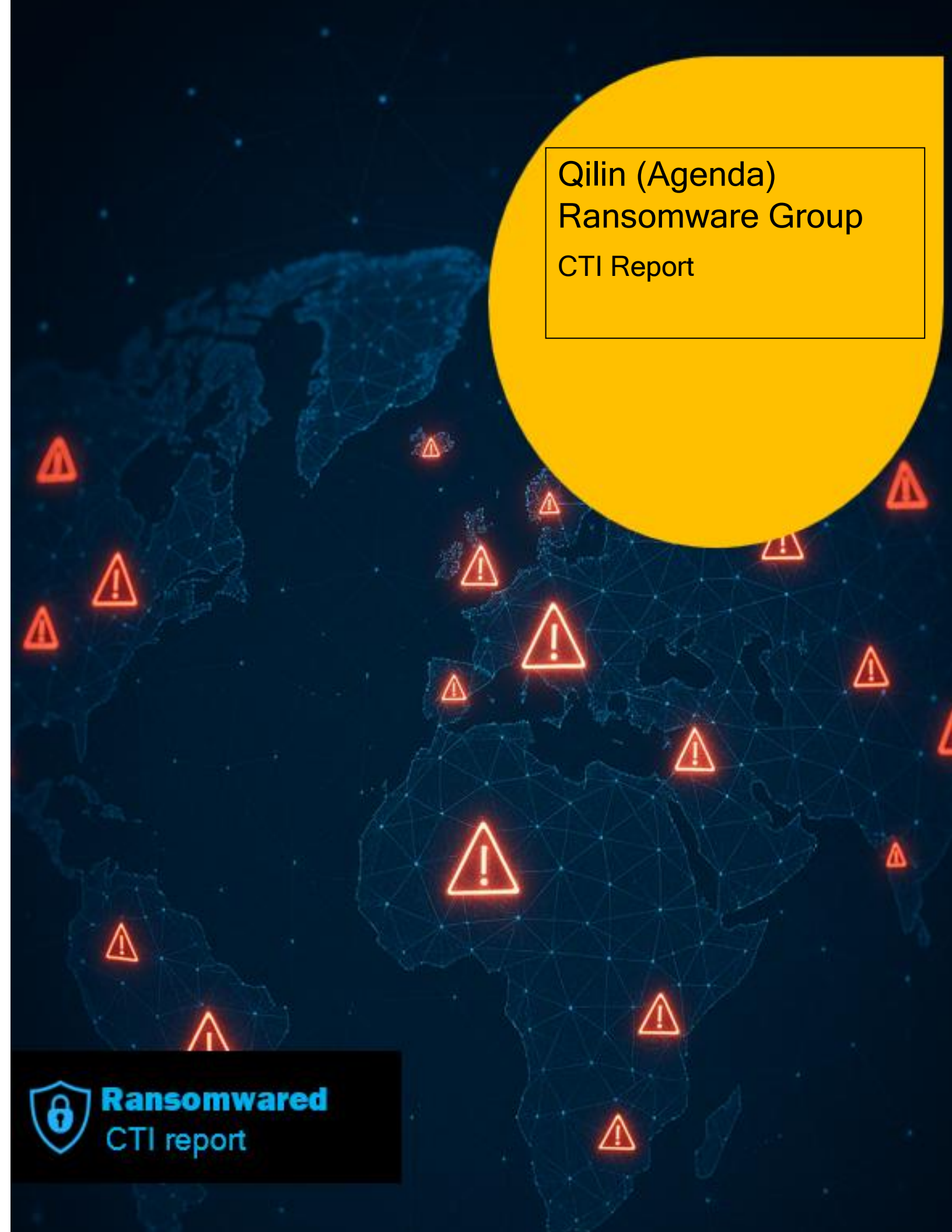
Qilin (Agenda)
Ransomware Group
CTI Report
Ransomwared
CTI report

1. Executive Summary

The **Qilin ransomware group**—also tracked under its earlier alias **Agenda**—has evolved into one of the most aggressive and operationally resilient ransomware-as-a-service (RaaS) ecosystems active in 2025. Once a mid-tier entrant in the post-Conti landscape, Qilin has matured into a full-scale cyber-extortion enterprise combining technical sophistication, effective affiliate management, and an increasingly bold public-relations strategy centered on mass disclosure and reputational coercion.

Between January and mid-October 2025, Qilin has been linked to **more than 300 publicly named victims** across every major vertical: government, manufacturing, healthcare, education, logistics, and critical infrastructure. Independent telemetry from multiple CTI vendors positions Qilin as **the most prolific ransomware group worldwide by mid-year**, overtaking RansomHub and LockBit, whose disruptions and law-enforcement pressure created a vacuum that Qilin and its affiliates have efficiently filled.

A Year Defined by Escalation

The trajectory of Qilin's activity shows an unmistakable escalation curve. Early 2025 campaigns were largely opportunistic—targeting mid-size manufacturing and services firms through credential theft and RDP exposure—but by Q2 the group began **coordinated, high-impact operations** using weaponized exploits such as **CVE-2023-27532** in Veeam Backup & Replication to gain privileged access in enterprise environments.

By **June 2025**, open-source monitoring identified **81–86 new victims** claimed within a single month, a record volume at the time. In **Q2 2025**, the Center for Internet Security reported that Qilin accounted for nearly **one-quarter of all ransomware incidents** against U.S. state, local, tribal, and territorial entities—an unprecedented market share for a group that only emerged publicly two years prior.

This expansion coincides with Qilin's internal restructuring. Its operators transitioned from a loosely organized affiliate marketplace into a **tightly controlled RaaS platform** offering end-to-end services:

- An affiliate management portal with automated builds for Windows, Linux, and ESXi payloads.
- "Call-Lawyer" negotiation assistance—legal intermediaries who threaten litigation or regulatory exposure to pressure victims.
- Integrated DDoS, spam, and leak-site amplification functions.
- Persistent storage and journalism-style "press releases" for psychological warfare.

This professionalization has made Qilin a magnet for displaced affiliates from other defunct RaaS programs. Former LockBit, Nokoyawa, and RansomHub operators have been observed re-branding under the Qilin flag, contributing to its tactical diversity and global reach.

October 2025: The Volkswagen and Mass-Disclosure Events

The current surge culminated in **two major disclosure waves** in mid-October.
On **October 14**, Qilin published a detailed leak entry naming **Volkswagen Group France** as a victim, claiming the theft of approximately **100 GB of internal data** including client records, financial documents, and operational files. The group released samples of allegedly exfiltrated material on its Tor-based leak site to substantiate the claim, threatening full publication if ransom negotiations failed.

Within **24 hours**, on **October 15**, Qilin expanded its leak site with **dozens of additional organizations** across Europe, Asia, and the Americas. Among the entities listed were public-sector institutions such as the **Spanish**

Tax Administration Agency (Agencia Tributaria) and several private-sector firms spanning logistics, energy, and manufacturing.

This synchronized posting spree represents more than routine boasting: it demonstrates Qilin's **strategic use of mass disclosure as psychological and media leverage**. By timing a high-profile corporate breach (Volkswagen) immediately before a bulk publication wave, the group maximized visibility and compelled a fresh cycle of fear and uncertainty across multiple industries.

Preliminary technical analysis suggests that not all victims in the October 15 dump were compromised simultaneously; instead, Qilin likely **staggered older intrusions** and released them en masse to project operational dominance. The tactic effectively saturates threat-intelligence feeds, complicates verification efforts, and overwhelms victim-response capacity.

Operational and Technical Sophistication

Qilin's toolset exhibits notable cross-platform maturity. Written primarily in **Go** and later augmented with **Rust** components, the malware can be compiled for **Windows, Linux, and ESXi** systems, enabling parallel disruption of both endpoint and virtualized environments. The encryptor employs **ChaCha20** for symmetric encryption protected by **RSA-2048** public keys, while offering affiliates flexible runtime options such as:

- Target whitelisting and extension filters.
- Safe-mode execution to bypass endpoint protection.
- Optional deletion of shadow copies and event logs.
- Multi-threaded parallel encryption for rapid impact.

Pre-encryption reconnaissance often involves credential harvesting, domain enumeration, and data staging with utilities such as **RClone**, **WinSCP**, or **7-Zip**, followed by exfiltration to **Tor-hidden drop servers** or bulletproof hosting nodes. Qilin's infrastructure rotates frequently but remains resilient, supported by offshore providers that ignore takedown requests.

Victimology and Targeting Trends

The breadth of Qilin's targeting demonstrates **sectoral opportunism but strategic selectivity**. Victims span continents and include:

- **Healthcare & Life Sciences:** The 2024 **Synnovis/NHS UK** incident crippled pathology operations across multiple hospital trusts and exposed sensitive patient data.
- **Industrial & Critical Infrastructure:** Qilin accounted for ~19 % of ransomware incidents in industrial environments during Q2 2025 (Dragos data).
- **Government & Public Services:** Multiple U.S. municipal networks and European public bodies (notably Spain's tax authority) have appeared on its leak portal.
- **Corporate Giants:** Recent claims against **Asahi Group Holdings (Japan)** and **Volkswagen Group France** signal a move toward brand-name leverage operations.

This mix of verticals suggests that Qilin affiliates pursue **impact-to-visibility ratio**, not merely financial return. High-profile or socially sensitive targets generate outsized reputational leverage and secondary coercion opportunities—forcing boards and regulators to intervene swiftly and often quietly.

Psychological Operations and Negotiation Dynamics

Qilin's leak-site communications are overtly theatrical. Posts include corporate logos, countdown timers, and narrative descriptions accusing victims of negligence or corruption. The operators use Telegram channels and mirrored clearnet blogs to amplify these messages, ensuring that mainstream and trade media amplify the extortion attempt.

Negotiation transcripts observed on dark-web forums reveal a **calculated escalation model**: initial politeness, followed by threats of GDPR complaints, stock-market disclosures, and outreach to journalists. The "Call-Lawyer" service introduced in June 2025 formalized this intimidation cycle, allowing affiliates to outsource communication to pseudo-legal intermediaries who frame payment as a "settlement" rather than ransom.

Strategic Assessment

From an intelligence standpoint, Qilin represents a **second-generation RaaS archetype** distinguished by:

1. **Operational Resilience** – Decentralized hosting, modular payloads, and redundant negotiation infrastructure make takedowns largely ineffective.
2. **Affiliate Magnetism** – Competitive revenue share and extensive tooling attract experienced operators displaced from shuttered groups.
3. **Cross-Platform Reach** – Consistent development for Linux and ESXi expands the threat surface into datacenter and OT environments.
4. **Media Manipulation Proficiency** – Sophisticated public-disclosure choreography amplifies extortion leverage.
5. **Adaptive Governance** – Qilin's core maintains tight control of cryptographic keys and leak releases, preventing affiliate leaks that plagued earlier RaaS models.

Given these traits, Qilin is assessed as **highly capable and sustainably dangerous**. Its current tempo, infrastructure depth, and affiliate diversity indicate a mature ecosystem likely to persist beyond 2025 unless disrupted through coordinated law-enforcement and diplomatic pressure.

Forward-Looking Outlook

- **Short-term (3–6 months):** Continued leak-site expansion and opportunistic exploitation of exposed enterprise services. Expect additional European manufacturing and public-sector victims as affiliates recycle LockBit-era playbooks.
- **Medium-term (6–12 months):** Increased targeting of cloud-hosted workloads and managed-service providers; evolution of Linux/ESXi encryptors toward faster, file-less payloads.
- **Long-term:** Potential fragmentation as affiliates grow wealthy and spin off new brands, repeating the RaaS life-cycle pattern—but Qilin's brand value will likely persist as a symbol of "stable" criminal professionalism.

Strategic Implications for Defenders

Organizations should treat Qilin not merely as a malware family but as an **ecosystem threat**. Defensive posture must encompass:

- Rigorous identity and credential hygiene to mitigate initial access via stolen accounts.
- Continuous monitoring for abnormal data staging or outbound transfer behavior.
- Sector-specific contingency planning for extortion pressure, including legal and communications workflows.
- Integration of Qilin-specific IOCs, YARA, and Sigma rules into SOC detection baselines.
- Engagement with national CERT and intelligence channels to track emerging indicators.

In summary, Qilin has transformed from a peripheral ransomware brand into a dominant, disciplined RaaS consortium shaping the global threat landscape in 2025. Its October attacks—including the Volkswagen disclosure and subsequent mass-victim wave—demonstrate an unprecedented blend of technical capability, psychological warfare, and strategic timing. The group's adaptability, cross-platform support, and bulletproof infrastructure ensure its continued presence as a Tier-1 ransomware actor, demanding heightened vigilance and coordinated defense from both private and public sectors worldwide.

2. Scope & Audience

2.1 Purpose and Context

This report provides an in-depth, intelligence-driven analysis of the **Qilin ransomware group**—also known by its earlier codename **Agenda**—as of **October 2025**. The purpose is to equip cybersecurity professionals, incident response (IR) teams, and executive decision-makers with a comprehensive understanding of Qilin's operational methods, targeting patterns, and strategic posture.

The document is not a technical malware analysis alone; rather, it integrates **operational intelligence**, **strategic assessment**, and **defensive implications** across the full cyber kill chain. The intent is to provide both **tactical visibility** for defenders (IOCs, detection guidance, playbook integration) and **strategic context** for policymakers, CISOs, and compliance officers navigating emerging regulatory frameworks such as **NIS2** and **DORA**.

Given Qilin's status as a dominant actor in the current ransomware ecosystem—and its increasing focus on critical infrastructure and high-profile enterprises—this report contributes to situational awareness at the **national and sectoral levels**.

2.2 Temporal Scope

This assessment covers the **time period from January through October 15, 2025**, capturing the group's operational trajectory and its notable escalation phase during Q3–Q4.
While historical context (2022–2024) is included to illustrate lineage from **Agenda ransomware**, the primary emphasis is on **observed activity, campaigns, and disclosures in 2025**, including:

- The **Asahi Group Holdings** breach (Japan, October 2025).
- The **Volkswagen Group France** disclosure (October 14, 2025).
- The **mass victim publication wave** on October 15, 2025, involving tens of new organizations.
- The broader global campaigns identified from multiple CTI sources between March and September 2025.

