ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Command and Scripting Interpreter: AutoHotKey & AutoIT (T1059.010) ❚ Command and Scripting Interpreter: Windows Command Shell (T1059.003)
Severity	Informational

Description

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

Attacker's Goals

Gain code execution on the host and evade security controls.

Investigative actions

- Check whether the command line executed is benign or normal for the host and/or user performing it.
  Check whether the user from the command line is an administrator or other sensitive account.

31.62 | Editing ld.so.preload for persistence and 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 with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Hijack Execution Flow: Dynamic Linker Hijacking (T1574.006)
Severity	Low

Description

Attackers may modify ld.so.preload to load their malicious code into every dynamically linked process.

Attacker's Goals

Gain persistence and inject itself into every program on the system.

Investigative actions

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

- Download the /etc/ld.so.preload file from the host and see if and what libraries are specified there.
  Download any library specified and see if it's benign.

31.63 | 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.

31.64 | A user created a pfx file for the first time

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials: Credentials In Files (T1552.001)
Severity	Informational

Description

A user created a pfx file for the first time.

Attacker's Goals

Attackers may export certificates to pfx files to use them for authentication, persistence or NTLM extraction.

Investigative actions

- Check if the pfx creation is legitimate for the user (testing, IT, etc.).
- Follow further actions done by the user (ex. authentication using certificates).

Variations

A user created a pfx in a suspicious folder for the first time

Synopsis

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

Description

A user created a pfx in a suspicious folder which is publicly accessible, for the first time.

Attacker's Goals

Attackers may export certificates to pfx files to use them for authentication, persistence or NTLM extraction.

Investigative actions

- Check if the pfx creation is legitimate for the user (testing, IT, etc.).
- Follow further actions done by the user (ex. authentication using certificates).

31.65 | 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.

31.66 | Unusual process accessed web browser cookies

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	Credentials Grabbing Analytics
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Steal Web Session Cookie (T1539)
Severity	Informational

Description

An unusual process has accessed a web browser's session cookie store.

Attacker's Goals

Obtain access to or hijack sessions to websites stored in the web browser's cookies.

Investigative actions

- Determine whether it is legitimate for the process to access session cookies directly.
- Analyze the process/application that accessed the cookie store.
  Check for any other suspicious actions that were performed by the process.
  Look for unusual access to resources using credentials cached in the web browser/cookie store.

Variations

Unusual unsigned process accessed web browser cookies

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Steal Web Session Cookie (T1539)
Severity	Low

Description

An unusual process has accessed a web browser's session cookie store.

Attacker's Goals

Obtain access to or hijack sessions to websites stored in the web browser's cookies.

Investigative actions

- Determine whether it is legitimate for the process to access session cookies directly.
  Analyze the process/application that accessed the cookie store.
  Check for any other suspicious actions that were performed by the process.

  Look for unusual access to resources using credentials cached in the web browser/cookie store.

31.67 | Executable or Script file written by a web server process

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Initial Access (TA0001) Persistence (TA0003)
ATT&CK Technique	External Remote Services (T1133) Server Software Component: Web Shell (T1505.003)
Severity	Informational

Description

An uncommon executable or script file was created, written or renamed by a web server process.

Attacker's Goals

Gaining the ability to execute commands on the host, as well as persistence.

Investigative actions

- Investigate the web server access logs for suspicious behavior.
- Check if the dropped file contains malicious content.

Variations

The driver file written by a web server process

Synopsis

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

Description

An uncommon driver file was created, written or renamed by a web server process.

Attacker's Goals

Gaining the ability to execute commands on the host, as well as persistence.

Investigative actions

- Investigate the web server access logs for suspicious behavior.
- Check if the dropped file contains malicious content.

Executable or Script file written by a web server process in an internet facing server

Synopsis

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

Description

An uncommon executable or script file was created, written or renamed by a web server process.

Attacker's Goals

Gaining the ability to execute commands on the host, as well as persistence.

Investigative actions

- Investigate the web server access logs for suspicious behavior.
- Check if the dropped file contains malicious content.

Executable or Script file written by a web server process with connections from various sources and high web traffic

Synopsis

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

Description

An uncommon executable or script file was created, written or renamed by a web server process.

Attacker's Goals

Gaining the ability to execute commands on the host, as well as persistence.

Investigative actions

Investigate the web server access logs for suspicious behavior.
Check if the dropped file contains malicious content.

31.68 | Sensitive browser credential files accessed by a rare non browser process

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	3 Days
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Credentials from Password Stores: Credentials from Web Browsers (T1555.003)
Severity	Low

Description

Sensitive browser credential files accessed by a rare non browser process.

Attacker's Goals

Accessing these files is done by attackers to collect user credentials.

Investigative actions

Investigate the actor process to determine if it was used for legitimate purposes or malicious activity.

31.69 | Suspicious process accessed certificate files

Synopsis

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

Required Data	- Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	- Unsecured Credentials (T1552) Steal or Forge Authentication Certificates (T1649)
Severity	Low

Description

A suspicious process accessed certificate files.

Attacker's Goals

Attackers may search for local certificate files for authentication, persistence or NTLM extraction.

Investigative actions

See whether this was a legitimate action.

- Follow process/user activities.

31.70 | 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.

31.71 | Suspicious usage of Microsoft's Active Directory PowerShell module remote discovery cmdlet

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Remote System Discovery (T1018)
Severity	Informational

Description

An attacker may use one of Microsoft's Active Directory PowerShell module remote discovery cmdlet to reconnaissance the network.

Attacker's Goals

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

Investigative actions

- Check whether the executing process is benign, and if this was a desired behavior as part of its normal execution flow.
- Understand what information the attacker had gathered from the command and investigate relevant assets.

31.72 | A remote service was created via RPC over SMB

Synopsis

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

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

Description

A remote service was created via RPC over SMB.

Attacker's Goals

Process creation on a remote host.

Investigative actions

Check whether the new process is benign, and that the new process is not doing suspicious activity.

Variations

A remote service with an uncommon name was created via RPC over SMB

Synopsis

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

Severity	Medium

Description

A remote service was created via RPC over SMB.

Attacker's Goals

Process creation on a remote host.

Investigative actions

Check whether the new process is benign, and that the new process is not doing suspicious activity.

31.73 | Unusual process accessed a crypto wallet's files

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	Sensitive Information Stealing Analytics

ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Data from Local System (T1005)
Severity	Low

Description

An unusual process has accessed files belonging to a cryptocurrency wallet.

Attacker's Goals

Obtain access to cryptocurrency stored in the wallet.

Investigative actions

Determine whether it is legitimate for the process to access such files.
Analyze the process/application that accessed the file.

Check for any other suspicious actions that were performed by the process.
Audit the usage of the cryptocurrency stored in the wallet.

31.74 | Possible use of a networking driver for network sniffing

Synopsis

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

Required Data	- Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006) Discovery (TA0007)
ATT&CK Technique	Network Sniffing (T1040)
Severity	Informational

Description

A process wrote a known networking driver with network sniffing capabilities to disk, attackers can use it to sniff passwords and other credentials from the network.

Attacker's Goals

Read raw network data over promiscuous mode, this can allow the attacker the capabilities to sniff passwords and other credentials from the organization's network, in other cases also interfere with the network.

Investigative actions

Verify if the process is known for the IT/ User.
Check if the driver installed recently, if it was installed with sc.exe this action can be malicious (check who ran sc.exe to verify that).

Variations

Possible use of a networking driver for network sniffing

Synopsis

ATT&CK Tactic	Credential Access (TA0006) Discovery (TA0007)
ATT&CK Technique	Network Sniffing (T1040)
Severity	Medium

Description

A process wrote a known and rare networking driver with network sniffing capabilities to not standard location for drivers on the disk, attackers can use it to sniff passwords and other credentials from the network.

Attacker's Goals

Read raw network data over promiscuous mode, this can allow the attacker the capabilities to sniff

passwords and other credentials from the organization's network, in other cases also interfere with the network.

Investigative actions

- Verify if the process is known for the IT/ User.
  Check if the driver installed recently, if it was installed with sc.exe this action can be malicious (check who ran sc.exe to verify that).

Possible use of a networking driver for network sniffing

Synopsis

ATT&CK Tactic	Credential Access (TA0006) Discovery (TA0007)
ATT&CK Technique	Network Sniffing (T1040)
Severity	Low

Description

A process wrote a known networking driver with network sniffing capabilities to not standard location for drivers on the disk, attackers can use it to sniff passwords and other credentials from the network.

Attacker's Goals

Read raw network data over promiscuous mode, this can allow the attacker the capabilities to sniff passwords and other credentials from the organization's network, in other cases also interfere with the network.

Investigative actions

- Verify if the process is known for the IT/ User.
  Check if the driver installed recently, if it was installed with sc.exe this action can be malicious (check who ran sc.exe to verify that).

31.75 | An uncommon file was created in the startup folder

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	7 Days
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	

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

Description

An uncommon file was created in the startup folder.

Attacker's Goals

Persistence on the host.

Investigative actions

Check if the file was written during an installation of a legitimate application (what other files that were written by the process).
Check what program opens this file by the extension - Check the registry at

HKEY_CLASSES_ROOT.[extension]\shell\[action]\command for the default application or command to execute.

Variations

An executable file with a non-default extension was added to the startup folder

Synopsis

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

Severity	Medium

Description

An executable file with a non-default extension was added to the startup folder.

Attacker's Goals

Persistence on the host.

Investigative actions

- Check if the file was written during an installation of a legitimate application (what other files that were written by the process).
  Check what program opens this file by the extension - Check the registry at

  HKEY_CLASSES_ROOT.[extension]\shell\[action]\command for the default application or command to execute.

An executable or script was added to the startup folder

Synopsis

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

Description

An executable or script was added to the startup folder, which may happen on new program installation, but may also indicate a malicious program persisting itself.

Attacker's Goals

Persistence on the host.

Investigative actions

Check if the file was written during an installation of a legitimate application (what other files that were written by the process).

- Check what program opens this file by the extension - Check the registry at HKEY_CLASSES_ROOT.[extension]\shell\[action]\command for the default application or command to execute.

