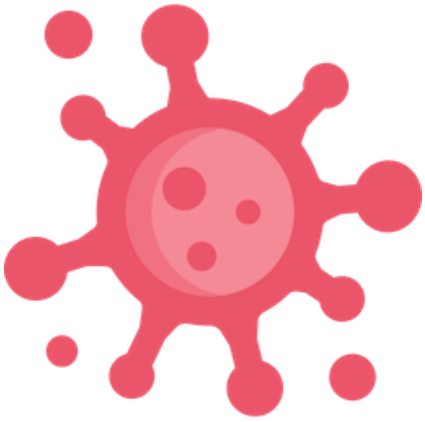


DRM / REPORT Q1 2023

Dashboard Ransomware Monitor

www.ransomfeed.it

Image generated by AI

INTRODUCTION

We are pleased to present the **first quarterly report of the year 2023** about the activities of ransomware groups globally. Thanks to our OSINT web platform, we have collected and analyzed a vast amount of data relating to these groups' claims, providing a comprehensive overview of emerging trends and patterns in the cybersecurity world.

During the first four months of the year, we have witnessed a **continuous increase in ransomware activity**, with an ever-increasing number of groups becoming the protagonists of attacks of various kinds. Thanks to our analysis tools, we have been able to identify the

tactics and techniques used by these groups, as well as the victims and countries most affected.

In this report, we'll dive into data collected during the first quarter of the year, providing valuable insights for anyone interested in cybersecurity and preventing ransomware attacks. We hope that this report will contribute to a greater awareness of online risks and threats, and to a greater ability to protect the information and systems of those who read us.

> An IBAN code or a credit card number can be replaced with an appointment at the office. Stolen personal data is lost forever.
>
> Dario Fadda

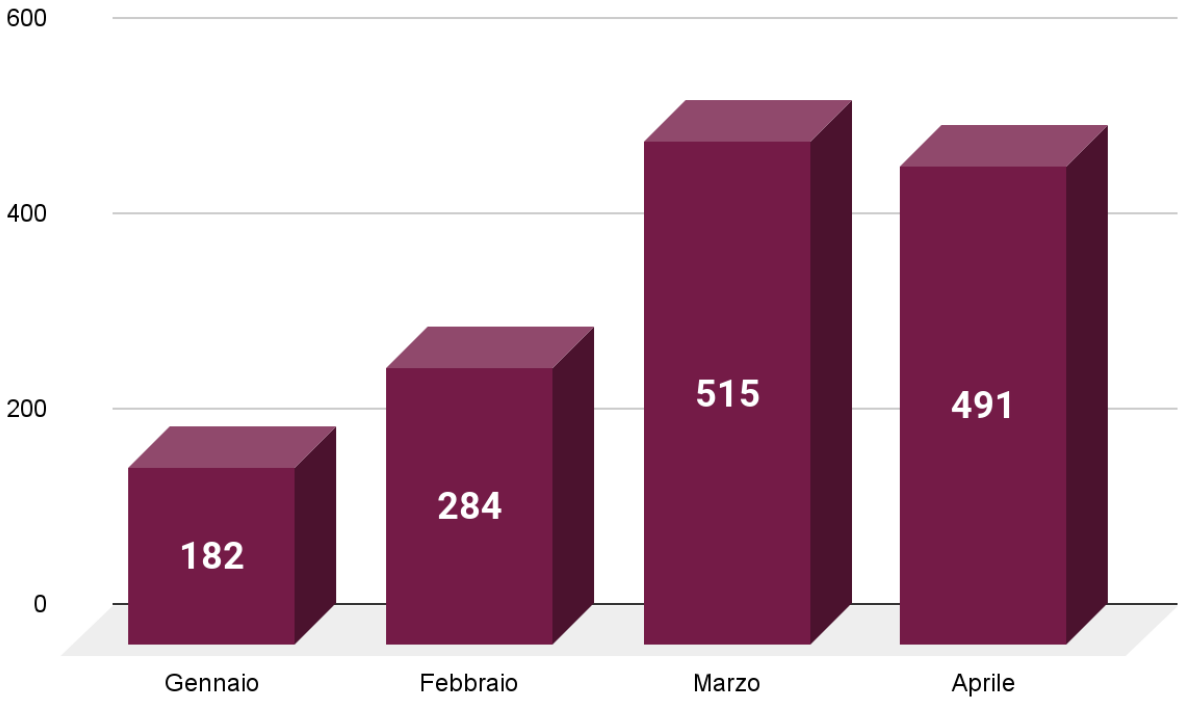
Overview

The following data was obtained from the **DRM platform** (www.ransomfeed.it) which performs it *scraping* periodically from various well-known dark web sites using the connection of the *torsock*. For this report, we will focus on the results collected in relation to the first quarter, globally, of all the monitored ransomware groups and, given the geographical affiliation of the DRM project, with a particular focus on Italy.

To do this, in the Q1 2023 platform monitored **149** cybercriminal groups operating with ransomware technologies, in addition **268** servers and

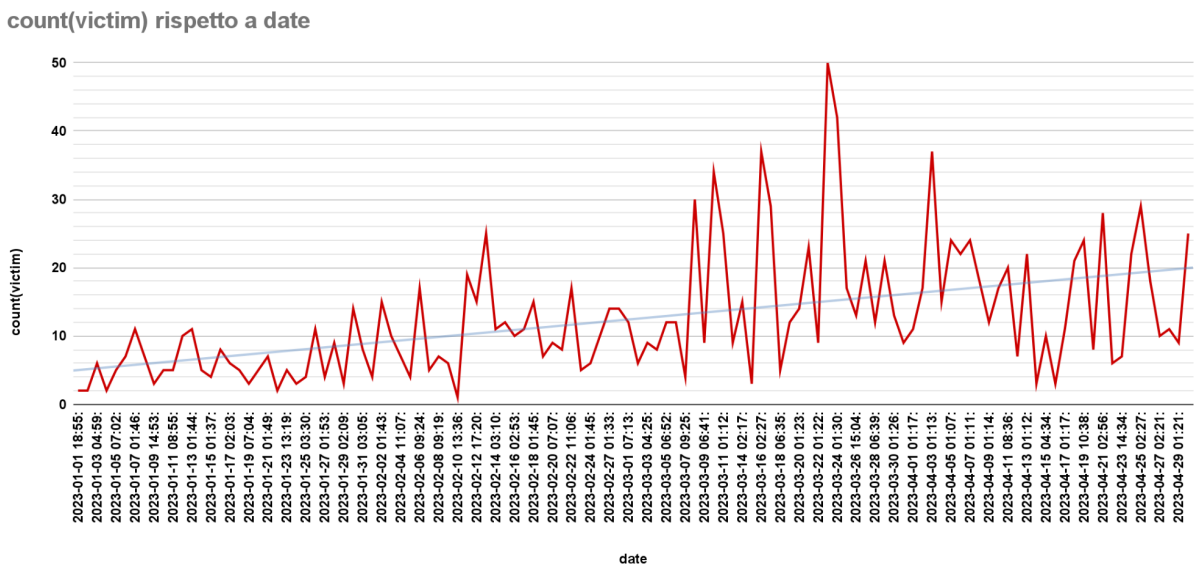
mirrors scattered across the Web; thus producing a collection of **1472** worldwide identified ransomware-type claims.

