INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-07-01 07:08 UTC

Browser Extension Threats Converge: Blockchain-Resilient Clipboard Hijacking and Staged Malicious Updates Target Crypto Users Globally

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0605
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Google Chrome, Microsoft Edge, Brave, Vivaldi, Opera, Mozilla Firefox, Chromium-based browsers; Windows endpoints (.NET and Golang installer variants); Bitcoin, Ethereum, Bitcoin Cash, Ripple, Dash, Solana
Published	2026-06-30T11:40:18
Discovery Source	Rss

Executive Summary

Two active browser extension campaigns are stealing cryptocurrency from users mid-transaction by intercepting and replacing wallet addresses copied to the clipboard. The first campaign, Silent Swap, uses blockchain-based C2 infrastructure to complicate traditional domain-takedown mitigation and installs a fake Google Notes extension without user consent; the second smuggled clipboard-theft code into VPN extensions on the Chrome Web Store and Firefox Add-ons store through post-publication updates. Any organization or individual conducting cryptocurrency transactions on Windows endpoints using Chromium-based browsers or Firefox faces direct risk of irreversible financial loss, as blockchain transactions cannot be reversed once submitted to a compromised address.

Technical Analysis

Two concurrent clipboard-hijacking campaigns target cryptocurrency wallet addresses across Bitcoin, Ethereum, Bitcoin Cash, Ripple, Dash, and Solana on Windows endpoints.

Campaign 1, Silent Swap (reported by The Hacker News citing McAfee Labs, linked to CountLoader):

- Deploys a fake 'Google Notes' extension by tampering with browser preference files, bypassing user consent (T1176, T1553)

- Uses blockchain-based C2 resolution to retrieve replacement wallet addresses, complicating traditional domain-takedown mitigation (T1568)

- Intercepts clipboard content at the moment of wallet address paste, silently substituting the attacker's address (T1115)

- Installer variants observed in both .NET and Golang; obfuscation noted (T1027)

- C2 communications use standard application-layer protocols to blend with legitimate traffic (T1071.001)

- Indicator cleanup observed post-execution (T1070.004)

Campaign 2, Malicious VPN Extensions (reported by The Hacker News citing Socket, operator unattributed):

- Extensions initially passed Chrome Web Store and Firefox Add-ons store review as benign

- Clipboard theft functionality introduced via staged post-publication updates, a deliberate supply chain evasion technique

- Exploits the trust gap between initial store vetting and subsequent extension updates (T1195.002)

- Defense evasion via disabling or bypassing security controls (T1562.001); non-standard port usage possible (T1571)

- VBScript execution observed in installer chain (T1059.005)

Relevant CWEs: CWE-312 (Cleartext Storage of Sensitive Information), CWE-693 (Protection Mechanism Failure), CWE-345 (Insufficient Verification of Data Authenticity), CWE-494 (Download of Code Without Integrity Check).

No CVE IDs are assigned to these campaigns. No vendor patch is available; mitigation is configuration and policy-based.

Action Checklist

1. Audit all installed browser extensions across the fleet immediately. Remove any extension not present on an approved allowlist, with priority on extensions named 'Google Notes' or recently installed VPN tools on Chromium-based browsers and Firefox. (Containment)
2. Block browser extensions from installing via preference-file tampering by enforcing managed browser policies (CIS 2.3, Address Unauthorized Software; CIS 4.6, Securely Manage Enterprise Assets and Software). (Containment)
3. Search endpoint logs and EDR telemetry for: (a) new browser extension directories created without a corresponding user-initiated install event; (b) clipboard access by browser extension processes (look for extension renderer processes reading and writing clipboard in rapid succession, particularly around wallet address string patterns such as 26-62 character alphanumeric strings beginning with 1, 3, bc1, 0x, r, X, or similar cryptocurrency address prefixes); (c) outbound DNS or HTTPS requests from browser processes to blockchain RPC endpoints (e.g., Ethereum JSON-RPC, BSC nodes) not associated with known business activity. (Detection)
4. Review AU-6 (Audit Record Review, Analysis, and Reporting) and AU-12 (Audit Record Generation) controls to ensure adequate logging coverage. (Detection)
5. Deploy a browser extension allowlist via Group Policy (Chrome: ExtensionInstallAllowlist / ExtensionInstallBlocklist; Firefox: managed policies JSON) to prevent unauthorized extension installation or update. (Eradication)

6. Remove confirmed malicious extensions and associated preference file modifications. (Eradication)

7. Re-image endpoints where Silent Swap installer artifacts (.NET or Golang variants) are identified, as post-execution cleanup behavior (T1070.004) may obscure full infection scope (CIS 2.1, Establish and Maintain a Software Inventory; NIST CM, Configuration Management family). (Eradication)

