INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-18 14:14 UTC

USB-Delivered Crypto Clipper Combines Tor C2, Worm Propagation, and Runtime Code Execution in Active Campaign

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0509
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Windows, detected as Trojan:Win32/CryptoBandits.A by Microsoft Defender for Endpoint and Microsoft Defender Antivirus
Published	2026-06-17T23:11:43+00:00
Discovery Source	Rss:T1 Threatintel

Executive Summary

Since February 2026, a cryptocurrency-stealing malware campaign has been spreading across Windows environments via infected USB drives. The malware, tracked as Trojan:Win32/CryptoBandits.A, silently intercepts cryptocurrency transactions and redirects funds to attacker-controlled wallets; a built-in backdoor capability also allows attackers to execute arbitrary commands on compromised systems. Any organization where employees connect USB drives to Windows workstations is exposed, with direct financial loss and potential full system compromise as the primary business risks.

Technical Analysis

Trojan:Win32/CryptoBandits.A is a Windows-targeting cryptocurrency clipper active since February 2026, distributed via malicious LNK files placed on USB drives (T1091, Replication Through Removable Media). On execution, the malware establishes a Tor-routed C2 channel (T1090.003, Proxy: Multi-hop Proxy) for covert command communication and performs clipboard hijacking (T1115, Clipboard Data) to intercept and substitute cryptocurrency wallet addresses mid-transaction, redirecting funds to attacker-controlled wallets (T1496, Resource Hijacking). A critical EVAL command capability converts the implant into a functional backdoor, enabling arbitrary runtime code execution via PowerShell (T1059.001), JavaScript (T1059.007), and Python (T1059.006). The malware employs multi-layer obfuscation (T1027), hides artifacts using hidden files and directories (T1564.001), achieves persistence via scheduled tasks and registry modifications (T1547.005, T1112, including Defender exclusions), and captures screen activity (T1113). Worm-like USB propagation

enables lateral spread without network connectivity. No CVE identifier is associated with this campaign. Relevant CWEs include CWE-494 (Download of Code Without Integrity Check), CWE-506 (Embedded Malicious Code), and CWE-311 (Missing Encryption of Sensitive Data). Detection name: Trojan:Win32/CryptoBandits.A (Microsoft Defender for Endpoint, Microsoft Defender Antivirus). Threat actor attribution is unknown. Primary source: Microsoft Security Blog, 2026-06-17.

