



Official Incident Report

Event ID: 161

Rule Name: SOC211 - Utilman.exe Winlogon Exploit Attempt

Table of contents

Official Incident Report	1
Event ID: 161	1
Rule Name: SOC211 - Utilman.exe Winlogon Exploit Attempt	1
Table of contents	2
Alert	3
Detection	4
Verify	4
Analysis	7
Containment	9
Summary	9
Lesson Learned	11
Remediation Actions	11
Appendix	12
MITRE ATT&CK	12
Artifacts	13

Alert

Based on the information that the alert provided, it appears that there is a suspicious file detected on a system named "**Henry**" with an IP address of **172.16.17.149**. The Alert is triggered by the **SOC211** rule for **Utilman.exe Winlogon Exploit Attempt**.

Utilman.exe is the utility program that is launched when the "Ease of Access" button on the login screen is clicked.

Upon reviewing the provided alarm, it is observed that a Utilman.exe process runs a command as a child process of Winlogon.exe which leads to the creation of a user account.

SEVERITY	DATE	RULE NAME	EVENTID	TYPE
Medium	2023-06-21 11:02	SOC211 - Utilman.exe Winlogon Exploit Attempt	161	LOLBin
EventID : 161				
Event Time : 2023-06-21 11:02				
Rule : SOC211 - Utilman.exe Winlogon Exploit Attempt				
Level : Security Analyst				
Hostname : Henry				
Ip Address : 172.16.17.149				
Process Name : Utilman.exe				
Process Hash : ded8fd7f36417f66eb6ada10e0c0d7c0022986e9				
Parent Process : Winlogon.exe				
Command Line : net user superman onepunch123 /add				
Trigger Reason : Command Launched from Winlogon				
Device Action : Allowed				

The device action is marked as "allowed", indicating that no action was taken by the device to prevent or block the execution of the file.

An alert was triggered due to a command being executed under the Winlogon process based on the trigger reason provided. The hash of the process is given in the details:
ded8fd7f36417f66eb6ada10e0c0d7c0022986e9

Overall, it appears that there may be suspicious activity occurring on the system, and further investigation is needed to identify the extent of the activity and determine any necessary actions to remediate the situation.

Detection

Verify

As a security analyst, one of the first steps we take to verify the alert and determine whether it is a false positive or a true positive incident is to analyze the logs collected from the host by our security products.

The first step we can take to investigate the hash value of the suspicious process is to use online threat intelligence platforms such as VirusTotal, Hybrid Analysis, and MalwareBazaar.

The screenshot shows the VirusTotal analysis interface for a file named 'Cmd.Exe'. The file is identified as 'File distributed by Microsoft' with a green checkmark. The hash value is 'bc866cfcdda37e24dc2634dc282c7a0e6f55209da17a8fa105b07414c0e7c527'. The file size is 272.00 KB and the last analysis date is 1 hour ago. The file is categorized as 'Cmd.Exe' and is marked as 'signed'. The signature verification shows 'Signed file, valid signature'. The file version information includes: Copyright © Microsoft Corporation. All rights reserved., Product Microsoft® Windows® Operating System, Description Windows Command Processor, Original Name Cmd.Exe, Internal Name cmd, File Version 10.0.17763.1697 (WinBuild.160101.0800), and Date signed 2022-07-16 08:16:00 UTC.

Based on the information provided by VirusTotal, it appears that the utilman.exe in fact is a Cmd.exe. It is legit and has been flagged as benign by all security vendors. The binary is "Signed", indicating that it is a legitimate Windows binary file.

The screenshot shows a 'Identify the Binary' dialog box. The dialog box has a title bar with a close button (X). The main text reads: 'Determine which binary is supplied by the operating system but is also home to suspicious activities. To do this, you can resort to the alert details on the Monitoring page or Endpoint Security.' Below the text, there are two bullet points: 'Monitoring' and 'Endpoint Security'. At the bottom right, there is a 'Next' button.

