

# PEEP: A Browser RAT Disguised as a Malicious Chrome Extension Threat Campaign

 [socradar.io/free-tools/campaigns/1881](https://socradar.io/free-tools/campaigns/1881)

SOCRadar

[Back to Campaigns](#)



## China-NexusBrowser-RATRedExt-Derived

SOCRadar's Threat Research Unit STRU identified and analyzed PEEP, a Chromium based post exploitation toolkit disguised as a Smart Bookmarks extension. Requiring prior administrative or code execution access, its PowerShell installer injects the extension into Chrome and Edge profiles by forging Chromium's Secure Preferences integrity values, bypassing Web Store checks and user prompts. A native messaging bridge extends it to host level shell, filesystem, and process control. The agent beacons every 30 seconds over plaintext HTTP, exfiltrating session cookies, browsing history, and tab metadata via 37 commands. Built on the open source RedExt framework as a RedExt derived toolkit. An exposed

## Indicators of Compromise

---

### Campaign Guidance

---

Remediation, mitigation, notes, history and related intelligence

#### Recommendations

- **Block C2 and Staging Infrastructure:** Implement immediate blocking rules at network perimeters and egress firewalls for IP address 206.237.30[.]232 across all traffic. Restrict and monitor access to TCP ports 5001 (control panel and agent API) and 5002 (open staging directory and payload distribution) to prevent command polling and payload delivery.
- **Inventory and Remove Malicious Tools:** Deploy enterprise management policies to identify and force-uninstall extension IDs ejkndncpkdcjckfhiamcdehdoegilbj (primary "Smart Bookmarks" payload) and bibjjhidpdmfcbkoddndmoejcloobdh (secondary variant). Purge associated registry keys under NativeMessagingHosts\com.peep.lab and remove host binary artifacts (nm\_host.exe) alongside local staging paths in %LOCALAPPDATA%\PEEP\.
- **Harden Browser Security Policy:** Enforce strict Chromium extension allow-listing via Group Policy (GPO) or MDM solutions. Explicitly disable developer mode (developer\_mode = false) enterprise-wide, restrict external sideloading permissions, and limit allowed native-messaging hosts exclusively to approved corporate binaries.
- **Deploy Host-Level Integrity Detection:** Configure Endpoint Detection and Response (EDR) rules to detect unauthorized modifications to browser Secure Preferences files, particularly writes initiated by non-browser utilities like PowerShell. Flag process activity attempting HMAC forgery (e.g., manipulation of protection.macs or super\_mac).
- **Protect Identity and Session Credentials:** Use App-Bound Encryption to protect browser storage and session cookies from process-level theft. Require phishing-resistant MFA (e.g., FIDO2/WebAuthn hardware keys) to prevent session hijacking and credential harvesting.

### Observed Countries250

---