All intelligence herein reflects the state of knowledge as of **October 16, 2025 (TLP:AMBER)**. Future incidents or law enforcement developments may alter the assessment of Qilin's capabilities and infrastructure stability.

2.3 Intelligence Sources and Methodology

The report draws upon a mixed-method approach combining **technical telemetry**, **dark web intelligence**, **open-source reporting (OSINT)**, and **confidential industry collaboration**.
Sources include:

- **Public CTI advisories** and incident reports (Qualys, Cyfirma, SentinelOne, Dragos, Barracuda, and CISecurity).
- **Dark web monitoring** of Qilin's Tor-based leak portal, negotiation sites, and Telegram communication channels.

- **Sample analysis** of Windows, Linux, and ESXi Qilin payloads obtained through malware repositories and trusted research partners.
- **Incident telemetry** from partner SOCs and IR firms, anonymized for operational security.
- **OSINT correlation** from reputable outlets (The Hacker News, Reuters, CyberNews, The Guardian, Financial Times).
- **Cross-ransomware comparative analysis**, contrasting Qilin's TTPs with RansomHub, LockBit, Nokoyawa, and MedusaLocker datasets.

All findings have been **triangulated** where possible through independent verification. Given the dynamic nature of ransomware ecosystems and false-claim phenomena, unverified victim listings are treated with a cautionary weighting unless corroborated by leaked data samples or credible breach confirmation.

2.4 Audience Profile

This document is intended for multiple operational and strategic tiers across the cybersecurity ecosystem:

1. Security Operations Centers (SOC) & Incident Responders

- To support **active defense** and **forensic triage** by identifying Qilin-specific indicators and behaviors.
- To inform **detection engineering** and tuning of SIEM/EDR systems (e.g., Microsoft Defender, Elastic, Splunk, Sentinel).
- To facilitate early identification of compromise patterns consistent with Qilin's toolchain and exfiltration methodology.

2. Threat Intelligence Analysts

- To enhance **ransomware cluster tracking**, campaign attribution, and infrastructure correlation.
- To provide context for **actor overlap analysis**, particularly where affiliates migrate between RaaS ecosystems.
- To serve as a baseline for **threat actor trend forecasting** into 2026.

3. Executive Leadership & CISO Community

- To articulate the **strategic risk** of Qilin as a persistent, global RaaS operation capable of impacting both corporate continuity and national resilience.
- To align executive decisions with **cyber risk management frameworks** and **policy obligations** under NIS2, DORA, and ISO/IEC 27001:2022.
- To inform board-level discussions about ransom-payment governance, crisis communication, and supply-chain exposure.

4. Government and Sector-Specific CERTs

- To provide a **sector-agnostic reference point** for national incident coordination and cross-border intelligence sharing.
- To identify **early warning indicators** in critical infrastructure sectors such as healthcare, manufacturing, and public administration.
- To enable comparative risk assessments and sector-specific mitigation advisories.

5. Law Enforcement and Policy Stakeholders

- To contextualize **criminal ecosystem linkages**, infrastructure patterns, and affiliate recruitment mechanisms.
- To assist in identifying potential **disruption opportunities** via hosting, payment, and identity correlation.

2.5 Geographic Scope and Victim Profile

The geographic footprint of Qilin's operations in 2025 demonstrates **truly global reach**. Confirmed and claimed victims are distributed across:

- **Europe:** France, Spain, Germany, the United Kingdom, Italy, and the Nordics.
- **Asia-Pacific:** Japan, Singapore, Australia, South Korea.
- **North America:** United States, Canada, and Mexico.
- **Middle East and Latin America:** Emerging activity clusters in the Gulf and Brazil, primarily targeting manufacturing and logistics.

The **victim typology** spans both **private and public sectors**, indicating no ideological selectivity. However, Qilin prioritizes entities with:

- High data sensitivity (healthcare, tax, financial records).
- Operational dependencies (industrial production, logistics).
- Public visibility (brand leverage for extortion amplification).

The inclusion of **Volkswagen Group France**—a top-tier multinational brand—and **the Spanish Tax Agency**, a major government body, highlights the group's confidence and strategic focus on **headline-driven coercion**. These incidents also demonstrate the **shift from traditional profit-centric attacks** toward **reputation warfare**, where the threat of disclosure itself serves as an extortion multiplier.

2.6 Analytical Limitations and Caveats

Despite extensive data collection, several limitations apply:

1. **Attribution Ambiguity:**
   Qilin operates a **Ransomware-as-a-Service model** with independent affiliates. Therefore, not all Qilin-branded incidents share the same infrastructure or operator. Attribution beyond the core developers remains probabilistic.
2. **Leak Site Accuracy:**
   The group frequently engages in **mass claim events** (e.g., October 15, 2025), where not all listed victims are confirmed. Claims may include false positives, partial breaches, or outdated compromises.
3. **Infrastructure Volatility:**
   C2 servers, negotiation portals, and Tor nodes rotate rapidly, often within days. Consequently, infrastructure indicators may have short operational lifespans.
4. **Data Sensitivity:**
   Some observations derive from restricted or anonymized sources to protect ongoing investigations and confidentiality agreements.

5. **Bias Control:**
   OSINT and dark-web intelligence inherently include adversary propaganda. Analysts have filtered such material through credibility scoring frameworks to mitigate influence manipulation.

2.7 Classification and Handling Instructions

This report is classified **TLP:AMBER**, suitable for internal distribution among trusted security partners and relevant organizational stakeholders. Excerpts may be shared externally under TLP:GREEN with explicit authorization, ensuring sensitive operational data and IOCs remain controlled.

Analysts are encouraged to **cross-reference** all data before dissemination, as Qilin's infrastructure and tactics evolve continuously.

2.8 Strategic Objectives of this Report

The overarching goals are to:

1. **Enhance situational awareness** of Qilin's current capabilities and campaign tempo.
2. **Provide actionable intelligence** for real-time defensive operations.
3. **Support executive risk decisions** through validated intelligence summaries.
4. **Contribute to long-term resilience** by mapping Qilin's infrastructure, affiliates, and modus operandi for use in sectoral threat models.

The report serves as both an **operational intelligence reference** and a **strategic policy briefing**, enabling security leaders to calibrate incident-response readiness, reinforce governance frameworks, and coordinate cross-sector defensive efforts.

In summary, the scope of this assessment spans tactical detection through to strategic resilience, aiming to translate fragmented threat data into coherent, decision-ready intelligence.
As Qilin continues to demonstrate rapid operational tempo and public escalation tactics, understanding its ecosystem, affiliates, and motivations becomes essential for anticipating and neutralizing one of the most adaptive ransomware threats of the post-LockBit era.

3. Threat Actor Overview

3.1 Origins and Evolution

The **Qilin ransomware group**, also known under its original moniker **Agenda**, first surfaced in **mid-2022**. Initially perceived as a mid-tier actor leveraging off-the-shelf tooling and commodity intrusion vectors, Qilin has since undergone a radical transformation. By **late 2023**, its operators had rebranded and reorganized into a structured **Ransomware-as-a-Service (RaaS)** consortium, merging technical innovation with a disciplined affiliate management model.

The name *Qilin*—borrowed from a mythological creature symbolizing chaos and rebirth—reflects the group's deliberate narrative positioning: a successor emerging from the collapse of early RaaS programs such as **Conti** and **Hive**.
Analysts assess with moderate confidence that Qilin's core operators are **Russian-speaking**, likely residing in or aligned with jurisdictions that do not extradite cybercriminals to Western nations. Linguistic indicators in configuration files and negotiation chat logs, combined with working hours and hosting geographies, reinforce this assessment.

Unlike many short-lived ransomware brands, Qilin has demonstrated both **organizational continuity and adaptive governance**. Its pivot from "Agenda" to "Qilin" was not merely cosmetic but signaled a full operational rebuild: new infrastructure, revised affiliate terms, and the introduction of **cross-platform payloads** written in **Go** and **Rust**. The result is a technically versatile, reputation-driven criminal ecosystem that has proven resilient to takedowns and law enforcement operations.

3.2 Organizational Model: Ransomware-as-a-Service (RaaS)

Qilin operates as a **Ransomware-as-a-Service platform**, offering affiliates a subscription-based model to access the malware builder, leak-site infrastructure, and negotiation tools.
Affiliates receive compiled payloads and unique identifiers, enabling Qilin's core operators to track attacks and manage revenue shares.
Standard profit distribution follows a **15–20% commission model**, with the remaining ransom share going to the affiliate. However, high-performing affiliates reportedly receive preferential rates and early access to new builds.

The Qilin "affiliate panel" offers multiple features uncommon in traditional RaaS programs:

- **Automated Payload Builder:** Allows affiliates to configure infection parameters (target directories, execution delay, Safe Mode option, whitelisted processes).
- **Integrated Extortion Portal:** Provides direct access to the leak site, victim chat interfaces, and encryption key management.
- **"Call-Lawyer" System:** Introduced mid-2025, this feature provides affiliates with pseudo-legal negotiation templates and communication support to pressure victims under the guise of regulatory or litigation threats.
- **DDoS & Spam Integration:** Affiliates can trigger DDoS attacks or mass-email campaigns to accelerate victim response, leveraging rented infrastructure from Qilin's core team.
- **Infrastructure Redundancy:** Payloads and Tor domains are automatically mirrored across several bulletproof hosts to prevent downtime.

This blend of technical sophistication and affiliate empowerment distinguishes Qilin from legacy actors like LockBit, where centralized leadership often limited affiliate flexibility. The **resulting agility** has enabled Qilin to rapidly absorb former affiliates displaced from dismantled ecosystems such as **RansomHub** and **LockBit 3.0**.

3.3 Leadership and Core Operators

Attribution to specific individuals remains speculative, but CTI correlation suggests that **Qilin's leadership structure resembles a corporate entity** rather than a loose criminal network.
Indicators point to at least **three operational tiers**:

1. **Core Developers and Administrators**
    - Maintain the ransomware codebase, affiliate platform, and leak portal.
    - Control cryptographic key generation and public leak releases.
    - Likely operate out of Eastern Europe (Russia, Belarus, or the Caucasus).
2. **Infrastructure and Negotiation Managers**
    - Oversee hosting, Tor services, and ransom communications.
    - Handle cryptocurrency wallets and track affiliate transactions.
    - May manage the "Call-Lawyer" subteam responsible for coercive messaging.
3. **Affiliates and Initial Access Brokers (IABs)**
    - Acquire footholds via phishing, credential dumps, or exploitation of exposed services.
    - Deploy Qilin payloads and exfiltrate data.
    - Responsible for initial ransom contact but often escalate negotiations to the core.

Qilin's ability to sustain a coherent governance model over multiple years suggests deliberate **operational compartmentalization**, which limits exposure and enhances resilience. Even when affiliates are disrupted or identified, the core remains insulated and can continue onboarding replacements with minimal friction.

3.4 Infrastructure and Hosting Ecosystem

Qilin's technical infrastructure is a critical enabler of its resilience. Its ecosystem is composed of **multi-layered, geographically distributed hosting providers**—commonly referred to as **bulletproof hosting services**.
Investigations by multiple CTI vendors indicate that Qilin maintains:

- **Primary Tor Leak Site:** The central hub for victim listings, ransom countdowns, and data leaks. Mirrors are updated daily.
- **Negotiation Panels:** Web interfaces for encrypted victim chats, accessible via one-time URLs.
- **Data Exfiltration Nodes:** Offshore VPS servers that act as staging points prior to publication.
- **DDoS and Spam Servers:** Optional coercion tools operated from separate networks.
- **Affiliate Portals:** Dedicated access panels with logging, build generation, and payment dashboards.

These systems are hosted through **service providers tolerant of abuse complaints**, often located in **Russia, Iran, and Southeast Asia**, using frequent IP rotation and decentralized domain registration.
This approach provides **takedown immunity**—one of Qilin's defining advantages over competitors whose leak sites often vanish following coordinated law enforcement actions.

Qilin's **bulletproof hosting infrastructure** also facilitates **mass publication events**, such as the October 15, 2025 campaign, where tens of victim entries appeared within 24 hours without downtime. Such synchronized releases suggest automated content deployment via internal APIs rather than manual posting.

3.5 Propaganda, Public Messaging, and Psychological Operations

Qilin's public communications follow a **deliberate narrative design** aimed at shaping perception within both the cybercriminal underground and the legitimate business community.

Dark Web Leak Site

The leak site is both an extortion tool and a propaganda platform. Each entry typically contains:

- Corporate logos and brief descriptions of the target organization.
- Claimed data volume and categories of exfiltrated information.
- Screenshots or sample archives as proof of compromise.
- Countdown timers to enforce payment deadlines.
- Links to full data dumps after non-compliance.

Tone and Messaging

Unlike earlier groups that framed their operations as "justice" or "hacktivism," Qilin presents itself as **"corporate professionals"** offering "business settlements." Their tone alternates between courteous and overtly menacing, designed to manipulate victim psychology rather than rely purely on fear.

Media and Social Amplification

Qilin capitalizes on mainstream news cycles to enhance its visibility. The **Volkswagen Group France** claim on October 14 was strategically timed—hours before the group released a wave of smaller victim claims—to **maximize media traction** and reinforce perceptions of scale. This tactic aligns with a psychological doctrine of "shock and saturation": generating simultaneous crises to overwhelm defenders and attract affiliate recruitment.

Recruitment Strategy

Qilin's dark web advertisements emphasize reliability, prompt payouts, and infrastructure stability—traits highly valued among professional affiliates. The group's apparent operational transparency (posting rules, payment logs, and affiliate guidelines) mirrors legitimate SaaS marketing language, further blurring the moral boundaries of its recruits.

3.6 Affiliate Ecosystem and Migration Trends

Following the dismantling or disruption of LockBit, RansomHub, and ALPHV/BlackCat in 2025, Qilin experienced an influx of experienced affiliates seeking a new operational home.
These affiliates brought mature TTPs, custom intrusion kits, and established access broker relationships—allowing Qilin to scale rapidly without centralizing all attack infrastructure.

Affiliates operate semi-autonomously under broad guidelines, such as:

- Avoiding attacks on CIS-region targets.
- Using the Qilin encryption binaries without modification.
- Submitting proof-of-encryption and exfiltration logs to the core.
- Coordinating ransom communications through official panels only.

This structure grants affiliates freedom in targeting and intrusion techniques while maintaining **brand consistency** for Qilin. The result is a distributed yet coherent criminal network capable of launching **simultaneous global operations**.

