
ransomfeed
ADVANCED DATADRIVEN CYBERNEWS
THIRD QUARTER
REPORT 2023
RANSOMFEED | RANSOMFEED.IT | AN ITALIAN PROJECT

ADVANCED **DATADRIVEN** CYBERNEWS

TABLE OF CONTENTS

ADVANCED **DATADRIVEN** CYBERNEWS

> Cybersecurity is not just a technological battle, but a constant war against increasingly sophisticated and pervasive threats, where resilience and preparedness are the most powerful weapons.
>
> *Dario Fadda*

ransomfeed

ADVANCED **DATADRIVEN** CYBERNEWS

INTRODUCTION TO THE REPORT

In an age when the boundaries between the virtual and the real are becoming increasingly thin, **cybersecurity** is often relegated to the last thought of the day; many companies **underestimate the importance** of a strategy aimed at **mitigating ransomware attacks** and prefer to deploy scarce resources to protect their data.

Ransomfeed's four-monthly report provides a comprehensive overview of the steady increase in this type of attack globally, with a particular focus on Italy, through **careful and extensive OSINT work**.

We conducted a **precise and detailed analysis** to identify and interpret trends in cybersecurity, highlighting how, in the last four months of 2023, ransomware attacks **have increased** in number and carat.

The platform monitored **185 criminal groups** operating worldwide, with continuous tracking of **342 servers** used to conduct illicit activities, for a total of **1771 claims**, of which **55 were registered in Italy**.

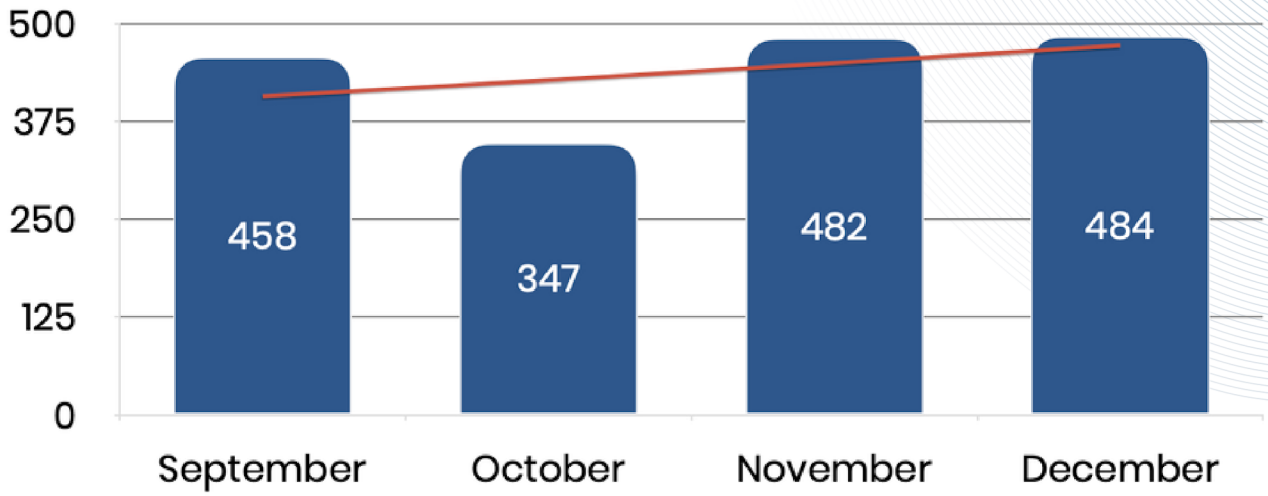
In addition to the data collected by the platform, sifted through to eliminate duplicates in records and groups, we cross-referenced the data with those publicly available on the official channels of threat actors.
It may happen, sometimes, research into possible links between victims could take days of in-depth analysis, but we are committed to make **the nature of the claim** clear for all to see.

ADVANCED **DATADRIVEN** CYBERNEWS

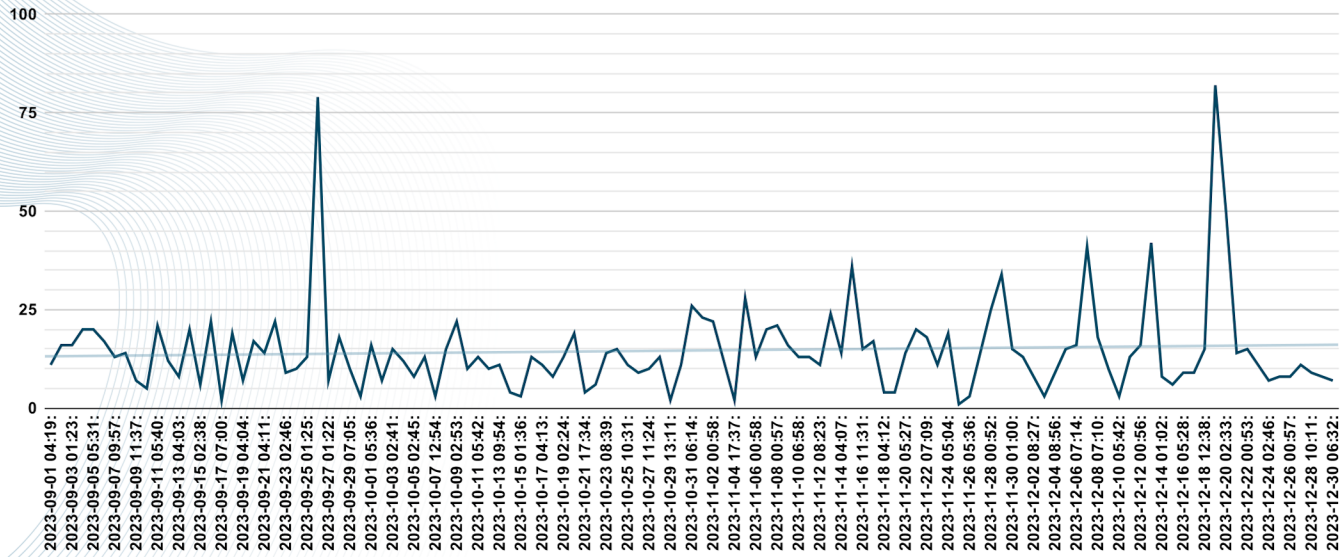
OVERVIEW

The data presented in this report show the **increasing complexity** of attacks.

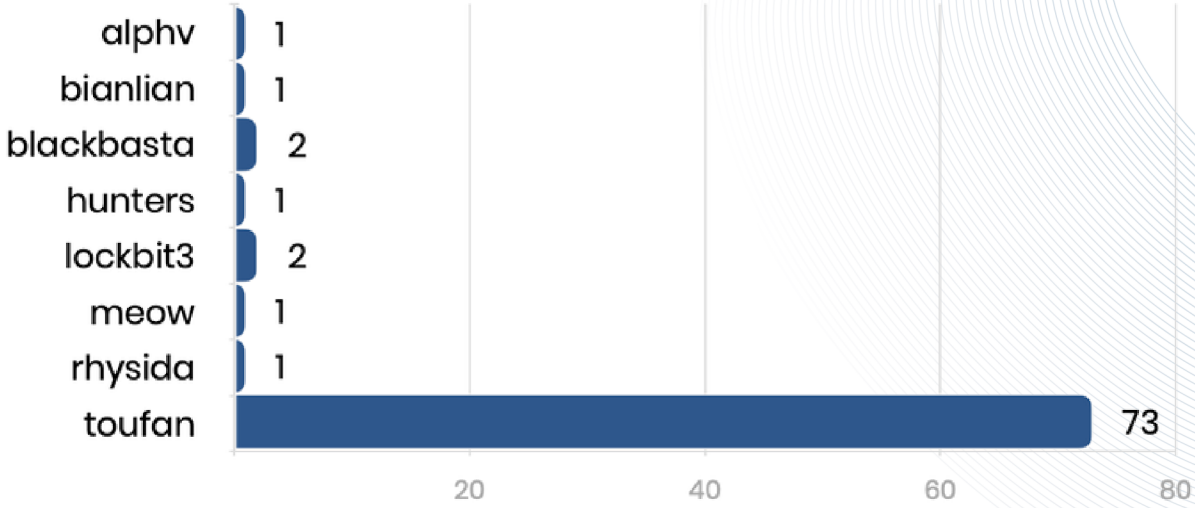
There, emerges a strong need for an **informed and precise vision** to address the daily challenges and devise the most effective defense strategy possible.

