INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-18 07:17 UTC

USB-Borne Crypto Clipper Weaponizes Tor Routing and EVAL-Based RCE to Drain Wallets and Maintain Persistent Backdoor Access

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0506
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Windows (Windows Script Host via WScript/CScript, PowerShell); detected by Microsoft Defender Antivirus and Microsoft Defender for Endpoint as Trojan:Win32/CryptoBandits.A
Published	2026-06-17T23:11:43+00:00
Discovery Source	Rss:T1 Threatintel

Executive Summary

Since February 2026, a financially motivated threat actor has been distributing a Windows cryptocurrency clipper, Trojan:Win32/CryptoBandits.A, via USB drives. The malware silently replaces cryptocurrency wallet addresses copied to the clipboard, redirecting transactions to attacker-controlled wallets, while simultaneously establishing a persistent backdoor over the Tor network and self-propagating to newly inserted USB devices. Organizations with employees handling cryptocurrency transactions or operating in environments where USB devices are in common use face direct financial loss, persistent compromise, and significant difficulty in attribution or infrastructure blocking.

Technical Analysis

Trojan:Win32/CryptoBandits.A spreads via malicious .lnk files on USB drives, executing through Windows Script Host (WScript/CScript) and PowerShell. The malware performs clipboard monitoring and wallet address substitution (T1115, T1565.001), intercepting cryptocurrency addresses at copy time and replacing them with attacker-controlled addresses before the user pastes. A runtime EVAL function fetches and executes arbitrary code without integrity verification (CWE-494), elevating the implant from a single-function clipper to a full remote code execution backdoor. Command-and-control traffic routes over Tor (T1090.003), complicating network-level blocking and infrastructure attribution. A worm component copies the malware to newly inserted USB drives (T1091), enabling propagation in air-gapped or network-restricted environments. Persistence is established via scheduled tasks (T1547.005). The malware employs obfuscation (T1027) and sandbox evasion via system

checks (T1497.001). Scripting interpreter abuse spans JavaScript (T1059.007), Python (T1059.006), and additional scripting engines (T1059.005, T1059.001). Screen capture capability (T1113) and exfiltration over the C2 channel (T1041) are also present. No CVE identifier is assigned; relevant CWEs are CWE-494 (Download of Code Without Integrity Check), CWE-506 (Embedded Malicious Code), and CWE-311 (Missing Encryption of Sensitive Data). Microsoft Defender Antivirus and Microsoft Defender for Endpoint detect the malware under the signature Trojan:Win32/CryptoBandits.A. Source: Microsoft Security Blog, 2026-06-17.

