
ransomfeed
ADVANCED DATADRIVEN CYBERNEWS
REPORT Q3 2023
RANSOMFEED.IT
RANSOMFEED | RANSOMFEED.IT | AN ITALIAN PROJECT

ADVANCED **DATADRIVEN** CYBERNEWS

INDICE

ADVANCED **DATADRIVEN** CYBERNEWS

> Cybersecurity non è solo una battaglia tecnologica, ma una guerra costante contro minacce sempre più sofisticate e pervasive, dove la resilienza e la preparazione sono le armi più potenti.
>
> *Dario Fadda*

ADVANCED **DATADRIVEN** CYBERNEWS

INTRODUZIONE AL REPORT

In un'epoca in cui le frontiere tra il virtuale e il reale si fanno sempre più sottili, la cybersecurity viene spesso relegata ad ultima ruota del carro; molte aziende sottovalutano l'importanza di una strategia mirata alla mitigazione di attacchi **ransomware** e preferiscono impiegare scarse risorse per la tutela dei propri dati.

Il **report quadrimestrale** di Ransomfeed offre una **panoramica esaustiva** sull'incremento costante di questo tipo di **attacchi** a livello globale, con un focus particolare sull'Italia, attraverso un attento e capillare lavoro di OSINT.

Abbiamo condotto un'**analisi dettagliata** per identificare e interpretare le **tendenze** nel campo della cybersecurity, evidenziando come, negli ultimi quattro mesi del 2023, gli attacchi ransomware sono aumentati di numero e di caratura.

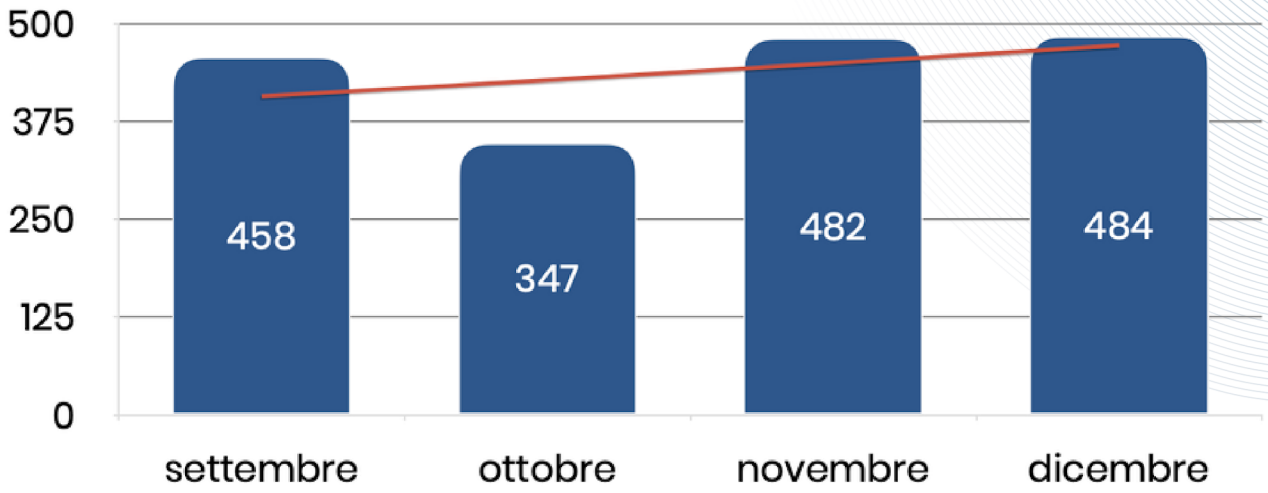
La piattaforma ha monitorato **185 gruppi** criminali operanti in tutto il mondo, con un tracciamento continuo di **342 server** impiegati per condurre attività illecite, per un totale di **1771 rivendicazioni**, di cui **55 registrate in Italia**.

Oltre ai dati rilevati dalla piattaforma, **passati al setaccio** per eliminare duplicati nei record e nei gruppi, abbiamo incrociato i dati con quelli pubblicamente disponibili sui canali ufficiali dei threat actors.
A volte le ricerche sui possibili collegamenti tra le vittime hanno richiesto **giorni di analisi** e approfondimento, ma siamo riusciti a **rendere chiara** per tutti la natura della rivendicazione.

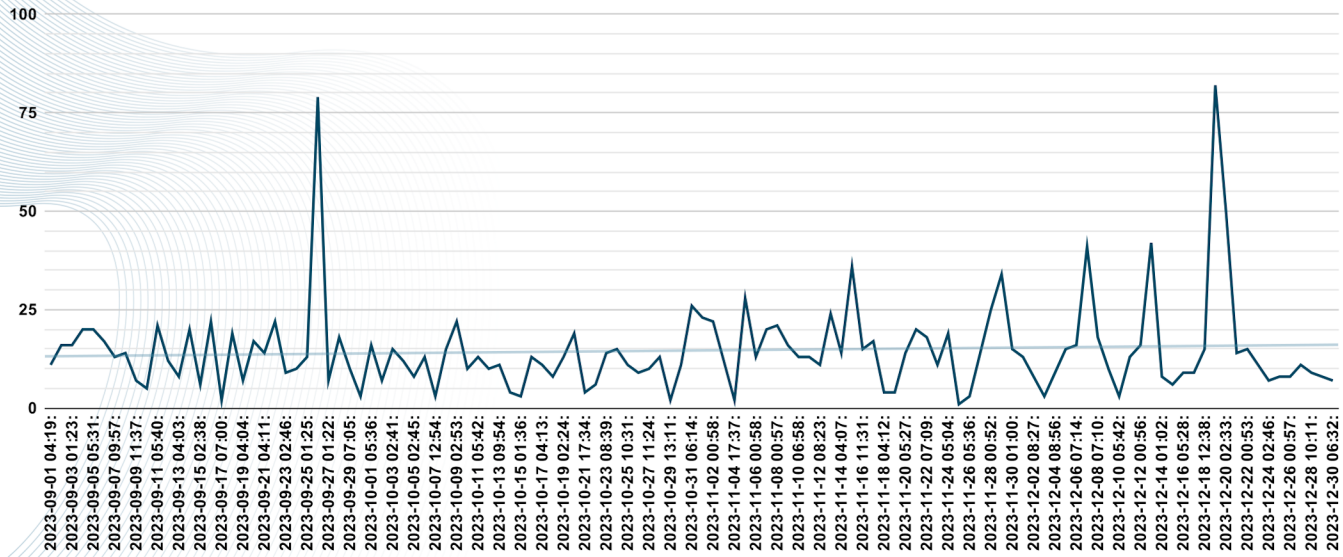
ADVANCED **DATADRIVEN** CYBERNEWS

PANORAMICA

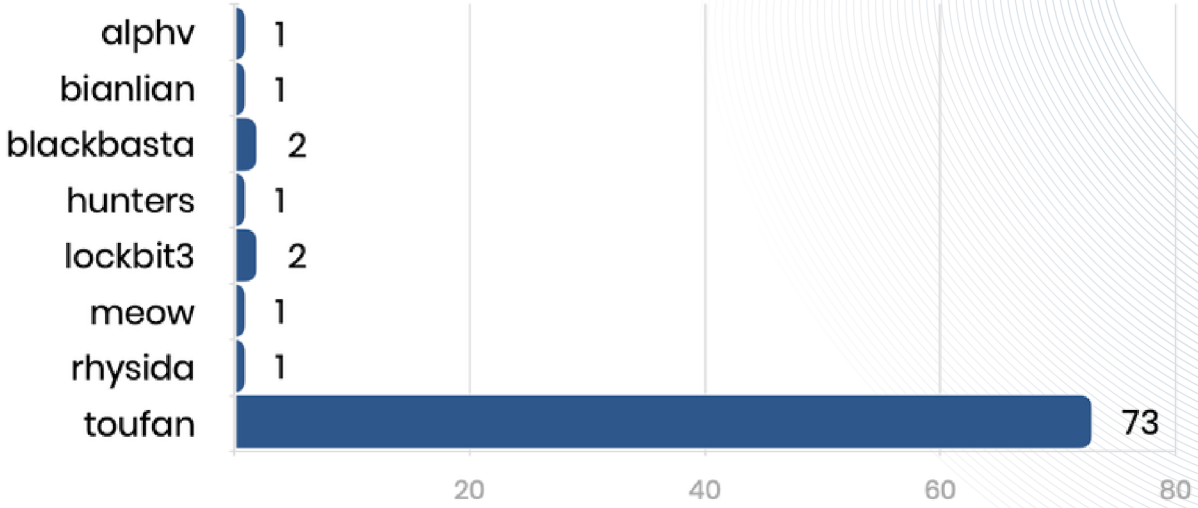
I dati presentati nel report sono lo specchio della **crescente complessità** degli attacchi. Emerge la forte necessità di una **visione consapevole** e **strategica** per affrontare le sfide quotidiane e mettere a punto una strategia di difesa quanto più efficace possibile.