A file with an uncommon extension was added to the startup folder

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Event Triggered Execution: Change Default File Association (T1546.001) Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)
Severity	Low

Description

A file with an uncommon extension was added to the startup folder, which may happen on new program installation, but may also indicate a malicious program persisting itself.

Attacker's Goals

Persistence on the host.

Investigative actions

- Check if the file was set during installation process (what other files were written by the process).
  Check the registry at HKEY_CLASSES_ROOT.[extension]\shell\[action]\command for the default application or command to execute.

A new shortcut (lnk) was added to the startup folder

Synopsis

ATT&CK Tactic	Persistence (TA0003)

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

Description

A new shortcut (lnk) file was added to the startup folder, which may happen on new program installation, but may also indicate a malicious program persisting itself.

Attacker's Goals

Persistence on the host.

Investigative actions

- Check if the file was written during an installation of a legitimate application (what other files that were written by the process).
  Check what program opens this file by the extension - Check the registry at
  HKEY_CLASSES_ROOT.[extension]\shell\[action]\command for the default application or command to execute.

31.76 | LDAP search query from an unpopular and unsigned process

Synopsis

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

Required Data	- Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	LDAP Analytics (Client)
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Account Discovery (T1087)
Severity	Low

Description

An unpopular and unsigned process performed an LDAP search query. This may be indicative of LDAP enumeration.

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.
- Determine whether the search query is generic. Generic search queries (often using wildcards) tend to be more suspicious.

31.77 | A process queried the ADFS database decryption key via

LDAP

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	LDAP Analytics (Client)
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Steal or Forge Authentication Certificates (T1649)
Severity	Low

Description

A process queried the ADFS database decryption key (DKM key) via LDAP.

Attacker's Goals

An attacker wanting to perform a golden SAML attack will want to steal the ADFS token-signing certificates.

- To steal the token-signing certificates, the attacker will need to access the ADFS database

To access the encrypted ADFS database, an attacker will attempt to retrieve the decryption key via an LDAP query.

Investigative actions

Check if the LDAP search query was allowed for the user (logged on at event time) or process.

- Check for unusual ADFS logins.

Check the process that initiated the query.

Investigate the LDAP search query for any suspicious indicators.

Variations

A process explicitly queried the ADFS database decryption key (DKM key) via LDAP

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Steal or Forge Authentication Certificates (T1649)
Severity	Medium

Description

A process queried the ADFS database decryption key (DKM key) via LDAP.

Attacker's Goals

An attacker wanting to perform a golden SAML attack will want to steal the ADFS token-signing certificates.

- To steal the token-signing certificates, the attacker will need to access the ADFS database

To access the encrypted ADFS database, an attacker will attempt to retrieve the decryption key via an LDAP query.

Investigative actions

Check if the LDAP search query was allowed for the user (logged on at event time) or process.

- Check for unusual ADFS logins.

Check the process that initiated the query.

Investigate the LDAP search query for any suspicious indicators.

31.78 | Uncommon browser extension loaded

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	Chromium Extensions Analytics
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Browser Extensions (T1176)
Severity	Informational

Description

An uncommon browser extension was loaded by a Chromium-based browser.

Attacker's Goals

- Gain persistency on a machine and steal sensitive browsing data.

Investigative actions

- Investigate the extension and how it was loaded.
  Check if this extension is currently present at the relevant extensions web store by looking up for its extension ID.

31.79 | Possible Persistence via group policy Registry keys

Synopsis

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

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

Description

The Registry group policy keys being read on reboot, this will cause the persistence mechanism to trigger and run the malware.

Attacker's Goals

Gain persistence on the host using the Window's Group Policy Mechanism.

Investigative actions

Check the registry key and determine what process it'll run.

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

31.80 | 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.

31.81 | 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.

31.82 | Rare service DLL was added to the registry

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	Malicious Service Analytics
ATT&CK Tactic	Defense Evasion (TA0005) Persistence (TA0003)
ATT&CK Technique	Masquerading: Masquerade Task or Service (T1036.004) Create or Modify System Process: Windows Service (T1543.003)

Severity	Low

Description

A service was added as a dll, which will be executed by svchost.exe. This is a stealthy technique attackers use to persist their malware.

Attacker's Goals

Masquerade execution on the host using a benign Windows process and achieve persistence.

Investigative actions

- Investigate the suspicious DLL and check for malicious content.
- Go to the service registry key and investigate it to find the associated executable that runs the service.
  Check whether the executing process is benign, and if this was a desired behavior as part of its normal execution flow.

Variations

Rare service DLL was added to the registry from an injected thread

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005) Persistence (TA0003)
ATT&CK Technique	Masquerading: Masquerade Task or Service (T1036.004) Create or Modify System Process: Windows Service (T1543.003)
Severity	Medium

Description

A service was added as a dll, which will be executed by svchost.exe. This is a stealthy technique attackers use to persist their malware.

Attacker's Goals

Masquerade execution on the host using a benign Windows process and achieve persistence.

Investigative actions

- Investigate the suspicious DLL and check for malicious content.
  Go to the service registry key and investigate it to find the associated executable that runs the service.

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

Rare service DLL was added to the registry from a rare unsigned actor process

Synopsis

ATT&CK Tactic	- Defense Evasion (TA0005) Persistence (TA0003)
ATT&CK Technique	- Masquerading: Masquerade Task or Service (T1036.004) - Create or Modify System Process: Windows Service (T1543.003)
Severity	High

Description

A service was added as a dll, which will be executed by svchost.exe. This is a stealthy technique attackers use to persist their malware.

Attacker's Goals

Masquerade execution on the host using a benign Windows process and achieve persistence.

Investigative actions

Investigate the suspicious DLL and check for malicious content.
Go to the service registry key and investigate it to find the associated executable that runs the service.

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

31.83 | Microsoft Office adds a value to autostart Registry key

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: ▯ XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)
Severity	Low

Description

Microsoft Office adds a value to a Registry entry (run keys, startup folders) to establish persistence.

Attacker's Goals

Gain persistence on the host using the Window's autostart Mechanism.

Investigative actions

- Check the registry key and determine what process it'll run.
- Check whether the executing process is benign, and if this was a desired behavior as part of its normal execution flow.

31.84 | A user created an abnormal password-protected archive

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Collection (TA0009)

ATT&CK Technique	- Archive Collected Data: Archive via Utility (T1560.001) - Data Staged (T1074)
Severity	Informational

Description

A user created an abnormal password-protected archive using an archive program.

Attacker's Goals

Collect data and stage it on an endpoint in the organization.

Investigative actions

- Check whether the command line executed is normal for the process and user performing it.
- Check whether the process that created the archive creates network connections as well.
- Check whether other users in the organization used the same process for password-protected archive file creation.

31.85 | Possible LDAP Enumeration Tool Usage

Synopsis

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

Required Data	• Requires: • XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	LDAP Analytics (Client), LDAP Analytics (Server)
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	• Account Discovery (T1087) Permission Groups Discovery: Domain Groups (T1069.002) Domain Trust Discovery (T1482) Remote System Discovery (T1018) • System Network Configuration Discovery (T1016)
Severity	Informational

Description

A user sent a suspicious enumeration query via LDAP. The query is associated with an LDAP enumeration tool that may be used during 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.
- Determine whether the search query is generic. Wide search queries (often using wildcards) tend to be more suspicious. In our case, we are looking for targeted search queries.

Variations

Possible admin enumeration via LDAP

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Account Discovery (T1087) Permission Groups Discovery: Domain Groups (T1069.002) Domain Trust Discovery (T1482) Remote System Discovery (T1018) System Network Configuration Discovery (T1016)
Severity	Informational

Description

A user sent a suspicious enumeration query via LDAP. The query is associated with an LDAP enumeration tool that may be used during 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.
  Determine whether the search query is generic. Wide search queries (often using wildcards) tend to be more suspicious. In our case, we are looking for targeted search queries.

A user executed an LDAP enumeration query with suspicious characteristics

Synopsis

ATT&CK Tactic	Discovery (TA0007)

ATT&CK Technique	- Account Discovery (T1087) - Permission Groups Discovery: Domain Groups (T1069.002) Domain Trust Discovery (T1482) Remote System Discovery (T1018) System Network Configuration Discovery (T1016)
Severity	Medium

Description

A user sent a suspicious enumeration query via LDAP. The query is associated with an LDAP enumeration tool that may be used during 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.
- Determine whether the search query is generic. Wide search queries (often using wildcards) tend to be more suspicious. In our case, we are looking for targeted search queries.

Rare LDAP enumeration query executed by a user

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Account Discovery (T1087) Permission Groups Discovery: Domain Groups (T1069.002) Domain Trust Discovery (T1482) - Remote System Discovery (T1018) - System Network Configuration Discovery (T1016)
Severity	Low

Description

A user sent a suspicious enumeration query via LDAP. The query is associated with an LDAP enumeration tool that may be used during 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.
- Determine whether the search query is generic. Wide search queries (often using wildcards) tend to be more suspicious. In our case, we are looking for targeted search queries.

31.86 | 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.

31.87 | 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.

31.88 | Unusual access to the AD Sync credential files

Synopsis

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

Deduplication Period	1 Day
Required Data	Requires: ▯ XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Cloud
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Credentials from Password Stores (T1555)
Severity	Informational

Description

The AD Sync credential files were accessed in an unusual way.

Attacker's Goals

- Extracting and decrypting stored Azure AD and Active Directory credentials from Azure AD Connect servers.

Investigative actions

See whether this was a legitimate action.

Follow the causality chain/user/host activities.
- Follow unusual actions of the AD Sync user.
- Check for remote SMB connections to the agent.

Check for unusual Azure AD authentications.
Check if this happened on other endpoints.

Check for unusual logins.

Variations

Suspicious process access to the AD Sync credential files

Synopsis

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

Description

The AD Sync credential files were accessed in an unusual way.

Attacker's Goals

- Extracting and decrypting stored Azure AD and Active Directory credentials from Azure AD Connect servers.

Investigative actions

See whether this was a legitimate action.
Follow the causality chain/user/host activities.

Follow unusual actions of the AD Sync user.
- Check for remote SMB connections to the agent.
- Check for unusual Azure AD authentications.

Check if this happened on other endpoints.
Check for unusual logins.

An abnormal process accessed the AD Sync credential files

Synopsis

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

Severity	Low

Description

The AD Sync credential files were accessed in an unusual way.

