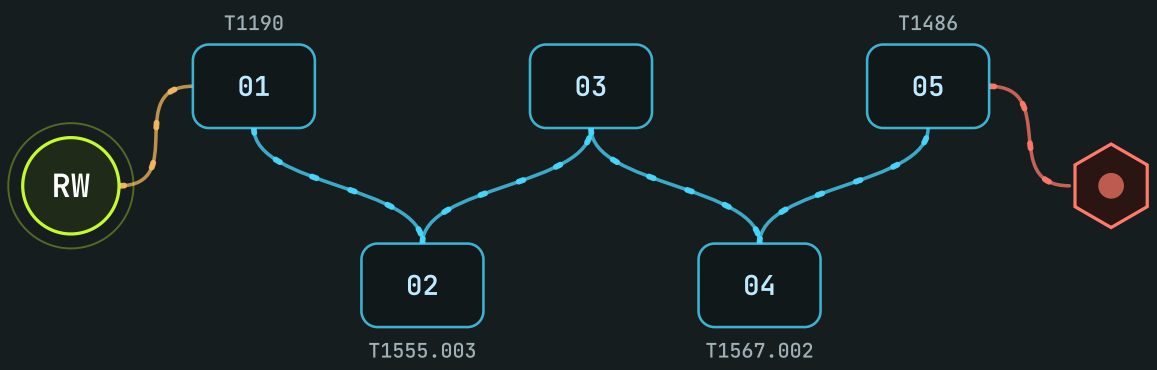


INTELLIGENCE BRIEF

Qilin still targets hospitals and critical infrastructure after an arrest

Synnovis fallout is still reaching NHS trusts, a Romanian pipeline operator confirmed Qilin data theft in 2026, and VPN zero-days now open the door. Patch edge gateways, enforce MFA and vet IT provider access.

EDITION
Fall/Winter 2026/2027 Edition
RW-02 · 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 on October 13, 2026 and has posted 2,367 since October 2022, with the leak site operating after a suspected leading member was detained. [2]

HEADLINE NUMBERS

2,367

victims listed on Qilin's leak site since October 2022, as of October 13, 2026 [2]

1

patient death King's College Hospital linked to the Synnovis outage [24]

almost 33,000

Synnovis-related patient records reported by Bedfordshire Hospitals alone, June 2026 [27]

28 of 33

Korean Leaks victims still public of those Qilin listed [15]

KEY FACTS

THREAT RATING

Critical. The rating holds on October 2026 evidence. [1]

HEALTHCARE HARM

King's College Hospital linked one patient death to the Synnovis outage; 170 harm cases recorded, 2 severe [24]

SUPPLY CHAIN

Korean Leaks: 33 victims posted (28 still public) after one IT provider compromise; Moonstone Sleet involvement only suspected [15]

INITIAL ACCESS

Check Point VPN zero-day and Palo Alto VPN bypass in 2026, after FortiGate flaws in 2025 [23]

CRITICAL INFRASTRUCTURE

Romania's national oil pipeline operator Conpet confirmed Qilin took company data in February 2026 and said operations were unaffected [30]

LAW ENFORCEMENT

One suspected leading member detained in Osaka in May 2026 and sent to Germany; more than 450 victims listed since June [5]

02 What happened

Z7's January 2026 Part 2 scored Qilin on seven threat-actor dimensions and rated three signature cases: the June 2024 Synnovis outage, the March 2025 Malaysia Airports incident and the September 2025 Korean Leaks campaign. Nine months on, the Synnovis harm is still being counted in patient records, a suspected leading Qilin member is in German custody, and the group's way in has shifted to VPN zero-days. Part 1 of this series covers the group's volumes and the arrest in full; this part follows the three cases and the scores that rest on them.

