INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-07-15 14:57 UTC

OkoBot Framework Injects Live Seed Phrase Phishing Inside Ledger and Trezor Apps, No Patch Exists

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0665
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Ledger Live, Trezor Suite, Windows OS, Chromium-based browsers, 1Password, Exodus Wallet, MetaMask, Tonkeeper
Published	2026-07-15T11:30:30
Discovery Source	Rss

Executive Summary

Kaspersky GReAT reported on July 15, 2026 that a modular Windows malware framework called OkoBot uses a process injection technique to embed fraudulent seed phrase recovery prompts directly inside Ledger Live and Trezor Suite, making the phishing prompt visually indistinguishable from a legitimate one. Because the attack targets companion software on the endpoint rather than the hardware device itself, the core security guarantee of hardware wallets is bypassed without touching the physical device. No patch exists from Ledger, Trezor, or Microsoft; organizations and individuals holding cryptocurrency assets on Windows endpoints running these applications are exposed with no vendor-provided remediation path as of the report date.

Technical Analysis

OkoBot is a modular Windows malware framework reported active since April 2025. Its SeedHunter module performs process injection (CWE-506, MITRE T1055) into the Ledger Live or Trezor Suite process at runtime, rendering a fraudulent seed phrase recovery prompt that is visually indistinguishable from the application's legitimate UI. This bypasses hardware wallet security by targeting the companion software layer on the endpoint rather than the hardware device itself. The framework also exhibits persistence via registry run keys (T1547.001), scheduled tasks (T1053.005), credential theft from browsers and password managers including 1Password, Exodus Wallet, MetaMask, and Tonkeeper (T1555, T1552.001), keylogging and form-grab techniques (T1056.001, T1056.004), C2 communication over application-layer protocols (T1071.002, T1102,

T1041), PowerShell execution (T1059.001), masquerading via legitimate binary names (T1036.005), registry modification (T1112), sandbox evasion (T1497), and browser extension abuse (T1176). The attack chain also involves download of unverified content (CWE-494) and absence of adequate protection mechanisms (CWE-693). No CVE has been assigned. No vendor patch from Ledger, Trezor, or Microsoft addresses this injection vector as of the Kaspersky GReAT report date of July 15, 2026. Source confidence is medium: technically plausible, attributed to a named research team, but not yet independently corroborated by Ledger, Trezor, or a second independent research organization.

