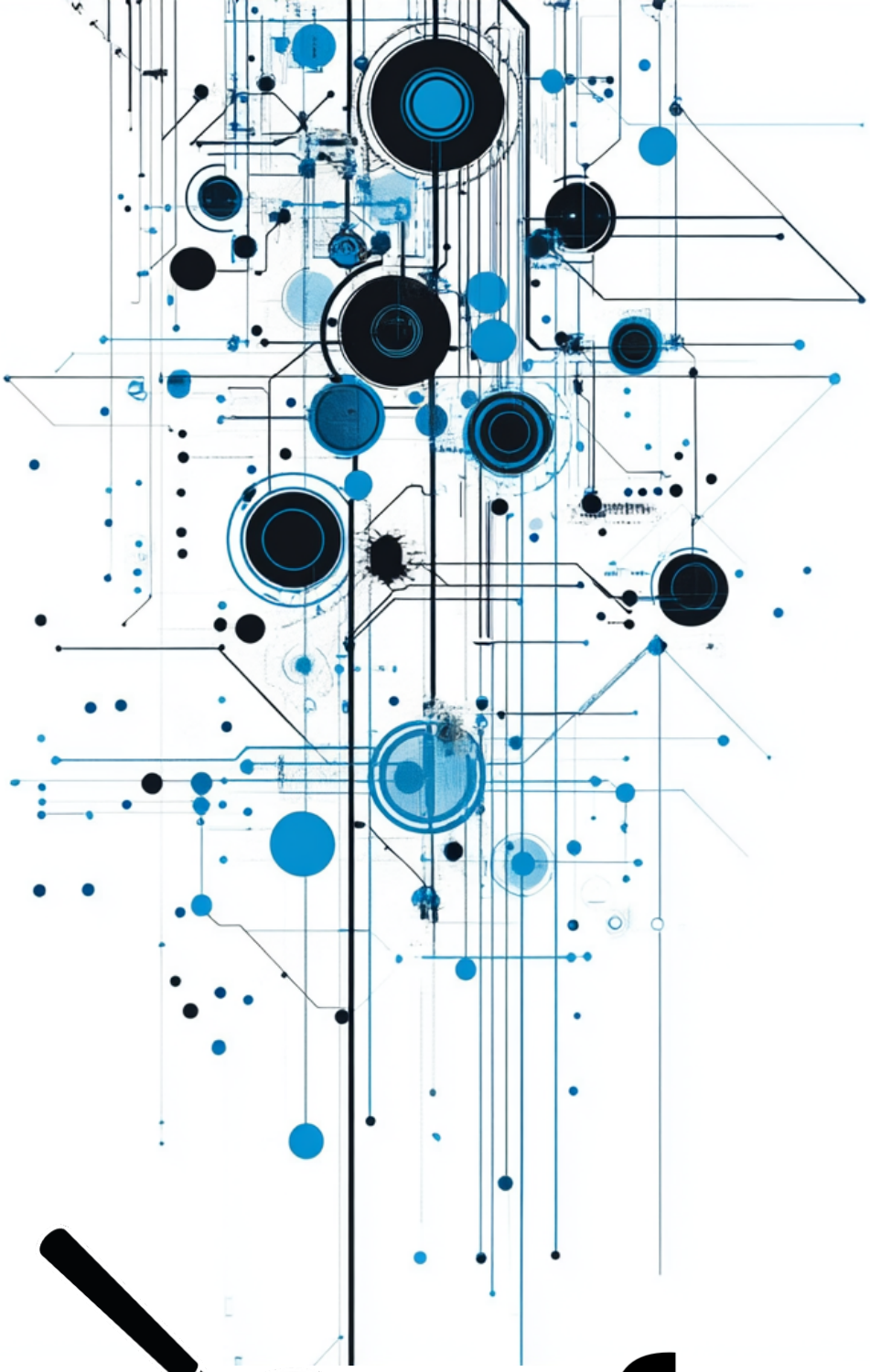


ransomfeed

ADVANCED **DATADRIVEN** CYBERNEWS

REPORT QUADRIMESTRALE
II-4M 2024

ver. glitch256_u01 - 05 novembre 2024

INDICE

Nel mondo del ransomware, ogni attacco non solo mette a rischio i dati, ma minaccia la fiducia che le organizzazioni costruiscono con i loro clienti.

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

Questo report fornisce un'analisi approfondita delle minacce **ransomware** osservate nel **secondo quadrimestre del 2024**, con un focus specifico sulle attività di monitoraggio condotte tramite la piattaforma OSINT **Ransomfeed**.

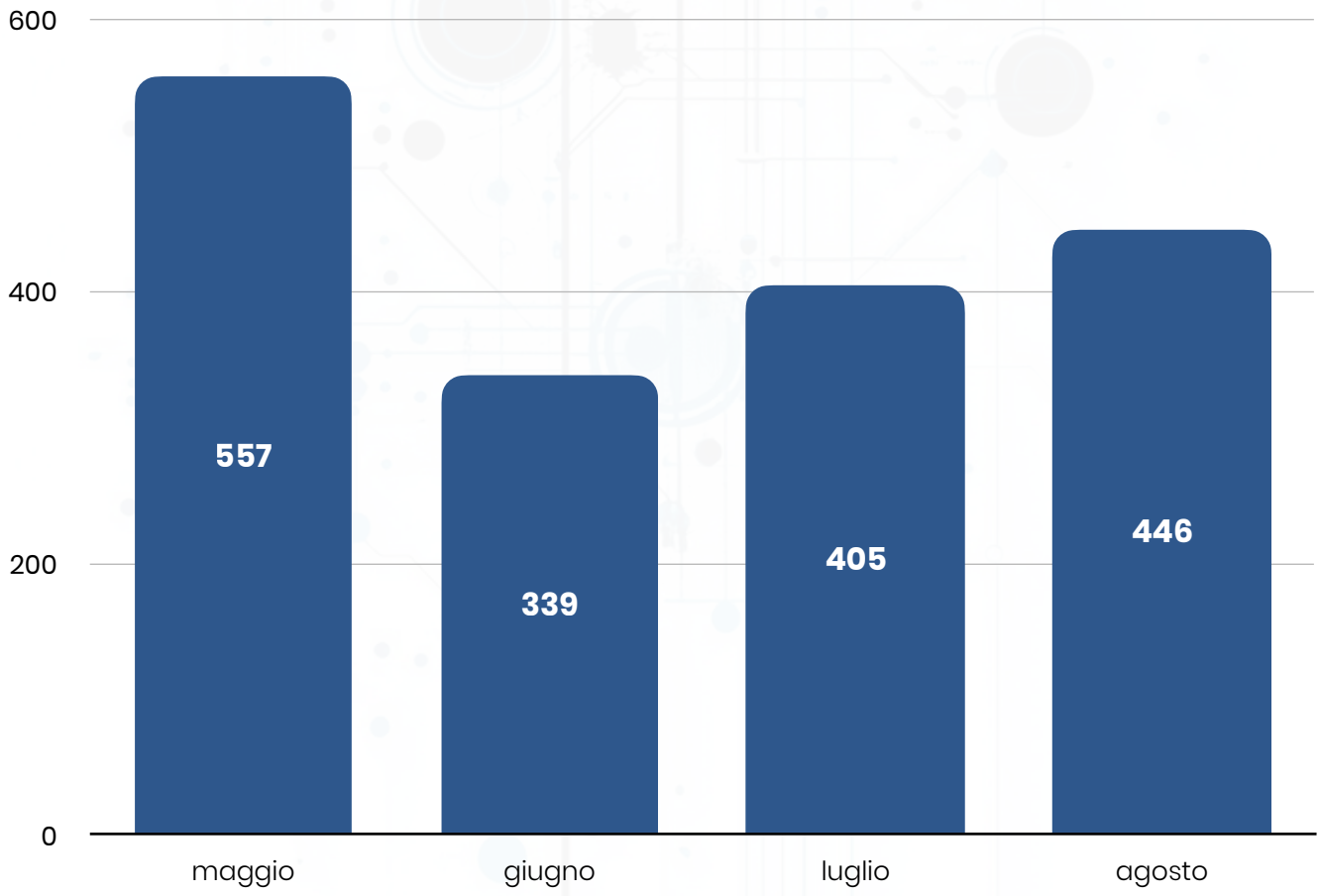
Durante il periodo in esame, sono stati tracciati **208 gruppi criminali** attivi a livello globale e monitorati **427 server** utilizzati per attacchi ransomware, registrando un totale di **1.747 rivendicazioni**, di cui **58 in Italia**.

Il report esaminerà la **distribuzione geografica** degli attacchi e i **settori più colpiti**. Particolare attenzione sarà dedicata agli incidenti verificatisi in Italia, per analizzare le sfide specifiche affrontate dal Paese in un periodo critico per la sicurezza informatica.

Panoramica

Tutti i dati inclusi in questo report sono stati raccolti tramite l'attività primaria di **Ransomfeed**, che effettua uno **scraping periodico** da fonti riconosciute del dark web. Il report si concentra sui dati del **secondo quadrimestre 2024**, offrendo prima una panoramica globale e poi un'analisi specifica per l'Italia.

Maggio 2024 è stato il mese più colpito, con **557 attacchi**, seguito da **agosto con 446**, **luglio con 405** e **giugno con 339**. Come emerge, il numero di attacchi è aumentato progressivamente nel corso del quadrimestre rispetto ai mesi precedenti.

