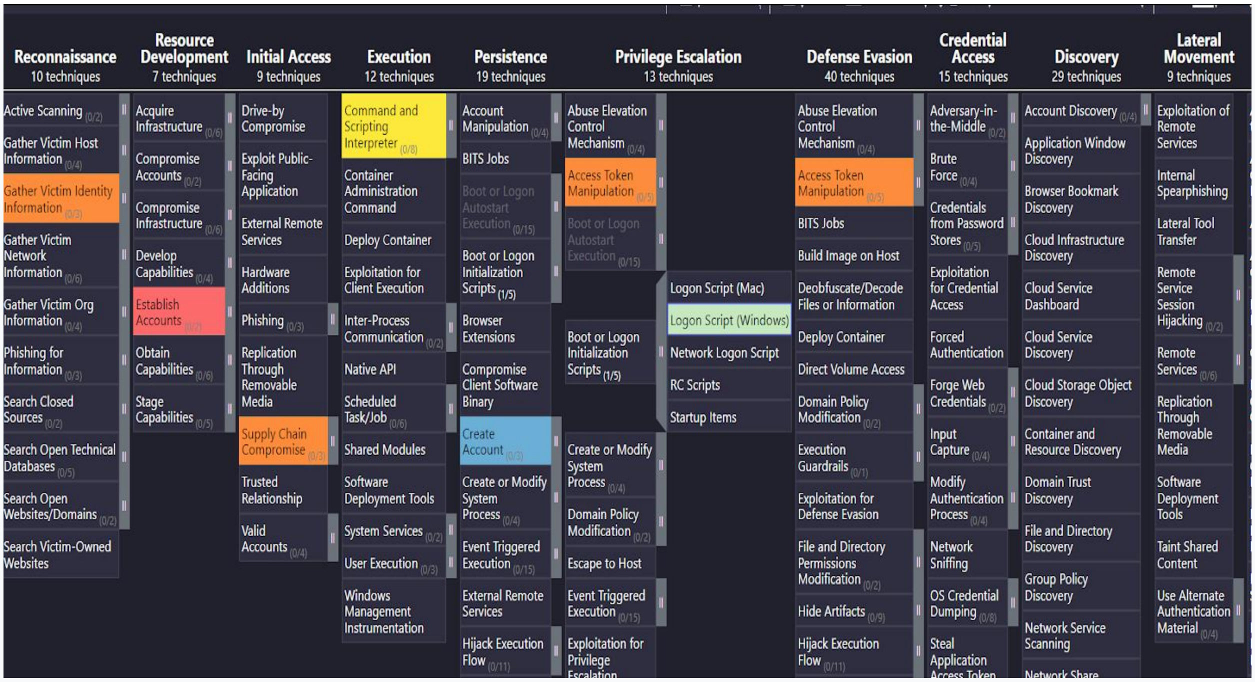

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques		Defense Evasion 40 techniques	Credential Access 15 techniques	Discovery 29 techniques	Lateral Movement 9 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Logon Script (Mac)	Abuse Elevation Control Mechanism (0/4)	Adversary-in-the-Middle (0/2)	Account Discovery (0/4)	Exploitation of Remote Services
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Logon Script (Windows)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (0/15)	Boot or Logon Autostart Execution (0/15)	Network Logon Script	BITS Jobs	Credentials from Password Stores (0/5)	Browser Bookmark Discovery	Lateral Tool Transfer
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (1/5)	Boot or Logon Initialization Scripts (1/5)	RC Scripts	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Inter-Process Communication (0/2)	Browser Extensions	Create or Modify System Process (0/4)	Startup Items	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services (0/6)
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (0/2)		Deploy Container	Forge Web Credentials (0/2)	Cloud Service Discovery	Replication Through Removable Media
Search Closed Sources (0/2)	Stage Capabilities (0/5)	Supply Chain Compromise (0/3)	Scheduled Task/Job (0/6)	Create Account (0/3)	Escape to Host		Direct Volume Access	Input Capture (0/4)	Cloud Storage Object Discovery	Software Deployment Tools
Search Open Technical Databases (0/5)		Trusted Relationship	Shared Modules	Create or Modify System Process (0/4)	Event Triggered Execution (0/15)		Domain Policy Modification (0/2)	Modify Authentication Process (0/4)	Container and Resource Discovery	Taint Shared Content
Search Open Websites/Domains (0/2)		Valid Accounts (0/4)	Software Deployment Tools	Event Triggered Execution (0/15)	Exploitation for Privilege Escalation		Execution Guardrails (0/1)	Network Sniffing	Domain Trust Discovery	Use Alternate Authentication Material (0/4)
Search Victim-Owned Websites			System Services (0/2)	External Remote Services			Exploitation for Defense Evasion	OS Credential Dumping (0/8)	File and Directory Discovery	
			User Execution (0/3)	Hijack Execution Flow (0/11)			File and Directory Permissions Modification (0/2)	Steal Application Access Token	Group Policy Discovery	
			Windows Management Instrumentation				Hide Artifacts (0/9)		Network Service Scanning	
							Hijack Execution Flow (0/11)		Network Share	

MITRE ATTACKS DETECTION RULES PART2

The MITRE ATT&CK Alerts For log point

Parastoo Razi

Multiple Failed Login Followed by Successful Login Followed by Logoff

- **Trigger Condition:** Multiple failed login attempts are followed by successful login, and then by log off from the same user are detected.
- **ATT&CK Category:** Defense Evasion, Persistence, Privilege Escalation, Initial Access, Credential Access
- **ATT&CK Tag:** Valid Accounts, Brute Force
- **ATT&CK ID:** T1078, T1110
- **Minimum Log Source Requirement:** Windows
- **Query:**
-
  ```
  [incident_name="Multiple Failed User Login Followed by Successful Login" incident_user=*] as FirstAlert followed by [norm_id=WinServer* label=User label=Logoff user=* -user IN EXCLUDED_USERS] as Logoff on FirstAlert.incident_user=Logoff.user | rename Logoff.user as User, FirstAlert.incident_address as SourceAddress
  ```

Mustang Panda Dropper Detected

- **Trigger Condition:** Specific process parameters used by Mustang Panda droppers are detected.
- **ATT&CK Category:** Resource Development, Defense Evasion
- **ATT&CK Tag:** Exploitation for Defense Evasion, Malware
- **ATT&CK ID:** T1211, T1587.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**
-
  ```
  label=Create label="Process" ((command in ["*Temp\wtask.exe /create*", "*%windir:~-3,1%%PUBLIC:~-9,1%*", "*/tn *Security Script*", "*%windir:~-1,1%*"] command ="*/E:vbscript*:\Users*.txt*/F*") OR ("process"="*\Temp\winwsh.exe"))
  ```

Named Pipe added to Null Session Detected

- **Trigger Condition:** Lateral Movement attempt by enabling of null session through named pipe is detected.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Remote Services
- **ATT&CK ID:** T1021
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

-
  ```
  norm_id=WindowsSysmon event_id=13 image="*reg.exe" target_object="*lanmanserver*NullSessionPipes" detail="Binary Data" -user IN EXCLUDED_USERS
  ```

Narrators Feedback-Hub Persistence Detected

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

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

Nefilim Ransomware Infected Host Detected

- **Trigger Condition:** Nefilim 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 NEFILIM_RANSOMWARE_HASHES
  ```

Net exe Execution Detected

- **Trigger Condition:** The execution of *Net.exe*, which can be suspicious or benign, is detected.
- **ATT&CK Category:** Lateral Movement, Discovery, Defense Evasion
- **ATT&CK Tag:** Obfuscated Files or Information, System Network Connections Discovery, Remote Services, Network Share Discovery
- **ATT&CK ID:** T1027, T1049, T1021, T1135
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

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

Net exe User Account Creation

- **Trigger Condition:** The creation of local users via the net.exe command is detected.
- **ATT&CK Category:** Persistence, Credential Access
- **ATT&CK Tag:** Create Account
- **ATT&CK ID:** T1136
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 image IN ["*\net.exe", "*\net1.exe"] command="*user*" command="*add*" -user IN EXCLUDED_USERS
```

NetNTLM Downgrade Attack Detected

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

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

Firewall Addition via Netsh Detected

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

```
norm_id=WindowsSysmon event_id=1 command IN ["*netsh firewall add*"] -user IN EXCLUDED_USERS
```

Netsh Helper DLL - Process Detected

- **Trigger Condition:** Adversaries use Netshell helper DLLs to execute arbitrary code persistently. *Netsh.exe* is a command-line scripting utility used to interact with the network configuration of a system.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Event Triggered Execution, Netsh Helper DLL
- **ATT&CK ID:** T1546, T1546.007
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

-
  ```
  norm_id=WindowsSysmon event_id=1 (image="*netsh.exe" command="*helper*") -user IN EXCLUDED_USERS
  ```

Netsh Helper DLL - Registry Detected

- **Trigger Condition:** Windows registry at *HKLMSOFTWAREMicrosoftNetsh* is detected. *HKLMSOFTWAREMicrosoftNetsh* is a path to registered *netsh.exe* helper DLLs.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Event Triggered Execution, Netsh Helper DLL
- **ATT&CK ID:** T1546, T1546.007
- **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\Netsh\*" -user IN EXCLUDED_USERS
  ```

Netsh Port Forwarding Detected

- **Trigger Condition:** The *netsh* command used in the configuration of port forwarding is detected. Port forwarding is a pivoting technique that redirects traffic from one port to another.
- **ATT&CK Category:** Lateral Movement, Command and Control
- **ATT&CK Tag:** Proxy, Exploitation of Remote Services
- **ATT&CK ID:** T1090, T1210
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

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

Netsh RDP Port Forwarding Detected

- **Trigger Condition:** The *netsh* command used in the configuration of port forwarding of port 3389 for RDP is detected.
- **ATT&CK Category:** Lateral Movement

- **ATT&CK Tag:** Remote Services
- **ATT&CK ID:** T1021
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

-
  ```
  norm_id=WindowsSysmon event_id=1 command IN ["netsh i* p*=3389 c*"] -user IN EXCLUDED_USERS
  ```

Network Share Connection Removed

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

-
  ```
  norm_id=WindowsSysmon event_id=1 (image="*net.exe" command="*net delete*") or command="*Remove-SmbShare*" or command="*Remove-FileShare*" -user IN EXCLUDED_USERS
  ```

Network Share Discovery

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

-
  ```
  norm_id=WindowsSysmon event_id=1 (image="*net.exe" (command="*net view*" or command="*net share*")) or command="*get-smbshare -Name*" -user IN EXCLUDED_USERS
  ```

Network Sniffing Detected

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

- **ATT&CK Tag:** Network Sniffing
- **ATT&CK ID:** T1040
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  norm_id=WindowsSysmon event_id=1 (image="*tshark.exe" or image="*windump.exe" or image="*logman.exe" or image="*tcpdump.exe" or image="*wprui.exe" or image="*wpr.exe") -user IN EXCLUDED_USERS
  ```

New Driver File Creation Detected

- **Trigger Condition:** Creation of a new driver file.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Shared Modules
- **ATT&CK ID:** T1129
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  norm_id=WindowsSysmon event_id=11 path="C:\Windows*Drivers*" -user IN EXCLUDED_USERS
  ```

New Firewall Port Opening Detected

- **Trigger Condition:** An opening of a new port in a firewall is detected.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Non-Standard Port
- **ATT&CK ID:** T1571
- **Minimum Log Source Requirement:** Windows
- **Query:**
-
  ```
  norm_id=WinServer event_id=4657 object=FirewallRules event_category=Registry  object_name="*ControlSet*FirewallPolicy\FirewallRules"  new_value=* -user IN EXCLUDED_USERS | norm on new_value <:all>Action=<action:word><:all>Active=<active:word><:all>Dir=<direction:word><:all>Protocol=<proto:int><:all>Port=<port:int><:all>Name=<rule:string><:'\|'> | process eval("protocol = if(proto == 6) {return 'TCP'} else {return 'UDP'}")
  ```

New RUN Key Pointing to Suspicious Folder Detected

- **Trigger Condition:** A new suspicious RUN key element pointing to an executable in a folder is detected.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Boot or Logon Autostart Execution, Registry Run Keys/Startup Folder
- **ATT&CK ID:** T1547, T1547.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  event_id=13 target_object IN ["*\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\*", "*\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\*"] detail IN ["*C:\Windows\Temp\*", "*\AppData\*", "%AppData%\*", "*C:\$Recycle
  ```

```
.bin\*", "*C:\Temp\*", "*C:\Users\Public\*", "%Public%\*", "*C:\Users\Default\*", "*C:\Users\Desktop\*", "wscript*", "cscript*"] -detail IN ["*\AppData\Local\Microsoft\OneDrive\\*"] -user IN EXCLUDED_USERS
```

New Service Creation

- **Trigger Condition:** When the creation of a new service is detected. Windows Services can allow the creation and management of long-running processes. It can start automatically and keep running for a long time after the user logs off. Adversaries might leverage this functionality to maintain persistence and escalate their privilege.
- **ATT&CK Category:** Persistence, Privilege Escalation
- **ATT&CK Tag**: T1543 - Create or Modify System Process (2), T1543.003 - Windows Service (2)
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Create" label="Process" "process" IN ["*sc.exe", "*powershell.exe", "*cmd.exe"] command IN ["*New-Service*BinaryPathName*", "*sc*create*binpath*", "*Get-WmiObject*Win32_Service*create*"] -user IN EXCLUDED_USERS
```

Non Interactive PowerShell Execution

- **Trigger Condition:** Non-interactive Command and Scripting Interpreter and PowerShell activity by looking at *powershell.exe* with no *explorer.exe* as a parent.
- **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" -parent_Image="*\explorer.exe" -user IN EXCLUDED_USERS
```

NoPowerShell Tool Activity Detected

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

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

NotPetya Ransomware Activity Detected

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

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

OceanLotus Registry Activity Detected

- **Trigger Condition:** Creation of registry keys in OceanLotus attacks, which is also known as APT32.
- **ATT&CK Category:** Persistence, Defense Evasion
- **ATT&CK Tag:** Modify Registry
- **ATT&CK ID:** T1112
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
event_id=13 target_object IN ["HKCR\CLSID\{E08A0F4B-1F65-4D4D-9A09-BD4625B9C5A1}\Model", "HKU\*_Classes\CLSID\{E08A0F4B-1F65-4D4D-9A09-BD4625B9C5A1}\Model",
"*\SOFTWARE\App\AppXbf13d4ea2945444d8b13e2121cb6b663\Application",
"*\SOFTWARE\App\AppXbf13d4ea2945444d8b13e2121cb6b663\DefaultIcon","*\SOFTWARE\App\AppX70162486c7554f7f80f481985d67586d\Application",
"*\SOFTWARE\App\AppX70162486c7554f7f80f481985d67586d\DefaultIcon",
"*\SOFTWARE\App\AppX37cc7fdccd644b4f85f4b22d5a3f105a\Application", "*\SOFTWARE\App\AppX37cc7fdccd644b4f85f4b22d5a3f105a\DefaultIcon",
"HKU\*_Classes\AppXc52346ec40fb4061ad96be0e6cb7d16a\*", "HKU\*_Classes\AppX3bbba44c6cae4d9695755183472171e2\*",
"HKU\*_Classes\CLSID\{E3517E26-8E93-458D-A6DF-8030BC80528B}\*"]
-user IN EXCLUDED_USERS
```

Office365 Multiple Failed Login from Different Host by Single User

- **Trigger Condition:** A user attempts multiple failed logins from distinct hosts with a count greater than one.
- **ATT&CK Category:** Credential Access, Persistence, Defense Evasion, Privilege Escalation, Initial Access

- **ATT&CK Tag:** Brute Force, Valid Accounts
- **ATT&CK ID:** T1110, T1078
- **Minimum Log Source Requirement:** Office365
- **Query:**

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

Office365 Multiple Failed Login from Same Host

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

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

Office365 Multiple Successful Login from Different Country by Single User

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

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

Office365 Multiple Successful Login From Different Host by Single User

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

- **Query:**

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

Office365 Password Resets

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

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

OpenWith Execution of Specified Binary Detected

- **Trigger Condition:** The execution of _OpenWith.exe_ is detected as a specified binary. It characterized as a malicious activity when executed from a location other than _C:WindowsSystem32*_ path.
- **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="*\OpenWith.exe" command="*/c*" -user IN EXCLUDED_USERS
  ```

Possible Operation Wocao Activity Detected

- **Trigger Condition:** Activity mentioned in Operation Wocao report is detected.
- **ATT&CK Category:** Defense Evasion,Execution, Persistence, Privilege Escalation
- **ATT&CK Tag:** Exploitation for Defense Evasion, Obfuscated Files or Information, Masquerade Task or Service, Masquerading, Scheduled Task/Job, Scheduled Task
- **ATT&CK ID:** T1211, T1012, T1036, T1036.004, T1053, T1053.005
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

-
  ```
  ((norm_id=WinServer event_id=4799 group="Administrators" "process"="*\checkadmin.exe") OR (norm_id=WindowsSysmon event_id=1 command IN ["*checkadmin.exe 127.0.0.1 -all*", "*netsh advfirewall firewall add rule name=powershell dir=in*", "*cmd /c powershell.exe -ep bypass -file c:\s.ps1*", "*/tn win32times /f*", "*create win32times binPath=*", "*\c$\windows\system32\devmgr.dll*", "* -exec bypass -enc JgAg*", "*type *keepass\KeePass.config.xml*", "*iie.exe iie.txt*", "*reg query HKEY_CURRENT_USER\Software\\*\PuTTY\Sessions\\*"])) -user IN EXCLUDED_USERS
  ```

Pandemic Registry Key Detected

- **Trigger Condition:** LogPoint detects pandemic Windows implant. It turns file servers into patient zero on a local network, infecting machines requesting files with trojanized replacements.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Remote File Copy
- **ATT&CK ID:** T1105
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  (event_id=13 target_object IN ["HKLM\SYSTEM\CurrentControlSet\services\null\Instance*"]) OR (event_id=1 command="loaddll -a *")
  ```

Password Change on DSRM Account Detected

- **Trigger Condition:** Password change in Directory Service Restore Mode (DSRM) account is detected.
- **ATT&CK Category:** Persistence, Privilege Escalation
- **ATT&CK Tag:** Account Manipulation
- **ATT&CK ID:** T1098
- **Minimum Log Source Requirement:** Windows
- **Query:**
-
  ```
  norm_id=WinServer event_id=4794 -user IN EXCLUDED_USERS
  ```

Password Dumper Remote Thread in LSASS

- **Trigger Condition:** Password dumper activity by monitoring remote thread creation event ID 8 in combination with the lsass.exe process as *TargetImage* is detected. The process in the field *Process* is a malicious program and a single execution can lead to hundreds of events.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  norm_id=WindowsSysmon event_id=8 image="C:\Windows\System32\lsass.exe" -start_module=* -user IN EXCLUDED_USERS
  ```

Password Spraying Attack Detected

- **Trigger Condition:** Password spraying attack is detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Brute Force
- **ATT&CK ID:** T1110
- **Minimum Log Source Requirement:** Windows

- **Query:**

-
  ```
  norm_id=WinServer event_id=4625 -user IN EXCLUDED_USERS -user IN EXCLUDED_USERS | chart distinct_count(user) as UserCount, distinct_list(user) as Users by source_address | search UserCount > 5
  ```

Persistence and Execution at Scale via GPO Scheduled Task

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

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

Petya Affected Hosts

- **Trigger Condition:** Applications and commands like wevtutil,wmic,rundll,or schtasks are executed for defense evasion. For this alert to work, you must update the list PETYA_COMMAND.
- **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:**

-
  ```
  norm_id=WinServer* event_id=106 event_source="Microsoft-Windows-TaskScheduler" task IN PETYA_COMMAND -user IN EXCLUDED_USERS
  ```

Petya Compromised Files

- **Trigger Condition:** A file with IOC's of Petya file digest value 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:** Integrity Scanner
- **Query:**

-
  ```
  norm_id=IntegrityScanner digest IN PETYA_DIGEST OR prev_digest IN PETYA_DIGEST path=*
  ```

Ping Hex IP Detected

- **Trigger Condition:** Ping command using a hex-encoded IP address is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Deobfuscate/Decode Files or Information, Obfuscated Files or Information
- **ATT&CK ID:** T1140, T1027
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  norm_id=WindowsSysmon event_id=1 command IN ["*\ping.exe 0x*", "*\ping 0x*"] -user IN EXCLUDED_USERS
  ```

Ping of Death Attack

- **Trigger Condition:** Datagrams with a size greater than 65536 are received.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Network Denial of Service, Direct Network Flood
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  label=Receive label=Packet (packet_length>65536 or fragment_length>65536)
  ```

Possible Access to ADMIN Share

- **Trigger Condition:** Access to $ADMIN share and may help to detect lateral movement attempts. Since Windows Admin Share activity is so common, it provides adversaries with a powerful, discreet way to move laterally within an environment. Self-propagating ransomware and cryptocurrency miners, both rapidly emerging threats, rely on Windows Admin Shares. Suppose an adversary can obtain legitimate Windows credentials. The hidden shares (C$, ADMIN$, and IPC$) can be accessed remotely via server message block (SMB) or the Net utility to transfer files and execute code. Windows Admin Shares are often used in conjunction with behaviors relating to Remote File Copy (T1105)—because adversaries commonly use the technique to copy files remotely—and Network Share Discovery (T1135). It can also occur with New Service (T1050) and Service Execution (T1035) because tools like PsExec deploys their receiver executable to admin shares, scheduling a service to execute it. Legitimate administrative activities may generate false positives and will require whitelisting.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Remote Services
- **ATT&CK ID:** T1021
- **Minimum Log Source Requirement:** Windows
- **Query:**
-
  ```
  norm_id=WinServer event_id=5140 share_name="Admin$" -user="*$" -user IN EXCLUDED_USERS
  ```

Possible Account Misuse-Abnormal Login

- **Trigger Condition:** Admin is logged in or running an application beyond regular office hours is detected.
- **ATT&CK Category:** Initial Access, Privilege Escalation, Defense Evasion, Persistence
- **ATT&CK Tag:** Valid Accounts
- **ATT&CK ID:** T1078
- **Minimum Log Source Requirement:** Windows
- **Query:**
-
  ```
  (label=User label=Login label=Successful user in ADMINS ((day_of_week(log_ts) IN ["Monday", "Tuesday", "Wednesday", "Thursday", "Friday"]) and (hour(log_ts)<9 or hour(log_ts)>17)) or (day_of_week(log_ts) IN ["Saturday", "Sunday"] )) or (label=User label=Login label=Successful sub_status_code="0xC000006F") user=* (workstation=* or source_address=*)
  ```

Possible Account Misuse-Privilege Escalation

- **Trigger Condition:** The non-admin users are assigned privileged access. The event maps to event ID of 4648 and 4672 in Windows.
- **ATT&CK Category:** Privilege Escalation, Persistence, Defense Evasion
- **ATT&CK Tag:** Account Manipulation, Abuse Elevation Control Mechanism, Bypass User Account Control
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Windows
- **Query:**
-
  ```
  ((label=Privilege label=Assign) or (label=Login label=Explicit label=Credential) user=* -user in ADMINS) OR (label=User label=Add label=Group user=* group=*admin*)
  ```

Possible Applocker Bypass Detected

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

Possible Bitsadmin Download Detected

- **Trigger Condition:** The use of *bitsadmin* downloading a file is detected.
- **ATT&CK Category:** Defense Evasion, Persistence
- **ATT&CK Tag:** BITS Jobs
- **ATT&CK ID:** T1197
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**
-
```
label="Process" label=Create ("process"="*\bitsadmin.exe"  (command IN ["* /create *","* /addfile *"] command="*http*") OR (command="* /transfer *")) OR (command="*copy bitsadmin.exe*") -user IN EXCLUDED_USERS
```

Possible Botnet Connection-DNS Server Modified

- **Trigger Condition:** An unauthorized default Application Layer Protocol and DNS server modification are detected in Unix or Windows Server.
- **ATT&CK Category:** Impact, Command and Control, Defense Evasion
- **ATT&CK Tag:** Network Denial of Service, Proxy, Exploitation for Defense Evasion
- **ATT&CK ID:** T1498, T1090, T1211
- **Minimum Log Source Requirement:** Windows
- **Query:**
-
```
((norm_id=Unix action="RUN" (file="etc/resolv.conf" or file="*\etc\host")) or (norm_id=WinServer* (label=File (label=Write or label=Modify) path="C:\Windows\System32\Drivers\etc" object="hosts") or (label=DNS label=Update (label=Successful or label=Request OR label=Fail)) (host=* or source_address=*))) -user IN EXCLUDED_USERS
```

Possible Botnet Connection-IRC Port

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

Possible Botnet Connection-Outbound DDOS

- **Trigger Condition:** Multiple hosts connecting to the same destination address is detected.
- **ATT&CK Category:** Impact, Command and Control, Defense Evasion

- **ATT&CK Tag:** Network Denial of Service, Proxy, Exploitation for Defense Evasion
- **ATT&CK ID:** T1498, T1090, T1211
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**
-
  ```
  label=Connection source_address in HOMENET destination_address=* | chart distinct_count(source_address) as source by destination_address| search source>100
  ```

Possible Botnet Connection-Outbound Spam

- **Trigger Condition:** An unauthorized email sent through an open relay is detected.
- **ATT&CK Category:** Command and Control, Defense Evasion, Impact
- **ATT&CK Tag:** Proxy, Exploitation for Defense Evasion, Network Denial of Service
- **ATT&CK ID:** T1090, T1211, T1498
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**
-
  ```
  (source_address=* or host=* method="HELO" or method="EHLO") or (label=Connection destination_port="25" source_address=* or host=*) | search -source_address IN MAIL_SERVER_IP
  ```

Possible CLR DLL Loaded Via Office Applications

- **Trigger Condition:** CLR DLL is loaded by an Office Product like WinWord, PowerPoint Excel, or Outlook.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** Phishing, Spearphishing Attachment
- **ATT&CK ID:** T1566, T1566.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  norm_id=WindowsSysmon event_id=7 source_image IN ["*\winword.exe", "*\powerpnt.exe", "*\excel.exe", "*\outlook.exe"] image IN ["*\clr.dll*"] -user IN EXCLUDED_USERS
  ```

Possible Credential Dump-Tools Named Pipes Detected

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

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

Possible Data Breach

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

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

Possible Data Breach-Off Hour Transfer

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

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

Possible DDOS Attack

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

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

Possible Detection of SafetyKatz

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

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

Possible DNS Rebinding Detected

- **Trigger Condition:** Different DNS answers by one domain with IPs from internal and external networks are detected. Typically, DNS-answer contains TTL greater than 100. Application Layer Protocol and DNS-record are saved in the host cache during TTL.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

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

Possible DoS Attack

- **Trigger Condition:** LogPoint detects DOS attack.
- **ATT&CK Category:** Initial Access, Impact
- **ATT&CK Tag:** Exploit Public-Facing Application, Network Denial of Service, Endpoint Denial of Service
- **ATT&CK ID:** T1190, T1498, T1499
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

-
  ```
  label=Dos label=Attack source_address=* destination_address=*
  ```

Possible Empire Monkey Detected

- **Trigger Condition:** LogPoint detects EmpireMonkey APT reported activity involving exploitation of *scrobj.dll* file using *cutil* or *regsvr32*.
- **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="*/i:%APPDATA%\logs.txt scrobj.dll" (image IN ["*\cutil.exe"] OR message IN ["Microsoft(C) Registerserver"]) -user IN EXCLUDED_USERS
  ```

Possible Executable Used by PlugX in Uncommon Location

- **Trigger Condition:** The execution of an executable used by PlugX for DLL side loading initated from an exotic location.
- **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=1 ((image="*\CamMute.exe" -image="*\Lenovo\Communication Utility\*") OR (image="*\chrome_frame_helper.exe" -image="*\Google\Chrome\application\*") OR (image="*\dvcemumanager.exe" -image="*\Microsoft Device Emulator\*") OR (image="*\Gadget.exe" -image="*\Windows Media Player\*") OR (image="*\hcc.exe" -image="*\HTML Help Workshop\*") OR (image="*\hkcmd.exe" -image IN ["*\System32\*", "*\SysNative\*", "*\SysWowo64\*"]) OR (image="*\Mc.exe" -image IN ["*\Microsoft Visual Studio*", "*\Microsoft SDK*", "*\Windows Kit*"]) OR (image="*\MsMpEng.exe" -image IN ["*\Microsoft Security Client\*", "*\Windows Defender\*", "*\AntiMalware\*"]) OR (image="*\msseces.exe" -image IN ["*\Microsoft Security Center\*", "*\Microsoft Security Client\*", "*\Microsoft Security Essentials\*"]) OR (image="*\OInfoP11.exe" -image="*\Common Files\Microsoft Shared\*") OR (image="*\OleView.exe" -image IN ["*\Microsoft Visual Studio*", "*\Microsoft SDK*", "*\Windows Kit*", "*\Windows Resource Kit\*"]) OR (image="*\rc.exe" -image IN ["*\Microsoft Visual Studio*", "*\Microsoft SDK*", "*\Windows Kit*", "*\Windows Resource Kit\*", "*\Microsoft.NET\*"])) -user IN EXCLUDED_USERS
  ```

Possible Exploitation for CVE-2015-1641 Detected

- **Trigger Condition:** Winword starting uncommon subprocess *MicroScMgmt.exe* used in exploits for CVE-2015-1641 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 parent_image="*\WINWORD.EXE" image="*\MicroScMgmt.exe " -user IN EXCLUDED_USERS
```

Possible Hijack of Legit RDP Session to Move Laterally

- **Trigger Condition:** The use of *tsclient* share to place a backdoor on the RDP source machine's startup folder is detected.
- **ATT&CK Category:** Persistence, Lateral Movement, Privilege Escalation
- **ATT&CK Tag:** Remote Service Session Hijacking, RDP Hijacking, Boot or Logon Autostart Execution, Registry Run Keys/Startup Folder
- **ATT&CK ID:** T1563, T1563.002, T1547, T1547.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=11 image="*\mstsc.exe" file="*\Microsoft\Windows\Start Menu\Programs\Startup\*" -user IN EXCLUDED_USERS
```

Possible Impacket Lateralization Detected

- **Trigger Condition:** *wmiexec/dcomexec/atexec/smbexec* from the Impacket framework is detected.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Windows Management Instrumentation, Inter-Process Communication, Inter-Process Communication, Component Object Model and Distributed COM
- **ATT&CK ID:** T1047, T1021, T1021.003, T1559, T1559.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 ((parent_image IN ["*\wmiprvse.exe", "*\mmc.exe", "*\explorer.exe", "*\services.exe"] command IN ["*cmd.exe* /Q /c * \\127.0.0.1\*&1*"]) OR (parent_command IN ["*svchost.exe -k netsvcs", "taskeng.exe*"] command IN ["cmd.exe /C *Windows\Temp\*&1"])) -user IN EXCLUDED_USERS
```

Possible Impacket SecretDump Remote Activity

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

-
  ```
  norm_id=WinServer event_id=5145 share_name="\*\ADMIN$" relative_target="SYSTEM32\*.tmp" -user IN EXCLUDED_USERS
  ```

Possible Inbound Spamming Detected

- **Trigger Condition:** LogPoint detects possible inbound spam.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Mail Server
- **Query:**

-
  ```
  (sender=* receiver=* -sender in KNOWN_DOMAINS) | chart distinct_count(receiver) as spam_receiver by sender | search spam_receiver>100
  ```

Possible Insider Threat

- **Trigger Condition:** LogPoint detects alerts like privilege escalation, unauthorized access, and data breach for the same user.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Logpoint
- **Query:**

-
  ```
  event_type="Possible Insider Threat" incident_user=* -incident_user in EXCLUDED_USERS| rename incident_user as user | chart distinct_count(incident_name) as AlertCount by user | search AlertCount>2
  ```

Possible Land Attack

- **Trigger Condition:** LogPoint detects a Cisco land-attack with event ID 106017.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Network Denial of Service
- **ATT&CK ID:** T1498
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

-
  ```
  event_id=106017 label=Connection label=Attack label=Deny
  ```

Possible Malicious Payload Download via Office Binaries Detected

- **Trigger Condition:** A payload is downloaded from a remote server with HTTP command using Microsoft Office applications such as PowerPoint, Word and Excel in a compromised system is detected.
- **ATT&CK Category:** Command and Control

- **ATT&CK Tag:** Ingress Tool Transfer
- **ATT&CK ID:** T1105
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

-
  ```
  label="Process" label=Create "process" IN ["*\powerpnt.exe", "*\winword.exe", "*\excel.exe"] command="*http*" -user IN EXCLUDED_USERS
  ```

Possible Malware Detected

- **Trigger Condition:** A file or software is detected as worm, virus, trojan, or malware.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Antivirus
- **Query:**

-
  ```
  (label=Malware or label=Threat or label=Virus or label=Quarantine or label=Risk) (malware=* OR risk=* OR virus=*) (file=* or application=* or url=*)
  ```

Possible Modification of Boot Configuration

- **Trigger Condition:** When the use of the bcdedit command to delete or modify Boot Configuration Data is detected. Boot Configuration Data (BCD) files provide a store that describes boot applications and application settings. Boot configuration data edit (bcdedit) allows manipulating BCD. This tactic is used by malware or attackers as a destructive technique to prevent system recovery. Legitimate usage can trigger this alert. We recommend including the legitimate user in the EXCLUDED_USERS list.
- **ATT&CK Category:** Impact, Defense Evasion, Persistence
- **ATT&CK Tag:** Inhibit System Recovery, Pre-OS Boot, Bootkit
- **ATT&CK ID:** T1490, T1542, T1542.003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

-
  ```
  norm_id=WindowsSysmon event_id=1 ((image="*\bcdedit.exe" command IN ["*delete*", "*import*","set"]) OR ((command="*bootstatuspolicy*" command="*ignoreallfailures*") OR (command="*recoveryenabled*" command="*no*"))) -user IN EXCLUDED_USERS
  ```

Possible Outbound Spamming Detected

- **Trigger Condition:** An outbound spamming is detected.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Mail Server

- **Query:**

-
  ```
  (sender=* receiver=* -receiver in KNOWN_DOMAINS sender in KNOWN_DOMAINS) | chart distinct_count(receiver) as spam_receiver by sender | search spam_receiver>100
  ```

Possible Pass the Hash Activity Detected

- **Trigger Condition:** When the attack technique passes the hash, which is used to move laterally inside the network. Pass the hash is a method of authenticating to a system using a password hash rather than the actual password. Adversaries may use this technique to gain unauthorized access to a system, bypassing normal authentication controls. Pass the hash attacks can be challenging to detect and prevent, as they do not involve using a clear-text password.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Use Alternate Authentication Material, Pass the Hash
- **ATT&CK ID:** T1550, T1550.002
- **Minimum Log Source Requirement:** Windows
- **Query:**

-
  ```
  norm_id=WinServer event_id=4624 ((caller_id="S-1-0-0" logon_type="3" logon_process="NtLmSsp" key_length="0") OR (logon_type="9" logon_process="seclogo")) -user="ANONYMOUS LOGON" -user IN EXCLUDED_USERS
  ```

