Condition:** Usage of the Windows tasks folder for evasion purposes. Adversaries can take advantage of this and load or influence any script hosts or any .NET application in tasks 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\*"]
```

2.292 LP_Terminal Service Process Spawn Detected

- **Trigger Condition:** Process spawned by the terminal service server process. 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
- **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"]
```

2.293 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
```

2.294 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
```

2.295 LP_Transfering Files with Credential Data via Network Shares

- **Trigger Condition:** This alert is triggered whenever sensitive files with well-known file names (such as the ones containing credential data) are transferred using network shares.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** LSASS Memory, Security Account Manager, NTDS
- **ATT&CK ID:** T1003.001, T1003.002, T1003.003

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

```
norm_id=WinServer event_id=5145 relative_target IN ["*\mimidrv*", "*\lsass*",
↪"*\windows\minidump\*", "*\hiberfil*", "*\sqldmpr*", "*\sam*", "*\ntds.dit*", "*\security*"]
```

2.296 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
```

2.297 LP_UAC Bypass via Event Viewer Detected

- **Trigger Condition:** Usage of *eventvwr.exe* to bypass UAC.
- **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*")
```

2.298 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
```

2.299 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=*
```

2.300 LP_Unsigned Driver Loading Detected

- **Trigger Condition:** Loading of an unsigned driver.
- **ATT&CK Category:** Privilege Escalation, Persistence
- **ATT&CK Tag:** Create or Modify System Process
- **ATT&CK ID:** T1543

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

```
norm_id=WindowsSysmon event_id=6 is_signed=false image=*
```

2.301 LP_Possible Ursnif Registry Activity

- **Trigger Condition:** This alert is triggered whenever it detects new registry key under AppDataLowSoftwareMicrosoft ,that was discovered to be 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\*"
```

2.301.1 LP_VBA DLL Loaded by Office

- **Trigger Condition:** Loading of DLL related to VBA macros by Office products. 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
```

2.302 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
```

2.303 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
```

2.304 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
```

2.305 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]
```

2.306 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.
- **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 ["4656", "4658", "4660", "4663"] object_name="*\wceaux.dll"
```

2.307 LP_Wdigest Registry Modification

- **Trigger Condition:** Modification of the wdigest registry value. Adversaries can enable wdigest authentication and retrieve users' plain text credentials.
- **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\UseLogonCredential"
```

2.308 LP_Weak Encryption Enabled for User

- **Trigger Condition:** Weak encryption enabled for a user profile, which is later used for hash or password cracking.
- **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=WinServer event_id=4738 user_account_control IN ["*DES*", "*Preauth*",
↪"*Encrypted*"] user_account_control="*Enabled*" -user IN EXCLUDED_USERS
```

2.309 LP_Potential Webshell Activity Detected

- **Trigger Condition:** Specific command line parameters 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_tomcatservice.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 \*"])))
```

2.310 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
```

2.311 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
```

2.312 LP_Windows Defender Antivirus Disable via Registry Modification

- **Trigger Condition:** This alert is triggered whenever the usage of "reg.exe" to tamper with different Windows Defender registry keys is detected.
- **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" IN ["*SOFTWARE\Microsoft\Windows Defender*",
 "*\SOFTWARE\Policies\Microsoft\Windows Defender*"]
((command = "*add*" command = "*d 0*"
command IN ["*DisallowExploitProtectionOverride*", "*EnableControlledFolderAccess*",
"*MpEnablePus*", "*PUAProtection*", "*SpynetReporting*", "*SubmitSamplesConsent*",
 "*TamperProtection*"])
OR
(command = "*add*" command = "*d 1*" command IN ["*DisableAntiSpyware*",
"*DisableAntiSpywareRealtimeProtection*", "*DisableAntiVirus*",
"*DisableArchiveScanning*", "*DisableBehaviorMonitoring*",
"*DisableBlockAtFirstSeen*", "*DisableConfig*", "*DisableEnhancedNotifications*",
"*DisableIntrusionPreventionSystem*", "*DisableIOAVProtection*",
"*DisableOnAccessProtection*", "*DisablePrivacyMode*", "*DisableRealtimeMonitoring*",
"*DisableRoutinelyTakingAction*", "*DisableScanOnRealtimeEnable*",
"*DisableScriptScanning*", "*Notification_Suppress*",
"*SignatureDisableUpdateOnStartupWithoutEngine*"]))
```

2.313 LP_Shadow Copy Deletion Using OS Utilities Detected

- **Trigger Condition:** Deletion of volume shadow copies using operating systems utilities. Adversaries can utilize Windows internal binaries such as Powershell, wmic, vssadmin, diskshadow, wbadmin and vssadmin to delete shadow copy from the system so that the data recovery and reverting system to saved state is impossible after dropping malware.
- **ATT&CK Category:** Impact, Defense Evasion
- **ATT&CK Tag:** Inhibit System Recovery, Indicator Removal
- **ATT&CK ID:** T1490, T1070
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="Process" label=Create
(
("process" IN ["*\powershell.exe", "*\pwsh.exe", "*\wmic.exe", "*\vssadmin.exe",
↪"*\diskshadow.exe"]
OR
file IN ["PowerShell.EXE", "pwsh.dll", "wmic.exe", "VSSADMIN.EXE", "diskshadow.exe" ])
command="*shadow*" command="*delete*"
```

(continues on next page)

(continued from previous page)

```
)
OR
(
("process"= "*\wbadmin.exe" OR file="WBADMIN.EXE")
command="*delete*" command="*catalog*" command="*quiet*"
)
OR
(
"process"="*\vssadmin.exe" OR file="VSSADMIN.EXE"
((command="*resize*" command="*shadowstorage*")
OR
command IN ["*unbound*","*/MaxSize=*"])
)
OR
(
command IN ["*Get-WmiObject*", "*gwmi*", "*Get-CimInstance*", "*gcim*"]
command="*'Win32_Shadowcopy*"
command IN ["*.Delete()*", "*Remove-WmiObject*", "*rwmi*", "*Remove-CimInstance*",
↪"*rcim*"]
)
```

2.314 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
```

2.315 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
```

2.316 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=Management label=Lock
↪user=* -user=*$] as s2 within 1 minute on s1.user=s2.user | rename s1.caller_user as caller_
↪user, s1.source_address as source_address, s2.host as host, s1.caller_domain as caller_domain,
↪ s2.target_domain as target_domain, s1.log_ts as last_failed_login_ts, s2.log_ts as locked_out_
↪ts
```

2.317 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
```

2.318 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 "process" IN ["*\winword.exe", "*\powerpnt.exe",
↪"*\excel.exe", "*\outlook.exe"] image IN ["*\wmiutils.dll", "*\wbemcomn.dll", "*\wbemprox.
↪dll", "*\wbemdisp.dll", "*\wbemsvc.dll"]
```

2.319 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
```

2.320 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-workspace-health.ps1*
↪"))
```

(continues on next page)

(continued from previous page)

2.321 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
```

2.322 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="*.pl*"))
-path IN ["*\AppData\Local\Temp*", "*\Windows\Temp*"]
```

2.323 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
```

2.324 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
```

2.325 LP_WMI Modules Loaded by Suspicious Process

- **Trigger Condition:** Loading of WMI modules by suspicious processes like a binary from ProgramData. 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 ["*wmiclnt.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",
↪"*\sdiagnhost.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\gpresult.exe",
↪"*\Windows\System32\tasklist.exe"]
```

2.326 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
```

2.327 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])
```

2.328 LP_ZOHO Dctask64 Process Injection Detected

- **Trigger Condition:** This alert is triggered whenever it detects suspicious process injection using ZOHO's dctask64.exe.
- **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
```

2.329 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
```

2.330 LP_Suspicious File Deletion Detected

- **Trigger Condition:** Adversaries remove 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:** File Deletion
- **ATT&CK ID:** 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
```

2.331 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:**

```
(label="Process" label=Create
("process"="*\findstr.exe" or file="findstr.exe")
command IN ["*virus*","*cylance*","*defender*","*cb*", "*avira*","*carbonblack*","*sophos*
↪","*symantec*","*kaspersky*","*malware*",
"*bitdefender*"])
OR
(norm_id=WindowsSysmon
"script_block" IN ["*get-process | \?*", "*get-process | where*", "*gps | \?*", "*gps | where*"]
"script_block"  IN ["*Company -like*", "*Description -like*", "*Name -like*", "*Path -like*",
↪"*Product -like*"]
"script_block"  IN ["*virus*","*cylance*","*defender*","*cb*", "*avira*","*carbonblack*",
↪"*sophos*","*symantec*","*kaspersky*","*malware*",
"*bitdefender*"])
```

2.332 LP_System Network Connections Discovery

- **Trigger Condition:** This alert is triggered whenever the discovery of network connections via system utilities like netstat, net, etc 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
```

2.333 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
```

2.334 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
```

2.335 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
```

2.336 LP_Process Execution from Suspicious Location

- **Trigger Condition:** Execution of a process from suspicious location.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Masquerading
- **ATT&CK ID:** T1036
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="Process" label=Create "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
↪"]
```

2.337 LP_Active Directory Enumeration via ADFind

- **Trigger Condition:** Enumeration of Active Directory using the ADfind tool. 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:** Command and Scripting Interpreter, PowerShell
- **ATT&CK ID:** T1059, T1059.001
- **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*"]
```

2.338 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 *"]
```

2.339 LP_Suspicious Taskkill Activity

- **Trigger Condition:** Multiple processes terminated in a short time via taskkill command that may signal malicious activity like ransomware.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Service Stop
- **ATT&CK ID:** T1489
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
label="Process" label=Create "process"="*\taskkill.exe" (command= "*f *" command="*im *
↪") OR command="*IM *" -parent_process IN ["*\AppData\Local\Temp*", "*\Windows\Temp*
↪"] -parent_process="*.tmp*"
```

2.340 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 *"
```

2.341 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*"
```

2.342 LP_Credential Access via LaZagne

- **Trigger Condition:** Credential accessed via the popular open-source LaZagne tool.
- **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:**

```
norm_id=WindowsSysmon event_id=10 call_trace="*C:\Windows\SYSTEM32\ntdll.
↪dll+*|C:\Windows\System32\KERNELBASE.dll+*_ctypes.pyd+*python27.dll+*"
```

2.343 LP_RDP Connection Inititated from Domain Controller

- **Trigger Condition:** Initiation of RDP connection from a domain controller.
- **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
```

2.344 LP_Active Directory Module Load in PowerShell

- **Trigger Condition:** Active Directory module is loaded via PowerShell.
- **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_id=4103 command IN ["*Import-Module*" , '*ipmo*'] payload=
↪"*ActiveDirectory*"
```

2.345 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).
- **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, PowerShell
- **Query:**

```
norm_id=WinServer event_id=4103 command="Get-ADComputer" payload=
↪"*DNSHostName*LastLogonDate*"
```

2.346 LP_Microsoft Defender Disabling Attempt via PowerShell

- **Trigger Condition:** Attempt to disable Microsoft Defender via PowerShell.
- **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, PowerShell
- **Query:**

```
norm_id=WinServer event_id=4104 script_block IN ["*Set-MpPreference -
↪DisableRealtimeMonitoring 1*", "*Set-MpPreference -DisableBehaviorMonitoring 1 *", "*Set-
↪MpPreference -DisableScriptScanning 1 *", "*Set-MpPreference -DisableBlockAtFirstSeen 1 *
↪", "*Set-MpPreference -DisableRealtimeMonitoring $true*", "*Set-MpPreference -
↪DisableBehaviorMonitoring $true*", "*Set-MpPreference -DisableScriptScanning $true*",
↪"*Set-MpPreference -DisableIOAVProtection $true*", "*Set-MpPreference -
↪DisableRealtimeMonitoring $true*", "*Set-MpPreference -DisableBlockAtFirstSeen $true*",
↪"*Set-MpPreference -drtm $true*", "*Set-MpPreference -dbm $true*", "*Set-MpPreference -
↪dscrptsc $true*", "*Set-MpPreference -dbaf $true*", "*Set-MpPreference -drtm 1 *", "*Set-
↪MpPreference -dbm 1 *", "*Set-MpPreference -dscrptsc 1 *", "*Set-MpPreference -dbaf 1 *"]
```

2.347 LP_Possible Kerberoasting via Rubeus

- **Trigger Condition:** Kerberoasting attack via popular open-source tool Rubeus.
- **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
```

2.348 LP_Suspicious Scheduled Task Creation

- **Trigger Condition:** Creation of a suspicious scheduled task in a Windows endpoint. 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:** Persistence
- **ATT&CK Tag:** Scheduled Task
- **ATT&CK ID:** 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\*"
```

2.349 LP_RDP Connection Inititated 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
```

2.350 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")
```

2.351 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=*")
```

2.352 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=Snort OR norm_id=SuricataIDS) message="*Windows RDP MS_T120*"
```

2.353 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*')
```

2.354 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*')
```

2.355 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*')
```

2.356 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*')
```

2.357 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
```

2.358 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
```

2.359 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
```

2.360 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']
```

2.361 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=*
```

2.362 LP_Safe DLL Search Mode Disabled

- **Trigger Condition:** Safe DLL search mode is disabled.
- **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=WindowSysmon event_id=13 target_object='*\CurrentControlSet\Control\Session
↪Manager\SafeDllSearchMode' detail="DWORD (0x00000000)"
```

2.363 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=*
```

2.364 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)"
```

2.365 LP_Suspicious Shells Spawn by SQL Server

- **Trigger Condition:** Suspicious shell process 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:**

```
label="Process" label=Create parent_process="*\sqlservr.exe" "process" IN ["*\cmd.exe",
↪"*\powershell.exe", "*\bash.exe", "*\sh.exe", "*\bitsadmin.exe", "*\netstat.exe", "*\nltest.
↪exe", "*\ping.exe", "*\pwsh.exe", "*\regsvr32.exe", "*\rundll32.exe", "*\systeminfo.exe",
↪"*\tasklist.exe", "*\wsl.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" *')
```

2.366 LP_Suspicious Microsoft SQL Server PowerShell Module Use Detected

- **Trigger Condition:** This alert detects the execution of a PowerShell code through the sqlps.exe utility, which is included in the standard set of utilities supplied with the MSSQL Server. Script blocks are not logged in this case, so this utility helps to bypass protection mechanisms based on the analysis of these logs.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Windows Sysmon

- **Query:**

```
label="Process" label=Create
("process"="*\sqlps.exe" OR parent_process="*\sqlps.exe" OR file="*\sqlps.exe" ) -(parent_
↪process="*\sqlagent.exe")
```

2.367 LP_UltraVNC Execution via Command Line

- **Trigger Condition:** Execution of UltraVNC via the command line. Gamaredon is known to use this technique to gain 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:*"
```

2.368 LP_Office Security Settings Changed

- **Trigger Condition:** Modification of Microsoft Office security settings in the registry.
- **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*"]
```

2.369 LP_Microsoft Defender AMSI Trigger

- **Trigger Condition:** Triggering of Microsoft Defender with AMSI as the detection source. AMSI is agnostic of antimalware vendors and is designed to allow for the most common malware scanning and protection techniques.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=1116 source_name=AMSI event_source="Microsoft-Windows-
↪Windows Defender"
```

2.370 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
```

2.371 LP_Impacket PsExec Execution

- **Trigger Condition:** Execution of Impacket's PsExec utility. Impacket is a collection of Python classes that work with network protocols. It is focused on providing low-level programmatic access to the packets and is commonly used in PoCs.
- **ATT&CK Category:** Lateral Movement

- **ATT&CK Tag:** Lateral Tool Transfer
- **ATT&CK ID:** T1570
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=5145 share_name="IPC$" relative_target IN ["*RemCom_stdint*
↪", "*RemCom_stdoutt*", "*RemCom_stderrt*"]
```

2.372 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:** Exploit Public-Facing Application
- **ATT&CK ID:** T1190
- **Minimum Log Source Requirement:** Firewall, Proxy Server
- **Query:**

```
norm_id=* request_method=GET url="*com.bea.console.handles.JndiBindingHandle*" url=
↪"*ldap://*" url="*AdminServer*"
```

2.373 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-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", "Find-InterestingFile", "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-ForeignUser", "Get-
↪DomainForeignUser", "Find-ForeignGroup", "Get-DomainForeignGroupMember", "Invoke-
↪MapDomainTrust", "Get-DomainTrustMapping"] -user IN EXCLUDED_USERS
```

2.374 LP_Stealthy VSTO Persistence

- **Trigger Condition:** Modification of office products Addins and VSTO inclusion registry keys. By modifying the registry keys adversaries can execute their payload through a malicious addins. Registry Auditing is required.
- **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"]
```

2.375 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:** Command and Scripting Interpreter
- **ATT&CK ID:** T1059
- **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*"]
```

2.376 LP_Suspicious WMPRVSE Child Process

- **Trigger Condition:** This alert is triggered whenever an uncommon or suspicious child process of the legitimate Windows Management Instrumentation Provider Service is detected. Attackers may leverage WMI (Windows Management Instrumentation) to execute commands and perform various tasks like evade detection or bypass security controls on a target system.
- **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"])
```

2.377 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*"
```

2.378 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:** Exploit Public-Facing Application, Web Shell
- **ATT&CK ID:** T1190, T1505.003

- **Minimum Log Source Requirement:** Web Server
- **Query:**

```
url=* url IN ["*/help/admin-guide/Reports/ReportGenerate.jsp*", "*/RestAPI/
↪LogonCustomization*", "*/RestAPI/Connection*"]
```

2.379 LP_Possible Access to ADMIN Share

- **Trigger Condition:** Access to $ADMIN share that may help 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. Legitimate administrative activities may generate false positives and will require whitelisting.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** SMB/Windows Admin Shares
- **ATT&CK ID:** T1021.002
- **Minimum Log Source Requirement:** Windows
- **Query:**

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

2.380 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 (norm_id=WindowsSysmon ((event_
↪id=11 file="PSEXESVC.exe") OR (event_id IN [17, 18] pipe="\PSEXESVC*")))
```

2.381 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
```

2.382 LP_Suspect Svchost Activity Detected

- **Trigger Condition:** Scvhost 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
```

2.383 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" -user IN EXCLUDED_
↪USERS
```

2.384 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\*"
```

2.385 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:** Windows 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*")
```

2.386 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*"]
```

2.387 LP_Conhost Spawning Suspicious Processes

- **Trigger Condition:** *conhost.exe* spawns other processes.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Indirect Command Execution

- **ATT&CK ID:** T1202
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
label="Process" label="Create" "parent_process"="*\conhost.exe" "process"=*
```

2.388 LP_Wlrmdr Lolbin Use as Launcher

- **Trigger Condition:** *wlrmdr.exe* is used to proxy launch other executables.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Indirect Command Execution
- **ATT&CK ID:** T1202
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
label="process" "process"="*\wlrmdr.exe" -"parent_process"="*\winlogon.exe" command IN [
↪'*-s *', '*-f *', '*-t *', '*-m *', '*-a *', '*-u *']
```

2.389 LP_Suspicious Process Execution via Pester Detected

- **Trigger Condition:** Execution of code via *Pester.bat*. The Pester is a Powershell module for testing purposes. Adversaries can use *Pester.bat* to execute other processes. Still, sometimes, legitimate use of a Pester for writing tests for Powershell scripts and modules could trigger false positives.
- **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" (("process"="*\powershell.exe" command="*Pester*"
↪command="*Get-Help*") OR ("process"="C:\Windows\System32\cmd.exe" command=
↪"*pester*" command="*;*" command IN ["*help*", "*?*"]))
```

2.390 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:** Install Root Certificate
- **ATT&CK ID:** T1553.004
- **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'>
```

2.391 LP_Suspicious process spawned by FTP

- **Trigger Condition:** Manipulation of *ftp.exe* to spawn a new process for file transfer. 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:** 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 IN ["*-s:*", "/*s:*"] ("process"="*\ftp.exe" OR file=
↪"*ftp.exe*")) OR (file="*ftp.exe*" -"process"="*\ftp.exe") OR parent_process="*\ftp.exe")
```

2.392 LP_Chromeloader Cross-Process Injection to Load Extention

- **Trigger Condition:** Chromeloader uses process injection using PowerShell and loads the malicious extension onto chrome. This alert is triggered when this exact scenario occurs.
- **ATT&CK Category:** Execution, Persistence, Privilege Escalation
- **ATT&CK Tag:** Process Injection, PowerShell, Browser Extensions
- **ATT&CK ID:** T1055, T1059.001, T1176
- **Minimum Log Source Requirement:** Windows
- **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"
```