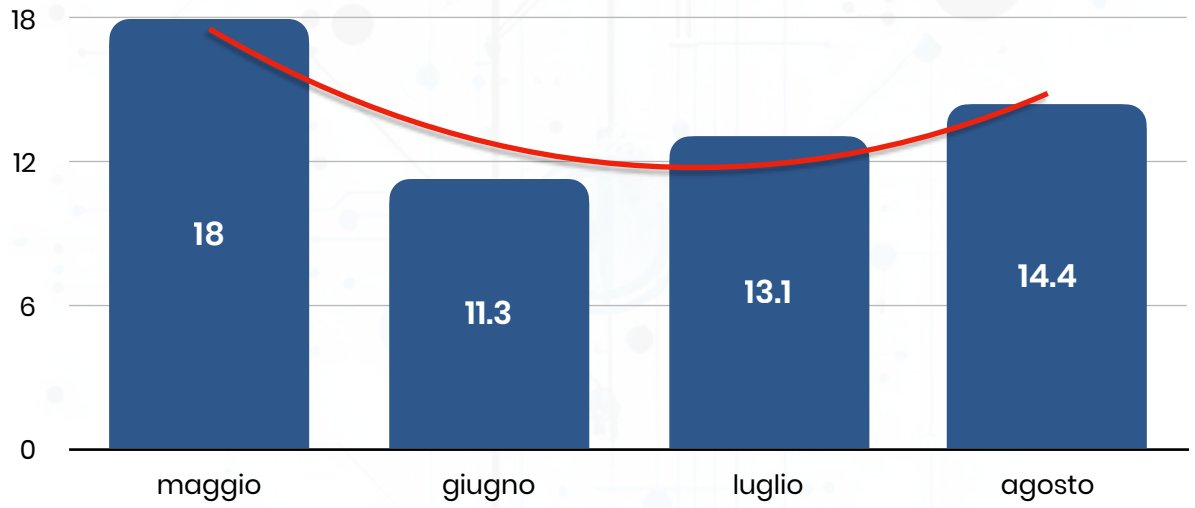


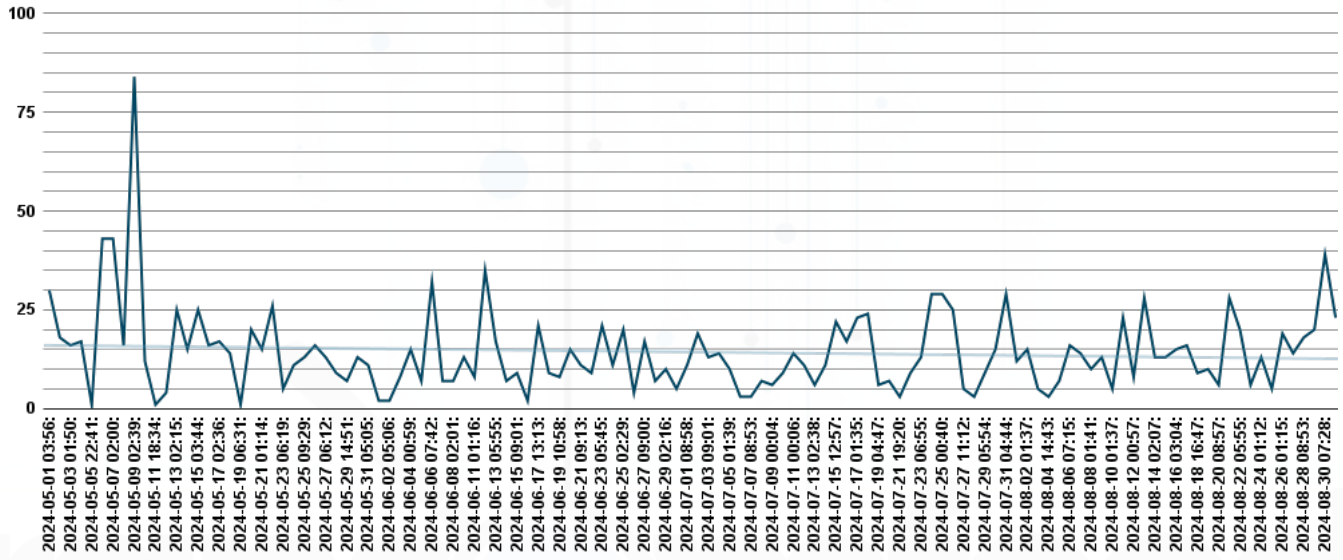
attacchi suddivisi per mese, fonte Ransomfeed.it

Il **9 maggio** si è registrato il **picco di attività ransomware** del quadrimestre, con ben **84 attacchi** rivendicati in un solo giorno, segno della capacità dei gruppi criminali di sfruttare rapidamente le vulnerabilità digitali. Questo incremento mette in evidenza l'urgenza di colmare le lacune nella sicurezza informatica e di rafforzare le difese contro minacce in continua crescita.

Al contrario, i giorni **5, 11 e 19 maggio** si sono distinti come i **meno colpiti**, con una sola rivendicazione ciascuno. Tale oscillazione tra i periodi di massimo e minimo attacco indica che, pur concentrandosi in certi giorni, il rischio resta costante e imprevedibile.

La **media di oltre 11,7 attacchi giornalieri** è un dato allarmante: il **trend crescente** minaccia non solo la sicurezza di dati sensibili e risorse finanziarie, ma anche la fiducia nelle infrastrutture su cui si basano aziende e governi.





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

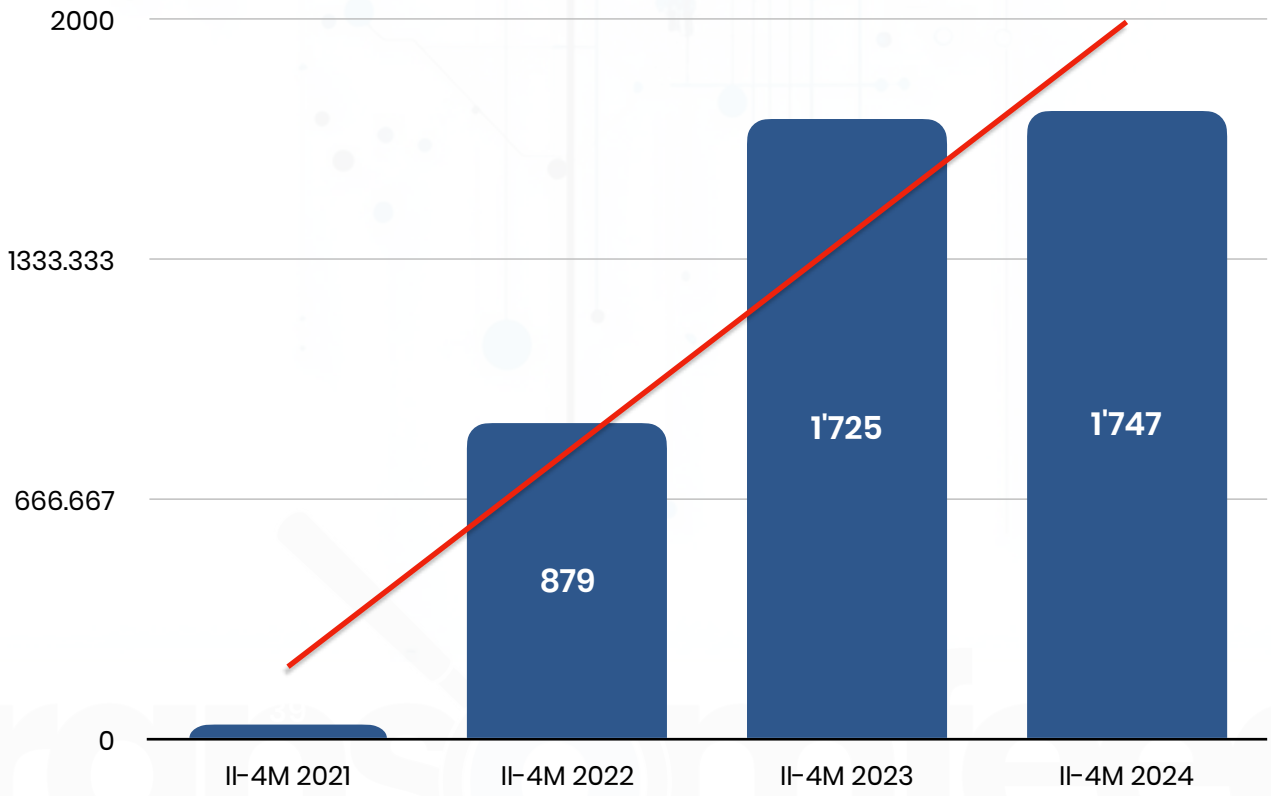
Quadrimestri a confronto

Per contestualizzare i dati della Panoramica, è stato condotto un **confronto** tra il secondo quadrimestre 2024 e i dati dei secondi quadrimestri degli ultimi tre anni, ricavati dallo **storico** di **Ransomfeed**, che risale fino al 12 gennaio 2020. Questo confronto retrospettivo consente di identificare **schemi ricorrenti**, variazioni stagionali e nuove tecniche utilizzate dai cybercriminali.

Dall'analisi storica emerge un **trend in costante crescita**, senza segni di riduzione degli attacchi. La **crescita** registrata nel secondo quadrimestre del 2024 appare significativa e, rispetto agli anni precedenti, il 2024 ha superato il 2023 con un **aumento dell'1.28%**, mentre il confronto con il 2022 evidenzia un **incremento** impressionante del **98.75%**.

