INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-18 19:05 UTC

USB Worm Chains LNK Abuse, Clipboard Hijacking, and Tor C2 to Drain Cryptocurrency Wallets

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0516
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Windows systems (wscript.exe, cscript.exe, PowerShell, cmd.exe, curl); cryptocurrency wallets including Bitcoin, Ethereum, Tron, and Monero
Published	2026-06-18T12:20:06
Discovery Source	Rss

Executive Summary

A self-propagating worm active since at least February 2026 spreads via USB drives and silently replaces cryptocurrency wallet addresses on infected Windows machines, redirecting transactions to attacker-controlled wallets across Bitcoin, Ethereum, Tron, and Monero. Any organization or individual conducting cryptocurrency transactions on Windows endpoints is at risk of irreversible financial loss; blockchain transactions cannot be reversed once confirmed. The threat uses legitimate Windows tools and Tor-based command-and-control, making it difficult to detect with signature-based security controls alone.

Technical Analysis

This campaign deploys a clipboard-hijacking cryptostealer via malicious LNK files carried on USB drives. When a user opens the shortcut, it executes payloads through Windows scripting hosts, wscript.exe, cscript.exe, PowerShell, cmd.exe, and curl, establishing persistence and launching clipboard monitoring. The malware watches for cryptocurrency wallet address patterns across seven formats (Bitcoin, Ethereum, Tron, Monero, and others) and substitutes attacker-controlled addresses before the user pastes. Command-and-control uses Tor (SOCKS5 proxy over .onion infrastructure), enabling remote code execution and screenshot exfiltration while evading network-based detection. The worm propagates to additional USB drives connected to the infected host, extending reach to air-gapped and offline environments. No CVE is assigned because the campaign exploits legitimate Windows functionality (LNK execution, scripting hosts, clipboard APIs) rather than a discrete software vulnerability. The threat is behavioral, not code-based. Relevant CWEs: CWE-693 (Protection

Mechanism Failure), CWE-74 (Injection), CWE-494 (Download of Code Without Integrity Check). MITRE ATT&CK techniques include T1091 (Replication Through Removable Media), T1115 (Clipboard Data), T1059.001/T1059.003/T1059.005/T1059.007 (scripting interpreter abuse), T1090.003 (Tor proxy), T1113 (Screen Capture), T1547/T1547.005 (Boot/Logon Autostart), T1573 (Encrypted Channel), T1027 (Obfuscated Files), and T1036.005 (Match Legitimate Name or Location). Microsoft Security Blog (2026-06-17) is the primary technical source.

