



Ransomware and Cyber Threat Insights

A GRIT® Report

Q3 2025
July-September 2025

Contents



Methodology



Quarterly Ransomware Summary



Threat Actor Trends



Threat Actor Spotlight: SafePay
and Rhysida



Industry Spotlight: Healthcare



Other Reporting and Events



RaaS Lifecycle Case Study:
from BlackLock to Global



Quarterly Wrap Up



Methodology

Data collected for this report was obtained from publicly available resources, including threat groups themselves, and has not been validated by alleged victims. Collected data is reviewed for potential duplications or inaccuracies and adjusted accordingly. Thus, the number of publicly observed attacks and the actual number of attacks conducted may not be equal. Some groups do not publicize all their victims, and almost all groups offer an option to withhold announcement if the victim pays a ransom within a specified timeframe and/or remove the victims once a ransom has been paid. Additionally, some groups include incomplete information about their victim or claim an attack despite successfully attacking only a small subset of their target. For these reasons, the data in this report is useful in aggregate, but should be evaluated as a report consisting of data sources that have variability. Despite the variability, this report is still an accurate representation of the total ransomware threat landscape.

We note that this report includes 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 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 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. While these actors and venues doubtless have impacts, we distinguish them from financially-motivated cybercrime and data extortion, which is the primary focus of this report. For this reason, our data may periodically reflect lower total numbers of incidents than other, similar public reports.

Quarterly Ransomware Summary

The third quarter (Q3) of 2025 continued what we had initially thought to be an anomaly in Q2 – an apparent “leveling off” or normalization of observed victim volume. After a spike from 1,577 observed victims in Q4 2024, to 2,063 in Q1 2025, we were surprised to see a reduction to 1,591 victims in Q2. However, the Q1 surge was likely driven by ransomware group Cl0p's mass exploitation campaigns. Once removed from the picture, we instead see something more interesting; an emerging consistent average of approximately 1,500-1,600 observed victims each quarter from Q4 2024 to Q3 2025. After years of high-speed growth, this current normalization is a welcome reprieve.

	Q3 2025	Q2 2025	Q1 2025 (excluding Cl0p)	Q4 2024
Total Publicly Posted Ransomware Victims	1,576	1,591	1,715	1,577

While total victim volume has normalized, the diversity of named extortion groups continues to grow, reaching another all-time high of 77 active groups in Q3. This represents an 8% increase quarter-over-quarter (QoQ), and a 57% year-over-year (YoY) increase. The plateauing victim count, despite continued growth in named groups, may seem counterintuitive, but we assess several possible explanations:

- The total number of ransomware operators remains constant, but operators are increasingly spread across a greater number of groups
- Many named groups are lower skill or ephemeral in nature, contributing a negligible number of total victims by our observations
- Several named ransomware groups are overlapping, with certain victims or victim types reserved for certain groups. For example, sensitive victims such as healthcare organizations are observed more frequently by some groups than others. A ransomware group could reserve posting such victims to a secondary group to keep the reputation or signature of the primary group “clean”

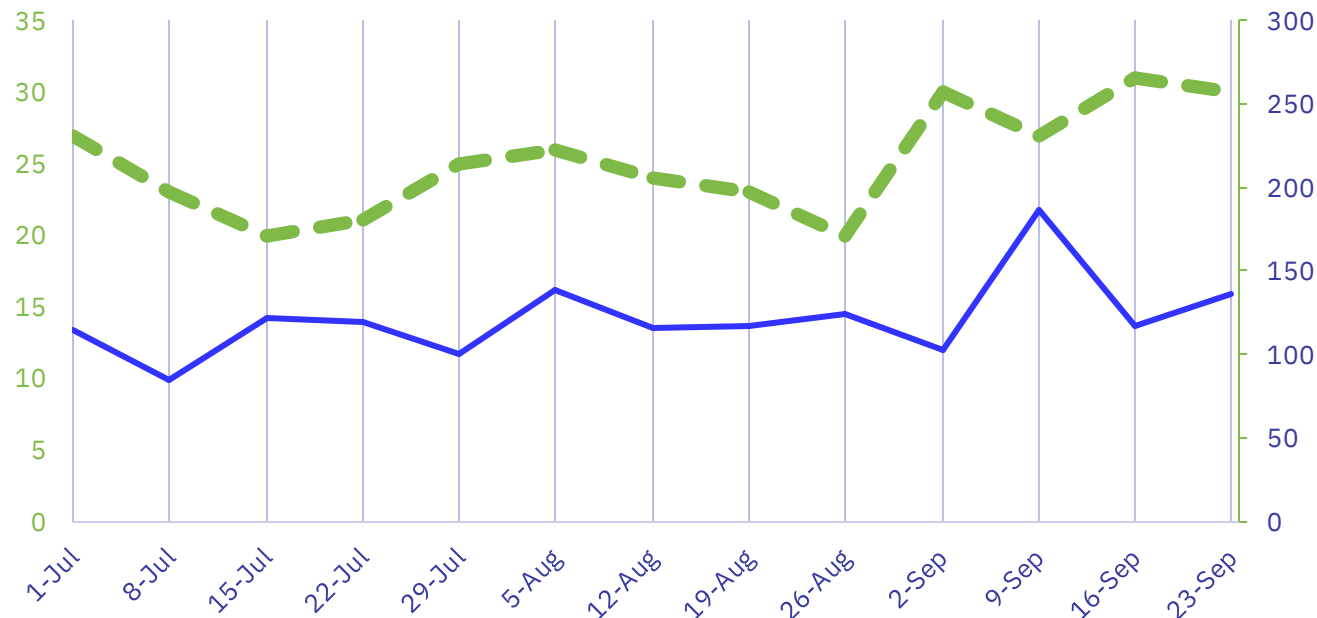
Q3 trends in terms of impacted countries and industries are within historical norms, and the bulk of victims remain attributed to the most prolific, established RaaS groups including Qilin, Akira, Inc., and Play. Notably, several established groups increased their total victim volume, while overall victims remained stagnant. This potentially signals greater consolidation among skilled affiliates.

In sum, Q3 solidifies what we are recognizing as a “new normal” baseline, but it is too soon to declare the problem of ransomware contained. Whether the months ahead will continue current trends, increase anew, or even decrease remains to be seen.