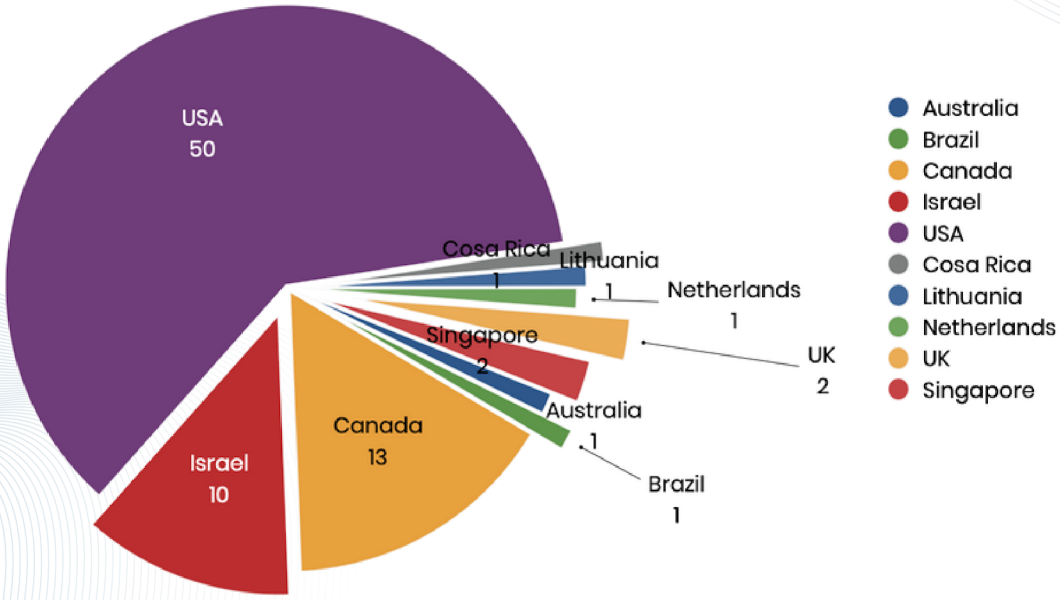


attacks broken down by month, third quarter 2023 (source ransomfeed.it)



The **average daily number** of attacks during the four-month period exceeds **14.6**; December 19 was the **richest day** with **82 claimed attacks**; the high number is due to the appearance on the scene of the **Cyber Toufan** criminal group, with **73 claims**.

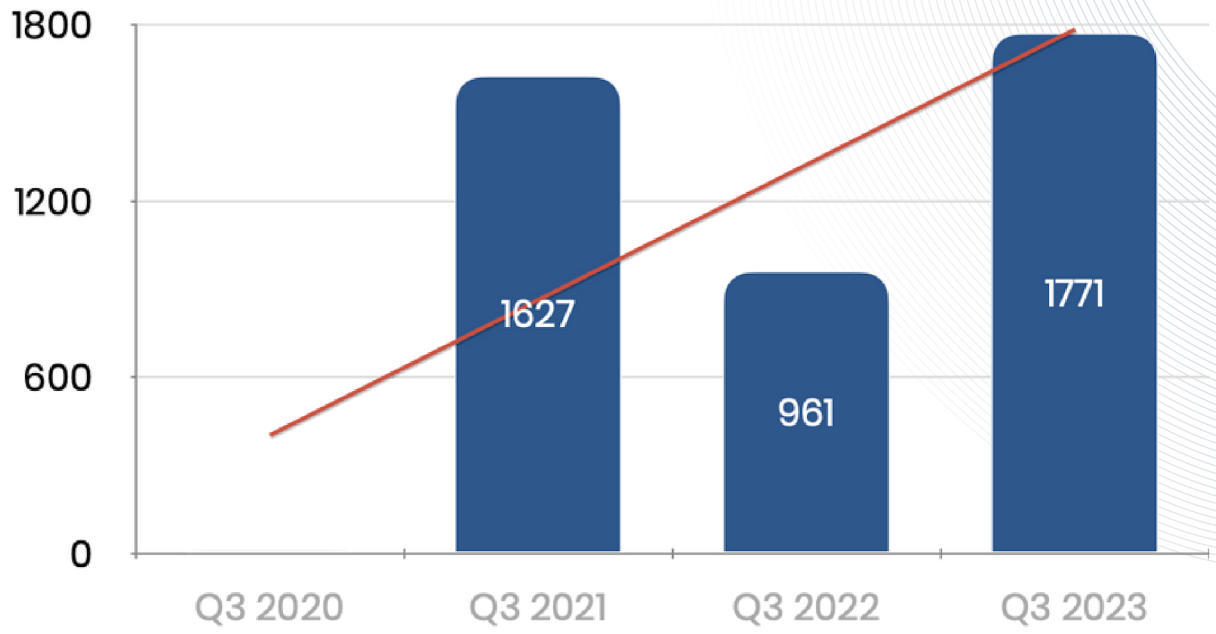




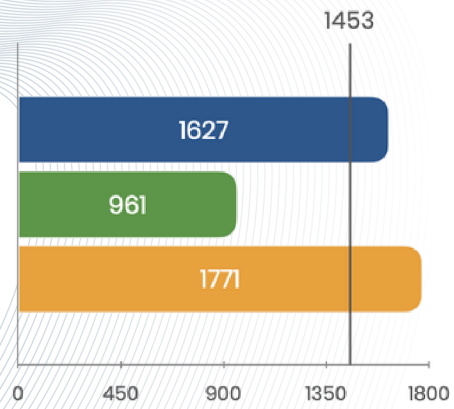
In contrast, **November 25** marked the **least significant day**, with **only one claim** against the Malaysian company **Kenso**, claimed by **Lockbit3**.

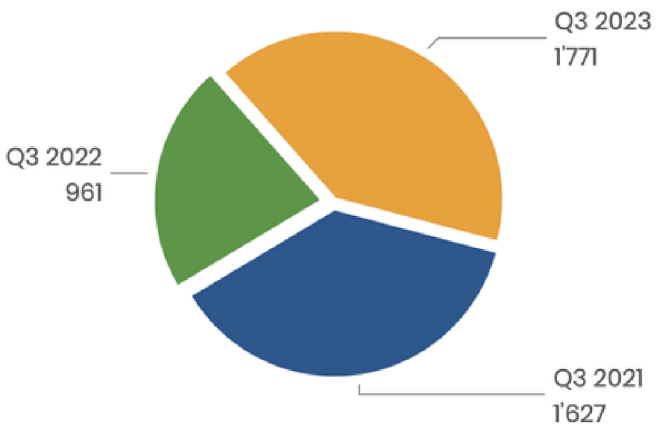
• QUARTERS COMPARISON

The differences between the four-months periods, here stated as Qs, of previous years (once more pointing out that the **Ransomfeed** platform was initially fed with data up to January 12, 2020) return a **rather telling picture of progression**.



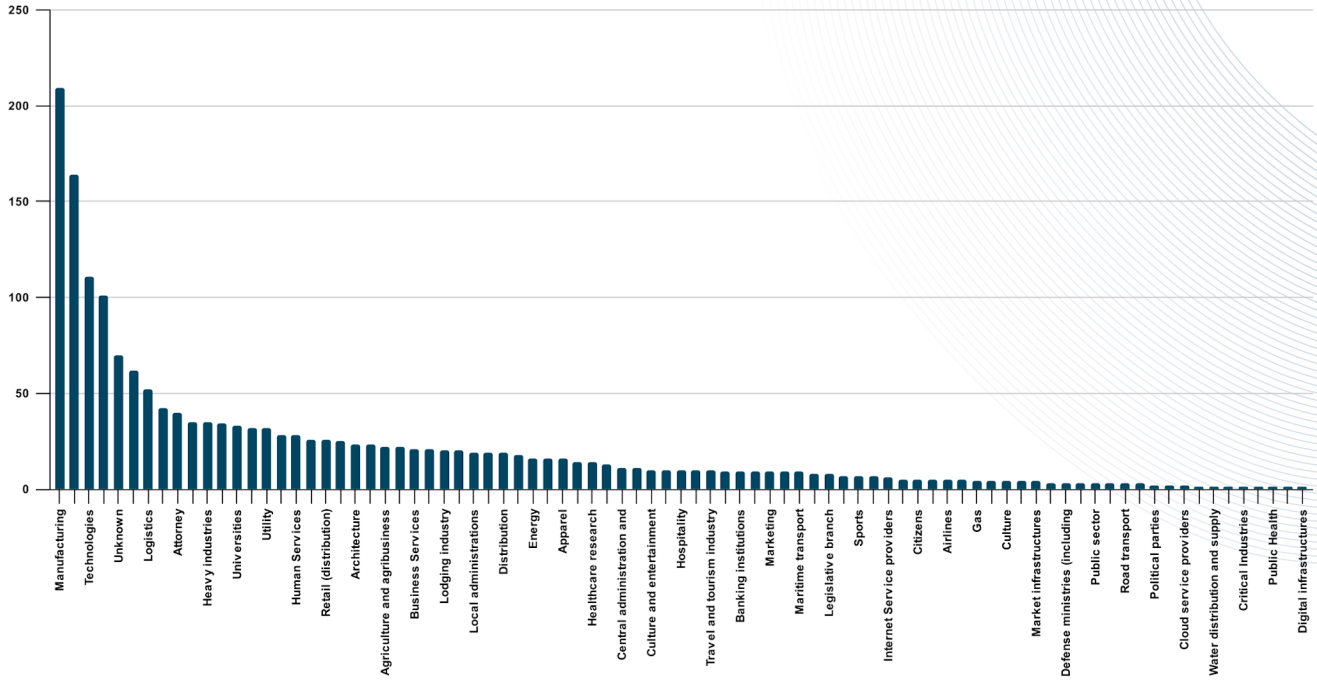
There is **no decrease**, globally, in fact, we are out-seeing a gradual increase: from Q3-2022 to Q3-2023 was **84.29%**





DISTRIBUTION OF RANSOMWARE PER BUSINESS SECTORS

Thanks to the collaboration between **Ransomfeed** and **Würth Phoenix** (led by expert **Massimo Giaimo**), has been possible to check and align all the missing data regarding each victims' **business sector**.



