Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

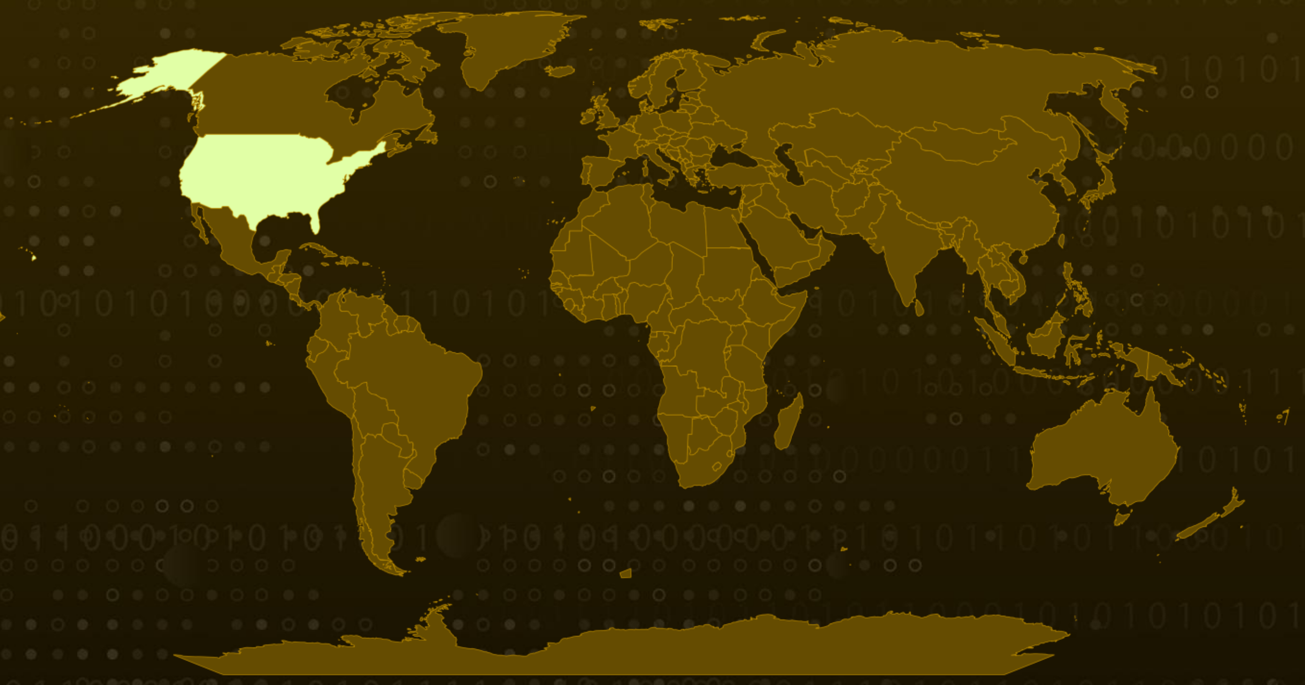
Fog Ransomware Targets US Sectors Via Compromised VPN Credentials

Date of Publication	Admiralty Code	TA Number
June 10, 2024	A1	TA2024222

Summary

Attack Discovered: May 2024
Attack Region: United States
Affected Industries: Education and Recreation
Malware: Fog Ransomware
Attack: A new ransomware operation named 'Fog,' launched in early May 2024, is targeting educational organizations and the recreation sector in the US. The threat actors were able to infiltrate victim environments by exploiting compromised VPN credentials, with the remote access occurring through two separate VPN gateway vendors.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1

In May 2024, the Fog ransomware emerged, significantly impacting organizations in the United States. The education sector bore the brunt, accounting for 80% of the attacks, while 20% targeted recreational facilities. The group behind Fog remains unidentified, but they infiltrated systems using stolen VPN credentials, with the last known attack occurring on May 23, 2024.

#2

The cybercriminals employed advanced methods, such as exploiting administrator accounts, using Remote Desktop Protocol (RDP) to access Windows Servers running Hyper-V and Veeam, and spreading via credential stuffing. They used PsExec to distribute the ransomware across multiple computers and accessed systems through RDP and SMB protocols. They also disabled Windows Defender, encrypted critical files, and deleted Veeam backups.

#3

Fog ransomware shares techniques with other ransomware variants. It creates a log file named `DbgLog.sys` in the `%AppData%` directory and gathers system information to manage its encryption tasks efficiently. It checks for specific command-line options and uses a JSON configuration file to direct its actions. It relies on outdated Windows APIs, `CryptImportKey` and `CryptEncrypt`, to encrypt files, adding new extensions and leaving ransom notes.

#4

The encryption process involves adding file extensions using the `MoveFile` Windows API and the `LockedExt` option, with extensions like `.FOG` and `.FLOCKED`. A ransom note is written to disk using the configured `Notefilename` option. Before terminating, the ransomware deletes volume shadow copies using the `CreateProcess` function with specific switches to ensure silent deletion.

#5

The attackers appear financially motivated, focusing on quickly encrypting virtual machine storage data without stealing information. This underscores the need for secure, off-site backups and a robust, layered security approach to detect and stop such threats early.

Recommendations

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Access Control and Least Privilege: Enforce the principle of least privilege, ensuring that users and applications have only the minimum access required to perform their functions. This limits the potential impact of a ransomware attack.

