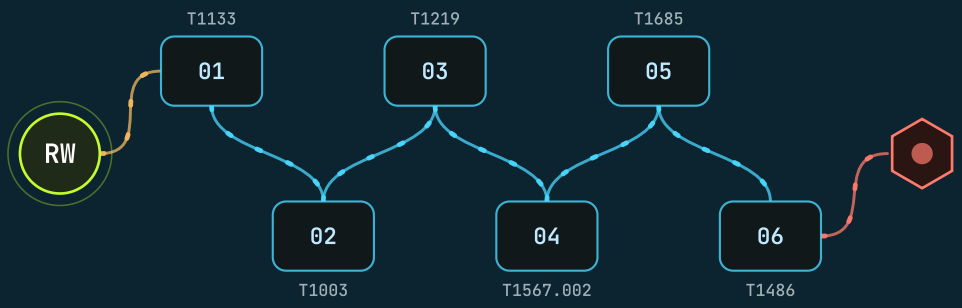



INTELLIGENCE BRIEF

# Qilin Still Tops Most Ransomware Counts after a Suspected Member's Arrest

Qilin still leads most ransomware counts and kept listing victims after Japan detained a suspected leading member in May 2026. Affiliates also exploit VPN authentication flaws. Patch VPN gateways and require MFA first.

EDITION
Fall/Winter 2026/2027 Edition
RW-01 · Ransomware group

PUBLISHED BY
Z7 Solutions LLC
Orlando, Florida

READ ONLINE
z7solutions.com
844-974-8669

# 01 At a Glance

## STATUS

**ACTIVE**

Qilin listed new victims as recently as October 13, 2026, and Ransomware.live counts 2,367 leak-site listings since October 2022. [25]

## HEADLINE NUMBERS

**165**

Qilin incidents ZeroFox counted in August 2026, the highest 2026 monthly figure for any group [4]

**17 months**

consecutive months as the most active group in ZeroFox's count, through August 2026 [4]

**2,367**

leak-site listings since October 2022, as of October 13, 2026 [25]

**478,188**

patients in Covenant Health's revised count for its May 2025 breach, which Qilin claimed [17]

## KEY FACTS

**ALSO KNOWN AS**

Agenda; launched July 2022, rebranded to Qilin in September 2022 [23]

**MODEL**

Ransomware-as-a-service; affiliates keep 80 to 85 percent of each ransom [8]

**INITIAL ACCESS**

Stolen VPN credentials where MFA is missing; in 2026, authentication bypasses in Palo Alto PAN-OS and Check Point VPN gateways [13]

**PLATFORMS**

Windows, Linux and VMware ESXi; the Linux encryptor is also run on Windows through WSL [11]

**LEAK-SITE LISTINGS**

2,367 listed since October 2022, as of October 13, 2026 [25]

**LAW ENFORCEMENT**

Japan detained a suspected leading member in May 2026 and extradited him to Germany; the leak site kept listing victims [2]

## 02 What Happened

Qilin, a Russian-speaking ransomware-as-a-service operation that launched as Agenda in 2022, was the most active ransomware group of 2025 by leak-site claims and still led most 2026 counts, though The Gentlemen passed it in some periods. Japan's National Police Agency confirmed on October 8, 2026 that a 28-year-old Russian national, reported as a suspected leading Qilin member, was detained in Osaka in May 2026 and extradited to Germany. Qilin kept listing victims afterward, and its affiliates kept exploiting edge-device flaws.

- ZeroFox counted at least 165 Qilin incidents in August 2026, a 2026 high for any single group, and 1,480 from September 2025 through August 2026 against 767 for The Gentlemen, the next group.
- NCC Group counted 1,073 ransomware victims in August 2026 and attributed 164 incidents to Qilin and 116 to The Gentlemen, and said the two groups have regularly traded places as the most prolific this year.
- In 2026 Qilin-linked intrusions also used VPN authentication bypasses: Arctic Wolf tied June 2026 intrusions to Palo Alto PAN-OS CVE-2026-0257, and Check Point assessed with medium confidence that the actor exploiting its CVE-2026-50751 uses Qilin ransomware. CISA's catalog marks both flaws as used in ransomware campaigns, and ReliaQuest said in advisories posted October 9, 2026 that Qilin and Settra were still exploiting the Palo Alto flaw.
- Healthcare stayed in scope: Covenant Health raised its count to 478,188 patients after a May 2025 breach claimed by Qilin, and Bedfordshire Hospitals NHS Foundation Trust notified patients on June 1, 2026 about data stolen in the 2024 Synnovis attack.
- Qilin listed the US Bureau of Alcohol, Tobacco, Firearms and Explosives on August 26, 2026; the ATF said a standalone system holding information about targets of its investigations was breached and designated the incident major.
- Reports say Germany wants the extradited suspect over a September 2024 attack on a logistics company in which more than $160,000 in cryptocurrency was extorted. No conviction has been reported, and Japan did not release his name.