In light of this activity, it is interesting to note that **months of March and April** are reported to be the most prolific of the quarter with 515 and 491 ransomware claims tracked, respectively.



Attacks broken down by month - DRM data source

While instead among the most active days those of the central part of the quarter (March) stand out. The “richest” day of ransomware criminal claims this quarter was **March 23** with **50 victims** globally. The “poorest” day of ransomware attacks was **February 10th** with a single claim. To complete the picture of the first 120 days of the year, there are two days without any claim, February 25 and March 12.

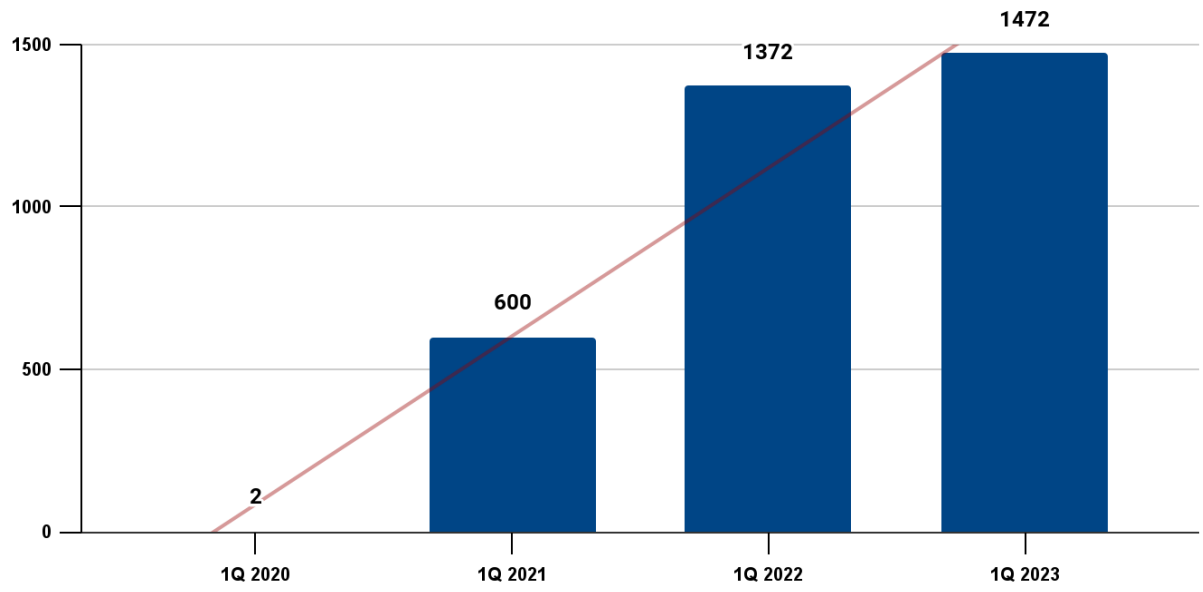


The bottom line shows the average overall trend (DRM data source)

The datum of this trend translates into a worldwide average of **12 ransomware-type attacks claimed every day**.

Comparison of quarters

With a view to accurately framing the data just presented in the Overview, we compared the data with some first quarters of the past. In fact, recalling that the DRM platform was initially fed with previous data up to January 12, 2020, we went back in time, thus interrogating the 1st Q of the last three years.

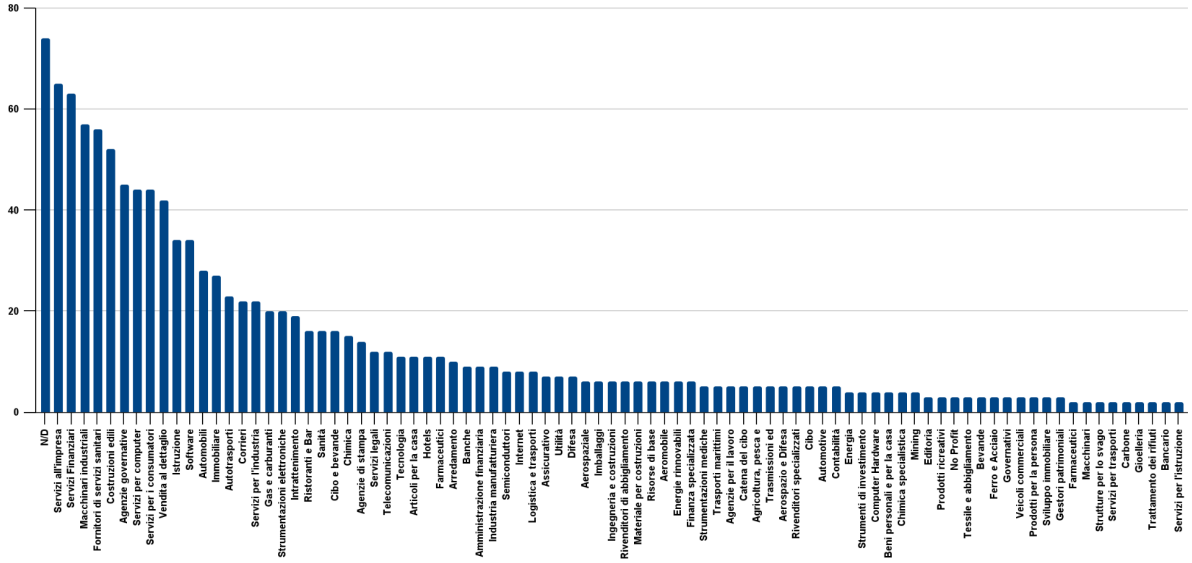


As can also be seen from the graph showing the data, **the trend is growing** and we still don't see a decrease in ransomware attacks. In this time frame, in fact, 2023 also shows an increase compared to Q1 2022 of almost **8%**. Instead, it is to be considered a positive **Rate of growth** compared to the quarters of previous years, which seems to start a downward trend. In fact, the data for Q1 2022 recorded a change compared to the same period of the previous year (2021) of as much as 129 percentage points.

DISTRIBUTION OF RANSOMWARE IN THE WORK SECTORS

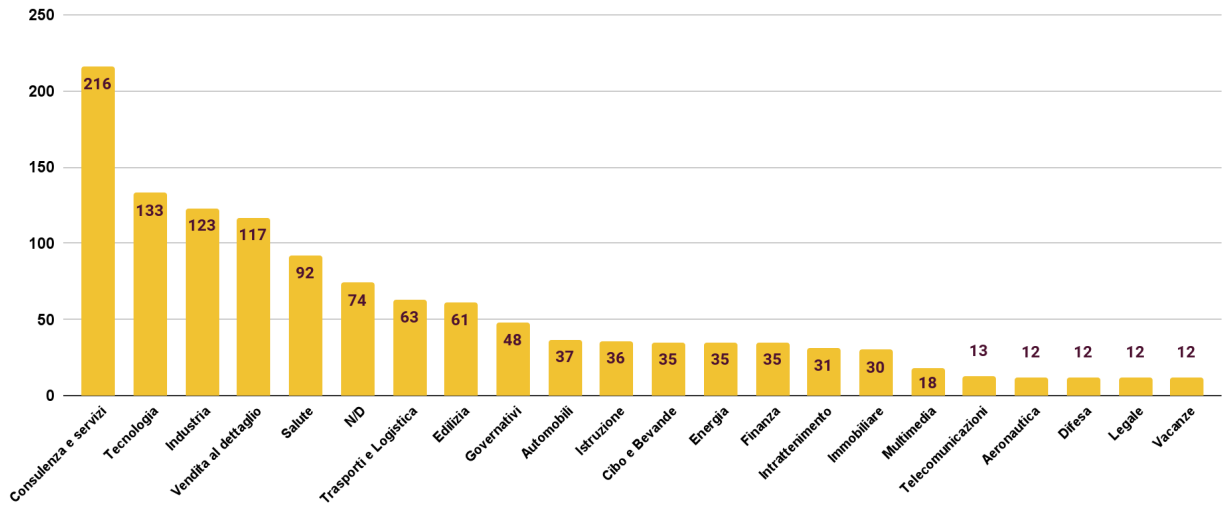
- - - - 2

From the analysis of the data of the victims involved, it can be concluded that the reference work sector most affected worldwide was that of **business services**. The result of the services sector is confirmed by the data aggregation in a specific way, with a detailed classification of 87 distinct economic categories.



