**[Job Trap Lab](https://cyberdefenders.org/blueteam-ctf-challenges/job-trap/)**

Scenario:

The SOC team received a high-priority alert regarding suspicious activity on an employee's workstation. The alert indicated that a Word document containing malicious macros was executed, followed by an established connection to a suspicious web server. After asking the affected employee, we found that he had opened what appeared to be a job application resume earlier that morning, enabling macros when prompted.

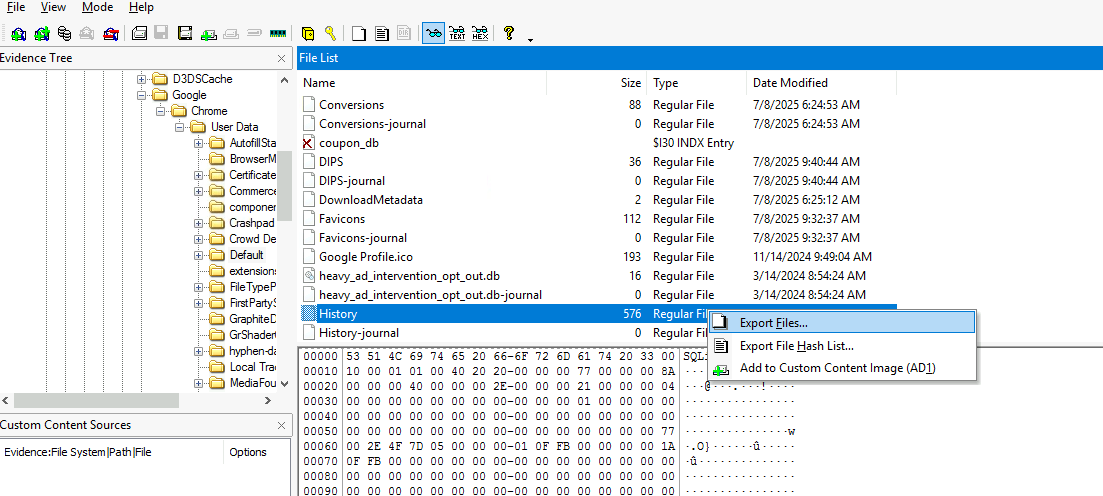
As a forensics investigator, you have been provided with a disk triage of the victim's workstation and tasked with conducting a comprehensive analysis to reconstruct the attack timeline, identify all malicious artifacts, and determine the full extent of the compromise.

Initial access

Q1: During the initial compromise phase, a malicious document was downloaded to the victim's system. What is the timestamp when this download activity began?

Top of Form

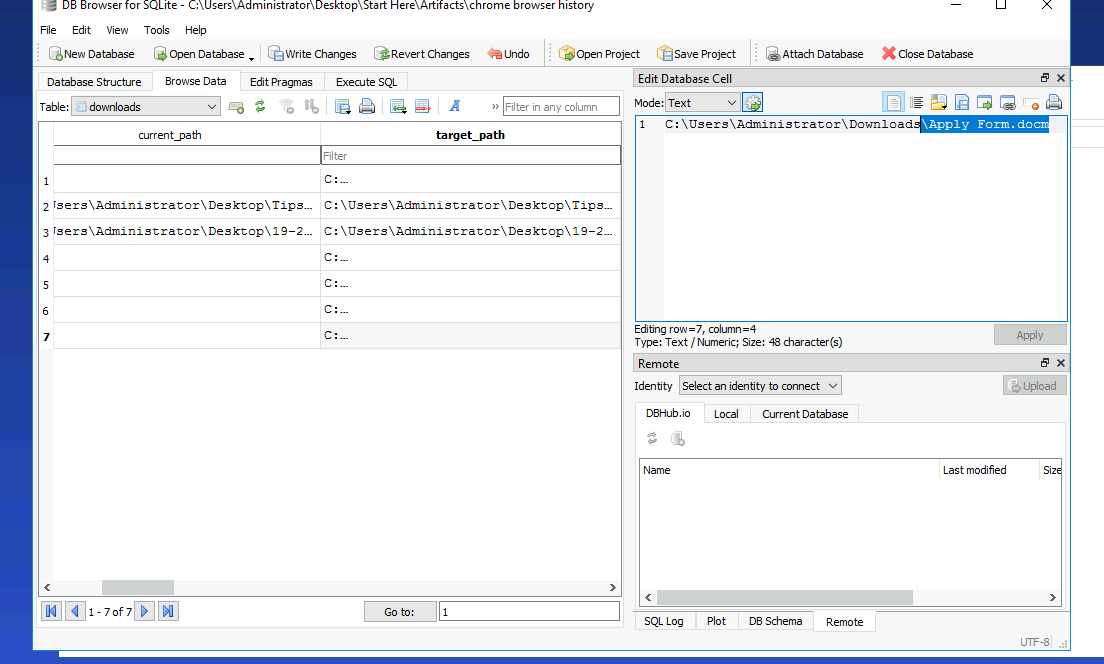
Loading the disk image into ftk imager I found this



A screenshot of a computer

AI-generated content may be incorrect.

