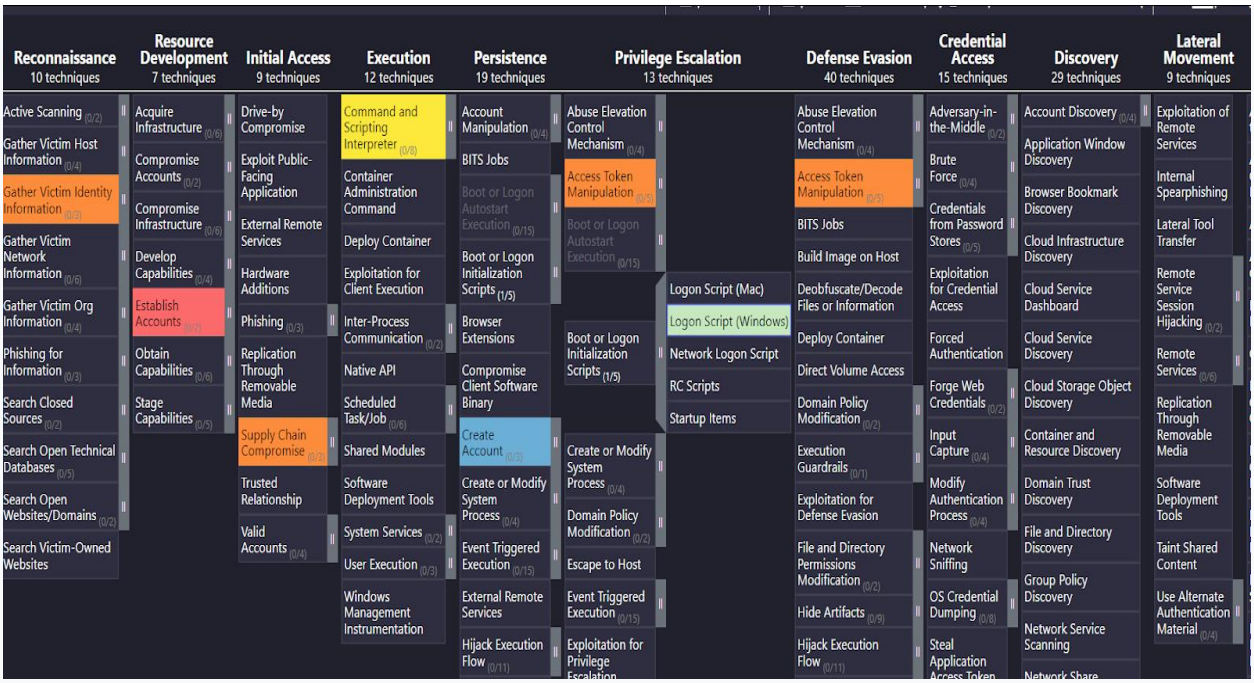

MITRE ATTACKS DETECTION RULES PART1

The MITRE ATT&CK Alerts For log point

Parastoo Razi

Suspicious Named Pipe Connection to Azure AD Connect Database

- **Trigger condition:** Named pipe connection to Azure AD Connect database from suspicious processes coming from command shells like PowerShell, which may indicate attackers attempting to dump plaintext credentials of AD and Azure AD connector account using tools such as AADInternals is detected.
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
- ```
  norm_id=WindowsSysmon label=Pipe label=Connect pipe="*\tsql\query" -image IN ["*\Program Files\Microsoft Azure AD Sync\Bin\miiserver.exe", "*\Tools\Binn\SqlCmd.exe"]
  ```

Suspicious Driver Loaded
  ```

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

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

AADInternals PowerShell Cmdlet Execution

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

```
norm_id=WinServer event_source="Microsoft-Windows-PowerShell" event_id=4104 sc
ript_block IN AADINTERNALS_CMDLETS
```

Suspicious Scheduled Task Creation via Masqueraded XML File

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

```
label=create label="process" "process"="*\schtasks.exe" command IN ["*/create*
", "*-create*"]  command IN ["*/xml*","*-xml*"] (-integrity_level=system OR -i
ntegrity_label=*system*) -command = *.xml* ((-parent_process IN ["*:\ProgramDa
ta\OEM\UpgradeTool\CareCenter_*\BUnzip\Setup_msi.exe", "*:\Program Files\Axis C
ommunications\AXIS Camera Station\SetupActions.exe", "*:\Program Files\Axis Co
mmunications\AXIS Device Manager\AdmSetupActions.exe", "*:\Program Files (x86)
\Zemana\AntiMalware\AntiMalware.exe", "*:\Program Files\Dell\SupportAssist\pcd
rcui.exe" ] ) OR (-parent_process = "*\rundll32.exe" command = "*:\\WINDOWS\\I
nstaller\\MSI*.tmp,zzzzInvokeManagedCustomActionOutOfProc" ))
```

Suspicious Microsoft Equation Editor Child Process

- **Trigger condition:** A suspicious child process of Microsoft's equation editor is detected as a sign of possible exploitation of CVE-2017-11882. CVE-2017-11882 is a vulnerability in Microsoft Office's Equation Editor component.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Exploitation for Client Execution
- **ATT&CK ID:** T1203
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
-
```
label="Process" label=Create parent_process="*\EQNEDT32.exe" -"process" IN ["C:\Windows\System32\WerFault.exe", "C:\Windows\SysWOW64\WerFault.exe"]
```

Windows Error Process Masquerading

- **Trigger condition:** Suspicious Windows error reporting process behavior, where network connections are made after execution is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Masquerading
- **ATT&CK ID:** T1036
- **Minimum Log Source Requirement:** Windows Sysmon
-
```
[norm_id=WindowsSysmon event_id=1 "process" IN ["*\WerMgr.exe", "*\WerFault.exe"]] as s1 followed by [norm_id=WindowsSysmon event_id=3 "process" IN ["*\WerMgr.exe", "*\WerFault.exe"]] as s2 within 1 minute on s1.process_guid=s2.process_guid | rename s1.host as host, s1.user as user, s1.domain as domain, s1.image as image, s2.destination_address as destination_address, s2.destination_port as destination_port
```

Bypass UAC via CMSTP Detected

- **Trigger condition:** Child processes of automatically elevated instances of Microsoft Connection Manager Profile Installer (*cmstp.exe*) are detected.
- **ATT&CK Category:** Privilege Escalation, Defense Evasion
- **ATT&CK Tag:** CMSTP, Abuse Elevation Control Mechanism, Bypass User Account Control
- **ATT&CK ID:** T1218.003, T1548, T1548.002
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**
-
```
label="Process" label=Create "process"="*\cmstp.exe" command IN ["*/s*", "*/au*", "*/ni*", "*-s*", "*-au*", "*-ni*"] -user IN EXCLUDED_USERS
```

Application Whitelisting Bypass via Dxcap Detected

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

- **Query:**

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

Suspicious WMIC XSL Script Execution

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

```
[norm_id=WindowsSysmon event_id=1 file="wmic.exe" command IN ["* format*:*", "*/format*:*", "*-format*:*"] -command IN ["*format:list*", "*format:table*", "*format:htable", "*format: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.image as image, s1.host as host, s1.domain as domain, s1.command as command, s2.image as loaded_image
```

Suspicious File Execution via MSHTA

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

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

Regsvr32 Anomalous Activity Detected

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

```
norm_id=WindowsSysmon event_id=1 ((image="*\regsvr32.exe" command="*\Temp\*") OR (image="*\regsvr32.exe" parent_image="*\powershell.exe") OR (image="*\regsvr32.exe" parent_image="*\cmd.exe") OR (image="*\regsvr32.exe" command IN ["*/i:
```

```
http* scrobj.dll", "*/i:ftp* scrobj.dll"]) OR (image="*\wscript.exe" parent_im
age="*\regsvr32.exe") OR (image="*\EXCEL.EXE" command="*..\..\..\Windows\Syste
m32\regsvr32.exe *")) -user IN EXCLUDED_USERS
```

Remote File Execution via MSIEXEC

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

```
norm_id=WindowsSysmon event_id=1 file="msiexec.exe" command="*http://*" comman
d IN ["*/i*", "*-i*"] command IN ["*/q*", "*/quiet*", "*/qn*", "*-q*", "*-quie
t*", "*-qn*"] -(parent_image="*setup*") -integrity_level=SYSTEM
```

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 Lt
d*","*3CX Desktop App*"] file_version IN ["*18.12.407*","18.12.416*"]
```

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"]
```

Suspicious Files Designated as System Files Detected

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

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

UAC Bypass Attempt via Windows Directory Masquerading

- **Trigger condition:** User Account Control (UAC) bypass attempt is detected by masquerading as a Microsoft trusted Windows directory. Masquerading is a technique where adversaries manipulate features of their artifacts to make them appear legitimate or benign to users and security tools.
- **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, Windows
- **Query:**

```
label="Process" label=Create integrity_level=High "process" IN ["C:\Windows \S
ystem32\*.exe", "C:\Windows \SysWOW64\*.exe", "C:\ Windows*\System32\*.exe", "
C:\ Windows*\SysWOW64\*.exe"]
```

Bypass User Account Control using Registry

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

```
norm_id=WindowsSysmon (event_id=12 or event_id=13 or event_id=14) (target_obje
ct="*\mscfile\shell\open\command\*" or target_object="*\ms-settings\shell\open
\command\*") -user IN EXCLUDED_USERS
```

LSASS Process Access by Mimikatz

- **Trigger condition:** Process access to LSASS is detected, which is typical for Mimikatz *(0x1000 PROCESS_QUERY_LIMITED_INFORMATION, 0x0400 PROCESS_QUERY_INFORMATION "only old versions", 0x0010 PROCESS_VM_READ)*.
- **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=10 image="C:\windows\system32\lsass.exe" access IN ["0x1410", "0x1010"] -user IN EXCLUDED_USERS
```

UAC Bypass via Sdclt Detected

- **Trigger condition:** User Account Control (UAC) bypass methods via changes to *HKCU:\Software\Classes\exefile\shell\runas\command\isolatedCommand* and *HKCU:\Software\Classes\Folder\shell\open\command*.
- **ATT&CK Category:** Defense Evasion, Privilege Escalation
- **ATT&CK Tag:** Bypass User Account Control
- **ATT&CK ID:** T1548, T1548.002
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id="13" target_object IN ["HKU\*Classes\exefile\shell\runas\command\isolatedCommand", "HKU\*Classes\Folder\shell\open\command"]
```

Unsigned Image Loaded Into LSASS Process

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

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

Usage of Sysinternals Tools Detected

- **Trigger condition:** The use of Sysinternals tools is detected 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
- **Query:**
- `(event_id="13" target_object="*\EulaAccepted") OR (event_id="1" command="* -acceptEula*")`

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*')`

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`

Mitre - Initial Access - Valid Account - Unauthorized IP Access

- **Trigger condition:** A user login event is detected from unauthorized countries. For this alert to work, you must update the KNOWN_COUNTRY list with countries where login is denied.
- **ATT&CK Category:** Initial Access, Persistence, Privilege Escalation, Defense Evasion
- **ATT&CK Tag:** Valid Accounts
- **ATT&CK ID:** T1078
- **Minimum Log Source Requirement:** Windows
- **Query:**
- `label=User label=Login source_address=* | process geoip(source_address) as country | search -country IN KNOWN_COUNTRY`

Windows CryptoAPI Spoofing Vulnerability Detected

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

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

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 *"
```

Suspicious process related to Rundll32 Detected

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

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

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*"
```

Suspicious Execution of Gpscript Detected

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

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

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*"
```

ScreenSaver Registry Key Set Detected

- **Trigger condition:** A file name masqueraded as *.scr* extension ran via rundll32 with desk.cpl, 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=Registry label=Value label=Set "process"="*\rundll32.exe" detail="*.scr" -detail in ["*C:\Windows\system32\*","*C:\Windows\SysWOW64\*" ] target_object="*\Control Panel\Desktop\SCRNSAVE.EXE"
```

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\*"
```

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 (2)
- **ATT&CK ID:** T1574.002
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

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

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*"
```

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*"))`

Suspicious ConfigSecurityPolicy Execution Detected

- **Trigger condition:** A local file upload via ConfigSecurityPolicy binary to attack the control server is detected.
- **ATT&CK Category:** Exfiltration
- **ATT&CK Tag:** Exfiltration Over Web Service
- **ATT&CK ID:** T1567
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**
- `label="Process" label="Create" "process"="*\ConfigSecurityPolicy.exe" command IN ["*https://*","*http://*","*ftp://*"]`

C-Sharp Code Compilation Using Ilasm Detected

- **Trigger condition:** C# code is either compiled into executables or into DLL using Ilasm utility.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Trusted Developer Utilities Proxy Execution
- **ATT&CK ID:** T1127
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
- `label="Process" label="Create" ("process"="*\ilasm.exe" OR file="ilasm.exe")`

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*"`

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*"
```

Accessibility features - Process

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

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

Accessibility Features-Registry

- **Trigger condition:** An adversary establishes 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
```

Account Discovery Detected

- **Trigger condition:** Adversaries attempt to get a listing of accounts on a system or within an environment that can help them determine which accounts exist to aid in follow-on behavior.
- **ATT&CK Category:** -
- **ATT&CK Tag:** Account Discovery, Local Account, Domain Account
- **ATT&CK ID:** T1087,T1087.001,T1087.002
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 (image="*net.exe" or image="*powershell.exe") (command="*net* user*" or command="*net* group*" or command="*net* localgroup*" or command="*cmdkey*\/list*" or command="*get-localuser*" or command="*get-l
```

```
ocalgroupmembers*" or command="*get-aduser*" or command="*query*user*") -user I
N EXCLUDED_USERS
```

Active Directory DLLs Loaded By Office Applications

- **Trigger condition:** Kerberos DLL or DSParse DLL loaded by the Office products like WinWord, Microsoft PowerPoint, Microsoft Excel, or Microsoft Outlook.
- **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*", "*\powerpn
t.exe*", "*\excel.exe*", "*\outlook.exe*"] image IN ["*\kerberos.dll*","*\dspa
rse.dll*"] -user IN EXCLUDED_USERS
```

DCSync detected

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

```
((norm_id=WinServer event_id=4662 access_mask="0x100" properties IN ["*1131f6a
a-9c07-11d1-f79f-00c04fc2dcd2*", "*1131f6ad-9c07-11d1-f79f-00c04fc2dcd2*", "*8
9e95b76-444d-4c62-991a-0facbeda640c*", "*Replicating Directory Changes All*"] -
user="*$" -user="MSOL_*") or (norm_id=WinServer event_id=4742
service="*GC/*"))-user IN EXCLUDED_USERS
```

Active Directory Replication User Backdoor

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

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

Active Directory Schema Change Detected

- **Trigger condition:** The directory service object is changed, created, moved, deleted, or restored.
- **ATT&CK Category:** Persistence, Privilege Escalation, Credential Access
- **ATT&CK Tag:** Create or Modify System Process, Windows Service, Exploitation for Credential Access, Exploitation for Privilege Escalation
- **ATT&CK ID:** T1212, T1068, T1543, T1543.003
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer* label=Directory label=Service label=Object (label=Change or label=Create or label=Move or label=Delete or label=Undelete) -user IN EXCLUDED_USERS
```

Activity Related to NTDS Domain Hash Retrieval

- **Trigger condition:** Suspicious commands related to an activity that uses volume shadow copy to steal and retrieve hashes from the *NTDS.dit* file remotely is detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** OS Credential Dumping, NTDS
- **ATT&CK ID:** T1003, T1003.003
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

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

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
```

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"] objec
t_name IN ["*-512", "*-502", "*-500", "*-505", "*-519", "*-520", "*-544", "*-5
51", "*-555", "*admin*"] -user IN EXCLUDED_USERS
```

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 (norm_id=WinServer event_id
=4738 -SidHistory IN ["-", "%%1793"])) -user IN EXCLUDED_USERS
```

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="Negot
iate" OR package="Negotiate") user="Admin-*" -user IN EXCLUDED_USERS | rename p
ackage as authentication_package
```

Adobe Flash Use-After-Free Vulnerability Detected

- **Trigger condition:** The exploitation of use-after-free vulnerability (CVE-2018-4878) in Adobe Flash is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** User Execution
- **ATT&CK ID:** T1204

- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
- `norm_id=WindowsSysmon label=Image label=Load source_image IN ["*winword.exe", "*excel.exe"] image='*Flash32*.ocx' -user IN EXCLUDED_USERS`

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*")`

Antivirus Exploitation Framework Detection

- **Trigger condition:** Antivirus's alert reports exploitation in a framework.
- **ATT&CK Category:** Execution, Command and Control
- **ATT&CK Tag:** Exploitation for Client Execution,Remote Access Tools
- **ATT&CK ID:** T1203,T1219
- **Minimum Log Source Requirement:** Antivirus
- **Query:**
- `signature IN ["*MeteTool*", "*MPreter*", "*Meterpreter*", "*Metasploit*", "*PowerSploit*", "*CobaltSrike*",  "*Swrort*", "*Rozena*", "*Backdoor.Cobalt*", "*Msfvenom*", "*armor*", "*Empire*" ,"*SilentTrinity*", "*Ntlmrelayx"]`

Antivirus Password Dumper Detected

- **Trigger condition:** Antivirus's alert reports a password dumper.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** OS Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
- `status IN ["*DumpCreds*", "*Mimikatz*", "*PWCrack*", "HTool/WCE", "*PSWtool*", "*PWDump*", "*SecurityTool*", "*PShlSpy*","*laZagne*"]`

Antivirus Web Shell Detected

- **Trigger condition:** Antivirus's alert reports a Web Shell.

- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Server Software Component, Web Shell
- **ATT&CK ID:** T1505, T1505.003
- **Minimum Log Source Requirement:** Antivirus
- **Query:**

```
signature IN ["PHP/Backdoor*", "JSP/Backdoor*", "ASP/Backdoor*", "Backdoor.PHP*", "Backdoor.JSP*", "Backdoor.ASP*", "*Webshell*"]
```

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>
```

AppCert DLLs Detected

- **Trigger condition:** Adversaries establish persistence and/or elevate privileges by executing malicious content triggered by AppCert DLLs loaded into processes.
- **ATT&CK Category:** Persistence, Privilege Escalation
- **ATT&CK Tag:** Event Triggered Execution, AppCert DLLs
- **ATT&CK ID:** T1546, T1546.009
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

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

Application Shimming - File Access Detected

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

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

Application Whitelisting Bypass via Bginfo Detected

- **Trigger condition:** Adversaries bypass the process and/or signature-based defenses by executing a VBscript code referenced within the *.bgi* file.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Signed Binary Proxy Execution
- **ATT&CK ID:** T1218
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 image="*\bginfo.exe" command="*/popup*" command="*/nolicprompt*" -user IN EXCLUDED_USERS
```

Application Whitelisting Bypass via DLL Loaded by odbcconf Detected

- **Trigger condition:** Adversaries bypass the process and/or signature-based defenses via *odbcconf.exe* execution to load DLL.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Signed Binary Proxy Execution, Odbcconf
- **ATT&CK ID:** T1218, T1218.008
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 ((image="*\odbcconf.exe" command IN ["*-f*", "*regsvr*"]) OR (parent_image="*\odbcconf.exe" image="*\rundll32.exe")) -user IN EXCLUDED_USERS
```

Application Whitelisting Bypass via Dnx Detected

- **Trigger condition:** Adversaries bypass the process and/or signature-based defenses by execution of C# code located in the *consoleapp* folder.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Signed Binary Proxy Execution
- **ATT&CK ID:** T1218
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

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

Audio Capture Detected

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

- **ATT&CK ID:** T1123
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

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

Authentication Package Detected

- **Trigger Condition:** The LSA process is loaded by services other than lssac, svchos, msiexec, and services. 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
- **ATT&CK Tag:** Boot or Logon Autostart Execution, Authentication Package, Security Support Provider
- **ATT&CK ID:** T1547, T1547.002, T1547.005
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon (event_id=12 or event_id=13 or event_id=14) (target_object="*\SYSTEM\CurrentControlSet\Control\Lsa\*") -image in ["*C:\WINDOWS\system32\lsass.exe","*C:\Windows\system32\svchost.exe","*C:\Windows\system32\services.exe","C:\Windows\system32\msiexec.exe","C:\Windows\system32\Msiexec.exe"]
-user IN EXCLUDED_USERS
```

Autorun Keys Modification Detected

- **Trigger Condition:** Modification of autostart extensibility point (ASEP) in the registry is detected. ASEP allows a particular program to run automatically when a user logs into the system. Adversaries may achieve persistence by adding a program to a startup folder or referencing it with a Registry run key.
- **ATT&CK Category:** Persistence, Privilege Escalation
- **ATT&CK Tag:** T1547 - Boot or Logon Autostart Execution (2), T1547.001 - Registry Run Keys / Startup Folder (2)
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=13 target_object IN ["*\software\Microsoft\Windows\CurrentVersion\Run*", "*\software\Microsoft\Windows\CurrentVersion\RunOnce*", "*\software\Microsoft\Windows\CurrentVersion\RunOnceEx*", "*\software\Microsoft\Windows\CurrentVersion\RunServices*", "*\software\Microsoft\Windows\CurrentVersion\RunServicesOnce*", "*\software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit*", "*\software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell*", "*\software\Microsoft\Windows NT\CurrentVersion\Windows*", "*\software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders*"] -user IN EXCLUDED_USERS
```

Batch Scripting Detected

- **Trigger Condition:** Adversaries abuse command and script interpreters to execute commands, scripts or binaries.
- **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 file in ["*.bat", "*.cmd"] -user IN EXCLUDED_USERS
```

BITS Jobs - Network Detected

- **Trigger Condition:** The BITS job network connection is detected. An adversary abuses BITS jobs to execute or clean up after executing malicious payload.
- **ATT&CK Category:** Defense Evasion, Persistence
- **ATT&CK Tag:** BITS Jobs
- **ATT&CK ID:** T1197
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=3 image="*bitsadmin.exe" -user IN EXCLUDED_USERS
```

BITS Jobs - Process Detected

- **Trigger Condition:** Creation of the BITS job process. An adversary abuses BITS jobs to execute or clean up after executing the malicious payload.
- **ATT&CK Category:** Defense Evasion, Persistence
- **ATT&CK Tag:** BITS Jobs
- **ATT&CK ID:** T1197
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 (image="*bitsamin.exe" or command="*Start-BitsTransfer*") -user IN EXCLUDED_USERS
```

Bloodhound and Sharphound Hack Tool Detected

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

```
norm_id=WindowsSysmon event_id=1 (image IN ["*\Bloodhound.exe*", "*\SharpHound.exe*"] OR command IN ["* -CollectionMethod All *", "*.exe -c All -d *", "*Invoke-Bloodhound*", "*Get-BloodHoundData*"] OR (command="* -JsonFolder *" comman
```

```
d="* -ZipFileName *") OR (command="* DCOnly *" command="* --NoSaveCache *")) -
user IN EXCLUDED_USERS
```

BlueMashroom DLL Load Detected

- **Trigger Condition:** DLL loading from AppData Local path described in BlueMashroom report is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Signed Binary Proxy Execution, Regsvr32
- **ATT&CK ID:** T1218, T1218.010
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

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

Browser Bookmark Discovery

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

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

CACTUSTORCH Remote Thread Creation Detected

- **Trigger Condition:** Creation of a remote thread from CACTUSTORCH.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Process Injection, Command and Scripting Interpreter
- **ATT&CK ID:** T1055, T1059
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=8 source_image IN ["*\System32\cscript.exe", "*
\System32\wscript.exe", "*\System32\mshta.exe", "*\winword.exe", "*\excel.exe"
] image="*\SysWOW64\*" -start_module=* -user IN EXCLUDED_USERS
```

Call to a Privileged Service Failed

- **Trigger Condition:** The privileged service call using *LsaRegisterLogonProcess* fails.
- **ATT&CK Category:** Privilege Escalation

- **ATT&CK Tag:** Valid Account
- **ATT&CK ID:** T1078
- **Minimum Log Source Requirement:** Windows
- **Query:**
- `norm_id=WinServer event_id=4673 service="LsaRegisterLogonProcess()" event_type="*Failure*" -user IN EXCLUDED_USERS`

Capture a Network Trace with netsh

- **Trigger Condition:** Network trace capture via *netsh.exe* trace functionality is detected.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Network Sniffing
- **ATT&CK ID:** T1040
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
- `norm_id=WindowsSysmon event_id=1 command="*netsh*" command="*trace*" command="*start*" -user IN EXCLUDED_USERS`

CEO Fraud - Possible Fraudulent Email Behavior

- **Trigger Condition:** An email received from a threat source in the internal network exhibits fraudulent behavior. For this alert to work, you must update the following:
    - HOME_DOMAIN, which is the list of selected domain names. For example, logpoint.com
    - MANAGERS, which is the list of selected managers and executives. For example, *Alice*
    - SERVER_ADDRESS, which is the list of trusted clients or servers from where the emails are received.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** Phishing
- **ATT&CK ID:** T1566, T1566.001
- **Minimum Log Source Requirement:** Exchange MT
- **Query:**
- `norm_id=ExchangeMT event_id=receive sender=* receiver IN HOME_DOMAIN original_client_address=* -original_client_address IN SERVER_ADDRESS | norm on sender <target_manager:all>@<domain:string> |`
- `norm on message_id @<original_domain:'.*'><:'\>'> | search target_manager IN MANAGERS`

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
```

Chafer Activity Detected

- **Trigger Condition:** The Chafer activity attributed to OilRig reported in Nyotron report in March 2018 is detected.
- **ATT&CK Category:** Execution, Persistence, Privilege Escalation
- **ATT&CK Tag:** Scheduled Task/Job, Scheduled Task
- **ATT&CK ID:** T1053, T1053.005
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WindowsSysmon event_id=1 (command="*Get-History*" or command="*AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt*" or command="*(Get-PSReadlineOption).HistorySavePath*") -user IN EXCLUDED_USERS
```

Change of Default File Association Detected

- **Trigger Condition:** A registry value is set to change the file association. Adversaries establish persistence by executing malicious content triggered by a file type association.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Event Triggered Execution, Change Default File Association
- **ATT&CK ID:** T1546, T1546.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

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

Citrix ADC VPN Directory Traversal Detected

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

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

Clear Command History

- **Trigger Condition:** Deletion of command history is detected. Adversaries delete or alter generated artifacts on a host system, including logs or captured files such as quarantined malware.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Indicator Removal on Host, Clear Command History
- **ATT&CK ID:** T1070, T1070.003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 (command="*rm (Get-PSReadlineOption).HistorySavePath*" or command="*del (Get-PSReadlineOption).HistorySavePath*" or command="*Set-PSReadlineOption -HistorySaveStyle SaveNothing*" or command="*Remove-Item (Get-PSReadlineOption).HistorySavePath*") -user IN EXCLUDED_USERS
```

Clearing of PowerShell Logs Detected

- **Trigger Condition:** Clearance of console history logs is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Indicator Removal on Host
- **ATT&CK ID:** T1070
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4103 (command_name="Remove-Item" OR command="Remove-Item") payload="*consolehost*history*" -user IN EXCLUDED_USERS | rename command_name as command
```

Clipboard Data Access Detected

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

```
norm_id=WindowsSysmon event_id=1 (image="*clip.exe" or command="*Get-Clipboard*") -user IN EXCLUDED_USERS
```

Clop Ransomware Emails Sent to Attacker

- **Trigger Condition:** Email communication is established to or from Clop Ransomware listed emails.
- **ATT&CK Category:** Exfiltration, Collection
- **ATT&CK Tag:** Exfiltration Over C2 Channel, Email Collection
- **ATT&CK ID:** T1041, T1114
- **Minimum Log Source Requirement:** Exchange MT
- **Query:**

- `(receiver in CLOP_RANSOMWARE_EMAILS OR sender in CLOP_RANSOMWARE_EMAILS) sender=* receiver=* (host=* OR source_host=*) | rename source_host as host`

Clop Ransomware Infected Host Detected

- **Trigger Condition:** Clop ransomware infected host is detected.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Data Encrypted for Impact
- **ATT&CK ID:** T1486
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
- `host=* hash=* hash IN CLOP_RANSOMWARE_HASHES`

Cmdkey Cached Credentials Recon Detected

- **Trigger Condition:** The usage of *cmdkey* to detect cached credentials.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
- `norm_id=WindowsSysmon event_id=1 image="*\cmdkey.exe" command="* /list *" -user IN EXCLUDED_USERS`

CMSTP Detected

- **Trigger Condition:** Adversary abuses CMSTP for proxy execution of malicious code. *CMSTP.exe* accepts an installation information file (INF) as a parameter and installs a service profile leveraged for remote access connections. Also, the adversary supplies *CMSTP.exe* with INF files infected with malicious commands.
- **ATT&CK Category:** Defense Evasion, Execution
- **ATT&CK Tag:** Signed Binary Proxy Execution, CMSTP
- **ATT&CK ID:** T1218, T1218.003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
- `norm_id=WindowsSysmon event_id=1 image="*CMSTP.exe" -user IN EXCLUDED_USERS`

CMSTP Execution Detected

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

```
(event_id=12 target_object="*\cmmgr32.exe*") OR (event_id=13 target_object="*\cmmgr32.exe*") OR (event_id=10 call_trace="*cmlua.dll*") OR (event_id=1 parent_image="*\cmstp.exe")
```

CMSTP UAC Bypass via COM Object Access

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

```
norm_id=WindowsSysmon event_id=1 parent_command="*\DllHost.exe" parent_command IN ["*{3E5FC7F9-9A51-4367-9063-A120244FBEC7}", "*{3E000D72-A845-4CD9-BD83-80C07C3B881F}"] -user IN EXCLUDED_USERS
```

CobaltStrike Process Injection Detected

- **Trigger Condition:** Creation of remote threat with specific characteristics that are typical for Cobalt Strike beacons.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Process Injection
- **ATT&CK ID:** T1055
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

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

Windows Command Line Execution with Suspicious URL and AppData Strings

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

- **Query:**

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

Compiled HTML File Detected

- **Trigger Condition:** Adversary abuses 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
```

Component Object Model Hijacking Detected

- **Trigger Condition:** Adversaries establish persistence by executing malicious content triggered by hijacked references to Component Object Model (COM) objects.
- **ATT&CK Category:** Defense Evasion, Persistence
- **ATT&CK Tag:** Inter-Process Communication, 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 or event_id=13 or event_id=14) target_object="*\Software\Classes\CLSID*" -user IN EXCLUDED_USERS
```

Connection to Hidden Cobra Source

- **Trigger Condition:** Hosts establish an outbound connection to Hidden Cobra sources.
- **ATT&CK Category:** Command and Control, Defense Evasion
- **ATT&CK Tag:** Command and Control, Defense Evasion
- **ATT&CK ID:** T1090, T1211
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

```
(source_address=* OR destination_address=*) destination_address in HIDDEN_COBRA_IPS | process dns(source_address) as host | process geoip(destination_address) as country
```

Console History Discovery Detected

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

```
norm_id=WindowsSysmon event_id=1 (command="*Get-History*" or command="*AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt*" or command="*(Get-PSReadlineOption).HistorySavePath*") -user IN EXCLUDED_USERS
```

Control Panel Items - Process Detected

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

```
norm_id=WindowsSysmon event_id=1 (command="*control \/name*" or command="*rundll32 shell32.dll, Control_RunDLL*") -user IN EXCLUDED_USERS
```

Control Panel Items - Registry Detected

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

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

Control Panel Items Detected

- **Trigger Condition:** Adversary attempts to use a control panel item (.cpl) outside the *System32* folder.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Signed Binary Proxy Execution, Control Panel Items
- **ATT&CK ID:** T1218, T1218.002
- **Minimum Log Source Requirement:** Windows Sysmon

- **Query:**

```
norm_id=WindowsSysmon event_id=1 command="*.cpl" -command IN ["*\System32\*", "*%System%*"] -user IN EXCLUDED_USERS
```

Copy from Admin Share Detected

- **Trigger Condition:** A copy command from a remote CorADMIN share is detected.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Remote Services, Remote File Copy
- **ATT&CK ID:** T1021, T1105
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 command IN ["*copy *\c*", "*copy*\ADMIN*"]-user IN EXCLUDED_USERS
```