Questa tendenza rappresenta un indicatore critico che suggerisce non solo una **crescita costante degli attacchi ransomware**, ma anche la possibile adozione di nuove tattiche e strategie. Il confronto con gli anni precedenti rivela che, sebbene gli attacchi aumentino in modo continuo, il ritmo di crescita varia: l'**incremento sostanziale tra il 2022 e il 2024** indica un'**escalation particolarmente preoccupante** negli ultimi due anni.

In sintesi, l'analisi storica offre un quadro completo, fondamentale sia per comprendere il contesto attuale sia per **anticipare potenziali sviluppi futuri**, evidenziando l'importanza di strategie di sicurezza adattive e aggiornate per affrontare questa minaccia in continua evoluzione.



fonte Ransomfeed.it

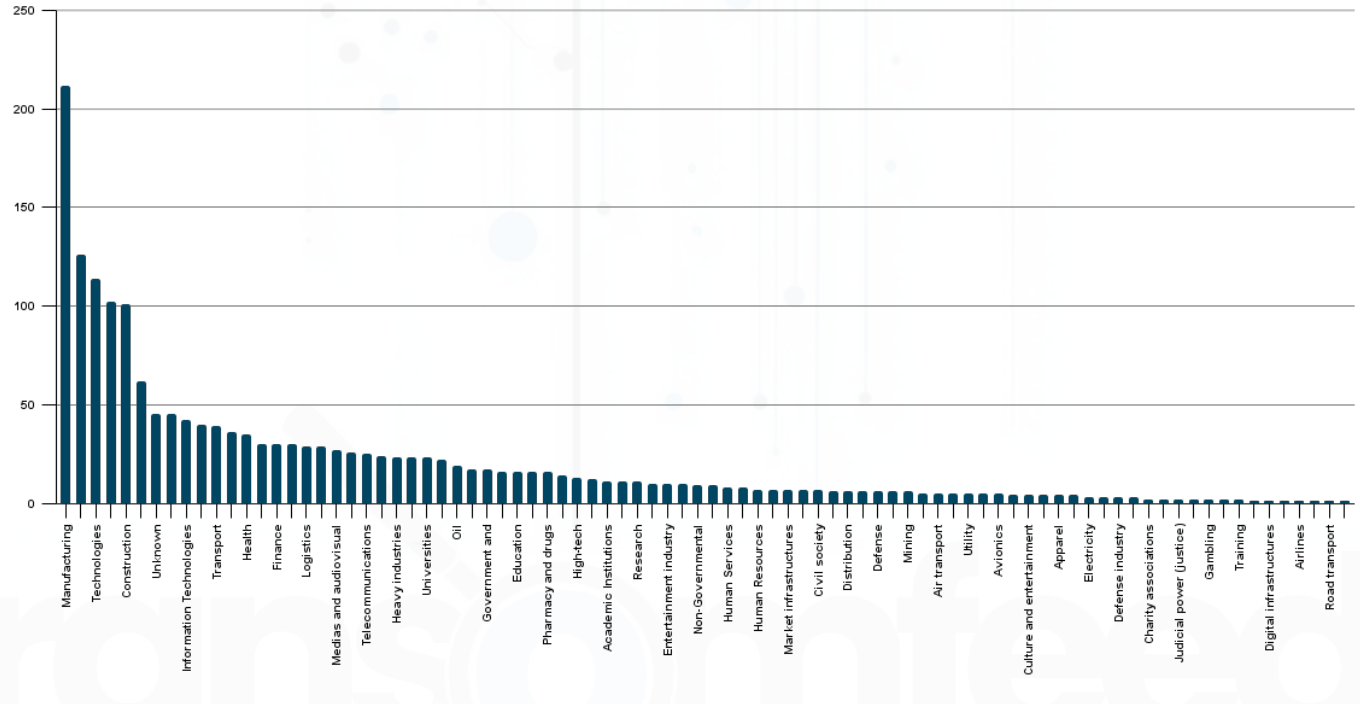
Distribuzione del ransomware nei settori lavorativi

Grazie al processo di **arricchimento dei dati**, reso possibile dalla collaborazione tra il progetto **Ransomfeed** e **Würth Phoenix** sotto la guida dell'esperto **Massimo Giaimo**, è stato possibile completare e allineare i dati mancanti relativi al settore lavorativo delle vittime colpite. Questa partnership ha permesso di generare **statistiche dettagliate** sui settori economici coinvolti, **migliorando la qualità e l'accuratezza** delle informazioni presenti nella piattaforma.

Con questi **dati potenziati**, è ora possibile presentare statistiche di categoria con **maggiore precisione e dettaglio**, permettendo di identificare in modo più chiaro i settori più esposti agli attacchi ransomware.
L'**analisi per settore economico** offre uno strumento prezioso per comprendere le aree vulnerabili e valutare quali misure di sicurezza adottare per **prevenire** o **mitigare** le minacce.

Queste le **prime cinque posizioni** del podio, a rappresentare il **56% del totale** degli attacchi:

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



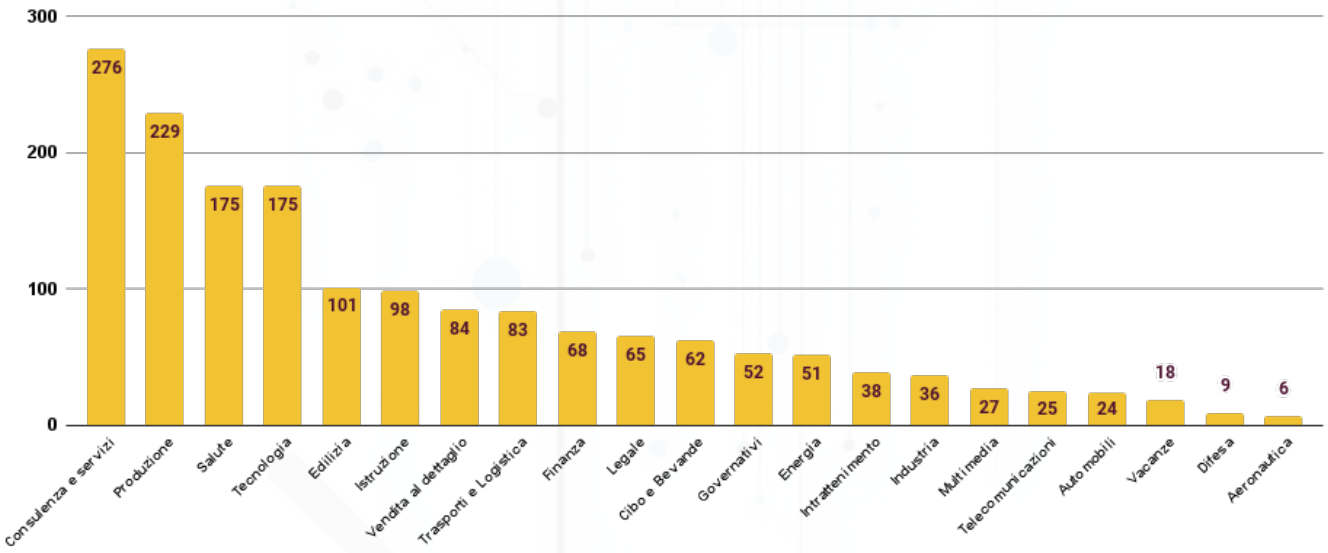
fonte Ransomfeed.it

Le **organizzazioni governative** occupano la **dodicesima posizione** tra le categorie che impattano sulla sicurezza nazionale, con **52 attacchi** rivendicati nel periodo analizzato; un incremento rispetto al quadrimestre precedente. Il **settore dell'istruzione**, significativo anche per la sicurezza nazionale, si colloca al **sesto posto con 98 attacchi** rivendicati. Questi dati evidenziano come i cybercriminali continuino a **colpire settori strategici**.

In particolare, le **istituzioni educative**, le **organizzazioni governative** e le **aziende di servizi terziari** sono tra i **bersagli preferiti** dei criminali informatici. Questi settori, infatti, offrono opportunità per amplificare le attività illecite grazie a una **rete estesa di connessioni** e alla loro **centralità nel tessuto socio-economico**.

Le istituzioni educative gestiscono un elevato volume di **dati sensibili** su studenti, personale e ricerca. Un attacco ransomware in questo ambito può compromettere tali informazioni e **interrompere le attività didattiche e di ricerca**, causando importanti disagi.
Le **scuole internazionali**, in particolare, sono un obiettivo allettante poiché gestiscono infrastrutture IT spesso vulnerabili e servono **famiglie influenti**.

