Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

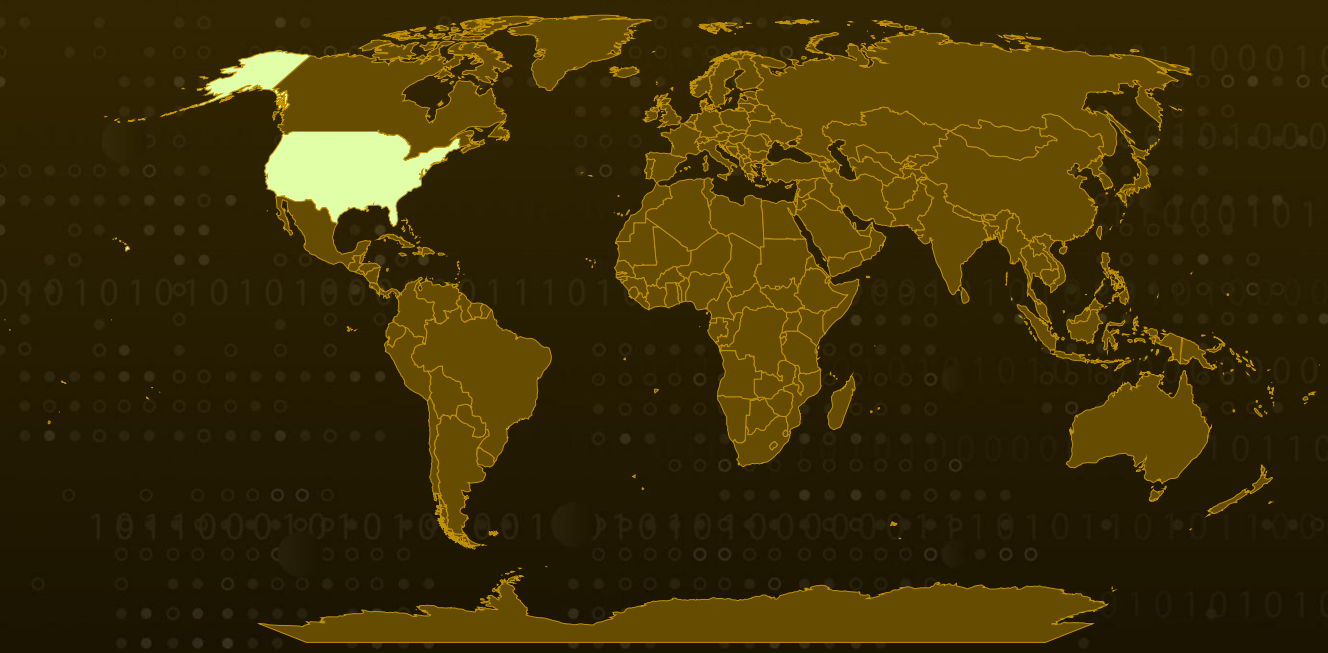
Dohdoor Malware Campaign Targeting U.S. Education and Healthcare Sectors

Date of Publication	Admiralty Code	TA Number
March 03, 2026	A1	TA2026058

Summary

First Seen: November 25, 2025
Targeted Region: United States
Targeted Platform: Windows
Targeted Industries: Education and Healthcare
Malware: Dohdoor
Attack: The Dohdoor campaign is a targeted intrusion operation impacting U.S. education and healthcare organizations, leveraging phishing to initiate a multi-stage malware infection chain. The threat actor abuses PowerShell, DLL sideloading, and legitimate Windows binaries to achieve stealthy execution and persistence. Command-and-control (C2) communications are conducted over DNS-over-HTTPS (DoH), enabling encrypted traffic to blend with legitimate web activity while facilitating in-memory payload delivery. Overall, the activity reflects a capable adversary employing fileless techniques, process injection, and advanced defense evasion to maintain persistent access within high-value environments.

Attack Regions



Targeted Non-Targeted

Attack Details

#1 The Dohdoor campaign is a targeted intrusion operation affecting organizations in the U.S. education and healthcare sectors. Tracked under the cluster UAT-10027, the activity involves a previously undocumented backdoor dubbed Dohdoor. The campaign demonstrates a structured, multi-stage infection chain with a strong emphasis on stealth, persistence, and encrypted command-and-control (C2) communications to maintain long-term access within compromised environments.

#2 Initial access is believed to occur through phishing or social engineering that prompts victims to execute a malicious PowerShell script. This script retrieves additional components using legitimate Windows utilities such as curl.exe, ultimately delivering a malicious DLL disguised as a legitimate system file. The attackers rely heavily on DLL sideloading, executing the malicious library through trusted binaries (e.g., OpenWith.exe or wksprt.exe) to blend into normal system activity. This approach enables the malware to evade endpoint defenses by running within the context of legitimate processes.

