ADVANCED **DATADRIVEN** CYBERNEWS

REPORT Q1 2024

ransomfeed.it | grep_13.06.2024_02

INDICE

Il fenomeno del ransomware sta impattando su documenti personali e sensibili di centinaia di migliaia di cittadini. Non si possono più ignorare queste attività malevole.

Dario Fadda

Il progetto Ransomfeed

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**.

L'intero servizio di monitoraggio è **gratuito e di libera consultazione**, raccoglie e analizza costantemente i dati relativi agli attacchi a livello internazionale.

La piattaforma è in grado di rilevare in modo efficace e tempestivo tutte le rivendicazioni pubblicate dai gruppi, mettendo i dati a disposizione di chiunque desideri comprendere l'entità e l'evoluzione degli attacchi informatici.

Introduzione al report

Il presente report si propone di fornire un **approfondimento dettagliato** sul panorama delle minacce **ransomware** durante il primo quadrimestre del 2024, con un particolare focus sulle attività di monitoraggio condotte dalla piattaforma OSINT Ransomfeed.

Durante questo periodo, sono stati monitorati **204 gruppi criminali** operanti in tutto il mondo, con un costante tracciamento di **404 server** impiegati per condurre attività di **ransomware**. I dati raccolti hanno evidenziato un totale di **1419 rivendicazioni**, di cui **39 registrate in Italia**.

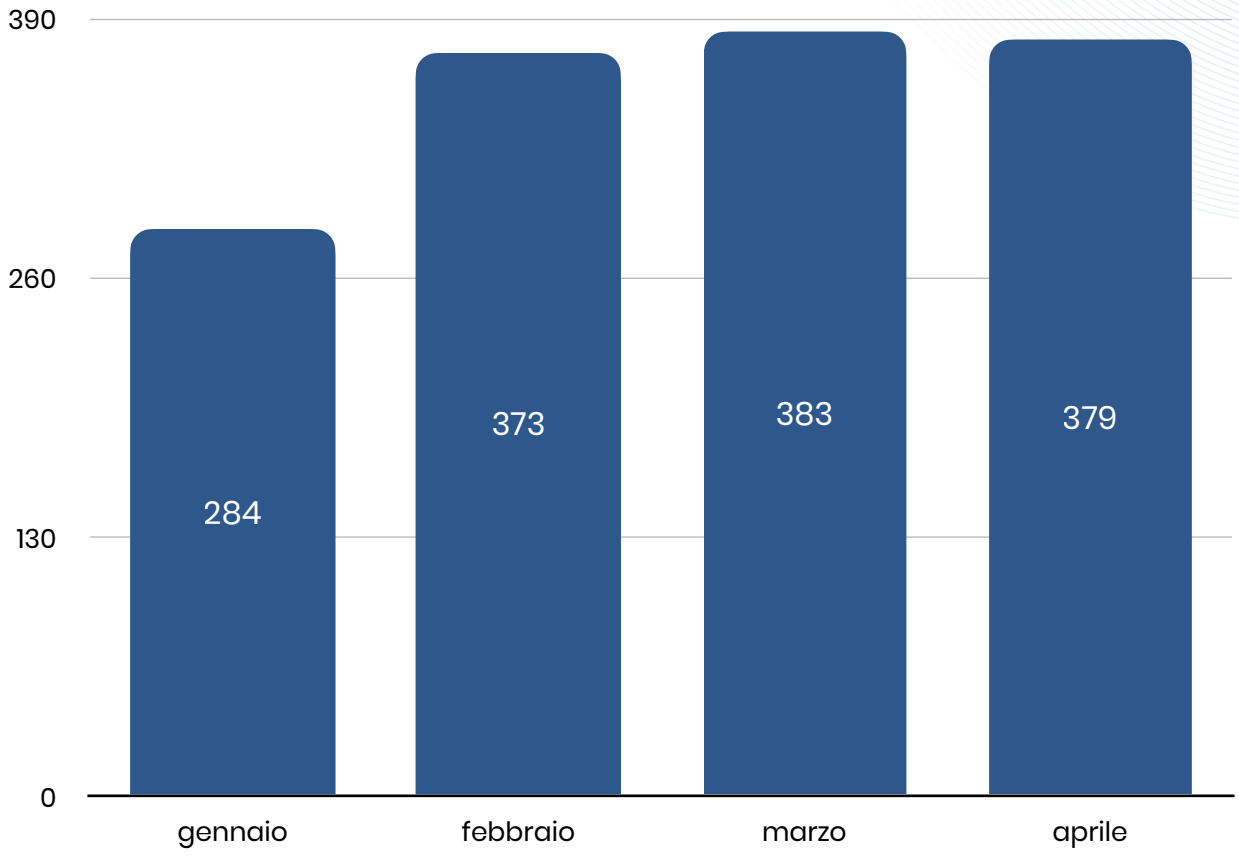
Questo report esaminerà attentamente la localizzazione geografica di tali attacchi, nonché il settore lavorativo maggiormente impattato. Inoltre, verrà dedicata un'attenzione speciale verso gli attacchi ransomware che hanno colpito l'Italia, al fine di comprendere le **sfide specifiche che il paese ha affrontato** durante questo periodo critico in materia di sicurezza informatica.

Panoramica

Tutti i dati presenti in questo report sono stati ottenuti tramite la primaria attività della piattaforma **Ransomfeed** di **scraping periodico** da vari siti noti del *dark web.* Per questo rapporto, ci concentreremo sui risultati raccolti relativamente al **primo quadrimestre 2024**, cominciando con una panoramica a livello globale seguita da un focus sull'Italia.

Per fare questo, la piattaforma nel Q1 2024 ha monitorato **204 gruppi** criminali operanti con tecnologie **ransomware**, in oltre **404 server** e mirrors; totalizzando così una definizione di **1419 rivendicazioni** identificate a livello mondiale.

I mesi di gennaio, febbraio, marzo e aprile hanno tutti presentato sfide uniche nel campo della cybersecurity. Il mese di **marzo è stato il più prolifico** del quadrimestre con **383 attacchi**, seguito da **aprile con 379**, **febbraio con 373** e **gennaio con 284**. Come si può notare il passare dei mesi rispetto all'inizio dell'anno, sono in crescendo.

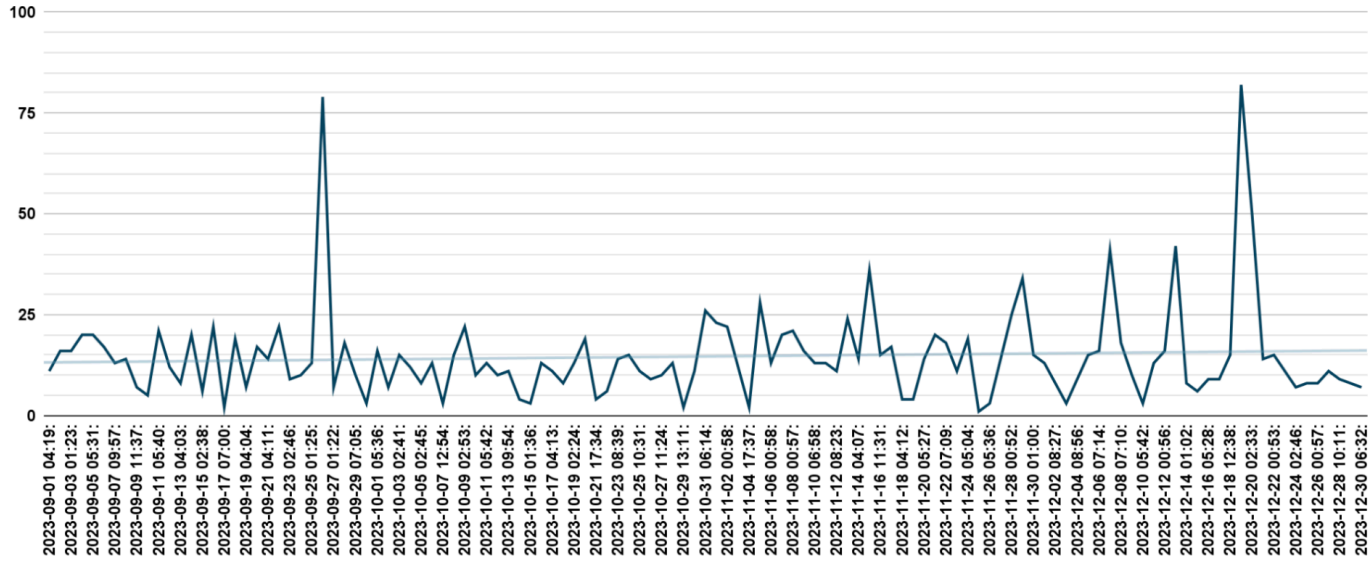


attacchi suddivisi per mese, fonte Ransomfeed.it

Il **27 marzo** è stato il **giorno più ricco** del quadrimestre con ben **49 attacchi** ransomware rivendicati, mettendo in luce la determinazione e l'abilità dei *threat actors* nello sfruttare le vulnerabilità. Questo picco di attività criminale evidenzia l'urgenza di affrontare le carenze nella sicurezza informatica e di rafforzare le difese contro le sempre più crescenti minacce. Al contrario, il **28 gennaio** e il **3 febbraio** hanno segnato i **giorni meno rilevanti** dei primi quattro mesi dell'anno, con solamente una rivendicazione ciascuno. Questa variazione significativa tra i giorni di massimo e minimo attacco indica che, sebbene gli attacchi possano essere concentrati in determinati periodi, il rischio è costante e imprevedibile.

