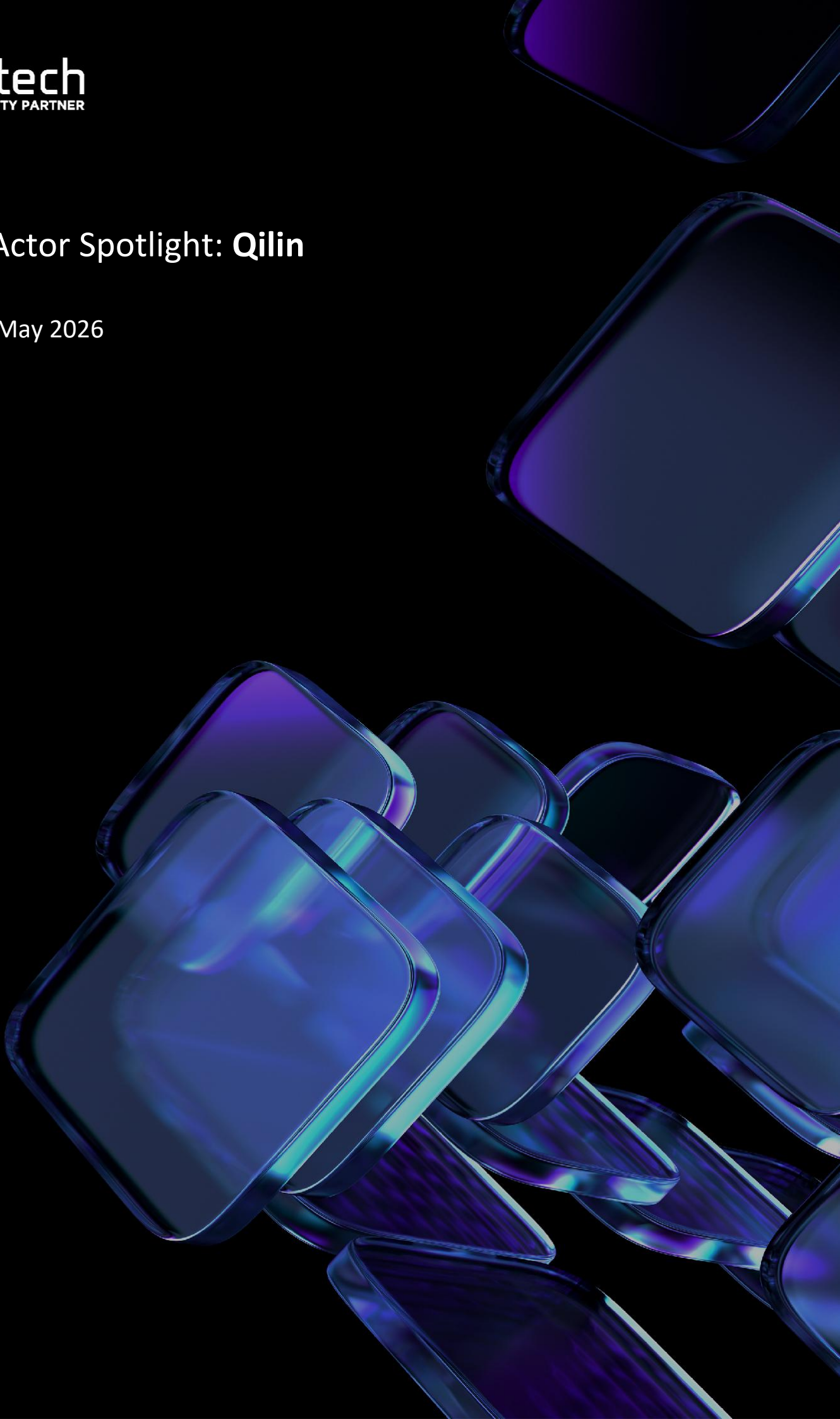
Smarttech
YOUR 24/7 SECURITY PARTNER

Threat Actor Spotlight: **Qilin**

Prepared: May 2026



Contents

Overview **3**

High-Profile Targets in 2026 ..... **5**

Healthcare — Most Consequential Incidents 5

Political / Government 5

Energy / Critical Infrastructure 6

Financial Services ..... **Error! Bookmark not defined.**

Known Exploited Vulnerabilities **6**

Recommendations **8**

References **11**

This report is based on Smarttech247-curated threat intelligence and may contain proprietary and confidential information. It must not be shared, forwarded, or entered into any Generative AI tools without Smarttech247's prior written consent.

