ADVANCED **DATADRIVEN** CYBERNEWS

REPORT Q1 2024

ransomfeed.it | grep_13.06.2024_02_en

INDEX

The phenomenon of ransomware is impacting the personal and sensitive documents of hundreds of thousands of citizens. These malicious activities can no longer be ignored..

Dario Fadda

Ransomfeed: the project

Ransomfeed.it is a continuous monitoring service for ransomware groups. Utilizing web scraping, extracting data from multiple websites through software programs and then structuring it, the platform stores all of the claims in a **permanent RSS feed**.

This entire monitoring service is **free and publicly accessible**, constantly collecting and analyzing data on attacks at an international level. The platform effectively and promptly detects all claims published by the groups, making the data available to anyone who wishes to understand the extent and evolution of cyber attacks.

Introduction to the report

This report aims to provide a detailed overview of the ransomware threat landscape during the **first four months period** of 2024, with a particular focus on the monitoring activities conducted by the OSINT platform Ransomfeed. During this period, **204 criminal groups** operating worldwide were monitored, with constant tracking of **404 servers** used to carry out ransomware activities. The collected data revealed a total of **1,419 claims**, with **39 registered in Italy**.

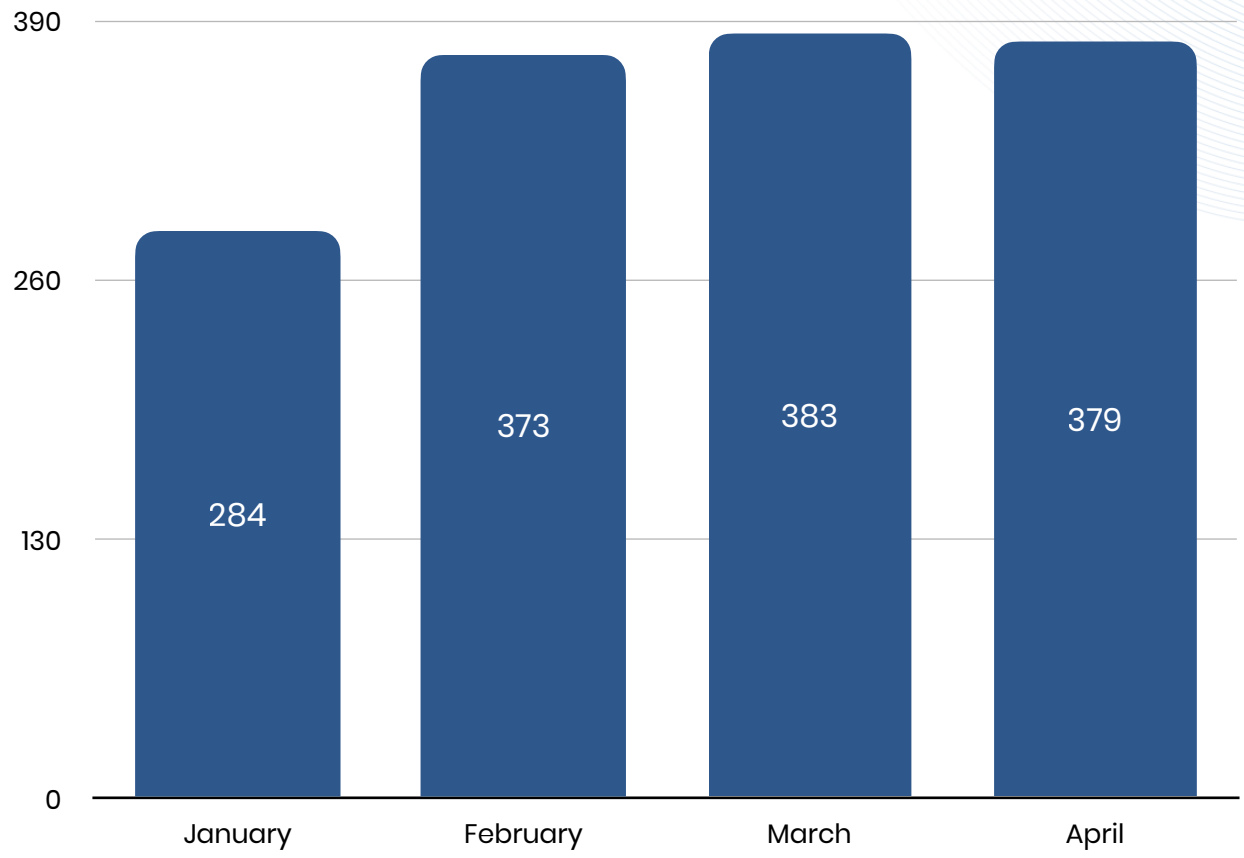
This report will closely examine the geographical distribution of these attacks, as well as the **most impacted industry sectors**. Additionally, special attention will be given to ransomware attacks that have targeted Italy, in order to understand the specific challenges the country has faced during this critical period in cybersecurity.

Overview

All the data in this report has been obtained through Ransomfeed's primary activity of **periodic scraping** from various well-known dark web sites. For this report, we will focus on the results collected for the first four months period of 2024, starting with a global overview followed by a focus on Italy.

During the first four months of 2024, the platform monitored **204 criminal groups** operating with ransomware technologies across **more than 404 servers and mirrors**, resulting in the identification of **1,419 claims worldwide**.

The months of January, February, March, and April each presented unique challenges in the field of cybersecurity. **March was the most prolific month** of the quarter with **383 attacks**, followed by **April with 379**, **February with 373**, and **January with 284**. As evident, the number of attacks has been increasing as the year progresses.

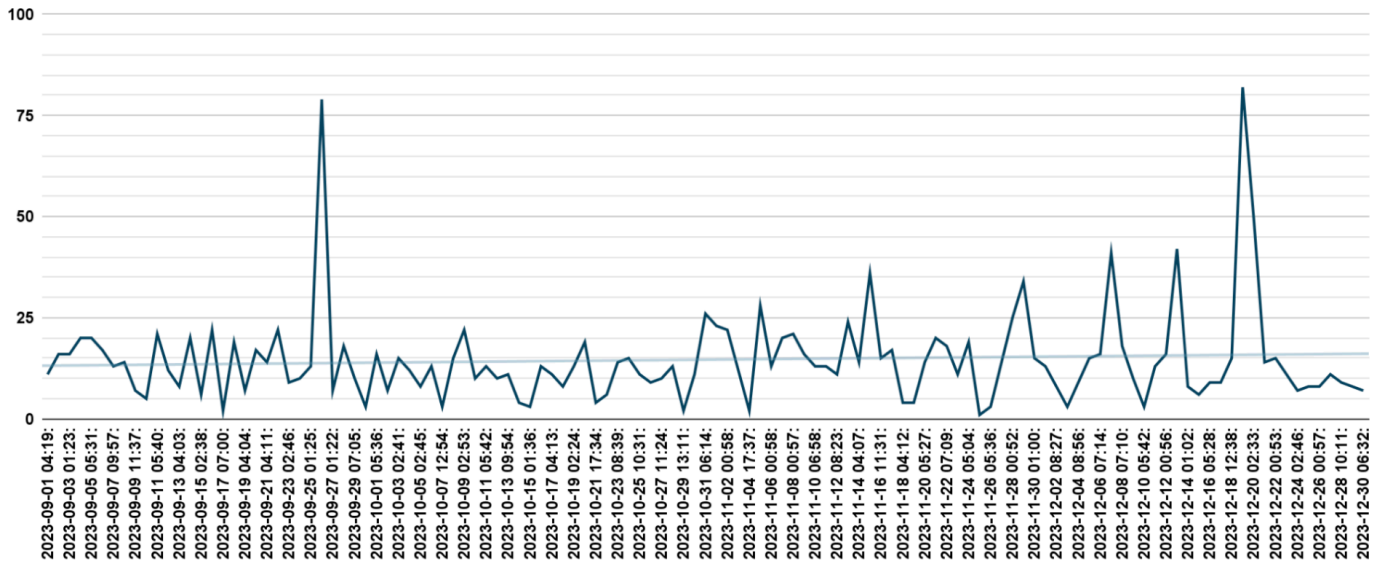


monthly attacks, source: Ransomfeed.it

March 27 was the richest day of the four-month period with as many as **49 ransomware attacks** claimed, highlighting the determination and skill of threat actors in exploiting vulnerabilities. This spike in criminal activity highlights the urgency of addressing cybersecurity gaps and strengthening defenses against the growing threats. In contrast, **January 28** and **February 3** marked the **least significant days** in the first four months of the year, with only one claim each. This significant variation between the highest and lowest attack days indicates that although attacks may be concentrated in certain periods, the risk is constant and unpredictable.