Also verifying with a different aggregation of data, generated by the distinction of the victims in 22 macro sectoral areas, the sector of

Services and consultancy, is always the hardest hit of the quarter **with 17.3% of attacks.**



The attacks for the 22 macro job categories (DRM data source)

The podium of the working sectors is completed by the second place with almost 11% for **Technology** It is **Industry** followed by **Retail** below 10% and **Health at 7.4%.**

Macro sectors	% 1Q-2023		
Consulting and services	17,3	Food and beverages	2,8
Technology	10,7	Energy	2,8
Industry	9,9	Finance	2,8
Retail	9,4	Entertainment	2,5
Salute	7,4	Real estate	2,4
N/D	5,9	Multimedia	1,4
Transportation and Logistics	5,1	Telecommunications	1,0
Building	4,9	Air Force	1,0
Governmental	3,9	Defence	1,0
Automobiles	3,0	link	1,0
Instruction	2,9	Vacation	1,0

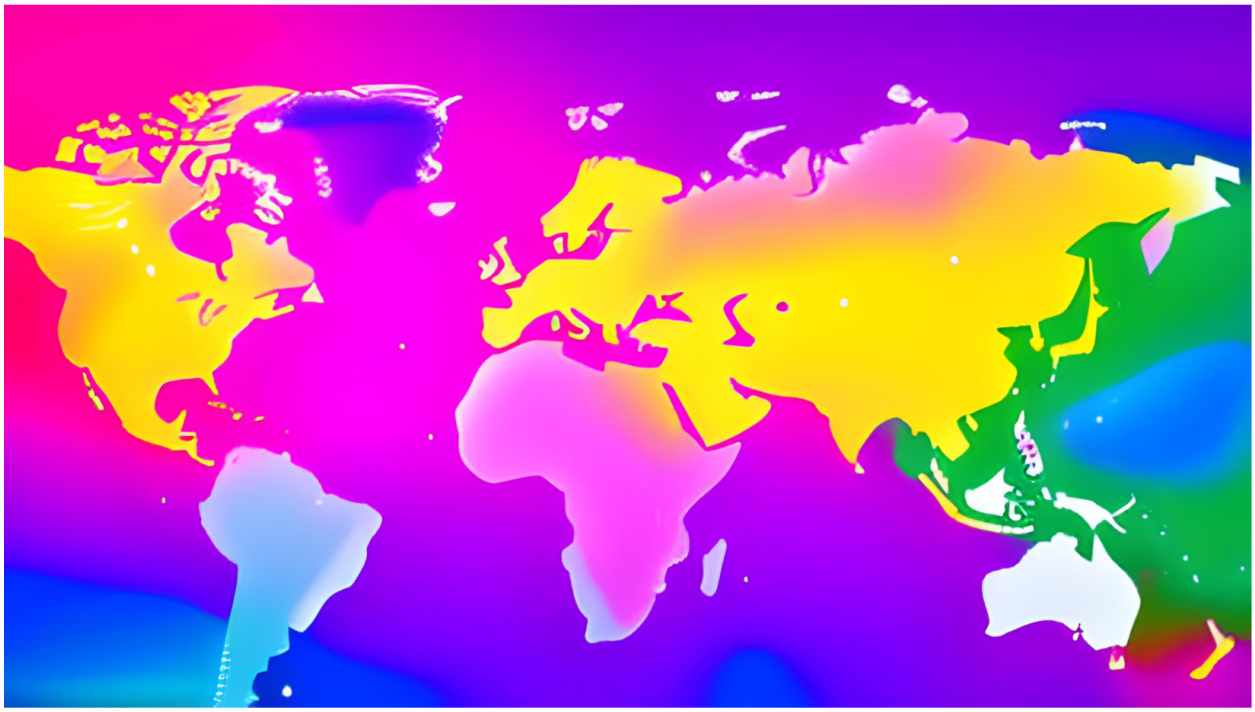


Image generated by AI

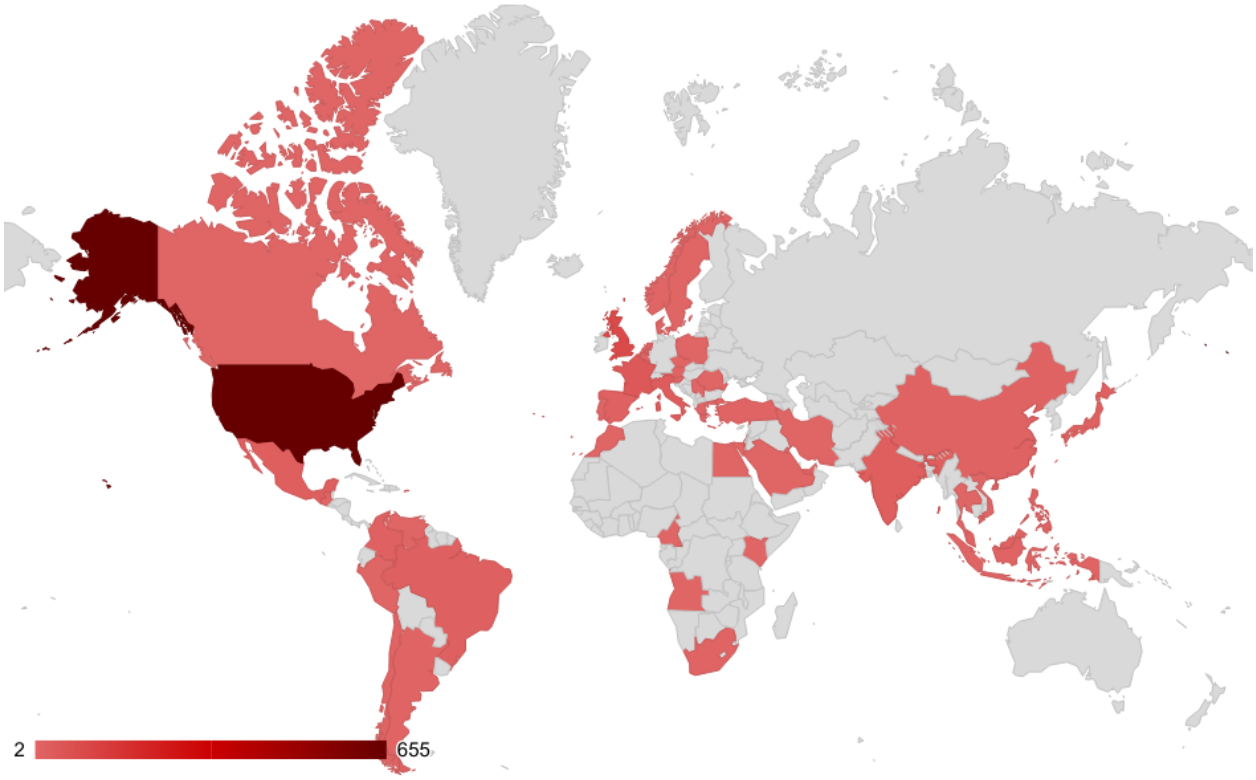
WORLDWIDE DISTRIBUTION OF RANSOMWARE

– – – – 3

The results of the DRM platform made it possible to investigate the geography of the victims claimed during the quarter.