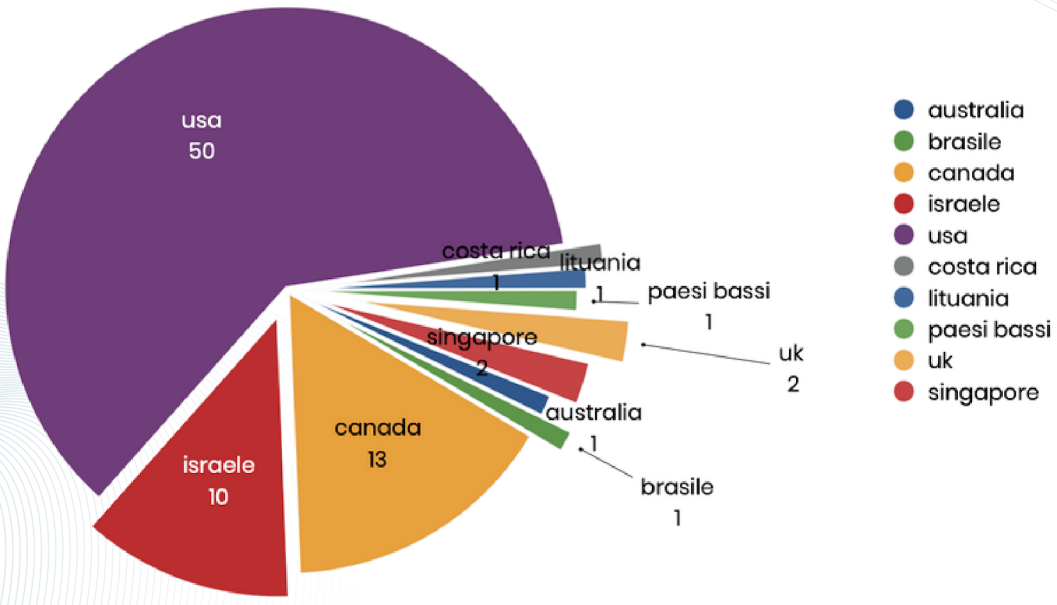


attacchi suddivisi per mese, Q3-2023 (fonte ransomfeed.it)



La **media giornaliera di attacchi** nel corso del quadrimestre supera i 14,6; il **19 dicembre** è stata la giornata più ricca del quadrimestre con **82 attacchi rivendicati**; il numero elevato è dovuto alla comparsa sulla scena del gruppo criminale **Cyber Toufan**, con **73 rivendicazioni**.

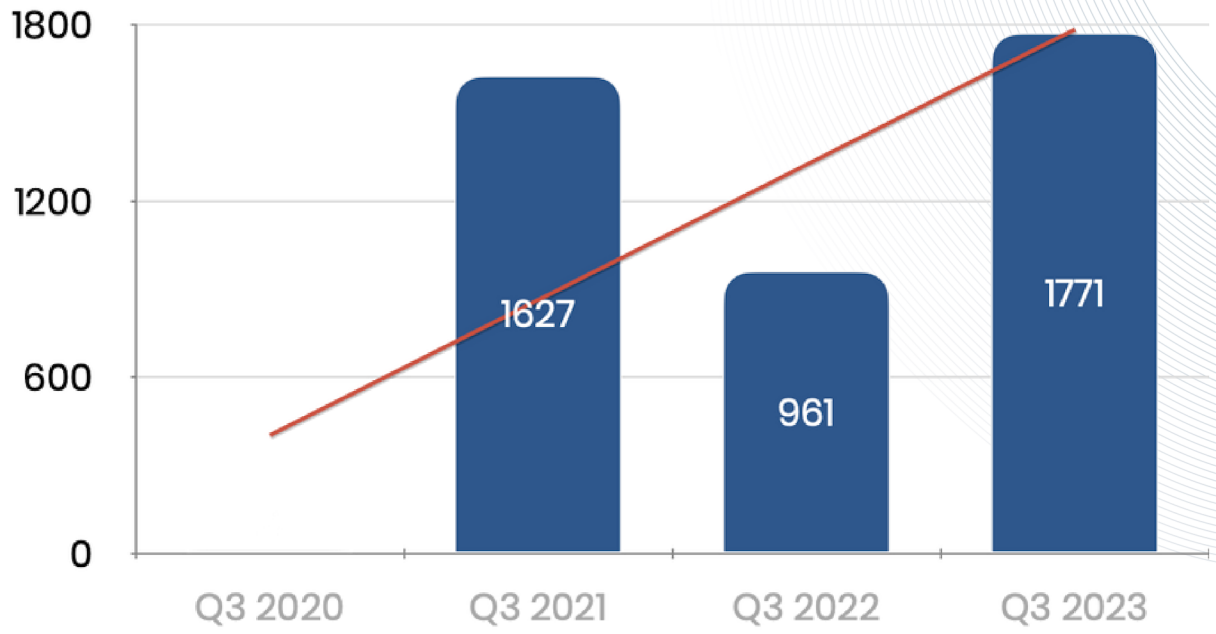




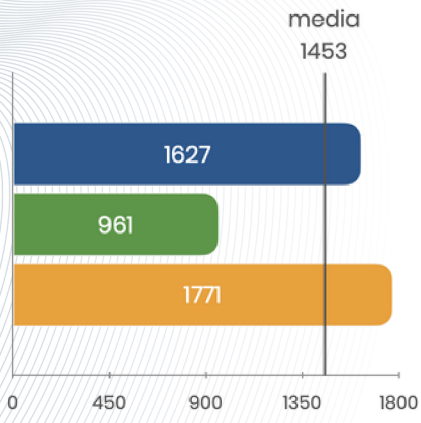
Al contrario, il **25 novembre** ha segnato il giorno meno rilevante, con **una sola** rivendicazione ai danni della **società malesiana Kenso**, rivendicata da **Lockbit3**.

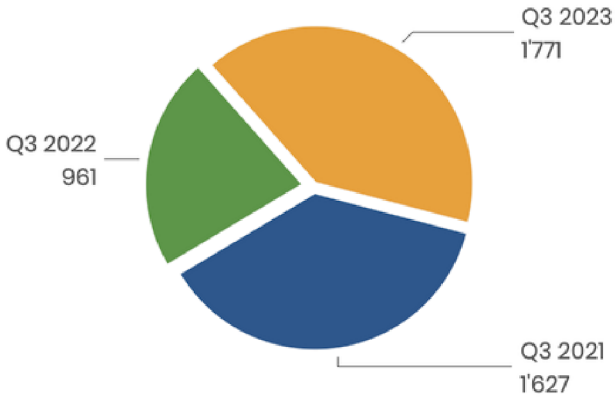
• QUADRIMESTRI A CONFRONTO

Le differenze tra i Q3 degli anni precedenti (sempre precisando che la piattaforma **Ransomfeed** è stata inizialmente alimentata con i dati pregressi **fino al 12 gennaio 2020**) restituiscono un quadro piuttosto eloquente della progressione.



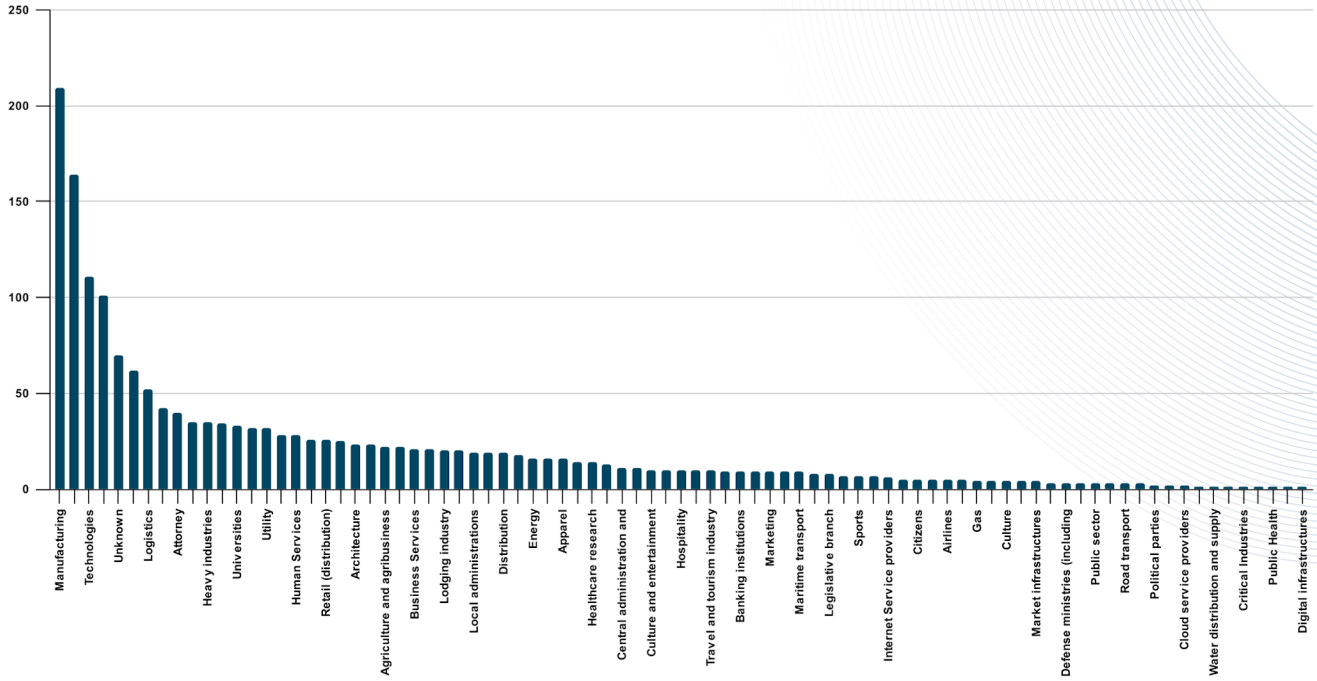
Non si registrano diminuzioni, a livello globale, anzi, stiamo assistendo ad un aumento progressivo: **l'incremento** dal Q3-2022 al Q3-2023 è stato dell'**84,29%**





DISTRIBUZIONE DEL RANSOMWARE PER SETTORI LAVORATIVI

Grazie alla collaborazione tra il nostro progetto **Ransomfeed** e **Würth Phoenix** (guidato dall'esperto **Massimo Giaimo**), è stato possibile controllare ed allineare tutti i dati mancanti riguardanti il settore lavorativo delle vittime.



