ultraviolet

THREAT ADVISORY

Browser Extension Threats

Services Performed By:
UltraViolet Cyber TIDE Team
tide@uvcyber.com

Published Date:
July 1, 2026
TLP:GREEN

Executive Snapshot

Three browser extension campaigns disclosed in late June 2026 confirm that extensions are now a mature, scalable attack surface reaching enterprise environments: a fake Perplexity Chrome extension intercepted user searches and address bar input, the Silent Swap campaign silently injected a counterfeit Google Notes extension to reroute cryptocurrency transactions, and Microsoft removed 119 Edge extensions that hid malware in image and font files to steal credentials and conduct ad fraud across up to 2.6 million installs. The common thread is the abuse of legitimate over-broad permissions and advanced evasion that defeats store review, including sideloading methods that bypass official marketplaces entirely, with payloads capable of credential theft, session hijacking that bypasses multifactor authentication, and irreversible financial loss. Extensions should be treated as first-class endpoints and governed with the same rigor as any other third-party software through the following internally owned actions:

- Enforce an approved-extension allow-list through browser enterprise policy and disable developer mode and sideloading on all managed devices to close both the store-based and installer-based infection paths.
- Deploy phishing-resistant authentication such as hardware security keys for corporate accounts, since these campaigns are proven to steal passwords and SMS-based second-factor codes.
- Establish continuous internal monitoring for changed browser search or proxy settings, anomalous extension permissions, and outbound traffic to unfamiliar domains, and rotate any credentials or secrets handled while a suspect extension was active.

TIDE Team Analysis

Browser extensions have emerged as one of the most persistent and underestimated attack surfaces in the enterprise, and three recent campaigns disclosed in June 2026 illustrate how varied and mature the threat has become. In the first case, a Chrome extension impersonating the AI search engine Perplexity quietly routed every user query, and every character typed into the address bar, through an attacker-controlled server before redirecting to legitimate results. In the second, McAfee documented a cryptocurrency clipper campaign dubbed Silent Swap that silently injects a fake Google Notes extension into Chromium browsers to swap copied wallet addresses. In the third, Microsoft removed 119 Edge extensions attributed to a single long-running threat actor operating since at least 2021, which concealed malicious payloads inside image and font files to steal credentials and conduct ad fraud across an install base of up to 2.6 million users. Together these cases signal that extensions are being weaponized at scale, across browsers, and against both consumers and the enterprise endpoints that share the same profiles.

The unifying theme is the abuse of legitimate, over-broad permissions. Extensions routinely request access to all URLs, browsing history, the clipboard, and search-provider settings, capabilities that are indistinguishable from those a genuine productivity tool might need. The fake Perplexity extension leveraged Chrome's sanctioned search-override and declarativeNetRequest features to intercept traffic; Silent Swap requested clipboard, all-URL, and history access to reroute transactions; and the StegoAd Edge extensions operated as ad blockers, VPNs, and translators that performed their advertised function while running credential theft underneath. Because these permissions are granted at install and are legitimately used by benign software, traditional allow-lists and user judgment provide weak protection. The permission model itself is the vulnerability that all three actors exploited.

Evasion and stealth have advanced to the point where store review and static analysis are no longer reliable gatekeepers. The StegoAd operation is the clearest example: it hid executable code after the IEND marker of PNG icons, later migrating to WebP images and WOFF2 font glyph ranges, and layered in multi-day install delays, server-side validation, a ten percent execution gate, and extended dormancy when developer tools were detected. Its command-and-control servers returned empty decoy responses to anyone probing directly, including researchers. Silent Swap similarly used the EtherHiding technique, storing its C2 address in a blockchain smart contract so operators can rotate infrastructure with a single transaction rather than redeploying malware. These techniques let malicious extensions live in official stores for years and defeat both automated scanning and manual review.

A second infection pathway bypasses the stores entirely. Silent Swap is delivered through unsigned .NET and Golang installers that terminate the browser, modify the protected Secure Preferences and Preferences files, and recalculate the integrity hashes so the browser believes the extension was installed legitimately. This sideloading approach, which in newer browser versions depends on socially engineering the user into enabling developer mode, means an endpoint can be compromised without any interaction with the Chrome Web Store or Edge Add-ons marketplace. For enterprises, this defeats the common assumption that restricting installs to official stores is sufficient, and it places the threat squarely in the domain of endpoint and installer controls rather than browser policy alone.

The business impact spans direct financial loss, credential compromise, and lateral risk to corporate systems. The clipper campaigns cause irreversible cryptocurrency theft and, in the VPN Go variants reported by Socket, exfiltrate any copied secret, including passwords, authentication codes, API keys, OAuth tokens, and seed phrases. StegoAd went considerably further, deploying a remote code execution backdoor, stealing Google credentials and second-factor codes at sign-in, harvesting WordPress admin logins, and exfiltrating session cookies in bulk for account takeover. Any of these outcomes on a managed device can translate into compromised corporate SaaS accounts, hijacked sessions that bypass multifactor authentication, and a foothold for broader intrusion. The AI-branding trend is a notable amplifier: Microsoft has tied related chat-skimming extensions to roughly 900,000 installs across more than 20,000 corporate networks, confirming these campaigns are reaching enterprise environments at meaningful

scale.