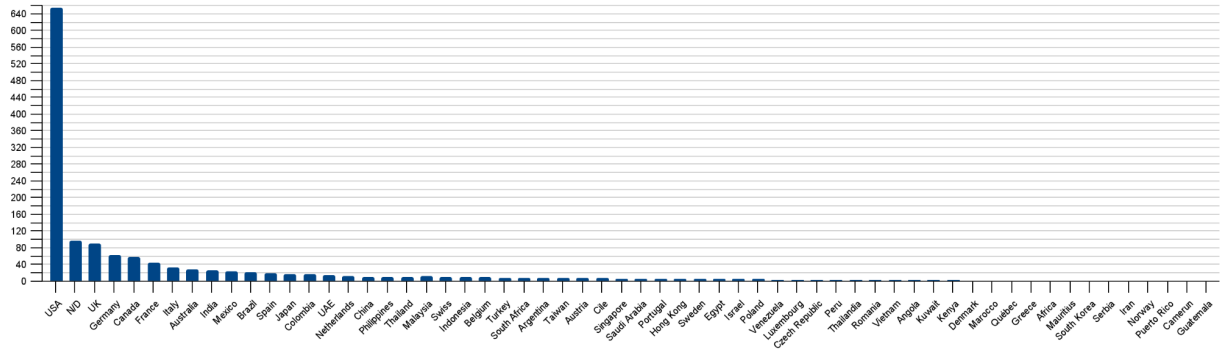
From a first massive data extraction it is possible to notice how **the northwestern part of the world** is the most severely impacted by cybercriminal groups.

In the following figure it is possible to highlight the effects of a map representation of this result.



In shades of red, states with victims (DRM data source)

A punctual translation of the entirety of the extracted data allows you to confirm the **USA as first country in the world by number of ransomware victims** in Q1-23, with 44.5% of the total. A total of 92 countries were involved (at the end of the section, the table with all the distributions recorded).



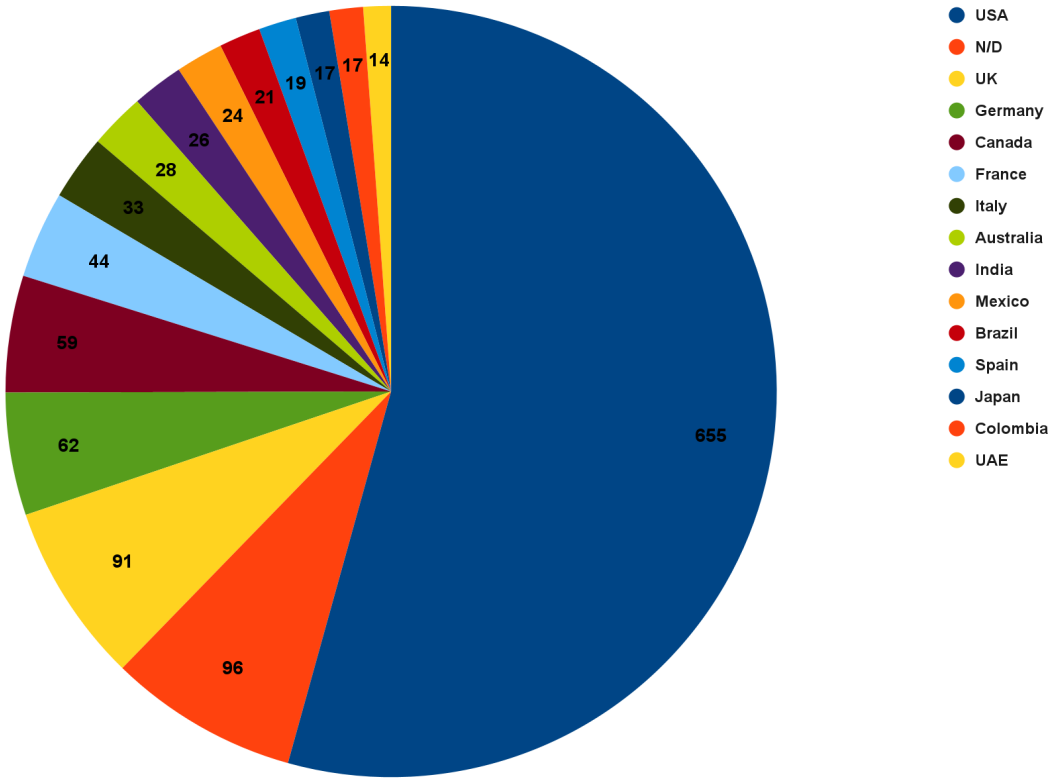
Considering that around 6.5% of the attacks analyzed are not punctually locatable geographically (due to missing or incomplete data), the United States is followed by the United Kingdom (6.2%), Germany (4.2%) and Canada (4%).

Italy is in sixth place with 2.2% of victims immediately after France (3%); in this regard, it should be noted that one of the next sections of this report is dedicated precisely to the "Focus on Italy", with **specialized data analysis**.

Country	%						
USA	44,5	Turkey	0,5	Kenya	0,2	Palestine	0,1
N/D	6,5	South Africa	0,5	Denmark	0,1	Dominican Republic	0,1
UK	6,2	Argentina	0,5	Morocco	0,1	Barbados	0,1
Germany	4,2	Taiwan	0,5	Quebec	0,1	Hungary	0,1
Canada	4,0	Austria	0,5	Greece	0,1	Pakistan	0,1
France	3,0	Chile	0,5	Africa	0,1	Algeria	0,1
Italy	2,2	Singapore	0,4	Mauritius	0,1	Slovakia	0,1
Australia	1,9	Saudi Arabia	0,4	South Korea	0,1	Saint Kitts and Nevis	0,1
India	1,8	Portugal	0,4	Serbia	0,1	Panama	0,1
Mexico	1,6	Hong Kong	0,4	Iran	0,1	Scandinavia	0,1
Brazil	1,4	Sweden	0,3	Norway	0,1	Tasmania	0,1
Spain	1,3	Egypt	0,3	Puerto Rico	0,1	Estonia	0,1
Japan	1,2	Israel	0,3	Cameroon	0,1	Finland	0,1
Colombia	1,2	Poland	0,3	Guatemala	0,1	Korea	0,1
UAE	1,0	Venezuela	0,3	Slovenia	0,1	Bangladesh	0,1
Netherlands	0,8	Luxembourg	0,3	Maldives	0,1	Cyprus	0,1
China	0,7	Czech Republic	0,3	Republic of Trinidad and Tobago	0,1	Macedonia	0,1
Philippines	0,7	Peru	0,3	Ecuador	0,1	Nigeria	0,1
Thailand	0,7	Thailand	0,2	Albania	0,1	My own	0,1
Malaysia	0,8	Romania	0,2	Jordan	0,1	Croatia	0,1
Swiss	0,6	Vietnam	0,2	Uruguay	0,1		
Indonesia	0,6	Angola	0,2	Ireland	0,1		
Belgium	0,6	Kuwait	0,2	Arrived	0,1		

TOP 15

Again, we aggregate the data to show it excluding countries under 1% of ransomware victims and graph it for the top 15 globally, each with the number of claims filed.