Copying Sensitive Files with Credential Data

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

```
norm_id=WindowsSysmon event_id=1 ((image="*\esentutl.exe" command IN ["*vss*", "* /m *", "* /y *"]) OR command IN ["*\windows\ntds\ntds.dit*", "*\config\sam*", "*\config\security*", "*\config\system *", "*\repair\sam*", "*\repair\system*", "*\repair\security*", "*\config\RegBack\sam*", "*\config\RegBack\system*", "*\config\RegBack\security*"]) -user IN EXCLUDED_USERS
```

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>
```

CrackMapExecWin Detected

- **Trigger Condition:** CrackMapExecWin activity as described by NCSC is detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 image IN ["*\crackmapexec.exe"] -user IN EXCLUDED_USERS
```

CreateMiniDump Hacktool Detected

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

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

CreateRemoteThread API and LoadLibrary

- **Trigger Condition:** The use of CreateRemoteThread API and LoadLibrary function to inject DLL into a process is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Process Injection
- **ATT&CK ID:** T1055
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

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

Command Obfuscation in Command Prompt

- **Trigger Condition:** Adversaries abuse the Windows command shell for the execution of commands, scripts, or binaries.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Command and Scripting Interpreter, Windows Command Shell
- **ATT&CK ID:** T1059, T1059.003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 parent_image='*cmd.exe' parent_command IN ['*^*^*^*^*', '*set*=*call*%*%*','*s^*e^*t*']
```

Command Obfuscation via Character Insertion

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

```
norm_id=WindowsSysmon event_id=1 parent_image='*cmd.exe' parent_command='cmd*/c*' | norm on parent_command <command_match:'[^\w](s\^+e\^*t|s\^*e\^+t)[^\w]'> | search command_match=*
```

Command Obfuscation via Environment Variable Concatenation Reassembly

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

```
norm_id=WindowsSysmon event_id=1 parent_image='*cmd.exe' parent_command='cmd*/c*' | norm on parent_command <command_match:'%[^%]+%{4}'> | search command_match=*
```

Credential Access via Input Prompt Detected

- **Trigger Condition:** Adversary captures user input to obtain credentials or collect information via Input Prompt.
- **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
- **Query:**

```
norm_id=WinServer event_id=4104 (scriptblocktext="*UI.prompt*credential*" OR script_block="*UI.prompt*credential*") -user IN EXCLUDED_USERS | rename scriptblocktext as script_block
```

Credential Dump Tools Dropped Files Detected

- **Trigger Condition:** Creation of files with a well-known filename (i.e., parts of credential dump software or files produced by them) is detected.
- **ATT&CK Category:** Credential Access

- **ATT&CK Tag:** Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

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

Credential Dumping - Process Creation

- **Trigger Condition:** An adversary attempts to dump credentials for obtaining account login and credential material using different commands like *ntdsutil*, *procdump*, *wce*, or *gsecdump*, in the form of a hash or a clear text password from operating systems and software.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 (command="*Invoke-Mimikatz -DumpCreds*" or command="*gsecdump -a*" or command="*wce -o*" or command="*procdump -ma lsass.exe" or command="*ntdsutil*ac i ntds*ifm*create full*") -user IN EXCLUDED_USERS
```

Credential Dumping - Process Access

- **Trigger Condition:** An adversary attempts to dump credentials for obtaining account login and credential material using different commands like *ntdsutil*, *procdump*, *wce*, or *gsecdump*, in the form of a hash or a clear text password from operating systems and software.
- **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=10 target_image="*C:\Windows\system32\lsass.exe" (access="*0x1010*" or access="*0x1410*" or access="*0x147a*" or access="*0x143a*") call_trace="*C:\Windows\SYSTEM32\ntdll.dll" or call_trace="*C:\Windows\system32\KERNELBASE.dll" or call_trace="*|UNKNOWN(*)" -user IN EXCLUDED_USERS
```

Credential Dumping - Registry Save

- **Trigger Condition:** Credential dumping activities is detected. Adversary attempts to dump credentials for obtaining account login and credential material exploiting registries, generally in the form of a hash or a clear text password from operating

systems and software using different commands like *ntdsutil*, *procdump*, *wce* or *gsecdump*.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label="create" "process"="*\reg.exe" command IN ["*save*HKLM\sam*", "*save*HKLM\system*"] -user IN EXCLUDED_USERS
```

Credential Dumping with ImageLoad Detected

- **Trigger Condition:** Adversaries dump credentials to obtain account login and credential material using *dll* images.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Credential Dumping
- **ATT&CK ID:** T1003, T1003.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=7 (image="*C:\Windows\System32\samlib.dll*" or image="*C:\Windows\System32\WinSCard.dll*" or image="*C:\Windows\System32\cryptdll.dll*" or image="*C:\Windows\System32\hid.dll*" or image="*C:\Windows\System32\vaultcli.dll*") (image!="*\Sysmon.exe" or image!="*\svchost.exe" or image!="*\logonui.exe") -user IN EXCLUDED_USERS
```

Credentials Access in Files Detected

- **Trigger Condition:** Adversaries searching for files containing insecurely stored credentials in local file systems and remote file shares are detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Unsecured Credentials, Credentials in Files
- **ATT&CK ID:** T1552, T1552.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 (command="*findstr* /si pass*" or command="*select-string -Pattern pass*" or command="*list vdir*/text:password*") -user IN EXCLUDED_USERS
```

Credentials in Registry Detected

- **Trigger Condition:** Adversaries search registry of compromised systems to 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

- **Query:**

```
norm_id=WindowsSysmon event_id=1 (command="*reg query HKLM \/f password \/t REG_SZ \/s*" or command="*reg query HKCU \/f password \/t REG_SZ \/s*" or command="*Get-UnattendedInstallFile*" or command="*Get-Webconfig*" or command="*Get-ApplicationHost*" or command="*Get-SiteListPassword*" or command="*Get-CachedGPPPassword*" or command="*Get-RegistryAutoLogon*") -user IN EXCLUDED_USERS
```

Curl Start Combination Detected

- **Trigger Condition:** Adversaries attempt to use curl to download payloads remotely and execute them. Windows 10 build 17063 and later includes *Curl* by default.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Signed Binary Proxy Execution
- **ATT&CK ID:** T1218
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 command="*curl* start *" -user IN EXCLUDED_USERS
```

CVE-2019-0708 RDP RCE Vulnerability Detected

- **Trigger Condition:** The use of a scanner by zerosum 0x0 discovers targets vulnerable to CVE-2019-0708 RDP RCE known as BlueKeep.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Exploitation of Remote Services
- **ATT&CK ID:** T1210
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4625 user="AAAAAAA" -user IN EXCLUDED_USERS
```

Data Compression Detected in Windows

- **Trigger Condition:** Adversary compresses and/or encrypts data that is collected before exfiltration is detected using PowerShell or RAR.
- **ATT&CK Category:** Collection
- **ATT&CK Tag:** Archive Collected Data
- **ATT&CK ID:** T1560
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label=Create label="Process" ("process"="*/powershell.exe" command="*-Recurse Compress-Archive*") or ("process"="*/rar.exe" command="*rar*a*") -user IN EXCLUDED_USERS
```

Data Staging Process Detected in Windows

- **Trigger Condition:** Adversaries attempt to stage collected data in a central location or directory before exfiltration is detected.
- **ATT&CK Category:** Collection
- **ATT&CK Tag:** Data Staged
- **ATT&CK ID:** T1074
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 ((command="*DownloadString" command="*Net.WebClient*") or (command="*New-Object" command="*IEX*")) -user IN EXCLUDED_USERS
```

Default Accepted Traffic From Bad IP

- **Trigger Condition:** A connection is allowed from known bad IP. For this alert to work, you must update the list ALERT_BAD_IP.
- **ATT&CK Category:** Command and Control, Initial Access
- **ATT&CK Tag:** Proxy, External Remote Services
- **ATT&CK ID:** T1090, T1133
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

```
label=Connection label=Allow source_address IN ALERT_BAD_IP
```

Default Account Created but Password Not Changed

- **Trigger Condition:** Creation of a new account with a default password and the password is not changed within 24 hours, is detected.
- **ATT&CK Category:** Defense Evasion, Persistence, Privilege Escalation, Initial Access
- **ATT&CK Tag:** Valid Accounts, Account Manipulation, Create Account
- **ATT&CK ID:** T1078, T1098, T1136
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
[label=User label=Create label=Account] as s1 left join [label=User label=Password (label=Change OR label=Reset)] as s2 on s1.target_user=s2.user | search -s2.user=* | rename s1.target_user as User, s1.log_ts as UserCreated_ts | process current_time(a) as time_ts | chart max((time_ts - UserCreated_ts)/60/60) as Duration by User, UserCreated_ts | search Duration>24
```

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
```

Default Audit Policy Changed

- **Trigger Condition:** An audit policy is changed in the system.
- **ATT&CK Category:** Defense Evasion, Privilege Escalation
- **ATT&CK Tag:** Domain Policy Modification, Group Policy Modification
- **ATT&CK ID:** T1484, T1484.001
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
label=Audit label=Policy label=Change
```

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
```

Default Blocked Outbound Traffic followed by Allowed Event

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

```
[norm_id=*firewall or norm_id=*IDS label=Block or label=Deny label=Connection source_address IN HOMENET -destination_address IN HOMENET] as s1 followed by [n
```

```
orm_id=*firewall label=Allow label=Connection source_address IN HOMENET -desti
nation_address IN HOMENET]
```
- ```
  as s2 on s1.source_address=s2.source_address | rename s1.source_address as sou
  rce
  ```

Default Brute Force Attack Attempt - Multiple Unique Sources

- **Trigger Condition:** Failed login attempts from the same user using multiple sources. The default value for multiple unique sources is five.
- **ATT&CK Category:** Credential Access, Privilege Escalation, Defense Evasion
- **ATT&CK Tag:** Brute Force, Forced Authentication, Valid Accounts
- **ATT&CK ID:** T1110, T1187, T1078
- **Minimum Log Source Requirement:** Windows
- **Query:**
- ```
  label=User label=Login label=Fail | rename target_user as user | chart distinc
  t_count(source_address) as DC by user | search DC>5
  ```

Default Brute Force Attack Attempt - Multiple Unique Users

- **Trigger Condition:** Multiple user authentication fails from the same source within ten minutes. The default value for unique multiple users is five.
- **ATT&CK Category:** Credential Access, Initial Access, Persistence, Privilege Escalation, Defense Evasion
- **ATT&CK Tag:** Brute Force, Forced Authentication, Valid Accounts
- **ATT&CK ID:** T1110, T1187, T1078
- **Minimum Log Source Requirement:** Windows
- **Query:**
- ```
  label=User label=Login label=Fail source_address=* -target_user=*$| rename tar
  get_user as user | chart distinct_count(user) as DC by source_address | search
  DC>5
  ```

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, Initial Access, Persistence, Privilege Escalation, Defense Evasion
- **ATT&CK Tag:** Brute Force, Forced Authentication, Valid Accounts
- **ATT&CK ID:** T1110, T1187, T1078
- **Minimum Log Source Requirement:** Windows
- **Query:**
- ```
  [label=User label=Login label=Fail -target_user=*$ | rename target_user as use
  r | chart count() as cnt by user | search cnt > 5 ] as s1 followed by [label=U
  ```

```
ser label=Login label=Successful | rename target_user as user] as s2 on s1.use
r = s2.user | rename s2.user as User
```

Default Connection Attempts on Closed Port

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

```
label=Connection -destination_port IN ALERT_OPEN_PORTS source_address=* destin
ation_port=*
```

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
```

Default Device Stopped Sending Logs for Half an Hour

- **Trigger Condition:** A device has not sent logs for more than half an hour. You can customize the time according to your need.
- **ATT&CK Category:** Impact, Defense Evasion
- **ATT&CK Tag:** Service Stop, Data Destruction, Indicator Removal on Host
- **ATT&CK ID:** T1489, T1485, T1070
- **Minimum Log Source Requirement:** All the log sources
- **Query:**

```
| chart max(col_ts) as max_time_ts by device_ip | process current_time(a) as t
ime | chart max(time-max_time_ts) as elapsed_time by max_time_ts, device_ip | s
earch elapsed_time>1800
```

Default DNS Tunneling Detection - Data Transfer Size

- **Trigger Condition:** The size of data transmitted using the Application Layer Protocol and DNS port is greater than 10MB in five minutes.
- **ATT&CK Category:** Command and Control, Exfiltration
- **ATT&CK Tag:** Application Layer Protocol, DNS, Data Transfer Size Limits

- **ATT&CK ID:** T1071, T1071.004, T1030
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

```
destination_port=53 source_address IN HOMENET -destination_address IN HOMENET | chart sum(datasize) as DNSBYTES by source_address | search DNSBYTES > 10000000
```

Default DNS Tunneling Detection - Multiple domains

- **Trigger Condition:** A source address with queries for more than 50 domains are detected.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Application Layer Protocol, DNS, Dynamic Resolution, Domain Generation Algorithms, Proxy, Domain Fronting
- **ATT&CK ID:** T1071, T1071.004, T1568, T1568.002, T1090, T1090.004
- **Minimum Log Source Requirement:** Webserver, Firewall
- **Query:**

```
norm_id=* (url=* OR domain=*) | process domain(url) as domain | chart distinct_count(domain) as DomainCount by source_address | search DomainCount > 50
```

Default DNS Tunneling Detection - Multiple Subdomains

- **Trigger Condition:** Domains with more than ten subdomains from a single source address are detected.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Application Layer Protocol, DNS, Dynamic Resolution, Domain Generation Algorithms, Proxy, Domain Fronting
- **ATT&CK ID:** T1071, T1071.004, T1568, T1568.002, T1090, T1090.004
- **Minimum Log Source Requirement:** Webserver, Firewall
- **Query:**

```
norm_id=* (url=* OR domain=*) | process domain(url) as domain | norm on domain <subdomain:.*><:'\.'><main_domain:'[a-z0-9]+.\w{3}'> | search subdomain=* | chart distinct_count(subdomain) as uniqueSubdomain by main_domain, source_address |search uniqueSubdomain>10
```

Default DNS Tunneling Detection - Query Size

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

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

Default Excessive Authentication Failures

- **Trigger Condition:** More than 100 authentication failures of a user within ten minutes is 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:**
- `label=Fail label=Authentication -user=*$| chart count() as cnt by user | search cnt>100`

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]`

Default Excessive HTTP Errors

- **Trigger Condition:** 20 or more unique HTTP errors are detected.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Network Denial of Service
- **ATT&CK ID:** T1498
- **Minimum Log Source Requirement:** Firewall, IDS/IPS, Webserver
- **Query:**
- `norm_id=* status_code IN HTTP_ERROR | chart distinct_count(status_code) as cnt by host, source_address, norm_id | search cnt>20`

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
  ```

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
  ```

Default High Unique DNS Traffic

- **Trigger Condition:** Application Layer Protocol and DNS traffic event greater than 50 is detected.
- **ATT&CK Category:** Command And Control
- **ATT&CK Tag:** Application Layer Protocol, DNS
- **ATT&CK ID:** T1071, T1071.004
- **Minimum Log Source Requirement:** Firewall, IDS/IPS, Webserver
- **Query:**
- ```
  destination_port=53 source_address=* | chart count() as Event by source_address | search Event>50
  ```

Default High Unique SMTP Traffic

- **Trigger Condition:** More than 50 SMTP traffics from the same source within a minute is detected.
- **ATT&CK Category:** Command And Control
- **ATT&CK Tag:** Application Layer Protocol, Mail Protocols
- **ATT&CK ID:** T1071, T1071.003
- **Minimum Log Source Requirement:** Firewall, IDS/IPS, Webserver
- **Query:**
- ```
  source_address=* destination_port=25 | chart count() as Event by source_address | search Event>50
  ```

Default High Unique Web-Server traffic

- **Trigger Condition:** More than 50 web server traffics from the same source within a minute is detected.
- **ATT&CK Category:** Command And Control
- **ATT&CK Tag:** Application Layer Protocol, Web Protocols
- **ATT&CK ID:** T1071, T1071.001
- **Minimum Log Source Requirement:** Firewall, IDS/IPS, Webserver
- **Query:**

```
source_address=* destination_port=80 | chart count() as Event by source_address | search Event>50
```

Default Inbound Connection with Non-Whitelist Country

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

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

Default Inbound Queries Denied by Firewalls

- **Trigger Condition:** A firewall denies more than 100 inbound connections within five minutes.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Network Denial of Service
- **ATT&CK ID:** T1498
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