Where are most likely looking for phishing attack



Just like the description

Using

```SELECT

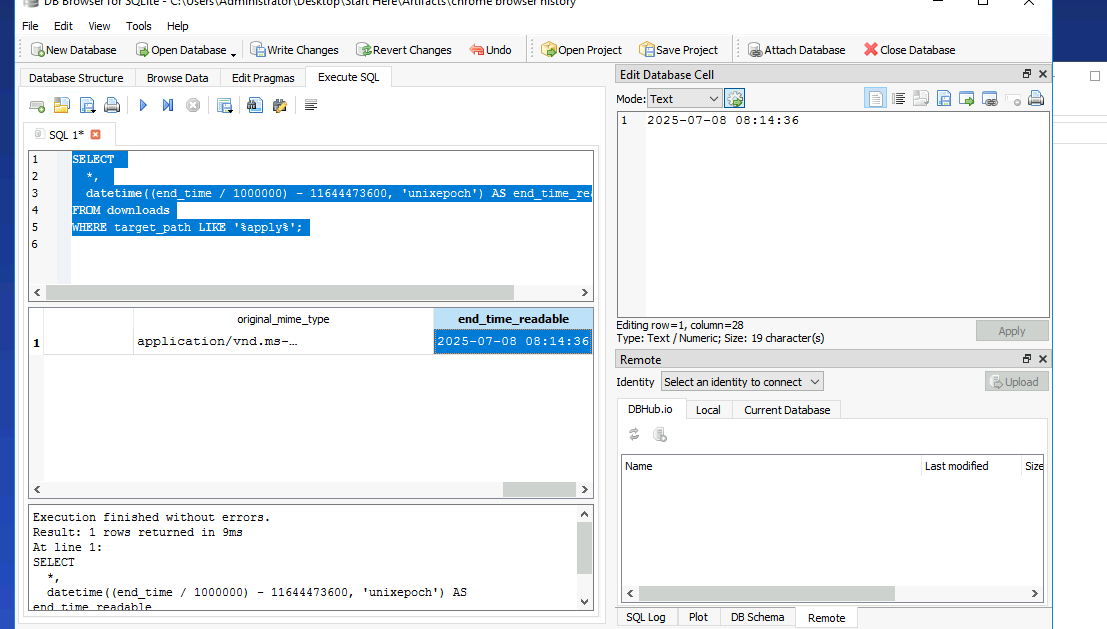
\*,

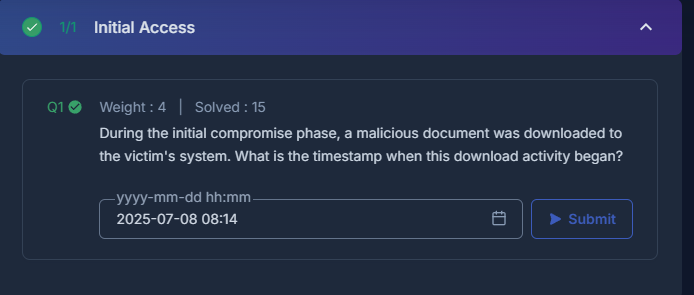
datetime((end\_time / 1000000) - 11644473600, 'unixepoch') AS end\_time\_readable

FROM downloads

WHERE target\_path LIKE '%apply%';

```





Execution

Q1

After the malicious document was executed, embedded code created additional files on the system. What is the full directory path where these secondary payloads were stored?

Running olevba I found this

A computer screen with white text

AI-generated content may be incorrect.

A screenshot of a computer error

AI-generated content may be incorrect.

Q2

What is the creation timestamp for the scripts generated by the malicious document? (in UTC)

Navigating to

C:\Users\Administrator\AppData\Local\Microsoft\Windows\Update

I found this

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Command and control

Q1

The malware established communication with external infrastructure for command and control purposes. What is the IP address of this C2 server?

