INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-23 06:38 UTC

Kyber Ransomware Introduces Post-Quantum Key Encapsulation Targeting Windows and VMware ESXi, U.S. Defense Contractor Confirmed Victim

THREAT CAMPAIGN | CRITICAL | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0205
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Windows file servers, VMware ESXi, Microsoft Hyper-V, Microsoft SQL Server, Microsoft Exchange
Published	2026-04-22T14:52:29
Discovery Source	Rss

Executive Summary

A new ransomware group called Kyber has reportedly deployed what incident responders at Rapid7 claim is genuine post-quantum encryption on Windows systems (medium confidence, not independently verified), which if accurate would make encrypted session keys theoretically unrecoverable even with future quantum computing capabilities. The group simultaneously targets VMware ESXi hypervisors, Windows file servers, Microsoft SQL Server, and Exchange, maximizing organizational disruption across a single attack. A claimed U.S. defense contractor victim elevates this to a critical threat for defense industrial base organizations and any enterprise running these platforms, pending verification.

Technical Analysis

Kyber ransomware operates two distinct encryptors. Based on vendor reporting (BleepingComputer citing Rapid7 incident response engagement, medium source confidence), the Windows variant allegedly implements Kyber1024 key encapsulation mechanism (KEM), standardized by NIST under FIPS 203 as ML-KEM. This claim has not been independently corroborated. The ESXi variant targets VMware ESXi hypervisors but reportedly does NOT implement post-quantum cryptography; Rapid7 analysis allegedly found those claims false for that payload. Affected platforms: Windows file servers, VMware ESXi, Microsoft Hyper-V, Microsoft SQL Server, Microsoft Exchange. No CVE is associated; access appears to leverage existing mechanisms rather than a

single disclosed vulnerability. Observed MITRE techniques include T1078 (Valid Accounts), T1021 (Remote Services), T1059 (Command and Scripting Interpreter), T1083 (File and Directory Discovery), T1057 (Process Discovery), T1486 (Data Encrypted for Impact), T1490 (Inhibit System Recovery), T1489 (Service Stop), T1485 (Data Destruction), T1070.001 (Clear Windows Event Logs), T1562.001 (Disable or Modify Tools). Relevant CWEs: CWE-693 (Protection Mechanism Failure, organizations lacking offline backups or MFA on administrative accounts), CWE-311 (Missing Encryption of Sensitive Data, backup security strategy reliance on classical recovery mechanisms). Note: CWE-327 does not apply; the attacker's use of Kyber1024 is cryptographically strong. The risk is organizational, not algorithmic. If confirmed, the Kyber1024 deployment would close the 'harvest now, decrypt later' recovery avenue that defenders have historically relied upon for post-incident key recovery.

