INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:39 UTC

Torg Grabber: Rapidly Expanding Infostealer Targets 728 Crypto Wallet Extensions with ABE Bypass and ClickFix Delivery

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0103
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Chromium-based browsers (Chrome, Brave, Edge, Vivaldi, Opera, and 20+ others), Firefox variants (8), cryptocurrency wallet extensions (728, including MetaMask, Phantom, TrustWallet, Coinbase, Binance, Exodus, TronLink, Ronin, OKX, Keplr, Rabby), password managers and 2FA tools (103, including LastPass, 1Password, Bitwarden, KeePass, NordPass, Dashlane, ProtonPass), messaging/gaming platforms (Discord, Telegram, Steam)
Published	2026-03-25
Discovery Source	Rss

Executive Summary

Torg Grabber is a newly identified infostealer actively targeting cryptocurrency wallet browser extensions, password managers, and 2FA tools across all major browsers. Delivered via ClickFix, a clipboard-hijacking technique requiring no file download or user-executed exploit, it bypasses Chrome's App-Bound Encryption and has produced 334 unique samples in roughly 60 days, indicating rapid iteration under a likely malware-as-a-service model. Organizations face credential theft risk wherever employees use personal browser profiles or store credentials in browser-based password managers, with particular exposure for any staff holding or transacting cryptocurrency assets.

Technical Analysis

Torg Grabber is an infostealer under active development, with 334 compiled samples observed between December 2025 and February 2026. Initial access uses ClickFix (MITRE T1204.002, T1566): the technique hijacks clipboard contents to stage and execute a malicious PowerShell command (T1059.001) without requiring a file drop or exploitation of a patched vulnerability; the user pastes and runs the command themselves under social engineering pressure. Key capabilities include: bypass of Chrome App-Bound Encryption (ABE), a privilege-isolation control introduced by Google to block credential extraction at user privilege level (maps to

CWE-693, Protection Mechanism Failure); credential harvesting from cryptocurrency wallet extensions including MetaMask, Phantom, TrustWallet, Coinbase, Binance, Exodus, Ronin, and Keplr (T1555.003); targeting of 103 password managers and 2FA tools including LastPass, 1Password, Bitwarden, KeePass, and Dashlane (T1552.001); session cookie theft (T1539); keylogging (T1056.001); screenshot capture (T1113); system enumeration (T1082); and exfiltration over HTTP/S (T1041, T1071.001). Persistence mechanisms are present (T1547). Obfuscation and packing techniques are in use (T1027, T1140). DLL injection has been observed (T1055.001). Installed security software is enumerated (T1518.001). Affected platforms span 25+ Chromium-based browsers (Chrome, Brave, Edge, Vivaldi, Opera) and 8 Firefox variants. No CVE is assigned; CWEs of note are CWE-494 (Download of Code Without Integrity Check), CWE-522 (Insufficiently Protected Credentials), CWE-312 (Cleartext Storage of Sensitive Information), and CWE-693 (Protection Mechanism Failure). No patch exists; mitigation is behavioral and architectural.