```
label=Connection label=Deny -source_address IN HOMENET destination_address in HOMENET | chart count() as Event by source_address, destination_address | search Event>100
```

Default Inbound RDP Connection

- **Trigger Condition:** Inbound RDP traffic events on destination port 3389 is detected.
- **ATT&CK Category:** Lateral Movement, Command And Control
- **ATT&CK Tag:** Remote Services, Application Layer Protocol
- **ATT&CK ID:** T1021, T1071

- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**
- `label=Connection -source_address IN HOMENET destination_address in HOMENET destination_port=3389`

Default Inbound SMB Connection

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

Default Inbound SMTP Connection

- **Trigger Condition:** Inbound SMTP traffic event on destination ports 25, 456, 587, 2525, and 2526 is detected.
- **ATT&CK Category:** Command And Control
- **ATT&CK Tag:** Application Layer Protocol
- **ATT&CK ID:** T1071
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**
- `label=Connection -source_address IN HOMENET destination_address in HOMENET destination_port in [25,465,587,2525,2526]`

Default Inbound SSH Connection

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

Default Internal Attack

- **Trigger Condition:** More than ten attack patterns from a home network are 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:** Firewall, IDS/IPS
- **Query:**

```
label=Attack -label=Deny source_address IN HOMENET | chart count() as Event by source_address, destination_address | search Event>10
```

Default Internal Virus Worm Outburst

- **Trigger Condition:** Ten or more viruses in a host is detected within an hour.
- **ATT&CK Category:** Impact, Defense Evasion
- **ATT&CK Tag:** Network Denial of Service, Endpoint Denial of Service
- **ATT&CK ID:** T1021, T1071
- **Minimum Log Source Requirement:** Antivirus
- **Query:**

```
(label=Worm OR label=Virus OR label=Malware) source_address IN HOMENET malware=* | chart distinct_count(malware) as Virus by source_address | search Virus>10
```

Default IRC connection

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

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

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
```

Default Malware Detected in Various Machines

- **Trigger Condition:** The same malware or virus is detected on multiple hosts.
- **ATT&CK Category:** Discovery, Defense Evasion
- **ATT&CK Tag:** Network Service Scanning, Exploitation for Defense Evasion, Software Discovery, Security Software Discovery, Impair Defenses,Impair Defenses, Disable or Modify Tools
- **ATT&CK ID:** T1046, T1211, T1518, T1518.001, T1562, T1562.001
- **Minimum Log Source Requirement:** Antivirus
- **Query:**

```
(label=Virus OR label=Malware ) (label=Detect OR label=Find) source_address=* malware=* | chart distinct_count(source_address) as Event by malware | search Event>1
```

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
```

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=*
```

Default Memory Usage Status

- **Trigger Condition:** The memory usage exceeds 90% of the total memory available.
- **ATT&CK Category:** Collection
- **ATT&CK Tag:** Automated Collection
- **ATT&CK ID:** T1119
- **Minimum Log Source Requirement:** LogPoint
- **Query:**

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

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)
```

Default Outbound Connection with Non-Whitelist Country

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

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

Default Outbound Traffic from Unusual Source

- **Trigger Condition:** Outbound traffic is detected from an unusual source. For this alert to work, you must update the list

ALERT_UNUSUAL_SOURCE with source addresses from which outbound connections are not established.

- **ATT&CK Category:** Command and Control, Exfiltration
- **ATT&CK Tag:** Proxy, Automated Exfiltration, Exfiltration Over C2 Channel
- **ATT&CK ID:** T1090, T1020, T1041
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

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

Default Port Scan Detected

- **Trigger Condition:** A source hits a destination on 50 different ports in five minutes.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Network Service Scanning
- **ATT&CK ID:** T1046
- **Minimum Log Source Requirement:** Firewall, IDS/IPS, Webserver
- **Query:**

```
destination_port=* | chart distinct_count(destination_port) as CNT by source_address, destination_address | search CNT>50
```

Default Possible Cross Site Scripting Attack Detected

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

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

Default Possible Network Performance Degradation Detected

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

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

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`

Default Possible Spamming Zombie

- **Trigger Condition:** Systems other than mail servers attempt to establish an outbound SMTP connection is detected. For this alert to work, you must update the list MAIL_SERVERS with possible mail servers to remove false positives. For example, *exchange*, *postfix*, and so on.
- **ATT&CK Category:** Command and Control, Impact
- **ATT&CK Tag:** Proxy, Application Layer Protocol, Network Denial of Service
- **ATT&CK ID:** T1090, T1071, T1498
- **Minimum Log Source Requirement:** All except Mail Server
- **Query:**
- `-norm_id IN MAIL_SERVERS destination_port IN ["25", "587"]`

Default Possible SQL Injection Attack

- **Trigger Condition:** SQL character injection in the input field of a web application is detected.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** Exploit Public-Facing Application
- **ATT&CK ID:** T1190
- **Minimum Log Source Requirement:** Firewall, IDS/IPS, Webserver
- **Query:**
- `norm_id=* url IN SQL_INJECTION_CHARACTER or resource IN SQL_INJECTION_CHARACTER | rename resource as url`

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]`

Default PowerSploit and Empire Schtasks Persistence

- **Trigger Condition:** Creation of a *schtask* via PowerSploit or Empire Default Configuration is detected.
- **ATT&CK Category:** Execution, Persistence, Privilege Escalation
- **ATT&CK Tag:** Scheduled Task/Job, Scheduled Task, Command and Scripting Interpreter, PowerShell + **ATT&CK ID:** T1053, T1053.005, T1059, T1059.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**
- `label="Process" label=Create parent_process="*\powershell.exe" "process"="*\schtasks.exe" command = "*/Create*" command = "*/SC*" (command in ["*ONLOGON*", "*DAILY*", "*ONIDLE*", "*Updater*"] command = "*/TN*" command = "*Updater*" command = "*/TR*"command = "*powershell*")`

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`

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
```

Default Suspicious DNS Queries with Higher Data Size

- **Trigger Condition:** DNS queries having data size greater than 2K signaling exfiltration of data via DNS.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Exfiltration Over Alternative Protocol, Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol
- **ATT&CK ID:** T1048, T1048.003
- **Minimum Log Source Requirement:** Firewall, IDS/IPS, Webserver
- **Query:**

```
datasize=* destination_port=53 datasize>2000
```

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")
```

Default TCP Port Scan

- **Trigger Condition:** 100 or more different TCP port sweep events are detected within five minutes from external sources.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Network Service Scanning
- **ATT&CK ID:** T1046
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

- `label=Connection label=Traffic -source_address IN HOMENET destination_address IN HOMENET protocol=TCP | chart distinct_count(destination_port) as DistinctPort by source_address, destination_address order by DistinctPort desc | search DistinctPort>100`

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]`

Default UDP Port Scan

- **Trigger Condition:** 100 or more different UDP port sweep events are detected within five minutes from an external source.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Network Service Scanning
- **ATT&CK ID:** T1046
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**
- `label=Connection label=Traffic -source_address IN HOMENET destination_address IN HOMENET protocol=UDP |`
- `chart distinct_count(destination_port) as DistinctPort by source_address, destination_address order by`
- `DistinctPort desc | search DistinctPort>100`

Default Unapproved Port Activity Detected

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

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
```

Detection of PowerShell Execution via DLL

- **Trigger Condition:** Command and Scripting Interpreter, PowerShell strings applied to *rundllas* observed in *PowerShdll.dll* is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, PowerShell
- **ATT&CK ID:** T1059, T1059.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 (image="*\rundll32.exe" OR message="*Windows-Hostprozess (Rundll32)*") command IN ["*Default.GetString*", "*FromBase64String*"] -user IN EXCLUDED_USERS
```

Devtoolslauncher Executes Specified Binary

- **Trigger Condition:** When adversaries attempt to bypass process and/or signature-based defenses by proxying execution of malicious content with signed binaries using devtoolslauncher (which is a part of VS/VScode installation) and LaunchForDeploy command.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Signed Binary Proxy Execution
- **ATT&CK ID:** T1218
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 image="*\devtoolslauncher.exe" command="*LaunchForDeploy*" -user IN EXCLUDED_USERS
```

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
```

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
```

DHCP Server Loaded the CallOut DLL

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

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

Direct Autorun Keys Modification Detected

- **Trigger Condition:** A modification to the direct autorun keys on a system (ASEP) in the registry using reg.exe. These keys are used to run programs or scripts automatically when a specific event occurs, such as when the system starts up or when a user logs in. Adversaries may use this technique to establish persistence on a system and ensure that their malware or other malicious programs are launched automatically whenever the system is restarted. They may also use it to evade detection by disguising their malware as a legitimate program automatically launched by the system. This alert requires registry auditing to be enabled. When an admin user modifies the keys, false positive alerts may be triggered.
- **ATT&CK Category:** Persistence

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

```
norm_id=WindowsSysmon event_id=1 image="*\reg.exe" command="*add*" command IN ["*\software\Microsoft\Windows\CurrentVersion\Run*", "*\software\Microsoft\Windows\CurrentVersion\RunOnce*", "*\software\Microsoft\Windows\CurrentVersion\RunOnceEx*", "*\software\Microsoft\Windows\CurrentVersion\RunServices*", "*\software\Microsoft\Windows\CurrentVersion\RunServicesOnce*", "*\software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit*", "*\software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell*", "*\software\Microsoft\Windows NT\CurrentVersion\Windows*", "*\software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders*", "*\system\CurrentControlSet\Control\SafeBoot\AlternateShell*"] -user IN EXCLUDED_USERS
```

Disable of ETW Trace Detected

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

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

MiniNt Registry Key Addition

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

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

Discovery of a System Time Detected

- **Trigger Condition:** The use of various commands to query a system's time is identified. Adversaries may attempt to manipulate the system time to throw off logs' accuracy or hide their activities. They may also use the system time to trigger the execution of malicious payloads or scripts at specific times.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** System Time Discovery
- **ATT&CK ID:** T1124
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 ((image IN ["*\net.exe", "*\net1.exe"] command="*time*") OR (image="*\w32tm.exe" command="*tz*") OR (image="*\powershell.exe" command="*Get-Date*")) -user IN EXCLUDED_USERS
```

Discovery using Bloodhound Detected

- **Trigger Condition:** Enumeration attempt by a user using the IPC$ share.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** System Owner/User Discovery
- **ATT&CK ID:** T1033
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=3 service=ldap image IN ['*cmd.exe', '*powershell.exe', '*sharphound.exe'] -user IN EXCLUDED_USERS | chart count() as eventCount by host, service, image | search eventCount > 10
```

Discovery via File and Directory Discovery Using Command Prompt

- **Trigger Condition:** A file and directory enumerated, or searching of a specific location of a host or network share within a file system using command prompt is detected.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** File and Directory Discovery
- **ATT&CK ID:** T1083
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4688 (commandline = "tree*" OR command = "tree*") -user IN EXCLUDED_USERS | rename commandline as command
```

Discovery via Discovery via PowerSploit Recon Module Detected

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

```
norm_id=WinServer event_id=4104 (scriptblocktext in POWERSPLOIT_RECON_MODULES OR script_block in POWERSPLOIT_RECON_MODULES) -user IN EXCLUDED_USERS | rename scriptblocktext as script_block
```

DLL Load via LSASS Detected

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

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

DNS Exfiltration Tools Execution Detected

- **Trigger Condition:** Execution of tools for Application Layer Protocol and DNS Exfiltration.
- **ATT&CK Category:** Exfiltration
- **ATT&CK Tag:** Exfiltration Over Alternative Protocol
- **ATT&CK ID:** T1048
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 (image="*\iodine.exe" OR image="*\dnscat2*") -user IN EXCLUDED_USERS
```

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"]
```

DNS ServerLevelPluginDll Install

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

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

Domain Trust Discovery Detected

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

```
norm_id=WindowsSysmon event_id=1 ((image="*\dsquery.exe" command="*-filter*" command="*trustedDomain*") OR (image="*\nltest.exe" command="*domain_trusts*")) -user IN EXCLUDED_USERS
```

DoppelPaymer Ransomware Connection to Malicious Domains

- **Trigger Condition:** Any connection to DoppelPaymer Double Extortion ransomware related domains is detected.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Proxy

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

```
norm_id=* (url IN DOPPELPAYMENR_RANSOMWARE_DOMAINS OR domain IN DOPPELPAYMENR_RANSOMWARE_DOMAINS)
```

DoppelPaymer Ransomware Exploitable Vulnerabilities Detected

- **Trigger Condition:** Vulnerability management detects the presence of vulnerability linked to DoppelPaymer ransomware.
- **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-2019-19781*"
```

DoppelPaymer Ransomware Infected Host Detected

- **Trigger Condition:** DoppelPaymer Double Extortion ransomware-infected host is detected.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Data Encrypted for Impact
- **ATT&CK ID:** T1486
- **Minimum Log Source Requirement:** Firewall, IDS/IPS, Windows Sysmon
- **Query:**

```
host=* hash=* hash IN DOPPELPAYMER_RANSOMWARE_HASHES
```

dotNET DLL Loaded Via Office Applications

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

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

DPAPI Domain Backup Key Extraction Detected

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

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

DPAPI Domain Master Key Backup Attempt

- **Trigger Condition:** An attempt to backup DPAPI master key is detected. The event is generated on the source and not on the Domain Controller.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows
- **Query:**

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

DragonFly - File Upload with Trojan Karagany

- **Trigger Condition:** Updation of a file with the use of Trojan Karagany is detected.
- **ATT&CK Category:** Defense Evasion, Credential Access, Privilege Escalation
- **ATT&CK Tag:** Exploitation for Defense Evasion, Exploitation for Credential Access, Exploitation for Privilege Escalation, Exploitation for Defense Evasion
- **ATT&CK ID:** T1211, T1212, T1068, T1211
- **Minimum Log Source Requirement:** -
- **Query:**

```
filename "identifiant"| norm on filename=<file:all>&identifiant | search file=*
```

DragonFly - Malicious File Creation

- **Trigger Condition:** Creation of a malicious file.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter
- **ATT&CK ID:** T1059
- **Minimum Log Source Requirement:** Integrity Scanner
- **Query:**

```
("*TMPprovider*" OR "*sysmain*" OR "*sydmain*") OR (norm_id=IntegrityScanner file_path IN DRAGONFLY_MALICIOUS_FILES OR file_path IN DRAGONFLY_MA
```

```
LICIOUS_FOLDER OR registry IN DRAGONFLY_MALICIOUS_FILES) | rename regist
ry as file_path | norm on file_path <path:.*>\<file:string> | process re
gex("(?P<file>(TMPprovider[0-9]{3}\.dll|sy[ds]main\.dll))", msg) | searc
h file=*
```

DragonFly - Watering Hole Sources

- **Trigger Condition:** Dragonfly watering hole sources are detected.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** Drive by Compromise
- **ATT&CK ID:** T1189
- **Minimum Log Source Requirement:** Firewall, IDS/IPS, Webserver
- **Query:**

```
norm_id=* url IN ["*script*iframe*", "*dwd", "*dwe", "*fnd", "*fne"] sou
rce_address=*
```

Dridex Process Pattern Detected

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

```
norm_id=WindowsSysmon event_id=1 (command="*\svchost.exe C:\Users\*\Desk
top\*" OR (parent_image="*\svchost.exe*" command IN ["*whoami.exe /all",
"*net.exe view"])) -user IN EXCLUDED_USERS
```

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
```

Drupal Arbitrary Code Execution Detected

- **Trigger Condition:** The exploitation of arbitrary code execution vulnerability (CVE-2018-7600) in Drupal, is detected.
- **ATT&CK Category:** Initial Access

- **ATT&CK Tag:** Exploit Public-Facing Application
- **ATT&CK ID:** T1190
- **Minimum Log Source Requirement:** Firewall, IDS/IPS, Webserver
- **Query:**

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

DTRACK Process Creation Detected

- **Trigger Condition:** Specific process parameters, as seen in DTRACK infections are detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Process Injection
- **ATT&CK ID:** T1055
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 command="* echo EEEE > *" -user IN EXCLUDED_USERS
```