	Q3 2025	Q2 2025 (QoQ)	Q3 2024 (YoY)
Total Publicly Posted Ransomware Victims	1,576	1,591	1,048
Active Ransomware Groups	77	71	49
Average Daily Victims	17.1	17.5	11.4

Threat Actor Trends

Rate of Publicly Posted Ransomware Victims, Q3 2025



Calendar Weeks: July – September 2025

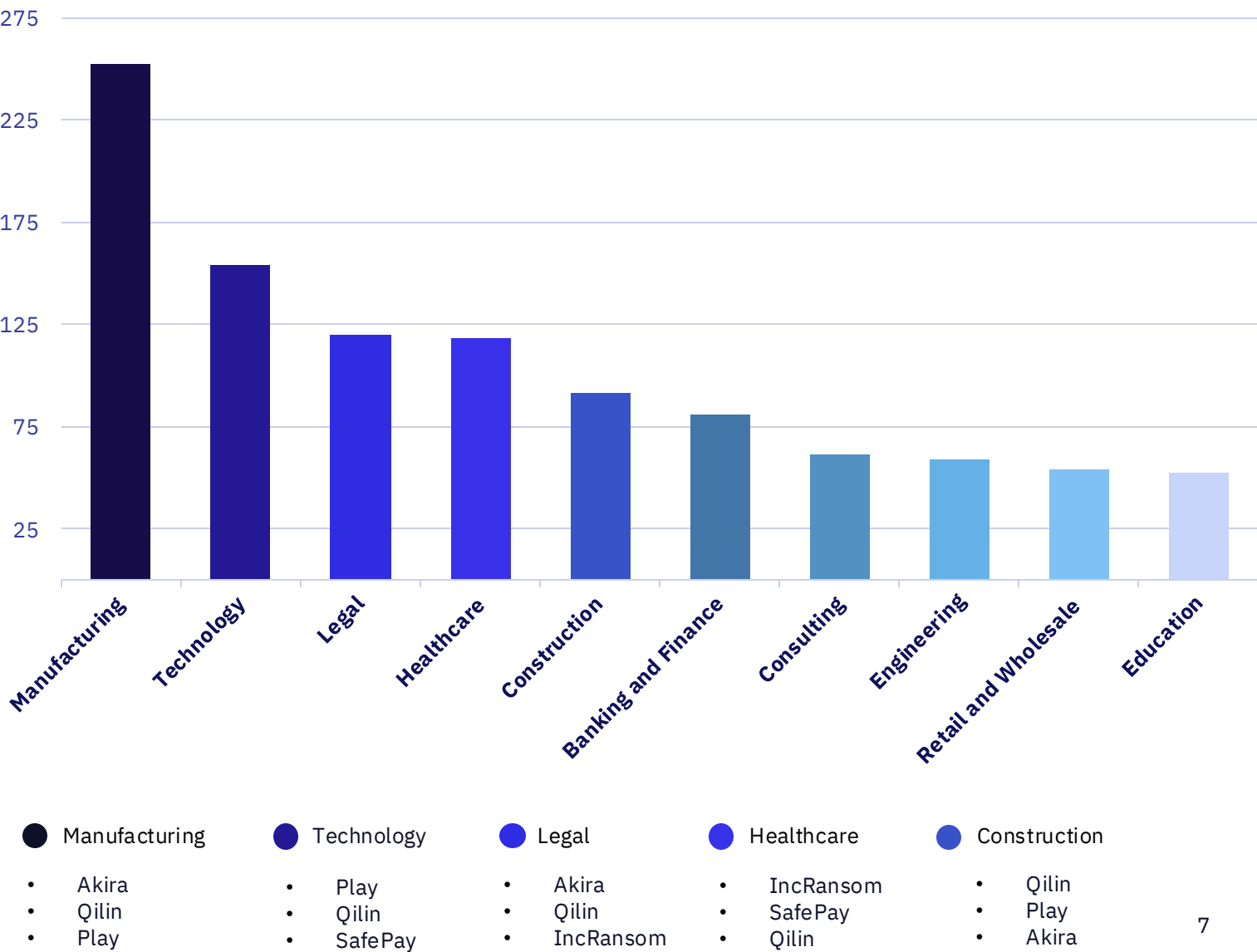
<div></div> Total Posts	<div></div> Total Groups	Average Posts per Week	Average Groups Posting per Week
1,576	77	121	25

Qilin had a record quarter with 234 victims, comprising 15% of the total count for Q3. They continue to lead the surge ahead of Akira, another major player in ransomware damage over the last two and a half years. While the major groups continue to elevate their game, we continue to observe new and emerging groups, contributing to the sustained wave of ransomware victims en masse.

