Cyberint

The Rise of RansomHub

August 2024

Table of Contents

Introduction

The RansomHub ransomware group has emerged as a significant player in the ransomware landscape, making bold claims and substantiating them with data leaks. The group emerged after the Federal Bureau of Investigation (FBI) disrupted ALPHV's ransomware operation on December 19, 2023. There are assumptions that RansomHub is a "spiritual successor" of the ALPHV group and operates with the help of former ALPHV affiliates.

On February 10, 2024, RansomHub announced its first victim, the Brazilian company YKP. As of August 22, 2024, the group has targeted 190 victims across the globe. According to our data, RansomHub has topped the list with the highest number of victims in July and August (so far). Notably, over 50% of their total attacks were carried out within these two months alone, suggesting a significant escalation in operations, likely driven by an increase in affiliate participation.

RansomHub clearly capitalized on the disruption inflicted on the LockBit gang by law enforcement in February 2024. The international crackdown on LockBit led to the seizure of some of its websites and decryption tools, while sending a clear message to affiliates that they were also under surveillance. As a result, many affiliates who had relied on LockBit's encryptors have now shifted their allegiance to competing RaaS groups.

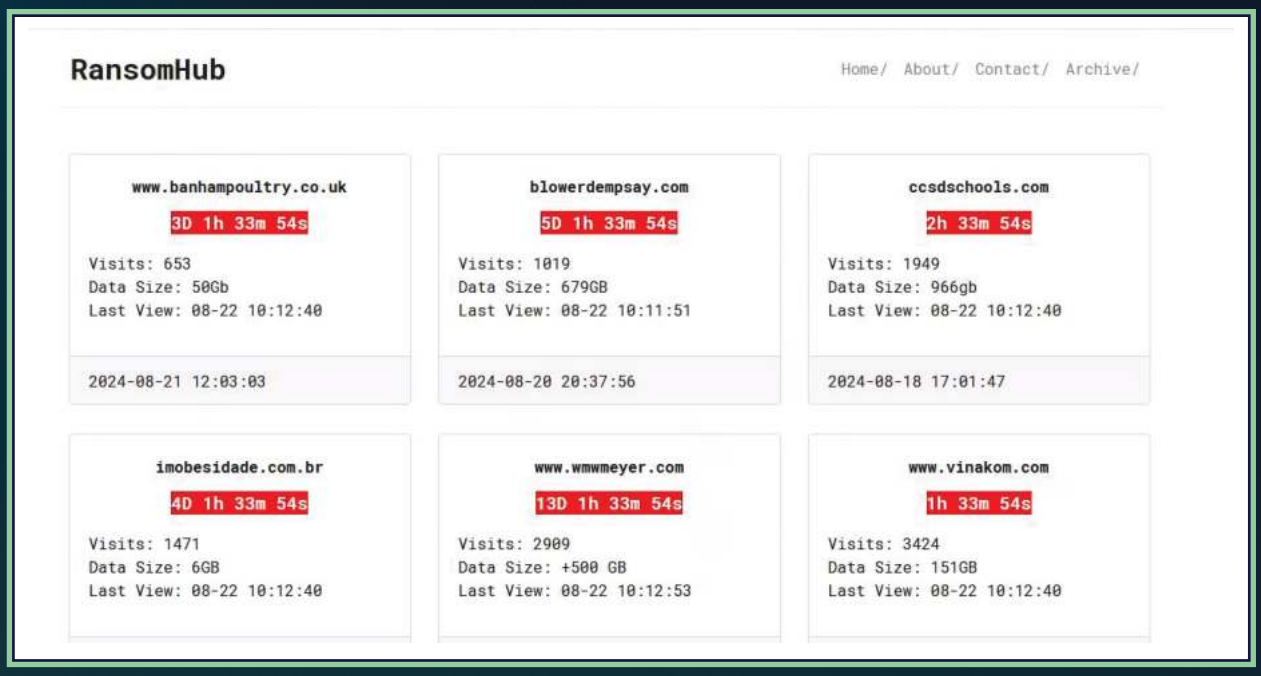

Figure 1: RansomHub Data Leak Site Home page

Money, Money, Money

RansomHub operates on a Ransomware-as-a-Service (RaaS) model, asserting that affiliates must adhere to the agreements and requirements set during negotiations, with non-compliance resulting in a ban and termination of collaboration. Affiliates receive 90% of the ransom, while the main group takes the remaining 10%.

