INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-25 06:49 UTC

Qilin Ransomware Group Dominance and Emerging Threats: Q2 2026 Trend Intelligence

THREAT CAMPAIGN | HIGH

SCC Item ID	SCC-CAM-2026-0218
Type	Threat Campaign
Severity	HIGH
Affected Products	Various industries globally including critical infrastructure, healthcare, manufacturing, and SLSH (Small/Large/Small-to-Medium/High-value) enterprises; multiple geographic regions
Published	2026-04-24
Discovery Source	Gemini

Executive Summary

Qilin ransomware, a prolific ransomware-as-a-service operation also tracked as Agenda, has conducted over 700 attacks across critical infrastructure, healthcare, manufacturing, and enterprise sectors and accelerated activity following the collapse of RansomHub in early 2026. The group combines data encryption with data theft and threatened public disclosure, meaning a successful attack carries dual exposure: operational shutdown and regulatory breach notification obligations. Organizations in targeted sectors face elevated risk of business disruption, data loss, and reputational harm with limited warning time given Qilin's demonstrated speed of execution.

Technical Analysis

Qilin (Agenda) operates as a RaaS platform written in Go and Rust, enabling affiliates to deploy cross-platform payloads targeting Windows, Linux, and VMware ESXi environments. No CVE identifier applies to this campaign item; the threat is actor-driven, not vulnerability-specific in the traditional sense. Confirmed MITRE ATT&CK techniques include: T1078 (Valid Accounts, credential abuse for initial access), T1059 (Command and Scripting Interpreter, payload execution), T1083 (File and Directory Discovery, pre-encryption enumeration), T1041 and T1567.002 (Exfiltration over C2 and to cloud storage, double extortion data staging), T1489 (Service Stop, disabling backup and security services pre-encryption), T1490 (Inhibit System Recovery, shadow copy deletion, backup tampering), and T1486 (Data Encrypted for Impact, ransomware execution). Qilin affiliates are reported to abuse valid credentials obtained through phishing and credential markets for initial access, followed by lateral movement and privilege escalation before detonating payloads. ESXi targeting is particularly significant for organizations running virtualized infrastructure, as a single payload can encrypt multiple guest VMs simultaneously. Secondary actors Payload and The_Gentleman were identified in Q2 2026 trend reporting;

technical details for these groups are not independently verified against primary authoritative sources and should be treated as low-confidence at this time. Source quality for this item is moderate (score 0.56); primary sources are vendor research (Check Point, Picus Security) and industry tracking blogs. No campaign-specific IOCs, CVSS scores, or attribution artifacts were available in the source dataset and none are fabricated here.

Action Checklist

1. Containment: Audit privileged account usage immediately - review VPN, RDP, and remote access logs for anomalous authentication (T1078). Isolate any systems showing unexpected service termination or volume shadow copy deletion activity. Prioritize ESXi hosts and backup infrastructure, which are high-value Qilin targets.
2. Detection: Deploy or validate detection rules for shadow copy deletion (vssadmin delete shadows, wmic shadowcopy delete), service stop commands targeting backup and AV processes, large outbound data transfers to cloud storage endpoints (T1567.002), and scripting interpreter abuse (PowerShell, cmd) executing from unusual parent processes (T1059). Query EDR telemetry for T1489 and T1490 indicators. Check Point and Picus Security have published Qilin-specific TTP breakdowns that can inform rule development.
3. Eradication: Enforce phishing-resistant MFA on all remote access and privileged accounts to reduce valid credential abuse (T1078). Restrict scripting interpreter execution via application control policies. Segment backup infrastructure from production networks and enforce immutable backup configurations. Remove any identified persistence mechanisms before recovery.
4. Recovery: Validate backup integrity before restoring from any backup set - Qilin affiliates specifically target backup systems. Restore from offline or immutable backups only. After restoration, rotate all privileged credentials, audit Active Directory for unauthorized accounts or group membership changes, and monitor for reinfection indicators for a minimum of 30 days.
5. Post-Incident: Conduct a gap assessment against NIST CSF PR.AC (Access Control) and RS.MI (Mitigation) controls. Review incident against CIS Benchmark hardening for ESXi and Windows Server environments. Evaluate whether phishing-resistant MFA is enforced across all remote access paths - credential abuse is the dominant initial access vector for this group. Document findings for regulatory notification assessment if data exfiltration occurred.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to executive leadership, legal counsel, and your sector ISAC if: ESXi hosts or backup infrastructure show confirmed encryption or shadow copy deletion (indicating ransomware detonation is in progress or complete), network flow analysis reveals exfiltration volumes consistent with data theft triggering breach notification obligations under HIPAA, GDPR, or applicable state law, or credential telemetry indicates Qilin affiliates retain active access to domain administrator or backup administrator accounts.

