**ResourcePacks Lab**

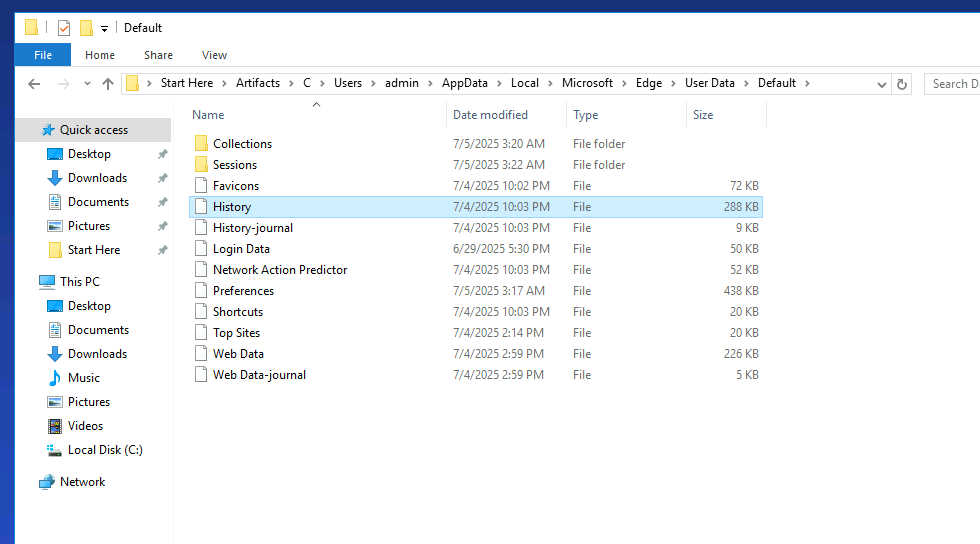
**SCENARIO:** **Manuel, an enthusiastic gamer, recently installed popular Minecraft resource packs on his new computer after classmates shared download links with him. Soon after, he noticed system slowdowns, unexpected pop-ups, and malfunctioning applications. You have been asked to investigate how a suspicious file infiltrated the machine, whether it created hidden persistence mechanisms, and assess any impact on personal data or overall system stability.**

Initial Access

Q1

The threat actor has set up a video to provide the link that hosts the filefix command file. What is the YouTube channel display name of the threat actor?

Start by checking user browser history and you will be able to see this



A screenshot of a computer

AI-generated content may be incorrect.

Going to the youtube link

<https://www.youtube.com/watch?v=oGrKXom1S7E>

A screenshot of a video game

AI-generated content may be incorrect.

Note:I will keep the video content as a surprise

A screenshot of a computer

AI-generated content may be incorrect.

Q2

Provide the full url that was used to deliver a malicious command to the victim.

We already have the short url link now we need to look for the full url

A screenshot of a computer

AI-generated content may be incorrect.

<http://ultimatempacks.at/autoinstall.html>

A screenshot of a computer error

AI-generated content may be incorrect.

Execution

Q1

When did the user execute the malicious command?

A white rectangular object with a black border

AI-generated content may be incorrect.

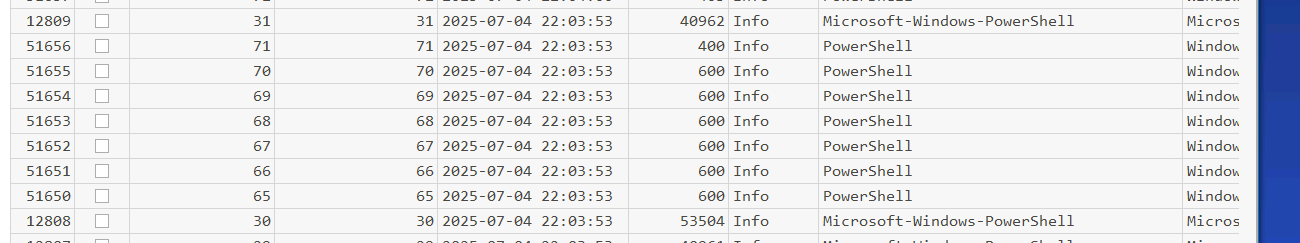
The user started the download at least after this time

2025-07-04 22:03:30

Using

EvtxECmd.exe -d "C:\Users\Administrator\Desktop\Start Here\Artifacts\C\Windows\System32\winevt\Logs" --csv "C:\Users\Administrator\Desktop\Start Here\Artifacts\Evtx\_Output"

I was able to found this



Further investigation confirmed it

A screenshot of a computer

AI-generated content may be incorrect.

Q2

Provide the full fake file path that appeared to trick the user into executing the command?

From previous log that we found

A screenshot of a computer program

AI-generated content may be incorrect.

