Required Data	- Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	- Obfuscated Files or Information: Encrypted/Encoded File (T1027.013) Deobfuscate/Decode Files or Information (T1140)
Severity	Medium

Description

Encoding/decoding to/from using certutil.exe could be used to evade detection.

Attacker's Goals

Evade detection by executing processes with obfuscated arguments.

Investigative actions

Check encoded/decoded command content and see whether it is benign or malicious.

30.37 | Uncommon remote service start via sc.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	Malicious Service Analytics
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	System Services: Service Execution (T1569.002)
Severity	Low

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

The Service Control command is used to create, start, stop, query, or delete Windows services. Attackers can use the command to attempt to execute and persist a binary, command, or script.

Investigative actions

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

- Check the remote host for any evidence of the executed service and investigate it.

30.38 | Possible collection of screen captures with Windows Problem Steps Recorder

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	Collection (TA0009)
ATT&CK Technique	Screen Capture (T1113)
Severity	Medium

Description

Windows Problem Steps Recorder (psr.exe), can record screen and clicks. Adversaries may abuse psr.exe to create screen captures and collect them afterward.

Attacker's Goals

Evading security controls and collecting screen captures of the desktop.

Investigative actions

Check the causality of execution and if the TSS script was executed (Microsoft Troubleshooting Script).

If output parameters in the command line are executed by the user.

- If the parent process is known in the organization as a support tool.

30.39 | Globally uncommon root-domain port combination 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 on a specific port 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 port combination 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 on a specific port 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 port combination 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 on a specific port 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 port combination 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 on a specific port 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 port combination 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 on a specific port 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.

30.40 | Unpopular rsync process 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	Kubernetes - AGENT, Containers
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Hide Artifacts: Hidden Files and Directories (T1564.001)
Severity	Informational

Description

An unpopular rsync process was executed on the host.

Attacker's Goals

Attackers may try to transfer tools or other files into a compromised host.

Investigative actions

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

Variations

Unpopular rsync process execution in a Kubernetes Pod

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Hide Artifacts: Hidden Files and Directories (T1564.001)
Severity	Informational

Description

An unpopular rsync process was executed on the host.

Attacker's Goals

Attackers may try to transfer tools or other files into a compromised host.

Investigative actions

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

30.41 | Rare SMB session to a remote host

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	2 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	NDR Lateral Movement Analytics
ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Services (T1021)
Severity	Low

Description

The endpoint performed a rare SMB activity to a remote host.

Attacker's Goals

Attackers may use the SMB protocol in an attempt to move laterally in the network, and expand their foothold in the organization.

Investigative actions

Check whether the username used in the SMB connection is legitimate.

Verify that this isn't IT activity.

Variations

Rare SMB session to a remote host

Synopsis

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

Description

The endpoint performed a rare SMB activity to a remote host.

Attacker's Goals

Attackers may use the SMB protocol in an attempt to move laterally in the network, and expand their foothold in the organization.

Investigative actions

Check whether the username used in the SMB connection is legitimate.
Verify that this isn't IT activity.

30.42 | Remote DCOM 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)
ATT&CK Technique	Remote Services: Distributed Component Object Model (T1021.003)
Severity	Low

Description

A remotely triggered DCOM initiated a command execution by a host that rarely executes processes using DCOM 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 DCOM call from the source host and understand which software initiated it.

Variations

Remote suspicious DCOM-MMC20.Application command execution

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008)

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

Description

A remotely triggered suspicious DCOM-MMC20.Application initiated a command execution by a host that rarely executes processes using DCOM 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 DCOM call from the source host and understand which software initiated it.

Remote suspicious DCOM-Excel.Application command execution

Synopsis

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

Description

A remotely triggered suspicious DCOM-Excel.Application initiated a command execution by a host that rarely executes processes using DCOM 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 DCOM call from the source host and understand which software initiated it.

Remote suspicious DCOM-Outlook.Application command execution

Synopsis

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

Description

A remotely triggered suspicious DCOM-Outlook.Application initiated a command execution by a host that rarely executes processes using DCOM 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 DCOM call from the source host and understand which software initiated it.

Remote suspicious DCOM command execution

Synopsis

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

Description

A remotely triggered suspicious DCOM initiated a command execution by a host that rarely executes processes using DCOM 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 DCOM call from the source host and understand which software initiated it.

30.43 | Abnormal Communication 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

An abnormal communication was seen from an internal entity to a rare external address.

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 Communication 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

An abnormal communication was seen from an internal entity to a rare external address.

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 Communication 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

An abnormal communication was seen from an internal entity to a rare external address.

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 Communication 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

An abnormal communication was seen from an internal entity to a rare external address.

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 Communication 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

An abnormal communication was seen from an internal entity to a rare external address.

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 Communication 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

An abnormal communication was seen from an internal entity to a rare external address.

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 Communication 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

An abnormal communication was seen from an internal entity to a rare external address.

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.

30.44 | Rare WinRM Session

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 Services: Windows Remote Management (T1021.006)
Severity	Informational

Description

Windows Remote Management (WinRM) enables users to interact with remote systems in different ways, including running executables on the remote system. WinRM sessions can be established using WinRM/WinRS commands or programs such as PowerShell. Attackers can use WinRM to execute code and move laterally within a compromised network.

Attacker's Goals

Windows Remote Management (WinRM) enables users to interact with remote systems in different ways, including running executables on the remote endpoint. WinRM sessions can be established using winrm/winrs commands or programs such as PowerShell. Attackers can use WinRM to execute code and move laterally within a compromised network.

Investigative actions

Investigate the endpoints participating in the session.

30.45 | Possible DLL Hijack into a Microsoft 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	DLL Hijacking Analytics
ATT&CK Tactic	Persistence (TA0003) Privilege Escalation (TA0004) Defense Evasion (TA0005)
ATT&CK Technique	Hijack Execution Flow: DLL Search Order Hijacking (T1574.001)
Severity	Low

Description

An unsigned DLL was loaded into a Microsoft signed process.
This DLL name is usually signed by Microsoft, which might indicate an attacker performing DLL Hijacking.

Attacker's Goals

An attacker is attempting to load an untrusted module into a trusted context to avoid detection, gain persistence or to perform privilege escalation.

Investigative actions

Investigate the loaded module to verify if it is malicious.

Investigate if the loading process and the loaded module reside in legitimate locations.

Variations

Possible DLL Hijack of a low entropy DLL into a Microsoft process

Synopsis

ATT&CK Tactic	Persistence (TA0003) Privilege Escalation (TA0004) Defense Evasion (TA0005)
ATT&CK Technique	Hijack Execution Flow: DLL Search Order Hijacking (T1574.001) Obfuscated Files or Information: Binary Padding (T1027.001)
Severity	High

Description

An unsigned DLL was loaded into a Microsoft signed process.
This DLL name is usually signed by Microsoft, which might indicate an attacker performing DLL Hijacking.

Attacker's Goals

An attacker is attempting to load an untrusted module into a trusted context to avoid detection, gain persistence or to perform privilege escalation.

Investigative actions

Investigate the loaded module to verify if it is malicious.
Investigate if the loading process and the loaded module reside in legitimate locations.

Possible DLL Side-Loading into a Microsoft process from a suspicious folder

Synopsis

ATT&CK Tactic	Persistence (TA0003) Privilege Escalation (TA0004) Defense Evasion (TA0005)
ATT&CK Technique	Hijack Execution Flow: DLL Search Order Hijacking (T1574.001) Hijack Execution Flow: DLL Side-Loading (T1574.002)

Severity	Medium

Description

An unsigned DLL was loaded into a Microsoft signed process.
This DLL name is usually signed by Microsoft, which might indicate an attacker performing DLL Hijacking.

Attacker's Goals

An attacker is attempting to load an untrusted module into a trusted context to avoid detection, gain persistence or to perform privilege escalation.

Investigative actions

- Investigate the loaded module to verify if it is malicious.
- Investigate if the loading process and the loaded module reside in legitimate locations.

DLL Hijack into a Microsoft process

Synopsis

ATT&CK Tactic	- Persistence (TA0003) - Privilege Escalation (TA0004) - Defense Evasion (TA0005)
ATT&CK Technique	Hijack Execution Flow: DLL Search Order Hijacking (T1574.001)
Severity	Medium

Description

An unsigned DLL was loaded into a Microsoft signed process.

This DLL name is usually signed by Microsoft, which might indicate an attacker performing DLL Hijacking.

Attacker's Goals

An attacker is attempting to load an untrusted module into a trusted context to avoid detection, gain persistence or to perform privilege escalation.

Investigative actions

- Investigate the loaded module to verify if it is malicious.
- Investigate if the loading process and the loaded module reside in legitimate locations.

Possible DLL Hijack into a Microsoft development or framework related process

Synopsis

ATT&CK Tactic	Persistence (TA0003) Privilege Escalation (TA0004) Defense Evasion (TA0005)
ATT&CK Technique	Hijack Execution Flow: DLL Search Order Hijacking (T1574.001)
Severity	Informational

Description

An unsigned DLL was loaded into a Microsoft signed process.
This DLL name is usually signed by Microsoft, which might indicate an attacker performing DLL Hijacking.

Attacker's Goals

An attacker is attempting to load an untrusted module into a trusted context to avoid detection, gain persistence or to perform privilege escalation.

Investigative actions

- Investigate the loaded module to verify if it is malicious.
- Investigate if the loading process and the loaded module reside in legitimate locations.

30.46 | A user accessed an uncommon AppID

Synopsis

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

Description

A user accessed an uncommon AppID that is rarely accessed by them or anyone else in the organization.

Attacker's Goals

A user accessed an uncommon AppID that is rarely accessed by them or anyone else in the organization. This may indicate an attempt to exfiltrate sensitive data.

Investigative actions

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

Variations

A user accessed an uncommon external peer-to-peer service

Synopsis

ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Exfiltration Over Web Service (T1567)
Severity	Informational

Description

A user accessed an uncommon external peer-to-peer service that is rarely accessed by them or anyone else in the organization.

Attacker's Goals

A user accessed an uncommon external peer-to-peer service that is rarely accessed by them or anyone else in the organization. This may indicate an attempt to exfiltrate sensitive data.

Investigative actions

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

A user accessed an uncommon external file-sharing service

Synopsis

ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Exfiltration Over Web Service (T1567)
Severity	Informational

Description

A user accessed an uncommon external file-sharing service that is rarely accessed by them or anyone else in the organization.

Attacker's Goals

A user accessed an uncommon external file-sharing service that is rarely accessed by them or anyone else in the organization. This may indicate an attempt to exfiltrate sensitive data.

Investigative actions

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

A user accessed an uncommon peer-to-peer service

Synopsis

ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Exfiltration Over Web Service (T1567)
Severity	Informational

Description

A user accessed an uncommon peer-to-peer service that is rarely accessed by them or anyone else in the organization.

Attacker's Goals

A user accessed an uncommon peer-to-peer service that is rarely accessed by them or anyone else in the organization. This may indicate an attempt to exfiltrate sensitive data.

Investigative actions

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

A user accessed an uncommon file-sharing service

Synopsis

ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Exfiltration Over Web Service (T1567)
Severity	Informational

Description

A user accessed an uncommon file-sharing service that is rarely accessed by them or anyone else in the organization.

Attacker's Goals

A user accessed an uncommon file-sharing service that is rarely accessed by them or anyone else in the organization. This may indicate an attempt to exfiltrate sensitive data.

Investigative actions

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

A user accessed an uncommon VPN service

Synopsis

ATT&CK Tactic	Exfiltration (TA0010)

ATT&CK Technique	Exfiltration Over Web Service (T1567)
Severity	Informational

Description

A user connected to an unusual VPN service that is rarely accessed by them or anyone else in the organization. This may indicate an attempt to hide their online activity.

Attacker's Goals

A user connected to an unusual VPN service that is rarely accessed by them or anyone else in the organization. This may indicate an attempt to hide their online activity.

Investigative actions

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

30.47 | Suspicious 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 one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Use Alternate Authentication Material: Pass the Hash (T1550.002)
Severity	Medium

Description

An Encrypting File System Remote call (EFSRPC) was made to a domain controller.

Attacker's Goals

An attacker is attempting to steal credentials and move laterally within a network.

Investigative actions

- Check for suspicious processes on the host.
- Check if the source host is a vulnerability scanner.
  Look for following suspicious connections using the DC machine account.

30.48 | Globally uncommon process execution 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	Execution (TA0002)
ATT&CK Technique	User Execution (T1204)
Severity	Informational

Description

A signed process has executed a process that, on a global level, it usually doesn't execute.

Attacker's Goals

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

Investigative actions

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

Variations

Globally uncommon process execution from a signed process from a known vendor

Synopsis

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

Description

A signed process has executed a process that, on a global level, it usually doesn't execute.

Attacker's Goals

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

Investigative actions

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

Globally rare process execution from a signed process

Synopsis

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

Severity	Medium

Description

A signed process has executed a process that, on a global level, it usually doesn't execute.

Attacker's Goals

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

Investigative actions

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

Globally uncommon process execution from an injected thread in a signed process

Synopsis

ATT&CK Tactic	Execution (TA0002) Defense Evasion (TA0005)
ATT&CK Technique	User Execution (T1204) Process Injection (T1055)
Severity	Low

Description

An injected thread in a signed process has executed a process that, on a global level, it usually doesn't execute.

Attacker's Goals

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

Investigative actions

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

Globally uncommon process execution from a web server process or CGO

Synopsis

ATT&CK Tactic	- Execution (TA0002) - Initial Access (TA0001) - Persistence (TA0003)
ATT&CK Technique	- User Execution (T1204) - External Remote Services (T1133) - Server Software Component: Web Shell (T1505.003)
Severity	Low

Description

A web server process or CGO has executed a process that, on a global level, it usually doesn't execute.

Attacker's Goals

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

Investigative actions

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

30.49 | Possible Kerberos relay attack

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	2 Days
Required Data	Requires one of the following data sources: - Windows Event Collector OR - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Abuse Elevation Control Mechanism (T1548)
Severity	Low

Description

A suspicious local network login was observed, which might indicate on Kerberos relay attack.

This attack can lead to privilege escalation by obtaining system privileges on the target.

Attacker's Goals

An attacker is attempting to elevate its privileges on the machine.

Investigative actions

- Check for any other suspicious activity related to the host involved in the alert.
- Look for a new machine that was added to the domain.

30.50 | Interactive login from a shared user account

Synopsis

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

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.

30.51 | Rare process execution by user

Synopsis

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

An unusual process was executed by a 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 process that was executed to determine if it was used for legitimate purposes or malicious activity.

30.52 | Recurring rare domain access to dynamic DNS domain

Synopsis

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

Deduplication Period	14 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	Command and Control (TA0011)
ATT&CK Technique	Application Layer Protocol (T1071)
Severity	Low

Description

The endpoint is periodically connecting to an external domain that it and its peers rarely use.
Access to this domain has occurred repeatedly over multiple days.
This connection pattern is consistent with malware connecting to its command and control server for updates and operating instructions.

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

Identify the process/user contacting the remote domain and determine whether the traffic is malicious.

- Look for other endpoints on your network that are also periodically contacting the suspicious domain.

30.53 | Abnormal network communication through TOR using an uncommon port

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	Command and Control (TA0011)
ATT&CK Technique	Application Layer Protocol (T1071) Non-Standard Port (T1571)

Severity	Low

Description

Suspicious connection from a known TOR IP to an uncommon port.

Attacker's Goals

Attackers might use TOR IP combined with random ports.to hide C2 inbound communication from inside a host.

Investigative actions

Investigate the network configuration related to the participating port.
Investigate processes that were listening to that port.

Variations

Abnormal network communication through TOR using an uncommon port and App-id

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Application Layer Protocol (T1071) Non-Standard Port (T1571)
Severity	Low

Description

Suspicious connection from a known TOR IP to an uncommon port and App-id.

Attacker's Goals

Attackers might use TOR IP combined with random ports.to hide C2 inbound communication from inside a host.

Investigative actions

Investigate the network configuration related to the participating port.
Investigate processes that were listening to that port.

Abnormal network communication through TOR using a suspicious port

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Application Layer Protocol (T1071) Non-Standard Port (T1571)
Severity	Low

Description

Suspicious connection from a known TOR IP to an uncommon potential C2 communication port.

Attacker's Goals

Attackers might use TOR IP combined with random ports.to hide C2 inbound communication from inside a host.

Investigative actions

Investigate the network configuration related to the participating port.
Investigate processes that were listening to that port.

30.54 | A compressed file was exfiltrated over SSH

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	Exfiltration (TA0010)
ATT&CK Technique	Exfiltration Over Alternative Protocol (T1048)
Severity	Informational

Description

Exfiltration of a compressed file over SSH.

Attacker's Goals

Attackers may try to exfiltrate data over encrypted network protocol.

Investigative actions

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

Variations

A compressed file was exfiltrated over SSH from a Kubernetes pod

Synopsis

ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Exfiltration Over Alternative Protocol (T1048)
Severity	Informational

Description

Exfiltration of a compressed file over SSH.

Attacker's Goals

Attackers may try to exfiltrate data over encrypted network protocol.

Investigative actions

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

30.55 | Discovery of host users via WMIC

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)
ATT&CK Technique	System Owner/User Discovery (T1033)
Severity	Informational

Description

Attackers may use wmic.exe to list the users of a host, and potentially its owner.

Attacker's Goals

Attackers can attempt to use the command to discover host users and enumerate a huge amount of information.

Investigative actions

Verify whether the command that was executed is benign or normal for the host and/or user performing it (for example, it may be an IT script).

30.56 | Weakly-Encrypted Kerberos Ticket Requested

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	30 Days
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 specifically requested weak and deprecated encryption in a Kerberos TGS request. This provides easy-to-crack hashes, and is typically a sign of a Kerberoasting attack.

Attacker's Goals

Crack account credentials by obtaining an easy-to-crack Kerberos ticket.

Investigative actions

Check who used the host at the time of the alert, to rule out a benign service or tool requesting weak Kerberos encryption.

Variations

Weakly-Encrypted Kerberos Ticket Requested on a sensitive server

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Steal or Forge Kerberos Tickets: Kerberoasting (T1558.003)
Severity	Medium

Description

A user specifically requested weak and deprecated encryption in a Kerberos TGS request. This provides easy-to-crack hashes, and is typically a sign of a Kerberoasting attack. This action occurred on a sensitive server, which may indicate a malicious activity.

Attacker's Goals

Crack account credentials by obtaining an easy-to-crack Kerberos ticket.

Investigative actions

Check who used the host at the time of the alert, to rule out a benign service or tool requesting weak Kerberos encryption.

30.57 | PsExec was executed with a suspicious command line

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) Privilege Escalation (TA0004)
ATT&CK Technique	- System Services: Service Execution (T1569.002) - Valid Accounts (T1078)
Severity	Informational

Description

PsExec.exe was executed.

Attacker's Goals

An adversary may attempt to use PsExec to gain execution capabilities, run remote commands or perform privilege escalation.

Investigative actions

- Check if any other suspicious activities happened under the same causality.
  Confirm the PsExec.exe command is benign.

Variations

PsExec was executed with a suspicious command line by a LOLBIN

Synopsis

ATT&CK Tactic	Execution (TA0002) Privilege Escalation (TA0004)
ATT&CK Technique	System Services: Service Execution (T1569.002) Valid Accounts (T1078)
Severity	Low

Description

PsExec.exe was executed with NT/System privilege level by a LOLBIN.

Attacker's Goals

An adversary may attempt to use PsExec to gain execution capabilities, run remote commands or perform privilege escalation.

Investigative actions

Check if any other suspicious activities happened under the same causality.
Confirm the PsExec.exe command is benign.

PsExec was executed with a suspicious command line by an unsigned actor

Synopsis

ATT&CK Tactic	Execution (TA0002) Privilege Escalation (TA0004)
ATT&CK Technique	System Services: Service Execution (T1569.002) Valid Accounts (T1078)
Severity	Medium

Description

PsExec.exe was executed with NT/System privilege level by an unsigned actor.

Attacker's Goals

An adversary may attempt to use PsExec to gain execution capabilities, run remote commands or perform privilege escalation.

Investigative actions

- Check if any other suspicious activities happened under the same causality.
- Confirm the PsExec.exe command is benign.

PsExec was executed with a suspicious command line

Synopsis

ATT&CK Tactic	Execution (TA0002) Privilege Escalation (TA0004)
ATT&CK Technique	System Services: Service Execution (T1569.002) Valid Accounts (T1078)
Severity	Low

Description

PsExec.exe was executed with NT/System privilege level.

Attacker's Goals

An adversary may attempt to use PsExec to gain execution capabilities, run remote commands or perform privilege escalation.

Investigative actions

Check if any other suspicious activities happened under the same causality.

Confirm the PsExec.exe command is benign.

PsExec was executed with a suspicious command line

Synopsis

ATT&CK Tactic	- Execution (TA0002) - Privilege Escalation (TA0004)
ATT&CK Technique	System Services: Service Execution (T1569.002) - Valid Accounts (T1078)
Severity	Low

Description

PsExec.exe was executed with plain-text credentials.

Attacker's Goals

An adversary may attempt to use PsExec to gain execution capabilities, run remote commands or perform privilege escalation.

Investigative actions

- Check if any other suspicious activities happened under the same causality.
  Confirm the PsExec.exe command is benign.

30.58 | Suspicious PowerShell Command Line

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	Command and Scripting Interpreter: PowerShell (T1059.001)
Severity	Low

Description

Attackers often leverage PowerShell one-liners, in which PowerShell is executed with suspicious options on the command line.

Attacker's Goals

Gain code execution on the host.

Investigative actions

Check whether the command line executed is benign or normal for the host and/or user performing it. For example, the command line may be an administrative script.

30.59 | Login by a dormant 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
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Valid Accounts: Domain Accounts (T1078.002)
Severity	Informational

Description

A dormant user logged on after having been unused for a month or longer.
This may indicate the account is misused by an attacker.

Attacker's Goals

Use a compromised user account which has not been used for a long time, and is therefore less likely to be noticed.

Investigative actions

- Confirm that the activity is benign (e.g. the user returned from a long leave of absence).
- See whether there are other abnormal actions done by the user (e.g. files\commands\other logins).
- Check whether you have issues with your Cloud Identity Engine failing to sync data from Active Directory.

