Sherlock - Unit42

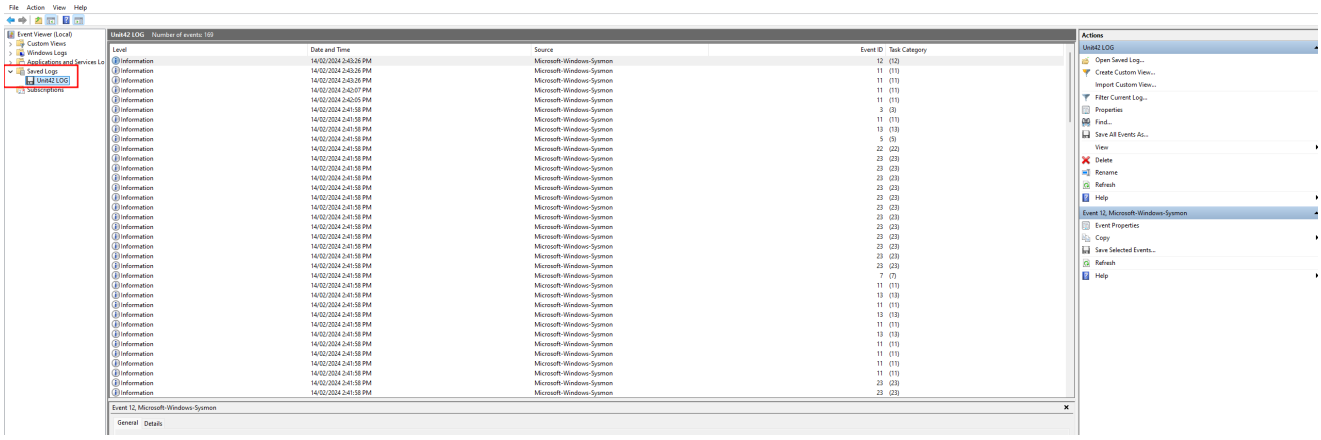
Sherlock Scenario:

In this Sherlock, you will familiarize yourself with Sysmon logs and various useful EventIDs for identifying and analyzing malicious activities on a Windows system. Palo Alto's Unit42 recently conducted research on an UltraVNC campaign, wherein attackers utilized a backdoored version of UltraVNC to maintain access to systems. This lab is inspired by that campaign and guides participants through the initial access stage of the campaign.

