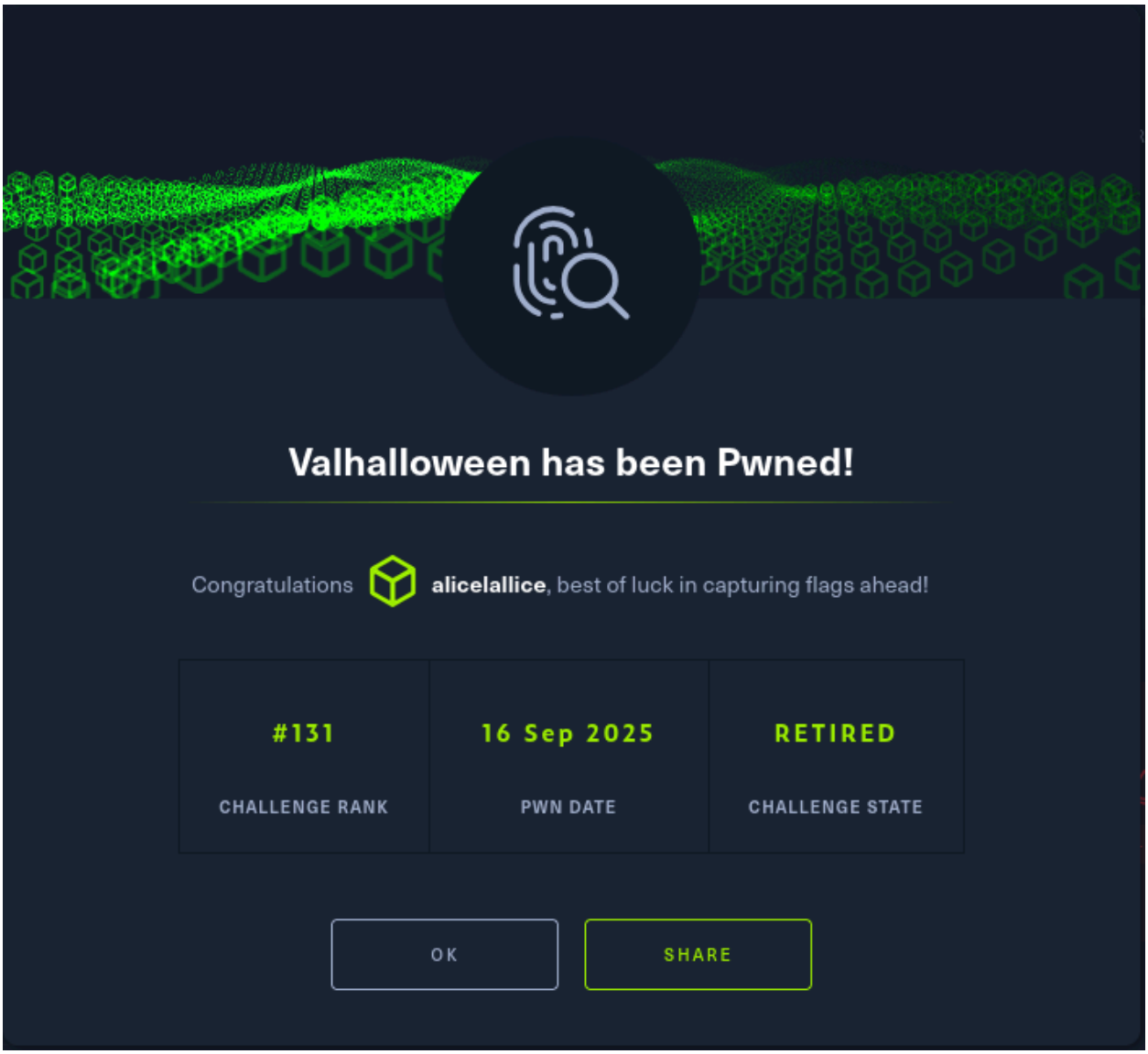
Valhalloween

Types	forensic
CTF	HTB



Valhalloween — forensic write-up

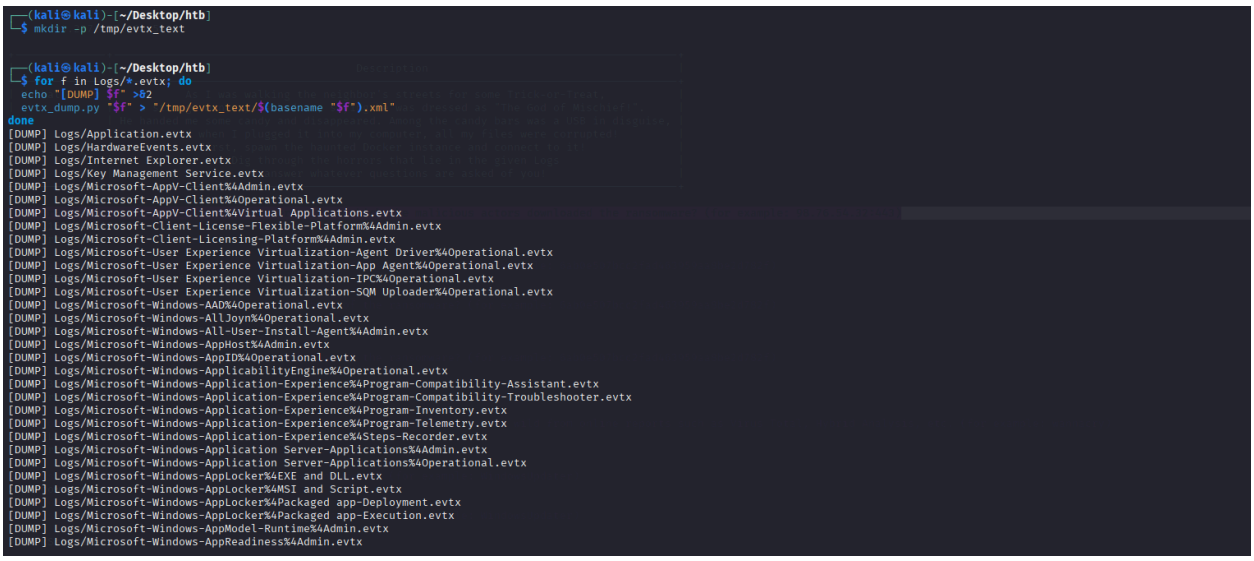
Scope: investigate provided Windows event logs (Sysmon, PowerShell, Task Scheduler, etc.) from the Valhalloween challenge and answer the posed questions: server IP:port, ransomware MD5, family label, scheduled task name, parent