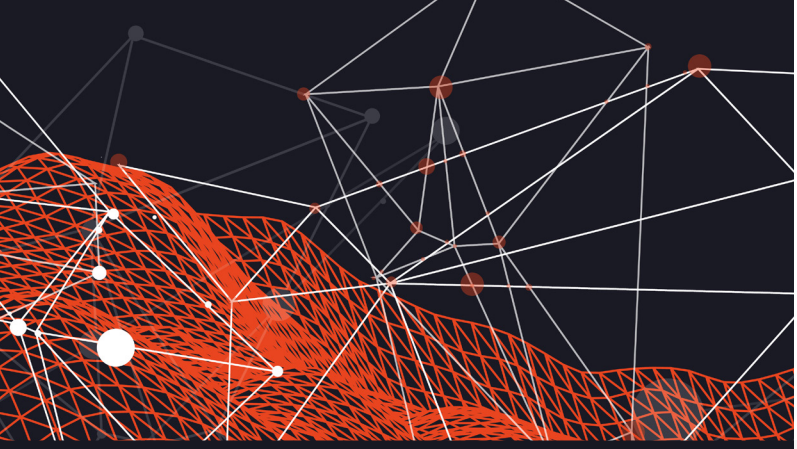
SEARCHLIGHT. CYBER

THE RANSOMWARE LANDSCAPE IN H2 2025

RANSOMWARE'S RECORD YEAR: TRACKING A VOLATILE LANDSCAPE IN H2 2025



SEARCHLIGHT.
CYBER

Searchlight Cyber was founded in 2017 with a mission to stop criminals from acting with impunity. With its pioneering Preemptive Threat Exposure Management (PTEM) offering, Searchlight helps organizations identify exposures and neutralize threats before attacks begin. Searchlight unifies leading Attack Surface Management, dark web intelligence, and risk management tools to help organizations separate the signal from the noise and prioritize the threats that matter. It is used by some of the world's largest enterprises, government and law enforcement agencies, and the Managed Security Service Providers at the forefront of protecting customers from external threats.

Find out more at **www.slcyber.io**.

ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM
CYBER ESSENTIALS
AICPA SOC
Crown Commercial Service Supplier

METHODOLOGY

The data in this report is a combination of Searchlight Cyber's dark web telemetry on ransomware groups and open source intelligence. All dark web data was collected from ransomware leak sites and forums and relates to the reporting period of 01 July 2025 - 31 December 2025, plus comparisons to full-year data and previous reporting to show trends over time. The purpose of this report is to demonstrate the insights that can be derived from the dark web but this data should always be used in conjunction with other open source information.

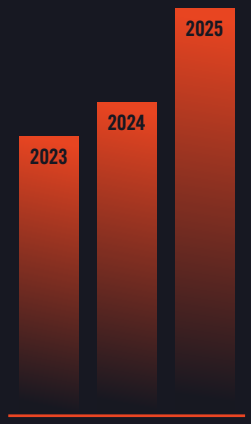
CONTENTS

EXECUTIVE SUMMARY:

RANSOMWARE IN 2025 IN NUMBERS

7,458

VICTIMS WERE LISTED BY RANSOMWARE GROUPS ACROSS 2025



THIS IS A **30% INCREASE** ON 2024 SIGNIFYING SUBSTANTIAL GROWTH.

2024 WAS **12% HIGHER** THAN IN 2023.

3,725

VICTIMS WERE LISTED BY RANSOMWARE GROUPS IN H2 2025

THIS IS A VERY SLIGHT **0.24% DECLINE ON H1 2025**, SIGNIFYING A STABLE AND CONSISTENT THREAT ACROSS THE YEAR.

93

DISTINCT RANSOMWARE GROUPS WERE OBSERVED IN H2 2025

2025 SAW A TOTAL OF **124 ACTIVE GROUPS.**

38 WERE COMPLETELY **NEW GROUPS.**

QILIN

WAS THE NUMBER ONE RANSOMWARE GROUP BY LISTED VICTIMS

AKIRA, **INCRANSOM**, **SINOBI**, AND **PLAY** COMPLETE THE TOP FIVE.

INTRODUCTION:

USING THE INTELLIGENCE RANSOMWARE GROUPS PROVIDE

Looking ahead to a year already defined by geopolitical instability and economic uncertainty, it's important to re-affirm why tracking and reporting on developments in the ransomware landscape is so important.

The financial stakes have never been higher. Global ransomware damage costs are projected to hit $57 billion USD this year alone. If current trajectories hold, we are looking at a staggering $265–275 billion USD in annual losses by 2031.

This isn't just an issue for the corporate balance sheets of individual companies; the U.S. authorities' decision to offer rewards of up to $15 million USD for information leading to the arrest of top-tier ransomware operators underscores the severity of the situation. Law enforcement is no longer just monitoring these groups, they are treating them as high-value state-level targets.

A PARADOX OF PROGRESS

While the second half of 2025 saw a marginal dip in publicly disclosed victim counts, any sense of victory is premature. Year-over-year data confirms that ransomware extortion victims are at an all-time high. We are witnessing the maturation of a professionalized ecosystem that remains devastatingly effective despite increased pressure from global authorities.

The landscape is currently defined by two contradictory trends:

Fragmentation:

Large, monolithic syndicates are fracturing into smaller, more agile cells, presenting a moving target and a complex ecosystem that is difficult to track by design.

The Rise of Supergroups:

Conversely, in 2025 we observed the emergence of "supergroups" like Scattered Lapsus$ Hunters, where actors pool their specialized talents to scale operations and become a defining threat across the year.

THE AI CATALYST AND EXPANDING ATTACK SURFACES

In the second half of the year and across 2025, we tracked more active ransomware groups than ever before, with the highest number of brand new groups appearing. AI has lowered the barrier to entry, allowing brand-new groups to automate their operations and scale their operations almost overnight. This, combined with frequent rebranding to evade detection, makes constant and active tracing of these groups a priority for defenders.

Furthermore, the "shadow exposure" within third-party software continues to be the Achilles' heel for organizations. Vulnerabilities are being weaponized faster than the average patch cycle can keep up, with sophisticated groups increasingly bypassing traditional perimeters by exploiting freshly discovered flaws in the software supply chain.

KEY ACTORS AND THE PATH FORWARD

Our analysis of the top five ransomware groups by victim count reveals a shifting leaderboard. Qilin dominated the latter half of the year, cementing its position as the most prolific threat actor, while newcomers like Sinobi have demonstrated an ability to chalk up substantial victim counts within just months of their debut.

The data in this report provides a stark warning, but it serves a vital purpose. Awareness and visibility are fundamental to defending against this threat. Law enforcement operations, such as the coordinated strikes against the BlackSuit (Royal) group last year, prove that putting continued pressure on these groups works, but as we see from the data, it cannot be the only solution.

For organizations in the crosshairs, the strategy must be preemptive. By maintaining early visibility into group tactics and a continuous, real-time view of exposures, businesses can get ahead of the threat. In the high-stakes game of ransomware in 2026, the only way to truly win is to ensure you aren't an eligible target in the first place.

LUKE DONOVAN

Head of Threat Intelligence
and Data Collection
Searchlight Cyber

RANSOMWARE ACTIVITY SNAPSHOT:

2025 END OF YEAR OVERVIEW

VOLUME AND SCALE OF VICTIMS

The second half of 2025 saw a reduction in the number of ransomware victims being named publicly on extortion sites compared to that seen during the first half of 2025. However the drop was slight. The first 6 months of the year saw 3,733 victims and the last 6 months saw 3,725 (**See Figure 1**). On the face of it, this is a positive, if only a slight step forward. The reality of the situation is that the ransomware landscape continues to grow and adapt.

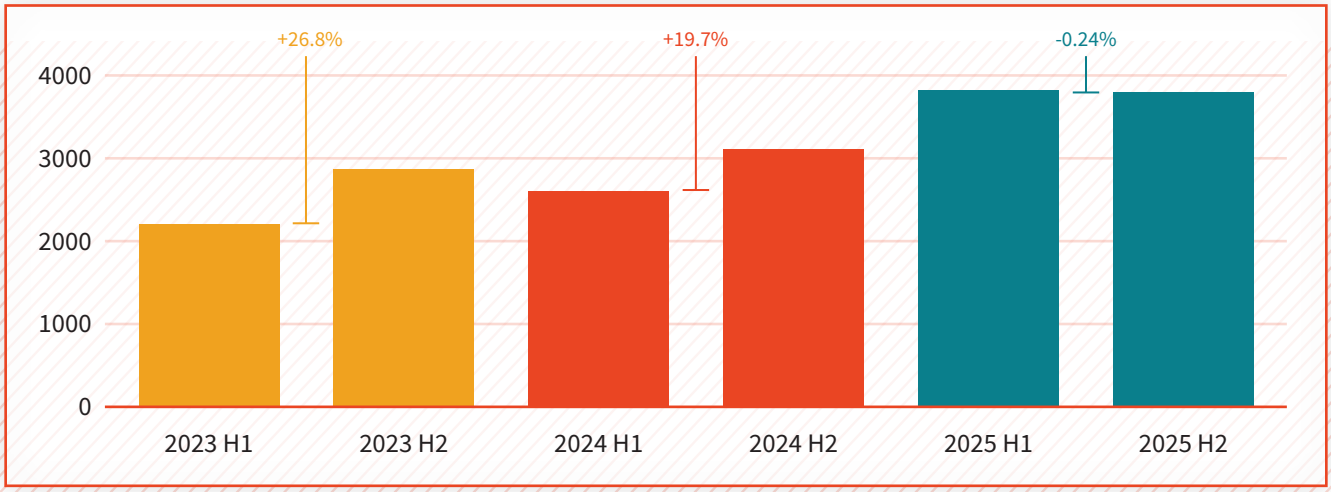


Figure 1: *Ransomware victims by half year, 2023 - 2025.*

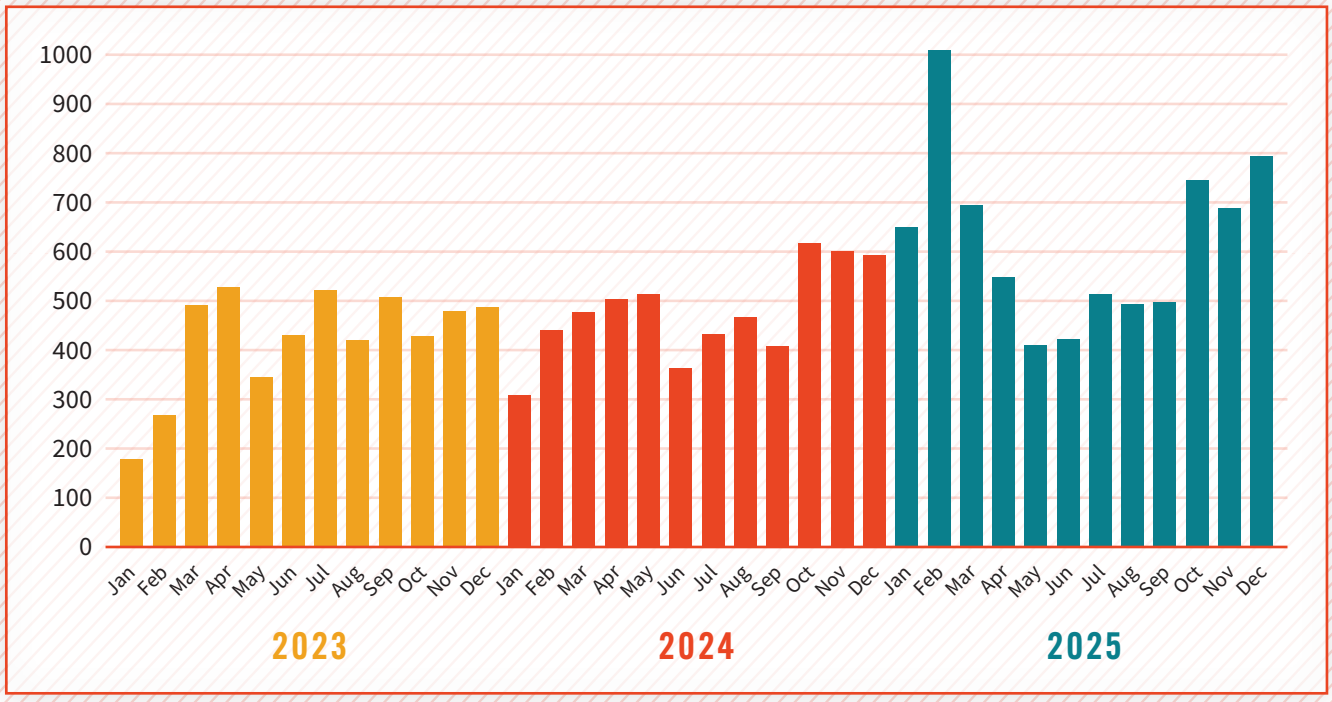


Figure 2: *Ransomware victims by month, January 2023 - December 2025.*

The second half of 2025 turned out to be the second highest number of victims observed since at least the start of 2023 when our data analysis begins. When yearly statistics based on the number of victims are determined the picture becomes clearer (**See Figure 2**). There continues to be a year-on-year increase in the number of victims being posted.

