INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-12 19:07 UTC

Ransomware Ecosystem Reconsolidation: Qilin, LockBit, and The Gentlemen Expand Influence in Q1 2026

THREAT ACTOR | HIGH

SCC Item ID	SCC-TAC-2026-0016
Type	Threat Actor
Severity	HIGH
Affected Products	Various organizations globally across multiple sectors targeted by ransomware-as-a-service and independent ransomware groups
Published	2026-05-12
Discovery Source	Gemini

Executive Summary

The ransomware ecosystem is consolidating in Q1 2026, with Qilin and LockBit (established groups) expanding their victim pools across multiple sectors globally, while The Gentlemen (a newer, less-documented group) has reported significant growth but carries lower attribution confidence. LockBit has resumed scaling operations despite the February 2024 law enforcement disruption (Operation Cronos). The business risk is elevated: organizations across industries face higher baseline probability of ransomware targeting, with operational disruption, data extortion, and recovery costs as primary exposures. Note: Specific growth metrics in this report carry low confidence pending primary source verification; however, the overall trend of ecosystem consolidation is assessed with medium confidence.

Technical Analysis

This item covers threat actor activity rather than a specific CVE. No CVSS or EPSS scores apply. The three groups operate primarily under the Ransomware-as-a-Service (RaaS) model, relying on affiliate networks to scale operations. Observed MITRE ATT&CK techniques span the full attack lifecycle: initial access via phishing (T1566) and external remote services (T1133), credential use through valid accounts (T1078), command execution via scripting interpreters (T1059), victim reconnaissance (T1591), service disruption (T1489), inhibit system recovery (T1490), data encryption for impact (T1486), and financial extortion (T1657). LockBit has historically used LockBit 3.0 (Black) encryptor tooling and has cycled through affiliate recruitment following Operation Cronos. Qilin (also tracked as Agenda) uses a Go-based encryptor targeting both Windows and VMware ESXi. The Gentlemen is a less-documented group; primary technical profiles are not yet established in

major threat intelligence repositories. All three groups use double-extortion tactics: encrypt and threaten to publish stolen data. Source quality for this item is limited (T3 sources, source quality score 0.56); verify current IOCs and group profiles against CISA advisories, MITRE ATT&CK Group pages, and primary vendor intelligence before actioning specific detections.

Action Checklist

1. Note: This item's sources (T3 tier) do not provide production-ready IOCs. For actionable indicators, consult the CISA and MITRE sources listed in Step 2 below.
2. Step 1: Exposure Reduction, Audit externally facing remote access services (RDP, VPN, Citrix) for exposed or weakly authenticated endpoints; disable unused external remote services. For CVE-based initial access, cross-reference CISA Known Exploited Vulnerabilities catalog; for credential-based access, prioritize MFA enforcement (see Step 3).
3. Step 2: Detection, Enable alerting on mass file rename/encryption events, volume shadow copy deletion (vssadmin delete shadows), and inhibit-recovery commands (bcdedit /set recoveryenabled no, wbadmin delete catalog). Review EDR telemetry for T1486 and T1490 behavioral indicators. Cross-reference any Qilin or LockBit IOCs from current CISA advisories and the MITRE ATT&CK pages for Qilin (G1015) and LockBit (G0032).
4. Step 3: Credential Hardening, Enforce MFA on all external-facing access points and privileged accounts (T1078 mitigation). Rotate credentials on any accounts exposed through prior phishing campaigns. Review Active Directory for anomalous account creation or privilege escalation.
5. Step 4: Backup Integrity Verification, Confirm offline or immutable backups exist and are current. Test restoration procedures. Ensure backup systems are segmented and not accessible from production endpoints that could be encrypted.
6. Step 5: Post-Incident Control Review, Map current detection coverage against the full technique list (T1078, T1489, T1133, T1486, T1591, T1059, T1657, T1566, T1490) using MITRE ATT&CK Navigator. Identify detection gaps. Update incident response playbooks to include Qilin and LockBit-specific indicators from CISA #StopRansomware advisories.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to senior IR leadership, legal counsel, and executive stakeholders if any host exhibits confirmed T1486 (data encryption) or T1490 (inhibit system recovery) behavioral indicators, if backup integrity verification fails indicating backups may be encrypted or deleted, or if exfiltration evidence is found suggesting double-extortion staging by Qilin or LockBit affiliates — the latter triggering breach notification assessment obligations under applicable data protection regulations (GDPR 72-hour notification, HIPAA 60-day, state breach notification statutes).

