Analyzing the Shift in Ransomware Dynamics: The Impact of Law Enforcement and Future Outlooks

By Andrei Moldovan

Published: 2024-06-27 · Archived: 2026-04-05 17:33:21 UTC

The landscape of ransomware attacks has witnessed significant shifts from Q4 2023 to Q1 2024 after several ransomware disruptions. Ransomware statistics analyzed by QuoIntelligence within this period indicates a 22% decrease in the number of publicly announced ransomware victims, a change potentially attributed to several dynamics within the ransomware threat landscape. Key factors include strategic actions by law enforcement agencies and the impact of Ransomware-as-a-Service (RaaS) operators executing exit scams on their affiliates. These exit scams, coupled with a rise in victims refusing to pay ransoms, led to a substantial 32% decline in ransom payments during this period.

Figure 1: Distribution of the number of ransomware victims since Q4 2023 to Q2 2024. Source: QuoIntelligence.

However, it is important to highlight that the spike observed in Q2 2024 during the month of May, where 174 of the reported victims were attributed to **LockBit**, occurred in retaliation against Operation Cronos. The data acquired during June 2024 is a partial subset of victims, updated to June 26th, and this number may change in the coming days.

Our main takeaways for this article includes:

- Despite the gradual decline of **LockBit** in recent months, new groups are expected to rise and exploit the current ransomware threat landscape to boost their visibility and reputation among cybercriminals and the underground community.
- While law enforcement actions may not yield immediate results, they have a significant long-term impact on the credibility of ransomware groups by gradually eroding the talent pool of skilled affiliates.
- Ransomware source code leaks will be pivotal in the emergence of future low-level operators and the reuse of code in prevalent ransomware families.
- The proliferation of FUD (Fear, Uncertainty, Doubt) content and unverified claims made by cybercriminals and media outlets is exponentially increasing the visibility that these ransomware groups seek to attract new talent.

Law Enforcement’s Role in Mitigating Ransomware Threats

The efforts of law enforcement actions, although challenging to quantify precisely, play a crucial role in reducing the threat posed by ransomware operators and their affiliates. These agencies focus on eroding the ransomware landscape and acting as a deterrent to potential cybercriminals. Even though only few operations have resulted in the arrest of ransomware operators or affiliates, the cumulative impact of these efforts has led to a reduction in the pool of skilled individuals capable of executing sophisticated attacks.

Law enforcement actions not only apprehend cybercriminals but also induce significant psychological stress and internal conflict among affiliates, disrupting their coordination and communication. This disruption is critical, as effective collaboration is essential for RaaS operators to maintain their operations and reputations. The seizure and dismantling of Dedicated Leak Sites (DLS) further cripples the operability of RaaS models, damaging their credibility and operational capabilities.

Notable Law Enforcement Actions and Internal Conflicts During 2023 and 2024

In recent years, law enforcement agencies have intensified their efforts to combat ransomware operations, achieving significant milestones in 2023 and 2024. These actions have disrupted major ransomware groups and affiliation models, affecting their operational capabilities and reducing their threat levels.

Here are some notable actions:

- **23 January 2023**: The Department of Justice (DoJ), in collaboration with the Federal Bureau of Investigation (FBI) and thirteen other international law enforcement agencies, successfully dismantled **HIVE**. This prominent RaaS model had claimed more than 1500 victims since 2021, making its takedown a critical victory in the fight against ransomware.
- **18 October 2023**: The pro-Ukraine group, **Ukraine Cyber Alliance (UCA)**, defaced and wiped the entire infrastructure of **Trigona**, a smaller RaaS model struggling with internal and management issues related to its DLS. This action significantly disrupted **Trigona**‘s operations.
- **20 October 2023**: Multiple European law enforcement agencies seized and dismantled the infrastructure of **Ragnar Locker**, a long-standing ransomware group that had not transitioned into a RaaS model, marking **Ragnar Locker**‘s operational end.
- **19 December 2023**: The FBI temporarily took down the infrastructure of the popular RaaS model **BlackCat/ALPHV**. Following this seizure and not yet confirmed, the operators reinstated their infrastructure but reportedly performed an exit scam against one of their affiliates two months later, stealing over EUR 20,000,000 and disappearing from the underground. There are unconfirmed theories that the new RaaS affiliation model, **RansomHub**, is a rebranding of **BlackCat/ALPHV**.
- **20 February 2024**: During Operation Cronos and subsequent months, multiple coordinated law enforcement agencies compromised **LockBit**‘s infrastructure via a PHP vulnerability. This operation took over most of **LockBit**‘s infrastructure and sensitive information stored on their DLSs. Although the operation was highly effective, **LockBit** continues to operate, albeit with questionable practices such as recycling old data and creating fake claims. After law enforcement agencies published the individual and the personal information behind **LockBitSupp**, QuoIntelligence noted an increase of victim announcement on **LockBit**‘s DLS, as well as a reduced online presence of **LockBitSupp**.

The following illustrations provides a high-level overview of the most important disruptions to ransomware:

Figure 2: Timeline of the major disruption events against ransomware groups since 2023.

The Emergence and Impact of Ghost Groups

Throughout 2023 and 2024, the outsourcing of threat operations to highly specialized groups, known as ghost groups, were a recurrent phenomenon. Consisting of freelance cybercriminals with advanced technical skills,

command higher percentages of ransom payments than typical affiliates and often go unreported due to an exceptional proficiency in securing payments from their victims. Prominent ghost groups, such as **Zeon** and **REvil**'s pentesters, have been linked to multiple RaaS models, including **BlackCat/ALPHV**, **Akira**, **LockBit**, and **BlackSuit**.

LockBit, in particular, has leveraged ghost groups for covert operations targeting high-value entities, causing significant financial distress. These operations are exceptionally challenging to trace, often compelling victims to pay ransoms to avoid exposure on the group's DLS. In spite of **LockBit**'s reputational decline, ghost groups like **Zeon** are likely transitioning to other emerging RaaS models, with **Akira** gaining notable popularity since March 2024.

Migration to Other Alternatives and New Entries: An Overview

After **Operation Cronos**, it is likely that skilled affiliates lost trust in **LockBit** and decided to part ways, either by developing their own affiliation model or their own closed-sourced group of trusted affiliates. It is important to pinpoint that an affiliate does not pledge alliance to a single affiliation program, but to more than one in order to use multiple ransomware builder and potentially to make profiling harder.

Excluding **LockBit** from our statistics, we have identified the 10 most active ransomware based on the reported victims in 2024:

Figure 3: Top 10 Ransomware Groups Ranked by Victims Excluding LockBit. Source: QuoIntelligence.

Based on internal telemetries and seasonal statistics, QuoIntelligence identified the following groups that are more likely to compete in the ransomware threat landscape due to high-level targets reported within their own DLS and arsenal sophistication:

- **Akira**: commencing operations in March 2023, it is distinguished by its 'retro aesthetic' on its DLS. The group targets large enterprises across various sectors, such as education, finance, manufacturing, real estate, and medical, prioritizing entities capable of fulfilling their substantial ransom demands.
- **RansomHub**: self-described as a collective of hackers from various global locations, the group's primary motivation is financial gain. The group claims to avoid attacks on organizations from CIS, Cuba, North Korea, and China, suggesting a possible Russian influence, although direct ties to Russia are speculative. There are unverified claims that RansomHub may be a rebranded version of the infamous **BlackCat/ALPHV** group or that it has integrated former **BlackCat/ALPHV** affiliates. Financial transactions favor affiliates, who receive 90% of the ransom payments, an arrangement designed to build trust among potential collaborators, especially in the wake of the **BlackCat/ALPHV** scam which eroded trust within the RaaS community.
- **Hunters International**: it is a highly sophisticated and adaptable group known for its targeted ransomware attacks and data exfiltration operations. Demonstrating advanced skills in malware development, social engineering, and exploiting network vulnerabilities, they are primarily driven by financial gain, encrypting victim data and demanding ransom payments, while also leveraging the strategic value of stolen information. **Hunters International** targets a wide range of sectors, including healthcare, finance, government entities, and critical infrastructure, operating globally with a significant focus on North America, Europe, and parts of Asia.

