Unit42 Writeup

Prepared by: Cyberjunkie & Sebh24

Machine Author(s): Cyberjunkie

Difficulty: Very Easy

Scenario

```
In this Lab, you will be made familiar with Sysmon logs, various useful EventID
to identify and analyze malicious activities on a windows system. Palo Alto
Unit42 recently conducted research on an UltraVNC campaign in which attackers
used backdoor version of ultravnc to maintain access to systems. This lab is
based on that campaign and take players through the initial access stage of this
campaign.

Only event viewer is required to answer the questions, and virustotal to
complement it (Optional). Here are some important Event IDs in sysmon which can
be used  in analysis

Event ID 1 : Process creation/execution. Includes process path,parent process
path,commandline arguments

Event ID 2 : File creation time changed. Includes the file making the change,
file to which change is being made,tampered timestamp and original timestamp
```

```
Event ID 3 : Network Connection . INcludes the process making the connection,
destination IP Address and port

Event ID 5 : Process Termination. Includes the process name which
killed/terminated itself

Event ID 11 : File created. Includes the process creating the file, the file
being created and full path

Event ID 22 : DNS Query . Includes the process querying the domain, the target
domain name and the IP Address they resolve to
```

Artefacts provided

1-UltraVNC_UNIT42.zip (zip file), sha1 : 1D8AC45395551187EAF23793CE525056C4136D6E

Skills Learnt

- Event Log Analysis
- Sysmon Log analysis
- UltraVNC infection campaign
- Timeline creation
- Contextual Analysis

Tags

- DFIR

Pre Reading

Prior to kicking into our analysis we need to ensure a basic understanding of Windows Event Logs & Sysmon, inclusive of what they are, their use cases and why they are important for security professionals and IT Admins alike.

Windows Event Logs

Windows Event Logs are a fundamental component of the Windows operating system that record a wide range of information about the computer's activities and operations. These logs are instrumental for system diagnostics, performance monitoring, and security auditing. They provide a detailed record of every event that occurs on the system, from system startups and shutdowns to software installations and security breaches.

Types of Windows Event Logs

Windows Event Logs are categorized into several types, each serving a specific purpose:

- **Application Logs**: Record events related to Windows applications. These include errors, warnings, and informational messages from software programs.
- **Security Logs**: Contain records of security-related events specified by the system's audit policy. Examples include successful and failed login attempts, changes to user privileges, and other security-related changes.

- **System Logs**: Document system events, such as driver failures, hardware issues, and other system-level notifications.
- **Setup Logs**: Log events related to the installation of Windows and other software components.
- **Forwarded Events**: Used to store events collected from remote computers.

Administrators and security teams use these logs to troubleshoot problems, monitor system performance, and ensure that the system is secure against unauthorized access and other security threats.

Viewing Windows Event Logs

Windows Event Logs can be viewed using the Event Viewer, a graphical tool available in Windows that allows users to see and analyze log entries. The Event Viewer categorises logs into different sections, making it easier to navigate through the logs and find specific events.

How else can we view them?

Alternatively we can convert the Event Logs into json or CSV using a tool named EvtxEcmd. This will not be completed during this Sherlock, however if you are intending to go "beyond" the investigation an explanation of EvtxEcmd has been provided.

We start by opening the event log file in EventViewer. We can see the total Count of events.

Sysmon (System Monitor)

Sysmon is a Windows system service and device driver that, once installed on a system, remains across system reboots to monitor and log system activity to the Windows Event Log. It is part of the Sysinternals suite of tools from Microsoft and provides detailed information about process creations, network connections, and changes to file creation time.

Sysmon is designed to assist in detection and analysis of advanced threats and malware. It extends the capabilities of Windows Event Logs by providing more detailed and specific information about system behavior and activity.

Uses of Sysmon

- **Process Tracking**: Logs process creation with full command line for both current and parent processes, providing context on process execution.
- **Network Monitoring**: Records information about incoming and outgoing network connections, including the source, destination, and protocol used, which is crucial for identifying malicious traffic.
- **File Creation Tracking**: Monitors creation of files, allowing analysts to track the spread of malware or the extraction of data by unauthorized processes.
- **Registry Events**: Logs changes to the Windows registry, which can indicate malware installation or configuration changes made by attackers.
- **Driver and DLL Loading**: Monitors loading of drivers and DLLs, which can help identify the use of exploit kits and rootkits.

Why They Are Helpful for Security Teams and Investigations?

Windows Event Logs and Sysmon data are invaluable resources for security teams and forensic investigators. They provide a wealth of information that can be used to detect, investigate, and respond to security incidents and breaches. Here are a few reasons why they are so helpful:

- **Detection of Malicious Activity**: By analysing logs, security teams can identify suspicious activities that may indicate a breach or an ongoing attack, such as unusual login attempts, unexpected process creations, and unauthorized network connections.
- **Incident Response and Forensics**: During a security incident, detailed logs are crucial for understanding the scope of the breach, the methods used by the attackers, and the systems and data affected. This information is critical for effectively containing and remediating the incident.
- **Compliance and Auditing**: Many regulatory frameworks require organisations to maintain detailed logs of system and network activity. Windows Event Logs and Sysmon can help organizations meet these requirements by providing comprehensive records of system activity.
- **System Troubleshooting**: Beyond security, these logs are also useful for identifying and resolving system errors and failures, improving system stability and performance.

As detailed in the scenario there are a variety of Sysmon Event IDs that may be useful to us. Lets look at these in a bit more detail:

Event ID 1: Process Creation

- **Description**: This event logs the creation (or execution) of a process and provides comprehensive details about it.
- Key Fields:
  - **Process Path**: The full path of the executable file for the newly created process.
  - **Parent Process Path**: The full path of the executable file for the parent process that created this process. This is crucial for understanding the chain of execution.
  - **Command Line Arguments**: The full command line used to execute the process, including all parameters. This can reveal the intent behind the process execution, especially if the process is malicious.
- **Security Relevance**: By analysing process creation events, security professionals can identify potentially malicious processes, understand attack chains, and detect the abuse of legitimate system utilities for nefarious purposes.

Event ID 2: File Creation Time Changed

- **Description**: Logs when the creation time of a file is modified, which might indicate an attempt to obscure the time of file creation or modification.
- Key Fields:
  - **File Making the Change**: The process responsible for altering the file's creation time.
  - **File to Which Change is Being Made**: The file whose creation time is being modified.
  - **Tampered Timestamp**: The new creation time being set.
  - **Original Timestamp**: The original creation time before it was altered.

- **Security Relevance**: Modifications to file creation times can be a tactic used by attackers to evade detection or to align with legitimate system activity to remain under the radar. Monitoring such changes can help uncover stealthy maneuvers.

Event ID 3: Network Connection

- **Description**: This event records outgoing network connections initiated by processes, providing visibility into network activity.
- Key Fields:
  - **Process Making the Connection**: The process initiating the network connection.
  - **Destination IP Address and Port**: The external endpoint to which the process is connecting. This includes both the IP address and the port number.
- **Security Relevance**: Monitoring network connections helps in identifying suspicious communications with external servers, data exfiltration attempts, and command and control (C2) traffic, which are common in malware operations.

