INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:37 UTC

Historical and Recent Ransomware Attack Campaigns: Overview

THREAT CAMPAIGN | CRITICAL | CVSS 9.8

SCC Item ID	SCC-CAM-2026-0004
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.8
Affected Products	Multiple platforms and sectors; Windows systems prominently affected (e.g., WannaCry targeted unpatched SMBv1 on Windows XP through Windows Server 2008 R2); additional campaigns targeted healthcare, critical infrastructure, financial, and government sectors across varied OS and application environments
Published	Dec 9, 2025

Executive Summary

Ransomware campaigns spanning 2017 through 2026 have caused hundreds of billions in aggregate damages across healthcare, critical infrastructure, financial services, and government sectors worldwide. Nation-state and criminal operators alike deploy ransomware through phishing, unpatched vulnerabilities, and supply chain compromises, frequently exfiltrating data before encrypting systems to maximize leverage. Organizations that lack patched perimeters, segmented networks, and tested recovery capabilities remain high-probability targets for operational disruption, regulatory exposure, and reputational harm.

Technical Analysis

This entry covers ransomware campaigns from 2017 to 2026 with varying technical profiles. WannaCry (May 2017) exploited CVE-2017-0144 (EternalBlue, CVSS 9.8, MS17-010) via SMBv1 on Windows XP through Server 2008 R2, achieving worm propagation without user interaction; attributed to Lazarus Group (DPRK) at high confidence per US-CERT/CISA. NotPetya (June 2017) combined EternalBlue with Mimikatz credential harvesting (T1003.001) and lateral movement via SMB (T1021.002), attributed to Sandworm (GRU Unit 74455) per US DOJ indictment (2020); CSIS estimates aggregate damages exceeded $10B. Subsequent RaaS operations, REvil, Conti, LockBit, ALPHV/BlackCat, Cl0p, introduced double extortion (T1486 + T1567), supply chain vectors (T1195.002; Kaseya VSA 2021, MOVEit Transfer 2023), and abuse of legitimate remote management tooling (T1078, T1047). ALPHV/BlackCat's Change Healthcare attack (2024) disrupted US pharmacy and claims processing infrastructure; attributed at high confidence per HHS and FBI advisories. Common CWEs across campaigns: CWE-119 (buffer overflow/memory corruption), CWE-287 (improper

authentication), CWE-522 (insufficiently protected credentials), CWE-494 (download without integrity check), CWE-434 (unrestricted file upload), CWE-798 (hard-coded credentials), CWE-502 (deserialization of untrusted data). Key MITRE ATT&CK techniques: T1566/T1566.001 (phishing), T1190 (exploit public-facing application), T1210 (exploitation of remote services), T1059/T1059.001 (command and scripting interpreter), T1570 (lateral tool transfer), T1489/T1490 (inhibit system recovery and service stop), T1486 (data encrypted for impact). Patch status: MS17-010 has been available since March 2017; MOVEit and Kaseya patches were released in response to active exploitation. Primary sources are CISA advisories and MITRE ATT&CK entries; supplementary sources include CrowdStrike, SentinelOne, TechTarget, and CSIS tracking.