Recovery Notes	Restore only from offline or immutable backups verified with pre-incident checksums — Qilin affiliates specifically enumerate and encrypt or corrupt online backup repositories before deploying the ransomware payload, making unverified backup sets unreliable. After restoration, maintain heightened monitoring for T1078 (Valid Accounts), T1490 (Inhibit System Recovery), and T1567.002 (Exfiltration to Cloud Storage) indicators for a minimum of 30 days, as Qilin affiliates have been observed re-entering environments through retained credentials or unremoved persistence mechanisms. Rotate all privileged credentials — including service accounts used by backup agents, RMM tools, and ESXi management interfaces — before reconnecting restored systems to production networks.
Forensic Artifacts	Windows Security Event Log — Event IDs 4624/4625/4648 from VPN concentrators and RDP gateways, establishing the initial valid credential abuse entry point and lateral movement pattern specific to Qilin's T1078 initial access technique | ESXi host logs at /var/log/hostd.log, /var/log/shell.log, and /var/log/vpxa.log — capturing VM power-off commands, snapshot deletion, and VMDK file access patterns left by Qilin's Linux/ESXi encryptor variant targeting virtual infrastructure | Volume Shadow Copy enumeration output (vssadmin list shadows captured before remediation) and Windows System Event Log Event ID 7036 bulk service-stop entries — direct forensic indicators of Qilin's pre-encryption defense evasion routine (T1490, T1489) | Network flow records (NetFlow/IPFIX) or proxy logs showing high-volume outbound transfers to rclone-compatible cloud storage endpoints (Google Cloud Storage, AWS S3, MEGA) in the hours preceding encryption, supporting exfiltration timeline reconstruction for regulatory breach notification | Active Directory replication metadata and NTDS.dit snapshot capturing unauthorized account creation or privileged group membership changes made by Qilin affiliates to establish persistence, recoverable via Get-ADReplicationAttributeMetadata or offline NTDS analysis with DSInternals

Per-Action IR Details

Containment — Audit privileged account usage immediately: review VPN, RDP, and remote access logs for anomalous authentication (T1078). Isolate any systems showing unexpected service termination or volume shadow copy deletion activity. Prioritize ESXi hosts and backup infrastructure, which are high-value Qilin targets.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST SI-4 (System Monitoring), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: For teams without EDR: enable Windows Security Event Log auditing and collect Event ID 4624 (successful logon), 4625 (failed logon), and 4648 (explicit credential use) filtered on Logon Type 3 (network) and Type 10 (remote interactive) — run `Get-WinEvent -LogName Security | Where-Object {$_.Id -in 4624,4625,4648}` via PowerShell. On ESXi hosts, review `/var/log/auth.log` and `/var/log/shell.log` for root or service account activity outside maintenance windows. Deploy Sysmon with a community config (SwiftOnSecurity baseline) to capture process creation and network connection events on Windows hosts. Immediately disable or reset passwords for any accounts showing anomalous RDP or VPN authentication before isolating suspect systems.

Evidence: Before isolating any system, capture: Windows Security Event Log entries for Event IDs 4624/4625/4648 showing lateral movement from the suspected initial access point; VPN gateway authentication logs timestamped against the earliest known anomaly; ESXi host logs at `/var/log/hostd.log` and `/var/log/vpxa.log` for unexpected VM power-off or snapshot deletion commands; Windows Event ID 7036 (Service Control Manager) and 7045 entries showing Qilin-characteristic service termination of backup agents (e.g., Veeam, Backup Exec) and AV processes; Volume Shadow Copy state via `vssadmin list shadows` output captured before any remediation — Qilin affiliates execute `vssadmin delete shadows /all /quiet` and `wmic shadowcopy delete` as a pre-encryption step, so absence of shadows on an active system is itself a forensic indicator.