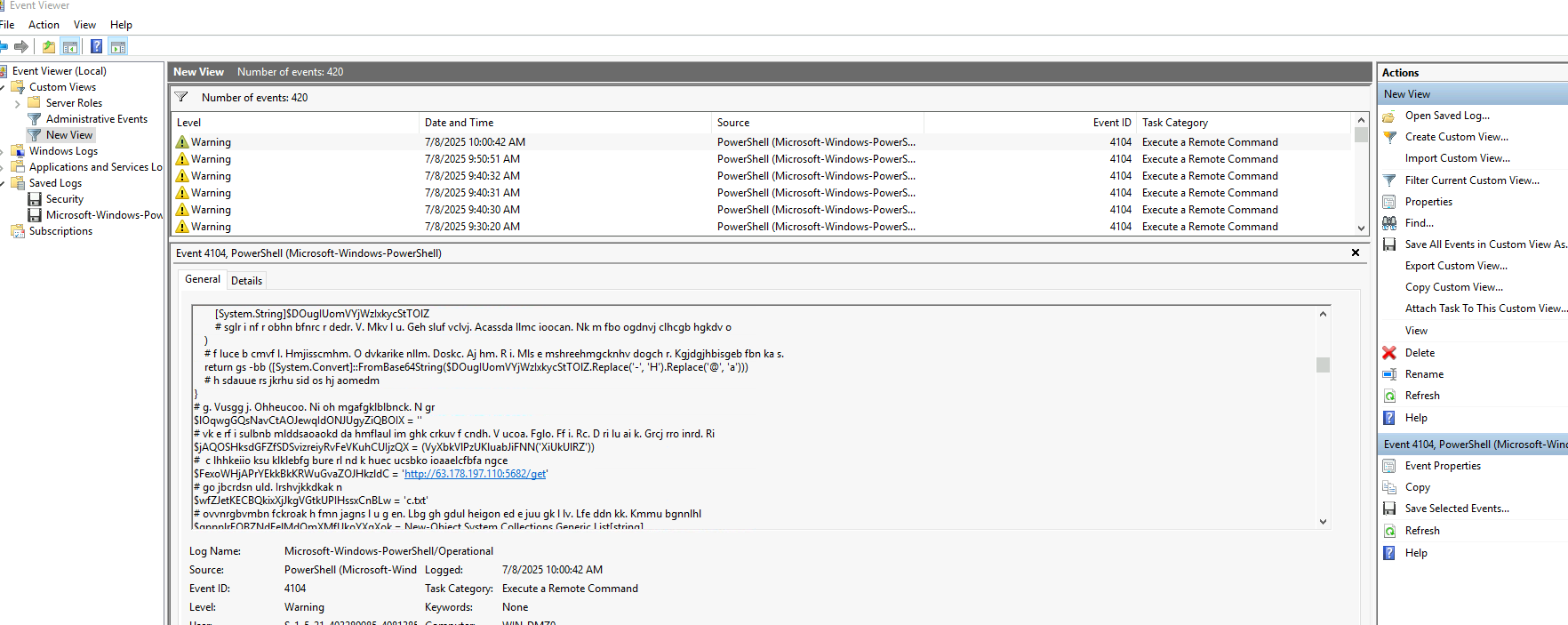
I looked for script.ps1 but I didn’t find it in its path so I exported security.evtx

And looked for event id 4688 (process creation)

Found nothing useful

So instead I exported Microsoft-Windows-PowerShell%4Operational.evtx

And looked for event id 4104 and found this



A screenshot of a computer

AI-generated content may be incorrect.

Persistence

Q1

To maintain access across system reboots, the malware registered a scheduled task. What is the complete command line that this scheduled task executes?

Based on our previous analysis

wscript "C:\Users\Administrator\AppData\Local\Microsoft\Windows\Update\Updater.vbs"

A screenshot of a computer

AI-generated content may be incorrect.

Q2

After the scheduled task executed, another malicious script was initiated. What command was used to launch this subsequent script?

Also based on our previous analysis

powershell.exe -Exec Bypass C:\Users\Administrator\AppData\Local\Microsoft\Windows\Update\Script.ps1

A screen shot of a computer program

AI-generated content may be incorrect.

Q3

The threat actor established a second persistence mechanism through an additional scheduled task. What is the name of this secondary scheduled task?

Navigating to C:\Windows\System32\Tasks\

A screenshot of a computer

AI-generated content may be incorrect.

