2024

RANSOMWARE RADAR REPORT

Rapid7 Labs

CONTENTS

EXECUTIVE SUMMARY

The first half of 2024 has witnessed a substantial evolution in the ransomware ecosystem, underscoring significant shifts in attack methodologies, victimology, and cybercriminal tactics. Rapid7 Labs has tracked more than 2,570 ransomware incidents so far this year, equating to an average of 14 publicly-claimed incidents per day. Since many incidents continue to go unreported, the actual numbers are likely much higher.

2,570+

in the first half of 2024

14

publicly-claimed incidents per day

Ransomware knows no borders and neither do the groups unleashing it. Rather than picturing these groups as a collection of individuals in hoodies, we must extend our collective imagination to fathom the international business model that delivers the end product — ransomware — to our doorsteps.

This research report provides a comprehensive analysis of ransomware incidents and binaries recorded and gathered globally, offering insights into trends, attacker profiles, ransomware families, and the implications for cybersecurity defenses.

The data used for this report comes from Rapid7's incident response teams and independent Rapid7 Labs research. The ransomware sample dataset we used consists of (i) prevalent and available ransomware families from 2023 which continued their operations into 2024, and (ii) new 2024 ransomware samples that were observed until the end of June, 2024.

KEY FINDINGS:

WELCOME TO THE PARTY: Within the first six months of 2024, Rapid7 observed **21 new ransomware groups entering the scene**. Some of these groups are brand new while others are previously known groups rebranding under a new name. One of the most notable of these new groups, RansomHub, has quickly established itself as a prominent extortion group by **making 181 posts to its leak site between February 10 and June 30, 2024.**

BUSINESS IS STRONG: The number of ransomware groups actively posting to leak sites is increasing, from an average of 24 groups posting per month in the first half of 2023 to **40 per month** in the same time period of 2024. Furthermore, 68 ransomware groups made a total of **2,611 leak site posts** between January and June, representing a **23% increase over the number of posts** made in the first half of 2023. While law enforcement efforts are making an impact (we see a drop in LockBit activity in June related to this), the carrot still appears to be much larger than the stick.

A $5MM SWEET SPOT: In examining the revenue distribution of companies listed within access broker postings, Rapid7 noted that companies with annual revenues around **$5 million are falling victim to ransomware** twice as often as those in the $30-50 million range and five times more frequently than those with a $100 million revenue. This finding could suggest that such companies are large enough to hold valuable data but not as well protected as their larger counterparts.

QUALITY OVER QUANTITY: The number of unique ransomware families observed in public incidents has decreased since the beginning of 2022. **Between 2022 and 2023, the number plummeted from 95 to 43 (-55%)**, and thus far in 2024 we have seen 23. Based on this, we can anticipate ransomware groups placing their focus on more specialized and highly effective ransomware variants to support their extortion operations.

THERE'S A KIT FOR THAT: Leaked builder kits and source code are facilitating the construction of many of today's ransomware strains. Rapid7 researchers used the Machoc Hash to uncover **3 major clusters of ransomware sharing substantial portions of code**. This signals the utilization of common builders as well as possible code exchange between different threat actors.

RANSOMWARE GROUP TRENDS

While seasoned gangs like LockBit have continued their disruptive activities, the rise of new groups in the first months of 2024 highlights the appeal of this cybercrime model. The ransomware success formula is still working and still attracting cybercriminals to start and/or participate in these operations. It's clear that the financial gain continues to outweigh the risk of being arrested.

In the first six months of 2024, Rapid7 observed 21 new or rebranded groups entering the scene. These groups are, in alphabetical order:

- 2023LOCK
- ALBABAT
- APT73
- ARCUS MEDIA
- BLACKOUT
- BRAIN CIPHER
- DONEX
- FSOCIETY
- FOG
- HELLOGOOKIE
- INSANE
- QIULONG
- RABBIT HOLE
- RANSOMHUB
- RED
- SENSAYQ
- SLUG
- SPACE BEARS
- TRINITYLOCK
- TRISEC
- ZERO TOLERANCE

Our analysis of these groups and the victim names they post on their leak sites found the following sectors targeted, with most individual groups not choosing favorites:

- HEALTHCARE & PHARMACEUTICALS
- TECHNOLOGY & IT SERVICES
- GOVERNMENT & PUBLIC SECTOR
- FINANCE & INSURANCE
- TRANSPORTATION & LOGISTICS
- AGRICULTURE
- EDUCATION
- MANUFACTURING
- RETAIL

An example of a completely new group that surfaced in April is FSociety, with their ransomware called FLocker. The group has its leak site on Tor, but it is also active on its own Telegram channel.

FSociety's message is clear: They want to build out their "business" and offer commission percentages to insiders willing to provide access to them.

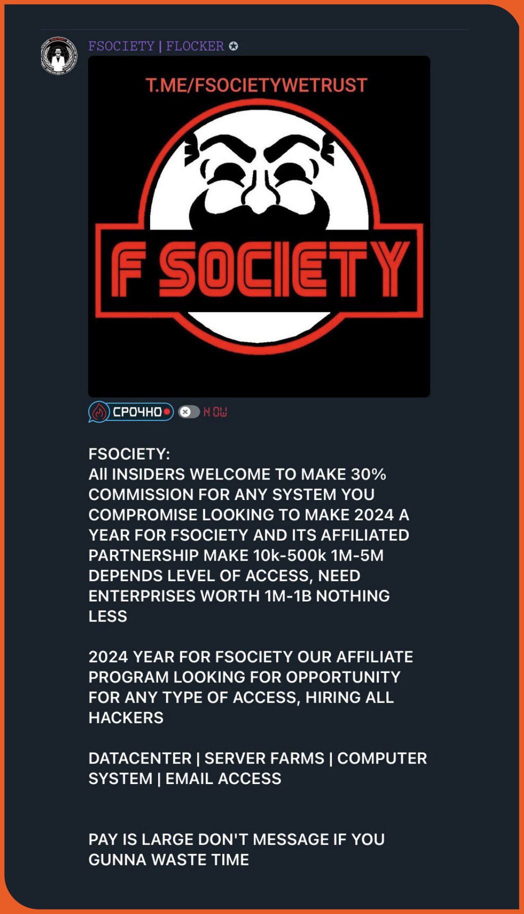
Digging more into their messaging, affiliates need to go through an "interview" to test if they are capable and suitable for this operation.

And if the whole business was not already very similarly run to a commercial business, they even run a bug bounty program offering high rewards to those who find vulnerabilities or errors in their infrastructure or code.

Once the first victims appeared on their leak site, the group posted additional guidance to which countries and sectors they prefer to target. Unfortunately, this is a group that doesn't hesitate to attack the healthcare and medical services sector.