process, initial-stage file path and when it was first opened (UTC).

> *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 EVTX 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

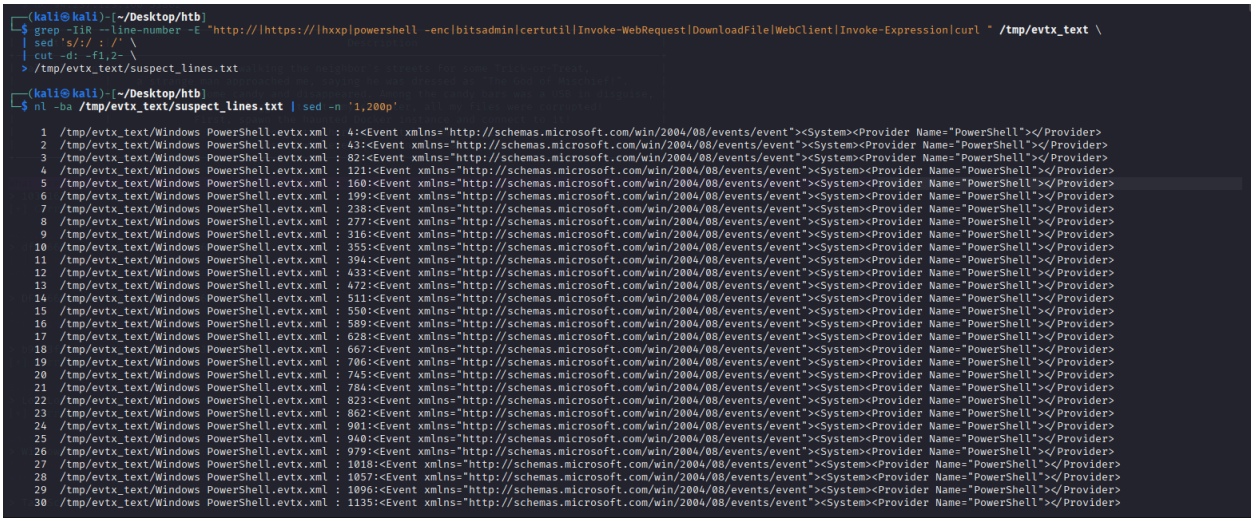
```
mkdir -p /tmp/evtx_text
for f in Logs/*.evtx; do
  echo "[DUMP] $f" >&2
  evtx_dump.py "$f" > "/tmp/evtx_text/$(basename "$f").xml"
done
```