Action Checklist

1. Step 1, Immediate: Verify MS17-010 (EternalBlue) patches are applied across all Windows systems; disable SMBv1 where not already done. Confirm MOVEit Transfer and Kaseya VSA instances are patched to current vendor-recommended versions (consult Kaseya and Progress/OpenText advisories for specific patch version numbers).
2. Step 2, Detection: Search endpoint and network telemetry for indicators of double-extortion staging, large outbound data transfers preceding encryption events, SMB lateral movement attempts, and LSASS memory access (T1003.001). Review CISA advisories AA21-265A (Conti), AA23-165A (LockBit), and AA23-158A (Cl0p) for actor-specific IOC lists.
3. Step 3, Assessment: Inventory public-facing applications and remote management tools (RMM, VPN, RDP) for unpatched vulnerabilities and exposed credentials. Map coverage against MITRE ATT&CK techniques T1190, T1078, T1021.002, T1047 to identify detection gaps.
4. Step 4, Communication: Brief executive leadership and legal counsel on current ransomware threat landscape relevance to your sector; confirm incident response retainer and cyber insurance policy terms are current. If healthcare or critical infrastructure, review HHS and CISA sector-specific advisories for mandatory reporting obligations.
5. Step 5, Long-term: Test backup integrity and recovery time objectives against ransomware scenarios, including encrypted-backup and shadow-copy-deletion conditions (T1490). Implement network segmentation to limit lateral movement blast radius. Integrate RaaS TTP profiles from CISA and MITRE ATT&CK into detection rule backlog and tabletop exercise scenarios on a recurring basis.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to external IR firm and legal counsel immediately if any system exhibits signs of active encryption, large outbound data transfers to unknown destinations, or multiple failed logon attempts on privileged accounts; critical infrastructure and healthcare organizations must notify CISA/HHS within 24 hours of suspected ransomware staging.

Recovery Notes	Post-containment: validate that all encrypted systems are isolated and backups are proven-clean before restoring. Implement a phased recovery plan that restores non-critical systems first to validate backup integrity, prioritize business-critical systems second, and reserve offline forensic images of encrypted systems for post-recovery analysis. Update detection rules with observed IOCs (file hashes, C2 domains, attacker-specific command patterns) and conduct a post-incident review to quantify dwell time, identify missed detection opportunities, and update incident response procedures.
Forensic Artifacts	Windows Event Logs: 4624, 4625, 4672 (privileged logon), 4688 (process creation), 4720 (account creation), 5140 (network share access), 5156 (firewall allow), and Sysmon Event IDs 1 (process creation), 3 (network connection), 7 (image load), 10 (process access to LSASS), 11 (file creation), 13 (registry set), 21 (WmiEvent) | Master File Table (MFT) and NTFS journal ($LogFile) from affected volumes to reconstruct file encryption timeline and identify initial encryption vectors | Windows Registry: HKLM\Software\Microsoft\Windows\CurrentVersion\WindowsUpdate (patch history), HKLM\System\CurrentControlSet\Services (RMM/VPN service configs), SAM and SECURITY hives (credential material), and HKEY_CLASSES_ROOT (file association changes for ransomware-generated extensions) | Prefetch files (C:\Windows\Prefetch) and ShimCache (HKLM\System\CurrentControlSet\Control\Session Manager\AppCompatFlags\ShimCache) to identify tools used for lateral movement and privilege escalation | Network artifacts: Firewall deny/allow logs, DNS query logs (queries to attacker-controlled domains), proxy/WAF logs (initial exploitation attempts on public-facing apps), NetFlow/sFlow records (volume and destination of data exfiltration), and full packet captures (pcap) from suspected data staging periods | Memory dumps from systems showing LSASS access (Event ID 4656) to detect in-memory credential theft via tools like Mimikatz, and pagefile analysis if LSASS process was dumped to disk | Shadow Copy metadata (if not deleted) via `vssadmin list shadows`, backup database logs (Veeam, Commvault, etc.) showing backup success/failure and access times, and deleted file recovery to identify overwritten backups or shadow copy deletion artifacts

Per-Action IR Details

Step 1, Immediate: Verify MS17-010 (EternalBlue) patches are applied across all Windows systems; disable SMBv1 where not already done. Confirm MOVEit Transfer and Kaseya VSA instances are patched to current vendor-recommended versions (consult Kaseya and Progress/OpenText advisories for specific patch version numbers).

