24.33 | 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.

24.34 | 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.

24.35 | 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.

24.36 | 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.

24.37 | 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.

24.38 | 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.

24.39 | 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.

24.40 | 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.

24.41 | Abnormal Recurring Communications to a Rare Domain

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: ▯ Palo Alto Networks Platform Logs OR - XDR Agent OR - Third-Party Firewalls

Detection Modules	
Detector Tags	NDR C2 Detection
ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Non-Application Layer Protocol (T1095)
Severity	Informational

Description

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

Attacker's Goals

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

Investigative actions

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

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

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

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

Variations

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

Synopsis

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

Description

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

Attacker's Goals

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

Investigative actions

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

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

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

Synopsis

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

Description

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

Attacker's Goals

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

Investigative actions

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

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

Synopsis

ATT&CK Tactic	Command and Control (TA0011)

ATT&CK Technique	Non-Application Layer Protocol (T1095)
Severity	Informational

Description

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

Attacker's Goals

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

Investigative actions

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

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

Synopsis

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

Description

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

Attacker's Goals

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

Investigative actions

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

24.42 | Abnormal Recurring Communications to a Rare IP

Synopsis

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

Required Data	- Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	
Detector Tags	NDR C2 Detection
ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Non-Application Layer Protocol (T1095)
Severity	Informational

Description

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

Attacker's Goals

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

Investigative actions

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

Variations

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

Synopsis

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

Description

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

Attacker's Goals

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

Investigative actions

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

Abnormal Recurring Communications to a Rare IP With a NetBIOS Port

Synopsis

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

Description

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

Attacker's Goals

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

Investigative actions

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

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

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

Synopsis

ATT&CK Tactic	Command and Control (TA0011)

ATT&CK Technique	Non-Application Layer Protocol (T1095)
Severity	Informational

Description

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

Attacker's Goals

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

Investigative actions

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

Abnormal Recurring Communications to a Rare IP Using a Gaming Protocol

Synopsis

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

Description

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

Attacker's Goals

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

Investigative actions

- Identify if the external IP address belongs to a reputable organization or an asset used in a public cloud.
  Identify if the source of the traffic is malware. If the source of the traffic is a malicious file,

  Cortex XDR Analytics also raises a malware alert for the file on the endpoint. Malware may contact legitimate IP addresses, therefore check for unusual apps used, or unusual ports or volumes accessed.
  View all related traffic generated by the suspicious process to understand the purpose.
  Look for other endpoints on your network that are also contacting the suspicious IP address.

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

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

Synopsis

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

Description

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

Attacker's Goals

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

Investigative actions

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

Abnormal Recurring Communications to a Rare IP From an Unmanaged Host

Synopsis

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

Description

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

Attacker's Goals

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

Investigative actions

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

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

24.43 | Rare MS-Update Server was detected

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
Detection Modules	
Detector Tags	
ATT&CK Tactic	Initial Access (TA0001)

ATT&CK Technique	Trusted Relationship (T1199)
Severity	Informational

Description

The endpoint requested an MS-Update operation from a rare update server.

Attacker's Goals

The Windows Server Update Services enables machines to discover and download software updates from a dedicated update server.

Attacker may use the MS-Update protocol to execute unauthorized code through Microsoft binaries.

Investigative actions

- Inspect the legitimacy of the server as a WSUS functioning server.
Verify that your MS-Update network routine is of HTTPS enforced
Verify that this MS-Update server is not a newly deployed server as part of a legitimate IT activity.

Variations

Rare MS-Update Server was detected

Synopsis

ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Trusted Relationship (T1199)
Severity	Informational

Description

The endpoint requested an MS-Update operation from a rare update server.

Attacker's Goals

- The Windows Server Update Services enables machines to discover and download software updates from a dedicated update server.
  Attacker may use the MS-Update protocol to execute unauthorized code through Microsoft binaries.

Investigative actions

- Inspect the legitimacy of the server as a WSUS functioning server.
- Verify that your MS-Update network routine is of HTTPS enforced
- Verify that this MS-Update server is not a newly deployed server as part of a legitimate IT activity.

24.44 | A Possible crypto miner was detected on a host

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	
Detector Tags	

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

Description

The host produced traffic consistent with the crypto mining.

Attacker's Goals

Abuse resources to mine crypto coins.

Investigative actions

Check the host for crypto mining client software.
Look for differences in the resource consumption from this host.

Examine the client's network traffic for suspicious domain affiliated with mining or mining pools.

24.45 | Multiple Weakly-Encrypted Kerberos Tickets Received

Synopsis

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

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

Description

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

Attacker's Goals

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

Investigative actions

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

24.46 | Random-Looking Domain Names

Synopsis

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

Description

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

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

Attacker's Goals

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

Investigative actions

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

24.47 | Download pattern that resembles Peer to Peer traffic

Synopsis

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

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

Description

A possible P2P protocol was spotted from an internal host.

Attacker's Goals

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

Investigative actions

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

24.48 | Multiple Suspicious FTP Login Attempts

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	2 Hours
Deduplication Period	1 Day
Required Data	Requires: - Palo Alto Networks Platform Logs
Detection Modules	
Detector Tags	
ATT&CK Tactic	▮ Initial Access (TA0001) Credential Access (TA0006)
ATT&CK Technique	▮ Brute Force (T1110) Valid Accounts (T1078)
Severity	Low

Description

Multiple suspicious FTP sessions were detected, which may indicate a brute-force attempt.

Attacker's Goals

Attackers may seek access to FTP accounts and use them to exfiltrate data, stage attack tools, or create command and control channels through trusted services.

Investigative actions

Examine the legitimacy of the application that produced this uncommon FTP connection. Examine the parent process of this application.

Verify that the connection attempts were not performed from an illegitimate source.

24.49 | NTLM Password Spray

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Palo Alto Networks Platform Logs OR ▯ XDR Agent
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)

ATT&CK Technique	Brute Force: Password Spraying (T1110.003)
Severity	Informational

Description

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

Attacker's Goals

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

Investigative actions

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

Variations

NTLM password spray on a sensitive entity

Synopsis

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

Description

A single host tried to perform an unusual amount of login attempts using NTLM in a short period of time on a sensitive entity.

This may be indicative of a NTLM password spray attack.

Attacker's Goals

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

Investigative actions

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

24.50 | Kerberos Pre-Auth Failures by Host

Synopsis

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

ATT&CK Technique	Brute Force (T1110)
Severity	Low

Description

The endpoint failed an unusual number of Kerberos pre-authentications (TGT requests) from at least three users when compared to its baseline.

This can indicate a password-spraying attack.

Attacker's Goals

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

Investigative actions

- Verify whether the host that generated the alert is normally used by many users (for example, a terminal server).
  Verify any later authentication success for the user accounts referenced by the alert, as these can indicate the attacker managed to guess the credentials.

24.51 | Subdomain Fuzzing

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	20 Minutes
Deduplication Period	1 Day

Required Data	- Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Reconnaissance (TA0043)
ATT&CK Technique	Active Scanning: Wordlist Scanning (T1595.003)
Severity	Low

Description

The root domain within the network is experiencing an unusually high number of access requests to its subdomains, significantly exceeding the typical activity levels for that domain.
This anomaly could suggest that someone is attempting to enumerate subdomains or uncover additional virtual hosts associated with the domain, possibly as part of a reconnaissance effort to identify vulnerable or less-secured entry points into the network.

Attacker's Goals

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

Investigative actions

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

Variations

Subdomain Fuzzing To a Rare Destination

Synopsis

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

Description

The root domain within the network is experiencing an unusually high number of access requests to its subdomains, significantly exceeding the typical activity levels for that domain.
This anomaly could suggest that someone is attempting to enumerate subdomains or uncover additional virtual hosts associated with the domain, possibly as part of a reconnaissance effort to identify vulnerable or less-secured entry points into the network.

Attacker's Goals

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

Investigative actions

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

24.52 | NTLM Relay

Synopsis

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

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

Description

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

Attacker's Goals

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

Investigative actions

Check that the alerted host is not a NAT or a proxy that duplicates traffic as part of its normal behavior.

- Check if the protocols used are vulnerable to an NTLM relay attack (e.g. LDAP, SMB). Ensure that SMB signing is enabled in the case of a possible SMB relay attack.

24.53 | Large Upload (HTTPS)

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Day
Deduplication Period	1 Day
Required Data	- Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent OR - Third-Party Firewalls
Detection Modules	
Detector Tags	
ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Exfiltration Over Alternative Protocol (T1048)

Severity	Low

Description

The endpoint transferred an excessive amount of data to an external site over HTTPS.
The destination is not a popular upload site for endpoints on your network, and the endpoint performing the upload has not previously downloaded a large amount of data from the site.
The upload is considered excessive based on comparison to baseline measurements of HTTPS data transfers on your network.
An attacker may be exfiltrating data directly to the internet.

Attacker's Goals

Transfer data she has stolen from your network to a location that is convenient and useful to her.

Investigative actions

- Check if this alert has been falsely triggered by DNS load balancers. If an endpoint routinely uploads data to a site that uses load balancers, the transfer might ordinarily be split into multiple sessions and across multiple subdomains, which can cause the baseline measurement to be incorrect. In that situation, a routine upload that randomly places the bulk of the data in a single session to a single subdomain can look excessive to the Cortex XDR Analytics detector.
- Check if the device performing the data transfer is a mobile phone performing a backup. Cortex XDR Analytics will not always measure the baseline properly for mobile devices, especially if the backups are performed infrequently and contain a great deal of data. If the data transfer is a mobile device running a backup, check to ensure that only appropriate data is included in the backup.
- Identify the process/user performing the data transfer to determine if the transfer is sanctioned.

Variations

Large Upload (HTTPS)

Synopsis

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

Severity	Informational

Description

The endpoint transferred an excessive amount of data to an external site over HTTPS.
The destination is not a popular upload site for endpoints on your network, and the endpoint performing the upload has not previously downloaded a large amount of data from the site.
The upload is considered excessive based on comparison to baseline measurements of HTTPS data transfers on your network.

An attacker may be exfiltrating data directly to the internet.

Attacker's Goals

Transfer data she has stolen from your network to a location that is convenient and useful to her.

Investigative actions

- Check if this alert has been falsely triggered by DNS load balancers. If an endpoint routinely uploads data to a site that uses load balancers, the transfer might ordinarily be split into multiple sessions and across multiple subdomains, which can cause the baseline measurement to be incorrect. In that situation, a routine upload that randomly places the bulk of the data in a single session to a single subdomain can look excessive to the Cortex XDR Analytics detector.
  Check if the device performing the data transfer is a mobile phone performing a backup. Cortex XDR Analytics will not always measure the baseline properly for mobile devices, especially if the backups are performed infrequently and contain a great deal of data. If the data transfer is a mobile device running a backup, check to ensure that only appropriate data is included in the backup.
  Identify the process/user performing the data transfer to determine if the transfer is sanctioned.

24.54 | Spam Bot Traffic

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	3 Days
Deduplication Period	3 Days
Required Data	Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent OR - Third-Party Firewalls
Detection Modules	
Detector Tags	
ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Resource Hijacking (T1496)
Severity	Low

Description

The endpoint connected to an excessive number of external SMTP servers.

A spambot may be trying to send spam email using multiple SMTP servers.
Spambots can cause your domain to be blacklisted, and can contain other malicious functionality. The same mechanism can also be used for exfiltration. Some VPN clients can also tunnel data over SMTP.

Note: This detection model looks for SMTP connections to external servers, but the volume of traffic is not considered. A count is performed based on the number of domains being contacted, as well as the number of unresolved IP addresses.

Attacker's Goals

The attacker uses the host as an SMTP client to send mails and hide their real origin.

Investigative actions

- Verify that the source is not an SMTP server. If Cortex XDR Analytics has failed to identify the process as a valid SMTP server, this alert will be a false positive.
- Verify that IP addresses are actually not being resolved by the non-SMTP process. If the process is performing DNS resolution with a DNS service outside your network, it is possible (depending on your network topology) that Cortex XDR Analytics will not observe that traffic. Because SMTP services typically use numerous IP addresses, this situation could cause a process to exceed a limit when it would otherwise fail to do so.
- If the SMTP connection activity turns out to be the result of malicious file activity, search on the Triage page for other endpoints infected with the file.

Variations

Spam Bot Traffic

Synopsis

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

Description

The endpoint connected to an excessive number of external SMTP servers.

A spambot may be trying to send spam email using multiple SMTP servers.
Spambots can cause your domain to be blacklisted, and can contain other malicious functionality.
The same mechanism can also be used for exfiltration. Some VPN clients can also tunnel data over SMTP.
Note: This detection model looks for SMTP connections to external servers, but the volume of traffic is not considered. A count is performed based on the number of domains being contacted, as well as the number of unresolved IP addresses.

Attacker's Goals

The attacker uses the host as an SMTP client to send mails and hide their real origin.

Investigative actions

Verify that the source is not an SMTP server. If Cortex XDR Analytics has failed to identify the process as a valid SMTP server, this alert will be a false positive.

- Verify that IP addresses are actually not being resolved by the non-SMTP process. If the process is performing DNS resolution with a DNS service outside your network, it is possible (depending on your network topology) that Cortex XDR Analytics will not observe that traffic.

  Because SMTP services typically use numerous IP addresses, this situation could cause a process to exceed a limit when it would otherwise fail to do so.
- If the SMTP connection activity turns out to be the result of malicious file activity, search on the Triage page for other endpoints infected with the file.

Failed Spam Bot Traffic

Synopsis

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

Description

The endpoint connected to an excessive number of external SMTP servers.
A spambot may be trying to send spam email using multiple SMTP servers.
Spambots can cause your domain to be blacklisted, and can contain other malicious functionality.
The same mechanism can also be used for exfiltration. Some VPN clients can also tunnel data over SMTP.

Note: This detection model looks for SMTP connections to external servers, but the volume of traffic is not considered. A count is performed based on the number of domains being contacted, as well as the number of unresolved IP addresses.

Attacker's Goals

The attacker uses the host as an SMTP client to send mails and hide their real origin.

Investigative actions

Verify that the source is not an SMTP server. If Cortex XDR Analytics has failed to identify the process as a valid SMTP server, this alert will be a false positive.

- Verify that IP addresses are actually not being resolved by the non-SMTP process. If the process is performing DNS resolution with a DNS service outside your network, it is possible (depending on your network topology) that Cortex XDR Analytics will not observe that traffic.

  Because SMTP services typically use numerous IP addresses, this situation could cause a process to exceed a limit when it would otherwise fail to do so.
- If the SMTP connection activity turns out to be the result of malicious file activity, search on the Triage page for other endpoints infected with the file.

24.55 | Massive upload to a rare storage or mail domain

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Day
Required Data	Requires: - Palo Alto Networks Platform Logs - Requires: XDR Agent
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Exfiltration (TA0010)

ATT&CK Technique	- Exfiltration Over Web Service (T1567) - Exfiltration Over Web Service: Exfiltration to Cloud Storage (T1567.002)
Severity	Informational

Description

A large amount of data was transferred to an external site that is used for mail or storage. This behavior may indicate data exfiltration.

Attacker's Goals

A user uploaded an abnormal amount of data to a file sharing service. This activity might indicate an attempt to exfiltrate files and data from the organization.

Investigative actions

Check for any other suspicious activity related to the host and the user involved in the alert.
Identify the user uploading the data to determine if the transfer is sanctioned.

Variations

A user uploaded over 500 MB to a rare storage or mail domain

Synopsis

ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	- Exfiltration Over Web Service (T1567) Exfiltration Over Web Service: Exfiltration to Cloud Storage (T1567.002)
Severity	Low

Description

A user uploaded over 500 MB to a file sharing service that is rarely accessed by them or anyone else in the organization.

Attacker's Goals

A user uploaded an abnormal amount of data to a file sharing service. This activity might indicate an attempt to exfiltrate files and data from the organization.

Investigative actions

- Check for any other suspicious activity related to the host and the user involved in the alert.
- Identify the user uploading the data to determine if the transfer is sanctioned.

24.56 | Large Upload (SMTP)

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Day
Deduplication Period	1 Day
Required Data	- Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent OR - Third-Party Firewalls
Detection Modules	

Detector Tags	
ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Exfiltration Over Alternative Protocol (T1048)
Severity	Low

Description

The endpoint, which is not an internal SMTP server, emailed an excessive amount of data from your network.

Attacker's Goals

Transfer data they have stolen from your network to a location that is convenient and useful to him.

Investigative actions

- Identify the process/user performing the data transfer to determine if the transfer is sanctioned.
- Verify that the source is not a mail server.
- Check if the target address represents a mail service that rarely used in the organization. If so, this might indicate on file exfiltration attempt.

Variations

Large Upload (SMTP)

Synopsis

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

Severity	Informational

Description

The endpoint, which is not an internal SMTP server, emailed an excessive amount of data from your network.

Attacker's Goals

Transfer data they have stolen from your network to a location that is convenient and useful to him.

Investigative actions

Identify the process/user performing the data transfer to determine if the transfer is sanctioned.

Verify that the source is not a mail server.

- Check if the target address represents a mail service that rarely used in the organization. If so, this might indicate on file exfiltration attempt.

24.57 | Increase in Job-Related Site Visits

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Day
Deduplication Period	1 Day
Required Data	Requires: - Palo Alto Networks Platform Logs

Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Reconnaissance (TA0043)
ATT&CK Technique	Search Open Websites/Domains (T1593)
Severity	Informational

Description

A user has visited multiple job-related sites in the past day.

Attacker's Goals

This may be an early indicator of an insider threat.

Investigative actions

Investigate the domains accessed and how popular they are in the organization.

- Check how long the user has been part of the organization.
- Verify that the user is not part of a department that accesses job sites as part of daily operations.

24.58 | NTLM Hash Harvesting

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	1 Hour
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Palo Alto Networks Platform Logs OR ▯ XDR Agent
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	OS Credential Dumping (T1003)
Severity	Medium

Description

An unusual number of users has sent NTLM to a target in the last hour. This may be indicative of poisoning and NTLM hash harvesting.

Attacker's Goals

The attacker may attempt to extract NTLM hashes for credential access.

Investigative actions

- Check that the destination is not a server.
- Verify that the destination is not external to the organization.

24.59 | SSH brute force attempt

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	2 Hours
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - AWS Flow Log OR - AWS OCSF Flow Logs OR - Azure Flow Log OR - Gcp Flow Log OR - Palo Alto Networks Platform Logs OR - Third-Party Firewalls - Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)

ATT&CK Technique	Brute Force (T1110)
Severity	Informational

Description

There were multiple attempts to authenticate via SSH to a host in your network. This may indicate a brute force attack.

Attacker's Goals

Attackers attempt to log in to a remote host.

Investigative actions

Audit the failed authentication attempts in the SSH server to identify the abused user. If the abused user can authenticate to the SSH server, it may indicate that the attacker managed to compromise the user credentials.

Variations

SSH brute force network detected from external source

Synopsis

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

Description

There were multiple attempts to authenticate via SSH to a host in your network. This may indicate a brute force attack.

Attacker's Goals

Attackers attempt to log in to a remote host.

Investigative actions

Audit the failed authentication attempts in the SSH server to identify the abused user. If the abused user can authenticate to the SSH server, it may indicate that the attacker managed to compromise the user credentials.

Rare SSH brute force attempt

Synopsis

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

Description

There were multiple attempts to authenticate via SSH to a host in your network. This may indicate a brute force attack.

Attacker's Goals

Attackers attempt to log in to a remote host.

Investigative actions

Audit the failed authentication attempts in the SSH server to identify the abused user. If the abused user can authenticate to the SSH server, it may indicate that the attacker managed to compromise the user credentials.

24.60 | SSH brute force attempt

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	2 Hours
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: AWS Flow Log OR AWS OCSF Flow Logs OR Azure Flow Log OR Gcp Flow Log OR Palo Alto Networks Platform Logs OR Third-Party Firewalls Requires one of the following data sources: Palo Alto Networks Platform Logs OR XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)

ATT&CK Technique	Brute Force (T1110)
Severity	Informational

Description

There were multiple attempts to authenticate via SSH to a host in your network. This may indicate a brute force attack.

Attacker's Goals

Attackers attempt to log in to a remote host.

Investigative actions

Audit the failed authentication attempts in the SSH server to identify the abused user. If the abused user can authenticate to the SSH server, it may indicate that the attacker managed to compromise the user credentials.

Variations

SSH brute force network detected from external source

Synopsis

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

Description

There were multiple attempts to authenticate via SSH to a host in your network. This may indicate a brute force attack.