These pricing arrangements are higher than the typical 80-70% range in the RaaS market. This lucrative rate is likely to attract seasoned affiliates from other platforms, leading to a surge in RansomHub-related infections and victims, as every month we've seen the group breaking its own records in the number of successful attacks.

Examining the group's earnings by analyzing their DLS and tallying the published data posts (indicating victims who refused to pay the ransom), we found that 160 out of 190 victims chose not to pay. Of the remaining 30, ten victims are still in negotiations. This means that, out of the 180 victims who have either resolved or refused payment, only 11.2% actually paid the ransom. Additionally, negotiations often result in a reduction of the original ransom amount demanded.

For the group's admin operators, the focus isn't on the payment rate but on volume. The more affiliates that join, the more attacks are launched, leading to increased revenue over time. Even if only 1 in 10 victims pays, the operation remains profitable, generating millions of dollars.

Figure 2: RansomHub publishes data of victims who refused to pay the ransom

Victimology

According to the group's About page, RansomHub consists of threat actors from various global locations, united by a shared goal of financial gain. The gang explicitly prohibits attacks on certain countries and non-profit organizations.

Moreover, RansomHub's DLS (Data Leak Site) indicates that they avoid targeting CIS, Cuba, North Korea, and China. Despite their claims that they are a global hacker community, their operations closely resemble a traditional Russian ransomware setup. Their stance on Russian-affiliated nations and the overlap with other Russian ransomware groups in targeted companies are notable.

Figure 3: "About" section in the group's DLS

As depicted in the graph below, the United States unsurprisingly is the most targeted country, with 66 victims to date. Based on our Q2 Ransomware Landscape report, we might have anticipated the United Kingdom or Canada to take the second spot, however, Brazil has unexpectedly taken that position with 17 victims in just six months. Notably, the first victim was a Brazilian organization (YKP), marking the initial step in targeting organizations in that country.

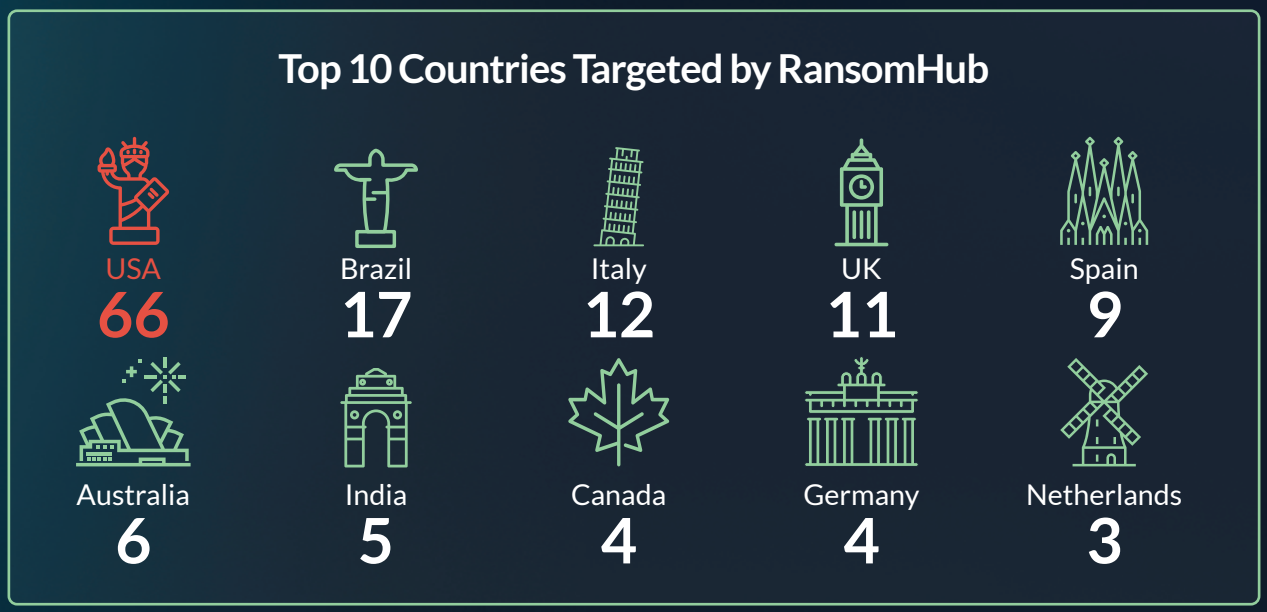

Figure 4: Top 10 countries targeted by RansomHub

As far as for industries, business services is the sector most impacted by RansomHub attacks, with 45 organizations in this category.

