GUIDEPOINT® SECURITY

2026 Ransomware and Cyber Threat Report

A GRIT® Report

2026 Annual

Contents

A Note From GRIT

Welcome to GRIT's 2026 Ransomware and Cyber Threat Insights report, our flagship annual review of the trends, tactics, and context that GuidePoint's Research and Intelligence Team (GRIT) have observed over the past year. This report is an annual labor of love, an opportunity for our analysts to look backward and forward to inform our friends, colleagues, and professional peers.

Artificial Intelligence / Large Language Models (AI/LLM) present as an inescapable force in this year's report, no matter how sick we all are of hearing the term in this industry. Threat actors continue to evolve in their tactics, techniques, and procedures (TTP), with AI/LLM enabling more rapid adaptation and continuing to reduce barriers to entry for less-skilled and unskilled actors. The news is not all bad here – trickle-down benefits of innovation introduced by skilled actors takes time, and Defenders have also benefited from this technology. We hope that by the end of this report, you will better understand the reality of this threat, free of unnecessary fear, uncertainty, or doubt.

Our report concludes with our annual signpost analysis and opportunity for our team to foot-stomp what we assess to be the most impactful and substantial elements that will impact the ransomware and cybercrime landscape in the near and mid-term. We encourage our colleagues to consider these factors in their intelligence programs and organizational threat modeling.

Finally, for our readers – thank you for joining us for this year's report. As an analytic organization as well as a services team, we believe that improvement is continuous. If you believe we have erred in our assessments, failed to consider key information, or just want to share your hot take from this year's report, we would love to hear from you. While we can't guarantee a response to everything, you can contact us at GRITBlog@guidepointsecurity.com

Happy Hunting.

- GRIT

Methodology

- Data collected for this report was obtained from publicly available resources, including the sites and blogs of threat groups themselves. It has not been validated by alleged victims. As a result of these sources, as well as unknowable outcomes and figures of victims which have not been publicly disclosed, the number of observed attacks in this report and the total number of attacks conducted will not be equal.
- Collected data has been reviewed by GRIT for potential duplications or inaccuracies and adjusted accordingly to best reflect the true impacts of ransomware and cybercrime. We note that ransomware and cybercrime groups are likely to employ denial and deception to complicate research efforts and retain or build credibility among peers. To this end, we have reviewed each group and validated that its claims are at least as likely as not to be genuine before including them in our data set. While our process does effectively rule out clear fabricators, we cannot completely rule out groups in which the number or qualities of victims may have been exaggerated or inflated. As a result of these differences in our approach, our numbers may periodically differ from other public reporting, particularly if this reporting does not scrutinize group claims and history.
- We note that throughout this report's analysis of ransomware, we include data and analysis of several groups that may be better described as "extortion" groups rather than "ransomware" groups. These groups may eschew encryption and instead focus only on data exfiltration and extortion. Or they may not perform intrusion operations of any kind, instead extorting or re-extorting organizations based on historically compromised data. While these groups do not deploy ransomware, we are including them in our ransomware reporting due to their relationships with other ransomware groups and their impact on the extortion-based cybercrime environment.
- Finally, we make efforts to exclude from our data those groups which self-identify as "hacktivists", compromised data brokers and markets, or non-financially motivated data thieves and leakers which may employ similar TTPs as ransomware and other cybercriminal groups. While these actors and venues doubtlessly have impacts, we distinguish them from financially-motivated cybercrime and data extortion, which is the primary focus of this report.
- Despite the above caveats, we have always and continue to assess that our reporting and our data is useful in aggregate while acknowledging that the underlying data sources have variability. We strongly believe that this report provides a consistent and accurate representation of the threat landscape over a given period, and that our observations of the underlying trends remain valuable for Defenders.
- In cases where we leverage datasets that were not uniquely collected by us, we endeavor to cite the source appropriately.

Annual Ransomware Summary

As we publish our fourth annual report analyzing ransomware, we close the chapter on another year of observing, fighting, and defending against contemporary crime. This one places a heavy emphasis on ransomware across the public and private sectors. What initially started as a somewhat "average" year in terms of growth surprised us by the end of December, shattering all records and resulting in a 58% Year-over-Year (YoY) increase in the number of observed ransomware victims, claimed by a record-breaking 124 distinct named groups.

2025 demonstrated the staying power and adaptability of contemporary ransomware operations. While we note and appreciate the efficacy of 2024's broad law enforcement disruption efforts, former mid-tier groups, such as Qilin and Akira, have stepped in to fill the spots formerly filled by LockBit and Alphv, likely absorbing affiliates in the process. Still other groups, such as RansomHub, have obtained short-term successes only to be undone by internal deceit and infighting – with the associated affiliates similarly reorganizing under other groups.

We continued to observe indications of threat actor adoption of AI/LLMs in their operations, though we have found concerns of super-affiliates deploying fully autonomous ransom-bots to be overstated. AI/LLM usage remains rudimentary among less mature threat actors, though the more sophisticated and experienced operators have prioritized finding new means and manners of incorporating AI. Their successes will almost certainly trickle down over time in the same way that vulnerability exploitation has for years.

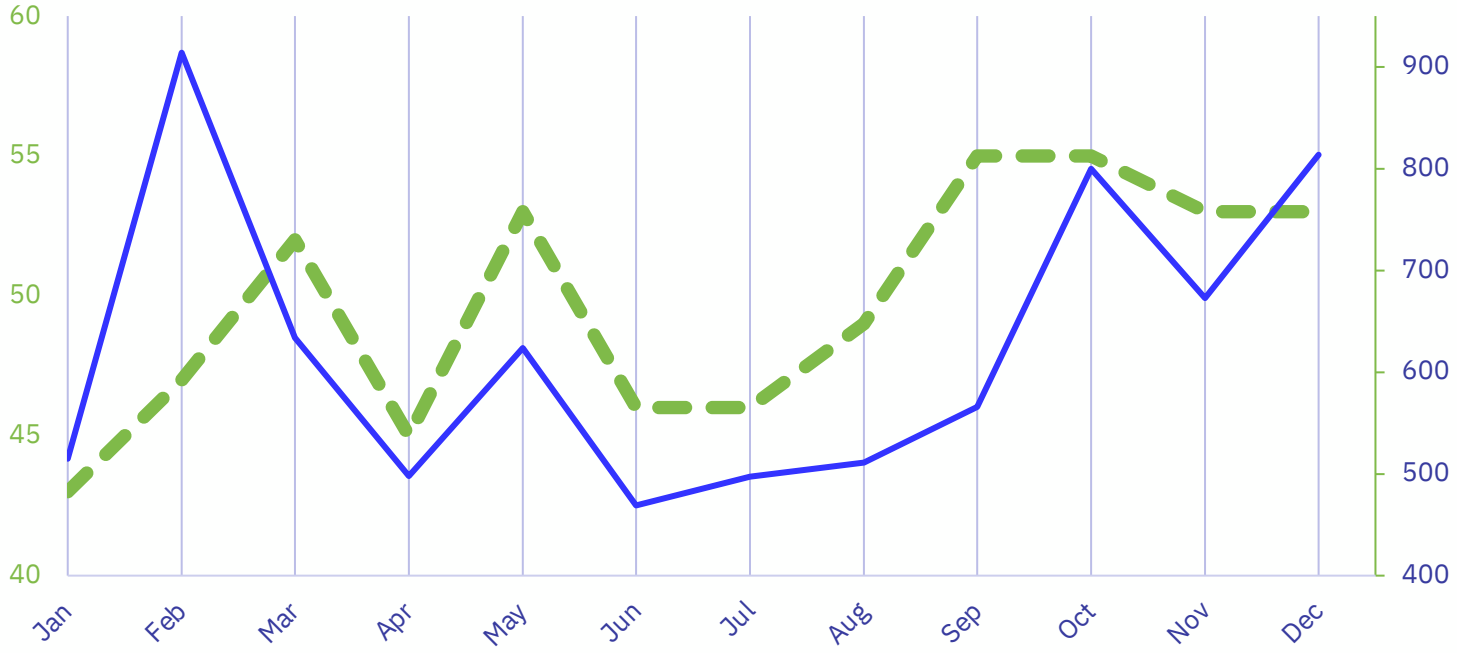
In this year's report, we have had the opportunity and interest to focus on threat actor innovation efforts, on the profitability of the most prolific ransomware groups, and on what we believe to be the most impactful variables that will drive or hinder ransomware activity across the near- and mid-term. To do so, we have leveraged new tools to provide new perspectives, while continuing to apply the insight and analysis gleaned from the hundreds of ransomware and cybercrime incident response cases that GuidePoint supports every year.

As always, with a litany of causes for concern come opportunities for optimism, as we continue to see growing international law enforcement collaboration and disruption efforts targeting not just ransomware, but cybercrime's underlying support infrastructure as well. As we enter 2026, we continue to view the age-old dynamic of criminals vs. defenders and law enforcement. Neither intend to slow down. More than ever, 2025 has highlighted the dense concentration of expertise and competence within an otherwise sprawling ecosystem.

Total Publicly Posted Ransomware Victims	7,515
Number of Tracked Ransomware Groups	124
Average Daily Victims	20.6

Annual and Q4 2025 Ransomware Trends

Rate of Publicly Posted Ransomware Victims, 2025



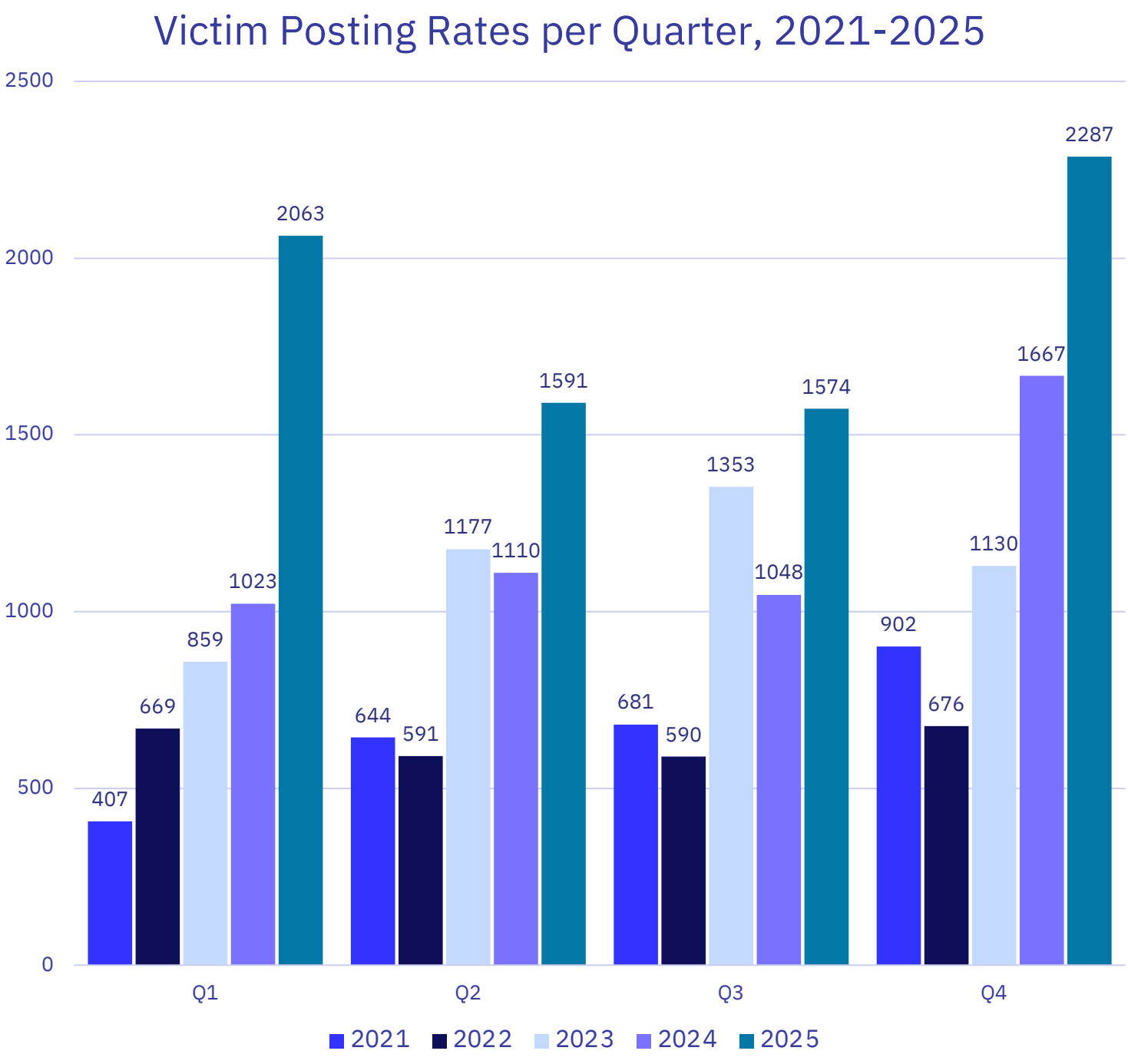
Total Posts	Total Groups	Average Posts per Week	Distinct Groups Posting per Week
7,515	**124**	**145**	**28**

2025 proved to be another record-setting year for ransomware activity. The number of ransomware victims we observed, as posted by ransomware groups, peaked fairly early in the year (in February), driven by activity from the data extortion group, Clop. We note this principally because the group's preceding mass exploitation campaign took place in 2024; however, victims were not posted en masse until 2025. We then observed what would appear to be a Q2 and Q3 decline, which we initially hoped could represent a "flattening of the curve." Regrettably, ransomware activity resurged throughout most of Q4 with record-breaking numbers closing out a record-breaking year.

As we have come to expect, the number of distinct named ransomware groups continues to rise YoY, with 124 distinct named groups observed over the course of 2025, a 46% YoY increase from 2024's 88. However, we note that no more than 28 distinct groups posted victims in any given week, reflecting the highly ephemeral nature of many new groups. Nonetheless, we observed numerous "newcomers" operating at a higher tempo suggestive of experienced operators, including "The Gentlemen" and "Coinbase Cartel."