Detection — Deploy or validate detection rules for: shadow copy deletion (vssadmin delete shadows, wmic shadowcopy delete), service stop commands targeting backup and AV processes, large outbound data transfers to cloud storage endpoints (T1567.002), and scripting interpreter abuse (PowerShell, cmd) executing from unusual parent processes (T1059). Query EDR telemetry for T1489 and T1490 indicators. Check Point and Picus Security have published Qilin-specific TTP breakdowns that can inform rule development — links in source data.

NIST Phase: Detection Analysis

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

Controls: NIST SI-4 (System Monitoring), NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without a SIEM, use these targeted queries and rules: (1) Sysmon Event ID 1 (Process Creation) — filter on `CommandLine` containing `vssadmin*delete*shadows` or `wmic*shadowcopy*delete` and parent processes `services.exe` or `cmd.exe` spawned from unexpected parents; (2) Sysmon Event ID 3 (Network Connection) — filter on large outbound connections to known cloud storage FQDNs (rclone common targets: `storage.googleapis.com`, `s3.amazonaws.com`, `api.mega.io`) — Qilin affiliates are documented using rclone for exfiltration (T1567.002); (3) Deploy the public Sigma rule `win_process_creation_shadowcopy_deletion.yml` (available in the SigmaHQ repository) and convert to native Windows Event Log queries using `sigma convert`; (4) Run `Get-WinEvent -LogName System | Where-Object {$_.Id -eq 7036 -and $_.Message -match 'stopped'}` to identify bulk service termination consistent with Qilin's pre-encryption service-kill routine targeting Veeam, SQL Server, and endpoint protection services.

Evidence: Capture before or concurrent with rule deployment: Sysmon Event ID 1 logs showing PowerShell or cmd.exe launched with encoded command strings (`-EncodedCommand` flag) from parent processes consistent with Qilin's Go-based ransomware loader; Windows Event ID 4688 (Process Creation, with command-line auditing enabled) for `net stop` commands executed in rapid succession against backup and AV service names; Firewall or proxy logs showing high-volume outbound transfers to rclone-compatible endpoints in the hours preceding encryption — Qilin's dual-extortion model requires successful exfiltration before payload deployment; ESXi `/var/log/shell.log` entries showing execution of `esxcli` or direct `vim-cmd` commands to power off or snapshot VMs, consistent with Qilin's Linux/ESXi encryptor variant targeting virtualized infrastructure.

Eradication — Enforce phishing-resistant MFA on all remote access and privileged accounts to reduce valid credential abuse (T1078). Restrict scripting interpreter execution via application control policies. Segment backup infrastructure from production networks and enforce immutable backup configurations. Remove any identified persistence mechanisms before recovery.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST CM-7 (Least Functionality), NIST SI-2 (Flaw Remediation), NIST SC-7 (Boundary Protection), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Without commercial application control: (1) Use Windows Software Restriction Policies (SRP) or AppLocker (available in Windows Server 2008 R2+ without additional licensing) to block PowerShell and cmd.exe execution from `%APPDATA%`, `%TEMP%`, and `%ProgramData%` paths — Qilin affiliates stage and execute scripts from these locations; (2) Enable PowerShell Constrained Language Mode via Group Policy (`__PSLockdownPolicy` registry key set to `4`) to prevent unrestricted script execution; (3) Network-segment backup servers using host-based Windows Firewall rules — block all inbound SMB (445) and RDP (3389) to backup hosts except from dedicated management IPs using `netsh advfirewall firewall add rule`; (4) For Linux backup systems, enforce immutability on backup directories with `chattr +i` on critical backup volumes and verify with `lsattr`; (5) Audit and remove scheduled tasks created by Qilin persistence (`Get-ScheduledTask | Where-Object {$_.TaskPath -notlike '\Microsoft\*'}`) and registry Run keys (`HKCU\Software\Microsoft\Windows\CurrentVersion\Run`).