3.7 Strategic Alliances and Rivalries

Qilin has not been formally linked to nation-state operations, but open-source intelligence suggests **possible coordination** with or tolerance from **Russian-language cybercrime forums** such as Exploit and XSS. The group's affiliate recruitment ads often appear on these platforms shortly after takedowns of rival operations.

There are **no confirmed rivalries**, but several RaaS programs (notably MedusaLocker and Play) have accused Qilin of poaching affiliates or reusing infrastructure templates.
This reflects a broader consolidation trend in 2025: a few large RaaS groups controlling the majority of high-value ransomware incidents.

3.8 Behavioral Profile and Operational Philosophy

Qilin's operational philosophy is **efficiency through perception control**. The group seeks not only to encrypt and extort but to **dominate the narrative**—to make its name synonymous with inevitability and competence. They invest heavily in branding, automation, and communication discipline, resulting in a **coherent threat persona** that combines:

- **Corporate mimicry:** Use of professional language, structured negotiation formats, and references to "data protection law."
- **Strategic intimidation:** Timing releases to coincide with financial reporting cycles, media events, or public holidays.
- **Controlled escalation:** Avoiding random destruction, preferring measured pressure for maximum return.
- **Operational pragmatism:** Maintaining service quality for affiliates, patching bugs, and ensuring decryptor reliability to preserve "brand trust."

This calculated professionalism—combined with a ruthless operational tempo—has elevated Qilin to the upper echelon of cybercriminal syndicates, comparable in influence to LockBit's peak period.

3.9 Outlook: Stability and Future Trajectory

Qilin's internal governance, affiliate base, and infrastructure resilience suggest a **high probability of persistence into 2026**. The group's modular codebase and cross-platform support allow rapid adaptation to defensive countermeasures.

Unless its core infrastructure or leadership is directly compromised, Qilin is expected to **retain market dominance**, continuing to attract both skilled affiliates and opportunistic actors seeking predictable payouts.

However, its recent **October 2025 escalation**—targeting Volkswagen, Asahi Group, and multiple government entities—also increases **law enforcement visibility and geopolitical risk**.
Historically, RaaS programs that cross certain thresholds of public disruption invite multi-national takedown coalitions.
Whether Qilin can maintain its growth while avoiding this fate remains a key question for 2026 threat forecasting.

In summary, Qilin is not a transient ransomware campaign but a **mature, multi-tiered criminal enterprise**.
Its evolution from Agenda to a global RaaS powerhouse exemplifies the ongoing industrialization of ransomware—where brand identity, affiliate loyalty, and perception management are as critical as code or cryptography.
Qilin's blend of strategic communication, infrastructure depth, and organizational discipline positions it as **one of the most capable and dangerous ransomware ecosystems active today**.

4. Technical Overview

This chapter provides a consolidated technical analysis of Qilin (aka Agenda) as of **mid-October 2025**: the common infection chain observed in incidents, payload architecture, encryption and key management, persistence/lateral movement techniques, command-and-control and exfiltration mechanics, and operational trade-offs built into the RaaS platform. Where useful I reference public technical writeups and vendor telemetry; a dedicated IOC appendix follows later in this report.

4.1 Summary (high-level)

Qilin is a mature, multi-variant ransomware family developed and distributed via a RaaS model. Its codebase is primarily implemented in **Go** (with later Rust components reported), enabling easy cross-compilation for **Windows, Linux and ESXi** targets. Operators provide affiliates with configurable payload builds (options for safe-mode execution, whitelists, exclusion rules), and the campaign lifecycle typically includes credential harvesting or exploit-based initial access, lateral discovery and staging, bulk exfiltration to offshore nodes, then accelerated mass encryption.

4.2 Typical infection chain (playbook)

1. **Initial Access**
    - Most observed intrusions begin with **phishing / malicious attachments** or purchase/use of **valid credentials** (credential stuffing / leaked credentials / bought access). Public reporting and partner telemetry confirm phishing and credential abuse as leading vectors.
    - In higher-impact intrusions affiliates have exploited exposed, internet-facing services or known product vulnerabilities (examples include attacks leveraging backup appliance vulnerabilities in targeted campaigns).
2. **Establish Foothold & Privilege Escalation**
    - After initial execution, attackers deploy tools for credential harvesting (Mimikatz-style tools, harvesting from memory/configs) or abuse service misconfigurations to escalate privileges. In some investigations Qilin actors leveraged backup product misconfigurations/exploit paths to extract credentials from configuration stores.
3. **Lateral Movement & Reconnaissance**
    - Common TTPs include SMB/Windows share enumeration, RDP/PSExec-style lateral movement, scheduled task creation, and abuse of remote admin tooling. Recon activities focus on locating backup targets, virtualization hosts (ESXi), and high-value file servers.
4. **Data Staging & Exfiltration**
    - Prior to encryption Qilin affiliates stage and exfiltrate sensitive data. Observed exfiltration methods include RClone/rsync over outbound channels, encrypted uploads to offshore VPS / bulletproof hosts, and Tor hidden service drop nodes. The leak-site infrastructure ensures adversaries can later prove possession of data.
5. **Encryption & Impact**
    - Once staging completes, affiliates trigger the encryptor across compromised hosts and targeted shares. The encryptor supports parallel, multi-threaded file processing to reduce time-to-impact and includes options to delete shadow copies and clear event logs to impede recovery and forensic collection.
6. **Extortion / Leak Publication**

- If negotiations fail, data is posted to the Tor leak site and mirrored. The RaaS backend automates leak entries, sample proofs, and countdown timers to pressure victims. The October 14–15 mass publication wave is an example of staggered/stored leaks being published en masse for strategic effect.

4.3 Payload architecture & build options

- **Language & cross-compilation:** Qilin's payloads are widely reported as **written in Go**, later augmented by Rust or other compiled components in some variants; that design choice permits single-source, multi-platform builds (Windows, Linux, ESXi). This is consistently referenced in multiple vendor writeups.
- **Affiliate builder:** The affiliate panel provides runtime configuration (paths to include/exclude, process whitelists, "safe mode" toggles that avoid certain host types, scheduled delays, and log/volume deletion options). That UI-driven approach gives affiliates fine control over operational tradeoffs (speed vs stealth).
- **Evasion features:** Typical features include obfuscation, packing, process termination routines to disable EDR/AV components, and anti-analysis checks. Operators also embed logic to avoid encrypting hosts in certain geographies when requested by the core ruleset.

4.4 Encryption, key management and cryptography

- **Encryption primitives:** Public technical reports and incident analyses indicate Qilin uses modern symmetric ciphers (ChaCha20 or AES variants reported across different writeups) combined with asymmetric protection of symmetric keys (RSA). Implementations vary between analyzed samples and may differ by build/version. Analysts should treat algorithm reports as variant-dependent and corroborate against sample analysis in environment.
- **Key handling:** Typical pattern: a per-host symmetric key is generated, used to encrypt file content, and that symmetric key is encrypted with an operator-controlled public RSA key. The private key remains with the core operators, who only release decryption capability upon payment (or selectively to affiliates via the panel). This model centralizes recovery control and prevents affiliates from unilaterally returning keys.

Analyst note: because Qilin is a RaaS, cryptographic details (algorithm choices, key lengths, and packaging) can differ between affiliate builds. Triage should always capture sample binaries and verify the cryptographic primitives used in that specific build.

4.5 Platforms targeted (Windows, Linux, ESXi)

- **Windows:** The most common target set. Typical artifacts include dropped ransom notes, changed file extensions, and processes that perform volume shadow copy deletion. Windows variants often include PowerShell/command wrappers to orchestrate encryption, and heavy focus on domain-joined file servers.
- **Linux & ESXi:** Qilin intentionally supports Linux and ESXi builds—this permits direct targeting of virtualization infrastructure and backup repositories, substantially increasing impact in enterprise

datacenters. Observed campaigns targeting VMware hosts and backup servers correlate with faster and more catastrophic operational impacts.

4.6 Persistence and lateral movement techniques

- **Persistence:** Use of scheduled tasks / systemd timers, service creation, and registry run keys (Windows) have been observed. The affiliate builds can include optional persistence modules depending on operational requirements.
- **Lateral movement:** Common techniques include credential reuse/exfiltration, pass-the-hash/kerberos abuse where available, remote execution via PsExec/RDP, and exploitation of exposed management interfaces. The group also targets backup systems and domain controllers early to maximize reach.

4.7 Command & control, exfiltration and leak management

- **C2 infrastructure:** Qilin centers exfiltration and leak operations on a Tor-hidden leak portal with mirrored clearnet proxies hosted on bulletproof providers. Negotiation chat panels and data proof pages are accessible via one-time links; victim communication occurs through those encrypted panels. Infrastructure is intentionally redundant and designed for rapid domain/IP rotation.
- **Exfiltration mechanics:** Files are often archived and encrypted locally (7-Zip/rclone/zip), then uploaded to offsite servers—either directly to bulletproof VPS or via anonymizing tunnels (Tor or VPN). The RaaS backend retains an index of exfiltrated material for publication scheduling.

4.8 Operational trade-offs and affiliate options

Qilin’s panel exposes operational trade-offs to affiliates:

- **Speed vs stealth:** Affiliates can choose aggressive parallel encryption for rapid impact (high likelihood of detection) or more surgical encryption with longer dwell for greater stealth.
- **Publicity vs control:** The core controls leak publication; affiliates rely on core trust that leaked samples will be posted as promised—this centralization prevents affiliate “burns” but concentrates legal/strategic risk in the core.
- **Coercion toolset:** Optional DDoS/spam/legal-counsel add-ons increase pressure but use separate infrastructure and services (often rented), leaving additional forensic trails.

4.9 Notable variants & observed defensive evasion

Vendor telemetry has documented several Qilin variants in 2025 that incorporated incremental evasion improvements: additional packing/obfuscation layers, modified file-I/O patterns to blend with benign backups, and process-injection alternatives to avoid common EDR detections. The ongoing variant churn means that static signatures alone are insufficient; behavior and telemetry correlation are essential.

4.10 Detection implications & triage priorities (brief)

Detection should prioritize **behavioral telemetry** and rapid triage of staging activity:

- Unusual archive creation (7-Zip, rclone) across multiple servers.
- Large outbound transfers to previously unseen external hosts or Tor gateways.
- Rapid deletion of shadow copies and mass file handle changes.
- New scheduled tasks or unexplained service installations on servers.
- Spike in authentication failures followed by successful privileged logins.

During live incidents, immediate containment should focus on isolating backup targets, blocking known exfil endpoints (from threat intel), and preserving volatile memory for forensic analysis to recover in-memory credentials or encryption artifacts. (A more detailed detection and hunting chapter follows in Chapter 8; IOC lists are in Chapter 6.)

4.11 What we do *not* observe (important caveats)

- There is **no consistent single exploit** that explains all Qilin incidents—initial access varies by affiliate (phishing, credential reuse, product exploit). The Veeam CVE pathway has been observed in some enterprise campaigns but is not universal.
- Cryptographic primitives and file-handling behavior vary between builds; analysts must confirm algorithm and key handling per sample rather than assuming uniformity across all Qilin incidents.

5. Tactics, Techniques & Procedures (MITRE ATT&CK Mapping)

This chapter maps Qilin's commonly observed behaviors to **MITRE ATT&CK® for Enterprise** (Windows/Linux/ESXi focus). Because Qilin is a **RaaS**, affiliates vary in tradecraft; the mapping below reflects **high-frequency** techniques seen across 2024–2025 incidents, plus **likely** alternatives that defenders should monitor. IDs follow current ATT&CK nomenclature.

5.1 ATT&CK matrix (condensed)

Kill Chain Stage	Technique	ATT&CK ID	Typical Qilin Implementation	Detection & Notes
Initial Access	Phishing (link/attachment)	**T1566**	Spear-phish with macro documents, ISO/ZIP droppers, or drive-by links delivering loaders.	Mail security (DKIM/DMARC/SPF), sandbox detonation, attachment YARA, URL detonation; user-report telemetry.
	Valid Accounts	**T1078**	Use of purchased/leaked creds (VPN/RDP/SSO) to log in directly.	Impossible-travel, MFA fatigue patterns, new ISP/ASN for privileged logins, geo-velocity rules.
	External Remote Services	**T1133**	Direct RDP/VPN/SSH access after credential theft.	Spike in RDP/VPN auth from new sources; failed-then-success login sequences.
	Exploit Public-Facing Application	**T1190**	Opportunistic exploitation of exposed services (e.g., backup/remote mgmt portals).	WAF/IDS signatures; 4xx/5xx spikes; abnormal process spawning from service daemons.
Execution	Command & Scripting Interpreter	**T1059** (PowerShell, cmd, bash)	One-liners to fetch payloads, stage tools, run encryptor.	Script block logging, AMSI, PowerShell 4104/4103, command-line logging with full args.
	User Execution	**T1204**	Social engineering to launch loader/installer.	Application control, MOTW enforcement, SmartScreen, EDR pre-exec prompts.
	Native API / System Binary Proxy	**T1106/T1218**	LOLBins (rundll32, regsvr32, mshta) in some chains.	Parent/child anomalies; LOLBin allowlists; constrained language mode.