# 03 How It Works

## 01 Get in through the VPN

MITRE ATT&CK T1133

Affiliates log in with stolen or leaked VPN credentials, including on portals without MFA, or exploit authentication-bypass flaws in Palo Alto GlobalProtect and Check Point remote access gateways to open sessions without a password.

## 02 Steal credentials across the domain

MITRE ATT&CK T1003

Operators dump LSASS memory and the Active Directory database (Arctic Wolf, 2026), and have pushed a Group Policy logon script that harvests passwords saved in Chrome on the machines that run it (Sophos, 2024).

## 03 Plant redundant remote access

MITRE ATT&CK T1219

AnyDesk, Ngrok, LogMeIn and MeshAgent (Arctic Wolf, 2026) and ScreenConnect (Talos and Trend Micro, 2025) give the intruder more than one way back in; registry Run keys and scheduled tasks keep it.

## 04 Exfiltrate before encrypting

MITRE ATT&CK T1567.002

Rclone, FileZilla and Proton Drive (Arctic Wolf) and Cyberduck (Talos) move data to cloud storage such as MEGA, though some intrusions skipped data theft and only encrypted.

## 05 Blind defenses and kill recovery

MITRE ATT&CK T1685

Vulnerable signed drivers such as eskle.sys terminate EDR, event logs are cleared, shadow copies are deleted and Defender real-time protection is switched off in some cases. Veeam backup infrastructure is attacked before encryption: Trend Micro saw credentials harvested from backup databases, and Arctic Wolf saw it targeted to remove recovery options.

## 06 Encrypt and extort

MITRE ATT&CK T1486

Encryptors target Windows, Linux and ESXi, and some affiliates run the Linux build on Windows through WSL to dodge Windows-focused EDR. Talos measured ransomware execution about six days on average after initial compromise across its Qilin cases.

## 04 Who Is at Risk

Any organization that exposes a VPN or remote access gateway and runs Windows, Linux or VMware estates is in the target set. Qilin disproportionately hits North America and has repeatedly listed hospitals and government agencies.

- Manufacturers, construction firms, professional services and retailers, the top sectors in ZeroFox's count.
- Healthcare providers and their diagnostic vendors: the 2024 Synnovis pathology attack contributed to the death of a patient, per a UK government statement, and Covenant Health was still revising its Qilin-claimed breach count in January 2026.
- State and local agencies, courts and school districts: Comparitech logged 40 government and 26 education claims for 2025 through October 23.
- Managed service providers and their clients: Bitdefender's most probable explanation for the Korean Leaks campaign is a compromise of an upstream IT provider, with 33 South Korean victims, mostly asset managers.
- Organizations running unpatched Palo Alto, Check Point or Fortinet VPN appliances, or any VPN without MFA.

**Sectors in scope:** manufacturing, construction, professional services, retail, healthcare, government, education, financial services.

## 05 What Changed Since the Last Edition

EACH CHANGE WITH ITS SOURCE

01 A suspected leading member was arrested: Japan's National Police Agency confirmed on October 8, 2026 that a 28-year-old Russian national, described by BleepingComputer as suspected of being a leading Qilin member, was detained at an Osaka hotel in May 2026 on a German arrest warrant and extradited to Germany. SecurityWeek says Germany wants him over a September 2024 attack on a logistics company. BleepingComputer reports Qilin has listed more than 450 victims since June.

SOURCE 1

02 Volume stayed high: ZeroFox counted 190 Qilin incidents in October 2025, 179 in December 2025 and 165 in August 2026, the highest figure of 2026 for any group, and 1,480 from September 2025 through August 2026 against 767 for The Gentlemen.

