INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-25 06:49 UTC

TGR-STA-1030 Shifts Focus to Americas: State-Aligned Espionage Group Expands Campaign After 37-Country Breach Spree

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0217
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	National telecommunications firms, finance ministries, police agencies, sector-level targeting across 37 countries; no specific vendor products or versions named
Published	2026-04-24T20:30:19+00:00
Discovery Source	Rss:T1 Threatintel

Executive Summary

TGR-STA-1030 (UNC6619), a state-aligned espionage group assessed with high confidence as operating out of Asia, has compromised at least 70 government and critical infrastructure organizations across 37 countries since early 2025 and has now shifted focus to Central and South America as of April 2026. Targeted sectors include telecommunications, law enforcement, and finance ministries. The group deploys a kernel-level eBPF rootkit that evades standard host-based security controls, making detection and eviction significantly harder than typical intrusion scenarios.

Technical Analysis

TGR-STA-1030 (UNC6619) is a state-aligned threat actor conducting long-running espionage operations against government and critical infrastructure targets. TTPs include geopolitically timed reconnaissance (T1595, T1589), spearphishing links and attachments (T1566.001, T1566.002), exploitation of internet-facing systems via n-day vulnerabilities (T1190), and command-and-control over standard application layer protocols (T1071, T1071.001) routed through web services (T1102) and proxies (T1090). Post-compromise activity includes deployment of a custom eBPF-based rootkit (T1014) for kernel-level persistence (T1543, T1547), indicator removal (T1070.001), defense evasion via obfuscation (T1027) and security tool disablement (T1562.001), system enumeration (T1082), data collection and archival (T1560), and use of valid accounts (T1078). The eBPF rootkit operates at the kernel layer, allowing it to intercept and suppress telemetry before it reaches user-space security tools. No specific CVEs are publicly attributed to this campaign. Associated CWEs:

CWE-693 (Protection Mechanism Failure), CWE-116 (Improper Encoding or Escaping of Output), CWE-829 (Inclusion of Functionality from Untrusted Control Sphere). Attribution source: Unit 42, assessed at high confidence based on TTP consistency and infrastructure overlap. Qualitative severity: Critical. Internal priority score: 0.875.

Action Checklist

1. Step 1: Containment. Audit internet-facing assets in telecommunications, finance, and law enforcement environments for signs of unauthorized access. Prioritize systems with external SSH, VPN endpoints, and web-facing management interfaces. Isolate any host showing anomalous kernel-level behavior or unexpected eBPF program loading.
2. Step 2: Detection. Query EDR and SIEM for eBPF program loads from unexpected processes (syscall bpf() calls outside approved tooling), kernel module additions, and suppressed or missing telemetry gaps. Review authentication logs for valid account use at unusual hours (T1078). Check network logs for C2 patterns using standard HTTP/S ports to cloud-hosted or anonymizing infrastructure (T1071.001, T1090, T1102). Cross-reference outbound connections against Unit 42's published infrastructure indicators for TGR-STA-1030.
3. Step 3: Eradication. No vendor patch applies; this is a TTP-based campaign without attributed CVEs. Remove unauthorized eBPF programs identified during detection. Rotate all credentials on affected systems, prioritizing service accounts and privileged accounts. Rebuild compromised hosts from verified clean images rather than attempting in-place remediation of rootkit-compromised systems.
4. Step 4: Recovery. Validate kernel integrity on restored systems before returning to production. Monitor rebuilt hosts for recurrence of eBPF loads, persistence mechanisms (T1543, T1547), and outbound connections matching known TGR-STA-1030 infrastructure patterns. Confirm security tooling is fully operational; this group disables defenses (T1562.001) as a standard TTP.
5. Step 5: Post-Incident. Assess gaps in kernel-level visibility: if your current EDR cannot detect eBPF rootkit activity, evaluate supplemental tooling with eBPF-aware detection capability. Review phishing controls for spearphishing link and attachment variants (T1566.001, T1566.002) that served as initial access vectors. Conduct a threat hunt across the full environment using Unit 42's TTP profile before closing the incident.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to executive leadership, legal counsel, and relevant national CERT/sector ISAC if any confirmed TGR-STA-1030 eBPF rootkit presence is detected on systems handling classified government data, telecommunications subscriber records, or financial ministry data subject to national breach notification requirements, or if dwell time exceeds 30 days indicating potential data exfiltration at scale across the 37-country campaign footprint.