Action Checklist

1. Step 1: Containment. Immediately prohibit entry of seed phrases into any desktop prompt on Windows endpoints running Ledger Live or Trezor Suite. Treat all seed phrase recovery prompts appearing in these applications as potentially fraudulent until process integrity can be verified. Isolate any Windows host where either application is installed AND anomalous process injection activity is detected or suspected based on endpoint detection tooling.
2. Step 2: Detection. Audit Windows endpoints for injected threads or anomalous memory regions within Ledger Live (ledger live.exe) and Trezor Suite (trezor suite.exe) processes using endpoint detection tooling. Review Windows Security event logs for process injection indicators (Event ID 8, CreateRemoteThread in Sysmon; suspicious ReadProcessMemory/WriteProcessMemory calls). Check for suspicious scheduled tasks (T1053.005) and Run key entries (T1547.001) referencing unknown executables. Monitor outbound C2 traffic patterns (MITRE T1071.002, T1102, T1041). Cross-reference host-based IOCs against Kaspersky GReAT's July 15, 2026 publication for specific hashes, domains, and IP indicators. (Note: IOC values were not included in the source material provided to this audit; obtain them directly from the primary report.)
3. Step 3: Eradication. No vendor patch exists as of July 15, 2026. Remove Ledger Live and Trezor Suite from general-purpose Windows endpoints where endpoint security posture cannot be fully validated. Re-image compromised hosts rather than attempting in-place remediation given the modular nature of the framework. Rotate all credentials stored in browsers and password managers (1Password, Exodus, MetaMask, Tonkeeper) on affected systems per D3-CRO. Revoke and reissue any API keys or wallet access credentials that may have been exposed.
4. Step 4: Recovery. Before restoring wallet application use, verify process integrity monitoring is active on the endpoint (D3-SFA). Confirm no persistence mechanisms remain via scheduled task and registry run key audits. Validate that only authorized software is present per CIS 2.1 and CIS 2.3. Re-enable wallet applications only on hardened, monitored endpoints with application allowlisting enforced. Monitor for re-infection attempts via C2 callbacks and reappearance of injection indicators.
5. Step 5: Post-Incident. Review endpoint detection coverage gaps for process injection (T1055) and in-process UI manipulation techniques not caught by signature-based tooling. Assess whether hardware wallet operations should be restricted to air-gapped or dedicated, non-general-purpose endpoints. Implement user awareness communication instructing staff and individuals to never enter seed phrases into any software prompt, regardless of appearance; seed phrases should only ever be entered directly on the hardware device's physical screen. Map gaps to NIST AC-6 (Least Privilege), NIST SI-4 (System Monitoring), and CIS 4.6 for endpoint configuration management.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to senior IR leadership, legal counsel, and — where applicable — financial regulators or breach notification authorities immediately if any evidence exists that a seed phrase was entered into an OkoBot-injected prompt, that wallet credentials stored in 1Password, MetaMask, Exodus, or Tonkeeper on the affected host were exfiltrated, or that the organization operates in a regulated sector (FinCEN, SEC, MiCA) where compromise of cryptographic wallet credentials may trigger mandatory incident reporting obligations.
Recovery Notes	Restored endpoints should not run Ledger Live or Trezor Suite until Sysmon process injection monitoring is confirmed active, WDAC application allowlisting is enforced, and a clean 24-hour behavioral baseline has been established with no EID 8 or EID 10 events targeting wallet processes. Because no vendor patch exists as of July 15, 2026, the compensating control posture (dedicated endpoint, process integrity monitoring, allowlisting) IS the recovery state — document this explicitly as an accepted residual risk with a patch-watch trigger tied to Ledger and Trezor's security advisories. Continue monitoring for OkoBot C2 callback attempts and reappearance of injection indicators for a minimum of 30 days post-recovery, given the modular and potentially dormant nature of the framework.
Forensic Artifacts	Sysmon Event ID 8 (CreateRemoteThread) and Event ID 10 (ProcessAccess) logs from `C:\Windows\System32\winevt\Logs\Microsoft-Windows-Sysmon%4Operational.evtx` — specifically entries where SourceImage is an unknown or unsigned process and TargetImage is `ledger live.exe` or `trezor suite.exe`, indicating OkoBot's injection of the fraudulent seed phrase UI overlay | Full process memory dumps of `ledger live.exe` and `trezor suite.exe` captured pre-isolation — these will contain the injected OkoBot module code, fraudulent UI payload, and potentially decrypted C2 configuration, and are the primary artifact for YARA rule development against the framework | Chromium browser credential database files (`%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data`, `Cookies`, `Web Data`) and MetaMask extension storage (`%LOCALAPPDATA%\Google\Chrome\User Data\Default\Local Extension Settings\nkbihfbeogaeaoehlefnkodbefgpgknn\`) — OkoBot's targeting of Chromium-based browsers means these stores should be treated as exfiltrated and are critical forensic artifacts for determining credential exposure scope | Windows Prefetch files `C:\Windows\Prefetch\LEDGER*.pf` and `C:\Windows\Prefetch\TREZOR*.pf` along with prefetch for any unrecognized executables in the same timeframe — prefetch preserves the execution history and file load order, which can reveal which OkoBot dropper or loader binary executed before injecting into the wallet process | Scheduled task XML files from `C:\Windows\System32\Tasks\` and registry exports of `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` and `HKLM\Software\Microsoft\Windows\CurrentVersion\Run` — OkoBot's modular framework requires persistence to survive reboots and re-inject on wallet application launch; these artifacts identify the specific persistence stub and its command-line arguments for IOC extraction

Per-Action IR Details

Step 1: Containment — Immediately prohibit entry of seed phrases into any desktop prompt on Windows endpoints running Ledger Live or Trezor Suite. Treat all seed phrase recovery prompts appearing in these applications as potentially fraudulent until process integrity can be verified. Isolate any Windows host where either application is installed and anomalous process injection activity is suspected.

NIST Phase: Containment

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

Controls: NIST AC-12 (Session Termination), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Before isolating, run the following volatile capture sequence on the suspect host: (1) `procdump.exe -ma ledger live.exe ledger_live.dmp` and `procdump.exe -ma trezor suite.exe trezor_suite.dmp` to capture full process memory of both wallet apps; (2) `netstat -ano > c:\ir\netstat_pre_isolate.txt` and `Get-NetTCPConnection | Export-Csv c:\ir\tcp_connections.csv` to record active outbound connections. Then isolate by disabling the NIC via `Disable-NetAdapter -Name * -Confirm:$false` rather than physical disconnection to preserve volatile network state in logs. On hosts without procdump, use Process Hacker (free) to dump memory from the wallet process before isolation.