Top 15 by number of victims (DRM data source)

From this graph it is more visible the **gap between the US and the rest of the world**, but the same indexing as the general classification is respected with **UK, Germany and Canada among the top positions**.

NEW CRIMINAL GROUPS

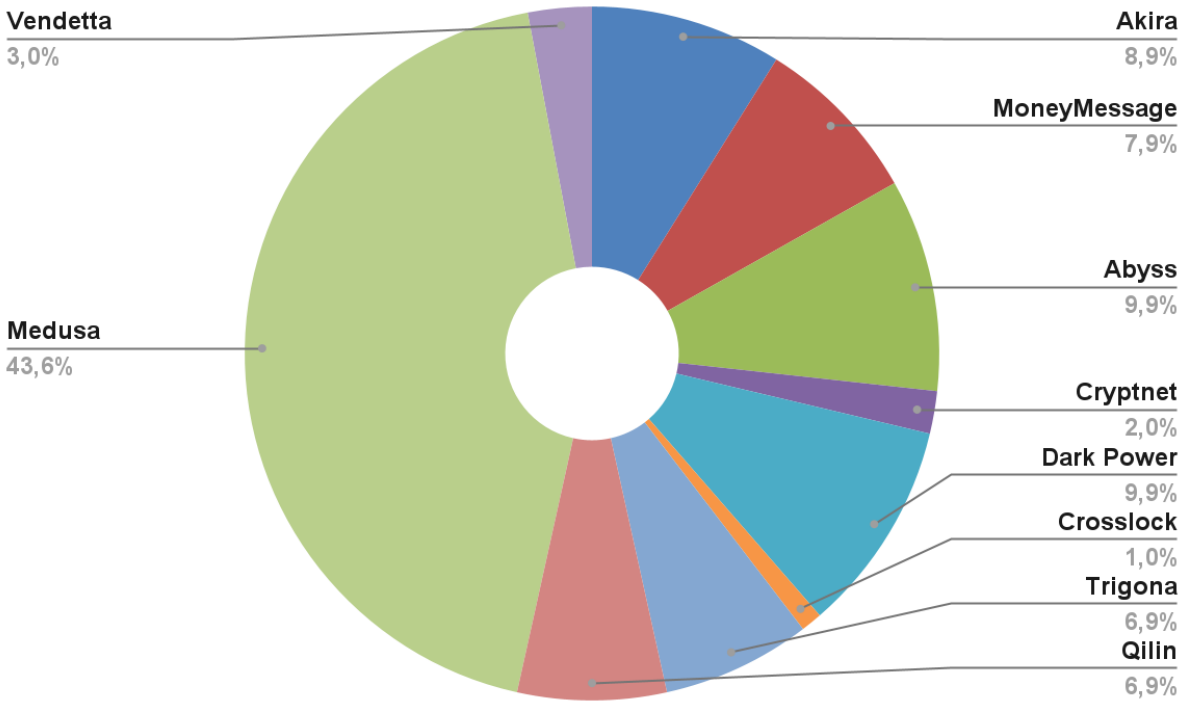
- - - - 4

As is known, the cybercrime scene, even in the case of the malware sector (in this specific case we analyze ransomware), frequently sees the growth of the workforce in the field.

Q1-23 is not excluded and has seen the appearance of **11 new groups** which together they claimed **101 cyber attacks** all over the world. Just under one attack per day, only from new groups just starting their own criminal operations.

NEW ADDED	
Akira	9
MoneyMessage	8
Abyss	10
Cryptnet	2
Dark Power	10
Crosslock	1
Trigona	7
Do it	7
Medusa	44
Vendetta	3
Nevada	0

The table above shows the groups that the DRM platform added to the monitoring in the 120 days of the first quarter, because they were disclosed in the same period.



Reporting the data in percentage terms, we can easily understand which, in Q1-23, were the most active new cyber gangs, with **Medusa exceeding 43%.**

