

RANSOMWARE YEARLY REPORT 2024

January 2025

TABLE OF CONTENTS

EXECUTIVE SUMMARY	3
Q4 FUELS RISE IN RANSOMWARE ATTACKS	5
2024 STATS VS. 2023	8
NEWCOMERS	19
ARRESTS	24
NEW TRENDS	27
RANSOMWARE LANDSCAPE PREDICTIONS FOR 2025	30
CONCLUSIONS	31
CONTACT US	32

EXECUTIVE SUMMARY

In 2024, the ransomware landscape recorded **5,414 published attacks** on organizations worldwide, representing an

11%

increase
compared to
2023

The quarter with the highest number of incidents in 2024 was Q4 with

33%

of all ransomware
attacks for the year

46
New
Ransomware Groups

The top 10 groups were responsible for

52.8%

of all
attacks

Most targeted countries



US



Canada



UK



Germany



Italy



In 2024, the ransomware landscape recorded 5,414 published attacks on organizations worldwide, representing an 11% increase compared to 2023. While the year began with a decline in ransomware activity during Q1, the frequency of attacks surged in Q2 and continued to rise through the remainder of the year. This culminated in a dramatic spike during Q4, which saw 1,827 incidents—33% of all ransomware attacks for the year—making it the most active quarter. The year also brought significant developments, including law enforcement actions targeting large ransomware operations like LockBit in February 2024, resulting in arrests, identity revelations of group leaders, and the seizure of cybercriminal infrastructure.

The crackdown on major ransomware groups led to their fragmentation, fostering increased competition among smaller ransomware gangs and enabling other threat actors to gain prominence. This shift is evident in the rise of 95 active ransomware groups in 2024, a 40% increase from the 68 groups active in 2023.

Among the 46 new groups that emerged, RansomHub stood out as a dominant force, even surpassing the well-established LockBit in activity. These new entrants, such as FOG, Lynx, APT73, and Eldorado, have reshaped the threat landscape, accounting for a growing share of ransomware incidents. Notably, the top 10 groups were responsible for 52.8% of attacks, highlighting both the influence of newcomers (most of whom Cyberint, a Check Point Company, suspects are extremely professional due to previous affiliation with legacy groups) and a decline in the dominance of legacy groups.

Unsurprisingly, the U.S. remained the most targeted country, and the business services sector continued to bear the brunt of ransomware attacks, mirroring trends from 2023. The combination of established leaders like RansomHub, LockBit, Play, Akira, IncRansom, and Medusa, alongside the rise of new groups, had devastating consequences for global organizations. High-profile victims in 2024 included Deloitte, Volkswagen Group, Schneider Electric, and others, underscoring the persistent and evolving threat posed by ransomware.

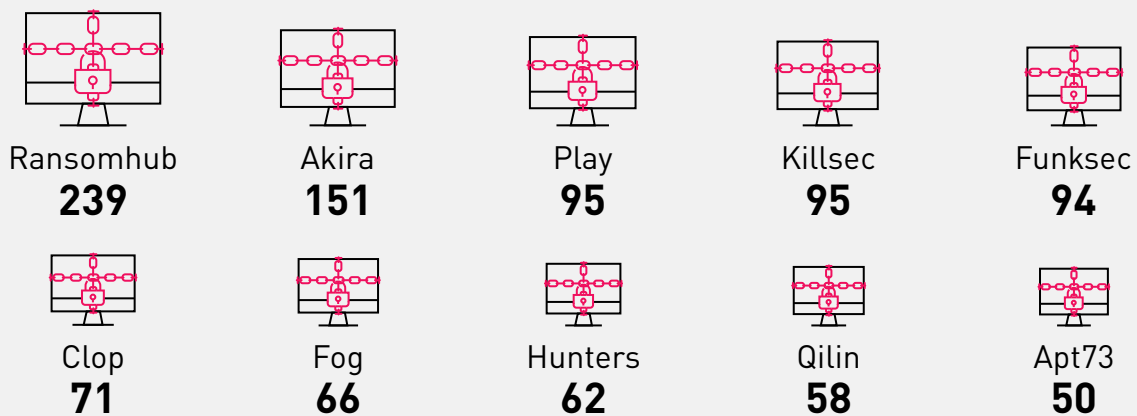
Q4 FUELS RISE IN RANSOMWARE ATTACKS

ACTIVE RANSOMWARE GROUPS

The fourth quarter of 2024 saw the highest number of ransomware attacks globally, with a staggering 1,827 incidents—a significant increase of approximately 30% compared to the previous three quarters. An intriguing observation is that the LockBit group, which ranked as the second most active ransomware group in 2023, did not even make it into the top 10 list for Q4. This decline can be attributed to law enforcement operations that significantly disrupted the group's activities throughout the year.

Additionally, it is notable that half of the top 10 ransomware groups of Q4 emerged in 2024, highlighting the rise of new players in the ransomware landscape. This shift underscores the dynamic and evolving nature of ransomware threats, with new groups quickly making their mark.

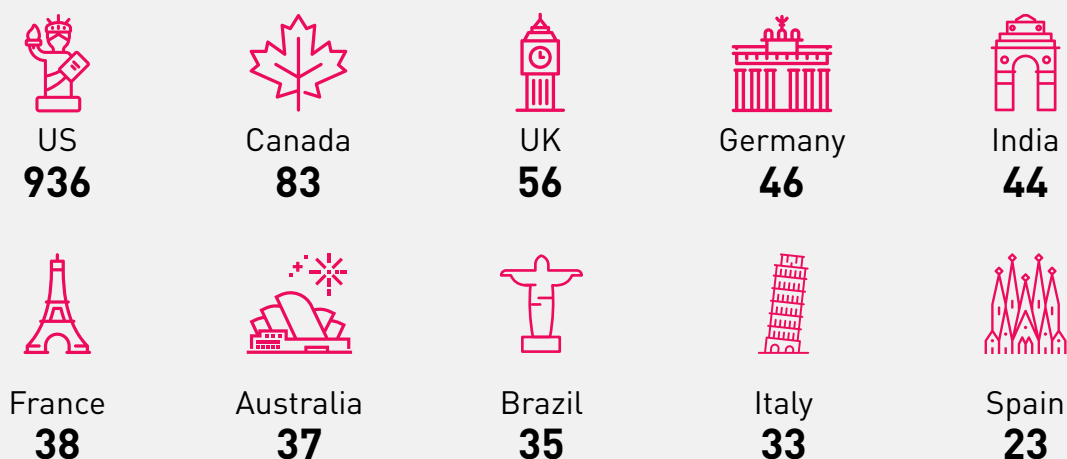
Top 10 Active Ransomware Groups in Q4 2024



TARGETED COUNTRIES

Unsurprisingly, the United States remained the most targeted country in the fourth quarter, experiencing 936 ransomware attacks within its borders. India, this quarter accounted for over 50% of the ransomware activity recorded throughout the entire year.

Top 10 Targeted Countries by Ransomware in Q4 2024

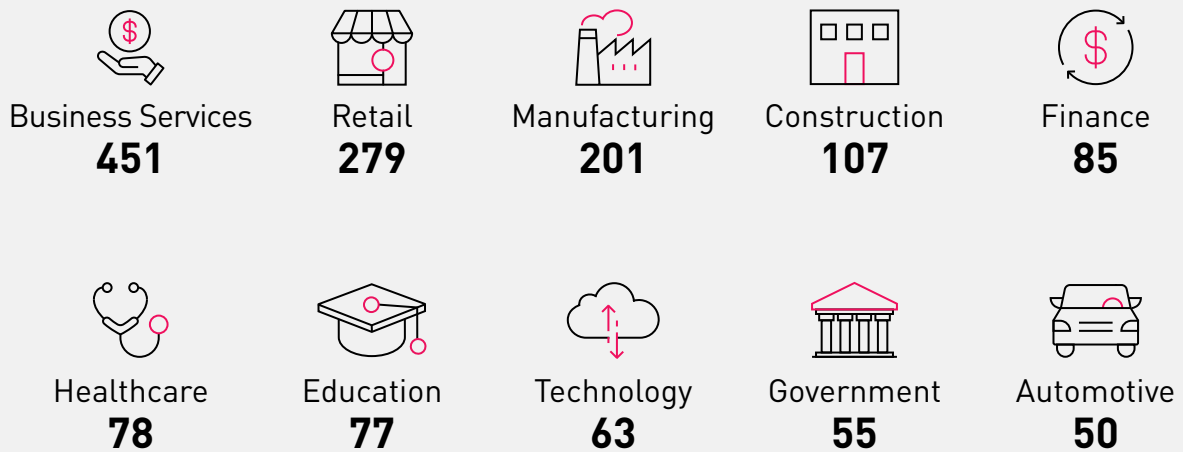


TARGETED SECTORS

As expected, the business services sector maintained its position as the most targeted industry in the fourth quarter of 2024, with 451 recorded attacks. The Q4 top 10 list closely mirrors the annual overview, with the notable exception of the automotive sector, which experienced 50 incidents during Q4 —accounting for over 30% of all ransomware activity in the industry for the entire year.