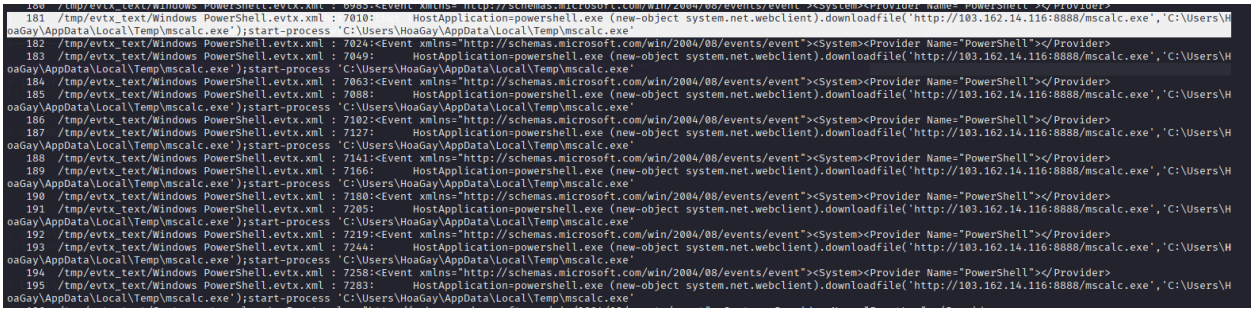

```
# search the dumps for suspicious download commands and extract candidat
```

```
e ip:port & urls
grep -IiR --line-number -E "http://|https://|hxxp|powershell -enc|bitsadmin|certutil|Invoke-WebRequest|DownloadFile|WebClient|Invoke-Expression|curl " /tmp/evtx_text \
  | sed 's/:/ : /' \
  | cut -d: -f1,2- \
  > /tmp/evtx_text/suspect_lines.txt

# show unique suspect lines (first 200 lines)
nl -ba /tmp/evtx_text/suspect_lines.txt | sed -n '1,200p'
```



suddeny i found the malicious log



Answer: **103.162.14.116:8888**

> *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.