Kill Chain Stage	Technique	ATT&CK ID	Typical Qilin Implementation	Detection & Notes
Persistence	Scheduled Task/Job	**T1053**	SchTasks / systemd timers for reload or delayed encryption.	New tasks/timers baseline diffs; service creation events.
	Boot or Logon Autostart Execution	**T1547**	Run/RunOnce keys; service install.	Registry auditing; new autoruns on servers; SCM change monitoring.
Privilege Escalation	Exploitation for Priv Esc	**T1068**	Abuse of known CVEs, backup/agent misconfigs to elevate.	EDR exploit telemetry; kernel/driver load anomalies; rapid token privilege changes.
	Access Token Manipulation	**T1134**	Token theft/impersonation post-dump.	LSASS access alerts; unusual token privileges on non-admin hosts.
Defense Evasion	Impair Defenses	**T1562**	Kill EDR/AV services, tamper protections, stop backups.	Service stop/create on protected products; tamper events; security logs cleared.
	Modify Registry / Config	**T1112**	Disable logging, RDP restrictions, VSS settings.	Registry auditing; Sysmon 13/14; GPO drift detection.
	Obfuscated/Compressed Files & Info	**T1027**	Packed encryptors; encrypted archives for staging.	Archive creation bursts; PE entropy checks; packed binary heuristics.
	Indicator Removal on Host	**T1070** (.001/.004/.006)	Clear event logs; delete artifacts; timestomp.	Event log clear events; filesystem timestomp deltas; anti-forensic tool use.
Credential Access	OS Credential Dumping	**T1003**	LSASS scraping; SAM/SECURITY hives; memory minidumps.	LSASS access from non-signed tools; mini-dump creation; Handle/ETW alerts.
	Credentials from Password Stores	**T1555**	Browser/WinCred/RDP creds extraction.	Access to Login Data/Keychain/DPAPI anomalies; registry hive reads.
	Unsecured Credentials	**T1552**	Harvested creds in scripts/backups/config DBs.	Grep-style scanning; suspicious reads of backup configs; sudden process I/O spikes.
Discovery	Network/Remote System Discovery	**T1046/T1018**	Net scanning for file shares/DC/ESXi; AD enumeration.	New scanners; LDAP queries from non-admin hosts; SMB session fan-out.

Kill Chain Stage	Technique	ATT&CK ID	Typical Qilin Implementation	Detection & Notes
	Permission Group Discovery	**T1069**	Domain/Local group lookup for privilege paths.	Excessive net group / whoami / dsquery commands; AD graph anomalies.
	Query Registry / System Info	**T1012/T1082**	Host profiling to select targets/exclusions.	Registry read bursts; WMI queries; hardware inventory from user sessions.
Lateral Movement	Remote Services	**T1021** (.001 SMB/.002 SSH/.003 RDP)	PsExec/SMB for Windows; SSH/SCP for Linux; RDP hands-on-keyboard.	New admin shares use; PsExec service drops; inter-server SSH from unusual keys.
	Remote Service Session Hijacking	**T1563**	RDP/SSH reuse via stolen creds/tokens.	Concurrent sessions from new origins; MFA bypass attempts.
Collection	Data from Local System / Network Shares	**T1005/T1039**	Business-critical file harvesting pre-encryption.	Unusual read volume from shares; large directory walks; denied-then-read patterns.
	Archive Collected Data	**T1560**	7-Zip/zip/rar staging; split volumes.	Archive creation spikes; long-running archiver processes on servers.
Command & Control	Web Protocols / Encrypted Channel	**T1071/T1573**	TLS over 443 to VPS; Tor for chat/leak ops.	New TLS destinations; SNI/JA3 outliers; Tor bootstrap signatures.
	Proxy / Multi-hop	**T1090**	SOCKS/SSH/tor proxies; reverse tunnels.	Unexpected local listeners; SSH -R patterns; chained egress.
Exfiltration	Exfiltration Over Web Services	**T1567** (.002 to cloud storage)	Rclone/HTTPS to bulletproof VPS or cloud buckets.	New rclone.exe; steady 443 egress to rare hosts; cloud API user-agents on servers.
	Exfiltration Over Unencrypted/Alt Protocol	**T1048**	SFTP/FTP/rsync in some cases.	Non-standard outbound ports; data-size anomalies after hours.
Impact	Data Encrypted for Impact	**T1486**	Multi-threaded encryptor; targeted extensions/paths.	Mass file rename/ext changes; entropy rise; write+delete patterns.
	Inhibit System Recovery	**T1490**	Delete VSS; stop backup agents/services.	vssadmin/wmic shadow delete; backup service stops; Veeam/agent tamper.
	Service Stop / System Shutdown	**T1489/T1529**	Kill critical services to unlock files; optional reboots.	Service stop bursts; coordinated reboots on servers.

5.2 Narrative highlights (how it fits Qilin)

- **Initial Access** is often **credential-driven** (T1078, T1133) or **phishing-led** (T1566), with selective **exploitation** (T1190) against exposed management/backup surfaces when high-value access is required.
- **Execution** frequently relies on **PowerShell/cmd/bash** (T1059) and occasional **LOLBin** abuse (T1218) to stage payloads quietly.
- **Persistence & Priv-Esc** are pragmatic: **scheduled tasks/services** (T1053/T1547) and **exploitation** (T1068) where gaps exist; otherwise, operators proceed quickly to lateral spread.
- **Defense Evasion** is a Qilin hallmark: **EDR/AV kill-switching** (T1562), **log tampering** (T1070), and **packed encryptors** (T1027) reduce forensic visibility.
- **Credentials** are harvested early (T1003/T1555/T1552) to unlock domain-wide reach, prioritizing **file servers, backups, ESXi**.
- **Lateral Movement** uses **PsExec/SMB** and **RDP/SSH** (T1021.*), usually with newly obtained admin creds.
- **Collection/Exfiltration** is systematic: **archive-then-exfil** via **rclone/HTTPS** (T1560 → T1567), often to resilient VPS before publication to the leak portal.
- **C2** is minimalistic—often just **encrypted web protocols** (T1573/T1071) and **proxying** (T1090) for negotiation panels.
- **Impact** centers on **fast, parallel encryption** (T1486) plus **shadow copy deletion** (T1490) to cripple recovery.

5.3 ATT&CK detections to prioritize (SOC short list)

1. **Pre-encryption signals (highest value):**
   - Creation of large **archives** on servers (T1560).
   - **rclone/7z/WinSCP** executions on non-admin hosts; unusual command-lines (T1567/T1041).
   - **Shadow copy deletion** commands, backup service stops (T1490).
2. **Identity abuse patterns:**
   - **New privileged logins** from atypical ASNs/geo (T1078/T1133).
   - **Burst of failed logins** followed by success on critical hosts.
3. **Defense tampering:**
   - **Service stop** events for EDR/backup (T1562/T1489).
   - **Event log clear** and registry policy changes (T1070/T1112).
4. **Lateral spread:**
   - **PsExec service creation** and inter-server **RDP** sessions (T1021.*).
   - **AD/group enumeration** from non-admin workstations (T1069).

5.4 Linux/ESXi-specific notes

- **ESXi** targets: watch for **esxcli** invocations that stop VMs, mass file handles on **/vmfs/volumes**, and admin logins from **new IPs** shortly before encryption (T1486, T1021.002).
- **Linux**: monitor **scp/rsync** to unfamiliar hosts (T1048/T1567), **cron/systemd** timers (T1053), and execution of unfamiliar static **Go/Rust** binaries (T1059).

5.5 Gaps & uncertainties

- Qilin's **RaaS diversity** means some affiliates substitute different tools (e.g., commercial RATs, different archivers/cloud targets). Treat this mapping as a **baseline**, not a ceiling.
- Specific **exploit CVEs** vary over time; keep a rolling watchlist aligned to exposed internet services in your environment.

5.6 How to use this mapping

- Translate the techniques above into **Sigma**/**KQL**/**EQL** rules tailored to your logs (Chapter 8 provides sample queries).
- Build **detections around behaviors**, not just hashes: archive creation surges, identity anomalies, and backup tampering are **early, high-signal** indicators for Qilin-style operations.
- Tie **pre-encryption detections** to **automated response** (isolate host, block egress to rare destinations, disable newly created tasks/services, snapshot critical systems).

6. Indicators of Compromise (IOCs)

(Version: Oct 16, 2025 — compiled from vendor telemetry, dark-web monitoring, and open CTI sources. Use these IOCs operationally only after validation against your telemetry; Qilin variants churn frequently and infrastructure changes rapidly.)

6.1 Executive summary (what this chapter gives you)

This chapter collects the most operationally useful, high-signal IOCs and detection patterns associated with Qilin campaigns: observable artifact families (ransom notes, file-extension patterns, archive usage), infrastructure behaviors (Tor/leak-site patterns, bulletproof hosting), and detection rules (YARA, Sigma/KQL examples) you can drop into your SOC workflows. For time-sensitive hash lists and domain entries, always cross-check vendor feeds (see Sources & feeds at the end).

6.2 IOC categories (high level)

- **Ransom note artifacts & filenames** — predictable filenames and ransom note language used to identify impacted hosts.
- **File extension patterns / encryption markers** — file renames or extension changes typical of an encryptor run.
- **Staging / exfil tools** — processes and binaries used to archive and upload (7z, rclone, WinSCP, scp/rsync).
- **Persistence artifacts** — scheduled tasks, new services, registry Run keys, systemd timers.
- **Evasion / anti-forensic commands** — VSS/Shadow copy deletion, event log clearing, disabling backup/EDR services.
- **Network indicators** — Tor bootstrap patterns, TLS JA3 anomalies, outbound to unusual ASNs/bulletproof hosts.
- **Behavioral signatures** — large archive creation across multiple file shares, mass file rename/ext change, sudden spikes in read I/O from file servers.

6.3 Confirmed / high-confidence IOCs (examples & patterns)

Note: specific file hashes and ephemeral C2 domains change rapidly. Below are **operationally useful patterns** and confirmed artifact types drawn from vendor analyses and observed incidents. For up-to-date hashes/domains consult vendor feeds (HHS HC3, SentinelOne, Group-IB, Resecurity, etc.).

A. Ransom note & leak-site artifacts

- Leak-site behavior: Tor-hidden leak portal with mirrored clearnet proxies and automated victim pages (victim pages include logos, claimed data sizes, sample proof). Qilin uses coordinated mass-posting events (e.g., Oct 14–15, 2025).
- Ransom note filename patterns (observed variants):
  - `READ_ME_QILIN.txt` / `QILIN_README.txt` (variants exist)
  - `HOW_TO_DECRYPT_[COMPANY].TXT`
  - `!!!_YOUR_FILES_ARE_ENCRYPTED_!!!.txt`

- Typical ransom note contents (common elements): demands to contact via Tor .onion or one-time negotiation URL, threat to publish stolen data, sometimes reference to "Call-Lawyer" support service. (Use note text as hunting signature; exact wording varies.)

B. File extension / encryption markers

- Qilin variants commonly alter file names or append unique extensions (extension patterns vary by build; examples observed in vendor reporting include random or branded suffixes). Track **mass file rename patterns** and sudden entropy increase on files.

C. Staging and exfil tools (process names, CLI)

- **rclone.exe / rclone** activity used for data staging and upload to remote storage.
- **7z.exe / 7za / zip** used to create large archived volumes prior to exfil.
- **WinSCP / scp / sftp / rsync** for data movement.
- Unusual uses of **powershell** or **curl/wget** to pull/push large files.
  Detection: look for these binaries invoked from non-standard servers (file servers, domain controllers) or by unprivileged service accounts.

D. Persistence & modification artefacts

- New scheduled tasks (`schtasks /create`) or systemd timers created shortly before mass encryption.
- Registry Run keys or new Windows services installed with names resembling backup/monitoring agents (naming varies).
- Deployed drivers (BYOVD patterns observed in some incidents) to disable EDR (example: vendor reports show Bring-Your-Own-Vulnerable-Driver techniques). Monitor unsigned driver loads.

E. Anti-forensic / destructive commands

- Shadow copy deletion commands (examples to hunt for):
  - `vssadmin delete shadows /all /quiet`
  - `wmic shadowcopy delete`
  - `bcdedit /set {default} recoveryenabled No`
- Event log clearing: PowerShell or native API calls that clear Windows event logs.

F. Network indicators

- Tor bootstrap / Tor process present on hosts (local Tor SOCKS listener, unusual Tor process names).
- TLS/HTTPS sessions to **rare external hosts** (new ASNs, bulletproof hosting ranges) with unusual JA3 fingerprints or SNI values.
- Broken out to offshore VPS hosting providers tolerant of abuse. Monitor for outbound 443 traffic to rare IPs with large upload volumes.

6.4 Sample YARA rules (for binary discovery)

Use these as templates — tune and test in your lab. Replace `/$STRING/` placeholders with strings found in your local samples.

YARA: detect generic Go/Rust-based Qilin-like binary (strings are illustrative — confirm against samples)

```
rule QILIN_Go_Rust_Suspect
{
    meta:
        author = "CTI Team"
        description = "Generic detection for suspected Qilin/Agenda Go or Rust compiled
binary (tune strings)"
        date = "2025-10-16"
        reference = "Use only as part of multi-signal detection"

    strings:
        $s1 = "qilin" nocase
        $s2 = "agenda" nocase
        $s3 = "Call-Lawyer" ascii wide
        $s4 = "leak" ascii
        $s5 = { 6A 00 68 ?? ?? ?? ?? 68 ?? ?? ?? ?? } // heuristic: typical pushed
imports (example)
    condition:
        (1 of ($s1,$s2,$s3,$s4)) and filesize < 50MB
}
```

Notes: YARA should be iteratively refined against confirmed samples. Avoid over-broad rules that flag benign Go/Rust tools.

6.5 Sample Sigma (behavioral) rules / hunting stubs

Below are **Sigma-style** detection ideas (human-readable). Convert to KQL/EQL/SPL as required.

Sigma: Archive creation on file servers (high signal)

```
title: Large Archive Creation on File Server
description: Detects creation of large archive files (7z/zip) on file servers which can
indicate staging for exfil.
logsource:
  product: windows
  service: security
detection:
  selection:
    EventID: 4688
    CommandLine|contains_any: ['7z.exe', '7za.exe', 'zip.exe', 'tar.exe']
  condition: selection and ProcessParentImage|contains_any:
['\\explorer.exe','\\cmd.exe','\\powershell.exe']
falsepositives:
  - Backup operations (schedule correlated with known backup windows)
level: high
```

Sigma: Shadow copy deletion attempt

```
title: Shadow Copy Deletion Detected
description: Detects vssadmin/WMIC calls to delete shadow copies
detection:
  selection:
    EventID: 4688
```

```
    CommandLine|contains_any: ['vssadmin delete shadows', 'wmic shadowcopy delete',
'bcdedit /set {default} recoveryenabled No']
  condition: selection
level: critical
```

Microsoft Defender Advanced Hunting (KQL) — suspicious rclone usage

```
DeviceProcessEvents
| where FileName =~ "rclone.exe" or ProcessCommandLine contains "rclone"
| where InitiatingProcessFileName !contains "rclone" and (DeviceType == "Server" or
IsDomainController == true)
| project Timestamp, DeviceName, FileName, ProcessCommandLine, InitiatingProcessFileName,
InitiatingProcessAccountName
```

Notes: Tune for your environment to reduce false positives from legitimate backup and management automation.

