INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-18 19:02 UTC

USB-Borne Windows Clipper Malware Uses Tor C2 and Runtime Code Execution to Target Cryptocurrency Users

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0511
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Windows OS (all versions supporting LNK execution and scheduled tasks); cryptocurrency wallet applications (unspecified vendors/versions)
Published	2026-06-18T10:30:42
Discovery Source	Rss

Executive Summary

Microsoft's Defender Security Research Team has disclosed an active malware campaign spreading via USB drives that targets cryptocurrency users on Windows systems. The malware silently replaces copied wallet addresses with attacker-controlled addresses, redirecting transactions, and also accepts remote code from a hidden Tor-based command server, giving attackers a persistent foothold beyond the initial theft. Organizations allowing uncontrolled USB access on Windows endpoints, particularly those handling cryptocurrency transactions or digital assets, face direct financial loss and potential broader system compromise.

Technical Analysis

An active Windows clipper campaign, disclosed by Microsoft Defender Security Research Team and first observed in February 2026, spreads via USB drives using LNK-disguised files (MITRE T1091, T1204.002) to lure users into execution. No CVE is assigned; CVSS base score is 7.5 (High) per source data. Relevant CWEs include CWE-693 (Protection Mechanism Failure), CWE-77 (Command Injection), CWE-425 (Direct Request), and CWE-494 (Download of Code Without Integrity Check). Once executed, the malware establishes persistence via Windows scheduled tasks and the Run registry key (T1547.001, T1547.005). C2 communications route through an embedded Tor client to a .onion hidden service (T1090.003), bypassing network-layer detection and attribution. Core clipper behavior monitors the clipboard (T1115) and substitutes cryptocurrency wallet addresses at copy time. A distinguishing capability: the malware accepts attacker-supplied

code via EVAL responses from the C2 (T1620, CWE-77, CWE-494), enabling dynamic payload execution and functioning as a lightweight backdoor. Additional techniques include obfuscation (T1027), sandbox evasion (T1497.001), screen capture (T1113), and scripted execution via VBScript and PowerShell (T1059, T1059.001, T1059.005). No patch exists; no CVE is assigned. Defenses must rely on behavioral detection, USB policy enforcement, and Tor traffic blocking. Primary source: Microsoft Defender Security Research Team (T1 source, source quality score 0.91).

Action Checklist

1. Step 1: Containment, Enforce USB storage device restrictions immediately on all Windows endpoints via Group Policy (USBSTOR registry key or Device Installation Restrictions policy). Prioritize endpoints used for cryptocurrency transactions or digital asset management. Reference: CIS 4.6 (Securely Manage Enterprise Assets and Software).
2. Step 2: Detection, Hunt for LNK files on USB-connected volumes and in user temp/download directories. Search Windows Task Scheduler logs (Event ID 4698, 4702) for recently created scheduled tasks with encoded or obfuscated commands. Monitor for outbound Tor traffic patterns: connections to port 9001/9030 or .onion resolution attempts via DNS. Review PowerShell and VBScript execution logs (Event IDs 4104, 4103) for EVAL-style dynamic code patterns. Reference: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs).
3. Step 3: Eradication, Remove identified scheduled tasks and Run registry persistence keys (HKCU\Software\Microsoft\Windows\CurrentVersion\Run) tied to the malware. Delete malicious LNK files and associated payloads from affected systems. Block Tor client binaries and .onion traffic at the network perimeter and on host-based firewalls. Reference: CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices).
4. Step 4: Recovery, After eradication, verify no residual scheduled tasks or registry run keys remain. Audit clipboard-sensitive applications (cryptocurrency wallets, exchange interfaces) on affected hosts. Confirm Tor traffic is blocked at perimeter. Monitor affected endpoints for 30 days for re-infection or C2 re-contact. Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (Information System Monitoring).
5. Step 5: Post-Incident, Conduct a USB policy audit across the enterprise; enforce default-deny device control where policy gaps are found. Review endpoint detection rule coverage for LNK-based execution, scheduled task creation by non-admin accounts, and outbound Tor traffic. Assess whether cryptocurrency transaction workflows have wallet-address verification steps. Reference: CIS 7.1 (Establish and Maintain a Vulnerability Management Process), NIST AC-19 (Access Control for Mobile Devices covers removable media policy context). D3FEND countermeasures (supplementary framework): D3-LAM (Local Account Monitoring), D3-SFA (System File Analysis).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate immediately to senior IR leadership and legal counsel if evidence indicates any cryptocurrency transactions were successfully redirected to attacker-controlled wallet addresses during the clipper's active window, as this constitutes confirmed financial fraud and may trigger regulatory breach notification obligations depending on whether organizational or customer funds were affected.
Recovery Notes	After eradication, do not return any cryptocurrency transaction workstation to production until wallet application binaries have been verified against vendor-published checksums and reinstalled from clean media, as the clipper may have persisted through or modified wallet executables. Monitor reinstated endpoints for 30 days using Sysmon Event ID 11 (LNK file creation on removable volumes) and daily Run key / scheduled task baseline diffs, specifically watching for re-insertion of USB drives that may carry the dropper LNK. Notify any external parties (exchanges, custodians) that may have received transactions from affected systems during the compromise window so they can flag potentially fraudulent transfers.
Forensic Artifacts	USBSTOR registry hive (HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR) — records every USB storage device ever connected, with device serial numbers and first/last connection timestamps, directly evidencing the USB drive used to introduce the clipper LNK dropper | Windows Task Scheduler Operational Event Log (Microsoft-Windows-TaskScheduler%4Operational.evtx) — Event IDs 4698 and 4702 capture creation and modification of scheduled tasks; the clipper uses scheduled tasks for persistence, so these entries will record the task name, trigger, and the encoded command used for runtime code execution from the Tor C2 | PowerShell ScriptBlock log (Microsoft-Windows-PowerShell%4Operational.evtx) — Event IDs 4103 and 4104 capture dynamically executed code; the malware's runtime code execution from the Tor C2 will appear here as Invoke-Expression or iex calls containing downloaded payload strings | Clipboard API hook artifacts in RAM — a full memory image of the wallet application process will contain the clipper's injected hook code and, potentially, the attacker's cryptocurrency wallet address that was staged as the clipboard replacement value, which is only recoverable from live memory before process termination | Network capture of outbound connections to TCP 9001/9030 — packet captures or firewall flow logs showing connections to these Tor OR ports from the affected endpoint provide direct evidence of C2 communication; DNS logs showing .onion resolution attempts corroborate the Tor-based C2 channel described in the campaign

