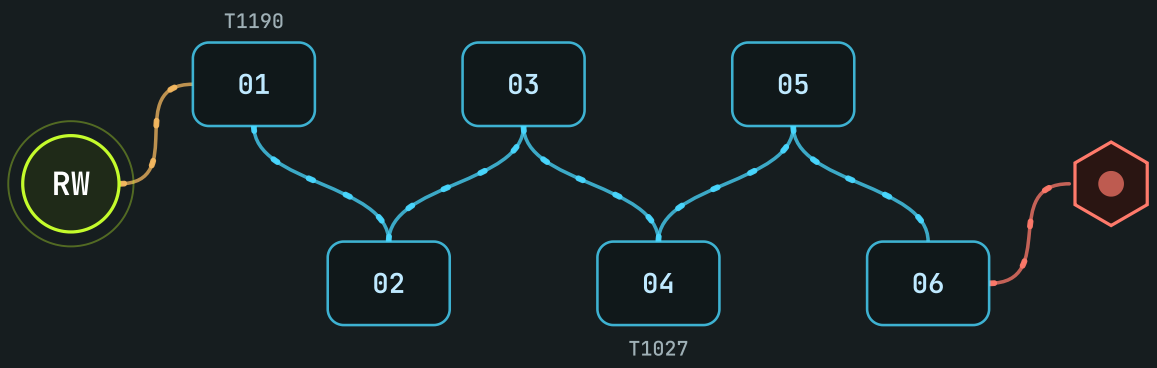


INTELLIGENCE BRIEF

Ransomware-as-a-service keeps fragmenting as Qilin and The Gentlemen lead

Leak-site groups reached 93 in Q2 2026. RansomHub vanished, Qilin led four quarters and The Gentlemen overtook it, while payment rates hit record lows. Harden edge devices, identity and hypervisors now.

EDITION
Fall/Winter 2026/2027 Edition
RW-06 · Ransomware ecosystem

PUBLISHED BY
Z7 Solutions LLC
Orlando, Florida

READ ONLINE
z7solutions.com
844-974-8669

01 At a glance

STATUS

ACTIVE

Check Point counted 2,139 leak-site victims from 93 active groups in the second quarter of 2026, up 33 percent on a year earlier. [1]

HEADLINE NUMBERS

93
active leak-site groups in Q2 2026 [1]

2,139
leak-site victims in Q2 2026 [1]

$820M+
on-chain ransomware payments in 2025 [2]

28%
of victims paid in 2025, a record low [2]

KEY FACTS

ACTIVE GROUPS
93 on leak sites in Q2 2026, up from 71 in Q1 [1]

TOP OPERATIONS
Qilin 279 victims, The Gentlemen 269 and ahead of Qilin in June [1]

PAYMENTS
More than $820 million on-chain in 2025; only 28 percent of victims paid [2]

ENTRY POINTS
Phishing and social engineering lead again; access is increasingly identity driven [3]

DATA THEFT
Exfiltration in 76 percent of cases; exfiltration-only payment rate 15 percent [3]

MOST REPORTED TO FBI
Akira, Qilin, then INC, Lynx and Sinobi in 2025 [4]

02 What happened

The original edition argued that the early-2024 takedowns of ALPHV/BlackCat and LockBit split the market into many smaller operations while fewer victims paid. Both points held through 2025 and 2026, but the names at the top changed: RansomHub stopped operating in April 2025, Qilin led from the third quarter of 2025, and The Gentlemen, launched in September 2025, overtook it in June 2026. Volume stayed near record levels while the share of victims who paid fell to its lowest on record.