Additionally, the manufacturing sector, that ranked third in both the yearly and Q4 lists, saw a significant surge in ransomware activity during the last three months of the year. With 201 incidents in Q4, this accounted for approximately 35% of all attacks on the sector in 2024, highlighting the increasing focus on this industry by ransomware operators.

Top 10 Targeted Industries by Ransomware in Q4 2024



THE UPCOMING LOCKBIT4.0 – NEXT LEVEL RANSOMWARE

The LockBit ransomware group appears to be staging a comeback after months of diminished activity following its February 2024 takedown. On December 19, LockBitSupp, a persona allegedly linked to the group's Ransomware-as-a-Service (RaaS) administrators, announced the upcoming launch of LockBit 4.0. The announcement, posted on their website, included promotional messaging: "Want a Lamborghini, Ferrari, and lots of *\$%^ girls? Sign up and start your pentester billionaire journey in 5 minutes with us." The post also revealed a dedicated website, lockbit4[dot]com, five TOR links, and a release date of February 3, 2025.

A spokesperson from the Cyber Threat Intelligence Academy commented on social media, suggesting that the multiple TOR links indicate LockBit is bolstering its infrastructure for more robust operations. Vx-Underground, a collective of security researchers, reported that LockBitSupp provided them with free access to the program, along with code samples for reverse-engineering. This announcement comes nearly 10 months after Operation Cronos, a global law enforcement effort that dismantled much of LockBit's infrastructure and recovered 7,000 decryption keys. Notably, the group was believed to have been developing the 4.0 version of its ransomware even before the raid occurred.

CLOP RANSOMWARE RESURGES WITH MAJOR CLEO EXPLOIT AND FRESH EXTORTION CAMPAIGNS

The Clop ransomware group, also known as ClOp, has reemerged after a period of reduced activity. Active since 2019, Clop has historically targeted a wide range of industries, including healthcare, retail, energy, and finance. Following a series of large-scale attacks in 2023, which included 384 breaches, Clop's activity slowed in 2024, with only 27 victims reported until December. However, on December 24, Clop escalated its operations, targeting 66 companies impacted by a recent Cleo attack and giving them just 48 hours to comply with ransom demands. The group directly contacted victims through secure chat links and email, warning that unresponsive companies would have their names publicly disclosed. The above alleged victim list likely represents only a portion of the total victims, as some companies may not yet have been identified.

The resurgence is tied to Clop's exploitation of a zero-day vulnerability (CVE-2024-50623) in Cleo LexiCom, VLTrader, and Harmony products. This vulnerability enables remote code execution through unauthorized file uploads and downloads. Although a patch (version 5.8.0.21) has been released, researchers warn it may be bypassed. Clop confirmed its involvement in the Cleo attack and announced plans to focus on current extortion efforts by deleting data from previous breaches. With Cleo's software reportedly used by over 4,000 organizations globally, the scale of the impact remains uncertain. This incident highlights Clop's persistent reliance on exploiting zero-day vulnerabilities to execute large-scale data breaches and extortion campaigns, raising

Dear companies

Due to recent events (attack of CLEO)

all links to data of all companies will be disabled and data will be permanently deleted from servers.

We will work only with new companies

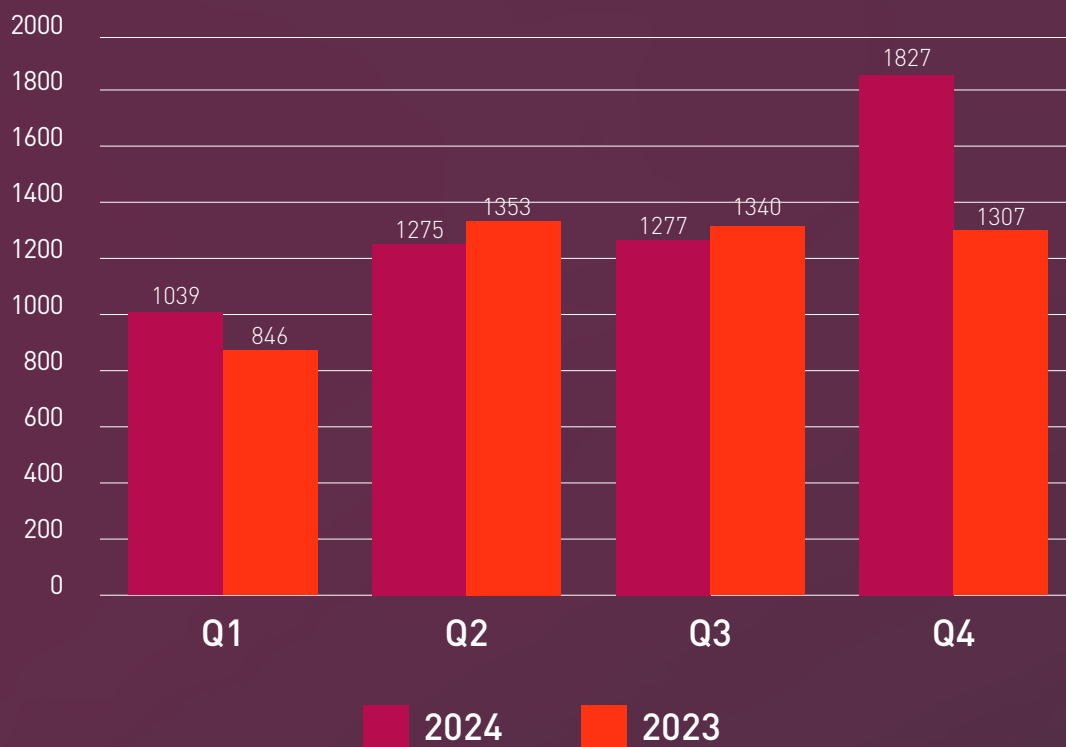
Happy New Year © CLOP^_

2024 STATS VS. 2023

According to our collection, the ransomware sector counted 5,414 published victims in 2024, reflecting an 11% increase compared to 2023. The fourth quarter of 2024 was particularly significant, with 1,827 published ransomware incidents, making it the most active quarter of the year and showing a 29% increase compared to the same period in 2023.

From a broader perspective, the second half of 2024 saw 46% more incidents than the first half and 17% more than the second half of 2023, highlighting a notable surge in ransomware activity during this period. This can be attributed to the significant jump in new professional groups potentially formed from experienced affiliates of legacy groups.

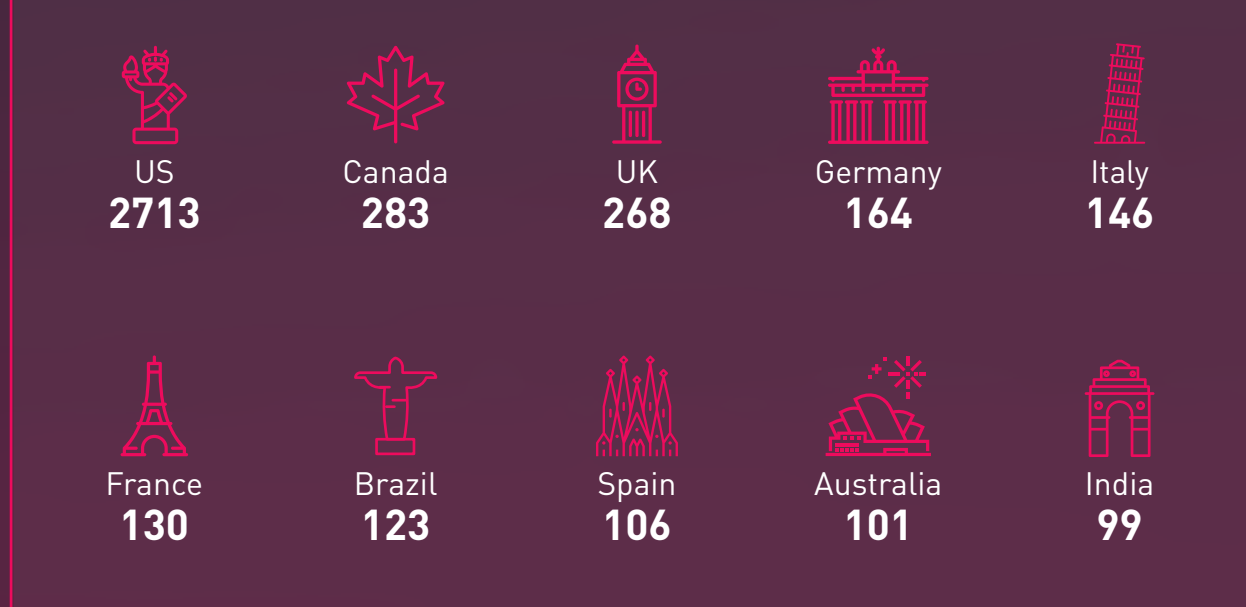
Quarter Comparison 2024 vs. 2023



TOP COUNTRIES

Regarding the most targeted countries, the U.S. remains the number one targeted country globally, with good reason. The world's number one economy was the victim of ransomware attacks this year in 50.2% of total cases, which is 2713 cases.

