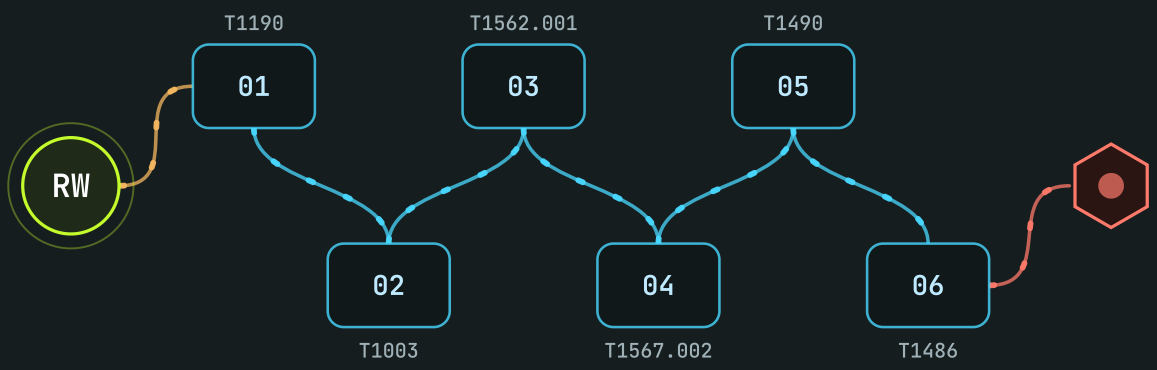


INTELLIGENCE BRIEF

Qilin, The Gentlemen and Akira now top the most dangerous cybercrime groups

Qilin, The Gentlemen and Akira now lead the field while ALPHV, RansomHub and Black Basta are gone and ShinyHunters-style data theft climbs. Patch edge devices, require phishing-resistant MFA and test backups first.

EDITION
Fall/Winter 2026/2027 Edition
RW-07 · Ransomware ecosystem

PUBLISHED BY
Z7 Solutions LLC
Orlando, Florida

READ ONLINE
z7solutions.com
844-974-8669

01 At a glance

STATUS

ONGOING RISK

Check Point counted 2,139 leak-site victims across a record 93 active groups in Q2 2026, up 33 percent on a year earlier, while the share of victims paying fell to about 23 percent. [1]

HEADLINE NUMBERS

2,139
leak-site victims in Q2 2026, up 33 percent year over year [1]

93
active groups in Q2 2026, a record for a quarter [1]

$820M+
on-chain ransomware payments in 2025, down 8 percent [8]

17 months
consecutive months Qilin led ZeroFox's monthly count, through August 2026 [3]

KEY FACTS

1. QILIN
First for 17 straight months by ZeroFox's count: 1,480 incidents in 12 months and a 2026 high of 165 in August [3]

2. THE GENTLEMEN
Fastest riser: claimed victims up about six-fold from late 2025 to early 2026; pays affiliates 90 percent [5]

3. AKIRA
Claimed $244.17 million by late September 2025; CISA flags an imminent threat to critical infrastructure [21]

4. SHINYHUNTERS
Vishing and SaaS data theft for extortion; the FBI says over $70 million extorted so far in 2026 [23]

5. DRAGONFORCE
Cartel model lets crews run their own brand on shared infrastructure; partners with Scattered Spider [16]

6. LOCKBIT 5.0
Relaunched September 2025; 163 victims in Q1 2026, fourth worldwide per Check Point; leader still at large [52]

02 What happened

The original edition, written in January 2026, sorted the field into tiers led by Scattered Spider, LockBit, ALPHV, Clop, RansomHub and Qilin. Nine months later the order has changed: Qilin still leads on most counts but The Gentlemen passed it for part of 2026, Akira and DragonForce sit in the top five, LockBit came back, and data-theft crews such as ShinyHunters and Clop hurt victims without encrypting anything. ALPHV, RansomHub and Black Basta have not listed a victim since early 2025 or earlier.