The **daily average of attacks exceeds 11.7 per day**, an alarming figure that calls for serious reflection regarding the security measures taken by organizations. The growing trend not only puts sensitive data and financial resources at risk, but also undermines trust in the infrastructure that businesses and governments rely on. Organizations must therefore take a **proactive approach** to managing cybersecurity by investing in advanced threat detection technologies, ongoing training for staff and rapid incident response plans.

In addition, collaboration between public and private sectors becomes essential to share information and develop effective strategies against cyber criminals. Only through collective and coordinated efforts will it be possible to mitigate the devastating impact of ransomware attacks and protect the critical infrastructure on which our digital society relies.



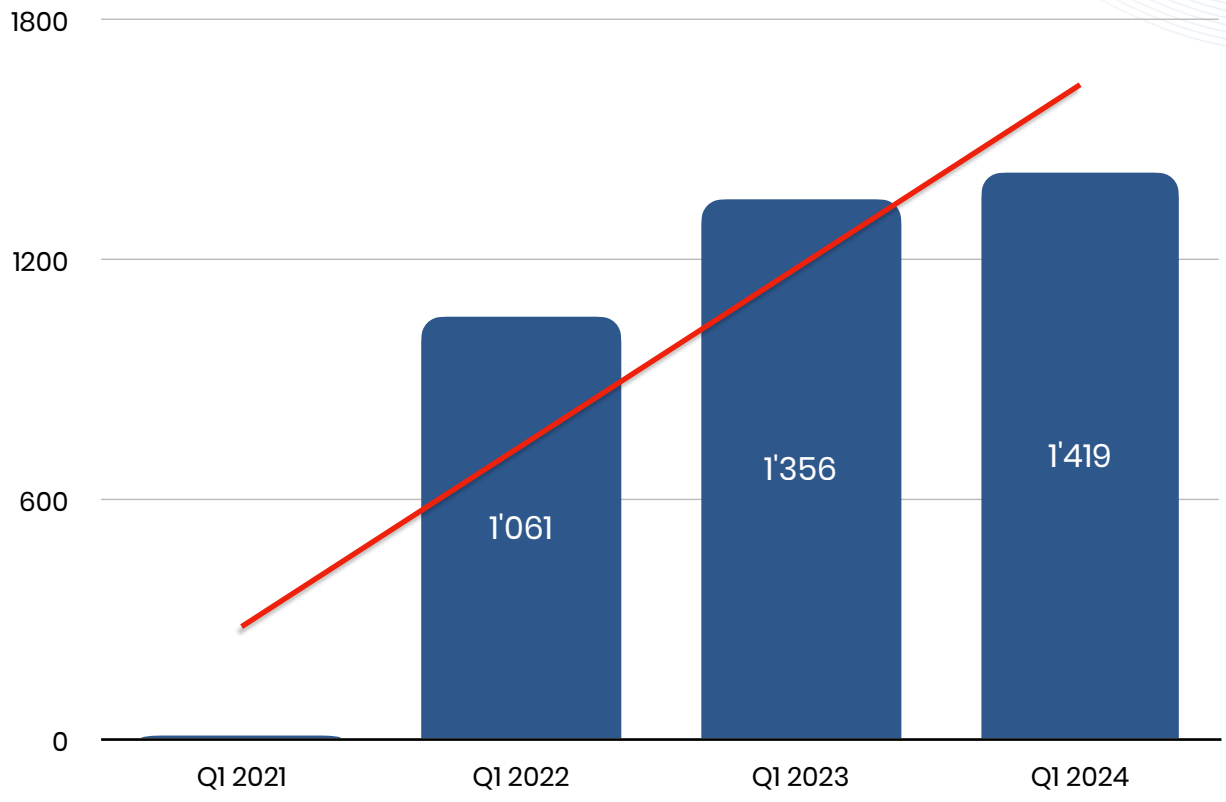
the bottom line shows the overall average trend, source Ransomfeed.it

Comparison of Quarters

As usual, in order to frame the data just presented in the **Overview** in a timely manner, we compared this dataset with those of other early four-month periods in the past. Recalling that the Ransomfeed platform was **initially fed with past data up to January 12, 2020**, we went back in time, thus querying the first four months of the past three years.

By analyzing the historical data, it is possible to identify **recurring patterns**, **seasonal variations**, and the emergence of new techniques used by cyber criminals. For example, comparison with previous years' quarters can reveal whether the recent increase in attacks is part of a steady growth or represents an abnormal spike. This historical analysis is critical for contextualizing current data and predicting possible future developments.

As the graph shows, the trend is upward and there is **still no decrease** in attacks. Compared to analyses of other quarters done during the year, the growth recorded in the first four months of the year is quite significant, creating an unreassuring trend; note how the year 2023 and the year 2024 are **exaggeratedly more prolific than 2021**. In fact, in this time frame, 2024 attests to an increase of about 5 percent over the previous year, while the **growth is 34%** if we compare it with the same period in 2022.



source Ransomfeed.it

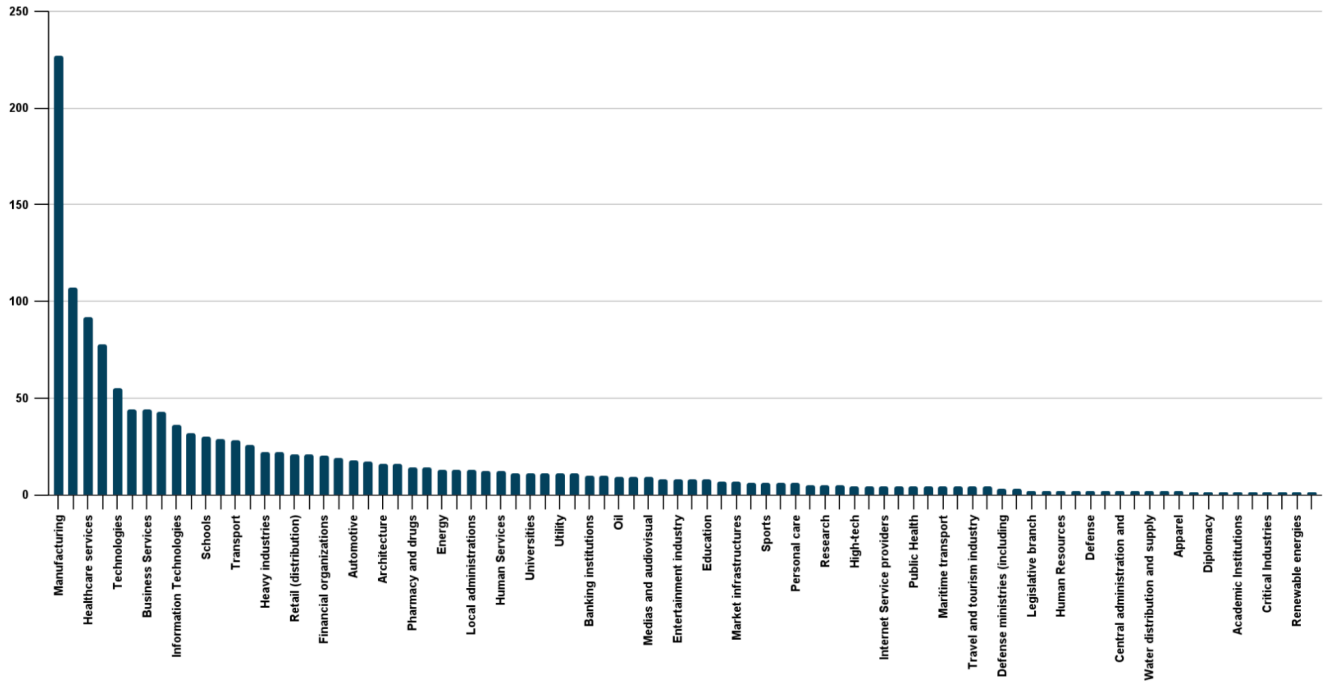
Distribution of ransomware by industry

Thanks to the data enrichment process, which was the result of a fruitful collaboration between the **Ransomfeed project** and **Würth Phoenix**, led by expert **Massimo Giaimo**, we were able to align and complete all the missing data related to the employment sector of the victims involved in the claims. This collaboration allowed us to provide **detailed statistics** on the economic sector of the claims on our platform.

Armed with this improvement in data quality, we can present category statistics in a more accurate and detailed manner. In addition, the **in-depth analysis by economic sector** allows for a better understanding of which areas are most impacted, and, consequently, to understand what security measures could be put in place to prevent and/or mitigate threats-keeping in high regard at all times **a policy of Zero Trust, Awareness & Training**, and, at the forefront, compliance with all those machine upgrade regulations.