Variations

Cached interactive login by a dormant user

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Valid Accounts: Domain Accounts (T1078.002)
Severity	Informational

Description

A dormant user logged on after having been unused for a month or longer.
This may indicate the account is misused by an attacker.

Attacker's Goals

Use a compromised user account which has not been used for a long time, and is therefore less likely to be noticed.

Investigative actions

- Confirm that the activity is benign (e.g. the user returned from a long leave of absence).
- See whether there are other abnormal actions done by the user (e.g. files\commands\other logins).
Check whether you have issues with your Cloud Identity Engine failing to sync data from Active Directory.

30.60 | Script 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
Detection Modules	
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Boot or Logon Autostart Execution (T1547)

Severity	Medium

Description

An attacker may add a script 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 commands on user login or computer boot.

Investigative actions

- Verify if the registered script is malicious.
  Check if the installing software is a malicious binary or script.

30.61 | System information discovery via psinfo.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
Detection Modules	

Detector Tags	
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	System Information Discovery (T1082)
Severity	Low

Description

Using psinfo.exe, the attacker can gather information about the network, and gain an in-depth understanding of which devices are relevant to attack.

Attacker's Goals

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

Investigative actions

- Check whether the executing process is benign, and if this was a desired behavior as part of its normal execution flow.
- Verify that this isn't sanctioned IT activity.
- Look for other hosts executing similar commands.

30.62 | Suspicious sshpass 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	Kubernetes - AGENT, Containers
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force: Credential Stuffing (T1110.004)
Severity	Low

Description

The sshpass command was executed, This could be an attempt to check for credential stuffing.

Attacker's Goals

Attackers may try to check and reuse credentials 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

Suspicious sshpass command execution in a Kubernetes pod

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force: Credential Stuffing (T1110.004)
Severity	Low

Description

The sshpass command was executed, This could be an attempt to check for credential stuffing.

Attacker's Goals

Attackers may try to check and reuse credentials 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.

30.63 | A contained executable was executed by an unusual 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	Privilege Escalation (TA0004) Persistence (TA0003)
ATT&CK Technique	Escape to Host (T1611) Boot or Logon Autostart Execution: Kernel Modules and Extensions (T1547.006)
Severity	Medium

Description

A docker contained executable from a mounted share was executed on a host.
Running a contained executable is highly dangerous and atypical.

Attacker's Goals

Gain high privileged command execution on the host machine via one of its running containers.

Investigative actions

Check what actions were made after the suspicious file execution.
Investigate the contained process and its process tree.

Variations

A contained executable was executed by the Linux kernel thread daemon

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004) Persistence (TA0003)
ATT&CK Technique	Escape to Host (T1611) Boot or Logon Autostart Execution: Kernel Modules and Extensions (T1547.006)
Severity	High

Description

A contained executable in a cloud machine was executed by the Linux kernel thread daemon. This behavior is suspicious as it may be a result of an attacker attempting to escape from a container, as the kernel thread daemon is usually used to spawn kernel processes only.

Attacker's Goals

Gain high privileged command execution on the host machine via one of its running containers.

Investigative actions

- Check what actions were made after the suspicious file execution.
  Investigate the contained process and its process tree.

A contained executable was executed by the Linux kernel thread daemon

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004) - Persistence (TA0003)
ATT&CK Technique	Escape to Host (T1611) - Boot or Logon Autostart Execution: Kernel Modules and Extensions (T1547.006)

Severity	High

Description

A contained executable was executed by the Linux kernel thread daemon.
This behavior is suspicious as it may be a result of an attacker attempting to escape from a container, as the kernel thread daemon is usually used to spawn kernel processes only.

Attacker's Goals

Gain high privileged command execution on the host machine via one of its running containers.

Investigative actions

- Check what actions were made after the suspicious file execution.
- Investigate the contained process and its process tree.

A contained executable was executed by an unusual process

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004) Persistence (TA0003)
ATT&CK Technique	Escape to Host (T1611) Boot or Logon Autostart Execution: Kernel Modules and Extensions (T1547.006)
Severity	Medium

Description

A docker contained executable from a mounted share on a cloud machine was executed on a host.
Running a contained executable is highly dangerous and atypical.

Attacker's Goals

Gain high privileged command execution on the host machine via one of its running containers.

Investigative actions

- Check what actions were made after the suspicious file execution.
- Investigate the contained process and its process tree.

30.64 | Suspicious docker image download from an unusual repository

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	User Execution: Malicious Image (T1204.003)
Severity	Informational

Description

The agent has pulled a docker image from a repository for the first time.

Attacker's Goals

Adversaries may rely on a user running a malicious image to facilitate execution.

Investigative actions

- Scan the docker image that was pulled.
  Check the repository designation.
  Check on which other agents the docker image is being used.

Variations

Suspicious docker image download from an unrecognized registry

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	User Execution: Malicious Image (T1204.003)
Severity	Low

Description

The agent has pulled a docker image from a registry that has never been used in the organization.

Attacker's Goals

Adversaries may rely on a user running a malicious image to facilitate execution.

Investigative actions

- Scan the docker image that was pulled.
- Check the repository designation.
  Check on which other agents the docker image is being used.

Suspicious docker image download from an unrecognized repository

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	User Execution: Malicious Image (T1204.003)
Severity	Low

Description

The agent has pulled a docker image from a repository that has never been used in the organization.

Attacker's Goals

Adversaries may rely on a user running a malicious image to facilitate execution.

Investigative actions

Scan the docker image that was pulled.
Check the repository designation.

Check on which other agents the docker image is being used.

30.65 | PowerShell suspicious flags

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	
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Command and Scripting Interpreter: PowerShell (T1059.001)
Severity	Medium

Description

Abbreviated flags in PowerShell indicate malicious intent.

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.

30.66 | Unusual Kubernetes dashboard communication from a

pod

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
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Container and Resource Discovery (T1613)
Severity	Low

Description

The Kubernetes dashboard was accessed by an unusual pod within the environment.

Attacker's Goals

Usage of the Kubernetes dashboard to perform operations inside the cluster.

Investigative actions

Check if there is an active attack against the Kubernetes cluster.

Variations

Unusual Kubernetes dashboard communication from a new pod

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Container and Resource Discovery (T1613)
Severity	Informational

Description

The Kubernetes dashboard was accessed by an unusual pod within the environment.

Attacker's Goals

Usage of the Kubernetes dashboard to perform operations inside the cluster.

Investigative actions

Check if there is an active attack against the Kubernetes cluster.

30.67 | Globally uncommon IP address connection 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	Informational

Description

A signed process 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 a signed 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 connection 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	Medium

Description

An injected thread in a signed process 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 a signed 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 connection from a signed process from a known vendor

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 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 a signed 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 connection 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	Low

Description

A signed process 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 a signed 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.

30.68 | Suspicious failed HTTP request - potential Spring4Shell exploit

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	Initial Access (TA0001)
ATT&CK Technique	Exploit Public-Facing Application (T1190)
Severity	Low

Description

A potentially malicious failed HTTP request was received, possibly as part of a Spring4Shell exploitation attempt.

Attacker's Goals

Gain the ability to execute code remotely or drop malware.

Investigative actions

- Check if suspicious process executions occurred after the request.
  Consider limiting access to the vulnerable serve.

Variations

Suspicious HTTP request - potential Spring4Shell exploit

Synopsis

ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Exploit Public-Facing Application (T1190)
Severity	Medium

Description

A potentially malicious HTTP request was received, possibly as part of a Spring4Shell exploitation attempt.

Attacker's Goals

Gain the ability to execute code remotely or drop malware.

Investigative actions

Check if suspicious process executions occurred after the request.
Consider limiting access to the vulnerable serve.

30.69 | Extracting credentials from Unix files

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	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials: Credentials In Files (T1552.001)
Severity	Low

Description

Suspicious Unix files containing insecurely stored credentials were accessed.

Attacker's Goals

Adversaries may search local file systems and remote file shares for files containing insecurely stored credentials.

Investigative actions

Investigate the process activities and use of the extracted credentials.

30.70 | A disabled user attempted to log in

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 disabled user attempted to log in.

Attacker's Goals

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

Investigative actions

- Confirm that the activity is benign (e.g. the user was recently enabled by an authorized entity).
  Check whether you have issues with your Cloud Identity Engine failing to sync data from Active Directory.

  Monitor services that may be running with a disabled user's credentials.

Variations

Cached interactive login attempt by a disabled user

Synopsis

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

Description

A disabled user attempted to log in.

Attacker's Goals

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

Investigative actions

- Confirm that the activity is benign (e.g. the user was recently enabled by an authorized entity).
  Check whether you have issues with your Cloud Identity Engine failing to sync data from Active Directory.
- Monitor services that may be running with a disabled user's credentials.

30.71 | Weakly-Encrypted Kerberos TGT Response

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	Credential Access (TA0006) Defense Evasion (TA0005) ▌ Persistence (TA0003)
ATT&CK Technique	Modify Authentication Process: Domain Controller Authentication (T1556.001)
Severity	Informational

Description

A weakly encrypted TGT was issued by a DC. The encryption type is abnormal to the DC and provides an easy-to-crack TGT. This might indicate a Skeleton Key attack.

Attacker's Goals

To patch the DC's authentication process, bypass standard authentication, and gain access to hosts and resources in single-factor authentication environments.

Investigative actions

Checked the user or entity that accessed the host during the alert-triggering timeframe, to eliminate the possibility of a benign service or application requesting weak Kerberos encryption.
Checking if the DC is patched for Skeleton key attack (CVE-2016-1567).

Variations

Abnormal Weakly-Encrypted Kerberos TGT Response

Synopsis

ATT&CK Tactic	- Credential Access (TA0006) Defense Evasion (TA0005) Persistence (TA0003)
ATT&CK Technique	Modify Authentication Process: Domain Controller Authentication (T1556.001)
Severity	Low

Description

A weakly encrypted TGT was issued by a DC. The encryption type is abnormal to the DC and provides an easy-to-crack TGT. This might indicate a Skeleton Key attack.

Attacker's Goals

To patch the DC's authentication process, bypass standard authentication, and gain access to hosts and resources in single-factor authentication environments.

Investigative actions

Checked the user or entity that accessed the host during the alert-triggering timeframe, to eliminate the possibility of a benign service or application requesting weak Kerberos encryption.
Checking if the DC is patched for Skeleton key attack (CVE-2016-1567).

30.72 | Compressing data using python

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	Collection (TA0009)
ATT&CK Technique	Archive Collected Data: Archive via Library (T1560.002)
Severity	Low

Description

Usage of a Python module to compress files.

Attacker's Goals

Collecting and staging data before exfiltration.

Investigative actions

Investigate the process and command line for access to sensitive files.

30.73 | Rare Remote Service (SVCCTL) RPC 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	NDR Lateral Movement Analytics
ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Services (T1021)
Severity	Informational

Description

The endpoint performed abnormal RPC activity via Service Control Manager interface 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 services.
  The service control manager RPC interface is used to create and start services on a local or a remote host.

Investigative actions

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

Variations

Rare remote service creation and initiation via Remote Service (SVCCTL) RPC interface

Synopsis

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

Description

The endpoint performed abnormal service creation and initiation via Remote Service (SVCCTL) RPC interface 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 services.

- The service control manager RPC interface is used to create and start services on a local or a remote host.

Investigative actions

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

Rare remote service change or creation via Remote Service (SVCCTL) RPC interface

Synopsis

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

Description

The endpoint performed abnormal service creation via Remote Service (SVCCTL) RPC interface 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 services.
  The service control manager RPC interface is used to create and start services on a local or a remote host.

Investigative actions

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

Rare Remote Service (SVCCTL) RPC activity

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008)

ATT&CK Technique	Remote Services (T1021)
Severity	Low

Description

The endpoint performed abnormal RPC activity via Service Control Manager interface 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 services.
- The service control manager RPC interface is used to create and start services on a local or a remote host.

Investigative actions

Review the action of services.exe on the remote host where possible.

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

- Verify that this isn't IT activity.

30.74 | Rare RDP session to a remote host

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	2 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	NDR Lateral Movement Analytics
ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Services: Remote Desktop Protocol (T1021.001)
Severity	Low

Description

The endpoint performed a rare RDP session to a remote host.

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

Rare RDP session to a remote host

Synopsis

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

Description

The endpoint performed a rare RDP session to a remote host.

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.

30.75 | Reading bash command history 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
Detection Modules	
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials: Bash History (T1552.003)
Severity	Low

Description

Attackers may access the bash history file to glean cleartext usernames and passwords that were entered on the command line.

Attacker's Goals

Adversaries may search the bash history file to search for insecurely stored credentials.

Investigative actions

Investigate the process activities and use of the extracted credentials.

30.76 | Network traffic to a crypto miner related domain 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
Detection Modules	
Detector Tags	Kubernetes - AGENT
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Resource Hijacking (T1496)
Severity	Informational

Description

A network connection attempt was performed to a suspected crypto miner related domain.

Attacker's Goals

Validate transactions on cryptocurrency networks and earn virtual currency.

Investigative actions

Block all network traffic to known crypto miners related domain.

Variations

Suspicious network traffic to a crypto miner related domain from within a Kubernetes pod

Synopsis

ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Resource Hijacking (T1496)
Severity	Medium

Description

A network connection was established to a suspected crypto miner related domain from within a Kubernetes Pod.

Attacker's Goals

Validate transactions on cryptocurrency networks and earn virtual currency.

Investigative actions

Block all network traffic to known crypto miners related domain.

Suspicious network traffic to a crypto miner related domain

Synopsis

ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Resource Hijacking (T1496)
Severity	Low

Description

A network connection was established to a suspected crypto miner related domain.

Attacker's Goals

Validate transactions on cryptocurrency networks and earn virtual currency.

Investigative actions

Block all network traffic to known crypto miners related domain.

Suspicious DNS traffic to a crypto miner related domain from within a Kubernetes pod

Synopsis

ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Resource Hijacking (T1496)
Severity	Low

Description

A DNS query was established to a suspected crypto miner related domain from within a Kubernetes Pod.

Attacker's Goals

Validate transactions on cryptocurrency networks and earn virtual currency.

Investigative actions

Block all network traffic to known crypto miners related domain.

Suspicious DNS traffic to a crypto miner related domain

Synopsis

ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Resource Hijacking (T1496)
Severity	Low

Description

A DNS query attempt was performed to a suspected crypto miner related domain.

Attacker's Goals

Validate transactions on cryptocurrency networks and earn virtual currency.

Investigative actions

Block all network traffic to known crypto miners related domain.

30.77 | Autorun.inf created in root C drive

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) Lateral Movement (TA0008)

ATT&CK Technique	- Hijack Execution Flow: Services File Permissions Weakness (T1574.010) Replication Through Removable Media (T1091)
Severity	Medium

Description

An autorun file installed at the root of a C:\ drive is suspicious, as autorun files are typically associated with removable drives.

Attacker's Goals

The Autorun and AutoPlay components of Microsoft Windows operating systems may use 'Autorun.inf' to automatically execute a program (without user interaction). Adversaries can manipulate this mechanism to run a malicious program.

Investigative actions

Read the content of the 'Autorun.inf' file from the root directory folder of the drive (the file may be hidden).

30.78 | WmiPrvSe.exe Rare Child Command Line

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) Execution (TA0002)
ATT&CK Technique	Remote Services (T1021) Remote Services: Windows Remote Management (T1021.006) Windows Management Instrumentation (T1047)
Severity	Low

Description

A remote WMI command executed a binary proxy, the Windows Management Instrumentation (WMI) Provider Host wmiprvse.exe, which executed a rare child command line. Executing a rare child process can be an indication of remote code execution abuse by an attacker.

Attacker's Goals

Gain code execution on a remote host.

Investigative actions

- Investigate the processes being spawned from WmiPrvse.exe on the host for malicious indicators.
- Correlate the RPC call from the source host and understand what initiated it.

Variations

WmiPrvSe.exe Rare Child Command Line

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008) Execution (TA0002)
ATT&CK Technique	Remote Services (T1021) Remote Services: Windows Remote Management (T1021.006) Windows Management Instrumentation (T1047)
Severity	Medium

Description

A remote WMI command executed a binary proxy, the Windows Management Instrumentation (WMI) Provider Host wmiprvse.exe, which executed a rare child command line. Executing a rare child process can be an indication of remote code execution abuse by an attacker.

Attacker's Goals

Gain code execution on a remote host.

Investigative actions

- Investigate the processes being spawned from WmiPrvse.exe on the host for malicious indicators.
  Correlate the RPC call from the source host and understand what initiated it.

30.79 | Contained process execution with a rare GitHub URL

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	N/A (single event)
Deduplication Period	3 Hours
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	User Execution: Malicious Image (T1204.003)
Severity	Low

Description

A contained process was executed with a suspicious GitHub url in the command line. This may be a legitimate use, but this technique is frequently used by attackers to download malicious payloads.

Attacker's Goals

Download a second stage payload for execution.

Investigative actions

- Check if the initiator process is malicious.
- Check the user activity on the same container in that time.
- Check if the container is a development container.
- Check if this installation was related to more installations at the same time.
- Check for additional file/network operations by the same process instance.

30.80 | Msiexec execution of an executable from an uncommon remote location

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	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	System Binary Proxy Execution: Msiexec (T1218.007)
Severity	Informational

Description

Msiexec is the command-line utility for the Windows Installer. Adversaries may abuse msiexec.exe to proxy execution of malicious payloads from remote locations.

Attacker's Goals

Evading security controls and executing arbitrary files from the web.

Investigative actions

- Check execution of msiexec and the IP/Domain that used.
- Is the URL that is encoded in the command line trusted.
  Is executed DLL or MSI file known as legitimate.
  Is the initiating process legitimate and the user running it knows of its use.

Variations

Msiexec execution of an executable from an uncommon remote location with a specific port

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	System Binary Proxy Execution: Msiexec (T1218.007)
Severity	High

Description

Msiexec is the command-line utility for the Windows Installer. Adversaries may abuse msiexec.exe to proxy execution of malicious payloads from remote locations.

Attacker's Goals

Evading security controls and executing arbitrary files from the web.

Investigative actions

- Check execution of msiexec and the IP/Domain that used.
  Is the URL that is encoded in the command line trusted.
  Is executed DLL or MSI file known as legitimate.

  Is the initiating process legitimate and the user running it knows of its use.

Msiexec execution of an executable from an uncommon remote location without properties

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	System Binary Proxy Execution: Msiexec (T1218.007)
Severity	Medium

Description

Msiexec is the command-line utility for the Windows Installer. Adversaries may abuse msiexec.exe to proxy execution of malicious payloads from remote locations. Execution without properties is more common in malware.

Attacker's Goals

Evading security controls and executing arbitrary files from the web.

Investigative actions

Check execution of msiexec and the IP/Domain that used.

Is the URL that is encoded in the command line trusted.

- Is executed DLL or MSI file known as legitimate.
- Is the initiating process legitimate and the user running it knows of its use.

30.81 | Kubernetes secret enumeration 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	Kubernetes - AGENT
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials: Container API (T1552.007)
Severity	Informational

Description

Kubectl secret enumeration command was executed.

Attacker's Goals

Attackers may gather sensitive information within a container environment.

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 secret enumeration activity from a Kubernetes Pod

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials: Container API (T1552.007)
Severity	Medium

Description

Kubectl secret enumeration command was executed.

Attacker's Goals

Attackers may gather sensitive information within a container environment.

Investigative actions

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

Kubernetes secret enumeration activity from a host

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials: Container API (T1552.007)
Severity	Low

Description

Kubectl secret enumeration command was executed.

Attacker's Goals

Attackers may gather sensitive information within a container environment.

Investigative actions

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

30.82 | Possible DCShadow 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: - 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 OR - XDR Agent
Detection Modules	

Detector Tags	
ATT&CK Tactic	- Credential Access (TA0006) - Defense Evasion (TA0005)
ATT&CK Technique	- OS Credential Dumping (T1003) - Rogue Domain Controller (T1207)
Severity	High

Description

Attackers may register a compromised host as a new DC to get other DCs to replicate data to it, and then push their malicious AD changes to all DCs.

Attacker's Goals

Retrieve Active Directory data, to later be able to push out malicious Active Directory changes.

Investigative actions

Check whether the destination is a new domain controller or a host that syncs with ADFS or Azure AD.

30.83 | Mimikatz command-line 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	Credential Access (TA0006)
ATT&CK Technique	OS Credential Dumping (T1003)
Severity	High

Description

These command-line arguments are often used by Mimikatz to dump and harvest credentials.

Attacker's Goals

An attacker is attempting to use Mimikatz, a known credential theft tool, to dump and harvest credentials.

Investigative actions

Investigate the executed process to verify if it is malicious.
Investigate the command line purpose.

30.84 | Suspicious process executed with a high integrity level

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	
ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Abuse Elevation Control Mechanism (T1548)
Severity	Informational

Description

A suspicious process spawned with a high/System integrity level, which is higher than its parent. This may be an indication of malicious privilege escalation.

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

Suspicious process executed with a high integrity level

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Abuse Elevation Control Mechanism (T1548)
Severity	Low

Description

A suspicious process spawned with a high/System integrity level, which is higher than its parent.

This may be an indication of malicious privilege escalation.

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.

30.85 | System shutdown or reboot

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	System Shutdown/Reboot (T1529)
Severity	Informational

Description

System shutdown or reboot using shutdown, reboot, halt or poweroff.

Attacker's Goals

Attackers may shut down or reboot hosts to disturb access to those hosts.

Investigative actions

- Verify that this isn't IT activity.

30.86 | Suspicious process accessed a site masquerading as Google

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) Defense Evasion (TA0005)
ATT&CK Technique	Web Service: Bidirectional Communication (T1102.002) Masquerading (T1036)
Severity	Informational

Description

A suspicious process accessed a site masquerading as Google.

Attacker's Goals

Masquerade legitimate looking Google services for defense evasion and C&C.

Investigative actions

- See whether this site has a malicious reputation.
  Follow process activities.
  Monitor traffic to the site.