Action Checklist

1. Step 1: Containment, Enforce USB device control policies to block unauthorized removable media on all Windows endpoints immediately. Disable AutoRun and AutoPlay via Group Policy (HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer, NoDriveTypeAutoRun). Isolate any host where Trojan:Win32/CryptoBandits.A has been detected. Reference: NIST AC-19 (Access Control for Mobile Devices).
2. Step 2: Detection, Confirm Microsoft Defender Antivirus definitions are current and scan all endpoints for the Trojan:Win32/CryptoBandits.A signature. In Microsoft Defender for Endpoint, query DeviceEvents for clipboard-related process activity (ClipboardSetContent events) initiated by WScript.exe, CScript.exe, or PowerShell. Hunt for .lnk files on removable media executing script interpreters. Look for outbound connections to Tor guard nodes (known Tor relay IP ranges and port 9001/9030). Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting); NIST SI-4 (System Monitoring); CIS 8.2 (Collect Audit Logs).
3. Step 3: Eradication, Remove all detected instances of Trojan:Win32/CryptoBandits.A using Microsoft Defender for Endpoint remediation actions. Remove all unauthorized .lnk files on removable media across the environment. Block EVAL-pattern script execution through application control policies (Windows Defender Application Control or AppLocker). Block Tor network traffic at the perimeter firewall and DNS layer. Reference: NIST CM-7 (Least Functionality); CIS 2.3 (Address Unauthorized Software); D3-FMBV (File Magic Byte Verification) to flag mismatched .lnk files.
4. Step 4: Recovery, After eradication, re-image affected hosts where persistent scheduled tasks (T1547.005) were confirmed. Remove all attacker-controlled scheduled tasks (audit Task Scheduler and registry Run keys). Verify clipboard behavior on recovered hosts with a controlled cryptocurrency address copy-paste test. Monitor for renewed Tor outbound connections for at least 30 days post-remediation. Reference: NIST IR-4 (Incident Handling); D3-LAM (Local Account Monitoring) to detect residual backdoor activity.
5. Step 5: Post-Incident, Conduct a USB device inventory and enforce CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) to include removable media. Implement CIS 6.3 and CIS 6.5 (Require MFA for Externally-Exposed Applications and Administrative Access) to limit blast radius if backdoor credentials were harvested. Review and enforce least-privilege policies (NIST AC-6) for accounts permitted to execute scripting engines. Brief employees handling cryptocurrency transactions on clipboard hijacking risks. Reference: CIS 7.1 (Establish and Maintain a Vulnerability Management Process).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate immediately to senior IR leadership, legal counsel, and — if cryptocurrency transactions were redirected and financial loss is confirmed or if any employee or customer financial account credentials may have transited the compromised clipboard — to the appropriate regulatory body and financial institutions; active self-propagation via USB means any uncontained host is a live infection vector across the entire physical campus.
Recovery Notes	Re-image all hosts where scheduled task persistence (Task Scheduler or registry Run-key entries created by Trojan:Win32/CryptoBandits.A) was confirmed rather than attempting in-place cleanup, as the EVAL-based RCE component may have deposited secondary payloads not yet detected by signature scanning. After reimaging, validate clipboard integrity on each recovered host using a controlled cryptocurrency address copy-paste test before returning the host to any employee involved in financial transactions. Maintain continuous monitoring of outbound connections to Tor guard-node IP ranges (ports 9001 and 9030) and Windows Security Event ID 4698/4702 (Scheduled Task Created/Updated) for a minimum of 30 days, as the Tor-based backdoor may attempt to re-establish persistence if any infected USB drive is reintroduced to the environment.
Forensic Artifacts	Windows Security Event Log — Event ID 4688 (Process Creation) entries showing WScript.exe or CScript.exe spawned with a command-line argument pointing to a path on a removable drive (e.g., E:*.vbs or E:*.js), establishing the LNK-triggered execution chain specific to CryptoBandits.A's USB propagation mechanism | Sysmon Event ID 23 (Clipboard Changed) records correlating clipboard modification timestamps to WScript.exe, CScript.exe, or PowerShell process PIDs — the direct forensic signature of the clipper replacing a cryptocurrency wallet address in memory | Windows Event ID 2003 and 2100 from the Microsoft-Windows-DriverFrameworks-UserMode/Operational log, recording USB device insertion timestamps and device serial numbers, which when cross-referenced with Sysmon Event ID 23 timestamps reconstruct the propagation timeline | Network flow or Windows Firewall log entries showing outbound TCP connections to known Tor guard-node IP ranges on ports 9001 or 9030, originating from WScript.exe, CScript.exe, or PowerShell — evidencing the active Tor-routed backdoor C2 channel established by Trojan:Win32/CryptoBandits.A | Task Scheduler XML files under C:\Windows\System32\Tasks\ and registry Run/RunOnce keys at HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run and HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run containing attacker-created entries referencing script interpreter paths, representing the persistence mechanism that survives reboots on unreimaged hosts

Per-Action IR Details

Step 1: Containment — Enforce USB device control policies to block unauthorized removable media on all Windows endpoints immediately. Disable AutoRun and AutoPlay via Group Policy (HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer, NoDriveTypeAutoRun). Isolate any host where Trojan:Win32/CryptoBandits.A has been detected. Reference: NIST AC-19 (Access Control for Mobile Devices).

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected systems and prevent lateral spread via the same removable-media vector before eradication begins

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 an MDM or enterprise GPO console: push the NoDriveTypeAutoRun DWORD (value 0xFF) to HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer via a one-line PowerShell script deployed through PsExec: `Set-ItemProperty -Path

'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer' -Name 'NoDriveTypeAutoRun' -Value 255`. For physical isolation of a confirmed host, pull the network cable and disable Wi-Fi via Device Manager before any software remediation to preserve volatile state.

Evidence: Before isolating any host flagged for Trojan:Win32/CryptoBandits.A, capture in this order: (1) full RAM image using WinPmem or Magnet RAM Capture — the clipper's clipboard-monitoring loop and any injected Tor client process will only exist in live memory; (2) active TCP/UDP connections via `Get-NetTCPConnection | Export-Csv` and `netstat -ano` — document any established connections to Tor guard-node IP ranges on ports 9001 or 9030; (3) running process list with parent-child relationships via `Get-Process` and `tasklist /v /fo csv`; (4) current clipboard contents snapshot; (5) list of all currently mounted removable drives via `Get-Volume`. Do NOT isolate the host until all five captures are complete.