As we identified the binary related to the suspicious activities is cmd.exe which is named utilman.exe. Now we can deeply analyze the related process for more context.

To do this we can filter Henry’s hostname or IP address in the “Endpoint Security” section.

Henry

Henry

172.16.17.149

Host Information

Hostname: Henry

Domain: LetsDefend

IP Address: 172.16.17.149

Bit Level: 64

OS: Windows 10

Primary User: Henry

Client/Server: Client

Last Login: Jun, 21, 2023, 12:24 PM

Containment: ☐

Processes 64

Network Action 74

Terminal History 8

Browser History 0

Results: 10

EVENT TIME	PROCESS NAME	PROCESS ID	COMMAND LINE
2023-06-21 10:00:20.441	winlogon.exe	784	winlogon.exe
2023-06-21 10:00:20.442	smss.exe	476	\SystemRoot\System32\smss.exe
2023-06-21 10:00:20.467	smss.exe	7860	\SystemRoot\System32\smss.exe 000000cc 00000084
2023-06-21 10:00:20.508	smss.exe	7860	\SystemRoot\System32\smss.exe 000000cc 00000084

There are 64 processes running on Henry’s machine. To verify the process utilman.exe we can filter the processes by “**Process Name contains utilman**”.

Processes 64

Network Action 74

Terminal History 8

Browser History 0

Results: 10

EVENT TIME	PROCESS NAME	PROCESS ID	COMMAND LINE
	lman.exe	5956	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
2023-06-21 11:00:00.743	utilman.exe	5956	net user

There are 6 processes of utilman.exe and they match with alert creation date.

Processes 64

Network Action 74

Terminal History 8

Browser History 0

Results: 10

EVENT TIME	PROCESS NAME	PROCESS ID	COMMAND LINE
2023-06-21 10:58:30.135	utilman.exe	5956	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
2023-06-21 11:00:00.743	utilman.exe	5956	net user
2023-06-21 11:00:09.52	utilman.exe	5956	whoami
2023-06-21 11:02:12.657	utilman.exe	5956	net user superman onepunch123 /add
2023-06-21 11:03:14.706	utilman.exe	5956	net localgroup administrators superman /add

We can click the arrow button next to the event time to inspect the details of the specific process. By looking at the details of the process that triggered the alert, we see the parent path of the process is: “C:\Windows\System32\winlogon.exe” and the image path of the process is “C:\Windows\System32\utilman.exe”

The screenshot shows a security monitoring interface with a top navigation bar containing tabs for 'Processes' (64), 'Network Action' (74), 'Terminal History' (8), and 'Browser History' (0). The 'Processes' tab is active. Below the navigation bar is a table with columns: 'EVENT TIME', 'PROCESS NAME', 'PROCESS ID', and 'COMMAND LINE'. The table lists several events, with the fourth event selected, indicated by a green arrow icon. The selected event has a time of '2023-06-21 11:02:12.657', process name 'utilman.exe', process ID '5956', and command line 'net user superman onepunch123 /add'. Below the table, a detailed view of the selected event is shown, including fields for 'Event Time', 'Process ID', 'Image Path', 'Process User', 'Parent Name', 'Parent Path', and 'Command Line'. The 'Image Path' is 'C:\Windows\System32\utilman.exe', the 'Process User' is 'NT AUTHORITY\SYSTEM', the 'Parent Name' is 'winlogon.exe', and the 'Parent Path' is 'C:\Windows\System32\winlogon.exe'. The 'Command Line' is 'net user superman onepunch123 /add'.