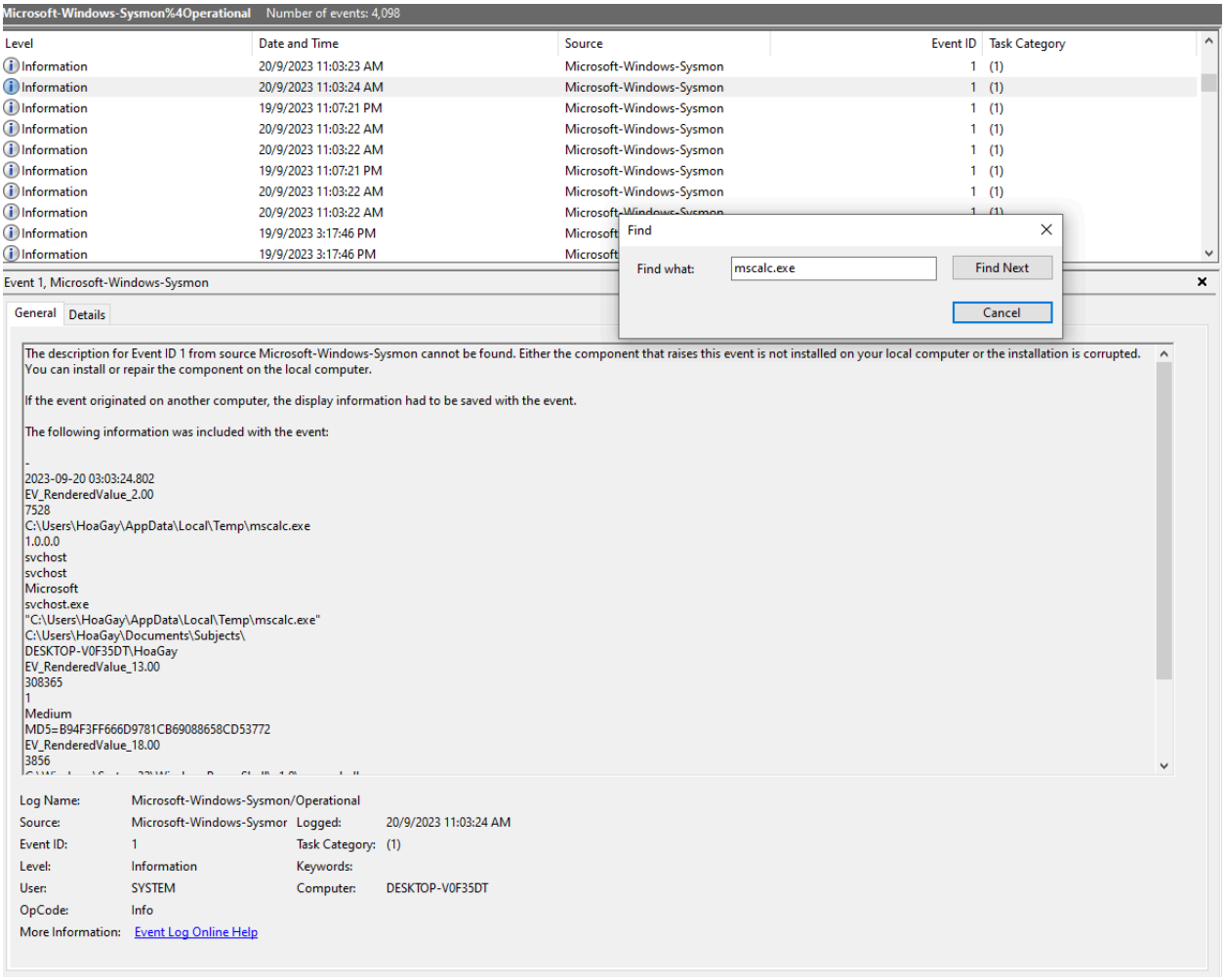
---

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.

