

DRM

AN ITALIAN PROJECT 

DASHBOARD RANSOMWARE MONITOR

REPORT Q2 2023

DASHBOARD RANSOMWARE MONITOR

INDEX

Introduction to this Report	1
Overview	2
• Quarterly comparison	
Distribution of ransomware across industries	6
Worldwide ransomware distribution	8
• Top 13	
New criminal cyber groups	11
Global activities of ransomware groups	13
Focus Italy Q2 2023	14
• Attacks by economic sector	
• The distribution of ransomware across territory	
• Most active criminal groups	
Wrapping up	20

DRM

AN ITALIAN PROJECT 

DASHBOARD RANSOMWARE MONITOR

Report presented by Ransomfeed.it • CC BY-NC

Dissemination of this Report is encouraged; any reproduction (total or partial) is free and not intended for commercial use, citing the source as per Creative Commons Attribution.

DRM

AN ITALIAN PROJECT 

DASHBOARD RANSOMWARE MONITOR

INTRODUZIONE AL REPORT

This report aims to provide a detailed insight into the ransomware threat landscape during the period between May and August 2023 (second quarter), with a particular focus on monitoring activities conducted by the OSINT DRM platform.

During this time period, 165 criminal groups operating worldwide were monitored, with constant tracking of 300 servers used to conduct ransomware activities.

The data collected showed a total of 1736 ransomware claims, of which 53 were solely registered in Italy.

The report closely examines the geographical location of these attacks, as well as the most affected business sector.

In addition, special attention is paid to the ransomware attacks that have affected Italy, in order to understand the specific challenges the country has faced during this critical period in terms of cybersecurity.

“

What we protect today in cyberspace
is what will preserve us tomorrow in our digital lives.

Dario Fadda

OVERVIEW

All data were obtained through the primary activity of the Ransomfeed DRM platform, which periodically scrapes from a selection of known sites on the dark web.

For this report, we will focus on the results collected for the second quarter of the year: first globally, with all monitored ransomware groups, then keeping a particular focus on Italy.

The DRM platform, during Q2 2023, monitored 165 cyber criminal groups operating with ransomware technologies in over 300 servers and mirrors, resulting in a total of 1736 ransomware claims identified globally.

The months of May, June, July and August all faced and presented unique cybersecurity challenges.

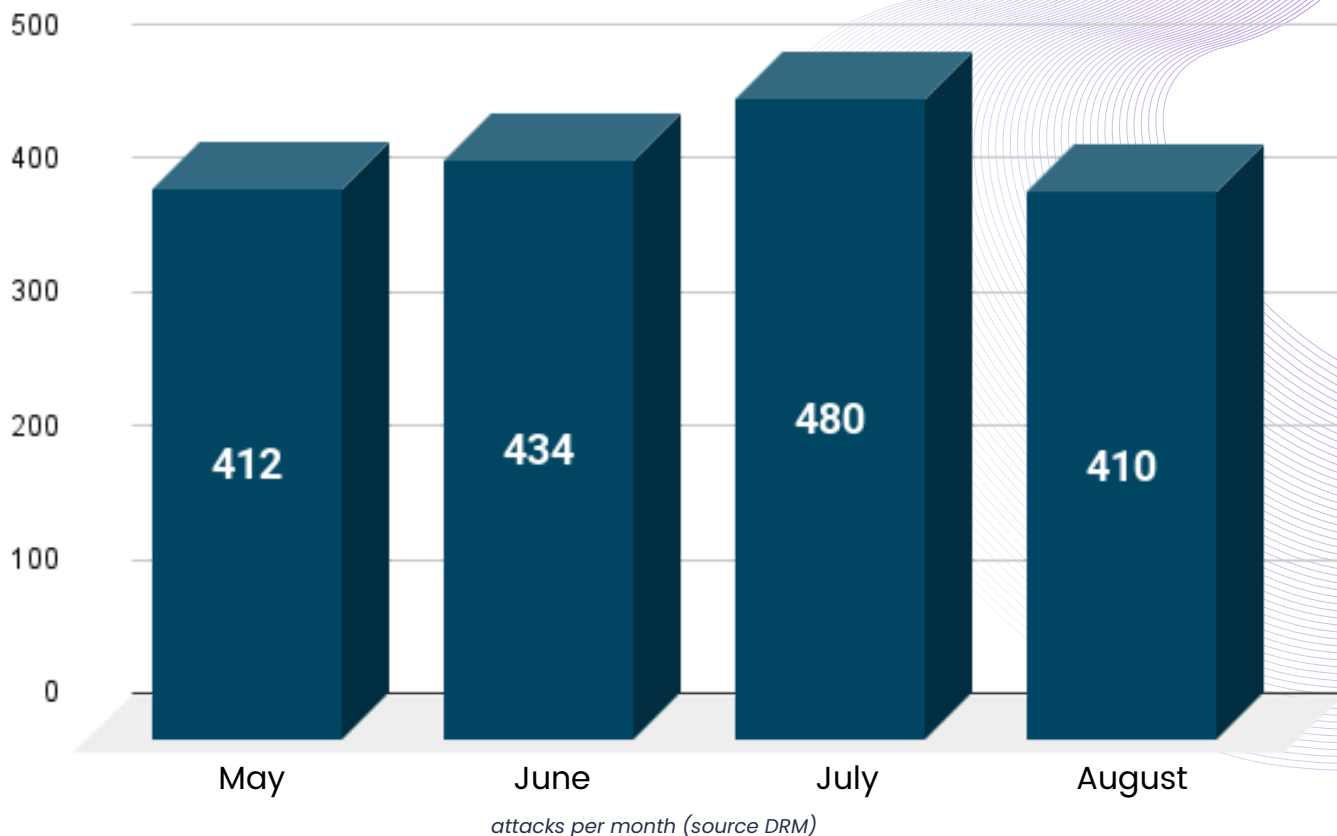
May opened the four-month period with 412 attacks, followed by June with 434, July with 480 and August with 410 attacks.

However, is on the detail of the days that relies an even more alarming picture.

DRM

AN ITALIAN PROJECT 

DASHBOARD RANSOMWARE MONITOR



May the 23rd labels the peak with 106 ransomware attacks claimed in a single day, highlighting the attackers' determination to exploit digital vulnerabilities.