Searchlight Cyber identified 7,458 victims over the course of 2025, representing a significant 30.2 percent increase over the 5,728 victims recorded in 2024. What this data shows is that the number of victims is growing, and it's growing faster than ever; the year-over-year increase from 2023 (5,081 victims) and 2024 (5,728 victims) was much more slight at just a 12.7 percent increase.

These initial findings corroborate Searchlight Cyber's 2025 H1 Ransomware report[1] assessment that the ransomware landscape would remain a pervasive and formidable threat throughout the second half of the year.

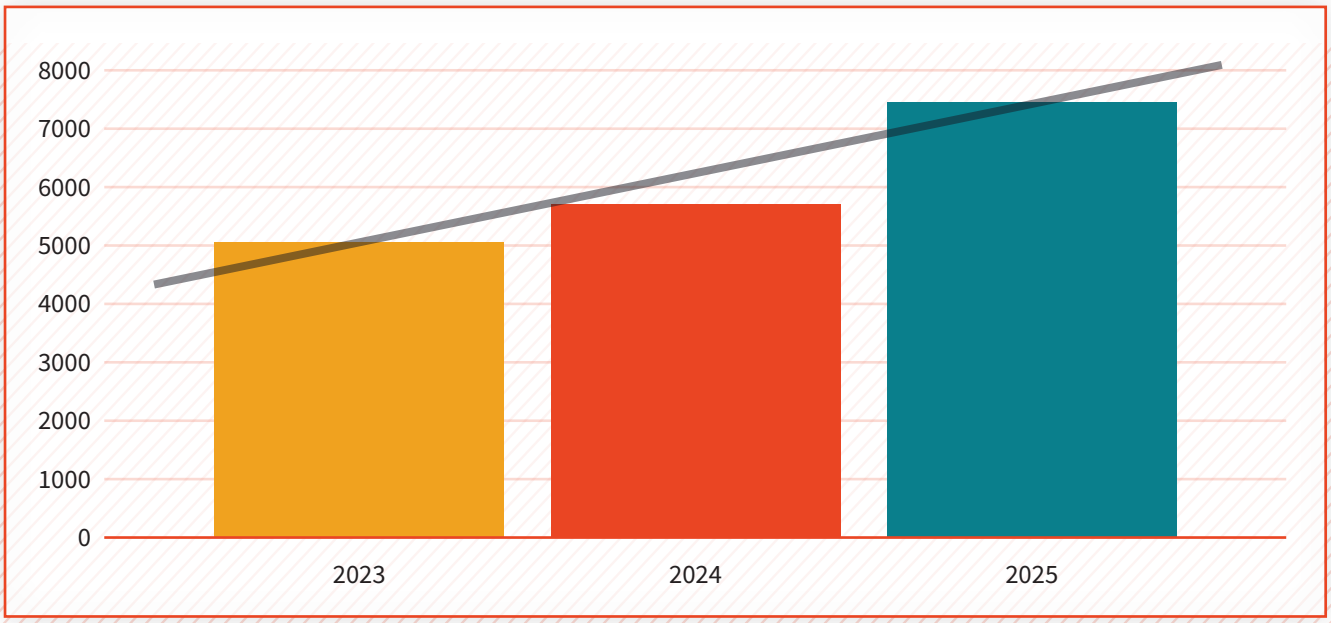


Figure 3: *Ransomware victims by year, 2023 - 2025.*

[1] https://slcyber.io/wp-content/uploads/2025/09/Ransomware-in-H1-2025-Report-Searchlight-Cyber.pdf#page=42

VOLUME AND SCALE OF RANSOMWARE GROUPS

The number of victims might have slightly dipped in the second half of the year, but what has not is the number of active ransomware groups. We previously reported that there were 88 ransomware groups operating in the first half of the year (a 16 percent increase on the 76 observed in the second half of 2024), during the second half of 2025 this had increased to a record high of 93. Groups will come and go due to a variety of factors outlined below, and so it can be useful to break down how many ransomware groups were operating per month (**See Figure 4**)

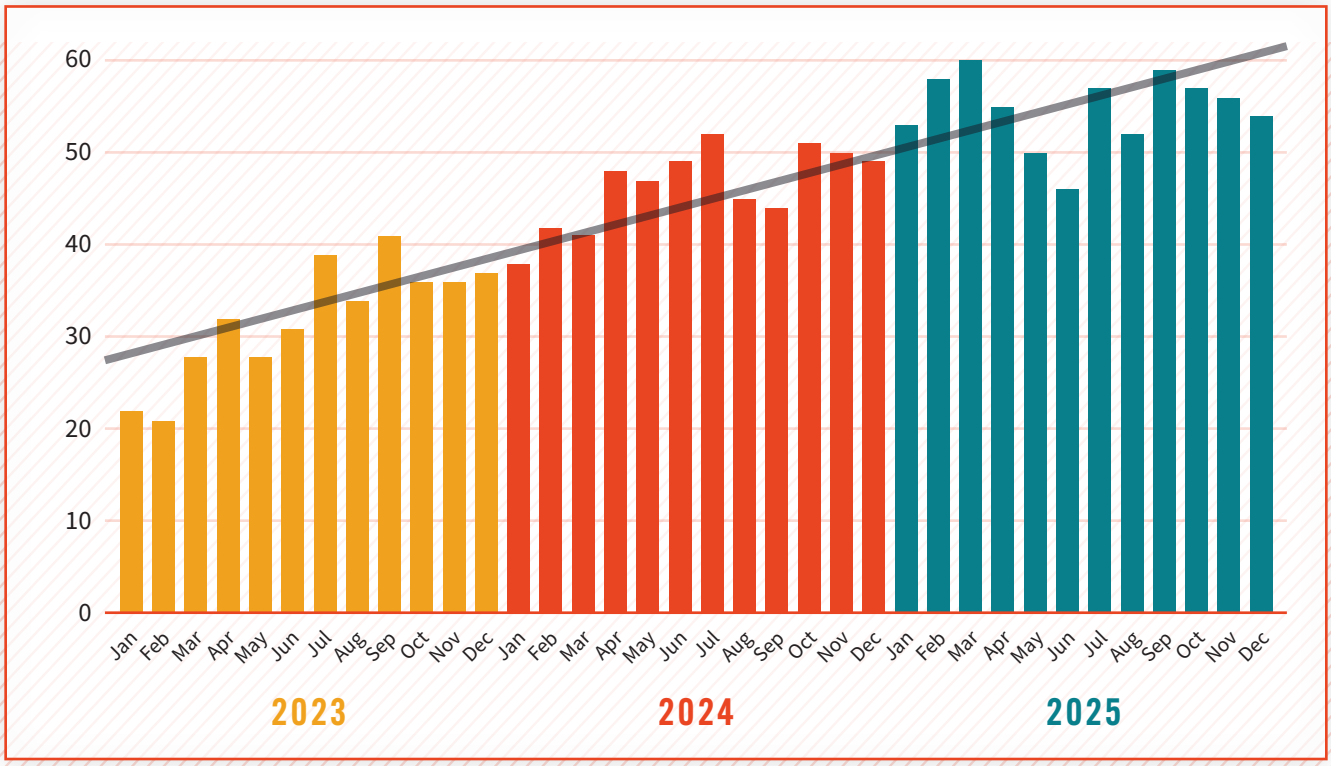


Figure 4: *Active ransomware groups by month*

As can be seen in Figure 4, there is a trend indicating a growing number of active ransomware groups per month and year. If we consider the total number of ransomware groups who posted a victim on a leak site/shaming blog, we see that 2025 resulted in 124 groups (**See Figure 5**).

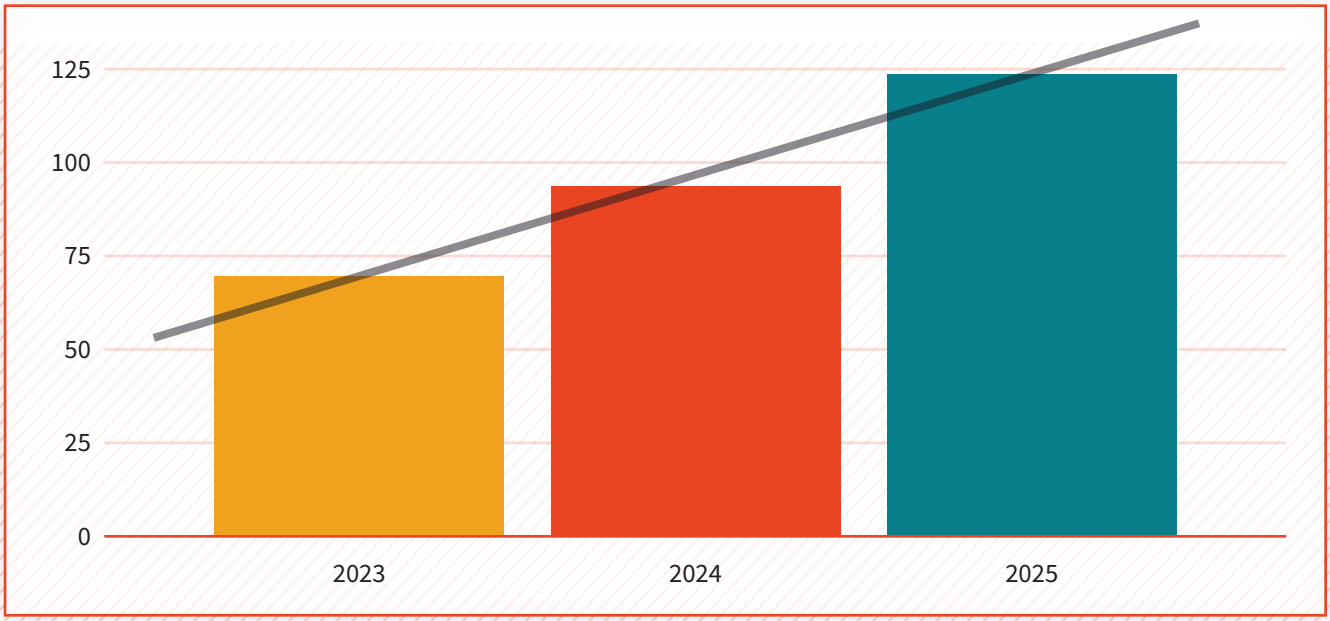


Figure 5: *Active ransomware groups by year.*

The frequency and trends behind new ransomware groups emerging can help develop an insight into the ecosystem.

Lower barrier of entry	With experience, the acquisition and amendment of ransomware malware and the exploitation of AI, more individuals become capable of conducting ransomware operations.
High profitability and weak deterrence	As more and more successful ransomware stories break on the news, with good payouts, conducting such operations becomes more appealing, particularly if law enforcement activity is viewed as a low deterrent.
Fragmentation and rebranding	Individuals within groups will move on to different projects and start up their own operations.
Global tension and safe havens	Some states will fail to take action against ransomware operators, particularly if it is deemed that their activity will benefit state goals.
Growing attack surface	As organizations' IT estates grow, the more targets there are. With a growing attack surface, traditional security methods struggle to keep up with exposures.
Improved visibility and tracking	Due to the threat posed by ransomware, the monitoring of emerging groups has become a higher priority. With greater visibility, we have a clearer view of when new groups emerge, diverge and rebrand.