EVENT TIME	PROCESS NAME	PROCESS ID	COMMAND LINE
2023-06-21 10:58:30.135	utilman.exe	5956	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
2023-06-21 11:00:00.743	utilman.exe	5956	net user
2023-06-21 11:00:09.52	utilman.exe	5956	whoami
2023-06-21 11:02:12.657	utilman.exe	5956	net user superman onepunch123 /add

Event Time : 2023-06-21 11:02:12.657
Process ID : 5956
Image Path : C:\Windows\System32\utilman.exe
Process User : NT AUTHORITY\SYSTEM
Parent Name : winlogon.exe
Parent Path : C:\Windows\System32\winlogon.exe
Command Line : net user superman onepunch123 /add

The NT "AUTHORITY/SYSTEM" created a new user with the name "Superman" and the password "onepunch123".

By looking at the processes of Henry's machine processes we verified the alert is **true positive** and the binary (utilman.exe named cmd.exe) has executed on the system.

Analysis

As part of the investigation process, the second step of the playbook requires us to determine the suspicious activity.

Incident Name:

Description:

Incident Type:

Created Date:

Determine Suspicious Activity

Previously, you found the related binary. Now, we'd like you to determine whether it was used for malicious purposes. You can use the link below to determine how legal binary can be used to perform malicious activities.

- LOLBAS Project

There are some characteristics common to command lines:

- They often have a file-path or other artifact as one of the arguments, that changes based on the user environment or machine, such as usernames or system GUIDs in file paths.
- The order of arguments in the command change, or a single argument has a slightly different value.
- They can have randomly generated strings in embedded URLs or file paths.
- They can be obfuscated on purpose by attackers (variable assignment, invocation of string expressions created on the fly, etc).

(list source: sophos.com)

Is the current activity suspicious?

No

Yes, suspicious

The terminal history can provide valuable insights into the commands executed by the user and help us understand the scope and intent of the suspicious activity. To access the terminal history, we can filter the endpoint security tab by username "Henry" and navigate to the user's Terminal History

