INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:35 UTC

LeakNet Ransomware Adopts ClickFix Social Engineering and Deno In-Memory Loader to Eliminate Access Broker Dependency

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0061
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Windows OS (msiexec.exe, cmd.exe, PsExec), Microsoft Teams, AWS S3, Deno JavaScript Runtime
Published	2026-03-21

Executive Summary

LeakNet ransomware has abandoned third-party access brokers in favor of direct social engineering through compromised websites and Microsoft Teams, reducing the group's operational costs and making early detection harder. The campaign uses an in-memory loader built on the Deno JavaScript runtime to execute ransomware without writing files to disk, bypassing most traditional antivirus controls. Organizations running Windows environments with Teams and AWS S3 face elevated risk of data encryption and exfiltration with fewer conventional warning signals.

Technical Analysis

LeakNet has retooled its initial access methodology, replacing purchased access from initial access brokers (IABs) with ClickFix-style social engineering lures delivered via compromised legitimate websites and Microsoft Teams messages. Victims are prompted to execute a malicious msiexec.exe command, which downloads and launches a Deno JavaScript runtime-based loader. The loader executes the ransomware payload entirely in memory (T1620, Reflective Code Loading; T1059.007, JavaScript interpreter abuse), bypassing on-disk antivirus detection (CWE-693: Protection Mechanism Failure). Post-exploitation follows a structured sequence: credential discovery via klist (T1558), lateral movement using PsExec (T1569.002, Service Execution), DLL side-loading (T1574.002), and data exfiltration to attacker-controlled AWS S3 buckets (T1537). Ransomware encryption executes as the final stage (T1486). No CVE is associated with this campaign; the attack chain relies on user execution (T1204.002) and living-off-the-land binaries (LOLBins) rather than software vulnerabilities. Source quality is T3-dominant with one T1 Microsoft reference on the broader Node.js/Deno abuse pattern; specific LeakNet technical indicators should be validated against primary threat intelligence feeds before

production use.

Action Checklist

1. Step 1, Immediate: Block or alert on Deno runtime (deno.exe) execution across all endpoints; it has no standard enterprise use case and its presence is a high-confidence anomaly.
2. Step 2, Immediate: Restrict or monitor msiexec.exe spawning child processes or making outbound network connections; apply AppLocker or WDAC rules to prevent msiexec.exe from executing payloads retrieved from remote URLs.
3. Step 3, Detection: Hunt for the post-exploitation sequence, klist execution followed by PsExec lateral movement followed by outbound S3 traffic, as a behavioral chain; any two of three in close succession warrants investigation.
4. Step 4, Detection: Review Microsoft Teams external message policies; restrict or disable the ability for external/unmanaged accounts to send executable content or links to internal users.
5. Step 5, Assessment: Inventory endpoints for Deno runtime installation and audit AWS S3 bucket policies and CloudTrail logs for unexpected PutObject calls from internal hosts.
6. Step 6, Communication: Notify SOC, endpoint, and cloud security teams of the behavioral indicators; brief IT help desk staff on ClickFix lure patterns so they can identify and escalate user-reported pop-ups requesting command execution.
7. Step 7, Long-term: Evaluate EDR telemetry coverage for in-memory JavaScript execution and reflective loading; tune SIEM rules to correlate msiexec.exe network activity, Deno process creation, PsExec service installation, and S3 exfiltration events into a single detection chain mapped to this kill chain.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to external IR firm or law enforcement if any deno.exe execution, PsExec lateral movement, or S3 exfiltration events are confirmed within your environment, or if ClickFix phishing emails with successful user interaction (opened, clicked link, ran command) reach more than 5 users.
Recovery Notes	Post-containment: re-image or forensically wipe any endpoint where deno.exe, unsigned msiexec.exe payloads, or PsExec service artifacts were discovered. Restore from clean backup or clean OS image dated before first suspected LeakNet contact. Verify S3 bucket integrity: compare object metadata (creation time, owner, size) against known good backup for any unexpected or modified objects; delete/restore modified objects from versioning history if S3 versioning was enabled. Force password reset for all service accounts with S3 access and any accounts that accessed the compromised endpoints during the exposure window. Implement EDR agent mandatory deployment; enable in-memory execution detection. Restrict Teams external federation to pre-approved list only.