Attacker's Goals

Attackers attempt to log in to a remote host.

Investigative actions

Audit the failed authentication attempts in the SSH server to identify the abused user. If the abused user can authenticate to the SSH server, it may indicate that the attacker managed to compromise the user credentials.

Rare SSH brute force attempt

Synopsis

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

Description

There were multiple attempts to authenticate via SSH to a host in your network. This may indicate a brute force attack.

Attacker's Goals

Attackers attempt to log in to a remote host.

Investigative actions

Audit the failed authentication attempts in the SSH server to identify the abused user. If the abused user can authenticate to the SSH server, it may indicate that the attacker managed to compromise the user credentials.

24.61 | Large Upload (FTP)

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Day
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: • Palo Alto Networks Platform Logs OR • XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Exfiltration Over Alternative Protocol (T1048)
Severity	Low

Description

The endpoint transferred an excessively large amounts of data to a single destination over FTP.

Cortex XDR Analytics assumes endpoint traffic towards a specific destination should be about the same over long periods of time.

For that reason, Cortex XDR detected this abnormal behavior of large data upload.
An attacker may be exfiltrating data directly to the internet using this protocol.

Attacker's Goals

Exfiltrate stolen data from the victim network to an attacker's controllable resource.

Investigative actions

Verify that the source is not an FTP server. If Cortex XDR Analytics has failed to identify the entity as a valid FTP server, this alert is likely to be a false positive.

Identify the entity performing the data transfer to determine if the transfer is sanctioned.
Use Pathfinder to interrogate the endpoint for suspicious artifacts that are using endpoint processes or loaded modules.

Variations

Large Upload (FTP)

Synopsis

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

Description

The endpoint transferred an excessively large amounts of data to a single destination over FTP.
Cortex XDR Analytics assumes endpoint traffic towards a specific destination should be about the same over long periods of time.
For that reason, Cortex XDR detected this abnormal behavior of large data upload.

An attacker may be exfiltrating data directly to the internet using this protocol.

Attacker's Goals

Exfiltrate stolen data from the victim network to an attacker's controllable resource.

Investigative actions

Verify that the source is not an FTP server. If Cortex XDR Analytics has failed to identify the entity as a valid FTP server, this alert is likely to be a false positive.

- Identify the entity performing the data transfer to determine if the transfer is sanctioned. Use Pathfinder to interrogate the endpoint for suspicious artifacts that are using endpoint processes or loaded modules.

24.62 | Rare access to known advertising domains

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Day
Deduplication Period	1 Day
Required Data	Requires: - Palo Alto Networks Platform Logs - Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Command and Control (TA0011) Persistence (TA0003)
ATT&CK Technique	Application Layer Protocol (T1071) Browser Extensions (T1176)

Severity	Informational

Description

The endpoint performed many connections to unpopular advertising domains.

This could indicate the presence of adware on the endpoint.

Attacker's Goals

Causing the user to view excessive advertising content.

Investigative actions

- Investigate the infected machine and search for suspicious browser extensions, See if changes were made to the homepage or if the browser is slower than usual, check whether sites that do not have ads usually, display ads when accessed from the possibly infected endpoint.

  Search for suspicious redirections or proxy configuration on the infected machine.
- Search for a C&C communication.

Variations

Rare access to known advertising domains from a Rare User Agent

Synopsis

ATT&CK Tactic	Command and Control (TA0011) Persistence (TA0003)
ATT&CK Technique	Application Layer Protocol (T1071) Browser Extensions (T1176)
Severity	Informational

Description

The endpoint performed many connections to unpopular advertising domains from a rare user agent.

This could indicate the presence of adware on the endpoint.

Attacker's Goals

Causing the user to view excessive advertising content.

Investigative actions

- Investigate the infected machine and search for suspicious browser extensions, See if changes were made to the homepage or if the browser is slower than usual, check whether sites that do not have ads usually, display ads when accessed from the possibly infected endpoint.
- Search for suspicious redirections or proxy configuration on the infected machine.
- Search for a C&C communication.

Suspicious Rare access to known advertising domains

Synopsis

ATT&CK Tactic	Command and Control (TA0011) Persistence (TA0003)
ATT&CK Technique	Application Layer Protocol (T1071) Browser Extensions (T1176)
Severity	Low

Description

The endpoint performed many connections to unpopular advertising domains.
This could indicate the presence of adware on the endpoint.

Attacker's Goals

Causing the user to view excessive advertising content.

Investigative actions

- Investigate the infected machine and search for suspicious browser extensions, See if changes were made to the homepage or if the browser is slower than usual, check whether sites that do not have ads usually, display ads when accessed from the possibly infected endpoint.
- Search for suspicious redirections or proxy configuration on the infected machine.
- Search for a C&C communication.

24.63 | Kerberos Pre-Auth Failures by User and Host

Synopsis

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

Description

The user account on this host failed Kerberos pre-authentications (TGT requests) an unusual number of times.
This can indicate a Kerberos brute-force attack.

Attacker's Goals

The attacker is attempting to guess the credentials for the user account.

Investigative actions

- Verify that the password for the account has not been changed recently, without updating the user or the program using it.
- Verify any later authentication success for the user accounts referenced by the alert, as these can indicate the attacker managed to guess the credentials.

24.64 | Large Upload (Generic)

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Day
Deduplication Period	1 Day
Required Data	❚ Requires one of the following data sources: ▯ Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	

Detector Tags	
ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Exfiltration Over Alternative Protocol (T1048)
Severity	Low

Description

The endpoint transferred large amounts of data to an external site using a different protocol from HTTP/s, FTP, or SMTP. (A specific detector is used for each of those protocols.)
Cortex XDR Analytics assumes that data transfers out of your network are ordinarily performed using one of those three services, so it expects that data transfers over all other ports to be low. For the same reason, Cortex XDR Analytics also assumes endpoint traffic towards a specific destination should be about the same over long periods of time.
An attacker may be exfiltrating data directly to the internet.

Attacker's Goals

Transfer data he has stolen from your network to a location that is convenient and useful to him.

Investigative actions

- Check if the traffic is related to SSH activity, it can trigger this alert. It is possible that someone on your network is legitimately engaged in SSH activity.
- Check if the traffic is to/from a misconfigured network.
- Check if the traffic is to a new external service or server that has recently been adopted for use by an organization in your enterprise.
- Identify the process/user performing the data transfer to determine if the transfer is sanctioned.

Variations

Large Upload (Generic)

Synopsis

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

Description

The endpoint transferred large amounts of data to an external site using a different protocol from HTTP/s, FTP, or SMTP. (A specific detector is used for each of those protocols.)
Cortex XDR Analytics assumes that data transfers out of your network are ordinarily performed using one of those three services, so it expects that data transfers over all other ports to be low.
For the same reason, Cortex XDR Analytics also assumes endpoint traffic towards a specific

destination should be about the same over long periods of time.
An attacker may be exfiltrating data directly to the internet.

Attacker's Goals

Transfer data he has stolen from your network to a location that is convenient and useful to him.

Investigative actions

Check if the traffic is related to SSH activity, it can trigger this alert. It is possible that someone on your network is legitimately engaged in SSH activity.

Check if the traffic is to/from a misconfigured network.
- Check if the traffic is to a new external service or server that has recently been adopted for use by an organization in your enterprise.
Identify the process/user performing the data transfer to determine if the transfer is sanctioned.

Large Upload (Generic)to a Frequently Used Upload Target

Synopsis

ATT&CK Tactic	Exfiltration (TA0010)

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

Description

The endpoint transferred large amounts of data to an external site using a different protocol from

HTTP/s, FTP, or SMTP. (A specific detector is used for each of those protocols.)
Cortex XDR Analytics assumes that data transfers out of your network are ordinarily performed using one of those three services, so it expects that data transfers over all other ports to be low. For the same reason, Cortex XDR Analytics also assumes endpoint traffic towards a specific destination should be about the same over long periods of time.

An attacker may be exfiltrating data directly to the internet.

Attacker's Goals

Transfer data he has stolen from your network to a location that is convenient and useful to him.

Investigative actions

- Check if the traffic is related to SSH activity, it can trigger this alert. It is possible that someone on your network is legitimately engaged in SSH activity.
  Check if the traffic is to/from a misconfigured network.

  Check if the traffic is to a new external service or server that has recently been adopted for use by an organization in your enterprise.
- Identify the process/user performing the data transfer to determine if the transfer is sanctioned.

24.65 | Upload pattern that resembles Peer to Peer traffic

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	30 Minutes
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - Third-Party Firewalls OR - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Command and Control (TA0011) - Initial Access (TA0001)
ATT&CK Technique	Application Layer Protocol (T1071) - Non-Standard Port (T1571) - Trusted Relationship (T1199) - Phishing (T1566)
Severity	Informational

Description

A possible P2P protocol was spotted from an internal host.

Attacker's Goals

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

Investigative actions

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

24.66 | Port Scan

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent OR - Third-Party Firewalls
Detection Modules	
Detector Tags	
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Network Service Discovery (T1046)

Severity	Informational

Description

The endpoint connected, or attempted to connect, to multiple privileged ports (lower than port 1024), which are infrequently used by other endpoints (i.e. destination ports that are normally used by many endpoints will not raise this alert).
Attackers perform port scans for reconnaissance purposes, to find computers or servers that accept connections on these ports, and to find vulnerable services that can be exploited.
Coverage for port scans using data arriving solely from Cortex agents is incomplete.

Attacker's Goals

An attacker is determining which ports are open or closed on remote endpoints in an attempt to identify the endpoint operating system, firewall configuration, and exploitable services.

Investigative actions

- New endpoints that use multiple ports can cause a false positive. Ensure that the endpoint is not new on the network, and is not hosting services such as FTP servers or domain controllers that are being contacted for the first time.
  Check if the activity is a SYN-ACK scan. These might result in Cortex XDR Analytics detecting the scan as coming from the wrong direction, and could mean that Cortex XDR Analytics used the wrong baseline in triggering the alert.
- Check for port map and/or X11 usage. These usually open multiple ports. If the protocol usage for the specific destination is sparse, Cortex XDR Analytics could raise a false alert.

Variations

Port scan by suspicious process

Synopsis

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

Description

The endpoint connected, or attempted to connect, to multiple privileged ports (lower than port 1024), which are infrequently used by other endpoints (i.e. destination ports that are normally used by many endpoints will not raise this alert).

Attackers perform port scans for reconnaissance purposes, to find computers or servers that accept connections on these ports, and to find vulnerable services that can be exploited. Coverage for port scans using data arriving solely from Cortex agents is incomplete.

Attacker's Goals

An attacker is determining which ports are open or closed on remote endpoints in an attempt to identify the endpoint operating system, firewall configuration, and exploitable services.

Investigative actions

New endpoints that use multiple ports can cause a false positive. Ensure that the endpoint is not new on the network, and is not hosting services such as FTP servers or domain controllers that are being contacted for the first time.

Check if the activity is a SYN-ACK scan. These might result in Cortex XDR Analytics detecting the scan as coming from the wrong direction, and could mean that Cortex XDR Analytics used the wrong baseline in triggering the alert.

Check for port map and/or X11 usage. These usually open multiple ports. If the protocol usage for the specific destination is sparse, Cortex XDR Analytics could raise a false alert.

Highly suspicious port scan

Synopsis

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

Description

The endpoint connected, or attempted to connect, to multiple privileged ports (lower than port 1024), which are infrequently used by other endpoints (i.e. destination ports that are normally used by many endpoints will not raise this alert).

Attackers perform port scans for reconnaissance purposes, to find computers or servers that accept connections on these ports, and to find vulnerable services that can be exploited. Coverage for port scans using data arriving solely from Cortex agents is incomplete.

Attacker's Goals

An attacker is determining which ports are open or closed on remote endpoints in an attempt to identify the endpoint operating system, firewall configuration, and exploitable services.

Investigative actions

- New endpoints that use multiple ports can cause a false positive. Ensure that the endpoint is not new on the network, and is not hosting services such as FTP servers or domain controllers that are being contacted for the first time.
- Check if the activity is a SYN-ACK scan. These might result in Cortex XDR Analytics detecting the scan as coming from the wrong direction, and could mean that Cortex XDR Analytics used the wrong baseline in triggering the alert.
- Check for port map and/or X11 usage. These usually open multiple ports. If the protocol usage for the specific destination is sparse, Cortex XDR Analytics could raise a false alert.

Suspicious port scan

Synopsis

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

Description

The endpoint connected, or attempted to connect, to multiple privileged ports (lower than port 1024), which are infrequently used by other endpoints (i.e. destination ports that are normally used by many endpoints will not raise this alert).
Attackers perform port scans for reconnaissance purposes, to find computers or servers that accept connections on these ports, and to find vulnerable services that can be exploited. Coverage for port scans using data arriving solely from Cortex agents is incomplete.

Attacker's Goals

An attacker is determining which ports are open or closed on remote endpoints in an attempt to identify the endpoint operating system, firewall configuration, and exploitable services.

Investigative actions

- New endpoints that use multiple ports can cause a false positive. Ensure that the endpoint is not new on the network, and is not hosting services such as FTP servers or domain controllers that are being contacted for the first time.

  Check if the activity is a SYN-ACK scan. These might result in Cortex XDR Analytics detecting the scan as coming from the wrong direction, and could mean that Cortex XDR Analytics used the wrong baseline in triggering the alert.
  Check for port map and/or X11 usage. These usually open multiple ports. If the protocol usage for the specific destination is sparse, Cortex XDR Analytics could raise a false alert.

24.67 | Rare LDAP enumeration

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
Deduplication Period	1 Day
Required Data	Requires: - Palo Alto Networks Platform Logs
Detection Modules	
Detector Tags	LDAP Analytics
ATT&CK Tactic	Discovery (TA0007)

ATT&CK Technique	Account Discovery (T1087)
Severity	Low

Description

Possible LDAP enumeration with a rare combination of queries.

Attacker's Goals

An adversary may utilize the LDAP protocol to gain information on the Active Directory environment and plan its lateral movement over the network.

Investigative actions

- Where possible, check the legitimacy of the process that executed these LDAP queries.
- Investigate the LDAP search query for any suspicious indicators.
- Determine whether the search query is generic, those search queries (often using wildcards) tend to be more suspicious.

Variations

Rare LDAP enumeration detected

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Account Discovery (T1087)
Severity	Low

Description

Possible LDAP enumeration with a rare combination of queries.

Attacker's Goals

An adversary may utilize the LDAP protocol to gain information on the Active Directory environment and plan its lateral movement over the network.

Investigative actions

- Where possible, check the legitimacy of the process that executed these LDAP queries.
- Investigate the LDAP search query for any suspicious indicators.
- Determine whether the search query is generic, those search queries (often using wildcards) tend to be more suspicious.

24.68 | A user accessed multiple time-consuming websites

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	12 Hours
Deduplication Period	1 Day
Required Data	▮ Requires: - Palo Alto Networks Platform Logs
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Reconnaissance (TA0043)

ATT&CK Technique	Search Open Websites/Domains (T1593)
Severity	Informational

Description

A user was observed visiting multiple domains for personal reasons. Time theft happens when an employee is paid to work but did not actually work during that time. It might affect your business as it reduces the employee's efficiency.

Attacker's Goals

A user may utilize work time for personal reasons.

Investigative actions

- Investigate the domains accessed and how popular they are in the organization.
- Verify that the user is not part of a department that visits these websites as part of daily their operations.

24.69 | New Administrative Behavior

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	12 Hours
Deduplication Period	1 Day

Required Data	- Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent OR - Third-Party Firewalls
Detection Modules	
Detector Tags	NDR Lateral Movement Analytics
ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Services (T1021)
Severity	Medium

Description

The endpoint performed new administrative actions, relative to its previously profiled behavior. It is possible that an endpoint will infrequently be used for administrative activities, so analytics is performed using logs collected over a long period of time, also comparing the activity to that of other endpoints. That is, if many endpoints are contacting the same destination with the same administrative activity, then this network activity is less likely to result in this alert.

An attacker may be operating on the host, probing other computers and moving laterally inside the network using a trusted computer and credentials. Attackers typically exhibit administrative behaviors when performing reconnaissance and lateral movement.

Attacker's Goals

An attacker is using administrative functions to move from one endpoint to another, or to scan the network for new endpoints to attack.

Investigative actions

Investigate the endpoint to determine if it is legitimately being used for administrative functions.

Variations

New SSH Administrative Behavior

Synopsis

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

Description

The endpoint performed new SSH administrative actions, relative to its previously profiled behavior. It is possible that an endpoint will infrequently be used for administrative activities, so analytics is performed using logs collected over a long period of time, also comparing the activity to that of other endpoints. That is, if many endpoints are contacting the same destination with the same administrative activity, then this network activity is less likely to result in this alert.

An attacker may be operating on the host, probing other computers and moving laterally inside the network using a trusted computer and credentials. Attackers typically exhibit administrative behaviors when performing reconnaissance and lateral movement.

Attacker's Goals

An attacker is using administrative functions to move from one endpoint to another, or to scan the network for new endpoints to attack.

Investigative actions

Investigate the endpoint to determine if it is legitimately being used for administrative functions.

24.70 | Failed DNS

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	2 Hours
Deduplication Period	2 Hours
Required Data	Requires one of the following data sources: Palo Alto Networks Platform Logs OR XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Dynamic Resolution: Domain Generation Algorithms (T1568.002)
Severity	Low

Description

The endpoint is performing DNS lookups that are failing at an excessively high rate when compared to its peer group. This alert might be symptomatic of malware that is trying to connect to its command and control (C2) servers.

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

Attacker's Goals

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

Investigative actions

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

24.71 | HTTP with suspicious characteristics

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	2 Hours
Deduplication Period	1 Day

Required Data	- Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	- Command and Control (TA0011) - Exfiltration (TA0010)
ATT&CK Technique	Web Service (T1102) - Exfiltration Over Web Service (T1567)
Severity	Low

Description

Uncommon HTTP communication was performed by the host that might indicate its attempt to hide malicious activities.

Attacker's Goals

Data exfiltration, attack tool staging or command and control channel through a trusted service.

Investigative actions

Examine the legitimacy of the application that produced this uncommon connection.
Examine the parent process of this application.
- Check for anomalies at the time when the communication occurred.

Variations

HTTP with suspicious characteristics which is repetitive

Synopsis

ATT&CK Tactic	Command and Control (TA0011) Exfiltration (TA0010)
ATT&CK Technique	Web Service (T1102) Exfiltration Over Web Service (T1567)
Severity	Low

Description

Repetitevne HTTP communication was performed by the host that might indicate its attempt to hide malicious activities.

Attacker's Goals

Data exfiltration, attack tool staging or command and control channel through a trusted service.

Investigative actions

- Examine the legitimacy of the application that produced this uncommon connection.
- Examine the parent process of this application.
- Check for anomalies at the time when the communication occurred.

HTTP with suspicious characteristics to an IP address

Synopsis

ATT&CK Tactic	Command and Control (TA0011) Exfiltration (TA0010)
ATT&CK Technique	Web Service (T1102) Exfiltration Over Web Service (T1567)
Severity	Low

Description

Uncommon HTTP communication to IP address was performed by the host that might indicate its attempt to hide malicious activities.

Attacker's Goals

Data exfiltration, attack tool staging or command and control channel through a trusted service.

Investigative actions

- Examine the legitimacy of the application that produced this uncommon connection.
- Examine the parent process of this application.
- Check for anomalies at the time when the communication occurred.

HTTP with suspicious characteristics that always fails

Synopsis

ATT&CK Tactic	- Command and Control (TA0011) Exfiltration (TA0010)
ATT&CK Technique	- Web Service (T1102) - Exfiltration Over Web Service (T1567)
Severity	Informational

Description

Unsuccessful HTTP communication to IP address was performed by the host that might indicate its attempt to hide malicious activities.

Attacker's Goals

Data exfiltration, attack tool staging or command and control channel through a trusted service.

Investigative actions

- Examine the legitimacy of the application that produced this uncommon connection.
- Examine the parent process of this application.
- Check for anomalies at the time when the communication occurred.

24.72 | Kerberos User Enumeration

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Account Discovery (T1087)
Severity	Medium

Description

A high amount of Kerberos principal unknown errors were generated on users in the last hour.

This may be indicative of Kerberos user enumeration.

Attacker's Goals

The attacker may attempt to gain an initial foothold in the domain by enumerating users and finding service accounts.