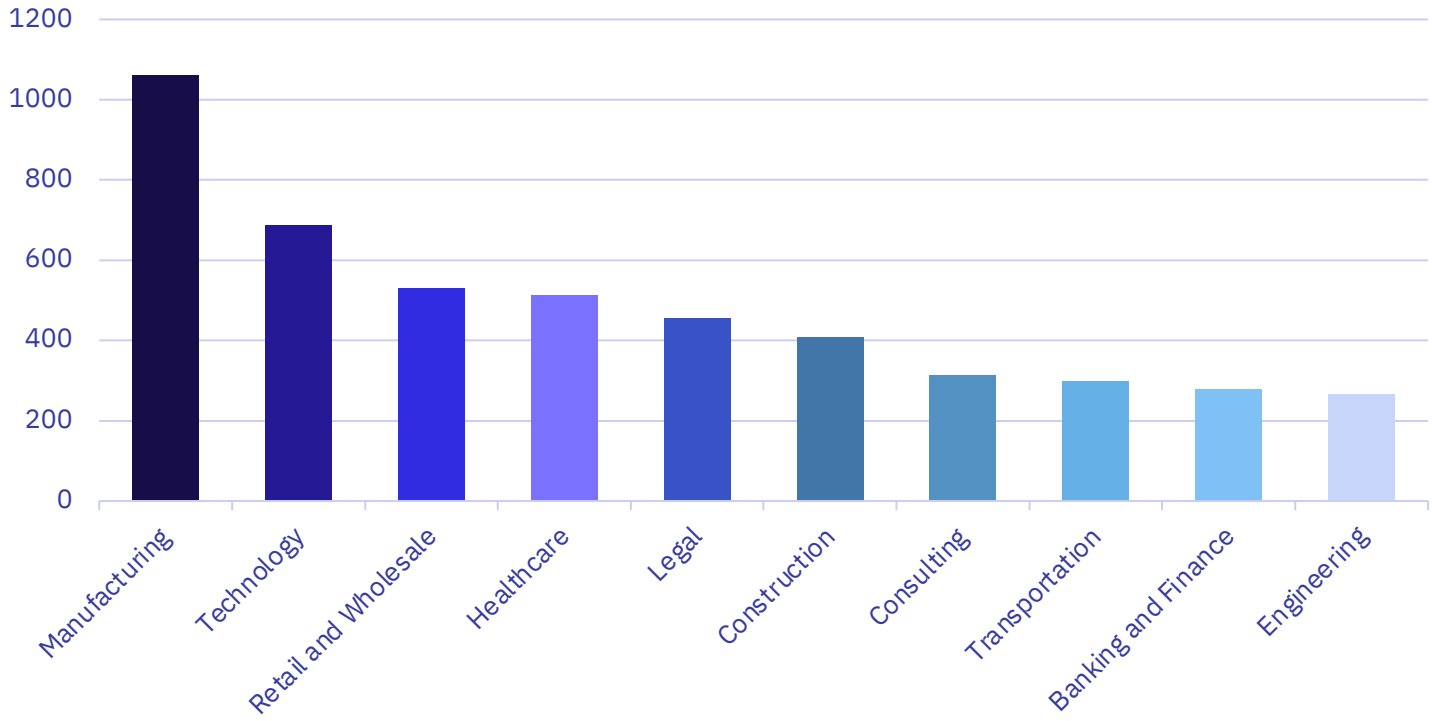
Each quarter of 2025 outpaced the same quarter of the preceding year by observed victim volume; Q1 provides the most vivid example, where 2025 (2,063 observed victims) more than doubled Q1 of 2024 (1023 observed victims).

The dramatic YoY increase was less pronounced over the remainder of 2025, but small differences added up. We observed similar “summer slowdowns” to those observed in 2024 and 2022, a trend we have hypothesized as attributable to summer vacations and warmer weather.



2025 Most Impacted Industries

- The Manufacturing industry claimed the most ransomware victim organizations in terms of volume, accounting for 1060 (or 14%) of all observed ransomware victims. Manufacturing remains a constant "most impacted" presence. Its increases have been both in real (+454 victims) and relative (+1.3%) YoY.
- The four most impacted industries in terms of victim volume – Manufacturing, Technology, Retail & Wholesale, and Healthcare – remained consistent in 2025 and 2024. While this can potentially be explained, in part, by the prevalence of the industries in the US economy, it also may speak to vulnerabilities or threats which uniquely impact organizations in these industries. We note that these industries are more likely to experience financial or operational losses from ransomware's impacts on networks, and to hold high-value or particularly sensitive data, such as PII and PHI.
- Akira claimed responsibility for the highest number of observed victims against four of five top industries, excluding only the Healthcare industry, which was disproportionately impacted by Qilin. Our observations show disparities in healthcare impacts by different groups in recent years, with some Ransomware as a Service (RaaS) groups prohibiting or discouraging attacks (or at least encryption) against healthcare organizations. While we do not know whether Akira employs such rules, we do expect to see a disparity in the healthcare industry in terms of "top offenders" relative to other industries.



Manufacturing
- Qilin
- Akira
- Play

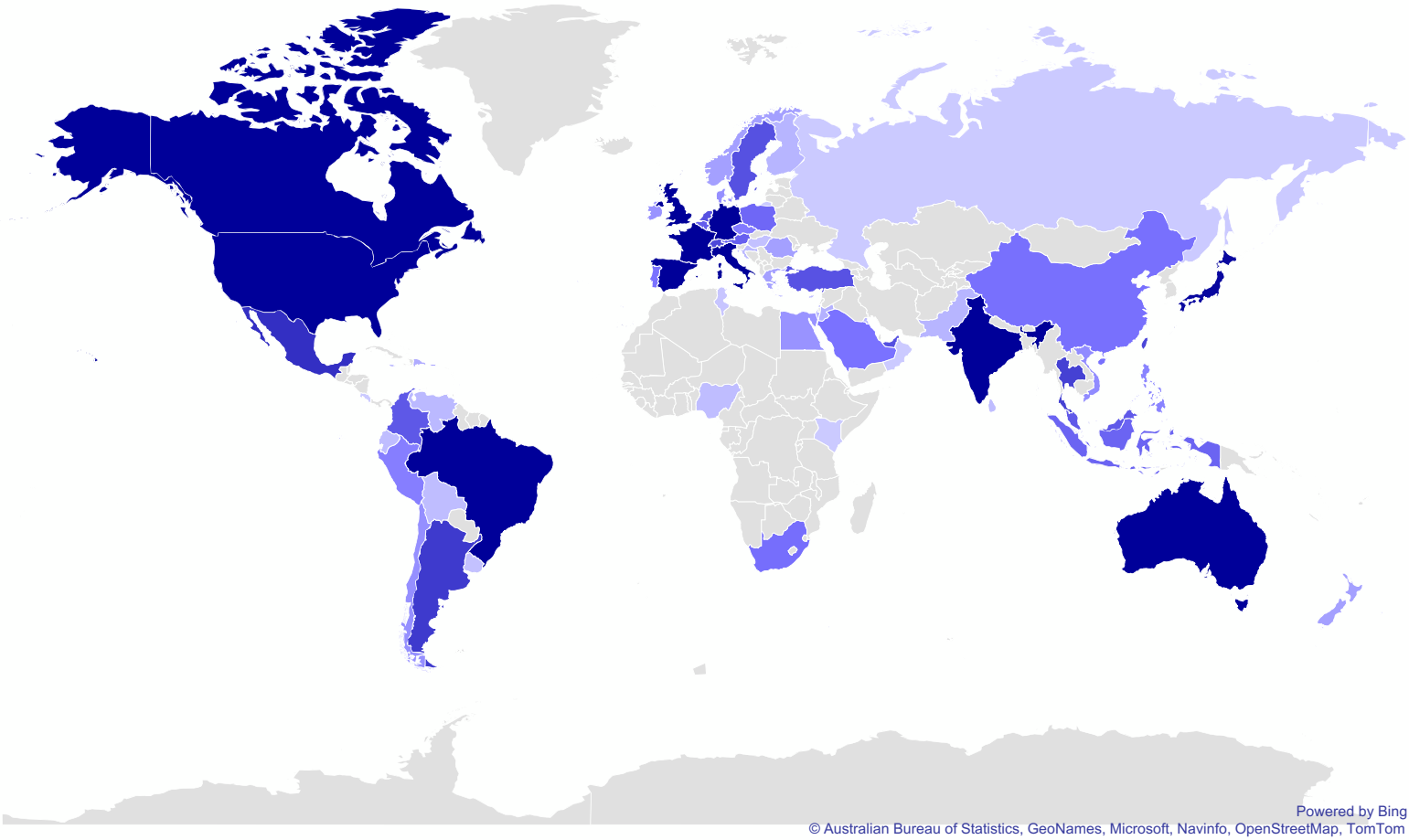
Technology
- Qilin
- Clop
- Akira

Retail & Wholesale
- Clop
- Qilin
- Akira

Healthcare
- Qilin
- INC Ransom
- SafePay

Legal
- Akira
- Qilin
- Silent

Geographic Breakdown of Ransomware Victims, 2025

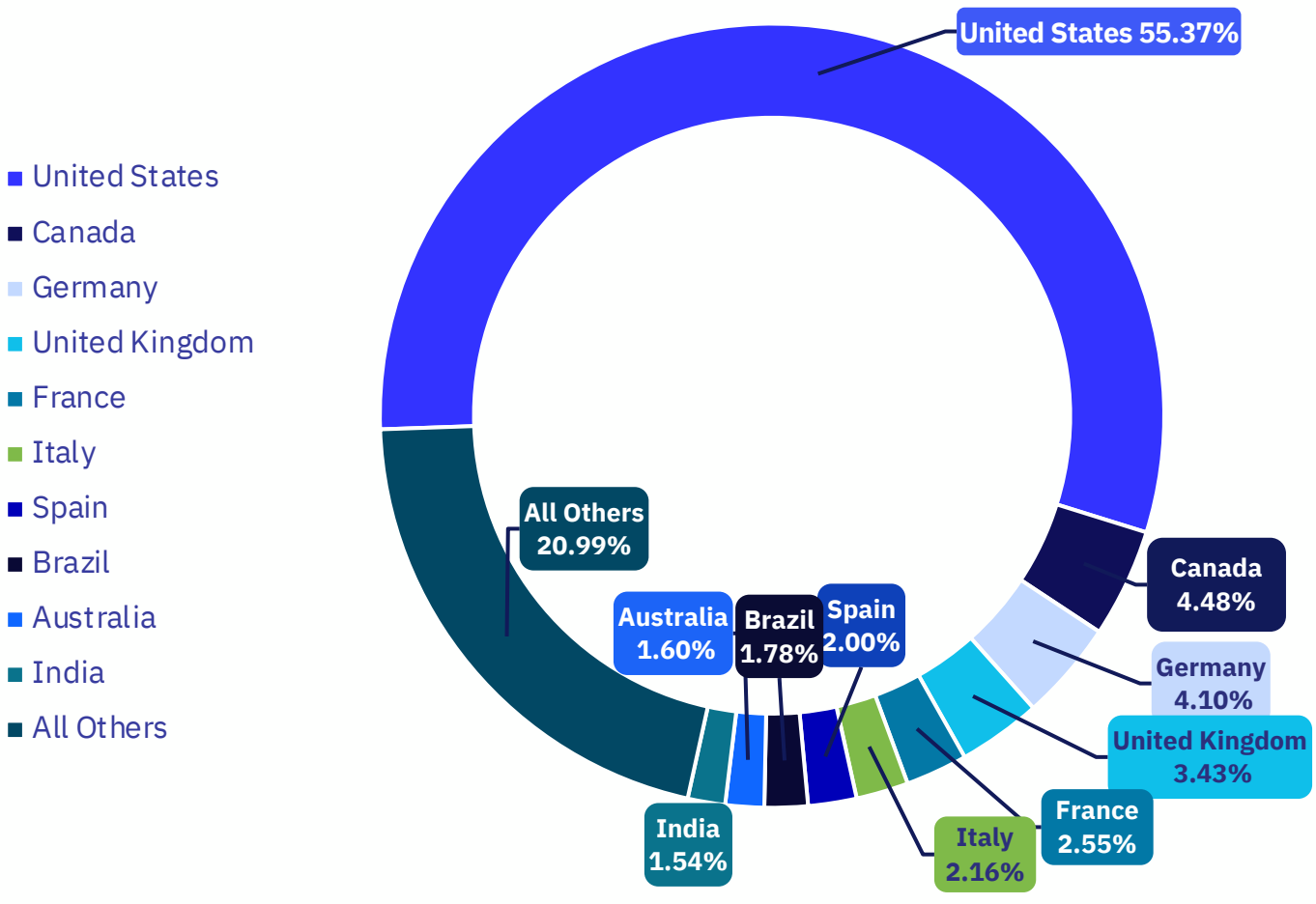


Top 10:

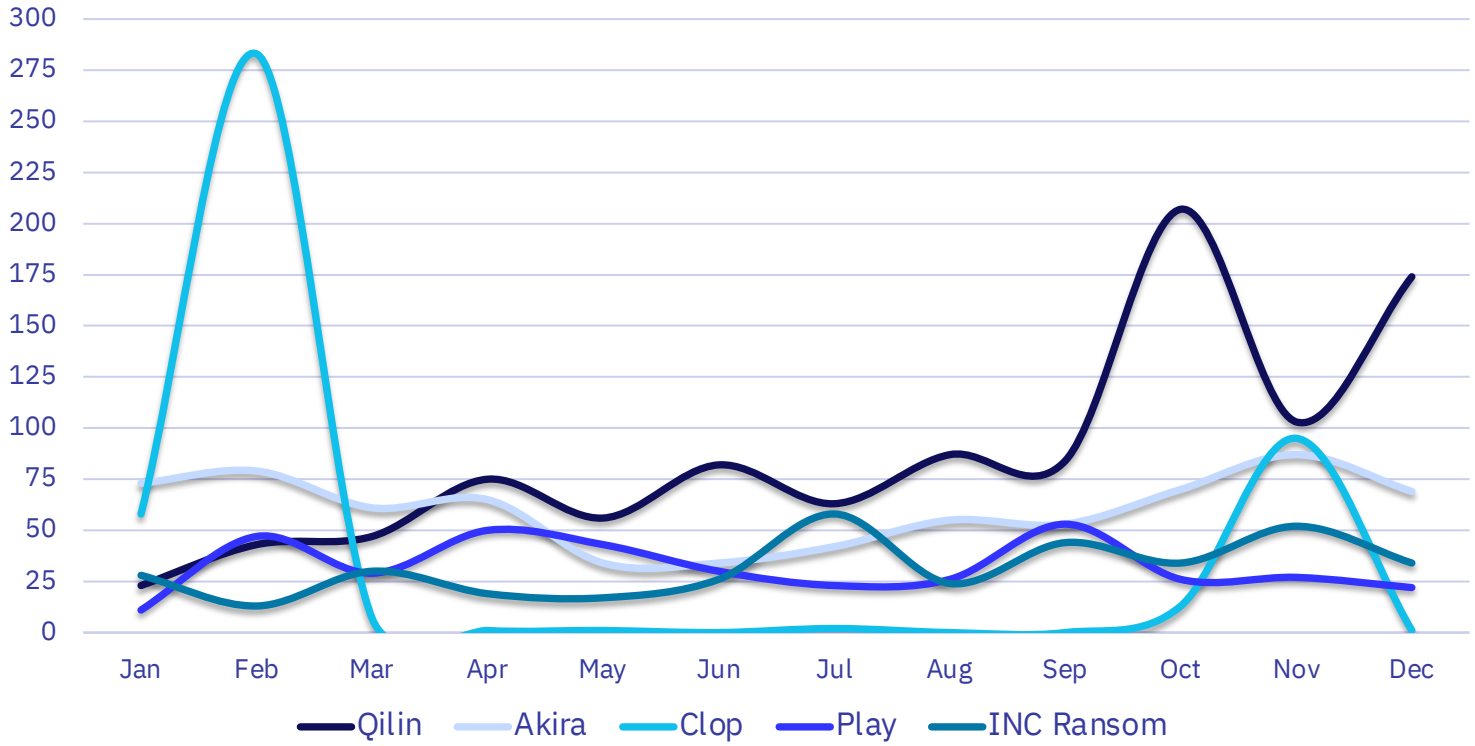
1.	United States	4161 (55.37%)
2.	Canada	337 (4.48%)
3.	Germany	308 (4.10%)
4.	United Kingdom	258 (3.43%)
5.	France	192 (2.55%)
6.	Italy	162 (2.16%)
7.	Spain	150 (2.00%)
8.	Brazil	134 (1.78%)
9.	Australia	120 (1.60%)
10.	India	116 (1.54%)

