Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

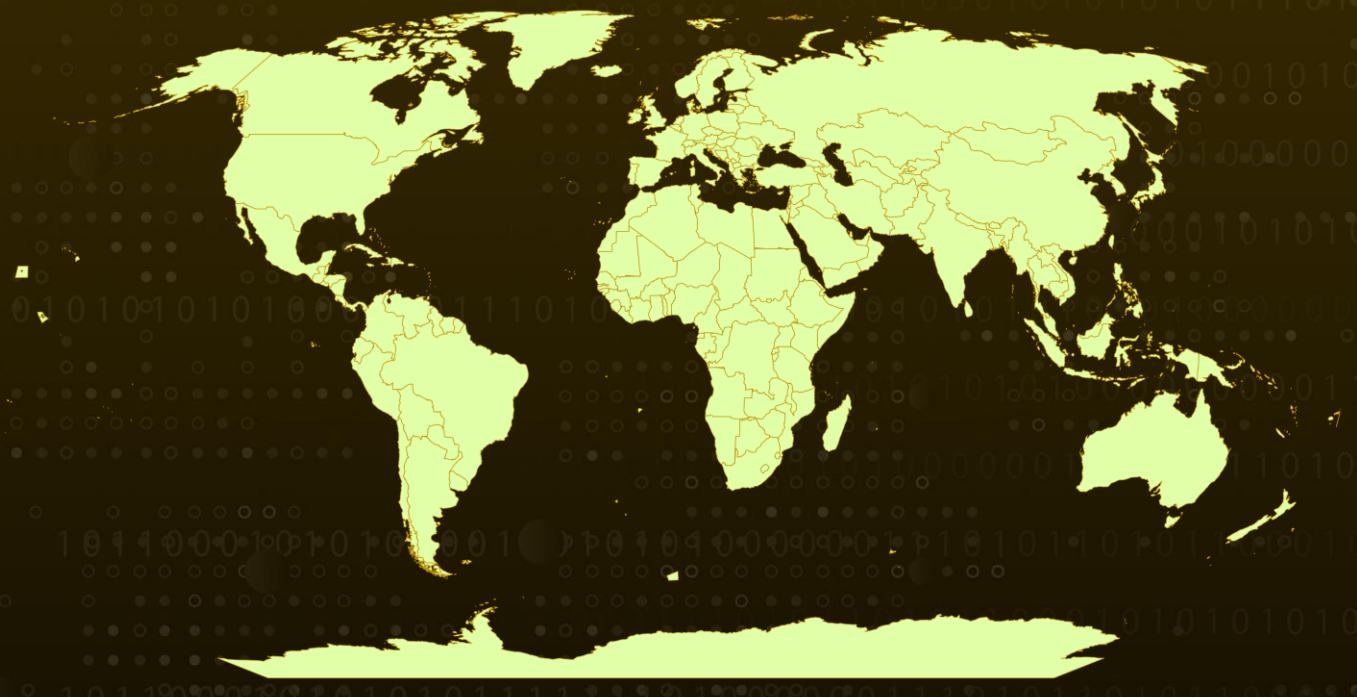
Fog Ransomware: A Growing Threat to the Financial Industry

Date of Publication	Admiralty Code	TA Number
September 10, 2024	A1	TA2024349

Summary

First Seen: May 2024
Targeted Countries: Worldwide
Malware: Fog ransomware (aka Lost in the Fog)
Targeted Industries: Finance
Affected Platforms: Windows and Linux
Attack: Fog Ransomware, previously targeting education and recreational sectors, has shifted its focus to the financial industry. It gains access through compromised VPN credentials, uses techniques like "pass-the-hash" to escalate privileges, and disables security before encrypting files and deleting backups. The attackers also exfiltrate sensitive data for double extortion, threatening to leak it if ransom demands aren't met. Fog's rapid evolution highlights its growing sophistication and expanded targeting strategies.

Attack Regions



Attack Details

#1 Fog ransomware is a newly emerged cyber threat that has been particularly targeting the U.S. education sector since its discovery in May 2024. This ransomware operation exploits compromised Virtual Private Network (VPN) credentials to gain initial access to networks, primarily in educational institutions, but it is also expanding its reach into other sectors, including financial services and recreation.

#2 The attackers use compromised VPN credentials, often obtained through credential theft or purchase from Initial Access Brokers. This allows them to bypass network defenses and gain entry into targeted environments.Once inside, Fog operators utilize techniques such as "pass-the-hash" attacks to escalate privileges, enabling them to access administrator accounts. They may also employ credential stuffing and custom scripts to extract passwords and maintain access to the network.

#3 After establishing a foothold, the ransomware is deployed, which involves disabling security measures like Windows Defender. Fog then encrypts files, particularly targeting Virtual Machine Disk (VMDK) files and deleting backups to prevent recovery. Encrypted files typically receive the extensions .FOG or .FLOCKED.

#4 Additionally, sensitive data is exfiltrated as part of a double-extortion scheme, where the attackers threaten to publish this data on a data leak site if the ransom is not paid. Ransom notes, usually named "readme.txt," are left in directories containing encrypted files, providing instructions for payment and a link to a Tor site for negotiations. Ransom demands can reach

#5 Since its emergence, Fog ransomware has shown a rapid evolution in its tactics and targeting strategies. Initially focused on educational institutions, it has begun to expand into more lucrative sectors, including financial services. This shift indicates a growing sophistication and ambition within the group behind Fog ransomware.

Recommendations

Strengthen Authentication: Implement multi-factor authentication (MFA) to protect against credential theft. Regularly rotate passwords for privileged accounts, especially for remote services like VPNs. Continuous monitoring of login attempts is essential to detect suspicious activity early.

