Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

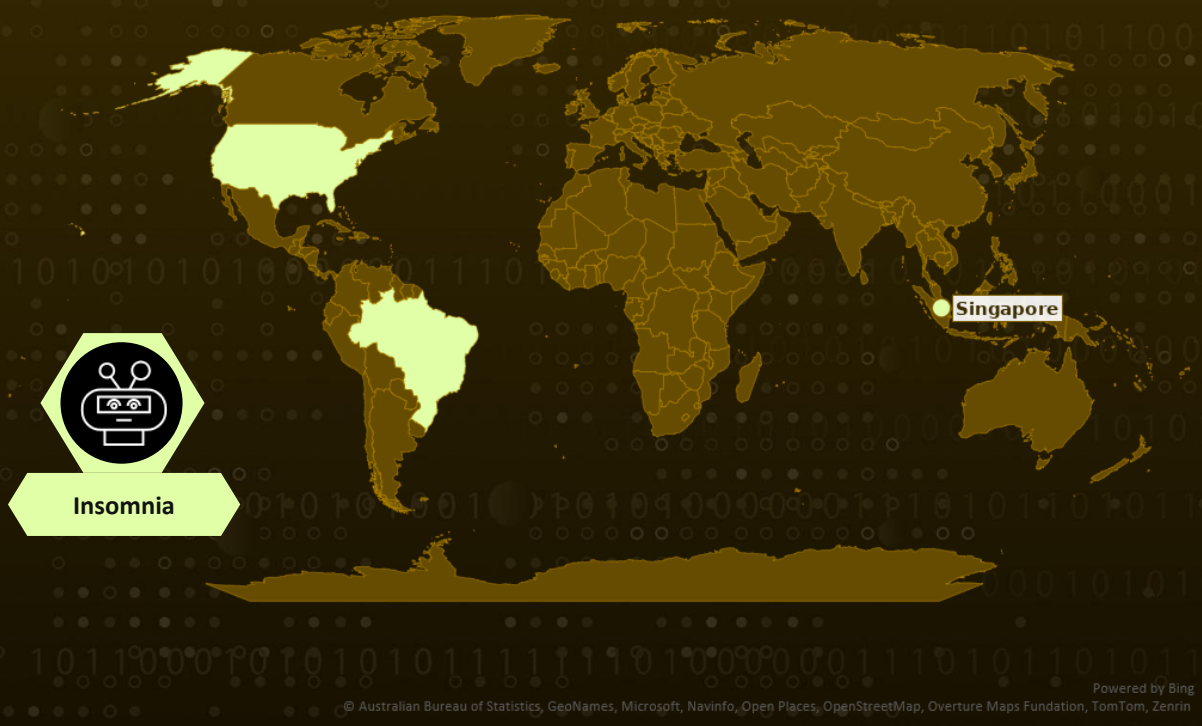
Insomnia: Data-Theft Extortion Operation Targeting US Healthcare

Date of Publication	Admiralty Code	TA Number
June 19, 2026	B2	TA2026173

Summary

First Seen: October 2025
Targeted Countries: United States, Singapore, Brazil
Targeted Platform: Windows
Targeted Industries: Healthcare, Business Services & Consulting, Manufacturing, Technology, Hospitality, Financial Services, Energy, Aerospace & Defense, Legal
Threat Actor: Insomnia
Attack: Insomnia is a data-theft-only extortion group active since October 2025 that operates without an encryptor, instead stealing sensitive records and publishing them for free on a Tor leak site to extort victims through the threat of exposure. The group gains entry via infostealer-harvested credentials and authentication bypass, then moves laterally using legitimate tools such as WSUS to evade detection, leaving no malicious payload behind. Targeting overwhelmingly small and mid-sized US healthcare providers, it has claimed over 30 victims, including a dermatology breach affecting more than 160,000 individuals with the US comprising roughly nine in ten claims. Because the threat is data exposure rather than encryption, backups and disaster-recovery plans offer no remediation once records leave the environment.

Attack Regions



Attack Details

#1 Insomnia is a data-theft-only extortion group that surfaced on the dark web in October 2025, operating with no encryptor, no negotiation portal, and no affiliate program. Rather than disrupting operations, the group steals sensitive records and publishes them for free download on a single Tor data leak site (DLS), relying on the threat of exposure rather than system disruption. It is best characterized as a data broker, with its model representing the broader ecosystem pivot away from encryption toward pure exfiltration leverage.

#2 The operation's first DLS entry is dated October 8, 2025, against a United States food and beverage company, with postings then accumulating across healthcare, legal, defense, and manufacturing. There is no predecessor group, forum recruitment, or builder advertisement preceding the launch, and no victim overlap with any prior leak-site database, consistent with a genuinely new operation rather than a rebrand. Targeting patterns are consistent with Russian-speaking operators, though this remains unconfirmed.

#3 Technically, initial access derives from stolen credentials harvested by infostealer malware from underground markets, combined with exploitation of authentication bypass vulnerabilities, with no specific CVEs attributed. For lateral movement the group abuses Windows Server Update Services (WSUS) and other legitimate administrative tooling to blend with normal IT activity, delivering no malicious payload and deploying no RMM, implant, or backdoor. Known infrastructure is limited to a single Tor hidden service running NGINX 1.22.1 and one Tox ID, the sole communication channel, with no email, negotiation portal, or dedicated chat, and no clear-web C2 or beaconing identified. The absence of any affiliate program, builder panel, or recruitment activity reinforces the assessment of a small operation or data brokerage.