8. After removing malicious extensions, verify browser preference files have been restored to a known-good state. (Recovery)

9. Confirm no unauthorized extensions reappear after browser restart. (Recovery)

10. Monitor clipboard-access events and outbound browser traffic for 72 hours post-remediation. (Recovery)

11. Notify any employees or users who conducted cryptocurrency transactions from affected endpoints during the exposure window that transactions may have been redirected; advise them to verify destination wallet addresses through an out-of-band channel against any transactions they submitted. (Recovery)

12. Review extension lifecycle controls: confirm your browser management policy blocks unsigned or unreviewed extension updates from propagating automatically without an additional approval gate. (Post-Incident)

13. Establish a recurring review cadence for approved extension versions (CIS 7.3, Perform Automated Operating System Patch Management; CIS 7.4, Perform Automated Application Patch Management). (Post-Incident)

14. Document how preference-file tampering bypassed existing endpoint controls and assess whether endpoint protection tooling needs tuning to alert on browser profile directory modifications. (Post-Incident)

15. Consider D3-UAP (User Account Permissions) to restrict which processes can write to browser profile directories. (Post-Incident)

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to legal and executive leadership if forensic review of browser history or blockchain transaction records confirms any cryptocurrency transaction was successfully redirected during the exposure window, as this constitutes confirmed financial fraud and may trigger regulatory breach notification obligations depending on jurisdiction and whether organizational funds or customer assets were involved.
Recovery Notes	After eradication, restore browser preference files from a known-good backup or a clean profile and re-validate the SHA-256 hash of the Preferences and Secure Preferences files after each browser restart for at least 72 hours to confirm no persistence mechanism is reinstating the malicious extension. Monitor Sysmon Event ID 11 under all browser extension directories and outbound browser network connections for resumed blockchain RPC endpoint contact, which would indicate incomplete eradication of the Silent Swap loader. Any user who copied a cryptocurrency wallet address on an affected endpoint during the exposure window must be treated as a potential fraud victim and advised to verify all submitted transactions on the relevant public blockchain explorer before considering recovery complete.

Forensic Artifacts	Chrome/Edge 'Preferences' and 'Secure Preferences' JSON files at '%LOCALAPPDATA%\Google\Chrome\User Data\Default\' — contain extension install timestamps, permission grants, and evidence of preference-file tampering used by Silent Swap to install the fake Google Notes extension without user consent | Browser extension directory contents at '%LOCALAPPDATA%\Google\Chrome\User Data\Default\Extensions\[extension_id]\' — the background service worker JavaScript files within this directory will contain the clipboard-interception logic, including the regex patterns targeting Bitcoin (1/3/bc1 prefix), Ethereum (0x prefix), Ripple (r prefix), and Dash (X prefix) wallet address formats | Windows Security Event Log Event ID 4688 (Process Creation) records for dotnet.exe, csc.exe, or unsigned Golang PE binaries executing from %TEMP% or %APPDATA% — these capture the .NET and Golang installer variants that deployed Silent Swap without a corresponding Chrome Web Store install event | Memory acquisition (WinPmem/DumpIt) from endpoints where Silent Swap installer artifacts are suspected — required because post-execution file cleanup (the T1070.004-style behavior noted in the advisory) may have removed the installer binary from disk, leaving injected code or the extension loader only in process memory | Outbound network connection logs (firewall, Sysmon Event ID 3, or Wireshark capture) filtered to chrome.exe, msedge.exe, or firefox.exe processes making HTTPS or DNS requests to Ethereum JSON-RPC endpoints (port 8545/8546) or BSC node hostnames — this artifact is specific to Silent Swap's blockchain-based C2 infrastructure used to retrieve replacement wallet addresses in a takedown-resilient manner

Per-Action IR Details

Containment — Audit all installed browser extensions across the fleet immediately. Remove any extension not present on an approved allowlist, with priority on extensions named 'Google Notes' or recently installed VPN tools on Chromium-based browsers and Firefox. Block browser extensions from installing via preference-file tampering by enforcing managed browser policies (CIS 2.3 — Address Unauthorized Software; CIS 4.6 — Securely Manage Enterprise Assets and Software).