2025 Ransomware Impacts by Country

- Continuing a long-established trend, the United States remains the country most impacted by ransomware. The US accounted for over 55% of observed victims and outpaced all other countries combined. This disparity can be driven by a myriad of factors, including the absence of bans on ransom payments, low reporting requirements, and economic viability of US victims to "afford" ransom payments. In other words, US victims remain attractive targets because they are more likely to pay.
- The remaining "top 10" countries by victim volume stay largely consistent with 2024, comprised primarily of western European developed economies (Germany, United Kingdom, France, Italy, Spain) and other "Western" nations (Canada, Australia). Brazil and India, as developing economies, are outliers but likely present a growing target-rich environment for attackers.



2025 Most Impactful Ransomware Groups



Qilin

- Qilin, which first appeared in 2024, rose to much greater prominence in 2025 by publicly claiming the most victims. While Qilin's open recruitment model for affiliates likely allows the group's affiliates to attack in greater numbers, the rate of payment vs. non-payment is lower than other groups, which we explore later in this report. Ultimately, this means that while Qilin is the most prolific in terms of victims, they are far from the most "profitable."

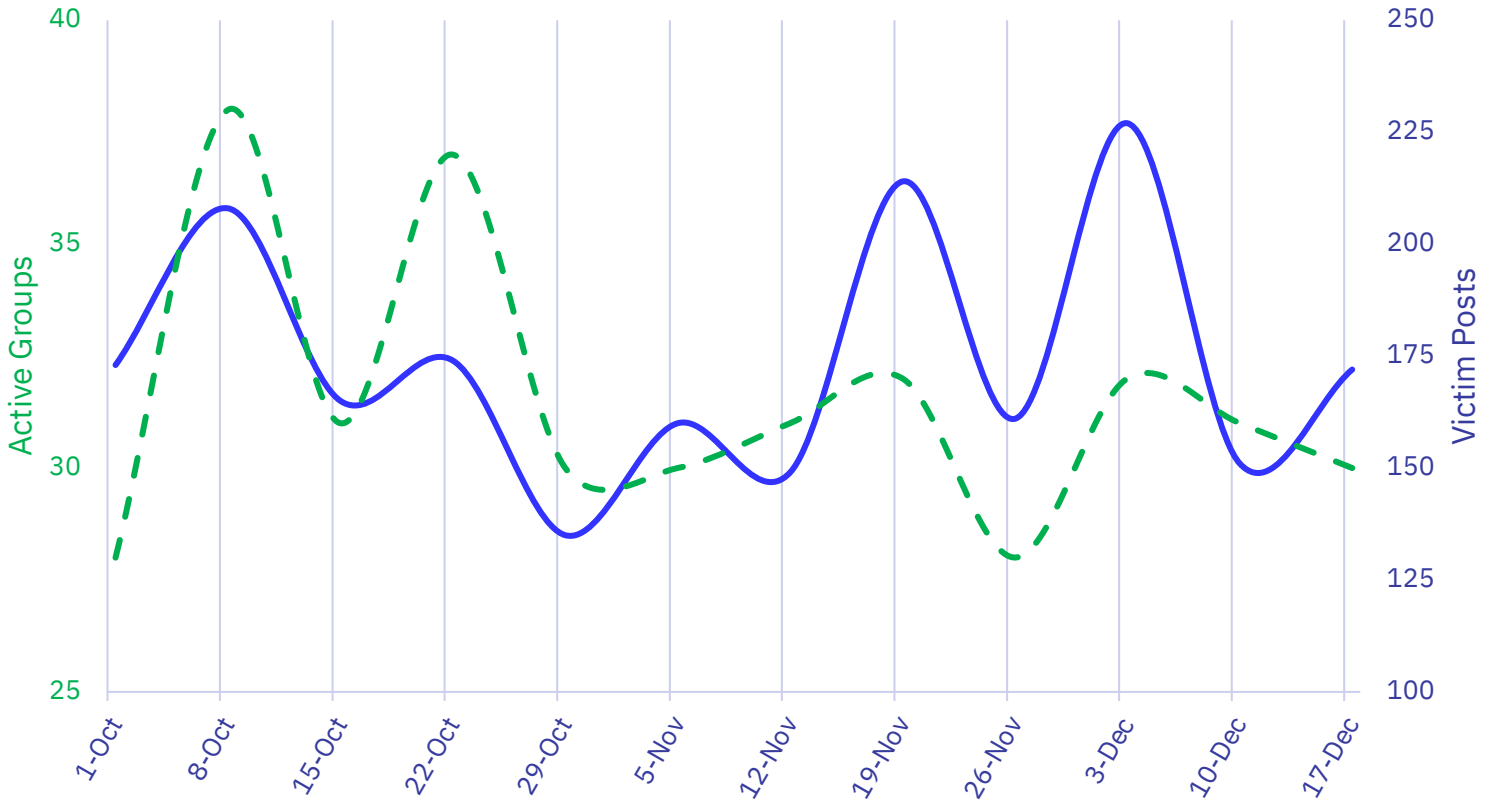
Akira

- Akira, one of the longest-operating RaaS groups (it emerged in 2023), remains prolific. It was responsible for the second-highest number of observed victims in 2025. In recent years, Akira has shown a propensity for exploiting "zero-day" and "n-day" vulnerabilities on perimeter devices. In 2025, Akira's mass exploitation of the SonicWall SSL VPNs led to a surge of attacks in Q3 and Q4. Notably, Akira operates on a seemingly closed recruitment model, suggesting a greater emphasis on experienced affiliates and/or operational security.

Clop

- Clop, a data extortion group that has eschewed ransomware deployment in favor of mass vulnerability exploitation campaigns, was responsible for two such campaigns between late 2024 and 2025. Clop's surge in February 2025 is a result of 2024 attacks against the Cleo managed file transfer platform. It's November surge was the result of a campaign targeting Oracle's eBusiness Suite (EBS). Cumulatively, these two campaigns accounted for 461 victims, though payment rates were extremely low relative to double-extortion ransomware groups.

Q4 2025 Daily Victim Posts and Active Groups by Week

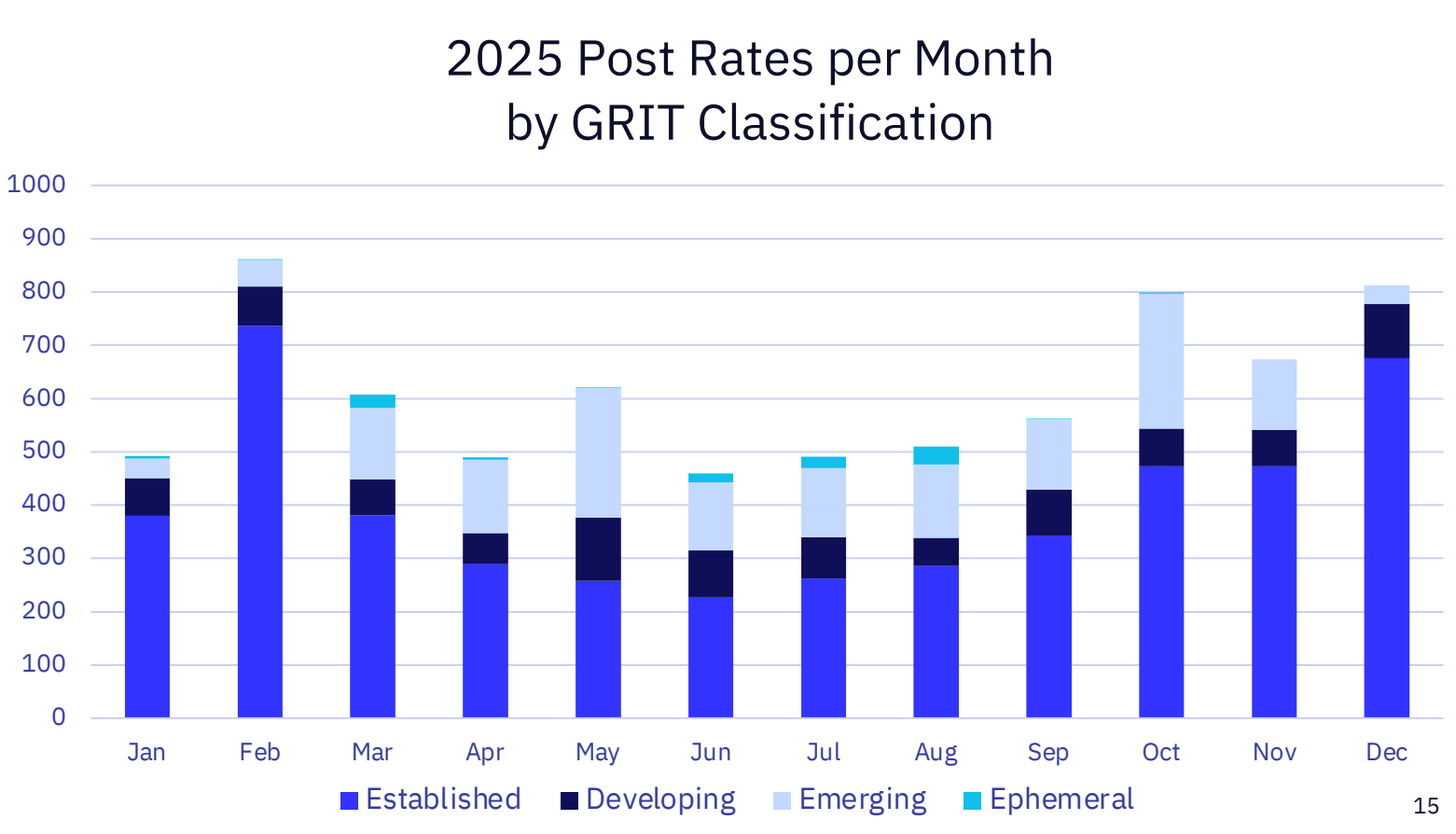


- Q4 shattered records for the highest number of observed ransomware victims in a single quarter since GRIT began tracking ransomware data in 2022. At 2,287 observed victims, Q4 accounted nearly a third of the year's total, and a 45% YoY increase over 2024's Q4 victim count of 1,576.
- LockBit has resurged in an apparent fifth iteration during Q4, despite numerous setbacks stemming from their 2024 disruption at the hands of international law enforcement and being relegated to near irrelevance by the imposition of international sanctions. In 2024, sanctions were imposed by the United States, United Kingdom, and Australia which proscribed payments to LockBit or its affiliates. "LockBit 5.0," whether under historical or new leadership, returned to prominence with 106 claimed victims in December 2025 alone.
- Sinobi, a relative newcomer, also increased operational activity in Q4. First observed in mid-2025, Sinobi claimed 149 victims in Q4, reflecting an operational tempo more closely associated with Established threat groups than Emerging or Developing ransomware groups. In addition, the group's data leak site is nearly identical to that of Lynx ransomware, and Sinobi's ransomware includes whitelisting for Lynx files. While not conclusive, these connections suggest that Sinobi boasts at least some experienced affiliates within its ranks.

Annual Taxonomy Trends

2025 Activity by GRIT Taxonomy Classification

- Established ransomware groups, or those we consider to be the most organized, prolific, and long-running, continued to account for the majority of observed victims in 2025. Established groups often benefit from more experienced affiliates, economies of scale, and visible data leak sites which support greater volumes of attacks.
- GRIT identified a swell of Emerging or newer groups that have not been ruled out as short-term Ephemeral groups in May and October. This increase impacted “market share” of victims relative to the longer-running Established and Developing groups.
- Manufacturing, Technology, and Healthcare remained the most impacted industries by all group types, reflecting their value and interest across groups of varying sizes and sophistication. Ephemeral groups were more likely to impact Banking and Finance victims, though we note that this observation does not provide insight into the breadth and depth of those attacks relative to more mature groups.
- The United States, Canada, and the United Kingdom, were among the most impacted countries across all group types except for Emerging and Ephemeral groups. Interestingly, these less mature groups were more likely to impact a wider swath, including Spanish and Indian victims.



Threat Actor Spotlight: Qilin

Threat Actor Spotlight: Qilin

Qilin emerged within the RaaS landscape in June 2024. It first gained wide recognition for its 2024 attack on Synnovis, a UK-based medical laboratory company. The attack reportedly resulted in over 40 million USD in loss to the company and a major disruption in operations. Although it had already made a name for itself through that attack, Qilin appears to have increased its number of affiliates and operational tempo substantially in 2025. The group went from 154 victims posted in 2024 to 1,044 by the end of 2025. This makes Qilin — by-far — the most prolific ransomware group GRIT observed in 2025.

