Synopsis

ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Inhibit System Recovery (T1490)
Severity	High

Description

A command line utility was used to clear the Windows Event Log.
It may be used to delete logs to cover the tracks of the malicious activity, making it harder to perform analysis.

Attacker's Goals

Delete logs to cover tracks of the malicious activity, making it harder to perform analysis.

Investigative actions

Check whether the executing process is benign, and if this was a desired behavior as part of its normal execution flow.

A Sensitive Windows Event Log was cleared using wevtutil.exe

Synopsis

ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Inhibit System Recovery (T1490)
Severity	Medium

Description

A command line utility was used to clear the Windows Event Log.
It may be used to delete logs to cover the tracks of the malicious activity, making it harder to

perform analysis.

Attacker's Goals

Delete logs to cover tracks of the malicious activity, making it harder to perform analysis.

Investigative actions

Check whether the executing process is benign, and if this was a desired behavior as part of its normal execution flow.

30.228 | Suspicious SearchProtocolHost.exe parent process

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	6 Hours
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Execution (TA0002) Defense Evasion (TA0005)

ATT&CK Technique	User Execution (T1204) System Binary Proxy Execution (T1218)
Severity	Medium

Description

SearchProtocolHost.exe has been launched from a process that is different from SearchIndexer.exe

This may indicate malicious activity (such as malware later being injected to it, or it being used for phantom DLL hijacking).

Attacker's Goals

Gain code execution on the host and evade security controls.

Investigative actions

Check whether the executing process is benign, and if this was a desired behavior as part of its normal execution flow.

30.229 | Remote service start from an uncommon source

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day

Required Data	- Requires: - XDR Agent
Detection Modules	
Detector Tags	Impacket Analytics
ATT&CK Tactic	Lateral Movement (TA0008) Execution (TA0002)
ATT&CK Technique	Remote Services (T1021) System Services: Service Execution (T1569.002)
Severity	Low

Description

A remotely triggered service initiated by a host that rarely triggers services to other remote hosts.

Attacker's Goals

Perform lateral movement to new hosts to expand the foothold within a network.

Investigative actions

- Investigate the service being spawned on the host for malicious activities.
- Correlate the RPC call from the source host and understand which software initiated it.

30.230 | Unsigned and unpopular process performed a DLL

injection

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	Injection Analytics
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Process Injection (T1055)
Severity	Low

Description

An unsigned process with low popularity injected a dll to another process.

Attacker's Goals

Attackers may inject DLLs into processes to evade process-based defenses, as well as possibly elevate privileges.

Investigative actions

> Check whether the injecting process is benign, and if this was a desired behavior as part of its normal execution flow.

Variations

Unsigned and unpopular process performed process hollowing DLL injection

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Process Injection (T1055)
Severity	High

Description

An unsigned process with low popularity injected a dll to another process.

Attacker's Goals

Attackers may inject DLLs into processes to evade process-based defenses, as well as possibly elevate privileges.

Investigative actions

> Check whether the injecting process is benign, and if this was a desired behavior as part of its normal execution flow.

Unsigned and unpopular process performed queue APC DLL injection

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Process Injection (T1055)

Severity	High

Description

An unsigned process with low popularity injected a dll to another process.

Attacker's Goals

Attackers may inject DLLs into processes to evade process-based defenses, as well as possibly elevate privileges.

Investigative actions

> Check whether the injecting process is benign, and if this was a desired behavior as part of its normal execution flow.

Unsigned and unpopular process performed a DLL injection to a sensitive process

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Process Injection (T1055)
Severity	Medium

Description

An unsigned process with low popularity injected a dll to another process.

Attacker's Goals

Attackers may inject DLLs into processes to evade process-based defenses, as well as possibly elevate privileges.

Investigative actions

> Check whether the injecting process is benign, and if this was a desired behavior as part of its normal execution flow.

Unsigned and unpopular process performed a DLL injection to a commonly abused process

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Process Injection (T1055)
Severity	High

Description

An unsigned process with low popularity injected a dll to another process.

Attacker's Goals

Attackers may inject DLLs into processes to evade process-based defenses, as well as possibly elevate privileges.

Investigative actions

> Check whether the injecting process is benign, and if this was a desired behavior as part of its normal execution flow.

Unsigned and unpopular process performed a DLL injection to a security vendor signed process

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Process Injection (T1055)
Severity	Medium

Description

An unsigned process with low popularity injected a dll to another process.

Attacker's Goals

Attackers may inject DLLs into processes to evade process-based defenses, as well as possibly elevate privileges.

Investigative actions

Check whether the injecting process is benign, and if this was a desired behavior as part of its normal execution flow.

30.231 | LOLBIN process executed with a high integrity level

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Abuse Elevation Control Mechanism (T1548)

Severity	Low

Description

A process spawned a suspicious LOLBIN process with a higher/system integrity level.
The LOLBIN process spawned with an uncommon command line. This may be an indication of malicious code execution to gain privileges.

Attacker's Goals

An attacker may attempt to gain higher privileges.

Investigative actions

- Check whether the command line executed is benign or normal for the host and/or user performing it.
  Investigate the endpoint to determine if it's a legitimate process that is supposed to run with privileges.

Variations

LOLBIN process executed with a high integrity level by a web server process or CGO

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004) Initial Access (TA0001) Persistence (TA0003)
ATT&CK Technique	Abuse Elevation Control Mechanism (T1548) External Remote Services (T1133) Server Software Component: Web Shell (T1505.003)
Severity	Medium

Description

A process spawned a suspicious LOLBIN process with a higher/system integrity level by a web server process or CGO.

The LOLBIN process spawned with an uncommon command line. This may be an indication of malicious code execution to gain privileges.

Attacker's Goals

An attacker may attempt to gain higher privileges.

Investigative actions

Check whether the command line executed is benign or normal for the host and/or user performing it.

Investigate the endpoint to determine if it's a legitimate process that is supposed to run with privileges.

30.232 | Suspicious External RDP Login

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	- Requires: ▯ XDR Agent
Detection Modules	Identity Analytics
Detector Tags	

ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	External Remote Services (T1133)
Severity	Informational

Description

An unusual successful RDP connection by a user from an external IP.
This may be indicative of using stolen credentials or malicious activity.

Attacker's Goals

The attacker attempts to gain access to the accounts through RDP from an external source.

Investigative actions

Identify the user performing RDP and check that it is authorized.
Check whether this IP has a malicious reputation.

Reset the user's password.
- Follow further actions done by the user.

30.233 | Mshta.exe launched with suspicious arguments

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day

Required Data	- Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	System Binary Proxy Execution: Mshta (T1218.005)
Severity	Low

Description

Microsoft HTML application host process has been launched with suspicious arguments, which may indicate malicious intent.

Attacker's Goals

Gain code execution on the host and evade security controls.

Investigative actions

Check whether the executing process is benign, and if this was a desired behavior as part of its normal execution flow.

30.234 | Kubernetes nsenter container escape

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	7 Days
Required Data	- Requires: - XDR Agent
Detection Modules	
Detector Tags	Kubernetes - AGENT, Containers
ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Escape to Host (T1611)
Severity	Informational

Description

The nsenter command was used to execute a process in the context of the initialization process.

Attacker's Goals

Attackers may break out of a container to run commands on the host.

Investigative actions

Check whether the executing process is benign, and if this was a desired behavior as part of its normal execution flow.

Variations

Kubernetes nsenter container escape from a new Pod

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Escape to Host (T1611)
Severity	Medium

Description

The nsenter command was used to execute a process in the context of the initialization process.

Attacker's Goals

Attackers may break out of a container to run commands on the host.

Investigative actions

Check whether the executing process is benign, and if this was a desired behavior as part of its normal execution flow.

Kubernetes nsenter container escape from a Pod

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Escape to Host (T1611)
Severity	Low

Description

The nsenter command was used to execute a process in the context of the initialization process.

Attacker's Goals

Attackers may break out of a container to run commands on the host.

Investigative actions

Check whether the executing process is benign, and if this was a desired behavior as part of its normal execution flow.

30.235 | Possible network service discovery via command-line tool

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	6 Hours
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Network Service Discovery (T1046)
Severity	Low

Description

An attacker may use command-line utilities to discover open ports and services on a remote host.

Attacker's Goals

Unavailable.

Investigative actions

Unavailable.

30.236 | Rare communication over email ports to external email server by unsigned process

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Hour

Required Data	- Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Non-Application Layer Protocol (T1095)
Severity	Low

Description

These methods are used by malware and attackers to leak data and remain undetected.

Attacker's Goals

Attackers might use well-known email ports as a C&C channel to evade detection and firewall rules.

Investigative actions

- Check whether the initiator process is benign or normal for the host and/or user performing it.
- Check whether additional malicious commands were executed from the same process.

30.237 | Uncommon Service Create/Config

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Hour
Required Data	- Requires: - XDR Agent
Detection Modules	
Detector Tags	Malicious Service Analytics
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	System Services: Service Execution (T1569.002)
Severity	Medium

Description

The Service Control command (sc.exe) is used to create, start, stop, query, or delete Windows services. Adversaries may attempt to use the command to execute and persist a binary, command, or script.

Attacker's Goals

Evading security controls and possibly persisting malware.

Investigative actions

Check whether the service created, or the configuration change to an existing service, is benign or normal for the host and/or user performing it.

30.238 | Possible code downloading from a remote host by Regsvr32

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	System Binary Proxy Execution: Regsvr32 (T1218.010)
Severity	Medium

Description

Regsvr32 may be used to fetch arbitrary code from a remote host and execute it without dropping the payload onto the disk. Known to be used for malicious purposes.

Attacker's Goals

Gain code execution on the host and evade security controls.

Investigative actions

Check whether the executing process is benign, and if this was a desired behavior as part of its normal execution flow.

30.239 | Rare security product signed executable executed in the network

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Exploitation for Defense Evasion (T1211)

Severity	Low

Description

Attackers may attempt to install a security product with a known vulnerability to bypass security features.

Attacker's Goals

Adversaries may exploit the application vulnerability to bypass security features.

Investigative actions

Check if the security product was installed by a legitimate user and intentionally.

30.240 | Suspicious runonce.exe parent process

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	6 Hours
Required Data	▌ Requires: ▯ XDR Agent
Detection Modules	

Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)
Severity	Low

Description

Runonce.exe executes commands under the Registry key HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce, typically on computer boot and user logon events.

Attacker's Goals

Command execution and persistence on the host.

Investigative actions

Check whether the executing process is benign, and if this was a desired behavior as part of its normal execution flow.

30.241 | Unusual Lolbins Process Spawned by InstallUtil.exe

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)

Deduplication Period	1 Day
Required Data	Requires: • XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	System Binary Proxy Execution: InstallUtil (T1218.004)
Severity	Low

Description

An unusual process was spawned by InstallUtil.exe, possibly indicating malicious local or remote code execution.

Attacker's Goals

Gain code execution on the host.

Investigative actions

Check whether the executing process is benign, and if this was a desired behavior as part of its normal execution flow.

30.242 | Abnormal Recurring Communications to a Rare Domain

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent OR - Third-Party Firewalls
Detection Modules	
Detector Tags	NDR C2 Detection
ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Non-Application Layer Protocol (T1095)
Severity	Informational

Description

Abnormal communications were seen from an internal entity to a rare external domain. This could be a case of beaconing to a C2 Server.

Attacker's Goals

Communicate with malicious code running on your network enabling further access to the endpoint and network, performing software updates on the endpoint, or for taking inventory of infected machines.

Investigative actions

Identify if the external domain belongs to a reputable organization or an asset used in a public cloud.

Identify if the source of the traffic is malware. If the source of the traffic is a malicious file, Cortex XDR Analytics also raises a malware alert for the file on the endpoint. Malware may contact legitimate domain names, therefore check for unusual apps used, or unusual ports or volumes accessed.
View all related traffic generated by the suspicious process to understand the purpose.

Look for other endpoints on your network that are also contacting the suspicious domain name.
Examine file-system operations performed by the process that initiated the traffic and look for potential artifacts on infected endpoints.

Variations

Abnormal Recurring Communications to a Rare Domain With a Port Commonly Used by Attack Platforms

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Non-Application Layer Protocol (T1095)
Severity	Low

Description

Abnormal communications were seen from an internal entity to a rare external domain. This could be a case of beaconing to a C2 Server.

Attacker's Goals

Communicate with malicious code running on your network enabling further access to the endpoint and network, performing software updates on the endpoint, or for taking inventory of infected machines.

Investigative actions

- Identify if the external domain belongs to a reputable organization or an asset used in a public cloud.
- Identify if the source of the traffic is malware. If the source of the traffic is a malicious file, Cortex XDR Analytics also raises a malware alert for the file on the endpoint. Malware may contact legitimate domain names, therefore check for unusual apps used, or unusual ports or volumes accessed.
- View all related traffic generated by the suspicious process to understand the purpose.
- Look for other endpoints on your network that are also contacting the suspicious domain name.
- Examine file-system operations performed by the process that initiated the traffic and look for potential artifacts on infected endpoints.

Abnormal Recurring Communications to a Rare Domain to a Suspicious Autonomous System (AS)

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Non-Application Layer Protocol (T1095)
Severity	Low

Description

Abnormal communications were seen from an internal entity to a rare external domain. This could be a case of beaconing to a C2 Server.

Attacker's Goals

Communicate with malicious code running on your network enabling further access to the endpoint and network, performing software updates on the endpoint, or for taking inventory of infected machines.

Investigative actions

- Identify if the external domain belongs to a reputable organization or an asset used in a public cloud.
  Identify if the source of the traffic is malware. If the source of the traffic is a malicious file, Cortex XDR Analytics also raises a malware alert for the file on the endpoint. Malware may

  contact legitimate domain names, therefore check for unusual apps used, or unusual ports or volumes accessed.
- View all related traffic generated by the suspicious process to understand the purpose. Look for other endpoints on your network that are also contacting the suspicious domain name.

  Examine file-system operations performed by the process that initiated the traffic and look for potential artifacts on infected endpoints.

Abnormal Recurring Communications to a Rare Domain With an Abnormal Domain Suffix

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Non-Application Layer Protocol (T1095)
Severity	Informational

Description

Abnormal communications were seen from an internal entity to a rare external domain. This could be a case of beaconing to a C2 Server.

Attacker's Goals

Communicate with malicious code running on your network enabling further access to the endpoint and network, performing software updates on the endpoint, or for taking inventory of infected machines.

Investigative actions

Identify if the external domain belongs to a reputable organization or an asset used in a public cloud.

- Identify if the source of the traffic is malware. If the source of the traffic is a malicious file, Cortex XDR Analytics also raises a malware alert for the file on the endpoint. Malware may contact legitimate domain names, therefore check for unusual apps used, or unusual ports or volumes accessed.
- View all related traffic generated by the suspicious process to understand the purpose.
- Look for other endpoints on your network that are also contacting the suspicious domain name.

Examine file-system operations performed by the process that initiated the traffic and look for potential artifacts on infected endpoints.

Abnormal Recurring Communications to a Rare Domain With a Less Common Port

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Non-Application Layer Protocol (T1095)
Severity	Low

Description

Abnormal communications were seen from an internal entity to a rare external domain. This could be a case of beaconing to a C2 Server.

Attacker's Goals

Communicate with malicious code running on your network enabling further access to the endpoint and network, performing software updates on the endpoint, or for taking inventory of infected machines.

Investigative actions

Identify if the external domain belongs to a reputable organization or an asset used in a public cloud.

- Identify if the source of the traffic is malware. If the source of the traffic is a malicious file, Cortex XDR Analytics also raises a malware alert for the file on the endpoint. Malware may contact legitimate domain names, therefore check for unusual apps used, or unusual ports or volumes accessed.
- View all related traffic generated by the suspicious process to understand the purpose.
- Look for other endpoints on your network that are also contacting the suspicious domain name.

Examine file-system operations performed by the process that initiated the traffic and look for potential artifacts on infected endpoints.

30.243 | A browser was opened in private mode

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)

ATT&CK Technique	- Impair Defenses: Indicator Blocking (T1562.006) - Hide Artifacts (T1564)
Severity	Informational

Description

A browser was opened in private mode, which may indicate an attempt to cover tracks.

Attacker's Goals

A browser was opened in private mode. Users might use private mode if they wish to stay anonymous online or hide their search and browsing history.

Investigative actions

Check for any other suspicious activity related to the host and the user involved in the alert.

30.244 | Uncommon Managed Object Format (MOF) compiler usage

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Hour

Required Data	- Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Event Triggered Execution: Windows Management Instrumentation Event Subscription (T1546.003)
Severity	Informational

Description

The mofcomp.exe WMI MOF compiled is used to compile code into the WMI repository that in turn may enable attackers to run scheduled or triggered code from the context of a Microsoft signed binary.

Attacker's Goals

Run code via triggers from the context of the WMI executor.

Investigative actions

Verify if the executing process is suspicious.
Check if the MOF file being compiled has any malicious indicators within it.

30.245 | New addition to Windows Defender exclusion list

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Hour
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Hide Artifacts: File/Path Exclusions (T1564.012) Impair Defenses: Disable or Modify Tools (T1562.001)
Severity	Low

Description

Windows Defender keeps the exclusion list in the Registry, and any addition to it will cause it to ignore a process, path or file extension.

Attacker's Goals

Gain code execution on the host and evade security controls.

Investigative actions

- Check whether the executing process is benign, and if this was a desired behavior as part of its normal execution flow.
  Check the excluded object type (process, path or extension) and nature.
  Check if the excluded object is malicious.

Variations

New addition to Windows Defender exclusion list from an unsigned process

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	- Hide Artifacts: File/Path Exclusions (T1564.012) Impair Defenses: Disable or Modify Tools (T1562.001)
Severity	Medium

Description

Windows Defender keeps the exclusion list in the Registry, and any addition to it will cause it to ignore a process, path or file extension.

Attacker's Goals

Gain code execution on the host and evade security controls.

Investigative actions

Check whether the executing process is benign, and if this was a desired behavior as part of its normal execution flow.

Check the excluded object type (process, path or extension) and nature.
- Check if the excluded object is malicious.

30.246 | Keylogging using system commands

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	Kubernetes - AGENT, Containers
ATT&CK Tactic	▌ Credential Access (TA0006) Collection (TA0009)
ATT&CK Technique	Input Capture: Keylogging (T1056.001)
Severity	Low

Description

Usage of a Linux system utility to capture input.

Attacker's Goals

Attackers may capture keystrokes to intercept user credentials.

Investigative actions

Check whether the executing process is benign, and if this was a desired behavior as part of its normal execution flow.

Variations

Keylogging using system commands in a Kubernetes pod

Synopsis

ATT&CK Tactic	- Credential Access (TA0006) - Collection (TA0009)
ATT&CK Technique	Input Capture: Keylogging (T1056.001)
Severity	Low

Description

Usage of a Linux system utility to capture input.

Attacker's Goals

Attackers may capture keystrokes to intercept user credentials.

Investigative actions

Check whether the executing process is benign, and if this was a desired behavior as part of its normal execution flow.

30.247 | Uncommon remote scheduled task creation

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	6 Hours
Required Data	- Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Scheduled Task/Job (T1053)
Severity	High

Description

The schtasks.exe command enables creating, deleting, querying, changing, running, and ending scheduled tasks on a local or remote computer. Adversaries may attempt to use the command to execute programs or persist malware on remote machines.

Attacker's Goals

Attackers can attempt to use the command to execute programs or persist malware on remote endpoints.

Investigative actions

Investigate the initiator process and whether it should create remote tasks.

Investigate the scheduled task execution on the remote machine.

30.248 | Abnormal Recurring Communications to a Rare IP

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	
Detector Tags	NDR C2 Detection
ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Non-Application Layer Protocol (T1095)
Severity	Informational

Description

Abnormal communications were seen from an internal entity to a rare external address. This could be a case of beaconing to a C2 Server.

Attacker's Goals

Communicate with malicious code running on your network enabling further access to the endpoint and network, performing software updates on the endpoint, or for taking inventory of infected machines.

Investigative actions

Identify if the external IP address belongs to a reputable organization or an asset used in a public cloud.

Identify if the source of the traffic is malware. If the source of the traffic is a malicious file, Cortex XDR Analytics also raises a malware alert for the file on the endpoint. Malware may contact legitimate IP addresses, therefore check for unusual apps used, or unusual ports or volumes accessed.
View all related traffic generated by the suspicious process to understand the purpose.

Look for other endpoints on your network that are also contacting the suspicious IP address.

- Examine file-system operations performed by the process that initiated the traffic and look for potential artifacts on infected endpoints.

Variations

Abnormal Recurring Communications to a Rare IP With a Port Commonly Used by Attack Platforms

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Non-Application Layer Protocol (T1095)
Severity	Informational

Description

Abnormal communications were seen from an internal entity to a rare external address. This could be a case of beaconing to a C2 Server.

Attacker's Goals

Communicate with malicious code running on your network enabling further access to the endpoint and network, performing software updates on the endpoint, or for taking inventory of infected machines.

Investigative actions

- Identify if the external IP address belongs to a reputable organization or an asset used in a public cloud.
  Identify if the source of the traffic is malware. If the source of the traffic is a malicious file, Cortex XDR Analytics also raises a malware alert for the file on the endpoint. Malware may contact legitimate IP addresses, therefore check for unusual apps used, or unusual ports or volumes accessed.
- View all related traffic generated by the suspicious process to understand the purpose.
  Look for other endpoints on your network that are also contacting the suspicious IP address.
  Examine file-system operations performed by the process that initiated the traffic and look for potential artifacts on infected endpoints.

Abnormal Recurring Communications to a Rare IP With a NetBIOS Port

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Non-Application Layer Protocol (T1095)
Severity	Informational

Description

Abnormal communications were seen from an internal entity to a rare external address. This could be a case of beaconing to a C2 Server.

Attacker's Goals

Communicate with malicious code running on your network enabling further access to the endpoint and network, performing software updates on the endpoint, or for taking inventory of infected machines.

Investigative actions

Identify if the external IP address belongs to a reputable organization or an asset used in a public cloud.

- Identify if the source of the traffic is malware. If the source of the traffic is a malicious file, Cortex XDR Analytics also raises a malware alert for the file on the endpoint. Malware may contact legitimate IP addresses, therefore check for unusual apps used, or unusual ports or volumes accessed.
- View all related traffic generated by the suspicious process to understand the purpose.
- Look for other endpoints on your network that are also contacting the suspicious IP address. Examine file-system operations performed by the process that initiated the traffic and look for potential artifacts on infected endpoints.

Abnormal Recurring Communications to a Rare IP Using a Peer to Peer Protocol

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Non-Application Layer Protocol (T1095)
Severity	Informational

Description

Abnormal communications were seen from an internal entity to a rare external address. This could be a case of beaconing to a C2 Server.

Attacker's Goals

Communicate with malicious code running on your network enabling further access to the endpoint and network, performing software updates on the endpoint, or for taking inventory of infected machines.

Investigative actions

Identify if the external IP address belongs to a reputable organization or an asset used in a public cloud.

- Identify if the source of the traffic is malware. If the source of the traffic is a malicious file, Cortex XDR Analytics also raises a malware alert for the file on the endpoint. Malware may contact legitimate IP addresses, therefore check for unusual apps used, or unusual ports or volumes accessed.
- View all related traffic generated by the suspicious process to understand the purpose.
- Look for other endpoints on your network that are also contacting the suspicious IP address. Examine file-system operations performed by the process that initiated the traffic and look for potential artifacts on infected endpoints.

Abnormal Recurring Communications to a Rare IP Using a Gaming Protocol

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Non-Application Layer Protocol (T1095)
Severity	Informational

Description

Abnormal communications were seen from an internal entity to a rare external address. This could be a case of beaconing to a C2 Server.

Attacker's Goals

Communicate with malicious code running on your network enabling further access to the endpoint and network, performing software updates on the endpoint, or for taking inventory of infected machines.

Investigative actions

Identify if the external IP address belongs to a reputable organization or an asset used in a public cloud.

- Identify if the source of the traffic is malware. If the source of the traffic is a malicious file, Cortex XDR Analytics also raises a malware alert for the file on the endpoint. Malware may contact legitimate IP addresses, therefore check for unusual apps used, or unusual ports or volumes accessed.
- View all related traffic generated by the suspicious process to understand the purpose.
- Look for other endpoints on your network that are also contacting the suspicious IP address. Examine file-system operations performed by the process that initiated the traffic and look for potential artifacts on infected endpoints.

Abnormal Recurring Communications to a Rare IP Using a Video and Audio Conversation Protocol

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Non-Application Layer Protocol (T1095)
Severity	Informational

Description

Abnormal communications were seen from an internal entity to a rare external address. This could be a case of beaconing to a C2 Server.

Attacker's Goals

Communicate with malicious code running on your network enabling further access to the endpoint and network, performing software updates on the endpoint, or for taking inventory of infected machines.

Investigative actions

Identify if the external IP address belongs to a reputable organization or an asset used in a public cloud.

- Identify if the source of the traffic is malware. If the source of the traffic is a malicious file, Cortex XDR Analytics also raises a malware alert for the file on the endpoint. Malware may contact legitimate IP addresses, therefore check for unusual apps used, or unusual ports or volumes accessed.
- View all related traffic generated by the suspicious process to understand the purpose.
- Look for other endpoints on your network that are also contacting the suspicious IP address. Examine file-system operations performed by the process that initiated the traffic and look for potential artifacts on infected endpoints.

Abnormal Recurring Communications to a Rare IP From an Unmanaged Host

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Non-Application Layer Protocol (T1095)
Severity	Informational

Description

Abnormal communications were seen from an internal entity to a rare external address. This could be a case of beaconing to a C2 Server.

Attacker's Goals

Communicate with malicious code running on your network enabling further access to the endpoint and network, performing software updates on the endpoint, or for taking inventory of infected machines.

Investigative actions

Identify if the external IP address belongs to a reputable organization or an asset used in a public cloud.

- Identify if the source of the traffic is malware. If the source of the traffic is a malicious file, Cortex XDR Analytics also raises a malware alert for the file on the endpoint. Malware may contact legitimate IP addresses, therefore check for unusual apps used, or unusual ports or volumes accessed.
- View all related traffic generated by the suspicious process to understand the purpose.
- Look for other endpoints on your network that are also contacting the suspicious IP address. Examine file-system operations performed by the process that initiated the traffic and look for potential artifacts on infected endpoints.

30.249 | Suspicious process execution by scheduled task

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	2 Days
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)

ATT&CK Technique	Scheduled Task/Job (T1053)
Severity	Low

Description

An unpopular unsigned process was executed by a scheduled task.

Attacker's Goals

Attackers may attempt to gain persistence on the endpoint using scheduled tasks.

Investigative actions

Review the process executed by the schedule task.

Investigate the specific scheduled task execution chain.

Variations

Suspicious process execution by scheduled task on a sensitive server

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Scheduled Task/Job (T1053)
Severity	Medium

Description

An unpopular unsigned process was executed by a scheduled task.

Attacker's Goals

Attackers may attempt to gain persistence on the endpoint using scheduled tasks.

Investigative actions

- Review the process executed by the schedule task.
- Investigate the specific scheduled task execution chain.

30.250 | Globally uncommon high entropy module was loaded

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Obfuscated Files or Information (T1027)
Severity	Informational

Description

A module with high entropy and a globally uncommon hash was loaded.

Attacker's Goals

Adversaries may attempt to make an executable difficult to discover or analyze by compressing, encrypting, encoding, or otherwise obfuscating its contents.

Investigative actions

Check if the module is either compressed, encrypted, obfuscated or packed.

30.251 | Interactive login by a machine account

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	▮ Requires: - XDR Agent
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Initial Access (TA0001)

ATT&CK Technique	Valid Accounts: Domain Accounts (T1078.002)
Severity	Informational

Description

A machine account performed an interactive or remote interactive login.

Attacker's Goals

Use an account that has access to resources to move laterally in the network and access privileged resources.

Investigative actions

- See whether the login was successful.
- Check whether the account has done any administrative actions it should not usually do.
- Look for more logins and authentications by the account throughout the network.

Variations

Successful interactive login by a machine account

Synopsis

ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts: Domain Accounts (T1078.002)
Severity	Low

Description

A machine account performed a successful interactive or remote interactive login.

Attacker's Goals

Use an account that has access to resources to move laterally in the network and access privileged resources.

Investigative actions

See whether the login was successful.
Check whether the account has done any administrative actions it should not usually do.

Look for more logins and authentications by the account throughout the network.

30.252 | Rare DCOM RPC activity

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	ꞁ Requires: ▯ XDR Agent
Detection Modules	
Detector Tags	NDR Lateral Movement Analytics
ATT&CK Tactic	Lateral Movement (TA0008)

ATT&CK Technique	Remote Services: Distributed Component Object Model (T1021.003)
Severity	Informational

Description

The endpoint performed abnormal DCOM RPC activity to a remote host.

Attacker's Goals

Attackers may attempt to gain persistence or move laterally over the network by executing code on remote hosts using the DCOM RPC interface.

The DCOM RPC interface is used to remotely invoke registered COM applications on remote hosts.

Investigative actions

- Review the action of the initiated COM application on the remote host.
  Correlate the RPC call from the source host and understand which software initiated it.
  Verify that this isn't IT activity.

Variations

Rare DCOM RPC activity

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Services: Distributed Component Object Model (T1021.003)
Severity	Low

Description

The endpoint performed abnormal DCOM RPC activity to a remote host.