Evidence: BEFORE isolating the host, capture: full memory dumps of ledger live.exe and trezor suite.exe (retain injected module code and fraudulent UI payload); `Get-NetTCPConnection` / `netstat -ano` output to record live C2 connections from the wallet process; Sysmon Event ID 8 (CreateRemoteThread) and Event ID 10 (ProcessAccess) logs from `C:\Windows\System32\winevt\Logs\Microsoft-Windows-Sysmon%4Operational.evtx`; running process list with parent-child relationships via `Get-CimInstance Win32_Process | Select-Object Name,ProcessId,ParentProcessId,CommandLine | Export-Csv c:\ir\processes.csv`; and a snapshot of `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` and `HKLM\Software\Microsoft\Windows\CurrentVersion\Run` for OkoBot persistence stubs.

Step 2: Detection — Audit Windows endpoints for injected threads or anomalous memory regions within Ledger Live (ledger live.exe) and Trezor Suite (trezor suite.exe) processes using endpoint detection tooling. Review Windows Security event logs for process injection indicators (Event ID 8, CreateRemoteThread in Sysmon; suspicious ReadProcessMemory/WriteProcessMemory calls). Check for suspicious scheduled tasks (T1053.005) and Run key entries (T1547.001) referencing unknown executables. Monitor outbound C2 traffic patterns consistent with T1071.002 and T1102. Cross-reference host-based IOCs against Kaspersky GReAT's July 15, 2026 publication for specific hashes, domains, and IP indicators — no IOCs were present in the provided source material.

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), CIS 8.2 (Collect Audit Logs)

Compensating: Without SIEM/EDR, deploy Sysmon with SwiftOnSecurity's config (minimum: enable Event IDs 1, 8, 10, 11, 12, 13) to capture CreateRemoteThread (EID 8) and ProcessAccess (EID 10) targeting ledger live.exe and trezor suite.exe. Query Sysmon logs with: `Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' | Where-Object {$_.Id -eq 8 -and $_.Message -like '*ledger*'}`. Use Process Hacker (free) to inspect live memory regions of wallet processes — look for executable memory regions (RWX pages) not backed by a file on disk, which indicate injected shellcode. For C2 detection, run Wireshark filtering on `tcp.port == 443 && ip.dst != [known-good-IPs]` during wallet app runtime and flag any TLS connections initiated by the wallet process to non-Ledger/non-Trezor infrastructure. Apply Sigma rule `win_susp_remote_thread_creation` (SigmaHQ) against Sysmon logs.

Evidence: Capture BEFORE any process termination or log clearance: Sysmon Event ID 8 logs showing source process injecting into ledger live.exe or trezor suite.exe (file path: `C:\Windows\System32\winevt\Logs\Microsoft-Windows-Sysmon%4Operational.evtx`); Sysmon Event ID 10 (ProcessAccess) entries where GrantedAccess includes 0x1F0FFF (full access) or 0x1010 (VM read/write) targeting wallet processes; Windows Security Event ID 4688 (Process Creation) showing wallet process spawning unexpected child processes; scheduled task XML exports from `C:\Windows\System32\Tasks\` for any task referencing non-standard executables; registry export of `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` and `HKLM\Software\Microsoft\Windows\CurrentVersion\Run`; and the full APPDATA path for both apps (`%APPDATA%\Ledger Live\` and `%APPDATA%\Trezor Suite\`) for unauthorized files or modified application bundles.

Step 3: Eradication — No vendor patch exists as of July 15, 2026. Remove Ledger Live and Trezor Suite from general-purpose Windows endpoints where endpoint security posture cannot be fully validated. Re-image compromised hosts rather than attempting in-place remediation given the modular nature of the framework. Rotate all credentials stored in browsers and password managers (1Password, Exodus, MetaMask, Tonkeeper) on affected systems per D3-CRO. Revoke and reissue any API keys or wallet access credentials

that may have been exposed.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), CIS 2.3 (Address Unauthorized Software), CIS 5.3 (Disable Dormant Accounts)

Compensating: Before reimaging, use Autoruns (Sysinternals, free) to enumerate and export all persistence locations — run `autorunsc.exe -a * -c > c:\ir\autoruns_export.csv` for a full machine export; flag any entries in `HKCU\Run`, `HKLM\Run`, scheduled tasks, or service entries referencing unsigned or unknown binaries. Revoke Chromium-stored credentials by exporting the Login Data SQLite database (`%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data`) for forensic copy before wiping, then forcing password resets for all accounts found there. For MetaMask, Tonkeeper, and Exodus, treat browser extension data directories as fully compromised — do not attempt to salvage. For 1Password, revoke the Emergency Kit and force re-enrollment on a clean device. Reimage using a known-good, offline image; do not restore user profile data from the compromised host.