Per-Action IR Details

Step 1: Containment — Enforce USB storage device restrictions immediately on all Windows endpoints via Group Policy (USBSTOR registry key or Device Installation Restrictions policy). Prioritize endpoints used for cryptocurrency transactions or digital asset management. Reference: CIS 4.6 (Securely Manage Enterprise Assets and Software).

NIST Phase: Containment

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

Controls: CIS 4.6 (Securely Manage Enterprise Assets and Software), NIST AC-19 (Access Control For Mobile Devices)

Compensating: For teams without MDM/GPO infrastructure, use PowerShell to set the USBSTOR Start registry value to 4 on all reachable endpoints: `Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\USBSTOR' -Name 'Start' -Value 4`. Deploy via PsExec across the estate or as a startup script. Physically document and tag any USB drives already in use, and bag-and-tag any drives found connected to cryptocurrency workstations as forensic evidence.

Evidence: Before enforcing USBSTOR restrictions, capture volatile state on any endpoint where a USB drive is currently inserted or was recently removed: enumerate active USB device history from

`HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR` and `HKLM\SYSTEM\CurrentControlSet\Enum\USB`; image the contents of any connected USB volume; collect Windows Event Log entries from the System log (Event ID 20001 — device driver installed, Event ID 20003 — driver service deleted) and Security log (Event ID 6416 — new external device recognized). Acquire these artifacts before GPO enforcement removes device access.

Step 2: Detection — Hunt for LNK files on USB-connected volumes and in user temp/download directories. Search Windows Task Scheduler logs (Event ID 4698, 4702) for recently created scheduled tasks with encoded or obfuscated commands. Monitor for outbound Tor traffic patterns: connections to port 9001/9030 or .onion resolution attempts via DNS. Review PowerShell and VBScript execution logs (Event IDs 4104, 4103) for EVAL-style dynamic code patterns. Reference: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs).

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), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with a config enabling Event ID 1 (Process Create), Event ID 11 (FileCreate for .lnk), and Event ID 22 (DNS query for .onion domains). Hunt LNK files with: `Get-ChildItem -Path E:\ -Recurse -Include *.lnk -ErrorAction SilentlyContinue` (substitute the USB drive letter). Use Wireshark or netsh trace to capture port 9001/9030 outbound traffic on cryptocurrency workstations. Use this PowerShell snippet to query scheduled tasks created in the last 72 hours with encoded arguments: `Get-ScheduledTask | Where-Object {$_.Actions.Arguments -match '-enc|-EncodedCommand|iex|Invoke-Expression'}`.