Attacker's Goals

- Attackers may attempt to gain persistence or move laterally over the network by executing code on remote hosts using the DCOM RPC interface.
  The DCOM RPC interface is used to remotely invoke registered COM applications on remote hosts.

Investigative actions

Review the action of the initiated COM application on the remote host.

- Correlate the RPC call from the source host and understand which software initiated it.
- Verify that this isn't IT activity.

30.253 | Suspicious Process Spawned by Adobe Reader

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	- Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Initial Access (TA0001)

ATT&CK Technique	Phishing: Spearphishing Attachment (T1566.001)
Severity	Low

Description

Unusual process spawned by Adobe Reader with an uncommon command line.

Attacker's Goals

An attacker attempts to gain code execution via a phishing document.

Investigative actions

Check the source of the document (received by mail or loaded locally).

Investigate the child processes for malicious activity and network connections to an external host.

30.254 | Rundll32.exe spawns conhost.exe

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: ▯ XDR Agent

Detection Modules	
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	System Binary Proxy Execution: Rundll32 (T1218.011)
Severity	Medium

Description

This unusual parent-child process relationship may indicate that an attacker has abused rundll32.exe to run a console-based application such as PowerShell.

Attacker's Goals

Evading detections by running code from a signed Microsoft executable.

Investigative actions

Check whether the executing process is benign, and if this was a desired behavior as part of its normal execution flow.

30.255 | Rare SSH Session

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	N/A (single event)
Deduplication Period	1 Hour
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Services (T1021)
Severity	Low

Description

Secure Shell (SSH) provides a secure means of remote administration. Attackers can use valid SSH credentials and keys to remotely connect to endpoints running the SSH service.

Attacker's Goals

Secure Shell (SSH) provides a secure means of remote administration. Attackers can use valid SSH credentials and keys to remotely connect to endpoints running the SSH service.

Investigative actions

Verify that the process is allowed in the organization.

Check if the user should access the destination and whether the session was successful or not.

30.256 | Unsigned and unpopular process performed an injection

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	Injection Analytics
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Process Injection (T1055)
Severity	Low

Description

An unsigned process with low popularity injected code to another process.

Attacker's Goals

Attackers may inject code into processes to evade process-based defenses, as well as possibly elevate privileges.

Investigative actions

- Check whether the injecting process is benign, and if this was a desired behavior as part of its normal execution flow.

Variations

Unsigned and unpopular process performed process hollowing injection

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Process Injection (T1055)
Severity	High

Description

An unsigned process with low popularity injected code to another process.

Attacker's Goals

Attackers may inject code into processes to evade process-based defenses, as well as possibly elevate privileges.

Investigative actions

Check whether the injecting process is benign, and if this was a desired behavior as part of its normal execution flow.

Unsigned and unpopular process performed queue APC injection

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Process Injection (T1055)

Severity	High

Description

An unsigned process with low popularity injected code to another process.

Attacker's Goals

Attackers may inject code into processes to evade process-based defenses, as well as possibly elevate privileges.

Investigative actions

> Check whether the injecting process is benign, and if this was a desired behavior as part of its normal execution flow.

Unsigned and unpopular process performed injection into a sensitive process

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Process Injection (T1055)
Severity	Medium

Description

An unsigned process with low popularity injected code to another process.

Attacker's Goals

Attackers may inject code into processes to evade process-based defenses, as well as possibly elevate privileges.

Investigative actions

> Check whether the injecting process is benign, and if this was a desired behavior as part of its normal execution flow.

Unsigned and unpopular process performed injection into svchost.exe

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005) Privilege Escalation (TA0004)
ATT&CK Technique	Process Injection (T1055)
Severity	High

Description

An unsigned process with low popularity injected code to another process. This process attempted to obtain System user permissions.

Attacker's Goals

Attackers may inject code into processes to evade process-based defenses, as well as possibly elevate privileges.

Investigative actions

Check whether the injecting process is benign, and if this was a desired behavior as part of its normal execution flow.

Unsigned and unpopular process performed injection into a commonly abused process

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Process Injection (T1055)
Severity	High

Description

An unsigned process with low popularity injected code to another process.

Attacker's Goals

Attackers may inject code into processes to evade process-based defenses, as well as possibly elevate privileges.

Investigative actions

Check whether the injecting process is benign, and if this was a desired behavior as part of its normal execution flow.

Unsigned and unpopular process performed injection into a process signed by a security vendor

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Process Injection (T1055)
Severity	Medium

Description

An unsigned process with low popularity injected code to another process.

Attacker's Goals

Attackers may inject code into processes to evade process-based defenses, as well as possibly elevate privileges.

Investigative actions

Check whether the injecting process is benign, and if this was a desired behavior as part of its normal execution flow.

30.257 | Suspicious time provider registered

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Boot or Logon Autostart Execution: Time Providers (T1547.003)
Severity	Medium

Description

The endpoint time provider has been tampered, this change may be used to gain persistence on the host by loading libraries into the time management service.

Attacker's Goals

Gain persistence using the legitimate windows time provider mechanism, which loads libraries into Windows services.

Investigative actions

- Verify if the registered library is malicious.
Check if the installing software is a malicious binary.
Check for any network activity from a "svchost.exe -k LocalService" process that seems suspicious.

Variations

Suspicious time provider registered manually by reg.exe

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Boot or Logon Autostart Execution: Time Providers (T1547.003)
Severity	High

Description

The endpoint time provider has been tampered, this change may be used to gain persistence on the host by loading libraries into the time management service.

Attacker's Goals

Gain persistence using the legitimate windows time provider mechanism, which loads libraries into Windows services.

Investigative actions

Verify if the registered library is malicious.

Check if the installing software is a malicious binary.

- Check for any network activity from a "svchost.exe -k LocalService" process that seems suspicious.

Suspicious time provider registered using an uncommon provider name

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Boot or Logon Autostart Execution: Time Providers (T1547.003)
Severity	High

Description

The endpoint time provider has been tampered, this change may be used to gain persistence on the host by loading libraries into the time management service.

Attacker's Goals

Gain persistence using the legitimate windows time provider mechanism, which loads libraries into Windows services.

Investigative actions

Verify if the registered library is malicious.

Check if the installing software is a malicious binary.

- Check for any network activity from a "svchost.exe -k LocalService" process that seems suspicious.

30.258 | Rare process spawned by srvany.exe

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	N/A (single event)
Deduplication Period	1 Hour
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	System Services: Service Execution (T1569.002)
Severity	Informational

Description

Unusual process spawned by srvany.exe, which allows applications to run as services with system privileges, this might be an indication of malicious local or remote code execution.

Attacker's Goals

Execute malware on the host in a manner that doesn't leave event logs within the system.

Investigative actions

Validate if the binary that srvany.exe executed is malicious.
Track down the source of the srvany.exe binary and the executed process.

Validate if this is a legitimate software installed by IT.

30.259 | A process connected to a rare external host

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Application Layer Protocol (T1071)
Severity	Informational

Description

A Process connected to an external host name or directly to an IP address, which are rarely connected to from the organization.

Attacker's Goals

Beacon to C2 server and/or exfiltrate data.

Investigative actions

Check whether the process was injected or otherwise subverted for malicious use.

Variations

MSBuild process connected to a rare external host

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005) Command and Control (TA0011)
ATT&CK Technique	Trusted Developer Utilities Proxy Execution: MSBuild (T1127.001) Application Layer Protocol (T1071)
Severity	High

Description

MSBuild normally does not make any network connections. This unusual activity may be malicious since attackers can leverage MSBuild for code execution.

Attacker's Goals

Beacon to C2 server and/or exfiltrate data.

Investigative actions

Check if CGO actor process is not code developing tool (IDE) and whether the actor process subverted for malicious use.

MSBuild process connected to a rare external host

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)

ATT&CK Technique	Trusted Developer Utilities Proxy Execution: MSBuild (T1127.001)
Severity	Medium

Description

MSBuild normally does not make any network connections. This unusual activity may be malicious since attackers can leverage MSBuild for code execution.

Attacker's Goals

Beacon to C2 server and/or exfiltrate data.

Investigative actions

Check if CGO actor process is not code developing tool (IDE) and whether the actor process subverted for malicious use.

LOLBIN spawned by an Office executable connected to a rare external host

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Application Layer Protocol (T1071)
Severity	High

Description

A LOLBIN run by an Office process connected to an external IP address or host, which is rarely connected to from the organization.

Attacker's Goals

Beacon to C2 server and/or exfiltrate data.

Investigative actions

Check whether the process was injected or otherwise subverted for malicious use.

A curl process connected to a rare external host

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Application Layer Protocol (T1071)
Severity	Informational

Description

A curl process connected to an external host name or directly to an IP address, which are rarely connected to from the organization.

Attacker's Goals

Beacon to C2 server and/or exfiltrate data.

Investigative actions

Check whether the process was injected or otherwise subverted for malicious use.

VSCode extension process connected to a rare external host

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Application Layer Protocol (T1071)
Severity	Low

Description

A VSCode extension connected to an external IP address or host, which is rarely connected to from the organization.

Attacker's Goals

Beacon to C2 server and/or exfiltrate data.

Investigative actions

Check whether the process was injected or otherwise subverted for malicious use.

UNIX LOLBIN process connected to a rare external host

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Application Layer Protocol (T1071)
Severity	Low

Description

A UNIX LOLBIN connected to an external IP address or host, which is rarely connected to from the organization.

Attacker's Goals

Beacon to C2 server and/or exfiltrate data.

Investigative actions

Check whether the process was injected or otherwise subverted for malicious use.

30.260 | Unusual AWS user added to group

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	- Requires: - XDR Agent
Detection Modules	
Detector Tags	Kubernetes - AGENT, Containers
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation (T1098)
Severity	Low

Description

AWS user added to AWS group, possibly to elevate privileges and gain more access to resources.

Attacker's Goals

Gain persistence and elevate privileges.

Investigative actions

- Check if the action was done using an automation service.
- Check if there are any other suspicious activities originated from the same machine/executing user.

Variations

Unusual AWS user added to group from a Kubernetes Pod

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation (T1098)
Severity	Low

Description

AWS user added to AWS group, possibly to elevate privileges and gain more access to resources.

Attacker's Goals

Gain persistence and elevate privileges.

Investigative actions

- Check if the action was done using an automation service.
  Check if there are any other suspicious activities originated from the same machine/executing user.

30.261 | Uncommon RDP connection

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	N/A (single event)
Deduplication Period	1 Hour
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Services: Remote Desktop Protocol (T1021.001)
Severity	Informational

Description

RDP is used by attackers to laterally move to new hosts. Standard processes do not usually implement RDP on their own, and attackers might inject or tunnel using a non-standard process.

Attacker's Goals

Use an account that was possibly compromised to gain access to the network.

Investigative actions

Validate if the process is a legitimate IT software.
Verify if the process is known to be malicious.

Look into actions done on the remote host.

30.262 | Rare Unix process divided files by size

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Hour
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Data Transfer Size Limits (T1030)
Severity	Informational

Description

A file was divided into sub-files by size limit by a rare process.

Attacker's Goals

This may assist an attacker to exfiltrate sensitive information.

Investigative actions

- Check if the user normally uses this capability.
- Check if this capability is used often on this endpoint.

30.263 | Suspicious Certutil AD CS contact

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Discovery (TA0007) Credential Access (TA0006)
ATT&CK Technique	- System Service Discovery (T1007) Steal or Forge Authentication Certificates (T1649)
Severity	Low

Description

A suspicious occurrence of Certutil attempted to contact the AD CS Request Interface.

Attacker's Goals

- An attacker might look for AD CS servers, certificate templates or request certificates.
- With the wrong setting or loose vulnerable templates or enabled enrollment, the attacker will be able to authenticate as users on the network.

Investigative actions

Look at further action done by the user.

Investigate whether other non-standard operations were done regarding the AD CS.

Variations

Suspicious Certutil AD CS Admin Interface contact

Synopsis

ATT&CK Tactic	Discovery (TA0007) Credential Access (TA0006)
ATT&CK Technique	System Service Discovery (T1007) Steal or Forge Authentication Certificates (T1649)
Severity	Medium

Description

A suspicious occurrence of Certutil attempted to contact the AD CS Admin Interface.

Attacker's Goals

An attacker might look for AD CS servers, certificate templates or request certificates.
With the wrong setting or loose vulnerable templates or enabled enrollment, the attacker will be able to authenticate as users on the network.

Investigative actions

Look at further action done by the user.

- Investigate whether other non-standard operations were done regarding the AD CS.

30.264 | Copy a user's GnuPG directory with rsync

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	- Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials: Private Keys (T1552.004)
Severity	Low

Description

Copy a user's GnuPG (.gnupg) directory on to a staging folder using the 'find' and 'rsync' commands.

Attacker's Goals

Adversaries may use rsync to exfiltrate secrets.

Investigative actions

Check whether the executing process is benign, and if this was a desired behavior as part of its normal execution flow.

30.265 | Adding execution privileges

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	Kubernetes - AGENT, Containers

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Command and Scripting Interpreter: Unix Shell (T1059.004)
Severity	Informational

Description

Using chmod to add execution privileges to a script before running it.

Attacker's Goals

Attackers may use the chmod commands for scripts or binary execution.

Investigative actions

- Verify that this isn't IT activity.
  Look for other hosts executing similar commands.

Variations

Adding execution privileges in a Kubernetes pod

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Command and Scripting Interpreter: Unix Shell (T1059.004)
Severity	Informational

Description

Using chmod to add execution privileges to a script before running it.

Attacker's Goals

Attackers may use the chmod commands for scripts or binary execution.

Investigative actions

- Verify that this isn't IT activity.
  Look for other hosts executing similar commands.

30.266 | Execution of the Hydra Linux password brute-force tool

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	Kubernetes - AGENT, Containers
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force: Password Guessing (T1110.001)

Severity	Medium

Description

Attackers may use brute-force techniques to gain access to accounts when usernames and/or passwords are unknown.

Attacker's Goals

The attacker attempts to gain access to the account or host.

Investigative actions

- Verify that the commands are executed from a trusted source.
- Audit the victim account or host and verify that they haven't been compromised.

Variations

Execution of the Hydra Linux password brute-force tool from a Kubernetes pod

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force: Password Guessing (T1110.001)
Severity	Medium

Description

Attackers may use brute-force techniques to gain access to accounts when usernames and/or passwords are unknown.

Attacker's Goals

The attacker attempts to gain access to the account or host.

Investigative actions

Verify that the commands are executed from a trusted source.

- Audit the victim account or host and verify that they haven't been compromised.

30.267 | Suspicious dump of ntds.dit using Shadow Copy with ntdsutil/vssadmin

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	OS Credential Dumping: NTDS (T1003.003)
Severity	High

Description

Attackers may attempt to dump the ntds.dit file, which stores all Active Directory account information, to later extract passwords and hashes from it.

Attacker's Goals

Retrieve Active Directory data, to perform malicious activities such as lateral movement.

Investigative actions

Check the initiator process for additional suspicious activity.

30.268 | Suspicious module load using direct syscall

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	▮ Requires: - XDR Agent
Detection Modules	
Detector Tags	Direct Syscall Analytics
ATT&CK Tactic	Execution (TA0002)

ATT&CK Technique	Native API (T1106)
Severity	Low

Description

A module was loaded to a process using a direct syscall.

Attacker's Goals

An attacker might try to use direct syscalls to evade detection and load a malicious module to a legitimate program.

Investigative actions

- Investigate the direct syscall mapped image to verify if it is malicious.
- Investigate the loaded module to verify if it is malicious.

Variations

A module was loaded to an unsigned process by using a direct syscall

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Native API (T1106)
Severity	Medium

Description

A module was loaded to an unsigned process using a direct syscall.

Attacker's Goals

An attacker might try to use direct syscalls to evade detection and load a malicious module to a legitimate program.

Investigative actions

- Investigate the direct syscall mapped image to verify if it is malicious.
- Investigate the loaded module to verify if it is malicious.

30.269 | Globally uncommon root domain from a signed process

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	Global Anomaly Analytics
ATT&CK Tactic	Defense Evasion (TA0005) Command and Control (TA0011)
ATT&CK Technique	System Binary Proxy Execution (T1218) Application Layer Protocol (T1071)
Severity	Low

Description

A signed process connected to an external domain that, on a global level, it usually doesn't connect to.

Attacker's Goals

Attackers may use various methods to execute code from a context of a signed process to avoid detection.

Investigative actions

Check the destination domain reputation.

Check if the actor process loaded a suspicious dll before the alert.
- Check if the actor process was injected before the alert.
- Check if the process execution and connections are legitimate.

Variations

Globally uncommon root domain from an injected thread in a signed process

Synopsis

ATT&CK Tactic	- Defense Evasion (TA0005) - Command and Control (TA0011)
ATT&CK Technique	- System Binary Proxy Execution (T1218) - Application Layer Protocol (T1071) Process Injection (T1055)
Severity	High

Description

An injected thread in a signed process connected to an external domain that, on a global level, it usually doesn't connect to.

Attacker's Goals

Attackers may use various methods to execute code from a context of a signed process to avoid detection.

Investigative actions

- Check the destination domain reputation.
- Check if the actor process loaded a suspicious dll before the alert.
  Check if the actor process was injected before the alert.

  Check if the process execution and connections are legitimate.

Globally uncommon root domain from a signed process

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005) Command and Control (TA0011)
ATT&CK Technique	System Binary Proxy Execution (T1218) Application Layer Protocol (T1071)
Severity	High

Description

A signed process connected to an external domain that, on a global level, it usually doesn't connect to.

Attacker's Goals

Attackers may use various methods to execute code from a context of a signed process to avoid detection.

Investigative actions

- Check the destination domain reputation.
  Check if the actor process loaded a suspicious dll before the alert.
  Check if the actor process was injected before the alert.

  Check if the process execution and connections are legitimate.

Globally uncommon root domain from a signed process

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005) Command and Control (TA0011)
ATT&CK Technique	System Binary Proxy Execution (T1218) Application Layer Protocol (T1071)
Severity	High

Description

A signed process connected to an external domain that, on a global level, it usually doesn't connect to.

Attacker's Goals

Attackers may use various methods to execute code from a context of a signed process to avoid detection.

Investigative actions

- Check the destination domain reputation.
- Check if the actor process loaded a suspicious dll before the alert.
  Check if the actor process was injected before the alert.
  Check if the process execution and connections are legitimate.

Globally uncommon root domain from a signed process

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005) Command and Control (TA0011)
ATT&CK Technique	System Binary Proxy Execution (T1218) Application Layer Protocol (T1071)

Severity	Medium

Description

A signed process connected to an external domain that, on a global level, it usually doesn't connect to.

Attacker's Goals

Attackers may use various methods to execute code from a context of a signed process to avoid detection.

Investigative actions

- Check the destination domain reputation.
- Check if the actor process loaded a suspicious dll before the alert.
- Check if the actor process was injected before the alert.
- Check if the process execution and connections are legitimate.

30.270 | Stored credentials exported using credwiz.exe

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	- Requires: - XDR Agent

Detection Modules	
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Credentials from Password Stores (T1555)
Severity	Low

Description

Attackers may abuse the credwiz tool to export stored accounts.

Attacker's Goals

An attacker may attempt to gain higher privileges.

Investigative actions

Check whether the executing process is benign, and if this was a desired behavior as part of its normal execution flow.

Variations

Stored credentials exported using credwiz.exe using keymgr.dll's KRShowKeyMgr function

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Credentials from Password Stores (T1555)
Severity	Medium

Description

Attackers may abuse the credwiz tool to export stored accounts using keymgr.dll's KRShowKeyMgr function.

Attacker's Goals

An attacker may attempt to gain higher privileges.

Investigative actions

Check whether the executing process is benign, and if this was a desired behavior as part of its normal execution flow.

Stored credentials exported using credwiz.exe over RDP

Synopsis

ATT&CK Tactic	Credential Access (TA0006) Lateral Movement (TA0008)
ATT&CK Technique	Credentials from Password Stores (T1555) Remote Services: Remote Desktop Protocol (T1021.001)
Severity	Low

Description

Attackers may abuse the credwiz tool to export stored accounts over RDP.

Attacker's Goals

An attacker may attempt to gain higher privileges.

Investigative actions

Check whether the executing process is benign, and if this was a desired behavior as part of its normal execution flow.

Stored credentials exported using credwiz.exe with a built-in Windows tool

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Credentials from Password Stores (T1555)
Severity	Low

Description

Attackers may abuse the credwiz tool to export stored accounts with a built-in Windows tool.

Attacker's Goals

An attacker may attempt to gain higher privileges.

Investigative actions

Check whether the executing process is benign, and if this was a desired behavior as part of its normal execution flow.

30.271 | A process was executed with a command line obfuscated by Unicode character substitution

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	6 Hours

Required Data	- Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Obfuscated Files or Information (T1027)
Severity	Medium

Description

A process was executed with a command line obfuscated by Unicode character substitution.

Attacker's Goals

Hide its action and avoid detection.

Investigative actions

Check whether the executing process is benign, and if this was a desired behavior as part of its normal execution flow.

30.272 | Possible malicious .NET compilation started by a commonly abused process

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	- Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Obfuscated Files or Information: Compile After Delivery (T1027.004)
Severity	Medium

Description

Attackers may use csc.exe to compile payloads on a compromised machine.

Attacker's Goals

Compile payloads on the host to evade detection.

Investigative actions

- Investigate the payload being compiled.
- Check whether the executing process is benign, and if this was a desired behavior as part of its normal execution flow.

30.273 | Uncommon kernel module load

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	Kubernetes - AGENT, Containers
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Rootkit (T1014)
Severity	Informational

Description

Loading of a kernel module using the modprobe command.

Attacker's Goals

Gain persistence using the kernel module.

Investigative actions

Verify that this isn't IT activity.

- Look for other hosts executing similar commands.

Variations

Uncommon kernel module load in a Kubernetes pod

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Rootkit (T1014)
Severity	Informational

Description

Loading of a kernel module using the modprobe command.

Attacker's Goals

Gain persistence using the kernel module.

Investigative actions

Verify that this isn't IT activity.

Look for other hosts executing similar commands.

30.274 | Microsoft Office injects code into a process

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	Injection Analytics
ATT&CK Tactic	Initial Access (TA0001) Defense Evasion (TA0005)
ATT&CK Technique	Phishing: Spearphishing Attachment (T1566.001) Process Injection (T1055)
Severity	Low

Description

An attacker may inject payloads into processes via Microsoft Office. While legitimate in certain cases, code injection can also be used in malicious ways.

Attacker's Goals

An attacker attempts to gain code execution via a phishing document.
Attackers may inject code into processes to evade process-based defenses, as well as possibly elevate privileges.

Investigative actions

Check the source of the document (received by mail or loaded locally).

- Check whether the injecting process is benign, and if this was a desired behavior as part of its normal execution flow.

Variations

Unsigned Microsoft Office injects code into a process

Synopsis

ATT&CK Tactic	- Initial Access (TA0001) - Defense Evasion (TA0005)
ATT&CK Technique	- Phishing: Spearphishing Attachment (T1566.001) - Process Injection (T1055) Masquerading: Match Legitimate Name or Location (T1036.005)
Severity	High

Description

An attacker may inject payloads into processes via Microsoft Office. While legitimate in certain cases, code injection can also be used in malicious ways.

Attacker's Goals

- An attacker attempts to gain code execution via a phishing document.
Attackers may inject code into processes to evade process-based defenses, as well as possibly elevate privileges.

Investigative actions

Check the source of the document (received by mail or loaded locally).

- Check whether the injecting process is benign, and if this was a desired behavior as part of its normal execution flow.

Microsoft Office injects code into a process to a non-standard PE section

Synopsis

ATT&CK Tactic	Initial Access (TA0001) Defense Evasion (TA0005)
ATT&CK Technique	Phishing: Spearphishing Attachment (T1566.001) Process Injection (T1055)
Severity	High

Description

An attacker may inject payloads into processes via Microsoft Office. While legitimate in certain cases, code injection can also be used in malicious ways.

Attacker's Goals

An attacker attempts to gain code execution via a phishing document.

Attackers may inject code into processes to evade process-based defenses, as well as possibly elevate privileges.

Investigative actions

- Check the source of the document (received by mail or loaded locally).
  Check whether the injecting process is benign, and if this was a desired behavior as part of its normal execution flow.

Microsoft Office injects code into a process to an undeclared memory page

Synopsis

ATT&CK Tactic	- Initial Access (TA0001) - Defense Evasion (TA0005)
ATT&CK Technique	- Phishing: Spearphishing Attachment (T1566.001) - Process Injection (T1055)

Severity	Medium

Description

An attacker may inject payloads into processes via Microsoft Office. While legitimate in certain cases, code injection can also be used in malicious ways.

Attacker's Goals

- An attacker attempts to gain code execution via a phishing document.
  Attackers may inject code into processes to evade process-based defenses, as well as possibly elevate privileges.

Investigative actions

  Check the source of the document (received by mail or loaded locally).
- Check whether the injecting process is benign, and if this was a desired behavior as part of its normal execution flow.

Microsoft Office injects code into a process from an unsigned process

Synopsis

ATT&CK Tactic	Initial Access (TA0001) Defense Evasion (TA0005)
ATT&CK Technique	Phishing: Spearphishing Attachment (T1566.001) Process Injection (T1055)
Severity	Medium

Description

An attacker may inject payloads into processes via Microsoft Office. While legitimate in certain cases, code injection can also be used in malicious ways.

Attacker's Goals

An attacker attempts to gain code execution via a phishing document.

- Attackers may inject code into processes to evade process-based defenses, as well as possibly elevate privileges.

Investigative actions

Check the source of the document (received by mail or loaded locally).

Check whether the injecting process is benign, and if this was a desired behavior as part of its normal execution flow.

Microsoft Office macro-enabled spreadsheet (XLSM) injects code into a process

Synopsis

ATT&CK Tactic	Initial Access (TA0001) ▮ Defense Evasion (TA0005)
ATT&CK Technique	Phishing: Spearphishing Attachment (T1566.001) ▮ Process Injection (T1055)
Severity	Medium

Description

An attacker may inject payloads into processes via Microsoft Office. While legitimate in certain cases, code injection can also be used in malicious ways.

Attacker's Goals

An attacker attempts to gain code execution via a phishing document.

- Attackers may inject code into processes to evade process-based defenses, as well as possibly elevate privileges.

Investigative actions

Check the source of the document (received by mail or loaded locally).

Check whether the injecting process is benign, and if this was a desired behavior as part of its normal execution flow.

30.275 | WebDAV drive mounted from net.exe over HTTPS

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Exfiltration Over Alternative Protocol (T1048)
Severity	Informational

Description

Attackers may mount a WebDAV drive over HTTPS to upload files to and download files from a compromised machine.

Attacker's Goals

Attackers might use WebDAV as a C&C or exfiltration channel to evade detection and firewall rules.

Investigative actions

- Check whether the initiator process is benign or normal for the host and/or user performing it.
Check whether additional malicious commands were executed from the same process.

30.276 | Uncommon user management via net.exe

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Discovery (TA0007) Persistence (TA0003)

ATT&CK Technique	- Account Discovery (T1087) - Create Account (T1136)
Severity	Informational

Description

The net.exe command is used to add, delete, and otherwise manage the users on a computer. Adversaries may attempt to use the command to discover or add local and domain user accounts.

Attacker's Goals

Attackers may attempt to use the command to discover or add local and domain user accounts. The created accounts are to gain additional access to endpoints within your network.

Investigative actions

Check whether the command line executed is benign or normal for the host and/or user performing it.

Check whether the user from the command line is an administrator or other sensitive account.

30.277 | Commonly abused process launched as a system service

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)

Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	System Services: Service Execution (T1569.002)
Severity	Informational

Description

This commonly abused host process has been launched by a services.exe parent, indicating it has been installed as a system service. This behavior can have legitimate uses, but often used by malware as a persistence mechanism.

Attacker's Goals

Attackers may use services to persist or execute commands on remote hosts.

Investigative actions

- Check whether additional malicious commands were executed from the same process.
- Verify if the command-line seems suspicious or contains malicious indicators.

30.278 | Screensaver process executed from Users or temporary

folder

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	6 Hours
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Event Triggered Execution: Screensaver (T1546.002)
Severity	Low

Description

An executable file with a screensaver extension was executed from the Users or temp folder. This is not a common behavior for screensavers and may indicate a malicious file disguised as a screensaver in the Users or temp folder.

It is recommended to further investigate the execution flow for malicious indicators.

Attacker's Goals

Gain persistence by configuring a new screensaver.

Investigative actions

Check whether the executing process (with the SCR extension) is benign, and if this was a desired behavior as part of its normal execution flow.

Variations

Screensaver process executed from Users or temporary folder by a scripting engine process

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Event Triggered Execution: Screensaver (T1546.002)
Severity	High

Description

An executable file with a screensaver extension was executed from the Users or temp folder by a scripting engine process. This is not a common behavior for screensavers and may indicate a malicious file disguised as a screensaver in the Users or temp folder.

It is recommended to further investigate the execution flow for malicious indicators.

Attacker's Goals

Gain persistence by configuring a new screensaver.

Investigative actions

Check whether the executing process (with the SCR extension) is benign, and if this was a desired behavior as part of its normal execution flow.