FILES INCLUDED

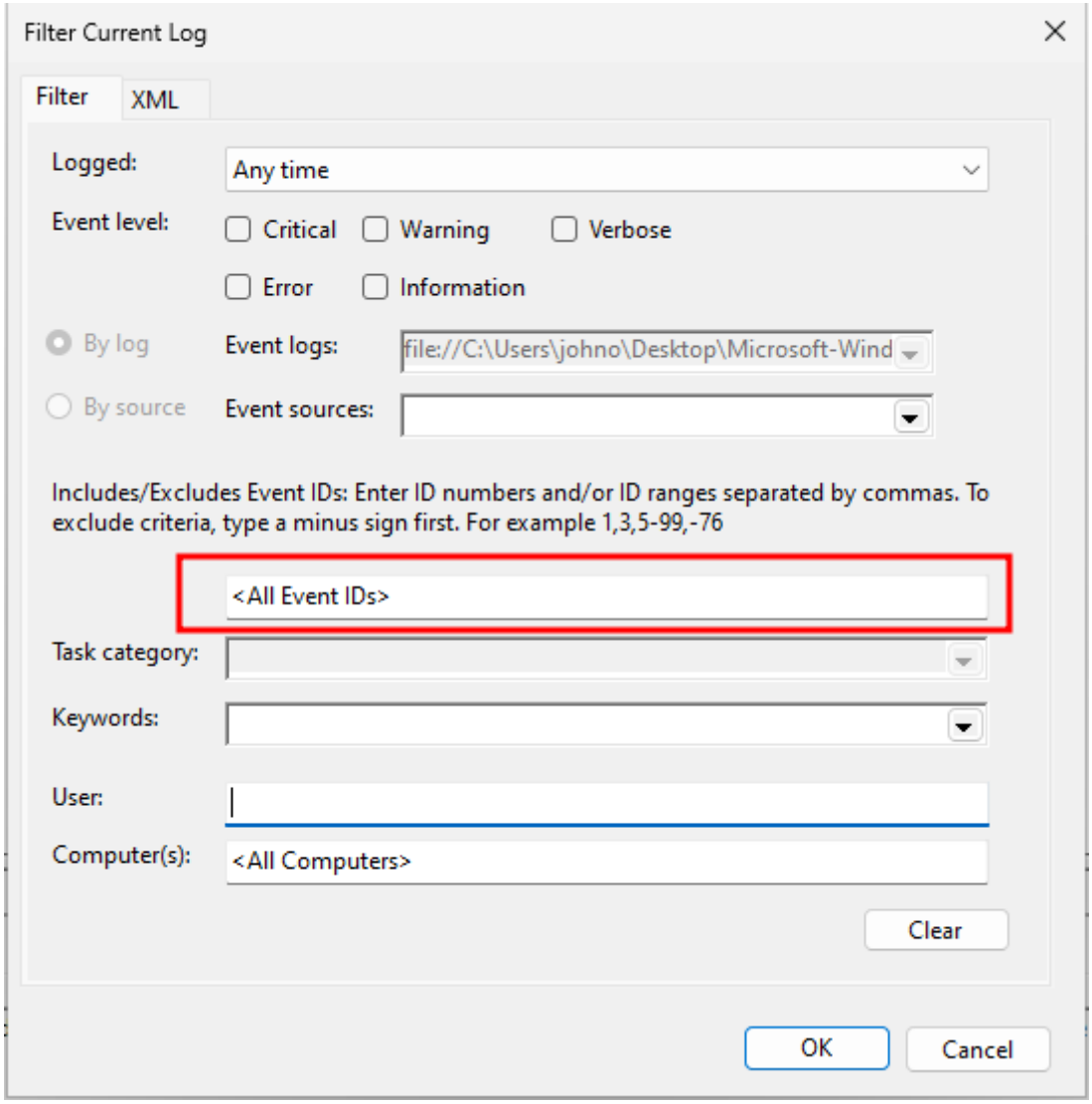
The file displayed in the screenshot is an `.evtx` file, which is a Microsoft Windows Event Log file, specifically the "Microsoft-Windows-Sysmon-Operational.evtx." Sysmon (System Monitor) is a Windows system service and device driver that logs system activity to the Windows event log.

Since this is a Sysmon file I'm going to use my Windows VM to view the file in Event Viewer

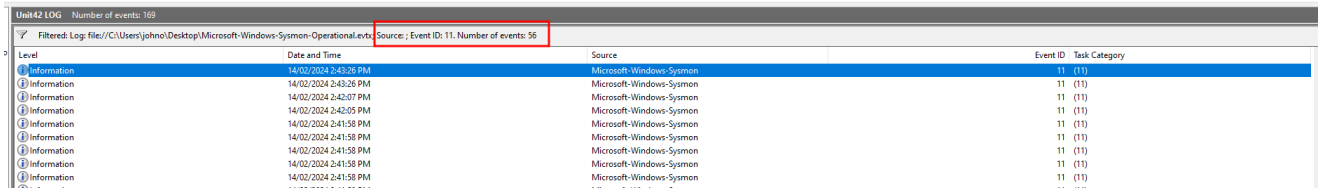


Q1 How many Event logs are there with Event ID 11?