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: CIS 2.3 (IG1/IG2/IG3) — Address Unauthorized Software, CIS 4.6 (IG1/IG2/IG3) — Securely Manage Enterprise Assets and Software, NIST AC-3 (Access Enforcement)

Compensating: On Windows endpoints without MDM/GPO, run: 'Get-ItemProperty HKCU:\Software\Google\Chrome\Extensions* | Select PSChildName, Path' and cross-reference against a known-good extension ID list. For Firefox, enumerate '%APPDATA%\Mozilla\Firefox\Profiles*\extensions.json' and flag any extension where 'userDisabled' is false but the ID is absent from your approved list. A 2-person team can script this across a flat network using PsExec or PowerShell remoting in under two hours.

Evidence: Before removing any extension, capture the following volatile state: (1) full copy of the Chrome/Edge 'Preferences' and 'Secure Preferences' JSON files from '%LOCALAPPDATA%\Google\Chrome\User Data\Default\' — these record extension install timestamps, permissions, and any preference-file tampering used by Silent Swap to persist without user consent; (2) enumerate running browser renderer/extension processes via 'Get-Process chrome,msedge,firefox | Select Id,Name,Path' and capture their loaded modules; (3) export the full extension directory listing from '%LOCALAPPDATA%\Google\Chrome\User Data\Default\Extensions\' with timestamps before deletion, as Silent Swap and the weaponized VPN extensions may share identical directory creation timestamps indicating coordinated staging.

Detection — Search endpoint logs and EDR telemetry for: (a) new browser extension directories created without a corresponding user-initiated install event; (b) clipboard access by browser extension processes (look for extension renderer processes reading and writing clipboard in rapid succession, particularly around wallet address string patterns such as 26–62 character alphanumeric strings beginning with 1, 3, bc1, 0x, r, X,

or similar cryptocurrency address prefixes); (c) outbound DNS or HTTPS requests from browser processes to blockchain RPC endpoints (e.g., Ethereum JSON-RPC, BSC nodes) not associated with known business activity (AU-6 — Audit Record Review, Analysis, and Reporting; AU-12 — Audit Record Generation). No confirmed IOC hashes or domains are available from current sources.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-12 (Audit Record Generation), NIST AU-2 (Event Logging)

Compensating: Deploy Sysmon with SwiftOnSecurity config and add a custom rule targeting FileCreate events under '%LOCALAPPDATA%*\Extensions\' by non-browser-installer processes (Event ID 11). For clipboard monitoring without EDR, use a lightweight PowerShell loop: 'while($true){$cb=Get-Clipboard;if($cb -match "^(1|3|bc1|0x|r|X)[a-zA-Z0-9]{25,61}$"){Write-Log $cb};Start-Sleep -Milliseconds 500}' — run as a scheduled task to detect wallet address patterns landing in clipboard and flag rapid overwrites. For network, capture browser DNS with Wireshark filter 'dns and frame contains "eth_"' or 'dns and frame contains "jsonrpc"' to surface Ethereum JSON-RPC lookups indicative of blockchain C2 infrastructure used by Silent Swap.

Evidence: This step is observational and does not alter live state; no pre-capture sequencing is required. However, preserve the following before any remediation actions follow: (1) Windows Security Event Log Event ID 4663 (Object Access — Clipboard) if object auditing is enabled; (2) browser process network connections via 'netstat -ano | findstr :443' filtered to chrome.exe or firefox.exe PIDs, cross-referenced against known Ethereum RPC ports (8545, 8546) or public BSC node hostnames; (3) Sysmon Event ID 3 (Network Connection) and Event ID 11 (FileCreate) logs from the extension staging window; (4) browser extension background service worker logs accessible at 'chrome://extensions/' developer mode console, which may contain JavaScript errors or fetch() calls to blockchain RPC endpoints made by the malicious clipboard-hijacking code.

Eradication — Deploy a browser extension allowlist via Group Policy (Chrome: ExtensionInstallAllowlist / ExtensionInstallBlocklist; Firefox: managed policies JSON) to prevent unauthorized extension installation or update. Remove confirmed malicious extensions and associated preference file modifications. Re-image endpoints where Silent Swap installer artifacts (.NET or Golang variants) are identified, as post-execution cleanup behavior (T1070.004) may obscure full infection scope (CIS 2.1 — Establish and Maintain a Software Inventory; NIST CM — Configuration Management family).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: CIS 2.1 (IG1/IG2/IG3) — Establish and Maintain a Software Inventory, CIS 2.3 (IG1/IG2/IG3) — Address Unauthorized Software, NIST AC-3 (Access Enforcement)

Compensating: For teams without GPO/MDM, manually drop a 'managed policies' JSON to '%PROGRAMFILES%\Policies\Google\Chrome\managed_policy.json' (Windows) or '/etc/chromium/policies/managed/' (Linux) enforcing 'ExtensionInstallBlocklist: ["*"]' with an explicit allowlist. For Firefox, place 'policies.json' in the Firefox installation directory under 'distribution\'. On endpoints where the .NET or Golang Silent Swap installer is suspected, run YARA against '%TEMP%', '%APPDATA%\Roaming', and '%LOCALAPPDATA%\Temp' for PE headers with Go or .NET CLR metadata combined with strings matching cryptocurrency address regex patterns before reimaging.

