

WORK WITH SEQUENCES AND EVALUATIONS

The platform's inventory of Sequences can be viewed in the Sequence Library and its Evaluations are available in the Evaluation Library. These two libraries have the same elements with one exception: **Run All Actions** is only available in the Evaluation Library. Both Libraries are also similar to the Action Library.

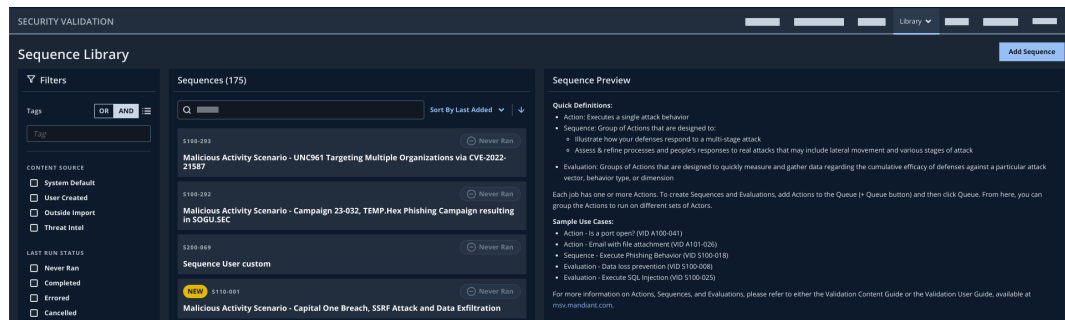
This topic discusses the Library elements, available features, and running content. Information on creating Sequences and Evaluations is available in [Creating Sequences and Evaluations \(https://docs.mandiant.com/home/creating-sequences-and-evaluations\)](https://docs.mandiant.com/home/creating-sequences-and-evaluations).



For clarity, this section only discusses the Sequence Library, which appears as the default view in Security Validation. If you go to **Library > Evaluations**, the same information applies.

1. Go to **Library > Sequences**.

- You can use the **Filters** (any mix of **Tags**, **Content Source**, **Last Run Status** with **AND/OR** operators), or search functionality to help identify the specific content that you want to run. You can use the **Sort By** option to reorder the results by **Name**, **VID**, **Modified**, **Last Added**, **Last Run**, or **Total Runs**.
- Clicking on a Sequence in the Sequences pane updates the Sequence Preview pane with that Sequence-specific Name, Description, Actions, and Tags (if applicable).



Sequence Preview pane

- When there are Actions in the queue, the **Queue** button appears next to the **Add Sequence** (or **Add Evaluation**) buttons.
- The Add Sequence button displays, allowing you to add a new Sequence.