2.393 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:** Indirect Command Execution
- **ATT&CK ID:** T1202
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="process" label=Create "process"="*\explorer.exe" "command"="*explorer*"
```

2.394 LP_Suspicious Root Certificate installation Detected

- **Trigger Condition:** This alert is triggered whenever installation of a root certificate is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Install Root Certificate
- **ATT&CK ID:** T1553.004
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create (command="*root*" (("process"="*\certutil.exe" command="*-addstore*") OR ("process"="*\CertMgr.exe" command="*/add*")))
```

2.395 LP_Windows Logon Reminder Usage as Launcher

- **Trigger Condition:** Manipulation of *Wlrmdr* to proxy launch other executables. *Wlrmdr* (Windows Logon Reminder) is a Microsoft Windows Binary used by Microsoft to display messages when logging in. Adversaries generally use *Wlrmdr* to pass parameters to ShellExecute.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Indirect Command Execution
- **ATT&CK ID:** T1202
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="process" label=create "process"="*\wlrmdr.exe" -"parent_process"="*\winlogon.exe" command IN ['*-s *', '*-f *', '*-t *', '*-m *', '*-a *', '*-u *']
```

2.396 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*"]
```

2.397 LP_Proxy Execution via Program Compatibility Wizard

- **Trigger Condition:** Pcwrun process is used to initiate a proxy execution. Pcwrun is a Microsoft Windows Operating System file used to invoke Program Compatibility Troubleshooter/Wizard. Adversaries uses pcwrun 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" "process"="*\pcwrun.exe" command="*../*"
```

2.398 LP_Suspicious Driver Installation via PnPUtil

- **Trigger Condition:** Pnputil process is used to install or add drivers. PnPUtil 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*", "*-a*
↪", "*/add-driver*", "*.inf*"]
```

2.399 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 IN ["*.xbap*","*http://*","*https://*","*ftp://*"] -command IN ["*\Windows\*",
↪"*\Program Files*"]
```

2.400 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\*"]
```

2.401 LP_Suspicious Use of Extrac32 Detected

- **Trigger Condition:** This alert is triggered when a 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 Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*\extrac32.exe"
command="*extrac32*" command IN ["*/C*", "*/Y*","* \\*"]
```

2.402 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"]
```

2.403 LP_DLL Injection with Tracker Detected

- **Trigger Condition:** This alert rule is triggered whenever DLL injection with tracker process is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1055.001 - Dynamic-link Library Injection
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="create" label="process" (("process"="*\tracker.exe" OR description="Tracker")
↪command="* /d *" command="* /c *")
-(command="* /ERRORREPORT:PROMPT *" OR (parent_proces IN [
↪"*\Msbuild\Current\Bin\MSBuild.exe","*\Msbuild\Current\Bin\amd64\MSBuild.exe"]))
```

2.404 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" IN ["*\vsimmersiveactivatehelper*.exe","*\devenv.exe"]
```

2.405 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 "process"="*\certoc.exe*" command IN ["* -LoadDll *", "* /
↪LoadDll *"] command="*.dll*"
```

- **Trigger Condition:** This alert is triggered when aspnet_compiler is used to build a C# program natively.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1127 - Trusted Developer Utilities Proxy Execution
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
label=Create label="Process" "process" ="C:\Windows\Microsoft.NET\Framework*" "process
↪"="*\aspnet_compiler.exe*"
```

2.406 LP_Suspicious Invocation PowerShell Diagnostic Script Execution

- **Trigger Condition:** This alert detects execution of malicious payloads via SyncInvoke in CL_Invocation.ps1 module.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1216 - Signed Script Proxy Execution
- **Minimum Log Source Requirement:** Windows

- **Query:**

```
command IN ["*\CL_Invocation.ps1", "*SyncInvoke*"] "Process"="*\powershell.exe"
```

2.407 LP_Registry Configured RunOnce Task Execution

- **Trigger Condition:** This alert gets triggered when the Run Once task executes, as configured in the registry or configuration of Run Once registry key is changed.
- **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*" OR command="*/r"))
 OR
(norm_id=WindowsSysmon label=Registry
target_object="HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components*" target_
↪object="*\StubPath"
-((detail="*\Program Files\Google\Chrome\Application\*" detail="*\Installer\chrmstp.exe*--
↪configure-user-settings --verbose-logging --system-level*") OR (detail IN ["*\Program Files
↪(x86)\Microsoft\Edge\Application\*","*\Program Files\Microsoft\Edge\Application\*"] detail=
↪"*\Installer\setup.exe*--configure-user-settings --verbose-logging --system-level --msedge --
↪channel=stable"))))
```

2.408 LP_Suspicious WSL Bash Execution

- **Trigger Condition:** This alert is triggered whenever it detects execution of Microsoft bash launcher with the "-c" flag.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1202 - Indirect Command Execution
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*\bash.exe" command="* -c *"
```

2.409 LP_Suspicious Usage of Csharp or Roslyn Csharp Interactive Console

- **Trigger Condition:** Usage of csi and rcsi binary are detected. Adversaries can use these binaries to execute their malicious C# code.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Software Deployment Tools, System Binary Proxy Execution
- **ATT&CK ID:** T1072, T1218
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create ("process" IN ["*\csi.exe", "*\rcsi.exe"]) OR (file in ["csi.exe",
↪"rcsi.exe"])
```

2.410 LP_Possible Commandline Obfuscation Detected

- **Trigger Condition:** This alert is triggered whenever suspicious characters are detected in the command indicating possible obfuscation of commands.
- **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*", "*¶*"]))
```

2.411 LP_Suspicious Use of Control Panel Items

- **Trigger Condition:** This alert is triggered whenever 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*"))))
```

2.412 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"])
```

2.413 LP_Suspicious File Download via Certreq

- **Trigger Condition:** This alert is triggered whenever file is downloaded using certreq binary.
- **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 *"
```

2.414 LP_Process Dump via Rundll32 and Comsvcs

- **Trigger Condition:** This alert is triggered whenever a process dump using Rundll32 with Comsvcs DLL is detected.
- **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*"]
```

2.415 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 Sysmon, Windows

- **Query:**

```
label="Process" label=Create "process"="*reg.exe" command="* query *" command=
↪"*SOFTWARE\Microsoft\Cryptography*" command IN ["*/v *", "*-v *"] command=
↪"*MachineGuid*"
```

2.416 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*"]
```

2.416.1 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 Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*\findstr.exe"
command="*findstr*" ((command="*/V*" command="*/L*") OR (command IN ["*/S*","*-S*"]
↪command IN ["*/I*","*-I*"]))
```

2.417 LP_Suspicious File Overwrite Using extrac32 Detected

- **Trigger Condition:** 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:** Signed Binary Proxy Execution
- **ATT&CK ID:** T1218
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*\extrac32.exe" command="*extrac32*"
↪command= "*/Y*" command IN ["*/C*", "* \\*"]
```

2.418 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:** Signed Binary Proxy Execution
- **ATT&CK ID:** T1218
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="Process" label=Create
("process"="*\ie4uinit.exe" OR file="ie4uinit.exe")
-(path IN ["*:\Windows\System32\", "*:\Windows\SysWOW64\"])
```

2.419 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=*
```

2.420 LP_Suspicious MSHTA Process Pattern

- **Trigger Condition:** 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" OR file="MSHTA.EXE")
(parent_process IN
["*\cmd.exe","*\powershell.exe","*\pwsh.exe","*\regsvr32.exe","*\rundll32.exe","*\wscript.
↪exe",
"*explorer.exe" ] OR command IN
["*\AppData\Local*", "*C:\Windows\Temp*", "*C:\Users\*"] command IN
["*.htm*", "*.hta*","*.vbs"]) OR(command="*http://*") OR -("process" IN [
↪"C:\Windows\System32*", "C:\Windows\SysWOW64*" ] OR command IN ["*mshta.exe",
↪"*mshta","*.htm*", "*.hta*" ])) OR (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"])
```

2.421 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*"
```

2.422 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  (command="*findstr*" ((command="*/V*" command="*/L*") OR (command="*/S*"
↪command="*/I*")) )))
OR (label="create" label="file" file in ADS_FILE_EXTENSIONS)
```

2.423 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:** NTFS File Attributes
- **ATT&CK ID:** T1564.004
- **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  ,s1.domain
↪as domain | chart count() by log_ts,user,domain,"process",parent_process,command order
↪by count() desc
```

(continues on next page)

(continued from previous page)

2.424 LP_Ngrok RDP Tunnel Detected

- **Trigger Condition:** 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:** Protocol Tunneling
- **ATT&CK ID:** T1572
- **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
```

2.425 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*"
```

2.426 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*"
```

2.427 LP_Code Compilation via Visual Basic Command Line Compiler

- **Trigger Condition:** This alert is triggered when successful compilation of code using Visual Basic Command Line Compiler is detected. "Vbc.exe" is Microsoft's Visual Basic compiler used to compile programs from within the Visual Studio integrated development environment (IDE). Adversaries can leverage it to compile their malicious code on the system in order to bypass defensive counter measures. Legitimate use of this tool can trigger false positives but it is hardly used in enterprise environment thus, detection of use is considered 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"
```

2.428 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*"]
```

2.429 LP_CLR DLL Loaded via Scripting Application

- **Trigger Condition:** This alert is triggered whenever common language runtime(CLR) DLL is loaded via scripting applications.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1218.005 - Mshta
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label=Image label=Load "process" IN ["*\wscript.exe","*\cscript.exe","*\mshta.exe","*\cmstp.
↪exe","*\msxsl.exe","*\regsvr32.exe","*\wmic.exe"] image IN ["*\clr.dll","*\mscoree.dll",
↪"*mscorlib.dll"]
```

2.430 LP_Microsoft Defender Logging Disabled

- **Trigger Condition:** This alert is triggered whenever windows defender registry key is modify to disable defender's logging.

- **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)"
```

2.431 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)"
```

2.432 LP_Process Dump via Sqldumper Detected

- **Trigger Condition:** This alert is triggered when a process dump via Sqldumper.exe is detected.
- **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*"]
```

- **Trigger Condition:** This alert is triggered whenever proxy execution of malicious payloads via Pubprn.bs is detected.
- **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:*"
```

2.433 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
```

2.434 LP_Remote Thread Created via Ttdinject

- **Trigger Condition:** This alert is triggered whenever remote thread or process is created by ttdinject binary.
- **ATT&CK Category:** Defense Evasion

- **ATT&CK Tag:** T1127 - Trusted Developer Utilities Proxy Execution
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
(label=Remote label=Create label=Thread "process"="*\ttdinject.exe")
OR (label="Process" label=Create ("process"="*\ttdinject.exe" OR file="TTDInject.EXE"))
```

2.435 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*"
```

2.436 LP_Remote Connection Established via Msbuild

- **Trigger Condition:** This alert is triggered whenever network connection is initiated via Msbuild while building an applications.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** MSBuild
- **ATT&CK ID:** T1127.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=3 "process"="*\msbuild.exe"  destination_port IN ["80",
↪"443"]
```

2.437 LP_Executables Started in Suspicious Folder

- **Trigger Condition:** This alert is triggered whenever it detects execution of binaries from suspicious folder.
- **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
↪" IN ["*SpeechUXWiz.exe","*SystemSettings.exe","*TrustedInstaller.exe","*PrintDialog.exe",
↪ "*MpSigStub.exe","*LMS.exe","*mpam-*.exe"]
```

2.438 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*")
```

2.439 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]
```

2.440 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"
```

2.441 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
```

2.442 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:** Windows, Unix
- **Query:**

```
event_source=OSQuery event_type=chrome_extension* columns_identifier IN MALICIOUS_
↪CHROME_EXTENSIONS
```

2.443 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:** Windows, Unix
- **Query:**

```
event_source=OSQuery event_type="chrome_extension*" columns_from_webstore=false
```

2.444 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*"
```

2.445 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/nspi*", "*/EWS*", "*X-
↪Rps-CAT*"]) OR url IN ["*autodiscover.json?@*", "*autodiscover.json%3f@*", "*%3f@foo.com*
↪", "*Email=autodiscover/autodiscover.json*", "*json?@foo.com*"])
```

2.446 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/nspi*", "*/EWS*", "*X-
↪Rps-CAT*"] status_code IN [200, 301])
```

2.447 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*"
```

2.448 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","*\ntdsutil.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\*"])
```

2.449 LP_Usage of Web Request Command

- **Trigger Condition:** Usage of various web request commands with commandline tools and Windows PowerShell cmdlets (including aliases) via commandline.
- **ATT&CK Category:** Execution

- **ATT&CK Tag:** PowerShell
- **ATT&CK ID:** T1059.001
- **Minimum Log Source Requirement:** Windows, Windows Sysmon, PowerShell
- **Query:**

```
(label="Process" label=Create
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*" ])
```

2.450 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" OR file="nltestrk.exe") ((command=
↪"*/server*" command="*/query*") OR command IN ["*/dclist:*","*/domain_trusts*","*/
↪trusted_domains*","*/user*","*/parentdomain*"])
```

2.451 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"]
```

2.452 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 (("process"="*\KrbRelayUp.exe" OR file="KrbRelayUp.exe") OR
↪(command="* relay *" command="* -Domain *" command="* -ComputerName *")
OR (command="* krbscm *" command="* -sc *") OR (command="* spawn *" command="* -d
↪*" command="* -cn *" command="* -cp *"))
```

2.453 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\*"]
```

2.454 LP_Network Connection to Suspicious Server

- **Trigger Condition:** Communication between hosts and domains mentioned in the query's list. The query will search for logs generated from the Windows system or proxies and firewalls. The sites mentioned in the query are either file-storing or hosting sites. Adversaries have utilized these 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:**

```
url IN ["*dl.dropboxusercontent.com*","*.pastebin.com*",
"*cdn.discordapp.com/attachments*","*mediafire.com*","*userstorage.mega.co.nz*",
"*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 domain IN ["*dropboxusercontent.com*","*pastebin.com*",
"*cdn.discordapp.com","*mediafire.com*","*userstorage.mega.co.nz",
"*mega.nz*","*ddns.net","*.paste.ee", "*.hastebin.com","*ghostbin.co",
"*ufile.io","*anonfiles.com", "send.exploit.in","transfer.sh", "privatlab.net",
"*privatlab.com","*sendspace.com","*pastetext.net","*pastebin.pl","*paste.e*",
"*api.telegram.org"]
```

2.455 LP_Activity Related to NTDS Domain Hash Retrieval

- **Trigger condition:** Copying of the* nods.dit* file, which is a database that stores Active Directory data, such as 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
(("process"="*\esentutl.exe" command IN ["*/y*", "*/vss*", "*/d*"]
command IN ["*\HarddiskVolumeShadowCopy*", "*\SYSTEM*", "*\\SECURITY*",
↪"*C:\tmp\log*","*\SAM*","*ntds.dit*"])
OR
(command IN ["*copy*","*xcopy*","*reg*"] command IN ["*\ntds.dit","*\System*"] -command=
↪"*system32*")
OR
("process"="*\ntdsutil.exe" command=""*ntds*" command=""*ifm*" command="*create*")
OR
("process"="*wmic.exe" command="*shadowcopy*" command="*call*" command="*create*
↪")
OR
(command="*gwmi*win32_shadowcopy*" command="*Create*")
OR
("process"="*\vssadmin.exe" command="*create*" command="*shadow*")
```

(continues on next page)

(continued from previous page)

```
OR
(command="*mklink*" command="*\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy*")
OR
("process"="*\diskshadow.exe" command="*\s*"))
```

2.456 LP_Application Shimming - File Access Detected

- **Trigger condition:** This alert is triggered whenever installation of new shims or registration of shims are 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, Windows
- **Query:**

```
(norm_id=WindowsSysmon event_id=11 path="C:\Windows\AppPatch\Custom*" file="*.sdb")
OR
(label=Registry label=Set label=Value target_object IN [
↪"HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\InstalledSDB\*
↪",
"HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Custom\*"])
OR
(label="Process" label=Create "process"="*\sdbinst.exe" command="*.sdb*" -command=
↪"*iisexpressshim.sdb'*")
```

2.457 LP_Audio Capture Detected

- **Trigger condition:** The alert is triggered whenever suspicious audio capture is detected.
- **ATT&CK Category:** Collection
- **ATT&CK Tag:** Audio Capture
- **ATT&CK ID:** T1123
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create (("process"="*\SoundRecorder.exe" command="*/FILE*") OR
↪(command IN ["*WindowsAudioDevice-Powershell-Cmdlet*", "*Toggle-AudioDevice*",
↪"*Get-AudioDevice *", "*Set-AudioDevice *", "*Write-AudioDevice *"])) -user IN EXCLUDED_
↪USERS
```

2.458 LP_Auditd High Volume of File Modification or Deletion in Short Span

- **Trigger Condition:** This alert is triggered whenever 30 file modification or deletion is detected in span of 1 minute.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Unix
- **Query:**

```
[30 label=File label=Info label=Path "process"=audit -name_type IN ["parent","normal"]
↪having same event_type,user_id,host,"process" within 1 minutes]
```

2.459 LP_Autorun Keys Modification Detected

- **Trigger Condition:** This alert is triggered whenever it detects modification of autostart extensibility point (ASEP) in registry.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **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 *"
```

2.460 LP_BlueMushroom DLL Load Detected

- **Trigger Condition:** This alert is triggered whenever it detects a suspicious DLL loading from the AppData Local path.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create
command = "*\regsvr32*" command = "*\AppData\Local\*" command = "*,DllEntry*"
↪command = "*.dll*"
-user IN EXCLUDED_USERS
```

2.461 LP_Capture a Network Trace with netsh

- **Trigger Condition:** This alert is triggered whenever it detects a network trace capture via netsh.exe trace functionality.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows

- **Query:**

```
label="Process" label=create
("process"="*\netsh.exe" OR file="netsh.exe")
command="*trace*" command="*start*"
```

- **Trigger Condition:** This alert is triggered whenever Osquery detects chrome extension installed with "devtools" permission. Look for unusual extensions installed with this permission and also check if the extension was installed from the webstore.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows, Unix
- **Query:**

```
event_source=OSQuery event_type="chrome_extension*" columns_permission="*devtools*"
```

2.462 LP_Citrix ADC VPN Directory Traversal Detected

- **Trigger Condition:** This alert is triggered whenever exploitation attempt of directory traversal vulnerability (CVE-2019-19781) in Citrix ADC is detected.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Web Server, Firewall
- **Query:**

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

2.463 LP_Cmdkey Cached Credentials Recon Detected

- **Trigger Condition:** This alert is triggered whenever it detects usage of cmdkey to look for cached credentials.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

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

2.464 LP_Command Obfuscation via Environment Variable Concatenation Reassembly

- **Trigger Condition:** This alert is triggered whenever command obfuscation in command prompt via environment variable concatenation reassembly is detected.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **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=*
```

2.465 LP_Control Panel Items - Registry Detected

- **Trigger Condition:** This alert is triggered whenever modification of Control Panel Registry sub-keys are detected.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label=Registry label=Set label=Value
target_object IN [
↪"*\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ControlPanel\NameSpace*",
↪"*\Software\Microsoft\Windows\CurrentVersion\Controls
↪Folder\*\Shellex\PropertySheetHandlers\*",
↪"*\Software\Microsoft\Windows\CurrentVersion\Control Panel\*"]
```

2.466 LP_Credentials Access in Files Detected

- **Trigger Condition:** This alert is triggered whenever command line arguments containing pattern to search "pass" in files are detected.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **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*"]
```

2.467 LP_Default Blocked Outbound Traffic followed by Allowed Event

- **Trigger Condition:** This alert is triggered whenever blocked outbound traffic is followed by allowed traffic.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **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
```

2.468 LP_Default Connection Attempts on Closed Port

- **Trigger Condition:** This alert is triggered whenever connection is attempted on closed ports. ALERT_OPEN_PORTS list needs to be updated with open ports.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Firewall, IDS, IPS
- **Query:**

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

2.469 LP_Default Unapproved Port Activity Detected

- **Trigger Condition:** This alert is triggered whenever a user uses ports that are not approved for use. It monitors traffic where the source_port, destination_port, or any port involved matches a port listed in the "UNAPPROVED_PORT" static list. Attackers may use unapproved ports to bypass security controls, such as firewalls or intrusion detection systems, which often monitor and restrict traffic on standard or known ports. The "UNAPPROVED_PORT" list is required to update on the organizational needs.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Firewall, IDS, IPS, Web Server
- **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
```