- How the ranking is built: Z7 weighs recent leak-site volume, damage per incident, staying power under enforcement and speed of adaptation. Check Point counted 2,139 victims across 93 active groups in Q2 2026, with the top ten's share down to 57.6 percent from 71 percent, and GuidePoint found the five busiest groups claimed more than 40 percent of attacks.
- Ranks 7 to 10 and why: Clop for mass exploitation (Oracle E-Business Suite in 2025, PTC Windchill in July 2026) despite weak monetization and a September 2026 defacement of its leak site by ShinyHunters; Play, with 1,329 victims listed but lower output in Q2 2026; the INC, Lynx and Sinobi family, third among the FBI's most reported variants; Medusa and SafePay, with over 500 critical infrastructure victims for Medusa and a SafePay recovery in Q2 2026.
- Off the list and why: ALPHV (about $395 million in US-reported payments from 2022 to 2024 per FinCEN, last listed victim March 2024; two incident response professionals who acted as its affiliates were sentenced and a third pleaded guilty), RansomHub (last listed victim March 31, 2025), Black Basta (collapsed, its alleged leader on Europol and Interpol lists), BlackSuit (disrupted in a coordinated action the DOJ announced on August 11, 2025) and Scattered Spider (sentenced and effectively halted).
- Fewer victims pay, so groups push volume and data theft: Chainalysis measured over $820 million in 2025 payments, down 8 percent, and Coveware recorded a record low payment rate in Q2 2026 with a median payment of $150,000.
- Enforcement is landing on infrastructure and on travelers, not on Russia-based leaders: Europol's Endgame actions hit loaders and stealers in November 2025 and June 2026, Treasury sanctioned the Media Land bulletproof host, Project Compass produced 30 arrests in The Com, and suspects were detained in Japan, Greece and Finland.
- The FBI's 2025 report counts $20.877 billion in losses across 1,008,597 complaints, up 26 percent, and ranks the ten most reported ransomware variants: Akira, Qilin, INC/Lynx/Sinobi, BianLian, Play, RansomHub, LockBit, DragonForce, SafePay and Medusa.

03 How it works

01 Get in through the edge or the phone

MITRE ATT&CK T1190

Qilin, Akira and The Gentlemen enter through VPN, firewall and remote access flaws or bought credentials, while ShinyHunters-branded crews phone help desks and send staff to fake sign-on pages.

02 Take credentials and spread

MITRE ATT&CK T1003

CISA documents Akira operators dumping credentials and reusing valid accounts to move through the network, and the other leading groups follow the same pattern.

03 Blind the defenses

MITRE ATT&CK T1562.001

EDR killers and signed vulnerable drivers switch off security tools; The Gentlemen use a framework called GentleKiller and CISA documents the driver technique in Akira cases.

04 Steal data first

MITRE ATT&CK T1567.002

Data goes to cloud storage before encryption, and several crews now skip encryption entirely, which Coveware says pays out only 15 percent of the time.

05 Break recovery and encrypt

MITRE ATT&CK T1490

Backups and hypervisors are targeted so recovery fails: Veeam servers in Akira cases, ESXi in The Gentlemen and DragonForce cases.

06 Extort the victim

MITRE ATT&CK T1486

A leak-site listing, a deadline and pressure on customers and executives follow; GuidePoint saw DragonForce use language models to draft pressure messages.

04 Who is at risk

Any organization with internet-facing VPN or firewall appliances, a help desk that resets credentials by phone, or a virtualized server estate is a candidate, and the mid-market is as exposed as the enterprise.

- Manufacturing, professional services, technology, healthcare and retail lead 2026 leak-site listings, with 1,405, 1,330, 1,050, 727 and 602 listings so far this year.
- Government and education organizations: 283 government and defense and 270 education listings in 2026, the FBI says its top ten variants most affected critical manufacturing, healthcare and public health, and government facilities, and in August 2026 the ATF confirmed a breach of a standalone system after Qilin listed the agency.
- Smaller firms outside critical sectors, where the FBI's non-critical complaints came mostly from legal services (18 percent), contractors (17 percent) and engineering firms (10 percent).
- Organizations running unpatched enterprise applications: Oracle E-Business Suite and PTC Windchill for Clop, Oracle PeopleSoft for ShinyHunters (a zero-day that Mandiant and Google reported in September 2026, per Krebs on Security), and any VPN gateway on the CISA exploited list.
- Customers of managed service providers and outsourced help desks, which DragonForce and ShinyHunters-branded crews use as a way in.

Sectors in scope: Manufacturing, Professional services, Technology, Healthcare and public health, Retail, Financial services, Government, Education.

05 What changed since the last edition

EACH CHANGE WITH ITS SOURCE

01 The leaderboard turned over. ReliaQuest counted 300 incidents for The Gentlemen against 289 for Qilin from March to May 2026, ending a year in which Qilin was the most prolific group every quarter, and leaked chat logs suggest The Gentlemen use AI tools to ship new versions faster than rivals.