La **media giornaliera** di attacchi **supera gli 11.7 al giorno**, un dato allarmante che richiede una seria riflessione in merito alle misure di sicurezza adottate dalle organizzazioni. Il trend crescente non solo mette a rischio **dati sensibili** e risorse finanziarie, ma **mina anche la fiducia** nelle infrastrutture su cui le aziende e i governi fanno affidamento. Le organizzazioni devono quindi adottare un **approccio proattivo** nella gestione della sicurezza informatica, investendo in tecnologie avanzate di rilevamento delle minacce, formazione continua per il personale e piani di risposta rapida agli incidenti.

Inoltre, la **collaborazione** tra settori pubblici e privati diventa essenziale per condividere informazioni e sviluppare strategie efficaci contro i cybercriminali. Solo attraverso un **impegno collettivo** e coordinato sarà possibile **mitigare l'impatto** devastante degli attacchi ransomware e proteggere le infrastrutture critiche su cui si basa la nostra società digitale.



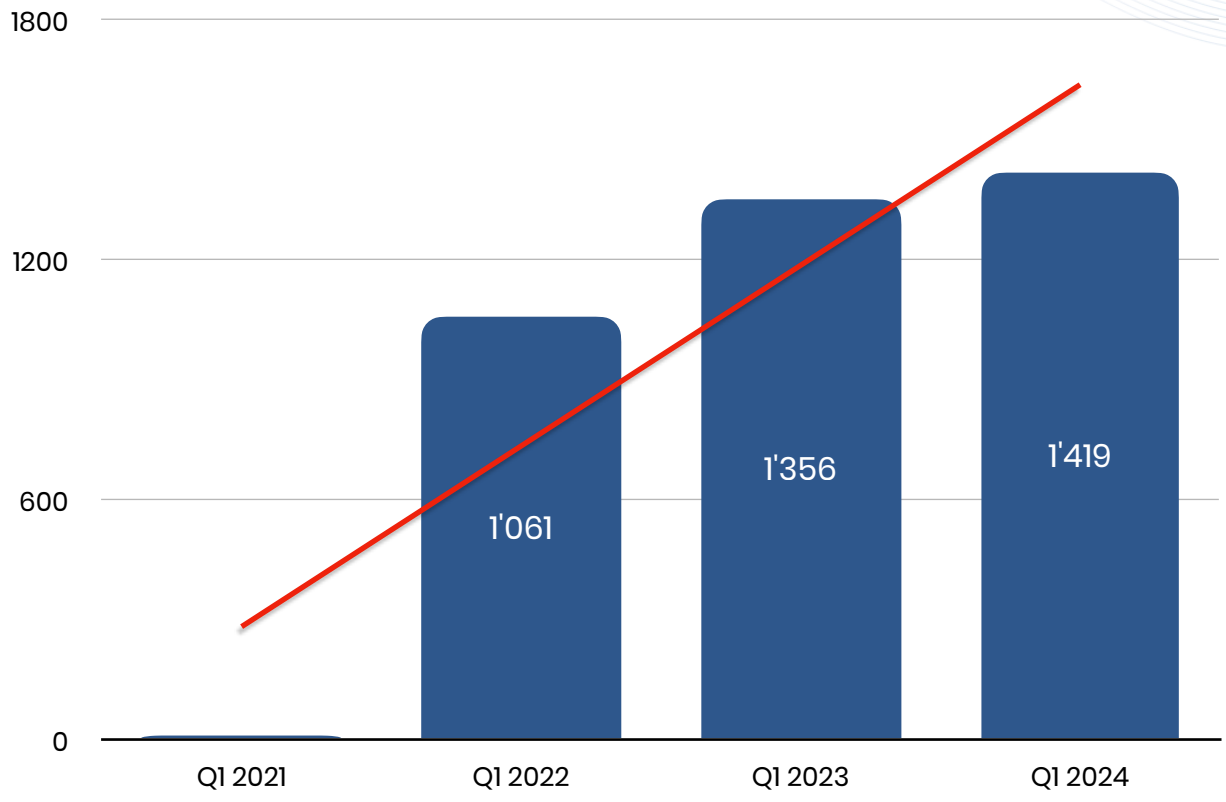
nella linea di fondo si evidenzia il trend complessivo medio, fonte Ransomfeed.it

Quadrimestri a confronto

Come di consueto, al fine di inquadrare in maniera puntuale i dati appena esposti nella Panoramica, abbiamo **confrontato** questo set di dati con quelli di altri primi quadrimestri del passato. Ricordiamo che la piattaforma Ransomfeed è stata inizialmente alimentata con i **dati pregressi fino al 12 gennaio 2020**, siamo tornati indietro nel tempo, interrogando così i primi quattro mesi degli **ultimi tre anni**.

Analizzando i dati storici è possibile **identificare pattern ricorrenti**, **variazioni stagionali** e l'emergere di **nuove tecniche** utilizzate dai cybercriminali. Ad esempio, il confronto con i quadrimestri degli anni precedenti può rivelare se il recente aumento degli attacchi è parte di una crescita costante o se rappresenta un picco anomalo. Questa analisi storica è fondamentale per **contestualizzare i dati attuali** e per prevedere possibili sviluppi futuri.

Come si evince dal grafico, **il trend è in crescita** e ancora non si registra una diminuzione degli attacchi. Rispetto alle analisi di altri quadrimestri fatti durante l'anno, la crescita registrata nei primi quattro mesi dell'anno è abbastanza importante, creando un **trend poco rassicurante**; da notare come l'anno 2023 e l'anno 2024 siano esageratamente **più prolifici** del 2021. In questo arco temporale, infatti, il 2024 attesta un aumento di circa il 5% rispetto all'anno precedente, mentre la **crescita è del 34%** se lo confrontiamo con lo stesso periodo del 2022.



fonte Ransomfeed.it

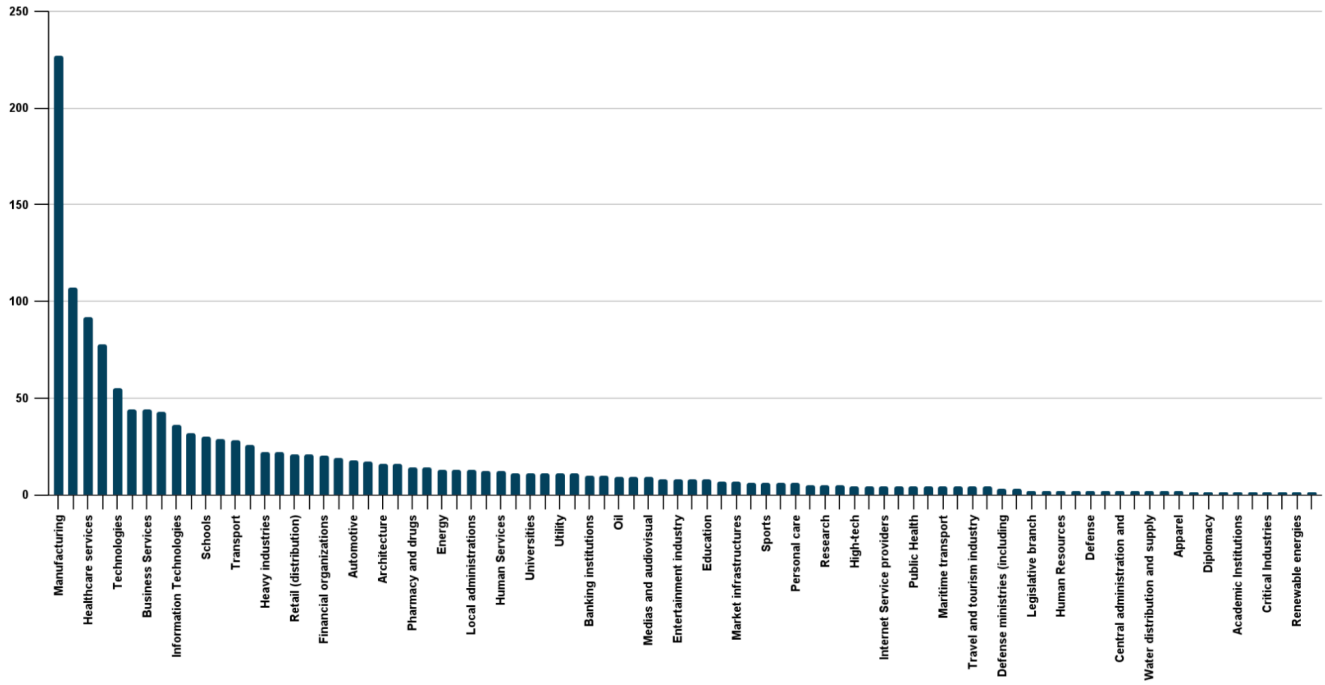
Distribuzione del ransomware nei settori lavorativi

Grazie al processo di **arricchimento dei dati**, risultato di una proficua collaborazione tra il progetto **Ransomfeed** e **Würth Phoenix**, guidato dall'esperto **Massimo Giaimo**, siamo riusciti ad allineare e completare tutti i dati mancanti relativi al settore lavorativo delle vittime coinvolte nelle rivendicazioni. Questa collaborazione ha permesso di fornire statistiche dettagliate sul settore economico delle rivendicazioni presenti sulla nostra piattaforma.

Forti di questo miglioramento nella qualità dei dati, possiamo presentare statistiche di categoria in modo **più preciso e dettagliato**. Inoltre, l'approfondita analisi per settore economico consente di comprendere meglio **quali ambiti siano maggiormente impattati**, e, di conseguenza, capire quali misure di sicurezza potrebbero essere poste in essere per prevenire e/o mitigare le minacce - tenendo sempre in alta considerazione una politica di Zero Trust, di Awareness & Training e, in prima linea, il rispetto di tutte quelle norme di aggiornamento delle macchine.