Attacker's Goals

- Extracting and decrypting stored Azure AD and Active Directory credentials from Azure AD Connect servers.

Investigative actions

See whether this was a legitimate action.
Follow the causality chain/user/host activities.

Follow unusual actions of the AD Sync user.

- Check for remote SMB connections to the agent.
- Check for unusual Azure AD authentications.

Check if this happened on other endpoints.
Check for unusual logins.

31.89 | 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.

31.90 | 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.

31.91 | An unusual archive file creation by a user

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	3 Days
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	
ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Archive Collected Data: Archive via Utility (T1560.001) - Data Staged (T1074)
Severity	Informational

Description

An archive file was created by a user who doesn't usually create such files. This might indicate an attempt to stage data before exfiltration.

Attacker's Goals

Stage data on an endpoint in the organization.

Investigative actions

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

Variations

A user created an archive file for the first time

Synopsis

ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Archive Collected Data: Archive via Utility (T1560.001) Data Staged (T1074)
Severity	Informational

Description

A user created an archive file for the first time. This might indicate an attempt to stage data before exfiltration.

Attacker's Goals

Stage data on an endpoint in the organization.

Investigative actions

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

31.92 | A suspicious direct syscall 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 with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	Direct Syscall Analytics
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Native API (T1106)
Severity	Low

Description

A suspicious direct syscall was executed.

Attacker's Goals

An attacker might try to use direct syscalls to evade detection from a legitimate program.

Investigative actions

- Investigate the direct syscall mapped image to verify if it is malicious.
- Check if this direct syscall is part of the process execution flow.

Variations

A suspicious direct syscall was executed by unsigned process from a user folder

Synopsis

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

Description

A suspicious direct syscall was executed by unsigned process from a user folder.

Attacker's Goals

An attacker might try to use direct syscalls to evade detection from a legitimate program.

Investigative actions

- Investigate the direct syscall mapped image to verify if it is malicious.
- Check if this direct syscall is part of the process execution flow.

A suspicious direct syscall was executed by a DLL host application

Synopsis

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

Severity	Medium

Description

A suspicious direct syscall was executed by a DLL host application.

Attacker's Goals

An attacker might try to use direct syscalls to evade detection from a legitimate program.

Investigative actions

- Investigate the direct syscall mapped image to verify if it is malicious.
  Check if this direct syscall is part of the process execution flow.

31.93 | Possible SPN enumeration

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	LDAP Analytics (Client), LDAP Analytics (Server)

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

Description

A possible SPN enumeration via LDAP was performed. Such enumeration may be used during 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.
- Determine whether the search query is generic. Wide search queries (often using wildcards) tend to be more suspicious. In our case, we are looking for targeted search queries.

Variations

Suspicious SPN enumeration via LDAP

Synopsis

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

Description

A possible SPN enumeration via LDAP was performed. Such enumeration may be used during 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.

- Determine whether the search query is generic. Wide search queries (often using wildcards) tend to be more suspicious. In our case, we are looking for targeted search queries.

31.94 | Elevation to SYSTEM via services

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	Malicious Service Analytics

ATT&CK Tactic	Execution (TA0002) Privilege Escalation (TA0004)
ATT&CK Technique	Create or Modify System Process: Windows Service (T1543.003) System Services: Service Execution (T1569.002)
Severity	Low

Description

Services were affected by a non SYSTEM integrity level process.

Attacker's Goals

Escalate privileges to system and execute commands.

Investigative actions

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

Variations

Elevation to SYSTEM via service creation

Synopsis

ATT&CK Tactic	Execution (TA0002) Privilege Escalation (TA0004)
ATT&CK Technique	Create or Modify System Process: Windows Service (T1543.003) System Services: Service Execution (T1569.002)
Severity	Low

Description

A service was created from a non SYSTEM integrity level process.

Attacker's Goals

Escalate privileges to system and execute commands.

Investigative actions

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

Elevation to SYSTEM via service modification

Synopsis

ATT&CK Tactic	Execution (TA0002) Privilege Escalation (TA0004)
ATT&CK Technique	Create or Modify System Process: Windows Service (T1543.003) System Services: Service Execution (T1569.002)
Severity	Low

Description

An existing service was modified from a non SYSTEM integrity level process.

Attacker's Goals

Escalate privileges to system and execute commands.

Investigative actions

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

31.95 | A WMI subscriber was created

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: • XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	Impacket Analytics
ATT&CK Tactic	Persistence (TA0003) Privilege Escalation (TA0004)
ATT&CK Technique	Event Triggered Execution: Windows Management Instrumentation Event Subscription (T1546.003)
Severity	Informational

Description

A WMI subscriber was created.

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.

31.96 | A user connected a new USB storage device to a host

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Collection (TA0009) Exfiltration (TA0010)

ATT&CK Technique	- Data Staged (T1074) - Exfiltration Over Physical Medium: Exfiltration over USB (T1052.001)
Severity	Informational

Description

A user connected a new USB storage device that was not seen for this user and host in the last 30 days.

Attacker's Goals

The attacker may use a USB storage device connection for data exfiltration or data collection.

Investigative actions

Investigate the USB storage device related process and file events to determine if it was used for legitimate purposes or malicious activity.

31.97 | SecureBoot was disabled

Synopsis

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

Required Data	- Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Pre-OS Boot (T1542)
Severity	Low

Description

SecureBoot was disabled, this might be indicative of someone trying to install an alternate non UEFI supported OS.

Attacker's Goals

Disable SecureBoot to install another OS on the machine.

Investigative actions

Check if a new operating system was installed on the same hardware.

31.98 | RDP connections enabled remotely via Registry

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	- Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	Remote Services: Remote Desktop Protocol (T1021.001)
Severity	Low

Description

An attacker may remotely enable RDP connections to a machine by setting the fDenyTSConnections Registry key to 0.

Attacker's Goals

Remotely enable RDP on the host for lateral movement.

Investigative actions

- Check whether the executing process is benign, and if this was a desired behavior as part of its normal execution flow.
  Search for RDP sessions to this host and investigate them for malicious activities.

Variations

RDP connections enabled by a remote process via Registry

Synopsis

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

Description

An attacker may remotely enable RDP connections to a machine by setting the fDenyTSConnections Registry key to 0.

Attacker's Goals

Remotely enable RDP on the host for lateral movement.

Investigative actions

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

Search for RDP sessions to this host and investigate them for malicious activities.

RDP connections enabled remotely via Registry using WinRM

Synopsis

ATT&CK Tactic	Lateral Movement (TA0008)
ATT&CK Technique	- Remote Services: Remote Desktop Protocol (T1021.001) - Remote Services: Windows Remote Management (T1021.006)
Severity	Low

Description

An attacker may remotely enable RDP connections to a machine by setting the fDenyTSConnections Registry key to 0.

Attacker's Goals

Remotely enable RDP on the host for lateral movement.

Investigative actions

- Check whether the executing process is benign, and if this was a desired behavior as part of its normal execution flow.
- Search for RDP sessions to this host and investigate them for malicious activities.

31.99 | Possible GPO Enumeration

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	- Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	LDAP Analytics (Client), LDAP Analytics (Server)

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Group Policy Discovery (T1615)
Severity	Informational

Description

A possible GPO enumeration via LDAP was performed. Such enumeration may be used during attacks against the organization.

Attacker's Goals

An attacker is attempting to enumerate Active Directory.

Investigative actions

Investigate the LDAP search query for any suspicious indicators.
Look for additional LDAP queries the user executed that might be suspicious.

Determine whether the search query is generic. Wide search queries (often using wildcards) tend to be more suspicious. In our case, we are looking for targeted search queries.

- Check if the process executes LDAP search queries as part of its normal behavior.

Variations

Suspicious GPO Enumeration by an LDAP tool

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Group Policy Discovery (T1615)
Severity	Medium

Description

A possible GPO enumeration via LDAP was performed. Such enumeration may be used during attacks against the organization.

Attacker's Goals

An attacker is attempting to enumerate Active Directory.

Investigative actions

Investigate the LDAP search query for any suspicious indicators.

Look for additional LDAP queries the user executed that might be suspicious.
- Determine whether the search query is generic. Wide search queries (often using wildcards) tend to be more suspicious. In our case, we are looking for targeted search queries.
Check if the process executes LDAP search queries as part of its normal behavior.

Possible GPO Enumeration by a Suspicious Process

Synopsis

ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Group Policy Discovery (T1615)
Severity	Low

Description

A possible GPO enumeration via LDAP was performed. Such enumeration may be used during attacks against the organization.

Attacker's Goals

An attacker is attempting to enumerate Active Directory.

Investigative actions

Investigate the LDAP search query for any suspicious indicators.
Look for additional LDAP queries the user executed that might be suspicious.

Determine whether the search query is generic. Wide search queries (often using wildcards) tend to be more suspicious. In our case, we are looking for targeted search queries.
- Check if the process executes LDAP search queries as part of its normal behavior.

31.100 | Unusual process accessed a web browser history file

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	Sensitive Information Stealing Analytics
ATT&CK Tactic	Discovery (TA0007) Collection (TA0009)
ATT&CK Technique	Browser Information Discovery (T1217) Data from Local System (T1005) Automated Collection (T1119)
Severity	Low

Description

An unusual process has accessed a web browser history file.

Attacker's Goals

Obtain access to the user's browsing history and steal their contents.

Investigative actions

- Determine whether it is legitimate for the process to access web browser history.
  Analyze the process/application that accessed the file.
  Check for any other suspicious actions that were performed by the process.

  Look for unusual access of resources using credentials that may be stored in the above file.

Variations

Unusual process accessed a web browser history file on Linux

Synopsis

ATT&CK Tactic	Discovery (TA0007) Collection (TA0009)
ATT&CK Technique	Browser Information Discovery (T1217) Data from Local System (T1005) Automated Collection (T1119)
Severity	Low

Description

An unusual process has accessed a web browser history file.

Attacker's Goals

Obtain access to the user's browsing history and steal their contents.

Investigative actions

Determine whether it is legitimate for the process to access web browser history.
- Analyze the process/application that accessed the file.
- Check for any other suspicious actions that were performed by the process.
Look for unusual access of resources using credentials that may be stored in the above file.

31.101 | 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.