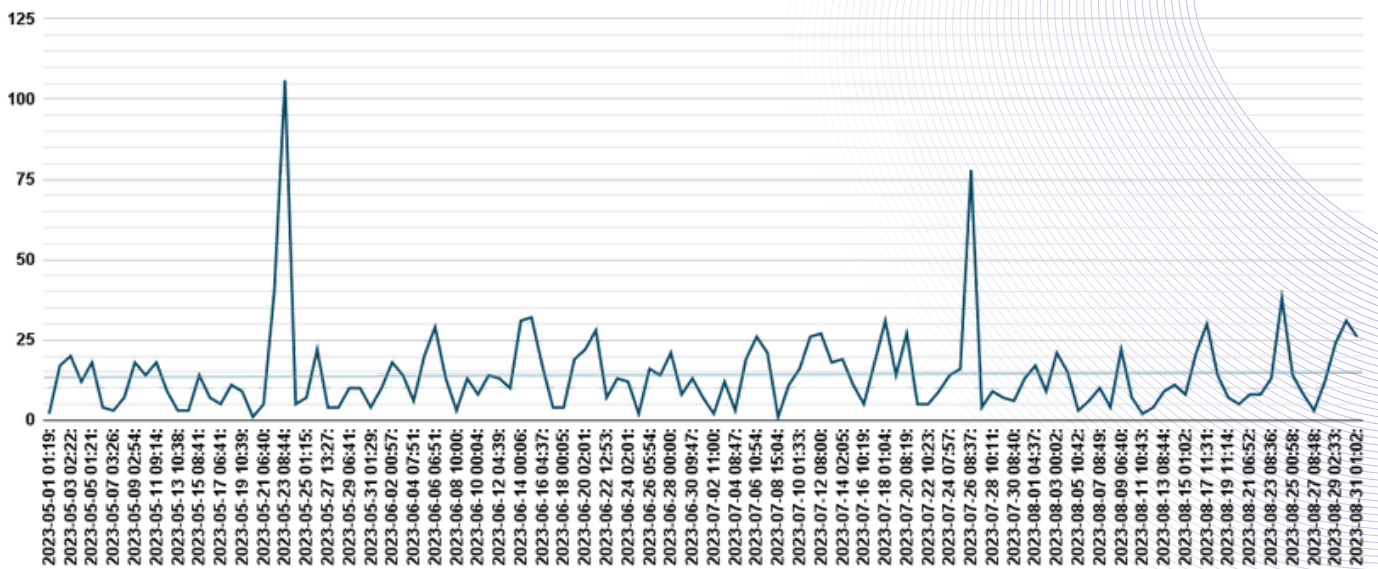
In contrast, on the 8th of July we can observe the least significant day of the four-month period, with only one claim.

DRM

AN ITALIAN PROJECT 

DASHBOARD RANSOMWARE MONITOR

The daily average number of attacks during the four-month period exceeds 14, a figure that calls for a very serious reflection on the security measures taken by organisations.

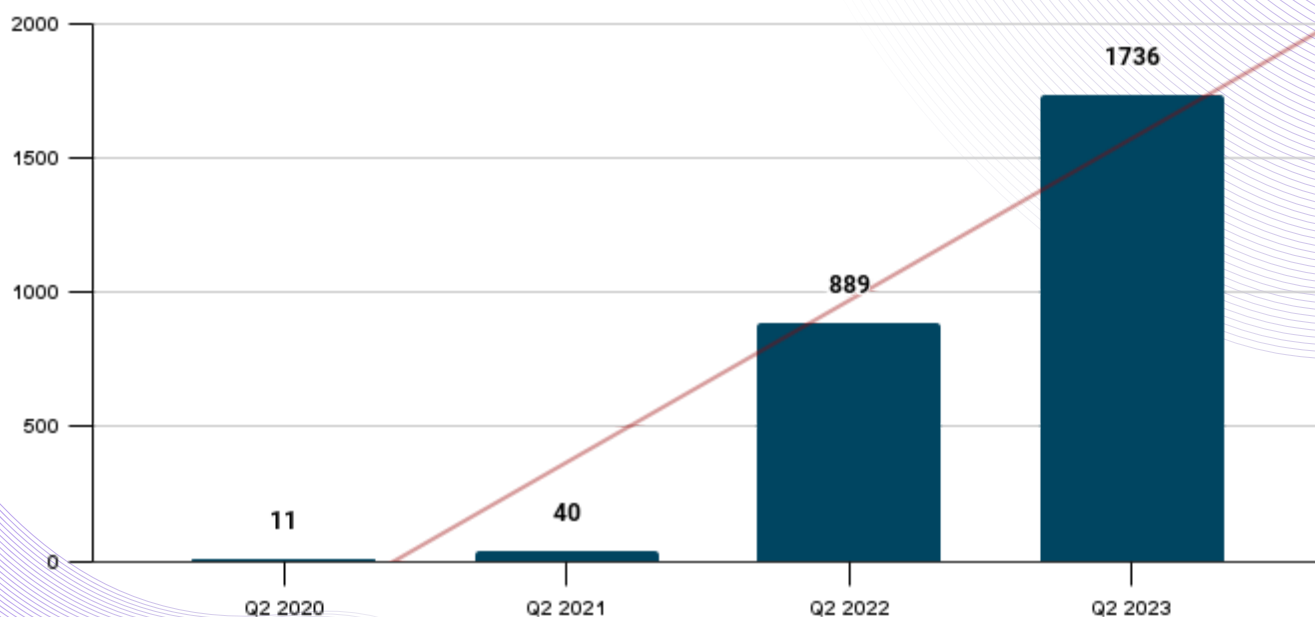


Averages on the bottom line, per day (source DRM)

• QUARTERLY COMPARISON

In order to represent data, already shown in the Overview section, in a timely manner, we have set a comparison with some past segments.

We'd like to remind you that the DRM platform was initially fed with past data up to 12 January 2020: it was therefore possible for us to go back in time, comparing the Q2 of the last three years.



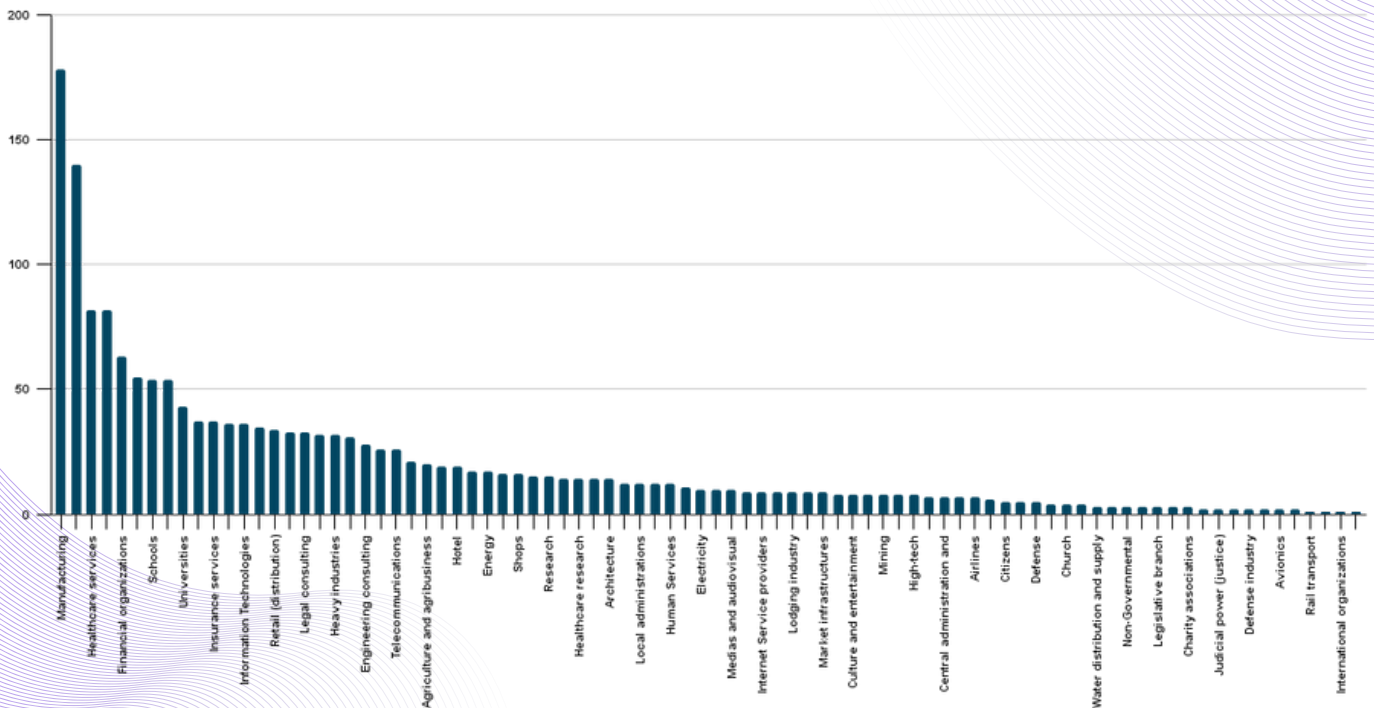
It's clear that the trend is growing and there is still no decrease in attacks in this time frame; 2023 also confirms an increase in ransomware attacks, compared to Q2 2022 of more than 51%.

