INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-30 06:54 UTC

Mustang Panda Deploys SHARDLOADER/MINIRECON/ZOHOMURK Against Indian Government and Energy Sectors via Zoho WorkDrive C2

THREAT CAMPAIGN | **HIGH** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0600
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	9.5
Affected Products	Zoho WorkDrive (abused as C2 dead-drop via legitimate cloud API); Solid PDF Creator (signed binary abused for DLL sideloading); Citrix Receiver (signed binary abused for DLL sideloading); Indian government administrative systems and hydropower infrastructure
Published	2026-06-29T11:03:40
Discovery Source	Rss

Executive Summary

China-aligned threat actor Mustang Panda is actively targeting Indian government administrative networks and hydropower infrastructure using three newly identified malware tools, according to reporting by The Hacker News citing Acronis Threat Research Unit. The campaign abuses legitimate cloud services, specifically Zoho WorkDrive's API, as a command-and-control channel, allowing attacker traffic to blend with normal enterprise cloud activity and evade perimeter detection. Organizations supporting or partnering with Indian government or energy sectors, particularly those using Zoho WorkDrive, Solid PDF Creator, or Citrix Receiver, face elevated risk of undetected, long-duration espionage operations.

Technical Analysis

According to Acronis Threat Research Unit as reported by The Hacker News, Mustang Panda has deployed three new tools in this campaign: SHARDLOADER (a malware loader), MINIRECON (a reconnaissance implant), and ZOHOMURK (a backdoor). ZOHOMURK communicates via the legitimate Zoho WorkDrive cloud API as a dead-drop command-and-control channel, a living-off-trusted-services (LOTS) technique mapped to MITRE T1102.001 (Web Service: Dead Drop Resolver). Initial access is assessed via spearphishing (T1566.001). The actor abuses signed legitimate binaries, Solid PDF Creator and Citrix Receiver, to sideload

malicious DLLs (T1574.002), evading endpoint detection that relies on binary signing validation. Persistence mechanisms include registry run key modification (T1547.001) and scheduled tasks (T1053.005). Obfuscation (T1027) and exfiltration over C2 channel (T1041) are also observed. Relevant CWEs: CWE-494 (Download of Code Without Integrity Check), CWE-506 (Embedded Malicious Code), CWE-798 (Use of Hard-coded Credentials). Attribution confidence is medium, tooling names and technical specifics derive from a single T2 source (The Hacker News); independent corroboration from CISA KEV, NVD, or a second named research organization has not been confirmed in the provided data. No CVE IDs are associated with this campaign. No vendor patches are applicable; the abuse vector exploits legitimate service APIs and signed binaries, not software vulnerabilities.

Action Checklist

1. Step 1: Containment, Identify all endpoints where Solid PDF Creator or Citrix Receiver are installed and assess whether DLL sideloading conditions exist (writable directories adjacent to signed executables). Restrict outbound API connections to Zoho WorkDrive to known, authorized business accounts via firewall policy or cloud access security broker (CASB) controls; flag or block unauthenticated or anomalous Zoho WorkDrive API calls from endpoints that have no documented business need. Prioritize systems used by senior administrative staff. [NIST AC-4, Information Flow Enforcement]
2. Step 2: Detection, Search endpoint detection logs for DLL loads originating from Solid PDF Creator (solidpdfcreator.exe) or Citrix Receiver (receiver.exe) where the loaded DLL resides in the same directory as the executable but is not part of the application's known-good manifest. Hunt for outbound HTTPS connections to workdrive.zoho.com or api.zoho.com from non-standard processes or at unusual hours. Review scheduled task creation events (Windows Event ID 4698) and registry run key modifications (HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run) for entries created by unexpected parent processes. Query for MINIRECON-style host enumeration: rapid sequential queries for system info, network adapters, and running processes within short time windows. [NIST AU-6, Audit Record Review, Analysis, and Reporting; NIST SI-4, System Monitoring and Information System Monitoring; CIS 8.2, Collect Audit Logs]
3. Step 3: Eradication, Remove unauthorized DLL files placed adjacent to Solid PDF Creator and Citrix Receiver binaries. Revoke and rotate any credentials or API tokens stored on compromised endpoints (D3-CRO, Credential Rotation). Disable or uninstall Solid PDF Creator and Citrix Receiver on systems where they serve no current business function (CIS 2.3, Address Unauthorized Software). Audit Zoho WorkDrive account permissions and revoke any API tokens not tied to documented service accounts (NIST AC-2, Account Management; D3-UAP, User Account Permissions).
4. Step 4: Recovery, After eradication, validate endpoint integrity by comparing current DLL manifests against known-good baselines for Solid PDF Creator and Citrix Receiver. Re-enable business-required Zoho WorkDrive access only after API token audit is complete. Monitor previously affected endpoints for 30 days post-remediation for recurrence of sideloading indicators or anomalous cloud API calls. Confirm scheduled tasks and run keys are clean. [NIST AU-6, Audit Record Review, Analysis, and Reporting; D3-SFA, System File Analysis]
5. Step 5: Post-Incident, This campaign exposes two control gaps: (1) insufficient application allowlisting that permits unsigned or unvalidated DLLs to load alongside signed binaries, and (2) absence of CASB or API-level inspection for cloud service misuse as C2. Implement DLL load validation controls and review the enterprise policy for third-party signed binary deployments. Establish monitoring rules specific to LOTS C2 patterns, outbound cloud API calls from unexpected processes. [NIST AC-6, Least Privilege; CIS 2.1,