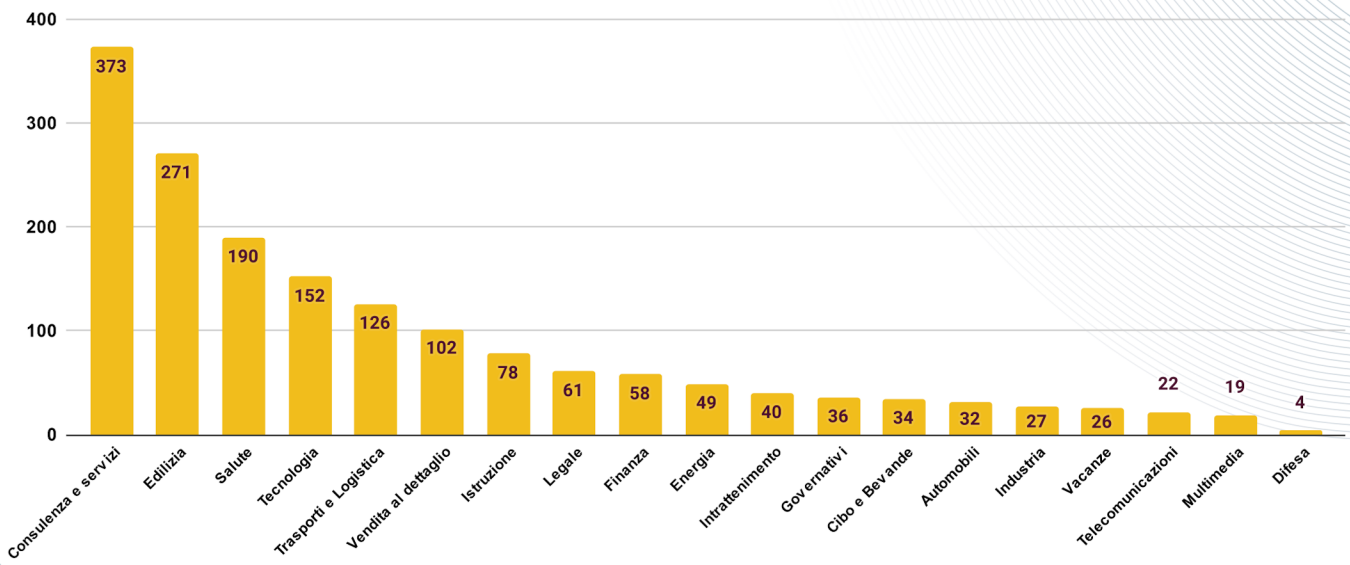
Let's see the very top five positions:

💼 **consulting/services** sectors
🏗️ **construction** sector
😷 **healthcare** sector
💻 **technology** sector
🛞 **logistics/transportation** sector

These are the very top sectors that share an **almost 60%** slice of the ransomware market globally (third quarter 2023 data).

The **increase in attacks** on agencies that deal with, and/or impact **national security**, jumps the category to **13th** position with **39 claimed attacks**.

Adding up the attacks recorded on the **defense**, **international governmental organizations**, and the **broad justice sector**, the figure becomes alarming: more than **40 claims** in the four-month period, accounting for about 4[of the total - a percentage that has doubled since the figure considered in the 2022 segment.



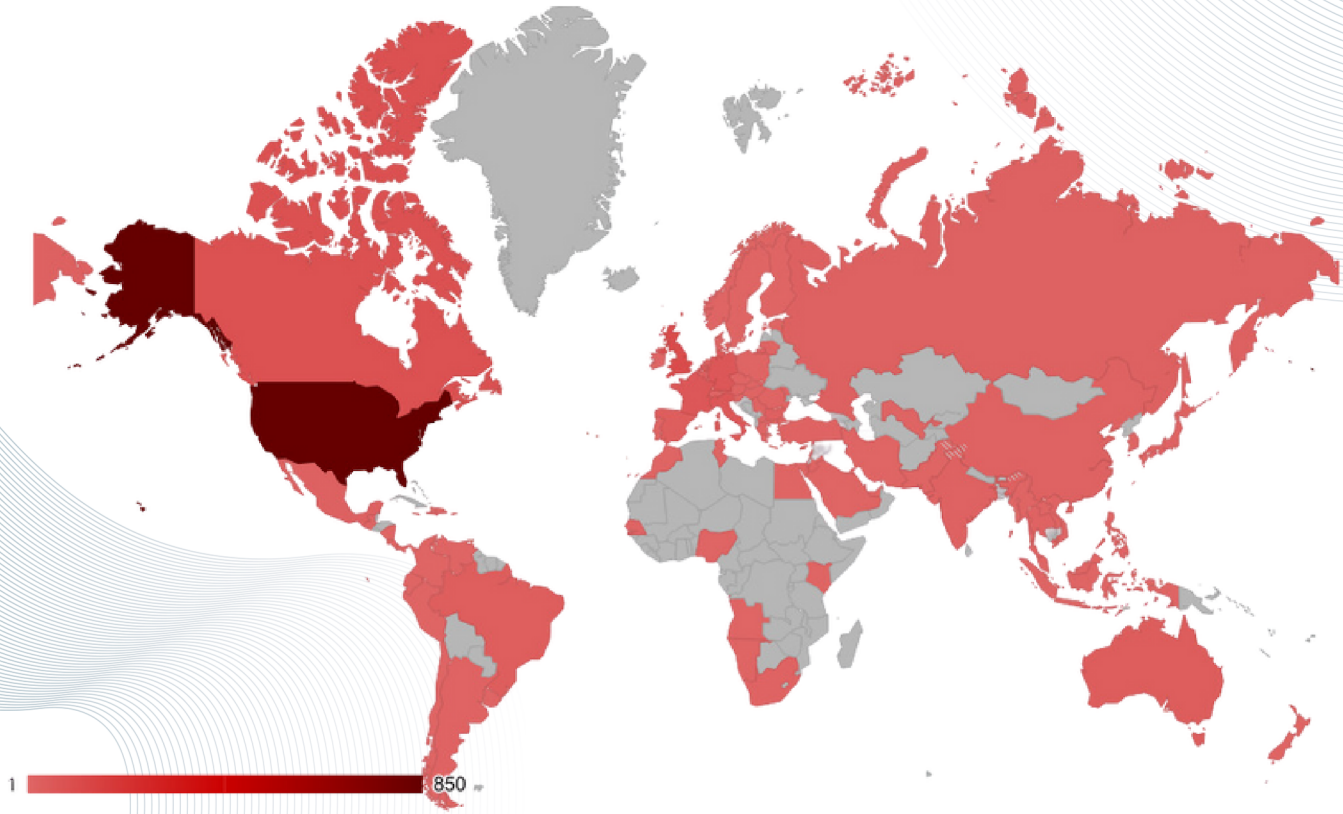
attacks broken down per business sector, third quarter 2023 (source ransomfeed.it)

DISTRIBUTION OF MALWARE IN THE WORLD

Post-scraping **research**, **control**, and **localization** work allows us to obtain a complete and timely picture of the geographical location of the attacks.

As we have often seen, most of the claims are to **be located in U.S.** territory, followed by **Europe**, **Canada**, and **Asia**.

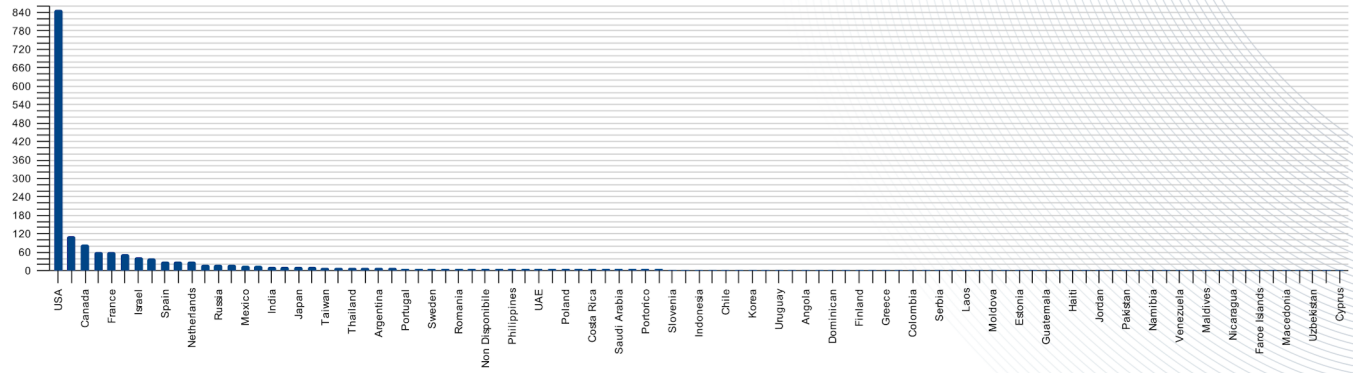
Many **states in Africa** are **less impacted** by ransomware attacks, partly due to a lack of technical infrastructures and partly due to a lack of targets considered "desirable" to criminals.



