Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

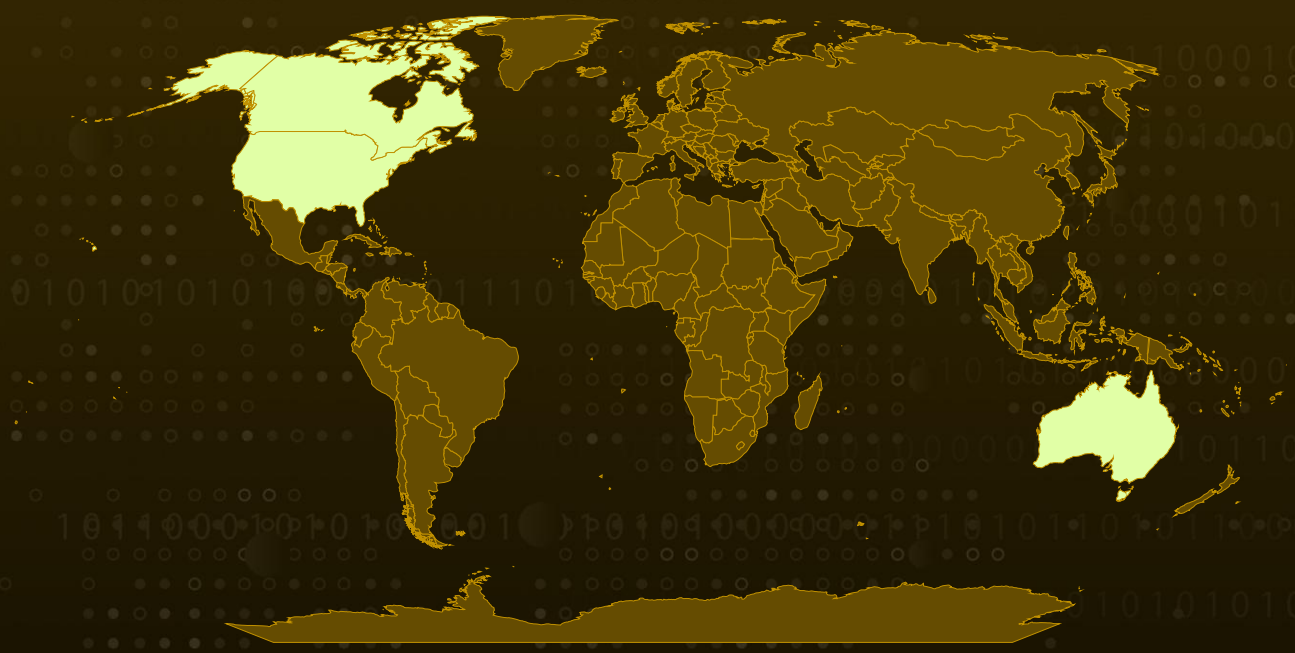
New CMD Organization Ransomware Hits U.S. Healthcare with Auction Extortion

Date of Publication	Admiralty Code	TA Number
June 8, 2026	B2	TA2026157

Summary

First Seen: Late March 2026
Targeted Countries: United States, Canada, Australia
Targeted Platform: Windows
Targeted Industries: Healthcare, Manufacturing, Retail, Business Services & Consulting, Technology, Religion, Charitable Organizations, Education, Legal
Malware: CMD Organization Ransomware, StealC, Meow
Attack: CMD Organization is a newly emerged ransomware operator, active since late March 2026, that has named over nineteen victims across three countries within its first eight weeks, with US Healthcare comprising roughly 38% of disclosures. The group operates a double-extortion model augmented by a novel public crypto-bidding platform that auctions stolen data alongside victim negotiations, demands ransoms of 7–8 BTC, and deploys an MSVC++ ChaCha20+RSA locker via Group Policy following IAB-sourced access, StealC credential harvesting, and "Meow" backdoor persistence.

Attack Regions



Targeted Non-Targeted

Attack Details

#1

CMD Organization emerged in late March 2026 as a new ransomware operator, with leak-site infrastructure (cmdofficial.com) registered through Namecheap on 29 March 2026 and the first victims posted in early April. By the end of May 2026 the group had named over nineteen victims across three countries, with US organizations accounting for roughly 84% of disclosures and Healthcare leading sector targeting at 38% of named victims. Confirmed ransom demands have ranged from 7 to 8 BTC (roughly USD 540,000–610,000), with affected entities concentrated in small-to-mid clinics.