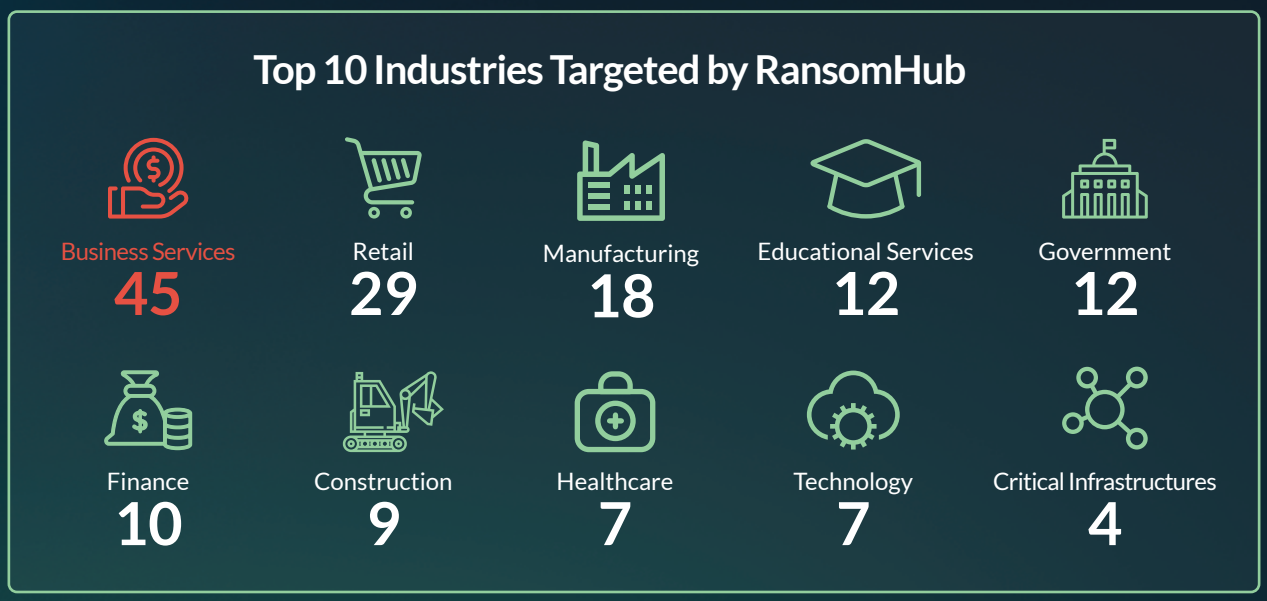

Figure 5: Top 10 industries targeted by RansomHub

It's All About the Numbers

Revenue

Since the starting RansomHub's operation in February, the Cyberint research team has closely monitored the group's operations and uncovered interesting insights about the company's size and revenues of targeted organizations.

The average revenue of the victims was calculated at approximately $444 million, with a median of $8 million. The significant gap between the median and average suggests a skew in the data. Upon closer examination (Figure 6), it becomes clear that 84% of the victims are organizations with revenues below $100 million. If we exclude the eight victims with revenues exceeding $1 billion, the average revenue drops to $59.68 million.