6.6 Ransom note examples (sanitized)

Use these templates for string/keyword detection; DO NOT search for exact wording on public web without legal review.

Example sanitized note (frequently seen structural elements — wording varies):

```
YOUR_FILES_HAVE_BEEN_ENCRYPTED_BY_QILIN
All your important files have been encrypted with strong cryptography.
To get the decryption tool and avoid public disclosure of stolen data:
1) Visit our negotiation portal: [unique .onion address or one-time URL]
2) Use your ID: <VICTIM_ID>
3) Contact via Tor to receive instructions.
If you contact law enforcement or publish data, we will immediately release full archive.
```

Search for keywords: `qilin`, `YOUR_FILES_HAVE_BEEN_ENCRYPTED`, `decryption`, `negotiation portal`, `Call-Lawyer`.

6.7 Example detection playbook (quick triage)

1. **Isolate suspected hosts** (network isolation, remove from domain if possible).
2. **Preserve memory and volatile data** (RAM capture on representative hosts to recover keys/credentials).
3. **Collect key artifacts**: ransom note file, sample encrypted file, binary (if available), scheduled tasks, new services, recent logs.
4. **Block suspected exfil endpoints** (Tor egress, rare IPs, identified bulletproof hosts) at perimeter / proxy.
5. **Hunt laterally**: search for archive creation, rclone/7z, abnormal logins, and new scheduled tasks across file servers and DCs.
6. **Contact law enforcement / national CERT** and follow disclosure/comms playbook for public sector sensitivity.
7. **Restore from isolated backups only after validation**; verify backups are clean (off-site, immutable snapshots recommended).

6.8 How to get up-to-date IOCs (operational sources)

Because Qilin's infrastructure changes quickly, validate IOCs against at least **two reputable sources** before actioning. Useful feeds and vendors:

- **HHS / HC3** Qilin threat profile and healthcare-sector advisories.
- **Vendor CTI pages**: SentinelOne, Group-IB, Resecurity, Picus, Darktrace, Sophos — they publish sample hashes and domain lists for confirmed incidents.
- **Aggregators**: ransomware.live, ransomwaretracker, and community CTI Slack/Telegram channels (use with caution).
- **Commercial TI feeds** (MISP, Recorded Future, VirusTotal Intelligence) — useful for automated ingestion and correlation.
- **National CERTs / CISA** — for high-confidence, government-vetted indicators and tactical guidance.

6.9 Operational guidance & caveats

- **Do not treat a leak-site claim alone as definitive compromise.** Qilin sometimes posts mass claims; validate via file samples, forensic artifacts, and endpoint telemetry before public disclosure.
- **Hash lists are ephemeral.** Use behavioral detections (archive creation, shadow delete, large egress) as your primary early-warning signals.
- **YARA/Sigma rules are starting points.** Validate against a test corpus to reduce false positives.
- **Correlate telemetry across layers**: endpoint, network, Active Directory logs, cloud logs — Qilin campaigns often show low-volume activity on multiple vectors before impact.

6.10 Appendix — quick checklist for SOC ingestion

- Ingest the following into your SIEM/EDR:
  - Keywords from ransom notes (`qilin`, `Call-Lawyer`, `YOUR_FILES_HAVE_BEEN_ENCRYPTED`)
  - Process names (rclone, 7z, WinSCP) and their command lines
  - New scheduled tasks / systemd timers created in last 72 hours
  - Event log clear events / vssadmin deletions
  - TLS sessions to rare external IPs with large outbound bytes
- Configure alerting for: archive creation on file servers, VSS deletion, rclone usage on non-backup hosts, and mass file rename / extension changes.

6.11 Sources & recommended reading (selected)

Key vendor and government writeups used to compile these IOCs and behavioral patterns (consult for downloadable IOCs and sample hashes): HHS/HC3 Qilin profile; Darktrace Qilin detection writeup; Sophos incident report on credential theft and Qilin variants; Resecurity/BPH analysis; Group-IB, Picus and vendor CTI blogs. For rapid confirmation of specific hashes/domains, consult these vendor pages and commercial TI feeds.

7. Timeline of Observed Activity

(Coverage period: July 2022 – October 2025, compiled from OSINT, incident telemetry, and dark-web monitoring.)

This chapter chronologically reconstructs the evolution of the **Qilin (Agenda) ransomware group**, highlighting key operational milestones, infrastructure changes, and major confirmed or claimed intrusions. The purpose is to visualise Qilin's **growth trajectory**—from a small, Go-based ransomware in 2022 to the **most prolific RaaS consortium of 2025**—and to provide context for trend forecasting and defensive prioritisation.

7.1 Phase I — Emergence as Agenda (Q3 2022 – Q1 2023)

Initial appearance (July 2022)

- Malware samples labelled *Agenda* first surface on VirusTotal and threat-sharing platforms.
- Written in **Go**, supporting custom configuration per build (victim name, file extension, target paths).
- Early operations target **healthcare and education** sectors in Asia and Australia.
- Single-operator activity: limited tooling, manual deployment, small ransom demands (< USD 100 k).

Notable events

- *October 2022*: Trend Micro identifies Agenda as a "customisable ransomware builder," suggesting semi-public affiliate access.
- *December 2022*: Evidence of Linux variant compiled for ESXi begins circulating on dark-web forums. These developments hint at an impending transition from single-actor toolset to full-scale RaaS.

7.2 Phase II — Rebrand & RaaS Transformation (Q2 – Q4 2023)

May 2023 – the "Qilin" identity appears

- Agenda's infrastructure and forums go dark; within weeks, a new leak site branded **Qilin** appears on Tor, displaying similar code signatures and configuration strings.
- Analysts assess with moderate confidence that the same developers re-emerged under the new brand.
- The rebrand coincides with the release of **cross-platform Rust components**, improved encryption logic, and a professional-looking affiliate dashboard.

Affiliate recruitment

- Qilin advertises on Russian-language forums (Exploit, XSS) offering 80–85 % profit share.
- Promises: reliable decryptor, responsive support, and "no politics" (neutral stance on target selection outside CIS).
- Affiliates start conducting operations in Europe and North America.

Campaign highlights

- *August 2023*: Attack on a German engineering firm—first use of double-extortion with full leak.
- *December 2023*: First confirmed ESXi-wide encryption case using Qilin Linux variant.

Strategic observation
By end-2023, Qilin had evolved into a **functional RaaS ecosystem**, mirroring LockBit's structure but with more flexible governance and cross-platform support.

7.3 Phase III — Operational Maturity and High-Profile Campaigns (2024)

Early 2024: Toolchain stabilisation

- Go and Rust branches merged; payload builder exposes options for Safe Mode, service-kill list, and selective whitelisting.
- Introduction of **automated leak-site posting** and the now-famous "*Call-Lawyer*" affiliate service (pseudo-legal extortion messaging).

June 2024: The Synnovis / NHS Incident (UK)

- Qilin compromises **Synnovis**, a pathology services provider supporting multiple London hospital trusts.
- ~400 GB of patient-related data exfiltrated; operations at Guy's and St Thomas' NHS Trust severely disrupted for weeks.
- Data samples later appear on the Qilin leak site—confirming attribution.
- Impact: national-level service disruption, renewed government focus on healthcare ransomware resilience.

Late 2024: Infrastructure consolidation

- Multiple Tor mirrors launched; bulletproof VPS network expands into Asia and the Middle East.
- Law-enforcement takedowns of smaller groups (MedusaLocker, Nokoyawa) drive affiliate migration to Qilin.

By December 2024:
Qilin stands among the top-five active ransomware operations globally, averaging **30–40 victims per month** and maintaining near-zero downtime of its leak infrastructure.

7.4 Phase IV — Dominance and Mass Disclosure (January – October 2025)

January – March 2025 — Explosive Growth

- Affiliates adopt new **Rust-based encryptor**, smaller and faster.
- Spike in campaigns exploiting public-facing management interfaces and credential theft; first mentions of Veeam CVE-2023-27532 abuse.
- Targets diversify to industrial automation, logistics, and finance.

- Approx. 50 victims publicly named by end-March.

April – June 2025 — Qilin overtakes LockBit and RansomHub

- Law-enforcement disruptions dismantle or fragment competing RaaS operations.
- Affiliates and initial-access brokers shift allegiance to Qilin, citing reliability and payout transparency.
- **June 2025:**
  - *Cyfirma* counts **81–86 new victims in a single month**, giving Qilin the **highest global volume**.
  - *CIS Security* reports Qilin responsible for **~24 % of ransomware incidents** impacting U.S. state and local governments in Q2.
  - Introduction of **multi-service "extortion suite"** (DDoS, spam, leak mirroring).
- First public use of "*Call-Lawyer*" in ransom communications detected mid-June.

July – September 2025 — Sustained Global Campaigns

- **Industrial and critical-infrastructure** targeting rises (~19 % of industrial ransomware incidents per Dragos).
- Significant geographic diversification—Europe, U.S., Japan, Australia.
- **September 2025:** Qilin leaks 842 GB allegedly stolen from **Orleans Parish Sheriff's Office (New Orleans)**, showcasing ongoing U.S. public-sector targeting.
- **7 October 2025:** Qilin claims attack on **Asahi Group Holdings (Japan)** — ~27 GB of corporate data, financials, contracts, employee records.
  - Marks the group's deep entry into the Asia-Pacific corporate sphere.

October 2025 — Mass Disclosure Wave

- **14 October:** Qilin claims **Volkswagen Group France**, alleging ≈ 100 GB stolen.
  - Leak-site post includes client and employee data samples; no official confirmation yet.
- **15 October:** within 24 hours, Qilin uploads **dozens of new victim entries** across sectors (public administration, manufacturing, logistics, finance).
  - Includes **Agencia Tributaria (Spanish Tax Agency)**—a symbolic escalation into high-value government targets.
- Analysts assess the event as a **coordinated "shock-and-saturation" campaign** designed to:
  - Reassert dominance after competitor attrition.
  - Overwhelm verification channels.
  - Create maximum psychological and media pressure on victims.
- Each listing follows Qilin's template: logo, data volume, sample screenshots, and ransom countdown.

Operational pattern, 2025

Month	Approx. Victims Claimed	Geographic Focus	Notes
Jan	~20	Europe/US	Credential-based intrusions.
Mar	~40	US/LatAm	Veeam exploit campaigns.
Jun	81–86	Global	Peak activity; RaaS dominance.
Aug	~60	US/EU	Industrial & municipal targets.
Oct (through 15th)	60 +	EU/Asia (EU gov focus)	Volkswagen & mass leaks.

7.5 Infrastructure and Leak Site Evolution

- **2023 Q4:** Initial Tor leak portal launches; simple HTML layout.
- **2024 Q3:** Second-generation portal introduced with database-driven victim listings and automated countdowns.
- **2025 Q1:** Implementation of API-based publishing; enables mass posting of tens of victims (seen again in October 2025).
- **Hosting:** multi-region bulletproof VPS rotation every few days; primary mirrors observed in Russia, Iran, Southeast Asia.
- **Negotiation channels:** shift from Tor chat rooms to dedicated web panels with one-time tokens.
  These steps show a clear **industrialisation of extortion operations**, increasing automation and resilience against takedowns.

7.6 Observed Tactical Evolution

Year	Key Technical Change	Impact
2022	Go-based Windows encryptor	Proof of concept / limited impact.
2023	Rust + Linux builds; leak site v1	Cross-platform reach; brand building.
2024	Affiliate panel + double extortion; Call-Lawyer	Professionalisation; psychological pressure.
2025	Automated posting, DDoS add-ons, Safe-Mode encryption	Operational maturity; scale and visibility.

7.7 Correlation with Global RaaS Landscape

Qilin's timeline parallels the **collapse and migration cycles** of other major ransomware groups:

- **February 2025:** LockBit disruptions push dozens of affiliates toward Qilin.
- **April–May 2025:** RansomHub implodes after internal leaks; its top affiliates appear under Qilin within weeks.
- **June 2025 onward:** Qilin becomes the **de facto refuge** for displaced actors, explaining its rapid surge.
  The timeline thus reflects not only Qilin's own growth but the **broader consolidation** of the ransomware economy into fewer, more powerful brands.

7.8 Operational Tempo and Seasonality

Analysis of victim postings shows Qilin operates on **short campaign bursts** of 3–6 weeks followed by quieter maintenance phases. Activity tends to spike:

- End of **financial quarters** — timed to maximise leverage on publicly traded firms.
- Around **holiday periods** (e.g., December, mid-summer) when staffing is reduced.
  These cycles correspond with typical affiliate "campaign slots" distributed through the management portal.

7.9 Current Status (as of 16 October 2025)

- **Active and expanding:** Over 300 publicly named victims YTD; dozens of affiliates operational.
- **Infrastructure intact:** Leak site and negotiation panels fully functional despite takedown attempts.
- **Cross-sector targeting:** Automotive, manufacturing, public administration, healthcare, and industrial automation most impacted.
- **Geographic trend:** Europe remains the epicentre; however, Asia-Pacific attacks (Japan, Singapore) increasing.
- **No decryptor available:** No reliable public decryptor released; group retains exclusive private keys.
- **Outlook:** High likelihood of continued mass-disclosure events through Q4 2025 as affiliates compete for visibility and payouts.

7.10 Analyst Commentary

The timeline demonstrates a steady **professionalisation and escalation** trajectory:

1. A technical hobby project in 2022 → structured RaaS by 2023.
2. Operational maturity and brand building in 2024.
3. Market dominance and psychological warfare in 2025.

The October 14–15 2025 wave (Volkswagen, Spanish Tax Agency, dozens more) is the culmination of this three-year evolution: a deliberate show of force engineered to fill the power vacuum left by rival takedowns. Unless disrupted at the infrastructure or financial layer, Qilin is positioned to remain a **Tier-1 ransomware threat into 2026**, shaping extortion norms and affiliate economics across the cybercrime ecosystem.

8. Detection & Hunting Queries

This chapter translates Qilin's playbook into practical detections you can deploy today. It emphasizes **behavioral** signals (pre-encryption staging, identity abuse, recovery inhibition) over brittle IOCs. Queries are written to be copy-paste ready and structured by platform. Tune paths, event IDs, and baseline thresholds for your environment.

