INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-12 14:15 UTC

Check Point Reports 48% Year-Over-Year Surge in Global Ransomware Attacks, May 2026

THREAT CAMPAIGN | HIGH

SCC Item ID	SCC-CAM-2026-0446
Type	Threat Campaign
Severity	HIGH
Affected Products	Global businesses across Business Services, Consumer Goods, Industrial Manufacturing, Agriculture, Hospitality, Travel, Recreation, and Construction sectors
Published	2026-06-12
Discovery Source	Gemini

Executive Summary

Check Point Research documented a 48% year-over-year increase in global ransomware attacks during May 2026, the sharpest growth rate recorded in 2026 to date, with 61 active threat groups operating simultaneously. Business Services is the most heavily targeted sector, followed by Consumer Goods and Industrial Manufacturing. Organizations across these verticals face elevated risk of operational shutdown, data extortion, and supply chain disruption as the threat landscape grows more fragmented and competitive among ransomware operators.

Technical Analysis

Check Point Research identified a 48% year-over-year surge in ransomware attack volume for May 2026, characterizing the landscape as highly fragmented across 61 active groups. Qilin ransomware was the most active operator during the period. No single CVE is attributed to this campaign; attack chains leverage multiple initial access vectors including external remote services (T1133), phishing (T1566), exploitation of public-facing applications (T1190), and valid account abuse (T1078). Post-access techniques include data encryption (T1486), service disruption (T1489), and backup/recovery inhibition (T1490). Source data is secondary-tier (Check Point Research summary via Gemini relay); sub-sector breakdowns and Qilin-specific IOCs from the original report were not directly verified at time of publication. No CVSS score applies to this campaign-level item.

Action Checklist

1. Step 1: Containment, Audit all external-facing remote access points (VPN, RDP, SSH) and enforce allowlisting; disable unused external services immediately per NIST AC-17 (Remote Access) and CIS 4.4 (Implement and Manage a Firewall on Servers). Prioritize Business Services, Consumer Goods, and Industrial Manufacturing environments.
2. Step 2: Detection, Enable and centralize audit logging across all enterprise assets per CIS 8.2 (Collect Audit Logs) and NIST AU-2 (Event Logging). Hunt for anomalous authentication events (T1078), lateral movement following external login, mass file rename or encryption activity (T1486), and service termination activity (T1489). Query EDR/SIEM for process creation events targeting vssadmin.exe, wbadmin.exe, or bcdedit.exe with deletion or disable arguments (T1490), and for processes terminating backup agents or security services.
3. Step 3: Eradication, Rotate all privileged credentials and service account passwords per NIST AC-2 (Account Management) and D3-CRO (Credential Rotation). Enforce MFA on all remote access and administrative interfaces per CIS 6.4 (Require MFA for Remote Network Access) and CIS 6.5 (Require MFA for Administrative Access). Patch all internet-facing systems, prioritizing known exploitable services per CIS 7.3 (Perform Automated Operating System Patch Management).
4. Step 4: Recovery, Validate backup integrity offline before restoration; confirm backup processes were not targeted by T1490 activity. Restore from clean, verified snapshots. Monitor post-recovery for re-infection indicators including unexpected outbound connections and re-emergence of encryption processes. Confirm logging is active per NIST AU-12 (Audit Record Generation) before returning systems to production.
5. Step 5: Post-Incident, Conduct a tabletop exercise against a Qilin-style ransomware scenario. Map control gaps to NIST IR controls and CIS 7.1 (Establish and Maintain a Vulnerability Management Process). Review separation of duties (NIST AC-5) for backup administrators to prevent single points of compromise. Document findings and update incident response playbooks to address fragmented multi-group threat environments.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to senior IR leadership and legal/compliance counsel if any of the following are confirmed: evidence of data exfiltration preceding encryption (indicating double-extortion and triggering breach notification obligations), encryption activity detected on OT/ICS-adjacent systems in Industrial Manufacturing environments (operational safety risk), compromise of backup infrastructure rendering recovery impossible without negotiation, or identification of a threat actor TTP set consistent with a nation-state-affiliated group among the 61 active ransomware operators documented in this campaign.