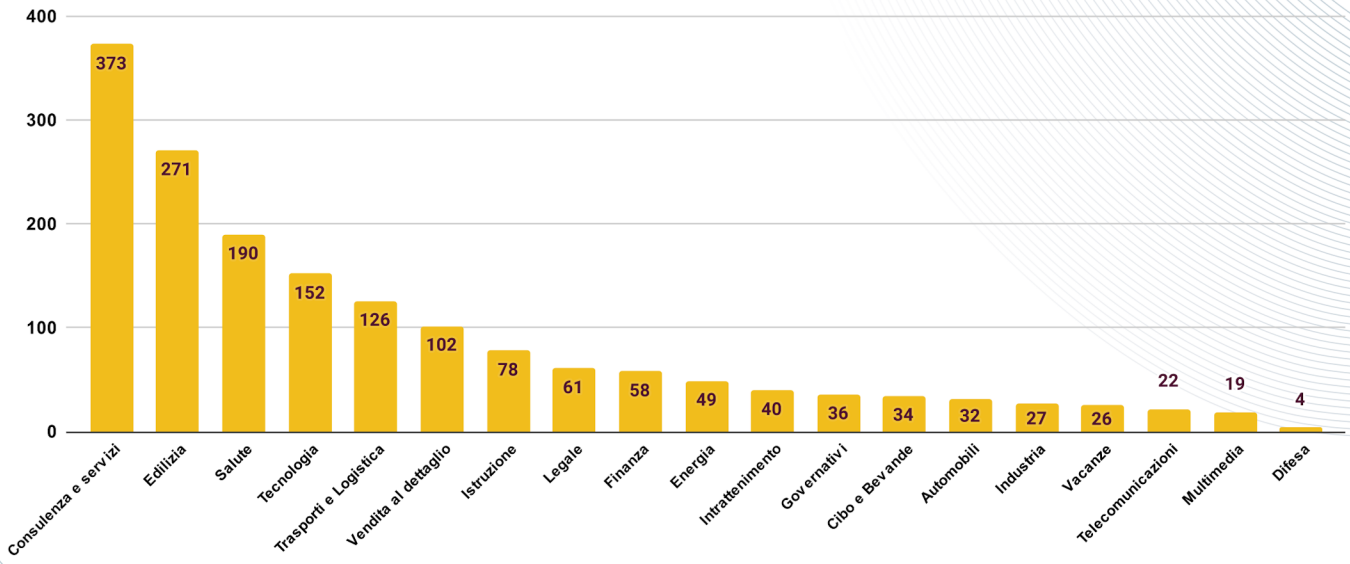
Nelle **prime cinque posizioni del podio**, troviamo:

- 💼 settori **consulenza/servizi**
- 🏗️ settore **edile**
- 😷 settore **sanitario**
- 🖥️ settore **tecnologico**
- 🛞 settore **logistica/trasporti**

Questi sono anche i settori che si dividono una fetta pari quasi al **60% del mercato ransomware** a livello globale (dati Q3-2023).

L'aumento degli attacchi ad **agenzie che si occupano, e/o impattano sulla sicurezza nazionale**, fa balzare la categoria alla **13esima posizione** con **39 attacchi** rivendicati.

Sommando gli attacchi registrati ai settori della **difesa**, delle **organizzazioni internazionali governative** e l'ampio settore della **giustizia**, il dato si fa allarmante: **oltre 40 rivendicazioni** nel quadrimestre, con una **incidenza di circa il 4% del totale**, percentuale raddoppiata rispetto al dato considerato nel segmento 2022.



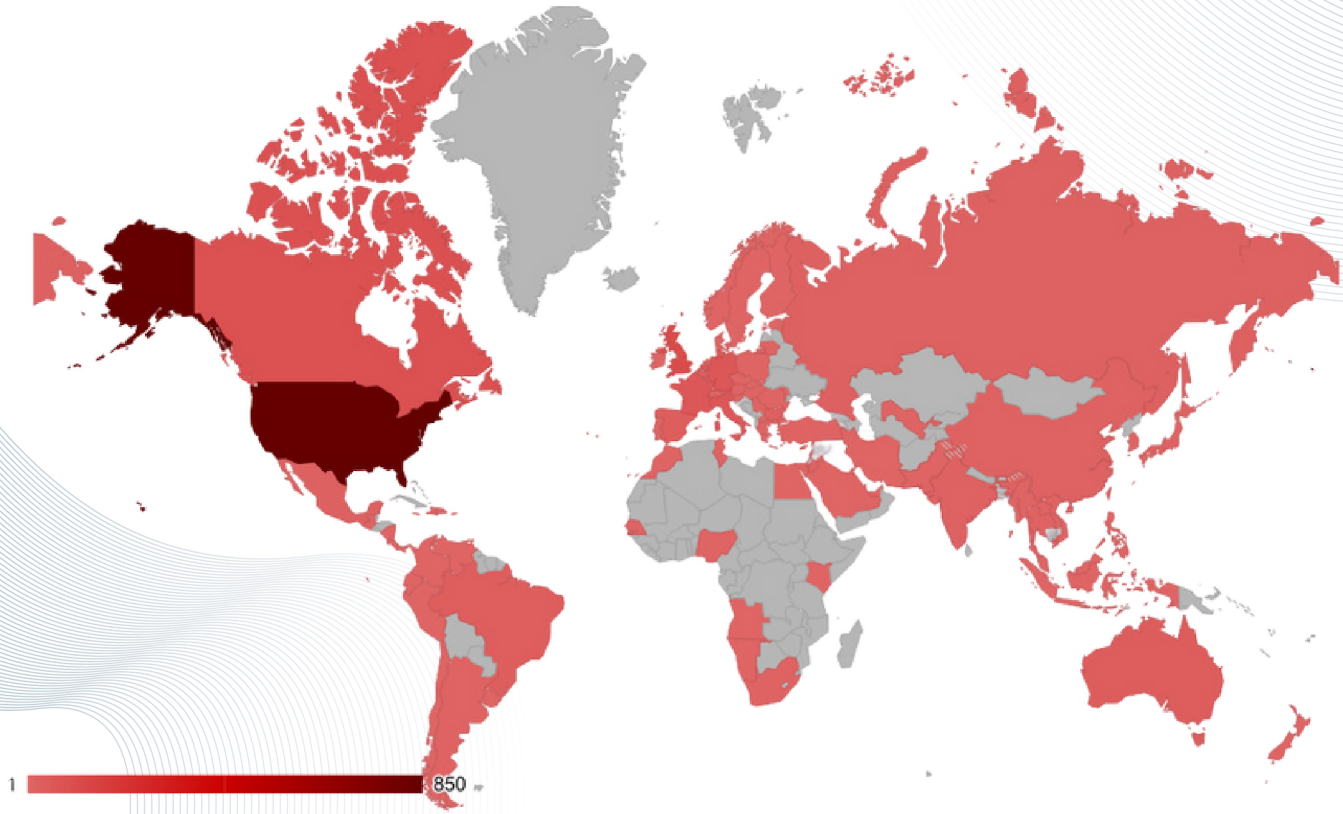
i settori colpiti (fonte Ransomfeed)

DISTRIBUZIONE DEL RANSOMWARE NEL MONDO

Il lavoro di **ricerca**, **controllo** e **localizzazione** post scraping ci consente di ottenere un quadro completo e tempestivo della posizione geografica degli attacchi.

Come spesso abbiamo visto, la **maggior parte delle rivendicazioni** è da collocarsi nel territorio degli **Stati Uniti**, seguono Europa, Canada e Asia.

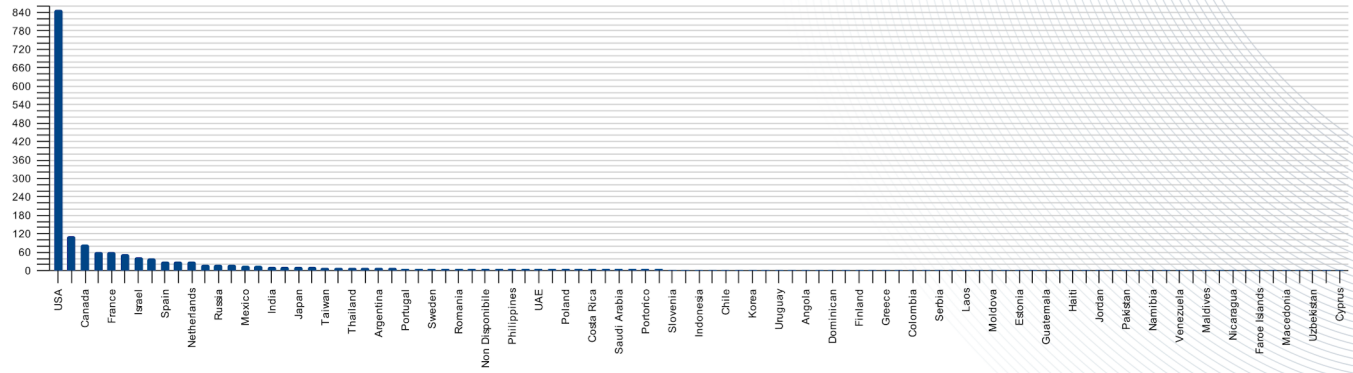
Molti stati **dell'Africa** sono meno impattati dagli attacchi ransomware, un po' per la **mancanza di infrastrutture** tecniche e un po' per **mancanza di obiettivi** considerati "appetibili" per i criminali.