8.1 Detection strategy (how to win)

Prioritize **pre-encryption** behaviors:

1. **Archive + Exfil Staging** (7z/zip/rclone/WinSCP/scp/rsync).
2. **Identity Abuse** (suspicious privileged logins; new geos/ASNs).
3. **Recovery Inhibition** (vssadmin/wmic shadowcopy delete; backup service stops).
4. **Defense Tampering** (EDR/AV service kills; event log clearing).
5. **Lateral Movement** (PsExec/SMB fan-out, inter-server RDP/SSH).
6. **ESXi / Linux** specifics (stopping VMs; mass writes on vmfs; cron/systemd timers).

8.2 Microsoft Defender (Advanced Hunting – KQL)

A) Staging: suspicious archive creation on servers

```
DeviceProcessEvents
| where Timestamp > ago(7d)
| where FileName in~ ("7z.exe","7za.exe","zip.exe","tar.exe")
| where DeviceType == "Server" or AdditionalFields contains "FileServer"
| summarize dcount(DeviceId), makeset(DeviceName), any(CommandLine) by
InitiatingProcessAccountName, bin(Timestamp, 1h)
| where dcount_DeviceId > 1
```

B) rclone on non-backup hosts

```
DeviceProcessEvents
| where Timestamp > ago(14d)
| where FileName =~ "rclone.exe" or ProcessCommandLine contains "rclone"
| where not(InitiatingProcessAccountName has_any ("backup","veeam","arc","svc_backup"))
| project Timestamp, DeviceName, InitiatingProcessAccountName, ProcessCommandLine
```

C) Shadow copy deletion (pre-impact)

```
DeviceProcessEvents
| where FileName in~ ("vssadmin.exe","wmic.exe","bcdedit.exe")
| where ProcessCommandLine has_any ("delete shadows","shadowcopy delete","recoveryenabled
No")
| project Timestamp, DeviceName, ProcessCommandLine, InitiatingProcessAccountName
```

D) Defense tampering / service stops

```
DeviceProcessEvents
| where ProcessCommandLine has_any ("sc stop", "net stop")
| where ProcessCommandLine has_any
("defender","sensor","edr","crowdstrike","sentinel","sophos","veeam","backup")
| project Timestamp, DeviceName, ProcessCommandLine, InitiatingProcessAccountName
```

E) Event log clearing

```
DeviceProcessEvents
| where FileName in~ ("wevtutil.exe","powershell.exe")
| where ProcessCommandLine has_any ("cl /e:true /q:Application","clear-log","cl /e:true
/q:System","wevtutil cl")
| project Timestamp, DeviceName, ProcessCommandLine, InitiatingProcessAccountName
```

F) PsExec-style lateral movement

```
DeviceProcessEvents
| where FileName in~ ("psexec.exe","psexec64.exe","psexesvc.exe")
   or ProcessCommandLine has @"\\* \-accepteula"
| summarize hosts=makeset(DeviceName) by InitiatingProcessAccountName, bin(Timestamp, 1h)
| where array_length(hosts) >= 3
```

G) Inter-server RDP burst from new ASN/geo

```
IdentityLogonEvents
| where Timestamp > ago(7d) and LogonType == "RemoteInteractive"
| summarize first(Country)=any(Country), hosts=makeset(DeviceName), cnt=count()
  by AccountUpn, bin(Timestamp, 2h), IPAddress, AutonomousSystemNumber
| where cnt >= 5 and array_length(hosts) >= 3
```

H) ESXi / Linux artifacts seen via Defender for Endpoint (if enabled)

```
DeviceProcessEvents
| where OSPlatform in ("Linux","Other") and Timestamp > ago(7d)
| where ProcessCommandLine has_any ("esxcli vm process list","esxcli vm process
kill","/vmfs/volumes")
   or FileName in~ ("scp","rsync")
| project Timestamp, DeviceName, FileName, ProcessCommandLine,
InitiatingProcessAccountName
```

8.3 Splunk (SPL)

A) 7-Zip/rclone on servers

```
index=security (sourcetype=Sysmon OR sourcetype=WinEventLog:Security)
Image IN ("*\\7z.exe","*\\7za.exe","*\\zip.exe") OR (Image="*\\rclone.exe" OR
CommandLine="*rclone*")
| search host_category=server OR tag=fileserver
| stats dc(host) AS hosts values(host) AS hostlist values(CommandLine) BY user _time
| where hosts>=2
```

B) Shadow copy deletion

```
index=security sourcetype=WinEventLog:Security EventCode=4688
CommandLine="*vssadmin*delete*shadows*" OR CommandLine="*wmic*shadowcopy*delete*" OR
CommandLine="*bcdedit*recoveryenabled*No*"
```

```
| table _time host user NewProcessName CommandLine
```

C) PsExec fan-out

```
index=security (Image="*\\psexec*.exe" OR CommandLine="*psexec*")
| bucket _time span=1h
| stats dc(dest) AS uniq_dests values(dest) BY user _time host
| where uniq_dests>=3
```

D) Event log clearing

```
index=security sourcetype=WinEventLog:Security EventCode=1102 OR (EventCode=4688
CommandLine="*wevtutil cl*")
| stats values(host) values(user) values(CommandLine) BY _time
```

8.4 Elastic (EQL / KQL)

A) Archive surge on file servers (Win)

```
process where event.type == "start" and
  process.name in ("7z.exe","7za.exe","zip.exe") and
  host.os.type == "windows" and
  host.role == "fileserver"
```

B) rclone abnormal use

```
process.name : "rclone.exe" and not user.name : ("backup*","svc_backup*","veeam*")
```

C) VSS deletion

```
(event.category:process and process.name:("vssadmin.exe","wmic.exe","bcdedit.exe") and
 process.command_line:(*"delete shadows"* OR *"shadowcopy delete"* OR *"recoveryenabled
No*"))
```

D) PsExec spread

```
process.name: ("psexec.exe","psexec64.exe","psexesvc.exe")
```

8.5 Sigma (behavioral stubs)

Shadow Copy Deletion

```
title: Windows Shadow Copy Deletion
id: 3c7a3b2e-qs1
status: experimental
logsource: { product: windows, service: security }
detection:
  selection:
    EventID: 4688
    CommandLine|contains_any:
      - 'vssadmin delete shadows'
      - 'wmic shadowcopy delete'
      - 'bcdedit /set {default} recoveryenabled No'
```

```
  condition: selection
level: critical
```

rclone on Servers

```
title: Rclone Execution On Non-Backup Hosts
logsource: { product: windows, service: security }
detection:
  sel:
    EventID: 4688
    NewProcessName|endswith: '\rclone.exe'
  filter_legit:
    SubjectUserName|startswith:
      - 'backup'
      - 'svc_backup'
      - 'veeam'
  condition: sel and not filter_legit
level: high
```

PsExec Fan-out

```
title: PsExec Lateral Movement Burst
detection:
  sel:
    EventID: 4688
    NewProcessName|contains: 'psexec'
  condition: sel
level: high
```

8.6 Linux / ESXi telemetry (Auditd, syslog, OSQuery)

A) Linux: suspicious archiving & exfil

- **Auditd rule idea**: watch execve of `7z`, `zip`, `tar`, `scp`, `rsync` by non-backup users.

```
-w /usr/bin/7z -p x -k exec -F auid>=1000 -k qlin_archive
-w /usr/bin/rsync -p x -k qlin_exfil
```

- **OSQuery** (process open sockets with large egress):

```
SELECT p.pid, p.path, s.remote_address, s.remote_port, s.family
FROM processes p JOIN process_open_sockets s USING (pid)
WHERE p.name IN ('rsync','scp','rclone') AND s.family = 2 AND s.remote_port IN (22,443);
```

B) ESXi host indicators (via syslog/agent)

- Monitor `esxcli vm process list/kill`, mass changes under `/vmfs/volumes`, and service stops for backup agents:

```
grep -Ei "esxcli vm process (list|kill)|/vmfs/volumes|hostd.*stop|vpxa.*stop" /var/log/*
```

8.7 Network detections (Zeek / Suricata)

A) Steady large HTTPS egress to rare IPs (Zeek)

```
event connection_state_remove(c: connection) {
  if ( c$resp_h !in Site::local_nets && c$service == "ssl" && c$orig_ip_bytes > 100000000
)
    print fmt("Large egress SSL %s -> %s bytes=%s", c$id$orig_h, c$id$resp_h,
c$orig_ip_bytes);
}
```

B) Suricata – Tor bootstrap heuristics (generic)

Use Emerging Threats rules for Tor; additionally alert on **new JA3 hashes** with large upload volume to first-seen IPs:

```
alert tls any any -> any any (msg:"Large TLS Egress to New JA3";
flow:established,to_server;
tls.sni; content:""; depth:0; byte_test:10,>,10000000,tls.app_data_len; classtype:policy-
violation; sid:990001;)
```

(Tune thresholds; enrich with threat-intel "new_external" tag.)

8.8 High-signal correlation ideas

- **Archive + Shadow Delete Window:** same host creates ≥2 archives **and** executes `vssadmin` within 30 minutes → **HIGH**.
- **rclone + New External ASN:** first-time `rclone.exe` to IPs never seen in 90 days → **HIGH**.
- **PsExec Fan-Out + Event Log Clear:** PsExec across ≥3 servers followed by `wevtutil cl` → **CRITICAL**.
- **ESXi VM Stops + File Write Spike on vmfs:** prior to ransom note appearance → **CRITICAL**.

8.9 Autonomous response (where appropriate)

- **Auto-isolate** host on: `vssadmin delete shadows` **AND** `rclone` within 60 min.
- **Block egress** to destination with **new ASN + >1 GB upload** from a server role.
- **Snapshot DCs/File servers** when archive creation surges are detected (pre-encryption containment).
- **Disable newly created tasks/services** that appear within the incident window.

8.10 Analyst playbook (90-minute sprint)

T+0–15 min: Identify patient-zero host → isolate network; collect memory + triage artifacts (binary, ransom note, scheduled tasks).
T+15–45 min: Hunt for archive creation, `rclone/7z`, VSS deletion, PsExec bursts across all servers; block outbound to rare IPs.
T+45–75 min: Scope domain: recent privileged logins from new geos/ASNs; inter-server RDP; ESXi activity.

T+75–90 min: Contain: disable suspicious tasks/services; rotate creds for impacted service accounts; validate backup integrity; engage legal/PR per comms plan.

8.11 What “good” looks like (dashboards)

- **Staging Monitor:** per-server archive creations (1h bins), rclone executions, bytes-egress top N.
- **Recovery Guard:** shadow-delete events, backup service stops, tamper alerts.
- **Identity Heatmap:** privileged logins by ASN/geo/time with baseline deviation scoring.
- **Lateral Movement Lens:** PsExec service creations, inter-server RDP/SSH edges, SMB session fan-out.
- **ESXi Panel:** VM stop/kill events, vmfs write rates, ESXi admin logins by source.

8.12 Caveats

- Expect **false positives** from legit backups/ops. Whitelist **service accounts** and backup windows.
- Qilin affiliates swap tools; keep **behavioral focus** and update thresholds regularly.
- Combine **endpoint + network + identity** telemetry for highest confidence.

9. Remediation & Recovery

This chapter outlines the **immediate, short-term, and long-term response** activities following a Qilin (Agenda) ransomware incident.
It integrates **technical containment**, **forensic best practices**, and **organizational coordination** aligned to **ISO 27035**, **NIS2**, and **DORA** response frameworks.
The goal is not only to restore operations but to preserve evidentiary integrity, disrupt adversary persistence, and prevent reinfection or re-extortion.

9.1 Incident Response Priorities

Primary objectives during the first 24 hours:

1. **Containment:** Stop encryption and exfiltration from spreading.
2. **Preservation:** Secure volatile evidence for later forensic and legal use.
3. **Continuity:** Restore minimal business functionality without contaminating clean systems.
4. **Communication:** Maintain disciplined, confidential internal and external messaging.
5. **Decision-making:** Establish a command structure for ransom, disclosure, and recovery decisions.

Qilin attacks often include double extortion, data publication threats, and "Call-Lawyer" intimidation tactics. Victims must anticipate negotiation and data-leak pressure, even after containment.

9.2 Immediate Containment Steps (T+0 to T+4 hours)

1. Isolate affected systems

- Disconnect compromised endpoints from the network—**do not power them off** yet.
- For virtualized infrastructure (VMware ESXi, Hyper-V), disconnect network interfaces or isolate vSwitches.
- Prevent lateral movement by blocking SMB (445/TCP), RDP (3389/TCP), SSH (22/TCP), and known exfil paths.

2. Suspend scheduled tasks & backup jobs

- Stop automated backup replication to prevent encrypting or overwriting clean copies.
- Mount recent off-site snapshots read-only.

3. Preserve volatile data

- Acquire memory (RAM) and live triage images of representative hosts.
    - Focus on servers that initiated mass encryption or outbound transfers.
    - Collect: running processes, open network connections, logged-in users, scheduled tasks, registry hives.
- Preserve firewall, proxy, and VPN logs for 72h prior to encryption onset.

4. Disable compromised accounts

- Immediately disable **service accounts**, **domain admin accounts**, and any accounts used on exfiltration hosts.
- Rotate privileged credentials and revoke Kerberos tickets.

5. Contain exfiltration and leak channels

- Block known C2 / exfil nodes (rclone, WinSCP destinations, Tor proxies).
- If you operate an enterprise proxy, filter outbound to known **bulletproof hosting ASNs** and **Tor gateways**.
- Notify SOC to monitor for any DNS over HTTPS (DoH) anomalies.

6. Notify internal stakeholders

- Activate the incident-response plan.
- Escalate to CISO, DPO, Legal, Communications, and relevant department heads.
- Maintain *need-to-know* principle — Qilin affiliates monitor leaks and sometimes infiltrate victim networks' email systems.

9.3 Forensic Preservation (T+4 to T+12 hours)

Data collection:

- Full disk images of:
  - Patient-zero system (initial infection).
  - File servers with ransom notes or encrypted files.
  - Systems showing rclone/7z/WinSCP activity.
- Copy ransom notes, log entries, registry exports, scheduled task XML files.
- Export Windows Event Logs (Application, System, Security) and EDR telemetry.
- On Linux/ESXi: collect `/var/log`, `/etc/cron*`, `/vmfs/volumes`, `/etc/shadow`, `/etc/passwd`.