In the top five podium positions (representing 60 percent of total attacks):

- 💼 **consulting/services** sector
- 🔌 **manufacturing** sector
- 😁 **healthcare** sector
- 🖥️ **technology** sector
- 🏗️ **construction** sector



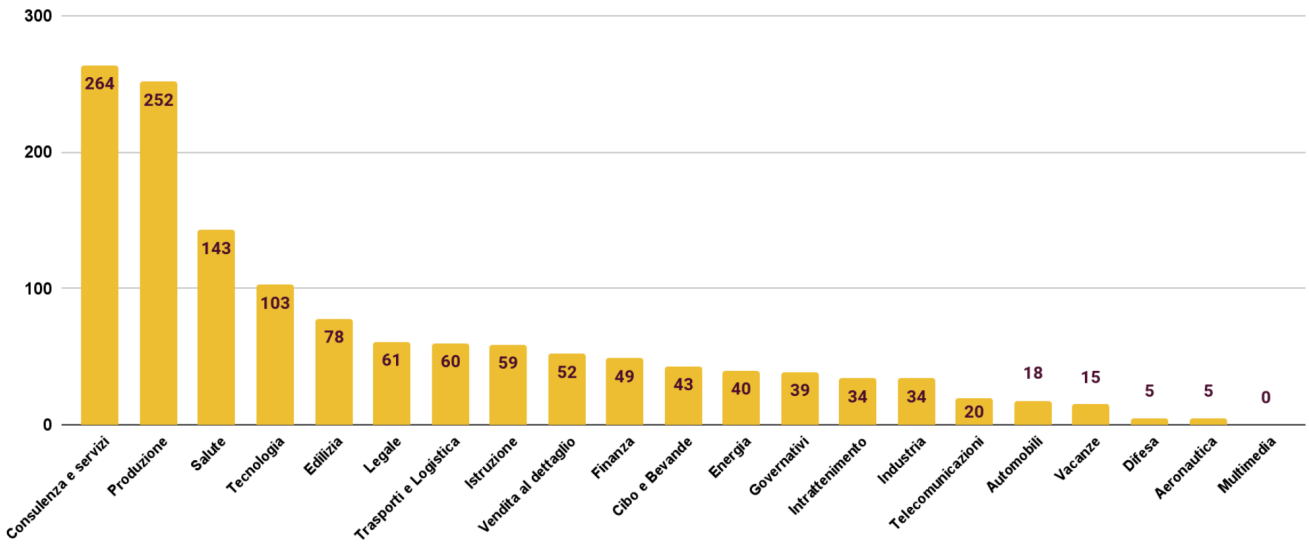
source Ransomfeed.it

As for categories that have an impact on national security, **government organizations are in thirteenth position with 39 attacks** claimed during the period. In addition, the education sector, which can have significant implications on **national security,** is in eighth position with **59 claims**. This figure underscores how cyber criminals continue to target key sectors, seeking to exploit vulnerabilities in areas critical to society.

Importantly, the **education sector**, **government organizations**, and **tertiary service companies** are **among the favorite targets** of cybercriminals. In fact, these sectors offer multiple opportunities for criminal actions to branch out, due to their extensive network of connections and centrality in the socioeconomic fabric.

Educational institutions, for example, handle a large amount of sensitive data related to students, staff, and academic research. A ransomware attack in this sector can not only compromise this information, but also disrupt teaching and research activities, causing significant disruption. If we then consider as a **highly attractive target** international interdisciplinary **schools**, where the children of leaders complete multiple educational cycles, it is easy to understand how much greater the desirability of their IT infrastructure- often not up to such sophisticated threats-is.

Government organizations, on the other hand, are a critical target because of the strategic information they handle, including citizens' personal data, financial information and national security data. An attack on these entities can have devastating consequences, affecting public trust and government operational stability.



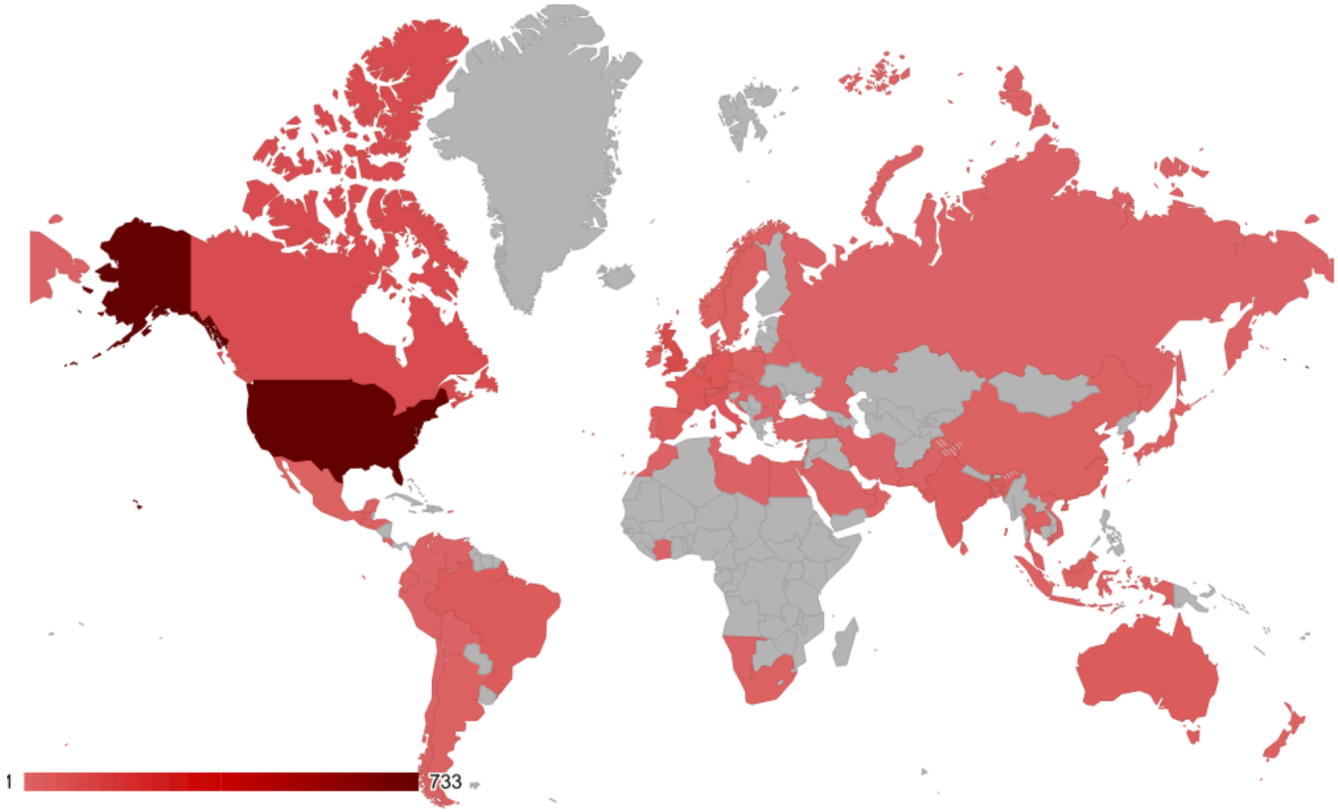
source Ransomfeed.it

Global distribution of ransomware

The continuous and **accurate OSINT work** on the platform, performed as a follow-up action to data scraping, allows each quarter to obtain a complete view of the geography of **cyber attacks based on their claims**.

Also in this four months period, as in the first and second of 2023, the northwestern region of the world appears to be the most severely affected by criminal groups.

The figure below clearly illustrates the effects of this geographic representation on a map.



in shades of red the states with victims, source Ransomfeed.it

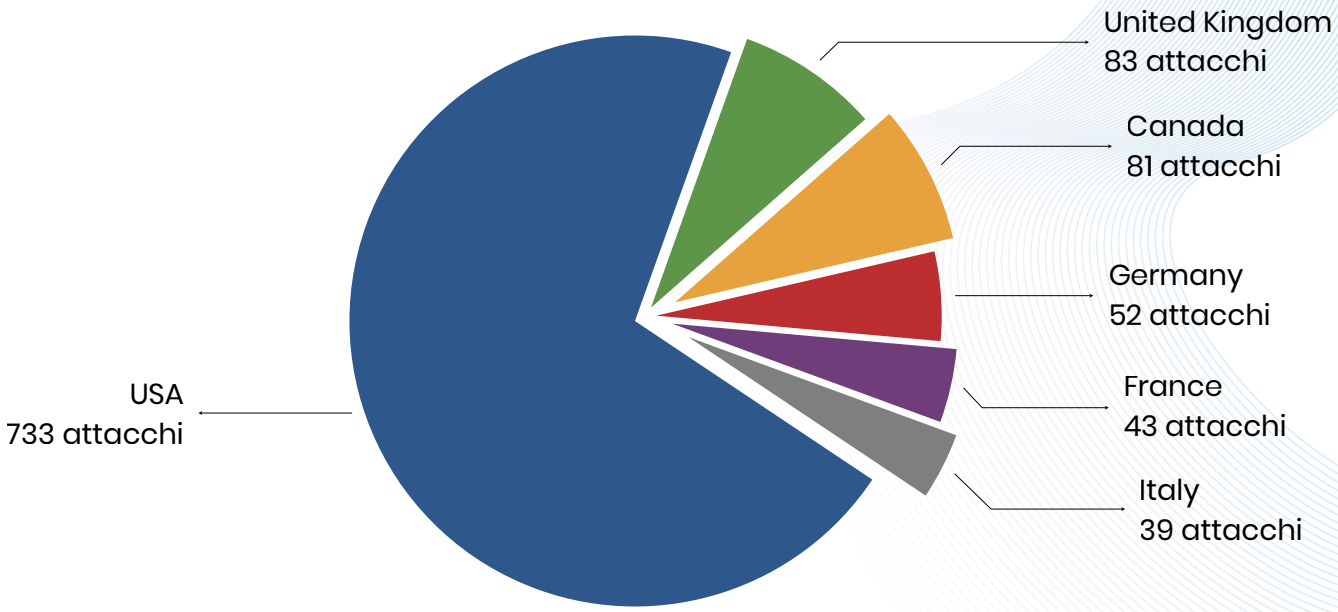
They are followed in the rankings, in order, by the **United Kingdom**, **Canada** and **Germany**, which hold the highest positions in terms of number of attacks.