Evidence: Capture BEFORE reimaging (order of volatility): full RAM dump of the compromised host using WinPmem (free) — `winpmem_mini_x64.exe memdump.raw`; Sysmon and Windows Security event logs archived to external storage; Autoruns export (`autorunsc.exe -a * -c`); full copies of `%APPDATA%\Ledger Live\` and `%APPDATA%\Trezor Suite\` directories including any unexpected DLLs or modified Electron app assets; browser credential databases (`Login Data`, `Cookies`, `Web Data` from Chromium profile) and 1Password local vault if present; prefetch files from `C:\Windows\Prefetch\` for LEDGER*.pf and TREZOR*.pf to establish execution history; and a disk image of the system volume prior to wipe using FTK Imager (free) for legal hold if financial loss has occurred.

Step 4: Recovery — Before restoring wallet application use, verify process integrity monitoring is active on the endpoint (D3-SFA). Confirm no persistence mechanisms remain via scheduled task and registry run key audits. Validate that only authorized software is present per CIS 2.1 and CIS 2.3. Re-enable wallet applications only on hardened, monitored endpoints with application allowlisting enforced. Monitor for re-infection attempts via C2 callbacks and reappearance of injection indicators.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 2.3 (Address Unauthorized Software), NIST AU-2 (Event Logging)

Compensating: On the restored, clean endpoint: deploy Sysmon prior to reinstalling wallet applications, using a config that specifically monitors ledger live.exe and trezor suite.exe for any incoming CreateRemoteThread (EID 8) or ProcessAccess (EID 10) events — treat any such event as immediate re-infection indicator. Enforce application allowlisting using Windows Defender Application Control (WDAC, built-in, free) with a deny-by-default policy that permits only signed Ledger and Trezor binaries. Validate software inventory by running `Get-WmiObject -Class Win32_Product | Select-Object Name,Version | Export-Csv c:\ir\software_inventory.csv` and diffing against a known-good baseline. Schedule a daily `schtasks /query /fo CSV /v > c:\ir\tasks_audit.csv` export and `reg export HKLM\Software\Microsoft\Windows\CurrentVersion\Run c:\ir\run_keys.reg` for ongoing persistence auditing.

Evidence: Before re-enabling wallet applications, verify no residual OkoBot artifacts remain: confirm `C:\Windows\System32\Tasks\` contains no tasks created or modified during the compromise window (compare timestamps against reimage date); verify `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` and `HKLM\Software\Microsoft\Windows\CurrentVersion\Run` contain only known-good entries; confirm `%APPDATA%\Ledger Live\` and `%APPDATA%\Trezor Suite\` contain only files matching the vendor-distributed installer hash (verify against Ledger and Trezor's official SHA-256 release hashes); and run a baseline Sysmon log capture for 24 hours post-restoration to establish a clean behavioral baseline before going live with wallet operations.

Step 5: Post-Incident — Review endpoint detection coverage gaps for process injection (T1055) and in-process UI manipulation techniques not caught by signature-based tooling. Assess whether hardware wallet operations should be restricted to air-gapped or dedicated, non-general-purpose endpoints. Implement user awareness communication instructing staff and individuals to never enter seed phrases into any

software prompt, regardless of appearance — seed phrases should only ever be entered directly on the hardware device's physical screen. Map gap to NIST AC-6 (Least Privilege) and NIST SI-4 (no mapped control in provided reference for system monitoring — reference knowledge base only) and CIS 4.6 for endpoint configuration management.

NIST Phase: Post Incident

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

Controls: NIST AC-6 (Least Privilege), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Document detection gaps specifically for Electron-based application injection (OkoBot targets Ledger Live and Trezor Suite, both Electron apps) — standard AV misses injected code executing within a trusted, signed Electron process. Draft a Sigma rule for Sysmon EID 8 with TargetImage matching `*ledger live.exe*` or `*trezor suite.exe*` and distribute via SigmaHQ or internal rule repository. Produce a one-page user brief stating: 'OkoBot can make a fake seed phrase prompt appear inside Ledger Live or Trezor Suite that is visually identical to the real one — your hardware wallet's physical screen is the only legitimate place to enter or confirm a seed phrase.' Assess dedicated-device policy: if hardware wallet operations are business-critical, formally document the risk decision of running Ledger Live or Trezor Suite on a general-purpose Windows endpoint given no patch exists as of July 15, 2026.

