ultraviolet

THREAT ADVISORY

PEEP Browser Exploit Framework

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

Published Date:
September 9 2026
TLP:GREEN

Executive Snapshot

PEEP demonstrates that the modern web browser has become a primary post-compromise attack surface, using forged Chromium integrity checks and a native-messaging bridge to turn Chrome and Edge into persistent, host-level backdoors capable of credential theft, session hijacking, and command execution once an attacker already has a foothold on a device. Because the malware operates inside a signed, trusted browser process and relies on layered persistence that survives partial remediation, organizations cannot rely solely on outsourced network and endpoint monitoring to close this gap; several of the most effective mitigations require internal policy decisions and governance changes that only the organization itself can authorize and enforce.

- **Set enterprise browser policy to disable developer mode and enforce extension allow listing.** Define which extensions are permitted via Group Policy or MDM and require business justification for any exception, since this removes the primary delivery path PEEP depends on.

- **Adopt phishing-resistant MFA (FIDO2/WebAuthn) as organizational policy for all identity and session-sensitive systems.** This limits the value of stolen session cookies and credentials even if an endpoint is already compromised.

- **Establish and communicate an internal AI tool usage policy that addresses "authorized testing" or "CTF" framing as a potential guardrail-bypass tactic.** Employees and internal developers should know that such framing is a known technique for lowering AI safety filters during malware development.

- **Require formal change management approval for any native-messaging host registration or enterprise force-install policy.** These are legitimate enterprise mechanisms that PEEP abuses directly, so ownership and sign-off should sit with IT leadership, not be left to default configurations.

TIDE Team Analysis

Researchers at SOCRadar have disclosed PEEP, a Chromium-based post-exploitation toolkit that repurposes Chrome and Edge as persistent backdoors on already-compromised hosts. Disguised as a benign extension named "Smart Bookmarks," PEEP is installed by an operator who already holds administrative or code-execution access on the target machine. Once deployed, its installer forges Chromium's Secure Preferences integrity values (protection.macs and super_mac), allowing the malicious extension to bypass Web Store verification and auto-enable without triggering the browser's normal tamper warnings. This is not an initial-access tool; it is a force multiplier for attackers who have already breached a device, and it converts a single endpoint compromise into a long-lived, browser-resident foothold.

The technical significance for enterprise environments lies in PEEP's native-messaging bridge, which extends the malware's reach beyond the browser sandbox into full host control. A companion binary (nm_host.exe) executes shell commands, manages files, and enumerates processes and services, all triggered through the browser's trusted, signed process. Because this activity runs inside a legitimate Chrome or Edge binary, conventional endpoint detection tuned to flag unsigned or newly introduced executables is far less likely to catch it. PEEP layers four independent persistence mechanisms, including a ScriptCache-based technique that lets a previously compiled malicious service worker survive even after the on-disk source files are overwritten with clean code, meaning a single remediation step will not fully evict it.

Operationally, PEEP beacons to a hardcoded command-and-control IP every 30 seconds over unencrypted HTTP, continuously harvesting session cookies, browsing history, active-tab metadata, and credential-like form data, while accepting broader tasking for screenshots, clipboard capture, JavaScript injection, and proxy manipulation. This combination directly threatens session integrity and identity infrastructure: stolen cookies and credentials enable session hijacking and lateral movement that can bypass MFA controls entirely if session tokens are reused before expiry. The toolkit is built on the open-source RedExt framework, which has separately surfaced in GlassWorm campaigns, indicating that browser-extension-based tradecraft is proliferating and being iterated on rather than remaining a one-off proof of concept.

Attribution remains unconfirmed, but Traditional Chinese-language QA artifacts recovered from an exposed staging server point to a Chinese-speaking developer or operator with moderate confidence. SOCRadar also found artifacts suggesting the operator used an "authorized CTF" pretext, possibly to reduce safety guardrails in AI coding tools during development. Operational security on the actor's side was notably poor: the C2 infrastructure exposed its own private signing key, source code, and build history via an open directory.

For enterprise defense, this threat argues for control at four levels. First, block the known C2 IP and domain at the network egress layer. Second, harden browser policy by disabling developer mode, enforcing strict extension allow-listing through GPO or MDM, and restricting native-messaging host registration to approved binaries only. Third, deploy EDR rules that flag non-browser processes, particularly PowerShell, writing to Secure Preferences or attempting HMAC manipulation, since this is the headline defense-evasion technique that lets the malicious extension pass Chromium's own integrity check. Fourth, adopt phishing-resistant MFA and app-bound encryption for browser-stored credentials and session tokens, since PEEP is designed specifically to steal and reuse them. The broader lesson is that the browser has become a first-class attack surface requiring host-level telemetry and native-messaging monitoring, not just URL filtering and marketplace reputation checks.

Why It Matters

Browser extensions have been a soft target for attackers for well over a decade, but the nature of that abuse has shifted substantially. Early browser-based threats were largely opportunistic: adware injected into legitimate-looking extensions, ad-fraud toolbars distributed through bundling, and simple credential-stealing scripts pushed through compromised Web Store listings. These campaigns relied on tricking users or slipping past marketplace review, and their impact was mostly confined to the browser itself, harvesting cookies, tracking browsing habits, or hijacking ad revenue. What PEEP represents is the maturation of that lineage into a purpose-built, post-compromise framework that assumes the attacker already has a foothold and uses the browser not as the target but as a durable, low-visibility pivot into the operating system itself.

The emergence of open-source frameworks like RedExt, and derivatives such as PEEP and its prior use in GlassWorm campaigns, signals that browser-based command-and-control is becoming productized and reusable rather than bespoke. This mirrors a pattern seen elsewhere in the threat landscape: once a capability is published as a research or red-team tool, it gets forked, extended, and operationalized by less sophisticated actors who inherit years of tradecraft refinement for free. PEEP's native-messaging bridge, its four-layer persistence model, and its Secure Preferences forgery technique all show a level of engineering investment that would have been uneconomical for a single-use campaign, but becomes worthwhile once built as a reusable platform. The apparent use of AI-assisted development and "authorized testing" framing to work around AI coding safety filters further suggests that the barrier to building these frameworks is dropping, letting a wider pool of developers produce capabilities that previously required specialized offensive security expertise.

Looking forward, defenders should expect browser-based post-exploitation frameworks to keep expanding in scope and stealth, particularly as browsers increasingly serve as the primary interface for enterprise SaaS, identity federation, and even emerging agentic AI workflows. As enterprises push more identity and session logic into the browser through SSO, passkeys, and browser-native security controls, that same surface becomes more valuable to attackers who can bridge the sandbox to the host, as PEEP already does. Future iterations are likely to add encrypted C2 channels, better operational security than PEEP's own exposed staging server, and possibly cross-browser or cross-platform support given the Linux tooling already found in this campaign. Organizations should treat browser telemetry and native-messaging host activity as a first-class monitoring priority going forward, not an afterthought bolted onto endpoint and network defenses.

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.
- Set enterprise browser policy to disable developer mode and enforce extension allow listing. Define which extensions are permitted via Group Policy or MDM and require business justification for any exception, since this removes the primary delivery path PEEP depends on.
- Perform annual tech refresh reviews to gain a holistic understanding of your infrastructure. Speak with your UltraViolet Cyber TAM Representative to schedule a Red Team or Purple Team 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

---