- King's College Hospital confirmed in June 2025 that a patient died unexpectedly during the Synnovis attack and that a long wait for a blood test result was one contributing factor; reported impact included 170 harm cases, 10,152 outpatient appointments and 1,710 elective procedures (Infosecurity Magazine).
- Synnovis said its stolen-data review took more than a year and told NHS organizations by November 2025; it has published no patient total. In June 2026 Bedfordshire Hospitals reported almost 33,000 patient records caught up in the breach and Mid and South Essex about 2,380 (The Register).
- Malaysia Airports said it detected a threat on March 23, 2025 and the prime minister said he refused a $10 million demand. Qilin claimed the attack on April 28, 2025, saying it took 2 TB, and the airport has not verified that claim, so the attribution rests on Qilin's own post.
- Bitdefender counted 33 Korean Leaks victims posted in three waves between September 14 and October 4, 2025 (28 still public), with more than 1 million files and 2 TB documented in the cases it could measure. It does not name the IT provider, and it calls Moonstone Sleet involvement plausible and probable, not confirmed.
- Microsoft said Moonstone Sleet began deploying Qilin at a limited number of organizations in late February 2025, the first time that actor used ransomware from a ransomware-as-a-service operator. CISA and the FBI had already reported in August 2024 that Iran-based actors worked directly with ALPHV, NoEscape and Ransomhouse affiliates.
- In February 2026 Conpet, Romania's national oil pipeline operator, confirmed that Qilin took data from its corporate IT network, after Qilin claimed nearly 1 TB.

03 How it works

01 Enter through edge or supplier access

MITRE ATT&CK T1190

Affiliates exploit VPN and firewall flaws: PRODAFT tied a May to June 2025 campaign to FortiGate bugs CVE-2024-21762 and CVE-2024-55591, and in 2026 the entry points were Check Point and Palo Alto authentication bypasses. They also reach clients through a compromised IT provider, as in Korean Leaks.

02 Harvest browser passwords by GPO

MITRE ATT&CK T1555.003

Sophos saw an intruder add a logon Group Policy Object that ran IPScanner.ps1 from SYSVOL, writing each machine's saved Chrome passwords into a SQLite file. Sophos cites a NordPass survey figure of 87 work passwords per user, so one harvest can reach third-party accounts.

03 Reach backups and hypervisors

Arctic Wolf saw intruders target Veeam backup infrastructure before running ransomware. Qilin's encryptors cover Windows, Linux and VMware ESXi, so a hypervisor and its backups can fall together.

04 Exfiltrate and clear the logs

MITRE ATT&CK T1567.002

In June 2026 cases the intruders moved data with Rclone, FileZilla and Proton Drive, mostly to MEGA, cleared Windows event logs and sometimes switched off Defender real-time protection.

05 Encrypt and add pressure

MITRE ATT&CK T1486

Halcyon describes Rust encryptors that pick AES-256-CTR or ChaCha20 and protect keys with RSA-4096, plus a leak site, a Call Lawyer feature, automated negotiation and DDoS added in 2025. No decryptor appears on the No More Ransom list.

04 Who is at risk

PRODAFT calls Qilin's target selection opportunistic, and its 2025 and 2026 victims include hospitals and their lab suppliers, a national pipeline operator and asset managers served by one IT provider. Any organization with an internet-facing VPN or firewall, or one outsourced IT provider, fits the pattern.

- Health systems and the lab, imaging and records suppliers they depend on: ransomware.live lists 199 healthcare victims since 2022, and NCC Group put healthcare at 12 percent of August 2026 ransomware incidents.
- Energy, transport and other critical infrastructure operators whose corporate IT is reachable from the internet, as Conpet showed in February 2026.
- Clients of managed service providers and other shared IT vendors, since one compromised provider exposed dozens of Korean financial firms.
- Organizations running Fortinet, Check Point or Palo Alto VPN gateways that are unpatched, lack MFA or still hold sessions opened before patching.
- Public bodies and schools: Comparitech counted 40 government and 26 education claims in 2025 through October.

Sectors in scope: healthcare and diagnostic suppliers, energy and pipelines, financial services and asset management, transportation and logistics, government, education, manufacturing, professional services.

05 What changed since the last edition

EACH CHANGE WITH ITS SOURCE

01 Japan's National Police Agency confirmed on October 8, 2026 (The Record) that a 28-year-old Russian national suspected of being a leading Qilin member was detained in Osaka in May and sent to Germany, where SecurityWeek says he is wanted over a September 2024 attack on a logistics company with over $160,000 extorted. The January 2026 edition's 'no core arrests' evidence behind Persistence and Resilience no longer holds, and Part 1 covers the arrest and the group's continued activity.

SOURCE 4

02 Synnovis says its stolen-data review took more than a year (17 months per HIPAA Journal) and it notified NHS organizations by November 2025; hospitals, not Synnovis, notify patients. In June 2026 Bedfordshire Hospitals reported almost 33,000 patient records caught up and Mid and South Essex about 2,380; no total has been published, and the 900,000 figure in the January 2026 edition is a third-party estimate.