With regard to the processing and presentation of the data for this second quarter, we need to inform you that, during these last months, we have introduced a "duplicate management system". This feature was created and refined internally, to filter and correct any duplicates that some cyber gangs generate in the publication of victims; the platform now presents purified data of all these 'fake' claims.

DISTRIBUTION OF RANSOMWARE ACROSS INDUSTRIES

Even in the data referable to the work categories, the DRM platform in the past four months, has seen important news.

There was an enrichment, the result of a fruitful collaboration between our Ransomfeed project and DeepDarkCTI (led by the expert Massimo Giaimo), which took care of aligning all the missing data on the labor sector of the victims involved in claims, effectively enriching the detail of our platform.



Thanks to this work, as of this quarter, we can count on a more precise and pure set of category data.

Here's the top five:

- industrial production
- technology
- healthcare
- construction
- financial

These are also the category sectors that **share the top 30%** of the ransomware market globally (Q2 2023 data).

For categories that impact **national security**, it's curious to find that **Government organizations** are placed in 48th position this quarter with 9 claimed attacks.

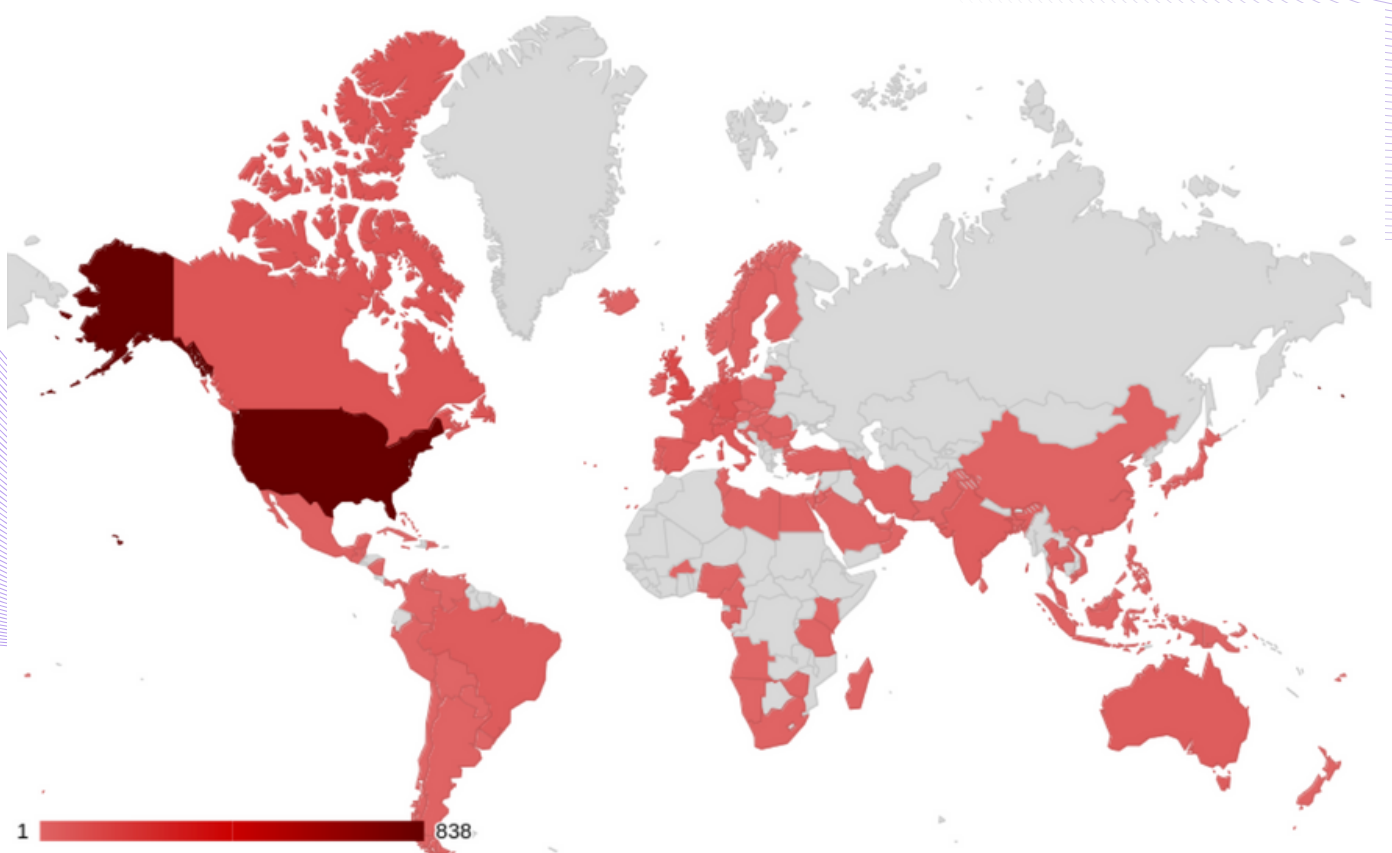
More, if we add the **country defense sectors**, **international governmental organizations** and the **justice sector**, data reaches the number of 33 claims, which account for 2% of the total.

WORLDWIDE RANSOMWARE DISTRIBUTION

The continuous and meticulous post-scraping OSINT work carried out on the platform allows, every four months, to present a complete picture of the geography of cyber attacks (starting from their claims).

Exactly as observed in Q1 2023, the north-western part of the world is the most seriously impacted by cyber criminal groups.

Take a look at the picture below to visually and quickly understand the spread of ransomware attacks.