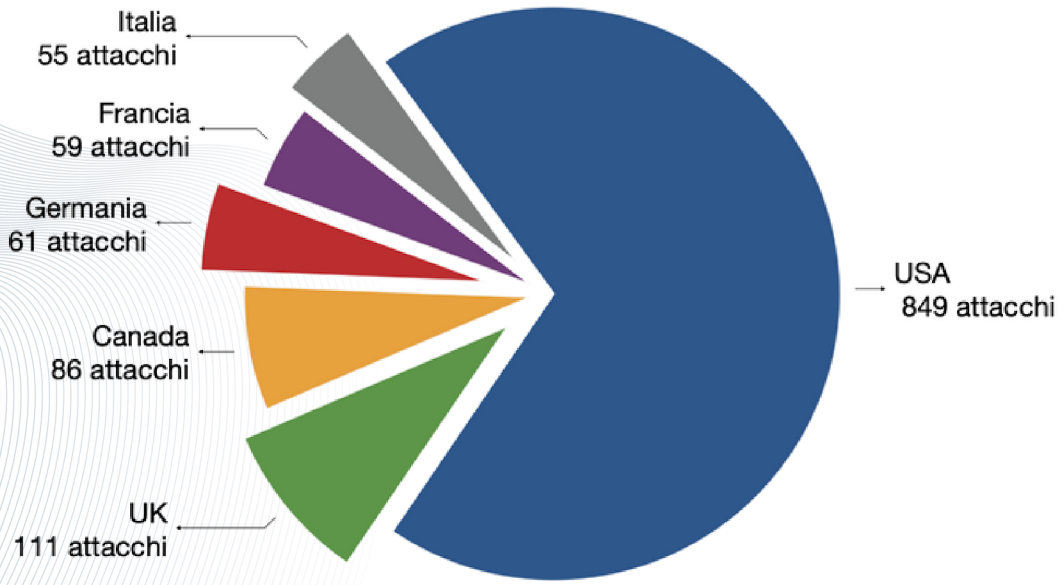
nelle gradazioni di rosso, gli attacchi con vittime (fonte Ransomfeed)

Rispetto al Q2 2023 abbiamo registrato un **incremento delle rivendicazioni** in **Russia**, per lo più dovuto a gruppi criminali schierati contro il governo.

Tra questi, il gruppo più attivo è **werevolves** con **16 rivendicazioni all'attivo**; nel corso del 2023, invece, è stato il gruppo **malas** a segnare il record di attacchi alla Russia: se ne contano **37**.



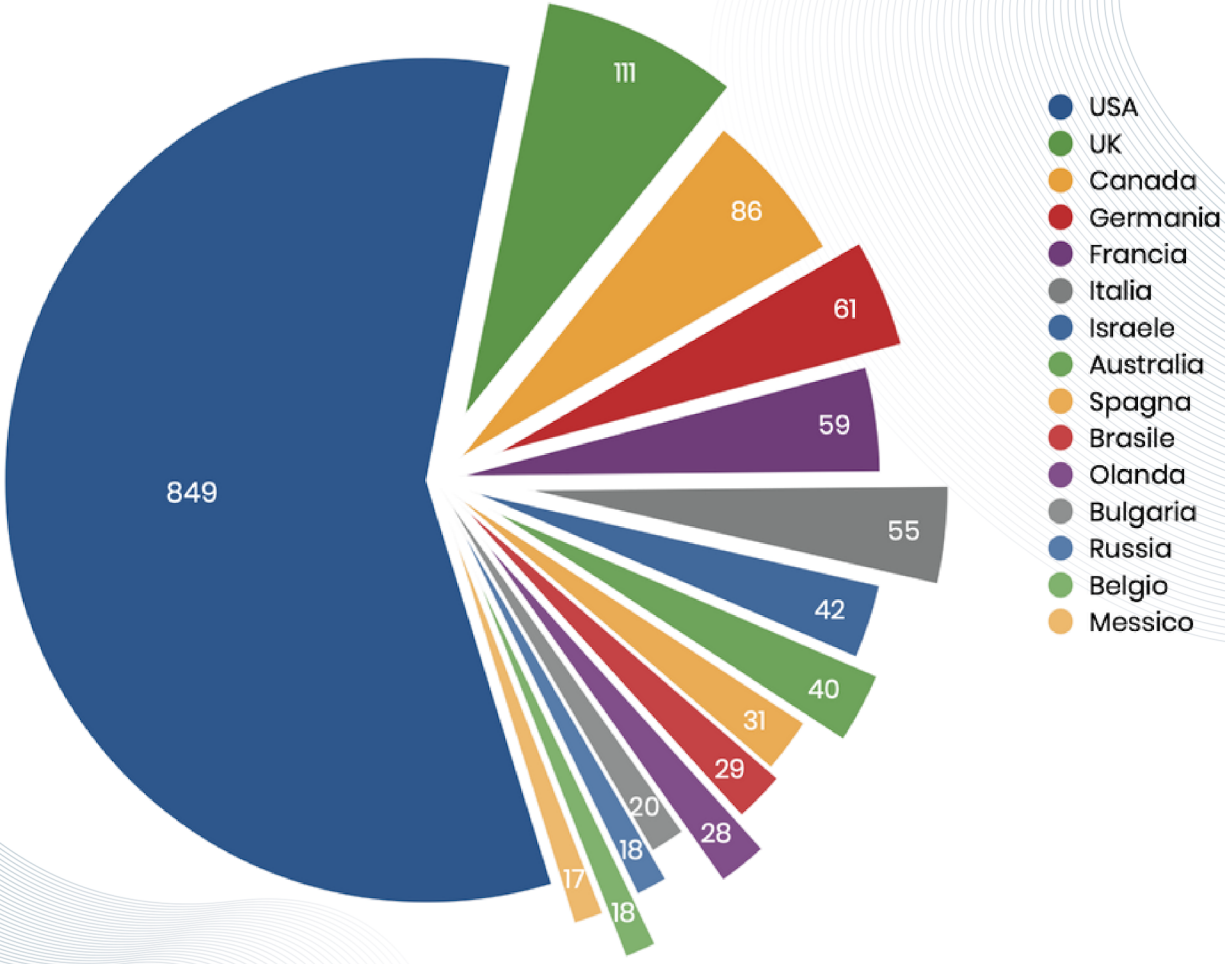
Gli **USA** (**849 attacchi**) restano al primo posto dei paesi attaccati, coprendo il 48% del totale; seguono Regno Unito, Canada e Germania. **L'Italia**, nel Q3 2023, si attesta in sesta posizione con **55 attacchi**.



rappresentazione dei primi sei paesi colpiti (fonte Ransomfeed)

• TOP 15

Nel grafico sono stati **esclusi** tutti i paesi con un numero di attacchi ransomware inferiore a 1%.



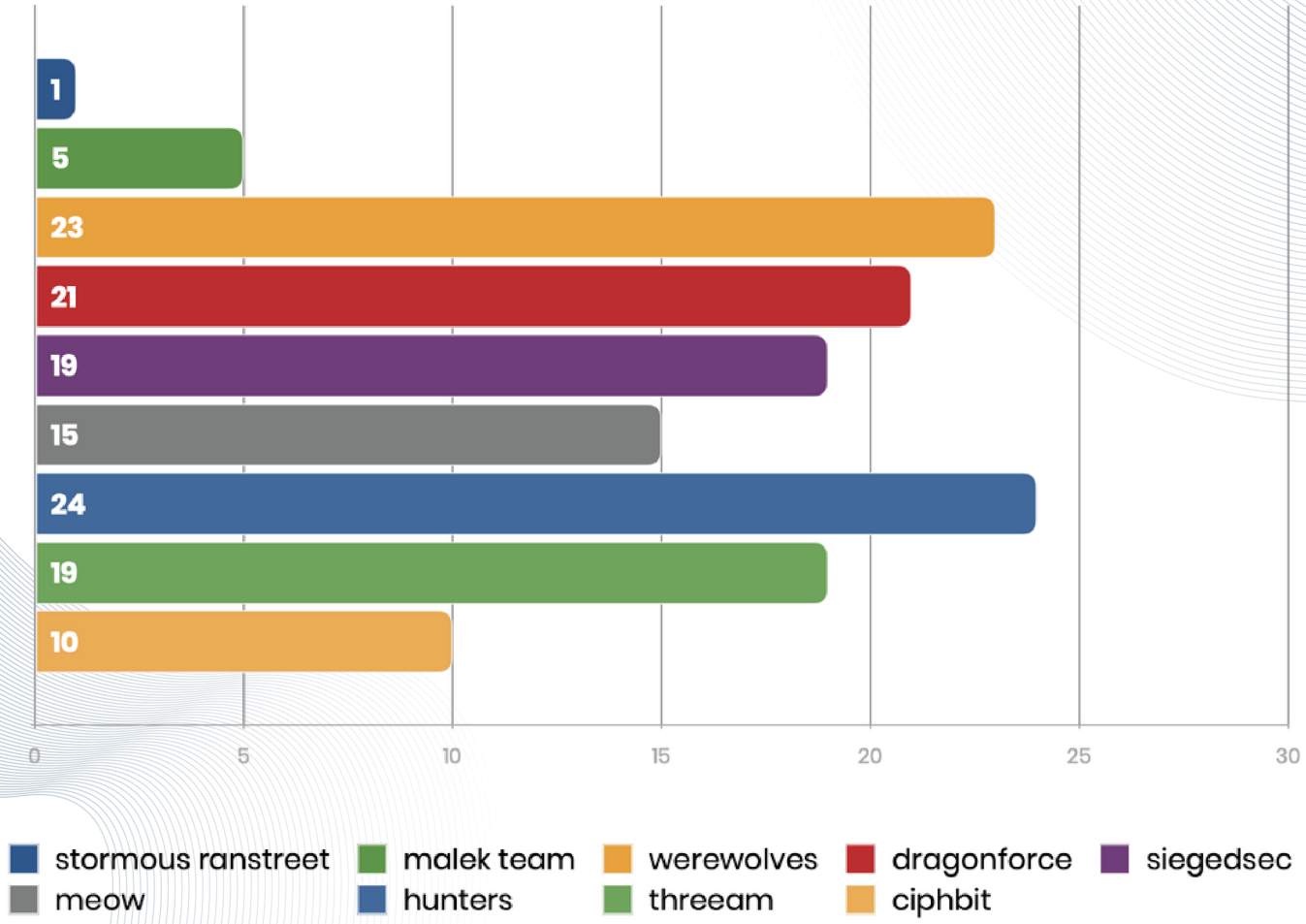
Top 15 per numero di vittime (fonte Ransomfeed)

