Smarttech
YOUR 24/7 SECURITY PARTNER

Smarttech
YOUR 24/7 SECURITY PARTNER

Qilin Ransomware Threat Guide

NSAI
INFORMATION SECURITY
NSAI Certified
QUALITY
NSAI Certified

www.smarttech247.com

Contents

Introduction 2
Methodology 2
Overview 2
Origins & Evolution 3
Targeting & Impact 3
Business Model & Ecosystem 4
Initial Access & Operators' Playbook 5
Post-Compromise TTPs (MITRE ATT&CK-mapped) 8
Malware & Technical Artifacts 11
Emulation & Testing 12
Detection & Telemetry Guide 12
Prevention & Hardening 13
Incident Response Playbook 14
References 14

Introduction

For defenders, Qilin represents the modern face of ransomware: cross-platform, affiliate-driven, and constantly evolving. Its operators adapt quickly to new security measures, employ layered evasion techniques, and exploit trusted tools to remain undetected until the encryption phase begins.

In recent months, Qilin's activity has intensified, with notable campaigns against organizations in the manufacturing and financial sectors-industries who's operational and data dependencies make them highly vulnerable to double-extortion tactics. The group employs a combination of phishing, credential abuse, and exploitation of exposed services to establish initial access, followed by lateral movement and encryption across critical systems.

This guide provides a focused overview of Qilin's evolution, tactics, and operational methods, along with actionable detection and mitigation strategies to help defenders anticipate and counter this growing ransomware threat.

Methodology

This report presents proprietary rising cyber threat data and research from the Smarttech247.

All the facts and statements about to be presented are gathered based on the information that the Smarttech247 team collects as part of its threat intelligence department.

Overview

Amid the growing wave of ransomware attacks disrupting global industries, Qilin has emerged as one of the most active and adaptable operations in 2025. Leveraging a flexible Ransomware-as-a-Service model, it enables affiliates to execute targeted intrusions that combine data theft, encryption, and extortion against high-value enterprises.

The group provides customizable builds to affiliates, enabling tailored encryption options, ransom note language, and persistence mechanisms. This flexibility has attracted a growing number of threat actors, making Qilin one of the more adaptable and modular ransomware families currently observed in the wild.

Qilin's operations follow a double-extortion model-stealing sensitive data before encryption to pressure victims into paying. Stolen data is often leaked on its dedicated dark-web site, which functions both as a shaming platform and as proof of compromise.

Recent campaigns show a surge in attacks on manufacturing and financial organizations, aligning with a broader ransomware trend toward targeting sectors with critical uptime requirements and valuable proprietary data. The group's tactics include exploitation of exposed services (such as RDP and VPN gateways), deployment of legitimate remote-management tools, and use of encrypted communication channels to hinder detection.

Qilin's combination of technical sophistication, affiliate growth, and strategic targeting positions it as a persistent and evolving threat within the global ransomware landscape.

Origins & Evolution

Qilin, originally known as Agenda, surfaced in mid-2022 and quickly gained attention for its Ransomware-as-a-Service (RaaS) model and flexible, customizable payloads. Early samples were compiled in Go, offering broad cross-platform compatibility and enabling affiliates to adapt the ransomware for different operating systems and enterprise environments.

By 2023, the developers transitioned the codebase to Rust, a move that improved performance, obfuscation, and evasion capabilities. Rust's memory-safe architecture and complexity hinder traditional static analysis, making detections more difficult for antivirus and EDR solutions. This rewrite also coincided with a shift toward affiliate recruitment on dark-web forums, signaling Qilin's full transformation into a mature RaaS ecosystem.

Over time, Qilin's operators expanded their infrastructure, introducing a dark-web leak site where stolen data is published to pressure victims during ransom negotiations. The group also began adopting enterprise-focused attack chains, using valid credentials, vulnerability exploitation, and remote management tools to infiltrate large organizations.

Qilin's continued development reflects a deliberate strategy to compete with other high-profile ransomware groups like LockBit, BlackCat, and Medusa. Its evolution from a single ransomware family into a fully operational RaaS with active affiliate partnerships, regular feature updates, and refined encryption routines highlights its persistence and adaptability in today's ransomware ecosystem.

Targeting & Impact

Primary Verticals

Qilin's campaigns predominantly target manufacturing and financial institutions, two sectors that are particularly vulnerable to operational disruption and data theft.