Using the "Filter Current Log" Action I can look through all the logs with the Event ID **11**



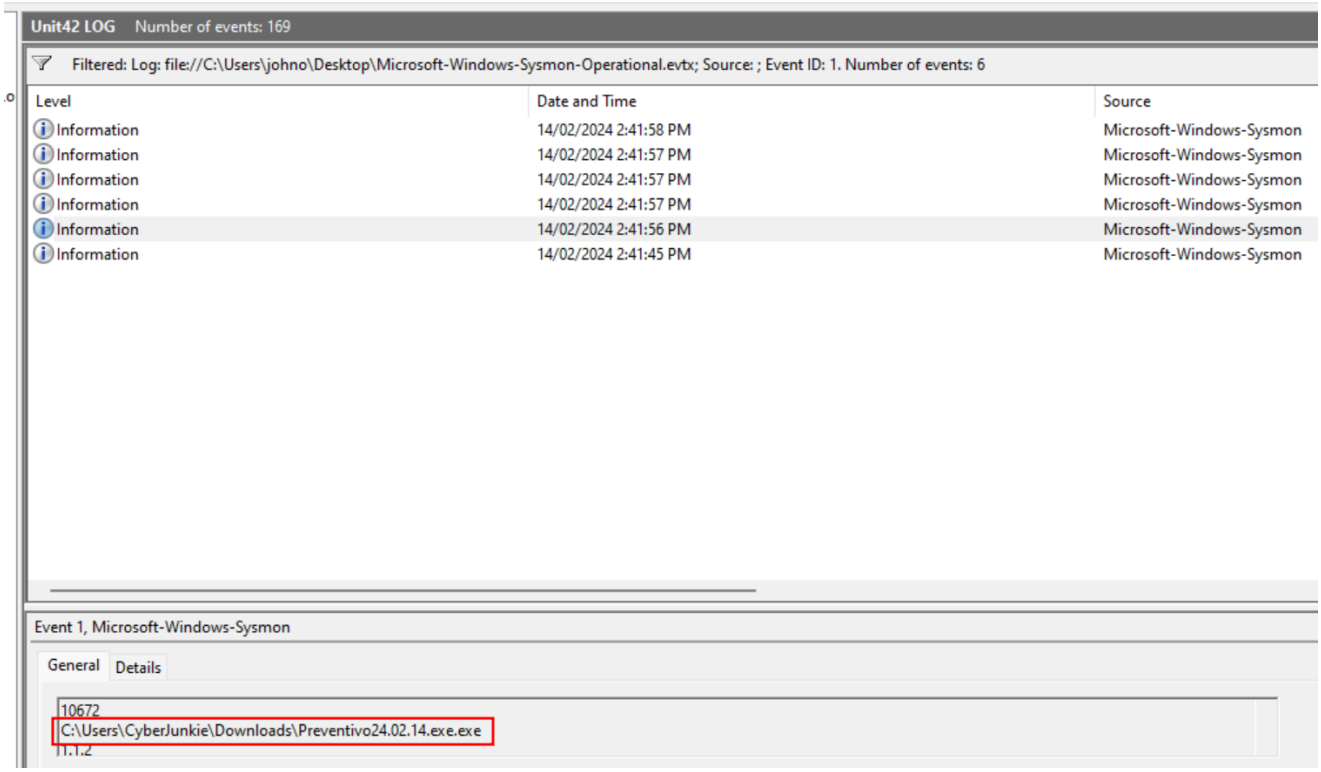
After setting the filter I can see that there are **56** Logs with the Event ID 11



Q2 Whenever a process is created in memory, an event with Event ID 1 is recorded with details such as command line, hashes, process path, parent process path, etc. This information is very useful for an analyst because it allows us to see all programs executed on a system, which means we can spot any malicious processes

being executed. What is the malicious process that infected the victim's system?

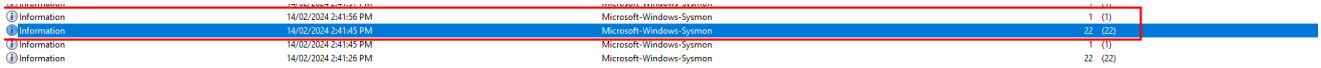
Going through all the logs with the Event ID 1 I can see that the malicious process that was executed is: C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe



Q3 Which Cloud drive was used to distribute the malware?