C:\manuel\AppData\Roaming\.minecraft\resourcespack\Hyper-Realistic-1.7.2.zip

A screenshot of a computer

AI-generated content may be incorrect.

Q3

Provide the name of the script that was executed by the user with this command?

In the same powershell command

A screen shot of a computer code

AI-generated content may be incorrect.

ultimatetexture.jpg

A screenshot of a computer

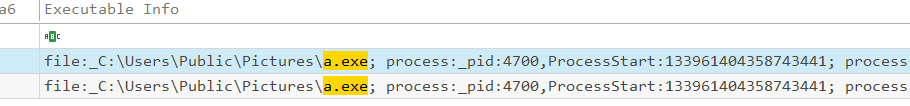
AI-generated content may be incorrect.

Q4

The script fetched an executable file from the C2 server and executed it from another built-in user folder. Provide the full path of this file.

Top of Form

Looking a little I found this



This cant be a normal exe file found in pictures

C:\USERS\PUBLIC\PICTURES\A.EXE A screenshot of a computer error

AI-generated content may be incorrect.

Discovery

Q1

The threat actor conducted some enumeration on the system once it gained initial access; how many times was `net.exe`Used by the threat actor during the discovery phase?

A screenshot of a computer

AI-generated content may be incorrect.

Also found a third one later on

A screenshot of a computer

AI-generated content may be incorrect.

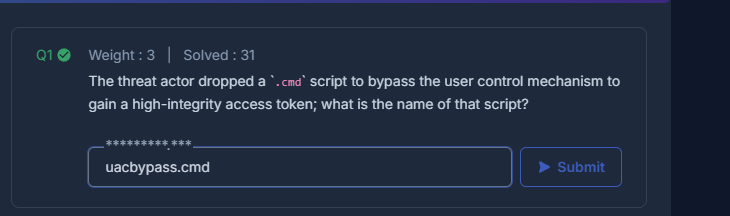
Privilege Escalation

Q1

The threat actor dropped a `.cmd` script to bypass the user control mechanism to gain a high-integrity access token; what is the name of that script?

By using pecmd output I looked for .cmd and found

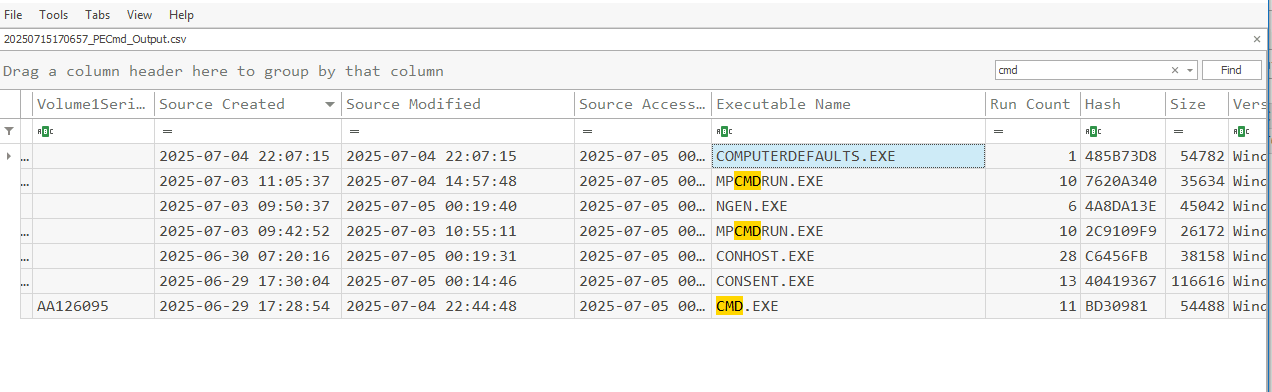
uacbypass.cmd



Q2

To understand the behavior of the threat actor, decode the Base64 string and find out how many seconds was set to delay before proceeding with the cleanup?

Top of Form

Top of Form

COMPUTERDEFAULTS.EXE

A screenshot of a computer

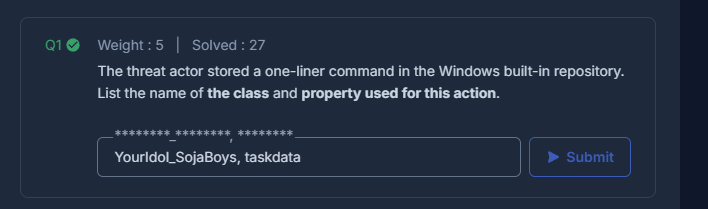
AI-generated content may be incorrect.

Persistence

Q1

The threat actor stored a one-liner command in the Windows built-in repository. List the name of **the class** and **property used for this action**.

A screenshot of a computer program

AI-generated content may be incorrect. 