Action Checklist

1. Immediate, Block ClickFix delivery vectors: deploy endpoint controls (EDR or DLP) to detect and block clipboard-to-PowerShell execution chains; use Group Policy to restrict clipboard redirection from remote sessions if applicable; educate users on ClickFix social engineering tactics (pasting commands from untrusted sources into Run or PowerShell); deploy or verify endpoint detection and response (EDR) coverage across all endpoints with browser access to cryptocurrency or financial platforms.
2. Detection, Hunt for ClickFix execution artifacts: query EDR and SIEM for PowerShell processes spawned from browser child processes or user-interactive sessions with no parent executable context (T1059.001 + T1204.002); search for clipboard-read API calls followed by PowerShell invocations within short time windows; review Windows Event ID 4104 (PowerShell script block logging) for encoded or obfuscated commands.
3. Assessment, Inventory credential exposure surface: identify all endpoints where employees access cryptocurrency wallets, browser-based password managers (LastPass, Bitwarden, 1Password, etc.), or 2FA browser extensions; flag environments where personal and corporate browser profiles share credential stores; assess whether Chrome ABE is enabled and whether any endpoint policy downgrades it.
4. Communication, Notify affected user populations: issue a targeted advisory to finance, treasury, and any staff with cryptocurrency custody responsibilities; include specific ClickFix awareness guidance, describe the technique (a fake CAPTCHA or error page instructs users to paste a command into Run or PowerShell); escalate to incident response if any endpoint shows indicators consistent with execution.
5. Long-term, Reduce browser-based credential risk structurally: migrate organizational credentials from browser-native password managers to enterprise vault solutions with hardware-backed authentication; enforce hardware security keys (FIDO2) for any account protecting cryptocurrency assets or privileged access; evaluate browser isolation or dedicated browser profiles for high-risk financial activity; monitor MITRE ATT&CK T1555.003 and T1539 detections for ongoing campaign evolution.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to external IR firm or law enforcement immediately if any endpoint shows confirmed execution of ClickFix (PowerShell spawned from browser with clipboard API call, or 4104 script block log containing obfuscated credential-stealing payloads), or if any cryptocurrency wallet or password manager credentials are confirmed compromised by monitoring for unauthorized transactions, failed login alerts, or credential reuse on external systems.
Recovery Notes	Post-containment, conduct full credential rotation for any user whose endpoint showed ClickFix indicators: reset all passwords stored in affected password managers, revoke and re-issue hardware security keys, and reset cryptocurrency wallet private keys if hosted in browser extensions. Perform a 30-day post-incident review analyzing all collected forensic artifacts (4104 logs, EDR telemetry, clipboard artifacts) to confirm no secondary infection occurred and to refine detection rules for T1059.001, T1204.002, and T1555.003 for long-term monitoring. Coordinate with finance/treasury to audit all cryptocurrency wallets and financial accounts for unauthorized activity in the 60-day window prior to detection.
Forensic Artifacts	Windows Event ID 4688 (Process Creation) and Event ID 4104 (PowerShell Script Block Logging) with parent process chain intact | Windows Prefetch files (C:\Windows\Prefetch*.pf) for execution timeline of powershell.exe, cmd.exe, and browser executables | Browser cache, cookies, and Local Storage (Chrome: %UserProfile%\AppData\Local\Google\Chrome\User Data; Firefox: %UserProfile%\AppData\Roaming\Mozilla\Firefox\Profiles) | Registry HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU and HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU (Run dialog history) | Clipboard history (Windows 11: Get-ClipboardHistory; Windows 10: registry HKEY_CURRENT_USER\Software\Microsoft\Clipboard) | Browser extension manifests and background script files from Extensions directories (Chrome: Extensions/*.js, Firefox: addons.sqlite) | Memory dump of any active PowerShell or cmd.exe process for command-line argument recovery and injected script analysis

Per-Action IR Details

Immediate — Block ClickFix delivery vectors: push browser policy to disable clipboard write access from unrecognized sites; block PowerShell execution via Group Policy or endpoint controls for users without a documented operational need; deploy or verify endpoint detection and response (EDR) coverage across all endpoints with browser access to cryptocurrency or financial platforms.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 (Preparation phase: tools, policies, training)

Controls: NIST 800-53 AC-3 (Access Control Policy), NIST 800-53 SI-4 (Information System Monitoring), CIS Controls 6.1 (Establish and Enforce Asset Management), CIS Controls 8.1 (Establish and Enforce Security Configuration Management)

Compensating: For teams without EDR: (1) Deploy Windows Defender ATP (free tier) or osquery (open-source, requires manual query tuning). (2) Block PowerShell via Group Policy: set 'Turn on Module Logging' (HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\ModuleLogging) and 'ScriptBlockLogging' to enabled. (3) Disable clipboard access in Chrome via GPO: set 'Disable Clipboard API' (cloud policy console or group_policy_template.adm). (4) For Firefox: disable dom.events.clipboardevents.enabled in about:config. (5) Create a scheduled task using logman.exe to capture process creation events to a local CSV file hourly.

Evidence: Before deploying policy: (1) Export current browser policies from Group Policy Editor (gpresult /h report.html for baseline). (2) Capture Windows Event ID 4688 (Process Creation) and Event ID 4104 (PowerShell Script Block Logging) from 30 days prior to establish baseline behavior. (3) Query EDR for all PowerShell spawned from browser processes (chrome.exe, firefox.exe, msedge.exe) in the last 90 days. (4) Screenshot current security configuration: gpsec.msc snap-in, Internet Options for all browser GPOs, and MDM policies if deployed.

Detection — Hunt for ClickFix execution artifacts: query EDR and SIEM for PowerShell processes spawned from browser child processes or user-interactive sessions with no parent executable context (T1059.001 + T1204.002); search for clipboard-read API calls followed by PowerShell invocations within short time windows; review Windows Event ID 4104 (PowerShell script block logging) for encoded or obfuscated commands.