Action Checklist

1. Step 1: Containment. Immediately enforce USB/removable media restrictions via Group Policy (Computer Configuration > Administrative Templates > System > Removable Storage Access) on all Windows endpoints, prioritizing systems used for cryptocurrency transactions. Disable AutoPlay and AutoRun across the environment. Isolate any endpoint showing anomalous wscript.exe, cscript.exe, PowerShell, or cmd.exe processes launched from removable media paths.
2. Step 2: Detection. Hunt for clipboard-monitoring behavior using endpoint detection telemetry: look for PowerShell or wscript.exe processes with unusually high runtime, LNK files in removable drive root directories, and outbound connections over Tor (port 9050/9150 or .onion DNS lookups). Review Windows Event ID 4688 (process creation) for parent process explorer.exe or USB-path executables. Check for scheduled tasks or registry run keys added by scripting hosts (Event IDs 4698, 4702; audit HKCU\Software\Microsoft\Windows\CurrentVersion\Run). Per NIST AU-2 (Audit Record Review, Analysis, and Reporting), ensure Event Logging is active. Per CIS 8.2 (Collect Audit Logs), confirm logging is enabled across all endpoints.
3. Step 3: Eradication. On confirmed-infected hosts: remove malicious LNK files from all connected USB drives; terminate and block wscript.exe/cscript.exe where not operationally required (via AppLocker or WDAC policy); remove persistence entries from registry Run keys and scheduled tasks created by scripting hosts; block Tor client binaries and .onion DNS resolution at the network layer and on-host firewall (CIS 4.4, CIS 4.5). Re-image endpoints where full scope of compromise cannot be confirmed.
4. Step 4: Recovery. After eradication, validate that clipboard contents are no longer being substituted by pasting a known test wallet address and confirming it is not altered. Monitor process creation logs for recurrence of scripting host activity from removable media. Confirm Tor outbound connections have ceased at the perimeter. Notify any cryptocurrency transaction recipients of potential address substitution during the exposure window and verify all pending or recent transactions were sent to intended addresses.
5. Step 5: Post-Incident. Conduct a lessons-learned review against NIST AC-19 (Access Control for Mobile Devices) and AC-3 (Access Enforcement) to formalize removable media policy. Implement application allowlisting (WDAC/AppLocker) to restrict scripting host execution to approved contexts. Evaluate whether cryptocurrency transaction workflows require a dedicated, hardened endpoint with clipboard isolation. Assess CIS 7.1 (Vulnerability Management Process) coverage for behavioral detection rules and ensure EDR behavioral detections for clipboard hijacking and LNK-based execution are active and tuned.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate immediately to senior IR leadership and legal counsel if any cryptocurrency transaction is confirmed redirected to an attacker-controlled address (irrecoverable financial loss), if more than five endpoints show evidence of wscript.exe/cscript.exe execution from removable media paths, or if organizational cryptocurrency custody wallets (as opposed to personal wallets) are determined to have been in the clipboard hijacking exposure window — the latter may trigger financial regulatory notification obligations depending on jurisdiction.
Recovery Notes	After eradication, maintain continuous monitoring of Windows Security Event ID 4688 and Sysmon Event ID 1 for scripting host re-execution from removable media for a minimum of 14 days, as USB-propagated worms can re-enter the environment through previously infected drives returned by employees or third parties. Validate clipboard integrity on all endpoints that handled cryptocurrency transactions during the exposure window by running a controlled address-substitution test before resuming any live transactions. All blockchain addresses used during the confirmed exposure window must be treated as potentially compromised — generate new wallet addresses on a confirmed-clean, isolated system before resuming cryptocurrency operations.
Forensic Artifacts	Malicious LNK files in the root directory of USB drives — parse with LECmd or lnk-parser to extract embedded target paths, working directories, and drive serial numbers that identify the infection source device and worm dropper location | Windows Prefetch files at C:\Windows\Prefetch\WSCRIPT.EXE-*.pf and CSCRIPT.EXE-*.pf — reveal first and last execution timestamps of the clipboard-hijacking VBScript payload, establishing the infection timeline and exposure window for affected cryptocurrency transactions | Registry key HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR — enumerates all USB storage devices ever connected to the host including device serial numbers, enabling identification of the patient-zero drive and all potentially infected removable media in the environment | Windows Security Event Log Event IDs 4698 and 4702 (Scheduled Task created/modified) and registry auditing events for HKCU\Software\Microsoft\Windows\CurrentVersion\Run — document persistence mechanisms installed by the wscript.exe/cscript.exe worm payload to survive reboots and maintain clipboard monitoring | Network connection logs and DNS query logs filtered for port 9050/9150 outbound connections and .onion hostname lookups — establish the timeline and frequency of Tor C2 beacon activity, which correlates with active clipboard-hijacking sessions and potential exfiltration of intercepted wallet addresses or transaction metadata to attacker infrastructure

Per-Action IR Details

Step 1: Containment — Immediately enforce USB/removable media restrictions via Group Policy (Computer Configuration > Administrative Templates > System > Removable Storage Access) on all Windows endpoints, prioritizing systems used for cryptocurrency transactions. Disable AutoPlay and AutoRun across the environment. Isolate any endpoint showing anomalous wscript.exe, cscript.exe, PowerShell, or cmd.exe processes launched from removable media paths.

NIST Phase: Containment

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

Controls: NIST AC-19 (Access Control for Mobile Devices), NIST AC-3 (Access Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: For teams without GPO-managed endpoints: run `reg add HKLM\SOFTWARE\Policies\Microsoft\Windows\RemovableStorageDevices /v Deny_All /t REG_DWORD /d 1 /f` on each host via PsExec batch script. Disable AutoRun via `reg add HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\IniFileMapping\Autorun.inf /ve /t REG_SZ /d @SYS:DoesNotExist /f`. Use Sysmon Event ID 1 (Process Create) filtered on `ParentImage` paths matching `E:\`, `F:\`, or other removable drive letters to identify hosts where wscript.exe or powershell.exe has already executed from USB.

Evidence: Before isolating any endpoint, capture volatile state: run `Get-NetTCPConnection -State Established | Where-Object {$_.RemotePort -in @(9050,9150)}` to document active Tor sessions; dump the live process list with `tasklist /v /fo csv > tasklist.csv` to record wscript.exe/cscript.exe/powershell.exe PIDs and their command lines; capture RAM with WinPmem or Magnet RAM Capture to preserve in-memory clipboard hook code and any injected shellcode before killing processes or disconnecting the host. Document all attached USB device identifiers from `HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR` before GPO enforcement flushes active sessions.