Possible Privilege Escalation via Weak Service Permissions

- **Trigger Condition:** The *sc.exe* utility spawning by a user with medium integrity level to change the service ImagePath or FailureCommand is detected.
- **ATT&CK Category:** Privilege Escalation
- **ATT&CK Tag:** Access Token Manipulation
- **ATT&CK ID:** T1134
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

-
  ```
  norm_id=WindowsSysmon event_id=1 image="*\sc.exe" integrity_level="Medium" command IN ["*config*", "*binPath*", "*failure*", "*command*"] -user IN EXCLUDED_USERS
  ```

Possible Process Hollowing Image Loading

- **Trigger Condition:** Loading of *samlib.dll* or *WinSCard.dll* from untypical process is detected. For example, through process hollowing by Mimikatz.
- **ATT&CK Category:** Defense Evasion, Privilege Escalation
- **ATT&CK Tag:** Hijack Execution Flow, DLL Side-Loading, Process Injection, Process Hollowing

- **ATT&CK ID:** T1574, T1574.002, T1055, T1055.012
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

-
  ```
  norm_id=WindowsSysmon event_id=7 source_image IN ["*\notepad.exe"] image IN ["*\samlib.dll", "*\WinSCard.dll"] -user IN EXCLUDED_USERS
  ```

Possible SPN Enumeration Detected

- **Trigger Condition:** *Service Principal Name Enumeration* used for Steal or Forge Kerberos Tickets and Kerberoasting is detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Steal or Forge Kerberos Tickets, Kerberoasting
- **ATT&CK ID:** T1558, T1558.003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

-
  ```
  norm_id=WindowsSysmon event_id=1 command="*-q*" (image="*\setspn.exe" OR message="*Query or reset the computer* SPN attribute*") -user IN EXCLUDED_USERS
  ```

Possible SquiblyTwo Detected

- **Trigger Condition:** WMI SquiblyTwo Attack with possible renamed WMI seeking for imphash is detected.
- **ATT&CK Category:** Defense Evasion, Execution
- **ATT&CK Tag:** Windows Management Instrumentation, Visual Basic, JavaScript, XSL Script Processing
- **ATT&CK ID:** T1047, T1059.005, T1059.007, T1220
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

-
  ```
  norm_id=WindowsSysmon event_id=1 file="wmic.exe" hash_imphash IN ["1B1A3F43BF37B5BFE60751F2EE2F326E", "37777A96245A3C74EB217308F3546F4C", "9D87C9D67CE724033C0B40CC4CA1B206"] command="*format:*" command="*http*"
  ```

Possible Taskmgr run as LOCAL_SYSTEM Detected

- **Trigger Condition:** Creation of a *taskmgr.exe* process in the context of LOCAL_SYSTEM is detected. *Taskmgr.exe* is the executable file for Windows Task Manager.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Masquerading
- **ATT&CK ID:** T1036
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

-
  ```
  label="Process" label=Create "process"="*\taskmgr.exe" user in ["*AUTHORI*", "*AUTORI*"]
  ```

Potential RDP Exploit CVE-2019-0708 Detected

- **Trigger Condition:** An error on protocol RDP potential CVE-2019-0708 is detected.
- **ATT&CK Category:** Initial Access, Lateral Movement
- **ATT&CK Tag:** Exploitation of Remote Services, Exploit Public-Facing Application
- **ATT&CK ID:** T1210, T1190
- **Minimum Log Source Requirement:** Windows
- **Query:**
-
  ```
  norm_id=WinServer event_id IN ["56", "50"] event_source="TermDD" -user IN EXCLUDED_USERS
  ```

Powershell AMSI Bypass via dotNET Reflection

- **Trigger Condition:** Request to *amsiInitFailed* used to disable AMSI Scanning is detected.
- **ATT&CK Category:** Execution, Defense Evasion
- **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 ["*System.Management.Automation.AmsiUtils*"] command IN ["*amsiInitFailed*"] -user IN EXCLUDED_USERS
  ```

PowerShell Base64 Encoded Shellcode Detected

- **Trigger Condition:** Base64 encoded shellcode is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Masquerading
- **ATT&CK ID:** T1036
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  norm_id=WindowsSysmon event_id=1 command="*AAAAYInlM*" command IN ["*OiCAAAAYInlM*", "*OiJAAAAYInlM*"] -user IN EXCLUDED_USERS
  ```

PowerShell Network Connections Detected

- **Trigger Condition:** LogPoint detects a Command and Scripting Interpreter and PowerShell process that opens network connections. We recommend you check suspicious target ports and systems, and adjust them according to your environment. For example, extend filters with the company’s IP range.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, PowerShell

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

-
  ```
  norm_id=WindowsSysmon event_id=3 image="*\powershell.exe" initiated="true" -destination_address IN HOMENET -user="NT AUTHORITY\SYSTEM" -user IN EXCLUDED_USERS
  ```

PowerShell Profile Modification

- **Trigger Condition:** Modification of Command and Scripting Interpreter and PowerShell profile is detected.
- **ATT&CK Category:** Persistence, Privilege Escalation, Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, Event Triggered Execution, PowerShell Profile, Powershell
- **ATT&CK ID:** T1546, T1546.013, T1059, T1059.001
- **Minimum Log Source Requirement:** Windows
- **Query:**

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

PowerShell Rundll32 Remote Thread Creation Detected

- **Trigger Condition:** Command and Scripting Interpreter and PowerShell remote thread creation in Signed Binary Proxy Execution and Rundll32.exe is detected.
- **ATT&CK Category:** Defense Evasion, Execution
- **ATT&CK Tag:** Signed Binary Proxy Execution, Rundll32, Command and Scripting Interpreter, PowerShell
- **ATT&CK ID:** T1218, T1218.011, T1059, T1059.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

-
  ```
  norm_id=WindowsSysmon event_id=8 source_image="*\powershell.exe" image="*\rundll32.exe" -user IN EXCLUDED_USERS
  ```

PowerShell Script Run in AppData Detected

- **Trigger Condition:** A suspicious command line execution that invokes Command and Scripting Interpreter and PowerShell concerning an AppData folder is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** 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 ["* /c powershell*\AppData\Local\*", "* /c powershell*\AppData\Roaming\*"] -user IN EXCLUDED_USERS
  ```

PowerShell Version Downgrade Detected

- **Trigger Condition:** The execution of Command and Scripting Interpreter and PowerShell v2 is detected. We recommend you avoid Powershell v2 as it offers zero-logging. PowerShell v5.x or higher offers better login.
- **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=400 host_version="2.0" -user IN EXCLUDED_USERS
  ```

Process Dump via Comsvcs DLL Detected

- **Trigger Condition:** Process memory dump via *comsvcs.dll* and *rundll32* is detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** OS Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  norm_id=WindowsSysmon event_id=1 (image="*\rundll32.exe" OR file="RUNDLL32.EXE") command IN ["*comsvcs*MiniDump*full*", "*comsvcs*MiniDumpW*full*"] -user IN EXCLUDED_USERS
  ```

Process Dump via Rundll32 and Comsvcs Detected

- **Trigger Condition:** Process memory dump performed via ordinal function 24 in *comsvcs.dll* is detected.
- **ATT&CK Category:** Defense Evasion, Credential Access
- **ATT&CK Tag:** Masquerading, OS Credential Dumping, LSASS Memory
- **ATT&CK ID:** T1036, T1003, T1003.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  norm_id=WindowsSysmon event_id=1 command IN ["*comsvcs.dll, #24*", "*comsvcs.dll, MiniDump*"] -user IN EXCLUDED_USERS
  ```

Process Hollowing Detected

- **Trigger Condition:** Adversaries attempt to inject malicious code into suspended and hollowed processes to evade process-based defenses.
- **ATT&CK Category:** Defense Evasion, Privilege Escalation
- **ATT&CK Tag:** Process Injection, Process Hollowing
- **ATT&CK ID:** T1055, T1055.012

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

```
norm_id=WindowsSysmon event_id=1 (image="*smss.exe" parent_command!="*smss.exe") or (image="*csrss.exe" (parent_command!="*smss.exe" and parent_command!="*svchost.exe")) or (image="*wininit.exe" parent_command!="*smss.exe") or (image="*winlogon.exe" parent_command!="*smss.exe") or (image="*lsass.exe" parent_command!="*wininit.exe") or (image="*LogonUI.exe" (parent_command!="*winlogon.exe"  and parent_command!="*wininit.exe")) or (image="*services.exe" parent_command!="*wininit.exe") or (image="*spoolsv.exe" parent_command!="*services.exe") or (image="*taskhost.exe" (parent_command!="*services.exe" and parent_command!="*svchost.exe")) or (image="*taskhostw.exe" (parent_command!="*services.exe" and parent_command!="*svchost.exe")) or (image="*userinit.exe" (parent_command!="*dwm.exe" and parent_command!="*winlogon.exe")) -user IN EXCLUDED_USERS
```

Process Injection Detected

- **Trigger Condition:** Adversaries inject code into processes to evade process-based defenses and possibly elevate privileges using commands like Invoke-DllInjection.
- **ATT&CK Category:** Defense Evasion, Privilege Escalation
- **ATT&CK Tag:** Process Injection
- **ATT&CK ID:** T1055
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 (command="*Invoke-DllInjection*" or command="*C:\windows\sysnative\*") -user IN EXCLUDED_USERS
```

Protected Storage Service Access Detected

- **Trigger Condition:** An access to a *protected_storage* service over the network is detected. The potential abuse of DPAPI to extract domain backup keys from Domain Controllers.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Remote Services
- **ATT&CK ID:** T1021
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=5145 share_name="*IPC*" relative_target="protected_storage" -user IN EXCLUDED_USERS
```

Prowli Malware Affected Host

- **Trigger Condition:** Widows Server is affected by Prowli malware.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -

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

-
  ```
  norm_id=Winserver* hash in PROWLI_FILE host=*
  ```

Prowli Malware Connection to Malicious Destination

- **Trigger Condition:** An outbound connection to Prowli Malware sources is established by hosts.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Proxy
- **ATT&CK ID:** T1090
- **Minimum Log Source Requirement:** Windows
- **Query:**

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

Prowli Malware Emails Sent to Attacker

- **Trigger Condition:** An email is sent to Prowli Malware 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 PROWLI_EMAIL (host=* OR source_host=*) | rename source_host as host
  ```

PsExec Tool Execution Detected

- **Trigger Condition:** PsExec service installation and execution event (Service and Sysmon) is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** System Services, Service Execution
- **ATT&CK ID:** T1569, T1569.002
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

-
  ```
  ((norm_id=WinServer service="PSEXESVC" event_id IN [7045, 7036]) OR (norm_id=WindowsSysmon event_id=1 "process"="*\PSEXESVC.exe" user="*SYSTEM*")) -user IN EXCLUDED_USERS
  ```

Psr Capture Screenshots Detected

- **Trigger Condition:** The *psr.exe* captures desktop screenshots and saves them in a local machine.

- **ATT&CK Category:** Collection
- **ATT&CK Tag:** Screen Capture
- **ATT&CK ID:** T1113
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

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

Pulse Secure Arbitrary File Reading Detected

- **Trigger Condition:** The exploitation of arbitrary file reading vulnerability (CVE-2019-11510) in Pulse Secure is detected.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** External Remote Services
- **ATT&CK ID:** T1113
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

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

QBot Process Creation Detected

- **Trigger Condition:** LogPoint detects QBot like process execution of wscript or use of commands to manipulate program data or ping local host.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, Visual Basic
- **ATT&CK ID:** T1059, T1059.005
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

-
  ```
  norm_id=WindowsSysmon event_id=1 ((parent_image="*\WinRAR.exe" image="*\wscript.exe") OR command="* /c ping.exe -n 6 127.0.0.1 & type *" OR (command="*regsvr32.exe*" command="*C:\ProgramData*" command="*.tmp*")) -user IN EXCLUDED_USERS
  ```

QuarksPwDump Clearing Access History Detected

- **Trigger Condition:** QuarksPwDump clearing access history in hive is detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** OS Credential Dumping, NTDS, Valid Accounts, Local Accounts
- **ATT&CK ID:** T1003, T1003.003, T1078, T1078.003
- **Minimum Log Source Requirement:** Windows
- **Query:**

-
  ```
  norm_id=WinServer event_id=16 hive="*\AppData\Local\Temp\SAM*" hive="*.dmp" -user IN EXCLUDED_USERS
  ```

QuarksPwDump Dump File Detected

- **Trigger Condition:** A dump file written by QuarksPwDump password dumper is detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** OS Credential Dumping, Security Account Manager
- **ATT&CK ID:** T1003, T1003.002
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

-
  ```
  event_id=11 file="*\AppData\Local\Temp\SAM-*.dmp*" -user IN EXCLUDED_USERS
  ```

Query Registry Network

- **Trigger Condition:** Adversaries use *reg.exe* component for network connection and interact with the Windows Registry to gather information about the system, configuration, and installed software.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Query Registry
- **ATT&CK ID:** T1012
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

-
  ```
  norm_id=WindowsSysmon event_id=3 image="*reg.exe" command="*reg query*" -user IN EXCLUDED_USERS
  ```

Rare Scheduled Task Creations Detected

- **Trigger Condition:** Rare scheduled task creations are detected. A software gets installed on multiple systems. The aggregation and count function selects tasks with rare names.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Scheduled Task/Job, Scheduled Task
- **ATT&CK ID:** T1053, T1053.005
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

-
  ```
  norm_id=WindowsSysmon event_id="106" | chart count() as val by task | search val < 5
  ```

RDP Login from Localhost Detected

- **Trigger Condition:** RDP login with a localhost source address that may be a tunneled login is detected.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Remote Services, Remote Desktop Protocol
- **ATT&CK ID:** T1021, T1021.001

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

```
norm_id=WinServer event_id=4624 logon_type="10" source_address IN ["::1", "127.0.0.1"] -user IN EXCLUDED_USERS
```

RDP Over Reverse SSH Tunnel Detected

- **Trigger Condition:** *svchost* hosting RDP *termsvcs* communicating with the loopback address and on TCP port 3389 is detected.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Remote Services, Remote Desktop Protocol
- **ATT&CK ID:** T1021, T1021.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=3 image="*\svchost.exe" initiated="true" source_port="3389" destination_address IN ["127.*", "::1"] -user IN EXCLUDED_USERS
```

RDP over Reverse SSH Tunnel WFP

- **Trigger Condition:** *svchost* hosting RDP *termsvcs* communicating with the loopback address is detected.
- **ATT&CK Category:** Command and Control, Lateral Movement
- **ATT&CK Tag:** Remote Services, Remote Desktop Protocol, Proxy
- **ATT&CK ID:** T1021, T1021.001, T1090
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=5156 ((source_port="3389" destination_address IN ["127.*", "::1"]) OR (destination_port="3389" source_address IN ["127.*", "::1"])) -user IN EXCLUDED_USERS
```

RDP Registry Modification

- **Trigger Condition:** Potential malicious modification of the property value of fDenyTS Connections and UserAuthentication to enable remote desktop connections is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Modify Registry
- **ATT&CK ID:** T1112
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=13 target_object IN ["*\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\UserAuthentication", "*\CurrentControlSet\Control\Terminal Server\fDenyTSConnections"] details="DWORD (0x00000000)" -user IN EXCLUDED_USERS
```

RDP Sensitive Settings Changed

- **Trigger Condition:** Changes to RDP terminal service sensitive settings are detected.
- **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 IN ["*\services\TermService\Parameters\ServiceDll*", "*\Control\Terminal Server\fSingleSessionPerUser*", "*\Control\Terminal Server\fDenyTSConnections*"] -user IN EXCLUDED_USERS
  ```

Reconnaissance Activity with Net Command

- **Trigger Condition:** A set of commands often used in recon stages by different attack groups to discover the victim's information, systems, or network are detected.
- **ATT&CK Category:** Discovery, Reconnaissance
- **ATT&CK Tag:** Account Discovery, System Information Discovery, Gather Victim Host Information, Gather Victim Identity Information
- **ATT&CK ID:** T1087, T1082, T1589, T1592
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

-
  ```
  norm_id=WindowsSysmon event_id=1 command IN ["tasklist", "net time", "systeminfo", "whoami", "nbtstat", "net start", "*\net1 start", "qprocess", "nslookup", "hostname.exe", "*\net1 user /domain", "*\net1 group /domain", "*\net1 group *domain admins* /domain", "*\net1 group *Exchange Trusted Subsystem* /domain", "*\net1 accounts /domain", "*\net1 user net localgroup administrators", "netstat -an"]
  ```

-
  ```
  -user IN EXCLUDED_USERS | chart count() as val by command | search val > 4
  ```

RedSocks Backdoor Connection

- **Trigger Condition:** A backdoor event is detected. Adversaries develop malware and malware components as backdoors, which are used during targeting.
- **ATT&CK Category:** Resource Development
- **ATT&CK Tag:** Develop Capabilities, Malware
- **ATT&CK ID:** T1587, T1587.001
- **Minimum Log Source Requirement:** Redsocks
- **Query:**

-
  ```
  norm_id=RedSocks description="*backdoor*" | process geoip(destination_address) as country
  ```

RedSocks Bad Neighborhood Detection

- **Trigger Condition:** A bad neighborhood is detected where adversaries use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a Command and Control server to avoid direct connections to their infrastructure.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Proxy
- **ATT&CK ID:** T1090
- **Minimum Log Source Requirement:** Redsocks
- **Query:**
-
  ```
  norm_id=RedSocks category="bad hood" | process geoip(destination_address) as country
  ```

RedSocks Blacklist URL Detection

- **Trigger Condition:** Blacklist URLs are detected.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Redsocks
- **Query:**
-
  ```
  norm_id=RedSocks category="URL blacklist" | process geoip(destination_address) as country
  ```

RedSocks FileSharing

- **Trigger Condition:** Filesharing using an alternate platform like 4Shared, FileHippo, Torrent, Picofile, or WeTransfer is detected.
- **ATT&CK Category:** Exfiltration
- **ATT&CK Tag:** Exfiltration over Alternative Protocol
- **ATT&CK ID:** T1048
- **Minimum Log Source Requirement:** Redsocks
- **Query:**
-
  ```
  norm_id=RedSocks category="Filesharing" description in ["*4share*","*torrent*" ,"*FileHippo*","*picofile*","*wetransfer*"]| process geoip(destination_address) as country
  ```

RedSocks Ransomware Connection

- **Trigger Condition:** A ransomware event is detected.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Disk Wipe, Disk Content Wipe, Data Encrypted for Impact, Data Destruction, Proxy
- **ATT&CK ID:** T1561, T1561.001, T1486, T1485, T1090

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

-
  ```
  norm_id=RedSocks description="*ransomware*" | process geoip(destination_address) as country
  ```

RedSocks Sinkhole Detection

- **Trigger Condition:** Sinkhole is detected.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Redsocks
- **Query:**

-
  ```
  norm_id=RedSocks category="Sinkhole" | process geoip(destination_address) as country
  ```

RedSocks Tor Connection

- **Trigger Condition:** A Tor connection is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Proxy
- **ATT&CK ID:** T1090
- **Minimum Log Source Requirement:** Redsocks
- **Query:**

-
  ```
  norm_id=RedSocks category="tor" | process geoip(destination_address) as country
  ```

RedSocks Trojan Connection

- **Trigger Condition:** A trojan event is detected.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Redsocks
- **Query:**

-
  ```
  norm_id=RedSocks description="*trojan*" | process geoip(destination_address) as country
  ```

Register new Logon Process by Rubeus

- **Trigger Condition:** Potential use of Rubeus via registered new trusted logon process is detected. Adversaries abuse a valid Kerberos ticket-granting ticket (TGT) or sniff network traffic to obtain a ticket-granting service (TGS) ticket that may be vulnerable to Brute Force.
- **ATT&CK Category:** Lateral Movement, Privilege Escalation

- **ATT&CK Tag:** Steal or Forge Kerberos Tickets, Kerberoasting
- **ATT&CK ID:** T1558, T1558.003
- **Minimum Log Source Requirement:** Windows
- **Query:**
-
  ```
  norm_id=WinServer event_id=4611 logon_process="User32LogonProcesss" -user IN EXCLUDED_USERS
  ```

Registry Persistence Mechanisms Detected

- **Trigger Condition:** Persistence registry keys at the current version folder for registry keys are detected. Adversaries establish persistence and/or elevate privileges by executing malicious content triggered by Image File Execution Options (IFEO) debuggers.
- **ATT&CK Category:** Privilege Escalation, Persistence
- **ATT&CK Tag:** Event Triggered Execution, Image File Execution Options Injection
- **ATT&CK ID:** T1546, T1546.012
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  event_id=13 target_object IN ["*\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\*\GlobalFlag", "*\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\*\ReportingMode", "*\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\*\MonitorProcess"] event_type="SetValue" -user IN EXCLUDED_USERS
  ```

Registry Persistence via Explorer Run Key Detected

- **Trigger Condition:** Persistence mechanism using a RUN key for Windows Explorer and pointing to a suspicious folder is detected.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Boot or Logon Autostart Execution, Registry Run Keys/Startup Folder
- **ATT&CK ID:** T1547, T1547.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  event_id=13 target_object="*\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run" detail IN ["C:\Windows\Temp\*", "C:\ProgramData\*", "*\AppData\*", "C:\$Recycle.bin\*", "C:\Temp\*", "C:\Users\Public\*", "C:\Users\Default\*"] -user IN EXCLUDED_USERS
  ```

Regsvcs-Regasm Detected

- **Trigger Condition:** Adversary abuses trusted Windows command line utilities *regsvcs* and *regasm* for proxy execution of code.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Signed Binary Proxy Execution, Regsvcs/Regasm

- **ATT&CK ID:** T1218, T1218.009
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  norm_id=WindowsSysmon event_id=3 (image="*regsvcs.exe" or image="*regasm.exe")
  ```

Remote PowerShell Session

- **Trigger Condition:** Remote Command and Scripting Interpreter and PowerShell sessions by monitoring network outbound connections to ports 5985 or 5986 from network service accounts 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=WinServer event_id IN ["4103", "400"] host="ServerRemoteHost" application="*wsmprovhost.exe*") OR (norm_id=WindowsSysmon event_id=1 (image="*\wsmprovhost.exe" OR parent_image="*\wsmprovhost.exe")) -user IN EXCLUDED_USERS | rename application as service
  ```

Remote System Discovery

- **Trigger Condition:** The components like net.exe and ping.exe are used to list other systems by IP address, hostname, or other logical identifiers on a network used for Lateral Movement from the current system.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Remote System Discovery
- **ATT&CK ID:** T1018
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  norm_id=WindowsSysmon (image="*net.exe" or image="*ping.exe") (command="*view*" or command="*ping*") -user IN EXCLUDED_USERS
  ```

Renamed Binary Detected

- **Trigger Condition:** The execution of a renamed binary used by attackers or malware leveraging new Sysmon OriginalFileName datapoint is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Masquerading
- **ATT&CK ID:** T1036
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  label="Process" label=Create file IN ["cmd.exe", "powershell.exe", "powershell_ise.exe", "psexec.exe", "psexec.c", "cscript.exe", "wscript.exe",
  ```

```
"mshta.exe", "regsvr32.exe", "wmic.exe", "certutil.exe", "rundll32.exe", "cmstp.exe", "msiexec.exe", "7z.exe", "winrar.exe", "wevtutil.exe", "net.exe", "net1.exe"] -"process" IN ["*\cmd.exe", "*\powershell.exe", "*\powershell_ise.exe", "*\psexec.exe", "*\psexec64.exe", "*\cscript.exe", "*\wscript.exe", "*\mshta.exe", "*\regsvr32.exe", "*\wmic.exe", "*\certutil.exe", "*\rundll32.exe", "*\cmstp.exe", "*\msiexec.exe", "*\7z.exe", "*\winrar.exe", "*\wevtutil.exe", "*\net.exe", "*\net1.exe"]
```

Renamed ProcDump Detected

- **Trigger Condition:** Execution of a renamed *ProcDump* executable used by attackers or malware.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Masquerading
- **ATT&CK ID:** T1036
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  norm_id=WindowsSysmon file="procdump" -image IN ["*\procdump.exe", "*\procdump64.exe"]
  ```

Renamed PsExec Detected

- **Trigger Condition:** Execution of a renamed *PsExec* used by attackers or malware.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Masquerading
- **ATT&CK ID:** T1036
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  norm_id=WindowsSysmon message="Execute processes remotely" product="Sysinternals PsExec" -image IN ["*\PsExec.exe", "*\PsExec64.exe"]
  ```

Renamed ZOHO Dctask64 Detected

- **Trigger Condition:** Renamed *dctask64.exe* used for process injection, command execution, and process creation with a signed binary by ZOHO Corporation is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Process Injection
- **ATT&CK ID:** T1055
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  norm_id=WindowsSysmon event_id=1 hash="6834B1B94E49701D77CCB3C0895E1AFD" -image="*\dctask64.exe" -user IN EXCLUDED_USERS
  ```

REvil-Sodinokibi Ransomware Connection to Malicious Domains

- **Trigger Condition:** The connection to REvil-Sodinokibi Double Extortion ransomware-related domains is detected. For the alert to work, you must use the list REVIL_RANSOMWARE_DOMAINS, which includes IOC domains for Sodinokibi ransomware.
- **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 REVIL_RANSOMWARE_DOMAINS
  ```

REvil-Sodinokibi Ransomware Connection to Malicious Sources

- **Trigger Condition:** Hosts establishing an outbound connection to REvil-Sodinokibi Double Extortion ransomware sources are deteted. For the alert to work, you must use the list REVIL_RANSOMWARE_IPS, which includes IOC IPs for Sodinokibi ransomware.
- **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 REVIL_RANSOMWARE_IPS OR source_address IN REVIL_RANSOMWARE_IPS) | process geoip(destination_address) as country
  ```

REvil-Sodinokibi Ransomware Exploitable Vulnerabilities Detected

- **Trigger Condition:** Vulnerability management detects the presence of vulnerabilities linked to REvil-Sodinokibi ransomware. For the alert to work, you must use the list REVIL_RANSOMWARE_CVE, which includes IOC CVE IDs for Sodinokibi ransomware.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Vulnerability Management
- **Query:**
-
  ```
  norm_id=VulnerabilityManagement cve_id IN REVIL_RANSOMWARE_CVE
  ```

REvil-Sodinokibi Ransomware Infected Host Detected

- **Trigger Condition:** REvil-Sodinokibi Double Extortion ransomware-infected host is detected. For the alert to work, you must use the list REVIL_RANSOMWARE_CVE, which includes IOC for Sodinokibi ransomware.
- **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 REVIL_RANSOMWARE_HASHES
  ```

RobbinHood Ransomware Exploitable Vulnerabilities Detected

- **Trigger Condition:** Vulnerability management detects GIGABYTE Drivers Elevation of Privilege Vulnerabilities linked to RobbinHood ransomware.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Vulnerability Management
- **Query:**
-
  ```
  norm_id=VulnerabilityManagement cve_id="*CVE-2018-19320*"
  ```

Robbinhood Ransomware Infected Host Detected

- **Trigger Condition:** RobbinHood ransomware-infected host is detected. For the alert to work, you must use the list REVIL_RANSOMWARE_HASHES, which includes Ioc CVE IDs for Sodinokibi ransomware.
- **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 ROBBINHOOD_RANSOMWARE_HASHES
  ```

Rogue Access Point Detected

- **Trigger Condition:** Rouge access point is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Exploitation for Defense Evasion, Exploitation for Defense Evasion, Software Discovery, Security Software Discovery

- **ATT&CK ID:** T1211, T1211, T1518, T1518.001
- **Minimum Log Source Requirement:** Firewall, IDS/IPS (ArubaOS, Cisco Controller)
- **Query:**

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

RSA SecurID Account Lockout

- **Trigger Condition:** User’s account is locked after entering the wrong passcode multiple times in a row.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Brute Force
- **ATT&CK ID:** T1110
- **Minimum Log Source Requirement:** RSA Secure ID
- **Query:**

```
norm_id=RSA_SecurID type=Runtime action=AUTHN_LOCKOUT_EVENT
```

RSA SecurID Account Lockout

- **Trigger Condition:** User’s account is locked after entering the wrong passcode multiple times in a row.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Brute Force
- **ATT&CK ID:** T1110
- **Minimum Log Source Requirement:** RSA Secure ID
- **Query:**

```
norm_id=RSA_SecurID type=Runtime action=AUTHN_LOCKOUT_EVENT
```

Rubeus Hack Tool Detected

- **Trigger Condition:** The Command line parameters like asreproast, dump, impersonate user, harvest, and other commands used by the Rubeus hack tool are detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** OS Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 command IN ["* asreproast *", "* dump /service:krbtgt *", "* kerberoast *", "* createnetonly /program:*", "* ptt /ticket:*", "* /impersonateuser:*", "* renew /ticket:*", "* asktgt /user:*", "* harvest /interval:*"] -user IN EXCLUDED_USERS
```

Run PowerShell Script from ADS Detected

- **Trigger Condition:** PowerShell script execution from Alternate Data Stream (ADS) is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Hide Artifacts, NTFS File Attributes
- **ATT&CK ID:** T1564, T1564.004
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  norm_id=WindowsSysmon event_id=1 parent_image="*\powershell.exe" image="*\powershell.exe" command="*Get-Content*" command="*-Stream*" -user IN EXCLUDED_USERS
  ```

Rundll32 Internet Connection Detected

- **Trigger Condition:** *rundll32* that communicates with public IP addresses are detected.
- **ATT&CK Category:** Defense Evasion, Execution
- **ATT&CK Tag:** Signed Binary Proxy Execution, Rundll32
- **ATT&CK ID:** T1218, T1218.011
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  norm_id=WindowsSysmon event_id=3 image="*\rundll32.exe" initiated="true" -destination_address IN HOMENET -user IN EXCLUDED_USERS
  ```

Ryuk Ransomware Affected Host

- **Trigger Condition:** Ryuk Ransomware infects a host. The alert uses the RYUK_RANSOMWARE_HASH list to compare hash, pre-digest value, or digest in the logs.
- **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:**
-
  ```
  hash IN RYUK_RANSOMWARE_HASH OR pre_digest IN RYUK_RANSOMWARE_HASH OR digest IN RYUK_RANSOMWARE_HASH host=* | rename object as file
  ```

SAM Registry Hive Dump via Reg Utility

- **Trigger Condition:** Handle to SAM registry hive via reg utility is detected.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Query Registry
- **ATT&CK ID:** T1012
- **Minimum Log Source Requirement:** Windows
- **Query:**
-
  ```
  norm_id=WinServer event_id=4656 object_type="Key" object_name="*\SAM" "process"="*\reg.exe" -user IN EXCLUDED_USERS
  ```

SAM Registry Hive Handle Request Detected

- **Trigger Condition:** Request to SAM registry hive is detected.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Query Registry
- **ATT&CK ID:** T1012
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4656 object_type="Key" object_name="*\SAM" -user IN EXCLUDED_USERS
```

Scheduled Task Creation Detected

- **Trigger Condition:** The use of *schtasks* for the creation of scheduled tasks in a user session is detected.
- **ATT&CK Category:** Execution, Persistence, Privilege Escalation
- **ATT&CK Tag:** Scheduled Task/Job, Scheduled Task
- **ATT&CK ID:** T1053, T1053.005
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 image="*\schtasks.exe" command="* /create *" -user="NT AUTHORITY\SYSTEM" -user IN EXCLUDED_USERS
```

SCM Database Handle Failure Detected

- **Trigger Condition:** Non-system user fails to get a handle of the SCM database.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Endpoint Denial of Service
- **ATT&CK ID:** T1499
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4656 object_type="SC_MANAGER OBJECT" object_name="servicesactive" event_type="Audit Failure" logon_id="0x3e4" -user IN EXCLUDED_USERS
```

SCM Database Privileged Operation Detected

- **Trigger Condition:** Non-system user performs privileged operation on the SCM database.
- **ATT&CK Category:** Privilege Escalation
- **ATT&CK Tag:** Abuse Elevation Control Mechanism, Bypass User Account Control
- **ATT&CK ID:** T1548, T1548.002
- **Minimum Log Source Requirement:** Windows
- **Query:**

-
  ```
  norm_id=WinServer event_id=4674 object_type="SC_MANAGER OBJECT" object_name="servicesactive" privilege="SeTakeOwnershipPrivilege" logon_id="0x3e4" -user IN EXCLUDED_USERS
  ```

Screensaver Activities Detected

- **Trigger Condition:** Adversaries use screensaver executable to establish persistence by executing malicious content triggered by user inactivity.
- **ATT&CK Category:** Persistence, Privilege Escalation
- **ATT&CK Tag:** Event Triggered Execution, Screensaver
- **ATT&CK ID:** T1546, T1546.002
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

-
  ```
  norm_id=WindowsSysmon (event_id=12 or event_id=13 or event_id=14) (target_object="*\Control Panel\Desktop\SCRNSAVE.exe") (parent_command!="*explorer.exe" or image!="*rundll32.exe" or command!="*shell32.dll, Control_RunDLL desk.cpl, ScreenSaver, *") -user IN EXCLUDED_USERS
  ```

Secure Deletion with SDelete

- **Trigger Condition:** LogPoint detects renaming of a file while deletion with SDelete tool.
- **ATT&CK Category:** Defense Evasion, Impact
- **ATT&CK Tag:** Indicator Removal on Host, File Deletion,Obfuscated Files or Information, Indicator Removal from Tools, Data Destruction, Subvert Trust Controls, Code Signing
- **ATT&CK ID:** T1070, T1070.004, T1027, T1027.005, T1485, T1553, T1553.002
- **Minimum Log Source Requirement:** Windows
- **Query:**

-
  ```
  norm_id=WinServer event_id IN ["4656", "4663", "4658"] object_name IN ["*.AAA", "*.ZZZ"] -user IN EXCLUDED_USERS
  ```

SecurityXploded Tool Detected

- **Trigger Condition:** Execution of the SecurityXploded tools.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** OS Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

-
  ```
  norm_id=WindowsSysmon event_id=1 (company="SecurityXploded" OR image="*PasswordDump.exe" OR file="*PasswordDump.exe") -user IN EXCLUDED_USERS
  ```

Shadow Copy Creation Using OS Utilities Detected

- **Trigger Condition:** Creation of shadow copies using Operating systems utilities like PowerShell, wmic, and vssadmin are detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** OS Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  norm_id=WindowsSysmon event_id=1 "process" IN ["*\powershell.exe", "*\wmic.exe", "*\vssadmin.exe"] command="*shadow*" command="*create*" -user IN EXCLUDED_USERS
  ```

Signed Binary Proxy Execution - Network Detected

- **Trigger Condition:** When adversaries bypass process and/or signature-based defenses by proxying execution of malicious content with signed binaries using windows components and commands like certutil, replace. Signed binary proxy execution is a technique that involves the use of a trusted, signed binary to execute malicious code. Adversaries may use this technique to bypass security controls and execute malicious code on a system without being detected.
- **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=3 (image="*certutil.exe" or command="*certutil*script:http*://*" or image="*\replace.exe") -user IN EXCLUDED_USERS
  ```

