Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

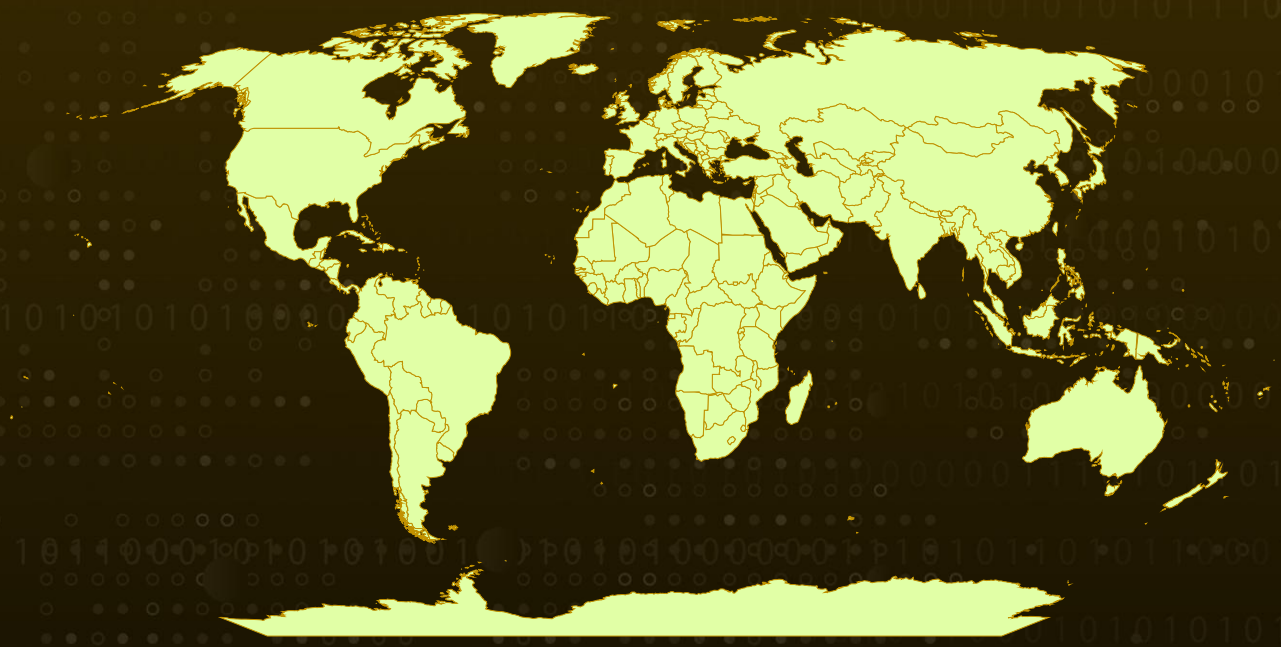
PEEP: The Bookmark Extension That Backdoors Your PC

Date of Publication	Admiralty Code	TA Number
September 09, 2026	A1	TA2026263

Summary

First Seen: 2026
Targeted Regions: Worldwide
Malware: PEEP
Attack: PEEP is a Chromium-based post-compromise toolkit that disguises itself as a "Smart Bookmarks" browser extension and quietly turns Chrome or Edge into a full backdoor. It has no way into a machine on its own; the operator must already hold code execution or administrative access, but once installed, it forges the browser's own integrity checks to load without prompts, beacons to its command server every 30 seconds over plain HTTP, and steals session cookies, browsing history, form data, and clipboard contents. A native-messaging companion (nm_host.exe) then bridges the browser to the operating system, letting the attacker run shell commands, move files, and enumerate processes and services. Built on the open-source RedExt framework, PEEP layers four persistence tricks so that removing the visible extension alone won't clear the infection.

Attack Regions



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

Targeted Non-Targeted

Attack Details

#1

PEEP is a Chromium-based post-exploitation toolkit disguised as a "Smart Bookmarks" extension, and it needs prior administrative or code-execution access to land, it is not an initial-access tool. With that foothold, its installer injects the extension directly into Chrome or Edge profiles, bypassing Web Store checks and user prompts by forging Chromium's Secure Preferences integrity values. In practice, PowerShell scripts rewrite the per-entry HMAC-SHA256 values and the top-level super_mac so the browser's integrity check passes and the sideloaded extension auto-enables at launch. If that route is blocked, the operator falls back on enterprise force-install policies or plain sideloading.

#2

Once the browser starts, the Manifest V3 service worker reads its hardcoded config for C2 details and begins automated collection, while a content script injects into every open page. The real escalation is the native-messaging host com.peep.lab, a Node.js binary packed as nm_host.exe. Browser-only tasks like screenshots or JavaScript injection run inside the extension, but anything that needs the operating system is handed to this host, which turns a browser spy into a remote-access tool. Persistence is stacked across four mechanisms: the forged Secure Preferences state, an enterprise force-install policy, the registered native host, and a "Ghost Anchor" ScriptCache trick that reloads a previously compiled malicious worker even after the on-disk files are swapped for clean shells. No single cleanup step removes all of it.

#3

Running in the logged-in user's context, with no privilege escalation, PEEP collects session cookies, browsing history, and open tabs every cycle, and grabs password-like fields the moment a form is submitted. On command, it dumps page content, local and session storage, clipboard text, downloads, and screenshots, and inventories installed extensions. Through the native host, it enumerates processes and services, searches and reads files, and runs shell commands via cmd, PowerShell, or bash. The stolen cookies are the sharpest edge: a valid one proves the user is already signed in, letting an attacker replay it into accounts without a password and often without a fresh MFA prompt until the session is revoked.