Recovery Notes	Before restoring any system, verify the backup media was created prior to the earliest confirmed adversary dwell time — both Qilin and LockBit affiliates frequently maintain persistence for weeks before deploying encryption, meaning recent backups may contain implanted backdoors or staging tools. After restoration, re-image from known-good OS baselines rather than restoring the full disk image of encrypted systems, and validate restored system integrity using file hash comparison against a pre-incident baseline before reconnecting to the production network. Maintain elevated monitoring of restored systems for a minimum of 30 days post-recovery, specifically watching for re-emergence of the lateral movement and discovery TTPs (T1069, T1087, T1135) that precede ransomware deployment in Qilin and LockBit campaigns.
Forensic Artifacts	Windows Event ID 4688 / Sysmon Event ID 1 process creation logs filtered for vssadmin.exe, bcdedit.exe, wbadmin.exe, and wmic.exe with shadow copy deletion arguments — direct forensic evidence of T1490 inhibit-recovery execution by Qilin and LockBit prior to or concurrent with encryption | File system Master File Table ($MFT) and $LogFile from affected volumes, preserving pre-encryption timestamps and file names to scope data loss, map encryption progression, and identify ransom note drop locations specific to Qilin (.qilin extension, README-RECOVER-FILES.txt) and LockBit (randomized extension, Restore-My-Files.txt, wallpaper BMP) | Windows Security Event ID 4624 / 4625 / 4648 authentication logs and Kerberos Event IDs 4768/4769/4771 from Domain Controllers covering the full estimated dwell period — critical for reconstructing T1078 (Valid Accounts) and T1021 (Remote Services) lateral movement paths used by LockBit and Qilin affiliates before encryption deployment | PowerShell ScriptBlock Logging (Event ID 4104) and Module Logging capturing AD reconnaissance commands (Get-ADUser, Invoke-BloodHound, PowerView functions) consistent with Qilin and LockBit affiliate pre-encryption discovery phases (T1069, T1087, T1135, T1591) | Network perimeter and internal flow logs (NetFlow/pcap) covering DNS queries, SMB lateral movement (TCP 445), and any beaconing patterns to known Qilin or LockBit C2 infrastructure published in current CISA #StopRansomware advisories — essential for determining exfiltration scope under double-extortion models used by both groups

Per-Action IR Details

Step 1: Exposure Reduction — Audit externally facing remote access services (RDP, VPN, Citrix) for exposed or weakly authenticated endpoints; disable unused external remote services. Reference: CISA Known Exploited Vulnerabilities catalog for currently abused initial access vectors.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establishing IR capability and reducing attack surface before incidents occur

Controls: NIST SI-2 (Flaw Remediation), NIST AC-17 (Remote Access), NIST SI-4 (System Monitoring), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Run 'netstat -ano | findstr LISTENING' on Windows hosts to enumerate open ports; cross-reference against expected service baseline. Use Shodan free tier or CISA's public-facing scanning service to identify internet-exposed RDP (TCP 3389), VPN concentrators, and Citrix ADC/Gateway instances. Disable RDP via GPO ('Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services') on all non-jump-server endpoints. For Citrix, review NetScaler access logs at /var/log/ns.log for unauthenticated or pre-auth probe patterns consistent with CVE abuse tracked in the current KEV catalog.

