Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

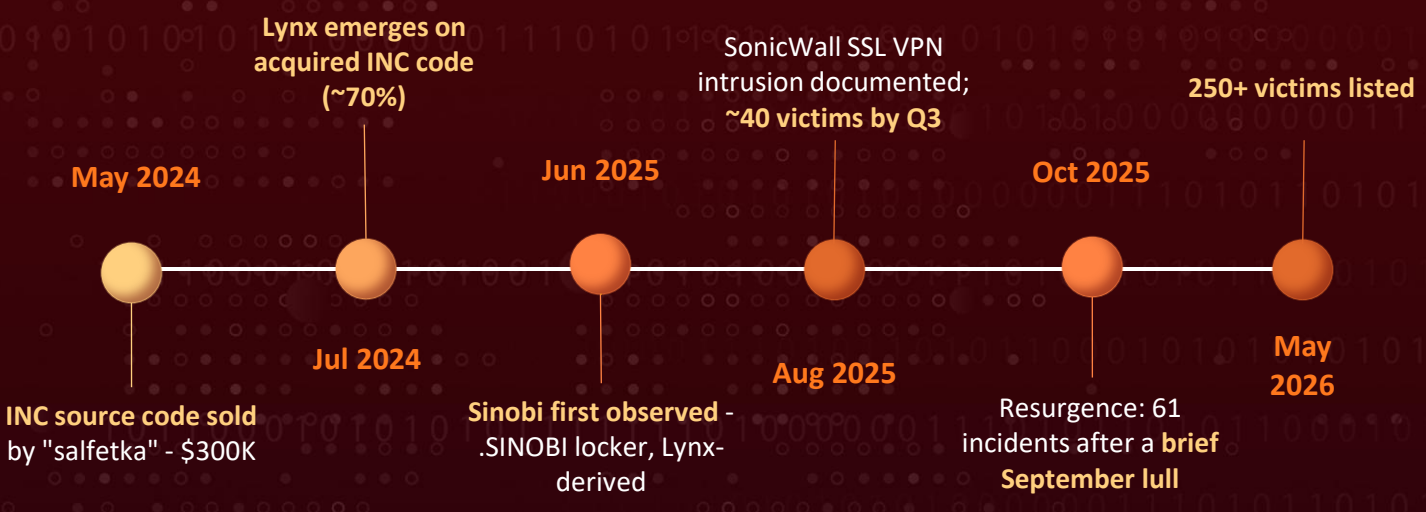
Sinobi Ransomware: A Fast-Rising Mid-Market Threat to Watch in 2026