2. After selecting a Sequence, the Sequence Preview Pane reflects different functions you can do with the Sequence.

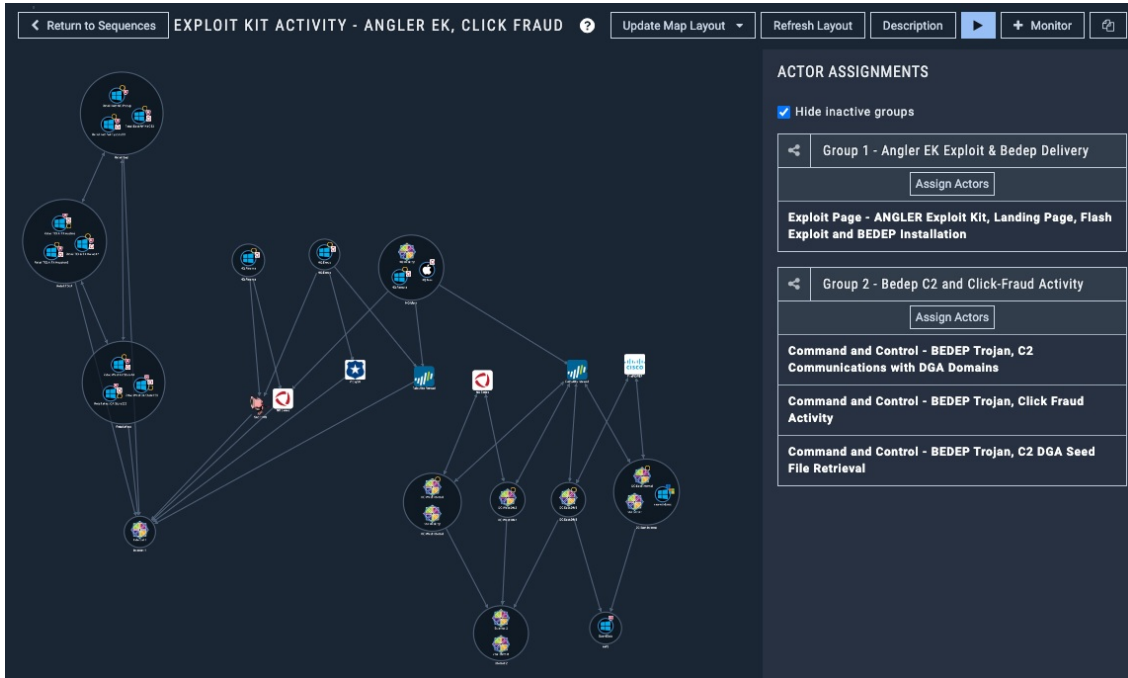
- **Run:** Displays the map and groups of Actions; this is where you select Actors to use for each group when the Sequence runs.
- **Run Bulk:** Displays Source and Destination Actor tag fields for each group in the Sequence
- **+ Queue:** Adds the Sequence groups into the queue (for use when creating Sequences and Evaluations)
- **Clone and Edit:** Creates a copy of the Sequence and allows you to customize it; or enables editing of the Sequence (user-created Sequences only)



NOTE: If a Sequence is part of a Monitor, you will only be able to edit the Name and Description. If you want to add or remove Actions, or change the grouping you need to either delete the Monitor or clone the Sequence.

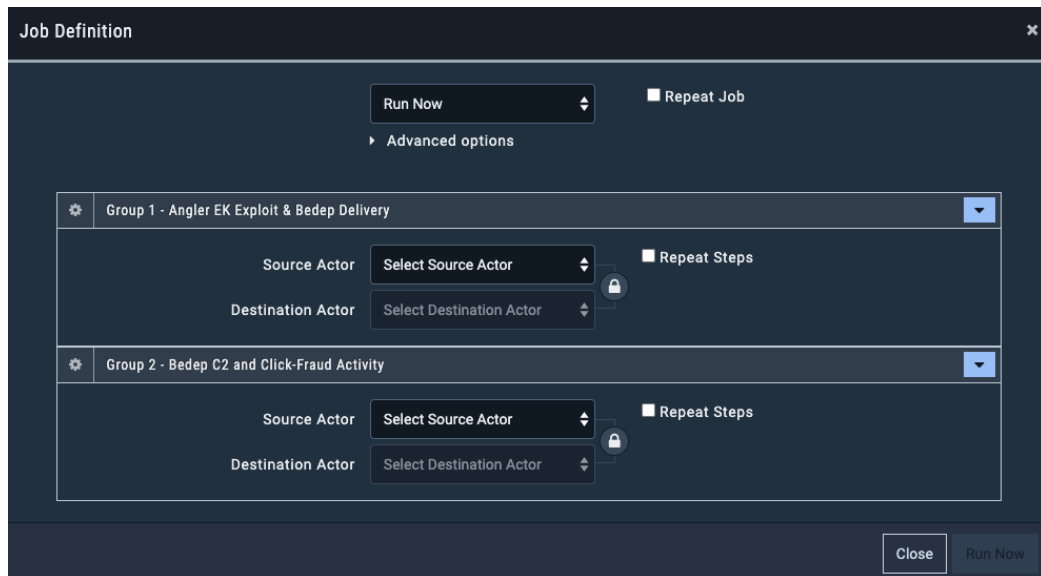
- **Clone:** Creates a copy of the Sequence and allows you to customize it

- **Delete:** Enables deletion of the Sequence (user-created Sequences only)
3. After clicking **Run**, the Assign Actors and Map page displays. There are five menu options and a sixth option for selecting Actors.