Forensic Artifacts	Windows Event Log 4688 (Process Creation) - klist.exe, deno.exe, msiexec.exe, PsExec execution with parent PID and command line | Sysmon Event IDs 1 (Process Creation), 3 (Network Connection), 5 (Process Termination), 10 (CreateRemoteThread) - in-memory loader signature and network beaconing | Windows Event Log 7045 (Service Installation) - PsExec service creation artifacts and service binary path | AWS CloudTrail logs (PutObject, ListBucket, GetObject API calls) - S3 exfiltration timeline, source IP, affected buckets and object keys | File system artifacts - deno.exe binary location, hash, timestamps, AppData/Local/Temp directories for unsigned executables and Deno cache directories (%USERPROFILE%\.deno)

Per-Action IR Details

Step 1 — Immediate: Block or alert on Deno runtime (deno.exe) execution across all endpoints; it has no standard enterprise use case and its presence is a high-confidence anomaly.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation phase: tools and resource acquisition)

Controls: NIST 800-53 SI-4 (Information System Monitoring), NIST 800-53 CA-7 (Continuous Monitoring), CIS Controls 6.1 (Establish and Maintain Detailed Asset Inventory), CIS Controls 8.1 (Establish and Maintain Endpoint Detection and Response)

Compensating: Organizations without EDR: Configure Windows Sysmon Event ID 1 (Process Creation) logging to capture deno.exe execution, filter on Image ends with 'deno.exe', export to CSV daily via Event Viewer or PowerShell Get-WinEvent. Set up file hash monitoring using baseline-compare approach: hash all executables in C:\Program Files and C:\Users via Tripwire or similar (free: use certUtil -hashfile script). Alert on hash mismatches or unexpected deno.exe presence in %TEMP%, %APPDATA%, or Downloads folders.

Evidence: Capture Windows Event Log 4688 (Process Creation) or Sysmon Event ID 1 for full command line of any deno.exe execution; preserve parent process, PPID, and file path. Export full event XML. Capture file metadata (creation time, modification time, digital signature) for any deno.exe found: certUtil -hashfile SHA256. Preserve memory dump if deno.exe is found running (tasklist /v | find deno, then run full process dump via procdump or WinDbg for in-memory analysis).

Step 2 — Immediate: Restrict or monitor msiexec.exe spawning child processes or making outbound network connections; apply AppLocker or WDAC rules to prevent msiexec.exe from executing payloads retrieved from remote URLs.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation: hardening and baseline control configuration)

Controls: NIST 800-53 CM-2 (Baseline Configuration), NIST 800-53 CM-6 (Configuration Settings), CIS Controls 2.3 (Address Unauthorized Software), CIS Controls 6.1 (Establish Endpoint Security Configuration)

Compensating: Organizations without AppLocker/WDAC: Create a Group Policy Restricted Groups policy to deny msiexec.exe execute permissions for all non-admin users (if applicable). For monitoring without blocking: enable Sysmon Event ID 1 (Process Creation) and Event ID 3 (Network Connection) filtering on Image='C:\Windows\System32\msiexec.exe'; correlate any child process creation (e.g., powershell.exe, cmd.exe spawned by msiexec.exe) or outbound traffic on ports 80/443/8080. Export daily to centralized log aggregation. Alternative: use Windows Defender Firewall rules to block msiexec.exe outbound on all ports except required MSI installation sources (internal file servers only); document approved source IPs in firewall rule descriptions.

Evidence: Before applying restrictions: export current msiexec.exe execution baseline from Event Log 4688 (last 30 days) to identify legitimate MSI deployments and establish baseline child processes and network destinations. Capture network traffic (Netmon .etl file or Wireshark pcap) during any msiexec.exe execution for 5 minutes before and 30 minutes after to establish normal vs. anomalous network behavior. Document all legitimately signed MSIs deployed in the environment by file hash (SHA256) for future baselining.