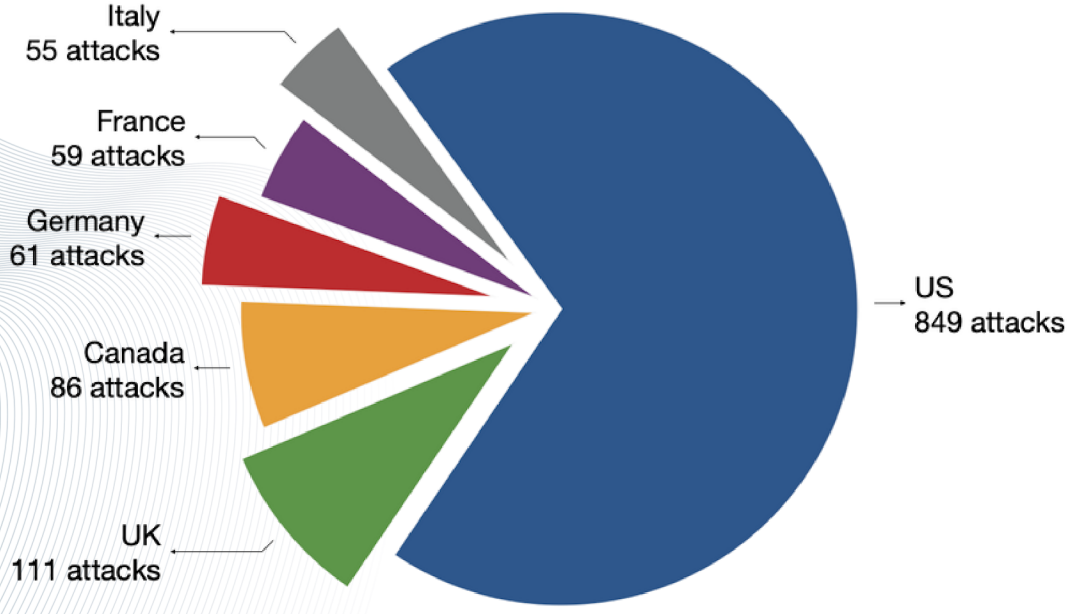
an overview of world attacks, divided by color (source ransomfeed.it)

Compared to second quarter of 2023 we recorded **an increase in claims in Russia**, mostly due to criminal groups aligned against the government.

Among them, the most active group is **werevolves** with **16 claims** to its credit; during 2023, however, it was the **malas** group that set the record for attacks on Russia: there were **37**.



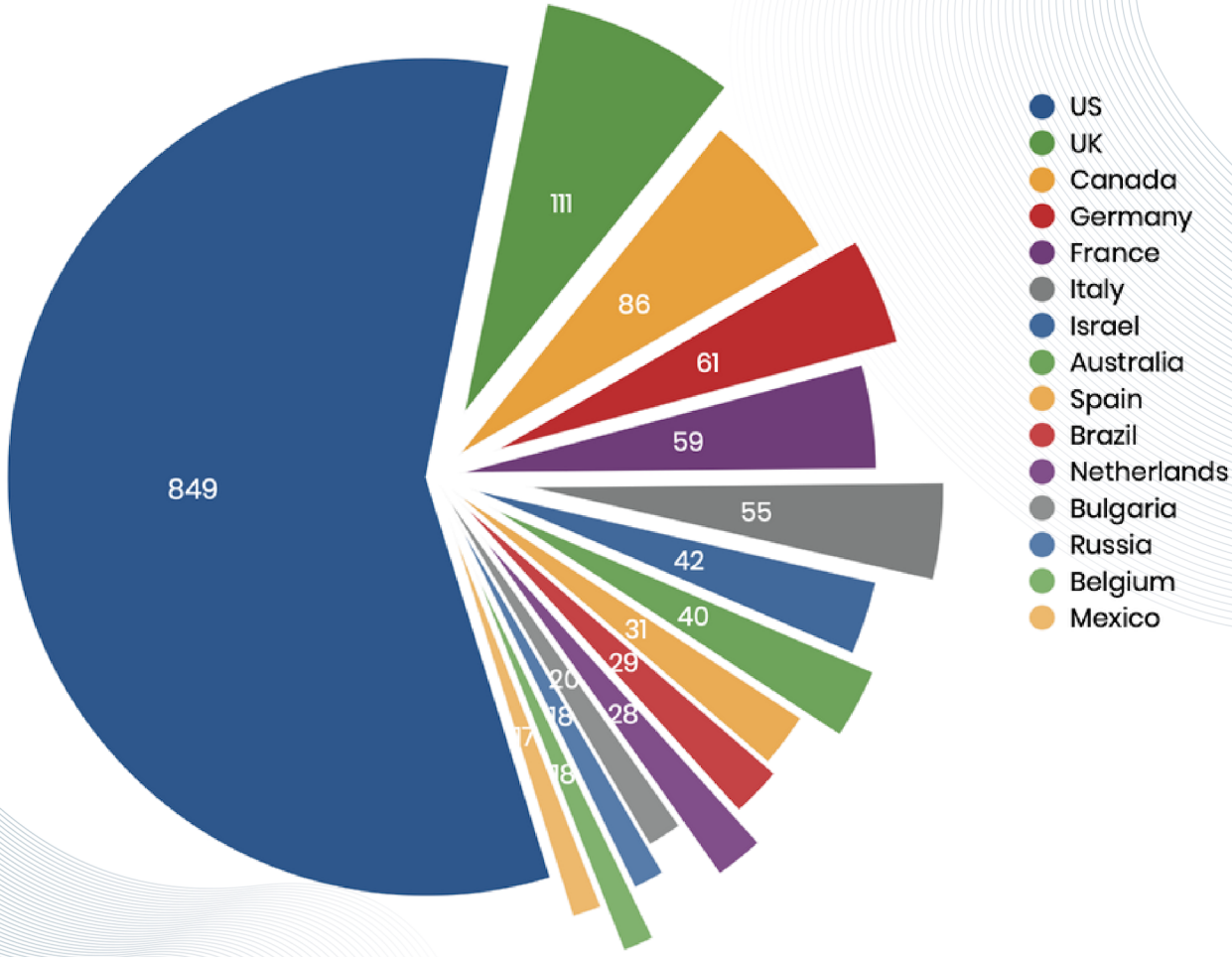
The U.S. (**849 attacks**) remains in first place of countries attacked, covering **48%** of the total; than UK, Canada and Germany follow. **Italy**, in third quarter 2023, ranks **sixth** with **55 attacks**.



first top six countries impacted (source ransomfeed.it)

• TOP 15

All countries with **fewer than 1% ransomware attacks** were excluded in the graph.



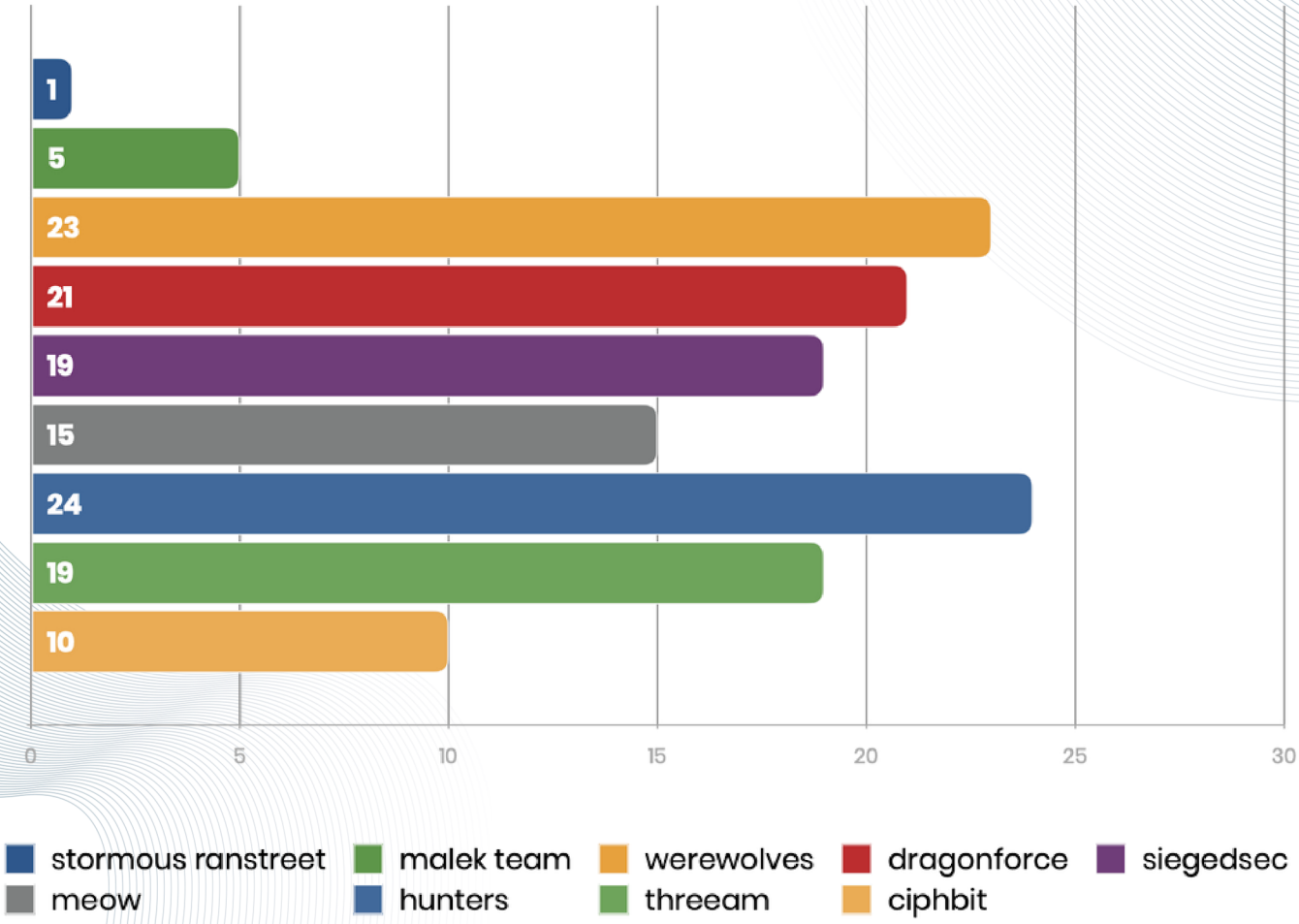
Top 15 as per victims number (source ransomfeed.it)