Recovery Notes	Before returning any system to production, verify that all persistence mechanisms identified during eradication (scheduled tasks, rogue services, registry Run keys, WMI subscriptions) have been removed and their absence confirmed against a known-good baseline — ransomware groups in this 61-actor landscape routinely stage secondary implants designed to survive a first-pass reimaging. Maintain elevated monitoring (Sysmon Event ID 1, 3, and 11 at full verbosity; firewall deny logs reviewed daily) for a minimum of 30 days post-recovery, as re-infection within 30 days is a documented pattern when initial access vectors (unpatched VPN, exposed RDP) are not fully remediated. For Business Services and Industrial Manufacturing organizations, validate that supply chain partners and managed service providers connected to the environment have confirmed their own clean bill of health before re-establishing any inter-organizational connectivity.
Forensic Artifacts	Windows Security Event Log: Event IDs 4624 (Logon Type 10 — RemoteInteractive for RDP), 4648 (Explicit Credential Use), 4732 (Local Admin Group Membership Change), and 7045 (New Service Installed) — collectively document the ransomware actor's initial access via exposed RDP/VPN, lateral movement using harvested credentials, and persistence installation sequence typical of groups operating in this campaign. | Volume Shadow Copy service state and vssadmin.exe execution history: captured via Sysmon Event ID 1 (Process Create) filtering on 'vssadmin delete shadows' or 'wmic shadowcopy delete' command lines — VSS deletion is a near-universal pre-encryption step across the ransomware groups active in this May 2026 surge and timestamps this artifact to within minutes of encryption detonation. | Filesystem metadata (MFT — Master File Table on NTFS): extract using 'mftdump' or Autopsy to identify mass file rename/extension-change events; ransomware encryption produces a characteristic MFT modification timestamp burst (hundreds to thousands of entries within a 1-5 minute window) that pinpoints detonation time and scope of encrypted files. | Outbound network flow logs (firewall NetFlow or Windows Firewall logs): review for large-volume transfers to Mega.nz, rclone command-and-control IPs, or Tor exit nodes in the 24-72 hours preceding encryption — double-extortion exfiltration, increasingly common among the fragmented 61-group threat landscape documented by Check Point, leaves a distinctive high-throughput outbound flow signature on ports 443 and 80 to non-business destinations. | Scheduled Tasks and WMI Subscriptions: export 'schtasks /query /fo CSV /v' output and query WMI persistence via 'Get-WMIObject -Namespace root\subscription -Class __EventFilter' — ransomware actors frequently install scheduled tasks or WMI subscriptions as secondary persistence to survive credential rotation or partial remediation, and these artifacts survive system reboots, making them critical to identify before any recovery restoration is declared complete.

Per-Action IR Details

Step 1: Containment — Audit all external-facing remote access points (VPN, RDP, SSH) and enforce allowlisting; disable unused external services immediately per NIST AC-17 (Remote Access) and CIS 4.4 (Implement and Manage a Firewall on Servers). Prioritize Business Services, Consumer Goods, and Industrial Manufacturing environments.

NIST Phase: Containment

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

Controls: NIST AC-17 (Remote Access), NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Run 'netstat -ano' (Windows) or 'ss -tulnp' (Linux) on all perimeter hosts to enumerate listening services; cross-reference against expected service list. Use Windows Firewall with Advanced Security (wf.msc) to create inbound block rules for RDP (3389) and non-approved SSH (22) sources. For VPN audit, pull active session logs from the VPN concentrator's local syslog export and flag sessions originating outside approved IP ranges. A

2-person team can script this with PowerShell 'Get-NetFirewallRule' and a CSV allowlist diff.

Evidence: BEFORE disabling or blocking any remote access service, capture volatile state: run 'Get-NetTCPConnection | Where-Object State -eq Established' (PowerShell) or 'netstat -ano' and record all active sessions with PIDs; capture 'qwinsta /server:localhost' output to enumerate active RDP sessions; export VPN active session table from concentrator admin console; acquire Windows Security Event Log filtering for Event ID 4624 (Successful Logon) with Logon Type 10 (RemoteInteractive) and Type 3 (Network) from the preceding 72 hours to baseline active remote access accounts before lockdown. Ransomware actors exploiting RDP and VPN in this campaign frequently establish persistence before deploying the encryptor — evicting sessions without capturing this data destroys attribution.

Step 2: Detection — Enable and centralize audit logging across all enterprise assets per CIS 8.2 (Collect Audit Logs) and NIST AU-2 (Event Logging). Hunt for anomalous authentication events (T1078), lateral movement following external login, mass file rename or encryption activity (T1486), and Volume Shadow Copy deletion (T1490). Query EDR/SIEM for processes terminating backup agents or security services (T1489).

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), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with SwiftOnSecurity config (sysmonconfig-export.xml) to capture Event ID 1 (Process Create), Event ID 3 (Network Connect), and Event ID 11 (File Create) — the trifecta for detecting ransomware staging. Hunt VSS deletion with: 'Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4688} | Where-Object {$_.Message -match "vssadmin|wmic.*shadowcopy"}'. For mass file rename activity (encryption in progress), use Sysmon Event ID 11 filtered on extensions '.locked', '.enc', '.qilin', or any high-frequency rename burst (>100 renames/minute on a single process). Use Sigma rule 'proc_creation_win_vssadmin_delete_shadows.yml' (available at github.com/SigmaHQ/sigma) against Windows Event Logs with Chainsaw or Hayabusa if no SIEM is available.