Establish and Maintain a Software Inventory; CIS 4.4, Implement and Manage a Firewall on Servers; D3-CH, Credential Hardening]

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to CISO, legal counsel, and national CERT (CERT-In for Indian government entities) if MINIRECON enumeration output or ZOHOMURK C2 beaconing is confirmed on any system processing classified government data or operational technology networks connected to hydropower infrastructure, as this meets the threshold for a critical infrastructure incident with potential regulatory notification obligations.
Recovery Notes	Restore Zoho WorkDrive access only to endpoints with confirmed clean DLL manifests and only for accounts with MFA enforced and API tokens freshly issued post-incident. Monitor all previously affected endpoints with Sysmon Event ID 7 filtering on the Solid PDF Creator and Citrix Receiver process names for a minimum of 30 days, as Mustang Panda campaigns have historically demonstrated persistence and re-entry via alternate sideloading candidates when initial access is disrupted. Validate that no ZOHOMURK-associated WorkDrive folders remain accessible by auditing active OAuth grants in the Zoho Admin Console and confirming no unauthorized shared folder access persists.
Forensic Artifacts	Sideloaded DLL files in the Solid PDF Creator install directory (default: C:\Program Files\Solid Documents\Solid PDF Creator\) or Citrix Receiver install directory — PE header analysis will reveal absence of legitimate vendor signature and likely recent creation timestamps coinciding with initial compromise. | Windows Sysmon Event ID 7 (ImageLoaded) records showing solidpdfcreator.exe or receiver.exe loading a DLL from their own application directory that is unsigned or signed by an unexpected certificate authority — the core forensic indicator of the SHARDLOADER sideloading mechanism. | HTTPS proxy or firewall logs showing periodic, low-volume, regularly spaced requests from a non-browser process to workdrive.zoho.com or api.zoho.com — SHARDLOADER's dead-drop polling pattern will be distinguishable from user-initiated Zoho traffic by process name, timing regularity, and absence of interactive session cookies. | Windows Security Event Log entries for Event ID 4698 (Scheduled Task Created) with task XML bodies referencing unexpected executables or encoded command-line arguments, and registry keys under HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run created by a process other than a legitimate installer — artifacts consistent with ZOHOMURK persistence mechanisms. | Volatile memory image from compromised endpoints containing in-memory MINIRECON artifacts: unpacked shellcode or reflectively loaded PE segments, enumeration API call sequences (GetAdaptersInfo, CreateToolhelp32Snapshot, GetSystemInfo), and any decrypted C2 configuration including the specific Zoho WorkDrive folder path used as the dead-drop channel.

Per-Action IR Details

Step 1: Containment — Identify all endpoints where Solid PDF Creator or Citrix Receiver are installed and assess whether DLL sideloading conditions exist (writable directories adjacent to signed executables). Restrict outbound API connections to Zoho WorkDrive to known, authorized business accounts via firewall policy or cloud access security broker (CASB) controls; flag or block unauthenticated or anomalous Zoho WorkDrive API calls from endpoints that have no documented business need. Prioritize systems used by senior administrative staff. [NIST AC-4 — Information Flow Enforcement]

NIST Phase: Containment

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

Controls: NIST AC-4 (Information Flow Enforcement), NIST AC-20 (Use Of External Systems), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Use PowerShell to enumerate directories adjacent to solidpdfcreator.exe and receiver.exe for writable permissions: `Get-Acl 'C:\Program Files\Solid Documents\Solid PDF Creator' | Format-List`. Block outbound HTTPS to workdrive.zoho.com and api.zoho.com at the host firewall using `netsh advfirewall firewall add rule name='Block Zoho WorkDrive' protocol=TCP dir=out remoteport=443 remoteip=workdrive.zoho.com action=block` on non-business endpoints. Where CASB is unavailable, apply DNS sinkholing via hosts file or internal DNS for Zoho WorkDrive domains on all endpoints lacking a documented business need.