Nelle prime cinque posizioni del podio (a rappresentare il **60% del totale** attacchi):

- 💼 settore **consulenza/servizi**
- 🔌 settore **produzione**
- 😁 settore **sanitario**
- 🖥️ settore **tecnologico**
- 🏗️ settore **edile**



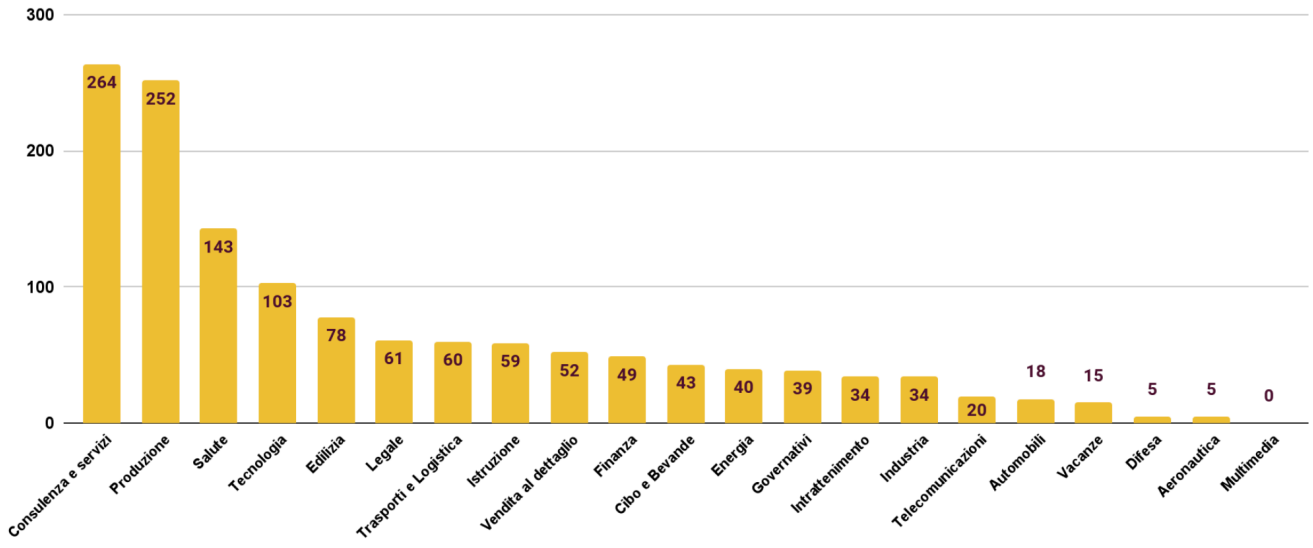
fonte Ransomfeed.it

Per quanto riguarda le categorie che hanno un impatto sulla sicurezza nazionale, le **organizzazioni governative** si trovano in tredicesima posizione, **con 39 attacchi** rivendicati nel periodo. Inoltre, il **settore dell'istruzione**, che può avere implicazioni significative sulla sicurezza nazionale, è in ottava posizione **con 59 rivendicazioni.** Questo dato sottolinea come i cybercriminali continuino a **mirare a settori chiave**, cercando di sfruttare le vulnerabilità in aree critiche per la società.

È importante notare che il settore dell'educazione, le organizzazioni governative e le aziende che si occupano di **servizi terziari** sono tra i **bersagli preferiti** dei criminali informatici. Questi settori, infatti, offrono molteplici possibilità di ramificare le azioni criminali, grazie alla loro ampia rete di connessioni e alla centralità nel tessuto socio-economico.

Le **istituzioni educative**, ad esempio, gestiscono una grande quantità di dati sensibili relativi a studenti, personale e ricerca accademica. Un attacco ransomware in questo settore non solo può compromettere queste informazioni, ma anche **interrompere le attività didattiche** e di ricerca, causando disagi significativi. Se poi consideriamo come target altamente interessante le **scuole interdisciplinari internazionali**, dove i figli dei dirigenti portano a compimento più cicli formativi, è facile comprendere quanto sia maggiore l'appetibilità delle loro infrastrutture IT - spesso non all'altezza di minacce così sofisticate.

Le **organizzazioni governative**, d'altro canto, rappresentano un **obiettivo critico** a causa delle informazioni strategiche trattate, inclusi dati personali dei cittadini, informazioni finanziarie e dati relativi alla **sicurezza nazionale**. Un attacco a queste entità può avere **conseguenze devastanti,** influenzando la fiducia pubblica e la stabilità operativa del governo.



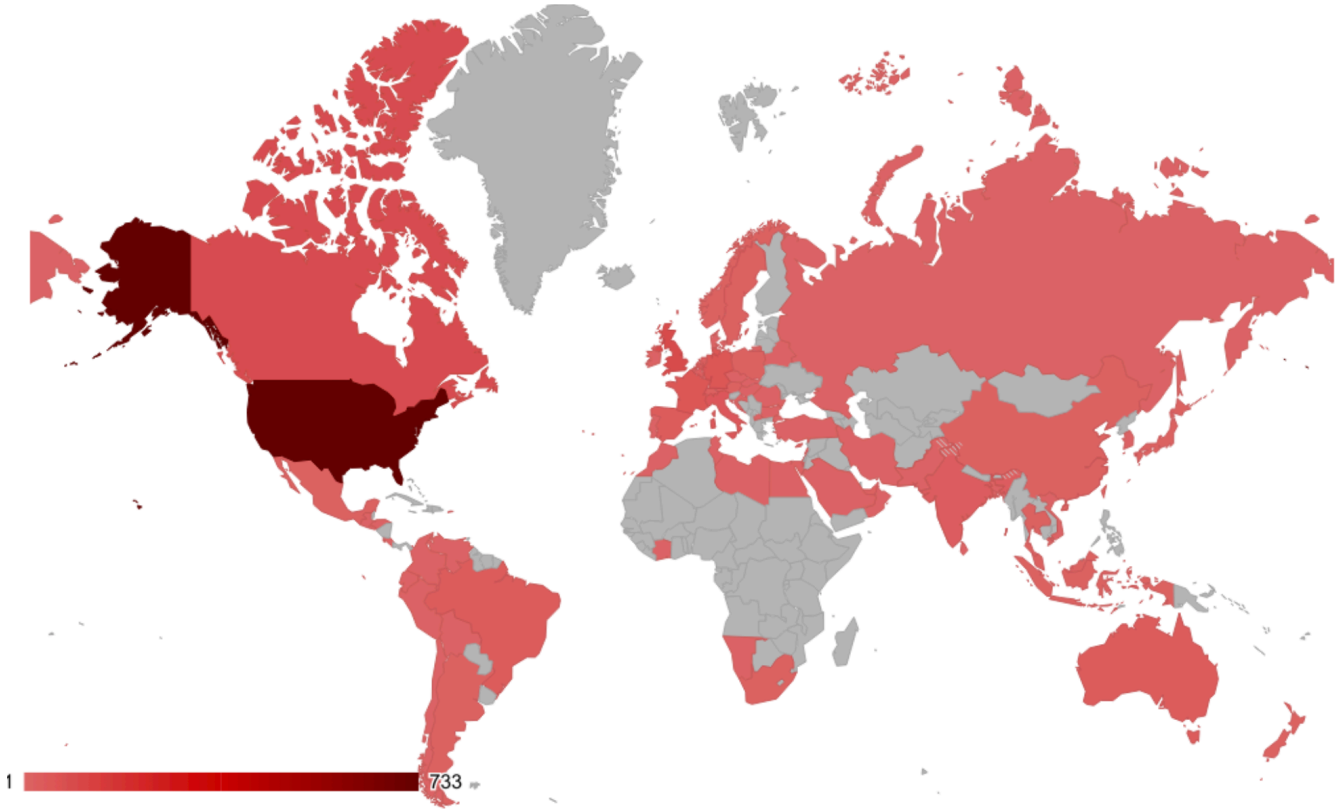
fonte Ransomfeed.it

Distribuzione del ransomware nel mondo

Il continuo e accurato lavoro di OSINT sulla piattaforma, eseguito come **azione successiva allo scraping dei dati**, consente ogni quadrimestre di ottenere una visione completa della **geografia degli attacchi** informatici basandosi sulle loro rivendicazioni.

Anche in questo quadrimestre, come nel primo e nel secondo del 2023, la **regione nord-occidentale del mondo** risulta essere la più gravemente colpita dai gruppi criminali.

La figura che segue illustra chiaramente gli effetti di questa rappresentazione geografica su mappa.



nelle gradazioni di rosso gli stati con vittime, fonte Ransomfeed.it

Se ci focalizziamo sulle differenze rispetto al primo quadrimestre del 2023, la distribuzione geografica degli attacchi rimane **decisamente simile e in linea** con i dati precedenti.

Tuttavia, emerge una novità significativa: **l'intera area russa** ha registrato 18 rivendicazioni di attacchi ransomware, un dato che non era presente nel quadrimestre precedente. Questo cambiamento indica una **intensificazione delle attività** cyber criminali in quella regione; in parte dovute al conflitto russo-ucraino ancora in corso, in parte allo schieramento "per aggregazione" di gruppi ransomware minori e/o emergenti.

Seguono in classifica, nell'ordine, il **Regno Unito**, il **Canada** e la **Germania**, che occupano le maggiori posizioni per numero di attacchi.

