Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

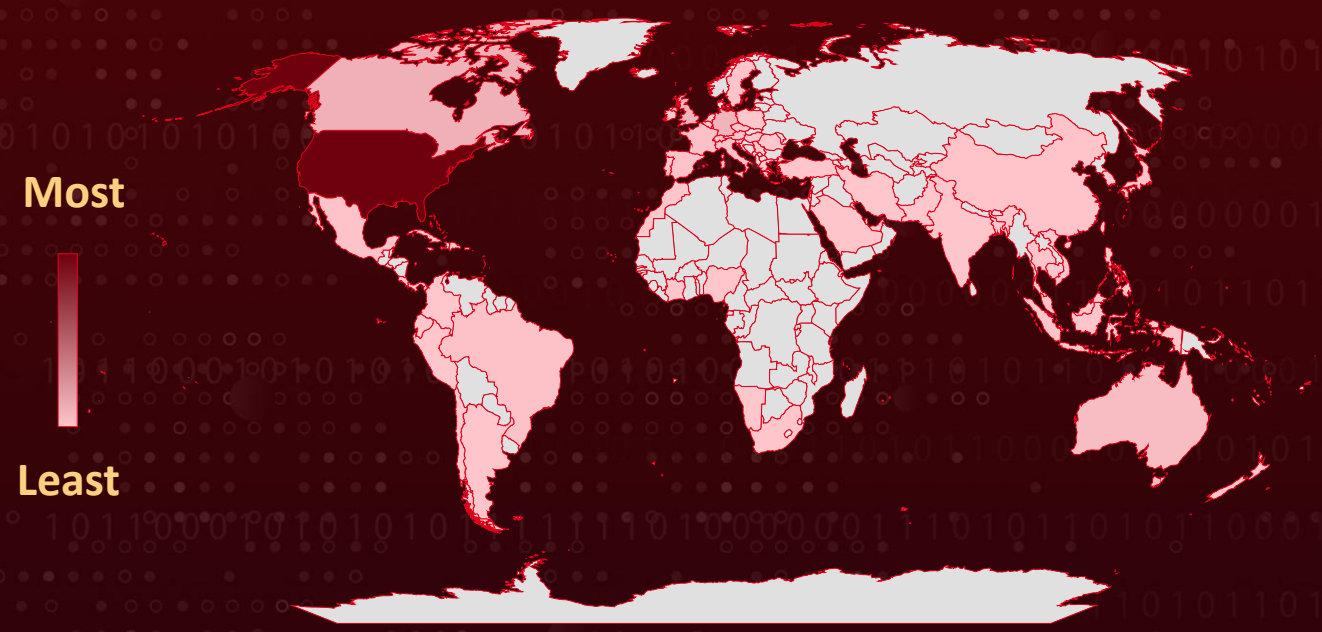
INC Ransomware: Rust-Based RaaS Exploiting Public-Facing Edge Devices

Date of Publication	Admiralty Code	TA Number
July 17, 2026	A1	TA2026203

Summary

First Seen: July 2023
Targeted Regions: Global (Except CIS countries)
Targeted Platforms: Windows, Linux, VMware ESXi
Targeted Industries: Manufacturing, Legal, Healthcare, Business Services & Consulting, Financial Services, Retail, Charitable Organizations, Government, Transportation, Technology, Education, Real Estate, Agriculture, Pharmaceutical, Energy, Telecommunications, Associations, Media, Aerospace, Defense, Insurance, Religion, Hospitality, Aviation, Food Service
Malware: INC ransomware (aka GOLD IONIC, G1032)
Attack: INC is a Rust-based ransomware-as-a-service operation (aka GOLD IONIC) that has claimed 800+ victims since 2023 and ranks among 2026's most active groups, hitting legal, manufacturing, healthcare, technology, and construction targets predominantly in the US. Operators gain entry via unpatched edge appliances (notably CVE-2023-3519 and CVE-2023-48788) or broker-supplied credentials, then use living-off-the-land binaries and a modified Veeam credential dumper to move laterally across Windows, Linux, and ESXi. Data is exfiltrated to attacker cloud storage before double-extortion encryption, with aggressive defense impairment via driver-dropping process killers and shadow-copy deletion. Pressure is applied through a Tor negotiation portal, a public leak site, wallpaper defacement, and ransom notes printed to networked printers.

Attack Regions



© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-3519	Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	✓	✓	✓
CVE-2023-48788	Fortinet FortiClient EMS SQL Injection Vulnerability	Fortinet FortiClient EMS	✗	✓	✓
CVE-2024-57727	SimpleHelp Path Traversal Vulnerability	SimpleHelp Remote Support Software	✗	✓	✓
CVE-2025-5777	CitrixBleed 2 (Citrix NetScaler Gateway Out-of-Bounds Read Vulnerability)	Citrix NetScaler ADC and NetScaler Gateway	✓	✓	✓

Attack Details

#1

INC Ransom is a Ransomware-as-a-Service (RaaS) operation that emerged in July 2023, also tracked under the alias GOLD IONIC. It established itself as a semi-private, affiliate-based operation rather than a rebrand, and by 2026 matured into a top-tier operator, with more than 800 victims claimed since 2023. Its rise was opportunistic, the disruption of LockBit and shutdown of BlackCat pushed affiliates and tooling toward INC.