Persistence of Lower-Level Affiliates and Future Outlooks

Lower-level affiliates continue to support the RaaS model, maintaining connections with leadership even after initial takedowns. This persistence highlights the resilience of RaaS operations and the ongoing challenges in dismantling such networks. The continuation of these lower-level activities underscores the need for sustained efforts in combating ransomware threats.

The recent leaks of multiple ransomware builders, including **LockBit**'s, suggest an imminent increase in the number of RaaS models. New groups are expected to emerge, potentially replacing **LockBit** in terms of reported incidents. However, replicating the distinct persona and branding of **LockBitSupp**, central to **LockBit**'s operational identity, is unlikely if the objective is to remain stealthy within media outlets, law enforcement agencies and security researchers. While it is definitely allowing RaaS models to grow exponentially, it also attracts unwanted attention.

High-profile media stunts have previously been used to divert attention from main ghost groups, this strategy is expected to diminish. Increased exposure from such activities can undermine the operational security of RaaS models, prompting a shift towards maintaining a lower profile to avoid detection.

Leaked Builders and Impersonations

When ransomware operators sell their ransomware builder's source code or it gets leaked on underground forums by rogue affiliates, it is unsurprising that new RaaS operators and low-level groups attempt to create their own versions of the tool. These groups often modify the ransom note or completely impersonate RaaS affiliates. A specific case in point is the emergence of a slightly modified **LockBit 3.0** variant, dubbed **LockBit 4.0**. This variant was first seen on February 24th, with 13 samples currently available on VirusTotal. This is one of many clones of **LockBit 3.0**, whose source code was leaked in August 2023, enabling the rise of new groups repurposing the code.

While the reuse of identical source code allows defenders to maintain effective detections without significant changes, the involvement of more skilled ransomware operators could pose a serious threat. These operators could introduce new capabilities, functionalities, and evasion techniques. A prime example is the leak of **Babuk**'s source code, which targeted ESXi servers and was quickly adopted by numerous ransomware operators.

It is not uncommon for lower-level affiliates and new groups to mimic and leverage the reputation of more established entities. **APT73**, not to be confused with commonly referenced Advanced Persistent Threat (APT) groups, published information on their first victim on April 25th. To date, they have 12 known victims.

A distinctive feature of **APT73** is the striking visual similarity between their data leak site (DLS) and that of **LockBit**. This resemblance likely aims to capitalize on **LockBit**'s established reputation, potentially attracting affiliates to join **APT73**'s program. Notably, there are no public advertisements on underground forums promoting **APT73**'s services.

The rationale behind the similar design of the DLS remains unclear. However, it is plausible that this mimicry is intended to signal to others that **APT73** operates at a level comparable to **LockBit**, potentially inspiring trust in new affiliates or low-level criminals willing to collaborate with **APT73**.

Taking Advantage of Fake Data Breaches

While impersonation and code reuse can be effective tactics to leverage the reputation of established groups, the most recurring and impactful strategy in the underground is the republication of old data or the creation of fake data breaches to attract media attention. This behavior is often amplified by several factors:

- **Sock Puppet Accounts**: Cybercriminals create fake accounts on social media platforms to publish and boost the visibility of their claims.
- **Media Attention**: Cybercriminals gain media attention by securing interviews with news reporters.
- **Spreading FUD (Fear, Uncertainty, Doubt)**: Individuals without malicious intent often spread sensational content without verifying the reliability of the source.
  Regardless of the tools and techniques used, increased visibility and discussion about a group enhance its reputation in the underground community. However, this strategy can backfire when cybercriminals fail to substantiate their claims. This has been observed repeatedly, even involving some underground forum moderators or **LockBit**‘s operators themselves.