SOURCE 4

02 Qilin kept posting after a suspected leading member was caught: a Russian national was detained at an Osaka hotel in May 2026 and extradited to Germany, where BleepingComputer reports he was arrested; Japan has confirmed the extradition, and reports differ on the handover date. BleepingComputer notes the group has listed more than 450 victims since June.

SOURCE 12

03 Akira, DragonForce and LockBit 5.0 hold the next three places by volume. Brandefense counted Akira at 169 victims, DragonForce at 144 and LockBit 5.0 at 115 in Q2 2026, with DragonForce new to the top five and LockBit back in it.

SOURCE 6

04 Data-theft crews moved up. The FBI says ShinyHunters extorted more than $70 million so far in 2026, and Krebs on Security reports arrests in the Netherlands and Pennsylvania in September and October 2026 and a reported detention of a suspect known as Rey.

SOURCE 23

05 Old leaders left the field. Ransomware.live shows ALPHV's last listed victim on March 3, 2024, Black Basta's on January 11, 2025, and RansomHub's and BianLian's on March 31, 2025.

SOURCE 31

06 Clop returned with a new mass-exploitation campaign against PTC Windchill and FlexPLM (CVE-2026-12569) in July 2026, using JSP web shells. PTC began patching on June 17, CISA added the flaw to its exploited list, and ReliaQuest says the actor is unconfirmed but the tradecraft resembles earlier Clop campaigns.

SOURCE 25

07 Payments fell while volume rose. Chainalysis measured over $820 million in 2025, down 8 percent from a revised $892 million for 2024, as claimed attacks rose about 50 percent and the median payment grew 368 percent to $59,556.

SOURCE 8

08 The FBI's 2025 IC3 report, published in April 2026, ranks Akira first and Qilin second among reported ransomware variants and reports $20.877 billion in total reported losses, up 26 percent from 2024.

SOURCE 2

06 What to do now

IN PRIORITY ORDER, HIGHEST IMPACT FIRST

01 DO FIRST **Patch, inventory and harden every internet-facing VPN, firewall and remote access gateway (Check Point, Palo Alto, SonicWall, Fortinet, Cisco), reset credentials on devices that ever ran vulnerable firmware, and enforce MFA.**

Qilin, Akira and The Gentlemen all enter through these devices, and patched systems have carried live attacker sessions.

02 **Move administrator, VPN and remote management access to phishing-resistant MFA (FIDO2 keys or passkeys) and remove SMS and push approval for admins.**

ShinyHunters-branded vishing captures one-time codes and registers the attacker's own device.

03 **Require callback verification and manager approval before any password or MFA reset, including by your outsourced help desk, and rehearse the vishing call.**

Help desk impersonation is the entry point for the crews that inherited Scattered Spider's playbook.

04 **Keep immutable, offline backups, separate backup credentials, and harden ESXi and Veeam hosts.**

Akira, The Gentlemen and DragonForce target hypervisors and backup servers to make recovery fail.

05 **Turn on EDR tamper protection and the Microsoft vulnerable driver blocklist, and alert on driver loads, security tool stops and event log clearing.**

EDR killers and signed vulnerable drivers are standard in Akira and The Gentlemen cases.

06 **Patch and hunt on enterprise and file-transfer applications within days: Oracle E-Business Suite and PeopleSoft, PTC Windchill and any managed file transfer product.**

Clop and ShinyHunters monetize mass exploitation and data theft without encrypting anything.

07 **Audit SaaS tenants and vendor access, including Salesforce guest permissions, MSP remote monitoring tools and contractor accounts.**

DragonForce and ShinyHunters-branded crews reach victims through providers and misconfigured cloud apps.

08 If nobody watches VPN logins, sign-on anomalies and backups overnight, Z7's 24/7 SOC and Microsoft 365 posture review cover that gap.

Breakout from first access to encryption is measured in days at best and often happens outside business hours.