Action Checklist

1. Step 1: Containment, Enforce USB/removable media restrictions via Group Policy (Computer Configuration > Administrative Templates > System > Removable Storage Access) on all Windows endpoints immediately. Isolate any host where Microsoft Defender has fired the Trojan:Win32/CryptoBandits.A detection from the network pending investigation. Disable autorun/autoplay across the environment if not already enforced (NIST CM controls; CIS 4.6, Securely Manage Enterprise Assets and Software).
2. Step 2: Detection, Query Microsoft Defender for Endpoint telemetry and antivirus logs for detection name 'Trojan:Win32/CryptoBandits.A'. Hunt for: anomalous LNK file executions from removable media paths (Event ID 4688, process creation logs); PowerShell, Python, or JavaScript processes spawned from unusual parent processes or USB-associated paths; outbound Tor traffic patterns (connections to known Tor entry nodes on port 9001/9030, or encrypted traffic to unlisted IPs over non-standard ports); scheduled task creation events (Event ID 4698) not tied to known software; and registry modifications under HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions. Cross-reference clipboard access events against cryptocurrency address regex patterns (Bitcoin: ^[13][a-km-zA-HJ-NP-Z1-9]{25,34}$; Ethereum: ^0x[a-fA-F0-9]{40}$). Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs).
3. Step 3: Eradication, On confirmed infected hosts: run a full Microsoft Defender offline scan to ensure detection and quarantine of Trojan:Win32/CryptoBandits.A. Remove any scheduled tasks, registry run keys, or Defender exclusion entries created by the malware. Purge malicious LNK files from USB drives and connected shares. Ensure Defender definitions are current (update via Windows Update or WSUS). Apply NIST SI-3 (Malicious Code Protection) principles: verify real-time protection is enabled and cloud-delivered protection is active across all endpoints.
4. Step 4: Recovery, Before returning isolated hosts to production, verify: Defender detections are resolved and no residual scheduled tasks or registry persistence artifacts remain; clipboard monitoring returns expected behavior with no address substitution; outbound Tor traffic has ceased. Monitor reinstated hosts for 72 hours using Defender for Endpoint behavioral alerts. Validate that USB policy enforcement is confirmed active via Group Policy Results (gpresult). Reference NIST AU-12 (Audit Record Generation) to confirm logging is intact post-remediation.
5. Step 5: Post-Incident, Conduct a USB usage policy review; implement device control policies restricting removable media to approved, inventoried devices (CIS 1.1, Establish and Maintain Detailed Enterprise Asset Inventory). Assess whether cryptocurrency-related applications or browser extensions are present on enterprise endpoints and evaluate whether they are authorized. Review Defender exclusion lists organization-wide for unauthorized entries (NIST AC-6, Least Privilege). Brief finance and treasury teams on clipboard-hijacking risks for any cryptocurrency transaction workflows. Consider deploying Defender Local Account Monitoring and Defender System File Analysis as ongoing countermeasures.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to senior IR leadership, legal counsel, and finance/treasury if: any confirmed transaction redirect is detected (indicating actual financial loss), if the backdoor command execution capability shows evidence of use beyond clipboard hijacking (e.g., data exfiltration artifacts or lateral movement beyond the initial USB infection vector), or if more than 10 endpoints show Trojan:Win32/CryptoBandits.A detections indicating worm propagation has reached a scale requiring coordinated enterprise-wide response and potential breach notification assessment.
Recovery Notes	Before returning any host to production, validate clipboard integrity with a live address-substitution test using a known cryptocurrency address pattern, confirm all Tor-associated network connections have ceased via 'Get-NetTCPConnection', and verify USB Group Policy restrictions are applied and confirmed via 'gpresult /r'. Monitor reinstated hosts for a minimum of 72 hours with Sysmon or MDE behavioral alerts focused specifically on LNK execution from removable media paths, scheduled task creation (Event ID 4698), and outbound connections to ports 9001/9030. Given the worm's self-propagation capability, any new Trojan:Win32/CryptoBandits.A Defender alert during the watch period should trigger immediate re-isolation and a fresh sweep of all USB drives that were connected to the reinstated host.
Forensic Artifacts	Windows Security Event Log Event ID 6416 (A new external device was recognized by the system) correlated with Event ID 4688 (Process Creation) on the same host within the same session — establishes USB insertion-to-execution timeline specific to CryptoBandits.A's USB delivery vector | Malicious LNK files recovered from infected USB drives and any network shares the worm propagated to — LNK targets will reveal the malware's execution chain (e.g., cmd.exe or wscript.exe launching the payload from the USB root path) | Registry export of HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions showing paths or process names the malware added to evade real-time Defender scanning — timestamps on these registry keys establish attacker dwell time | Windows Task Scheduler operational log (Microsoft-Windows-TaskScheduler/Operational) Event ID 106 (task registered) and Event ID 200 (task executed) for tasks created by Trojan:Win32/CryptoBandits.A to maintain persistence across reboots — cross-reference task creation timestamps with USB insertion events | Memory image (RAM dump) analyzed for injected clipboard-monitoring code and active Tor circuit state — in-memory artifacts will show the attacker-controlled wallet addresses the clipper was substituting and any Tor relay node IPs used for C2 communication

Per-Action IR Details

Step 1: Containment — Enforce USB/removable media restrictions via Group Policy (Computer Configuration > Administrative Templates > System > Removable Storage Access) on all Windows endpoints immediately. Isolate any host where Microsoft Defender has fired the Trojan:Win32/CryptoBandits.A detection from the network pending investigation. Disable autorun/autoplay across the environment if not already enforced (NIST CM controls; CIS 4.6 — Securely Manage Enterprise Assets and Software).

NIST Phase: Containment

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

Controls: NIST AC-3 (Access Enforcement), NIST AC-19 (Access Control For Mobile Devices), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: Without enterprise MDM/GPO infrastructure, use the free Microsoft Security Compliance Toolkit (SCT) to push a local Group Policy object blocking removable storage (set HKLM\SOFTWARE\Policies\Microsoft\Windows\RemovableStorageDevices to Deny_All = 1 via reg.exe). For immediate network isolation of a confirmed host, run 'netsh advfirewall set allprofiles firewallpolicy blockinbound,blockoutbound' from an elevated command prompt. Document the exact timestamp of isolation.