2.470 LP_Direct Autorun Keys Modification Detected

- **Trigger Condition:** This alert is triggered whenever it detects a modification to the direct autorun keys on a system (ASEP) in the registry using reg.exe.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **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
↪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*"]
```

2.471 LP_Empire PowerShell UAC Bypass Detected

- **Trigger Condition:** This alert is triggered whenever it detects some Empire Command and Scripting Interpreter, PowerShell UAC bypass methods. Empire is a post-exploitation framework featuring a fully PowerShell-based agent for Windows (version 2.0) and a Python-based agent for Linux and OS X (compatible with Python 2.6 and 2.7).
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create command IN ["* -NoP -NonI -w Hidden -c $x=$((gp
↪HKCU:Software\Microsoft\Windows Update).Update)*", "* -NoP -NonI -c $x=$((gp
↪HKCU:Software\Microsoft\Windows Update).Update)*"]
```

2.472 LP_Execution in Outlook Temp Folder Detected

- **Trigger Condition:** This alert is triggered whenever it detects a suspicious program execution in Outlook temp folder.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*\Temporary Internet Files\Content.Outlook\*"
```

2.473 LP_Execution of Temporary Files via Office Application

- **Trigger Condition:** This alert is triggered whenever office application creates a child process which executes a file with ".tmp" extension.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, windows
- **Query:**

```
label="Process" label="Create" "parent_process" IN ["*\winword.exe", "*\powerpnt.exe",
↪"*\excel.exe","*\onenote.exe","*\mspub.exe","*\vision.exe","*\msaccess.exe" ] "process"=
↪"*.tmp"
```

2.474 LP_External Disk Drive or USB Storage Device Detected

- **Trigger Condition:** This alert is triggered whenever it detects external diskdrives or plugged in USB devices.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows
- **Query:**

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

2.475 LP_File Downloaded from Suspicious URL Using GfxDownloadWrapper

- **Trigger Condition:** This alert is triggered when download of files from suspicious (non-standard) url using GfxDownloadWrapper.exe is detected.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Create" label="Process" "process"="*\GfxDownloadWrapper.exe" command IN [
↪"*https://*","*http://*"] - command="*gameplayapi.intel.com*" - parent_process=
↪"*\GfxDownloadWrapper.exe"
```

2.476 LP_Hidden Files and Directories Detected

- **Trigger Condition:** This alert is triggered whenever it detects the use of attrib.exe binary to change a file property to hidden or system.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

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

2.477 LP_IIS Native-Code Module Command Line Installation

- **Trigger Condition:** This alert is triggered whenever it detects suspicious installation of IIS native-code module via the command line. IIS Native-Code module is a component of Microsoft's Internet Information Services (IIS) that allows developers to extend IIS functionality as per the need. Adversaries can leverage it as a covert backdoor into servers, which allows them to hide deep in target environments and provide them with a durable persistence mechanism. However, Legitimate installation from the command line might also trigger false positives.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create ((("process"="*\appcmd.exe" OR file="appcmd.exe")
↪command="*install*" command="*module*" command IN ["*/name:*", "*-name:*"]) -
↪parent_process="C:\Windows\System32\inetsrv\iissetup.exe")
```

2.478 LP_Install Root Certificate

- **Trigger Condition:** This alert is triggered when a root certificate or related registry value is set up or modified.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label=Registry label=Set label=Value
"process"!="*\svchost.exe"
target_object IN ["*\SOFTWARE\Microsoft\EnterpriseCertificates\Root\Certificates\*" ,
↪"*\Microsoft\SystemCertificates\Root\Certificates\*"]
```

2.479 LP_LanmanServer Registry Value Modified

- **Trigger Condition:** This alert is triggered whenever lanmanserver registry value -MaxMpxCt, is modified.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label=Registry label=Set target_object=
↪"*\CurrentControlSet\Services\LanmanServer\Parameters\MaxMpxCt"
```

2.480 LP_Large ICMP Traffic

- **Trigger Condition:** This attack is triggered when ICMP Datagrams with size>1024 is received.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **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)
```

2.481 LP_Lsass Memory Dump with MiniDumpWriteDump API Detected

- **Trigger Condition:** This alert is triggered whenever it detects the use of MiniDumpWriteDump API for dumping lsass.exe memory in a stealthy way. Tools like ProcessHacker and some attacker tradecraft use this API found in dbghelp.dll or dbgcore.dll. As an 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:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=7 (image IN ["*\dbghelp.dll", "*\dbgcore.dll"]
"process" IN ["*\msbuild.exe", "*\cmd.exe","*\rundll32.exe", "*\word.exe", "*\excel.exe",
"*\powerpnt.exe", "*\outlook.exe", "*\monitoringhost.exe", "*\wmic.exe", "*\msiexec.exe",
↪"*\bash.exe", "*\wscript.exe", "*\cscript.exe", "*\mshta.exe", "*\dnx.exe", "*\regsvcs.exe",
↪"*\sc.exe", "*\scriptrunner.exe"])
OR (image IN ["*\dbghelp.dll", "*\dbgcore.dll"] Signed="FALSE")
-((command="C:\WINDOWS\\WinSxS\*" command="*\TiWorker.exe -Embedding")
OR "process"="*\svchost.exe" command IN ["*-k LocalServiceNetworkRestricted", "*-k
↪WerSvcGroup"]
OR "process"="*\rundll32.exe" command IN ["*/d srrstr.dll,ExecuteScheduledSPPCreation*",
↪"*aepdu.dll,AePduRunUpdate*","*shell32.dll,OpenAs_RunDL*","*Windows.Storage.
↪ApplicationData.dll,CleanupTemporaryState*"] )
```

2.482 LP_MSHTA Spawned by SVCHOST Detected

- **Trigger Condition:** This alert is triggered whenever MSHTA binary is spawned by Svchost process.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

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

2.483 LP_Malicious Use of Print Binary Detected

- **Trigger Condition:** This alert is triggered whenever print.exe is used for remote file copy.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

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

2.484 LP_Malware Threat Connection to Malicious Destination

- **Trigger Condition:** This alert is triggered when outbound connection to malicious sources is made by any hosts.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **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
```

2.485 LP_Memory Dump via Adplus

- **Trigger Condition:** This alert is triggered whenever LSASS process dump via adplus.exe is detected.
- **ATT&CK Category:** N/A

- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*\adplus.exe" command IN ["* -hang *" ,"* -pn *",
↪"* -pmn *" ,"* -p *","* -po *","* -c *","* -sc *"]
```

2.486 LP_MiniNt Registry Key Addition

- **Trigger Condition:** This alert is triggered whenever it detects the addition of a key 'MiniNt' to the registry.
- **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 label=Registry label=Set label=Value target_object=
↪"HKLM\SYSTEM\CurrentControlSet\Control\MiniNt"
```

2.487 LP_Netsh Port Forwarding Detected

- **Trigger Condition:** This alert is triggered whenever it detects netsh commands that configure a port forwarding.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*\netsh.exe"command in ["*interface portproxy add
↪v4tov4 *", "*i p a v*"]
```

2.488 LP_Network Share Discovery

- **Trigger Condition:** This alert is triggered when network share discovery activities are detected.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **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$*"])
```

2.489 LP_Non Interactive PowerShell Execution

- **Trigger Condition:** This alert is triggered whenever it detects non-interactive Command and Scripting Interpreter, PowerShell activity. Non-interactive powershell is an execution of powershell.exe without explorer.exe as a parent.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create
("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 *")
```

2.490 LP_Non-Existent User Login Attempt Detected

- **Trigger Condition:** This alert is triggered whenever 8 non-existent user login attempt on SSH service is detected within 1 minute.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Unix
- **Query:**

```
[8 label=Invalid label=User "process"=sshd having same source_address within 1 minutes]
```

2.491 LP_NotPetya Ransomware Activity Detected

- **Trigger Condition:** This alert is triggered whenever it detects NotPetya ransomware activity where the extracted passwords are passed back to the main module via a named pipe, the file system journal of drive C is deleted and Windows event logs are cleared using wevtutil binary.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create (command IN ["*wevtutil cl Application & fsutil usn deletejournal /
↪D C:*", "*dllhost.dat %WINDIR%\ransoms*"]
OR ("process"="*\rundll32.exe" command IN ["*.dat,#1", "*.dat #1", "*.zip.dll\*,#1"])
OR "*\perfc.dat*")
```

2.492 LP_Obfuscation Script Usage via MSHTA to Execute Vbscript

- **Trigger Condition:** This alert is triggered whenever execution of invoke-obfuscation powershell script with mshta to execute vbscript is detected.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create command="*&&*" command="*mshta*" command=
↪"*vbscript:createobject*" command="*.run*" command="*(window.close)*"
```

- **Trigger Condition:** This Alert is triggered whenever unauthorized transfer of sensitive data is detected using mail applications,cloud applications or other medium. Lists included are RESIGNED_EMPLOYEES,KNOWN_DOMAINS,CLOUD_APPLICATIONS.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **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=*)
```

2.493 LP_Possible Emotet Activity Detected

- **Trigger Condition:** This alert is triggered whenever it detects process creation events related to Emotet.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create
(command IN ["* -e* PAA*", "*JABlAG4AdgA6AHUAcwBlAHIAcAByAG8AZgBpAGwAZQ*",
↪"*QAZQBuAHYAOgB1AHMAZQByAHAAcgBvAGYAaQBsAGUA*",
↪"*kAGUAbgB2ADoAdQBzAGUAcgBwAHIAbwBmAGkAbABlA*",
↪"*IgAoACcAKgAnACkAOwAkA*", "*IAKAAnACoAJwApADsAJA*",
↪"*iACgAJwAqACcAKQA7ACQA*", "*JABGAGwAeAByAGgAYwBmAGQ*"])
( -command IN [
↪"fAAgAEMAbwBuAHYAZQByAHQAVABvAC0ASgBzAG8AbgAgAC0ARQByAHIAbwByAEEAYwB0AGkAbwBu
↪",
↪"wAIABDAG8AbgB2AGUAcgB0AFQAbwAtAEoAcwBvAG4AIAAtAEUAcgByAG8AcgBBAGMAdABpAG8AbgA
↪",
↪"8ACAAQwBvAG4AdgBlAHIAdABUAG8ALQBKAHMAbwBuACAALQBFAHIAcgBvAHIAQQBjAHQAaQBvAG4
↪"])
-user IN EXCLUDED_USERS
```

2.494 LP_Possible File Transfer Using Finger Detected

- **Trigger Condition:** This alert is triggered whenever execution of Finger.exe is detected.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label="create" "process"="*\finger.exe"
```

2.495 LP_Possible Impacket Lateral Movement Detected

- **Trigger Condition:** This alert is triggered whenever it detect instances of lateral movement using the Impacket framework, specifically when utilizing the wmiexec, dcomexec, atexec, and smbexec tools.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **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\*")
```

2.496 LP_Possible SquiblyTwo Detected

- **Trigger Condition:** This alert is triggered whenever it detects WMI SquiblyTwo Attack with possible renamed WMI by looking for imphash.
- **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=1 file="wmic.exe" hash_imphash IN [
↪"1B1A3F43BF37B5BFE60751F2EE2F326E", "37777A96245A3C74EB217308F3546F4C",
↪"9D87C9D67CE724033C0B40CC4CA1B206"] command="*format:*" command="*http*"
```

- **Trigger Condition:** This alert is triggered when usage of suspicious tools to bypass User Access Control (UAC) is detected.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
label="Process" label=Create (command IN ["*eventvwr.exe*", "*wscript.exe*"] OR token_
↪elevation_type="TokenElevationTypeLimited*") -user IN EXCLUDED_USERS
```

2.497 LP_PowerShell ADRecon Execution

- **Trigger Condition:** This alert is triggered whenever the execution of the ADRecon PowerShell script for AD reconnaissance is detected.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4104 script_block IN ["*Function Get-ADRExcelComOb*",
↪"*ADRecon-Report.xlsx*","*Get-ADRGPO*","*Get-ADRDomainController*"]
```

2.498 LP_PowerShell Encoded FromBase64String Detected

- **Trigger Condition:** This alert detects the use of the .NET method "FromBase64String" to decode a Base64-encoded string. Base64 is a widely used encoding scheme that represents binary data in an ASCII string format. It is often used to encode data for transfer over networks or to store data in databases or files.
- **ATT&CK Category:** N/A

- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create command IN [
↪"*OgA6AEYAcgBvAG0AQgBhAHMAZQA2ADQAUwB0AHIAaQBuAGcA*",
↪"*oAOgBGAHIAbwBtAEIAYQBzAGUANgA0AFMAdAByAGkAbgBnA*",
↪"*6ADoARgByAG8AbQBCAGEAcwBlADYANABTAHQAcgBpAG4AZw*" ]
```

2.499 LP_PowerShell Rundll32 Remote Thread Creation Detected

- **Trigger Condition:** This alert is triggered whenever it detects the creation of a remote thread from a Powershell process in a rundll32 process.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **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
```

2.500 LP_Powershell AMSI Bypass via dotNET Reflection

- **Trigger Condition:** This alert is triggered whenever it detects a Request to amsiInitFailed that can be used to disable AMSI Scanning. AMSI is a feature in Windows that allows applications to request the scanning of scripts and other content for malicious behavior.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A

- **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
```

2.501 LP_Powershell Code Execution via SyncAppvPublishingServer

- **Trigger Condition:** This alert is triggered when arbitrary Powershell command is executed via SyncAppvPublishingServer.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Create" label="Process"
command="*\SyncAppvPublishingServer.vbs*" command="*;*"
```

2.502 LP_Process Creation via Time Travel Tracer

- **Trigger Condition:** This alert is triggered when a new child process is spawned via tttracer.exe.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "parent_process"="*\tttracer.exe"
```

2.503 LP_Proxy Execution via Xwizard

- **Trigger Condition:** This alert is triggered whenever execution of xwizard tool with "runwizard" and CLSID arguments are utilized to achieve proxy execution.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **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=*
```

2.504 LP_Pulse Secure Arbitrary File Reading Detected

- **Trigger Condition:** This alert is triggered whenever exploitation of arbitrary file reading vulnerability (CVE-2019-11510) in Pulse Secure is detected.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Firewall, IDS, IPS
- **Query:**

```
norm_id=* url IN ['*dana*guacamole*', '*lmdb*data.mdb*', '*data*mtmp/system*']
```

2.505 LP_Reconnaissance using Windows Binaries Detected

- **Trigger Condition:** This alert is triggered whenever possible reconnaissance activities using windows binaries is detected such as execution of several discovery.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create"process" IN ["*\whoami.exe", "*\nltest.exe", "*\net1.exe",
↪"*\ipconfig.exe","*\systeminfo.exe", "*\net.exe", "*\route.exe", "*\quser.exe","*\qwinsta.exe
↪", "*\netstat.exe","*nbtstat.exe"]
|chart distinct_count(command) as cnt, distinct_list(command) as command by user,host
↪|search cnt > 4
```

2.506 LP_Registry Key Import Detected

- **Trigger Condition:** This alert is triggered whenever registry key import is detected via regedit.exe.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="Process" label="Create" ("process"="*\regedit.exe" OR file="regedit.exe") command
↪IN ["*/i *","*-i *"] command="*.reg*" -command IN ["*/e *","*/a *","*/c *","*-e *","*-a *","*-
↪c *" ]
```

2.507 LP_Registry Run Key Pointing to a Suspicious Folder

- **Trigger Condition:** This alert is triggered whenever it detects registry modification where the value of "Run" key is pointing to a suspicious folder.
- **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=13 event_type=SetValue
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\*", "*\AppData\Local\Temp\*", "*%temp%\*", "*%tmp%\*", "wscript*",
↪"cscript*"]
-detail IN ["*\AppData\Local\Microsoft\*"]
```

2.508 LP_Remote Code Execution using WMI Win32_Service Class over WinRM

- **Trigger Condition:** This alert is triggered when Application Whitelisting Bypass and Arbitrary Unsigned Code Execution Technique is attempted, using winrm.vbs. It detects the execution of attacker-controlled WsmPty.xsl or WsmTxt.xsl via winrm.vbs and copied cscript.exe (can be renamed).
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="Process" label=Create
command="*winrm*" command IN ['*format:pretty*', '*format:"pretty"*', '*format:"text"*',
↪'*format:text*'] -("process" IN ["C:\Windows\System32\*", "C:\Windows\SysWOW64\*"])
```

2.509 LP_Run PowerShell Script from ADS Detected

- **Trigger Condition:** This alert is triggered whenever PowerShell script execution from Alternate Data Stream (ADS) is detected.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **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
```

2.510 LP_RunOnce Registry Key Configuration Change

- **Trigger Condition:** This alert gets triggered when the configuration of Run Once registry key is changed.
- **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 label=Registry
target_object="HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components*" target_
↪object="*\StubPath"
-((detail="*\Program Files\Google\Chrome\Application\*" detail="*\Installer\chrmstp.exe*--
↪configure-user-settings --verbose-logging --system-level*") OR (detail IN ["*\Program Files
↪(x86)\Microsoft\Edge\Application\*","*\Program Files\Microsoft\Edge\Application\*"] detail=
↪"*\Installer\setup.exe*--configure-user-settings --verbose-logging --system-level --msedge --
↪channel=stable"))
```

2.511 LP_Rundll32 Internet Connection Detected

- **Trigger Condition:** This alert is triggered whenever it detects a rundll32 that communicates with public IP addresses.
- **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=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*")))
```

2.512 LP_Scheduled Task Creation Detected

- **Trigger Condition:** This alert is triggered whenever it detects the creation of scheduled task.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **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
```

(continues on next page)

(continued from previous page)

```
(norm_id=WinServer event_id=4698
(-command IN ["*MpCmdRun.exe","*msfeedssync.exe","*usoclient.exe"] OR (-task=
↪"\CreateExplorerShellUnelevatedTask" command="*explorer.exe")))
```

2.513 LP_Shell Spawn via HTML Help Detected

- **Trigger Condition:** This alert gets triggered when Hh (HTML Help) spawns shell processes.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **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"]
```

2.514 LP_Suspicious Atbroker Registry Change Detected

- **Trigger Condition:** This alert is triggered whenever creation/modification of Assistive Technology registry value 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 label=Registry label=Set target_object IN [
↪"*\Software\Microsoft\Windows NT\CurrentVersion\Accessibility\ATs*",
↪"*\Software\Microsoft\Windows NT\CurrentVersion\Accessibility\Configuration*"]
-(("process"="*\Windows\system32\atbroker.exe" target_object="*\Microsoft\Windows
↪NT\CurrentVersion\Accessibility\Configuration*" detail="(Empty)") OR "process"=
↪"*\Windows\Installer\MSI*" target_object="*Software\Microsoft\Windows
↪NT\CurrentVersion\Accessibility\ATs*")
```

(continues on next page)

(continued from previous page)

- **Trigger Condition:** This alert is triggered whenever it detects execution of CSharp or FSharp interactive console by scripting utilities such as WScript, Cscript PowerShell, etc.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **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"]
```

2.515 LP_Suspicious Child Process Creation via OneNote

- **Trigger Condition:** This alert is triggered whenever it detects creation of suspicious child processes, execution of binaries from non-default paths, and script file execution through OneNote.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create parent_process ="*\onenote.exe"
("process" 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 ("process"="*\explorer.exe" command IN ["*.hta*","*.vb*","*.wsh*","*.js*","*.ps*","*.scr*",
"*.pif*","*.bat","*.cmd*"])
OR "process" IN ["*\AppData\*","*\Users\Public\*","*\ProgramData\*","*\Windows\Tasks\*",
"*\Windows\Temp\*","*\Windows\System32\Tasks\*"])
```

2.516 LP_Suspicious Code Page Switch Detected

- **Trigger Condition:** This alert is triggered whenever switching of code page in the command line or batch scripts to a different, normally a rare language is detected.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*\chcp.com"command IN ["* 936", "* 1258"] -user
↪IN EXCLUDED_USERS
```

2.517 LP_Suspicious ConfigSecurityPolicy Execution Detected

- **Trigger Condition:** This alert is triggered whenever file upload is detected via ConfigSecurityPolicy binary.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

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

2.518 LP_Suspicious DLL Execution Using Windows Address Book

- **Trigger Condition:** This alert is triggered when suspicious DLL is executed using Wab.exe.

- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label=Registry label=Set target_object="*\Software\Microsoft\WAB\DLLPath*"  - detail="
↪%CommonProgramFiles%\System\wab32.dll"
```

