Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

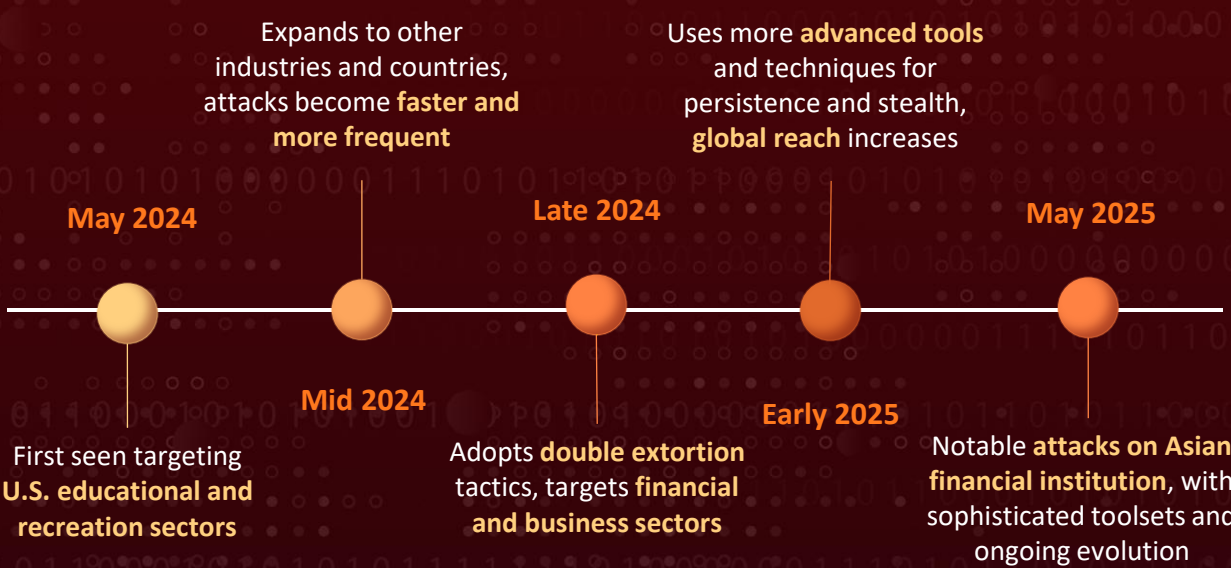
Fog Ransomware: From Financial Extortion to Covert Espionage