SOURCE 4

03 Leadership became contested: ReliaQuest counted The Gentlemen ahead of Qilin, 300 to 289, from March to May 2026, and Check Point has The Gentlemen outpacing Qilin in June 2026 even though Qilin led the quarter with 279 victims to 269. ZeroFox and NCC Group still show Qilin first in August 2026.

SOURCE 22

04 Palo Alto VPN flaw: Arctic Wolf traced multiple June 2026 Qilin intrusions to PAN-OS CVE-2026-0257, an authentication bypass in GlobalProtect that let attackers open VPN sessions without credentials.

SOURCE 13

05 Check Point VPN zero-day: Check Point said CVE-2026-50751 was exploited from at least May 7, 2026, about a month before its June 8 advisory and hotfixes, against a few dozen organizations, and assessed with medium confidence that the actor behind it uses Qilin ransomware. CISA added the flaw to its Known Exploited Vulnerabilities catalog on June 8 with ransomware use marked Known.

SOURCE 39

06 A US federal law enforcement agency was hit: Qilin listed the ATF on August 26, 2026, and the ATF said a standalone system containing information about targets of its investigations was breached. It designated the incident major and is investigating with the Department of Justice.

SOURCE 19

07 Healthcare harm continued: Covenant Health revised the count for its May 2025 breach, which Qilin claimed in June 2025, from 7,864 to 478,188 patients and began mailing notification letters on December 31, 2025.

SOURCE 17

08 Talos's April 2026 analysis found ransomware execution about six days after initial compromise on average across its Qilin cases, stolen credentials as Qilin's main way in (obtained through Telegram, BreachForums and other platforms), and an affiliate EDR killer able to disable more than 300 EDR drivers.

SOURCE 10

## 06 What to Do Now

IN PRIORITY ORDER, HIGHEST IMPACT FIRST

01 DO FIRST **Patch and audit every VPN gateway now: Check Point CVE-2026-50751 (hotfix per sk185033; disable IKEv1 and legacy clients), Palo Alto PAN-OS CVE-2026-0257 (then terminate active GlobalProtect sessions), and any other exposed VPN such as Fortinet SSL-VPN.**

Both flaws are authentication bypasses linked to Qilin, and Arctic Wolf and Rapid7 advise ending existing sessions and hunting for compromise even after patching.

02 **Require phishing-resistant MFA on VPN, RDP and every remote management tool, and remove local VPN accounts.**

In the Sophos case and one Talos case, attackers used compromised credentials on a VPN portal that had no MFA.

03 **Disable browser password storage by policy and move staff to an enterprise password manager.**

Qilin has used a Group Policy logon script that harvests passwords saved in Chrome from every machine that runs it.

04 **Turn on the Microsoft vulnerable driver blocklist and alert on driver loads, Defender tamper events and event-log clearing (Event ID 1102).**

Affiliates load signed vulnerable drivers to kill EDR before encrypting.

05 **Keep immutable, offline backups and lock down Veeam: separate credentials, MFA on the console, and no domain-joined backup servers.**

Trend Micro saw Qilin harvest credentials from Veeam backup databases, and Arctic Wolf saw Veeam backup infrastructure targeted before the ransomware ran.

06 **Block or alert on unsanctioned AnyDesk, ScreenConnect, Ngrok, LogMeIn, MeshAgent, Rclone, Cyberduck and MEGA traffic.**

These tools carried Qilin remote access and exfiltration in the 2025 and 2026 cases.

07 **Monitor WSL installation and Linux ELF execution on Windows servers, and alert on writes to C:\PerfLogs and on PsExec service creation.**

Qilin runs its Linux encryptor inside WSL and stages win.exe in PerfLogs to slip past Windows-only detections.

08 **If nobody is watching VPN logs and driver loads overnight, Z7's 24/7 SOC and Microsoft 365 posture review are built for that gap.**

Talos measured ransomware execution about six days after initial compromise on average, which leaves time to catch the earlier steps if someone is watching.