#2

What differentiates CMD Organization is its extortion monetization model. Alongside double-extortion mechanics combining encryption with data exfiltration, the group has integrated a crypto-bidding platform directly into its leak site, allowing third-party buyers to bid for exclusive access to stolen datasets in parallel with victim negotiations. This auction model converts stolen data into a tradable asset before public release, expanding monetization beyond direct victim payments and amplifying coercion through public pricing. The bidding panel currently operates in a beta state without wallet validation or escrow controls, but the strategic intent represents a meaningful evolution in the extortion economy.

#3

Initial access in documented intrusions has occurred via SEO-poisoned search results delivering JavaScript loaders that stage StealC infostealer payloads, with subsequent credential handoff to operators consistent with initial access broker patterns. Reconnaissance and lateral movement leverage commodity tooling: Advanced IP Scanner and Advanced Port Scanner for network mapping, followed by Invoke-SMBRemoting, a publicly available in-memory SMB execution utility, for remote command execution using harvested credentials. Persistence is established through a backdoor DLL designated "Meow" (named after its sole significant export), observed as Netdrv.dll and beaconing over HTTPS to 188[.]190[.]2[.]165[:]666, with HKCU Run-key entries disguised as fake Microsoft Teams update installers carrying iterative version numbers.

#4

The CMD locker is propagated across victim environments via Group Policy and SYSVOL replication as paste1.exe, indicating Domain Admin-tier compromise prior to encryption. The locker is an MSVC++ binary with main function Lockit, using a ChaCha20+RSA hybrid scheme with an embedded public key. Encrypted files contain a metadata footer delimited by [CMD] start and end tags recording original file size, encryption mode, and key material, a distinctive forensic fingerprint. The locker explicitly targets database file extensions (MS Access, Oracle, Exchange), KeePass credential stores, and Lotus Notes archives, with partial encryption reserved for VMDK virtual disk files as a performance optimization. A __README__.html ransom note is dropped and auto-opened in Chrome on completion.

#5 While CMD Organization currently demonstrates limited operational maturity, outsourced locker tooling without built-in propagation, an unproven bidding platform in beta state, and operator OPSEC errors including verbose runtime logging within the binary, the group's healthcare-skewed targeting, novel auction extortion model, and observed end-to-end intrusion-to-impact capability warrant active monitoring.

Recommendations

Defend Against SEO-Poisoned Malvertisement Delivery: CMD's initial access begins with poisoned search results delivering archives masquerading as PDFs. Restrict execution of script file types (.js, .vbs, .wsf, .hta) from user download paths via WDAC or AppLocker, constrain cscript.exe and wscript.exe to administrative contexts, and deploy DNS filtering against newly registered and low-reputation domains.

Harden Against Infostealer-Driven Initial Access: Credential exposure through StealC and similar infostealers is the principal pivot point in CMD's intrusion chain. Enforce phishing-resistant FIDO2 or hardware-token MFA across VPN, RDP, SaaS, and privileged accounts. Subscribe to infostealer log monitoring services, rotate any exposed credentials immediately, and treat KeePass or browser credential exposure as confirmed compromise.

Harden and Monitor Active Directory and SYSVOL: CMD's locker is propagated via Group Policy and SYSVOL replication, indicating Domain Admin-tier compromise prior to encryption. Monitor for unauthorized GPO modifications, unexpected executables introduced into SYSVOL, and bulk PowerShell AD enumeration from non-administrative source hosts. Tier administrative accounts, restrict interactive logons on Domain Controllers, and alert on Invoke-SMBRemoting-style fileless lateral movement.

Prepare for Auction-Extortion Pressure: CMD's leak site hosts a public crypto-bidding platform that auctions stolen data to third-party buyers in parallel with victim negotiations. Update incident response playbooks for this vector, brief legal and communications teams on regulatory disclosure pressure from public data pricing, and monitor the CMD leak site for indications of organizational data exposure.