Il divario tra gli **attacchi registrati in USA** e quelli registrati nel **resto del mondo**, ancora una volta, è davvero enorme.
Non solo la superficie territoriale più ampia, anche la diversa distribuzione delle aziende (possibili target) rende gli Stati Uniti un **paese molto appetibile** per i gruppi criminali.

NUOVI GRUPPI CRIMINALI

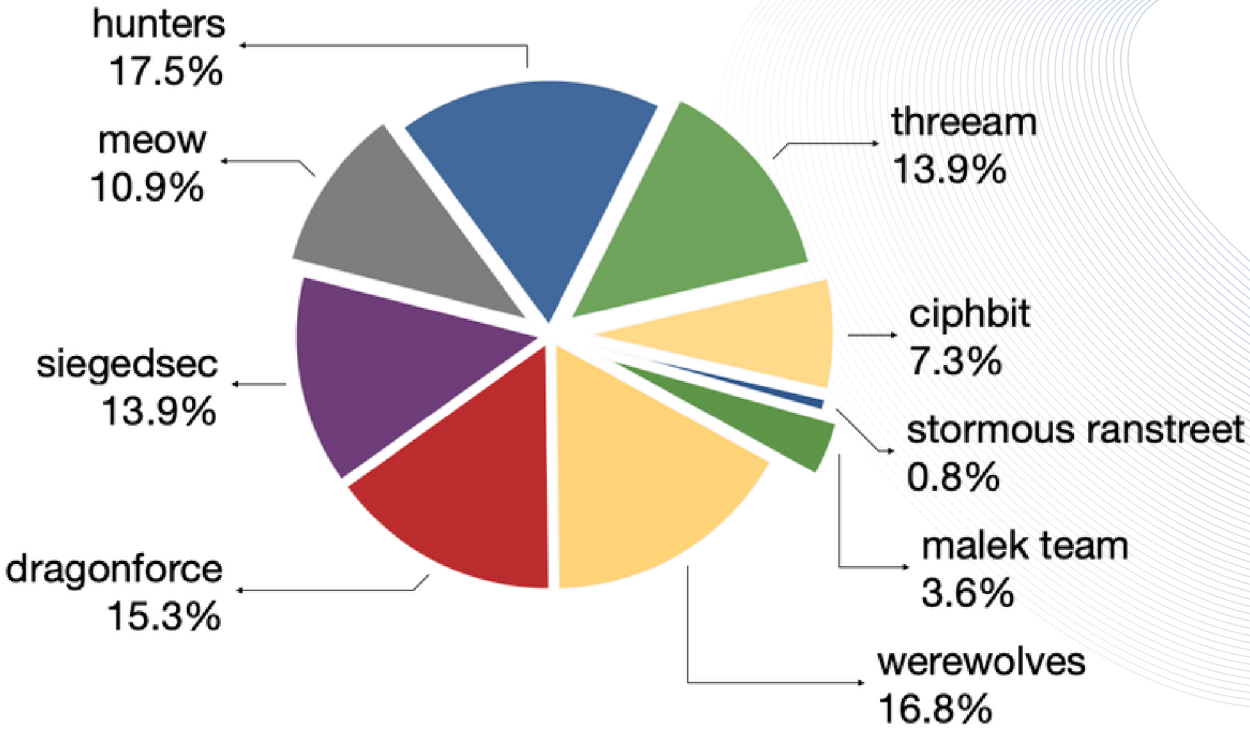
Gli ultimi mesi dell'anno hanno visto **9 nuovi gruppi** affacciarsi sulla scena cyber, alcuni seguiti da non poche polemiche, come nel caso **RansomedVC**.
Il gruppo ha terminato le operazioni come RansomedVC in favore di un rebrand sotto il nome di **Raznatovic**, per poi presentarsi nuovamente sulla scena come **rVC**.

Dal momento che RansomedVC/Raznatovic/rVC non è un nuovo gruppo, non è stato aggiunto alla lista dei monitorati.

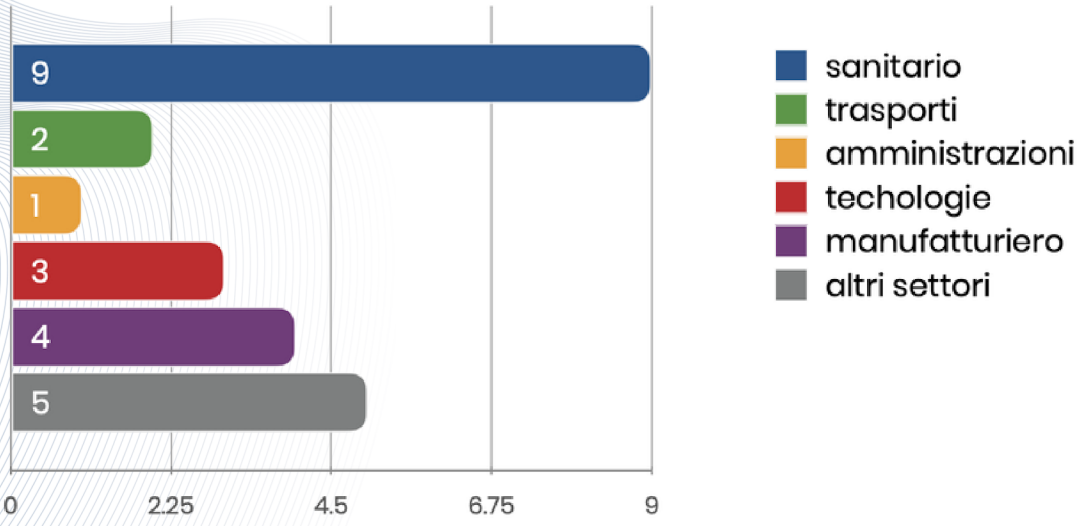


Si contano, complessivamente, 137 attacchi dai nuovi gruppi, tra cui **The Coca Cola Singapore** (dragonforce), **ClearWater** (Threeam) e **ForaBank** (werewolves).

Hunters International è il gruppo, tra i nuovi aggiunti, più prolifico; ben **24 attacchi** nei 120 giorni considerati per il Q3.



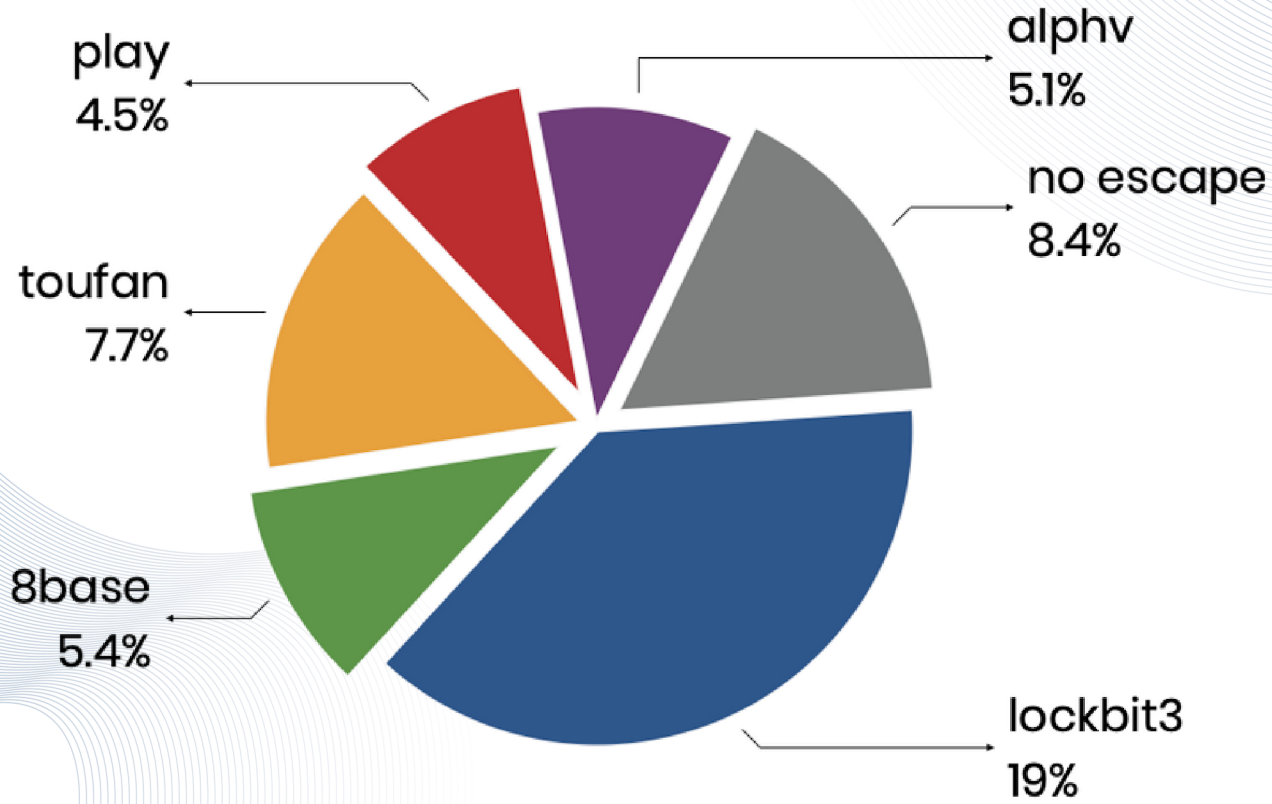
Con una predilezione per gli istituti sanitari e centri medici, è responsabile dell'attacco ad AUSL Modena dello scorso 11 dicembre.