YourIdol\_SojaBoys, taskData

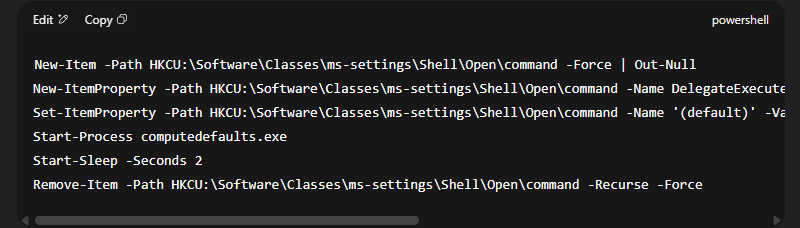
Q2

To understand the behavior of the threat actor, decode the Base64 string and find out how many seconds was set to delay before proceeding with the cleanup?

Using evtxcmd output

A screenshot of a computer

AI-generated content may be incorrect.



A screenshot of a computer

AI-generated content may be incorrect.

Q3

The threat actor created a backdoor user with a name that mimics the actual user on this machine. When was that backdoor created?

Using evtxcmd output again I searched for event id 4720 that represented account creation and found this

A screenshot of a computer

AI-generated content may be incorrect. A screenshot of a computer

AI-generated content may be incorrect. A screenshot of a computer

AI-generated content may be incorrect.

Privilege Escalation(again)

Q1

The threat actor dropped another script to add special privileges to the newly created backdoor account without adding it to the Administrators group. What is the name of this script?

A screenshot of a computer

AI-generated content may be incorrect. A screenshot of a computer

AI-generated content may be incorrect.

Q2

Which privilege was assigned to the backdoor user?

A screenshot of a computer

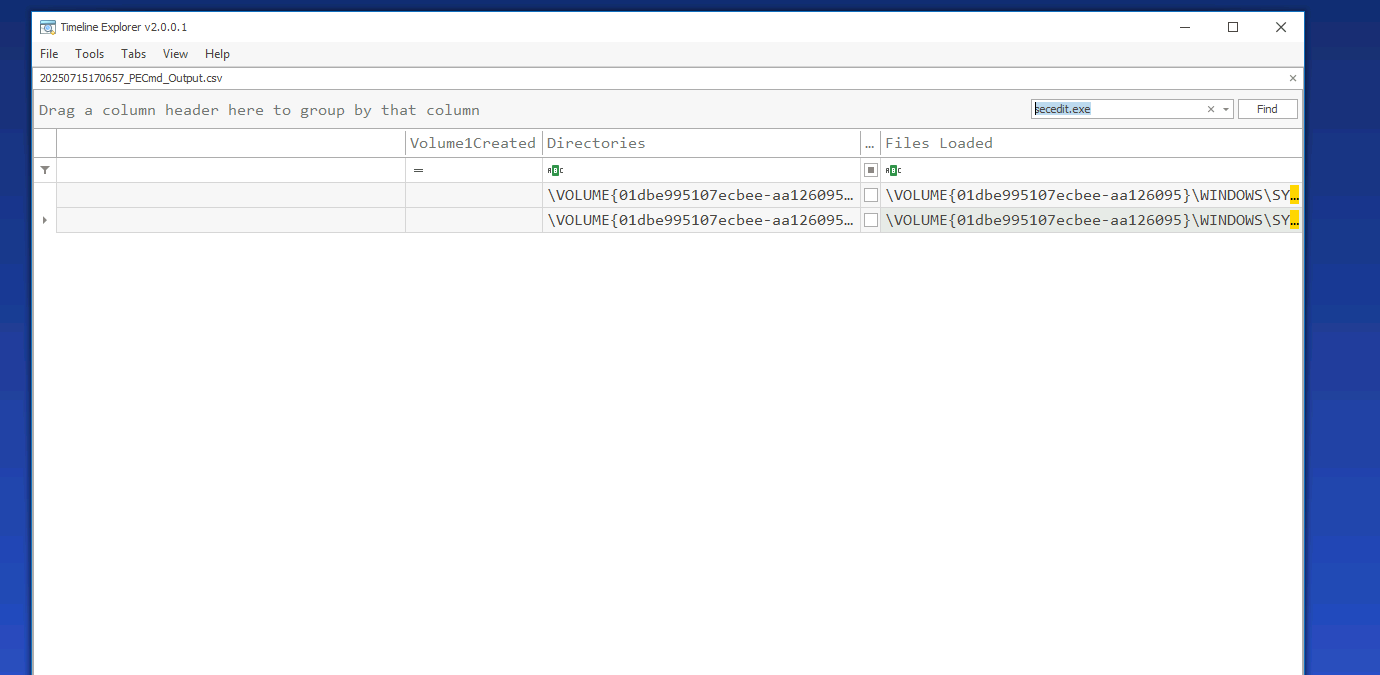
AI-generated content may be incorrect.