Top 10 Targeted Countries by Ransomware in 2024



The second most targeted country in 2024 is Canada, with 283 cases, far behind the U.S. Finally, the United Kingdom is in third place with 268 ransomware cases this year. Even when focusing on the top three countries, we can see that there is no doubt that the U.S. threat actors prefer the US due to reaping the most rewards there, be it reputation, financial or other reward.

In comparison to last year, the four most targeted countries in Europe – United Kingdom, Germany, Italy and France saw a dramatic decrease in the number of ransomware incidents in 2024, with 11%, 15%, 12% and 21% respectively.

The top 10 list for most targeted countries in 2024 remains nearly unchanged compared to 2023, with the only difference being the tenth position. India replaced the Netherlands, recording 99 incidents, a 38% increase from the previous year. Meanwhile, the Netherlands saw a decrease of 41 incidents, marking a 36% decline compared to last year.

UNITED STATES

The group that targeted the United States most was Play, with 283 ransomware incidents, approximately 80% of their entire attacks in 2024.

The most targeted industries in the United States were Business services, Retail, and Manufacturing with 736, 398, and 319 ransomware incidents respectively.



TOP SECTORS

As expected, the business services sector was the most targeted in 2024, with 24.1% of the ransomware cases, followed by the retail and manufacturing sectors, with 15.2% and 10.5%, respectively.

The construction industry should be a growing concern, as ransomware incidents increased by 50% 2024 vs. 2023. This surge jumped the construction industry to fourth place, overtaking the Financial, Education, and Healthcare sectors, that ranked higher in 2023.

Top 10 Targeted Industries by Ransomware in 2024



Business Services
1302



Retail
820



Manufacturing
573



Construction
287



Finance
257



Healthcare
248



Education
204



Government
191



Technology
174



Transportation
163

INCIDENTS



December has been consistently the month with the most incidents for the past 2 years. December 2024 had a total of 659 incidents, which is a significant increase on December 2023, where there were only 481 incidents.



January has been consistently the month with the least incidents for the past 2 years. January 2024 had a total of 284 incidents, up on January 2023, where there were 171 incidents.

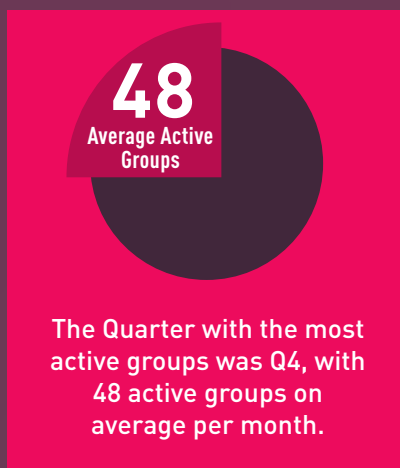


The quarter with the highest number of incidents in 2024 was Q4, with 1827 incidents. In comparison, in 2023 it was Q2 with 1353 incidents.



The quarter with the lowest number of incidents in 2024 was Q1, with 1048 incidents. In comparison, in 2023, it was Q1 with 842 incidents.

ACTIVE GROUPS



FINANCIALS & INSIGHTS

VICTIM DETAILS



1,925

Average number of company employees*



\$565M

Average revenue of company*



UP 50%

The construction industry was the target of 50% more attacks in 2024 vs. 2023.

* based on 85% of the data



The spread of ransomware attacks among continents remains unchanged as per 2023.



Due to the effect of the Russia-Ukraine war, the number of incidents in Russia went down from 55 in 2023, to only 5 at 2024.



Iran went down from 22 ransomware incidents in 2023, to only 2 in 2024.



In comparison to last year, the four most targeted countries in Europe, United Kingdom, Germany, Italy and France saw a dramatic decrease in the number of ransomware incidents in 2024, with drops of 11%, 15%, 12% and 21% respectively



The group that targeted the United States the most was Play, with 283 ransomware incidents directed at the country, which accounts for approximately 80% of their entire attacks in 2024.

TOP FAMILIES

While it was a successful fourth quarter, and year for the entire ransomware industry - three families rose above all. **RansomHub** was the most dominant ransomware group, with 531 new victims, claimin 9.8% of all ransomware cases.

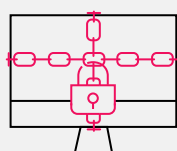
The second spot was saved for last year's winners, the **LockBit** group. Although the group had major struggles this year with law enforcement operations against it, the group affiliates still managed to pull off a large number of attacks with 522 successful ones.

Coming third was the **Play** ransomware group, which claimed a significant number of victims 355, 7.5% of all ransomware cases. **Play** continues to be a dominant power in the ransomware landscape.

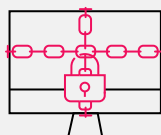
Ransomware as a Service (RaaS) is a business model where affiliates pay to use ransomware attacks developed by operators. It mirrors the software-as-a-service (SaaS) model. This approach significantly contributes ti ransomware attacks' global proliferation and persistence. The rise of RaaS models has notably impacted the ransomware landscape, exemplified by the **RansomHub** group, which claimed the first spot this year, while the runners up **LockBit** are also managing a wide RaaS program for their affiliates.

In the current landscape, where ransomware groups are closing their operations more rapidly than previously observed, a group that consistently executes dozens of successful ransomware attacks every month and sustains its activities for over a year can be deemed a veteran. Therefore, the fourth and fifth places are also reserved for other veteran groups: the **Akira** group, with 315 victims this year, and the **Hunters** group, with 227 victims.

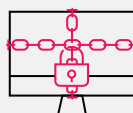
Top 10 Active Ransomware Groups in 2024



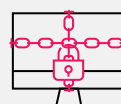
RansomHub
531



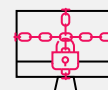
LockBit 3.0
522



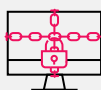
Play
355



Akira
315



Hunters
227



Medusa
211



BlackBasta
183



Qilin
182



BianLian
168



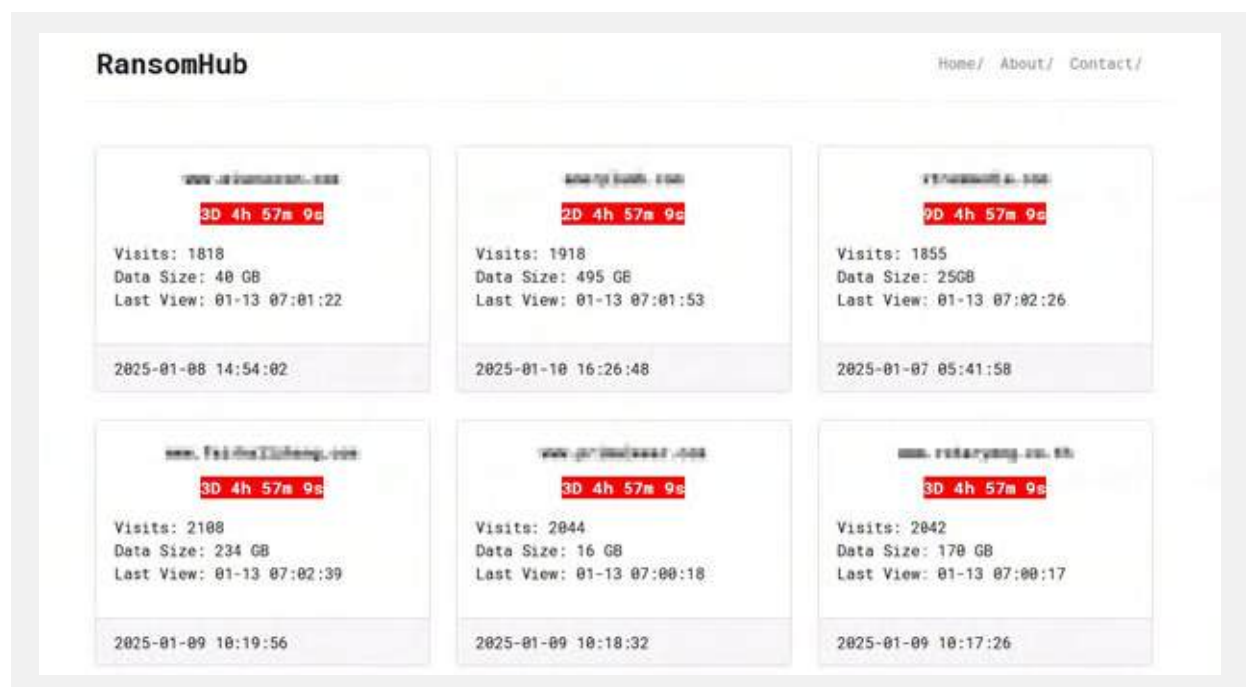
INC. Ransom
159

RansomHub

Since RansomHub started its operations in February, the Cyberint (now a Check Point Company) research team has closely monitored the group's operations and uncovered interesting insights about targeted organizations company size and revenue.

