INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:38 UTC

Top 10 Ransomware Attacks Over The Past Year: Campaign Overview

THREAT CAMPAIGN | CRITICAL | CVSS 9.0

SCC Item ID	SCC-CAM-2026-0005
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.0
Affected Products	Multiple sectors including healthcare, finance, critical infrastructure, manufacturing, and government; specific products and versions vary by individual incident
Published	1 month ago

Executive Summary

Over the past year, ransomware groups including LockBit, ALPHV/BlackCat, Cl0p, Black Basta, and Rhysida have executed high-impact campaigns against healthcare, finance, critical infrastructure, manufacturing, and government organizations globally. These actors consistently combine file encryption with data theft and public leak threats, a double- or triple-extortion model that amplifies pressure on victims and increases regulatory exposure. Organizations that lack phishing-resistant authentication, segmented networks, and offline backup strategies face the highest risk of operational disruption and material financial loss.

Technical Analysis

These campaigns share a common attack chain documented across open-source reporting: initial access via phishing (T1566), exploitation of public-facing applications (T1190), or valid account abuse (T1078); credential harvesting using tools such as Mimikatz or similar (T1003); lateral movement over RDP (T1021.001) and SMB (T1021.002); file discovery (T1083); and command execution via scripting interpreters (T1059), frequently paired with living-off-the-land binaries to evade detection. Pre-encryption stages include exfiltration to attacker-controlled infrastructure (T1041, T1567.002). Ransomware detonation (T1486) is followed by inhibition of system recovery (T1490) and service disruption (T1489). Underlying weaknesses map to CWE-287 (improper authentication), CWE-522 (insufficiently protected credentials), CWE-269 (improper privilege management), CWE-494 (download of code without integrity check), and CWE-693 (protection mechanism failure). No single CVE governs this campaign set; specific CVEs exploited vary by actor and incident and require per-incident source review for verification. These actors operate under Ransomware-as-a-Service (RaaS) models, meaning affiliate TTPs may vary from core group patterns. Source data is aggregated from T3 open-source reporting;

technical specifics for individual incidents should be verified against primary vendor or CISA advisories before operational use.

Action Checklist

1. Step 1, Immediate: Enforce phishing-resistant MFA (FIDO2 or certificate-based) on all externally accessible systems, VPN, RDP, and privileged accounts; disable or restrict RDP exposure at the network perimeter where not operationally required.
2. Step 2, Detection: Hunt for unauthorized use of LOLBins (wmic, psexec, certutil, bitsadmin, mshta), abnormal SMB lateral movement, large outbound data transfers, and credential access tool signatures (Mimikatz, LaZagne) in SIEM and EDR telemetry.
3. Step 3, Assessment: Inventory all public-facing applications and confirm patch status against known exploited vulnerabilities tracked in the CISA KEV catalog (cisa.gov/known-exploited-vulnerabilities-catalog); identify accounts with excessive privileges and apply least-privilege remediation.
4. Step 4, Backup and Recovery: Verify that offline or immutable backups exist for all critical systems, test restoration procedures, and confirm backups are isolated from the primary network to prevent ransomware propagation to backup infrastructure.
5. Step 5, Communication: Brief executive leadership and legal counsel on current ransomware exposure, confirm incident response retainer and cyber insurance coverage terms are current, and validate that your IR playbook addresses double-extortion scenarios including data leak notification obligations.
6. Step 6, Long-term: Conduct tabletop exercises simulating ransomware detonation and data exfiltration; review and update network segmentation to limit blast radius; align detection rules to MITRE ATT&CK techniques T1566, T1190, T1078, T1021.001, T1021.002, T1003, T1486, and T1490.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and external IR firm immediately if: (1) phishing-resistant MFA cannot be deployed org-wide within 30 days, (2) CISA KEV critical patches affect >20% of externally exposed systems, (3) offline backups do not exist or restoration testing fails, or (4) ransomware incident is detected in production.
Recovery Notes	Post-containment recovery requires parallel workstreams: (1) forensic evidence preservation and law enforcement notification within 24 hours; (2) isolated restoration of critical systems from offline backups in segregated lab environment with integrity verification before network reconnection; (3) credential rotation for all accounts with access to recovered systems; (4) network segmentation validation to prevent re-infection via lateral movement; (5) 30-day enhanced monitoring post-recovery with SOC alert thresholds lowered and EDR tuning to ATT&CK techniques observed during incident. Root cause analysis (RCA) must identify initial compromise vector (phishing, unpatched app, exposed credential) and remediate within 60 days.