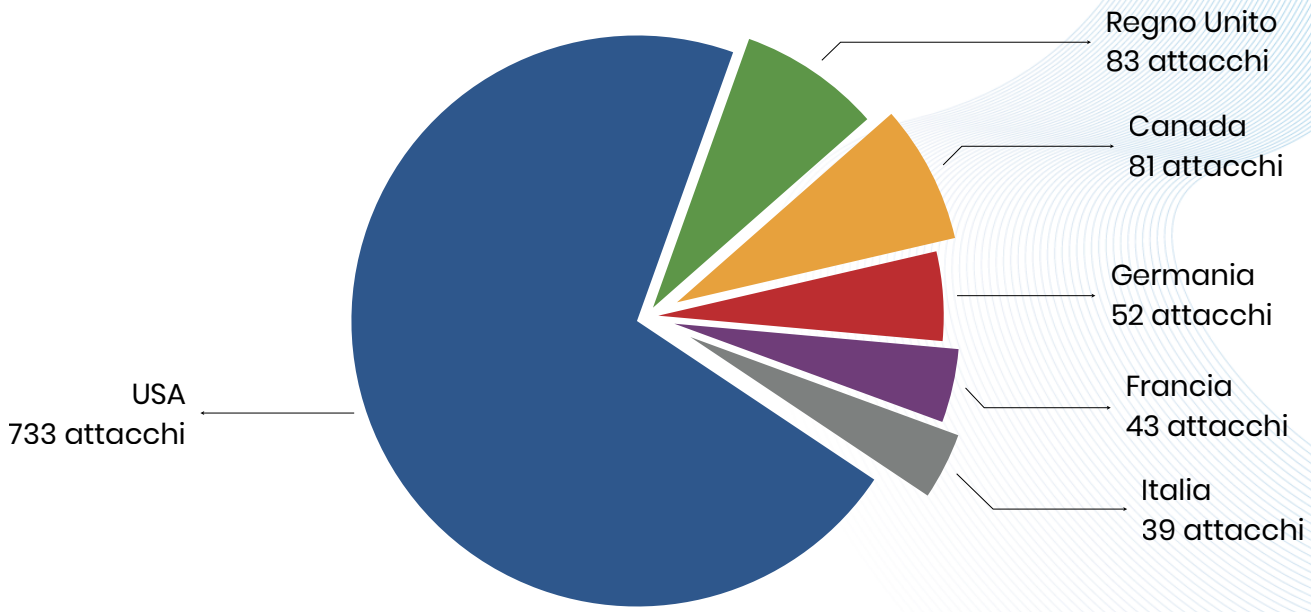
Questi paesi, come gli Stati Uniti, ospitano numerose attività economiche di rilievo e infrastrutture tecnologiche avanzate, rendendoli obiettivi privilegiati per gli attacchi ransomware.

USA, 51.6%	**Singapore**, 0.6%	**Danimarca**, 0.1%	**Lussemburgo**, 0.1%
Regno Unito, 5.8%	**Austria**, 0.6%	**Vietnam**, 0.1%	**Croazia**, 0.1%
Canada, 5.7%	**Tailandia**, 0.6%	**Portogallo**, 0.1%	**Costa d'Avorio**, 0.1%
Germania, 3.7%	**Polonia**, 0.6%	**Tunisia**, 0.1%	**Iran**, 0.1%
Francia, 3.0%	**Nuova Zelanda**, 0.5%	**Libano**, 0.1%	**Russia**, 0.1%
Italia, 2.7%	**Norvegia**, 0.5%	**Slovacchia**, 0.1%	**Macedonia**, 0.1%
Brasile, 2.1%	**Giappone**, 0.5%	**Cile**, 0.1%	**Turchia**, 0.1%
Spagna, 2.0%	**Taiwan**, 0.5%	**Sud Corea**, 0.1%	**Namibia**, 0.1%
Australia, 2.0%	**Cina**, 0.5%	**Rep. Ceca**, 0.1%	**Bulgaria**, 0.1%
India, 1.3%	**Argentina**, 0.5%	**Hong Kong**, 0.1%	**Bangladesh** 0.1%
Svizzera, 1.2%	**Irlanda**, 0.4%	**Pakistan**, 0.1%	**Honduras**, 0.1%
Olanda, 1.2%	**Romania**, 0.4%	**El Salvador**, 0.1%	**Bermuda**, 0.1%
Svezia, 1.1%	**Arabia Saudita**, 0.4%	**Ungheria**, 0.1%	**Seychelles**, 0.1%
Belgio, 1.0%	**Israele**, 0.4%	**Costa Rica**, 0.1%	**Palau**, 0.1%
Messico, 0.9%	**Colombia**, 0.4%	**Barbados**, 0.1%	**Oman**, 0.1%
Emirati Arabi, 0.8%	**Perù**, 0.3%	**Venezuela**, 0.1%	**Sri Lanka**, 0.1%
Malesia, 0.6%	**Egitto**, 0.3%	**Cipro**, 0.1%	**Portorico**, 0.1%
Sud Africa, 0.6%	**Non Disponibile**, 0.3%	**Bolivia**, 0.1%	**Marocco**, 0.1%
Indonesia, 0.6%	**Ecuador**, 0.2%	**Guatemala**, 0.1%	**Libia**, 0.1%

fonte Ransomfeed.it

In sintesi, la distribuzione geografica degli attacchi mantiene una certa continuità rispetto al passato.

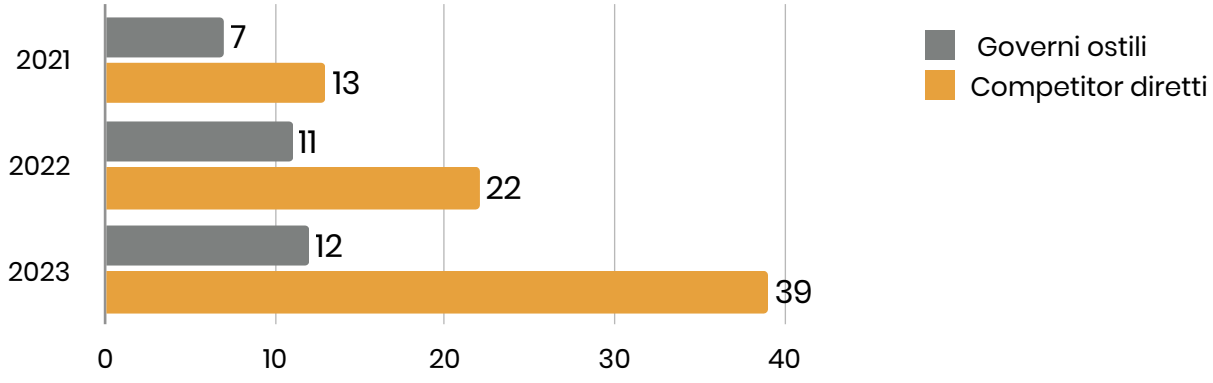
L'**Italia**, nel primo quadrimestre del 2024, si attesta in **sesta posizione con 39 attacchi**. Questo dato segnala un **incremento** rispetto ai periodi precedente.



fonte Ransomfeed.it

L'Impatto degli attacchi ransomware sulle **economie dei paesi coinvolti** è spesso devastante, con un dispendio di risorse non indifferente, sia a livello economico che di personale.

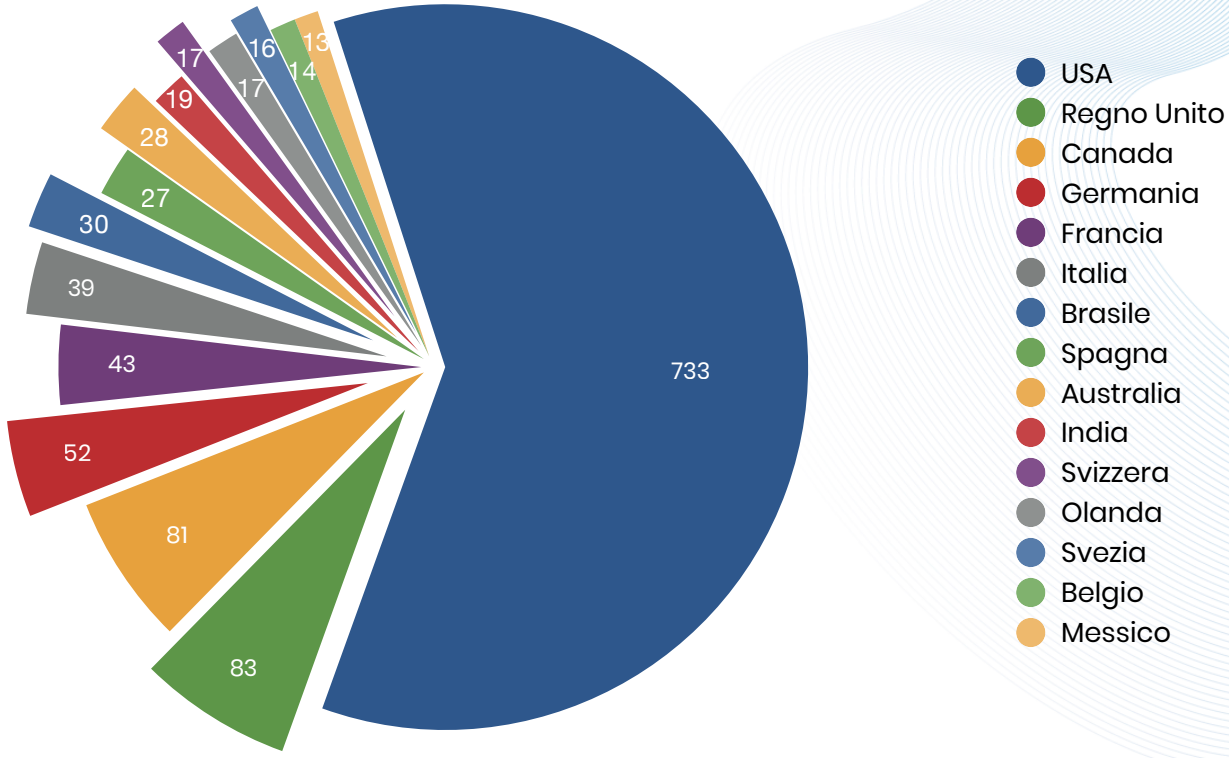
Fermare la produttività per giorni o settimane, mandare in stallo le operazioni di approvvigionamento e mantenimento delle strutture IT, fino alla perdita di fiducia e di reputazione, sono elementi che fanno molta gola ai concorrenti.
È uno dei motivi per cui i gruppi criminali vengono **assoldati,** da aziende rivali come da governi ostili.