Evidence: This step is analytical and does not alter live state, but before any subsequent containment or process termination: capture a full RAM image using WinPmem or Magnet RAM Capture to preserve in-memory clipboard-hooking code injected by the clipper component; collect `Get-NetTCPConnection` output to document active Tor circuit connections; export the Task Scheduler operational log (`C:\Windows\System32\winevt\Logs\Microsoft-Windows-TaskScheduler%4Operational.evtx`); export PowerShell ScriptBlock logs (`Microsoft-Windows-PowerShell%4Operational.evtx`) for Event IDs 4103/4104 containing EVAL or Invoke-Expression patterns; record clipboard contents if safe to do so, as the clipper may have staged an attacker wallet address.

Step 3: Eradication — Remove identified scheduled tasks and Run registry persistence keys (HKCU\Software\Microsoft\Windows\CurrentVersion\Run) tied to the malware. Delete malicious LNK files and associated payloads from affected systems. Block Tor client binaries and .onion traffic at the network perimeter and on host-based firewalls. Reference: CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Remove malicious scheduled tasks via: `Unregister-ScheduledTask -TaskName '' -Confirm:$false`. Remove Run key persistence via: `Remove-ItemProperty -Path 'HKCU:\Software\Microsoft\Windows\CurrentVersion\Run' -Name ''`. Block Tor on Windows Firewall using netsh: `netsh advfirewall firewall add rule name='Block Tor 9001' dir=out action=block protocol=TCP remoteport=9001` and repeat for port 9030. Use ClamAV with a YARA rule targeting the clipper's clipboard-hook pattern or known LNK dropper structure to sweep remaining endpoints.

Evidence: Volatile evidence MUST be captured before any eradication action: acquire full RAM image to preserve injected clipboard-hooking code and any in-memory Tor circuit state before killing malware processes; export `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` and `HKLM\Software\Microsoft\Windows\CurrentVersion\Run` hive snapshots; collect `schtasks /query /fo LIST /v` full output; preserve copies of all malicious LNK files and payload binaries (do not delete originals — image them to forensic storage first); capture `Get-NetTCPConnection` and `netstat -ano` output documenting active Tor connections

before firewall rules terminate them.

Step 4: Recovery — After eradication, verify no residual scheduled tasks or registry run keys remain. Audit clipboard-sensitive applications (cryptocurrency wallets, exchange interfaces) on affected hosts. Confirm Tor traffic is blocked at perimeter. Monitor affected endpoints for 30 days for re-infection or C2 re-contact. Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (not independently confirmable from provided knowledge base — no mapped control).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Run a final scheduled-task audit: `schtasks /query /fo CSV /v | Select-String -Pattern 'Enabled|Ready'` and compare against a known-good baseline. Verify Run key cleanliness: `Get-ItemProperty 'HKCU:\Software\Microsoft\Windows\CurrentVersion\Run'` and `HKLM` equivalent. For 30-day re-infection monitoring without EDR, deploy Sysmon Event ID 11 alerts on LNK creation in %TEMP% and removable drive paths, and schedule a daily PowerShell job checking for new scheduled tasks and Run key entries against a saved baseline hash. Reinstall cryptocurrency wallet applications from vendor-verified installers after confirming no residual payload.

Evidence: Before returning any affected system to production, verify integrity of cryptocurrency wallet binaries by comparing file hashes against vendor-published checksums — the clipper may have replaced or trojanized wallet executables. Confirm clipboard API hooks are gone by reviewing loaded modules in wallet processes using `Get-Process -Name '' | Select-Object -ExpandProperty Modules`. Retain all forensic images, memory captures, and log exports for a minimum of 90 days to support any subsequent financial fraud investigation or law enforcement referral related to redirected cryptocurrency transactions.

Step 5: Post-Incident — Conduct a USB policy audit across the enterprise; enforce default-deny device control where policy gaps are found. Review endpoint detection rule coverage for LNK-based execution, scheduled task creation by non-admin accounts, and outbound Tor traffic. Assess whether cryptocurrency transaction workflows have wallet-address verification steps. Reference: CIS 7.1 (Establish and Maintain a Vulnerability Management Process), NIST AC-19 (Access Control for Mobile Devices covers removable media policy context), D3-LAM (Local Account Monitoring), D3-SFA (System File Analysis).