Host Information

Hostname: Henry

Domain: LetsDefend

IP Address: 172.16.17.149

Bit Level: 64

OS: Windows 10

Primary User: Henry

Client/Server: Client

Last Login: Jun, 21, 2023, 12:24 PM

Action

Containment: ☐

Processes 64

Network Action 74

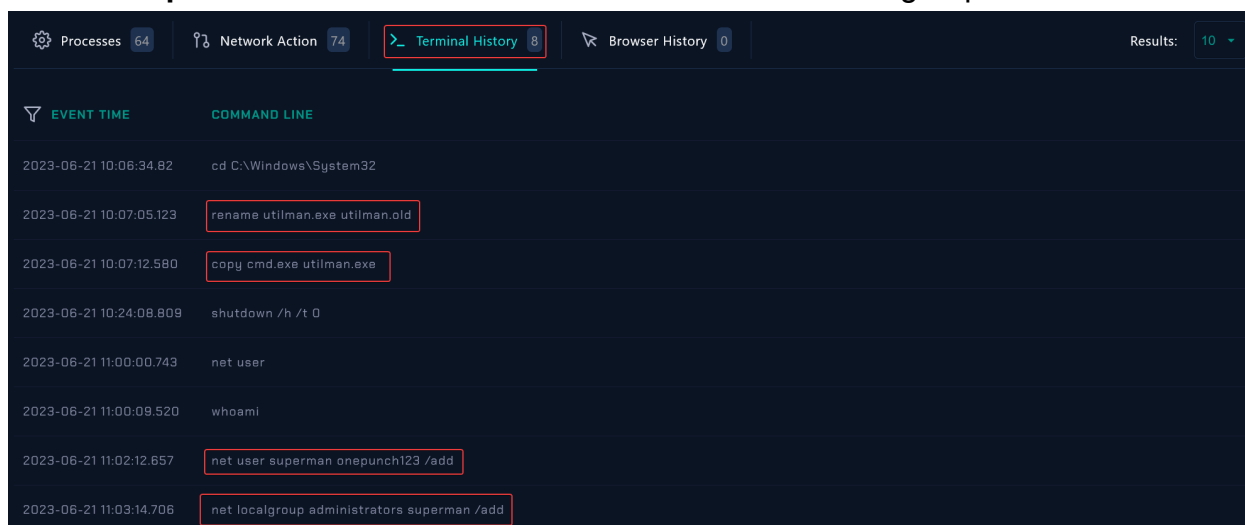
>_ Terminal History 8

Browser History 0

Results: 10

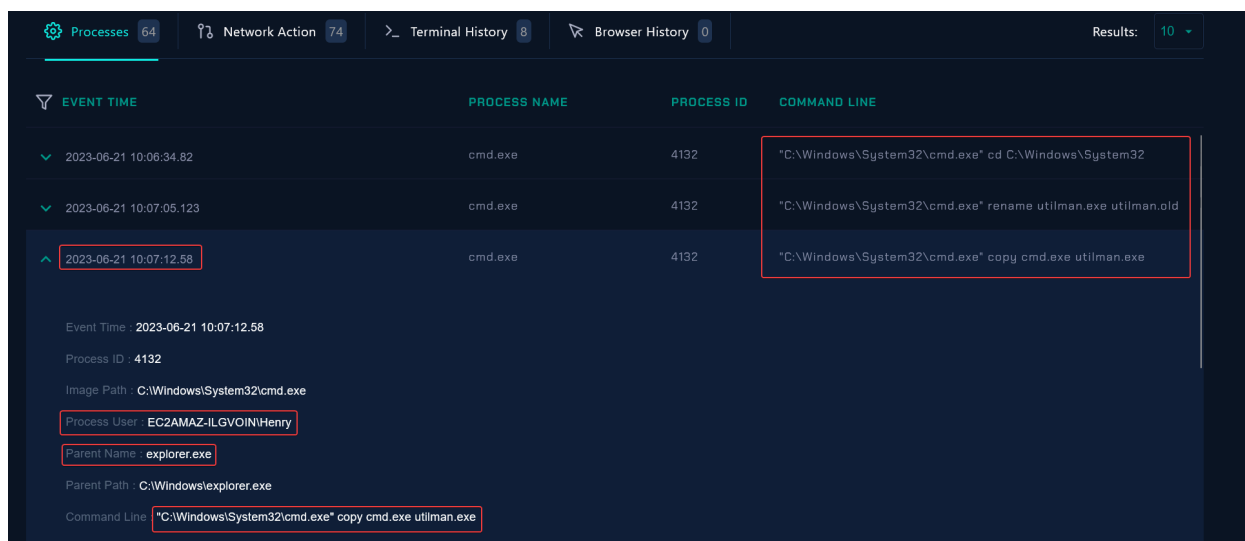
By examining the terminal history, we can gain a better understanding of the general situation and the commands that the user executed.

As we look at the terminal history we can see that there are indicators of exploiting utilman.exe. After the user reboots the host machine he gained system access and added a **superman** named new user to the administrators localgroup.



EVENT TIME	COMMAND LINE
2023-06-21 10:06:34.82	cd C:\Windows\System32
2023-06-21 10:07:05.123	rename utilman.exe utilman.old
2023-06-21 10:07:12.580	copy cmd.exe utilman.exe
2023-06-21 10:24:08.809	shutdown /h /t 0
2023-06-21 11:00:00.743	net user
2023-06-21 11:00:09.520	whoami
2023-06-21 11:02:12.657	net user superman onepunch123 /add
2023-06-21 11:03:14.706	net localgroup administrators superman /add