Groups that rebrand under a new name typically do so as a result of ongoing actions by global law enforcement against them. From a rebrand perspective, there has been much speculation about the exit scam of the ALPHV group after they received a large ransom payout from a healthcare provider. Following this exit scam, a new group suspiciously surfaced at the end of February called RansomHub.

While some were quick to draw a link between the ending of ALPHV and the beginning of RansomHub, the technical evidence shows the two groups are likely not associated. On underground forums and posts from RansomHub themselves, it appears that affiliates operated with a different group of actors. Also, when comparing code between the two groups, there are some similarities but not enough to convincingly prove the rebranding.



FSOCIETY:
All INSIDERS WELCOME TO MAKE 30% COMMISSION FOR ANY SYSTEM YOU COMPROMISE LOOKING TO MAKE 2024 A YEAR FOR FSOCIETY AND ITS AFFILIATED PARTNERSHIP MAKE 10k-500k 1M-5M DEPENDS LEVEL OF ACCESS, NEED ENTERPRISES WORTH 1M-1B NOTHING LESS

2024 YEAR FOR FSOCIETY OUR AFFILIATE PROGRAM LOOKING FOR OPPORTUNITY FOR ANY TYPE OF ACCESS, HIRING ALL HACKERS

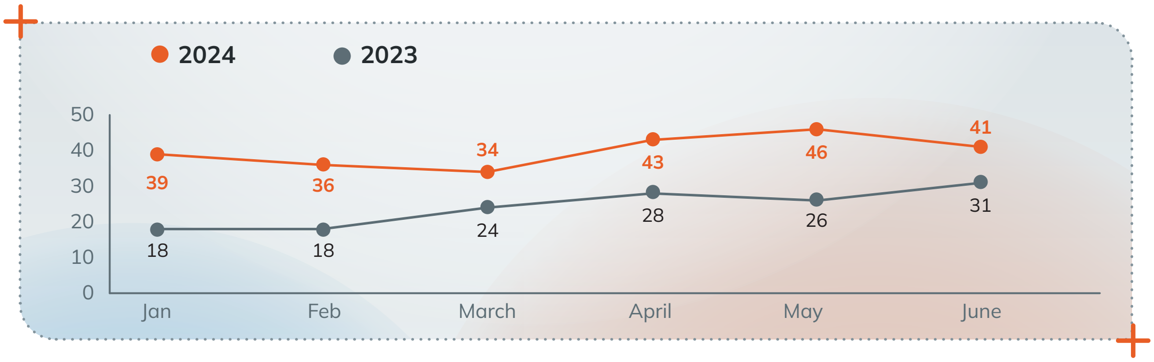
DATACENTER | SERVER FARMS | COMPUTER SYSTEM | EMAIL ACCESS

PAY IS LARGE DON'T MESSAGE IF YOU GUNNA WASTE TIME

An examination of active groups

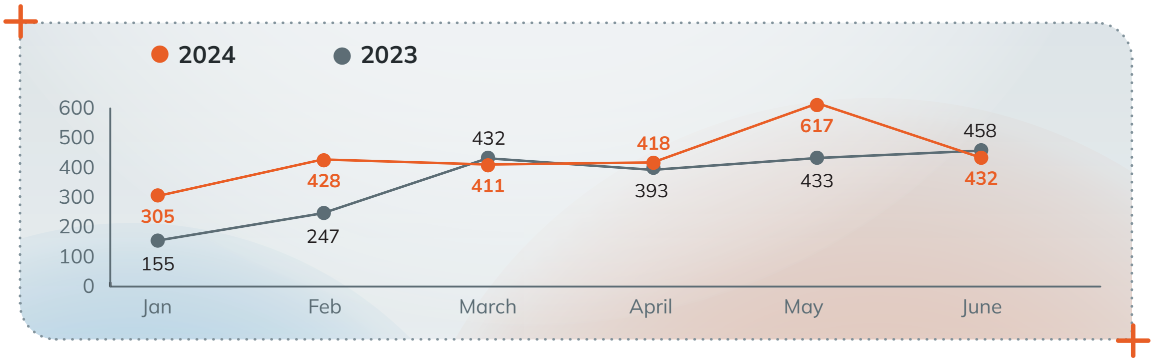
Over the course of the first half of 2024, Rapid7 observed a total of 68 distinct ransomware groups actively posting ransomed datasets to their individual leak sites at one point or another. Each of these posts represents an extortion attempt against an individual organization.

Looking at only the active groups by month, and comparing those numbers to the same period last year, we see the following:



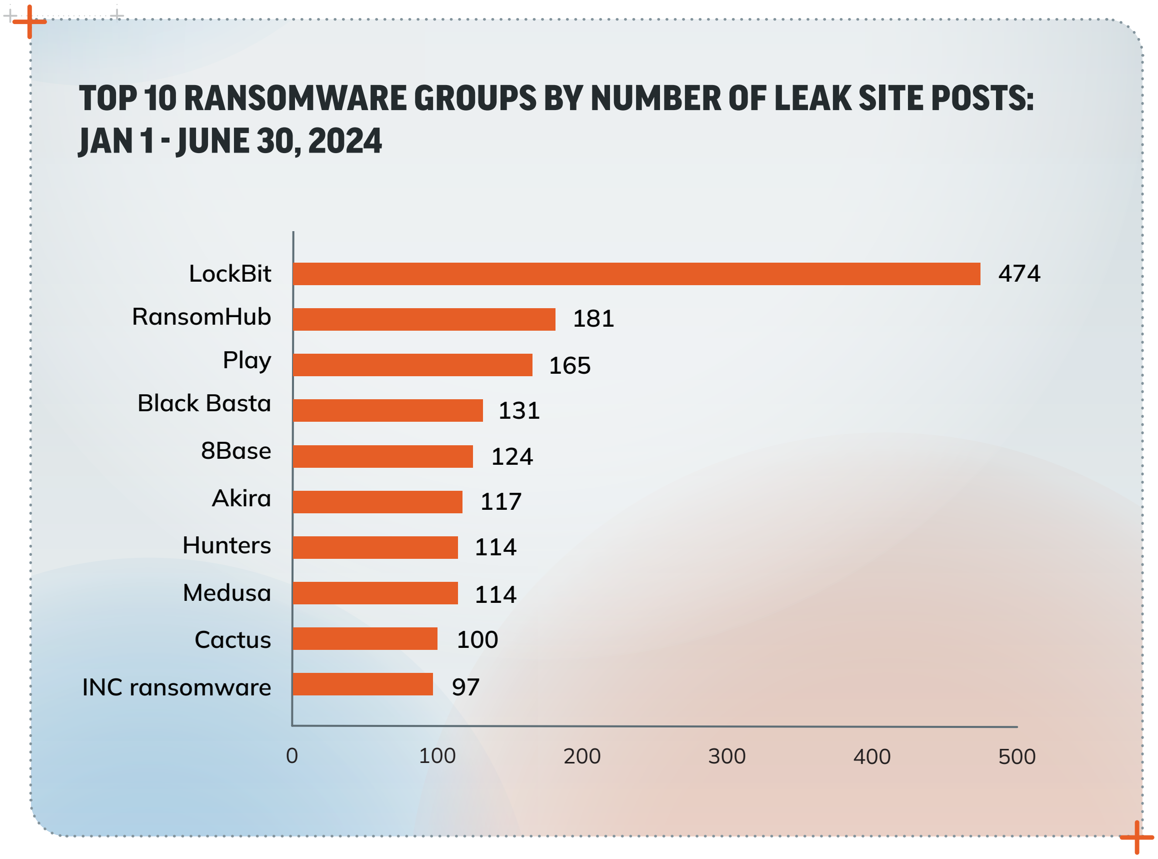
This comparison reveals that there has been a sizable increase in the number of ransomware groups actively posting to leak sites on a monthly basis. In the first half of 2023 there was an average of 24 groups posting per month, as opposed to 40 in the first half of 2024 — that's a 67% upsurge.

