Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

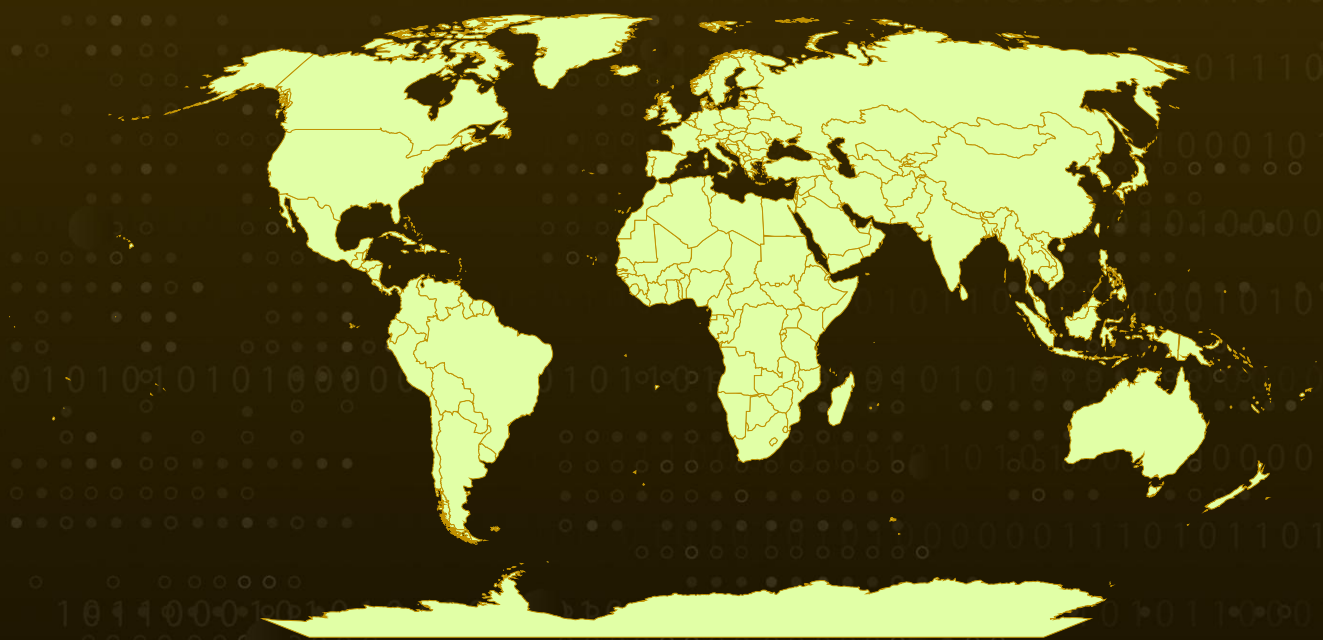
DoubleClick Deception: Malspam Campaign Delivers Stealthy .NET Malware

Date of Publication	Admiralty Code	TA Number
June 04, 2026	A1	TA2026154

Summary

First Seen: May 2026
Targeted Regions: Worldwide
Targeted Platforms: Microsoft Windows
Attack: A malspam campaign delivers a fileless .NET loader through a five-stage chain that routes initial lure links through Google's DoubleClick (ad.doubleclick[.]net) for reputation evasion, then stages execution through HTML meta-refresh, JScript, PowerShell, and reflective .NET assembly loading. The loader performs process hollowing into signed Microsoft binaries, patches AMSI and ETW at the native API level, and communicates with DDNS-based C2 infrastructure over encrypted TCP.

Attack Regions



Attack Details

#1 In May 2026, incident responders investigated a sophisticated malware campaign that began with a malspam email, a tactic that remains one of the most common initial access vectors. The email carried a malicious HTML attachment named Bestellung_2026.html ("purchase order" in German), which redirected victims through a trusted Google DoubleClick tracking URL before leading them to a phishing kit. The kit dynamically customized its appearance using the recipient's email address, company branding, and geolocation details, making the lure appear more convincing.

#2 Victims were prompted to download a supposed PDF document, but instead received a ZIP archive containing an obfuscated JScript loader. Once executed, the script established persistence, reconstructed a hidden PowerShell payload, and performed connectivity and anti-analysis checks. If debugging, sandboxing, or malware-analysis tools were detected, the malware attempted to evade scrutiny by rebooting the system.

#3 The PowerShell loader then downloaded additional components and launched a second-stage .NET assembly directly in memory. To remain stealthy, the malware leveraged legitimate Microsoft binaries such as InstallUtil.exe or MSBuild.exe for process injection. The .NET stager conducted extensive checks for virtual machines, sandbox environments, remote desktop sessions, and security tools before proceeding with the infection.

#4 To further reduce detection, the malware attempted to disable Microsoft Defender protections when certain third-party security products were absent. It retrieved multiple obfuscated payloads, decoded them through several stages, and established persistence using Registry Run keys, Startup folder entries, and scheduled tasks. The malware also disguised its files and directories using NVIDIA-themed names to blend in with legitimate software.