Signed Binary Proxy Execution - Process Detected

- **Trigger Condition:** Adversaries bypass process and/or signature-based defenses by proxying execution of malicious content with signed binaries using Windows components and commands like *certutil* or *replace*.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Signed Binary Proxy Execution
- **ATT&CK ID:** T1218
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  label="process" label=create ("process"="*mavinject.exe" or command="*\/injectrunning*" or command="*mavinject32*\/injectrunning*" or command="*certutil*script:http*://*" or command="*msiexec*http*://*") -user IN EXCLUDED_USERS
  ```

Signed Script Proxy Execution

- **Trigger Condition:** Adversaries use scripts signed with trusted certificates for proxy execution of malicious files using cscript, wscript, certutil, and jjs.
- **ATT&CK Category:** Defense Evasion

- **ATT&CK Tag:** Signed Script Proxy Execution
- **ATT&CK ID:** T1216
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon image IN ["*cscript*", "*wscript*", "*certutil*" , "*jjs"] command!="* /nologo *MonitorKnowledgeDiscovery.vbs*" -user IN EXCLUDED_USERS
```

SILENTTRINITY Stager Execution Detected

- **Trigger Condition:** The use of SILENTTRINITY stager is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** System Services, Service Execution
- **ATT&CK ID:** T1569, T1569.002
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
(event_id=7 OR event_id="1") message="*st2stager*"
```

smbexec Service Installation Detected

- **Trigger Condition:** *smbexec.py* tool is detected by identifying a specific service installation.
- **ATT&CK Category:** Lateral Movement, Execution
- **ATT&CK Tag:** Remote Services, System Services, Service Execution
- **ATT&CK ID:** T1021, T1569, T1569.002
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=7045 service="BTOBTO" service="*\execute.bat" -user IN EXCLUDED_USERS
```

SolarisLDAP Group Remove from LDAP Detected

- **Trigger Condition:** The removal of a group from LDAP is detected.
- **ATT&CK Category:** Credential Access, Persistence, Impact, Defense Evasion
- **ATT&CK Tag:** Account Manipulation, Account Access Removal
- **ATT&CK ID:** T1098, T1531
- **Minimum Log Source Requirement:** Solaris LDAP
- **Query:**

```
norm_id=SolarisLDAP label=Remove label=Member label=Management label=Group
```

SolarisLDAP Possible Bruteforce Attack Detected

- **Trigger Condition:** Bruteforcing of a user’s LDAP credentials is detected.
- **ATT&CK Category:** Credential Access, Persistence

- **ATT&CK Tag:** Brute Force, Forced Authentication, Valid Accounts, Account Manipulation
- **ATT&CK ID:** T1110, T1110.001, T1110.002, T1110.004, T1187, T1078, T1098
- **Minimum Log Source Requirement:** Solaris LDAP
- **Query:**

```
norm_id=SolarisLDAP label=User (label=Login OR label=Authentication) label=Fail | chart count() as cnt by user | search cnt > 5
```

SolarisLDAP User Account Lockout Detected

- **Trigger Condition:** A locked user account is detected.
- **ATT&CK Category:** Defense Evasion, Persistence, Privilege Escalation, Initial Access
- **ATT&CK Tag:** Valid Accounts, Abuse Elevation Control Mechanism, Bypass User Access Control
- **ATT&CK ID:** T1078, T1548
- **Minimum Log Source Requirement:** Solaris LDAP
- **Query:**

```
norm_id=SolarisLDAP label=User label=Account label=Lock
```

Sophos XG Firewall - Inbound Attack Detected by IDP

- **Trigger Condition:** An inbound attack defined in IDP policy is detected.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Network Denial of Service, Endpoint Denial of Service
- **ATT&CK ID:** T1498, T1499
- **Minimum Log Source Requirement:** Sophos XG Firewall
- **Query:**

```
norm_id=SophosXGFirewall label=Attack label=Detect label=IDP destination_address=* -source_address in HOMENET | process geoip(source_address) as country
```

Sophos XG Firewall - Outbound Attack Detected by IDP

- **Trigger Condition:** An outbound attack defined in IDP policy is detected.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Network Denial of Service, Endpoint Denial of Service
- **ATT&CK ID:** T1498, T1499
- **Minimum Log Source Requirement:** Sophos XG Firewall
- **Query:**

```
norm_id=SophosXGFirewall label=Attack label=Detect label=IDP destination_address=* -destination_address in HOMENET | process geoip(destination_address) as country
```

SophosUTM Policy Violation

- **Trigger Condition:** Different policy violation from a source is detected. For this alert to work, the following list must be updated;
    - EXTREMIST _CONTENT, for example, weapons.
    - CONCERNED _CONTENT, for example, alcohol, tobacco, gambling, and so on.
    - CRIMINAL _CONTENT, for example, hacking, drugs, and so on.
    - VULNERABLE _CONTENT, for example, abuse, and so on.
- **ATT&CK Category:** Defense Evasion, Privilege Escalation, Credential Access
- **ATT&CK Tag:** Abuse Elevation Control Mechanism, Bypass User Access Control, Group Policy Modification, Exploitation for Credential Access, Exploitation for Privilege Escalation
- **ATT&CK ID:** T1548, T1484, T1212, T1068
- **Minimum Log Source Requirement:** Sophos UTM
- **Query:**
-
  ```
  norm_id=SophosUTM category_name=* source_address=* | chart count(category_name IN EXTREMIST_CONTENT) as Extremist, count(category_name IN CONCERNED_CONTENT) as Concerning, count(category_name IN CRIMINAL_CONTENT) as Criminal, count(category_name IN VULNERABLE_CONTENT) as Vulnerable by source_address, user | chart sum(Extremist+Concerning+Criminal+Vulnerable) as Violation by Extremist, Concerning, Criminal, Vulnerable, source_address,
  ```
-
  ```
  user order by Violation | search Violation>1
  ```

SourceFire DNS Tunneling Detection - Multiple domains

- **Trigger Condition:** The source address is detected with queries for more than 50 domains.
- **ATT&CK Category:** Impact, Command and Control
- **ATT&CK Tag:** Network Denial of Service, Proxy, Domain Fronting
- **ATT&CK ID:** T1498, T1090, T1090.004, T1568, T1568.002
- **Minimum Log Source Requirement:** Sourcefire
- **Query:**
-
  ```
  norm_id=SourceFire domain=* -domain in HOME_DOMAIN | norm on message <:all><:'(?i)dns request'><:all><:'domain'><domain:string> | chart distinct_count(domain) as DomainCount by source_address | search DomainCount > 50
  ```

SSHD Connection Denied

- **Trigger Condition:** Ten denied connections are detected from the same source.
- **ATT&CK Category:** Lateral Movement, Command and Control, Impact
- **ATT&CK Tag:** Remote Services, Commonly Used Port, Network Denial of Service, Endpoint Denial of Service
- **ATT&CK ID:** T1021, T1498, T1499
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**
-
  ```
  [10 norm_id=Unix label=Connection label=Deny having same source_address within 10 seconds]
  ```

Stealthy Scheduled Task Creation via VBA Macro Detected

- **Trigger Condition:** Creation of stealthy scheduled tasks via VBA macro is detected.
- **ATT&CK Category:** Execution, Persistence, Privilege Escalation
- **ATT&CK Tag:** Scheduled Task/Job, Scheduled Task
- **ATT&CK ID:** T1053, T1053.005
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

-
  ```
  norm_id=WindowsSysmon event_id=7 image="*taskschd.dll" source_image in ["*winword.exe", "*excel.exe", "*powerpnt.exe", "*outlook.exe"] -user IN EXCLUDED_USERS
  ```

Sticky Key Like Backdoor Usage Detected

- **Trigger Condition:** The use and installation of a backdoor that uses an option to register a malicious debugger for built-in tools that are accessible on the login screen. Sticky keys are a Windows accessibility feature that allows a user to press a modifier key (For example, Shift, Ctrl, Alt) and remain active until another key is pressed. Adversaries may use a sticky key-like backdoor to gain unauthorized access to a system by pressing a specific combination of keys. This can allow them to execute malicious code or bypass security controls.
- **ATT&CK Category:** Privilege Escalation, Persistence
- **ATT&CK Tag:** Event Triggered Execution, Accessibility Features
- **ATT&CK ID:** T1546, T1546.008
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

-
  ```
  (norm_id=WindowsSysmon event_id=13 target_object IN ["*\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\*\Debugger"] event_type="SetValue") OR (event_id=1 parent_image="*\winlogon.exe" command IN ["*cmd.exe sethc.exe *", "*cmd.exe utilman.exe *", "*cmd.exe osk.exe *", "*cmd.exe Magnify.exe *", "*cmd.exe Narrator.exe *", "*cmd.exe DisplaySwitch.exe *"])
  ```

StoneDrill Service Install Detected

- **Trigger Condition:** Service install of the malicious Microsoft Network Realtime Inspection Service described in StoneDrill report by Kaspersky is detected.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** New Service
- **ATT&CK ID:** T1543
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=7045 service_type="NtsSrv" service="* LocalService" -user IN EXCLUDED_USERS
```

Stop Windows Service Detected

- **Trigger Condition:** Windows Service stops.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Service Stop
- **ATT&CK ID:** T1489
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 image IN ["*\sc.exe", "*\net.exe", "*\net1.exe"] command="*stop*" -user IN EXCLUDED_USERS
```

Successful Lateral Movement to Administrator via Pass the Hash using Mimikatz Detected

- **Trigger Condition:** Lateral Movement is successful in compromising the admin account via Pass the Hash method.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Use Alternate Authentication Material, Pass the Hash
- **ATT&CK ID:** T1550, T1550.002
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
[norm_id=WinServer event_id=4624 logon_type=9 logon_process=seclogo package=Negotiate label=User label=Login label=Successful -user IN EXCLUDED_USERS] as s1
followed by [norm_id=WinServer event_id=4672 label=Privilege label=Assign] as s2 on s1.user=s2.user | rename s1.log_ts
as log_ts, s1.user as user, s1.domain as domain, s1.user_id as user_id, s1.host as host
```

Successful Overpass the Hash Attempt

- **Trigger Condition:** Successful logon with logon type 9 (NewCredentials), which matches the Overpass the Hash behavior of Mimikatz’s sekurlsa::pth module is detected.
- **ATT&CK Category:** Lateral Movement, Defense Evasion
- **ATT&CK Tag:** T1550 - Use Alternate Authentication Material (2), T1550.002 - Pass the Hash (2)
- **Minimum Log Source Requirement:** Windows
- **Query:**

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

Suspect Svchost Activity Detected

- **Trigger Condition:** Scvhost activity is detected. It is abnormal for svchost.exe to spawn without any CLI arguments and is observed when a malicious process spawns the process and injects code into the process memory space.
- **ATT&CK Category:** Defense Evasion, Privilege Escalation
- **ATT&CK Tag:** Process Injection
- **ATT&CK ID:** T1055
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 -command=* image="*\svchost.exe" -parent_image IN ["*\rpcnet.exe", "*\rpcnetp.exe"] -user IN EXCLUDED_USERS
```

Suspect Svchost Memory Access

- **Trigger Condition:** When access to svchost process memory such as that used by Invoke-Phantom to kill the winRM windows event logging service is detected. The “svchost.exe” process is a legitimate system that hosts multiple Windows services. However, adversaries may use this process to execute malicious code or gain unauthorized system access.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Impair Defenses, Disable or Modify Tools
- **ATT&CK ID:** T1562, T1562.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=10 image="*\windows\system32\svchost.exe" access="0x1f3fff" call_trace="*unknown*" -user IN EXCLUDED_USERS
```

Suspicious Access to Sensitive File Extensions

- **Trigger Condition:** Sensitive file extensions are detected.
- **ATT&CK Category:** Collection
- **ATT&CK Tag:** Data Staged
- **ATT&CK ID:** T1074
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=5145 relative_target IN ["*.pst", "*.ost", "*.msg", "*.nst", "*.oab", "*.edb", "*.nsf",
"*.bak", "*.dmp", "*.kirbi", "*\groups.xml", "*.rdp"] -user IN EXCLUDED_USERS
```

Suspicious Calculator Usage Detected

- **Trigger Condition:** The use of calc.exe with command line parameters or in a suspicious directory, which is likely caused by some PoC or detection evasion, is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Masquerading
- **ATT&CK ID:** T1036

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

```
norm_id=WindowsSysmon event_id=1 (command="*\calc.exe *" OR (event_id=1 image="*\calc.exe" -image="*\Windows\Sys*")) -user IN EXCLUDED_USERS
```

Suspicious Call by Ordinal Detected

- **Trigger Condition:** When suspicious calls of DLLs through RUNDLL32 via ordinal. This search looks for executing scripts with rundll32. Adversaries may abuse rundll32.exe to proxy the execution of malicious code. Using rundll32.exe, vice executing directly, may avoid triggering security tools that may not monitor the execution of the rundll32.exe process because of allowlists or false positives from normal operations.
- **ATT&CK Category:** Defense Evasion, Execution
- **ATT&CK Tag:** Signed Binary Proxy Execution, Rundll32
- **ATT&CK ID:** T1218, T1218.011
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WinServer event_id=4688 "process"="*\rundll32.exe" command IN ["*,#*", "*, #*", "*.dll #*", "*.ocx #*"] -command IN ["*EDGEHTML.DLL*", "*#141*"] -user IN EXCLUDED_USERS
```

Suspicious Certutil Command Detected

- **Trigger Condition:** Microsoft certutil execution with subcommands like *decode* used to decode malicious code with the built-in certutil utility is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Deobfuscate/Decode Files or Information, Remote File Copy
- **ATT&CK ID:** T1140, T1105
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label="process" label=create command IN ["* -decode *", "* /decode *", "* -decodehex *", "* /decodehex *", "* -urlcache *", "* /urlcache *", "* -verifyctl *", "* /verifyctl *", "* -encode *", "* /encode *", "*certutil* -URL*", "*certutil* /URL*", "*certutil* -ping*", "*certutil* /ping*"] -user IN EXCLUDED_USERS
```

Suspicious Code Page Switch Detected

- **Trigger Condition:** Code page switch in a command line or batch scripts to a rare language is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Deobfuscate/Decode Files or Information
- **ATT&CK ID:** T1140
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 command IN ["chcp* 936", "chcp* 1258"] -user IN EXCLUDED_USERS
```

Suspicious Commandline Escape Detected

- **Trigger Condition:** Suspicious processes that use escape characters.
- **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=WindowsSysmon event_id=1 command IN ["*h^t^t^p*", "*h\t\t\p*"] -user IN EXCLUDED_USERS
```

Suspicious Compression Tool Parameters

- **Trigger Condition:** Suspicious command line arguments of data compression tools are detected.
- **ATT&CK Category:** Collection
- **ATT&CK Tag:** Automated Exfiltration, Data Compressed, Archive Collected Data
- **ATT&CK ID:** T1020, T1560
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 file IN ["7z*.exe", "*rar.exe", "*Command*Line*RAR*"] command IN ["* -p*", "* -ta*", "* -tb*", "* -sdel*", "* -dw*", "* -hp*"] -parent_image="C:\Program*" -user IN EXCLUDED_USERS
```

Suspicious Control Panel DLL Load Detected

- **Trigger Condition:** Execution of a suspicious Signed Binary Proxy Execution or Rundll32 from *control.exe* used by Equation Group and Exploit Kits.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Hijack Execution Flow, DLL Side-Loading,Signed Binary Proxy Execution, Rundll32
- **ATT&CK ID:** T1574, T1574.002, T1218, T1218.011
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 parent_image="*\System32\control.exe" command="*\rundll32.exe *" -command="*Shell32.dll*" -user IN EXCLUDED_USERS
```

Suspicious Csc Source File Folder Detected

- **Trigger Condition:** Execution of *csc.exe* that uses a source in a suspicious folder is detected. For example, AppData.
- **ATT&CK Category:** Execution, Defense Evasion

- **ATT&CK Tag:** Obfuscated Files or Information, Compile After Delivery, User Execution
- **ATT&CK ID:** T1027, T1027.004, T1204
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create "process"="*\csc.exe" command IN ["*\AppData\*", "*\Windows\Temp\*"] -(parent_process ="*:\Program Files*" parent_process in ["*\sdiagnhost.exe", "*\w3wp.exe", "*\choco.exe"] ) -user IN EXCLUDED_USERS
```

Suspicious Debugger Registration Detected

- **Trigger Condition:** Registration of a debugger for a program available in the logon screen (sticky key backdoor).
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Obfuscated Files or Information, Compile After Delivery
- **ATT&CK ID:** T1027, T1027.004
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label="process" label=create command IN ["*\CurrentVersion\Image File Execution Options\sethc.exe*", "*\CurrentVersion\Image File Execution Options\utilman.exe*", "*\CurrentVersion\Image File Execution Options\osk.exe*", "*\CurrentVersion\Image File Execution Options\magnify.exe*", "*\CurrentVersion\Image File Execution Options\narrator.exe*", "*\CurrentVersion\Image File Execution Options\displayswitch.exe*", "*\CurrentVersion\Image File Execution Options\atbroker.exe*"]
```

Suspicious Double Extension Detected

- **Trigger Condition:** The use of double .exe extension of file is detected. The query searches for double extension in process name and in command line.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Double File Extension
- **ATT&CK ID:** T1036.007
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create ("process" IN ["*.doc.exe", "*.docx.exe", "*.tmp.bat","*.xls.exe","*.bat.exe","*.xlsx.exe", "*.ppt.exe", "*.pptx.exe", "*.rtf.exe", "*.pdf.exe", "*.bat.exe", "*.txt.exe", "* .exe", "*______.exe"] OR command IN ["*.doc.exe", "*.docx.exe", "*.tmp.bat","*.xls.exe","*.bat.exe","*.xlsx.exe", "*.ppt.exe", "*.pptx.exe", "*.rtf.exe", "*.pdf.exe", "*.bat.exe", "*.txt.exe", "* .exe", "*______.exe"] )
```

Suspicious Driver Load from Temp

- **Trigger Condition:** Driver load from a temporary directory is detected.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** New Service

- **ATT&CK ID:** T1543
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  norm_id=WindowsSysmon event_id=6 image="*\Temp\*" -user IN EXCLUDED_USERS
  ```

Suspicious Eventlog Clear or Configuration Using Wevtutil Detected

- **Trigger Condition:** Clearing or configuration of eventlogs uwing wevtutil, PowerShell and wmic is detected. It is used by ransomware during the attack as seen by NotPetya and others.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Indicator Removal on Host
- **ATT&CK ID:** T1070
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  label="Process" label=Create ((("process" IN ["*\powershell.exe","*\pwsh.exe*"] command IN ["*Clear-EventLog*", "*Remove-EventLog*", "*Limit-EventLog*","*Clear-WinEvent*"]) OR ("process"="*\wmic.exe" command="* ClearEventLog *")) OR ("process"="*\wevtutil.exe" command IN ["*clear-log*", "* cl *", "*set-log*", "* sl *"])) -user IN EXCLUDED_USERS
  ```

Suspicious Execution from Outlook

- **Trigger Condition:** *EnableUnsafeClient MailRules* used for Script Execution from Outlook is detected.
- **ATT&CK Category:** Execution, Defense Evasion
- **ATT&CK Tag:** Command and Scripting Interpreter, Indirect Command Execution
- **ATT&CK ID:** T1059, T1202
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**
-
  ```
  label="Process" label=Create (command="*EnableUnsafeClientMailRules*" OR (parent_process="*\outlook.exe" command="\\*\*.exe")) -user IN EXCLUDED_USERS
  ```

Suspicious GUP Usage Detected

- **Trigger Condition:** Execution of the Notepad++ updater in a suspicious directory used in DLL side-loading attacks.
- **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=1 image="*\GUP.exe" -image IN ["C:\Users\*\AppData\Local\Notepad++\updater\gup.exe",  "C:\Users\*\AppData\Roaming\Notepad++\updater\gup.exe",
  ```

-
  ```
  "C:\Program Files\Notepad++\updater\gup.exe", "C:\Program Files (x86)\Notepad++\updater\gup.exe"] -user IN EXCLUDED_USERS
  ```

Suspicious HWP Sub Processes Detected

- **Trigger Condition:** Hangul Word Processor (Hanword) sub-processes that could indicate exploitation are detected.
- **ATT&CK Category:** Execution, Defense Evasion, Initial Access
- **ATT&CK Tag:** Command-Line Interface, Indirect Command Execution, Phishing, Spearphishing Attachment
- **ATT&CK ID:** T1059, T1202, T1566, T1566.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

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

Suspicious In-Memory Module Execution Detected

- **Trigger Condition:** An access to processes by other suspicious processes that have reflectively loaded libraries in their memory space are detected.
- **ATT&CK Category:** Privilege Escalation
- **ATT&CK Tag:** Process Injection
- **ATT&CK ID:** T1055
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

-
  ```
  norm_id=WindowsSysmon event_id=10 (call_trace IN ["C:\Windows\SYSTEM32\ntdll.dll+*", "C:\Windows\System32\KERNELBASE.dll+*", "*UNKNOWN(*)"] OR (call_trace="*UNKNOWN*" access IN ["0x1F0FFF", "0x1F1FFF", "0x143A", "0x1410", "0x1010", "0x1F2FFF", "0x1F3FFF", "0x1FFFFF"])) -user IN EXCLUDED_USERS
  ```

Suspicious Kerberos RC4 Ticket Encryption

- **Trigger Condition:** Service ticket requests using the RC4 encryption type are detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Steal or Forge Kerberos Tickets, Kerberoasting
- **ATT&CK ID:** T1558, T1558.003
- **Minimum Log Source Requirement:** Windows
- **Query:**

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

Suspicious Keyboard Layout Load Detected

- **Trigger Condition:** Keyboard preload installation with a suspicious keyboard layout is detected. For example, Chinese, Iranian, or Vietnamese layout load in user sessions on systems maintained by US staff only.
- **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 IN ["*\Keyboard Layout\Preload\\*", "*\Keyboard Layout\Substitutes\\*"] detail IN ["*00000429*", "*00050429*", "*0000042a*"]
-user IN EXCLUDED_USERS
```

Suspicious MsiExec Directory Detected

- **Trigger Condition:** Suspicious *msiexec* process starting in a different directory 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 image="*\msiexec.exe" -image IN ["C:\Windows\System32\*", "C:\Windows\SysWOW64\*", "C:\Windows\WinSxS\*"]
-user IN EXCLUDED_USERS
```

Suspicious Named Pipes Detected

- **Trigger Condition:** Suspicious named pipes 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:**

```
event_id IN ["17", "18"] pipe IN ["\isapi_http", "\isapi_dg", "\isapi_dg2", "\sdlrpc", "\ahexec", "\winsession", "\lsassw", "\46a676ab7f179e511e30dd2dc41bd388",
"\9f81f59bc58452127884ce513865ed20", "\e710f28d59aa529d6792ca6ff0ca1b34", "\rpch 3", "\NamePipe_MoreWindows", "\pcheap_reuse", "\msagent_*", "\gruntsvc", "*\PSEXESVC*",
"*\PowerShellISEPipeName_*", "*\csexec*", "*\paexec*", "*\remcom*"] -user IN EXCLUDED_USERS
```

Suspicious Outbound Kerberos Connection

- **Trigger Condition:** An outbound network activity via Kerberos default port indicating possible lateral movement or first stage PrivEsc via delegation is detected.

- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Steal or Forge Kerberos Tickets, Kerberoasting
- **ATT&CK ID:** T1558, T1558.003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

-
  ```
  norm_id=Windows* (event_id=3 OR event_id=5156) destination_port="88" -image IN ["*\lsass.exe", "*\opera.exe", "*\chrome.exe", "*\firefox.exe"] -user IN EXCLUDED_USERS
  ```

Suspicious Outbound RDP Connections Detected

- **Trigger Condition:** Non-Standard tools connecting to TCP port 3389 indicating possible Lateral Movement are detected.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Exploitation of Remote Services
- **ATT&CK ID:** T1210
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

-
  ```
  norm_id=WindowsSysmon event_id=3 destination_port="3389" initiated="true" -image IN ["*\mstsc.exe", "*\RTSApp.exe", "*\RTS2App.exe", "*\RDCMan.exe", "*\ws_TunnelService.exe", "*\RSSensor.exe",
  ```

-
  ```
  "*\RemoteDesktopManagerFree.exe", "*\RemoteDesktopManager.exe", "*\RemoteDesktopManager64.exe", "*\mRemoteNG.exe", "*\mRemote.exe", "*\Terminals.exe", "*\spiceworks-finder.exe", "*\FSDiscovery.exe", "*\FSAssessment.exe", "*\MobaRTE.exe", "*\chrome.exe", "*\thor.exe", "*\thor64.exe"] -user IN EXCLUDED_USERS
  ```

Suspicious Parent of Csc Detected

- **Trigger Condition:** Suspicious parent of csc.exe is a sign of payload delivery 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 image="*\csc.exe*" parent_image IN ["*\wscript.exe", "*\cscript.exe", "*\mshta.exe"] -user IN EXCLUDED_USERS
  ```

Suspicious PowerShell Invocation Based on Parent Process

- **Trigger Condition:** PowerShell invocations from interpreters or unusual programs like wscript or IIS worker process(w3wp.exe) are detected. Admins can add other suspicious parent processes to increase visibility.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, PowerShell

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

```
label="process" label=create parent_process  IN ["*\mshta.exe", "*\wscript.exe", "*\cscript.exe", "*\rundll32.exe", "*\regsvr32.exe", "*\services.exe", "*\winword.exe", "*\wmiprvse.exe", "*\powerpnt.exe", "*\excel.exe", "*\msaccess.exe", "*\mspub.exe", "*\visio.exe", "*\outlook.exe", "*\amigo.exe", "*\chrome.exe", "*\firefox.exe", "*\iexplore.exe", "*\microsoftedgecp.exe", "*\microsoftedge.exe", "*\browser.exe", "*\vivaldi.exe", "*\safari.exe", "*\sqlagent.exe", "*\sqlserver.exe", "*\sqlservr.exe", "*\w3wp.exe", "*\httpd.exe", "*\nginx.exe", "*\php-cgi.exe", "*\jbosssvc.exe", "*MicrosoftEdgeSH.exe", "*tomcat*"]  "process"="*\powershell.exe" -path="*\Health Service State\*" (command IN ["*powershell*", "*pwsh*"] ) -user IN EXCLUDED_USERS
```

Suspicious PowerShell Parameter Substring Detected

- **Trigger Condition:** Suspicious Command and Scripting Interpreter and PowerShell invocation with a parameter substring 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:**

```
label=create label="process" "process"="*\powershell.exe" command IN ["* -en*", "* -ec *", "* -noni*", "* -nop*", "* -exe* bypass*", "* -ep bypass*", "* -win* hid*", "* -w hid*", "* -sta *"]
```

Suspicious Process Start Locations Detected

- **Trigger Condition:** Execution of processes run from an unusual locations like Recycle bin or Fonts folder 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 image IN ["*:\RECYCLER\*", "*:\SystemVolumeInformation\*", "C:\Windows\Tasks\*", "C:\Windows\debug\*", "C:\Windows\fonts\*", "C:\Windows\help\*", "C:\Windows\drivers\*", "C:\Windows\addins\*", "C:\Windows\cursors\*", "C:\Windows\system32\tasks\*", "*\Windows\IME\*",
"C:\Perflogs\*", "*\Windows\IME\*"] -user IN EXCLUDED_USERS
```

Suspicious Program Location with Network Connections

- **Trigger Condition:** Network connections run in suspicious file system locations.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Masquerading

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

```
norm_id=WindowsSysmon event_id=3 image IN ["*\$Recycle.bin", "*\Users\All Users\*", "*\Users\Default\*", "*\Users\Public\*", "*\Users\Contacts\*", "*\Users\Searches\*", "C:\Perflogs\*", "*\config\systemprofile\*", "*\Windows\Fonts\*", "*\Windows\IME\*", "*\Windows\addins\*"] -user IN EXCLUDED_USERS
```

Suspicious PsExec Execution Detected

- **Trigger Condition:** Execution of *psexec* or *paexec* with the renamed service name.This rule helps filter out the noise if psexec is used for legitimate purposes or if an attacker uses a different psexec client other than sysinternal one.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Remote Services
- **ATT&CK ID:** T1021
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=5145 share_name="IPC$" relative_target IN ["*-stdin", "*-stdout", "*-stderr"] -relative_target="PSEXESVC*" -user IN EXCLUDED_USERS
```

Suspicious RDP Redirect Using TSCON Detected

- **Trigger Condition:** A suspicious RDP session redirect using *tscon.exe*.
- **ATT&CK Category:** Lateral Movement, Privilege Escalation
- **ATT&CK Tag:** Remote Services, Remote Desktop Protocol
- **ATT&CK ID:** T1021, T1021.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 command="* /dest:rdp-tcp:*" -user IN EXCLUDED_USERS
```

Suspicious Remote Thread Created

- **Trigger Condition:** The suspicious processes (like word.exe or outlook.exe) create remote threads on other processes. This technique is used by malware to inject code and hide in other processes. The event indicates the source and target process. It gives information on the code that will run in the new thread: StartAddress, StartModule and StartFunction.
- **ATT&CK Category:** Privilege Escalation
- **ATT&CK Tag:** Process Injection
- **ATT&CK ID:** T1055
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=8 source_image IN ["*\bash.exe", "*\cvtres.exe", "*\defrag.exe", "*\dnx.exe", "*\esentutl.exe", "*\excel.exe", "*\expand.exe", "*\explorer.exe", "*\find.exe",
"*\findstr.exe", "*\forfiles.exe", "*\git.exe", "*\gpupdate.exe", "*\hh.exe", "*\iexplore.exe", "*\installutil.exe", "*\lync.exe", "*\makecab.exe", "*\mDNSResponder.exe", "*\monitoringhost.exe",
"*\msbuild.exe", "*\mshta.exe", "*\msiexec.exe", "*\mspaint.exe", "*\outlook.exe", "*\ping.exe", "*\powerpnt.exe", "*\powershell.exe", "*\provtool.exe", "*\python.exe", "*\regsvr32.exe", "*\robocopy.exe", "*\runonce.exe",
"*\sapcimc.exe", "*\schtasks.exe", "*\smartscreen.exe", "*\spoolsv.exe", "*\tstheme.exe", "*\userinit.exe", "*\vssadmin.exe", "*\vssvc.exe", "*\w3wp.exe*", "*\winlogon.exe", "*\winscp.exe", "*\wmic.exe", "*\word.exe", "*\wscript.exe"]
-source_image="*Visual Studio*" -user IN EXCLUDED_USERS
```

Suspicious RUN Key from Download Detected

- **Trigger Condition:** A suspicious RUN keys created by software located in the Download or temporary Outlook/Internet Explorer directories.
- **ATT&CK Category:** Persistence, Privilege Escalation
- **ATT&CK Tag:** Boot or Logon Autostart Execution, Registry Run Keys/Startup Folder
- **ATT&CK ID:** T1547, T1547.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=13 image IN ["*\Downloads\*", "*\Temporary Internet Files\Content.Outlook\*", "*\Local Settings\Temporary Internet Files\*"] target_object="*\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\*" -user IN EXCLUDED_USERS
```

Suspicious Rundll32 Activity Detected

- **Trigger Condition:** Processes related to the RunDLL32 system binary based on its command-line arguments. Adversaries may abuse RunDLL32 to proxy code executions and avoid triggering security tools that may not monitor the execution of the rundll32.exe process because of allowlists or false positives from normal operations. Whitelisting is required due to the inherent system noise of RunDLL32.
- **ATT&CK Category:** Defense Evasion, Execution
- **ATT&CK Tag:** Signed Binary Proxy Execution, Rundll32
- **ATT&CK ID:** T1218, T1218.011
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label="process" label=create ((command IN ["*\rundll32.exe* url.dll, *OpenURL *", "*\rundll32.exe* url.dll, *OpenURLA *", "*\rundll32.exe* url.dll, *FileProtocolHandler *", "*\rundll32.exe* zipfldr.dll, *RouteTheCall *", "*\rundll32.exe* Shell32.dll, *Control_RunDLL *", "*\rundll32.exe javascript:*", "* url.dll, *OpenURL *", "* url.dll, *OpenURLA *", "* url.dll, *FileProtocolHandler *", "* zipfldr.dll, *RouteTheCall *", "* Shell32.dll, *Control_RunDLL *", "* javascript:*", "*.RegisterXLL*", "*\rundll32*C:\PerfLogs\*", "*\rundll32*C:\ProgramData\*", "*\rundll32*\AppData\Local\Temp\*"]) OR ("process"="*\rundll32.exe" pare
nt_process IN ["*\cmd.exe", "*\powershell.exe"] parent_command="*.lnk*" parent_command IN ["* /c *", "* /k *"] parent_command IN ["C:\ProgramData\", "*\AppData\Local\Temp\*", "*\AppData\Roaming\Temp\*", "C:\Users\Public\", "C:\Windows\tracing\"])) -user IN EXCLUDED_USERS
```

Suspicious Scripting in a WMI Consumer

- **Trigger Condition:** Suspicious scripting in the WMI Event Consumers.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, PowerShell
- **ATT&CK ID:** T1059, T1059.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  norm_id=WindowsSysmon event_id=20 destination IN ["*new-object .webclient).downloadstring(*", "*new-object .webclient).downloadfile(*", "*new-object net.webclient).downloadstring(*", "*new-object net.webclient).downloadfile(*", "* iex(*", "*WScript.shell*", "* -nop *", "* -noprofile *", "* -decode *", "* -enc *"] -user IN EXCLUDED_USERS
  ```

Suspicious Service Path Modification Detected

- **Trigger Condition:** Modification of service path to *powershell/cmd*.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Modify Existing Service
- **ATT&CK ID:** T1569, T1569.002
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  norm_id=WindowsSysmon event_id=1 image="*\sc.exe" command IN ["*powershell*", "*cmd*"] command IN ["*binpath*", "*config*"] -user IN EXCLUDED_USERS
  ```

Suspicious Svchost Process Detected

- **Trigger Condition:** Suspicious *svchost* process starts.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Masquerading, Match Legitimate Name or Location
- **ATT&CK ID:** T1036, T1036.005
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  norm_id=WindowsSysmon event_id=1 image="*\svchost.exe" -parent_image IN ["*\services.exe", "*\MsMpEng.exe", "*\Mrt.exe", "*\rpcnet.exe", "*\svchost.exe"] parent_image=* -user IN EXCLUDED_USERS
  ```

Suspicious SYSVOL Domain Group Policy Access

- **Trigger Condition:** Access to Domain Group Policies stored in SYSVOL detected.
- **ATT&CK Category:** Credential Access