The graphic below shows the month-by-month total number of leak site posts, for January through June, 2023 and 2024.



Looking closely, we see that the total number of posts for the first half of 2024 was 2,611, which represents a 23% increase over the same time period last year where there were a total of 2,118 leak site posts.

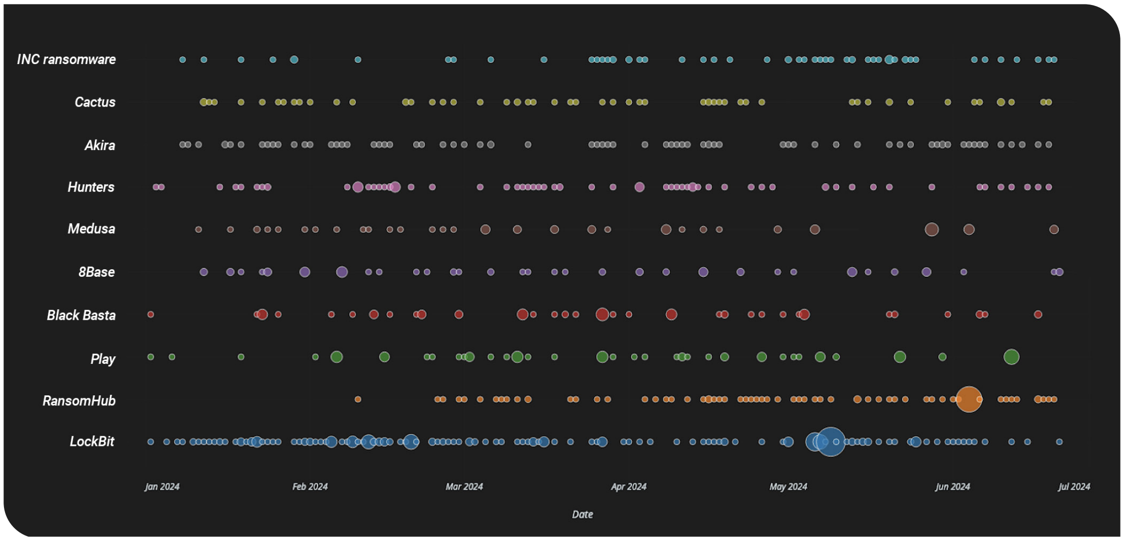
Now, let's look at the top 10 ransomware groups in terms of number of leak site posts in 2024.



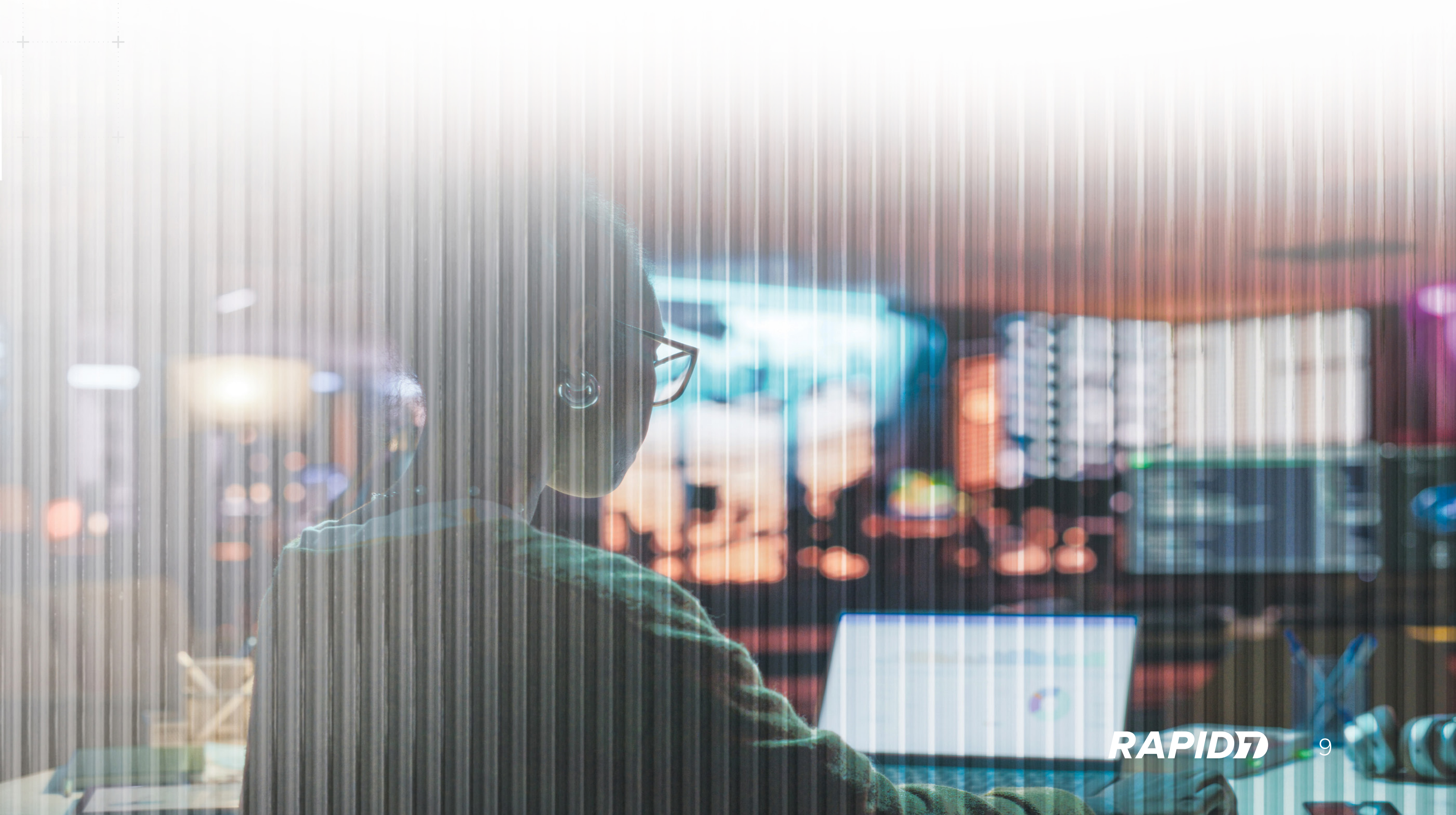
The first thing that clearly stands out is the commanding lead held by LockBit — no one else comes close. LockBit was by far the most active group, with 474 leak site posts in the first half of 2024 (162% more posts than the second-most active group, RansomHub). Play was the third-most active group and behind them with 131 posts was Black Basta, which Rapid7 recently linked to an ongoing social engineering campaign.