Event ID 5: Process Termination

- **Description**: Logs the termination of a process.
- Key Fields:
  - **Process Name**: The name of the process that was terminated.
- **Security Relevance**: Knowing when and which processes are terminated can help in understanding the behavior of malware (which may terminate security processes) or tracking the lifecycle of a legitimate but compromised process.

Event ID 11: File Created

- **Description**: This event is logged when a file is created, offering insights into files being generated by processes.
- Key Fields:
  - **Process Creating the File**: The process responsible for creating the new file.
  - **File Being Created and Full Path**: The name and full path of the newly created file.
- **Security Relevance**: The creation of files is a common behavior in software execution, but in a security context, monitoring file creation can help detect the dropping of malware payloads, unauthorised data collection, or temporary files created as part of an attack.

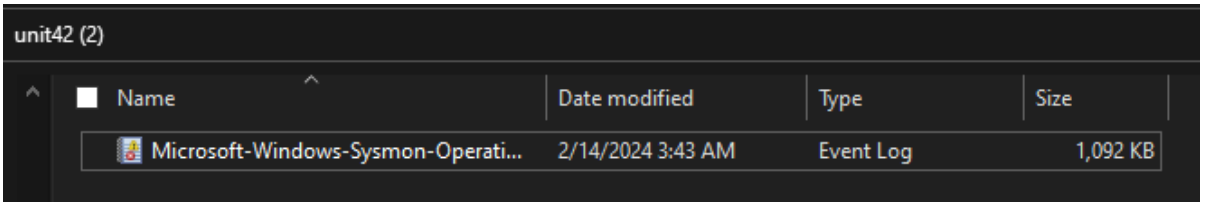
Event ID 22: DNS Query

- **Description**: Captures DNS queries made by processes, which can be essential for identifying domain names involved in malicious activities.
- Key Fields:
  - **Process Querying the Domain**: The process that initiated the DNS query.
  - **Target Domain Name**: The domain name that was queried.
  - **IP Address They Resolve To**: The IP addresses returned in response to the DNS query.

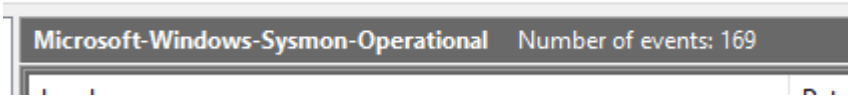
- **Security Relevance**: DNS queries can reveal a lot about network behavior, including potential contact with malicious domains, domain generation algorithms (DGA) used by malware, and data exfiltration over DNS. Monitoring DNS queries can aid in early detection of threat indicators.

Initial Analysis

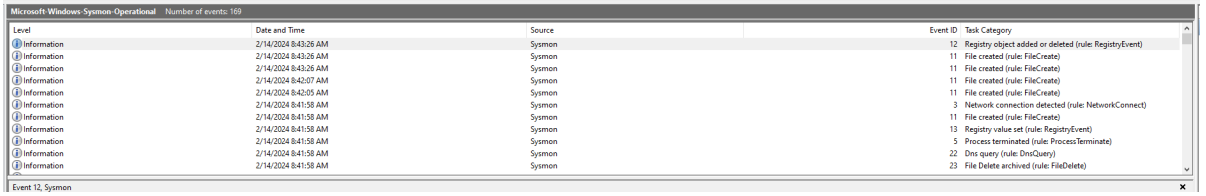
Upon downloading the artefacts we unzip them using the password `hacktheblue` utilising 7zip, and then view we are presented with an evtx file named `Microsoft-Windows-Sysmon-Operational.evtx`.



We double click the file and it automatically opens in EventViewer. We are presented with 169 Sysmon events.



We will answer the questions by filtering for relevant Event ID to quickly get the answer. Its important to note that the time showed in event log pane is your local configured time. The true Event Timestamp is stored in log details itself. We will explore this soon.

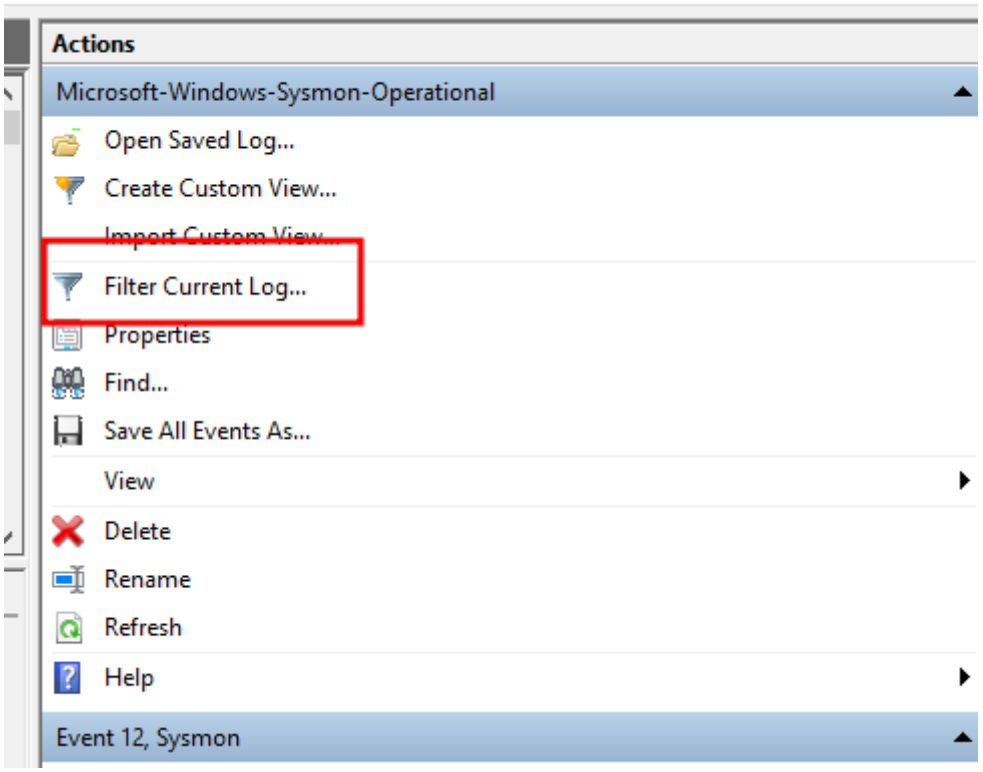


Questions :