Step 2: Detection — Hunt for clipboard-monitoring behavior using endpoint detection telemetry: look for PowerShell or wscript.exe processes with unusually high runtime, LNK files in removable drive root directories, and outbound connections over Tor (port 9050/9150 or .onion DNS lookups). Review AU-2 (Event Logging) sources for process creation events (Windows Event ID 4688) where parent process is explorer.exe or a USB-path executable. Check for scheduled tasks or registry run keys added by scripting hosts (Event IDs 4698, 4702, registry auditing on HKCU\Software\Microsoft\Windows\CurrentVersion\Run). Use CIS 8.2 (Collect Audit Logs) to confirm logging is active across endpoints.

NIST Phase: Detection Analysis

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

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

Compensating: Without SIEM, deploy Sysmon with a configuration that logs Event ID 1 (Process Create), Event ID 3 (Network Connect), and Event ID 11 (File Create). Run this PowerShell one-liner to hunt LNK files on all attached drives: `Get-ChildItem -Path ([System.IO.DriveInfo]::GetDrives() | Where-Object {$_.DriveType -eq 'Removable'} | Select-Object -ExpandProperty RootDirectory) -Filter *.lnk -Recurse -Force 2>$null | Select FullName, LastWriteTime`. For Tor detection without a SIEM, run `netstat -ano | findstr ':9050 :9150'` and cross-reference PIDs against tasklist output. Use `schtasks /query /fo LIST /v | findstr /i 'wscript\|cscript\|powershell'` to surface persistence via scheduled tasks. Apply the public Sigma rule `win_susp_lnk_file_execution_from_removable.yml` against collected Windows Security and Sysmon EVTX exports using chainsaw or sigma-cli.

Evidence: This is a detection/analysis step that does not directly alter live state, but analysts must capture current clipboard contents (screenshot or `Get-Clipboard` output) and active network connections before any remediation begins. Pull Windows Security Event Log (Event ID 4688 filtered on `NewProcessName` containing `wscript.exe`, `cscript.exe`, or `powershell.exe` with `ProcessCommandLine` referencing a removable drive path such as `E:\` or `F:\`); pull Scheduled Task creation events (4698, 4702) and registry auditing events for `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`; export the full contents of `%TEMP%` and `%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup` for VBS/JS/PS1 dropper files; collect DNS cache via `ipconfig /displaydns` to identify any .onion hostname lookups that may indicate the Tor C2 beacon has already fired.

Step 3: Eradication — On confirmed-infected hosts: remove malicious LNK files from all connected USB drives; terminate and block wscript.exe/cscript.exe where not operationally required (via AppLocker or WDAC policy); remove persistence entries from registry Run keys and scheduled tasks created by scripting hosts; block Tor client binaries and .onion DNS resolution at the network layer and on-host firewall (CIS 4.4, CIS 4.5). Re-image endpoints where full scope of compromise cannot be confirmed.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication and Recovery

Controls: NIST SI-2 (Flaw Remediation), NIST CM-7 (Least Functionality), CIS 2.3 (Address Unauthorized Software), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Without AppLocker or WDAC licensing, use Software Restriction Policies (SRP) set to Disallowed for `%WINDIR%\System32\wscript.exe` and `cscript.exe` via `secpol.msc`. Manually enumerate and delete registry persistence with: `reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Run` and `reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Run`, removing any entries pointing to `.vbs`, `.js`, `.ps1`, or `.lnk` files. For Tor binary blocking on-host without EDR, add outbound Windows Firewall rules: `netsh advfirewall firewall add rule name="Block Tor 9050" dir=out action=block protocol=tcp remoteport=9050` and repeat for port 9150. For

DNS blocking of .onion, push a HOSTS file entry or configure the upstream resolver to NXDOMAIN all `.onion` queries.

Evidence: CRITICAL — before terminating processes, re-imaging, or removing persistence entries: acquire a full RAM dump (WinPmem) to capture the in-memory clipboard hook implementation, any injected DLLs, and the live Tor circuit state. Run `Get-NetTCPConnection` and `netstat -ano` and save output to document all established Tor connections with remote IPs. Export the full contents of `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` and `HKLM\Software\Microsoft\Windows\CurrentVersion\Run` via `reg export` before deletion. Copy (do not cut) all identified malicious LNK files from USB to a forensic staging share, preserving original timestamps with `robocopy /COPYALL`. Pull Prefetch files from `C:\Windows\Prefetch\` for WSCRIPT.EXE-*.pf and CSCRIPT.EXE-*.pf to establish first-execution timestamps before re-imaging destroys them.