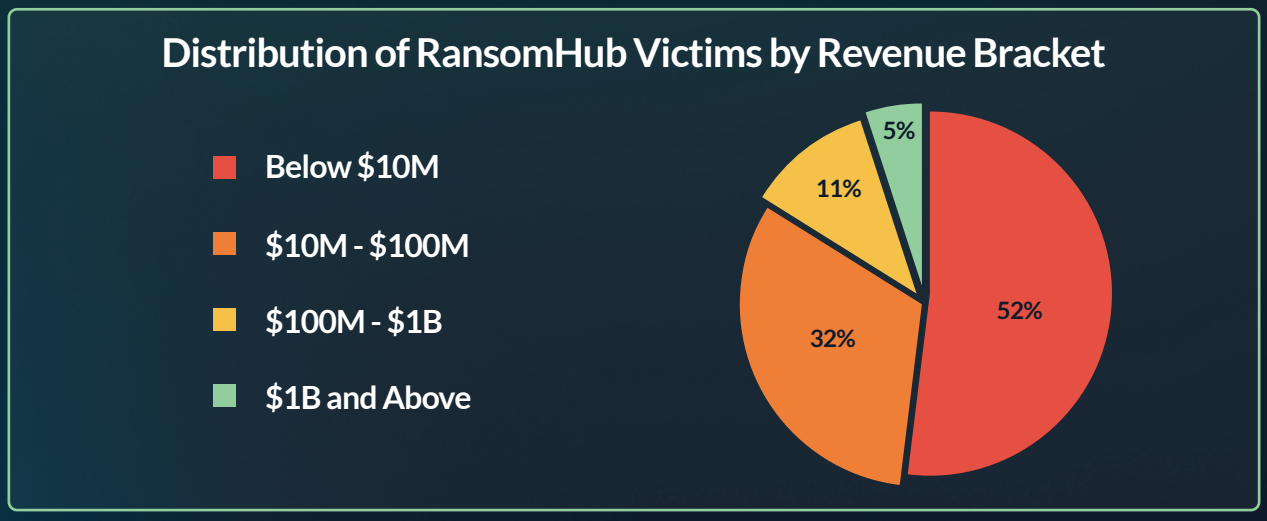

Figure 6: Distribution of RansomHub Victims by Revenue Bracket

Company Size

The number of employees in a company can often reflect its revenue and other factors such as industry and the number of facilities.
In our analysis, we found employee data for 90% of the victims. The chart below shows a positive correlation between the number of employees and revenue, with 60% of the victims being organizations with fewer than 100 employees.

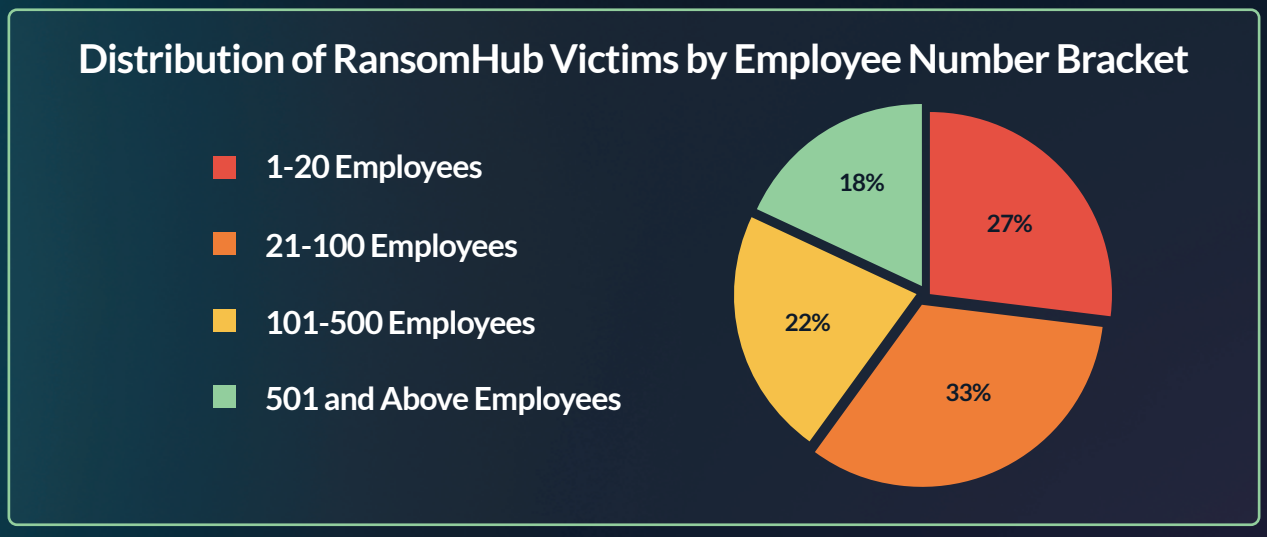

Figure 7: Distribution of RansomHub Victims by Employee Number Bracket

Malware, Toolset & TTPs

Notably, RansomHub's ransomware is written in Golang, similar to other ransomware groups like GhostSec, indicating a potential trend. The group promises to send victims a decryptor for free if the affiliate fails to provide one after payment or if an off-limits organization is attacked. The ransomware used by the gang can encrypt data before exfiltration.