ATTIVITÀ GLOBALI DEI GRUPPI RANSOMWARE

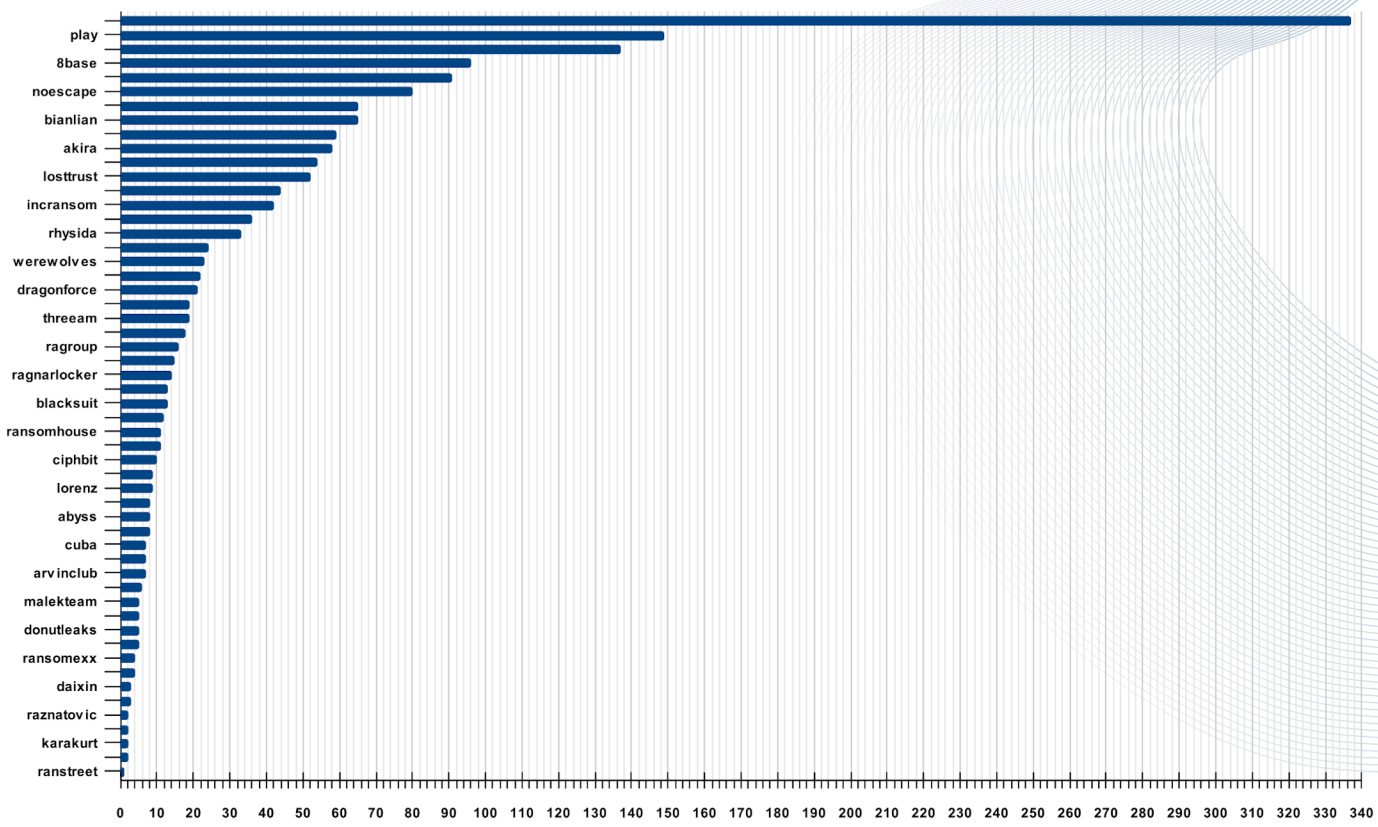
Di tutti i gruppi monitorati, nel Q3-2023 soltanto **54 sono risultati attivi**; tra i più prolifici, **sei gruppi** che, da soli, si sono **spartiti oltre il 50%** del totale degli attacchi.

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



Tra gli attacchi più eclatanti di questi gruppi ricordiamo: NorthWave SRL, Korean Petroleum, la Polizia Nazionale peruviana, VF Corporation, ed una pletora di **istituti scolastici**, per lo più americani, di ordine superiore.

Nel grafico sottostante, il dettaglio di tutti i gruppi attivi, e la progressività delle rispettive rivendicazioni.



gruppi attivi (fonte Ransomfeed)

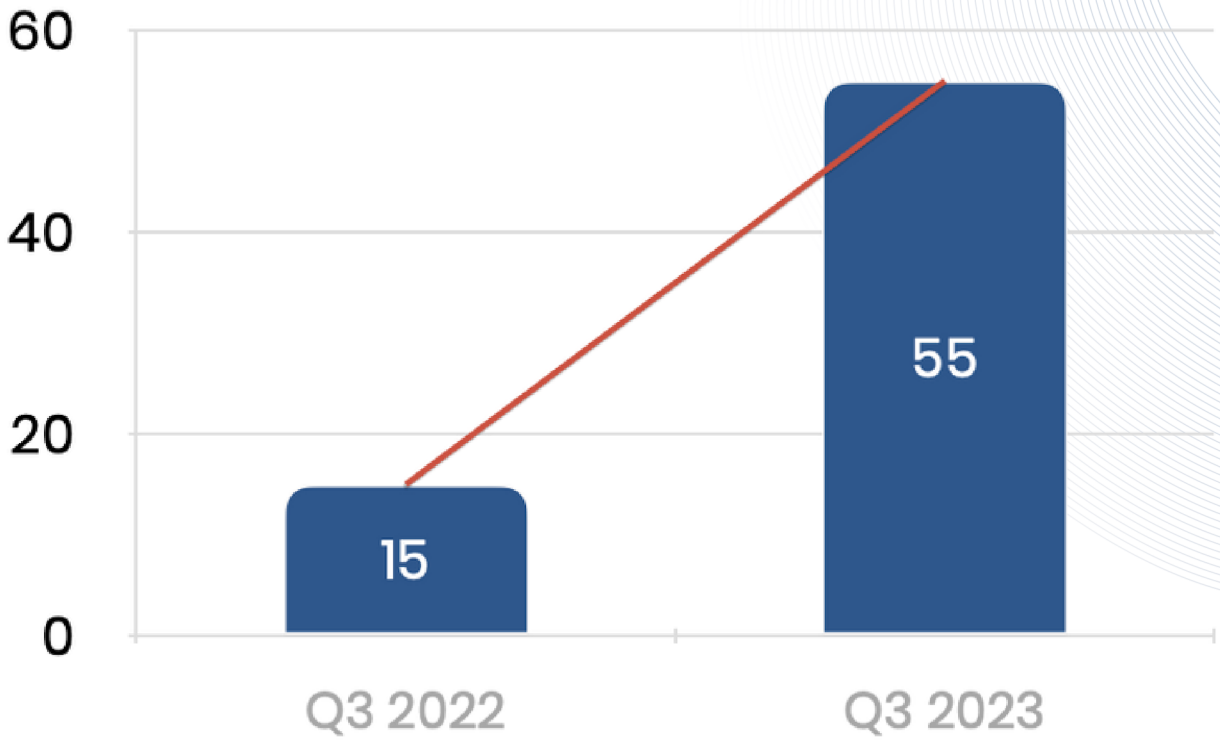
Si evince come, anche i gruppi meno attivi, restano monitorati, per garantire sempre trasparenza e correttezza dei dati.

Su **Ransomfeed** è possibile eseguire diversi tipi di ricerca, ad esempio per **Gruppi/Mesi** o per **Paesi/Mesi**. Il focus sull'Italia è garantito sia tramite una statistica **Italia/Mesi** che tramite la funzione di filtraggio dati - disponibile anche per la **Svizzera**.

E ancora, è possibile avere una panoramica sui **Gruppi** e sui **Paesi**, riuscendo a visualizzare i dati ordinando per nome, data o per volume degli attacchi.