Evidence: This is a detection/analysis step that does not alter live system state; however, if discovery reveals an active encryption process on any host, treat that host as a live compromise and immediately capture RAM (using WinPmem or DumpIt), active process list ('tasklist /v /fo csv'), network connections ('Get-NetTCPConnection'), and running service state ('sc query type= all state= all') BEFORE any containment action. Key detection artifacts specific to ransomware campaigns operating in May 2026 surge context: Windows Security Event Log Event ID 4732 (member added to local admins group), Event ID 4648 (explicit credential use), and Event ID 7045 (new service installed) — the latter frequently used by groups like Qilin for persistence prior to detonation.

Step 3: Eradication — Rotate all privileged credentials and service account passwords per NIST AC-2 (Account Management) and D3-CRO (Credential Rotation). Enforce MFA on all remote access and administrative interfaces per CIS 6.4 (Require MFA for Remote Network Access) and CIS 6.5 (Require MFA for Administrative Access). Patch all internet-facing systems, prioritizing known exploitable services per CIS 7.3 (Perform Automated Operating System Patch Management).

NIST Phase: Eradication

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

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Before rotating credentials, document all service accounts and their dependencies using 'Get-ADServiceAccount -Filter *' and 'Get-WmiObject Win32_Service | Select Name, StartName' to prevent service outages post-rotation. For MFA enforcement without enterprise tooling, implement Windows Hello for Business or enable Azure AD Conditional Access free tier for externally exposed apps. For credential rotation, use 'net user /domain' for domain accounts and script bulk rotation via PowerShell 'Set-ADAccountPassword'. Force KRBTGT account rotation twice (48 hours apart) if domain compromise is suspected, per Microsoft guidance on Golden Ticket invalidation.

Evidence: BEFORE rotating any credential or applying any patch, capture the following volatile state on potentially compromised systems: memory dump (WinPmem) to preserve any injected credential material or in-memory implants; export LSASS process memory artifact list (do NOT dump LSASS directly without EDR safeguards — use task manager protected process approach or a signed tool); capture 'reg query HKLM\SYSTEM\CurrentControlSet\Services' to document all registered services; export scheduled tasks ('schtasks /query /fo CSV /v > tasks_pre_rotation.csv') since ransomware groups operating in this 61-group fragmented landscape frequently install scheduled tasks as persistence mechanisms before credential rotation would evict them. Patch action must be preceded by snapshot of current patch state: 'Get-HotFix | Sort-Object InstalledOn -Descending' for Windows, 'rpm -qa --last' or 'dpkg -l' for Linux.

Step 4: Recovery — Validate backup integrity offline before restoration; confirm backup processes were not targeted by T1490 activity. Restore from clean, verified snapshots. Monitor post-recovery for re-infection indicators including unexpected outbound connections and re-emergence of encryption processes. Confirm logging is active per NIST AU-12 (Audit Record Generation) before returning systems to production.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-12 (Audit Record Generation), NIST AU-9 (Protection Of Audit Information), CIS 8.2 (Collect Audit Logs), CIS 3.4 (Enforce Data Retention)

Compensating: Validate backup integrity offline using hash verification: compute SHA-256 checksums on backup archives using 'certutil -hashfile SHA256' (Windows) or 'sha256sum' (Linux) and compare against checksums recorded at backup creation time. To confirm backups were not encrypted by ransomware, mount backup volumes in a sandboxed VM (not connected to production network) and verify file headers of critical data types using a hex editor or 'file' command (Linux) — ransomware-encrypted files will show randomized headers rather than expected magic bytes (e.g., PDF should start with '%PDF-'). For post-recovery monitoring, configure Sysmon Event ID 3 (Network Connect) alerts on any restored host for outbound connections to non-approved IPs, and watch for re-emergence of mass Sysmon Event ID 11 activity indicating re-encryption.

Evidence: Before restoring any system to production, confirm that VSS deletion activity (vssadmin.exe or wmic shadowcopy delete command lines visible in pre-incident Sysmon Event ID 1 logs) has been scoped — determine whether the attacker deleted backups only or also exfiltrated data before encrypting, as the 61 active groups in this campaign increasingly use double-extortion. Check outbound traffic logs (firewall or NetFlow exports) from the 72-hour window before encryption detonation for large-volume transfers to cloud storage endpoints (Mega.nz, rclone-associated IPs) or unusual ports. Confirm that restored systems do not carry dormant implants: run ClamAV with updated signatures against the restored filesystem before connecting to production network, and verify startup registry keys ('reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run') match a known-good baseline.