Step 3 — Detection: Hunt for the post-exploitation sequence — klist execution followed by PsExec lateral movement followed by outbound S3 traffic — as a behavioral chain; any two of three in close succession warrants investigation.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 (Detection and Analysis phase: indicators of compromise and attack chains)

Controls: NIST 800-53 SI-4 (Information System Monitoring), NIST 800-53 AU-6 (Audit Review, Analysis, and Reporting), CIS Controls 8.4 (Ensure Adequate Audit Logging is Enabled), CIS Controls 8.7 (Perform Search Query Audits)

Compensating: Organizations without SIEM: Aggregate Windows Event Logs from a central collection server daily using WinRM Pull Subscription or logstash-free alternative (e.g., filebeats + rsyslog). Hunt manually for: (1) Event ID 4688 or Sysmon 1 for 'klist.exe' execution with timestamp; (2) Event ID 4688 for 'psexec' or remote service installation (Event ID 5145 SMB object open, or Event ID 5156 outbound connection to TCP 445); (3) AWS CloudTrail logs showing PutObject calls to S3 buckets within 10-30 minutes of klist+psexec events. Correlate manually by endpoint hostname and timestamp. Export matches to ticket. Establish threshold: any two of three = investigate.

Evidence: Capture Windows Event Log 4688 (Process Creation) entries for klist.exe with full command line and PPID; Event ID 7045 (Service Installation) for any psexec-style service creation; Event ID 5145 (SMB Network Object Open) for remote file share access; Sysmon Event ID 3 (Network Connection) for outbound TCP 445 or 139; AWS CloudTrail logs (API calls: PutObject, ListBucket, GetObject) filtered by source IP matching internal endpoints. Preserve system uptime/boot time (Get-CimInstance Win32_OperatingSystem LastBootUpTime) to correlate with event sequence timing.

Step 4 — Detection: Review Microsoft Teams external message policies; restrict or disable the ability for external/unmanaged accounts to send executable content or links to internal users.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation: access control and communication policies)

Controls: NIST 800-53 AC-2 (Account Management), NIST 800-53 AC-3 (Access Enforcement), NIST 800-53 CA-7 (Continuous Monitoring), CIS Controls 5.3 (Disable Dormant Accounts), CIS Controls 6.2 (Enforce Authorized Operating System and Applications)

Compensating: Organizations without Azure AD integration: Audit Teams client policy settings (Teams Desktop Client: Settings > Privacy > External Access). Manually document all federated partner tenants permitted for external Teams communication. Establish a manual approval workflow for new federated domains — require security review before enabling. For link scanning: configure Teams to disable preview/rendering of files from external links (Settings > File Sharing). Enforce message retention policy: 90 days minimum. Monitor Teams audit logs (Office 365 Security & Compliance Center > Audit Log Search) for external user sign-in, message forward, and file share events weekly. Create alert for any message containing .exe, .msi, .ps1, .bat, .cmd, .scr, .vbs file extensions from external senders.

Evidence: Export current Teams external access policies from Microsoft Teams admin center (Settings > Org-wide Settings > Guest Access, External Access). Document all federated partner organizations currently permitted. Export Teams audit logs (Microsoft 365 Compliance Center > Audit) for past 90 days filtered on: (1) UserType='Guest' or 'External', (2) Operations containing 'MessageCreate' or 'FileUploaded', (3) RecordType='TeamsSession'. Preserve list of all Teams channels with external member access. Capture screenshots of current Teams client policy settings on sample endpoints.