In essence, while the amplification of claims can elevate a group’s standing, the inability to provide credible evidence can lead to reputational damage, undermining the group’s credibility in the underground ecosystem.

Current Situation of LockBit and LockBitSupp

Following the release of personal information about the individual behind the **LockBitSupp** persona by law enforcement agencies, the following events were observed in quick succession:

- Initially, **LockBitSupp** denied the allegations. However, the persona gradually faded from both media outlets and underground forums.
- Concurrently, the DLS saw an increased publication rate of victims, suggesting either ongoing negotiations with affiliates or a retaliatory response against law enforcement agencies. Additionally, several companies that had previously paid the ransom were re-published, despite promises that their data would be deleted. This was corroborated by law enforcement agencies during **Operation Cronos**, which uncovered the supporting infrastructure and terabytes of data that should have been deleted but were instead backed up.
- Targets shifted towards new victims in the academic and healthcare sectors, indicating a potential loss of control and credibility over affiliates by those managing the ransomware operations and the well established rules of engagement.
- During the end of June 2024, the number of new victims greatly decreased.
- On June 25th, the group allegedly claimed of having breached the Federal Reserve and exfiltrating 33 TBs of data. While every media outlet exponentially amplified this claim without further validations, the group failed yet again to provide solid proofs of the breach and the DLS redirected users to an unrelated breach. On June 26th, the targeted company was not the Federal Reserve but Evolve Bank, an US-based financial entity who confirmed the data breach.

QuoIntelligence was unable to identify further data to substantiate these claims, suggesting they may be used as a tactic to divert law enforcement agencies by shifting internal resources into investigating the claims within the Federal Reserve. It is important to highlight that **LockBit**‘s operators have, on multiple occasions, orchestrated

fake claims and reused old data breaches to attract attention. A notable example is their claim of a breach against Mandiant after the security vendor published a detailed report on **UNC2165**, a financially motivated threat actor known for deploying ransomware, which had shifted their tools to **LockBit**'s ransomware to evade sanctions.

QuoIntelligence assessed with medium confidence that, based on historical data and events, similar claims are likely motivated by retaliation against entities to damage their reputation while amplifying media attention towards **LockBit**. This tactic is very likely being used to attract more affiliates by leveraging the enhanced visibility and perceived notoriety. While affiliates have the complete control of what information to publish on **LockBit**'s DLS, the administrators are unlikely to verify the claims made by the affiliates.

Although **Operation Cronos** significantly impacted **LockBit**'s infrastructure and its affiliates, it is unlikely that the group will cease operations in the near future. Affiliates are expected to continue leveraging **LockBit**'s reputation and sophisticated ransomware. Notably, since the end of May, two weeks after law enforcement agencies released personal information about the persona known as **LockBitSupp**, its online presence has diminished. The future of **LockBit** is uncertain, as **LockBitSupp** was the primary figure attracting attention and visibility, crucial for the group's proliferation within the underground.

Conclusions

Despite the potential emergence of numerous inexperienced ransomware groups and RaaS models, the overall threat level of ransomware attacks is anticipated to remain stable. The pool of highly skilled attackers may diminish over time, but organizations must remain vigilant. Even adversaries with lower sophistication can exploit minor security oversights, leading to significant breaches.

Research by Andrei Moldovan, Threat Researcher at QuoIntelligence.

Andrei brings extensive expertise in malware reverse engineering and criminology, backed by years of experience in a Security Operations Center (SOC). His passion for malware and offensive security drives him to shed light on unknown threats to combat cybercrime and cybercriminals.

Source: https://quointelligence.eu/2024/06/analyzing-shift-in-ransomware-dynamics/