Step 4: Recovery — After eradication, validate that clipboard contents are no longer being substituted by pasting a known test wallet address and confirming it is not altered. Monitor process creation logs for recurrence of scripting host activity from removable media. Confirm Tor outbound connections have ceased at the perimeter. Notify any cryptocurrency transaction recipients of potential address substitution during the exposure window and verify all pending or recent transactions were sent to intended addresses.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST SI-3 (Malicious Code Protection), CIS 8.2 (Collect Audit Logs)

Compensating: Without EDR for continuous process monitoring: schedule a recurring Sysmon EVTX export and parse it hourly using `Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' -FilterXPath "*[System[EventID=1] and EventData[Data[@Name='Image'] and (contains(.,"wscript") or contains(.,"cscript") or contains(.,"powershell"))]]"`. For clipboard validation: write a test Bitcoin address (a known invalid/test address such as `1A1zP1eP5QGefi2DMPTfTL5SLmv7Divf`Na) to the clipboard and immediately read it back with `Get-Clipboard` in a loop for 60 seconds — any substitution confirms residual hook activity. For perimeter Tor monitoring without a SIEM, configure DNS server query logging and grep for `.onion` lookups on a scheduled basis using a cron/Task Scheduler job.

Evidence: Recovery validation does not require pre-action volatile capture since eradication is complete, but retain and review: perimeter firewall logs for outbound port 9050/9150 connections originating from previously infected hosts for a minimum of 72 hours post-eradication; Windows Security Event ID 4688 logs for any recurrence of wscript.exe or cscript.exe spawned from removable media paths; blockchain transaction records for all wallet addresses used during the exposure window (Bitcoin, Ethereum, Tron, Monero) to identify any transactions redirected to attacker-controlled addresses — these are irrecoverable but must be documented for financial loss reporting and law enforcement referral.

Step 5: Post-Incident — Conduct a lessons-learned review against NIST AC-19 (Access Control for Mobile Devices) and AC-3 (Access Enforcement) to formalize removable media policy. Implement application allowlisting (WDAC/AppLocker) to restrict scripting host execution to approved contexts. Evaluate whether cryptocurrency transaction workflows require a dedicated, hardened endpoint with clipboard isolation. Assess CIS 7.1 (Vulnerability Management Process) coverage for behavioral detection rules and ensure EDR behavioral detections for clipboard hijacking and LNK-based execution are active and tuned.

NIST Phase: Post Incident

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

Controls: NIST AC-19 (Access Control for Mobile Devices), NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 2.2 (Ensure Authorized Software is Currently Supported)

Compensating: For teams without commercial EDR: write and deploy a YARA rule targeting the clipboard hijacking VBScript pattern (matching `CreateObject("htmlfile")`, `WScript.CreateObject`, and cryptocurrency address regex patterns for Bitcoin `[13][a-km-zA-HJ-NP-Z1-9]{25,34}`, Ethereum `0x[a-fA-F0-9]{40}`, Tron `T[a-zA-Z0-9]{33}` in the same script body) and run it nightly via ClamAV or a scheduled YARA scan against `%TEMP%`, `%APPDATA%`, and all removable media mount points. Publish a Sigma rule to detect LNK execution from removable media (`ParentImage: explorer.exe` + `CommandLine` containing drive letters D through Z with `.lnk` extension) and run it

weekly against archived Sysmon EVTX logs. Document the clipboard-isolation architecture decision (dedicated air-gapped or VM-isolated endpoint for cryptocurrency signing) in a formal policy update referencing this incident.

Evidence: Post-incident evidence collection for lessons-learned: compile a timeline from Prefetch artifacts (`C:\Windows\Prefetch\WSCRIPT.EXE-*.pf`), Windows Security Event ID 4688 logs, and Sysmon Event ID 1 logs to establish the worm's first execution date on each infected host; cross-reference against USB device insertion history from `HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR` and the Windows Portable Devices registry key to identify patient-zero USB device serial numbers; pull blockchain transaction history for all organizational wallet addresses used during the exposure window to quantify financial loss; retain all forensic RAM dumps, malicious LNK files, and VBScript payloads collected during eradication as evidence for law enforcement referral and threat intelligence sharing (e.g., submission to CISA or an ISAC).