Forensic Artifacts	Windows Event Log Security (Event ID 4688 Process Creation, 4624/4625 Logon, 4648 Explicit Cred Use, 4698 Task Creation, 5140 SMB Share Access, 4659 Handle to Object Deleted) | Windows Event Log System (Event ID 7034 Service Crash, 7035 Service Control) | Sysmon logs (Event ID 1 Process Create, 3 Network Connection, 7 DLL Loaded, 10 CreateRemoteThread, 11 File Created, 12-14 Registry Modified, 21-22 WMI Event) | Zeek/network pcaps (DNS queries for C2 domains, SMB lateral movement, RDP/SSH sessions, HTTP/HTTPS exfil) | Application logs (web server access logs for exploitation attempts, database audit logs for credential access, VPN logs for unauthorized access, email gateway logs for phishing campaigns) | File system artifacts (ransomware note files, encrypted file extensions, $RECYCLE.BIN for deleted files, Volume Shadow Copy (vssadmin list shadows), prefetch files at C:\Windows\Prefetch*.pf for execution history) | Registry hives (HKLM\Software for installed software versions, HKCU\Software\Microsoft\Windows\CurrentVersion\Run for persistence, SAM/SECURITY hives for credential artifacts) | Memory dump (hiberfil.sys, pagefile.sys for malware/credential injection artifacts)

Per-Action IR Details

Step 1, Immediate: Enforce phishing-resistant MFA (FIDO2 or certificate-based) on all externally accessible systems, VPN, RDP, and privileged accounts; disable or restrict RDP exposure at the network perimeter where not operationally required.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation phase); §3.2.1 (containment via access control)

Controls: NIST 800-53 IA-2(1), IA-4, AC-2(1), AC-3, CIS v8 5.3, 6.5

Compensating: If FIDO2 unavailable: enforce certificate-based MFA via Windows Hello for Business or PIV cards on RDP; use OpenSSH key-based auth on *nix systems with `PermitRootLogin no` and `PasswordAuthentication no` in /etc/ssh/sshd_config. For VPN without native MFA: deploy free reverse proxy (Caddy, nginx) with OIDC bridge to free identity provider (Keycloak). Immediately disable RDP on internet-facing systems; if required, firewall to specific IPs only and require jump-host access.

Evidence: Before enforcement: export RDP connection logs from Windows Security Event Log (Event ID 4624, 4625, 4648) for past 90 days to establish baseline of legitimate external access. Capture current MFA configuration state via `Get-MsolUser -All | Select-Object UserPrincipalName, StrongAuthenticationMethods` (Azure/M365) or equivalent IAM export. Document all externally accessible services via port scan (nmap -p 22,3389,443,8443 -oA scan_baseline) and network ACL audit.

Step 2, Detection: Hunt for unauthorized use of LOLBins (wmic, psexec, certutil, bitsadmin, mshta), abnormal SMB lateral movement, large outbound data transfers, and credential access tool signatures (Mimikatz, LaZagne) in SIEM and EDR telemetry.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.2 (analysis phase: event signature analysis); §3.2.3 (containment: stopping attack)

Controls: NIST 800-53 SI-4(1), AU-2(a)(1), AU-12(c), CIS v8 8.2, 8.6, 8.7

Compensating: SIEM unavailable: use Splunk Free (500MB/day) or ELK Stack (open-source); ingest Windows Event Log 4688 (Process Creation) from domain controller via Winlogbeat. Hunt manually via PowerShell: `Get-WinEvent -FilterHashtable @{LogName='Security'; ID=4688; StartTime=(Get-Date).AddDays(-7)} | Where-Object {$_.Properties[5] -match 'wmic|psexec|certutil|bitsadmin|mshta'} | Export-Csv hunt_results.csv`. For SMB lateral movement: analyze Zeek SMB logs or tcpdump pcaps for SMB2_TREE_CONNECT and SMB2_CREATE to unusual shares (C$, IPC$, ADMIN$) via tshark: `tshark -r traffic.pcap -Y 'smb2 and smb2.tree contains ADMIN' -T fields -e ip.src -e ip.dst -e smb2.tree > smb_lateral.txt`. For data exfil: `netstat -abno | grep ESTABLISHED | awk '{print $2, $3}' > established_conns.txt` and correlate against known C2 domains via grep/OSINT.