#4 Victimology skews heavily toward small and mid-sized US healthcare providers with $5M - $57M revenue and 11 - 200 employees. The largest confirmed impact is a US dermatology practice, where an autumn 2025 intrusion exposed data on over 160,000 individuals per the HHS OCR filing. Following a bulk site ingestion in early February 2026, postings have averaged one to two per week, surpassing 30 victims by late April 2026, with the US accounting for roughly nine in ten claims and healthcare for about a third.

#5 The end objective is bulk theft of sensitive data followed by extortion. Insomnia exfiltrates records such as patient files, drivers' licenses, tax forms, and sensitive correspondence, and then leverages the threat of disclosure, or actual free release, on its Tor-based leak site. The operation has been observed practicing direct extortion, double extortion, and free public data leaks, and there are indications it may also function as a broker or platform that monetizes stolen data, potentially in cooperation with separate actors that supply initial network access. The result is a data-exposure threat that backups and disaster-recovery plans cannot remediate once records have left the environment.

Recommendations

Harden Against Infostealer-Driven Credential Access: Insomnia's access begins with valid credentials harvested by infostealers and bought on underground markets, not malware delivery. Enforce phishing-resistant FIDO2/hardware-token MFA across VPN, RDP, webmail, and SaaS, subscribe to infostealer log monitoring, and treat any credential surfaced in stealer logs as confirmed compromise.

Close Authentication-Bypass Exposure on Edge Services: The group is also reported to exploit authentication-bypass weaknesses at exposed access points, with no CVE attributed. Inventory internet-facing access services, apply patches and bypass mitigations promptly, disable legacy protocol paths, and alert on logins that skip expected MFA challenges.

Detect Credential-Based Intrusion Without Malware: Insomnia deploys no encryptor, ransom note, RMM, or backdoor, operating interactively with held access. Shift to identity and behavioral detection, impossible-travel logins, off-hours access to sensitive shares, and valid accounts used outside their normal scope.

Monitor and Constrain Windows Server Update Services (WSUS): Lateral movement abuses WSUS and other sanctioned admin tooling to blend with routine IT. Restrict WSUS access to tiered accounts, baseline normal use, and alert on unexpected configuration changes or update-package activity.

Protect Against Bulk Data Exfiltration: The objective is bulk theft of patient files, IDs, tax forms, and correspondence, backups cannot remediate once data leaves. Deploy DLP and egress monitoring for anomalous outbound transfers, govern consumer file-sharing, and encrypt PHI/PII repositories.

Prepare for Exfiltration-Only Extortion: Stolen data is released free on the Tor leak site with countdown timers, with possible brokering to third parties. Update IR playbooks for exposure where payment may not prevent release, brief legal on HHS OCR notification timelines, and monitor the leak site for organizational exposure.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1650: Acquire Access	
Initial Access	T1078: Valid Accounts	
	T1190: Exploit Public-Facing Application	
Lateral Movement	T1072: Software Deployment Tools	
Collection	T1005: Data from Local System	
Exfiltration	T1567: Exfiltration Over Web Service	
Impact	T1657: Financial Theft	

Indicators of Compromise (IOCs)

TYPE	VALUE
TOR Address	i62huw7ve22rpyw6lnq3kmfump2dmsg4xpveec3ere73njwatrz74gad[.]onion, R3keoxye5mki4fqcvlk4hpfqqzxmakchjpmem7oppynobcieamdbmcyd[.]onion
TOX ID	FA21E360945F602504728A05A39758C38B6A5B5DA1969717AF05838D14FDCD3DE17455833F11
DLS Server Banner	NGINX 1.22.1

Recent Breaches

https://www.thevantgroup.com
https://www.mchra.com
https://www.metosystems.com
https://www.unitedmd.com
https://www.nobleoilfieldservices.com
https://www.atlasoceanvoyages.com
https://www.vfhc.org
https://www.belmontplasticsurgeryva.com
https://www.rippleneuro.com
https://www.thrashco.com
https://www.zaner.com
https://www.admarkasiagroup.com
https://www.aspdd.com
https://www.thesyversongroup.com
https://www.copiercareers.com
https://www.aviam.com
https://www.integratedfresh.com
https://www.devallcs.com
https://www.partslifeinc.com
https://www.enviro-hub.com
https://www.rella-associates.com
https://www.siderm.com
https://www.aclapath.com
https://www.carlyleflorence.com
https://www.dunnanddunn.com
https://www.fhdks.com
https://www.immct.com
https://www.gmnp.com
https://www.schuremed.com
https://www.optimumhealth.org
https://www.chiarottino.com.br
https://www.digestivewellness.net
https://www.ahp.agency

References

https://www.halcyon.ai/threat-group/insomnia#classifications

https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/insomnia

https://www.hipaajournal.com/data-breach-southern-illinois-dermatology-heart-south-cardiovascular-group/

https://github.com/TheRavenFile/Daily-Hunt/blob/main/Insomnia%20Ransomware

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 19, 2026 • 09:00 AM

More at www.hivepro.com