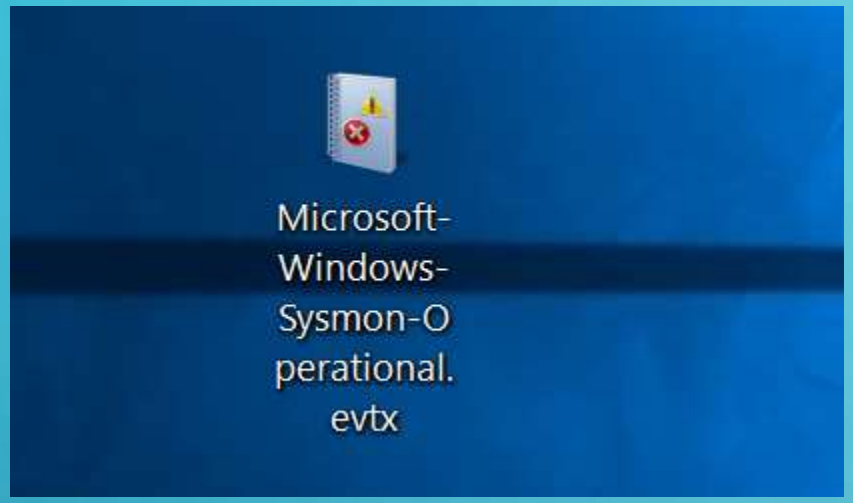
HTB SHERLOCKS – UNIT42

WRITE UP BY CHANAN SHENKER

- Start:

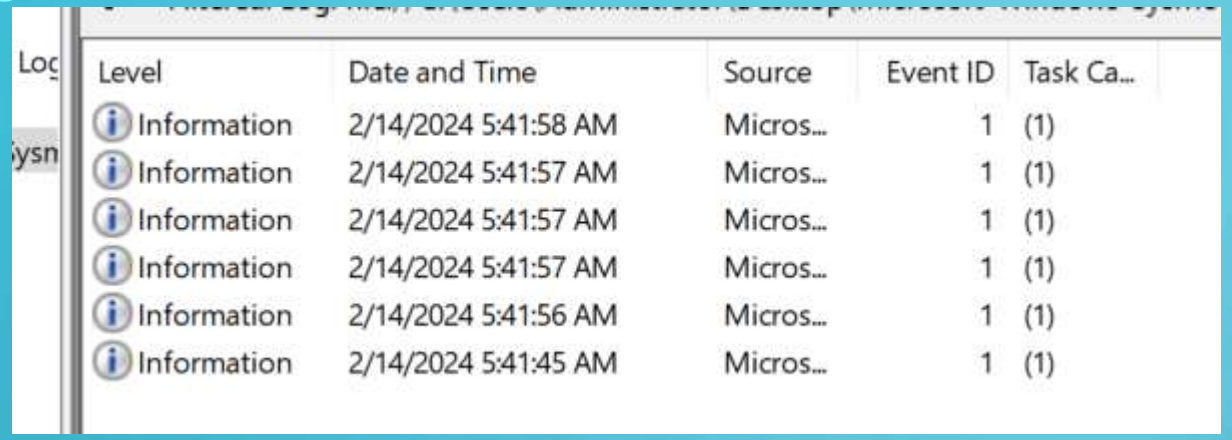


- We start with a Sysmon event log file.
- Sysmon is an application that creates event logs with its own special event ids. These event ids are mainly to detect suspicious activity on the host. And the events are tailored to specific attack.
- With that said lets start.

- Question 1: How many Event logs are there with Event ID 11?