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation: awareness and tools)

Controls: NIST 800-53 SI-2 (Flaw Remediation), NIST 800-53 CM-3 (Change Control), CIS 2.3 (Address Unauthorized Software), CIS 7.4 (Maintain Secure Configuration Standards)

Compensating: Use Microsoft Baseline Security Analyzer (MBSA, free) or Windows Update inventory scripts (PowerShell: `Get-HotFix | Select HotFixID, InstalledOn`) to audit patch status across domain-joined systems. For air-gapped networks, maintain offline patch manifests and apply via WSUS. Disable SMBv1 via PowerShell: `Disable-WindowsOptionalFeature -FeatureName SMB1Protocol -Online -NoRestart` on each system or via Group Policy (Computer Configuration > Policies > Administrative Templates > Network > Lanman Workstation > "Disable SMBv1 Client Driver").

Evidence: Before patching: capture `Get-HotFix` output and Windows Update history (Registry: HKLM\Software\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update\Results\Install) to establish pre-patch vulnerability baseline. Document SMBv1 status via `Get-SmbServerConfiguration | Select EnableSMB1Protocol` and network packet captures (tcpdump: `tcpdump -i eth0 -w smb_baseline.pcap 'tcp port 445'`) to confirm lateral movement vectors before remediation.

Step 2, Detection: Search endpoint and network telemetry for indicators of double-extortion staging, large outbound data transfers preceding encryption events, SMB lateral movement attempts, and LSASS memory access (T1003.001). Review CISA advisories AA21-265A (Conti), AA23-165A (LockBit), and AA23-158A (Cl0p) for actor-specific IOC lists.

NIST Phase: Detection Analysis

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

Controls: NIST 800-53 SI-4 (Information System Monitoring), NIST 800-53 AU-6 (Audit Review, Analysis, and Reporting), CIS 8.1 (Unified Logging and Log Analysis), CIS 8.8 (Implement Logging for External Removable Media)

Compensating: Without SIEM: parse Windows Event Logs locally using PowerShell to detect T1003.001 (LSASS access via Event ID 4656 with Object Name containing 'lsass.exe'). Search for lateral movement via SMB using Event ID 5140 (SMB share access) and Event ID 4625 (failed logon spikes). For data exfiltration, monitor Firewall logs (Event ID 5152–5158) for outbound connections to non-whitelisted destinations, and use NetFlow (if available) or tcpdump with Zeek IDS (free, open-source) to baseline outbound traffic. Cross-reference CISA IOC feeds manually: parse CVE/ATT&CK data, extract IP/domain/hash indicators, and search endpoint logs with grep or PowerShell `-Match`.

Evidence: Before detection rule deployment: capture 7–14 days of baseline Windows Event Logs (4624, 4625, 4688, 4720, 5140, 5156), Sysmon logs (if deployed; Event IDs 1, 3, 7, 10, 11, 13), DNS query logs, HTTP/HTTPS proxy logs (if available), and Firewall deny/allow logs. Preserve full packet captures (tcpdump) during known high-risk windows (off-hours, maintenance). Document process execution baseline on critical systems via `Get-Process` snapshots and Task Scheduler history (Event ID 106, 200).

Step 3, Assessment: Inventory public-facing applications and remote management tools (RMM, VPN, RDP) for unpatched vulnerabilities and exposed credentials. Map coverage against MITRE ATT&CK techniques T1190, T1078, T1021.002, T1047 to identify detection gaps.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation: risk assessment and mitigation strategies)

Controls: NIST 800-53 CM-2 (Baseline Configuration), NIST 800-53 RA-3 (Risk Assessment), NIST 800-53 AC-2 (Account Management), CIS 4.1 (Inventory and Control of Enterprise Assets), CIS 5.3 (Configure Data Access Control Lists)

Compensating: Use free tools: Nessus Essentials (free community scanner, 16 IPs max), OpenVAS (open-source, unlimited), or Qualys FreeScan for vulnerability scans on public-facing assets. For credential exposure: query `nltest /domain_trusts` and `net group "Domain Admins" /domain` to enumerate privileged accounts; audit RDP access logs (Event ID 4624, LogonType=10) and VPN logs for dormant or overprivileged accounts. Create a manual ATT&CK mapping spreadsheet: list each public-facing tool (e.g., RDP on port 3389, Kaseya VSA on port 9191), note current patch level, cross-reference against MITRE ATT&CK techniques (T1190=exploit public-facing app, T1078=valid accounts, T1021.002=RDP, T1047=WMI exec), and document which detection methods exist (log monitoring, EDR, network IDS).