Action Checklist

1. Containment: Audit external exposure of Windows file servers, VMware ESXi hosts, Hyper-V hosts, SQL Server, and Exchange immediately. Confirm RDP, SSH, and ESXi management interfaces (port 443, 902) are not directly internet-facing. Isolate any host showing anomalous encryption activity or mass file modifications. Verify ESXi hosts are patched against CVE-2024-37085 (VMware ESXi authentication bypass) as documented in Microsoft's July 2024 security advisory. This vulnerability has been observed in hypervisor-layer ransomware delivery chains; patch status is a prerequisite for containment.
2. Detection: Query Windows Security Event Logs for Event ID 4625 (failed logon), 4648 (explicit credential logon), and 4688 (process creation) for unusual execution chains involving cmd.exe, PowerShell, or wscript. Search for VSS deletion commands: 'vssadmin delete shadows', 'wmic shadowcopy delete', 'bcdedit /set recoveryenabled no'. On ESXi, review /var/log/hostd.log and /var/log/auth.log for unexpected VM power-off sequences and mass vmdk encryption activity. Flag processes terminating SQL Server (sqlservr.exe) or Exchange transport services abnormally. Monitor for creation of ransom note files (pattern: *.txt or *.html dropped in multiple directories in rapid succession).
3. Eradication: If compromise is confirmed, isolate affected hosts from the network before attempting any recovery action. Engage incident response; do NOT attempt in-place decryption without IR guidance. If Kyber's post-quantum implementation claim is verified, standard key recovery approaches will not apply to the Windows variant. For ESXi: apply VMware security patches current as of your ESXi version line. Rotate all service accounts and administrative credentials used on affected systems. Remove any unauthorized scheduled tasks, startup entries, or installed services identified during forensic review.
4. Recovery: Restore from offline or immutable backups only. Verify backup integrity before restoration, confirm backup files were not accessed or modified during the attacker's dwell time. After restoration, validate that VSS, Windows Backup, and ESXi snapshot capabilities are fully restored and functional. Monitor restored systems for re-infection indicators for a minimum of 30 days. Confirm Exchange and SQL Server service accounts have been rotated and MFA is enforced on all administrative access.
5. Post-Incident: Conduct a privileged access review: T1078 (Valid Accounts) and T1021 (Remote Services) indicate the group likely used legitimate credentials for lateral movement. Evaluate whether post-quantum cryptographic resilience affects your backup key management strategy; if session keys in encrypted backups rely on classical key exchange, review those assumptions. Document the Kyber1024 KEM deployment claim for your threat model; if verified, this represents an emerging capability that closes a historical decryption recovery avenue. Report confirmed or suspected DIB-sector incidents to CISA and DC3 per applicable reporting obligations.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to CISO, legal counsel, and external IR retainer if any of the following are confirmed: ESXi VMDK encryption activity detected, SQL Server or Exchange databases rendered inaccessible, any DIB-sector data (CUI, ITAR-controlled) present on affected systems triggering DFARS 252.204-7012 72-hour CISA notification requirement, or forensic evidence suggests Kyber1024 KEM keys were successfully generated (rendering encrypted files unrecoverable without backup restoration).
Recovery Notes	Restore only from backups predating the earliest confirmed Kyber activity timestamp — do not trust any backup touched during attacker dwell time without hash verification against pre-incident checksums, as Kyber operators may have staged exfiltration or tampered with backup catalogs. After restoration, deploy Sysmon with file-creation monitoring (Event ID 11) scoped to bulk file-rename patterns (*.kyber or operator-specific extensions) and run daily `vssadmin list shadows` checks for 30 days to confirm VSS integrity is maintained. Given the post-quantum KEM implementation, maintain forensic-grade images of all encrypted systems indefinitely — do not destroy them — as future cryptanalytic developments or law enforcement key seizures may enable eventual recovery.
Forensic Artifacts	ESXi /var/log/hostd.log and /var/log/shell.log: contain timestamped VM power-off sequences (`vim-cmd vmsvc/power.off`) and interactive SSH commands executed by Kyber operators immediately before bulk VMDK encryption — the chronological gap between power-off events and VMDK modification timestamps establishes attacker dwell and encryption timeline | Windows Security Event Log Event ID 4688 (Process Creation) with ProcessCommandLine field: captures the exact VSS destruction command (`vssadmin delete shadows /all /quiet`, `bcdedit /set recoveryenabled no`) spawned by the Kyber dropper process, establishing the ransomware execution chain and parent process ancestry | VMFS datastore VMDK and -delta.vmdk file metadata: filesystem modification timestamps on `/vmfs/volumes//*.vmdk` files establish the per-VM encryption sequence and confirm whether ESXi CVE-2024-37085 authentication bypass was the hypervisor entry vector by correlating with hostd.log authentication failures preceding the encryption window | Windows registry key HKLM\SYSTEM\CurrentControlSet\Services\ and HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run: Kyber persistence mechanism artifacts — unauthorized services (Event ID 7045) or Run key entries created during dwell time; export full hive (`reg export HKLM\SYSTEM C:\ir\SYSTEM.reg`) before eradication | Memory dump of the ransomware process (if caught pre-completion) via ProcDump (`procdump.exe -ma C:\ir\kyber_memdump.dmp`): the Kyber1024 KEM implementation may leave the encapsulated session key or partial key material in process memory during active encryption, representing the only viable path to key recovery and warranting immediate capture before process termination or system reboot

Per-Action IR Details

Containment — Audit external exposure of Windows file servers, VMware ESXi hosts, Hyper-V hosts, SQL Server, and Exchange immediately. Confirm RDP, SSH, and ESXi management interfaces (port 443, 902) are not directly internet-facing. Isolate any host showing anomalous encryption activity or mass file modifications. Verify ESXi hosts are patched against CVE-2024-37085 (VMware ESXi authentication bypass, documented in Microsoft's July 2024 blog), as that vulnerability has been widely exploited for hypervisor-layer ransomware delivery.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST CM-7 (Least Functionality), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Run `netstat -ano | findstr ':3389 :443 :902'` on each Windows/ESXi host to enumerate active listeners; cross-reference PIDs against Task Manager or `tasklist /svc`. For ESXi exposure, use `esxcli network firewall ruleset list` via SSH to confirm management interface lockdown. Block ports 443/902 inbound at the perimeter firewall or host-based Windows Firewall (`netsh advfirewall firewall add rule name='Block ESXi Mgmt' protocol=TCP dir=in localport=902 action=block`). Validate CVE-2024-37085 patch status by running `vmware -v` on each ESXi host and comparing against VMware VMSA-2024-0013 fixed build numbers.