The RansomHub ransomware group has claimed the top spot in the ransomware landscape for 2024, with an impressive 531 published attacks on their Data Leak Site (DLS). Emerging as a major player following the FBI's disruption of ALPHV's ransomware operation on December 19, 2023, RansomHub is widely considered the "spiritual successor" to ALPHV, potentially involving former affiliates of the dismantled group. Operating under a Ransomware-as-a-Service (RaaS) model, RansomHub enforces strict adherence to affiliate agreements, with non-compliance resulting in bans and termination of partnerships. Affiliates retain 90% of ransom payments, while the core group collects the remaining 10%.

According to their About page, RansomHub is composed of threat actors from various global regions, unified by a shared goal of financial gain. The group explicitly avoids targeting certain countries, including CIS nations, Cuba, North Korea, and China, as well as non-profit organizations. However, despite their claims of being a global hacker community, RansomHub's operations strongly align with a traditional Russian ransomware setup. Their avoidance of Russian-affiliated nations and overlap with other Russian ransomware groups in targeted companies further highlights their likely connections to Russia's cybercrime ecosystem.



The screenshot shows the RansomHub website interface. At the top, there is a navigation bar with links for Home, About, and Contact. Below this, there is a grid of six data leak sites, each with a URL, a timer, and statistics for visits, data size, and last view. The sites are arranged in two rows of three.

URL	Timer	Visits	Data Size	Last View	Timestamp
www.100m.com	3D 4h 57m 9s	1818	48 GB	01-13 07:01:22	2025-01-08 14:54:02
www.100m.com	2D 4h 57m 9s	1918	495 GB	01-13 07:01:53	2025-01-10 16:26:48
www.100m.com	9D 4h 57m 9s	1855	25GB	01-13 07:02:26	2025-01-07 05:41:58
www.100m.com	3D 4h 57m 9s	2108	234 GB	01-13 07:02:39	2025-01-09 10:19:56
www.100m.com	3D 4h 57m 9s	2044	16 GB	01-13 07:00:18	2025-01-09 10:18:32
www.100m.com	3D 4h 57m 9s	2042	170 GB	01-13 07:00:17	2025-01-09 10:17:26

On one of our [reports](#) this year on the Ransomhub group, we found out (August 2024) 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.

Malware, Toolset & TTPs

Notably, 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.

The group's ransomware program is like other ransomware groups such as 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 to or a rebrand of the ALPHV ransomware group. Therefore, tools and TTPs could be like those used by ALPHV.

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



Lockbit

The phrase "Nothing else matters" perfectly encapsulates the relentless activity surrounding the LockBit ransomware operation.

In February, an international operation led to the arrest of at least three individuals associated with the notorious LockBit ransomware group in Poland and Ukraine. Despite this disruption to its infrastructure, LockBit remained highly active, ranking as the most prolific threat actor in May and the second most active in July. However, some of this activity may have stemmed from other groups using its leaked ransomware builder. By October and November, LockBit had dropped out of the top ten most active threat actors.

Nevertheless, the group managed to attack hundreds of victims in 2024, recording 522 successful attacks published on their Data Leak Site (DLS).

The group now appears to be staging a comeback following months of diminished activity after the February 2024 takedown. On December 19, LockBitSupp, a persona reportedly linked to the Ransomware-as-a-Service (RaaS) administrators, announced the upcoming release of LockBit 4.0 on its website. The announcement included promotional language such as, "Want a Lamborghini, Ferrari and lots of **f65=% girls? Sign up and start your pentester billionaire journey in 5 minutes with us." They provided details about a new website (lockbit4[.]com), five TOR sites, and a planned release date of February 3, 2025.



Play

In 2024, the Play ransomware group targeted over 350 organizations globally, surpassing their previous record of 301 victims in 2023. Notably, January 2024 saw the group attack only three victims, marking their lowest activity in two years. However, activity quickly surged, with the group averaging 30 attacks per month since then.

Emerging in 2022 as a significant cyber threat, the Play ransomware group, also known as PlayCrypt, has targeted a wide range of sectors, including business, government, critical infrastructure, healthcare, and media, with a focus on North America, South America, and Europe. Operating as a closed group, Play employs a double-extortion strategy, exfiltrating sensitive data before encrypting victims' systems. This approach pressures victims to pay ransoms under the threat of data leaks.



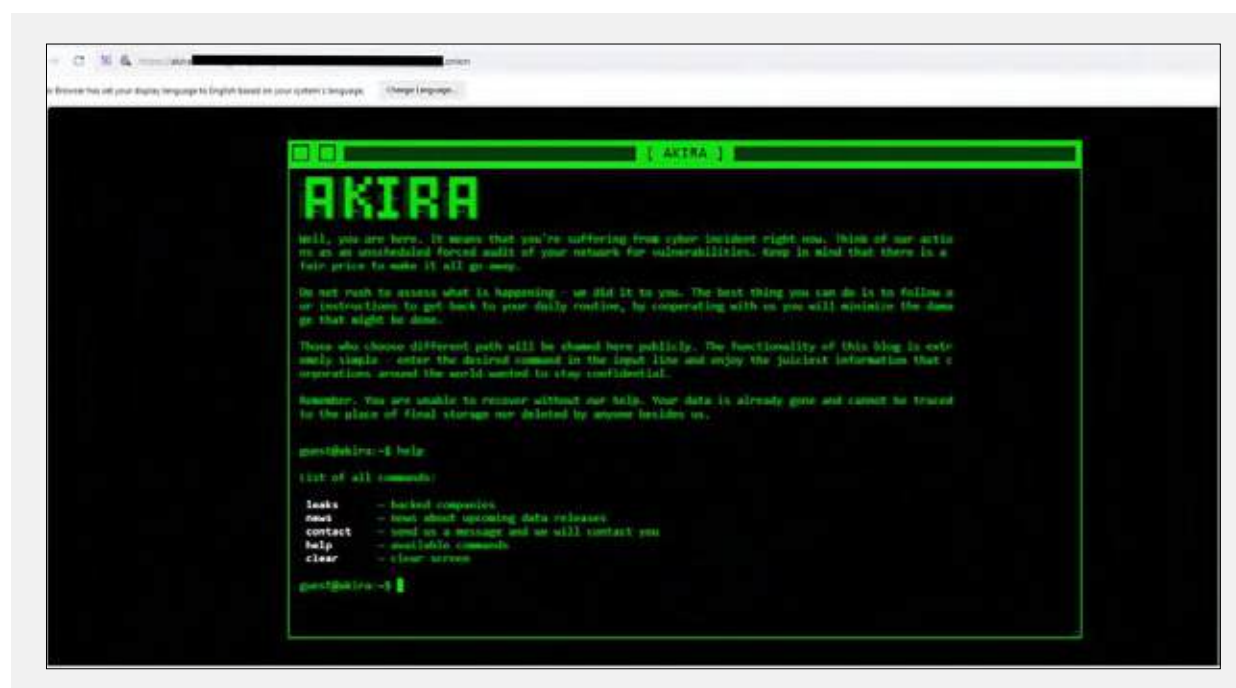
FAMILIES WORTH NOTING

Akira

Since its discovery in March 2023, Akira has already compromised at least 300 victims. Interestingly, Akira is offered as a ransomware-as-a-service. Preliminary research suggests a connection between the Akira group and threat actors associated with the notorious ransomware operation Conti.

In 2024, Akira reported 315 successful attacks published on their Data Leak Site (DLS), securing fourth place among the most active ransomware groups of the year.