Using Event ID 22 we can see if there were any DNS queries being made around the same time that the process was executed.

I can see that 10 seconds before the process was executed there was a DNS query to **dropbox** as seen in the screenshot below which was most likely the cloud platform used to distribute the malware.



Q4 The initial malicious file time-stamped (a defense evasion technique, where the file creation date is changed to make it appear old) many files it created on disk. What was the timestamp changed to for a PDF file?

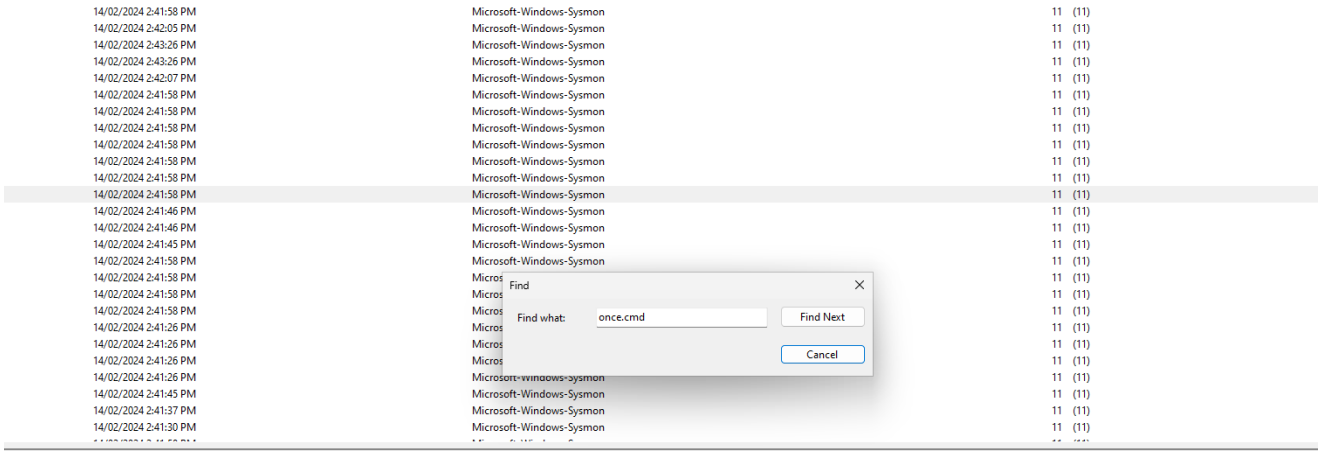
We can check this using Event ID 2 as this Event ID records any file creation time changes on any files on the system.

Looking at the pdf file log I can see the time changed to is **2024-01-14 08:10:06.029

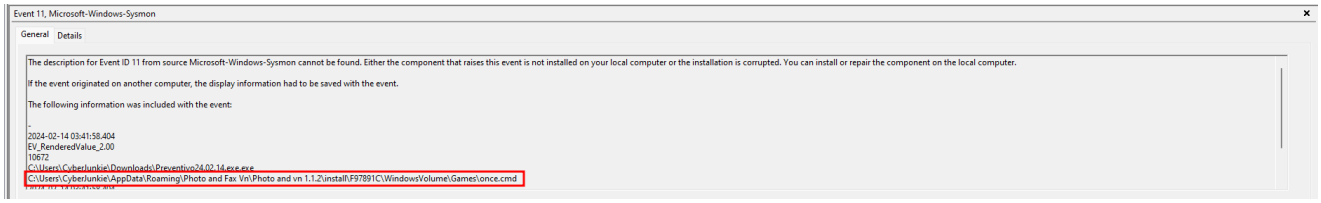
Q5 The malicious file dropped a few files on disk. Where was "once.cmd" created on disk? Please answer with the full path along with the filename.