Evidence: Before disabling or modifying any remote access service, capture: Windows Security Event Log Event ID 4624 (successful logon) filtered on Logon Type 10 (RemoteInteractive) and Logon Type 3 (Network) for the past 90 days to identify accounts that accessed systems via RDP or VPN prior to hardening; Windows Event ID 4625 (failed

logon) for brute-force patterns consistent with LockBit and Qilin initial access TTPs (T1133, T1078); VPN/Citrix authentication logs showing successful pre-MFA logins, source IPs, and session durations; firewall or perimeter logs showing inbound connections to TCP 3389, 443 (Citrix), and common VPN ports from non-corporate IP ranges.

Step 2: Detection — Enable alerting on mass file rename/encryption events, volume shadow copy deletion (vssadmin delete shadows), and inhibit-recovery commands (bcdedit /set recoveryenabled no, wbadmin delete catalog). Review EDR telemetry for T1486 and T1490 behavioral indicators. Cross-reference any Qilin or LockBit IOCs from current CISA advisories and the MITRE ATT&CK pages for Qilin (G1015) and LockBit (G0032).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection & Analysis: Monitoring, correlating, and triaging indicators of ransomware-stage activity

Controls: NIST SI-4 (System Monitoring), NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST IR-4 (Incident Handling), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with the SwiftOnSecurity or Olaf Hartong config to capture Process Creation (Event ID 1) and detect vssadmin.exe, bcdedit.exe, and wbadmin.exe invocations. Write a PowerShell file-system watcher script that alerts on more than 20 file extension changes per minute on file servers (indicative of Qilin's .qilin or LockBit's randomized extension mass-rename behavior). Apply the public Sigma rule 'proc_creation_win_vssadmin_delete_shadows' (SigmaHQ repository) to Windows Event logs using Chainsaw (free, Rust-based log scanner) — run 'chainsaw hunt C:\Windows\System32\winevt\Logs --sigma rules/ --mapping mappings/sigma-event-logs-all.yml'. For IOC matching, ingest current Qilin (G1015) and LockBit (G0032) IOCs from CISA #StopRansomware advisories into a local YARA rule set and scan with ClamAV or standalone YARA binary.

Evidence: Capture before and during detection: Windows Security Event ID 4688 (Process Creation, requires audit policy enabled) or Sysmon Event ID 1 filtering on CommandLine containing 'vssadmin delete shadows', 'bcdedit /set recoveryenabled no', 'wbadmin delete catalog', and 'wmic shadowcopy delete'; Windows System Event ID 7045 (new service installed) and 7036 (service state change) for ransomware persistence mechanisms used by LockBit (creates a service for payload execution); file system MFT ($MFT) snapshot to record pre-encryption file state and timestamps for later recovery scoping; Qilin-specific: look for files named 'README-RECOVER-FILES.txt' or variant ransom notes and '.qilin' extension artifacts in directory listings; LockBit-specific: 'Restore-My-Files.txt' ransom note and LockBit wallpaper BMP dropped to %TEMP% or desktop paths.

Step 3: Credential Hardening — Enforce MFA on all external-facing access points and privileged accounts (T1078 mitigation). Rotate credentials on any accounts exposed through prior phishing campaigns. Review Active Directory for anomalous account creation or privilege escalation.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment: Limiting adversary access and lateral movement capability during or after confirmed or suspected compromise

Controls: NIST AC-17 (Remote Access), NIST IA-2 (Identification and Authentication — Organizational Users), NIST IR-4 (Incident Handling), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: Use the free Microsoft tool 'Get-ADUser -Filter * -Properties LastLogonDate,PasswordLastSet,MemberOf | Export-CSV' to enumerate all AD accounts and flag accounts with no MFA registration, stale passwords (>90 days), or unexpected Domain Admin or Enterprise Admin group membership. Run 'net localgroup administrators' on all endpoints to detect local admin account additions — Qilin and LockBit affiliates frequently create local admin accounts post-initial-access for persistence (T1136). For phishing-exposed credential rotation, cross-reference staff email addresses against HaveIBeenPwned API (free bulk lookup) or recent infostealer dump notifications. Enforce Windows Credential Guard via GPO to block LSASS credential dumping (T1003) used in lateral movement phases preceding ransomware deployment.