We can also look at how these top 10 groups have posted over time via the following scatter plot:

DISTRIBUTION OF POSTS OVER TIME BY TOP 10 GROUPS

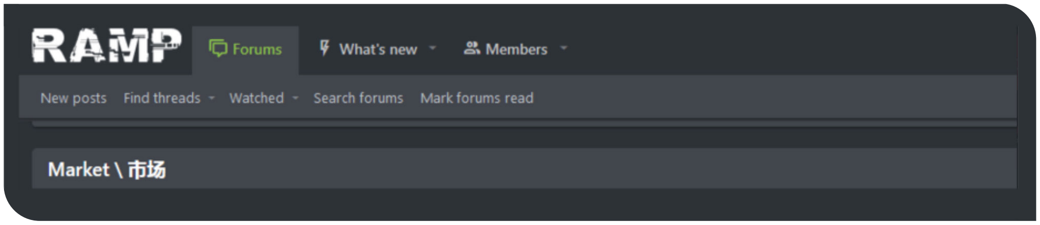


The first observation is that the posting frequency of the LockBit group became less frequent in June. We can speculate that their operations were impacted by law enforcement making decryption keys available. We can also see in the chart where the RansomHub group began its activity in early February and began posting on a regular basis later that month, with a burst of activity in early June.



KNOCK KNOCK... INITIAL ACCESS

Ransomware begins with initial access, and access brokers are the life's blood of underground forums. One of the most well-known forums playing host to access brokers is the RAMP (Ransomware and Advanced Malware Protection) forum, an underground cybercriminal hub originally known as Payload.bin that was re-launched/branded in 2021. With a primary focus on ransomware, RAMP is a multilingual platform catering to Russian, Chinese, and English speakers and boasts over 14,000 registered members.



RAMP serves as both a forum and a marketplace, offering ransomware kits, malware, and stolen data, while also providing comprehensive guides and tutorials for cyberattacks. It facilitates ransomware-as-a-service (RaaS) operations, enabling affiliates to deploy ransomware for a share of the profits.

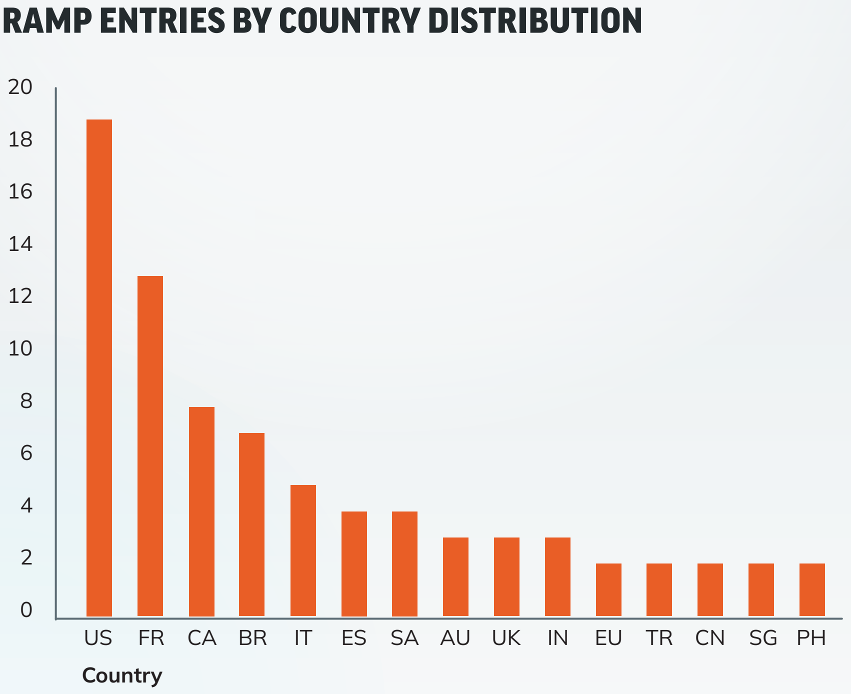
Despite its $500 registration fee, a stark contrast to the $120 annual fee for premium XSS users, RAMP's closed community is a critical resource for many threat actors. The forum's design mimics Silk Road-like darknet markets, including escrow features, and it operates primarily off-the-record to avoid law enforcement detection. Its administrator claims an annual revenue of around $250,000, benefiting from its predominantly Russian user base and a strict policy against selling certain illegal goods and services.

To investigate the trends and context around the selling of access to corporate networks, we analyzed all the postings on the RAMP forum from January to June 2024. Some of these posts were cross-posted on other underground forums as well.