- **ATT&CK Tag:** Unsecured Credentials, Group Policy Preferences
- **ATT&CK ID:** T1552, T1552.006
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

-
  ```
  norm_id=WindowsSysmon event_id=1 command="*\SYSVOL\*\policies\*" -user IN EXCLUDED_USERS
  ```

Suspicious TSCON Start

- **Trigger Condition:** *tscon.exe* process execution as LOCAL SYSTEM is detected. If *tscon.exe* run as SYSTEM, users can gain access to the currently logged-in session without credential.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Remote Access Software
- **ATT&CK ID:** T1219
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

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

Suspicious Typical Malware Back Connect Ports Detected

- **Trigger Condition:** Programs connecting to a typical malware back connect ports based on statistical analysis from two different sandbox system databases are detected.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Non-Standard Port
- **ATT&CK ID:** T1571
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

-
  ```
  destination_port IN ["4443", "2448", "8143", "1777", "1443", "243", "65535", "13506", "3360", "200", "198", "49180", "13507", "6625", "4444", "4438", "1904", "13505", "13504", "12102", "9631", "5445",
  ```

-
  ```
  "2443", "777", "13394", "13145", "12103", "5552", "3939", "3675", "666", "473", "5649", "4455", "4433", "1817", "100", "65520", "1960", "1515", "743", "700", "14154", "14103", "14102", "12322", "10101", "7210", "4040", "9943"] -image="*\Program Files*"
  ```

-
  ```
  -destination_address IN HOMENET -user IN EXCLUDED_USERS
  ```

Suspicious CSharp or FSharp Interactive Console Execution

- **Trigger Condition:** Execution of CSharp or FSharp interactive console by scripting utilities like WScript or PowerShell detected. The alert warns you of the use of the .NET framework by attackers for offensive purposes.
- **ATT&CK Category:** Defense Evasion

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

-
  ```
  norm_id=WindowsSysmon event_id=1 image IN ["*\csi.exe", "*\fsi.exe"] parent_image IN ["*\cmd.exe", "*\powershell.exe", "*\wscript.exe", "*\cscript.exe"] -user IN EXCLUDED_USERS
  ```

Suspicious Userinit Child Process

- **Trigger Condition:** Suspicious child process of *userinit* 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 parent_image="*\userinit.exe" -command="*\net logon\*" -image="*\explorer.exe" -user IN EXCLUDED_USERS
  ```

Suspicious Windows ANONYMOUS LOGON Local Account Creation

- **Trigger Condition:** Creation of suspicious accounts similar to ANONYMOUS LOGON like using additional spaces, is detected. It is created to catch the exclusion of Logon Type 3 from ANONYMOUS LOGON accounts.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Create Account
- **ATT&CK ID:** T1136
- **Minimum Log Source Requirement:** Windows
- **Query:**

-
  ```
  norm_id=WinServer event_id=4720 user="*ANONYMOUS*LOGON*" -user IN EXCLUDED_USERS
  ```

Suspicious WMI Execution Detected

- **Trigger Condition:** When WMI executing suspicious commands including but not limited to AV product enumeration and remote process creation are detected. WMIC.exe is a built-in Microsoft program that allows command-line access to the Windows Management Instrumentation. Adversaries can use this technique to create remote or local processes, get details about antivirus and firewalls, delete shadow copies and modify defender configurations.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Windows Management Instrumentation
- **ATT&CK ID:** T1047
- **Minimum Log Source Requirement:** Windows Sysmon

- **Query:**

```
label="Process" label=Create ("process"="*\wmic.exe" or file=wmic.exe) command IN ["*/node:*process call create *", "* path AntiVirusProduct get *", "* path FirewallProduct get *", "* shadowcopy delete *","*csproduct get*UUID*", "*NAMESPACE:\\root\Microsoft\Windows\Defender*"]
```

Svchost DLL Search Order Hijack Detected

- **Trigger Condition:** Svchost DLL Search Order Hijack is detected. By default, IKEEXT and SessionEnv service call LoadLibrary on files that does not exist within *C:/Windows/System 32/*. An attacker can place their malicious logic within the PROCESS_ATTACH block of their library and restart the services mentioned above *svchost.exe -k netsvcs* to gain code execution on a remote machine.
- **ATT&CK Category:** Persistence, Privilege Escalation, Defense Evasion
- **ATT&CK Tag:** Hijack Execution Flow, DLL Side-Loading, DLL Search Order Hijacking
- **ATT&CK ID:** T1574, T1574.002, T1574.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=7 source_image IN ["*\svchost.exe"] image IN ["*\tsmsisrv.dll", "*\tsvipsrv.dll", "*\wlbsctrl.dll"] -image IN ["C:\Windows\WinSxS\*"] -user IN EXCLUDED_USERS
```

SysKey Registry Keys Access

- **Trigger Condition:** Requests and access operations to specific registry keys to calculate the SysKey are detected. Adversaries use a tool (like Mimikatz) or a script (like Invoke-PowerDump) to get the SysKey to decrypt Security Account Manager (SAM) database entries from registry or hive and get NTLM and LM hashes of local accounts passwords.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Query Registry
- **ATT&CK ID:** T1012
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id IN [4656, 4663] object_type="key" object_name IN ["*lsa\JD", "*lsa\GBG", "*lsa\Skew1", "*lsa\Data"]
-user IN EXCLUDED_USERS
```

Sysmon Configuration Modification Detected

- **Trigger Condition:** Modification in Sysmon configuration.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Impair Defenses, Indicator Blocking
- **ATT&CK ID:** T1562, T1562.006
- **Minimum Log Source Requirement:** Windows Sysmon

- **Query:**

```
norm_id=WindowsSysmon label=Sysmon label=Config label=Change -user IN EXCLUDED_USERS
```

Sysmon Driver Unload Detected

- **Trigger Condition:** Unloading of Sysmon driver is detected. After error events are logged, logs will not be collected and parsed by Sysmon.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Impair Defenses, Disable or Modify Tools
- **ATT&CK ID:** T1562, T1562.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=255 id="DriverCommunication" -user IN EXCLUDED_USERS
```

Sysmon Error Event Detected

- **Trigger Condition:** Sysmon error event is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Impair Defenses, Disable or Modify Tools
- **ATT&CK ID:** T1562, T1562.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=255 -user IN EXCLUDED_USERS
```

System File Execution Location Anomaly Detected

- **Trigger Condition:** Starting a Windows program executable in a suspicious folder is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Masquerading
- **ATT&CK ID:** T1036
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process" IN ["*\svchost.exe", "*\rundll32.exe", "*\services.exe", "*\powershell.exe", "*\regsvr32.exe", "*\spoolsv.exe", "*\lsass.exe", "*\smss.exe", "*\csrss.exe", "*\conhost.exe", "*\wininit.exe", "*\lsm.exe", "*\winlogon.exe", "*\explorer.exe", "*\taskhost.exe"] -"process" IN ["C:\Windows\System32\*", "C:\Windows\SysWow64\*", "C:\Windows\explorer.exe", "C:\Windows\winsxs\*", "\SystemRoot\System32\*"] -user IN EXCLUDED_USERS
```

System Information Discovery

- **Trigger Condition:** Discovery of system information via *sysinfo* or *net* command is detected.

- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** System Information Discovery
- **ATT&CK ID:** T1082
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**
-
  ```
  label=Create label="Process" ("process"="*\sysinfo.exe" OR command="*net* config*") -user IN EXCLUDED_USERS
  ```

System Owner or User Discovery

- **Trigger Condition:** Detected MITRE ATT&CK T1033.
- **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=1 (image IN ["*\whoami.exe", "*\qwinsta.exe", "*\quser.exe"] OR command="*wmic* useraccount get*")
  ```

System Service Discovery

- **Trigger Condition:** Detected MITRE ATT&CK T1007.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** System Service Discovery
- **ATT&CK ID:** T1007
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  norm_id=WindowsSysmon event_id=1 (image="*net.exe" or image="*tasklist.exe" or image="*sc.exe" or image="*wmic.exe") (command="*net.exe* start*" or command="*tasklist.exe* /SVC" command="*sc.exe* query*" or command="*wmic.exe* service where*") -user IN EXCLUDED_USERS
  ```

System Time Discovery

- **Trigger Condition:** LogPoint detects an attempt to discover system time. The information is useful to perform other techniques, like executing a file with a scheduled task or discovering locality information based on time zone to assist in victim targeting.
- **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="*net* time*") or image="*w32tm.exe" or command="*Get-Date*" -user IN EXCLUDED_USERS
  ```

Tap Driver Installation Detected

- **Trigger Condition:** Installation of TAP software. It indicates possible preparation for data exfiltration using tunneling techniques.
- **ATT&CK Category:** Exfiltration
- **ATT&CK Tag:** Exfiltration Over Alternative Protocol
- **ATT&CK ID:** T1048
- **Minimum Log Source Requirement:** Windows
- **Query:**

-
  ```
  ((norm_id=WindowsSysmon event_id=6) OR (norm_id=WinServer (event_id=7045 OR event_id=4697))) (path="*tap0901*" OR file="*tap0901*") -user IN EXCLUDED_USERS
  ```

Taskmgr as Parent Detected

- **Trigger Condition:** Creation of a process from the Windows Task Manager.
- **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 parent_image="*\taskmgr.exe" -image IN ["*\resmon.exe", "*\mmc.exe", "*\taskmgr.exe"] -user IN EXCLUDED_USERS
  ```

Tasks Folder Evasion Detected

- **Trigger Condition:** Evasion of task folder is detected. Task folder in system32 and syswow64 are globally writable paths. Adversaries can take advantage to load or influence script hosts, or any .NET application in task to load and execute a custom assembly into cscript, wscript, regsvr32, mshta, and eventvwr.
- **ATT&CK Category:** Persistence, Privilege Escalation, Defense Evasion
- **ATT&CK Tag:** Hijack Execution Flow, DLL Side-Loading
- **ATT&CK ID:** T1574, T1574.002
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

-
  ```
  norm_id=WinServer event_id=4688 command IN ["*echo *", "*copy *", "*type *", "*file createnew*"] command IN ["* C:\Windows\System32\Tasks\*", "* C:\Windows\SysWow64\Tasks\*"]
  ```

Terminal Service Process Spawn Detected

- **Trigger Condition:** Process spawned by the terminal service server process is detected. It can be used as an indicator for the exploitation of CVE-2019-0708.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Exploitation of Remote Services
- **ATT&CK ID:** T1210

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

```
norm_id=WindowsSysmon event_id=1 parent_command="*\svchost.exe*termsvcs" -image="*\rdpclip.exe" -user IN EXCLUDED_USERS
```

Threat Intel Allowed Connections from Suspicious Sources

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

```
norm_id=* label=Allow label=Connection -source_address in HOMENET destination_address in HOMENET  | process ti(source_address) | rename et_ip_address as SourceAddress, cs_ip_address as SourceAddress, et_category as Category,
cs_category as Category, rf_ip_address as SourceAddress, rf_category as Category,et_score as Score,cs_score as Score,rf_score as Score,destination_port as Port | fields Category,SourceAddress,Score,Port
```

Threat Intel Connections with Suspicious Domains

- **Trigger Condition:** A connection is established with a suspicious domain.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

```
label=Connection (url=* OR domain=*)| process domain(url) as domain | process ti(domain) | rename et_category as Category, cs_category as Category, rf_category as Category,et_score as Score,cs_score as Score,rf_score as Score ,rf_domain as Domain, et_domain as Domain,cs_domain as Domain
```

Threat Intel Excessive Denied Connections Attempt from IOC

- **Trigger Condition:** Multiple denied connections are received from suspicious sources.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

```
norm_id=* label=Connection label=Deny -source_address in HOMENET destination_address in HOMENET | process ti(source_address) | rename rf_ti_category as Cate
```

```
gory, rf_ip_address as SourceAddress, rf_score as Score, destination_port as Port | chart count() as cnt by SourceAddress | search cnt>5
```

Threat Intel Internal Machine Connecting to Multiple IOCs

- **Trigger Condition:** A user establishes connections to unique destination.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

-
  ```
  norm_id=* label=Connection source_address IN HOMENET -destination_address IN HOMENET | process ti(destination_address) | rename rf_ti_category as Category, rf_ip_address as DestinationAddress, rf_score as Score, destination_port as Port | chart distinct_count(DestinationAddress) as DC by source_address | search DC>5
  ```

Threat Intel IOC Connecting to Multiple Internal Machines

- **Trigger Condition:** An inbound connection from suspicious sources to multiple destinations is detected.
- **ATT&CK Category:** Command and Control, Defense Evasion
- **ATT&CK Tag:** Proxy, Exploitation for Defense Evasion
- **ATT&CK ID:** T1090, T1211
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

-
  ```
  norm_id=* label=Connection -source_address in HOMENET destination_address in HOMENET | process ti(source_address) | rename rf_ti_category as Category, rf_ip_address as SourceAddress, rf_score as Score, destination_port as Port | chart distinct_count(destination_address) as DC by source_address | search DC>5
  ```

Time-Stomping of Users Directory Files Detected

- **Trigger Condition:** Time-stomping of user directory file is detected. Sysmon can only detect a change of CreationTime and not LastWriteTime and LastAccessTime. Therefore, we recommend that whitelist legitimate noisy processes like browsers, slack, or teams to reduce false positives.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Indicator Removal on Host, Timestomp
- **ATT&CK ID:** T1070, T1070.006
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=2 path="C:\Users*" -source_image IN ["*iexplore.exe", "*cortana*", "*\StartMenuExperienceHost.exe", "C:\Windows\system32\cleanmgr.exe", "C:\Windows\Explorer.EXE", "*\LocalBridge.exe", "*\svchost.exe",
"*\RuntimeBroker.exe", "*\msedge.exe"]-path="*\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations" -user IN EXCLUDED_USERS
```

Transfering Files with Credential Data via Network Shares

- **Trigger Condition:** Transfer of sensitive files with credential data using a network share.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows
- **Query:**

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

TrendMicroDeepSecurity Virus Quarantined

- **Trigger Condition:** A virus-infected file is quarantined.
- **ATT&CK Category:** Defense Evasion, Discovery
- **ATT&CK Tag:** Obfuscated Files or Information, Indicator Removal from Tools, Network Service Scanning
- **ATT&CK ID:** T1027, T1027.005, T1046
- **Minimum Log Source Requirement:** Trend Micro Deep Security
- **Query:**

```
norm_id=TrendMicroDeepSecurity label=Virus OR label=Malware label=File label=Quarantine
```

UAC Bypass via Event Viewer Detected

- **Trigger Condition:** UAC bypass method using the Windows Event Viewer is detected.
- **ATT&CK Category:** Defense Evasion, Privilege Escalation
- **ATT&CK Tag:** Abuse Elevation Control Mechanism, Bypass User Access Control
- **ATT&CK ID:** T1548, T1548.002
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
(event_id=13 target_object="HKU\*\mscfile\shell\open\command") OR ((event_id=1
parent_image="*\eventvwr.exe") -(image="*\mmc.exe"))
```

Unix Possible Bruteforce Attack

- **Trigger Condition:** An account is not present but is used repeatedly to login. This may be a brute force attack by a bot, malware, or threat agent.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Brute Force
- **ATT&CK ID:** T1110
- **Minimum Log Source Requirement:** Unix
- **Query:**
-
  ```
  norm_id=Unix ((label=Account label=Absent) OR (label=User label=Authentication label=Fail)) user=* | chart count() as cnt by user | search cnt>10
  ```

Unix User Deleted

- **Trigger Condition:** Deletion of a user account.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Account Access Removal
- **ATT&CK ID:** T1531
- **Minimum Log Source Requirement:** Unix
- **Query:**
-
  ```
  norm_id=Unix label=User label=Account label=Management label=Delete label=Remove user=*
  ```

Unsigned Driver Loading Detected

- **Trigger Condition:** Loading of an unsigned driver is detected.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  norm_id=WindowsSysmon event_id=6 is_sign=False image=* -user IN EXCLUDED_USERS
  ```

Possible Ursnif Registry Activity

- **Trigger Condition:** A new registry key under *AppDataLowSoftwareMicrosoft* is detected, which was used by Ursnif malware.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Modify Registry
- **ATT&CK ID:** T1112
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  norm_id=WindowsSysmon event_id=13 target_object="*\Software\AppDataLow\Software\Microsoft\*" -user IN EXCLUDED_USERS
  ```

Valak Malware Connection to Malicious Domains

- **Trigger Condition:** Connection to VALAK malware-related domains are detected.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Firewall, IDS/IPS, Webserver
- **Query:**
-
```
norm_id=* (url=* OR domain=*) | process domain(url) as domain | search domain in VALAK_DOMAINS
```

Valak Malware Infected Host Detected

- **Trigger Condition:** Valak malware infected host is detected.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Firewall, IDS/IPS, Windows Sysmon
- **Query:**
-
```
host=* hash=* hash IN VALAK_HASHES
```

VBA DLL Loaded by Office

- **Trigger Condition:** Loading of DLL related to VBA macros by Office products id detected. To reduce false positives, we recommend you filter the use of the legitimate macro.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** Phishing, Spearphishing Attachment
- **ATT&CK ID:** T1566, T1566.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
```
norm_id=WindowsSysmon event_id=7 source_image IN ["*\winword.exe*", "*\powerpnt.exe*", "*\excel.exe*", "*\outlook.exe*"] image IN ["*\VBE7.DLL*", "*\VBEUI.DLL*", "*\VBE7INTL.DLL*"] -user IN EXCLUDED_USERS
```

VM - High Risk Vulnerability on High Impact Assets

- **Trigger Condition:** High-risk vulnerability is detected in high impact assets.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Network Service Scanning
- **ATT&CK ID:** T1046
- **Minimum Log Source Requirement:** Qualys, Vulnerability Management
- **Query:**
-
```
(col_type=qualys* or col_type=Nessus or norm_id=VulnerabilityManagement) (severity=4 or severity=5) source_address IN HIGH_IMPACT_ASSETS
```

VM - High Risk Vulnerability on Low Impact Assets

- **Trigger Condition:** High-risk vulnerability is detected in low impact assets.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Network Service Scanning
- **ATT&CK ID:** T1046
- **Minimum Log Source Requirement:** Qualys, Vulnerability Management
- **Query:**
- `(col_type=qualys* or col_type=Nessus or norm_id=VulnerabilityManagement) (severity=4 OR severity=5) source_address IN LOW_IMPACT_ASSETS`

VM - High Risk Vulnerability on Medium Impact Assets

- **Trigger Condition:** High-risk vulnerability is detected in medium impact assets.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Network Service Scanning
- **ATT&CK ID:** T1046
- **Minimum Log Source Requirement:** Qualys, Vulnerability Management
- **Query:**
- `(col_type=qualys* or col_type=Nessus or norm_id=VulnerabilityManagement) (severity=4 or severity=5) source_address IN MEDIUM_IMPACT_ASSETS`

VM - Medium Risk Vulnerability on High Impact Assets

- **Trigger Condition:** Medium-risk vulnerability is detected in high impact assets.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Network Service Scanning
- **ATT&CK ID:** T1046
- **Minimum Log Source Requirement:** Qualys, Vulnerability Management
- **Query:**
- `(col_type=qualys* or col_type=Nessus or norm_id=VulnerabilityManagement) (severity=2 or severity=3) source_address IN HIGH_IMPACT_ASSETS`

VM - Medium Risk Vulnerability on Low Impact Assets

- **Trigger Condition:** Medium-risk vulnerability is detected in low impact assets.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Network Service Scanning
- **ATT&CK ID:** T1046
- **Minimum Log Source Requirement:** Qualys, Vulnerability Management
- **Query:**
- `(col_type=qualys* or col_type=Nessus or norm_id=VulnerabilityManagement) (severity=2 OR severity=3) source_address IN LOW_IMPACT_ASSETS`

VM - Medium Risk Vulnerability on Medium Impact Assets

- **Trigger Condition:** Medium-risk vulnerability is detected in medium impact assets.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Network Service Scanning
- **ATT&CK ID:** T1046
- **Minimum Log Source Requirement:** Qualys, Vulnerability Management
- **Query:**
- `(col_type=qualys* or col_type=Nessus or norm_id=VulnerabilityManagement) (severity=2 or severity=3) source_address IN MEDIUM_IMPACT_ASSETS`

WannaCry File Encryption

- **Trigger Condition:** File encryption due to WannaCry ransomeware.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Data Encrypted for Impact
- **ATT&CK ID:** T1486
- **Minimum Log Source Requirement:** Windows
- **Query:**
- `col_type=lpagent new_file IN WANNACRY_EXTENSION`

WannaCry MS17-010 Vulnerable Sources

- **Trigger Condition:** MS17-010 vulnerability is detected.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Qualys, Vulnerability Management
- **Query:**
- `col_type=qualys* qualys_id IN [91345, 91357, 91359, 91360, 70077, 91360, 91345]`

WannaCry Sources in Connections to Sinkhole Domain

- **Trigger Condition:** A source tries to connect to the WannaCry sinkhole domain.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Proxy
- **ATT&CK ID:** T1090
- **Minimum Log Source Requirement:** Firewall, IDS/IPS, Webserver
- **Query:**
- `norm_id=* url IN WANNACRY_DOMAIN or domain IN WANNACRY_DOMAIN`

WastedLocker Ransomware Connection to Malicious Domains

- **Trigger Condition:** A connection to WastedLocker ransomware related domains is detected.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Firewall, IDS/IPS, Webserver
- **Query:**

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

WastedLocker Ransomware Connection to Malicious Sources

- **Trigger Condition:** A host establishes an outbound connection to WastedLocker ransomware sources.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Firewall, IDS/IPS
- **Query:**

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

WastedLocker Ransomware Infected Host Detected

- **Trigger Condition:** WastedLocker 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 WASTEDLOCKER_HASHES
```

WCE wceaux dll Access Detected

- **Trigger Condition:** *wceaux.dll* access during Windows Credential Editor (WCE) pass-the-hash remote command execution on the source host is detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Credential Dumping
- **ATT&CK ID:** T1003
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id IN ["4656", "4658", "4660", "4663"] object_name="*\wceaux.dll" -user IN EXCLUDED_USERS
```

Wdigest Registry Modification

- **Trigger Condition:** Modification of the property value of UseLogonCredential from *HKLM:/SYSTEM /CurrentControlSet/Control/Security Providers/WDigest* to enable clear-text credentials is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Modify Registry
- **ATT&CK ID:** T1112
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=13 target_object="*WDigest\UseLogonCredential" -user IN EXCLUDED_USERS
```

Weak Encryption Enabled for User

- **Trigger Condition:** Weak encryption is enabled for a user profile, which is later used for hash or password cracking.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Modify Registry
- **ATT&CK ID:** T1112
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WinServer event_id=4738 user_account_control IN ["*DES*", "*Preauth*", "*Encrypted*"] user_account_control="*Enabled*" -user IN EXCLUDED_USERS
```

Webshell Detection With Command Line Keywords

- **Trigger Condition:** Command line parameters used during reconnaissance activity via WebShell are detected.
- **ATT&CK Category:** Privilege Escalation, 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 parent_image IN ["*\apache*", "*\tomcat*", "*\w3wp.exe", "*\php-cgi.exe", "*\nginx.exe", "*\httpd.exe"] command IN ["*whoami*", "*net user *", "*ping -n *", "*systeminfo",
"*&cd&echo*", "*cd /d*"] -user IN EXCLUDED_USERS
```

Windows 10 Scheduled Task SandboxEscaper 0 day Detected

- **Trigger Condition:** Modification of potential malicious property value of UseLogonCredential from`HKLM:SYSTEMCurrentControlSetControlSecurityProvidersWDigest` to enable storing of clear-text credentials in memory.

- **ATT&CK Category:** Privilege Escalation, Execution
- **ATT&CK Tag:** Scheduled Task/Job, Scheduled Task
- **ATT&CK ID:** T1053, T1053.005
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
```
norm_id=WindowsSysmon event_id=1 image="schtasks.exe" command="*/change*/TN*/R
U*/RP*" -user IN EXCLUDED_USERS
```

Windows Admin Shares - Process

- **Trigger Condition:** The use of hidden network shares (like CandIPC and IPC) are accessible only to administrators. Adversaries use this technique in conjunction with administrator-level accounts to remotely access a networked system over SMB, interact with systems using RPC calls, or transfer files.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Remote Services, SMB/Windows Admin Share
- **ATT&CK ID:** T1021, T1021.002
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
```
norm_id=WindowsSysmon event_id=1 (image="*net.exe" or image="*powershell.exe")
((command="*net* use*∗" orcommand=" *net * session*"  or command="*net* file*$*
") or command="*New-PSDrive*root*") -user IN EXCLUDED_USERS
```

Windows Audit Logs Cleared

- **Trigger Condition:** Security events 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* label=Audit label=Log label=Clear -user IN EXCLUDED_USERS
```

Windows Credential Editor Detected

- **Trigger Condition:** The use of Windows Credential Editor (WCE) 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 (hash IN ["a53a02b997935fd8eedcb5f7abab9b9f"
, "e96a73c7bf33a464c510ede582318bf2"] OR command="*.exe -S" parent_image="*\se
rvices.exe")) OR (norm_id=WindowsSysmon event_id=13 target_object="*Services\WCESERVICE\Start*") -user IN EXCLUDED_USERS
```

Windows Data Copied to Removable Device

- **Trigger Condition:** A file is copied to removable storage. For this alert to work, you must update the list CRITICAL_HOSTS, which includes hosts where admin monitors file copy across removable storage.
- **ATT&CK Category:** Exfiltration
- **ATT&CK Tag:** Exfiltration Over Physical Medium, Exfiltration over USB
- **ATT&CK ID:** T1052, T1052.001
- **Minimum Log Source Requirement:** Windows
- **Query:**

-
  ```
  norm_id=WinServer* event_id=4663 event_category="Removable Storage" access="WriteData*" or access="*AppendData*" host IN CRITICAL_HOSTS -user IN EXCLUDED_USERS
  ```

Windows Defender Exclusion Set Detected

- **Trigger Condition:** When Windows Defender Antivirus exclusion is added. Windows Defender Antivirus is a built-in antivirus program for Windows 10. It provides real-time protection against malware, viruses, spyware and other malicious software. Windows Defender allows users to exclude specific files, folders or processes from scanning to improve performance and reduce false positives. Adversaries can abuse the file exclusion feature in Windows Defender to evade detection of their malicious binaries by excluding the file type or file from being scanned.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Impair Defenses, Disable or Modify Tools
- **ATT&CK ID:** T1562, T1562.001
- **Minimum Log Source Requirement:** Windows
- **Query:**

-
  ```
  (norm_id=WinServer event_source="Microsoft-Windows-Windows Defender" event_id=5007 new_value="HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\*") OR (norm_id=WindowsSysmon event_id=13 target_object="*\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Extensions\*" event_type=setvalue)
  ```

Windows Domain Policy Change

- **Trigger Condition:** The domain policy is changed on a Domain Controller.
- **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:**

```
norm_id=WinServer* label=Domain label=Policy label=Change user=*$ -user IN EXCLUDED_USERS| rename target_domain as domain
```

Windows Excessive Amount of Files Copied to Removable Device

- **Trigger Condition:** A user copies more than 100 files in the removable storage.
- **ATT&CK Category:** Exfiltration
- **ATT&CK Tag:** Exfiltration Over Physical Medium, Exfiltration over USB
- **ATT&CK ID:** T1052, T1052.001
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer* event_id=4663 event_category="Removable Storage" access="WriteData*" or access="*AppendData*" -user IN EXCLUDED_USERS | chart distinct_count(object) as DataCopied by user | search DataCopied>100
```

Windows Failed Login Attempt Using Service Account

- **Trigger Condition:** A user fails to log in using a service account. Generally, failed logon events with logon type 5 indicate the password change without updating the service; however, a possibility of malicious users at work exists. Conversely, the existence of malicious users is less likely to happen as creating a new service or editing an existing service by default requires membership in Administrators or Server Operators. Also, malicious users will already have the authority to perpetuate their desired goal.
- **ATT&CK Category:** Defense Evasion, Persistence, Privilege Escalation, Initial Access
- **ATT&CK Tag:** Valid Accounts
- **ATT&CK ID:** T1078
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer* label=User label=Login label=Fail target_user=*ORuser=∗logon_type = 5 -user IN EXCLUDED_USERS | rename target_user as user, target_domain as domain
```

Windows Failed Login Followed by Lockout Event

- **Trigger Condition:** A failed login attempt followed by account lockout is detected.
- **ATT&CK Category:** Defense Evasion, Persistence, Privilege Escalation, Initial Access
- **ATT&CK Tag:** Valid Accounts, Exploitation for Credential Access, Exploitation for Privilege Escalation, Exploitation for Defense Evasion, Brute Force
- **ATT&CK ID:** T1078, T1212, T1068, T1211 ,T1110
- **Minimum Log Source Requirement:** Windows
- **Query:**

-
  ```
  [norm_id=WinServer label=User label=Login label=Fail -user IN EXCLUDED_USERS] as s1 followed by [norm_id=WinServer label=User label=Account label=Lock user=*] as s2 on s1.user=s2.user | rename s1.user as User, s1.source_address as SourceAddress, s2.workstation as ComputerName, s2.caller_domain as Domain, s1.log_ts as LastFailedLogin_ts, s2.log_ts as LockedOut_ts
  ```

Windows Local User Management

- **Trigger Condition:** A user is created on a non-domain controller. For the alert to work, you must update the list DOMAIN with domain controllers.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Create Account, Local Account
- **ATT&CK ID:** T1136, T1136.001
- **Minimum Log Source Requirement:** Windows
- **Query:**

-
  ```
  norm_id=WinServer* label=User label=Create -target_user=*-user=* -target_domain IN DOMAIN -domain IN DOMAIN -user IN EXCLUDED_USERS
  ```

WMI DLL Loaded by Office

- **Trigger Condition:** Loading of DLLs related to WMI by Office products signaling VBA macros executing WMI Commands.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** User Execution, Malicious File
- **ATT&CK ID:** T1204, T1204.002
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

-
  ```
  norm_id=WindowsSysmon event_id=7 source_image IN ["*\winword.exe", "*\powerpnt.exe", "*\excel.exe", "*\outlook.exe"] image IN ["*\wmiutils.dll", "*\wbemcomn.dll", "*\wbemprox.dll", "*\wbemdisp.dll", "*\wbemsvc.dll"]
  ```

-
  ```
  -user IN EXCLUDED_USERS
  ```

Windows Multiple Password Changed by User

- **Trigger Condition:** A user changes its own password more than once in a given period of time.
- **ATT&CK Category:** Persistence, Credential Access, Privilege Escalation, Defense Evasion
- **ATT&CK Tag:** Account Manipulation, Abuse Elevation Control Mechanism, Bypass User Access Control, Exploitation for Credential Access, Exploitation for Privilege Escalation
- **ATT&CK ID:** T1098, T1548, T1212, T1068
- **Minimum Log Source Requirement:** Windows
- **Query:**

-
  ```
  norm_id=WinServer* label=User label=Password label=Change -target_user=*-calleruser=*-calleruser=* -user IN EXCLUDED_USERS | rename caller_user as user | process compare(target_user, user) as match | search match=True | chart count()
  ```

```
as Event by target_user | search Event>1
```

Windows Processes Suspicious Parent Directory Detected

- **Trigger Condition:** Suspicious parent processes of Windows processes are 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 image IN ["*\svchost.exe", "*\taskhost.exe", "*\lsm.exe", "*\lsass.exe", "*\services.exe", "*\lsaiso.exe", "*\csrss.exe", "*\wininit.exe", "*\winlogon.exe"] -parent_image IN ["*\System32\*", "*\SysWOW64\*", "*\SavService.exe", "*\Windows Defender\*\MsMpEng.exe"] parent_image=* -user IN EXCLUDED_USERS
```

Windows Registry Persistence COM Key Linking Detected

- **Trigger Condition:** COM object hijacking via TreatAs subkey is detected. It is rare, but there are some cases where system utilities use linking keys for backward compatibility.
- **ATT&CK Category:** Privilege Escalation, Persistence
- **ATT&CK Tag:** Event Triggered Execution, Component Object Model Hijacking
- **ATT&CK ID:** T1546, T1546.015
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=12 target_object="HKU\*_Classes\CLSID\*\TreatAs" -user IN EXCLUDED_USERS
```

Windows Shell Spawning Suspicious Program

- **Trigger Condition:** A suspicious child process of Windows Shell is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter
- **ATT&CK ID:** T1059
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 parent_image IN ["*\mshta.exe", "*\powershell.exe", "*\rundll32.exe", "*\cscript.exe", "*\wscript.exe", "*\wmiprvse.exe"] image IN ["*\schtasks.exe", "*\nslookup.exe", "*\certutil.exe", "*\bitsadmin.exe", "*\mshta.exe"]
-path="*\ccmcache\*" -user IN EXCLUDED_USERS
```

Windows SMB Remote Code Execution Vulnerability CVE-2017-0143 Detected

- **Trigger Condition:** Remote code execution in Windows SMB (CVE-2017-0143) is detected.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Remote Services
- **ATT&CK ID:** T1021
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon label=Detect label=Network label=Connection destination_port=445 rule=SMB source_address IN MOST_EXPLOITABLE_IPS -user IN EXCLUDED_USERS
```

Windows Suspicious Creation of User Accounts

- **Trigger Condition:** Creation of an account, followed by its deletion in a day is detected.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Account Create
- **ATT&CK ID:** T1136
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
[norm_id=WinServer* label=User label=Create -target_user=*–calleruser=∗–calleruser=∗ -user=*$ -user IN EXCLUDED_USERS | rename target_user as Account, caller_user as user] as s1 followed by [norm_id=WinServer* label=User (label=Delete or label=Remove) | rename target_user as Account, caller_user as user]
as s2 on s1.Account=s2.Account| rename s1.col_ts as CreatedTime_ts, s2.col_ts as DeletedTime_ts, s1.user as CreatedUser, s2.user as DeletedUser, s1.Account as Account
```

Windows User Account Created via Command Line

- **Trigger Condition:** Creation of a user account via CLI like PowerShell or net utility is detected.
- **ATT&CK Category:** Execution, Persistence
- **ATT&CK Tag:** Create Account, PowerShell, Local Account
- **ATT&CK ID:** T1136, T1059.001, T1136.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label="create" (command="*New-LocalUser*" or command="*net user add*")
```

Windows Unusual User Access to an Object

- **Trigger Condition:** A file or object is accessed by a user more than ten times in a given time.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** File and Directory Discovery, Data from Network Shared Drive, Network Share Discovery
- **ATT&CK ID:** T1083, T1039, T1135
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer* label=Access label=Object access="*Read*Control*" path=* -user=*$ -user IN EXCLUDED_USERS | chart distinct_count(object) as FileAccessed by user, path order by FileAccessed desc | search FileAccessed>10
```