These countries, like the **United States**, are home to many major economic activities and advanced technological infrastructures, making them prime targets for ransomware attacks.

USA, 51.6%	**Singapore**, 0.6%	**Denmarc**, 0.1%	**Luxenburg**, 0.1%
UK, 5.8%	**Austria**, 0.6%	**Vietnam**, 0.1%	**Croatia**, 0.1%
Canada, 5.7%	**Thailand**, 0.6%	**Portugal**, 0.1%	**Ivory Coast**, 0.1%
Germany, 3.7%	**Poland**, 0.6%	**Tunisia**, 0.1%	**Iran**, 0.1%
France, 3.0%	**New Zealand**, 0.5%	**Lebanon**, 0.1%	**Russia**, 0.1%
Italy, 2.7%	**Norway**, 0.5%	**Slovakia**, 0.1%	**Macedonia**, 0.1%
Brazil, 2.1%	**Japan**, 0.5%	**Chile**, 0.1%	**Turkey**, 0.1%
Spain, 2.0%	**Taiwan**, 0.5%	**South Korea**, 0.1%	**Namibia**, 0.1%
Australia, 2.0%	**China**, 0.5%	**Czech Republic**, 0.1%	**Bulgaria**, 0.1%
India, 1.3%	**Argentina**, 0.5%	**Hong Kong**, 0.1%	**Bangladesh** 0.1%
Switzerland, 1.2%	**Ireland**, 0.4%	**Pakistan**, 0.1%	**Honduras**, 0.1%
Netherlands, 1.2%	**Romania**, 0.4%	**El Salvador**, 0.1%	**Bermuda**, 0.1%
Sweden, 1.1%	**Saudi Arabia**, 0.4%	**Hungary**, 0.1%	**Seychelles**, 0.1%
Belgium, 1.0%	**Israel**, 0.4%	**Costarica**, 0.1%	**Palau**, 0.1%
Mexico, 0.9%	**Colombia**, 0.4%	**Barbados**, 0.1%	**Oman**, 0.1%
UAE, 0.8%	**Peru**, 0.3%	**Venezuela**, 0.1%	**Sri Lanka**, 0.1%
Malaysia, 0.6%	**Egypt**, 0.3%	**Cyprus**, 0.1%	**Puertorico**, 0.1%
South Africa, 0.6%	**Not Available**, 0.3%	**Bolivia**, 0.1%	**Morocco**, 0.1%
Indonesia, 0.6%	**Ecuador**, 0.2%	**Guatemala**, 0.1%	**Lybia**, 0.1%

source Ransomfeed.it

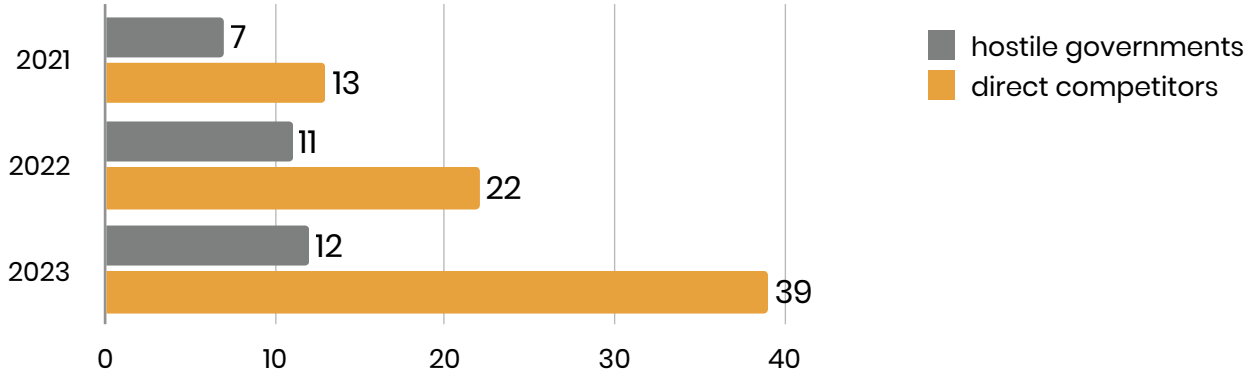
Italy, in the first four months of 2024, **ranks sixth with 39 attacks**. This figure signals an increase from previous periods.



source Ransomfeed.it

The **impact of ransomware** attacks on the economies of the countries involved is often devastating, expending not inconsiderable resources, both economically and in terms of personnel.

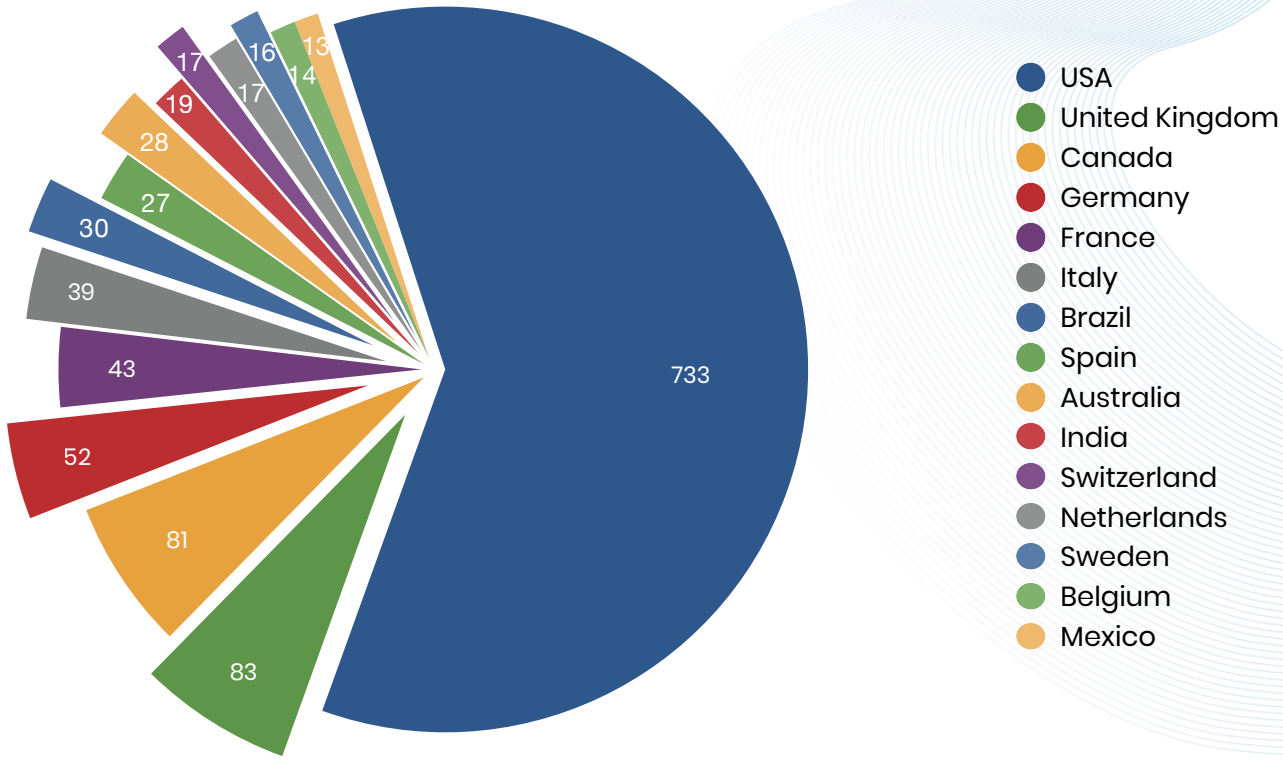
Bringing productivity to a halt for days or weeks, sending I**T procurement** and maintenance operations to a standstill, to the loss of trust and reputation, are elements that are highly coveted by competitors.
It is one reason why criminal groups are hired, by rival companies as well as by hostile governments.