Date of Publication	Admiralty Code	TA Number
June 16, 2026	B2	TA2026169

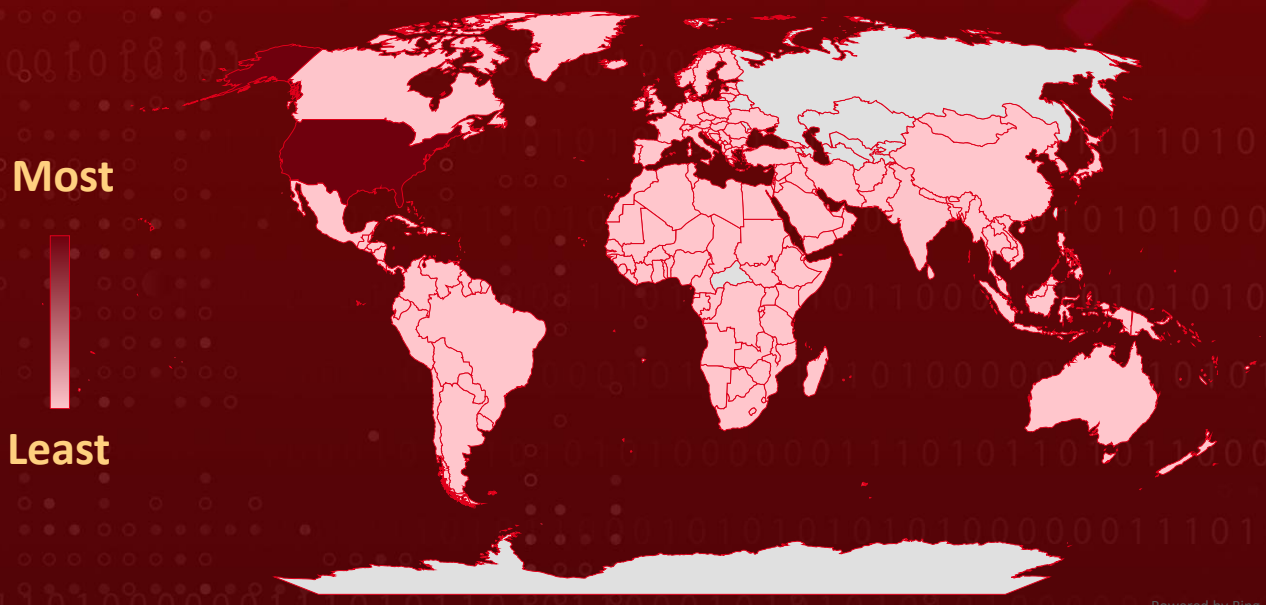
Summary

First Active: Late June 2025
Targeted Regions: Global, primarily the United States (Except CIS countries)
Targeted Platform: Windows
Targeted Industries: Manufacturing, Construction, Healthcare, Technology, Business Services, Financial Services, Consumer Services, Agriculture and Food Production, Energy, Hospitality and Tourism, Education
Malware: Sinobi Ransomware
Attack: Sinobi is a financially motivated, closed vetted-affiliate ransomware-as-a-service operation that emerged in late June 2025 and is assessed with medium confidence as a rebrand or successor of Lynx (itself INC-derived). It gains access primarily through compromised SonicWall SSL VPN credentials and over-privileged accounts, removes EDR, and exfiltrates data with RClone and WinSCP before deploying a Curve25519/AES-128-CTR locker that deletes shadow copies and appends .SINOBI, enforcing double extortion via a 7-day ransom deadline. Targeting mid-to-large US organizations in manufacturing, construction, healthcare, and professional services, Sinobi has scaled rapidly to 250+ leak-site victims by May 2026, and given its inherited tooling maturity and recovery-inhibition tradecraft should be treated as a serious mid-market threat through 2026.

Ransomware Timeline



Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-53704	SonicWall SonicOS SSLVPN Improper Authentication Vulnerability	SonicWALL NSv devices, SonicWall SSLVPN	✗	✓	✓
CVE-2024-40766	SonicWall SonicOS Improper Access Control Vulnerability	SonicWall SonicOS	✗	✓	✓

Attack Details

#1

Sinobi is a financially motivated ransomware operation that emerged in late June 2025, running a closed, vetted-affiliate Ransomware-as-a-Service model in which a core team maintains the encryptor, infrastructure, and negotiation/leak portals while a small set of screened affiliates conduct intrusions. Code and data-leak-site overlaps support a medium-confidence assessment that Sinobi is a rebrand or successor of Lynx, which is itself INC-derived. The genealogy traces to early May 2024, when INC ransomware source code was offered for sale on Russian-speaking forums by the actor "salfetka" for $300,000; Lynx is widely suspected to have acquired it, with Sinobi the later evolution. Despite shinobi branding, consistent avoidance of Russia/CIS victims points to Russian or Eastern-European cybercrime rather than a state actor.

#2

Initial access in the primary first-party incident came through compromised third-party MSP SonicWall SSL VPN credentials mapped to an over-privileged domain-administrator account, enabling RDP into a file server. Secondary trackers additionally attribute Sinobi access to exploitation of CVE-2024-53704 (SSL VPN authentication bypass) and CVE-2024-40766 (improper access control), the latter a credential-carryover flaw exploited by multiple ransomware groups. Phishing and initial-access-broker credentials are also reported vectors.

#3

After entry, operators create rogue local/domain-administrator accounts, move laterally via RDP and shared mounts, and remove EDR (observed: Carbon Black uninstalled from the file server). Data is exfiltrated before encryption using RClone and WinSCP to cloud storage, establishing double-extortion leverage.
The encryptor pairs Curve25519 with AES-128-CTR, generating a per-file key via CryptGenRandom, meaning no cryptographic shortcut to decryption exists. It empties the Recycle Bin, deletes volume shadow copies through a low-level DeviceIoControl resize, optionally terminates backup/database/mail processes, appends .SINOBI, and writes a README.txt note with Tor negotiation links and a 7-day deadline, then replaces the desktop wallpaper.