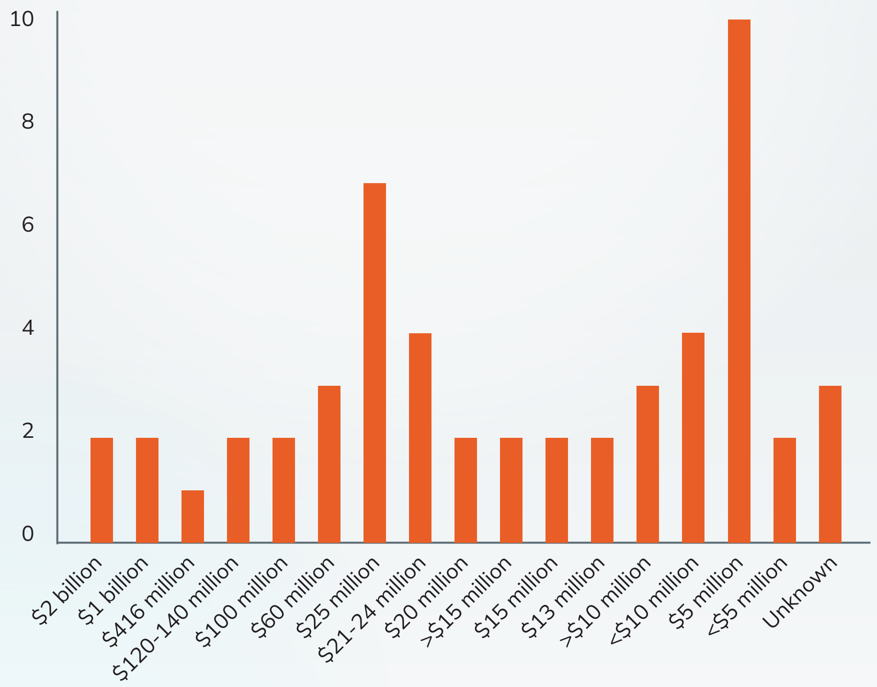
Company revenue, headquarter location, and the type of access are each a basis for how the threat actor formulates their asking price, which can range widely based on the perceived value of the target network. It is common for prices to spike based on the specific attributes of the target (e.g., revenue, security posture, type of data accessible).

Key insights from our RAMP analysis are as follows:

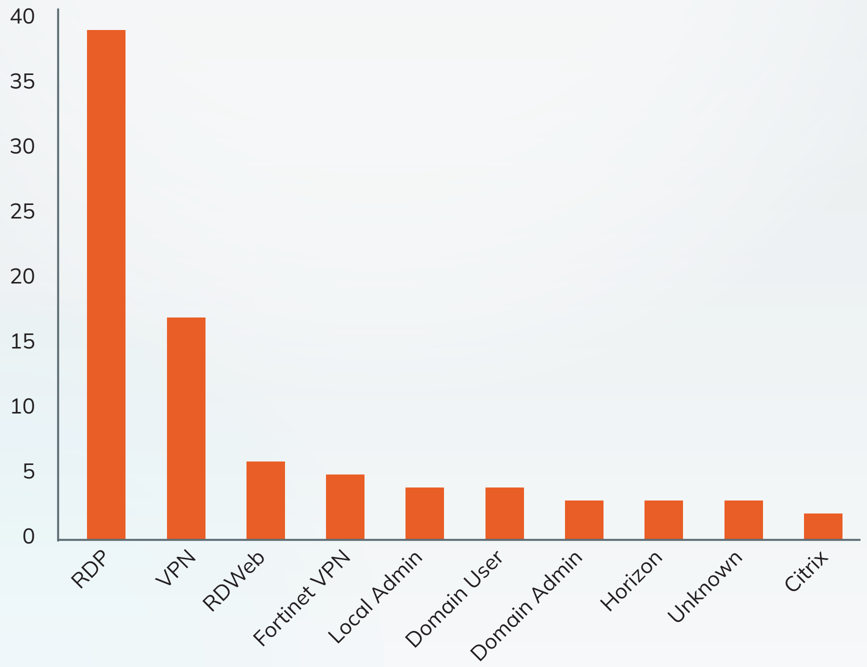
- **Revenue Distribution:** Companies with revenues in the $5 million range appear twice as often as those in the $30-50 million range and 5 times more frequently than those with a $100 million revenue. This could indicate that such companies are large enough to hold valuable data but perhaps not as well protected as larger corporations. Regardless, this finding shows that companies with $5 million in revenue are attractive targets and represents an interesting shift from access brokers only targeting the "big fish."
- **Access Type Distribution:** Remote Desktop Protocol (RDP) is the most common access type, followed by VPN. VPN presents a greater possibility of remaining undetected. That, in combination with the level of access (user or privileged user), demands a higher price. RDP is often used for remote work and system management, and it can be a significant vulnerability if not properly secured. The prevalence of RDP underscores the importance of securing remote access points.
- **Country Distribution:** Companies based in Western countries command a higher price due to their perceived wealth and easier access to resources for payment. Thus far in 2024, the high-to-low distribution of entries referencing the country of the company to which attackers have credentials or access is what would be expected. The only exception to this is Brazil, likely due to Brazilian affiliates that target larger Brazilian businesses.



RAMP ENTRIES BY REVENUE DISTRIBUTION



RAMP ENTRIES BY ACCESS TYPE DISTRIBUTION

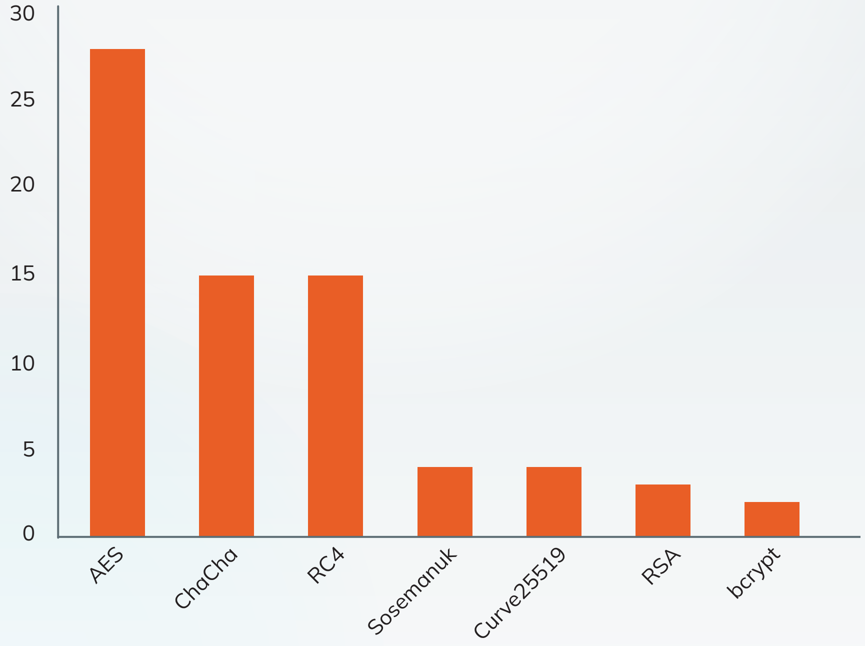


ENCRYPTION ALGORITHM TRENDS

One of the basic actions of ransomware is the encryption of essential data to extort payment for decryption keys. Our investigation focused on these encryption mechanisms to identify trends and patterns. Through examining the variety and intricacy of encryption techniques in our sample set, our study seeks to offer insights into the current tactics employed by cybercriminals.