Date of Publication	Admiralty Code	TA Number
June 13, 2025	A1	TA2025188

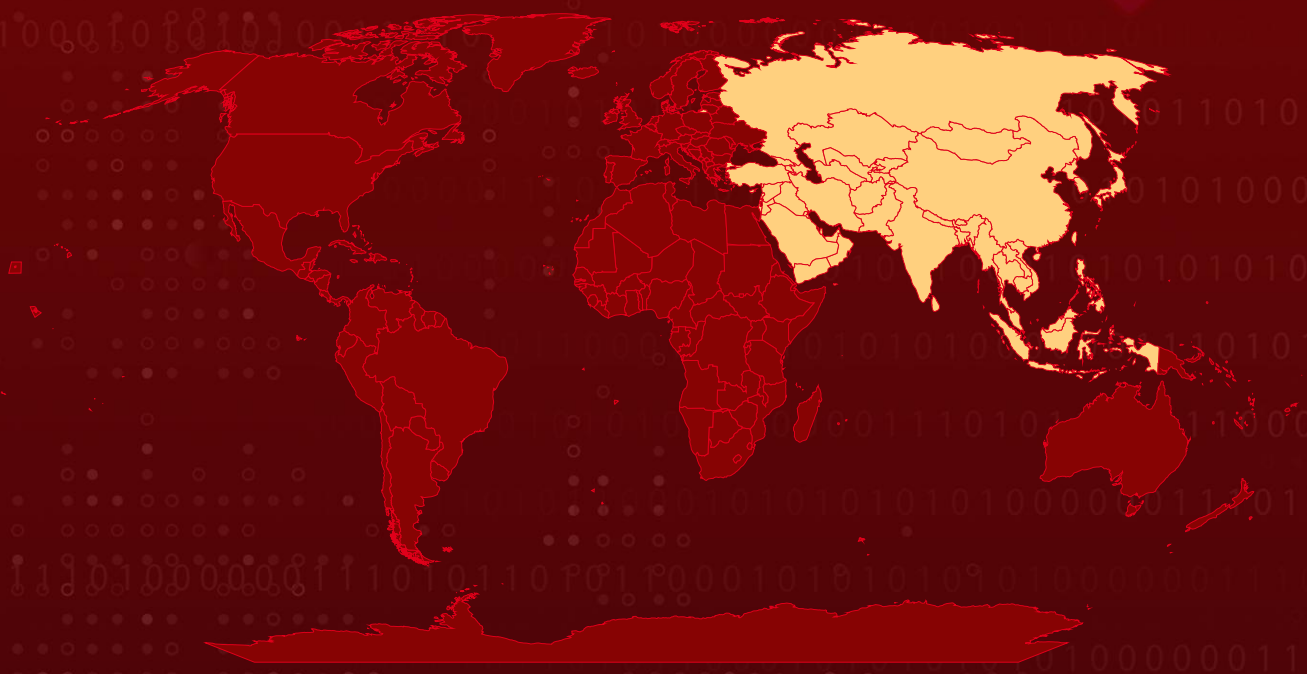
Summary

Attack Commended: May 2025
Targeted Region: Asia
Malware: Fog ransomware
Targeted Industry: Financial services
Targeted Platform: Windows
Attack: Fog ransomware recently struck an Asian financial institution, with attackers dwelling inside the network for about two weeks before deploying the ransomware and setting up a persistent service. The intrusion featured an unusual mix of legitimate monitoring software (Syteca/Ekran) and open-source pentesting tools like GC2, Adaptix C2, and Stowaway to stealthily harvest data and move laterally. Evolving since its emergence in May 2024, Fog now supports modular operations, enabling double-extortion and campaign customization, used by multiple actors sharing infrastructure. Its stealth, flexibility, and sophisticated toolkit underscore the critical need for robust patching, vigilant monitoring, and layered defenses.

Campaign Timeline



Attack Regions



Attack Details

#1

The recent Fog ransomware attack on an Asian financial institution marks a significant evolution in cybercriminal tactics. Unlike typical ransomware operations that prioritize quick encryption and ransom demands, this attack demonstrated a level of stealth and persistence more commonly associated with cyber-espionage. The attackers infiltrated the network and maintained access for approximately two weeks before deploying the ransomware payload, indicating deliberate planning and a broader set of goals beyond financial gain.

#2

A notable feature of this campaign was the use of legitimate and open-source tools to avoid detection. These included remote administration utilities like PsExec and SMBExec for lateral movement, and pentesting frameworks such as GC2 and Adaptix C2. However, what stood out most was the deployment of Syteca (formerly Ekran), an employee-monitoring tool used to record keystrokes and capture screen activity. This suggests the attackers were gathering intelligence or credentials before initiating the encryption phase, further supporting the espionage theory.

#3

The Fog ransomware group appears to be evolving rapidly. Initially observed in 2024 targeting educational institutions through stolen VPN credentials and exposed Veeam backup systems, they've since diversified their targets to include critical infrastructure sectors like finance and manufacturing. Their operations have matured, now incorporating double extortion techniques, stealing sensitive data in addition to encrypting it, and maintaining covert access to compromised systems even after deploying ransomware.

#4

Fog does not seem to be controlled by a single group; instead, it functions as a modular toolset used by multiple threat actors who share infrastructure and techniques. Its flexible design allows customization for each campaign, from the extent of encryption to the language of ransom notes. This adaptability, combined with opportunistic targeting and the use of advanced tools, underscores the urgent need for organizations across all sectors to strengthen defenses, patch vulnerabilities, and continuously monitor for suspicious activity.