NEW RANSOMWARE GROUPS ON THE SCENE

The general trend of the ransomware environment growing over previous years and throughout 2025 continues when we look at the number of new groups that have formed. The second half of 2025 saw the largest number of new ransomware groups emerge, with 38 recorded. This was slightly more than the 35 identified in the first half of the year (**See Figure 6**).

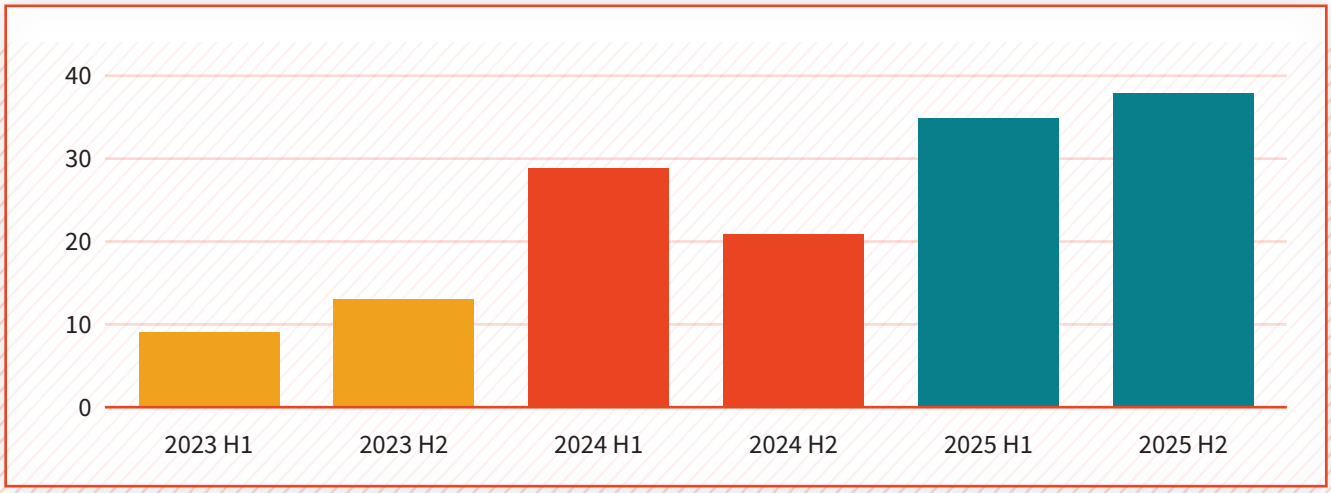


Figure 6: *Newly identified ransomware groups by half years.*

In terms of full years, 2023 saw 22 new ransomware groups, 2024 saw 50 new groups and 2025 saw 73.

As alluded to in Figure 5 and also previously reported on by Searchlight Cyber, the ransomware landscape is becoming more fragmented. This is due to the disruption of some of the big ransomware groups and an increase in the number of active groups conducting ransomware operations. The statistics at the close of 2025 continue to back this up; not only have the number of victims increased year on year but on average the monthly number of active ransomware groups has continued to increase since 2023.

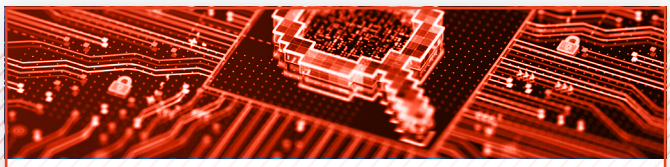
The pace of change and the emergence of brand new groups presents a growing challenge for defenders to keep up with. When it comes to 'knowing your enemy', organizations aren't simply defending against individual adversaries but a highly complex and professionalized ecosystem. As demonstrated later in this report, a small and emerging group can quickly become a dominant and dangerous adversary in mere months. For governments and law enforcement, ransomware groups are the ultimate moving target, and the continued fragmentation impacts where to focus resources in terms of offensive measures. The increased complexity of the ransomware threat underscores the continued importance of detailed monitoring and tracking of this activity.

AI IN THE RANSOMWARE ARSENAL

For ransomware groups, AI acts as a force multiplier, automating the most labor-intensive stages of an attack. This lowers the barrier to entry for less technically skilled actors, and allows established and sophisticated groups to scale their operations even further.

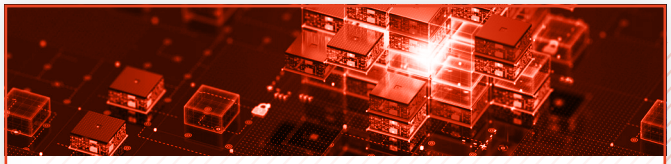
HYPER-PERSONALIZED SOCIAL ENGINEERING

AI has effectively eliminated the language barrier for ransomware groups. Threat actors now use Large Language Models (LLMs) to craft flawless, culturally nuanced phishing lures in any language, removing the grammatical red flags that once served as a primary defense for users. This allows social engineering to be highly targeted and effective; adjusting tone and urgency in real-time based on victim interaction, at far greater speed and scale.



AUTOMATED BREACHED CONTENT ANALYSIS

The trend towards large scale data theft presents ransomware groups with the issue of processing terabytes of stolen data to identify sensitive information that can be exploited. AI-driven analysis tools now allow groups to ingest breached content and instantly surface sensitive information; such as legal documents, financial records, or credentials, that can be weaponized for secondary extortion or used to map out future attack vectors within a supply chain.



MALWARE CREATION AND REFINEMENT

While RaaS affiliates still largely rely on provided payloads, the core developers behind these groups are increasingly using AI to refine their code. Ransomware creators can prompt AI to iteratively review, debug, and amend malicious scripts, allowing them to rapidly adapt the code to new security patches and updated security measures. AI's ability to write malware code from scratch, which is continually improving, is another factor lowering the barrier to entry for less-skilled actors.

24/7 VICTIM COMMUNICATIONS & AUTOMATED NEGOTIATION

In 2026 we also saw groups employing AI tools in the negotiation phase. Groups like Global Ransomware have pioneered the use of custom AI chatbots to handle victim communications. These bots manage initial triage, verify decryption capabilities, and maintain constant pressure with automated countdown timers and scripted threats. By removing the need for a human negotiator to be awake and online, groups can manage dozens of victims simultaneously across every time zone, ensuring the extortion process never loses momentum.

ATTACK DISTRIBUTION

The distribution of ransomware victims across continents in the second half of 2025 remained consistent with the first half of the year, showing no notable shifts (**See Figure 7**).

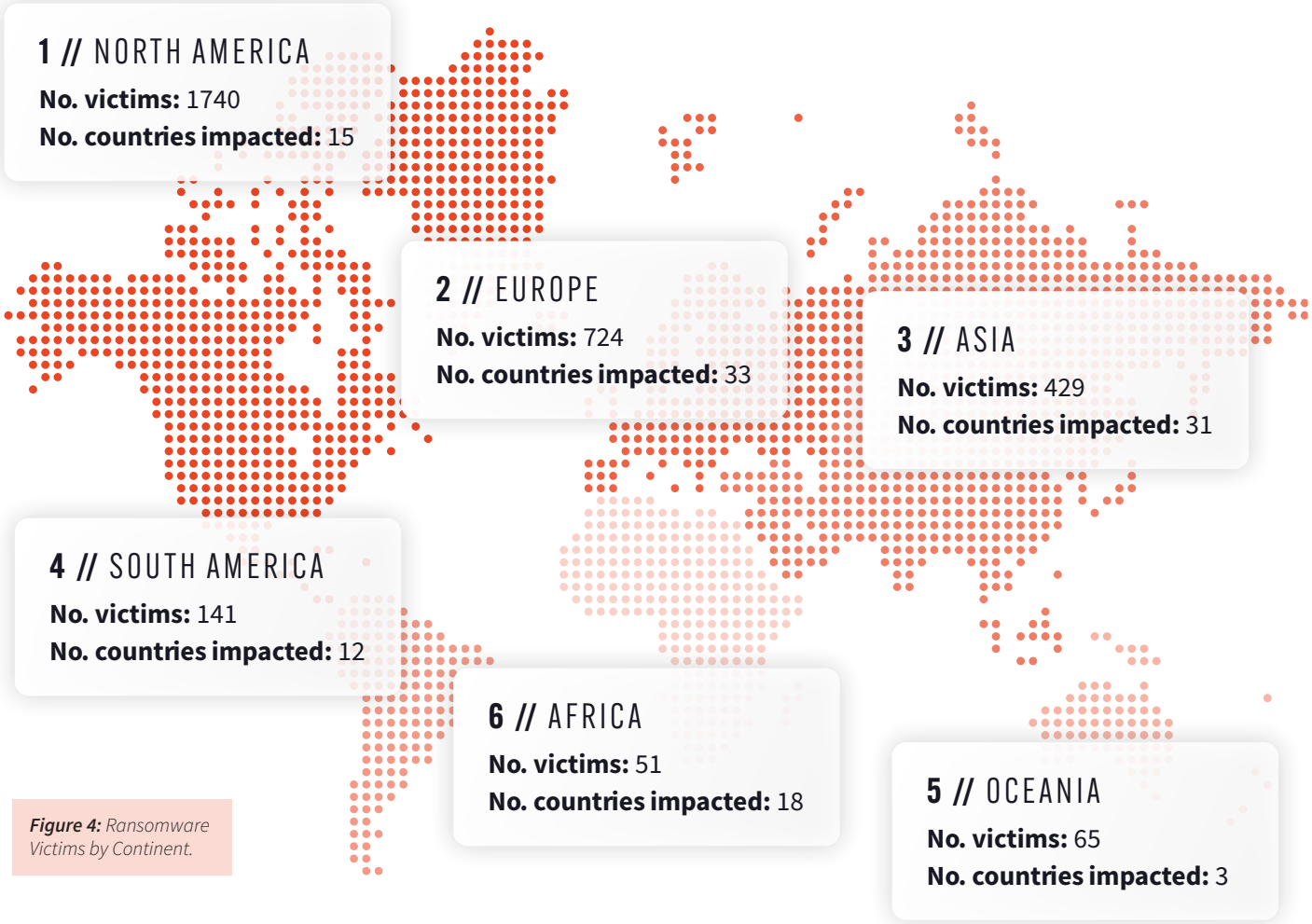


Figure 4: *Ransomware Victims by Continent.*

The same goes for the top 5 countries based on the number of victims made public (**See Figure 8**).