fonti aggregate dal dark web

Top 15

Abbiamo aggregato i dati per visualizzarli **escludendo** i paesi con **meno dell'1% di vittime** ransomware.



fonte Ransomfeed.it

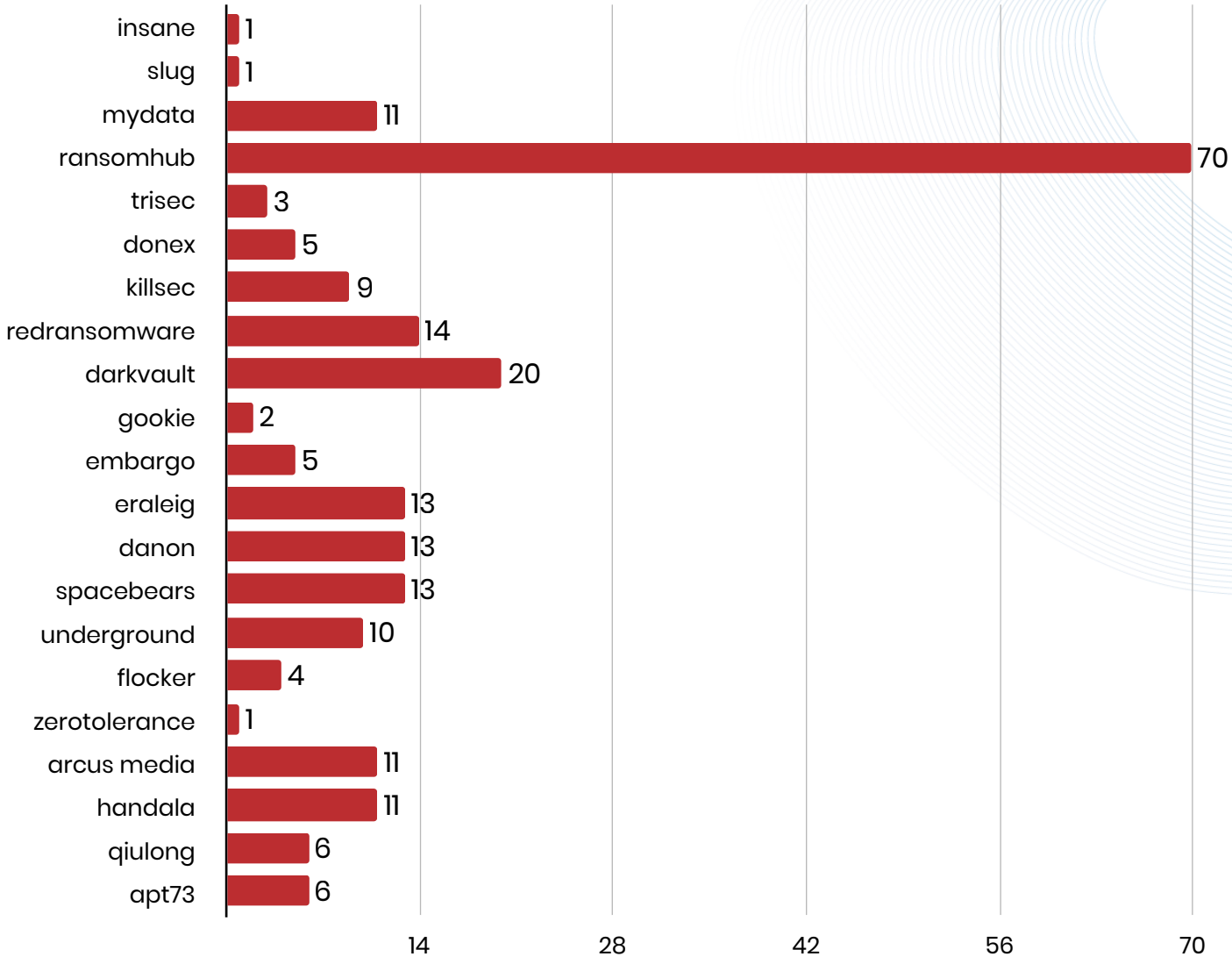
Anche per questo **primo quadrimestre del 2024**, il grafico evidenzia un grande **divario** tra gli Stati Uniti e il resto del mondo, mostrando chiaramente come queste quantità siano suddivise. Gli Stati Uniti, con una quantità significativamente maggiore di attacchi ransomware, emergono come il paese più colpito. Questo riflette, naturalmente, la **maggiore concentrazione di infrastrutture** industriali e aziendali negli USA rispetto ad altri paesi.

La centralità economica e politica degli USA, a livello globale, li rende un bersaglio strategico per gli attacchi ransomware. I criminali sanno che **colpire aziende e istituzioni americane** può avere un impatto su scala mondiale, **destabilizzando** mercati e creando effetti a catena in diverse industrie.

Mentre altri paesi stanno migliorando le loro difese cibernetiche, è lampante che gli Stati Uniti devono continuare a innovare e adattare le loro strategie per rimanere al passo con l'evoluzione delle minacce.

Nuovi gruppi criminali

Nel **primo quadrimestre del 2024**, come spesso accade, sono emersi **nuovi gruppi** criminali che hanno rapidamente guadagnato terreno nella scena. Ransomfeed, sempre attenta alle evoluzioni del panorama delle minacce, ha rilevato e aggiunto questi nuovi threat actors al suo **monitoraggio quotidiano.** Complessivamente, sono stati registrati **226 nuovi attacchi** ransomware rivendicati, distribuiti tra **25 nuovi gruppi criminali**.

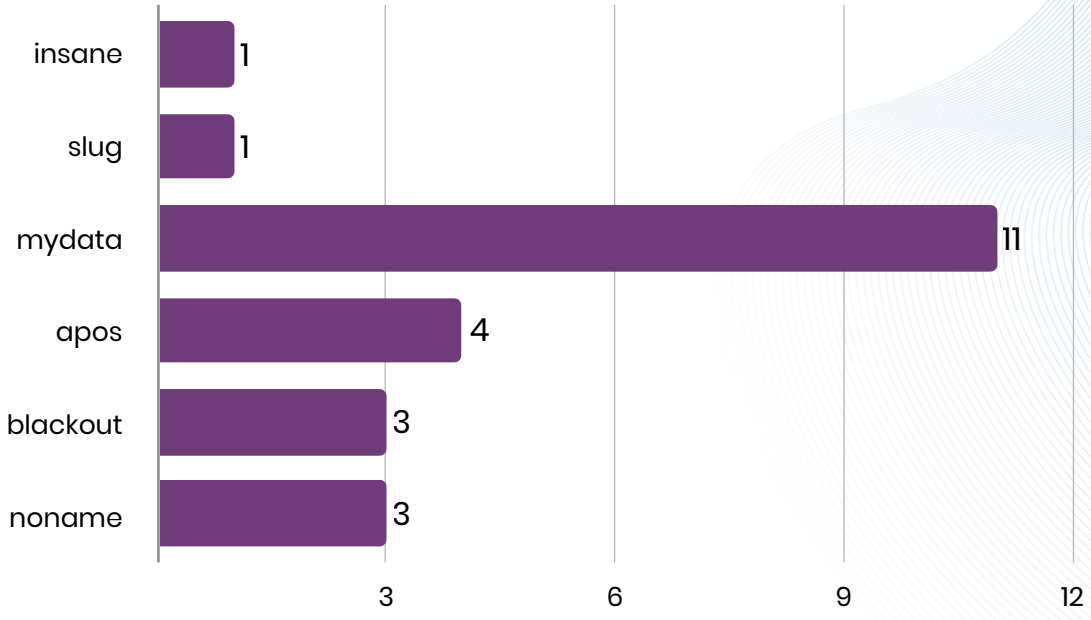


fonte Ransomfeed.it

Per quello che riguarda i gruppi **eraleig** e **apt73**, registriamo la fusione dei due, sotto il solo nome di *apt73*, successivo all'entrata in monitoraggio di entrambi; abbiamo voluto espressamente tenere separati i due gruppi per un miglior conteggio statistico.

Escluso dal monitoraggio è il gruppo *mogilevich*, che non è risultato essere un reale threat actor.

Il proliferare di nuovi gruppi sulla scena ransomware costituisce un problema significativo non solo per aziende e istituzioni, ma anche per l'organizzazione della **scena criminale**.