#4

Everything funnels back to a single host. The agent beacons over unencrypted HTTP to the hardcoded IP 206[.]237[.]30[.]232, fronted by xfjcc[.]fun in AS55933 polling /api/commands for tasks. Auto-collected data posts to /api/exfil and command results to /api/agents/<id>/task_result, with registration, heartbeats, and payload updates handled through /api/register, /api/agents/<id>/heartbeat, /api/extension_update/, and /api/extension_crx/. The control panel runs on TCP port 5001 (Flask and SQLite), with an exposed development and staging repository on port 5002. The native host's code supports AES-256-GCM, but the shipped configuration never uses it, so the channel stays in the clear, a notable weakness for an otherwise capable toolkit.

Recommendations

Block PEEP's C2 and Staging Infrastructure: Add blocking rules at the network perimeter and egress firewalls for the IP 206[.]237[.]30[.]232 and the domain xfjcc[.]fun along with its new[.], newadmin[.], and newapi[.] subdomains. Restrict and monitor traffic to TCP ports 5001 (control panel and agent API) and 5002 (open staging directory) to cut off both command polling and payload delivery.

Force-Remove the Malicious Extensions and Host: Use enterprise management policies to identify and force-uninstall extension IDs ejkndncpkdcjcikfhiamcdehdoegilbj (the primary "Smart Bookmarks" payload) and bibjjhidpdmfcbkodddndmoejcloobdh (the smoke-agent variant). Delete the native-messaging registration under NativeMessagingHosts\com.peep.lab, remove nm_host.exe, and clear the staging path at %LOCALAPPDATA%\PEEP.

Watch for Secure Preferences Tampering: Configure EDR rules to flag writes to the browser's Secure Preferences file by anything other than the browser itself, especially PowerShell, and alert on manipulation of protection.macs or super_mac values, which is the headline technique behind PEEP's silent install.

Lock Down Browser Extension Policy: Enforce strict extension allow-listing through Group Policy or MDM, disable developer mode across the enterprise, restrict external sideloading, and permit only approved corporate binaries as native-messaging hosts.

Protect Sessions and Stored Credentials: Turn on App-Bound Encryption to shield cookies and browser storage from process-level theft, and require phishing-resistant MFA such as FIDO2 or WebAuthn hardware keys to blunt session hijacking and credential replay.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1583: Acquire Infrastructure	
	T1587: Develop Capabilities	T1587.001: Malware
Persistence	T1176: Browser Extensions	
Execution	T1059: Command and Scriptinsg Interpreter	T1059.001: PowerShell
		T1059.003: Windows Command Shell
		T1059.007: JavaScript
Defense Evasion	T1553: Subvert Trust Controls	
	T1112: Modify Registry	
	T1036: Masquerading	
	T1027: Obfuscated Files or Information	
Credential Access	T1539: Steal Web Session Cookie	

Tactic	Technique	Sub-technique
Credential Access	T1056: Input Capture	T1056.003: Web Portal Capture
	T1115: Clipboard Data	
Discovery	T1057: Process Discovery	
	T1007: System Service Discovery	
	T1083: File and Directory Discovery	
	T1518: Software Discovery	
	T1217: Browser Information Discovery	
Collection	T1113: Screen Capture	
	T1005: Data from Local System	
	T1119: Automated Collection	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1571: Non-Standard Port	
	T1105: Ingress Tool Transfer	
	T1090: Proxy	
Exfiltration	T1041: Exfiltration Over C2 Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	86a5fb2f14d175d1c13a7b49b55b968b2a5e96afc944d85a31b3db906af00beb, 6700e30a3224248085d30f2eb727cea28dec288355fca6753449a26d1c1d1eee, 9402c0198ae5c8bed14cdeaabe7e8b25625debbc62a900cfcdb82d34a35ab528, 8edd653910f3217c96a603e8ce9e5e409d3b8674476f22e0a3afe870bf3870b1, 87db7138a80117ddf2989827c1dde09ee73c7a252d511c74ed66af2fe34e2987, 259d8eddb6caf509d7bffa2b4c0dd7d89668800c870f529729ac2efdc1853fb6, e46aee4ca43ba66666f6572c62365cf57642f2cf1f6eca00fcf8eb33a291d66d, f031c00f592aa5e98893b4532f743362fed7fb0a485e8a3c0ad4de677f1d7415, a43bf7f81507c8f9d0942fed331e7590a43044a6d219ec1005974bf1a819774a1, b4e3ca8f44477b9ade1272f92516202f83a80219c8bd6176527a6d624214e893, 8e988b915b75dd749e3f4e1ca7ee21746885b4fe34e8a246e6f10f5d892a675f, 9c6b269e5087a40b4552f72e9ff13d9b39e433af5075ad68f57e9b5240a590d8, 207e0d47c4e5493ef7313eb1faeb1c6195923c89f263e548609a6838dd91ec0c
IPv4	206[.]237[.]30[.]232
Domains	xfjcc[.]fun, new[.]xfjcc[.]fun, newadmin[.]xfjcc[.]fun, newapi[.]xfjcc[.]fun
HTTP Header	X-PEEP-Agent-Key, X-PEEP-Agent-Id, realm="PEEP"

TYPE	VALUE
Extension ID	ejkndncpkdcjcikfhiamcdehdoegilbj, bibjjhidpdmfcbkodddndmoejcloobdh, hpjgilbbdmfcnaapjbofmmmjjfijbdki, akhljhifabhkcoboncoiekfpdodjaack, eljagiodakpnjbaceijefgmidmpmfimg
Native Messaging Host	com.peep.lab
Agent Key	a6dfab5a6e510ece, 348e99545a69b184
Encryption Key	peep_nm_host_aes256_key_32bytes!

References

https://socradar.io/blog/peep-browser-rat-chrome-extension/

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

September 09, 2026 • 09:20 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com