Elevated Command Prompt Activity by Non-Admin User Detected

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

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

Elise Backdoor Detected

- **Trigger Condition:** Elise backdoor activity used by APT32 is detected.
- **ATT&CK Category:** Execution, Privilege Escalation, Defense Evasion
- **ATT&CK Tag:** Windows Command Shell, Abuse Elevation Control Mechanism
- **ATT&CK ID:** T1059.003, T1548
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label="Create" (("process"="*\Microsoft\Network\svchost.exe") OR (command = "*\Windows\Caches\NavShExt.dll*" command = "*/c del* " )) OR (command in ["*\AppData\Roaming\MICROS~1\Windows\Caches\NavShExt.dll", "*\AppData\Roaming\Microsoft\Windows\Caches\NavShExt.dll"] command="*,Setting*")
```

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
```

Emissary Panda Malware SLLauncher Detected

- **Trigger Condition:** The execution of DLL side-loading malware used by threat group Emissary Panda, also known as APT27 is 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="*\sllauncher.exe" image="*\svchost.exe" -user IN EXCLUDED_USERS
```

Emotet Process Creation Detected

- **Trigger Condition:** Emotet like process executions that are not covered by the more generic rules are detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Process Injection
- **ATT&CK ID:** T1055
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 command IN ["* -e* PAA*", "*JABlAG4AdgA6AHUAcwBlAHIAcAByAG8AZgBpAGwAZQ*", "*QAZQBuAHYAOgB1AHMAZQByAHAAcgBvAGYAaQBsAGUA*", "*kAGUAbgB2ADoAdQBzAGUAcgBwAHIAbwBmAGkAbABlA*", "*IgAoACcAKgAnACkAOwAkA*",
"*IAKAAnACoAJwApADsAJA*", "*iACgAJwAqACcAKQA7ACQA*", "*JABGAGwAeAByAGgAYwBmAGQ*"] -user IN EXCLUDED_USERS
```

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
- **Query:**

```
norm_id=WindowsSysmon event_id=1 command IN ["* -NoP -sta -NonI -W Hidden -Enc *", "* -noP -sta -w 1 -enc *", "* -NoP -NonI -W Hidden -enc *"] -user IN EXCLUDED_USERS
```

Empire PowerShell UAC Bypass Detected

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

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

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, thay will be allowed to control other Active Directory user's objects.
- **ATT&CK Category:** Privilege Escalation
- **ATT&CK Tag:** Valid Accounts
- **ATT&CK ID:** T1078
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4704 message="*SeEnableDelegationPrivilege*" -user IN EXCLUDED_USERS
```

Encoded FromBase64String Detected

- **Trigger Condition:** The .NET method "FromBase64String" decodes a Base64-encoded string. Base64 is a widely used encoding scheme representing binary data in an ASCII string format. It is often used to encode data for transfer over networks or store data in databases or files. Adversaries may use Base64 encoding to conceal the contents of their payloads or communications, making it more difficult for defenders to detect and analyze their activities. They may also use the "FromBase64String"

method to decode Base64-encoded data as part of their attack. False Positive: Some legitimate processes might use encoded commands

- **ATT&CK Category:** Execution, Defense Evasion
- **ATT&CK Tag:** Command and Scripting Interpreter, PowerShell, Deobfuscate/Decode Files or Information
- **ATT&CK ID:** T1059, T1059.001, T1140
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 command IN ["*OjpGcm9tQmFzZTY0U3RyaW5n*", "*o6RnJvbUJhc2U2NFN0cmluZ*", "*6OkZyb21CYXNlNjRTdHJpbm*"] -user IN EXCLUDED_USERS
```

Encoded IEX Detected

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

```
norm_id=WindowsSysmon event_id=1 command IN ["*SUVYIChb*", "*lFWCAoW*", "*JRVggKF*", "*aWV4IChb*", "*lleCAoW*", "*pZXggKF*", "*aWV4IChOZX*", "*lleCAoTmV3*", "*pZXggKE5ld*", "*SUVYIChOZX*", "*lFWCAoTmV3*", "*JRVggKE5ld*"] -user IN EXCLUDED_USERS
```

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:** Command and Scripting Interpreter, PowerShell
- **ATT&CK ID:** T1059, T1059.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 image="*powershell.exe" command IN ["*-enc*", "*-ec*"] -user IN EXCLUDED_USERS
```

Endpoint Protect Multiple Failed Login Attempt

- **Trigger Condition:** A user fails to log in even after multiple attempts.
- **ATT&CK Category:** Defense Evasion, Persistence, Privilege Escalation, Initial Access
- **ATT&CK Tag:** Exploitation for Credential Access, Exploitation for Privilege Escalation, Exploitation for Defense Evasion, Brute Force
- **ATT&CK ID:** T1212, T1068, T1211, T1110
- **Minimum Log Source Requirement:** EndPoint Protector
- **Query:**

```
norm_id=EndPointProtector label=User (label=Login OR label=Authenticatio
n) label= Fail user=* caller_user=* | chart count() as CNT by user, call
er_user order by CNT desc | search "CNT">5
```

Equation Group DLL_U Load Detected

- **Trigger Condition:** A specific tool and export used by the EquationGroup is detected.
- **ATT&CK Category:** Execution, Defense Evasion
- **ATT&CK Tag:** Command-Line Interface, Signed Binary Proxy Execution, Rundll32
- **ATT&CK ID:** T1059, T1218, T1218.011
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 ((image="*\rundll32.exe" command="*, dl
l_u") OR command="* -export dll_u *") -user IN EXCLUDED_USERS
```

Eventlog Cleared Detected

- **Trigger Condition:** One of the Windows Event logs has been cleared.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Indicator Removal on Host
- **ATT&CK ID:** T1070
- **Minimum Log Source Requirement:** Windows
- **Query:**

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

ExchangeMT Possible Data Theft - Email with Attachment Outside Organization

- **Trigger Condition:** An email with attachment is sent to the receiver outside the organization domain.
- **ATT&CK Category:** Exfiltration, Collection
- **ATT&CK Tag:** Exfiltration Over C2 Channel, Email Collection

- **ATT&CK ID:** T1041, T1114
- **Minimum Log Source Requirement:** ExchangeMT
- **Query:**

```
norm_id=ExchangeMT -receiver IN HOME_DOMAIN datasize=* |chart sum(datasize/1000000) as "Emailsize(MB)" by sender |search "Emailsize(MB)">50
```

ExchangeMT Unusual Outbound Email

- **Trigger Condition:** 60 or more emails are sent from the same sender within an hour.
- **ATT&CK Category:** Command and Control, Exfiltration, Collection
- **ATT&CK Tag:** Proxy, Exfiltration Over C2 Channel, Automated Exfiltration, Email Collection
- **ATT&CK ID:** T1090, T1041, T1020, T1114
- **Minimum Log Source Requirement:** ExchangeMT
- **Query:**

```
norm_id=ExchangeMT sender=* receiver=* -receiver in HOME_DOMAIN| chart count(receiver=*) as MailSent by sender | search MailSent>60
```

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
```

Execution in Non-Executable Folder Detected

- **Trigger Condition:** Execution of a suspicious program from a different folder is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Masquerading
- **ATT&CK ID:** T1036
- **Minimum Log Source Requirement:** Office365
- **Query:**

```
norm_id=WindowsSysmon event_id=1 image IN ["*\$Recycle.bin", "*\Users\All Users\*", "*\Users\Default\*", "*\Users\Public\*", "C:\Perflogs\*", "*\config\systemprofile\*", "*\Windows\Fonts\*", "*\Windows\IME\*", "*\Windows\addins\*"] -user IN EXCLUDED_USERS
```

Execution in Outlook Temp Folder Detected

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

```
norm_id=WindowsSysmon event_id=1 image="*\Temporary Internet Files\Content.Outlook\*" -user IN EXCLUDED_USERS
```

Execution in Webserver Root Folder Detected

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

```
norm_id=WindowsSysmon event_id=1 image="*\Temporary Internet Files\Content.Outlook\*" -user IN EXCLUDED_USERS
```

Execution of Renamed PaExec Detected

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

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

Execution via Control Panel Items

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

- `norm_id=WindowsSysmon event_id=1 image="*control.exe" command="*control* cpl*" -user IN EXCLUDED_USERS`

Execution via HTA using IE JavaScript Engine Detected

- **Trigger Condition:** The execution of an HTA (HTML Application) file using the Internet Explorer JavaScript engine. HTAs are standalone applications written in HTML and can execute scripts, such as JavaScript or VBScript, on a system. Adversaries may use HTAs as a delivery mechanism for their payloads or execute arbitrary code on a system. Adversaries may use HTAs as a way to bypass security controls or to evade detection. They may also use them to execute arbitrary code on a system, potentially allowing them to access sensitive information or compromise the system.
- **ATT&CK Category:** Execution, Defense Evasion
- **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=7 source_image="*mshta.exe" image="*jscript9.dll" -user IN EXCLUDED_USERS`

Execution via Squiblydoo Technique Detected

- **Trigger Condition:** Execution of the Squiblydoo technique is detected. Squiblydoo runs payloads or scripts by leveraging the Windows Script Host (WSH) and its default file associations. Adversaries may use Squiblydoo to bypass security controls or to evade detection. Adversaries may use the Squiblydoo technique to execute arbitrary code on a system, potentially allowing them to access sensitive information or compromise the system. They may also use it to hide their activities' true nature or evade detection.
- **ATT&CK Category:** Execution, Defense Evasion
- **ATT&CK Tag:** Signed Binary Proxy Execution, Regsvr32
- **ATT&CK ID:** T1218, T1218.01
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
- `norm_id=WindowsSysmon event_id=7 image="*scrobj.dll" -user IN EXCLUDED_USERS`

Execution via Windows Scripting Host Component Detected

- **Trigger Condition:** This alert detects the execution of a script using the Windows Scripting Host (WSH) component on a system. WSH is a Microsoft technology that allows users to run scripts and automate tasks on Windows systems. Adversaries may use WSH to execute their payloads or

automate their system activities. Adversaries may use the WSH component to execute arbitrary code on a system, potentially allowing them to access sensitive information or compromise the system. They may also use it to hide their activities' true nature or evade detection.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter
- **ATT&CK ID:** T1059
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
- `norm_id=WindowsSysmon event_id=7 image in ["*wshom.ocs", "*scrrun.dll", "*vbscript.dll"] -user IN EXCLUDED_USERS`

Exfiltration and Tunneling Tools Execution

- **Trigger Condition:** Execution of tools for data exfiltration and tunneling are detected.
- **ATT&CK Category:** Exfiltration
- **ATT&CK Tag:** Automated Exfiltration
- **ATT&CK ID:** T1020
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
- `norm_id=WindowsSysmon event_id=1 new_process IN ["*\plink.exe", "*\socat.exe", "*\stunnel.exe", "*\httptunnel.exe"] -user IN EXCLUDED_USERS`

Exim MTA Remote Code Execution Vulnerability Detected

- **Trigger Condition:** Remote code execution vulnerability in Exim MTA is detected. The U.S. National Security Agency (NSA) reported that Russian military cyber actors, also known as Sandworm Team, have been actively exploiting a critical vulnerability in Exim MTA since August 2019.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Network Service Scanning, Software Discovery, Security Software Discovery
- **ATT&CK ID:** T1046, T1518, T1518.001
- **Minimum Log Source Requirement:** Vulnerability Management
- **Query:**
- `norm_id=VulnerabilityManagement cve_id="*CVE-2019-10149*"`

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*"`

Existing Service Modification Detected

- **Trigger Condition:** A modification of an existing service via the *sc.exe* system utility is detected. Adversaries abuse the Windows Service Control Manager to execute malicious commands or payloads without creating new services.
- **ATT&CK Category:** Persistence, Privilege Escalation
- **ATT&CK Tag:** Create or Modify System Process, Windows Service
- **ATT&CK ID:** T1543, T1543.003
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**
- `label="Create" label="Process" "process" IN ["*sc.exe", "*powershell.exe", "*cmd.exe"] command="*sc*" command="*config*" command="*binpath*" -user IN EXCLUDED_USERS`

Exploit for CVE-2017-0261 Detected

- **Trigger Condition:** *Winword* initiating an uncommon subprocess *FLTLDR.exe* used for exploitation of CVE-2017-0261 and CVE-2017-0262 is detected.
- **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 parent_image="*\WINWORD.EXE" image="*\FLTLDR.exe*" -user IN EXCLUDED_USERS`

Exploit for CVE-2017-8759 Detected

- **Trigger Condition:** Winword starting unfamiliar subprocess csc.exe used in exploits for CVE-2017-8759 is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Exploitation for Client Execution
- **ATT&CK ID:** T1203
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
- `norm_id=WindowsSysmon event_id=1 parent_image="*\WINWORD.EXE" image="*\csc.exe" -user IN EXCLUDED_USERS`

Exploiting SetupComplete CVE-2019-1378 Detected

- **Trigger Condition:** The exploitation attempt of privilege escalation vulnerability via *Setup Complete.cmd* and *PartnerSetup Complete.cmd* described in CVE-2019-1378 is detected.
- **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 parent_command IN ["*\cmd.exe /c C:\Windows\Setup\Scripts\SetupComplete.cmd", "*\cmd.exe /c C:\Windows\Setup\Scripts\PartnerSetupComplete.cmd"] -image IN ["C:\Windows\System32\*", "C:\Windows\SysWOW64\*", "C:\Windows\WinSxS\*", "C:\Windows\Setup\*"] -user IN EXCLUDED_USERS
```

External Disk Drive or USB Storage Device Detected

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

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

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
```

File and Directory Discovery Using PowerShell Detected

- **Trigger Condition:** Enumeration of files and directories via Command and Scripting Interpreter and PowerShell is detected.
- **ATT&CK Category:** Discovery

- **ATT&CK Tag:** File and Directory Discovery
- **ATT&CK ID:** T1083
- **Minimum Log Source Requirement:** Windows
- **Query:**
- ```
  norm_id=WinServer event_id=4103 (command_name="get-childitem*" OR command="get-childitem*") -user IN EXCLUDED_USERS | rename command_name as command
  ```

File Creation by PowerShell Detected

- **Trigger Condition:** The creation of a new file using PowerShell on a system. PowerShell is a powerful scripting language that is built into Windows and can be used to automate a wide variety of tasks. Adversaries may use PowerShell to create new files, potentially to drop and execute malicious payloads or store data for later retrieval. False positive Notice: Administrative tasks and genuine processes might cause the alert to trigger as well. Proper analysis and whitelisting are recommended.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, PowerShell
- **ATT&CK ID:** T1059, T1059.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
- ```
  norm_id=WindowsSysmon event_id=11 file=* source_image="*powershell.exe" -file IN ["__PSScriptPolicyTest_*", "PowerShell_transcript.*", "powershell.exe.log", "StartupProfileData*", "ModuleAnalysisCache"] -user IN EXCLUDED_USERS -file IN ["*.mui"]
  ```

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
  ```

File or Folder Permissions Modifications

- **Trigger Condition:** Modifications to the permissions of files or folders on a system. File and folder permissions control a system's access to files and
  ```

directories and determine which users and processes are allowed to read, write, or execute them. Adversaries may attempt to modify these permissions to gain unauthorized access to sensitive files or to execute arbitrary code on a system. They may also use these modifications to escalate their system privileges or move laterally within an organization's network.

- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** File and Directory Permissions Modification
- **ATT&CK ID:** T1222
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 ((image IN ["*\takeown.exe", "*\cacls.exe", "*\icacls.exe"] command="*/grant*") OR (image="*\attrib.exe" command="*-r*")) -user IN EXCLUDED_USERS
```

File System Permissions Weakness

- **Trigger Condition:** A weakness in the file system permissions on a system is detected. File system permissions control access to files and directories and determine which users and processes can read, write, or execute them. Adversaries may exploit weaknesses in file system permissions to gain unauthorized access to sensitive files or execute arbitrary code on a system.
- **ATT&CK Category:** Persistence, Privilege Escalation, Defense Evasion
- **ATT&CK Tag:** Hijack Execution Flow, Services File Permissions Weakness
- **ATT&CK ID:** T1574,T1574.010
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