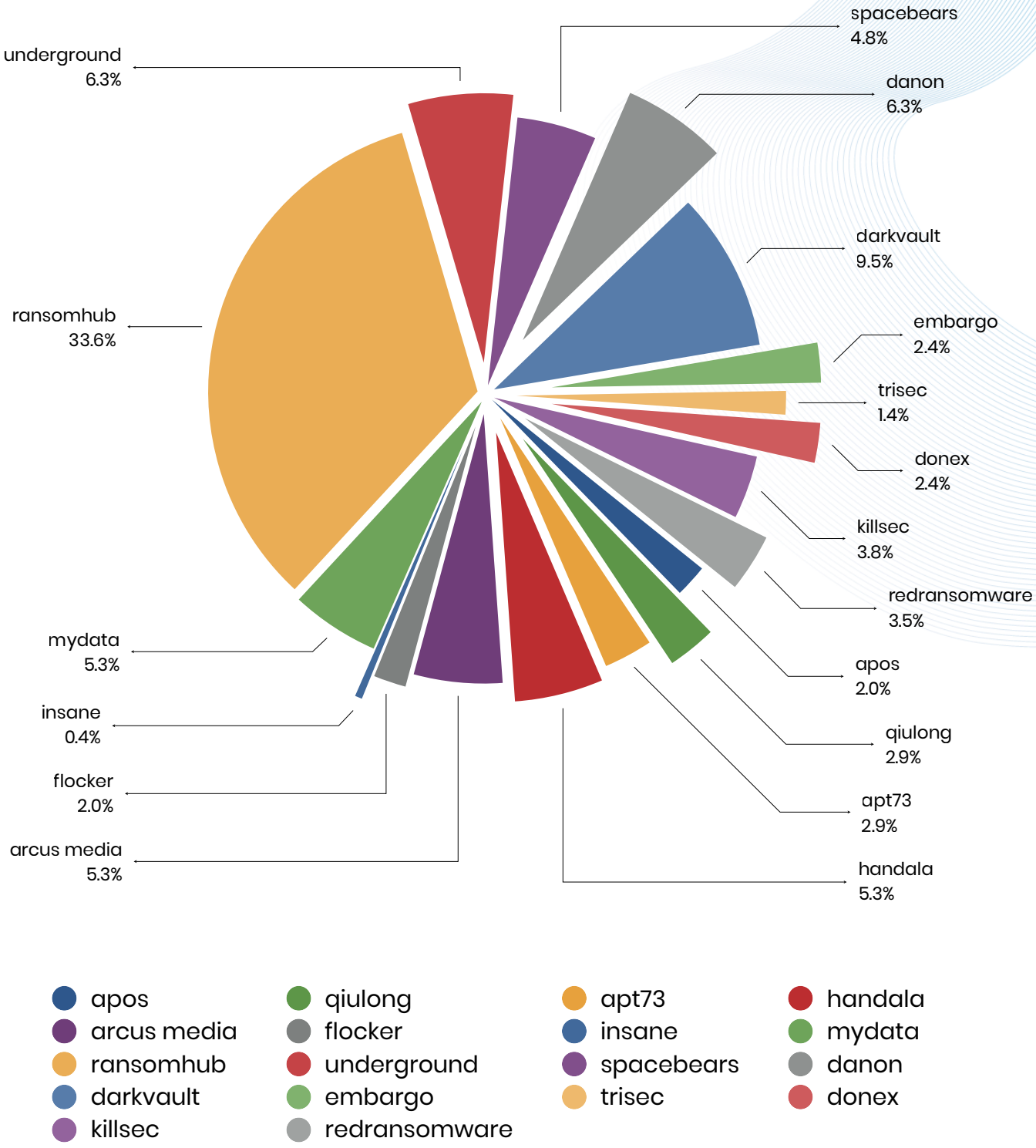
fonte Ransomfeed.it

La tabella sopra riportata evidenzia i gruppi che Ransomfeed ha aggiunto al monitoraggio nell'arco dei **120 giorni del terzo quadrimestre**, perché resi noti proprio nel medesimo periodo.

Ogni gruppo sviluppa le proprie peculiarità, sfruttando risorse interne e, spesso, **affiliandosi** a gruppi più grandi e stabili - per accedere a tecnologie avanzate e infrastrutture che, da soli, non potrebbero permettersi.
Si parla, ad esempio, di investimenti di un gruppo ransomware per **dotarsi di computer quantici**, in grado di elaborare informazioni molto più velocemente e dettagliatamente; si parla anche di grossi investimenti sullo **storage privato** di dati sensibili, piuttosto che affidarsi a servizi terzi di hosting.

Ransomfeed, attraverso il monitoraggio costante, fornisce dati preziosi per comprendere meglio questi nuovi sviluppi e per aiutare le organizzazioni a **prepararsi** e **rispondere** in modo efficace. Identificare e tracciare l'attività di questi nuovi gruppi è fondamentale per anticipare le loro mosse e adottare, ove possibile, misure preventive in grado di mitigare l'impatto dei loro attacchi.

ransomhub risulta essere, a tutti gli effetti, il gruppo con la maggiore attività **nel periodo considerato** (quasi il 34%, nel cluster), con attacchi diversificati a target internazionali, con una predilezione per gli Stati Uniti.



fonte Ransomfeed.it

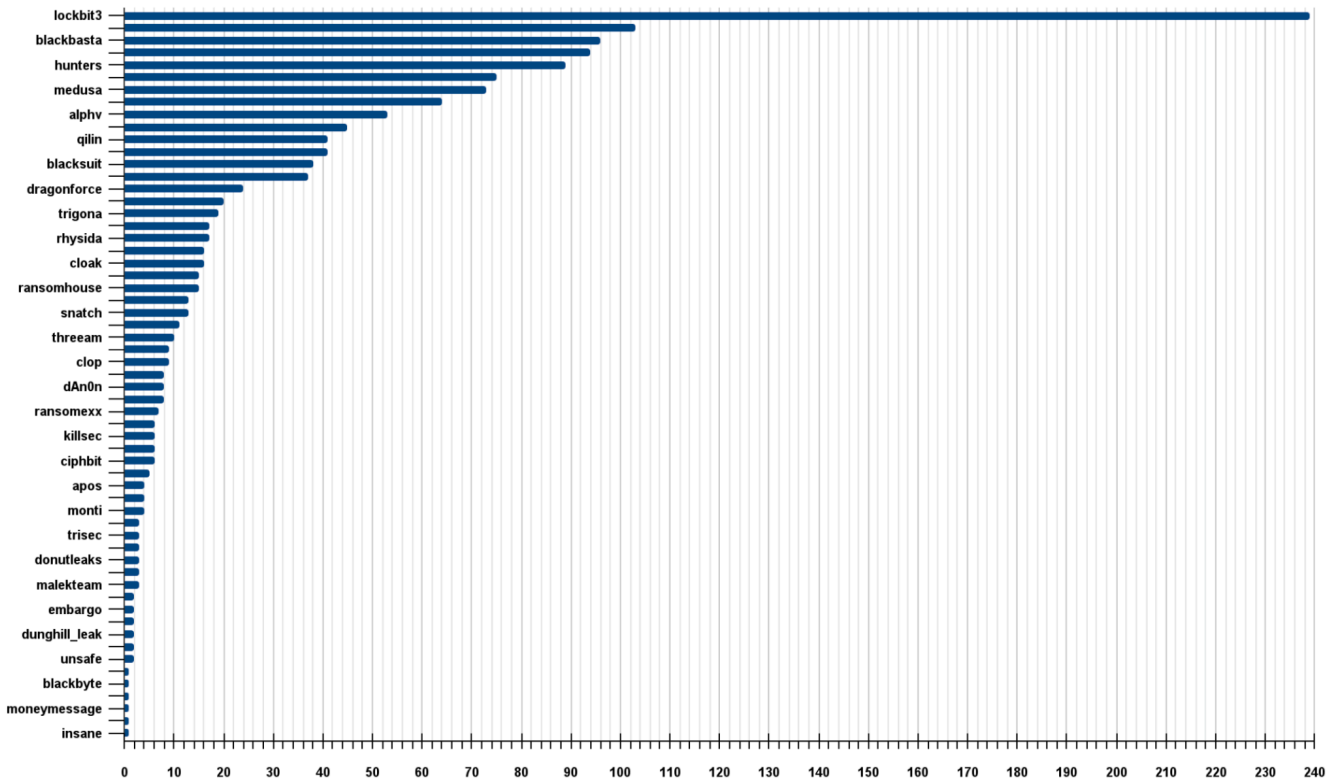
Le attività globali dei gruppi ransomware

Abbiamo isolato i singoli gruppi che hanno generato attività nei primi quattro mesi dell'anno. Tra tutti i gruppi costantemente monitorati, la piattaforma ha rilevato attività durante il quadrimestre per 59 di questi. Gli altri gruppi non menzionati sono risultati **inattivi**, indicando una **temporanea sospensione delle loro operazioni** o una possibile riorganizzazione interna.

Le attività di questi **59 gruppi** hanno messo in luce una leadership assoluta di sei gang estremamente attive, che da sole si sono **spartite il 50% degli attacchi totali** registrati.

- **lockbit3**: leader indiscusso con il **17% degli attacchi**, sebbene in calo rispetto al Q3 2023
- **play**: con il **7.3% degli attacchi**, si posiziona come il secondo gruppo più attivo
- **blackbasta**: responsabile del **6.8% degli attacchi**, al terzo posto
- **8base**: con il **6.6% degli attacchi**, dimostra una notevole attività
- **hunters**: registra al suo attivo il **6.3% degli attacchi**
- **akira**: chiude il gruppo di testa con il **5.3% degli attacchi**