NIST Phase: Detection Analysis

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

Controls: NIST 800-53 SI-4 (Information System Monitoring), NIST 800-53 IR-4 (Incident Handling), CIS Controls 8.5 (Log All Access and Changes of Administrative Event Data), CIS Controls 8.11 (Monitor and Alert on Account Login Behavior)

Compensating: For teams without SIEM/EDR: (1) Enable PowerShell Script Block Logging via Group Policy (Computer Configuration → Administrative Templates → Windows PowerShell → Turn on PowerShell Script Block Logging). (2) Export Windows Event Log 4688 (Process Creation) and 4104 (Script Block Logging) daily using wevtutil: `wevtutil qe Security /q:*[System[(EventID=4688 or EventID=4104)]] /rd:true /f:csv > powershell_hunts.csv`. (3) Parse for patterns: `findstr /R "chrome.exe\|firefox.exe\|msedge.exe" powershell_hunts.csv | findstr "powershell.exe\|pwsh.exe"`. (4) Search for Base64-encoded strings in 4104 logs using: `Get-EventLog -LogName Security -InstanceId 4104 | Select-Object -ExpandProperty Message | findstr /I "base64\|encode\|-enc\|-e"`. (5) Manually review Prefetch files (C:\Windows\Prefetch) for suspicious execution order using WinPrefetchView (free tool from Nirsoft).

Evidence: Collect before analysis: (1) Full Windows Security Event Log (minimum 30 days) exported as .evtx format. (2) PowerShell Operational and Analytic logs (C:\Windows\System32\winevt\Logs\Windows PowerShell.evtx and Microsoft-Windows-PowerShell%4Operational.evtx). (3) Clipboard history from affected user accounts (use Get-ClipboardHistory if Windows 11, or check %UserProfile%\AppData\Local\Microsoft\Windows\Clipboard\SourceTitles for File Explorer access). (4) Browser debug logs: Chrome cache/History, Firefox places.sqlite, and Edge WebData databases. (5) Memory dump of any PowerShell process identified in logs (use Volatility or WinDbg to extract command-line arguments and scripts).

Assessment — Inventory credential exposure surface: identify all endpoints where employees access cryptocurrency wallets, browser-based password managers (LastPass, Bitwarden, 1Password, etc.), or 2FA browser extensions; flag environments where personal and corporate browser profiles share credential stores; assess whether Chrome ABE is enabled and whether any endpoint policy downgrades it.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.3 (Determine scope of the incident)

Controls: NIST 800-53 CA-7 (Continuous Monitoring), NIST 800-53 IA-4 (Identifier Management), CIS Controls 2.1 (Establish and Maintain a Software Inventory), CIS Controls 6.2 (Ensure Authorized Software is Current)

Compensating: For teams without SIEM inventory tools: (1) Use GPO reporting: `gpresult /h gpoinventory.html` on each endpoint to enumerate applied policies. (2) Query installed browser extensions via command line: (Chrome) `Get-ChildItem "$env:UserProfile\AppData\Local\Google\Chrome\User Data\Default\Extensions"` for all user profiles. (Firefox) `Get-ChildItem "$env:UserProfile\AppData\Roaming\Mozilla\Firefox\Profiles\*\extensions"`. (3) Enumerate password managers: `Get-ItemProperty HKCU:\Software\Microsoft\Windows\CurrentVersion\Uninstall\* | Select-Object DisplayName | findstr /I "lastpass bitwarden 1password keepass dashlane nordpass protonpass"`. (4) Check Chrome ABE status: query HKEY_LOCAL_MACHINE\Software\Policies\Google\Chrome\ChromeVariations\RestrictedDomains and verify presence of encryption-related registry keys. (5) Audit browser profiles: check %UserProfile%\AppData\Local\Google\Chrome\User Data for non-corporate or mixed profiles.

Evidence: Collect before assessment: (1) HKEY_LOCAL_MACHINE and HKEY_CURRENT_USER registry hives exported from all endpoints (reg save HKLM C:\hive_HKLM & reg save HKCU C:\hive_HKCU). (2) Extension manifests from Chrome/Brave/Edge User Data folders (*.json files in Extensions directories). (3) Browser startup files and preferences (Chrome: Preferences, Local State; Firefox: prefs.js, user.js; Edge: Preferences). (4) Outputs of software inventory tools or manual audits listing all password manager and crypto wallet software. (5) Screenshots or exports of Group Policy Applied settings (gpresult /h) from sample endpoints in each department.