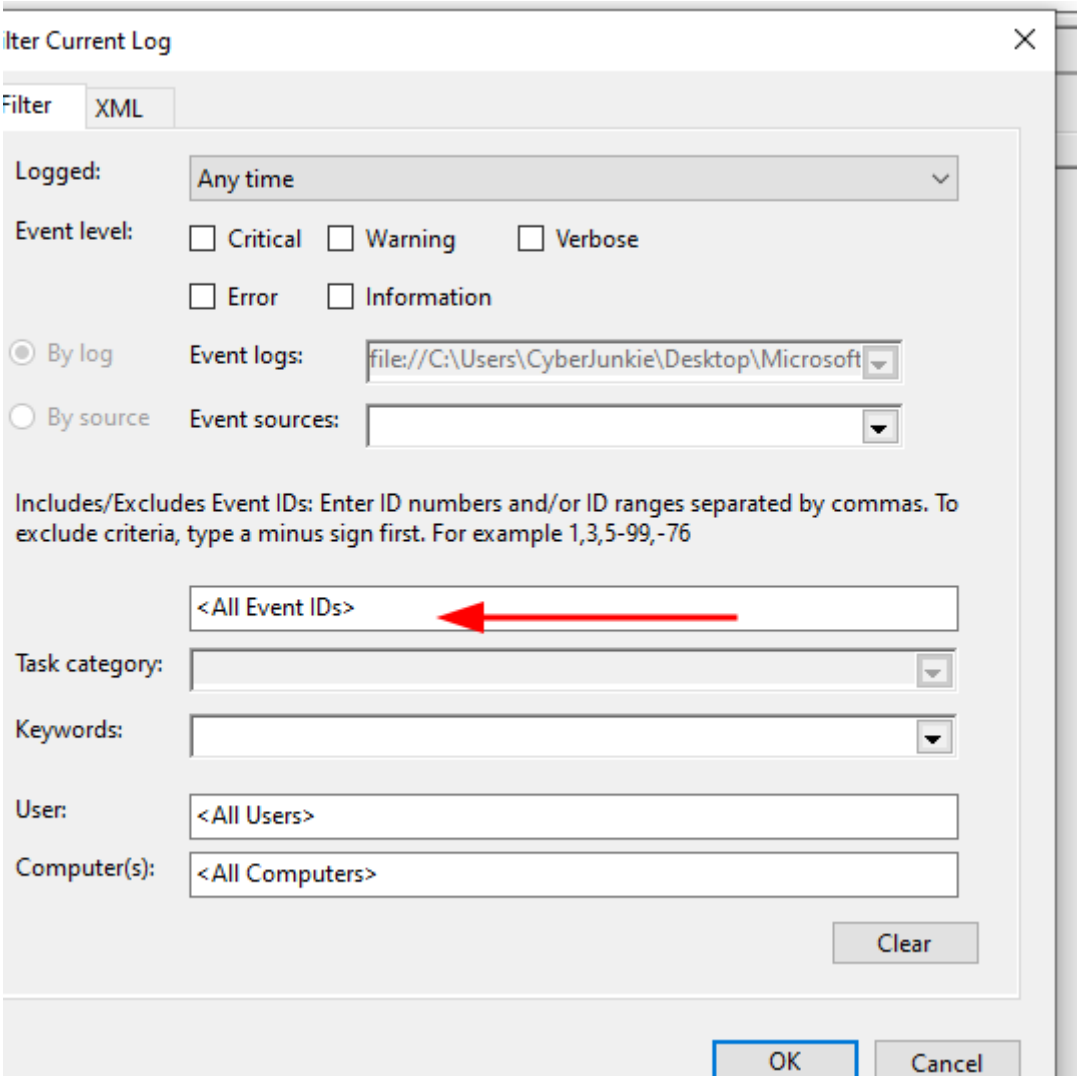
Q1 How many Event logs are there with Event ID 11?

Hint : Go to Filter Current Log and in Event ID field type 1. Then click Apply.

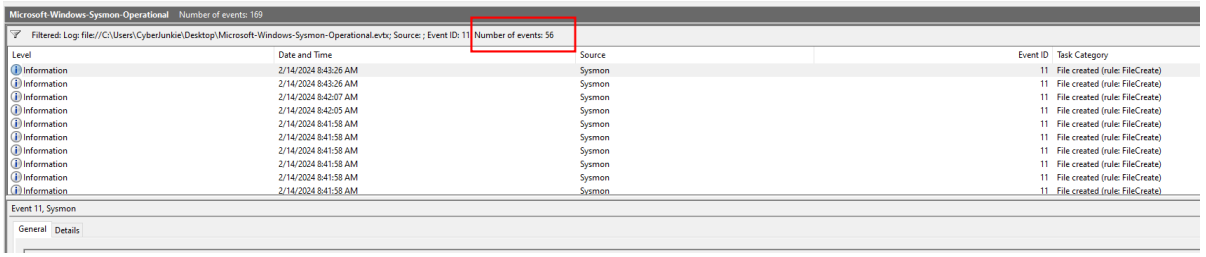
Our task here is to confirm the number of event logs with the Event ID 11. Event ID 11 indicates a file has been created on a host within Sysmon logs. We will use the Filter Current Log action within Event Viewer, detailed below.



Next we enter the event ID `11` into the text field shown below.



We are able to confirm there are 56 events within the evtx file with the Event ID of 11.



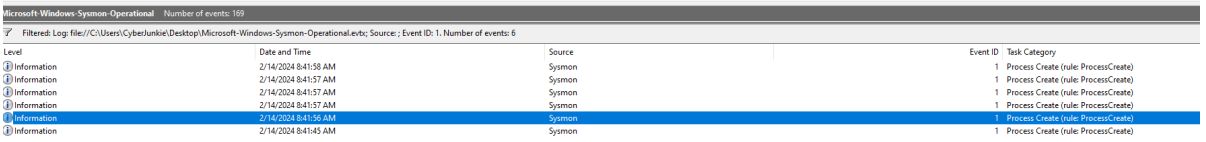
Ans: 56

Q2 Whenever a process is created in memory an event with Event ID 1 is recorded with details as command line,hashes,process path, parent process path etc. This all information is very useful for an analyst because this let's us see all programs executed on a system which means we can spot any malicious processes being executed. What is the malicious process which infected the Victim's system?

Hint : Filter events for Event ID 1. Look for any suspicious file name executing from odd directory.

Our task here is to spot the malicious process which likely infected the compromised host. Using the same process as detailed in question 1 we filter for Event ID 1, which is the event id for process creation. We are looking for the event ID for process creation as it will detail the process names, potentially highlighting what is suspicious or malicious.

Once filtered, we locate only 6 events with Event ID 1 - Process Creation.