- Claimed ransomware victims rose about 50 percent in 2025, the most active year on record, and Check Point logged a record 2,416 leak-site victims in the fourth quarter of 2025; the second quarter of 2026 held at 2,139, and NCC Group recorded 1,073 attacks in August 2026, the highest month of that year.
- On-chain payments exceeded $820 million in 2025, about 8 percent below Chainalysis's restated 2024 total of $892 million; the share of victims paying fell to a record 28 percent while the median payment rose 368 percent to $59,556.
- RansomHub, which had averaged about 75 listed victims a month, stopped operating in early April 2025; many affiliates moved to Qilin, whose monthly postings nearly doubled, and DragonForce claimed RansomHub had joined its cartel. Barracuda reports Qilin claimed more than 1,000 leak-site victims in 2025.
- Qilin led four straight quarters through mid-2026, with 338 victims in Q1 and 279 in Q2, until The Gentlemen reached 269 in Q2 and outpaced it in June. Check Point says The Gentlemen was founded by a former Qilin affiliate and that leaked chats show a core team of about nine operators who built their management panel with AI coding assistants in about three days.
- CISA and the FBI report Akira's claimed proceeds at about $244 million by late September 2025 and count roughly 900 entities affected by Play as of May 2025, while the FBI's IC3 ranked Akira, Qilin and INC, Lynx and Sinobi as the three most reported variants of 2025.
- Enforcement targeted infrastructure and people: the FBI seized the RAMP ransomware forum in January 2026, an Operation Endgame phase neutralized 326 servers and 142 domains in June 2026, including the SocGholish loader often used to install ransomware, Japan arrested a 28-year-old Russian national on a German warrant over a Qilin-linked attack (Japan's police confirmed it in October 2026), and two Scattered Spider members were sentenced to five years and six months each in July 2026.

03 How it works

01 Get in through edge devices

MITRE ATT&CK T1190

Affiliates buy or exploit access: Akira likely abused a SonicWall flaw (CVE-2024-40766), Check Point assessed with medium confidence that a Qilin affiliate used a VPN authentication bypass (CVE-2026-50751), and Play-linked brokers exploited SimpleHelp. Check Point reports The Gentlemen holds roughly 14,700 pre-exploited FortiGate devices.

02 Take over identities

Coveware sees access shift toward identity: MFA and password-reset abuse, help desk manipulation, OAuth grants and stolen credentials. Cisco Talos traced one Qilin case to leaked administrator credentials on a VPN with no MFA.

03 Steal data before encrypting

Exfiltration appeared in 76 percent of Coveware's second-quarter cases. Only 15 percent of exfiltration-only victims paid, and Coveware ties its largest Q2 payments to data-theft extortion, including vishing campaigns against law firms.

04 Evade defenses

MITRE ATT&CK T1027

Play recompiles its binary for every deployment so each hash is unique, and ReliaQuest says The Gentlemen's affiliate kit bundles an attack playbook, tunneling tools and single-host SMB encryption.

05 Encrypt servers and hypervisors

Play carries an ESXi variant that powers off virtual machines, and in a June 2025 incident Akira was seen encrypting Nutanix AHV virtual disks for the first time.

06 Extort and split the proceeds

Operators recruit affiliates to run intrusions; Akira alone claimed about $244 million in proceeds by late September 2025. Play victims receive unique contact addresses and some are called by phone.

04 Who is at risk

Any organization with an exposed VPN or remote management tool, a help desk that resets credentials on a phone call, or a virtual estate that cannot be restored quickly is in scope, whatever its size. The FBI says the ten most reported variants most affected critical manufacturing, healthcare and public health, and government facilities.

- Industrial (31 percent), consumer goods and services (18 percent), healthcare (12 percent) and information technology (11 percent) led NCC Group's August 2026 attack counts, and North America took 44 percent of them.
- CISA names a notable Akira preference for educational institutions, and says it mainly targets small and medium-sized businesses while also hitting larger ones.
- Healthcare remains a standing target: the Qilin attack on pathology provider Synnovis in June 2024 contributed to more than 10,000 cancelled appointments, and Barracuda says Qilin affiliates are not disciplined about avoiding healthcare providers.
- Outside critical sectors, the FBI received more than 1,400 ransomware complaints, with legal services (18 percent) and contracting services (17 percent) the most reported industries; Coveware ties a spike in large payments to vishing campaigns against law firms.
- Organizations that hold data in cloud platforms are exposed to data-theft crews, as the 2024 Snowflake campaign showed: credentials stolen by infostealers on accounts without MFA affected well over 150 organizations.

Sectors in scope: critical manufacturing, industrial and consumer goods, healthcare and public health, government facilities, education, legal and professional services, information technology, financial services.

05 What changed since the last edition

EACH CHANGE WITH ITS SOURCE

01 RansomHub, the fastest-growing group in the original edition, stopped operating in early April 2025 with no explanation. Its affiliates, who averaged about 75 listed victims a month, largely moved to Qilin, and DragonForce claimed RansomHub had joined its cartel, a claim Check Point could not verify.