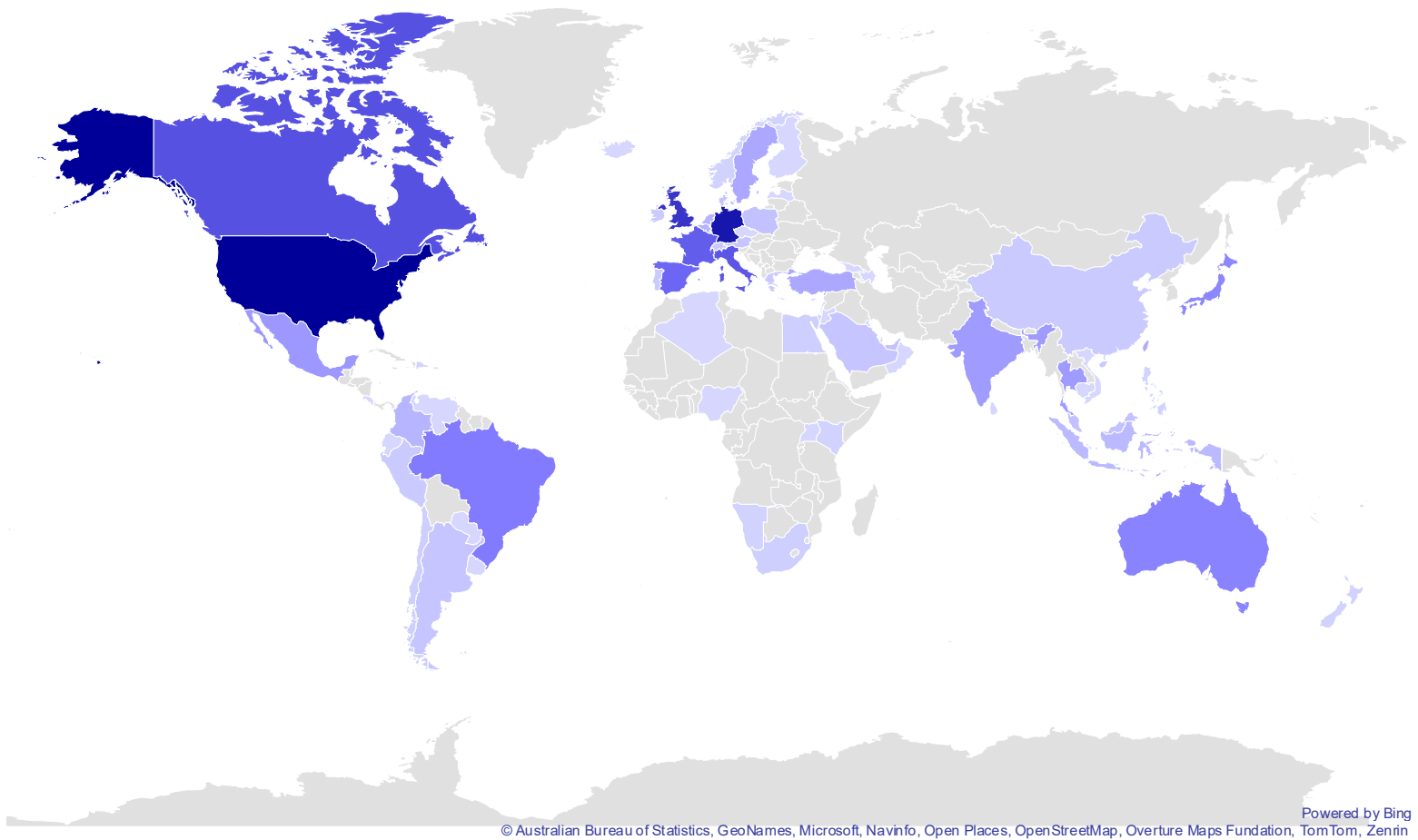
The victim count remained steady throughout the third quarter of 2025, with only one noticeable spike in mid-September. An emerging threat group dubbed as "The Gentlemen" posted 32 victims on a single day once their Data Leak Site (DLS) went live. The group went on to claim 38 total victims across the month of September, joining many other emerging groups that seemingly hit the ground running. As such, there is a slight increase in the number of active groups, which may also correlate to the end of month increase. GRIT continues to see new groups emerge with tactics like more established groups and taking a backlog of victim data with them. This activity could be indicative of splinter groups trying to evade the ever-evolving heat of law enforcement pressure.

Most Impacted Industries, Q3 2025

The "top 10" most impacted industries from ransomware attacks remained largely stagnant when compared to Q2 2025. The most notable change is Engineering and Education replacing Transportation and “Entertainment, Hospitality, and Tourism”. Manufacturing continues to be a mainstay as the most affected industry vertical by ransomware operations. Despite almost the same number of total victims, Q3 saw a 26% increase in manufacturing organizations suffering a ransomware attack, with 252 publicly claimed victims compared to Q2 2025 (200). Last quarter we noted that Akira, while being among the most active threat groups, appears to refrain from attacking Healthcare entities. Although Akira is among the "top 3" of ransomware outfits that impact victims within the Technology vertical, the group attacks victims within this industry at a much lower rate than their "peers."



Geographic Breakdown of Ransomware Victims, Q3 2025



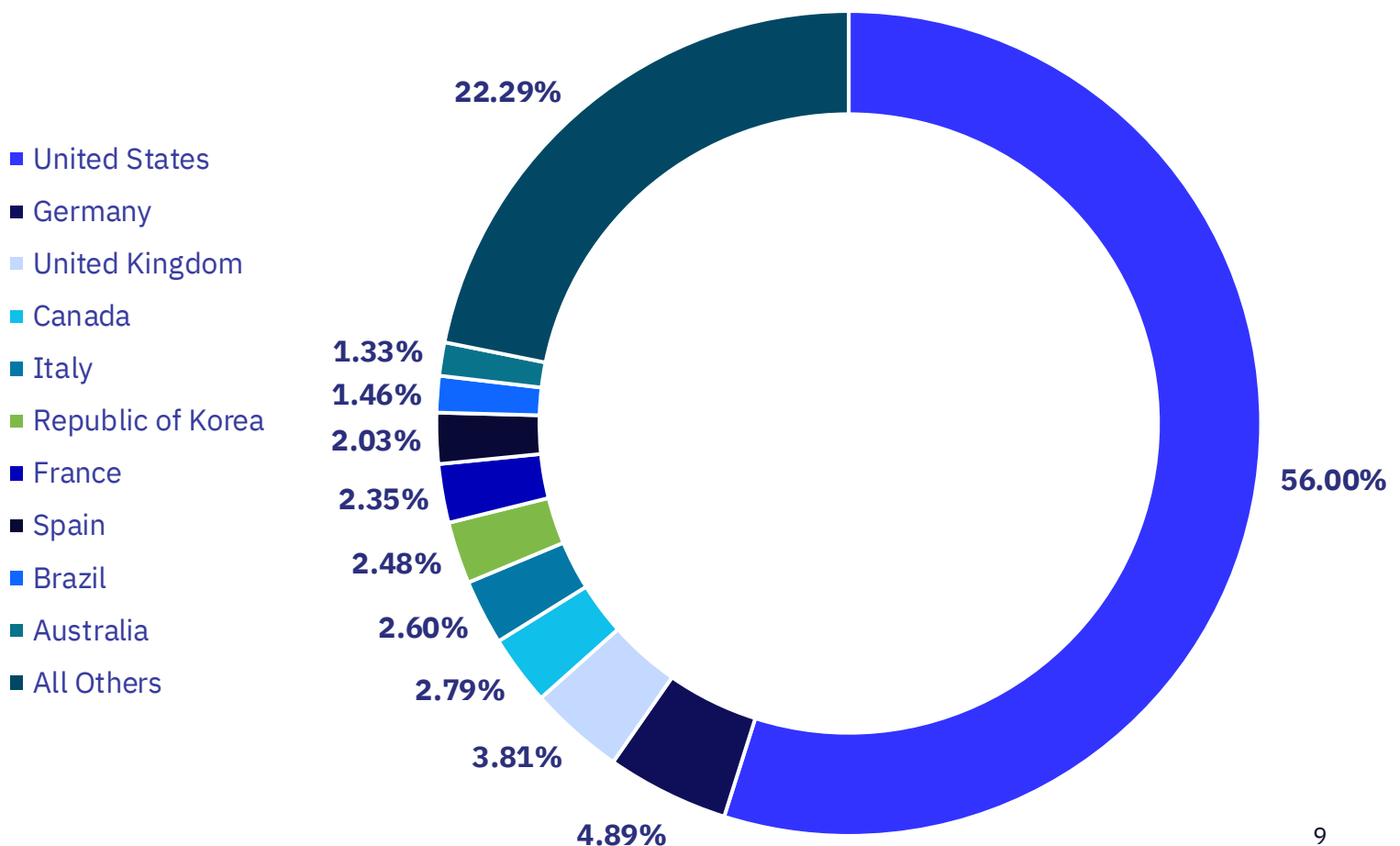
Top 10:

- | | |
|-------------------|----------------------|
| 1. United States | 6. Republic of Korea |
| 2. Germany | 7. France |
| 3. United Kingdom | 8. Spain |
| 4. Canada | 9. Brazil |
| 5. Italy | 10. Australia |

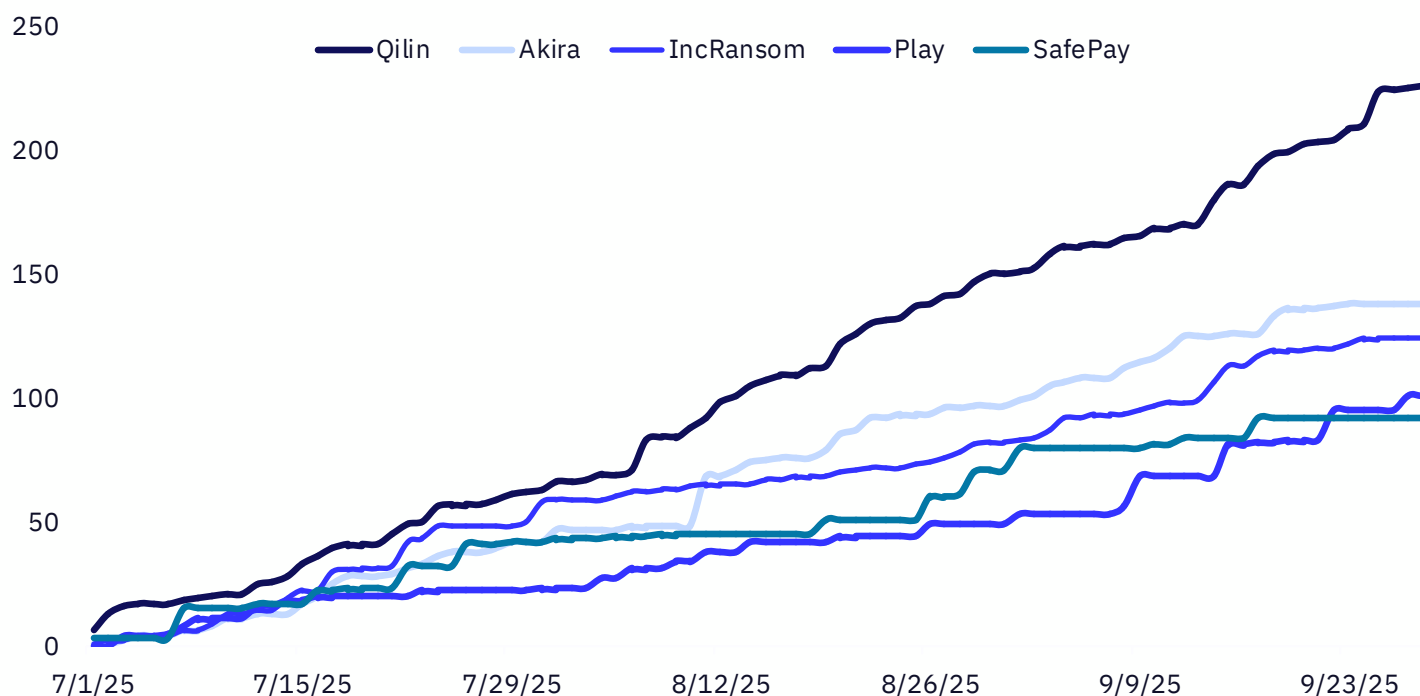
Ransomware Impacts by Country, Q3 2025

Just like Manufacturing in the industry section, the United States also remains the most impacted by ransomware attacks. The share of US victims in Q3 was 56%, an increase from 52.1% in the prior quarter. Canada, Germany, and the United Kingdom consistently remain within the "top 5" most impacted.

The Republic of Korea saw an increase in victimization throughout Q3 2025. This growth in attacks was fueled by what is seemingly a mid-September Qilin campaign targeting multiple Korean financial and accounting entities. In this campaign, Qilin claimed 29 financial victims headquartered in the Republic of Korea to their DLS. It is difficult to assess whether this swath of Korean victims is the catalyst for other threat groups expanding their targeting to claim more victims in East Asia, or if this spur of Korean victims is a "flash in the pan."



Cumulative Victims by Threat Group



Qilin

Qilin continued to be the most active ransomware outfit for the second quarter in a row. The group's victim count of 234 dwarfs all other group's activities. Despite an overall slight decrease in the total number of ransomware victims in Q3, Qilin managed to claim 9% more victims to their DLS. This activity also marks a 318% YoY increase in activity, compared to the 56 victims Qilin claimed during the same quarter in 2024.

Akira

Akira also demonstrated slight QoQ rise in activity, with 13% more victims in Q3 (150) than Q2 (133). Although not as dramatic as Qilin's YoY surge, Akira's victim count in Q3 is 212% higher than the same period in 2024 (48). Akira experienced a single day spike of 20 claimed victims on August 11th, which added significantly to their total victim count for the quarter.

IncRansom

IncRansom, first emerging in August 2023, remained what we consider the "middle class" of ransomware operations through most of their lifespan. While staying relatively "quiet" throughout Q1 and Q2, 2025, with only 71 and 62 victim claims each quarter, respectively, the group surged in activity during Q3. The group's Q3 126 victim count positions them as the third most active group for the quarter. It is unclear if IncRansom will be able to maintain this new, higher operational tempo, or if they will resume their previous level of operations through the end of the year.