#4

Targeting skews to mid-to-large organizations with $10–50 million annual revenue, with the vast majority of victims in the United States. The top 2025 vertical was Manufacturing, followed by Construction, Healthcare, Technology and Business Services. Given Sinobi's inherited tooling maturity, rapid victim accumulation, credential-led intrusion model, and recovery-inhibition tradecraft, organizations should treat the group as a serious, mid-market-focused threat through 2026.

Recommendations

Eliminate Over-Privileged Remote-Access Identities: Sinobi's primary documented intrusion abused a third-party MSP's SonicWall SSL VPN credentials tied to a domain-administrator account, enabling immediate RDP to a file server. Strip domain and local admin rights from all VPN and remote-access identities, enforce strict tiering of administrative accounts, and treat MSP/third-party credentials as in-scope for continuous monitoring and least-privilege review.

Enforce MFA and Patch SonicWall SSL VPN: Apply MFA across all SonicWall SSL VPN, RDP, and privileged accounts, and patch CVE-2024-40766 and CVE-2024-53704. Because CVE-2024-40766 is a credential-carryover flaw from Gen 6 to Gen 7 firewall migrations, reset all local SSL VPN account passwords that were imported during migration rather than relying on patching alone.

Enable EDR Tamper Protection: Sinobi affiliates uninstalled Carbon Black from the file server, with the deregistration code suspected to have been stored on an accessible network share. Enable anti-tamper and anti-uninstall protections on all endpoint agents, alert on EDR service reconfiguration and removal (e.g. sc config <edr_service> start= disabled), and never store EDR uninstall or deregistration codes on file shares or mapped drives.

Monitor Account-Creation and Privilege-Escalation Sequences: Operators created a rogue local account and elevated it into local Administrators and Domain Admins for lateral movement. Alert on the net user … /add followed by net localgroup "domain admins" … /add sequence from a single session, restrict net, net localgroup, and sc config execution from non-administrative hosts, and monitor RDP and network-share access between internal systems.

Maintain Offline, Immutable Backups: Sinobi's encryptor empties the Recycle Bin and deletes volume shadow copies through a low-level DeviceIoControl resize, removing local recovery options before encryption. Maintain offline, immutable backups, monitor VSS health, alert on programmatic shadow-copy deletion, and regularly test restoration against this encryptor's recovery-destruction behavior to ensure recovery without paying the ransom.

Constrain Exfiltration and Prepare for Double Extortion: Data is staged and exfiltrated using RClone and WinSCP to cloud storage before encryption, establishing leak-site leverage. Apply egress monitoring and controls for RClone, WinSCP, and bulk transfers to unfamiliar hosting ASNs, and update incident response playbooks to account for data-leak pressure and 7-day ransom deadlines during active negotiations.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1133: External Remote Services	
	T1078: Valid Accounts	T1078.002: Domain Accounts
	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	T1059.003: Windows Command Shell
Persistence	T1136: Create Account	T1136.001: Local Account
	T1543: Create or Modify System Process	T1543.003: Windows Service
Privilege Escalation	T1134: Access Token Manipulation	
	T1098: Account Manipulation	
Defense Evasion	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
Discovery	T1082: System Information Discovery	
	T1057: Process Discovery	
	T1083: File and Directory Discovery	
	T1135: Network Share Discovery	