Overview

Qilin is the #1 most prolific ransomware operation globally. Qilin is a ransomware-as-a-service (RaaS) operation active since at least 2022 and associated with financially motivated cybercriminal activity targeting organizations across multiple sectors. The group operates ransomware variants written in Go and Rust, enabling cross-platform encryption capabilities against Windows, Linux, and VMware ESXi environments.

Qilin has demonstrated continued operational activity and capabilities within the evolving ransomware ecosystem, maintaining relevance through sustained campaigns and affiliate-driven operations. While Qilin's core tradecraft remains consistent with previously observed ransomware operations, recent public reporting continues to highlight the group's active use of credential abuse, remote management tooling, BYOVD techniques, and cross-platform encryption.

Observed Tactics, Techniques, and Procedures (TTPs)

Qilin, also known as Agenda ransomware, is a persistent ransomware-as-a-service threat within the cybercrime ecosystem. The group's tooling is highly adaptable, allowing affiliates to tailor operations based on the target environment, including operating systems, enterprise services, remote access infrastructure, and virtualization platforms.

A representation of the tactics and techniques utilized by the Qilin group can be found below:

Tactic	Techniques
Initial Access	Valid Accounts, Exploit Public-Facing Application, Phishing: Spearphishing via Service
Execution	Command and Scripting Interpreter (PowerShell, Unix Shell)
Persistence	Scheduled Task/Job: Scheduled Task
Defense Evasion	Obfuscated Files or Information, Disable or Modify Tools (BYOVD)
Credential Access	OS Credential Dumping: LSASS Memory, Credentials from Web Browsers
Discovery	Network Service Discovery, System Information Discovery
Lateral Movement	Remote Services: Remote Desktop Protocol (RDP), SMB/Windows Admin Shares
Collection	Archive Collected Data: Archive via Utility

Exfiltration	Exfiltration Over Web Service: Exfiltration to Cloud Storage
Command and Control	Application Layer Protocol: Web Protocols
Impact	Data Encrypted for Impact, Inhibit System Recovery

The group systematically combines credential access, privilege escalation, and broad discovery capabilities to establish and expand footholds within enterprise environments.

Initial access is primarily achieved through exploitation of public-facing applications and services, including exposed enterprise platforms and remote access infrastructure such as Citrix and RDP. Phishing remains an additional delivery vector, leveraging both malicious attachments and links to facilitate initial compromise.

Post-compromise activity focuses on credential access and privilege escalation, including token manipulation, LSASS memory dumping via embedded tooling, and bypass of user access controls. These techniques enable escalation to domain-level privileges and support broader lateral movement.

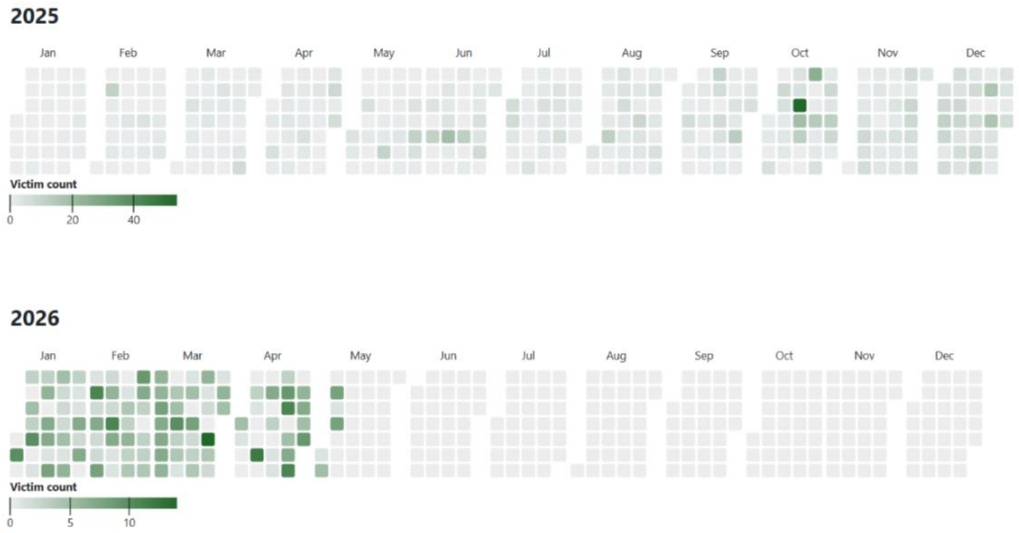
Discovery operations are extensive and automated, covering local and domain account enumeration, network share discovery, system and service discovery, and Active Directory enumeration via PowerShell. Additional capabilities include virtual machine and infrastructure awareness, particularly in VMware ESXi environments, indicating adaptation to virtualized enterprise infrastructures.