- **Manufacturing:** Qilin exploits the heavy reliance on continuous operations and integrated OT/IT environments. Attacks in this sector often result in production downtime and supply-chain interruptions, forcing rapid incident response and negotiation under pressure.
- **Finance:** Financial organizations are prime targets due to the sensitivity of client data, payment infrastructures, and potential reputational damage. Qilin affiliates frequently leverage credential abuse or exposed remote-access points to reach internal systems.
- **Other sectors:** Beyond its core targets, Qilin has also struck entities in healthcare, education, and government, following a broader ransomware trend toward public-facing and data-rich organizations. These attacks aim to maximize leverage through exposure of confidential or personally identifiable information (PII).

Geography & Victimology Trends

While Qilin claims victims worldwide, available data indicates a concentration in Europe, North America, and parts of the Asia-Pacific region.

- The group demonstrates a global reach, yet prefers victims operating in regions with mature IT infrastructure and higher ransom-paying potential.
- European manufacturing and U.S. financial services have emerged as consistent targets, with occasional activity reported in Australia and Japan.
- The affiliate structure allows operators from different geographic backgrounds to conduct independent campaigns, contributing to a varied but persistent global footprint.

Qilin's victim selection reflects a balance between high-value disruption potential and data monetization, with affiliates choosing targets that ensure quick access, broad impact, and strong extortion leverage.

Notable Incidents & Recent Victims

Recent months have seen Qilin increasingly active on dark-web leak sites, publicly naming victims to amplify pressure.

- **Asahi Group Holdings (Japan)** – A high-profile manufacturing and beverage conglomerate reportedly listed as a victim in mid-2025, highlighting the group's focus on large industrial enterprises with extensive digital supply chains.
- **Financial institutions and technology service providers** in Europe have also appeared on Qilin's leak portal, suggesting targeted campaigns against organizations handling sensitive transactional or client data.
- **Healthcare and education organizations** have faced smaller-scale but still damaging attacks, often resulting in operational disruptions and data exposure.

The frequency and diversity of these incidents underscore Qilin's operational maturity and adaptability, positioning it among the more active ransomware threats in 2025.

Business Model & Ecosystem

RaaS Structure, Recruitment Hooks & "Brand" Signals

Qilin operates as a Ransomware-as-a-Service (RaaS) program, providing affiliates with pre-compiled ransomware payloads, custom configuration options, and access to a dark-web control panel for managing attacks and tracking victims. The core operators believed to be based in Eastern Europe act as service providers, maintaining the infrastructure, encryption tools, and leak platform, while affiliates conduct the intrusions.

Recruitment occurs through underground forums and encrypted communication channels, where Qilin advertises features such as:

- **Customizable builds** (extensions, ransom notes, encryption scope)
- **Cross-platform support** for Windows, Linux, and ESXi systems
- **Private negotiation portals** and payment infrastructure
- **Technical assistance and profit sharing** for skilled affiliates

These offerings, along with promises of reliability and anonymity, have helped establish Qilin as a recognizable "brand" within the cybercriminal ecosystem. Their leak site, styled with a polished interface and active victim listings, reinforces credibility and competitive positioning against other RaaS operations like LockBit and BlackCat.

Infrastructure & Bulletproof Hosting Dependencies

Qilin's infrastructure reflects a well-distributed and resilient design typical of mature RaaS programs. The group relies heavily on bulletproof hosting (BPH) providers for both their leak portal and command-and-control (C2) operations. These services, often located in jurisdictions with limited cybercrime cooperation, allow Qilin to evade takedowns and maintain operational continuity.

Key characteristics include:

- **Multi-layered hosting chains**, using reverse proxies and mirrored domains to obscure true backend locations
- **Tor-based negotiation and leak sites**, ensuring victim anonymity and secure payment communications
- **Encrypted traffic channels and domain rotation** to bypass network detections and blocklists
- **Redundant servers and backup nodes**, enabling rapid restoration in case of takedown attempts

This resilient infrastructure supports long-term campaigns and provides affiliates with dependable uptime, enhancing the "service quality" of the Qilin operation. The combination of structured affiliate management, polished branding, and hardened infrastructure positions Qilin as a competitive and durable RaaS threat within today's ransomware landscape.