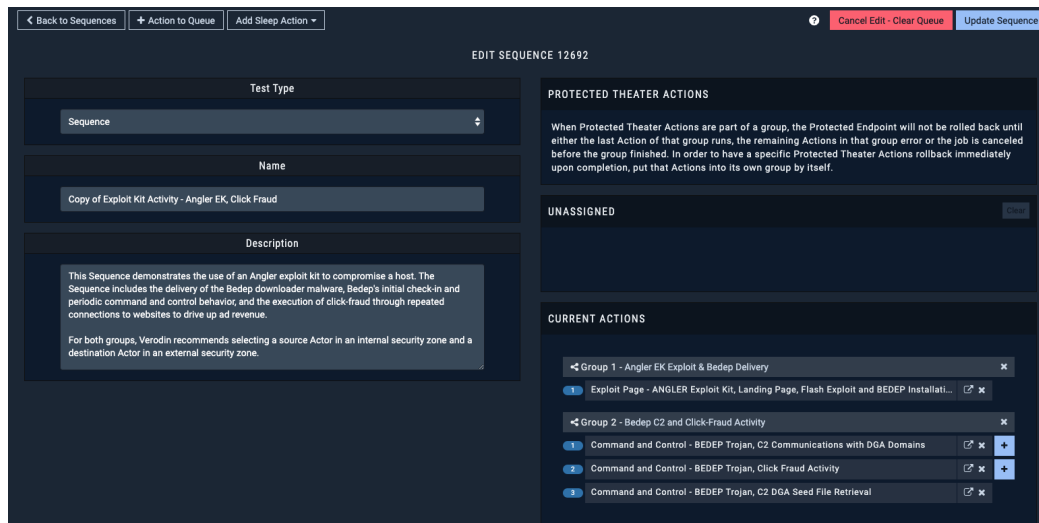
Selecting Actors for a Sequence

- a. **Description** displays the Sequence's description.
- b. **Run** displays the Job Definition form where you can review the Actor selections and submit the Sequences to run.



Job definition for a Sequence

- c. **+ Monitor** displays the Monitor Definition wizard for creating a Monitor.
- d. **Clone and Edit** displays the Edit Sequence interface that enables changes to the Sequence. (user created Sequences only).



Editing a Sequence

- e. **Delete** removes the Sequence from the platform (user-created Sequences only).
- f. **Assign Actors:** Use this to choose your Source and Destination Actors for each Group.

Sort Sequences and Evaluations

You can sort sequences and evaluations using the **Sort by** drop-down next to the search field. This drop-down list allows you to sort by **Name**, **VID**, **Modified**, **Last Added**, **Last Run**, and **Total Runs**.




For clarity, this section only discusses the Sequence Library. If you go to **Library > Evaluations**, the same information applies.

- Go to **Library > Sequences**.
- From the drop-down, choose an option for sorting the content:
 - **Sort by Name:** The Sequences appear in alphabetical order in the results list.