Evidence: Before reimaging any endpoint or deleting preference file modifications, capture: (1) a full RAM acquisition using WinPmem or DumpIt — the .NET or Golang Silent Swap installer variants may reside only in memory if cleanup behavior (file deletion post-execution) has already run, making memory the sole source for process hollowing artifacts or injected extension loader code; (2) a forensic copy of the browser 'Preferences' and 'Secure Preferences' files showing the tampered extension entries, as these constitute evidence of the preference-file injection vector; (3) Windows Security Event Log Event ID 4688 (Process Creation) records showing the .NET (csc.exe, dotnet.exe) or Golang binary execution chain that installed the Silent Swap extension without a user install event; (4) registry key 'HKCU\Software\Google\Chrome\PreferenceMACs' which Chrome uses to detect preference tampering — its state before cleanup is forensically significant.

Recovery — After removing malicious extensions, verify browser preference files have been restored to a known-good state. Confirm no unauthorized extensions reappear after browser restart. Monitor clipboard-access events and outbound browser traffic for 72 hours post-remediation. Notify any employees or users who conducted cryptocurrency transactions from affected endpoints during the exposure window that transactions may have been redirected; advise them to verify destination wallet addresses through an out-of-band channel against any transactions they submitted (AU-6 — Audit Record Review, Analysis, and Reporting).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-2 (Event Logging)

Compensating: Validate preference file integrity by comparing SHA-256 hashes of restored 'Preferences' and 'Secure Preferences' files against a known-good baseline captured from a clean browser profile on a reference machine. For the 72-hour clipboard monitoring period, repurpose the PowerShell wallet-pattern detection loop from the detection step as a scheduled task logging to a local CSV. For transaction verification, instruct users to check the raw blockchain transaction record on a public explorer (e.g., Etherscan for Ethereum, Blockchain.com for Bitcoin) for any transaction submitted during the exposure window and compare the recipient address byte-for-byte against their intended destination — clipboard hijacking swaps the entire address, so a single character mismatch confirms interception.

Evidence: Recovery does not typically destroy volatile evidence if eradication was completed correctly; however, before confirming clean state and standing down monitoring, preserve: (1) final browser extension directory listing and Preferences file snapshots as the post-remediation baseline for future comparison; (2) 72-hour window of Sysmon Event ID 11 (FileCreate) logs under extension directories to detect any persistence mechanism attempting to reinstall the malicious extension after removal; (3) outbound network logs (firewall or Sysmon Event ID 3) from browser processes for the 72-hour watch period, specifically flagging any resumed connections to blockchain RPC endpoints that would indicate the eradication was incomplete.

Post-Incident — Review extension lifecycle controls: confirm your browser management policy blocks unsigned or unreviewed extension updates from propagating automatically without an additional approval gate. Establish a recurring review cadence for approved extension versions (CIS 7.3 — Perform Automated Operating System Patch Management; CIS 7.4 — Perform Automated Application Patch Management). Document how preference-file tampering bypassed existing endpoint controls and assess whether endpoint protection tooling needs tuning to alert on browser profile directory modifications. Consider D3-UAP (User Account Permissions) to restrict which processes can write to browser profile directories.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: CIS 7.3 (IG1/IG2/IG3) — Perform Automated Operating System Patch Management, CIS 7.4 (IG1/IG2/IG3) — Perform Automated Application Patch Management, CIS 2.2 (IG1/IG2/IG3) — Ensure Authorized Software is Currently Supported, NIST AC-6 (Least Privilege)

Compensating: For teams without a formal change-approval pipeline for extensions, implement a manual version-pin policy: lock approved extension versions via GPO 'ExtensionSettings' with 'update_url' overridden to an internal proxy or 'blocked' for automatic updates, forcing a human review before any extension version bump is permitted fleet-wide. To detect future preference-file tampering, add a Sysmon rule (Event ID 11 and Event ID 1) alerting on any non-browser process writing to '%LOCALAPPDATA%\Google\Chrome\User Data\Default\Preferences' or '%APPDATA%\Mozilla\Firefox\Profiles*\extensions.json' — this directly addresses the Silent Swap installation vector. Document the gap formally in a lessons-learned report citing that the Chrome Web Store's post-publication update mechanism and preference-file write access were the two uncontrolled attack surfaces exploited in this campaign.