Evidence: Before restricting Zoho WorkDrive egress or modifying firewall rules, capture: (1) active outbound TCP connection table via `Get-NetTCPConnection | Where-Object {$_.RemoteAddress -match 'zoho'}` to document live C2 sessions; (2) full RAM image using Magnet RAM Capture or WinPmem to preserve SHARDLOADER loader artifacts and any in-memory MINIRECON payloads that have not been written to disk; (3) current DNS cache via `ipconfig /displaydns` to record resolution of workdrive.zoho.com and api.zoho.com; (4) directory listing with timestamps of all DLLs in Solid PDF Creator and Citrix Receiver install directories prior to any file remediation.

Step 2: Detection — Search endpoint detection logs for DLL loads originating from Solid PDF Creator (solidpdfcreator.exe) or Citrix Receiver (receiver.exe) where the loaded DLL resides in the same directory as the executable but is not part of the application's known-good manifest. Hunt for outbound HTTPS connections to workdrive.zoho.com or api.zoho.com from non-standard processes or at unusual hours. Review scheduled task creation events (Windows Event ID 4698) and registry run key modifications (HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run) for entries created by unexpected parent processes. Query for MINIRECON-style host enumeration: rapid sequential queries for system info, network adapters, and running processes within short time windows. [NIST AU-6 — Audit Record Review, Analysis, and Reporting; NIST SI-4 — no mapped control from provided KB; 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-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with SwiftOnSecurity config; Event ID 7 (ImageLoaded) will record DLL loads by solidpdfcreator.exe and receiver.exe — filter for DLLs in the application directory that are not Microsoft-signed. Use a Sigma rule matching Sysmon Event ID 7 where `Image` ends in `solidpdfcreator.exe` OR `receiver.exe` AND `ImageLoaded` path equals the executable's own directory AND `Signed` is false or signer is not the expected vendor. For network hunting without SIEM, run `netstat -ano` and cross-reference PIDs against `tasklist /v` to identify non-browser processes connecting to Zoho domains. Parse Windows Event ID 4698 from the Security log with `wevtutil qe Security /q:"*[System[EventID=4698]]" /f:text` to surface ZOHOMURK-associated persistence tasks.

Evidence: This step is read-only analysis and does not alter live state; however, before any subsequent containment or process termination, preserve: (1) Sysmon Event ID 7 logs showing DLL load chain from solidpdfcreator.exe or receiver.exe; (2) Windows Security Event Log entries for Event ID 4698 (Scheduled Task Created) with task XML bodies, noting parent process and command-line; (3) registry export of HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run and HKCU equivalent at time of discovery; (4) HTTPS proxy or firewall logs showing connection timing, byte counts, and frequency of calls to workdrive.zoho.com — SHARDLOADER's dead-drop polling will produce periodic, low-volume, regularly spaced GET/POST requests to a shared WorkDrive folder, distinguishable from normal user-driven traffic.

Step 3: Eradication — Remove unauthorized DLL files placed adjacent to Solid PDF Creator and Citrix Receiver binaries. Revoke and rotate any credentials or API tokens stored on compromised endpoints (D3-CRO — Credential Rotation). Disable or uninstall Solid PDF Creator and Citrix Receiver on systems where they serve no current business function (CIS 2.3 — Address Unauthorized Software). Audit Zoho WorkDrive

account permissions and revoke any API tokens not tied to documented service accounts (NIST AC-2 — Account Management; D3-UAP — User Account Permissions).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), CIS 2.3 (Address Unauthorized Software), CIS 6.2 (Establish an Access Revoking Process)

Compensating: After forensic capture, delete sideloaded DLLs identified during Step 2 and verify removal with `Get-FileHash` against known-good hashes published in Acronis TRU reporting. Uninstall Solid PDF Creator and Citrix Receiver on non-business systems via `wmic product where name='Solid PDF Creator' call uninstall`. Revoke Zoho WorkDrive API tokens via the Zoho Admin Console under Security → OAuth Applications; document each revoked token with timestamp. Rotate Windows credentials on affected hosts using `net user ` and force GPO-driven password reset for domain accounts accessed from compromised endpoints.