One of Qilin's logos from the group's Data Leak Site
Source: Ransomlook.io

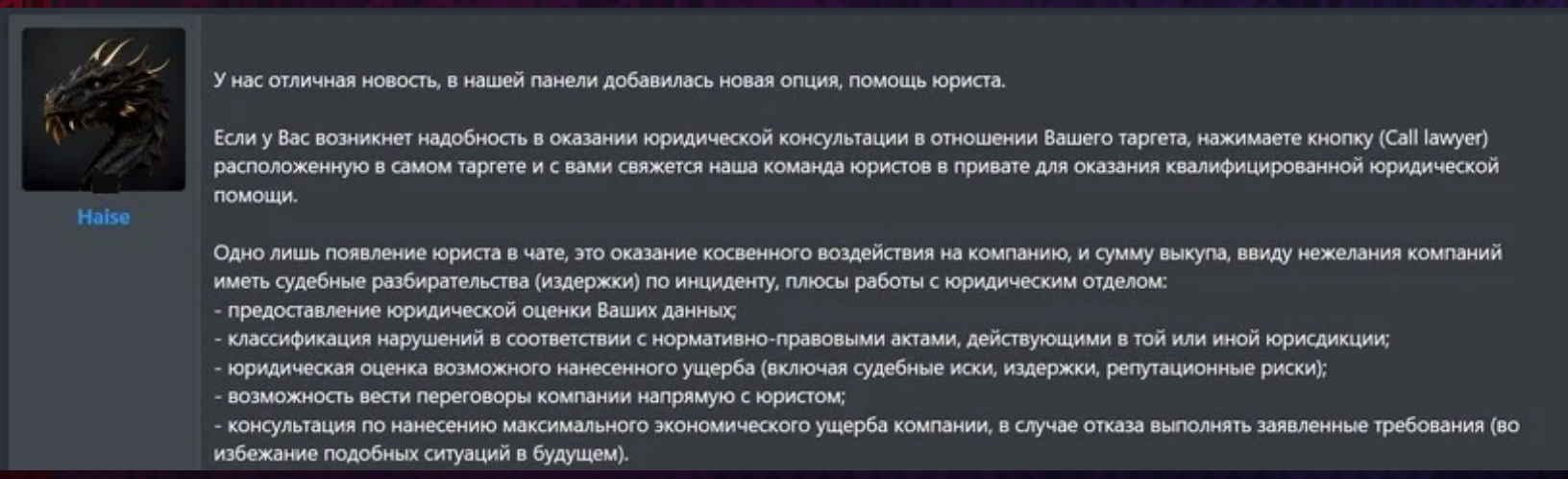
Qilin's affiliates are believed to operate primarily from eastern Europe, though limited reporting indicates that North Korean actors may have successfully deployed Qilin ransomware as part of revenue-generating operations. While Qilin emerged under its current name in 2024, the Qilin "brand" is assessed to be a rebrand of "Agenda" ransomware, a group that dates back to September 2022. Qilin primarily employs double-extortion ransomware tactics. These tactics rely on both encryption and data extortion to coerce compliance from victims.

Threat Actor Spotlight: Qilin

We assess that Qilin's growth in 2025 was likely fueled in part by affiliates who migrated to Qilin after the April shutdown of former major RaaS player, RansomHub. Following RansomHub's shutdown, the group increased its victim volume by 280%, rising from 188 victims at the end of April 2025 to nearly 800 by late October of the same year.

As a RaaS operator, Qilin uses an affiliate system that openly recruits potential affiliates on Dark Web forums. It licenses its ransomware to affiliates who conduct attacks, with the core group keeping a percentage of the ransom in exchange for maintaining the software and providing access to Qilin's data leak site and chat infrastructure. Qilin's affiliate program is competitive, with affiliates allegedly earning 80% on payments of $3 million USD or lower, and 85% for payments above $3 million USD.

Throughout 2025, Qilin added several features to its panel to increase its attractiveness to affiliates, including spam campaigns and automated ransom negotiation tools. The group introduced a "Call Lawyer" feature for affiliates in June 2025 that claims to provide legal counsel to increase pressure on victims during negotiations. It also offers "in-house journalists" to assist with writing blog posts for Qilin's data leak site. Our own experience in communications suggests the both tools are very likely simple AI/LLM tools designed to parse and summarize exfiltrated data.



Qilin post on RAMP forum advertising new features

Threat Actor Spotlight: Qilin

Qilin ransomware samples have been observed in the wild, written in both Golang and Rust. They are capable of targeting both Windows and Linux operating systems. Affiliates can configure settings, including file exclusion lists, process and service termination settings, partial or full encryption modes, and encrypted file extensions. In October 2024, cybersecurity company Halcyon reported on an enhanced version of Qilin's ransomware, dubbed "Qilin.B." which supports AES-256-CTR in addition to Chacha20 encryption. It also includes RSA-4096 with OAEP padding to further protect against decryption without purchasing the attacker's private key.

Like most RaaS groups, Qilin affiliate targeting appears to be opportunistic and at the discretion individual affiliates. As such, while the group's observed attacks have heavily impacted victims in the manufacturing, healthcare, technology, and legal industries, there is no indication that this is a result of deliberate targeting by the group. At least some subset of the group's affiliates has been observed exploiting Fortinet vulnerabilities (CVE-2024-21762, CVE-2024-55591) in automated attacks targeting FortiOS/FortiProxy SSL-VPN devices, as well as pre-disclosure vulnerabilities in SAP NetWeaver Visual Composer (CVE-2025-31324).

A logo and graphics from Qilin's data leak site
Source: ransomlook.io

Threat Actor Spotlight: Qilin

Ultimately, Qilin remains among the most prolific ransomware groups but likely enjoys and suffers from the benefits and limitations inherent in any open or semi-open RaaS operation. The group's affiliates range in sophistication and competence. They often employ widely different tactics in their attacks. As we will explore later in this report, Qilin's high operational tempo should not be mistaken for profitability, as a substantial portion of Qilin's victims do not comply with the group's ransom demands. Anecdotally, we can attribute this at least in part to a rigid communications approach and inflexibility in negotiations.

We assess that Qilin's operations will almost certainly continue into 2026, though their efficacy my increase or decrease based a variety of factors. A body of reporting reflecting internal complaints and disagreements suggests there may be opportunities for infighting and reputational risks to the group among ransomware operators, particularly in the event of exit-scams or suspected law enforcement infiltration. Finally, Qilin's high victim count coupled with its open or semi-open affiliate structure strongly increases the likelihood of actual law enforcement infiltration and intelligence collection, making the group a prime target for law enforcement disruption efforts over the next year.

Industry Spotlight: Legal

Industry Spotlight: Legal

While ransomware victim counts continue to increase in general, GRIT has observed a notable surge in law firm and attorneys' offices becoming public victims on ransomware data leak sites. The numbers tell a stark story where legal industry ransomware victims more than doubled YoY from 196 in 2024 to 455 in 2025. This represents a 132% YoY increase. Of the 455 legal sector victims in 2025, 335 (74%) were located in the United States. As one may imagine, legal entities face significant risk in the digital space due to the sensitivity of the data they handle and store.

Ransomware incidents affecting law firms rarely stop at the firm itself. Legal industry victims often preside over a veritable treasure trove of sensitive data, including client PII, client PHI, and sensitive information pertaining to planned or ongoing litigation, or protected under attorney-client privilege.

As a result, when attackers compromise a legal practice and remove data, threats and risks quickly spreads to clients, counterparties, courts, regulators, and insurers. For ransomware actors, access to legal data offers influence over outcomes that matter to multiple parties, not just a singular firm experiencing the intrusion.

Industry Spotlight: Legal

Based on our experience and that of our partners, data exfiltration in legal industry cases is often extensive, supported by record retention rules, and structured data organization in legal environments. This increases the depth and breadth of impacted data in cases of data extortion. It also arguably increases the ransomware actor's coercive leverage.

Anecdotally, organizations in the legal sector may be more likely to carry cybersecurity insurance, a fact which may be exploited by ransomware affiliates to justify high ransom demands and reject counter-offers during negotiations. This risk increases substantially in cases where copies of the insurance policy are maintained on-network, allowing the attacker to reference coverage and deductible details in their demands.

Finally, except for the largest firms, many legal organizations do not maintain robust in-house security capabilities. Instead, they depend on out-sourced support, Managed Detection and Response (MDR) and Managed Security Service Providers (MSSPs) for basic security. While this approach is cost-effective, it often prevents deep understanding of impacted data, the deployment of more advanced security solutions, such as Data Loss Prevention (DLP), and the testing or validation of backup systems. This can result in “scrambling” to understand the full scope and recoverability of a breach during early hours and days of incident response efforts.

Organizations within the legal industry do benefit, however, from robust resources and guidance on preparing for and defending against ransomware. The American Bar Association provides cybersecurity handbooks, guides, and resources, and federal government resources from CISA and the FBI remain viable starting points for developing and validating internal cybersecurity practices.

For legal organizations focused on the threat of ransomware, the greatest variable remains the data to which they are entrusted. Legal organizations should emphasize measures that complicate or prevent data theft, such as network segmentation, least-privilege or zero-trust architectures, and attack surface reduction. Secondarily, emplacement and validation of immutable backup solutions segmented from the main IT network can provide legal organizations with the ability to recover without paying for decryption keys, increasing their business resilience and continuity of operations.

Annual Vulnerability Analysis

Annual Vulnerability Analysis

2025 witnessed a critical evolution in the RaaS landscape, characterized by simultaneous fragmentation of threat groups and highly strategic, large-scale exploitation campaigns led by longstanding established groups such as Qilin, Akira, Clop and PLAY. While key players within the ecosystem fragmented, with a recorded 117 groups observed throughout 2025, the most significant financial and operational damage stemmed from vulnerability exploitation campaigns leveraging zero-day and critical Common Vulnerabilities and Exposures (CVEs) in internet-facing enterprise applications and network perimeter devices.

This analysis is scoped specifically to CVEs disclosed in 2025 or Q4 2024 and exploited as part of Ransomware campaigns throughout 2025.

GRIT has identified the overarching trends of consistent critical business infrastructure, enterprise software suites, and VPN appliance exploitation throughout the year. These trends are exemplified by not only the deployment of complex zero-days for mass data extortion, such as Clop's exploitation of Oracle E-Business Suite (EBS) flaws (CVE-2025-61882 and CVE-2025-61884), but also the consistent high-volume monetization of critical, unpatched Known Exploited Vulnerabilities (KEVs) in VPN infrastructure, such as through Akira's ongoing targeting of SonicWall systems (CVE-2024-40766).

The 2025 Ransomware Ecosystem and Vulnerability Focus

There was significant instability in the structure of 2025's ransomware market. While the traditional RaaS model remained the most prevalent form of ransomware, the ecosystem experienced both structural fragmentation and collaboration between disparate groups during 2025. Fragmentation and disruption of major RaaS brands, including RansomHub, BianLian, and 8Base, drove a proliferation of smaller, more agile actors. This resulted in a record 117 groups monitored by GRIT. Nonetheless, a handful of high-impact groups, specifically Clop, Qilin, Akira, and RansomHub, remained the most prolific key players, filling the vacuum left by earlier disruptions like LockBit and ALPHV/BlackCat from 2024. The reappearance of LockBit and the emergence of ShinyLapsusHunters, however, suggest a potential countertrend in which criminal brands retain their weight.

Ransomware operators consistently attack sectors where operational disruption creates heavy pressure to pay the ransom. GRIT's tracking victims and threat groups highlighted a concentration of activity against Manufacturing organizations, accounting for 22% of all attacks, followed closely by victims in the Technology industry at 14%.

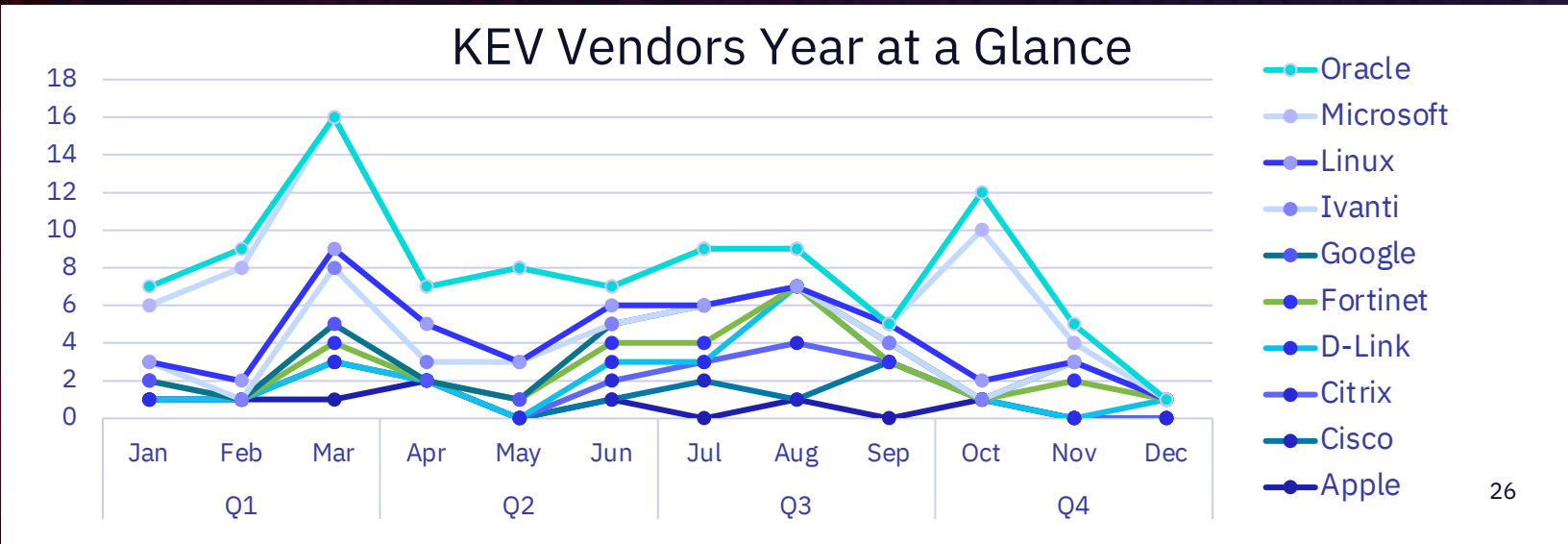
Annual Vulnerability Analysis

Analysis of 2025 Known Exploited Vulnerabilities

Our analysis of the Known Exploited Vulnerabilities (KEV) catalog reveals critical trends in attacker impacts throughout 2025. The first half of the year saw a dramatic increase in exploitation activity. Specifically, Q1 2025 recorded a massive 82.5% YoY increase in the number of new vulnerabilities added to the KEV, and a 32.7% month-over-month (MoM) increase when comparing Q1 2025 to Q4 2024. This surge signals a significantly higher baseline of observed zero-day and n-day exploitation early in 2025. Interestingly, the number of vulnerabilities actively exploited in the second half of 2025 sharpy declined quarter-over-quarter (QoQ), potentially indicating a shift from vulnerabilities in favor of other access vectors in 2H 2025.