Evidence: Before isolating any host that fired Trojan:Win32/CryptoBandits.A, capture: (1) live memory image using Magnet RAM Capture or WinPmem to preserve in-memory Tor circuit state and injected clipboard-hijacking code; (2) full 'netstat -ano' and 'Get-NetTCPConnection' output to record active Tor relay connections on ports 9001/9030; (3) running process list via 'tasklist /v /fo csv' and 'Get-Process | Select-Object *' to capture any worm propagation processes or Python/JS runtimes spawned from USB paths; (4) contents of all currently mounted removable media paths (e.g., E:\ or D:\) including hidden and system files to capture LNK files and malware payloads before the drive is removed. All captures must precede network isolation.

Step 2: Detection — Query Microsoft Defender for Endpoint telemetry and antivirus logs for detection name 'Trojan:Win32/CryptoBandits.A'. Hunt for: anomalous LNK file executions from removable media paths (Event ID 4688, process creation logs); PowerShell, Python, or JavaScript processes spawned from unusual parent processes or USB-associated paths; outbound Tor traffic patterns (connections to known Tor entry nodes on port 9001/9030, or encrypted traffic to unlisted IPs over non-standard ports); scheduled task creation events (Event ID 4698) not tied to known software; and registry modifications under HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions. Cross-reference clipboard access events against cryptocurrency address regex patterns (Bitcoin: ^[13][a-km-zA-HJ-NP-Z1-9]{25,34}$; Ethereum: ^0x[a-fA-F0-9]{40}$). Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs).

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-2 (Event Logging), CIS 8.2 (Collect Audit Logs)

Compensating: Without MDE, deploy Sysmon with a configuration that enables ProcessCreate (Event ID 1), NetworkConnect (Event ID 3), and FileCreate (Event ID 11) events; use the SwiftOnSecurity Sysmon config as a baseline and add a rule filtering for image paths matching removable media drive letters. Use Sigma rule 'proc_creation_win_lnk_from_removable_media' to detect LNK execution from USB paths. For Tor detection without a SIEM, run 'Get-NetTCPConnection | Where-Object {$_.RemotePort -eq 9001 -or $_.RemotePort -eq 9030}' hourly via Task Scheduler. Use Wireshark with display filter 'tcp.port == 9001 || tcp.port == 9030' on the network gateway. For clipboard monitoring, deploy a lightweight YARA rule scanning memory for Bitcoin (regex ^[13][a-km-zA-HJ-NP-Z1-9]{25,34}$) and Ethereum (^0x[a-fA-F0-9]{40}$) address patterns.

Evidence: This step is analytical and does not alter live state; however, before querying or touching any suspect host interactively, confirm volatile capture from Step 1 is complete. Key evidence sources for this campaign: Windows Security Event Log Event ID 4688 filtered on parent process being explorer.exe or the USB drive path (e.g., E:\) spawning cmd.exe, powershell.exe, python.exe, or wscript.exe; Event ID 4698 in the Task Scheduler log (Microsoft-Windows-TaskScheduler/Operational) for tasks created during the suspected compromise window; registry export of HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions to identify paths or processes the malware whitelisted to evade detection; Defender quarantine log at C:\ProgramData\Microsoft\Windows Defender\Support\MPLog-*.log for Trojan:Win32/CryptoBandits.A detection timestamps; Windows Defender event log (Event ID 1116 — malware detected, Event ID 1117 — remediation action taken) for detection history across all endpoints.

Step 3: Eradication — On confirmed infected hosts: run a full Microsoft Defender offline scan to ensure detection and quarantine of Trojan:Win32/CryptoBandits.A. Remove any scheduled tasks, registry run keys, or Defender exclusion entries created by the malware. Purge malicious LNK files from USB drives and connected shares. Ensure Defender definitions are current (update via Windows Update or WSUS). Apply NIST SI-3 (Malicious Code Protection) principles: verify real-time protection is enabled and cloud-delivered

protection is active across all endpoints.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-6 (Least Privilege), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Without WSUS or centralized patch management, run 'Update-MpSignature' via PowerShell on each host to force Defender definition update, then trigger an offline scan with 'Start-MpScan -ScanType OfflineScan'. To enumerate and remove malicious scheduled tasks, run 'Get-ScheduledTask | Where-Object {$_.Date -gt (Get-Date).AddDays(-30)} | Export-Csv suspicious_tasks.csv' and manually review output against known-good baselines. Remove confirmed malicious tasks with 'Unregister-ScheduledTask -TaskName -Confirm:$false'. For registry persistence cleanup, export and diff HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run and HKCU equivalent against a known-clean baseline using 'reg export'. Use SysinternalsSuite Autoruns (free) to enumerate all persistence mechanisms including scheduled tasks, run keys, and Defender exclusions in a single view — review against VirusTotal integration to flag malicious entries.