It was also observed that RansomHub, based on their past ransomware attacks, could somehow be related or a rebrand of the ALPHV ransomware group. Therefore, tools and TTPs could be similar to those used by ALPHV.

The group's ransomware is developed in Golang and C++ and targets Windows, Linux, and ESXi instances. One of its distinguishing features is its fast encryption speed compared to other RaaS options.

According to Sophos research, RansomHub is also being compared with Knight Ransomware, where there are similar indicators being used by both ransomware groups, such as:

1. Ransomware Payloads written in Go Language. These payloads are obfuscated using GoObfuscate.
2. Ransomware Payload command line menus are the same:

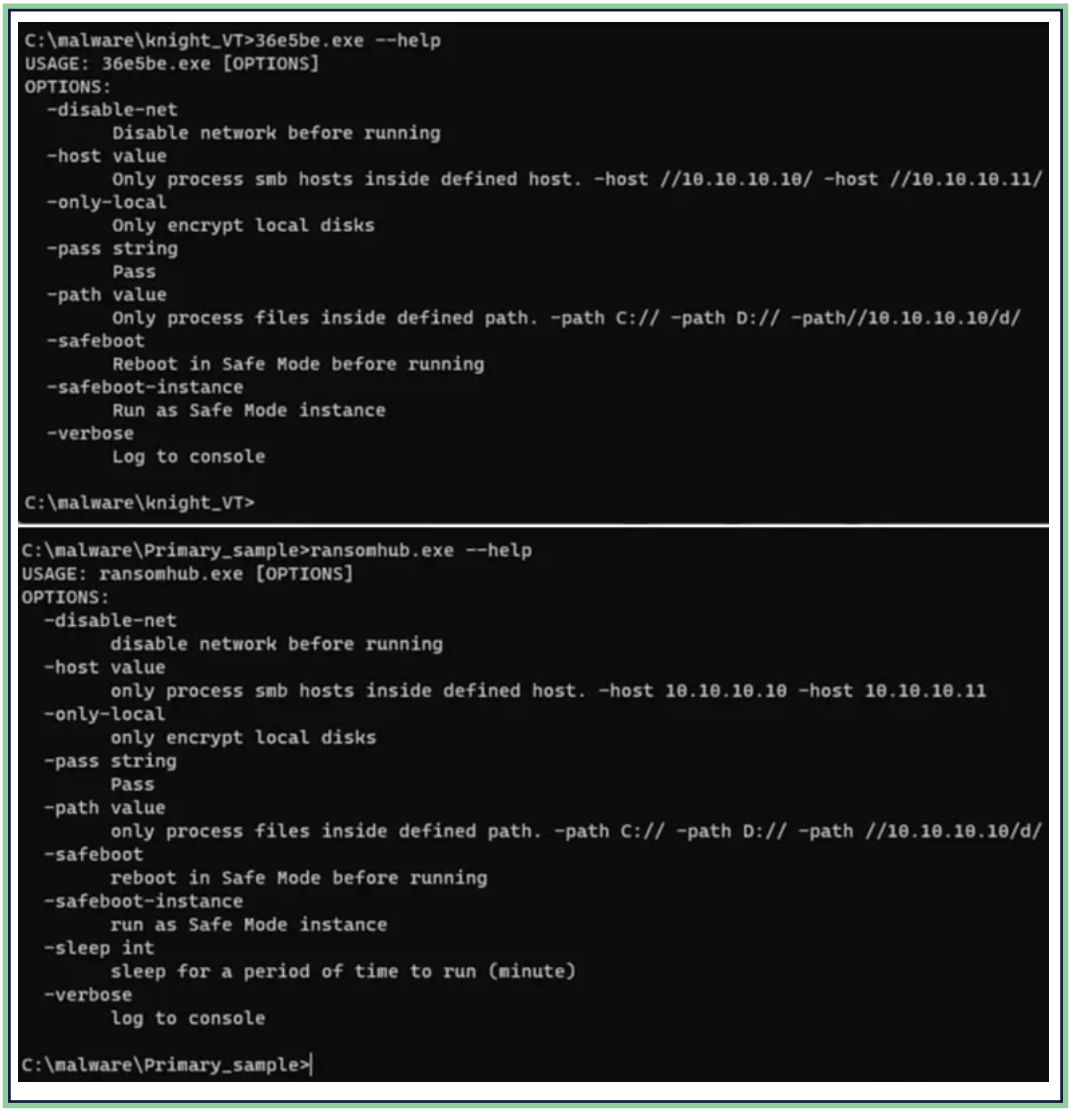

Figure 8: Similarities between Knight ransomware and RansomHub

EDRKillShifter

The RansomHub group has started to deploy a new malicious tool designed to disable Endpoint Detection and Response (EDR) solutions, allowing them to bypass security measures and gain full control over targeted systems. The tool, named EDRKillShifter, was uncovered by Sophos, following a failed attack in May 2024. EDRKillShifter functions as a bootloader, enabling a Bring Your Own Vulnerable Driver (BYOVD) attack, where a legitimate but vulnerable driver is exploited to elevate privileges, disable security features, and take control of the system.

Sophos identified two distinct EDRKillShifter samples, both leveraging publicly available proof-of-concept exploits from GitHub. One sample targets the vulnerable RentDrv2 driver, while the other exploits the ThreatFireMonitor driver, part of an outdated system monitoring package. EDRKillShifter can load different drivers based on the attacker's requirements.