Recovery Notes	Rebuilt hosts must remain under elevated eBPF-specific monitoring — via Falco or Tracee with custom bpf() syscall rules — for a minimum of 90 days post-recovery, as TGR-STA-1030 has demonstrated re-compromise capability against organizations that did not address initial access vectors (T1566 phishing) in parallel with host remediation. Validate that all service account credentials rotated during eradication have not been reused on non-rebuilt adjacent systems, as lateral movement using harvested valid credentials (T1078) is a primary TTP of this group. Confirm log forwarding integrity and auditd rule persistence survive the next scheduled system reboot before closing the recovery phase, as T1562.001 defense disabling may target startup services.
Forensic Artifacts	/sys/fs/bpf/ directory contents — pinned eBPF maps and programs created by TGR-STA-1030's kernel rootkit persist here across process restarts and represent a unique on-disk artifact of this group's specific persistence mechanism | LiME memory dump analyzed with Volatility3 ebpf plugin — the rootkit's in-kernel hook table, suppressed telemetry functions, and active C2 socket structures are only fully visible in a live memory image, not recoverable from disk after the rootkit loads | auditd logs filtered for 'syscall=bpf' (audit key: ebpf_activity) — each invocation of the bpf() syscall during rootkit installation, map pinning, and program re-loading creates an immutable auditd record that survives rootkit attempts to suppress syslog, as auditd writes to a separate kernel ring buffer | Zeek conn.log and ssl.log capturing periodic HTTPS beacon intervals to TGR-STA-1030 C2 infrastructure — consistent beacon jitter patterns to recently-registered domains or cloud provider ASNs (AWS/GCP/Azure) in the C2 timeline corroborate active exfiltration sessions attributed to T1071.001 and T1102 | Spearphishing email artifacts from mail gateway (MTA) logs and quarantine — sender IP headers, weaponized attachment SHA-256 hashes, and embedded link URLs tied to T1566.001/T1566.002 initial access establish the intrusion entry point and campaign start date required for regulatory breach notification scoping

Per-Action IR Details

Step 1: Containment — Audit internet-facing assets in telecommunications, finance, and law enforcement environments for signs of unauthorized access. Prioritize systems with external SSH, VPN endpoints, and web-facing management interfaces. Isolate any host showing anomalous kernel-level behavior or unexpected eBPF program loading.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SI-4 (System Monitoring), NIST AC-17 (Remote Access), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Run 'bpftool prog list' and 'bpftool map list' on each Linux host to enumerate all loaded eBPF programs and maps — any entry outside your approved observability tooling (e.g., Datadog agent, Cilium, Falco) is suspect. For SSH and VPN exposure, run 'ss -tlnp | grep -E "22|443|1194|4443"' and cross-reference against your asset inventory. Use 'last -F' and 'lastb' to surface authentication anomalies at the OS level without EDR. Immediately ACL-restrict management interfaces to jump-host-only access using host firewall rules: 'iptables -A INPUT -p tcp --dport 22 -s <jump-host-ip> -j ACCEPT; iptables -A INPUT -p tcp --dport 22 -j DROP'.

Evidence: Before isolating any host, capture: (1) full output of 'bpftool prog list --json' and 'bpftool map list --json' to document all eBPF programs loaded at time of discovery — TGR-STA-1030's kernel rootkit will appear here if not actively hiding from bpftool itself; (2) /proc/kallsyms snapshot for unexpected symbol additions indicating kernel module injection; (3) 'lsmod' output to identify unauthorized kernel modules used as eBPF loader scaffolding; (4) active network connections via 'ss -antp' and 'netstat -antp' to capture live C2 sessions before network isolation severs them; (5) /var/log/auth.log and /var/log/secure for SSH authentication records showing valid account use from unexpected source IPs consistent with T1078 credential abuse.

Step 2: Detection — Query EDR and SIEM for eBPF program loads from unexpected processes (syscall bpf() calls outside approved tooling), kernel module additions, and suppressed or missing telemetry gaps. Review authentication logs for valid account use at unusual hours (T1078). Check network logs for C2 patterns using standard HTTP/S ports to cloud-hosted or anonymizing infrastructure (T1071.001, T1090, T1102). Cross-reference outbound connections against Unit 42's published infrastructure indicators for TGR-STA-1030.