Evidence: Before rotating credentials or modifying AD, preserve: Windows Security Event ID 4720 (user account created), 4728/4732/4756 (member added to security-enabled group), and 4672 (special privileges assigned) for the

30 days preceding this action; NTDS.dit shadow copy (if accessible) or a DC-level Volume Shadow Copy to support forensic AD timeline reconstruction; PowerShell ScriptBlock Logging (Event ID 4104) and Module Logging for any PowerShell-based AD reconnaissance consistent with LockBit affiliate use of PowerView or SharpHound (BloodHound ingestor) for domain enumeration (T1069, T1087); Kerberos Event ID 4769 (Kerberoasting — TGS requests with RC4 encryption) and 4771 (Kerberos pre-auth failures) indicating credential attack activity.

Step 4: Backup Integrity Verification — Confirm offline or immutable backups exist and are current. Test restoration procedures. Ensure backup systems are segmented and not accessible from production endpoints that could be encrypted.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: Verifying restoration capability and ensuring recovery infrastructure integrity before it is needed

Controls: NIST CP-9 (System Backup), NIST CP-10 (System Recovery and Reconstitution), NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 11.1 (Establish and Maintain a Data Recovery Process), CIS 11.2 (Perform Automated Backups), CIS 11.3 (Protect Recovery Data)

Compensating: Verify backup segmentation by running 'Test-NetConnection -ComputerName -Port 445' from a standard production workstation — any successful SMB connection indicates the backup server is reachable from production and at risk of Qilin/LockBit encryption targeting backup shares. Use 'Get-WmiObject Win32_ShadowCopy' to confirm VSS snapshots exist locally, but treat these as secondary only — both Qilin and LockBit explicitly target and delete VSS copies (T1490) as a first post-execution step. Validate immutable backup integrity using SHA-256 checksums generated at backup creation time; re-hash current backup files and compare. For offline media, physically verify tape or detached drive accessibility and log the test date. Perform a documented partial restore of a non-critical system to confirm the process works end-to-end.

Evidence: Before touching backup infrastructure, document: output of 'vssadmin list shadows' and 'Get-WmiObject Win32_ShadowCopy' to establish current VSS state as a baseline (and detect if ransomware has already run T1490); backup server access logs showing which production accounts or systems have connected to backup shares in the past 30 days (to identify potential ransomware lateral movement staging toward backup targets); Windows Security Event ID 4663 (object access — file/folder) on backup server shares filtered for mass read or write operations that could indicate ransomware reconnaissance or staging; network flow records between production VLANs and backup infrastructure segments to confirm or deny segmentation posture.

Step 5: Post-Incident Control Review — Map current detection coverage against the full technique list (T1078, T1489, T1133, T1486, T1591, T1059, T1490, T1657, T1566, T1490) using MITRE ATT&CK Navigator. Identify detection gaps. Update incident response playbooks to include Qilin and LockBit-specific indicators from CISA #StopRansomware advisories.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Lessons learned, detection improvement, playbook updates, and intelligence sharing after an incident or near-miss

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-5 (Security Alerts, Advisories, And Directives), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST RA-3 (Risk Assessment), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Load the MITRE ATT&CK Navigator (navigator.attack.mitre.org, free, browser-based) and import the Qilin (G1015) and LockBit (G0032) group layers directly from ATT&CK to visualize their full technique coverage; overlay your current Sysmon + Windows Event Log detection rules to identify uncovered techniques. For each gap, search the SigmaHQ GitHub repository for existing Sigma rules (free) — prioritize T1059 (command-line execution), T1566 (phishing), and T1657 (financial extortion/data exfiltration staging). Document findings in a structured gap register with columns: Technique ID | Technique Name | Current Detection | Gap | Remediation Owner | Target Date. Ingest current CISA #StopRansomware advisories for Qilin and LockBit as structured IOC feeds into a local MISP instance (free, open-source) or a simple CSV-based IOC watchlist consumed by Sysmon or Windows Defender.