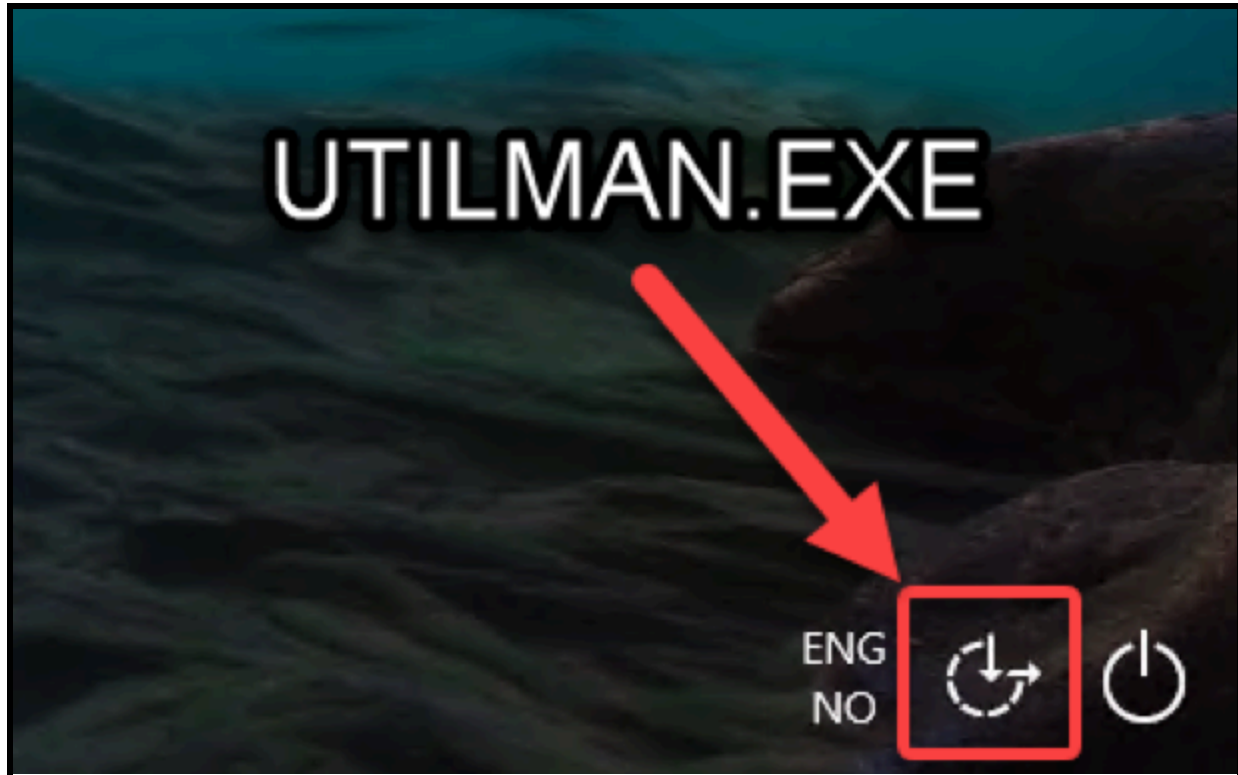
And by looking at the processes, we can see that the parent process of the commands was explorer.exe.



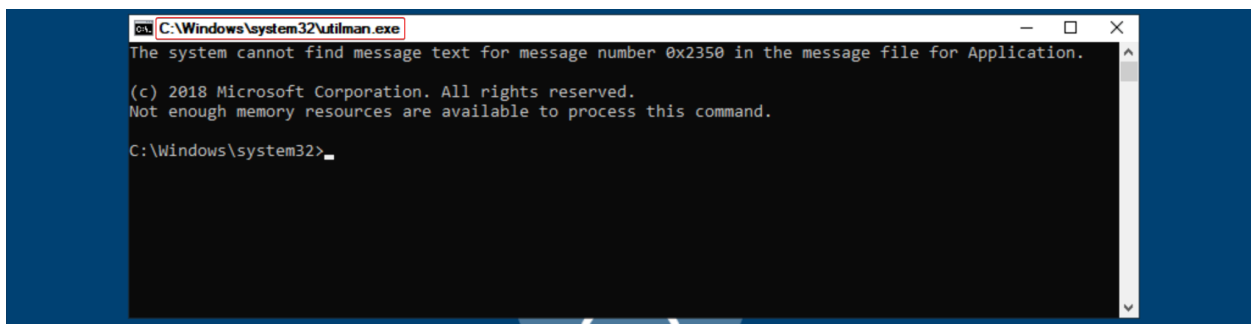
EVENT TIME	PROCESS NAME	PROCESS ID	COMMAND LINE
2023-06-21 10:06:34.82	cmd.exe	4132	"C:\Windows\System32\cmd.exe" cd C:\Windows\System32
2023-06-21 10:07:05.123	cmd.exe	4132	"C:\Windows\System32\cmd.exe" rename utilman.exe utilman.old
2023-06-21 10:07:12.58	cmd.exe	4132	"C:\Windows\System32\cmd.exe" copy cmd.exe utilman.exe