Variations

Suspicious process resolved the DNS name of a site masquerading as Google

Synopsis

ATT&CK Tactic	Command and Control (TA0011) Defense Evasion (TA0005)
ATT&CK Technique	Web Service: Bidirectional Communication (T1102.002) Masquerading (T1036)
Severity	Informational

Description

A suspicious process resolved the DNS name of a site masquerading as Google.

Attacker's Goals

Masquerade legitimate looking Google services for defense evasion and C&C.

Investigative actions

See whether this site has a malicious reputation.
Follow process activities.

Monitor traffic to the site.

30.87 | Possible IPFS traffic was detected

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	Exfiltration (TA0010) Initial Access (TA0001)
ATT&CK Technique	Exfiltration Over Alternative Protocol (T1048) Phishing (T1566)
Severity	Informational

Description

The host attempted to access other nodes in an IPFS manner.

Attacker's Goals

IPFS access may expose your organization to new malware or allow attackers/ malicious insiders to exfiltrate data.

Investigative actions

Check the host for IPFS client software.
Examine the client's network traffic for uploaded or downloaded file hashes.

30.88 | Bronze-Bit exploit

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	Execution (TA0002)
ATT&CK Technique	User Execution (T1204)
Severity	High

Description

A forwardable Kerberos ticket for delegation of a Protected User was observed.

Attacker's Goals

Gain a special user's Kerberos ticket to move laterally.

Investigative actions

- Check the initiating service account delegation privileges.
  Check the delegated account credentials and if it has high privileges.
  Check the ticket destination to verify whether it is a sensitive asset.

30.89 | Hidden Attribute was added to a file using attrib.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	Hide Artifacts: Hidden Files and Directories (T1564.001)
Severity	Informational

Description

Hidden attribute was added to a file using attrib.exe, adversaries may set files to be hidden to evade detection mechanisms.

Attacker's Goals

Hide malware or staged files from standard file explorers.

Investigative actions

Check if the hidden file is malicious.
- Verify if the process executing the command is malicious.
- Check for more suspicious actions done by the user and process.

30.90 | Signed process performed an unpopular 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	Informational

Description

A signed process performed an unpopular DLL injection 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

Signed process that got injected performed an unpopular and suspicious dll injection

Synopsis

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

Description

A signed process performed an unpopular DLL injection 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.

Signed process that got injected performed an unpopular and suspicious dll injection

Synopsis

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

Description

A signed process performed an unpopular DLL injection 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.

Signed process that got injected performed an unpopular dll injection

Synopsis

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

Description

A signed process performed an unpopular DLL injection 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.

Signed process performed an unpopular DLL injection

Synopsis

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

Description

A signed process performed an unpopular DLL injection 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.

30.91 | Unusual AWS credentials creation

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	Account Manipulation: Additional Cloud Credentials (T1098.001)
Severity	Low

Description

AWS utility was used to create an access key and a secret key.

Attacker's Goals

Maintain access to an AWS provider.

Investigative actions

Check the machine timeline and look for abnormal activity.

Investigate what other calls were made to the AWS account.

30.92 | Suspicious process execution from tmp folder

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	Hide Artifacts: Hidden Files and Directories (T1564.001)
Severity	Informational

Description

An unpopular process was executed from the tmp folder.

Attacker's Goals

Attackers may try to run the executable application from a folder that is writable to all users and use it to avoid detection.

Investigative actions

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

Variations

A web server process executed an unpopular application from the tmp folder

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Hide Artifacts: Hidden Files and Directories (T1564.001)
Severity	Medium

Description

An executable application ran from the tmp folder by a web server process.

Attacker's Goals

Attackers may try to run the executable application from a folder that is writable to all users and use it to avoid detection.

Investigative actions

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

Suspicious cron job task execution of a binary from the tmp folder

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Hide Artifacts: Hidden Files and Directories (T1564.001)
Severity	Medium

Description

An unpopular process was executed from the tmp folder.

Attacker's Goals

Attackers may try to run the executable application from a folder that is writable to all users and use it to avoid detection.

Investigative actions

Verify that this isn't IT activity.

Look for other hosts executing similar commands.

Suspicious interactive execution of a binary from the tmp folder

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Hide Artifacts: Hidden Files and Directories (T1564.001)
Severity	Medium

Description

An unpopular process was executed from the tmp folder.

Attacker's Goals

Attackers may try to run the executable application from a folder that is writable to all users and use it to avoid detection.

Investigative actions

Verify that this isn't IT activity.

Look for other hosts executing similar commands.

Suspicious process execution from tmp folder in a Kubernetes pod

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Hide Artifacts: Hidden Files and Directories (T1564.001)
Severity	Informational

Description

An unpopular process was executed from the tmp folder.

Attacker's Goals

Attackers may try to run the executable application from a folder that is writable to all users and use it to avoid detection.

Investigative actions

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

30.93 | Suspicious .NET process loads an MSBuild DLL

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	Trusted Developer Utilities Proxy Execution: MSBuild (T1127.001)
Severity	Medium

Description

A suspicious process in the Microsoft .NET directory loaded the Microsoft Build Framework DLL. This may occur if an attacker masquerades a process like MSBuild (PowerLessShell).

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.

30.94 | Rundll32.exe executes a rare unsigned module

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	Low

Description

Rundll32.exe executes a rare unsigned module, which can indicate an attacker's malicious execution.

Attacker's Goals

Evading detections by running code from a signed Microsoft executable.

Investigative actions

Check whether the loaded module with the corresponding hash is benign, and if this was a desired behavior as part of its normal execution flow.

Variations

Rundll32.exe executes a rare unsigned module with very high entropy

Synopsis

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

Description

Rundll32.exe executes a rare unsigned module, which can indicate an attacker's malicious execution. The module executed by Rundll32 has very high entropy.

Attacker's Goals

Evading detections by running code from a signed Microsoft executable.

Investigative actions

Check whether the loaded module with the corresponding hash is benign, and if this was a desired behavior as part of its normal execution flow.

Rundll32.exe executes a rare unsigned module with suspicious characteristics

Synopsis

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

Description

Rundll32.exe executes a rare unsigned module, which can indicate an attacker's malicious execution.

Attacker's Goals

Evading detections by running code from a signed Microsoft executable.

Investigative actions

Check whether the loaded module with the corresponding hash is benign, and if this was a desired behavior as part of its normal execution flow.

30.95 | TGT request with a spoofed sAMAccountName - Network

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	3 Hours
Required Data	Requires: ▯ XDR Agent
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 authentication ticket (TGT) 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.
- Check if any associated service tickets were granted.
  Follow actions by the account and if it performed a DCSync.

30.96 | Unprivileged process opened a registry hive

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: Credentials In Files (T1552.001)
Severity	High

Description

An unprivileged process opened a registry hive directly.

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.

30.97 | Suspicious execution of ODBCConf

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: Odbcconf (T1218.008)
Severity	Medium

Description

Attackers may abuse the Odbcconf.exe Windows utility to proxy the execution of malicious DLL files.

Attacker's Goals

Execute arbitrary code or load malicious DLL modules undetected within Microsoft signed program from Microsoft signed process.

Investigative actions

- Check the execution command-line, in case of 'REGSVR' points to a DLL, then check it. If the command-line contains '/f' argument (for script file) check the content of the script.

30.98 | Unsigned process injecting into a Windows system binary with no command line

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) Privilege Escalation (TA0004)

ATT&CK Technique	Process Injection (T1055)
Severity	Medium

Description

An attacker may be trying to avoid detection by injecting their malicious code into a legitimate Windows system binary.

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.

30.99 | Run downloaded script using pipe

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

Downloading a script using wget or curl and executing it using a pipe to a shell.

Attacker's Goals

Attackers may try to download a script using wget or curl.

Investigative actions

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

Variations

Run downloaded script using pipe in a Kubernetes pod

Synopsis

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

Description

Downloading a script using wget or curl and executing it using a pipe to a shell.

Attacker's Goals

Attackers may try to download a script using wget or curl.

Investigative actions

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

30.100 | Rare file transfer over SMB protocol

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	2 Days
Required Data	Requires: - Palo Alto Networks Platform Logs ▮ 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 an abnormal file transfer over SMB to a remote host.

Attacker's Goals

- Attackers may attempt to gain persistence or move laterally over the network by dropping executable files and scripts on remote hosts using the SMB protocol.

Investigative actions

Inspect the file that was transferred to the remote host.

Verify that this isn't IT activity.

30.101 | Scripting engine 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) Execution (TA0002)
ATT&CK Technique	Application Layer Protocol (T1071) Command and Scripting Interpreter (T1059)
Severity	Low

Description

Scripts connecting to external IP addresses may be sanctioned IT scripts. However, when those external IP addresses are only receiving connections from a few specific endpoints in the organization, these scripts may be an indicator of more suspicious activity. Security testers and adversaries use offensive frameworks that employ forms of scripting which result in this type of network activity.

Attacker's Goals

Connect to the attacker's Command and Control server.

Investigative actions

- Check the external address the process connects to.
- Fetch and investigate the executed script.

Variations

Scripting engine failed to connect to a rare external host

Synopsis

ATT&CK Tactic	Command and Control (TA0011) Execution (TA0002)
ATT&CK Technique	Application Layer Protocol (T1071) Command and Scripting Interpreter (T1059)
Severity	Informational

Description

Scripts connecting to external IP addresses may be sanctioned IT scripts. However, when those external IP addresses are only receiving connections from a few specific endpoints in the organization, these scripts may be an indicator of more suspicious activity. Security testers and adversaries use offensive frameworks that employ forms of scripting which result in this type of network activity.

Attacker's Goals

Connect to the attacker's Command and Control server.

Investigative actions

Check the external address the process connects to.
Fetch and investigate the executed script.

Windows LOLBIN scripting engine connected to a rare external host

Synopsis

ATT&CK Tactic	Command and Control (TA0011) Execution (TA0002)
ATT&CK Technique	Application Layer Protocol (T1071) Command and Scripting Interpreter (T1059)

Severity	Medium

Description

Scripts connecting to external IP addresses may be sanctioned IT scripts. However, when those external IP addresses are only receiving connections from a few specific endpoints in the organization, these scripts may be an indicator of more suspicious activity. Security testers and adversaries use offensive frameworks that employ forms of scripting which result in this type of network activity.

Attacker's Goals

Connect to the attacker's Command and Control server.

Investigative actions

- Check the external address the process connects to.
- Fetch and investigate the executed script.

30.102 | Login attempt by a honey user

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	Identity Analytics
Detector Tags	Honey User Analytics
ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Low

Description

A login attempt was made by a honey user, a decoy account created to detect unauthorized access. This may indicate potential attacker activity attempting to use valid or stolen credentials.

Attacker's Goals

An attacker is attempting to gain unauthorized access by exploiting valid or stolen credentials.

Investigative actions

- Confirm that the alert was triggered by a honey user account.
- Check for other login attempts on different accounts from the same source IP.
  Analyze any subsequent actions performed by the user after the login attempt.
  Follow further actions performed by the user.

Variations

Successful login by a honey user

Synopsis

ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts (T1078)

Severity	Medium

Description

A login attempt was made by a honey user, a decoy account created to detect unauthorized access. This may indicate potential attacker activity attempting to use valid or stolen credentials.

Attacker's Goals

An attacker is attempting to gain unauthorized access by exploiting valid or stolen credentials.

Investigative actions

Confirm that the alert was triggered by a honey user account.
Check for other login attempts on different accounts from the same source IP.

Analyze any subsequent actions performed by the user after the login attempt.
- Follow further actions performed by the user.

30.103 | Uncommon msiexec execution of an arbitrary file from a remote location

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: Msiexec (T1218.007)
Severity	Low

Description

Msiexec is the command-line utility for the Windows Installer. Adversaries may abuse msiexec.exe to proxy execution of malicious payloads from remote locations.

Attacker's Goals

Evading security controls and executing arbitrary files from the web.

Investigative actions

- Is the URL that is encoded in the command line trusted.
- Is executed DLL or MSI file known as legitimate.
  Is the initiating process legitimate and the user running it knows of its use.
  Note - the MSI executable can run from other LAN locations, the alert will raise on the WAN connection.

Variations

Suspicious msiexec execution on an internet-facing endpoint

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)

ATT&CK Technique	System Binary Proxy Execution: Msiexec (T1218.007)
Severity	Low

Description

Suspicious msiexec execution of an arbitrary file from the web on an internet-facing server.

Attacker's Goals

Evading security controls and executing arbitrary files from the web.

Investigative actions

- Is the URL that is encoded in the command line trusted.
- Is executed DLL or MSI file known as legitimate.
- Is the initiating process legitimate and the user running it knows of its use.
Note - the MSI executable can run from other LAN locations, the alert will raise on the WAN connection.

30.104 | Uncommon net localgroup 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	
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Permission Groups Discovery (T1069)
Severity	Informational

Description

The 'net localgroup' command is used to add, display, or modify groups local to the host. Adversaries may attempt to use the command to find host groups and permissions settings or modify local group memberships.

Attacker's Goals

Attackers can attempt to use the command to find endpoint groups and permissions settings or modify local group memberships.

Investigative actions

Check if the queried group is a sensitive one (e.g. administrators).
Check whether the initiating process has executed additional discovery commands.

30.105 | Possible DCSync from a non 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
Detection Modules	
Detector Tags	Impacket Analytics
ATT&CK Tactic	- Credential Access (TA0006) - Defense Evasion (TA0005)
ATT&CK Technique	OS Credential Dumping: DCSync (T1003.006) - Rogue Domain Controller (T1207)
Severity	Low

Description

Attackers may pose a compromised host as a DC to replicate data to it (DCSync).

Attacker's Goals

An attacker is trying to retrieve Active Directory data, including password hashes.

Investigative actions

Check whether one of the machines is a new domain controller.

Variations

DCSync from a non domain controller from a non-standard process

Synopsis

ATT&CK Tactic	Credential Access (TA0006) Defense Evasion (TA0005)
ATT&CK Technique	OS Credential Dumping: DCSync (T1003.006) Rogue Domain Controller (T1207)
Severity	High

Description

Attackers may pose a compromised host as a DC to replicate data to it (DCSync).

Attacker's Goals

An attacker is trying to retrieve Active Directory data, including password hashes.

Investigative actions

Check whether one of the machines is a new domain controller.

Large DCSync from a non domain controller by AppID

Synopsis

ATT&CK Tactic	- Credential Access (TA0006) - Defense Evasion (TA0005)
ATT&CK Technique	- OS Credential Dumping: DCSync (T1003.006) - Rogue Domain Controller (T1207)
Severity	Medium

Description

Attackers may pose a compromised host as a DC to replicate data to it (DCSync).

Attacker's Goals

An attacker is trying to retrieve Active Directory data, including password hashes.

Investigative actions

Check whether one of the machines is a new domain controller.

Large DCSync from a non domain controller

Synopsis

ATT&CK Tactic	Credential Access (TA0006) Defense Evasion (TA0005)
ATT&CK Technique	OS Credential Dumping: DCSync (T1003.006) Rogue Domain Controller (T1207)
Severity	Medium

Description

Attackers may pose a compromised host as a DC to replicate data to it (DCSync).

Attacker's Goals

An attacker is trying to retrieve Active Directory data, including password hashes.

Investigative actions

Check whether one of the machines is a new domain controller.

Possible DCSync from an internet-facing server

Synopsis

ATT&CK Tactic	Credential Access (TA0006) Defense Evasion (TA0005)

ATT&CK Technique	▮ OS Credential Dumping: DCSync (T1003.006) Rogue Domain Controller (T1207)
Severity	Medium

Description

Attackers may pose a compromised host as a DC to replicate data to it (DCSync).

Attacker's Goals

An attacker is trying to retrieve Active Directory data, including password hashes.

Investigative actions

Check whether one of the machines is a new domain controller.

DCSync from a non domain controller

Synopsis

ATT&CK Tactic	▮ Credential Access (TA0006) Defense Evasion (TA0005)
ATT&CK Technique	▮ OS Credential Dumping: DCSync (T1003.006) Rogue Domain Controller (T1207)
Severity	Low

Description

Attackers may pose a compromised host as a DC to replicate data to it (DCSync).

Attacker's Goals

An attacker is trying to retrieve Active Directory data, including password hashes.

Investigative actions

Check whether one of the machines is a new domain controller.

30.106 | Uncommon local scheduled task creation via schtasks.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	Persistence (TA0003)
ATT&CK Technique	Scheduled Task/Job (T1053)
Severity	Low

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 gain persistence on this host using scheduled tasks.

Attacker's Goals

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

Investigative actions

- Review the process that creates the schedule task.
- Investigate the specific scheduled task execution chain.

30.107 | Abnormal Communication 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

An abnormal communication was seen from an internal entity to a rare domain.

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 Communication 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

An abnormal communication was seen from an internal entity to a rare domain.

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 Communication 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

An abnormal communication was seen from an internal entity to a rare domain.

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 Communication 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	Informational

Description

An abnormal communication was seen from an internal entity to a rare domain.

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.

30.108 | Uncommon DLL-sideloading from a logical CD-ROM (ISO) device

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	DLL Hijacking Analytics
ATT&CK Tactic	Execution (TA0002) Defense Evasion (TA0005) Privilege Escalation (TA0004)
ATT&CK Technique	Hijack Execution Flow: DLL Side-Loading (T1574.002) User Execution: Malicious File (T1204.002)
Severity	Medium

Description

A DLL was loaded by an executable from the same folder on a logical CD-ROM device (ISO).

Attacker's Goals

An attacker is attempting to load untrusted code into trusted contexts to avoid detection or escalate privileges.

Investigative actions

Investigate the loaded module and verify if it is malicious.
Check if the disk is a mounted CD-ROM (for example from an ISO file), and if it contains hidden files and folders.

- Check the content of an 'autorun.inf' or '
- .lnk' files if exists.

30.109 | Execution of an uncommon process at an early startup

stage

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	Generic Persistence Analytics
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Boot or Logon Autostart Execution (T1547)
Severity	Informational

Description

Uncommon execution of an executable found in an early startup stage.

Attacker's Goals

Adversaries continuously find and develop new undetectable, novel methods of launching malware during startup.

- Attackers aim to get persistence to continue operating even after a reboot.

Investigative actions

Check if the CGO (causality group owner) is familiar and if one of it configuration/parameters/registry keys has been modified.

Variations

Execution of an uncommon process at an early startup stage with suspicious characteristics

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Boot or Logon Autostart Execution (T1547)
Severity	Medium

Description

Uncommon execution of an executable found in an early startup stage.

Attacker's Goals

Adversaries continuously find and develop new undetectable, novel methods of launching malware during startup.

- Attackers aim to get persistence to continue operating even after a reboot.

Investigative actions

Check if the CGO (causality group owner) is familiar and if one of it configuration/parameters/registry keys has been modified.

Execution of an uncommon process at an early startup stage with uncommon characteristics

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Boot or Logon Autostart Execution (T1547)
Severity	Low

Description

Uncommon execution of an executable found in an early startup stage.

Attacker's Goals

- Adversaries continuously find and develop new undetectable, novel methods of launching malware during startup.
  Attackers aim to get persistence to continue operating even after a reboot.

Investigative actions

Check if the CGO (causality group owner) is familiar and if one of it

configuration/parameters/registry keys has been modified.

30.110 | Remote code execution into Kubernetes Pod

Synopsis

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

Deduplication Period	5 Days
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	Kubernetes - AGENT
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Container Administration Command (T1609)
Severity	Informational

Description

A container administration service was used to execute commands within a Kubernetes Pod.

Attacker's Goals

Attackers may use the container administration commands to execute commands within a Kubernetes Pod.

Investigative actions

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

Variations

Remote code execution into Kubernetes Pod from another Pod for the first time

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Container Administration Command (T1609)
Severity	Medium

Description

A container administration service was used to execute commands within a Kubernetes Pod.

Attacker's Goals

Attackers may use the container administration commands to execute commands within a Kubernetes Pod.

Investigative actions

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

Remote code execution into Kubernetes Pod from another Pod

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Container Administration Command (T1609)
Severity	Low

Description

A container administration service was used to execute commands within a Kubernetes Pod.

Attacker's Goals

Attackers may use the container administration commands to execute commands within a Kubernetes Pod.

Investigative actions

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

Remote code execution into Kubernetes Pod for the first time

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Container Administration Command (T1609)
Severity	Low

Description

A container administration service was used to execute commands within a Kubernetes Pod.

Attacker's Goals

Attackers may use the container administration commands to execute commands within a Kubernetes Pod.

Investigative actions

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

30.111 | A Torrent client 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 OR - Third-Party Firewalls
Detection Modules	
Detector Tags	
ATT&CK Tactic	- Exfiltration (TA0010) - Initial Access (TA0001)
ATT&CK Technique	Exfiltration Over Alternative Protocol (T1048) - Phishing (T1566)
Severity	Informational

Description

The host produced traffic consistent with the BitTorrent protocol.
Torrents may expose your organization to new malware or allow attackers/ malicious insiders to exfiltrate data.

Attacker's Goals

Exfiltrate data or as a phishing entry point.

Investigative actions

- Check the host for torrent client software.
- Look at the download's folder for foreign files or Torrent files.
- Examine the client's network traffic for uploaded or downloaded file hashes.

Variations

A Torrent client was detected on a host

Synopsis

ATT&CK Tactic	Exfiltration (TA0010) Initial Access (TA0001)
ATT&CK Technique	Exfiltration Over Alternative Protocol (T1048) Phishing (T1566)
Severity	Informational

Description

The host produced traffic consistent with the BitTorrent protocol.
Torrents may expose your organization to new malware or allow attackers/ malicious insiders to exfiltrate data.

Attacker's Goals

Exfiltrate data or as a phishing entry point.

Investigative actions

- Check the host for torrent client software.
- Look at the download's folder for foreign files or Torrent files.
  Examine the client's network traffic for uploaded or downloaded file hashes.

30.112 | Possible compromised 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	
Detector Tags	
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	User Execution (T1204)
Severity	Medium

Description

A Kerberos TGT for machine account has been used and does not match the hostname.

Attacker's Goals

Gain a special user Kerberos ticket to move laterally.

Investigative actions

- Check the source host for possible credential dumping.
  Check the delegated account credentials and if it has high privileges.
  Check the ticket destination to verify whether it is a sensitive asset.

