Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

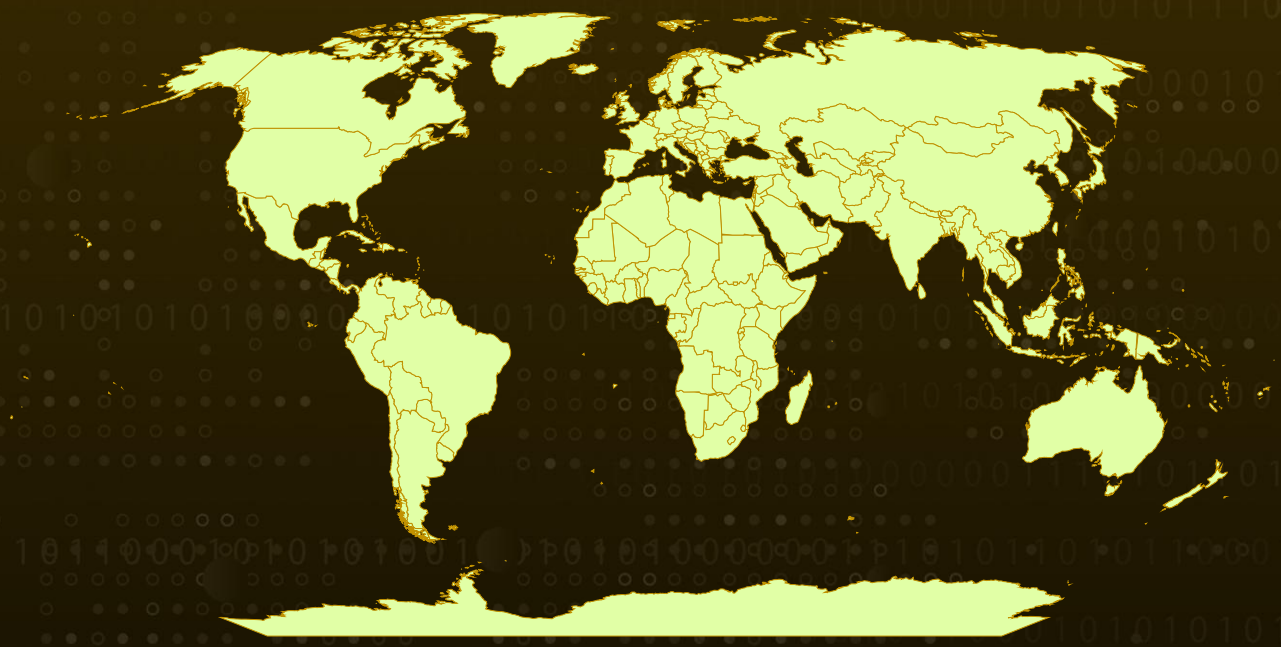
MLTBackdoor: ClickFix to Ransomware Foothold

Date of Publication	Admiralty Code	TA Number
June 11, 2026	A1	TA2026163

Summary

First Seen: 2026
Targeted Regions: Worldwide
Targeted Platforms: Windows
Malware: MLTBackdoor
Attack: A newly identified malware, MLTBackdoor, has emerged as a sophisticated post-exploitation tool believed to be used by a likely ransomware-linked threat actor to establish a foothold and enable lateral movement within compromised networks. The malware is delivered through a multi-stage ClickFix infection chain that starts with a lure hosted on an automotive-themed website. When a victim copies, pastes, and executes the malicious content, a series of commands downloads a compressed archive from a DGA-generated domain, decrypts an RC4-encrypted payload, and sideloads the backdoor through a legitimate, signed Microsoft Defender executable. Once active, MLTBackdoor provides file management capabilities and, more notably, features a Beacon Object File (BOF) loader, allowing attackers to dynamically deploy additional in-memory modules and extend the malware's functionality as required.

Attack Regions



Targeted Non-Targeted

Attack Details

#1 A newly discovered malware family, MLTBackdoor, is attracting attention for its sophisticated multi-stage attack chain and stealth-focused design. Rather than exploiting a software flaw, the malware relies on social engineering, demonstrating how threat actors continue to leverage user interaction to gain initial access.

#2 The infection starts with a ClickFix lure hosted on an automotive-themed website. Victims are tricked into copying and executing malicious content, which launches a headless conhost.exe process. This process creates a temporary directory, downloads a payload from a domain generated through a daily DGA, extracts the archive, and executes a malicious DLL via rundll32. The archive contains data.bin and endpointdlp.dll, with the DLL acting as a loader for the next stage of the attack.

#3 After execution, endpointdlp.dll decrypts the RC4-encrypted data.bin file to deploy MLTBackdoor. The malware then performs a self-update and disguises itself by sideloading through the legitimate Microsoft Defender executable mpextms.exe. To hinder analysis, it employs heavy obfuscation techniques such as Mixed Boolean-Arithmetic (MBA) and Control Flow Flattening (CFF), dynamically resolves APIs and system calls using DJB2 hashing, and leverages Hell's Gate-style indirect syscalls to evade security monitoring.