aggregate sources from the dark web

Top 15

We aggregated the data to display it excluding countries with less than 1% ransomware victims.



source Ransomfeed.it

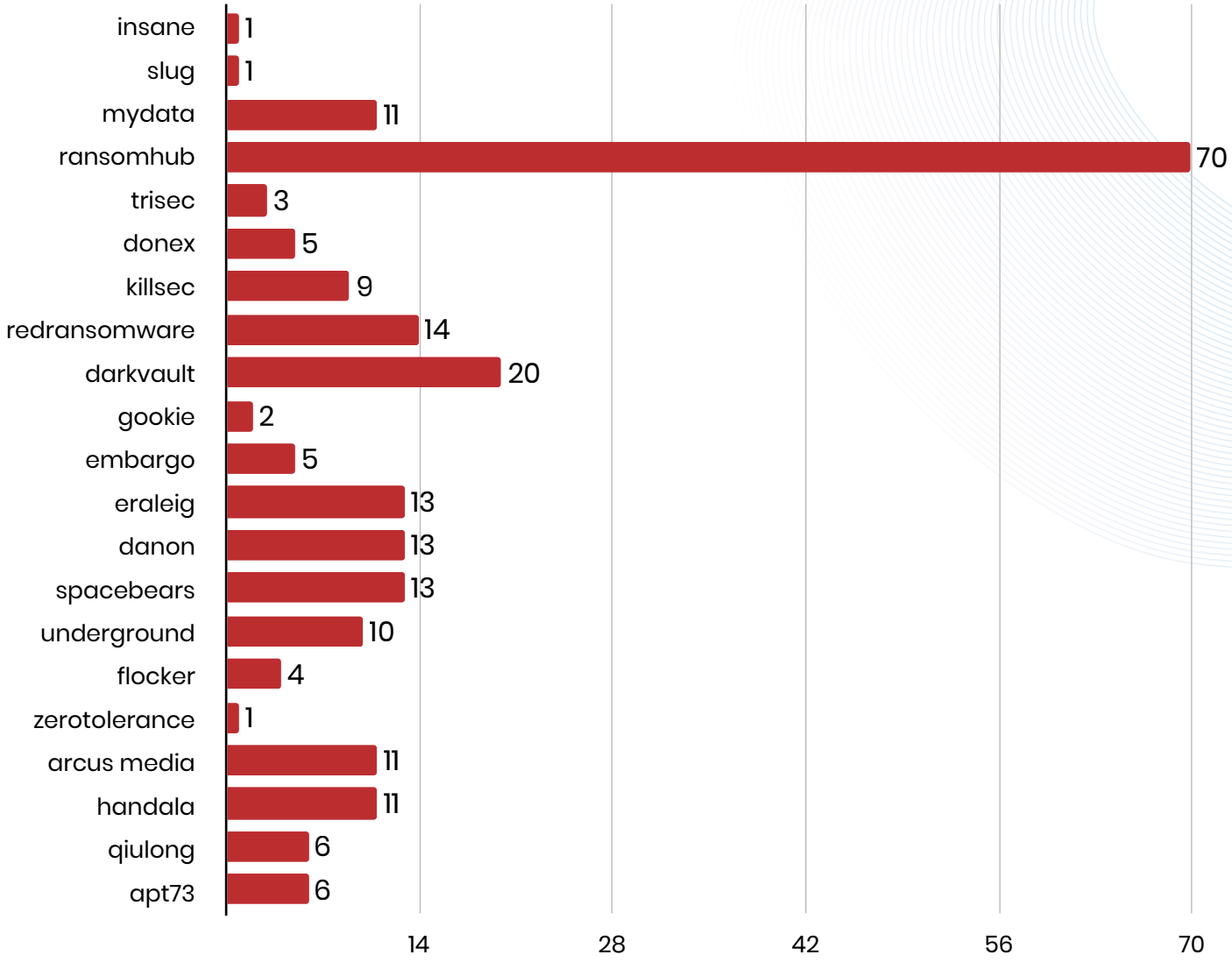
Even for this first four months of 2024, the graph shows **a large gap** between the United States and the rest of the world, clearly showing how these quantities are divided. The **United States**, with significantly more ransomware attacks, emerges as the **most affected country**. This reflects, of course, the greater concentration of industrial and corporate infrastructure in the U.S. compared to other countries.

The economic and political centrality of the U.S., globally, makes it a strategic target for ransomware attacks. Criminals know that targeting U.S. companies and institutions can have a worldwide impact, **destabilizing markets** and creating ripple effects across multiple industries.

While other countries are improving their cyber defenses, it is clear that the United States **must continue to innovate and adapt** its strategies to stay ahead of evolving threats.

New criminal groups

In the first four months period of 2024, as is often the case, **new criminal groups emerged** and **quickly gained ground** in the scene. Ransomfeed, always alert to the evolving threat landscape, detected and added these new threat actors to its daily monitoring. **A total of 226 new claimed ransomware attacks** were recorded, distributed among **25 new criminal groups**.

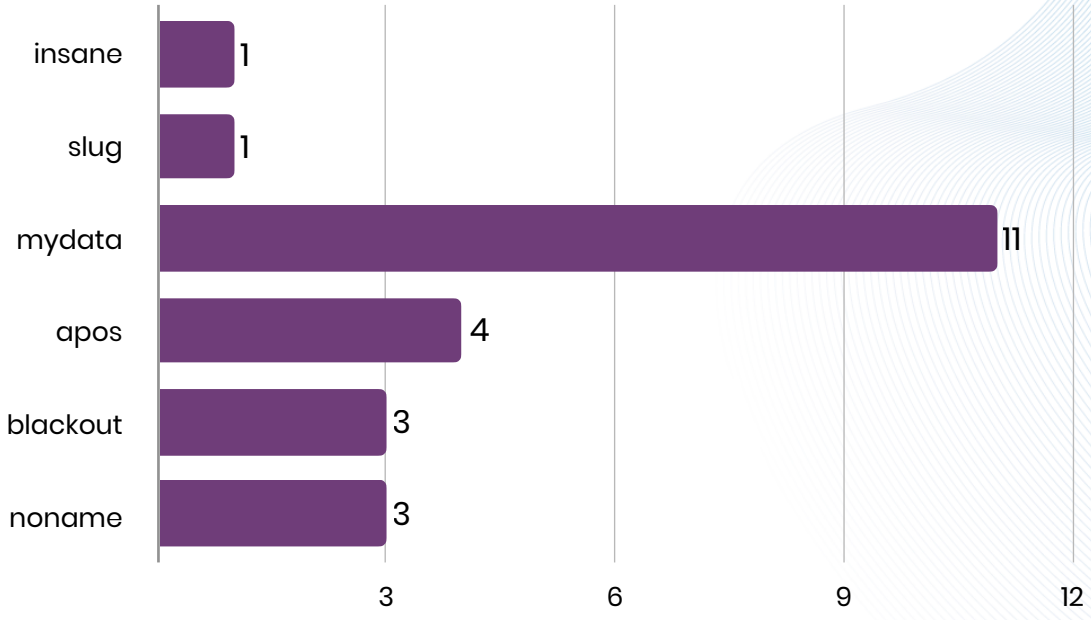


source Ransomfeed.it

Regarding the **eraleig** and **apt73** groups, we record the merger of the two, under the single name of apt73, subsequent to the entry of both into monitoring; we expressly wanted to keep the two groups separate for a better statistical count.

Excluded from monitoring is the **mogilevich** group, which **was not found** to be a real threat actor.