NIST Phase: Detection Analysis

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

Controls: NIST SI-4 (System Monitoring), NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Deploy Falco (open-source, CNCF) with the default ruleset plus a custom rule targeting the bpf() syscall: 'condition: syscall.type = bpf and proc.name != "" — this fires on any process invoking BPF outside your allowlist. For telemetry gap detection (TGR-STA-1030's rootkit suppresses host agent output), compare expected log volume baselines in /var/log/syslog against actual output using a simple cron-driven line-count script; a sudden drop in syslog rate on a normally verbose telecom gateway is itself an IOC. For C2 detection without SIEM, run Zeek (formerly Bro) on a network tap or SPAN port and apply the ET Open ruleset filtering for HTTP beaconing intervals to cloud providers (AWS/GCP/Azure egress ranges). Query WHOIS and BGP data for outbound connections to recently-registered domains (less than 90 days) using 'whois' and the abuse.ch URLhaus feed parsed with a simple bash loop.

Evidence: Capture before completing detection sweep: (1) auditd logs filtered for syscall=bpf (audit rule: '-a always,exit -F arch=b64 -S bpf -k ebpf_activity') — the TGR-STA-1030 rootkit loader will generate bpf() syscalls during installation and periodic re-pinning; (2) /sys/fs/bpf/ directory listing to identify pinned eBPF maps that persist across process restarts, a persistence mechanism specific to this group's rootkit; (3) SIEM or raw syslog telemetry gap analysis — identify hosts where log forwarding went silent for any period, as the rootkit suppresses agent telemetry (T1562.001); (4) NetFlow or PCAP captures showing periodic HTTPS beacon intervals (consistent jitter patterns) to cloud-hosted infrastructure, particularly to hosting providers in jurisdictions consistent with Asia-origin attribution; (5) /var/log/wtmp and /run/utmp binary records parsed via 'utmpdump' to reconstruct login sessions that may have been partially wiped by the rootkit.

Step 3: Eradication — No vendor patch applies; this is a TTP-based campaign without attributed CVEs. Remove unauthorized eBPF programs identified during detection. Rotate all credentials on affected systems, prioritizing service accounts and privileged accounts. Rebuild compromised hosts from verified clean images rather than attempting in-place remediation of rootkit-compromised systems.

NIST Phase: Eradication

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

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST IA-5 (Authenticator Management), CIS 5.2 (Use Unique Passwords), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: Because TGR-STA-1030 operates a kernel-level eBPF rootkit, in-place removal is forensically unreliable — the rootkit can re-pin eBPF programs from a userland persistence stub even after apparent removal. For teams without automated rebuild pipelines: provision a clean VM from a known-good image hash (validate with 'sha256sum'), restore only configuration and data (not binaries) from pre-compromise backups confirmed via 'rpm -Va' or 'debsums -c' integrity checks. Credential rotation must occur from a clean, out-of-band management host, not from the compromised environment — TGR-STA-1030's use of T1078 (valid accounts) means credentials entered on compromised hosts may be re-captured. Use 'chage -d 0 ' on Linux to force immediate password reset for all service accounts on rebuilt hosts, and audit /etc/sudoers and /etc/sudoers.d/ for unauthorized privilege escalation entries the group may have inserted.

Evidence: Before wiping compromised hosts, complete forensic imaging: (1) full disk image via 'dc3dd if=/dev/sda | tee >(sha256sum > image.sha256) > host_image.raw' for chain-of-custody preservation; (2) memory acquisition using LiME (Linux Memory Extractor) — the TGR-STA-1030 eBPF rootkit's in-memory structures, hooked functions, and active C2 connection state will only be visible in a memory dump, not on disk; (3) extract and preserve all pinned eBPF objects from /sys/fs/bpf/ before host wipe, as these are forensic artifacts unique to this group's persistence mechanism; (4) dump /proc//maps and /proc//fd for any suspicious process identified during detection to capture memory-mapped rootkit components; (5) collect /etc/passwd, /etc/shadow, /etc/sudoers, and crontab files (-l for all users) to document any backdoor accounts or scheduled persistence tasks TGR-STA-1030 established alongside the rootkit.

Step 4: Recovery — Validate kernel integrity on restored systems before returning to production. Monitor rebuilt hosts for recurrence of eBPF loads, persistence mechanisms (T1543, T1547), and outbound connections matching known TGR-STA-1030 infrastructure patterns. Confirm security tooling is fully operational — this group disables defenses (T1562.001) as a standard TTP.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST SI-6 (Security and Privacy Function Verification), NIST SI-7 (Software, Firmware, and Information Integrity), NIST SI-4 (System Monitoring), NIST IR-4 (Incident Handling), NIST AU-9 (Protection of Audit Information), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 8.2 (Collect Audit Logs)

Compensating: For kernel integrity validation on rebuilt Linux hosts, run 'rpm -Va' (RHEL/CentOS) or 'debsums -c' (Debian/Ubuntu) against all installed packages to detect any binary tampering before production return. Validate that the running kernel matches the expected version and hash: 'sha256sum /boot/vmlinuz-$(uname -r)' compared against the distribution's published checksum. Deploy Falco immediately on rebuilt hosts with a custom rule alerting on any bpf() syscall from processes outside a strict allowlist — this provides the eBPF-aware detection capability the group specifically targets to disable. For tooling health verification (counter T1562.001), use a simple watchdog cron job every 5 minutes that checks Falco, auditd, and your log forwarder process health: 'systemctl is-active falco auditd rsyslog || alert_oncall.sh'.