The gap between attacks recorded in the U.S. and those recorded in the rest of the world, once again, is **really huge**.
Not only the **larger land area**, also the different distribution of companies (possible targets) makes the U.S. a **very attractive country** for criminal groups.

NEW CRIMINAL GROUPS

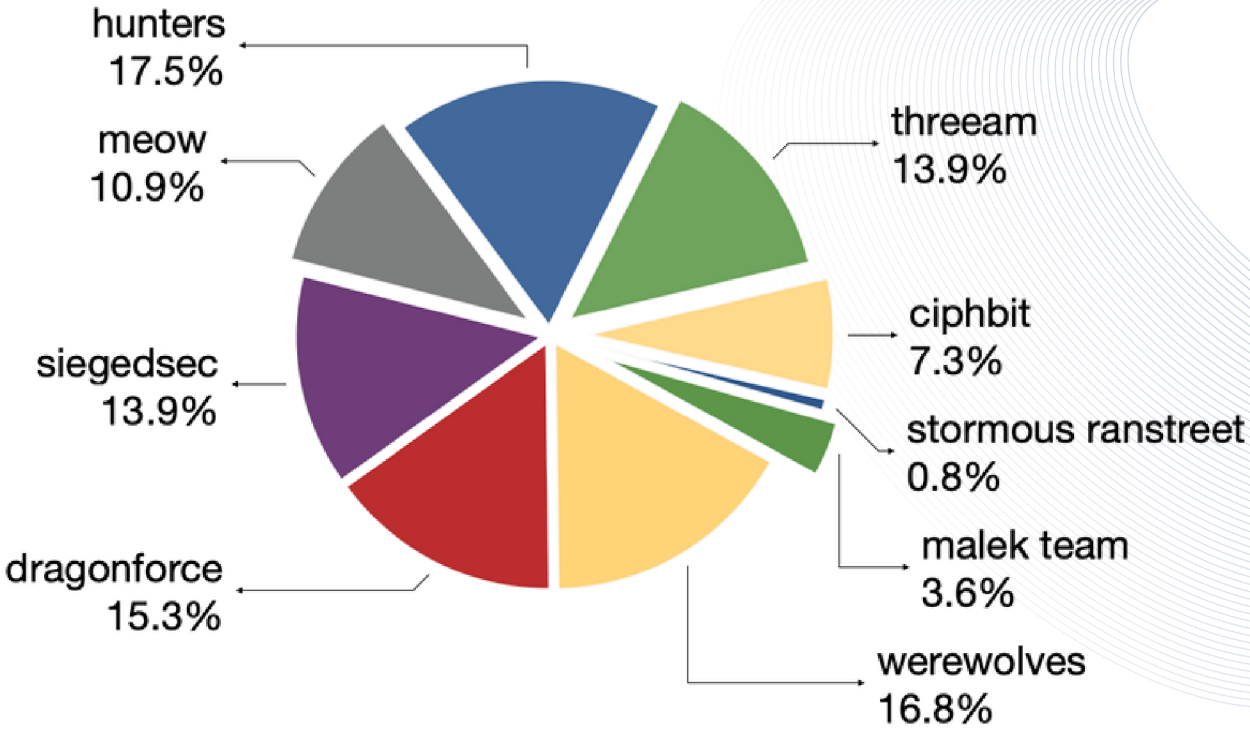
The last months of the year saw **9 new groups** appear on the cyber scene, some followed by no small amount of controversy, as in the case of **RansomedVC**.
The group ended operations as RansomedVC in favor of a **rebrand under the name Raznatovic**, and then reappeared on the scene as **rVC**.

Since RansomedVC/Raznatovic/rVC is not a new group, it was not added to the monitored list.

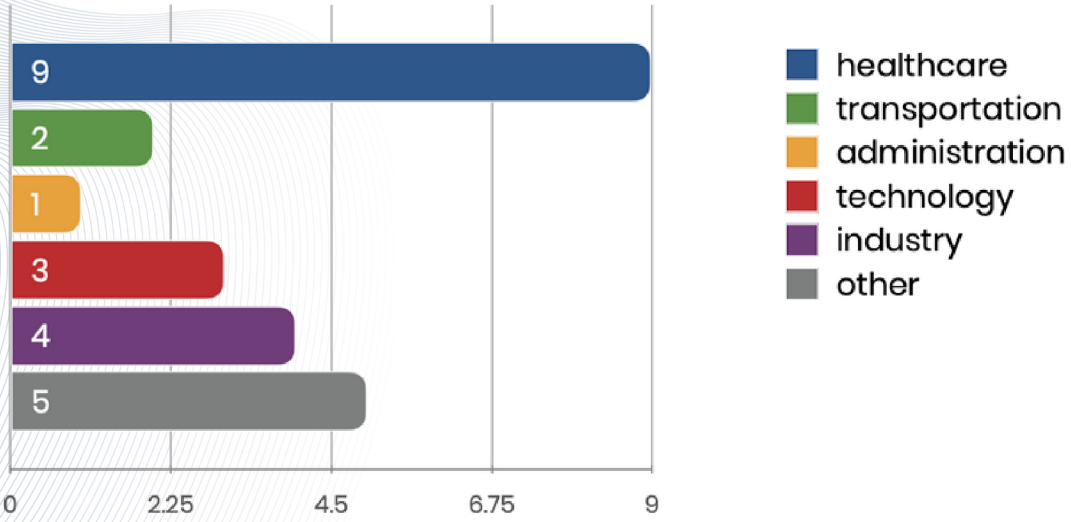


There are, in total, **137 attacks** from the new groups, including **The Coca Cola Singapore** (dragonforce), **ClearWater** (Threeam) and **ForaBank** (werewolves).

Hunters International is the most prolific group, among new additions; as many as 24 attacks in the 120 days considered for the last four-months period.