Evidence: Before executing eradication, document and preserve: Active Directory replication metadata (`Get-ADReplicationAttributeMetadata`) to identify unauthorized account creation or group membership changes — Qilin affiliates create rogue admin accounts for persistence; Registry export of `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` and `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce` for persistence artifacts; Full list of scheduled tasks on compromised hosts exported via `schtasks /query /fo CSV /v`; Network traffic captures (pcap via Wireshark or `tcpdump`) of any active C2 sessions before network changes — Qilin's Go-based implant uses encrypted C2 communications that should be preserved for IOC extraction; File system timeline from compromised hosts using `fls` (Sleuth Kit) or `dir /T:C /O:D` to establish attacker dwell time and identify all files written during the intrusion window.

Recovery — Validate backup integrity before restoring from any backup set — Qilin affiliates specifically target backup systems. Restore from offline or immutable backups only. After restoration, rotate all privileged credentials, audit Active Directory for unauthorized accounts or group membership changes, and monitor for reinfection indicators for a minimum of 30 days.

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 IA-5 (Authenticator Management), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: For teams without enterprise backup validation tooling: (1) Verify backup integrity before restoration using SHA-256 checksums against pre-incident baseline hashes stored offline — `Get-FileHash -Algorithm SHA256` on Windows or `sha256sum` on Linux; compare against known-good hashes stored in a physically separate location; (2) Test restore to an isolated VLAN or air-gapped VM before production restoration — do not restore directly to production without sandbox validation given Qilin's documented backup-targeting behavior; (3) Post-restoration, run `Get-ADUser -Filter * -Properties PasswordLastSet,LastLogonDate,MemberOf` to enumerate all AD accounts and compare against a pre-incident user inventory for unauthorized additions; (4) Deploy osquery with the `ad_config_changes` and `scheduled_tasks` packs to monitor for reinfection indicators — query `SELECT * FROM processes WHERE name IN ('vssadmin.exe','wmic.exe') AND cmdline LIKE '%shadow%'` at 5-minute intervals for the first 72 hours post-recovery.

Evidence: Before beginning recovery, capture and preserve in write-protected forensic storage: Full memory dump of any ESXi hosts that were live during the incident using `vm-support` bundle or `esxcli system coredump` — Qilin's ESXi encryptor may leave decryption key material in memory on hosts that were not fully encrypted; Encrypted file samples with original filenames and Qilin ransom note (`[random].README.txt` or similar) from at least three affected systems for potential future decryption tool matching; Complete Active Directory database dump (`ntdsutil` snapshot) from a domain controller taken before any credential rotation — this establishes the authoritative account state at time of incident; Network flow logs (NetFlow/IPFIX) from the 72 hours preceding ransomware detonation to support exfiltration timeline reconstruction required for regulatory breach notification assessment.

Post-Incident — Conduct a gap assessment against NIST CSF PR.AC (Access Control) and RS.MI (Mitigation) controls. Review incident against CIS Benchmark hardening for ESXi and Windows Server environments. Evaluate whether phishing-resistant MFA is enforced across all remote access paths — credential abuse is the dominant initial access vector for this group. Document findings for regulatory notification assessment if data exfiltration occurred.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST AU-11 (Audit Record Retention), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: For teams without a GRC platform: (1) Conduct the NIST CSF gap assessment using the free CISA CPG (Cross-Sector Cybersecurity Performance Goals) self-assessment spreadsheet, mapping Qilin's observed TTPs

— credential abuse (T1078), shadow copy deletion (T1490), exfiltration via cloud (T1567.002) — to specific CPG goals with pass/fail status; (2) Use the free CIS-CAT Lite tool to benchmark ESXi and Windows Server configurations against CIS Benchmark profiles — prioritize CIS VMware ESXi 7.x Benchmark Section 7 (logging) and Section 3 (access control) given Qilin's ESXi targeting; (3) Document exfiltration evidence (network flow volumes, destination IPs, data classification of affected file shares) in a structured incident report as the basis for legal counsel's regulatory notification assessment — retain all forensic artifacts per NIST AU-11 (Audit Record Retention) minimums for your applicable regulatory regime (HIPAA: 6 years; PCI DSS: 1 year; GDPR: as required by supervisory authority).