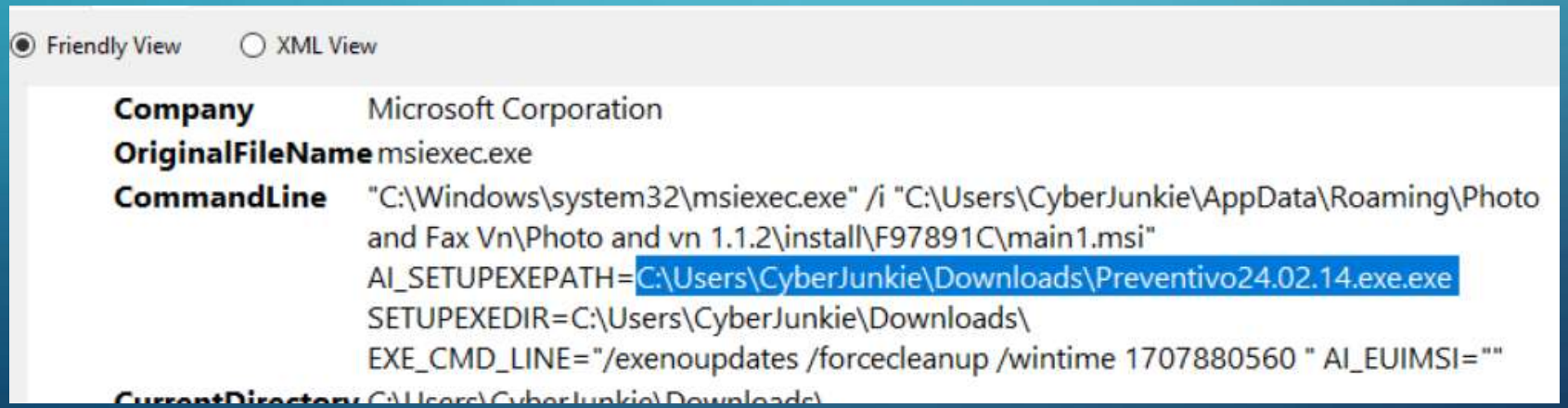
```
PS C:\Users\Administrator\Desktop> (Get-WinEvent -Path .\Microsoft-Windows-Sysmon-Operational.evtx | Where-Object {$_.id
 -eq '11'}).count
56
PS C:\Users\Administrator\Desktop>
```

- Not much to explain here…
- Answer 1: 56.
- Question 2: 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…. What is the malicious process that infected the victim's system?
- So lets look for Sysmon event id 1.



Level	Date and Time	Source	Event ID	Task Ca...
Information	2/14/2024 5:41:58 AM	Micros...	1	(1)
Information	2/14/2024 5:41:57 AM	Micros...	1	(1)
Information	2/14/2024 5:41:57 AM	Micros...	1	(1)
Information	2/14/2024 5:41:57 AM	Micros...	1	(1)
Information	2/14/2024 5:41:56 AM	Micros...	1	(1)
Information	2/14/2024 5:41:45 AM	Micros...	1	(1)

- Sysmon event id 1 is a event triggered by a process being created. And here we can see if a malicious executable was executed.