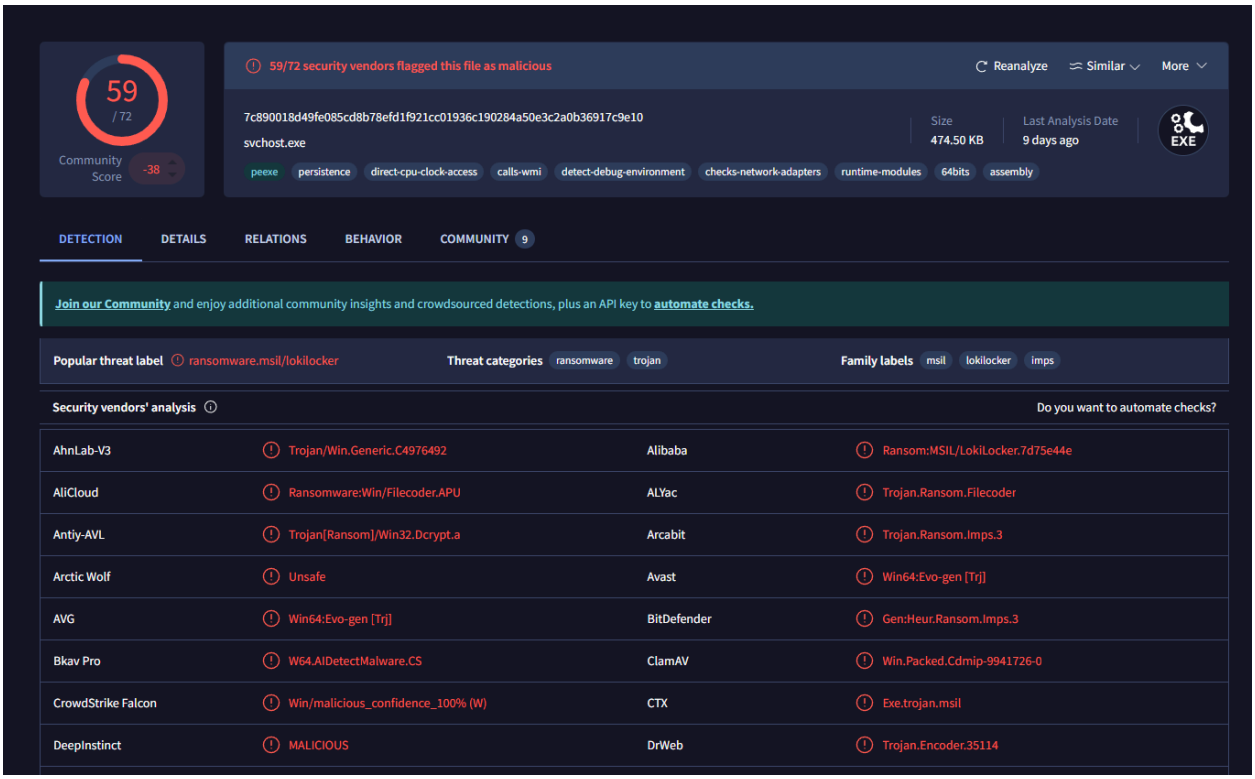


The Sysmon **Process Creation** event (`Event ID 1`) for `C:\Users\HoaGay\AppData\Local\Temp\mscalc.exe` shows the **actual ransomware binary** being executed, and its MD5 hash is:

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

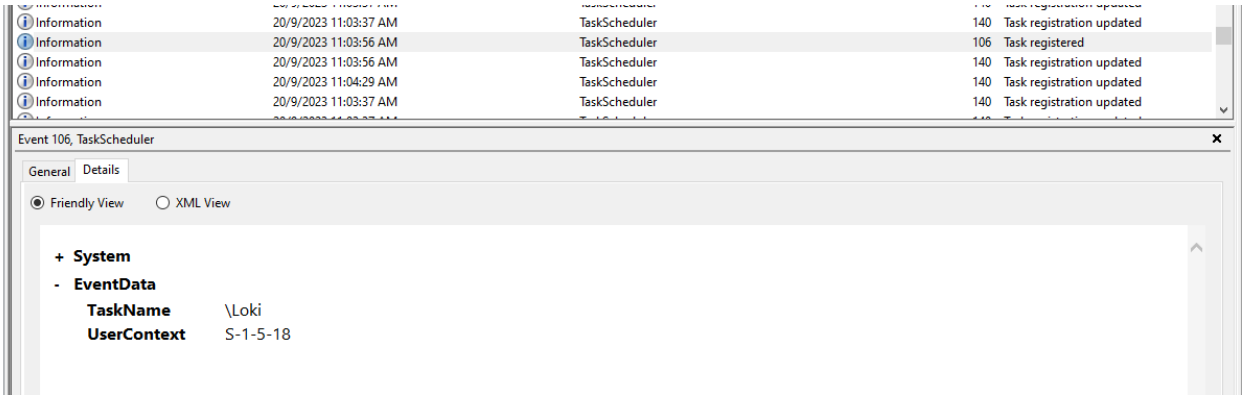


From those detections we can clearly see the **dominant family label** is:

