Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

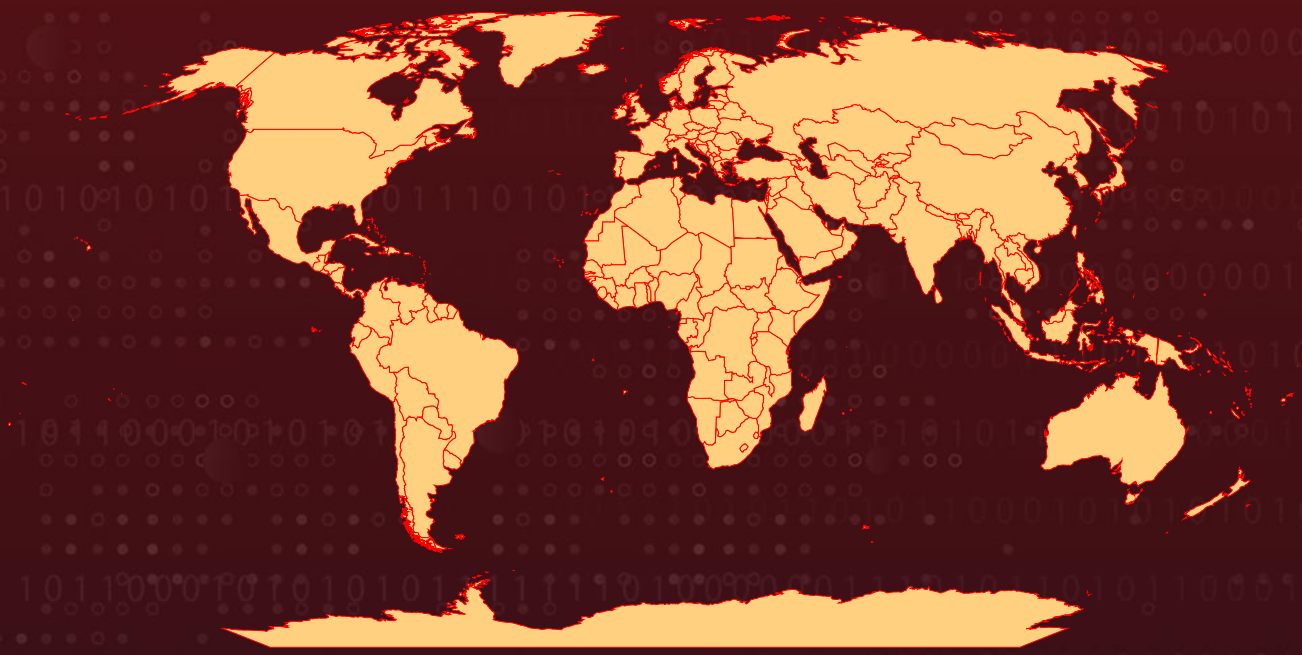
GhostPoster: A Multi-Stage Malware Campaign Hiding Inside Firefox Extensions

Date of Publication	Admiralty Code	TA Number
December 19, 2025	A1	TA2025385

Summary

Attack Discovered: September 2025
Targeted Region: Worldwide
Malware: GhostPoster
Campaign: GhostPoster
Attack: GhostPoster is a stealthy malware campaign that abuses trusted Firefox extensions to compromise users at scale, hiding malicious JavaScript inside PNG logo files using steganography. Active since September 2025, the operation spread through 17 extensions published on Mozilla's official Add-ons marketplace and has already affected more than 50,000 users by posing as legitimate tools such as free VPNs, translators, weather apps, and ad blockers. The attack unfolds in stages, with hidden code extracted from the extension's logo acting as a loader that quietly contacts attacker-controlled servers using delayed and randomized check-ins to evade detection. Once active, the final payload manipulates browser behavior for profit by hijacking affiliate links, injecting tracking, stripping security headers, bypassing CAPTCHA, and embedding hidden iframes, effectively turning the victim's browser into a monetization platform without their knowledge.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

Attack Details

#1 Browser extensions often rely on familiar logos to signal legitimacy and build user trust. GhostPoster is a sophisticated malware campaign leveraging steganographic techniques to conceal malicious JavaScript payloads within PNG icon files of Firefox browser extensions. First observed in September 2025, the campaign distributed 17 malicious extensions through Mozilla's official Firefox Add-ons marketplace, collectively infecting over 50,000 users. The extensions masqueraded as legitimate utilities including VPNs, translation tools, weather forecasts, and ad blockers.

#2 Free VPN Forever has been available on the Firefox Add-ons marketplace since September 2025 and has already been installed by more than 16,000 users. It is not an isolated case. These add-ons present themselves as useful tools offering free VPN access, translation, weather updates, or ad blocking. In reality, they deliver a multi-stage malware framework that weakens browser security, monitors user activity, and can ultimately enable remote code execution.

#3 The attack unfolds in carefully designed stages. First, the extension loads its logo image and extracts hidden JavaScript code embedded inside the PNG using steganography. This hidden script acts as a loader, reaching out to attacker-controlled servers primarily liveupdt[.]com, with dealctr[.]com as a fallback to request the real payload. To avoid detection, the loader checks in only once every 48 hours and downloads the payload just 10% of the time, making its behavior appear inconsistent and harder to trace. When the payload is finally retrieved, it is decoded and encrypted using a custom method tied to the extension's unique runtime ID, allowing it to persist quietly within the browser.

#4 Once active, the final payload focuses on monetizing and exploiting the user's browsing activity without consent. It hijacks affiliate links to divert commissions, injects stealthy tracking using analytics frameworks, removes security headers from websites, bypasses CAPTCHA protections, and plants hidden iframes to support ad and click fraud. These actions erode browser defenses across every site the user visits, all while remaining largely invisible. The real danger lies not in one flashy trick, but in the extension's broad and persistent access to the browser environment.