Sequence Library

Filters

Tags **OR** **AND** 

CONTENT SOURCE

- System Default
- User Created
- Outside Import
- Threat Intel

LAST RUN STATUS



- Never Ran
- Completed
- Errored
- Cancelled








CONTENT PACKS

- > 2023-08-22 - Content Expansion
- > 2023-08-08 - Content Expansion
- > 2023-07-28 - Content Expansion

Show All

Sequences (145)

Search Sort By Name  

S100-136	
Active Directory Reconnaissance with ADFIND.EXE	
S200-010	
add seq	
S100-036	
Anonymous FTP Access with Sensitive Data Exfil	
S100-027	
B734K Web Shell Activity	
S200-007	
Copy of Malicious Activity Scenario - TEMP.Armageddon Targets Organizations with BADBORSCH and DOUBLEDINO	
S100-052	
EMOTET Phishing and Post Compromise	
NEW S100-015	
Exploit Kit Activity - ANGLER EK, Click Fraud modified	

Sort by Name

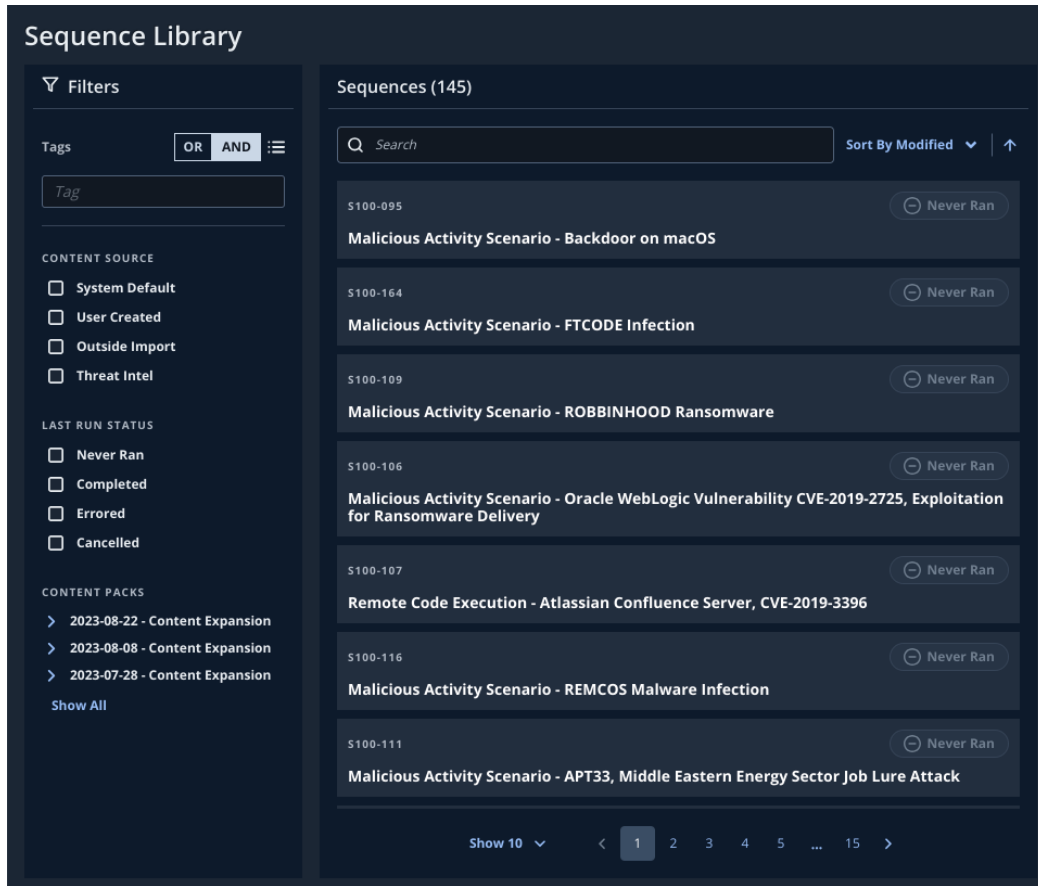
- **Sort by VID:** The Sequences appear in numeric order in the results list.