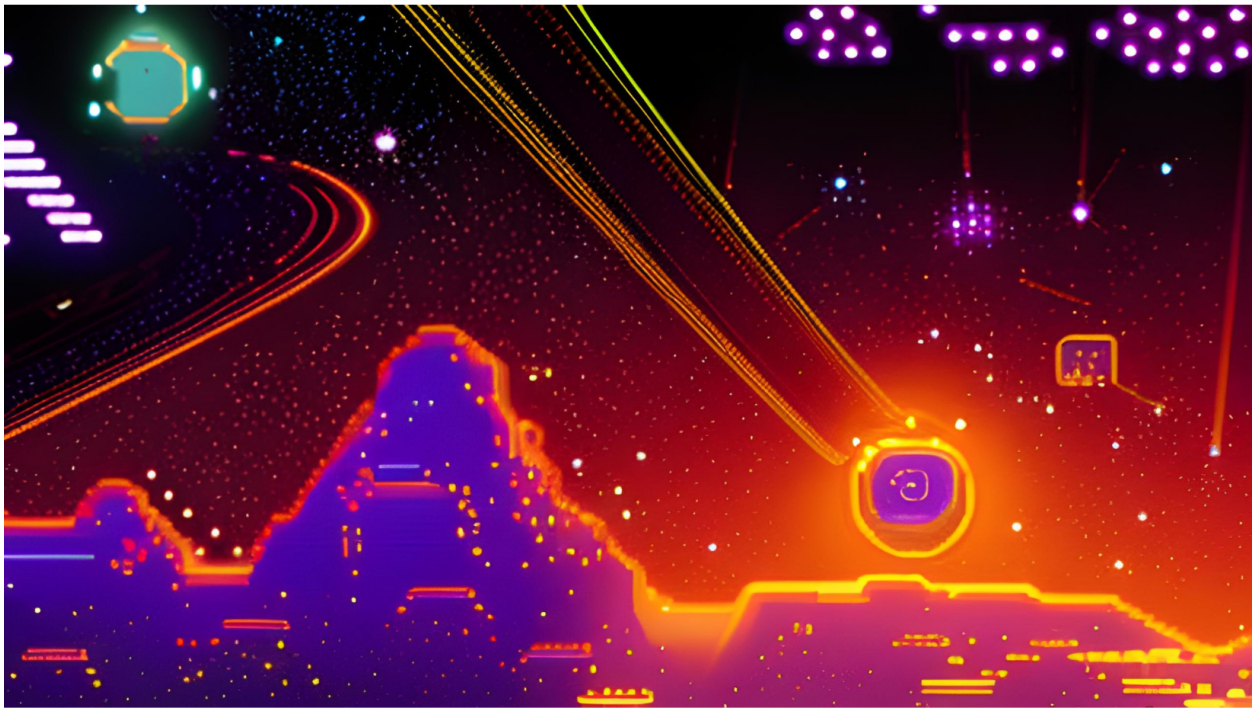


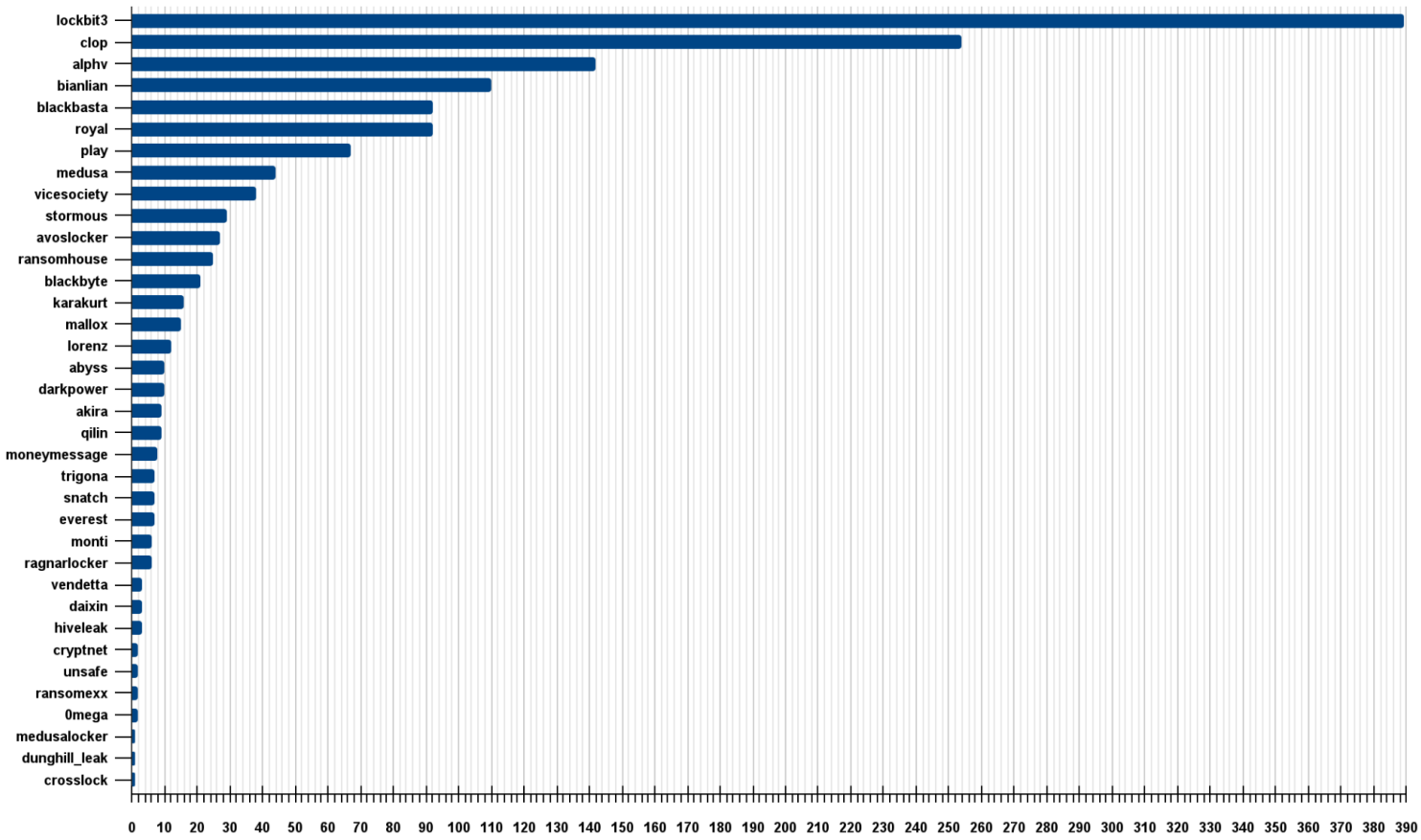
Image generated by AI

THE GLOBAL ACTIVITIES OF RANSOMWARE GROUPS

One of the clusters analyzed for this report contains data on individual criminal groups. Of all the groups that are constantly monitored, the platform detected activity in the quarter for 36 of them. The others were inactive.

The activities of these groups have produced the total of data that we are analyzing in the pages of this report and have seen an absolute leadership of three extremely active groups, capable by themselves of dividing 53% of the attacks. The trio is led by the criminal group **LockBit which alone accounts for 26.4%** of the attacks; followed by **Clop** and **ALPHV/BlackCat** with 17.3% and 9.6% respectively.

A precise detail of all the 36 active cyber gangs is offered by the following graph, whose reference value is attributed to the number of victims claimed. In this way we can also monitor the activity, at a global level, of the currently less active groups.



In this regard, it should be noted that the LockBit data reported here can be attributed to the lockbit3 operation (the previous ones are in fact abandoned and no longer active) and that this new rebranding was completed recently, with a change that took place in the month of June 2022.