Event ID 11 looks for files that are created so using this and I finding the "once.cmd" log I can find the answer to this question.

Using the find option to find it easier

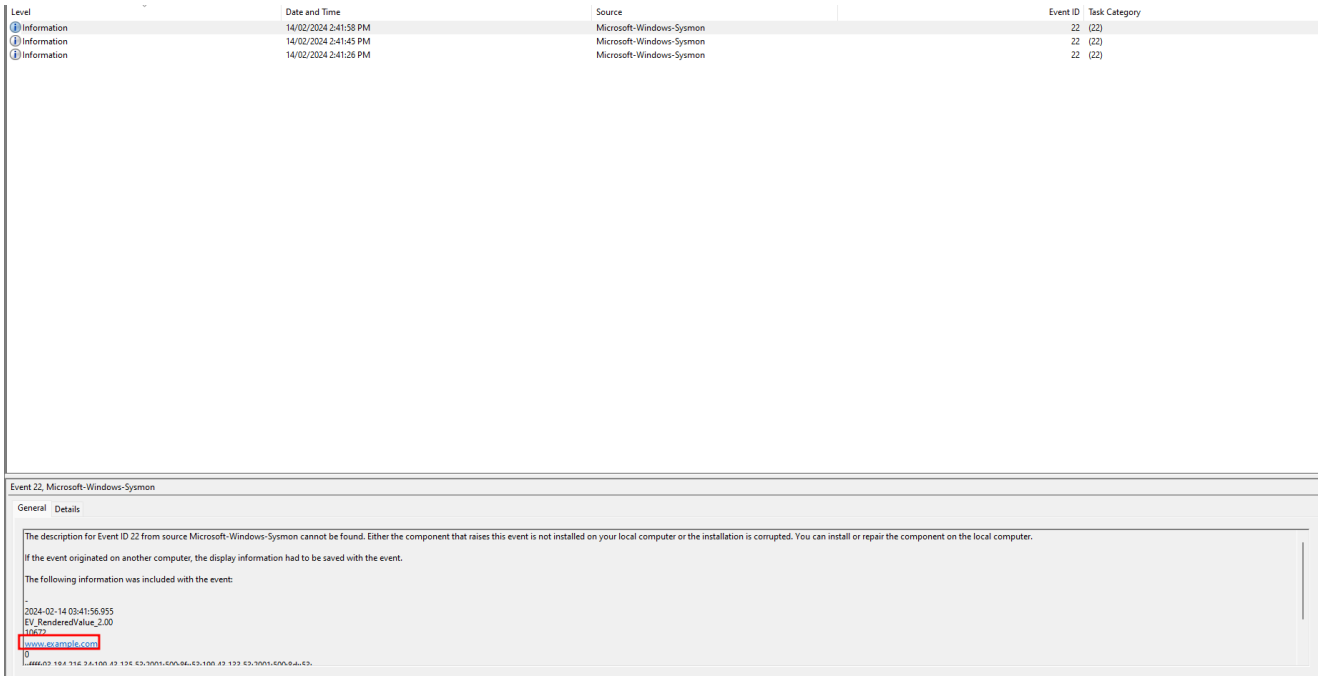


And I see the path: **C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\once.cmd**