30.279 | Cloud Unusual Instance Metadata Service (IMDS) access

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	Cloud
Detector Tags	Kubernetes - AGENT
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials: Cloud Instance Metadata API (T1552.005)
Severity	Informational

Description

A request to cloud Instance Metadata Service (IMDS) was made by an unusual process. An attacker might exploit a web vulnerability to execute this technique.

Attacker's Goals

Extract sensitive cloud tokens to access restricted resources.

Investigative actions

- Check if a web service was exploited to execute this technique.
- Check what other commands were executed.
  Check the instance profile attached to the victim machine and its permissions, to find out which resources may be affected.

Variations

Cloud Unusual Instance Metadata Service (IMDS) access from an unusual known shell or scripting process in a Kubernetes pod

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials: Cloud Instance Metadata API (T1552.005)
Severity	Low

Description

A request to cloud Instance Metadata Service (IMDS) was made by an unusual process. An attacker might exploit a web vulnerability to execute this technique.

Attacker's Goals

Extract sensitive cloud tokens to access restricted resources.

Investigative actions

Check if a web service was exploited to execute this technique.
Check what other commands were executed.

Check the instance profile attached to the victim machine and its permissions, to find out which resources may be affected.

Cloud Unusual Instance Metadata Service (IMDS) access from an unusual known web service in a

Kubernetes pod

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials: Cloud Instance Metadata API (T1552.005)
Severity	Low

Description

A request to cloud Instance Metadata Service (IMDS) was made by an unusual process. An attacker might exploit a web vulnerability to execute this technique.

Attacker's Goals

Extract sensitive cloud tokens to access restricted resources.

Investigative actions

- Check if a web service was exploited to execute this technique.
Check what other commands were executed.
Check the instance profile attached to the victim machine and its permissions, to find out which resources may be affected.

Cloud Unusual Instance Metadata Service (IMDS) access in a Kubernetes pod

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials: Cloud Instance Metadata API (T1552.005)
Severity	Informational

Description

A request to cloud Instance Metadata Service (IMDS) was made by an unusual process. An attacker might exploit a web vulnerability to execute this technique.

Attacker's Goals

Extract sensitive cloud tokens to access restricted resources.

Investigative actions

- Check if a web service was exploited to execute this technique.
- Check what other commands were executed.
- Check the instance profile attached to the victim machine and its permissions, to find out which resources may be affected.

Cloud Unusual Instance Metadata Service (IMDS) access from an unusual known web service

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials: Cloud Instance Metadata API (T1552.005)
Severity	Low

Description

A request to cloud Instance Metadata Service (IMDS) was made by an unusual process. An attacker might exploit a web vulnerability to execute this technique.

Attacker's Goals

Extract sensitive cloud tokens to access restricted resources.

Investigative actions

- Check if a web service was exploited to execute this technique.
- Check what other commands were executed.
- Check the instance profile attached to the victim machine and its permissions, to find out which resources may be affected.

Cloud Unusual Instance Metadata Service (IMDS) access from an unusual known shell or scripting process

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials: Cloud Instance Metadata API (T1552.005)
Severity	Low

Description

A request to cloud Instance Metadata Service (IMDS) was made by an unusual process. An attacker might exploit a web vulnerability to execute this technique.

Attacker's Goals

Extract sensitive cloud tokens to access restricted resources.

Investigative actions

Check if a web service was exploited to execute this technique.

Check what other commands were executed.

- Check the instance profile attached to the victim machine and its permissions, to find out which resources may be affected.

Cloud Unusual internet-facing Instance Metadata Service (IMDS) access

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials: Cloud Instance Metadata API (T1552.005)
Severity	Low

Description

A request to cloud Instance Metadata Service (IMDS) was made by an unusual process. An attacker might exploit a web vulnerability to execute this technique.

Attacker's Goals

Extract sensitive cloud tokens to access restricted resources.

Investigative actions

- Check if a web service was exploited to execute this technique.
- Check what other commands were executed.
- Check the instance profile attached to the victim machine and its permissions, to find out which resources may be affected.

30.280 | Commonly abused AutoIT script connects to an external domain

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: XDR Agent
Detection Modules	

Detector Tags	
ATT&CK Tactic	Exfiltration (TA0010) Execution (TA0002)
ATT&CK Technique	Command and Scripting Interpreter: AutoHotKey & AutoIT (T1059.010) Automated Exfiltration (T1020)
Severity	Medium

Description

AutoIT scripts have legitimate uses, but are often abused by malware to execute in a signed process context.

Attacker's Goals

Communicate with malware running on your network to control malware activities, perform software updates on the malware, or to take inventory of infected machines.

Investigative actions

- AutoIT scripts have legitimate uses, but are often abused by malware to execute in a signed process context.
  Identify the process contacting the remote domain and determine whether the traffic is malicious.

30.281 | A TCP stream was created directly in a shell

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Command and Scripting Interpreter (T1059)
Severity	Medium

Description

Attackers may create a TCP stream using the shell command line to generate a reverse shell, enabling remote access to the endpoint.

Attacker's Goals

Attackers may use this device file to create sockets though shell commands as part of a reverse shell.

Investigative actions

Review the command line used.

Search for the corresponding network event.

- Check the prevalence of the target IP/domain.

30.282 | PowerShell runs suspicious base64-encoded commands

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Command and Scripting Interpreter: PowerShell (T1059.001)
Severity	Medium

Description

Running PowerShell with a base64-encoded payload in the command line is often used by attackers to evade detection.

Attacker's Goals

Run code to perform actions or download other malicious programs.

Investigative actions

- Check if the initiator process is malicious.
- Check for other operations by the PowerShell instance.

30.283 | Possible RDP session hijacking using tscon.exe

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	- Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Service Session Hijacking: RDP Hijacking (T1563.002)

Severity	Medium

Description

The executable tscon.exe can be used to hijack other sessions on the same computer. The attacker may use another user's credentials to proceed with the lateral movement or disguise the activity.

Attacker's Goals

Attackers might hijack existing sessions on the same host to gain access to private data or leverage the logged-in user credentials to laterally move across the network.

Investigative actions

Verify if the executing process is suspicious.
Investigate if the interactive user did any more suspicious or malicious actions.

30.284 | Remote PsExec-like command execution

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent

Detection Modules	
Detector Tags	Impacket Analytics
ATT&CK Tactic	Lateral Movement (TA0008) Execution (TA0002)
ATT&CK Technique	Remote Services (T1021) System Services: Service Execution (T1569.002) Lateral Tool Transfer (T1570)
Severity	Informational

Description

A remotely triggered service initiated a command execution in a PsExec-like manner by a host that rarely triggers services to other remote hosts.

Attacker's Goals

Perform lateral movement to new hosts to expand the foothold within a network.

Investigative actions

- Investigate the processes being spawned on the host for malicious activities.
- Correlate the RPC call from the source host and understand which software initiated it.

Variations

Remote PsExec-like LOLBIN command execution from an unsigned non-standard PsExec service

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008) Execution (TA0002)

ATT&CK Technique	▌ Remote Services (T1021) ▌ System Services: Service Execution (T1569.002) Lateral Tool Transfer (T1570)
Severity	High

Description

A remotely triggered service initiated a command execution in a PsExec-like manner by a host that rarely triggers services to other remote hosts.

Attacker's Goals

Perform lateral movement to new hosts to expand the foothold within a network.

Investigative actions

Investigate the processes being spawned on the host for malicious activities.
Correlate the RPC call from the source host and understand which software initiated it.

Remote PsExec-like LOLBIN command execution from a signed non-standard PsExec service

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008) ▌ Execution (TA0002)
ATT&CK Technique	Remote Services (T1021) ▌ System Services: Service Execution (T1569.002) ▌ Lateral Tool Transfer (T1570)
Severity	Medium

Description

A remotely triggered service initiated a command execution in a PsExec-like manner by a host that rarely triggers services to other remote hosts.

Attacker's Goals

Perform lateral movement to new hosts to expand the foothold within a network.

Investigative actions

- Investigate the processes being spawned on the host for malicious activities.
Correlate the RPC call from the source host and understand which software initiated it.

Remote PsExec-like command execution from an unsigned non-standard PsExec service

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008) Execution (TA0002)
ATT&CK Technique	Remote Services (T1021) System Services: Service Execution (T1569.002) Lateral Tool Transfer (T1570)
Severity	Medium

Description

A remotely triggered service initiated a command execution in a PsExec-like manner by a host that rarely triggers services to other remote hosts.

Attacker's Goals

Perform lateral movement to new hosts to expand the foothold within a network.

Investigative actions

- Investigate the processes being spawned on the host for malicious activities.
- Correlate the RPC call from the source host and understand which software initiated it.

Remote PsExec-like command execution from a signed non-standard PsExec service

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008) Execution (TA0002)
ATT&CK Technique	Remote Services (T1021) System Services: Service Execution (T1569.002) Lateral Tool Transfer (T1570)
Severity	Low

Description

A remotely triggered service initiated a command execution in a PsExec-like manner by a host that rarely triggers services to other remote hosts.

Attacker's Goals

Perform lateral movement to new hosts to expand the foothold within a network.

Investigative actions

- Investigate the processes being spawned on the host for malicious activities.
- Correlate the RPC call from the source host and understand which software initiated it.

Remote PsExec command execution

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008) Execution (TA0002)
ATT&CK Technique	Remote Services (T1021) System Services: Service Execution (T1569.002) Lateral Tool Transfer (T1570)
Severity	Low

Description

A remotely triggered service initiated a command execution in a PsExec-like manner by a host that rarely triggers services to other remote hosts.

Attacker's Goals

Perform lateral movement to new hosts to expand the foothold within a network.

Investigative actions

Investigate the processes being spawned on the host for malicious activities.

Correlate the RPC call from the source host and understand which software initiated it.

30.285 | Rare Unsigned Process Spawned by Office Process Under Suspicious Directory

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	User Execution (T1204)
Severity	Low

Description

Microsoft Office executed an unsigned process in a suspicious directory. This behavior is common with malicious macros.

Attacker's Goals

Attackers execute commands after infiltrating by using phishing or exploiting a vulnerability in an office.

Investigative actions

Investigate the executed process.
Investigate the document/email that initiated it.

30.286 | A service was disabled

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day

Required Data	- Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Service Stop (T1489)
Severity	Informational

Description

A service was disabled abnormally. This may be performed by malicious actors in an attempt to evade detection or limit functionality.

Attacker's Goals

- Evade detection by certain programs.
- Limit the functionality and availability of systems, services, and network resources.

Investigative actions

- Check if the disabled service could potentially threaten a malicious actor, or if holds a critical role.
- Investigate the disabling process to understand if it performed other suspicious actions.

Variations

A service was disabled without using the ServiceControlManager RPC interface

Synopsis

ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Service Stop (T1489)
Severity	Informational

Description

A service was disabled abnormally through the registry. This may be performed by malicious actors in an attempt to evade detection or limit functionality.

Attacker's Goals

- Evade detection by certain programs.
  Limit the functionality and availability of systems, services, and network resources.

Investigative actions

Check if the disabled service could potentially threaten a malicious actor, or if holds a critical role.

- Investigate the disabling process to understand if it performed other suspicious actions.

An injected process performed an uncommon service deactivation

Synopsis

ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Service Stop (T1489)
Severity	Informational

Description

A service was disabled abnormally. This may be performed by malicious actors in an attempt to evade detection or limit functionality.

Attacker's Goals

Evade detection by certain programs.
Limit the functionality and availability of systems, services, and network resources.

Investigative actions

- Check if the disabled service could potentially threaten a malicious actor, or if holds a critical role.
- Investigate the disabling process to understand if it performed other suspicious actions.

An unsigned process performed an uncommon service deactivation

Synopsis

ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Service Stop (T1489)
Severity	Low

Description

A service was disabled abnormally. This may be performed by malicious actors in an attempt to evade detection or limit functionality.

Attacker's Goals

- Evade detection by certain programs.
- Limit the functionality and availability of systems, services, and network resources.

Investigative actions

Check if the disabled service could potentially threaten a malicious actor, or if holds a critical role.

Investigate the disabling process to understand if it performed other suspicious actions.

30.287 | Globally uncommon IP address by a common process (sha256)

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	Global Anomaly Analytics
ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Application Layer Protocol (T1071)
Severity	Informational

Description

A process with a common sha256 connected to an external IP address that, on a global level, it usually doesn't connect to.

Attacker's Goals

Attackers may use various methods to execute code from a context of another process to avoid detection.

Investigative actions

- Check the destination IP address reputation.
  Check if the actor process loaded a suspicious DLL before the alert.
  Check if the actor process was injected before the alert.

  Check if the process execution and connections are legitimate.

Variations

Globally uncommon IP address by a common process (sha256) from an injected thread

Synopsis

ATT&CK Tactic	Command and Control (TA0011) Defense Evasion (TA0005)
ATT&CK Technique	Application Layer Protocol (T1071) Process Injection (T1055)
Severity	High

Description

A process with a common sha256 connected to an external IP address that, on a global level, it usually doesn't connect to.

Attacker's Goals

Attackers may use various methods to execute code from a context of another process to avoid detection.

Investigative actions

- Check the destination IP address reputation.
- Check if the actor process loaded a suspicious DLL before the alert.
- Check if the actor process was injected before the alert.
- Check if the process execution and connections are legitimate.

Globally uncommon IP address by a common process (sha256) from a known vendor

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Application Layer Protocol (T1071)
Severity	Medium

Description

A process with a common sha256 connected to an external IP address that, on a global level, it usually doesn't connect to.

Attacker's Goals

Attackers may use various methods to execute code from a context of another process to avoid detection.

Investigative actions

- Check the destination IP address reputation.
- Check if the actor process loaded a suspicious DLL before the alert.
- Check if the actor process was injected before the alert.
- Check if the process execution and connections are legitimate.

Globally uncommon and very rare IP address by a common process (sha256)

Synopsis

ATT&CK Tactic	Command and Control (TA0011)

ATT&CK Technique	Application Layer Protocol (T1071)
Severity	Medium

Description

A process with a common sha256 connected to an external IP address that, on a global level, it usually doesn't connect to.

Attacker's Goals

Attackers may use various methods to execute code from a context of another process to avoid detection.

Investigative actions

- Check the destination IP address reputation.
Check if the actor process loaded a suspicious DLL before the alert.
Check if the actor process was injected before the alert.

  Check if the process execution and connections are legitimate.

Globally uncommon and a rare IP address by a common process (sha256)

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Application Layer Protocol (T1071)
Severity	Low

Description

A process with a common sha256 connected to an external IP address that, on a global level, it usually doesn't connect to.

Attacker's Goals

Attackers may use various methods to execute code from a context of another process to avoid detection.

Investigative actions

- Check the destination IP address reputation.
- Check if the actor process loaded a suspicious DLL before the alert.
- Check if the actor process was injected before the alert.
- Check if the process execution and connections are legitimate.

30.288 | Cached credentials discovery with cmdkey

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	- Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006) Discovery (TA0007)

ATT&CK Technique	- OS Credential Dumping (T1003) - Account Discovery (T1087)
Severity	Low

Description

Cmdkey is a built-in Windows tool that can cache domain user credentials for use on specific target machines, Attackers can access cached user credentials using cmdkey /list.

Attacker's Goals

Access cached user credentials.

Investigative actions

- Check the initiator process for additional suspicious activity.
- Check if the host is a shared host that multiple users' credentials can be extracted from.

Variations

The process cmdkey runs with modified name and extract cached credentials

Synopsis

ATT&CK Tactic	- Credential Access (TA0006) - Discovery (TA0007)
ATT&CK Technique	- OS Credential Dumping (T1003) - Account Discovery (T1087)
Severity	High

Description

Cmdkey is a built-in Windows tool that can cache domain user credentials for use on specific target machines, Attackers can access cached user credentials using cmdkey /list.

Attacker's Goals

Access cached user credentials.

Investigative actions

- Check the initiator process for additional suspicious activity.
  Check if the host is a shared host that multiple users' credentials can be extracted from.

Transfer cached credentials with cmdkey to other standard output

Synopsis

ATT&CK Tactic	Credential Access (TA0006) Discovery (TA0007)
ATT&CK Technique	OS Credential Dumping (T1003) Account Discovery (T1087)
Severity	Medium

Description

Cmdkey is a built-in Windows tool that can cache domain user credentials for use on specific target machines, Attackers can access cached user credentials using cmdkey /list.

Attacker's Goals

Access cached user credentials.

Investigative actions

Check the initiator process for additional suspicious activity.
- Check if the host is a shared host that multiple users' credentials can be extracted from.

30.289 | Tampering with Internet Explorer Protected Mode

configuration

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Impair Defenses: Disable or Modify Tools (T1562.001)
Severity	Informational

Description

When an add-on is running inside Protected Mode attempts to launch a broker process (or any other program), the ElevationPolicy Registry key is checked to determine how the process should be launched. Internet Explorer will run a broker process with higher rights that can use the current user's permissions to take actions that would otherwise be prohibited when rendering content inside the Protected Mode sandbox.

https://blogs.msdn.microsoft.com/ieinternals/2009/11/30/understanding-the-protected-mode-elevation-dialog/.

Attacker's Goals

- When an add-on is running inside Protected Mode attempts to launch a broker process, this key is checked to determine how the process should be launched.
  Attackers may change this value to make the process launch with higher privileges.

Investigative actions

Check whether the injecting process is benign, and if this was a desired behavior as part of its normal execution flow.

Variations

Tampering with Internet Explorer Protected Mode default configuration

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Impair Defenses: Disable or Modify Tools (T1562.001)
Severity	Medium

Description

When an add-on is running inside Protected Mode attempts to launch a broker process (or any other program), the ElevationPolicy Registry key is checked to determine how the process should be launched. Internet Explorer will run a broker process with higher rights that can use the current user's permissions to take actions that would otherwise be prohibited when rendering content inside the Protected Mode sandbox.

https://blogs.msdn.microsoft.com/ieinternals/2009/11/30/understanding-the-protected-mode-elevation-dialog/.

Attacker's Goals

When an add-on is running inside Protected Mode attempts to launch a broker process, this key is checked to determine how the process should be launched.
Attackers may change this value to make the process launch with higher privileges.

Investigative actions

- Check whether the injecting process is benign, and if this was a desired behavior as part of its normal execution flow.

Tampering with Internet Explorer Protected Mode specific app configuration

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Impair Defenses: Disable or Modify Tools (T1562.001)
Severity	Informational

Description

When an add-on is running inside Protected Mode attempts to launch a broker process (or any other program), the ElevationPolicy Registry key is checked to determine how the process should be launched. Internet Explorer will run a broker process with higher rights that can use the current user's permissions to take actions that would otherwise be prohibited when rendering content inside the Protected Mode sandbox. https://blogs.msdn.microsoft.com/ieinternals/2009/11/30/understanding-the-protected-mode-elevation-dialog/.

Attacker's Goals

- When an add-on is running inside Protected Mode attempts to launch a broker process, this key is checked to determine how the process should be launched.
Attackers may change this value to make the process launch with higher privileges.

Investigative actions

Check whether the injecting process is benign, and if this was a desired behavior as part of its normal execution flow.

30.290 | Uncommon routing table listing via route.exe

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Hour
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	System Network Configuration Discovery (T1016)
Severity	Low

Description

The route.exe command is used to display and modify entries in the local IP routing table. Adversaries may attempt to use the command to discover remote systems they could compromise.

Attacker's Goals

Attackers can attempt to use the command to discover remote systems they could compromise.

Investigative actions

Check whether the command line executed is benign or normal for the host and/or user performing it (e.g. an IT script).

30.291 | Suspicious authentication package registered

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	14 Days
Required Data	- Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)

ATT&CK Technique	Boot or Logon Autostart Execution: Authentication Package (T1547.002)
Severity	Medium

Description

The endpoint registered a suspicious authentication package, which may be used to gain persistence on the host by loading libraries into the time management service.

Attacker's Goals

Gain persistence using the legitimate Windows authentication package mechanism, which loads libraries into Windows services.

Investigative actions

- Verify if the registered library is malicious.
  Check if the installing software is a malicious binary.
  Check for any suspicious network activity from "lsass.exe".

30.292 | The CA policy EditFlags was queried

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day

Required Data	- Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Medium

Description

The CA policy EditFlags was queried.

Attacker's Goals

Querying this registry value can indicate an attacker is looking for an enabled

EDITF_ATTRIBUTESUBJECTALTNAME2 flag.

- When this flag is enabled, it allows users to request certificates with a Subject Alternate Name(SAN).
  This can allow an attacker to obtain a certificate with higher privileges.

Investigative actions

Check if the action was allowed by the user.
Monitor certificate enrollments with Subject Alternate Names.

Check for unusual high privilege users certificate authentications.

30.293 | A Possible crypto miner was detected on a host

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Palo Alto Networks Platform Logs OR ▯ XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Resource Hijacking (T1496)
Severity	Medium

Description

The host produced traffic consistent with the crypto mining.

Attacker's Goals

Abuse resources to mine crypto coins.

Investigative actions

- Check the host for crypto mining client software.
- Look for differences in the resource consumption from this host.
  Examine the client's network traffic for suspicious domain affiliated with mining or mining pools.

30.294 | Suspicious systemd timer activity

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Execution (TA0002) Persistence (TA0003) Privilege Escalation (TA0004)

ATT&CK Technique	Scheduled Task/Job: Systemd Timers (T1053.006)
Severity	Low

Description

Suspicious systemd timer activity, which may indicate an attempt to establish persistence.

Attacker's Goals

An adversary may use systemd timers to execute malicious code at system startup or on a scheduled basis for persistence.

Investigative actions

Check the systemd timer file change and try to understand the impact of the systemd timers change.

30.295 | NTLM Brute Force on a Service Account

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
Deduplication Period	1 Day
Required Data	Requires: ▯ XDR Agent

Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force (T1110)
Severity	Low

Description

This may indicate a NTLM brute-force attack.

Attacker's Goals

The attacker attempts to gain access to the service accounts.

Investigative actions

Verify any successful authentication by the user account referenced by the alert, as these can indicate the attacker managed to guess the credentials.

30.296 | Possible TGT reuse from different hosts (pass the ticket)

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Hours

Deduplication Period	1 Day
Required Data	Requires: • XDR Agent
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Use Alternate Authentication Material: Pass the Ticket (T1550.003)
Severity	Informational

Description

We observed two different hosts sending TGS using the same TGT. This may indicate a TGT was stolen and passed to another host.

Attacker's Goals

Lateral movement using stolen user-account credentials.

Investigative actions

Check if the mentioned hosts are not the same, and investigate if the ticket was stolen from one of them.

Variations

TGT reuse from different hosts (pass the ticket)

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Use Alternate Authentication Material: Pass the Ticket (T1550.003)
Severity	Low

Description

We observed two different hosts sending TGS using the same TGT. This may indicate a TGT was stolen and passed to another host.

Attacker's Goals

Lateral movement using stolen user-account credentials.

Investigative actions

Check if the mentioned hosts are not the same, and investigate if the ticket was stolen from one of them.

30.297 | Multiple Weakly-Encrypted Kerberos Tickets Received

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
Deduplication Period	1 Hour

Required Data	- Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Steal or Forge Kerberos Tickets: Kerberoasting (T1558.003)
Severity	Low

Description

A user accessed a number of services associated with user accounts in the 10 minutes leading to the alert, generating a number of weakly encrypted Kerberos TGS (ticket granting service) tickets that is significantly larger than the number of weakly encrypted TGS tickets received by that user in the 30 days leading to the alert.
Services associated with user accounts are a common target for Kerberoasting due to default weak encryption.

Attacker's Goals

Crack account credentials by obtaining easy-to-crack Kerberos tickets.

Investigative actions

Check who used the host at the time of the alert, to rule out a benign service or tool accessing those services.

30.298 | Random-Looking Domain Names

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Day
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Dynamic Resolution: Domain Generation Algorithms (T1568.002)
Severity	Medium

Description

The endpoint performed DNS lookups to an excessively large number of apparently random root domain names. This alert might be symptomatic of malware that is trying to connect to its command and control (C2) servers.

The attacker's C2 server runs on one or more domains that can eventually be identified and blacklisted. To avoid this, malware will sometimes use Domain Generation Algorithms (DGA) that produce many unique, random-looking domain names every day. Because only a few of these domains are ever registered, the installed malware must blindly try to access each generated domain name in an effort to locate an active one, which may also trigger the Failed DNS alert.

Attacker's Goals

Communicate with malware running on your network for controlling malware activities, performing software updates on the malware, or for taking inventory of infected machines.

Investigative actions

- Make sure your DNS servers are not misconfigured and are responsive. This detector assumes that most DNS lookups succeed, and will only raise an alert when it sees many failed lookups. Misconfigured or unresponsive DNS servers can result in a false positive. Make sure you do not have external domains configured as internal domains. This can result in clients attempting to (for example) resolve google.com.local first, before resolving google.com. This can result in a false positive for this alert.
- Ensure that the endpoint is configured properly for your DNS servers. Make sure it is configured to use the correct DNS IP address, and that the IP address is not for a firewalled DNS server. Misconfigured DNS clients can result in many failed lookups, which will result in a false positive for this alert.
- Make sure the endpoint is not a DNS, Proxy, NAT or VPN gateway server. If these have been misdetected by Cortex XDR Analytics, then their ordinary operations can trigger this alert.

30.299 | Download pattern that resembles Peer to Peer traffic

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	30 Minutes
Deduplication Period	1 Day

Required Data	- Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Command and Control (TA0011) - Initial Access (TA0001)
ATT&CK Technique	Application Layer Protocol (T1071) - Non-Standard Port (T1571) - Trusted Relationship (T1199) Phishing (T1566)
Severity	Informational

Description

A possible P2P protocol was spotted from an internal host.

Attacker's Goals

An attacker may use peer-to-peer communication to gain initial access, as a C&C tool, or an exfiltration tool.

Investigative actions

- confirm that the port accessed is a P2P port/ is run by a P2P application.
- View the downloaded content and determine it's not malicious.
  Check for large uploads from this host and check for sensitive information that might not be required on the host.

30.300 | Remote account enumeration

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Discovery (TA0007) Credential Access (TA0006)
ATT&CK Technique	Account Discovery (T1087) Brute Force (T1110)
Severity	Informational

Description

Multiple non-existing accounts failed to remotely log in to a host in a short period of time.

This may indicate an attacker is trying to remotely enumerate accounts.

Attacker's Goals

Discover valid accounts to gain credentials.

Investigative actions

Check if the login attempts were part of a legitimate misunderstanding of the system or part of an attack.

Variations

Suspicious Remote domain account enumeration

Synopsis

ATT&CK Tactic	- Discovery (TA0007) - Credential Access (TA0006)
ATT&CK Technique	- Account Discovery (T1087) - Brute Force (T1110)
Severity	Medium

Description

Multiple non-existing accounts failed to remotely log in to a host in a short period of time.

This may indicate an attacker is trying to remotely enumerate accounts.

Attacker's Goals

Discover valid accounts to gain credentials.

Investigative actions

Check if the login attempts were part of a legitimate misunderstanding of the system or part of an attack.

Remote account enumeration on domain accounts

Synopsis

ATT&CK Tactic	Discovery (TA0007) Credential Access (TA0006)
ATT&CK Technique	Account Discovery (T1087) Brute Force (T1110)
Severity	Low

Description

Multiple non-existing accounts failed to remotely log in to a host in a short period of time. This may indicate an attacker is trying to remotely enumerate accounts.

Attacker's Goals

Discover valid accounts to gain credentials.

Investigative actions

Check if the login attempts were part of a legitimate misunderstanding of the system or part of an attack.

30.301 | Abnormal RDP connections to multiple hosts

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	5 Hours

Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	NDR Lateral Movement Analytics
ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Services: Remote Desktop Protocol (T1021.001)
Severity	Informational

Description

The endpoint attempted to initiate rare RDP connections to multiple hosts.

Attacker's Goals

- Attackers may attempt to move laterally over the network by using compromised accounts or machines to connect to remote hosts using the RDP protocol.

Investigative actions

Inspect the legitimacy of the user which the RDP made the connection with.

Verify that this isn't IT activity.

Variations

Abnormal RDP connections to multiple hosts

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Services: Remote Desktop Protocol (T1021.001)
Severity	Low

Description

The endpoint attempted to initiate rare RDP connections to multiple hosts.

Attacker's Goals

- Attackers may attempt to move laterally over the network by using compromised accounts or machines to connect to remote hosts using the RDP protocol.

Investigative actions

Inspect the legitimacy of the user which the RDP made the connection with.
Verify that this isn't IT activity.

30.302 | NTLM Password Spray

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
Deduplication Period	1 Day

Required Data	- Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force: Password Spraying (T1110.003)
Severity	Informational

Description

A single host tried to perform an unusual amount of login attempts using NTLM in a short period of time.
This may be indicative of a NTLM password spray attack.

Attacker's Goals

The attacker may attempt to guess user credential by password spray attack over multiple machines.

Investigative actions

Verify any successful authentication made by one of the user accounts referenced by the alert, as these may indicate the attacker managed to guess the credentials.

Variations

NTLM password spray on a sensitive entity

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force: Password Spraying (T1110.003)
Severity	Low

Description

A single host tried to perform an unusual amount of login attempts using NTLM in a short period of time on a sensitive entity.
This may be indicative of a NTLM password spray attack.

Attacker's Goals

The attacker may attempt to guess user credential by password spray attack over multiple machines.

Investigative actions

Verify any successful authentication made by one of the user accounts referenced by the alert, as these may indicate the attacker managed to guess the credentials.