30.113 | Possible new DHCP server

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	Adversary-in-the-Middle (T1557)
Severity	Medium

Description

A DHCP response was sent from an unknown DHCP server.
Attackers may send a DHCP response to a host in his LAN to inject a DNS server, route or WPAD server.

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 if the source agent is a legitimate DHCP server.
- Check if the attacked host send DNS queries to an unusual IP.
- Check if the attacked host send WPAD HTTP/S requests to an unusual host.

30.114 | RDP Connection to localhost

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	Medium

Description

RDP connection to localhost can be used for privilege escalation by leveraging Windows Accessibility Features.

Attacker's Goals

An attacker may initiate RDP tunneling for a more convenient and stable interface.

Investigative actions

Identify the process/user performing RDP and check that it is authorized.

Check whether the initiating process also connects to an external host.

30.115 | SMB Traffic from Non-Standard 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	Discovery (TA0007)
ATT&CK Technique	Network Service Discovery (T1046)
Severity	Low

Description

SMB traffic is usually performed by a standard set of privileged processes through designated ports.
The endpoint had a non-standard process communicating over ports normally used by SMB.

An attacker might be moving laterally by using tools that implement a custom version of the SMB protocol.

Attacker's Goals

using a custom protocol implementation that offers malicious functionality

- Using the well-known SMB port with a different protocol to evade detection.

Either way, the attacker's goal is to gain access to another endpoint on your network.
The attacker could also be surveying your network by performing service scans over the well-known SMB or Kerberos ports.

Investigative actions

Make sure the process is not a scanner that implements its version of the protocol, and that the scanner use is for sanctioned purposes. For example, nmap enumerating SMB.

- Make sure the process is not a sanctioned security product that creates standalone binaries for its use. For example, Illusive Network honeypots.

Investigate the process to see if the high-level language used to implement the application is the source of the alert. Some high-level programming languages provide their protocol implementations. For example, Java uses its Kerberos implementation.

- Examine the endpoint to see if it is infected with malware. If the parent-child chain of initiating processes has been infiltrated with a malicious replacement, then that replacement could be known malware.

Variations

SMB Traffic from Non-Standard Process on a sensitive server

Synopsis

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

Description

SMB traffic is usually performed by a standard set of privileged processes through designated

ports.
The endpoint had a non-standard process communicating over ports normally used by SMB.
An attacker might be moving laterally by using tools that implement a custom version of the SMB protocol.

Attacker's Goals

- using a custom protocol implementation that offers malicious functionality
- Using the well-known SMB port with a different protocol to evade detection.
  Either way, the attacker's goal is to gain access to another endpoint on your network.
  The attacker could also be surveying your network by performing service scans over the

  well-known SMB or Kerberos ports.

Investigative actions

- Make sure the process is not a scanner that implements its version of the protocol, and that the scanner use is for sanctioned purposes. For example, nmap enumerating SMB.
  Make sure the process is not a sanctioned security product that creates standalone binaries for its use. For example, Illusive Network honeypots.

  Investigate the process to see if the high-level language used to implement the application is the source of the alert. Some high-level programming languages provide their protocol implementations. For example, Java uses its Kerberos implementation.
  Examine the endpoint to see if it is infected with malware. If the parent-child chain of

  initiating processes has been infiltrated with a malicious replacement, then that replacement could be known malware.

30.116 | Possible Pass-the-Hash

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	Lateral Movement (TA0008)
ATT&CK Technique	Use Alternate Authentication Material: Pass the Hash (T1550.002)
Severity	Low

Description

An account was successfully logged on to with new credentials. This login type is rare and may be an attacker's attempt to pass-the-hash and move laterally within a network.

Attacker's Goals

An attacker is attempting to steal credentials and move laterally within a network.

Investigative actions

- Audit all login events and review for discrepancies.
- Look for LSASS process access, an indication of an attacker attempting to obtain password hashes.
  Check for the RunAs command with the /netonly option.

30.117 | Office process creates a scheduled task via file 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	
Detector Tags	
ATT&CK Tactic	Execution (TA0002) Persistence (TA0003)
ATT&CK Technique	Scheduled Task/Job (T1053)
Severity	Medium

Description

A Microsoft Office process created a scheduled task via file access. Attackers may create scheduled tasks for execution and to establish persistence.

Attacker's Goals

An attacker may gain persistence and execute malicious tools via scheduled tasks.

Investigative actions

Check the created task file and look for the action triggered by the task.

30.118 | LOLBAS executable injects into another 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	Defense Evasion (TA0005)
ATT&CK Technique	Process Injection (T1055)
Severity	Informational

Description

A signed binary, which can be abused to run code, injected code to another process.

Attacker's Goals

Gain code execution on the host and evade security controls.

Investigative actions

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

Variations

LOLBAS executable injects into another process using process hollowing

Synopsis

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

Description

A signed binary, which can be abused to run code, injected code to another process.

Attacker's Goals

Gain code execution on the host and evade security controls.

Investigative actions

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

Scripting engine injects into another process

Synopsis

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

Severity	Informational

Description

A signed binary, which can be abused to run code, injected code to another process.

Attacker's Goals

Gain code execution on the host and evade security controls.

Investigative actions

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

LOLBAS executable that's used to host DLLs injects into another process

Synopsis

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

Description

A signed binary, which can be abused to run code, injected code to another process.

Attacker's Goals

Gain code execution on the host and evade security controls.

Investigative actions

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

LOLBAS executable that's used to host DLLs injects into another process

Synopsis

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

Description

A signed binary, which can be abused to run code, injected code to another process.

Attacker's Goals

Gain code execution on the host and evade security controls.

Investigative actions

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

Rare LOLBAS executable injects into another process

Synopsis

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

Description

A signed binary, which can be abused to run code, injected code to another process.

Attacker's Goals

Gain code execution on the host and evade security controls.

Investigative actions

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

30.119 | Interactive at.exe privilege escalation method

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) Privilege Escalation (TA0004)
ATT&CK Technique	Scheduled Task/Job (T1053) Scheduled Task/Job: At (T1053.002)
Severity	Medium

Description

Detects an interactive AT scheduled task, which may be used as a form of privilege escalation.

Attacker's Goals

Attackers may attempt to use the command to gain persistence on the endpoint using recurring tasks.

Investigative actions

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

30.120 | The Linux system firewall was disabled

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	10 Minutes
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Impair Defenses: Disable or Modify System Firewall (T1562.004)
Severity	Low

Description

The system firewall was disabled.

Attacker's Goals

Exfiltrate data or move laterally in the organization.

Investigative actions

- Examine the command to understand which ip or port were affected. Check the communication allowed by the created firewall rule.

30.121 | Rare NTLM Access By User To 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	Identity Analytics
Detector Tags	
ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Use Alternate Authentication Material (T1550)
Severity	Informational

Description

An unusual NTLM authentication attempt by a user to host
This may be indicative of using stolen credentials or access tokens to access restricted hosts.

Attacker's Goals

The attacker is attempting to move laterally within a compromised network.

Investigative actions

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

30.122 | Suspicious SMB connection from domain controller

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	7 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	Lateral Movement (TA0008)
ATT&CK Technique	Use Alternate Authentication Material: Pass the Hash (T1550.002)
Severity	Low

Description

A domain controller has initiated an SMB connection to another host. The domain controllers usually communicate over SMB only with other domain controllers. An attacker can abuse such sessions for relay attacks.

Attacker's Goals

An attacker is attempting to steal credentials and move laterally within a network.

Investigative actions

- Check if the destination is domain controller, if it is, exclude it.
- Look for earlier connections to the DC which may cause it to initiate the session.

30.123 | Suspicious certutil command line

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) Defense Evasion (TA0005)

ATT&CK Technique	- System Binary Proxy Execution (T1218) - Ingress Tool Transfer (T1105)
Severity	Medium

Description

An attacker may use certutil to download malware.

Attacker's Goals

An attacker may use certutil to download malware.

Investigative actions

- Check whether the URL is benign, and if this was a desired behavior as part of its normal execution flow.
- Check whether the downloaded file is malicious.

30.124 | AppleScript process executed with a rare command line

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	AppleScript Analytics
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Command and Scripting Interpreter: AppleScript (T1059.002)
Severity	Informational

Description

The AppleScript interpreter process was executed with an uncommon command line.

Attacker's Goals

Perform various actions via AppleScript code, such as establishing persistence, evading detection, executing secondary payloads or injecting remote processes.

Investigative actions

- Analyze the command line and determine whether it performs any malicious/suspicious actions.
  Check the events generated by the process or its children for potential malicious behavior.
  Check whether the process was executed in an unusual way.

Variations

AppleScript process executed with a rare command line, possibly using Finder to perform operations

Synopsis

ATT&CK Tactic	Execution (TA0002)

ATT&CK Technique	Command and Scripting Interpreter: AppleScript (T1059.002)
Severity	High

Description

The AppleScript interpreter process was executed with an uncommon command line.

Attacker's Goals

Perform various actions via AppleScript code, such as establishing persistence, evading detection, executing secondary payloads or injecting remote processes.

Investigative actions

- Analyze the command line and determine whether it performs any malicious/suspicious actions.
  Check the events generated by the process or its children for potential malicious behavior.
  Check whether the process was executed in an unusual way.

AppleScript process executed with a rare command line with an unusual password prompt

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Command and Scripting Interpreter: AppleScript (T1059.002)
Severity	Low

Description

The AppleScript interpreter process was executed with an uncommon command line.

Attacker's Goals

Perform various actions via AppleScript code, such as establishing persistence, evading detection, executing secondary payloads or injecting remote processes.

Investigative actions

- Analyze the command line and determine whether it performs any malicious/suspicious actions.
Check the events generated by the process or its children for potential malicious behavior.
Check whether the process was executed in an unusual way.

AppleScript process executed with a rare command line, possibly injecting JavaScript into a browser

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Command and Scripting Interpreter: AppleScript (T1059.002)
Severity	Low

Description

The AppleScript interpreter process was executed with an uncommon command line.

Attacker's Goals

Perform various actions via AppleScript code, such as establishing persistence, evading detection, executing secondary payloads or injecting remote processes.

Investigative actions

Analyze the command line and determine whether it performs any malicious/suspicious actions.
- Check the events generated by the process or its children for potential malicious behavior.
Check whether the process was executed in an unusual way.

AppleScript process executed with a rare command line, possibly establishing persistence

Synopsis

ATT&CK Tactic	Execution (TA0002)

ATT&CK Technique	Command and Scripting Interpreter: AppleScript (T1059.002)
Severity	Low

Description

The AppleScript interpreter process was executed with an uncommon command line.

Attacker's Goals

Perform various actions via AppleScript code, such as establishing persistence, evading detection, executing secondary payloads or injecting remote processes.

Investigative actions

- Analyze the command line and determine whether it performs any malicious/suspicious actions.
  Check the events generated by the process or its children for potential malicious behavior.
  Check whether the process was executed in an unusual way.

AppleScript process executed with a rare command line, possibly installing a proxy

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Command and Scripting Interpreter: AppleScript (T1059.002)
Severity	Low

Description

The AppleScript interpreter process was executed with an uncommon command line.

Attacker's Goals

Perform various actions via AppleScript code, such as establishing persistence, evading detection, executing secondary payloads or injecting remote processes.

Investigative actions

- Analyze the command line and determine whether it performs any malicious/suspicious actions.
  Check the events generated by the process or its children for potential malicious behavior.

  Check whether the process was executed in an unusual way.

AppleScript process executed with a rare command line performing clipboard access

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Command and Scripting Interpreter: AppleScript (T1059.002)
Severity	Low

Description

The AppleScript interpreter process was executed with an uncommon command line.

Attacker's Goals

Perform various actions via AppleScript code, such as establishing persistence, evading detection, executing secondary payloads or injecting remote processes.

Investigative actions

Analyze the command line and determine whether it performs any malicious/suspicious

actions.

- Check the events generated by the process or its children for potential malicious behavior.
- Check whether the process was executed in an unusual way.

30.125 | Vulnerable driver loaded

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	
ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Exploitation for Privilege Escalation (T1068)
Severity	Medium

Description

A new and uncommon driver that is vulnerable was loaded.
Attackers may install a legitimate kernel driver and exploit its vulnerability to gain kernel access.

Attacker's Goals

Gain code execution on the host kernel.

Investigative actions

- Check whether the driver was installed by IT / User.
- Check if the host has the device of the driver - driver for Lenovo and the PC host brand is Asus.
- Check driver file creation time and if in that time legitimate operations occur.

30.126 | Kerberos Traffic from Non-Standard 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	Discovery (TA0007)
ATT&CK Technique	Network Service Discovery (T1046)
Severity	Medium

Description

The endpoint had a non-standard process communicating over ports normally used by Kerberos. An attacker might be using malicious tools to move laterally.

Attacker's Goals

- using a custom protocol implementation that offers malicious functionality
  Using the well-known Kerberos port with a different protocol to evade detection.
  Either way, the attacker's goal is to gain access to another endpoint on your network.

  The attacker could also be surveying your network by performing service scans over the well-known SMB or Kerberos ports.

Investigative actions

- Make sure the process is not a scanner that implements its version of the protocol, and that the scanner use is for sanctioned purposes. For example, nmap enumerating SMB.
  Make sure the process is not a sanctioned security product that creates standalone binaries

  for its use. For example, Illusive Network honeypots.
- Investigate the process to see if the high-level language used to implement the application is the source of the alert. Some high-level programming languages provide their protocol implementations. For example, Java uses its Kerberos implementation.
  Examine the endpoint to see if it is infected with malware. If the parent-child chain of

  initiating processes has been infiltrated with a malicious replacement, then that replacement could be known malware.
- Check if this process was running on other endpoints as well.

Variations

Rare Kerberos Traffic from a Process

Synopsis

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

Description

The endpoint had a non-standard process communicating over ports normally used by Kerberos. An attacker might be using malicious tools to move laterally.

Attacker's Goals

using a custom protocol implementation that offers malicious functionality
Using the well-known Kerberos port with a different protocol to evade detection.

Either way, the attacker's goal is to gain access to another endpoint on your network.
The attacker could also be surveying your network by performing service scans over the well-known SMB or Kerberos ports.

Investigative actions

Make sure the process is not a scanner that implements its version of the protocol, and that the scanner use is for sanctioned purposes. For example, nmap enumerating SMB.
Make sure the process is not a sanctioned security product that creates standalone binaries for its use. For example, Illusive Network honeypots.
Investigate the process to see if the high-level language used to implement the application is the source of the alert. Some high-level programming languages provide their protocol implementations. For example, Java uses its Kerberos implementation.

Examine the endpoint to see if it is infected with malware. If the parent-child chain of initiating processes has been infiltrated with a malicious replacement, then that replacement could be known malware.
Check if this process was running on other endpoints as well.

30.127 | Linux network share discovery

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)
ATT&CK Technique	Network Share Discovery (T1135)
Severity	Informational

Description

An adversary might use known tools to discover SMB shares within the compromised network.

Attacker's Goals

Exfiltrate or hide sensitive data.

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.

30.128 | Attempt to execute a command on a remote host using PsExec.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	Malicious Service Analytics
ATT&CK Tactic	Lateral Movement (TA0008) Execution (TA0002)
ATT&CK Technique	Remote Services: SMB/Windows Admin Shares (T1021.002) System Services: Service Execution (T1569.002)
Severity	Low

Description

There was an attempt to run a command on a remote host using PsExec.exe.

Attacker's Goals

Execute commands and run processes remotely.

Investigative actions

Confirm that the connection is benign and occurred as a part of normal behavior.

Variations

Attempt to execute a command on a remote host using PsExec.exe

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008) Execution (TA0002)
ATT&CK Technique	Remote Services: SMB/Windows Admin Shares (T1021.002) System Services: Service Execution (T1569.002)
Severity	Low

Description

There was an attempt to run a command on a remote host using PsExec.exe., the connection to the remote host was successful.

Attacker's Goals

Execute commands and run processes remotely.

Investigative actions

Confirm that the connection is benign and occurred as a part of normal behavior.

30.129 | Possible path traversal via HTTP request

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	N/A (single event)
Deduplication Period	2 Days
Required Data	Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	File and Directory Discovery (T1083)
Severity	Low

Description

The endpoint received a suspicious URI via an HTTP request that resembles a path traversal attempt.

Attacker's Goals

Attackers may exploit server components or misconfigurations to access arbitrary sensitive files on the web server.

Investigative actions

- Inspect the legitimacy of the URI path.
- Ensure that the rare URI is not a legitimate result of routine development actions on the web server.

Variations

Possible sensitive path traversal via HTTP request

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	File and Directory Discovery (T1083)
Severity	Medium

Description

The endpoint received a suspicious URI via an HTTP request that resembles a path traversal attempt.

Attacker's Goals

- Attackers may exploit server components or misconfigurations to access arbitrary sensitive files on the web server.

Investigative actions

Inspect the legitimacy of the URI path.

Ensure that the rare URI is not a legitimate result of routine development actions on the web server.

Possible path traversal via HTTP request from a TOR exit node

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	File and Directory Discovery (T1083)
Severity	Medium

Description

The endpoint received a suspicious URI via an HTTP request that resembles a path traversal attempt.

Attacker's Goals

Attackers may exploit server components or misconfigurations to access arbitrary sensitive files on the web server.

Investigative actions

Inspect the legitimacy of the URI path.

- Ensure that the rare URI is not a legitimate result of routine development actions on the web server.

Possible credential path traversal via HTTP request

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	File and Directory Discovery (T1083)
Severity	Medium

Description

The endpoint received a suspicious URI via an HTTP request that resembles a path traversal attempt.

Attacker's Goals

- Attackers may exploit server components or misconfigurations to access arbitrary sensitive files on the web server.

Investigative actions

Inspect the legitimacy of the URI path.
Ensure that the rare URI is not a legitimate result of routine development actions on the web server.

30.130 | Rare Scheduled Task RPC activity

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 Lateral Movement Analytics
ATT&CK Tactic	Lateral Movement (TA0008) Persistence (TA0003)
ATT&CK Technique	Remote Services (T1021) Scheduled Task/Job (T1053)
Severity	Informational

Description

The endpoint performed abnormal Scheduled Task 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 scheduled tasks.
- The ITaskSchedulerService RPC interface is used to query and manage services on a local or a remote host.

Investigative actions

- Review the action of the created scheduled task 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 remote task registration and creation via Scheduled Task RPC interface

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008) Persistence (TA0003)
ATT&CK Technique	Remote Services (T1021) Scheduled Task/Job (T1053)
Severity	Medium

Description

The endpoint performed abnormal task registration and creation via Scheduled Task RPC interface 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 scheduled tasks.
- The ITaskSchedulerService RPC interface is used to query and manage services on a local or a remote host.

Investigative actions

Review the action of the created scheduled task 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.

Rare remote task creation via Scheduled Task RPC interface

Synopsis

ATT&CK Tactic	- Lateral Movement (TA0008) Persistence (TA0003)
ATT&CK Technique	- Remote Services (T1021) Scheduled Task/Job (T1053)
Severity	Medium

Description

The endpoint performed abnormal task registration or creation via Scheduled Task RPC interface 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 scheduled tasks.
  The ITaskSchedulerService RPC interface is used to query and manage services on a local or a remote host.

Investigative actions

- Review the action of the created scheduled task 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.

Rare Scheduled Task RPC activity

Synopsis

ATT&CK Tactic	- Lateral Movement (TA0008) - Persistence (TA0003)

ATT&CK Technique	- Remote Services (T1021) - Scheduled Task/Job (T1053)
Severity	Low

Description

The endpoint performed abnormal Scheduled Task 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 scheduled tasks.
The ITaskSchedulerService RPC interface is used to query and manage services on a local or a remote host.

Investigative actions

Review the action of the created scheduled task 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.

30.131 | Suspicious process execution in a privileged container

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) Privilege Escalation (TA0004)
ATT&CK Technique	Container Administration Command (T1609) Escape to Host (T1611)
Severity	Informational

Description

A process was executed in a privileged Kubernetes Pod for the first time in the past 30 days.

Attacker's Goals

Perform lateral movement to new hosts to expand the foothold within a network and gain higher privileges.

Investigative actions

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

Variations

Suspicious process execution in a new privileged container

Synopsis

ATT&CK Tactic	Execution (TA0002) Privilege Escalation (TA0004)
ATT&CK Technique	Container Administration Command (T1609) Escape to Host (T1611)
Severity	Informational

Description

A process was executed in a privileged Kubernetes Pod for the first time in the past 30 days.

Attacker's Goals

Perform lateral movement to new hosts to expand the foothold within a network and gain higher privileges.

Investigative actions

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

30.132 | Globally uncommon root-domain port combination 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 domain in a specific port 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 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 port combination 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 domain in a specific port 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 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 root-domain port combination 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 domain in a specific port 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 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 port combination 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 domain in a specific port 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 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 rare root-domain port combination 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 domain in a specific port 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 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.

30.133 | Modification of PAM

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) Defense Evasion (TA0005) Credential Access (TA0006)
ATT&CK Technique	Modify Authentication Process: Pluggable Authentication Modules (T1556.003)
Severity	Informational

Description

Modification of PAM configuration files.

Attacker's Goals

Credential access, defense evasion or persistence.

Investigative actions

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

Variations

Modification of PAM from a Kubernetes pod

Synopsis

ATT&CK Tactic	Persistence (TA0003) Defense Evasion (TA0005) Credential Access (TA0006)
ATT&CK Technique	Modify Authentication Process: Pluggable Authentication Modules (T1556.003)
Severity	Informational

Description

Modification of PAM configuration files.

Attacker's Goals

Credential access, defense evasion or persistence.

Investigative actions

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

30.134 | Failed Login For a Long Username With Special Characters

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	Initial Access (TA0001)
ATT&CK Technique	Exploit Public-Facing Application (T1190)
Severity	Informational

Description

A long username containing special characters failed to log in to the domain.

Attacker's Goals

An attacker is trying to get code execution on internet-facing assets through command injection.

Investigative actions

Is the host running internet-facing services?
Are we looking at sanction vulnerability scanning?