07 Sources

[1] **Check Point Warns Ransomware Threat Is Spreading Wider (reporting Check Point's State of Ransomware, Q2 2026)** Security MEA · August 2026. https://securitymea.com/?p=68298

[2] **2025 Internet Crime Report** FBI Internet Crime Complaint Center · April 2026 (PDF dated April 16, 2026). https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[3] **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/

[4] **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/

[5] **Hospitality Hacks and Retail Reality Checks: The Gentlemen ransomware** Palo Alto Networks Unit 42 · July 10, 2026. https://unit42.paloaltonetworks.com/the-gentlemen-ransomware/

[6] **Top 5 Ransomware Groups in Q2 2026: Who They Are, How They Operate, and What They Target** Brandefense · Q2 2026 review. https://brandefense.io/blog/top-5-ransomware-groups-q2-2026/

[7] **Ransomware activity concentrated in a few groups (reporting GuidePoint GRIT Q2 2026 report)** Cybersecurity Dive · July 9, 2026. https://www.cybersecuritydive.com/news/ransomware-concentrated-ai-guidepoint/824828/

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

[9] **Adverse cyber extortions are more common than commonly advised (Q2 2026 quarterly report)** Coveware by Veeam · July 29, 2026. https://coveware.com/2026/07/adverse-cyber-extortions-are-more-common-than-commonly-advised/

[10] **Insider Threats Loom while Ransom Payment Rates Plummet (Q3 2025 quarterly report)** Coveware by Veeam · October 24, 2025. https://coveware.com/2025/10/insider-threats-loom-while-ransom-payment-rates-plummet/

[11] **Why Zero-Day Downstream Mass Data Extortion Campaigns are Losing Their Bite (Q4 2025 quarterly report)** Coveware by Veeam · February 3, 2026. https://coveware.com/2026/02/why-zero-day-downstream-mass-data-extortion-campaigns-are-losing-their-bite/

[12] **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/

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

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

[15] **Threat group profile: LockBit (5.0)** Halcyon · updated July 27, 2026. https://www.halcyon.ai/threat-group/lockbit

[16] **Threat group profile: DragonForce** Halcyon · updated July 27, 2026. https://www.halcyon.ai/threat-group/dragonforce

[17] **Threat group profile: Play** Halcyon · updated July 27, 2026. https://www.halcyon.ai/threat-group/play

[18] **Threat group profile: INC Ransom** Halcyon · updated July 27, 2026. https://www.halcyon.ai/threat-group/inc-ransom

[19] **Threat group profile: SafePay** Halcyon · updated July 27, 2026. https://www.halcyon.ai/threat-group/safepay

[20] **Threat group profile: ShinyHunters** Halcyon · updated July 27, 2026. https://www.halcyon.ai/threat-group/shinyhunters

[21] **#StopRansomware: Akira Ransomware (AA24-109A)** CISA, FBI, Europol EC3 and partners · April 18, 2024, updated November 13, 2025. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a

[22] **#StopRansomware: Medusa Ransomware (AA25-071A)** CISA, FBI and MS-ISAC · March 12, 2025, updated August 18, 2026. https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-071a

[23] **FBI Arrests Founder of Ransomware Negotiation Firm** Krebs on Security · October 9, 2026. https://krebsonsecurity.com/2026/10/fbi-arrests-founder-of-ransomware-negotiation-firm/

[24] **ShinyHunters Extorted Boeing Spin-off Prior to Arrests** Krebs on Security · October 7, 2026. https://krebsonsecurity.com/2026/10/shinyhunters-extorted-boeing-spin-off-prior-to-arrests/

[25] **Clop ransomware targets Windchill, FlexPLM in data theft attacks** BleepingComputer · July 24, 2026. https://www.bleepingcomputer.com/news/security/clop-ransomware-targets-windchill-flexplm-in-data-theft-attacks/

[26] **ShinyHunters hacks Clop leak site, threatens to extort ransomware gang** BleepingComputer · September 19, 2026. https://www.bleepingcomputer.com/news/security/shinyhunters-hacks-clop-leak-site-threatens-to-extort-ransomware-gang/

[27] **Black Basta boss makes it onto Interpol's 'Red Notice' list** BleepingComputer · January 16, 2026. https://www.bleepingcomputer.com/news/security/black-basta-boss-makes-it-onto-interpols-red-notice-list/

[28] **US ransomware negotiators get 4 years in prison over BlackCat attacks** BleepingComputer · May 1, 2026. https://www.bleepingcomputer.com/news/security/us-ransomware-negotiators-get-4-years-in-prison-over-blackcat-attacks/

[29] **Check Point links VPN zero-day attacks to Qilin ransomware gang** BleepingComputer · June 8, 2026. https://www.bleepingcomputer.com/news/security/check-point-links-vpn-zero-day-attacks-to-qilin-ransomware-gang/