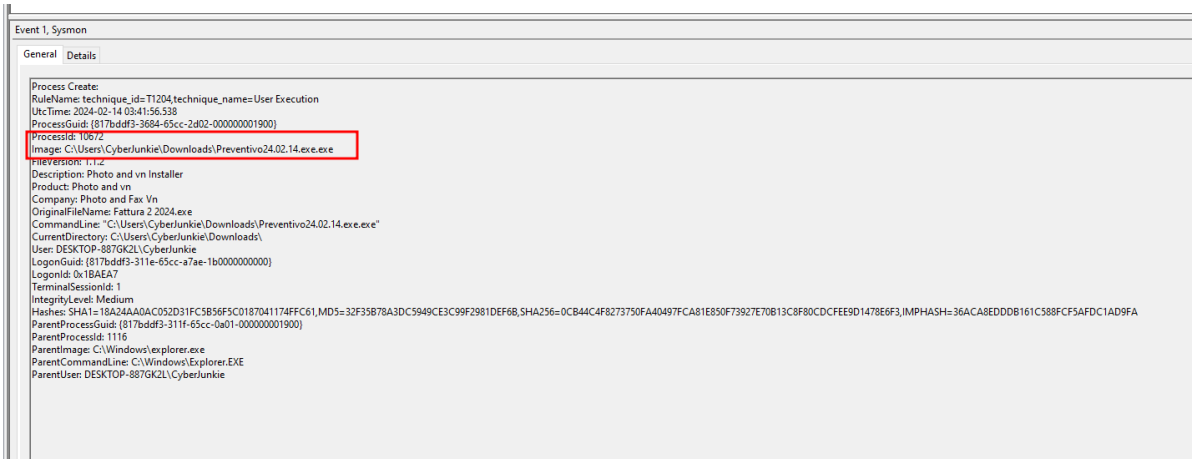
We don't need to perform anything fancy due to the low amount of events, so we click through the events reading through the logs. Please see below a breakdown of the fields within Event ID 1 - Process Creation:

- **UtcTime**: The timestamp of when the event was generated, in Coordinated Universal Time (UTC). This is crucial for correlating events across different systems and time zones.
- **ProcessGuid**: A unique identifier for the process. Sysmon generates this to track the process uniquely across its lifetime, even if its process ID (PID) changes due to system restarts or other factors.
- **ProcessId**: The Process ID (PID) assigned by Windows. This is a numeric identifier that the operating system uses to manage processes.
- **Image**: The full path to the executable file of the process. This is essential for identifying exactly what program ran.
- **FileVersion**: The version number of the executable file. This can be useful for determining whether a specific patch or version of an application, which may have vulnerabilities, was running.
- **Description**: A brief description of the executable file, often provided by the software developer. This can help with identifying the purpose of the process at a glance.
- **Product**: The name of the product this executable is part of. Like the description, this aids in quickly understanding the process's origin and purpose.

- **Company**: The company that created the executable. This information can be used to verify the legitimacy of the process; processes from unknown or suspicious companies might warrant further investigation.
- **OriginalFileName**: The original name of the executable file as designated by the developer. This can be useful for identifying processes that are masquerading as legitimate ones by using misleading file paths or names.
- **CommandLine**: The command line that was used to start the process, including any parameters or arguments. This is critically important for understanding the context in which a process was started, especially if it includes unusual or suspicious commands.
- **CurrentDirectory**: The directory from which the process was started. Malware often operates from temporary or unusual directories, so this can be a clue to malicious behavior.
- **User**: The username under which the process is running. This can indicate whether the process has elevated privileges or if it's running under the context of a regular user.
- **LogonGuid** and **LogonId**: These fields provide information about the user session that started the process. This can help determine if a process was started as a result of user interaction or if it was automatically started by the system.
- **TerminalSessionId**: Identifies the Terminal Services (Remote Desktop) session in which the process is running. This can be particularly useful in analyzing remote access activities.
- **IntegrityLevel**: Indicates the integrity level of the process, which is a measure of the process's potential to harm the system. Higher integrity levels (like "System") have more access to system resources, whereas lower levels (like "Low") are more restricted.
- **Hashes**: Provides hashes (e.g., MD5, SHA1, SHA256) of the process executable. Hashes are unique fingerprints of files and are indispensable for confirming the exact identity of the executable, especially when comparing against known malicious files or verifying file integrity.
- **ParentProcessGuid** and **ParentProcessId**: These fields identify the process that created (or spawned) this process, providing insights into the chain of process creation that can reveal malicious parent processes initiating seemingly legitimate ones.
- **ParentImage**: The full path to the executable of the parent process. This helps in understanding the relationship between processes and identifying suspicious chains of process execution.
- **ParentCommandLine**: The command line used by the parent process. This can give context to how and why the process was started, which is useful in uncovering malicious activity chains.

As detailed above, Sysmon provides an extremely granular amount of detail. When performing the initial investigation we will focus on the Image, Parent Image and CommandLine fields. This is due to being able to confirm the name of the executable that started the process and also any CommandLine output generated. Malicious activity can often by confirmed by an `unusual` process name or unusual CommandLine output.

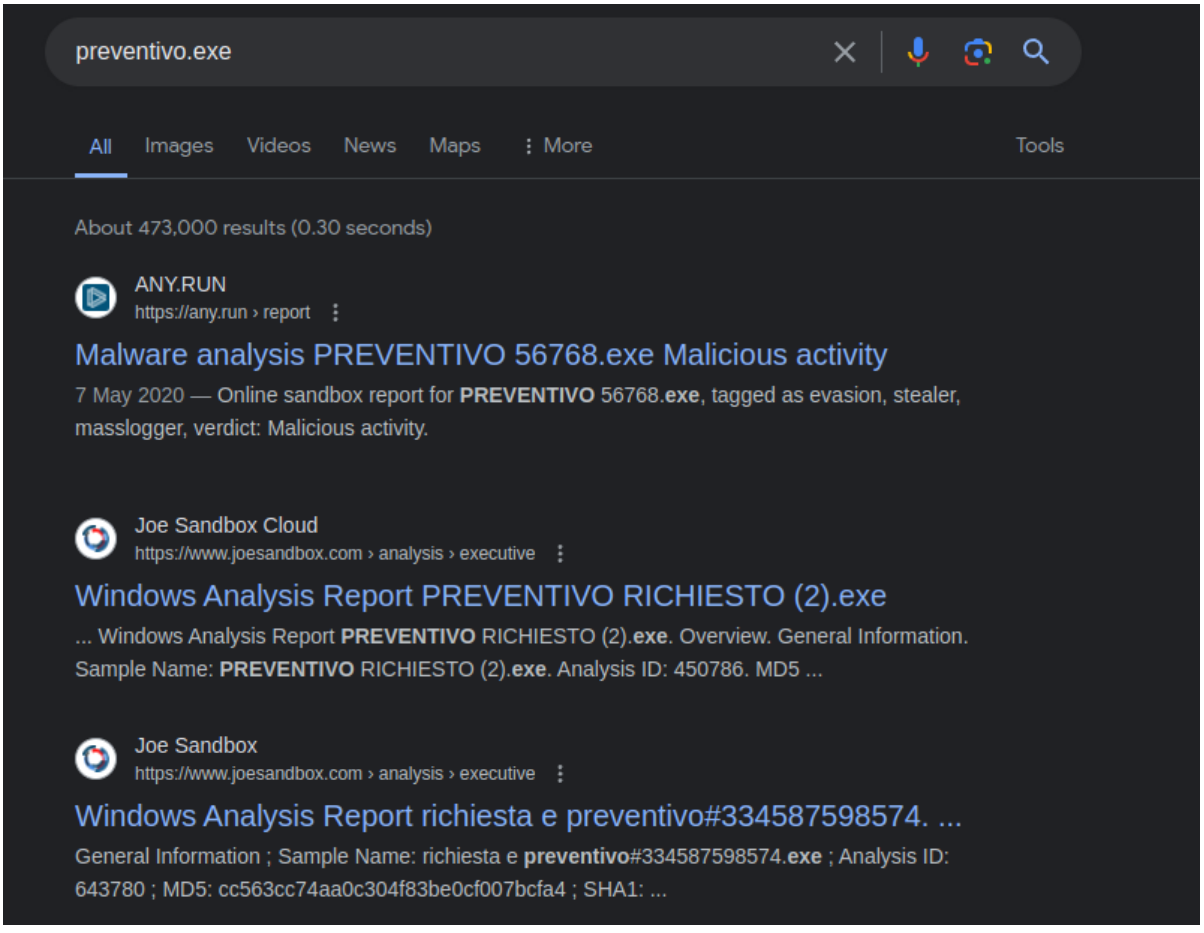
When browsing through the 6 events we locate, as detailed below, an unusual event where a Windows executable is executed.