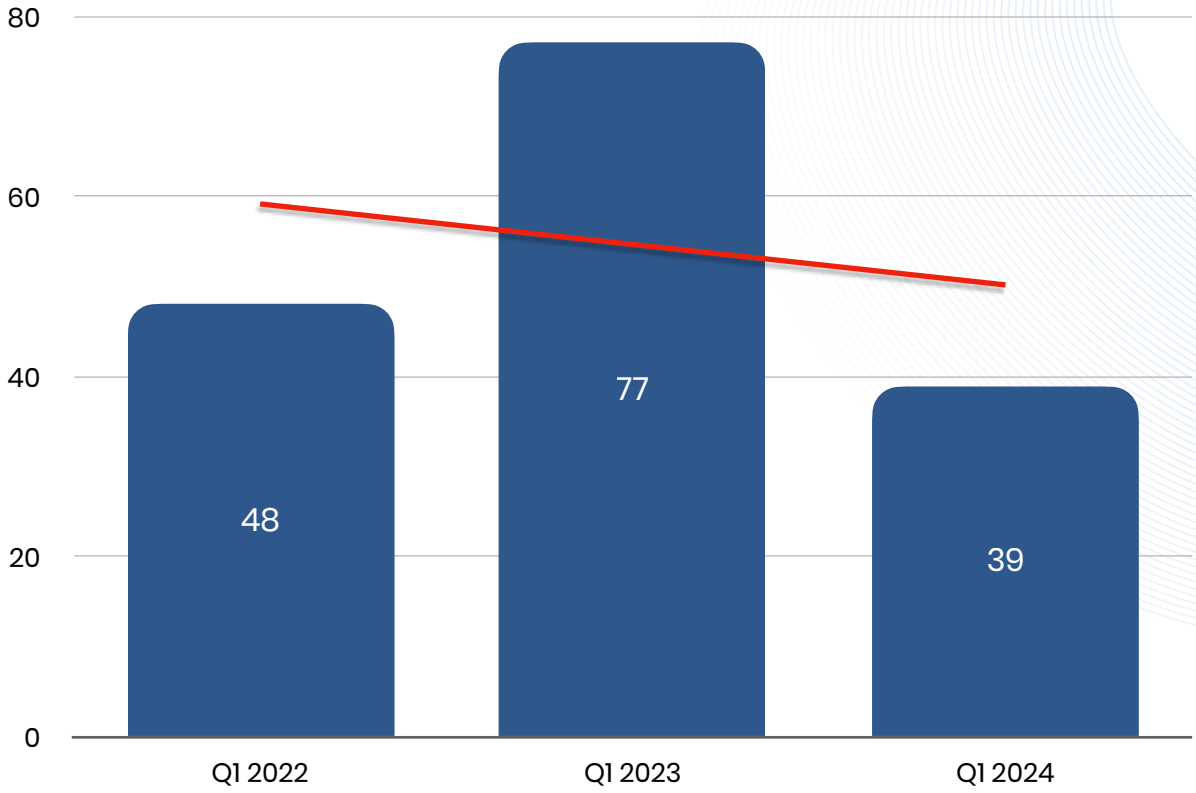
Il grafico mostra il dettaglio di tutte le **cyber gang attive**, con il valore di riferimento attribuito al numero di vittime rivendicate.



fonte Ransomfeed.it

Focus Italia

In questa sezione del report analizzeremo i dati dei cluster già presentati a livello globale, concentrandoci in particolare sulla **situazione dell'Italia**. Un primo dato che sicuramente emerge è la **significativa diminuzione** del numero di attacchi ransomware che hanno coinvolto l'Italia nel primo quadrimestre del 2024. Durante questo periodo, sono stati registrati **39 attacchi**, corrispondenti a poco più di **uno ogni tre giorni**.



fonte Ransomfeed.it

Si registra quindi un **calo** rispetto ai quadrimestri precedenti, suggerendo una possibile riduzione delle vulnerabilità sfruttabili o un miglioramento delle misure di sicurezza adottate. Tuttavia, nonostante la diminuzione, **il numero di attacchi rimane rilevante**.

In questo quadrimestre rispetto al Q1 2023 e 2022, il dato vede una **inversione del trend** globale, in diminuzione rispetto allo stesso periodo dell'anno precedente. Bisogna contestualizzare questo dato nella globale diminuzione in questo quadrimestre, rispetto alla fine dell'anno e **rispetto a diverse azioni di polizia internazionale** che hanno sicuramente impattato sui risultati delle rivendicazioni, nei primi mesi dell'anno, per poi recuperare nei mesi seguenti.

Confrontando questi dati con quelli globali, possiamo ottenere una visione più completa del panorama delle minacce ransomware e delle tendenze emergenti; grazie inoltre all'analisi specifica, riusciamo ad estrarre preziose informazioni per comprendere lo stato di salute di aziende e istituzioni, e dell'efficacia delle loro strategie di mitigazione.

Dall'analisi dei settori e dalle tipologie di aziende colpite, emerge chiaramente che le **aziende tecnologiche**, o quelle che operano con tecnologie avanzate, sono particolarmente appetibili per i criminali informatici.

Queste aziende, pur **investendo significativamente** (rispetto alla media dichiarata) in strategie di difesa, rappresentano obiettivi attraenti a causa del **valore dei dati** e della **criticità delle loro operazioni**.

D'altro canto, sono fin troppo spesso colpite anche quelle **aziende che non investono** adeguatamente nella sicurezza delle proprie infrastrutture. Trascurando gli aggiornamenti dei sistemi e le misure di protezione, queste realtà diventano **bersagli facili** per gli attacchi: la mancanza di investimenti in sicurezza **rende vulnerabili**, esponendo tutta la struttura a un maggiore rischio di compromissione e di danni significativi.

In sintesi, si evidenzia una **polarizzazione nel panorama** degli attacchi ransomware: da un lato, **aziende tecnologiche** ben **protette** ma costantemente nel mirino dei criminali, e dall'altro, **aziende meno protette** che non aggiornano i loro sistemi e sono quindi facili prede per i cybercriminali.

Questo sottolinea l'importanza di investire **continuamente** in sicurezza informatica per tutte le aziende, **indipendentemente dal settore** in cui operano.

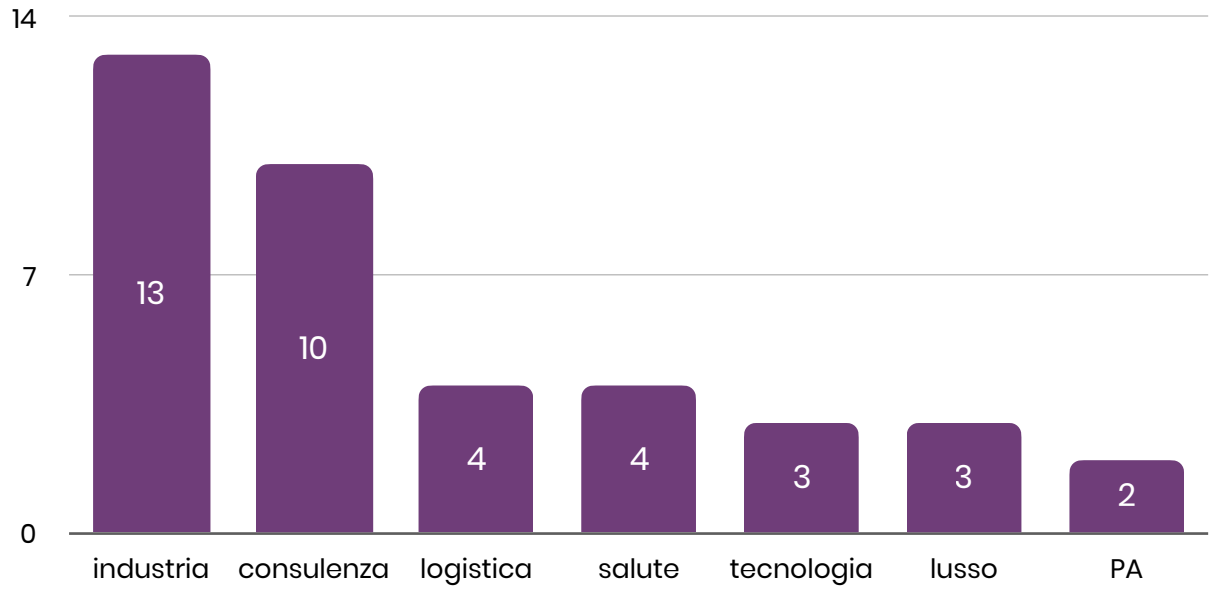
Attività globali dei gruppi ransomware

L'**industria** e la **consulenza** si rivelano essere i settori lavorativi **più colpiti** anche nel focus specifico sull'Italia. Nel primo quadrimestre del 2024, questi settori hanno subito **rispettivamente 13 e 10 attacchi ransomware**. All'interno del settore **industriale**, le industrie **farmaceutiche**, **meccaniche**, **metallurgiche** ed **elettroniche** sono state particolarmente bersagliate. Anche gli **studi professionali**, parte integrante del settore della consulenza, hanno subito numerosi attacchi.

A seguire, i settori della **logistica**, della **salute**, della **tecnologia** e del **lusso**; tutti hanno registrato un numero significativo di attacchi. È chiaro che questi siano i settori più bersagliati a causa dell'elevato valore dei dati che gestiscono e della criticità delle loro operazioni, che li rende molto vulnerabili alle richieste di riscatto.

- 🏭 industria, 33.3%
- 💼 consulenza, 17.9%
- 🚚 logistica, 7.7%
- 😁 salute, 10.3%
- 🖥️ tecnologia, 7.7%
- 💍 lusso, 3.0%
- 🏢 pubblica amministrazione, 5.1%

Il settore della **Pubblica Amministrazione**, pur avendo subito **solo 2 attacchi** ransomware nel Q1 2024, mostra un impatto considerevole. Il segmento principalmente colpito è stato il settore della **sanità pubblica**, tuttavia, il numero di aziende private colpite che operano come fornitori o partner della PA è di gran lunga superiore.



fonte Ransomfeed.it

La distribuzione del ransomware nel territorio

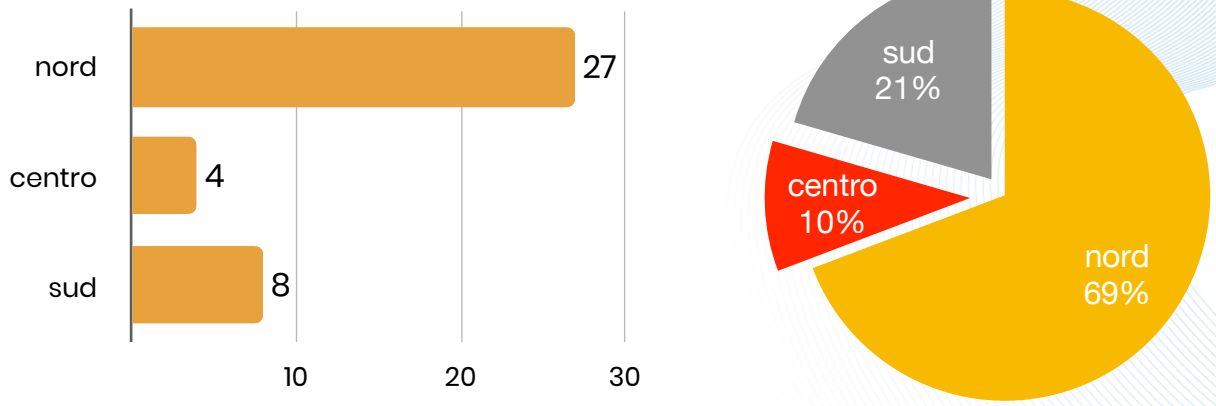
Grazie ai dati sulla **localizzazione** delle vittime raccolti su Ransomfeed, siamo stati in grado di creare una mappa che illustra la **distribuzione geografica degli attacchi** ransomware in Italia per il primo quadrimestre del 2024. La mappa, consultabile anche online con **funzioni interattive**, è disponibile a questo indirizzo o cliccando direttamente sulla stessa.

fonte Ransomfeed.it

Come osservato anche in precedenza, l'attenzione degli attacchi ransomware è spesso rivolta **principalmente al nord Italia**, un dato che si conferma costante nel tempo. Anche in questo quadrimestre, oltre l'**80% delle rivendicazioni** riguarda organizzazioni ed enti situati in quest'area.