Investigative actions

- Check whether any service principal names (SPNs) were not set correctly, as they will always return a principal unknown error.

24.73 | Failed Connections

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Day
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent OR - Third-Party Firewalls
Detection Modules	
Detector Tags	

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Remote System Discovery (T1018)
Severity	Low

Description

The endpoint has failed connections to other endpoints that have been inactive for more than 24 hours, or that Cortex XDR Analytics has never seen on the network. The endpoint has made an abnormally large number of these failed connections and/or is attempting to connect to an abnormal mixture of missing or inactive endpoints.

Your network might contain legitimate scanners that could cause a false positive for this alert. Cortex XDR Analytics attempts to filter these out by checking if a scanner has been active for a long consecutive period of time. Consequently, if this alert is seen, it represents new activity on your network.

An attacker may be trying to move laterally, or to scan different parts of the network to look for other endpoints that expose a specific service. Worms also perform a similar activity to automatically infect additional hosts in the network.

Attacker's Goals

An attacker does not know your network and is exploring it for new or unknown subnets.

Investigative actions

- Validate that the source is not a sanctioned port scanner.
- Check for suspicious artifacts in the endpoint profile.

Variations

Failed Connections

Synopsis

ATT&CK Tactic	Discovery (TA0007)

ATT&CK Technique	Remote System Discovery (T1018)
Severity	Informational

Description

The endpoint has failed connections to other endpoints that have been inactive for more than 24 hours, or that Cortex XDR Analytics has never seen on the network. The endpoint has made an abnormally large number of these failed connections and/or is attempting to connect to an abnormal mixture of missing or inactive endpoints.

Your network might contain legitimate scanners that could cause a false positive for this alert. Cortex XDR Analytics attempts to filter these out by checking if a scanner has been active for a long consecutive period of time. Consequently, if this alert is seen, it represents new activity on your network.

An attacker may be trying to move laterally, or to scan different parts of the network to look for other endpoints that expose a specific service. Worms also perform a similar activity to automatically infect additional hosts in the network.

Attacker's Goals

An attacker does not know your network and is exploring it for new or unknown subnets.

Investigative actions

- Validate that the source is not a sanctioned port scanner.
  Check for suspicious artifacts in the endpoint profile.

Failed Connections with a rare causality and actor processes relations

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Remote System Discovery (T1018)
Severity	Informational

Description

The endpoint has failed connections to other endpoints that have been inactive for more than 24 hours, or that Cortex XDR Analytics has never seen on the network. The endpoint has made an abnormally large number of these failed connections and/or is attempting to connect to an abnormal mixture of missing or inactive endpoints.

Your network might contain legitimate scanners that could cause a false positive for this alert. Cortex XDR Analytics attempts to filter these out by checking if a scanner has been active for a long consecutive period of time. Consequently, if this alert is seen, it represents new activity on your network.

An attacker may be trying to move laterally, or to scan different parts of the network to look for other endpoints that expose a specific service. Worms also perform a similar activity to automatically infect additional hosts in the network.

These failed connections originated from a rare relation between an actor process and its causality.

Attacker's Goals

An attacker does not know your network and is exploring it for new or unknown subnets.

Investigative actions

Validate that the source is not a sanctioned port scanner.
Check for suspicious artifacts in the endpoint profile.

24.74 | DNS Tunneling

Synopsis

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

Required Data	- Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Command and Control (TA0011) - Exfiltration (TA0010)
ATT&CK Technique	Application Layer Protocol (T1071) - Exfiltration Over Alternative Protocol (T1048)
Severity	Low

Description

10 KB or more were sent encoded in subdomain names during a 10-minute window. All subdomains queried were under a single suspicious domain.

DNS tunneling encodes data in DNS queries and responses, allowing an attacker to bypass firewalls and proxies to reach his or her command and control server, even when HTTP/S traffic is blocked.

The endpoint may be remotely controlled by an attacker, and/or an attacker may have exfiltrated data from it. This detector is not supported when networking events arrive solely from Cortex XDR Linux agents.

Attacker's Goals

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

Investigative actions

Verify that the source device or process is not an approved security solution.

- Verify if the DNS query types are non-standard. DNS tunnels use uncommon query types that enable encoding of more data. Examples include: INIT, PRIVATE, NULL, SRV, KEY, and TXT.

If the affected endpoint is operating Windows, verify that the DNS traffic is coming from svchost.exe and search for other processes that ran when the alert triggered. On Windows, the DNS requests go through svchost.exe.

- Verify the responses per DNS query. Many responses per query may indicate a tool being downloaded.

Verify the destination domain details and compare the number of endpoints in your network that access the domain over time to see if this is an uncommonly contacted domain.

- Verify the source web-browser traffic to determine if the process was generated by user action, if the user did not initiate the traffic it can be indicative of malicious activity.

Verify non-DNS traffic to the domain. Any traffic except DNS queries to the destination domain may indicate a legitimate domain and not used solely for command-and-control or data exfiltration.

Variations

DNS Tunneling

Synopsis

ATT&CK Tactic	Command and Control (TA0011) Exfiltration (TA0010)
ATT&CK Technique	Application Layer Protocol (T1071) Exfiltration Over Alternative Protocol (T1048)
Severity	Medium

Description

10 KB or more were sent encoded in subdomain names during a 10-minute window. All subdomains queried were under a single suspicious domain.

DNS tunneling encodes data in DNS queries and responses, allowing an attacker to bypass firewalls and proxies to reach his or her command and control server, even when HTTP/S traffic is blocked.

The endpoint may be remotely controlled by an attacker, and/or an attacker may have exfiltrated data from it. This detector is not supported when networking events arrive solely from Cortex XDR Linux agents.

Attacker's Goals

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

Investigative actions

Verify that the source device or process is not an approved security solution.

Verify if the DNS query types are non-standard. DNS tunnels use uncommon query types that enable encoding of more data. Examples include: INIT, PRIVATE, NULL, SRV, KEY, and TXT.
If the affected endpoint is operating Windows, verify that the DNS traffic is coming from svchost.exe and search for other processes that ran when the alert triggered. On Windows, the DNS requests go through svchost.exe.

- Verify the responses per DNS query. Many responses per query may indicate a tool being downloaded.
Verify the destination domain details and compare the number of endpoints in your network that access the domain over time to see if this is an uncommonly contacted domain.

Verify the source web-browser traffic to determine if the process was generated by user action, if the user did not initiate the traffic it can be indicative of malicious activity.

- Verify non-DNS traffic to the domain. Any traffic except DNS queries to the destination domain may indicate a legitimate domain and not used solely for command-and-control or data exfiltration.

24.75 | Suspicious DNS traffic

Synopsis

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

Required Data	- Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Command and Control (TA0011) - Exfiltration (TA0010)
ATT&CK Technique	Application Layer Protocol (T1071) - Exfiltration Over Alternative Protocol (T1048)
Severity	Informational

Description

10 KB or more were sent encoded in subdomain names during a 10-minute window. All subdomains queried were under a single suspicious domain.
DNS tunneling encodes data in DNS queries and responses, allowing an attacker to bypass firewalls and proxies to reach his or her command and control server, even when HTTP/S traffic is blocked.

Attacker's Goals

- DNS tunneling, allowing an attacker to bypass firewalls and proxies to reach his or her command and control server, even when HTTP/S traffic is blocked.
  An attacker may also use this protocol to exfiltrated data from the compromised endpoint outside the network.

Investigative actions

Verify that the source device or process is not an approved security solution.

- Verify if the DNS query types are non-standard. DNS tunnels use uncommon query types that enable encoding of more data. Examples include: INIT, PRIVATE, NULL, SRV, KEY, and TXT.

If the affected endpoint is operating Windows, verify that the DNS traffic is coming from svchost.exe and search for other processes that ran when the alert triggered. On Windows, the DNS requests go through svchost.exe.

- Verify the responses per DNS query. Many responses per query may indicate a tool being downloaded.

Verify the destination domain details and compare the number of endpoints in your network that access the domain over time to see if this is an uncommonly contacted domain.

- Verify the source web-browser traffic to determine if the process was generated by user action, if the user did not initiate the traffic it can be indicative of malicious activity.

Verify non-DNS traffic to the domain. Any traffic except DNS queries to the destination domain may indicate a legitimate domain and not used solely for command-and-control or data exfiltration.

Variations

Suspicious DNS traffic with a rarely seen domain

Synopsis

ATT&CK Tactic	Command and Control (TA0011) Exfiltration (TA0010)
ATT&CK Technique	Application Layer Protocol (T1071) Exfiltration Over Alternative Protocol (T1048)
Severity	Low

Description

10 KB or more were sent encoded in subdomain names during a 10-minute window. All subdomains queried were under a single suspicious domain.

DNS tunneling encodes data in DNS queries and responses, allowing an attacker to bypass firewalls and proxies to reach his or her command and control server, even when HTTP/S traffic is blocked.

This domain was rarely seen in this tenant.

Attacker's Goals

DNS tunneling, allowing an attacker to bypass firewalls and proxies to reach his or her command and control server, even when HTTP/S traffic is blocked.

- An attacker may also use this protocol to exfiltrated data from the compromised endpoint outside the network.

Investigative actions

Verify that the source device or process is not an approved security solution.

Verify if the DNS query types are non-standard. DNS tunnels use uncommon query types that enable encoding of more data. Examples include: INIT, PRIVATE, NULL, SRV, KEY, and TXT.
If the affected endpoint is operating Windows, verify that the DNS traffic is coming from svchost.exe and search for other processes that ran when the alert triggered. On Windows,

the DNS requests go through svchost.exe.

- Verify the responses per DNS query. Many responses per query may indicate a tool being downloaded.
Verify the destination domain details and compare the number of endpoints in your network that access the domain over time to see if this is an uncommonly contacted domain.

Verify the source web-browser traffic to determine if the process was generated by user action, if the user did not initiate the traffic it can be indicative of malicious activity.

- Verify non-DNS traffic to the domain. Any traffic except DNS queries to the destination domain may indicate a legitimate domain and not used solely for command-and-control or data exfiltration.

Suspicious DNS traffic with a globally rare DNS query length

Synopsis

ATT&CK Tactic	Command and Control (TA0011) Exfiltration (TA0010)
ATT&CK Technique	Application Layer Protocol (T1071) Exfiltration Over Alternative Protocol (T1048)
Severity	Low

Description

10 KB or more were sent encoded in subdomain names during a 10-minute window. All subdomains queried were under a single suspicious domain.

DNS tunneling encodes data in DNS queries and responses, allowing an attacker to bypass firewalls and proxies to reach his or her command and control server, even when HTTP/S traffic is

blocked.
The combination of the DNS queries along with this root domain is globally rare.

Attacker's Goals

- DNS tunneling, allowing an attacker to bypass firewalls and proxies to reach his or her command and control server, even when HTTP/S traffic is blocked.
  An attacker may also use this protocol to exfiltrated data from the compromised endpoint outside the network.

Investigative actions

- Verify that the source device or process is not an approved security solution.
- Verify if the DNS query types are non-standard. DNS tunnels use uncommon query types that enable encoding of more data. Examples include: INIT, PRIVATE, NULL, SRV, KEY, and TXT.

  If the affected endpoint is operating Windows, verify that the DNS traffic is coming from svchost.exe and search for other processes that ran when the alert triggered. On Windows, the DNS requests go through svchost.exe.
  Verify the responses per DNS query. Many responses per query may indicate a tool being downloaded.

  Verify the destination domain details and compare the number of endpoints in your network that access the domain over time to see if this is an uncommonly contacted domain.
- Verify the source web-browser traffic to determine if the process was generated by user action, if the user did not initiate the traffic it can be indicative of malicious activity.
  Verify non-DNS traffic to the domain. Any traffic except DNS queries to the destination domain may indicate a legitimate domain and not used solely for command-and-control or data exfiltration.

25 | Palo Alto Networks Url Logs

25.1 | Uncommon network tunnel creation

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	N/A (single event)
Deduplication Period	12 Hours
Required Data	Requires: - Palo Alto Networks Url Logs
Detection Modules	
Detector Tags	
ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Protocol Tunneling (T1572)
Severity	Informational

Description

An uncommon network tunnel 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

Uncommon network tunnel creation

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Protocol Tunneling (T1572)
Severity	Informational

Description

An uncommon network tunnel was established using ACS_ssh.exe.

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 tunnel to unpopular IP address

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Protocol Tunneling (T1572)
Severity	Low

Description

An uncommon SSH tunnel was established to an unpopular remote IP address at the organization.

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 network tunnel was established over the default SSH port

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Protocol Tunneling (T1572)
Severity	Low

Description

An unpopular process and command line created a network tunnel over the default 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.

25.2 | Non-browser access to a pastebin-like site

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: Ī Palo Alto Networks Url Logs
Detection Modules	
Detector Tags	
ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Web Service (T1102)
Severity	Low

Description

Non-browser access to a pastebin-like site.

Attacker's Goals

Data exfiltration or attack tool staging.

Investigative actions

- Examine the host to verify that the host was not part of infiltration or data exfiltration from the organization.
Verify that the host doesn't have sensitive company data that can be easily exfiltrated.

Variations

Non-browser access to google sheets API

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Web Service (T1102)
Severity	Low

Description

Non-browser access to google sheets API.

Attacker's Goals

Data exfiltration or attack tool staging.

Investigative actions

Examine the host to verify that the host was not part of infiltration or data exfiltration from the organization.
- Verify that the host doesn't have sensitive company data that can be easily exfiltrated.

Non-browser failed access to a pastebin-like site

Synopsis

ATT&CK Tactic	Command and Control (TA0011)

ATT&CK Technique	Web Service (T1102)
Severity	Low

Description

Non-browser failed access to a pastebin-like site.

Attacker's Goals

Data exfiltration or attack tool staging.

Investigative actions

- Examine the host to verify that the host was not part of infiltration or data exfiltration from the organization.
  Verify that the host doesn't have sensitive company data that can be easily exfiltrated.

Rare non-browser access to a pastebin-like site

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Web Service (T1102)
Severity	Medium

Description

Rare non-browser access to a pastebin-like site.

Attacker's Goals

Data exfiltration or attack tool staging.

Investigative actions

Examine the host to verify that the host was not part of infiltration or data exfiltration from the organization.

- Verify that the host doesn't have sensitive company data that can be easily exfiltrated.

25.3 | Rare connection to external IP address or host by an application using RMI-IIOP or LDAP protocol

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 Url Logs
Detection Modules	
Detector Tags	
ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Application Layer Protocol (T1071)
Severity	Informational

Description

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

Attacker's Goals

Connect to a server to retrieve commands or exfiltrate data.

Investigative actions

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

Variations

Rare connection to external IP address or host by a java application using LDAP protocol

Synopsis

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

Description

A Java Process that never created LDAP connection before connected to an external IP address or host, which is rarely connected to from the organization using LDAP protocol.

Attacker's Goals

Connect to a server to retrieve commands or exfiltrate data.

Investigative actions

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

Rare connection to external IP address or host by a java application using LDAP protocol

Synopsis

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

Description

A Java Process that never created RMI-IIOP connection before connected to an external IP address or host, which is rarely connected to from the organization using LDAP protocol.

Attacker's Goals

Connect to a server to retrieve commands or exfiltrate data.

Investigative actions

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

Rare connection to external IP address or host by a java application using LDAP protocol

Synopsis

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

Description

A Java Process connected to an external IP address or host, which is rarely connected to from the organization using LDAP protocol.

Attacker's Goals

Connect to a server to retrieve commands or exfiltrate data.

Investigative actions

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

Rare connection to external IP address or host by a java application using RMI-IIOP protocol

Synopsis

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

Description

A Java Process connected to an external IP address or host, which is rarely connected to from the organization using RMI-IIOP protocol.

Attacker's Goals

Connect to a server to retrieve commands or exfiltrate data.

Investigative actions

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

25.4 | PowerShell Initiates a Network Connection to GitHub

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 Url Logs
Detection Modules	
Detector Tags	
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Command and Scripting Interpreter: PowerShell (T1059.001)
Severity	Low

Description

PowerShell initiates a Network Connection to GitHub with an uncommon command line. This may have legitimate uses, but this technique is frequently used by attackers to serve malicious payloads.

Attacker's Goals

Download a second stage payload for execution.

Investigative actions

Check if the initiator process is malicious.
Check for additional file/network operations by the same PowerShell instance.

Variations

PowerShell Initiates a Network Connection to GitHub from a sensitive server

Synopsis

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

Description

PowerShell initiates a Network Connection to GitHub with an uncommon command line. This may have legitimate uses, but this technique is frequently used by attackers to serve malicious payloads.

Attacker's Goals

Download a second stage payload for execution.

Investigative actions

Check if the initiator process is malicious.

Check for additional file/network operations by the same PowerShell instance.

25.5 | A non-browser process accessed a website UI

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 Url Logs
Detection Modules	
Detector Tags	
ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Web Service (T1102)
Severity	Informational

Description

An uncommon network communication between a non-browser process and a website UI.

Attacker's Goals

Data exfiltration or attack tool staging.

Investigative actions

- Examine the host to verify that the host was not part of infiltration or data exfiltration from the organization.
  Verify that the host doesn't have sensitive company data that can be easily exfiltrated.

Variations

Suspicious content upload to a known text share website by Non browser process

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Web Service (T1102)
Severity	High

Description

Uncommon data upload to a known text share website through a Non-browser process.

Attacker's Goals

Data exfiltration or attack tool staging.

Investigative actions

- Examine the host to verify that the host was not part of infiltration or data exfiltration from the organization.
  Verify that the host doesn't have sensitive company data that can be easily exfiltrated.

Uncommon data upload to a website through a Non-browser process

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Web Service (T1102)
Severity	Low

Description

Uncommon data upload to a website through a Non browser process.

Attacker's Goals

Data exfiltration or attack tool staging.

Investigative actions

Examine the host to verify that the host was not part of infiltration or data exfiltration from the organization.
Verify that the host doesn't have sensitive company data that can be easily exfiltrated.

Uncommon data download from a known text share website through a Non-browser process

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Web Service (T1102)
Severity	Medium

Description

Uncommon content download from a known text share website through a Non browser process.

Attacker's Goals

Data exfiltration or attack tool staging.

Investigative actions

Examine the host to verify that the host was not part of infiltration or data exfiltration from the organization.

Verify that the host doesn't have sensitive company data that can be easily exfiltrated.

26 | PingOne

26.1 | Suspicious SSO access from ASN

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: - AzureAD OR - Azure SignIn Log OR - Duo OR ▯ Google Workspace Authentication OR - Okta OR I OneLogin OR - PingOne
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 suspicious SSO authentication was made by a user.

Attacker's Goals

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

Investigative actions

- Confirm that the activity is benign (e.g. the user has switched locations and providers).
- Verify if the ASN is an approved ASN to authenticate from.
- Follow further actions done by the user.

Variations

Google Workspace - Suspicious SSO access from ASN

Synopsis

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

Description

A suspicious SSO authentication was made by a user.

Attacker's Goals

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

Investigative actions

Confirm that the activity is benign (e.g. the user has switched locations and providers).

- Verify if the ASN is an approved ASN to authenticate from.
- Follow further actions done by the user.

26.2 | SSO with abnormal user agent

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: - Okta OR - AzureAD OR - Azure SignIn Log OR - Duo OR - PingOne
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 user successfully authenticated via SSO with an abnormal user agent.

Attacker's Goals

Use a legitimate user and authenticate via an SSO service to gain access to the network.

Investigative actions

Confirm that the activity is benign (e.g. the user has really moved to a new user agent app).

Follow actions and suspicious activities regarding the user.

Variations

SSO with an offensive user agent

Synopsis

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

Description

A user successfully authenticated via SSO with an offensive user agent.

Attacker's Goals

Use a legitimate user and authenticate via an SSO service to gain access to the network.

Investigative actions

- Confirm that the activity is benign (e.g. the user has really moved to a new user agent app).
- Follow actions and suspicious activities regarding the user.

26.3 | SSO authentication 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 one of the following data sources: - AzureAD OR - Okta OR - OneLogin OR - PingOne
Detection Modules	Identity Analytics
Detector Tags	Honey User Analytics
ATT&CK Tactic	Initial Access (TA0001)

ATT&CK Technique	Valid Accounts (T1078)
Severity	Low

Description

An SSO authentication attempt was made by a honey user, a decoy account created specifically to detect unauthorized access. This may indicate potential attacker activity.