Recommendations

Restrict access and patch systems: Grant administrative privileges sparingly and keep all security software up to date. Regularly scan for vulnerabilities and ensure endpoint protection can identify or block unknown malware.

Deploy Advanced Threat Detection and Response: Invest in real-time monitoring tools and EDR solutions that can detect obfuscated payloads, credential theft, and "living-off-the-land" techniques. Monitor for the use of uncommon tools like GC2, Adaptix C2, or Syteca, and flag unusual service creation or suspicious command-line activity.

Strengthen Email and Web Security: Deploy advanced email gateways and web filters to block phishing attempts, malicious links, and attachments that may deliver initial payloads. Educate employees to recognize social engineering tactics, such as fake software updates and deceptive IT support prompts

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 an Fog ransomware attack, up-to-date backups enable recovery without paying the ransom.

Potential MITRE ATT&CK TTPs

TA0010 Exfiltration	TA0040 Impact	TA0001 Initial Access	TA0002 Execution
TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command and Control
TA0003 Persistence	TA0005 Defense Evasion	T1027 Obfuscated Files or Information	T1082 System Information Discovery
T1059 Command and Scripting Interpreter	T1021.002 SMB/Windows Admin Shares	T1021 Remote Services	T1543.003 Windows Service
T1543 Create or Modify System Process	T1036 Masquerading	T1218 System Binary Proxy Execution	T1056 Input Capture
T1113 Screen Capture	T1056.001 Keylogging	T1018 Remote System Discovery	T1090 Proxy
T1486 Data Encrypted for Impact	T1490 Inhibit System Recovery		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	181cf6f9b656a946e7d4ca7c7d8a5002d3d407b4e89973ecad60cee028ae5afa, 90a027f44f7275313b726028eaaed46f6918210d3b96b84e7b1b40d5f51d7e85, f6cfd936a706ba56c3dcae562ff5f75a630ff5e25fcb6149fe77345afd262aab, fcf1da46d66cc6a0a34d68fe79a33bc3e8439affdee942ed82f6623586b01dd1,

TYPE	VALUE
SHA256	4d80c6fcd685961e60ba82fa10d34607d09dacf23d81105df558434f82d67a5e, 8ed42a1223bfaec9676780137c1080d248af9ac71766c0a80bed6eb4a1b9b4f1, e1f571f4bc564f000f18a10ebb7ee7f936463e17ebff75a11178cc9fb855fca4, f1c22cbd2d13c58ff9bafae2af33c33d5b05049de83f94b775cdd523e393ec40, 279f32c2bb367cc50e053fbd4b443f315823735a3d78ec4ee245860043f72406, b448321baae50220782e345ea629d4874cbd13356f54f2bbee857a90b5ce81f6, f37c62c5b92eecf177e3b7f98ac959e8a67de5f8721da275b6541437410ffae1, 3d1d4259fc6e02599a912493dfb7e39bd56917d1073fdba3d66a96ff516a0982, 982d840de531e72a098713fb9bd6aa8a4bf3ccaff365c0f647e8a50100db806d, fd9f6d828dea66ccc870f56ef66381230139e6d4d68e2e5bcd2a60cc835c0cc6, bb4f3cd0bc9954b2a59d6cf3d652e5994757b87328d51aa7b1c94086b9f89be0, ba96c0399319848da3f9b965627a583882d352eb650b5f60149b46671753d7dd, 44bb7d9856ba97271d8f37896071b72dfbed2d9fb6c70ac1e70247cddbd54490, 13d70c27dfa36ba3ae1b10af6def9bf34de81f6e521601123a5fa5b20477f277
IPv4	66[.]112[.]216[.]232, 97[.]64[.]81[.]119
Domain	amanda[.]protoflint[.]com