The proliferation of new groups on the ransomware scene is a **significant problem** not only for companies and institutions, but also for the organization of the crime scene.



source Ransomfeed.it

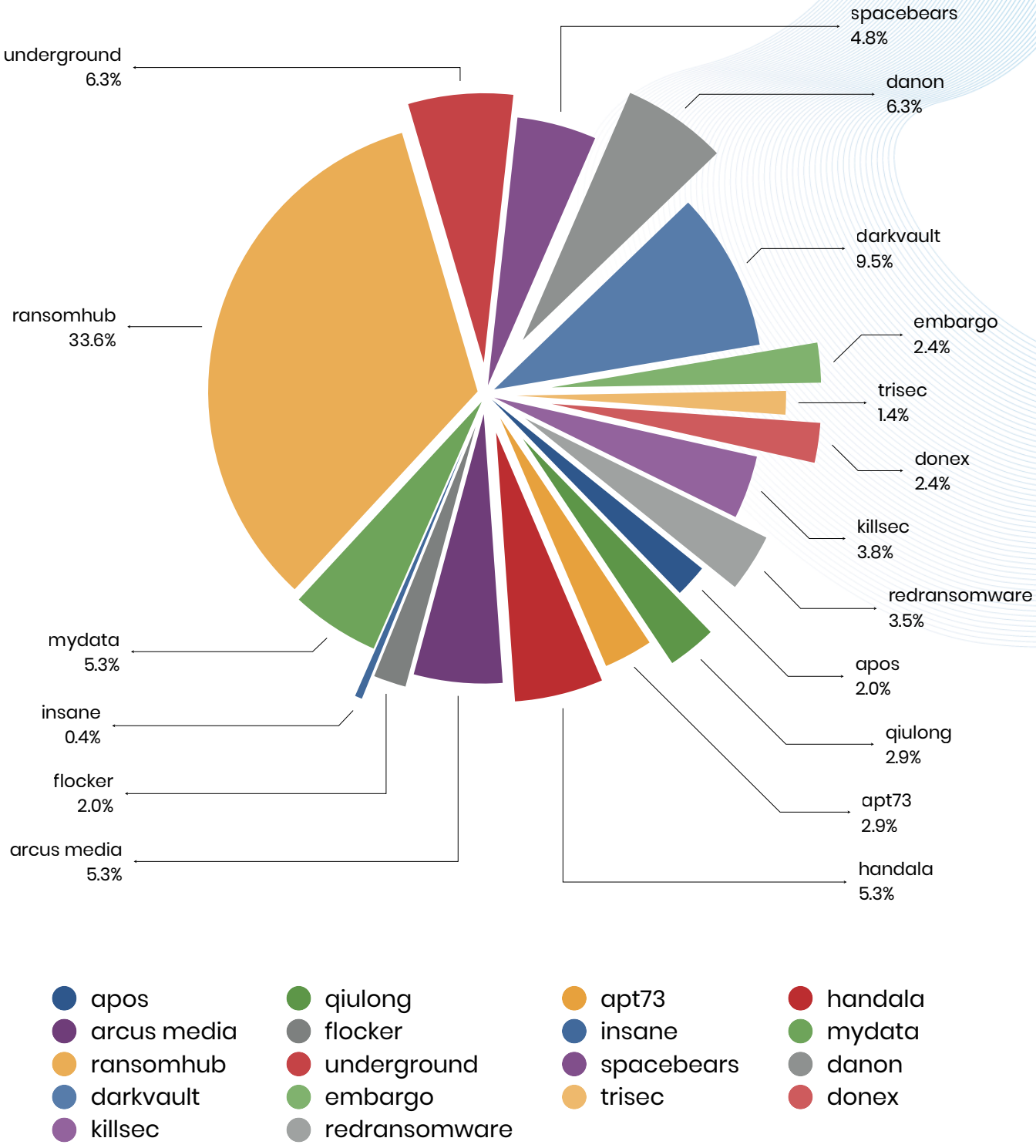
The table above highlights the groups that Ransomfeed added to its monitoring over the 120-day period of the third quarter, because they were made known during the same period.

Each group develops its own peculiarities, leveraging internal resources and, often, affiliating with larger, more stable groups - to gain access to advanced technologies and infrastructure that, on their own, they could not afford.

For example, there is talk of a ransomware group investing in equipping itself with **quantum computers**, which can process information much faster and in much greater detail; there is also talk of **large investments** on private storage of sensitive data, rather than relying on third-party hosting services.

Ransomfeed, through constant monitoring, provides valuable data to better understand these new developments and to help organizations prepare and respond effectively. Identifying and tracking the activity of these new groups is critical to anticipating their moves and taking preventive measures where possible to **mitigate the impact** of their attacks.

ransomhub turns out to be, for all intents and purposes, the group **with the most activity** during the period under consideration (**nearly 34%**, in the cluster), with diverse attacks to international targets, with a predilection for the United States.



source Ransomfeed.it

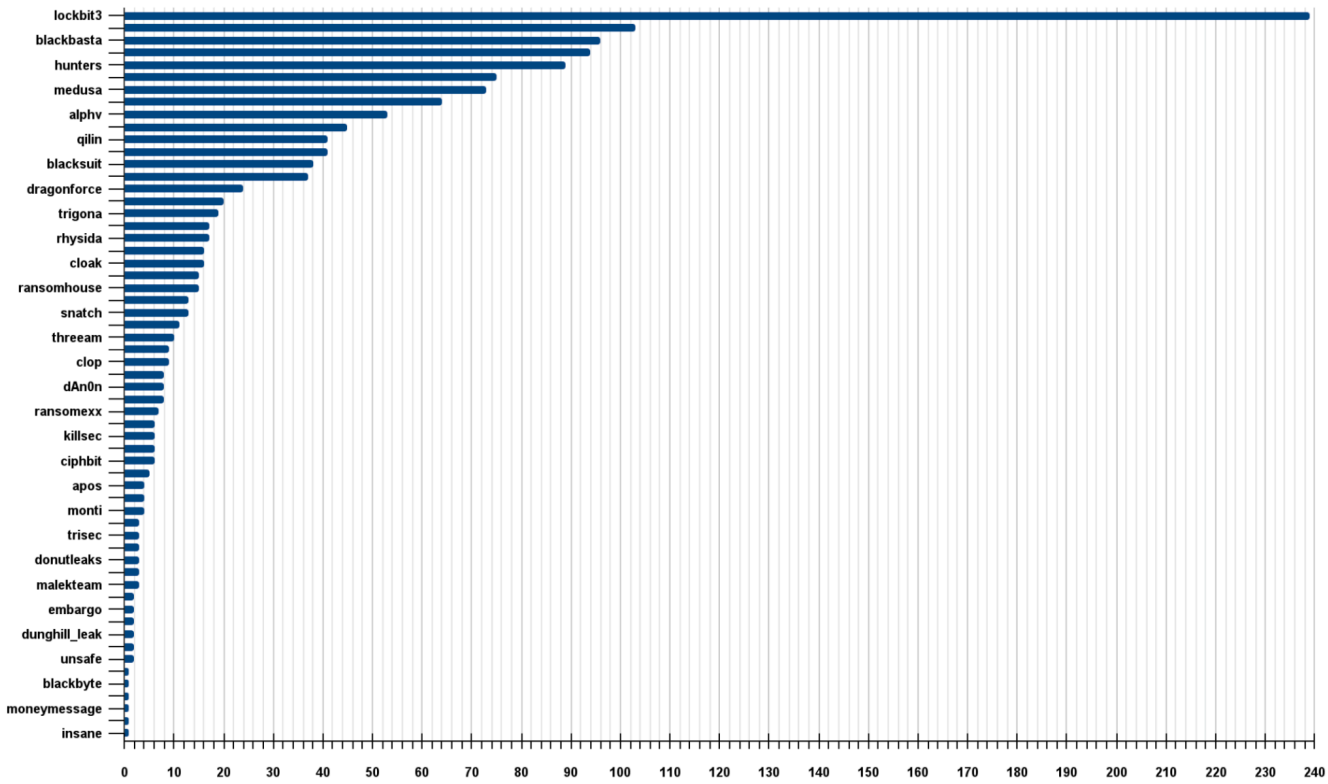
Global ransomware group activities

We isolated individual groups that generated activity in the first four months of the year. Among all the groups constantly monitored, the platform detected activity during the four-month period for **59 of them**. The other groups not mentioned were inactive, indicating a temporary suspension of their operations or possible internal reorganization.

The activities of these 59 groups revealed an **absolute leadership** of six extremely active gangs, which **alone shared 50% of the total** attacks recorded.