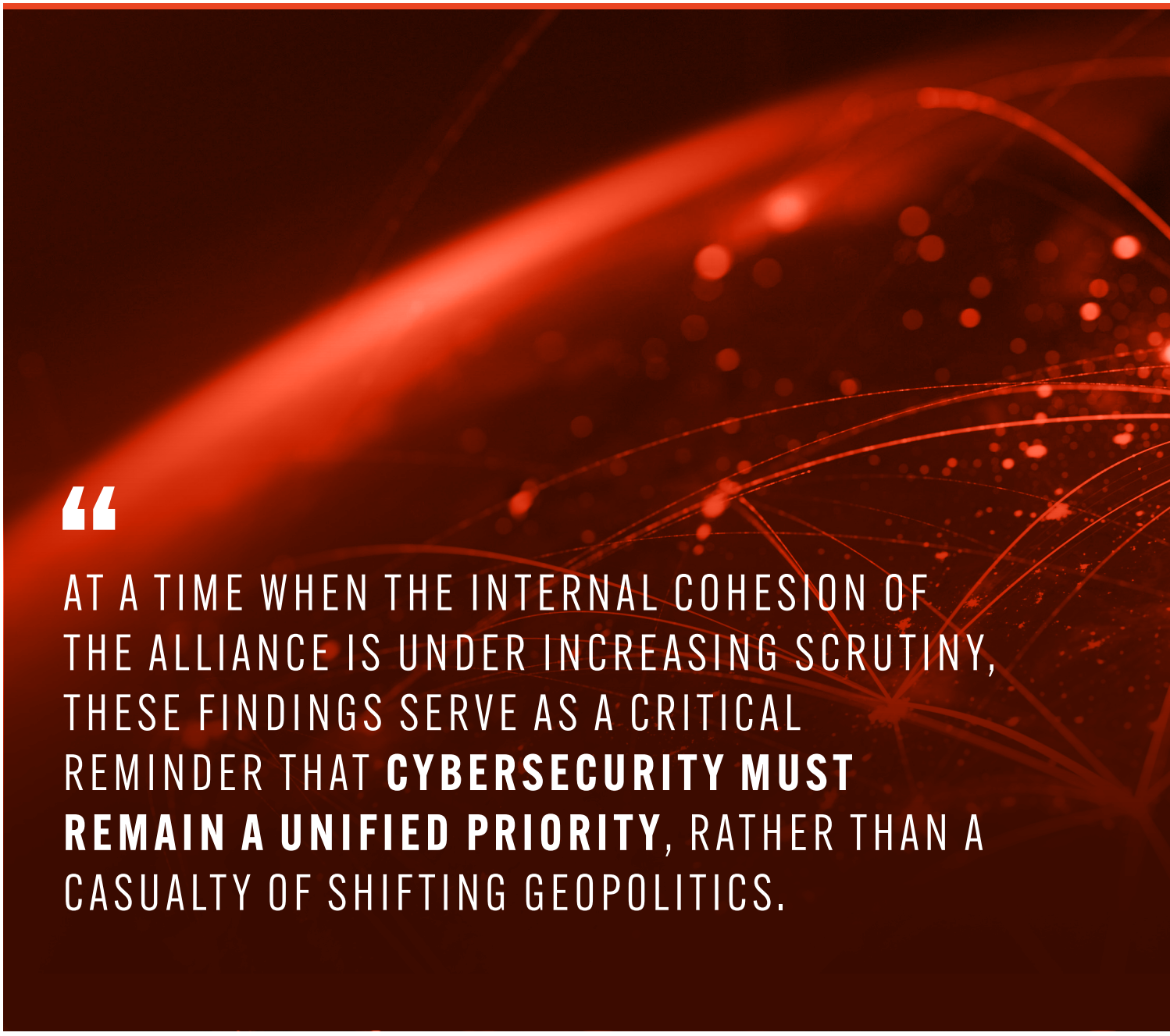
SERIAL	COUNTRY	NO. OF VICTIMS
1	UNITED STATES	1,536
2	CANADA	182
3	GERMANY	167
4	UNITED KINGDOM	131
5	FRANCE	79

Figure 8: *Ransomware Victims by Country.*

As outlined in our H1 report, the trends observed clearly indicate a sustained and aggressive ransomware campaign targeting organizations worldwide, with a notable emphasis on North America and Europe.

This geographic focus can be explained through a number of factors, such as the high economic value of these regions, their expansive technological attack surfaces, and shifting geopolitical motivations aimed at NATO members.

Building on our findings from the first half of 2025, the geographical distribution of ransomware victims remains skewed toward NATO member states. This persistent trend underscores the need to prioritize unified defensive measures, including scaled-up cybersecurity funding and strengthened collaboration through intelligence sharing. At a time when the internal cohesion of the alliance is under increasing scrutiny, these findings serve as a critical reminder that cybersecurity must remain a unified priority, rather than a casualty of shifting geopolitics.



THE TOP RANSOMWARE GROUPS OF H2 2025

SERIAL	RANSOMWARE GROUP	RAAS	NO. OF VICTIMS
1	QILIN	YES	679

Emerging in mid-2022, this RaaS group was originally called "Agenda" before rebranding as Qilin. They predominantly use social engineering to gain initial access and then target victims using the Windows, Linux, and ESXi operating systems.

2	AKIRA	YES	384

Identified in March 2023, Akira is a prolific RaaS operation that has claimed over 1,200 victims using double extortion tactics. The group gains access through IABs as well as through exploiting technical vulnerabilities in VPN and RDP software.

3	INCRANSOM	YES	213

Financially motivated RaaS operator IncRansom uses double extortion to pressure victims across a diverse range of global industries and sectors, utilizing a wide range of initial access vectors from phishing to vulnerability exploitation.

4	SINOBI	NO	180

First appearing in July 2025, Sinobi is a hybrid RaaS group that likely emerged as a rebrand or successor to Lynx and IncRansom. The group maintains a low profile on hacking forums, often gaining entry through IABs or breached credentials.

5	PLAY	NO	164

Unlike the other groups on this list, Play doesn't use the RaaS model, instead operating as a closed and select ransomware group. It's known to obtain breached credentials from stealer logs to launch attacks, as well as exploit vulnerabilities to gain access.

The following table (**Figure 9**) details the top 5 groups based on the number of victims across the whole of 2025. A comparison has been made as to the position of the group in 2024, if applicable.

SERIAL	GROUP	NO. OF VICTIMS	PREVIOUS POSITION
1	QILIN	968	7
2	AKIRA	729	4
3	CLOP	518	19
4	PLAY	362	3
5	INCRANSOM	338	10

Figure 9: *Most prolific Ransomware Groups (2025).*

SERIAL	GROUP	2023	2024	2025	TREND
1	QILIN	45	186	968	INCREASE
2	AKIRA	163	315	729	INCREASE
3	CLOP	389	93	518	MIXED
4	PLAY	318	366	362	STABLE
5	INCRANSOM	46	165	338	INCREASE

Figure 10: *Year Comparison.*

MOVERS AND SHAKERS

Qilin's rise to the top

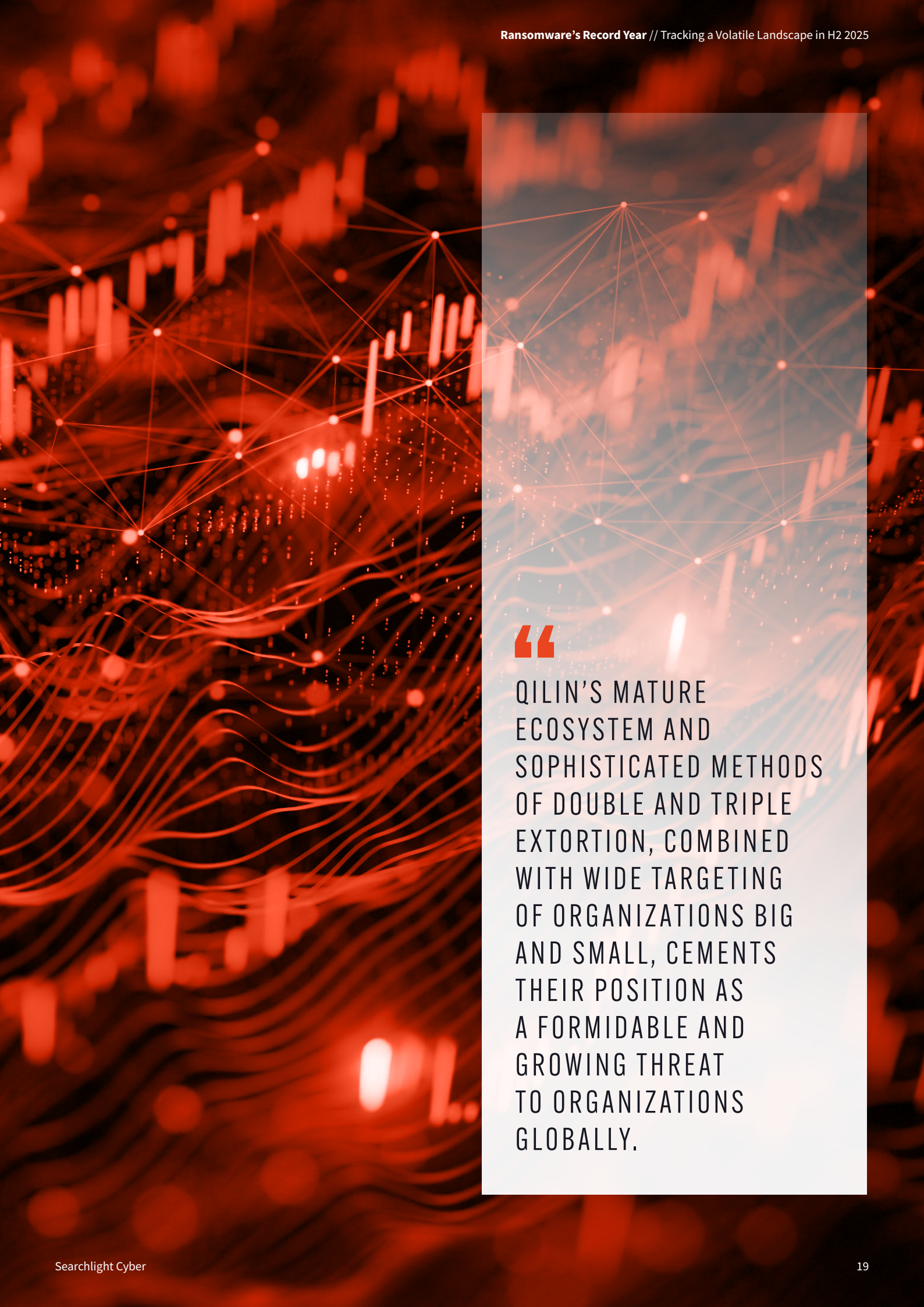
Placing at number 3 by victim count in the first half of the year, Qilin's prolific activity in H2 shot them to the top spot. On a year-over-year basis, the group saw a staggering 420 percent increase in victims, and stands out as the only group generally listing greater volumes of victims month-over-month. Their mature ecosystem and sophisticated methods of double and triple extortion, combined with wide targeting of organizations big and small, cements their position as a formidable and growing threat to organizations globally.

Cl0p's drop

Taking the top step of the podium in the first half of the year, Cl0p's complete absence from the top 5 in H2 is notable. However, this sporadic activity is typical of the group, who specialize in exploiting novel zero-day vulnerabilities, often facilitating widespread supply chain attacks. This force-multiplier results in a flurry of victims, such as in February 2025, where the group posted hundreds of victims compromised through zero-day exploits in Cleo managed file transfer products. As such, it would be a grave error to count them out. Barring any major disruptions to their operations, we could well see this experienced and well-resourced group back with a bang in 2026.

New faces in the top 5

IncRansom and Sinobi made their first appearances in the top 5 in the second half of the year, with the more-established IncRansom RaaS operation gradually stepping up their widespread double extortion tactics. Sinobi represents a newly-branded player coming in straight away to the top 4 through a professionalized and disciplined RaaS structure, primarily targeting industries where operational downtime can have a significant impact, such as manufacturing and production.



> QILIN'S MATURE ECOSYSTEM AND SOPHISTICATED METHODS OF DOUBLE AND TRIPLE EXTORTION, COMBINED WITH WIDE TARGETING OF ORGANIZATIONS BIG AND SMALL, CEMENTS THEIR POSITION AS A FORMIDABLE AND GROWING THREAT TO ORGANIZATIONS GLOBALLY.

PROFILES OF THE FIVE MOST PROLIFIC RANSOMWARE GROUPS

#1 QILIN

Qilin is a prolific ransomware group using the RaaS business model. The group became active in mid 2022, initially using the name "Agenda". At the time of writing this report, the group has claimed over 1300 victims via its extortion site.

The initial ransomware variant was developed using the Go programming language, however, this was rewritten using Rust and later C. Variants target systems using the Windows, Linux and ESXi operating systems. The group is known to heavily rely on social engineering techniques to gain initial access.

A member of the Ramp cybercrime forum using the 'Haise' handle is a representative of the ransomware group and often advertises the affiliate program with the intention of recruiting new members. The forum user claimed that the ransomware is capable of delivering four types of encryption, encrypting a file in full or in part. Successful candidates for the RaaS scheme are granted access to a panel featuring the build configurator, dialogue support, and spam calling and SMS services.

Qilin has made several updates over the course of 2025, and added an option to conduct distributed denial-of-service (DDoS) attacks against victims to pressure them into paying the ransom. This is known as triple extortion. Additionally, affiliates are offered legal advice on how to negotiate with victims based on their jurisdiction and type of compromised data, tailoring, and streamlining their negotiation process to each victim.

> COMPARED TO THE OTHER TOP MOST ACTIVE GROUPS, QILIN HAS GENERALLY POSTED MORE VICTIMS MONTH-ON-MONTH IN 2025

In the latest update, the Qilin spokesperson stated that a call center available in seven languages would be soon opened to contact victims and their customers. All of this suggests an acceleration of activity and - indeed - compared to the other top most active groups, Qilin has generally posted more victims month-on-month.