Conduct Regular Data Backups and Test Restoration: Regularly backup critical data and systems, storing them securely offline. Test restoration processes to ensure backup integrity and availability. In case of a ransomware attack, up-to-date backups enable recovery without paying the ransom.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement	TA0040 Impact
T1133 External Remote Services	T1078 Valid Accounts	T1046 Network Service Discovery	T1135 Network Share Discovery
T1021 Remote Services	T1021.001 Remote Desktop Protocol	T1021.002 SMB/Windows Admin Shares	T1570 Lateral Tool Transfer
T1003 OS Credential Dumping	T1003.003 NTDS	T1555 Credentials from Password Stores	T1110 Brute Force

T1110.004 Credential Stuffing	T1136 Create Account	T1136.001 Local Account	T1059 Command and Scripting Interpreter
T1059.003 Windows Command Shell	T1569 System Services	T1569.002 Service Execution	T1562 Impair Defenses
T1562.001 Disable or Modify Tools	T1550 Use Alternate Authentication Material	T1550.002 Pass the Hash	T1140 Deobfuscate/Decode Files or Information
T1070 Indicator Removal	T1070.004 File Deletion	T1486 Data Encrypted for Impact	T1490 Inhibit System Recovery
T1489 Service Stop			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	f7c8c60172f9ae4dab9f61c28ccae7084da90a06, 507b26054319ff31f275ba44ddc9d2b5037bd295, e1fb7d15408988df39a80b8939972f7843f0e785, 83f00af43df650fda2c5b4a04a7b31790a8ad4cf, 44a76b9546427627a8d88a650c1bed3f1cc0278c, eeafa71946e81d8fe5ebf6be53e83a84dcca50ba, 763499b37aacd317e7d2f512872f9ed719aacae1, 3477a173e2c1005a81d042802ab0f22cc12a4d55, 90be89524b72f330e49017a11e7b8a257f975e9a
Hostname	DESKTOP-7G1IC87, Kali, VPS65CCB8B75352, PACKERP-VUDV41R
Filename	readme.txt, DBgLog.sys, Veeam-Get-Creds.ps1, PSEXESVC.exe, netscan.exe
IPv4	5[.]230[.]33[.]176, 77[.]247[.]126[.]200, 107[.]161[.]50[.]26

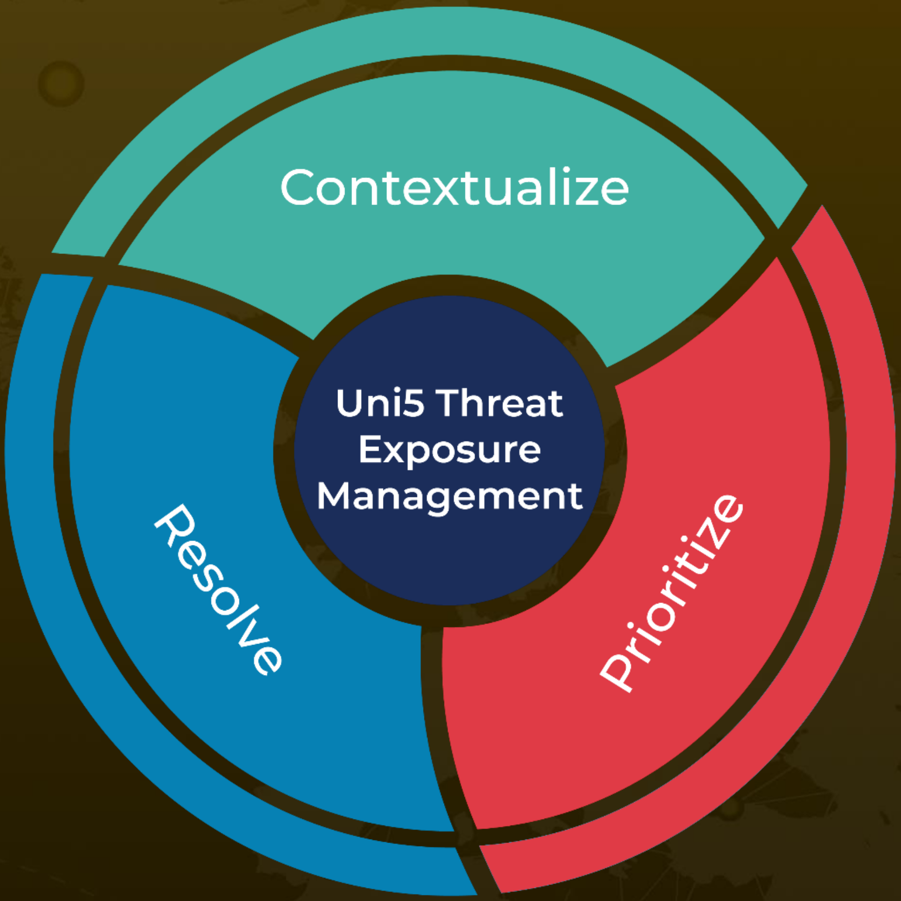
References

https://arcticwolf.com/resources/blog/lost-in-the-fog-a-new-ransomware-threat/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

June 10, 2024 • 7:30 AM

More at www.hivepro.com