30.135 | Execution of dllhost.exe with an empty command line

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 (T1218)
Severity	Low

Description

The process dllhost.exe was executed with an empty command line. This behavior is suspicious, and may be caused by a malicious actor using 'Image File Execution Options' in the registry to evade detection.

Attacker's Goals

Evade detection when running suspicious commands.

Investigative actions

- Check if an entry for dllhost.exe was added in the registry, under HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options.

Variations

Execution of unsigned dllhost from a non-typical path with empty command line

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Masquerading: Masquerade Task or Service (T1036.004)
Severity	High

Description

An unsigned process was executed with the name dllhost.exe from a non-typical path, this behavior is suspicious and maybe performed by a malicious actor in an attempt to hide their actions.

Attacker's Goals

Evade detection when performing suspicious actions.

Investigative actions

- Review actions performed by the executed process and the causality owner, and check if they are suspicious.

Globally uncommon execution of dllhost.exe with an empty command line

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	System Binary Proxy Execution (T1218)
Severity	Low

Description

The process dllhost.exe was executed with an empty command line. This behavior is suspicious, and may be caused by a malicious actor using 'Image File Execution Options' in the registry to evade detection.

Attacker's Goals

Evade detection when running suspicious commands.

Investigative actions

> Check if an entry for dllhost.exe was added in the registry, under
>
> HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options.

30.136 | Unusual SSH activity that resembles SSH proxy

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: - 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	Command and Control (TA0011)
ATT&CK Technique	Proxy: Internal Proxy (T1090.001)
Severity	Informational

Description

A host initiated and received an unusual SSH connection, which is consistent with being an SSH proxy.
This behavior may indicate an attempt to establish covert command and control communication or to exfiltrate data.

Attacker's Goals

Attackers aim to establish a covert command and control channel or relay communications through a compromised SSH connection.

Investigative actions

Review the SSH connections to identify any unusual proxy activity or traffic patterns. Investigate the user accounts involved in the SSH connections to determine if credentials were compromised. Additionally, examine logs for any unexpected data transfers or commands that may indicate malicious intent.

Variations

High Volume Unusual SSH activity that resembles SSH proxy

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Proxy: Internal Proxy (T1090.001)
Severity	Low

Description

A host initiated and received an unusual SSH connection, which is consistent with being an SSH proxy.
This behavior may indicate an attempt to establish covert command and control communication or to exfiltrate data.

Attacker's Goals

Attackers aim to establish a covert command and control channel or relay communications through a compromised SSH connection.

Investigative actions

Review the SSH connections to identify any unusual proxy activity or traffic patterns. Investigate the user accounts involved in the SSH connections to determine if credentials were compromised.

Additionally, examine logs for any unexpected data transfers or commands that may indicate malicious intent.

Suspicious SSH activity that resembles SSH proxy

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Proxy: Internal Proxy (T1090.001)
Severity	Low

Description

A host initiated and received an unusual SSH connection, which is consistent with being an SSH proxy.
This behavior may indicate an attempt to establish covert command and control communication or to exfiltrate data.

Attacker's Goals

Attackers aim to establish a covert command and control channel or relay communications through a compromised SSH connection.

Investigative actions

Review the SSH connections to identify any unusual proxy activity or traffic patterns. Investigate the user accounts involved in the SSH connections to determine if credentials were compromised.

Additionally, examine logs for any unexpected data transfers or commands that may indicate malicious intent.

Unusual SSH activity that resembles SSH proxy detected

Synopsis

ATT&CK Tactic	Command and Control (TA0011)

ATT&CK Technique	Proxy: Internal Proxy (T1090.001)
Severity	Low

Description

A host initiated and received an unusual SSH connection, which is consistent with being an SSH proxy.

This behavior may indicate an attempt to establish covert command and control communication or to exfiltrate data.

Attacker's Goals

Attackers aim to establish a covert command and control channel or relay communications through a compromised SSH connection.

Investigative actions

Review the SSH connections to identify any unusual proxy activity or traffic patterns. Investigate the user accounts involved in the SSH connections to determine if credentials were compromised. Additionally, examine logs for any unexpected data transfers or commands that may indicate malicious intent.

30.137 | Possible Email collection using Outlook RPC

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	Collection (TA0009)
ATT&CK Technique	Email Collection: Local Email Collection (T1114.001)
Severity	Informational

Description

Outlook was executed using RPC by an uncommon parent process, this may be an indication of email collection activities.

Attacker's Goals

An attacker is trying to perform email collection or manipulation using Outlook.

Investigative actions

Investigate the endpoint to determine if it's a legitimate process that is supposed to use Outlook in its operation to send or extract emails.

30.138 | File transfer from unusual IP using known tools

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	Command and Control (TA0011)
ATT&CK Technique	Ingress Tool Transfer (T1105)
Severity	Informational

Description

An adversary might use known tools to transfer tools/payloads into the compromised machine.

Attacker's Goals

Expand attack vectors and compromise the rest of the network.

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

File transfer from unusual IP using known tools in a Kubernetes pod

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Ingress Tool Transfer (T1105)
Severity	Low

Description

An adversary might use known tools to transfer tools/payloads into the compromised machine.

Attacker's Goals

Expand attack vectors and compromise the rest of the network.

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.

30.139 | Ping to localhost from an uncommon, unsigned parent 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	Defense Evasion (TA0005)
ATT&CK Technique	Virtualization/Sandbox Evasion (T1497)
Severity	Informational

Description

Ping is often used by malware and attackers to delay the execution of suspicious commands in sandbox environments.

Attacker's Goals

Use ping as an easy way to wait to try and evade detection between executions.

Investigative actions

Validate if the executing process is malicious.

30.140 | Possible DLL Side-Loading

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	DLL Hijacking Analytics
ATT&CK Tactic	- Persistence (TA0003) Privilege Escalation (TA0004) Defense Evasion (TA0005)
ATT&CK Technique	Hijack Execution Flow: DLL Side-Loading (T1574.002)
Severity	Informational

Description

An attacker might abuse the Windows DLL search order by planting in the same folder a signed binary that will load the attacker's malicious module.

Attacker's Goals

An attacker is attempting to load an untrusted module into a trusted context to avoid detection, gain persistence or to perform privilege escalation.

Investigative actions

- Investigate the loaded module to verify if it is malicious.
  Investigate if the loading process and the loaded module reside in legitimate locations.

Variations

Possible DLL Side-Loading of a module with highly suspicious characteristics

Synopsis

ATT&CK Tactic	Persistence (TA0003) Privilege Escalation (TA0004) Defense Evasion (TA0005)
ATT&CK Technique	Hijack Execution Flow: DLL Side-Loading (T1574.002)
Severity	Medium

Description

An attacker might abuse the Windows DLL search order by planting in the same folder a signed binary that will load the attacker's malicious module.

Attacker's Goals

An attacker is attempting to load an untrusted module into a trusted context to avoid detection, gain persistence or to perform privilege escalation.

Investigative actions

Investigate the loaded module to verify if it is malicious.

Investigate if the loading process and the loaded module reside in legitimate locations.

Globally Uncommon DLL Side-Loading

Synopsis

ATT&CK Tactic	Persistence (TA0003) Privilege Escalation (TA0004) - Defense Evasion (TA0005)
ATT&CK Technique	Hijack Execution Flow: DLL Side-Loading (T1574.002)
Severity	Low

Description

An attacker might abuse the Windows DLL search order by planting in the same folder a signed binary that will load the attacker's malicious module.

Attacker's Goals

An attacker is attempting to load an untrusted module into a trusted context to avoid detection,

gain persistence or to perform privilege escalation.

Investigative actions

- Investigate the loaded module to verify if it is malicious.
- Investigate if the loading process and the loaded module reside in legitimate locations.

Possible DLL Side-Loading of a module with suspicious characteristics

Synopsis

ATT&CK Tactic	Persistence (TA0003) Privilege Escalation (TA0004) - Defense Evasion (TA0005)
ATT&CK Technique	Hijack Execution Flow: DLL Side-Loading (T1574.002)
Severity	Low

Description

An attacker might abuse the Windows DLL search order by planting in the same folder a signed binary that will load the attacker's malicious module.

Attacker's Goals

An attacker is attempting to load an untrusted module into a trusted context to avoid detection, gain persistence or to perform privilege escalation.

Investigative actions

- Investigate the loaded module to verify if it is malicious.
- Investigate if the loading process and the loaded module reside in legitimate locations.

Possible DLL Side-Loading by a known actor in the organization

Synopsis

ATT&CK Tactic	- Persistence (TA0003) Privilege Escalation (TA0004) Defense Evasion (TA0005)
ATT&CK Technique	Hijack Execution Flow: DLL Side-Loading (T1574.002)
Severity	Low

Description

An attacker might abuse the Windows DLL search order by planting in the same folder a signed binary that will load the attacker's malicious module.

Attacker's Goals

An attacker is attempting to load an untrusted module into a trusted context to avoid detection, gain persistence or to perform privilege escalation.

Investigative actions

Investigate the loaded module to verify if it is malicious.

Investigate if the loading process and the loaded module reside in legitimate locations.

30.141 | Rare AppID usage to a rare destination

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	14 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	Command and Control (TA0011)
ATT&CK Technique	Application Layer Protocol (T1071) Non-Standard Port (T1571)
Severity	Informational

Description

Rare AppID with port usage to rare destination.

Attacker's Goals

Attackers might use well-known ports with uncommon applications to avoid being detected by a non-application aware firewall, or to bypass firewall rules based only on ports.

Investigative actions

Investigate the endpoints participating in the session.

Variations

Rare AppID usage to a rare destination using an unsigned process

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Application Layer Protocol (T1071) ▮ Non-Standard Port (T1571)
Severity	Low

Description

Rare AppID with port usage to rare destination.

Attacker's Goals

Attackers might use well-known ports with uncommon applications to avoid being detected by a non-application aware firewall, or to bypass firewall rules based only on ports.

Investigative actions

Investigate the endpoints participating in the session.

Rare AppID usage to a rare destination from an internet-facing server

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	- Application Layer Protocol (T1071) Non-Standard Port (T1571)
Severity	Low

Description

Rare AppID with port usage to rare destination.

Attacker's Goals

Attackers might use well-known ports with uncommon applications to avoid being detected by a non-application aware firewall, or to bypass firewall rules based only on ports.

Investigative actions

Investigate the endpoints participating in the session.

30.142 | Rare SMTP/S Session

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	
ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Exfiltration Over Alternative Protocol (T1048)
Severity	Informational

Description

The Simple Mail Transfer Protocol (SMTP) and its SSL-secured variant SMTPS are used to send email. Attackers can use SMTP/S to exfiltrate data from your network.

Attacker's Goals

SMTP and its SSL-secured variant SMTPS are used to send email. Attackers can use SMTP/S to exfiltrate data from your network.

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.

30.143 | Possible Microsoft process masquerading

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	Masquerading: Match Legitimate Name or Location (T1036.005)
Severity	Medium

Description

An attacker might leverage Microsoft Windows well-known image names to run malicious processes without being caught.

Attacker's Goals

An attacker is attempting to masquerade as standard windows images by using a trusted name to execute malicious code.

Investigative actions

Investigate the executed process image and verify if it is malicious.

30.144 | Microsoft Office process spawns 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	- Execution (TA0002) - Initial Access (TA0001)

ATT&CK Technique	- User Execution (T1204) - Phishing: Spearphishing Attachment (T1566.001)
Severity	Low

Description

Microsoft Office process spawns a commonly abused process with an uncommon command.

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.

30.145 | Execution of renamed lolbin

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	Masquerading (T1036)
Severity	Low

Description

Lolbins can be renamed and run as a way to avoid detection.

Attacker's Goals

Command execution via lolbins and detection avoidance via file rename.

Investigative actions

Isolate the host and verify if the file is malicious or not.

Variations

Execution of process that never seen before on the host from renamed lolbin process

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Masquerading (T1036)
Severity	Medium

Description

Lolbins can be renamed and run as a way to avoid detection.

Attacker's Goals

Command execution via lolbins and detection avoidance via file rename.

Investigative actions

Isolate the host and verify if the file is malicious or not.

Execution of unpopular renamed lolbin process from suspicious folder

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Masquerading (T1036)
Severity	Medium

Description

Lolbins can be renamed and run as a way to avoid detection.

Attacker's Goals

Command execution via lolbins and detection avoidance via file rename.

Investigative actions

Isolate the host and verify if the file is malicious or not.

Execution of unpopular renamed lolbin process

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)

ATT&CK Technique	Masquerading (T1036)
Severity	Medium

Description

Lolbins can be renamed and run as a way to avoid detection.

Attacker's Goals

Command execution via lolbins and detection avoidance via file rename.

Investigative actions

Isolate the host and verify if the file is malicious or not.

30.146 | Possible Kerberoasting without SPNs

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	Credential Access (TA0006)
ATT&CK Technique	Steal or Forge Kerberos Tickets: Kerberoasting (T1558.003)
Severity	Low

Description

A user specifically requested weak and deprecated encryption in a Kerberos TGS request. This provides easy-to-crack hashes, and is typically a sign of a Kerberoasting attack.

The requested service was specified by using a suspicious SPN type, which is often used by Kerberoasting tools to request by SAN instead of SPN.

Attacker's Goals

Crack service account credentials by obtaining an easy-to-crack Kerberos ticket.

Investigative actions

Check who used the host at the time of the alert, to rule out a benign service or tool requesting weak Kerberos encryption.

Variations

Possible Kerberoasting without SPNs on a sensitive server

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Steal or Forge Kerberos Tickets: Kerberoasting (T1558.003)

Severity	Medium

Description

A user specifically requested weak and deprecated encryption in a Kerberos TGS request. This provides easy-to-crack hashes, and is typically a sign of a Kerberoasting attack.
The requested service was specified by using a suspicious SPN type, which is often used by Kerberoasting tools to request by SAN instead of SPN.

Attacker's Goals

Crack service account credentials by obtaining an easy-to-crack Kerberos ticket.

Investigative actions

Check who used the host at the time of the alert, to rule out a benign service or tool requesting weak Kerberos encryption.

30.147 | Remote command execution via wmic.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	Execution (TA0002)
ATT&CK Technique	Windows Management Instrumentation (T1047)
Severity	Low

Description

Remote command execution using the Windows Management Instrumentation command-line tool.

Attacker's Goals

The attacker is expanding his reach into your network by executing commands on a remote endpoint.

Investigative actions

- Examine Alert Details > Overview to identify the source endpoint, process running the command execution, process owner, and execution destination.

Variations

Remote command execution via wmic.exe

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Windows Management Instrumentation (T1047)
Severity	Medium

Description

Remote command execution using the Windows Management Instrumentation command-line tool.

Attacker's Goals

The attacker is expanding his reach into your network by executing commands on a remote endpoint.

Investigative actions

Examine Alert Details > Overview to identify the source endpoint, process running the command execution, process owner, and execution destination.

30.148 | Possible use of IPFS was detected

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	- Exfiltration (TA0010) - Initial Access (TA0001)
ATT&CK Technique	- Exfiltration Over Alternative Protocol (T1048) - Phishing (T1566)
Severity	Informational

Description

The host produced traffic consistent with IPFS.

Attacker's Goals

IPFS access may expose your organization to new malware or allow attackers/ malicious insiders to exfiltrate data.

Investigative actions

- Check the host for IPFS client software.
- Look at the user's website history for IPFS url's and check the content ID (CID) for malicious indicators.
- Examine the client's network traffic for uploaded or downloaded file hashes.

Variations

Possible use of IPFS was detected

Synopsis

ATT&CK Tactic	Exfiltration (TA0010) Initial Access (TA0001)
ATT&CK Technique	- Exfiltration Over Alternative Protocol (T1048) Phishing (T1566)
Severity	Informational

Description

The host produced traffic consistent with IPFS.

Attacker's Goals

IPFS access may expose your organization to new malware or allow attackers/ malicious insiders to exfiltrate data.

Investigative actions

- Check the host for IPFS client software.
- Look at the user's website history for IPFS url's and check the content ID (CID) for malicious indicators.
- Examine the client's network traffic for uploaded or downloaded file hashes.

30.149 | A user logged in from an abnormal country or ASN

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	- Credential Access (TA0006) - Resource Development (TA0042)
ATT&CK Technique	- Compromise Accounts (T1586) - Brute Force: Password Guessing (T1110.001)
Severity	Informational

Description

A user logged in from an unusual country or ASN. This may indicate that the account was compromised.

Attacker's Goals

Gain user-account credentials.

Investigative actions

Check if the user is currently located in the aforementioned country.
- Check for any other suspicious activity related to the account.
- Check other ASNs and Countries that the user logged in from.
Look for additional login attempts.

Variations

A service account successfully logged in from a new country or ASN

Synopsis

ATT&CK Tactic	Credential Access (TA0006) Resource Development (TA0042)
ATT&CK Technique	- Compromise Accounts (T1586) Brute Force: Password Guessing (T1110.001)
Severity	Low

Description

A service account successfully logged in to an internet facing server from an unusual country or ASN. This may indicate that the account was compromised.

Attacker's Goals

Gain user-account credentials.

Investigative actions

- Check if the user is currently located in the aforementioned country.
- Check for any other suspicious activity related to the account.
- Check other ASNs and Countries that the user logged in from.
- Look for additional login attempts.

30.150 | VM Detection attempt on Linux

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) - Discovery (TA0007)
ATT&CK Technique	Virtualization/Sandbox Evasion: System Checks (T1497.001)
Severity	Informational

Description

A Process executed a command and/or accessed a file 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 process for additional malicious actions.

Check for any additional alerts raised within the same context of the script.

Variations

VM Detection attempt on Linux with further reconnaissance commands

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005) - Discovery (TA0007) - Discovery (TA0007)
ATT&CK Technique	Virtualization/Sandbox Evasion: System Checks (T1497.001) - System Owner/User Discovery (T1033)
Severity	Medium

Description

A Process executed a command and/or accessed a file 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 process for additional malicious actions.
Check for any additional alerts raised within the same context of the script.

VM Detection attempt on Linux using an unpopular technique

Synopsis

ATT&CK Tactic	- Defense Evasion (TA0005) - Discovery (TA0007)
ATT&CK Technique	Virtualization/Sandbox Evasion: System Checks (T1497.001)
Severity	Low

Description

A Process executed a command and/or accessed a file 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 process for additional malicious actions.
- Check for any additional alerts raised within the same context of the script.

30.151 | Netcat makes or gets connections

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	Proxy: Multi-hop Proxy (T1090.003)
Severity	High

Description

Malicious actors can use Netcat for privilege escalation, remote code execution, data exfiltration and protocol tunneling to evade detection.

Attacker's Goals

Establish command and control channel.
- Propagate in the victim network.

Investigative actions

Verify that the usage of Netcat/Netcat64 is from an authorized personnel and that user has the right to access the remote host.

30.152 | Possible data obfuscation

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	Deobfuscate/Decode Files or Information (T1140)
Severity	Informational

Description

A command that can be used for file obfuscation was executed with an uncommon command line.

Attacker's Goals

Attackers may use obfuscated files to cover their tracks.

Investigative actions

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

Variations

Possible data obfuscation in a Kubernetes pod

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Deobfuscate/Decode Files or Information (T1140)
Severity	Low

Description

A command that can be used for file obfuscation was executed with an uncommon command line.

Attacker's Goals

Attackers may use obfuscated files to cover their tracks.

Investigative actions

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

30.153 | Unsigned process creates a scheduled task via file access

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

Description

A scheduled task was created via file access from an unsigned process. This is uncommon and may indicate malicious activity.

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

Unsigned process creates a scheduled task via file access on a sensitive server

Synopsis

ATT&CK Tactic	Execution (TA0002) Persistence (TA0003)
ATT&CK Technique	Scheduled Task/Job (T1053)
Severity	Medium

Description

A scheduled task was created via file access from an unsigned process. This is uncommon and may indicate malicious activity.

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.

30.154 | LDAP traffic from non-standard 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	Discovery (TA0007)
ATT&CK Technique	Account Discovery (T1087)
Severity	Informational

Description

LDAP traffic is usually performed by a standard set of processes.
The endpoint had a non-standard process communicating over ports normally used by LDAP.
This may be indicative of Active Directory domain enumeration, which may be used during attacks against the organization.

Attacker's Goals

An attacker is attempting to enumerate Active Directory.

Investigative actions

- Make sure the process is not a scanner that implements its version of the protocol, and that the scanner use is for sanctioned purposes. For example, nmap enumerating LDAP.
Make sure the process is not a sanctioned security product that creates standalone binaries for its use. For example, Illusive Network honeypots.
Investigate the process to see if the high-level language used to implement the application is the source of the alert. Some high-level programming languages provide their protocol implementations.
Examine the endpoint to see if it is infected with malware. If the parent-child chain of initiating processes has been infiltrated with a malicious replacement, then that replacement could be known malware.

Variations

LDAP traffic from reverse SSH tunnel

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Account Discovery (T1087)
Severity	Medium

Description

LDAP traffic is usually performed by a standard set of processes.
The endpoint had a non-standard process communicating over ports normally used by LDAP.
This may be indicative of Active Directory domain enumeration, which may be used during attacks against the organization.

Attacker's Goals

An attacker is attempting to enumerate Active Directory.

Investigative actions

- Make sure the process is not a scanner that implements its version of the protocol, and that the scanner use is for sanctioned purposes. For example, nmap enumerating LDAP.
  Make sure the process is not a sanctioned security product that creates standalone binaries for its use. For example, Illusive Network honeypots.

  Investigate the process to see if the high-level language used to implement the application is the source of the alert. Some high-level programming languages provide their protocol implementations.
  Examine the endpoint to see if it is infected with malware. If the parent-child chain of

  initiating processes has been infiltrated with a malicious replacement, then that replacement could be known malware.

30.155 | Rare Windows Remote Management (WinRM) HTTP Activity

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

Description

The endpoint performed unfamiliar WinRM HTTP activity to a remote host.

Attacker's Goals

- Attackers may use WinRM to execute code on remote hosts, in an attempt to gain persistence or move laterally in the network.

Investigative actions

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

30.156 | SUID/GUID permission discovery

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)
ATT&CK Technique	File and Directory Discovery (T1083)
Severity	Low

Description

Attackers may search for potential to elevate permissions using binaries that have the SUID or GUID bit enabled.