Communication — Notify affected user populations: issue a targeted advisory to finance, treasury, and any staff with cryptocurrency custody responsibilities; include specific ClickFix awareness guidance — describe the technique (a fake CAPTCHA or error page instructs users to paste a command into Run or PowerShell); escalate to incident response if any endpoint shows indicators consistent with execution.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 (Containment, Eradication, and Recovery) — communication component

Controls: NIST 800-53 AT-1 (Security Awareness and Training), NIST 800-53 IR-6 (Incident Reporting), CIS Controls 12.3 (Address Unauthorized Software), CIS Controls 17.1 (Map and Inventory All Devices)

Compensating: For teams without formal communication infrastructure: (1) Draft advisory in plain language: describe ClickFix as a social engineering attack (fake error or CAPTCHA prompting a code paste into Windows Run dialog or PowerShell). (2) Include visual examples: annotated screenshot showing a phishing page mimicking a CAPTCHA, with red box highlighting 'paste this command' instruction. (3) Distribute via email with clear subject line (All-Hands: Critical Security Advisory - Cryptocurrency Wallet Threats). (4) Post on internal wiki/intranet with instructions to report any suspicious prompts to security-team@company.com. (5) Schedule optional 15-minute webinar for finance/treasury teams with Q&A. (6) Create a simple detection checklist: 'Did you paste a command into PowerShell after visiting a website? Report it immediately.' (7) Provide a secure reporting form (Google Form or internal ticketing system) with fields: time, domain/website, command pasted (if remembered), endpoint name.

Evidence: Preserve before communication: (1) Copy of all prior advisory templates and distribution lists. (2) Email server logs showing successful delivery to targeted groups. (3) Screenshot or archive of intranet post and any posted graphics. (4) Timestamps and attendance records for any webinar held. (5) A baseline of incoming security reports 7 days prior to assess reporting uptake post-advisory.

Long-term — Reduce browser-based credential risk structurally: migrate organizational credentials from browser-native password managers to enterprise vault solutions with hardware-backed authentication; enforce hardware security keys (FIDO2) for any account protecting cryptocurrency assets or privileged access; evaluate browser isolation or dedicated browser profiles for high-risk financial activity; monitor MITRE ATT&CK T1555.003 and T1539 detections for ongoing campaign evolution.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.4 (Post-Incident Activities) and §2.1 (Policy and Planning)

Controls: NIST 800-53 IA-2 (Authentication), NIST 800-53 IA-5 (Authentication Mechanism Management), NIST 800-53 SC-7 (Boundary Protection), CIS Controls 5.2 (Use Multi-Factor Authentication for All Administrative Access), CIS Controls 6.8 (Implement Flag and Remove Suspicious Email Messages)

Compensating: For resource-constrained teams: (1) Phase migration: begin with high-risk accounts (treasury, crypto custody, privileged access). Use open-source vaults (Bitwarden self-hosted or KeePass with encrypted cloud sync) as intermediate step before enterprise solution. (2) Hardware keys: procure Yubikey 5 or Titan keys (~$40–60 per unit) for finance/treasury; enforce FIDO2 for single sign-on (SSO) provider as minimum compliance. (3) Browser isolation: implement at pilot scale using Windows Sandbox (native to Windows 10/11 Pro) for financial browsing, or Docker containers (free) for segregated browser sessions. Create a startup script: launch a separate Chrome profile for crypto/financial domains only. (4) Monitoring: set up free alert rules in Splunk Free (if deployed) or use auditd (Linux) to monitor for T1555.003 (credential extraction from password stores) and T1539 (data from cloud storage) by watching for unexpected process access to credential files. (5) Documentation: create a runbook for crypto/treasury staff: 'If you see a CAPTCHA or error page on a financial site, close the tab immediately and contact security. Do not paste code.'

Evidence: Archive for compliance and future reference: (1) Current credential storage locations and formats (browser password stores, local files, cloud services) documented before migration. (2) Baseline MITRE ATT&CK detections for T1555.003 and T1539 from 90 days prior (set this as floor for monitoring). (3) Records of all hardware security keys distributed (serial numbers, user assignments). (4) Browser isolation/profile test results: screenshots of isolated profile behavior and access logs. (5) Signed approval from finance and security leadership for long-term credential management strategy change. (6) Post-implementation audit: verification that no credentials remain in browser password stores after migration cutoff date.