Without further investigation the MicrosoftEdgeUpdateTaskMachineUC is not legitimate task name and it was created during malware execution time

(note:the legit task name is MicrosoftEdgeUpdateTaskMachineUA)

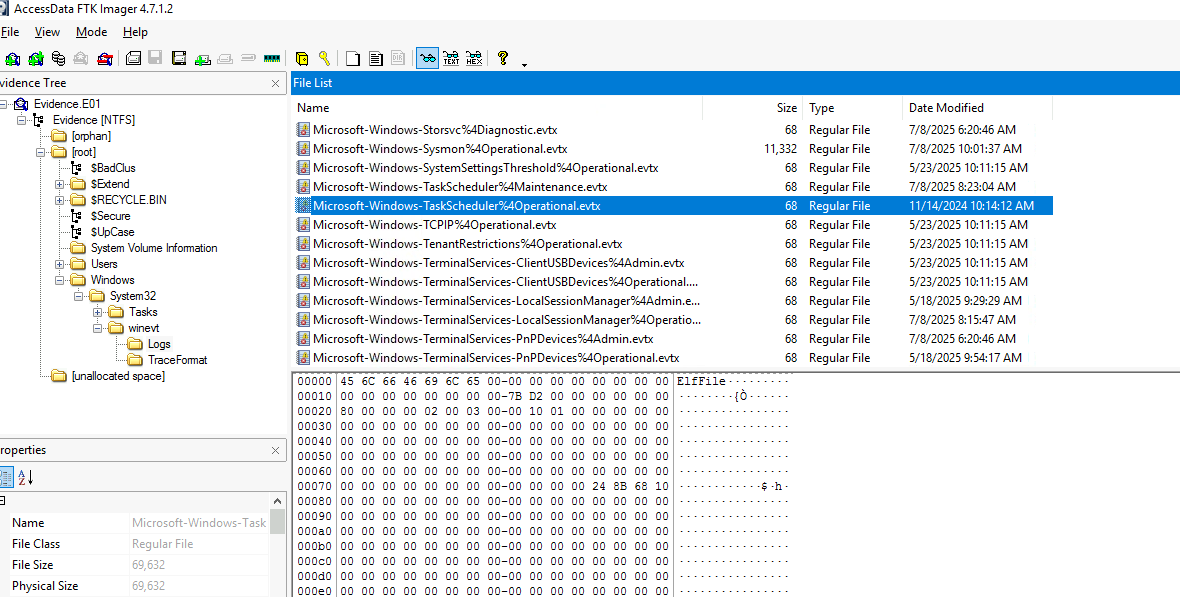
A screenshot of a computer

AI-generated content may be incorrect.

Q4

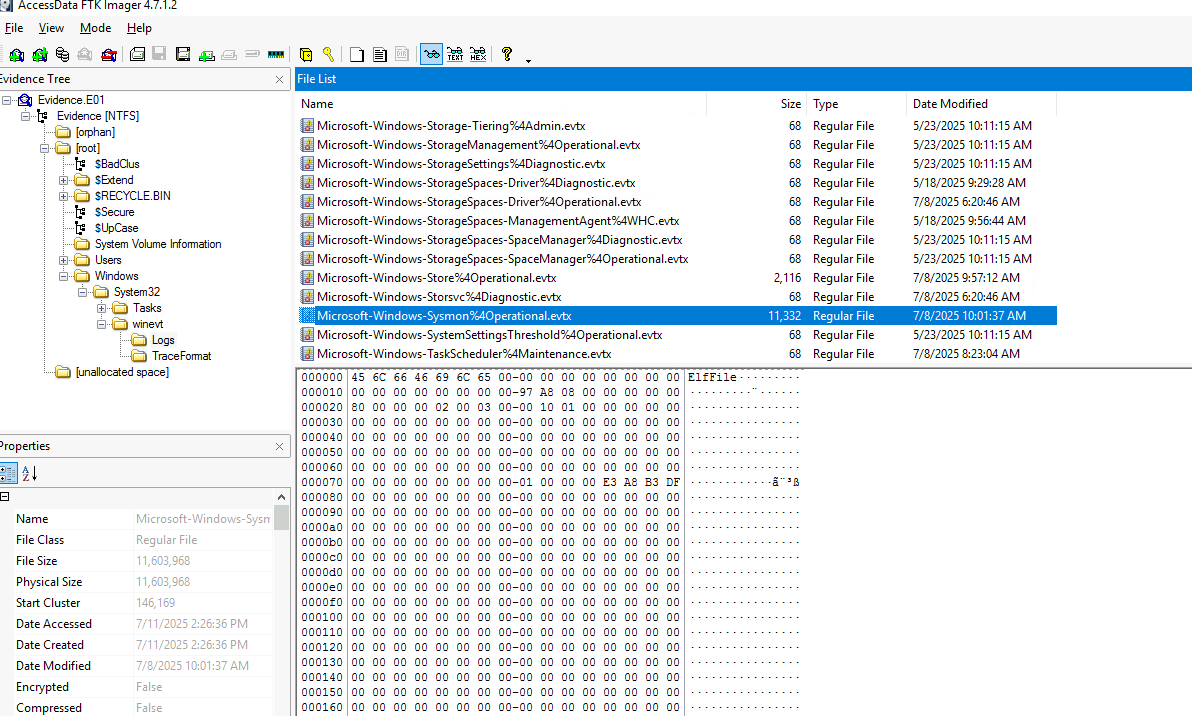
The threat actor remotely triggered manual execution of their secondary scheduled task via C2 communications. What is the timestamp when this remote execution command was processed? (in UTC)