Step 5 — Assessment: Inventory endpoints for Deno runtime installation and audit AWS S3 bucket policies and CloudTrail logs for unexpected PutObject calls from internal hosts.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 (Detection and Analysis phase: evidence gathering and scoping)

Controls: NIST 800-53 CM-8 (Information System Component Inventory), NIST 800-53 CA-7 (Continuous Monitoring), NIST 800-53 AU-2 (Audit Events), CIS Controls 1.1 (Establish and Maintain Detailed Asset Inventory), CIS Controls 4.6 (Collect Audit Logs)

Compensating: Organizations without configuration management tools: Deploy a PowerShell discovery script to all endpoints via Group Policy (Computer Configuration > Policies > Windows Settings > Scripts > Startup): script searches for deno.exe in %PATH%, C:\Program Files, C:\Program Files (x86), C:\Users, %TEMP%, HKLM\SOFTWARE (Uninstall registry hive) and %APPDATA% installations. Output results to shared network drive by hostname and timestamp. For S3 audit without cost: enable CloudTrail logging to S3 (free tier: 90-day retention in CloudTrail console). Query CloudTrail via AWS CLI locally (aws cloudtrail lookup-events --lookup-attributes AttributeKey=ResourceName,AttributeValue= --max-results 50) filtered for PutObject events from internal source IP ranges (list from internal network documentation). Export to CSV for analysis. Exclude known backup/replication service accounts.

Evidence: Capture file system scan results for deno.exe presence (file path, hash, timestamps, owner). Export Windows Registry HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall and HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall for 'Deno' entries (if installed via installer). Preserve AWS CloudTrail logs (JSON format, minimum 30 days) for S3 bucket showing: userIdentity, eventTime, eventName (PutObject), sourceIPAddress, requestParameters (bucket, key). Document all internal service accounts with S3 access (check IAM role trust relationships and inline policies). Capture VPC Flow Logs showing outbound traffic from internal IPs to S3 API endpoints (s3.amazonaws.com, s3-.amazonaws.com) during suspected exfiltration window.

Step 6 — Communication: Notify SOC, endpoint, and cloud security teams of the behavioral indicators; brief IT help desk staff on ClickFix lure patterns so they can identify and escalate user-reported pop-ups requesting command execution.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.6 (Detection and Analysis: reporting and communication)

Controls: NIST 800-53 IR-6 (Incident Reporting), NIST 800-53 CP-2 (Contingency Planning), CIS Controls 3.3 (Configure Data Access Control Lists), CIS Controls 17.1 (Designate Leadership and Establish Responsibilities)

Compensating: Organizations without formal IR team: Create a standardized incident alert email template including: threat name, IoCs (deno.exe, msiexec.exe anomalies, specific PsExec execution patterns), expected locations, how users will observe it (pop-up type, lure text examples), and required escalation path (email SOC@company.com, do not click, screenshot and report). Distribute to all IT staff, help desk, and power users via authenticated SharePoint/Wiki page with monthly refresh. Train help desk staff (30 min session) on ClickFix pattern recognition: fake Windows Update pop-ups, Microsoft Support phone number scareware, urgent 'Your subscription has expired' messages requesting RunAs or Administrator prompt. Create one-page printable reference card ('If you see this, escalate it') distributed to all help desk personnel. Establish escalation email: escalations@company.com monitored by security team during business hours.

Evidence: Preserve all user-reported pop-up screenshots or browser history showing the lure source domain. Capture browser download history (e.g., C:\Users\\AppData\Local\Microsoft\Windows\INetCache) showing malicious executable downloads. Export browser extension list and recent browser activity (cookies, visited URLs). Preserve network proxy logs or web filter logs showing the initial phishing link access and any subsequent C2 communication. Document user's system state before any cleanup (open processes, running services, scheduled tasks via tasklist /v, Get-ScheduledTask, services.msc).

Step 7 — Long-term: Evaluate EDR telemetry coverage for in-memory JavaScript execution and reflective loading; tune SIEM rules to correlate msiexec.exe network activity, Deno process creation, PsExec service installation, and S3 exfiltration events into a single detection chain mapped to this kill chain.