#4 MLTBackdoor also incorporates extensive anti-analysis measures, checking for virtual machines, debuggers, sandbox artifacts, low-memory environments, and other indicators of analysis systems. Rather than stopping when detected, it reports these findings back to its command-and-control (C2) server. While the malware supports basic file operations, its most notable capability is a built-in Beacon Object File (BOF) loader, allowing operators to execute custom post-exploitation modules directly in memory without writing files to disk, a feature consistent with ransomware-related operations.

#5 For communications, MLTBackdoor uses a custom encrypted protocol over TLS on port 443, disguising traffic as legitimate Microsoft telemetry. It employs ECDH key exchange and AES-256-GCM encryption, while a date-based DGA generates new domains daily to maintain contact if primary C2 infrastructure is disrupted. In one observed case, the same DGA-generated domain was used for both malware delivery and command-and-control communications, highlighting the malware's tightly integrated and resilient infrastructure.

Recommendations

Block Known MLTBackdoor Indicators: Immediately block the SHA256 hashes, C2 domains, and update URL identified in the IoC section across endpoint, network, and DNS controls to stop active beaconing and payload retrieval.

Disrupt ClickFix Social Engineering: Educate users that legitimate websites never require copying and pasting commands into the Run dialog or a terminal, and deploy controls that flag or block this behavior. Treat clipboard-to-shell execution patterns as high-risk.

Monitor for Abuse of Legitimate Microsoft Binaries: Watch for mpextms.exe sideloading a DLL named endpointdlp.dll, and more broadly for trusted Microsoft Defender binaries loading DLLs from user-writable or temporary directories, which indicates DLL sideloading abuse.

Inspect Outbound Traffic on Port 443: Flag TLS connections to the fixed URL path /api/v1/telemetry and outbound requests carrying the Microsoft-Delivery-Optimization/10.1 User-Agent to atypical or newly registered domains, as MLTBackdoor uses these to blend in.

Counter the Domain Generation Algorithm: Because the DGA produces a new C2 domain daily, supplement static domain blocklists with detection of newly registered and algorithmically generated domains, and integrate the published DGA tooling into proactive blocking where feasible.

Deploy and Tune Endpoint Detection Despite Evasion: Since MLTBackdoor uses indirect system calls to bypass user-mode API hooks, prioritize kernel-level telemetry, ETW-based detection, and behavioral analytics rather than relying solely on inline API hooking.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1566: Phishing	
Execution	T1204: User Execution	T1204.001: Malicious Link
	T1059: Command and Scripting Interpreter	T1059.003: Windows Command Shell
	T1106: Native API	
Defense Evasion	T1574: Hijack Execution Flow	T1574.001: DLL
	T1027: Obfuscated Files or Information	
	T1106: Native API	
	T1497: Virtualization/Sandbox Evasion	
	T1622: Debugger Evasion	
	T1620: Reflective Code Loading	
	T1027: Obfuscated Files or Information	T1027.007: Dynamic API Resolution
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1573: Encrypted Channel	T1573.002: Asymmetric Cryptography
		T1573.001: Symmetric Cryptography

Tactic	Technique	Sub-technique
Command and Control	T1568: Dynamic Resolution	T1568.002: Domain Generation Algorithms
	T1105: Ingress Tool Transfer	
Discovery	T1057: Process Discovery	
	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
Exfiltration	T1041: Exfiltration Over C2 Channel	
Impact	T1486: Data Encrypted for Impact	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	1e41c7bfaa6aa3b93b6cc024274a10e33f3e12fe7c98c1db387ef8927f9d1984, 46b2155c1e71b840d4b7a2e94410b89a61e2446523e6f497206d402eb02e0e93, 9e52cc90cff150abe21f0a6440e86e0a99ff383b81061b96def8948e21d0ac66, ced6b0f44410f6133ad63b61e04613a8b56cc3338d7b34497540e9541163e7ec, 1d09357b6a096fdc35cd5c873eed15665d6b3c879d20c8cf01e6bca0005512cf, 2cd88d5280a61714836f5f07a16df190911c5b952af2998dbbcda910b3b1c494, d34e4038c5c80728f9648ba84833f69bc1ccea82e2e8e748b7b7f02fb687b92b
Domains	hrs2y15sungu[.]com, carrolc[.]com, cwrtwright[.]com, thomphon[.]com
URL	hxxps[:]//powwowski[.]com/payloads/update[.]zip

References

https://www.zscaler.com/blogs/security-research/technical-analysis-mltbackdoor

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 11, 2026 • 08:30 AM

More at www.hivepro.com