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

Abnormal SSO authentication by a honey user

Synopsis

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

Description

An SSO authentication attempt was made by a honey user, a decoy account created specifically to detect unauthorized access. This may indicate potential attacker activity.

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.

26.4 | A user connected from a new country

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: - AzureAD OR - Azure SignIn Log OR - Duo OR - Okta OR - OneLogin OR - PingOne

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 connected from an unusual country that the user has not connected from before. This may indicate the account was compromised.

Attacker's Goals

Gain user-account credentials.

Investigative actions

Check if the user is currently located in the aforementioned country, or routed its traffic there via a VPN.

Variations

A user connected from a new country using an anonymized proxy

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 user connected from an unusual country that the user has not connected from before. This may indicate the account was compromised.

Attacker's Goals

Gain user-account credentials.

Investigative actions

Check if the user is currently located in the aforementioned country, or routed its traffic there via a VPN.

26.5 | First SSO access from ASN in organization

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: - AzureAD OR - Azure SignIn Log OR - Duo OR - Google Workspace Authentication OR - Okta OR - OneLogin OR - PingOne
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts: Domain Accounts (T1078.002)
Severity	Informational

Description

An SSO authentication was made with a new ASN.

Attacker's Goals

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

Investigative actions

- Confirm that the activity is benign (e.g. the provider or location is allowed or a new user).
  Verify if the ASN is an approved ASN to authenticate from.
  Follow further actions done by the user.

Variations

First successful SSO access from ASN in the organization

Synopsis

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

Description

An SSO authentication was made with a new ASN.

Attacker's Goals

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

Investigative actions

- Confirm that the activity is benign (e.g. the provider or location is allowed or a new user).
  Verify if the ASN is an approved ASN to authenticate from.
  Follow further actions done by the user.

Google Workspace - First SSO access from ASN in organization

Synopsis

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

Description

An SSO authentication was made with a new ASN.

Attacker's Goals

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

Investigative actions

Confirm that the activity is benign (e.g. the provider or location is allowed or a new user).

Verify if the ASN is an approved ASN to authenticate from.
Follow further actions done by the user.

26.6 | SSO authentication by a machine account

Synopsis

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

Required Data	- Requires one of the following data sources: - AzureAD OR - Azure SignIn Log OR - Duo OR - Okta OR - OneLogin OR - PingOne
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 machine account successfully authenticated via SSO.

Attacker's Goals

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

Investigative actions

- 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.

26.7 | First SSO access from ASN for user

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: - AzureAD OR - Azure SignIn Log OR - Duo OR - Google Workspace Authentication OR - Okta OR - OneLogin OR - PingOne
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 user successfully authenticated via SSO with a new ASN.

Attacker's Goals

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

Investigative actions

- Confirm that the activity is benign (e.g. the user has switched locations and providers).
- Verify if the ASN is an approved ASN to authenticate from.
- Follow further actions done by the user.

Variations

First SSO access from ASN for user using an anonymized proxy

Synopsis

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

Description

A user successfully authenticated via SSO with a new ASN. using an anonymized proxy.

Attacker's Goals

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

Investigative actions

Confirm that the activity is benign (e.g. the user has switched locations and providers).
- Verify if the ASN is an approved ASN to authenticate from.
- Follow further actions done by the user.

Google Workspace - First SSO access from ASN for user

Synopsis

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

Description

A user successfully authenticated via SSO with a new ASN.

Attacker's Goals

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

Investigative actions

- Confirm that the activity is benign (e.g. the user has switched locations and providers).
- Verify if the ASN is an approved ASN to authenticate from.
Follow further actions done by the user.

26.8 | A user logged in at an unusual time via SSO

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	N/A (single event)
Deduplication Period	1 Hour
Required Data	Requires one of the following data sources: - AzureAD OR ▯ Azure SignIn Log OR - Duo OR ▯ Google Workspace Authentication OR - Okta OR - OneLogin OR ▯ PingOne
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

A user connected via SSO on a day and hour that is unusual for this user. This may indicate that the account was compromised.

Attacker's Goals

An attacker is attempting to evade detection.

Investigative actions

- Check the login of the user.
  Check further actions done by the account (e.g. creating files in suspicious locations, creating users, elevating permissions, etc.).

  Check if the user accessing remote resources or connecting to other services.
- Check if the user is logging in from an unusual time zone while traveling.
- Check if the user usually logs in from this country.

Variations

Google Workspace - A user logged in at an unusual time via SSO

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

A user connected via SSO on a day and hour that is unusual for this user. This may indicate that the account was compromised.

Attacker's Goals

An attacker is attempting to evade detection.

Investigative actions

- Check the login of the user.
- Check further actions done by the account (e.g. creating files in suspicious locations, creating users, elevating permissions, etc.).
- Check if the user accessing remote resources or connecting to other services.
- Check if the user is logging in from an unusual time zone while traveling.
- Check if the user usually logs in from this country.

26.9 | User attempted to connect from a suspicious country

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: - AzureAD OR - Azure SignIn Log OR - Duo OR - Okta OR - OneLogin OR - PingOne
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 connected from an unusual country. This may indicate the account was compromised.

Attacker's Goals

Gain user-account credentials.

Investigative actions

Check if the user is currently located in the aforementioned country, or routed its traffic there via a VPN.

Variations

User successfully connected from a suspicious country

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 user successfully connected from an unusual country. This may indicate the account was compromised.

Attacker's Goals

Gain user-account credentials.

Investigative actions

Check if the user is currently located in the aforementioned country, or routed its traffic there via a VPN.

26.10 | First connection from a country in organization

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: - AzureAD OR - Azure SignIn Log OR - Duo OR - Okta OR - OneLogin OR - PingOne
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 connected to an SSO service from an unusual country that no one from this organization has connected from before. This may indicate the account was compromised.

Attacker's Goals

Gain user-account credentials.

Investigative actions

Check if the user is currently located in the aforementioned country, or routed its traffic there via a VPN.

Variations

First successful SSO connection from a country in organization

Synopsis

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 successfully connected from an unusual country that no one from this organization has connected from before. This may indicate the account was compromised.

Attacker's Goals

Gain user-account credentials.

Investigative actions

Check if the user is currently located in the aforementioned country, or routed its traffic there via a VPN.

26.11 | SSO authentication 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 one of the following data sources: - AzureAD OR ▯ Azure SignIn Log OR - Duo OR ▯ Okta OR - OneLogin OR - PingOne
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 successfully authenticated via SSO.

Attacker's Goals

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

Investigative actions

- 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

Rare non-interactive SSO authentication 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 successfully authenticated via SSO.

Attacker's Goals

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

Investigative actions

- 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.

First time SSO authentication by a service account

Synopsis

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

Severity	Medium

Description

A service account successfully authenticated via SSO.

Attacker's Goals

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

Investigative actions

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.

26.12 | A disabled user attempted to authenticate via SSO

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: - AzureAD OR - Azure SignIn Log OR - Duo OR - Okta OR - OneLogin OR - PingOne
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 authenticate via SSO.

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 returned from a long leave of absence).
- Check whether you have issues with your Cloud Identity Engine failing to sync data from Active Directory.

26.13 | First SSO Resource Access in the Organization

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: - AzureAD OR - Azure SignIn Log OR - Duo OR - Okta OR - OneLogin OR - PingOne
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	- Initial Access (TA0001) Discovery (TA0007)
ATT&CK Technique	- Valid Accounts: Domain Accounts (T1078.002) - Cloud Service Discovery (T1526)

Severity	Informational

Description

A resource was accessed for the first time via SSO.

Attacker's Goals

Use a possibly compromised account to access privileged resources.

Investigative actions

- Confirm that the activity is benign (e.g. this is a newly approved resource).
- Follow further actions done by the user that attempted to access the resource.

Variations

Abnormal first access to a resource via SSO in the organization

Synopsis

ATT&CK Tactic	Initial Access (TA0001) Discovery (TA0007)
ATT&CK Technique	Valid Accounts: Domain Accounts (T1078.002) Cloud Service Discovery (T1526)
Severity	Low

Description

A resource was accessed for the first time via SSO with suspicious characteristics.

Attacker's Goals

Use a possibly compromised account to access privileged resources.

Investigative actions

Confirm that the activity is benign (e.g. this is a newly approved resource).

- Follow further actions done by the user that attempted to access the resource.

26.14 | A successful SSO sign-in from TOR

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Hour
Required Data	- Requires one of the following data sources: ▯ AzureAD OR - Azure SignIn Log OR ▯ Duo OR - Okta OR - OneLogin OR ▯ PingOne
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 sign-in 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.

Variations

A successful SSO sign-in from TOR via Mobile Device

Synopsis

ATT&CK Tactic	- Initial Access (TA0001) - Command and Control (TA0011)
ATT&CK Technique	- Proxy: Multi-hop Proxy (T1090.003) - Valid Accounts (T1078)
Severity	Medium

Description

A successful sign-in 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.

26.15 | A user accessed multiple unusual resources via SSO

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - AzureAD OR - Azure SignIn Log OR - Duo OR - Okta OR - OneLogin OR - PingOne

Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Discovery (TA0007) Initial Access (TA0001)
ATT&CK Technique	Valid Accounts (T1078) Cloud Service Dashboard (T1538) Cloud Service Discovery (T1526)
Severity	Informational

Description

A user accessed multiple resources via SSO that are unusual for this user. This may be indicative of a compromised account.

Attacker's Goals

Unusual resources may be accessed for various purposes, including exfiltration, lateral movement, etc.

Investigative actions

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

Variations

A user accessed multiple resources via SSO using an anonymized proxy

Synopsis

ATT&CK Tactic	Discovery (TA0007) Initial Access (TA0001)

ATT&CK Technique	- Valid Accounts (T1078) Cloud Service Dashboard (T1538) Cloud Service Discovery (T1526)
Severity	Medium

Description

A user accessed multiple resources via SSO, using an anonymized proxy, that are unusual for this user. This may be indicative of a compromised account.

Attacker's Goals

Unusual resources may be accessed for various purposes, including exfiltration, lateral movement, etc.

Investigative actions

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

Suspicious user access to multiple resources via SSO

Synopsis

ATT&CK Tactic	- Discovery (TA0007) - Initial Access (TA0001)
ATT&CK Technique	- Valid Accounts (T1078) - Cloud Service Dashboard (T1538) Cloud Service Discovery (T1526)
Severity	Low

Description

A user accessed multiple resources via SSO that are unusual for this user. This may be indicative of a compromised account.

Attacker's Goals

Unusual resources may be accessed for various purposes, including exfiltration, lateral movement, etc.

Investigative actions

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

26.16 | SSO Brute Force

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - AzureAD OR - Azure SignIn Log OR - Duo OR - Okta OR - OneLogin OR - PingOne

Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006) Resource Development (TA0042)
ATT&CK Technique	Brute Force (T1110) Brute Force: Password Guessing (T1110.001) Compromise Accounts (T1586)
Severity	Informational

Description

An abnormally high amount of SSO authentication attempts were seen within a short period of time.
This may have resulted from a brute-force attack.

Attacker's Goals

An attacker is attempting to gain access to an account secured with MFA.

Investigative actions

- Check the legitimacy of this activity and determine whether it is malicious or not.
- Check if the user usually logs in from this country.
- Check whether a successful login was made after unsuccessful attempts.

Variations

SSO Brute Force Threat Detected

Synopsis

ATT&CK Tactic	Credential Access (TA0006) Resource Development (TA0042)

ATT&CK Technique	Brute Force (T1110) Brute Force: Password Guessing (T1110.001) Compromise Accounts (T1586)
Severity	Medium

Description

An abnormally high amount of SSO authentication attempts were seen within a short period of time.
This may have resulted from a brute-force attack.

Attacker's Goals

An attacker is attempting to gain access to an account secured with MFA.

Investigative actions

- Check the legitimacy of this activity and determine whether it is malicious or not.
- Check if the user usually logs in from this country.
- Check whether a successful login was made after unsuccessful attempts.

SSO Brute Force Activity Observed

Synopsis

ATT&CK Tactic	Credential Access (TA0006) Resource Development (TA0042)
ATT&CK Technique	Brute Force (T1110) Brute Force: Password Guessing (T1110.001) Compromise Accounts (T1586)
Severity	Low

Description

An abnormally high amount of SSO authentication attempts were seen within a short period of time.

This may have resulted from a brute-force attack.

Attacker's Goals

An attacker is attempting to gain access to an account secured with MFA.

Investigative actions

- Check the legitimacy of this activity and determine whether it is malicious or not.
  Check if the user usually logs in from this country.
  Check whether a successful login was made after unsuccessful attempts.

26.17 | Impossible traveler - SSO

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	6 Hours
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - AzureAD OR - Azure SignIn Log OR - Duo OR - Okta OR - OneLogin OR - PingOne

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	Low

Description

User connected from several remote countries, at least one of which is not commonly used in the organization, within a short period of time.
This may indicate the account is compromised.

Attacker's Goals

Gain user-account credentials.

Investigative actions

Check if the user routed their traffic via a VPN, or shared their credentials with a remote employee.

Variations

Impossible traveler - non-interactive SSO authentication

Synopsis

ATT&CK Tactic	Credential Access (TA0006) Resource Development (TA0042)

ATT&CK Technique	▮ Compromise Accounts (T1586) Brute Force: Password Guessing (T1110.001)
Severity	Informational

Description

User connected from several remote countries, at least one of which is not commonly used in the organization, within a short period of time.
This may indicate the account is compromised.

Attacker's Goals

Gain user-account credentials.

Investigative actions

Check if the user routed their traffic via a VPN, or shared their credentials with a remote employee.

Possible Impossible traveler via SSO

Synopsis

ATT&CK Tactic	Credential Access (TA0006) Resource Development (TA0042)
ATT&CK Technique	Compromise Accounts (T1586) Brute Force: Password Guessing (T1110.001)
Severity	Informational

Description

User connected from several remote countries, at least one of which is not commonly used in the organization, within a short period of time.
This may indicate the account is compromised.

Attacker's Goals

Gain user-account credentials.

Investigative actions

Check if the user routed their traffic via a VPN, or shared their credentials with a remote employee.

SSO impossible traveler from a VPN or proxy

Synopsis

ATT&CK Tactic	Credential Access (TA0006) Resource Development (TA0042)
ATT&CK Technique	Compromise Accounts (T1586) Brute Force: Password Guessing (T1110.001)
Severity	Informational

Description

User connected from several remote countries, at least one of which is not commonly used in the organization, within a short period of time.
This may indicate the account is compromised.

Attacker's Goals

Gain user-account credentials.

Investigative actions

Check if the user routed their traffic via a VPN, or shared their credentials with a remote employee.

26.18 | SSO Password Spray

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Hour
Required Data	Requires one of the following data sources: - AzureAD OR - Azure SignIn Log OR - Duo OR - Okta OR - OneLogin OR - PingOne
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	- Credential Access (TA0006) Resource Development (TA0042)

ATT&CK Technique	Brute Force: Password Spraying (T1110.003) Brute Force: Password Guessing (T1110.001) Compromise Accounts (T1586)
Severity	Informational

Description

An abnormally high amount of SSO authentication attempts were seen within a short period of time.
This may have resulted from a login password spray attack.

Attacker's Goals

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

Investigative actions

See whether this was a legitimate action.
Check if the user usually logs in from this country.

Check whether a successful login was made after unsuccessful attempts.

Variations

SSO Password Spray Threat Detected

Synopsis

ATT&CK Tactic	Credential Access (TA0006) Resource Development (TA0042)
ATT&CK Technique	Brute Force: Password Spraying (T1110.003) Brute Force: Password Guessing (T1110.001) Compromise Accounts (T1586)
Severity	Medium

Description

An abnormally high amount of SSO authentication attempts were seen within a short period of time.
This may have resulted from a login password spray attack.

Attacker's Goals

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

Investigative actions

- See whether this was a legitimate action.
- Check if the user usually logs in from this country.
- Check whether a successful login was made after unsuccessful attempts.

SSO Password Spray Activity Observed

Synopsis

ATT&CK Tactic	Credential Access (TA0006) Resource Development (TA0042)
ATT&CK Technique	Brute Force: Password Spraying (T1110.003) Brute Force: Password Guessing (T1110.001) Compromise Accounts (T1586)
Severity	Low

Description

An abnormally high amount of SSO authentication attempts were seen within a short period of time.
This may have resulted from a login password spray attack.

Attacker's Goals

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

Investigative actions

See whether this was a legitimate action.

- Check if the user usually logs in from this country.
- Check whether a successful login was made after unsuccessful attempts.

26.19 | Intense SSO failures

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - AzureAD OR - Azure SignIn Log OR - Duo OR - Okta OR - OneLogin OR - PingOne
Detection Modules	Identity Analytics
Detector Tags	

ATT&CK Tactic	▮ Credential Access (TA0006) Initial Access (TA0001)
ATT&CK Technique	▮ Valid Accounts (T1078) ▮ Brute Force: Password Spraying (T1110.003) Brute Force: Password Guessing (T1110.001)
Severity	Informational

Description

An abnormally high amount of SSO authentication attempts were seen within a short period of time.
This could be the outcome of a brute-force login attempt.

Attacker's Goals

An attacker is attempting to gain access to an account secured with MFA.

Investigative actions

Check the legitimacy of this activity and determine whether it is malicious or not.
Check whether a successful login was made after unsuccessful attempts.

Variations

Intense SSO failures with suspicious characteristics

Synopsis

ATT&CK Tactic	Credential Access (TA0006) Initial Access (TA0001)
ATT&CK Technique	Valid Accounts (T1078) Brute Force: Password Spraying (T1110.003) Brute Force: Password Guessing (T1110.001)

Severity	Low

Description

An abnormally high amount of SSO authentication attempts were seen within a short period of time.
This could be the outcome of a brute-force login attempt.

Attacker's Goals

An attacker is attempting to gain access to an account secured with MFA.

Investigative actions

Check the legitimacy of this activity and determine whether it is malicious or not.

Check whether a successful login was made after unsuccessful attempts.

27 | Third-Party Firewalls

27.1 | Recurring access to rare IP

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	21 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	Non-Application Layer Protocol (T1095)
Severity	Low

Description

The endpoint is periodically accessing an external fixed-IP address that its peers rarely use. Access to this external IP address has occurred repeatedly over many 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 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 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 to look for potential artifacts on infected endpoints.

27.2 | 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.

27.3 | 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.

27.4 | 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.

27.5 | 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.

27.6 | 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.

27.7 | 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.

27.8 | 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.

27.9 | 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.

27.10 | 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.

27.11 | 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.

27.12 | 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.

27.13 | 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.

27.14 | 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.

27.15 | Abnormal Recurring Communications to a Rare Domain

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: Palo Alto Networks Platform Logs OR XDR Agent OR Third-Party Firewalls
Detection Modules	

Detector Tags	NDR C2 Detection
ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Non-Application Layer Protocol (T1095)
Severity	Informational

Description

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

Attacker's Goals

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

Investigative actions

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

Variations

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

Synopsis

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

Description

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

Attacker's Goals

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

Investigative actions

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

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

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

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

Synopsis

ATT&CK Tactic	Command and Control (TA0011)

ATT&CK Technique	Non-Application Layer Protocol (T1095)
Severity	Low

Description

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

Attacker's Goals

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

Investigative actions

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

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

Synopsis

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

Description

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

Attacker's Goals

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

Investigative actions

- Identify if the external domain belongs to a reputable organization or an asset used in a public cloud.
  Identify if the source of the traffic is malware. If the source of the traffic is a malicious file,

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

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

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

Synopsis

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

Description

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

Attacker's Goals

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

Investigative actions

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

- Identify if the source of the traffic is malware. If the source of the traffic is a malicious file, Cortex XDR Analytics also raises a malware alert for the file on the endpoint. Malware may contact legitimate domain names, therefore check for unusual apps used, or unusual ports or volumes accessed.

View all related traffic generated by the suspicious process to understand the purpose.

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

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

27.16 | Large Upload (HTTPS)

Synopsis

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

Required Data	- Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent OR - Third-Party Firewalls
Detection Modules	
Detector Tags	
ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Exfiltration Over Alternative Protocol (T1048)
Severity	Low

Description

The endpoint transferred an excessive amount of data to an external site over HTTPS.
The destination is not a popular upload site for endpoints on your network, and the endpoint performing the upload has not previously downloaded a large amount of data from the site.

The upload is considered excessive based on comparison to baseline measurements of HTTPS data transfers on your network.
An attacker may be exfiltrating data directly to the internet.