Lets delve into why its suspicious:

- The binary is named with a double .exe extension, this is unusual.
- The binary is executed directly from the `C:\Users\Cyberjunkie\Downloads\` directory.

As part of our analysis process we can also perform a brief Google search for the name of the executable. We perform this activity to try and locate any potential low hanging fruit - has this file name been seen in other campaigns? Is it known to be malicious or suspicious? Is it a legitimate piece of software that we'd expect to see on our host?



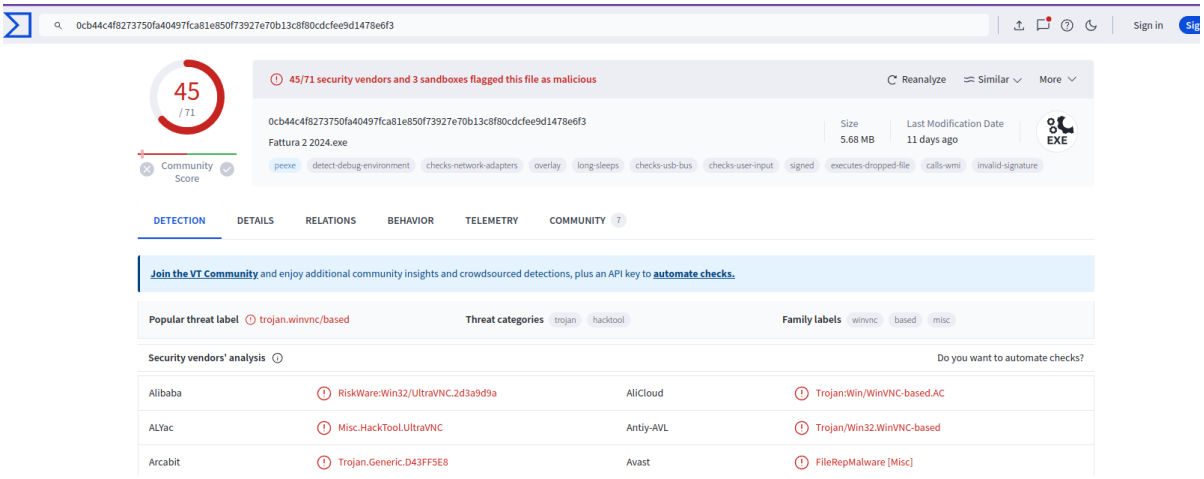
The Google search further adds to our suspicion this is a malicious executable due to a wide variety of analysis reports existing from various Analysis sites. Additionally, there are no indications of this binary falling in line with the Description & Product field of our sysmon log, which indicate this is a `Photo and Fax vn` based executable.

Due to Sysmon containing the SHA1, MD5 and ImpHash we are able to perform a search in VirusTotal for the hash.

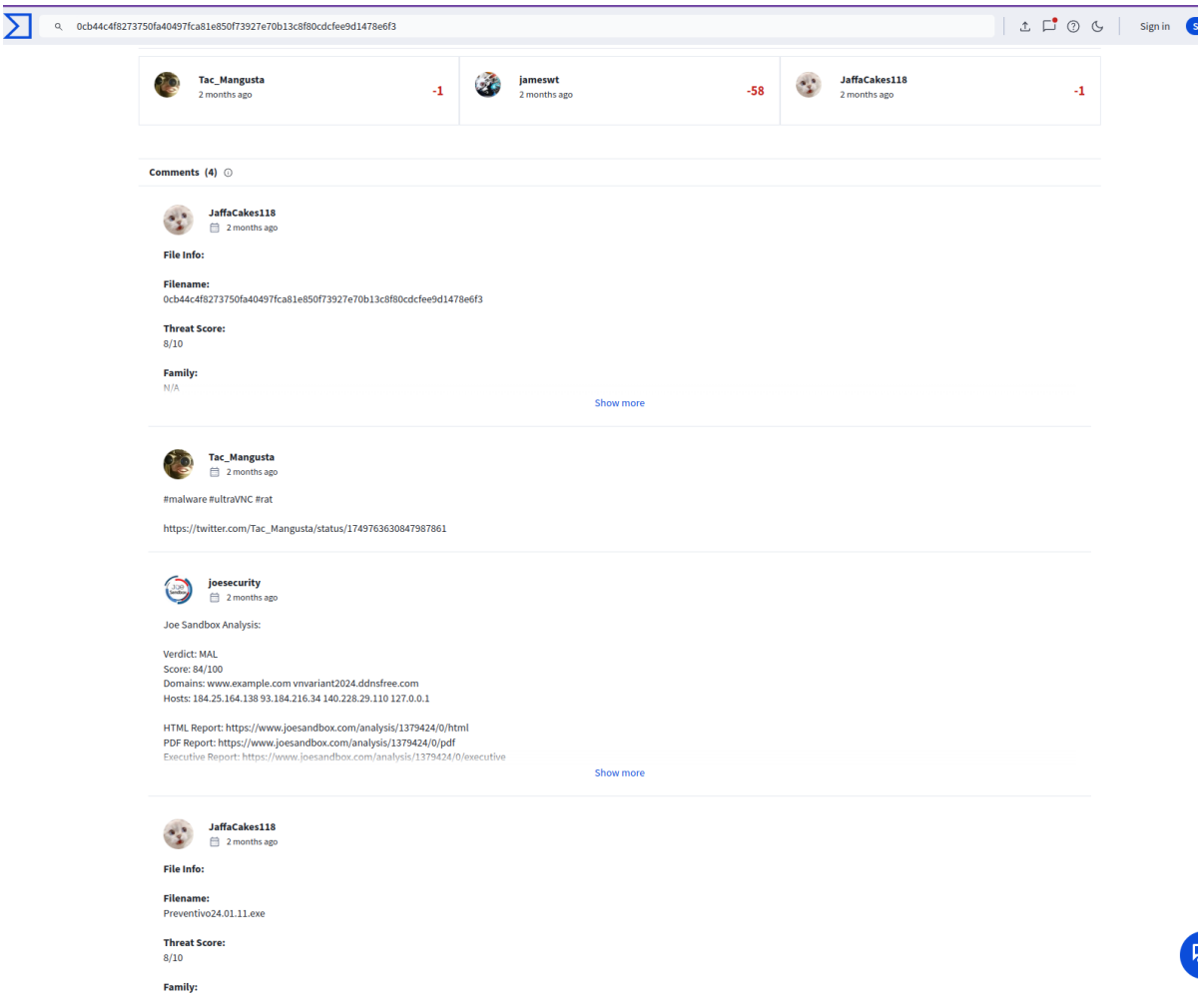
```
Medium
SHA1=18A24AA0AC052D31FC5B56F5C0187041174FFC61,MD5=32F35B78A3DC5949CE3C99F2981DEF6B,SHA256=0CB44C4F8273750FA40497FCA81E850F73927E70B13C8F80CDCFEE9D1478E6F3,IMPHASH=
36ACA8EDDDB161C588FCF5AFDC1AD9FA
```

