FOG Ransomware Targets Higher Education

By Sarah Becker, Marc Messer, Dan Cox

Published: 2024-08-20 · Archived: 2026-04-02 11:14:46 UTC

In Q2 2024, the Kroll Cyber Threat Intelligence (CTI) Team observed an increase in activity around a new ransomware group named FOG. FOG was initially observed in May 2024, and since then has been heavily targeting higher educational institutions in the U.S. by exploiting compromised VPN credentials. Kroll's review of a recent FOG binary (1.exe) found no exfiltration or persistence mechanisms directly integrated. FOG is known to utilize third-party tools and cloud services for exfiltration during attacks, which have often led to double extortion to put more pressure on victims to pay the ransom . Double extortion is a tactic leveraged by threat actors where they both encrypt and exfiltrate data, increasing the likelihood that a victim will pay their ransom. At the time of writing, FOG operates a Data Leak Site where they threaten to post and eventually publish victims' leaked data if a ransom is not paid.

TTPs

Below are some key tactics, techniques and procedures (TTPs) the Kroll CTI Team has observed during investigations involving FOG ransomware:

Initial Access

FOG ransomware has been observed leveraging compromised VPN credentials or valid user credentials for initial access.

Privilege Escalation

After breaching a network, FOG operators are observed abusing "pass-the-hash" attacks on administrator accounts. Further, brute forcing of user accounts, custom PowerShell scripts and extracting passwords from user browsers and NT Directory Service (NTDS.dit) are also utilized to escalate privileges.

Persistence

To maintain persistence, the group establishes Remote Desktop Protocol (RDP) connections on Windows servers. FOG may also employ credential stuffing to hijack additional user accounts and even create new user accounts solely for persistence. They've also leveraged FileZilla and reverse SSH Shells to ensure a foothold on the system.

Enumeration

The group is known to deploy Metasploit and PsExec across multiple hosts. Kroll has also observed the use of Advanced Port Scanner, LOLBins, SharpShares and SoftPerfect Network Scanner to gather data.

Evasion

On compromised Windows servers, the attackers disabled Windows Defender and multiple processes and services to avoid detection before deploying the ransomware.

FOG then leveraged Windows API calls to gather system information and terminate further specific processes and services. The ransomware encrypts a wide variety of files, including Virtual Machine Disks (VMDKs), and deletes backups from Veeam and Windows Volume Shadow copies before appending the .FOG or .FLOCKED extension to encrypted files.

Ransomware

Once the ransomware has been executed and files have been encrypted, a ransom note, typically named "readme.txt", is left in affected directories to provide instructions on how to pay for decryption. The note includes a link to a Tor site for negotiations, which features a chat interface for discussing the ransom and providing proof of stolen files. Ransom demands vary and may reach multiple hundreds of thousands of dollars for larger organizations.

Exfiltration

When exfiltrating data, the group has been known to leverage 7-Zip, third-party cloud services and WinRAR.

Malware Analysis

Our Malware Analysis and Reverse Engineering Team recently reviewed a Fog binary (1.exe). In this particular sample, no exfiltration or persistence mechanisms were observed integrated into the binary. The ransomware can be executed with a number of flags, such as:

- id [string identifying the target]
- nomutex [specified so multiple instances of the malware can be run simultaneously]
- procoff [stops processes specified in config under ShutdownProcesses]
- uncoff [disables network share enumeration and encryption]
- size [integer, specifies AES block size]
- console [specifies console output saving to DbgLog.sys]
- target [path for encryption/enumeration]

Within the configuration file, several other values can be specified:

- RSAPubKey [key used for encryption]
- LockedExt [file extension]
- NotefileName [ransom note name]
- ShutdownProcesses [specifies processes to stop prior to encryption]
- ShutdownServices [specifies services to stop prior to encryption]

When executed, the malware goes through a few steps:

- A file named DbgLog.sys is created within the directory from which the sample is executed. This file contains information about the malware as it executes, saving the console output for debugging

information.

- System information enumerating the drives and processors available is then queried, and a number of threads is assigned accordingly. Shadow volumes are subsequently deleted via “vssadmin.exe delete shadows /all / quiet”.

During execution, the encryption is handled via symmetric encryption. A symmetric key is generated at runtime, and this encryption key is subsequently encrypted using an asymmetric key. As a result of this process, the threat actor’s private key is necessary to recover the symmetric key for decryption. Function calls to accomplish this are largely handled by resolving functions via the Process Environment Block (PEB), allowing for functionality to be somewhat hidden as the pointers for each function can be resolved without directly referencing the API function.

Ransom notes named "readme.txt" are dropped within each directory containing encrypted files.

```
If you are reading this, then you have been the victim of a cyber attack. We call
ourselves Fog and we take responsibility for this incident. We are the ones who
encrypted your data and also copied some of it to our internal resource. The sooner
you contact us, the sooner we can resolve this incient and get you back to work.
To contact us you need to have Tor browser installed:

1. Follow this link: xql562evsy7njcsngacphc2erzjfecwotdkobn3m4uxu2gthq26newid.onion
2. Enter this code: XXXXXXXXXXXXXXXXXXXXXXXX
3. Now we can communicate safely.

If you are decision-maker, you will get all the details when you get in touch. We are
waiting for you.
```

Source: https://www.kroll.com/en/insights/publications/cyber/fog-ransomware-targets-higher-education