Detection Guidance

Primary detection opportunities are behavioral, not signature-based. Key indicators: (1) LNK files present in the root directory of USB/removable drives; flag any LNK with a target pointing to wscript.exe, cscript.exe, PowerShell, cmd.exe, or curl; (2) Windows Event ID 4688 (process creation) showing wscript.exe or cscript.exe launched with a working directory or argument path referencing a removable drive letter; (3) PowerShell script block logging (Event ID 4104) capturing clipboard-access APIs (e.g., Get-Clipboard, SetText, or .NET System.Windows.Forms.Clipboard calls); (4) Scheduled task creation (Event ID 4698) or registry Run key writes (audit HKCU/HKLM Run paths) by scripting host processes; (5) Outbound network connections to Tor infrastructure - block and alert on port 9050/9150 egress, connections to known Tor guard node IPs, or .onion DNS resolution attempts; (6) Screenshot activity - look for unexpected file writes of .png or .bmp to temp directories by non-user-initiated processes. Correlate scripting host process trees with removable media insertion events (Event ID 6416 for new device recognition). Per NIST AU-6 (Audit Record Review, Analysis, and Reporting), these log sources should be reviewed at a defined frequency with automated alerting. D3FEND countermeasures applicable: D3-SFA (System File Analysis) for monitoring startup/registry modifications; D3-LAM (Local Account Monitoring) for detecting persistence under user accounts; D3-UAP (User Account Permissions) to restrict scripting host execution rights.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`.onion C2 infrastructure (specific addresses not published in available sources)`	Tor-based command-and-control used for remote code execution and screenshot exfiltration — block all Tor egress rather than specific indicators	LOW
URL	`https://www.microsoft.com/en-us/security/blog/2026/06/17/crypto-clipper-uses-tor-worm-like-propagation-for-persistence-control/`	Microsoft Security Blog primary technical analysis — IOC details including hashes and C2 indicators published at this source	HIGH

Framework Mappings

MITRE-ATTACK

- **T1091** — Replication Through Removable Media
- **T1547** — Boot or Logon Autostart Execution
- **T1071.003** — Mail Protocols
- **T1113** — Screen Capture
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1059.005** — Visual Basic
- **T1115** — Clipboard Data
- **T1564.001** — Hidden Files and Directories
- **T1059.003** — Windows Command Shell
- **T1547.005** — Security Support Provider
- **T1204.001** — Malicious Link
- **T1059.001** — PowerShell
- **T1573** — Encrypted Channel
- **T1059.007** — JavaScript
- **T1090.003** — Multi-hop Proxy
- **T1027** — Obfuscated Files or Information
- **T1071.001** — Web Protocols

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **SI-10** — Information Input Validation
- **CM-3** — Configuration Change Control

OWASP-TOP10-2021

- **A03:2021** — Injection
- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **8.2** — Collect Audit Logs

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1091	Replication Through Removable Media	Lateral-Movement
T1547	Boot or Logon Autostart Execution	Persistence
T1071.003	Mail Protocols	Command-And-Control
T1113	Screen Capture	Collection
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
T1059.005	Visual Basic	Execution
T1115	Clipboard Data	Collection
T1564.001	Hidden Files and Directories	Defense-Evasion
T1059.003	Windows Command Shell	Execution
T1547.005	Security Support Provider	Persistence
T1204.001	Malicious Link	Execution
T1059.001	PowerShell	Execution
T1573	Encrypted Channel	Command-And-Control
T1059.007	JavaScript	Execution
T1090.003	Multi-hop Proxy	Command-And-Control
T1027	Obfuscated Files or Information	Defense-Evasion
T1071.001	Web Protocols	Command-And-Control

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/usb-worm-spreads-cry...	T3
Crypto Clipper uses Tor and worm-like propagation for ...	https://www.microsoft.com/en-us/security/blog/2026/06/17/crypto-cli...	T1
$2 MILLION DOLLARS STOLEN in Bitcoin/Ethereum	https://www.youtube.com/watch?v=k-nFdF5FEwA	T3

Source	URL	Tier
PowerShell script stealing crypto and ...	https://www.reddit.com/r/PowerShell/comments/1ccrr2w/powershell_scr...	T3
Technical Advisory: Mass Exploitation of CVE-2024-4577	https://businessinsights.bitdefender.com/technical-advisory-update-...	T3

Generated 2026-06-18 19:05 UTC by TJS Security Command Center