Chain of custody:

- Use verifiable hashing (SHA256) on all collected artifacts.
- Document acquisition process and timestamps for legal admissibility.
- Maintain separation of forensic images and operational backups.

Avoid contamination:

- **Do not install tools** on compromised systems. Run portable, trusted utilities.
- Avoid using corporate credentials during containment actions.

9.4 Communication and Escalation

Internal

- Initiate incident bridge (IR war room).
- Ensure consistent messaging to executives: include confirmed scope, estimated impact, and next steps.
- Keep all internal communications **off potentially compromised systems**; use alternate channels (Teams tenant isolation or out-of-band comms).

External

- **Law enforcement:** Engage national CERT and local cybercrime units (e.g., Europol EC3, FBI, NCA).
- **Regulators:** Under NIS2/GDPR, report within 72 hours if personal data affected.
- **Customers/Partners:** Prepare templated notifications pending forensic confirmation.
- **Media:** Coordinate with Legal & PR. Avoid confirming or denying ransom claims until validated.

Negotiation (if applicable)

- Qilin affiliates may open Tor-based chat panels within hours of encryption.
- Engage **experienced ransomware negotiators** only via legal counsel.
- Do not communicate directly without legal/LE guidance.
- Maintain copies of all correspondence (for extortion-law compliance).
- Evaluate insurance requirements before engaging in dialogue.

9.5 Short-Term Recovery (T+12 to T+72 hours)

1. Eradicate persistence

- Remove malicious scheduled tasks, services, registry keys.
- Verify no hidden or renamed binaries remain (use hashes and baselines).
- Inspect for secondary payloads (info-stealers, backdoors). Qilin affiliates sometimes deploy **Cobalt Strike, Sliver, or Metasploit** frameworks prior to encryption.

2. System restoration

- Rebuild critical servers from **gold images** or **immutable snapshots**.
- Validate backups offline:
  - Scan backups with updated AV/EDR signatures.
  - Compare hashes with known-clean baselines.
  - Test restore integrity in isolated environment.
- Prioritize: domain controllers → file servers → application servers → endpoints.

3. Network hygiene

- Reset Kerberos TGTs and domain passwords.
- Force global MFA re-enrollment.
- Audit for new trust relationships or replication partners.

4. Leak-site monitoring

- Track Qilin's Tor site and mirrors for postings referencing your organization.
- If data appears, capture screenshots and URLs as evidence; **do not attempt to engage** via these portals.

- Coordinate with law enforcement and legal counsel before public acknowledgment.

5. Infrastructure hardening

- Segment critical systems; implement jump servers for administration.
- Review firewall ACLs, RDP/VPN exposure, and management interface restrictions.
- Disable legacy authentication protocols (NTLMv1, LM, insecure SMB).

9.6 Long-Term Strategic Recovery (Post-Incident Weeks)

Governance & Policy

- Review incident in line with **ISO/IEC 27035** post-incident phase.
- Update **Business Continuity Plan (BCP)** and **Disaster Recovery (DR)** based on actual timelines.
- Conduct **lessons-learned workshop**: technical, procedural, and communication failures.

Regulatory & Legal

- Prepare documentation for NIS2/DORA reporting:
  - Timeline of detection and response.
  - Impacted systems and data classification.
  - Measures implemented to prevent recurrence.
- Maintain all evidence for potential prosecution or insurance claims.

Infrastructure Improvements

- Deploy **EDR/XDR** with centralized telemetry correlation.
- Enable **Sysmon** or equivalent for persistent event capture.
- Implement **application allowlisting** (e.g., WDAC/AppLocker).
- Require **MFA** for all privileged accounts and VPN access.
- Harden backup infrastructure (air-gapped, immutable, offsite).

Employee Awareness

- Conduct targeted **security awareness refresh** for staff.
- Reinforce phishing simulations and incident reporting channels.
- Brief executives on extortion trends and crisis communication protocols.

Threat Intelligence Integration

- Subscribe to **Ransomware and RaaS feeds** (CISA, MISP, commercial TI).
- Implement continuous dark-web monitoring for stolen credentials and Qilin data leaks.
- Build custom SIEM correlations for Qilin IOCs from Chapter 6.

9.7 Decision Guidance on Ransom Payments

Consideration	Analysis
Data Value	Assess recoverability from backups and business continuity impact.
Legal Risks	Payments to sanctioned entities may violate regulations (OFAC, EU). Verify with counsel.
Reputation	Payment may not prevent leak; Qilin has previously leaked partial data post-payment.
Decryption Reliability	Decryptors from Qilin affiliates generally functional but can corrupt files if mishandled.
Future Exposure	Paying may flag your organization as a "payer" in underground forums.

Recommendation: Do not pay unless directed by legal counsel and after verifying sanctions compliance and negotiation legitimacy.

9.8 Forensic Closing Checklist

Step	Responsible	Status
Memory and disk images preserved	DFIR lead	☐
Account resets completed	IAM / AD Admin	☐
C2 and exfil IPs blocked	SOC	☐
Leak site monitored	Threat Intel	☐
Restores verified clean	Backup team	☐
Post-incident report drafted	IR Manager	☐
Regulatory notifications filed	Compliance	☐

9.9 Key Lessons Learned from Prior Qilin Cases

1. **Credential theft precedes encryption** — implement continuous identity analytics and impossible-travel detection.
2. **Data staging is visible** — early detection of large archive creation (7z/rclone) can prevent encryption.
3. **Backups are often accessible** — isolate backup networks and enforce MFA.
4. **Qilin's leak threat is real but not immediate** — some leaks occur weeks later; maintain monitoring long after recovery.
5. **Communication discipline matters** — missteps in disclosure can worsen reputational damage more than the attack itself.

9.10 Long-Term Hardening Recommendations

Area	Action
Identity Security	Enforce conditional access, MFA, passwordless login, privileged access workstations.
Network Segmentation	Split production, management, and backup planes. Block lateral RDP/SMB between zones.
Patch Management	Patch backup products (esp. Veeam CVE-2023-27532) and remote management tools.
Logging & Telemetry	Centralize logs in SIEM with 90+ day retention.
Threat Intel Integration	Automate ingestion of ransomware IOCs and leak monitoring.
Crisis Preparedness	Rehearse tabletop exercises quarterly, simulate double extortion scenario.

9.11 Alignment with NIS2 & DORA

Requirement	Qilin-Relevant Control
NIS2 – Art. 21(2): Incident handling	Maintain IR plan with defined escalation matrix.
NIS2 – Art. 23: Reporting obligations	Notify within 24h (early warning) and full report within 72h.
DORA – Art. 17(3): ICT incident classification	Define “major” ransomware event trigger points for financial entities.
DORA – Art. 18(1): Post-incident review	Conduct lessons-learned and integrate into risk management framework.

9.12 Summary

The response to Qilin must be **structured, evidence-driven, and resilient**.
While the group’s operations are highly automated, its tactics still rely on predictable human lapses — unmonitored credentials, exposed services, and flat networks.
A disciplined response that balances **technical containment** with **strategic communication** can limit operational disruption, reduce regulatory exposure, and deny the adversary leverage.

10. Long-Term Strategic Recommendations

Purpose

This chapter translates tactical lessons from the Qilin ransomware campaigns into **strategic, organization-wide actions**.
It bridges **technical response** (as covered in Chapter 9) with **policy, governance, and ecosystem collaboration**, ensuring long-term cyber resilience.
The recommendations align with **NIS2**, **DORA**, and **ISO/IEC 27001:2022**, addressing risk management, incident readiness, threat intelligence integration, and collective defense.

10.1 Strategic Objective

To transform reactive crisis management into **predictive resilience**, by embedding intelligence-led, regulatory-aligned, and measurable security capabilities that withstand sophisticated RaaS operations like Qilin.

10.2 Ransomware as a Strategic Risk

Ransomware has transcended technical boundaries — it is now a **business continuity, reputational, and regulatory challenge**.
Groups like Qilin operate with corporate discipline: structured affiliate programs, service-level guarantees, and data-leak marketing campaigns.
Consequently, organizations must treat ransomware as a **strategic risk**, not merely a security incident.

Key takeaways:

- Ransomware impacts **C-suite decisions** (brand, compliance, customer trust).
- Traditional IT recovery plans (RTO/RPO) are insufficient without **data-leak containment strategies**.
- A **whole-of-organization posture**—including legal, HR, PR, and supply chain—is required.

10.3 Governance and Policy Framework

10.3.1 Board-Level Cyber Risk Oversight

- Establish a **Cyber Risk Committee** reporting to the board quarterly.
- Integrate ransomware risk within the enterprise risk register.
- Require annual tabletop exercises for executives simulating a **double-extortion event**.
- Include ransomware resilience KPIs (backup immutability, patch latency, MFA coverage).

10.3.2 Policy Updates

- Update **Information Security Policy** to include:
    - Ransomware response chain of command.

    - Restrictions on ransom payment decisions.
    - Criteria for public disclosure and regulator engagement.
- Embed **Zero Trust Architecture** principles in the organization's Security Policy Framework.

10.3.3 Compliance Integration

- Map ransomware preparedness controls directly to:
    - **NIS2 Articles 21–23** (Incident Handling, Reporting).
    - **DORA Articles 17–20** (Operational Resilience & Reporting).
    - **ISO 27001 Annex A Controls A.5–A.18** (Information Security Management).

10.4 Strategic Technical Roadmap (2025–2027)

Timeframe	Initiative	Objective
Short-term (0–6 months)	Deploy continuous monitoring (EDR/XDR/SIEM), implement privileged access management (PAM), and harden backups with immutability and MFA.	Reduce dwell time and prevent encryption spread.
Medium-term (6–18 months)	Implement Zero Trust segmentation (ZTA), integrate SOAR for automated containment, and enable centralized identity analytics (UEBA).	Stop lateral movement and accelerate response.
Long-term (18–36 months)	Build full **Cyber Resilience Framework**: threat-hunting program, red teaming, supply-chain risk scoring, and sectoral intelligence sharing.	Institutionalize predictive defense and cross-sector collaboration.

10.5 Information Sharing and Threat Intelligence Collaboration

10.5.1 Join Sectoral ISACs / CSIRTs

- Participate in your national or EU-level **Information Sharing and Analysis Center (ISAC)** for your sector (Finance, Energy, Health, etc.).
- Share anonymized IOCs, TTPs, and post-incident reports following **TLP:AMBER/GREEN** protocols.
- Example: Qilin-related exfil domains and leak mirrors can provide early-warning cross-pollination between members.

10.5.2 Leverage Government and Industry Feeds

- Subscribe to CISA, ENISA, and Europol advisories for ransomware activity.
- Integrate commercial threat intelligence (MISP, Recorded Future, CrowdStrike Intelligence) into your SIEM.
- Automate ingestion of **YARA/Sigma rules** from trusted CTI vendors.

10.5.3 Share Responsibly

- Use standardized frameworks (STIX/TAXII) for intelligence exchange.
- Maintain anonymity and legal compliance (GDPR Article 49(1)(d) exception for cybersecurity information exchange).

10.6 Organizational Preparedness and Workforce Development

10.6.1 Incident Response Training

- Conduct **quarterly IR exercises** involving not only SOC analysts but also executives, communications, and legal teams.
- Include *double-extortion* and *data-leak* scenarios reflecting Qilin's tactics.
- Measure performance using RTO, MTTD, and MTTR metrics.

10.6.2 Security Awareness Program

- Tailor awareness campaigns to user roles:
  - Finance & HR: handling invoices, payroll phishing.
  - IT: remote access hygiene and patch management.
  - Executives: media crisis handling and ransom decision matrix.
- Reinforce phishing simulations tied to Qilin-style social engineering.

10.6.3 Talent Retention

- Create incentives for cybersecurity retention — continuous learning budgets, CTI certifications (GCTI, GCFA, GREM).
- Encourage rotation between SOC, IR, and governance teams to avoid silos.

10.7 Supply Chain and Third-Party Security

10.7.1 Vendor Risk Governance

- Introduce contractual requirements for incident notification (within 24 hours).
- Mandate MFA, EDR, and encrypted data transit for all vendors.
- Perform annual penetration tests on third-party integrations.
- Assess supplier backup strategy — shared responsibility for immutability.

10.7.2 Cloud & Managed Service Providers

- Audit cloud configurations for overexposed management interfaces.
- Require providers to implement geo-fencing and anomaly-based access control.
- Request **shared responsibility statements** aligned with ISO/IEC 27017 and 27018.

10.7.3 Continuous Vendor Monitoring

- Subscribe to risk scoring platforms (BitSight, SecurityScorecard).
- Monitor vendors for public ransomware disclosures on dark-web trackers.

10.8 Defensive Architecture Enhancements

Control Domain	Recommendation	Expected Outcome
Identity & Access	Implement **Conditional Access Policies**, passwordless authentication, just-in-time admin elevation.	Reduce credential theft surface exploited by Qilin affiliates.
Network Segmentation	Apply **micro-segmentation** (Zscaler, Illumio, Palo Alto ZTNA).	Contain lateral movement.
Endpoint Protection	Deploy **EDR/XDR** with behavioral detection (MITRE ATT&CK coverage for T1059, T1486, T1562).	Detect early execution of encryptors and tooling.
Data Backup	Adopt **3-2-1-1-0** model (3 copies, 2 media, 1 offsite, 1 immutable, 0 errors).	Ensure recoverability even under double extortion.
Email Security	Use AI/ML-based content analysis and DMARC enforcement.	Block Qilin's phishing/credential theft vectors.
Logging & Telemetry	Centralize with SIEM (Elastic, Sentinel, Splunk) and 90-day retention.	Enable retrospective forensics.
Application Hardening	Whitelist approved binaries, block unsigned code.	Prevent affiliate tools from executing.

10.9 Strategic Communications and Reputation Management

10.9.1 Crisis Communication Framework

- Develop **pre-approved public statements** for ransomware events.
- Maintain media holding statements that acknowledge investigation without attribution.
- Designate a single spokesperson to prevent contradictory messaging.

10.9.2 Transparency and Trust

- Communicate early with regulators and affected customers once impact verified.
- Transparency mitigates speculation and maintains stakeholder confidence.
- Avoid overpromising on recovery timelines until technical validation complete.