FOCUS ITALIA Q3 2023

Il **focus sull'Italia** fa emergere un andamento costante degli attacchi, con una frequenza media di **quasi un attacco ogni due giorni**.



Tra gli attacchi più importanti del quadrimestre segnaliamo quello all'**Azienda USL di Modena** (dicembre 2023) ad opera del gruppo **Hunters International**, con **954,7GB di dati esfiltrati**.

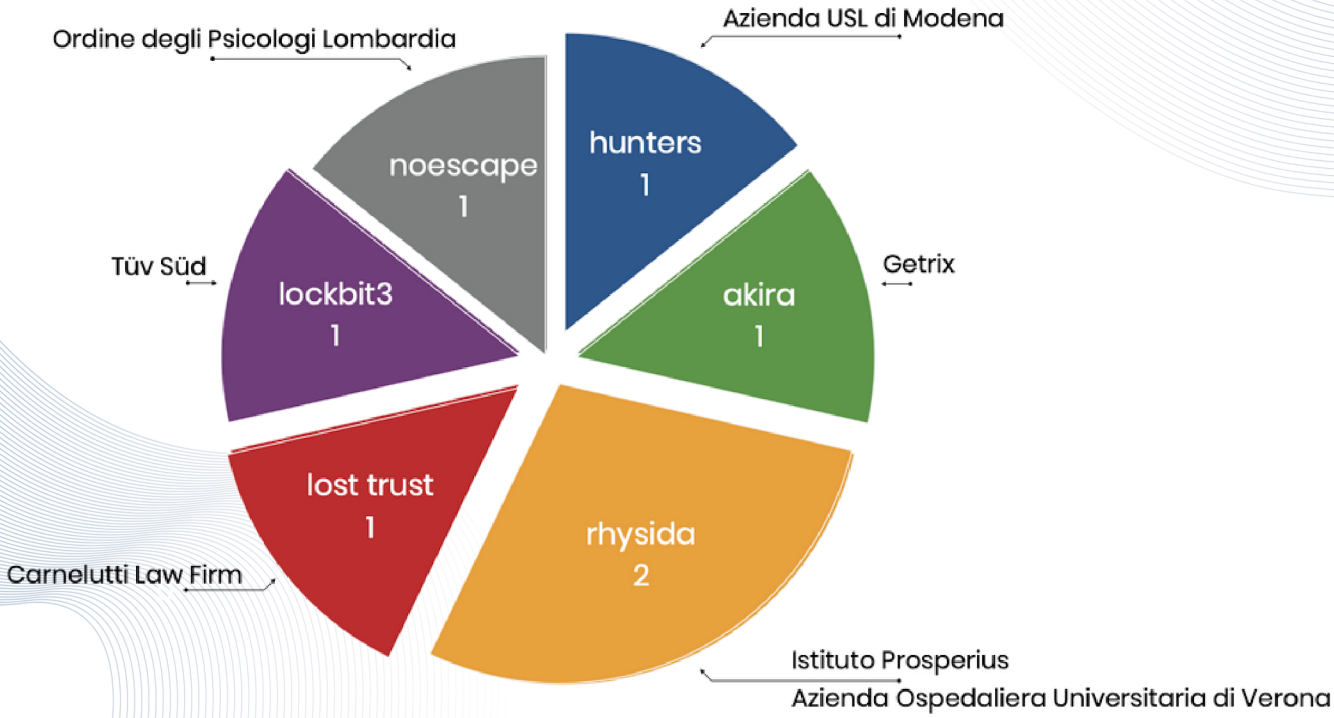
Sempre a dicembre, **akira** ha attaccato l'azienda **Getrix**, produttrice e responsabile dei **gestionali del gruppo Immobiliare.it**; i dati non sono disponibili.

Il gruppo **Rhysida** ha colpito l'**Istituto Prosperius** di Firenze a settembre, esfiltrando dati per **234GB**; sul loro sito hanno rilasciato solo la metà dei dati. Nota curiosa: all'interno del dataset sanitario del Prosperius sono stati rinvenuti documenti relativi ad un'indagine sulla **calciopoli toscana**, copiati direttamente dalla Procura di Prato e Firenze.

Settembre è stato un mese particolarmente interessante per l'entità delle vittime: il gruppo **Lost Trust** (attualmente inattivo) ha attaccato lo **studio legale Carnelutti**, uno dei più conosciuti a livello nazionale. Sconosciuta l'entità dei dati esfiltrati e se siano stati o meno pubblicati.

L'ente certificatore **Tüv Süd** è stato vittima di **Lockbit3**, con **33GB** di dati sottratti. Colpito anche l'**Ordine degli Psicologi della Lombardia**, ad ottobre, con un totale di **7GB** di dati esfiltrati; ad attaccare è stato il gruppo **NoEscape**.

A novembre troviamo di nuovo il gruppo **Rhysida**, con un attacco all'**Azienda Ospedaliera Universitaria Integrata di Verona**, dalla quale sono usciti **612GB**.



distribuzione degli attacchi italiani (fonte Ransomfeed)

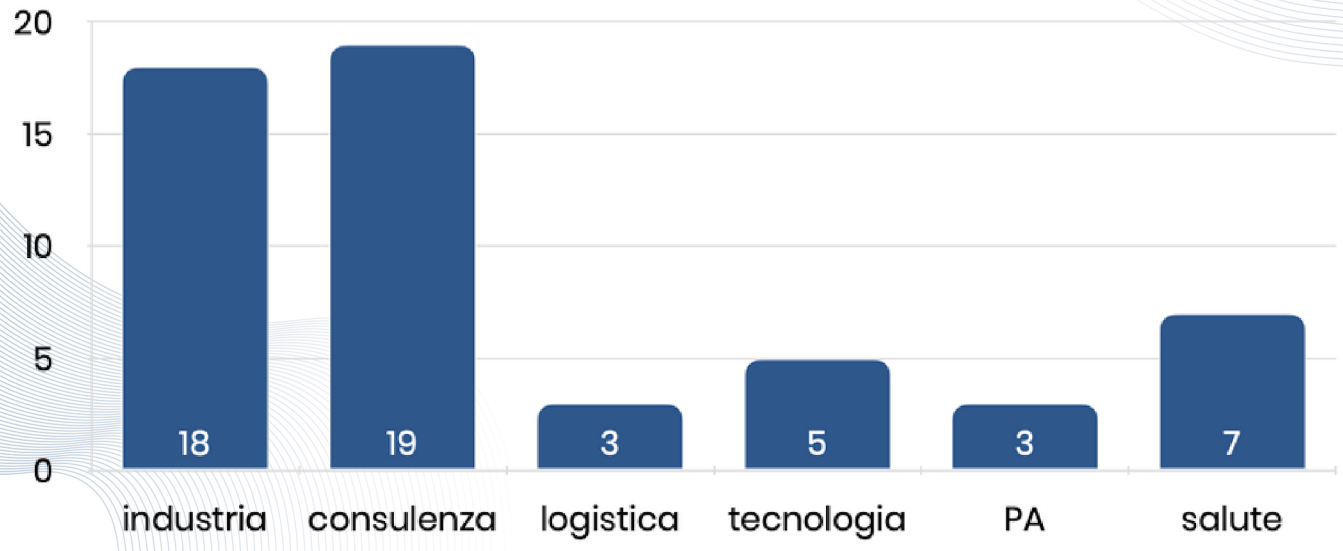
• GLI ATTACCHI PER SETTORE ECONOMICO

Industria e consulenza sono i settori lavorativi più colpiti con, rispettivamente, 18 e 19 attacchi sul territorio; di seguito una panoramica:

- industria farmaceutica
- industria meccanica
- industria metallurgica
- industria elettronica

} 32.7%

- studi professionali, 34.5%
- salute, 12.7%
- tecnologia, 9.1%
- logistica, 5.5%
- Pubblica Amministrazione, 5.5%