The execution process involves three steps: First, the attacker runs a binary file with a password to decrypt and execute a built-in BIN resource in memory. The code then decompresses and executes the final payload, loading the vulnerable driver to elevate privileges, disable active processes, and neutralize EDR systems. The malware then creates a new service for the driver, starts it, and loads the driver, entering an infinite loop in which it continuously monitors running processes and terminates them if their names match those on an encrypted list of targets.

Remote Ransomware Abilities

On July 18, the threat actor announced a significant update to the ransomware program (Figure 9). The group stated that affiliates would no longer need to upload the file locker to the victims' encrypted machines; instead, the new locker now supports remote encryption.

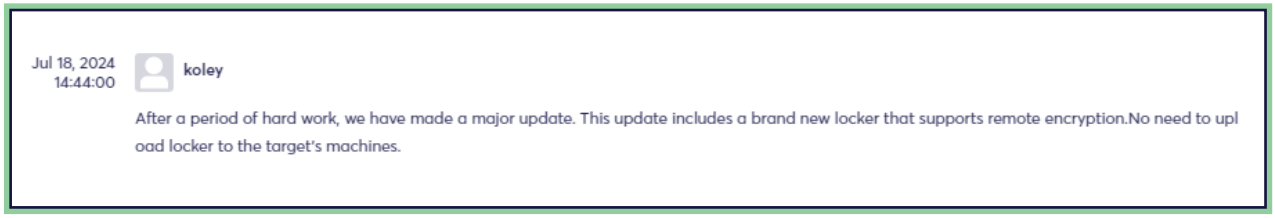

Figure 9: Koley's announcement about a major update

Remote encryption, also known as remote ransomware, occurs when a compromised endpoint is used to encrypt data on other devices in the same network. In October 2023, Microsoft reported that approximately 60% of ransomware attacks now utilize remote encryption to reduce their footprint, with over 80% of these compromises originating from unmanaged devices. This method has a key advantage: It bypasses process-based remediation measures, as managed machines are unable to detect the malicious activity that is confined to an unmanaged device. Additionally, host-based defenses on managed systems cannot identify the ransomware, since it resides solely on the unmanaged machine. The only sign of malicious activity is the transmission of documents.

Dark Web Activity

RansomHub primarily recruits affiliates from the predominantly Russian RAMP Forum, operated by a threat actor known as Koley. Cyberint's research team identified Koley as a representative of the RansomHub ransomware group, who regularly posts updates and guidelines for joining the affiliate program on the forum. In the past three months, Koley has made several notable announcements.

On May 1, Koley announced updates to the group's VIP version (RAAS), including file modification features and enhanced encryption methods.