#5 In its final stage, the malware used process hollowing to inject malicious code into trusted processes and communicate with command-and-control servers through encrypted channels. It gathered system information, patched AMSI and ETW functions to limit security visibility, and supported multiple payload delivery methods, including in-memory execution and encrypted file drops. The campaign's use of trusted redirection services, layered obfuscation, anti-analysis techniques, and stealthy persistence highlights a highly sophisticated malware delivery chain designed to evade modern security defenses.

Recommendations

Neutralize Script-Based Attachments via GPO: Configure an Active Directory Group Policy Object that forces script file types such as .js, .vbs, and .hta to open in Notepad or Notepad++ by default, removing their ability to execute on double-click and stopping the chain at its first stage before any PowerShell or .NET payload is dropped.

Sandbox Attachments and Links at the Email Gateway: Deploy an email security gateway capable of detonating attachments and inspecting links before delivery, and block or quarantine script-based and macro-enabled attachments at the mail layer; because DoubleClick fronts the chain, time-of-delivery inspection of the attachment is the most reliable point to break it.

Enforce Email Authentication: Implement SPF, DKIM, and DMARC records to harden the email perimeter and reduce the likelihood that spoofed or impersonated malspam reaches end users.

Enable Time-of-Click URL and Attachment Protection: Where available, enable Safe Links and Safe Attachments (or an equivalent) so that URLs and files are re-inspected at the moment of interaction rather than only at delivery, countering redirect chains that hide behind trusted domains like DoubleClick.

Restrict Unnecessary Elevation and Persistence Paths: Tighten UAC settings, monitor for runas-driven self-elevation, and audit HKCU Run/RunOnce keys, the user Startup folder, and newly created repeating scheduled tasks with randomized or driver-themed names for unexpected entries.

Reinforce the Human Layer: Run regular phishing-awareness training and internal simulated phishing campaigns, since dynamically branded, geolocation-aware lures are designed to defeat user suspicion and the human remains the most consistently exploited entry point.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1566: Phishing	T1566.001: Spearphishing Attachment
Execution	T1204: User Execution	T1204.001: Malicious Link
		T1204.002: Malicious File
	T1059: Command and Scripting Interpreter	T1059.007: JavaScript
		T1059.001: PowerShell
	T1047: Windows Management Instrumentation	
	T1106: Native API	
Defense Evasion	T1620: Reflective Code Loading	
	T1027: Obfuscated Files or Information	
	T1140: Deobfuscate/Decode Files or Information	
	T1055: Process Injection	T1055.012: Process Hollowing
	T1218: System Binary Proxy Execution	T1218.004: InstallUtil
	T1127: Trusted Developer Utilities Proxy Execution	T1127.001: MSBuild
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
		T1562.006: Indicator Blocking
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
	T1622: Debugger Evasion	

Tactic	Technique	Sub-technique
Defense Evasion	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
	T1112: Modify Registry	
	T1070: Indicator Removal	
	T1480: Execution Guardrails	
Persistence	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
Discovery	T1518: Software Discovery	T1518.001: Security Software Discovery
	T1082: System Information Discovery	
	T1057: Process Discovery	
Command and Control	T1071: Application Layer Protocol	
	T1571: Non-Standard Port	
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
		T1573.002: Asymmetric Cryptography
	T1568: Dynamic Resolution	
	T1105: Ingress Tool Transfer	
Privilege Escalation	T1548: Abuse Elevation Control Mechanism	

Indicators of Compromise (IOCs)

TYPE	VALUE
Filenames	Bestellung_2026.html, A02118552lS210008-11521.zip, A02118552lS210008-11521.js, ktncm.js, zkrbx.txt, gglhn.txt, nlbzl.ps1, shmvg_01.ps1
Filepath	%USERPROFILE%\AppData\LocalLow\LocalLow Windows\Program Rules\Program Rules NVIDEO\Program Rules\Program Rules NVIDEO
Domains	fostercareintheus[.]optimizationprime[.]com, bth[.]startthewave[.]org, andrefelipedonascime1778799406970[.]2241107[.]meusitehostgator[.]com[.]br, catalogo[.]castrouria[.]com, xtadts[.]ddns[.]net, afxwd[.]ddns[.]net
URLs	hxxps[:]//bth[.]startthewave[.]org/a/, hxxps[:]//pengajian[.]muliastudy[.]com/images/edu/u[.]php, hxxps[:]//andrefelipedonascime1778799406970[.]2241107[.]meusitehostgator[.]com[.]br/GpazlLUWIJ_14_05_Meus_ArquivosDeTexto/01[.]txt, hxxps[:]//andrefelipedonascime1778799406970[.]2241107[.]meusitehostgator[.]com[.]br/GpazlLUWIJ_14_05_Meus_ArquivosDeTexto/02[.]txt, hxxps[:]//andrefelipedonascime1778799406970[.]2241107[.]meusitehostgator[.]com[.]br/GpazlLUWIJ_14_05_Meus_ArquivosDeTexto/03[.]txt, hxxps[:]//andrefelipedonascime1778799406970[.]2241107[.]meusitehostgator[.]com[.]br/GpazlLUWIJ_14_05_Meus_ArquivosDeTexto/PeNo, hxxp[:]//catalogo[.]castrouria[.]com/c84da/bl[.]txt

References

https://www.huntress.com/blog/malspam-to-loader-delivery-chain-analysis

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 04, 2026 • 09:30 AM

More at www.hivepro.com