ESPIONAGE BEHIND ENCRYPTION? FOG RANSOMWARE HITS ASIAN FINANCIAL SECTOR WITH APT-LEVEL TACTICS

Vairav Security News Report

Date: June 16, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

In May 2025, a major financial institution in Asia fell victim to an advanced Fog ransomware campaign that has left cybersecurity experts questioning its true intent. According to the Symantec Threat Hunter Team, this attack deviated sharply from typical ransomware operations, showcasing tactics and tools more aligned with cyber-espionage than financial extortion.

CAMPAIGN HIGHLIGHTS

- **Ransomware Used:**

  First observed in May 2024, Fog attacked U.S. educational institutions via stolen VPN credentials. It evolved to exploit CVE-2024-40711 (Veeam) and later used phishing with Elon Musk-themed lures.

- **New Vector:**

  Fog was paired with advanced persistence and surveillance tools in the latest attack, including legitimate software typically used in corporate environments.

TOOLS USED

Tool/Tactics	Description
Syteca (Ekran)	Employee monitoring software is used for keylogging and screen captures. First known use in ransomware campaigns.
GC2 (Google C2)	Open-source backdoor leveraging Google Sheets/SharePoint for command execution and data theft. Previously seen in APT41 ops.
Adaptix C2 Agent	Lightweight and encrypted beaconing framework, a Cobalt Strike alternative.
Process Watchdog	Ensured persistence by restarting malware components like *AppxModels.exe*.
Living-off-the-Land	Tools like PsExec, SMBExec, FreeFileSync, 7-Zip, and MegaSync are used for lateral movement and data exfiltration.

ESPIONAGE INDICATORS

- **Persistence after Encryption:**

  Attackers created a Windows service **"**SecurityHealthIron**"** days *after* ransomware deployment — a highly unorthodox move in ransomware attacks.
- **Long-Term Access Tactics:**

  Tools and techniques to maintain a stealthy presence, not just immediate impact.
- **APT-style Tool Usage:**

  Especially GC2, linked to the Chinese state-sponsored group APT41.

ASSESSMENT & IMPLICATIONS

This campaign blurs the lines between financially motivated ransomware and nation-state cyber-espionage. The combination of dual-use tools, sophisticated persistence mechanisms, and stealth C2 channels points to a hybrid threat actor possibly seeking sensitive financial intelligence under the guise of a ransomware event.

INDICATORS OF COMPROMISE (IOCs)

File Hashes
181cf6f9b656a946e7d4ca7c7d8a5002d3d407b4e89973ecad60cee028ae5afa
90a027f44f7275313b726028eaaed46f6918210d3b96b84e7b1b40d5f51d7e85
f6cfd936a706ba56c3dcae562ff5f75a630ff5e25fcb6149fe77345afd262aab
fcf1da46d66cc6a0a34d68fe79a33bc3e8439affdee942ed82f6623586b01dd1
4d80c6fcd685961e60ba82fa10d34607d09dacf23d81105df558434f82d67a5e
8ed42a1223bfaec9676780137c1080d248af9ac71766c0a80bed6eb4a1b9b4f1
e1f571f4bc564f000f18a10ebb7ee7f936463e17ebff75a11178cc9fb855fca4
f1c22cbd2d13c58ff9bafae2af33c33d5b05049de83f94b775cdd523e393ec40
279f32c2bb367cc50e053fbd4b443f315823735a3d78ec4ee245860043f72406
b448321baae50220782e345ea629d4874cbd13356f54f2bbee857a90b5ce81f6
f37c62c5b92eecf177e3b7f98ac959e8a67de5f8721da275b6541437410ffae1
3d1d4259fc6e02599a912493dfb7e39bd56917d1073fdba3d66a96ff516a0982
982d840de531e72a098713fb9bd6aa8a4bf3ccaff365c0f647e8a50100db806d
fd9f6d828dea66ccc870f56ef66381230139e6d4d68e2e5bcd2a60cc835c0cc6
bb4f3cd0bc9954b2a59d6cf3d652e5994757b87328d51aa7b1c94086b9f89be0
ba96c0399319848da3f9b965627a583882d352eb650b5f60149b46671753d7dd
44bb7d9856ba97271d8f37896071b72dfbed2d9fb6c70ac1e70247cddbd54490
13d70c27dfa36ba3ae1b10af6def9bf34de81f6e521601123a5fa5b20477f277

C2		
66.112.216[.]232	*amanda[.]protoflint[.]com*	*97.64.81[.]119*

RECOMMENDATIONS

1. **Monitor Legitimate Tools**
   - Regularly audit for unauthorized use of monitoring tools like Syteca.
   - Use EDR to detect abuse of legitimate software for surveillance.
2. **Watch for Cloud-based C2**
   - Monitor unusual access to Google Sheets or SharePoint.
   - Use CASB tools to detect suspicious API or OAuth activity.
3. **Restrict LOLBins**
   - Block or monitor PsExec, SMBExec, and PowerShell via AppLocker or EDR.
   - Detect lateral movement and command execution attempts.
4. **Patch Critical Software**
   - Prioritize patching backup, VPN, and remote access systems.
   - Address known exploits like CVE-2024-40711.
5. **Detect Post-Infection Persistence**
   - Hunt for unusual service creation or registry changes after ransomware deployment.
   - Monitor scheduled tasks and unknown binaries.
6. **Isolate Backups**
   - Use offline or immutable backups and test recovery processes regularly.
   - Segment networks to protect critical systems.
7. **Update IR Plans**
   - Prepare for hybrid attacks blending ransomware and espionage.
   - Run tabletop exercises with multi-phase threat scenarios.

REFERENCES

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

https://securityonline.info/ransomware-or-espionage-fog-ransomware-attack-in-asia-raises-suspicion-with-rare-toolset/

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com