SOURCE 27

03 Romania's national oil pipeline operator Conpet confirmed on February 12, 2026 that Qilin stole company data, after Qilin claimed nearly 1 TB. Conpet says operations were unaffected and that it is working with Romania's national cyber security directorate.

SOURCE 30

04 Initial access moved from FortiGate bugs (PRODAFT, May to June 2025) to VPN authentication bypasses: Check Point believes a Qilin affiliate exploited CVE-2026-50751, with the earliest observed exploitation on May 7, 2026, and Arctic Wolf traced June 2026 Qilin intrusions to PAN-OS CVE-2026-0257. CISA lists both in its Known Exploited Vulnerabilities catalog with ransomware use marked Known.

SOURCE 23

05 Correction: the January 2026 edition described the March 2025 Malaysia Airports incident as a Qilin attack. The airport and Malaysian authorities named no attacker, Qilin claimed it on April 28, 2025, and the airport has not verified the claim; no later confirmation was found, so the case is Qilin-claimed.

SOURCE 10

06 Correction: the '$50 million+ in ransom payments in 2024' headline could not be sourced. The only $50 million figure in the sources checked is the demand made of Synnovis, which Synnovis did not pay.

SOURCE 9

07 Correction: Microsoft described Moonstone Sleet's use of Qilin as the first time that actor used ransomware from a ransomware-as-a-service operator, not the first state-linked adoption of one. CISA and the FBI reported Iran-based actors working directly with ALPHV, NoEscape and Ransomhouse affiliates in August 2024.

SOURCE 14

06 What to do now

IN PRIORITY ORDER, HIGHEST IMPACT FIRST

01 DO FIRST **Patch and audit every internet-facing VPN and firewall gateway now (Fortinet, Check Point, Palo Alto), then terminate existing VPN sessions and rotate credentials that passed through them.**

Qilin affiliates used FortiGate flaws in 2025 and VPN authentication bypasses in 2026, and Arctic Wolf advises ending active GlobalProtect sessions after patching so unauthorized sessions are invalidated.

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

In the Sophos case the intruder entered through a VPN portal that had no MFA.

03 **Disable browser password storage by policy, deploy an enterprise password manager, and alert on edits to the default domain policy and new .ps1 or .bat files in SYSVOL.**

Qilin's logon GPO turns one domain compromise into every saved Chrome password across the estate.

04 **Keep Veeam on a current supported release, with separate credentials, MFA on the console, immutable or offline copies and monthly restore tests.**

CISA lists four Veeam flaws with known ransomware use, and Arctic Wolf saw Qilin intruders target Veeam infrastructure before encrypting.

05 **Isolate ESXi and other hypervisor management on a dedicated network, keep SSH off unless in use, and alert on new administrator sessions.**

Qilin's encryptors target VMware ESXi, so hypervisor access decides how much encrypts at once.

06 **Treat IT providers and lab or diagnostic suppliers as part of your attack surface: MFA, least privilege, segmented access, log sharing, quarterly access reviews and a contract clause for breach notice and data inventory.**

One provider compromise reached dozens of Korean firms, and Synnovis needed more than a year to scope what was stolen.

07 **Write and rehearse downtime procedures for outsourced critical services such as pathology, billing and dispatch.**

The Synnovis outage left clinicians waiting on blood test results, and King's College Hospital named that wait as a contributing factor in a patient death.

08 **If nobody watches VPN, identity and log-clearing alerts overnight, Z7's 24/7 SOC and Microsoft 365 posture review cover that gap.**

Arctic Wolf saw Qilin clear event logs and disable Defender real-time protection before encrypting.

07 Indicators

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

FILE	`IPScanner.ps1` and `logon.bat` in a new SYSVOL directory, run by a logon Group Policy Object added to the default domain policy [17]
FILE	Per-host SQLite database named `LD` and a text file `temp.log` written back to SYSVOL at each user logon [17]
BEHAVIOR	Event logs cleared estate-wide and Microsoft Defender real-time protection disabled shortly before ransomware deployment [22]

08 Sources

[1] **Qilin Ransomware: Z7-TAF Threat Actor Analysis and Z7-BAF Attack Assessments, version 1.0** Z7 Solutions LLC · January 2, 2026. https://z7solutions.com/z7-cyber/qilin-part-2/