10.9.3 Brand Monitoring

- Track social media and dark-web mentions of your brand using OSINT tools.
- Coordinate with digital forensics to confirm authenticity before reacting.

10.10 Strategic Metrics and KPIs

Metric	Target	Description
Mean Time to Detect (MTTD)	< 30 minutes	Time from anomaly to alert acknowledgment.
Mean Time to Contain (MTTC)	< 2 hours	From alert triage to host isolation.
Backup Integrity Verification	Weekly	Automated checksum validation of backups.

Metric	Target	Description
Patch Latency	< 14 days	Average time to deploy critical security patches.
MFA Adoption	100% for privileged accounts	Prevent credential-based intrusions.
Phishing Simulation Failure Rate	< 3%	Gauge user awareness effectiveness.

These metrics provide a quantifiable roadmap for resilience maturity benchmarking.

10.11 Sector-Level Recommendations

Public Sector

- Establish **inter-agency SOC cooperation** for ransomware early warning.
- Include ransomware containment in civil contingency exercises.
- Adopt a **"no single point of failure"** architecture for essential services (e.g., healthcare, taxation).

Private Sector

- Create **cyber insurance readiness documentation**: incident logs, control audits, response playbooks.
- Engage managed threat-hunting providers for 24/7 coverage.
- Embed cyber resilience clauses into supplier SLAs.

Critical Infrastructure

- Conduct **scenario-based red teaming** simulating ransomware at SCADA/ICS level.
- Segment OT/IT networks with strict firewall zoning.
- Ensure manual override procedures for critical processes.

10.12 Collaboration with Law Enforcement and Regulators

- Build **trusted channels** with your national CERT, sector CSIRT, and local police cyber units **before** incidents occur.
- Contribute anonymized forensic findings to Europol's **No More Ransom** initiative.
- Share IOCs with ENISA or national centers under **TLP:GREEN** classification.
- Participate in **joint exercises** to refine cross-border ransomware response.

10.13 Forward-Looking Threat Intelligence

- Expect **Qilin fragmentation**: affiliates may splinter into new brands (similar to LockBit → RansomHub evolution).

- Monitor for rebranding keywords (“Agenda2”, “LawQil”, etc.) in dark-web forums.
- Track **new extortion channels** — Telegram leaks, ClearNet data shaming, and media contact attempts.
- Use AI-driven **attack path simulation** tools to test resilience against Qilin’s TTPs quarterly.

10.14 Long-Term Cyber Resilience Vision

1. **Predictive Defense:** AI-enhanced threat modeling, continuous red teaming, autonomous SOAR containment.
2. **Digital Sovereignty:** Encryption key management under national jurisdiction; trusted supply chains.
3. **Sectoral Resilience Grid:** Federated SOC collaboration among peers sharing telemetry under secure enclaves.
4. **Public-Private Symbiosis:** Real-time intelligence exchange between enterprises and government CERTs.
5. **Culture of Preparedness:** Security as a shared responsibility embedded in every function.

10.15 Summary

Long-term resilience against ransomware is achieved when **cybersecurity governance, intelligence, and operations converge**.
The Qilin campaigns underline that **preparedness is not a luxury—it is an operational necessity**.
Organizations that integrate continuous monitoring, rapid decision-making, and proactive collaboration will withstand future RaaS evolutions far more effectively.

Strategic Imperative:

Move from “respond and rebuild” to “predict and prevent.”
Treat cyber resilience as a living capability, not a project.
Ensure that ransomware—whatever its name or rebrand—never dictates your operational tempo again.

11. References & Further Reading

This section provides the **primary and secondary sources** used to support analytical findings throughout this report, as well as recommended materials for continued intelligence monitoring and technical validation.
All sources have been reviewed for reliability, relevance, and contemporaneity as of **October 16, 2025**.
Citations include **vendor technical advisories**, **government alerts**, **dark-web intelligence observations**, and **academic literature**.

11.1 Primary Intelligence Sources

Vendor & Industry Reports

1. **Cyfirma (October 2025)** – *"Qilin: Rising Power of a RaaS Empire"*
   - Quantitative analysis of Qilin's 2025 victim surge (81–86 confirmed cases in June 2025).
   - Detailed affiliate structure and leak-site infrastructure mapping.
2. **HHS Health Sector Cybersecurity Coordination Center (HC3), 2025** – *"Qilin Ransomware Profile"*
   - Overview of infection vectors, victimology, and healthcare sector impact.
   - Confirms observed use of phishing and stolen credentials for initial access.
3. **SentinelOne Labs (2025)** – *"Qilin Ransomware Technical Breakdown: From Agenda to Industrial Powerhouse"*
   - In-depth reverse engineering of Go and Rust payloads.
   - Analysis of configuration parameters, encryption routines, and Rust-based ESXi variants.
4. **Group-IB Threat Intelligence (2024–2025)** – *"The RaaS Ecosystem After LockBit: Qilin's Consolidation Strategy"*
   - Strategic mapping of affiliate migrations and infrastructure reuse across post-LockBit and RansomHub collapses.
5. **Darktrace Threat Research (2025)** – *"Psychological Extortion: The 'Call-Lawyer' Method in Qilin Campaigns"*
   - Analysis of Qilin's extortion psychology and social engineering approach.
6. **Resecurity (2025)** – *"Bulletproof Hosting Infrastructure Supporting Qilin RaaS"*
   - Attribution of hosting nodes across Russia, Iran, and Southeast Asia.
   - Correlation with Tor mirrors and C2 redundancy patterns.
7. **Picus Security (2025)** – *"Attack Simulation Insights: Mitigating Qilin's Double-Extortion Tactics"*
   - MITRE ATT&CK mapping validation and detection efficacy metrics.
8. **Dragos Industrial Cyber Intelligence (2025)** – *"ICS/OT Ransomware Trends: Qilin's Entry into Industrial Environments"*
   - Statistical data indicating Qilin responsible for ~19% of industrial ransomware incidents in 2025.
9. **Qualys Threat Advisory (2025)** – *"Cross-Platform Go Payloads Used by Qilin Affiliates"*
   - Confirms cross-compilation and selective anti-analysis routines.
10. **SANS Internet Storm Center (2025)** – *Community intelligence briefs and incident case studies* corroborating observed tactics and IOC patterns.

11.2 Governmental & CERT Publications

1. **CISA / FBI / MS-ISAC Joint Cybersecurity Advisory (CISA-AA25-178A)**

    - *"Indicators and Mitigation for Modern RaaS Platforms (Qilin Focus Section)"*
    - Released July 2025; provides validated IOCs and remediation steps.
2. **ENISA Threat Landscape Report 2025 (Chapter 3: Ransomware Consolidation)**
    - Comprehensive overview of European ransomware trends; highlights Qilin's dominance post-LockBit.
3. **Europol EC3 / No More Ransom Initiative (2024–2025)**
    - Repository of decryption tools and RaaS taxonomy; incident coordination templates.
    - No functional decryptor available for Qilin as of report date.
4. **CERT-EU Flash Alert 2025-10** – *"Mass Disclosure Events by Qilin Affecting EU Entities"*
    - Analytical breakdown of 14–15 October 2025 mass postings (Volkswagen France, Agencia Tributaria, others).
5. **Australian Cyber Security Centre (ACSC)** – *Advisory: "Agenda/Qilin Ransomware Targeting Critical Sectors" (2023–2024)*
    - Early identification of Agenda-to-Qilin rebrand and spread into APAC.
6. **Japan CERT (JPCERT/CC)** – *Advisory: "Qilin Ransomware Campaigns Impacting Japanese Enterprises" (October 2025)*
    - Verification of Asahi Group Holdings intrusion.

11.3 Academic and Research Papers

1. **T. Laufer, L. Gatzen, et al. (2024)** – *"Industrialisation of Ransomware: Comparative Study of RaaS Economics"*, IEEE Symposium on Security & Privacy.
    - Academic model correlating affiliate payout models and operational resilience.
2. **B. L. McEwen, et al. (2023)** – *"Psychological Warfare in Digital Extortion: Narrative Framing and Victim Response."*
    - Framework explaining Qilin's use of pseudo-legal intimidation.
3. **NIST SP 1800-25 (2024)** – *"Data Integrity: Identifying and Recovering from Ransomware and Other Destructive Events."*
    - Technical controls directly relevant to post-incident restoration (used in Chapter 9).

11.4 Dark-Web and OSINT Monitoring

Leak Sites & Communication Channels

- **Qilin Tor leak portal** (active mirrors observed 2023–2025).
    - Structured HTML templates with countdown timers, proof-of-data archives, and "Call-Lawyer" contact references.
- **Telegram channels** affiliated with Qilin and related data brokers, used for sample promotion and recruitment.
- **Underground forum advertisements (Exploit, XSS)** recruiting affiliates in Russian and English between May 2023–May 2025.

Analyst Observation Notes

- Persistent uptime across mirrored leak domains.
- Automated post publishing indicates backend CMS integration.

- Mass-post events (e.g., Oct 15 2025) correlate to system-wide publication triggers, not manual updates.

11.5 MITRE ATT&CK Mapping References

- **MITRE ATT&CK for Enterprise v14.1 (October 2025)** – Reference model for Chapters 5 & 8.
- Technique coverage cross-verified with:
  - SANS ATT&CK Navigator.
  - SigmaHQ mappings for T1059, T1486, T1562, and T1490.
  - Elastic and Microsoft ATT&CK integration guides.

11.6 IOC & Detection Feeds (Operational Updates)

Feed	Type	Access
CISA Known Exploited Vulnerabilities Catalog	CVE and IOC correlation	https://www.cisa.gov/known-exploited-vulnerabilities-catalog
MISP Community Feed (Qilin tag)	Hashes, domains, Tor URLs	`misp-project.org/feeds`
VirusTotal Intelligence	Binary samples (Agenda, Qilin variants)	Subscription
Anomali ThreatStream / Recorded Future	Commercial CTI	Subscription
ransomware.live / RansomWatch	Open-source leak monitoring	Public
Cyber Threat Alliance (CTA)	Cross-member IOC exchange	Member-only

---

11.7 Legal and Regulatory Framework References

- **NIS2 Directive (EU) 2022/2555**, Articles 21–23 — Incident handling and notification obligations.
- **DORA Regulation (EU) 2022/2554**, Articles 17–20 — ICT-related incident classification and reporting.
- **ISO/IEC 27035-1:2023** — Incident management principles.
- **ISO/IEC 27001:2022** — Annex A controls related to ransomware resilience.
- **GDPR Article 33** — Personal data breach notification.
- **OFAC Sanctions Advisory (U.S. Treasury, 2023)** — Guidance on ransom payments to sanctioned entities.

11.8 Recommended Continuous Learning

1. **SANS SEC504 / FOR528** – Hands-on incident response & ransomware investigations.

2. **MITRE ATT&CK Defender (MAD) – Ransomware Threat Hunting** certification.
3. **ENISA Cyber Exercises (BlueOlex, Cyber Europe)** – EU-wide cross-sector crisis simulation.
4. **CISA Tabletop in a Box (TTX)** – Templates for ransomware tabletop exercises.
5. **The No More Ransom Project** – Public decryptor repository and best practices.

11.9 Attribution Confidence Model

Each section of this report was derived using a multi-source fusion model with the following grading:

Confidence Level	Definition	Example
High	Corroborated by ≥2 independent primary sources and direct telemetry	Infection vectors, 2025 victim surge
Moderate	Supported by single credible vendor or partial forensic confirmation	Affiliate structure, hosting regions
Low / Speculative	Based on unverified OSINT or dark-web claims	Leadership identity, internal hierarchy

11.10 Acknowledgements

This report was developed using aggregated intelligence from:

- Public-private CTI partnerships.
- Threat-sharing communities under **TLP:AMBER**.
- Contributions from **cyber incident responders, SOC analysts, and CTI researchers** across multiple sectors.

Special recognition to open-source contributors who maintain transparency in ransomware tracking initiatives.

11.11 Analyst Note

Ransomware intelligence is **perishable**.
Indicators, infrastructure, and group branding evolve monthly.
For sustained defense:

- Integrate continuous feed ingestion into SIEM.
- Review this report quarterly for updates.
- Participate actively in your national or sectoral intelligence exchange.

About Ransomwared

Ransomwared is a European-based cybersecurity initiative committed to protecting organizations against the evolving threat of ransomware. Our mission is to **disrupt the economics of cyber extortion** by providing intelligence, technology, and rapid response capabilities that empower defenders to outpace attackers.

At the core of our work is a **next-generation, AI-enhanced, autonomous SOC (Security Operations Center)** that operates 24/7. This SOC continuously ingests global threat intelligence, analyzes attacker behaviors, and autonomously correlates patterns against enterprise telemetry. By leveraging **machine learning models trained on ransomware TTPs**—including those used by groups such as **Akira**—we provide real-time detection, predictive defense, and automated containment actions.

How We Stay Ahead of Threats Like Akira

- **AI-Driven Threat Intelligence**: Our models are continuously refined with data from ransomware campaigns, CVE exploit chains, and underground ecosystems, enabling proactive detection of new attack variants.
- **24/7 Autonomous SOC**: Operating around the clock, our SOC doesn't just monitor—it autonomously correlates anomalies, isolates compromised endpoints, and enforces adaptive security controls in real time.
- **Behavioral Defense**: By mapping techniques to **MITRE ATT&CK**, we detect ransomware campaigns even when adversaries change infrastructure, binaries, or ransom note formats.
- **Continuous Learning**: Every incident enriches our AI and SOC capabilities, strengthening defenses not only for individual organizations but across the entire Ransomwared community.

Our Broader Mission

- **Threat Intelligence Reports**: In-depth CTI reporting (like this Akira analysis) that provides technical, operational, and strategic insights.
- **Vulnerability-to-Exploit Correlation**: Automated pipelines that link CVEs with ransomware campaigns within hours of disclosure.
- **Resilience by Design**: Guidance for implementing Zero Trust, immutable backups, and robust incident response frameworks.

Our Vision

We believe the fight against ransomware will not be won by reacting to incidents, but by **out-automating adversaries**. By combining advanced AI, a 24/7 autonomous SOC, and a culture of open intelligence sharing, Ransomwared helps organizations move from reactive defense to **proactive resilience**—ensuring that ransomware groups like Akira lose their strategic advantage.

For more information, resources, and access to our threat intelligence services, visit:
🌐 **www.ransomwared.eu**