Evidence: Before running the Defender offline scan or deleting any artifacts (which will alter or destroy evidence), ensure the following are preserved from the live system: (1) full registry export of HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, and HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions; (2) export of all scheduled tasks via 'schtasks /query /fo CSV /v > schtasks_export.csv'; (3) copy of all malicious LNK files from USB drives and any network shares the worm reached — preserve them in a password-protected ZIP for forensic review; (4) Prefetch files from C:\Windows\Prefetch\ for any executables launched from USB paths (e.g., filenames containing drive letters E:\ or F:\) to establish execution history before they are overwritten; (5) a disk image or at minimum a file hash inventory (SHA-256) of all files in the malware's identified drop directories before eradication deletes them.

Step 4: Recovery — Before returning isolated hosts to production, verify: Defender detections are resolved and no residual scheduled tasks or registry persistence artifacts remain; clipboard monitoring returns expected behavior with no address substitution; outbound Tor traffic has ceased. Monitor reinstated hosts for 72 hours using Defender for Endpoint behavioral alerts. Validate that USB policy enforcement is confirmed active via Group Policy Results (gpresult). Reference NIST AU-12 (Audit Record Generation) to confirm logging is intact post-remediation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-12 (Audit Record Generation), NIST AU-3 (Content Of Audit Records), CIS 8.2 (Collect Audit Logs)

Compensating: Without MDE behavioral alerting for the 72-hour watch period, configure a Sysmon + Windows Event Forwarding (WEF) rule to a central collector (even a single Windows Server with a shared folder and a scheduled PowerShell aggregation script) monitoring for Event ID 4688 (process creation from non-standard paths), Event ID 3 (Sysmon NetworkConnect to Tor ports 9001/9030), and Event ID 13 (Sysmon RegistryValueSet under Defender exclusion keys). Validate clipboard integrity by opening a known-good cryptocurrency address in Notepad, copying it, and pasting into a second window — if the pasted value differs, clipboard hijacking is still active. Run 'gpresult /r /scope computer' on each reinstated host and confirm 'Removable Storage Access' policies appear under Applied GPOs.

Evidence: Before reconnecting an isolated host to the production network, confirm: (1) a clean Defender offline scan result with no Trojan:Win32/CryptoBandits.A detections (log at C:\ProgramData\Microsoft\Windows Defender\Support\MPLog-*.log); (2) 'Get-NetTCPConnection' output showing no established or time-wait connections to Tor relay IPs or ports 9001/9030 — document this output with a timestamp; (3) a final Autoruns export showing no unauthorized scheduled tasks, run keys, or Defender exclusions remain; (4) confirmation that Windows Security Event Log auditing (Event IDs 4688, 4698) and Sysmon are generating events correctly — run a benign test process and verify it appears in the log within 60 seconds to confirm logging is intact and was not disabled by the malware.

Step 5: Post-Incident — Conduct a USB usage policy review; implement device control policies restricting removable media to approved, inventoried devices (CIS 1.1 — Establish and Maintain Detailed Enterprise Asset Inventory). Assess whether cryptocurrency-related applications or browser extensions are present on enterprise endpoints and evaluate whether they are authorized. Review Defender exclusion lists organization-wide for unauthorized entries (NIST AC-6 — Least Privilege). Brief finance and treasury teams on clipboard-hijacking risks for any cryptocurrency transaction workflows. Consider deploying D3-LAM (Local Account Monitoring) and D3-SFA (System File Analysis) as ongoing countermeasures.

NIST Phase: Post Incident

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

Controls: NIST AC-6 (Least Privilege), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Without enterprise device management for USB allowlisting, use Windows built-in Device Installation Restrictions via Group Policy (Computer Configuration > Administrative Templates > System > Device Installation > Device Installation Restrictions) to permit only devices matching approved hardware IDs — export approved device IDs with 'Get-PnpDevice | Select-Object FriendlyName, InstanceId | Export-Csv approved_devices.csv'. For a free software inventory to identify unauthorized cryptocurrency wallets or browser extensions, use Sysinternals Autoruns and 'Get-ItemProperty HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall*' combined with a manual review of Chrome/Edge extension IDs under %LOCALAPPDATA%\Google\Chrome\User Data\Default\Extensions. For ongoing Defender exclusion auditing, schedule a weekly PowerShell script running 'Get-MpPreference | Select-Object ExclusionPath, ExclusionProcess, ExclusionExtension | Export-Csv defender_exclusions_$(Get-Date -f yyyyMMdd).csv' and diff against the previous week's output.