30.303 | Multiple Rare Process Executions in Organization

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour

Deduplication Period	30 Days
Required Data	Requires: • XDR Agent
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	User Execution (T1204)
Severity	Informational

Description

Multiple unusual processes were executed in the organization. This may be indicative of a compromised account.

Attacker's Goals

Unusual processes may be executed for various purposes, including exfiltration, lateral movement, etc.

Investigative actions

Investigate the processes that were executed to determine if they were used for legitimate purposes or malicious activity.

30.304 | Kerberos Pre-Auth Failures by Host

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
Deduplication Period	1 Hour
Required Data	Requires one of the following data sources: - Palo Alto Networks Platform Logs OR ⫿ XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force (T1110)
Severity	Low

Description

The endpoint failed an unusual number of Kerberos pre-authentications (TGT requests) from at least three users when compared to its baseline.
This can indicate a password-spraying attack.

Attacker's Goals

The attacker is attempting to gain an initial foothold in the domain using a list of valid users and a guessed password.

Investigative actions

- Verify whether the host that generated the alert is normally used by many users (for example, a terminal server).

  Verify any later authentication success for the user accounts referenced by the alert, as these can indicate the attacker managed to guess the credentials.

30.305 | Brute-force attempt on a local account

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	15 Minutes
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)

ATT&CK Technique	Brute Force (T1110)
Severity	Informational

Description

A local user account failed to log in multiple times in a short time period. This may indicate a brute-force attack.

Attacker's Goals

The attacker attempts to gain access to the account.

Investigative actions

Verify any successful authentication by the user account referenced by the alert, as these can indicate the attacker managed to guess the credentials.

Variations

Brute force on a local account

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force (T1110)
Severity	Low

Description

A local user account failed to log in multiple times in a short time period. This may indicate a brute-force attack.

Attacker's Goals

The attacker attempts to gain access to the account.

Investigative actions

Verify any successful authentication by the user account referenced by the alert, as these can indicate the attacker managed to guess the credentials.

30.306 | Multiple discovery-like commands

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Remote System Discovery (T1018) System Information Discovery (T1082) System Network Configuration Discovery (T1016) System Service Discovery (T1007)

Severity	Informational

Description

The alerted process performed multiple consecutive discovery commands in a short time frame.

Attacker's Goals

Collect information about the host, network and user configuration for lateral movement and privilege escalation.

Investigative actions

- Verify if the script or process initiating the discovery commands is benign.
- Verify that this isn't sanctioned IT activity.
  Look for other hosts executing similar commands.

Variations

Multiple discovery-like commands by web server process

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Remote System Discovery (T1018) System Information Discovery (T1082) System Network Configuration Discovery (T1016) System Service Discovery (T1007)
Severity	Low

Description

The web server process performed multiple consecutive discovery commands in a short time frame.

Attacker's Goals

Collect information about the host, network and user configuration for lateral movement and privilege escalation.

Investigative actions

Verify if the script or process initiating the discovery commands is benign.

Verify that this isn't sanctioned IT activity.
Look for other hosts executing similar commands.

Multiple discovery-like commands on a Linux host

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Remote System Discovery (T1018) System Information Discovery (T1082) System Network Configuration Discovery (T1016) System Service Discovery (T1007)
Severity	Informational

Description

The alerted process performed multiple consecutive discovery commands in a short time frame.

Attacker's Goals

Collect information about the host, network and user configuration for lateral movement and privilege escalation.

Investigative actions

Verify if the script or process initiating the discovery commands is benign.
Verify that this isn't sanctioned IT activity.

Look for other hosts executing similar commands.

Multiple discovery-like commands

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	- Remote System Discovery (T1018) System Information Discovery (T1082) System Network Configuration Discovery (T1016) System Service Discovery (T1007)
Severity	Informational

Description

The alerted process performed multiple consecutive discovery commands in a short time frame.

Attacker's Goals

Collect information about the host, network and user configuration for lateral movement and privilege escalation.

Investigative actions

- Verify if the script or process initiating the discovery commands is benign.
- Verify that this isn't sanctioned IT activity.
  Look for other hosts executing similar commands.

30.307 | Suspicious ICMP traffic that resembles smurf attack

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	1 Hour
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	- Endpoint Denial of Service: Service Exhaustion Flood (T1499.002) - Network Denial of Service (T1498)
Severity	Low

Description

ICMP smurf attack was used.

Attacker's Goals

Attempt to perform a denial-of-service attack by network exhaustion.

Investigative actions

- Check if the ICMP message to broadcast was used for a legitimate reason.
- If not, check for denial-of-service impact on the subnet.

30.308 | External Login Password Spray

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force: Password Spraying (T1110.003)
Severity	Informational

Description

An abnormally high amount of user account login attempts were seen on a host within a short period of time.
This may have resulted from a login password spray attack.

Attacker's Goals

An attacker may be attempting to gain unauthorized access to user accounts.

Investigative actions

- Check the amount of time in between each login attempt.
- Investigate the reason behind the login failures and if any accounts were locked out. Look for any successful login attempts and the ratio of login success versus login failures.

Variations

Successful External Login Password Spray on a Domain Controller

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force: Password Spraying (T1110.003)
Severity	Medium

Description

An abnormally high amount of user account login attempts were seen on a domain controller within a short period of time.

Attacker's Goals

An attacker may be attempting to gain unauthorized access to user accounts.

Investigative actions

- Check the amount of time in between each login attempt.
- Investigate the reason behind the login failures and if any accounts were locked out. Look for any successful login attempts and the ratio of login success versus login failures.

Successful External Login Password Spray on a sensitive server

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force: Password Spraying (T1110.003)
Severity	Medium

Description

An abnormally high amount of user account login attempts were seen on a sensitive server within a short period of time.

Attacker's Goals

An attacker may be attempting to gain unauthorized access to user accounts.

Investigative actions

Check the amount of time in between each login attempt.
Investigate the reason behind the login failures and if any accounts were locked out.

Look for any successful login attempts and the ratio of login success versus login failures.

Successful External Login Password Spray

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force: Password Spraying (T1110.003)
Severity	Low

Description

An abnormally high amount of user account login attempts were seen on a host within a short period of time.

This may have resulted from a login password spray attack.

Attacker's Goals

An attacker may be attempting to gain unauthorized access to user accounts.

Investigative actions

- Check the amount of time in between each login attempt.
  Investigate the reason behind the login failures and if any accounts were locked out.
  Look for any successful login attempts and the ratio of login success versus login failures.

External Login Password Spray on a Domain Controller

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force: Password Spraying (T1110.003)
Severity	Low

Description

An abnormally high amount of user account login attempts were seen on a domain controller within a short period of time.

Attacker's Goals

An attacker may be attempting to gain unauthorized access to user accounts.

Investigative actions

Check the amount of time in between each login attempt.
Investigate the reason behind the login failures and if any accounts were locked out.

Look for any successful login attempts and the ratio of login success versus login failures.

30.309 | Subdomain Fuzzing

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	20 Minutes
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Reconnaissance (TA0043)
ATT&CK Technique	Active Scanning: Wordlist Scanning (T1595.003)
Severity	Low

Description

The root domain within the network is experiencing an unusually high number of access requests to its subdomains, significantly exceeding the typical activity levels for that domain.
This anomaly could suggest that someone is attempting to enumerate subdomains or uncover

additional virtual hosts associated with the domain, possibly as part of a reconnaissance effort to identify vulnerable or less-secured entry points into the network.

Attacker's Goals

Scan a known external facing asset to gain knowledge about the organization.

Investigative actions

- Verify that the domain doesn't host numerous subdomains.
  Verify that the source of the scan is not a known external scanner.

Variations

Subdomain Fuzzing To a Rare Destination

Synopsis

ATT&CK Tactic	Reconnaissance (TA0043)
ATT&CK Technique	Active Scanning: Wordlist Scanning (T1595.003)
Severity	Medium

Description

The root domain within the network is experiencing an unusually high number of access requests to its subdomains, significantly exceeding the typical activity levels for that domain.

This anomaly could suggest that someone is attempting to enumerate subdomains or uncover additional virtual hosts associated with the domain, possibly as part of a reconnaissance effort to identify vulnerable or less-secured entry points into the network.

Attacker's Goals

Scan a known external facing asset to gain knowledge about the organization.

Investigative actions

Verify that the domain doesn't host numerous subdomains.

Verify that the source of the scan is not a known external scanner.

30.310 | Interactive local account enumeration

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	▮ Discovery (TA0007) Credential Access (TA0006)
ATT&CK Technique	▮ Account Discovery (T1087) ▮ Brute Force (T1110)
Severity	Low

Description

Multiple non-existing accounts failed to interactive local log in to a host in a short period of time.

This may indicate an attacker has physical access to the host, and is trying to enumerate accounts.

Attacker's Goals

Discover valid accounts to gain credentials.

Investigative actions

Check if the login attempts were part of a legitimate misunderstanding of the system or part of an attack.

30.311 | Abnormal SMB activity to multiple hosts

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	5 Hours
Deduplication Period	1 Day
Required Data	- Requires: - XDR Agent
Detection Modules	
Detector Tags	NDR Lateral Movement Analytics
ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Services (T1021)

Severity	Low

Description

An endpoint performed a new, unfamiliar SMB activity to multiple hosts on the network.

Attacker's Goals

An adversary may use different protocols to enumerate and plan its lateral movement over the network.

Investigative actions

- Verify if the host is a newly deployed server that consists of SMB services to multiple hosts.
- Verify the legitimacy of the actor process (and its causality) that initiated this SMB traffic.

Variations

Highly rare SMB activity to multiple hosts

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Services (T1021)
Severity	Low

Description

An endpoint performed a new, and highly rare, SMB activity to multiple hosts on the network.

Attacker's Goals

An adversary may use different protocols to enumerate and plan its lateral movement over the network.

Investigative actions

- Verify if the host is a newly deployed server that consists of SMB services to multiple hosts.
- Verify the legitimacy of the actor process (and its causality) that initiated this SMB traffic.

Highly rare SMB activity to multiple hosts

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Services (T1021)
Severity	Medium

Description

An endpoint performed a new, and highly rare SMB activity to multiple hosts on the network.

Attacker's Goals

An adversary may use different protocols to enumerate and plan its lateral movement over the network.

Investigative actions

- Verify if the host is a newly deployed server that consists of SMB services to multiple hosts.
- Verify the legitimacy of the actor process (and its causality) that initiated this SMB traffic.

Abnormal SMB activity to multiple hosts

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Services (T1021)
Severity	Medium

Description

An endpoint performed a new, unfamiliar SMB activity to multiple hosts on the network.

Attacker's Goals

An adversary may use different protocols to enumerate and plan its lateral movement over the network.

Investigative actions

Verify if the host is a newly deployed server that consists of SMB services to multiple hosts.

Verify the legitimacy of the actor process (and its causality) that initiated this SMB traffic.

Abnormal SMB activity to multiple hosts

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Services (T1021)
Severity	Low

Description

An endpoint performed a new, unfamiliar SMB activity to multiple hosts on the network.

Attacker's Goals

An adversary may use different protocols to enumerate and plan its lateral movement over the network.

Investigative actions

Verify if the host is a newly deployed server that consists of SMB services to multiple hosts.

- Verify the legitimacy of the actor process (and its causality) that initiated this SMB traffic.

30.312 | NTLM Relay

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: ▯ Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006) ▮ Lateral Movement (TA0008)
ATT&CK Technique	Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay (T1557.001) ▮ Use Alternate Authentication Material: Pass the Hash (T1550.002)
Severity	Informational

Description

An NTLM NTProofStr was seen from more than one source.
This indicates that NTLM authentication data has been relayed.

Attacker's Goals

The attacker is attempting a man-in-the-middle NTLM relay attack to intercept authentication attempts and move laterally within an environment.

Investigative actions

- Check that the alerted host is not a NAT or a proxy that duplicates traffic as part of its normal behavior.
- Check if the protocols used are vulnerable to an NTLM relay attack (e.g. LDAP, SMB).
- Ensure that SMB signing is enabled in the case of a possible SMB relay attack.

30.313 | Multiple discovery commands on a Windows host by the same process

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	

Detector Tags	
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Remote System Discovery (T1018) System Information Discovery (T1082) System Network Configuration Discovery (T1016) System Service Discovery (T1007)
Severity	Low

Description

The alerted process performed multiple discovery commands in a short timeframe.

Attacker's Goals

Collect information about the host, network and user configuration for lateral movement and privilege escalation.

Investigative actions

- Verify if the script or process initiating the discovery commands is benign.
- Verify that this isn't sanctioned IT activity.
- Look for other hosts executing similar commands.

Variations

Remote Multiple discovery commands on a Windows host by the same IP

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008) Discovery (TA0007)

ATT&CK Technique	Remote Services (T1021) Remote System Discovery (T1018) System Information Discovery (T1082) System Network Configuration Discovery (T1016) System Service Discovery (T1007)
Severity	High

Description

The alerted process performed multiple discovery commands in a short timeframe.

Attacker's Goals

Collect information about the host, network and user configuration for lateral movement and privilege escalation.

Investigative actions

- Verify if the script or process initiating the discovery commands is benign.
- Verify that this isn't sanctioned IT activity.
- Look for other hosts executing similar commands.

Multiple discovery commands on a Windows host by the same process from a web server CGO

Synopsis

ATT&CK Tactic	Persistence (TA0003) Discovery (TA0007)
ATT&CK Technique	Server Software Component: Web Shell (T1505.003) Remote System Discovery (T1018) System Information Discovery (T1082) System Network Configuration Discovery (T1016) System Service Discovery (T1007)
Severity	Medium

Description

The alerted process performed multiple discovery commands in a short timeframe.

Attacker's Goals

Collect information about the host, network and user configuration for lateral movement and privilege escalation.

Investigative actions

- Verify if the script or process initiating the discovery commands is benign.
- Verify that this isn't sanctioned IT activity.
- Look for other hosts executing similar commands.

Multiple discovery commands on a Windows host by the same process from an SQL server CGO

Synopsis

ATT&CK Tactic	Persistence (TA0003) Discovery (TA0007)
ATT&CK Technique	Server Software Component: SQL Stored Procedures (T1505.001) Remote System Discovery (T1018) System Information Discovery (T1082) System Network Configuration Discovery (T1016) System Service Discovery (T1007)
Severity	Medium

Description

The alerted process performed multiple discovery commands in a short timeframe.

Attacker's Goals

Collect information about the host, network and user configuration for lateral movement and privilege escalation.

Investigative actions

- Verify if the script or process initiating the discovery commands is benign.
- Verify that this isn't sanctioned IT activity.
- Look for other hosts executing similar commands.

Multiple discovery commands on a Windows host by the same process from a remote CGO

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008) Discovery (TA0007)
ATT&CK Technique	Remote Services (T1021) Remote System Discovery (T1018) System Information Discovery (T1082) System Network Configuration Discovery (T1016) System Service Discovery (T1007)
Severity	Medium

Description

The alerted process performed multiple discovery commands in a short timeframe.

Attacker's Goals

Collect information about the host, network and user configuration for lateral movement and privilege escalation.

Investigative actions

- Verify if the script or process initiating the discovery commands is benign.
- Verify that this isn't sanctioned IT activity.
- Look for other hosts executing similar commands.

Rare Multiple discovery commands on a Windows host by the same process

Synopsis

ATT&CK Tactic	Discovery (TA0007)

ATT&CK Technique	- Remote System Discovery (T1018) - System Information Discovery (T1082) System Network Configuration Discovery (T1016) System Service Discovery (T1007)
Severity	Medium

Description

The alerted process performed multiple discovery commands in a short timeframe.

Attacker's Goals

Collect information about the host, network and user configuration for lateral movement and privilege escalation.

Investigative actions

Verify if the script or process initiating the discovery commands is benign.

Verify that this isn't sanctioned IT activity.

- Look for other hosts executing similar commands.

30.314 | Sudoedit Brute force attempt

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Day

Required Data	- Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Exploitation for Privilege Escalation (T1068)
Severity	Medium

Description

An unusual amount of sudoedit commands executed in a short period of time.
This may indicate an attempt to exploit CVE-2021-3156.

Attacker's Goals

The attacker may gain higher privileges via exploitation of sudoedit.

Investigative actions

Verify that the current version of sudo in not vulnerable to CVE-2021-3156.

30.315 | Multiple Rare LOLBIN Process Executions by User

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	1 Hour
Deduplication Period	30 Days
Required Data	Requires: - XDR Agent
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	User Execution (T1204)
Severity	Low

Description

A user executed multiple living-off-the-land binary (LOLBIN) processes that are unusual for this user. This may be indicative of a compromised account.

Attacker's Goals

Unusual processes may be executed for various purposes, including exfiltration, lateral movement, etc.

Investigative actions

Investigate the processes that were executed to determine if they were used for legitimate purposes or malicious activity.

Variations

Multiple curl process executions by user

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	User Execution (T1204)
Severity	Informational

Description

A user executed multiple living-off-the-land binary (LOLBIN) processes that are unusual for this user. This may be indicative of a compromised account.

Attacker's Goals

Unusual processes may be executed for various purposes, including exfiltration, lateral movement, etc.

Investigative actions

Investigate the processes that were executed to determine if they were used for legitimate purposes or malicious activity.

30.316 | Multiple discovery commands on a Linux host by the same process

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	10 Minutes
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Remote System Discovery (T1018) System Information Discovery (T1082) System Network Configuration Discovery (T1016) System Service Discovery (T1007)
Severity	Informational

Description

The alerted process performed multiple consecutive discovery commands in a short timeframe.

Attacker's Goals

Collect information about the host, network and user configuration for lateral movement and privilege escalation.

Investigative actions

- Verify if the script or process initiating the discovery commands is benign.
- Verify that this isn't sanctioned IT activity.
  Look for other hosts executing similar commands.

Variations

Multiple discovery commands on a Linux host by the same process

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Remote System Discovery (T1018) System Information Discovery (T1082) System Network Configuration Discovery (T1016) System Service Discovery (T1007)
Severity	Medium

Description

The alerted process performed multiple consecutive discovery commands in a short timeframe.

Attacker's Goals

Collect information about the host, network and user configuration for lateral movement and privilege escalation.

Investigative actions

- Verify if the script or process initiating the discovery commands is benign.
- Verify that this isn't sanctioned IT activity.
  Look for other hosts executing similar commands.

Multiple discovery commands on a Linux host by the same process

Synopsis

ATT&CK Tactic	Discovery (TA0007)

ATT&CK Technique	- Remote System Discovery (T1018) - System Information Discovery (T1082) System Network Configuration Discovery (T1016) System Service Discovery (T1007)
Severity	Low

Description

The alerted process performed multiple consecutive discovery commands in a short timeframe.

Attacker's Goals

Collect information about the host, network and user configuration for lateral movement and privilege escalation.

Investigative actions

Verify if the script or process initiating the discovery commands is benign.

Verify that this isn't sanctioned IT activity.

- Look for other hosts executing similar commands.

30.317 | Large Upload (HTTPS)

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Day
Deduplication Period	1 Day

Required Data	- Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent OR - Third-Party Firewalls
Detection Modules	
Detector Tags	
ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Exfiltration Over Alternative Protocol (T1048)
Severity	Low

Description

The endpoint transferred an excessive amount of data to an external site over HTTPS.
The destination is not a popular upload site for endpoints on your network, and the endpoint performing the upload has not previously downloaded a large amount of data from the site.

The upload is considered excessive based on comparison to baseline measurements of HTTPS data transfers on your network.
An attacker may be exfiltrating data directly to the internet.

Attacker's Goals

Transfer data she has stolen from your network to a location that is convenient and useful to her.

Investigative actions

Check if this alert has been falsely triggered by DNS load balancers. If an endpoint routinely uploads data to a site that uses load balancers, the transfer might ordinarily be split into multiple sessions and across multiple subdomains, which can cause the baseline measurement to be incorrect. In that situation, a routine upload that randomly places the bulk of the data in a single session to a single subdomain can look excessive to the Cortex XDR Analytics detector.

- Check if the device performing the data transfer is a mobile phone performing a backup. Cortex XDR Analytics will not always measure the baseline properly for mobile devices, especially if the backups are performed infrequently and contain a great deal of data. If the data transfer is a mobile device running a backup, check to ensure that only appropriate data is included in the backup.
- Identify the process/user performing the data transfer to determine if the transfer is sanctioned.

Variations

Large Upload (HTTPS)

Synopsis

ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Exfiltration Over Alternative Protocol (T1048)
Severity	Informational

Description

The endpoint transferred an excessive amount of data to an external site over HTTPS.
The destination is not a popular upload site for endpoints on your network, and the endpoint performing the upload has not previously downloaded a large amount of data from the site.

The upload is considered excessive based on comparison to baseline measurements of HTTPS data transfers on your network.
An attacker may be exfiltrating data directly to the internet.

Attacker's Goals

Transfer data she has stolen from your network to a location that is convenient and useful to her.

Investigative actions

Check if this alert has been falsely triggered by DNS load balancers. If an endpoint routinely uploads data to a site that uses load balancers, the transfer might ordinarily be split into multiple sessions and across multiple subdomains, which can cause the baseline measurement to be incorrect. In that situation, a routine upload that randomly places the bulk of the data in a single session to a single subdomain can look excessive to the Cortex XDR Analytics detector.

- Check if the device performing the data transfer is a mobile phone performing a backup. Cortex XDR Analytics will not always measure the baseline properly for mobile devices, especially if the backups are performed infrequently and contain a great deal of data. If the data transfer is a mobile device running a backup, check to ensure that only appropriate data is included in the backup.
- Identify the process/user performing the data transfer to determine if the transfer is sanctioned.

30.318 | Spam Bot Traffic

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	3 Days
Deduplication Period	3 Days
Required Data	- Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent OR - Third-Party Firewalls
Detection Modules	

Detector Tags	
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Resource Hijacking (T1496)
Severity	Low

Description

The endpoint connected to an excessive number of external SMTP servers.
A spambot may be trying to send spam email using multiple SMTP servers.
Spambots can cause your domain to be blacklisted, and can contain other malicious functionality.
The same mechanism can also be used for exfiltration. Some VPN clients can also tunnel data over SMTP.

Note: This detection model looks for SMTP connections to external servers, but the volume of traffic is not considered. A count is performed based on the number of domains being contacted, as well as the number of unresolved IP addresses.

Attacker's Goals

The attacker uses the host as an SMTP client to send mails and hide their real origin.

Investigative actions

Verify that the source is not an SMTP server. If Cortex XDR Analytics has failed to identify the process as a valid SMTP server, this alert will be a false positive.

Verify that IP addresses are actually not being resolved by the non-SMTP process. If the process is performing DNS resolution with a DNS service outside your network, it is possible (depending on your network topology) that Cortex XDR Analytics will not observe that traffic. Because SMTP services typically use numerous IP addresses, this situation could cause a process to exceed a limit when it would otherwise fail to do so.

If the SMTP connection activity turns out to be the result of malicious file activity, search on the Triage page for other endpoints infected with the file.

Variations

Spam Bot Traffic

Synopsis

ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Resource Hijacking (T1496)
Severity	Informational

Description

The endpoint connected to an excessive number of external SMTP servers.
A spambot may be trying to send spam email using multiple SMTP servers.
Spambots can cause your domain to be blacklisted, and can contain other malicious functionality.
The same mechanism can also be used for exfiltration. Some VPN clients can also tunnel data over SMTP.

Note: This detection model looks for SMTP connections to external servers, but the volume of traffic is not considered. A count is performed based on the number of domains being contacted, as well as the number of unresolved IP addresses.

Attacker's Goals

The attacker uses the host as an SMTP client to send mails and hide their real origin.

Investigative actions

- Verify that the source is not an SMTP server. If Cortex XDR Analytics has failed to identify the process as a valid SMTP server, this alert will be a false positive.
- Verify that IP addresses are actually not being resolved by the non-SMTP process. If the process is performing DNS resolution with a DNS service outside your network, it is possible (depending on your network topology) that Cortex XDR Analytics will not observe that traffic. Because SMTP services typically use numerous IP addresses, this situation could cause a process to exceed a limit when it would otherwise fail to do so.
- If the SMTP connection activity turns out to be the result of malicious file activity, search on the Triage page for other endpoints infected with the file.

Failed Spam Bot Traffic

Synopsis

ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Resource Hijacking (T1496)
Severity	Informational

Description

The endpoint connected to an excessive number of external SMTP servers.
A spambot may be trying to send spam email using multiple SMTP servers.
Spambots can cause your domain to be blacklisted, and can contain other malicious functionality.
The same mechanism can also be used for exfiltration. Some VPN clients can also tunnel data over SMTP.

Note: This detection model looks for SMTP connections to external servers, but the volume of traffic is not considered. A count is performed based on the number of domains being contacted, as well as the number of unresolved IP addresses.

Attacker's Goals

The attacker uses the host as an SMTP client to send mails and hide their real origin.

Investigative actions

Verify that the source is not an SMTP server. If Cortex XDR Analytics has failed to identify the process as a valid SMTP server, this alert will be a false positive.

- Verify that IP addresses are actually not being resolved by the non-SMTP process. If the process is performing DNS resolution with a DNS service outside your network, it is possible (depending on your network topology) that Cortex XDR Analytics will not observe that traffic. Because SMTP services typically use numerous IP addresses, this situation could cause a process to exceed a limit when it would otherwise fail to do so.
- If the SMTP connection activity turns out to be the result of malicious file activity, search on the Triage page for other endpoints infected with the file.

30.319 | A user authenticated with weak NTLM to multiple hosts

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Use Alternate Authentication Material (T1550)
Severity	Informational

Description

A user account authenticated to multiple hosts via NTLMv1 or LM authentication for the first time in the past 30 days.

Attacker's Goals

The attacker attempts to gain access to the accounts.

Investigative actions

- Audit all login events with a weaker protocol and review any anomalous usage.
- Investigate the mentioned user for additional suspicious activity.

30.320 | Possible brute force or configuration change attempt on cytool

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force: Password Guessing (T1110.001)
Severity	High

Description

An unusual amount of cytool commands were executed in a short period from a user who doesn't usually run these commands.
This may indicate an attempt to guess the Administrator password.

Attacker's Goals

The attacker may disable the agent to perform malicious activities.

Investigative actions

Verify which user ran these commands and if it is a legitimate behavior on this host.

30.321 | Massive upload to a rare storage or mail domain

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Day
Required Data	Requires: - Palo Alto Networks Platform Logs Requires: - XDR Agent
Detection Modules	Identity Threat Module

Detector Tags	
ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Exfiltration Over Web Service (T1567) Exfiltration Over Web Service: Exfiltration to Cloud Storage (T1567.002)
Severity	Informational

Description

A large amount of data was transferred to an external site that is used for mail or storage. This behavior may indicate data exfiltration.

Attacker's Goals

A user uploaded an abnormal amount of data to a file sharing service. This activity might indicate an attempt to exfiltrate files and data from the organization.

Investigative actions

Check for any other suspicious activity related to the host and the user involved in the alert.

- Identify the user uploading the data to determine if the transfer is sanctioned.

Variations

A user uploaded over 500 MB to a rare storage or mail domain

Synopsis

ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Exfiltration Over Web Service (T1567) Exfiltration Over Web Service: Exfiltration to Cloud Storage (T1567.002)

Severity	Low

Description

A user uploaded over 500 MB to a file sharing service that is rarely accessed by them or anyone else in the organization.

Attacker's Goals

A user uploaded an abnormal amount of data to a file sharing service. This activity might indicate an attempt to exfiltrate files and data from the organization.

Investigative actions

Check for any other suspicious activity related to the host and the user involved in the alert.

Identify the user uploading the data to determine if the transfer is sanctioned.

30.322 | Large Upload (SMTP)

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Day
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: ▯ Palo Alto Networks Platform Logs OR - XDR Agent OR - Third-Party Firewalls

Detection Modules	
Detector Tags	
ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Exfiltration Over Alternative Protocol (T1048)
Severity	Low

Description

The endpoint, which is not an internal SMTP server, emailed an excessive amount of data from your network.

Attacker's Goals

Transfer data they have stolen from your network to a location that is convenient and useful to him.

Investigative actions

- Identify the process/user performing the data transfer to determine if the transfer is sanctioned.
  Verify that the source is not a mail server.
  Check if the target address represents a mail service that rarely used in the organization. If so, this might indicate on file exfiltration attempt.

Variations

Large Upload (SMTP)

Synopsis

ATT&CK Tactic	Exfiltration (TA0010)

ATT&CK Technique	Exfiltration Over Alternative Protocol (T1048)
Severity	Informational

Description

The endpoint, which is not an internal SMTP server, emailed an excessive amount of data from your network.

Attacker's Goals

Transfer data they have stolen from your network to a location that is convenient and useful to him.

Investigative actions

- Identify the process/user performing the data transfer to determine if the transfer is sanctioned.
  Verify that the source is not a mail server.
  Check if the target address represents a mail service that rarely used in the organization. If so, this might indicate on file exfiltration attempt.

30.323 | NTLM Hash Harvesting

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Day

Required Data	- Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	OS Credential Dumping (T1003)
Severity	Medium

Description

An unusual number of users has sent NTLM to a target in the last hour.
This may be indicative of poisoning and NTLM hash harvesting.

Attacker's Goals

The attacker may attempt to extract NTLM hashes for credential access.

Investigative actions

- Check that the destination is not a server.
  Verify that the destination is not external to the organization.