Attacker's Goals

Transfer data she has stolen from your network to a location that is convenient and useful to her.

Investigative actions

Check if this alert has been falsely triggered by DNS load balancers. If an endpoint routinely uploads data to a site that uses load balancers, the transfer might ordinarily be split into multiple sessions and across multiple subdomains, which can cause the baseline measurement to be incorrect. In that situation, a routine upload that randomly places the bulk of the data in a single session to a single subdomain can look excessive to the Cortex XDR Analytics detector.

- Check if the device performing the data transfer is a mobile phone performing a backup. Cortex XDR Analytics will not always measure the baseline properly for mobile devices, especially if the backups are performed infrequently and contain a great deal of data. If the data transfer is a mobile device running a backup, check to ensure that only appropriate data is included in the backup.
- Identify the process/user performing the data transfer to determine if the transfer is sanctioned.

Variations

Large Upload (HTTPS)

Synopsis

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

Description

The endpoint transferred an excessive amount of data to an external site over HTTPS.
The destination is not a popular upload site for endpoints on your network, and the endpoint performing the upload has not previously downloaded a large amount of data from the site.

The upload is considered excessive based on comparison to baseline measurements of HTTPS data transfers on your network.
An attacker may be exfiltrating data directly to the internet.

Attacker's Goals

Transfer data she has stolen from your network to a location that is convenient and useful to her.

Investigative actions

Check if this alert has been falsely triggered by DNS load balancers. If an endpoint routinely uploads data to a site that uses load balancers, the transfer might ordinarily be split into multiple sessions and across multiple subdomains, which can cause the baseline measurement to be incorrect. In that situation, a routine upload that randomly places the bulk of the data in a single session to a single subdomain can look excessive to the Cortex XDR Analytics detector.

- Check if the device performing the data transfer is a mobile phone performing a backup. Cortex XDR Analytics will not always measure the baseline properly for mobile devices, especially if the backups are performed infrequently and contain a great deal of data. If the data transfer is a mobile device running a backup, check to ensure that only appropriate data is included in the backup.
- Identify the process/user performing the data transfer to determine if the transfer is sanctioned.

27.17 | Spam Bot Traffic

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	3 Days
Deduplication Period	3 Days
Required Data	- Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent OR - Third-Party Firewalls
Detection Modules	

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

Description

The endpoint connected to an excessive number of external SMTP servers.
A spambot may be trying to send spam email using multiple SMTP servers.
Spambots can cause your domain to be blacklisted, and can contain other malicious functionality.
The same mechanism can also be used for exfiltration. Some VPN clients can also tunnel data over SMTP.

Note: This detection model looks for SMTP connections to external servers, but the volume of traffic is not considered. A count is performed based on the number of domains being contacted, as well as the number of unresolved IP addresses.

Attacker's Goals

The attacker uses the host as an SMTP client to send mails and hide their real origin.

Investigative actions

- Verify that the source is not an SMTP server. If Cortex XDR Analytics has failed to identify the process as a valid SMTP server, this alert will be a false positive.
- Verify that IP addresses are actually not being resolved by the non-SMTP process. If the process is performing DNS resolution with a DNS service outside your network, it is possible (depending on your network topology) that Cortex XDR Analytics will not observe that traffic. Because SMTP services typically use numerous IP addresses, this situation could cause a process to exceed a limit when it would otherwise fail to do so.
- If the SMTP connection activity turns out to be the result of malicious file activity, search on the Triage page for other endpoints infected with the file.

Variations

Spam Bot Traffic

Synopsis

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

Description

The endpoint connected to an excessive number of external SMTP servers.
A spambot may be trying to send spam email using multiple SMTP servers.
Spambots can cause your domain to be blacklisted, and can contain other malicious functionality.
The same mechanism can also be used for exfiltration. Some VPN clients can also tunnel data over SMTP.

Note: This detection model looks for SMTP connections to external servers, but the volume of traffic is not considered. A count is performed based on the number of domains being contacted, as well as the number of unresolved IP addresses.

Attacker's Goals

The attacker uses the host as an SMTP client to send mails and hide their real origin.

Investigative actions

Verify that the source is not an SMTP server. If Cortex XDR Analytics has failed to identify the process as a valid SMTP server, this alert will be a false positive.

- Verify that IP addresses are actually not being resolved by the non-SMTP process. If the process is performing DNS resolution with a DNS service outside your network, it is possible (depending on your network topology) that Cortex XDR Analytics will not observe that traffic. Because SMTP services typically use numerous IP addresses, this situation could cause a process to exceed a limit when it would otherwise fail to do so.
- If the SMTP connection activity turns out to be the result of malicious file activity, search on the Triage page for other endpoints infected with the file.

Failed Spam Bot Traffic

Synopsis

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

Description

The endpoint connected to an excessive number of external SMTP servers.
A spambot may be trying to send spam email using multiple SMTP servers.
Spambots can cause your domain to be blacklisted, and can contain other malicious functionality.
The same mechanism can also be used for exfiltration. Some VPN clients can also tunnel data over SMTP.

Note: This detection model looks for SMTP connections to external servers, but the volume of traffic is not considered. A count is performed based on the number of domains being contacted, as well as the number of unresolved IP addresses.

Attacker's Goals

The attacker uses the host as an SMTP client to send mails and hide their real origin.

Investigative actions

Verify that the source is not an SMTP server. If Cortex XDR Analytics has failed to identify the process as a valid SMTP server, this alert will be a false positive.

- Verify that IP addresses are actually not being resolved by the non-SMTP process. If the process is performing DNS resolution with a DNS service outside your network, it is possible (depending on your network topology) that Cortex XDR Analytics will not observe that traffic. Because SMTP services typically use numerous IP addresses, this situation could cause a process to exceed a limit when it would otherwise fail to do so.
- If the SMTP connection activity turns out to be the result of malicious file activity, search on the Triage page for other endpoints infected with the file.

27.18 | Large Upload (SMTP)

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Day
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent OR - Third-Party Firewalls
Detection Modules	
Detector Tags	
ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Exfiltration Over Alternative Protocol (T1048)
Severity	Low

Description

The endpoint, which is not an internal SMTP server, emailed an excessive amount of data from your network.

Attacker's Goals

Transfer data they have stolen from your network to a location that is convenient and useful to him.

Investigative actions

- Identify the process/user performing the data transfer to determine if the transfer is sanctioned.
  Verify that the source is not a mail server.

  Check if the target address represents a mail service that rarely used in the organization. If so, this might indicate on file exfiltration attempt.

Variations

Large Upload (SMTP)

Synopsis

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

Description

The endpoint, which is not an internal SMTP server, emailed an excessive amount of data from your network.

Attacker's Goals

Transfer data they have stolen from your network to a location that is convenient and useful to him.

Investigative actions

Identify the process/user performing the data transfer to determine if the transfer is sanctioned.

Verify that the source is not a mail server.

- Check if the target address represents a mail service that rarely used in the organization. If so, this might indicate on file exfiltration attempt.

27.19 | SSH brute force attempt

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	2 Hours
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - AWS Flow Log OR - AWS OCSF Flow Logs OR - Azure Flow Log OR ▯ Gcp Flow Log OR - Palo Alto Networks Platform Logs OR I Third-Party Firewalls ▮ Requires one of the following data sources: I Palo Alto Networks Platform Logs OR - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)

ATT&CK Technique	Brute Force (T1110)
Severity	Informational

Description

There were multiple attempts to authenticate via SSH to a host in your network. This may indicate a brute force attack.

Attacker's Goals

Attackers attempt to log in to a remote host.

Investigative actions

Audit the failed authentication attempts in the SSH server to identify the abused user. If the abused user can authenticate to the SSH server, it may indicate that the attacker managed to compromise the user credentials.

Variations

SSH brute force network detected from external source

Synopsis

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

Description

There were multiple attempts to authenticate via SSH to a host in your network. This may indicate a brute force attack.

Attacker's Goals

Attackers attempt to log in to a remote host.

Investigative actions

Audit the failed authentication attempts in the SSH server to identify the abused user. If the abused user can authenticate to the SSH server, it may indicate that the attacker managed to compromise the user credentials.

Rare SSH brute force attempt

Synopsis

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

Description

There were multiple attempts to authenticate via SSH to a host in your network. This may indicate a brute force attack.

Attacker's Goals

Attackers attempt to log in to a remote host.

Investigative actions

Audit the failed authentication attempts in the SSH server to identify the abused user. If the abused user can authenticate to the SSH server, it may indicate that the attacker managed to compromise the user credentials.

27.20 | Upload pattern that resembles Peer to Peer traffic

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	30 Minutes
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - Third-Party Firewalls OR - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	- Command and Control (TA0011) - Initial Access (TA0001)
ATT&CK Technique	Application Layer Protocol (T1071) - Non-Standard Port (T1571) - Trusted Relationship (T1199) Phishing (T1566)
Severity	Informational

Description

A possible P2P protocol was spotted from an internal host.

Attacker's Goals

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

Investigative actions

confirm that the port accessed is a P2P port/ is run by a P2P application.
View the downloaded content and determine it's not malicious.

Check for large uploads from this host and check for sensitive information that might not be required on the host.

27.21 | Port Scan

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: ▯ Palo Alto Networks Platform Logs OR - XDR Agent OR - Third-Party Firewalls

Detection Modules	
Detector Tags	
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Network Service Discovery (T1046)
Severity	Informational

Description

The endpoint connected, or attempted to connect, to multiple privileged ports (lower than port 1024), which are infrequently used by other endpoints (i.e. destination ports that are normally used by many endpoints will not raise this alert).
Attackers perform port scans for reconnaissance purposes, to find computers or servers that accept connections on these ports, and to find vulnerable services that can be exploited.
Coverage for port scans using data arriving solely from Cortex agents is incomplete.

Attacker's Goals

An attacker is determining which ports are open or closed on remote endpoints in an attempt to identify the endpoint operating system, firewall configuration, and exploitable services.

Investigative actions

- New endpoints that use multiple ports can cause a false positive. Ensure that the endpoint is not new on the network, and is not hosting services such as FTP servers or domain controllers that are being contacted for the first time.
  Check if the activity is a SYN-ACK scan. These might result in Cortex XDR Analytics detecting the scan as coming from the wrong direction, and could mean that Cortex XDR Analytics used the wrong baseline in triggering the alert.
- Check for port map and/or X11 usage. These usually open multiple ports. If the protocol usage for the specific destination is sparse, Cortex XDR Analytics could raise a false alert.

Variations

Port scan by suspicious process

Synopsis

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

Description

The endpoint connected, or attempted to connect, to multiple privileged ports (lower than port 1024), which are infrequently used by other endpoints (i.e. destination ports that are normally used by many endpoints will not raise this alert).
Attackers perform port scans for reconnaissance purposes, to find computers or servers that accept connections on these ports, and to find vulnerable services that can be exploited.

Coverage for port scans using data arriving solely from Cortex agents is incomplete.

Attacker's Goals

An attacker is determining which ports are open or closed on remote endpoints in an attempt to identify the endpoint operating system, firewall configuration, and exploitable services.

Investigative actions

New endpoints that use multiple ports can cause a false positive. Ensure that the endpoint is not new on the network, and is not hosting services such as FTP servers or domain controllers that are being contacted for the first time.

- Check if the activity is a SYN-ACK scan. These might result in Cortex XDR Analytics detecting the scan as coming from the wrong direction, and could mean that Cortex XDR Analytics used the wrong baseline in triggering the alert.

Check for port map and/or X11 usage. These usually open multiple ports. If the protocol usage for the specific destination is sparse, Cortex XDR Analytics could raise a false alert.

Highly suspicious port scan

Synopsis

ATT&CK Tactic	Discovery (TA0007)

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

Description

The endpoint connected, or attempted to connect, to multiple privileged ports (lower than port 1024), which are infrequently used by other endpoints (i.e. destination ports that are normally used by many endpoints will not raise this alert).
Attackers perform port scans for reconnaissance purposes, to find computers or servers that accept connections on these ports, and to find vulnerable services that can be exploited.
Coverage for port scans using data arriving solely from Cortex agents is incomplete.

Attacker's Goals

An attacker is determining which ports are open or closed on remote endpoints in an attempt to identify the endpoint operating system, firewall configuration, and exploitable services.

Investigative actions

- New endpoints that use multiple ports can cause a false positive. Ensure that the endpoint is not new on the network, and is not hosting services such as FTP servers or domain controllers that are being contacted for the first time.

  Check if the activity is a SYN-ACK scan. These might result in Cortex XDR Analytics detecting the scan as coming from the wrong direction, and could mean that Cortex XDR Analytics used the wrong baseline in triggering the alert.
  Check for port map and/or X11 usage. These usually open multiple ports. If the protocol usage for the specific destination is sparse, Cortex XDR Analytics could raise a false alert.

Suspicious port scan

Synopsis

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

Description

The endpoint connected, or attempted to connect, to multiple privileged ports (lower than port 1024), which are infrequently used by other endpoints (i.e. destination ports that are normally used by many endpoints will not raise this alert).
Attackers perform port scans for reconnaissance purposes, to find computers or servers that accept connections on these ports, and to find vulnerable services that can be exploited.
Coverage for port scans using data arriving solely from Cortex agents is incomplete.

Attacker's Goals

An attacker is determining which ports are open or closed on remote endpoints in an attempt to identify the endpoint operating system, firewall configuration, and exploitable services.

Investigative actions

- New endpoints that use multiple ports can cause a false positive. Ensure that the endpoint is not new on the network, and is not hosting services such as FTP servers or domain controllers that are being contacted for the first time.
- Check if the activity is a SYN-ACK scan. These might result in Cortex XDR Analytics detecting the scan as coming from the wrong direction, and could mean that Cortex XDR Analytics used the wrong baseline in triggering the alert.
- Check for port map and/or X11 usage. These usually open multiple ports. If the protocol usage for the specific destination is sparse, Cortex XDR Analytics could raise a false alert.

27.22 | New Administrative Behavior

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	12 Hours
Deduplication Period	1 Day

Required Data	▮ Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent OR ▯ Third-Party Firewalls
Detection Modules	
Detector Tags	NDR Lateral Movement Analytics
ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Services (T1021)
Severity	Medium

Description

The endpoint performed new administrative actions, relative to its previously profiled behavior. It is possible that an endpoint will infrequently be used for administrative activities, so analytics is performed using logs collected over a long period of time, also comparing the activity to that of other endpoints. That is, if many endpoints are contacting the same destination with the same administrative activity, then this network activity is less likely to result in this alert.

An attacker may be operating on the host, probing other computers and moving laterally inside the network using a trusted computer and credentials. Attackers typically exhibit administrative behaviors when performing reconnaissance and lateral movement.

Attacker's Goals

An attacker is using administrative functions to move from one endpoint to another, or to scan the network for new endpoints to attack.

Investigative actions

Investigate the endpoint to determine if it is legitimately being used for administrative functions.

Variations

New SSH Administrative Behavior

Synopsis

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

Description

The endpoint performed new SSH administrative actions, relative to its previously profiled behavior. It is possible that an endpoint will infrequently be used for administrative activities, so analytics is performed using logs collected over a long period of time, also comparing the activity to that of other endpoints. That is, if many endpoints are contacting the same destination with the same administrative activity, then this network activity is less likely to result in this alert.

An attacker may be operating on the host, probing other computers and moving laterally inside the network using a trusted computer and credentials. Attackers typically exhibit administrative behaviors when performing reconnaissance and lateral movement.

Attacker's Goals

An attacker is using administrative functions to move from one endpoint to another, or to scan the network for new endpoints to attack.

Investigative actions

Investigate the endpoint to determine if it is legitimately being used for administrative functions.

27.23 | Failed Connections

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Day
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Palo Alto Networks Platform Logs OR - XDR Agent OR - Third-Party Firewalls
Detection Modules	
Detector Tags	
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Remote System Discovery (T1018)
Severity	Low

Description

The endpoint has failed connections to other endpoints that have been inactive for more than 24 hours, or that Cortex XDR Analytics has never seen on the network. The endpoint has made an abnormally large number of these failed connections and/or is attempting to connect to an abnormal mixture of missing or inactive endpoints.

Your network might contain legitimate scanners that could cause a false positive for this alert. Cortex XDR Analytics attempts to filter these out by checking if a scanner has been active for a long consecutive period of time. Consequently, if this alert is seen, it represents new activity on your network.

An attacker may be trying to move laterally, or to scan different parts of the network to look for other endpoints that expose a specific service. Worms also perform a similar activity to automatically infect additional hosts in the network.

Attacker's Goals

An attacker does not know your network and is exploring it for new or unknown subnets.

Investigative actions

- Validate that the source is not a sanctioned port scanner.
- Check for suspicious artifacts in the endpoint profile.

Variations

Failed Connections

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Remote System Discovery (T1018)
Severity	Informational

Description

The endpoint has failed connections to other endpoints that have been inactive for more than 24 hours, or that Cortex XDR Analytics has never seen on the network. The endpoint has made an abnormally large number of these failed connections and/or is attempting to connect to an abnormal mixture of missing or inactive endpoints.

Your network might contain legitimate scanners that could cause a false positive for this alert.

Cortex XDR Analytics attempts to filter these out by checking if a scanner has been active for a long consecutive period of time. Consequently, if this alert is seen, it represents new activity on your network.

An attacker may be trying to move laterally, or to scan different parts of the network to look for other endpoints that expose a specific service. Worms also perform a similar activity to automatically infect additional hosts in the network.

Attacker's Goals

An attacker does not know your network and is exploring it for new or unknown subnets.

Investigative actions

Validate that the source is not a sanctioned port scanner.
Check for suspicious artifacts in the endpoint profile.

Failed Connections with a rare causality and actor processes relations

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Remote System Discovery (T1018)
Severity	Informational

Description

The endpoint has failed connections to other endpoints that have been inactive for more than 24 hours, or that Cortex XDR Analytics has never seen on the network. The endpoint has made an abnormally large number of these failed connections and/or is attempting to connect to an abnormal mixture of missing or inactive endpoints.

Your network might contain legitimate scanners that could cause a false positive for this alert. Cortex XDR Analytics attempts to filter these out by checking if a scanner has been active for a long consecutive period of time. Consequently, if this alert is seen, it represents new activity on your network.

An attacker may be trying to move laterally, or to scan different parts of the network to look for other endpoints that expose a specific service. Worms also perform a similar activity to automatically infect additional hosts in the network.

These failed connections originated from a rare relation between an actor process and its causality.

Attacker's Goals

An attacker does not know your network and is exploring it for new or unknown subnets.

Investigative actions

Validate that the source is not a sanctioned port scanner.
Check for suspicious artifacts in the endpoint profile.

28 | Third-Party VPNs

28.1 | A disabled user attempted to log in to a VPN

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 Global Protect OR - Third-Party VPNs
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 disabled user attempted to log in suspiciously to a VPN.

Attacker's Goals

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

Investigative actions

See whether the service authentication was successful.
Confirm that the activity is benign (e.g. a contractor user).
Check whether you have issues with your Cloud Identity Engine failing to sync data from Active Directory.

Variations

Possible VPN login attempt by 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 suspiciously to a VPN.

Attacker's Goals

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

Investigative actions

See whether the service authentication was successful.
Confirm that the activity is benign (e.g. a contractor user).

Check whether you have issues with your Cloud Identity Engine failing to sync data from Active Directory.

28.2 | First VPN access attempt from a country in organization

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 Global Protect OR Third-Party VPNs
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 attempted to connect from an unusual country that no one from this organization has connected from before. This may indicate the account was compromised.

Attacker's Goals

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

Investigative actions

- See whether the service authentication was successful.
- Confirm that the activity is benign (e.g. the user has switched locations and providers).
- Verify if the country is an approved country to connect from.
- Follow further actions done by the user.

Variations

First successful VPN access from a country in organization

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 user successfully connected from an unusual country that no one from this organization has connected from before. This may indicate the account was compromised.

Attacker's Goals

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

Investigative actions

See whether the service authentication was successful.

Confirm that the activity is benign (e.g. the user has switched locations and providers).

- Verify if the country is an approved country to connect from.
- Follow further actions done by the user.

28.3 | VPN 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 one of the following data sources: - Palo Alto Networks Global Protect OR - Third-Party VPNs
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 to a VPN service 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 while, and therefore is 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 if the user initiated other logins aside from a VPN login.

Check whether you have issues with your Cloud Identity Engine failing to sync data from Active Directory.