31.102 | Suspicious Kubernetes pod token access

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	5 Days
Required Data	- Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	Kubernetes - AGENT
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials: Credentials In Files (T1552.001)
Severity	Medium

Description

A Kubernetes pod has accessed the access token of another pod.
This could indicate potential unauthorized access or a security breach within the cluster.

Attacker's Goals

Gain access to the Kubernetes environment.

Investigative actions

Look for additional suspicious activities.
Verify if the exposed credentials were used to access the API server.

Investigate which operations were used against the Kubernetes cluster with the exposed credentials.

Variations

Suspicious Kubernetes pod token access by an unusual pod

Synopsis

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

Description

A Kubernetes pod has accessed the access token of another pod.
This could indicate potential unauthorized access or a security breach within the cluster.

Attacker's Goals

Gain access to the Kubernetes environment.

Investigative actions

Look for additional suspicious activities.
- Verify if the exposed credentials were used to access the API server.
- Investigate which operations were used against the Kubernetes cluster with the exposed credentials.

Suspicious Kubernetes pod token access by an unusual process

Synopsis

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

Description

A Kubernetes pod has accessed the access token of another pod.

This could indicate potential unauthorized access or a security breach within the cluster.

Attacker's Goals

Gain access to the Kubernetes environment.

Investigative actions

- Look for additional suspicious activities.
  Verify if the exposed credentials were used to access the API server.
  Investigate which operations were used against the Kubernetes cluster with the exposed credentials.

31.103 | 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.

31.104 | Modification of NTLM restrictions in the Registry

Synopsis

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

Detection Modules	
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	OS Credential Dumping (T1003)
Severity	Medium

Description

Allowing the transmission of NTLM could be part of an NTLM downgrade or an Internal Monologue attack.

Attacker's Goals

Downgrading to a lower NTLM version gives the attacker an easy way to retrieve NTLM hashes from a Windows machine.

Investigative actions

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

31.105 | Rare process accessed a Keychain file

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	Credentials Grabbing Analytics
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Credentials from Password Stores: Keychain (T1555.001)
Severity	Informational

Description

An unusual process accessed a Keychain file. This might indicate a credential grabbing attempt.

Attacker's Goals

Obtain access to credentials stored in the Keychain file.

Investigative actions

- Determine whether it is legitimate for the process to access credential data directly.
  Analyze the process/application that touched the Keychain.
  Check for any other suspicious actions that were performed by the process.

  Look for unusual access to resources using credentials stored on said Keychain.

Variations

Rare process accessed a Keychain file using the networksetup tool

Synopsis

ATT&CK Tactic	Credential Access (TA0006) Reconnaissance (TA0043)
ATT&CK Technique	Credentials from Password Stores: Keychain (T1555.001) Gather Victim Host Information (T1592)
Severity	High

Description

An unusual process accessed a Keychain file. This might indicate a credential grabbing attempt.

Attacker's Goals

Obtain access to credentials stored in the Keychain file.

Investigative actions

- Determine whether it is legitimate for the process to access credential data directly.
- Analyze the process/application that touched the Keychain.
- Check for any other suspicious actions that were performed by the process.
- Look for unusual access to resources using credentials stored on said Keychain.

Rare process accessed a Keychain file while installing a new certificate

Synopsis

ATT&CK Tactic	Credential Access (TA0006) Defense Evasion (TA0005)
ATT&CK Technique	Credentials from Password Stores: Keychain (T1555.001) Subvert Trust Controls: Install Root Certificate (T1553.004)
Severity	Medium

Description

An unusual process accessed a Keychain file. This might indicate a credential grabbing attempt.

Attacker's Goals

Obtain access to credentials stored in the Keychain file.

Investigative actions

- Determine whether it is legitimate for the process to access credential data directly.
- Analyze the process/application that touched the Keychain.
- Check for any other suspicious actions that were performed by the process.
- Look for unusual access to resources using credentials stored on said Keychain.

Rare process accessed a Keychain file initiated by a causality actor with a rare path

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Credentials from Password Stores: Keychain (T1555.001)
Severity	Low

Description

An unusual process accessed a Keychain file. This might indicate a credential grabbing attempt.

Attacker's Goals

Obtain access to credentials stored in the Keychain file.

Investigative actions

- Determine whether it is legitimate for the process to access credential data directly.
- Analyze the process/application that touched the Keychain.
- Check for any other suspicious actions that were performed by the process.
- Look for unusual access to resources using credentials stored on said Keychain.

Rare process accessed a Keychain file initiated by an unsigned causality actor

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Credentials from Password Stores: Keychain (T1555.001)
Severity	Low

Description

An unusual process accessed a Keychain file. This might indicate a credential grabbing attempt.

Attacker's Goals

Obtain access to credentials stored in the Keychain file.

Investigative actions

- Determine whether it is legitimate for the process to access credential data directly.
  Analyze the process/application that touched the Keychain.
  Check for any other suspicious actions that were performed by the process.

  Look for unusual access to resources using credentials stored on said Keychain.

Rare unsigned process accessed a Keychain file

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Credentials from Password Stores: Keychain (T1555.001)
Severity	Low

Description

An unusual process accessed a Keychain file. This might indicate a credential grabbing attempt.

Attacker's Goals

Obtain access to credentials stored in the Keychain file.

Investigative actions

- Determine whether it is legitimate for the process to access credential data directly.
  Analyze the process/application that touched the Keychain.

  Check for any other suspicious actions that were performed by the process.
  Look for unusual access to resources using credentials stored on said Keychain.

31.106 | User discovery via WMI query execution

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: ▯ XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Execution (TA0002) Discovery (TA0007)

ATT&CK Technique	- Windows Management Instrumentation (T1047) System Owner/User Discovery (T1033) Account Discovery (T1087)
Severity	Informational

Description

Attackers or malware may use WMI queries to list the users of a host, and potentially its owner.

Attacker's Goals

Attacker or malware can use WMI queries to discover host users and enumerate a huge amount of information.

Investigative actions

- Examine the process that executed the WMI query and verify that the process is from a trusted source.
  Inspect the system for suspicious activity that is related to that process.

Variations

User discovery via WMI query execution by an unsigned process

Synopsis

ATT&CK Tactic	Execution (TA0002) Discovery (TA0007)
ATT&CK Technique	Windows Management Instrumentation (T1047) System Owner/User Discovery (T1033) Account Discovery (T1087)
Severity	Low

Description

Attackers or malware may use WMI queries to list the users of a host, and potentially its owner.

Attacker's Goals

Attacker or malware can use WMI queries to discover host users and enumerate a huge amount of information.

Investigative actions

Examine the process that executed the WMI query and verify that the process is from a trusted source.

- Inspect the system for suspicious activity that is related to that process.

User modification via WMIC query execution

Synopsis

ATT&CK Tactic	- Execution (TA0002) Persistence (TA0003)
ATT&CK Technique	- Windows Management Instrumentation (T1047) - Account Manipulation (T1098)
Severity	Low

Description

Attackers or malware may use WMI queries to modify the users of a host, and potentially its owner.

Attacker's Goals

Attacker or malware can use WMI queries to discover host users and enumerate a huge amount of information.

Investigative actions

Examine the process that executed the WMI query and verify that the process is from a trusted source.

Inspect the system for suspicious activity that is related to that process.

User discovery via WMIC query execution

Synopsis

ATT&CK Tactic	Execution (TA0002) Discovery (TA0007)
ATT&CK Technique	Windows Management Instrumentation (T1047) System Owner/User Discovery (T1033) Account Discovery (T1087)
Severity	Informational

Description

Attackers or malware may use WMI queries to list the users of a host, and potentially its owner.

Attacker's Goals

Attacker or malware can use WMI queries to discover host users and enumerate a huge amount of information.

Investigative actions

- Examine the process that executed the WMI query and verify that the process is from a trusted source.
  Inspect the system for suspicious activity that is related to that process.

31.107 | Known service name with an uncommon image-path

Synopsis

Activation Period	14 Days

Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	Malicious Service Analytics
ATT&CK Tactic	Persistence (TA0003) Execution (TA0002)
ATT&CK Technique	Create or Modify System Process: Windows Service (T1543.003) System Services: Service Execution (T1569.002)
Severity	Low

Description

A Service with a known service name has an uncommon image-path.

Attacker's Goals

Run malicious code within seemingly trustworthy services.

Investigative actions

- Investigate the image-path of the newly created service.
- Investigate the causality actor process - which initiated the activity.

Variations

Known Palo Alto service name with an uncommon image-path

Synopsis

ATT&CK Tactic	Persistence (TA0003) Execution (TA0002)
ATT&CK Technique	Create or Modify System Process: Windows Service (T1543.003) System Services: Service Execution (T1569.002)
Severity	Medium

Description

A Service with a known service name has an uncommon image-path.

Attacker's Goals

Run malicious code within seemingly trustworthy services.

Investigative actions

- Investigate the image-path of the newly created service.
- Investigate the causality actor process - which initiated the activity.

Known service name with an uncommon image-path in a suspicious folder

Synopsis

ATT&CK Tactic	Persistence (TA0003) Execution (TA0002)

ATT&CK Technique	- Create or Modify System Process: Windows Service (T1543.003) - System Services: Service Execution (T1569.002)
Severity	Medium

Description

A Service with a known service name has an uncommon image-path.

Attacker's Goals

Run malicious code within seemingly trustworthy services.

Investigative actions

- Investigate the image-path of the newly created service.
- Investigate the causality actor process - which initiated the activity.

31.108 | 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.

31.109 | 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.

31.110 | User set insecure CA registry setting for global SANs

Synopsis

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

Description

A user enabled the EDITF_ATTRIBUTESUBJECTALTNAME2 registry flag, allowing custom Subject Alternative Names (SANs) to be specified on all certificate templates. This could enable attackers to bypass security controls by requesting certificates with user-defined SANs.

Attacker's Goals

This flag can allow an attacker to obtain a certificate with higher privileges and escalate to Domain Admin.

Investigative actions

- Confirm whether the registry change was authorized by the user or system administrator.
  Monitor certificate enrollments with Subject Alternate Names.
  Restore the secure configuration by disabling the EDITF_ATTRIBUTESUBJECTALTNAME2

  flag and enforcing strict certificate policies.
- Investigate any unusual authentication attempts or certificates issued to high-privilege users or accounts.