In September 2025, on a closed Russian hacking forum, DragonForce announced a coalition with other RaaS operators, namely Qilin and LockBit. The proposed aim of the coalition was to pool resources and work together to increase overall income. Since this announcement, as evidenced by our data, Qilin's victim count and prominence increased, potentially demonstrating another example of the success of the 'Super Group' collaboration model.

Posted by **dragonforce** @ Ramp
2025.09.15 English

> I'm excited to share our latest updates with you! We have revamped our
> products, offering more stability and speed! We have launched a ticketing
> system for all our *FREE* services, including our call service (the best
> in the world for reaching your goals), hash decryption (we break
> everything that seems unbreakable), *and 24/7 support to help you with
> your inquiries*. Our roadmap is still quite extensive, so stay tuned for
> more news!
> Click to expand...
>

The coalition,

>
> The coalition between *Qilin* , *Lock Bit* , and *DragonForce* is uniting
> our efforts as we collaboratively develop our direction. Our doors are
> open to anyone who cares about the future of our challenging field. If you
> have a partnership program, feel free to reach out to us, and together we
> can maximize our overall income! More updates on this topic will be coming
> soon, so keep an eye out for news.
> Click to expand...
>

- *TOX, BLOG, FS*

Figure 11: *DragonForce forum post announcing a 'coalition' with Qilin and LockBit, September 2025.*

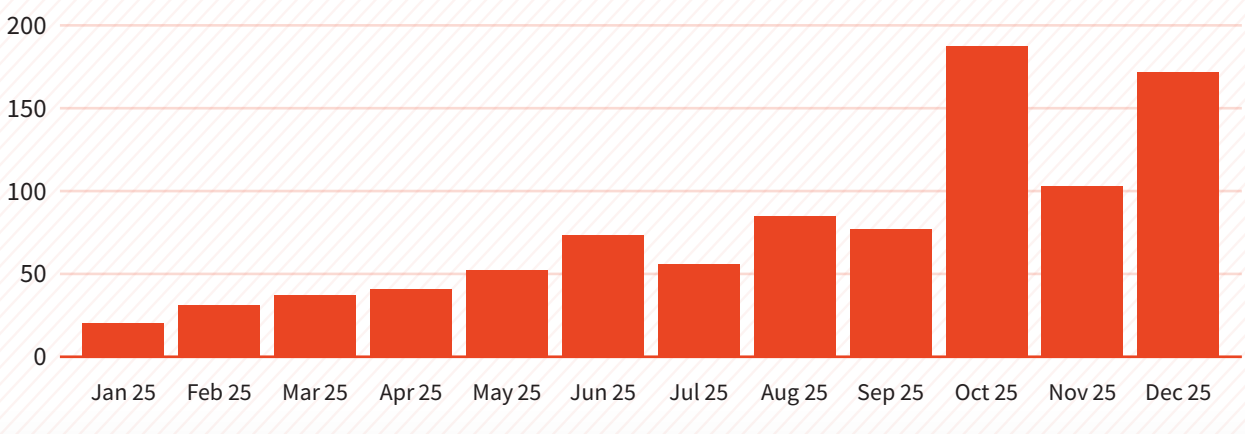


Figure 12: *Qilin victims per month, 2025.*

#2 AKIRA

Akira is a prolific ransomware group operating under the RaaS business model. The group was first identified in March 2023 and claimed at least 1200 victims (as of the end of 2025) via their extortion site.

The ransomware variant employed by the group has evolved over time, with first strains being developed using the C++ programming language and giving files the .akira extension when encryption was completed. The group has started using the Megazord ransomware variant as well, which uses the .powerranges extension.

Like many other ransomware groups, Akira's affiliates obtain initial access from a multitude of sources, such as stealer logs or Initial Access Brokers. Access is also obtained by exploiting technical vulnerabilities found in common commercial solutions such as Cisco or SonicWall VPN software and remote desktop protocol (RDP) apps. Social engineering such as phishing and spearphishing are also part of their tactics.

Once an initial foothold is established, the group often employs an attack technique known as Kerberoasting to dump the Local Security Authority Subsystem Service (LSASS) and obtain additional credentials.

Mimikatz and LaZagne have also been used to obtain additional credentials. Exfiltration is done by leveraging legitimate tools including FileZilla, Rclone, WinSCP and WinRAR.

Although Akira is likely a self-established group with no major links to other ransomware groups, past or present, there are some indications that certain elements of the malware itself were inspired by Conti. Moreover, some cryptocurrency payments can be traced to former members of the Conti affiliate program.

The ransomware strain is sophisticated and uses a hybrid encryption method, however, a decryptor was created and shared in the community on two different occasions, one in 2023 and one in early 2025. The latter was particularly interesting as it uses GPUs to bruteforce to decrypt keys. However, it only worked on Linux-based systems and required a significant upfront investment to purchase numerous GPUs. It was also a lengthy process to obtain a decryption key, it took 16 high end GPUs 10 hours to decrypt one single key.

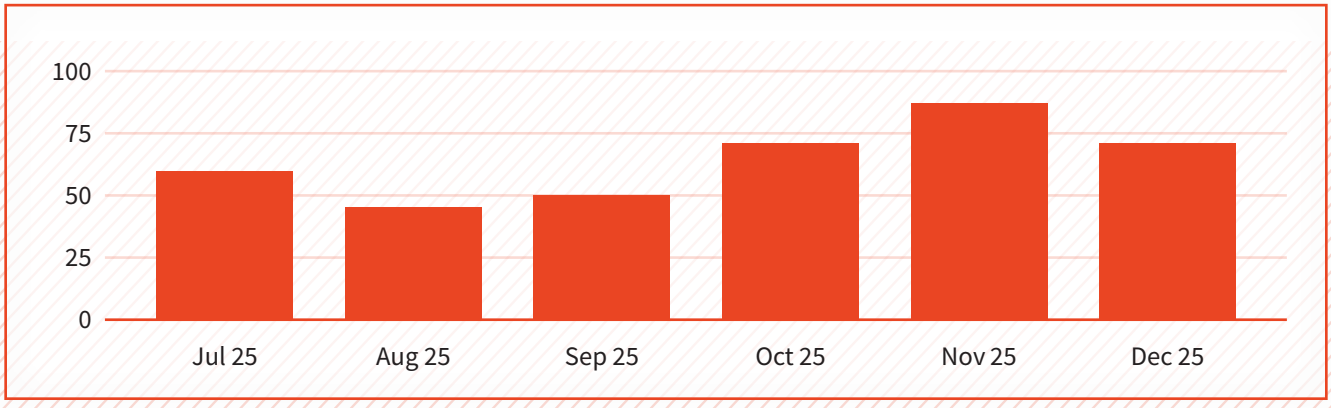


Figure 13: *Akira victims per month, H2 2025.*

#3 INCRANSOM

IncRansom is a financially motivated group that emerged in 2023. The group have operated a RaaS model and so victims are spread across sectors/industries and geographically. As with many ransomware groups, double extortion, the encrypting, downloading and applying pressure on the victim is the general tactic utilized. Again, similar to many RaaS operators, a mixture of initial access vectors are exploited, ranging from using purchased credentials, conducting phishing campaigns or exploiting known vulnerabilities.

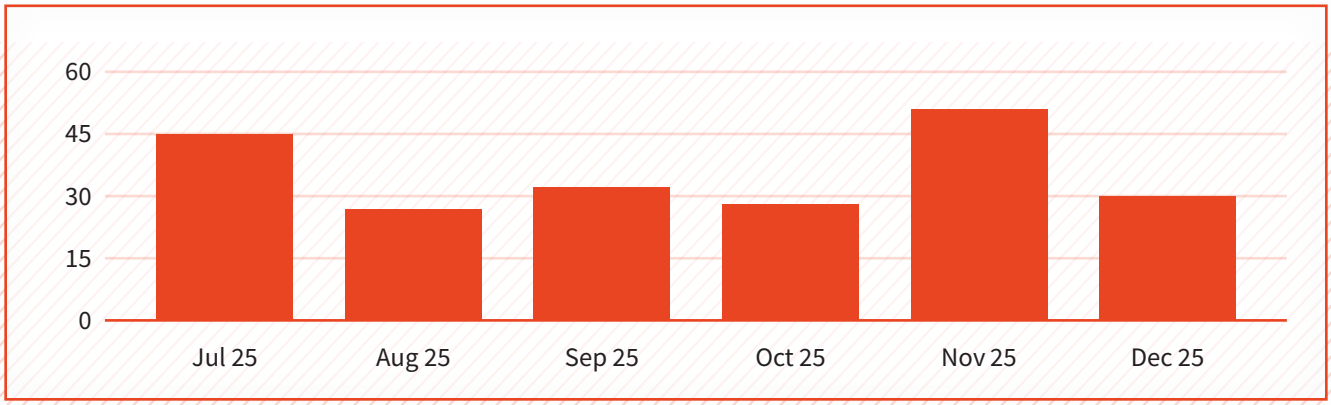
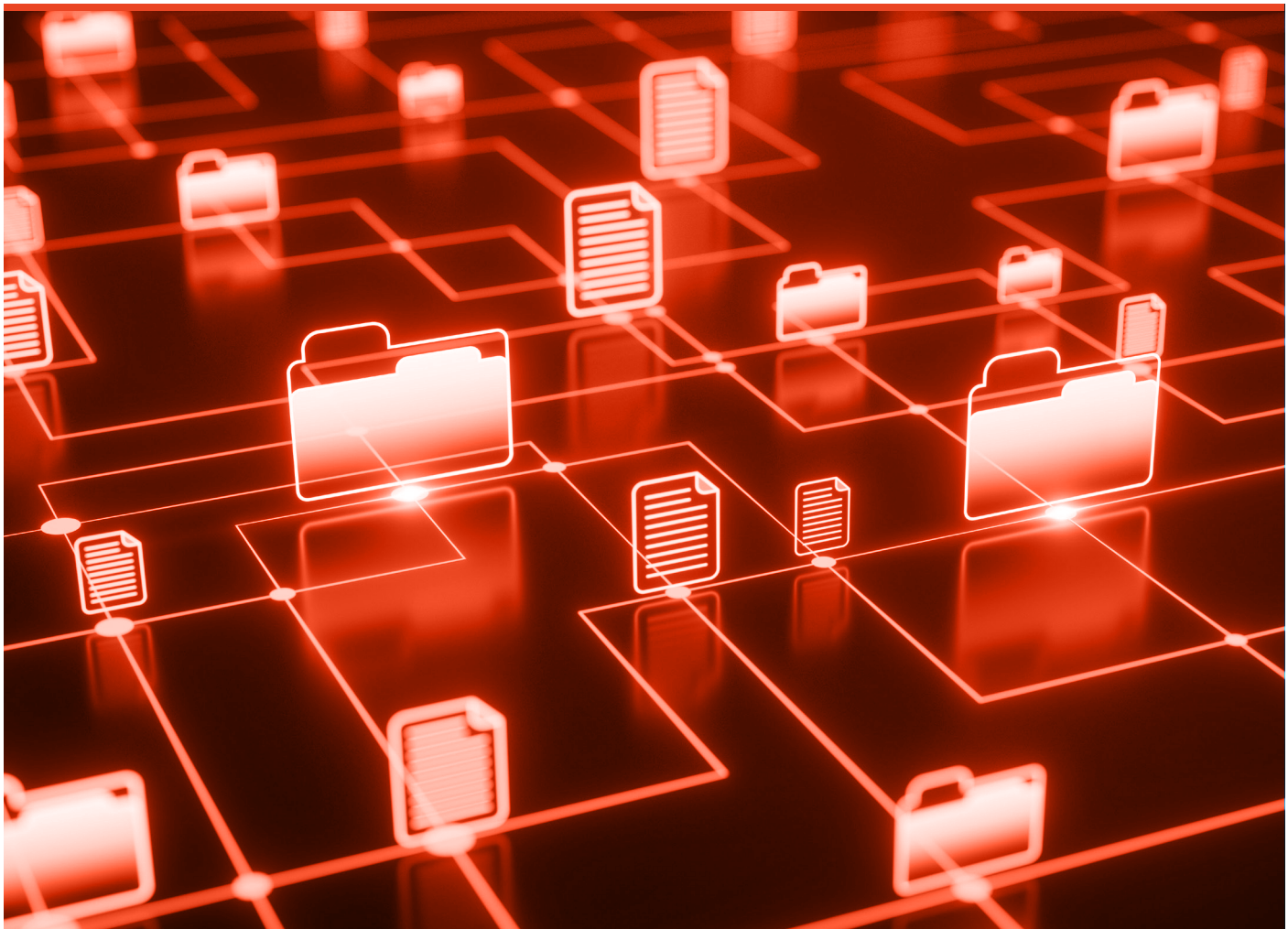


Figure 14: *IncRansom ransomware victims by month, H2 2025.*



#4 SINOBI

Sinobi, the Japanese term for ninja, are a new ransomware group having emerged in July 2025. The group have links with the Lynx and IncRansom operations. These links stem from when the IncRansom source code was offered for sale on a hacking forum and similarities in their extortion site. It is therefore difficult to ascertain whether the group is a rebrand, successor or brand new operation from Lynx.