Evidence: CRITICAL — order of volatility must be satisfied before any eradication action. Before removing DLL files, rotating credentials, or uninstalling applications: (1) acquire a full disk image or at minimum a targeted forensic copy of the Solid PDF Creator and Citrix Receiver install directories including all DLLs, their metadata, and PE headers for malware triage; (2) export the complete contents of HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, scheduled task XML definitions, and any WMI subscriptions (via `Get-WMIObject -Namespace root\subscription -Class __EventFilter`); (3) capture process memory of any running solidpdfcreator.exe or receiver.exe instances before termination to preserve in-memory SHARDLOADER or MINIRECON artifacts; (4) export Zoho WorkDrive API access logs from the admin console before token revocation, as revocation may clear session audit trails.

Step 4: Recovery — After eradication, validate endpoint integrity by comparing current DLL manifests against known-good baselines for Solid PDF Creator and Citrix Receiver. Re-enable business-required Zoho WorkDrive access only after API token audit is complete. Monitor previously affected endpoints for 30 days post-remediation for recurrence of sideloading indicators or anomalous cloud API calls. Confirm scheduled tasks and run keys are clean. [NIST AU-6 — Audit Record Review, Analysis, and Reporting; D3-SFA — System File Analysis]

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-11 (Audit Record Retention), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: Generate SHA-256 hashes of all DLLs in the reinstalled Solid PDF Creator and Citrix Receiver directories using `Get-FileHash -Algorithm SHA256 -Path 'C:\Program Files\...' -Recurse | Export-Csv dll_baseline.csv` and compare against vendor-published manifests or a clean reference installation. For Zoho WorkDrive access re-enablement, restrict to named service accounts with MFA enforced via the Zoho Admin Console before unblocking egress firewall rules. Schedule daily Sysmon Event ID 7 log review for 30 days using a Task Scheduler job that exports and diffs new DLL loads against the validated baseline CSV, alerting on any addition to the Solid PDF Creator or Citrix Receiver directories.

Evidence: Recovery phase is lower-volatility but still requires validation artifacts: (1) re-run `Get-NetTCPConnection` filtered for Zoho destinations daily for the first week to confirm no re-establishment of SHARDLOADER C2 sessions; (2) export and diff HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run and scheduled task list against the clean post-eradication state at 7-day intervals; (3) retain all Sysmon logs from the affected endpoints for a minimum of 90 days per NIST AU-11 to support post-incident analysis or potential regulatory review given the government and critical infrastructure targeting context of this campaign.

Step 5: Post-Incident — This campaign exposes two control gaps: (1) insufficient application allowlisting that permits unsigned or unvalidated DLLs to load alongside signed binaries, and (2) absence of CASB or API-level inspection for cloud service misuse as C2. Implement DLL load validation controls and review the enterprise policy for third-party signed binary deployments. Establish monitoring rules specific to LOTS C2 patterns — outbound cloud API calls from unexpected processes. [NIST AC-6 — Least Privilege; CIS 2.1 —

Establish and Maintain a Software Inventory; CIS 4.4 — Implement and Manage a Firewall on Servers; D3-CH — Credential Hardening]

NIST Phase: Post Incident

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

Controls: NIST AC-6 (Least Privilege), NIST AU-2 (Event Logging), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Implement Windows Defender Application Control (WDAC) or AppLocker policies that enforce DLL load restrictions for Solid PDF Creator and Citrix Receiver install directories, blocking unsigned or non-vendor-signed DLLs at the OS level without requiring commercial EDR. Develop and publish Sigma rules for community SIEM platforms targeting: (1) ImageLoaded events from known sideloading-abused binaries (solidpdfcreator.exe, receiver.exe) where the DLL is not in a system32 or vendor-verified path; (2) outbound HTTPS connections to workdrive.zoho.com from any process other than a browser or documented Zoho client. Submit IOCs from this incident (DLL hashes, WorkDrive folder paths used as dead-drops, MINIRECON process enumeration patterns) to MISP or a shared threat intel platform to benefit peer organizations in the Indian government and energy sectors targeted by this Mustang Panda campaign.

Evidence: Post-incident documentation must include: (1) a lessons-learned report capturing the specific DLL sideloading vector (named binary, DLL filename, and directory path) to anchor future detection rules; (2) a timeline reconstruction of Mustang Panda's kill chain — from initial sideloading of SHARDLOADER through MINIRECON enumeration to ZOHOMURK C2 establishment — derived from correlated Sysmon, Windows Security, and proxy logs; (3) documentation of the Zoho WorkDrive folder(s) used as dead-drop C2 channels, including any file naming conventions or polling intervals observed, to support threat intelligence sharing and future LOTS C2 detection tuning.