Attacker's Goals

Attackers may use GUID/SUID binaries to elevate privileges.

Investigative actions

Check whether additional malicious commands were executed from the same process.

Verify if the command-line seems suspicious or contains malicious indicators.

30.157 | A suspicious process enrolled for a certificate

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 (T1552) ▮ Steal or Forge Authentication Certificates (T1649)
Severity	Low

Description

A suspicious process enrolled for a certificate.

Attacker's Goals

Attackers may authenticate as users using a certificate.

- If a policy is configured with permissive options, the attacker can authenticate as a user with high privileges.

Investigative actions

See whether this was a legitimate action.
Follow process/user activities.

Check for suspicious certificate authentications.

Variations

An unsigned suspicious process enrolled for a certificate

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	- Unsecured Credentials (T1552) Steal or Forge Authentication Certificates (T1649)
Severity	Medium

Description

An unsigned suspicious process enrolled for a certificate.

Attacker's Goals

- Attackers may authenticate as users using a certificate.
If a policy is configured with permissive options, the attacker can authenticate as a user with high privileges.

Investigative actions

See whether this was a legitimate action.

- Follow process/user activities.
- Check for suspicious certificate authentications.

30.158 | Unusual Azure AD sync 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	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	OS Credential Dumping (T1003)
Severity	Low

Description

A process that does not usually load the Azure AD Sync mcrypt.dll loaded the module.

Attacker's Goals

Attackers can abuse the Azure AD Connect database files to get access to the AD Sync account.

- The AD Sync account is a highly privileged account that can perform a DCSync and get access to on-premise password hashes.

Investigative actions

See whether this was a legitimate action.

Follow process/user/host activities.

- Follow unusual actions of the AD Sync user.
- Check for unusual Azure AD authentications.

Check for a possible DCSync.

Variations

Unusual Azure AD sync module load by suspicious process

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	OS Credential Dumping (T1003)
Severity	Medium

Description

A suspicious process that does not usually load the Azure AD Sync mcrypt.dll loaded the module.

Attacker's Goals

Attackers can abuse the Azure AD Connect database files to get access to the AD Sync account.

- The AD Sync account is a highly privileged account that can perform a DCSync and get access to on-premise password hashes.

Investigative actions

See whether this was a legitimate action.

- Follow process/user/host activities.
- Follow unusual actions of the AD Sync user.

Check for unusual Azure AD authentications.

Check for a possible DCSync.

30.159 | Reverse SSH tunnel to external domain/ip

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	12 Hours
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Protocol Tunneling (T1572)
Severity	Medium

Description

A reverse SSH tunnel might have been created.

Attacker's Goals

Attackers may use SSH to create an encrypted tunnel to allow an attacker to covertly connect to an internal host.

Investigative actions

Review the external ip/domain.
Investigate the causality of the process.

30.160 | Injection into rundll32.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	Injection Analytics

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

Description

A process injected into an instance of rundll32.exe.

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.

30.161 | Uncommon ARP cache listing via arp.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 arp.exe command is used to display and modify entries in the Address Resolution Protocol (ARP) cache. Adversaries may attempt to use the command to discover remote systems they could compromise.

Attacker's Goals

Adversaries may attempt to use the command to discover remote systems they could compromise.

Investigative actions

Check whether the initiating process is allowed in your organization. (If the parent process is cmd.exe, check the process that spawned it).

30.162 | Unusual DB process spawning 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	Initial Access (TA0001) Lateral Movement (TA0008)
ATT&CK Technique	Exploit Public-Facing Application (T1190) Exploitation of Remote Services (T1210)
Severity	Informational

Description

A DB related process abnormally spawned a shell. This might indicate an exploitation attempt.

Attacker's Goals

Obtain access to either the database or its hosting machine for various purposes like privilege escalation, lateral movement, and data theft.

Investigative actions

- Review the commands/processes executed by the shell for malicious actions.
  Check if and what else the DB process has executed.
  Check for any additional alerts raised in the context of the DB process.

  Audit the query/access logs of the DB for suspicious actions (Such as SQL injection or similar).

Variations

Unusual DB process spawning a shell with a possible reconnaissance command

Synopsis

ATT&CK Tactic	Initial Access (TA0001) Lateral Movement (TA0008)
ATT&CK Technique	Exploit Public-Facing Application (T1190) Exploitation of Remote Services (T1210)
Severity	Low

Description

A DB related process abnormally spawned a shell. This might indicate an exploitation attempt.

Attacker's Goals

Obtain access to either the database or its hosting machine for various purposes like privilege escalation, lateral movement, and data theft.

Investigative actions

Review the commands/processes executed by the shell for malicious actions.
- Check if and what else the DB process has executed.
- Check for any additional alerts raised in the context of the DB process.
Audit the query/access logs of the DB for suspicious actions (Such as SQL injection or similar).

Unusual DB process spawning a shell with a possible web download/access command

Synopsis

ATT&CK Tactic	Initial Access (TA0001) Lateral Movement (TA0008)
ATT&CK Technique	Exploit Public-Facing Application (T1190) Exploitation of Remote Services (T1210)
Severity	Low

Description

A DB related process abnormally spawned a shell. This might indicate an exploitation attempt.

Attacker's Goals

Obtain access to either the database or its hosting machine for various purposes like privilege escalation, lateral movement, and data theft.

Investigative actions

Review the commands/processes executed by the shell for malicious actions.
- Check if and what else the DB process has executed.
- Check for any additional alerts raised in the context of the DB process.
Audit the query/access logs of the DB for suspicious actions (Such as SQL injection or similar).

Unusual DB process spawning a shell with an unusual command line

Synopsis

ATT&CK Tactic	Initial Access (TA0001) Lateral Movement (TA0008)
ATT&CK Technique	Exploit Public-Facing Application (T1190) Exploitation of Remote Services (T1210)
Severity	Low

Description

A DB related process abnormally spawned a shell. This might indicate an exploitation attempt.

Attacker's Goals

Obtain access to either the database or its hosting machine for various purposes like privilege escalation, lateral movement, and data theft.

Investigative actions

Review the commands/processes executed by the shell for malicious actions.

- Check if and what else the DB process has executed.
- Check for any additional alerts raised in the context of the DB process.

Audit the query/access logs of the DB for suspicious actions (Such as SQL injection or similar).

30.163 | Unusual compressed file password protection

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	Collection (TA0009)
ATT&CK Technique	Archive Collected Data: Archive via Utility (T1560.001)
Severity	Low

Description

An adversary might compress sensitive files with password protection to bypass security mitigations when attempting to exfiltrate them.

Attacker's Goals

Exfiltrate or hide sensitive data.

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 compressed file password protection in a Kubernetes pod

Synopsis

ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Archive Collected Data: Archive via Utility (T1560.001)
Severity	Low

Description

An adversary might compress sensitive files with password protection to bypass security mitigations when attempting to exfiltrate them.

Attacker's Goals

Exfiltrate or hide sensitive data.

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.

30.164 | Linux process execution with a rare GitHub URL

Synopsis

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

Deduplication Period	3 Hours
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Command and Scripting Interpreter (T1059)
Severity	Informational

Description

A process was executed with an uncommon GitHub URL in its command line. This may have legitimate uses, but it might also be used by attackers to download malicious payloads.

Attacker's Goals

Download a second stage payload for execution.

Investigative actions

- Check if the initiator process is malicious.
- Check the user activity on the same agent at that time.
- Check if the host is a development server.
- Check if this installation was related to more installations at the same time.
- Check for additional file/network operations by the same process instance.

30.165 | New FTP Server

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	
ATT&CK Tactic	- Initial Access (TA0001) - Collection (TA0009)
ATT&CK Technique	Data from Information Repositories (T1213) - Valid Accounts (T1078)
Severity	Low

Description

A new FTP server has been detected.

Attacker's Goals

- Attackers may seek to access FTP resources to exfiltrate data, stage attack tools or create a command and control channel through a trusted service.

Investigative actions

Verify that the new service is legitimate.
Examine the legitimacy of the application that produced this uncommon FTP.

Examine the parent process of this application.

Variations

New FTP Server Accessed Via a Port Scan

Synopsis

ATT&CK Tactic	Initial Access (TA0001) Collection (TA0009)
ATT&CK Technique	Data from Information Repositories (T1213) Valid Accounts (T1078)
Severity	Informational

Description

A new FTP server has been detected.

Attacker's Goals

Attackers may seek to access FTP resources to exfiltrate data, stage attack tools or create a command and control channel through a trusted service.

Investigative actions

Verify that the new service is legitimate.

- Examine the legitimacy of the application that produced this uncommon FTP.
- Examine the parent process of this application.

New FTP Server from an external source

Synopsis

ATT&CK Tactic	- Initial Access (TA0001) Collection (TA0009)
ATT&CK Technique	- Data from Information Repositories (T1213) Valid Accounts (T1078)
Severity	Low

Description

A new FTP server has been detected.

Attacker's Goals

- Attackers may seek to access FTP resources to exfiltrate data, stage attack tools or create a command and control channel through a trusted service.

Investigative actions

Verify that the new service is legitimate.
Examine the legitimacy of the application that produced this uncommon FTP.

Examine the parent process of this application.

30.166 | Windows LOLBIN executable 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	Medium

Description

Scripts connecting to external IP addresses may be sanctioned IT scripts. However, when those external IP addresses are only receiving connections from a few specific endpoints in the organization, these scripts may be an indicator of more suspicious activity. Security testers and adversaries use offensive frameworks that employ forms of scripting which result in this type of network activity.

Attacker's Goals

Connect to the attacker's Command and Control server.

Investigative actions

- Check the external address the process connects to.

Variations

Windows LOLBIN executable connected to a rare external host on a newly activated agent

Synopsis

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

Description

Scripts connecting to external IP addresses may be sanctioned IT scripts. However, when those external IP addresses are only receiving connections from a few specific endpoints in the organization, these scripts may be an indicator of more suspicious activity. Security testers and adversaries use offensive frameworks that employ forms of scripting which result in this type of network activity.

Attacker's Goals

Connect to the attacker's Command and Control server.

Investigative actions

- Check the external address the process connects to.

Windows LOLBIN executable connected to a rare external host

Synopsis

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

Description

Scripts connecting to external IP addresses may be sanctioned IT scripts. However, when those external IP addresses are only receiving connections from a few specific endpoints in the organization, these scripts may be an indicator of more suspicious activity. Security testers and adversaries use offensive frameworks that employ forms of scripting which result in this type of network activity.

Attacker's Goals

Connect to the attacker's Command and Control server.

Investigative actions

- Check the external address the process connects to.

30.167 | Svchost.exe loads a rare unsigned module

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	Malicious Service Analytics
ATT&CK Tactic	Defense Evasion (TA0005) Persistence (TA0003)
ATT&CK Technique	Masquerading: Masquerade Task or Service (T1036.004) Create or Modify System Process: Windows Service (T1543.003)
Severity	Low

Description

Svchost.exe loads a rare unsigned module, which can indicate an attacker's malicious service execution.

Attacker's Goals

Evading detections by running code from a signed Microsoft executable.

Investigative actions

Check whether the loaded module with the corresponding hash is benign, and if this was a desired behavior as part of its normal execution flow.

Go to the 'Services' registry key and investigate its sub keys to find the service associated with the loaded dll.

30.168 | Suspicious container runtime connection from within a Kubernetes Pod

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	Kubernetes - AGENT, Containers
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Container Administration Command (T1609) Deploy Container (T1610)
Severity	Informational

Description

A process from within a Kubernetes Pod communicated with the container runtime daemon using the runtime socket.
This may indicate an adversary attempting to escape from the Kubernetes Pod to the host.

Attacker's Goals

Escape from a container to the host machine and expand the foothold in the network.

Investigative actions

- Change the container socket configuration.
- Check if the default docker daemon binding to TCP changed - if it did, every non-root user might access the container.

Variations

Suspicious container runtime connection from within a Kubernetes Pod using the curl client

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	- Container Administration Command (T1609) - Deploy Container (T1610)
Severity	Low

Description

A process from within a Kubernetes Pod communicated with the container runtime daemon using the runtime socket.
This may indicate an adversary attempting to escape from the Kubernetes Pod to the host.

Attacker's Goals

Escape from a container to the host machine and expand the foothold in the network.

Investigative actions

Change the container socket configuration.
Check if the default docker daemon binding to TCP changed - if it did, every non-root user might access the container.

Suspicious container runtime connection from within a Kubernetes Pod using the docker client

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Container Administration Command (T1609) Deploy Container (T1610)
Severity	Medium

Description

A process from within a Kubernetes Pod communicated with the container runtime daemon using the runtime socket.
This may indicate an adversary attempting to escape from the Kubernetes Pod to the host.

Attacker's Goals

Escape from a container to the host machine and expand the foothold in the network.

Investigative actions

- Change the container socket configuration.
- Check if the default docker daemon binding to TCP changed - if it did, every non-root user might access the container.

30.169 | Executable moved to Windows system folder

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) Privilege Escalation (TA0004) Persistence (TA0003)
ATT&CK Technique	Masquerading (T1036) Event Triggered Execution: Accessibility Features (T1546.008)
Severity	Medium

Description

Attackers may replace Windows system executables with malicious ones for persistence and privilege escalation.

Attacker's Goals

- An adversary can replace a common Windows application to elevate privileges or to create persistence that is action triggered.
  The replaced application can be triggered with a key combination, remote connection for user interaction.

Investigative actions

Check if the digital signature of common applications in the Windows folder is valid.

30.170 | Phantom DLL Loading

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	DLL Hijacking Analytics
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Hijack Execution Flow: DLL Side-Loading (T1574.002)
Severity	Medium

Description

An attacker might leverage existing processes missing module loads to load malicious code into trusted processes.

Attacker's Goals

An attacker is attempting to load untrusted code into trusted contexts to avoid detection, persist or escalate privileges.

Investigative actions

Investigate the loaded module and verify if it is malicious.

30.171 | Suspicious ICMP packet

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	Command and Control (TA0011)

ATT&CK Technique	Protocol Tunneling (T1572)
Severity	Low

Description

An ICMP router advertisement was sent by a host.

Attacker's Goals

Make the victim change his routing table.

Investigative actions

Investigate why the source host sent an ICMP router advertisement and if it changed the destination target routing table.

Variations

Suspicious ICMP packet that resemble an ICMP redirect attack

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Protocol Tunneling (T1572)
Severity	Informational

Description

ICMP redirect was sent by a user.

Attacker's Goals

Make the victim change his routing table.

Investigative actions

Investigate why the source host sent an ICMP router advertisement and if it changed the destination target routing table.

30.172 | Uncommon net group or localgroup 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	
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Permission Groups Discovery (T1069)
Severity	Informational

Description

The 'net' group or localgroup command is used to add, display, or modify local or domain-level groups. Adversaries may attempt to use the command to find local or domain-level groups and permissions settings or modify local or domain-level group memberships.

Attacker's Goals

Attackers may attempt to use the command to find local or domain-level groups permissions settings or modify local or domain-level memberships.

Investigative actions

- Check if the queried group is a sensitive one (e.g. administrators).
- Check whether the initiating process has executed additional discovery commands.

Variations

Uncommon unsigned net group administrators command execution

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Permission Groups Discovery (T1069)
Severity	High

Description

The 'net' group command is used to add, display, or modify domain-level groups. Adversaries may attempt to use the command to find domain-level groups and permissions settings or modify domain-level group memberships.

Attacker's Goals

Attackers may attempt to use the command to find domain-level groups permissions settings or modify domain-level memberships.

Investigative actions

Check if the queried group is a sensitive one (e.g. administrators).

- Check whether the initiating process has executed additional discovery commands.

Uncommon remote net group administrators command execution

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Permission Groups Discovery (T1069)
Severity	Low

Description

The 'net' group command is used to add, display, or modify domain-level groups. Adversaries may attempt to use the command to find domain-level groups and permissions settings or modify domain-level group memberships.

Attacker's Goals

Attackers may attempt to use the command to find domain-level groups permissions settings or modify domain-level memberships.

Investigative actions

- Check if the queried group is a sensitive one (e.g. administrators).

Check whether the initiating process has executed additional discovery commands.

Uncommon net group administrators command execution

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Permission Groups Discovery (T1069)

Severity	Medium

Description

The 'net' group command is used to add, display, or modify domain-level groups. Adversaries may attempt to use the command to find domain-level groups and permissions settings or modify domain-level group memberships.

Attacker's Goals

Attackers may attempt to use the command to find domain-level groups permissions settings or modify domain-level memberships.

Investigative actions

- Check if the queried group is a sensitive one (e.g. administrators).
- Check whether the initiating process has executed additional discovery commands.

Uncommon net group execution

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Permission Groups Discovery (T1069)
Severity	Low

Description

The 'net' group command is used to add, display, or modify domain-level groups. Adversaries may attempt to use the command to find domain-level groups and permissions settings or modify domain-level group memberships.

Attacker's Goals

Attackers may attempt to use the command to find domain-level groups permissions settings or modify domain-level memberships.

Investigative actions

Check if the queried group is a sensitive one (e.g. administrators).

- Check whether the initiating process has executed additional discovery commands.

Uncommon remote net group execution

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Permission Groups Discovery (T1069)
Severity	Low

Description

The 'net' group command is used to add, display, or modify domain-level groups. Adversaries may attempt to use the command to find domain-level groups and permissions settings or modify domain-level group memberships.

Attacker's Goals

Attackers may attempt to use the command to find domain-level groups permissions settings or modify domain-level memberships.

Investigative actions

- Check if the queried group is a sensitive one (e.g. administrators).

Check whether the initiating process has executed additional discovery commands.

Uncommon administrator net group execution by scripting engine or command prompt

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Permission Groups Discovery (T1069)

Severity	Medium

Description

The 'net' group command is used to add, display, or modify domain-level groups. Adversaries may attempt to use the command to find domain-level groups and permissions settings or modify domain-level group memberships.

Attacker's Goals

Attackers may attempt to use the command to find domain-level groups permissions settings or modify domain-level memberships.

Investigative actions

- Check if the queried group is a sensitive one (e.g. administrators).
- Check whether the initiating process has executed additional discovery commands.

Uncommon net localgroup administrators command execution by a web server process or CGO

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Permission Groups Discovery (T1069)
Severity	Medium

Description

The 'net' localgroup command is used to add, display, or modify local groups. Adversaries may attempt to use the command to find local groups and permissions settings or modify local group memberships. When executed from a web server, it might be executed from an installed Webshell.

Attacker's Goals

Attackers may attempt to use the command to find local groups permissions settings or modify local memberships.

Investigative actions

- Check if the queried group is a sensitive one (e.g. administrators).
- Check whether the initiating process has executed additional discovery commands.

Uncommon unsigned net localgroup administrators command execution

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Permission Groups Discovery (T1069)
Severity	Medium

Description

The 'net' localgroup command is used to add, display, or modify local groups. Adversaries may attempt to use the command to find local groups and permissions settings or modify local group memberships.

Attacker's Goals

Attackers may attempt to use the command to find local groups permissions settings or modify local memberships.

Investigative actions

- Check if the queried group is a sensitive one (e.g. administrators).
- Check whether the initiating process has executed additional discovery commands.

Uncommon net localgroup administrators command execution

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Permission Groups Discovery (T1069)

Severity	Low

Description

The 'net' localgroup command is used to add, display, or modify local groups. Adversaries may attempt to use the command to find local groups and permissions settings or modify local group memberships.

Attacker's Goals

Attackers may attempt to use the command to find local groups permissions settings or modify local memberships.

Investigative actions

- Check if the queried group is a sensitive one (e.g. administrators).
- Check whether the initiating process has executed additional discovery commands.

Uncommon net localgroup execution

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Permission Groups Discovery (T1069)
Severity	Low

Description

The 'net' localgroup command is used to add, display, or modify local groups. Adversaries may attempt to use the command to find local groups and permissions settings or modify local group memberships.

Attacker's Goals

Attackers may attempt to use the command to find local groups permissions settings or modify local memberships.

Investigative actions

- Check if the queried group is a sensitive one (e.g. administrators).
- Check whether the initiating process has executed additional discovery commands.

Uncommon remote net localgroup execution

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Permission Groups Discovery (T1069)
Severity	Low

Description

The 'net' localgroup command is used to add, display, or modify local groups. Adversaries may attempt to use the command to find local groups and permissions settings or modify local group memberships.

Attacker's Goals

Attackers may attempt to use the command to find local groups permissions settings or modify local memberships.

Investigative actions

- Check if the queried group is a sensitive one (e.g. administrators).
- Check whether the initiating process has executed additional discovery commands.

Uncommon administrator net localgroup execution by scripting engine or command prompt

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Permission Groups Discovery (T1069)

Severity	Medium

Description

The 'net' localgroup command is used to add, display, or modify local groups. Adversaries may attempt to use the command to find local groups and permissions settings or modify local group memberships.

Attacker's Goals

Attackers may attempt to use the command to find local groups permissions settings or modify local memberships.

Investigative actions

- Check if the queried group is a sensitive one (e.g. administrators).
- Check whether the initiating process has executed additional discovery commands.

30.173 | Remote WMI process execution

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	3 Days
Required Data	- Requires: - XDR Agent
Detection Modules	

Detector Tags	Impacket Analytics
ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Services (T1021) Remote Services: Windows Remote Management (T1021.006)
Severity	Medium

Description

A host that rarely initiates WMI to other remote hosts triggered a remote process execution by using WMI RPC.

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 process or software initiated it.

Variations

Suspicious remote WMI process execution

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Services (T1021) Remote Services: Windows Remote Management (T1021.006)

Severity	High

Description

A host that rarely initiates WMI to other remote hosts triggered a suspicious remote process execution by using WMI RPC.

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 process or software initiated it.

30.174 | Uncommon DotNet module load relationship

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	Reflective Code Loading (T1620)
Severity	Informational

Description

A signed process that usually doesn't use DotNet loaded a common DotNet module.

Attacker's Goals

Adversaries may reflectively load DotNet code into a process to conceal the execution of malicious payloads.

Investigative actions

- Investigate the actor processes for malicious activities.
  Check for recent service installation that may load DotNet modules.