Evidence: Assemble for the post-incident record and regulatory assessment: Complete timeline of attacker dwell time from initial valid credential use to ransomware detonation, reconstructed from VPN/RDP logs, Windows Security Event Log, and Sysmon telemetry — Qilin affiliates are documented with dwell times ranging from hours to weeks depending on the target's detection capability; Network flow summary quantifying total outbound data volume and destination endpoints during the exfiltration window, required to assess whether a reportable data breach occurred under applicable regulations (HIPAA, GDPR, state breach notification laws); Ransom note text and encrypted file extension (Qilin uses variable extensions per affiliate configuration) for threat intelligence sharing with CISA, MS-ISAC, or sector-specific ISAC under the voluntary sharing provisions of CIRCIA; Lessons-learned documentation mapping each Qilin TTP observed during the incident to the specific detection or prevention control that failed or was absent, as input to the updated IR plan per NIST IR-8 (Incident Response Plan).

Detection Guidance

Focus detection on pre-ransomware behaviors rather than the encryption event itself. Key behavioral indicators for Qilin-style operations: (1) Volume shadow copy deletion - Event ID 4688 or EDR process telemetry showing vssadmin.exe or wmic.exe with shadow copy delete arguments; (2) Mass service termination - sequences of Service Control Manager events (Event ID 7036) stopping backup, AV, or database services in rapid succession; (3) Anomalous file enumeration - T1083 activity from non-standard processes touching large file trees, particularly on file servers and backup repositories; (4) Outbound bulk data transfer - NetFlow or proxy logs showing large volumes transferred to cloud storage endpoints (Mega, cloud file-sharing services) outside normal business hours, consistent with T1567.002 and T1041 staging; (5) Credential reuse from unfamiliar source IPs - authentication events (Event ID 4624, 4625) using valid accounts from IPs not associated with the user's normal geography or device. For ESXi environments, monitor esxcli and vim-cmd invocations for snapshot deletion or VM power-off commands issued outside change windows. No verified Qilin-specific IOC hashes, IPs, or domains are available in this dataset; consult Check Point and Picus Security published research for current indicators and validate their freshness before operationalizing.

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1059** — Command and Scripting Interpreter
- **T1489** — Service Stop
- **T1567.002** — Exfiltration to Cloud Storage
- **T1490** — Inhibit System Recovery
- **T1083** — File and Directory Discovery
- **T1041** — Exfiltration Over C2 Channel
- **T1486** — Data Encrypted for Impact

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **CM-6** — Configuration Settings
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **IR-4** — Incident Handling
- **SC-13** — Cryptographic Protection

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

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.5.21** — Managing information security in the ICT supply chain
- **A.8.24** — Use of cryptography

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1059	Command and Scripting Interpreter	Execution
T1489	Service Stop	Impact
T1567.002	Exfiltration to Cloud Storage	Exfiltration

Technique ID	Technique Name	Tactic
T1490	Inhibit System Recovery	Impact
T1083	File and Directory Discovery	Discovery
T1041	Exfiltration Over C2 Channel	Exfiltration
T1486	Data Encrypted for Impact	Impact

Sources

Source	URL	Tier
Qilin Dominance and SLSH Enterprise Targeting - Ransom-DB	https://www.ransom-db.com/blog/weekly-ransomware-trends-april-24-2026	T3
Qilin ransomware escalates rapidly in 2025, targeting critical sectors ...	https://industrialcyber.co/ransomware/qilin-ransomware-escalates-ra...	T3
Active Ransomware Groups Q2 Trends and Intellig… - PurpleOps	https://purple-ops.io/blog/active-ransomware-groups-q2-report-apr-24	T3
Qilin Ransomware (Agenda): A Deep Dive - Check Point Software	https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/q...	T3
Qilin Ransomware Analysis: Critical TTPs and Defense	https://www.picussecurity.com/resource/blog/qilin-ransomware	T3

Generated 2026-04-25 06:49 UTC by TJS Security Command Center