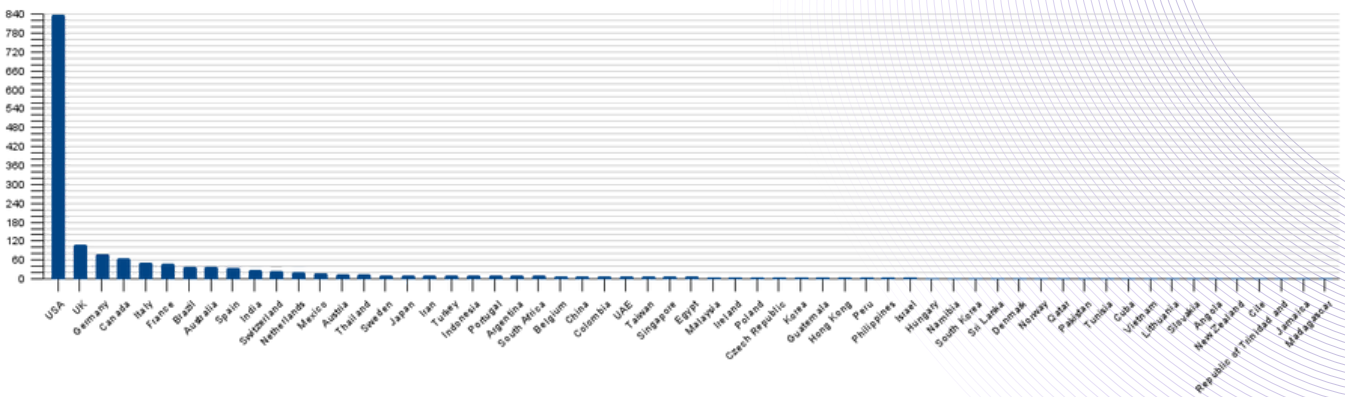
worldwide attacks (source DRM)

DRM






AN ITALIAN PROJECT 






DASHBOARD RANSOMWARE MONITOR

Focusing on the differences, compared to Q1 2023, the geographical distribution is decidedly similar and in line with the previous data. Only the data for Australia and New Zealand is added, for a new color of the oceanic continent.

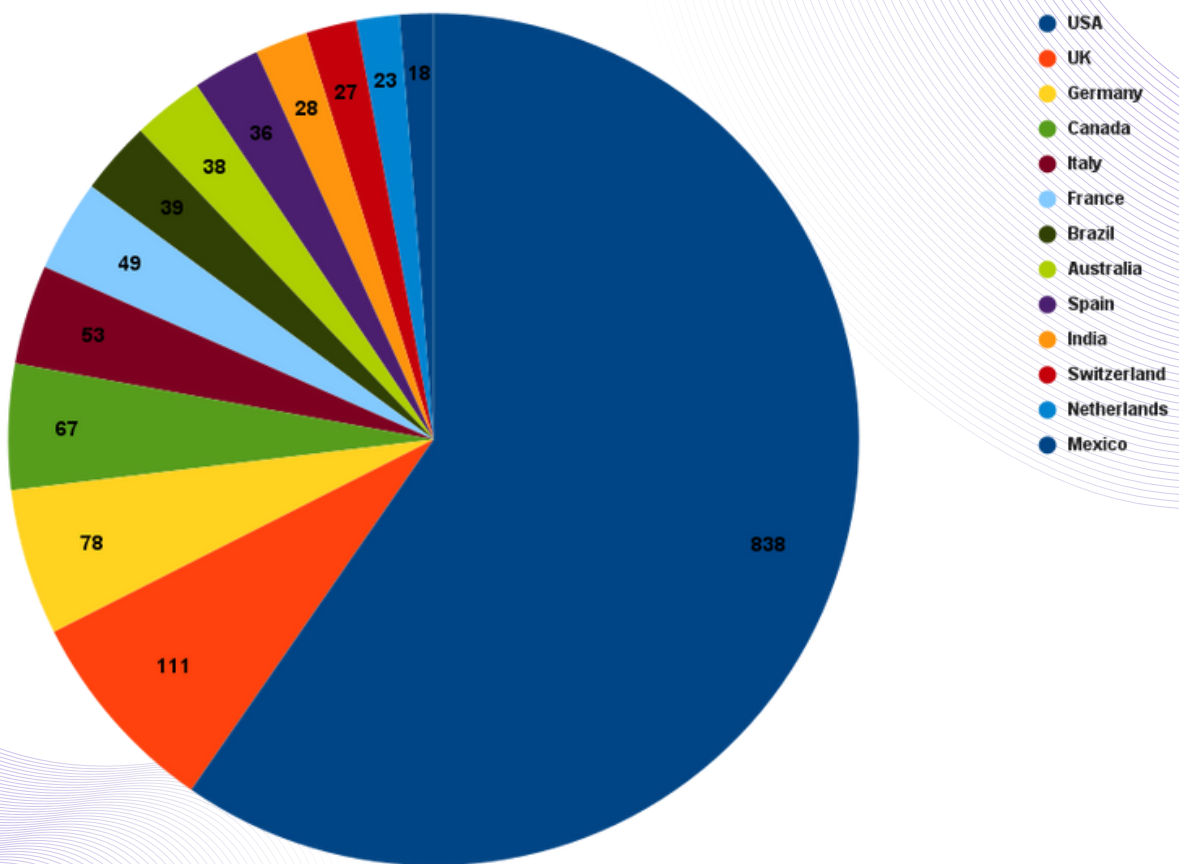


With the United States (838 attacks) covering almost 50% of all attacks, the other top positions are occupied by UK, Germany and Canada. In Q2 2023, Italy stands in fifth position with 53 attacks, moving up one position – in Q1 2023 it occupied sixth position.

 USA	48.3%
 UK	6.4%
 GERMANY	4.5%
 CANADA	3.9%
 ITALY	3.1%

 FRANCE	2.8%
 BRAZIL	2.2%
 AUSTRALIA	2.2%
 SPAIN	2.1%
 INDIA	1.6%

This graph shows the Top 13 countries affected by ransomware attacks, each with the exact number of claims registered. Countries with under 1% of registered attacks are excluded from the visualization.



There's a large gap between the USA and the rest of the world, a gap which, pondering all the necessary considerations regarding the industrial and company distribution as possible targets in the USA (compared to other countries) highlights the capillarity of criminal groups.

NEW CRIMINAL CYBER GROUPS

During the given period, as often happens, we have seen the birth of new groups that have made baldly space in the cyber scene.

DRM detected them and added them to its daily monitoring, totaling 174 new claimed attacks with 8 new criminal groups.