Event Time : 2023-06-21 10:07:12.58
Process ID : 4132
Image Path : C:\Windows\System32\cmd.exe
Process User : EC2AMAZ-ILGVOIN\Henry
Parent Name : explorer.exe
Parent Path : C:\Windows\explorer.exe
Command Line : "C:\Windows\System32\cmd.exe" copy cmd.exe utilman.exe

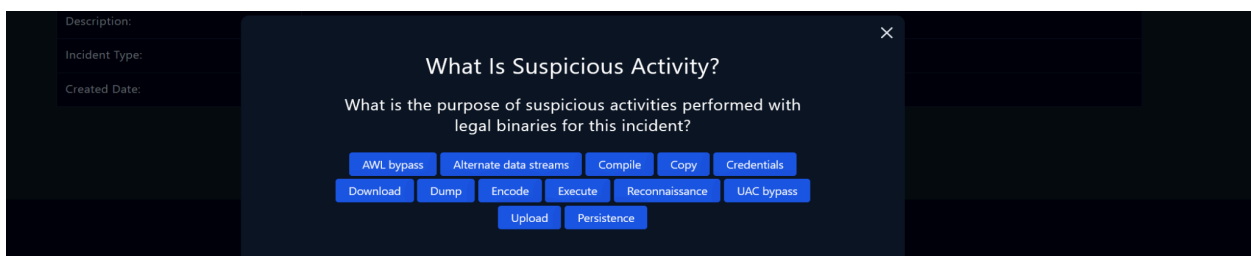
The user started by navigating to the System32 directory and renaming the legitimate "utilman.exe" file to "utilman.old." This action was followed by copying the "cmd.exe" file and renaming it as "utilman.exe." the attacker can gain access to the cmd terminal on logon screen.



By clicking on the symbol the attacker gains access to cmd.

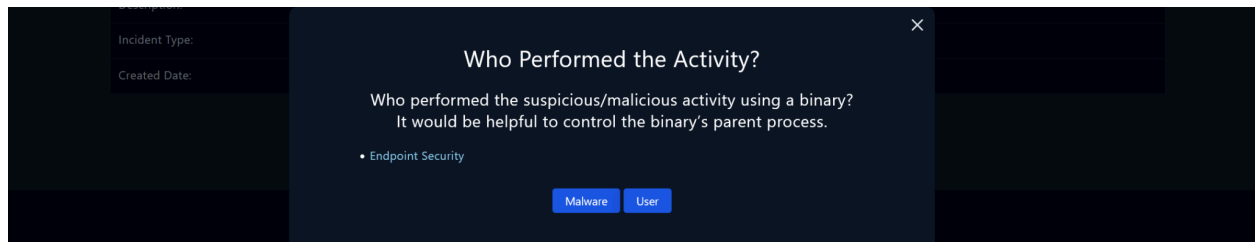


The commands executed indicate a clear intent to manipulate system files and potentially establish persistent access. So the answer for the next playbook question is **“Persistence”**



The user started by navigating to the System32 directory and renaming the legitimate "utilman.exe" file to "utilman.old." This action was followed by copying the "cmd.exe" file and renaming it as "utilman.exe."