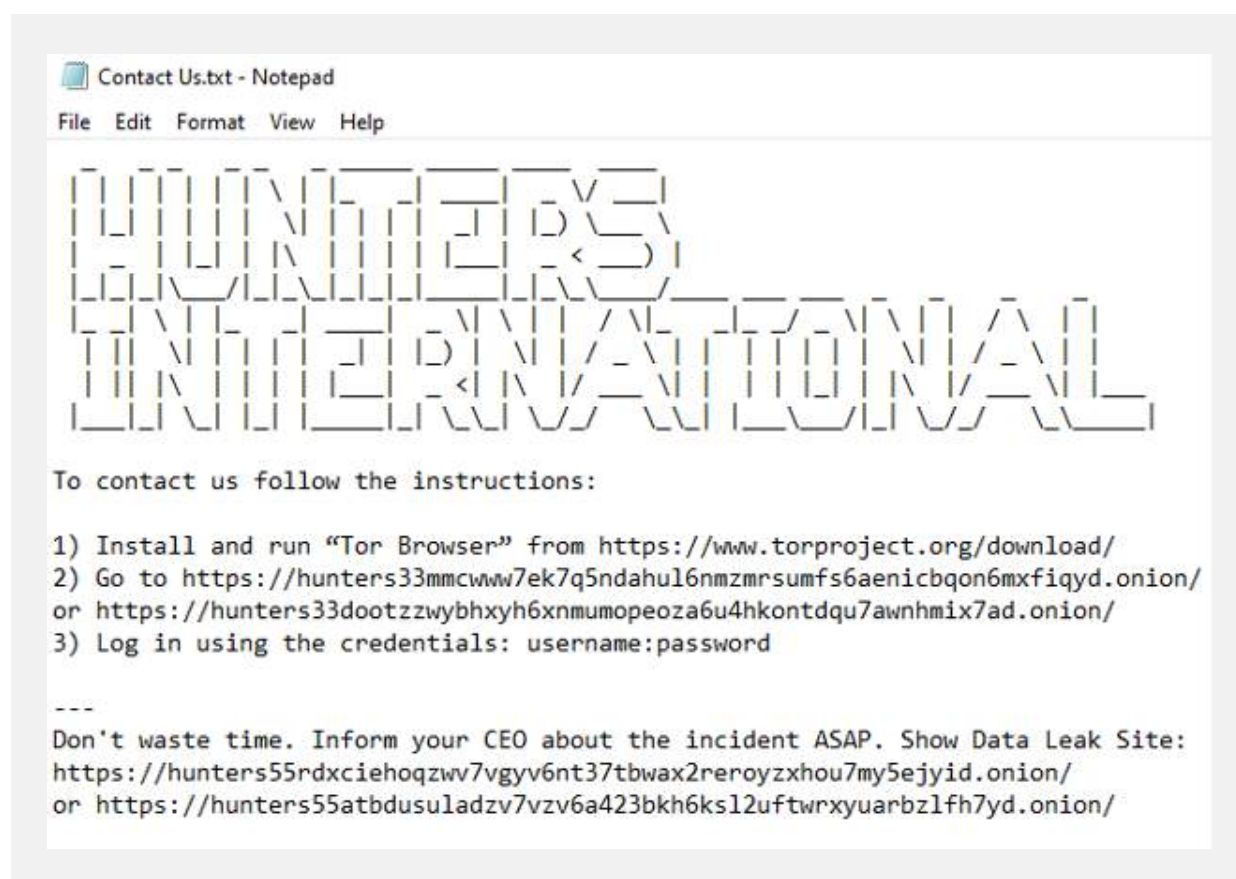
This ransomware, identified as having an impact on both Windows and Linux systems, operates by exfiltrating and encrypting data, coercing victims into paying a twofold ransom to regain access and restore their files. The collective responsible for this ransomware has already directed its attention towards numerous victims, with a primary focus on those situated in the U.S. Furthermore, the group operates an active leak site for the Akira ransomware, where they publish information, including their latest data breaches.



Hunters

Amid the disruption of the Hive ransomware group by law enforcement agencies, Hunters International emerged onto the cyber scene in Q3 of 2023, displaying notable technical similarities with Hive, hinting at an evolutionary progression or branch-off from the dismantled group. This transition underscores the adaptive nature of cybercriminal networks, persisting in their illicit activities despite law enforcement actions. The inception and modus operandi of Hunters International underscore an ongoing threat in the realm of cyber extortion and data breaches.

2024 proved to be a highly successful year for the team, with 227 organizations targeted globally, taking the fifth place in top active ransomware groups list. They showed no preference for specific countries or industries, capitalizing on a wide range of targets to maximize profits.



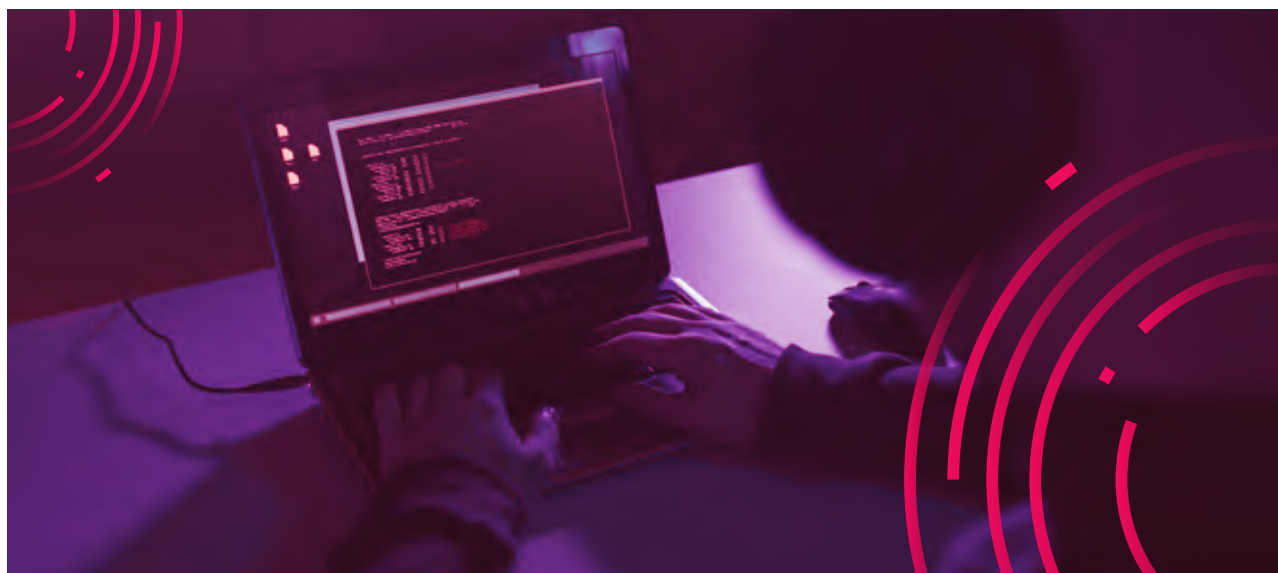
Medusa

Operating under the Ransomware-as-a-Service (RaaS) model, the Medusa Ransomware group collaborates with global affiliates, significantly expanding its reach and impact.

In 2024, the Medusa group carried out over 200 attacks, earning the sixth position among the most active ransomware groups of the year. Building on their operations from 2023, Medusa maintained a high attack volume, targeting organizations worldwide and demanding substantial ransom payments.

Medusa Ransomware distinguishes itself as a multifaceted threat, akin to the serpentine tendrils of Medusa's hair. Each encrypted file, marked with various extensions, mirrors the numerous snakes that adorned the Gorgon's head. The prominent ".MEDUSA" extension serves as a distinctive hallmark of this ransomware's destructive touch.

Analyzing the countries where Medusa has targeted companies indicates a concentration of attacks in North and South America and Europe. The United States is the primary target, followed by the United Kingdom, experiencing more attacks than any other country.



Killsec

The KillSec group emerged as one of the most notable surprises among newcomers in 2024, targeting over 130 organizations globally. Interestingly, India ranked as the second most affected country by their ransomware attacks, with 20 reported incidents.

The group's activities appear to have commenced in October 2023, as suggested by their Telegram channel. In their first public announcement, they openly sought individuals with expertise in areas such as "network penetration," "web penetration," and "malware creation," signaling a strong focus on offensive cyber operations aimed at compromising networks and websites. These recruitment efforts suggested that the group intended to operate beyond mere hacktivism, despite initial allegations to the contrary.

These indications proved accurate by June 2024, roughly a year after the Telegram channel's launch, when the threat actor officially unveiled their new Ransomware-as-a-Service (RaaS) operation.

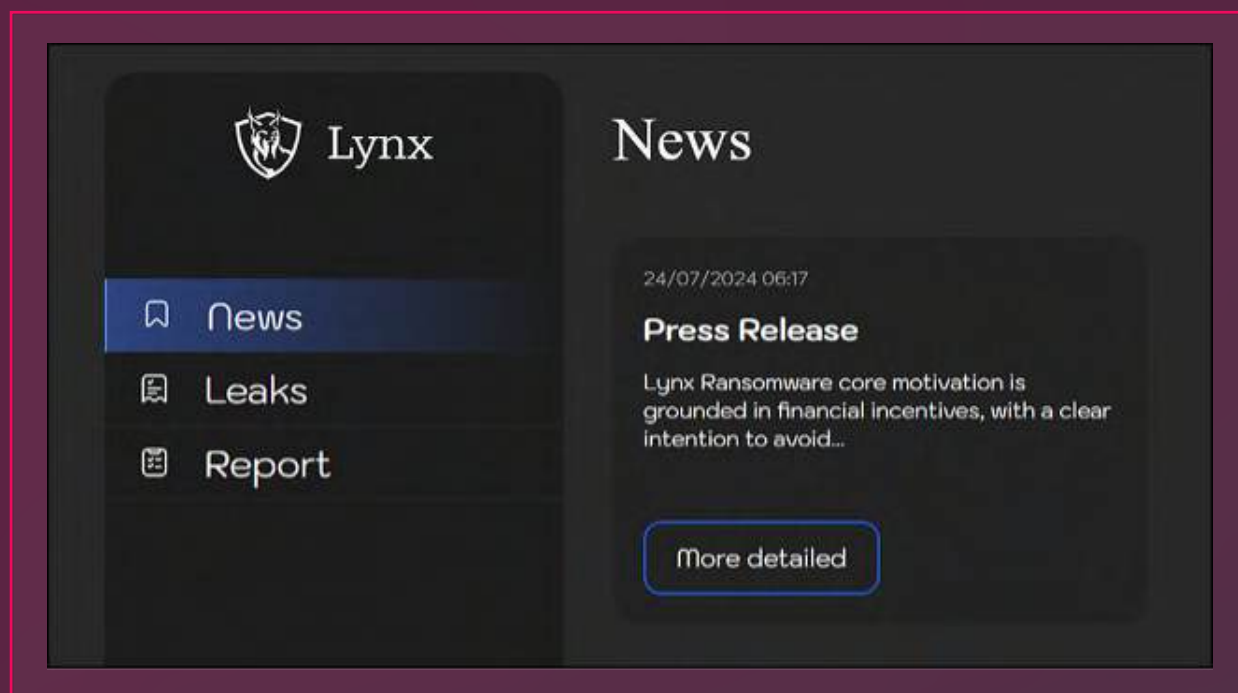


NEWCOMERS

In 2024, 46 new ransomware groups emerged, shaping the threat landscape. While this report does not delve into every group, it highlights those that significantly impacted the ransomware ecosystem. The **RansomHub** group, for instance, has already been discussed in detail in the Stats section. Despite being categorized as a newcomer, having published its first victim in 2024, RansomHub has already made a notable mark.