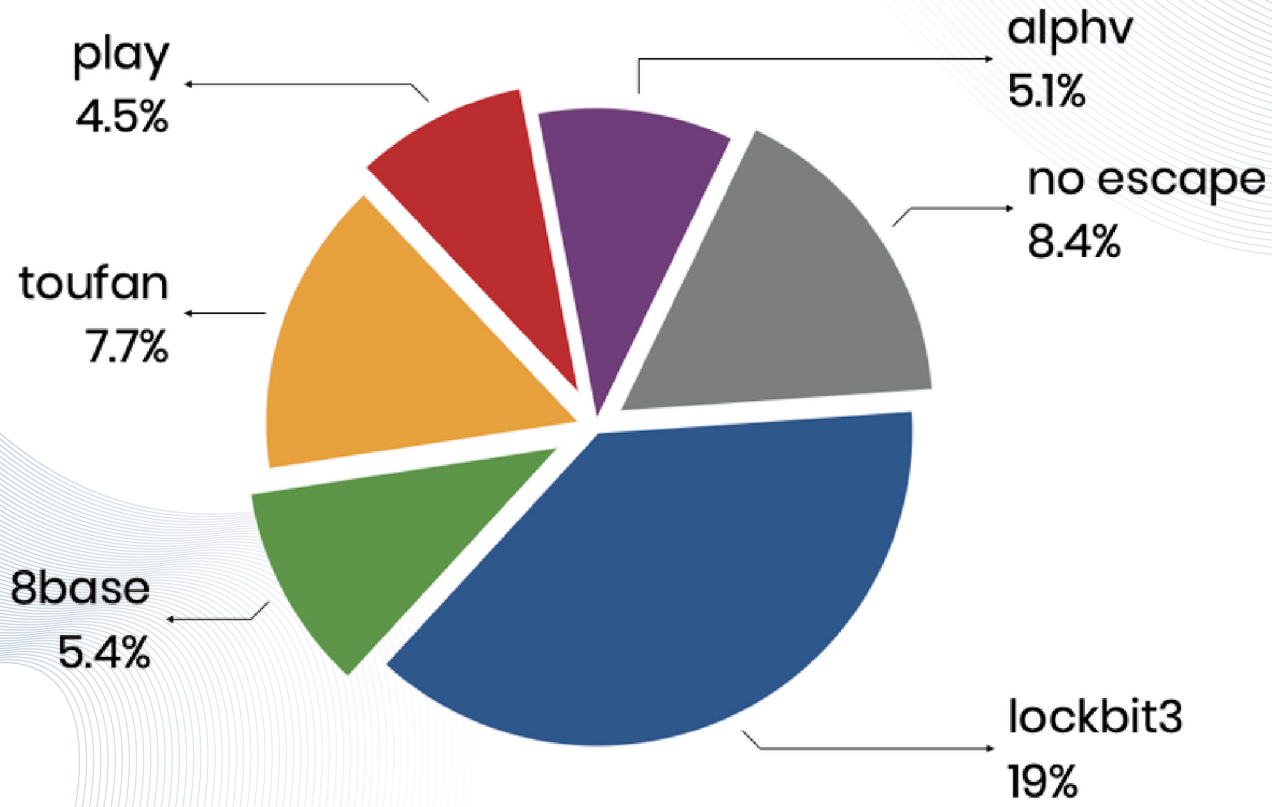
With a predilection for healthcare institutions and medical centers, it is responsible for the attack on AUSL Modena last Dec. 11.



GLOBAL ACTIVITIES OF RANSOMWARE GROUPS

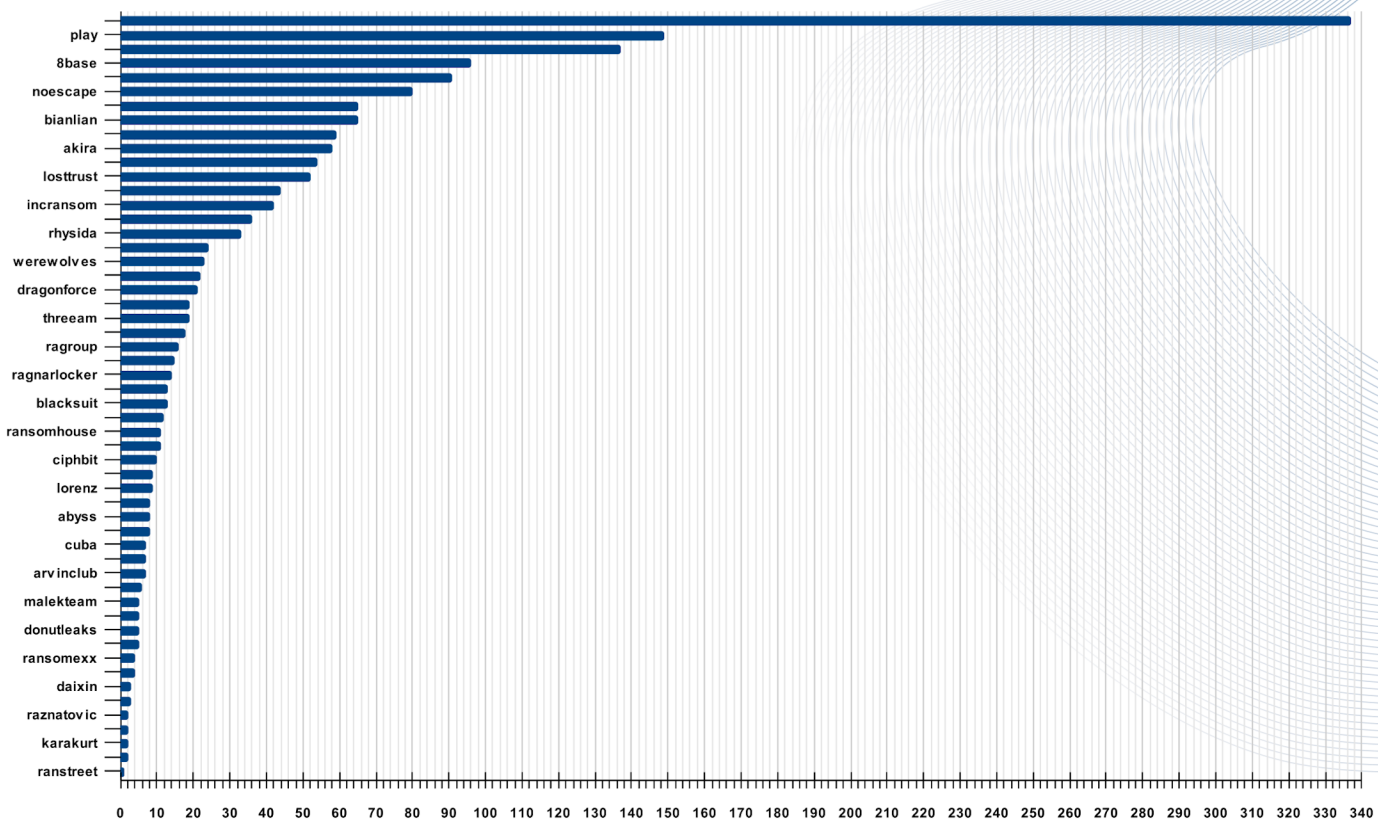
Of all the groups monitored, **only 54 were active** in third quarter of 2023; among the most prolific were **six groups** that alone shared more than 50[of the total attacks.

- Lockbit3
- Play
- Alphv/BlackCat
- 8base
- Cyber Toufan
- NoEscape



Some of the most egregious attacks by these groups include: **NorthWave SRL**, **Korean Petroleum**, the **Peruvian National Police**, **VF Corporation**, and a plethora of mostly U.S.-based higher education institutions.

The chart below shows the detail of **all active groups**, and the progressiveness of their respective claims.



active groups (source ransomfeed.it)

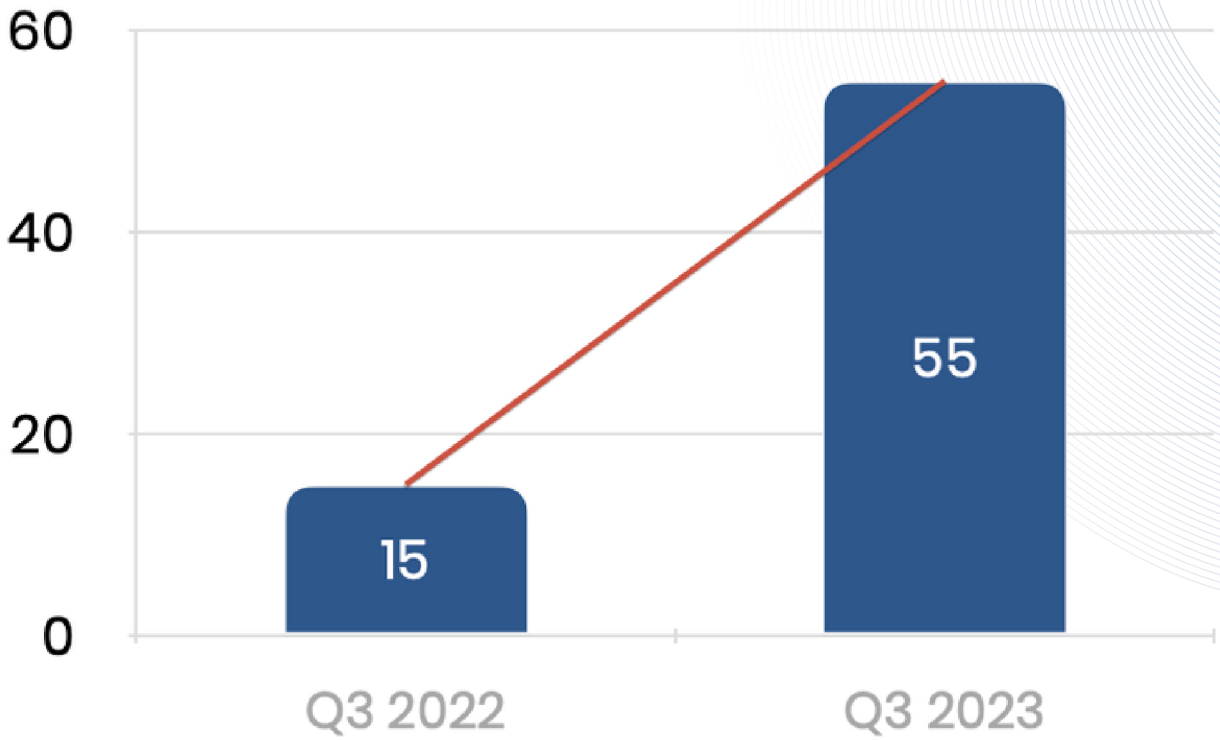
It shows how, even the least active groups, remain monitored, to ensure **transparency and correctness of data** at all times.