Quarter	Vulns Added	2025 vs 2024 Change	QoQ Change
Q1 2024	40	N/A	N/A
Q2 2024	33	N/A	-17.50%
Q3 2024	58	N/A	75.80%
Q4 2024	55	N/A	-5.20%
Q1 2025	73	82.50%	32.70%
Q2 2025	59	78.80%	-19.20%
Q3 2025	51	-12.10%	-13.60%
Q4 2025	48	-12.70%	-5.90%

KEV vulnerabilities disproportionately impacted Microsoft products in 2025. Their share of new KEVs doubled from 7 occurrences in Q1 2024 to 16 occurrences in Q1 2025. This concentrated targeting underpins the prevalence of Windows-based exploitations observed in groups like PLAY (CVE-2025-29824) and compared to overall market share being predominantly Microsoft around the world. Furthermore, attackers demonstrated a clear shift toward infrastructure-based vulnerabilities, with Fortinet and Cisco maintaining top 5 most-targeted vendors in 2025, replacing earlier targets like Google from last year.



Annual Vulnerability Analysis

Analysis of 2025 Known Exploited Vulnerabilities

Despite this surge in volume, the number of KEV entries used specifically by ransomware groups saw a reported decline throughout 2025. It dropped YoY from 42.5% of new KEV entries in Q1 2024 to just 13.7% of new KEV entries in Q1 2025. While this data reflects a reduction in novel vulnerabilities employed by ransomware actors, we note a typical delay from vulnerability publication to exploitation “in the wild” with many sub-critical vulnerabilities. High-severity but historical vulnerabilities continue to be widely leveraged by Initial Access Brokers (IABs) and RaaS affiliates. We see a large attribution of KEVs related to ransomware campaigns typically in the first and last quarters of each year. This is supported by the relatively stable numbers in Q2 and Q3 in both 2024 and 2025 compared with Q1 and Q4 numbers of the same year. This does not indicate a lull in exploitation, but rather a general trend of delay between vulnerability identification and exploitation.

Quarter	Known Ransomware KEVs	YoY Change	QoQ Change
Q1 2024	17	N/A	N/A
Q2 2024	7	N/A	-58.80%
Q3 2024	5	N/A	-28.60%
Q4 2024	9	N/A	80%
Q1 2025	10	-41.20%	11.10%
Q2 2025	5	-28.60%	-50%
Q3 2025	5	0.00%	0%
Q4 2025	2	-77.80%	-60%

Annual Vulnerability Analysis: Qilin Case Studies

Qilin, a RaaS group, has cemented its position as one of the most prolific and impactful ransomware threat groups of 2025. Known for operating a double-extortion model, the group and its affiliates not only encrypt data but also exfiltrate and threaten to leak sensitive information, significantly increasing the pressure on victims.

The groups known victims reflect an outsized impact against organizations where downtime and data exposure carry severe consequences. The group distinguished itself in 2025 by demonstrating early access to, and systematic exploitation of several high-severity vulnerabilities. In doing so, Qilin's affiliates have showcased a level of capability and sophistication that GRIT associates with highly experienced and established threat groups.

- Security researchers have observed Qilin regularly leveraging multiple vulnerabilities in their pursuit of initial access to victim infrastructure. CVE-2025-31324 is a critical (CVSS 9.8) Unrestricted File Upload vulnerability in the SAP NetWeaver Visual Composer Metadata Uploader. This vulnerability allowed Qilin to achieve unauthenticated Remote Code Execution (RCE). Various sources have reportedly observed Qilin exploiting this vulnerability as early as March 2025, at least three weeks before its public disclosure and official patching in April 2025, confirming its use as a "zero-day" exploit. Successful exploitation of the vulnerability ultimately allows attackers to upload malicious files, such as JSP-based webshells, to victim environments in order maintain persistent access.
    - Additionally, Qilin was observed exploiting CVE-2025-32756, a stack-based buffer overflow flaw (CVSS 9.8) in multiple Fortinet products (including FortiVoice, FortiMail, and FortiNDR) that allows a remote unauthenticated attacker to execute arbitrary code. This vulnerability was added to the CISA KEV catalog in May 2025, while Qilin was observed leveraging this RCE to deploy ransomware.
    - Researchers also observed Qilin's use in 2025 of several FortiGate vulnerabilities initially disclosed in 2024. These vulnerabilities included CVE-2024-21762, (CVSS 9.8) an out-of-bounds write vulnerability impacting Fortinet FortiOS and FortiProxy that allows an attacker to execute unauthorized code or commands; and CVE-2024-55591, (CVSS 9.8), an authentication bypass vulnerability also affecting FortiOS and FortiProxy which allows a remote attacker to gain "super-admin" privileges. These vulnerabilities were patched in 2024 and early 2025, respectively, and were used to gain initial access in a mid-summer 2025 campaign. At the time of exploitation, Bleeping Computer reported that the ShadowServer Foundation had identified over 150,000 devices still vulnerable to CVE-2024-21762 attacks.

Annual Vulnerability Analysis: Akira Case Study

Akira, a similarly prolific RaaS group, maintained a persistent focus throughout 2025 on vulnerabilities and weak security controls impacting remote access solutions to establish initial access. GRIT previously reported on Akira's active targeting of SonicWall VPN products, emphasizing the group's focus on perimeter network infrastructure as an initial access vector.

Specifically, Akira affiliates frequently leveraged CVE-2024-40766 (CVSS 9.8), an Improper Access Control vulnerability in SonicWall SonicOS. This vulnerability was added to the CISA KEV catalog in September 2024 due to active exploitation, though Akira's subsequent exploitation began in July 2025 and continued through at least November 2025. As previously referenced, RaaS groups, including Akira, will continue to exploit historical vulnerabilities so long as they remain effective against a body of vulnerable systems.

The group's initial access strategy is often multi-faceted, employing traditional credential-based methods, such as brute-forcing VPN endpoints and employing password spraying techniques, to precede or follow vulnerability exploitation.

Furthermore, security researchers later noted that even in cases where impacted SonicWall devices had been patched, Akira could still target the Virtual Office Portal. It reused previously stolen credentials and exploiting system misconfigurations to potentially bypass multi-factor authentication (MFA). This again reflects the use of a vulnerability as a singular component of a comprehensive initial access strategy.

The continued weaponization of vulnerabilities like CVE-2024-40766 provides Akira with a "force multiplier," offering a highly reliable, documented path for unauthorized access into unpatched networks when credential theft alone fails or is insufficient. These reliable methods of obtaining access enable the rapid execution of an affiliate's post-exploitation playbook, a characteristic of successful RaaS operations that prioritize speed and efficiency over complexity.

Annual Vulnerability Analysis: Clop Case Studies

The Clop (sometimes stylized as “Cl0p”) data extortion group launched a significant large-scale extortion campaign beginning in September 2025 targeting Oracle E-Business Suite (EBS) customers. Analysis by Google Threat Intelligence Group (GTIG) and Mandiant indicated that the underlying intrusions had begun as early as August 2025. This campaign continued Clop’s established track record of mass exploitation directed at vulnerable enterprise software, often with “zero-day” exploits. Previous Clop campaigns included mass exploitation of the MOVEit and GoAnywhere managed file transfer applications, both in 2023, and Cleo’s MFT in 2024.

The operation specifically leveraged two zero-day vulnerabilities in EBS to exfiltrate data to adversary infrastructure, which Clop subsequently used to pressure victims into paying ransoms to avoid data publication. Clop currently claims over 100 organizations as impacted by its EBS campaign, and it has published data from more than 70 victims on its Data Leak Site so far.

This two “zero-day” vulnerabilities exploited as part of Clop’s EBS campaign both enabled unauthenticated access to core components:

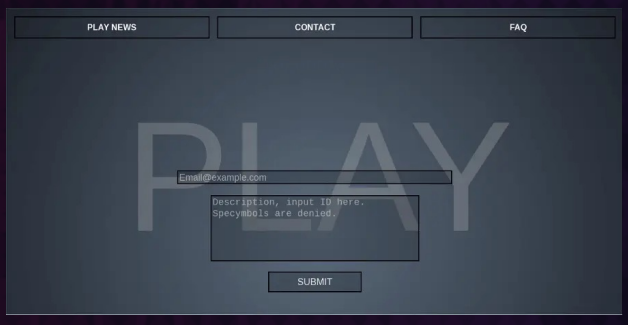
- The first vulnerability, tracked as CVE-2025-61882 (CVSS 9.8), provided Clop with the ability to execute remote code over HTTP without requiring valid login credentials. This successful RCE path granted immediate control over compromised systems. Security researchers confirmed that the exploit chain demonstrated a high degree of technical skill, reportedly involving up to five separate bugs, some of which were patched in Oracle’s July 2025 Critical Patch Update.
- The second vulnerability, tracked as CVE-2025-61884 (CVSS 7.5) allowed remote attackers to access sensitive configuration data and trigger internal requests without requiring credentials.

Annual Vulnerability Analysis: PLAY Case Studies

The PLAY ransomware group was linked to the exploitation of a 2025 zero-day vulnerability tracked as CVE-2025-29824 (CVSS 7.8), a Use-After-Free flaw in the Microsoft Windows Common Log File System (CLFS) Driver. Disclosed and patched in April 2025, this vulnerability is classified as an escalation of privilege flaw. Successful exploitation allows an authorized attacker to gain elevated privileges locally on affected Windows systems, including various versions of Windows 10 and 11.

According to Microsoft, threat actors tracked as Storm-2460, and widely believed to be affiliates of the PLAY ransomware group, were observed leveraging this CLFS zero-day. In the attack chain, the exploitation followed the deployment of a malware identified as PipeMagic. Unlike the perimeter flaws used by Clop and Akira, this vulnerability is not an initial access vector but rather a key privilege escalation vulnerability. This enabled the ransomware group to move from user-level access to the SYSTEM-level access to enable widespread encryption and system control.

Additionally, according to a CISA advisory update for PLAY in June 2025, the group was also observed exploiting a vulnerability tracked as CVE-2024-57727 (CVSS 7.5) in the remote monitoring and management (RMM) tool SimpleHelp following the vulnerability's disclosure on 16 January 2025. This vulnerability stems from a path traversal flaw in the SimpleHelp web application, which allows improperly sanitized user input. By sending specially crafted requests, an attacker can navigate the file system and gain access to sensitive files. Attackers can exploit this flaw to access files like /etc/passwd or SSH private keys, ultimately allowing for further exploitation of compromised systems via privilege escalation or remote login using compromised credentials.



Annual Vulnerability Analysis

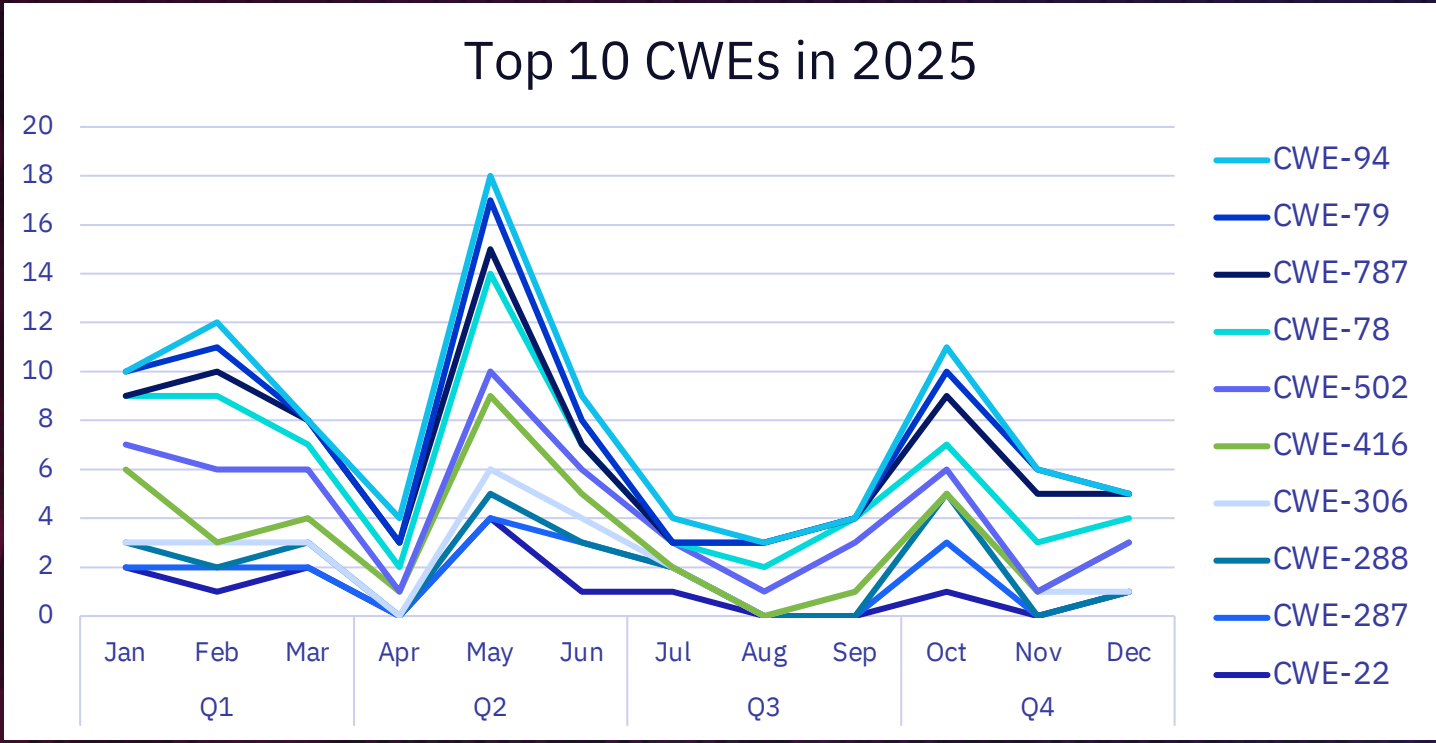
Attributed Ransomware Campaigns Exploiting 2025 / Late 2024 CVEs