2.519 LP_Suspicious Debugger Registration Detected

- **Trigger Condition:** This alert is triggered whenever it detects the registration of a debugger for a program that is available in the logon screen (sticky key backdoor).
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **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*","*\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
↪Execution Options\HelpPane.exe\Debugger"]
```

2.520 LP_Suspicious Download Using Diantz

- **Trigger Condition:** This alert is triggered when a remote file is downloaded suspiciously using diantz.exe and is stored by compressing it into a .cab file on the local machine.
- **ATT&CK Category:** N/A

- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create command="*diantz.exe*" command="* \\*" command="*.cab*"
```

2.521 LP_Suspicious Execution from Outlook

- **Trigger Condition:** This alert is triggered whenever it detects EnableUnsafeClientMailRules used for Script Execution from Outlook.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create
(
command="*EnableUnsafeClientMailRules*"
OR
(
parent_process="*\outlook.exe"
(command="\\*\*.exe" OR "process"="\\*\*.exe")
)
)
```

2.522 LP_Suspicious Execution of Dump64

- **Trigger Condition:** This alert is triggered when suspicious usage of dump64.exe is detected.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A

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

```
label="Process" label="Create" "process"="*\dump64.exe" (-("process"=
↪"*\Installer\Feedback\dump64.exe*") OR command IN ["* -ma *", "*accpeteula*"])
```

2.523 LP_Suspicious Execution of LNK File

- **Trigger Condition:** This alert is triggered whenever execution of suspicious LNK files that either spawns powershell or command prompt and has high entropy in the command field is detected.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **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
```

2.524 LP_Suspicious Files Dropped in Perflogs Folder

- **Trigger Condition:** This alert is triggered whenever an EXE or DLL file is dropped in Windows's Perflog directory.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label=File label=Create label=Overwrite file IN ["*.dll", "*.exe", "*.bat*", "*.chm*", "*.hta", "*.
↪lnk", "*.ps1*", "*.psm1*", "*.py*", "*.scr*", "*.sys*", "*.vbe*", "*.vbs*", "*.zip*"] path=
↪"C:\Perflogs*"
```

2.525 LP_Suspicious HWP Sub Processes Detected

- **Trigger Condition:** This alert is triggered whenever it detects suspicious Hangul Word Processo (Hanword) sub-processes that could indicate exploitation.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create parent_process="*\Hwp.exe" "process"="*\gbb.exe"
```

2.526 LP_Suspicious Invocation of Microsoft Workflow Compiler

- **Trigger Condition:** This alert is triggered when usage of Microsoft Workflow Compiler is detected.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **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*"))
```

2.527 LP_Suspicious LSASS Dump Creation in CrashDumps

- **Trigger Condition:** This alert is triggered whenever it detects the creation of an LSASS dump file in %LocalAppData%CrashDumps folder, which is in context of NT/Authority is C:Windowssystem32configsystemprofileAppDataLocalCrashDumps, possibly patterns seen in LSASS Shtinkering attack.
- **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=11
path="*\AppData\Local\CrashDumps*"
file="*lsass.exe.*"
file="*.dmp*"
```

2.528 LP_Suspicious LoadAssembly PowerShell Diagnostic Script Execution

- **Trigger Condition:** This alert detects the use of a Microsoft signed script to execute commands and bypass AppLocker.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
command IN ["*\CL_LoadAssembly.ps1", "*LoadAssemblyFromPath*"] "Process"=
↪"*\powershell.exe"
```

2.529 LP_Suspicious Outbound RDP Connections Detected

- **Trigger Condition:** This alert is triggered whenever it detects non-standard tools initiating outbound connections over TCP port 3389, indicating possible lateral movement using Remote Desktop Protocol (RDP).
- **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=3 destination_port="3389" initiated="true" -"process" 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"]
```

2.530 LP_Suspicious PowerShell Parameter Substring Detected

- **Trigger Condition:** This alert is triggered whenever it detects PowerShell invocation with a suspicious parameter substring.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create
"process" IN ["*\powershell.exe", "*\pwsh.exe"]
command IN ["* -wi*h*", "* -nopr*", "* -nonin*", "* -ec*", "* -en*", "* -executionp*", "* -e*
↪bypass*", "* -sta *","*FromBase64String*", "*irm*iex*", "Invoke-RestMethod*Invoke-
↪Expression*"]
```

2.531 LP_Suspicious RDP Redirect Using TSCON Detected

- **Trigger Condition:** This alert is triggered whenever it detects a suspicious RDP session redirect using tscon.exe.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create command="*tscon*" command="*rdp-tcp*"
```

2.532 LP_Suspicious Remote Binary Usage Detected

- **Trigger Condition:** This alert is triggered whenever remote.exe binary is used to bypass application whitelisting and execute or run a local/remote file.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="Process" label=Create "process"="*\remote.exe" command="* /s *"
```

2.533 LP_Suspicious Scripting in a WMI Consumer

- **Trigger Condition:** This alert is triggered whenever it detects suspicious scripting in WMI Event Consumers.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A

- **Minimum Log Source Requirement:** Windows Sysmon, PowerShell
- **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 *", "*System.Security.Cryptography.FromBase64Transform*"]
```

2.534 LP_Suspicious Setup Information File Invoked via DefaultInstall

- **Trigger Condition:** This alert gets triggered when InfDefaultInstall.exe is used to install an INF file.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="Process" label=Create "process"="*\InfDefaultInstall.exe"
command="InfDefaultInstall*" command="*.inf"
```

2.535 LP_Suspicious Svchost Process Detected

- **Trigger Condition:** This alert is triggered whenever any suspicious svchost process creation is detected.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create  "process"="*\svchost.exe"
command IN ["*svchost.exe","*svchost"] command=* parent_process=*
-parent_process IN [ "*\MsMpEng.exe", "*\Mrt.exe", "*\rpcnet.exe","*\TiWorker.exe", "*\ngen.
↪exe", "C:\Windows\System32\svchost.exe"]
 (-parent_process="*\services.exe" -command="* -k *")
```

2.536 LP_Suspicious Sysmon Driver Unload Detected

- **Trigger Condition:** This alert is triggered when suspicious unload of SysmonDrv Filter Driver is detected.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label="Create"  "process"="*\fltmc.exe" command="*unload*" command =
↪"*sys*"
```

2.537 LP_Suspicious Usage of SQLToolsPS Detected

- **Trigger Condition:** This alert rule is triggered when it detects the proxy execution of PowerShell code through the SQLToolsPS.exe.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **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")))
```

2.538 LP_Suspicious Usage of Windows Binaries for Ingress Tool Transfer

- **Trigger Condition:** This alert is triggered whenever it detects suspicious activities of windows binaries for indicative attempts of ingress tool transfer.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create
("process" IN ["*\AppInstaller.exe", "*\CertOC.exe", "*\certutil.exe", "*\Desktopimgdownldr.
↪exe", "*\Esentutl.exe", "*\Expand.exe", "*\IMEWDBLD.exe", "*\ieexec.exe", "*\InstallUtil.exe
↪", "*\MpCmdRun.exe", "*\msedge.exe", "*\Mshta.exe", "*\Presentationhost.exe",
↪"*\regsvr32", "*\tar.exe", "*\winget.exe", "*\msedge_proxy.exe", "*MsoHtmEd.exe*",
↪"*\Mspub.exe", "*\msxsl.exe", "*\ProtocolHandler.exe", "*\squirrel*", "*\update.exe"]
OR
command IN ["*appinstaller*", "*certoc*", "*certutil*", "*Desktopimgdownldr*", "*Esentutl*",
↪"*IMEWDBLD*", "*ieexec*", "*InstallUtil*", "*MpCmdRun*", "*msedge*", "*Mshta*",
↪"*Presentationhost*", "*regsvr32*", "*tar.exe*", "winget*", "*msedge_proxy*",
↪"*MsoHtmEd*", "*Mspub*", "*msxsl*", "*ProtocolHandler.exe", "*squirrel*", "*update.exe*
↪"])
|process regex("(?P<new_command>(https?:\/\/\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}))", command)
|search command="*http*" OR new_command=*
```

2.539 LP_Suspicious WMIC ActiveScriptEventConsumer Created

- **Trigger Condition:** This alert is triggered whenever WMIC is executed to create a event consumer.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows

- **Query:**

```
label="Process" label=Create command="*ActiveScriptEventConsumer*" command="*
↪CREATE *"
```

- **Trigger Condition:** This alert is triggered whenever if a Windows program executable is detected to started in a suspicious folder.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **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", "*\lsm.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", "*\LsaIso.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"])
```

2.540 LP_System Network Configuration Discovery

- **Trigger Condition:** This alert is triggered whenever discovery of network configuration via system utilities like ipconfig, route, netsh, etc is detected.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A

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

```
label="Process" label=Create (("process" IN ["*\ipconfig.exe","*\nbtstat.exe","*\arp.exe",
↪"*\route.exe"]) OR (command IN ["*netsh advfirewall*","*netsh.exe*interface show",
↪"*net*config"]))
```

2.541 LP_TerraMaster TOS CVE-2020-28188 Exploitation

- **Trigger Condition:** This alert is triggered whenever possible exploitation of the TerraMaster TOS vulnerability CVE-2020-28188 is detected. CVE-2020-28188 is a remote command execution (RCE) vulnerability in TerraMaster TOS <= 4.2.06 that allows remote unauthenticated attackers to inject OS commands.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **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*"]
```

2.542 LP_UAC Bypass via CMLUA or CMSTPLUA

- **Trigger Condition:** This alert is triggered whenever user CMLUA OR CMSTPLUA DLL is loaded to perform user account control(UAC) bypass.
- **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" label=Image label=Load image IN ["*\cmlua.dll","*\cmstplua.dll",
↪"*\cmluautil.dll"] -"process" IN ["*\cmstp.exe","*\cmmgr32.exe"] -"process" IN [
↪"*\windows\*","*\program files\*"]
```

- **Trigger Condition:** This alert is triggered whenever high risk vulnerability is detected in low impact assets.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **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
```

2.543 LP_VM - Medium Risk Vulnerability on High Impact Assets

- **Trigger Condition:** This alert is triggered whenever medium risk vulnerability is detected in high impact assets.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **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
```

2.544 LP_VM - Medium Risk Vulnerability on Medium Impact Assets

- **Trigger Condition:** This alert is triggered whenever medium risk vulnerability is detected in medium impact assets.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **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
```

2.545 LP_VMware View Planner CVE-2021-21978 Exploitation

- **Trigger Condition:** This alert is triggered whenever possible 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 logupload web application.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Firewall, Proxy Server
- **Query:**

```
norm_id=* request_method=POST url="*logupload*" url="*logMetaData*" url="*wsgi_log_
↪upload.py*"
```

2.546 LP_WER Full User Mode Dumps Enable Detected

- **Trigger Condition:** Alert Trigger: This alert is activated upon detecting a modification to the registry value "DumpType," set to 2, located within the HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsWindows Error ReportingLocalDumps key. This registry configuration, introduced with Windows Server 2008 and Windows Vista SP1, enables the collection and local storage of full user-mode dumps following a user-mode application crash. It's important to note that applications employing custom crash reporting mechanisms, such as .NET applications, are not supported by this feature.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label=Registry label=Set
target_object="HKLM\SOFTWARE\Microsoft\Windows\Windows Error
↪Reporting\LocalDumps\DumpType"
"detail"="DWORD (0x00000002)"
-"process"="*\svchost.exe"
```

2.547 LP_WMI Persistence - Script Event Consumer Detected

- **Trigger Condition:** This alert is triggered whenever it detects Windows Management Instrumentation (WMI) script event consumers.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **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
```

2.548 LP_WSL Execution Detected

- **Trigger Condition:** This alert is triggered whenever possible usage of Windows Subsystem for Linux (WSL) binary is used to execute linux commands.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="Process" label=Create "process"="*\wsl.exe" command IN ["* -e *","* --exec*","* --
↪system*", "* --shell-type *","* /mnt/c*","* --user root*","* -u root*","*--debug-shell*"]
-(parent_process="*\cmd.exe" command="* -d *" command="* -e kill *")
```

2.549 LP_WannaCry Sources in Connections to Sinkhole Domain

- **Trigger Condition:** This alert is triggered whenever a source tries to connect to wannacry sinkhole domain.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Firewall, IDS, IPS, Web Server
- **Query:**

```
norm_id=* url IN WANNACRY_DOMAIN or domain IN WANNACRY_DOMAIN
```

2.550 LP_Windows Defender Antivirus Definitions Removal Detected

- **Trigger Condition:** This alert is triggered when Microsoft Defender Antivirus signature definitions are removed from the system.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*\MpCmdRun.exe" command=
↪"*RemoveDefinitions*"
```

- **Trigger Condition:** This alert is triggered whenever it detects suspicious parent processes of well-known Windows processes.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create  parent_process="*"
"process" IN ["*\svchost.exe", "*\taskhost.exe", "*\lsm.exe", "*\lsass.exe", "*\services.exe",
↪"*\lsaiso.exe", "*\csrss.exe", "*\wininit.exe", "*\winlogon.exe"]
-((parent_process IN ["*\SavService.exe", "*\ngen.exe", "*\System32\*", "*\SysWOW64\*"])
OR (parent_process IN ["*\Windows Defender\*", "*\Microsoft Security Client\*"] parent_
↪process="*\MsMpEng.exe*")
OR (parent_process="-"))
```

2.551 LP_Windows RDP Port Modified

- **Trigger Condition:** This alert is triggered whenever remote desktop protocol (RDP) for windows protocol is modified.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label=Registry label=Value label=Set
target_object="*\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-
↪Tcp\PortNumber"
-detail="DWORD (0x00000d3d)"
```

2.552 LP_Windows Security Health Disable via Registry Modification

- **Trigger Condition:** This alert is triggered whenever Windows Security Health registry values are added/modified to set it to a disabled state.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="Process" label=Create "process"="*\reg.exe" command=
↪"*HKLM\System\CurrentControlSet\Services\SecurityHealthService*" command="*add*4*"
```

2.553 LP_Windows User Account Created via Command Line

- **Trigger Condition:** This alert is triggered whenever the creation of a user account via CLI like PowerShell or via net utility is detected. The creation of a user account is a process by which a user or administrator creates a new user profile on a system. Attackers may create new user accounts to maintain or enhance their access to a system or domain. This can be used as a means of persistence, where the attacker can maintain access to a compromised system even if their initial access is detected and removed. Alternatively, the attacker may create new accounts with elevated privileges to expand their access to additional resources or systems. Effective monitoring and access controls can help detect and prevent unauthorized account creation and mitigate the risks associated with this type of attack.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create (command="*New-LocalUser*" or command="*net user add*")
```

2.554 LP_XSL Script Processing Detected

- **Trigger Condition:** This alert is triggered whenever application control bypass attempt via execution of embedded scripts inside Extensible Stylesheet Language (XSL) files is detected.This alert also detects another variation of this technique, dubbed "Squiblytwo" that utilizes WMI to invoke JScript or VBScript within an XSL file. XSL stands for Extensible Stylesheet Language and is used to express the style sheets. It supports scripting to do formatting on XML files. Adversaries may abuse XSL to bypass application whitelisting and execute arbitrary code due to its legitimate functionality.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **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
```

- **Trigger Condition:** Inbox rule configured in Microsoft Exchange to manipulate incoming emails containing specific terms like phish, malware and alert.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Email Hiding Rules
- **ATT&CK ID:** T1564.008
- **Minimum Log Source Requirement:** Office365
- **Query:**

```
norm_id=Office365 action="New-InboxRule" | process eval ("result_body= has_any(body_
↪contains_words, 'phishing, malware, compromised, unauthorized, security update, reset
↪password, verify identity, alert, bank details, ransomware, CEO, wire transfer, payment
↪confirmation, suspicious login')") | process eval ("result_subject = has_any(subject_contains_
↪words, 'urgent, alert, security, verify, login, update, password, invoice, salary, phish, malware,
↪hacked, compromised, ransomware')") | process eval ("action_present=case(forward_to ->
↪True, redirect_to -> True, delete_message -> True, soft_delete_message -> True, move_to_
↪folder -> True, mark_as_read -> True, true -> 'False')") | process eval("keyword_
↪present=case(result_body -> True, result_subject -> True, true -> 'False')") | search keyword_
↪present="True" OR action_present="True"
```

2.555 LP_Successful Microsoft 365 Login with Reconnaissance User Agents

- **Trigger Condition:** User agents associated with known reconnaissance tools like AADInternals and AzureHound, presented during successful logins to Microsoft 365.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Permission Groups Discovery, Cloud Account, Cloud Service Discovery

- **ATT&CK ID:** T1069, T1087.004, T1526
- **Minimum Log Source Requirement:** Office365
- **Query:**

```
norm_id=office365 label=User label=Login label=Successful user_agent IN ["AadInternals",
↪"azurehound*"]
```

2.556 LP_Sensitive Mail Read Application Permission Assigned

- **Trigger Condition:** Application in Microsoft Entra ID (formerly Azure AD) with the Mail.Read permission granted.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Additional Email Delegate Permissions
- **ATT&CK ID:** T1098.002
- **Minimum Log Source Requirement:** Office365
- **Query:**

```
norm_id=Office365 action="Add app role assignment to service principal" app_role_value=
↪"Mail.Read"
```

2.557 LP_Multiple Exchange Mailboxes Accessed via API in Short Span

- **Trigger Condition:** High number of mailboxes accessed via an API, such as Microsoft Graph API or Exchange Web Services, within a short period.
- **ATT&CK Category:** Collection
- **ATT&CK Tag:** Remote Email Collection
- **ATT&CK ID:** T1114.002
- **Minimum Log Source Requirement:** Office365
- **Query:**

```
norm_id="Office365" action="MailItemsAccessed" user_type="Application" | process eval(
↪"match=like(client_information, 'Client=WebServices;ExchangeWebServices%')") | process
↪eval("search_result=if(match) {return 1} else-if(target_application=='Microsoft Graph') {return
↪1} else {return 0}") | filter search_result=1 | timechart distinct_count(upn) as user_mailbox_
↪count, distinct_list(user) as user_list, distinct_list(source_address) as source_address by target_
↪application every 10 minutes | filter user_mailbox_count > 5
```

2.558 LP_Microsoft Purview eDiscovery Activities

- **Trigger Condition:** Microsoft purview activities related to searching for files and data in all of Sharepoint, Exchange and public folders via edisocvery were performed or the search results were exported. Microsoft Purview eDiscovery is a legal compliance tool that helps organizations search for, identify, collect, and export data for legal investigations, litigation and compliance audits.
- **ATT&CK Category:** Collection, Exfiltration
- **ATT&CK Tag:** Email Collection, Exfiltration Over Web Service
- **ATT&CK ID:** T1114, T1567
- **Minimum Log Source Requirement:** Office365
- **Query:**

```
norm_id=Office365 application="SecurityComplianceCenter"
((operation="SearchStarted"
(exchange_locations="Include:[All]" sharepoint_locations="Include:[All]" public_folder_
↪locations="Include:[All]"))
OR
"operation"="SearchExported")
```

2.559 LP_Microsoft Purview Audit Disabled

- **Trigger Condition:** Microsoft Purview Audit (formerly Advanced Auditing) subscription removed from a user.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Disable or Modify Cloud Logs
- **ATT&CK ID:** T1562.008
- **Minimum Log Source Requirement:** Office365

- **Query:**

```
norm_id=office365 "action"="Update user" additional_detail="*DisabledPlans=[M365_
↪ADVANCED_AUDITING]]*"
```

2.560 LP_Microsoft 365 Unified Audit Logging Disabled

- **Trigger Condition:** Disabling of Unified Audit Log in Microsoft 365 (formerly Office 365).
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Disable or Modify Cloud Logs
- **ATT&CK ID:** T1562.008
- **Minimum Log Source Requirement:** Office365
- **Query:**

```
norm_id=Office365 action="Set-AdminAuditLogConfig" unified_audit_log_ingestion_
↪enabled=False
```

2.561 LP_Microsoft 365 Multiple MFA Prompt Denied

- **Trigger Condition:** User denied multiple MFA prompts.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Multi-Factor Authentication Request Generation
- **ATT&CK ID:** T1621
- **Minimum Log Source Requirement:** Office365
- **Query:**

```
norm_id=office365 label=login -user="Not Available" logon_
↪error=UserStrongAuthClientAuthNRequiredInterrupt | timechart count() as fail_mfa by user
↪every 10 minutes | search fail_mfa > 2
```

2.562 LP_File with Suspicious Extension Sent in Microsoft Teams Message

- **Trigger Condition:** File with a potentially dangerous extension, such as .exe, .bat and .ps1, shared within a Microsoft Teams chat or channel.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Additional Email Delegate Permissions
- **ATT&CK ID:** T1098.002
- **Minimum Log Source Requirement:** Office365
- **Query:**

```
norm_id=office365 application=OneDrive application_display_name="Microsoft Teams*"
↪action="fileuploaded" file IN ["*.exe", "*.msi", "*.bin", "*.dll", "*.bat", "*.ps1", "*.vbs", "*.js
↪", "*.scr", "*.cab", "*.gz", "*.bz2" ]
```

2.563 LP_File Shared to Guest in SharePoint

- **Trigger Condition:** SharePoint file shared with an external guest user.
- **ATT&CK Category:** Collection
- **ATT&CK Tag:** Sharepoint
- **ATT&CK ID:** T1213.002
- **Minimum Log Source Requirement:** Office365
- **Query:**

```
norm_id=Office365 "event_source"="SharePoint" target_user_type=Guest action IN [
↪"SharingInvitationCreated", "AddedToSecureLink"]
```

2.564 LP_Exchange Mailbox Folder Delegation Configured

- **Trigger Condition:** Addition of delegation permissions to the Exchange mailbox folders.

- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Additional Email Delegate Permissions
- **ATT&CK ID:** T1098.002
- **Minimum Log Source Requirement:** Office365
- **Query:**

```
norm_id=Office365 ((action IN ["Add-MailBoxFolderPermission", "Set-MailBoxFolderPermission
↪"] -identity IN ["*:\Calendar", "*:\Contacts"]) OR (action IN ["AddFolderPermissions",
↪"ModifyFolderPermissions"] item_parent_folder_member_rights="*ReadAny*" -item_parent_
↪folder_name IN ["Calendar", "Contacts"]))
```

2.565 LP_Exchange Mailbox Delegation Configured

- **Trigger Condition:** Addition of delegation permissions to an Exchange mailbox.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Additional Email Delegate Permissions
- **ATT&CK ID:** T1098.002
- **Minimum Log Source Requirement:** Office365
- **Query:**

```
norm_id=Office365 action IN ["Add-MailboxPermission", "Set-MailboxPermission"] access_
↪rights=* -user="NT AUTHORITY\SYSTEM (Microsoft.Exchange.ServiceHost)"
```

2.566 LP_Exchange Mailbox Audit Bypass Configured

- **Trigger Condition:** Use of Set-MailboxAuditBypassAssociation cmdlet to exempt a user or service account from mailbox audit logging in Exchange Online.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Disable or Modify Cloud Logs
- **ATT&CK ID:** T1562.008
- **Minimum Log Source Requirement:** Office365

- **Query:**

```
norm_id=Office365 action="Set-MailboxAuditBypassAssociation" audit_bypass_enabled=True
```

2.567 LP_Exchange Email Auto Forward Enabled

- **Trigger Condition:** Email auto-forwarding within Exchange mailbox which can lead to data leakage, especially if configured to send emails to external addresses without proper authorization.
- **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="Set-Mailbox" forwarding_email=*
```

2.568 LP_Entra ID User Consent Denied for OAuth Application

- **Trigger Condition:** User denied consent to an OAuth application requesting permissions.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Steal Application Access Token
- **ATT&CK ID:** T1528
- **Minimum Log Source Requirement:** Office365
- **Query:**

```
norm_id="Office365" request_type="Consent:set" logon_error="UserDeclinedConsent"
```

2.569 LP_Entra ID Suspicious Permission Granted to Application

- **Trigger Condition:** User granted consent to an application with suspicious privileges.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Additional Cloud Roles
- **ATT&CK ID:** T1098.003
- **Minimum Log Source Requirement:** Office365
- **Query:**

```
norm_id=Office365 action="Add app role assignment to *" status=Success app_role_value IN [
↪"*Mail.Read*","*Mail.Send*","*Files.Read.All*","*Files.ReadWrite.All*","*Application.
↪ReadWrite.All*","*Directory.ReadWrite.All*","*RoleManagement.ReadWrite.Directory*",
↪"*PrivilegedAccess.ReadWrite.AzureAD*","*User.DeleteRestore.All*", "*AppRoleAssignment.
↪ReadWrite.All*"]
```

2.570 LP_Entra ID Suspicious Authorization Policy Updated

- **Trigger Condition:** Updated Entra ID/Azure AD authorization policy to grant user consent to apps identified as risky by Microsoft Entra ID Protection.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Impair Defenses
- **ATT&CK ID:** T1562
- **Minimum Log Source Requirement:** Office365
- **Query:**

```
norm_id=Office365 action="Update authorization policy" updated_property=
↪"AllowUserConsentForRiskyApps*" allow_user_consent_for_risky_apps="True"
```

2.571 LP_Entra ID Privileged Role Assignment via PIM

- **Trigger Condition:** Addition of a privileged role user through Microsoft Entra Privileged Identity Management (PIM).
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Additional Cloud Roles
- **ATT&CK ID:** T1098.003
- **Minimum Log Source Requirement:** EntraID
- **Query:**

```
norm_id=MicrosoftGraph activity_display_name="Add member to role in PIM*" result="success
↪" | rename initiated_by_user_display_name as "user" ,"activity_display_name" as "message",
↪ operation_type as operation,initiated_by_user_id as user_id |process json_parser(target_
↪resources,".[2].userPrincipalName") as target_user
```

2.572 LP_Entra ID Privileged Role Assignment

- **Trigger Condition:** Privileged role assigned to a user or a service principal in Entra ID.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Account Manipulation, Additional Cloud Roles
- **ATT&CK ID:** T1098, T1098.003
- **Minimum Log Source Requirement:** Office365
- **Query:**

```
norm_id="Office365" label=Add label=Role label=User role_template_id IN ENTRA_ID_
↪PRIVILEGED_ROLES | filter status="Success" | process json_expand(target,x) | process eval(
↪"target_upn=if(Type == 5){ return object_id}") | process eval("target_user=if(match(ID,
↪'ServicePrincipal_.*')){ return ID}") | search target_upn=* OR target_user=*
```

2.573 LP_Entra ID Privileged Application Role Assignment by Service Principal

- **Trigger Condition:** Privileged application roles assigned to security principals in Entra ID by service principals.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Account Manipulation, Additional Cloud Roles
- **ATT&CK ID:** T1098, T1098.003
- **Minimum Log Source Requirement:** Office365
- **Query:**

```
norm_id=Office365 action IN ["Add app role assignment to service principal"] user=
↪"serviceprincipal_*" status=Success
```

2.574 LP_Entra ID PowerShell Sign-In

- **Trigger Condition:** User logged in using the Azure Active Directory PowerShell module, Azure CLI, or sign-ins using the Microsoft Graph PowerShell SDK.
- **ATT&CK Category:** Execution, Defense Evasion
- **ATT&CK Tag:** Cloud API, Cloud Accounts
- **ATT&CK ID:** T1059.009, T1078.004
- **Minimum Log Source Requirement:** EntraID
- **Query:**

```
norm_id="MicrosoftGraph" api_endpoint="auditLogs/signIns" app_display_name IN [
↪"AzureActive Directory PowerShell", "Microsoft Graph Command Line Tools"] source_
↪address=* status_error_code="0" | rename location_state as "region",location_country as
↪"country", client_app_used as application_used,device_detail_is_compliant as is_device_
↪compliant, device_detail_is_managed as is_device_managed
```

2.575 LP_Entra ID New Owner Added to Service Principal or Application

- **Trigger Condition:** Successfull addition of a new owner to a service principal or application.
- **ATT&CK Category:** Persistence, Privilege Escalation
- **ATT&CK Tag:** Additional Cloud Roles
- **ATT&CK ID:** T1098.003
- **Minimum Log Source Requirement:** Office365
- **Query:**

```
norm_id=office365 status=Success action IN ["Add owner to service principal","Add owner to
↪application"] status=Success
```

2.576 LP_Entra ID High Risk User Sign-In

- **Trigger Condition:** When Microsoft Entra ID Protection flags user sign-in activities as “at risk.”
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** EntraID
- **Query:**

```
norm_id=MicrosoftGraph risk_state="atRisk" api_endpoint_name="signIns" status_error_
↪code=0 risk_level_during_sign_in="high"
```

2.577 LP_Entra ID Full Access Permission Assigned to Application

- **Trigger Condition:** User granted full access to office and office applications.
- **ATT&CK Category:** Persistence

- **ATT&CK Tag:** Additional Email Delegate Permissions, Additional Cloud Roles
- **ATT&CK ID:** T1098.002, T1098.003
- **Minimum Log Source Requirement:** Office365
- **Query:**

```
norm_id=Office365 "app_role_value"="full_access_as_app" action="Add app role assignment
↪to service principal" | rename service_principal_display_name as service_principal
```

2.578 LP_Entra ID External User Invited

- **Trigger Condition:** External guest user invited within ENTRA ID.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Cloud Account
- **ATT&CK ID:** T1136.003
- **Minimum Log Source Requirement:** Office365
- **Query:**

```
norm_id="Office365" creation_type="Invitation" action="Add user"
```

2.579 LP_Entra ID Device Code Authentication Detected

- **Trigger Condition:** Successful authentication using a device code authenticator.
- **ATT&CK Category:** Initial Access, Credential Access
- **ATT&CK Tag:** Steal Application Access Token, Phishing
- **ATT&CK ID:** T1528, T1566
- **Minimum Log Source Requirement:** Office365
- **Query:**

```
norm_id=office365 label=Login label=Successful "request_type"="Cmsi:Cmsi"
```

2.580 LP_Entra ID Credential Added to Application or Service Principal

- **Trigger Condition:** Addition of a new credential, either a client secret or certificate, to an application or service principal within Microsoft Entra ID.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Additional Cloud Credentials
- **ATT&CK ID:** T1098.001
- **Minimum Log Source Requirement:** Office365
- **Query:**

```
norm_id=Office365 status=Success action IN ["Add service principal credentials", "Update
↪application – Certificates and secrets management*"] | process json_expand(target, x) | filter
↪Type=1 | rename ID as name
```

2.581 LP_Entra ID Conditional Access Policy Modification

- **Trigger Condition:** Addition or update of a Microsoft Entra Conditional Access policy.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Conditional Access Policies
- **ATT&CK ID:** T1556.009
- **Minimum Log Source Requirement:** EntraID
- **Query:**

```
norm_id=MicrosoftGraph activity_display_name="*Conditional Access Policy" result=Success
↪|rename operation_type as operation, activity_display_name as message,initiated_by_user_
↪user_principal_name as "user" ,initiated_by_user_ip_address as source_address ,initiated_by_
↪user_id as user_id | process json_parser(target_resources,".[0].displayName") as policy |
↪process json_expand(target_resources,x) | process json_expand(modifiedProperties,x) |
↪process json_parser(modifiedProperties,".newValue") as new_value | process json_
↪parser(modifiedProperties,".oldValue") as old_value | process json_parser(modifiedProperties,
↪ ".newValue") as new_value| process json_parser(new_value,".state") as state
```

2.582 LP_Entra ID Conditional Access Policies Implementing MFA Deleted

- **Trigger Condition:** When users deleted conditional access policies implementing Multi-Factor Authentication (MFA).
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Multi-Factor Authentication
- **ATT&CK ID:** T1556.006
- **Minimum Log Source Requirement:** EntraID
- **Query:**

```
"norm_id"="MicrosoftGraph" "activity_display_name"="Delete conditional access policy"
↪"api_endpoint_name"="directoryAudit" | process json_expand(target_resources,x) | process
↪json_expand(modifiedProperties,x) | process json_expand(oldValue,x) | search grantControls_
↪builtInControls="*mfa*"
```

2.583 LP_Entra ID Conditional Access Policies Blocking Device Code Authentication Modified

- **Trigger Condition:** When users deleted or modified conditional access policies preventing Device Code Authentication flow.
- **ATT&CK Category:** Modify Authentication Process
- **ATT&CK Tag:** Sharepoint
- **ATT&CK ID:** T1556
- **Minimum Log Source Requirement:** EntraID
- **Query:**

```
"norm_id"="MicrosoftGraph" "api_endpoint_name"="directoryAudit" ("activity_display_name
↪"="Delete conditional access policy" OR activity_display_name ="Update conditional access
↪policy") | process json_expand(target_resources,x) | process json_expand(modifiedProperties,
↪ x) | process json_expand(oldValue,x) | process json_parser(conditions_authenticationFlows,".
↪transferMethods") as transfer_method | search transfer_method="1" and grantControls_
↪builtInControls="*block*" | rename initiated_by_user_user_principal_name as upn, initiated_
↪by_user_ip_address as source_address
```

2.584 LP_Creation of Anonymous Sharing Link in SharePoint

- **Trigger Condition:** Creation of anonymous sharing links in SharePoint.
- **ATT&CK Category:** Collection
- **ATT&CK Tag:** Sharepoint
- **ATT&CK ID:** T1213.002
- **Minimum Log Source Requirement:** Office365
- **Query:**

```
norm_id=Office365 "event_source"="SharePoint" action="AnonymousLinkCreated"
```

2.585 LP_Block Network Connections from EDR via WFP

- **Trigger Condition:** When an Endpoint Detection and Response (EDR) network connection is blocked by the Windows Filtering Platform (WFP).
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Impair Defenses
- **ATT&CK ID:** T1562
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id="Winserver" event_id="5157" application IN EDR_PROCESS
```

2.586 LP_RDP Extension File Dropped in Outlook Folder

- **Trigger Condition:** Creation of a file with .rdp extension in the Outlook folder.
- **ATT&CK Category:** Initial Access, Lateral Movement
- **ATT&CK Tag:** Remote Desktop Protocol, Spearphishing Attachment
- **ATT&CK ID:** T1021.001, T1566.001

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

```
label="Create" label="File" file="*.rdp" path IN ["*\AppData\Local\Packages\Microsoft.
↪Outlook_*", "*\AppData\Local\Microsoft\Olk\Attachments\*"] OR (path=
↪"*\AppData\Local\Microsoft\Windows\*" path="*\Content.Outlook\*")
```

2.587 LP_File Creation with RTLO Character for Filename Obfuscation

- **Trigger Condition:** Detects file creation events where filenames use the Right-to-Left Override (RLO) character (U+202E) to disguise malicious extensions (e.g., .msc or .exe) as legitimate document formats (e.g., .pdf, .docx).
- **ATT&CK Category:** Initial Access, Defense Evasion
- **ATT&CK Tag:** Right-to-Left Override, Spearphishing Attachment
- **ATT&CK ID:** T1036.002, T1566.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label=Create label=File target_file IN ["*\u202e*", "*???*"] target_file IN ["*fdp.*", "*xcod.*",
↪"*cod.*", "*xtpp.*", "*xslx.*", "*slx.*", "*ftr.*", "*tdo.*", "*lmth.*"]
```

2.588 LP_Suspicious AutoIt Execution

- **Trigger Condition:** Execution of a suspicious AutoIt in a suspicious context. Adversaries leverage AutoIt for automation and payload delivery due to its flexibility and ability to evade detection.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** AutoHotKey & AutoIT
- **ATT&CK ID:** T1059.010
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="Create" label="Process" "process"="*\Autoit*.exe" OR file="AutoIt*.exe" -"process"
↪IN ["*:\Program Files (x86)\AutoIt*\", "*:\Program Files\AutoIt*\"]
```

2.589 LP_CVE-2024-38112 Exploitation Detected

- **Trigger Condition:** This alert is triggered whenever it detects events where svchost.exe process has spawned iexplore.exe process and the same iexplore.exe process has drop an ".hta" file.
- **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="*\svchost.exe" "process"="*\iexplore.exe"
↪process_guid=*] as s1 followed by [norm_id=WindowsSysmon event_id=11 "process"=
↪"*\iexplore.exe" file="*.hta*"] as s2 within 1 minute on s1.process_guid=s2.process_guid
↪rename s1.process as "process", s1.host as host, s1.parent_process as parent_process, s1.
↪user as user, s2.path as path, s2.file as file
```

2.590 LP_Certipy Tool Execution for AD CS Abuse

- **Trigger Condition:** This rule detects the execution of Certipy, a hacktool commonly used for Active Directory Certificate Services (AD CS) abuse. Digital certificates are often used to sign and encrypt messages and/or files. Certificates are also used as authentication material. Certipy is part of a suite of tools developed for Red Team operations and security testing. It allows attackers to interact with AD CS to enumerate and exploit configurations and vulnerabilities. It is particularly useful for abusing certificate templates, forging certificates, and performing privilege escalation attacks. Adversaries may use this tool to steal or forge certificates used for authentication to access remote systems or resources. False positives for this rule are unknown.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Steal or Forge Authentication Certificates
- **ATT&CK ID:** T1649

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

```
label="Process" label=Create
("process"="*\Certipy.exe" OR file="Certipy.exe" OR description="*Certipy*")
OR
(command IN ["* auth *", "* find *", "* forge *", "* relay *", "* req *", "* shadow *"]
command IN ["* -bloodhound*", "* -ca-pfx *", "* -dc-ip *", "* -kirbi*", "* -old-bloodhound*",
↪"* -pfx *", "* -target*", "* -username *", "* -vulnerable*", "*auth -pfx*", "*shadow auto*",
↪"*shadow list*"])
```

2.591 LP_Certify Tool Execution for AD CS Abuse

- **Trigger Condition:** This rule detects execution of Certify, a hacktool commonly used for Active Directory Certificate abuse. Digital certificates are often used to sign and encrypt messages and/or files. Certificates are also used as authentication material. Certify is part of a suite of tools developed for Red Team operations and security testing. It allows attackers to interact with AD CS to enumerate and exploit configurations and vulnerabilities. It is particularly useful for abusing certificate templates, forging certificates, and performing privilege escalation attacks. Adversaries may use this tool to steal or forge certificates used for authentication to access remote systems or resources. False positives for this rule is unkown
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Steal or Forge Authentication Certificates
- **ATT&CK ID:** T1649
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create
("process"="*\Certify.exe" OR file="Certify.exe" OR description="*Certify*")
OR
(command IN ["*.exe cas *", "*.exe find *", "*.exe pkiobjects *", "*.exe request *", "*.exe
↪download *"]
command IN ["* /vulnerable*", "* /template:*", "* /altname:*", "* /domain:*", "* /path:*", "* /
↪ca:*"])
```

2.592 LP_Password Dumper Activity on LSASS

- **Trigger Condition:** Process handle on the LSASS process with a specific access mask and SAM_DOMAIN object type. Tools like Mimikatz create a process handle on the LSASS process with an elevated access mask for dumping purposes. This alert detects Mimikatz lsadump attempts.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** LSA Secrets
- **ATT&CK ID:** T1003.004
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id IN [4656,4663] "process"="*\lsass.exe" access="0x705" object_
↪type="SAM_DOMAIN"
```

2.593 LP_Disabling of UAC Detected

- **Trigger Condition:** Disabling of User Access Control (UAC) in the endpoint. Adversaries may disable UAC to execute code directly with high integrity.
- **ATT&CK Category:** Privilege Escalation, Defense Evasion
- **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 label=Registry label=Set label=Value target_object="*EnableLUA*"
↪detail="DWORD (0x00000000)"
```

2.594 LP_Behavior Related to Named Pipe Impersonation

- **Trigger Condition:** Suspicious events related to named pipe impersonation are detected, such as creating a named pipe, creating a service with a named pipe, and using a named pipe in the command line. Adversaries use named pipe impersonation for privilege escalation and to evade defense.