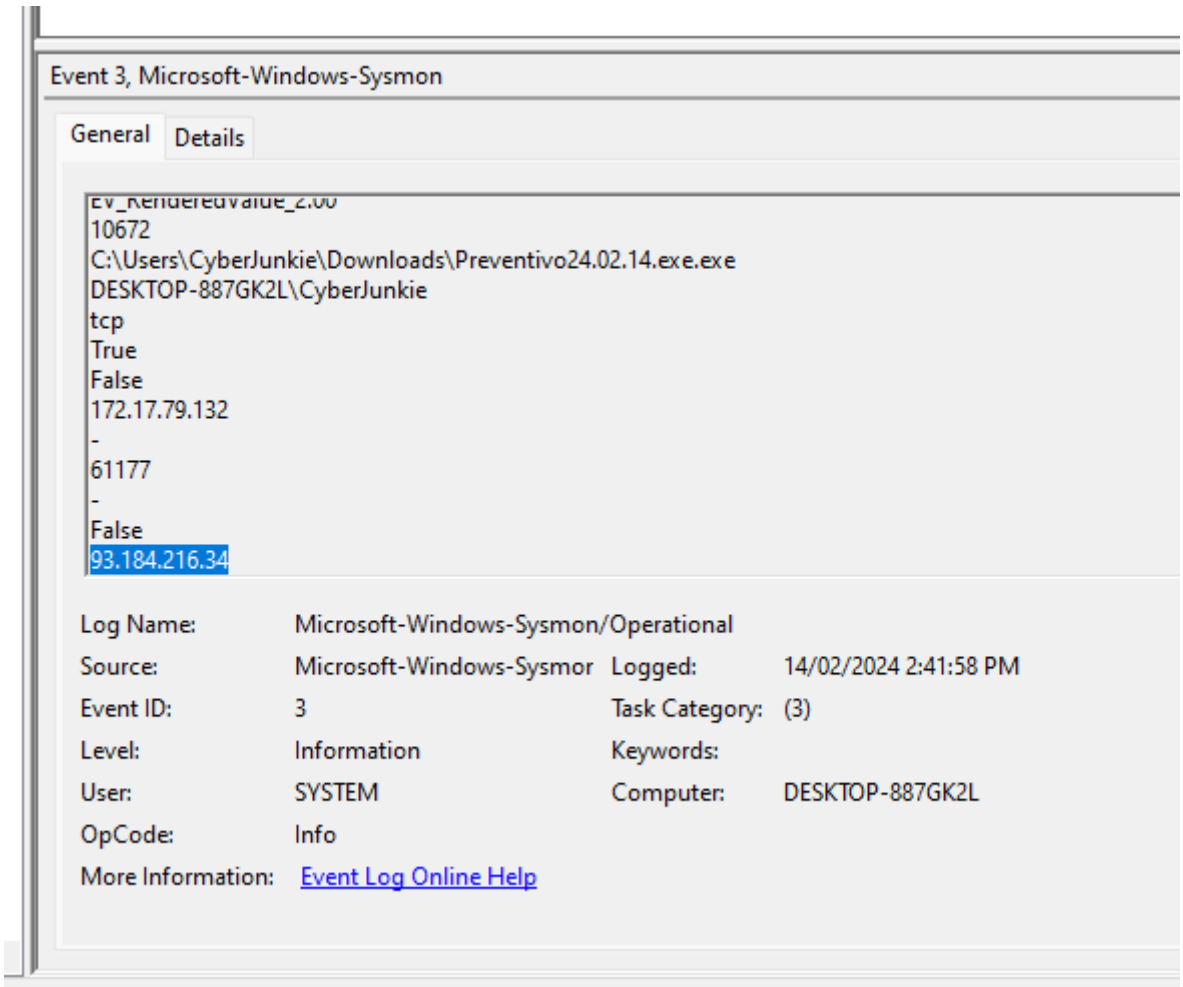
Q6 The malicious file attempted to reach a dummy domain, most likely to check the internet connection status. What domain name did it try to connect to?

Using Event ID 22 again to see what DNS queries were requested I can see that the dummy domain the file tried to reach was www.example.com



Q7 Which IP address did the malicious process try to reach out to?