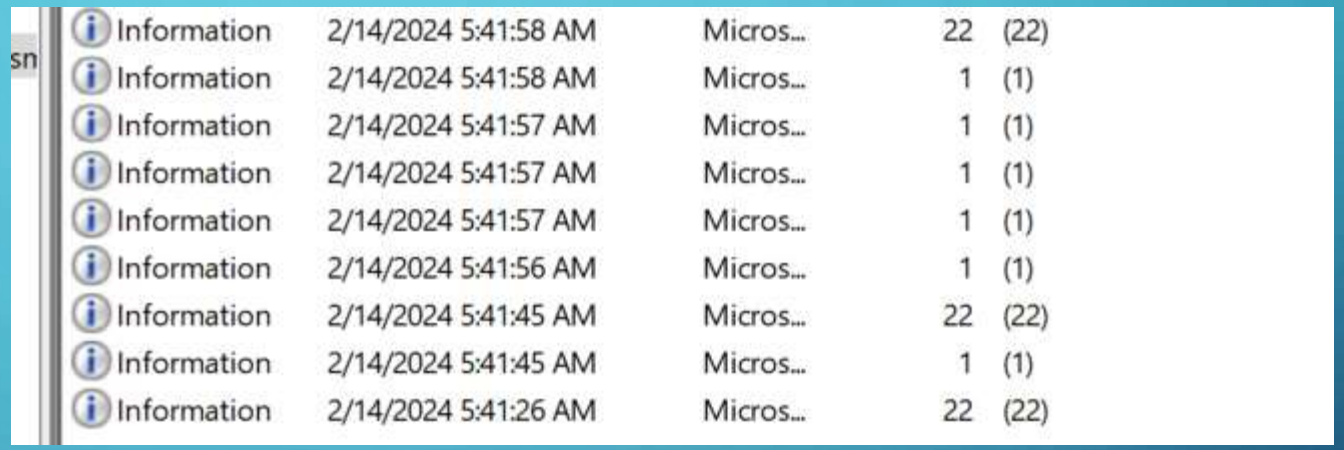
Friendly View XML View

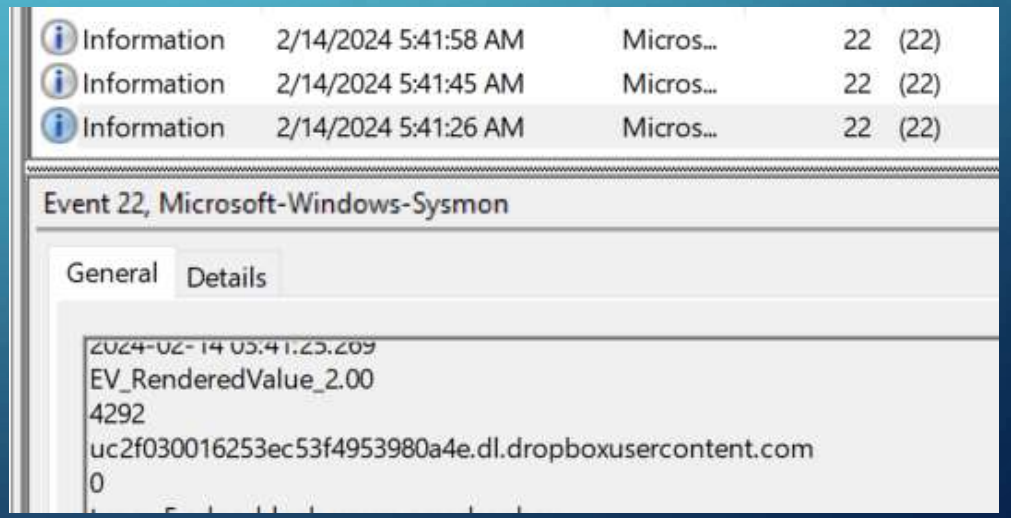
Company Microsoft Corporation
OriginalFileName msiexec.exe
CommandLine "C:\Windows\system32\msiexec.exe" /i "C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\main1.msi" AI_SETUPEXEPATH=C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe SETUPEXEDIR=C:\Users\CyberJunkie\Downloads\ EXE_CMD_LINE="/exenoupdates /forcecleanup /wintime 1707880560 " AI_EUIMSI=""
CurrentDirectory C:\Users\CyberJunkie\Downloads\

- And here I found an interesting file name. “preventive.24.02.14.exe.exe”.
- Firstly ‘exe.exe’ is already pretty suspicious, but a quick search led me to find a webpage talking about this exact malware.

- Obviously its no the same exact file version but From what I could understand it checks a bunch of network setting on the target machine.
- Answer 2: C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe

- Question 3: Which Cloud drive was used to distribute the malware?
- The hint that came with this event advised to look for events with the id 22, which are related to any DNS queries that were made, that appeared near the event log of the malicious file being executed.
- Looking at these event we can see that the 2 event with the id 2 that were after the file was executed have link to dropbox.
- Answer 3: dropbox





- Question 4: 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?

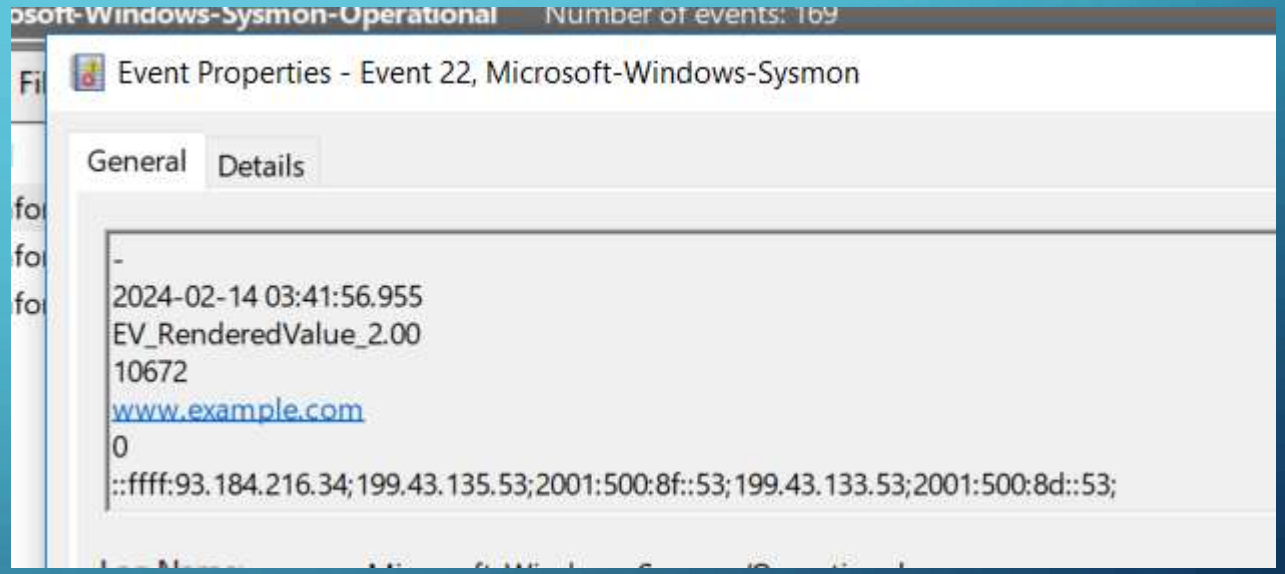
- For this one I remembered that Sysmon event id 2 is triggered by changing the metadata of when the file was created, thus making the file look older that it was to maybe blend in better on the target machine