Initial Access & Operators' Playbook

Phishing, Valid Credentials, Exposed Services

Tactics observed

- **Spear-phishing & credential harvesting:** Targeted emails with malicious attachments or links that harvest credentials or drop initial malware loaders.
- **Valid-credential reuse / brute-force / password spray:** Use of stolen or weak credentials to access VPNs, webmail, and remote-desktop gateways.
- **Exposed remote services:** Direct targeting of publicly accessible services (RDP, VPN concentrators, remote management panels, Citrix/VMware consoles) to bypass perimeter controls.

Typical operator flow

1. Phish to obtain initial credentials or a foothold.

2. Use harvested credentials to log into exposed services (RDP, VPN, webmail) or pivot to internal resources.
3. Escalate access using local tools and credentials found in scripts/configs.

Detection signals

- Unusual login patterns (VPN/RDP logins from rare geolocations, impossible travel, or new device fingerprints).
- Multiple failed authentication attempts followed by successful access from the same source.
- New or anomalous forwarding rules, mailbox rules, or OAuth app consents in mail systems.
- Web server logs showing access to admin endpoints from unknown IPs.

Immediate mitigations

- Force password resets for compromised accounts, enable MFA, and require reauthentication on high-risk accounts.
- Block/limit external RDP/VPN access; enforce VPN with conditional access policies.
- Quarantine affected mailboxes and review recent mail rules and sign-in history.
- Apply IP/geo blocks for suspicious login sources and implement step-up authentication.

Vulnerability Exploitation (Citrix ADC, Fortinet, ESXi/RDP highlights)

Tactics observed

- Exploitation of internet-exposed appliances and management planes (e.g., Citrix ADC, Fortinet SSL VPN, VMware ESXi) to gain remote code execution or authentication bypass.
- Chaining of initial RCE with credential theft to establish persistent admin-level access.

Typical operator flow

1. Scan for vulnerable management endpoints and public-facing appliances.
2. Exploit known CVEs (public exploit code is often used) to obtain shell or admin access.
3. Move laterally, dump credentials, and deploy tooling (including Cobalt Strike or native scripts) for wider compromise.

Detection signals

- High-volume or anomalous scanning activity (massive requests, unusual URIs) to management endpoints.
- Unexpected service restarts, file drops in appliance consoles, or changes to appliance configurations.
- Logs showing successful exploitation patterns (known exploit payloads, unusual POSTs to management endpoints).

- Jump-host creation or new administrative accounts appearing after access.

Immediate mitigations

- Identify and patch exposed appliances immediately; if patching is not possible, restrict access to trusted IPs only.
- Implement network segmentation so management interfaces are not reachable from the internet.
- Harden appliance management: change default ports, disable unused services, enforce MFA for admin consoles, and enable logging/alerting.
- Use host-based EDR to detect post-exploit behavior (shell activity, suspicious child processes).

Use of IABs (Initial Access Brokers), RMM Tools, Cobalt Strike

Tactics observed

- **Initial Access Brokers (IABs):** Affiliates sometimes purchase or lease initial access (user accounts, VPN access, footholds) from third parties shortening time-to-compromise.
- **Legitimate Remote Management & Admin tools (RMM):** Abuse of remote desktop tools, legitimate IT admin tools, and remote monitoring management platforms to execute payloads and persist.
- **Cobalt Strike & commodity C2:** Deployment of frameworks like Cobalt Strike (or custom C2) for command-and-control, lateral movement, and payload distribution.

Typical operator flow

1. Acquire an initial foothold via IAB access or phishing.
2. Deploy RMM tools or living-off-the-land binaries (PowerShell, PsExec, WMI) to move laterally and stage for encryption.
3. Install/beacon with Cobalt Strike or similar for robust C2 and orchestration of encryption across many hosts.

Detection signals

- Unusual installation or usage of RMM agents from accounts that don't normally deploy them.
- Beacons or long-lived outbound connections to suspicious domains/IPs, especially on non-standard ports or tunneled over HTTPS/Tor.
- Use of native admin tools executed in unusual patterns (e.g., psexec-like connections across many endpoints, wmiexec from service accounts).
- Discovery artifacts: AD enumeration (net group, nltest, dsquery), LDAP queries, or unexpected Kerberos/SPN lookups.

Immediate mitigations

- Monitor for new RMM installs and require strict change control/approval for RMM deployment.
- Egress filtering to block known C2 domains and restrict outbound traffic to necessary destinations only.
- Apply endpoint hardening: block or alert on living-off-the-land execution patterns, restrict usage of PsExec, WMI, and remote PowerShell where possible.
- Harden privileged accounts: implement Just-In-Time (JIT) and Just-Enough-Administration (JEA), remove local admin rights where feasible, and audit service-account use.