#2

The group's ecosystem influence is distinctive. In May 2024 the source code was listed on underground forums for $300,000; shortly after, the Lynx operation emerged with substantial code overlap, and Sinobi later appeared, the original brand continues to operate while its codebase propagates into adjacent families. Victimology is US-centric: the United States accounts for 60% of victims, with a long tail led by Australia, Canada, and Germany, and a complete absence of CIS-region victims, suggesting CIS-based operators. The 2026 top five sectors are legal services, manufacturing, technology, healthcare, and construction, a shift away from the earlier education focus.

#3

The attack chain favors known techniques. Initial access comes via spear-phishing, IAB credentials, and public-facing exploits, CVE-2023-3519 (Citrix NetScaler), CVE-2023-48788 (Fortinet EMS), CVE-2024-57727 (SimpleHelp), and CVE-2025-5777 (Citrix Bleed 2). A modified Veeam credential dumper upgraded for salted-DPAPI, RDP/PsExec lateral movement, a BYOVD process terminator that drops vulnerable drivers, remote-access tooling for C2, and 7-Zip plus rclone exfiltration round out the toolkit.

#4

Both payloads are now Rust-based. The Windows encryptor deletes shadow copies, uses a hybrid Salsa20/AES scheme with Curve25519 ECC, and appends a .INC extension. The Linux/ESXi variant supports --esxi (VM shutdown via vim-cmd), --motd, --daemon, and fast/medium/slow modes, deriving per-file AES-128-CTR keys via X25519 ECDH. Extortion is double-sided, a credentialed negotiation site plus a public leak site, combined with wallpaper hijacking, INC-README notes, and automated network printing of ransom notes.

Recommendations

Patch Exploited Edge Appliances: Prioritize remediation of the internet-facing vulnerabilities tied to INC intrusions, CVE-2023-3519 (Citrix NetScaler ADC/Gateway), CVE-2023-48788 (Fortinet FortiClient EMS), CVE-2024-57727 (SimpleHelp RMM), and CVE-2025-5777 (Citrix Bleed 2), and maintain a vulnerability management program that fast-tracks fixes for flaws known to be exploited by ransomware operators.

Harden and Monitor Remote Access: Restrict RDP and SSH exposure from the internet, harden and monitor external remote services, and enforce multifactor authentication on all remote and privileged access points to blunt the value of broker-supplied and stolen credentials.

Protect Veeam and Backup Infrastructure: Isolate backup servers, apply least-privilege service accounts, and monitor for base64-encoded PowerShell execution and unauthorized SQL queries against Veeam credential stores that indicate use of the modified Veeam-Get-Creds credential dumper.

Enforce Strong Identity Controls: Require complex, regularly rotated alphanumeric passwords, watch for the creation of new privileged accounts, and alert on off-hours authentication and anomalous administrative activity.

Maintain Offline, Immutable Backups: Follow the 3-2-1 backup rule with at least one offline or immutable copy stored off-site under separate credentials, and routinely test restoration to ensure recovery without paying a ransom.

Deploy Anti-Tamper EDR: Run endpoint detection and response with behavioral detection and anti-tamper protections enabled, and monitor for driver-based process termination (including the vulnerable drivers filwfp.sys, filnk.sys, and fildds.sys), Volume Shadow Copy deletion, and safe-mode boot manipulation.

Monitor Living-off-the-Land and RMM Tooling: Alert on suspicious use of PsExec, WMIC, net, and network scanners such as Advanced IP Scanner and netscan, and inventory or restrict unsanctioned remote management tools including AnyDesk, ScreenConnect, and TeamViewer.

Detect Staging and Exfiltration: Watch for 7-Zip archiving of large data sets and outbound transfers via rclone or MegaSync to cloud storage such as Mega.nz, and block or closely monitor access to unsanctioned file-sharing services.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
	T1566: Phishing	T1566.001: Spearphishing Attachment
	T1078: Valid Accounts	
Execution	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.003: Windows Command Shell
Persistence	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1136: Create Account	
Privilege Escalation	T1078: Valid Accounts	
Defense Evasion	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
		T1562.009: Safe Boot Mode
	T1070: Indicator Removal	
Credential Access	T1003: OS Credential Dumping	