VirusTotal is a comprehensive online service that allows users to analyse files, URLs, domains, and IP addresses for malicious content using a variety of antivirus engines and website scanners. It aggregates multiple antivirus products and online scan engines to provide a high level of accuracy in detecting potential threats. By submitting a file or a URL to VirusTotal, it is checked against databases of known malware and suspicious behaviour patterns, making it a valuable resource for cybersecurity professionals, researchers, and forensic investigators.

Using a browser of your choice, browse to https://www.virustotal.com and copy and paste the MD5 hash found in the Event.



We confirm that the executable is a known malicious binary, based on the threat label likely associated with a WinVNC based trojan. Within VirusTotal we can also click on the `Community` tab for additional information. We can view community comments and analysis from other sandbox sites such as JoeSandbox.



As detailed in the comments we see numerous users having reported this as an UltraVNC RAT, with JaffaCakes even highlighting a similar file name to the one seen in our investigation.

Ans C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe

Q3 Which Cloud drive was used to distribute the malware?

Hint : Event ID 22 can be used to look for any DNS Queries made by the system. Do not filter for any specific event id, start analysing the Events from oldest available event. If you see the events related to the malicious file being created, look for Event ID 22 event surrounding that event.

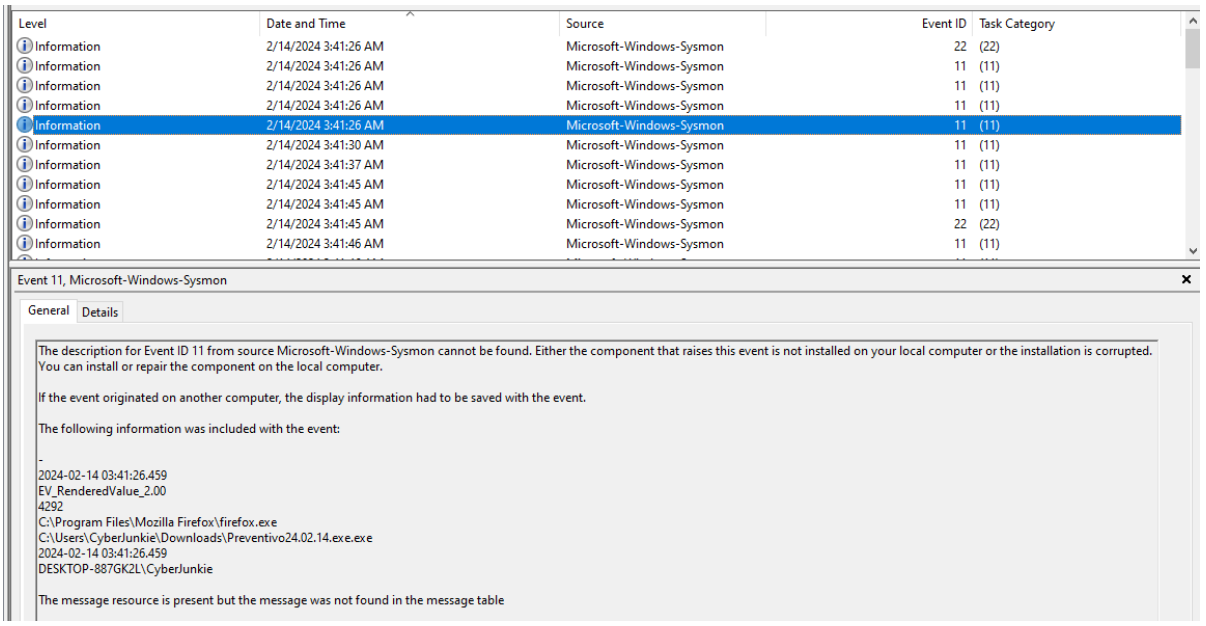
Cloud services are a common method utilised by Threat Actors to distribute malware. These often aren't flagged as malicious and won't often be dropped by company perimeter devices. Due to Sysmon being installed on the host we are able to filter for Event ID 22, and view DNS queries made by the host within a similar time period of the compromise.

We are presented with three events, with the Event ID of 22.

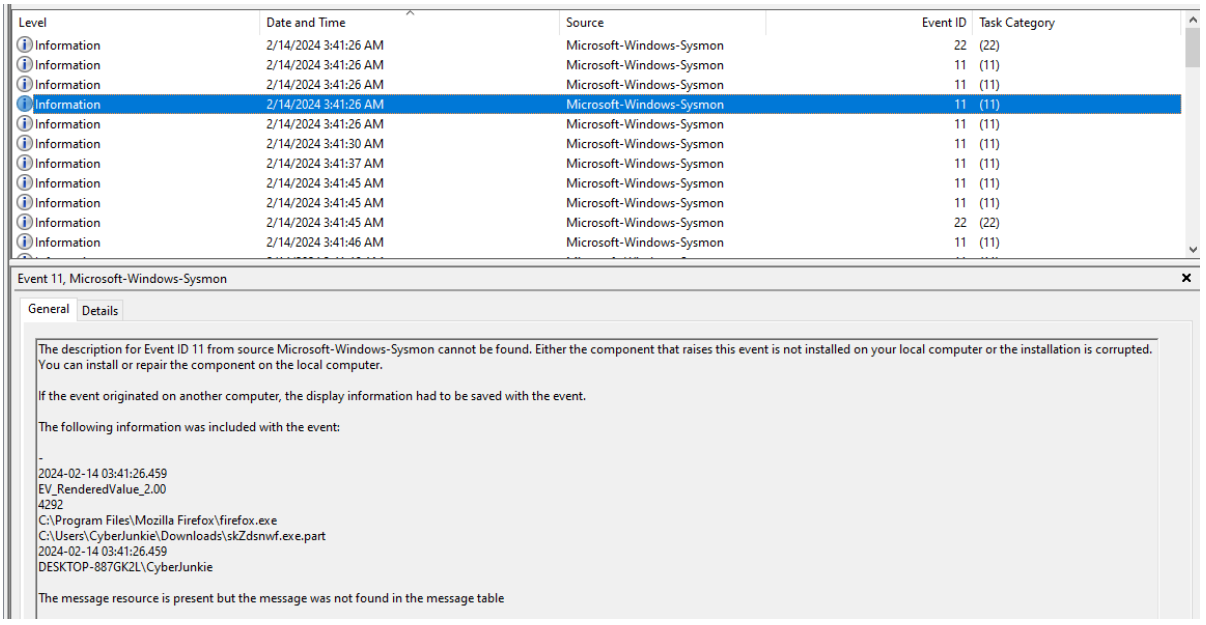
Level	Date and Time	Source	Event ID	Task Category
Information	2/14/2024 3:41:26 AM	Microsoft-Windows-Sysmon	22	(22)
Information	2/14/2024 3:41:45 AM	Microsoft-Windows-Sysmon	22	(22)
Information	2/14/2024 3:41:58 AM	Microsoft-Windows-Sysmon	22	(22)