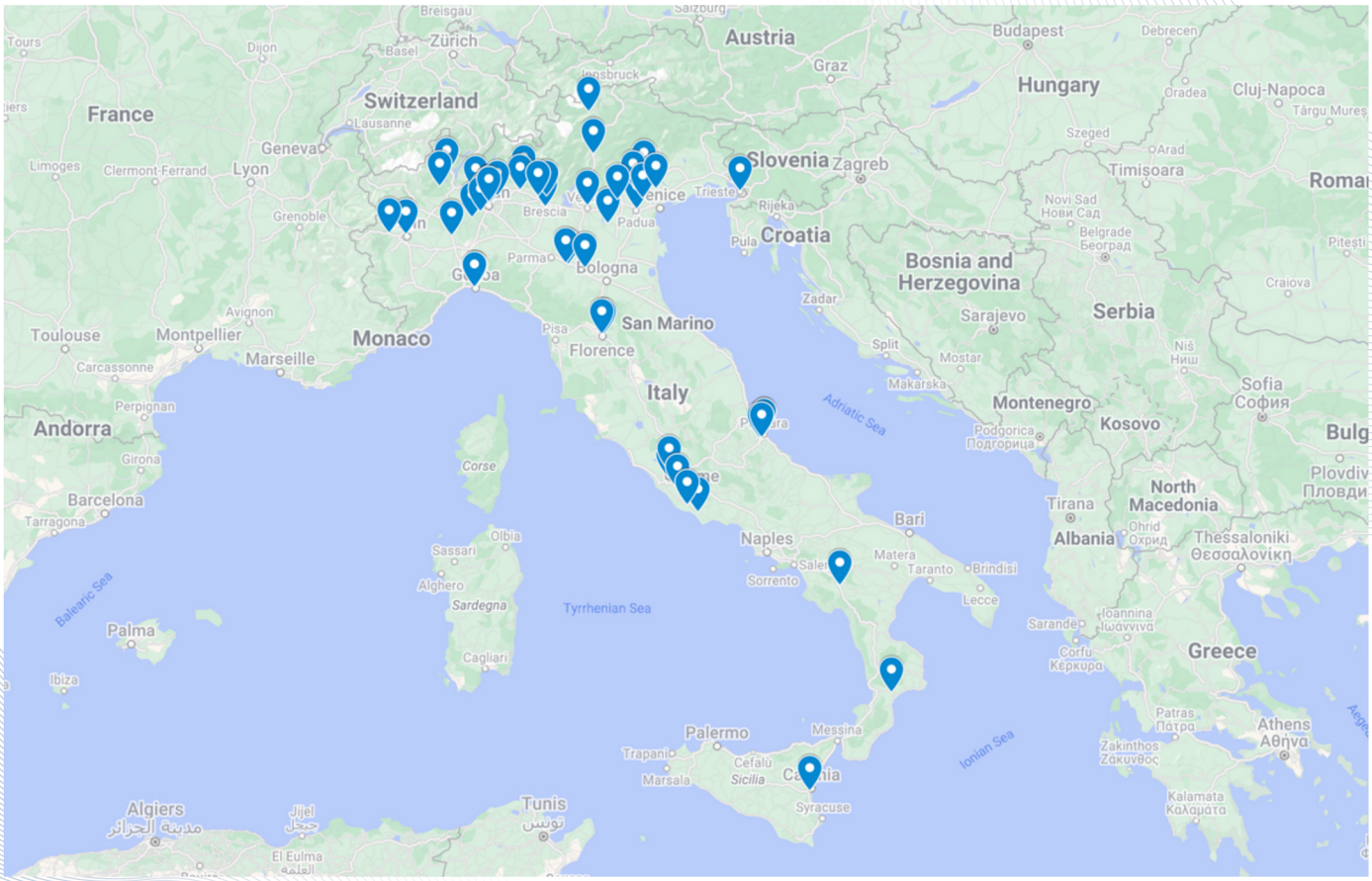


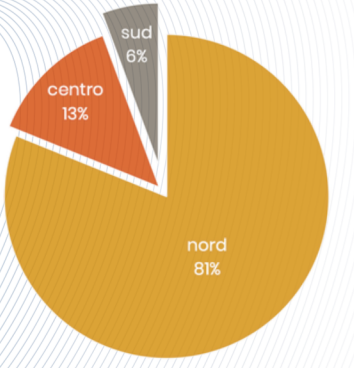
diversificazione per settori lavorativi (fonte Ransomfeed)

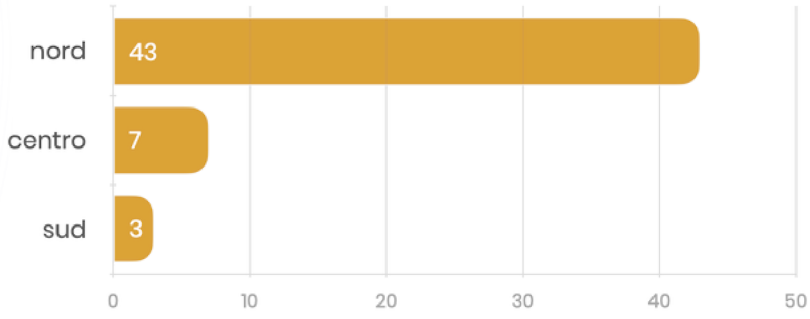
• LA DISTRIBUZIONE DEL RANSOMWARE NEL TERRITORIO

Grazie al lavoro di **localizzazione delle vittime**, possiamo disegnare una mappa per definire la **distribuzione geografica** del ransomware in Italia per il quadrimestre di riferimento. Oltre l'**80% delle vittime** si trova nel nord Italia.

Nota: la mappa è consultabile anche online, con la funzione interattiva, cliccando sulla stessa.



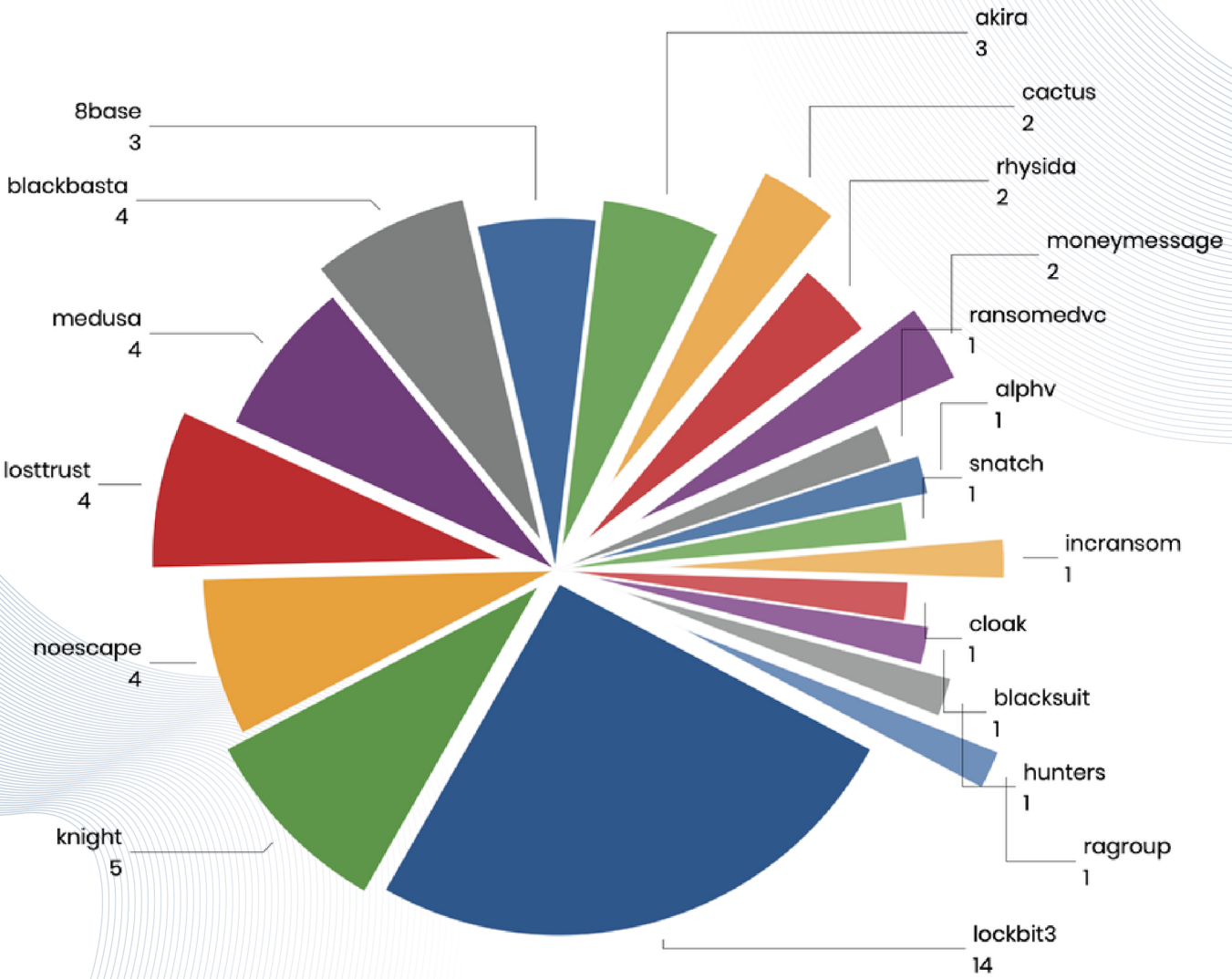




• I GRUPPI CRIMINALI PIÙ ATTIVI

Il gruppo **Lockbit3** si attesta come **il più attivo anche in Italia**, con il 25% degli attacchi registrati nel quadrimestre.

Torna ad essere visibile una **netta distanza** tra l'operato di Lockbit3 e le altre cyber gang, sottolineando un'attività predominante ed una costanza non indifferente.



ADVANCED **DATADRIVEN** CYBERNEWS

IL PROGETTO

Ransomfeed.it è un servizio di **monitoraggio continuo** dei gruppi **ransomware**; utilizzando l'attività di scraping, ovvero l'estrazione di dati da più siti web per mezzo di programmi software e la successiva strutturazione degli stessi, la piattaforma memorizza le rivendicazioni in un feed RSS permanente, disponibile per la libera consultazione.

Il servizio di monitoraggio è **gratuito** e **fruibile da tutti**, raccoglie e analizza costantemente i dati relativi agli attacchi a livello internazionale.

La piattaforma è in grado di rilevare in modo tempestivo gli attacchi, mettendo i **dati a disposizione** di chiunque desideri comprendere l'entità e l'evoluzione degli attacchi informatici.

Il progetto è **libero da vincoli economici**, **non legato a sponsor** o a sostenitori di alcun tipo; l'apporto dello staff **non è retribuito** in alcun modo.

Le **aziende** che desiderano avere un **report personalizzato**, con analisi dei pattern e statistiche rilevanti per settore di attività, possono richiedere una consulenza privata.

Per saperne di più: **ransomfeed.it**


ransomfeed
ADVANCED DATADRIVEN CYBERNEWS
GRAZIE
RANSOMFEED | RANSOMFEED.IT | AN ITALIAN PROJECT