Campaign	Group	CVE ID	Type and CVSS	Product	Reported Exploitation Window
NetWeaver Campaign	Qilin	CVE-2025-31324	RCE – 9.8	SAP Netweaver	H1 2025
Fortinet Campaign	Qilin	CVE-2025-32756 CVE-2024-21762	RCE – 9.8 RCE – 9.8	Fortinet FortiOS	Mid-2025
SonicWall SSL VPN	Akira	CVE-2024-40766	EoP – 9.8	SonicWall SonicOS	2025-Ongoing
Oracle EBS	Clop	CVE-2025-61882 CVE-2025-61884	RCE – 9.8 EoP – 7.5	Oracle EBS	Q4 2025
Windows CLFS	PLAY	CVE-2025-29824 CVE-2024-57727	EoP – 7.8 AuthBypass – 7.5	Windows CLFS SimpleHelp RMM	H1 2025

How Exploits Enable RaaS Playbooks

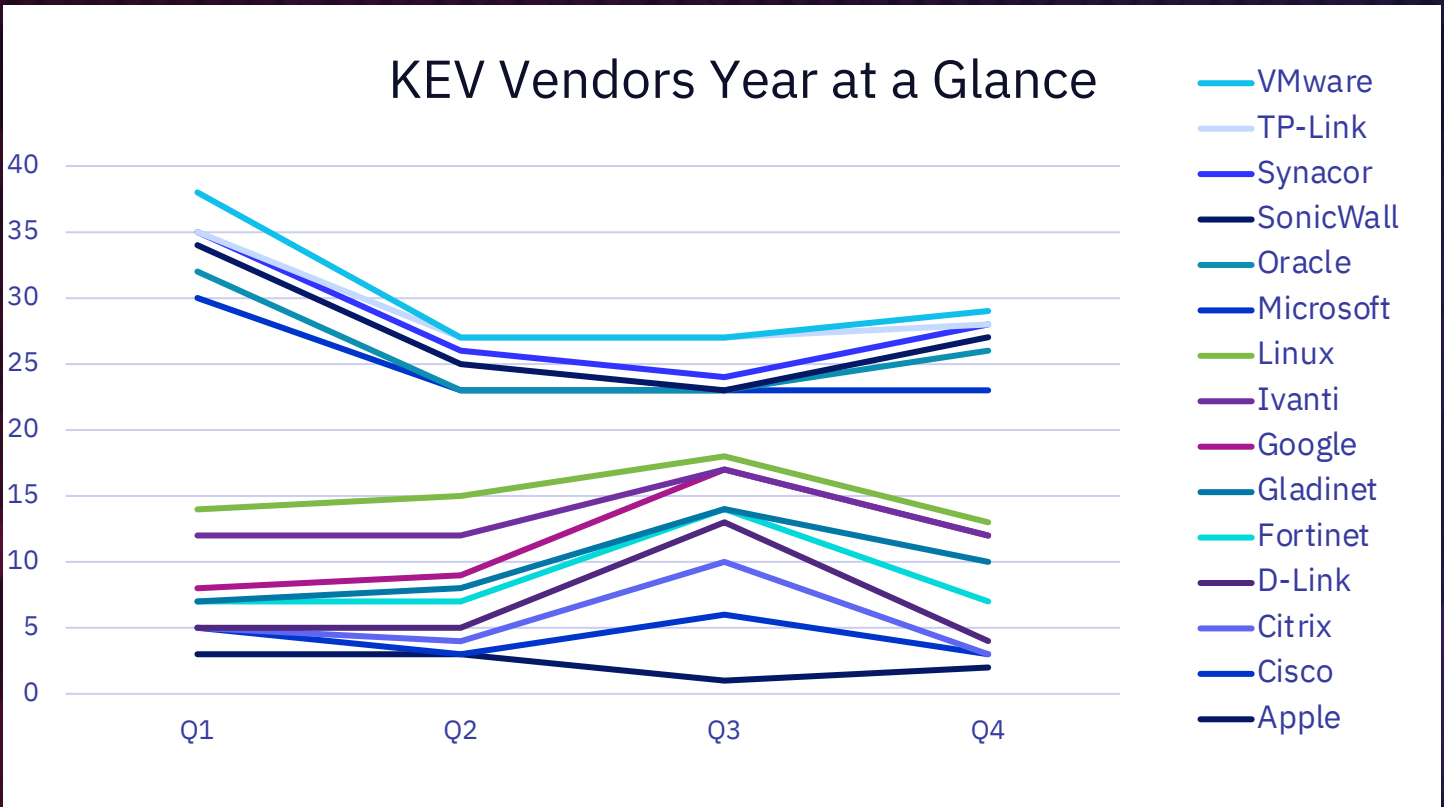
Analysis of 2025 ransomware activity reveals a correlation, in many cases, between the type of vulnerability exploited and the subsequent TTPs employed by the threat actor. Furthermore, analysis of the KEV catalog indicates that attackers exploited two core Common Weakness Enumeration (CWE) categories throughout the year more than any other weaknesses: CWE-502 (Insecure Deserialization) and CWE-78 (OS Command Injection).

Annual Vulnerability Analysis



The CWEs observed as associated with 2025's exploitation campaigns indicate a reliance on exploitation of complex RCE flaws in enterprise software (like Clop's Oracle EBS zero-day, CVE-2025-61882 and CVE-2025-61884). This also aligns with the rise of Insecure Deserialization (CWE-502) as the second most exploited underlying weakness for known exploited vulnerability types throughout 2025. These logic flaws can grant immediate network access, ultimately allowing the threat actor to focus on rapid data exfiltration. Conversely, groups exploiting common perimeter flaws (such as Akira's use of CVE-2024-40766) continue to rely heavily on OS Command Injection (CWE-78), which was consistently the most commonly exploited flaw category across all quarters. Successful command injection often precedes the execution of standardized post-exploitation playbooks, which consistently feature heavy use of legitimate tools (Living-off-the-Land) for command and control, lateral movement, and defense evasion to navigate network structure.

Annual Vulnerability Analysis



Furthermore, the prevalence of attacks on Microsoft continues the YoY pattern of exploiting core Windows components (e.g., CVE-2025-29824 for Privilege Escalation), likely due to its widespread implementation throughout enterprises worldwide. VMware emerging in the top 5 vendor targets during Q1 confirms the strategic shift toward exploiting core Windows components (e.g., CVE-2025-29824 for Privilege Escalation) and data center virtualization infrastructure (ESXi targeting by Akira).

The ongoing CVE exploitations that added to the KEV catalog in late 2024 (e.g., CVE-2024-40766) and early 2024 (e.g., CVE-2024-1709) continued throughout 2025. This demonstrates that vulnerabilities do not lose their value to RaaS groups once vendor patches are released. A good example is Akira's continued SonicWall SSL VPN campaign success. These flaws provide a reliable, documented means of compromise for criminal enterprises monetizing the organizational "patch-gap."

Meanwhile, the initial exploitation of high and critical-severity 2025 zero-days (such as CVE-2025-29824 in Windows CLFS) often precedes its rapid commoditization and subsequent sale within the RaaS initial access broker ecosystem. The window between initial exploitation and RaaS adoption is seemingly shrinking, compelling defenders to treat all critical zero-days as potential avenues to ransomware threats, irrespective of initial threat attribution. This urgency is reinforced by the massive 82.5% spike in KEV volume observed in Q1 2025.

Other Reporting and Events

Innovation in Ransomware

The ransomware threat landscape underwent significant evolution in 2025, marked by the democratization of advanced techniques and the operationalization of artificial intelligence. Two trends stand out: the widespread adoption of Bring Your Own Vulnerable Driver (BYOVD) attacks — formerly primarily observed in nation-state level tactics — and the measured integration of AI into attack chains. While threat actors have begun deploying AI for victim negotiations and data analysis, the industry has not yet witnessed fully autonomous, AI-coded malware at scale in the wild. This segment examines these innovations from the threat actor perspective, analyzing how ransomware operators are evolving their tradecraft to maximize impact and evade detection.

1. BYOVD: From Advanced Persistent Threat Use to Affiliate Commodity Tactic

BYOVD techniques have proliferated in ransomware operations following Akira ransomware's pioneering deployments in early 2024. In those operations, Akira operators leveraged legitimate, vendor-signed drivers including the Zemana AntiMalware driver (*zamguard64.sys*) and Intel's ThrottleStop CPU tuning driver (*rwdrv.sys*) to disable endpoint detection and response (EDR) solutions at the kernel level. This technique grants threat actors kernel-level privileges to execute code, enabling them to terminate security processes before deploying ransomware payloads.

Investigations by CISA and the FBI found that Akira's success with BYOVD sparked rapid adoption across the ransomware ecosystem. By mid-2024, multiple major groups such as Qilin (CVE-2024-1853) and RansomHub had integrated similar capabilities.

The most notable BYOVD attacks in 2025 came again from Akira during a series of operations observed exploiting a zero-day vulnerability in SonicWall VPNs. In these operations, GRIT observed malicious use of two drivers, *rwdrv.sys* and *hlpdrv.sys*, used to facilitate AD/EDR evasion.

Innovation in Ransomware

By late 2024, BYOVD had evolved from advanced technique to commodity tool. The packaging of these capabilities into user-friendly toolkits like PowerTool and "Killer Ultra" transformed what once required deep Windows internals expertise into a point-and-click capability for mid-tier ransomware affiliates. This technique's proliferation has made it easy to access, require less technical skill, and low cost; fundamentally lowering the barrier to entry for BYOVD attacks.

What distinguishes 2025's BYOVD landscape from earlier attacks is how the techniques are packaged and commoditized. Tools like PowerTool and pre-made malware such as "Killer Ultra" have transformed BYOVD from a technique requiring deep Windows internals expertise into a capability accessible to mid-tier ransomware affiliates.

The LOLDrivers project has catalogued around 500 legitimate drivers available for attackers to exploit. This extensive catalog exists because of a fundamental Windows security constraint: while Microsoft has tightened requirements for new drivers, mandating extended validation (EV) certificate signing and Hardware Lab Kit (HLK) compatibility testing, these enhanced security measures do not apply retroactively. As a result, legacy drivers that were legitimately signed years ago can still load into kernel space based on historical signatures without undergoing current security scrutiny. This creates a persistent attack surface of hundreds of trusted-but-vulnerable drivers that attackers weaponize in BYOVD attacks.

Implications for 2026

In 2024 and 2025, GRIT observed the BYOVD attack chain through operations from major threat groups such as Akira, RansomHub, and Qilin. In 2026, as this attack chain is used more frequently by major groups, GRIT anticipates it will become more visible and "popularly" used by more threat actors.

The BYOVD trend challenges endpoint security architectures by exploiting the fact that legacy Windows driver signatures remain authenticatable even after updated versions are released. As defenders continue to improve security measures through enhanced driver signing requirements, creating malicious Windows kernel drivers becomes increasingly difficult. However, this security improvement paradoxically makes legacy vulnerable drivers more valuable to attackers. Expect continued exploitation of the extensive catalog of vendor-signed, vulnerable drivers, with threat actors potentially developing automated tools to identify and weaponize newly discovered driver vulnerabilities.

Innovation in Ransomware

2. AI in Ransomware Operations

AI-Use in Operations

Contrary to popular predictions, artificial intelligence deployment remained tactical rather than transformative in 2025 ransomware operations. GRIT finds that Threat Actors (TAs) primarily use AI to augment previously existing capabilities:

Negotiations and Communication: LockBit and other ransomware-as-a-service operations have deployed AI-powered chatbots to conduct victim negotiations. These systems employ formulaic approaches to preset demands, personalize communications based on victim responses, and maintain consistent pressure without emotional variance. Qilin ransomware emerged as a notable adopter, offering "AI-assisted negotiations" and legal assistance services to review stolen data for regulatory violations.

Social Engineering: AI-generated content enables attackers to overcome language barriers, personalize messages at scale, and craft contextually appropriate lures that bypass traditional detection.

Data Analysis and Targeting: Ransomware operators use AI to analyze exfiltrated data, identifying high-value information (financial records, intellectual property, regulated data) and determining appropriate ransom demands based on victim revenue and data sensitivity.

Agentic AI Remains to be Seen

Despite vendor warnings that 76% of organizations struggle to match the speed of AI-powered attacks, the industry has not observed:

Fully autonomous AI malware capable of independent decision-making across the entire attack lifecycle

AI-coded malware used at scale in the wild, although Anthropic reported that its researchers disrupted a sophisticated cybercriminal who weaponized Claude Code (an agentic AI tool) to conduct large-scale data theft and extortion targeting at least 17 organizations across healthcare, emergency services, and government sectors.

Self-evolving attack chains that adapt in real-time to defensive measures

The gap between current capabilities and predicted threats reflects technical limitations, ethical AI safeguards that are being bypassed only by determined actors, and the reality that traditional techniques remain highly effective.

Innovation in Ransomware

2026 Outlook

The Anthropic case study suggests we are approaching an inflection point where:

- **Agentic AI capabilities** become accessible enough for broader threat actor adoption
  AI-driven reconnaissance compresses attack timelines from hours to minutes
  Adaptive malware uses machine learning to evade behavioral detection in real-time

However, vendors predict that initial deployments will focus on augmenting human operators rather than replacing them, with fully autonomous AI-driven ransomware campaigns remaining an emerging rather than widespread threat through 2026.

Conclusion

The ransomware landscape of 2025 demonstrates that threat actors are becoming more efficient, professional, and business-like. They are adopting enterprise techniques including automation, AI integration, and franchise-style operations. The democratization of advanced capabilities — exemplified by BYOVD's spread from nation-state toolkits to commodity ransomware — combined with compressed attack timelines and intensified extortion tactics, creates a perfect storm for defenders.

The year 2026 will likely see continued convergence of criminal innovation and AI capabilities, demanding that defenders adopt equally sophisticated technologies and intelligence-led approaches. The organizations best positioned to withstand this evolution will be those that prioritize rapid detection and response, implement comprehensive identity and access controls, and integrate AI-powered defenses as essential components of their security architecture rather than experimental additions.

2025 Law Enforcement Operations

In 2025, international law enforcement continued to challenge ransomware-facilitating criminal operations with coordinated takedowns, arrests, and infrastructure seizures. These actions reflect a broader shift from singular arrests to sustained, ecosystem-level disruption, where authorities are not only chasing individual threat actors, but targeting the services, tooling, and infrastructure that enable ransomware deployment and monetization.