## 07 Indicators

Indicators the sources publish, as they print them. Hunt with them, and check the source before you block.

| | |
|---|---|
| BEHAVIOR | GlobalProtect VPN sessions from client hostname kali, often from hosting or VPS address ranges [13] |
| FILE | `C:\PerfLogs\win.exe (Qilin payload staging path; also \\host\c$\Windows\Temp\win.exe)` [13] |
| REGISTRY | `Run key value named with an asterisk followed by six random lowercase letters, pointing to C:\PerfLogs\win.exe` [13] |
| IP | `108.61.229[.]217` [13] |
| IP | `108.61.75[.]232` [13] |
| IP | `2.188.33[.]52` [13] |
| IP | `199.247.22[.]193` [13] |
| IP | `70.34.205[.]43` [13] |
| FILE | `eskle.sys vulnerable signed driver, followed by sideloaded rwdrv.sys and hlpdrv.sys` [11] |
| BEHAVIOR | Linux ELF encryptor copied with WinSCP and launched through Splashtop SRManager.exe inside WSL on a Windows host [11] |
| FILE | `IPScanner.ps1 and logon.bat deployed from a SYSVOL directory by a logon GPO; per-host LD SQLite database and temp.log written back to SYSVOL` [35] |

# 08 Sources

[1] **Japan confirms arrest of Russian Qilin operative, extradition to Germany** The Record (Recorded Future News), reporting Japan's National Police Agency release · October 9, 2026. https://therecord.media/japan-germany-ransomware-arrest

[2] **Germany arrests alleged core Qilin ransomware member after extradition** BleepingComputer · October 9, 2026. https://www.bleepingcomputer.com/news/security/germany-arrests-alleged-core-qilin-ransomware-member-after-extradition/

[3] **Qilin Ransomware Suspect Arrested in Japan, Extradited to Germany** SecurityWeek · October 7, 2026. https://www.securityweek.com/qilin-ransomware-suspect-arrested-in-japan-extradited-to-germany/

[4] **Flash Report: Qilin Claims Record Number of Monthly Attacks for 2026** ZeroFox Intelligence · September 9, 2026. https://www.zerofox.com/intelligence/flash-report-qilin-claims-record-number-of-monthly-attacks-for-2026/

[5] **Ransomware Attacks Reach Record High for 2026** Infosecurity Magazine, reporting NCC Group's August 2026 Cyber Threat Intelligence Report · September 23, 2026. https://www.infosecurity-magazine.com/news/ransomware-attacks-reach-record/

[6] **Qilin ransomware surges into 2026** Barracuda Networks · January 15, 2026. https://blog.barracuda.com/2026/01/15/qilin-ransomware-surges-into-2026

[7] **Qilin ransomware: stats on attacks, ransoms, data breaches** Comparitech · updated October 23, 2025. https://www.comparitech.com/news/qilin-ransomware-stats-on-attacks-ransoms-data-breaches/

[8] **The State of Ransomware, Q3 2025** Check Point Research · November 13, 2025. https://research.checkpoint.com/2025/the-state-of-ransomware-q3-2025/

[9] **Uncovering Qilin attack methods exposed through multiple cases** Cisco Talos · October 26, 2025. https://blog.talosintelligence.com/uncovering-qilin-attack-methods-exposed-through-multiple-cases/

[10] **An overview of ransomware threats in Japan in 2025 and early detection insights from Qilin cases** Cisco Talos · April 2, 2026. https://blog.talosintelligence.com/an-overview-of-ransomware-threats-in-japan-in-2025-and-early-detection-insights-from-qilin-cases

[11] **Qilin ransomware abuses WSL to run Linux encryptors in Windows** BleepingComputer, reporting Trend Micro research · October 28, 2025. https://www.bleepingcomputer.com/news/security/qilin-ransomware-abuses-wsl-to-run-linux-encryptors-in-windows/

[12] **Qilin Ransomware Combines Linux Payload with BYOVD Exploit in Hybrid Attack** The Hacker News, reporting Trend Micro research · October 27, 2025. https://thehackernews.com/2025/10/qilin-ransomware-combines-linux-payload.html

[13] **Cookie Crumbles: How Exploitation of CVE-2026-0257 Leads to Qilin Ransomware** Arctic Wolf Labs · July 20, 2026. https://arcticwolf.com/resources/blog/exploitation-of-cve-2026-0257-leads-to-qilin-ransomware/