Conduct Regular Data Backups and Test Restoration: Regularly back up critical data and systems, store offline and immutably, and segregate backup infrastructure from production Active Directory. The CMD locker explicitly targets databases (MS Access, Oracle, Exchange), KeePass stores, and Lotus Notes archives, prioritize protection of these data stores and assume credential theft from any encrypted endpoint.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
		T1583.008: Malvertising
	T1608: Stage Capabilities	T1608.006: SEO Poisoning
	T1650: Acquire Access	
Initial Access	T1189: Drive-by Compromise	
	T1078: Valid Accounts	
Execution	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.007: JavaScript
	T1204: User Execution	
	T1218: System Binary Proxy Execution	
Defense Evasion	T1027: Obfuscated Files or Information	T1027.010: Command Obfuscation
	T1140: Deobfuscate/Decode Files or Information	
	T1036: Masquerading	T1036.004: Masquerade Task or Service
		T1036.005: Match Legitimate Name or Location
	T1070: Indicator Removal	T1070.004: File Deletion
Credential Access	T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers
Discovery	T1018: Remote System Discovery	
	T1046: Network Service Discovery	
	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
	T1033: System Owner/User Discovery	

Tactic	Technique	Sub-technique
Lateral Movement	T1021: Remote Services	T1021.002: SMB/Windows Admin Shares
	T1570: Lateral Tool Transfer	
	T1484: Domain or Tenant Policy Modification	T1484.001: Group Policy Modification
Collection	T1005: Data from Local System	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1105: Ingress Tool Transfer	
	T1090: Proxy	
	T1573: Encrypted Channel	T1573.002: Asymmetric Cryptography
Impact	T1486: Data Encrypted for Impact	
	T1657: Financial Theft	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	69aa0eeab454e6967e9c860d02749857b0b4c4ea8c55ba0c1a1af12af5a25bca
SHA1	07c14b82f673ba5caa8c1188f052ea31583f0af7, 8ed2c2e67ae8d3cfe1fca15d5c7b33e7011bb8dd, c18cef4610d272caa3c51ec5803439aff3b4982e, 463554c76a0aa472daf9b42e9414942910b4ac54, c5c9fa0f36c08a1457af48737f7656de298bac43
IPv4	185[.]196[.]10[.]231, 209[.]99[.]186[.]211, 188[.]190[.]2[.]165, 213[.]165[.]47[.]49, 167[.]99[.]233[.]78
Domains	cmdofficial[.]com, clubsoar[.]com, artistichairlounge[.]com
URLs	hxxps[:]//clubsoar[.]com/fd/patricia%20va%20a%20california%20pdf[.]zip, hxxps[:]//artistichairlounge[.]com/bestbooklibrarycom/template[.]php?q=patricia%20va%20a%20california%20pdf, hxxp[:]//213[.]165[.]47[.]49/b0c9ed38f2b14c119546[.]php, hxxp[:]//167[.]99[.]233[.]78/mbd
File Names	paste1.exe, Patricia-va-a-california-pdf.zip, qlgdhgk.ps1, qu.ps1, Netdrv.dll, Advanced_Port_Scanner_2.5.3869.exe, Invoke-SMBRemoting, Openssl.exe, __README__.html
File Paths	C:\ProgramData\paste1.exe, C:\SYSVOL\sysvol\[domain]\Policies\[GUID]\, %APPDATA%\[fake-teams-installer-name]\

TYPE	VALUE
Emails	Cmd2official[@]onionmail[.]org, Cmdhtmnjksgkuhilrtrh[@]onionmail[.]org, MitsueWhite[@]onionmail[.]org, JedAdams[@]onionmail[.]org
Tor Leak Site	cmdnkiqjije2tllr3biee2sjgj3i4robg2cbtilbnytdhh2wy3syrlyd[.]onion

Recent Breaches

https://seewritehear.com
https://lwsd.wednet.edu
https://leelawoffices.org
https://capitalfamilymd.com
https://heartofamericaeyecare.com
https://hospicesavannah.org
https://www.ndsm.org
https://stonehengetc.com
https://theholynameofjesus.org
https://wholehealthchicago.com
https://raisethebottomidaho.com
https://houstoneye.com
https://www.goldbergcoins.com
https://www.goodstone.com.au
https://aspg.com
https://penneastern.com
https://jgstewart.ca
https://www.cytekbio.com
https://zampell.com

References

https://labs.beazley.security/articles/cmd-organization-new-ransomware-operator-moves-to-place-public-bidding-wars-on-ransomed-data

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

https://hivepro.com/threat-advisory/stealc-v2-spreads-via-malicious-blender-files/

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 8, 2026 • 03:30 AM

More at www.hivepro.com