Based on our analysis of the dataset, there were a total of seven encryption algorithms used by the ransomware samples. The following chart ranks these algorithms by their frequency of appearance:

FREQUENCY OF ENCRYPTION ALGORITHMS USED BY RANSOMWARE FAMILIES



According to our sample set, the top 3 encryption algorithms are clearly the most popular among cybercriminals. Let's compare and contrast these algorithms.

AES (ADVANCED ENCRYPTION STANDARD)

Unlike ChaCha and RC4, AES is a block cipher that encrypts data in fixed-size blocks (128 bits) rather than a stream. It uses a set number of rounds to process the plaintext into ciphertext, with the number of rounds depending on the key size (128, 192, or 256 bits).

Security: AES is considered very secure, with no effective attacks known that are better than brute force. It is the de facto encryption standard used worldwide for secure data encryption.

Performance: AES is highly efficient on a wide range of hardware, with many modern CPUs offering built-in support for AES operations (e.g., AES-NI instruction set in Intel and AMD processors), which speeds up encryption and decryption processes considerably.

CHACHA

ChaCha is a high-speed stream cipher; it is part of the "Salsa20" family of ciphers designed by Daniel J. Bernstein. ChaCha operates by generating a pseudorandom stream of bits that is then XORed with plaintext to produce ciphertext.

Security: ChaCha is considered highly secure and has not been compromised to date. It is resistant to cryptanalytic (side-channel) attacks and is used in modern security protocols, including TLS and for disk encryption in Android devices.

Performance: It is designed for efficiency in software implementations, particularly on platforms without specialized cryptographic hardware, offering high speeds and good data throughput.

RC4

RC4 is a stream cipher that was more widely used in the past. It generates a pseudorandom stream of bits (keystream) which is then XORed with plaintext to produce ciphertext.

Security: RC4 is now considered insecure and vulnerable to several types of attacks, such as the Fluhrer, Mantin, and Shamir attack, which exploits weaknesses in the key scheduling algorithm of RC4. As a result, its use is generally discouraged and it has been phased out of many applications, including TLS.

Performance: RC4 was popular due to its simplicity and speed in software implementations, but security vulnerabilities have overshadowed its performance benefits.

The choice between AES, RC4, and ChaCha by ransomware actors would largely depend on their specific needs for security, speed, and stealth, as well as the environments they target. While AES offers unparalleled security and speed with hardware support, ChaCha provides excellent security and performance even on platforms without specialized hardware. The characteristics of ChaCha, combined with its ease of implementation, make it a rising candidate for becoming the top encryption algorithm being used.

While some may find it surprising that the less-secure RC4 ranks in the top 3 in terms of usage, seemingly going head-to-head with ChaCha, cybercriminals will still accept it for its simplicity and speed, particularly in less sophisticated ransomware strains targeting older or less secure environments.

A few words on Sosemanuk

Although our dataset had only four hits on the Sosemanuk encryption algorithm, we often observe this encryption algorithm being used in ransomware targeting Linux platforms. Sosemanuk is a stream cipher that combines elements of the SNOW 2.0 cipher with Serpent block cipher S-boxes for enhanced security and efficiency. It uses an initialization process with a key and initialization vector to set up its internal state, then generates a keystream that is XORed with plaintext to produce ciphertext. Known for its speed and low resource requirements, Sosemanuk is a popular choice for ransomware encryption due to its quick data encryption capabilities.

RANSOMWARE CODE INSIGHTS

While the number of unique ransomware families reported across 2023 incidents decreased by more than half, from 95 new families observed in 2022 to 43 in 2023, we were curious to see how things were looking thus far in 2024. An initial look finds 23 new, unique ransomware families as of June 30, but have leaked ransomware builders like HelloKitty and LockBit 3.0 impacted the scene?

95 new ransomware families observed in 2022 **43** in 2023

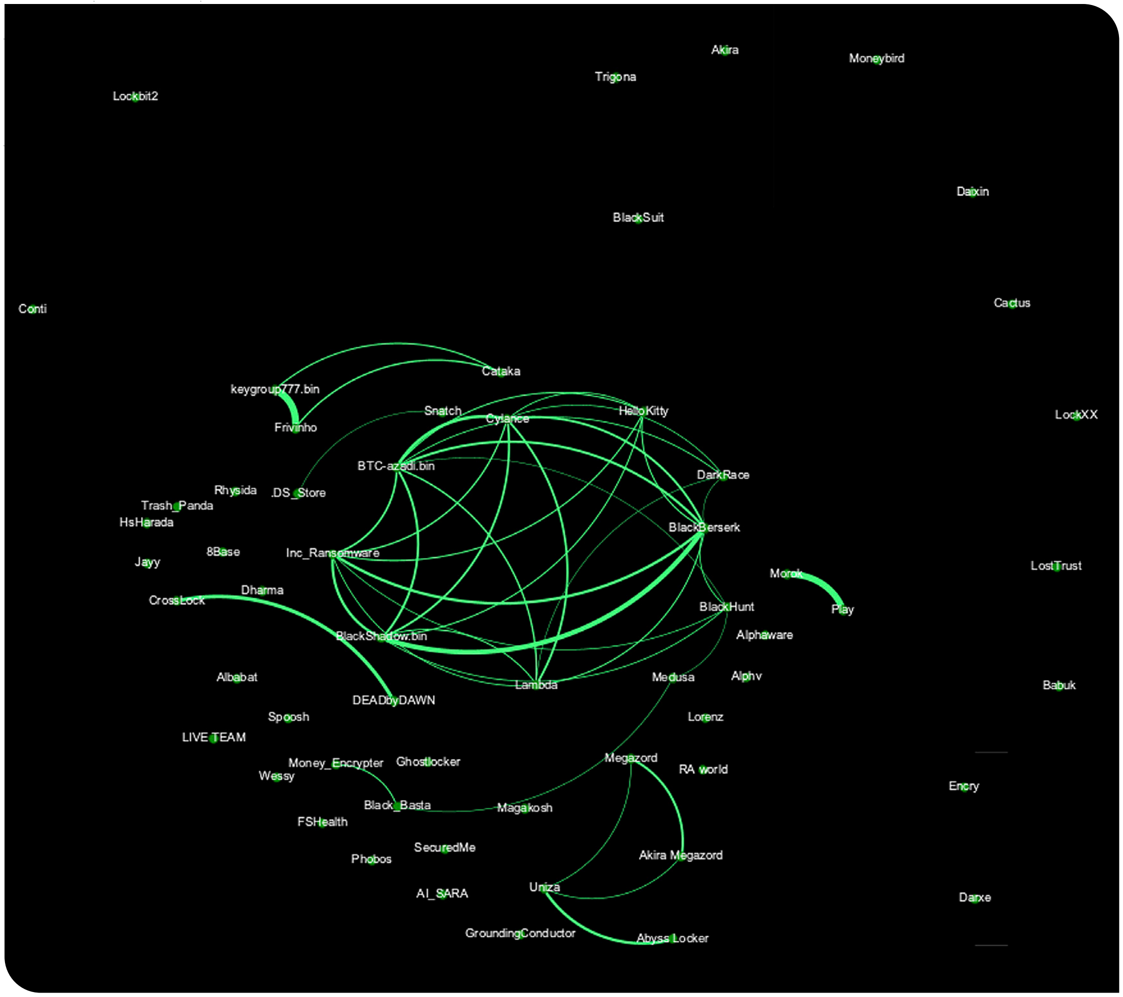
By using a sample set from ransomware samples observed being active in 2023 and 2024, we conducted a few comparisons.