Interestingly looking at the data within the event that occurred at `03:41:26` we are able to view the utilisation of Dropbox, a cloud file storage site. Lets add an additional filter, EventID 11 and view the combination of File Creation Events alongside our DNS queries to correlate the two in our viewer.

We are now able to confirm the correlation of the download of our malicious binary from what we believe is the Dropbox cloud storage location.



Interestingly, the three events prior to the FileCreation event of Prevntivo24.02.14.exe.exe are events showcasing the Firefox functionality of a temporary "part" file.



Based on our analysis, with the timing of the download of the file we can conclude that Dropbox was likely the delivery mechanism of the malware.

Ans: dropbox

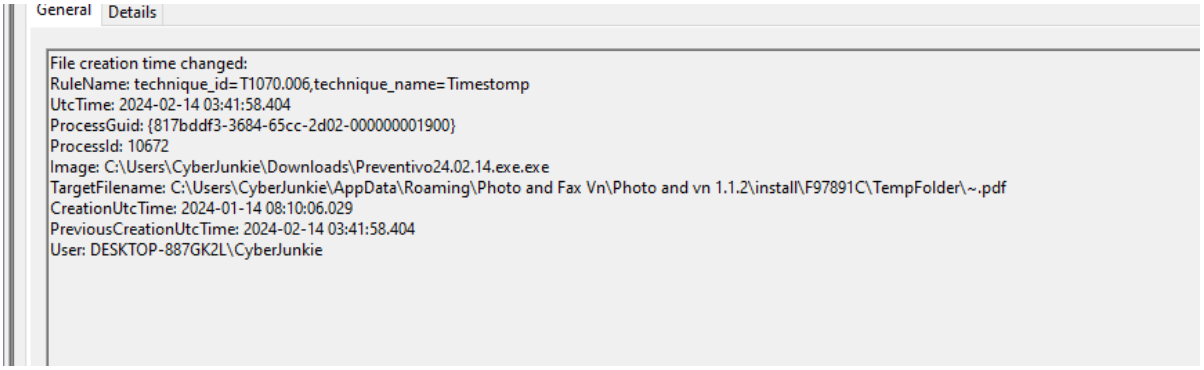
Q4 The Initial malicious file time stomped (A defense evasion technique , where file creation date is changed to make it appear old) many files it created on disk. What was the timestamp changed to for a pdf file?

Hint : Filter for Event ID2. This event id records any file creation time change on any files on the system.

The question indicates timestomping has been performed on the host, which would be detected by EventID 2 within the Sysmon logs. This event records any file creation time changes on the system. Timestomping is a technique often used by Threat Actors to manipulate the timestamps of files within a computer system. These timestamps include the date and time a file was created, last modified, and last accessed. By changing these details, someone can hide their tracks, making it

harder for investigators or security software to determine when the files were actually altered or created.

Using our the same method of filtering as previously covered, we filter for EventID `2` and are able to view the modification of the date & time of the malicious file dropped onto the host as detailed below:



Ans: 2024-01-14 08:10:06

Q5 The malicious file dropped few files on disk. Where was once.cmd created on disk?

Hint :Filter for Event ID 11 and notice the files created where the Image name is the name of malicious file.

We begin by filtering for Event ID 11, which corresponds to file creation events. Subsequently, we utilise the find feature of event logs to search for the filename "once.cmd". This search yields two results: one instance where the file was created by msiexec, and another where it was created by preventivo24.02.14.exe. It is the latter instance in which we are particularly interested.

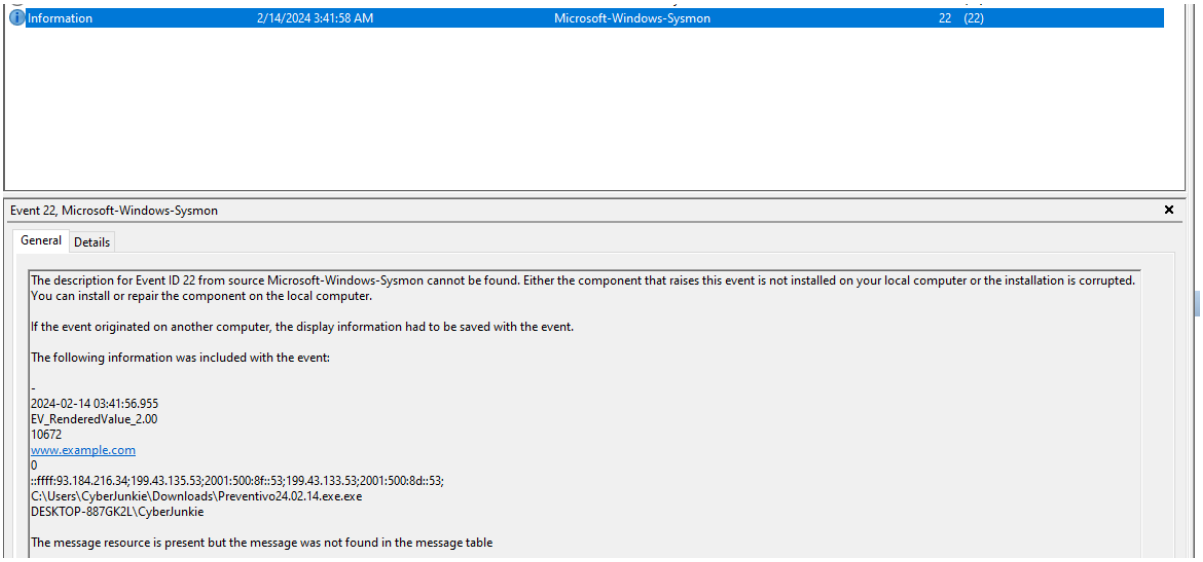
We can also observe from this event that the malicious file is depositing additional files along the path: "C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games".

Ans: 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 tried to reach a dummy Domain, most probably to check internet connection status. What domain name it tried to connect to?

Hint : Filter for event id 22 and look for the image field. The process name should be the malicious file making the connection.

We need to refer back to our EventId22 again here, using our previously taught method of filtering. We are able to ascertain that the malicious binary attempts to communicate to the www.example.com domain.