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

Fireball Archer Installation Detected

- **Trigger Condition:** Invocation of an *Archer* malware via rundll32 is detected.
- **ATT&CK Category:** Execution, Defense Evasion
- **ATT&CK Tag:** Command-Line Interface,Signed Binary Proxy Execution, Rundll32
- **ATT&CK ID:** T1059, T1218, T1218.011
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 command="*\rundll32.exe *, InstallArcherSvc" -user IN EXCLUDED_USERS
```

Firewall Configuration Modification Detected

- **Trigger Condition:** When there is a change or modification to the Windows firewall configuration on a system. This could indicate malicious activity, as an adversary may be attempting to disable or bypass the firewall to gain unauthorized access to the system or network. False Positive Notice: Legitimate system maintenance or system administration tasks may involve the modification of firewall configurations, and these could potentially trigger the alert. It is essential to carefully review and investigate any instances of this alert before taking action to ensure that the activity detected is genuinely malicious.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Non-Standard Port
- **ATT&CK ID:** T1571
- **Minimum Log Source Requirement:** Windows
- **Query:**
- `norm_id=WinServer event_id=4946 rule=* -user IN EXCLUDED_USERS`

Firewall Disabled via Netsh Detected

- **Trigger Condition:** *netsh* command turns off the Windows firewall.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Process Injection
- **ATT&CK ID:** T1055
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
- `norm_id=WindowsSysmon event_id=1 command IN ["netsh firewall set opmode mode=disable", "netsh advfirewall set * state off"] -user IN EXCLUDED_USERS`

First Time Seen Remote Named Pipe

- **Trigger Condition:** The alert rule excludes the named pipes accessible remotely and notifies on new cases. Also, it helps to detect lateral movement and remote execution using named pipes.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Remote Services
- **ATT&CK ID:** T1021
- **Minimum Log Source Requirement:** Windows
- **Query:**
- `norm_id=WinServer event_id=5145 share_name="IPC$" -relative_target IN ["atsvc", "samr", "lsarpc", "winreg", "netlogon", "srvsvc", "protected_storage", "wkssvc", "browser", "netdfs", "svcctl", "spoolss", "ntsvcs", "LSM_API_service", "HydraLsPipe", "TermSrv_API_service", "MsFteWds"] -user IN EXCLUDED_USERS`

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`

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`

Formbook Process Creation Detected

- **Trigger Condition:** Formbook like process executions injecting code into a set of files in the System32 folder, which executes a unique command line to delete the dropper from the AppData Temp folder is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Process Injection
- **ATT&CK ID:** T1055
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
- `norm_id=WindowsSysmon event_id=1 parent_command IN ["C:\Windows\System32\*.exe", "C:\Windows\SysWOW64\*.exe"] command IN ["* /c del *C:\Users\*\AppData\Local\Temp\*.exe", "* /c del *C:\Users\*\Desktop\*.exe", "* /C type nul > *C:\Users\*\Desktop\*.exe"] -user IN EXCLUDED_USERS`

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=*`

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
```

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
```

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
```

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
```

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
```

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
```

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
```

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
```

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
```

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=*
```

FromBase64String Command Line Detected

- **Trigger Condition:** When the “FromBase64String” command is used in a command line interface on a system. This command decodes a string that has been encoded using base64 encoding. The FromBase64String command is not necessarily malicious, as it can be used for legitimate purposes such as decoding base64-encoded data. However, an adversary may use this command as part of a malicious attack. For example, they may use it to decode a base64-encoded payload injected into the system to execute arbitrary code. False positive Notice: Legitimate system maintenance or system administration tasks may involve the use of the FromBase64String command, and these could potentially trigger the alert. It is essential to carefully review and investigate any instances of this alert before taking any action to ensure that the activity being detected is truly malicious.

- **ATT&CK Category:** Defense Evasion, Execution
- **ATT&CK Tag:** T1059.001 - PowerShell, T1059.003 - Windows Command Shell, T1140 - Deobfuscate/Decode Files or Information
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
- ```
  norm_id=WindowsSysmon event_id=1 command="*::FromBase64String(*" -user I
  N EXCLUDED_USERS
  ```

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
  ```

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=*
  ```

Fsutil Suspicious Invocation Detected

- **Trigger Condition:** When the “fsutil” command is used in a suspicious or potentially malicious way on a system. The fsutil command is a utility that allows users to perform various file system tasks, such as creating hard links, managing to reparse points and dismounting volumes. It might indicate that a ransomware attack (seen by NotPetya and others) has occurred.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Indicator Removal on Host
- **ATT&CK ID:** T1070
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
- ```
  norm_id=WindowsSysmon event_id=1 (image="*\fsutil.exe" OR file="fsutil.e
  xe") command IN ["*deletejournal*", "*createjournal*"] -user IN EXCLUDED
  _USERS
  ```

GAC DLL Loaded Via Office Applications Detected

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

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

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
```

Grabbing Sensitive Hives via Reg Utility

- **Trigger Condition:** Grabbing of Sensitive Hives via Reg Utility.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 image="*\reg.exe" command IN ["*save*", "*export*"] command IN ["*hklm*", "*hkey_local_machine*"] command IN ["*\system", "*\sam", "*\security"] -user IN EXCLUDED_USERS
```

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
```

HH Execution Detected

- **Trigger Condition:** When the “hh.exe” process is detected running on a system. HH.exe is a legitimate process associated with the Windows HTML Help feature and is used to display compiled help files (.chm) on a system. While the execution of hh.exe in itself is not necessarily malicious, an adversary may use this process as part of a larger attack. For example, they may embed malicious code in a compiled help file and use hh.exe to execute it on a target system. False Positive Note: Legitimate applications or system processes may use hh.exe to display help files, which could potentially trigger the alert. It is essential to carefully review and investigate any instances of this alert before taking any action to ensure that the activity being detected is truly malicious.
- **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" command="*.chm*" -user IN EXCLUDED_USERS
```

Hidden Cobra Affected Host

- **Trigger Condition:** Windows Server is affected by Hidden Cobra.
- **ATT&CK Category:** Discovery
- **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:** Windows
- **Query:**

```
(object IN HIDDEN_COBRA_FILES OR file in HIDDEN_COBRA_FILES OR hash in HIDDEN_COBRA_FILES) host=* | rename object as file
```

Hidden Cobra Emails Sent to Attacker

- **Trigger Condition:** LogPoint detects an email sent to Hidden Cobra listed emails.
- **ATT&CK Category:** Exfiltration, Collection
- **ATT&CK Tag:** Exfiltration Over C2 Channel, Email Collection
- **ATT&CK ID:** T1041, T1114
- **Minimum Log Source Requirement:** Mail Server
- **Query:**

- `sender=* receiver=* receiver in HIDDEN_COBRA_EMAIL (host=* OR source_host=*) | rename source_host as host`

Hidden Cobra Vulnerable Sources

- **Trigger Condition:** Vulnerability Scanning Tools detect Hidden Cobra's vulnerable hosts.
- **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:** Vulnerability Management
- **Query:**
- `cve_id in HIDDEN_COBRA_CVE source_address=* | rename title as vulnerability, domain as host`

Hidden Files and Directories - VSS Detected

- **Trigger Condition:** Adversaries hide files and directories to evade detection.
- **ATT&CK Category:** Defense Evasion, Persistence
- **ATT&CK Tag:** Hide Artifacts, Hidden Files and Directories
- **ATT&CK ID:** T1564, T1564.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
- `norm_id=WindowsSysmon event_id=1 (image="*\VolumeShadowCopy*\*" or command="*\VolumeShadowCopy*\*") -user IN EXCLUDED_USERS`

Hidden Files and Directories Detected

- **Trigger Condition:** When the presence of hidden files and directories on a system is detected. Adversaries may use hidden files and directories to conceal malicious files or activities from the victim. They may also use these files to store command and control information or to persist on a system after an initial compromise. By hiding their files and directories, adversaries can make it more difficult for defenders to detect and respond to their activities.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Hide Artifacts, Hidden Files and Directories
- **ATT&CK ID:** T1564, T1564.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
- `norm_id=WindowsSysmon event_id=1 image="*attrib.exe" (command="*+h*" or command="*+s*") -user IN EXCLUDED_USERS`

Hidden PowerShell Window Detected

- **Trigger Condition:** When a hidden PowerShell window is detected on the system. Adversaries can use hidden PowerShell windows to conceal their actions and execute malicious code without the victim's knowledge. These windows can be challenging to detect and can be used to persist on a system after an initial compromise. It is important to identify and address hidden PowerShell windows, as they may indicate an active adversary on the system. Log source requirement: This alert requires the log source to be a system event log with Event ID 1074.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Hide Artifacts, Hidden Window
- **ATT&CK ID:** T1564, T1564.003
- **Minimum Log Source Requirement:** Windows
- **Query:**
- `norm_id=WinServer event_id=4688 "process"="*powershell.exe" (commandline="*-w*hid*" OR command="*-w*hid*") -user IN EXCLUDED_USERS`

Hiding Files with Attrib Detected

- **Trigger Condition:** The use of *attrib.exe* to hide files from users is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Hide Artifacts, Hidden Files and Directories
- **ATT&CK ID:** T1564, T1564.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**
- `label=Create label="Process" "process"="*\attrib.exe" command = "* +h *" -(command = "*\desktop.ini*" OR (parent_process = "*\cmd.exe" command = "*+R +H +S +A \*.cui*" parent_command = "*C:\WINDOWS\system32\*.bat*"))`

Hurricane Panda Activity Detected

- **Trigger Condition:** LogPoint detects Hurricane Panda activity.
- **ATT&CK Category:** Privilege Escalation
- **ATT&CK Tag:** Exploitation for Privilege Escalation
- **ATT&CK ID:** T1068
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
- `norm_id=WindowsSysmon event_id=1 command IN ["* localgroup administrators admin /add", "*\Win64.exe*"] -user IN EXCLUDED_USERS`

IIS Native-Code Module Command Line Installation

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

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

Image File Execution Options Injection

- **Trigger Condition:** 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, Defense Evasion
- **ATT&CK Tag:** Event Triggered Execution, Image File Execution Options Injection
- **ATT&CK ID:** T1546, T1546.012
- **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\Image File Execution Options\*" or target_object="*\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\*") -user IN EXCLUDED_USERS
```

Service Stop Detected

- **Trigger Condition:** Adversaries maliciously modify components of a victim environment to hinder or disable defensive mechanisms.
- **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:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 (image="*net.exe" or image="*sc.exe") command="*stop*" -user IN EXCLUDED_USERS
```

In-memory PowerShell Detected

- **Trigger Condition:** Loading of essential DLL used by PowerShell, but not by the process *powershell.exe* is detected. In addition, it detects the Meterpreter's *Load PowerShell* extension.
- **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=7 image IN ["*\System.Management.Automation.Dll", "*\System.Management.Automation.ni.Dll"] -source_image IN ["*\powershell.exe", "*\powershell_ise.exe", "*\WINDOWS\System32\sdiagnhost.exe", "*\mscorsvw.exe", "*\WINDOWS\System32\RemoteFXvGPUDisablement.exe"] -user="NT AUTHORITY\SYSTEM" -user IN EXCLUDED_USERS
  ```

Indicator Blocking - Driver Unloaded

- **Trigger Condition:** Adversary 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
  ```

Indicator Blocking - Sysmon Registry Edited

- **Trigger Condition:** An indicator blocking via registry editing is detected. Adversaries might block indicators or events typically captured by sensors from being gathered and analyzed to evade detection.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Impair Defenses, Indicator Blocking
- **ATT&CK ID:** T1562, T1562.006
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
- ```
  norm_id=WindowsSysmon event_id IN [12,13,14] target_object in ["*HKLM\System\CurrentControlSet\Services\SysmonDrv*","*HKLM\System\CurrentControlSet\Services\Sysmon*","*HKLM\System\CurrentControlSet\Services\Sysmon64*"]  -"process" IN ["*\Sysmon64.exe","*\Sysmon.exe"] -event_type=INFO -user IN EXCLUDED_USERS
  ```

Indirect Command Execution Detected

- **Trigger Condition:** When indirect command execution via Program Compatibility Assistant is detected. pcalua.exe, forfiles.exe. or pcalua.exe is a command-line tool that allows users to run programs with administrator access rights on Windows operating systems. It is useful for running programs that require elevated permissions, such as installing or modifying system-level software. forfiles.exe is a command-line tool that enables a user to run a command on multiple files in a specified directory. It helps
  ```

batch process multiple files, such as deleting or renaming them. Adversaries can use it to achieve indirect command execution.
- **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 parent_image IN ["*\pcalua.exe", "*\forfiles.exe"] -user IN EXCLUDED_USERS`

Install Root Certificate

- **Trigger Condition:** Adversaries undermine security controls that will either warn users of the untrusted activity or prevent the execution of untrusted programs.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Subvert Trust Controls, Install Root Certificate
- **ATT&CK ID:** T1553, T1553.004
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
- `norm_id=WindowsSysmon (event_id=12 or event_id=13 or event_id=14) image!="*svchost.exe" (target_object="*\SOFTWARE\Microsoft\EnterpriseCertificates\Root\Certificates\*" or target_object="*\Microsoft\SystemCertificates\Root\Certificates\*") -user IN EXCLUDED_USERS`

Suspicious InstallUtil Execution

- **Trigger Condition:** Adversaries use *InstallUtil* for proxy execution of code through a trusted Windows utility. *InstallUtil* is a command-line utility that allows installation and uninstallation of resources by executing specific installer components specified in .NET binaries. Typically, adversaries will utilize the most commonly found way to invoke via the InstallUtil Uninstall method.
- **ATT&CK Category:** Defense Evasion, Execution
- **ATT&CK Tag:** Signed Binary Proxy Execution, InstallUtil
- **ATT&CK ID:** T1218, T1218.004
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
- `norm_id=WindowsSysmon event_id=3 (image="*InstallUtil.exe" or command="*\/logfile= \/LogToConsole=false \/U*") -user IN EXCLUDED_USERS`

InvisiMole Malware Connection to Malicious Domains

- **Trigger Condition:** A connection with domain related to the InvisiMole Malware is detected.
- **ATT&CK Category:** Command and Control

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

```
norm_id=* (url=* OR domain=*) | process domain(url) as domain | search domain in INVISIMOLE_MALWARE_DOMAINS
```

InvisiMole Malware Connection to Malicious Sources

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

```
(destination_address IN INVISIMOLE_MALWARE_IPS OR source_address IN INVISIMOLE_MALWARE_IPS) | process geoip(destination_address) as country
```

InvisiMole Malware Exploitable Vulnerabilities Detected

- **Trigger Condition:** Vulnerability Management detects the presence of vulnerabilities linked to InvisiMole malware that targets high-profile military and diplomatic entities.
- **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-2017-0144*" OR cve_id="*CVE-2019-0708*")
```

InvisiMole Malware Infected Host Detected

- **Trigger Condition:** InvisiMole malware-infected host is detected.
-
- **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)
```

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
```

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
```

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
```

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*"`

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`

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`

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`

Kerberoasting via PowerShell Detected

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

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

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

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]
```

Koadic Execution Detected

- **Trigger Condition:** Command line parameters used by the Koadic hack tool is detected.
- **ATT&CK Category:** 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 command IN ["*cmd.exe* /q /c chcp *"] -user IN EXCLUDED_USERS
```

KRACK Vulnerable Source Detected

- **Trigger Condition:** Sources vulnerable to KRACK are detected.
- **ATT&CK Category:** Discovery
- **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:** Qualys, Vulnerability Management
- **Query:**

```
qualys_id=* qualys_id IN [176179, 91411, 196947, 170424, 170428, 196947] source_address=*
```

Large ICMP Traffic

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

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

Local Account Creation on Workstation Detected

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

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

Local Accounts Discovery Detected

- **Trigger Condition:** Valid Accounts, Account Discovery, or Local Accounts Discovery is detected.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** System Owner/User Discovery, Account Discovery
- **ATT&CK ID:** T1033, T1087
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
(norm_id=WindowsSysmon event_id=1 (((image="*\whoami.exe" OR (image="*\wmic.exe" command="*useraccount*" command="*get*") OR image IN ["*\quser.exe", "*\qwinsta.exe"] OR (image="*\cmdkey.exe" command="*/list*") OR (image="*\cmd.exe" command="*/c*" command="*dir *" command="*\Users\\*")) -(command IN ["* rmdir *"])) OR ((image IN ["*\net.exe", "*\net1.exe"] command="*user*") -(command IN ["*/domain*", "*/add*", "*/delete*", "*/active*", "*/expires*", "*/passwordreq*", "*/scriptpath*", "*/times*", "*/workstations*"])))) -user IN EXCLUDED_USERS
```

Local Port Monitor

- **Trigger Condition:** Adversaries configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems.
- **ATT&CK Category:** Persistence, Privilege Escalation