First, we compared the set against strings using the Jaccard index. The Jaccard Index, also known as the Jaccard similarity coefficient, is a statistic used in understanding the similarity and diversity of sample sets. It measures the similarity between finite sample sets and is defined as the size of the intersection divided by the size of the union of the sample sets.

The Jaccard Index ranges from 0 to 1.

- **0:** Indicates no similarity (the sets do not share any elements).
- **1:** Indicates that the sets are identical (all elements are shared).

In our research as visualized below, the thicker the line is, the more similar the samples are, which may indicate that the ransomware family is derived from the other ransomware family or a builder has been used.

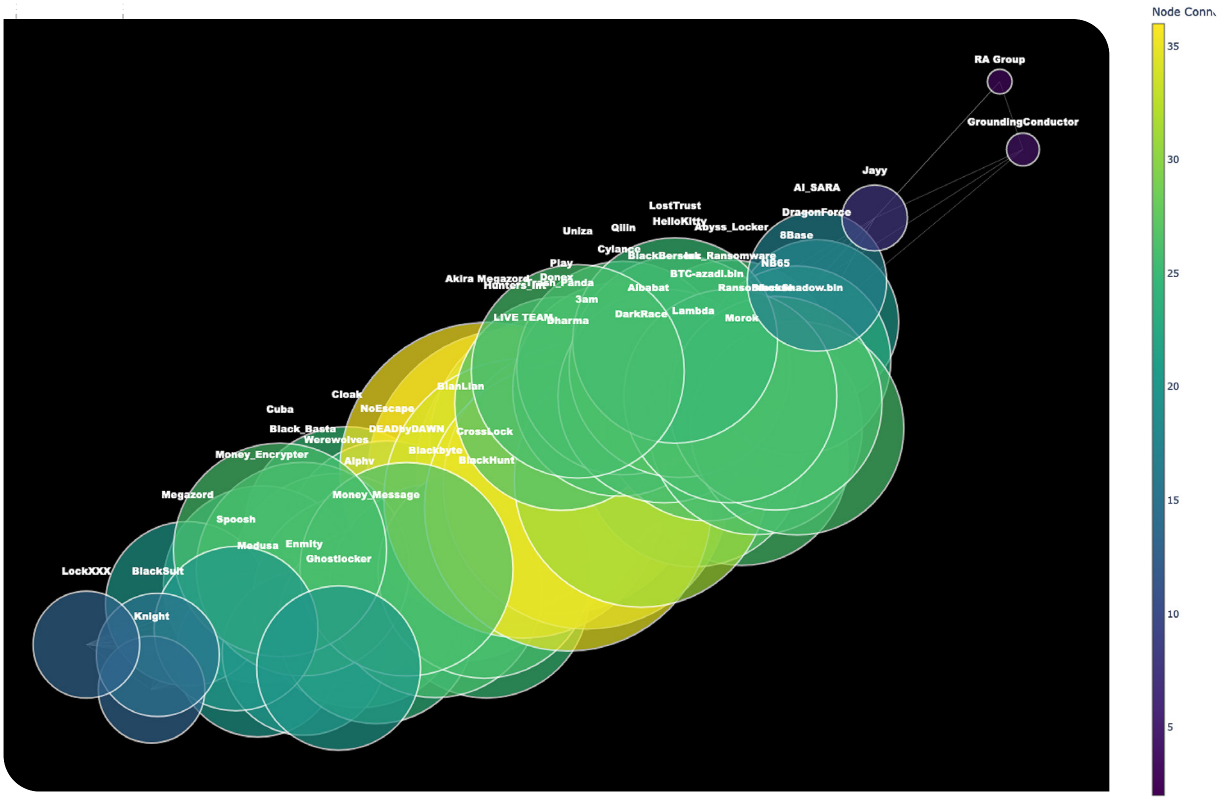


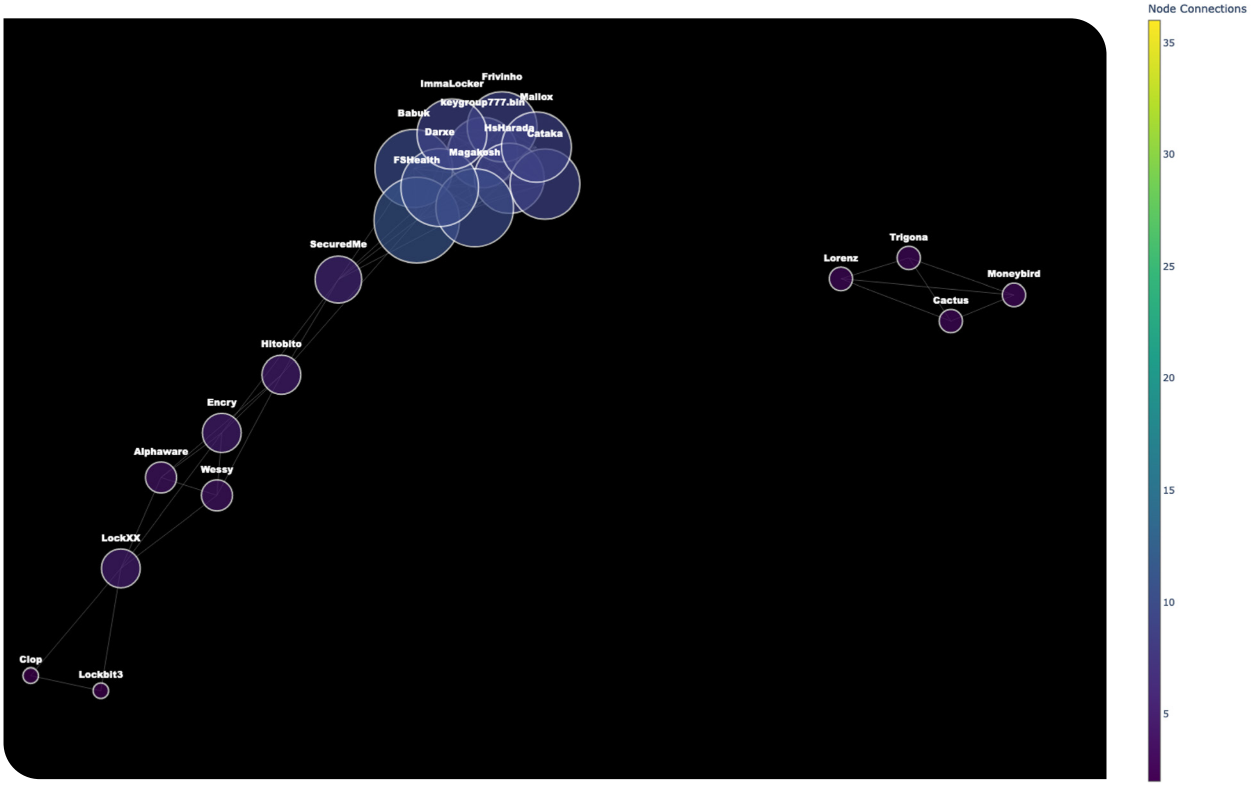
The string comparison reveals intriguing links between the ransomware families. An interesting discovery, for example, is the strong link between Play ransomware and the Morok ransomware family that surfaced in February 2024.