On **Ransomfeed** it is possible to perform **different types of searches**, such as by **Groups/Months** or by **Countries/Months**. The focus on Italy is guaranteed both through an **Italy/Months** statistic and through the **data filtering function** - available also for **Switzerland**.

What's more, it is possible to get an **overview of Groups and Countries**, being able to view data by sorting by name, date or attack volume.

FOCUS ITALIY THIRD QUARTER 2023

The focus on Italy reveals a **steady trend of attacks**, with an average frequency of almost **one attack every two days**.



Among the most important attacks in the four-month period is the attack on the **Modena USL** (December 2023) by the **Hunters International** group, with **954,7GB** of data exfiltrated.
Also in December, **akira** attacked the company **Getrix**, producer and manager of the **Immobiliare.it** group's management software; **data are not available**.

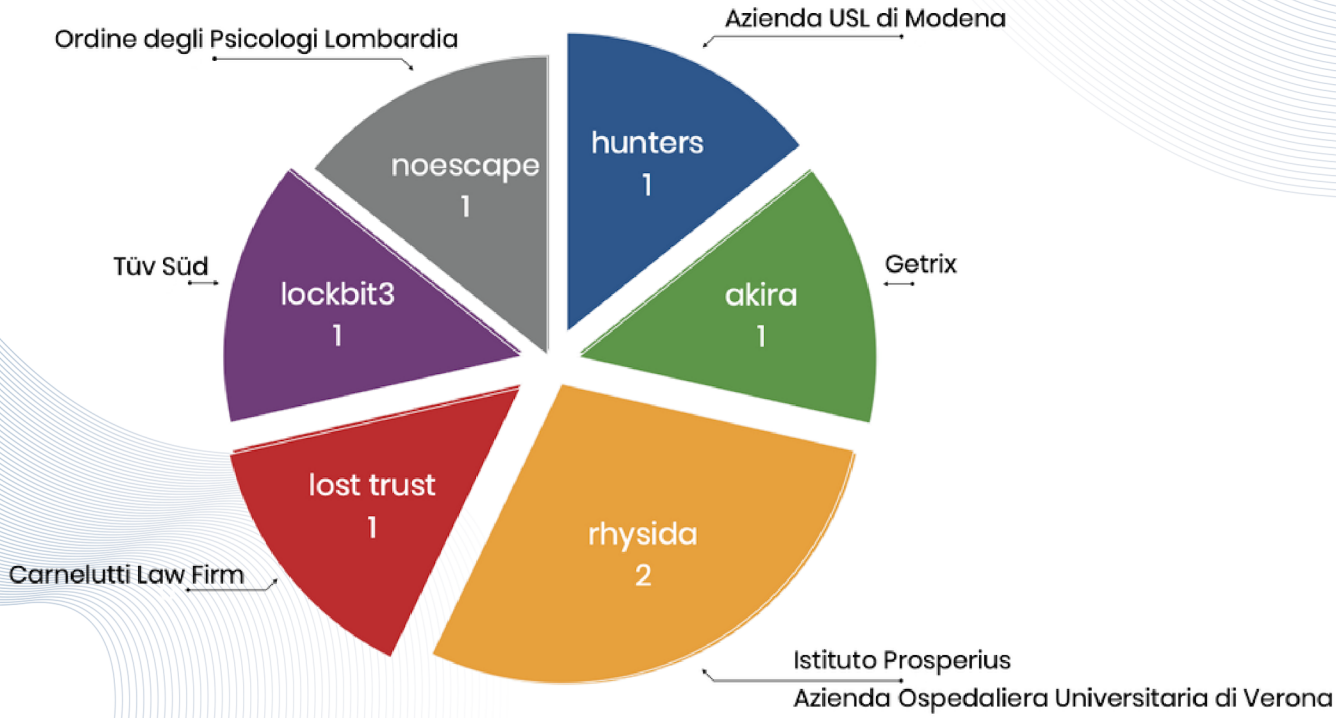
The **Rhysida** group hit the **Istituto Prosperius** in Florence in September, exfiltrating **234GB** worth of data; they released only half the data on their site.

Curious note: within the Prosperius health dataset were found documents related to an investigation into the **Tuscan calciopoli**, copied directly from the Prosecutor's Office in Prato and Florence.

September was a **particularly interesting month** because of the extent of the casualties: the **Lost Trust** group (currently inactive) attacked the **Carnelutti law firm**, one of the best known nationwide. Unknown how much data was exfiltrated and whether or not it was published.

Certifying institute **Tüv Süd** fell victim to **Lockbit3**, with **33GB** of data stolen.
Also hit was the **Ordine degli Psicologi della Lombardia**, in October, with a total of **7GB of exfiltrated** data; attacking was the **NoEscape** group.

In November we find the **Rhysida** group again, with an attack on the **Azienda Ospedaliera Universitaria Integrata di Verona**, from which **612GB** came out.



distribution of the attacks performed in Italy (source ransomfeed.it)

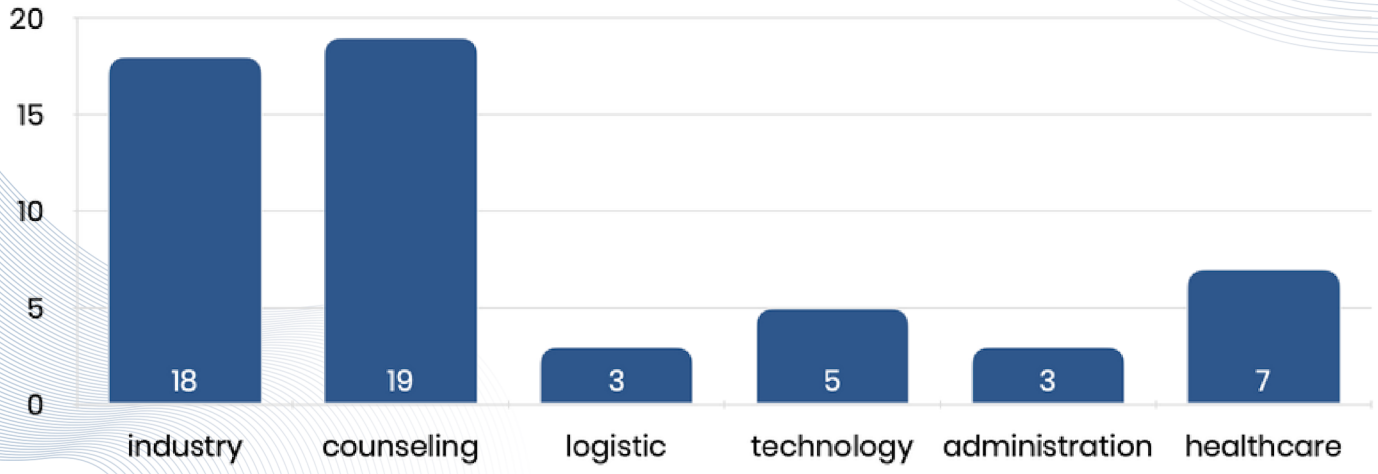
• ATTACKS PER BUSINESS SECTOR

Industry and counseling are the most affected labor sectors with, respectively, 18 and 19 attacks in the territory; below is an overview:

- pharmaceutical industry
- mechanical industry
- metal industry
- electronics industry

} 32.7%

- professional studies, 34.5%
- health, 12.7%
- technology, 9.1%
- logistics, 5.5%
- public administration, 5.5%