30.175 | Office process spawned with suspicious command-line 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	Process Injection: Process Hollowing (T1055.012)
Severity	Medium

Description

An Office process was run with LOLBIN-like command-line arguments. This behavior is exhibited in the VBA-RunPE tool that runs executables from the memory of Word/Excel/PowerPoint.

Attacker's Goals

Execute arbitrary code or run malicious applications undetected.

Investigative actions

Check the file that spawns the office application, and search for macros, formulas, or scripts.

Variations

PowerPoint process accesses a suspicious PPAM file

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Process Injection: Process Hollowing (T1055.012)
Severity	Medium

Description

A PowerPoint process opened a PPAM file which might be used to execute a malicious code.

Attacker's Goals

Execute arbitrary code or run malicious applications undetected.

Investigative actions

Check the file that spawns the office application, and search for macros, formulas, or scripts.

30.176 | Unicode RTL Override Character

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	High

Description

An attacker may use a special right-to-left (RTL) override character to trick users into executing malicious files that look like benign file types.

Attacker's Goals

Trick users into executing malicious files by making their file types seem benign.

Investigative actions

Investigate the executed process. There is no reason for benign files to contain the Unicode right-to-left override character in their name.

30.177 | Suspicious data encryption

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) Defense Evasion (TA0005)
ATT&CK Technique	Data Encrypted for Impact (T1486) Obfuscated Files or Information: Encrypted/Encoded File (T1027.013)
Severity	Low

Description

Known applications were used to encrypt data within a machine's local file system.

Attacker's Goals

Damage or hide data on the local file system.

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.

30.178 | A contained executable from a mounted share initiated a suspicious outbound network connection

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	Escape to Host (T1611)
Severity	Medium

Description

A contained executable from a mounted share initiated a suspicious outbound network connection.
Running binaries from a mounted share is highly dangerous and not typical.

Attacker's Goals

Gain high privileged command execution on the host machine via one of its running containers.

Investigative actions

Check if the requested IP address is known or malicious.

Investigate the contained process and its process tree.

Variations

A contained executable from a mounted share initiated a suspicious outbound network connection

Synopsis

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

Description

A cloud machine contained executable from a mounted share initiated a suspicious outbound network connection.
Running binaries from a mounted share is highly dangerous and not typical.

Attacker's Goals

Gain high privileged command execution on the host machine via one of its running containers.

Investigative actions

Check if the requested IP address is known or malicious.

Investigate the contained process and its process tree.

30.179 | Suspicious usage of File Server Remote VSS Protocol (FSRVP)

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	Use Alternate Authentication Material: Pass the Hash (T1550.002)
Severity	High

Description

A suspicious usage of File Server Remote VSS Protocol (FSRVP) was done.

Attacker's Goals

An attacker is attempting to steal credentials and move laterally within a network.

Investigative actions

- Check for suspicious processes on the source host.
- Check if the source host is a vulnerability scanner.
  Look for additional suspicious activities by users.

30.180 | Suspicious RunOnce Parent 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	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 login events.

Attacker's Goals

An attacker is trying to perform an action on the system at a later point, achieving persistence.

Investigative actions

Investigate the endpoint to determine if it's a legitimate process that is supposed to use RunOnce in its operation.

30.181 | Bitsadmin.exe persistence using command-line callback

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	BITS Jobs (T1197)
Severity	Medium

Description

BITSAdmin.exe was used with a command-line that may indicate a malware trying to gain persistence on the machine.

Attacker's Goals

Gain persistence using the legitimate bitsadmin 'setnotifycmdline' mechanism, which triggers process executions once a Bits job is done or fails.

Investigative actions

- Check if the command line contains any malicious indicators.
- Check if the parent process is suspicious.
Check if the command-line used to persist is malicious or references a malicious binary.

30.182 | Indicator blocking

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	Impair Defenses: Indicator Blocking (T1562.006)
Severity	Informational

Description

Auditing or logging configuration changes on Linux host.

Attacker's Goals

Impairing host defenses.

Investigative actions

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

Variations

Indicator blocking in a Kubernetes pod

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Impair Defenses: Indicator Blocking (T1562.006)
Severity	Low

Description

Auditing or logging configuration changes on Linux host.

Attacker's Goals

Impairing host defenses.

Investigative actions

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

30.183 | A rare local administrator 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	Valid Accounts (T1078)
Severity	Informational

Description

A rare local administrator login was observed. This may indicate an attempt to change sensitive settings on the host.

Attacker's Goals

The attacker attempts to change sensitive settings on the host.

Investigative actions

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

Variations

Suspicious local administrator login

Synopsis

ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Low

Description

A rare local administrator login was observed. This may indicate an attempt to change sensitive settings on the host.

Attacker's Goals

The attacker attempts to change sensitive settings on the host.

Investigative actions

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

30.184 | Masquerading as the Linux crond 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	Kubernetes - AGENT, Containers
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Masquerading: Masquerade Task or Service (T1036.004)
Severity	Low

Description

Copies a file and renames it as crond.

Attacker's Goals

Attackers may masquerade as the crond executable.

Investigative actions

Verify that this isn't IT activity.

Look for other hosts executing similar commands.

Variations

Masquerading as the Linux crond process from a Kubernetes pod

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Masquerading: Masquerade Task or Service (T1036.004)
Severity	Low

Description

Copies a file and renames it as crond.

Attacker's Goals

Attackers may masquerade as the crond executable.

Investigative actions

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

30.185 | Rare signature signed executable executed in the network

Synopsis

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

Required Data	- Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Subvert Trust Controls: Code Signing (T1553.002)
Severity	Informational

Description

Attackers may use signed executables by less known vendors to bypass security features.

Attacker's Goals

Adversaries may use signed binaries to bypass security features.

Investigative actions

Check if this is legitimate software installed by a legitimate user and intentionally.

Variations

Rare signature signed forensic tool remotely executed in the network

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Subvert Trust Controls: Code Signing (T1553.002)

Severity	Medium

Description

Attackers may use signed executables by less known vendors to bypass security features.

Attacker's Goals

Adversaries may use signed binaries to bypass security features.

Investigative actions

- Check the capabilities of the forensic tool, for example if it can read data directly from the disk.
  Check other activities seen from the same remote IP address.

Rare signature signed forensic tool executed in the network

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Subvert Trust Controls: Code Signing (T1553.002)
Severity	Low

Description

Attackers may use signed executables by less known vendors to bypass security features.

Attacker's Goals

Adversaries may use signed binaries to bypass security features.

Investigative actions

- Check the capabilities of the forensic tool, for example if it can read data directly from the disk.

30.186 | Uncommon cloud CLI tool usage

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	Requires: - XDR Agent
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Command and Scripting Interpreter: Cloud API (T1059.009)
Severity	Informational

Description

An uncommon execution of a cloud CLI tool.

Attacker's Goals

Abuse cloud APIs to execution malicious commands.

Investigative actions

- Check what cloud CLI commands were executed.
- Verify which cloud resources may have been affected.

Variations

Uncommon cloud CLI tool usage within a web server pod

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Command and Scripting Interpreter: Cloud API (T1059.009)
Severity	Low

Description

An uncommon execution of a cloud CLI tool.

Attacker's Goals

Abuse cloud APIs to execution malicious commands.

Investigative actions

- Check what cloud CLI commands were executed.
- Verify which cloud resources may have been affected.

Uncommon cloud CLI tool usage within a web server

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Command and Scripting Interpreter: Cloud API (T1059.009)

Severity	Low

Description

An uncommon execution of a cloud CLI tool.

Attacker's Goals

Abuse cloud APIs to execution malicious commands.

Investigative actions

- Check what cloud CLI commands were executed.
  Verify which cloud resources may have been affected.

Uncommon cloud CLI tool usage within a cloud instance

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Command and Scripting Interpreter: Cloud API (T1059.009)
Severity	Low

Description

An uncommon execution of a cloud CLI tool.

Attacker's Goals

Abuse cloud APIs to execution malicious commands.

Investigative actions

- Check what cloud CLI commands were executed.
- Verify which cloud resources may have been affected.

Uncommon cloud CLI tool usage within a Kubernetes pod

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Command and Scripting Interpreter: Cloud API (T1059.009)
Severity	Informational

Description

An uncommon execution of a cloud CLI tool.

Attacker's Goals

Abuse cloud APIs to execution malicious commands.

Investigative actions

- Check what cloud CLI commands were executed.
  Verify which cloud resources may have been affected.

30.187 | Download a script using the python requests module

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: Python (T1059.006)
Severity	Low

Description

Download a shell script from a remote location using the Python requests module.

Attacker's Goals

Adversaries may abuse Python commands and scripts to download additional malicious files or for exfiltration.

Investigative actions

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

30.188 | Uncommon SSH session was established

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 Lateral Movement Analytics
ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	- Application Layer Protocol (T1071) Non-Standard Port (T1571)
Severity	Low

Description

An uncommon SSH session was established.

Attacker's Goals

Attackers may use SSH or any similar utility to create a network tunnel to allow an attacker to covertly connect to an internal host.

Investigative actions

- Review the external IP/domain using known intelligence tools.
- Investigate the causality of the process and its user ID to find uncommon behaviors.
- Search for processes or files that were created by this SSH instance.

Variations

An Uncommon SSH session was established using a rare server HASSH for the ssh server

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Application Layer Protocol (T1071) Non-Standard Port (T1571)
Severity	Low

Description

An Uncommon SSH session was established using a rare server HASSH for the ssh server.

Attacker's Goals

Attackers may use SSH or any similar utility to create a network tunnel to allow an attacker to covertly connect to an internal host.

Investigative actions

- Review the external IP/domain using known intelligence tools.
- Investigate the causality of the process and its user ID to find uncommon behaviors.
- Search for processes or files that were created by this SSH instance.

An Uncommon SSH session was established using a rare client HASSH for the agent

Synopsis

ATT&CK Tactic	Command and Control (TA0011)

ATT&CK Technique	- Application Layer Protocol (T1071) - Non-Standard Port (T1571)
Severity	Low

Description

An Uncommon SSH session was established using a rare client HASSH for the agent.

Attacker's Goals

Attackers may use SSH or any similar utility to create a network tunnel to allow an attacker to covertly connect to an internal host.

Investigative actions

- Review the external IP/domain using known intelligence tools.
  Investigate the causality of the process and its user ID to find uncommon behaviors.
  Search for processes or files that were created by this SSH instance.

An Uncommon SSH session was established using a rare request banner for the agent

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Application Layer Protocol (T1071) Non-Standard Port (T1571)
Severity	Low

Description

An Uncommon SSH session was established using a rare request banner for the agent.

Attacker's Goals

Attackers may use SSH or any similar utility to create a network tunnel to allow an attacker to covertly connect to an internal host.

Investigative actions

- Review the external IP/domain using known intelligence tools.
- Investigate the causality of the process and its user ID to find uncommon behaviors.
  Search for processes or files that were created by this SSH instance.

An Uncommon SSH session was established using a rare Response banner for the ssh server

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	- Application Layer Protocol (T1071) Non-Standard Port (T1571)
Severity	Low

Description

An Uncommon SSH session was established using a rare Response banner for the ssh server.

Attacker's Goals

Attackers may use SSH or any similar utility to create a network tunnel to allow an attacker to covertly connect to an internal host.

Investigative actions

- Review the external IP/domain using known intelligence tools.
- Investigate the causality of the process and its user ID to find uncommon behaviors.
- Search for processes or files that were created by this SSH instance.

An Uncommon SSH session was established using a rare Response banner

Synopsis

ATT&CK Tactic	Command and Control (TA0011)

ATT&CK Technique	- Application Layer Protocol (T1071) - Non-Standard Port (T1571)
Severity	Low

Description

An Uncommon SSH session was established using a rare Response banner.

Attacker's Goals

Attackers may use SSH or any similar utility to create a network tunnel to allow an attacker to covertly connect to an internal host.

Investigative actions

- Review the external IP/domain using known intelligence tools.
  Investigate the causality of the process and its user ID to find uncommon behaviors.
  Search for processes or files that were created by this SSH instance.

An Uncommon SSH session was established using a rare request banner

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Application Layer Protocol (T1071) Non-Standard Port (T1571)
Severity	Low

Description

An Uncommon SSH session was established using a rare request banner.

Attacker's Goals

Attackers may use SSH or any similar utility to create a network tunnel to allow an attacker to covertly connect to an internal host.

Investigative actions

- Review the external IP/domain using known intelligence tools.
- Investigate the causality of the process and its user ID to find uncommon behaviors. Search for processes or files that were created by this SSH instance.

An Uncommon SSH session was established using a rare Client HASSH

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	- Application Layer Protocol (T1071) Non-Standard Port (T1571)
Severity	Low

Description

An Uncommon SSH session was established using a rare Client HASSH.

Attacker's Goals

Attackers may use SSH or any similar utility to create a network tunnel to allow an attacker to covertly connect to an internal host.

Investigative actions

Review the external IP/domain using known intelligence tools.

Investigate the causality of the process and its user ID to find uncommon behaviors.
- Search for processes or files that were created by this SSH instance.

An Uncommon SSH session was established using a rare Server HASSH

Synopsis

ATT&CK Tactic	Command and Control (TA0011)

ATT&CK Technique	- Application Layer Protocol (T1071) - Non-Standard Port (T1571)
Severity	Low

Description

An Uncommon SSH session was established using a rare Server HASSH.

Attacker's Goals

Attackers may use SSH or any similar utility to create a network tunnel to allow an attacker to covertly connect to an internal host.

Investigative actions

- Review the external IP/domain using known intelligence tools.
  Investigate the causality of the process and its user ID to find uncommon behaviors.

  Search for processes or files that were created by this SSH instance.

A suspicious SSH session was established

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Application Layer Protocol (T1071) Non-Standard Port (T1571)
Severity	Low

Description

A suspicious SSH session was established to a globally rare external IP using a nonstandard SSH port.

Attacker's Goals

Attackers may use SSH or any similar utility to create a network tunnel to allow an attacker to covertly connect to an internal host.

Investigative actions

Review the external IP/domain using known intelligence tools.
Investigate the causality of the process and its user ID to find uncommon behaviors.

Search for processes or files that were created by this SSH instance.

An Uncommon SSH session was established to a rare IP address

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Application Layer Protocol (T1071) Non-Standard Port (T1571)
Severity	Low

Description

An uncommon SSH session was established to a rare remote IP address.

Attacker's Goals

Attackers may use SSH or any similar utility to create a network tunnel to allow an attacker to covertly connect to an internal host.

Investigative actions

- Review the external IP/domain using known intelligence tools.
- Investigate the causality of the process and its user ID to find uncommon behaviors.
Search for processes or files that were created by this SSH instance.

An Uncommon SSH session was established using a nonstandard SSH port

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	- Application Layer Protocol (T1071) Non-Standard Port (T1571)
Severity	Low

Description

An uncommon SSH session was established with a destination port using a nonstandard SSH port.

Attacker's Goals

Attackers may use SSH or any similar utility to create a network tunnel to allow an attacker to covertly connect to an internal host.

Investigative actions

- Review the external IP/domain using known intelligence tools.
- Investigate the causality of the process and its user ID to find uncommon behaviors.
- Search for processes or files that were created by this SSH instance.

Uncommon SSH session was established to an internal IP

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Application Layer Protocol (T1071) Non-Standard Port (T1571)
Severity	Informational

Description

An uncommon SSH session was established to an internal IP.

Attacker's Goals

Attackers may use SSH or any similar utility to create a network tunnel to allow an attacker to covertly connect to an internal host.

Investigative actions

- Review the external IP/domain using known intelligence tools.
- Investigate the causality of the process and its user ID to find uncommon behaviors.
- Search for processes or files that were created by this SSH instance.

30.189 | Windows Installer exploitation for local privilege escalation

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	Exploitation for Privilege Escalation (T1068)
Severity	Medium

Description

The Windows installer (msiexec.exe) was likely exploited to run a malicious rollback script (.rbs file) instead of the original.
Users should not be able to modify config.msi during the installation process, only SYSTEM should have access to it.

Attacker's Goals

An attacker is attempting to gain SYSTEM privileges.

Investigative actions

- Investigate the actor process SID and path and whether it's benign or normal for this host. This action is not common, but allowed on Windows versions older than Windows 8. On those systems, check the file reputation for both the CGO and OS actor executables that ran the installation.

30.190 | Possible network sniffing attempt via tcpdump or tshark

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	Network Sniffing (T1040)
Severity	Low

Description

Attackers may monitor network traffic for cleartext credentials or to learn the network's configuration.

Attacker's Goals

Gain user-account credentials.

Investigative actions

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

30.191 | Globally uncommon high entropy process was executed

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 process with high entropy and a globally uncommon hash was executed.

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 process' file is either compressed, encrypted, obfuscated or packed.

Variations

Globally uncommon high entropy process was executed by a web server process or CGO

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005) - Initial Access (TA0001) - Persistence (TA0003)
ATT&CK Technique	Obfuscated Files or Information (T1027) - External Remote Services (T1133) - Server Software Component: Web Shell (T1505.003)
Severity	Low

Description

A process with high entropy and a globally uncommon hash was executed by a web server process or CGO.

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 process' file is either compressed, encrypted, obfuscated or packed.

30.192 | Command execution via wmiexec

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	Windows Management Instrumentation (T1047)
Severity	Informational

Description

Attackers may use WMI to execute commands on the target host.

Attacker's Goals

Execute commands on the victim host.

Investigative actions

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

30.193 | MSI accessed a web page running a server-side script

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	System Binary Proxy Execution (T1218)
Severity	Medium

Description

The Microsoft installer command line included a URL to a web page running a server-side script, which is suspicious.

Attacker's Goals

An attacker may use this technique to install a malicious tool from a remote server.

Investigative actions

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

Variations

MSI accessed a web page running a server-side script

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	System Binary Proxy Execution (T1218)
Severity	High

Description

MSI on an internet-facing server accessed a web page running a server-side script.

Attacker's Goals

An attacker may use this technique to install a malicious tool from a remote server.

Investigative actions

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

30.194 | Python HTTP server started

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: Exfiltration Over Unencrypted Non-C2 Protocol (T1048.003)
Severity	Informational

Description

Python HTTP server started - possible exfiltration over HTTP.

Attacker's Goals

Attackers might use a Python server as a C&C or exfiltration channel.

Investigative actions

- Check whether the initiator process is benign or normal for the host and/or user performing it.

30.195 | Globally uncommon image load 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, DLL Hijacking Analytics
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	- System Binary Proxy Execution (T1218) Hijack Execution Flow: DLL Side-Loading (T1574.002)

Severity	Informational

Description

A signed process loaded a DLL that, on a global level, it usually doesn't load.

Attacker's Goals

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

Investigative actions

- 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 image load from a signed process from a known vendor

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	System Binary Proxy Execution (T1218) Hijack Execution Flow: DLL Side-Loading (T1574.002)
Severity	Medium

Description

A signed process loaded a DLL that, on a global level, it usually doesn't load.

Attacker's Goals

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

Investigative actions

- 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 unsigned image side loaded to a signed process

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	System Binary Proxy Execution (T1218) Hijack Execution Flow: DLL Side-Loading (T1574.002)
Severity	Medium

Description

A signed process side loaded an unsigned DLL that, on a global level, it usually doesn't load.

Attacker's Goals

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

Investigative actions

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 image load from a signed process

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)

ATT&CK Technique	▪ System Binary Proxy Execution (T1218) ▪ Hijack Execution Flow: DLL Side-Loading (T1574.002)
Severity	Medium

Description

A signed process loaded a DLL that, on a global level, it usually doesn't load.

Attacker's Goals

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

Investigative actions

- 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 image load from an injected thread in a signed process

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	System Binary Proxy Execution (T1218) Hijack Execution Flow: DLL Side-Loading (T1574.002) ▪ Process Injection (T1055)
Severity	Low

Description

An injected thread in a signed process loaded a DLL that, on a global level, it usually doesn't load.

Attacker's Goals

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

Investigative actions

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.

30.196 | Suspicious PowerShell Enumeration of Running Processes

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	Process Discovery (T1057)
Severity	Low

Description

Attackers often enumerate running processes to find and disable security tools.

Attacker's Goals

Understand the type of host according to the processes running on it; find and disable security tools.

Investigative actions

Verify whether the command that was executed is benign or normal for the host and/or user performing it (for example, it may be an IT script).

30.197 | Recurring rare domain access from an unsigned process

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

Description

An unsigned process is periodically connecting to an external domain that it and its peers rarely use.

Access to this domain has occurred repeatedly over multiple days.
This connection pattern is consistent with malware connecting to its command and control server for updates and operating instructions.

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

- Identify the process contacting the remote domain and determine whether the traffic is malicious.
- Look for other endpoints on your network that are also periodically contacting the suspicious domain.
- Inspect the domain or URL for suspicious indicators or its presence in malicious reputation lists.

Variations

Recurring rare domain access from an uncommon unsigned process

Synopsis

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

Description

An unsigned process is periodically connecting to an external domain that it and its peers rarely use.
Access to this domain has occurred repeatedly over multiple days.
This connection pattern is consistent with malware connecting to its command and control server for updates and operating instructions.

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

- Identify the process contacting the remote domain and determine whether the traffic is malicious.
  Look for other endpoints on your network that are also periodically contacting the suspicious domain.
- Inspect the domain or URL for suspicious indicators or its presence in malicious reputation lists.

Recurring access to a rare domain associated with known threats

Synopsis

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

Severity	Medium

Description

An unsigned process is periodically connecting to an external domain that it and its peers rarely use.
Access to this domain has occurred repeatedly over multiple days.
This connection pattern is consistent with malware connecting to its command and control server for updates and operating instructions.

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

- Identify the process contacting the remote domain and determine whether the traffic is malicious.
  Look for other endpoints on your network that are also periodically contacting the suspicious domain.
- Inspect the domain or URL for suspicious indicators or its presence in malicious reputation lists.

30.198 | Suspicious Process Spawned by wininit.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	Masquerading (T1036)
Severity	Medium

Description

An unusual process was spawned by wininit.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.

30.199 | A LOLBIN was copied to a different location

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	Masquerading: Rename System Utilities (T1036.003)
Severity	Informational

Description

To evade detection, attackers may copy a LOLBIN executable to a different location.

Attacker's Goals

Command execution via lolbins and detection avoidance via file rename.

