

New Fog ransomware targets US education sector via breached VPNs

By **Bill Toulas**



June 6, 2024



02:29 PM



0



A new ransomware operation named 'Fog' launched in early May 2024, is using compromised VPN credentials to breach the networks of educational organizations in the U.S.

Fog was discovered by Artic Wolf Labs, which reported that the ransomware operation has not set up an extortion portal yet and was not observed stealing data.

However, BleepingComputer can confirm the ransomware gang steals data for double-extortion attacks, using the data as leverage to scare victims into paying.

VPNs for initial access

Fog's operators accessed victim environments using compromised VPN credentials from at least two different VPN gateway vendors.

"In each of the cases investigated, forensic evidence indicated that threat actors were able to access victim environments by leveraging compromised VPN credentials," explains [Artic Wolf Labs](#).

"Notably, the remote access occurred through two separate VPN gateway vendors. The last documented threat activity in our cases occurred on May 23, 2024."

Once they gain access to the internal network, the attackers perform "pass-the-hash" attacks on administrator accounts, which are used to establish RDP connections to Windows servers running Hyper-V.

Alternatively, credential stuffing is used to hijack valuable accounts, followed by PsExec deployment on multiple hosts.

On Windows servers, Fog operators disable Windows Defender to prevent notifications alerting the victim before the execution of the encrypter.

When the ransomware is deployed, it performs Windows API calls to gather information about the system, such as the number of available logical processors to allocate threads for a multi-threaded encryption routine.

Before starting the encryption, the ransomware terminates a list of processes and services based on a hardcoded list in its configuration.

The ransomware encrypts VMDK files in Virtual Machine (VM) storage and deletes backups from object storage in Veeam and Windows volume shadow copies to prevent easy restoration.

Encrypted files are appended the **'FOG'** or **'FLOCKED'** extension, though this can be set from the JSON-based configuration block to anything the operator wants.

Finally, a ransom note is created and dropped on impacted directories, providing instructions to the victims on paying for a decryption key that will help them get their files back.

From an attack seen by BleepingComputer, the ransom note is named **readme.txt** and contains a link to a Tor dark website used for negotiation. This site is a basic chat interface allowing the ransomware victim to negotiate a ransom demand with the threat actors and get a list of stolen files.

```
1 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 incident and get you back to work.
2 To contact us you need to have Tor browser installed:
3
4 1. Follow this link: xq1562evsy7njcsngacphc2erzjfecwotdkobn3m4uxu2gtqh26newid.onion
5 2. Enter the code: [REDACTED]
6 3. Now we can communicate safely.
7
8 If you are decision-maker, you will get all the details when you get in touch. We are
waiting for you.
9
```

Fog ransom note

Source: BleepingComputer

BleepingComputer can also confirm that the Tor negotiation site is the same for both the .FOG and .FLOCKED extensions, with ongoing attacks using either extension.

In an attack seen by BleepingComputer, the ransomware gang demanded hundreds of thousands to receive a decryptor and delete the stolen data. However, it is likely more for larger companies.

Arctic Wolf Labs says it is currently unclear if Fog operates as an open ransomware-as-a-service (RaaS) that accepts affiliates or if a small private circle of cybercriminals is behind it.

EDUCATION

ENCRYPTION

FOG RANSOMWARE

RANSOMWARE

VPN





BILL TOULAS

Bill Toulas is a tech writer and infosec news reporter with over a decade of experience working on various online publications, covering open-source, Linux, malware, data breach incidents, and hacks.

[< PREVIOUS ARTICLE](#)

[NEXT ARTICLE >](#)