Lateral movement and execution are facilitated through legitimate administrative protocols and tooling, including PsExec, SMB/Windows admin shares, SSH, and remote management software such as Splashtop. Persistence is achieved through scheduled tasks and Group Policy Objects.

Impact is delivered through data encryption using strong cryptographic standards (AES-256/ChaCha20 with RSA-2048/4096 key protection). Prior to encryption, Qilin performs defensive evasion actions including deletion of shadow copies, disruption of backup and high-availability systems, and termination of security-related processes and services.

To evade detection and hinder forensic analysis, Qilin deletes logs and other artifacts that could support investigation efforts. This includes clearing event logs and removing temporary files generated during execution.

Overall, the observed TTP set reflects a well-rounded ransomware toolkit optimized for rapid privilege escalation, lateral movement, and large-scale encryption in enterprise and virtualized environments.



These heatmaps illustrate the rapid industrialization of the Qilin ransomware group. While 2025 shows periodic clusters of activity (peaking in late Q3/Q4), the 2026 data reveal a shift toward a sustained, daily operational model. By the end of Q1 2026, Qilin established itself as the most prolific global threat actor, consistently claiming over 100 victims per month. The density of the 2026 chart highlights that Qilin is no longer operating in "waves" but is maintaining a saturated level of daily compromises, making them the primary threat to the logistics and cargo sectors today.

High-Profile Targets in 2026

Healthcare — Most Consequential Incidents

London Healthcare Provider (February 2026)

Qilin gained access to a key provider in the London healthcare system, resulting in 170+ cases of patient harm, including two cases of long-term or permanent harm and one patient death. The organisation has not been publicly named. This mirrors the 2024 Synnovis pattern and signals continued targeting of NHS-adjacent infrastructure.
Covenant Health — US (Disclosed January 2026, attack May 2025)
Nearly 480,000 patients of the Massachusetts-based Catholic healthcare network began receiving breach notifications in January 2026. Qilin claimed responsibility for a May 2025 attack, alleging theft of 852GB of health data. This is a disclosure-lag example — the attack predates 2026 but its full impact (patient notifications, regulatory exposure) landed in January.
Aroostook Mental Health Services (March 2026)
Qilin posted a claim on its dark web leak site on March 24, targeting a rural community mental health organisation serving a patient population in the northeastern US. The full scope of data access had not been confirmed at time of reporting.

Political / Government

Die Linke — Germany (March 2026)

Qilin claimed responsibility for a cyberattack on Die Linke, a German left-wing political party. The party confirmed the incident on March 27, taking parts of its IT systems offline and filing a criminal complaint with authorities. Qilin threatened to leak stolen data if demands were not

met. Significance: This is a notable target-profile expansion — political parties are outside Qilin's traditional focus on manufacturing, healthcare, and professional services, and the timing (post-German election cycle) adds geopolitical sensitivity.

Energy / Critical Infrastructure

Grupo Tomza — Mexico (February 2026)
Qilin claimed an attack on Grupo Tomza, a leader in the LPG market across Central America, indicating that critical energy infrastructure remains a high-priority target for groups seeking to cause significant economic disruption. Ransom-db

Sysco – United States (May 2026)
The Qilin ransomware group claimed an attack on Sysco, one of the world's largest food distribution companies serving restaurants, hospitals, schools, airlines, hotels, and government facilities worldwide. The group published alleged internal documents, including confidential pricing lists, customer invoices, and tax-related records, while threatening to release additional data if ransom negotiations were not initiated before its deadline.