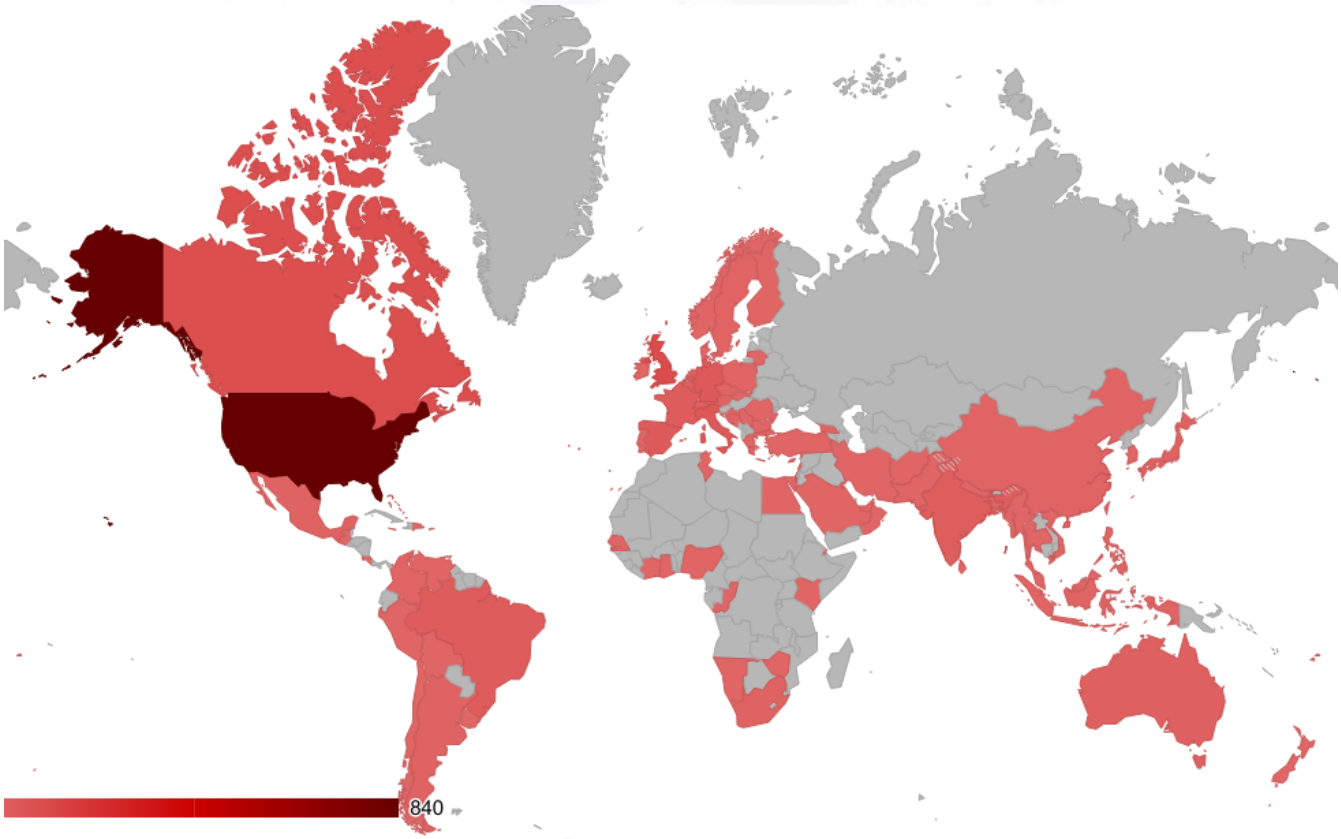
Le **organizzazioni governative**, per il loro trattamento di informazioni strategiche, inclusi dati personali e informazioni sulla sicurezza nazionale, rappresentano un **obiettivo critico**. Un attacco a queste entità può avere conseguenze devastanti, minando la fiducia pubblica e la **stabilità operativa del governo**.



fonte Ransomfeed.it

Distribuzione del ransomware nel mondo

Il **costante lavoro di OSINT** sulla piattaforma, effettuato dopo lo scraping dei dati, fornisce ogni quadrimestre una visione chiara della **geografia degli attacchi informatici** in base alle loro rivendicazioni. Anche in questo quadrimestre, come nei primi due del 2023, la **regione nord-occidentale del mondo** si conferma la **più colpita** dai gruppi criminali.
L'immagine che segue illustra l'impatto di questa rappresentazione geografica.



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

Analizzando le differenze rispetto al primo quadrimestre del 2024, la distribuzione geografica degli attacchi rimane sostanzialmente **invariata e coerente** con i dati precedenti.

Il conflitto israelo-palestinese ha chiaramente **contribuito all'aumento degli attacchi** registrati nelle aree interessate e nei paesi che supportano una delle due fazioni.
Molti nuovi gruppi criminali, infatti, sono nati in risposta all'ideologia politica di una delle parti, contribuendo alla guerra cibernetica e al caos digitale.

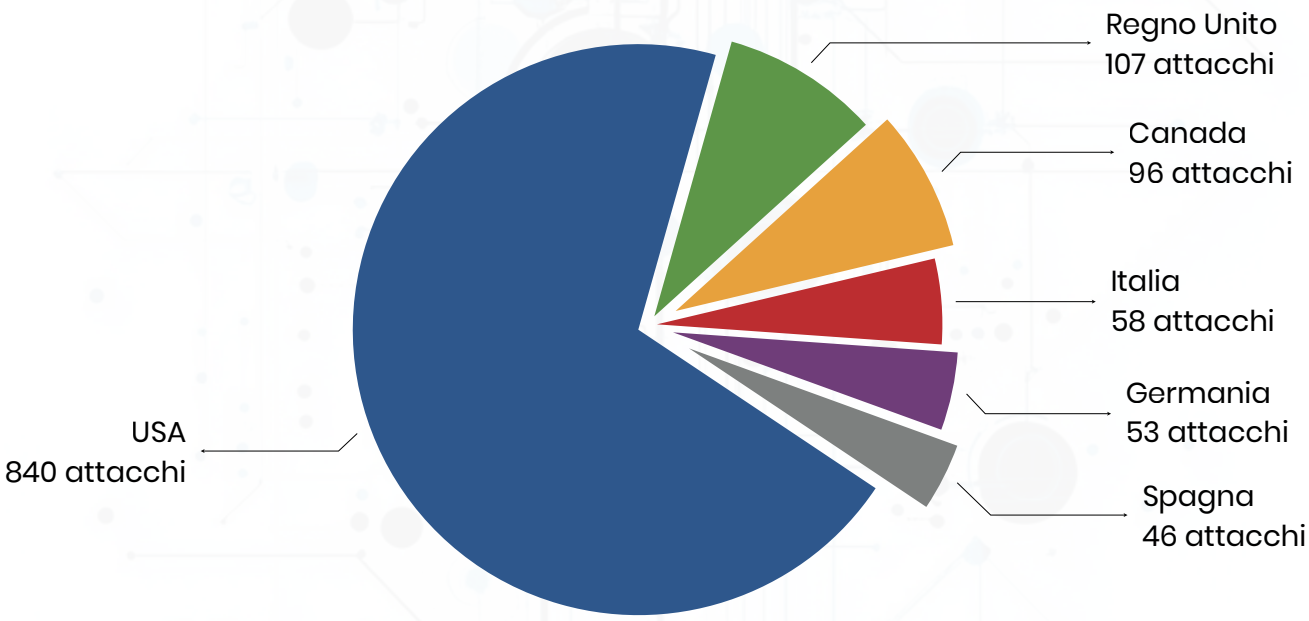
Gli **Stati Uniti** rappresentano una quota significativa degli attacchi, con il **48% del totale**, corrispondente a **840 rivendicazioni**.

Seguono il **Regno Unito**, il **Canada** e l'**Italia**, che occupano le posizioni più alte per numero di attacchi. Questi paesi sono sede di importanti attività economiche e dispongono di infrastrutture tecnologiche avanzate, rendendoli **obiettivi privilegiati** per i cyber attacchi.

USA, 48.1%	**Svezia**, 0.6%	**Egitto**, 0.2%	**Costa Rica**, 0.1%
Regno Unito, 6.1%	**Taiwan**, 0.5%	**Guatemala**, 0.2%	**Gibuti**, 0.1%
Canada, 5.5%	**Austria**, 05%	**Libano**, 0.2%	**Finlandia**, 0.1%
Italia, 3.3%	**Cina**, 0.5%	**Norvegia**, 0.2%	**Georgia**, 0.1%
Germania, 3.0%	**Colombia**, 0.5%	**Pakistan**, 0.2%	**Ghana**, 0.1%
Spagna, 2.6%	**Indonesia**, 0.5%	**Portorico**, 0.2%	**Iran**, 0.1%
Francia, 2.5%	**Rep. Ceca**, 0.4%	**Zimbabwe**, 0.2%	**Giamaica**, 0.1%
Brasile, 2.4%	**Irlanda**, 0.4%	**Rep. Dominicana**, 0.1%	**Lituania**, 0.1%
India, 1.9%	**Nuova Zelanda**, 0.4%	**Fiji**, 0.1%	**Lussemburgo**, 0.1%
Israele, 1.7%	**Romania**, 0.4%	**Costa d'Avorio**, 0.1%	**Myanmar**, 0.1%
Australia, 1.5%	**Sud Corea**, 0.4%	**Kenya**, 0.1%	**Namibia**, 0.1%
Giappone, 1.0%	**Perù**, 0.3%	**Kuwait**, 0.1%	**Nepal**, 0.1%
Belgio, 0.9%	**Turchia**, 0.3%	**Oman**, 0.1%	**Nigeria**, 0.1%
Emirati Arabi, 0.9%	**Cile**, 0.3%	**Seychelles**, 0.1%	**Grenadine**, 0.1%
Messico, 0.8%	**Croazia**, 0.3%	**Slovacchia**, 0.1%	**Senegal**, 0.1%
Paesi Bassi, 0.8%	**Hong Kong**, 0.3%	**Venezuela**, 0.1%	**Serbia**, 0.1%
Argentina, 0.7%	**Filippine**, 0.3%	**Afganistan**, 0.1%	**Sri Lanka**, 0.1%
Sud Africa, 0.7%	**Tailandia**, 0.3%	**Bahamas**, 0.1%	**Timor Leste**, 0.1%
Svizzera, 0.7%	**Grecia**, 0.2%	**Bangladesh** 0.1%	**Trinidad**, 0.1%
Danimarca, 0.6%	**Malesia**, 0.2%	**Bolivia**, 0.1%	**Tunisia**, 0.1%
Non Disponibile, 0.6%	**Portogallo**, 0.2%	**Bosnia**, 0.1%	**Uruguay**, 0.1%
Polonia, 0.6%	**Vietnam**, 0.2%	**Bulgaria**, 0.1%	**Isole Vergini,** 0.1%
Singapore, 0.6%	**Cipro**, 0.2%	**Congo**, 0.1%	