- **lockbit3**: undisputed leader with **17% of attacks**, although down from the same period in 2023
- **play**: with **7.3% of attack**s, it ranks as the second most active group
- **blackbasta**: responsible for **6.8% of attacks**, ranking third
- **8base**: with **6.6% of attack**s, it demonstrates considerable activity
- **hunters**: records **6.3% of attacks** to its credit
- **akira**: closes the top group with **5.3%** of attacks

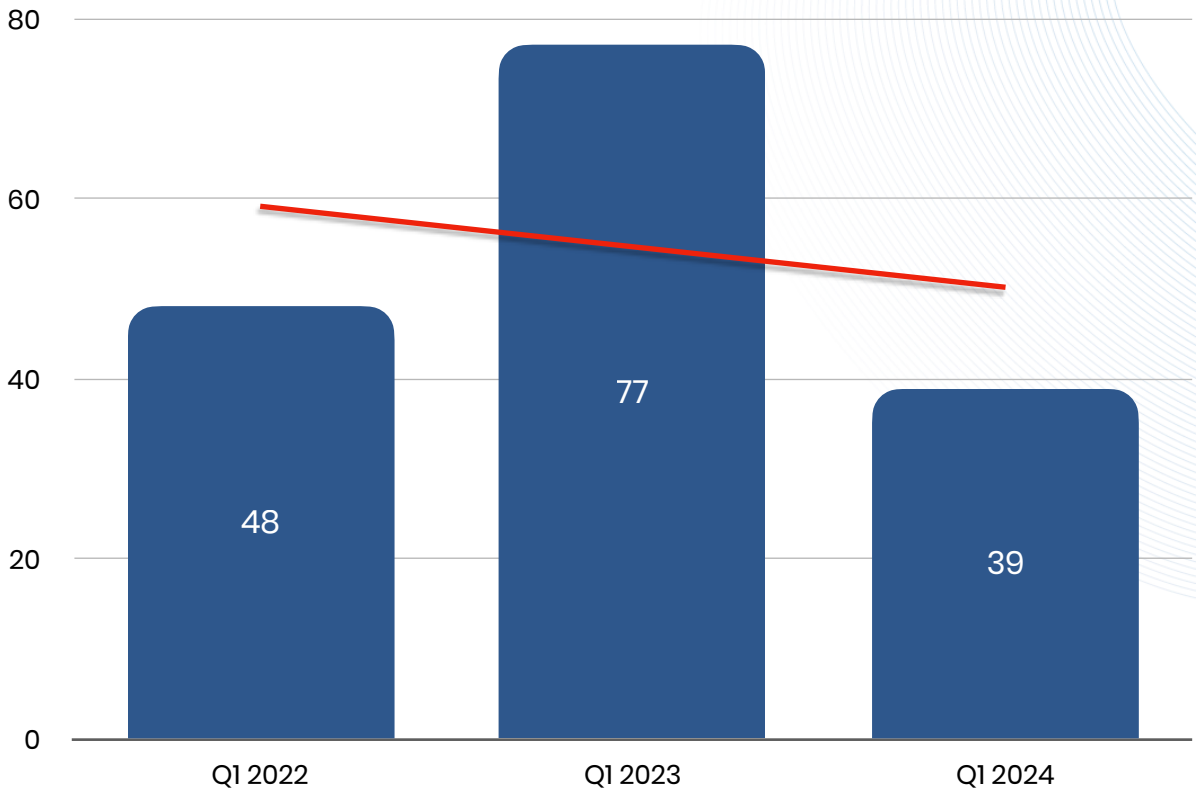
The graph shows the detail of all active cyber gangs, with the baseline value attributed to the number of victims claimed.



source Ransomfeed.it

Focus on Italy

In this section of the report we will **analyze the cluster data** already presented at the global level, focusing in particular on the **situation in Italy**. A first piece of data that certainly stands out is the **significant decrease in the number of ransomware attacks** involving Italy in the first four months of 2024. During this period, **39 attacks were recorded**, corresponding to **just over one every three days**.



source Ransomfeed.it

Thus, there was **a decrease compared to previous periods**, suggesting a **possible reduction in exploitable vulnerabilities** or an improvement in the security measures taken. However, despite the decrease, the number of attacks remains significant.

In this quarter compared to the very same months in 2023 and in 2022, the figure sees a **reversal of the overall trend**, decreasing compared to the same period in the previous year. One must contextualize this figure in the overall decrease in this four-month period, compared to the end of the year and compared to several international police actions that certainly impacted the results of the claims, in the first months of the year, and then recovered in the following months.

By **comparing this data with global data**, we can gain a more complete view of the ransomware threat landscape and emerging trends; and through specific analysis, we are **able to extract valuable information** to understand the health of companies and institutions, and the effectiveness of their mitigation strategies.

From the analysis of the sectors and types of companies affected, it is clear that technology companies, or those operating with advanced technologies, are particularly attractive to cybercriminals.

These companies, while investing significantly (compared to the stated average) in **defense strategies**, are attractive targets because of the value of their data and the criticality of their operations.

On the other hand, those **companies that do not adequately invest** in the security of their infrastructure are also all too often affected. By neglecting systems upgrades and protection measures, these realities become easy targets for attacks: lack of investment in security makes them vulnerable, exposing the entire structure to a greater risk of compromise and significant damage.

In summary, there is **evidence of a polarization** in the ransomware attack landscape: on the one hand, technology companies that are **well protected but constantly in the crosshairs** of criminals, and on the other hand, **less protected companies** that do not update their systems and are therefore easy prey for cyber criminals.

This underscores the importance of continuous investment in cybersecurity for all companies, regardless of the industry in which they operate.

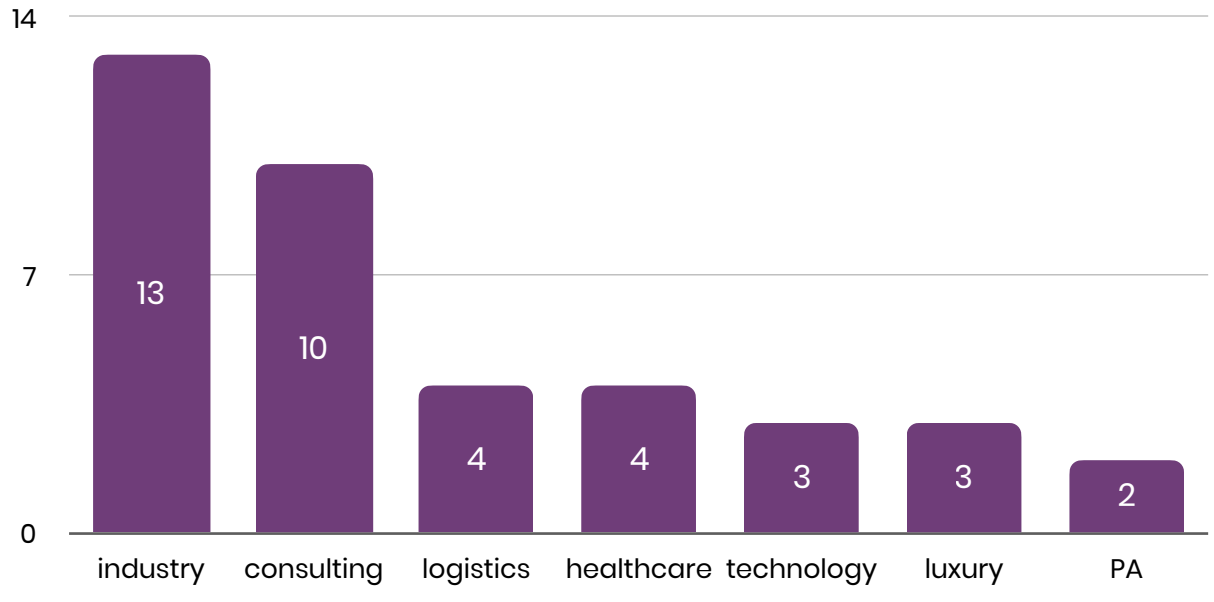
Attacks by economic area

Industry and **consulting** turn out to be the **hardest hit** business sectors in the Italy-specific focus as well. In the first four months of 2024, these sectors **suffered 13 and 10 ransomware attacks**, respectively. Within the **industrial** sector, the **pharmaceutical**, **mechanical**, **metal**, and **electronics** industries were particularly targeted. Professional firms, an integral part of the consulting sector, also suffered numerous attacks.

This was followed by the **logistics**, **healthcare**, **technology**, and **luxury** sectors; all experienced a **significant number of attacks**. Clearly, these are the most targeted sectors because of the high value of the data they handle and the criticality of their operations, making them very vulnerable to ransomware demands.

- 🏭 **industry**, 33.3%
- 💼 **consulting**, 17.9%
- 🚚 **logistics**, 7.7%
- 😷 **health**, 10.3%
- 🖥️ **technology**, 7.7%
- 💍 **luxury**, 3.0%
- 🏛️ **public administration**, 5.1%

Although the **Public Administration sector suffered only 2 ransomware attacks** in the very first four months of 2024, it shows a considerable impact. The segment mainly affected was the public health sector, however, the number of affected private companies operating as PA suppliers or partners is far higher.



source Ransomfeed.it

Distribution of ransomware across the territory

Using victim location data collected on Ransomfeed, we were able to create a **map illustrating the geographic distribution of ransomware attacks** in Italy for the first four months of 2024.