Threat Actor Spotlight: SafePay and Rhysida

Threat Actor Spotlight: SafePay

SafePay is an insular ransomware group that first appeared in late 2024. Unlike bigger groups such as Qilin and Akira, SafePay does not operate as a Ransomware-as-a-Service (RaaS) group. Instead, it keeps its operational capabilities limited to a select group of insiders. SafePay has not historically advertised its services on forums commonly associated with ransomware advertisements. Despite its insular nature, SafePay has become a notable Developing group, with a prolific victim set spread across the world and across industry verticals.

In Q3 2025, the group impacted 71 victims across 19 industries and 16 countries. In contrast, in Q2 2025, SafePay impacted 111 victims spread across 27 industries and 18 countries. This is a 36% decrease in victim impact QoQ, but the group is still a top performer among tracked Developing groups. SafePay claims a year-to-date total impact of 258 victims across 29 distinct industries and 30 countries. Across the previous two quarters, the primary location of impacted victims is the United States, with Germany, the United Kingdom, Canada, and Mexico rounding out the top five.

As with many ransomware groups, SafePay posts its victims to its DLS on the dark web. Notably, the group has a banner across the top of its DLS indicating that it “has never provided and does not provide the RaaS”:

SafePay ransomware has never provided and does not provide the RaaS

Search the blog

Search

Threat Actor Spotlight: SafePay


This banner aligns with GRIT's observed behavior of the group, particularly their lack of advertisement on traditional community forums and more insular nature. This behavior notably helps isolate the group against traditional threats against operational security (OPSEC) and allows them to be selective in inducting new members. Additionally, a closed operation like SafePay may also benefit members from an earnings perspective. Specifically, not having to share a cut of their ransoms nets them a larger individual profit on each ransom, though the true nature of the profit-sharing is unknown.

Among the shifting power struggles in the ransomware ecosystem post-Lockbit and -ALPHV, SafePay remains a strong contender within the scene. Their insular nature and lack of advertisement helps keep SafePay out of the spotlight and out of the headlines. Given the breadth of their victim impacts across industries and verticals, barring law enforcement action or an unexpected dissolution of the group, we assess SafePay will continue to be a notable actor in the ransomware space.

Threat Actor Spotlight: Rhysida

Rhysida is an “Established” ransomware group that first appeared in June 2023. The group is significantly less active in comparison to other Established groups. At the time of this report, Rhysida has claimed over 200 victims to their dark web DLS. In comparison, Qilin, another Established group, surpassed this number of victims in Q3 2025 alone. Despite Rhysida's more limited activity, their victims typically fall within industry verticals that are historically considered more “sensitive” by other RaaS groups, such as Education, Healthcare, and Government. Some RaaS groups have previously applied prohibitions against targeting such organizations within their “affiliate rules”. LockBit, for example, “prohibited” attacks on critical infrastructure and medical institutions where “damage of files could lead to death.” This choice is likely not altruistic, but rather to avoid the law enforcement attention that attacks on those industries would attract.

Rhysida welcomes attention from media outlets and openly welcomes journalists and “fans” to contact them for “collaboration” in a section on its dark web DLS. The group also requests that users who come across any news articles detailing their attacks “send them to us, and we will post it here.” Rhysida may be attention-seeking to leverage the reporting as credentials in future negotiations. Threat actors often ask members of GRIT to “Google them” during ransomware negotiations, which is likely an effort to provide us with tangible evidence of their capabilities and other victims. Their active solicitation of media personnel and news articles is novel, but the tactic can help threat actors “build their brand” to aid their negotiations.

NEWS	Contact Us Form
<p>We will post news about our company here If you see news about us, send them to us and we will post it here</p>	<p>Journalists, Recoveries, Fans, fill out the form and you will be contacted for collaboration</p>
<div><p>Undercode News Rhysida Ransomware Strikes Again: First Baptist Church of Hammond in the Crosshairs</p><p>More News</p></div>	<p>Share your contact details and leave a message</p> <p>We'll get back to you soon (Or maybe not, depending on who you are)</p> <p>Contact Us</p>

Rhysida's solicitation for media articles and journalists



Industry Spotlight: Healthcare

Industry Spotlight: Healthcare

Ransomware attacks on healthcare organizations carry higher stakes than other industries due to direct impacts on patient health and safety. The urgency to restore operations and protect patient care can make healthcare entities attractive targets for threat actors seeking leverage for higher ransom payments. This quarter, ransomware groups claimed 118 Healthcare victims, accounting for 7.5% of all ransomware attacks. This represents a QoQ increase in both volume and proportion compared with Q2 2025's 92 reports (5.8%).

The potential threat to human life increases law enforcement engagement with ransomware attacks on healthcare industry victims. This may dissuade some ransomware outfits from targeting these entities. Despite their prominence in the ransomware ecosystem, groups such as Akira, Play, and Lynx had limited impact on healthcare during Q3, with only Akira claiming one healthcare industry victim on their DLS. Other groups, however, appear to focus on healthcare organizations, with IncRansom (14), SafePay (11), and Qilin (10) accounting for 30% of the 118 healthcare victims in Q3.

Case in point, Qilin's June 2024 attack on Synnovis, which provides services for the UK's National Health Service (NHS), illustrates the dangers that come with attacks on the healthcare industry. Recent findings from the incident, published in June of 2025, tied the attack directly to an individual's death. The attack caused a blood shortage that delayed vital blood test results. The effects of the blood shortage are reportedly ongoing, more than a year later.



Qilin Ransomware



Other Reporting and Events

Cybercriminal Forums Disrupted by Law Enforcement

Law enforcement took effective action against cybercriminals in Q3 2025. This is consistent with an overall increase in cybercriminal engagement by law enforcement this year. One method law enforcement officials use is targeting community and communications platforms used by cybercriminals. Currently, there are many online places where criminals feel safe discussing their business and making new connections. By infiltrating and shutting down these havens, law enforcement seeks to make the life of the average cybercriminal more difficult and introduce a healthy amount of paranoia.