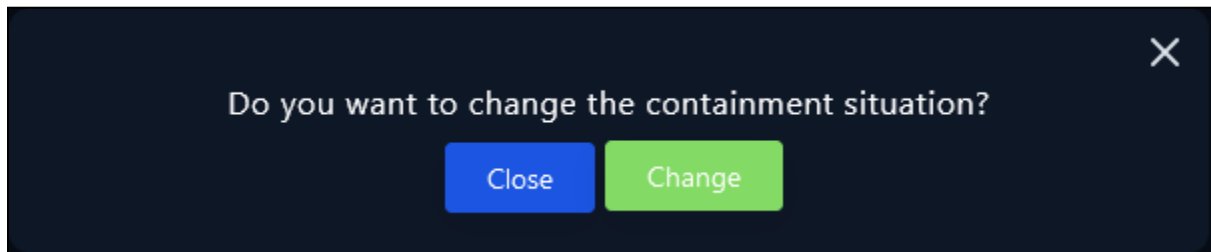
By looking at the parent process of the commands we have identified the user performed the activity.



The most alarming commands involve the creation of a new user account named "superman" with the password "onepunch123" using the "net user" command. The user then added this newly created account to the local administrators group with the "net localgroup administrators superman /add" command. These actions signify an explicit attempt to establish a backdoor account with elevated privileges, potentially granting unauthorized access and control over the system.

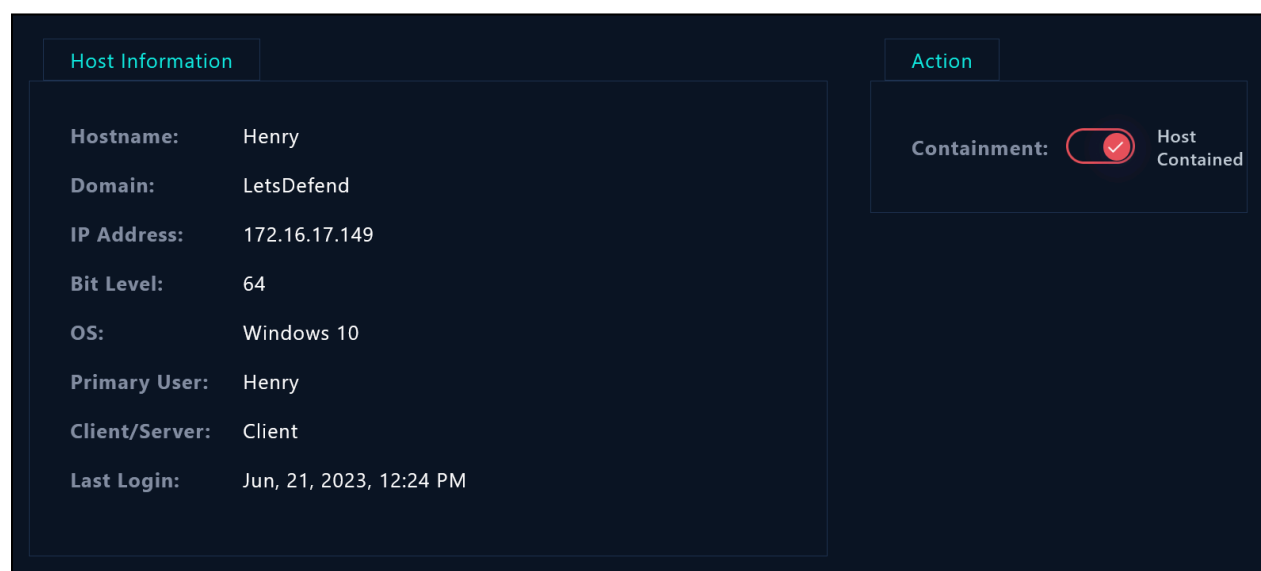
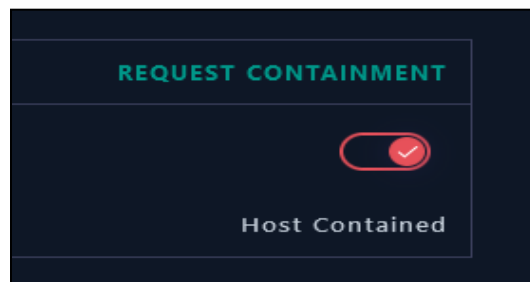
Containment

Based on the information gathered during the investigation, it is highly likely that the system has been compromised. To prevent further data loss or unauthorized access, it is recommended to isolate the system from the network immediately.