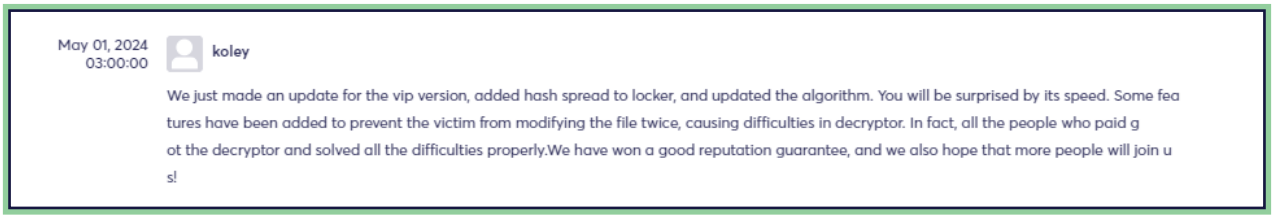

Figure 10: Another Koley announcement, this time on the VIP version

The threat actor also outlined the rules for joining the group, emphasizing that reputation on the forum, participation in the alliance's guarantee verification program, and other criteria are essential for membership. Additionally, starting June 21, threat actors without a forum account to verify their identity are required to pay a $5,000 deposit.

Koley also reiterated that sharing samples and screenshots of the affiliates' personal panels with others is strictly prohibited and can result in the panel being disabled and the forfeiture of their deposits.

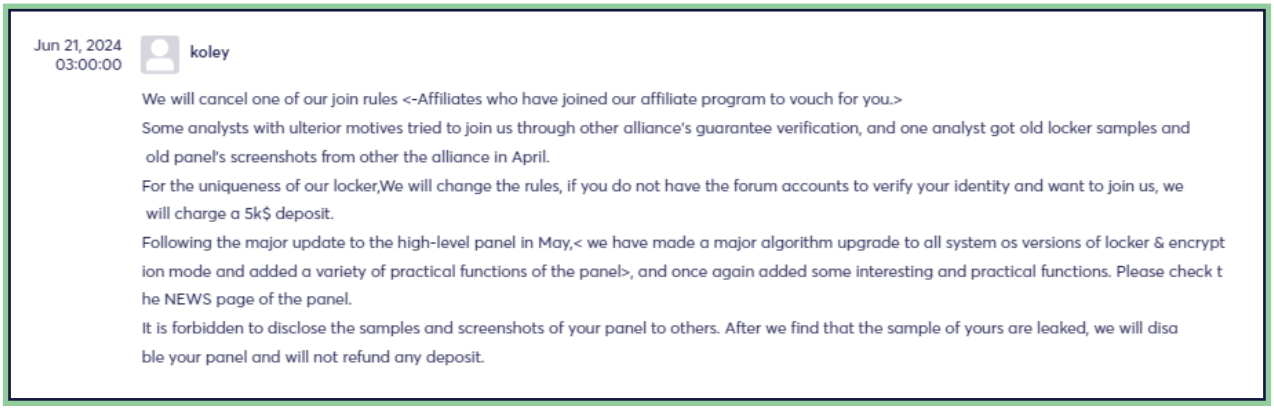

Figure 11: Koley outlines the rules for joining the group

A significant update regarding ransomware remote encryption was posted by Koley on July 18 as we seen in Figure 8 followed by a further update six days later, focusing on the fast mode of encryption.

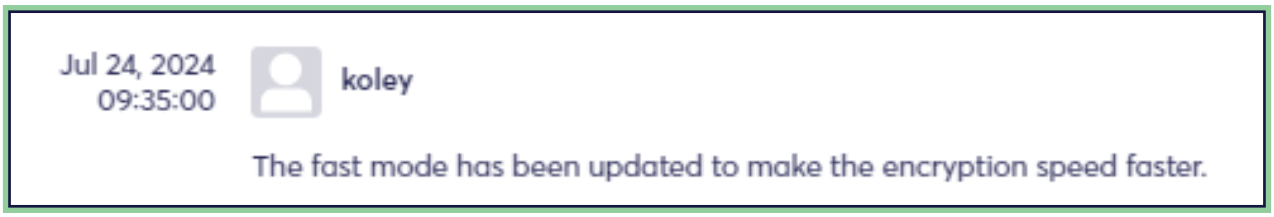

Figure 12: Another significant update by RansomHub

Conclusion

RansomHub has quickly risen to prominence in the ransomware landscape, capitalizing on the disruption of major players like ALPHV and LockBit. With its roots likely in Russia and connections to former ALPHV affiliates, the group has established itself as a formidable force by leveraging its Ransomware-as-a-Service (RaaS) model, which offers attractive profit-sharing terms to affiliates. This approach has led to a surge in attacks, particularly in July and August 2024, when over half of their total attacks have taken place.