L'alta concentrazione di attacchi nel nord Italia può essere attribuita alla presenza di **numerose aziende tecnologiche**, **industriali** e di **consulenza**, che rappresentano bersagli ricchi e spesso vulnerabili.

Suddividendo la mappa in **macro aree geografiche**, otteniamo una rappresentazione sinottica della distribuzione degli attacchi ransomware. Il grafico seguente illustra questa suddivisione, evidenziando le **differenze di impatto tra le varie regioni italiane**.



fonte Ransomfeed.it

Nel **nord Italia** si trova la più alta concentrazione di aziende industriali e manifatturiere del paese; ha una omogenea presenza di piccole e medie imprese che operano in settori quali meccanica, metallurgia, chimica, automotive e tecnologia.

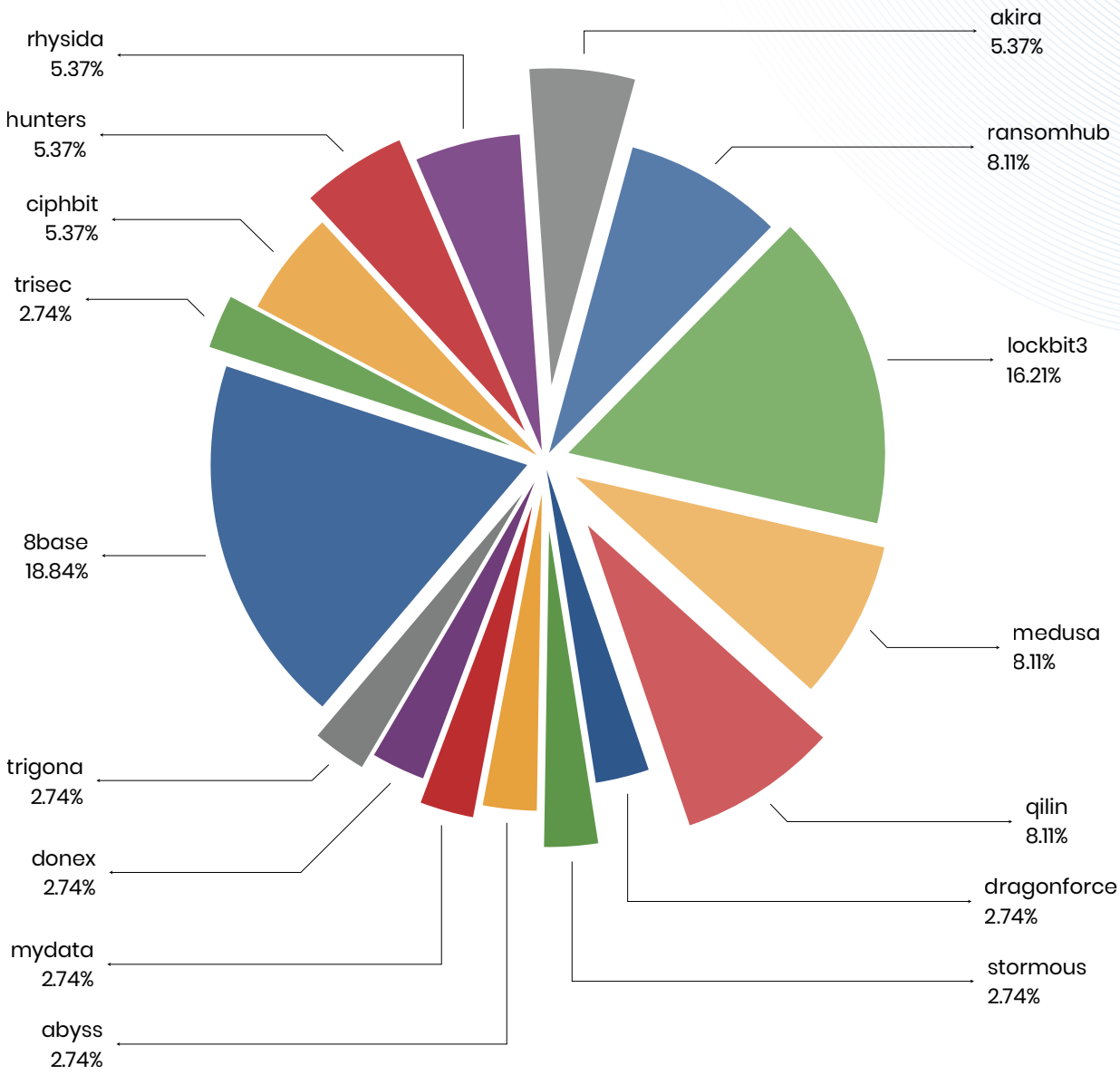
Rispetto al sud Italia, dove la **densità industriale è minore** e l'economia è per lo più basata su agricoltura, pesca, turismo e industria leggera, il nord ha una lunga tradizione di sviluppo economico, infrastrutture avanzate e una rete di trasporti molto sviluppata.
L'innovazione tecnologica ha delle lacune, sia imprenditoriali che sociali, con un minore afflusso di investimenti a buon fine; questi fattori rendono le **aziende del nord più appetibili**, grazie anche alla fitta rete di connessioni di cui possono vantare.

I gruppi criminali più attivi

Anche per il Q1 2024, il dato mondiale si riflette anche nell'analisi delle cyber gang che hanno condotto e rivendicato gli attacchi sul territorio nazionale, mostrando **tendenze più o meno in linea con i dati globali.** In effetti, il gruppo **8base** si è affermato come il **più attivo in Italia** durante questo periodo, con il **18% degli attacchi totali**.

8base e **lockbit3** mostrano una predominanza chiara nelle attività ransomware in Italia, evidenziando una maggiore efficienza e capacità organizzativa, nonostante i problemi giudiziari dei secondi.

Entrambi i gruppi sono noti per l'uso di tattiche avanzate, che includono il ricorso a exploit 0day, attacchi di phishing mirati e l'adozione di infrastrutture di comando e controllo (C2) difficili da rilevare e neutralizzare senza un'adeguata conoscenza dell'ecosistema.



fonte Ransomfeed.it

Conclusione

Complessivamente, sono stati **monitorati 204 gruppi** criminali operanti a livello globale, con **1419 rivendicazioni ransomware**, di cui **39 in Italia**.

In sintesi:

- **sei gruppi criminali attivi** hanno rappresentato il **50% degli attacchi**, con lockbit3 in testa, con il **17% del totale**;
- rispetto al Q1 2023 e Q1 2022, si è registrata una **diminuzione** globale degli attacchi ransomware;
- i settori più colpiti sono stati **l'industria** e la **consulenza**, con l'industria farmaceutica, meccanica, metallurgica ed elettronica tra i bersagli principali;
- in Italia, si è notata una **significativa diminuzione degli attacchi** nel Q1 2024, con 39 rivendicazioni registrate;
- i settori consulenza/servizi, produzione, salute, tecnologia ed edilizia hanno rappresentato il **60% del mercato ransomware** a livello globale;
- le **organizzazioni governative** si sono posizionate al **13° posto** per attacchi rivendicati, mentre il settore dell'istruzione è all'ottavo posto con 59 rivendicazioni.

La crescita continua degli attacchi ransomware a livello globale e nazionale è inequivocabile; tuttavia, nonostante la **crescente frequenza e sofisticazione degli attacchi**, emerge un quadro preoccupante: la consapevolezza delle minacce cibernetiche rimane spesso **insufficiente**, sia tra le aziende che tra le istituzioni pubbliche. Questo **gap di consapevolezza** si traduce in una risposta inadeguata e in ritardi nell'adozione di misure di sicurezza efficaci.

I dati presentati nel nostro report sottolineano come settori chiave dell'economia, continuino ad essere **bersagli privilegiati** dai cybercriminali. Nonostante l'evidenza della minaccia, gli investimenti in ambito cybersecurity sono ancora **scarsi**. Molte aziende, infatti, **non destinano risorse sufficienti** per aggiornare e proteggere le loro infrastrutture, esponendosi così a rischi significativi.

È fondamentale attuare un **approccio proattivo alla sicurezza**. Ciò include non solo l'implementazione di tecnologie avanzate per il rilevamento e la difesa, ma anche l'investimento in **formazione e sensibilizzazione del personale**. La cybersecurity non deve essere vista come un costo, ma come un **investimento indispensabile** per la protezione delle informazioni e la continuità operativa.

fonte Ransomfeed.it

ransomfeed

ADVANCED **DATADRIVEN** CYBERNEWS

thank you ;)