fonte Ransomfeed.it

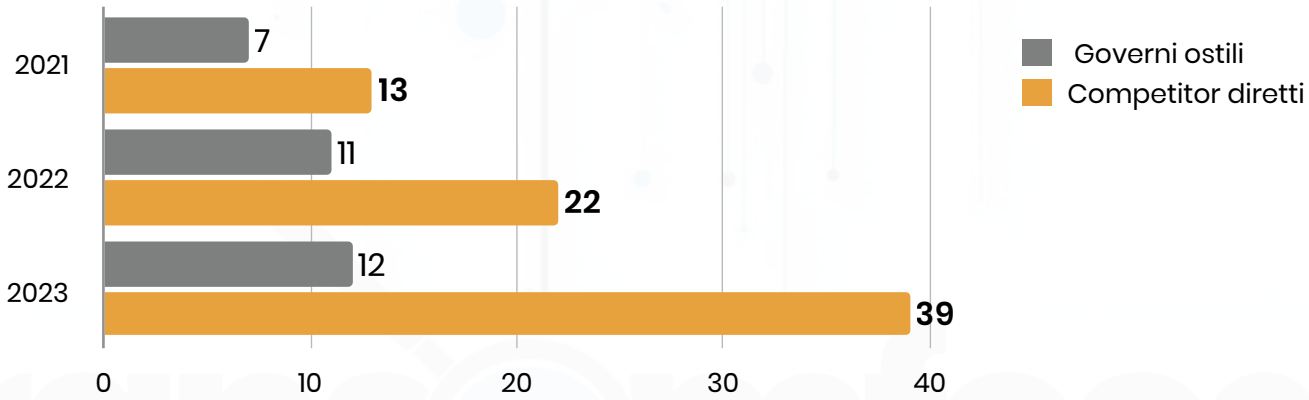
Nel **secondo quadrimestre** del 2024, l'**Italia** si posiziona al **quarto posto con 58 attacchi**, segnando un **incremento** rispetto ai periodi precedenti.



fonte Ransomfeed.it

L'**impatto degli attacchi** ransomware sulle economie dei paesi colpiti è spesso devastante, comportando un **notevole dispendio di risorse** sia economiche sia umane. **Interruzioni della produttività** che durano giorni o settimane, **paralisi nelle operazioni** di approvvigionamento e nella gestione delle infrastrutture IT, e **perdite di fiducia e reputazione** sono fattori che attirano l'attenzione dei concorrenti.

Questi aspetti sono tra i più frequenti motivi per cui i **gruppi criminali vengono assoldati**, sia da aziende rivali che da governi ostili.

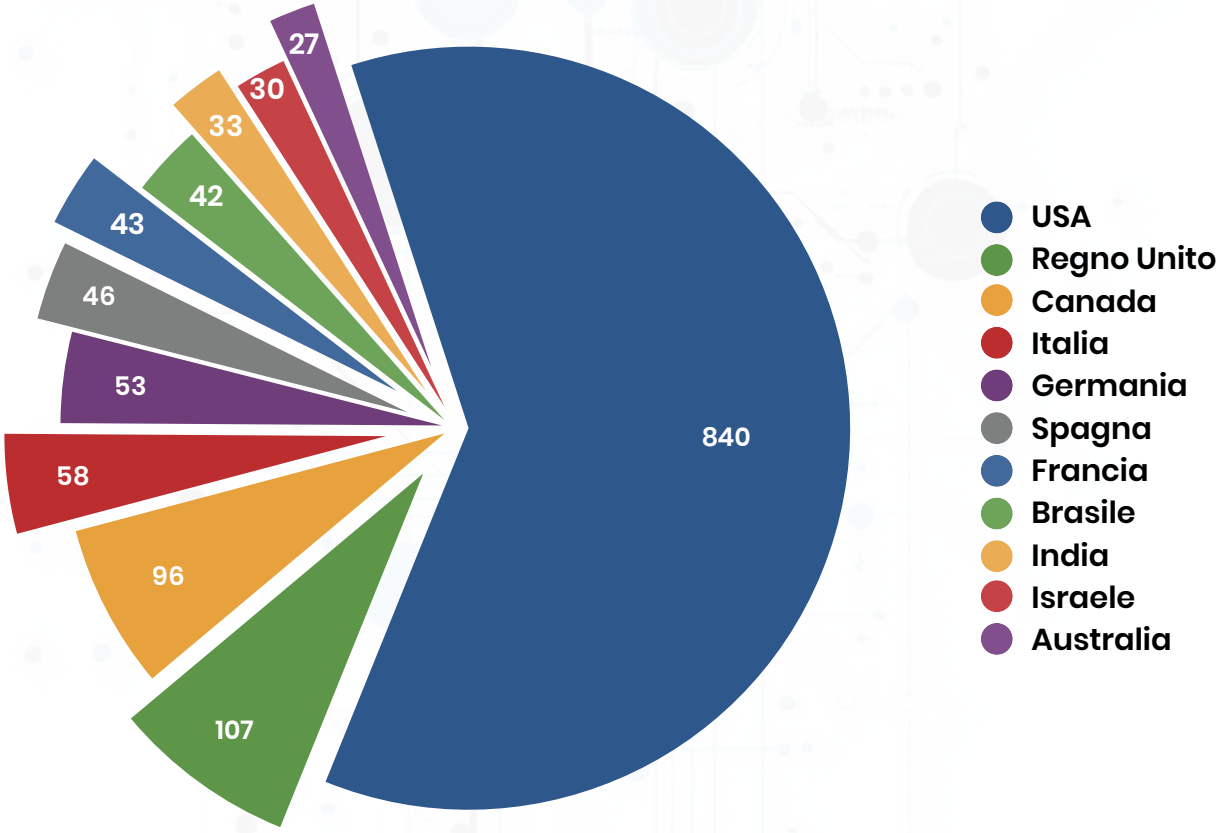


fonti aggregate dal dark web

Top 10

Anche nel **secondo quadrimestre del 2024**, il grafico evidenzia un **ampio divario** tra gli Stati Uniti e il resto del mondo, mostrando chiaramente la distribuzione degli attacchi. Gli USA, con un numero significativamente superiore, si confermano come il paese più colpito.

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



fonte Ransomfeed.it

Questo fenomeno riflette la **maggiore concentrazione** di infrastrutture industriali e aziendali rispetto ad altri paesi. La **centralità economica e politica** degli Stati Uniti, a livello globale, li rende un **obiettivo strategico** per attacchi informatici di vario tipo (DDoS, malware, ransomware, ..).