The group operate a hybrid RaaS, whereby there are core members to the operation but also vetted affiliates. The group offer and utilize the double extortion tactic. Access to victims is achieved via multiple methods including the purchasing of access via Initial Access Brokers, the obtaining of breached credentials, or the exploitation of vulnerabilities in software.

An actor (Minako) on a hacking forum (DarkForums) posted messages offering the sale of unauthorized access to two companies: Roche (healthcare) & HMM (shipping) on 19 August 2025 and 20 August 2025. Although not confirmed as a member of Sinobi, the user utilises a profile image matching the Sinobi logo.

There is very little information relating to Sinobi across hacking forums, with the group preferring to keep themselves under the radar. Ransom notes indicate that the group is not politically motivated but are, like many ransomware groups, driven by financial motivations.

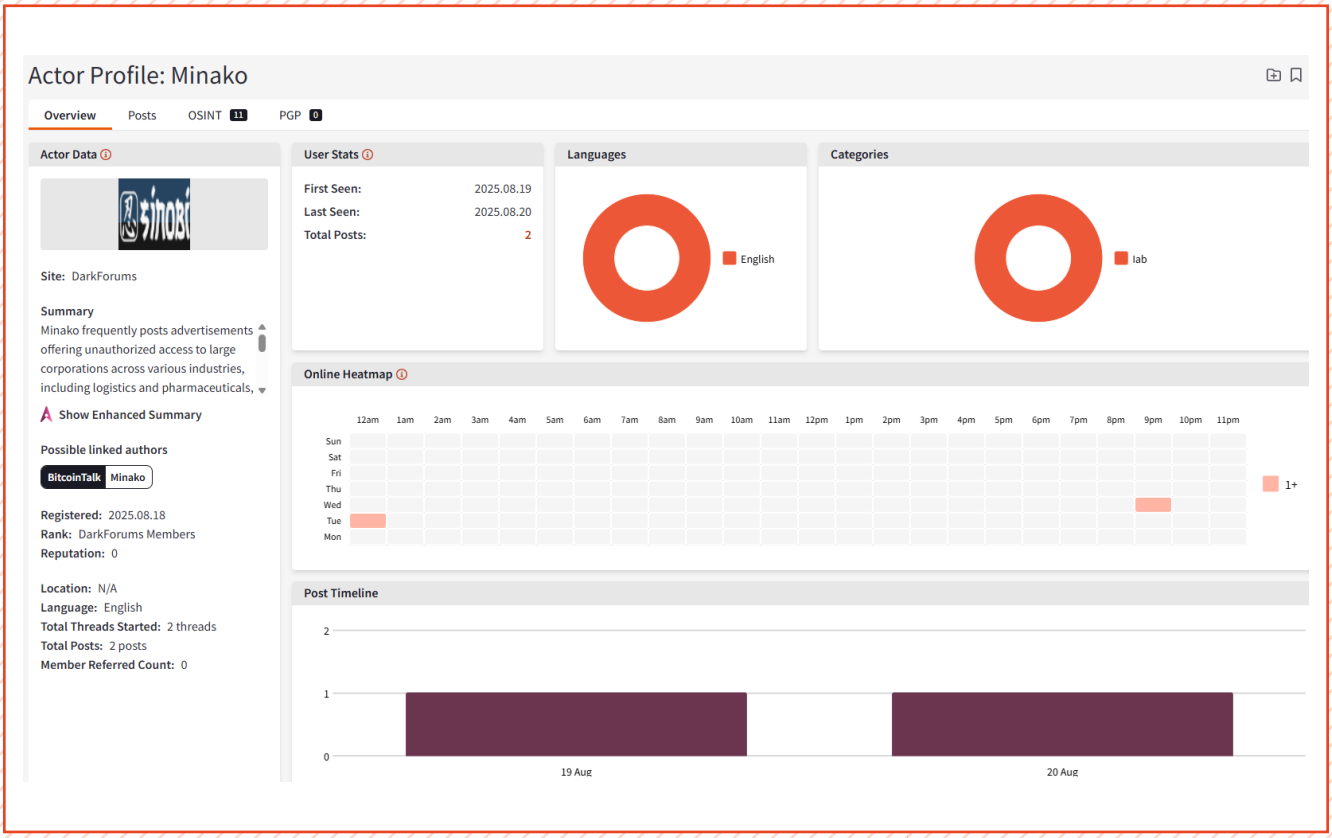


Figure 15: *Profile of suspected Sinobi-affiliated actor 'Minako' taken from Searchlight Cyber's Cerberus investigation platform.*

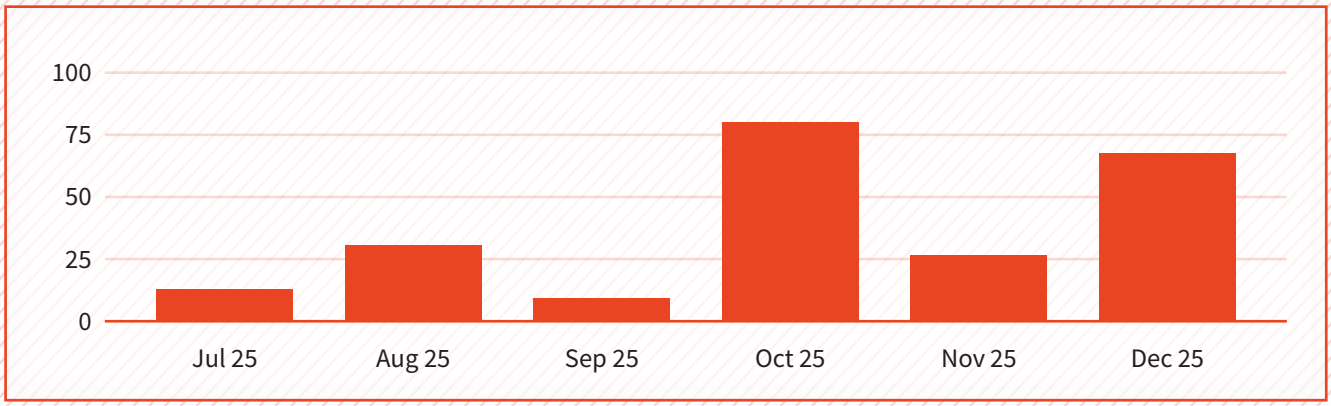


Figure 16: *Sinobi victims per month, H2 2025.*

#5 PLAY

The Play ransomware group have been active since late 2022 and claimed over 1100 victims via their dark web leak site, with about 225 victims being posted in 2025 alone. What sets Play apart from other groups is that they don't use a RaaS business model, they are a closed group and are not actively recruiting new members.

The group is known to obtain compromised credentials from stealer logs, use VPN and RDP services for initial access, exploit technical vulnerabilities and use information stealer malware such as Grixba, which is a custom-developed tool with additional features which has the ability to scan for and enumerate software and services on a network and exports the findings back to the user. The group also uses another custom-developed tool to copy volume shadow copies.

Besides custom tools, the group also utilizes software seen with other ransomware gangs, such as Cobalt Strike and SystemBC for command and control, PsExec for lateral movement, Mimikatz to dump credentials and Windows Privilege Escalation Awesome Scripts (WinPEAS) to enumerate vulnerabilities. Executables are distributed via Group Policy Objects.

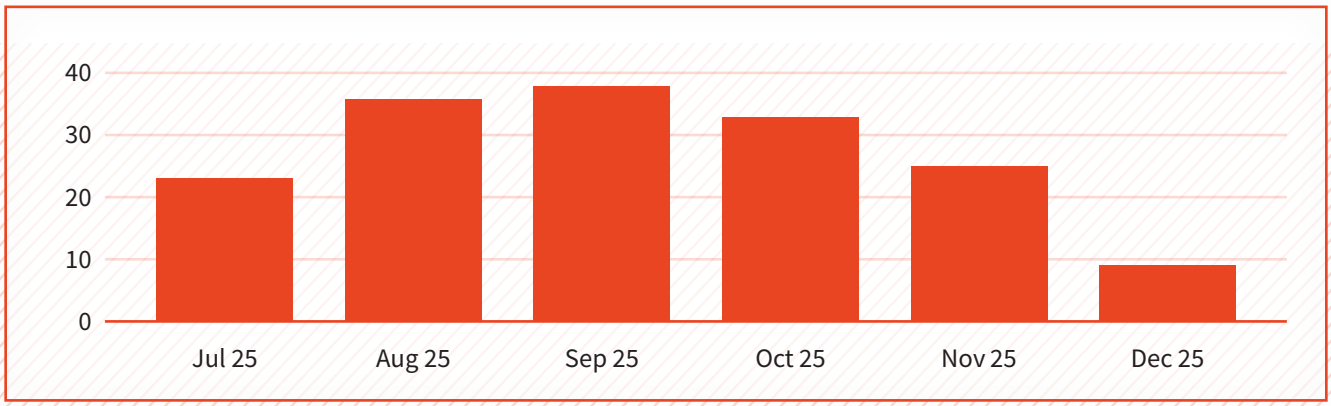


Figure 17: *Play victims per month, H2 2025.*

HOW THE MOST PROLIFIC RANSOMWARE GROUPS SAW SUCCESS IN H2

Evolution of Extortion: Beyond Traditional Encryption

Double and triple extortion remain the driving force behind the operations of the top 5, and the majority of successful ransomware groups. Some attacks bypass traditional ransomware encryption altogether, continuing to lower the barrier of entry for those without the skillset. Ransomware groups will do whatever is necessary to get a payment, and this most often involves the theft of sensitive data to pile the pressure on. In cases of triple extortion, groups employ other methods of disruption and causing operational downtime, such as Qilin's DDoS offering.

The Professionalization of RaaS

RaaS models continued to lead the way, operated by the top three groups in H2 and all five when looking across the full year of 2025. However, following the disruption of LockBit and the exposure of previous models as fraught with distrust, infighting and vulnerability to law enforcement, the top groups we track have taken a more controlled and professionalized approach. Groups like Qilin demonstrated a selective and stable affiliate ecosystem with centralized oversight and well-resourced affiliates, driving its continued victim growth.

Playing the Numbers Game: Why Every Organization is a Target

One of the main takeaways from the tactics employed by the most prolific ransomware groups, is the victimology. Victims continue to be sporadic, geographically diverse, and comprise both large multinationals and small businesses. We are not seeing any indication of 'Big Game Hunting', meaning that in theory, any and all organizations are a target. Ransomware groups are playing a numbers game at scale, automatically scanning for vulnerabilities in third party software and using AI to speed up their processes, weeding out the weakest defences.

LAW ENFORCEMENT OPERATIONS

On 24 July 25, Law enforcement conducted an operation against the BlackSuit (Royal) ransomware group. The dark web extortion site was seized along with associated infrastructure.

Figure 18: *BlackSuit seizure banner.*

On 10 September 25 a new ransomware group called Radar emerged. The group is a rebranded Dispossesor. Dispossessor first appeared in April 2024 before a Law Enforcement operation was conducted in August 2024 resulting in the seizure of their dark web extortion sites and associated infrastructure.