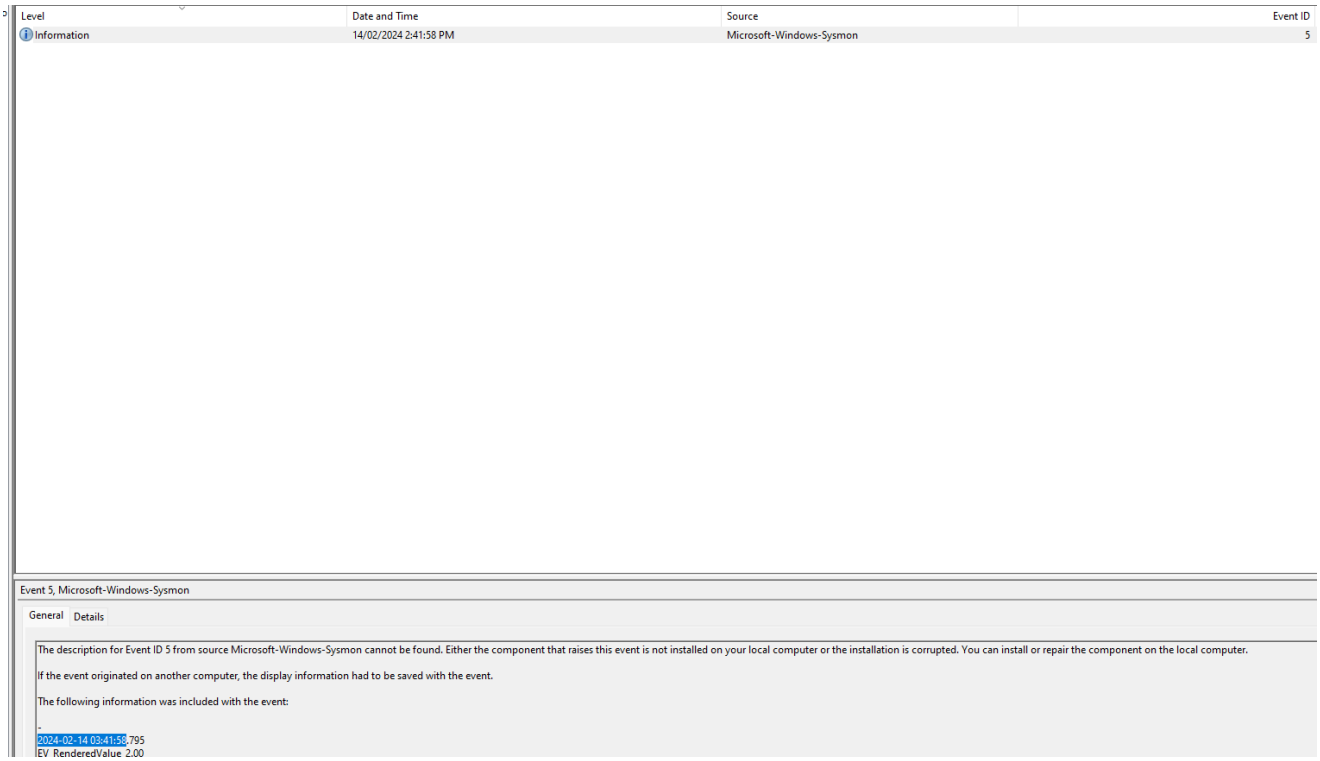
I can find the answer to this using Event ID 3. It records the IP address, port, and the process trying to make the connection.



The malicious process terminated itself after infecting the PC with a backdoored variant of UltraVNC. When did the process terminate itself?

We can use Event ID 5 to find logs of terminations of processes.

Filtering by ID 5 I can see that it was terminated at **2024-02-14 03:41:58**



SHERLOCK COMPLETE

TAKEAWAYS:

- **Sysmon Event IDs**: The writeup underscores the importance of Sysmon Event IDs in detecting malicious activities, focusing on IDs like 1, 2, 3, 5, 11, and 22.
- **Malware Indicators**: It identifies Dropbox as the malware distribution platform via DNS queries and highlights the use of file time-stamping for evasion.
- **Process Investigation**: The analysis tracks a malicious process, `Preventivo24.02.14.exe.exe`, showing how to trace its actions, including file drops and external connections.