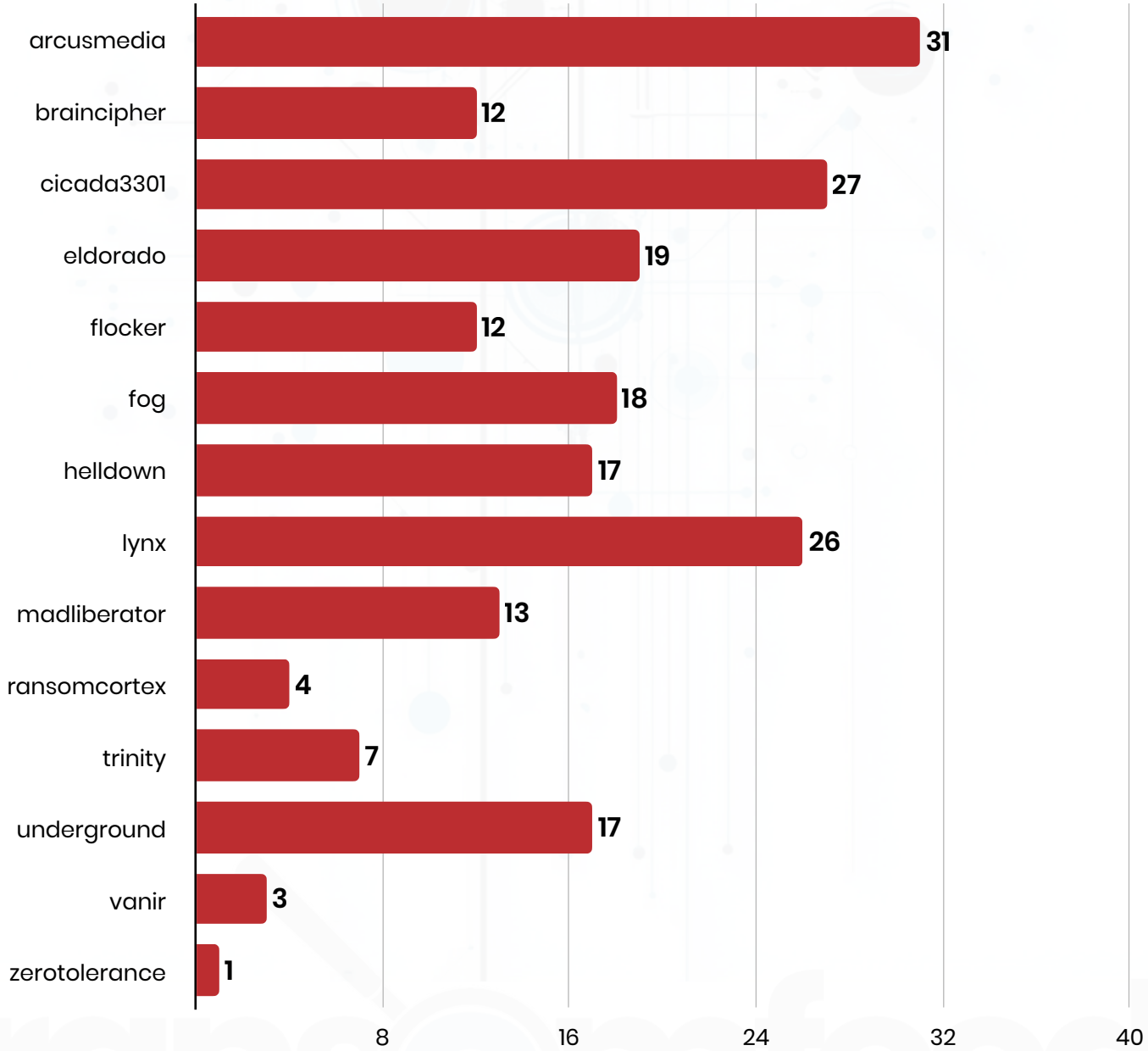
I criminali comprendono che **colpire aziende e istituzioni** americane può generare **ripercussioni a livello mondiale**, destabilizzando mercati e innescando effetti a catena in diverse industrie. Inoltre, è stato registrato un picco di attacchi contro infrastrutture critiche in concomitanza con l'avvicinarsi del periodo elettorale nel paese.

Nuovi gruppi criminali

Nel **secondo quadrimestre del 2024**, sono emersi **nuovi gruppi criminali** che hanno rapidamente guadagnato visibilità nel panorama delle minacce. La piattaforma ha rilevato e integrato questi nuovi threat actors nel suo monitoraggio quotidiano.

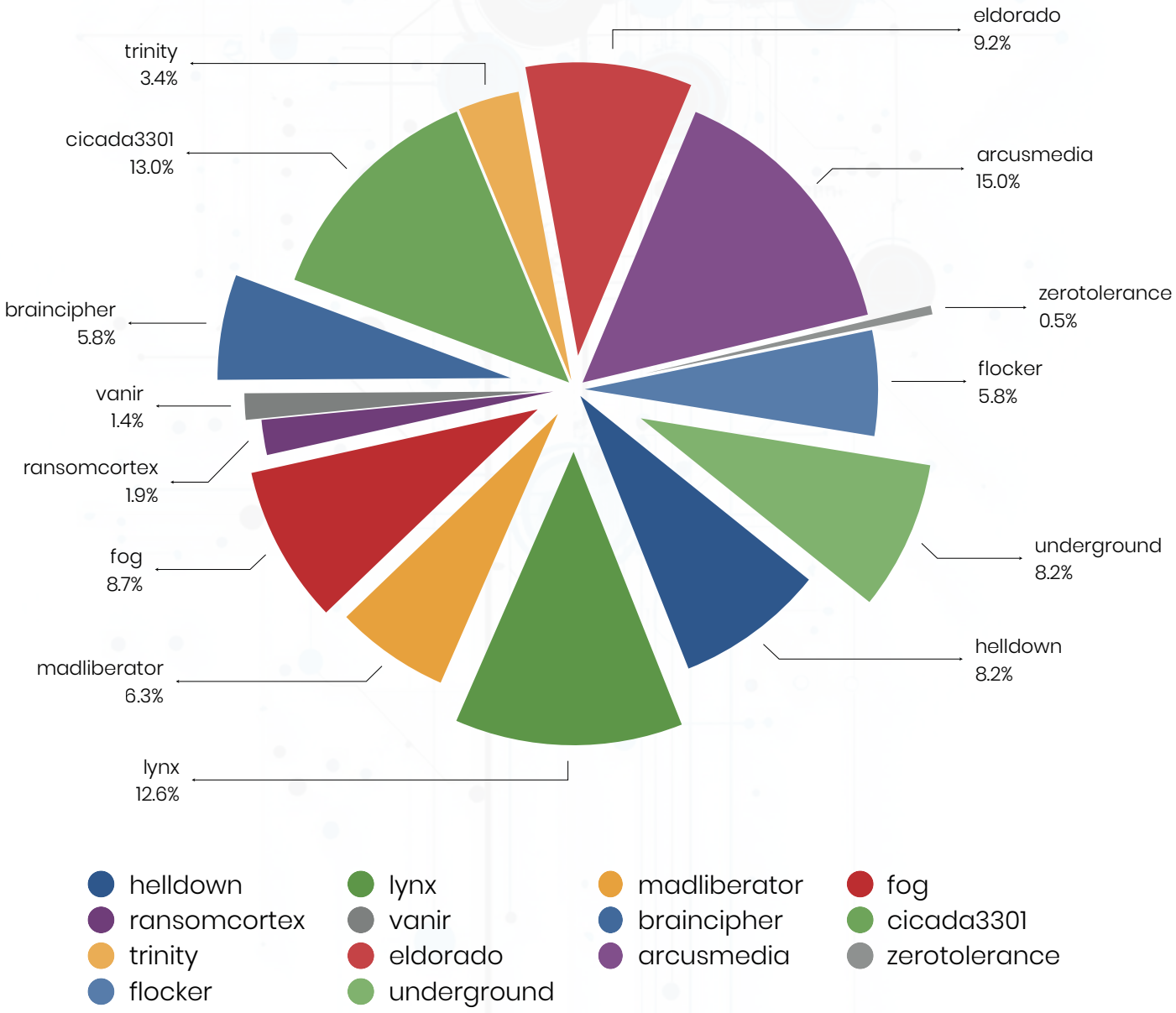
In totale, sono stati registrati **207 nuovi attacchi** ransomware rivendicati, provenienti da **14 gruppi criminali** distinti.

Tra questi, **Arcus Media** si distingue come la cybergang **più attiva** del secondo quadrimestre, con il **15% delle rivendicazioni** all'interno del proprio cluster.



fonte Ransomfeed.it

Il **proliferare di nuovi gruppi** nella scena ransomware rappresenta una sfida significativa non solo per aziende e istituzioni, ma anche per l'organizzazione del crimine stesso. Ogni gruppo sviluppa **caratteristiche uniche**, sfruttando risorse interne e, spesso, affiliandosi a gruppi più grandi e consolidati per **accedere a tecnologie avanzate** e infrastrutture che non potrebbero permettersi autonomamente.



fonte Ransomfeed.it

Nei prossimi mesi, implementeremo **nuove soluzioni grafiche** e **statistiche**, affiancate da un **approfondito lavoro di threat intelligence** e OSINT sui gruppi, per migliorare la comprensione delle attuali minacce, tenendo conto anche del contesto geopolitico.

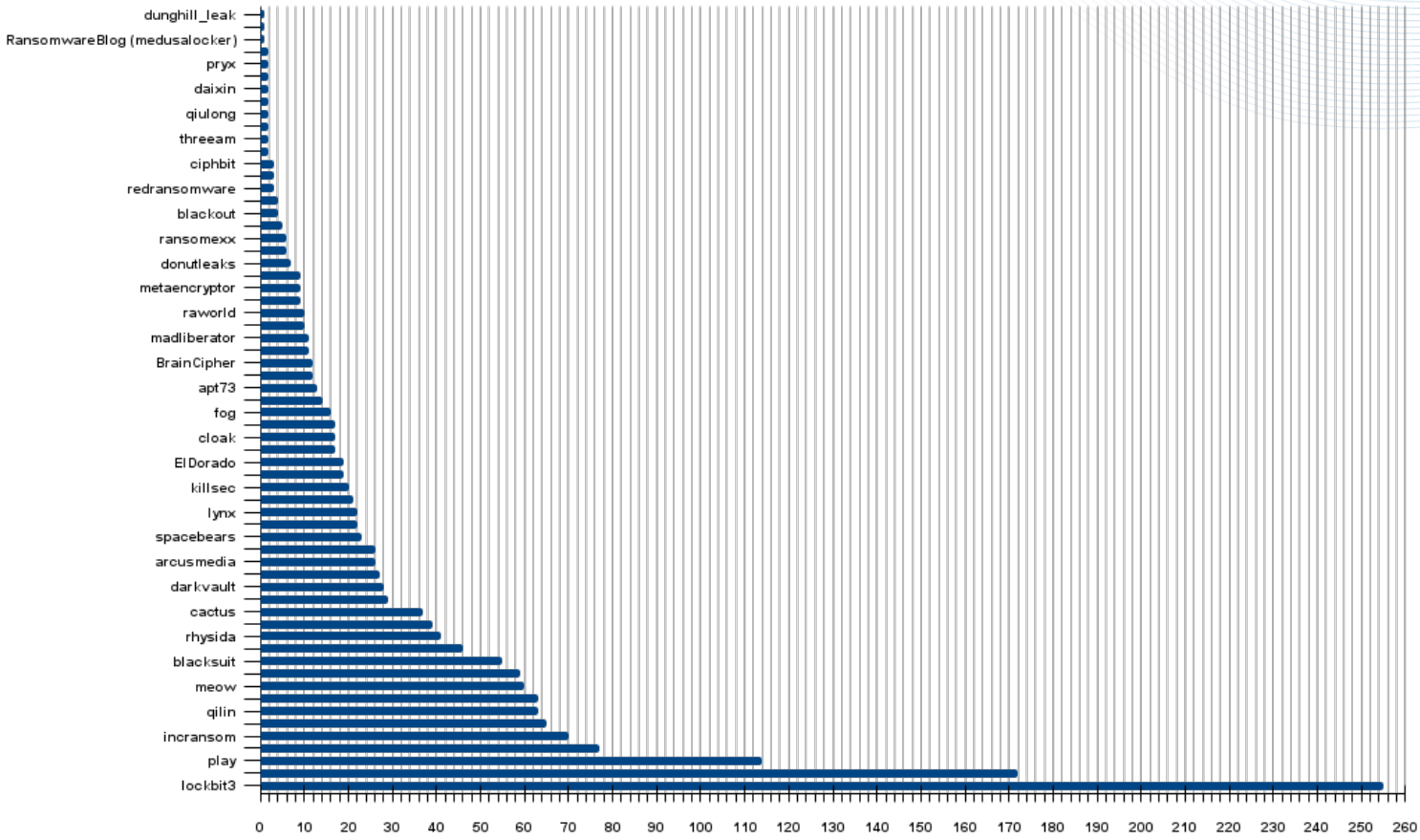
Le attività globali dei gruppi ransomware