Despite a low ransom payment rate—only 11.2% of victims have paid—the group's strategy focuses on volume rather than individual payouts. The growing number of affiliates and the corresponding increase in attacks ensure continued profitability, even if only a small fraction of victims pay. The group's victimology reflects a traditional Russian ransomware operation, avoiding targets in CIS, Cuba, North Korea, and China, while primarily focusing on organizations in the United States and Brazil.

From a financial perspective, RansomHub's victims span a wide range of company sizes and revenues. The average revenue of the attacked organizations is around $444 million, though the majority (84%) of victims are smaller organizations with revenues below $100 million. When excluding the few large organizations with over $1 billion in revenue, the average drops significantly to $59.68 million. Furthermore, 60% of the victims are small companies with fewer than 100 employees, highlighting the group's broad targeting strategy.

In conclusion, RansomHub's rapid growth, attractive affiliate program, and deliberate targeting strategies position it as a significant contender in the evolving ransomware landscape. Cyberint is highly confident that RansomHub is striving to establish itself as a dominant RaaS leader in the near future.

Mitigations

Ransomware attackers don't openly share their identities, motives, or strategies like legitimate businesses do, and there are no quarterly reports or press conferences. However, they do leave behind valuable information that skilled analysts can use to profile their operations and mitigate threats—exactly what we specialize in at Cyberint. By focusing on broad defense strategies rather than tracking numerous similar threat groups, organizations can strengthen their resilience against ransomware. Following are some key mitigation steps:

- Regular Data Backup: Establish a comprehensive backup strategy to ensure critical data is regularly backed up and readily available for recovery in the event of a ransomware attack.
- Security Awareness Training: Educate employees on ransomware threats, phishing tactics, and cybersecurity best practices to minimize the likelihood of falling victim to attacks.
- Patch and Update Management: Regularly update operating systems, software, and applications with the latest security patches to address vulnerabilities that ransomware could exploit.
- Network Segmentation: Implement network segmentation to isolate critical systems and sensitive data from less secure areas, reducing the potential impact of a ransomware breach.
- Access Control: Enforce the principle of least privilege by restricting user access and privileges, minimizing the attack surface and limiting the spread of ransomware through the network.
- Email and Web Security: Deploy advanced email filtering and web security solutions to block malicious attachments, links, and phishing attempts that could deliver ransomware.
- Endpoint Protection: Utilize endpoint security solutions, including antivirus software, Intrusion Detection Systems (IDS), and Endpoint Detection and Response (EDR) tools, to detect and mitigate ransomware on endpoints.
- Incident Response Plan: Create and regularly test a ransomware-specific incident response plan that outlines procedures for identifying, containing, mitigating, and recovering from attacks.
- Regular Security Audits: Perform routine security audits, vulnerability assessments, and penetration testing to identify and address security gaps that could be exploited by ransomware attackers.

Contact Us

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

ISRAEL

Tel: +972 3-7286-777
17 Ha-Mefalsim St 4951447 Petah Tikva

UNITED KINGDOM

Tel: +44-203-514-1515
3rd Floor, Great Titchfield House
14-18 Great Titchfield Street,
London, W1W 8BD

USA – TX

Tel: +1-646-568-7813
7250 Dallas Pkwy STE 400
Plano, TX 75024-4931

SINGAPORE

Tel: +65-3163-5760
135 Cecil St. #10-01 MYP PLAZA 069536

USA - MA

Tel: +1-646-568-7813
22 Boston Wharf Road Boston, MA 02210

JAPAN

Tel: +81-3-3242-5601
27F, Tokyo Sankei Building, 1-7-2 Otemachi,
Chiyoda-ku, Tokyo 100-0004

ABOUT CYBERINT

Cyberint, the Impactful Intelligence company, reduces risk by helping organizations detect and mitigate external cyber threats before they have an adverse impact. The Cyberint Argos platform's patented technology provides superior visibility through continuous discovery of the evolving attack surface, combined with the automated collection and analysis of vast quantities of intelligence from across the open, deep and dark web. A team of global military-grade cybersecurity experts work alongside customers to rapidly detect, investigate, and disrupt relevant threats – before they have the chance to develop into major incidents. Global customers, including Fortune 500 leaders across all major market verticals, rely on Cyberint to protect themselves from an array of external risks, including vulnerabilities, misconfigurations, phishing, impersonation attacks, malware infections, exposed credentials, data leaks, fraud, and 3rd party risks.

For more information visit: https://Cyberint.com.