- **ATT&CK Tag:** Boot or Logon Autostart Execution, Port Monitors
- **ATT&CK ID:** T1547, T1547.01
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon (event_id=12 or event_id=13 or event_id=14) target_object="*\SYSTEM\CurrentControlSet\Control\Print\Monitors\*" -user IN EXCLUDED_USERS
```

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
```

LockerGoga Malware Affected Host

- **Trigger Condition:** LockerGoga malware infects a 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:** Firewall, IDS/IPS, Windows Sysmon
- **Query:**

```
host=* (hash IN LOCKERGOGA_HASHES OR hash_sha1 IN LOCKERGOGA_HASHES OR hash_sha256 IN LOCKERGOGA_HASHES OR file IN LOCKERGOGA_FILES OR object IN LOCKERGOGA_FILES) | rename hash_sha1 as hash, hash_sha256 as hash, object as file
```

LockerGoga Malware Emails Sent to Attacker

- **Trigger Condition:** An email is sent to or from LockerGoga malware listed emails.
- **ATT&CK Category:** Command and Control, Exfiltration
- **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 LOCKERGOGA_EMAILS OR sender in LOCKERGOGA_EMAILS) sender=* receiver=* (host=* OR source_host=*) | rename source_host as host
```

Log Files Creation of Dot-Net-to-JS Detected

- **Trigger Condition:** Creation of log files of Dot-Net-to-JavaScript.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter
- **ATT&CK ID:** T1059
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
```
norm_id=WindowsSysmon event_id=11 path="*UsageLogs*" file in ["*cscript.exe.log", "*wscript.exe.log", "*wmic.exe.log", "*mshta.exe.log", "*svchost.exe.log", "*regsvr32.exe.log", "*rundll32.exe.log"] -user IN EXCLUDED_USERS
```

Login with WMI Detected

- **Trigger Condition:** Logins performed with WMI are detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Windows Management Instrumentation
- **ATT&CK ID:** T1047
- **Minimum Log Source Requirement:** Windows
- **Query:**
```
norm_id=WinServer event_id=4624 "process"="*\WmiPrvSE.exe" -user IN EXCLUDED_USERS
```

Logon Scripts Detected

- **Trigger Condition:** Creation or execution of *UserInitMprLogon Script* persistence method.
- **ATT&CK Category:** Persistence, Lateral Movement
- **ATT&CK Tag:** Logon Scripts
- **ATT&CK ID:** T1037
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
```
norm_id=WindowsSysmon (event_id=1 ((parent_image="*\userinit.exe" -image="*\explorer.exe" -command IN ["*\netlogon.bat", "*\UsrLogon.cmd"]) OR (command="*UserInitMprLogonScript*"))) OR (event_id IN ["11", "12", "13", "14"] target_object="*UserInitMprLogonScript*") -user IN EXCLUDED_USERS
```

LSASS Access from Non System Account Detected

- **Trigger Condition:** Potential mimikatz-like tools accessing LSASS from non system account is detected.

- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows
- **Query:**

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

LSASS Memory Dump Detected

- **Trigger Condition:** Process LSASS memory dump using *procdump* or *taskmgr* based on the CallTrace pointing to *dbghelp.dll* or *dbgcore.dll* for Winodws10 is detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=10 image="C:\windows\system32\lsass.exe" access="0x1fffff" call_trace IN ["*dbghelp.dll*", "*dbgcore.dll*"] -user IN EXCLUDED_USERS
```

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
```

LSSAS Memory Dump with MiniDumpWriteDump API Detected

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

- **ATT&CK Tag:** Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

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

LSASS Memory Dumping Detected

- **Trigger Condition:** Creation of dump files containing the memory space of *lsass.exe*, containing sensitive credentials is detected. It identifies the use of Sysinternals *procdump.exe* to export the memory space of *lsass.exe* containing sensitive credentials.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 ((command="*lsass*" command="*.dmp*" -image="*\werfault.exe") OR (image="*\procdump*" image="*.exe" command="*lsass*")) -user IN EXCLUDED_USERS
```

Macro file Creation Detected

- **Trigger Condition:** Creation of a macro file is detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Command and Scripting Interpreter
- **ATT&CK ID:** T1059
- **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"] -user IN EXCLUDED_USERS
```

Magecart Exploitable Vulnerabilities Detected

- **Trigger Condition:** Vulnerability Management detects the presence of Magento vulnerability linked to Magecart Card Skimming attack on E-Commerce Business.
- **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-2016-4010*"
```

Magecart Threat Connection to Malicious Domains

- **Trigger Condition:** Any connection to Magecart related domains is detected.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Proxy
- **ATT&CK ID:** T1090
- **Minimum Log Source Requirement:** Firewall, IDS/IPS, Webserver
- **Query:**

```
norm_id=* (url=* OR domain=*) | process domain(url) as domain | search domain in MAGECART_DOMAINS
```

Magecart Threat Connection to Malicious Sources

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

```
(destination_address IN MAGECART_IPS OR source_address IN MAGECART_IPS) | process geoip(destination_address) as country
```

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 hide 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*", "*RIUkVBRF9JTkZPNj*",
- "*SFJFQURfSU5GTzY0*", "*VABIAFIARQBBAEQAXwBJAE4ARgBPADYANA*", "*VEhSRUFEX0lORk82N*",
- "*AHIAZQBhAHQAZQBSAGUAbQBvAHQAZQBUAGgAcgBlAGEAZA*", "*cmVhdGVSZW1vdGVUaHJlYW*", "*MAcgBlAGEAdABlAFIAZQBtAG8AdABlAFQAaAByAGUAYQBkA*", "*NyZWF0ZVJlbW90ZVRocmVhZ*", "*Q3JlYXRlUmVtb3RlVGhyZWFk*",
- "*QwByAGUAYQB0AGUAUgBlAG0AbwB0AGUAVABoAHIAZQBhAGQA*", "*0AZQBtAG0AbwB2AGUA*", "*1lbW1vdm*", "*AGUAbQBtAG8AdgBlA*", "*bQBlAG0AbQBvAHYAZQ*", "*bWVtbW92Z*", "*ZW1tb3Zl*"] -user IN EXCLUDED_USERS

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

Malicious PowerShell Commandlet Names Detected

- **Trigger Condition:** LogPoint detects Commandlet names from well-known Command and Scripting Interpreter, and PowerShell exploitation frameworks.
- **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=11 file IN MALICIOUS_POWERSHELL_COMMANDLET_NAMES) or (norm_id=WinServer command IN MALICIOUS_POWERSHELL_COMMANDS) -user IN EXCLUDED_USERS
  ```

Malicious Service Installations Detected

- **Trigger Condition:** Malicious service installs appearing in lateral movement, credential dumping, and other suspicious activity are detected.
- **ATT&CK Category:** Persistence, Privilege Escalation
- **ATT&CK Tag:** Credential Dumping, System Services, Service Execution, New Service
- **ATT&CK ID:** T1003, T1569, T1569.002, T1543
- **Minimum Log Source Requirement:** Windows
- **Query:**
- ```
  norm_id=WinServer event_id=7045 service in ["*\PAExec*", "mssecsvc2.0", "*net user*", "WCESERVICE", "WCE SERVICE", "winexesvc.exe*", "*\DumpSvc.exe", "pwdump*", "gsecdump*", "cachedump*"] -user IN EXCLUDED_USERS
  ```

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, Signed Binary Proxy Execution, Verclsid
- **ATT&CK ID:** T1055, T1218, T1218.012
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
- ```
  event_id=10 image="*\verclsid.exe" access="0x1FFFFF" (call_trace="*|UNKNOWN(*VBE7.DLL*" OR (source_image="*\Microsoft Office*" call_trace="*|UNKNOWN*")) -user IN EXCLUDED_USERS
  ```

Malware Threat Affected Host

- **Trigger Condition:** A malware infects a 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:** Windows
- **Query:**
- ```
  (object IN MALWARE_FILES OR file in MALWARE_FILES OR hash in MALWARE_HASHES) host=* | rename object as file
  ```

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 countr
y
```

Malware Threat Connection to Malicious Destination

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

```
(source_address=* OR destination_address=*) destination_address in MALWA
RE_IP source_address IN HOMENET |process geoip(destination_address) as c
ountry
```

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
```

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=* receiv
er=* (host=* OR source_host=*) | rename source_host as host
```

Masquerading Extension Detected

- **Trigger Condition:** Masquerading of file extension is detected. Adversaries manipulate features of their artifacts to evade defenses and observation.
- **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 (image="*.doc.*" or image="*.docx.*" or image="*.xls.*" or image="*.xlsx.*" or image="*.pdf.*" or image="*.rtf.*" or image="*.jpg.*" or image="*.png.*" or image="*.jpeg.*" or image="*.zip.*" or image="*.rar.*" or image="*.ppt.*" or image="*.pptx.*") -user IN EXCLUDED_USERS
```

Masquerading File Location Detected

- **Trigger Condition:** Masquerading of file location is detected. Adversaries manipulate features of their artifacts to evade defenses and observation.
- **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=11 (source_image="*SysWOW64*" or source_image="*System32*" or source_image="*AppData*" or image="*Temp*") (file="*.exe" or file="*.dll*" or file="*.bat*" or file="*.com*" or file="*.ps1*" or file="*.py*" or file="*.js*" or file="*.vbs*" or file="*.hta*") -user IN EXCLUDED_USERS
```

Matrix Encrypted Files

- **Trigger Condition:** Matrix malware encrypted files are detected.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Data Encrypted for Impact, Data Encrypted, Data Destruction
- **ATT&CK ID:** T1486, T1022, T1485
- **Minimum Log Source Requirement:** Integrity Scanner
- **Query:**

```
norm_id=IntegrityScanner label="Rename" label=File new_file IN MATRIX_FILE | norm on new_file <path:.*><:'\\'><EncryptedFileName:string> | norm on file_path <:.*><:'\\'><OriginalFileName:string>
```

Matrix Vulnerable Sources

- **Trigger Condition:** Vulnerability scanner detects vulnerability related to Internet Explorer and Flash Player that relates to the Matrix Ransomware.
- **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:** Vulnerability Management
- **Query:**
- `cve_id="*CVE-2016-0189*" or cve_id="*CVE-2015-8651*" source_address=*`

Maze Ransomware Connection to Malicious Domains

- **Trigger Condition:** Maze Double Extortion ransomware-related domains is detected.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Proxy
- **ATT&CK ID:** T1090
- **Minimum Log Source Requirement:** Firewall, IDS/IPS, Webserver
- **Query:**
- `norm_id=* (url=* OR domain=*) | process domain(url) as domain | search domain in MAZE_RANSOMWARE_DOMAINS`

Maze Ransomware Connection to Malicious Sources

- **Trigger Condition:** Hosts make an outbound connection to Maze Double Extortion ransomware sources.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Proxy
- **ATT&CK ID:** T1090
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**
- `(destination_address IN MAZE_RANSOMWARE_IPS OR source_address IN MAZE_RANSOMWARE_IPS) | process geoip(destination_address) as country`

Maze Ransomware Exploitable Vulnerabilities Detected

- **Trigger Condition:** Vulnerability management detects presence of vulnerability linked to Maze Double Extortion Ransomware.
- **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 MAZE_RANSOMWARE_CVE`

Maze Ransomware Infected Host Detected

- **Trigger Condition:** MAZE Double Extortion ransomware-infected host is detected.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Data Encrypted for Impact
- **ATT&CK ID:** T1486
- **Minimum Log Source Requirement:** Firewall, IDS/IPS, Windows Sysmon
- **Query:**

```
host=* hash=* hash IN MAZE_RANSOMWARE_HASHES
```

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 so
urce_address | chart count() by source_address, severity, cve_id, soluti
on order by count() desc
```

Meterpreter or Cobalt Strike Getsystem Service Start Detected

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

```
norm_id=WindowsSysmon event_id=1 parent_image="*\services.exe" command I
N ['*cmd* /c * echo *\pipe\*', '*%COMPSEC%* /c * echo *\pipe\*', '*rundl
l32*.dll,a*/p:*'] -command="*MpCmdRun*" -user IN EXCLUDED_USERS
```

Microsoft ActiveX Control Code Execution Vulnerability Detected

- **Trigger Condition:** Remote code execution in Microsoft ActiveX Control (CVE-2012-0158) is detected.

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

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

Microsoft Binary Github Communication Detected

- **Trigger Condition:** Executable accessing GitHub in the Windows folder is detected.
- **ATT&CK Category:** Microsoft Build Engine Loading Credential Libraries
- **ATT&CK Tag:** Ingress Tool Transfer
- **ATT&CK ID:** T1105
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=3 initiated="true" destination_host IN ["*.github.com", "*.githubusercontent.com"] image="C:\Windows\*" -user IN EXCLUDED_USERS
```

Microsoft DotNET Framework Remote Code Execution Detected

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

```
norm_id=WindowsSysmon label="Process" label=Create parent_image='*WINWORD.exe' parent_command='*.rtf*' image='*csc.exe' -user IN EXCLUDED_USERS
```

Microsoft Office Memory Corruption Vulnerability CVE-2015-1641 Detected

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

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

Microsoft Office Memory Corruption Vulnerability CVE-2017-0199 Detected

- **Trigger Condition:** The exploitation of memory corruption vulnerability (CVE-2017-0199) in Microsoft Office is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** User Execution
- **ATT&CK ID:** T1204
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
- `norm_id=WindowsSysmon label=Network label=Connection image='*WINWORD.exe' destination_address IN MOST_EXPLOITABLE_IPS -user IN EXCLUDED_USERS`

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`

Microsoft Office Product Spawning Windows Shell

- **Trigger Condition:** When Windows command line executables started from Microsoft Word, Excel, Powerpoint, Publisher and Visio are detected. Adversaries can use phishing to deliver malicious office documents and lure victims into executing the malicious file and gaining initial access to the system.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** T1059 - Command and Scripting Interpreter, T1059.001 - PowerShell, T1059.003 - Windows Command Shell, T1204.002 - Malicious File
- **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", "*\OUTLOOK.EXE", "*\MSACCESS.EXE","*EQNEDT32.EXE", "*\Onenote.exe"]
- "process" IN ["*\cmd.exe", "*\powershell.exe", "*\pwsh.exe", "*\wscript.exe", "*\cscript.exe", "*\sh.exe", "*\bash.exe", "*\scrcons.exe", "*\schtasks.exe", "*\regsvr32.exe", "*\hh.exe", "*\wmic.exe", "*\mshta.exe", "*\rundll32.exe", "*\msiexec.exe", "*\forfiles.exe", "*\scriptrunner.exe", "*\mftrace.exe", "*\AppVLP.exe", "*\svchost.exe","*\msbuild.exe"]

Mimikatz Command Line Detected

- **Trigger Condition:** *mimikatz* command line argument is detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
- norm_id=WindowsSysmon event_id=1 command IN ["*DumpCreds*", "*Invoke-Mimikatz*", "*rpc::*", "*token::*", "*crypto::*", "*dpapi::*", "*sekurlsa::*", "*kerberos::*", "*lsadump::*", "*privilege::*", "*process::*", "*misc::aadcookie*", "*misc::detours*", "*misc::memssp*", "*misc::mflt*", "*misc::ncroutemon*", "*misc::ngcsign*", "*misc::printnightmare*", "*misc::skeleton*", "*service::preshutdown*", "*ts::mstsc*", "*ts::multirdp*"] -user IN EXCLUDED_USERS

Mitre - Initial Access - Hardware Addition - Removable Storage Connected

- **Trigger Condition:** Removable storage is connected.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** Hardware Additions
- **ATT&CK ID:** T1200
- **Minimum Log Source Requirement:** Windows
- **Query:**
- norm_id=WinServer* event_id=2003 event_source="Microsoft-Windows-DriverFrameworks-UserMode/Operational" -user IN EXCLUDED_USERS

Mitre - Initial Access - Valid Accounts - Impossible Travel

- **Trigger Condition:** A user logs in from more than one GeoIP location.
- **ATT&CK Category:** Initial Access, Persistence, Privilege Escalation and Defense Evasion
- **ATT&CK Tag:** Valid Accounts
- **ATT&CK ID:** T1078
- **Minimum Log Source Requirement:** Windows
- **Query:**

- `label=User label=Login source_address=* | process geoip(source_address) as country | chart distinct_count(country) as DC, distinct_list(country) as countries by user | search DC>1`