Evidence: Preserve for lessons-learned and future detection improvement: archived Sysmon and Windows Security event logs from the full incident timeline (from initial injection detection through reimaging); memory dump artifacts showing the injected OkoBot UI payload within the wallet process address space for YARA rule development; any captured C2 network traffic (Wireshark PCAP) showing OkoBot beacon patterns for network detection rule creation; Autoruns export from the compromised host showing persistence mechanism details; and a written timeline correlating Kaspersky GReAT's July 15, 2026 IOC publication against the organization's first detection event to calculate mean time to detect (MTTD) for gap analysis.

Detection Guidance

Detection relies on behavioral and memory-based indicators given the absence of a patch and the in-process injection technique. Key detection approaches based on the provided source material: (1) Monitor for anomalous thread creation or memory writes into Ledger Live and Trezor Suite processes using Sysmon Event ID 8 (CreateRemoteThread) and Event ID 10 (ProcessAccess with rights including PROCESS_VM_WRITE). (2) Alert on unexpected child processes or DLL loads originating from wallet application process space. (3) Hunt for new or modified registry Run keys (HKCU\Software\Microsoft\Windows\CurrentVersion\Run and HKLM equivalent) and scheduled tasks created by non-standard executables, consistent with T1547.001 and T1053.005. (4) Monitor for outbound connections from wallet processes to non-Ledger, non-Trezor infrastructure (MITRE T1071.002, T1041, T1102, C2 communication patterns). (5) Apply D3-SFA (System File Analysis) to monitor wallet application binaries and configuration files for unexpected modification. (6) Apply D3-LAM (Local Account Monitoring) to detect lateral movement or privilege escalation activity on affected hosts. Specific IOC values (hashes, domains, IP addresses) were not available in the provided source material; obtain these directly from the Kaspersky GReAT July 15, 2026 publication.

Framework Mappings

MITRE-ATTACK

- **T1112** — Modify Registry
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1071.002** — File Transfer Protocols

- **T1041** — Exfiltration Over C2 Channel
- **T1055** — Process Injection
- **T1547.001** — Registry Run Keys / Startup Folder
- **T1059.001** — PowerShell
- **T1195.002** — Compromise Software Supply Chain
- **T1497** — Virtualization/Sandbox Evasion
- **T1056.001** — Keylogging
- **T1056.004** — Credential API Hooking
- **T1053.005** — Scheduled Task
- **T1552.001** — Credentials In Files
- **T1555** — Credentials from Password Stores
- **T1176** — Software Extensions
- **T1566** — Phishing
- **T1021.001** — Remote Desktop Protocol
- **T1102** — Web Service

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **AC-6** — Least Privilege
- **SI-3** — Malicious Code Protection
- **CM-7** — Least Functionality
- **SI-7** — Software, Firmware, and Information Integrity
- **SA-9** — External System Services
- **SR-3** — Supply Chain Controls and Processes
- **AT-2** — Literacy Training and Awareness
- **SI-8** — Spam Protection
- **CM-3** — Configuration Change Control

OWASP-TOP10-2021

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

CIS-V8

- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **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

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information
- **A.5.21** — Managing information security in the ICT supply chain

HIPAA-SECURITY

- **164.308(a)(5)(i)** — Security Awareness and Training

SOC2-TSC

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1112	Modify Registry	Defense-Evasion
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
T1071.002	File Transfer Protocols	Command-And-Control
T1041	Exfiltration Over C2 Channel	Exfiltration
T1055	Process Injection	Defense-Evasion
T1547.001	Registry Run Keys / Startup Folder	Persistence
T1059.001	PowerShell	Execution
T1195.002	Compromise Software Supply Chain	Initial-Access
T1497	Virtualization/Sandbox Evasion	Defense-Evasion
T1056.001	Keylogging	Collection
T1056.004	Credential API Hooking	Collection
T1053.005	Scheduled Task	Execution
T1552.001	Credentials In Files	Credential-Access
T1555	Credentials from Password Stores	Credential-Access
T1176	Software Extensions	Persistence
T1566	Phishing	Initial-Access
T1021.001	Remote Desktop Protocol	Lateral-Movement
T1102	Web Service	Command-And-Control

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/07/okobot-malware-framework-injects-...	T2
Trezor Hardware Wallet (Official) | Bitcoin & Crypto Security ...	https://trezor.io/?srsltid=AfmBOopMhU6P5W8sIDxXQz4_6hLhtFJqZ6x4BT7P...	T3
Exodus + Trezor Hardware Wallet	https://www.exodus.com/trezor-wallet	T3
How to connect a Trezor, Ledger, or other hardware wallet ...	https://support.metamask.io/more-web3/wallets/how-to-connect-a-trez...	T3

Generated 2026-07-15 14:57 UTC by TJS Security Command Center