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

[3] **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

[4] **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/

[5] **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/

[6] **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/

[7] **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/

[8] **Qilin threat group profile** Halcyon · page checked October 13, 2026 (lists activity through September 28, 2026). https://www.halcyon.ai/threat-group/qilin

[9] **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/

[10] **Ransomware gang claims cyber attack on Malaysia Int'l Airport** Comparitech · April 28, 2025. https://comparitech.com/news/ransomware-gang-says-it-hacked-the-malaysias-kuala-lumpur-international-airport

[11] **Malaysia rejects $10 million ransom demand after cyberattack on Kuala Lumpur airport (headline paraphrased)** Teiss · March 26, 2025. https://www.teiss.co.uk/news/malaysia-rejects-10-million-ransom-demand-after-cyberattack-on-kuala-lumpur-airport-15550

[12] **Moonstone Sleet emerges as new North Korean threat actor with new bag of tricks** Microsoft Threat Intelligence · May 28, 2024. https://www.microsoft.com/en-us/security/blog/2024/05/28/moonstone-sleet-emerges-as-new-north-korean-threat-actor-with-new-bag-of-tricks/

[13] **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/

[14] **Iran-based Cyber Actors Enabling Ransomware Attacks on US Organizations (advisory AA24-241A)** CISA, FBI and Department of Defense Cyber Crime Center · August 28, 2024. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-241a

[15] **The Korean Leaks: analyzing the hybrid geopolitical campaign targeting South Korean financial services with Qilin RaaS** Bitdefender · November 24, 2025. https://www.bitdefender.com/en-us/blog/businessinsights/korean-leaks-campaign-targets-south-korean-financial-services-qilin-ransomware

[16] **Qilin Ransomware Turns South Korean MSP Breach Into 28-Victim 'Korean Leaks' Data Heist** The Hacker News · November 26, 2025. https://thehackernews.com/2025/11/qilin-ransomware-turns-south-korean-msp.html

[17] **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

[18] **Critical Fortinet flaws now exploited in Qilin ransomware attacks** BleepingComputer, reporting PRODAFT · June 6, 2025. https://www.bleepingcomputer.com/news/security/critical-fortinet-flaws-now-exploited-in-qilin-ransomware-attacks/

[19] **Known Exploited Vulnerabilities Catalog (entries for CVE-2023-27532, CVE-2024-21762, CVE-2024-55591, CVE-2025-31324, CVE-2026-0257 and CVE-2026-50751)** CISA · catalog version 2026.10.13, checked October 13, 2026. https://www.cisa.gov/known-exploited-vulnerabilities-catalog

[20] **NVD record for CVE-2025-31324 (SAP NetWeaver)** NIST National Vulnerability Database · checked October 13, 2026. https://nvd.nist.gov/vuln/detail/CVE-2025-31324

[21] **KB4424: CVE-2023-27532** Veeam · checked October 13, 2026. https://www.veeam.com/kb4424

[22] **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/

[23] **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/

[24] **Patient Death Linked to NHS Cyber-Attack** Infosecurity Magazine · June 26, 2025. https://www.infosecurity-magazine.com/news/patient-death-linked-nhs-cyber/

[25] **Qilin ransomware attack on NHS supplier contributed to patient fatality** The Register · June 26, 2025. https://www.theregister.com/2025/06/26/qilin_ransomware_nhs_death/

[26] **NHS supplier ends probe into ransomware attack that contributed to patient death** The Register · November 13, 2025. https://www.theregister.com/2025/11/13/synnovis_qilin_investigation/

[27] **NHS trusts report patient records caught up in the Synnovis breach (headline paraphrased)** The Register · June 9, 2026. https://www.theregister.com/a/5252663

[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] **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

[30] **Romania's oil pipeline operator Conpet confirms data stolen in attack** BleepingComputer · February 12, 2026. https://www.bleepingcomputer.com/news/security/romanias-oil-pipeline-operator-conpet-confirms-data-stolen-in-attack/

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

NEXT STEP

Put the same team on your environment

Talk to the team that runs the Z7 Solutions™ SOC about what this brief means for your environment. We will tell you what applies and what does not.

ALSO IN THIS EDITION

- Qilin still tops most ransomware counts
  Start with part 1 of 2 · z7solutions.com/z7-cyber/qilin/
- 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 CALL	z7solutions.com/book/

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