Post-Compromise TTPs (MITRE ATT&CK-mapped)

Discovery & Credential Access

What Qilin affiliates do

- Enumerate AD, local accounts, groups, sessions, and shares to locate high-value targets (Domain Controllers, backup servers, finance systems).
- Search for credentials in files, scripts, scheduled task configs, and credential stores.
- Use credential dumping tools (Mimikatz-like behavior), pass-the-hash, or brute-force/password-spray to escalate access and pivot.

Signals to hunt

- Unusual LDAP/AD enumeration queries, large or rapid net user / nltest / dsquery activity.
- High volume of Credential Dumping indicators: suspicious use of LSASS dumps, attempts to access \Windows\System32\config hives, or tools invoking sekurlsa APIs.
- Reuse of credentials from geographically unusual locations or impossible-travel alerts.
- Discovery commands executed from non-admin hosts or by non-privileged accounts.

Quick mitigations

- Enforce MFA on all admin and remote access paths.
- Reduce standing administrative privileges (JIT/JEA) and rotate service account secrets.
- Monitor and alert on sensitive Recon commands and LSASS memory access attempts; block unauthorized credential-dumping tools.

Persistence & Privilege Escalation

What Qilin affiliates do

- Establish persistence via autostart mechanisms (registry Run/RunOnce entries, scheduled tasks, services) and install remote-management agents or web shells.

- Escalate privileges by exploiting unpatched local vulnerabilities, misconfigured services, or abusing valid service accounts.

Signals to hunt

- New or modified Registry Run keys or anomalous RunOnce activity.
- Creation of suspicious scheduled tasks, new Windows services, or unexpected service binary paths.
- Sudden enabling or modification of AutoLogon, Sticky Keys, or other registry modifications.
- Exploit-style behavior: kernel/privilege escalation events or use of exploit PoC tool markers.

Quick mitigations

- Monitor and restrict changes to autostart locations (registry, startup folders, scheduled tasks).
- Harden workstations and servers: patch prioritization, application allowlists, and limit local admin.
- Block or alert on unsigned binaries being registered as services or scheduled tasks.

Lateral Movement

What Qilin affiliates do

- Move laterally using RDP, SMB/admin shares, PsExec/WinRM, stolen creds, and remote management tools to reach critical servers and backup repositories.
- Target domain controllers, file servers, and virtualization hosts (ESXi) to maximize impact.

Signals to hunt

- Spike in RDP sessions from an account to multiple endpoints, or RDP logins at unusual hours.
- Mass file access over SMB (many files read/written from a single account) and sudden creation of admin shares.
- Use of remote administration utilities from endpoints that don't normally use them.
- Lateral execution patterns: single account authenticating across many hosts within a short window.

Quick mitigations

- Restrict RDP exposure; require jump hosts with MFA and session logging.
- Limit lateral auth: block SMB from user workstations to servers, apply microsegmentation.
- Monitor for and block abnormal multi-host authentication behavior.

Defense Evasion

What Qilin affiliates do

- Disable, tamper with, or evade EDR/antivirus (stop services, remove agents, or use signed binaries to proxy execution).
- Use Safe Mode or drivers (bring-your-own vulnerable drivers / BYOVD) to bypass controls, and clear/overwrite logs to hinder forensic trails.
- Employ process injection, living-off-the-land binaries (LOLBins), and encrypted C2 channels to obscure activity.

Signals to hunt

- Sudden stops or crashes of security services or unexpected driver installations.
- Event-log gaps, deletion of specific Windows Event Log channels, or commands that clear logs.
- Signed binary proxy execution patterns (e.g., authorities executing unusual arguments), anomalous use of rundll32, regsvr32, msiexec, PowerShell with encoded commands.
- Outbound encrypted sessions to rare destinations and long-lived beacons.

Quick mitigations

- Harden EDR: prevent tampering, protect agent processes, use kernel-level protections where possible.
- Alert on service stops, driver installs, and log-clear events.
- Restrict use of high-risk LOLBins via application control and script-blocking policies.