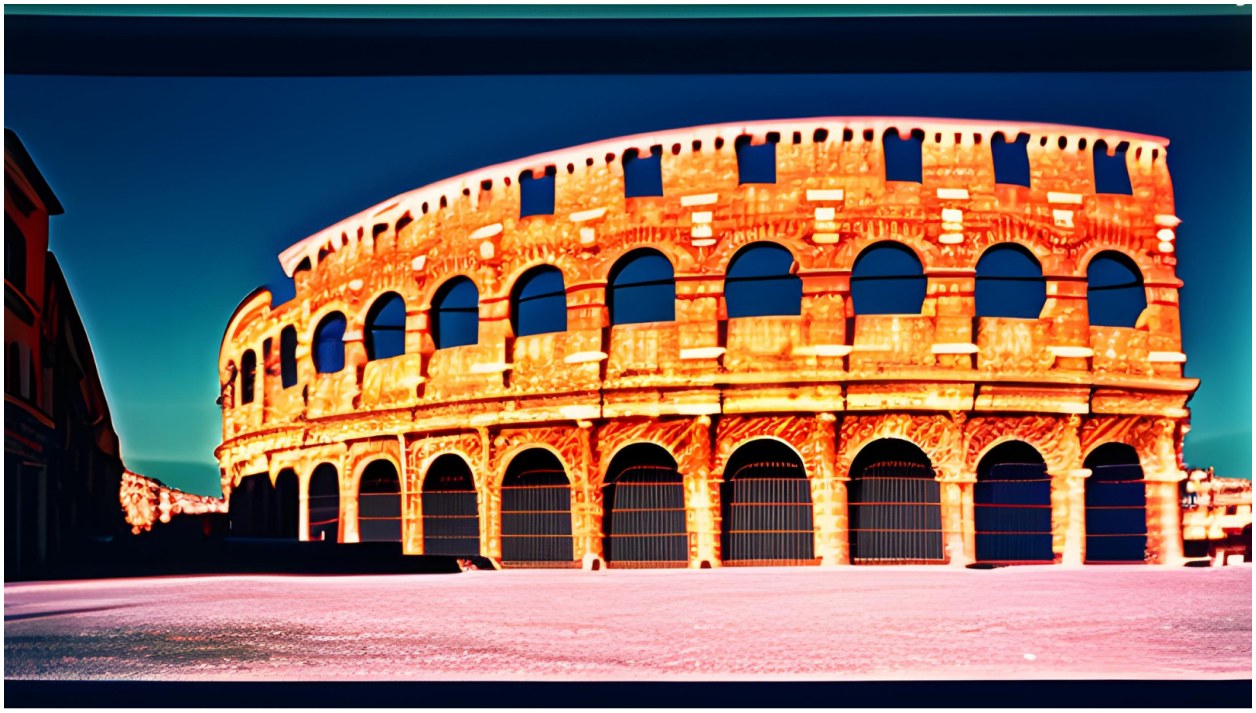


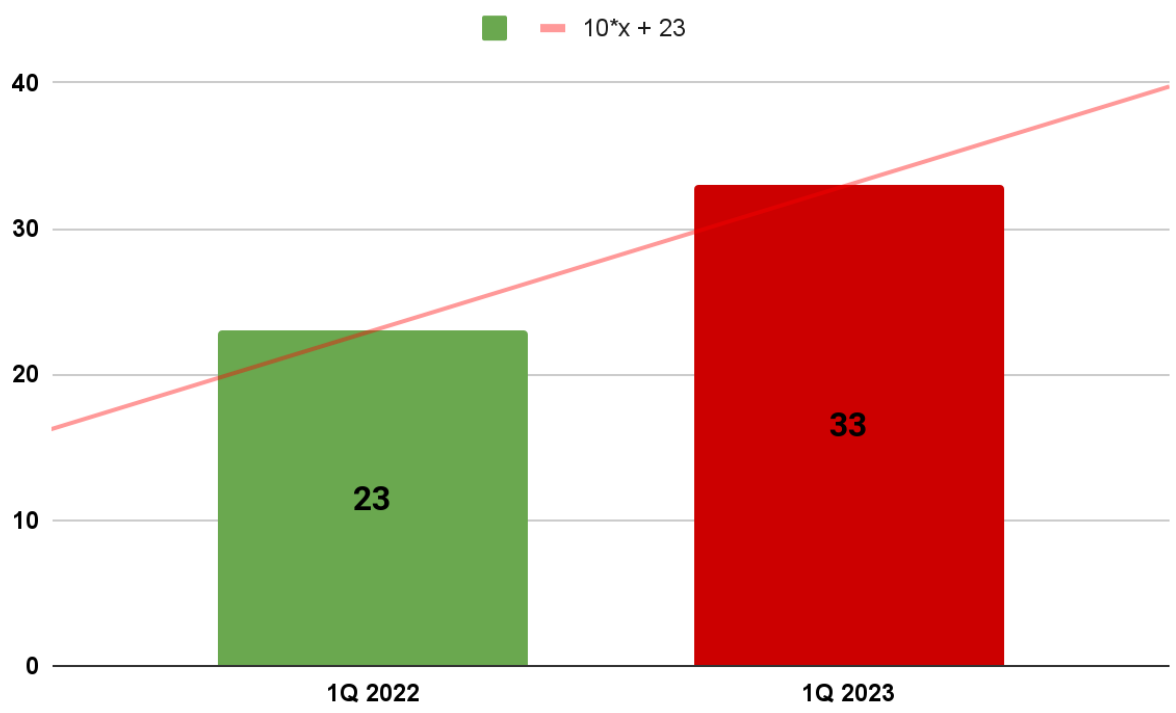
Image generated by AI

FOCUS ITALY Q1-23

As stated in the Introduction of this report, since the DRM (Dashboard Ransomware Monitor) platform is an Italian project, we feel obliged to dedicate a section of this report to the analysis of data relating to Italy.

This section therefore reports all the analyzes already previously treated globally in the previous sections, but with the *query* specific for Italy.

The first datum that surely emerges is the number of **Ransomware attacks involving Italy in Q1-23 totaled 33**. About one every 84 hours.



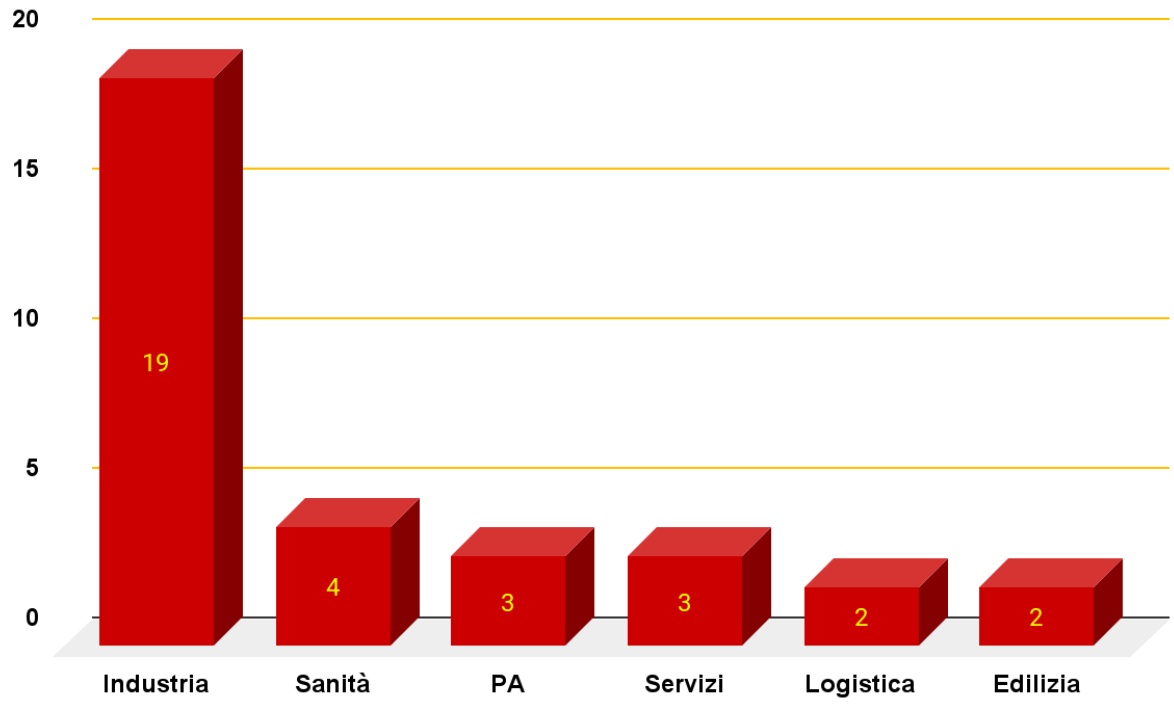
This data perfectly reflects the global trend, which is constantly growing compared to the same period of the previous year. However the **growth rate in Italy is 44%** compared to 2022.

Attacks by economic sector

The category most affected by ransomware-type attacks, in Q1-23 we highlight the **Industry**, in a generic way (among these, the pharmaceutical, mechanical, metallurgical and electronic sectors), with 19 claimed ransomware attacks in the period.

Beyond the **57% occupied by industry**, follows the **healthcare sector** and that of the **Public administration**, whose numbers however drop and distance themselves from the primary sector, between 12% and 9%.

A precise breakdown of the data, of all the working sectors, is shown in the graph below.



In percentage terms, we can also read this data with the table below, which helps us in the analysis phase to interpret them for each category, with respect to the total number of attacks.