Mitre - Initial Access - Valid Accounts - Inactive User Accounts

- **Trigger Condition:** User accounts are inactive for more than 30 days.
- **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:**
- `table AD_Users -lastLogon=0 lastLogon=* | process current_time(a) as time| chart max((time- (lastLogon/10000000 - 11644473600))/60/60/24) as number_of_days by sAMAccountName | search number_of_days>29`

Mitre Command and Control Using Uncommonly used Port Detected

- **Trigger Condition:** Command and Control activity using uncommonly used ports is detected.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Non-Standard Port
- **ATT&CK ID:** T1571
- **Minimum Log Source Requirement:** Proxy Server
- **Query:**
- `norm_id=*Proxy* source_address=* destination_address=* destination_port IN COMMON_PORTS | process ti(destination_address)| rename et_category as ti_category | process eval("attack_class='Command and Control'")| process eval("technique='Commonly Used Port'") | search ti_category="*Command and Control*"`

Mitre Credential Access Using Credentials from Web Browsers Detected

- **Trigger Condition:** Credential Access is detected using credentials from password stores and credentials from web browsers.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Credentials from Password Stores, Credentials from Web Browsers
- **ATT&CK ID:** T1555, T1555.003
- **Minimum Log Source Requirement:** Windows
- **Query:**

- ```
  norm_id=WinServer label=Object label=Access label=File "process"="*wsus.exe" (path="*firefox*" OR path="*chrome*") -user IN EXCLUDED_USERS | process eval("attack_class='Credential Access'")| process eval("technique='Credentials from Web Browsers'") | chart count() by user, domain, host, log_ts, path, file, attack_class, technique order by count() desc limit 10
  ```

Mitre Credential Access Using Credentials in File Detected

- **Trigger Condition:** Credential Access using attack technique Credentials in File is detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Credentials in Files
- **ATT&CK ID:** T1552, T1552.001
- **Minimum Log Source Requirement:** Windows
- **Query:**
- ```
  norm_id=WinServer label="Process" label=Create (commandline="*laZagne*.exe*" OR command="*laZagne*.exe*") -user IN EXCLUDED_USERS | process eval("attack_class='Credential Access'")| process eval("technique='Credentials in File'") | rename commandline as command | chart count() by user, host, domain, log_ts, command, attack_class, technique order by count() desc limit 10
  ```

Mitre Defense Evasion Using Decode Files or Information Detected

- **Trigger Condition:** Defense evasion uses decode files or information.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Deobfuscate/Decode Files or Information
- **ATT&CK ID:** T1140
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
- ```
  norm_id=WinServer label="Process" label=Create (command="*certutil.exe*" OR commandline="*certutil.exe*") -user IN EXCLUDED_USERS| process eval("attack_class='Defense Evasion'")| process eval("technique='Deobfuscate/Decode Files or Information'")| rename commandline as command
  ```

Mitre Defense Evasion Using File Deletion Detected

- **Trigger Condition:** Defense evasion uses file deletion technique.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Data Destruction, Indicator Removal on Host, File Deletion
- **ATT&CK ID:** T1485, T1070, T1070.004
- **Minimum Log Source Requirement:** Windows
- **Query:**
  ```

- ```
  norm_id=WinServer label=Object label=Access access="*delete*" (relative_target="*.exe" OR relative_target="*.bat") -user IN EXCLUDED_USERS | process eval("attack_class='Defense Evasion'")| process eval("technique='File Deletion'") | rename relative_target as file
  ```

Mitre Discovery Using Account Discovery Detected

- **Trigger Condition:** An attack Discovery uses an attack technique Account Discovery.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Account Discovery
- **ATT&CK ID:** T1087
- **Minimum Log Source Requirement:** Windows
- **Query:**
- ```
  norm_id=WinServer label="Process" label=Create (commandline="*dsquery*" OR command="*dsquery*") -user IN EXCLUDED_USERS | process eval("attack_class='Discovery'")| process eval("technique='Account Discovery'") | rename commandline as command | chart count() by user, host, domain, log_ts, command, attack_class, technique order by count() desc limit 10
  ```

Mitre Discovery Using File and Directory Discovery Detected

- **Trigger Condition:** Discovery uses an attack technique File and Directory Discovery.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** File and Directory Discovery
- **ATT&CK ID:** T1083
- **Minimum Log Source Requirement:** Windows
- **Query:**
- ```
  norm_id=WinServer label="Process" label=Create -commandline="*findstr*" (commandline="*cmd.exe*dir *" OR commandline="*tree.com*") -user IN EXCLUDED_USERS | process eval("attack_class='Discovery'")| process eval("technique='File and Directory Discovery'") | rename commandline as command | chart count() by user, host, domain, log_ts, command, attack_class, technique order by count() desc limit 10
  ```

Mitre Discovery Using Network Service Scanning Detected

- **Trigger Condition:** Discovery uses an attack technique Network Service Scanning.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Network Service Scanning
- **ATT&CK ID:** T1046
- **Minimum Log Source Requirement:** Windows
  ```

- **Query:**

```
norm_id=WinServer label="Process" label=Create (commandline="*nmap*" OR commandline="*RpcPing.exe*" OR commandline="*telnet.exe*") -user IN EXCLUDED_USERS | process eval("attack_class='Discovery'")| process eval("technique='Network Service Scanning'") | rename commandline as command | chart count() by user, host, domain, log_ts, command, attack_class, technique order by count() desc limit 10
```

Mitre Discovery Using Network Sniffing Detected

- **Trigger Condition:** Discovery uses an attack technique Network Sniffing.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Network Sniffing
- **ATT&CK ID:** T1040
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer label="Process" label=Create commandline="*tshark.exe*" -user IN EXCLUDED_USERS | process eval("attack_class='Discovery'")| process eval("technique='Network Sniffing'") | rename commandline as command | chart count() by user, host, domain, log_ts, command, attack_class, technique order by count() desc limit 10
```

Mitre Discovery Using Password Policy Discovery Detected

- **Trigger Condition:** Discovery uses an attack technique Password Policy Discovery.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Password Policy Discovery
- **ATT&CK ID:** T1201
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer label="Process" label=Create commandline="*net.exe* accounts*" -user IN EXCLUDED_USERS | process eval("attack_class='Discovery'")| process eval("technique='Password Policy Discovery'") | rename commandline as command | chart count() by user, host, domain, log_ts, command, attack_class, technique order by count() desc limit 10
```

Mitre Discovery Using Permission Groups Discovery Detected

- **Trigger Condition:** Discovery uses an attack technique Permission Groups Discovery.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Permission Groups Discovery
- **ATT&CK ID:** T1069

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

```
norm_id=WinServer label="Process" label=Create (command="*net*localgroup*" OR command="*net*group*" OR command="*get*localgroup*" OR commandline="*net*localgroup*" OR commandline="*net*group*" OR commandline="*get*localgroup*") -user IN EXCLUDED_USERS | process eval("attack_class='Discovery'")| process eval("technique='Permission Groups Discovery'") | rename commandline as command | chart count() by user, host, domain, log_ts, command, attack_class, technique order by count() desc limit 10
```

Mitre Discovery Using Query Registry Detected

- **Trigger Condition:** Discovery uses an 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
```

Mitre Discovery Using Security Software Discovery Detected

- **Trigger Condition:** Discovery uses an attack techniques Software Discovery and Security Software Discovery.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Software Discovery, Security Software Discovery
- **ATT&CK ID:** T1518, T1518.001
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer label="Process" label=Create (commandline="*findstr.exe*virus" OR commandline="*findstr.exe*cylance" OR commandline="*findstr.exe*defender" OR commandline="*findstr.exe*cb") -user IN EXCLUDED_USERS | process eval("attack_class='Discovery'")| process eval("technique='Security Software Discovery'") | rename commandline as command |
chart count() by user, host, domain, log_ts, command, attack_class, technique order by count() desc limit 10
```

Mitre Discovery Using System Information Discovery Detected

- **Trigger Condition:** Discovery uses an attack technique System Information Discovery.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** System Information Discovery
- **ATT&CK ID:** T1082
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer label="Process" label=Create commandline="*net.exe*config*" -user IN EXCLUDED_USERS | process eval("attack_class='Discovery'") | process eval("technique='System Information Discovery'") | rename commandline as command | chart count() by user, host, domain, log_ts, command, attack_class, technique order by count() desc limit 10
```

Mitre Discovery Using System Network Configuration Discovery Detected

- **Trigger Condition:** Discovery uses an 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
```

Mitre Discovery Using System Owner or User Discovery Detected

- **Trigger Condition:** Discovery uses an attack technique System Owner or User Discovery.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** System Owner/User Discovery
- **ATT&CK ID:** T1033
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer label="Process" label=Create (commandline="*whoami*" OR commandline="*quser*" OR commandline="*wmic.exe*useraccount get*") -user IN EXCLUDED_USERS | process eval("attack_class='Discovery'")| process eval("technique='System Owner/User Discovery'") | rename commandline as
```

```
command | chart count() by user, host, domain, log_ts, command, attack_class, technique order by count() desc limit 10
```

Mitre Discovery Using System Service Discovery Detected

- **Trigger Condition:** Discovery uses an attack technique System Service Discovery.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** System Service Discovery
- **ATT&CK ID:** T1007
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer label="Process" label=Create (commandline="*net.exe*start*" OR commandline="*tasklist.exe*") -user IN EXCLUDED_USERS | process eval("attack_class='Discovery'")| process eval("technique='System Service Discovery'") | rename commandline as command | chart count() by user, host, domain, log_ts, command, attack_class, technique order by count() desc limit 10
```

Mitre Exfiltration Over Alternative Protocol Detected

- **Trigger Condition:** LogPoint detects exfiltration of data over alternative protocol.
- **ATT&CK Category:** Exfiltration
- **ATT&CK Tag:** Exfiltration Over Alternative Protocol Detected
- **ATT&CK ID:** T1048
- **Minimum Log Source Requirement:** Proxy Server
- **Query:**

```
norm_id=*Proxy* source_address=* destination_address=* destination_address IN CLOUD_APPLICATION_IP | process eval("attack_class='Exfiltration'") | process eval("technique='Exfiltration Over Alternative Protocol'")
```

Mitre Lateral Movement Using Remote Services Detected

- **Trigger Condition:** Lateral Movement uses an attack technique Remote Services.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Exploitation of Remote Services
- **ATT&CK ID:** T1210
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=7045 start_type="auto start" service="remotesvc" -user IN EXCLUDED_USERS | process eval("attack_class='Lateral Movement'")| process eval("technique='Remote Services'") | chart count() by user, image, log_ts, service, service_type, attack_class, technique order by count() desc limit 10
```

Mitre Persistence Attack through Accessibility Process Feature

- **Trigger Condition:** An OS's accessibility features are used adversely to get a command prompt or backdoor without logging in to the system.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Event Triggered Execution, Accessibility Features
- **ATT&CK ID:** T1546, T1546.008
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
(label="Process" label=Create "process" IN PERSISTENCE_ACCESSIBILITY_PROCESS) OR (parent_image IN PERSISTENCE_ACCESSIBILITY_PROCESS) OR (target_object IN PERSISTENCE_ACCESSIBILITY_OBJECT) -user IN EXCLUDED_USERS
```

Mitre Persistence Attack through AppInit DLLs

- **Trigger Condition:** Suspicious AppInit_DLL functionality is detected in an environment that could be a persistence attack.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Event Triggered Execution, AppInit DLLs
- **ATT&CK ID:** T1546, T1546.01
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
(target_object="HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs" OR target_object="HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows\LoadAppInit_DLLs")
```

Mitre Persistence Using Account Creation Detected

- **Trigger Condition:** The creation of an account with persistence is detected.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Account Manipulation
- **ATT&CK ID:** T1098
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer label="Process" label=Create commandline="*net*/add /y" -user IN EXCLUDED_USERS | process eval("attack_class='Persistence'")| process eval("technique='Create Account'") | rename commandline as command
```

Mitre Persistence Using Account Manipulation Detected

- **Trigger Condition:** Persistence uses an attack technique Account Manipulation.

- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Account Manipulation
- **ATT&CK ID:** T1098
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer label="Process" label=Create commandline="*net.exe*localgroup*/add" -user IN EXCLUDED_USERS | process eval("attack_class='Persistence'")| process eval("technique='Account Manipulation'") | rename commandline as command
```

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
```

Mitre Possible Privilege Escalation using Application Shimming

- **Trigger Condition:** Installation or registration of shim databases to escalate privilege in an environment is detected.
- **ATT&CK Category:** Privilege Escalation
- **ATT&CK Tag:** Event Triggered Execution, Application Shimming
- **ATT&CK ID:** T1546, T1546.011
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
('process'=*sdbinst.exe OR image=*sdbinst.exe OR target_object IN APPLICATION_SHIM_OBJECTS) | rename 'process' as image
```

Mitre Privilege Escalation Using Bypass User Access Control Detected

- **Trigger Condition:** Privilege Escalation using Abuse Elevation Control Mechanism or Bypass User Access Control is detected.
- **ATT&CK Category:** Privilege Escalation
- **ATT&CK Tag:** Abuse Elevation Control Mechanism, Bypass User Access Control
- **ATT&CK ID:** T1548
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

- `(norm_id=WindowsSysmon 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 | process eval("attack_class='Privilege Escalation'")| process eval("technique='Bypass User Access Control'") | rename commandline as command`

MMC Spawning Windows Shell Detected

- **Trigger Condition:** Windows command line executable starting from MMC is detected.
- **ATT&CK Category:** Execution, Defense Evasion
- **ATT&CK Tag:** Command and Scripting Interpreter, Indirect Command Execution
- **ATT&CK ID:** T1059, T1202
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
- `norm_id=WindowsSysmon event_id=1 parent_image="*\mmc.exe" image IN ["*\cmd.exe", "*\powershell.exe", "*\wscript.exe", "*\cscript.exe", "*\sh.exe", "*\bash.exe", "*\reg.exe", "*\regsvr32.exe", "*\BITSADMIN*"] -user IN EXCLUDED_USERS`

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`

MS Office Product Spawning Exe in User Dir

- **Trigger Condition:** An executable in the users directory from Microsoft Word, Excel, Powerpoint, Publisher, or Visio is detected.
- **ATT&CK Category:** Execution, Defense Evasion
- **ATT&CK Tag:** Command-Line Interface, Indirect Command Execution
- **ATT&CK ID:** T1059, T1202
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
- `norm_id=WindowsSysmon event_id=1 parent_image IN ["*\WINWORD.EXE", "*\EXCEL.EXE", "*\POWERPNT.exe", "*\MSPUB.exe", "*\VISIO.exe", "*\OUTLOOK.EXE"] image IN ["C:\users\*.exe"] -user IN EXCLUDED_USERS`

MSHTA - File Access Detected

- **Trigger Condition:** Creation of a file with *.hta* extension. 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=11 or event_id=15) file="*.hta*" -user IN EXCLUDED_USERS
```

MSHTA - Activity Detected

- **Trigger Condition:** LogPoint detects network connection events initiated by *mshta.exe*. 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
```

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
```

MSHTA Spawning Windows Shell Detected

- **Trigger Condition:** Windows command line executable started from MSHTA 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 parent_image="*\mshta.exe" image IN ["*\cmd.exe", "*\powershell.exe", "*\wscript.exe", "*\cscript.exe", "*\sh.exe", "*\bash.exe", "*\reg.exe", "*\regsvr32.exe", "*\BITSADMIN*"] -user IN EXCLUDED_USERS
```

MSHTA Spwaned by SVCHOST Detected

- **Trigger Condition:** *mshta.exe* spawned by SVCHOST observed in LethalHTA 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 parent_image="*\svchost.exe" image="*\mshta.exe" -user IN EXCLUDED_USERS
```

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
```

MsiExec Web Install Detected

- **Trigger Condition:** The *msiexec* process starts with the web address as a parameter.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Signed Binary Proxy Execution, Msiexec
- **ATT&CK ID:** T1218, T1218.007
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 command="* msiexec*://*" -user IN EXCLUDED_USERS
```

MSTSC Shadowing Detected

- **Trigger Condition:** Hijacking of Remote Desktop Protocol (RDP) session using Microsoft Terminal Services Client (MSTSC) shadowing is detected.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Remote Service Session Hijacking, RDP Hijacking
- **ATT&CK ID:** T1563, T1563.002
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**
- ```
  label=Create label="Process" command="*noconsentprompt*" command="*shadow:*" -user IN EXCLUDED_USERS
  ```
  ```