- **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=Registry label=Set label=Value target_object=
↪"*HKLM\System\CurrentControlSet\Services\*\ImagePath*" detail="*\\.\pipe\*") OR
↪(label=Service label=Install path="*\\.\pipe*") OR (label="Process" label=Create
↪user=System "process" IN ["*\cmd.exe","*\powershell.exe"] command="*\\.\pipe*"))
```

2.595 LP_Usage of Ngrok Utility Detected

- **Trigger Condition:** This alert is triggered whenever it detects the execution of Ngrok utility is detected. Ngrok is a cross-platform applications that allows users to expose local servers behind NATs and firewalls to the public internet over secure tunnels. Threat actors often use Ngrok to expose internal services to the internet like making RDP publicly accessible. False positives could arise from another tools that uses the same command line switches as Ngrok. ‘
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Protocol Tunneling
- **ATT&CK ID:** T1572
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create (("process"="*\ngrok.exe" command IN ["* tcp *", "* http *", "*
↪authtoken *"])
OR (command="* start *" command="*--all*" command="*.yml*" command="*--config*")
OR (command IN ["* tcp 139*", "* tcp 445*", "* tcp 3389*", "* tcp 5985*", "* tcp 5986*"]))
```

2.596 LP_Chrome Addition of VPN Extension

- **Trigger Condition:** This alert rule detects the addition of well known VPN Extension in Chrome. Extensions are small software programs that customize the browsing experience, while VPN extension allows VPN functionality within the browser.

Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. False positives may occur when a VPN Extension is added in Chrome for legitimate reasons. List 'CHROME_VPN_EXTENSIONS' is required for this alert rule.

- **ATT&CK Category:** Initial Access, Persistence
- **ATT&CK Tag:** External Remote Services
- **ATT&CK ID:** T1133
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label="Registry" label="Set"
target_object="*Software\Wow6432Node\Google\Chrome\Extensions*"
target_object IN CHROME_VPN_EXTENSIONS
target_object="*update_url"
```

2.597 LP_Outlook Security Settings Change

- **Trigger Condition:** Modification to Outlook configuration through creating a security registry key. Changes to configuration can allow adversaries to run macros covertly without notifying 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="*\Outlook\Security\Level*" detail=
↪"DWORD (0x00000001)"
```

2.598 LP_Suspicious Certutil Command Detected

- **Trigger Condition:** Suspicious Certutil utility execution with parameters like decode or urlcache, which adversaries can use to download payloads from remote locations or encode/decode base64 obfuscated payloads.
- **ATT&CK Category:** Defense Evasion, Command and Control
- **ATT&CK Tag:** Ingress Tool Transfer, Deobfuscate/Decode Files or Information
- **ATT&CK ID:** T1105, T1140
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create ("process"="*\certutil.exe" OR file="CertUtil.exe") command IN [
↪"* -decode *", "* /decode *", "* -decodehex *", "* /decodehex *", "* -urlcache *", "* /
↪urlcache *", "* -verifyctl *", "* /verifyctl *", "* -encode *", "* /encode *","* /exportPFX *","* -
↪exportPFX *" ]
```

2.599 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"] )
```

2.600 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*"])
```

2.601 LP_System Service Reconnaissance through WMI

- **Trigger Condition:** This alert is triggered whenever usage of WMI for service reconnaissance is detected.
- **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*"]
```

2.602 LP_Process Reconnaissance through WMI

- **Trigger Condition:** This alert is triggered whenever it detects the usage of WMI for listing Processes running on the compromised host.
- **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*"]
```

2.603 LP_Process Created through WMI

- **Trigger Condition:** This alert is triggered whenever it detects the usage of WMI to spawn new processes either on local or remote host.
- **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*"
```

2.604 LP_Local Users Reconnaissance through WMI

- **Trigger Condition:** This alert is triggered whenever it detects the usage of WMI for listing all local user accounts.
- **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*"
```

2.605 LP_Installed Software Updates Reconnaissance through WMI

- **Trigger Condition:** This alert is triggered whenever it detects the usage of WMI to list installed Software hotfix and patches.
- **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*"
```

2.606 LP_Application uninstall via WMIC

- **Trigger Condition:** This alert rule is triggered when the Windows Management Instrumentation Command-line (WMIC) tool is detected uninstalling applications on a system.
- **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*"
```

2.607 LP_AppInit DLLs Detected

- **Trigger Condition:** Adversaries establish persistence and/or elevate privileges by executing malicious content triggered by AppInit DLLs loaded into processes.
- **ATT&CK Category:** Persistence, Privilege Escalation
- **ATT&CK Tag:** Event Triggered Execution, AppInit DLLs
- **ATT&CK ID:** T1546, T1546.010
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **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\WindowsNT\CurrentVersion\Windows\Appinit_
↪Dlls\*") -user IN EXCLUDED_USERS
```

2.608 LP_High Severity EPP Alert

- **Trigger Condition:** High or critical severity alert 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, Trend Vision
- **Query:**

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

2.609 LP_Host Generating Multiple Medium Severity EPP Alert

- **Trigger Condition:** Multiple medium severity alerts 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, Trend Vision
- **Query:**

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

2.610 LP_Host Generating Multiple High Severity EPP Alert

- **Trigger Condition:** Multiple high or critical severity alerts 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, Trend Vision
- **Query:**

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

2.611 LP_Medium Severity EPP Alert

- **Trigger Condition:** Medium severity alert 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, Trend Vision
- **Query:**

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

2.612 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
```

2.613 LP_Suspicious Hack Tools Execution

- **Trigger Condition:** This alert is triggered whenever it detects the execution of different Windows based hacktools via their import hash (imphash) even if the files have been renamed. The List 'MALICIOUS_TOOLS_IMPHASH' must be imported beforehand 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
```

2.614 LP_Suspicious Execution of XORDump Utility for LSASS Memory Dump

- **Trigger Condition:** This alert is triggered whenever it detects suspicious execution of XORDump Utility, commonly used for LSASS Memory Dump. It is used to dump LSASS memory while also bypassing security measures like AV, EDR etc. In some cases, lsass.exe minidump files are signatured by AV and deleted. The dll loaded into this bin for minidumping (dgbhelp) ALWAYS writes the minidump to disk, but before this binary closes the file handle, it re-reads the contents into memory, closes the handle and immediately deletes the file. the output is safe in memory and passed to an Xor function which then re-writes the xor'd data to disk, where it can be safely exfilled. Adversaries may use this tool to steal LSASS minidump files stealthy bypassing the security.
- **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 *"]
```

2.615 LP_Suspicious Execution of Createdump Utility for Memory Dump

- **Trigger Condition:** This alert is triggered whenever it detects the usage of the createdump.exe LOLOBIN utility to dump process memory. createdump.exe is Microsoft .NET Runtime Crash Dump Generator (included in .NET Core). Attackers often leverage this utility to dump LSASS process memory while also evasing the defense. lsass.exe, which stands for Local Security Authority Subsystem Service, is a crucial Windows system process responsible for various security-related functions, including user authentication and managing security policies. 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*"]
```

2.616 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*")
```

2.617 LP_Suspicious Activities Associated with NTDS Exfiltration

- **Trigger Condition:** This alert is triggered whenever it detects suspicious activities related to the Active Directory Domain Database (ntds.dit). NTDS file is present in the DC and contains sensitive information such as Active Directory data, including

credentials, information about user objects, groups, and group membership. Adversaries may attempt to access or create a copy of the Active Directory domain database in order to steal credential information, as well as obtain other 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\*"]))
```

2.618 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"
```

2.619 LP_Possible LSASS Dump Via SilentProcessExit Technique

- **Trigger Condition:** This alert is triggered whenever it detects a possible LSASS dump Via the SilentProcessExit Technique. It Detects changes to the Registry in which a monitor program gets registered to dump the memory of the lsass.exe process. SilentProcessExit method relies on a mechanism introduced in Windows 7 called Silent Process Exit, which provides the ability to trigger specific actions for a monitored process in one of two scenarios; either the process terminates itself by calling ExitProcess(), or another process terminates it via the TerminateProcess() API.
- **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*"
```

2.620 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*"]
```

2.621 LP_Microsoft IIS Service Account Password Dumped

- **Trigger Condition:** This alert is triggered whenever it detects the execution of Information Services (IIS) command-line tool, AppCmd, being used to list passwords. 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*", "*:\*"])
```

2.622 LP_Dumpert Process Dumper Execution

- **Trigger Condition:** This alert is triggered whenever it detects the use of Dumpert process dumper, which dumps the lsass.exe process memory. lsass.exe, which stands for Local Security Authority Subsystem Service, is a crucial Windows system process responsible for various security-related functions, including user authentication and managing security policies. Adversaries often seek to dump the lsass.exe process memory because it contains sensitive information, such as

user credentials and authentication tokens. By extracting this information from lsass.exe, attackers can potentially gain unauthorized access to a system or escalate their privileges, making it a high-value target for malicious actors. Detecting and preventing such memory dumps is critical to safeguarding the security of a Windows system.

- **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*"
```

2.623 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*" )
```

2.624 LP_Malicious PowerShell Commandlets Detected

- **Trigger Condition:** Execution of malicious PowerShell commandlets.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** PowerShell
- **ATT&CK ID:** T1059.001
- **Minimum Log Source Requirement:** PowerShell, Windows
- **Query:**

```
event_source="Microsoft-Windows-PowerShell" ((event_id="4103" command IN MALICIOUS_
↪POWERSHELL_COMMANDLET_NAMES -command="*Get-SystemDriveInfo*") OR (event_id=
↪"4104" script_block IN MALICIOUS_POWERSHELL_COMMANDLET_NAMES -script_block=
↪"*Get-SystemDriveInfo*" ))
```

2.625 LP_Suspicious Base64 Encoded PowerShell Command

- **Trigger Condition:** Execution of suspicious base64 encoded commands via PowerShell.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** PowerShell
- **ATT&CK ID:** T1059.001
- **Minimum Log Source Requirement:** Windows, PowerShell, Windows Sysmon
- **Query:**

```
label="Process" label=Create
("process" IN ["*\powershell.exe", "\*pwsh.exe"] OR file IN ["PowerShell.EXE", "pwsh.dll"])
command IN ["* hidden *",
 "*AGkAdABzAGEAZABtAGkAbgAgAC8AdAByAGEAbgBzAGYAZQByA*",
 "*aXRzYWRtaW4gL3RyYW5zZmVy*",
 "*IAaQB0AHMAYQBkAG0AaQBuACAALwB0AHIAYQBuAHMAZgBlAHIA*",
 "*JpdHNhZG1pbiAvdHJhbnNmZX*",
 "*YgBpAHQAcwBhAGQAbQBpAG4AIAAvAHQAcgBhAG4AcwBmAGUAcg*",
 "*Yml0c2FkbWluIC90cmFuc2Zlc*", "*AGMAaAB1AG4AawBfAHMAaQB6AGUA*",
```

(continues on next page)

(continued from previous page)

```
"*JABjAGgAdQBuAGsAXwBzAGkAegBlA*", "*JGNodW5rX3Npem*",
"*QAYwBoAHUAbgBrAF8AcwBpAHoAZQ*", "*RjaHVua19zaXpl*", "*Y2h1bmtfc2l6Z*",
"*AE8ALgBDAG8AbQBwAHIAZQBzAHMAaQBvAG4A*",
"*kATwAuAEMAbwBtAHAAcgBlAHMAcwBpAG8Abg*", "*lPLkNvbXByZXNzaW9u*",
"*SQBPAC4AQwBvAG0AcAByAGUAcwBzAGkAbwBuA*", "*SU8uQ29tcHJlc3Npb2*",
"*Ty5Db21wcmVzc2lvb*", "*AE8ALgBNAGUAbQBvAHIAeQBTAHQAcgBlAGEAbQ*",
"*kATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtA*", "*lPLk1lbW9yeVN0cmVhb*",
"*SQBPAC4ATQBlAG0AbwByAHkAUwB0AHIAZQBhAG0A*", "*SU8uTWVtb3J5U3RyZWFt*",
"*Ty5NZW1vcnlTdHJlYW*", "*4ARwBlAHQAQwBoAHUAbgBrA*", "*5HZXRDaHVua*",
"*AEcAZQB0AEMAaAB1AG4Aaw*", "*LgBHAGUAdABDAGgAdQBuAGsA*",
"*LkdldENodW5r*", "*R2V0Q2h1bm*", "*AEgAUgBFAEEARABfAEkATgBGAE8ANgA0A*",
"*QASABSAEUAQQBEAF8ASQBOAEYATwA2ADQA*", "*RlUkVBRF9JTkZPNj*",
"*SFJFQURfSU5GTzY0*", "*VABlAFIARQBBAEQAXwBJAE4ARgBPADYANA*",
"*VEhSRUFEX0lORk82N*",
"*AHIAZQBhAHQAZQBSAGUAbQBvAHQAZQBUAGgAcgBlAGEAZA*",
"*cmVhdGVSZW1vdGVUaHJlYW*",
"*MAcgBlAGEAdABlAFIAZQBtAG8AdABlAFQAaAByAGUAYQBkA*",
"*NyZWF0ZVJlbW90ZVRocmVhZ*", "*Q3JlYXRlUmVtb3RlVGhyZWFk*",
"*QwByAGUAYQB0AGUAUgBlAG0AbwB0AGUAVABoAHIAZQBhAGQA*",
"*0AZQBtAG0AbwB2AGUA*", "*1lbW1vdm*", "*AGUAbQBtAG8AdgBlA*",
"*bQBlAG0AbQBvAHYAZQ*", "*bWVtbW92Z*", "*ZW1tb3Zl*"]
```

2.626 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 *"]
```

2.627 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"]
```

2.628 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"]
```

2.629 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*"]
```

2.630 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
↪Browserprotection\DisallowExploitProtectionOverride", "*\Features\TamperProtection",
↪"*\MpEngine\MpEnablePus", "*\PUAProtection", "*\SignatureUpdate\ForceUpdateFromMU
↪", "*\SpyNet\SpynetReporting", "*\SpyNet\SubmitSamplesConsent", "*\Windows Defender
↪Exploit Guard\ControlledFolder Access\EnableControlledFolderAccess"] )
```

(continues on next page)

(continued from previous page)

2.631 LP_Executable Files Created and Executed by Office Applications

- **Trigger Condition:** Executable file dropped or modified via office applications and executed within a specific time range.
- **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
```

2.632 LP_WMI Backdoor in Exchange Transport Agent

- **Trigger Condition:** This alert is triggered whenever it detects a WMI backdoor in Exchange Transport Agents (ETA) via WMI event filters. Microsoft Exchange Server's Exchange Transport Agents enable customization and expansion of the mail flow process and are in charge of checking, processing and altering messages as they move through the transport pipeline of the Exchange Server. Adversaries plant WMI backdoors in ETA using WMI event filters in order to maintain persistence or privilege escalation.
- **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:\ProgramFiles\Microsoft\Exchange Server\*" "process"="*\Bin\OleConverter.exe")))
-user IN EXCLUDED_USERS
```

2.633 LP_Suspicious Msiexec Usage Detected

- **Trigger Condition:** A .msi file executed from the publicly writable folder, and a command prompt or powershell spawned by msiexec. Adversaries can use this technique to execute their payload by evading defence.
- **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 ["*C:\Users*","*\ProgramData*", "*\AppData\Local*", "*\AppData\Roaming*",
↪"*\Users\Public*"] command="*msi*")
OR
(command ="*://*")
OR
(command IN ["*/i*", "*-i*"] ((command IN ["*/q*", "*/quiet*", "*/qn*", "*-q*", "*-quiet*", "*-
↪qn*"])
OR (command IN ["*-Q-I*", "*-I-Q*", "*/q-i*", "*-q/i*", "*/q/i*" ]))
-(parent_image="*setup*") -integrity_level=SYSTEM)
OR
("process"="*/msiexec.exe" command="*http*")
OR
(-"process" IN ["C:\Windows\System32\*", "C:\Windows\SysWOW64\*",
↪"C:\Windows\WinSxS\*"])
)
OR
("parent_process"="*\msiexec.exe"
"process" IN ["*\cmd.exe","*\powershell.exe","*\icacls.exe","*\expand.exe", "*\rundll32.exe",
↪ "*\pwsh.exe"]))
```

2.634 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="*/lng*"))
```

2.635 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 ["*AUTHORI*", "*AUTORI*"]) OR (target_object=
↪"*Control\Print\Monitors\MONVNC\Driver*") OR (target_object=
↪"*Control\Print\Environments\*" target_object="*\Drivers\*" target_object="*\VNC Printer*
↪"))
```

2.636 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"]
```

2.637 LP_Alternate PowerShell Hosts via Powershell Module

- **Trigger Condition:** Alternate PowerShell host trying to bypass detections based on powershell.exe. Adversaries can use this technique to potentially bypass detections looking for powershell.exe. They can use it to discover information or execute malicious code.
- **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_source="Microsoft-Windows-PowerShell" 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*", "*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*"])
```

(continues on next page)

(continued from previous page)

2.638 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, Windows
- **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*" ]
```

2.639 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
```

2.640 LP_Alternate PowerShell Hosts via Named Pipe

- **Trigger Condition:** This alert is triggered whenever it detects alternate Command and Scripting Interpreter, PowerShell hosts. PowerShell commands/scripts can also be executed without directly invoking the powershell.exe binary. Adversaries might use this technique to potentially bypass detections looking for powershell.exe. Logging for named pipe events must be configured in Sysmon config for this alert to work. However, Programs using PowerShell directly without invocation of a dedicated interpreter might trigger false positives.
- **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"]
```

- **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
↪", "*\onenoteim.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","regsvcs.exe","regsvr32.exe","rundll32.exe","schtasks.exe",
↪"scriptrunner.exe","wmic.exe","workfolders.exe","wscript.exe"])
```

2.641 LP_RClone Utility Execution

- **Trigger Condition:** Execution of the RClone tool or command line option used in the tool. Adversaries can utilize this utility to exfiltrate data to cloud storage.
- **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 *"])
```

2.642 LP_UAC Bypass via SDCLT

- **Trigger Condition:** Attempt to bypass User Account Control (UAC) via SDCLT.exe or modification to registry keys HKCU:SoftwareClassesexefileshellrunascommandisolatedCommand and HKCU:SoftwareClassesFoldershellopencommand indicating UAC bypass via 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*"])
```

2.643 LP_Suspicious Binary Execution in User Directory

- **Trigger condition:** Execution of binaries from the users directory by Microsoft Office software such as Word and Excel. This may indicate dropping and subsequent execution of payloads by malicious Microsoft Office documents.
- **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
↪", "*\onenote.exe", "*\onenoteim.exe"] "process"="C:\Users\*.exe" -"process"=
↪"*\Microsoft\Teams\current\Teams.exe"
```

(continues on next page)

(continued from previous page)

2.644 LP_Suspicious WMIC Child Process

- **Trigger condition:** Suspicious child process of WMIC is detected. Adversaries can utilize this technique to execute arbitrary commands, payloads, and evade defenses by using Windows internal binary.
- **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"]
```

2.645 LP_Suspicious File Execution Using Wscript or Cscript

- **Trigger condition:** This alert is triggered whenever file with extensions of jse,vbe,js,vba is executed using wscript or cscript. Wscript and cscript are windows binaries that provides an environment in which users can execute scripts in a variety of languages or starts a script to run in a command-line environment. Adversaries can write malicious payloads in file with above mention extensions and execute it using wscript or cscript and bypass detection.
- **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="Process" label="Create"
"process" IN ["*\wscript.exe", "*\cscript.exe"]
command IN ["*.jse*", "*.vbe*", "*.js*", "*.vba*","*.vbs*"]
-path IN ["C:\Program Files\Microsoft Monitoring Agent\Agent\Health Service State\*"]
-command IN ["*.json*","*C:\Windows\system32\slmgr.vbs*-rearm*"]
```

2.646 LP_BCDEdit Safe Mode Command Execution

- **Trigger condition:** This alert is triggered whenever spawning of BCDEDIT from suspicious processes is detected to configure reboot into Safe Mode. Safe Mode is a diagnostic mode in Windows that starts the system with a limited set of drivers and services, allowing users to troubleshoot problems that may be preventing the system from starting normally. Bcdedit is Windows internal binary that allows users to view and modify the boot configuration data (BCD) settings. Adversaries can use Safe Mode commands such as "minimal", "network", and "safebootalternateshell" to bypass security mechanisms and execute arbitrary commands with elevated privileges as limited softwares are services are only available in safe boot mode.
- **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*", "*delete*", "*import*", "*safeboot*"] parent_
↪process IN ["*\WINWORD.EXE", "*\EXCEL.EXE", "*\POWERPNT.EXE", "*\MSACCESS.EXE",
↪ "*\MSPUB.EXE", "*\OUTLOOK.EXE", "*\fltldr.exe", "*\cscript.exe", "*\powershell.exe",
↪"*\pwsh.exe", "*\wscript.exe", "*\cmd.exe", "*\rundll32.exe", "*\regsvr32.exe", "*\mshta.exe
↪", "*\msbuild.exe"]
```

2.647 LP_Suspicious Encoded PowerShell Command Line

- **Trigger condition:** 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 aWV4I*", "* -e SQBFAFgA*", "* -e aQBlAHgA*", "* -enc
↪SUVYI*", "* -enc aWV4I*", "* -enc SQBFAFgA*", "* -enc aQBlAHgA*"] -command="* -
↪ExecutionPolicy remotesigned *" -user IN EXCLUDED_USERS
```

2.648 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"]
```

2.649 LP_Firewall Rule Addition via Netsh Detected

- **Trigger condition:** This alert is triggered whenever a connection is allowed by a port or application on the Windows firewall. An attacker can use the Netsh utility to add or modify firewall rules to allow unauthorized network traffic to bypass the firewall and reach its target. For example, an attacker could use Netsh to allow inbound connections on a specific. Legitimate administration activity and software installations and removal also trigger this alert.