Known Exploited Vulnerabilities

2025

CVE	Impacted Product	CVSS Score
CVE-2025-42964	SAP NetWeaver Enterprise Portal Administration	9.1
CVE-2025-42980	SAP NetWeaver Enterprise Portal Federated Portal Network	9.1
CVE-2025-30012	SAP Supplier Relationship Management (SRM)	9.8
CVE-2025-49704	Microsoft SharePoint Server	8.8
CVE-2025-26633	Microsoft Windows 10 1507	7
CVE-2025-53771	Microsoft SharePoint Server	6.5
CVE-2025-0282	Ivanti Connect Secure / Policy Secure / Neurons for ZTA	9
CVE-2025-42999	SAP NetWeaver Visual Composer Metadata Uploader	9.1
CVE-2025-5777	Citrix NetScaler Application Delivery Controller	7.5
CVE-2025-31324	SAP NetWeaver	9.8
CVE-2025-53770	Microsoft SharePoint Server	9.8
CVE-2025-42966	SAP NetWeaver XML Data Archiving Service	9.1
CVE-2025-42963	SAP NetWeaver Application Server for Java Log Viewer	9.1
CVE-2025-49706	Microsoft SharePoint Enterprise Server	6.5
CVE-2025-0108	Palo Alto Networks PAN-OS	9.1
CVE-2025-49113	Roundcube Webmail	8.8
CVE-2025-24071	Microsoft Windows 10 1507	6.5
CVE-2025-32433	Cisco Cisco Products	10
CVE-2025-31161	CrushFTP	9.8

2024

CVE	Impacted Product	CVSS Score

CVE-2024-55956	Cleo Harmony before 5.8.0.24, VLTrader before 5.8.0.24, and LexiCom before 5.8.0.24	9.8
CVE-2024-21887	Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x)	9.1
CVE-2024-21893	Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) and Ivanti Neurons for ZTA	8.2
CVE-2024-4577	PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8	9.8
CVE-2024-55591	FortiOS version 7.0.0 - 7.0.16 and FortiProxy version 7.0.0 - 7.2.12	9.8
CVE-2024-21762	Fortinet FortiOS / FortiProxy multi-branch vulnerability (6.x–7.4.x / 1.x–7.4.x)	9.8
CVE-2024-26169	Windows Error Reporting Service	7.8

Generic IOCs Observed in Past Qilin Operations

Network indicators (domains)

- cloudflariz[.]com
- cloudflariz[.]com/comm.php
- cloudflariz[.]com/auload.php
- ikea0[.]com
- lebondogicoin[.]com
- gfs440n010[.]userstorage[.]mega[.]co[.]nz
- hxxp://serverlogs295[.]xyz/statweb255/index[.]php
- hxxp://servblog475[.]cfd/statweb255/index[.]php
- hxxp://demblog797[.]xyz/statweb255/index[.]php
- hxxp://admlogs457[.]cfd/statweb255/index[.]php
- hxxp://blogmstat599[.]xyz/statweb255/index[.]php
- hxxp://bloglogs757[.]cfd/statweb255/index[.]php
- hxxp://pzh1966[.]com/statweb255/index[.]php
- hxxp://mxblog77[.]cfd/777/
- serverlogs295[.]xyz
- servblog475[.]cfd
- demblog797[.]xyz
- admlogs457[.]cfd
- blogmstat599[.]xyz

- bloglogs757[.]cfd
- pzh1966[.]com
- mxblog77[.]cfd
- cloud[.]screenconnect[.]is
- cloud[.]screenconnect[.]com[.]vc
- cloud[.]screenconnect[.]com[.]so
- cloud[.]screenconnect[.]com[.]se
- cloud[.]screenconnect[.]com[.]ph
- cloud[.]screenconnect[.]com[.]ng
- cloud[.]screenconnect[.]com[.]ly
- cloud[.]screenconnect[.]com[.]cm
- cloud[.]screenconnect[.]com[.]bo
- cloud[.]screenconnect[.]com[.]am
- cloud[.]screenconnect[.]com[.]za
- cloud[.]screenconnect[.]cl
- cloud[.]screenconnect[.]eu
- cloud[.]screenconnect[.]com[.]mx

SHA-256

- a51c8fcde0bcc9fe8273f99c8b23e63ca4cd0f66b22cadd0bcb0f3adb0fa05fa
- a4e3f6633f3ececd39f0ba8c9644962bb0dd677ee0ecf22a99986d5c80e34bd7

Recommendations

1. Strengthen Preventive Controls
   - Enforce phishing-resistant MFA for VPN, VDI, RDP gateways, privileged accounts, backup consoles, and VMware vCenter.
   - Disable or tightly restrict internet-facing RDP; route administrative access through hardened jump servers.
   - Keep operating systems, VPN appliances, firewalls, hypervisors, backup platforms, and remote access tools fully patched.
   - Enable antivirus and EDR protections at all times and ensure tamper protection is enforced.
   - Enable vulnerable-driver protection such as Microsoft vulnerable driver blocklist, WDAC, or equivalent controls to reduce BYOVD risk.