Abbiamo analizzato i gruppi che hanno generato attività nei secondi quattro mesi dell'anno. Tra i gruppi costantemente monitorati, la piattaforma ha rilevato movimenti per 63 di essi durante il quadrimestre in esame.

Tra questi **63 gruppi**, **sei gang** estremamente attive hanno dimostrato una leadership netta, rappresentando insieme il **50% degli attacchi totali** registrati.

- **lockbit3**: fino a questo momento è leader indiscusso con il **14% degli attacchi**, sebbene in calo rispetto al II-4M 2023
- **ransomhub**: con il **9.8% degli attacchi**, si posiziona come il secondo gruppo più attivo
- **play**: responsabile del **6.8% degli attacchi**, al terzo posto
- **akira**: con il **4.4% degli attacchi**
- **incransom**: registra al suo attivo il **4% degli attacchi**
- **medusa**: chiude il gruppo di testa con il **3.7% degli attacchi**

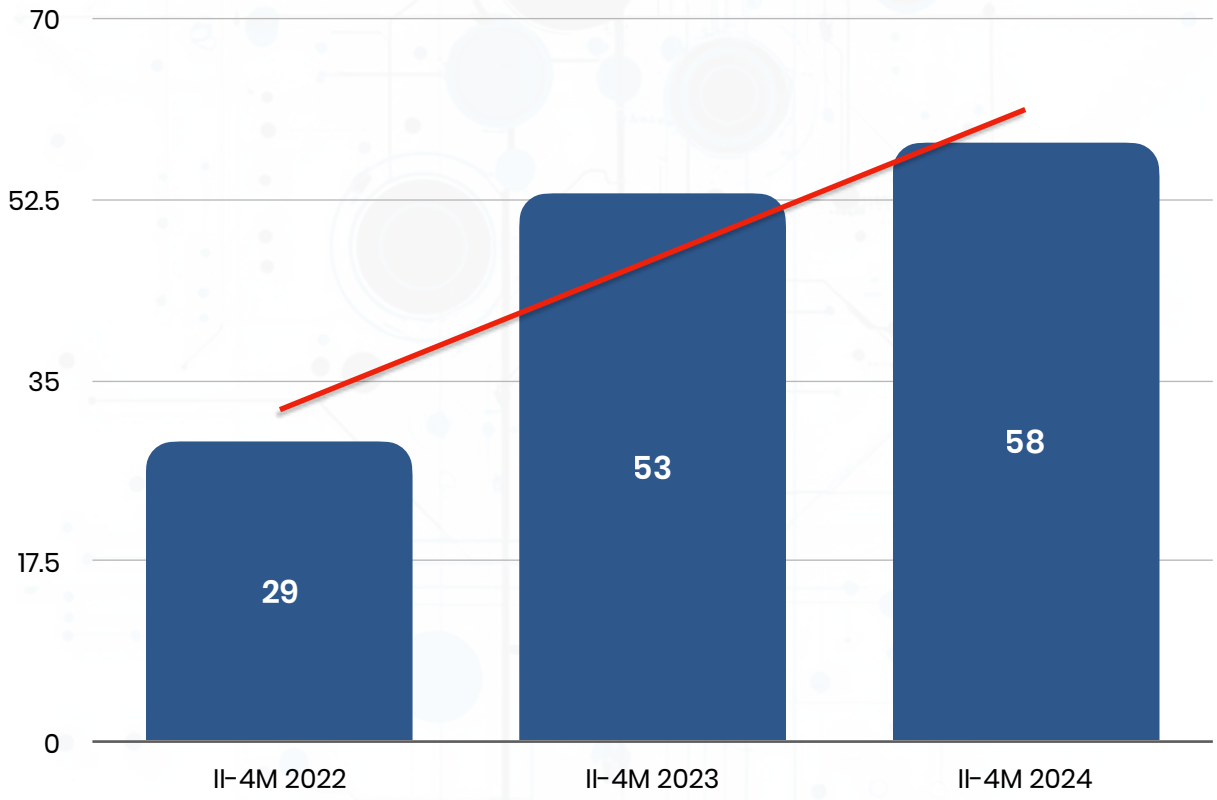
Gli altri gruppi non menzionati risultano **inattivi**, suggerendo una possibile **sospensione** (temporanea) delle operazioni o una **riorganizzazione** interna.



fonte Ransomfeed.it

Focus Italia

In questa sezione del report, analizziamo i dati dei cluster presentati a livello globale, concentrandoci in particolare sulla **situazione in Italia**. Durante questo periodo, sono stati registrati **58 attacchi**, equivalenti a poco più di **uno ogni due giorni**.



fonte Ransomfeed.it

Rispetto al secondo quadrimestre del 2023 e del 2022, questo dato si **allinea al trend** globale, mostrando un incremento rispetto allo stesso periodo dell'anno precedente.
L'**incremento percentuale** degli attacchi dal 2022 ad 2024 è **quasi del 100%**.

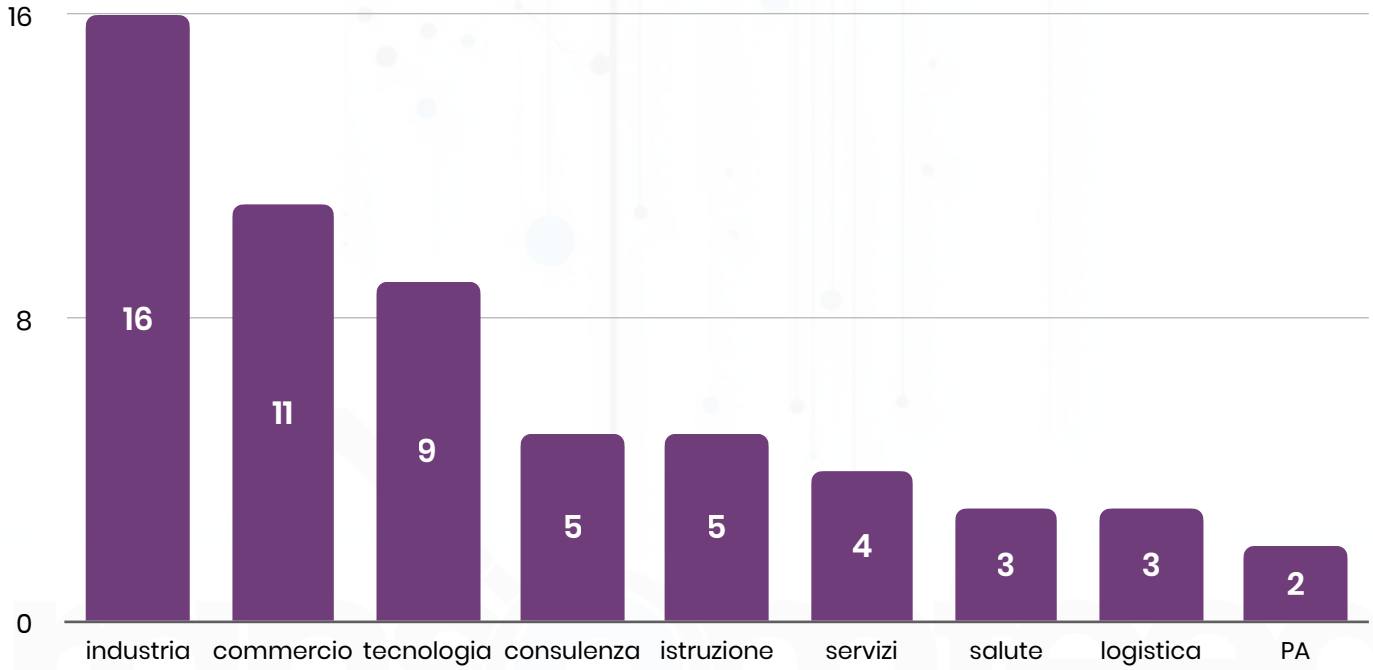
Confrontando questi dati con quelli globali, otteniamo una visione più completa del panorama delle minacce ransomware e delle tendenze emergenti. Inoltre, grazie a un'analisi specifica, possiamo estrarre **informazioni preziose** per valutare lo stato di salute delle aziende e delle istituzioni, nonché l'efficacia delle loro strategie di mitigazione.