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 destination path of the lolbin and try to see if it's benign.

Variations

A LOLBIN was copied to a different location using a rare command line

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Masquerading: Rename System Utilities (T1036.003)
Severity	High

Description

To evade detection, attackers may copy a LOLBIN executable to a different location.

Attacker's Goals

Command execution via lolbins and detection avoidance via file rename.

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 destination path of the lolbin and try to see if it's benign.

A LOLBIN was copied to a different location using a rare command line via a commonly used method

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Masquerading: Rename System Utilities (T1036.003)
Severity	Low

Description

To evade detection, attackers may copy a LOLBIN executable to a different location.

Attacker's Goals

Command execution via lolbins and detection avoidance via file rename.

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 destination path of the lolbin and try to see if it's benign.

30.200 | Service execution via sc.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	Malicious Service Analytics
ATT&CK Tactic	Execution (TA0002)

ATT&CK Technique	System Services: Service Execution (T1569.002)
Severity	Informational

Description

Sc.exe has the ability to start services on local and remote hosts. An attacker may abuse it to execute malicious services on a host.

Attacker's Goals

Execute commands and run code on local or remote hosts.

Investigative actions

Check whether the service that was created via sc.exe is benign, and if this was a desired behavior as part of its normal execution flow.

30.201 | Indirect command execution using the Program Compatibility Assistant

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	Indirect Command Execution (T1202)
Severity	Medium

Description

Pcalua.exe (Program Compatibility Assistant) is used for running old programs that have compatibility issues. Attackers can use pcalua.exe to indirectly execute their malicious programs.

Attacker's Goals

Evading detection by indirectly executing their malicious programs.

Investigative actions

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

30.202 | Wscript/Cscript loads .NET DLLs

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	Process Injection (T1055)
Severity	Low

Description

An unusual script loads .NET DLLs, possibly indicating JScriptToDotnet 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.

30.203 | Procdump executed from an atypical 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	Defense Evasion (TA0005) Credential Access (TA0006)
ATT&CK Technique	Hide Artifacts: Hidden Files and Directories (T1564.001) OS Credential Dumping: LSASS Memory (T1003.001)
Severity	Medium

Description

Procdump.exe is a SysInternals tool used to dump process memory; it can be used to dump lsass.exe memory to extract credentials.

Attacker's Goals

Attackers may attempt to dump the memory of sensitive processes.

Investigative actions

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

30.204 | Suspicious curl user agent

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	Command and Control (TA0011)
ATT&CK Technique	Application Layer Protocol: Web Protocols (T1071.001)

Severity	Informational

Description

Suspicious user agent provided to curl command.

Attacker's Goals

Impairing host defenses.

Investigative actions

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

Variations

Suspicious curl user agent from within a Kubernetes Pod

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Application Layer Protocol: Web Protocols (T1071.001)
Severity	Low

Description

Suspicious user agent provided to curl command.

Attacker's Goals

Impairing host defenses.

Investigative actions

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

30.205 | Rare LOLBIN Process Execution by User

Synopsis

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

A user executed a living-off-the-land binary (LOLBIN) process that is 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 process that was executed to determine if it was used for legitimate purposes or malicious activity.

30.206 | MpCmdRun.exe was used to download files into the system

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	Ingress Tool Transfer (T1105)
Severity	Low

Description

Attackers might be using legitimate Windows Defender executables to download malicious code onto the system.

Attacker's Goals

Download malicious tools onto the host for more activities.

Investigative actions

Check if the downloaded file malicious.
- Verify if the process executing the command is malicious.
- Check for more suspicious actions done by the user and process.

30.207 | Abnormal process connection to default Meterpreter port

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-Standard Port (T1571)
Severity	Informational

Description

This process has probably been compromised by Meterpreter, and is now used by it to run malicious commands.

Attacker's Goals

Run Metasploits's malicious post exploitation tool named Meterpreter to further compromise the host.

Investigative actions

- Verify if the destination IP is running a Metasploit server.
  Look for malicious action being done by the suspicious process.

Variations

Abnormal process connection to default Meterpreter port on an internet-facing server

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Non-Standard Port (T1571)

Severity	Low

Description

This process has probably been compromised by Meterpreter, and is now used by it to run malicious commands.

Attacker's Goals

Run Metasploits's malicious post exploitation tool named Meterpreter to further compromise the host.

Investigative actions

Verify if the destination IP is running a Metasploit server.

Look for malicious action being done by the suspicious process.

30.208 | Rundll32.exe running with no command-line 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: Rundll32 (T1218.011)
Severity	Medium

Description

Rundll32.exe is meant to run with parameters, so the absence of them is extremely suspicious; this behavior is used in the default configuration of Cobalt Strike.

Attacker's Goals

- Run as a signed Microsoft executables to avoid detection.
- Rundll32 is the default process used by Cobalt Strike for running post-exploitation tools.

Investigative actions

Check for any injection event to the Rundll32 process.
Check the causality of execution for any injections.

30.209 | Certutil pfx parsing

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	Collection (TA0009)
ATT&CK Technique	Data from Local System (T1005)
Severity	Low

Description

Certutil was used to parse a pfx certificate file.

Attacker's Goals

Attackers want to check pfx details. If details suffice, the correct certificate can be used for authentication, persistence or NTLM extraction.

Investigative actions

Check if the pfx parsing is legitimate for the user (Testing, IT, etc.).

Follow further actions done by the user (ex. authentication using certificates).

30.210 | Unusual process accessed the PowerShell history 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
Detection Modules	
Detector Tags	
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Command and Scripting Interpreter: PowerShell (T1059.001)
Severity	Informational

Description

An abnormal process accessed the PowerShell console history file.
This may be a sign of malicious PowerShell execution without directly invoking the powershell.exe binary.

Attacker's Goals

An attacker is attempting to run PowerShell without powershell.exe to evade detection.

Investigative actions

- Investigate the process and command line executed and whether it's benign or normal for this host.

30.211 | Suspicious process loads a known PowerShell module

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	8 Hours
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	Informational

Description

A non-PowerShell process loaded a known PowerShell module. This image load may be an indication of PowerShell execution without directly invoking the PowerShell.exe binary.

Attacker's Goals

An attacker is attempting to run PowerShell without PowerShell.exe to evade detection.

Investigative actions

Investigate the process and command line executed and whether it's benign or normal for this host.

Variations

Suspicious unsigned process loads a known PowerShell module

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Command and Scripting Interpreter: PowerShell (T1059.001)
Severity	Low

Description

A non-PowerShell process loaded a known PowerShell module. This image load may be an indication of PowerShell execution without directly invoking the PowerShell.exe binary.

Attacker's Goals

An attacker is attempting to run PowerShell without PowerShell.exe to evade detection.

Investigative actions

Investigate the process and command line executed and whether it's benign or normal for this host.

Office process loads a known PowerShell DLL

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Command and Scripting Interpreter: PowerShell (T1059.001)
Severity	High

Description

A Microsoft Office process loaded a known PowerShell module. This image load may be a sign of PowerShell execution without directly invoking the PowerShell.exe binary.

Attacker's Goals

An attacker is attempting to run PowerShell without PowerShell.exe to evade detection.

Investigative actions

Investigate the process and command line executed and whether it's benign or normal for this host.

30.212 | Abnormal User Login 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
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Lateral Movement (TA0008) Privilege Escalation (TA0004)
ATT&CK Technique	Valid Accounts (T1078) Use Alternate Authentication Material (T1550)
Severity	Informational

Description

A user account has successfully logged on to a Domain Controller (DC), generating a Windows Event Log. This may be a sign of DC and Active Directory (AD) compromise.

Attacker's Goals

A malicious user may attempt to access a domain controller to access and control Active Directory.

Investigative actions

Ensure that the user is not a Domain Admin account. By default, Administrator groups have permission to access the domain controller.

- Check if the user is a service account that accesses a domain controller as part of its normal behavior.

Verify that the user is not authenticating to group policy.

Variations

Rare RDP User Login to Domain Controller by an Abnormal Department

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008) Privilege Escalation (TA0004)
ATT&CK Technique	Valid Accounts (T1078) Use Alternate Authentication Material (T1550)
Severity	Medium

Description

A user account has successfully interactively logged on to a Domain Controller (DC), generating a Windows Event Log. This may be a sign of DC and Active Directory (AD) compromise.

Attacker's Goals

A malicious user may attempt to access a domain controller to access and control Active Directory.

Investigative actions

Ensure that the user is not a Domain Admin account. By default, Administrator groups have permission to access the domain controller.

- Check if the user is a service account that accesses a domain controller as part of its normal behavior.

Verify that the user is not authenticating to group policy.

Abnormal RDP User Login to Domain Controller

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008) Privilege Escalation (TA0004)
ATT&CK Technique	Valid Accounts (T1078) Use Alternate Authentication Material (T1550)
Severity	Low

Description

A user account has successfully interactively logged on to a Domain Controller (DC), generating a Windows Event Log. This may be a sign of DC and Active Directory (AD) compromise.

Attacker's Goals

A malicious user may attempt to access a domain controller to access and control Active

Directory.

Investigative actions

- Ensure that the user is not a Domain Admin account. By default, Administrator groups have permission to access the domain controller.
  Check if the user is a service account that accesses a domain controller as part of its normal behavior.

  Verify that the user is not authenticating to group policy.

RDP User Login to Domain Controller

Synopsis

ATT&CK Tactic	- Lateral Movement (TA0008) Privilege Escalation (TA0004)
ATT&CK Technique	- Valid Accounts (T1078) Use Alternate Authentication Material (T1550)

Severity	Informational

Description

A user account has successfully logged on to a Domain Controller (DC), generating a Windows Event Log. This may be a sign of DC and Active Directory (AD) compromise.

Attacker's Goals

A malicious user may attempt to access a domain controller to access and control Active Directory.

Investigative actions

- Ensure that the user is not a Domain Admin account. By default, Administrator groups have permission to access the domain controller.
- Check if the user is a service account that accesses a domain controller as part of its normal behavior.
- Verify that the user is not authenticating to group policy.

Abnormal User Login to Domain Controller by an Abnormal Department

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008) Privilege Escalation (TA0004)
ATT&CK Technique	Valid Accounts (T1078) Use Alternate Authentication Material (T1550)
Severity	Informational

Description

A user account has successfully logged on to a Domain Controller (DC), generating a Windows Event Log. This may be a sign of DC and Active Directory (AD) compromise.

Attacker's Goals

A malicious user may attempt to access a domain controller to access and control Active Directory.

Investigative actions

Ensure that the user is not a Domain Admin account. By default, Administrator groups have permission to access the domain controller.

Check if the user is a service account that accesses a domain controller as part of its normal behavior.

- Verify that the user is not authenticating to group policy.

30.213 | Memory dumping with comsvcs.dll

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	Credential Access (TA0006)

ATT&CK Technique	- OS Credential Dumping (T1003) - OS Credential Dumping: LSASS Memory (T1003.001)
Severity	High

Description

A process memory dump was performed using comsvcs.dll MiniDump. This method is commonly used by attackers to dump Lsass.exe (Local Security Authority Subsystem Service) process memory to a file, so they could later extract credentials from the memory dump.

Attacker's Goals

Attackers may attempt to dump the memory of sensitive processes.

Investigative actions

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

30.214 | An uncommon service was started

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) Privilege Escalation (TA0004)
ATT&CK Technique	Create or Modify System Process: Systemd Service (T1543.002)
Severity	Low

Description

An uncommon service was started using systemctl or service processes.

Attacker's Goals

Attackers may create systemd services to run malicious payloads.

Investigative actions

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

Variations

An uncommon service was started in a Kubernetes pod

Synopsis

ATT&CK Tactic	- Persistence (TA0003) - Privilege Escalation (TA0004)

ATT&CK Technique	Create or Modify System Process: Systemd Service (T1543.002)
Severity	Low

Description

An uncommon service was started using systemctl or service processes.

Attacker's Goals

Attackers may create systemd services to run malicious payloads.

Investigative actions

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

30.215 | Unusual weak authentication 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
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 a host via NTLMv1 or LM authentication for the first time in the past 30 days. This may be indicative 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.

30.216 | Execution of an uncommon process with a local/domain user SID at an early startup stage by Windows system binary

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	Generic Persistence Analytics
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Boot or Logon Autostart Execution (T1547)
Severity	Low

Description

Execution of an uncommon process with a local/domain user SID at an early startup stage by Windows system binary may be an indication of a persistent mechanism on boot that is being actively abused.

Attacker's Goals

Attackers aim to get persistence to continue operating even after a reboot.

Investigative actions

Check if the Causality Group Owner (CGO) has a related persistence mechanism that may have been abused by an attacker.

Variations

Execution of an uncommon process with a local/domain user SID at an early startup stage by Windows system binary - Explorer CGO

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Boot or Logon Autostart Execution (T1547)
Severity	Informational

Description

Execution of an uncommon process with a local/domain user SID at an early startup stage by Windows system binary may be an indication of a persistent mechanism on boot that is being actively abused.

Attacker's Goals

Attackers aim to get persistence to continue operating even after a reboot.

Investigative actions

Check if the user is responsible for the action process creation; otherwise, examine the Run//RunOnce (Autoruns) registry keys for possible persistence.

Execution of an uncommon process with a local/domain user SID at an early startup stage with a suspicious characteristics by Windows system binary

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Boot or Logon Autostart Execution (T1547)
Severity	Medium

Description

Execution of an uncommon process with a local/domain user SID at an early startup stage by Windows system binary may be an indication of a persistent mechanism on boot that is being actively abused.

Attacker's Goals

Attackers aim to get persistence to continue operating even after a reboot.

Investigative actions

Check if the Causality Group Owner (CGO) has a related persistence mechanism that may have been abused by an attacker.

Execution of an uncommon process with a local/domain user SID at an early startup stage with an uncommon characteristics by Windows system binary

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Boot or Logon Autostart Execution (T1547)
Severity	Low

Description

Execution of an uncommon process with a local/domain user SID at an early startup stage by Windows system binary may be an indication of a persistent mechanism on boot that is being actively abused.

Attacker's Goals

- Attackers aim to get persistence to continue operating even after a reboot.

Investigative actions

Check if the Causality Group Owner (CGO) has a related persistence mechanism that may have been abused by an attacker.

30.217 | Interactive login by a service 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	Low

Description

A service 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

Interactive login by a service account to a sensitive server

Synopsis

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

Description

Interactive login by a service account to a sensitive server.

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.

Failed interactive login by a service account

Synopsis

ATT&CK Tactic	Initial Access (TA0001)

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

Description

A service 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.

30.218 | Unusual Kubernetes API server communication from a pod

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days

Required Data	- Requires: - XDR Agent
Detection Modules	
Detector Tags	Kubernetes - AGENT
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Container and Resource Discovery (T1613)
Severity	Low

Description

The Kubernetes API server was accessed by an unusual process from within a pod.

Attacker's Goals

Usage of the Kubernetes API server to perform operations inside the cluster.

Investigative actions

Check if there is an active attack against the Kubernetes cluster.

Variations

Unusual Kubernetes API server communication from a new pod

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Container and Resource Discovery (T1613)

Severity	Informational

Description

The Kubernetes API server was accessed by an unusual process from within a pod.

Attacker's Goals

Usage of the Kubernetes API server to perform operations inside the cluster.

Investigative actions

Check if there is an active attack against the Kubernetes cluster.

30.219 | Execution of an uncommon process with a local/domain user SID at an early startup stage

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	Generic Persistence Analytics
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Boot or Logon Autostart Execution (T1547)
Severity	Informational

Description

Execution of an uncommon process with a local/domain user SID at an early startup stage may be an indication of a persistent mechanism on boot that is being actively abused.

Attacker's Goals

- Attackers aim to get persistence to continue operating even after a reboot.

Investigative actions

- Check if the CGO (causality group owner) is familiar and if one of it configuration/parameters/registry keys has been modified.

Variations

Execution of an uncommon process with a local/domain user SID at an early startup stage with suspicious characteristics

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Boot or Logon Autostart Execution (T1547)
Severity	Medium

Description

Execution of an uncommon process with a local/domain user SID at an early startup stage may be an indication of a persistent mechanism on boot that is being actively abused.

Attacker's Goals

Attackers aim to get persistence to continue operating even after a reboot.

Investigative actions

Check if the CGO (causality group owner) is familiar and if one of it

configuration/parameters/registry keys has been modified.

Execution of an uncommon process with a local/domain user SID at an early startup stage with uncommon characteristics

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Boot or Logon Autostart Execution (T1547)
Severity	Low

Description

Execution of an uncommon process with a local/domain user SID at an early startup stage may be an indication of a persistent mechanism on boot that is being actively abused.

Attacker's Goals

Attackers aim to get persistence to continue operating even after a reboot.

Investigative actions

- Check if the CGO (causality group owner) is familiar and if one of it configuration/parameters/registry keys has been modified.

30.220 | Suspicious print processor 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: Print Processors (T1547.012)
Severity	Medium

Description

The endpoint registered a new print processor, 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 print processor 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 svchost.exe or spoolsv.exe.

30.221 | Possible DLL Search Order Hijacking

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	DLL Hijacking Analytics

ATT&CK Tactic	- Persistence (TA0003) - Privilege Escalation (TA0004) Defense Evasion (TA0005)
ATT&CK Technique	- Hijack Execution Flow: DLL Search Order Hijacking (T1574.001) Hijack Execution Flow: Path Interception by PATH Environment Variable (T1574.007) Hijack Execution Flow: Path Interception by Unquoted Path (T1574.009) - Hijack Execution Flow: Path Interception by Search Order Hijacking (T1574.008)
Severity	Low

Description

An attacker might abuse the Windows DLL search order to trigger known, signed processes to load the attacker's malicious module.

Attacker's Goals

An attacker is attempting to load an untrusted module into a trusted context to avoid detection, gain persistence or to perform privilege escalation.

Investigative actions

- Investigate the loaded module to verify if it is malicious.
  Investigate if the loading process and the loaded module reside in legitimate locations.

Variations

Possible DLL Search Order Hijacking by DLL Substitution

Synopsis

ATT&CK Tactic	Persistence (TA0003) Privilege Escalation (TA0004) Defense Evasion (TA0005)

ATT&CK Technique	Hijack Execution Flow: DLL Search Order Hijacking (T1574.001) Hijack Execution Flow: Path Interception by PATH Environment Variable (T1574.007) Hijack Execution Flow: Path Interception by Unquoted Path (T1574.009) Hijack Execution Flow: Path Interception by Search Order Hijacking (T1574.008) Masquerading (T1036) Masquerading: Match Legitimate Name or Location (T1036.005)
Severity	Low

Description

An attacker might abuse the Windows DLL search order to trigger known, signed processes to load the attacker's malicious module.

Attacker's Goals

An attacker is attempting to load an untrusted module into a trusted context to avoid detection, gain persistence or to perform privilege escalation.

Investigative actions

- Investigate the loaded module to verify if it is malicious.
- Investigate if the loading process and the loaded module reside in legitimate locations.

30.222 | Possible Search For Password Files

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	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials: Credentials In Files (T1552.001)
Severity	Medium

Description

Attackers often search for files that have passwords in them.

Attacker's Goals

Gain user-account credentials.

Investigative actions

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

30.223 | A Successful login from TOR

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	Identity Analytics
Detector Tags	
ATT&CK Tactic	- Initial Access (TA0001) Command and Control (TA0011)
ATT&CK Technique	- Proxy: Multi-hop Proxy (T1090.003) - Valid Accounts (T1078)
Severity	High

Description

A successful login from a TOR exit node.

Attacker's Goals

Gain initial access to organization and hiding itself.

Investigative actions

- Block all web traffic to and from public Tor entry and exit nodes.
  Search for additional logins from the same user around the alert timestamp.

30.224 | Setuid and Setgid file bit 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
Detection Modules	
Detector Tags	Kubernetes - AGENT, Containers
ATT&CK Tactic	Privilege Escalation (TA0004) Defense Evasion (TA0005)
ATT&CK Technique	Abuse Elevation Control Mechanism: Setuid and Setgid (T1548.001)

Severity	Low

Description

The setuid or setgid bits were set on a file.

Attacker's Goals

Attackers may try to run the executable application as a different user.

Investigative actions

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

Variations

Setuid and Setgid file bit manipulation in a Kubernetes pod

Synopsis

ATT&CK Tactic	- Privilege Escalation (TA0004) - Defense Evasion (TA0005)
ATT&CK Technique	Abuse Elevation Control Mechanism: Setuid and Setgid (T1548.001)
Severity	Low

Description

The setuid or setgid bits were set on a file.

Attacker's Goals

Attackers may try to run the executable application as a different user.

Investigative actions

Verify that this isn't IT activity.

- Look for other hosts executing similar commands.

30.225 | Command execution in a Kubernetes pod

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
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Container Administration Command (T1609)
Severity	Informational

Description

Container administration commands were executed within a Kubernetes pod.

Attacker's Goals

Attackers may use the container administration commands to execute commands within a Kubernetes Pod.

Investigative actions

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

Variations

Command execution in a Kubernetes pod for the first time

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Container Administration Command (T1609)
Severity	Low

Description

Container administration commands were executed within a Kubernetes pod.

Attacker's Goals

Attackers may use the container administration commands to execute commands within a Kubernetes Pod.

Investigative actions

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

Command execution in a Kubernetes pod in the kube-system namespace

Synopsis

ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Container Administration Command (T1609)
Severity	Informational

Description

Container administration commands were executed within a Kubernetes pod.

Attacker's Goals

Attackers may use the container administration commands to execute commands within a Kubernetes Pod.

Investigative actions

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

30.226 | Wbadmin deleted files in quiet 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	
Detector Tags	
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Inhibit System Recovery (T1490)
Severity	High

Description

Wbadmin was used to delete files in quiet mode.

Attacker's Goals

Adversaries may delete the backup catalog to prevent recovery of a corrupted system.

Investigative actions

Check if the delete action was legitimate and performed by an authorized user.

30.227 | Windows Event Log was cleared using wevtutil.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	Impact (TA0040)
ATT&CK Technique	Inhibit System Recovery (T1490)
Severity	Low

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.

Variations

Security Event Log was cleared using wevtutil.exe