Evidence: Capture Windows Event Logs 4688 (Process Creation), 4625 (Failed Login), 4648 (Explicit Credential Use), 4698 (Scheduled Task Created), 5140 (SMB share accessed), 3389 RDP logs if available. Preserve Sysmon logs (Event ID 1: Process Create, 3: Network Connection, 7: DLL Loaded) for 7 days prior to discovery. Export DNS query logs from recursive resolver or Zeek DNS logs to identify C2 domain resolution. Capture full process trees via Get-Process with module hashes: `Get-Process | ForEach-Object {Get-FileHash $_.Path -ErrorAction SilentlyContinue} | Export-Csv process_baseline.csv`. Preserve memory artifacts (Windows pagefile, hiberfil.sys) before analysis.

Step 3, Assessment: Inventory all public-facing applications and confirm patch status against known exploited vulnerabilities tracked in the CISA KEV catalog (cisa.gov/known-exploited-vulnerabilities-catalog); identify accounts with excessive privileges and apply least-privilege remediation.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation: tools and resources); NIST 800-53 RA-3(1), CM-2(3), CM-8(1)

Controls: NIST 800-53 SI-2(2), RA-5, CM-5(1), CIS v8 2.2, 6.2, 7.3

Compensating: No vulnerability scanner: use Shodan (free tier), Censys, or ZoomEye to identify externally exposed services. Download CISA KEV CSV (cisa.gov/known-exploited-vulnerabilities) and cross-reference against software inventory via PowerShell: `Get-WmiObject -Class Win32_Product | Select-Object Name, Version > inventory.csv`, then grep against KEV list. For privilege audit without PAM: export AD users via `Get-ADUser -Filter * -Properties memberOf > users_groups.csv` and parse for Domain Admins, Enterprise Admins, Schema Admins. Audit local admin groups on each system: `net localgroup administrators > local_admins.txt`. Use Windows Defender for patch audit: `Get-HotFix | Select-Object HotFixID, InstalledOn > patches.csv`; correlate against CISA KEV for missing critical patches.

Evidence: Before remediation: export current AD group memberships via LDAP query or Powershell; capture local admin group membership on all systems via WMI. Document all public-facing services via firewall rule export, WAF logs, and network device configurations. Take baseline screenshots of running services via `Get-Service | Where-Object {$_.Status -eq 'Running'} > services_baseline.csv`. Preserve application version strings: `wmic product list > installed_apps.csv`. Export patch status via Windows Update history: `Get-HotFix | Export-Csv patches_baseline.csv`. Document current privilege level assignments for all application service accounts and database admins.

Step 4, Backup and Recovery: Verify that offline or immutable backups exist for all critical systems, test restoration procedures, and confirm backups are isolated from the primary network to prevent ransomware propagation to backup infrastructure.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation: recovery tools); §3.4 (Recovery phase); NIST 800-53 CP-9(1), CP-10(2)

Controls: NIST 800-53 CP-6(1), CP-7(1), SC-7(5), CIS v8 3.3, 10.1

Compensating: No enterprise backup appliance: use free/open-source alternatives. Linux: rsync with immutable flag (`rsync -aR --backup-dir=/immutable_backups/$(date +%Y%m%d) /critical /offline_mount/`) and store on external USB (disconnected except during backup window). Windows: robocopy with /MIR and VSS: `robocopy C:\critical \\offline_nas\backups /MIR /DCOPY:DAT /TIMFIX`. Enable immutability via filesystem ACL: `icacls offline_mount /grant:r Everyone:F /inheritance:e` then remove write perms after backup completes. Test restoration quarterly: boot VM from backup snapshot, verify database consistency (DBCC CHECKDB for SQL Server, `mysqlcheck -u root -p` for MySQL), confirm application startup and data integrity. Document RTO/RPO per business unit. Keep 3-month offline backup rotation disconnected from network.

Evidence: Document current backup inventory: which systems, backup frequency, retention period, storage location. Verify immutability: check filesystem mount options (`mount | grep ro`), ACL permissions, and backup appliance retention lock settings. Capture backup metadata: timestamps, size, checksum via `Get-FileHash` or `sha256sum`. Test restoration in isolated lab environment and document results (success/failure, time required, data integrity checks performed). Preserve pre-backup system state snapshots (VM snapshots or disk image checksum) to enable comparative analysis post-recovery. Document network isolation proof: network diagram showing backup infrastructure disconnected from production; firewall rules blocking production-to-backup traffic.