Answer: **LokiLocker**

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

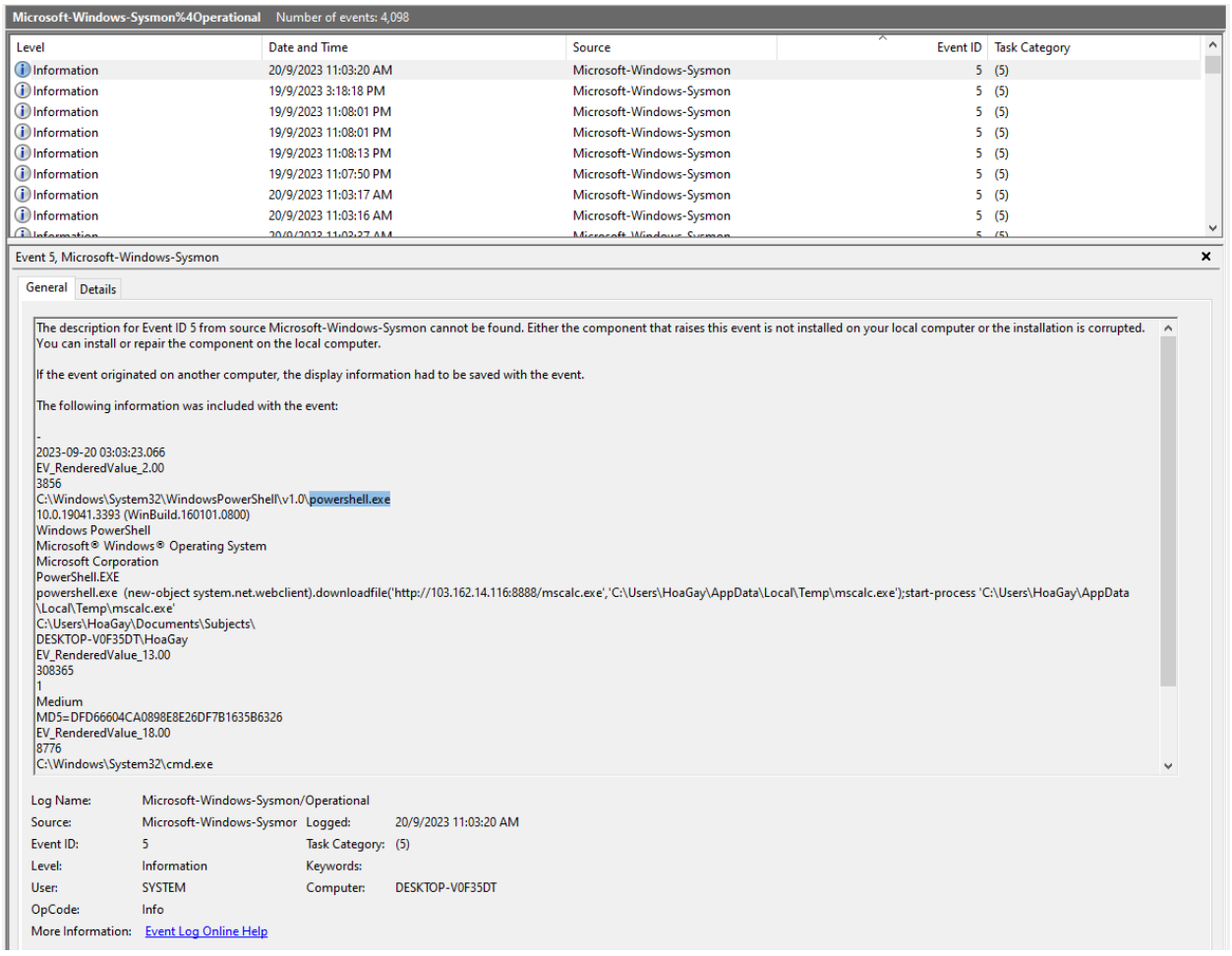
In `Microsoft-Windows-Sysmon%4Operational.evtx`, we see a persistent scheduled task created called “Loki”. You can also see this same process in behavioral statistics in VirusTotal .