Detection Guidance

Detection for this campaign requires behavioral and cloud telemetry analysis, not signature-based blocking. Key indicators, per Acronis Threat Research Unit as reported by The Hacker News: (1) DLL Sideloading, Alert on DLL image load events where the loading process is solidpdfcreator.exe or receiver.exe (Citrix) and the DLL path matches the executable's working directory but the DLL is not in a known-good hash inventory for that application version. Sysmon Event ID 7 (ImageLoaded) with filtering on these parent processes is the recommended log source. (2) ZOHOMURK C2, Hunt for HTTPS POST or GET requests to workdrive.zoho.com or *.zoho.com originating from non-browser, non-Zoho-client processes. Establish a baseline of legitimate Zoho API consumers in your environment; flag deviations. (3) MINIRECON Reconnaissance, Correlate rapid sequential execution of system enumeration commands (systeminfo, ipconfig /all, tasklist, net user) within a 60-second window from a single process that is not an authorized IT management tool. (4) Persistence, Windows Event ID 4698 (scheduled task created) and registry modification events on HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run by processes that are not software installers. (5) Spearphishing Initial Access, Review email gateway logs for messages delivering documents targeting Indian government or energy sector themes; inspect attached documents for embedded macros or links to staged loaders. Note: No specific file hashes, IP addresses, or domain IOCs were confirmed in the provided source material. IOC data should be requested directly from Acronis Threat Research Unit or CERT-In. [NIST AU-6; CIS 8.2; D3-SFA, System File Analysis; D3-LAM, Local Account Monitoring]

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`workdrive.zoho.com (abused)`	Zoho WorkDrive API used as ZOHOMURK C2 dead-drop channel; legitimate domain abused — block or monitor by process, not by domain alone	MEDIUM
DOMAIN	`api.zoho.com (abused)`	Zoho API endpoint potentially used for C2 communication by ZOHOMURK backdoor	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1587.001** — Malware
- **T1547.001** — Registry Run Keys / Startup Folder
- **T1574.002** — DLL Side-Loading
- **T1071.001** — Web Protocols
- **T1059** — Command and Scripting Interpreter
- **T1053.005** — Scheduled Task
- **T1102.001** — Dead Drop Resolver
- **T1027** — Obfuscated Files or Information
- **T1041** — Exfiltration Over C2 Channel
- **T1566.001** — Spearphishing Attachment
- **T1036.001** — Invalid Code Signature
- **T1583.003** — Virtual Private Server
- **T1003** — OS Credential Dumping
- **T1583.006** — Web Services

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
- **AT-2** — Literacy Training and Awareness
- **SI-8** — Spam Protection
- **AC-6** — Least Privilege
- **IA-5** — Authenticator Management
- **CM-3** — Configuration Change Control

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **16.10** — Apply Secure Design Principles in Application Architectures
- **8.2** — Collect Audit Logs

ISO-27001-2022

- **A.8.28** — Secure coding
- **A.5.23** — Information security for use of cloud services

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1587.001	Malware	Resource-Development
T1547.001	Registry Run Keys / Startup Folder	Persistence
T1574.002	DLL Side-Loading	Persistence
T1071.001	Web Protocols	Command-And-Control
T1059	Command and Scripting Interpreter	Execution
T1053.005	Scheduled Task	Execution
T1102.001	Dead Drop Resolver	Command-And-Control
T1027	Obfuscated Files or Information	Defense-Evasion
T1041	Exfiltration Over C2 Channel	Exfiltration
T1566.001	Spearphishing Attachment	Initial-Access
T1036.001	Invalid Code Signature	Defense-Evasion
T1583.003	Virtual Private Server	Resource-Development
T1003	OS Credential Dumping	Credential-Access
T1583.006	Web Services	Resource-Development

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/06/mustang-panda-uses-zoho-workdrive.. .	T2
DLL Sideloading Attacks: Signed Malware Risks - Ontinue	https://www.ontinue.com/resource/blog-signed-sideloaded-compromised/	T3
PDFSider Malware: Abuse of DLL Side-Loading for Stealthy ...	https://nucleon-security.com/en/blogs/PDFSider-DLL-Side-Loading-Nuc...	T3
How Attackers Masquerade and Abuse Digital Signatures in DLL ...	https://community.fortinet.com/blogs-103/how-attackers-masquerade-a...	T1
PDFSIDER Malware - Exploitation of DLL Side-Loading for AV and ...	https://www.resecurity.com/blog/article/pdfsider-malware-exploitati...	T3

Generated 2026-06-30 06:54 UTC by TJS Security Command Center