31.111 | A suspicious executable with multiple file extensions was created

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	- Execution (TA0002) - Defense Evasion (TA0005)

ATT&CK Technique	- User Execution: Malicious File (T1204.002) - Masquerading: Double File Extension (T1036.007)
Severity	Medium

Description

An executable file with multiple extensions was created. This technique is frequently used to disguise malware as user content.

Attacker's Goals

Bypassing defenses and/or tricking the user into executing a file that seems like a trustworthy file.

Investigative actions

Investigate the actor process and the file created to determine if it was used for legitimate purposes or malicious activity.

31.112 | LOLBIN created a PSScriptPolicyTest PowerShell script file

Synopsis

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

Required Data	- Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Execution (TA0002)
ATT&CK Technique	Command and Scripting Interpreter: PowerShell (T1059.001)
Severity	Informational

Description

A LOLBIN created a PSScriptPolicyTest file. This may be a sign of malicious PowerShell execution without directly invoking the powershell.exe binary.

Attacker's Goals

Executing PowerShell scripts in a stealthy manner.

Investigative actions

- Investigate the process and command line that created the file and whether it's benign or normal for this host.
- Investigate the created PowerShell file for potential malicious commands.

Variations

LOLBIN created a larger than usual PSScriptPolicyTest PowerShell script file

Synopsis

ATT&CK Tactic	Execution (TA0002)

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

Description

A LOLBIN created a PSScriptPolicyTest file. This may be a sign of malicious PowerShell execution without directly invoking the powershell.exe binary.

Attacker's Goals

Executing PowerShell scripts in a stealthy manner.

Investigative actions

- Investigate the process and command line that created the file and whether it's benign or normal for this host.
  Investigate the created PowerShell file for potential malicious commands.

31.113 | Unusual process accessed web browser credentials

Synopsis

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

Detection Modules	
Detector Tags	Credentials Grabbing Analytics
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Credentials from Password Stores: Credentials from Web Browsers (T1555.003)
Severity	Informational

Description

An unusual process has accessed a web browser credentials file.

Attacker's Goals

Obtain access to credentials (such as cached logins) stored in the web browser.

Investigative actions

- Determine whether it is legitimate for the process to access web browser credential data directly.
  Analyze the process/application that accessed the credentials.
  Check for any other suspicious actions that were performed by the process.

  Look for unusual access to resources using credentials cached in the web browser.

Variations

Unusual process accessed web browser credentials and executed by a terminal process

Synopsis

ATT&CK Tactic	Credential Access (TA0006)

ATT&CK Technique	Credentials from Password Stores: Credentials from Web Browsers (T1555.003)
Severity	High

Description

An unusual process has accessed a web browser credentials file.

Attacker's Goals

Obtain access to credentials (such as cached logins) stored in the web browser.

Investigative actions

- Determine whether it is legitimate for the process to access web browser credential data directly.
  Analyze the process/application that accessed the credentials.
  Check for any other suspicious actions that were performed by the process.
- Look for unusual access to resources using credentials cached in the web browser.

Unusual unsigned process accessed web browser credentials

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Credentials from Password Stores: Credentials from Web Browsers (T1555.003)
Severity	Low

Description

An unusual process has accessed a web browser credentials file.

Attacker's Goals

Obtain access to credentials (such as cached logins) stored in the web browser.

Investigative actions

- Determine whether it is legitimate for the process to access web browser credential data directly.
  Analyze the process/application that accessed the credentials.
  Check for any other suspicious actions that were performed by the process.

  Look for unusual access to resources using credentials cached in the web browser.

31.114 | Suspicious PowerSploit's recon module (PowerView) used to search for exposed hosts

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Remote System Discovery (T1018)

Severity	Medium

Description

An attacker may use PowerSploit to reconnaissance the network for exposed hosts to move laterally to.

Attacker's Goals

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

Investigative actions

- Verify that the relevant function was indeed run by PowerSploit (https://powersploit.readthedocs.io/#recon).
  Understand what information the attacker had gathered from the command and investigate relevant assets.

31.115 | Possible Distributed File System Namespace Management (DFSNM) abuse

Synopsis

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

Required Data	- Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	- Forced Authentication (T1187) Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay (T1557.001)
Severity	High

Description

A possible abuse of Distributed File System Namespace Management (DFSNM).

Attacker's Goals

- An attacker can abuse the Distributed File System Namespace Management protocol to coerce an authentication from a DC.
  This authentication can later be used for obtaining a DC certificate for DCSync.

Investigative actions

Check for a suspicious process on the initiator.
Check if the source host is a vulnerability scanner.

Look for unusual AD CS certificate requests.
- Check for possible DCSync alerts.

31.116 | 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.

31.117 | Linux system firewall was modified

Synopsis

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

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

Description

The system firewall was modified.

Attacker's Goals

Exfiltrate data or move laterally in the organization.

Investigative actions

Examine the command to understand which IPs or ports were affected.

Check the communication allowed by the modified firewall rule.

31.118 | Uncommon PowerShell commands used to create or alter scheduled task parameters

Synopsis

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

Detection Modules	
Detector Tags	
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Scheduled Task/Job: Scheduled Task (T1053.005)
Severity	Low

Description

Attackers may create or alter scheduled task parameters to gain higher privileges or persistence on the system.

Attacker's Goals

Create a new scheduled task or alter an existing one to gain persistence in the system or to gain higher privileges.

Investigative actions

- Examine the PowerShell command to identify suspicious scheduled task creation or modification.
  Inspect the system for suspicious activity that is triggered by a scheduled task.

31.119 | Unusual ADConnect database file access

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials (T1552)
Severity	Informational

Description

An unusual process accessed the ADConnect database files.

Attacker's Goals

- Attackers can abuse the Azure AD Connect database files to get access to the AD Sync account.
  The AD Sync account is a highly privileged account that can perform a DCSync and get access to on-premise password hashes.

Investigative actions

See whether this was a legitimate action.

- Follow process/user/host activities.
- Follow unusual actions of the AD Sync user.
  Check for unusual Azure AD authentications.
  Check for a possible DCSync.

Variations

Suspicious access to ADConnect database file

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials (T1552)
Severity	Medium

Description

An unusual process accessed the ADConnect database files with some suspicious characteristics that flagged this access attempt as a suspicious.

Attacker's Goals

- Attackers can abuse the Azure AD Connect database files to get access to the AD Sync account.
  The AD Sync account is a highly privileged account that can perform a DCSync and get access to on-premise password hashes.

Investigative actions

- See whether this was a legitimate action.
- Follow process/user/host activities.
  Follow unusual actions of the AD Sync user.
  Check for unusual Azure AD authentications.
  Check for a possible DCSync.

Access to ADConnect database file by an unsigned or unusual process

Synopsis

ATT&CK Tactic	Credential Access (TA0006)

ATT&CK Technique	Unsecured Credentials (T1552)
Severity	Low

Description

An unusual process accessed the ADConnect database files with some suspicious characteristics that flagged this access attempt as a suspicious access.

Attacker's Goals

- Attackers can abuse the Azure AD Connect database files to get access to the AD Sync account.
- The AD Sync account is a highly privileged account that can perform a DCSync and get access to on-premise password hashes.

Investigative actions

- See whether this was a legitimate action.
- Follow process/user/host activities.
- Follow unusual actions of the AD Sync user.
- Check for unusual Azure AD authentications.
- Check for a possible DCSync.

31.120 | Suspicious PowerSploit's recon module (PowerView) net function 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 with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Remote System Discovery (T1018)
Severity	Medium

Description

An attacker may use PowerSploit to reconnaissance the network.

Attacker's Goals

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

Investigative actions

Verify that the relevant function was indeed run by PowerSploit

(https://powersploit.readthedocs.io/#recon).

- Understand what information the attacker had gathered from the command and investigate relevant assets.

31.121 | Unusual process accessed FTP Client credentials

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	Credentials Grabbing Analytics
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials: Credentials In Files (T1552.001)
Severity	Low

Description

An unusual process has accessed a third-party FTP client's credential file.

Attacker's Goals

Obtain access to passwords stored in the FTP client.

Investigative actions

- Determine whether it is legitimate for the process to access FTP passwords directly.
- Analyze the process/application that accessed the credentials.
- Check for any other suspicious actions that were performed by the process.
- Look for unusual access to resources using credentials cached in the FTP client.

31.122 | Uncommon creation or access operation of sensitive shadow copy

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	- Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	OS Credential Dumping (T1003)

Severity	Low

Description

An uncommon creation or access of a sensitive Shadow Copy volume path.

Attacker's Goals

Attackers may try to copy sensitive data or dump OS credentials from the host file system by using Shadow Copy volume utilities.

Investigative actions

- Verify if the shadow copy operation is part of an IT activity.
- Look for other hosts performing the same shadow copy event with similar causality process behavior.
  Inspect the causality process and its characteristics as they appear on other hosts.

Variations

Uncommon creation or access operation of sensitive shadow copy by a remote actor

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	OS Credential Dumping (T1003)
Severity	Low

Description

An uncommon creation or access of a sensitive Shadow Copy volume path.

Attacker's Goals

Attackers may try to copy sensitive data or dump OS credentials from the host file system by using Shadow Copy volume utilities.

Investigative actions

- Verify if the shadow copy operation is part of an IT activity.
- Look for other hosts performing the same shadow copy event with similar causality process behavior.

  Inspect the causality process and its characteristics as they appear on other hosts. Investigate the remote machine, search for the stolen shadow copies and for any infection that may initiated the activity.

Uncommon creation or access operation of sensitive shadow copy by a high-risk process

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	OS Credential Dumping (T1003)
Severity	High

Description

An uncommon creation or access of a sensitive Shadow Copy volume path by a high-risk process.

Attacker's Goals

Attackers may try to copy sensitive data or dump OS credentials from the host file system by using Shadow Copy volume utilities.

Investigative actions

- Verify if the shadow copy operation is part of an IT activity.
  Look for other hosts performing the same shadow copy event with similar causality process behavior.

  Inspect the causality process and its characteristics as they appear on other hosts.

31.123 | 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.