NIST Phase: Recovery

Reference: NIST 800-61r3 §4.2 (Post-Incident Activities: recommendations for future prevention)

Controls: NIST 800-53 CA-7 (Continuous Monitoring), NIST 800-53 SI-4 (Information System Monitoring), NIST 800-53 IR-4 (Incident Handling), CIS Controls 8.1 (Establish and Maintain Endpoint Detection and Response), CIS Controls 8.8 (Collect Detailed Audit Logs)

Compensating: Organizations without EDR or SIEM: Build manual correlation workflow in spreadsheet or database: create daily scheduled task to export Sysmon Event IDs 1 (Process Creation), 3 (Network Connection), 5 (Process

Termination), and 10 (CreateRemoteThread) to centralized location. Similarly export Windows Event Logs 4688 (Process Creation), 5145 (SMB), 5156 (Firewall Outbound Connection). Write PowerShell script to correlate: IF (msiexec.exe network connection within 5 min of deno.exe creation) AND (service creation event 7045 containing 'psexec' within 10 min) THEN flag for review. Export matches weekly. For S3 correlation: pull CloudTrail daily, filter for PutObject calls from internal IPs during correlation window, cross-reference source IP against endpoint process creation logs. Publish matches to shared alert board. Alternatively: if using free-tier SIEM alternative (e.g., Splunk Trial, Elastic stack), construct equivalent correlation rule using SPL or KQL and schedule as weekly search.

Evidence: Collect baseline EDR/SIEM telemetry for normal msiexec.exe behavior (legitimate MSI installations) for 30 days to establish false-positive threshold. Document all in-memory JavaScript execution events (Deno process spawning child processes, reflective DLL injection attempts — look for CreateRemoteThread events). Preserve historical SIEM/EDR logs for any confirmed incidents or near-misses for rule tuning. Capture EDR product capabilities matrix: which process creation, network, and file events are natively collected; any blind spots or configuration gaps. Export current detection rule set and document coverage gaps for this specific kill chain.

Detection Guidance

Primary detection opportunity is behavioral, the attack chain is consistent and uses identifiable LOLBin sequences before ransomware detonation. Key indicators by stage:

1. Initial Execution: Process creation event where msiexec.exe is the parent and spawns cmd.exe, PowerShell, or network-connected child processes. Windows Security Event ID 4688 or Sysmon Event ID 1 with msiexec.exe as parent process and network activity (Sysmon Event ID 3) shortly after.

2. Deno Loader: Process creation for deno.exe or any JavaScript runtime binary from a non-standard path (e.g., %TEMP%, %APPDATA%, user-writable directories). Sysmon Event ID 1 filtering on Image path containing 'deno'. No legitimate enterprise workload should spawn Deno from these paths.

3. Credential Activity: klist.exe execution in close temporal proximity to msiexec.exe or deno.exe activity. Event ID 4688 for klist.exe spawned by non-standard parent processes.

4. Lateral Movement: PsExec service installation on remote hosts (Windows System Event ID 7045, new service named 'PSEXESVC' or variant). Correlate with originating host's prior Deno or msiexec activity.

5. Exfiltration: Outbound HTTPS connections to s3.amazonaws.com or regional S3 endpoints from hosts that do not normally access S3. In AWS CloudTrail, look for PutObject or CreateMultipartUpload API calls from internal host IPs or roles not associated with backup or data pipeline workloads.

6. DLL Side-Loading: Sysmon Event ID 7 (Image Loaded) for DLLs loaded from user-writable directories by processes that should load system DLLs from System32 only.

Recommended SIEM correlation: Chain events, msiexec.exe network connection OR deno.exe process creation → klist.exe execution → PsExec service install on lateral host → S3 outbound traffic, within a 60-minute window on the same originating host. Any partial match (two or more stages) on a single host should generate a high-priority alert. Sources for query reference: Elastic Security rule for suspicious msiexec execution (Elastic documentation); Microsoft blog on Node.js/Deno abuse patterns (T1 source, April 2025).