Isolation of the host can be made from the endpoint security tab.

Hostname	Henry
IP Address	172.16.17.149



Summary

The incident involves a compromised system named "Henry" with an IP address of 172.16.17.149. The alert was triggered by the detection of a suspicious file, "utilman.exe," based on the SOC211 rule for the Winlogon Exploit Attempt.

Upon further analysis, it was discovered that the suspicious process involved the execution of a command as a child process of "winlogon.exe," leading to the creation of a user account.

Investigation into the alert involved verifying its validity. The suspicious file, identified as "cmd.exe" masquerading as "utilman.exe," was confirmed as legitimate and benign by various security vendors. The analysis of Henry's processes revealed six instances of "utilman.exe," matching the alert creation date, further substantiating the alert's authenticity.

Terminal history examination revealed a series of malicious commands executed by the user. These actions included renaming the original "utilman.exe," copying "cmd.exe" as "utilman.exe," performing system shutdown, retrieving user account information, and creating a new user account with administrative privileges.

The findings indicate a deliberate attempt to replace a legitimate system utility with another file, manipulate user accounts, and escalate privileges. The incident raises concerns about unauthorized access and persistence by creating new user.

Based on the findings of the incident, immediate action was taken to isolate the compromised system, named "Henry," with the IP address 172.16.17.149. Isolation is a critical step to prevent further unauthorized access and potential spread of the compromise to other systems within the network.

Lesson Learned

- Monitoring and analyzing user behavior, such as terminal history and command execution, can help detect and prevent unauthorized activities, enabling early detection of compromises and potential insider threats.
- Anti-virus software is not always 100% effective and should not be relied upon as the only line of defense.
- Regularly monitor and analyze process trees to identify any unusual or suspicious parent-child relationships, which can provide insights into the execution techniques employed by attackers.

Remediation Actions

- Delete any unauthorized user accounts created during the incident to eliminate potential backdoors or access points for attackers.
- Identify and remove any malicious files, such as the disguised "utilman.exe" (cmd.exe) file
- Restrict user permissions on System32: Modify user permissions and access controls on the System32 directory to prevent unauthorized write access.
- Isolate the compromised machine from the network to prevent the attacker from accessing other resources and systems within the organization.

Appendix

MITRE ATT&CK

Persistence	Privilege Escalation	Defense Evasion
T1136: Create Account	T1546: Event Triggered Execution	T1036: Masquerading
T1136.003: Cloud Account	T1546.008: Accessibility Features	T1036.007: Double File Extension
T1136.002: Domain Account		T1036.001: Invalid Code Signature
T1136.001: Local Account		T1036.008: Masquerade File Type
T1546: Event Triggered Execution		T1036.004: Masquerade Task or Service
T1546.008: Accessibility Features		T1036.005: Match Legitimate Name or Location
		T1036.003: Rename System Utilities
		T1036.002: Right-to-Left Override
		T1036.006: Space after Filename

MITRE Tactics	MITRE Techniques
Persistence	T1136 Create Account
Persistence	T1546 EventTriggered Execution
Privilege Escalation	T1546 EventTriggered Execution
Defense Evasion	T1036 Masquerading

Artifacts

Filename	SHA256 Value - Path
utilman.exe (cmd)	DED8FD7F36417F66EB6ADA10E0C0D7C0022986E9
utilman.old	C:\Windows\System32\utilman.old

IOC TYPE	VALUE
User	superman
password	onepunch123