Windows User Account Change to End with Dollar Sign

- **Trigger Condition:** A user account is changed to end with the dollar sign ($).
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Account Manipulation
- **ATT&CK ID:** T1098
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer* label=User label=Account label=Change label=Name new_user=*$ -user IN EXCLUDED_USERS | rename caller_user as user, caller_domain as domain
```

Windows Webshell Creation Detected

- **Trigger Condition:** Creation of WebShell file on a static web site. The alert has been directly translated from sigma rule.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Server Software Component, Web Shell
- **ATT&CK ID:** T1505, T1505.003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=11 ((path="*\inetpub\wwwroot*" file IN ["*.asp", "*.ashx", "*.ph"]) OR (path IN ["*\www\*", "*\htdocs\*", "*\html\*"] file="*.ph") OR (file="*.jsp" path="*\cgi-bin\*" path="*.pl*"))
-path IN ["*\AppData\Local\Temp*", "*\Windows\Temp*"]
```

Winlogon Helper DLL

- **Trigger Condition:** Modification of registry entries related to winlogon.exe to load and execute possible malicious DLLs and/or executables is detected.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** Boot or Logon Autostart Execution, Winlogon Helper DLL
- **ATT&CK ID:** T1547, T1547.004
- **Minimum Log Source Requirement:** Windows Sysmon

- **Query:**

```
norm_id=WindowsSysmon (event_id=12 or event_id=13 or event_id=14) (target_object="*\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\user_nameinit\*" or target_object="*\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell\*" or target_object="*\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\*")
-user IN EXCLUDED_USERS
```

WMI - Network Connection

- **Trigger Condition:** A network connection from wmic.exe is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Windows Management Instrumentation
- **ATT&CK ID:** T1047
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

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

WMI Backdoor Exchange Transport Agent

- **Trigger Condition:** WMI backdoor in Exchange Server Software Component and Transport Agents via WMi event filters is detected.
- **ATT&CK Category:** Privilege Escalation, Persistence
- **ATT&CK Tag:** Event Triggered Execution, Windows Management Instrumentation Event Subscription
- **ATT&CK ID:** T1546, T1546.003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 parent_image="*\EdgeTransport.exe" -user IN EXCLUDED_USERS
```

WMI Modules Loaded by Suspicious Process

- **Trigger Condition:** Loading of WMI modules by suspicious processes like a binary from ProgramData is detected. Legitimate system processes and third-party utilities extensively use WMI. We recommend you whitelist to reduce false-positive flooding. Also, do not monitor _C:Windows*_ as extensive whitelisting is required, which may hamper query's performance.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Windows Management Instrumentation
- **ATT&CK ID:** T1047
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=7 image IN ["*wmiclnt.dll", "*WmiApRpl.dll", "*wmiprov.dll", "*wmiutils.dll", "*wbemcomn.dll", "*wbemprox.dll", "*WMINet_Utils.dll", "*wbemsvc.dll", "*fastprox.dll"] source_image IN ["C:\Users\*", "C:\Pr
ogramData*", "C:\Windows\Temp*"] -source_image IN ["*\Microsoft\Teams\Update.exe", "*\MsMpEng.exe"]
```

WMI Persistence - Script Event Consumer Detected

- **Trigger Condition:** Windows Management Instrumentation (WMI) script event consumers are detected. Attackers leverage WMI ActiveScriptEventConsumers remotely to move laterally in the network.
- **ATT&CK Category:** Privilege Escalation, Persistence
- **ATT&CK Tag:** Event Triggered Execution, Windows Management Instrumentation Event Subscription
- **ATT&CK ID:** T1546, T1546.003
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*:\WINDOWS\system32\wbem\scrcons.exe" parent_process="*:\Windows\System32\svchost.exe" -user IN EXCLUDED_USERS
```

WMI Persistence - Script Event Consumer File Write

- **Trigger Condition:** File writes of WMI script event consumer are detected.
- **ATT&CK Category:** Privilege Escalation
- **ATT&CK Tag:** Event Triggered Execution, Windows Management Instrumentation Event Subscription
- **ATT&CK ID:** T1546, T1546.003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=11 source_image="C:\WINDOWS\system32\wbem\scrcons.exe" -user IN EXCLUDED_USERS
```

WMI Process Execution

- **Trigger Condition:** Execution of processes related to WMI is detected. You must whitelist installed security tools or software that uses WMI to reduce false positives.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Windows Management Instrumentation
- **ATT&CK ID:** T1047
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 (parent_command="*wmiprvse.exe" or image="*wmic.exe" or command="*wmic*") -user IN EXCLUDED_USERS
```

WMI Spawning Windows Shell

- **Trigger Condition:** WMI spawning Command and Scripting Interpreter and PowerShell are detected.

- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, PowerShell, Windows Management Instrumentation
- **ATT&CK ID:** T1059, T1059.001, T1047
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  norm_id=WindowsSysmon event_id=1 parent_image="*\wmiprvse.exe" image="*\powershell.exe" -user IN EXCLUDED_USERS
  ```

WMIExec VBS Script Detected

- **Trigger Condition:** Execution of a VBS script by *wscript* and *cscript*.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, Visual Basic
- **ATT&CK ID:** T1059, T1059.005
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  norm_id=WindowsSysmon event_id=1 image IN ["*\cscript.exe", "*\wscript.exe"] command="*.vbs /shell *" -user IN EXCLUDED_USERS
  ```

Wmiprvse Spawning Process

- **Trigger Condition:** *wmiprvse* spawning unusual processes are detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Windows Management Instrumentation
- **ATT&CK ID:** T1047
- **Minimum Log Source Requirement:** Windows
- **Query:**
-
  ```
  norm_id=WinServer event_id=4688 parent_process="*WmiPrvSe.exe" -target_logon_id="0x3e7" -logon_id="0x3e7" -"process" IN ["*\WmiPrvse.exe", "*\Werfault.exe"] -user IN EXCLUDED_USERS
  ```

WScript or CScript Dropper Detected

- **Trigger Condition:** Execution of *wscript* or *cscript* scripts in user directories is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, Visual Basic, JavaScript
- **ATT&CK ID:** T1059.007, T1059.005, T1059
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**
-
  ```
  label="Process" label=Create "process" IN ["*\wscript.exe", "*\cscript.exe"] command IN ["*:\Users\*", "*:\ProgramData\*"] command IN ["*.jse", "*.vbe", "*.js", "*.vba", "*.vbs"] -parent_process = "*\winzip*"
  ```

Wsreset UAC Bypass Detected

- **Trigger Condition:** A method that uses the Wsreset.exe tool used to reset the Windows Store bypassing UAC is detected.
- **ATT&CK Category:** Privilege Escalation, Defense Evasion
- **ATT&CK Tag:** Abuse Elevation Control Mechanism, Bypass User Access Control
- **ATT&CK ID:** T1548, T1548.002
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

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

XSL Script Processing Detected

- **Trigger Condition:** Application control bypass attempt via execution of embedded scripts inside Extensible Stylesheet Language (XSL) files is detected. The alert detects another variation of this technique, dubbed *Squiblytwo*, that utilizes WMI to invoke JScript or VBScript within an XSL file. Legitimate invocations of *msxsl* employ the *-o* command-line argument should be whitelisted to reduce false positives.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** XSL Script Processing
- **ATT&CK ID:** T1220
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

-
  ```
  label="Process" label=Create  ((("process"="*\wmic.exe" command IN ["* format*:*", "*/format*:*", "*-format*:*"]  ) -command in ["*Format:List", "*Format:htable", "*Format:hform", "*Format:table", "*Format:mof", "*Format:value", "*Format:rawxml", "*Format:xml", "*Format:csv"] ) OR ("process"="*\msxsl.exe" -command="* -o *")) -user IN EXCLUDED_USERS
  ```

ZOHO Dctask64 Process Injection Detected

- **Trigger Condition:** Process injection using ZOHO’s dctask64.exe 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 image="*\dctask64.exe" -command="*DesktopCentral_Agent\agent*" -user IN EXCLUDED_USERS
  ```

ZxShell Malware Detected

- **Trigger Condition:** Proxy execution of ZxShell 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 image="*\rundll32.exe" command IN ["*zxFunction*", "*RemoteDiskXXXXX*"] -user IN EXCLUDED_USERS
  ```

APT 34 Initial Access Using Spearphishing Link Detected

- **Trigger Condition:** Entry vectors try to gain their initial foothold within a network using Spearphishing link with IOCs' attacks related to APT34. For the alert to work, it uses lists; IRANIAN_SPEARPHISHING_DOMAINS and IRANIAN_SPEARPHISHING_IP.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** Spearphishing Link
- **ATT&CK ID:** T1566
- **Minimum Log Source Requirement:** EmailServer
- **Query:**
-
  ```
  norm_id=* label=Detect label=Malicious label=URL (source_address in IRANIAN_SPEARPHISHING_IP OR domain in IRANIAN_SPEARPHISHING_DOMAINS) -user IN EXCLUDED_USERS
  ```

Automated Collection Detected

- **Trigger Condition:** An adversary uses automated techniques like scripting for collecting internal data.
- **ATT&CK Category:** Collection
- **ATT&CK Tag:** Automated Collection
- **ATT&CK ID:** T1119
- **Minimum Log Source Requirement:** Windows
- **Query:**
-
  ```
  norm_id=WinServer (event_id=4104 ( scriptblocktext="*Get-ChildItem -Recurse*Copy-Item*" OR scriptblocktext="*Get-ChildItem*" OR scriptblocktext="*Get-Process*" OR scriptblocktext="*Get-Service*" OR scriptblocktext="*cmd.exe dir*findstr /e*" OR scriptblocktext="*wmic process list*" OR script_block="*Get-ChildItem -Recurse*Copy-Item*" OR script_block="*Get-ChildItem*" OR script_block="*Get-Process*" OR script_block="*Get-Service*" OR script_block="*cmd.exe dir*findstr /e*" OR script_block="*wmic process list*")) -user IN EXCLUDED_USERS | rename scriptblocktext as command | rename script_block as command
  ```

Screenshot Capture Detected

- **Trigger Condition:** An adversary captures the screen of the desktop to gather information throughout an operation.
- **ATT&CK Category:** Collection
- **ATT&CK Tag:** Automated Collection
- **ATT&CK ID:** T1113
- **Minimum Log Source Requirement:** Windows

- **Query:**

```
norm_id=WinServer (event_id=4104 (scriptblocktext="*Get-ScreenShot.ps1*" OR script_block="*Get-ScreenShot.ps1*")) -user IN EXCLUDED_USERS | rename scriptblocktext as command | rename script_block as command
```

APT 34 Command and Control Using Commonly used Ports Detected

- **Trigger Condition:** An adversary communicates over a commonly used port to bypass firewalls or network detection systems and blend with regular network activity to avoid detailed inspection. The alert uses lists IRANIAN_CNC_IP, IRANIAN_CNC_DOMAIN, and COMMON_PORTS.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** ProxyServer
- **Query:**

```
norm_id=*Proxy* source_address=* destination_address=* destination_port IN COMMON_PORTS destination_address in IRANIAN_CNC_IP destination_host in IRANIAN_CNC_DOMAIN -user IN EXCLUDED_USERS
```

APT 34 Command and Control Using Standard Application Layer Protocol Detected

- **Trigger Condition:** An adversary communicates using a common, standardized Application Layer protocol such as HTTP, HTTPS, SMTP, or DNS to avoid detection by blending in with existing traffic. The alert uses lists STANDARD_APPLICATION_PORTS, RANIAN_CNC_DOMAIN, and IRANIAN_CNC_IP.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Application Layer Protocol
- **ATT&CK ID:** T1071
- **Minimum Log Source Requirement:** ProxyServer
- **Query:**

```
norm_id=*proxy source_address=* destination_address=* destination_port IN STANDARD_APPLICATION_PORTS destination_address in IRANIAN_CNC_IP destination_host in IRANIAN_CNC_DOMAIN -user IN EXCLUDED_USERS
```

APT 34 Command and Control Using Uncommonly used Port Detected

- **Trigger Condition:** An adversary conducts Command and Control communications over a non-standard port to bypass proxy and firewalls that are misconfigured. The alert uses lists IRANIAN_CNC_IP, IRANIAN_CNC_DOMAIN, and UNCOMMON_PORTS.

- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Non-Standard Port
- **ATT&CK ID:** T1571
- **Minimum Log Source Requirement:** ProxyServer
- **Query:**

```
norm_id=*Proxy* source_address=* destination_address=* destination_port IN UNCOMMON_PORTS destination_address in IRANIAN_CNC_IP destination_host in IRANIAN_CNC_DOMAIN -user IN EXCLUDED_USERS
```

Credential Dumping using procdump Detected

- **Trigger Condition:** An adversary obtains account login and password information using procdump, generally in the form of a hash or a clear text password, from the operating system 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 label=File label=Create file=*.dmp source_image="*procdump.exe" -user IN EXCLUDED_USERS | rename source_image as image
```

Access Using Browser Stored Credential Detected

- **Trigger Condition:** Adversary acquires credentials from web browsers by reading files specific to the target browser and using password stores, credentials from web browsers. The alert is triggered when process *wsus* is detected on path of 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
```

GUI Input Capture Detected

- **Trigger Condition:** Credential access using input capture technique is detected. Adversaries use this technique to obtain valid account credentials on the target system and other sensitive user information that may assist in the attack campaign.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** GUI Input Capture

- **ATT&CK ID:** T1056.002
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon label=Set label=Registry "process"="*keylogger_directx.exe" -user IN EXCLUDED_USERS
```

Files and Directory Discovery Process Detected

- **Trigger Condition:** An adversary enumerates files and directories, or searches in a specific host or network share locations for particular information within a file system.
- **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 -command="*findstr*" (command="*cmd.exe*dir *" OR command="*tree.com*" ) -user IN EXCLUDED_USERS | rename commandline as command
```

Account Discovery Process 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:** Discovery
- **ATT&CK Tag:** Account Discovery, Domain Account
- **ATT&CK ID:** T1087, T1087.002
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer label="Process" label=Create command="*dsquery user*" user IN EXCLUDED_USERS
```

Suspicious File Deletion Detected

- **Trigger Condition:** Adversaries remove trail files for an intrusion to keep their footprint low or remove them at the end as part of the post-intrusion cleanup process. For the alert to work, you must configure ACLs on paths and extensions you want to monitor for deletion operations.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Indicator Removal on Host, File Deletion
- **ATT&CK ID:** T1070, T1070.004
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer label=Object label=Access access="*delete*" (relative_target="*.exe" OR relative_target="*.bat" OR relative_target="*.ps1" OR relative_target="*.cmd") -user IN EXCLUDED_USERS | rename relative_target as file
```

File or Information Decode Process Detected

- **Trigger Condition:** An adversary implements Obfuscated Files or Information to hide artifacts of an intrusion from analysis and employ spcific decoding to use them.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Decode Files or Information
- **ATT&CK ID:** T1140
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer label="Process" label=Create (commandline="*certutil.exe*-encode*calc.exe*T1140_calc.txt" OR commandline="*certutil.exe*-decode*T1140_calc.txt*T1140_calc_decoded.exe" OR command="*certutil.exe*-encode*calc.exe*T1140_calc.txt" OR command="*certutil.exe*-decode*T1140_calc.txt*T1140_calc_decoded.exe")
-user IN EXCLUDED_USERS | rename commandline as command
```

Access of Password Policy Detected

- **Trigger Condition:** The use of command *net** accounts is detected. Adversary accesses detailed information about the password policy used within an enterprise network.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Password Policy Discovery
- **ATT&CK ID:** T1021
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
((norm_id=WinServer label="Process" label=Create) OR (norm_id=WindowsSysmon event_id=11 ) command="*net*accounts*") -user IN EXCLUDED_USERS
```

Access of Permission Groups Detected

- **Trigger Condition:** The use of commands net and get is detected. Adversary finds a local system or domain-level groups and permissions settings using these commands.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Permission Group Discovery, Local Groups, Domain Groups
- **ATT&CK ID:** T1069, T1069.001, T1069.002
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
((norm_id=WinServer label="Process" label=Create) OR (norm_id=WindowsSysmon event_id=1 image="*net.exe")) (command="*net*user*" OR command="*net*group*" OR c
ommand="*get*group*" OR command="*get*ADPrinicipalGroupMembership*") -user IN EXCLUDED_USERS
```

Security Software Discovery Process Detected

- **Trigger Condition:** Adversary attempts to get a listing of security software, configurations, defensive tools, and sensors that are installed on the system.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Security Software Discovery
- **ATT&CK ID:** T1518
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer label="Process" label=Create (command="*findstr.exe*virus" OR command="*findstr.exe*cylance" OR command="*findstr.exe*defender" OR command="*findstr.exe*cb" ) -user IN EXCLUDED_USERS
```

System Network Configuration Discovery

- **Trigger Condition:** Discovery of network configuration via system utilities like ipconfig, route, or netsh is detected.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** System Network Configuration Discovery
- **ATT&CK ID:** T1016
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer label="Process" label=Create (command="*ipconfig.exe*" OR command="*route.exe*" OR command="*netsh advfirewall*" OR command="*arp.exe*" OR command="*nbtstat.exe*" OR command="*netsh.exe*interface show" OR command="*net*config" ) -user IN EXCLUDED_USERS | rename commandline as command
```

System Network Connections Discovery

- **Trigger Condition:** Discovery of network connections via system utilities like netstat or net is detected.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** System Network Connections Discovery
- **ATT&CK ID:** T1049
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create ("process" IN ["*net.exe","*netstat.exe"] command IN ["*net* use*","*net* sessions*","*net* file*","*netstat*"]) OR command="*Get-NetTCPConnection*" -user IN EXCLUDED_USERS
```

Exfiltration over Cloud Application Detected

- **Trigger Condition:** Adversary performs data exfiltration with a different protocol from the main Command and Control protocol or channel.
- **ATT&CK Category:** Exfiltration
- **ATT&CK Tag:** Exfiltration Over Alternative Protocol
- **ATT&CK ID:** T1048
- **Minimum Log Source Requirement:** ProxyServer
- **Query:**
-
```
norm_id=*Proxy* source_address=* destination_address=* destination_address IN CLOUD_APPLICATION_IP -user IN EXCLUDED_USERS
```

Remote File Copy Detected

- **Trigger Condition:** Files are copied from one system to another to stage adversary tools or other files throughout an operation.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Remote File Copy
- **ATT&CK ID:** T1105
- **Minimum Log Source Requirement:** Windows
- **Query:**
-
```
norm_id=WinServer label=Object label=Access access=* (relative_target="*.exe" OR relative_target="*.bat") -user IN EXCLUDED_USERS | rename relative_target as file
```

Account Created for Persistence Detected

- **Trigger Condition:** The use of net commands is detected. An adversary with a sufficient level of access may create a local system, domain, or cloud tenant account, use for persistence employing this command.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Create Account
- **ATT&CK ID:** T1136
- **Minimum Log Source Requirement:** Windows
- **Query:**
-
```
((norm_id=WinServer label="Process" label=Create) OR (norm_id=WindowsSysmon image="*net.exe*")) command="*net*/add*" -user IN EXCLUDED_USERS
```

Account Manipulated for Persistence Detected

- **Trigger Condition:** The use of net commands is detected. Adversary performs actions for modifying permissions, credentials, adding or changing permission groups, modifying account settings, or authentication settings using this command.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Account Manipulation
- **ATT&CK ID:** T1098
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
((norm_id=WinServer label="Process" label=Create) OR (norm_id=WindowsSysmon image="*net.exe*")) command="*net*localgroup*/add" -user IN EXCLUDED_USERS
```

Privilege Escalation - Bypassing User Account Control Detected

- **Trigger Condition:** Adversary uses techniques to elevate a user's privileges manipulating UAC to administer if the target process is unprotected.
- **ATT&CK Category:** Privilege Escalation
- **ATT&CK Tag:** Bypass User Account Control
- **ATT&CK ID:** T1548
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
(norm_id=WindowsSysmon OR ((command=* OR commandline=*) norm_id=WinServer)) label="Process" label=Create (command="*eventvwr.exe*" OR commandline="*eventvwr.exe*" OR command="*wscript.exe*" OR commandline="*wscript.exe*" OR token_elevation_type="TokenElevationTypeLimited*")
-user IN EXCLUDED_USERS | rename commandline as command
```

Executable Dropped in Suspicious Location

- **Trigger Condition:** When the dropping of an executable file is in a suspicious location on a system. Suspicious locations may include directories not commonly used to store executables, such as temporary folders or user profiles, or locations that users do not typically access. Adversaries may use this technique to drop and execute malicious payloads or scripts on a system. They may attempt to place these files in locations that are not easily visible or accessible to users to evade detection. False Positive notice: It is essential to whitelist noisy system processes like Microsoft Defender, Visual Studio, etc, to reduce false positives.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

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

Process Execution from Suspicious Location

- **Trigger Condition:** Execution of a process from suspicious location is detected.
- **ATT&CK Category:** -

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

-
  ```
  norm_id=WinServer event_id=4688 "process" IN ["C:\ProgramData\*.exe", "*\AppData\Local\*.exe", "*\AppData\Roaming\*.exe", "C:\Users\Public\*"] -"process" IN ["*\Teams.exe", "*\Teams\Update.exe", "*\Temp\*\dismhost.exe", "*Microsoft\OneDrive\*\FileCoAuth.exe", "C:\ProgramData\Microsoft\*\MpCmdRun.exe", "*\Local\Temp\*\BackgroundDownload.exe", "*Microsoft\Windows Defender\*\NisSrv.exe", "C:\ProgramData\Microsoft\*\MsMpEng.exe"]
  ```

Active Directory Enumeration via ADFind

- **Trigger Condition:** When enumeration of Active Directory using the ADfind tool is detected. AdFind is a CLI-based utility that can be used for gathering information from Active Directory like organizational units, users, computers, and groups. Adversaries can use this utility to gather information related to the Active Directory.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** T1059 - Command and Scripting Interpreter, T1059.001 - PowerShell
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

-
  ```
  label="Process" label=Create "process"="*.exe" command IN ["* -f *objectcategory=*", "* -sc trustdmp*", "*lockoutduration*", "*lockoutthreshold", "*lockoutobservationwindow*", "*maxpwdage*", "*minpwdage*", "*minpwdlength*", "*pwdhistorylength*", "*pwdproperties*", "*-sc admincountdmp*", "*-sc exchaddresses*"]
  ```

Antivirus Software Discovery via WMI

- **Trigger Condition:** Antivirus software discovery activity via WMI is detected.
- **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 event_id=4688 "process"="*\wmic.exe" command="*SecurityCenter2*AntiVirusProduct*"
  ```

Possible Command Prompt Process Hollowing

- **Trigger Condition:** Possible process hollowing of the command prompt is detected using applications like net.exe, nltest.exe or ipfconfig. Adversaries inject malicious code into suspended and hollowed processes to evade process-based defenses.
- **ATT&CK Category:** Defense Evasion, Privilege Escalation
- **ATT&CK Tag:** Process Injection, Process Hollowing

- **ATT&CK ID:** T1055, T1055.012
- **Minimum Log Source Requirement:** Windows
- **Query:**

-
  ```
  norm_id=WindowsSysmon event_id=1 parent_image="*\cmd.exe" image IN ["*\net.exe", "*\net1.exe", "*\nltest.exe", "*\ipconfig.exe"] -parent_command IN ["* /c *", "* /k *"]
  ```

Suspicious Taskkill Activity

- **Trigger Condition:** More than two processes are terminated quickly via taskkill command that may signal malicious activity like ransomware.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Service Stop
- **ATT&CK ID:** T1489
- **Minimum Log Source Requirement:** Windows
- **Query:**

-
  ```
  norm_id=WinServer event_id=4688 "process"="*\taskkill.exe"| chart count() as cnt by host, "process" | search cnt > 2
  ```

Suspicious File or Directory Permission Modification

- **Trigger Condition:** Permission modification of suspicious file or directory is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** File and Directory Permissions Modification, Windows File and Directory Permissions Modification
- **ATT&CK ID:** T1222.001
- **Minimum Log Source Requirement:** Windows
- **Query:**

-
  ```
  norm_id=WinServer event_id=4688 "process"="*\icacls.exe" command="icacls*:*/grant everyone*"
  ```

Ryuk Wake-On-LAN Activity

- **Trigger Condition:** Ryuks Wake-On-LAN activity is detected.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Windows
- **Query:**

-
  ```
  norm_id=WinServer event_id=4688 "process"="*.exe" command="* 8 LAN *"
  ```

EXE or DLL Dropped in Perflogs Folder

- **Trigger Condition:** The EXE or DLL file is dropped in Windows's Perflog directory.

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

```
norm_id=WindowsSysmon event_id=11 file IN ["*.dll", "*.exe"] path="C:\Perflogs*"
```

Credential Access via LaZagne

- **Trigger Condition:** Credential access via the popular open-source LaZagne tool is detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** OS Credential Dumping, LSASS Memory
- **ATT&CK ID:** T1003,T1003.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

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

RDP Connection Inititated from Domain Controller

- **Trigger Condition:** Initiation of RDP connection from a domain controller is detected.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Remote Services, Remote Desktop Protocol
- **ATT&CK ID:** T1021, T1021.001
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer  event_source="Microsoft-Windows-TerminalServices-RemoteConnectionManager" event_id=1149 |
rename eventxml.param3 as source_address | search source_address IN WINDOWS_DC
```

Active Directory Module Load in PowerShell

- **Trigger Condition:** Active Directory module loading in PowerShell is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, PowerShell
- **ATT&CK ID:** T1059, T1059.001
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4103 command="Import-Module" payload="*ActiveDirectory*"
```

Possible Active Directory Enumeration via AD Module

- **Trigger Condition:** Enumeration of Active Directory via PowerShell’s AD module is detected.
- **ATT&CK Category:** Execution, Discovery
- **ATT&CK Tag:** Remote System Discovery, Command and Scripting Interpreter, PowerShell
- **ATT&CK ID:** T1018, T1059, T1059.001
- **Minimum Log Source Requirement:** Windows
- **Query:**

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

Microsoft Defender Disabling Attempt via PowerShell

- **Trigger Condition:** An attempt to disable Microsoft Defender via PowerShell is detected.
- **ATT&CK Category:** Defense Evasion, Execution
- **ATT&CK Tag:** Impair Defenses, Disable or Modify Tools, Command and Scripting Interpreter, PowerShell
- **ATT&CK ID:** T1562, T1562.001, T1059, T1059.001
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4104 script_block="Set-MpPreference -DisableRealtimeMonitoring $true"
```

Possible Kerberoasting via Rubeus

- **Trigger Condition:** Kerberoasting attack via popular open-source tool Rubeus is detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Steal or Forge Kerberos Tickets, Kerberoasting
- **ATT&CK ID:** T1558, T1558.003
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=7 -source_image="C:\Windows\System32\*" image IN ["*\clr.dll", "*\kerberos.dll", "*\cryptdll.dll", "*\dsparse.dll"]
| chart distinct_count(image) as dc, distinct_list(image) as images | search dc=4
```

Suspicious Scheduled Task Creation

- **Trigger Condition:** When a suspicious scheduled task creation is detected in a Windows endpoint. The suspicious task here refers to tasks running scripts or programs from temp directories or insecure locations (writable by any user). Adversaries may abuse the Windows Task Scheduler to perform task scheduling for the initial or recurring execution of malicious code to achieve persistence, lateral movement, execution, detection evasion, and privilege escalation. Also, it is prevalent among ransomware to use public directories for scheduled task creation.

- **ATT&CK Category:** Execution, Persistence, Privilege Escalation
- **ATT&CK Tag:** Scheduled Task/Job, Scheduled Task
- **ATT&CK ID:** T1053, T1053.005
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer label=Schedule label=Task label=Create command IN ["*C:\Users\*", "*C:\Windows\Temp\*", "*C:\ProgramData\*"] -command="C:\ProgramData\Microsoft\Windows Defender\Platform\*"
```

RDP Connection Inititated from Suspicious Country

- **Trigger Condition:** Initiation of RDP connection from a domain controller is detected.
- **ATT&CK Category:** Defense Evasion, Persistence, Privilege Escalation, Initial Access
- **ATT&CK Tag:** Valid Accounts, Domain Accounts
- **ATT&CK ID:** T1078, T1078.002
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer  event_source="Microsoft-Windows-TerminalServices-RemoteConnectionManager" event_id=1149 -eventxml.param3 IN HOMENET | rename eventxml.param3 as source_address
| process geoip(source_address) as country | search country IN SUSPICIOUS_COUNTRY
```

Scheduled Task Deletion

- **Trigger Condition:** Deletion of a scheduled task is detected using schtasks utility with delete command.
- **ATT&CK Category:** Execution, Persistence, Privilege Escalation
- **ATT&CK Tag:** Scheduled Task/Job, Scheduled Task
- **ATT&CK ID:** T1053, T1053.005
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 image='*\schtasks.exe' command='*delete*'
```

Possible GootKit WScript Execution

- **Trigger Condition:** GootKit banking trojan’s WScript execution activity is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** Command and Scripting Interpreter, Visual Basic
- **ATT&CK ID:** T1059, T1059.003
- **Minimum Log Source Requirement:** Windows

- **Query:**

```
norm_id=WinServer event_id=4688 "process"="*\wscript.exe" command="*\APPDATA\*.js*"
```

Winnti IoC Domain Match

- **Trigger Condition:** A match for Winnti (APT41) group’s IoC domain is found. The IoC reference is PT ESC Threat Intelligence, January 14, 2021.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Firewall, Proxy Server
- **Query:**

```
(domain IN WINNTI_DOMAINS OR query IN WINNTI_DOMAINS) | rename query as ioc, domain as ioc
```

Winnti IoC Hash Match

- **Trigger Condition:** A match for Winnti (APT41) group’s IoC hash is found. The IoC reference is PT ESC Threat Intelligence, January 14, 2021.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** Antivirus, EDR, Sysmon
- **Query:**

```
(hash IN WINNTI_HASHES OR hash_sha1 IN WINNTI_HASHES OR hash_sha256 IN WINNTI_HASHES) | rename hash as ioc, hash_sha1 as ioc, hash_sha256 as ioc
```

Zerologon CVE-2020-1472 Exploitation Detected

- **Trigger Condition:** The exploitation of Zerologon (CVE-2020-1472) in domain controllers is detected. For this alert to work, you must update the list WINDOWS_DC with a computer name of domain controllers ending with $ in the Active Directory. By default, in Active Directory, the domain computers submit a request to change the password every 30 days, hence you can expect some false positives.
- **ATT&CK Category:** Privilege Escalation
- **ATT&CK Tag:** Exploitation for Privilege Escalation
- **ATT&CK ID:** T1068
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
(hash IN WINNTI_HASHES OR hash_sha1 IN WINNTI_HASHES OR hash_sha256 IN WINNTI_HASHES) | rename hash as ioc, hash_sha1 as ioc, hash_sha256 as ioc
```

Allowed NetLogon Connections - CVE-2020-1472

- **Trigger Condition:** Any vulnerable Netlogon connections detected after installation of the Zerologon patch during the initial deployment phase.
- **ATT&CK Category:** Privilege Escalation
- **ATT&CK Tag:** Exploitation for Privilege Escalation
- **ATT&CK ID:** T1068
- **Minimum Log Source Requirement:** Windows
- **Query:**
- `norm_id=WinServer event_id=5829`

Denied NetLogon Connections - CVE-2020-1472

- **Trigger Condition:** Any denied vulnerable Netlogon connections detected after installation of the Zerologon patch.
- **ATT&CK Category:** Privilege Escalation
- **ATT&CK Tag:** Exploitation for Privilege Escalation
- **ATT&CK ID:** T1068
- **Minimum Log Source Requirement:** Windows
- **Query:**
- `norm_id=WinServer event_id IN ["5827", "5828"]`

Allowed NetLogon Connections via Group Policy - CVE-2020-1472

- **Trigger Condition:** Any allowed vulnerable Netlogon connections detects *Domain controller: allow vulnerable Netlogon secure channel connections* in Group Policy setting.
- **ATT&CK Category:** Privilege Escalation
- **ATT&CK Tag:** Exploitation for Privilege Escalation
- **ATT&CK ID:** T1068
- **Minimum Log Source Requirement:** Windows
- **Query:**
- `norm_id=WinServer event_id IN ["5830", "5831"]`

Exchange Remote Code Execution CVE-2020-0688 Attempt

- **Trigger Condition:** A remote code execution attempt via CVE-2020-0688 in Microsoft Exchange is detected.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** External Remote Services
- **ATT&CK ID:** T1133
- **Minimum Log Source Requirement:** Firewall, Proxy Server
- **Query:**

```
norm_id=* (url="*/ecp/default.aspx*__VIEWSTATEGENERATOR*VIEWSTATE=*" OR resource="*__VIEWSTATEGENERATOR*VIEWSTATE=*")
```

BlueKeep Vulnerability CVE-2019-0708 Exploitation

- **Trigger Condition:** The exploitation of BlueKeep, a remote desktop services remote code execution vulnerability, also known as CVE-2019-0708 is detected.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** Exploitation of Remote Services
- **ATT&CK ID:** T1210
- **Minimum Log Source Requirement:** IDS/IPS
- **Query:**

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

Confluence Remote Code Execution CVE-2019-3398 Attempt

- **Trigger Condition:** A remote code execution via CVE-2019-3398 in Confluence Server and Data Center is detected.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** Exploit Public-Facing Application
- **ATT&CK ID:** T1190
- **Minimum Log Source Requirement:** Firewall, Proxy Server
- **Query:**

```
norm_id=* request_method=POST (url='*plugins/drag-and-drop/upload.action*filename=../../*.jsp*' OR resource='*plugins/drag-and-drop/upload.action*filename=../../*.jsp*')
```

ZoHo ManageEngine Pre-Auth File Upload CVE-2019-8394 Exploitation Attempt

- **Trigger Condition:** A pre-auth file upload vulnerability CVE-2019-8394 in ZoHo ManageEngine ServiceDesk Plus is detected.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** Exploit Public-Facing Application
- **ATT&CK ID:** T1190
- **Minimum Log Source Requirement:** Firewall, Proxy Server
- **Query:**

```
norm_id=* request_method=POST (url='*/common/FileAttachment.jsp?module=CustomLogin*' OR resource='*/common/FileAttachment.jsp?module=CustomLogin*')
```

ZoHo ManageEngine Desktop Central CVE-2020-10189 Exploitation Attempt

- **Trigger Condition:** A remote code execution attempt via CVE-2019-11580 in ZoHo ManageEngine Desktop Central is detected.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** Exploit Public-Facing Application
- **ATT&CK ID:** T1190
- **Minimum Log Source Requirement:** Firewall, Proxy Server
- **Query:**

```
norm_id=* request_method=POST (url='*/mdm/client/v1/mdmLogUploader*webapps*_chart*' OR resource='*/mdm/client/v1/mdmLogUploader*webapps*_chart*')
```