- So I filtered for event id 2 and search for any events with the word 'pdf' I only found this one
- Answer 4:
- 2024-01-14 08:10:06

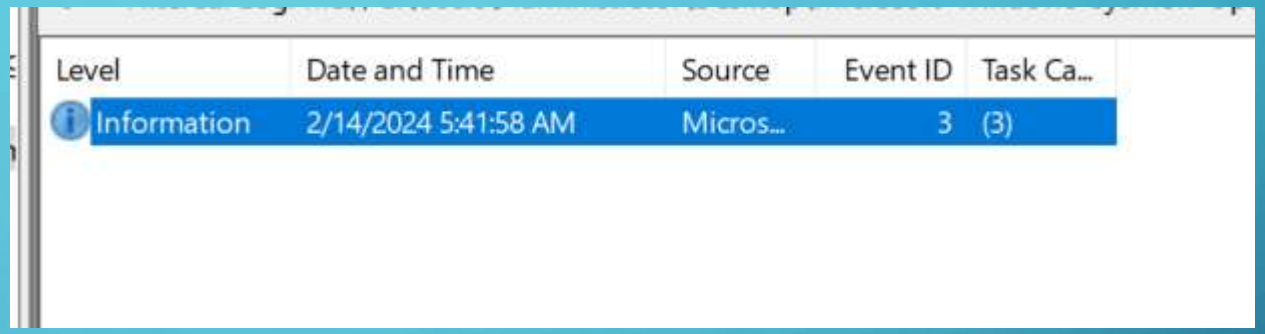
- Question 5: The malicious file dropped a few files on disk. Where was "once.cmd" created on disk? Please answer with the full path along with the filename.
- For this there's Sysmon event id 11, which is triggered by a file being created.
- So same with the previous one I filtered for event id 11 and searched for events with the text “once.cmd” and found only one again.

- Answer 5 : C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\once.cmd

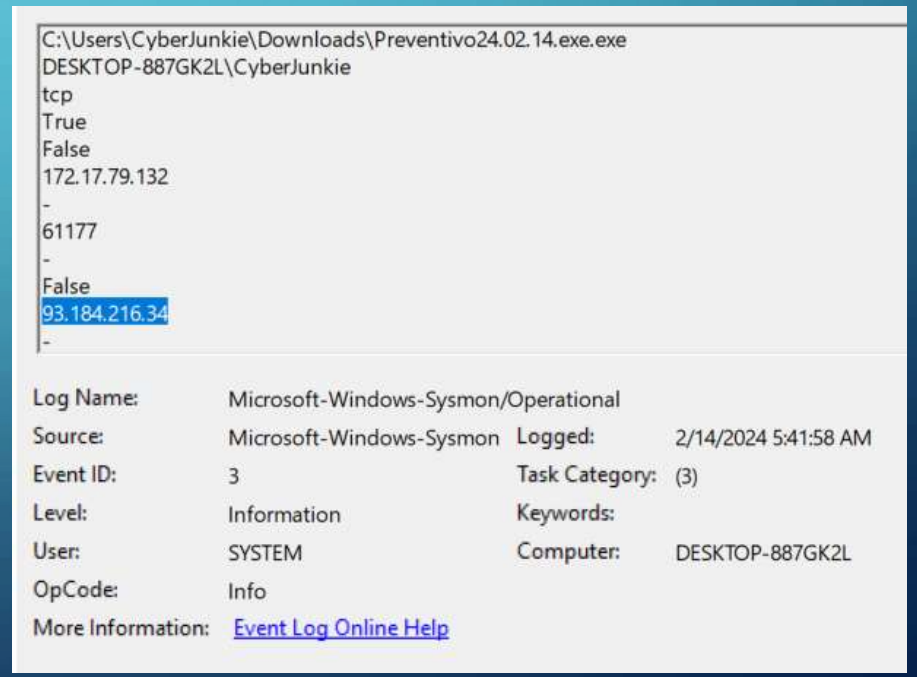
- Question 6: The malicious file attempted to reach a dummy domain, most likely to check the internet connection status. What domain name did it try to connect to?
- For this we go back to event id 22 since its an attempt to look for a domain.
  - When searching for the mentioned event I only found 3 events. So I took a quick look and saw this domain 'www.example.com' which is obviously a fake website.
  - Answer 6: www.example.com