[14] **Qilin ransomware affiliate exploited Check Point VPN zero-day (CVE-2026-50751)** Help Net Security, reporting Check Point's advisory · June 8, 2026. https://www.helpnetsecurity.com/2026/06/08/check-point-cve-2026-50751-qilin-ransomware/

[15] **Critical Check Point VPN Zero-Day Exploited in the Wild (CVE-2026-50751)** Rapid7 · June 8, 2026, updated June 11, 2026. https://www.rapid7.com/blog/post/etr-critical-check-point-vpn-zero-day-exploited-in-the-wild-cve-2026-50751/

[16] **Known Exploited Vulnerabilities Catalog, entries CVE-2026-0257 (added May 29, 2026) and CVE-2026-50751 (added June 8, 2026)** CISA · checked October 13, 2026. https://www.cisa.gov/known-exploited-vulnerabilities-catalog

[17] **Covenant Health says May data breach impacted nearly 478,000 patients** BleepingComputer, reporting Covenant Health's Maine Attorney General notice · January 2, 2026. https://www.bleepingcomputer.com/news/security/covenant-health-says-may-data-breach-impacted-nearly-478-000-patients/

[18] **ATF confirms major incident after recent Qilin breach claims** BleepingComputer, reporting the ATF press release · August 27, 2026. https://www.bleepingcomputer.com/news/security/atf-confirms-major-incident-after-recent-qilin-breach-claims

[19] **ATF says standalone system holding investigation target data was breached after Qilin claim** The Record (Recorded Future News) · August 27, 2026. https://therecord.media/doj-atf-cyberattack-qilin-ransomware

[20] **Asahi says ransomware incident exposed data of about 1.5 million customers** The Record (Recorded Future News), reporting Asahi Group's disclosure · November 28, 2025. https://therecord.media/asahi-says-ransomware-incident-exposed-data

[21] **FBI Takes Down RAMP Ransomware Forum** Infosecurity Magazine · January 29, 2026. https://infosecurity-magazine.com/news/fbi-takes-down-ramp-ransomware

[22] **The Gentlemen Overtakes Qilin as Most Prolific Ransomware Threat** Infosecurity Magazine, reporting ReliaQuest research · July 17, 2026. https://infosecurity-magazine.com/news/the-gentlemen-most-prolific

[23] **Qilin threat group profile** Halcyon · updated August 25, 2026. https://www.halcyon.ai/threat-group/qilin

[24] **21 months, $100 million, one Qilin suspect in custody** Barracuda Networks · October 13, 2026. https://blog.barracuda.com/2026/10/13/21-months-100-million-one-Qilin-suspect-in-custody

[25] **Qilin group page, victim listings** Ransomware.live · checked October 13, 2026. https://www.ransomware.live/group/qilin

[26] **Written ministerial statement HCWS1046 on cyber security (Synnovis cost and patient impact)** UK Parliament · November 12, 2025. https://questions-statements.parliament.uk/written-statements/detail/2025-11-12/hcws1046

[27] **Synnovis Cyber Incident** Portsmouth Hospitals University NHS Trust · December 2025 entries. https://www.porthosp.nhs.uk/departments-and-services/pathology/synnovis-cyber-incident

[28] **NHS Pathology Provider Synnovis Notifies Organizations Affected by June 2024 Ransomware Attack** HIPAA Journal · November 12, 2025. https://www.hipaajournal.com/care-disrupted-at-london-hospitals-due-to-ransomware-attack-on-pathology-vendor/

[29] **Summer 2025 update (amber alert on blood stocks stood down)** NHS Blood and Transplant · Summer 2025. https://www.blood.co.uk/news-and-campaigns/the-donor/latest-stories/summer-2025-update/

[30] **UK Cybercrime Journal: Qilin Ransomware Rampage in H1 2026** BushidoToken (Will Thomas), citing Bedfordshire Hospitals NHS Foundation Trust · August 5, 2026. https://blog.bushidotoken.net/2026/07/uk-cybercrime-journal-qilin-ransomware.html

[31] **Drug R&D Firm Facing Costs, Lawsuits in Alleged Qilin Attack** GovInfoSecurity (ISMG), reporting Inotiv's SEC filings and Maine AG notice · December 10, 2025. https://www.govinfosecurity.com/drug-rd-firm-facing-costs-lawsuits-in-alleged-qilin-attack-a-30248