Atlassian Crowd Remote Code Execution CVE-2019-11580 Exploitation Attempt

- **Trigger Condition:** A remote code execution attempt via CVE-2019-11580 in Atlassian Crowd is detected.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** Exploit Public-Facing Application
- **ATT&CK ID:** T1190
- **Minimum Log Source Requirement:** Firewall, Proxy Server
- **Query:**

```
norm_id=* request_method=POST content_type="multipart/mixed*" (url='*/crowd/admin/uploadplugin.action*' OR resource='*/crowd/admin/uploadplugin.action*')
```

Fortinet Pre-Auth File Read CVE-2018-13379 Exploitation Attempt

- **Trigger Condition:** The exploitation of pre-auth file read vulnerability (2018-13379) in Fortinet FortiOS is detected.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** External Remote Services
- **ATT&CK ID:** T1133
- **Minimum Log Source Requirement:** Firewall, Proxy Server
- **Query:**

```
norm_id=* (url='*lang=/../../*/dev/cmdb/sslvpn_websession*' OR resource='*lang=/../../*/dev/cmdb/sslvpn_websession*')
```

Adobe ColdFusion Remote Code Execution CVE-2018-15961 Attempt

- **Trigger Condition:** The exploitation of arbitrary file upload vulnerability (CVE-2018-15961) to upload JSP webshell for remote code execution in Adobe ColdFusion is detected.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** Exploit Public-Facing Application

- **ATT&CK ID:** T1190
- **Minimum Log Source Requirement:** Firewall, Proxy Server
- **Query:**

-
  ```
  norm_id=* request_method=POST (url='*/cf_scripts/*/upload.cfm*' OR resource='*/cf_scripts/*/upload.cfm*')
  ```

Creation of Encrypted Winrar archive via CLI

- **Trigger Condition:** Creation of an encrypted RAR archive via CLI is detected.
- **ATT&CK Category:** Execution, Collection
- **ATT&CK Tag:** Obfuscated Files or Information, Software Packing, Archive Collected Data, Archive via Utility
- **ATT&CK ID:** T1027, T1027.002, T1560, T1560.001
- **Minimum Log Source Requirement:** Windows
- **Query:**

-
  ```
  norm_id=WindowsSysmon event_id=1 image='*\rar.exe' command='*-hp*'
  ```

Default Hard disk Usage Status

- **Trigger Condition:** The hard disk uses storage greater than or equal to 80%.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** LogPoint
- **Query:**

-
  ```
  label=Harddisk label=Usage label=Metrics use>=80
  ```

Default License Grace State

- **Trigger Condition:** LogPoint’s license has expired and is operating in grace state.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** LogPoint
- **Query:**

-
  ```
  norm_id=LogPoint label=Audit label=License label=Grace
  ```

Default License Invalid

- **Trigger Condition:** LogPoint’s license is no longer valid.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **ATT&CK ID:** -
- **Minimum Log Source Requirement:** LogPoint
- **Query:**

-
  ```
  norm_id=LogPoint label=Audit label=License label=Invalid
  ```

Microsoft Build Engine Loading Credential Libraries

- **Trigger Condition:** Loading of credential libraries by Microsoft Build engine is detected.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** OS Credential Dumping, Security Account Manager
- **ATT&CK ID:** T1003, T1003.002
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

-
  ```
  norm_id=WindowsSysmon event_id=7 source_image='*msbuild.exe' image IN ['vaultcli.dll', 'SAMLib.DLL']
  ```

Microsoft Build Engine started by Office

- **Trigger Condition:** Execution of Microsoft Build engine by Office products is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Trusted Developer Utilities Proxy Execution, MSBuild
- **ATT&CK ID:** T1127, T1127.001
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

-
  ```
  norm_id=WindowsSysmon event_id=1 image='*msbuild.exe' parent_image IN ['*eqnedt32.exe', '*excel.exe', '*fltldr.exe', '*msaccess.exe', '*winword.exe', '*mspub.exe', '*outlook.exe', '*powerpnt.exe']
  ```

Potential Botnet Infected Host Detected

- **Trigger Condition:** Botnet-infected host 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:** -
- **Query:**

-
  ```
  label=Botnet label=Detect source_address=* destination_address=* (host=* or device_address=*) | rename device_address as host
  ```

Potential Phishing Attack Detected

- **Trigger Condition:** Phishing attack is detected
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** Phishing, Spearphishing Attachment
- **ATT&CK ID:** T1566, T1566.001
- **Minimum Log Source Requirement:** MailServer

- **Query:**

-
  ```
  label=Detect label=Malicious label=File file=* sender=* receiver=* hash=*
  ```

Potential Malware Infected Host Detected

- **Trigger Condition:** A ransomware-infected host is detected.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Data Encrypted for Impact
- **ATT&CK ID:** T1486
- **Minimum Log Source Requirement:** -
- **Query:**

-
  ```
  (label=Detect label=Malware label=Infection malware="*Ransom*") OR (hash IN MALWARE_HASH) host=* hash=*
  ```

PowerShell Module Logging Setting Discovery

- **Trigger Condition:** Enumeration of PowerShell module logging setting is detected.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** Query Registry
- **ATT&CK ID:** T1012
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

-
  ```
  norm_id=WindowsSysmon event_id=13 target_object="*\PowerShell\ModuleLogging*"
  ```

PowerShell Module Logging Setting Discovery

- **Trigger Condition:** Multiple failed user logins followed by successful login 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:**

-
  ```
  [4 norm_id=WinServer* label=User label=Login label=Fail user!=*user=∗havingsameuser]asFailfollowedby[normid=WinServer∗label=Userlabel=Loginlabel=Successfuluser!=∗user=∗havingsameuser]asFailfollowedby[normid=WinServer∗label=Userlabel=Loginlabel=Successfuluser!=∗ user=*]
  ```

-
  ```
  as Login on Fail.user=Login.user | rename user as User, Login.source_address as SourceAddress
  ```

Safe DLL Search Mode Disabled

- **Trigger Condition:** Safe DLL search mode is disabled.

- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Impair Defenses, Indicator Blocking
- **ATT&CK ID:** T1562, T1562.001
- **Minimum Log Source Requirement:** Windows
- **Query:**
-
  ```
  norm_id=WindowSysmon event_id=13 target_object='*\CurrentControlSet\Control\Session Manager\SafeDllSearchMode' detail="DWORD (0x00000000)"
  ```

Potential Intrusion Detected

- **Trigger Condition:** An intrusion by IDS or IPS devices is detected.
- **ATT&CK Category:** Command and Control, Defense Evasion
- **ATT&CK Tag:** Proxy, Exploitation for Defense Evasion
- **ATT&CK ID:** T1090, T1211
- **Minimum Log Source Requirement:** -
- **Query:**
-
  ```
  label=Intrusion label=Detect source_address=* destination_address=*
  ```

Windows Crash Dump Disabled

- **Trigger Condition:** Windows’s crash dump registry setting is disabled.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Modify Registry
- **ATT&CK ID:** T1112
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  norm_id=WindowsSysmon event_id=13 target_object="HKLM\System\CurrentControlSet\Control\CrashControl\CrashDumpEnabled" detail="DWORD (0x00000000)"
  ```

Suspicious Shells Spawn by SQL Server

- **Trigger Condition:** A suspicious shell process is spawned by the SQL Server process which may indicate exploitation of a vulnerability.
- **ATT&CK Category:** Initial Access, Execution
- **ATT&CK Tag:** Exploit Public-Facing Application, PowerShell
- **ATT&CK ID:** T1190, T1059.001
- **Minimum Log Source Requirement:** Windows
- **Query:**
-
  ```
  norm_id=WinServer event_id=4688 parent_process="*\sqlservr.exe" "process" IN ["*\cmd.exe", "*\powershell.exe", "*\bash.exe", "*\sh.exe", "*\bitsadmin.exe"] -(parent_process IN ["C:\Program Files\Microsoft SQL Server\*", "*DATEV_DBENGINE\MSSQL\Binn\sqlservr.exe"] "process"="C:\Windows\System32\cmd.exe" command='"C:\Windows\system32\cmd.exe" *')
  ```

HermeticWiper Driver Load

- **Trigger Condition:** When loading of HermeticWiper's driver IoC hashes is detected.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=6 (hash IN HERMETIC_WIPER_DRIVER_HASHES OR hash_sha1 IN HERMETIC_WIPER_DRIVER_HASHES OR hash_sha256 IN HERMETIC_WIPER_DRIVER_HASHES) | rename hash as ioc, hash_sha1 as ioc, hash_sha256 as ioc
```

UltraVNC Execution via Command Line

- **Trigger Condition:** When UltraVNC execution via the command line is detected. Gamaredon is known to use this technique for gaining remote access.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** Remote Access Software
- **ATT&CK ID:** T1219
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
norm_id=WinServer event_id=4688 command="*-autoreconnect *" command="*-connect *" command="*-id:*"
```

Office Security Settings Changed

- **Trigger Condition:** When modification of Microsoft Office security settings in the registry is detected.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Modify Registry
- **ATT&CK ID:** T1112
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=13 target_object In ["*\Security\Trusted Documents\TrustRecords*", "*\Security\AccessVBOM*", "*\Security\VBAWarnings*"]
```

HermeticWiper IoC Hashes Detected

- **Trigger Condition:** When any Hermetic Wiper IoC hash match is found. IoC Reference: Hashes are latest up to March 2022.
- **ATT&CK Category:** Resource Development
- **ATT&CK Tag:** Malware
- **ATT&CK ID:** T1588.001
- **Minimum Log Source Requirement:** IDS, IPS, Firewall, Windows Sysmon
- **Query:**

-
  ```
  (hash IN HERMETIC_WIPER_HASHES OR hash_sha1 IN HERMETIC_WIPER_HASHES OR hash_sha256 IN HERMETIC_WIPER_HASHES) | rename hash as ioc, hash_sha1 as ioc, hash_sha256 as ioc
  ```

IsaacWiper IoC Hashes Detected

- **Trigger Condition:** When any Issac Wiper IoC hash match is found. IoC Reference: Hashes are latest up to March 2022.
- **ATT&CK Category:** Resource Development
- **ATT&CK Tag:** Malware
- **ATT&CK ID:** T1588.001
- **Minimum Log Source Requirement:** IDS, IPS, Firewall, Windows Sysmon
- **Query:**

-
  ```
  (hash IN ISAAC_WIPER_HASHES OR hash_sha1 IN ISAAC_WIPER_HASHES OR hash_sha256 IN ISAAC_WIPER_HASHES) | rename hash as ioc, hash_sha1 as ioc, hash_sha256 as ioc
  ```

Actinium IoC Hashes Detected

- **Trigger Condition:** When any Actinium IoC hash match is found. IoC Reference: Hashes are latest up to March 2022.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** IDS, IPS, Firewall, Windows Sysmon
- **Query:**

-
  ```
  (hash IN ACTINIUM_HASHES OR hash_sha1 IN ACTINIUM_HASHES OR hash_sha256 IN ACTINIUM_HASHES) | rename hash as ioc, hash_sha1 as ioc, hash_sha256 as ioc
  ```

WhisperGate IoC Hashes Detected

- **Trigger Condition:** When any WhisperGate IoC hash match by DEV-0586 is found. IoC Reference: Hashes are latest up to Feb 2022.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** IDS, IPS, Firewall, Windows Sysmon
- **Query:**

-
  ```
  (hash IN WHISPERGATE_HASHES OR hash_sha1 IN WHISPERGATE_HASHES OR hash_sha256 IN WHISPERGATE_HASHES) | rename hash as ioc, hash_sha1 as ioc, hash_sha256 as ioc
  ```

GhostWriter IoC Detected

- **Trigger Condition:** When any Belarusian threat actor GhostWriter (UNC1151) IoC domains or IP Address match is found. IoC Reference: IoCs are latest up to Feb 2022.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** Phising
- **ATT&CK ID:** T1566
- **Minimum Log Source Requirement:** IDS, IPS, Firewall, Windows Sysmon
- **Query:**

```
(domain IN GHOSTWRITER_DOMAINS OR source_address IN GHOSTWRITER_IPS OR destination_address IN GHOSTWRITER_IPS)
```

Actinium IoC Domains Detected

- **Trigger Condition:** When any Actinium IoC domain match is found. IoC Reference: Hashes are latest up to Feb 2022.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** IDS, IPS, Firewall
- **Query:**

```
domain IN ACTINIUM_DOMAINS
```

Suspicious VMToolsd Child Process

- **Trigger Condition:** Creation of a suspicious child process of the VMware Tools process that may indicate persistence set up by attackers.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** T1059 - Command and Scripting Interpreter
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer event_id=4688 parent_process="*\vmtoolsd.exe" image IN ["*\cmd.exe", "*\powershell.exe", "*\wscript.exe", "*\cscript.exe", "*\rundll32.exe", "*\regsvr32.exe"] -command IN ["*\VMware\VMware Tools\poweron-vm-default.bat*", "*\VMware\VMware Tools\poweroff-vm-default.bat*", "*\VMware\VMware Tools\resume-vm-default.bat*", "*\VMware\VMware Tools\suspend-vm-default.bat*"]
```

Credential Access via Pypykatz

- **Trigger Condition:** Credential access via the popular open-source Pypykatz tool. Pypykatz is a Mimikatz implementation in the Python version >= 3.6.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** T1003.001 - LSASS Memory
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=10 image="*\lsass.exe" call_trace="*C:\Windows\SYSTEM32\ntdll.dll+*" call_trace="*C:\Windows\System32\KERNELBASE.dll+*" call_
```

```
trace="*libffi-7.dll*" call_trace="*_ctypes.pyd+*" call_trace="*python3*.dll+*"
```

Atlassian Confluence CVE-2021-26084 Exploitation

- **Trigger Condition:** Spawning of suspicious child processes by Atlassian Confluence server process that may indicate successful exploitation of CVE-2021-26084. CVE-2021-26084 is an OGNL injection vulnerability in Confluence Server and Data Center that allows an unauthenticated attacker to execute arbitrary code on a Confluence Server or Data Center instance. Confluence Server and Data Center versions before v6.13.23, v6.14.0 before v7.4.11, v7.5.0 before 7.11.6, and v7.12.0 before v7.12.5 are affected by this vulnerability.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** T1190 - Exploit Public-Facing Application
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

-
  ```
  label="Process" label=Create parent_process="*\Atlassian\Confluence\jre\bin\java.exe" command IN ["*cmd /c*", "*cmd /k*", "*powershell*", "*certutil*", "*curl*", "*whoami*", "*ipconfig*"]
  ```

Impacket PsExec Execution

- **Trigger Condition:** Execution of Impacket’s PsExec utility is detected. Impacket is a collection of Python classes for working with network protocols. Impacket focuses on providing low-level programmatic access to the packets and is commonly used in PoCs.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** T1570 - Lateral Tool Transfer
- **Minimum Log Source Requirement:** Windows
- **Query:**

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

Oracle WebLogic CVE-2021-2109 Exploitation

- **Trigger Condition:** Possible exploitation of the Oracle WebLogic server vulnerability CVE-2021-2109 is detected. This vulnerability allows a high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** T1190 - Exploit Public-Facing Application
- **Minimum Log Source Requirement:** Firewall, Proxy Server
- **Query:**

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

Possible JSP Webshell Detected

- **Trigger Condition:** JSP Webshell is detected in the URL. This may indicate springshell is being exploited. However, if .jsp and .class files are commonly used in the network, the result may be false positives.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** T1505.003 - Web Shell
- **Minimum Log Source Requirement:** -
- **Query:**
-
  ```
  status_code=200 request_method IN ["POST", "GET"] url in ["*.jsp*", "*.class*"]
  ```

PowerShell ADRecon Execution

- **Trigger Condition:** Execution of the ADRecon PowerShell script for AD reconnaissance is detected. The script is reported to be actively used by FIN7. For the alert to work, the Script block logging must be enabled.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** T1059 - Command and Scripting Interpreter, T1059.001 - PowerShell
- **Minimum Log Source Requirement:** Windows
- **Query:**
-
  ```
  norm_id=WinServer event_id=4104 script_block IN ["*Function Get-ADRExcelComOb*", "*ADRecon-Report.xlsx*"] -user IN EXCLUDED_USERS
  ```

PowerView PowerShell Commandlets

- **Trigger Condition:** Execution of PowerShell commandlets of the popular PowerView module of the PowerSploit framework is detected. For the alert to work, the script block logging must be enabled.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** T1059 - Command and Scripting Interpreter, T1059.001 - PowerShell
- **Minimum Log Source Requirement:** Windows
- **Query:**
-
  ```
  norm_id=WinServer event_id=4104 script_block IN ["Export-PowerViewCSV", "Get-IPAddress", "Resolve-IPAddress", "Convert-NameToSid", "ConvertTo-SID", "Convert-ADName", "ConvertFrom-UACValue", "Add-RemoteConnection", "Remove-RemoteConnection", "Invoke-UserImpersonation", "Invoke-RevertToSelf", "Request-SPNTicket", "Get-DomainSPNTicket", "Invoke-Kerberoast", "Get-PathAcl", "Get-DNSZone", "Get-DomainDNSZone", "Get-DNSRecord", "Get-DomainDNSRecord", "Get-NetDomain", "Get-Domain", "Get-NetDomainController", "Get-DomainController", "Get-NetForest", "Get-Forest", "Get-NetForestDomain", "Get-ForestDomain", "Get-NetForestCatalog", "Get-ForestGlobalCatalog", "Find-DomainObjectPropertyOutlier", "Get-NetUser", "Get-DomainUser", "New-DomainUser", "Set-DomainUserPassword", "Get-UserEvent", "Get-DomainUserEvent", "Get-NetComputer", "Get-DomainComputer", "Get-ADObject", "Get-DomainObject", "Set-ADObject", "Set-DomainObject", "Get-ObjectAcl", "
  ```

```
Get-DomainObjectAcl", "Add-ObjectAcl", "Add-DomainObjectAcl", "Invoke-ACLScann
er", "Find-InterestingDomainAcl", "Get-NetOU", "Get-DomainOU", "Get-NetSite", "
Get-DomainSite", "Get-NetSubnet", "Get-DomainSubnet", "Get-DomainSID", "Get-Ne
tGroup", "Get-DomainGroup", "New-DomainGroup", "Find-ManagedSecurityGroups", "
Get-DomainManagedSecurityGroup", "Get-NetGroupMember", "Get-DomainGroupMember"
, "Add-DomainGroupMember", "Get-NetFileServer", "Get-DomainFileServer", "Get-D
FSshare", "Get-DomainDFSShare", "Get-NetGPO", "Get-DomainGPO", "Get-NetGPOGrou
p", "Get-DomainGPOLocalGroup", "Find-GPOLocation", "Get-DomainGPOUserLocalGrou
pMapping", "Find-GPOComputerAdmin", "Get-DomainGPOComputerLocalGroupMapping", "
Get-DomainPolicy", "Get-NetLocalGroup", "Get-NetLocalGroupMember", "Get-NetSha
re", "Get-NetLoggedon", "Get-NetSession", "Get-LoggedOnLocal", "Get-RegLoggedO
n", "Get-NetRDPSession", "Invoke-CheckLocalAdminAccess", "Test-AdminAccess", "
Get-SiteName", "Get-NetComputerSiteName", "Get-Proxy", "Get-WMIRegProxy", "Get
-LastLoggedOn", "Get-WMIRegLastLoggedOn", "Get-CachedRDPConnection", "Get-WMIR
egCachedRDPConnection", "Get-RegistryMountedDrive", "Get-WMIRegMountedDrive", "
Get-NetProcess", "Get-WMIProcess", "Find-InterestingFile", "Invoke-UserHunter"
, "Find-DomainUserLocation", "Invoke-ProcessHunter", "Find-DomainProcess", "In
voke-EventHunter", "Find-DomainUserEvent", "Invoke-ShareFinder", "Find-DomainS
hare", "Invoke-FileFinder", "Find-InterestingDomainShareFile", "Find-LocalAdmi
nAccess", "Invoke-EnumerateLocalAdmin", "Find-DomainLocalGroupMember", "Get-Ne
tDomainTrust", "Get-DomainTrust", "Get-NetForestTrust", "Get-ForestTrust", "Fi
nd-ForeignUser", "Get-DomainForeignUser", "Find-ForeignGroup", "Get-DomainFore
ignGroupMember", "Invoke-MapDomainTrust", "Get-DomainTrustMapping"] -user IN E
XCLUDED_USERS
```

PowerView PowerShell Commandlets

- **Trigger Condition:** Execution of PowerShell commandlets of the popular PowerView module of the PowerSploit framework is detected. For the alert to work, the script block logging must be enabled.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** T1059 - Command and Scripting Interpreter, T1059.001 - PowerShell
- **Minimum Log Source Requirement:** Windows
- **Query:**
-
```
norm_id=WinServer event_id=4104 script_block IN ["Export-PowerViewCSV", "Get-I
PAddress", "Resolve-IPAddress", "Convert-NameToSid", "ConvertTo-SID", "Convert
-ADName", "ConvertFrom-UACValue", "Add-RemoteConnection", "Remove-RemoteConnec
tion", "Invoke-UserImpersonation", "Invoke-RevertToSelf", "Request-SPNTicket",
"Get-DomainSPNTicket", "Invoke-Kerberoast", "Get-PathAcl", "Get-DNSZone", "Get
-DomainDNSZone", "Get-DNSRecord", "Get-DomainDNSRecord", "Get-NetDomain", "Get
-Domain", "Get-NetDomainController", "Get-DomainController", "Get-NetForest", "
Get-Forest", "Get-NetForestDomain", "Get-ForestDomain", "Get-NetForestCatalog"
, "Get-ForestGlobalCatalog", "Find-DomainObjectPropertyOutlier", "Get-NetUser"
, "Get-DomainUser", "New-DomainUser", "Set-DomainUserPassword", "Get-UserEvent
", "Get-DomainUserEvent", "Get-NetComputer", "Get-DomainComputer", "Get-ADObje
ct", "Get-DomainObject", "Set-ADObject", "Set-DomainObject", "Get-ObjectAcl", "
Get-DomainObjectAcl", "Add-ObjectAcl", "Add-DomainObjectAcl", "Invoke-ACLScann
er", "Find-InterestingDomainAcl", "Get-NetOU", "Get-DomainOU", "Get-NetSite", "
Get-DomainSite", "Get-NetSubnet", "Get-DomainSubnet", "Get-DomainSID", "Get-Ne
tGroup", "Get-DomainGroup", "New-DomainGroup", "Find-ManagedSecurityGroups", "
Get-DomainManagedSecurityGroup", "Get-NetGroupMember", "Get-DomainGroupMember"
, "Add-DomainGroupMember", "Get-NetFileServer", "Get-DomainFileServer", "Get-DFSshare", "Get-DomainDFSShare", "Get-NetGPO", "Get-DomainGPO", "Get-NetGPOGroup", "Get-DomainGPOLocalGroup", "Find-GPOLocation", "Get-DomainGPOUserLocalGroupMapping", "Find-GPOComputerAdmin", "Get-DomainGPOComputerLocalGroupMapping", "Get-DomainPolicy", "Get-NetLocalGroup", "Get-NetLocalGroupMember", "Get-NetShare", "Get-NetLoggedon", "Get-NetSession", "Get-LoggedOnLocal", "Get-RegLoggedOn", "Get-NetRDPSession", "Invoke-CheckLocalAdminAccess", "Test-AdminAccess", "Get-SiteName", "Get-NetComputerSiteName", "Get-Proxy", "Get-WMIRegProxy", "Get-LastLoggedOn", "Get-WMIRegLastLoggedOn", "Get-CachedRDPConnection", "Get-WMIRegCachedRDPConnection", "Get-RegistryMountedDrive", "Get-WMIRegMountedDrive", "Get-NetProcess", "Get-WMIProcess", "Find-InterestingFile", "Invoke-UserHunter", "Find-DomainUserLocation", "Invoke-ProcessHunter", "Find-DomainProcess", "Invoke-EventHunter", "Find-DomainUserEvent", "Invoke-ShareFinder", "Find-DomainShare", "Invoke-FileFinder", "Find-InterestingDomainShareFile", "Find-LocalAdminAccess", "Invoke-EnumerateLocalAdmin", "Find-DomainLocalGroupMember", "Get-NetDomainTrust", "Get-DomainTrust", "Get-NetForestTrust", "Get-ForestTrust", "Find-ForeignUser", "Get-DomainForeignUser", "Find-ForeignGroup", "Get-DomainForeignGroupMember", "Invoke-MapDomainTrust", "Get-DomainTrustMapping"] -user IN EXCLUDED_USERS
```

SpringShell Indicators of Compromise Detected

- **Trigger Condition:** SpringShell indicator of compromise is detected. This alerts checks if any of the request method parameter and URL is being used in conjunction to access a command injection once a file has been created.
- **ATT&CK Category:** Execution, Persistence, Command and Control
- **ATT&CK Tag:** T1102 - Web Service, T1204.002 - Malicious File, T1505.003 - Web Shell
- **Minimum Log Source Requirement:** -
- **Query:**

```
request_method in ["POST", "GET"] url IN ["*?class.module.classloader.resources.context.parent.pipeline.first.*",  "*java.io.InputStream%20in%20%3D%20%25%7Bc1%7Di*", "*pwd=*", "*cmd=*", "*.getParameter(%22pwd%22)*"]
```

SpringShell Indicators of Compromise Detected

- **Trigger Condition:** SpringShell indicator of compromise is detected. This alerts checks if any of the request method parameter and URL is being used in conjunction to access a command injection once a file has been created.
- **ATT&CK Category:** Execution, Persistence, Command and Control
- **ATT&CK Tag:** T1102 - Web Service, T1204.002 - Malicious File, T1505.003 - Web Shell
- **Minimum Log Source Requirement:** -
- **Query:**

```
request_method in ["POST", "GET"] url IN ["*?class.module.classloader.resources.context.parent.pipeline.first.*",  "*java.io.InputStream%20in%20%3D%20%25%7Bc1%7Di*", "*pwd=*", "*cmd=*", "*.getParameter(%22pwd%22)*"]
```

SpringShell Webshell Detected in URL

- **Trigger Condition:** Successful SpringShell resources are requested. Based on the POC, the alert rule may be false positives if the pages are hosted with .jsp or .class files in the network.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** T1505.003 - Web Shell
- **Minimum Log Source Requirement:** -
- **Query:**
-
  ```
  status_code=200 url IN ["*.jsp*", "*.class*"]| norm on url <webShell:'\/.*\.(jsp|class)\?.*=.*'> | filter webShell=*
  ```

Stealthy VSTO Persistence

- **Trigger Condition:** Persistence via Visual Studio Tools for Office (VSTO) add-ins in Office application.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** T1137.006 - Add-ins
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  norm_id=WindowsSysmon event_id=13 target_object IN ["*\Software\Microsoft\Office\Outlook\Addins\*", "*\Software\Microsoft\Office\Word\Addins\*", "*\Software\Microsoft\Office\Excel\Addins\*", "*\Software\Microsoft\Office\Powerpoint\Addins\*", "*\Software\Microsoft\VSTO\Security\Inclusion\*"] -user IN EXCLUDED_USERS -image IN ["*\msiexec.exe", "*\regsvr32.exe", "*\winword.exe", "*\integrator.exe", "*\OfficeClickToRun.exe"]
  ```

Suspicious DLL or VBS Files being created in ProgramData

- **Trigger Condition:** When a file is created with .dll or vbs extension to the ProgramData folder. A DLL is a library containing code and data that can be used by multiple programs simultaneously. VBScript is an interpreted script language from Microsoft that is a subset of its Visual Basic programming language designed for interpretation by Microsoft's Internet Explorer web browser. Attackers use these techniques for the execution of malicious payloads. This method is predominantly used in Bumblebee attacks.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** T1204.002 - Malicious File
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  norm_id=WindowsSysmon event_id=11 file IN ["*.dll", "*.vbs"] path="C:\ProgramData*"
  ```

Suspicious VMToolsd Child Process

- **Trigger Condition:** Creation of suspicious child process VMware Tools process, which may indicate persistence set up by attackers.

- **ATT&CK Category:** Execution
- **ATT&CK Tag:** T1059 - Command and Scripting Interpreter
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
```
norm_id=WinServer event_id=4688 parent_process="*\vmtoolsd.exe" image IN ["*\cmd.exe", "*\powershell.exe", "*\wscript.exe", "*\cscript.exe", "*\rundll32.exe", "*\regsvr32.exe"] -command IN ["*\VMware\VMware Tools\poweron-vm-default.bat*", "*\VMware\VMware Tools\poweroff-vm-default.bat*", "*\VMware\VMware Tools\resume-vm-default.bat*", "*\VMware\VMware Tools\suspend-vm-default.bat*"]
```

Suspicious WMPRVSE Child Process

- **Trigger Condition:** A suspicious child process of WMIC is detected.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** T1047 - Windows Management Instrumentation
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
```
norm_id=WindowsSysmon event_id=1 parent_image="*\wmprvse.exe" -image IN ["C:\Windows\System32\conhost.exe", "C:\Windows\system32\wbem\WMIC.exe", "C:\Windows\syswow64\wbem\WMIC.exe", "C:\Windows\system32\WerFault.exe", "C:\Windows\SysWOW64\WerFault.exe"]
```

TerraMaster TOS CVE-2020-28188 Exploitation

- **Trigger Condition:** The exploitation of the TerraMaster TOS vulnerability CVE-2020-28188 is detected. CVE-2020-28188 is a remote command execution (RCE) vulnerability in TerraMaster TOS <= v4.2.06 that allows remote unauthenticated attackers to inject OS commands.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** T1190 - Exploit Public-Facing Application
- **Minimum Log Source Requirement:** Firewall, Proxy Server
- **Query:**
-
```
norm_id=* request_method=GET url="*/include/makecvs.php*" url="*?Event=*" url IN ["*curl*", "*wget*", "*.py*", "*.sh*", "*chmod*", "*_GET*"]
```

VMware VSphere CVE-2021-21972 Exploitation

- **Trigger Condition:** The exploitation of VSphere Remote Code Execution vulnerability CVE-2021-21972 is detected.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** T1190 - Exploit Public-Facing Application
- **Minimum Log Source Requirement:** Firewall, Proxy Server
- **Query:**
-
```
norm_id=* request_method=POST url="*/ui/vropspluginui/rest/services/uploadova*"
```

VMware View Planner CVE-2021-21978 Exploitation

- **Trigger Condition:** The exploitation of the VMware View Planner vulnerability CVE-2021-21978 is detected. CVE-2021-21978 is a flaw due to proper input validation and lack of authorization leading to arbitrary file upload in Log Upload web applications.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** T1190 - Exploit Public-Facing Application
- **Minimum Log Source Requirement:** Firewall, Proxy Server
- **Query:**
-
  ```
  norm_id=* request_method=POST url="*logupload*" url="*logMetaData*" url="*wsgi_log_upload.py*"
  ```

Zoho ManageEngine ADSelfService Plus CVE-2021-40539 Exploitation

- **Trigger Condition:** The REST API authentication bypass vulnerability (CVE-2021-40539) in Zoho ManageEngine ADSelfService Plus (v6113 and prior) is detected. Administrators must have fetched logs from `\ManageEngine\ADSelfService Plus\logs` path for the detection to work.
- **ATT&CK Category:** Initial Access, Persistence
- **ATT&CK Tag:** T1190 - Exploit Public-Facing Application, T1505.003 - Web Shell
- **Minimum Log Source Requirement:** Web Server
- **Query:**
-
  ```
  url=* url IN ["*/help/admin-guide/Reports/ReportGenerate.jsp*", "*/RestAPI/LogonCustomization*", "*/RestAPI/Connection*"]
  ```

Possible Access to ADMIN Share

- **Trigger Condition:** Access to $ADMIN share that may help detect lateral movement attempts is detected. Since Windows Admin Share activity is so common, it provides adversaries with a powerful, discreet way to move laterally within an environment. Self-propagating ransomware and cryptocurrency miners, both rapidly emerging threats, rely on Windows Admin Shares. Suppose an adversary can obtain legitimate Windows credentials. The hidden shares (C$, ADMIN$, and IPC$) can be accessed remotely via server message block (SMB) or the Net utility to transfer files and execute code. Windows Admin Shares are often used in conjunction with behaviors relating to Remote File Copy (T1105)—because adversaries commonly use the technique to copy files remotely—and Network Share Discovery (T1135). It can also occur with New Service (T1050) and Service Execution (T1035) because tools like PsExec deploys their receiver executable to admin shares, scheduling a service to execute it. Legitimate administrative activities may generate false positives and will require whitelisting.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** T1021.002 - SMB/Windows Admin Shares

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

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

PsExec Tool Execution Detected

- **Trigger Condition:** PsExec service installation and execution events (service and Sysmon).
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** T1569 - System Services, T1569.002 - Service Execution
- **Minimum Log Source Requirement:** Windows
- **Query:**

-
  ```
  ((norm_id=WinServer service="PSEXESVC" event_id IN [7045, 7036]) OR (event_id=1 image="*\PSEXESVC.exe" user="SYSTEM")) -user IN EXCLUDED_USERS
  ```

Screensaver Activities Detected

- **Trigger Condition:** Adversaries modification of registry key containing the path to binary used as screensaver executable is detected to establish persistence.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** T1546 - Event Triggered Execution, T1546.002 - Screensaver
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

-
  ```
  norm_id=WindowsSysmon (event_id=12 or event_id=13 or event_id=14) (target_object="*\Control Panel\Desktop\SCRNSAVE.exe") (parent_command!="*explorer.exe" or image!="*rundll32.exe" or command!="*shell32.dll, Control_RunDLL desk.cpl, ScreenSaver, *") -user IN EXCLUDED_USERS
  ```

Suspect Svchost Activity Detected

- **Trigger Condition:** Scvhost activity is detected. It is abnormal for svchost.exe to spawn without any CLI arguments and is normally observed when a malicious process spawns the process and injects code into the process memory space.
- **ATT&CK Category:** Privilege Escalation, Defense Evasion
- **ATT&CK Tag:** T1055 - Process Injection
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

-
  ```
  norm_id=WindowsSysmon event_id=1 image="*\svchost.exe" parent_image=* -parent_image IN ["*\rpcnet.exe", "*\rpcnetp.exe", "*\svchost.exe", "*\Mrt.exe", "*\MsMpEng.exe"] command=* command="*svchost.exe" -user IN EXCLUDED_USERS
  ```

Time-Stomping of Users Directory Files Detected

- **Trigger Condition:** Time-stomping of user directory file is detected. Sysmon can only detect a change of CreationTime and not LastWriteTime and

LastAccessTime. Whitelisting legitimate noisy processes like browsers, Slack, or Teams are required to reduce false positives.

- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1070 - Indicator Removal on Host, T1070.006 - Timestomp
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**
-
  ```
  norm_id=WindowsSysmon event_id=2 path="C:\Users*" -source_image IN ["*iexplore.exe", "*cortana*", "*\StartMenuExperienceHost.exe", "C:\Windows\system32\cleanmgr.exe", "C:\Windows\Explorer.EXE", "*\LocalBridge.exe", "*\svchost.exe", "*\RuntimeBroker.exe", "*\msedge.exe", "*\SearchApp.exe", "C:\Windows\system32\ServerManager.exe", "*\ServiceHub.RoslynCodeAnalysisService32.exe"] -path="*\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations" -user IN EXCLUDED_USERS
  ```

Windows Defender Exclusion Set Detected

- **Trigger Condition:** Added Windows Defender exclusion in the registry where an entity bypasses antivirus scanning from Windows Defender.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1562 - Impair Defenses, T1562.001 - Disable or Modify Tools
- **Minimum Log Source Requirement:** Windows
- **Query:**
-
  ```
  norm_id=WinServer event_source="Microsoft-Windows-Windows Defender" event_id=5007 new_value="HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\*"
  ```

Suspicious Netsh DLL Persistence Detected

- **Trigger Condition:** Detects persistence via Netsh Helper.
- **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:** Window Sysmon
- **Query:**
-
  ```
  (norm_id=WindowsSysmon event_id=1 image="*\netsh.exe" command IN ["*add*", "*helper*"] -user IN EXCLUDED_USERS) OR (label=Create label="Process" "process" IN ["*\netsh.exe", "*\Netsh.exe"]  command="*add*" command="*helper*")
  ```

Suspicious Use of Procdump Detected

- **Trigger Condition:** Suspicious uses of the SysInternals ProcDump utility by using a command-line parameter combined with the *lsass.exe* process. It uses a command-line parameters “-ma” and “-accepteula” in a single step. This alert can detect if an attacker renames the *procdump.exe*.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** T1003 - OS Credential Dumping, T1003.001 - LSASS Memory
- **Minimum Log Source Requirement:** Windows Sysmon

- **Query:**

```
(norm_id=WindowsSysmon event_id=1 ((command IN ["* -ma *"] command IN ["* lsass*"]) OR command IN ["* -ma ls*"]) -user IN EXCLUDED_USERS) OR (label="Create" label="Process" command="* -ma *" command="* -accepteula *")
```

Usage of Procdump Detected

- **Trigger Condition:** Suspicious use of the SysInternals ProcDump utility tool is detected.
- **ATT&CK Category:** -
- **ATT&CK Tag:** -
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
label="Create" label="Process" "process" IN ["*\procdump.exe",  "*\procdump64.exe"] command="* -ma*" command="*.exe"
```

Conhost Spawning Suspicious Processes

- **Trigger Condition:** *conhost.exe* spawns other processes.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1202 - Indirect Command Execution
- **Minimum Log Source Requirement:** Windows
- **Query:**

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

Proxy Execution via Explorer

- **Trigger Condition:** *explorer.exe* is used in *cmd.exe* to proxy execution.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1202 - Indirect Command Execution
- **Minimum Log Source Requirement:** Windows
- **Query:**

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

Wlrmdr Lolbin Use as Launcher

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

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

Suspicious Process Execution via Pester Detected

- **Trigger Condition:** Detects code execution via *Pester.bat* (Pester - Powershell Modulte for testing).
- **ATT&CK Category:** Defense Evasion, Execution
- **ATT&CK Tag:** T1059.001 - PowerShell, T1216 - Signed Script Proxy Execution
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label="create" label="process"  event_source="Microsoft-Windows-Sysmon" ("process"="*
\powershell.exe" command="*Pester*Get-Help*") OR ("process"="C:\Windows\System32\cmd.
exe" command="*pester*;*" command IN ["*help*", "*?*"])
```

Root Certificate Installation Detected

- **Trigger Condition:** Adversaries may install a root certificate on a compromised system to avoid warnings when connecting to adversary-controlled web servers. This alert can detect the installation of a root certificate.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1553.004 - Install Root Certificate
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label="Create" label="Process" event_source="Microsoft-Windows-Sysmon" command="*root
*" ("process"="C:\Windows\System32\certutil.exe" command="*-addstore*") OR ("process"
="*\CertMgr.exe" command="*/add*") | norm on command <certificate:'\S+.cer'>
```

Suspicious process spawned by FTP

- **Trigger Condition:** *ftp.exe* is used to file transfer, but it can be abused by spawning a new process using *ftp.exe*. The alert detects; renamed *ftp.exe*, *ftp.exe* script execution, and child processes run by *ftp.exe*.
- **ATT&CK Category:** Execution, Defense Evasion
- **ATT&CK Tag:** T1059 - Command and Scripting Interpreter, T1202 - Indirect Command Execution
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label="create" label="process" event_source="Microsoft-Windows-Sysmon" (command="*-s:
*" ("process"="C:\Windows\System32\ftp.exe" OR file="*ftp.exe*")) OR (file="*ftp.exe*
" -"process"="C:\Windows\System32\ftp.exe") OR parent_process="C:\Windows\System32\ft
p.exe"
```

ChromeLoader IoC Domains Detected

- **Trigger Condition:** When any domains match with the list of known malicious domains used in the ChromeLoader Malware campaign.
- **ATT&CK Category:** Resource Development, Initial Access
- **ATT&CK Tag:** T1566 - Phishing, T1587.001 - Malware

- **Minimum Log Source Requirement:** Firewall, Proxy Server, IDS
- **Query:**

```
device_category IN ["Firewall", "ProxyServer", "IDS"] domain IN CHROMELOADER_DOMAINS
OR query IN CHROMELOADER_DOMAINS
```

ChromeLoader IoC Hashes Detected

- **Trigger Condition:** Hashes match with the list of known malicious hashes used in the ChromeLoader Malware campaign.
- **ATT&CK Category:** Resource Development
- **ATT&CK Tag:** T1587.001 - Malware
- **Minimum Log Source Requirement:** -
- **Query:**

```
hash IN CHROMELOADER_HASHES OR hash_sha1 IN CHROMELOADER_HASHES OR hash_sha256 IN CHR
OMELOADER_HASHES | rename hash as ioc, hash_sha1 as ioc, hash_sha256 as ioc
```

Chromeloader Cross-Process Injection to Load Extention

- **Trigger Condition:** Chromeloader uses process injection using PowerShell and loads the malicious extension in Chrome.
- **ATT&CK Category:** Execution, Persistence, Privilege Escalation
- **ATT&CK Tag:** T1055 - Process Injection, T1059.001 - PowerShell, T1176 - Browser Extensions
- **Minimum Log Source Requirement:** -
- **Query:**

```
label="Process" label=Create parent_process="*powershell" parent_command = "*-exe* by
p* -win* hid* -e* JAB*" command IN ["*--load-extension=*", "*Appdata\\local\\chrome*"
] "process" = "*chrome"
```

Proxy Execution via Explorer

- **Trigger Condition:** When Explorer is used to proxy execution. Explorer is a Microsoft Windows GUI shell used for task-based file management systems. Adversaries generally use Explorer to proxy the execution of other commands or processes, evading defense mechanisms.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1202 - Indirect Command Execution
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

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

Suspicious Root Certificate installation Detected

- **Trigger Condition:** Installation of a root certificate is detected. Adversaries may install a root certificate on a compromised system to avoid warnings when connecting to adversary-controlled web servers. However, sometimes Help Desk or IT may need to add a corporate Root CA on occasion manually. So they need to test if the GPO push doesn’t trigger a False Positive.

- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1553.004 - Install Root Certificate
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

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

Windows Logon Reminder Usage as Launcher

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

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

Suspicious File Transfer Using Replace

- **Trigger Condition:** Replace is used to transfer (copy or download files) files. *Replace.exe* is a Microsoft Windows executable that allows replacing existing or adding new files in a directory if used with the /a option. Adversaries use the replace process to silently download or copy files in the target system.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1105 - Ingress Tool Transfer
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="process" label=create "process"="*\replace.exe" command IN ["*/a*", "*-a*"]
```

Proxy Execution via Program Compatibility Wizard

- **Trigger Condition:** Pcwrun process is used to initiate a proxy execution. Pcwrun is a Microsoft Windows Operating System file used to invoke Program Compatibility Troubleshooter/Wizard. Adversaries generally use pcwrun to proxy the execution of other commands, processes, or executables in order to evade defense mechanisms. However, the specific focus needs to be on outlier events, for example unique counts, instead of commonly seen artifacts to prevent false positives.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1218 - Signed Binary Proxy Execution

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

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

Suspicious Driver Installation via PnPUtil

- **Trigger Condition:** Pnputil process is used to install or add drivers. PnPUtil is a Microsoft Windows process that lets an administrator perform actions on driver packages. Adversaries use pnputil to install or add malicious drivers. Anyone who uses pnputil.exe who is not a system administrator should be investigated, even when they have system change permissions.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** T1547 - Boot or Logon Autostart Execution, T1547.006 - Kernel Modules and Extensions
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="process" label=create "process"="*\pnputil.exe" command IN ["*-i*", "*/install*", "*-a*", "*/add-driver*", "*.inf*"]
```

Application Whitelisting Bypass via PresentationHost

- **Trigger Condition:** Presentationhost process is used to execute browser applications. Presesntationhost is a Microsoft Windows application that enables the hosting of WPF applications in compatible browsers (including Microsoft Internet Explorer 6 and later). Adversaries use presentationhost.exe to evade application whitelisting and execute malicious XAML Browser Application (XBAP) files.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1218 - Signed Binary Proxy Execution
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="process" label=create "process"="*\presentationhost.exe" command="*.xbap*"
```

Suspicious File Extraction via Expand Detected

- **Trigger Condition:** Expand process is used for file transfer (copy or download files). Expand is a Microsoft Windows binary file provided by Microsoft that can extract one or more compressed files and retrieve them from distribution disks. Adversaries use expand to silently download or copy files into the target system or location.
- **ATT&CK Category:** Defense Evasion, Command and Control
- **ATT&CK Tag:** T1105 - Ingress Tool Transfer, T1218 - Signed Binary Proxy Execution
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="process" label=create "process"="*\expand.exe" command IN ["*.cab*", "*/F:*", "*-F:*", "*C:\ProgramData\*", "*C:\Public\*", "*\AppData\Local\Temp\*", "*\AppData\Roaming\Temp\*"]
```

Shell spawn via HTML Help Detected

- **Trigger Condition:** *Hh (HTML Help)* spawns shell processes. *Hh.exe* is a Microsoft Windows executable program that allows developers to compile .chm file(s) with expanding tables of contents, shortcuts, keyword search, and pop-up topics. Adversaries use *Hh* as a target for overwriting and executing their malicious commands, spawning other processes.
- **ATT&CK Category:** Execution, Defense Evasion
- **ATT&CK Tag:** T1047 - Windows Management Instrumentation, T1218.001 - Compiled HTML File
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="process" label=create parent_process="*\hh.exe" "process" IN ["*\cmd.exe", "*\powershell.exe", "*\wscript.exe", "*\cscript.exe", "*\regsvr32.exe", "*\wmic.exe", "*\rundll32.exe"]
```

DLL Injection with Tracker Detected

- **Trigger Condition:** DLL injection with the tracker process is detected. Tracker.exe is a legitimate internal Windows binary file required to incrementally generate resources like building on a 64-bit OS using 32-bit MSBuild. Adversaries can use it to bypass application whitelisting solutions by proxy execution of an arbitrary DLL into another process.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1055.001 - Dynamic-link Library Injection
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="create" label="process" (("process"="*\tracker.exe" OR description="Tracker") command="* /d *" command="* /c *")
```

Powershell Code Execution via SyncAppvPublishingServer

- **Trigger Condition:** Arbitrary Powershell command is executed via SyncAppvPublishingServer. VBScript files, such as SyncAppvPublishingServer.vbs, are trusted scripts, often signed with certificates. Adversaries can use SyncAppvPublishingServer.vbs to proxy execute PowerShell code.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1216 - Signed Script Proxy Execution, T1218 - Signed Binary Proxy Execution
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label='create' label='process' command='*\SyncAppvPublishingServer.vbs*' command='*;*'
```

Malicious PE Execution by Microsoft Visual Studio Debugger

- **Trigger Condition:** Arbitrary Powershell command is executed via SyncAppvPublishingServer. VBScript files, such as SyncAppvPublishingServer.vbs, are trusted scripts, often signed with certificates. Adversaries can use SyncAppvPublishingServer.vbs to proxy execute PowerShell code.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1218 - Signed Binary Proxy Execution
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="Create" label="Process"(parent_process="*\vsjitdebugger.exe"  -(("process"="*\vsimmersiveactivatehelper*.exe" OR "process"="*\devenv.exe")))
```

Suspicious Atbroker Registry Change Detected

- **Trigger Condition:** Creation or modification of Assistive Technology (AT) registry value is detected. Atbroker is a Windows internal helper binary that provides accessibility tools like screen readers, speech input and text readers, people with disabilities use to accomplish tasks. Adversaries can modify the assistive technology registry value and include their malicious application to maintain persistence.
- **ATT&CK Category:** Persistence, Defense Evasion
- **ATT&CK Tag:** T1218 - Signed Binary Proxy Execution, T1547 - Boot or Logon Autostart Execution
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon label=Registry label=Set target_object IN ["*\Software\Microsoft\Windows NT\CurrentVersion\Accessibility\ATs*", "*\Software\Microsoft\Windows NT\CurrentVersion\Accessibility\Configuration*"]
```

DLL loaded Via Certoc Binary Detected

- **Trigger Condition:** DLL loading is detected using certoc binary. Certoc is Windows internal binary used to install certificates, but it also has a feature to load a DLL by LoadDll tag. Adversaries can use certoc binary to load their malicious DLL even when they don’t have the relevant access rights.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1218 - Signed Binary Proxy Execution
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="Process" label=Create command="*certoc.exe*" command IN ["* -LoadDll *", "* /LoadDll *"] command="*.dll*"
```

Suspicious Remote Binary Usage Detected

- **Trigger Condition:** remote.exe binary is used to bypass application whitelisting and execute or run a local or remote file. Remote.exe is a Windows binary server/client tool that allows users to run command-line programs on remote computers. Adversaries can use the remote.exe binary to spawn a new Powershell session, AWL bypass, and execute other commands.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1127 - Trusted Developer Utilities Proxy Execution
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

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

Suspicious File Execution Using wscript or cscript

- **Trigger Condition:** A file with extensions of .jse, .vbe, .js, or .vba is executed using wscript or cscript. Wscript and cscript are windows binaries that provide an environment in which users can execute scripts in various languages or start a script to run in a command-line environment. Adversaries can code malicious scripts in files with above mention extensions and execute them using wscript or cscript and bypass detection.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** T1059.005 - Visual Basic, T1059.007 - JavaScript
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

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

Suspicious ASP NET Compiler Execution Detected

- **Trigger Condition:** A file with the extension .jse, .vbe, .js, or .vba is executed using wscript or cscript. Wscript and cscript are Windows binaries that provide an environment in which users can execute scripts in various languages or start a script to run in a command-line environment. Adversaries can code malicious scripts in .jse, .vbe, .js, or .vba files and execute them using wscript or cscript and bypass detection.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1127 - Trusted Developer Utilities Proxy Execution
- **Minimum Log Source Requirement:** -
- **Query:**

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

Suspicious LoadAssembly PowerShell Diagnostic Script Execution

- **Trigger Condition:** Microsoft signed script is used to execute commands and bypass AppLocker. CL_LoadAssembly.ps1, a windows native diagnostic script, provides two functions (LoadAssemblyFromNS and LoadAssemblyFromPath) for loading .NET/C# assemblies (DLLs/EXEs). An attacker can bypass Constrained Language mode by invoking PowerShell version 2 (Note: this must be enabled) and bypass AppLocker by loading an assembly through CL_LoadAssembly.ps1.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1216 - Signed Script Proxy Execution
- **Minimum Log Source Requirement:** -
- **Query:**

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

Suspicious Invocation PowerShell Diagnostic Script Execution

- **Trigger Condition:** The execution of malicious payloads via SyncInvoke in CL_Invocation.ps1 module is detected. CL_Invocation is a PowerShell Diagnostic script, but an attacker can import it and then call SyncInvoke to launch a malicious executable.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1216 - Signed Script Proxy Execution
- **Minimum Log Source Requirement:** -
- **Query:**

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

Registry Configured RunOnce Task Execution

- **Trigger Condition:** The RunOnce task executes as configured in the registry. Runonce.exe is a Microsoft Windows Operating System component called the *Run Once Wrapper Utility* that allows the installation program to reboot after initial start up to enable the user to make further configurations. Adversaries use the runonce executable to evade defense mechanisms while running their programs/code through registry entries in the host machine.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1112 - Modify Registry
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="process" label=create "process"="*\runonce.exe" command="* /AlternateShellStartup*"
```

RunOnce Registry Key Configuration Change

- **Trigger Condition:** When the configuration of Run Once registry key is changed. Runonce.exe is a Microsoft Windows Operating System component called the *Run Once Wrapper Utility* that allows the installation program to reboot after initial start up to enable the user to make further configurations. Adversaries use/change the runonce registry key values to evade defense mechanisms while running their programs/code in the host machine.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1112 - Modify Registry
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label="process" label=create "process"="*\runonce.exe" command="* /AlternateShellStar
tup*"
```

Suspicious WSL Bash Execution

- **Trigger Condition:** When bash is used to execute the Linux command. Bash is a Unix shell and command language. Adversaries can use bash to execute a specified file or commands in the Windows subsystem for Linux and can be used as a defensive evasion mechanism. Executing programs using bash can trigger this alert, so alerts must be further analyzed to determine legitimate or illegitimate use.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1202 - Indirect Command Execution
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Create" label="Process" command="*bash* -c *"
```

WSL Execution Detected

- **Trigger Condition:** When Windows subsystem for Linux (WSL) binary is used to execute Linux commands. WSL is a compatibility layer that allows running Linux binaries in Windows. Adversaries can use the wsl binary to execute Windows and Linux binaries, execute arbitrary Linux commands as root without a password or download files.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1202 - Indirect Command Execution
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Create" label="Process" "process"="*\wsl.exe" command in ["* -e *", "*--exec *
"]
```

Supsicious Usage of Csharp or Roslyn Csharp Interactive Console

- **Trigger Condition:** When the use of csi and rcsi binary are detected. Csi.exe is a Microsoft signed binary that provides C# interactive capabilities. Rcsi.exe is a Microsoft signed binary that can execute C# code. Adversaries can use these binaries to execute their malicious C# code.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** T1072 - Software Deployment Tools
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

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

Suspicious Use of CSharp Interactive Console Detected

- **Trigger Condition:** The execution of the CSharp interactive console by using PowerShell is detected. Csi.exe is a Microsoft signed binary that provides C# interactive capabilities. PowerShell is a task automation and configuration management program from Microsoft. Adversaries can run CSharp interactive console from PowerShell and execute their malicious code.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1127 - Trusted Developer Utilities Proxy Execution
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label="Create" "process"="*\csi.exe" file="csi.exe" parent_process="*
\powershell.exe"
```

Suspicious File Download via Certreq

- **Trigger Condition:** When a file is downloaded using certreq binary. Certreq is a Windows binary used to manage and request a certificate from the certificate authority. Adversaries can use certreq to download payload from their C2 server.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** T1105 - Ingress Tool Transfer
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label="Create" "process"="*\certreq.exe" command="*certreq*" command
IN ["* -Post *"," /Post *"] command IN ["* -config *","* /config *"] command="* http*
" command="* C:\windows\win.ini *"
```

Process Dump via Rundll32 and Comsvcs

- **Trigger Condition:** When LSASS dump using Rundll32 with Comsvcs DLL is detected. Rundll32.exe is a Windows binary that loads and runs 32-bit dynamic-link libraries. comsvcs.dll is a DLL file used by COM+ Services created by Microsoft. Adversaries can use the binary and DLL to perform a dump of the LSASS process.
- **ATT&CK Category:** Defense Evasion, Credential Access

- **ATT&CK Tag:** T1003.001 - LSASS Memory, T1036 - Masquerading
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label="Process" label=Create "process"="*\rundll32.exe" command IN ["*comsvcs.dll*#24*", "*comsvcs.dll*MiniDump*" ] -user IN EXCLUDED_USERS
```

Registry Key Import Detected

- **Trigger Condition:** When registry key import is detected via regedit.exe. Regedit is a Windows binary to access and manipulate the Windows registry. This hierarchical database stores low-level settings for the Microsoft Windows operating system and applications that opt to use the registry. A registry key is an organizational unit in the Windows registry. Adversaries can use Regedit to import their malicious registry key to achieve persistence.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1112 - Modify Registry
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

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

Suspicious MachineGUID Query Detected

- **Trigger Condition:** When reg.exe is used to detect query machine GUID. Reg.exe is a Windows binary that performs operations on registry subkey information and values in registry entries. MachineGUID is a unique identifier for a machine. Adversaries can use this technique to get MachineGuid information. Also, ransomware abuses this technique to keep track of infected systems using a unique ID.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** T1082 - System Information Discovery
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

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

Process Injection Via Mavinject Detected

- **Trigger Condition:** When DLL is injected into a running process. Microsoft Application Virtualization Injector (Mavinject) is a Windows utility that can inject code into external processes as part of Microsoft Application Virtualization (App-V). Adversaries can use mavinject to inject malicious DLL to obtain arbitrary code execution.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1218.013 - Mavinject

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

```
label="Process" label="Create" "process"="*\mavinject.exe" command IN ["* /injectrunn
ing*", "* -injectrunning*", "*.dll*"]
```

Possible File Transfer Using Finger Detected

- **Trigger Condition:** When the execution of Finger.exe is detected. It is a simple Windows binary that displays user information on a specified remote computer running the Finger service or daemon. It can be abused as a data transfer tool and makeshift C2 channel. However, general administrative use can trigger false positives, but it is still unclear why they use finger.exe.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** T1105 - Ingress Tool Transfer
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

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

Suspicious Use of Findstr Detected

- **Trigger Condition:** When suspicious actions such as credential access, file download, or creation of alternate data stream using findstr are detected. Generally, it is used to search for strings in files or to filter command line output. Adversaries can exploit it for defense evasion. However, general administrative use of findstr can trigger false positives.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1218 - Signed Binary Proxy Execution
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="create" label="process" "process"="*\findstr.exe" command="*findstr*" ((comman
d="*/V*" command="*/L*") OR (command="*/S*" command="*/I*"))
```

Suspicious File Overwrite Using extrac32 Detected

- **Trigger Condition:** When suspicious actions such as credential access, file download, or creation of alternate data stream using findstr are detected. Generally, it is used to search for strings in files or to filter command line output. Adversaries can exploit it for defense evasion. However, general administrative use of findstr can trigger false positives.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1218 - Signed Binary Proxy Execution
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="create" label="process" "process"="*\findstr.exe" command="*findstr*" ((comman
d="*/V*" command="*/L*") OR (command="*/S*" command="*/I*"))
```

Suspicious Sysmon Driver Unload Detected

- **Trigger Condition:** When suspicious unload of SysmonDrv Filter Driver is detected. Fltmc.exe program is a system-supplied command line utility for mini-filter driver management operations. Adversaries can abuse its functionality to unload the filter driver, which can affect sysmon and stop from collecting the data.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1070 - Indicator Removal on Host, T1562 - Impair Defenses, T1562.002 - Disable Windows Event Logging
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="process" label="create" "process"="*\fltmc.exe" command="*unload*" command ="*
sys*"
```

Windows Packet Monitoring Tool Usage Detected

- **Trigger Condition:** When the execution of pktmon (Packet Monitor) is detected. Pktmon.exe is an in-box, cross-component network diagnostics tool of Microsoft Windows used for packet capture, packet drop detection, packet filtering, counting, and visibility within the networking stack. Adversaries generally abuse pktmon.exe to sniff network traffic and capture information about an environment, including authentication material sent over an insecure, unencrypted protocol, revealing configuration details necessary for subsequent Lateral Movement and/or Defense Evasion activities.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** T1040 - Network Sniffing
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

```
label="process" label=create ("process"="*\pktmon.exe" OR file="pktmon.exe")
```

Suspicious Execution via IE per User Utility

- **Trigger Condition:** When ie4uinit is executed from unusual file directories. Ie4uinit.exe (Internet Explorer (for) Each User Initialization) file is a software component of Internet Explorer by Microsoft Corporation. Adversaries generally abuse ie4uinit.exe to overwrite malicious programs on it and spread them via the internet to execute them on target machines as legitimate processes.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1218 - Signed Binary Proxy Execution
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

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

Proxy Execution via xWizard

- **Trigger Condition:** When the execution of the xWizard tool with runwizard and CLSID arguments are utilized to achieve proxy execution. xWizard is Windows internal binary used to run the Windows component object model (COM). COM is operated to enable inter-process communication. Class ID (CLSID) is a unique number representing a single application component in windows. Adversaries can bypass the defense mechanism by proxying the execution of malicious content via xWizard.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1218 - System Binary Proxy Execution
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*\xwizard.exe" | process regex("(?P<new_comma
nd>{\w{8}-\w{4}-\w{4}-\w{4}-\w{12}})",command) | filter new_command=*
```

Suspicious MSHTA Process Pattern

- **Trigger Condition:** When suspicious *mshta.exe* process patterns, such as binary run from a non-default path, mshta.exe binary masquerading as different binary, and execution of HTML application (HTA) masquerading as non-HTA file are detected. Mshta.exe is a utility that executes HTA files. HTAs are standalone applications based on HTML and VBScript that can access local system resources, run scripts and display dynamic content. Adversaries may abuse mshta.exe to evade defense by proxy, executing malicious files and Javascript or VBScript through a trusted Windows utility.
- **ATT&CK Category:** Defense Evasion, Execution
- **ATT&CK Tag:** Mshta, Native API
- **ATT&CK ID:** T1218.005, T1106
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create "process"="*\mshta.exe"
((parent_process IN ["*\cmd.exe","*\powershell.exe"] OR command IN ["*\AppData\Local*
", "*C:\Windows\Temp*", "*C:\Users\Public*"]) OR (-"process" IN ["C:\Windows\System32
*", "C:\Windows\SysWOW64*" ]) OR  (-command IN ["*mshta.exe","*mshta"] -command IN ["
*.htm*", "*.hta*" ]))
```

COM Object Execution via Shell Extension CLSID Verification Host

- **Trigger Condition:** When verclsid.exe is used to run COM object via GUID. Verclsid.exe (Verify COM Shell Extension CLSID) is a Microsoft Windows Native Shell Extension CLSID (Class ID) verification host responsible for verifying each shell extension before Windows Explorer or the Windows Shell uses them. Adversaries may abuse verclsid.exe to execute malicious payloads-COM Scriptlets, by running verclsid.exe and referencing files by Class ID (CLSID), a unique identification number used to identify COM objects.
- **ATT&CK Category:** -

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

```
label="process" label="create" "process"="*\verclsid.exe" command="*/C*" command="*/S*"
```

Suspicious Setup Information File Invoked via DefaultInstall

- **Trigger Condition:** When InfDefaultInstall.exe is used to install an INF file. InfDefaultInstall.exe is a Microsoft Windows native tool invoked when an INF (Setup Information) file is selected to install. Adversaries use InfDefaultInstall to install on the target system through maliciously crafted INF files.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1562.001 - Disable or Modify Tools
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

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

Creation of Alternate Data Stream

- **Trigger Condition:** When an alternate data stream is created. Alternate Data Stream (ADS) is the ability of an NTFS file system to store different streams of data, in addition to the default stream, which is used for a file. Attackers can leverage a little-known compatibility feature to hide hacking tools, keyloggers, and other malware on a compromised system and subsequently execute them undetected. Also, it can be used for data exfiltration. The alert requires the ADS_FILE_EXTENSIONS list to work.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1564.004 - NTFS File Attributes
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
(label="create" label="process" command IN ADS_FILE_EXTENSIONS ((command="*type *" command="* > *") OR (command="*makecab *" command="*.cab*") OR (command="*reg *" command="* export *") OR (command ="*diantz.exe*" command="*.cab*") OR (command="*regedit *" command="* /E *") OR (command="*print*" command IN ["*/D:*", "*/d:*"]) OR (command="*expand*") OR (command="*extrac32*" command="*.cab*") OR (command="*curl*" command IN ["*--output*", "*-o*"]) OR (command="*certutil*" command="*-urlcache*") OR  (command="*esentutl*" command="*/y*" command="*/d*") OR (command="*esentutl *" command="* /y*" command="* /d *" command="* /o *"))) OR (label="create" label="file" file in ADS_FILE_EXTENSIONS)
```

Alternate Data Stream Created using Findstr

- **Trigger Condition:** When findstr is used to create an alternate data stream. Findstr is generally used to search for strings in files or to filter command line output. Adversaries can exploit it to create an alternate data stream for defense evasion. For this alert to work, the ADS_FILE_EXTENSIONS list is required.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1564.004 - NTFS File Attributes
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
[label="create" label="process" "process"="*\findstr.exe" command="*findstr*" ((command="*/V*" command="*/L*") OR (command="*/S*" command="*/I*"))] as s1 followed by [label="Create" label="File" file in ADS_FILE_EXTENSIONS] as s2 on s1.process_id=s2.process_id | rename s1.process as "process", s1.log_ts as log_ts,s1.command as command,s1.host as host, s1.user as user, s1.parent_process as parent_process
```

Suspicious Download Using Diantz

- **Trigger Condition:** When a remote file is downloaded using diantz.exe and stored by compressing it into a .cab file on a local machine. It performs a similar function as makecab.exe, which compresses a file into a smaller file with a .cab file extension. Adversaries can use diantz.exe for ingress tool transfer to evade the defenses and establish a c2 connection.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** T1105 - Ingress Tool Transfer
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

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

Ngrok RDP Tunnel Detected

- **Trigger Condition:** When it detects the execution of Ngrok utility for tunneling RDP connection. Threat actors often use Ngrok to expose internal services to the internet, like making RDP publicly accessible. 16777216 artifact gets logged when an incoming RDP connection is established via ngrok.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** T1572 - Protocol Tunneling
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
norm_id=WinServer ((event_source IN ["Microsoft-Windows-TerminalServices-LocalSessionManager", "Microsoft-Windows-TerminalServices-RemoteConnectionManager"]) OR (channel=Security event_id=4779)) (source_address="::%16777216" OR eventxml.address="::%16777216") | rename eventxml.address as source_address
```

Ngrok Execution

- **Trigger Condition:** When it detects the execution of the Ngrok utility used for port forwarding and protocol tunneling. Threat actors often use Ngrok to expose internal services to the internet, like making RDP publicly accessible.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** T1572 - Protocol Tunneling
- **Minimum Log Source Requirement:** Windows, Windows Sysmon
- **Query:**

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

AD Privesc CVE-2022-26923 Exploitation

- **Trigger Condition:** When it detects the creation of a computer account spoofing a domain controller name, it successfully requests a machine certificate template from the CA server. This indicates the privilege escalation vulnerability (CVE-2022-26923) exploitation in the Active Directory (AD) patched on May 10, 2022. For this alert to work, you need the WINDOWS_DC list containing all the FQDNs of the domain controllers operating in your domain.
- **ATT&CK Category:** Privilege Escalation
- **ATT&CK Tag:** T1068 - Exploitation for Privilege Escalation
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
[ norm_id=WinServer label=Computer label=Account label=Create dns_host IN WINDOWS_DC ] as s1 followed by [ norm_id=WinServer label=Certificate label=Request label=Approve attributes="CertificateTemplate:Machine" | norm on requester \<requester_account:'\S+'> ] as s2 within 1 hour on s1.computer=s2.requester_account | rename s1.log_ts as account_creation_ts, s1.computer as computer, s1.user as user, s1.service as service, s1.dns_host as dns_host, s2.subject as certificate_subject | chart count() by account_creation_ts, computer, user, service, dns_host, certificate_subject
```

Possible Ransomware Deletion Volume Shadow Copies Detected

- **Trigger Condition:** When LogPoint detects commands that delete all local volume shadow copies as used by different Ransomware families.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** T1490 - Inhibit System Recovery
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 command IN ["*vssadmin* delete shadows*", "*wmic* SHADOWCOPY*DELETE*"] -user IN EXCLUDED_USERS
```

Windows Defender Uninstall via PowerShell

- **Trigger Condition:** When PowerShell is used to uninstall Windows Defender. PowerShell is a Microsoft task automation and configuration management program consisting of a command-line shell with its scripting language. Microsoft Defender Antivirus is an anti-malware component of Microsoft Windows. Adversaries can use this technique to avoid the detection of their malware.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1562 - Impair Defenses
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process"="*\powershell.exe" command="*Uninstall-Windows
Feature*Name*Windows-Defender*"
```

Hijacked Binary Execution via Settings Synchronizer

- **Trigger Condition:** When SettingSyncHost is used to run hijacked binaries. SettingSyncHost is a Microsoft Windows host process that synchronizes system settings with other devices, including Internet Explorer, a mail application, OneDrive, Xbox and other application settings. Adversaries can exploit SettingSyncHost to run hijacked binaries and other specified files.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1574.008 - Path Interception by Search Order Hijacking
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label="create" -"process" IN ["C:\Windows\System32\*", "C:\Windows\Sy
sWOW64\*"] parent_command IN ["*cmd.exe /c*", "*cmd /c*"] parent_command="*RoamDiag.c
md*" parent_command="*-outputpath*"
```

Suspicious Execution of Dump64

- **Trigger Condition:** When suspicious use of dump64.exe is detected. dump64.exe is a memory dump tool bundled with Microsoft Visual Studio. Adversaries can leverage it to create a memory dump and parse it offline to retrieve credentials. Adversaries can bypass Microsoft Defender by renaming a tool to dump64.exe and placing it in a Visual Studio folder, for example, procdump.exe. It can trigger false positives if dump64.exe is executed from any folder other than excluded one, even for a legitimate purpose.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** T1003.001 - LSASS Memory
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label="create" "process"="*\dump64.exe" (-("process"="*\Installer\Fee
dback\dump64.exe*") OR command IN ["* -ma *", "*accpeteula*"])
```

Code Compilation via Visual Basic Command Line Compiler

- **Trigger Condition:** When a successful compilation of code using Visual Basic Command Line Compiler is detected. vbc.exe is Microsoft's Visual Basic compiler used to compile programs within the Visual Studio integrated development environment (IDE). Adversaries can leverage it to collect malicious code on the system to bypass defensive countermeasures. The legitimate use of this tool can trigger false positives, but it is barely used in enterprise environments, so the detection of service is suspicious.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1027.004 - Compile After Delivery
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