- Block unauthorized remote management tools such as AnyDesk, Atera, ScreenConnect, Splashtop, TeamViewer, MeshAgent, and Remotely unless explicitly approved.
- Restrict application execution using allowlisting or application control to prevent execution from temporary folders, user profiles, downloads, and SMB shares.
- Limit administrative privileges and ensure employees operate with standard user accounts wherever possible.
- Remove standing domain administrator access and use just-in-time privileged access for administrative tasks.
- Restrict PsExec, remote service creation, and administrative share abuse to reduce ransomware propagation.
- Segment critical environments including Active Directory, backup infrastructure, VMware ESXi/vCenter, file servers, production systems, and user networks.
- Restrict use of personal or unmanaged devices on corporate networks unless strong device posture, EDR, encryption, and access controls are enforced.
- Monitor and restrict high-risk file-transfer tools such as Cyberduck, WinSCP, Rclone, MEGAsync, FileZilla, and s5cmd.

2. Build a Resilient Recovery Strategy

- Develop and regularly update the ransomware response plan covering credential compromise, RMM abuse, data exfiltration, ESXi targeting, backup disruption, and encryption.
- Maintain offline, encrypted, and immutable backups for critical systems and data.
- Test restoration procedures frequently to confirm that backups are usable and clean
- Keep backup infrastructure isolated from standard domain credentials and user networks.
- Maintain clean golden images for critical servers, endpoints, domain controllers, and recovery systems.
- Define clear recovery priorities for crown-jewel assets such as identity systems, backup platforms, ERP, EHR, file shares, VMware infrastructure, and production systems.
- Ensure backup administrators, domain administrators, and virtualization administrators use separate accounts and separate access paths.
- Monitor for backup deletion, failed backup jobs, VSS deletion, disabled backup agents, and suspicious backup-console logins.
- Preserve critical logs outside the compromised domain, including EDR, VPN, DNS, proxy, firewall, Active Directory, backup, and vCenter logs.
- Maintain an up-to-date emergency contact directory for executives, IT, security, legal, communications, cyber insurance, external incident response vendors, law enforcement, regulators, and key suppliers.
- Pre-approve crisis communication templates for employees, customers, regulators, partners, and media.
- Establish clear ransom decision-making authority, including legal, sanctions, insurance, executive, and board-level escalation.