Between January and April 2025, authorities from 26 countries identified and dismantled over 20,000 malicious IPs and domains tied to 69 infostealer variants as a part of Operation Secure. In addition to these infrastructure seizures, Interpol also announced the arrest of 32 suspects accused of helping operate these critical pieces of malware. In the past two years, info stealing malware has become a significant upstream component of the ransomware ecosystem. They provide a steady stream of valid credentials to systems around the world, credentials which are often repackaged and sold to ransomware actors seeking initial access to their targets' networks. By collapsing large segments of the infostealer market, Operation Secure temporarily cut into a reliable revenue stream for ransomware actors who were forced to become more creative when gaining a foothold on victim networks while the market rebuilt itself.

2025 Law Enforcement Operations

Later, in May of 2025, United States and European authorities announced a coordinated action against LummaC2, historically one of the most pervasive infostealer services. The US Department of Justice and the FBI seized multiple domains used as command-and-control panels for the malware, enabling them to issue commands essentially wiping out all active infections. In addition, as a part of the seizures, law enforcement was able to capture a significant portion of the credentials stolen by the LummaC2 service. This enabled law enforcement and their private industry partners to proactively notify organizations whose corporate credentials were compromised by the malware. This undoubtably disrupted several attacks in progress and prevented future abuse of the stolen credentials, essentially making them worthless on the otherwise booming credential resale market. Disrupting LummaC2 temporarily elevated the barrier for entry for lower tier ransomware actors who relied on the firehose of stolen credentials for initial access.

Between January and April 2025, authorities from 26 countries identified and dismantled over 20,000 malicious IPs and domains tied to 69 infostealer variants as a part of Operation Secure. In addition to these infrastructure seizures, Interpol also announced the arrest of 32 suspects accused of helping operate these critical pieces of malware. In the past two years, info stealing malware has become a significant upstream component of the ransomware ecosystem. They provide a steady stream of valid credentials to systems around the world, credentials which are often repackaged and sold to ransomware actors seeking initial access to their targets' networks. By collapsing large segments of the infostealer market, Operation Secure temporarily cut into a reliable revenue stream for ransomware actors who were forced to become more creative when gaining a foothold on victim networks while the market rebuilt itself.

2025 Law Enforcement Operations

In November, the Operation Endgame monicker was once again invoked to announce one of the largest coordinated seizures of malware infrastructure to date. In all, more than 1025 servers responsible for facilitating the infection and spread of various infostealers, remote access trojans, and botnets were seized by law enforcement. Rhadamanthys, one of the largest operating infostealers, which gained popularity in the wake of the Lumma disruption, was fully disabled for a period of time, although the underlying actor appears to have partially rebuilt their infrastructure in the months following. The Elysium botnet, a malicious proxy service offered by the developers of Rhadmanthys, was also maimed by these law enforcement actions.

In parallel, the remote access trojan VenomRAT had its core infrastructure disabled as law enforcement arrested one individual in Greece suspected of developing and operating the malware. In its announcement of the activities in November, Europol was keen to note that Operation Endgame is not over. The successive attacks against the ransomware supply chain inflict significant harm and costs to the underlying operators. Even if law enforcement cannot arrest every single individual responsible for every portion of a ransomware attack, they can force them to rebuild their code and infrastructure which takes time and money. The more time cybercriminals spend hiding from law enforcement and retooling their operations, the less time they spend inflicting harm on their victims.

2025 Law Enforcement Operations

Finally, not all law enforcement action in 2025 was focused on disrupting the ransomware supply chain. In addition to making their lives harder, authorities also proved that they still have the ability to hunt down and arrest actual ransomware operators should the opportunity present itself. In 2025, at least two individuals reportedly involved with Scattered Spider were arrested, one in the United Kingdom and one in the United States. The individuals were charged for their links to some of the most impactful and expensive breaches over the last few years of the group's operations. Specifically, they were tied to the extortion of multiple UK based retailers and US based casino operators, which both led to hundreds of millions of dollars in damages. The individuals, both teenagers at the time of their arrest, allegedly received over $100 million in extortion payments as a result of their activities. Their arrests hopefully give pause to any other individuals associated with the Scattered Spider group.

Cybercriminals often become overly confident and begin to behave with impunity when they think they can never be caught. Although not every ransomware operator can be tracked and brought to justice, making headlines with the arrests of individuals in the same space can strike fear, uncertainty, and doubt into the minds of their coconspirators. In addition, arresting individuals involved in cybercriminal collectives, such as Scattered Spider, presents a unique opportunity to gather intelligence on the group's operations and other members. Suspects can be compelled to cooperate with law enforcement by providing information on other individuals in the group in exchange for more lenient sentencing. Ideally, the arrests of these two individuals are not some isolated incidents, but rather the first domino to fall in the eventual dissolution of the Scattered Spider collective.

Ransomware Payment Rate Case Studies: Akira and Qilin

For four years, this report has analyzed changes in the ransomware and cybercrime landscape principally through the lens of observed victims: how many organizations are posted, by which overarching groups, in what industries, etc. This approach, while insightful, risks exposing us to only one portion of ransomware's victims – the ones that did not pay the ransom. Over the past year, we've worked to address this by expanding our intelligence collection and integrating new intelligence sources that review ransomware negotiation outcomes. This is enabled through a new partnership with TRM labs. In the process, we've been able to expand the aperture and tell the other side of this story.

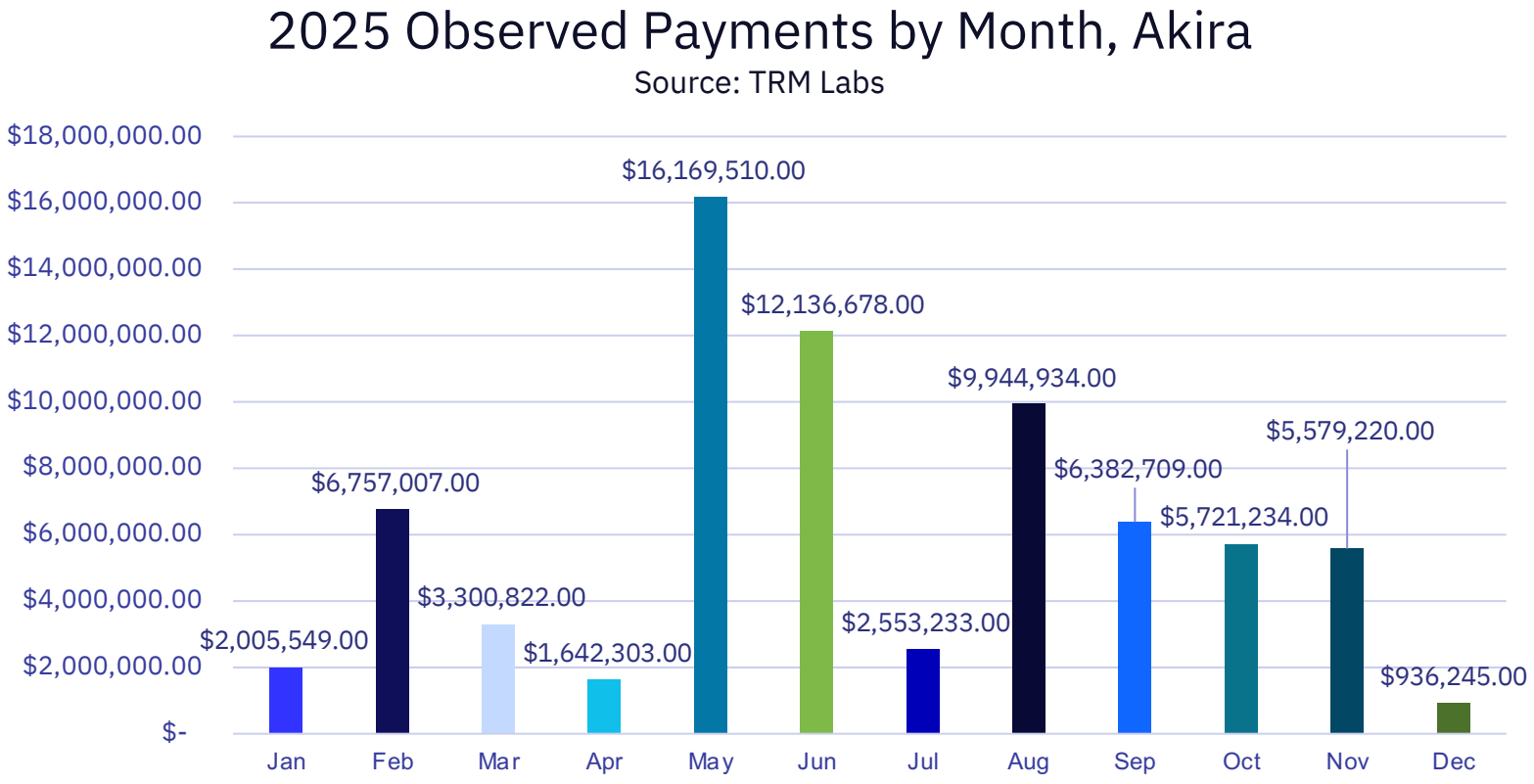
In 2024 and 2025, we have observed multiple reports detailing a decrease in ransomware payments, with alleged payment rates of between 25% and 50%. Coveware, in particular, continues a series of quarterly reports covering this topic, which we have found invaluable in comparing to our direct experience. In their most recent Q3 2025 report, for example, Coveware cites ransom payment rates "plummeting" to a "historic low of 23%," reflecting less than 1 in 4 ransomware victims opting to pay the attackers demands. This is certainly good news – fewer ransom payments means less revenue for cybercriminals. We would in turn expect to disincentivize the expansion of ransomware operations we've noted year over year. But we have struggled to reconcile this apparent drop off in payment rates with the continued ubiquity of ransomware.

Ransomware Payment Rate Case Studies: Akira and Qilin

While reviewing our own internal data and tagged cryptocurrency wallets from TRM labs, we did not find that reviewing the payment outcomes of every group would be plausible or helpful for this format, so we instead opted to dive deeper into two of the most prolific ransomware groups of 2025: Akira and Qilin. Both groups have claimed thousands of victims this year – Akira claimed 722 and Qilin claimed 1,044 – and as such, we would expect to observe several hundred cases of payment. To some extent, this held true.

Akira Payment Rates

In the case of Akira, we observed 653 posted victims, who presumably did not pay Akira's demands. On the blockchain, we observed at least 160 transactions which we assessed to reflect ransomware payments, resulting in a payment rate of at least 24.5%. The amount of these transactions varied substantially, from lows of approximately $50,000 USD equivalent, to a high of $7MM. Across the year, cryptocurrency wallets associated with Akira and its affiliates received at least $73MM, with an average ransom payment of approximately $457,000.

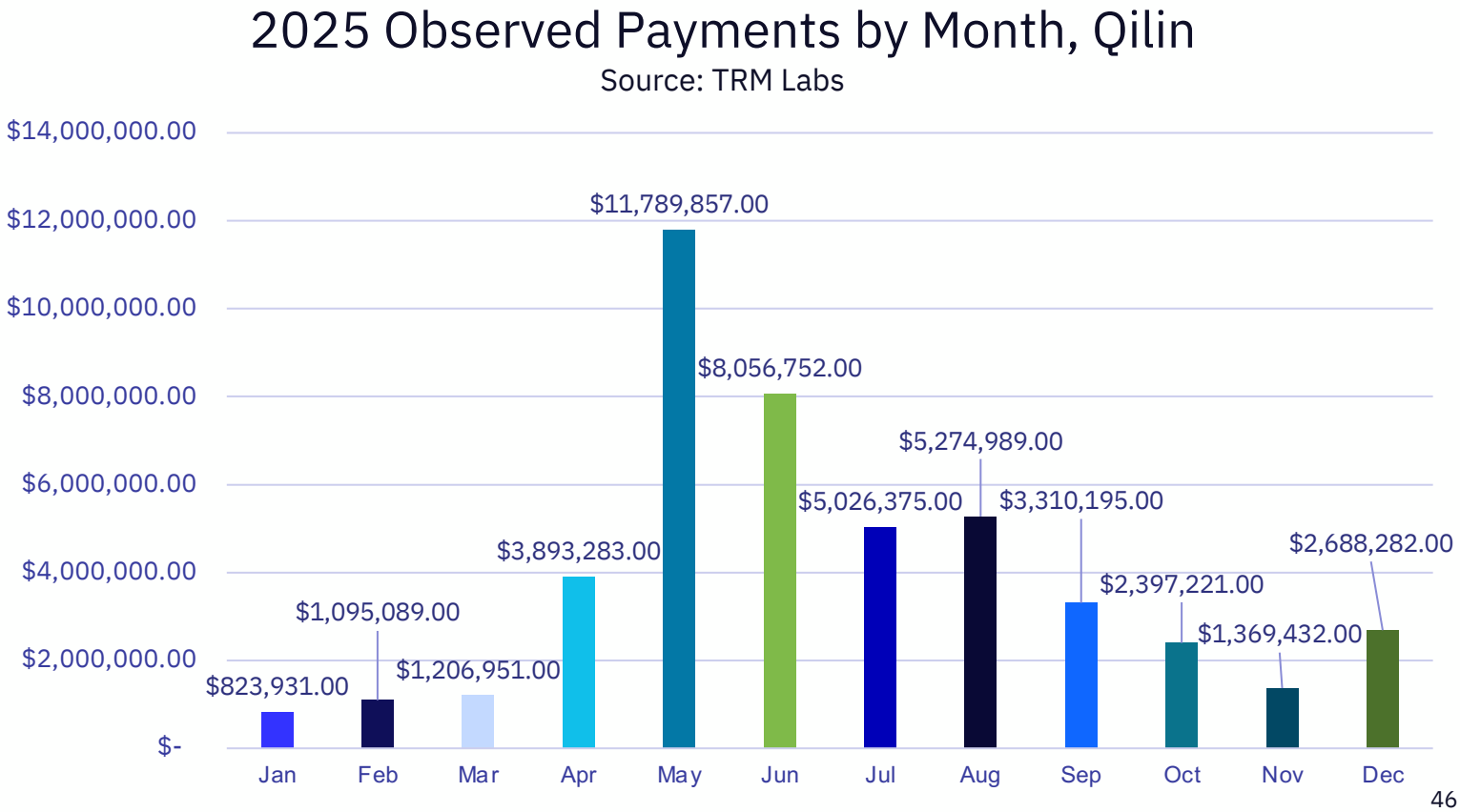


Ransomware Payment Rate Case Studies: Akira and Qilin

For the sake of comparison, we turned to our internal payment outcomes tracking. We'll begin by acknowledging the risk of selection bias in these numbers, as most victims seeking out Threat Actor Communications, or ransomware negotiations, will likely at least be considering some level of payment, and may be more capable of doing so relative to those who do not. These biases aside, we observed approximately 53% of Akira victims opting not to make a ransom payment.