SOURCE 5

02 The leaders changed. Qilin was the most prolific group for a fourth straight quarter in Q2 2026 with 279 victims, down 17 percent, while The Gentlemen rose 62 percent to 269 and outpaced Qilin in June.

SOURCE 1

03 The market fragmented further. Active groups rose from 71 to 93 between Q1 and Q2 2026 and the top ten's share of victims fell from 71 percent to 57.6 percent, so the original edition's 85-plus operations is now a floor that moves each quarter.

SOURCE 1

04 LockBit came back despite the 2024 takedown. LockBit 5.0 launched on the RAMP forum in September 2025, charged new affiliates a deposit of about $500, and posted 163 victims in Q1 2026, up 106 percent on Q4 2025 and fourth place overall.

SOURCE 6

05 Payments fell further while attack volume rose. Chainalysis restated 2024 payments from $813 million to $892 million, put 2025 at more than $820 million (down 8 percent), recorded a payment rate of 28 percent, and said claimed victims rose 50 percent.

SOURCE 2

06 Incident-response data tells a different story from leak sites. Coveware's Q2 2026 caseload was led by lone-wolf actors (17 percent), ShinyHunters (12 percent), Akira (9 percent) and The Gentlemen (8 percent); phishing and social engineering returned to the top of the entry list, and the average payment of $1.88 million sat far above the $150,000 median.

SOURCE 3

07 Akira grew well past the original edition's $42 million. CISA's November 2025 update puts its claimed proceeds at about $244 million as of late September 2025, adds exploitation of SonicWall CVE-2024-40766, and records the first Akira encryption of Nutanix AHV virtual disks.

SOURCE 7

08 The FBI took down the RAMP forum, first noticed on January 28, 2026. It was a hub where new and mid-tier ransomware groups advertised and where LockBit, Qilin, DragonForce and others are understood to have operated, although analysts expect little effect on top-tier groups.

SOURCE 8

06 What to do now

IN PRIORITY ORDER, HIGHEST IMPACT FIRST

01 DO FIRST **Patch or isolate internet-facing VPNs, firewalls and remote management tools within days of a CISA Known Exploited Vulnerabilities listing, and retire end-of-support gateways.**

Akira, Qilin and Play-linked brokers each broke in through a named edge or remote-management flaw, and four of the Check Point branches affected by CVE-2026-50751 are end of support.

02 **Require phishing-resistant MFA on every VPN, email and administrative account, and use IKEv2 with machine certificate authentication on VPN gateways instead of allowing legacy clients.**

Talos found a Qilin intrusion through a VPN with no MFA, and the Check Point VPN bypass worked where machine certificates were not required.

03 **Tighten help desk identity checks for password resets, MFA changes and new device enrollment, and review OAuth app consents.**

Coveware reports access is increasingly identity driven, including help desk manipulation, MFA and password-reset abuse, and OAuth grants.

04 **Keep offline, immutable backups that include hypervisor-level copies, and test a full restore every quarter.**

Play and Akira both ship encryptors for VMware ESXi and Akira has now encrypted Nutanix AHV, so a backup on the same virtual estate is not a backup.

05 **Restrict hypervisor and backup management interfaces to a separate admin network with its own credentials.**

One compromised host can encrypt dozens of servers, and Talos documented Qilin changing ESXi root passwords and enabling SSH.

06 **Run EDR with tamper protection on servers and endpoints, and alert on bulk archiving, staging and large outbound transfers to cloud storage.**

Data theft occurs in 76 percent of cases and happens before encryption, which is the window in which an intrusion can still be stopped.

07 **Decide your ransom policy with counsel and an OFAC sanctions check before an incident, and plan notification on the assumption that stolen data will be published.**

Only 15 percent of exfiltration-only victims paid in Q2 2026, and paying does not guarantee deletion.

08 **Report incidents to the FBI and CISA and keep a current, tested incident response plan; Z7 Solutions™ provides 24/7 monitoring and Microsoft 365 posture review for mid-size organizations, school districts and public agencies.**

The FBI's IC3 relies on victim reports to act on groups such as BlackSuit, and early reporting also speeds recovery.