On July 22, 2025, Europol coordinated a series of enforcement actions that compromised the long running Russian-language cybercrime forum XSS, including the arrest of its alleged administrator “Toha.” Toha was charged in Ukraine for personally profiting over €7 million from trading malware, stolen data, and malicious access on his platform. Europol claims it also seized a significant amount of data related to the forum and its users. This move hints that this information may assist in investigations of other major threat actors. Predictably, large swaths of XSS users then left the site in favor of other outlets such as Exploit and DamageLib, but a few moderators remained and have attempted to revive the embattled forum. In these new landing spots, ex-power users of XSS struggle to balance between maintaining their reputation and protecting themselves from future law enforcement action. DamageLib forum administrators first advised new refugees to not use the same handle that they used on XSS to throw off the trail of any investigations into their personas; however, they have since developed policies whereby reputable users could port their reputation over to the new forum. This reputation is the lifeline for many dark web vendors who largely operate off trust built over years of forum activity. By introducing friction into this ecosystem, law enforcement encourages fear, uncertainty, and doubt in these purveyors as they seek to continue their operations.

Ohio Pens New Rules Surrounding Ransom Payments

As discussed in previous reports, disruption of cybercriminal operations does not always need to take the form of individual arrests. In some cases, local and national governments can take steps to influence the incentives surrounding cybercrime. In response to a deluge of ransomware attacks against local governments in Ohio, state lawmakers passed a series of new standards aimed at improving the resiliency of these entities. Among these new standards is a statute that controls the ability of local governments to pay ransom payments. Under this new law, in the event of a ransomware attack, government-owned entities in Ohio must seek public approval before paying a threat actor.

The stated goal of this statute is to improve transparency in local governments surrounding extortion attacks where any payment must inherently be made using taxpayer funds. These rules fall just short of banning payments outright; a potential solution often hotly debated in the information security community. However, introducing bureaucracy and oversight is almost certain to reduce the number of payments through friction alone. Ideally, legal factors restricting payments would mean that threat actors would reconsider expending the effort to impact these entities. However, it is unclear so far if threat actors respond to, or are even aware, of these restrictions.

Ohio Pens New Rules Surrounding Ransom Payments

As lawmakers consider new and creative strategies for reducing the impact of ransomware attacks on their constituents, one can consider the efforts of Florida as a case study. In July of 2022, Florida amended the State Cybersecurity Act to enforce an outright ban on paying ransoms by state agencies, counties, and municipalities. Since then, GRIT has observed 14 publicly disclosed ransomware attacks against such entities in the state. This begs the question: was this ban effective at reducing attacks, or did the new law do nothing to dissuade financially motivated threat actors? Absent a true control group, it is difficult to draw a substantive conclusion.

In all, the best conclusion we can draw is that a full ransomware payment ban does not stop an opportunistic threat actor from carrying out attacks on specific entities. A ban may reduce the likelihood of public funds being used to pay ransoms, but it does not reduce attacker incentives or fix underlying security weaknesses. This is not to say that a payment ban could never be effective; perhaps a larger scale national action could have more noticeable effects, but as ransomware continues to have significant impact on the operations and finances of government entities, lawmakers will continue to search for ways to soften the blow.

RaaS Lifecycle Case Study: From BlackLock to Global

The world of organized cybercrime, particularly the Ransomware-as-a-Service (RaaS) ecosystem, is defined by relentless organizational agility and often instability. The public-facing brand of a ransomware group is increasingly a disposable, short-term asset, strategically cycled to maximize profit and evade the inevitable fall. The rapid, volatile lifecycle of the group operated by the user \$\$\$ on the dark web forum RAMP, who cycled through the names Eldorado, BlackLock, Mamona RIP, and finally GLOBAL, serves as a critical case study in this modern, high-velocity criminal enterprise model.

This analysis tracks a highly ambitious RaaS operator who, in under two years, displayed an unprecedented tactic of strategic rebranding and market saturation, only to fall victim to the two greatest threats to a criminal syndicate: internal betrayal and a catastrophic OPSEC failure.

The first emergence of \$\$\$'s operations occurred in March 2024 as a new entrant to the RaaS ecosystem. \$\$\$ first gained notoriety under the name Eldorado Ransomware. Its initial RaaS offering, posted on RAMP on March 30, 2024, was straightforward: a "locker for rent" with a modest 10% to 15% revenue split for the core operator.


[RaaS] 2024

\$\$\$ · Mar 30, 2024

Reply

Forums > Market > Partners Program \ RaaS \ Partner Prog...

Watch



\$\$\$

Well-known member

Nov 1, 2023

Messages 554

Reaction score 718

Points 93

Mar 30, 2024

<

□

#1

I offer a locker for rent
The standard chat partition is the locker itself.
You negotiate and accept the money into your own accounts.
I will only issue the locker after checking the target
I'll give it to you for 15%, whoever shows me lower, I'll give it to you for 10%
good luck to everyone

Report

Like Reply

Initial recruitment post by \$\$\$ on March 30, 2024

21

RaaS Lifecycle Case Study: From BlackLock to Global

This initial ransomware group eventually transformed into a more ambitious project known as BlackLock. By January 14, 2025, \$\$\$ relaunched the fully fleshed-out “partner program” (or PP as it’s referred to on RAMP) under the name “RaaS Black Lock”. The advertisement revealed a technologically sophisticated offering:

RaaS Global Black Lock


\$\$\$ · Jan 14, 2025

Forums > Market > Partners Program \ RaaS \ 合作伙伴计划

1 2 Next >

Watch

Reply



Well-known member
Nov 1, 2023
Messages 554
Reaction score 718
Points 93

Jan 14, 2025

A powerful tool for fast and secure data encryption

Our software is a universal solution for secure encryption of files and directories.

Key features:

- Support for multiple platforms
Compatibility with ARM, ARM64, i386, and AMD64 architectures allows our software to be used on a wide range of devices—from compact single-board computers to powerful servers.
- Support for various operating systems
Our product runs on Windows, Linux, ESXi, NAS and FreeBSD, providing flexibility for various infrastructures.
- Working with network protocols
Support for the SMB protocol and the use of Pass-the-Hash technology for advanced authentication capabilities.
- Reliable encryption
Cryptographically strong algorithms based on elliptic curves are used for encryption, ensuring a high level of security.
- The “spot” encryption method
Data is encrypted point-by-point, allowing for rapid processing of large volumes of information. The size of the spots can be adjusted via the command line (default is 1%).
- Delayed launch
The program can be launched on a timer or at a specified time, which provides flexibility in settings.
- Safe self-removal
Once finished, the program automatically removes itself, leaving your system clean and secure.