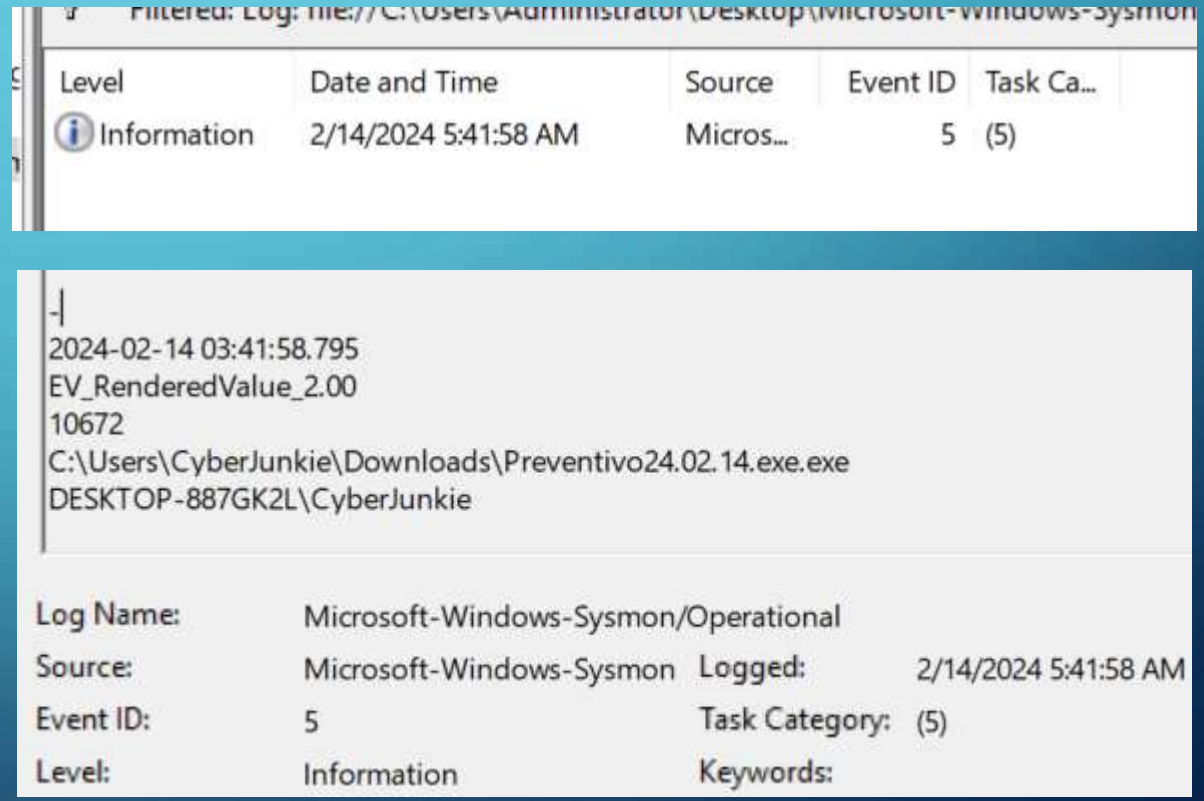
- Question 7: Which IP address did the malicious process try to reach out to?
- For this part we take a look at event id 3, which is triggered by a network connection being made.



  - Again only one appears, so I opened it to check and look and saw 2 sets of ips. One internal and the other external.
  - So the one trying to be contacted has ti be the external.
  - Answer 7: 93.184.216.34



- Question 8: The malicious process terminated itself after infecting the PC with a backdoored variant of UltraVNC. When did the process terminate itself?
- Like the previous questions to find the answer we can look for a relevant event log id. In this case it Sysmon event id 5, which indicates a process being terminated.
- And yet again all I could fine was one event log. Opening the event we can see that it was the original malicious file that was terminated.
- Answer 8: 2024-02-14 03:41:58




UNIT42
VNC
Unit42 has been Solved!
Congratulations chananshenker, best of luck in capturing flags ahead!