Step 5, Communication: Brief executive leadership and legal counsel on current ransomware exposure, confirm incident response retainer and cyber insurance coverage terms are current, and validate that your IR playbook addresses double-extortion scenarios including data leak notification obligations.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation: roles and responsibilities); §3.1 (Detection and Analysis: communication)

Controls: NIST 800-53 IR-1, IR-4, CA-7, CIS v8 9.1, 9.5

Compensating: No IR retainer: engage flat-fee forensic firm (e.g., Mandiant, Kroll, Stroz Friedberg) in writing with pre-agreed scope, SLA, and escalation path before incident occurs. Create written playbook internally addressing: incident declaration criteria, notification timelines per jurisdiction (HIPAA 60 days, GDPR 72 hours, state AG per breach law), data classification for leak risk assessment, decision matrix for ransom payment (legal counsel input), insurance claim process, and law enforcement notification trigger. Validate cyber insurance policy in writing: confirm ransomware coverage, coverage limits, deductible, requirement for law enforcement reporting, 3rd-party forensics provider restrictions, and ransom negotiation coverage if applicable. Document business continuity contacts: C-suite, board, legal, privacy officer, insurance broker, law enforcement (FBI/Secret Service).

Evidence: Preserve copy of current IR retainer agreement and insurance policy in accessible location (not on IT network). Document communication plan with timestamps showing legal/executive sign-off. Capture current cyber insurance declarations and policy limits. Maintain written attestation that playbook was reviewed by legal counsel and covers ransomware + double-extortion scenarios. Document incident commander designation and escalation authority.

Step 6, Long-term: Conduct tabletop exercises simulating ransomware detonation and data exfiltration; review and update network segmentation to limit blast radius; align detection rules to MITRE ATT&CK techniques T1566, T1190, T1078, T1021.001, T1021.002, T1003, T1486, and T1490.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §3.5 (Post-incident activities); NIST 800-53 IR-3(2), SI-12(1), CA-7(1)

Controls: NIST 800-53 AU-1(b), IR-4(2), SI-4(2), CIS v8 1.3, 4.1, 8.5

Compensating: Tabletop: use NIST Cybersecurity Framework worksheets (free, ncsc.gov) or SANS incident handling posters as scenario templates. Conduct annual 4-hour exercise with representatives from IT, security, legal, finance, communications; document assumptions, decisions, timelines, and gaps. Network segmentation without SDN: use VLAN trunking and firewall ACLs to isolate critical systems (healthcare databases, finance, manufacturing control systems) on separate subnets; deny lateral movement by default (implicit deny all inter-VLAN traffic). Detection rules: map each ATT&CK technique to Windows Event Log signature: T1566 (phishing) → 4688 (PowerShell w/ suspicious cmdlets), T1190 (exploit) → 4688 + 4720 (new local account), T1078 (valid creds) → 4625 repeated failures, T1021.001 (RDP) → Event 4624 (Logon Type 10), T1021.002 (SMB) → 5140 + unusual share, T1003 (credential dump) → Sysmon Event 10 (CreateRemoteThread on lsass.exe), T1486 (encryption) → file activity spikes in %TEMP% + bulk file extension change, T1490 (backup deletion) → 4688 (vssadmin delete shadows) or 4659 (backup deletion events).

Evidence: Document tabletop exercise results: scenario narrative, timeline of simulated decisions, identified gaps, assigned remediation owners and dates. Preserve network segmentation baseline: current firewall rules, VLAN assignments, access control list audit. Capture baseline detection rule tuples: SIEM query logic for each ATT&CK technique, false positive rate, alert volume. Create detection engineering backlog with rule tuning priorities. Document any manual detection procedures for low-signal techniques (file extension enumeration, backup system audit).