Indicators of Compromise

Type	Value	Context	Confidence
PROCESS	`deno.exe`	Deno JavaScript runtime used as in-memory loader for ransomware payload; execution from user-writable directories is high-confidence anomaly	MEDIUM
BEHAVIORAL	`msiexec.exe spawning network-connected child processes`	User-initiated msiexec.exe command used as initial execution vector per T1204.002 and T1218.007; msiexec making outbound connections or spawning cmd.exe/PowerShell is anomalous	MEDIUM
BEHAVIORAL	`klist.exe executed by non-standard parent process`	Credential mapping stage post-initial-access; klist spawned outside normal user session context indicates T1558 activity	MEDIUM
BEHAVIORAL	`PSEXESVC service installation on remote hosts`	PsExec-based lateral movement per T1569.002; Windows Event ID 7045 with service name PSEXESVC or variant	MEDIUM
BEHAVIORAL	`Outbound HTTPS to s3.amazonaws.com from non-baseline hosts`	Data exfiltration to attacker-controlled AWS S3 bucket per T1537; correlate with prior Deno or msiexec activity on same host	MEDIUM
URL	`Compromised legitimate websites delivering ClickFix lures`	No specific domains confirmed in available T3 sources; treat any website prompting users to run msiexec.exe or paste commands into Run/cmd as a ClickFix lure pattern — specific domains require primary threat intel feed validation	LOW

Framework Mappings

MITRE-ATTACK

- **T1204.002** — Malicious File
- **T1071.001** — Web Protocols
- **T1566** — Phishing
- **T1486** — Data Encrypted for Impact
- **T1569.002** — Service Execution
- **T1204.002** — Malicious File
- **T1558** — Steal or Forge Kerberos Tickets
- **T1620** — Reflective Code Loading
- **T1059.007** — JavaScript
- **T1567.002** — Exfiltration to Cloud Storage

- **T1486** — Data Encrypted for Impact
- **T1569.002** — Service Execution
- **T1218.007** — Msiexec
- **T1537** — Transfer Data to Cloud Account
- **T1620** — Reflective Code Loading
- **T1059.007** — JavaScript
- **T1574.002** — DLL Side-Loading

NIST-800-53R5

- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **SI-10** — Information Input Validation
- **SI-7** — Software, Firmware, and Information Integrity
- **IR-4** — Incident Handling
- **SR-2** — Supply Chain Risk Management Plan
- **SI-4** — System Monitoring

OWASP-TOP10-2021

- **A03:2021** — Injection

CIS-V8

- **16.10**
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **15.1** — Establish and Maintain an Inventory of Service Providers
- **8.2** — Collect Audit Logs

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **GV.SC-01** — Cybersecurity supply chain risk management program
- **DE.CM-01** — Networks and network services are monitored

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.5.21** — Managing information security in the ICT supply chain
- **A.5.23** — Information security for use of cloud services

SOC2-TSC

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1204.002	Malicious File	Execution
T1071.001	Web Protocols	Command-And-Control
T1566	Phishing	Initial-Access
T1486	Data Encrypted for Impact	Impact
T1569.002	Service Execution	Execution
T1558	Steal or Forge Kerberos Tickets	Credential-Access
T1620	Reflective Code Loading	Defense-Evasion
T1059.007	JavaScript	Execution
T1567.002	Exfiltration to Cloud Storage	Exfiltration
T1218.007	Msiexec	Defense-Evasion
T1537	Transfer Data to Cloud Account	Exfiltration
T1574.002	Hijack Execution Flow: DLL Side-Loading	

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/03/leaknet-ransomware-uses-clickfix-...	T3
LeakNet Ransomware's Low-Cost High-Scale Infection Strategy	https://hivepro.com/threat-advisory/leaknet-ransomware-low-cost-hig...	T3
Threat actors misuse Node.js to deliver malware and other malicious ...	https://www.microsoft.com/en-us/security/blog/2025/04/15/threat-act...	T1
Suspicious Execution via MSIEXEC | Elastic Security [8.19]	https://www.elastic.co/guide/en/security/8.19/suspicious-execution-...	T3
Defender alert msiexec.exe /V lsass : r/DefenderATP - Reddit	https://www.reddit.com/r/DefenderATP/comments/1jfkwxk/defender_aler...	T3

Generated 2026-03-29 18:35 UTC by TJS Security Command Center