The screenshot displays the 'Sequence Library' interface. On the left, there is a 'Filters' sidebar with sections for 'Tags', 'CONTENT SOURCE' (System Default, User Created, Outside Import, Threat Intel), 'LAST RUN STATUS' (Never Ran, Completed, Errored, Cancelled), and 'CONTENT PACKS' (2023-08-22 - Content Expansion, 2023-08-08 - Content Expansion, 2023-07-28 - Content Expansion, Show All). The main area, titled 'Sequences (145)', features a search bar, a 'Sort By VID' dropdown, and a list of sequences. The sequences are sorted by VID, with the most recent (S100-015) at the top. Each sequence entry includes a VID, a title, and a 'Never Ran' status button. A 'NEW' badge is present next to S100-015. At the bottom, there is a pagination control showing 'Show 10' and page numbers 1 through 15.

VID	Sequence Name	Status
S100-010	Malicious Activity Scenario - MAZE Ransomware	Never Ran
S100-015	Exploit Kit Activity - ANGLER EK, Click Fraud modified	Never Ran
S100-016	Host Compromise via BARTALEX, PONY Loader, and VAWTRAK Trojan	Never Ran
S100-018	Post-Phishing Workstation & Database Compromises with Data Exfil	Never Ran
S100-019	Exploit Kit Activity - NUCLEAR Exploit Kit, Host Compromise	Never Ran
S100-020	Host Compromise via HUNTER Exploit Kit	Never Ran
S100-021	Exploit Kit Activity - NEUTRINO Exploit Kit - Afraidgate Campaign	Never Ran

Sort by VID

- **Sort by Modified:** The Sequences appear by when they were last updated.



Sequence Library

Filters

Tags: OR AND

CONTENT SOURCE

- System Default
- User Created
- Outside Import
- Threat Intel

LAST RUN STATUS

- Never Ran
- Completed
- Errored
- Cancelled

CONTENT PACKS

- > 2023-08-22 - Content Expansion
- > 2023-08-08 - Content Expansion
- > 2023-07-28 - Content Expansion

Show All

Sequences (145)