Features of working on the Windows platform:

- Automatic processing of all connected disks
The program automatically detects and encrypts all connected devices, including external drives.
- Deleting shadow copies and emptying the Recycle Bin
To prevent data recovery, the program deletes all shadow copies and empties the Recycle Bin.
- Stopping processes that have occupied a file
The program can stop processes blocking access to the file to complete its encryption.

RaaS Lifecycle Case Study: From BlackLock to Global

By March 11, 2025, the \$\$\$ operator announced the launch of a new infrastructure named Mamona RIP. With Mamona RIP, \$\$\$ offered a staggering 85% revenue split for affiliates, retaining only 15% for the core developers. This move optimized for market presence over immediate, high-margin profit, akin to the initial recruitment push of newcomer RansomHub around the same time.

MAMONA R.I.P


\$\$\$ · Mar 11, 2025

Reply

Forums > Market \ 市场 > Partners Program \ RaaS \ 合作伙伴计划

123Next

Watch



\$\$\$

Well-known member

Nov 1, 2023

Messages554

Reaction score718

Points93

Mar 11, 2025

Мы рады предоставить вам абсолютно новый продукт с учетом всех наших проб и ошибок в данной сфере деятельности!

Welcome to Mamona RIP

We've been hard at work developing our ransomware infrastructure, and we're excited to announce that we are ready to launch!

Revenue Split:
85/15. The payment is sent directly to your wallet, and then you send us our share.

INFO PANEL

Below are the key features of our affiliate panel:

Panel

Each affiliate gets a unique TOR link for their panel.

Chat

Each chat has a distinct onion address. From here, you can:

- Provide a decryptor
- Mark as paid (for clients who have only paid for data deletion)
- Upload files
- Edit messages
- Download decryptor for yourself
- Choose authentication when building chats
- And much more

Upload

All affiliates receive a dedicated storage space on the panel. Depending on your performance, your storage capacity may increase or decrease. You can upload zip files, extract them, and download a file tree of all stolen data to show everything that's been stolen.

Builder

Generate locker builds with various configurations for:

- ESXi
- Windows
- Linux/NAS

Mamona RIP recruitment post by \$\$\$ on March 11, 2025

23

RaaS Lifecycle Case Study: From BlackLock to Global

On March 28, 2025, another RAMP user named Bratislava posted about a critical OPSEC failure suffered by the BlackLock Ransomware. Security researchers had successfully exploited a misconfiguration on the group's DLS, which was supposed to be hidden on the network. This is provided both in a blog by Resecurity, as well as the defaced BlackLock DLS site with Rescurity's name on it, as shown below.

Mar 28, 2025

what a good PP

Bratislava
Member
July 27, 2023
Messages 41
Reaction score 45
Points 18

Blacklock Ransomware - DLS Local File Include (LFI)
Resecurity
BLACKLOCK
EVAS
akamha.fr
haza-org.com
DATASCAN
01:29

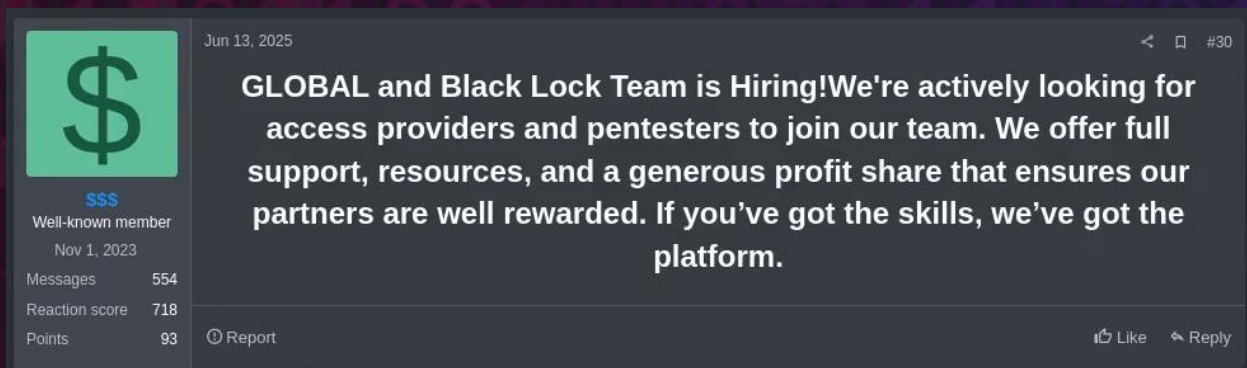
"They call me crazy now."
👍🤔 Vorkuta, Shahmen, 11B-X-1371 and 4 others

Report Like Reply

RAMP user Bratislava highlights Resecurity's defacement of BlackLock's DLS

RaaS Lifecycle Case Study: From BlackLock to Global


This growth culminated in a massive recruitment push on June 13, 2025, under the new names of GLOBAL and Black Lock Team, eventually becoming known as GLOBAL Group. The group specifically sought specialized roles like access providers and pentesters. This tactic, common in mature RaaS operations, is a critical component of the syndicate's business logic: outsourcing the high-risk, time-consuming initial access phase to dedicated Initial Access Brokers (IABs) and pentesters to dramatically accelerate the overall attack lifecycle.



GLOBAL and BlackLock recruitment comment by \$\$\$

The speed of this evolution (four distinct names in a little over a year) is a textbook example of the Accelerated Brand Cycling model. Despite the aggressive growth, BlackLock's centralized structure led to fatal vulnerabilities. On June 26, 2025, \$\$\$ stated that a "previous coder stole payments and was dishonest," forcing the entire operation to announce a necessary merger and restructuring. This organizational breakdown exposed a profound failure of internal trust and compartmentalization, risking the public exposure of technical documentation and operational procedures.

RaaS Lifecycle Case Study: From BlackLock to Global



\$\$\$
Well-known member
Nov 1, 2023
Messages 554
Reaction score 718
Points 93

Jun 26, 2025

Expect a merger with a new Affiliate Program where there will be honesty and results
Unfortunately, the previous coder stole payments and was dishonest with me.
Please be understanding and please let everyone else just pass by.
Thank you all, gentlemen

Last edited: Sep 17, 2025

👍👎 Fantomas, dopa and 11B-X-1371

🔔 Report


👍 Like ↩ Reply

Breakdown and merger comment by \$\$\$

On July 16, 2025, RAMP user Bratislava posted about another critical OPSEC failure suffered by the BlackLock Ransomware. Security researchers had successfully exploited a misconfiguration on the group's DLS, which was supposed to be hidden on the Tor network. The resulting intrusion compromised the organization at its most sensitive point. It exposed

- The group's real-world, clear-net hosting IP address
- Internal command history
- Copy-pasted credentials used by the main actor to manage the server

This failure of a core component of the criminal business confirmed the syndicate's immediate and public unraveling.