Step 5: Post-Incident — Conduct a tabletop exercise against a Qilin-style ransomware scenario. Map control gaps to NIST IR controls and CIS 7.1 (Establish and Maintain a Vulnerability Management Process). Review separation of duties (NIST AC-5) for backup administrators to prevent single points of compromise. Document findings and update incident response playbooks to address fragmented multi-group threat environments.

NIST Phase: Post Incident

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

Controls: NIST AC-5 (Separation Of Duties), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For teams without a dedicated tabletop facilitator, use the CISA Tabletop Exercise Packages (CTEPs) available at cisa.gov — the ransomware-specific CTEP includes inject scenarios directly applicable to multi-group campaigns. Document control gaps using a simple NIST CSF 2.0 gap spreadsheet: list each IR and AC control from this incident, score current vs. target maturity (1-4), and assign owners. For backup admin separation of duties with a small team, implement a 'two-person rule' operationally: require a second team member to approve and observe any backup deletion or schedule modification, logged via a shared ticketing system (even a free Jira or GitHub Issues board).

Evidence: Post-incident, preserve all forensic artifacts and IR timeline documentation for a minimum of 12 months to support potential law enforcement referral (FBI IC3) and regulatory notification requirements — the Business Services and Consumer Goods sectors targeted in this campaign frequently handle PII subject to state breach notification laws (e.g., CCPA, various US state statutes) and potentially HIPAA if healthcare-adjacent. Retain: full disk images of compromised hosts, all collected memory dumps, exported SIEM/event log archives, firewall and VPN session logs covering the incident window, and the complete chain-of-custody documentation for each artifact. These are not volatile at this phase but must be write-protected (use a hardware write blocker or forensic copy stored on WORM media or immutable cloud storage) before the post-incident review begins.

Detection Guidance

Hunt for the following behavioral indicators across SIEM, EDR, and network telemetry. For T1133 (External Remote Services): anomalous VPN or RDP authentication from new geolocations or outside business hours. For T1078 (Valid Accounts): logins from accounts not recently active, privilege escalation shortly after authentication, or accounts accessing systems outside their normal scope, correlate against NIST AC-2 baselines. For T1566 (Phishing): email gateway logs showing high-volume delivery of password-protected archives or macro-enabled documents to Business Services or Manufacturing staff. For T1486 (Data Encrypted for Impact): EDR alerts on mass file extension changes, high-volume file I/O from a single process, or ransomware note creation. For T1490 (Inhibit System Recovery): process creation events targeting vssadmin.exe, wbadmin.exe, or bcdedit.exe with deletion or disable arguments. For T1489 (Service Stop): service control manager events (Windows Event ID 7036, 7040) showing backup agents, AV, or EDR services being stopped. No confirmed public Qilin IOCs are included in the source data; monitor Check Point Research and MITRE ATT&CK Group pages for updated indicators as they are published.

Framework Mappings

MITRE-ATTACK

- **T1133** — External Remote Services
- **T1486** — Data Encrypted for Impact
- **T1489** — Service Stop
- **T1566** — Phishing
- **T1490** — Inhibit System Recovery
- **T1190** — Exploit Public-Facing Application
- **T1078** — Valid Accounts

NIST-800-53R5

- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SC-7** — Boundary Protection
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution

- **CM-6** — Configuration Settings
- **SI-4** — System Monitoring
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SI-3** — Malicious Code Protection
- **SI-8** — Spam Protection
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IR-4** — Incident Handling

NIST-CSF-2

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

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan

ISO-27001-2022

- **A.5.29** — Information security during disruption

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1133	External Remote Services	Persistence
T1486	Data Encrypted for Impact	Impact
T1489	Service Stop	Impact
T1566	Phishing	Initial-Access
T1490	Inhibit System Recovery	Impact
T1190	Exploit Public-Facing Application	Initial-Access
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
Industries in Alphabetical Order : U.S. Bureau of Labor Statistics	https://www.bls.gov/iag/tgs/iag_index_alpha.htm	T1
Industry Research Reports for United States - IBISWorld	https://www.ibisworld.com/united-states/list-of-industries/	T3
Retail and consumer services – UNEP FI Human Rights Toolkit	https://www.unepfi.org/humanrightstoolkit/retail-and-consumer-servi...	T3
Glossary of Industries - Crunchbase | Knowledge Center	https://support.crunchbase.com/hc/en-us/articles/27690673553555-Glo...	T3
[PDF] International Standard Industrial Classification of All Economic ...	https://unstats.un.org/unsd/publication/seriesm/seriesm_4rev4e.pdf	T3

Generated 2026-06-12 14:15 UTC by TJS Security Command Center