#3 A defining feature of Dohdoor is its use of DNS-over-HTTPS (DoH) for C2 communications. By encrypting DNS traffic within HTTPS sessions over port 443 and leveraging trusted cloud-hosted infrastructure, the malware conceals its network activity within normal encrypted web traffic. The infrastructure uses obfuscated and irregularly capitalized subdomains designed to resemble legitimate software update services. C2 responses are decrypted using a custom position-dependent XOR-SUB routine with SIMD acceleration, expanding payload data prior to reflective, in-memory execution, minimizing disk artifacts and complicating forensic analysis.

#4 Post-compromise activity includes process hollowing and in-memory injection of secondary payloads, often involving commercially available red team frameworks to support lateral movement, privilege escalation, and persistence. The malware also incorporates defense evasion techniques such as NTDLL unhooking, API hashing for dynamic resolution, artifact clearing, and self-deletion. While there are limited technical overlaps with previously documented state-aligned threat activity, attribution remains low confidence. Overall, the campaign reflects a capable threat actor leveraging encrypted communications, fileless execution, and advanced evasion tradecraft to maintain stealth in high-value target networks.

Recommendations

Strengthen Email & Script Controls: Implement advanced phishing protection and sandboxing to reduce malicious attachment delivery. Restrict and log PowerShell execution, including Script Block and Module Logging. Enforce application control policies to block unauthorized script and binary execution.

Prevent DLL Sideloading Abuse: Audit and restrict execution of non-essential Windows binaries commonly abused for sideloading (e.g., OpenWith.exe, wksprt.exe, mblctr.exe). Enforce code-integrity policies to allow only trusted, signed DLLs. Monitor for suspicious child processes spawned by legitimate system binaries.

Monitor and Restrict DNS-over-HTTPS (DoH): Limit DoH usage to approved resolvers and block unauthorized encrypted DNS traffic. Monitor outbound HTTPS for anomalous DoH patterns and suspicious domain naming (e.g., irregular capitalization). Leverage TLS metadata and behavioral analytics to detect covert C2 activity.

Enhance Endpoint Behavioral Detection: Enable logging and detection for process injection, process hollowing, and reflective in-memory loading. Monitor for syscall unhooking and API hashing behaviors. Align detections with relevant MITRE ATT&CK techniques (e.g., T1574.002, T1055.001) for proactive threat hunting.

Strengthen Post-Compromise Resilience: Enforce least-privilege access and implement network segmentation to reduce blast radius. Monitor privileged account usage and credential abuse indicators. Maintain updated incident-response playbooks and ensure centralized log retention for rapid detection and containment.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1566: Phishing	
Execution	T1204: User Execution	T1204.002: Malicious File
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.003: Windows Command Shell
	T1129: Shared Modules	

Tactic	Technique	Sub-technique
Persistence	T1574: Hijack Execution Flow	T1574.001: DLL
Defense Evasion	T1027: Obfuscated/Encrypted Files	
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
	T1070: Indicator Removal on Host	T1070.004: File Deletion
	T1055: Process Injection	T1055.012: Process Hollowing
	T1027: Obfuscated Files or Information	
	T1140: Deobfuscate/Decode Files or Information	
	T1106: Native API	
	T1218: System Binary Proxy Execution	
	T1036: Masquerading	
Privilege Escalation	T1055: Process Injection	T1055.001: Dynamic-link Library Injection
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
		T1071.004: DNS
	T1573: Encrypted Channel	
	T1568: Dynamic Resolution	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	54e18978c6405f56cd59ba55a62291436639f21cf325ae509f0599b15e8f7f53, 0bb130b1fafb17705d31fe5dd25e7b2d62176578609d75cc57911ef5582ef17a, 54545fa3a2d8da6746021812ebaa9d26f33bba4f63c6f7f35caa6fa4ee8c0e6a, 8e97c677aec905152f8a92fed50bb84ef2e8985d5c29330c5a05a4a2afcbd4a5, 800faaf15d5f42f2ab2c1d2b6b65c8a9e4def6dc10f6ce4e269dcf23f4e8dae2, b1bd8f7d4488977cca03954a57f5c8ad7bfd4609bcc3bae92326830fcbd3232c, 2ce3e75997f89b98dd280d164a5f21f7565f4de26eed61243badde04b480700e
URLs	hxxp[://]gITkzxd[.]pNUIScKMhWAgZvdyJRlBEFT[.]SoFtwaRE/X111111, hxxp[://]GppiwoGwNdiakkDU[.]pnuiSckMHwaGzvDYjRLbeFt[.]SoFTWARe/111111?sub=s, hxxp[://]lBaNDUgZCFG[.]deepInspectiOnSYSTEM[.]oNLiNE/X111111, hxxp[://]CJiTDrpwnnA[.]MswINsoFTUPDLoad[.]deSigN/x111111, hxxp[://]LsyPdQGXrEDfPx[.]MSwInSofTUpDloAd[.]dESign/111111?sub=s, hxxp[://]sDXsIol[.]PNUIsckmHwAgzVdYJRlbeFT[.]SoftWarE/X111111, hxxp[://]ezQrvkFgEJWCTDNc[.]pNuiSCKMhwAgZvdyjrlBEFT[.]softwarE/111111?sub=d, hxxp[://]lLalWpIJnjskClwY[.]PnUiscKMhWaGzVdyJRlBEfT[.]SofTWaRe/111111?sub=s
Host Names	CJiTDrpwnnA[.]MswINsoFTUPDLoad[.]deSigN, LBaNDUgZCFG[.]deepInspectiOnSYSTEM[.]oNLiNE, LsyPdQGXrEDfPx[.]MSwInSofTUpDloAd[.]dESign, YHDJTyLNsMWVuU[.]DEEPinSPeCTioNsyStEM[.]OnLiNe, SDXsIol[.]PNUIsckmHwAgzVdYJRlbeFT[.]SoftWarE, EzQrvkFgEJWCTDNc[.]pNuiSCKMhwAgZvdyjrlBEFT[.]softwarE, txjIQslrRIg[.]MSwINSOFTUPDLoaD[.]DesiGN, QHtcKZBXtKdVyr[.]mSWinSoFTUpdLOAD[.]DeSIgn, GITkzxd[.]pNUIScKMhWAgZvdyJRlBEFT[.]SoFtwaRE, GppiwoGwNdiakkDU[.]pnuiSckMHwaGzvDYjRLbeFt[.]SoFTWARe