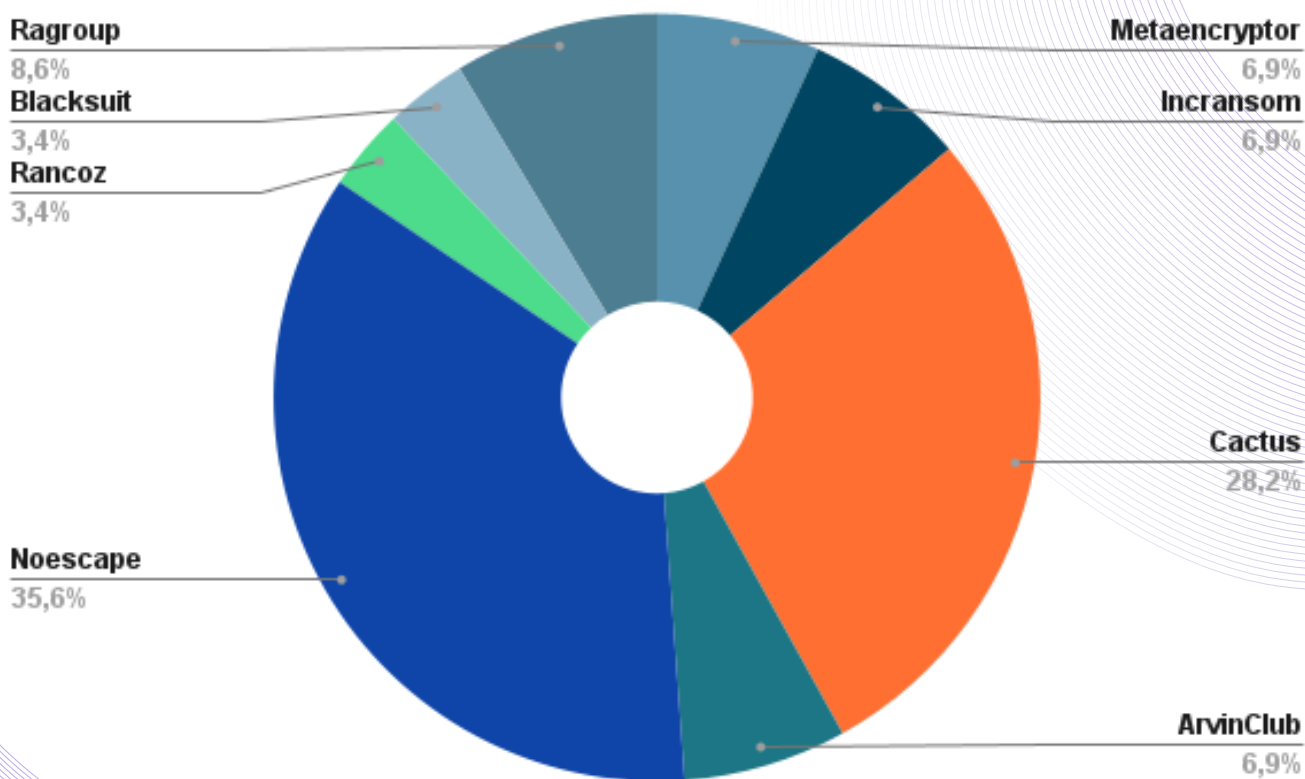
METAENCRYPTOR	12
INCRANSOM	12
CACTUS	49
ARVINCLUB	12
NOESCAPE	62
RANCOZ	6
BLACKSUIT	6
RAGROUP	15

DRM

AN ITALIAN PROJECT 

DASHBOARD RANSOMWARE MONITOR

The following table highlights all new the groups that the DRM platform added while monitoring the scene over the 120 days of the second quarter.



Noescape scores first place, being the most active new cyber in Q2 2023, with more than 35% of ransomware claims inside its cluster.

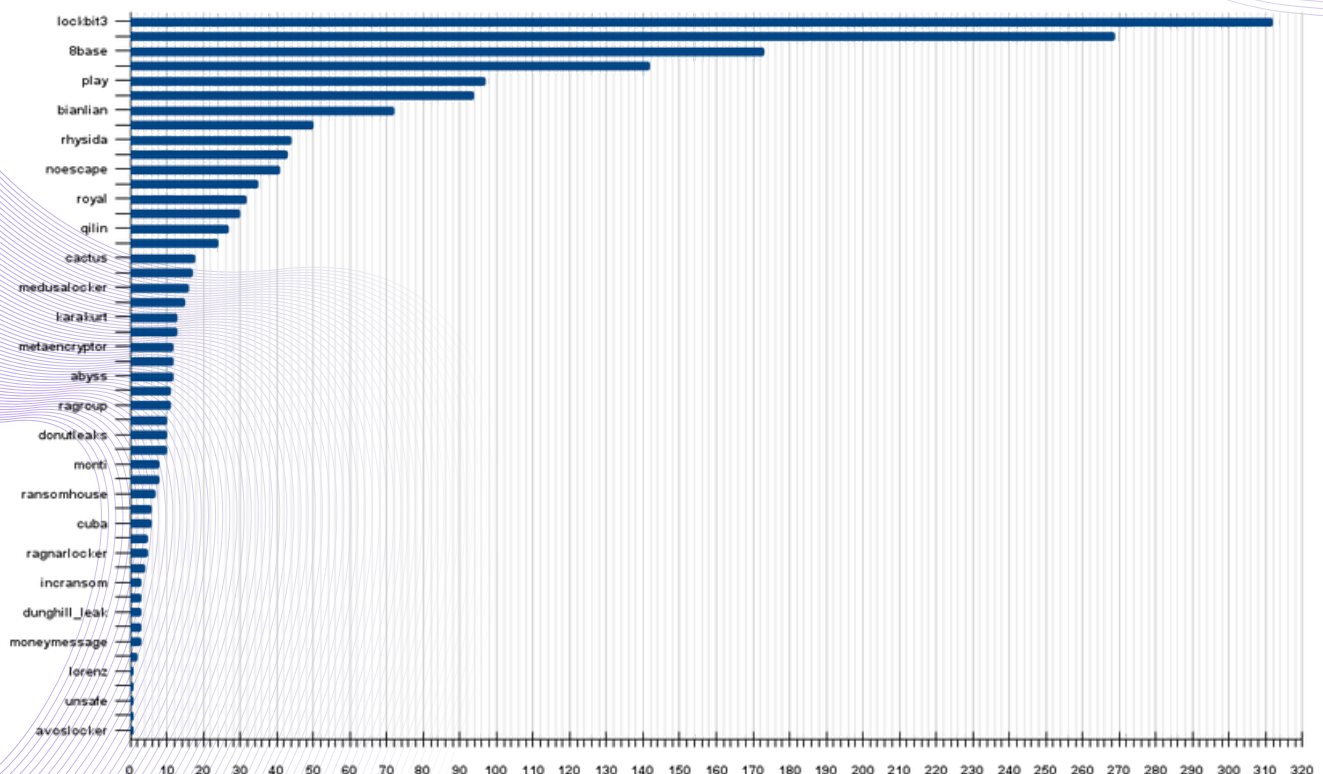
GLOBAL ACTIVITIES OF RANSOMWARE GROUPS

We isolated the individual ransomware clusters that generated activity. Among all the groups that are constantly monitored, the platform detected activity in the four-month period for 49 of these. The other not mentioned groups were found to be inactive.

The activities of these groups produced the whole total data, that we are analyzing in the pages of this report, and saw an absolute leadership of four extremely active gangs, capable of sharing 52% of the attacks.

They are led by Lockbit which, alone, accounts for 18% of attacks (down from Q1 2023). Followed by Clop, 8base, ALPHV/BlackCat with 15.5%, 10% and 8.2% respectively.