31.124 | Change of sudo caching configuration

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	- Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	Kubernetes - AGENT, Containers
ATT&CK Tactic	Defense Evasion (TA0005) Privilege Escalation (TA0004)

ATT&CK Technique	Abuse Elevation Control Mechanism: Sudo and Sudo Caching (T1548.003)
Severity	Low

Description

Change of sudo caching configuration may have been intended to enable privilege escalation.

Attacker's Goals

Attackers may use the sudoers file to elevate privileges.

Investigative actions

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

Variations

Change of sudo caching configuration in a Kubernetes pod

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005) Privilege Escalation (TA0004)
ATT&CK Technique	Abuse Elevation Control Mechanism: Sudo and Sudo Caching (T1548.003)
Severity	Low

Description

Change of sudo caching configuration may have been intended to enable privilege escalation.

Attacker's Goals

Attackers may use the sudoers file to elevate privileges.

Investigative actions

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

31.125 | A process modified an SSH authorized_keys file

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	Kubernetes - AGENT, Containers
ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation: SSH Authorized Keys (T1098.004)

Severity	Informational

Description

A process modified an SSH authorized_keys file, which is used in SSH authentication. An attack can add or remove an SSH key to gain access to a targeted host.

Attacker's Goals

Adversaries use this to ensure that they are possessing the corresponding private key and may log in as an existing user via SSH.

Investigative actions

Check the file modification, try to understand the impact of the related processes and network connections.

Variations

A process modified an SSH authorized_keys2 file

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation: SSH Authorized Keys (T1098.004)
Severity	Low

Description

A process modified an SSH authorized_keys file, which is used in SSH authentication. An attack can add or remove an SSH key to gain access to a targeted host.

Attacker's Goals

Adversaries use this to ensure that they are possessing the corresponding private key and may log in as an existing user via SSH.

Investigative actions

Check the file modification, try to understand the impact of the related processes and network connections.

A process modified an SSH authorized_keys file from within a Kubernetes Pod

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation: SSH Authorized Keys (T1098.004)
Severity	Low

Description

A process modified an SSH authorized_keys file, which is used in SSH authentication. An attack can add or remove an SSH key to gain access to a targeted host.

Attacker's Goals

Adversaries use this to ensure that they are possessing the corresponding private key and may log in as an existing user via SSH.

Investigative actions

Check the file modification, try to understand the impact of the related processes and network connections.

Unpopular process modified the SSH authorized_keys file

Synopsis

ATT&CK Tactic	Persistence (TA0003)
ATT&CK Technique	Account Manipulation: SSH Authorized Keys (T1098.004)

Severity	Low

Description

An unpopular process modified the SSH authorized_keys file.

Attacker's Goals

Adversaries use this to ensure that they are possessing the corresponding private key and may log in as an existing user via SSH.

Investigative actions

Check the file modification, try to understand the impact of the related processes and network connections.

31.126 | Suspicious LDAP search query 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 with eXtended Threat Hunting (XTH)
Detection Modules	

Detector Tags	LDAP Analytics (Client)
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Account Discovery (T1087)
Severity	Low

Description

A suspicious and unpopular LDAP search query was executed. This may be indicative of Active Directory domain enumeration, which may be used during attacks against the organization.

Attacker's Goals

An attacker is attempting to enumerate Active Directory.

Investigative actions

- Check if the process executes LDAP search queries as part of its normal behavior.
  Investigate the LDAP search query for any suspicious indicators.
  Determine whether the search query is generic. Wide search queries (often using wildcards) tend to be more suspicious. In our case, we are looking for targeted search queries.

Variations

Suspicious LDAP search query executed

Synopsis

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

Description

A suspicious and unpopular LDAP search query was executed. This may be indicative of Active Directory domain enumeration, which may be used during attacks against the organization.

Attacker's Goals

An attacker is attempting to enumerate Active Directory.

Investigative actions

- Check if the process executes LDAP search queries as part of its normal behavior.
- Investigate the LDAP search query for any suspicious indicators.
- Determine whether the search query is generic. Wide search queries (often using wildcards) tend to be more suspicious. In our case, we are looking for targeted search queries.

31.127 | A suspicious process queried AD CS objects via LDAP

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	LDAP Analytics (Client)

ATT&CK Tactic	- Discovery (TA0007) Credential Access (TA0006)
ATT&CK Technique	- File and Directory Discovery (T1083) - Steal or Forge Authentication Certificates (T1649)
Severity	Informational

Description

A suspicious process queried AD CS objects via LDAP.

Attacker's Goals

An attacker might look for AD CS servers, certificate templates or request certificates.

With the wrong setting or loose vulnerable templates or enabled enrollment, the attacker will be able to authenticate as users on the network.

Investigative actions

- Check if the LDAP search query was allowed for the user (logged on at event time) or process.
  Investigate the LDAP search query for any suspicious indicators.

Variations

A user suspiciously queried AD CS objects via LDAP

Synopsis

ATT&CK Tactic	Discovery (TA0007) Credential Access (TA0006)
ATT&CK Technique	- File and Directory Discovery (T1083) Steal or Forge Authentication Certificates (T1649)
Severity	Low

Description

A user suspiciously queried AD CS objects via LDAP.

Attacker's Goals

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

Investigative actions

- Check if the LDAP search query was allowed for the user (logged on at event time) or process.
- Investigate the LDAP search query for any suspicious indicators.

31.128 | Suspicious disablement of the Windows Firewall using PowerShell 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 with eXtended Threat Hunting (XTH)
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 using PowerShell. 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 Windows event logs to see the PowerShell command or script that was executed. Check whether the PowerShell command is benign or normal for the host and/or user performing it.

  Investigate the endpoint to determine if it's a legitimate process that disabled the firewall.

31.129 | PowerShell pfx certificate extraction

Synopsis

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

Deduplication Period	1 Day
Required Data	Requires: • XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials: Credentials In Files (T1552.001)
Severity	Informational

Description

PowerShell was used to extract a pfx certificate file.

Attacker's Goals

Attackers may export certificates to .pfx files to use them for authentication, persistence or NTLM extraction.

Investigative actions

Check if the pfx creation is legitimate for the user (Testing, IT, etc.).

Follow further actions done by the user (ex. authentication using certificates).

Variations

Suspicious PowerShell pfx certificate extraction

Synopsis

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

Description

A user used PowerShell to extract a pfx certificate file.

Attacker's Goals

Attackers may export certificates to .pfx files to use them for authentication, persistence or NTLM extraction.

Investigative actions

Check if the pfx creation is legitimate for the user (Testing, IT, etc.).
Follow further actions done by the user (ex. authentication using certificates).

31.130 | Unusual access to the Windows Internal Database on an ADFS 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 with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Credentials from Password Stores (T1555)
Severity	Informational

Description

The Windows Internal Database (WID) was queried in an unusual way on an ADFS server.

Attacker's Goals

- Attackers can attempt to extract and decrypt the ADFS certificate that is used to sign SAML tokens, and fabricate a new SAML token.

Investigative actions

See whether this was a legitimate action.

Follow the causality chain/user/host activities.
- Monitor suspicious LDAP queries to the ADFS container in Active Directory.
- Check the possibility of a compromised ADFS server.
Check for unusual Azure AD authentications.
Check for unusual logins.

Variations

Suspicious access to the Windows Internal Database on an ADFS server

Synopsis

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

Description

The Windows Internal Database (WID) was queried in an unusual way on an ADFS server.

Attacker's Goals

- Attackers can attempt to extract and decrypt the ADFS certificate that is used to sign SAML tokens, and fabricate a new SAML token.

Investigative actions

See whether this was a legitimate action.
Follow the causality chain/user/host activities.

Monitor suspicious LDAP queries to the ADFS container in Active Directory.
- Check the possibility of a compromised ADFS server.
- Check for unusual Azure AD authentications.

Check for unusual logins.

31.131 | Uncommon access to Microsoft Teams credential files

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials (T1552)
Severity	Low

Description

Sensitive Microsoft Teams credential files were accessed.

Attacker's Goals

Accessing these files is done by attackers to collect user credentials.

Investigative actions

Investigate the actor process to determine if it was used for legitimate purposes or malicious activity.

Variations

Uncommon access to Microsoft Teams credential files by an unsigned and unpopular process

Synopsis

ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials (T1552)
Severity	Low

Description

Sensitive Microsoft Teams credential files were accessed. by an unsigned and unpopular process.

Attacker's Goals

Accessing these files is done by attackers to collect user credentials.

Investigative actions

Investigate the actor process to determine if it was used for legitimate purposes or malicious activity.

31.132 | Suspicious DotNet log file created

Synopsis

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

Required Data	- Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	- Reflective Code Loading (T1620) Process Injection (T1055)
Severity	Low

Description

Payloads that use the DotNet framework may generate suspicious Microsoft DotNet log files.

Attacker's Goals

Run/Inject DotNet code in the context of a signed process.

Investigative actions

Verify if the actor process is using DotNet in a valid way.
- Check if a new application was recently installed on the host at the time of the alert.

Variations

DotNet log file created by svchost from 'Absolute software Corp' causality

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)

ATT&CK Technique	- Reflective Code Loading (T1620) - Process Injection (T1055)
Severity	Informational

Description

Causality 'Absolute software Corp' loads/injects into svchost and creates DotNet log files.

Attacker's Goals

Run/Inject DotNet code in the context of a signed process.

Investigative actions

- Verify if the actor process is using DotNet in a valid way.
- Check if a new application was recently installed on the host at the time of the alert.

Suspicious DotNet log file created from an injected thread

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	- Reflective Code Loading (T1620) Process Injection (T1055)
Severity	Low

Description

Payloads that use the DotNet framework may generate suspicious Microsoft DotNet log files.

Attacker's Goals

Run/Inject DotNet code in the context of a signed process.

Investigative actions

- Verify if the actor process is using DotNet in a valid way.
- Check if a new application was recently installed on the host at the time of the alert.

Suspicious DotNet log file created

Synopsis

ATT&CK Tactic	Defense Evasion (TA0005)
ATT&CK Technique	Reflective Code Loading (T1620) Process Injection (T1055)
Severity	Low

Description

Payloads that use the DotNet framework may generate suspicious Microsoft DotNet log files.

Attacker's Goals

Run/Inject DotNet code in the context of a signed process.