Evidence: Before deploying detection rules: capture baseline configurations (RDP registry: HKLM\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp, port bindings, firewall rules via `netstat -ab`), enumerate installed RMM/VPN software and versions via `HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall`, audit local admin and service accounts (SAM registry, `net user` output), and document public IP/DNS resolution history (DNS logs, firewall logs, reverse DNS).

Step 4, Communication: Brief executive leadership and legal counsel on current ransomware threat landscape relevance to your sector; confirm incident response retainer and cyber insurance policy terms are current. If healthcare or critical infrastructure, review HHS and CISA sector-specific advisories for mandatory reporting obligations.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.2 (Preparation: roles and responsibilities)

Controls: NIST 800-53 IR-1 (Incident Response Policy), NIST 800-53 SI-1 (System and Information Integrity Policy), NIST 800-53 SA-3 (System Development Life Cycle), CIS 19.1 (Document Incident Response Procedures)

Compensating: No technical tooling required. Document communication plan in plain text or email: identify C-suite contacts (CISO, CFO, General Counsel, COO), establish escalation thresholds (e.g., >100 systems encrypted = executive briefing within 1 hour), and prepare sector-specific talking points using CISA sector alerts (healthcare: HHS 405(d) breach notification, critical infrastructure: NERC CIP mandatory reporting, financial: SEC Form 8-K disclosure if material). Create a one-page IR retainer summary from counsel stating response firm SLAs, insurance policy excerpt confirming coverage limits and notification requirements, and a list of mandatory external reporters (HHS/FBI/DHS CISA regional office contact details).

Evidence: Preserve evidence of policy review and approval: email confirmations from legal/CISO on incident response plan sign-off, copies of insurance policy declarations page and endorsements, proof of IR retainer contract execution (signature and date), and screenshots/copies of CISA and HHS advisories reviewed (AA21-265A, AA23-165A, AA23-158A for ransomware actors, plus sector-specific guidance).

Step 5, Long-term: Test backup integrity and recovery time objectives against ransomware scenarios, including encrypted-backup and shadow-copy-deletion conditions (T1490). Implement network segmentation to limit lateral movement blast radius. Integrate RaaS TTP profiles from CISA and MITRE ATT&CK into detection rule backlog and tabletop exercise scenarios on a recurring basis.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.4 (Recovery) and §2.1 (Preparation: tools and techniques)

Controls: NIST 800-53 CP-4 (Contingency Plan Testing), NIST 800-53 SC-7 (Boundary Protection), NIST 800-53 CP-9 (Information System Backup), NIST 800-53 IR-4 (Incident Handling), CIS 11.3 (Address Unauthorized Software), CIS 3.6 (Ensure Adequate Audit Log Storage)

Compensating: Backup testing: perform monthly restore drills on a sandbox network; validate backup files are read-only and immutable (test `attrib +r` on Windows or filesystem ACLs on Linux), and confirm shadow copies are protected (disable user deletion via `vssadmin list shadows` audit). For network segmentation without enterprise appliances: use Windows Firewall with Advanced Security (WFAS) Group Policies to restrict traffic between subnets (e.g., workstations block port 445/139 to servers outside their segment, isolate SCADA networks on separate VLANs with manual air-gap if possible). Build detection rules from MITRE ATT&CK profiles: download MITRE Navigator JSON for ransomware campaigns (Conti, LockBit, Cl0p), extract technique IDs (T1490=inhibit system recovery, T1027.010=encrypted files, T1083=file enumeration), and map to available logs (PowerShell Script Block Logging for obfuscation, Windows Defender quarantine logs, Sysmon Event ID 11 for file creation patterns ending in .crypted/.locked/.paid, etc.). Schedule tabletop exercises quarterly: simulate double-extortion scenario, track detection time-to-first-alert, test backup recovery, measure RTO/RPO against business tolerance.