Figure 19: *Disposessor seizure banner.*

Although the number of ransomware groups and victims is growing year-on-year, increased law enforcement operations continue to disrupt. The rebranding of ransomware groups and shift of resources could be an indication that actors feel the pressure of law enforcement operations and are consistently attempting to muddy attribution and adapt to the changing landscape.

Law enforcement operations are vital to continue piling the pressure on the ransomware ecosystem. Consistent disruption leaves criminals on the back foot and has contributed positively to the fragmentation of some of the most dangerous operations we've analyzed previously (e.g. LockBit). This underscores the critical importance of closely monitoring the ransomware landscape through dark web investigation tools which assist law enforcement in gathering information to produce intelligence, connecting aliases and breaking the perceived anonymity that ransomware groups believe they have.

However, our findings from 2025, characterized by record highs across active groups, new groups, and victim numbers, show that offensive operations alone cannot eradicate the threat on the scale required to shift the overall balance of power. With so many new groups appearing, the threat of repercussions has not served as a particularly strong deterrent.

As an organization, the way to win the ransomware game is by not playing. With clear and relevant visibility into attacker behavior, security weaknesses and the early warning signs of an attack, more targets can avoid becoming the next victim.

EMERGENCE OF A 'SUPERGROUP'

Within the cyber threat ecosystem, partnerships are often formed by different threat groups. These groups might share a common ideological agenda, or seek to combine their specialized skills to achieve mutually beneficial outcomes.

This phenomenon can be seen in the ransomware landscape with the rise of 'supergroups', where previously small and relatively insignificant players have rapidly become a dominant threat through collaboration and the development of an efficient supply chain.

2025 saw the combination of three highly notorious and previously independent entities: Scattered Spider, LAPSUS$ and ShinyHunters. The merger of operations, resources and expertise resulted in the formation of the group "Scattered LAPSUS$ Hunters".

The combination of the three groups allow the unified group to exploit each other's strengths:

SCATTERED SPIDER

Scattered Spider's historical strength lies in its exploitation of initial access vectors, often through highly effective and personalized social engineering campaigns and SIM swapping. This group is instrumental in conducting social engineering and initial access, bypassing perimeter defenses and establishing a persistent foothold within target networks. Scattered Spider's origins started as one of many smaller ransomware affiliates for Ransomhub, formerly one of the most active RaaS groups we tracked before going offline in March 2025. Rather than remain a mere affiliate, Scattered Spider's strengths when paired with its fellow supergroup members rocketed it into the headlines with high profile attacks on a number of household name targets.

LAPSUS$

LAPSUS$ brings expertise in the acquisition of privileged credentials, often through engagements on underground markets. The group have conducted SIM-swapping, and other sophisticated techniques targeting identity and access management systems. Crucially, they also contribute the tactic of employing public pressure and leaks to coerce victims into compliance and expedite ransom payments.

SHINYHUNTERS

ShinyHunters is the specialized final phase operative, focusing on large-scale data exfiltration and the subsequent monetization of the stolen information. Their expertise ensures that whether or not the ransom is paid, the maximum financial value is extracted from the operation, either through private sales or distribution on dark web marketplaces.

Figure 20: *ShinyHunters leak site.*

This new supergroup operates extensively on Telegram and in 2025 produced their own ransomware extortion site with a Ransomware as a Service offering.

The fusion of the three groups helps indicate how groups grow in capability and can become bigger threats over time. This particular collaboration has proved effective; the group have been linked to or claimed responsibility for several breaches in H2 2025 against high profile global companies.

The emergence of Scattered Lapsus$ Hunters shows just how quickly the source and scale of the ransomware threat can change. While 2025 may have been the year of Scattered Spider, we expect the supergroup's development to continue in 2026 through its RaaS offering.

CAUSES OF A RANSOMWARE ATTACK AND WHAT CAN BE DONE

Fundamentally, a successful cyber attack; whether it culminates in data encryption for ransom or the theft of sensitive information for extortion, is a symptom of underlying security vulnerabilities and weaknesses. These can manifest in several critical areas:

INSIDER THREAT

Malicious actions or gross negligence by current or former employees, contractors, or trusted partners who have legitimate access to systems. This is often the most difficult vector to defend against, as it bypasses many perimeter security measures.

FAILURE OF PROCESS

Gaps in the security framework, such as inadequate patching cycles, missing multi-factor authentication (MFA) enforcement on critical services, poor log management, or a lack of employee security awareness training. This category encompasses operational shortcomings rather than technical flaws alone.

BREACH OF CREDENTIALS

The compromise of legitimate user accounts through phishing, brute-force attacks, or credential stuffing using previously leaked data. Once valid credentials are obtained, attackers can move laterally within the network, escalating privileges to reach high-value assets.

TECHNICAL EXPLOITS

The utilization of software flaws, including the exploitation of zero-days or, more commonly, known vulnerabilities for which a patch exists but has not been applied by the target organization. These exploits can provide the initial foothold necessary for reconnaissance and eventual payload delivery.

EXPLOITATION OF INITIAL ACCESS BROKERS (IABS)

The purchase of pre-vetted, confirmed access to a target organization's network from certain actors. This significantly reduces the time and effort required for the ransomware group to launch its attack, often leveraging remote desktop protocol (RDP) vulnerabilities, compromised virtual private network (VPN) accounts, or unpatched internet-facing servers.

GROWING ATTACK SURFACES:
TACKLING SHADOW EXPOSURE

Shadow exposure refers to the hidden, unmanaged, or poorly understood security risks inherent in authorized third-party software and enterprise systems. Unlike traditional vulnerabilities that might be identified through a simple patch management list, shadow exposure exists in the blind spots of widely deployed software, VPN appliances, ITSM platforms, and network management tools that organizations trust and rely on for daily operations.

It is "shadow" not because the software is unknown to the organization, but because the true extent of the software's attack surface and exploitability is hidden from the security team. These exposures often manifest as vulnerabilities or architectural flaws that allow attackers to bypass security perimeters entirely.

The well-understood concept of 'Shadow IT' is all about visibility of assets themselves; unknown or unauthorized hardware and software, such as a marketing team spinning up an unmanaged cloud server or an employee connecting an IoT device. The primary challenge here is discovery: you can't protect what you don't know exists.

But the real issue we see is a lack of visibility of exposures affecting authorized assets. These are the software and systems that are officially procured, vetted, and often cost millions of dollars. Therefore it's easy to be lulled into a false sense of security. The risk isn't that the asset is "unknown," but that the vendor's security posture is opaque. Despite undergoing RFPs and SOC2 audits, these "known" systems often harbor critical zero-day vulnerabilities or undocumented entry points that security teams assume are safe because they are "Enterprise Grade".

Many prolific Ransomware actors have compromised victims through the exploitation of fresh and novel vulnerabilities in enterprise software. And the scary part is just how fast they are able to jump on these opportunities. Shadow exposure is the door unwittingly left open that facilitates this.

Attackers target high-value, third-party software because they know organizations grant these systems deep internal access. The issue remains that too many organizations rely on reactive patching, and this cannot keep up with exploitation involving vulnerabilities that haven't been publicly disclosed yet (zero-days) or issues in systems where the vendor is opaque about the risks.

"

ATTACKERS TARGET HIGH-VALUE, THIRD-PARTY SOFTWARE BECAUSE THEY KNOW ORGANIZATIONS GRANT THESE SYSTEMS DEEP INTERNAL ACCESS.

Because these systems are often pre-authentication points, an attacker can gain a foothold in the internal network without needing a single set of stolen credentials.

To defend against this initial access that facilitates ransomware, organizations must move beyond static security visibility and reactive scanning. Addressing shadow exposure through Attack Surface Management (ASM) is vital for several reasons:

- **Continuous Discovery & Enrichment:**
  ASM tools identify every point of presence a piece of software has on the internet, ensuring that security teams understand exactly where their exposures lie in real-time.
- **Proactive Research vs. Reactive Patching:**
  Effective ASM incorporates offensive security research to identify high-signal exposures. This allows organizations to mitigate risks before a vendor release or a public exploit becomes available.
- **Challenging Vendor Opacity:**
  By monitoring the actual attack surface rather than relying on a vendor's self-attestation, organizations gain an objective view of their most critical exposures.

To adequately defend themselves, organizations must adopt an attacker's eye view through Attack Surface Management, identifying and closing these hidden doors before they are exploited.

EXPLOITED VULNERABILITIES

Despite the continued focus of many ransomware groups on gaining initial access through social engineering and insider threats, advanced ransomware operations are stepping up their exploitation of novel and existing, unpatched vulnerabilities in third-party software as a direct route into victim organizations. Looking at the cybercrime landscape as a whole, vulnerability exploitation was up 34 percent in 2025 (Verizon)[2].

The following table details the CVEs that were added to the Known Exploited Vulnerabilities (KEV Catalog in the second half of 2025, along with any known ransomware groups that exploited the vulnerability.

SERIAL	CVE	PRODUCT	RANSOMWARE GROUP
1	CVE-2025-5777	FORTINET FORTIOS	UNKNOWN
2	CVE-2025-53770	CITRIX NETSCALER ADC AND GATEWAY	WARLOCK / LOCKBIT
3	CVE-2025-49706	MICROSOFT SHAREPOINT	WARLOCK / LOCKBIT
4	CVE-2025-49704	MICROSOFT SHAREPOINT	WARLOCK / LOCKBIT
5	CVE-2025-10035	FORTRA GOANYWHERE MFT	MEDUSA RANSOMWARE
6	CVE-2025-61882	ORACLE E-BUSINESS SUITE	UNKNOWN
7	CVE-2025-61884	ORACLE E-BUSINESS SUITE	CLOP
8	CVE-2025-55182	META REACT SERVER COMPONENTS	UNKNOWN

Figure 21: *Known Exploited Vulnerabilities.*

As outlined, ransomware groups may find and exploit these vulnerabilities themselves, or increasingly utilize the Initial Access Broker (IAB) market to obtain access. What is most alarming is how fast vulnerabilities are being exploited by malicious actors. In 2025, nearly 30 percent of known exploited vulnerabilities[3] were exploited before being publicly disclosed, or on the day they were reported. When organizations are in a race with ransomware groups that could be won or lost within hours, the importance of continuous threat exposure management within a preemptive security posture could not be higher.

[2] https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf
[3] https://www.infosecurity-magazine.com/news/zeroday-exploits-surge-vulncheck/

WHAT CAN BE DONE

Searchlight Cyber has consistently emphasized that reducing the likelihood of a ransomware attack hinges on identifying indicators and warnings, as documented in this and previous reports.

COMBATING INITIAL ACCESS BROKERS

Initial Access Brokers (IABs) are one of the most common threats to organizations that we observe on the dark web. They are cybercriminals that specialize in breaking into networks and establishing a foothold. They then sell this foothold, or "access", onto other cybercriminals, often ransomware groups, to exploit.

This makes them a critical part of the cybercriminal ecosystem, with ransomware operators routinely using IABs so they don't have to go through the effort of breaking into the network themselves.

In order for this ecosystem to function there has to be a point of exchange – and that takes place on dark web forums such as Exploit and XSS. Here, IABs sell or auction their exploits to ransomware groups and the wider cybercriminal community.

While these incidents should set alarm bells ringing, IAB posts advertising access provide a crucial opportunity for security teams to spot the early warning signs of attack because it is a point when the cybercriminals are exposed – forced to give away key information about their targets, their tactics, and even their identities.

"IAB POSTS ADVERTISING ACCESS PROVIDE A CRUCIAL OPPORTUNITY FOR SECURITY TEAMS TO SPOT THE EARLY WARNING SIGNS OF ATTACK BECAUSE IT IS A POINT WHEN THE CYBERCRIMINALS ARE EXPOSED - FORCED TO GIVE AWAY KEY INFORMATION ABOUT THEIR TARGETS, THEIR TACTICS, AND EVEN THEIR IDENTITIES.

NEW TOOLS FOR INVESTIGATORS: INITIAL ACCESS BROKER DASHBOARD

Recognizing the scale of this challenge for defenders, Searchlight Cyber has added a new Initial Access Broker (IAB) Dashboard to our investigation platform, Cerberus.

This new dashboard makes it possible for analysts to detect threats operating in the Initial Access (TA0001) tactic in the MITRE ATT&CK framework – enabling faster identification of unauthorized network access before it can be sold and exploited.