30.324 | SSH brute force attempt

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	2 Hours
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - AWS Flow Log OR - AWS OCSF Flow Logs OR - Azure Flow Log OR - Gcp Flow Log OR - Palo Alto Networks Platform Logs OR - Third-Party Firewalls - Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)

ATT&CK Technique	Brute Force (T1110)
Severity	Informational

Description

There were multiple attempts to authenticate via SSH to a host in your network. This may indicate a brute force attack.

Attacker's Goals

Attackers attempt to log in to a remote host.

Investigative actions

Audit the failed authentication attempts in the SSH server to identify the abused user. If the abused user can authenticate to the SSH server, it may indicate that the attacker managed to compromise the user credentials.

Variations

SSH brute force network detected from external source

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force (T1110)
Severity	Informational

Description

There were multiple attempts to authenticate via SSH to a host in your network. This may indicate a brute force attack.

Attacker's Goals

Attackers attempt to log in to a remote host.

Investigative actions

Audit the failed authentication attempts in the SSH server to identify the abused user. If the abused user can authenticate to the SSH server, it may indicate that the attacker managed to compromise the user credentials.

Rare SSH brute force attempt

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force (T1110)
Severity	Low

Description

There were multiple attempts to authenticate via SSH to a host in your network. This may indicate a brute force attack.

Attacker's Goals

Attackers attempt to log in to a remote host.

Investigative actions

Audit the failed authentication attempts in the SSH server to identify the abused user. If the abused user can authenticate to the SSH server, it may indicate that the attacker managed to compromise the user credentials.

30.325 | Large Upload (FTP)

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Day
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Palo Alto Networks Platform Logs OR ▯ XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Exfiltration Over Alternative Protocol (T1048)
Severity	Low

Description

The endpoint transferred an excessively large amounts of data to a single destination over FTP.

Cortex XDR Analytics assumes endpoint traffic towards a specific destination should be about the same over long periods of time.

For that reason, Cortex XDR detected this abnormal behavior of large data upload.
An attacker may be exfiltrating data directly to the internet using this protocol.

Attacker's Goals

Exfiltrate stolen data from the victim network to an attacker's controllable resource.

Investigative actions

- Verify that the source is not an FTP server. If Cortex XDR Analytics has failed to identify the entity as a valid FTP server, this alert is likely to be a false positive.
  Identify the entity performing the data transfer to determine if the transfer is sanctioned.
- Use Pathfinder to interrogate the endpoint for suspicious artifacts that are using endpoint processes or loaded modules.

Variations

Large Upload (FTP)

Synopsis

ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Exfiltration Over Alternative Protocol (T1048)
Severity	Informational

Description

The endpoint transferred an excessively large amounts of data to a single destination over FTP.
Cortex XDR Analytics assumes endpoint traffic towards a specific destination should be about the same over long periods of time.
For that reason, Cortex XDR detected this abnormal behavior of large data upload.

An attacker may be exfiltrating data directly to the internet using this protocol.

Attacker's Goals

Exfiltrate stolen data from the victim network to an attacker's controllable resource.

Investigative actions

Verify that the source is not an FTP server. If Cortex XDR Analytics has failed to identify the entity as a valid FTP server, this alert is likely to be a false positive.

- Identify the entity performing the data transfer to determine if the transfer is sanctioned. Use Pathfinder to interrogate the endpoint for suspicious artifacts that are using endpoint processes or loaded modules.

30.326 | A user logged on to multiple workstations via Schannel

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	- Persistence (TA0003) - Privilege Escalation (TA0004) Credential Access (TA0006)
ATT&CK Technique	- Account Manipulation (T1098) Valid Accounts (T1078) Steal or Forge Authentication Certificates (T1649)

Severity	Informational

Description

A user logged on to multiple workstations with a certificate via Schannel. This may be indicative of a compromised account.

Attacker's Goals

Elevate permissions and establish persistence.

Investigative actions

- Verify the activity with the performing user.
- Check for possible certificate authentications with the subject user.
  Check if the user logged in to other endpoints via Schannel.

Variations

Rare user authentication with a certificate via Schannel

Synopsis

ATT&CK Tactic	Persistence (TA0003) Privilege Escalation (TA0004) Credential Access (TA0006)
ATT&CK Technique	Account Manipulation (T1098) Valid Accounts (T1078) Steal or Forge Authentication Certificates (T1649)
Severity	Low

Description

A rare user authentication with a certificate via Schannel was observed. This may be indicative of a compromised account.

Attacker's Goals

Elevate permissions and establish persistence.

Investigative actions

- Verify the activity with the performing user.
  Check for possible certificate authentications with the subject user.
  Check if the user logged in to other endpoints via Schannel.

Abnormal authentication with a certificate via Schannel

Synopsis

ATT&CK Tactic	Persistence (TA0003) Privilege Escalation (TA0004) Credential Access (TA0006)
ATT&CK Technique	Account Manipulation (T1098) Valid Accounts (T1078) Steal or Forge Authentication Certificates (T1649)
Severity	Informational

Description

An abnormal authentication with a certificate via Schannel was observed. This may be indicative of a compromised account.

Attacker's Goals

Elevate permissions and establish persistence.

Investigative actions

Verify the activity with the performing user.
Check for possible certificate authentications with the subject user.

Check if the user logged in to other endpoints via Schannel.

30.327 | Possible brute force on sudo user

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force: Password Guessing (T1110.001)
Severity	Informational

Description

A user executed an unusual amount of sudo commands in a short time period. This may indicate an attempt to guess the sudo password.

Attacker's Goals

The attacker may gain full privileges to the host.

Investigative actions

Verify which user ran these commands and if it is a legitimate behavior on this host.

Variations

Possible brute force on sudo user

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force: Password Guessing (T1110.001)
Severity	Low

Description

A user executed an unusual amount of sudo commands in a short time period.
This may indicate an attempt to guess the sudo password.

Attacker's Goals

The attacker may gain full privileges to the host.

Investigative actions

Verify which user ran these commands and if it is a legitimate behavior on this host.

30.328 | Rare access to known advertising domains

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	1 Day
Deduplication Period	1 Day
Required Data	- Requires: - Palo Alto Networks Platform Logs Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	- Command and Control (TA0011) - Persistence (TA0003)
ATT&CK Technique	- Application Layer Protocol (T1071) - Browser Extensions (T1176)
Severity	Informational

Description

The endpoint performed many connections to unpopular advertising domains. This could indicate the presence of adware on the endpoint.

Attacker's Goals

Causing the user to view excessive advertising content.

Investigative actions

Investigate the infected machine and search for suspicious browser extensions, See if changes were made to the homepage or if the browser is slower than usual, check whether sites that do not have ads usually, display ads when accessed from the possibly infected endpoint.
Search for suspicious redirections or proxy configuration on the infected machine.

Search for a C&C communication.

Variations

Rare access to known advertising domains from a Rare User Agent

Synopsis

ATT&CK Tactic	Command and Control (TA0011) Persistence (TA0003)
ATT&CK Technique	Application Layer Protocol (T1071) Browser Extensions (T1176)
Severity	Informational

Description

The endpoint performed many connections to unpopular advertising domains from a rare user agent.
This could indicate the presence of adware on the endpoint.

Attacker's Goals

Causing the user to view excessive advertising content.

Investigative actions

- Investigate the infected machine and search for suspicious browser extensions, See if changes were made to the homepage or if the browser is slower than usual, check whether sites that do not have ads usually, display ads when accessed from the possibly infected endpoint.

  Search for suspicious redirections or proxy configuration on the infected machine.
- Search for a C&C communication.

Suspicious Rare access to known advertising domains

Synopsis

ATT&CK Tactic	Command and Control (TA0011) Persistence (TA0003)
ATT&CK Technique	Application Layer Protocol (T1071) Browser Extensions (T1176)
Severity	Low

Description

The endpoint performed many connections to unpopular advertising domains.
This could indicate the presence of adware on the endpoint.

Attacker's Goals

Causing the user to view excessive advertising content.

Investigative actions

Investigate the infected machine and search for suspicious browser extensions, See if changes were made to the homepage or if the browser is slower than usual, check whether sites that do not have ads usually, display ads when accessed from the possibly infected endpoint.
Search for suspicious redirections or proxy configuration on the infected machine.

Search for a C&C communication.

30.329 | Kerberos Pre-Auth Failures by User and Host

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	10 Minutes
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Palo Alto Networks Platform Logs OR ▯ XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force (T1110)
Severity	Informational

Description

The user account on this host failed Kerberos pre-authentications (TGT requests) an unusual number of times.
This can indicate a Kerberos brute-force attack.

Attacker's Goals

The attacker is attempting to guess the credentials for the user account.

Investigative actions

- Verify that the password for the account has not been changed recently, without updating the user or the program using it.
  Verify any later authentication success for the user accounts referenced by the alert, as these can indicate the attacker managed to guess the credentials.

30.330 | NTLM Brute Force

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force (T1110)
Severity	Informational

Description

- This may indicate an NTLM brute force attack.

Attacker's Goals

The attacker attempts to gain access to the accounts.

Investigative actions

Verify any successful authentication by the user account referenced by the alert, as these can indicate the attacker managed to guess the credentials.

Variations

NTLM brute force on a sensitive user

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force (T1110)
Severity	Medium

Description

- This may indicate an NTLM brute force attack.

Attacker's Goals

The attacker attempts to gain access to the accounts.

Investigative actions

Verify any successful authentication by the user account referenced by the alert, as these can indicate the attacker managed to guess the credentials.

High-frequency NTLM brute force attempts detected

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force (T1110)

Severity	Low

Description

This may indicate an NTLM brute force attack.

Attacker's Goals

The attacker attempts to gain access to the accounts.

Investigative actions

Verify any successful authentication by the user account referenced by the alert, as these can indicate the attacker managed to guess the credentials.

30.331 | Abnormal sensitive RPC traffic to multiple hosts

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	5 Hours
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	NDR Lateral Movement Analytics

ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Services (T1021)
Severity	Low

Description

The endpoint performed unfamiliar RPC activity to multiple hosts using a known sensitive interface.

Attacker's Goals

An adversary may enumerate different protocols to gain information and plan its lateral movement over the network.

Investigative actions

- Check if the host is a newly deployed server that provides RPC based services to multiple hosts.
- Verify the legitimacy of the actor process (and its causality) that initiated this RPC traffic.

Variations

Abnormal sensitive RPC traffic to multiple IPs

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Services (T1021)
Severity	Informational

Description

The endpoint performed unfamiliar RPC activity to multiple hosts using a known sensitive interface.

Attacker's Goals

An adversary may enumerate different protocols to gain information and plan its lateral movement over the network.

Investigative actions

- Check if the host is a newly deployed server that provides RPC based services to multiple hosts.
- Verify the legitimacy of the actor process (and its causality) that initiated this RPC traffic.

30.332 | Large Upload (Generic)

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Day
Deduplication Period	1 Day
Required Data	- Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	

Detector Tags	
ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Exfiltration Over Alternative Protocol (T1048)
Severity	Low

Description

The endpoint transferred large amounts of data to an external site using a different protocol from HTTP/s, FTP, or SMTP. (A specific detector is used for each of those protocols.)
Cortex XDR Analytics assumes that data transfers out of your network are ordinarily performed using one of those three services, so it expects that data transfers over all other ports to be low.
For the same reason, Cortex XDR Analytics also assumes endpoint traffic towards a specific destination should be about the same over long periods of time.
An attacker may be exfiltrating data directly to the internet.

Attacker's Goals

Transfer data he has stolen from your network to a location that is convenient and useful to him.

Investigative actions

- Check if the traffic is related to SSH activity, it can trigger this alert. It is possible that someone on your network is legitimately engaged in SSH activity.
  Check if the traffic is to/from a misconfigured network.

  Check if the traffic is to a new external service or server that has recently been adopted for use by an organization in your enterprise.
- Identify the process/user performing the data transfer to determine if the transfer is sanctioned.

Variations

Large Upload (Generic)

Synopsis

ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Exfiltration Over Alternative Protocol (T1048)
Severity	Informational

Description

The endpoint transferred large amounts of data to an external site using a different protocol from HTTP/s, FTP, or SMTP. (A specific detector is used for each of those protocols.)
Cortex XDR Analytics assumes that data transfers out of your network are ordinarily performed using one of those three services, so it expects that data transfers over all other ports to be low.
For the same reason, Cortex XDR Analytics also assumes endpoint traffic towards a specific destination should be about the same over long periods of time.
An attacker may be exfiltrating data directly to the internet.

Attacker's Goals

Transfer data he has stolen from your network to a location that is convenient and useful to him.

Investigative actions

Check if the traffic is related to SSH activity, it can trigger this alert. It is possible that someone on your network is legitimately engaged in SSH activity.

Check if the traffic is to/from a misconfigured network.
- Check if the traffic is to a new external service or server that has recently been adopted for use by an organization in your enterprise.
Identify the process/user performing the data transfer to determine if the transfer is sanctioned.

Large Upload (Generic)to a Frequently Used Upload Target

Synopsis

ATT&CK Tactic	Exfiltration (TA0010)

ATT&CK Technique	Exfiltration Over Alternative Protocol (T1048)
Severity	Informational

Description

The endpoint transferred large amounts of data to an external site using a different protocol from HTTP/s, FTP, or SMTP. (A specific detector is used for each of those protocols.)

Cortex XDR Analytics assumes that data transfers out of your network are ordinarily performed using one of those three services, so it expects that data transfers over all other ports to be low.
For the same reason, Cortex XDR Analytics also assumes endpoint traffic towards a specific destination should be about the same over long periods of time.
An attacker may be exfiltrating data directly to the internet.

Attacker's Goals

Transfer data he has stolen from your network to a location that is convenient and useful to him.

Investigative actions

- Check if the traffic is related to SSH activity, it can trigger this alert. It is possible that someone on your network is legitimately engaged in SSH activity.
  Check if the traffic is to/from a misconfigured network.
  Check if the traffic is to a new external service or server that has recently been adopted for use by an organization in your enterprise.
- Identify the process/user performing the data transfer to determine if the transfer is sanctioned.

30.333 | Upload pattern that resembles Peer to Peer traffic

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	30 Minutes
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - Third-Party Firewalls OR - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Command and Control (TA0011) Initial Access (TA0001)
ATT&CK Technique	Application Layer Protocol (T1071) Non-Standard Port (T1571) Trusted Relationship (T1199) Phishing (T1566)
Severity	Informational

Description

A possible P2P protocol was spotted from an internal host.

Attacker's Goals

An attacker may use peer-to-peer communication to gain initial access, as a C&C tool, or an exfiltration tool.

Investigative actions

confirm that the port accessed is a P2P port/ is run by a P2P application.
- View the downloaded content and determine it's not malicious.
- Check for large uploads from this host and check for sensitive information that might not be required on the host.

30.334 | Port Scan

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Day
Required Data	- Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent OR - Third-Party Firewalls
Detection Modules	
Detector Tags	
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Network Service Discovery (T1046)

Severity	Informational

Description

The endpoint connected, or attempted to connect, to multiple privileged ports (lower than port 1024), which are infrequently used by other endpoints (i.e. destination ports that are normally used by many endpoints will not raise this alert).
Attackers perform port scans for reconnaissance purposes, to find computers or servers that accept connections on these ports, and to find vulnerable services that can be exploited.
Coverage for port scans using data arriving solely from Cortex agents is incomplete.

Attacker's Goals

An attacker is determining which ports are open or closed on remote endpoints in an attempt to identify the endpoint operating system, firewall configuration, and exploitable services.

Investigative actions

- New endpoints that use multiple ports can cause a false positive. Ensure that the endpoint is not new on the network, and is not hosting services such as FTP servers or domain controllers that are being contacted for the first time.
  Check if the activity is a SYN-ACK scan. These might result in Cortex XDR Analytics detecting the scan as coming from the wrong direction, and could mean that Cortex XDR Analytics used the wrong baseline in triggering the alert.
- Check for port map and/or X11 usage. These usually open multiple ports. If the protocol usage for the specific destination is sparse, Cortex XDR Analytics could raise a false alert.

Variations

Port scan by suspicious process

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Network Service Discovery (T1046)
Severity	Low

Description

The endpoint connected, or attempted to connect, to multiple privileged ports (lower than port 1024), which are infrequently used by other endpoints (i.e. destination ports that are normally used by many endpoints will not raise this alert).
Attackers perform port scans for reconnaissance purposes, to find computers or servers that accept connections on these ports, and to find vulnerable services that can be exploited.
Coverage for port scans using data arriving solely from Cortex agents is incomplete.

Attacker's Goals

An attacker is determining which ports are open or closed on remote endpoints in an attempt to identify the endpoint operating system, firewall configuration, and exploitable services.

Investigative actions

- New endpoints that use multiple ports can cause a false positive. Ensure that the endpoint is not new on the network, and is not hosting services such as FTP servers or domain controllers that are being contacted for the first time.
- Check if the activity is a SYN-ACK scan. These might result in Cortex XDR Analytics detecting the scan as coming from the wrong direction, and could mean that Cortex XDR Analytics used the wrong baseline in triggering the alert.
- Check for port map and/or X11 usage. These usually open multiple ports. If the protocol usage for the specific destination is sparse, Cortex XDR Analytics could raise a false alert.

Highly suspicious port scan

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Network Service Discovery (T1046)
Severity	Medium

Description

The endpoint connected, or attempted to connect, to multiple privileged ports (lower than port 1024), which are infrequently used by other endpoints (i.e. destination ports that are normally used by many endpoints will not raise this alert).
Attackers perform port scans for reconnaissance purposes, to find computers or servers that

accept connections on these ports, and to find vulnerable services that can be exploited. Coverage for port scans using data arriving solely from Cortex agents is incomplete.

Attacker's Goals

An attacker is determining which ports are open or closed on remote endpoints in an attempt to identify the endpoint operating system, firewall configuration, and exploitable services.

Investigative actions

New endpoints that use multiple ports can cause a false positive. Ensure that the endpoint is not new on the network, and is not hosting services such as FTP servers or domain controllers that are being contacted for the first time.

- Check if the activity is a SYN-ACK scan. These might result in Cortex XDR Analytics detecting the scan as coming from the wrong direction, and could mean that Cortex XDR Analytics used the wrong baseline in triggering the alert.

Check for port map and/or X11 usage. These usually open multiple ports. If the protocol usage for the specific destination is sparse, Cortex XDR Analytics could raise a false alert.

Suspicious port scan

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Network Service Discovery (T1046)
Severity	Low

Description

The endpoint connected, or attempted to connect, to multiple privileged ports (lower than port 1024), which are infrequently used by other endpoints (i.e. destination ports that are normally used by many endpoints will not raise this alert).

Attackers perform port scans for reconnaissance purposes, to find computers or servers that accept connections on these ports, and to find vulnerable services that can be exploited. Coverage for port scans using data arriving solely from Cortex agents is incomplete.

Attacker's Goals

An attacker is determining which ports are open or closed on remote endpoints in an attempt to identify the endpoint operating system, firewall configuration, and exploitable services.

Investigative actions

- New endpoints that use multiple ports can cause a false positive. Ensure that the endpoint is not new on the network, and is not hosting services such as FTP servers or domain controllers that are being contacted for the first time.
  Check if the activity is a SYN-ACK scan. These might result in Cortex XDR Analytics

  detecting the scan as coming from the wrong direction, and could mean that Cortex XDR Analytics used the wrong baseline in triggering the alert.
- Check for port map and/or X11 usage. These usually open multiple ports. If the protocol usage for the specific destination is sparse, Cortex XDR Analytics could raise a false alert.

30.335 | SSH authentication brute force attempts

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	15 Minutes
Deduplication Period	3 Hours
Required Data	Requires: - XDR Agent
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)

ATT&CK Technique	Brute Force (T1110)
Severity	Informational

Description

A user attempted to authenticate via SSH an excessive number of times in a short period. This may indicate a brute force attack.

Attacker's Goals

Attackers attempt to log in to a remote host.

Investigative actions

Verify any successful authentication by the user account referenced by the alert, as these can indicate the attacker managed to guess the credentials.

Variations

Successful SSH Brute Force

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force (T1110)
Severity	Low

Description

A user successfully authenticated via SSH after an excessive number of failures in a short period.

Attacker's Goals

Attackers attempt to log in to a remote host.

Investigative actions

Verify any successful authentication by the user account referenced by the alert, as these can indicate the attacker managed to guess the credentials.

Possible SSH Brute Force

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force (T1110)
Severity	Low

Description

A user attempted to authenticate via SSH an excessive number of times in a short period. This may indicate a brute force attack.

Attacker's Goals

Attackers attempt to log in to a remote host.

Investigative actions

Verify any successful authentication by the user account referenced by the alert, as these can indicate the attacker managed to guess the credentials.

30.336 | New Shared User Account

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	10 Hours
Deduplication Period	30 Days
Required Data	- Requires: - XDR Agent
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Low

Description

A user account has been seen active on multiple hosts.

Shared accounts are often considered 'bad practice' and may present multiple security risks to the organization.

Attacker's Goals

Gaining access to a shared account and multiple hosts and systems throughout the organization.

Investigative actions

Ensure that the shared account is legitimate and has a justified role in the organization.

30.337 | Abnormal ICMP echo (PING) to multiple hosts

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	5 Hours
Deduplication Period	2 Days
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Remote System Discovery (T1018)
Severity	Low

Description

An endpoint performed an abnormal ICMP echo (PING) to multiple hosts on the network.

Attacker's Goals

An adversary may use the ICMP protocol to map IP addresses, hostnames and segments to plan its lateral movement over the network.

Investigative actions

- Verify if the host is a newly deployed host.
- Verify if newly services or applications that require network mapping were installed on the initiating host.

30.338 | Multiple users authenticated with weak NTLM to a host

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Day
Required Data	- Requires: - XDR Agent
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Use Alternate Authentication Material (T1550)
Severity	Informational

Description

Multiple user accounts authenticated to a host via NTLMv1 or LM authentication for the first time in the past 30 days. This may be a result of an NTLM downgrade attack
A downgrade attack may force the client to authenticate with a weaker hash/protocol (such as NTLMv1 or even LM) instead of NTLMv2.

Attacker's Goals

The attacker attempts to gain access to the accounts.

Investigative actions

- Audit all login events with a weaker protocol and review any anomalous usage.
- Investigate the mentioned host for additional suspicious activity.

30.339 | Internal Login Password Spray

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	Identity Analytics
Detector Tags	

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force: Password Spraying (T1110.003)
Severity	Informational

Description

An abnormally high amount of user account login attempts were seen from a host within a short period of time.
This may have resulted from a login password spray attack.

Attacker's Goals

An attacker may be attempting to gain unauthorized access to user accounts.

Investigative actions

- Check the amount of time in between each authentication attempt.
- Investigate the reason behind the login failures and if any accounts were locked out.
- Look for any successful authentication attempts and the ratio of login success versus login failures.

Variations

Suspicious intensive and short internal Login Password Spray

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force: Password Spraying (T1110.003)
Severity	Medium

Description

An abnormally high number of login attempts within a very short period of time and suspicious automated behavior.

Attacker's Goals

An attacker may be attempting to gain unauthorized access to user accounts.

Investigative actions

Check the amount of time in between each authentication attempt.

Investigate the reason behind the login failures and if any accounts were locked out.

- Look for any successful authentication attempts and the ratio of login success versus login failures.

Internal Login Password Spray with many wrong password attempts

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force: Password Spraying (T1110.003)
Severity	Low

Description

An abnormally high amount of user account login attempts with wrong password were seen with a wrong password within a short period of time.

Attacker's Goals

An attacker may be attempting to gain unauthorized access to user accounts.

Investigative actions

- Check the amount of time in between each authentication attempt.
  Investigate the reason behind the login failures and if any accounts were locked out.
  Look for any successful authentication attempts and the ratio of login success versus login failures.

Internal Login Password Spray attempt on local user

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force: Password Spraying (T1110.003)
Severity	Low

Description

An abnormally high number of login attempts with the same username to different domains or local machines within a short period of time.

Attacker's Goals

An attacker may be attempting to gain unauthorized access to user accounts.

Investigative actions

Check the amount of time in between each authentication attempt.
Investigate the reason behind the login failures and if any accounts were locked out.

Look for any successful authentication attempts and the ratio of login success versus login failures.

30.340 | Possible external RDP Brute-Force

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	10 Minutes
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force: Password Guessing (T1110.001)
Severity	Low

Description

Multiple failed remote logins originated from an external ip with at least one successful login. This may indicate a successful brute-force attack.

Attacker's Goals

The attacker attempts to gain access to the accounts.

Investigative actions

If the source IP is an internal IP, adjust network ip ranges.
Identify the user performing RDP and check that it is authorized.

Check whether this IP has a malicious reputation.
- Reset the user's password.
- Follow further actions done by the user.

Variations

Potential External Brute-Force via RDP on Sensitive User

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force: Password Guessing (T1110.001)
Severity	Medium

Description

Multiple failed remote logins from an external IP with a sensitive user and at least one successful login.
This may indicate a successful brute-force attack.

Attacker's Goals

The attacker attempts to gain access to the accounts.

Investigative actions

- If the source IP is an internal IP, adjust network ip ranges.
- Identify the user performing RDP and check that it is authorized.
- Check whether this IP has a malicious reputation.
- Reset the user's password.
- Follow further actions done by the user.

30.341 | New Administrative Behavior

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	12 Hours
Deduplication Period	1 Day
Required Data	- Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent OR - Third-Party Firewalls
Detection Modules	
Detector Tags	NDR Lateral Movement Analytics
ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Services (T1021)
Severity	Medium

Description

The endpoint performed new administrative actions, relative to its previously profiled behavior. It is possible that an endpoint will infrequently be used for administrative activities, so analytics is performed using logs collected over a long period of time, also comparing the activity to that of other endpoints. That is, if many endpoints are contacting the same destination with the same administrative activity, then this network activity is less likely to result in this alert.

An attacker may be operating on the host, probing other computers and moving laterally inside the network using a trusted computer and credentials. Attackers typically exhibit administrative behaviors when performing reconnaissance and lateral movement.

Attacker's Goals

An attacker is using administrative functions to move from one endpoint to another, or to scan the network for new endpoints to attack.

Investigative actions

Investigate the endpoint to determine if it is legitimately being used for administrative functions.

Variations

New SSH Administrative Behavior

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Services (T1021)
Severity	Informational

Description

The endpoint performed new SSH administrative actions, relative to its previously profiled behavior. It is possible that an endpoint will infrequently be used for administrative activities, so analytics is performed using logs collected over a long period of time, also comparing the activity to that of other endpoints. That is, if many endpoints are contacting the same destination with the same administrative activity, then this network activity is less likely to result in this alert.

An attacker may be operating on the host, probing other computers and moving laterally inside the network using a trusted computer and credentials. Attackers typically exhibit administrative behaviors when performing reconnaissance and lateral movement.

Attacker's Goals

An attacker is using administrative functions to move from one endpoint to another, or to scan the network for new endpoints to attack.

Investigative actions

Investigate the endpoint to determine if it is legitimately being used for administrative functions.

30.342 | Account probing

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Initial Access (TA0001) Credential Access (TA0006)
ATT&CK Technique	Valid Accounts (T1078) Brute Force (T1110)
Severity	Low

Description

A user failed to log in to multiple hosts it never accessed before in a short amount of time. This may indicate the account is compromised and an attacker is probing for a host it can access with those credentials.

Attacker's Goals

Gain access to hosts by using stolen user-account credentials.

Investigative actions

Check if the user account was compromised, and which resources it could access.

30.343 | Failed DNS

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	2 Hours
Deduplication Period	2 Hours
Required Data	Requires one of the following data sources: - Palo Alto Networks Platform Logs OR ▯ XDR Agent
Detection Modules	
Detector Tags	

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Dynamic Resolution: Domain Generation Algorithms (T1568.002)
Severity	Low

Description

The endpoint is performing DNS lookups that are failing at an excessively high rate when compared to its peer group. This alert might be symptomatic of malware that is trying to connect to its command and control (C2) servers.

The attacker's C2 server runs on one or more domains that can eventually be identified and blacklisted. To avoid this, malware will sometimes use Domain Generation Algorithms (DGA) that produce many domain names every day. Because only a few of these domains are ever registered, the installed malware must blindly try to access each generated domain name in an effort to locate an active one.

Attacker's Goals

Communicate with malware running on your network to control malware activities, perform software updates on the malware, or to take inventory of infected machines.

Investigative actions

- Make sure your DNS servers are not misconfigured and are responsive. This detector assumes that most DNS lookups succeed, and will only raise an alert when it sees large numbers of failed lookups. Misconfigured or unresponsive DNS servers can result in a false positive.
- Make sure you do not have external domains configured as internal domains. This can result in clients attempting to (for example) resolve google.com.local first, before resolving google.com. This can result in a false-positive for this alert.
  Make sure the endpoint is configured properly for your DNS servers. For example, make sure it is configured to use the correct DNS IP address, and that the IP address is not for a firewalled DNS server. Misconfigured DNS clients can result in many failed lookups, which will result in a false-positive for this alert.
- Make sure the endpoint is not a DNS, Proxy, NAT or VPN gateway server. If these have been misdetected by Cortex XDR Analytics, then their ordinary operations can trigger this alert.

30.344 | Multiple discovery commands

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
Deduplication Period	1 Day
Required Data	Requires: XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Remote System Discovery (T1018) System Information Discovery (T1082) System Network Configuration Discovery (T1016) System Service Discovery (T1007)
Severity	Low

Description

The alerted causality performed multiple discovery commands in a short timeframe.