Evidence: Before isolating, capture full network connection state: `netstat -ano > c:\ir\netstat_$(hostname).txt` and ESXi `esxcli network connection list > /tmp/connections.txt`. Snapshot ESXi host memory via `vm-support -w /vmfs/volumes/` for post-quantum KEM artifact recovery. Preserve Windows Security Event Log (`wevtutil epl Security C:\ir\Security.evtx`) and ESXi `/var/log/hostd.log`, `/var/log/vpxa.log` before any remediation. Document which VMDKs are actively encrypted by listing `/vmfs/volumes//*.vmdk` modification timestamps.

Detection — Query Windows Security Event Logs for Event ID 4625 (failed logon), 4648 (explicit credential logon), and 4688 (process creation) for unusual execution chains involving cmd.exe, PowerShell, or wscript. Search for VSS deletion commands: 'vssadmin delete shadows', 'wmic shadowcopy delete', 'bcdedit /set recoveryenabled no'. On ESXi, review /var/log/hostd.log and /var/log/auth.log for unexpected VM power-off sequences and mass vmdk encryption activity. Flag processes terminating SQL Server (sqlservr.exe) or Exchange transport services abnormally. Monitor for creation of ransom note files (pattern: *.txt or *.html dropped in multiple directories in rapid succession).

NIST Phase: Detection Analysis

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

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with SwiftOnSecurity config (github.com/SwiftOnSecurity/sysmon-config) to capture Event ID 1 (Process Create) and Event ID 8 (CreateRemoteThread) for Kyber's service-termination behavior. Run this PowerShell on each Windows host to detect VSS destruction: `Get-WinEvent -LogName Security | Where-Object {$_.Message -match 'vssadmin|shadowcopy|bcdedit'} | Select TimeCreated,Message | Export-Csv C:\ir\vss_events.csv`. On ESXi, run `grep -i 'poweroff\|vmdk\|encrypt' /var/log/hostd.log` to surface VM shutdown sequences preceding encryption. Use Sigma rule `win_ransomware_babuk` (adapted) to detect the sqlservr.exe and Exchange MSExchangeTransport service-kill pattern via Windows Event Forwarding.

Evidence: Collect Sysmon Event ID 1 logs showing cmd.exe or powershell.exe spawned under the context of IIS worker process (w3wp.exe) or MSSQLSERVER service — Kyber's initial access via internet-facing services would produce this parent-child chain. Capture `HKLM\SYSTEM\CurrentControlSet\Services\VSS` registry state to confirm VSS service tampering. On ESXi, extract `/var/log/shell.log` for interactive SSH commands and `/var/log/hostd.log` entries timestamped within the attacker dwell window showing `vim-cmd vmsvc/power.off` calls preceding bulk vmdk modification. Capture Exchange `MSExchange Management` event log for unexpected transport service stop events (Event ID 1005/1007).

Eradication — If compromise is confirmed, isolate affected hosts from the network before attempting any recovery action. Engage incident response; do NOT attempt in-place decryption without IR guidance — the Kyber1024 KEM implementation means standard key recovery approaches will not apply to the Windows variant. For ESXi: apply VMware security patches current as of your ESXi version line. Rotate all service accounts and administrative credentials used on affected systems. Remove any unauthorized scheduled tasks, startup entries, or installed services identified during forensic review.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST IA-5 (Authenticator Management), NIST CM-7 (Least Functionality), CIS 5.2 (Use Unique Passwords), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 7.3 (Perform Automated Operating System Patch Management)

Compensating: Enumerate all scheduled tasks created during attacker dwell window: `schtasks /query /fo LIST /v | findstr /i 'Task Name\|Run As\|Last Run\|Status'` and compare creation timestamps against known-good baseline. List installed services modified in the same window: `sc query type= all state= all` and cross-reference with `Get-WinEvent -LogName System | Where-Object {$_.Id -eq 7045}` (new service installed). For ESXi persistence, check `/etc/rc.local.d/` and `/etc/vmware/hostd/` for unauthorized startup scripts. Rotate all AD service accounts used by SQL Server, Exchange transport, and ESXi vCenter using `Set-ADAccountPassword` and force immediate Kerberos ticket invalidation via `klist purge` on all domain controllers.