Extracting this file

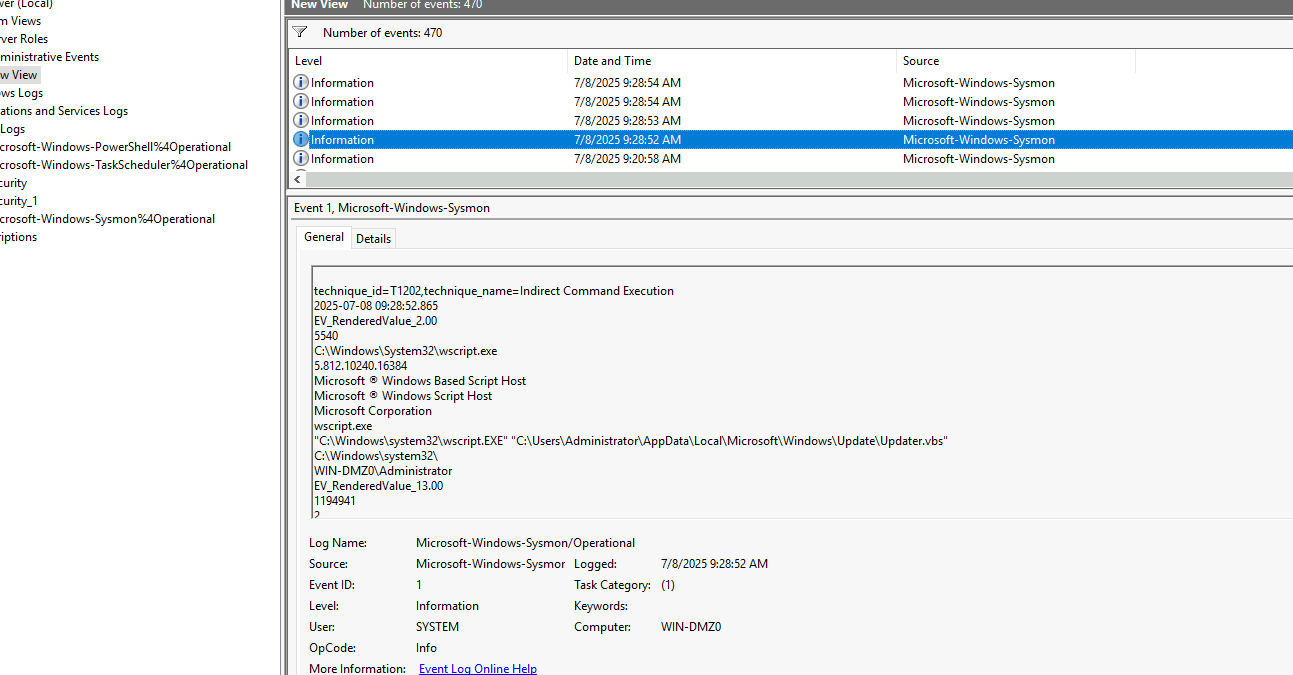


Found no evidence

Then I tried this one



After exporting I filtered by event id 1 (Process Creation)

 A screenshot of a computer

AI-generated content may be incorrect.

Top of Form

Discovery

Q1:

During the reconnaissance phase, the attacker executed a command to gather detailed information about the current user context and privileges. What specific command was used?

Ngl b4 I started searching I tried whomai /all which is the most common one and it was correct

A screen shot of a computer error

AI-generated content may be incorrect.

Q2

The threat actor performed network reconnaissance to map the infrastructure topology. Which Windows built-in utility was leveraged for this network discovery activity?

Looking a little about this online I found this command that is used for network reconnaissance

A screenshot of a computer error

AI-generated content may be incorrect.