Investigative actions

- Verify if the actor process is using DotNet in a valid way.
- Check if a new application was recently installed on the host at the time of the alert.

31.133 | Image file execution options (IFEO) registry key set

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	- Privilege Escalation (TA0004) Persistence (TA0003)
ATT&CK Technique	Event Triggered Execution: Image File Execution Options Injection (T1546.012)
Severity	Low

Description

Attackers may use the Image File Execution Options Registry key to launch their executable whenever the user attempts to execute a certain executable.

Attacker's Goals

Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by Image File Execution Options debuggers.

Investigative actions

- Check whether the executing process is benign, and if this was a desired behavior as part of its normal execution flow.
  Also look at the debugged process and what it is executing to determine if it is malicious.

Variations

Image file execution options (IFEO) registry key set to execute a shell or scripting engine process

Synopsis

ATT&CK Tactic	Privilege Escalation (TA0004) Persistence (TA0003)
ATT&CK Technique	Event Triggered Execution: Image File Execution Options Injection (T1546.012)
Severity	High

Description

Attackers may use the Image File Execution Options Registry key to launch their executable whenever the user attempts to execute a certain executable.

Attacker's Goals

Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by Image File Execution Options debuggers.

Investigative actions

- Check whether the executing process is benign, and if this was a desired behavior as part of its normal execution flow.
  Also look at the debugged process and what it is executing to determine if it is malicious.

Image file execution options (IFEO) registry key set to activate Windows licenses illegally

Synopsis

ATT&CK Tactic	- Privilege Escalation (TA0004) - Persistence (TA0003)

ATT&CK Technique	Event Triggered Execution: Image File Execution Options Injection (T1546.012)
Severity	Medium

Description

Attackers may use the Image File Execution Options Registry key to launch their executable whenever the user attempts to execute a certain executable. This is also used by tools that were made to activate Windows licenses illegally.

Attacker's Goals

Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by Image File Execution Options debuggers.

Investigative actions

- Check whether the executing process is benign, and if this was a desired behavior as part of its normal execution flow.
- Also look at the debugged process and what it is executing to determine if it is malicious.

Image file execution options (IFEO) registry key set using reg.exe

Synopsis

ATT&CK Tactic	- Privilege Escalation (TA0004) Persistence (TA0003)
ATT&CK Technique	Event Triggered Execution: Image File Execution Options Injection (T1546.012)
Severity	High

Description

Attackers may use the Image File Execution Options Registry key to launch their executable whenever the user attempts to execute a certain executable.

Attacker's Goals

Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by Image File Execution Options debuggers.

Investigative actions

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

Also look at the debugged process and what it is executing to determine if it is malicious.

31.134 | Rare scheduled task created

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	N/A (single event)
Deduplication Period	1 Day
Required Data	Requires: ▯ XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	Impacket Analytics
ATT&CK Tactic	Persistence (TA0003)

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

Description

A new rare scheduled task was created with a rare path and a rare command line.

Attacker's Goals

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

Investigative actions

- Review the action of the created scheduled task.
- Investigate the execution chain of the process creating the scheduled task.

Variations

Uncommon remote scheduled task created

Synopsis

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

Description

A new uncommon remote scheduled task was created with a rare path and a rare command line.

Attacker's Goals

Attackers may attempt to gain persistence or perform lateral movement to new hosts to expand the foothold within a network.

Investigative actions

Review the action of the created scheduled task.
Correlate the RPC call from the source host and understand which software initiated it.

Uncommon local scheduled task created

Synopsis

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

Description

A new uncommon local scheduled task was created with a rare path and a rare command line.

Attacker's Goals

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

Investigative actions

Review the action of the created scheduled task.
Investigate the execution chain of the process creating the scheduled task.

31.135 | Massive file compression by user

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	3 Hours
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Archive Collected Data: Archive via Utility (T1560.001) Data Staged (T1074)
Severity	Informational

Description

Multiple archive files were created by a user. This might indicate an attempt to stage data before exfiltration.

Attacker's Goals

Stage data on an endpoint in the organization.

Investigative actions

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

31.136 | Possible data exfiltration over a USB storage device

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Day
Required Data	▪ Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Collection (TA0009) Exfiltration (TA0010)

ATT&CK Technique	- Exfiltration Over Physical Medium: Exfiltration over USB (T1052.001) Data Staged: Local Data Staging (T1074.001)
Severity	Informational

Description

A process generated massive file creation, renaming and write activity to a USB storage device.

Attacker's Goals

Collect data and stage it on an endpoint in the organization.

Investigative actions

- Check whether the process that created the massive file activity creates network connections as well.
  Check whether the USB storage device is new to the organization.
  Check whether other users in the organization used the same process for massive file activity.

31.137 | 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.

31.138 | Suspicious access to cloud credential files

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Cloud
Detector Tags	Cloud Lateral Movement Analytics
ATT&CK Tactic	Credential Access (TA0006)
ATT&CK Technique	Unsecured Credentials: Credentials In Files (T1552.001)

Severity	Informational

Description

A process accessed multiple cloud credential files, which may indicate a credential theft activity.

Attacker's Goals

Gain initial access to the cloud environment.

Investigative actions

Verify if the executing process is doing more suspicious activities.

- Verify if the exposed credential files were used to access to the cloud environment.
- Verify which operations were used against the cloud environment with the exposed credentials.

Variations

Suspicious access to cloud credential files of various cloud providers within a cloud instance

Synopsis

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

Description

A process accessed multiple cloud credential files, which may indicate a credential theft activity.

Attacker's Goals

Gain initial access to the cloud environment.

Investigative actions

Verify if the executing process is doing more suspicious activities.

- Verify if the exposed credential files were used to access to the cloud environment.
- Verify which operations were used against the cloud environment with the exposed credentials.

Suspicious access to cloud credential files within a cloud instance

Synopsis

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

Description

A process accessed multiple cloud credential files, which may indicate a credential theft activity.

Attacker's Goals

Gain initial access to the cloud environment.

Investigative actions

- Verify if the executing process is doing more suspicious activities.
- Verify if the exposed credential files were used to access to the cloud environment.
  Verify which operations were used against the cloud environment with the exposed credentials.

Suspicious access to Windows cloud credential files of various cloud providers

Synopsis

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

Severity	Medium

Description

A process accessed multiple cloud credential files, which may indicate a credential theft activity.

Attacker's Goals

Gain initial access to the cloud environment.

Investigative actions

- Verify if the executing process is doing more suspicious activities.
- Verify if the exposed credential files were used to access to the cloud environment.
- Verify which operations were used against the cloud environment with the exposed credentials.

Suspicious access to Windows cloud credential files by an unusual process

Synopsis

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

Description

A process accessed multiple cloud credential files, which may indicate a credential theft activity.

Attacker's Goals

Gain initial access to the cloud environment.

Investigative actions

Verify if the executing process is doing more suspicious activities.
Verify if the exposed credential files were used to access to the cloud environment.

Verify which operations were used against the cloud environment with the exposed credentials.

Suspicious access to cloud credential files of various cloud providers

Synopsis

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

Description

A process accessed multiple cloud credential files, which may indicate a credential theft activity.

Attacker's Goals

Gain initial access to the cloud environment.

Investigative actions

- Verify if the executing process is doing more suspicious activities.
Verify if the exposed credential files were used to access to the cloud environment.
Verify which operations were used against the cloud environment with the exposed credentials.

Suspicious access to cloud credential files by an unusual process

Synopsis

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

Description

A process accessed multiple cloud credential files, which may indicate a credential theft activity.

Attacker's Goals

Gain initial access to the cloud environment.

Investigative actions

Verify if the executing process is doing more suspicious activities.
Verify if the exposed credential files were used to access to the cloud environment.

Verify which operations were used against the cloud environment with the exposed credentials.

31.139 | A user established an SMB connection to multiple hosts

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
Deduplication Period	1 Day
Required Data	■ Requires: ▯ XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics
Detector Tags	

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

Description

A user established an SMB connection to multiple hosts. This might indicate an enumeration attempt by a compromised account.

Attacker's Goals

Adversaries can effectively map out and strategize their lateral movement within a network by leveraging diverse protocols for reconnaissance.

Investigative actions

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

Look for the process that initiated this activity on the remote host.

- Check if the user is authorized to perform such activity.

Variations

A user established an SMB connection to multiple hosts for the first time

Synopsis

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

Description

A user established an SMB connection to multiple hosts. This might indicate an enumeration attempt by a compromised account.

Attacker's Goals

Adversaries can effectively map out and strategize their lateral movement within a network by leveraging diverse protocols for reconnaissance.

Investigative actions

- Verify if the host is a newly deployed server that consists of SMB services to multiple hosts.
- Look for the process that initiated this activity on the remote host.
- Check if the user is authorized to perform such activity.

A user performed an abnormal SMB activity to multiple hosts

Synopsis

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

Description

A user established an SMB connection to multiple hosts. This might indicate an enumeration attempt by a compromised account.

Attacker's Goals

Adversaries can effectively map out and strategize their lateral movement within a network by leveraging diverse protocols for reconnaissance.

Investigative actions

Verify if the host is a newly deployed server that consists of SMB services to multiple hosts.
Look for the process that initiated this activity on the remote host.

Check if the user is authorized to perform such activity.

31.140 | 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.

31.141 | 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.

31.142 | User collected remote shared files in an archive

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	- Archive Collected Data: Archive via Utility (T1560.001) - Data Staged (T1074)

Severity	Low

Description

Multiple files from remote shares were archived in a local file. This may indicate collection of data and staging before exfiltration.

Attacker's Goals

Collect data and stage it on an endpoint in the organization.

Investigative actions

- Check whether the process that created the archive creates network connections as well.
- Check whether other users in the organization used the same process for remote archive file activity.

31.143 | A user executed multiple LDAP enumeration queries

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Analytics

Detector Tags	LDAP Analytics (Server)
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	Account Discovery (T1087) Permission Groups Discovery: Domain Groups (T1069.002) Domain Trust Discovery (T1482) Remote System Discovery (T1018) System Network Configuration Discovery (T1016)
Severity	Informational

Description

A user executed multiple LDAP enumeration 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

A user executed suspicious LDAP enumeration queries

Synopsis

ATT&CK Tactic	Discovery (TA0007)

ATT&CK Technique	- Account Discovery (T1087) - Permission Groups Discovery: Domain Groups (T1069.002) Domain Trust Discovery (T1482) Remote System Discovery (T1018) System Network Configuration Discovery (T1016)
Severity	Low

Description

A user executed multiple LDAP enumeration 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.