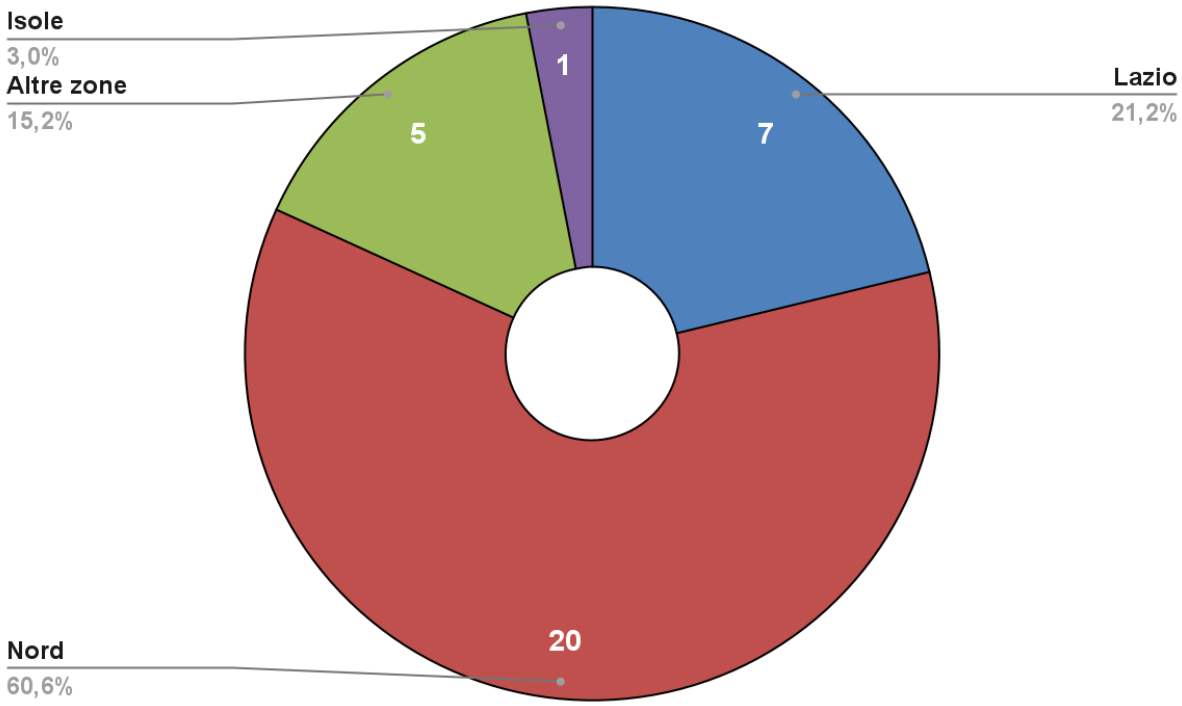
Aggregate sectors	%
Industry	57,6
Healthcare	12,1
Public Administrations	9,1
Services	9,1
Logistics	6,1
Building	6,1

The distribution of ransomware in the territory

With the data on the location of the victims operated by the DRM platform we were able to draw a map to define the geographical distribution of the ransomware in Italy, for Q1-23. The following map can also be consulted online, with the interactive functions, at the following address: https://www.google.com/maps/d/u/1/edit?mid=1qDLdY_C-QX8XwhS5YI1VRJ0nARXQ2PI&usp=sharing

Beyond the **60%** of the claims is related to organizations and agency of **Northern Italy**.

If we divide the map into geographical macro areas we obtain a synoptic representation as in the following graph.

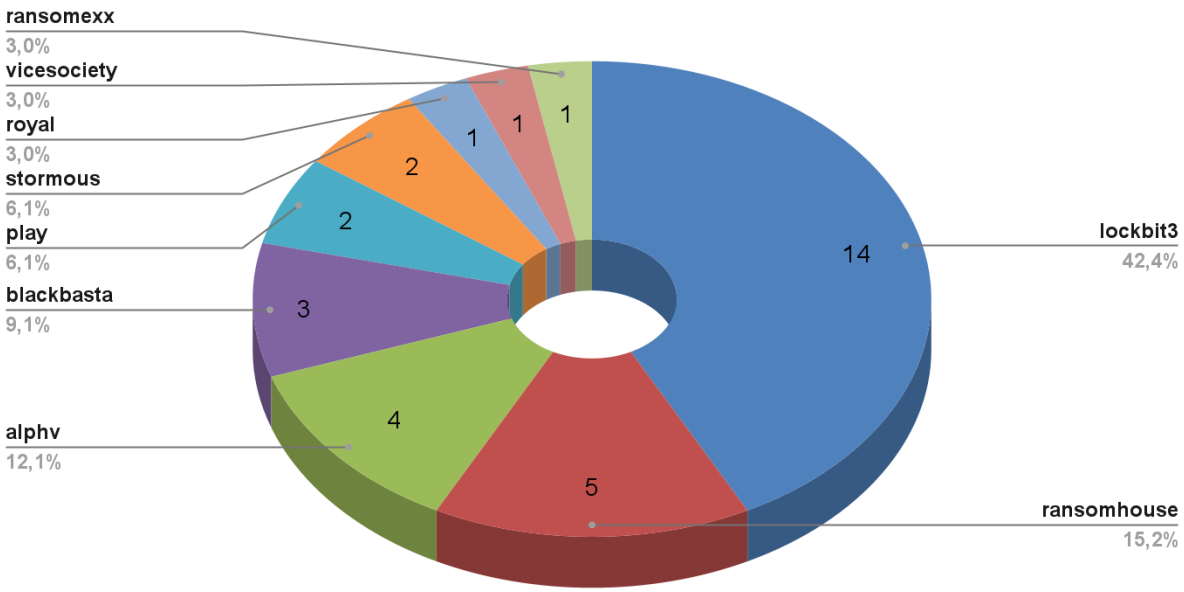


The most active criminal groups

The global data is also reflected in the analysis of the cyber gangs that carried out/claimed the attacks on the national territory.

Effectively **LockBit** proves to be **the most active group also in Italy**, for the quarter with 42.4% of attacks.

They follow, at an important distance, **Ransomhouse** and **ALPHV/BlackCat**, which together divide the 27.3% almost evenly.



The graph shows all the attacks against Italian victims, reporting the percentages of each group and with the data inside, the number of victims claimed.

CONCLUSION

The data that this report has brought to light and analyzed show how ransomware, including Italy throughout the world, is not a threat to be forgotten. It is following an ever-increasing trend compared to the same period of previous years, a growth rate of 8% which however generates optimistic behavior when compared to the rate of the same period two years earlier (which was 129%).

Italy is the sixth country in the world for the number of ransomware attacks, while the United States occupies the first position with 44.5% of attacks located within its geographical area.

LockBit (operation 3) establishes itself as the most prolific criminal group in the world, both globally and in Italy.

In summary, the analysis of the data on the operations of ransomware groups shows a trend towards an increase in the number of attacks and the sophistication of the techniques used. The spread of these attacks poses a growing threat to organizations of all industries and sizes. Protecting against these attacks requires a combination of advanced security technologies, robust security practices, and employee training. Furthermore, cooperation between organizations and governments at the national and international levels is essential to mitigate the impact of ransomware on global communities.

Dashboard Ransomware Monitor

www.ransomfeed.it