Collection & Exfiltration (Double-Extortion Flow)

What Qilin affiliates do

- Aggregate sensitive data (databases, IP, financial records) to staged locations, compress/encrypt stolen material, then exfiltrate to attacker-controlled infrastructure prior to encryption.
- Publish exfiltrated datasets to a public leak site as leverage if ransom negotiations fail (double-extortion).

Signals to hunt

- Large and unusual data transfers from file servers or DB hosts to internal staging systems, followed by outbound transfers.
- Creation of archive files (.zip, .7z, .rar) or use of data staging accounts that don't normally move bulk files.
- Outbound connections with sustained high volumes, especially to uncommon endpoints or via proxy/Tor gateways.

Quick mitigations

- Monitor for abnormal data aggregation behaviors and bulk file archive creation.

- Enforce egress filtering, DLP controls, and traffic anomaly detection; block known exfil destinations and Tor exit nodes.
- Ensure offline, immutable backups and encrypt backups at rest.

Impact (Encryption & Recovery)

What Qilin affiliates do

- Execute coordinated encryption across endpoints, servers, and virtual hosts; delete or corrupt backups and shadow copies to impede recovery (shadow copy deletion).
- Use strong encryption primitives (hybrid AES for file encryption + asymmetric RSA for key protection) to make recovery without keys infeasible.

Signals to hunt

- Rapid mass file modification patterns (file renames, new extension applied to many files) and mass deletion of VSS snapshots.
- Creation of ransom notes (common filenames), or sudden spikes in file IO errors and antivirus alerts due to encryption processes.
- Unexpected access to backup services or management consoles preceding file tampering.

Quick mitigations

- Isolate impacted hosts immediately to prevent spread.
- Have tested recovery playbooks using immutable/offline backups; validate backup integrity regularly.
- Harden backup servers: network isolation, separate credentials, and strict access controls; block processes that perform VSS deletion unless authorized.

Malware & Technical Artifacts

Codebase (Rust/Go) & cross-platform variants

Qilin began as *Agenda* with Go-based samples and later moved to Rust, a deliberate rewrite observed in public reporting that improves obfuscation and cross-platform capability. The family now offers builds for Windows, Linux, and ESXi, enabling affiliates to target endpoints, servers and virtual infrastructure. This multi-language, multi-target approach increases operational reach and complicates static analysis.

Config knobs: extensions, kill lists, ransom notes

Qilin binaries and builder panels expose configuration options commonly used by affiliates: file extension filters/allowlists, process/hostname “kill lists” (to avoid encrypting security tooling or chosen systems), custom ransom-note templates and language selection, and modules to exclude specific paths (backups, AV). These knobs let affiliates tune impact and reduce collateral damage to

maximize leverage. Dark-web profiles and leak-site samples show consistent use of tailored ransom notes and victim-specific messaging.

Encryption details & recovery considerations

Qilin employs a hybrid cryptographic model typical of modern ransomware: symmetric encryption (e.g., AES) for file content and asymmetric protection (e.g., RSA) for keys, making offline recovery difficult without keys. Operators also target recovery artifacts (VSS/Shadow Copies) and backup access prior to encryption. Recovery guidance should therefore prioritize immutable, offline backups, segmented backup credentials, and validated restore drills; forensic capture prior to any attempted remediation is critical

Emulation & Testing

Stages & ATT&CK techniques

Emulation should reflect the full Qilin kill chain: Initial Access (phishing, exposed services, IAB access) → Execution & Persistence (payload drop, scheduled tasks, services) → Privilege Escalation & Discovery (credential dump, AD enumeration) → Lateral Movement (RDP, SMB, PsExec/WinRM) → Collection & Exfiltration (staging + C2 egress) → Impact (VSS deletion, mass encryption). Map each stage to MITRE ATT&CK techniques before test design.

Priority test scenarios

Create prioritized, safe emulation scenarios that validate detection and response for high-risk behaviors:

- **Shadow copy deletion** (Impact) - simulate deletion of VSS snapshots and confirm alerts.
- **Event/log clearing** (Defense Evasion) - simulate log tampering and verify integrity controls.
- **RDP lateral movement** (Lateral Movement) - emulate mass remote sessions from one user to many hosts.
- **Sample drop & execution** (Execution) - drop a benign test artifact and confirm EDR catches execution and persistence attempts.

Expanding scenarios

Broaden testing to chained scenarios: PaExec-style remote script execution, AD discovery and Kerberoasting-like lookups, mock exfil over encrypted channels, and abuse of legitimate RMM tools. These validate detection gaps when attackers use living-off-the-land techniques or authorized admin tooling.