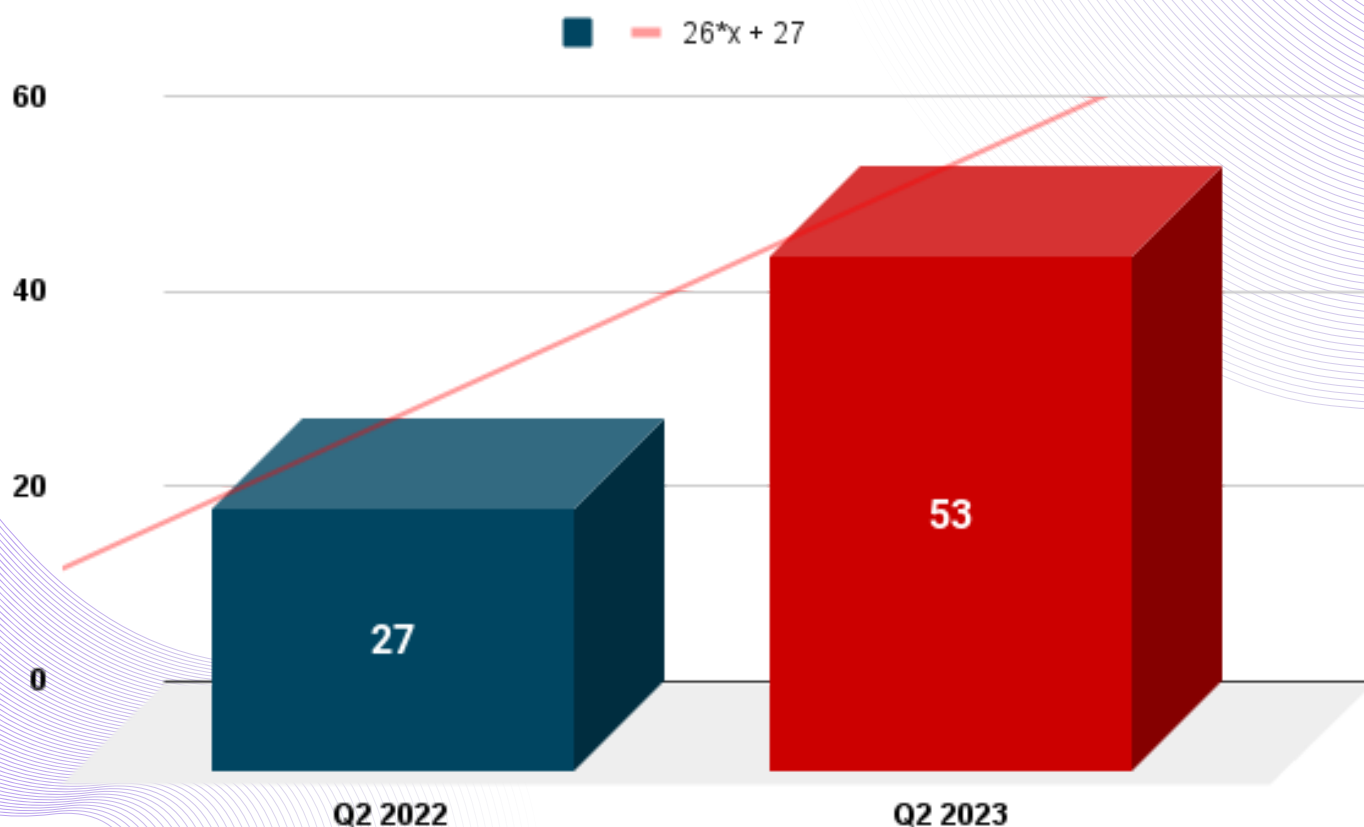
The graph shows the detail of all active cyber gangs, whose reference value is attributed to the number of claimed victims.



FOCUS ITALY Q2 2023

This part of the report is fully dedicated to the analysis of the clusters seen in the global feature, standing for a particular attention for Italian scenario.

At a very first sight, it appears clear that ransomware attacks, expressed in numbers, for Q2 2023, is stunning: 53 attacks. Almost one every two days.



As for Q1 2023, this data truly reflects the global trend, which is dramatically increasing - considering the very same given date of 2022.

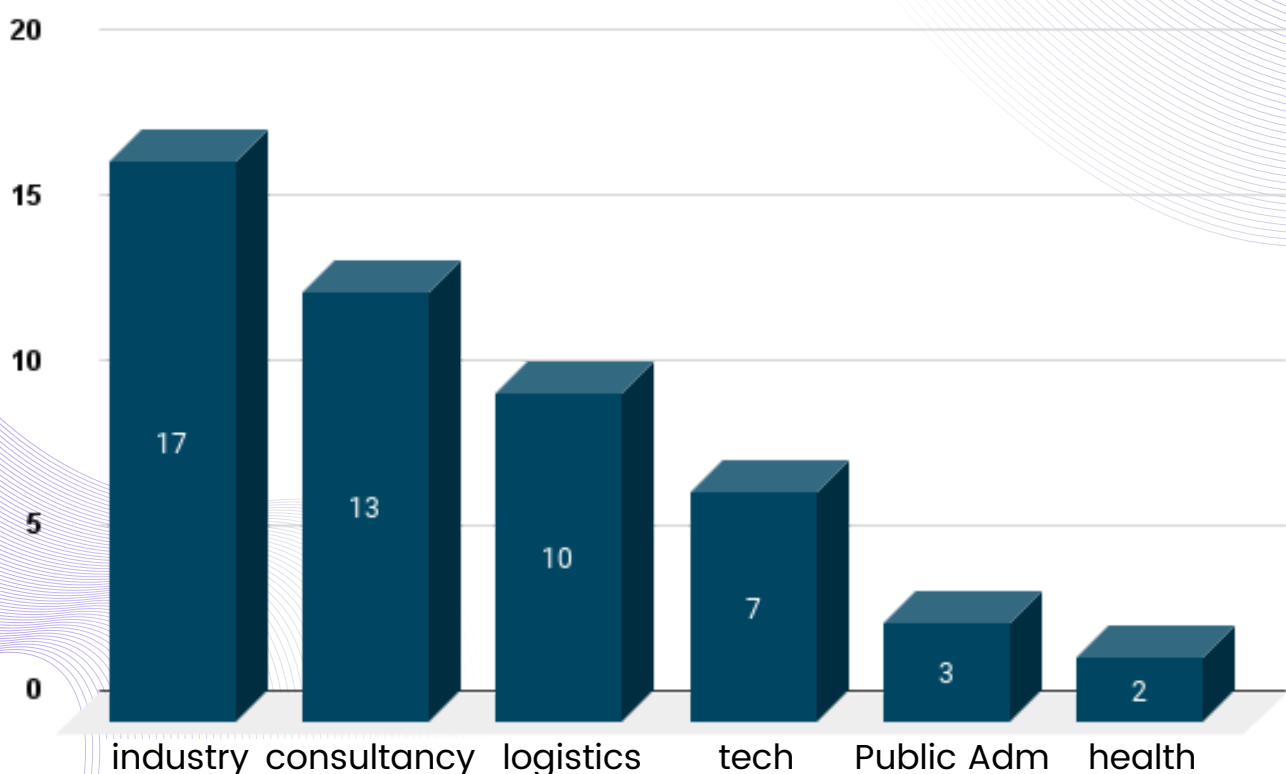
So far, in Italy, the growth rate is 96% since Q2 2022.