Step 2: Detection — Confirm Microsoft Defender Antivirus definitions are current and scan all endpoints for the Trojan:Win32/CryptoBandits.A signature. In Microsoft Defender for Endpoint, query DeviceEvents for clipboard-related process activity (ClipboardSetContent events) initiated by WScript.exe, CScript.exe, or PowerShell. Hunt for .lnk files on removable media executing script interpreters. Look for outbound connections to Tor guard nodes (known Tor relay IP ranges and port 9001/9030). Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting); NIST SI-4 (System Monitoring — mapped from knowledge base as applicable monitoring control); CIS 8.2 (Collect Audit Logs).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate clipboard-hijack indicators, script-interpreter telemetry, removable-media LNK execution, and Tor C2 beaconing to confirm scope and classify the incident

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

Compensating: Without MDE: deploy Sysmon with a configuration that enables Event ID 23 (ClipboardChange) and Event ID 1 (Process Create) — filter for WScript.exe, CScript.exe, or powershell.exe as parent or child processes. Use the following PowerShell one-liner to hunt LNK files on all removable drives: `Get-ChildItem -Path (Get-Volume | Where DriveType -eq Removable | ForEach {$_.DriveLetter+':\'}) -Filter *.lnk -Recurse -Force 2>$null | Select FullName, LastWriteTime`. For Tor traffic without a SIEM, run Wireshark on the network egress point filtering for `tcp.port==9001 || tcp.port==9030` and cross-reference destination IPs against the public Tor relay consensus list (https://check.torproject.org/exit-addresses). Use a Sigma rule targeting Sysmon Event ID 3 (Network Connection) with destination port 9001/9030.

Evidence: This is a detection step that does not alter live system state; however, if a live host is being analyzed interactively, capture volatile data (RAM, netstat, process list) before running any scan that could trigger Defender quarantine and destroy artifacts. Key evidence sources specific to this clipper: (1) Windows Event Log — Microsoft-Windows-Sysmon/Operational, Event ID 23 (Clipboard changed), correlating process name to WScript.exe or CScript.exe; (2) Defender scan logs at C:\ProgramData\Microsoft\Windows Defender\Support\MPLog-*.log for Trojan:Win32/CryptoBandits.A detection timestamps; (3) removable media LNK target paths in Windows Event Log Event ID 4688 (Process Creation) showing script interpreter command lines; (4) DNS query logs or proxy logs for .onion resolver attempts or Tor guard-node IPs.

Step 3: Eradication — Remove all detected instances of Trojan:Win32/CryptoBandits.A using Microsoft Defender for Endpoint remediation actions. Audit and remove all unauthorized .lnk files on removable media across the environment. Block EVAL-pattern script execution through application control policies (e.g., Windows Defender Application Control or AppLocker). Block Tor network traffic at the perimeter firewall and DNS layer. Reference: NIST CM-7 (Least Functionality — no mapped control from knowledge base for application allowlisting specifically; citing general least-functionality principle); CIS 2.3 (Address Unauthorized Software); D3-FMBV (File Magic Byte Verification) to flag mismatched .lnk files.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove the clipper binary, propagation artifacts (weaponized LNK files), persistence mechanisms, and attacker C2 channel from all confirmed hosts before recovery begins

Controls: CIS 2.3 (Address Unauthorized Software), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Without MDE automated remediation: use Microsoft Defender CLI (`MpCmdRun.exe -Scan -ScanType 2`) on each host, then manually delete any quarantined-but-not-removed files. For LNK auditing without enterprise tooling, run: `Get-ChildItem -Path E:\ -Recurse -Force -Include *.lnk | Select-Object FullName, Target` (replace E:\ with the removable drive letter) and review any LNK whose target resolves to wscript.exe, cscript.exe, or powershell.exe. Block Tor at the DNS layer by adding a sinkhole entry for known Tor DNS bootstrapping domains (e.g., torproject.org) in your local DNS server or hosts file. For EVAL-pattern blocking without WDAC, use a Software Restriction Policy (SRP) via Local Group Policy to deny execution from %TEMP% and all removable drive paths.

Evidence: Before running Defender remediation (which will quarantine and potentially delete files), capture: (1) a full forensic image or at minimum a directory listing with hashes (`Get-FileHash`) of all Trojan:Win32/CryptoBandits.A-related files at their discovered paths; (2) export all current scheduled tasks via `schtasks /query /fo CSV /v > tasks_before_eradication.csv` — the clipper's persistence mechanism (T1547.005 Boot/Logon Autostart: Security Support Provider) may appear here; (3) export registry Run/RunOnce keys: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` and `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`; (4) copy all weaponized LNK files to a forensic collection share before deletion, preserving metadata; (5) export Windows Firewall connection logs and any perimeter firewall logs showing established Tor sessions before the block rule takes effect.