Lynx

Lynx, a double-extortion ransomware group, has been highly active recently, listing numerous companies as victims on their site. However, the group claims to avoid targeting government entities, hospitals, non-profits, and other socially crucial sectors. Once inside a system, Lynx encrypts files, adds the .LYNX extension, and leaves a ransom note titled "README.txt" in multiple directories. Lynx had claimed over 70 victims in 2024, highlighting their ongoing activity and strength in the ransomware landscape.



FOG

Fog ransomware emerged in early April 2024, targeting organizational networks in the U.S. education sector by exploiting compromised virtual private network (VPN) credentials. It employs a multi-faceted extortion model, using a TOR-based data leak site (DLS) to expose non-compliant victims and host stolen data.

In 2024, the group attacked 87 organizations worldwide.

A November 2024 report from Arctic Wolf reveals that the Fog ransomware operation has carried out at least 30 intrusions, all initiated via remote access through compromised SonicWall VPN accounts. Of these incidents, 75% were linked to Akira, while the remaining cases were attributed to Fog ransomware. Notably, the two threat groups seem to share infrastructure, indicating an ongoing informal collaboration between them.

Fog ransomware primarily targets the education, business services, travel, and manufacturing sectors, with a strong focus on the U.S. This is one of the only groups in the ransomware landscape where the education sector is marked first in most targeted industries.



ArcusMedia

The Arcus Media ransomware group, active since May 2024, is a relatively new threat actor known for its direct and double extortion methods. They gain initial access through phishing emails, deploy custom ransomware binaries, and use obfuscation techniques to evade detection. Their tactics include phishing emails with malicious attachments, obfuscated scripts for executing payloads, and privilege escalation using tools like Mimikatz.

This actor has claimed multiple victims in recent months across various sectors, including government, banking, construction, IT services, and entertainment.

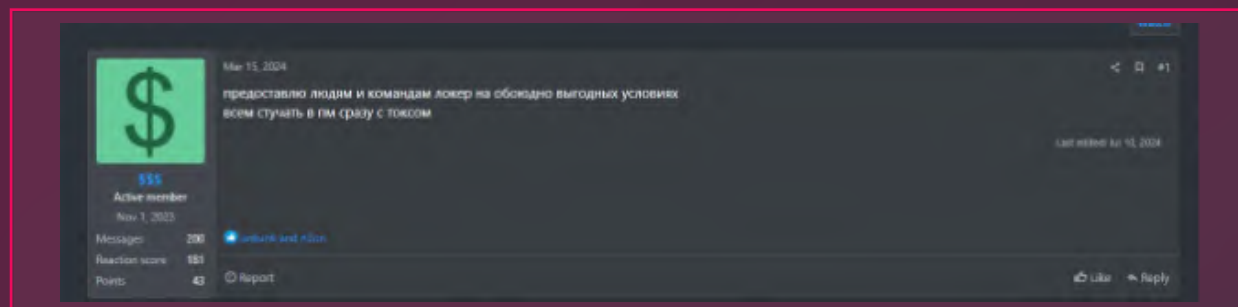
In 2024, ArcusMedia group attacked 56 organizations worldwide.



Eldorado

In March 2024, a new affiliate program was introduced on the ransomware forum "RAMP." The advertisement promoted a locker and loader service, actively recruiting penetration testers to join the operation. According to Group-IB analysts, who claimed to have infiltrated the Eldorado group, the group's representative was a Russian speaker. The ransomware builder requested the domain administrator's password or NTLM (Windows New Technology LAN Manager) hash, along with other parameters, to generate customized ransomware samples.

On March 16, 2024, a user with the alias "\$\$\$" launched the Eldorado Ransomware affiliate program by posting on the underground forum "RAMP."

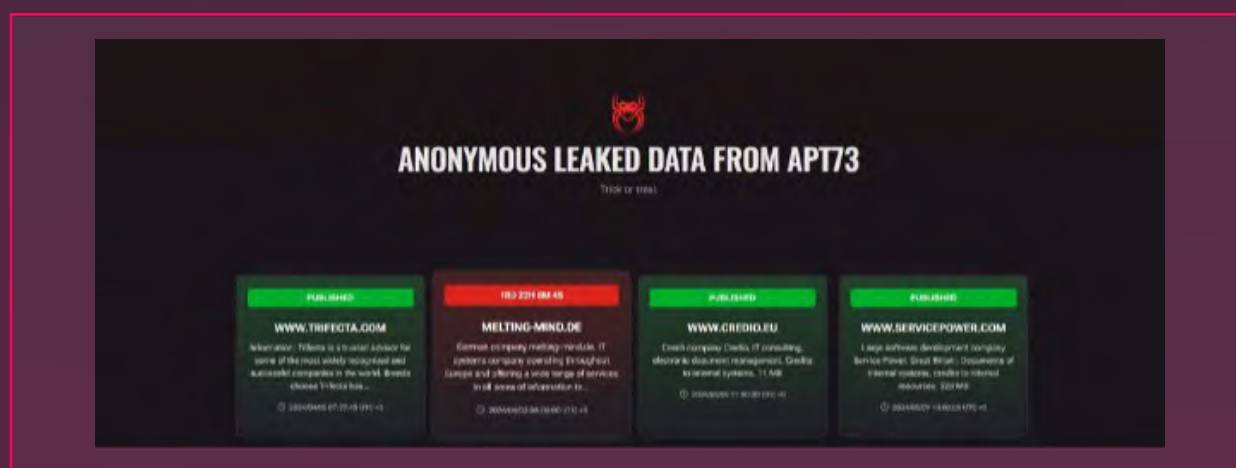


In 2024, the group published 60 victims on their DLS, targeting mostly the business services sector, and the United States. Among the notable victims we can find **Puerto Rico Federal Affairs Administration**, **Tiendas Carrion & Fernandez**, and others.

APT73/Bashe

In contrast to other naming conventions that researchers use to identify threat actors, this group has chosen to refer to themselves as "APT" (Advanced Persistent Threat) followed by a number, specifically APT73, a ransomware group modeled on LockBit. This was observed through similarities in their "Contact Us," "How to Buy Bitcoin," and "Web Security & Bug Bounty" pages, which closely resemble the layout of the LockBit Data Leak Site (DLS). The content on these pages mirrors that of LockBit, indicating that this is essentially a LockBit-style Ransomware Data Leak Site (DLS). One notable difference is the "Mirrors" section, which lacks any active mirrors, unlike LockBit, highlighting a level of amateurism within this group.

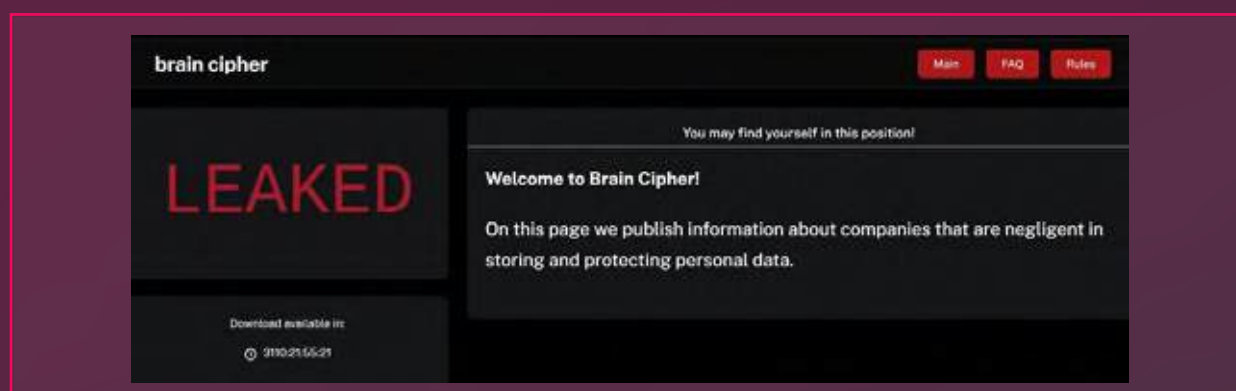
In 2024, the group has targeted a total of 65 victims in various locations worldwide, including Germany, Canada, the Czech Republic, and the United States. Their attacks have been exclusively focused on the business services sector.