31.144 | Suspicious reconnaissance using LDAP

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	10 Minutes
Deduplication Period	7 Days

Required Data	- Requires: - 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

A process executed multiple suspicious LDAP search queries.
This may be indicative of LDAP enumeration.

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.
- Determine whether the search query is generic. Generic search queries (often using wildcards) tend to be more suspicious.

Variations

Suspicious reconnaissance using LDAP from untrusted process

Synopsis

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

Description

A process executed multiple suspicious LDAP search queries.
This may be indicative of LDAP enumeration.

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.

Determine whether the search query is generic. Generic search queries (often using wildcards) tend to be more suspicious.

31.145 | Possible LDAP enumeration by unsigned process

Synopsis

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

Deduplication Period	1 Day
Required Data	Requires: ▯ 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 unsigned process performed multiple different LDAP search queries.
This may be indicative of LDAP enumeration.

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.
- Determine whether the search query is generic. Generic search queries (often using wildcards) tend to be more suspicious.

Variations

Possible LDAP enumeration by unsigned process

Synopsis

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

Description

An unsigned process performed multiple different LDAP search queries.
This may be indicative of LDAP enumeration.

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.

Determine whether the search query is generic. Generic search queries (often using wildcards) tend to be more suspicious.

Possible LDAP enumeration by unsigned process

Synopsis

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

Description

An unsigned process performed multiple different LDAP search queries.
This may be indicative of LDAP enumeration.

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.
- Determine whether the search query is generic. Generic search queries (often using wildcards) tend to be more suspicious.

31.146 | 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.

31.147 | A user performed suspiciously massive file activity

Synopsis

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

Required Data	- Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	- Automated Collection (T1119) Data Staged: Local Data Staging (T1074.001) Data Staged: Remote Data Staging (T1074.002)
Severity	Informational

Description

A user generated massive file activity by size or distinct file count.

Attacker's Goals

Collect data and stage it on an endpoint in the organization.

Investigative actions

- Check whether the process that created the massive file activity creates network connections as well.
  Check which files the process performed the activity on.
  Check whether other users in the organization used the same process for file activity.

Variations

A user performed suspiciously large file activities over 1 GB in a short period of time

Synopsis

ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	- Automated Collection (T1119) Data Staged: Local Data Staging (T1074.001) Data Staged: Remote Data Staging (T1074.002)
Severity	Low

Description

A user generated massive file activity by size or distinct file count.

Attacker's Goals

Collect data and stage it on an endpoint in the organization.

Investigative actions

Check whether the process that created the massive file activity creates network connections as well.
- Check which files the process performed the activity on.
- Check whether other users in the organization used the same process for file activity.

31.148 | User and Group Enumeration via SAMR

Synopsis

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

Deduplication Period	1 Day
Required Data	Requires: ▯ XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	▮ Account Discovery (T1087) ▮ Permission Groups Discovery (T1069)
Severity	Informational

Description

The endpoint performed unfamiliar SAMR querying activity to a domain controller.

Attacker's Goals

An adversary may enumerate users and groups to gain information and plan its lateral movement over the network.

Investigative actions

Check if the host is a newly deployed server that provides RPC-based services to multiple hosts.
Check if there are any other suspicious activities originating from the same machine.

31.149 | A user took numerous screenshots

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Screen Capture (T1113) Data Staged: Local Data Staging (T1074.001)
Severity	Informational

Description

A user took numerous screenshots. A valuable organization's information may have been collected in this way.

Attacker's Goals

Collect data and stage it on an endpoint in the organization.

Investigative actions

- Check whether this activity fits the user profile.
- Check for any other suspicious activity related to the host and the user involved in the alert.
  Check if there was a suspicious file upload following the massive screenshot activity.
  Check whether other users in the organization used the same process for file activity.

31.150 | 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.

31.151 | 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.

31.152 | Outlook files accessed by an unsigned process

Synopsis

Activation Period	14 Days
Training Period	30 Days

Test Period	1 Hour
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	
Detector Tags	
ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Data Staged: Local Data Staging (T1074.001) Email Collection: Local Email Collection (T1114.001)
Severity	Low

Description

An attacker may use an uncommon and unsigned process to access Outlook data files.

Attacker's Goals

Gain access to the data in the compromised mailbox.

Investigative actions

Examine the process command and file activity to identify the mailbox.
Check if the process performed any other suspicious file activity.

Check if the process generated network connections.

31.153 | A user accessed an abnormal number of files on a remote shared folder

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Discovery (TA0007)
ATT&CK Technique	File and Directory Discovery (T1083)
Severity	Informational

Description

A user remotely accessed an abnormal number of files on a remote shared folder. This might indicate an attempt to collect data before exfiltration.

Attacker's Goals

Collect valuable data about the organization for exfiltration purposes.

Investigative actions

- Check for other suspicious activity made by the user at the time of the event.
- Go over the list of files and check if such user should have access to those files.

31.154 | 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.

31.155 | A user connected a new USB storage device to multiple hosts

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Hour
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Collection (TA0009) Exfiltration (TA0010)
ATT&CK Technique	Data Staged (T1074) Exfiltration Over Physical Medium: Exfiltration over USB (T1052.001)
Severity	Low

Description

A user connected a new USB storage device to multiple endpoints.

Attacker's Goals

The attacker may use a USB storage device connection for data exfiltration or data collection.

Investigative actions

Investigate the USB storage device related process and file events to determine if it was used for legitimate purposes or malicious activity.

31.156 | A user accessed an abnormal number of remote shared folders

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Threat Module
Detector Tags	

ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Data from Network Shared Drive (T1039)
Severity	Informational

Description

A user accessed an abnormal number of remote shared folders. This might indicate an attempt to collect data before exfiltration.

Attacker's Goals

Collect valuable data about the organization for exfiltration purposes.

Investigative actions

- Check for other suspicious activity made by the user at the time of the event.
- Inspect the shared folder and verify if the user should have accessed to that folder.
- Go over the list of files and check if such user should have access to those files.

Variations

A user accessed an abnormal number of remote shared folders for the first time

Synopsis

ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Data from Network Shared Drive (T1039)
Severity	Low

Description

A user accessed for the first time to an abnormal number of remote shared folders. This might indicate an attempt to collect data before exfiltration.

Attacker's Goals

Collect valuable data about the organization for exfiltration purposes.

Investigative actions

Check for other suspicious activity made by the user at the time of the event.
Inspect the shared folder and verify if the user should have accessed to that folder.
Go over the list of files and check if such user should have access to those files.

31.157 | 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.

31.158 | Possible internal data exfiltration over a USB storage device

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	- Collection (TA0009) - Exfiltration (TA0010)
ATT&CK Technique	- Exfiltration Over Physical Medium: Exfiltration over USB (T1052.001) - Data Staged: Local Data Staging (T1074.001)
Severity	Informational

Description

A user generated abnormal massive file activity to a connected USB storage device.

Attacker's Goals

Collect data and stage it on an endpoint in the organization.

Investigative actions

- Check whether the process that created the massive file activity creates network connections as well.
Check whether the USB storage device is new to the organization.
Check whether other users in the organization used the same process for massive file activity.

Variations

Possible internal data exfiltration of over 500 MB via USB storage device

Synopsis

ATT&CK Tactic	Collection (TA0009) Exfiltration (TA0010)
ATT&CK Technique	Exfiltration Over Physical Medium: Exfiltration over USB (T1052.001) Data Staged: Local Data Staging (T1074.001)
Severity	Low

Description

A user generated abnormal massive file activity to a connected USB storage device.

Attacker's Goals

Collect data and stage it on an endpoint in the organization.

Investigative actions

Check whether the process that created the massive file activity creates network connections as well.

- Check whether the USB storage device is new to the organization.

Check whether other users in the organization used the same process for massive file activity.

31.159 | 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.

31.160 | A contained process attempted to escape using the 'notify on release' feature

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	

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

Description

A contained process attempted to escape the host by leveraging the Docker's 'notify on release' feature.
The calling process modified relevant files that might trigger a command on the host.

Attacker's Goals

Execute arbitrary commands on the host and gain a larger foothold.

Investigative actions

Check which commands were executed on the host afterward.
Look for the root cause of the execution within the container.

Examine the release_agent script content on the container.

Variations

A contained process attempted to escape using the 'notify on release' feature

Synopsis

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

Description

A contained process attempted to escape the host by leveraging the Docker's 'notify on release' feature.
The calling process modified relevant files that might trigger a command on the cloud host.

Attacker's Goals

Execute arbitrary commands on the host and gain a larger foothold.

Investigative actions

- Check which commands were executed on the host afterward.
- Look for the root cause of the execution within the container.
- Examine the release_agent script content on the container.

31.161 | 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.

31.162 | Massive file activity abnormal to process

Synopsis

Activation Period	14 Days
Training Period	30 Days
Test Period	1 Hour
Deduplication Period	1 Day
Required Data	Requires: - XDR Agent with eXtended Threat Hunting (XTH)
Detection Modules	Identity Threat Module
Detector Tags	
ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	Automated Collection (T1119) Data Staged: Local Data Staging (T1074.001)
Severity	Informational

Description

A user generated massive file activity by size or distinct file count.

Attacker's Goals

Collect data and stage it on an endpoint in the organization.

Investigative actions

- Check whether the process that created the massive file activity creates network connections as well.
- Check which files the process performed the activity on.
- Check whether other users in the organization used the same process for file activity.

Variations

Massive file activity over 500 MB abnormal to process

Synopsis

ATT&CK Tactic	Collection (TA0009)
ATT&CK Technique	- Automated Collection (T1119) - Data Staged: Local Data Staging (T1074.001)
Severity	Low

Description

A user generated massive file activity by size or distinct file count.

Attacker's Goals

Collect data and stage it on an endpoint in the organization.

Investigative actions

- Check whether the process that created the massive file activity creates network connections as well.
- Check which files the process performed the activity on.
- Check whether other users in the organization used the same process for file activity.

31.163 | 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.