28.4 | VPN login with a machine account

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Palo Alto Networks Global Protect OR ▯ Third-Party VPNs
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts: Domain Accounts (T1078.002)
Severity	Informational

Description

A machine account successfully logged in to a VPN service.

Attacker's Goals

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

Investigative actions

- See whether the service 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

Rare VPN login with a machine account

Synopsis

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

Description

A machine account successfully logged in to a VPN service.

Attacker's Goals

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

Investigative actions

See whether the service 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.

28.5 | A user connected to a VPN from a new country

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 Global Protect OR - Third-Party VPNs
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 connected to a VPN from an unusual country that the user has not connected from before. This may indicate the account was compromised.

Attacker's Goals

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

Investigative actions

See whether the service authentication was successful.

- Confirm that the activity is benign (e.g. the user has switched locations and providers).
- Verify if the country is an approved country to connect from.

Follow further actions done by the user.

Variations

A user connected to a VPN from a suspicious country

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 user connected to a VPN service from an unusual country. This may indicate the account was compromised.

Attacker's Goals

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

Investigative actions

See whether the service authentication was successful.
Confirm that the activity is benign (e.g. the user has switched locations and providers).

Verify if the country is an approved country to connect from.

- Follow further actions done by the user.

28.6 | A user logged in at an unusual time via VPN

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Hour
Required Data	Requires one of the following data sources: - Palo Alto Networks Global Protect OR - Third-Party VPNs
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

A user connected to a VPN on a day and hour, which is unusual for this user. This may indicate that the account was compromised.

Attacker's Goals

An attacker is attempting to evade detection.

Investigative actions

- Check the amount of traffic and how long it continues.
- Follow further actions done by the user.

28.7 | First VPN access from ASN for user

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 Global Protect OR - Third-Party VPNs
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 user logged in to a VPN with a new ASN.

Attacker's Goals

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

Investigative actions

- Confirm that the activity is benign (e.g. the user has switched locations and providers).
- Verify if the ASN is an approved ASN to authenticate from.
- Follow further actions done by the user.

Variations

Unusual VPN access from ASN

Synopsis

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

Description

An unusual VPN login was made by a user.

Attacker's Goals

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

Investigative actions

- Confirm that the activity is benign (e.g. the user has switched locations and providers).
  Verify if the ASN is an approved ASN to authenticate from.
  Follow further actions done by the user.

28.8 | A Successful VPN connection from TOR

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Hour
Required Data	Requires one of the following data sources: - Palo Alto Networks Global Protect OR ▯ Third-Party VPNs
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 VPN connection 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.

Variations

A Successful VPN connection from TOR via Mobile Device

Synopsis

ATT&CK Tactic	- Initial Access (TA0001) - Command and Control (TA0011)
ATT&CK Technique	- Proxy: Multi-hop Proxy (T1090.003) - Valid Accounts (T1078)
Severity	Medium

Description

A successful VPN connection 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.

28.9 | VPN 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 one of the following data sources: - Palo Alto Networks Global Protect OR - Third-Party VPNs
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 attempted to log in to a VPN service.

Attacker's Goals

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

Investigative actions

See whether the service authentication 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

Rare VPN login by an administrative service account

Synopsis

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

Description

An administrative service account attempted to log in to a VPN service.

Attacker's Goals

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

Investigative actions

See whether the service authentication 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.

28.10 | VPN 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 one of the following data sources: - Palo Alto Networks Global Protect OR ▯ Third-Party VPNs
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 VPN login attempt was made by a honey user, a decoy account created specifically to detect unauthorized access. This may indicate potential attacker activity.

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

Abnormal VPN login by a honey user

Synopsis

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

Description

A VPN login attempt was made by a honey user, a decoy account created specifically to detect unauthorized access. This may indicate potential attacker activity.

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.

28.11 | First VPN access from ASN in organization

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 Global Protect OR ▯ Third-Party VPNs
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 VPN connection was attempted from a new ASN.

Attacker's Goals

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

Investigative actions

- See whether the connection was successful.
  Confirm that the activity is benign (e.g. the provider or location is allowed or a new user).
  Verify if the ASN is an approved ASN to authenticate from.

  Follow further actions done by the user.

28.12 | VPN access with an abnormal operating system

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 Global Protect OR - Third-Party VPNs
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 user accessed a VPN with an abnormal operating system.

Attacker's Goals

Use a legitimate user and connect to a VPN service to gain access to the network.

Investigative actions

- See whether the service authentication was successful.
  Confirm that the activity is benign (e.g. the user has really moved to a new operating system).

  Follow actions and suspicious activities regarding the user.

Variations

VPN access with a suspicious operating system

Synopsis

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

Description

A user accessed a VPN with an abnormal operating system.

Attacker's Goals

Use a legitimate user and connect to a VPN service to gain access to the network.

Investigative actions

See whether the service authentication was successful.

Confirm that the activity is benign (e.g. the user has really moved to a new operating system).

- Follow actions and suspicious activities regarding the user.

VPN access from an abnormal operating system with suspicious characteristics

Synopsis

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

Description

A user accessed a VPN from an abnormal operating system with some more suspicious characteristics that flagged this login attempt as a suspicious login.

Attacker's Goals

Use a legitimate user and connect to a VPN service to gain access to the network.

Investigative actions

- See whether the service authentication was successful.
- Confirm that the activity is benign (e.g. the user has really moved to a new operating system).

Follow actions and suspicious activities regarding the user.

28.13 | Impossible traveler - VPN

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	3 Hours
Deduplication Period	7 Days
Required Data	Requires one of the following data sources: - Palo Alto Networks Global Protect OR - Third-Party VPNs
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	Low

Description

A user connected to a VPN service from multiple remote countries in a short period of time, which should normally be impossible.

This may indicate the account is compromised.

Attacker's Goals

Gain user-account credentials.

Investigative actions

Check if the user routed their traffic via a proxy, or shared their credentials with a remote employee.

Variations

Possible Impossible traveler via VPN

Synopsis

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 connected to a VPN service from multiple remote countries in a short period of time, which should normally be impossible.
This may indicate the account is compromised.

Attacker's Goals

Gain user-account credentials.

Investigative actions

Check if the user routed their traffic via a proxy, or shared their credentials with a remote employee.

VPN impossible traveler from a VPN or proxy

Synopsis

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 connected to a VPN service from multiple remote countries in a short period of time, which should normally be impossible.
This may indicate the account is compromised.

Attacker's Goals

Gain user-account credentials.

Investigative actions

Check if the user routed their traffic via a proxy, or shared their credentials with a remote employee.

VPN impossible traveler with an unusual parameter

Synopsis

ATT&CK Tactic	Credential Access (TA0006) Resource Development (TA0042)
ATT&CK Technique	Compromise Accounts (T1586) Brute Force: Password Guessing (T1110.001)
Severity	Medium

Description

A user connected to a VPN service from multiple remote countries in a short period of time, which should normally be impossible.
This may indicate the account is compromised.

Attacker's Goals

Gain user-account credentials.

Investigative actions

Check if the user routed their traffic via a proxy, or shared their credentials with a remote employee.

28.14 | VPN login Brute-Force attempt

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Day
Required Data	▪ Requires one of the following data sources: - Palo Alto Networks Global Protect OR - Third-Party VPNs
Detection Modules	Identity Analytics
Detector Tags	

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

Description

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

Attacker's Goals

The attacker attempts to gain access to the accounts.

Investigative actions

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

Variations

VPN Login Brute Force

Synopsis

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

Description

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

Attacker's Goals

The attacker attempts to gain access to the accounts.

Investigative actions

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

29 | Windows Event Collector

29.1 | Sensitive account password reset attempt

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: Windows Event Collector OR XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Impact (TA0040)

ATT&CK Technique	Account Access Removal (T1531)
Severity	Informational

Description

An attempt was made to reset a sensitive account's password.

Attacker's Goals

An attacker may attempt to gain access to the account.

Investigative actions

Verify this action with the user who performed the change.

Variations

Sensitive account password reset attempt for the first time

Synopsis

ATT&CK Tactic	Impact (TA0040)
ATT&CK Technique	Account Access Removal (T1531)
Severity	Low

Description

An attempt was made to reset a sensitive account's password.

Attacker's Goals

An attacker may attempt to gain access to the account.

Investigative actions

Verify this action with the user who performed the change.

29.2 | A user certificate was issued with a mismatch

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Persistence (TA0003) Privilege Escalation (TA0004) - Credential Access (TA0006)
ATT&CK Technique	Account Manipulation (T1098) - Valid Accounts (T1078) - Steal or Forge Authentication Certificates (T1649)

Severity	Informational

Description

A certificate was issued to a user who was not the requester, this may indicate a certificate manipulation.

Attacker's Goals

Attackers may try to obtain certificates for privileged accounts or systems they do not normally have access to, to gain elevated access and move laterally within the network.

Investigative actions

- Verify the activity with the performing user.
  Identify if the requester is a user or system that normally requests certificates on behalf of other entities (e.g., a Mobile Device Management system).

  Search for further indicators of potential compromise, including atypical login behaviors, unauthorized attempts at privilege escalation, or lateral movements within the network attributed to the requester.
  Examine whether the mismatch between the requester and the subject is consistent with known and anticipated practices, or if it represents an unusual deviation.

  Check for possible certificate authentications with the subject user.

Variations

Suspicious certificate issuance with a mismatch

Synopsis

ATT&CK Tactic	Persistence (TA0003) Privilege Escalation (TA0004) Credential Access (TA0006)
ATT&CK Technique	Account Manipulation (T1098) Valid Accounts (T1078) Steal or Forge Authentication Certificates (T1649)
Severity	Low

Description

A user certificate was issued with a mismatch. This requester doesn't usually ask for a certificates on behalf of another subject. This may indicate a certificate manipulation.

Attacker's Goals

Attackers may try to obtain certificates for privileged accounts or systems they do not normally have access to, to gain elevated access and move laterally within the network.

Investigative actions

- Verify the activity with the performing user.
- Identify if the requester is a user or system that normally requests certificates on behalf of other entities (e.g., a Mobile Device Management system).
- Search for further indicators of potential compromise, including atypical login behaviors, unauthorized attempts at privilege escalation, or lateral movements within the network attributed to the requester.
- Examine whether the mismatch between the requester and the subject is consistent with known and anticipated practices, or if it represents an unusual deviation.
- Check for possible certificate authentications with the subject user.

29.3 | Mailbox Client Access Setting (CAS) changed

Synopsis

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

Required Data	- Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Data Staged: Local Data Staging (T1074.001)
Severity	Medium

Description

An attacker may use PowerShell to change the Client Access Settings (CAS) for a mailbox, hence gaining access to the data.

Attacker's Goals

Gain access to the data in the compromised mailbox.

Investigative actions

Examine the PowerShell command to identify which mailbox's access setting has been modified.

verify that the change in the client access setting was executed by a trusted source.

29.4 | Service ticket request with a spoofed sAMAccountName

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	3 Hours
Required Data	Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Privilege Escalation (TA0004) Persistence (TA0003)
ATT&CK Technique	Account Manipulation (T1098) Valid Accounts (T1078)
Severity	Medium

Description

A Kerberos service ticket (ST) was requested for an account with a spoofed sAMAccountName.

Attacker's Goals

Elevate privileges from standard domain user to domain admin.

Investigative actions

- Check if the domain controller is patched or vulnerable to the attack.
- Look for associated sAMAccountName rename events.
  Follow actions by the account and if it performed a DCSync.

29.5 | PowerShell used to remove mailbox export request logs

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Execution (TA0002)

ATT&CK Technique	Command and Scripting Interpreter: PowerShell (T1059.001)
Severity	High

Description

An attacker may use PowerShell to remove evidence of an export request for a mailbox as part of the clean-up stage.

Attacker's Goals

Remove evidence for mailbox export commands.

Investigative actions

- Examine the PowerShell command to identify which mailbox has been compromised.
- Investigate the host that executes the command for potential further exploitation.

29.6 | VM Detection attempt

Synopsis

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

Required Data	- Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	- Defense Evasion (TA0005) - Discovery (TA0007)
ATT&CK Technique	Virtualization/Sandbox Evasion: System Checks (T1497.001)
Severity	Informational

Description

A script has executed commands that can be used to detect VM environments.

Attacker's Goals

Avoid malware analysis by identifying execution from within sandboxes and virtual machines.

Investigative actions

Review the script for additional malicious actions.
Check for any additional alerts raised within the same context of the script.

29.7 | 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.

29.8 | Unusual user account unlock

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Initial Access (TA0001)

ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

A user unlocked an account. This user does not usually unlock user accounts.

Attacker's Goals

An attacker may unlock a user account to gain unauthorized access.

Investigative actions

Investigate the associated authentication attempts and login failures (e.g. 4625, 4776 events).

- Check if the user is authorized to unlock accounts.
- Confirm that the user unlock was expected.

Monitor services that may be running with a user's credentials, resulting in lockouts.

Variations

Unusual sensitive user account unlock

Synopsis

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

Description

A user unlocked a sensitive account. This user does not usually unlock user accounts.

Attacker's Goals

An attacker may unlock a user account to gain unauthorized access.

Investigative actions

- Investigate the associated authentication attempts and login failures (e.g. 4625, 4776 events).
- Check if the user is authorized to unlock accounts.
- Confirm that the user unlock was expected.
- Monitor services that may be running with a user's credentials, resulting in lockouts.

29.9 | User account delegation change

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	

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

Description

A user account was modified with delegation to a service.

Attacker's Goals

An attacker may attempt to control an Active Directory environment.

Investigative actions

Verify this action with the user who performed the change.
Check if the account modified is a service account.

Follow actions by the user, including TGT and TGS requests.
Monitor for anomalous Kerberos activity.

Variations

User account delegation to KRBTGT

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Steal or Forge Kerberos Tickets (T1558)
Severity	High

Description

A user account was modified with delegation to the KRBTGT service.

Attacker's Goals

An attacker may attempt to control an Active Directory environment.

Investigative actions

- Verify this action with the user who performed the change.
- Check if the account modified is a service account.
- Follow actions by the user, including TGT and TGS requests.
- Monitor for anomalous Kerberos activity.

User account delegation to a DC

Synopsis

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

Description

A user account was modified with delegation to a service on a domain controller.

Attacker's Goals

An attacker may attempt to control an Active Directory environment.

Investigative actions

- Verify this action with the user who performed the change.
- Check if the account modified is a service account.
- Follow actions by the user, including TGT and TGS requests.
- Monitor for anomalous Kerberos activity.

29.10 | Administrator groups enumerated via LDAP

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: • Windows Event Collector OR • XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	LDAP Analytics (Client)
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Account Discovery (T1087)
Severity	Informational

Description

An LDAP search query that collects information about administrators was executed. This may be indicative of Active Directory domain enumeration, which can be used to perform attacks against the organization.

Attacker's Goals

An attacker is attempting to enumerate Active Directory.

Investigative actions

- Check if the process executes LDAP search queries as part of its normal behavior.
- Investigate the LDAP search query for any suspicious indicators.

29.11 | Rare machine account creation

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)

ATT&CK Technique	Create Account (T1136)
Severity	Informational

Description

A user was observed creating a machine account for the first time.

Attacker's Goals

Persistence using a valid account.

Investigative actions

Verify the activity of the user who created the account.

Follow actions performed by the new machine account.

29.12 | A machine certificate was issued with a mismatch

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Windows Event Collector OR ▯ XDR Agent with eXtended Threat Hunting (XTH)

Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Valid Accounts: Domain Accounts (T1078.002)
Severity	Medium

Description

A machine certificate was issued with a mismatch between the requester and the subject.

Attacker's Goals

An attacker may attempt to exploit the Active Directory Certificate Services to escalate privileges to a domain controller machine account.

Investigative actions

- Check who owns the certificate requester account.
- Check if the requester DNS name attribute was changed recently.
  Investigate actions done by the requester, and its owner.
  Check for possible DCSync alerts.

29.13 | A user was added to a Windows security group

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Persistence (TA0003) Privilege Escalation (TA0004)
ATT&CK Technique	Account Manipulation (T1098) Valid Accounts (T1078)
Severity	Informational

Description

A user was added to a Windows security group.

Attacker's Goals

Privilege escalation using a valid account.

Investigative actions

- Check the user who added the account to the group and verify its activity.

Variations

User added a member to a Windows privileged group for the first time

Synopsis

ATT&CK Tactic	Persistence (TA0003) Privilege Escalation (TA0004)
ATT&CK Technique	Account Manipulation (T1098) Valid Accounts (T1078)
Severity	Medium

Description

A user was added to a Windows security privileged group.

Attacker's Goals

Privilege escalation using a valid account.

Investigative actions

Check the user who added the account to the group and verify its activity.

User added to a Windows privileged group

Synopsis

ATT&CK Tactic	❚ Persistence (TA0003) Privilege Escalation (TA0004)
ATT&CK Technique	❚ Account Manipulation (T1098) Valid Accounts (T1078)
Severity	Low

Description

A user was added to a Windows security privileged group.

Attacker's Goals

Privilege escalation using a valid account.

Investigative actions

- Check the user who added the account to the group and verify its activity.

User removed from a Windows privileged group

Synopsis

ATT&CK Tactic	Persistence (TA0003) Privilege Escalation (TA0004)
ATT&CK Technique	Account Manipulation (T1098) Valid Accounts (T1078)
Severity	Informational

Description

A user was removed from a Windows security privileged group.

Attacker's Goals

Privilege escalation using a valid account.

Investigative actions

- Check the user who removed the account from the group and verify its activity.

A user was removed from a Windows security group

Synopsis

ATT&CK Tactic	Persistence (TA0003) Privilege Escalation (TA0004)
ATT&CK Technique	Account Manipulation (T1098) Valid Accounts (T1078)
Severity	Informational

Description

A user was removed from a Windows security group.

Attacker's Goals

Privilege escalation using a valid account.

Investigative actions

Check the user who removed the account from the group and verify its activity.

29.14 | A user changed the Windows system time

Synopsis

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

Required Data	- Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	System Time Discovery (T1124)
Severity	Informational

Description

A user changed the Windows system time. This may be indicative of a malicious activity and may affect authentication from the source machine.

Attacker's Goals

A malicious insider might change their Windows system time. This action might affect the machine's ability to authenticate to the domain.

Investigative actions

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

29.15 | User added SID History to an account

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Hour
Required Data	Requires one of the following data sources: I Windows Event Collector OR II XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Privilege Escalation (TA0004) Defense Evasion (TA0005)
ATT&CK Technique	Access Token Manipulation: SID-History Injection (T1134.005)
Severity	Informational

Description

A user added SID history to an account. This may be indicative of a user's migration between domains or a SID injection attack.

Attacker's Goals

Adversaries may use SID history to escalate privileges and bypass access controls.

Investigative actions

- Verify if migration between domains was involved.
  Search for suspicious actions by the user, such as forged Kerberos tickets.

Variations

Suspicious SID History Addition

Synopsis

ATT&CK Tactic	▮ Privilege Escalation (TA0004) Defense Evasion (TA0005)
ATT&CK Technique	Access Token Manipulation: SID-History Injection (T1134.005)
Severity	Medium

Description

A user added SID history to an account. The account was not migrated between domains, which may indicate a SID injection attack.

Attacker's Goals

Adversaries may use SID history to escalate privileges and bypass access controls.

Investigative actions

- Verify if migration between domains was involved.
- Search for suspicious actions by the user, such as forged Kerberos tickets.

29.16 | Masquerading as a default local account

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005) Persistence (TA0003)
ATT&CK Technique	Hide Artifacts: Hidden Users (T1564.002) Valid Accounts: Default Accounts (T1078.001) Masquerading (T1036)
Severity	Low

Description

A user created a new local account with the name of a default local account, such as Guest and DefaultAccount.
An attacker may create a user with these known names to evade detection.

Attacker's Goals

An attacker is attempting to evade detection.

Investigative actions

Check what rights and permissions were granted to the new user.

Verify the action with the user who created the new account.

- Follow actions and activities of the newly created default account.
- Monitor the addition of the user to different groups.

Variations

Masquerading as a default local account for the first time

Synopsis

ATT&CK Tactic	▮ Defense Evasion (TA0005) Persistence (TA0003)
ATT&CK Technique	▮ Hide Artifacts: Hidden Users (T1564.002) ▮ Valid Accounts: Default Accounts (T1078.001) Masquerading (T1036)
Severity	Medium

Description

A user created a new local account with the name of a default local account, such as Guest and DefaultAccount.
An attacker may create a user with these known names to evade detection.