Evidence: Post-incident documentation should include: (1) the complete forensic timeline of the CryptoBandits.A campaign across all affected hosts, correlating USB insertion events (Event ID 6416 — new external device recognized) with first malware execution timestamps from Event ID 4688 and Defender detection logs; (2) a list of all cryptocurrency wallet addresses the malware attempted to substitute, extracted from clipboard capture artifacts or memory analysis during the investigation phase — these should be reported to relevant cryptocurrency exchanges as threat intelligence; (3) the full Defender exclusion registry export from all hosts showing which exclusions were unauthorized and when they were created, to establish attacker dwell time; (4) a final report correlating the worm propagation path across the environment by mapping USB insertion events across all hosts during the campaign window, identifying patient zero and all downstream infections.

Detection Guidance

Primary detection signal: Microsoft Defender for Endpoint and Microsoft Defender Antivirus alert on detection name Trojan:Win32/CryptoBandits.A. For environments without full EDR coverage, layer the following: (1) Process creation logs (Event ID 4688), flag wscript.exe, cscript.exe, powershell.exe, python.exe, or node.exe spawned from removable media drive letters or %TEMP% paths; (2) Scheduled task creation (Event ID 4698/4702), review tasks created outside standard software deployment windows; (3) Registry modification events (Event ID 4657), monitor writes to HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions and common persistence keys under HKCU\Software\Microsoft\Windows\CurrentVersion\Run; (4) Network telemetry, flag outbound connections to Tor infrastructure (known Tor relay IPs, port 9001/9030, or high-entropy domain patterns); (5) Clipboard behavioral indicators, monitor for clipboard access by non-UI processes, particularly at times coinciding with browser or wallet activity; (6) LNK file creation on removable media, alert on .lnk files written to USB-attached volumes. IOC patterns for wallet address substitution: monitor clipboard contents for substitution of Bitcoin (^[13][a-km-zA-HJ-NP-Z1-9]{25,34}$) or Ethereum (^0x[a-fA-F0-9]{40}$) addresses not matching expected organizational wallet addresses. Reference NIST AU-2 (Event Logging) and AU-6 (Audit Record Review) for logging scope requirements.

Indicators of Compromise

Type	Value	Context	Confidence
HASH	`Trojan:Win32/CryptoBandits.A`	Microsoft Defender detection name for the USB-delivered cryptocurrency clipper; use as hunt string in Defender for Endpoint alert telemetry	HIGH

Framework Mappings

MITRE-ATTACK

- **T1090.003** — Multi-hop Proxy
- **T1071** — Application Layer Protocol
- **T1041** — Exfiltration Over C2 Channel
- **T1027** — Obfuscated Files or Information
- **T1564.001** — Hidden Files and Directories
- **T1115** — Clipboard Data
- **T1091** — Replication Through Removable Media
- **T1547** — Boot or Logon Autostart Execution
- **T1547.005** — Security Support Provider
- **T1113** — Screen Capture
- **T1112** — Modify Registry
- **T1059.001** — PowerShell
- **T1059** — Command and Scripting Interpreter
- **T1059.007** — JavaScript
- **T1496** — Resource Hijacking
- **T1059.006** — Python

NIST-800-53R5

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1090.003	Multi-hop Proxy	Command-And-Control
T1071	Application Layer Protocol	Command-And-Control
T1041	Exfiltration Over C2 Channel	Exfiltration
T1027	Obfuscated Files or Information	Defense-Evasion
T1564.001	Hidden Files and Directories	Defense-Evasion
T1115	Clipboard Data	Collection
T1091	Replication Through Removable Media	Lateral-Movement
T1547	Boot or Logon Autostart Execution	Persistence
T1547.005	Security Support Provider	Persistence
T1113	Screen Capture	Collection
T1112	Modify Registry	Defense-Evasion
T1059.001	PowerShell	Execution
T1059	Command and Scripting Interpreter	Execution
T1059.007	JavaScript	Execution
T1496	Resource Hijacking	Impact
T1059.006	Python	Execution

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://thehackernews.com/2026/06/microsoft-details-windows-clipper...	T3
	https://www.microsoft.com/en-us/security/blog/2026/02/02/infosteale...	T1

Source	URL	Tier
r/antivirus - Windows Defender picked up a Trojan, what do I do?	https://www.reddit.com/r/antivirus/comments/1t2l6tk/windows_defende...	T3

Generated 2026-06-18 14:14 UTC by TJS Security Command Center