Evidence: Before returning any rebuilt host to production, collect baseline forensic markers for future comparison: (1) 'bpftool prog list --json' output on the clean host establishing the approved eBPF program baseline — any future deviation from this snapshot is an IOC; (2) 'sha256sum /boot/vmlinuz-$(uname -r) /boot/initrd.img-$(uname -r)' for kernel and initrd integrity anchors; (3) auditd rule validation output ('auditctl -l') confirming bpf() syscall monitoring is active and has not been suppressed; (4) initial 24-hour Zeek/Suricata connection log baseline for each rebuilt host documenting expected outbound destinations — deviations toward TGR-STA-1030's known cloud-hosted C2 infrastructure will stand out against this baseline; (5) 'systemctl list-units --type=service --state=enabled' and 'crontab -l' for all users to establish clean persistence baseline against which T1543 (Create or Modify System Process) and T1547 (Boot or Logon Autostart Execution) recurrence can be measured.

Step 5: Post-Incident — Assess gaps in kernel-level visibility: if your current EDR cannot detect eBPF rootkit activity, evaluate supplemental tooling with eBPF-aware detection capability. Review phishing controls for spearphishing link and attachment variants (T1566.001, T1566.002) that served as initial access vectors. Conduct a threat hunt across the full environment using Unit 42's TTP profile before closing the incident.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-3 (Malicious Code Protection), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST RA-3 (Risk Assessment), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For the kernel-visibility gap assessment, test your current EDR by loading a benign eBPF program using the bcc tools package ('apt install bpfcc-tools; opensnoop-bpfcc') and verify whether the EDR fires an alert — if it does not, you have a confirmed blind spot exploitable by TGR-STA-1030. As a free supplement, deploy Tracee (Aqua Security, open-source) which uses eBPF itself to detect malicious eBPF usage, providing detection-in-kind. For phishing control review, test email gateway filtering against T1566.001/T1566.002 using GoPhish (open-source) targeting your own organization with spearphishing templates mimicking the diplomatic/government lure themes

associated with TGR-STA-1030's Asia-origin campaigns. For the threat hunt, implement published MITRE ATT&CK Sigma rules for T1078, T1071.001, T1090, and T1562.001 against your log archive using 'sigma convert' to translate to your native query language (Elastic, Splunk, or raw grep), covering the campaign's active period from early 2025.

Evidence: Post-incident documentation must include: (1) complete timeline of bpf() syscall events from auditd logs spanning the full suspected compromise window (early 2025 onward for this campaign), correlated against authentication events from /var/log/auth.log to establish TGR-STA-1030 dwell time; (2) all spearphishing email artifacts preserved from mail gateway logs — headers, sender IPs, link URLs, attachment hashes — tied to the T1566.001/T1566.002 initial access phase; (3) network flow records (NetFlow/IPFIX or Zeek logs) documenting the full C2 communication timeline to TGR-STA-1030 infrastructure, including first-seen and last-seen timestamps for regulatory breach notification scoping; (4) inventory of all accounts accessed or created by the threat actor (from /etc/passwd history, SIEM auth logs, and VPN access logs) to support breach notification assessment for law enforcement and finance ministry regulatory obligations; (5) EDR telemetry gap report showing time ranges where host agent data was suppressed by T1562.001 — this gap period represents unconfirmed attacker activity and must be disclosed in the post-incident report as unverifiable dwell time.