Bratislava
Member
July 27, 2023
Messages 41
Reaction score 45
Points 18

July 16, 2025

fuck...

<https://blog.eclecticiq.com/global-group-emerging-ransomware-as-a-service>

GLOBAL GROUP's current infrastructure uses the same provider at IP address 193.19.119[.]4 under port 3304. **This connection was revealed through an operational security (OPSEC) mistake in GLOBAL GROUP's infrastructure. The group attempted to hide their leak site behind a Tor hidden service. However, an exposed API endpoint /posts returned JSON metadata that revealed the real-world hosting environment.** Inside the returned JSON field, the sshConnectionName section for each victim entry included IP address 193.19.119[.]4 and a SSH username as dataleak. This leak confirmed that victim data was stored on a misconfigured system, reachable over the internet.

"They call me crazy now."

👉 firki

🔔 Report

👍 Like ↩ Reply

RAMP user Bratislava highlighted IP infrastructure revealed by EclecticIQ

RaaS Lifecycle Case Study: From BlackLock to Global

A subsequent edit to the conflict post on September 17, 2025, shows the protracted struggle to manage the internal and external fallout, confirming the group's ultimate failure to recover and decision to merge with another RaaS operator to continue operations.

The short, high turnover ransomware life of the \$\$\$ operations is best understood when juxtaposed with the strategic persistence and failure points of other historical RaaS groups. The common thread is that the groups, namely the skilled personnel and their methodology, are the enduring threat outlasting any single brand name.

Take the Conti group for example, operated by “Wizard Spider”. It represents the gold standard for organizational survival. When faced with existential threats of geopolitical backlash and massive internal data leaks, Conti executed a dissolution. The group intentionally destroyed the public brand to save the underlying organization, ultimately splintering into smaller, compartmentalized successor “cells”, such as Black Basta and BlackCat (Alphv). This fragmentation ensured that the core skills and operational methodology migrated, achieving resilience through decentralization.

The DarkSide RaaS provides a clear example of reactive rebranding driven by brand toxicity. Following the affiliate-executed attack on Colonial Pipeline in May 2021, the event instantly generated intense government scrutiny. DarkSide almost immediately announced its closure. Two months later, BlackMatter emerged, explicitly advertising itself as the successor, while publicly announcing a policy to avoid critical infrastructure. This was a calculated move to shed the toxic political profile associated with the previous brand. It also demonstrated that a catastrophic security event may mandate brand dissolution to protect the underlying criminal business.

RaaS Lifecycle Case Study: From BlackLock to Global

Meanwhile, the disruption of LockBit 3.0 contrasts sharply with the planned retreat of Conti. LockBit was successfully targeted in February 2024 by Operation Cronos, which focused on the centralized operational infrastructure. Law enforcement seized and controlled LockBit's administration environment and DLS. This seizure of the centralized affiliate control panel, which was essentially a single point of failure, crippled the group's ability to conduct business and exposed its entire network.

As such, \$\$\$ group's failure was a less sophisticated version of the LockBit scenario. Their centralized infrastructure was compromised (albeit not by law enforcement) by a simple API misconfiguration, confirming the high organizational risk inherent in relying on an unfragmented RaaS structure.

The swift succession of Eldorado, Mamona RIP, BlackLock, and GLOBAL by the same underlying operator demonstrates the adoption of an accelerated brand cycling model. This strategy prioritizes immediate market expansion over brand longevity, treating the name as a disposable marketing asset.

However, the group's ultimate demise confirms two immutable laws of the RaaS ecosystem:

1. Organizational persistence is the ultimate goal for any RaaS
2. Also, a lack of structural compartmentalization and basic operational security can destroy even the most technologically sophisticated criminal enterprise



Quarterly Wrap Up

Q3 closes with what appears to be a new “baseline” for ransomware activity, at least temporarily pausing the exponential QoQ growth we have observed in recent years. While we presented three plausible hypotheses up front for what could be driving this stagnation concurrent with the growth of distinct named groups, GRIT finds the most plausible explanation to be a combination: we are observing greater consolidation of skilled actors within prolific, Established RaaS groups, while at the same time witnessing an increase in low-skill or Ephemeral groups on the scene.

We have observed the increase in claimed victims from Established groups and have witnessed the increase in their attacks (including those unclaimed) directly through GuidePoint’s Incident Response practice, and this is one half of our assessment. But we have also observed, anecdotally, an increase in attacks not attributable to any known group, or where the threat actor may even outright refuse to identify themselves. This can plausibly be the result of growing distrust in the RaaS construct, reduced barriers to entry for aspiring cybercriminals, or splintering of existing groups resulting in outcast affiliates forced to find a new home. In the months and quarters ahead, we will specifically be looking to determine the timelines, efficacy, and victim outputs of such groups to aid in our ongoing analysis and determinations.

Law Enforcement, both within the United States and internationally, continues to play an important role in reducing incentives and increasing the costs of contemporary cybercrime. The cybercrime ecosystem suffers from a diverse attack surface as a direct result of the “-as-a-Service” construct that has been so readily adopted. Initial Access Brokers must sell access, infostealer logs must be sold on marketplaces, aspiring script kiddies must make a name for themselves on illicit forums, and even the most Established RaaS groups must communicate internally. Law Enforcement continues to recognize and seize on these multiple attack surfaces as opportunities for disruption, disinformation, and infiltration. Frankly, we love to see it.

In sum, what some may dismiss as “yet another quarter of ransomware”, we see it as a new baseline of operational activity. We hope you will join us at the start of next year for our flagship Annual report, where we will review the year in aggregate and present our forecasts for ransomware and cybercrime in 2026. In the meantime, we encourage Defenders to first emphasize security best practices, which less-sophisticated attackers will pursue as targets of opportunity, and then to emphasize defense against the most prolific – and relatively templated – attacks of the most established actors.

Happy Hunting.