Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

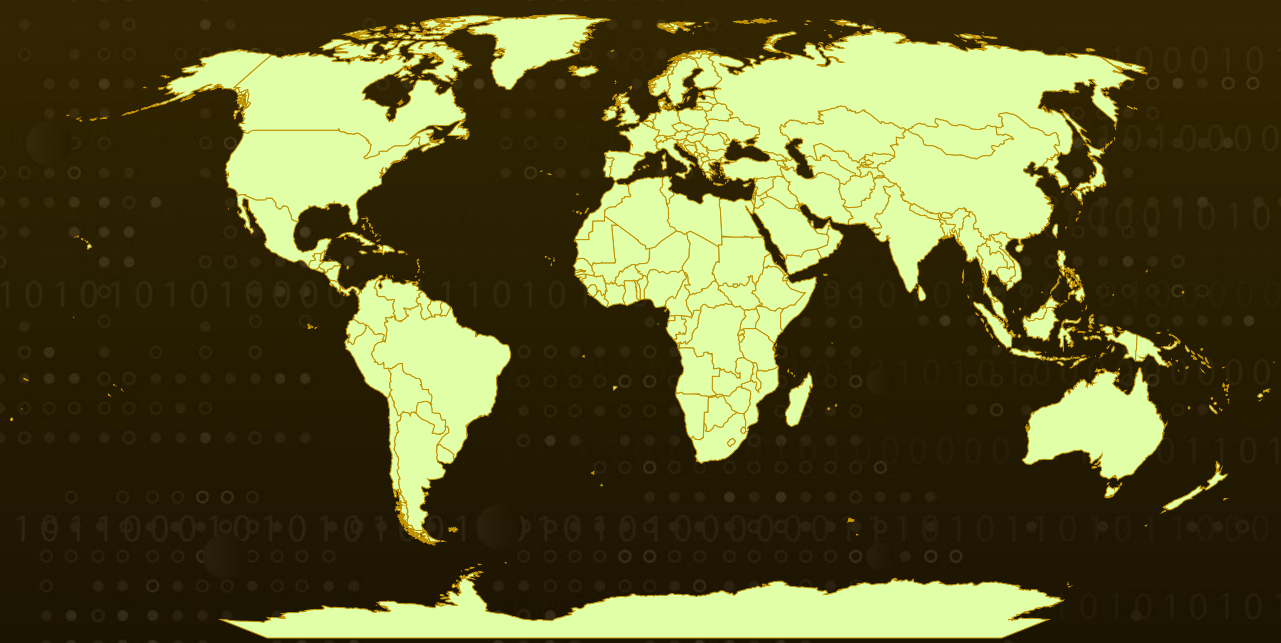
Malware in Disguise: How GitHub Became a Dropper's Playground

Date of Publication	Admiralty Code	TA Number
July 11, 2025	A1	TA2025214

Summary

Targeted Countries: Worldwide
Targeted Platform: Windows
Malware: Lumma Stealer
Attack: A seemingly innocent GitHub repository promising tools like “Free VPN for PC” or “Minecraft Skin” turned out to be a cleverly disguised trap. Behind these names, a stealthy dropper was hiding Lumma Stealer, a powerful info-stealing malware that slips past detection by injecting itself into memory using layers of encryption and obfuscation. It mimics trusted processes, hides in plain sight, and silently harvests sensitive data, all while appearing harmless. This attack highlights how threat actors are abusing popular platforms like GitHub to trick users and spread sophisticated malware with ease.

Attack Regions



Attack Details

#1 GitHub has long been a trusted resource for developers around the world, but that trust is now being increasingly exploited by cybercriminals. In a recent incident, a threat actor uploaded files under innocent names like “free-vpn-for-pc” and “minecraft-skin,” hoping to lure unsuspecting users. Beneath these seemingly harmless titles, however, was a sophisticated dropper designed to silently deliver **Lumma Stealer**, a powerful info-stealing malware. The payload, cleverly hidden as a Base64-encoded DLL tucked behind a block of French text, was designed to fly under the radar of most antivirus tools.

#2 The campaign, traced to a GitHub user known as SAMAIOEC, used classic social engineering tactics, offering seemingly useful tools within password-protected ZIP archives. This packaging technique helps bypass browser-based security checks, making the malware harder to detect during download. Once opened, the user would unknowingly launch a dropper named Launch.exe. This dropper appears to have been created with a malware builder that injects fake metadata to confuse static analysis tools. It uses Windows API calls to dynamically load its malicious payload directly into memory, avoiding traditional detection.

#3 What makes this dropper particularly evasive is its use of layered obfuscation. It employs trigonometric decryption functions and bitwise operations to decode the Base64 DLL and write it to disk only to hide the file immediately afterward. The DLL is then executed and kept alive using an infinite wait loop, giving the malware a persistent foothold on the system. Once active, the DLL exports a function and includes checks to detect debugging environments.

#4 The malware allocates memory and writes the unpacked payload. The malicious code is then injected into trusted Windows processes, helping it blend in and avoid suspicion. These process injection techniques make it significantly harder for endpoint security tools to detect the malware once it's running. A fake msvcp110.dll is also dropped into the user's AppData directory as part of the payload.

#5 This campaign bears all the hallmarks of Lumma Stealer activity, from infrastructure similarities and domain patterns to behavioural overlaps seen in previous attacks. The attacker even uploaded a second sample disguised as a “Minecraft Skin” tool, again offering no identifying information, a stark reminder of how easily threat actors can remain anonymous while abusing public platforms.