Detection Guidance

No public IOCs (hashes, IPs, domains) have been confirmed from primary-tier sources for this campaign as of the configuration date; treat any IOC-level data from secondary or unverified sources with caution before blocking production traffic. Behavioral detection is the primary viable approach. Key indicators: (1) PowerShell processes launched interactively from Run dialog or terminal without a parent process chain consistent with administrative tooling, especially with encoded commands or web-retrieved payloads (Event ID 4104, 4688); (2) browser extension data directories accessed by non-browser processes, watch for reads of %APPDATA%\Local\Google\Chrome\User Data\Default\Local Extension Settings or equivalent paths by processes other than the browser itself; (3) clipboard API access followed immediately by shell execution; EDR platform capabilities vary - consult your EDR vendor documentation for clipboard-to-execution chain detection, or build correlation rules at the SIEM layer using Event ID 4104 (PowerShell script block logging) paired with network connection logs within 60-second windows; (4) outbound connections from PowerShell or cmd.exe to non-categorized or newly registered domains (exfiltration via T1071.001); (5) DLL injection events targeting browser processes (T1055.001); (6) enumeration of installed applications consistent with security software discovery (T1518.001). If SIEM ingests endpoint telemetry, build a correlation rule: PowerShell script block log (4104) with base64-encoded content AND a network connection event within 60 seconds, flagged for analyst review. Source attribution: BleepingComputer and community forums (secondary-tier sources, recommend verification with primary threat intelligence before tuning production detection rules).

Indicators of Compromise

Type	Value	Context	Confidence
HASH	`[not confirmed from primary-tier sources]`	334 unique samples reported compiled Dec 2025 – Feb 2026; hashes not confirmed from primary-tier sources as of 2026-03-04. Check threat intelligence platforms (VirusTotal, MalwareBazaar) for Torg Grabber family tags before operationalizing.	LOW

Framework Mappings

MITRE-ATTACK

- **T1115** — Clipboard Data
- **T1056.001** — Keylogging
- **T1113** — Screen Capture
- **T1027** — Obfuscated Files or Information
- **T1082** — System Information Discovery
- **T1560** — Archive Collected Data
- **T1539** — Steal Web Session Cookie
- **T1204.002** — Malicious File
- **T1041** — Exfiltration Over C2 Channel

- **T1518.001** — Security Software Discovery
- **T1059.001** — PowerShell
- **T1547** — Boot or Logon Autostart Execution
- **T1055.001** — Dynamic-link Library Injection
- **T1566** — Phishing
- **T1552.001** — Credentials In Files
- **T1140** — Deobfuscate/Decode Files or Information
- **T1071.001** — Web Protocols
- **T1555.003** — Credentials from Web Browsers

NIST-800-53R5

- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **CM-7** — Least Functionality
- **SI-7** — Software, Firmware, and Information Integrity
- **AT-2** — Literacy Training and Awareness
- **SI-8** — Spam Protection
- **CM-3** — Configuration Change Control
- **IA-5** — Authenticator Management
- **SC-13** — Cryptographic Protection
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures
- **A04:2021** — Insecure Design
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **2.5**
- **2.6**
- **5.2**
- **6.3** — Require MFA for Externally-Exposed Applications
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

HIPAA-SECURITY

- **164.308(a)(5)(ii)(D)** — Password Management
- **164.312(d)** — Person or Entity Authentication

- **164.312(e)(1)** — Transmission Security

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.8.24** — Use of cryptography

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1115	Clipboard Data	Collection
T1056.001	Keylogging	Collection
T1113	Screen Capture	Collection
T1027	Obfuscated Files or Information	Defense-Evasion
T1082	System Information Discovery	Discovery
T1560	Archive Collected Data	Collection
T1539	Steal Web Session Cookie	Credential-Access
T1204.002	Malicious File	Execution
T1041	Exfiltration Over C2 Channel	Exfiltration
T1518.001	Security Software Discovery	Discovery
T1059.001	PowerShell	Execution
T1547	Boot or Logon Autostart Execution	Persistence
T1055.001	Dynamic-link Library Injection	Defense-Evasion
T1566	Phishing	Initial-Access
T1552.001	Credentials In Files	Credential-Access
T1140	Deobfuscate/Decode Files or Information	Defense-Evasion
T1071.001	Web Protocols	Command-And-Control
T1555.003	Credentials from Web Browsers	Credential-Access

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/new-torg-grabber-inf...	T3
PSA: New Zero-Day vulnerability found impacting most password ...	https://www.reddit.com/r/webdev/comments/1mvuk92/psa_new_zeroday_vu...	T3
Zero-Day Clickjacking Vulnerabilities in Major Password Managers	https://discuss.privacyguides.net/t/zero-day-clickjacking-vulnerabi...	T3
Top 10 Crypto Browser Extensions For 2025 - Milk Road	https://milkroad.com/browser-extension/	T3
One Exploit to Rule them All or "The Sky is Falling..." - YouTube	https://www.youtube.com/watch?v=_5vY1dGJt0o	T3

Generated 2026-03-29 18:39 UTC by TJS Security Command Center