3. Empower with Risk Awareness & Preparedness

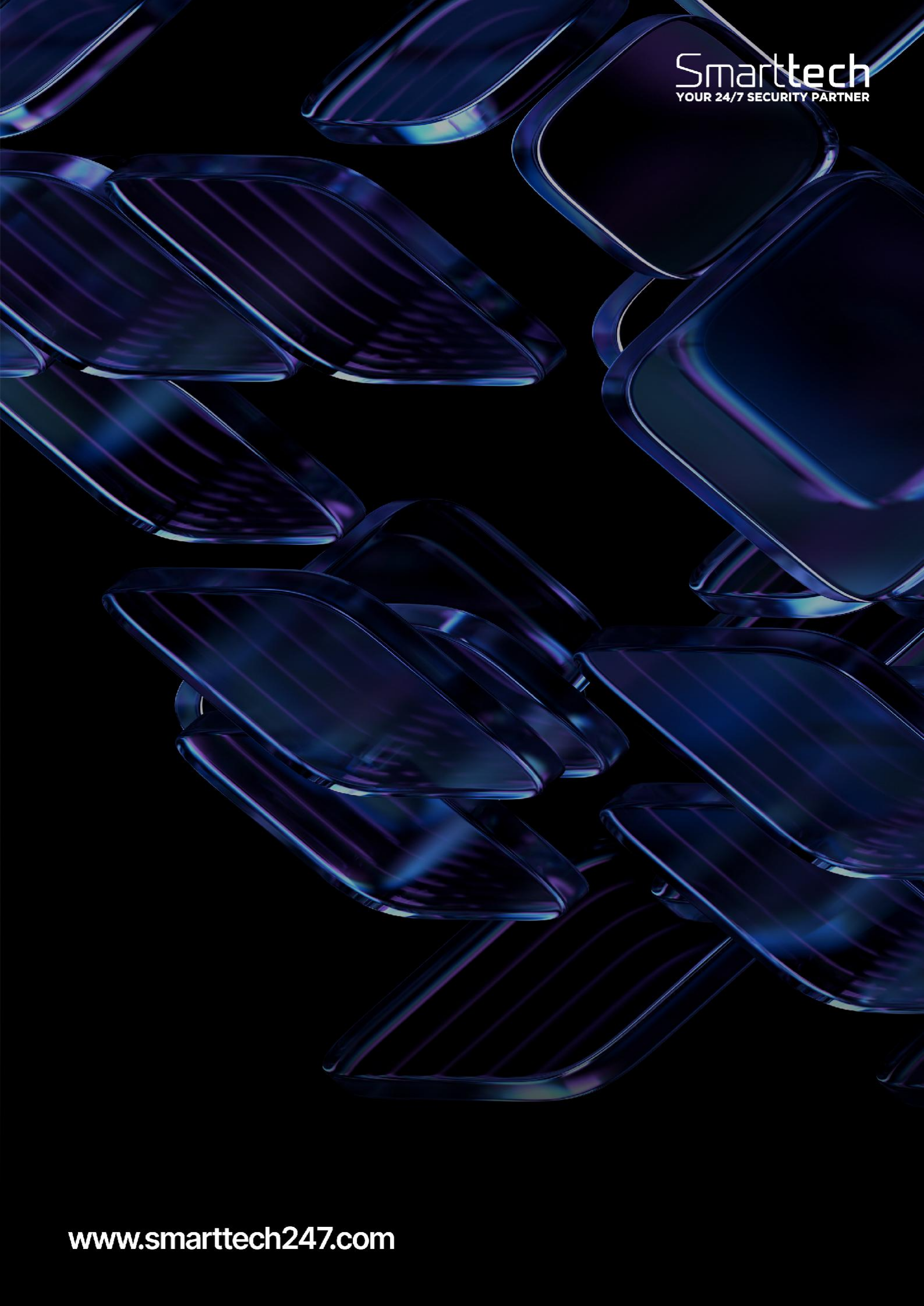
- Conduct routine tabletop exercises simulating Qilin-style ransomware scenarios, including VPN compromise, unauthorized RMM deployment, data theft, ESXi encryption, and backup disruption.
- Train employees to recognize phishing attempts, suspicious links, fake CAPTCHA pages, malicious installers, MFA fatigue attempts, and unusual system behavior.
- Train helpdesk teams to detect social engineering attempts related to password resets, MFA resets, remote access enrollment, and account recovery.
- Maintain an accurate asset inventory covering endpoints, servers, cloud assets,

VMware infrastructure, backup systems, privileged accounts, remote access tools, and critical applications.

- Maintain network flow inventories to understand how critical systems communicate and where segmentation is required.
- Identify and document crown-jewel data locations, including HR, finance, legal, customer data, patient data, source code, intellectual property, and regulated information.
- Review third-party and MSP access regularly, ensuring vendors use MFA, named accounts, least privilege, session logging, and time-bound access.
- Review ransomware readiness metrics with executive leadership, including MFA coverage, EDR health, backup restore success, privileged account count, patching SLA compliance, and RMM exceptions.

References

https://www.cisa.gov/stopransomware/ransomware-guide
https://www.scworld.com/brief/nearly-half-of-march-ransomware-attacks-in-tied-to-just-3-groups
https://www.osibeyond.com/blog/qilin-ransomware-remains-a-major-threat-to-smbs/
https://socradar.io/blog/dark-web-profile-qilin-agenda-ransomware/
https://www.cm-alliance.com/cybersecurity-blog/major-cyber-attacks-data-breaches-ransomware-attacks-in-april-2026
https://attack.mitre.org/software/S1242/
https://attack.mitre.org/groups/G1050/
https://www.breachsense.com/ransomware-reports/annual-report-2025


Smarttech
YOUR 24/7 SECURITY PARTNER
www.smarttech247.com