Tactic	Technique	Sub-technique
Discovery	T1046: Network Service Scanning	
	T1057: Process Discovery	
	T1087: Account Discovery	
Lateral Movement	T1021: Remote Services	T1021.001: Remote Desktop Protocol
		T1021.002: SMB/Windows Admin Shares
Command and Control	T1219: Remote Access Software	
Collection	T1560: Archive Collected Data	T1560.001: Archive via Utility
Exfiltration	T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage
Impact	T1486: Data Encrypted for Impact	
	T1490: Inhibit System Recovery	
	T1491: Defacement	T1491.001: Internal Defacement
	T1529: System Shutdown/Reboot	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	31800380c359143ae82c4f9011eee653dd22443d03d6a499148203bbfc275502, ea721240c14e3d14f8d88e0020880448c6c602f1180a1e5dbe40871cfeedcc22, 8d1a22c430252f29611766b8e4a82af0fba60d609246463466b384d6d4793df4, bf8c45e5aa9551a17eefbd1d179422c32b4309c47ee9a3f315bb80ed6d4f7efc, 6bf155b269d452f3c3b62832b27bbebe4da436e228dbf521155b1d5989e3743f, 1898d056463284d849801cbdea6a3dec6c9f568f01569912c3868a5eea9a5449, 24f6c0ca39b2a5593086ff56d818ddfbde121f8e44d54faa762e510397dc9db7, dc9938f51150d13a69fc25f3f19052eacb1bf0a086fd5cf39762501fb3ddd7da, acce811c4fc2a6e3fddd4231e386f1648ca44f039d2d275316bc0a0fc96e0af4, 90e46e89fec2108a1cb4850bb33e3563e92a14d04e1e613ac8c9311f152d294c, ff5da8f0330a4c581c37284c74aae2683c007dc6e406e1e2e6803e7bb398b77b, 97aebda5482899fef84a24e456bff055acaa47e5ab4029f768d9e0c62a660ce2, 1d10d8f5a420d0e4683b4cb40bcf0c984d1e7ea1f3b4442a00a525584632ac11, f6a01d0246ce31faf6938ea488086d4358505405a4ef5c5faa482e79e92cb347, d65120291dee76c694f8bea54841f7f68329b499b28f4aee5ea5c9369a7432cb, 765508aa2ec6a1b73a76a23f4fa559d32355622748c91a46ed7b315eae2ee60a, d26bfb0147f60dc6500a9298d521ee67b49daaf4b8f8be54e7cc8fd86a597570

TYPE	VALUE
SHA256	589d9480fbfec2d8e61638eb0b537183d0f9977411fd1d2c0f8eb611feebe880, 7f37351979c249417cb180b4ede0ed17e5fe2a1f08add4d72606b589f8fdb245, 5cc212f84d2bf3fbab165aaf09b16e00fcf2f1ccd880d24b14404c53dcdbf241, 60aeb9f7bccf377ff02ed64783e66a62c0f976878d9729b067bc7e5b0b9da9d6, 6cd349eda0fa6c8b274a0920852c68f8b727afea1fdbc69ad183cef05d9cf141
Domains	incblog[.]su, Incbackend[.]top, Incapt[.]blog
TOR Addresses	incblog6qu4y4mm4zvw5nrmue6qbwtgjsxpw6b7ixzssu36tsajldoad[.]onion, incpaykabjqc2mtdxq6c23nqh4x6m5dkps5fr6vgdkgzp5njssx6qkid[.]onion, incblog7vmuq7rktic73r4ha4j757m3ptym37tyvifzp2roedyyzzxid[.]onion, incbackrlasjesgpfu5brktfjknbqoahe2hhmqfhasc5fb56mtukn4yd[.]onion, incbacg6bfwtrlzwdbqc55gsfl763s3twdtwhp27dzuik6s6rwdcityd[.]onion
Filenames	INC-README.txt, INC-README.html, ipscan.exe, Advanced_IP_Scanner_2.5.3850.exe, netscan.exe, pskill.exe, ProcessTerminator.exe, filwfp.sys, filnk.sys, fildds.sys, Veeam-Get-Creds.ps1
File Paths	C:\Program Files\Angry IP Scanner\ipscan.exe, C:\ProgramData\VMware\libsm2\netscan.exe

Patch Links

CVE-2023-3519:
https://support.citrix.com/supporthome/kbsearch/article?articleNumber=CTX561482

CVE-2023-48788: https://fortiguard.fortinet.com/psirt/FG-IR-24-007

CVE-2024-57727: https://guides.simple-help.com/kb---security-vulnerabilities-01-2025#security-vulnerabilities

CVE-2025-5777: https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX693420

Recent Breaches

https://www.kyokuto.com/en/
https://www.statebankofnauvoo.com/
https://asa-international.com
https://oakparkmi.gov
https://samberger24.de
https://tecnocurva.com.br
https://carvalima.com.br
https://tricountyhs.org
https://ezortea.com.br
https://tambasa.com
https://hamilton-eye.com
https://acworth-ga.gov
https://www.roundshield.com/

References

https://www.acronis.com/en/tru/posts/from-emerging-threat-to-top-tier-ransomware-as-a-service-the-evolution-of-inc-ransomware/

https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/inc-ransom-group-detection-and-prevention/

https://www.bitsight.com/underground/threat-actors/inc-ransom

https://www.rescana.com/post/inc-ransomware-incident-analysis-exploiting-citrix-netscaler-and-fortinet-vulnerabilities-through-double-extortion-attac

https://www.fortiguard.com/threat-actor/6333/inc-ransomware

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

July 17, 2026 • 09:40 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com