BrainCipher

Brain Cipher is a recently launched ransomware operation that initiated attacks on organizations globally earlier this year. They began in June 2024. Over the last year, the group attacked 25 victims all over the world, targeting crucial industries and organizations.

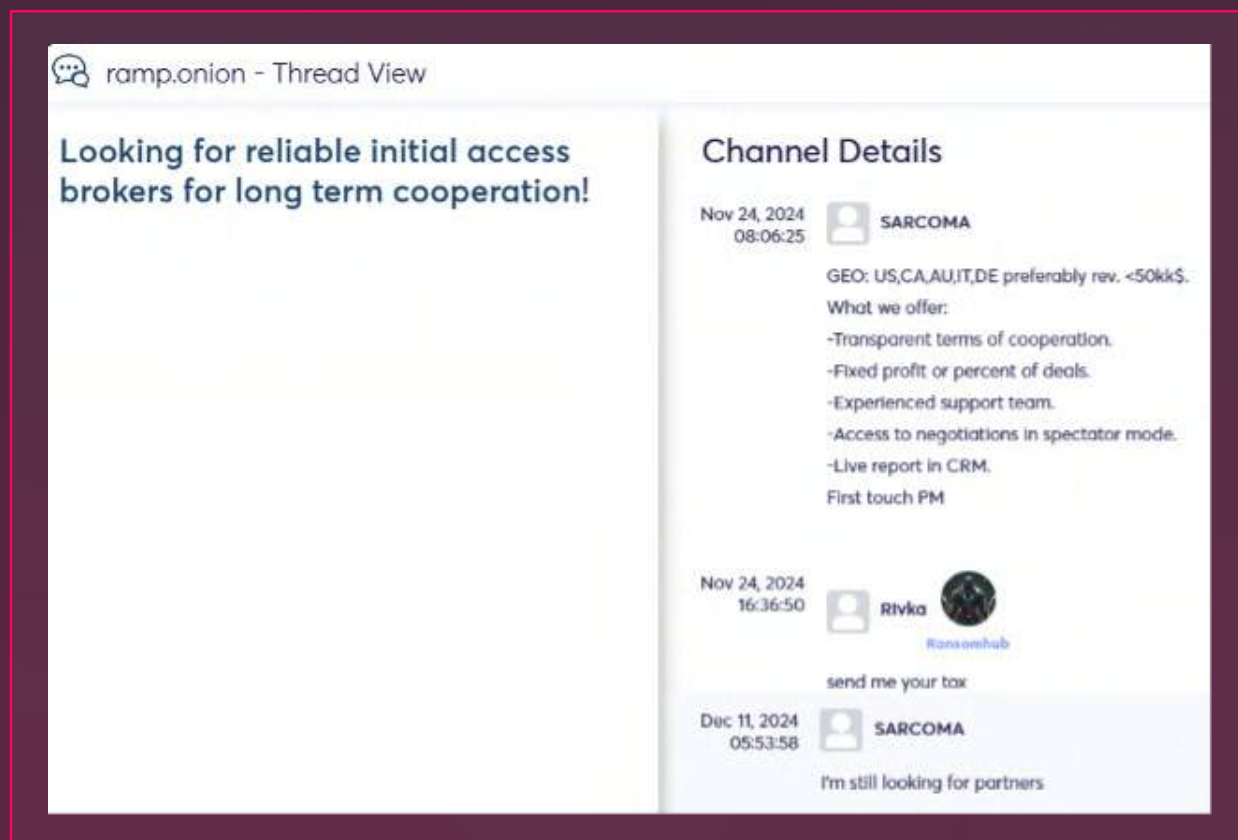
Initially, the ransomware gang operated without a data leak site. However, their latest ransom notes now link to one, indicating they are engaging in double-extortion schemes by threatening to release stolen data. Brain Cipher operators have targeted multiple critical industries, including medical, educational, and manufacturing entities. The group is also known to attack government and law enforcement targets, with a previous target being Indonesia's National Data Center. This particular attack caused significant disruptions to public services, including immigration and new student registration systems.



Sarcoma

The Sarcoma Group, a relatively new ransomware entity, emerged in October 2024. By the end of November, the group had already listed 38 companies on its data leak site. Maintaining a high tempo of operations, Sarcoma concluded 2024 with a total of 58 attacks attributed to its name. The group created headlines very fast and continues to operate and attack entities around the world.

The group has a user account on the underground RAMP forum. The group is using this account to post updates, and sometimes search for partners, such as in this example:



Sarcoma employs sophisticated and varied tactics to infiltrate and compromise systems with precision. The group frequently relies on phishing attacks, sending deceptive emails to trick recipients into clicking malicious links or downloading infected attachments. These emails often mimic legitimate business communications to increase the likelihood of engagement. Additionally, Sarcoma actively exploits unpatched software and operating system vulnerabilities to gain unauthorized access, highlighting the importance of timely application of security patches and updates.

Remote Desktop Protocol (RDP) exploitation is another favored method, as the group targets misconfigured RDP settings to access systems remotely. These vulnerabilities, often stemming from weak credentials or improper configurations, serve as common entry points. Moreover, Sarcoma has a history of targeting supply chains, compromising vendors and suppliers to infiltrate more extensive networks. This strategy enables the group to maximize its reach with a single intrusion.



ARRESTS

FBI DISRUPTS DISPOSSESSOR RANSOMWARE OPERATION, SEIZES SERVERS

On August 12, 2024, in a significant international collaboration, the FBI successfully disrupted the Radar/Dispossessor ransomware operation. The agency seized servers and websites associated with the group, marking a major victory against the cybercrime network. The takedown follows a thorough investigation involving law enforcement agencies worldwide, as they continue to target organized cybercriminal groups. This operation highlights ongoing efforts to dismantle ransomware organizations that have been responsible for numerous attacks globally.

GERMANY SEIZES 47 CRYPTO EXCHANGES LINKED TO RANSOMWARE GANGS

German authorities successfully seized 47 cryptocurrency exchanges used by ransomware gangs for laundering illicit gains. This move was part of a larger effort to crack down on cybercriminal networks exploiting digital currencies to obscure their financial activities. These exchanges were found to have facilitated the laundering of funds linked to ransomware attacks, further highlighting the increasing use of cryptocurrencies by threat actors for illicit transactions. The action comes as part of a coordinated global initiative to target platforms that provide ransomware operators with the financial infrastructure needed to hide their ransoms and profits. This effort demonstrates law enforcement's growing focus on digital currencies as a critical part of disrupting cybercriminal operations.

LOCKBITSUPP IDENTITY REVEALED - \$10 MILLION REWARD FOR HIS ARREST

The UK, US, and Australia have revealed the identity of Dmitry Khoroshev, a Russian national and the leader of the once-notorious LockBit ransomware group, following an international disruption campaign led by the National Crime Agency (NCA).

Dmitry Khoroshev, also known as LockBitSupp, who previously operated in secrecy and offered a \$10 million reward to uncover his identity, is now facing sanctions announced by the FCDO in coordination with the US Department of the Treasury's Office of Foreign Assets Control (OFAC) and the Australian Department of Foreign Affairs.

These sanctions include asset freezes and travel bans. Additionally, the US has unsealed an indictment against Khoroshev and is offering a reward of up to \$10 million for information leading to his arrest or conviction.

These actions are part of an extensive investigation into the LockBit group conducted by the NCA, FBI, and other international partners forming the Operation Cronos taskforce.

- 1) [Hacker arrested: Wanted Russian Hacker Linked to Hive and LockBit Ransomware Arrested](#)
- 2) <https://thehackernews.com/2024/02/lockbit-ransomwares-darknet-domains.html>



THREAT ACTOR LINKED TO THE SCATTERED SPIDER GROUP ARRESTED IN SPAIN

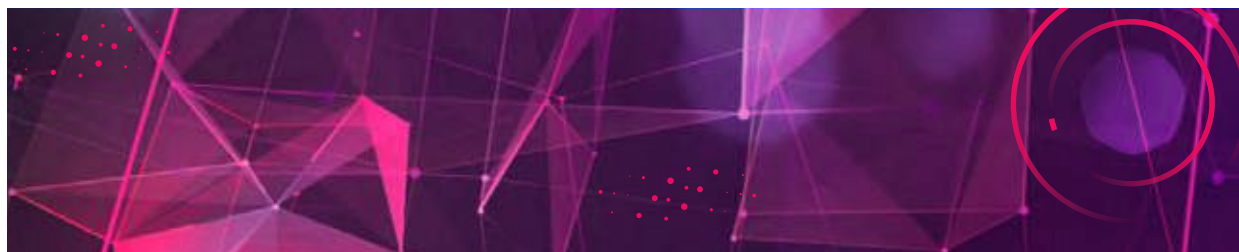
A 22-year-old British national allegedly linked to the Scattered Spider hacking group and responsible for attacks on 45 U.S. companies has been arrested in Palma de Mallorca, Spain. The suspect is believed to be a leader of a cybercrime gang focused on stealing data and cryptocurrencies from organizations and extorting them to prevent the publication of sensitive data. Investigators report that the group stole \$27,000,000 worth of cryptocurrencies using this scheme.