Qilin Payment Rates

Qilin's figures differed slightly. Across 2025, we observed 869 posted victims who likely did not pay Qilin's demands. On the blockchain, we observed at least 128 payments which we assessed to reflect ransomware payments, resulting in a payment rate of at least 14.79%. The amount of these transactions varied along similar lines, with lows of approximately $50,000 USD equivalent, to a high of nearly $4MM. Throughout the year, cryptocurrency wallets associated with Qilin and its affiliates received at least $47MM, with an average ransom payment of approximately $366,000. Among our internal data, we observed much higher demands and much lower rates of payment from Qilin victims, with 2 out of every 3 victims opting not to pay.



Ransomware Payment Rate Case Studies: Key Takeaways

- Our payment rate observations in 2025 across Qilin and Akira victims are substantially consistent with other reporting, including Coveware's, which reflects reduced frequency of payments. The ransom payment amounts we observed were similarly consistent. While both Akira and Qilin received outlier payments in the millions, these accounted for less than 10% of observed payments. The average ransom payment across both groups was between $366,000 and $457,000.
- When accounting for rates of non-payment, we observe at least 813 victims from Akira, and at least 997 victims from Qilin in 2025. Based on average payments and rates of non-payment, the ROI per attack drops to $90,000 or less for Akira, and $47,000 or less per attack for Qilin. These amounts subsequently need to be dispersed, typically on an 80/20 split, between the affiliate and the core group since affiliates may owe a "cut" of their payment to Initial Access Brokers. The core group, similarly, may owe a "cut" of their payment to support staff.
- The results of Threat Actor Communications / Ransomware negotiation can be substantive for reducing the amount paid to a threat actor. While the efficacy of negotiations is almost certainly a product of the victim's negotiator, the threat actor's negotiator, the size of the victim, and the initial demand, we consistently observed reductions ranging from 44 to 80 percent, potentially reducing the final amount paid to threat actors by millions across the year.
- Both Akira and Qilin appear to have a relatively hard "floor" of $50,000 in their ransom demands, with only a handful of observed payments falling below this level. Anecdotally, we have observed, in claim and in practice, a "floor" of $100,000 from both groups. We assess that the group's affiliates generally consider amounts below "six figures" to be unacceptable, except in outlier cases of smaller victim organizations and incomplete extortion, such as failed data exfiltration or encryption efforts.

2025 Signpost Analysis

Signposts Analysis: 2026 Outlook

In reviewing 2025's ransomware trends, GRIT analyzed and considered potential signposts or indicators contributing to increases or decreases in ransomware operations, their efficacy, or their profitability. These indicators are based on a combination of open-source reporting, GuidePoint Incident Response observations, and GRIT internal analysis over the preceding year. The goal of providing these "signposts" is to provide near and mid-term forecasting for analysts, defenders, and security executives – in other words, to give a glimpse ahead.

For the sake of readability, we have opted to break these signposts down into three categories:

- **Tactics, Techniques, and Procedures (TTP):** Signpost indicators pertaining to the methods employed by ransomware threat actors to achieve desired ends during an intrusion.
- **Ecosystem and Organization:** Signpost indicators pertaining to the overall ransomware landscape, including group structure, organizational behavior, and extortion mechanisms.
- **Disruption and Instability:** Signpost indicators pertaining to law enforcement, policy, and destabilizing internal factors which could jeopardize or complicate ransomware's efficacy.

For each signpost, the following standards are applied :

Projected Impact on Ransomware	Discourages, complicates, or reduces ransomware operations or payments	Has no or negligible impact on ransomware operations or payments	Encourages, enables, or facilitates ransomware operations or payments
			

Tactics, Techniques, and Procedures

	Projected Impact
Threat Actors increasingly use AI/LLMs by default While the earliest instances of AI/LLM usage by ransomware threat actors (TA) skewed towards social engineering and translation, we've increasingly observed their use to overcome roadblocks and rudimentary scripting efforts. More widespread adoption of AI/LLM in TA workflows will likely further reduce technical barrier to entry for less experienced operators. Truly novel or more sophisticated implementation of AI/LLMs is expected to be less likely but would have more substantial downstream impacts.	
Perimeter device exploitation campaigns increase 2025 features several campaigns targeting vulnerabilities in VPNs, firewalls, and other edge devices as a reliable means of obtaining a foothold. In particular, Akira's exploitation of SonicWall SSLVPN contributed directly to root cause in a substantial portion of its victims over the course of H2 2025. As these devices are commonly exposed to the internet and as TAs become more familiar with exploitation, we will very likely observe exploitation of new vulnerabilities in perimeter devices as part of ransomware attack chains, either as "zero-day" or "n-day" exploits.	
Novel malware and custom tooling continue to decrease in prevalence; RMMs and LotL persist Offensive Security Tools (OSTs) such as Cobalt Strike and Sliver have become less ubiquitous and were not observed in the majority of GuidePoint IR cases involving ransomware in 2025. The same holds true of novel or customized tooling and malware. In their place, we continue to see abuse of legitimate Remote Monitoring and Management (RMM) tools and Living off the Land (LotL) techniques in the majority of ransomware intrusions, which are frequently not detected on or dismissed as false positives by victims. We expect this trend to continue based on familiarity, low costs, and effectiveness against corporate environments.	
Social Engineering tactics increase in frequency, targeting The proliferation of ClickFix, FileFix, and Shai-Hulud in 2025 emphasized the success rates of social engineering techniques and trust relationships in overcoming technical controls via human exploitation. The success of these tactics have led to adoption by nation-state actors in addition to traditional cybercrime. They can augment or replace direct human interaction such as that seen by IT Help Desk worker deceit campaigns. Social engineering dependent on human interaction will likely remain a strength of groups with western or English-speaking constituents, whereas technical campaigns will be enabled and believability improved by AI/LLMs.	
BYOVD tactics persist, expand EDR remains a significant barrier to intrusion efforts, particularly among more voluminous and less sophisticated ransomware or data extortion operators. To address this, the use of Bring Your Own Vulnerable Driver (BYOVD) attacks to deploy "EDR Killer" malware has become more frequently observed. While these techniques struggle against class-leading EDR solutions, they remain effective against Small and Midsize Businesses (SMBs) which employ less robust or more vulnerable EDR and AV solutions. As proliferation of EDR continues, we expect the use of these tools and tactics to increase in kind.	

Ecosystem and Organization

Projected Impact

Distinct Named Groups continue to increase

GRIT continued to observe an increase in distinct named threat groups. While this has corresponded with a rise in total ransomware volume, most new groups are short-term, ephemeral groups that do not go on to become prolific or more established players. We assess that the rise in distinct named groups will likely continue, driven in part by reduced barriers to entry for new operators, as well as splintering or rebranding of existing groups.

RaaS types and forms persist

We principally observe ransomware groups taking one of three forms:

- Open RaaS: anyone can pay or be vouched for to join as an affiliate;
- Closed RaaS: affiliation methods are obfuscated or opaque, and membership is typically obtained through relationships and experience; and
- Insular ransomware groups: a RaaS construct is eschewed for in-house, broader spectrum expertise.

Each of these forms have their own advantages. Other than the very limited number of "insular" ransomware groups, we expect operators to align with groups based on historical relationships, maturity, and operational security preferences.

Double Extortion loses steam

The prevalence of effective, immutable backups in corporate backups increasingly renders single-extortion, or traditional ransomware ineffective against larger targets. This is evidenced by the rise of double-extortion and our own experience across incident response and ransomware negotiation cases. Despite this, data extortion – the second part of "double-extortion" – has retained its efficacy in encouraging compliance from victims. We have observed an increasing willingness by groups large and small to pursue "extortion-only" data extortion operations. We assess that this model will become more attractive for operators due to its efficacy, reduced footprint, retention of ransom payments, and reduced need for technical skill over the next two years.

Ransom demands "level out" – with floors and ceilings

Over the past 3 years, GRIT's internal data has shown a reduction in 8-figure ransom demands, and a rise in 6-figure demands with the occasional 7-figure outlier. This is likely in response to observations of the amount victims are and are not willing to pay. We have similarly observed, through blockchain analysis, typical "floors," or minimum payment amounts, that Established ransomware groups appear willing to accept. We assess that the most prolific and Established ransomware groups will continue to adapt their "floors" and "ceilings" for ransom demands in order to maximize their illicit revenue, and that these figures will likely fall as victims become less likely to pay.

Ransomware "influencers" attract Law Enforcement scrutiny

The most prolific and Established groups that we observed in 2025 tended to keep a "low profile," likely wary of attracting excess law enforcement or intelligence community scrutiny in ways that could lead to their downfall or disruption. We have similarly observed the increased visibility of more juvenile, attention-seeking actors that show no such compunction. Hellcat and Scattered Lapsus$ Hunters serve as examples of this behavior, which often takes the form of braggadocios social media behavior and overt public threats against current or potential victims. Fortunately, this behavior has been repeatedly shown to lead to law enforcement attention, often because of operational security mistakes. We assess that disruption efforts and law enforcement campaigns will continue, successfully, to target this "low lying fruit" over the next year

Lowered barriers to entry result in increased ephemeral groups

From the modern RaaS construct to AI/LLMs, potential cybercriminals need less technical skill than ever to impact public and private networks of victims. In 2025, we observed dozens of low-sophistication actors taking rudimentary and, at times, perplexing actions inside of environments to which they were able to gain a foothold. Ransom demands in these circumstances are typically lower, but this does not reduce the real impact in costs and productivity that result. We expect this trend to continue as the use of AI/LLMs, including "agentic" AI, becomes more well documented and easier to replicate by unskilled actors.

Disruption and Instability

	Projected Impact
Ransomware reporting requirements persist; bans unlikely in USA While we continue to assess that outright bans are unlikely to be politically tenable in the US, mandatory and optional statutory and regulatory reporting requirements at the state and federal level have substantially removed incentives for victims to pay to "cover up" a ransomware incident, thereby reducing ransomware's coercive leverage.	
Cryptocurrency valuations stall or decrease As cryptocurrency support becomes more mainstream in policy, additional outlets and avenues for its acquisition and use continue to emerge. While we are not experts on the economics of cryptocurrency and its value, increases and decreases have corresponding impacts to the finances of cybercrime and ransomware actors, who frequently keep substantial sums on the blockchain. Substantial deviations in valuations could alter individual calculus – for better or worse – in the years ahead.	
Law enforcement disruption efforts continue and expand International law enforcement cooperation has expanded in recent years and continues to bear fruit in the form of high-profile disruption and takedowns. However, the long-term efficacy of these operations is more of a mixed bag, with some as-a-Service providers rebounding and restoring operations within months. Nonetheless, we anticipate this trend will continue in Europe and the US, increasing uncertainty and costs for cybercrime enablers and ransomware groups.	
US private sector organizations' offensive capabilities unleashed As a very large unknown, recent reporting suggesting federal support for offensive cyber operations conducted by private organizations has potential – both good and bad. We assess the key variable to be the language of any such authorization, protections put in place by the administration, and the willingness of cybercrime and nation state actors alike to seek retribution for any such operations. While it's too soon to tell whether this will materialize, it would be a mistake to overlook its potential impact.	
Greater use of international sanctions against distinct groups Over the past two years, nothing has been more effective in completely interrupting the profitability of a particular ransomware group as the international sanctions emplaced against LockBit in 2024, which effectively made the formerly prolific group irrelevant. However, we acknowledge that LockBit presented a unique organization, in which payments to any affiliate could not be effectively separated from payments to the group's core administrator, "LockBitSupp," a feature of the group that is not repeated across all ransomware groups.	
Increased observed nation-state influence or direction of ransomware Cybercrime has traditionally been held as distinct from nation-state cyber operations, which are often broadly referred to as "Advanced Persistent Threats" or APTs. This distinction was less clear in the case of Russia, which has long turned a blind eye to cybercrime operations directed against the West. Through 2025, North Korea also leveraged conventional ransomware, deploying Qilin encryptors in a departure from historical operations in which DPRK-specific ransomware or malware functioned as DPRK's tool of choice. APT operations are more likely to garner significant "strategic" attention and resources and to be perceived as a "national security" threat beyond the criminal. If further evidence of connections between nation-state actors and cybercrime continues to emerge, we may see greater collective and federal resources apportioned to countering ransomware.	

Annual Wrap Up

As we enter 2026, we find it useful to reflect on last year's assessments. Our prior assessments that the most prolific Established ransomware groups will persist barring disruption or internal destabilization has borne out. Akira and Qilin continue to attack at scale, and former leaders RansomHub and Black Basta fell by the wayside in response to internal scams and leaks, respectively. We assess that this trend will continue and more groups may adopt Akira's "closed" or "semi-closed" RaaS model to minimize these risks and preserve operational security. Those that do not are likely operating on borrowed time until internal discord or law enforcement penetration render them ineffective.

The perimeter of enterprise networks remains a focal point for attackers, and we expect to see continued emphasis on targeting firewalls, VPNs, and publicly exposed platforms as a way to both gain an initial foothold for full-scale intrusions, and to "smash-and-grab" in support of rudimentary but widescale data extortion campaigns. Regrettably, as more of these campaigns come to pass, we expect more affiliates to become familiar and comfortable with perimeter device exploitation, placing greater importance on "secure by design" efforts from leading vendors in the space. Failures in this regard will almost certainly be exploited as widely as possible in 2026.

The same growing risks apply to adversary use of AI/LLMs, which, while not yet dominant, is growing. A substantial portion of the ransomware ecosystem consisting of less experienced and mature affiliates feeds on the "scraps" of the most capable. As this has been true with vulnerability exploitation, we expect to see the same in AI/LLM usage. What is innovative today will almost certainly become routine within the next year.

Policy pertaining to and targeting cybercrime remains a shifting black box, and it remains too soon to tell whether bold ideas such as unleashing private sector offensive capabilities on nation-state and cybercrime actors will come to pass. In spite of that, we have high confidence that the US operating environment is unlikely to face ransom payment bans or strong cryptocurrency reporting requirements over the next year.

Overall, progress against ransomware and cybercrime remains consistently visible, albeit slow and largely reactive in nature. We hope that you have found at least some new knowledge and insights in this report, and that we will all continue to do our jobs in the broader sense throughout the new year at the expense of our adversaries.

Happy Hunting,

GRIT