Tactic	Technique	Sub-technique
Discovery	T1120: Peripheral Device Discovery	
	T1087: Account Discovery	
Lateral Movement	T1021: Remote Services	T1021.001: Remote Desktop Protocol
		T1021.002: SMB/Windows Admin Shares
Credential Access	T1003: OS Credential Dumping	
Collection	T1005: Data from Local System	
Command and Control	T1090: Proxy	T1090.003: Multi-hop Proxy
Exfiltration	T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage
Impact	T1486: Data Encrypted for Impact	
	T1489: Service Stop	
	T1490: Inhibit System Recovery	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	1b2a1e41a7f65b8d9008aa631f113cef36577e912c13f223ba8834bbefa4bd14, 676dc8e28c90e64000a998ec257c014cb1152e7a5bdccab3916d8fba401853da, 9432b065c803baa54f1fefac20d97affce212dec2bb9a597fc010064d391fc24, 8bb8c6e72d20e9b07bb55e0b0d168efe99d0088122131ae96d13fa01d3325a17, 82cd0af26bc1e9e3b0bfcfe6c61cf467992367a31d87e6bd7e2efa8e9fecbb25, d4919a7402d7ae02516589fbdfb3cc436749544052843a37b5d36ac4b7385b18
SHA1	3ebf5f01ac8ca704f4ab9e12acd11139f3ff838f, 2101541061fb52b178165e7ef22244ec42601aea, 3055b209cfdd3bd297029ef4270b77b50f76dc03, 86233a285363c2a6863bf642deab7e20f062b8eb
File Path	c:\programdata\rclone-ssh.conf, C:\programdata\bin.exe, %TEMP%\background-image.jpg, README.txt
Registry Key	HKCU\Control Panel\Desktop\Wallpaper
File Extension	.SINOBI
Tor Domain	sinobi6ftrg27d6g4sjdt65malds6cfptlnjyw52rskakqjda6uvb7yd[.]onion, sinobi6rlec6f2bgn6rd72xo7hvds4a5ajiu2if4oub2sut7fg3gomqd[.]onion, sinobi6ywgmmvg2gj2yygkb2hxbimaxpqkyk27wti5zjwhfcldhackid[.]onion, sinobi7l3wet3uqn4cagjiessuomv75aw3bvgah4jpj43od7xndb7kad[.]onion, sinobi7sukclb3ygtorysbtrodgdbnrmgbhov45rwzipubbzhiu5jvqd[.]onion, sinobi23i75c3znmqqxxyuzqvhxnjsar7actgvc4nqeuhgcn5yvz3zqd[.]onion, sinobia6mw6ht2wcdjphessyzpy7ph2y4dyqbd74bgobgju4ybytmkqd[.]onion,

TYPE	VALUE
Tor Domain	sinobi7yuoppj76qnkwiobwfc2qve2xkv2ckvzyyjblwd7ucpptl62ad[.]onion/login, sinobi57mfegeov2naiufkidlkpze263jtbldokimfjqmk2mye6s4yqd[.]onion/login, sinobibjqytwqxjw24zuerqcjyd3hoow6zia7z6kzvwawivamu7nqayd[.]onion/login, sinobicrh73ongfuxjajmlyyhalvkhlcgttxkxaxz3gvsgdcgf76uiqd[.]onion/login

Recent Breaches

https://www.neurotrials.com
https://www.scalesassoc.com
https://www.elgielectric.com
https://www.ourams.com
https://www.summaenergy.com
https://www.interpacknorthwest.com
https://www.ecosoundbuilders.com
https://www.mcafeetool.com
https://www.teco.com
https://www.gentegra.com
https://www.graymatter.com
https://www.iblesoft.com
https://www.saltechsystems.com
https://www.electriduct.com
https://www.mayfairhotels.com
https://www.halcyontechnologies.com
https://www.bcsprosoft.com
https://www.sundhergroup.com
https://www.venesco.com
https://www.snyderdiamonds.com
https://www.halcyontek.com
https://www.accountnet.com
https://www.pennfencing.com
https://www.exco.com
https://www.infomontreal.com
https://www.wsiron.com
https://www.reillyfoam.com

Patch Links

CVE-2024-53704: https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0003

CVE-2024-40766: https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015

References

https://www.esentire.com/blog/threat-actors-deploy-sinobi-ransomware-via-compromised-sonicwall-ssl-vpn-credentials

https://www.picussecurity.com/threat-database/how-sinobi-ransomware-encrypts-files-and-destroys-backups

https://www.halcyon.ai/threat-group/sinobi

https://darkwebsonar.io/blog/dark-web-most-wanted-2025-sinobi/

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 Demo of **HivePro**.

REPORT GENERATED ON

June 16, 2026 • 06:30 AM

More at www.hivepro.com