• ATTACKS PER ECONOMIC SECTOR

Industry, as in the global scenario, turns out to be the most affected work sector even in the Italian focus, alongside pharmaceutical, mechanical, metallurgical and electronics, with 17 ransomware attacks claimed in the given period.

This is followed by the consulting, logistics and technology sectors; it should be noted that the Public Administration field had an impact with only 3 claims.

A precise breakdown of the data for all work sectors is shown in the graph below:



Here's a breakdown of the most impacted sectors; percentages are quite explanatory about ransomware groups preferred targets.

INDUSTRY	51.5%
CONSULTANCY	39.4%
LOGISTICS	30.3%
TECHNOLOGY	21.2%
PUBLIC ADMINISTRATION	9.1%
HEALTH	6.1%

DRM

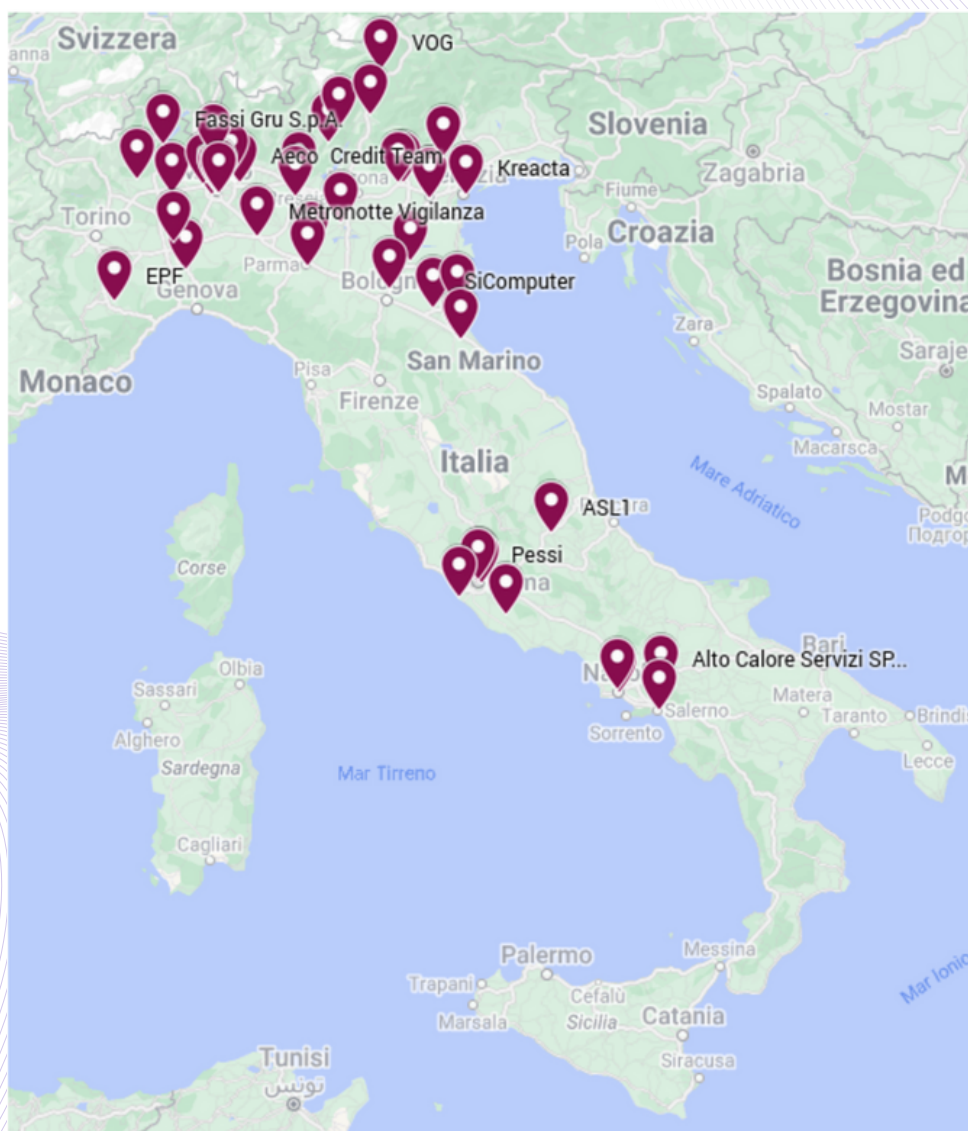
AN ITALIAN PROJECT 

DASHBOARD RANSOMWARE MONITOR

• THE DISTRIBUTION OF RANSOMWARE ACROSS TERRITORY

Using all the location data collected, we were able to draw a map to define the geographical distribution of ransomware in Italy for the Q2 period.

Note: you can consult the map online, and use the interactive function, by simply clicking on it.