Ans www.example.com

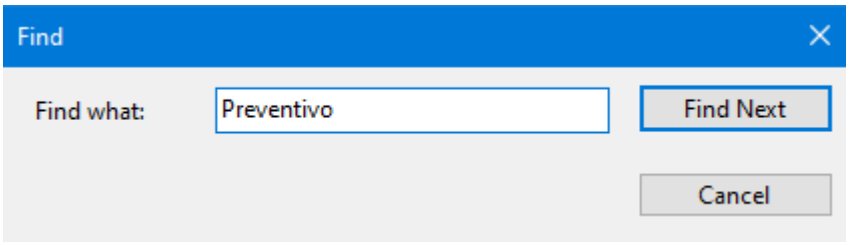
Q7 Which IP Address did the malicious process tried to reach out to?

Hint : Look for EventID3. It records the IP Address, port and the process trying to make the connection

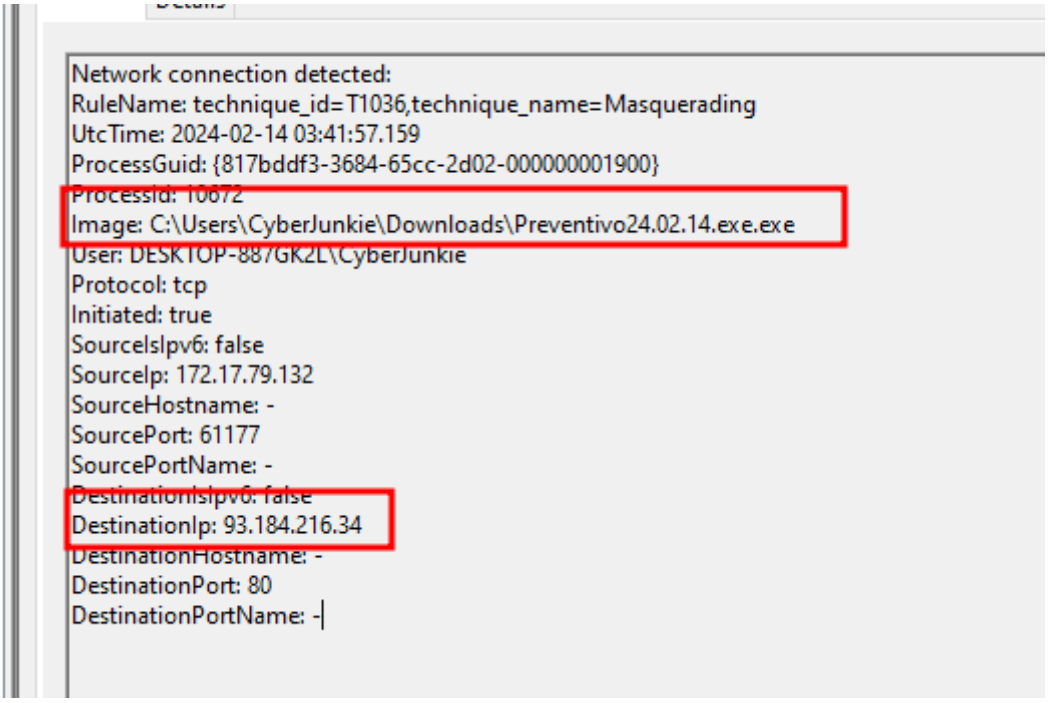
When hunting for IP addresses communicated with by a process, we must filter for EventId 3, which is the event id for network connection detected. See below for a breakdown of the fields of EventId3.

1. **UtcTime**: The timestamp when the event was generated in UTC.
2. **ProcessGuid**: A unique identifier for the process that initiated the connection, allowing correlation with other events.
3. **ProcessId**: The ID of the process that initiated the connection.
4. **Image**: The file path of the executable for the process.
5. **User**: The security context under which the process was running, often including the domain, username, and logon ID.
6. **Protocol**: The protocol used for the connection, such as TCP or UDP.
7. **Initiated**: Indicates whether the connection was initiated by the process. A true value means the process initiated the connection; false means it was receiving an incoming connection.
8. **SourceIsIpv6**: Indicates whether the source IP address is IPv6.
9. **SourceIp**: The source IP address of the connection.
10. **SourceHostname**: The resolved name of the source IP, if available.
11. **SourcePort**: The source port number of the connection.
12. **SourcePortName**: The name of the source port, if available.
13. **DestinationIsIpv6**: Indicates whether the destination IP address is IPv6.
14. **DestinationIp**: The destination IP address of the connection.
15. **DestinationHostname**: The resolved name of the destination IP, if available.
16. **DestinationPort**: The destination port number of the connection.
17. **DestinationPortName**: The name of the destination port, if available.

Our filter this time can include the filter for EventId 3, and then use the "Find" Action to search for any logs containing Preventivo.



Whilst only one log exists within this Event Log file, this Find action would be useful had it being a larger event log file with more events. We are able to locate the malicious process communicating with `93.184.216.34`.

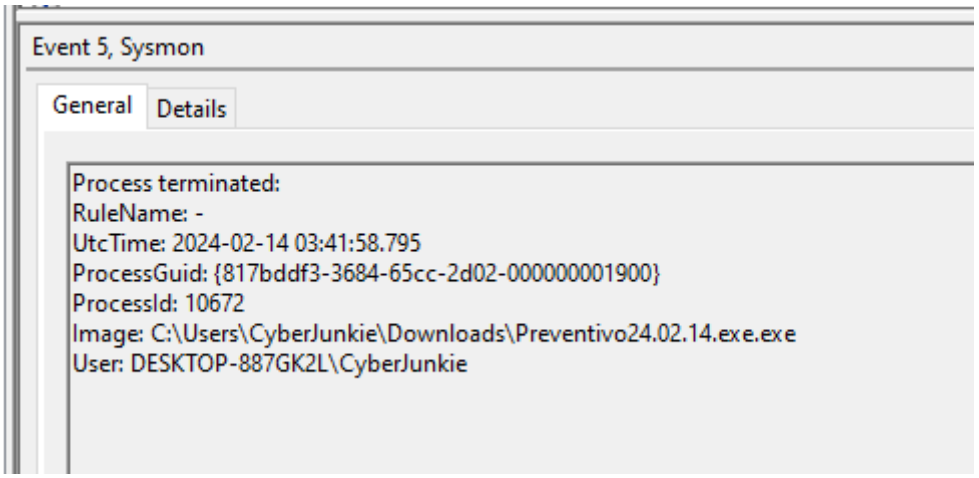


Ans 93.184.216.34

Q8 The malicious process terminated itself after infecting the pc with UltraVnc backdoored variant. When did the process terminated itself?

Hint : Filter for event ID 5 and look for the Image name which should be the malicious process.

Event ID 5 within Sysmon logs indicates Process Termination. We will use an identical flow, Filter for EventID 5 and locate the termination of Preventivo. We can confirm the process terminated at 2024-02-14 03:41:58.



Ans 2024-02-14 03:41:58