Recent Breaches

https://newtownfriends.org
https://rae.es
https://udmi.net
https://elcaminorealacademy.com
https://wilkinsonrogers.com
https://magnoliamanor.com
https://oberlin.net

https://wjccschools.org
https://about.gitlab.com
https://scolaro.com
https://baston.com.br
https://pampili.com.br
https://centralmcgowan.com
https://kleskmetalstamping.com
https://synelixis.com
https://gitlab.com
https://hagginoaks.com
https://hochschule-trier.de
https://gcasd.org
https://pamyra.de
https://about.gitlab.com
https://mozo-grau.com
https://vulsee.com
https://hess-gmbh.de
https://nd.edu.au
https://saintgeorge.cl
https://aurorak12.org
https://maxvytech.com
https://about.gitlab.com
https://econceptions.mobi
https://about.gitlab.com
https://su.se
https://karadenizholding.com

References

https://www.security.com/threat-intelligence/fog-ransomware-attack

https://blog.barracuda.com/2025/04/29/a-closer-look-at-fog-ransomware-

https://hivepro.com/threat-advisory/fog-ransomware-a-growing-threat-to-the-financial-industry/

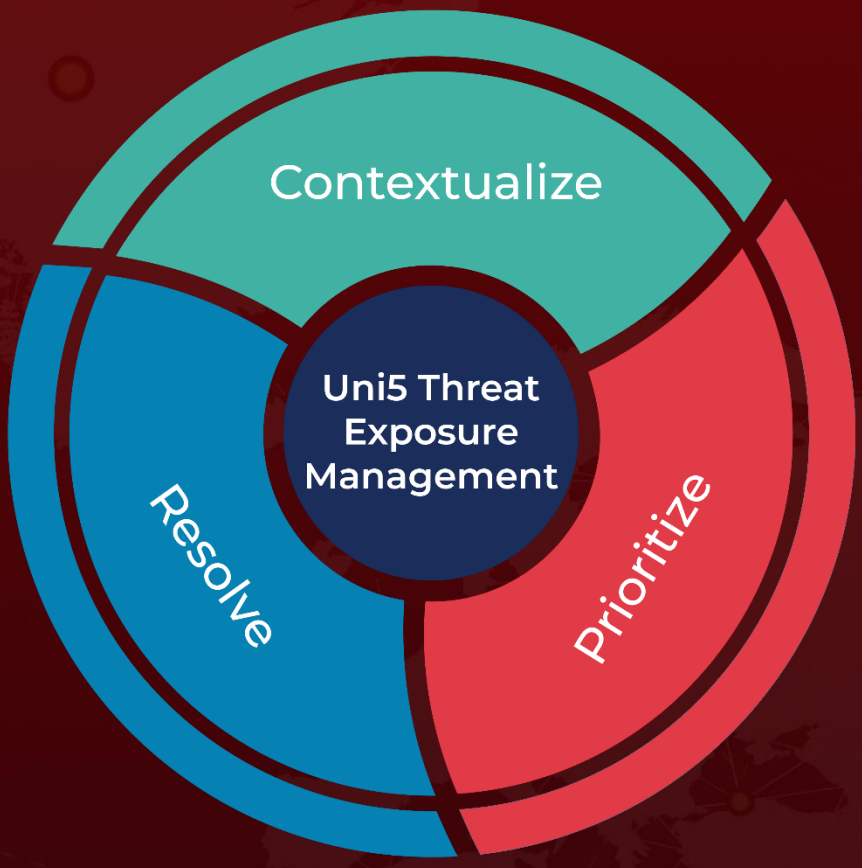
https://hivepro.com/threat-advisory/fog-ransomware-targets-us-sectors-via-compromised-vpn-credentials/

https://hivepro.com/threat-advisory/veeam-backup-replication-rce-flaw-opens-door-for-ransomware-attacks/

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 13, 2025 • 8:00 AM

More at www.hivepro.com