07 Indicators

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

BEHAVIOR	Ransom contact addresses at gmx.de or web.de that are unique to each victim, and a recompiled binary with a unique hash for each deployment (Play) [9]
BEHAVIOR	Remote access VPN gateways using IKEv1 without machine certificate authentication, and unexpected authentication bypasses on Check Point Remote Access, Mobile Access and Spark gateways (CVE-2026-50751) [10]
BEHAVIOR	SonicWall VPN access through CVE-2024-40766, stolen credentials or brute forcing, followed by encryption of VMware, Hyper-V or Nutanix AHV virtual disks (Akira) [7]

08 Sources

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

[2] **Crypto Ransomware: 2026 Crypto Crime Report** Chainalysis · February 26, 2026. https://www.chainalysis.com/blog/crypto-ransomware-2026/

[3] **Adverse cyber extortions are more common than commonly advised (Q2 2026 quarterly report)** Coveware by Veeam · July 2026. https://coveware.com/2026/07/adverse-cyber-extortions-are-more-common-than-commonly-advised/

[4] **Internet Crime Report 2025** FBI Internet Crime Complaint Center · annual report covering 2025; publication date not printed. https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[5] **The State of Ransomware, Q2 2025** Check Point Research · July 31, 2025. https://research.checkpoint.com/2025/the-state-of-ransomware-q2-2025/

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

[7] **#StopRansomware: Akira Ransomware (AA24-109A)** CISA and FBI · updated November 13, 2025. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a

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

[9] **#StopRansomware: Play Ransomware (AA23-352A)** CISA and FBI · updated June 4, 2025. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a

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

[11] **LockBit Returns, and It Already Has Victims** Check Point Research · October 2025. https://blog.checkpoint.com/research/lockbit-returns-and-it-already-has-victims/

[12] **Cost of a Data Breach Report 2026** IBM · 2026 edition; publication date not printed. https://www.ibm.com/reports/data-breach

[13] **Care Disrupted at London Hospitals Due to Ransomware Attack on Pathology Vendor** HIPAA Journal · November 2025 update. https://www.hipaajournal.com/care-disrupted-at-london-hospitals-due-to-ransomware-attack-on-pathology-vendor/

[14] **Two Scattered Spider Hackers Sentenced to Jail in UK** SecurityWeek · July 16, 2026. https://www.securityweek.com/two-scattered-spider-hackers-sentenced-to-jail-in-uk/

[15] **Scattered Spider affiliate sentenced to 10 years in prison** The Record (Recorded Future News) · August 21, 2025. https://therecord.media/scattered-spider-affiliate-sentenced-10-years

[16] **Change Healthcare Responding to Cyberattack** HIPAA Journal · page updated through November 17, 2025. https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/

[17] **Snowflake Hacker Pleads Guilty Over Breach of 165+ Organizations (reporting the DOJ release)** The Hacker News · August 6, 2026. https://thehackernews.com/2026/08/snowflake-hacker-pleads-guilty-over.html

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

[19] **#StopRansomware: ALPHV Blackcat (AA23-353A)** CISA and FBI · updated February 27, 2024. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a

[20] **The Gentlemen Overtakes Qilin as Most Prolific Ransomware Threat (reporting ReliaQuest, March to May 2026)** Infosecurity Magazine · July 17, 2026. https://www.infosecurity-magazine.com/news/the-gentlemen-most-prolific/

[21] **Ransomware Attacks Reach Record High for 2026 (reporting NCC Group's August 2026 threat report)** Infosecurity Magazine · September 23, 2026. https://www.infosecurity-magazine.com/news/ransomware-attacks-reach-record/

[22] **Japan confirms arrest of Russian Qilin operative, extradition to Germany** The Record (Recorded Future News) · October 9, 2026. https://therecord.media/japan-germany-ransomware-arrest

[23] **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/

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

[25] **The State of Ransomware 2026** Sophos · 2026 edition; publication date not printed. https://www.sophos.com/en-us/content/state-of-ransomware

[26] **Operation Endgame continues: international coalition takes malware offline** Eurojust · June 24, 2026. https://www.eurojust.europa.eu/news/operation-endgame-continues-international-coalition-takes-malware-offline

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
More from the edition · z7solutions.com/z7-cyber/qilin/

Qilin still hits hospitals and infrastructure
More from the edition · z7solutions.com/z7-cyber/qilin-part-2/

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

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.