Answer: **Loki**

> *What are the parent process name and ID of the ransomware process? (for example: svchost.exe_4953)*

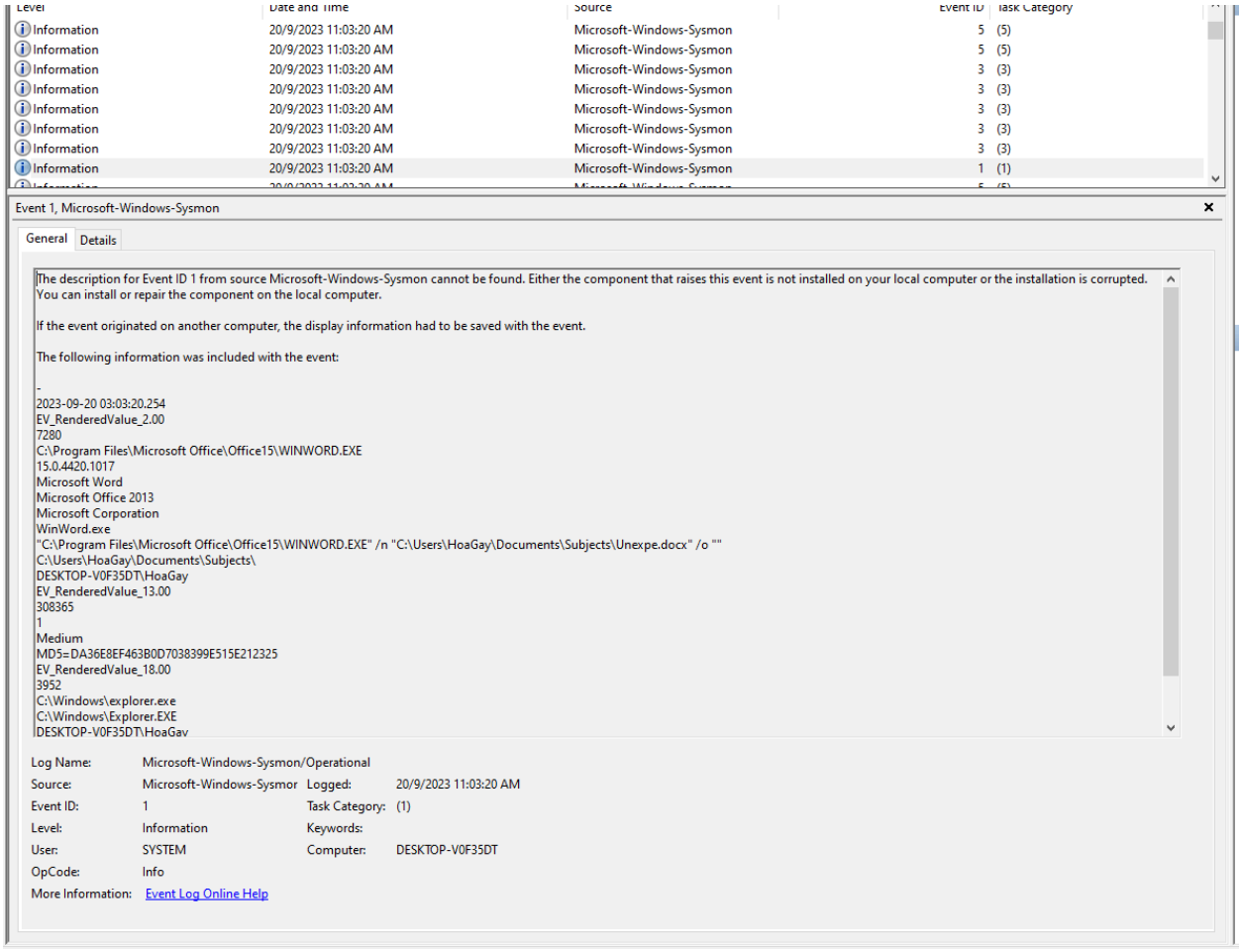
In `Microsoft-Windows-Sysmon%4Operational.evtx`, we see the parent process id is 3856 from `powershell.exe`.



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\Hoa Gay\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 Ta
sk (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)