Detection & Telemetry Guide

Host-based signals (EDR / Windows Eventing)

Key host signals: LSASS memory access and dumps, new scheduled tasks/services, changes to Registry Run/RunOnce, process injection attempts, mass file rename/IO spikes, VSS snapshot deletion events, and sudden creation of archive files. Instrument EDR to alert on these behaviors and collect memory/volatile evidence for triage.

Network-based signals (C2, exfil, BPH indicators)

Network telemetry should look for long-lived outbound beacons, unusual DNS patterns, large outbound data transfers to abnormal endpoints, Tor/egress to BPH-hosted infrastructure, and domain rotation patterns. Correlate destination hosting characteristics with known bulletproof-hosting profiles tied to Qilin.

SIEM content ideas (Splunk / QRadar)

- **High-priority correlation rules:** mass authentication across multiple hosts by a single account; VSS deletion followed by archive creation; new service installs by non-admin users; EDR agent stops + outbound to Tor/BPH IPs.
- **Dashboards:** lateral-movement heatmap, backup-access timeline, high-risk credential usage, and dark-web leak-monitor widget. Map each rule to ATT&CK technique IDs for traceability.

Validation workflow mapped to emulation plan

1. Run a low-impact emulation scenario (e.g., benign file creation + simulated VSS deletion).
2. Verify SIEM/EDR caught expected telemetry and triggered playbooks.
3. Iterate with higher-fidelity scenarios (RDP movement, archive+exfil) and tune detections to reduce false positives while preserving sensitivity.

Prevention & Hardening

External surface: Citrix/Fortinet/ESXi control baselines & patch priorities

Prioritize patching and exposure reduction for internet-facing appliances and hypervisors (Citrix ADC, Fortinet SSL-VPN, VMware ESXi). If immediate patching isn't possible, restrict management-plane access to trusted IPs, enforce MFA, and monitor appliance logs for exploit-like activity. These controls significantly reduce the most commonly observed initial-access vectors.

Credential hygiene & RDP hardening

Enforce organization-wide MFA, remove or rotate stale service and local admin accounts, apply JIT/JEA for privileged access, and eliminate direct RDP exposure by using hardened bastion/jump hosts with session recording and MFA. Password hygiene and conditional access are primary controls against credential-based intrusions.

EDR hardening against BYOVD / Safe Mode bypass tactics

Harden EDR agents: protect agent processes from tampering, enable kernel-level protections where feasible, monitor driver installations and Safe Mode boots, and enforce application allowlisting to limit signed-binary proxying. Regularly test EDR resilience against known BYOVD techniques.

Third-party & BPH exposure reduction

Audit third-party suppliers and remote management vendors for exposure risk, require secure vendor access patterns, and monitor for BPH-hosted leak or C2 infrastructure. Use threat intelligence feeds to block or monitor known BPH ranges and act quickly on indicators.

Incident Response Playbook

First hour: containment, privilege & lateral control

- Isolate identified footholds (network-level segmentation, disable VPN/RDP access where abuse detected).
- Revoke or rotate credentials for implicated accounts; enforce MFA re-enrollment for critical users.
- Freeze or snapshot affected VMs (for forensics) and block outbound traffic to suspected C2 endpoints.

Forensics: artifact collection & triage

Collect volatile data (memory, running processes), EDR telemetry, Windows Event logs, appliance logs (Citrix/ESXi), and copies of any ransom notes. Preserve timeline of file operations and backup-access events before remediation. Maintain chain-of-custody for legal review.

Communication, legal, & negotiation considerations

Activate legal and executive channels early; coordinate disclosure with regulators where required (sector-specific rules for finance/health). If exfiltration is suspected, engage legal counsel and consider specialized negotiators; document all interactions and preserve evidence of extortion demands posted to leak sites.

Restore & lessons learned

Restore from verified immutable backups only after ensuring attacker persistence is removed. Conduct post-incident reviews to identify gaps (patching cadence, credential hygiene, detection coverage), and update tabletop exercises and playbooks accordingly.

References

- https://securityaffairs.com/183447/security/qilin-ransomware-announced-new-victims.html
- https://socradar.io/dark-web-profile-qilin-agenda-ransomware/
- https://www.halcyon.ai/threat-group/qilin
- https://www.attackiq.com/2025/10/02/emulating-qilin-ransomware/