Attacker's Goals

An attacker is attempting to evade detection.

Investigative actions

- Check what rights and permissions were granted to the new user.
  Verify the action with the user who created the new account.
  Follow actions and activities of the newly created default account.

  Monitor the addition of the user to different groups.

Masquerading as a default Administrator account

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005) - Persistence (TA0003)
ATT&CK Technique	Hide Artifacts: Hidden Users (T1564.002) Valid Accounts: Default Accounts (T1078.001) - Masquerading (T1036)
Severity	Informational

Description

A user created a new local account with the name of a default local account, such as Guest and

DefaultAccount.
An attacker may create a user with these known names to evade detection.

Attacker's Goals

An attacker is attempting to evade detection.

Investigative actions

Check what rights and permissions were granted to the new user.
Verify the action with the user who created the new account.

Follow actions and activities of the newly created default account.
- Monitor the addition of the user to different groups.

29.17 | Security tools detection attempt

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005) Discovery (TA0007)
ATT&CK Technique	Virtualization/Sandbox Evasion (T1497) Virtualization/Sandbox Evasion: System Checks (T1497.001)
Severity	Informational

Description

A script has executed commands that can be used to detect security tools.

Attacker's Goals

Avoid detection by identifying execution alongside security tools that may alert on a malicious script.

Investigative actions

- Review the script for additional malicious actions.
  Check for any additional alerts raised within the same context of the script.

29.18 | Suspicious modification of the AdminSDHolder's ACL

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)

ATT&CK Technique	Account Manipulation (T1098)
Severity	Low

Description

A user modified the AdminSDHolder ACL, which may be an indication of a privilege escalation attack.

Attacker's Goals

Attackers attempt to obtain full control privileges and then move laterally.

Investigative actions

- Check if a new user was added to the AdminSDHolder object.
- Check if a suspicious user account was recently created.
- Check if a user was added to a privileged group (e.g. Domain Admins).
- Investigate any other potentially suspicious behavior from the compromised user.
- Search for actions that may trigger SDProp, such as modifying the registry or executing an LDAP query.

29.19 | Member added to a Windows local security group

Synopsis

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

Required Data	- Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	- Persistence (TA0003) - Privilege Escalation (TA0004)
ATT&CK Technique	- Account Manipulation (T1098) - Valid Accounts (T1078)
Severity	Informational

Description

A member was added to a Windows local security group.

Attacker's Goals

Privilege escalation using a valid account.

Investigative actions

Check the user who added the account to the group and verify its activity.

Variations

User added to the Windows local Administrator group

Synopsis

ATT&CK Tactic	Persistence (TA0003) Privilege Escalation (TA0004)
ATT&CK Technique	Account Manipulation (T1098) Valid Accounts (T1078)
Severity	Low

Description

A member was added to a Windows local security group.

Attacker's Goals

Privilege escalation using a valid account.

Investigative actions

Check the user who added the account to the group and verify its activity.

Member added to the Windows local Administrator group

Synopsis

ATT&CK Tactic	Persistence (TA0003) Privilege Escalation (TA0004)
ATT&CK Technique	Account Manipulation (T1098) Valid Accounts (T1078)
Severity	Informational

Description

A member was added to a Windows local security group.

Attacker's Goals

Privilege escalation using a valid account.

Investigative actions

Check the user who added the account to the group and verify its activity.

29.20 | A user account was modified to password never expires

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Initial Access (TA0001)
ATT&CK Technique	Valid Accounts (T1078)

Severity	Informational

Description

A user account was modified to password never expires.

Attacker's Goals

An attacker may attempt to gain access to the account.

Investigative actions

- Confirm that the account is not a temporary account that could be exploited by an attacker.
- Verify this action with the user who performed the change.
- Ensure the organization has a strong password aging policy.

Variations

A sensitive account was modified to password never expires

Synopsis

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

Description

A sensitive user account was modified to password never expires. This account is a sensitive account as part of a sensitive built-in Active Directory group.

Attacker's Goals

An attacker may attempt to gain access to the account.

Investigative actions

Confirm that the account is not a temporary account that could be exploited by an attacker.

- Verify this action with the user who performed the change.
- Ensure the organization has a strong password aging policy.

29.21 | Machine account was added to a domain admins group

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	- Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Valid Accounts: Domain Accounts (T1078.002)
Severity	Medium

Description

A machine account was added to a domain admins group.

Attacker's Goals

Privilege escalation using a valid account.

Investigative actions

- Check the user who added the account to the group and verify its activity.

29.22 | Local user account creation

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	- Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Valid Accounts: Local Accounts (T1078.003)
Severity	Informational

Description

A user was observed creating a rare local user account.

Attacker's Goals

Persistence using a valid account.

Investigative actions

Check the user who created the account and verify its activity.
Investigate whether the same account was created on different hosts as part of an installation process.

Variations

Suspicious local user account creation

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Valid Accounts: Local Accounts (T1078.003)
Severity	Low

Description

A user was observed creating a rare local user account. This user has not been seen creating user accounts in the past 30 days.

Attacker's Goals

Persistence using a valid account.

Investigative actions

Check the user who created the account and verify its activity.
Investigate whether the same account was created on different hosts as part of an installation process.

29.23 | Suspicious domain user account creation

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: • Windows Event Collector OR • XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)

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

Description

A user was observed creating a rare domain account.

Attacker's Goals

Persistence using a valid account.

Investigative actions

Check the user who created the account and verify its activity.

29.24 | Suspicious hidden user created

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Windows Event Collector OR ▯ XDR Agent with eXtended Threat Hunting (XTH)

Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Persistence (TA0003) Defense Evasion (TA0005)
ATT&CK Technique	Create Account (T1136) Hide Artifacts: Hidden Users (T1564.002)
Severity	Medium

Description

A user account was created with a name that mimics a machine account.

Attacker's Goals

Evasion using a valid account.

Investigative actions

- Check the user account created and verify its activity.

29.25 | SPNs cleared from a machine account

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Privilege Escalation (TA0004) Persistence (TA0003)
ATT&CK Technique	Account Manipulation (T1098) Valid Accounts (T1078)
Severity	Low

Description

Service principal names were cleared from a machine account.

Attacker's Goals

Elevate privileges from standard domain user to domain admin.

Investigative actions

- Follow actions performed by the user.
- Look for associated sAMAccountName rename events.

Variations

SPNs cleared from a machine account for the first time

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004) Persistence (TA0003)
ATT&CK Technique	Account Manipulation (T1098) Valid Accounts (T1078)
Severity	Medium

Description

Service principal names were cleared from a machine account.

Attacker's Goals

Elevate privileges from standard domain user to domain admin.

Investigative actions

Follow actions performed by the user.

Look for associated sAMAccountName rename events.

29.26 | A user enabled a default local account

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Windows Event Collector OR ▯ XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Initial Access (TA0001) Persistence (TA0003)
ATT&CK Technique	Valid Accounts: Default Accounts (T1078.001) Account Manipulation (T1098)
Severity	Informational

Description

A user enabled a default local account. Enabling a default account may pose a security risk, as they are often exploited by attackers.

Attacker's Goals

An attacker may attempt to gain access to the account and escalate privileges.

Investigative actions

- Check what rights and permissions were granted to the user.
  Verify this action with the user who performed the change.
  Follow actions and activities of the newly enabled default account.

Variations

A user enabled the Windows DefaultAccount

Synopsis

ATT&CK Tactic	Initial Access (TA0001) Persistence (TA0003)
ATT&CK Technique	Valid Accounts: Default Accounts (T1078.001) Account Manipulation (T1098)
Severity	Low

Description

A user enabled the Windows DefaultAccount. Enabling a default account may pose a security risk, as they are often exploited by attackers.

Attacker's Goals

An attacker may attempt to gain access to the account and escalate privileges.

Investigative actions

- Check what rights and permissions were granted to the user.
- Verify this action with the user who performed the change.
- Follow actions and activities of the newly enabled default account.

A user enabled the Windows default Guest account

Synopsis

ATT&CK Tactic	Initial Access (TA0001) Persistence (TA0003)
ATT&CK Technique	Valid Accounts: Default Accounts (T1078.001) Account Manipulation (T1098)

Severity	Low

Description

A user enabled a default local account. Enabling a default account may pose a security risk, as they are often exploited by attackers.

Attacker's Goals

An attacker may attempt to gain access to the account and escalate privileges.

Investigative actions

Check what rights and permissions were granted to the user.
Verify this action with the user who performed the change.

Follow actions and activities of the newly enabled default account.

29.27 | Suspicious sAMAccountName change

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: ▯ Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)

Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Privilege Escalation (TA0004) Persistence (TA0003)
ATT&CK Technique	Account Manipulation (T1098) Valid Accounts (T1078)
Severity	Low

Description

The name of a machine account was changed to a sAMAccountName with a missing trailing dollar sign.

Attacker's Goals

Elevate privileges from standard domain user to domain admin.

Investigative actions

Check if the domain controller is patched or vulnerable to the attack.
Check if any associated TGTs or service tickets were granted.

Follow actions by the account and if it performed a DCSync.

Variations

Suspicious sAMAccountName change to DC hostname

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004) Persistence (TA0003)

ATT&CK Technique	Account Manipulation (T1098) Valid Accounts (T1078)
Severity	Medium

Description

The name of a machine account was changed to a sAMAccountName with a missing trailing dollar sign.

Attacker's Goals

Elevate privileges from standard domain user to domain admin.

Investigative actions

Check if the domain controller is patched or vulnerable to the attack.
Check if any associated TGTs or service tickets were granted.
Follow actions by the account and if it performed a DCSync.

29.28 | A computer account was promoted to DC

Synopsis

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

Required Data	- Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	- Persistence (TA0003) - Privilege Escalation (TA0004)
ATT&CK Technique	- Account Manipulation (T1098) - Valid Accounts (T1078)
Severity	Low

Description

A computer account was promoted to a domain controller via a User Account Control (UAC) change.

Attacker's Goals

An attacker may attempt to gain domain administrator privileges.

Investigative actions

- Verify if the domain controller promotion is expected.
- Check if the computer account is a new account.
- Confirm this action with the user who performed the change.
- Follow actions by the account and if it performed a DCSync.

29.29 | TGT request with a spoofed sAMAccountName - Event

log

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	3 Hours
Required Data	Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Privilege Escalation (TA0004) Persistence (TA0003)
ATT&CK Technique	Account Manipulation (T1098) Valid Accounts (T1078)
Severity	Medium

Description

A Kerberos 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.

29.30 | PowerShell used to export mailbox contents

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Collection (TA0009)

ATT&CK Technique	Data Staged: Local Data Staging (T1074.001)
Severity	Medium

Description

An attacker may use PowerShell to export the contents of a mailbox as part of the data staging before exfiltration.

Attacker's Goals

Export the content of a mailbox, preparing for data exfiltration.

Investigative actions

Examine the PowerShell command to identify which mailbox has been exported.

- verify that this command was executed by a trusted source.

29.31 | Multiple TGT requests for users without Kerberos pre-authentication

Synopsis

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

Required Data	- Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Steal or Forge Kerberos Tickets: AS-REP Roasting (T1558.004)
Severity	Informational

Description

Multiple TGT requests for users that do not require Kerberos pre-authentication were observed. This is typically a sign of an AS-REP 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

An excessive number of TGT requests were sent for users that do not require Kerberos pre-authentication

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Steal or Forge Kerberos Tickets: AS-REP Roasting (T1558.004)
Severity	Low

Description

Multiple TGT requests for users that do not require Kerberos pre-authentication were observed. This is typically a sign of an AS-REP 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.

A TGT request was sent for a user who does not require Kerberos pre-authentication

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Steal or Forge Kerberos Tickets: AS-REP Roasting (T1558.004)
Severity	Informational

Description

A TGT request was sent for a user who does not require Kerberos pre-authentication. This might indicate an AS-REP 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.

29.32 | Multiple user accounts were deleted

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	- Persistence (TA0003) Impact (TA0040)

ATT&CK Technique	• Valid Accounts (T1078) Account Access Removal (T1531)
Severity	Informational

Description

A user deleted multiple user accounts.

Attacker's Goals

Persistence using a valid account.

Investigative actions

Check the user who deleted the accounts and verify the activity.

- Look into the recent activity of the deleted accounts and whether they were temporary or dormant.

Variations

A user deleted multiple users for the first time

Synopsis

ATT&CK Tactic	• Persistence (TA0003) • Impact (TA0040)
ATT&CK Technique	• Valid Accounts (T1078) • Account Access Removal (T1531)
Severity	Low

Description

A user deleted multiple user accounts.

Attacker's Goals

Persistence using a valid account.

Investigative actions

Check the user who deleted the accounts and verify the activity.
Look into the recent activity of the deleted accounts and whether they were temporary or dormant.

29.33 | Multiple suspicious user accounts were created

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)

ATT&CK Technique	Create Account (T1136)
Severity	Low

Description

A user was observed creating multiple rare user accounts.

Attacker's Goals

Persistence using a valid account.

Investigative actions

Check the user who created the accounts and verify the activity.

29.34 | A user printed an unusual number of files

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	2 Hours
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Windows Event Collector OR ▯ XDR Agent with eXtended Threat Hunting (XTH)

Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Exfiltration (TA0010)
ATT&CK Technique	Exfiltration Over Physical Medium (T1052)
Severity	Informational

Description

A user printed an unusual number of files. This may be indicative of malicious activity and an attempt to exfiltrate data.

Attacker's Goals

In an attempt to exfiltrate data, a malicious insider might print an unusual number of files.

Investigative actions

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

29.35 | A user sent multiple TGT requests to irregular service

Synopsis

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

Deduplication Period	1 Day
Required Data	Requires one of the following data sources: ▯ Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Steal or Forge Kerberos Tickets: Kerberoasting (T1558.003)
Severity	Low

Description

A user sent multiple TGT requests to services other than KRBTGT and KADMIN. This 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

A user sent an excessive number of TGT requests to irregular services

Synopsis

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

Description

A user sent multiple TGT requests to services other than KRBTGT and KADMIN. This 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.

A user sent a TGT request to irregular service

Synopsis

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

Description

A user sent a TGT request to a service other than KRBTGT and KADMIN. This might indicate an attempt to perform 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.

29.36 | A user received multiple weakly encrypted service tickets

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Windows Event Collector OR ▯ XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)

ATT&CK Technique	Steal or Forge Kerberos Tickets: Kerberoasting (T1558.003)
Severity	Informational

Description

A user received multiple weakly encrypted service tickets. This 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

Abnormal issuance of weakly encrypted service tickets to a user

Synopsis

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

Description

A user received multiple weakly encrypted service tickets. This 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.

29.37 | User added to a group and removed

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Hours
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	▮ Persistence (TA0003) Privilege Escalation (TA0004)
ATT&CK Technique	▮ Account Manipulation (T1098) Valid Accounts (T1078)

Severity	Informational

Description

A user was added to an Active Directory group and removed within a short period of time, which may be a sign of compromise.

Attacker's Goals

Elevate permissions and establish persistence.

Investigative actions

- Verify the activity with the performing user.
- Confirm that the group addition was not accidental.
  Check for any suspicious actions performed by the added user.
  Check for a possible compromise of the initiating user.

Variations

Rare privileged group addition and removal

Synopsis

ATT&CK Tactic	Persistence (TA0003) Privilege Escalation (TA0004)
ATT&CK Technique	Account Manipulation (T1098) Valid Accounts (T1078)
Severity	Medium

Description

A user was added to an Active Directory privileged group and removed within a short period of time, which may be a sign of compromise.

Attacker's Goals

Elevate permissions and establish persistence.

Investigative actions

- Verify the activity with the performing user.
  Confirm that the group addition was not accidental.

  Check for any suspicious actions performed by the added user.
  Check for a possible compromise of the initiating user.

User added to a privileged group and removed

Synopsis

ATT&CK Tactic	- Persistence (TA0003) - Privilege Escalation (TA0004)
ATT&CK Technique	Account Manipulation (T1098) - Valid Accounts (T1078)
Severity	Low

Description

A user was added to an Active Directory privileged group and removed within a short period of time, which may be a sign of compromise.

Attacker's Goals

Elevate permissions and establish persistence.

Investigative actions

- Verify the activity with the performing user.
  Confirm that the group addition was not accidental.
  Check for any suspicious actions performed by the added user.

  Check for a possible compromise of the initiating user.

29.38 | Excessive user account lockouts

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: • Windows Event Collector OR • XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Brute Force (T1110)
Severity	Low

Description

A high amount of user accounts were locked out in a short time period.

This may be the result of a brute-force or password spray attack.

Attacker's Goals

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

Investigative actions

- Investigate the associated authentication attempts and login failures (e.g. 4625, 4776 events).
  Check if any programs were cached with old credentials, resulting in account lockouts.
  Find the computer responsible for the lockouts and verify if it exists on the domain.
- Monitor services that may be running with a user's credentials.

Variations

Excessive user account lockouts from a suspicious source

Synopsis

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

Description

A high amount of user accounts were locked out in a short time period.
This may be the result of a brute-force or password spray attack.

Attacker's Goals

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

Investigative actions

Investigate the associated authentication attempts and login failures (e.g. 4625, 4776 events).

- Check if any programs were cached with old credentials, resulting in account lockouts.
- Find the computer responsible for the lockouts and verify if it exists on the domain.
  Monitor services that may be running with a user's credentials.

Excessive account lockouts on suspicious users

Synopsis

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

Description

A high amount of user accounts were locked out in a short time period.
This may be the result of a brute-force or password spray attack.

Attacker's Goals

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

Investigative actions

- Investigate the associated authentication attempts and login failures (e.g. 4625, 4776 events).
- Check if any programs were cached with old credentials, resulting in account lockouts.
- Find the computer responsible for the lockouts and verify if it exists on the domain.
- Monitor services that may be running with a user's credentials.

29.39 | A new machine attempted Kerberos delegation

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	12 Hours
Deduplication Period	1 Day
Required Data	Requires one of the following data sources: - Windows Event Collector OR ▯ XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Abuse Elevation Control Mechanism (T1548)
Severity	Medium

Description

A newly created machine attempted to perform a Kerberos delegation. This suspicious activity might indicate a Kerberos relay attack.

Attacker's Goals

Elevate privileges from standard domain user to system.

Investigative actions

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

29.40 | Short-lived user account

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Hour
Required Data	Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Low

Description

A user was created and deleted within a short period of time.

Attacker's Goals

Evasion using a valid account.

Investigative actions

- Check the user who created the account and verify the activity.
  Confirm that the account creation was not accidental.

Variations

Abnormal short-lived user account

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Low

Description

A user was observed creating and deleting an account a short time later. This user does not regularly create and delete accounts.

Attacker's Goals

Evasion using a valid account.

Investigative actions

- Check the user who created the account and verify the activity.
- Confirm that the account creation was not accidental.

Short-lived hidden user account

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Medium

Description

A user was created with a name that mimics a machine account and later deleted within a short period of time. This may be an attacker's attempt to evade detection.

Attacker's Goals

Evasion using a valid account.

Investigative actions

Check the user who created the account and verify the activity.
Confirm that the account creation was not accidental.

29.41 | A user requested multiple service tickets

Synopsis

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

Required Data	- Requires one of the following data sources: - Windows Event Collector OR - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Steal or Forge Kerberos Tickets: Kerberoasting (T1558.003)
Severity	Informational

Description

A user requested multiple service tickets. This 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

Abnormal issuance of service tickets to a user

Synopsis

ATT&CK Tactic	Credential Access (TA0006)

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

Description

A user requested multiple service tickets. This 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.

30 | XDR Agent

30.1 | Recurring access to rare IP

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	21 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	Non-Application Layer Protocol (T1095)
Severity	Low

Description

The endpoint is periodically accessing an external fixed-IP address that its peers rarely use.
Access to this external IP address has occurred repeatedly over many 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 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 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 to look for potential artifacts on infected endpoints.

30.2 | Uncommon communication to an instant messaging 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	Command and Control (TA0011)
ATT&CK Technique	Web Service (T1102)

Severity	Informational

Description

A rare communication between a process to a known instant messaging server.

Attacker's Goals

Data exfiltration or attack tool staging through a trusted service.

Investigative actions

- Examine the legitimacy of the application that made the communication with the provider's server.
- Examine the parent process of this application.
- Check for anomalies regarding the time frame where the communication occurred.

Variations

Uncommon communication to an instant messaging server by a suspicious process

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Web Service (T1102)
Severity	Low

Description

A rare communication by a suspicious process to a known instant messaging server.