- **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
```

2.650 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*"])
```

2.651 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\SophosEndpoint*\SEDEnabled",
↪"*\CurrentControlSet\Services\Sophos Endpoint*\SAVEnabled "] detail="DWORD
↪(0x00000000)"
```

2.652 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=*
```

2.653 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\*"])
```

2.654 LP_Suspicious WerFault File Creation

- **Trigger condition:** A non-system process drops the WerFault.exe binary inside the C:WindowsWinSxSfolder 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\Systems32\*","C:\Windows\SysWOW64\*","*C:\Windows\WinSxS\*"]
```

2.655 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")
```

2.656 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*"])
```

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

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

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

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

2.659 LP_AADInternals PowerShell Cmdlet Execution

- **Trigger condition:** 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
```

2.660 LP_Suspicious Scheduled Task Creation via Masqueraded XML File

- **Trigger condition:** Creation of a suspicious scheduled task using an XML file with a masqueraded extension.
- **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
- **Query:**

```
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
↪CameraStation\SetupActions.exe", "*:\Program Files\Axis Communications\AXIS
↪DeviceManager\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" ))
```

2.661 LP_Suspicious Microsoft Equation Editor Child Process

- **Trigger condition:** This alert is triggered whenever suspicious child process of Microsoft's equation editor is detected which is a sign of possible exploitation of CVE-2017-11882. CVE-2017-11882 is a vulnerability in Microsoft Office's Equation Editor component. An attacker might use the vulnerability to execute arbitrary code on a target system by producing a malicious Microsoft Office file (such as a Word document) that, when opened, activates the vulnerability.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Exploitation for Client Execution
- **ATT&CK ID:** T1203
- **Minimum Log Source Requirement:** Windows Sysmon, Windows

- **Query:**

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

2.662 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
- **Query:**

```
[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
```

2.663 LP_Bypass UAC via CMSTP Detected

- **Trigger condition:** Child processes of automatically elevated Microsoft Connection Manager Profile Installer instances like cmstp.exe are detected.
- **ATT&CK Category:** Privilege Escalation, Defense Evasion
- **ATT&CK Tag:** CMSTP, Bypass User Account Control
- **ATT&CK ID:** T1218.003, 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*"])
OR
(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"])
)
-user IN EXCLUDED_USERS
```

2.664 LP_Application Whitelisting Bypass via Dxcap Detected

- **Trigger condition:** This alert is triggered whenever adversaries bypass process and/or signature-based defenses by execution of Dxcap.exe is detected. DXCap.exe is a command-line tool for graphics diagnostics capture and playback. Adversaries may take advantage of this trusted developer utility to proxy the execution of malicious payloads. Legitimate execution of dxcap.exe by a legitimate user could generate false-positives.
- **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
```

2.665 LP_Suspicious WMIC XSL Script Execution

- **Trigger condition:** Loading of a Windows Script module through WMIC by Microsoft Core XML Services (MSXML) process to bypass application whitelisting. Adversaries may abuse this functionality to execute arbitrary files while potentially bypassing application control.

- **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:texttablewsys*", "*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
```

2.666 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*"]
```

2.667 LP_Regsvr32 Anomalous Activity Detected

- **Trigger condition:** This alert is triggered whenever it detects various anomalous Regsvr32.exe activities. Regsvr32 is a command-line utility used to register and unregister object linking and embedding controls, including dynamic link libraries (DLLs), on Windows systems. Adversaries often abuses Regsvr32 for proxy execution of malicious code.

- **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, Windows
- **Query:**

```
label="Process" label=Create
((("process"="*\regsvr32.exe" (command IN ["*\AppData\Local*", "*C:\Users\*", "*\Temp\*"]
↪OR command="*\\*\*"))
OR ("process"="*\regsvr32.exe" parent_process IN ["*\powershell.exe", "*\pwsh.exe",
↪"*\powershell_ise.exe","*\cmd.exe"]) OR ("process"="*\regsvr32.exe" command="*/i:*"
↪command="*http*" command="*scrobj.dll") OR ("process"="*\regsvr32.exe" command="*/
↪i:*" command="*ftp*" command="*scrobj.dll") OR ("process" IN ["*\cscript.exe", "*\wscript.
↪exe"] parent_process="*\regsvr32.exe") OR ("process"="*\EXCEL.EXE" command="*..\..\..
↪\Windows\System32\regsvr32.exe *") OR (parent_process="*\mshta.exe" "process"=
↪"*\regsvr32.exe") OR ("process"="*\regsvr32.exe" command IN ["*\AppData\Local*",
↪"*C:\Users\Public*"]) OR ("process"="*\regsvr32.exe" command IN ["*.jpg", "*.jpeg", "*.png
↪", "*.gif", "*.bin", "*.tmp", "*.temp", "*.txt"]))
-(command IN ["*\AppData\Local\Microsoft\Teams*",
↪"*\AppData\Local\WebEx\WebEx64\Meetings\atucfobj.dll*"] OR (parent_process=
↪"C:\Program Files\Box\Box\FS\streem.exe" command="*\Program Files\Box\Box\Temp\*"
↪OR command="*/s C:\Windows\System32\RpcProxy\RpcProxy.dll"))
```

2.668 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*"]
```

2.669 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"]
```

2.670 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="Process" label=Create "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*"
```

2.671 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 *mscfileshellopencommand* or *ms-settingsshellopencommand*.
- **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\*"]
```

2.672 LP_Unsigned Image Loaded Into LSASS Process

- **Trigger condition:** Loading unsigned images like DLL or EXE into the LSASS process.
- **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
```

2.673 LP_Usage of Sysinternals Tools Detected

- **Trigger condition:** Usage of Sysinternals tools due to the addition of accepteula key to a registry.
- **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*"])
```

2.674 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*')
```

2.675 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
```

2.676 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 *"
```

2.677 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*"
```

2.678 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="Process" label=Create "process"="*\gpscript.exe" command IN ["* /logon*", "* /
↪startup*"] -parent_command="*\windows\system32\svchost.exe -k netsvcs -p -s gpsvc"
```

2.679 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*"
```

2.680 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\*
↪"
```

2.681 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 [
↪"*:\Program Files\Windows Defender\*",
↪"*:\ProgramData\Microsoft\WindowsDefender\Platform\*"] image="*\mpclient.dll"
```

2.682 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*"
```

2.683 LP_Credentials Capture via Rpcping Detected

- **Trigger condition:** The creation of Remote Procedure Call (RPC) via Rpcping 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"="*\rpcping.exe" command="*s *" ( (command=
↪"*u *" command="*NTLM*") OR ( command="*t *" command="*ncacn_np*"))
```

2.684 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, Windows
- **Query:**

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

2.685 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="*fullmemdmp*"
```

2.686 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*"
```

2.687 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
```

2.688 LP_Active Directory DLLs Loaded By Office Applications

- **Trigger condition:** This alert is triggered whenever it detects Kerberos DLL or DSParse DLL are loaded by Office Products such as winword, powerpoint, excel, outlook.
- **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*", "*\mspub.exe", "*\onenote.exe", "*\onenoteim.exe"]
↪image IN ["*\kerberos.dll*","*\c.dll*"]
```

2.689 LP_DCSync detected

- **Trigger condition:** Misuse of Active Directory Replication Service (ADRS) 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="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/*"))
```

2.690 LP_Active Directory Replication User Backdoor

- **Trigger condition:** This alert is triggered whenever it detects modification of the security descriptor of a domain object to grant all the active directory replication permissions to any user. The security descriptor contains the access control lists (ACLs) of the resource. With directory replication permission adversaries can perform DCsync attack.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** File and Directory Permissions Modification, Windows File and Directory Permissions Modification, DCSync
- **ATT&CK ID:** T1222, T1222.001, T1003.006
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=5136 ldap_display="ntsecuritydescriptor" attribute_value=
↪"*1131f6aa-9c07-11d1-f79f-00c04fc2dcd2*1131f6ad-9c07-11d1-f79f-00c04fc2dcd2*89e95b76-
↪444d-4c62-991a-0facbeda640c*" operation_type="Value Added"
```

2.691 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
```

2.692 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
```

2.693 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
```

2.694 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
```

2.695 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\*")
```

2.696 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>
```

2.697 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, Windows
- **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
```

2.698 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
```

2.699 LP_Authentication Package Detected

- **Trigger Condition:** The LSA process loaded by services other than lssac, svchos, msiexec 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, Windows
- **Query:**

```
label=Registry label=Set label=Value
target_object="*System\CurrentControlSet\Control\Lsa\Authentication Packages*" -"process"
↪in ["*C:\WINDOWS\system32\lsass.exe","*C:\Windows\system32\svchost.exe",
↪"*C:\Windows\system32\services.exe","C:\Windows\system32\msiexec.exe"]
```

2.700 LP_Bloodhound and Sharphound Hack Tool Detected

- **Trigger Condition:** This alert is triggered whenever it detects usage of Bloodhound and Sharphound hack tools through command line or process. BloodHound is an Active Directory (AD) reconnaissance tool that can reveal hidden relationships and identify attack paths within an AD environment. SharpHound is the official data collector for BloodHound. Adversaries can use these tools to perform reconnaissance and identify vulnerable endpoint.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Account Discovery
- **ATT&CK ID:** T1087
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

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

2.701 LP_LSASS Access from Non System Account Detected

- **Trigger Condition:** This alert is triggered whenever it detects potential mimikatz-like tools accessing LSASS from non system account. Local Security Authority Subsystem Service (Lsass.exe) is the process on an Active Directory domain controller. It's responsible for providing Active Directory database lookups, authentication, and replication. The credential data inside LSASS may include Kerberos tickets, NTLM password hashes, LM password hashes, and even clear-text passwords (to support WDigest and SSP authentication among others. Adversaries look to get access to the credential data and do so by finding a way to access the contents of memory of the LSASS process. Looking for non-system accounts getting a handle on and accessing lsass is crucial to detect lsass dumping attempts.
- **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"
access IN ["0x40", "0x1400", "0x100000", "0x1410", "0x1010", "0x1438", "0x143a", "0x1418",
↪"0x1f0fff", "0x1f1fff", "0x1f2fff", "0x1f3fff", "40", "1400", "1000", "100000", "1410", "1010",
↪"1438", "143a", "1418", "1f0fff", "1f1fff", "1f2fff", "1f3fff"]
-(
user="*$"
```

(continues on next page)

(continued from previous page)

```
OR "process" IN ["C:\Program Files*", "*\SteamLibrary\steamapps\*"]
OR ("process"="C:\Windows\System32\wbem\WmiPrvSE.exe" access="0x1410")
)
```

2.702 LP_LSASS Memory Dump Detected

- **Trigger Condition:** Process access to lsass.exe with elevated access rights. Adversaries can use this technique to gain access to lsass process memory and dump credentials.
- **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 IN [
↪"0x1fffff", "0x1038", "0x1438", "0x143a"]call_trace IN ["*dbghelp.dll*", "*dbgcore.dll*",
↪"*ntdll.dll*","*kernel32.dll*","*kernelbase.dll*"]-("process"="*\Sysmon64.exe" OR (call_
↪trace="*:\Windows\Temp\asgard2-agent\*" call_trace="*\thor\thor64.exe+*" call_trace=
↪"*|UNKNOWN(*" access="0x103800"))-"process"="*\Sysmon64.exe"
```

2.703 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
```

2.704 LP_LSSAS Memory Dump with MiniDumpWriteDump API Detected

- **Trigger condition:** This alert is triggered whenever it detects the use of MiniDumpWriteDump API for dumping lsass.exe memory in a stealthy way. Tools like ProcessHacker and some attacker tradecraft use this API found in dbghelp.dll or dbgcore.dll. As an 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:** 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
```

2.705 LP_Macro file Creation Detected

- **Trigger Condition:** This alert is triggered whenever macro file creation is detected. A macro is a script or program that automates tasks within applications like Microsoft Office through VBScripting. It is essential to detect the creation of macro files in the system as Adversaries often use macro-enabled files to deliver malware, exploit vulnerabilities, or trick users into enabling malicious code.
- **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","*.vdm"]
```

2.706 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*",
 "*aXRzYWRtaW4gL3RyYW5zZmVy*",
 "*IAaQB0AHMAYQBkAG0AaQBuACAALwB0AHIAYQBuAHMAZgBlAHIA*",
 "*JpdHNhZG1pbiAvdHJhbnNmZX*",
 "*YgBpAHQAcwBhAGQAbQBpAG4AIAAvAHQAcgBhAG4AcwBmAGUAcg*",
 "*Yml0c2FkbWluIC90cmFuc2Zlc*",
 "*AGMAaAB1AG4AawBfAHMAaQB6AGUA*", "*JABjAGgAdQBuAGsAXwBzAGkAegBlA*",
 "*JGNodW5rX3Npem*","*QAYwBoAHUAbgBrAF8AcwBpAHoAZQ*", "*RjaHVua19zaXpl*",
 "*Y2h1bmtfc2l6Z*",
 "*AE8ALgBDAG8AbQBwAHIAZQBzAHMAaQBvAG4A*",
 "*kATwAuAEMAbwBtAHAAcgBlAHMAcwBpAG8Abg*", "*lPLkNvbXByZXNzaW9u*",
 "*SQBPAC4AQwBvAG0AcAByAGUAcwBzAGkAbwBuA*", "*SU8uQ29tcHJlc3Npb2*",
 "*Ty5Db21wcmVzc2lvb*", "*AE8ALgBNAGUAbQBvAHIAeQBTAHQAcgBlAGEAbQ*",
 "*kATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtA*",
 "*lPLk1lbW9yeVN0cmVhb*","*SQBPAC4ATQBlAG0AbwByAHkAUwB0AHIAZQBhAG0A*",
 "*SU8uTWVtb3J5U3RyZWFt*", "*Ty5NZW1vcnlTdHJlYW*",
 "*4ARwBlAHQAQwBoAHUAbgBrA*", "*5HZXRDaHVua*","*AEcAZQB0AEMAaAB1AG4Aaw*",
 "*LgBHAGUAdABDAGgAdQBuAGsA*", "*LkdldENodW5r*","*R2V0Q2h1bm*",
 "*AEgAUgBFAEEARABfAEkATgBGAE8ANgA0A*",
 "*QASABSAEUAQQBEAF8ASQBOAEYATwA2ADQA*", "*RlUkVBRF9JTkZPNj*",
 "*SFJFQURfSU5GTzY0*", "*VABIAFIARQBBAEQAXwBJAE4ARgBPADYANA*",
 "*VEhSRUFEX0lORk82N*",
 "*AHIAZQBhAHQAZQBSAGUAbQBvAHQAZQBUAGgAcgBlAGEAZA*",
```

(continues on next page)

(continued from previous page)

```
"*cmVhdGVSZW1vdGVUaHJlYW*",
"*MAcgBlAGEAdABlAFIAZQBtAG8AdABlAFQAaAByAGUAYQBkA*",
"*NyZWF0ZVJlbW90ZVRocmVhZ*", "*Q3JlYXRlUmVtb3RlVGhyZWFk*",
"*QwByAGUAYQB0AGUAUgBlAG0AbwB0AGUAVABoAHIAZQBhAGQA*",
"*0AZQBtAG0AbwB2AGUA*", "*1lbW1vdm*", "*AGUAbQBtAG8AdgBlA*",
"*bQBlAG0AbQBvAHYAZQ*", "*bWVtbW92Z*", "*ZW1tb3Zl*"] -user IN EXCLUDED_USERS
```

2.707 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
```

2.708 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="0x1FFFFF" (call_
↪trace="*|UNKNOWN(*VBE7.DLL*" OR ("process"="*\Microsoft Office\*" call_trace=
↪"*|UNKNOWN*")) -user IN EXCLUDED_USERS
```

2.709 LP_RSA SecurID Passcode Reuse

- **Trigger Condition:** This alert is triggered when passcode reuse event occurs.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Brute Force
- **ATT&CK ID:** T1110
- **Minimum Log Source Requirement:** RSA Secure ID

```
norm_id=RSA_SecurID type=Runtime label=Passcode label=Reuse
```

2.710 LP_Suspicious Atbroker Execution Detected

- **Trigger Condition:** This alert is triggered whenever Atbroker executing non-default Assistive Technology applications is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** System Binary Proxy Execution
- **ATT&CK ID:** T1218
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="Process" label="Create" "process"="*\atbroker.exe" command="*start*" -command
↪IN ["*animations*","*audiodescription*","*caretbrowsing*","*caretwidth*","*colorfiltering*",
↪"*cursorscheme*","*filterkeys*","*focusborderheight*","*focusborderwidth*","*highcontrast*
↪","*keyboardcues*","*keyboardpref*","*magnifierpane*","*messageduration*",
↪"*minimumhitradius*","*mousekeys*","*Narrator*","*osk*","*overlappedcontent*",
↪"*showsounds*","*soundsentry*","*stickykeys*","*togglekeys*","*windowarranging*",
↪"*windowtracking*","*windowtrackingtimeout*","*windowtrackingzorder*"]
```

2.711 LP_Suspicious MMC Process Pattern

- **Trigger Condition:** This alert is triggered when .msc (Microsoft Management Console) files are executed from outside the default Windows path: C:WindowsSystem32.
- **ATT&CK Category:** Defense Evasion

- **ATT&CK Tag:** MMC
- **ATT&CK ID:** T1218.014
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="Process" label=Create
"process"="*\mmc.exe" command="*.msc*"
| process regex('(?P<filter_command>\S+\.msc")',command, "filter = true")
| search -filter_command="*C:\Windows\System32*"
```

2.712 LP_Windows unBlock Inheritance on OU or Domain

- **Trigger Condition:** This alert is triggered whenever inheritance is set to unblock on OU or domain.
- **ATT&CK Category:** Defense Evasion, Privilege Escalation
- **ATT&CK Tag:** Group Policy Modification
- **ATT&CK ID:** T1484.001
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label=Change label=Service label=Directory
(value=0 OR attribute_value=0) class IN ["domainDNS", "organizationalUnit"]
-user IN EXCLUDED_USERS
```

2.713 LP_Application Whitelisting Bypass with DLL load via ODBC

- **Trigger Condition:** This alert gets triggered when the odbcconf executable loads DLLs.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Odbcconf
- **ATT&CK ID:** T1218.008

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

```
label="process" label=create
(("process"="*\odbcconf.exe" command IN ["*-f*", "*regsvr*"]) OR (parent_process=
↪"*\odbcconf.exe" "process"="*\rundll32.exe"))
```

2.714 LP_Possible UAC Bypass via System Configuration Utility

- **Trigger Condition:** This alert gets triggered when msconfig token modification is used to possibly bypass UAC.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Bypass User Account Control
- **ATT&CK ID:** T1548.002
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
    label="Process" label="Create"
"process"="*\msconfig.exe" "command"="*msconfig*-5*"
integrity_level IN ["High", "System"]
```

CHAPTER

THREE

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:** VMmware'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.
- **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
```

3.15.1 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\fSingleSessionPerUser*", "*\Control\Terminal Server\fDenyTSConnections*"] -user IN
↪EXCLUDED_USERS
```

3.16 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
```

3.17 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
```

3.18 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.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create
command="*winrm*"  command="*invoke Create wmicimv2/Win32_*" command="*-r:http*"
```

3.18.1 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.
- **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\*"])
```

3.19 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.
- **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")
```

3.20 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.
- **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*")
```

3.21 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.
- **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*"
```

3.22 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.