For security leadership, the practical implication is that browser extensions warrant the same governance rigor applied to other third-party software. Recommended controls include enforcing an approved-extension allow-list through browser enterprise policy, disabling developer mode and sideloading on managed devices, and monitoring for changed search or proxy settings, anomalous extension permissions, and traffic to unfamiliar domains. Given that these campaigns steal credentials and second-factor codes, phishing-resistant authentication such as hardware security keys should be prioritized over SMS-based codes, which the StegoAd payloads defeated. Organizations should also treat any secret handled while a compromised extension was active as exposed and rotate it accordingly. The broader lesson from all three disclosures is that the browser is now a first-class endpoint, and extension activity must be inventoried, restricted, and monitored as deliberately as any installed application.

Why It Matters

Malicious browser extensions are not a new phenomenon, but the threat has evolved steadily from opportunistic nuisance to organized, persistent operation. Early malicious extensions were dominated by adware and search hijacking, simple monetization schemes that injected ads or redirected queries for affiliate revenue. Over time, attackers recognized that the browser sits at the center of nearly all sensitive activity, from banking and email to corporate SaaS and administrative consoles, and that the extension permission model grants sweeping access to that activity with a single user click. This drove a shift toward credential theft, session cookie exfiltration, and financial fraud. The campaigns disclosed in June 2026 show how far the tradecraft has matured: the StegoAd operation ran for roughly five years across more than a hundred extensions, hiding code inside image and font files and layering in delayed execution, analyst-detection checks, and decoy server responses to survive both store review and researcher scrutiny. The Silent Swap clipper, meanwhile, abandoned fragile hard-coded infrastructure in favor of blockchain-resolved command-and-control and sideloading that tampers with protected browser files to bypass the official stores entirely. What began as annoying but low-stakes activity is now a professionalized supply-chain problem with real footholds in enterprise networks.

The trajectory points toward greater stealth, faster infrastructure rotation, and more convincing social engineering, which matters because the controls many organizations rely on are increasingly insufficient on their own. AI branding has become a powerful lure, exploiting the rush to adopt new tools, and related chat-skimming extensions have already reached tens of thousands of corporate networks. Blockchain-based C2 and abuse of trusted platforms such as Cloudflare Workers and GitHub Pages make takedowns harder and let operators outlast disruption. As browsers themselves become platforms for AI agents and automated workflows, the potential blast radius of a compromised extension grows accordingly, extending from passive data theft toward active manipulation of the actions those agents take on a user's behalf. For enterprises, the implication is that store-based trust and user judgment can no longer be the primary line of defense. Browser extensions must be inventoried, restricted, and monitored as deliberately as any installed application, and security programs should assume that the next generation of these campaigns will be harder to detect and quicker to adapt than the ones seen today.

How to Respond

- Strictly adhere to cybersecurity fundamentals and ensure all personnel undergo annual phishing and social engineering training. Speak with your UltraViolet Cyber TAM Representative to schedule a live phishing engagement.
- Enforce a browser extension allow list through your Authorized User Agreement and global policies.
- Perform annual tech refresh reviews to gain a holistic understanding of your infrastructure. Speak with your UltraViolet Cyber TAM Representative to schedule a RedTeam or PurpleTeam engagement to gain insight into the vulnerabilities in your environment.

What UltraViolet Cyber is Doing

- Tracking new CVEs and high impact vulnerabilities, analyzing and deploying public Proof-Of-Concept code against custom built targets.
- Proactively enabling custom detections based on the collected artifacts, tactics, techniques, and procedures identified in this activity.
- Performing hypothesis driven threat hunts based on threat actor behavior and artifacts. UVCyber customers will be informed of the results through secure channels.
- Parsing available victim dump data for any social, financial, business, or technical relations to UVCyber Clients and partner organizations.
- Aggregating threat intelligence from myriad sources and applying the most up-to-date knowledge to proactive threat hunting and response.

About UltraViolet Cyber

UltraViolet Cyber is a leading tech-enabled managed security services provider, delivering unparalleled cybersecurity expertise that fills technology and talent gaps across Global 2000 and Federal Government customers. Founded and operated by security practitioners from the national intelligence community, UltraViolet Cyber connects offensive security, application security, detection and response, and security engineering to deliver a differentiated approach to cybersecurity operations. Transforming customers' security programs, UltraViolet Cyber's flagship security-as-a-service solution, UV Lens, removes complex operational silos, replacing them with integrated security capabilities. UltraViolet is headquartered in McLean, Virginia with technology centers across the world.

443.351.7630 / info@uvcyber.com | UltraViolet Cyber | @uv_cyber

---