Implement Robust Endpoint Protection: Deploy advanced endpoint protection solutions that include behavior-based detection, machine learning algorithms, and threat intelligence. These solutions can detect and block malicious activities associated with Fog ransomware, such as file encryption and unauthorized processes. Regularly update endpoint security software to ensure protection against the latest threats.

Patch and Update Software: Regularly apply security patches to systems, VPNs, and remote access services. Keeping software up-to-date helps close vulnerabilities that ransomware like Fog exploits for initial access.

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

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0042 Resource Development	TA0008 Lateral Movement	TA0040 Impact
TA0001 Initial Access	TA0002 Execution	TA0007 Discovery	TA0006 Credential Access
TA0011 Command and Control	TA0005 Defense Evasion	TA0010 Exfiltration	T1561 Disk Wipe

T1059 Command and Scripting Interpreter	T1555.003 Credentials from Web Browsers	T1555 Credentials from Password Stores	T1059.001 PowerShell
T1484.002 Domain Trust Modification	T1135 Network Share Discovery	T1078 Valid Accounts	T1046 Network Service Discovery
T1484 Domain Policy Modification	T1550.002 Pass the Hash	T1550 Use Alternate Authentication Material	T1595 Active Scanning
T1586 Compromise Accounts	T1047 Windows Management Instrumentation	T1486 Data Encrypted for Impact	T1561.001 Disk Content Wipe

Indicators of Compromise (IOCs)

TYPE	VALUE
File paths	C:\programdata\advanced_port_scanner_2.5.3869 (1).exe, C:\users\xxxxx\appdata\local\temp\advanced_port_scanner_2.5.3869 (1).tmp, C:\users\xxxxx\appdata\local\temp\advanced_port_scanner.exe C:\programdata\locker.exe, C:\Windows\System32\vssadmin.exe delete shadows /all /quiet, C:\ProgramData\SharpShares.exe
IPV4	85[.]209[.]11[.]227, 85[.]209[.]11[.]254, 85[.]209[.]11[.]27
File names	advanced_port_scanner_2.5.3869(1).exe, advanced_port_scanner_2.5.3869(1).tmp, advanced_port_scanner.exe, rclone.exe, locker.exe, vssadmin.exe, SharpShares.exe
TOR Address	Xql562evsy7njcsngacphc2erzjfecwotdkobn3m4uxu2gtqh26newid[.]onion

Recent Breaches

https://seawaymfg.com
https://ioigroup.com
https://ziba.com
https://hi-p.com
https://basf-nunhems.com
https://odessa.edu
https://www.wsutech.edu
https://www.gutech.edu.om
https://wawm.k12.wi.us
https://djgprojects.com
https://www.alvinisd.net
https://verweijelektrotechniek.nl
https://asburyseminary.edu
https://glc.vic.edu.au

References

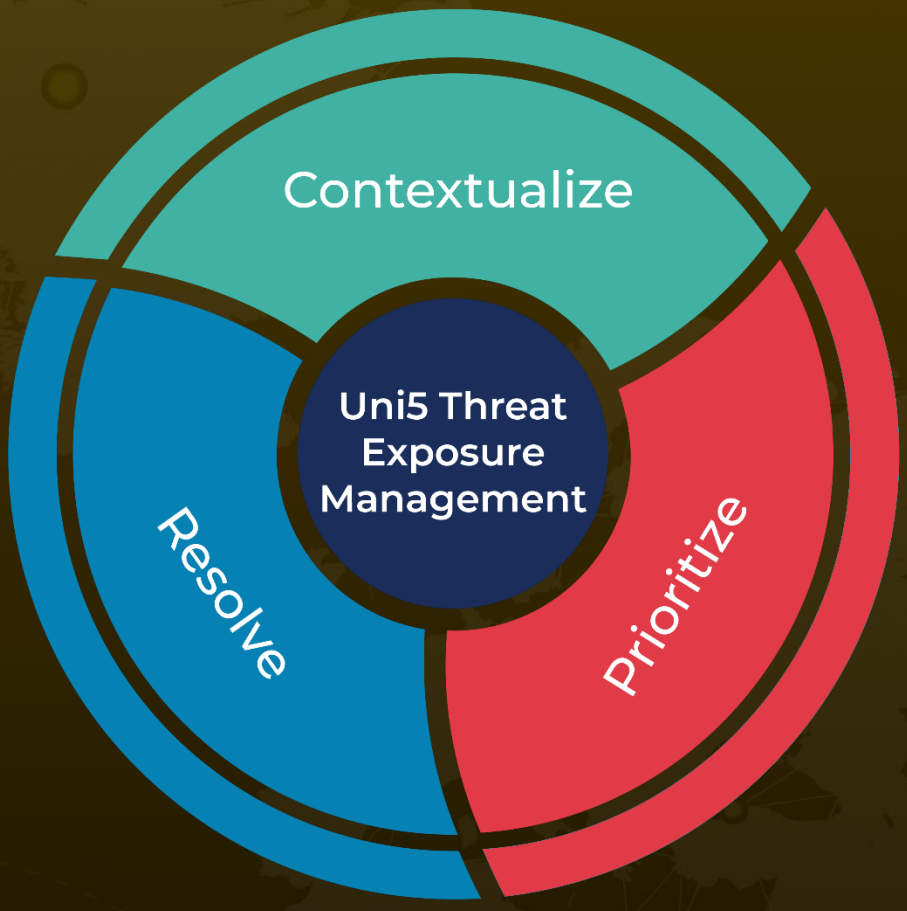
https://adlumin.com/post/fog-ransomware-now-targeting-the-financial-sector/

https://www.hivepro.com/threat-advisory/fog-ransomware-targets-us-sectors-via-compromised-vpn-credentials/

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

September 10, 2024 . 11:00 PM

More at www.hivepro.com