Step 4: Recovery — After eradication, re-image affected hosts where persistent scheduled tasks (T1547.005) were confirmed. Validate that no attacker-controlled scheduled tasks remain (audit Task Scheduler and registry Run keys). Verify clipboard behavior on recovered hosts with a controlled cryptocurrency address copy-paste test. Monitor for renewed Tor outbound connections for at least 30 days post-remediation. Reference: NIST IR-4 (Incident Handling — no mapped control in knowledge base; noting gap); D3-LAM (Local Account Monitoring) to detect residual backdoor activity.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore affected systems to a verified clean state, confirm eradication of clipboard-hijack and backdoor persistence, and establish monitoring to detect any reinfection via the USB propagation vector

Controls: NIST AC-2 (Account Management), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: Without enterprise imaging infrastructure: perform a clean OS reinstall from verified installation media (not from a USB that could be infected), then restore user data only after scanning it with an offline Defender boot scan or ClamAV. For the clipboard validation test without a formal test harness, open Notepad, type a known Bitcoin or Ethereum address, copy it, then paste into a second Notepad window and visually confirm the address is unchanged — perform this test before reconnecting the host to the network. For 30-day Tor monitoring without a SIEM, schedule a daily cron-equivalent PowerShell task that runs `Get-NetTCPConnection | Where-Object {$_.RemotePort -eq 9001 -or $_.RemotePort -eq 9030}` and emails the output to the SOC alias.

Evidence: Before reimaging, capture a final forensic image of the affected host's disk for evidentiary preservation, and collect: (1) full export of Task Scheduler XML definitions from `C:\Windows\System32\Tasks\` and `C:\Windows\SysWOW64\Tasks\`; (2) registry export of all autorun locations: HKLM and HKCU Run/RunOnce, `HKLM\SYSTEM\CurrentControlSet\Services` (for any rogue service installed by the backdoor), and `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon` (for SSP/Notify persistence); (3) a final `netstat -ano` and `Get-NetTCPConnection` to confirm no active Tor sessions remain; (4) Windows Security Event Log filtered for Event ID 4698 (Scheduled Task Created) and 4702 (Scheduled Task Updated) covering the infection window.

Step 5: Post-Incident — Conduct a USB device inventory and enforce CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) to include removable media. Implement CIS 6.3 and CIS 6.5 (Require MFA for Externally-Exposed Applications and Administrative Access) to limit blast radius if backdoor credentials were harvested. Review and enforce least-privilege policies (NIST AC-6) for accounts permitted to execute scripting engines. Brief employees handling cryptocurrency transactions on clipboard hijacking risks. Reference: CIS

7.1 (Establish and Maintain a Vulnerability Management Process) to track USB-borne threat remediation.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: conduct lessons-learned review, update USB device control and scripting execution policies, and improve detection coverage to prevent reintroduction of the CryptoBandits clipper via the same removable-media propagation chain

Controls: CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), NIST AC-6 (Least Privilege), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Without a formal asset management platform: maintain the USB device inventory as a versioned CSV in a shared drive, recording device serial number, assigned user, date of last scan, and authorization status — review weekly per CIS 1.2. For MFA on administrative accounts without an enterprise IdP, enable Windows Hello for Business or use free TOTP (e.g., Google Authenticator with a PAM-compatible wrapper) for any admin account. For scripting engine least-privilege enforcement without WDAC, use Local Group Policy to set 'Allow log on locally' and script-engine execution rights to named admin accounts only, removing standard user permissions to invoke WScript.exe and CScript.exe directly.

Evidence: Post-incident evidence collection for lessons learned and potential regulatory notification: (1) compile the full timeline of Trojan:Win32/CryptoBandits.A detections across all endpoints from Defender logs, correlated with USB insertion events (Windows Event ID 2003/2100 from Microsoft-Windows-DriverFrameworks-UserMode/Operational) to establish the propagation chain; (2) inventory all cryptocurrency transactions made by affected users during the infection window — compare clipboard-captured addresses against blockchain transaction records to determine whether any financial loss occurred and quantify the blast radius; (3) extract all unique attacker-controlled wallet addresses observed in clipboard-swap events from memory forensics and log analysis for threat intelligence sharing; (4) document all accounts that authenticated to the Tor-backed backdoor C2 channel for credential-rotation prioritization.