NIST Phase: Post Incident

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

Controls: CIS 7.1 (Establish and Maintain a Vulnerability Management Process), NIST AC-19 (Access Control For Mobile Devices), NIST AU-2 (Event Logging)

Compensating: Use the free Sigma rule set (github.com/SigmaHQ/sigma — search-retrieved, recommend human validation) to identify community rules covering LNK execution from removable media and scheduled task creation by standard users, and translate them to native Windows Event Log queries using sigmac. Author a standing PowerShell audit job that weekly exports all scheduled tasks and Run keys to a versioned CSV baseline and diffs against the prior week. Document a wallet-address verification step in any cryptocurrency transaction SOP: require visual confirmation of the full destination address character-by-character after paste, since this clipper silently substitutes the clipboard value.

Evidence: No live-state-altering action occurs in this phase; evidence collection here focuses on documentation: compile the full timeline of USB device insertions from USBSTOR registry history and Event ID 6416 entries across the affected population; produce a complete inventory of all scheduled tasks and Run key entries that were removed, with before/after registry hive exports attached; document all cryptocurrency wallet processes running on affected hosts at time of detection, including version numbers, to assess whether any transactions may have been silently redirected during the clipper's active window and to support financial loss quantification.

Detection Guidance

Focus detection on behavioral indicators; signature-based tools are insufficient per source data. Key detection points: (1) LNK file execution from USB-connected volumes, monitor Windows Event ID 4688 (process creation) for lnk-launched processes originating from removable drives. (2) Scheduled task creation, Windows Event IDs 4698 and 4702 for new or modified tasks; flag any task with Base64-encoded or obfuscated command lines. (3) Registry persistence, monitor HKCU and HKLM Run keys for additions tied to non-standard executables (MITRE T1547.001, T1547.005). (4) Tor traffic, block and alert on outbound connections to known Tor guard nodes (ports 9001, 9030, 9050), .onion DNS queries, and bundled Tor binary hashes if available from Microsoft's advisory. (5) Clipboard monitoring behavior, endpoint detection rules for processes making repeated calls to clipboard APIs (OpenClipboard, GetClipboardData) outside of known productivity applications. (6) Dynamic code execution, PowerShell Script Block Logging (Event ID 4104) and VBScript execution (Event ID 4104 via AMSI) for EVAL-equivalent patterns (Invoke-Expression, [System.Reflection.Assembly]::Load). Reference NIST AU-2, AU-6, AU-12, CIS 8.2. D3FEND countermeasures (supplementary framework): D3-SFA (System File Analysis for scheduled task and config changes), D3-LAM (Local Account Monitoring for persistence artifacts).

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`.onion C2 (specific address not disclosed in available source material)`	Tor hidden service used for C2 communication and EVAL-based payload delivery	LOW
URL	`https://www.microsoft.com/en-us/security/blog/author/windows-defender-research/`	Microsoft Defender Security Research Team blog — primary source for campaign indicators; check for updated IOC releases	HIGH

Framework Mappings

MITRE-ATTACK

- **T1091** — Replication Through Removable Media
- **T1620** — Reflective Code Loading
- **T1547.001** — Registry Run Keys / Startup Folder
- **T1113** — Screen Capture
- **T1059.005** — Visual Basic
- **T1115** — Clipboard Data
- **T1547.005** — Security Support Provider
- **T1090.003** — Multi-hop Proxy
- **T1059.001** — PowerShell
- **T1027** — Obfuscated Files or Information
- **T1497.001** — System Checks
- **T1059** — Command and Scripting Interpreter

- **T1204.002** — Malicious File

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

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
T1620	Reflective Code Loading	Defense-Evasion
T1547.001	Registry Run Keys / Startup Folder	Persistence
T1113	Screen Capture	Collection
T1059.005	Visual Basic	Execution
T1115	Clipboard Data	Collection
T1547.005	Security Support Provider	Persistence
T1090.003	Multi-hop Proxy	Command-And-Control
T1059.001	PowerShell	Execution
T1027	Obfuscated Files or Information	Defense-Evasion
T1497.001	System Checks	Defense-Evasion

Technique ID	Technique Name	Tactic
T1059	Command and Scripting Interpreter	Execution
T1204.002	Malicious File	Execution

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/06/microsoft-details-windows-clipper...	T3
Microsoft Defender Security Research Team posts	https://www.microsoft.com/en-us/security/blog/author/windows-defend...	T1
From poisoned search results to GPU mining - Microsoft	https://www.microsoft.com/en-us/security/blog/2026/05/26/poisoned-s...	T1
A newly disclosed Windows zero-day called MiniPlasma is already ...	https://www.facebook.com/Kaspersky/posts/a-newly-disclosed-windows-...	T3
Microsoft Security Response Center Blog	https://www.microsoft.com/en-us/msrc/blog	T1

Generated 2026-06-18 19:02 UTC by TJS Security Command Center