#5 This campaign reflects a familiar and troubling pattern, particularly among free VPN extensions that promise privacy but deliver surveillance instead. GhostPoster stands out because of its layered evasion techniques and its scale, tens of thousands of active users unknowingly granting attackers deep browser access. These malicious extensions are still available on the Firefox marketplace, underscoring the need for stronger detection. The campaign has directly impacted over 50,000 Firefox users globally. The malware strips critical browser security headers from ALL websites visited, exponentially increasing exposure to secondary attacks. Steganography is no longer a niche tactic and is appearing in many recent campaigns, making awareness of hidden threats in seemingly benign files increasingly important.

Recommendations

Be Selective with Browser Extensions: Users should think carefully before installing browser extensions, especially those offering free VPNs, ad blocking, or other "too good to be free" services. Always review the extension's publisher, update history, and user feedback. If an add-on requests broad access to all websites or browser data without a clear explanation, it should be considered a red flag.

Limit Extensions in Work Environments: Organizations should avoid allowing unrestricted installation of browser extensions on corporate systems. Using allow-lists and approving only trusted, business-necessary add-ons can significantly reduce risk. Periodic reviews of installed extensions help ensure that outdated or unnecessary tools are removed before they become a security liability.

Rethink Visual Trust Signals: Logos, high download numbers, and featured listings can create a false sense of safety. This campaign shows that even familiar-looking extensions can hide serious threats. Treat the browser as a critical attack surface and keep extension usage minimal to reduce exposure and protect privacy.

Regularly Review and Remove Unused Add-ons: Users should periodically audit their installed extensions and remove those they no longer use. Sudden changes in browsing behavior, such as excessive ads, redirects, or slower performance, can be warning signs of malicious activity and should be investigated promptly.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0009 Collection	TA0011 Command and Control	T1189 Drive-by Compromise	T1204 User Execution
T1204.001 Malicious Link	T1176 Software Extensions	T1027 Obfuscated Files or Information	T1027.003 Steganography

T1140 Deobfuscate/Decode Files or Information	T1071 Application Layer Protocol	T1071.001 Web Protocols	T1104 Multi-Stage Channels
T1185 Browser Session Hijacking	T1059 Command and Scripting Interpreter	T1059.007 JavaScript	

Indicators of Compromise (IOCs)

TYPE	VALUE
Extensions	free-vpn-forever, screenshot-saved-easy, weather-best-forecast, crxmouse-gesture, cache-fast-site-loader, freemp3downloader, google-translate-right-clicks, google-traductor-esp, world-wide-vpn, dark-reader-for-ff, translator-gbbd, i-like-weather, google-translate-pro-extension, 谷歌-翻译, libretv-watch-free-videos, ad-stop, right-click-google-translate
Domains	www[.]liveupdt[.]com, www[.]dealctr[.]com, mitarchive[.]info, refeuficn[.]github[.]io

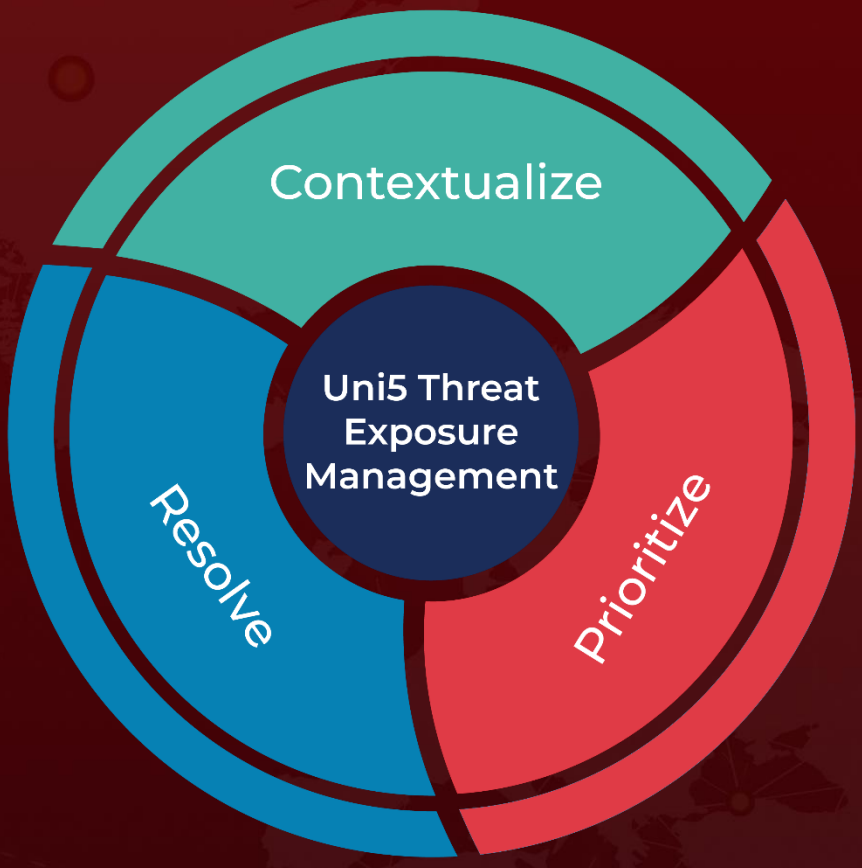
References

https://www.koi.ai/blog/inside-ghostposter-how-a-png-icon-infected-50-000-firefox-browser-users#intro

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

December 19, 2025 • 7:00 AM

© 2025 All Rights are Reserved by Hive Pro

More at www.hivepro.com