Attacker's Goals

Data exfiltration or attack tool staging through a trusted service.

Investigative actions

- Examine the legitimacy of the application that made the communication with the provider's server.
- Examine the parent process of this application.
- Check for anomalies regarding the time frame where the communication occurred.

Uncommon communication to an instant messaging server by an uncommon scripting engine execution

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Web Service (T1102)
Severity	Low

Description

A rare communication by an uncommon execution of a scripting engine to a known instant messaging server.

Attacker's Goals

Data exfiltration or attack tool staging through a trusted service.

Investigative actions

- Examine the legitimacy of the application that made the communication with the provider's server.
- Examine the parent process of this application.
- Check for anomalies regarding the time frame where the communication occurred.

30.3 | Scrcons.exe Rare Child 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) Persistence (TA0003)
ATT&CK Technique	Windows Management Instrumentation (T1047) Event Triggered Execution: Windows Management Instrumentation Event Subscription (T1546.003)
Severity	Informational

Description

The Windows Management Instrumentation (WMI) standard event consumer scrcons.exe executed a rare VBScript or PowerShell script. Executing a rare script can be an indication of local or remote code execution abuse by an attacker.

Attacker's Goals

The attacker is trying to gain Persistence via WMI script registration.

Investigative actions

- Search for any executions of the Managed Object Format (MOF) compiler mofcomp.exe and review the process that ran it.
- Review registered WMI ActiveScriptEventConsumer by running "WMIC /namespace:\\root\default path ActiveScriptEventConsumer get ".

Variations

Scrcons.exe Rare Child Process

Synopsis

ATT&CK Tactic	Execution (TA0002) Persistence (TA0003)
ATT&CK Technique	Windows Management Instrumentation (T1047) Event Triggered Execution: Windows Management Instrumentation Event Subscription (T1546.003)
Severity	Medium

Description

The Windows Management Instrumentation (WMI) standard event consumer scrcons.exe executed a rare VBScript or PowerShell script. Executing a rare script can be an indication of local or remote code execution abuse by an attacker.

Attacker's Goals

The attacker is trying to gain Persistence via WMI script registration.

Investigative actions

- Search for any executions of the Managed Object Format (MOF) compiler mofcomp.exe and review the process that ran it.
Review registered WMI ActiveScriptEventConsumer by running "WMIC

  /namespace:\\root\default path ActiveScriptEventConsumer get
  ".

30.4 | Copy a process memory 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	Kubernetes - AGENT, Containers
ATT&CK Tactic	Credential Access (TA0006)

ATT&CK Technique	OS Credential Dumping: Proc Filesystem (T1003.007)
Severity	High

Description

Copy a process memory file using the dd utility.

Attacker's Goals

Read another process memory, mainly for credential access.

Investigative actions

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

Variations

Copy a process memory file from a Kubernetes pod

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	OS Credential Dumping: Proc Filesystem (T1003.007)
Severity	High

Description

Copy a process memory file using the dd utility.

Attacker's Goals

Read another process memory, mainly for credential access.

Investigative actions

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

30.5 | Signed process performed an unpopular 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 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 injection

Synopsis

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

Description

A signed process performed an unpopular 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 injection

Synopsis

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

Description

A signed process performed an unpopular 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 injection

Synopsis

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

Description

A signed process performed an unpopular 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.

Commonly abused signed process performed a globally unpopular injection to a Microsoft signed process

Synopsis

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

Description

A signed process performed an unpopular 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 injection

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)

ATT&CK Technique	Process Injection (T1055)
Severity	Low

Description

A signed process performed an unpopular 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.

30.6 | Delayed Deletion of 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	Defense Evasion (TA0005)
ATT&CK Technique	Indicator Removal: File Deletion (T1070.004)
Severity	Low

Description

A command line deleting files used the time-out or ping commands to delay the file deletion. This is suspicious, as malware sometimes uses these techniques to cover their tracks.

Attacker's Goals

Evade security controls and possibly 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.

30.7 | Installation of a new System-V service

Synopsis

Activation Period	14 Days
Training Period	30 Days

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

Installation of a new System-V service.

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

Installation of a new System-V service 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

Installation of a new System-V service.

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.

30.8 | Microsoft Office Process Spawning a Suspicious One-Liner

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	Medium

Description

A Microsoft Office process spawned a commonly abused process with a full command (not a script), this is a typically malicious behavior.

Attacker's Goals

An attacker is trying to 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, employees working in finance may have legitimate use cases for complex Excel commands.

30.9 | Uncommon IP Configuration Listing via ipconfig.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 'ipconfig' command is used to display TCP/IP network configuration information and refresh the Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Adversaries may use the command to discover network configuration details.

Attacker's Goals

Attackers can use the ipconfig command to discover network configuration details.

Investigative actions

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

30.10 | Rare NTLM Usage by User

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

Rare authentication by user account to host via NTLM.
The user has not authenticated with NTLM in the past 30 days.
This may be indicative of downgrade attacks from Kerberos to NTLM.

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.

30.11 | Local account 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	Account Discovery: Local Account (T1087.001)
Severity	Informational

Description

One of several local account discovery commands were executed.

Attacker's Goals

Account discovery.

Investigative actions

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

30.12 | Uncommon Remote Monitoring and Management Tool

Synopsis

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

Deduplication Period	1 Day
Required Data	Requires: • XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Remote Access Software (T1219)
Severity	Low

Description

An uncommon Remote Monitoring and Management (RMM) product was observed.

Attacker's Goals

- Accessing a remote machine with full interactive graphic interface capabilities.

Investigative actions

Check if the product usage is approved.

Ask the owners of the machine if they knowingly used this software.
Investigate why the software was being used.

- Check if it was executed remotely or locally.

Variations

Uncommon renamed Remote Monitoring and Management Tool

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Remote Access Software (T1219)
Severity	Medium

Description

An uncommonrenamed Remote Monitoring and Management (RMM) product was observed.

Attacker's Goals

- Accessing a remote machine with full interactive graphic interface capabilities.

Investigative actions

- Check if the product usage is approved.
  Ask the owners of the machine if they knowingly used this software.
  Investigate why the software was being used.

  Check if it was executed remotely or locally.

Uncommon Remote Monitoring and Management Tool (browser origin)

Synopsis

ATT&CK Tactic	Command and Control (TA0011)
ATT&CK Technique	Remote Access Software (T1219)
Severity	Informational

Description

An uncommon Remote Monitoring and Management (RMM) product was observed. (browser origin).

Attacker's Goals

- Accessing a remote machine with full interactive graphic interface capabilities.

Investigative actions

- Check if the product usage is approved.
- Ask the owners of the machine if they knowingly used this software.
- Investigate why the software was being used.
- Check if it was executed remotely or locally.

30.13 | Authentication Attempt From a Dormant Account

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	31 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	Defense Evasion (TA0005)

ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

A dormant user account tried to authenticate to a service using a TGS, after having been unused for a year or more. This may indicate the account is misused by an attacker.

Attacker's Goals

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

Investigative actions

- See whether the service authentication was successful.
- Confirm that the activity is benign (e.g. the user returned from a long leave of absence). Check whether you have issues with your Cloud Identity Engine failing to sync data from Active Directory.

Variations

Authentication Attempt From a Dormant Account to a sensitive server

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Low

Description

A dormant user account tried to authenticate to a service using a TGS, after having been unused for a year or more. This may indicate the account is misused by an attacker on a sensitive server.

Attacker's Goals

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

Investigative actions

See whether the service authentication was successful.
Confirm that the activity is benign (e.g. the user returned from a long leave of absence).

Check whether you have issues with your Cloud Identity Engine failing to sync data from Active Directory.

30.14 | Multiple uncommon SSH Servers with the same Server host key

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	
Detector Tags	

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Adversary-in-the-Middle (T1557)
Severity	Low

Description

Multiple uncommon SSH Servers with the same Server host key.

Attacker's Goals

Attackers may attempt to move laterally within the network by exploiting and relaying stolen client credentials to another SSH server.

Investigative actions

- Audit the authentication attempts to SSH server using the same key.
- Look for unusual or repeated connections from the same or unexpected hosts.
- Audit Client Credentials, check for any signs of compromised client credentials being used on different SSH servers.

30.15 | Globally uncommon injection 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	Injection Analytics, Global Anomaly Analytics
ATT&CK Tactic	Defense Evasion (TA0005) Persistence (TA0003)
ATT&CK Technique	System Binary Proxy Execution (T1218) Process Injection (T1055) Compromise Host Software Binary (T1554)
Severity	Informational

Description

A signed process injected to another process that, on a global level, it usually doesn't inject into.

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 suspicious injection from a signed process

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005) Persistence (TA0003)
ATT&CK Technique	System Binary Proxy Execution (T1218) Process Injection (T1055) Compromise Host Software Binary (T1554)
Severity	Medium

Description

A non-injected thread in a signed process with a suspicious injection type injected to another process that, on a global level, it usually doesn't inject into.

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 injection from a signed process

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005) Persistence (TA0003)
ATT&CK Technique	System Binary Proxy Execution (T1218) Process Injection (T1055) Compromise Host Software Binary (T1554)

Severity	Low

Description

A signed process injected to another process that, on a global level, it usually doesn't inject into.

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.

30.16 | Wsmprovhost.exe Rare Child 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	Lateral Movement (TA0008) Execution (TA0002)
ATT&CK Technique	Remote Services: Windows Remote Management (T1021.006) Command and Scripting Interpreter: PowerShell (T1059.001)
Severity	Low

Description

The PowerShell host wsmprovhost.exe is a proxy process executed remotely through PowerShell when using Windows Remote Management (WinRM). It has executed a rare child process, which may indicate 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 Wsmprovhost.exe on the host for malicious indicators.
- Correlate the initiator process (most likely PowerShell) to the source host and investigate it.

30.17 | Fodhelper.exe UAC bypass

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Privilege Escalation (TA0004)
ATT&CK Technique	Abuse Elevation Control Mechanism: Bypass User Account Control (T1548.002)
Severity	Medium

Description

Attackers may use Fodhelper.exe to bypass UAC (User Account Control) by having it spawn their malicious process.

Attacker's Goals

Gain higher privileges by bypassing the User Account Control (UAC).

Investigative actions

Search for a registry event that changes the key Software\Classes\ms-settings.
- Review the process that made the registry key.
- Check whether the executing process is benign, and if this was a desired behavior as part of its normal execution flow.

30.18 | Suspicious proxy environment variable setting

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	Proxy: Internal Proxy (T1090.001)
Severity	Informational

Description

Suspicious proxy environment variable change or definition with a rare command line.

Attacker's Goals

Adversaries may use an internal proxy to direct command and control traffic between two or more systems in a compromised environment.

Investigative actions

Investigate the process activities and try to understand the network impact os the new proxy setting.

30.19 | Manipulation of netsh helper DLLs Registry keys

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	6 Hours
Required Data	Requires: ▯ XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Event Triggered Execution: Netsh Helper DLL (T1546.007)
Severity	Medium

Description

Registering netsh helper DLLs is uncommon, and could be used by malware for persistence.

Attacker's Goals

Command execution and persistence on the host.

Investigative actions

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

30.20 | Permission Groups discovery commands

Synopsis

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

ATT&CK Technique	Permission Groups Discovery: Local Groups (T1069.001)
Severity	Informational

Description

Permission group discovery command execution.

Attacker's Goals

Collect information about the host.

Investigative actions

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

Verify that this isn't sanctioned IT activity.

- Look for other hosts executing similar commands.

Variations

Permission Groups discovery commands in a Kubernetes pod

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Permission Groups Discovery: Local Groups (T1069.001)
Severity	Informational

Description

Permission group discovery command execution.

Attacker's Goals

Collect information about the host.

Investigative actions

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

30.21 | Remote service command execution from an uncommon source

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	- Requires: - XDR Agent
Detection Modules	
Detector Tags	Impacket Analytics
ATT&CK Tactic	Lateral Movement (TA0008) Execution (TA0002)
ATT&CK Technique	Remote Services (T1021) System Services: Service Execution (T1569.002)

Severity	High

Description

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

Attacker's Goals

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

Investigative actions

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

30.22 | Kubernetes vulnerability scanner 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	Execution (TA0002) Discovery (TA0007)
ATT&CK Technique	Deploy Container (T1610) Container and Resource Discovery (T1613)
Severity	Medium

Description

A Kubernetes cluster was scanned by a known vulnerability scanner.

Attacker's Goals

Usage of known tools and frameworks to exploit Kubernetes clusters.

Investigative actions

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

Variations

Kubernetes vulnerability scanner activity from within a Kubernetes Pod

Synopsis

ATT&CK Tactic	Execution (TA0002) Discovery (TA0007)
ATT&CK Technique	Deploy Container (T1610) Container and Resource Discovery (T1613)
Severity	Medium

Description

A Kubernetes cluster was scanned by a known vulnerability scanner from within a container.

Attacker's Goals

Usage of known tools and frameworks to exploit Kubernetes clusters.

Investigative actions

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

30.23 | Execution of an uncommon process 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

Uncommon execution of an executable found in an early startup stage by Windows system binary.

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 at an early startup stage by Windows system binary 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 by Windows system binary.

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 at an early startup stage by Windows system binary 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 by Windows system binary.

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.

30.24 | Failed Login For Locked-Out Account

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	Defense Evasion (TA0005)
ATT&CK Technique	Valid Accounts (T1078)
Severity	Informational

Description

A locked-out user account (event ID 4725 or 4740) was used in a Kerberos TGT pre-authentication attempt.

Attacker's Goals

Authenticate using the principal in the TGT, not knowing that it has been revoked.

Investigative actions

Check whether you have issues with your Cloud Identity Engine failing to sync data from Active Directory.

- Check whether the attempt to use the principals (user accounts) specified in the alert are legitimate. For example, a user or a script that was not updated that the account has been revoked.

  The lockout can be temporary, for example, in the case of too many login attempts, and may not be visible after the account was released.
- Search for Windows Event Log 4740 to ascertain whether the account was locked out during the time of the alert.

30.25 | Suspicious container orchestration job

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	Execution (TA0002) Persistence (TA0003) - Privilege Escalation (TA0004)

ATT&CK Technique	Scheduled Task/Job: Container Orchestration Job (T1053.007)
Severity	Low

Description

A suspicious orchestration job ran with a rare command line.

Attacker's Goals

Adversaries may abuse task scheduling functionality provided by container orchestration tools

The adversaries do that to schedule deployment of containers configured to execute malicious code.

Investigative actions

Investigate The process activities and impact on the relevant container.

30.26 | Rare process execution in organization

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 in the organization. This may be indicative of a compromised account.

Attacker's Goals

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

Investigative actions

Investigate the process that was executed to determine if it was used for legitimate purposes or malicious activity.

30.27 | Rare process executed by an AppleScript

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	Low

Description

An uncommon process has been executed by the AppleScript interpreter process.

Attacker's Goals

Use the AppleScript interpreter to execute a second stage payload.

Investigative actions

- Analyze the AppleScript and executed process to determine whether they perform any malicious/suspicious actions.
  Check the events generated by the process or its children for potential malicious behavior.

  Check whether the AppleScript was executed in an unusual way.

30.28 | Possible binary padding using dd

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	Obfuscated Files or Information: Binary Padding (T1027.001)
Severity	Informational

Description

A suspicious dd command ran and added data to a binary. This may indicate binary padding to change the hash of a file.

Attacker's Goals

An adversary may use binary padding to avoid hash-based blacklists and static antivirus signatures.

Investigative actions

Check the padded file and try to understand the impact of padding this specific binary.

30.29 | Suspicious disablement of the Windows Firewall

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	Impair Defenses: Disable or Modify System Firewall (T1562.004)

Severity	Medium

Description

The Windows Firewall has been disabled. Malware may turn it off to exfiltrate data and communicate with C2 servers.

Attacker's Goals

An attacker may turn the firewall off to exfiltrate data and communicate with C2 servers.

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 the process is legitimately disabling the firewall.

30.30 | Kubernetes version disclosure

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	7 Days
Required Data	- Requires: - XDR Agent
Detection Modules	

Detector Tags	Kubernetes - AGENT
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Container and Resource Discovery (T1613)
Severity	Informational

Description

The Kubernetes API server was inquired about the Kubernetes version by a process from within a pod.

Attacker's Goals

Usage of the Kubernetes API server to disclose information about the Kubernetes environment.

Investigative actions

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

30.31 | Iptables configuration command 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	Impair Defenses: Disable or Modify System Firewall (T1562.004)
Severity	Informational

Description

The iptables process was executed with a command to add or delete rules on the host.

Attacker's Goals

Adding or deleting system firewalls rules to avoid possible detection.

Investigative actions

Verify that this isn't IT activity.

Look for other hosts executing similar commands.

Variations

Rare iptables port forward command was executed

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)

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

Description

An iptables command was executed to perform port forward, This command is unpopular.

Attacker's Goals

Adding or deleting system firewalls rules to avoid possible detection.

Investigative actions

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

Uncommon iptables port forward command was executed on the host

Synopsis

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

Description

An iptables command was executed to perform port forward, This command is uncommon for the host.

Attacker's Goals

Adding or deleting system firewalls rules to avoid possible detection.

Investigative actions

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

Rare iptables delete command was executed

Synopsis

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

Description

An iptables command was executed to delete rule, This command is unpopular.

Attacker's Goals

Adding or deleting system firewalls rules to avoid possible detection.

Investigative actions

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

A rare iptables delete command was executed on the host

Synopsis

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

Description

An iptables command was executed to delete rule, This command is uncommon for the host.

Attacker's Goals

Adding or deleting system firewalls rules to avoid possible detection.

Investigative actions

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

A rare iptables flush all command was executed

Synopsis

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

Description

An iptables command was executed to flush all rules, This command is unpopular.

Attacker's Goals

Adding or deleting system firewalls rules to avoid possible detection.

Investigative actions

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

A rare iptables flush command was executed

Synopsis

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

Severity	Low

Description

An iptables command was executed to flush all rules, This command is unpopular.

Attacker's Goals

Adding or deleting system firewalls rules to avoid possible detection.

Investigative actions

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

A rare iptables flush command was executed on the host

Synopsis

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

Description

An iptables command was executed to flush rules, This command is uncommon for the host.

Attacker's Goals

Adding or deleting system firewalls rules to avoid possible detection.

Investigative actions

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

30.32 | Suspicious setspn.exe 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	Credential Access (TA0006)
ATT&CK Technique	Steal or Forge Kerberos Tickets (T1558)
Severity	Low

Description

A Service Principal Name (SPN) is a unique identifier for a service, mapped to a specific account. Setspn.exe can be used to retrieve SPN information, which may indicate an attacker's attempt to "Kerberoast".

Attacker's Goals

Retrieving SPN information to perform related attacks like 'Kerberoast'.

Investigative actions

- Investigate the user who executed setspn.exe and find out if the act was malicious.

30.33 | Registration of Uncommon .NET Services and/or Assemblies

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: Regsvcs/Regasm (T1218.009)

Severity	Informational

Description

Regasm.exe and regsvcs.exe are used to register .NET COM assemblies, which are typically located in specific paths, attackers might leverage that to execute code within a Microsoft signed binary.

Attacker's Goals

Load untrusted code into a trusted Microsoft context to evade detection.

Investigative actions

- Verify if the loaded dll is known to be malicious.
  Track down which process dropped the library being loaded.
  Validate if the actions being done by the regasm.exe process are malicious.

30.34 | Command running with COMSPEC in the command line argument

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: Windows Command Shell (T1059.003)
Severity	Low

Description

COMSPEC is an environmental variable that points to cmd.exe. Attackers may use this command to obfuscate their command and avoid detection.

Attacker's Goals

Attackers might use environment variables to try and avoid being detected and obfuscate their commands.

Investigative actions

Investigate the actor and the command line that executed with COMSPEC Verify that the command executed from a trusted source.

30.35 | Conhost.exe spawned a suspicious cmd process

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent
Detection Modules	
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	System Binary Proxy Execution (T1218)
Severity	Low

Description

Attackers may abuse the conhost process to execute malicious files and evade detection.

Attacker's Goals

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

Investigative actions

An adversary may use the conhost process to evade detection.

Variations

Conhost.exe spawned a suspicious child process

Synopsis

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

Description

Attackers may abuse the conhost process to execute malicious files and evade detection.

Attacker's Goals

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

Investigative actions

An adversary may use the conhost process to evade detection.

30.36 | Encoded information using Windows certificate management tool

Synopsis

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