INDEXED VIEW OF INITIAL ACCESS BROKER POSTS

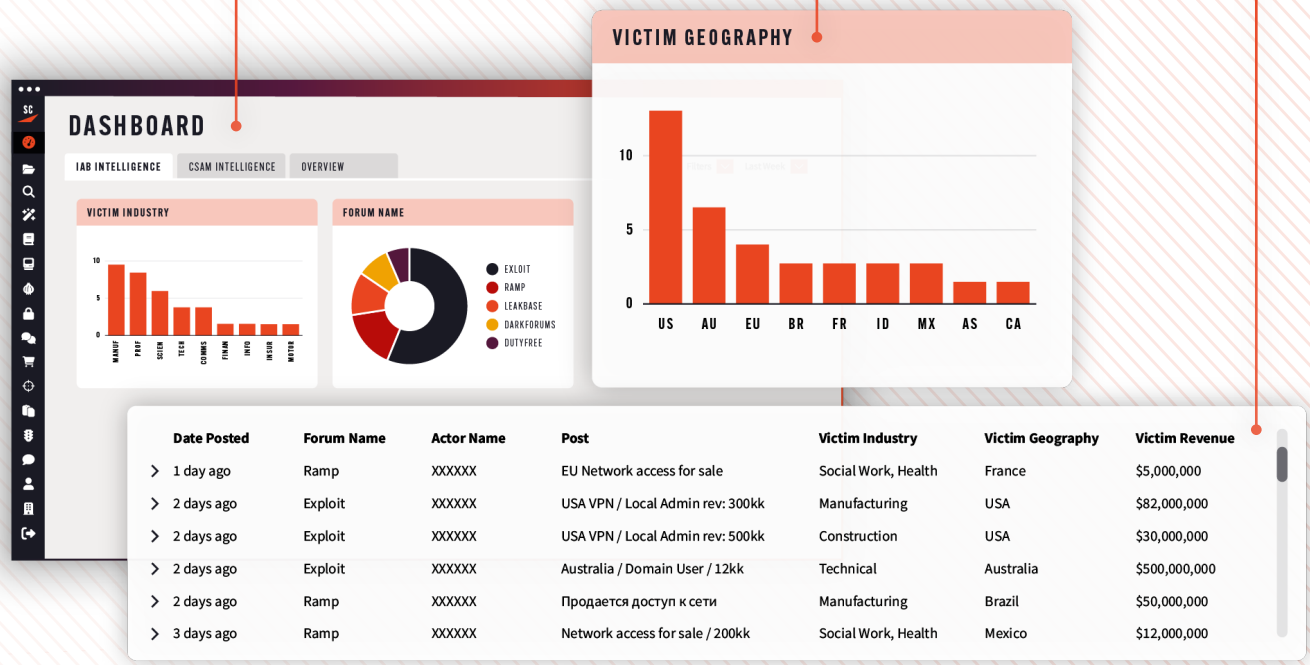
Searchlight's AI Agent automatically identifies IAB posts on dark web forums and collates these into a single dashboard.

FILTER BY SECTOR, GEOGRAPHY, AND REVENUE

Analysts can apply filters and set alerts to surface posts matching their company's description.

VIEW AND PIVOT ON ANY POST AND ACTOR

Quickly determine whether the threat is genuine and gather more information on the nature of the threat, based on the broker's captured past activity.



Date Posted	Forum Name	Actor Name	Post	Victim Industry	Victim Geography	Victim Revenue
1 day ago	Ramp	XXXXXX	EU Network access for sale	Social Work, Health	France	$5,000,000
2 days ago	Exploit	XXXXXX	USA VPN / Local Admin rev: 300kk	Manufacturing	USA	$82,000,000
2 days ago	Exploit	XXXXXX	USA VPN / Local Admin rev: 500kk	Construction	USA	$30,000,000
2 days ago	Exploit	XXXXXX	Australia / Domain User / 12kk	Technical	Australia	$500,000,000
2 days ago	Ramp	XXXXXX	Продается доступ к сети	Manufacturing	Brazil	$50,000,000
3 days ago	Ramp	XXXXXX	Network access for sale / 200kk	Social Work, Health	Mexico	$12,000,000

Preemptive approach to ransomware: Success stories

In the short time since its launch, Searchlight users have successfully identified IAB listings offering access to high-value internal assets, including VPN access and SQL databases. Critically, these findings were made before the access or compromise was publicly disclosed to the impacted victims, such as a global restaurant chain and a national governing body.

AVOID THE RANSOMWARE BLAST RADIUS - VISIBILITY INTO LEAKED DATA

The vast majority of ransomware analysis focuses on the primary victims of ransomware attacks, but for each of the 7,458 primary victims in 2025 there is a frequently unknown but expansive blast radius of impact, implicating countless more organizations. Ransomware leak sites, which we monitor as part of the research for this report, serve as a public-facing site where ransomware groups publish sensitive data stolen from compromised organizations, aiming to amplify the psychological and reputational pressure on victims, thereby increasing the likelihood of a ransom payment. Due to the increasingly interconnected business landscape, these leaks inadvertantly reveal details about third party organizations within the primary victim's supply chain.

According to the National Bureau of Economic Research,[4] only 10.5 percent of worldwide ransomware incidents are disclosed by victims, notifying their suppliers and connected third parties, meaning most organizations never learn when their sensitive files are circulating on ransomware leak sites.

This lack of visibility can leave enterprises and public sector organizations vulnerable to a multitude of risks, from the exposure of sensitive intellectual property and trade secrets to a heightened risk of phishing and knock-on ransomware attacks.

Within this leaked data lies an opportunity for early preemptive action. If a victim's data includes information pertaining to their partners, suppliers, or clients, it can alert those entities to potential compromise, even if they were not the primary target of the initial ransomware attack. This proactive monitoring enables affected third parties to initiate their own incident response protocols, mitigating potential downstream damage.

However, despite the fact that this leaked data is publicly accessible, obtaining and processing the file-tree structures and data behind them is technical, time consuming and can bring with it operational risk. The key to taking a preemptive approach is to be able to quickly identify if your organization's data has been compromised as part of an attack, and what has been compromised, before it is used against you.

NEW TOOLS FOR INVESTIGATORS: RANSOMWARE FILE EXPLORER

To help organizations get ahead of the blast radius resulting from undisclosed ransomware attacks, Searchlight Cyber recently launched the Ransomware File Explorer in our investigation platform, Cerberus.

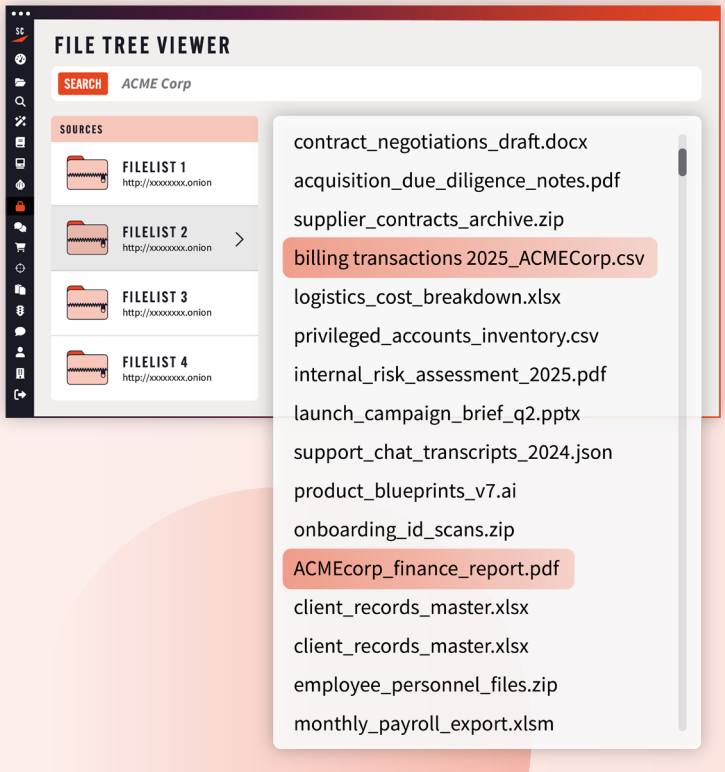
Although leak data is publicly accessible, obtaining and processing the file-tree structures and data behind them is highly time-consuming. Searchlight automatically gathers and indexes this information, making it searchable forever – even if the file-tree is later deleted from the dark web.

This addresses the exfiltration tactics (TA0010) in the MITRE ATT&CK Framework.

Preemptively detect leaked PII & intellectual property
Search for keywords relating to your business to accelerate incident response, even when your organization is not the primary victim.

Set alerts for keywords found in file names
Get notified when sensitive documents, files, and intellectual property belonging to your organization have been leaked in third-party breaches.

Prevent operational, legal, or reputational damage
Mitigate any risk associated with breached sensitive content and help prevent future ransomware attacks against your own business.



Preemptive approach to ransomware: Success stories

Although this feature has only just been added to Searchlight, during testing, our Threat Intelligence team was able to use the module to identify a database containing over 300GB of personal data records belonging to a major sportswear manufacturer, and preemptively alert them to this potential breach.

FORECAST: RANSOMWARE DEVELOPMENTS IN 2026

At the time of writing this report reviewing H2 2025's developments in early 2026, it is clear to see the tactics and evolutions that will continue to define the ransomware landscape across the rest of the year.

The Evolution of Extortion

A major factor that made our top five ransomware groups so successful was their employment of double and triple extortion methods. Many industry data sources cite a significant reduction in ransom payment values, with more and more victims refusing to pay up. As organizations have bolstered their resilience through immutable backups and rapid recovery protocols, ransomware groups have pivoted away from traditional malware encryption and will try multiple different methods to get their payday. As such, we have seen a surge in data-theft-only incidents, and multiple angles of attack including auctioning off data, DDoS, harassment of third-parties and customers, and even physical intimidation.

This shift renders traditional defenses and recovery plans insufficient. If a group is already inside your network exfiltrating data, the damage is done. In 2026, the only way to properly defend against ransomware is through preemptive action.

The Shifting Underground Economy

The underground economy is also changing in response to intensified law enforcement pressure. The high-profile disruption of legacy forums like XSS, BreachForums, and now RAMP at the time of writing has an important impact, affecting the trust ransomware groups place in these platforms. This shifting operational environment does however make things more challenging for threat intelligence teams.

Monitoring ransomware group communications means staying on top of the sources they are operating in, and we may see ransomware group communications go even darker than before.

Sophisticated actors are also moving toward closed, highly vetted RaaS models. Newly branded groups such as Sinobi have moved away from loud, public recruitment on common forums in favor of private, invitation-only Telegram channels and encrypted relays. RaaS developers are becoming more selective with their affiliates, prioritizing quality and reliability, reducing the number of liabilities in their operation.

The New Defensive Paradigm

Despite these shifts in tactics keeping defenders on their toes, the one thing that remains grimly predictable is that ransomware victim numbers will continue to rise. This has been the trend over the past three years and our data shows that the rate of increase is also rising. Ransomware groups are able to operate sophisticated operations at scale, against victims big and small, and across a varied geographical footprint. No organization is too small or too niche to be a target.

The takeaway for 2026 is that visibility and preemptive action is the key to modern ransomware defense. Relying on reactive security and hoping for the best is a losing strategy in the age of triple extortion, rapid zero-day exploitation and AI-powered social engineering. Success now requires a continuous view of your attack surface and the intelligence-driven capability to identify and neutralize threats in their earliest stages.

“

SUCCESS NOW REQUIRES A CONTINUOUS VIEW OF YOUR ATTACK SURFACE AND THE INTELLIGENCE-DRIVEN CAPABILITY TO IDENTIFY AND NEUTRALIZE THREATS IN THEIR EARLIEST STAGES

SEARCHLIGHT CYBER

VISIT **WWW.SLCYBER.IO** TO FIND OUT MORE OR BOOK A DEMO NOW.

UK HEADQUARTERS
Suite 63, Pure Offices,
1 Port Way, Port Solent,
Portsmouth PO6 4TY
United Kingdom

US HEADQUARTERS
44 Merrimac Street,
Newburyport,
MA 01950
United States