[30] **Critical Palo Alto VPN bug now exploited by Qilin ransomware gang** BleepingComputer (reporting Arctic Wolf Labs) · July 21, 2026. https://www.bleepingcomputer.com/news/security/critical-globalprotect-vpn-bug-now-exploited-in-ransomware-attacks/

[31] **Ransomware.live group listings** Ransomware.live · checked October 14, 2026. https://www.ransomware.live/groups

[32] **Ransomware.live statistics** Ransomware.live · checked October 14, 2026. https://www.ransomware.live/stats

[33] **Police disrupts Rhadamanthys, VenomRAT, and Elysium malware operations** BleepingComputer (reporting Europol) · November 13, 2025. https://www.bleepingcomputer.com/news/security/police-disrupts-rhadamanthys-venomrat-and-elysium-malware-operations/

[34] **Amadey, StealC malware operations disrupted in Operation Endgame action** BleepingComputer (reporting Europol) · June 24, 2026. https://www.bleepingcomputer.com/news/security/amadey-stealc-malware-operations-disrupted-in-operation-endgame-action/

[35] **United States, Australia, and United Kingdom Sanction Russian Cybercrime Infrastructure Supporting Ransomware** U.S. Department of the Treasury · November 19, 2025. https://home.treasury.gov/news/press-releases/sb0319

[36] **Europol-led crackdown on The Com hackers leads to 30 arrests** BleepingComputer (reporting Europol) · February 27, 2026. https://www.bleepingcomputer.com/news/security/police-crackdown-on-the-com-cybercrime-gang-leads-to-30-arrests/

[37] **Europol disrupts pro-Russian NoName057(16) DDoS hacktivist group** BleepingComputer (reporting Europol) · July 16, 2025. https://www.bleepingcomputer.com/news/security/europol-disrupts-pro-russian-noname05716-ddos-hacktivist-group/

[38] **Ukrainian hacker charged with helping Russian hacktivist groups** BleepingComputer (reporting the DOJ) · December 10, 2025. https://www.bleepingcomputer.com/news/security/ukrainian-hacker-charged-with-helping-russian-hacktivist-groups/

[39] **Spain arrests suspected member of pro-Russian hacktivist groups** BleepingComputer (reporting Spain's National Police) · July 7, 2026. https://www.bleepingcomputer.com/news/security/spain-arrests-suspected-member-of-pro-russian-hacktivist-groups/

[40] **Checkmarx confirms LAPSUS$ hackers leaked its stolen GitHub data** BleepingComputer · April 28, 2026. https://www.bleepingcomputer.com/news/security/checkmarx-confirms-lapsus-hackers-leaked-its-stolen-github-data/

[41] **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/

[42] **2025 crypto theft: over $3.4 billion stolen through early December** Chainalysis · December 2025. https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2026/

[43] **Change Healthcare Responding to Cyberattack (running tracker)** HIPAA Journal · updated August 6, 2025. https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/

[44] **FinCEN says ransomware gangs extorted over $2.1B from 2022 to 2024** BleepingComputer (reporting FinCEN) · December 8, 2025. https://www.bleepingcomputer.com/news/security/fincen-says-ransomware-gangs-extorted-over-21b-from-2022-to-2024/

[45] **Record ransomware surge as 7,458 victims named in 2025 (reporting Searchlight Cyber)** SecurityBrief UK · February 18, 2026. https://securitybrief.co.uk/story/record-ransomware-surge-as-7-458-victims-named-in-2025

[46] **Cost of a Data Breach Report 2026** IBM and Ponemon Institute · 2026 edition. https://www.ibm.com/reports/data-breach

[47] **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/

[48] **United Kingdom National Charged in Connection with Multiple Cyber Attacks, Including on Critical Infrastructure** U.S. Department of Justice · September 18, 2025. https://justice.gov/opa/pr/united-kingdom-national-charged-connection-multiple-cyber-attacks-including-critical

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

[50] **Scattered Spider Hacker Arrests Halt Attacks, Mandiant Says** The Hacker News (reporting Mandiant Consulting) · July 30, 2025. https://thehackernews.com/2025/07/scattered-spider-hacker-arrests-halt.html

[51] **Scattered Lapsus$ Hunters extortion site goes dark: What's next?** CSO Online · October 14, 2025. https://www.csoonline.com/article/4072244/scattered-lapsus-hunters-extortion-site-goes-dark-whats-next.html

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

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.