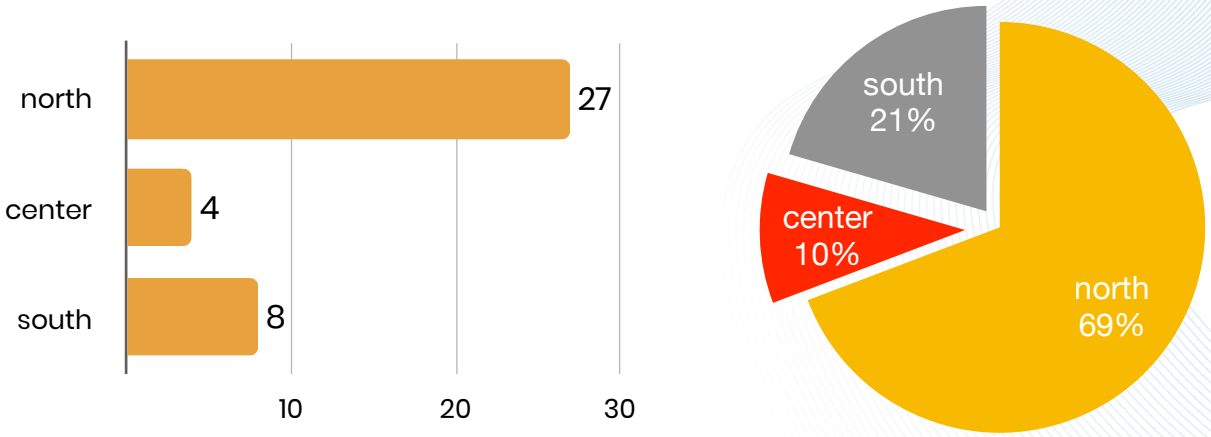
The map, which can also be viewed online with interactive features, is available at this address or by clicking directly on it.

source Ransomfeed.it

As also noted above, the **focus of ransomware attacks is often primarily on northern Italy**, a fact that has remained constant over time. Even in this period, **more than 80%** of the claims involve organizations and entities located in this area.

The high concentration of attacks in northern Italy can be attributed to the **presence of numerous technology, industrial and consulting companies**, which represent rich and often vulnerable targets.

By dividing the map into **macro geographical areas**, we obtain a synoptic representation of the distribution of ransomware attacks. The graph below illustrates this division, **highlighting the differences in impact** between the various Italian regions.



source Ransomfeed.it

Northern Italy has the highest concentration of industrial and manufacturing companies in the country; it has a homogeneous presence of s**mall and medium-sized companies** operating in sectors such as **mechanics**, **metallurgy**, **chemistry**, **automotive** and **technology**.

Compared with **southern Italy**, where industrial **density is lower** and the economy is mostly based on agriculture, fishing, tourism and light industry, the north has a long tradition of economic development, advanced infrastructure and a highly developed transportation network.

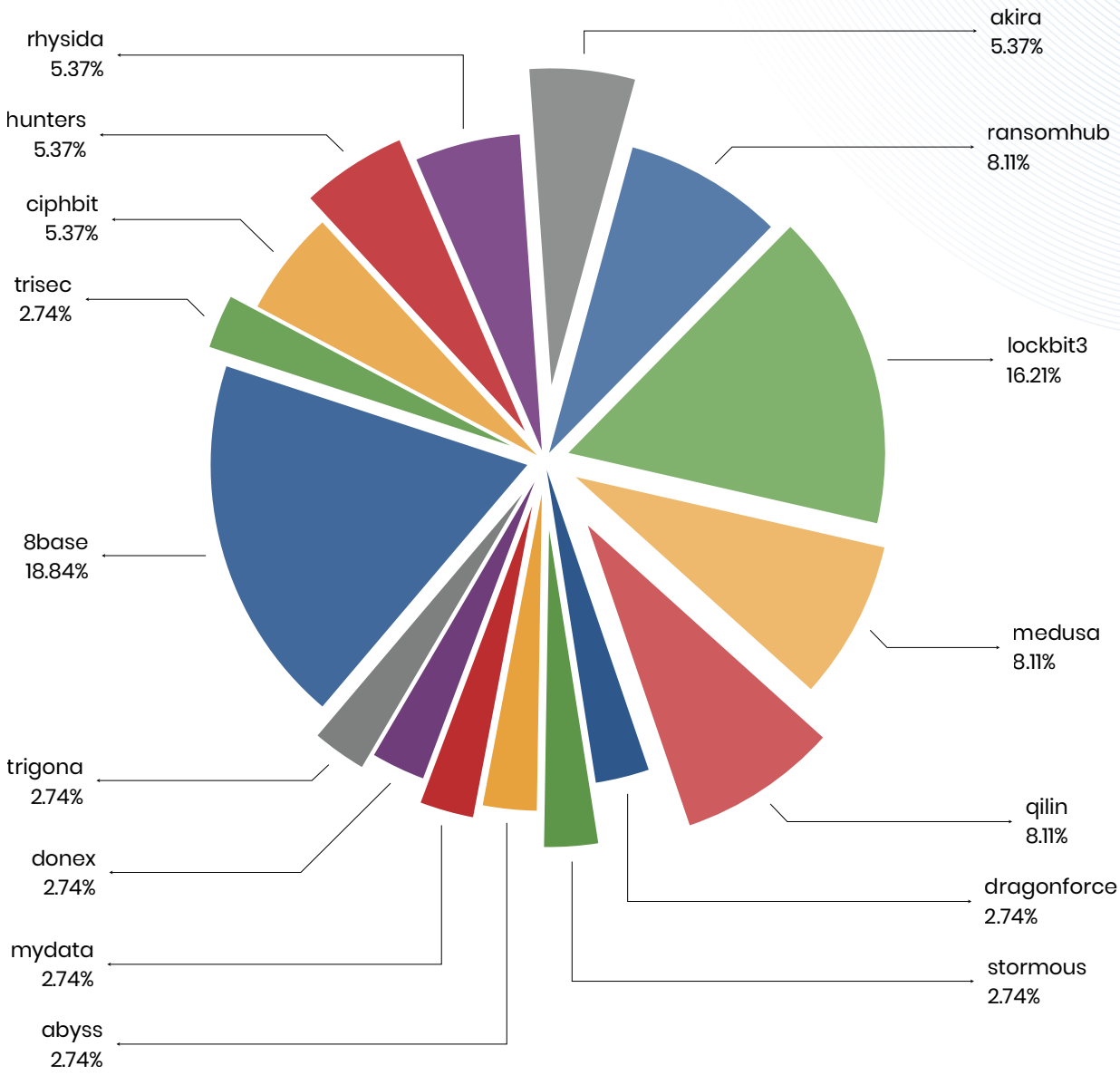
Technological innovation has gaps, both entrepreneurial and social, with a lower influx of successful investment; these factors make northern companies more attractive, thanks in part to the dense network of connections they can boast.

Most active criminals

For the first four months period of 2024, the global figure is also reflected in the analysis of cyber gangs that conducted and claimed **attacks domestically**, showing trends more or less in line with the global data. In fact, the 8base group emerged as the most active in Italy during this period, accounting for 18 percent of total attacks.

8base and **lockbit3** show a clear **predominance** in ransomware activities in Italy, showing greater efficiency and organizational capacity, despite the latter's judicial problems.

Both groups are known to **use advanced tactics**, which include the use of **0day exploits**, targeted **phishing** attacks, and the adoption of **command-and-control** (C2) infrastructures that are difficult to detect and neutralize without proper knowledge of the ecosystem.



source Ransomfeed.it

Conclusion

A **total of 204 criminal groups** operating globally were monitored, with **1,419 ransomware claims**, including **39 in Italy**.

In summary:

- **six active criminal groups** accounted for 50% of the attacks, with **lockbit3** leading the way with 17% of the total;
- compared to the same periods in 2023 and in 2022, there was an **overall decrease** in ransomware attacks;
- the most affected sectors were **industry** and **consulting**, with **pharmaceuticals**, **mechanics**, **metallurgy** and **electronics** among the main targets;
- in **Italy**, a **significant decrease** in attacks was noted in the first four months period of 2024, with **39 claims recorded**;
- the **consulting/services**, **manufacturing**, **healthcare**, **technology** and **construction** sectors accounted for **60%** of the ransomware market globally;
- **government organizations ranked 13th** in terms of claimed attacks, while the education sector ranked 8th with **59 claims**.

The **continued growth of ransomware** attacks globally and domestically is unequivocal; however, despite the increasing frequency and **sophistication** of attacks, a troubling picture emerges: awareness of cyber threats often remains insufficient, both among companies and public institutions. This **awareness gap** results in inadequate response and delays in the adoption of effective security measures.

The data presented in our report highlights how key sectors of the economy, continue to be prime targets for cyber criminals. Despite the evidence of the threat, **investment in cybersecurity is still low**. In fact, many companies do not allocate sufficient resources to upgrade and protect their infrastructure, thus exposing themselves to significant risks.

Implementing a **proactive approach to security is critical**. This includes not only implementing advanced detection and defense technologies, but also investing in staff training and awareness. Cybersecurity should not be viewed as a cost, but as an **indispensable investment** in information protection and business continuity.

source Ransomfeed.it

ransomfeed

ADVANCED **DATADRIVEN** CYBERNEWS

thank you ;)