#6 Ultimately, the "Free-VPN-For-PC" sample wasn’t a VPN at all, it was a stealthy and sophisticated malware loader. Its use of multiple evasion layers, in-memory execution, and trusted process abuse underscores a growing trend: cybercriminals are embedding malware in plain sight, using familiar tools and services to deliver harmful payloads.

Recommendations

- **Be cautious with free tools from unknown sources:** Avoid downloading tools like “free VPNs” or “game skins” from unverified GitHub users or unfamiliar websites.
- **Scan ZIP files before extracting:** Even if a ZIP file is password-protected or looks harmless, it can still contain malware. Use a reliable antivirus or endpoint security solution to scan archive files before opening or extracting them.
- **Monitor GitHub and other platforms for threats:** Actively monitor public platforms like GitHub for suspicious uploads. Threat actors often use these sites because they’re trusted by default. Automated threat intelligence feeds can help flag malicious repositories early.
- **Keep an Eye on Unusual DLL Activity:** Watch for the creation or execution of suspicious DLL files especially in locations like AppData\Roaming\msvcp110.dll. If you see these files being dropped or run by unknown programs, it’s a strong sign something malicious could be happening and should be investigated immediately.
- **Enhance Endpoint Protection:** Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0007** Discovery	**TA0009** Collection	**TA0011** Command and Control
T1189 Drive-by Compromise	**T1059** Command and Scripting Interpreter	**T1574** Hijack Execution Flow	**T1574.001** DLL
T1036 Masquerading	**T1497** Virtualization/Sandbox Evasion	**T1140** Deobfuscate/Decode Files or Information	**T1027** Obfuscated Files or Information

T1095 Non-Application Layer Protocol	**T1010** Application Window Discovery	**T1071** Application Layer Protocol	**T1083** File and Directory Discovery
T1082 System Information Discovery	**T1560** Archive Collected Data	**T1573** Encrypted Channel	**T1105** Ingress Tool Transfer

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	acbaa6041286f9e3c815cd1712771a490530f52c90ce64da20f28cfa0955a5ca, 15b644b42edce646e8ba69a677edcb09ec752e6e7920fd982979c714aece3925
Domains	Explorationmsn[.]store, Snailyeductyi[.]sbs, Ferrycheatyk[.]sbs, Deepymouthi[.]sbs, Wrigglesight[.]sbs, Captaitwik[.]sbs, Sidercotay[.]sbs, Heroicmint[.]sbs, monstourtu[.]sbs
MD5	bbc7fc957d4fff6a55bd004a3d124dda
Filename	Launch.exe

References

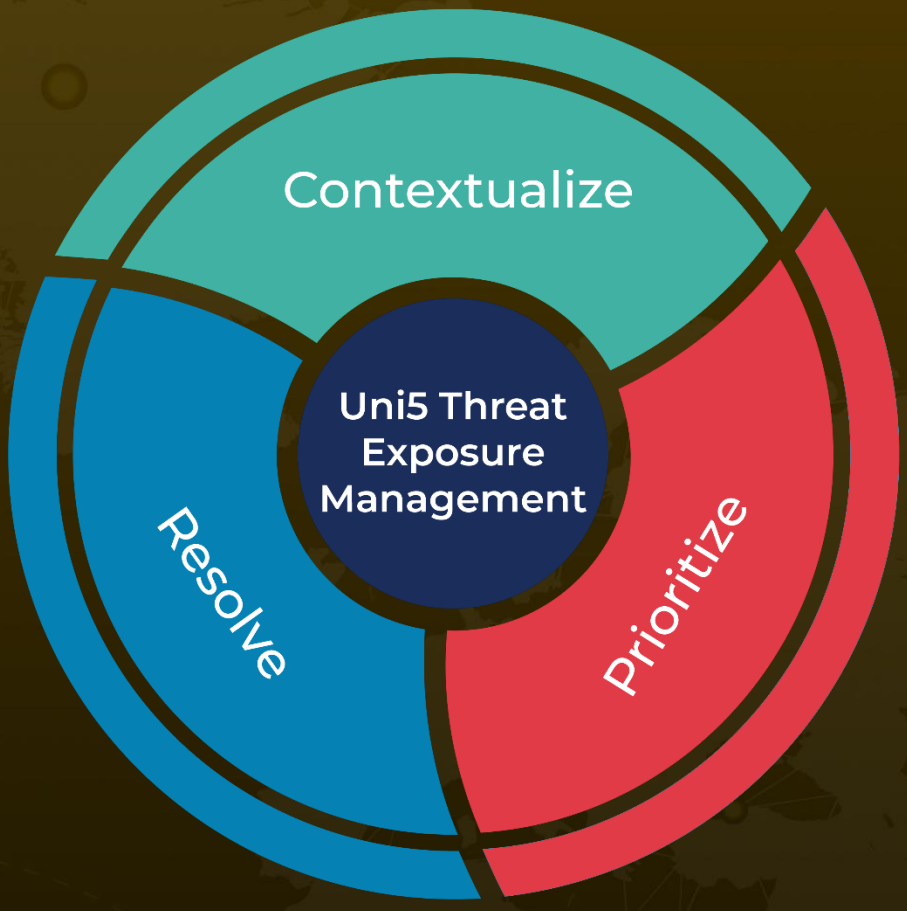
https://www.cyfirma.com/research/github-abused-to-spread-malware-disguised-as-free-vpn/

https://hivepro.com/threat-advisory/malware-as-a-service-in-action-lumma-stealers-expanding-attack-methods/

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

July 11, 2025 • 4:40 AM

More at www.hivepro.com