Evidence: For post-incident gap analysis, preserve and analyze: the complete Sysmon operational log and Windows Event Log archives from the review period (minimum 90 days) stored to a write-once location before any log rotation occurs; a point-in-time export of all current detection rules, SIEM alerts, and EDR policies as a configuration baseline to measure improvement against; network flow data (NetFlow, sFlow, or pcap from perimeter taps) covering the analysis period to identify any C2 beaconing patterns consistent with Qilin's use of Cobalt Strike or LockBit's use of custom C2 infrastructure; a copy of all CISA #StopRansomware advisories for Qilin and LockBit published through the review date, archived locally, to serve as the authoritative IOC and TTP reference for playbook updates.

Detection Guidance

Focus detection on post-compromise ransomware staging behaviors rather than group-specific IOCs, which rotate frequently. Key behavioral indicators: (1) Volume shadow copy deletion, Windows Event Log, Security/System channels; Sysmon Event ID 1 for vssadmin.exe or wmic.exe with 'delete' arguments. (2) Mass file extension changes, EDR file system telemetry; alert on high-volume rename events within short time windows. (3) Recovery inhibition, Sysmon Event ID 1 for bcdedit.exe with /set recoveryenabled or wbadmin delete commands. (4) Lateral movement via valid accounts, Windows Security Event ID 4624 (logon type 3) from unexpected sources; correlate with T1078 detections. (5) External remote service abuse, Firewall and VPN logs for authentication anomalies on RDP (TCP 3389), RDP gateway, or SSL VPN endpoints. For group-specific IOCs (hashes, C2 infrastructure), consult current CISA #StopRansomware advisories and the MITRE ATT&CK pages for Qilin (G1015) and LockBit (G0032). IOCs from T3 sources in this dataset are not included here due to insufficient confidence for production use.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`[not available — see note]`	Group-specific C2 infrastructure for Qilin, LockBit, and The Gentlemen rotates frequently. Current IOCs are not included here due to T3 source quality and rapid staleness. Source current IOCs from CISA #StopRansomware advisories and MITRE ATT&CK Group pages (Qilin: G1015, LockBit: G0032).	LOW

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1489** — Service Stop
- **T1133** — External Remote Services
- **T1486** — Data Encrypted for Impact
- **T1591** — Gather Victim Org Information
- **T1059** — Command and Scripting Interpreter
- **T1657** — Financial Theft

- **T1566** — Phishing
- **T1490** — Inhibit System Recovery

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CM-6** — Configuration Settings
- **SI-4** — System Monitoring
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **SC-7** — Boundary Protection
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-7** — Software, Firmware, and Information Integrity
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SI-8** — Spam Protection
- **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
T1078	Valid Accounts	Defense-Evasion
T1489	Service Stop	Impact
T1133	External Remote Services	Persistence
T1486	Data Encrypted for Impact	Impact

Technique ID	Technique Name	Tactic
T1591	Gather Victim Org Information	Reconnaissance
T1059	Command and Scripting Interpreter	Execution
T1657	Financial Theft	Impact
T1566	Phishing	Initial-Access
T1490	Inhibit System Recovery	Impact

Sources

Source	URL	Tier
Top 15 Ransomware Groups Targeting U.S. Businesses	https://www.dcgla.com/top-ransomware-groups-us-businesses/	T3
Top 10 Ransomware Groups and the 15 Most Frequently Targeted ...	https://www.linkedin.com/pulse/top-10-ransomware-groups-david-sehye...	T3
Inventory of Active Ransomware Attack Groups in 2025 - Antiy Labs	https://www.antiy.net/p/inventory-of-active-ransomware-attack-group...	T3
8 Most Dangerous Ransomware Groups: M.O., Victims, and More	https://heimdalsecurity.com/blog/most-dangerous-ransomware-groups/	T3
Rogues gallery: 15 worst ransomware groups active today	https://www.csoonline.com/article/3838121/the-dirty-dozen-12-worst-...	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 2026-05-12 19:07 UTC by TJS Security Command Center