Attacker's Goals

Collect information about the host, network and user configuration for lateral movement and privilege escalation.

Investigative actions

- Verify if the script or process initiating the discovery commands is benign.
  Verify that this isn't sanctioned IT activity.

  Look for other hosts executing similar commands.

Variations

Multiple discovery commands from a web server CGO

Synopsis

ATT&CK Tactic	Persistence (TA0003) Discovery (TA0007)
ATT&CK Technique	Server Software Component: Web Shell (T1505.003) Remote System Discovery (T1018) System Information Discovery (T1082) System Network Configuration Discovery (T1016) System Service Discovery (T1007)
Severity	Medium

Description

The alerted causality performed multiple discovery commands in a short timeframe.

Attacker's Goals

Collect information about the host, network and user configuration for lateral movement and privilege escalation.

Investigative actions

Verify if the script or process initiating the discovery commands is benign.
- Verify that this isn't sanctioned IT activity.
- Look for other hosts executing similar commands.

Multiple discovery commands from an SQL server CGO

Synopsis

ATT&CK Tactic	Persistence (TA0003) Discovery (TA0007)
ATT&CK Technique	Server Software Component: SQL Stored Procedures (T1505.001) Remote System Discovery (T1018) System Information Discovery (T1082) System Network Configuration Discovery (T1016) System Service Discovery (T1007)
Severity	Medium

Description

The alerted causality performed multiple discovery commands in a short timeframe.

Attacker's Goals

Collect information about the host, network and user configuration for lateral movement and privilege escalation.

Investigative actions

- Verify if the script or process initiating the discovery commands is benign.
Verify that this isn't sanctioned IT activity.
Look for other hosts executing similar commands.

Multiple discovery commands from an unsigned causality

Synopsis

ATT&CK Tactic	Discovery (TA0007)

ATT&CK Technique	- Remote System Discovery (T1018) - System Information Discovery (T1082) - System Network Configuration Discovery (T1016) - System Service Discovery (T1007)
Severity	Medium

Description

The alerted causality performed multiple discovery commands in a short timeframe.

Attacker's Goals

Collect information about the host, network and user configuration for lateral movement and privilege escalation.

Investigative actions

- Verify if the script or process initiating the discovery commands is benign.
- Verify that this isn't sanctioned IT activity.
- Look for other hosts executing similar commands.

Multiple discovery commands from a standard IT tool

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	- Remote System Discovery (T1018) - System Information Discovery (T1082) - System Network Configuration Discovery (T1016) - System Service Discovery (T1007)
Severity	Informational

Description

The alerted causality performed multiple discovery commands in a short timeframe.

Attacker's Goals

Collect information about the host, network and user configuration for lateral movement and privilege escalation.

Investigative actions

Verify if the script or process initiating the discovery commands is benign.
Verify that this isn't sanctioned IT activity.

Look for other hosts executing similar commands.

30.345 | Possible Brute-Force attempt

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	15 Minutes
Deduplication Period	1 Day
Required Data	Requires: ▯ XDR Agent
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	▮ Credential Access (TA0006) Lateral Movement (TA0008)

ATT&CK Technique	Brute Force (T1110) Remote Services (T1021)
Severity	Informational

Description

This may indicate a brute-force attack.

Attacker's Goals

The attacker attempts to gain access to the accounts.

Investigative actions

Verify any successful authentication by the user account referenced by the alert, as these can indicate the attacker managed to guess the credentials.

Variations

Possible Brute-Force attempt with a successful login and suspicious characteristics

Synopsis

ATT&CK Tactic	Credential Access (TA0006) Lateral Movement (TA0008)
ATT&CK Technique	Brute Force (T1110) Remote Services (T1021)
Severity	Low

Description

This may indicate a brute-force attack.

Attacker's Goals

The attacker attempts to gain access to the accounts.

Investigative actions

Verify any successful authentication by the user account referenced by the alert, as these can indicate the attacker managed to guess the credentials.

30.346 | HTTP with suspicious characteristics

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	2 Hours
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Palo Alto Networks Platform Logs OR ▯ XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	ı Command and Control (TA0011) Exfiltration (TA0010)

ATT&CK Technique	- Web Service (T1102) - Exfiltration Over Web Service (T1567)
Severity	Low

Description

Uncommon HTTP communication was performed by the host that might indicate its attempt to hide malicious activities.

Attacker's Goals

Data exfiltration, attack tool staging or command and control channel through a trusted service.

Investigative actions

- Examine the legitimacy of the application that produced this uncommon connection.
- Examine the parent process of this application.
  Check for anomalies at the time when the communication occurred.

Variations

HTTP with suspicious characteristics which is repetitive

Synopsis

ATT&CK Tactic	- Command and Control (TA0011) Exfiltration (TA0010)
ATT&CK Technique	- Web Service (T1102) Exfiltration Over Web Service (T1567)
Severity	Low

Description

Repetitevne HTTP communication was performed by the host that might indicate its attempt to hide malicious activities.

Attacker's Goals

Data exfiltration, attack tool staging or command and control channel through a trusted service.

Investigative actions

- Examine the legitimacy of the application that produced this uncommon connection.
  Examine the parent process of this application.
  Check for anomalies at the time when the communication occurred.

HTTP with suspicious characteristics to an IP address

Synopsis

ATT&CK Tactic	Command and Control (TA0011) Exfiltration (TA0010)
ATT&CK Technique	Web Service (T1102) Exfiltration Over Web Service (T1567)
Severity	Low

Description

Uncommon HTTP communication to IP address was performed by the host that might indicate its attempt to hide malicious activities.

Attacker's Goals

Data exfiltration, attack tool staging or command and control channel through a trusted service.

Investigative actions

- Examine the legitimacy of the application that produced this uncommon connection.
- Examine the parent process of this application.
  Check for anomalies at the time when the communication occurred.

HTTP with suspicious characteristics that always fails

Synopsis

ATT&CK Tactic	Command and Control (TA0011) Exfiltration (TA0010)
ATT&CK Technique	Web Service (T1102) Exfiltration Over Web Service (T1567)
Severity	Informational

Description

Unsuccessful HTTP communication to IP address was performed by the host that might indicate its attempt to hide malicious activities.

Attacker's Goals

Data exfiltration, attack tool staging or command and control channel through a trusted service.

Investigative actions

Examine the legitimacy of the application that produced this uncommon connection.

- Examine the parent process of this application.
- Check for anomalies at the time when the communication occurred.

30.347 | Kerberos User Enumeration

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour

Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Account Discovery (T1087)
Severity	Medium

Description

A high amount of Kerberos principal unknown errors were generated on users in the last hour.

This may be indicative of Kerberos user enumeration.

Attacker's Goals

The attacker may attempt to gain an initial foothold in the domain by enumerating users and finding service accounts.

Investigative actions

- Check whether any service principal names (SPNs) were not set correctly, as they will always return a principal unknown error.

30.348 | Failed Connections

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Day
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent OR - Third-Party Firewalls
Detection Modules	
Detector Tags	
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Remote System Discovery (T1018)
Severity	Low

Description

The endpoint has failed connections to other endpoints that have been inactive for more than 24 hours, or that Cortex XDR Analytics has never seen on the network. The endpoint has made an abnormally large number of these failed connections and/or is attempting to connect to an abnormal mixture of missing or inactive endpoints.

Your network might contain legitimate scanners that could cause a false positive for this alert. Cortex XDR Analytics attempts to filter these out by checking if a scanner has been active for a long consecutive period of time. Consequently, if this alert is seen, it represents new activity on your network.

An attacker may be trying to move laterally, or to scan different parts of the network to look for other endpoints that expose a specific service. Worms also perform a similar activity to automatically infect additional hosts in the network.

Attacker's Goals

An attacker does not know your network and is exploring it for new or unknown subnets.

Investigative actions

- Validate that the source is not a sanctioned port scanner.
  Check for suspicious artifacts in the endpoint profile.

Variations

Failed Connections

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Remote System Discovery (T1018)
Severity	Informational

Description

The endpoint has failed connections to other endpoints that have been inactive for more than 24 hours, or that Cortex XDR Analytics has never seen on the network. The endpoint has made an abnormally large number of these failed connections and/or is attempting to connect to an abnormal mixture of missing or inactive endpoints.

Your network might contain legitimate scanners that could cause a false positive for this alert.

Cortex XDR Analytics attempts to filter these out by checking if a scanner has been active for a long consecutive period of time. Consequently, if this alert is seen, it represents new activity on your network.

An attacker may be trying to move laterally, or to scan different parts of the network to look for other endpoints that expose a specific service. Worms also perform a similar activity to automatically infect additional hosts in the network.

Attacker's Goals

An attacker does not know your network and is exploring it for new or unknown subnets.

Investigative actions

Validate that the source is not a sanctioned port scanner.
Check for suspicious artifacts in the endpoint profile.

Failed Connections with a rare causality and actor processes relations

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Remote System Discovery (T1018)
Severity	Informational

Description

The endpoint has failed connections to other endpoints that have been inactive for more than 24 hours, or that Cortex XDR Analytics has never seen on the network. The endpoint has made an abnormally large number of these failed connections and/or is attempting to connect to an abnormal mixture of missing or inactive endpoints.

Your network might contain legitimate scanners that could cause a false positive for this alert. Cortex XDR Analytics attempts to filter these out by checking if a scanner has been active for a long consecutive period of time. Consequently, if this alert is seen, it represents new activity on your network.

An attacker may be trying to move laterally, or to scan different parts of the network to look for other endpoints that expose a specific service. Worms also perform a similar activity to automatically infect additional hosts in the network.

These failed connections originated from a rare relation between an actor process and its causality.

Attacker's Goals

An attacker does not know your network and is exploring it for new or unknown subnets.

Investigative actions

Validate that the source is not a sanctioned port scanner.
Check for suspicious artifacts in the endpoint profile.

30.349 | DNS Tunneling

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Palo Alto Networks Platform Logs OR ▯ XDR Agent
Detection Modules	
Detector Tags	

ATT&CK Tactic	- Command and Control (TA0011) - Exfiltration (TA0010)
ATT&CK Technique	- Application Layer Protocol (T1071) - Exfiltration Over Alternative Protocol (T1048)
Severity	Low

Description

10 KB or more were sent encoded in subdomain names during a 10-minute window. All subdomains queried were under a single suspicious domain.

DNS tunneling encodes data in DNS queries and responses, allowing an attacker to bypass firewalls and proxies to reach his or her command and control server, even when HTTP/S traffic is blocked.

The endpoint may be remotely controlled by an attacker, and/or an attacker may have exfiltrated data from it. This detector is not supported when networking events arrive solely from Cortex XDR Linux agents.

Attacker's Goals

Communicate with malware running on your network to control malware activities, perform software updates on the malware, or to take inventory of infected machines.

Investigative actions

Verify that the source device or process is not an approved security solution.

- Verify if the DNS query types are non-standard. DNS tunnels use uncommon query types that enable encoding of more data. Examples include: INIT, PRIVATE, NULL, SRV, KEY, and TXT.

If the affected endpoint is operating Windows, verify that the DNS traffic is coming from svchost.exe and search for other processes that ran when the alert triggered. On Windows, the DNS requests go through svchost.exe.

- Verify the responses per DNS query. Many responses per query may indicate a tool being downloaded.

Verify the destination domain details and compare the number of endpoints in your network that access the domain over time to see if this is an uncommonly contacted domain.

- Verify the source web-browser traffic to determine if the process was generated by user action, if the user did not initiate the traffic it can be indicative of malicious activity.

Verify non-DNS traffic to the domain. Any traffic except DNS queries to the destination domain may indicate a legitimate domain and not used solely for command-and-control or data exfiltration.

Variations

DNS Tunneling

Synopsis

ATT&CK Tactic	Command and Control (TA0011) Exfiltration (TA0010)
ATT&CK Technique	Application Layer Protocol (T1071) Exfiltration Over Alternative Protocol (T1048)
Severity	Medium

Description

10 KB or more were sent encoded in subdomain names during a 10-minute window. All subdomains queried were under a single suspicious domain.

DNS tunneling encodes data in DNS queries and responses, allowing an attacker to bypass firewalls and proxies to reach his or her command and control server, even when HTTP/S traffic is blocked.

The endpoint may be remotely controlled by an attacker, and/or an attacker may have exfiltrated data from it. This detector is not supported when networking events arrive solely from Cortex XDR Linux agents.

Attacker's Goals

Communicate with malware running on your network to control malware activities, perform software updates on the malware, or to take inventory of infected machines.

Investigative actions

- Verify that the source device or process is not an approved security solution.
- Verify if the DNS query types are non-standard. DNS tunnels use uncommon query types that enable encoding of more data. Examples include: INIT, PRIVATE, NULL, SRV, KEY, and TXT.
- If the affected endpoint is operating Windows, verify that the DNS traffic is coming from svchost.exe and search for other processes that ran when the alert triggered. On Windows, the DNS requests go through svchost.exe.
- Verify the responses per DNS query. Many responses per query may indicate a tool being downloaded.
- Verify the destination domain details and compare the number of endpoints in your network that access the domain over time to see if this is an uncommonly contacted domain.
- Verify the source web-browser traffic to determine if the process was generated by user action, if the user did not initiate the traffic it can be indicative of malicious activity.
- Verify non-DNS traffic to the domain. Any traffic except DNS queries to the destination domain may indicate a legitimate domain and not used solely for command-and-control or data exfiltration.

30.350 | Suspicious container reconnaissance activity in a Kubernetes pod

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes

Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	Kubernetes - AGENT, Containers
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	- Remote System Discovery (T1018) - System Information Discovery (T1082) System Network Configuration Discovery (T1016) System Service Discovery (T1007) Container and Resource Discovery (T1613)
Severity	Informational

Description

A process performed multiple consecutive container discovery commands from within a Kubernetes Pod.

Attacker's Goals

Collect information about the host, network and user configuration for lateral movement and privilege escalation.

Investigative actions

Verify if the script or process initiating the discovery commands is benign.

Verify that this isn't sanctioned IT activity.

- Look for other hosts executing similar commands.

Variations

Suspicious container reconnaissance activity in a Kubernetes pod

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Remote System Discovery (T1018) System Information Discovery (T1082) System Network Configuration Discovery (T1016) System Service Discovery (T1007) Container and Resource Discovery (T1613)
Severity	Medium

Description

A process performed multiple consecutive container discovery commands from within a Kubernetes Pod.

Attacker's Goals

Collect information about the host, network and user configuration for lateral movement and privilege escalation.

Investigative actions

- Verify if the script or process initiating the discovery commands is benign.
- Verify that this isn't sanctioned IT activity.
- Look for other hosts executing similar commands.

Suspicious container reconnaissance activity in a Kubernetes pod

Synopsis

ATT&CK Tactic	Discovery (TA0007)

ATT&CK Technique	Remote System Discovery (T1018) System Information Discovery (T1082) System Network Configuration Discovery (T1016) System Service Discovery (T1007) Container and Resource Discovery (T1613)
Severity	Low

Description

A process performed multiple consecutive container discovery commands from within a Kubernetes Pod.

Attacker's Goals

Collect information about the host, network and user configuration for lateral movement and privilege escalation.

Investigative actions

- Verify if the script or process initiating the discovery commands is benign.
- Verify that this isn't sanctioned IT activity.
- Look for other hosts executing similar commands.

30.351 | Suspicious DNS traffic

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
Deduplication Period	1 Hour

Required Data	- Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Command and Control (TA0011) - Exfiltration (TA0010)
ATT&CK Technique	Application Layer Protocol (T1071) - Exfiltration Over Alternative Protocol (T1048)
Severity	Informational

Description

10 KB or more were sent encoded in subdomain names during a 10-minute window. All subdomains queried were under a single suspicious domain.
DNS tunneling encodes data in DNS queries and responses, allowing an attacker to bypass firewalls and proxies to reach his or her command and control server, even when HTTP/S traffic is blocked.

Attacker's Goals

- DNS tunneling, allowing an attacker to bypass firewalls and proxies to reach his or her command and control server, even when HTTP/S traffic is blocked.
  An attacker may also use this protocol to exfiltrated data from the compromised endpoint outside the network.

Investigative actions

Verify that the source device or process is not an approved security solution.

- Verify if the DNS query types are non-standard. DNS tunnels use uncommon query types that enable encoding of more data. Examples include: INIT, PRIVATE, NULL, SRV, KEY, and TXT.

  If the affected endpoint is operating Windows, verify that the DNS traffic is coming from svchost.exe and search for other processes that ran when the alert triggered. On Windows, the DNS requests go through svchost.exe.
- Verify the responses per DNS query. Many responses per query may indicate a tool being downloaded.

  Verify the destination domain details and compare the number of endpoints in your network that access the domain over time to see if this is an uncommonly contacted domain.
- Verify the source web-browser traffic to determine if the process was generated by user action, if the user did not initiate the traffic it can be indicative of malicious activity.

  Verify non-DNS traffic to the domain. Any traffic except DNS queries to the destination domain may indicate a legitimate domain and not used solely for command-and-control or data exfiltration.

Variations

Suspicious DNS traffic with a rarely seen domain

Synopsis

ATT&CK Tactic	Command and Control (TA0011) Exfiltration (TA0010)
ATT&CK Technique	Application Layer Protocol (T1071) Exfiltration Over Alternative Protocol (T1048)
Severity	Low

Description

10 KB or more were sent encoded in subdomain names during a 10-minute window. All subdomains queried were under a single suspicious domain.

DNS tunneling encodes data in DNS queries and responses, allowing an attacker to bypass firewalls and proxies to reach his or her command and control server, even when HTTP/S traffic is blocked.

This domain was rarely seen in this tenant.

Attacker's Goals

DNS tunneling, allowing an attacker to bypass firewalls and proxies to reach his or her command and control server, even when HTTP/S traffic is blocked.

- An attacker may also use this protocol to exfiltrated data from the compromised endpoint outside the network.

Investigative actions

Verify that the source device or process is not an approved security solution.

Verify if the DNS query types are non-standard. DNS tunnels use uncommon query types that enable encoding of more data. Examples include: INIT, PRIVATE, NULL, SRV, KEY, and TXT.
If the affected endpoint is operating Windows, verify that the DNS traffic is coming from svchost.exe and search for other processes that ran when the alert triggered. On Windows,

the DNS requests go through svchost.exe.

- Verify the responses per DNS query. Many responses per query may indicate a tool being downloaded.
Verify the destination domain details and compare the number of endpoints in your network that access the domain over time to see if this is an uncommonly contacted domain.

Verify the source web-browser traffic to determine if the process was generated by user action, if the user did not initiate the traffic it can be indicative of malicious activity.

- Verify non-DNS traffic to the domain. Any traffic except DNS queries to the destination domain may indicate a legitimate domain and not used solely for command-and-control or data exfiltration.

Suspicious DNS traffic with a globally rare DNS query length

Synopsis

ATT&CK Tactic	Command and Control (TA0011) Exfiltration (TA0010)
ATT&CK Technique	Application Layer Protocol (T1071) Exfiltration Over Alternative Protocol (T1048)
Severity	Low

Description

10 KB or more were sent encoded in subdomain names during a 10-minute window. All subdomains queried were under a single suspicious domain.
DNS tunneling encodes data in DNS queries and responses, allowing an attacker to bypass

firewalls and proxies to reach his or her command and control server, even when HTTP/S traffic is

blocked.
The combination of the DNS queries along with this root domain is globally rare.

Attacker's Goals

- DNS tunneling, allowing an attacker to bypass firewalls and proxies to reach his or her command and control server, even when HTTP/S traffic is blocked.
  An attacker may also use this protocol to exfiltrated data from the compromised endpoint outside the network.

Investigative actions

- Verify that the source device or process is not an approved security solution.
- Verify if the DNS query types are non-standard. DNS tunnels use uncommon query types that enable encoding of more data. Examples include: INIT, PRIVATE, NULL, SRV, KEY, and TXT.

  If the affected endpoint is operating Windows, verify that the DNS traffic is coming from svchost.exe and search for other processes that ran when the alert triggered. On Windows, the DNS requests go through svchost.exe.
  Verify the responses per DNS query. Many responses per query may indicate a tool being downloaded.

  Verify the destination domain details and compare the number of endpoints in your network that access the domain over time to see if this is an uncommonly contacted domain.
- Verify the source web-browser traffic to determine if the process was generated by user action, if the user did not initiate the traffic it can be indicative of malicious activity.
  Verify non-DNS traffic to the domain. Any traffic except DNS queries to the destination domain may indicate a legitimate domain and not used solely for command-and-control or data exfiltration.

30.352 | NTLM Brute Force on an Administrator Account

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes

Deduplication Period	1 Day
Required Data	Requires: ▯ XDR Agent
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force (T1110)
Severity	Low

Description

- This may indicate an NTLM brute-force attack.

Attacker's Goals

The attacker attempts to gain access to the administrator accounts.

Investigative actions

Verify any successful authentication by the user account referenced by the alert, as these can indicate the attacker managed to guess the credentials.

31 | XDR Agent with eXtended Threat Hunting (XTH)

31.1 | Space after filename

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Masquerading: Space after Filename (T1036.006)
Severity	Informational

Description

A file was created or renamed to have a space at the end of its name.

Attacker's Goals

Attackers may try to change the extension of the file to evade detection.

Investigative actions

- Verify that this isn't IT activity.
- Look for other hosts executing similar commands.

31.2 | Unusual Netsh PortProxy rule

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	- Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005) Command and Control (TA0011)
ATT&CK Technique	Impair Defenses: Disable or Modify System Firewall (T1562.004) Proxy: Internal Proxy (T1090.001)

Severity	Low

Description

Attackers may use Netsh PortProxy rules as part of malicious actions performed in an organizational network (e.g., for tunneling).

Attacker's Goals

Adding or deleting netsh forwarding rules as a proxy and to avoid possible detection.

Investigative actions

- Check the connect address and if it's a known IP/domain.
- Check whether the causality group owner (CGO) process is benign, and if this was a desired behavior as part of its normal execution flow.

Variations

Unusual Netsh PortProxy rule by non-netsh process

Synopsis

ATT&CK Tactic	- Defense Evasion (TA0005) Command and Control (TA0011)
ATT&CK Technique	- Impair Defenses: Disable or Modify System Firewall (T1562.004) Proxy: Internal Proxy (T1090.001)
Severity	Medium

Description

Attackers may use Netsh PortProxy rules as part of malicious actions performed in an organizational network (e.g., for tunneling).

Attacker's Goals

Adding or deleting netsh forwarding rules as a proxy and to avoid possible detection.

Investigative actions

- Check the connect address and if it's a known IP/domain.
- Check whether the causality group owner (CGO) process is benign, and if this was a desired behavior as part of its normal execution flow.

Unusual Netsh PortProxy rule by an unsigned causality actor

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005) Command and Control (TA0011)
ATT&CK Technique	Impair Defenses: Disable or Modify System Firewall (T1562.004) Proxy: Internal Proxy (T1090.001)
Severity	Medium

Description

Attackers may use Netsh PortProxy rules as part of malicious actions performed in an organizational network (e.g., for tunneling).

Attacker's Goals

Adding or deleting netsh forwarding rules as a proxy and to avoid possible detection.

Investigative actions

Check the connect address and if it's a known IP/domain.
- Check whether the causality group owner (CGO) process is benign, and if this was a desired behavior as part of its normal execution flow.

31.3 | Uncommon SetWindowsHookEx API invocation of a

possible keylogger

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	- Credential Access (TA0006) Collection (TA0009)
ATT&CK Technique	Input Capture: Keylogging (T1056.001)
Severity	Medium

Description

A process installed a Windows desktop hook by calling the SetWindowsHookEx API function with an unpopular module. This behavior is commonly seen in keyloggers.

Attacker's Goals

Attackers can monitor keyboard events as another way for credential gathering or to collect more user data over time for espionage purposes.

Investigative actions

- Check if the process has a user interface (a visible window).
  Check if the process has an option to set or modify keyboard hot-keys.

  Check if the process is part of a remote control tool.
  Check if the process is a known user application that was updated recently.
- Check if the process is built with AutoHotkey and is known to the user.
- If the process is a scripting engine or a hosting executable, check the actor process command line.
  Investigate the endpoint if the process writes files to disk.

31.4 | Uncommon Security Support Provider (SSP) registered via a registry key

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	

Detector Tags	
ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Boot or Logon Autostart Execution: Security Support Provider (T1547.005)
Severity	Low

Description

Security Support Provider (SSP) exposes a number of callbacks to be invoked during certain authentication and authorization events.
An attacker may register SSP to try and gain access to clear text passwords.

Attacker's Goals

Gain clear text passwords and persistency in the network.

Investigative actions

Audit the specific key values to verify that the additional values are trusted.

31.5 | Suspicious Print System Remote Protocol usage by a process

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)

Deduplication Period	1 Day
Required Data	Requires: • XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Forced Authentication (T1187)
Severity	Low

Description

A host which is trusted for unconstrained delegation initiated an SMB connection to a DC using the Print System Remote Protocol. An attacker can abuse such sessions for relay attacks.

Attacker's Goals

Elevate privileges from standard domain user to domain admin.

Investigative actions

- Check if the domain controller is patched or vulnerable to the attack.
- Check if the suspected account is compromised.
- Check if the source machine is trusted for unconstrained delegation and verify that the machine's configuration should stay that way.
- Follow actions by the account and if it performed a DCSync.

31.6 | Suspicious Udev driver rule execution manipulation

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: • XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Persistence (TA0003) Privilege Escalation (TA0004)
ATT&CK Technique	Boot or Logon Autostart Execution: Kernel Modules and Extensions (T1547.006)
Severity	Low

Description

Udev driver rule was modified with unusual pattern, might be used by adversaries to backdoor existing drivers.

Attacker's Goals

Adversaries can use this technique to execute arbitrary commands once the machine boots.

Investigative actions

- Check if the action was done using an automation service.
- Check the rule modification content and look for any suspicious payloads.
Check if there are any other suspicious activities originated from the same machine/executing user.

Variations

Unusual Udev driver rule execution manipulation

Synopsis

ATT&CK Tactic	Persistence (TA0003) Privilege Escalation (TA0004)
ATT&CK Technique	Boot or Logon Autostart Execution: Kernel Modules and Extensions (T1547.006)
Severity	Low

Description

Udev driver rule was modified with unusual pattern, might be used by adversaries to backdoor existing drivers.

Attacker's Goals

Adversaries can use this technique to execute arbitrary commands once the machine boots.

Investigative actions

Check if the action was done using an automation service.

Check the rule modification content and look for any suspicious payloads.

- Check if there are any other suspicious activities originated from the same machine/executing user.

31.7 | A compiled HTML help file wrote a script file to the disk

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	System Binary Proxy Execution: Compiled HTML File (T1218.001)
Severity	Low

Description

A compiled HTML help file wrote a script file to the disk. Compiled HTLM help files usually don't write script files to the disk. This behavior is often employed by malware that leverage malicious CHM files to deliver a 2nd stage payload.

Attacker's Goals

Deliver a 2nd stage payload or to avoid detection.

Investigative actions

- Check whether the initiator process is benign or normal for the host and/or user performing it.
  Check the file that was written to the disk for malicious activities.

31.8 | Potential SCCM credential harvesting using WMI detected

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Execution (TA0002) Credential Access (TA0006)

ATT&CK Technique	- Windows Management Instrumentation (T1047) - Unsecured Credentials (T1552)
Severity	Low

Description

Attackers or malware may use WMI queries to obtain domain credentials that are used by the SCCM.

Attacker's Goals

Obtain credentials used by the SCCM service.

Investigative actions

- Examine the process that executed the WMI query and the CGO and verify that the processes are from a trusted source.
  Inspect the system for malicious activity that is related to that process.

Variations

Potential SCCM credential harvesting using WMI detected from a remote machine

Synopsis

ATT&CK Tactic	- Execution (TA0002) Credential Access (TA0006)
ATT&CK Technique	- Windows Management Instrumentation (T1047) Unsecured Credentials (T1552)
Severity	Medium

Description

Attackers or malware may use WMI queries to obtain domain credentials that are used by the SCCM.

Attacker's Goals

Obtain credentials used by the SCCM service.

Investigative actions

- Examine the process that executed the WMI query and the CGO and verify that the processes are from a trusted source.
  Inspect the system for malicious activity that is related to that process.

Potential SCCM inventory query using WMI detected

Synopsis

ATT&CK Tactic	Execution (TA0002) Credential Access (TA0006)
ATT&CK Technique	Windows Management Instrumentation (T1047) Unsecured Credentials (T1552)
Severity	Low

Description

Attackers or malware may use WMI queries to obtain domain credentials that are used by the SCCM.

Attacker's Goals

Obtain credentials used by the SCCM service.

Investigative actions

- Examine the process that executed the WMI query and the CGO and verify that the processes are from a trusted source.
  Inspect the system for malicious activity that is related to that process.

31.9 | A browser extension was installed or loaded in an

uncommon way

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	Chromium Extensions Analytics
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Browser Extensions (T1176)
Severity	Informational

Description

A browser extension was installed or loaded in an uncommon way.

Attacker's Goals

Gain persistency on a machine and steal sensitive browsing data.

Investigative actions

Investigate the extension files and the process that installed it.

- Check if this extension is currently present at the relevant extensions web store by looking up for its extension ID.

Variations

A browser was forced to load an extension using a special command line argument

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Browser Extensions (T1176)
Severity	Low

Description

A browser was forced to load an extension using a special command line argument, an uncommon method.