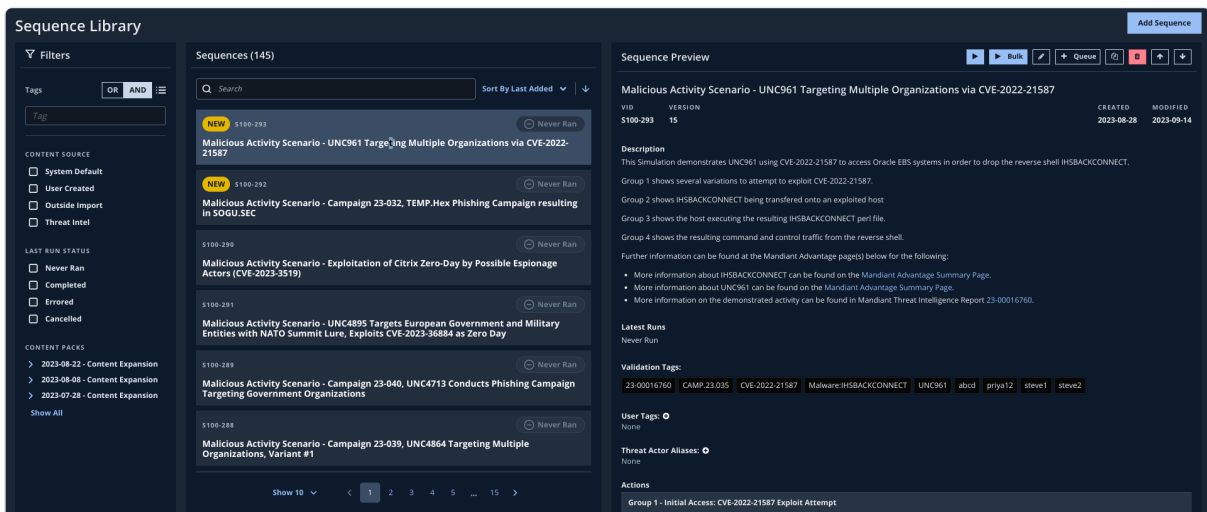
Search Sort By Modified

- S100-095 Never Ran
Malicious Activity Scenario - Backdoor on macOS
- S100-164 Never Ran
Malicious Activity Scenario - FTCODE Infection
- S100-109 Never Ran
Malicious Activity Scenario - ROBBINHOOD Ransomware
- S100-106 Never Ran
Malicious Activity Scenario - Oracle WebLogic Vulnerability CVE-2019-2725, Exploitation for Ransomware Delivery
- S100-107 Never Ran
Remote Code Execution - Atlassian Confluence Server, CVE-2019-3396
- S100-116 Never Ran
Malicious Activity Scenario - REMCOS Malware Infection
- S100-111 Never Ran
Malicious Activity Scenario - APT33, Middle Eastern Energy Sector Job Lure Attack

Show 10 1 2 3 4 5 ... 15

Sort by Last Updated

- **Last Added:** The Sequences appear when they were last added (with a New indicator, if they were added in the last two weeks).



Sequence Library

Filters

Tags: OR AND

CONTENT SOURCE

- System Default
- User Created
- Outside Import
- Threat Intel

LAST RUN STATUS

- Never Ran
- Completed
- Errored
- Cancelled

CONTENT PACKS

- > 2023-08-22 - Content Expansion
- > 2023-08-08 - Content Expansion
- > 2023-07-28 - Content Expansion

Show All

Sequences (145)

Search Sort By Last Added

- NEW** S100-293 Never Ran
Malicious Activity Scenario - UNC961 Targeting Multiple Organizations via CVE-2022-21587
- NEW** S100-292 Never Ran
Malicious Activity Scenario - Campaign 23-032, TEMP.Hex Phishing Campaign resulting in SOGU.SEC
- S100-290 Never Ran
Malicious Activity Scenario - Exploitation of Citrix Zero-Day by Possible Espionage Actors (CVE-2023-3519)
- S100-291 Never Ran
Malicious Activity Scenario - UNC4895 Targets European Government and Military Entities with NATO Summit Lure, Exploits CVE-2023-36894 as Zero Day
- S100-289 Never Ran
Malicious Activity Scenario - Campaign 23-040, UNC4713 Conducts Phishing Campaign Targeting Government Organizations
- S100-288 Never Ran
Malicious Activity Scenario - Campaign 23-039, UNC4864 Targeting Multiple Organizations, Variant #1

Show 10 1 2 3 4 5 ... 15

Sequence Preview

Malicious Activity Scenario - UNC961 Targeting Multiple Organizations via CVE-2022-21587

VID: S100-293 VERSION: 15 CREATED: 2023-08-28 MODIFIED: 2023-09-14

Description

This Simulation demonstrates UNC961 using CVE-2022-21587 to access Oracle EBS systems in order to drop the reverse shell IHSBACKCONNECT.

Group 1 shows several variations to attempt to exploit CVE-2022-21587.
Group 2 shows IHSBACKCONNECT being transferred onto an exploited host
Group 3 shows the host executing the resulting IHSBACKCONNECT perl file.
Group 4 shows the resulting command and control traffic from the reverse shell.

Further information can be found at the Mandiant Advantage pagets) below for the following:

- More information about IHSBACKCONNECT can be found on the Mandiant Advantage Summary Page.
- More information about UNC961 can be found on the Mandiant Advantage Summary Page.
- More information on the demonstrated activity can be found in Mandiant Threat Intelligence Report 23-00016760.

Latest Runs

Never Ran

Validation Tags:

23-00016760 CAMP-23-035 CVE-2022-21587 Malware:IHSBACKCONNECT UNC961 abcd priya12 steve1 steve2

User Tags:

None

Threat Actor Aliases:

None

Actions

Group 1 - Initial Access: CVE-2022-21587 Exploit Attempt

Sort by Last Added

- **Last Run:** The Sequences appear when they were last run, including the last run status.