Evidence: Before credential rotation, export Active Directory last-logon timestamps for all service accounts: `Get-ADUser -Filter {ServicePrincipalName -ne '$null'} -Properties LastLogonDate,ServicePrincipalName | Export-Csv C:\ir\svc_accounts.csv` to establish attacker lateral movement timeline via T1078. Preserve a full copy of Windows Task Scheduler XML files from `C:\Windows\System32\Tasks\` and `C:\Windows\SysWOW64\Tasks\` before removal. On ESXi, capture `esxcli software vib list` output pre-patch to document unauthorized VIB installations (a known ESXi persistence mechanism). Image affected Windows hosts to forensic-grade copies before OS rebuild to preserve Kyber1024 KEM artifacts for potential future cryptographic analysis.

Recovery — Restore from offline or immutable backups only. Verify backup integrity before restoration — confirm backup files were not accessed or modified during the attacker's dwell time. After restoration, validate that VSS, Windows Backup, and ESXi snapshot capabilities are fully restored and functional. Monitor restored systems for re-infection indicators for a minimum of 30 days. Confirm Exchange and SQL Server service accounts have been rotated and MFA is enforced on all administrative access.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST CP-9 (System Backup), NIST CP-10 (System Recovery and Reconstitution), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: Verify backup integrity by comparing SHA-256 hashes of backup catalog files against hashes recorded at backup creation time: `Get-FileHash -Algorithm SHA256 -Path '\*.bkf'`. Confirm backup media was not mounted or accessed during attacker dwell by reviewing `C:\Windows\System32\winevt\Logs\Microsoft-Windows-Backup%4Operational.evtx` for unauthorized backup access events. Re-enable and validate VSS: `vssadmin list writers` should return all writers in a Stable/No error state; `vssadmin list shadows` should show current shadow copies. For ESXi recovery, restore VMs from a datastore backup predating the earliest confirmed Kyber activity timestamp in `/var/log/hostd.log`. Enforce MFA on Exchange OWA and EAC using Windows Hello for Business or a free RADIUS+Google Authenticator deployment for admin RDP sessions.

Evidence: Before restoring any system, audit backup access logs in Windows Event Log `Microsoft-Windows-Backup` channel and any backup agent logs (Veeam, Windows Server Backup) for unauthorized `Read` or `Export` operations during the confirmed attacker dwell window — Kyber operators likely staged data exfiltration from backup repositories before encrypting. Capture ESXi snapshot delta-disk (`.vmdk` and `-delta.vmdk`) modification timestamps to establish the precise encryption start time per VM. Document SQL Server database file (`.mdf`/`.ldf`) last-modified timestamps from forensic images to confirm whether databases were exfiltrated prior to encryption, informing breach notification obligations.

Post-Incident — Conduct a privileged access review: T1078 (Valid Accounts) and T1021 (Remote Services) indicate the group likely used legitimate credentials for lateral movement. Evaluate whether post-quantum cryptographic resilience affects your backup key management strategy — if session keys in encrypted backups rely on classical key exchange, review those assumptions. Document the Kyber1024 KEM deployment for your threat model; this is an emerging capability that closes a historical decryption recovery avenue. Report confirmed or suspected DIB-sector incidents to CISA and DC3 per applicable reporting obligations.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST IR-5 (Incident Monitoring), NIST IR-6 (Incident Reporting), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST AC-2 (Account Management), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.3 (Disable Dormant Accounts)

Compensating: Conduct privileged access review using `Get-ADUser -Filter {Enabled -eq $true} -Properties LastLogonDate,MemberOf | Where-Object {$_.MemberOf -match 'Domain Admins|Enterprise Admins|Schema Admins'}` and flag any account with LastLogonDate within the attacker dwell window but not associated with known admin activity. Cross-reference against MITRE ATT&CK T1078.002 (Domain Accounts) and T1021.001 (Remote Desktop Protocol) by reviewing Event ID 4648/4624 Type 10 logons. For post-quantum backup key review, audit whether your backup encryption uses RSA or ECDH key wrapping (classical) versus CRYSTALS-Kyber or similar NIST PQC-standardized algorithm — document the gap for your CISO. Submit incident report to CISA via https://www.cisa.gov/report and to DC3 Cyber Crime Center via https://www.dc3.mil/Missions/Cyber-Forensics/DC3-Cyber-Crime-Center/ per DFARS 252.204-7012 obligations for DIB-sector entities.

Evidence: Compile the full attacker timeline from correlated Event IDs: 4624 (successful logon) → 4648 (explicit credential use) → 4688 (process creation for ransomware binary) → 7045 (new service install) → 4625 spikes (credential stuffing pre-access), mapped against ESXi `/var/log/hostd.log` VM power-off timestamps to reconstruct the kill chain. Preserve all forensic disk images, memory captures, and log archives for a minimum of 3 years given DIB-sector regulatory retention requirements. Document Kyber1024 KEM binary samples (hash them: `Get-FileHash -Algorithm SHA256`) and submit to CISA's Malware Analysis Service and VirusTotal for community threat intelligence contribution.