Attacker's Goals

Gain persistency on a machine and steal sensitive browsing data.

Investigative actions

- Investigate the extension files and the process that installed it.
- Check if this extension is currently present at the relevant extensions web store by looking up for its extension ID.

A browser extension was installed or loaded in an uncommon way by a LOLBIN process

Synopsis

ATT&CK Tactic	Persistence (TA0003)

ATT&CK Technique	Browser Extensions (T1176)
Severity	Low

Description

A browser extension was installed or loaded in an uncommon way.

Attacker's Goals

Gain persistency on a machine and steal sensitive browsing data.

Investigative actions

Investigate the extension files and the process that installed it.

- Check if this extension is currently present at the relevant extensions web store by looking up for its extension ID.

A browser extension was installed or loaded in an uncommon way by an uncommon process

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Browser Extensions (T1176)
Severity	Low

Description

A browser extension was installed or loaded in an uncommon way.

Attacker's Goals

Gain persistency on a machine and steal sensitive browsing data.

Investigative actions

Investigate the extension files and the process that installed it.

- Check if this extension is currently present at the relevant extensions web store by looking up for its extension ID.

31.10 | Unusual Encrypting File System Remote call (EFSRPC) to domain controller

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	- Requires: ▯ XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	- Forced Authentication (T1187) Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay (T1557.001)

Severity	Low

Description

An unusual Encrypting File System Remote call (EFSRPC) was made to a domain controller.

Attacker's Goals

An attacker can abuse the Encrypting File System Remote Protocol to coerce an authentication from a DC.

- This authentication can later be used for obtaining a DC certificate for DCSync.

Investigative actions

- Check for a suspicious process on the initiator.
  Check if the source host is a vulnerability scanner.
  Check for unusual connections from the server of the requested file location (it may be a relay server).
- Look for unusual AD CS certificate requests.
- Look for following suspicious connections using the DC machine account.
  Check for possible DCSync alerts.

Variations

A suspicious Encrypting File System Remote call (EFSRPC) was made to a domain controller

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Forced Authentication (T1187) Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay (T1557.001)
Severity	Medium

Description

An unusual Encrypting File System Remote call (EFSRPC) was made to a domain controller.

Attacker's Goals

- An attacker can abuse the Encrypting File System Remote Protocol to coerce an authentication from a DC.
  This authentication can later be used for obtaining a DC certificate for DCSync.

Investigative actions

Check for a suspicious process on the initiator.
Check if the source host is a vulnerability scanner.
- Check for unusual connections from the server of the requested file location (it may be a relay server).
Look for unusual AD CS certificate requests.
Look for following suspicious connections using the DC machine account.

Check for possible DCSync alerts.

31.11 | Unusual use of a 'SysInternals' tool

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: ▯ XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Obfuscated Files or Information (T1027)
Severity	Informational

Description

An attacker may be trying to avoid detection by using obfuscated copy of SysInternals tools.

Attacker's Goals

- Attacker may use SysInternals tools for lateral movement, credentials access or delete recovery backups for impact.

Investigative actions

Check if the file is familiar to the user, if not, investigate further the source of it.

Variations

Unusual use of a 'SysInternals' tool by a process with an invalid or non-standard signature

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Obfuscated Files or Information (T1027)
Severity	High

Description

An attacker may be trying to avoid detection by using obfuscated copy of SysInternals tools.

Attacker's Goals

> Attacker may use SysInternals tools for lateral movement, credentials access or delete recovery backups for impact.

Investigative actions

- Check if the file is familiar to the user, if not, investigate further the source of it.

Unusual use of a 'SysInternals' tool that can be used for offensive operations

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Obfuscated Files or Information (T1027)
Severity	High

Description

An attacker may be trying to avoid detection by using obfuscated copy of SysInternals tools.

Attacker's Goals

> Attacker may use SysInternals tools for lateral movement, credentials access or delete recovery backups for impact.

Investigative actions

- Check if the file is familiar to the user, if not, investigate further the source of it.

31.12 | System profiling WMI query execution

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Execution (TA0002) Discovery (TA0007)
ATT&CK Technique	Windows Management Instrumentation (T1047) System Information Discovery (T1082)
Severity	Informational

Description

Attackers or malware may use WMI queries to identify the system and evade execution in sandbox environments.

Attacker's Goals

Attacker or malware can use WMI queries to identify system components and prevent execution in sandbox \ virtualized environments to evade detection.

Investigative actions

Examine the process that executed the WMI query and verify that the process is from a trusted source.

- Inspect the system for suspicious activity that is related to that process.

31.13 | Browser Extension Installed

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	❙ Requires: ▯ XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	Chromium Extensions Analytics
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Browser Extensions (T1176)
Severity	Informational

Description

Uncommon browser extension installed.

Attacker's Goals

Establish persistent access to victim systems through Chromium-based browser, steal sensitive data such credentials, cookies hijacking and financial data.

Investigative actions

- Investigate the extension and how it was loaded.
  Check if this extension is currently present at the relevant extensions web store by looking up for its extension ID.

Variations

Uncommon Browser Extension Installed

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Browser Extensions (T1176)
Severity	Low

Description

Uncommon browser extension installed.

Attacker's Goals

Establish persistent access to victim systems through Chromium-based browser, steal sensitive data such credentials, cookies hijacking and financial data.

Investigative actions

- Investigate the extension and how it was loaded.
  Check if this extension is currently present at the relevant extensions web store by looking up for its extension ID.

31.14 | Sensitive account password reset attempt

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Account Access Removal (T1531)
Severity	Informational

Description

An attempt was made to reset a sensitive account's password.

Attacker's Goals

An attacker may attempt to gain access to the account.

Investigative actions

- Verify this action with the user who performed the change.

Variations

Sensitive account password reset attempt for the first time

Synopsis

ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Account Access Removal (T1531)
Severity	Low

Description

An attempt was made to reset a sensitive account's password.

Attacker's Goals

An attacker may attempt to gain access to the account.

Investigative actions

Verify this action with the user who performed the change.

31.15 | Uncommon jsp file write by a Java process

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Server Software Component: Web Shell (T1505.003)
Severity	Medium

Description

An uncommon jsp file was written by a Java process.

Attacker's Goals

Persistence on the host.

Investigative actions

- Check if the file was added during regular java process actions.
- Check if the jsp file contains malicious content.

31.16 | Discovery of misconfigured certificate templates using LDAP

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	LDAP Analytics (Client), LDAP Analytics (Server)
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	File and Directory Discovery (T1083)
Severity	Medium

Description

An LDAP query searching for misconfigured certificate templates was executed.

Attacker's Goals

An attacker can use misconfigured certificate templates for escalation and authentication.

Investigative actions

- Check if the LDAP search query was allowed for the user (logged on at event time) or process.
  Investigate the LDAP search query for any suspicious indicators.

31.17 | A user certificate was issued with a mismatch

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	

ATT&CK Tactic	Persistence (TA0003) Privilege Escalation (TA0004) Credential Access (TA0006)
ATT&CK Technique	Account Manipulation (T1098) Valid Accounts (T1078) Steal or Forge Authentication Certificates (T1649)
Severity	Informational

Description

A certificate was issued to a user who was not the requester, this may indicate a certificate manipulation.

Attacker's Goals

Attackers may try to obtain certificates for privileged accounts or systems they do not normally have access to, to gain elevated access and move laterally within the network.

Investigative actions

- Verify the activity with the performing user.
- Identify if the requester is a user or system that normally requests certificates on behalf of other entities (e.g., a Mobile Device Management system).
- Search for further indicators of potential compromise, including atypical login behaviors, unauthorized attempts at privilege escalation, or lateral movements within the network attributed to the requester.
- Examine whether the mismatch between the requester and the subject is consistent with known and anticipated practices, or if it represents an unusual deviation.
- Check for possible certificate authentications with the subject user.

Variations

Suspicious certificate issuance with a mismatch

Synopsis

ATT&CK Tactic	Persistence (TA0003) Privilege Escalation (TA0004) Credential Access (TA0006)
ATT&CK Technique	Account Manipulation (T1098) Valid Accounts (T1078) Steal or Forge Authentication Certificates (T1649)
Severity	Low

Description

A user certificate was issued with a mismatch. This requester doesn't usually ask for a certificates on behalf of another subject. This may indicate a certificate manipulation.

Attacker's Goals

Attackers may try to obtain certificates for privileged accounts or systems they do not normally have access to, to gain elevated access and move laterally within the network.

Investigative actions

- Verify the activity with the performing user.
- Identify if the requester is a user or system that normally requests certificates on behalf of other entities (e.g., a Mobile Device Management system).
- Search for further indicators of potential compromise, including atypical login behaviors, unauthorized attempts at privilege escalation, or lateral movements within the network attributed to the requester.
- Examine whether the mismatch between the requester and the subject is consistent with known and anticipated practices, or if it represents an unusual deviation.
- Check for possible certificate authentications with the subject user.

31.18 | Mailbox Client Access Setting (CAS) changed

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Data Staged: Local Data Staging (T1074.001)
Severity	Medium

Description

An attacker may use PowerShell to change the Client Access Settings (CAS) for a mailbox, hence gaining access to the data.

Attacker's Goals

Gain access to the data in the compromised mailbox.

Investigative actions

- Examine the PowerShell command to identify which mailbox's access setting has been modified.
  verify that the change in the client access setting was executed by a trusted source.

31.19 | Service ticket request with a spoofed sAMAccountName

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	3 Hours
Required Data	- Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	- Privilege Escalation (TA0004) - Persistence (TA0003)

ATT&CK Technique	- Account Manipulation (T1098) - Valid Accounts (T1078)
Severity	Medium

Description

A Kerberos service ticket (ST) was requested for an account with a spoofed sAMAccountName.

Attacker's Goals

Elevate privileges from standard domain user to domain admin.

Investigative actions

Check if the domain controller is patched or vulnerable to the attack.

- Look for associated sAMAccountName rename events.
- Follow actions by the account and if it performed a DCSync.

31.20 | PowerShell used to remove mailbox export request logs

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day

Required Data	- Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Command and Scripting Interpreter: PowerShell (T1059.001)
Severity	High

Description

An attacker may use PowerShell to remove evidence of an export request for a mailbox as part of the clean-up stage.

Attacker's Goals

Remove evidence for mailbox export commands.

Investigative actions

- Examine the PowerShell command to identify which mailbox has been compromised. Investigate the host that executes the command for potential further exploitation.

31.21 | A user connected a USB storage device for the first time

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: ▯ XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Collection (TA0009) Exfiltration (TA0010)
ATT&CK Technique	׀ Data Staged (T1074) Exfiltration Over Physical Medium: Exfiltration over USB (T1052.001)
Severity	Informational

Description

A user connected a USB storage device for the first time in the past 30 days.

Attacker's Goals

The attacker may use a USB storage device connection for data exfiltration or data collection.

Investigative actions

Investigate the USB storage device related process and file events to determine if it was used for legitimate purposes or malicious activity.

31.22 | Uncommon NtWriteVirtualMemoryRemote API invocation with a PE header buffer

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	Injection Analytics
ATT&CK Tactic	- Defense Evasion (TA0005) - Privilege Escalation (TA0004)

ATT&CK Technique	Process Injection: Portable Executable Injection (T1055.002)
Severity	Low

Description

A process wrote a PE header to another process by calling the NtWriteVirtualMemoryRemote API function.

Attacker's Goals

Gain code execution on the host in the context of another process.

Investigative actions

- Investigate the acting process for other malicious activities.
- Check if the target process was injected and for anomalies in its behavior after this event.

Variations

Uncommon NtWriteVirtualMemoryRemote API invocation with a PE header buffer from an office process

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005) Privilege Escalation (TA0004)
ATT&CK Technique	Process Injection: Portable Executable Injection (T1055.002)
Severity	High

Description

An office process wrote a PE header to another process by calling the NtWriteVirtualMemoryRemote API function.

Attacker's Goals

Gain code execution on the host in the context of another process.

Investigative actions

- Investigate the acting process for other malicious activities.
Check if the target process was injected and for anomalies in its behavior after this event.

Uncommon NtWriteVirtualMemoryRemote API invocation with a PE header buffer from an injected thread

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005) Privilege Escalation (TA0004)
ATT&CK Technique	Process Injection: Portable Executable Injection (T1055.002)
Severity	Medium

Description

An injected thread wrote a PE header to another process by calling the NtWriteVirtualMemoryRemote API function.

Attacker's Goals

Gain code execution on the host in the context of another process.

Investigative actions

Investigate the acting process for other malicious activities.
- Check if the target process was injected and for anomalies in its behavior after this event.

Uncommon NtWriteVirtualMemoryRemote API invocation with a PE header buffer from a LOLBIN process

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005) Privilege Escalation (TA0004)
ATT&CK Technique	Process Injection: Portable Executable Injection (T1055.002)
Severity	Medium

Description

A LOLBIN process wrote a PE header to another process by calling the NtWriteVirtualMemoryRemote API function.

Attacker's Goals

Gain code execution on the host in the context of another process.

Investigative actions

- Investigate the acting process for other malicious activities.
- Check if the target process was injected and for anomalies in its behavior after this event.

Uncommon NtWriteVirtualMemoryRemote API invocation with a PE header buffer from an unsigned process

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005) Privilege Escalation (TA0004)
ATT&CK Technique	Process Injection: Portable Executable Injection (T1055.002)
Severity	Medium

Description

An unsigned process wrote a PE header to another process by calling the NtWriteVirtualMemoryRemote API function.

Attacker's Goals

Gain code execution on the host in the context of another process.

Investigative actions

Investigate the acting process for other malicious activities.

Check if the target process was injected and for anomalies in its behavior after this event.

31.23 | Uncommon AT task-job creation by user

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: ▯ XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)

ATT&CK Technique	Scheduled Task/Job: At (T1053.002)
Severity	Low

Description

An unpopular AT task-job was created by a user.

Attacker's Goals

Attackers may use at task-jobs for persistence or executing malicious files.

Investigative actions

Check the AT job task for suspicious activity.

Variations

Uncommon AT task-job creation by user from a web server process

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Scheduled Task/Job: At (T1053.002)
Severity	Medium

Description

A web process used the AT command to create a new AT task-job.

Attacker's Goals

Attackers may use at task-jobs for persistence or executing malicious files.

Investigative actions

Check the AT job task for suspicious activity.

Uncommon AT task-job creation by user from unpopular process

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Scheduled Task/Job: At (T1053.002)
Severity	Low

Description

An unpopular process created an AT task-job on the host, which is not popular in the organization.

Attacker's Goals

Attackers may use at task-jobs for persistence or executing malicious files.

Investigative actions

Check the AT job task for suspicious activity.

31.24 | DSC (Desired State Configuration) lateral movement using PowerShell

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	N/A (single event)
Deduplication Period	1 Hour
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	- Lateral Movement (TA0008) - Execution (TA0002)
ATT&CK Technique	Windows Management Instrumentation (T1047) - Remote Services: Windows Remote Management (T1021.006)
Severity	Informational

Description

An attacker is using the DSC feature with PowerShell to remotely modify / execute content / components on the machine.

Attacker's Goals

Execute malicious content on and move laterally across machine in the network.

Investigative actions

Search for suspicious WinRM sessions and the user created them, can be found at Event ID: 4102.

- Additionally, search for the DSC resource executed and related IOC, can be found at Event IDs: 400 or 4104.

Variations

DSC (Desired State Configuration) lateral movement using PowerShell to execute a script

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008) Execution (TA0002)
ATT&CK Technique	Windows Management Instrumentation (T1047) Remote Services: Windows Remote Management (T1021.006)
Severity	High

Description

An attacker may use the DSC feature with PowerShell to execute script remotely on a machine.

Attacker's Goals

Execute malicious content on and move laterally across machine in the network.

Investigative actions

Search for suspicious WinRM sessions and the user created them, can be found at Event ID: 4102.

- Additionally, search for the DSC resource executed and related IOC, can be found at Event IDs: 400 or 4104.
  The executed script is logged under Event ID 4104.

DSC (Desired State Configuration) lateral movement using PowerShell to execute a new service

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008) Execution (TA0002)

ATT&CK Technique	- Windows Management Instrumentation (T1047) - Remote Services: Windows Remote Management (T1021.006)
Severity	Medium

Description

An attacker may use the DSC feature with PowerShell to create and execute a service on the host.

Attacker's Goals

Execute malicious content on and move laterally across machine in the network.

Investigative actions

- Search for suspicious WinRM sessions and the user created them, can be found at Event ID: 4102.
  Additionally, search for the DSC resource executed and related IOC, can be found at Event IDs: 400 or 4104.

DSC (Desired State Configuration) lateral movement using PowerShell to modify the registry

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008) - Execution (TA0002)
ATT&CK Technique	Windows Management Instrumentation (T1047) - Remote Services: Windows Remote Management (T1021.006)
Severity	Medium

Description

An attacker may use the DSC feature with PowerShell to create/modify/dump registry keys/values.

Attacker's Goals

Execute malicious content on and move laterally across machine in the network.

Investigative actions

- Search for suspicious WinRM sessions and the user created them, can be found at Event ID: 4102.
  Additionally, search for the DSC resource executed and related IOC, can be found at Event IDs: 400 or 4104.

31.25 | Suspicious process modified RC script file

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	Kubernetes - AGENT, Containers
ATT&CK Tactic	Persistence (TA0003) Privilege Escalation (TA0004)
ATT&CK Technique	Boot or Logon Initialization Scripts: RC Scripts (T1037.004)

Severity	Low

Description

A suspicious process modified an RC script file.
These files allow system administrators to map and start custom services at startup for different run levels.
This may be done to establish persistence.

Attacker's Goals

Adversaries may establish persistence by modifying RC scripts, which are executed during a Unix-like system's startup.

Investigative actions

Check the modified RC script file and try to understand the impact of the file modification.

Variations

Suspicious process modified RC script file in a Kubernetes pod

Synopsis

ATT&CK Tactic	Persistence (TA0003) Privilege Escalation (TA0004)
ATT&CK Technique	Boot or Logon Initialization Scripts: RC Scripts (T1037.004)
Severity	Low

Description

A suspicious process modified an RC script file.
These files allow system administrators to map and start custom services at startup for different run levels.
This may be done to establish persistence.

Attacker's Goals

Adversaries may establish persistence by modifying RC scripts, which are executed during a Unix-like system's startup.

Investigative actions

Check the modified RC script file and try to understand the impact of the file modification.

31.26 | Unusual process accessed a macOS notes DB file

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	Sensitive Information Stealing Analytics
ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Data from Information Repositories (T1213)

Severity	Informational

Description

An unusual process has accessed a user's notes DB file.

Attacker's Goals

Obtain access to user's notes and steal their contents.

Investigative actions

- Determine whether it is legitimate for the process to access user's notes.
- Analyze the process/application that accessed the DB file.
- Check for any other suspicious actions that were performed by the process.
- Look for unusual access of resources using credentials that may be stored in the above notes.

Variations

Unusual unsigned process accessed a macOS notes DB file

Synopsis

ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Data from Information Repositories (T1213)
Severity	Low

Description

An unusual process has accessed a user's notes DB file.

Attacker's Goals

Obtain access to user's notes and steal their contents.

Investigative actions

- Determine whether it is legitimate for the process to access user's notes.
- Analyze the process/application that accessed the DB file.
  Check for any other suspicious actions that were performed by the process.
  Look for unusual access of resources using credentials that may be stored in the above notes.

31.27 | VM Detection attempt

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005) Discovery (TA0007)

ATT&CK Technique	Virtualization/Sandbox Evasion: System Checks (T1497.001)
Severity	Informational

Description

A script has executed commands that can be used to detect VM environments.

Attacker's Goals

Avoid malware analysis by identifying execution from within sandboxes and virtual machines.

Investigative actions

Review the script for additional malicious actions.

Check for any additional alerts raised within the same context of the script.

31.28 | A user added a Windows firewall rule

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)

Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Impair Defenses: Disable or Modify System Firewall (T1562.004)
Severity	Informational

Description

A user added a new Windows Firewall rule. Adding a firewall rule may indicate an attempt to bypass controls limiting network usage or to disrupt network communications.

Attacker's Goals

Firewall rules determine what traffic your firewall will block or allow. A malicious insider might want to change these rules in an attempt to bypass network limitations or disrupt network communication.

Investigative actions

Check for any other suspicious activity related to the host and the user involved in the alert.
Check Windows Defender Firewall with Advanced Security for a new rule that was added.

Check if the new rule was added to different machines as well.

31.29 | Office process accessed an unusual .LNK file

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	7 Days
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Execution (TA0002) Persistence (TA0003)
ATT&CK Technique	User Execution (T1204) Boot or Logon Autostart Execution: Shortcut Modification (T1547.009)
Severity	Low

Description

An attacker may embed a .LNK file in an Office document to execute malicious code.

Attacker's Goals

Modify or create a shortcut to gain code or program execution.

Investigative actions

Check if the Office document contains a shortcut object.

- Check the content (strings) of the document object for a .LNK shortcut.
- Check the content of the shortcut.

31.30 | Executable created to disk by lsass.exe

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	6 Hours
Required Data	- Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Process Injection (T1055)
Severity	Medium

Description

Lsass.exe does not normally create executables to disk. This activity was seen as part of several exploits, like EternalBlue and DoublePulsar, used during the WannaCry attacks.

Attacker's Goals

This activity was an important stage for several exploits.

Investigative actions

Check the file that was written to the disk for malicious activities.

31.31 | Unusual process accessed a messaging app's files

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	▮ Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	Sensitive Information Stealing Analytics

ATT&CK Tactic	- Collection (TA0009) - Reconnaissance (TA0043)
ATT&CK Technique	- Data from Local System (T1005) - Gather Victim Host Information (T1592)
Severity	Low

Description

An unusual process has accessed files belonging to a messaging app.

Attacker's Goals

Obtain access to the user's message history and steal their contents.

Investigative actions

Determine whether it is legitimate for the process to access such files.
Analyze the process/application that accessed the file.

- Check for any other suspicious actions that were performed by the process.
- Look for unusual access of resources using credentials that may have been associated with the above messaging app.

31.32 | An uncommon file added to startup-related Registry keys

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)

Deduplication Period	1 Day
Required Data	Requires: ▯ XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Boot or Logon Autostart Execution (T1547)
Severity	Informational

Description

An attacker may add a file to the Registry "Run Keys" or the "Winlogon\Userinit" key to cause it to be executed as the user logs in.

Attacker's Goals

Gain persistence using the legitimate Windows registry run key mechanism, which executes files or scripts on user login or computer boot.

Investigative actions

Verify if the registered file is malicious.
- Check if the installing software is a malicious binary or script.

Variations

An uncommon file added to startup-related Registry keys by an unsigned and unpopular CGO process

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Boot or Logon Autostart Execution (T1547)
Severity	Low

Description

An attacker may add a file to the Registry "Run Keys" or the "Winlogon\Userinit" key to cause it to be executed as the user logs in.

Attacker's Goals

Gain persistence using the legitimate Windows registry run key mechanism, which executes files or scripts on user login or computer boot.

Investigative actions

Verify if the registered file is malicious.

Check if the installing software is a malicious binary or script.

An uncommon script added to startup-related Registry keys

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Boot or Logon Autostart Execution (T1547)
Severity	Low

Description

An attacker may add a script to the Registry "Run Keys" or the "Winlogon\Userinit" key to cause it to be executed as the user logs in.

Attacker's Goals

Gain persistence using the legitimate Windows registry run key mechanism, which executes files or scripts on user login or computer boot.

Investigative actions

Verify if the registered file is malicious.
Check if the installing software is a malicious binary or script.

An uncommon file added to startup-related Registry keys by a commonly known and signed application

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Boot or Logon Autostart Execution (T1547)
Severity	Low

Description

An attacker may add a file to the Registry "Run Keys" or the "Winlogon\Userinit" key to cause it to be executed as the user logs in.

Attacker's Goals

Gain persistence using the legitimate Windows registry run key mechanism, which executes files or scripts on user login or computer boot.

Investigative actions

- Verify if the registered file is malicious.
- Check if the installing software is a malicious binary or script.

An uncommon LOLBIN added to startup-related Registry keys

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Boot or Logon Autostart Execution (T1547)
Severity	Low

Description

An attacker may add a LOLBIN to the Registry "Run Keys" or the "Winlogon\Userinit" key to cause it to be executed as the user logs in.

Attacker's Goals

Gain persistence using the legitimate Windows registry run key mechanism, which executes files or scripts on user login or computer boot.

Investigative actions

Verify if the registered file is malicious.

Check if the installing software is a malicious binary or script.

An uncommon file added to startup-related Registry keys by a remote actor

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Boot or Logon Autostart Execution (T1547)
Severity	Low

Description

A remote attacker may add a file to the Registry "Run Keys" or the "Winlogon\Userinit" key to cause it to be executed as the user logs in.

Attacker's Goals

Gain persistence using the legitimate Windows registry run key mechanism, which executes files or scripts on user login or computer boot.

Investigative actions

Verify if the registered file is malicious.
Check if the installing software is a malicious binary or script.

31.33 | Possible webshell file written by a web server process

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Initial Access (TA0001) Persistence (TA0003)

ATT&CK Technique	- External Remote Services (T1133) - Server Software Component: Web Shell (T1505.003)
Severity	Informational

Description

An uncommon file with a web file extension was created, written or renamed by a web server process.

Attacker's Goals

Gaining the ability to execute commands on the host, as well as persistence.

Investigative actions

- Investigate the web server access logs for suspicious behavior.
- Check if the dropped file contains malicious content.

Variations

Possible webshell file written by a node web server process

Synopsis

ATT&CK Tactic	- Initial Access (TA0001) - Persistence (TA0003)
ATT&CK Technique	- External Remote Services (T1133) - Server Software Component: Web Shell (T1505.003)
Severity	Informational

Description

An uncommon file with a web file extension was created, written or renamed by a web server process.

Attacker's Goals

Gaining the ability to execute commands on the host, as well as persistence.

Investigative actions

- Investigate the web server access logs for suspicious behavior.
  Check if the dropped file contains malicious content.

Possible webshell file written by a web server process in an internet facing server

Synopsis

ATT&CK Tactic	Initial Access (TA0001) Persistence (TA0003)
ATT&CK Technique	External Remote Services (T1133) Server Software Component: Web Shell (T1505.003)
Severity	Low

Description

An uncommon file with a web file extension was created, written or renamed by a web server process.

Attacker's Goals

Gaining the ability to execute commands on the host, as well as persistence.

Investigative actions

Investigate the web server access logs for suspicious behavior.

- Check if the dropped file contains malicious content.

Possible webshell file written by a web server process with connections from various sources and high web traffic

Synopsis

ATT&CK Tactic	Initial Access (TA0001) Persistence (TA0003)
ATT&CK Technique	External Remote Services (T1133) Server Software Component: Web Shell (T1505.003)
Severity	Low

Description

An uncommon file with a web file extension was created, written or renamed by a web server process.

Attacker's Goals

Gaining the ability to execute commands on the host, as well as persistence.

Investigative actions

- Investigate the web server access logs for suspicious behavior.
- Check if the dropped file contains malicious content.

31.34 | Suspicious AMSI decode attempt

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)

Deduplication Period	1 Minute
Required Data	Requires: • XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Deobfuscate/Decode Files or Information (T1140)
Severity	Informational

Description

A script has executed commands that can be used to decode commands or files.

Attacker's Goals

Avoid security mitigations and detections.

Investigative actions

Check the payload for malicious activity.

31.35 | Windows event logs were cleared with PowerShell

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	- Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Indicator Removal: Clear Windows Event Logs (T1070.001)
Severity	Low

Description

Windows event logs were cleared or deleted with PowerShell.

Attacker's Goals

Attackers may clear events from Windows event logs to remove traces of their malicious activity.

Investigative actions

- Validate if the script that was executed is from a legitimate IT activity.
- Look for additional suspicious actions that were executed on the host.

Variations

Suspicious clear or delete security provider event logs with PowerShell

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Indicator Removal: Clear Windows Event Logs (T1070.001)
Severity	High

Description

Windows event logs were cleared or deleted with PowerShell.

Attacker's Goals

Attackers may clear events from Windows event logs to remove traces of their malicious activity.

Investigative actions

- Validate if the script that was executed is from a legitimate IT activity.
  Look for additional suspicious actions that were executed on the host.

Suspicious clear or delete default providers event logs with PowerShell

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Indicator Removal: Clear Windows Event Logs (T1070.001)
Severity	Medium

Description

Windows event logs were cleared or deleted with PowerShell.

Attacker's Goals

Attackers may clear events from Windows event logs to remove traces of their malicious activity.

Investigative actions

Validate if the script that was executed is from a legitimate IT activity.
Look for additional suspicious actions that were executed on the host.

31.36 | Scheduled Task hidden by registry modification

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)

ATT&CK Technique	- Modify Registry (T1112) - Hide Artifacts (T1564)
Severity	Low

Description

Attackers may try to hide a Scheduled Task by deleting the Scheduled Task's software descriptor (SD) value in the registry.

Attacker's Goals

Adversaries may hide their malicious Scheduled Task to evade detection.

Investigative actions

- Check the appropriate Scheduled Task to verify its legitimacy.
- You can also check the executing executable to verify its purpose.

31.37 | An unpopular process accessed the microphone on the host

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	7 Days

Required Data	- Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	- Audio Capture (T1123) Video Capture (T1125)
Severity	Low

Description

An unpopular process accessed the microphone on the host, the process can abuse this device.