Detection Guidance

Focus detection on pre-ransomware behaviors rather than detonation events, as encryption typically occurs after attacker objectives are already met. Key behavioral indicators: (1) Credential access, process creation events showing lsass.exe memory access, or execution of known credential dumping tools; correlate with SIEM alerts on Event ID 4624 (logon) followed by rapid lateral movement. (2) Lateral movement, Event ID 4648

(explicit credential logon) combined with SMB connections to multiple hosts in a short window; RDP sessions originating from non-standard workstations or outside business hours. (3) Discovery activity, rapid sequential execution of net.exe, whoami, ipconfig, nltest, or BloodHound-style LDAP queries against Active Directory. (4) Exfiltration, large outbound transfers to cloud storage services (Mega, rclone targets) or anomalous external IPs; monitor for rclone.exe or similar sync tool execution (T1567.002). (5) Impact precursors, deletion of Volume Shadow Copies via vssadmin.exe or wmic shadowcopy delete (T1490); modification or stopping of backup and AV services (T1489). MITRE ATT&CK Navigator layers for LockBit, ALPHV/BlackCat, Cl0p, Black Basta, and Rhysida are available at attack.mitre.org and should be used to tune detection rules to each group's documented TTP set. No campaign-wide IOCs are provided here; per-incident IOCs require direct review of source reporting and vendor threat intelligence feeds, as indicators change frequently and aged IOCs carry high false-positive risk.

Indicators of Compromise

Type	Value	Context	Confidence
NOTE	`No verified campaign-wide IOCs available`	IOCs for these campaigns are actor- and incident-specific. They change frequently across RaaS affiliates and degrade rapidly. Consult current vendor threat intelligence feeds, ISAC advisories, and CISA alerts for verified, time-stamped indicators before operational use. Publishing aged or unverified IOCs increases false-positive rates and operational noise.	LOW

Framework Mappings

MITRE-ATTACK

- **T1021.001** — Remote Desktop Protocol
- **T1567.002** — Exfiltration to Cloud Storage
- **T1059** — Command and Scripting Interpreter
- **T1003** — OS Credential Dumping
- **T1078** — Valid Accounts
- **T1083** — File and Directory Discovery
- **T1489** — Service Stop
- **T1566** — Phishing
- **T1190** — Exploit Public-Facing Application
- **T1021.002** — SMB/Windows Admin Shares
- **T1486** — Data Encrypted for Impact
- **T1041** — Exfiltration Over C2 Channel
- **T1490** — Inhibit System Recovery

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
- **IA-5** — Authenticator Management
- **AC-2** — Account Management
- **IA-2** — Identification and Authentication (Organizational Users)
- **CM-6** — Configuration Settings
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-8** — Spam Protection
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **CM-3** — Configuration Change Control
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **IR-4** — Incident Handling
- **SC-13** — Cryptographic Protection

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control
- **A04:2021** — Insecure Design
- **A07:2021** — Identification and Authentication Failures
- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **5.4**
- **6.8**
- **5.2**
- **2.5**
- **2.6**
- **6.3**
- **6.4**
- **6.5**
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

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

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

NIST-CSF-2

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

ISO-27001-2022

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1021.001	Remote Desktop Protocol	Lateral-Movement
T1567.002	Exfiltration to Cloud Storage	Exfiltration
T1059	Command and Scripting Interpreter	Execution
T1003	OS Credential Dumping	Credential-Access
T1078	Valid Accounts	Defense-Evasion
T1083	File and Directory Discovery	Discovery
T1489	Service Stop	Impact
T1566	Phishing	Initial-Access
T1190	Exploit Public-Facing Application	Initial-Access
T1021.002	SMB/Windows Admin Shares	Lateral-Movement
T1486	Data Encrypted for Impact	Impact
T1041	Exfiltration Over C2 Channel	Exfiltration

Technique ID	Technique Name	Tactic
T1490	Inhibit System Recovery	Impact

Sources

Source	URL	Tier
Cybersecurityventures	https://cybersecurityventures.com/top-10-ransomware-attacks-over-th...	T3
26 Ransomware Examples Explained in 2026 - SentinelOne	https://www.sentinelone.com/cybersecurity-101/cybersecurity/ransomw...	T3
Dec 2025: Biggest Cyber Attacks, Ransomware Attacks and Data ...	https://www.cm-alliance.com/cybersecurity-blog/dec-2025-biggest-cyb...	T3
10 Ransomware Examples from Recent High-Impact Attacks	https://securityscorecard.com/blog/10-examples-of-recent-and-impact...	T3
Data Breaches 2025: Biggest Cybersecurity Incidents So Far	https://www.pkware.com/blog/recent-data-breaches	T3

Generated 2026-03-29 18:38 UTC by TJS Security Command Center