Evidence: Before long-term implementation: baseline backup metadata (size, date, restore-test results, storage location and retention), document network topology and current segmentation (firewall rules, VLAN assignments, data flow diagrams), preserve MITRE ATT&CK baseline detection rules (rule version, coverage map, false-positive rates from prior quarter), and record tabletop exercise outcomes (detection gaps, recovery time actual vs. target, communication delays).

Detection Guidance

Detection should target behavioral patterns common across documented campaigns rather than static IOCs alone, as RaaS operators rotate infrastructure frequently. Key behavioral indicators: (1) LSASS process memory access from non-system processes, correlates with T1003.001/Mimikatz credential harvesting; query Windows Security Event ID 4656/4663 with target object lsass.exe. (2) Lateral SMB connections from workstations to workstations, correlates with T1021.002/EternalBlue propagation; alert on SMB traffic from endpoints outside standard server-to-endpoint patterns. (3) Volume Shadow Copy deletion via vssadmin.exe or wmic.exe, direct indicator of T1490 pre-encryption activity; alert on process creation events matching 'vssadmin delete shadows' or 'wmic shadowcopy delete'. (4) Bulk file rename or extension change events in short time windows, primary encryption activity indicator (T1486); EDR telemetry or file integrity monitoring with rate thresholds. (5) Large

outbound transfers to cloud storage or unusual endpoints before encryption, double extortion staging (T1567); monitor DLP and proxy logs for anomalous upload volumes. (6) Scheduled tasks or services created by non-standard parent processes, persistence and staging (T1059). For supply chain vectors (T1195.002), monitor software update processes for unexpected network connections or unsigned binary execution. Reference CISA advisories (available at cisa.gov/advisories): AA23-158A (Cl0p/MOVEit), AA23-165A (LockBit), AA21-265A (Conti), and MITRE ATT&CK Group entries G0032 (Lazarus), G0034 (Sandworm), for actor-specific detection signatures. Note: static IOCs for campaigns of this age have low residual detection value; behavioral detection is the primary recommended approach.

Indicators of Compromise

Type	Value	Context	Confidence
HASH	`Not providing, static hashes for 2017-2026 campaign variants have low detection value due to polymorphism and variant proliferation; consult current CISA advisories and threat intel feeds for active IOC lists.`	WannaCry, NotPetya, REvil, LockBit, ALPHV/BlackCat, Cl0p, campaign-specific hashes available via CISA, FBI, and vendor threat intel portals	LOW
URL	`https://www.cisa.gov/news-events/cybersecurity-advisories`	CISA advisory index, source for current IOC lists for LockBit (AA23-165A), Cl0p/MOVEit (AA23-158A), Conti (AA21-265A), ALPHV/BlackCat, and REvil/Sodinokibi joint advisories. URL retrieved from known CISA domain; recommend human validation.	HIGH
URL	`https://attack.mitre.org/groups/`	MITRE ATT&CK Groups index, actor profiles for Lazarus Group (G0032), Sandworm (G0034), and associated software entries with linked IOCs. URL retrieved from known MITRE domain; recommend human validation.	HIGH

Framework Mappings

MITRE-ATTACK

- **T1059** — Command and Scripting Interpreter
- **T1059.001** — PowerShell
- **T1210** — Exploitation of Remote Services
- **T1003.001** — LSASS Memory
- **T1489** — Service Stop
- **T1570** — Lateral Tool Transfer
- **T1195.002** — Compromise Software Supply Chain