Although we acknowledge that string comparison of the ransomware is a nice start, let's take it a level deeper. The Machoc Hash, introduced by the French Cybersecurity Agency (ANSSI) as part of the Polychombr framework, is designed to compute a fuzzy hash of the Control Flow Graph (CFG). The CFG is a detailed representation of the function calls in binary, crucial for analyzing the underlying structure of software. To generate the Machoc Hash, it is necessary to disassemble every sample in our ransomware dataset to produce the CFG and then compute the hash.

The process used extracts the hash of the CFG and calculates the Jaccard distance between each generated Machoc Hash. This similarity metric is instrumental in identifying samples that share code, highlighting potential collaborations or reuse of the codebase within different samples.

In the following graphs, the similarity between ransomware families based on the above described process is visualized:





In this overview, we observe three major clusters that could be pointing to the (re)usage of source code, a builder, evolution of code in a particular ransomware family, or code exchange between groups. For example, in the first graph, where the biggest cluster is visualized, the brighter the color (yellows/greens) the more overlap in code was discovered. In the second graph, the colors are darker and there are some relations in the two clusters, but far less than in the first major cluster.

So, to answer our initial question: Yes, the leaked builders have impacted the 2024 scene, since now many threat actors have access to solid and proven ransomware builders which can be used as a basis for creating any number of new Frankenstein's Monsters.

From a detection engineering point of view, the clusters and additional information, such as the usage and type of encryption algorithms, help us uplevel hunting techniques and prevention, detection, and response technologies. Rapid7 continually investigates new techniques used by threat actors and ransomware operators, tests them against our patented Ransomware Prevention technology, and creates new preventions to ensure customers are protected against the latest threats.

Programming language/framework distribution

Rapid7 Labs researchers looked at the programming languages used across the ransomware samples prevalent in 2023, through June 2024. Among this dataset, only five languages are represented (where some could not be determined due to the way static analysis was performed). C and C++ are combined in our results where .Net is a framework and heavily connected to C#, we decided to use the .Net reference. C and C++ are still the top languages in which ransomware is written, however RUST is increasing in popularity.

C/C++	58 SAMPLES
.NET	13 SAMPLES
RUST	10 SAMPLES
GO	6 SAMPLES
BORLAND DELPHI	1 SAMPLE

CONCLUSION

While we can all agree that 2023 was an exceptional year in terms of the depth and breadth of ransomware attacks, the first half of 2024 has revealed that these unprecedented times continue. This report emphasizes the complexity of the ransomware business model, with groups coming and going, extortion tactics intensifying, builders and code "leaking" — and all the while, the overall scope of the threat only expanding.

The use of encryption algorithms like AES, RC4, and particularly ChaCha highlights a strategic choice by ransomware groups to optimize performance and security evasion. This evolution in encryption techniques aligns with the broader trend of cybercriminals adopting more sophisticated tools to enhance the effectiveness of their attacks.

Additionally, the report sheds light on initial access tactics, which remain a critical part of the ransomware attack chain. The frequent misuse of valid accounts (offered by access brokers in underground markets), as well as the exploitation of vulnerabilities and many businesses' insufficient application of multi-factor authentication (MFA) provide attackers with initial footholds. This aspect of the threat landscape calls for a rigorous reassessment of perimeter security and identity management practices within organizations.

Moreover, the continued decline in the number of unique ransomware families suggests a move toward more specialized and highly effective ransomware variants, solely extortion operations, rather than a broad array of less sophisticated malware. This shift indicates that ransomware groups are focusing on quality over quantity, refining their techniques, and utilizing proven tools that allow for targeted and disruptive attacks.

The report's insights into the ransomware landscape are crucial for informing cybersecurity strategies. Organizations must add proactive security measures like attack surface management and ransomware prevention technologies to their layered defense, which will further help mitigate the risk of initial access and subsequent ransomware deployment. As the ransomware threat evolves, so too must the strategies to combat it, requiring continuous vigilance and adaptation to these dynamic cyber threats.

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attacker methodology. Trusted by more than 11,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

RAPID7

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management

Application Security
Orchestration & Automation
Managed Services

To learn more or start a free trial, visit: https://www.rapid7.com/try/insight/

CONTACT US

rapid7.com/contact

The information provided in this report is intended for informational purposes only and Rapid7 makes no warranties, express or implied, regarding the suitability of the content for any specific purpose. The content within this report is based on data and findings available up to the date of its publication, which is mentioned within the document.

The information contained herein is provided "as is," and readers are advised to use their own discretion when applying the information to their specific situations. Furthermore, any third-party sources, tools, or software mentioned in this report are included for informational purposes only. Rapid7 does not take responsibility for the accuracy, functionality, or security of these external resources.

Rapid7 is not liable for any damages, losses, or consequences that may arise from the use of the information provided within. This includes but is not limited to direct, indirect, incidental, or consequential damages related to actions taken based on the content of this report.

Any reproduction, distribution, or unauthorized use of this report's contents without explicit permission from the authors and publishers is strictly prohibited.