Sequence Library

Filters

Tags OR AND

Tag

CONTENT SOURCE

System Default

User Created

Outside Import

Threat Intel

LAST RUN STATUS

Never Ran

Completed

Errored

Cancelled

CONTENT PACKS

> 2023-08-22 - Content Expansion

> 2023-08-08 - Content Expansion

> 2023-07-28 - Content Expansion

Show All

Sequences (145)

Q Search Sort By Last Run

S100-095 LAST RAN 2023-09-28: Completed

Malicious Activity Scenario - Backdoor on macOS

S100-109 LAST RAN 2023-09-28: Errored

Malicious Activity Scenario - ROBBINHOOD Ransomware

S100-107 LAST RAN 2023-09-28: Completed

Remote Code Execution - Atlassian Confluence Server, CVE-2019-3396

S100-164 Never Ran

Malicious Activity Scenario - FTCODE Infection

S100-106 Never Ran

Malicious Activity Scenario - Oracle WebLogic Vulnerability CVE-2019-2725, Exploitation for Ransomware Delivery

S100-116 Never Ran

Malicious Activity Scenario - REMCOS Malware Infection

S100-111 Never Ran

Malicious Activity Scenario - APT33, Middle Eastern Energy Sector Job Lure Attack

Sort by Last Run

- **Total Runs:** The Sequences appear based on the total number of times that they were run. The Preview pane lists the Latest Runs.

Sequence Library

Filters

Tags OR AND

Tag

CONTENT SOURCE

System Default

User Created

Outside Import

Threat Intel

LAST RUN STATUS

Never Ran

Completed

Errored

Cancelled

CONTENT PACKS

> 2023-08-22 - Content Expansion

> 2023-08-08 - Content Expansion

> 2023-07-28 - Content Expansion

Show All

Sequences (145)

Q Search Sort By Total Runs

S100-095 LAST RAN 2023-09-28: Completed

Malicious Activity Scenario - Backdoor on macOS

S100-109 LAST RAN 2023-09-28: Errored

Malicious Activity Scenario - ROBBINHOOD Ransomware

S100-107 LAST RAN 2023-09-28: Completed

Remote Code Execution - Atlassian Confluence Server, CVE-2019-3396

S100-164 Never Ran

Malicious Activity Scenario - FTCODE Infection

S100-106 Never Ran

Malicious Activity Scenario - Oracle WebLogic Vulnerability CVE-2019-2725, Exploitation for Ransomware Delivery

S100-116 Never Ran

Malicious Activity Scenario - REMCOS Malware Infection

S100-111 Never Ran

Malicious Activity Scenario - APT33, Middle Eastern Energy Sector Job Lure Attack

Sequence Preview

Malicious Activity Scenario - Backdoor on macOS

VID S100-095 VERSION 2 CREATED 2023-03-27 MODIFIED 2023-03-27

Description

This Sequence demonstrates a malicious scenario where a backdoor is created on a macOS device. The Sequence starts with the malicious file transfer of ncst. The specific file leverages a vulnerability in Apple's App signing process and appears to be signed by Apple. Once transferred, the built-in application firewall is disabled, and the backdoor is set up on the host.

For group one, Mandiant Security Validation recommends selecting an Actor in an internal security zone as the source and an Actor in an external untrusted security zone as the destination. A macOS Actor must be selected for group two.

Job ID	Run On	Run By	Status
93	2023-09-28 16:35:30 UTC	Default Admin	Completed
90	2023-09-28 16:16:58 UTC	Default Admin	Completed

User Tags: None

Threat Actor Aliases: None

Actions

Group 1 - Malicious File Transfer of Ncat

Malicious File Transfer - Ncat Code Signed by Apple, Download



You can toggle the order of the results from ascending to descending by clicking the up/down arrow next to **Sort by**.