- **T1490** — Inhibit System Recovery
- **T1195** — Supply Chain Compromise
- **T1027** — Obfuscated Files or Information
- **T1566** — Phishing
- **T1003** — OS Credential Dumping
- **T1190** — Exploit Public-Facing Application
- **T1021.002** — SMB/Windows Admin Shares
- **T1078** — Valid Accounts
- **T1047** — Windows Management Instrumentation
- **T1566.001** — Spearphishing Attachment
- **T1567** — Exfiltration Over Web Service
- **T1486** — Data Encrypted for Impact
- **T1071** — Application Layer Protocol

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **CM-6** — Configuration Settings
- **SA-9** — External System Services
- **SR-3** — Supply Chain Controls and Processes
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **SR-2** — Supply Chain Risk Management Plan
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SI-8** — Spam Protection
- **IA-5** — Authenticator Management
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **AC-2** — Account Management
- **IA-2** — Identification and Authentication (Organizational Users)
- **CM-3** — Configuration Change Control
- **SI-10** — Information Input Validation
- **IA-8** — Identification and Authentication (Non-Organizational Users)

- **SI-16** — Memory Protection
- **IR-4** — Incident Handling
- **SC-13** — Cryptographic Protection

OWASP-TOP10-2021

- **A04:2021** — Insecure Design
- **A07:2021** — Identification and Authentication Failures
- **A08:2021** — Software and Data Integrity Failures
- **A03:2021** — Injection

CIS-V8

- **5.2**
- **2.5**
- **2.6**
- **16.10**
- **6.3**
- **6.4**
- **6.5**
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **15.1** — Establish and Maintain an Inventory of Service Providers

HIPAA-SECURITY

- **164.308(a)(5)(ii)(D)** — Password Management
- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.308(a)(5)(i)** — Security Awareness and Training
- **164.308(a)(6)(ii)** — Response and Reporting
- **164.312(e)(1)** — Transmission Security

ISO-27001-2022

- **A.8.28** — Secure coding
- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information
- **A.5.21** — Managing information security in the ICT supply chain
- **A.8.24** — Use of cryptography

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC7.4** — Responds to identified security incidents
- **CC9.2** — Manages risks associated with vendors and business partners

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **GV.SC-01** — Cybersecurity supply chain risk management program

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1059	Command and Scripting Interpreter	Execution
T1059.001	PowerShell	Execution
T1210	Exploitation of Remote Services	Lateral-Movement
T1003.001	LSASS Memory	Credential-Access
T1489	Service Stop	Impact
T1570	Lateral Tool Transfer	Lateral-Movement
T1195.002	Compromise Software Supply Chain	Initial-Access
T1490	Inhibit System Recovery	Impact
T1195	Supply Chain Compromise	Initial-Access
T1027	Obfuscated Files or Information	Defense-Evasion
T1566	Phishing	Initial-Access
T1003	OS Credential Dumping	Credential-Access
T1190	Exploit Public-Facing Application	Initial-Access
T1021.002	SMB/Windows Admin Shares	Lateral-Movement
T1078	Valid Accounts	Defense-Evasion
T1047	Windows Management Instrumentation	Execution
T1566.001	Spearphishing Attachment	Initial-Access
T1567	Exfiltration Over Web Service	Exfiltration
T1486	Data Encrypted for Impact	Impact
T1071	Application Layer Protocol	Command-And-Control

Sources

Source	URL	Tier
Trendmicro	https://www.trendmicro.com/en/what-is/ransomware/ransomware-example...	T3
26 Ransomware Examples Explained in 2026 - SentinelOne	https://www.sentinelone.com/cybersecurity-101/cybersecurity/ransomw...	T3
15 of the Biggest Ransomware Attacks in History - TechTarget	https://www.techtarget.com/searchsecurity/tip/The-biggest-ransomwar...	T3
16 Ransomware Examples From Recent Attacks | CrowdStrike	https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/rans...	T3
Significant Cyber Incidents | Strategic Technologies Program - CSIS	https://www.csis.org/programs/strategic-technologies-program/signif...	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-03-29 18:37 UTC by TJS Security Command Center