Detection Guidance

Primary behavioral indicators: (1) Rapid mass file extension modification across Windows file servers, monitor for high-volume rename or overwrite events via Windows Security Event ID 4663 (object access) with audit policies enabled on file shares. (2) VSS and backup deletion commands, alert on process creation events (Event ID 4688 or Sysmon Event ID 1) containing 'vssadmin', 'wmic shadowcopy', or 'bcdedit' with recovery-disabling arguments. (3) Security tool termination, monitor for processes killing AV/EDR services (T1562.001); Sysmon Event ID 1 for parent/child process chains terminating known security processes. (4) Windows Event Log clearing, Event ID 1102 (Security log cleared) and 104 (System log cleared) are direct indicators of T1070.001. (5) ESXi-specific: monitor for simultaneous VM power-off events across multiple VMs in a short window, followed by vmdk file modifications, this pattern is consistent with hypervisor-layer bulk encryption. (6) Exchange and SQL Server service stops outside maintenance windows, alert on Service Control Manager events (Event ID 7036) for these services stopping unexpectedly. IOC note: No confirmed file hashes, IPs, or domains have been published at time of analysis. This means behavioral indicators are the primary detection layer, which carries higher false-positive risk until technical IOCs are released. Security teams should correlate behavioral alerts with contextual investigation (e.g., recent credential compromise, open RDP ports) before escalating to incident response.

Indicators of Compromise

Type	Value	Context	Confidence
HASH	not published	No file hashes for Kyber Windows or ESXi encryptors have been publicly released as of this analysis. Monitor Rapid7 and BleepingComputer for subsequent IOC releases.	LOW
DOMAIN	not published	No C2 domains or ransom payment infrastructure have been publicly attributed to Kyber at time of analysis.	LOW

Framework Mappings

MITRE-ATTACK

- **T1490** — Inhibit System Recovery
- **T1083** — File and Directory Discovery
- **T1486** — Data Encrypted for Impact
- **T1021** — Remote Services
- **T1070.001** — Clear Windows Event Logs
- **T1059** — Command and Scripting Interpreter
- **T1489** — Service Stop
- **T1078** — Valid Accounts
- **T1562** — Impair Defenses
- **T1562.001** — Disable or Modify Tools
- **T1485** — Data Destruction
- **T1057** — Process Discovery

NIST-800-53R5

- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AC-17** — Remote Access
- **AC-3** — Access Enforcement
- **CM-7** — Least Functionality
- **IA-2** — Identification and Authentication (Organizational Users)
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **CM-6** — Configuration Settings
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-5** — Authenticator Management

- **AU-9** — Protection of Audit Information
- **SC-13** — Cryptographic Protection
- **IR-4** — Incident Handling

OWASP-TOP10-2021

- **A02:2021** — Cryptographic Failures

ISO-27001-2022

- **A.8.24** — Use of cryptography
- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information

NIST-CSF-2

- **RS.MI-01** — Incidents are contained

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.312(e)(1)** — Transmission Security

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1490	Inhibit System Recovery	Impact
T1083	File and Directory Discovery	Discovery
T1486	Data Encrypted for Impact	Impact
T1021	Remote Services	Lateral-Movement
T1070.001	Clear Windows Event Logs	Defense-Evasion
T1059	Command and Scripting Interpreter	Execution
T1489	Service Stop	Impact
T1078	Valid Accounts	Defense-Evasion
T1562	Impair Defenses	Defense-Evasion
T1562.001	Disable or Modify Tools	Defense-Evasion
T1485	Data Destruction	Impact
T1057	Process Discovery	Discovery

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/kyber-ransomware-gan...	T3
Ransomware operators exploit ESXi hypervisor vulnerability for ...	https://www.microsoft.com/en-us/security/blog/2024/07/29/ransomware...	T1
The Great VM Escape: ESXi Exploitation in the Wild - Huntress	https://www.huntress.com/blog/esxi-vm-escape-exploit	T3
Microsoft calls out apparent ESXi vulnerability that some ... - Reddit	https://www.reddit.com/r/cybersecurity/comments/1eg0hcj/microsoft_c...	T3
Microsoft December 2025 Security Updates / FYI	https://learn.microsoft.com/en-ca/answers/questions/5653856/microso...	T1

Generated 2026-04-23 06:38 UTC by TJS Security Command Center