- **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 *"]
```

3.23 LP_Process Pattern Match For CVE-2021-40444 Exploitation

- **Trigger Condition:** The process pattern for CVE-2021-40444 is detected. CVE-22021-4044 is a remote code execution vulnerability in MSHTML, which is Microsoft's proprietary browser engine for Internet Explorer.
- **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"
```

3.24 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"]
```

3.25 LP_Proxy Execution via Workfolders

- **Trigger Condition:** This alert is triggered whenever it detects the usage of workfolders binary to execute other process.
- **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"
```

3.26 Proxy Execution via Windows Update Client

- **Trigger Condition:** When wuauclt.exe is used to proxy execute codes.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label="Create" ("process"="*\wuauclt.exe" OR file="wuauclt.exe")
(command="*UpdateDeploymentProvider*" command="*.dll*" command=
↪"*RunHandlerComServer*")
-(command IN ["* /UpdateDeploymentProvider UpdateDeploymentProvider.dll *", "* wuaueng.
↪dll *"])
```

3.27 Suspicious DLL Execution Using Windows Address Book

- **Trigger Condition:** When a suspicious DLL is executed using wab.exe.

- **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"
```

3.28 LP_Suspicious Use of Dotnet Detected

- **Trigger Condition:** This alert is triggered when execution of either suspicious DLL or unsigned code using dotnet.exe is detected.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create command IN ["*.dll", "*.csproj"] "process"="*\dotnet.exe"
```

3.29 Execution of Arbitrary Executable Using Stordiag

- **Trigger Condition:** When a renamed arbitrary executable is executed using stordiag.exe. stordiag.exe collects storage and file system diagnostic logs and outputs to a folder.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Create" label="Process" parent_process="*\stordiag.exe" "process" IN ["*\schtasks.exe
↪", "*\systeminfo.exe", "*\fltmc.exe"] - parent_process IN ["C:\windows\system32\*",
↪"C:\windows\syswow64\*"]
```

3.30 Process Creation via Time Travel Tracer

- **Trigger Condition:** When a new child process is spawned via tttracer.exe.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create "parent_process"="*\tttracer.exe"
```

3.31 LP_Time Travel Debugging Utility DLL Loaded

- **Trigger Condition:** This alert is triggered whenever time travel debugging utility DLLs are loaded. Ttdrecord.dll, ttdwriter.dll and ttdloader.dll are part of time travel debugging utility.
- **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"]
```

3.32 File Execution via Msdeploy

- **Trigger Condition:** This alert is triggered whenever Msdeploy is used to execute files. Microsoft deploy (Msdeploy) is a binary that allows user to deploy Web Apllications.
- **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*"
```

3.33 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.
- **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"]
```

3.34 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).
- **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"
```

3.35 LP_Suspicious Usage of BitLocker Management Script

- **Trigger Condition:** This alert is triggered whenever proxy execution of malicious payloads via Manage-bde.wsf is detected.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label="Create" (("process"="*\wscript.exe" OR file="wscript.exe") command=
↪"*manage-bde.wsf*")
OR ( parent_process IN ["*\cscript.exe", "*\wscript.exe"] command="*manage-bde.wsf*" -
↪"process"="*\cmd.exe")
```

3.36 Proxy Execution of Payloads via Microsoft Signed Script

- **Trigger Condition:** This alert rule is triggered when it detects proxy execution of PowerShell code via Microsoft signed script “CL_Mutexverifiers.ps1”.
- **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 *"]
```

3.37 Execution of Windows Defender Offline Shell from Suspicious Folder

- **Trigger Condition:** When OfflineScannerShell.exe is executed from a folder other than the default.

- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="Create" label="Process" ("process"="*\OfflineScannerShell.exe" -((path="C:\Program
↪Files\Windows Defender\Offline\") OR (-path=*)))
```

3.38 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*"
↪command="*.dll*"
```

- **Trigger Condition:** When proxy execution of binaries via appvlp.exe is detected.
- **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*"]
```

3.39 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*"]
```

3.40 Suspicious Usage of Squirrel Binary

- **Trigger Condition:** When squirrel.exe is run via using arguments download, update and updateRoolback arguments.
- **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*"]
```

3.41 LP_Suspicious File Share Permission

- **Trigger Condition:** This alert is triggered whenever it detects execution of binaries from suspicious folder.
- **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*"
```

3.42 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
↪"]
```

3.43 LP_Default Possible Non-PCI Compliant Inbound Network Traffic Detected

- **Trigger Condition:** This alert is triggered whenever inbound connection is seen into secure devices over non-compliant ports as specified by PCI compliance practices. NON_PCI_COMPLIANT_PORT list needs to be updated for this query to work properly.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Firewall, IDS, IPS

- **Query:**

```
label=Inbound label=Connection destination_port IN NON_PCI_COMPLIANT_
↪PORT -source_address IN HOMENET
```

3.44 LP_High Severity EPP Alert

- **Trigger Condition:** This alert is triggered whenever a high or critical severity alert is generated by any Endpoint Protection Platform (EPP).
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** CrowdStrikeEPO, Microsoft Defender ATP, Trend Vision
- **Query:**

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

3.45 LP_Medium Severity EPP Alert

- **Trigger Condition:** This alert is triggered whenever a medium severity alert is generated by any Endpoint Protection Platform (EPP).
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** CrowdStrikeEPO, Microsoft Defender ATP, Trend Vision
- **Query:**

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

3.46 LP_Proxy Execution via Appvlp

- **Trigger Condition:** This alert is triggered whenever proxy execution of binaries via appvlp.exe is detected.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **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*"]
```

3.47 LP_Suspicious Extexport Execution Detected

- **Trigger Condition:** This alert is triggered when a service is created by loading a DLL using the ExtExport service in IE.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create command IN ["*ExtExport*", "extexport"]
```

3.48 LP_Suspicious Usage of Squirrel Binary

- **Trigger Condition:** This alert is triggered whenever squirrel.exe is run via using arguments download, update, and updateRoolback arguments.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A

- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*\Squirrel.exe" command IN ["*download*",
↪"*update*"]
```

3.49 LP_Threat Intel Connections with Suspicious Domains

- **Trigger Condition:** This alert is triggered when a connection is established with suspicious domain.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** IDS, Firewall, 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
```

CHAPTER

FOUR

ALERT RULES ANALYTICS

4.1 Alert Rules Dashboard

4.1.1 LP_Mitre Attack Analytics Overview

This dashboard consists of the following widgets:

Widget Name	Description
Triggered Attack Tactics	The count of different attack tactics triggered by attackers in your system based on the MITRE ATT&CK framework, categorized and summed by various tactics such as Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration and Impact. It helps administrators enhance their security posture, prioritize incident response, allocate resources effectively, and improve overall threat detection and mitigation strategies.
Triggered Attack Tactics - Timetrend	An hourly trend of various attack tactics triggered within your system, categorized according to the MITRE ATT&CK framework. It helps administrators maintain a robust and responsive security posture, ensuring timely detection and mitigation of potential threats.
Mitre Att&ck Matrix	An ATT&CK chart, a heatmap describing the attacks carried out in your system using attack tactics, techniques and procedures defined by MITRE. It shows the count of each attack ID within its respective attack category, helping administrators enhance their security posture, prioritize defences, and improve incident response and threat analysis.

Continued on next page

Table 1 – continued from previous page

Widget Name	Description
Top Recurring Attacks	The top ten recurring attacks within your system, categorized by attack type and frequency, allowing administrators to quickly identify the most common and persistent threats. 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 ten users based on the number of distinct attack tactics they were associated with, providing insights into which users are most frequently targeted or involved in diverse attack activities.
Top Hosts in Attack	The top ten hosts based on the number of distinct attack tactics they were associated with, providing insights into which hosts are most frequently targeted or involved in diverse attack activities.

4.1.2 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** of *LP_Mitre Attack Analytics Overview*.
4. Click **Choose Repos**.

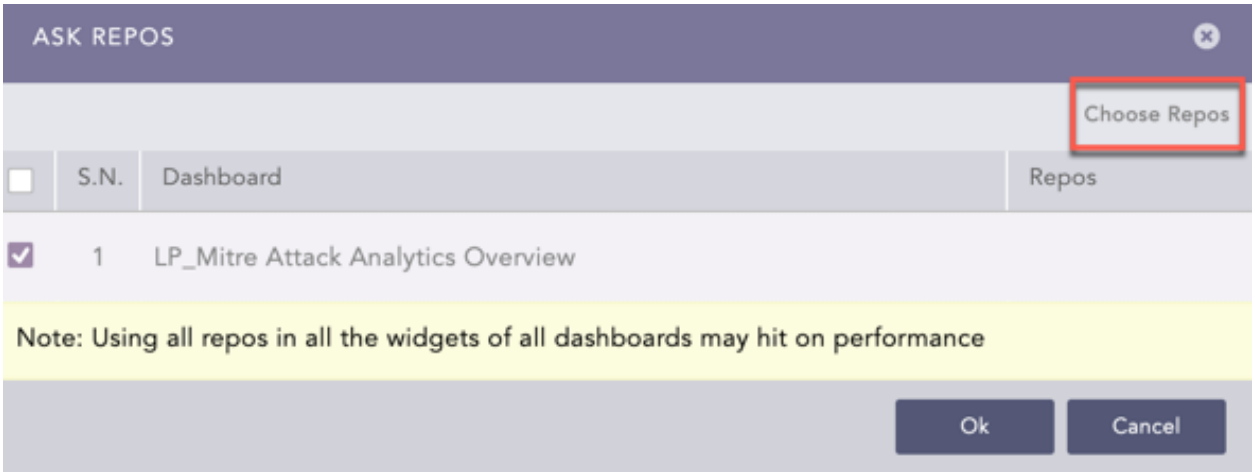

Fig. 1: Selecting Repos

5. Select the repo and click **Done**.

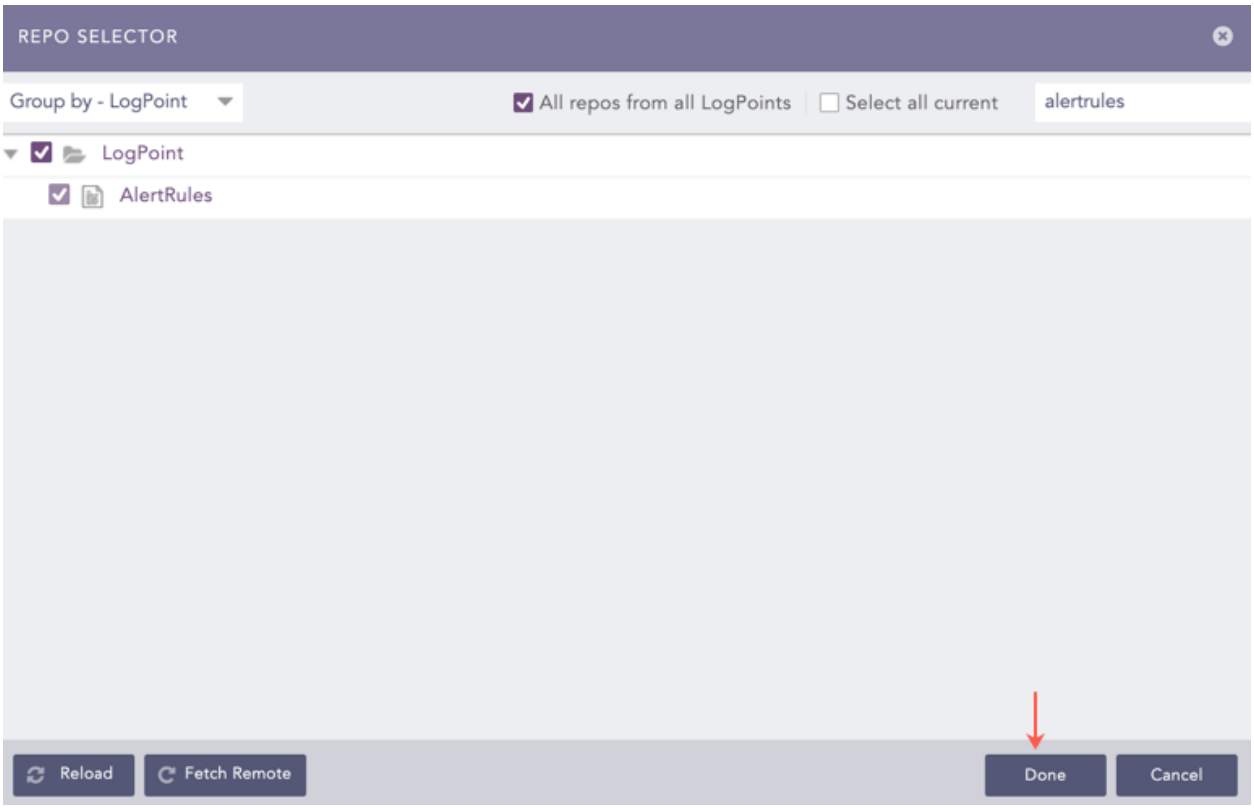

Fig. 2: Selecting Repos

6. Click **Ok**.

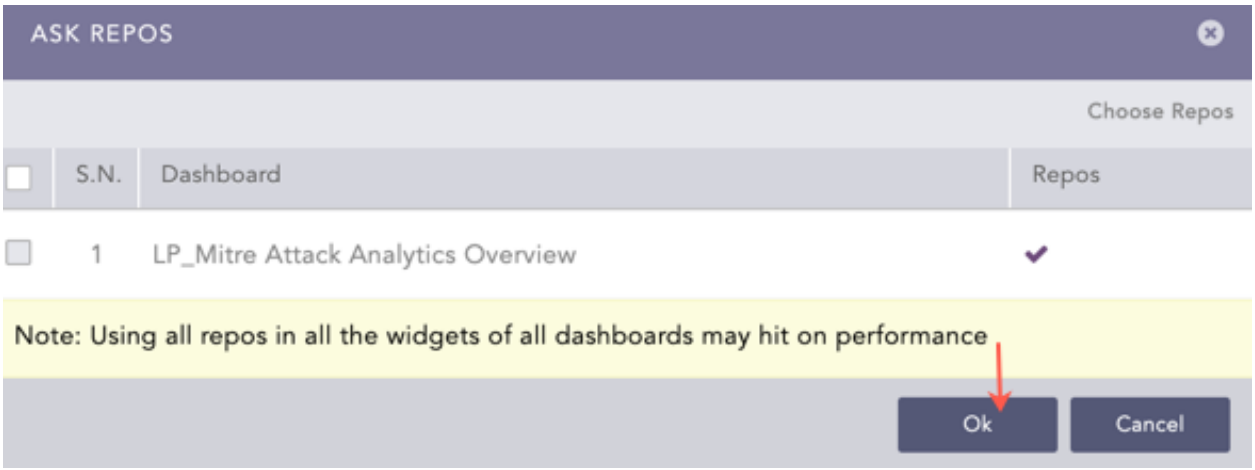

Fig. 3: Confirmation for Repo

You can find the Alert Rules dashboard under **Dashboards**.

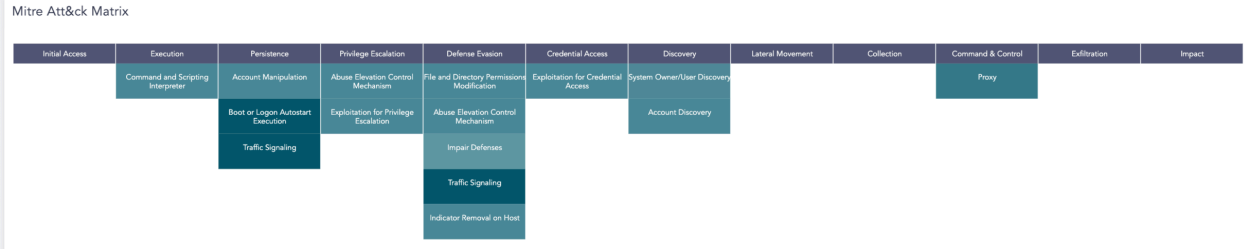

Fig. 4: Alert Rules Dashboard

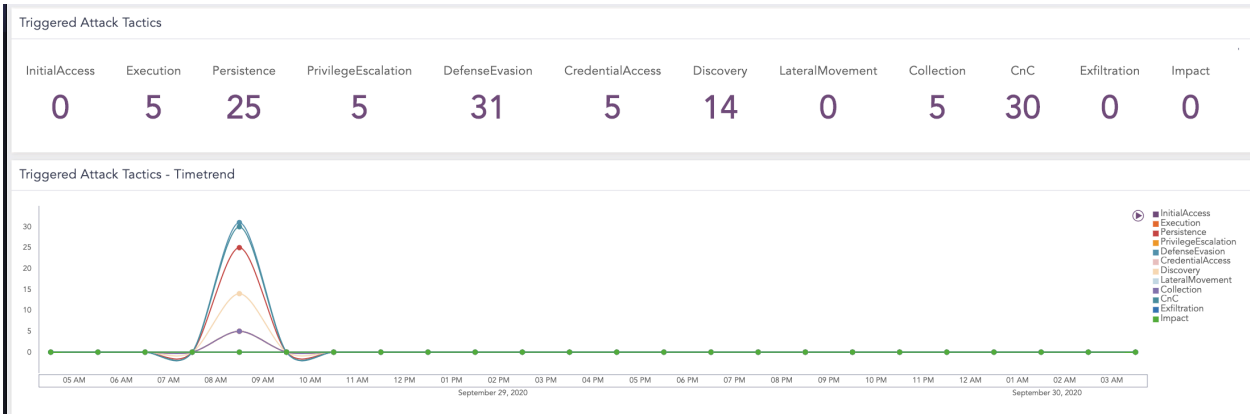

Fig. 5: Alert Rules Dashboard

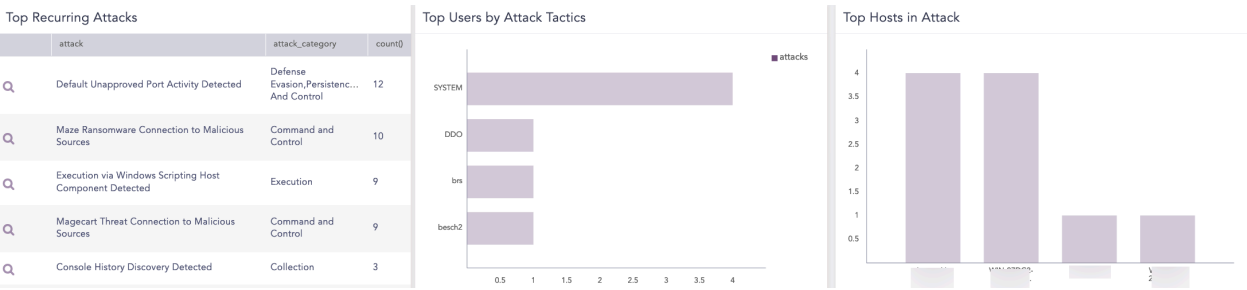

Fig. 6: Alert Rules Dashboard

4.2 Search Template

LP_Mitre Attack Analytics Overview: It stores the search queries that provides information on tactics triggered, attack tactics, recurring incidents, and attacks details.

4.2.1 Using the Salesforce Search Templates

1. Go to *Settings >> Knowledge Base* from the navigation bar and click **Search Templates**.

2. Select **VENDOR SEARCH TEMPLATES** from the drop-down, search and click **LP_Mitre Attack Analytics Overview**.

3. In **Update Parameters**, enter the required parameters.

    3.1 Select **Override widget time range** to set a time range for the search query.
    3.2 Select **REPOS** to choose repos which contains Alert Rules logs.
    3.3 Click **Update**.

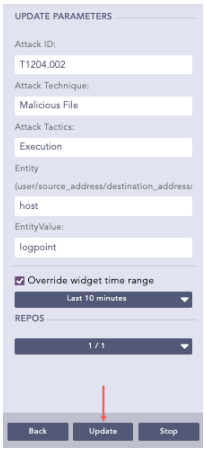

Fig. 7: Updating Salesforce Search Template

After updating, the widgets start displaying the result. Logpoint forwards you to **Search Template View** to access the dashboards of the search template.

CHAPTER

FIVE

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
- CHROME_VPN_EXTENSIONS
- 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
- EDR_PROCESS
- 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
- SUSPICIOUS_DRIVER
- 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*.