Evidence: Post-incident activity does not alter live endpoint state on remediated systems; evidence capture requirements here apply to any newly discovered affected systems identified during the lessons-learned review. The primary forensic output of this phase is documentation: (1) a timeline mapping extension install timestamps from Preferences files against user activity logs to establish the exposure window for each affected endpoint; (2) a record of which specific extension IDs (the weaponized VPN extensions and the fake Google Notes extension ID) were present,

to feed into threat intelligence sharing with CISA or sector ISACs; (3) endpoint protection gap analysis documenting that browser profile directory writes by non-browser processes were not alerted on, which is the specific control failure this campaign exploited.

Detection Guidance

No confirmed IOC hashes, domains, or IP addresses are available from the current source material. Organizations should request IOC data directly from McAfee Labs and Socket before implementing detection rules. The following behavioral indicators are derived from the campaign descriptions and MITRE technique mappings and should be treated as hypothesis-driven hunting guidance pending authoritative corroboration.

Clipboard hijacking pattern: Monitor for browser extension renderer processes that access the system clipboard within milliseconds of a paste event and immediately write a different value. On Windows, Sysmon Event ID 10 (ProcessAccess) targeting clipboard APIs from browser child processes, combined with clipboard content change events, is a viable detection signal.

Browser preference tampering (Silent Swap): Alert on file write events to Chrome, Edge, Brave, Vivaldi, Opera, or Firefox profile directories (e.g., '%LOCALAPPDATA%\Google\Chrome\User Data\Default\Preferences') by processes other than the browser itself. Sysmon Event ID 11 (FileCreate) or EDR file-write telemetry covering those paths is the relevant log source.

Blockchain C2 resolution: Identify outbound HTTPS or WebSocket connections from browser processes to known public blockchain RPC endpoints (Infura, Alchemy, QuickNode, or direct node IPs on ports 8545, 8546, or 443) where no business justification exists. Correlate with DNS query logs for blockchain infrastructure hostnames.

Staged extension update evasion: Compare currently installed extension versions against the version present at the time of store review or last approved baseline. A version increment without a corresponding approved-update record is a detection signal.

Recommended log sources: EDR process and file telemetry, Sysmon (Events 1, 10, 11, 22), browser management console extension audit logs, proxy/DNS logs for blockchain RPC traffic.

Relevant controls: AU-2 (Event Logging), AU-6 (Audit Record Review, Analysis, and Reporting).

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`No confirmed IOCs available from current sources`	Primary source (The Hacker News, T2) did not publish specific hashes, domains, or IPs at time of analysis. Monitor McAfee Labs and Socket security blogs for published IOC sets.	LOW

Framework Mappings

MITRE-ATTACK

- **T1571** — Non-Standard Port

- **T1562.001** — Disable or Modify Tools
- **T1027** — Obfuscated Files or Information
- **T1568** — Dynamic Resolution
- **T1176** — Software Extensions
- **T1553** — Subvert Trust Controls
- **T1115** — Clipboard Data
- **T1059.005** — Visual Basic
- **T1071.001** — Web Protocols
- **T1070.004** — File Deletion

NIST-800-53R5

- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **CM-3** — Configuration Change Control
- **SR-2** — Supply Chain Risk Management Plan

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **15.1** — Establish and Maintain an Inventory of Service Providers

NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program

ISO-27001-2022

- **A.5.21** — Managing information security in the ICT supply chain

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1571	Non-Standard Port	Command-And-Control
T1562.001	Disable or Modify Tools	Defense-Evasion
T1027	Obfuscated Files or Information	Defense-Evasion
T1568	Dynamic Resolution	Command-And-Control

Technique ID	Technique Name	Tactic
T1176	Software Extensions	Persistence
T1553	Subvert Trust Controls	Defense-Evasion
T1115	Clipboard Data	Collection
T1059.005	Visual Basic	Execution
T1071.001	Web Protocols	Command-And-Control
T1070.004	File Deletion	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/06/silent-swap-crypto-clipper-uses-f...	T2
Past Security Bulletins - Office of Information Technology	https://oit.nd.edu/cybersecurity/security-bulletin/past-security-bu...	T1
Chrome and Chromium-based browsers receive fixes for exploited ...	https://fieldeffect.com/blog/chrome-chromium-browsers-fixes-exploit...	T3
■Vulnerability Alert■Chromium-Based Browsers Have 74 High ...	https://lis.mcut.edu.tw/p/406-1013-79067,r11.php?Lang=en	T3

Generated 2026-07-01 07:08 UTC by TJS Security Command Center