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

File Downloaded from Suspicious URL Using GfxDownloadWrapper

- **Trigger Condition:** When downloading files from suspicious (non-standard) URLs using GfxDownloadWrapper.exe is detected. Intel Graphics Executable Download Wrapper (GfxDownloadWrapper) is an application file that allows you to update your graphics card module. It downloads JSON files from *https://gameplayapi.intel.com*. Adversaries can leverage its functionality to download files from other non-standard URLs.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** T1105 - Ingress Tool Transfer
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Create" label="Process" "process"="*\GfxDownloadWrapper.exe"  - command="*game
playapi.intel.com*"  - parent_process="*\GfxDownloadWrapper.exe"
```

Suspicious CLR Logs File Creation

- **Trigger Condition:** When .NET code is executed via applications, such as mshta, cscript, wscript, regsvr32 and wmic. .NET is a developer platform with tools and libraries for building applications, including web, mobile, desktop, games, IoT, cloud, and microservices. Common Language Runtime in a .NET environment runs code and provides services to make the development process more manageable. The binaries included in the query are Windows internal binary which adversaries can use to execute their malicious scripts.
- **ATT&CK Category:** Privilege Escalation
- **ATT&CK Tag:** T1055 - Process Injection
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label=File label=Create label=Overwrite path="*\AppData\Local\Microsoft\CLR*\UsageLog
s\*" file IN ["mshta*","cscript*","wscript*","regsvr32*","wmic*"]
```

CLR DLL Loaded via Scripting Application

- **Trigger Condition:** When Common Language Runtime (CLR) DLL is loaded via scripting applications. mshta.exe, wscript.exe and cscript.exe are Windows internal binary. Common Language Runtime works in the .NET environment, which runs the code and provides services that make the development process more manageable. Adversaries can use this technique to execute malicious scripts.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1218.005 - Mshta
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label=image label=load source_image IN ["*\wscript.exe","*\cscript.exe","*\mshta.exe"]  image IN ["*\clr.dll","*\mscoree.dll","*mscorlib.dll"]
```

Obfuscation Script Usage via MSHTA to Execute Vbscript

- **Trigger Condition:** When execution of invoke-obfuscation PowerShell script with mshta to execute vbscript is detected. mshta.exe file is a software component of Windows Internet Explorer that runs HTML application(HTA) files. Invoke Obfuscation is a PowerShell command and script obfuscation framework. VBScript is an Active Scripting language developed by Microsoft modeled on Visual Basic. Adversaries can use this technique to bypass defensive mechanisms.
- **ATT&CK Category:** Defense Evasion, Execution
- **ATT&CK Tag:** T1027 - Obfuscated Files or Information, T1059.001 - PowerShell
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create command=* |  process regex("(?P<new_command>(?i).*(set).*(&&).*(mshta).*(vbscript:createobject).*(\.run).*\(window\.close\).*)",command) | filter new_command=*
```

Microsoft Defender Logging Disabled

- **Trigger Condition:** When Windows Defender Registry key is modified to disable Windows Defender’s logging. Windows Defender is an anti-malware component of Microsoft Windows. Adversaries use this technique to disable logs generated from Windows Defender and avoid detection.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1562 - Impair Defenses
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label=Registry label=Value label=Set target_object="*\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels\Microsoft-Windows-Windows Defender/Operational\Enabled" detail="DWORD (0x00000000)"
```

UAC Bypass via CMLUA or CMSTPLUA

- **Trigger Condition:** When user CMLUA OR CMSTPLUA DLL is loaded to perform user account control (UAC) bypass.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1562 - Impair Defenses
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label=Image label=Load image IN ["*\cmlua.dll","*\cmstplua.dll","*\cmluautil.dll"] -"process" IN ["*\cmstp.exe","*\cmmgr32.exe"] -source_image IN ["*\windows\*","*\program files\*"]
```

High Number of Service Stop or Task Kill in Short Span

- **Trigger Condition:** When suspicious mshta.exe process patterns like binary run from a non-default path, execution of mshta.exe binary masquerading as different binary and execution of HTML application (HTA) masquerading as non-HTA file are detected. mshta.exe is a utility that executes HTA files. HTAs are standalone applications that run using the same models and technologies as Internet Explorer but outside the browser. Adversaries may abuse mshta.exe to evade defense by proxy, executing malicious files and Javascript/VBScript through a trusted Windows utility.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** T1489 - Service Stop
- **Minimum Log Source Requirement:** Windows
- **Query:**

```
(label="process" label=create "process"="*\taskkill.exe" (command= "*f *" command="*im *") OR command="*IM *") OR (label="process" label=create ("process" IN ["*\sc.exe", "*\net.exe", "*\net1.exe"] command="*stop*") OR ("process"="*\sc.exe" command="*delete*") -user IN EXCLUDED_USERS) | chart count() as occurrence by user,host,domain,"process",parent_process  | search occurrence > 8
```

LSA Protected Process Light Disabled

- **Trigger Condition:** When modification of the registry value of Protection Process Light (PPL) to disable, it is detected. Protected Process can be accessed by executables that are digitally signed with a unique Windows Media, with administrator privilege. Protected Process Light is an extension of a protected process where a process can be assigned a different level of protection. Adversaries can use this technique to access the LSASS process and dump it to retrieve credentials.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1112 - Modify Registry
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label=Registry label=Set label=Value target_object="*\System\CurrentControlSet\Control\Lsa\RunAsPPL" detail="DWORD (0x00000000)"
```

Suspicious Invocation of Microsoft Workflow Compiler

- **Trigger Condition:** When the use of Microsoft Workflow Compiler is detected. Microsoft Workflow Compiler is a utility included by default in the .NET framework, capable of compiling and executing arbitrary, unsigned C# or VB.net code. Adversaries can leverage it for the proxy execution of executables to evade detection. The use of MWC in an enterprise environment is highly unlikely. However, legitimate use can trigger false positives.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1127 - Trusted Developer Utilities Proxy Execution
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label="create" ("process"="*\Microsoft.Workflow.Compiler.exe" OR (file="Microsoft.Workflow.Compiler.exe" command="*.xml*"))
```

Process Dump via Sqldumper Detected

- **Trigger Condition:** When a process dump via Sqldumper.exe is detected. The Sqldumper.exe is a debugging utility, included with Microsoft SQL Server, which generates memory dumps of SQL Server and of related processes for debugging purposes. Adversaries can leverage its functionality to dump processes like LSASS. Legitimate MSSQL Server actions can trigger false positives.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** T1003 - OS Credential Dumping, T1003.001 - LSASS Memory
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label="create" "process"="*\sqldumper.exe" command IN ["*0x0110*", "*0x01100:40*"]
```

Suspicious Usage of SQLToolsPS Detected

- **Trigger Condition:** When the proxy execution of PowerShell code through the SQLToolsPS.exe is detected. SQLToolsPS.exe is a utility shipped along with Microsoft SQL Server Management Studio that loads SQL Server cmdlts. Adversaries can leverage its functionality to execute malicious powershell codes and bypass the detection methods. Direct execution of PowerShell codes via SQLToolsPS.exe are uncommon. However, the child process sqltoolsps.exe spawned by smss.exe is a legitimate action.
- **ATT&CK Category:** Execution, Defense Evasion
- **ATT&CK Tag:** T1059.001 - PowerShell, T1127 - Trusted Developer Utilities Proxy Execution
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label="create" (("process"="*\sqltoolsps.exe" OR parent_process="*\sqltoolsps.exe") OR (file="\sqltoolsps.exe"  -(parent_process="*\smss.exe")))
```

Proxy Execution of Malicious Payload via Pubprn

- **Trigger Condition:** When proxy execution of malicious payloads via PubPrn.bs is detected. PubPrn.vbs is a signed Visual Basic script that publishes a printer to Active Directory Domain Services. Adversaries can abuse PubPrn to execute malicious payloads hosted on remote sites.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1216.001 - PubPrn
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label="create" command="*\pubprn.vbs*" command="*script:*"
```

File Download via IMEWDBLD

- **Trigger Condition:** When a network connection is detected via the IMEWDBLD.exe binary. IMEWDBLD.EXE is a part of Microsoft Input Method Editor (IME). IME is a software component that enables a user to enter text in a language that can’t easily be typed using a standard keyboard. Adversaries can use this technique to download remote system payload.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** T1105 - Ingress Tool Transfer
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label=Connection label=Network label=Detect "process"="*\IMEWDBLD.exe" is_initiated=t
rue
```

Memory Dump via Adplus

- **Trigger Condition:** When LSASS process dump via adplus.exe is detected. Local Security Authority Server Service (LSASS) is a process in Microsoft Windows operating systems that is responsible for enforcing the security policy on the system and handles authentication, password change and tokens. ADPlus is a console-based Visual Basic script included with Microsoft Debugging Tools for Windows installation. Adversaries may attempt to access credentials stored in the process memory of the LSASS.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** T1003.001 - LSASS Memory
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

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

TTDInject Usage Detected

- **Trigger Condition:** When the use of ttdinject binary is detected. Ttdinject is a binary that is a part of the Time Travel Debugging utility, which is used in Windows 10 v1809. Time Travel Debugging is a tool that captures a process trace as it executes and allows to replay it later. Adversaries can use this technique to proxy execute malicious payloads.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1127 - Trusted Developer Utilities Proxy Execution
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

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

Remote Thread Created via Ttdinject

- **Trigger Condition:** When a remote thread is created by ttdinject binary. Ttdinject is a binary that is a part of the Time Travel Debugging utility, which is used in Windows 10 v1809. Time Travel Debugging is a tool that captures a process trace as it executes and allows to replay it later. Adversaries can use this technique to proxy execute malicious payloads.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1127 - Trusted Developer Utilities Proxy Execution
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

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

Proxy Download via OneDriveStandaloneUpdater

- **Trigger Condition:** When OneDriveStandaloneUpdater registry value is modified. OneDriveStandaloneUpdater.exe is a binary that belongs to the Standalone Updater process and comes with Microsoft OneDrive. Adversaries can use this technique for transferring tools or other files to the victim system from a URL that is set in the OneDriveStandaloneUpdater registry. Registry auditing must be enabled and permission must be allowed for auditing the OneDriveStandaloneUpdater registry.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** T1105 - Ingress Tool Transfer
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label=registry label=value label=set target_object="*\SOFTWARE\Microsoft\OneDrive\Upd
ateOfficeConfig\UpdateRingSettingURLFromOC*"
```

Suspicious WMIC ActiveScriptEventConsumer Created

- **Trigger Condition:** When WMIC is executed to create an event consumer. ActiveScriptEventConsumer is a class that runs a predefined script in an arbitrary scripting language when an event is delivered to it. Adversaries may establish persistence and elevate privileges by executing malicious content triggered by a Windows Management Instrumentation (WMI) event subscription.

- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** T1546.003 - Windows Management Instrumentation Event Subscription
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create command="*ActiveScriptEventConsumer*" command="* CREATE
*"
```

Remote Connection Established via Msbuild

- **Trigger Condition:** When a network connection is initiated via MSBuild while building an application is detected. Microsoft Build (MSBuild) Engine is a platform for building applications. Adversaries can use this technique to build their payload and establish a network connection to their controlled server.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1127.001 - MSBuild
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=windowssysmon image="*\msbuild.exe" event_id=3 destination_port IN ["80","443
"] is_initiated=true
```

Executables Started in Suspicious Folder

- **Trigger Condition:** When the execution of binaries from a suspicious folder is detected. Paths mentioned in lists are not Windows default paths from where native and internal binaries are executed. Adversaries may attempt to masquerade their payload as legitimate binaries and execute from non-default paths to avoid detection. Legitimate binaries executed from those paths can trigger an alert, so include those binaries in the excluded process list.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1036 - Masquerading
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label="process" label=create "process" IN SUSPICIOUS_FOLDER_EXE_EXECUTION
-"process" IN ["*SpeechUXWiz.exe","*SystemSettings.exe","*TrustedInstaller.exe","*Pri
ntDialog.exe",
"*MpSigStub.exe","*LMS.exe","*mpam-*.exe"]
```

Windows RDP Port Modified

- **Trigger Condition:** When remote desktop protocol (RDP) for Windows protocol is modified. RDP is a protocol that allows users to have GUI access to a remote desktop. Adversaries can modify the RDP port to evade the defense mechanism used to detect connections in the default RDP port.

- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** T1021.001 - Remote Desktop Protocol
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label=Registry label=Value label=Set target_object="*\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\PortNumber"
```

Binary Creation in System Folder Detected

- **Trigger Condition:** When a binary or DLL is dropped in the Windows root folder by a system process. System folders are used by the operating system to store files necessary for proper function. A system folder is a primary location for DLL files. Adversaries may copy files between internal victim systems to support lateral movement using inherent file-sharing protocols, such as file sharing over SMB/Windows Admin Shares to connected network shares or with authenticated connections via Remote Desktop Protocol.
- **ATT&CK Category:** Lateral Movement
- **ATT&CK Tag:** T1570 - Lateral Tool Transfer
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label=File label=Create label=Overwrite "process"=system path IN ["C:\windows\*"]  file IN ["*.exe", "*.dll"]
```

Curl Silent Mode Execution Detected

- **Trigger Condition:** When curl is run in silent mode. Client URL (curl) is a command line tool that is used to transfer data to and from a server. Adversaries can use this technique to prevent showing file transfer progress and redirect output to a file.
- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** T1105 - Ingress Tool Transfer
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create command="*curl*" ((command="*-s*" command="*-o*") OR command="*-s*")
```

High Volume of File Modification or Deletion in Short Span

- **Trigger Condition:** When 30 file modifications or deletions are detected within a single minute. A large number of file modifications and deletions is an indicator of ransomware. Based on requirements and the number of detected false positives, a user can modify the number of events needed or the time frame. To generate logs, enable the auditing policy of the relevant folders. When a user/software modifies a large number of files this can result in a false positive. To reduce the number of false positives events exclude the process in the query.

- **ATT&CK Category:** Impact
- **ATT&CK Tag:** T1565 - Data Manipulation
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
[30 label=File label=Object label=Storage access IN ["Delete*","writedata*"] -"process" IN ["*\tiworker.exe","*\poqexec.exe","*\msiexec.exe"] having same host,domain,user,"process" within 1 minutes]
```

Non-Existent User Login Attempt Detected

- **Trigger Condition:** When eight non-existent user login attempts on SSH service are detected within a minute. Secure Shell (SSH) is a protocol that provides a secure way to access a computer over a network. Adversaries can perform username brute force to find a valid username. Based on the requirement and false positive, the user can modify the number of invalid login attempts and time frame.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** T1110 - Brute Force
- **Minimum Log Source Requirement:** Unix
- **Query:**

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

Execution of Temporary Files Via Office Application

- **Trigger Condition:** When Office applications creates a child process that executes a file with .tmp extension. Adversaries use this technique to avoid detection by using the legit application to run a payload that is masquerading as a temporary file.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1036 - Masquerading
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

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

Execution of Temporary Files Via Office Application

- **Trigger Condition:** When Office applications creates a child process that executes a file with .tmp extension. Adversaries use this technique to avoid detection by using the legit application to run a payload that is masquerading as a temporary file.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1036 - Masquerading
- **Minimum Log Source Requirement:** Windows Sysmon, Windows

- **Query:**

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

Malicious Image Loaded Via Excel

- **Trigger Condition:** When an unsigned image is loaded via Excel. An XLL file is an add-in used by Microsoft Excel. It contains extra functions, templates, or other tools that enhance the capabilities of Excel. Examples of add-ins include custom chart generators and template managers. Adversaries can use this technique to load their malicious unsigned add-ins to execute their payload or download malware from a remote server.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** T1137 - Office Application Startup, T1137.001 - Office Template Macros
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
label=Image label=Load "process"="*\excel.exe" file IN ["*.xlam ","*.xla","*.xll"]  is_sign=false
```

Malicious Chrome Extension Detected

- **Trigger Condition:** When malicious Chrome extension IDs are detected by Osquery. This analytic relies on chrome_extensions table and requires analysts to keep an up-to-date list of malicious chrome extension IDs.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** T1176 - Browser Extensions
- **Minimum Log Source Requirement:** -
- **Query:**

```
event_source=OSQuery event_type=chrome_extension* columns_identifier IN MALICIOUS_CHROME_EXTENSIONS
```

Chrome Extension Installed Outside of the Webstore

- **Trigger Condition:** When malicious chrome extensions are installed from outside the official Chrome webstore. Adversaries can manually install the browser extension via their batch, PowerShell or VBS scripts. Analysts need to make sure they place the correct event types in the query.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** T1176 - Browser Extensions
- **Minimum Log Source Requirement:** -
- **Query:**

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

Chrome Extension Installed with DevTools Permission

- **Trigger Condition:** When OSQuery detects the chrome extension installed with devtools permission. Analyst must check for unusual extensions installed with this permission and also check if the extensions were installed from the webstore.
- **ATT&CK Category:** Persistence
- **ATT&CK Tag:** T1176 - Browser Extensions
- **Minimum Log Source Requirement:** -
- **Query:**

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

Defender SpyNet Reporting Disabled

- **Trigger Condition:** When the SpyNet reporting feature is disabled via registry value modification. SpyNet reporting is a feature of windows defender antivirus that sends information about potential threats and suspicious activity to Microsoft. The submitted file is analyzed to improve the software's threat detection and response capabilities. Adversaries use this technique to prevent their malware from being sent to Microsoft.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1562.001 - Disable or Modify Tools
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=13 target_object="*\SOFTWARE\Microsoft\Windows Defende
r\SpyNet\SpyNetReporting" detail IN ["0","DWORD (0x00000000)"]  event_type=SetValue
```

Suspicious WMIC Process Creation

- **Trigger Condition:** When WMIC executes "Process Call Create," suspicious calls to processes such as, rundll32, regsrv32, mshta. The WMI command-line (WMIC) utility provides a command-line interface for Windows Management Instrumentation (WMI). WMI is a Microsoft technology that provides a common framework for managing and monitoring Windows-based systems. Adversaries can use this technique to proxy execute their malicious files and payloads via wmic.exe.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** T1047 - Windows Management Instrumentation
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create  command="process" command=call command=create
command IN ["*rundll32*","*bitsadmin*","*regsvr32*","*cmd.exe /c *","*cmd.exe /k *","
*cmd.exe /r *","*cmd /c *","*cmd /k *",
"*cmd /r *", "*powershell*","*pwsh*","*certutil*","*cscript*","*wscript*", "*mshta*",
"*\Users\Public\*", "*\Windows\Temp\*", "*\AppData\Local\*","*%temp%*","*%tmp%*","*%P
rogramData%*","*%appdata%*","*%comspec%*","*%Localappdata%"]
```

Browser Credential Files Accessed

- **Trigger Condition:** When access to a browser (Chrome, Edge & Firefox) using stored credential is detected. When a user saves any credentials in the browser, those credentials are stored in files that are included in the query. Adversaries can access those files in an attempt to retrieve the stored credentials.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1202 - Indirect Command Execution
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label=File label=Access ((path IN ["*\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies*","*\Appdata\Local\Chrome\User Data\Default\Login Data*","*\AppData\Local\Google\Chrome\User Data\Local State*"] object_name IN ["*\Appdata\Local\Microsoft\Windows\WebCache\WebCacheV01.dat","*\cookies.sqlite"])
OR object_name IN ["*\Microsoft\Edge\User Data\Default\Web Data", "*Firefox*release\logins.json","*firefox*release\key3.db","*firefox*release\key4.db"])
-"process" IN ["*\firefox.exe", "*\chrome.exe","C:\Program Files\*","C:\Program Files (x86)\*","C:\WINDOWS\system32\*","*\MsMpEng.exe","*\MpCopyAccelerator.exe","*\thor64.exe","*\thor.exe"] -parent_process IN ["C:\Windows\System32\msiexec.exe"] -("process"=system parent_process=idle) "access"="ReadData*"
```

Windows Defender Antivirus Definitions Removal Detected

- **Trigger Condition:** When Microsoft Defender Antivirus signature definitions are removed from the system. Microsoft Defender Antivirus (formerly Windows Defender) offers protection against all threats on Windows devices. The Malware Protection Command Line Utility (MpCmdRun) is a Microsoft Windows internal command-line tool dedicated to automating and managing Microsoft Defender Antivirus operations on Windows devices. Adversaries leverage this method to remove Antivirus definitions and ultimately avoid detection.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1562.001 - Disable or Modify Tools
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create "process"="*\MpCmdRun.exe" command="*RemoveDefinitions*"
```

Exchange ProxyShell Pattern Detected

- **Trigger Condition:** When a URL pattern associated with ProxyShell exploitation attempts (both successful and failure) against Exchange servers is detected. ProxyShell is an attack chain that exploits three known vulnerabilities in Microsoft Exchange: CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207. Adversaries may exploit these vulnerabilities to perform remote code execution.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** T1190 - Exploit Public-Facing Application
- **Minimum Log Source Requirement:** Webserver
- **Query:**

```
norm_id=* ((url="*/autodiscover.json*" url IN ["*/powershell*", "*/mapi/nspi*", "*/EW
S*", "*X-Rps-CAT*"]) OR url IN ["*autodiscover.json?@*", "*autodiscover.json%3f@*", "
*%3f@foo.com*", "*Email=autodiscover/autodiscover.json*", "*json?@foo.com*"])
```

Successful Exchange ProxyShell Attack

- **Trigger Condition:** When a URL pattern and status code associated with a successful ProxyShell exploitation attack against Exchange servers are detected. ProxyShell is an attack chain that exploits three known vulnerabilities in Microsoft Exchange: CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207. Adversaries may exploit these vulnerabilities to perform remote code execution.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** T1190 - Exploit Public-Facing Application
- **Minimum Log Source Requirement:** Webserver
- **Query:**

```
norm_id=* (url="*/autodiscover.json*" url IN ["*/powershell*", "*/mapi/nspi*", "*/EWS
*", "*X-Rps-CAT*"] status_code IN [200, 301])
```

Malicious Base64 Encoded PowerShell Keywords in Command Lines Detected

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

```
label="process" label=create "process"="*\powershell.exe" command IN ["* hidden *", "
*AGkAdABzAGEAZABtAGkAbgAgAC8AdAByAGEAbgBzAGYAZQByA*", "*aXRzYWRtaW4gL3RyYW5zZmVy*", "
*IAaQB0AHMAYQBkAG0AaQBuACAALwB0AHIAYQBuAHMAZgBlAHIA*",  "*JpdHNhZG1pbiAvdHJhbnNmZX*",
"*YgBpAHQAcwBhAGQAbQBpAG4AIAAvAHQAcgBhAG4AcwBmAGUAcg*", "*Yml0c2FkbWluIC90cmFuc2Zlc*"
, "*AGMAaAB1AG4AawBfAHMAaQB6AGUA*", "*JABjAGgAdQBuAGsAXwBzAGkAegBlA*", "*JGNodW5rX3Np
em*", "*QAYwBoAHUAbgBrAF8AcwBpAHoAZQ*", "*RjaHVua19zaXpl*", "*Y2h1bmtfc2l6Z*", "*AE8A
LgBDAG8AbQBwAHIAZQBzAHMAaQBvAG4A*", "*kATwAuAEMAbwBtAHAAcgBlAHMAcwBpAG8Abg*", "*lPLkN
vbXByZXNzaW9u*", "*SQBPAC4AQwBvAG0AcAByAGUAcwBzAGkAbwBuA*", "*SU8uQ29tcHJlc3Npb2*", "
*Ty5Db21wcmVzc2lvb*", "*AE8ALgBNAGUAbQBvAHIAeQBTAHQAcgBlAGEAbQ*", "*kATwAuAE0AZQBtAG8
AcgB5AFMAdAByAGUAYQBtA*", "*lPLk1lbW9yeVN0cmVhb*", "*SQBPAC4ATQBlAG0AbwByAHkAUwB0AHIA
ZQBhAG0A*", "*SU8uTWVtb3J5U3RyZWFt*", "*Ty5NZW1vcnlTdHJlYW*", "*4ARwBlAHQAQwBoAHUAbgB
rA*", "*5HZXRDaHVua*", "*AEcAZQB0AEMAaAB1AG4Aaw*", "*LgBHAGUAdABDAGgAdQBuAGsA*", "*Lk
dldENodW5r*", "*R2V0Q2h1bm*", "*AEgAUgBFAEEARABfAEkATgBGAE8ANgA0A*", "*QASABSAEUAQQBE
AF8ASQBOAEYATwA2ADQA*", "*RIUkVBRF9JTkZPNj*", "*SFJFQURfSU5GTzY0*", "*VABIAFIARQBBAEQ
AXwBJAE4ARgBPADYANA*", "*VEhSRUFEX0lORk82N*", "*AHIAZQBhAHQAZQBSAGUAbQBvAHQAZQBUAGgAc
gBlAGEAZA*", "*cmVhdGVSZW1vdGVUaHJlYW*", "*MAcgBlAGEAdABlAFIAZQBtAG8AdABlAFQAaAByAGUA
YQBkA*", "*NyZWF0ZVJlbW90ZVRocmVhZ*", "*Q3JlYXRlUmVtb3RlVGhyZWFk*", "*QwByAGUAYQB0AGU
AUgBlAG0AbwB0AGUAVABoAHIAZQBhAGQA*", "*0AZQBtAG0AbwB2AGUA*", "*1lbW1vdm*", "*AGUAbQBt
AG8AdgBlA*", "*bQBlAG0AbQBvAHYAZQ*", "*bWVtbW92Z*", "*ZW1tb3Zl*"] -user IN EXCLUDED_U
SERS
```

DLL Loaded Via AllocConsole and RunDLL32

- **Trigger Condition:** When DLL loading through allocconsole function and rundll32. AllocConsole is a Windows internal function that allocates a new console for the calling process. Rundll32.exe is a Windows internal binary that loads and runs 32-bit dynamic-link libraries (DLLs). Adversaries can use this technique to execute their payload using rundll32 to load a malicious DLL by invoking the AllocConsole function.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1218.011 - Rundll32
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="process" label=create "process" ="*\rundll32.exe" command="*.dll*" command="*allocconsole*"
```

Active Directory Database Dump Attempt

- **Trigger Condition:** When an attempt to dump the ntds.dit file is detected. NTDS.dit file is a database that stores the Active Directory data (including users, groups, security descriptors and password hashes). Adversaries can use this technique to retrieve credentials and obtain other domain information.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** T1003.003 - NTDS
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

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

Suspicious Child Process Creation via OneNote

- **Trigger Condition:** When the creation of suspicious child processes, execution of binaries from non-default paths and script file execution through OneNote are detected. Adversaries can use malicious OneNote files to social engineer users to execute it and drop their malicious payload or execute commands in the victim system.
- **ATT&CK Category:** Initial Access, Execution
- **ATT&CK Tag:** T1204.002 - Malicious File, T1566.001 - Spearphishing Attachment
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon event_id=1 parent_image="*\onenote.exe"
```

```
(file IN ["RUNDLL32.exe","REGSVR32.exe","bitsadmin.exe","CertUtil.exe","InstallUtil.exe","schtasks.exe","wmic.exe","cscript.exe","wscript.exe","CMSTP.EXE","Microsoft.Workflow.Compiler.exe","RegAsm.exe","RegSvcs.exe","MSHTA.EXE","Msxsl.exe","IEExec.exe","Cmd.Exe","PowerShell.EXE","HH.exe","javaw.exe","pcalua.exe","curl.exe","ScriptRunner.exe","CertOC.exe","WorkFolders.exe","odbcconf.exe","msiexec.exe","msdt.exe"] OR (image="*\explorer.exe" command IN ["*.hta*","*.vb*","*.wsh*","*.js*","*.ps*","*.scr*","*.pif*","*.bat","*.cmd*"]) OR image IN ["*\AppData\*","*\Users\Public\*","*\ProgramData\*","*\Windows\Tasks\*","*\Windows\Temp\*","*\Windows\System32\Tasks\*"])
```

Usage of Web Request Command

- **Trigger Condition:** The usage of various web request commands with CommandLine tools and Windows PowerShell cmdlets (including aliases) via CommandLine are detected. Adversaries can utilize this technique to download malicious payloads. However, the Usage of Get-Command and Get-Help modules referencing Invoke-WebRequest and Start-BitsTransfer might trigger false positives. Script Block Logging must be enabled for this alert rule to work.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** PowerShell
- **ATT&CK ID:** T1059.001
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
norm_id=WinServer script_block IN ["*Invoke-WebRequest*", "*iwr *", "*wget *", "*curl *", "*Net.WebClient*", "*Start-BitsTransfer*", "*Resume-BitsTransfer*", "*[System.Net.WebRequest]::create*", "*Invoke-RestMethod*", "*WinHttp.WinHttpRequest*"] -path="C:\Packages\Plugins\Microsoft.GuestConfiguration.ConfigurationforWindows\*"
```

Reconnaissance Activity with Nltest

- **Trigger Condition:** When possible reconnaissance activity via nltest binary is detected. Nltest is a Windows command-line utility that comes with a Windows Server, which is used to list domain controllers and enumerate domain trusts. The binary is available if you have installed the AD DS or the AD LDS server role. It is also available if you install the Active Directory Domain Services Tools that are part of the Remote Server Administration Tools (RSAT). Adversaries can use this technique to discover domain controllers, users and query the domain trust relationship.
- **ATT&CK Category:** Discovery
- **ATT&CK Tag:** T1016 - System Network Configuration Discovery, T1482 - Domain Trust Discovery
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create" process"="*\nltest.exe" file="nltestrk.exe" ((command = "*/server*" command="*/query*")  OR command IN ["*/dclist:*","*/domain_trusts*","*/trusted_domains*","*/user*","*/parentdomain*"])
```

Regsvr32 Network Activity Detected

- **Trigger Condition:** When network connections and Application Layer Protocol, DNS queries initiated via regsvr32 binary are detected. Regsvr32 is a command-line utility to register and unregister OLE controls, such as DLLs and ActiveX controls, in the Windows Registry. Adversaries utilized regsvr32 to run their malicious DLL, which downloads their other stager payload.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1218 - Signed Binary Proxy Execution, T1218.010 - Regsvr32
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WindowsSysmon image="*\regsvr32.exe"event_id IN ["3", "22"]
```

Possible Reconnaissance Activity

- **Trigger Condition:** When possible, reconnaissance activity, like the execution of several discovery commands in a short time, is detected. The binary in the process list is Window’s internal binary. Adversaries use this technique to discover the OS, user, network, subnets, file shares and domain trust, which will be used for further actions.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** T1016 - System Network Configuration Discovery, T1033 - System Owner/User Discovery, T1069 - Permission Groups Discovery, T1069.002 - Domain Groups, T1082 - System Information Discovery, T1087 - Account Discovery, T1087.002 - Domain Account, T1135 - Network Share Discovery, T1482 - Domain Trust Discovery
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create "process" IN ["*\whoami.exe", "*\nltest.exe", "*\net1.exe", "*\ipconfig.exe", "*\systeminfo.exe"]  | chart count() as cnt, distinct_list(command) as command by log_ts,user,host,domain   | search cnt > 3
```

Privilege Escalation via Kerberos KrbRelayUp

- **Trigger Condition:** KrbRelayUp performs a universal no-fix local privilege escalation in Windows domain environments where LDAP signing is not enforced. KrbRelayUp is a wrapper that can streamline the use of some features in Rubeus, KrbRelay, SCMUACBypass, PowerMad/SharpMad, Whisker and ADCSPwn tools in attacks.
- **ATT&CK Category:** Credential Access, Lateral Movement
- **ATT&CK Tag:** Pass the Ticket, Kerberoasting
- **ATT&CK ID:** T1550.003, T1558.003
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create
(parent_image="KrbRelayUp.exe" OR image="KrbRelayUp.exe" OR
(command=" relay " AND command=" -Domain " AND command=" -ComputerName ") OR
(command=" krbscm " AND command=" -sc ") OR
(command=" spawn " AND command=" -d " AND command=" -cn " AND command=" -cp *"))
```

Suspicious Execution of LNK File

- **Trigger Condition:** When the execution of suspicious LNK files that either spawns Powershell or command prompt and has high entropy in the command field is detected. A LNK file is a Windows Shortcut that is a pointer to open a file, folder or application. Adversaries can utilize LNK files to embed their malicious scripts and commands and lure victims into executing the payload to gain initial access and evade defense. For this alert to work, an entropy plugin is required. Analysts can set the entropy value depending on the environment to filter out false positives. In our environment, legitimate use entropy was below five, so we used an entropy value greater than five to filter out false positives. The baseline time for using the process entropy command to detect such events is 90 days.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** T1204.002 - Malicious File
- **Minimum Log Source Requirement:** Windows Sysmon, Windows
- **Query:**

```
label="Process" label=Create parent_process="*\explorer.exe" "process" IN ["*\cmd.exe","*\powershell.exe"]
| process entropy(command) as command_entropy
| search command_entropy > 5
```

Insecure Policy Set via Set-ExecutionPolicy

- **Trigger Condition:** When the Set-ExecutionPolicy command is utilized to set insecure policies such as Unrestricted, bypass, RemoteSigned. Set-ExecutionPolicy is a PowerShell command that can change PowerShell execution policies for Windows systems. The bypass option allows the script to be executed without warning or prompt. The RemoteSigned option allows the scripts downloaded from the internet to be executed. The unsigned option will allow scripts that are not digitally signed to be executed. Adversaries can utilize this technique to change the execution policy to run their choice of malicious PowerShell scripts. To generate relevant logs, Script Block Logging should be enabled.
- **ATT&CK Category:** Execution
- **ATT&CK Tag:** T1059.001 - PowerShell
- **Minimum Log Source Requirement:** Windows Sysmon
- **Query:**

```
norm_id=WinServer event_id=4104 script_block="*Set-ExecutionPolicy*" script_block IN ["*Unrestricted*","*bypass*","*RemoteSigned*"] -script_block IN ["*\AppData\Roaming\Code\*"]
```

Network Connection to Suspicious Server

- **Trigger Condition:** When communication between hosts and domains is mentioned in the query’s list. The query will search for logs generated from the Windows system or proxies and firewalls. The mentioned sites are either file storing or hosting sites. Adversaries have utilized such sites in many campaigns to upload and download data.

- **ATT&CK Category:** Command and Control
- **ATT&CK Tag:** T1105 - Ingress Tool Transfer
- **Minimum Log Source Requirement:** Windows Sysmon, Firewall, Proxy Server, WAF
- **Query:**

```
(norm_id=WindowsSysmon event_id=3 "image" IN ["C:\Windows\*","C:\Users\Public\*"] des
tination_host IN ["*dl.dropboxusercontent.com*","*.pastebin.com*","*.githubuserconten
t.com*", "*cdn.discordapp.com/attachments*","*mediafire.com*","*mega.nz*","*ddns.net*
",
"*.paste.ee*","*.hastebin.com/raw/*","*.ghostbin.co/*", "*ufile.io*","*anonfiles.com*
", "*send.exploit.in*","*transfer.sh*","*privatlab.net*","*privatlab.com*","*sendspac
e.com*","*pastetext.net*","*pastebin.pl*","*paste.ee*","*api.telegram.org*"]) OR
(device_category IN ["Firewall", "ProxyServer"] url IN ["*dl.dropboxusercontent.com*"
,"*.pastebin.com*","*.githubusercontent.com*", "*cdn.discordapp.com/attachments*","*m
ediafire.com*","*mega.nz*","*ddns.net*",
"*.paste.ee*","*.hastebin.com/raw/*","*.ghostbin.co/*", "*ufile.io*","*anonfiles.com*
", "*send.exploit.in*","*transfer.sh*","*priva
```