Attacker's Goals

Surround recording or video capture in the workplace may leak corporate data.

- Surround recording or video capture of the user space can expose them to potential risks as worker extortion, sextortion, etc.

Investigative actions

- Check if the application that registered in the Microsoft privacy settings (ConsentStore in registry) is legitimate.
  Check if the user was aware of the use of the device.

Variations

An unpopular process accessed the webcam on the host

Synopsis

ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Audio Capture (T1123) Video Capture (T1125)
Severity	Low

Description

An unpopular process accessed the webcam on the host, the process can abuse this device.

Attacker's Goals

- Surround recording or video capture in the workplace may leak corporate data.
- Surround recording or video capture of the user space can expose them to potential risks as worker extortion, sextortion, etc.

Investigative actions

- Check if the application that registered in the Microsoft privacy settings (ConsentStore in registry) is legitimate.
- Check if the user was aware of the use of the device.

31.38 | A user queried AD CS objects via LDAP

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)

Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	LDAP Analytics (Server)
ATT&CK Tactic	- Discovery (TA0007) Credential Access (TA0006)
ATT&CK Technique	- File and Directory Discovery (T1083) Steal or Forge Authentication Certificates (T1649)
Severity	Informational

Description

A user queried AD CS objects via LDAP.

Attacker's Goals

An attacker might look for AD CS servers, certificate templates or request certificates.

With the wrong setting or loose vulnerable templates or enabled enrollment, the attacker will be able to authenticate as users on the network.

Investigative actions

- Check if the LDAP search query was allowed for the user (logged on at event time).
  Investigate the LDAP search query for any suspicious indicators.

Variations

A user enumerated AD CS objects using suspicious LDAP query

Synopsis

ATT&CK Tactic	Discovery (TA0007) Credential Access (TA0006)
ATT&CK Technique	File and Directory Discovery (T1083) Steal or Forge Authentication Certificates (T1649)
Severity	Low

Description

A user enumerated AD CS objects using suspicious LDAP query.

Attacker's Goals

An attacker might look for AD CS servers, certificate templates or request certificates.
With the wrong setting or loose vulnerable templates or enabled enrollment, the attacker will be able to authenticate as users on the network.

Investigative actions

- Check if the LDAP search query was allowed for the user (logged on at event time).
- Investigate the LDAP search query for any suspicious indicators.

31.39 | Known service display name with uncommon image-path

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)

Deduplication Period	1 Day
Required Data	- Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	Malicious Service Analytics
ATT&CK Tactic	Persistence (TA0003) Execution (TA0002)
ATT&CK Technique	Create or Modify System Process: Windows Service (T1543.003) System Services: Service Execution (T1569.002)
Severity	Low

Description

Service created with a known display name but has an uncommon image-path.

Attacker's Goals

Run malicious code with seemingly trustworthy services.

Investigative actions

- Investigate the image-path of the newly created service.
  Investigate the causality actor process - which initiated the activity.

Variations

Known service display name with uncommon image-path created by an untrusted CGO

Synopsis

ATT&CK Tactic	Persistence (TA0003) Execution (TA0002)
ATT&CK Technique	Create or Modify System Process: Windows Service (T1543.003) System Services: Service Execution (T1569.002)
Severity	Medium

Description

Service created with a known display name but has an uncommon image-path.

Attacker's Goals

Run malicious code with seemingly trustworthy services.

Investigative actions

- Investigate the image-path of the newly created service.
- Investigate the causality actor process - which initiated the activity.

Known Palo Alto service display name with uncommon image-path

Synopsis

ATT&CK Tactic	Persistence (TA0003) Execution (TA0002)
ATT&CK Technique	Create or Modify System Process: Windows Service (T1543.003) System Services: Service Execution (T1569.002)
Severity	Medium

Description

Service created with a known display name but has an uncommon image-path.

Attacker's Goals

Run malicious code with seemingly trustworthy services.

Investigative actions

- Investigate the image-path of the newly created service.
- Investigate the causality actor process - which initiated the activity.

Known service display name with uncommon image-path in a suspicious folder

Synopsis

ATT&CK Tactic	Persistence (TA0003) Execution (TA0002)
ATT&CK Technique	Create or Modify System Process: Windows Service (T1543.003) System Services: Service Execution (T1569.002)
Severity	Medium

Description

Service created with a known display name but has an uncommon image-path.

Attacker's Goals

Run malicious code with seemingly trustworthy services.

Investigative actions

- Investigate the image-path of the newly created service.
- Investigate the causality actor process - which initiated the activity.

31.40 | Unusual user account unlock

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

A user unlocked an account. This user does not usually unlock user accounts.

Attacker's Goals

An attacker may unlock a user account to gain unauthorized access.

Investigative actions

- Investigate the associated authentication attempts and login failures (e.g. 4625, 4776 events).
  Check if the user is authorized to unlock accounts.
  Confirm that the user unlock was expected.

  Monitor services that may be running with a user's credentials, resulting in lockouts.

Variations

Unusual sensitive user account unlock

Synopsis

ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Low

Description

A user unlocked a sensitive account. This user does not usually unlock user accounts.

Attacker's Goals

An attacker may unlock a user account to gain unauthorized access.

Investigative actions

- Investigate the associated authentication attempts and login failures (e.g. 4625, 4776 events).
  Check if the user is authorized to unlock accounts.

  Confirm that the user unlock was expected.
- Monitor services that may be running with a user's credentials, resulting in lockouts.

31.41 | User account delegation change

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation (T1098)
Severity	Informational

Description

A user account was modified with delegation to a service.

Attacker's Goals

An attacker may attempt to control an Active Directory environment.

Investigative actions

- Verify this action with the user who performed the change.
- Check if the account modified is a service account.
  Follow actions by the user, including TGT and TGS requests.
  Monitor for anomalous Kerberos activity.

Variations

User account delegation to KRBTGT

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Steal or Forge Kerberos Tickets (T1558)
Severity	High

Description

A user account was modified with delegation to the KRBTGT service.

Attacker's Goals

An attacker may attempt to control an Active Directory environment.

Investigative actions

- Verify this action with the user who performed the change.
- Check if the account modified is a service account.
  Follow actions by the user, including TGT and TGS requests.
  Monitor for anomalous Kerberos activity.

User account delegation to a DC

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation (T1098)
Severity	Low

Description

A user account was modified with delegation to a service on a domain controller.

Attacker's Goals

An attacker may attempt to control an Active Directory environment.

Investigative actions

- Verify this action with the user who performed the change.
  Check if the account modified is a service account.
  Follow actions by the user, including TGT and TGS requests.

  Monitor for anomalous Kerberos activity.

31.42 | Creation or modification of the default command executed when opening an application

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)

Deduplication Period	1 Day
Required Data	- Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Abuse Elevation Control Mechanism: Bypass User Account Control (T1548.002)
Severity	Informational

Description

Creation or modification of these registry keys can cause the execution of the specified programs, bypassing UAC.

Attacker's Goals

Gain higher privileges by bypassing the User Account Control (UAC).

Investigative actions

- Check the registry data modified for a potentially malicious command line.
- Look for processes running matching the command line for malicious activity.

Variations

Creation or modification of the default command executed when opening the Microsoft optional features settings (Fodhelper.exe)

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Abuse Elevation Control Mechanism: Bypass User Account Control (T1548.002)
Severity	Medium

Description

Creation or modification of these registry keys can cause the execution of the specified programs, bypassing UAC.

Attacker's Goals

Gain higher privileges by bypassing the User Account Control (UAC).

Investigative actions

Check the registry data modified for a potentially malicious command line.

Look for processes running matching the command line for malicious activity.

Creation or modification of the default command executed when opening an MMC application

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Abuse Elevation Control Mechanism: Bypass User Account Control (T1548.002)
Severity	Medium

Description

Creation or modification of these registry keys can cause the execution of the specified programs, bypassing UAC.

Attacker's Goals

Gain higher privileges by bypassing the User Account Control (UAC).

Investigative actions

Check the registry data modified for a potentially malicious command line.

Look for processes running matching the command line for malicious activity.

Creation or modification of the default command executed when opening Windows backup and restore (sdclt.exe)

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Abuse Elevation Control Mechanism: Bypass User Account Control (T1548.002)
Severity	Medium

Description

Creation or modification of these registry keys can cause the execution of the specified programs, bypassing UAC.

Attacker's Goals

Gain higher privileges by bypassing the User Account Control (UAC).

Investigative actions

- Check the registry data modified for a potentially malicious command line.
  Look for processes running matching the command line for malicious activity.

Creation or modification of the default command executed when opening Windows Store settings (Wsreset.exe)

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Abuse Elevation Control Mechanism: Bypass User Account Control (T1548.002)
Severity	Medium

Description

Creation or modification of these registry keys can cause the execution of the specified programs, bypassing UAC.

Attacker's Goals

Gain higher privileges by bypassing the User Account Control (UAC).

Investigative actions

Check the registry data modified for a potentially malicious command line.

Look for processes running matching the command line for malicious activity.

31.43 | New process created via a WMI call

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)

Deduplication Period	1 Day
Required Data	Requires: XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Windows Management Instrumentation (T1047)
Severity	Informational

Description

A new process created via a WMI call.

Attacker's Goals

Create a new process on the host.

Investigative actions

Check whether the process that created via the WMI call is benign, and if this was a desired behavior as part of its normal execution flow.

31.44 | Uncommon GetClipboardData API function invocation of

a possible information stealer

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Clipboard Data (T1115)
Severity	Informational

Description

An unpopular process accessed clipboard content by calling the GetClipboardData API function. This behavior may indicate potential threats such as a keylogger or a RAT.

Attacker's Goals

Attackers can monitor the clipboard as another way for credential gathering or to collect more user data over time for espionage purposes.

Investigative actions

- Check if the process has a user interface (a visible window).
Check if the process is a known user application that was updated recently.

31.45 | Browser bookmark files accessed by a rare non-browser process

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: ▯ XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Discovery (TA0007)

ATT&CK Technique	Browser Information Discovery (T1217)
Severity	Informational

Description

Browser bookmark files accessed by a rare non-browser process.

Attacker's Goals

Accessing these files is done by attackers to collect information about the endpoint.

Investigative actions

Investigate the actor process to determine if it was used for legitimate purposes or malicious activity.

31.46 | An uncommon executable was remotely written over SMB to an uncommon destination

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	▮ Requires: - XDR Agent with eXtended Threat Hunting (XTH)

Detection Modules	
Detector Tags	
ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Services: SMB/Windows Admin Shares (T1021.002)
Severity	Low

Description

An uncommon executable was remotely written over SMB to a destination which was not involved in significant similar activity during last month.

Attacker's Goals

Transfer tools as part of lateral movement activity across the network.

Investigative actions

- Verify if the shared file is malicious.
- Investigate if the file was executed on the host.
  Check the remote SMB client for other suspicious activities.

Variations

An uncommon executable was remotely written over SMB to a highly suspicious destination

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Services: SMB/Windows Admin Shares (T1021.002)

Severity	High

Description

An uncommon executable was remotely written over SMB to a highly suspicious destination which was not involved in significant similar activity during last month.

Attacker's Goals

Transfer tools as part of lateral movement activity across the network.

Investigative actions

Verify if the shared file is malicious.
Investigate if the file was executed on the host.

Check the remote SMB client for other suspicious activities.

An uncommon executable with SCR extension was remotely written over SMB to an uncommon destination

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Services: SMB/Windows Admin Shares (T1021.002)
Severity	Medium

Description

An uncommon executable with SCR extension was remotely written over SMB to a destination which was not involved in significant similar activity during last month.

Attacker's Goals

Transfer tools as part of lateral movement activity across the network, leveraging lesser known PE extension to masquerade a malicious file.

Investigative actions

Verify if the shared file is malicious.

- Investigate if the file was executed on the host.
- Check the remote SMB client for other suspicious activities.

Verify whether or not the executable file is a genuine screensaver, possibly by detonating it in a controlled environment.

PsExec remote service component was remotely written over SMB to an uncommon destination

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Services: SMB/Windows Admin Shares (T1021.002)
Severity	Low

Description

PsExec remote service component was remotely written over SMB to a destination which was not involved in significant similar activity during last month.

Attacker's Goals

Transfer tools as part of lateral movement activity across the network.

Investigative actions

Verify if the shared file is malicious.
Investigate if the file was executed on the host.

Check the remote SMB client for other suspicious activities.

- Verify whether this is part of authorized activity or not as PsExec can be used for both benign and malicious purposes.

31.47 | Administrator groups enumerated via LDAP

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	LDAP Analytics (Client)
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Account Discovery (T1087)
Severity	Informational

Description

An LDAP search query that collects information about administrators was executed. This may be indicative of Active Directory domain enumeration, which can be used to perform attacks against the organization.

Attacker's Goals

An attacker is attempting to enumerate Active Directory.

Investigative actions

- Check if the process executes LDAP search queries as part of its normal behavior.
- Investigate the LDAP search query for any suspicious indicators.

31.48 | Suspicious access to shadow file

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	7 Days
Required Data	- Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	Kubernetes - AGENT, Containers
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	OS Credential Dumping (T1003)

Severity	Informational

Description

An unpopular process accessed the shadow file.

Attacker's Goals

Attackers may attempt to dump the contents of these sensitive files to perform offline password cracking.

Investigative actions

- Check the process for more suspicious activity.
- Check whether this was a legitimate action.

Variations

Suspicious access to shadow file in a Kubernetes Pod using a known text editor

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	OS Credential Dumping (T1003)
Severity	Medium

Description

An unpopular process accessed the shadow file in a Kubernetes Pod.

Attacker's Goals

Attackers may attempt to dump the contents of these sensitive files to perform offline password cracking.

Investigative actions

Check the process for more suspicious activity.

- Check whether this was a legitimate action.

Suspicious access to shadow file using a known text editor

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	OS Credential Dumping (T1003)
Severity	Medium

Description

An unpopular process accessed the shadow file.

Attacker's Goals

Attackers may attempt to dump the contents of these sensitive files to perform offline password cracking.

Investigative actions

Check the process for more suspicious activity.

- Check whether this was a legitimate action.

Suspicious access to shadow file in a Kubernetes Pod

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	OS Credential Dumping (T1003)
Severity	Low

Description

An unpopular process accessed the shadow file.

Attacker's Goals

Attackers may attempt to dump the contents of these sensitive files to perform offline password cracking.

Investigative actions

Check the process for more suspicious activity.

Check whether this was a legitimate action.

Suspicious access to shadow file

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	OS Credential Dumping (T1003)
Severity	Low

Description

An unpopular process accessed the shadow file.

Attacker's Goals

Attackers may attempt to dump the contents of these sensitive files to perform offline password cracking.

Investigative actions

Check the process for more suspicious activity.

Check whether this was a legitimate action.

31.49 | Suspicious active setup registered

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Boot or Logon Autostart Execution: Active Setup (T1547.014)
Severity	Informational

Description

The endpoint registered a new active setup, which may be used to gain persistence on the host by loading libraries into the time management service.

Attacker's Goals

Gain persistence using the legitimate windows active setup mechanism, which executes binary on system startup.

Investigative actions

- Verify if the registered binary is malicious.
  Check if the installing software is a malicious binary.

31.50 | Access to Kubernetes configuration file

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	- Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	Kubernetes - AGENT
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials: Credentials In Files (T1552.001)

Severity	Informational

Description

A process accessed a Kubernetes node configuration file.

Attacker's Goals

Gain access to the Kubernetes environment.

Investigative actions

- Look for additional suspicious activities.
- Verify if the exposed credentials were used to access the API server.
- Investigate which operations were used against the Kubernetes cluster with the exposed credentials.

Variations

Access to Kubernetes configuration file by an unusual process

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials: Credentials In Files (T1552.001)
Severity	Low

Description

A process accessed a Kubernetes node configuration file.

Attacker's Goals

Gain access to the Kubernetes environment.

Investigative actions

Look for additional suspicious activities.
- Verify if the exposed credentials were used to access the API server.
- Investigate which operations were used against the Kubernetes cluster with the exposed credentials.

Access to Kubernetes configuration file from an unusual Kubernetes pod

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials: Credentials In Files (T1552.001)
Severity	Low

Description

A process accessed a Kubernetes node configuration file.

Attacker's Goals

Gain access to the Kubernetes environment.

Investigative actions

- Look for additional suspicious activities.
- Verify if the exposed credentials were used to access the API server.

Investigate which operations were used against the Kubernetes cluster with the exposed credentials.

Access to Kubernetes configuration file from a Kubernetes pod

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials: Credentials In Files (T1552.001)

Severity	Informational

Description

A process accessed a Kubernetes node configuration file.

Attacker's Goals

Gain access to the Kubernetes environment.

Investigative actions

- Look for additional suspicious activities.
  Verify if the exposed credentials were used to access the API server.
  Investigate which operations were used against the Kubernetes cluster with the exposed credentials.

31.51 | Rare machine account creation

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)

Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Create Account (T1136)
Severity	Informational

Description

A user was observed creating a machine account for the first time.

Attacker's Goals

Persistence using a valid account.

Investigative actions

- Verify the activity of the user who created the account.
- Follow actions performed by the new machine account.

31.52 | LSASS dump file written to disk

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)

Deduplication Period	1 Day
Required Data	Requires: • XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	OS Credential Dumping (T1003)
Severity	Medium

Description

Dumping Lsass.exe (Local Security Authority Subsystem Service) memory to file allows attackers to later extract credentials from the memory dump.

Attacker's Goals

Attackers may try to extract OS credentials from the dumped Lsass.exe file.

Investigative actions

Check the dumping process for more suspicious activity.

31.53 | A machine certificate was issued with a mismatch

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Windows Event Collector OR ▯ XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Valid Accounts: Domain Accounts (T1078.002)
Severity	Medium

Description

A machine certificate was issued with a mismatch between the requester and the subject.

Attacker's Goals

An attacker may attempt to exploit the Active Directory Certificate Services to escalate privileges to a domain controller machine account.

Investigative actions

- Check who owns the certificate requester account.
- Check if the requester DNS name attribute was changed recently.
- Investigate actions done by the requester, and its owner.
- Check for possible DCSync alerts.

31.54 | NTDS.dit file written by an uncommon executable

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)

ATT&CK Technique	- OS Credential Dumping (T1003) - OS Credential Dumping: NTDS (T1003.003)
Severity	Low

Description

The Active Directory database file was written by an uncommon process to a non-default location.

Attacker's Goals

Dump the sensitive contents of the database to masquerade as legitimate domain users.

Investigative actions

- Investigate the nature of the process writing the sensitive file - is it a standard backup procedure?
- Check the path the file was written to - is it local? Are there other relevant artifacts in this location?

Variations

NTDS.dit file written by a rare executable

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	- OS Credential Dumping (T1003) - OS Credential Dumping: NTDS (T1003.003)
Severity	Medium

Description

The Active Directory database file was written by a rare process to a non-default location.

Attacker's Goals

Dump the sensitive contents of the database to masquerade as legitimate domain users.

Investigative actions

- Investigate the nature of the process writing the sensitive file - is it a standard backup procedure?

  Check the path the file was written to - is it local? Are there other relevant artifacts in this location?

31.55 | Unusual Kubernetes service account file read

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	7 Days
Required Data	Requires: ▯ XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	Kubernetes - AGENT
ATT&CK Tactic	Credential Access (TA0006)

ATT&CK Technique	Unsecured Credentials: Credentials In Files (T1552.001)
Severity	Informational

Description

An unusual process opened a Kubernetes service account file for the first time.

Attacker's Goals

Utilize the Kubernetes service account files to perform additional actions on the cluster.

Investigative actions

Check the exposed Kubernetes service account usage in the cluster.

Check if any other suspicious activity was performed inside the pod.

Variations

Unusual Kubernetes service account file read within a new pod

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials: Credentials In Files (T1552.001)
Severity	Informational

Description

An unusual process opened a Kubernetes service account file for the first time.

Attacker's Goals

Utilize the Kubernetes service account files to perform additional actions on the cluster.

Investigative actions

- Check the exposed Kubernetes service account usage in the cluster.
- Check if any other suspicious activity was performed inside the pod.

Kubernetes service account file read

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials: Credentials In Files (T1552.001)
Severity	Informational

Description

An unusual process opened a Kubernetes service account file for the first time.

Attacker's Goals

Utilize the Kubernetes service account files to perform additional actions on the cluster.

Investigative actions

- Check the exposed Kubernetes service account usage in the cluster.
- Check if any other suspicious activity was performed inside the pod.

Suspicious Kubernetes service account file read from the projected volume path

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials: Credentials In Files (T1552.001)
Severity	Medium

Description

An unusual process opened a Kubernetes service account file for the first time.

Attacker's Goals

Utilize the Kubernetes service account files to perform additional actions on the cluster.

Investigative actions

Check the exposed Kubernetes service account usage in the cluster.
Check if any other suspicious activity was performed inside the pod.

Suspicious Kubernetes service account token read by an unusual process

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials: Credentials In Files (T1552.001)
Severity	Medium

Description

An unusual process opened the Kubernetes service account token file for the first time.

Attacker's Goals

Utilize the Kubernetes service account files to perform additional actions on the cluster.

Investigative actions

Check the exposed Kubernetes service account usage in the cluster.
Check if any other suspicious activity was performed inside the pod.

Suspicious Kubernetes service account file read by an unusual process

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials: Credentials In Files (T1552.001)
Severity	Low

Description

An unusual process opened a Kubernetes service account file for the first time.

Attacker's Goals

Utilize the Kubernetes service account files to perform additional actions on the cluster.

Investigative actions

- Check the exposed Kubernetes service account usage in the cluster.
  Check if any other suspicious activity was performed inside the pod.

Suspicious Kubernetes service account token read

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials: Credentials In Files (T1552.001)
Severity	Low

Description

An unusual process opened the Kubernetes service account token file for the first time.

Attacker's Goals

Utilize the Kubernetes service account files to perform additional actions on the cluster.

Investigative actions

- Check the exposed Kubernetes service account usage in the cluster.
- Check if any other suspicious activity was performed inside the pod.

31.56 | A rare file path was added to the AppInit_DLLs registry value

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: ▯ XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	Injection Analytics
ATT&CK Tactic	Persistence (TA0003) Privilege Escalation (TA0004)
ATT&CK Technique	Event Triggered Execution (T1546)
Severity	Low

Description

A rare file path was added to AppInit_DLLs registry value.

Attacker's Goals

Establish persistence and/or elevate privileges by injecting malicious content triggered by AppInit DLLs loaded into processes.

Investigative actions

- Investigate the path of the modified value.
- Investigate the causality actor process - which initiated the activity.

Variations

A rare file path was added to the AppInit_DLLs registry valueusing a manual registry tool

Synopsis

ATT&CK Tactic	Persistence (TA0003) Privilege Escalation (TA0004)
ATT&CK Technique	Event Triggered Execution (T1546)
Severity	Medium

Description

A rare file path was added to AppInit_DLLs registry value.

Attacker's Goals

Establish persistence and/or elevate privileges by injecting malicious content triggered by AppInit DLLs loaded into processes.

Investigative actions

- Investigate the path of the modified value.
- Investigate the causality actor process - which initiated the activity.

A rare file path was added to the AppInit_DLLs registry valuewith a commonly abused path

Synopsis

ATT&CK Tactic	Persistence (TA0003) Privilege Escalation (TA0004)
ATT&CK Technique	Event Triggered Execution (T1546)
Severity	Medium

Description

A rare file path was added to AppInit_DLLs registry value.

Attacker's Goals

Establish persistence and/or elevate privileges by injecting malicious content triggered by AppInit DLLs loaded into processes.

Investigative actions

Investigate the path of the modified value.

Investigate the causality actor process - which initiated the activity.

31.57 | A user was added to a Windows security group

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Persistence (TA0003) Privilege Escalation (TA0004)
ATT&CK Technique	- Account Manipulation (T1098) Valid Accounts (T1078)
Severity	Informational

Description

A user was added to a Windows security group.

Attacker's Goals

Privilege escalation using a valid account.

Investigative actions

- Check the user who added the account to the group and verify its activity.

Variations

User added a member to a Windows privileged group for the first time

Synopsis

ATT&CK Tactic	Persistence (TA0003) Privilege Escalation (TA0004)
ATT&CK Technique	Account Manipulation (T1098) Valid Accounts (T1078)
Severity	Medium

Description

A user was added to a Windows security privileged group.

Attacker's Goals

Privilege escalation using a valid account.

Investigative actions

Check the user who added the account to the group and verify its activity.

User added to a Windows privileged group

Synopsis

ATT&CK Tactic	Persistence (TA0003) Privilege Escalation (TA0004)
ATT&CK Technique	Account Manipulation (T1098) Valid Accounts (T1078)
Severity	Low

Description

A user was added to a Windows security privileged group.

Attacker's Goals

Privilege escalation using a valid account.

Investigative actions

- Check the user who added the account to the group and verify its activity.

User removed from a Windows privileged group

Synopsis

ATT&CK Tactic	Persistence (TA0003) Privilege Escalation (TA0004)
ATT&CK Technique	Account Manipulation (T1098) Valid Accounts (T1078)
Severity	Informational

Description

A user was removed from a Windows security privileged group.

Attacker's Goals

Privilege escalation using a valid account.

Investigative actions

- Check the user who removed the account from the group and verify its activity.

A user was removed from a Windows security group

Synopsis

ATT&CK Tactic	Persistence (TA0003) Privilege Escalation (TA0004)
ATT&CK Technique	Account Manipulation (T1098) Valid Accounts (T1078)
Severity	Informational

Description

A user was removed from a Windows security group.

Attacker's Goals

Privilege escalation using a valid account.

Investigative actions

Check the user who removed the account from the group and verify its activity.

31.58 | A user changed the Windows system time

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Hour

Required Data	- Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	System Time Discovery (T1124)
Severity	Informational

Description

A user changed the Windows system time. This may be indicative of a malicious activity and may affect authentication from the source machine.

Attacker's Goals

A malicious insider might change their Windows system time. This action might affect the machine's ability to authenticate to the domain.

Investigative actions

Check for any other suspicious activity related to the host and the user involved in the alert.

31.59 | User added SID History to an account

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Hour
Required Data	Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Privilege Escalation (TA0004) Defense Evasion (TA0005)
ATT&CK Technique	Access Token Manipulation: SID-History Injection (T1134.005)
Severity	Informational

Description

A user added SID history to an account. This may be indicative of a user's migration between domains or a SID injection attack.

Attacker's Goals

Adversaries may use SID history to escalate privileges and bypass access controls.

Investigative actions

- Verify if migration between domains was involved.
- Search for suspicious actions by the user, such as forged Kerberos tickets.

Variations

Suspicious SID History Addition

Synopsis

ATT&CK Tactic	- Privilege Escalation (TA0004) - Defense Evasion (TA0005)
ATT&CK Technique	Access Token Manipulation: SID-History Injection (T1134.005)
Severity	Medium

Description

A user added SID history to an account. The account was not migrated between domains, which may indicate a SID injection attack.

Attacker's Goals

Adversaries may use SID history to escalate privileges and bypass access controls.

Investigative actions

- Verify if migration between domains was involved.
- Search for suspicious actions by the user, such as forged Kerberos tickets.

31.60 | Tampering with the Windows User Account Controls

(UAC) configuration

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	ǀ Requires: ▯ XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Abuse Elevation Control Mechanism: Bypass User Account Control (T1548.002)
Severity	Informational

Description

EnableLUA specifies whether Windows User Account Controls (UAC) notifies the user when programs try to modify the computer. UAC was formerly known as Limited User Account (LUA).

Attacker's Goals

Gain higher privileges by bypassing the User Account Control (UAC).

Investigative actions

Check whether the executing process is benign, and if this was a desired behavior as part of its normal execution flow.

Variations

Tampering with the Windows User Account Controls (UAC) configuration by a remote host

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Abuse Elevation Control Mechanism: Bypass User Account Control (T1548.002)
Severity	Medium

Description

EnableLUA specifies whether Windows User Account Controls (UAC) notifies the user when programs try to modify the computer. UAC was formerly known as Limited User Account (LUA).

Attacker's Goals

Gain higher privileges by bypassing the User Account Control (UAC).

Investigative actions

Check whether the executing process is benign, and if this was a desired behavior as part of its normal execution flow.

Tampering with the Windows User Account Controls (UAC) configuration

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Abuse Elevation Control Mechanism: Bypass User Account Control (T1548.002)
Severity	Low

Description

EnableLUA specifies whether Windows User Account Controls (UAC) notifies the user when programs try to modify the computer. UAC was formerly known as Limited User Account (LUA).

Attacker's Goals

Gain higher privileges by bypassing the User Account Control (UAC).

Investigative actions

Check whether the executing process is benign, and if this was a desired behavior as part of its normal execution flow.

Tampering with the Windows User Account Controls (UAC) configuration

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Abuse Elevation Control Mechanism: Bypass User Account Control (T1548.002)
Severity	Low

Description

EnableLUA specifies whether Windows User Account Controls (UAC) notifies the user when programs try to modify the computer. UAC was formerly known as Limited User Account (LUA).

Attacker's Goals

Gain higher privileges by bypassing the User Account Control (UAC).

Investigative actions

Check whether the executing process is benign, and if this was a desired behavior as part of its normal execution flow.

31.61 | Commonly abused AutoIT script drops an executable file to disk

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	