References

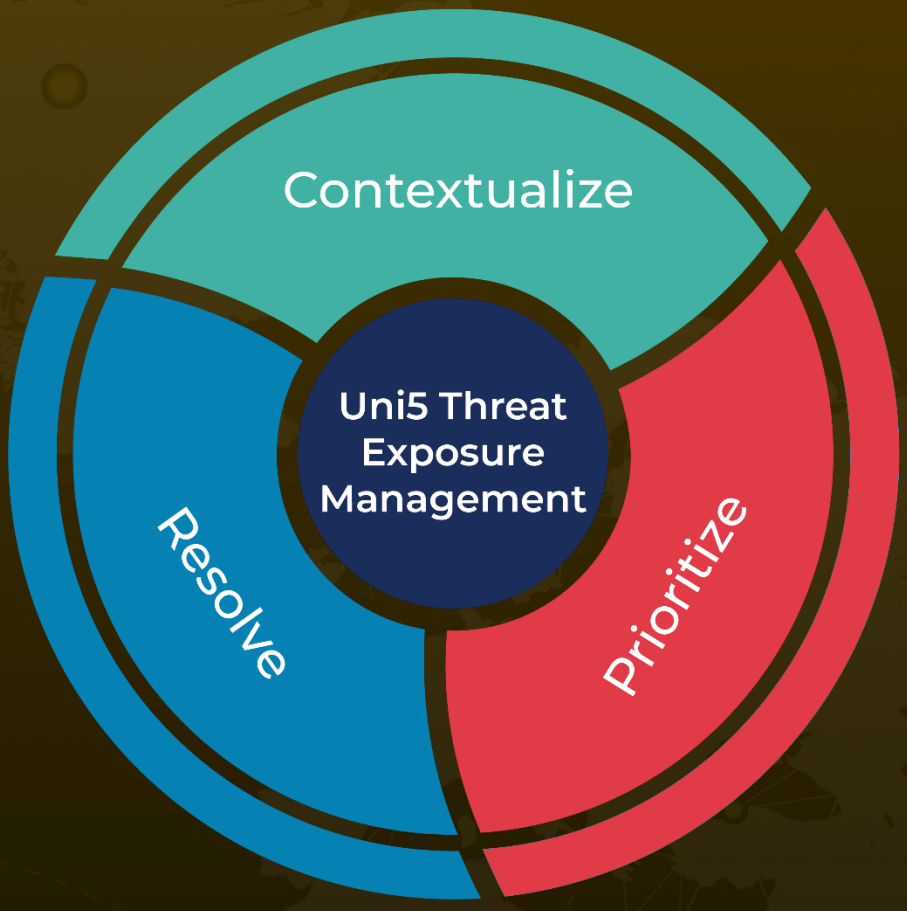
https://blog.talosintelligence.com/new-dohdoor-malware-campaign/

https://github.com/Cisco-Talos/IOCs/blob/main/2026/02/new-dohdoor-malware-campaign.txt

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 free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

March 03, 2026 • 06:30 AM

More at www.hivepro.com