Defense Evasion

Q15

To import a security template file, the threat actor needs to export the config file to an `.inf` file, and a `.sdb` file will be created during import. List the file names of both files.

So I first found the .inf script here

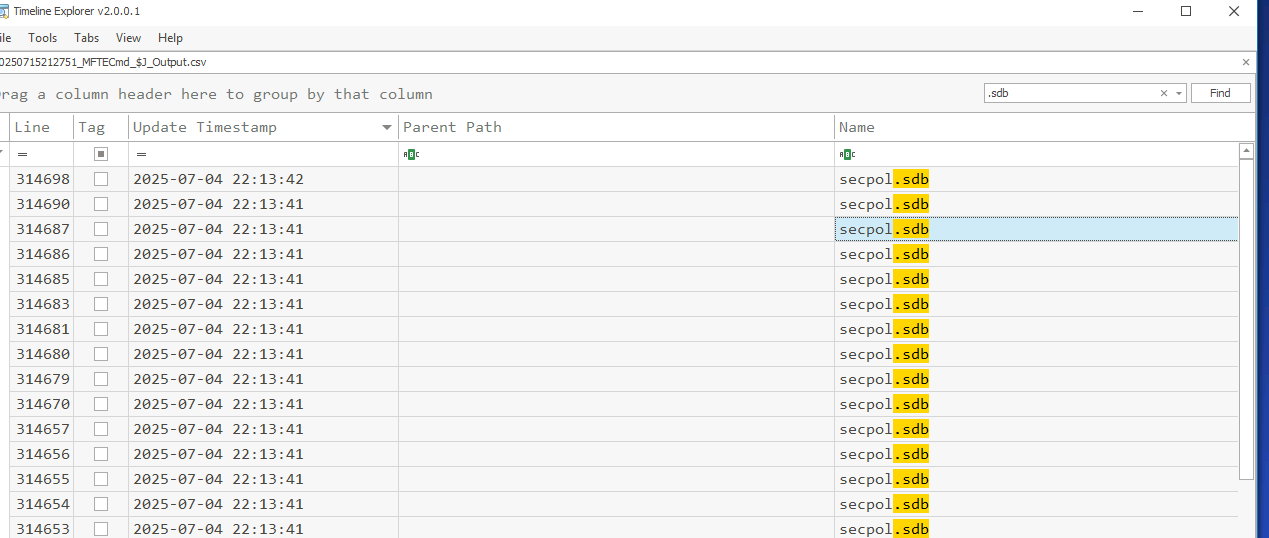


Secedit is the one that Is used to import a security template in windows

A screenshot of a computer

AI-generated content may be incorrect.

But I couldn’t find the .sdb file so I tried to load the $Extended/$J via

MFTECmd.exe -f "C:\Users\Administrator\Desktop\Start Here\Artifacts\C\$Extend\$UsnJrnl\$J" --csv "C:\Users\Administrator\Desktop\Start Here\Artifacts\C\MFTE\_USN\_Output.csv" 

And found it

A screenshot of a computer error

AI-generated content may be incorrect.

Defense Evasion

Q15

To import a security template file, the threat actor needs to export the config file to an `.inf` file, and a `.sdb` file will be created during import. List the file names of both files.

With pecmd output I tried to search for powershell command and found ibackdoor.ps1

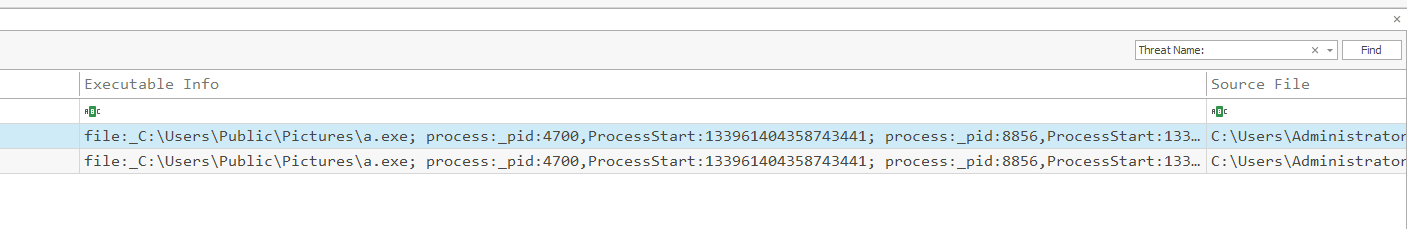
A screenshot of a computer

AI-generated content may be incorrect.

Q16

It appears that Windows Defender has detected the malicious executable and taken some measures against it. Please list the process ID (PID) of the two processes that were detected by Windows Defender.

Using evtxcmd output

 A screenshot of a computer error

AI-generated content may be incorrect.