Detection Guidance

Priority detection focus is the eBPF rootkit (T1014). Look for: (1) unexpected invocations of the bpf() syscall from processes outside approved observability or networking tooling; (2) eBPF programs of type BPF_PROG_TYPE_KPROBE or BPF_PROG_TYPE_TRACEPOINT loaded by non-standard processes; (3) gaps or suppressions in expected telemetry streams that suggest kernel-level interception. For initial access, hunt spearphishing delivery (T1566.001, T1566.002): review email gateway logs for links to newly registered domains and attachments with scripting content (T1059). For persistence, check for new or modified systemd services (T1543.002) and run key/startup entry changes (T1547.001). For C2, flag outbound connections using standard HTTP/S to cloud platforms and proxy chains (T1071.001, T1090, T1102) with irregular beacon timing or large outbound data volumes (T1560). For defense evasion, alert on security tool process terminations or service stops not initiated by authorized change management (T1562.001). MITRE ATT&CK techniques: T1014, T1071, T1071.001, T1078, T1090, T1102, T1543, T1547, T1562.001, T1566.001, T1566.002, T1560. No public IOC list is embedded in this record; refer to Unit 42's published reporting at https://unit42.paloaltonetworks.com/shadow-campaigns-uncovering-global-espionage/ for infrastructure indicators (URL is source-provided; recommend human validation before operationalizing).

Indicators of Compromise

Type	Value	Context	Confidence
OTHER	`eBPF rootkit — specific hashes not publicly released in available source data`	Kernel-level rootkit deployed by TGR-STA-1030 for persistent access; evasion of user-space EDR tooling is a primary design goal	HIGH
OTHER	`Infrastructure indicators — refer to Unit 42 published reporting`	Specific IPs, domains, and file hashes are documented in Unit 42 campaign reporting; not reproduced here to avoid transcription error	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1071** — Application Layer Protocol
- **T1078** — Valid Accounts
- **T1543** — Create or Modify System Process
- **T1566.002** — Spearphishing Link
- **T1070.001** — Clear Windows Event Logs
- **T1566** — Phishing
- **T1059** — Command and Scripting Interpreter
- **T1027** — Obfuscated Files or Information
- **T1102** — Web Service
- **T1082** — System Information Discovery
- **T1583** — Acquire Infrastructure
- **T1547** — Boot or Logon Autostart Execution
- **T1562.001** — Disable or Modify Tools
- **T1589** — Gather Victim Identity Information
- **T1190** — Exploit Public-Facing Application
- **T1560** — Archive Collected Data
- **T1595** — Active Scanning
- **T1071.001** — Web Protocols
- **T1014** — Rootkit
- **T1105** — Ingress Tool Transfer
- **T1090** — Proxy
- **T1497** — Virtualization/Sandbox Evasion
- **T1566.001** — Spearphishing Attachment

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AT-2** — Literacy Training and Awareness
- **SI-3** — Malicious Code Protection
- **SI-8** — Spam Protection
- **CM-7** — Least Functionality
- **SI-7** — Software, Firmware, and Information Integrity

- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information

CIS-V8

- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **8.2** — Collect Audit Logs

HIPAA-SECURITY

- **164.308(a)(5)(i)** — Security Awareness and Training

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1071	Application Layer Protocol	Command-And-Control
T1078	Valid Accounts	Defense-Evasion
T1543	Create or Modify System Process	Persistence
T1566.002	Spearphishing Link	Initial-Access
T1070.001	Clear Windows Event Logs	Defense-Evasion
T1566	Phishing	Initial-Access
T1059	Command and Scripting Interpreter	Execution
T1027	Obfuscated Files or Information	Defense-Evasion
T1102	Web Service	Command-And-Control
T1082	System Information Discovery	Discovery
T1583	Acquire Infrastructure	Resource-Development
T1547	Boot or Logon Autostart Execution	Persistence
T1562.001	Disable or Modify Tools	Defense-Evasion
T1589	Gather Victim Identity Information	Reconnaissance

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access
T1560	Archive Collected Data	Collection
T1595	Active Scanning	Reconnaissance
T1071.001	Web Protocols	Command-And-Control
T1014	Rootkit	Defense-Evasion
T1105	Ingress Tool Transfer	Command-And-Control
T1090	Proxy	Command-And-Control
T1497	Virtualization/Sandbox Evasion	Defense-Evasion
T1566.001	Spearphishing Attachment	Initial-Access

Sources

Source	URL	Tier
Unit 42	https://unit42.paloaltonetworks.com/new-activity-central-south-amer...	T3
	https://industrialcyber.co/ransomware/unit-42-identifies-tgr-sta-10...	T3
	https://unit42.paloaltonetworks.com/shadow-campaigns-uncovering-glo...	T3
	https://www.cybersecuritydive.com/news/asian-governments-espionage-...	T3
Surveillance vendors caught abusing access to telcos to track ...	https://techcrunch.com/2026/04/23/surveillance-vendors-caught-abusi...	T2

Generated 2026-04-25 06:49 UTC by TJS Security Command Center