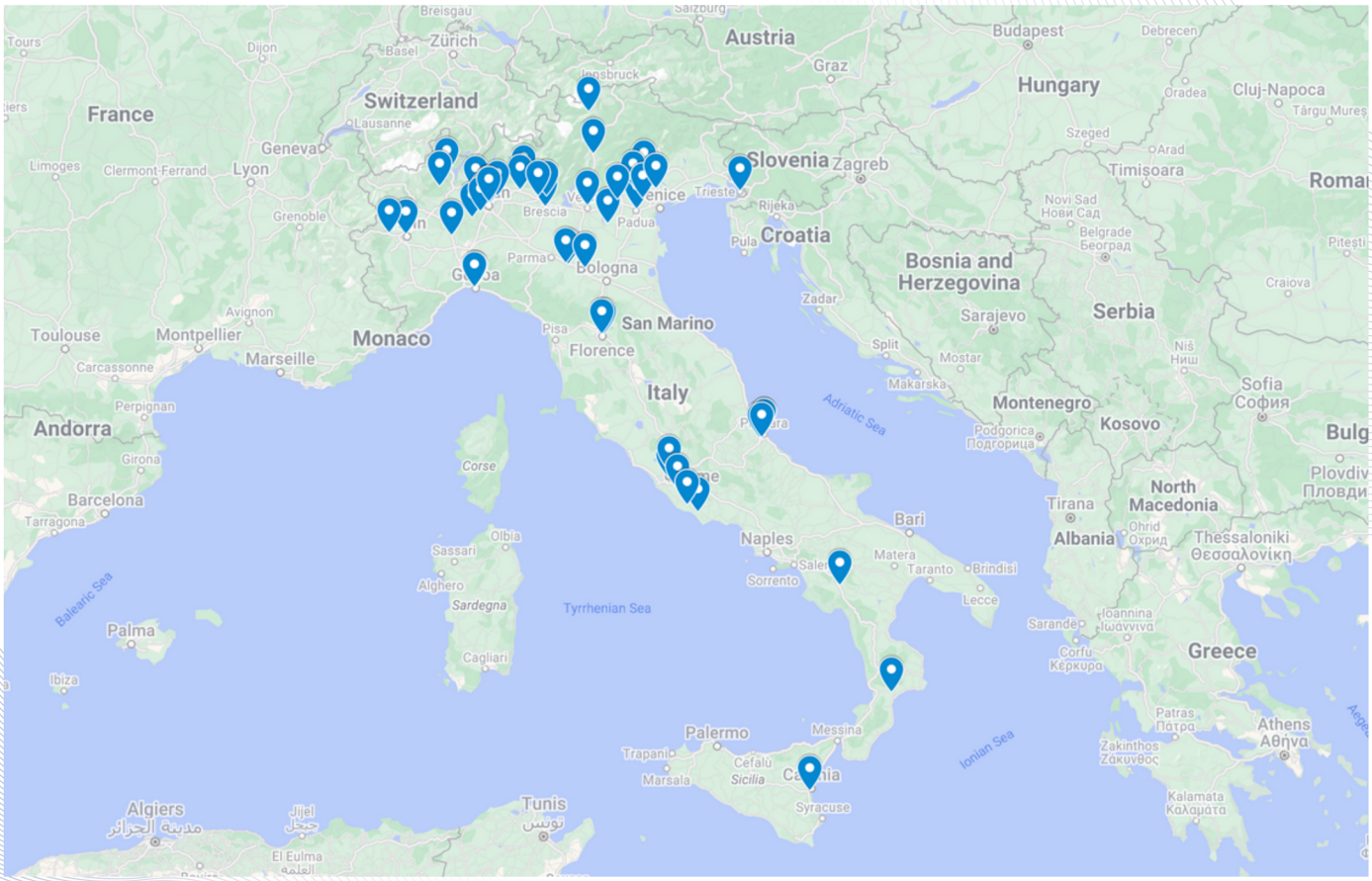


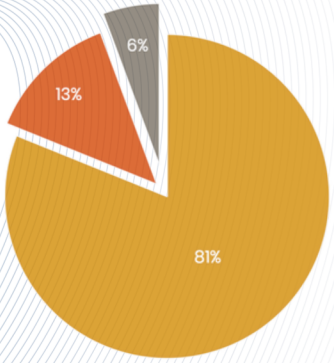
diversification by labor sectors (source ransomfeed.it)

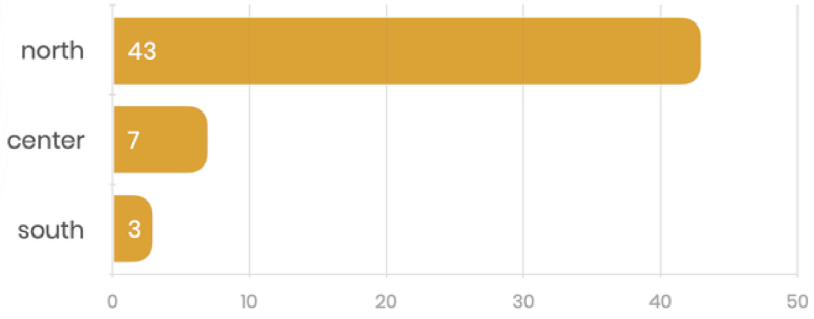
• DISTRIBUTION OF RANSOMWARE ACROSS TERRITORY

By localizing all the victims, we can draw a map to define the geographical **distribution of ransomware** in Italy for the four-month reporting period. More than 80% of the victims are located in **northern Italy**.

Note: The map can also be viewed online, with its interactive feature, by clicking on it.



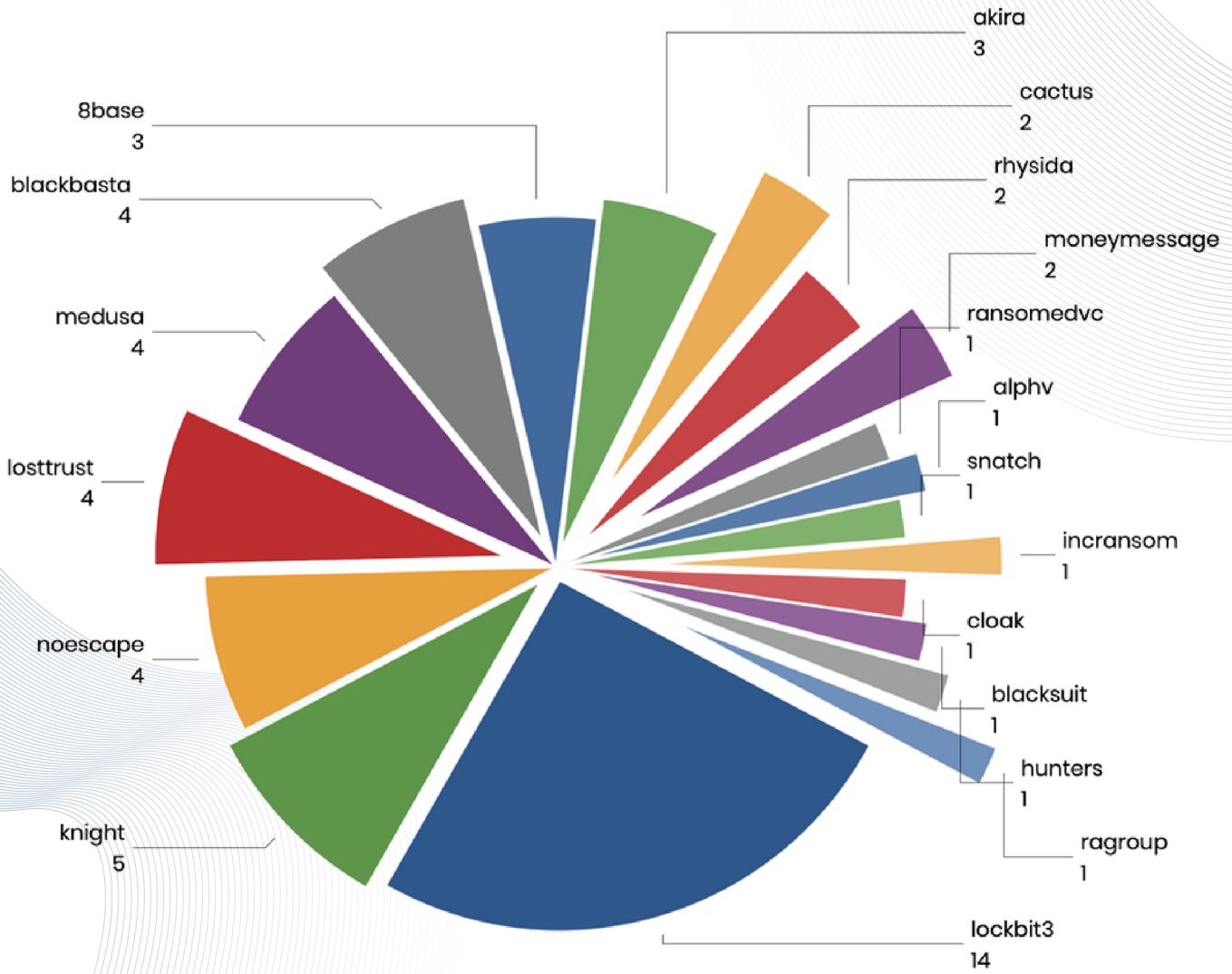




• MOST ACTIVE CRIMINAL GROUPS

The **Lockbit3** group emerges as the **most active in Italy**, with **25% of attacks** recorded in the four-month period.

A clear distance between Lockbit3's operations and the other cyber gangs becomes visible again, underscoring a predominant activity and a constancy that is not inconsiderable.



ADVANCED **DATADRIVEN** CYBERNEWS

THE PROJECT

Ransomfeed is a **continuous monitoring service** for ransomware groups; using scraping, which is the extraction of data from multiple websites by means of software programs and the subsequent structuring of the same, the platform stores the claims in a **permanent RSS feed**, available for free consultation.

The monitoring **service is free** and usable by all, and constantly collects and analyzes data on attacks internationally.

The platform is able to detect attacks in a timely manner, making the data available to anyone wishing to understand the extent and evolution of cyber attacks.

The project is **free of financial constraints**, **not tied to sponsors** or supporters of any kind; staff is not paid in any way.

Companies wishing to have a customized report, with pattern analysis and relevant statistics by business sector, can request a private consultation.

Learn more: ransomfeed.it


ransomfeed
ADVANCED DATADRIVEN CYBERNEWS
THANK YOU
RANSOMFEED | RANSOMFEED.IT | AN ITALIAN PROJECT