Detection Guidance

Primary detection signature: Trojan:Win32/CryptoBandits.A in Microsoft Defender Antivirus and Microsoft Defender for Endpoint. Ensure definitions are current before scanning.

Behavioral indicators to hunt in Microsoft Defender for Endpoint Advanced Hunting:

- WScript.exe or CScript.exe spawning PowerShell, or PowerShell executing base64-encoded or EVAL-pattern commands (look for Invoke-Expression combined with web requests).

- .lnk files on removable media volumes (DeviceFileEvents where FolderPath starts with removable drive letter and FileName ends in .lnk) spawning script interpreters.

- ClipboardSetContent events where the setting process is a script interpreter rather than a user-facing application.

- Scheduled task creation (DeviceRegistryEvents targeting HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache) by non-standard parent processes.

- Outbound TCP connections to Tor guard relay IP ranges on ports 9001 or 9030 from endpoint processes.

Network-level indicators:

- DNS queries for .onion domains or Tor directory authority hostnames.

- Unexpected encrypted outbound traffic on ports 9001/9030 from workstations.

Host-level indicators:

- New scheduled tasks with randomized names or pointing to script files in %TEMP% or %APPDATA%.

- Registry Run/RunOnce keys referencing WScript, CScript, or PowerShell with encoded arguments.

- Unusual .lnk files in USB drive root directories.

Reference: NIST AU-6, AU-12; CIS 8.2; D3-SFA (System File Analysis) for monitoring script interpreter startup configuration; D3-LAM (Local Account Monitoring) for backdoor-related account activity.

Indicators of Compromise

Type	Value	Context	Confidence
HASH	`not-disclosed-in-source`	No file hashes for Trojan:Win32/CryptoBandits.A were published in the referenced Microsoft Security Blog post. Use the Microsoft Defender detection signature for identification.	LOW
DOMAIN	`Tor network infrastructure (C2 routes over Tor anonymization network)`	C2 communications route over Tor; no specific .onion addresses or Tor guard relay IPs were disclosed in source reporting. Block Tor relay ranges and port 9001/9030 at the perimeter.	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1115** — Clipboard Data
- **T1059.007** — JavaScript
- **T1071.001** — Web Protocols
- **T1059.001** — PowerShell
- **T1041** — Exfiltration Over C2 Channel
- **T1547** — Boot or Logon Autostart Execution
- **T1565.001** — Stored Data Manipulation
- **T1497.001** — System Checks
- **T1091** — Replication Through Removable Media
- **T1059.006** — Python
- **T1059.005** — Visual Basic
- **T1547.005** — Security Support Provider
- **T1027** — Obfuscated Files or Information
- **T1113** — Screen Capture
- **T1025** — Data from Removable Media
- **T1090.003** — Multi-hop Proxy

- **T1140** — Deobfuscate/Decode Files or Information

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary 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
- **8.2** — Collect Audit Logs

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1115	Clipboard Data	Collection
T1059.007	JavaScript	Execution
T1071.001	Web Protocols	Command-And-Control
T1059.001	PowerShell	Execution
T1041	Exfiltration Over C2 Channel	Exfiltration
T1547	Boot or Logon Autostart Execution	Persistence
T1565.001	Stored Data Manipulation	Impact
T1497.001	System Checks	Defense-Evasion
T1091	Replication Through Removable Media	Lateral-Movement
T1059.006	Python	Execution

Technique ID	Technique Name	Tactic
T1059.005	Visual Basic	Execution
T1547.005	Security Support Provider	Persistence
T1027	Obfuscated Files or Information	Defense-Evasion
T1113	Screen Capture	Collection
T1025	Data from Removable Media	Collection
T1090.003	Multi-hop Proxy	Command-And-Control
T1140	Deobfuscate/Decode Files or Information	Defense-Evasion

Sources

Source	URL	Tier
Microsoft Security Blog	https://www.microsoft.com/en-us/security/blog/2026/06/17/crypto-cli...	T1
	https://www.microsoft.com/en-us/security/blog/2026/06/17/crypto-cli...	T1
	https://www.microsoft.com/en-us/security/blog/2026/02/02/infosteale...	T1
	https://www.microsoft.com/en-us/security/blog/2025/12/09/shai-hulud...	T1
Microsoft Defender Antivirus in Windows Overview	https://learn.microsoft.com/en-us/defender-endpoint/microsoft-defen...	T1

Generated 2026-06-18 07:17 UTC by TJS Security Command Center