The arrest followed an investigation initiated by a tip from the FBI, which led to the issuance of an International Arrest Warrant (OID). The Spanish police arrested the suspect on May 31, 2024, at Palma airport as he was about to depart for Naples, Italy. During the arrest, his laptop and mobile phone were confiscated for forensic examination.

Authorities have not yet disclosed details about the specific threat group, but VX-Underground alleges without confirmation that the suspect is "Tyler," a SIM swapping specialist from the notorious Scattered Spider group.

Scattered Spider is a loose-knit collective of English-speaking cybercriminals known for accessing their targets' networks through social engineering, phishing, multi-factor authentication (MFA) fatigue, and SIM swapping. Some members of this group have also acted as affiliates with the Russian-speaking BlackCat ransomware gang.

In September 2023, Scattered Spider breached entertainment giant MGM Resorts, deploying a BlackCat/ALPHV encryptor, stealing data, and causing significant operational disruption.



POLICE ARREST CONTI AND LOCKBIT RANSOMWARE CRYPTER SPECIALIST

The Ukraine cyber police arrested a 28-year-old Russian man in Kyiv for collaborating with the Conti and LockBit ransomware operations. He specialized in making their malware undetectable by antivirus software and conducted at least one attack himself.

Supported by information from the Dutch police, the investigation linked the man to a ransomware attack on a Dutch multinational. He was arrested on April 18, 2024, as part of 'Operation Endgame,' which targeted various botnets and their operators.

The suspect developed custom crypters to make ransomware payloads appear as safe files, selling these services to Conti and LockBit. The Dutch police confirmed his involvement in a 2021 ransomware attack using a Conti payload. During the arrest, authorities seized computer equipment, mobile phones, and handwritten notes. The investigation is ongoing, and the suspect, charged under Part 5 of Article 361 of the Criminal Code of Ukraine, faces up to 15 years in prison.



NEW TRENDS

THE DECLINE OF MAJOR RANSOMWARE GROUPS FUELS A SURGE IN SUSTAINABLE EMERGING THREATS

In 2023, international law enforcement agencies intensified their efforts against ransomware, leading to the decline of groups like Hive and Ragnar Locker, as well as the dismantling of ALPHV (BlackCat). These actions underscore the increasing challenges ransomware groups face. A significant operation in February 2024 targeted LockBit, resulting in arrests and the seizure of its data leak sites and servers, marking one of the largest law enforcement actions against a major ransomware operation.

Despite these crackdowns, ransomware continued to attract new threat actors. Leak site data revealed the emergence of at least 25 new ransomware groups in 2023, although many, including Toufan, Darkrace, and CryptNet, disappeared by mid-year. In 2024, this trend accelerated, with 46 new groups emerging, representing 48% of all active groups that year. These newcomers accounted for approximately 30% of all ransomware attacks recorded in 2024.

To gauge group activity, one approach is to track the number of victims they publish on their data leak sites each month. However, this metric does not fully reflect a group's activity, as many operations target victims without publicizing the attacks, especially when negotiations occur privately. Nevertheless, analysing these statistics provides insights into a group's sustained activity over the year.

From our data, the average lifespan of new ransomware groups in 2024, measured by the number of months they published victims on data leak sites, was 3.9 months. Notably, 21 of the 46 new groups remained active for more than four months, and 16 of these were active for six months or longer. This demonstrates that while many new groups fade quickly, a subset manages to sustain operations over an extended period.

RANSOMWARE GROUPS TARGETING LINUX AND VMWARE ESXI SYSTEMS AND DEVELOPING NEW CAPABILITIES

In recent years, ransomware groups have increasingly shifted their focus towards Linux-based systems and VMware ESXi servers, recognizing them as valuable targets with incorporate infrastructures. These systems often host critical virtual machines (VMs) that, if compromised, can cause widespread disruption.

- Play Ransomware developed a Linux variant specifically to attack VMware ESXi servers, a hypervisor that is widely used in enterprise environments.
- Cicada3301 Ransomware followed a similar strategy by launching attacks on VMware ESXi servers, highlighting the growing focus on exploiting Linux-based virtualized environments.
- BlackByte and BlackBasta have also adapted their tactics, with BlackByte using vulnerabilities in VMware ESXi to launch attacks that exploit authentication bypass techniques, allowing them to encrypt virtual machines.

These attacks are part of a broader trend where ransomware operators target Linux systems due to the increasing reliance on these platforms for hosting critical business infrastructure. The growing focus on virtualization environments is also driven by the potential to impact large-scale operations with just one attack, as compromising ESXi servers can lead to encryption of numerous virtualized resources in one go.



Furthermore, ransomware capabilities have evolved considerably over the past year, with attackers developing more sophisticated techniques to evade detection and maximize damage. Black Basta, for instance, has adopted custom malware designed to bypass security tools, making it more evasive and effective against modern defences. In addition, ransomware groups like RansomHub are leveraging legitimate tools like Kaspersky's TDSSKiller to disable endpoint detection and response (EDR) software, allowing them to operate undetected in compromised environments.

Another significant development is the abuse of cloud-based tools for data theft. For example, ransomware operators, including BianLian and Rhysida, are now using Microsoft's Azure Storage Explorer and AzCopy tools to steal data from victim networks and store it in cloud-based infrastructure, adding a new layer of complexity to their operations. These developments demonstrate the growing sophistication of ransomware, with groups increasingly targeting more robust systems and leveraging new capabilities to outsmart security measures across various environments.



RANSOMWARE LANDSCAPE PREDICTIONS FOR 2025

The ransomware landscape in 2025 is expected to continue evolving with an increase in sophistication and adaptability from threat actors. With a record-breaking Q4 in 2024, marking 1,827 ransomware incidents, ransomware groups are likely to intensify their operations, targeting high-value industries and leveraging advanced technologies like artificial intelligence to improve their attack efficacy.

Groups like LockBit and Cl0p, which announced their resurgence in late 2024, will likely focus on more robust operations, using updated ransomware variants and exploiting zero-day vulnerabilities to maintain their dominance. These groups, alongside emerging players such as RansomHub, are expected to expand their attack vectors to target under-protected industries, emphasizing Linux and VMware ESXi systems.



The rise of Ransomware-as-a-Service (RaaS) is anticipated to further lower entry barriers for new actors in the ransomware ecosystem, leading to a surge in new groups and more diversified attack strategies. The focus on double and triple extortion models will grow, with threat actors increasingly employing data theft, public shaming, and persistent denial-of-service (DDoS) tactics to amplify ransom demands. Additionally, the abuse of cloud-based tools for exfiltration, as seen in 2024, will likely continue as threat actors exploit organizations' increasing reliance on cloud infrastructure.



CONCLUSIONS

The 2024 statistics reveal a rapidly expanding ransomware ecosystem, with 46 new groups emerging, reflecting a 48% increase in active groups compared to the previous year. This growth underscores the resilience of ransomware operators, even in the face of intensified law enforcement actions and technological countermeasures. The continued focus on critical industries, such as business services, construction, and manufacturing, highlights the economic and operational vulnerabilities that ransomware groups aim to exploit.

Looking ahead, global cooperation among law enforcement agencies will be pivotal in disrupting ransomware networks. The success of operations like the takedown of LockBit's infrastructure and the arrest of its leader, coupled with efforts such as Germany's seizure of cryptocurrency exchanges, demonstrates the potential for effective countermeasures. However, the adaptability of ransomware groups indicates that the fight against this evolving threat will remain a significant challenge in 2025, requiring constant innovation in defense strategies and proactive measures to mitigate risks.

CONTACT US

ISRAEL

Tel: +972-73-226-4555
5 Shlomo Kaplan Street
Tel Aviv 6789159

USA

Tel: 1-800-429-4391
100 Oracle Parkway, Suite 800
Redwood City, CA 94065

SINGAPORE

Tel: +65-6435-1318
78 Shenton Way, #09-01 Tower 1,
Singapore 079120

PHILIPPINES

Tel: +63 2 8465 9200
Unit 2005, 20th Floor, Zuellig Building,
Makati Avenue, corner Paseo de Roxas
Makati City 1223, Metro Manila

UK AND IRELAND

Tel: +44 20 7628 4211
85 London Wall, 4th Floor,
London, EC2M 7AD

JAPAN

Tel: +81-3-6205-8340
Toranomon Kotohira Tower 25F,
1-2-8, Toranomon Minato-ku, Tokyo 105-0001

ABOUT CYBERINT

Cyberint, now a Check Point company, reduces risk by helping organizations detect and mitigate external cyber threats before they have an adverse impact. The Check Point External Risk Management solution 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 Check Point External Risk Management 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> / checkpoint.com/erm

© Cyberint, 2025. All Rights Reserved.