DRM

AN ITALIAN PROJECT 

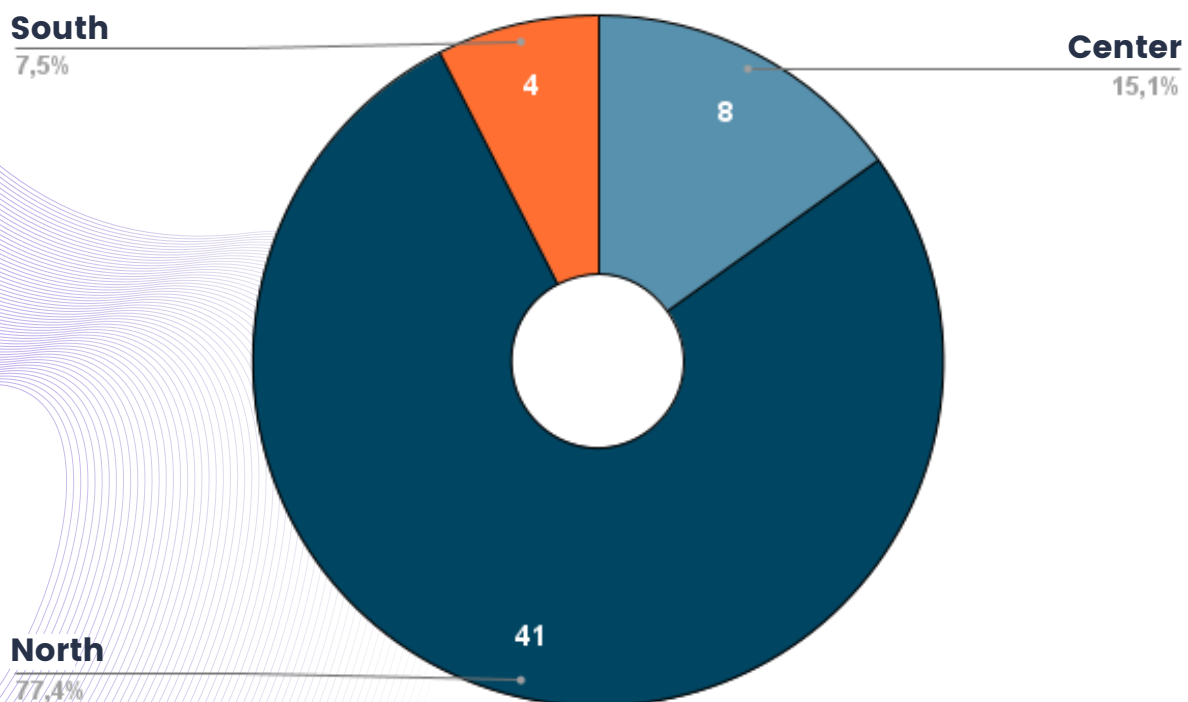
DASHBOARD RANSOMWARE MONITOR

By focusing on the macro-localization, it is clear that North of Italy is a way preferred location for attacks; this is also a recurrent geographic pattern in time. Q2 sees more than 77% of claims in the northern area.

NORTH	41
CENTER	8
SOUTH	4

Almost 80% of ransomware attacks comes from North Italian targets (organizations and public entities).

In the graph below, a quick visual understanding of the depicted areas.



DRM

AN ITALIAN PROJECT 

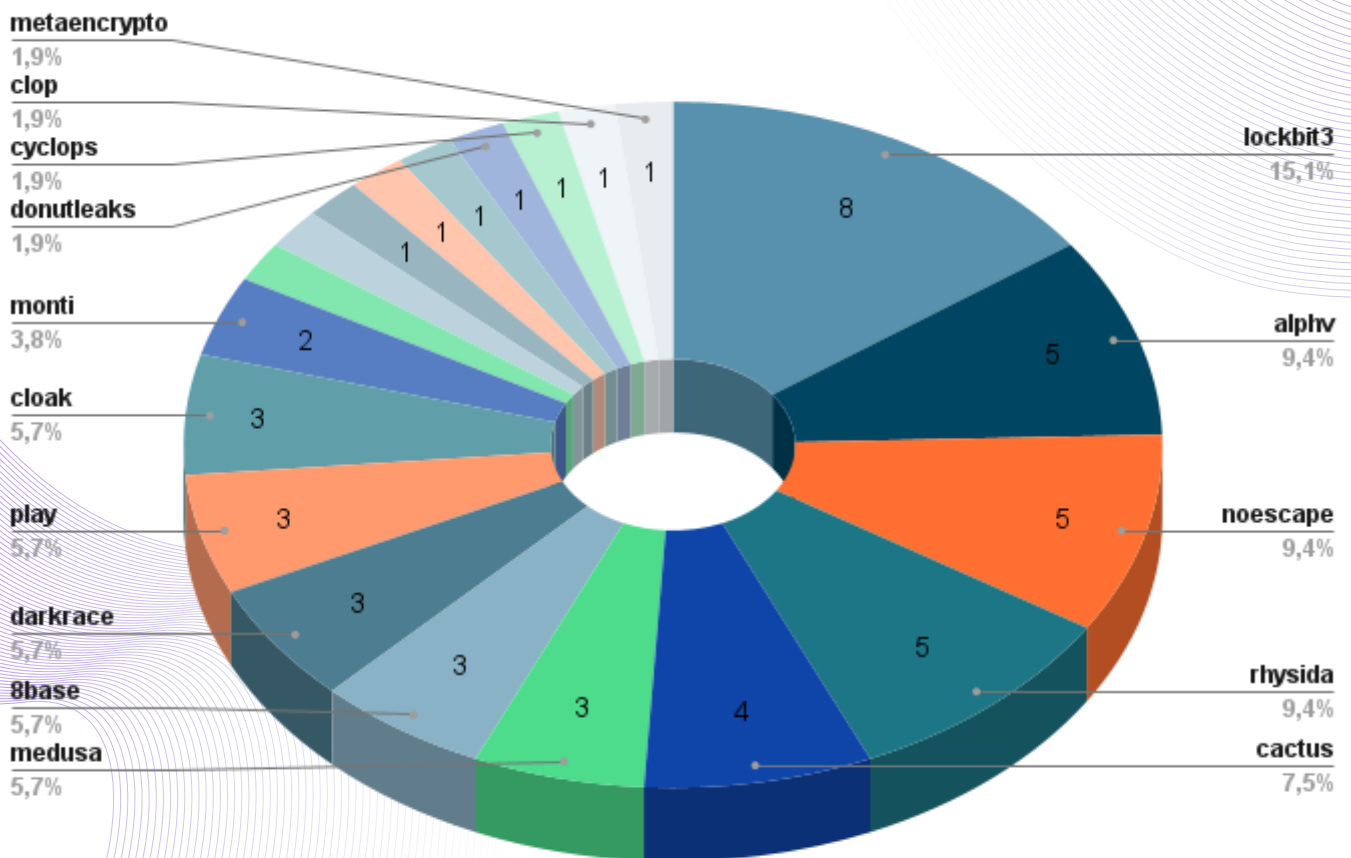
DASHBOARD RANSOMWARE MONITOR

• MOST ACTIVE CRIMINALS

No need to highlight that cyber gangs claiming attacks in Italy are quite following the general and global trend.

Lockbit is the most active group in Italy, for this segment, with 15% of attacks.

Since Q1, however, ransomware groups are more homogeneous: there is no such “distance” between Lockbit and the rest of the cyber gangs operating in the Country.



Note, in this graph, attacks to Italian targets, filled with percentages per group and number of claims.

WRAPPING UP

This second quarter of 2023 showcases a period of **growing concerns** in the ransomware threat landscape, with numerous organizations and entities around the world suffering **devastating attacks**.

The DRM platform played (and, actually, plays) a crucial role in **monitoring and collecting relevant data**, highlighting the activity of **165 criminal groups** and identifying **1736 ransomware claims**, of which **53 were in Italy**.

The geographic location and employment sector of the victims provided valuable information for understanding the **emerging trends and threats**. In particular, ransomware attacks in Italy require **continuous attention and advanced mitigation strategies** to ensure the security of national organizations.

This report offers a **detailed overview** of these events, with the aim of supporting efforts in **strengthening cybersecurity** and preventing future ransomware attacks.



DASHBOARD RANSOMWARE MONITOR

DASHBOARD RANSOMWARE MONITOR

Dashboard Ransomware Monitor (DRM) is a ransomware group monitoring service; using scraping, i.e. the extraction of data from multiple websites using software programs and their subsequent structuring, DRM stores each claim in a permanent RSS feed, available for free consultation.

The monitoring service is available to everyone, free of charge, and constantly collects and analyzes data relating to ransomware attacks at an international level.

The platform is able to detect attacks in a timely manner and analyze their patterns, providing rich data available to anyone who wishes to understand the extent and evolution of cyber attacks.

Visit ransomfeed.it to learn more about the platform

DRM

AN ITALIAN PROJECT 

DASHBOARD RANSOMWARE MONITOR

TY ;)