[32] **Pharmaceutical Firm Inotiv Discloses Ransomware Attack and Data Breach** HIPAA Journal · December 9, 2025. https://www.hipaajournal.com/inotiv-data-breach-ransomware-attack/

[33] **Microsoft: North Korean hackers now deploying Qilin ransomware** BleepingComputer, reporting Microsoft Threat Intelligence · March 7, 2025. https://www.bleepingcomputer.com/news/security/microsoft-north-korean-hackers-now-deploying-qilin-ransomware/

[34] **The Korean Leaks: analysing the hybrid geopolitical campaign targeting South Korean financial services with Qilin RaaS** Bitdefender (guest research published by iTWire) · November 25, 2025. https://itwire.com/guest-articles/guest-research/the-korean-leaks-%E2%80%93-analysing-the-hybrid-geopolitical-campaign-targeting-south-korean-financial-services-with-qilin-raas.html

[35] **Qilin ransomware caught stealing credentials stored in Google Chrome** Sophos X-Ops · August 2024 (activity observed July 2024). https://www.sophos.com/en-us/blog/qilin-ransomware-caught-stealing-credentials-stored-in-google-chrome/

[36] **Qilin ransomware gang hits hundreds of orgs in 2025** The Record (Recorded Future News), reporting Comparitech and Cisco Talos · October 28, 2025. https://therecord.media/qilin-ransomware-gang-hits-hundreds-of-orgs-2025

[37] **Qilin Ransomware Group Publishes Over 40 Cases Monthly** Infosecurity Magazine, reporting Cisco Talos · October 27, 2025. https://www.infosecurity-magazine.com/news/qilin-ransomware-40-cases-monthly

[38] **Decryption Tools (no Qilin or Agenda entry)** No More Ransom · checked October 13, 2026. https://www.nomoreransom.org/en/decryption-tools.html

[39] **Check Point VPN Zero-Day Exploited in Qilin Ransomware Attacks** SecurityWeek · June 9, 2026. https://www.securityweek.com/check-point-vpn-zero-day-exploited-in-qilin-ransomware-attacks/

[40] **Q3 2026 Sets New Record for Ransomware Attacks** Infosecurity Magazine, reporting Comparitech's Q3 2026 analysis · October 9, 2026. https://www.infosecurity-magazine.com/news/q3-new-record-ransomware/

[41] **The State of Ransomware Q2 2026** Check Point Research · August 13, 2026. https://research.checkpoint.com/2026/the-state-of-ransomware-q2-2026/

[42] **The State of Ransomware Q1 2026** Check Point Research · May 11, 2026. https://research.checkpoint.com/2026/the-state-of-ransomware-q1-2026/

[43] **Months-Old Palo Alto VPN Vulnerability Remains a Target for Ransomware Groups** Infosecurity Magazine, reporting ReliaQuest · October 12, 2026. https://www.infosecurity-magazine.com/news/palo-alto-vpn-vulnerability-target/

[44] **Notification, Synnovis Cyber Incident** Bedfordshire Hospitals NHS Foundation Trust · June 1, 2026. https://www.bedfordshirehospitals.nhs.uk/news/notification-synnovis-cyber-incident/

NEXT STEP

# What does this mean for your security?

Bring your questions about Qilin, your environment and the controls you rely on. Talk through the most useful next step with Z7 Solutions LLC.

### 01 / Exposure

Bring one question about how this threat could affect your environment.

### 02 / Priorities

Bring your current safeguards, open gaps and budget questions.

ALSO IN THIS EDITION

Qilin still hits hospitals and infrastructure
Continue with part 2 of 2 · z7solutions.com/z7-cyber/qilin-part-2/

LockBit 5.0 returns after Operation Cronos
More from the edition · z7solutions.com/z7-cyber/lockbit/

Akira still exploits SonicWall VPNs in 2026
More from the edition · z7solutions.com/z7-cyber/akira-ransomware/

CALL 844-974-8669

EMAIL sales@z7solutions.com

BOOK A SECURITY CONVERSATION Book a Security Conversation ↗

Z7 Solutions™, Z7-Claw™ and Z7-Guard™ are trademarks of Z7 Solutions LLC.