Attacchi per settore economico

Nel contesto italiano, l'**industria** e il **commercio** si attestano come i **settori più colpiti**. Nel primo quadrimestre del 2024, questi settori hanno subito **rispettivamente 16** e **11 attacchi** ransomware. All'interno del **settore industriale**, le industrie **farmaceutiche**, **meccaniche**, **metallurgiche** ed **elettroniche** sono state particolarmente vulnerabili. Anche gli **studi professionali**, parte integrante del settore della consulenza, hanno subito numerosi attacchi.

Seguono i settori della **tecnologia**, della **consulenza**, dell'**istruzione** e dei **servizi**, tutti con un numero significativo di attacchi. È evidente che questi settori siano i più bersagliati a causa dell'elevato valore dei dati che gestiscono e della criticità delle loro operazioni, che li rende altamente suscettibili alle richieste di riscatto.

- 🏭 **industria**, 41.0%
- 🤝 **commercio**, 28.2%
- 🖥️ **tecnologia**, 23.1%
- 💼 **consulenza**, 12.8%
- 🏫 **istruzione**, 12.8%
- 🔌 **servizi**, 10.3%
- 😁 **salute**, 7.7%
- 🚚 **logistica**, 7.7%
- 🏢 **pubblica amministrazione**, 5.1%



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 secondo quadrimestre del 2024. La mappa, consultabile anche online con **funzioni interattive**, è disponibile a questo indirizzo o cliccando direttamente sulla stessa.

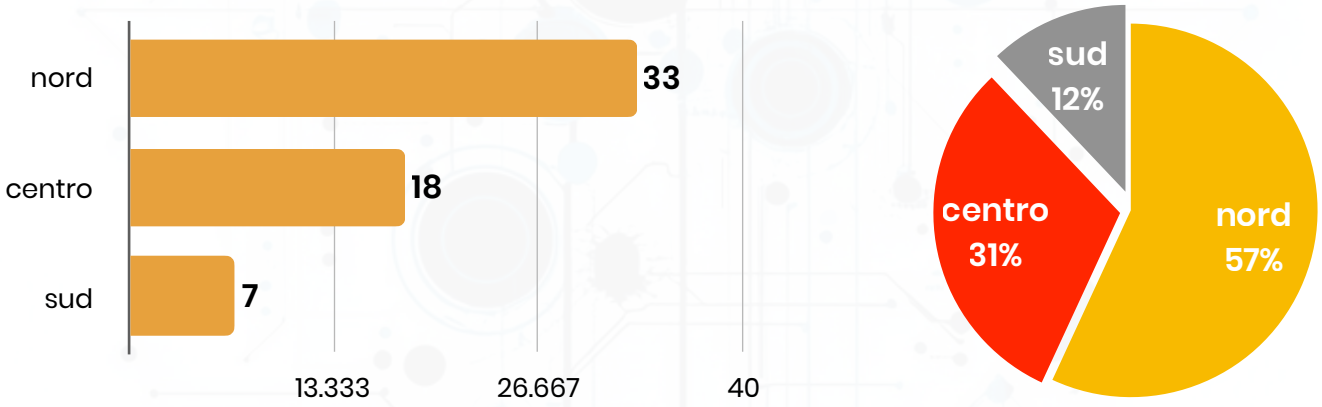
fonte Ransomfeed.it

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 il **56% delle rivendicazioni** riguarda organizzazioni ed enti situati in quest'area.

L'alta concentrazione di attacchi nel settentrione può essere attribuita alla presenza di **numerosi poli tecnologici**, **industriali** e di **consulenza**, che rappresentano bersagli ricchi e spesso vulnerabili.

Analizzando la mappa e suddividendola **in macro aree geografiche**, possiamo ottenere una rappresentazione sinottica della distribuzione degli attacchi ransomware in Italia.

Il grafico seguente illustra la suddivisione, mettendo in evidenza le **differenze di impatto** tra le varie regioni italiane.



fonte Ransomfeed.it

Il **confronto tra il sud e il nord Italia** rivela differenze significative.
Nel sud, la **densità industriale è minore**, con un'economia prevalentemente basata su agricoltura, pesca, turismo e industria leggera. Al contrario, il nord Italia vanta una **consolidata tradizione di sviluppo economico**, con infrastrutture avanzate e una rete di trasporti altamente sviluppata.

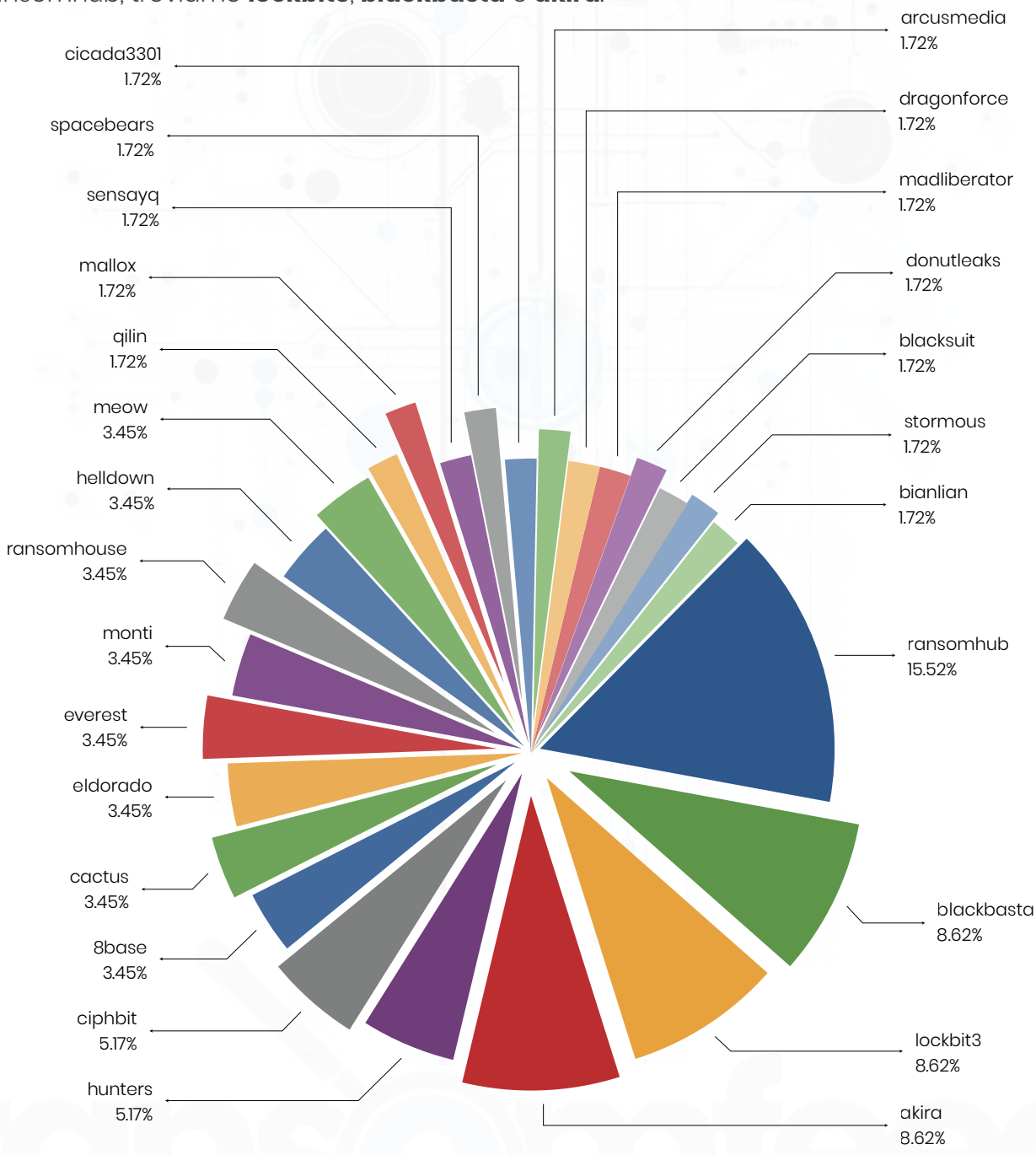
Tuttavia, l'innovazione tecnologica presenta ancora delle **lacune**, sia sul piano imprenditoriale che sociale, evidenziate da un **ridotto afflusso di investimenti a lungo termine**. Questi fattori, uniti alla maggiore concentrazione di aziende e al loro interscambio, rendono le imprese del nord più appetibili per i gruppi di cybercriminali, i quali mirano a sfruttare le vulnerabilità legate alla complessità e all'interconnessione delle operazioni aziendali.

In questo contesto, è fondamentale comprendere come le **specifiche caratteristiche economiche e infrastrutturali** di ciascuna regione possano influenzare il rischio di attacchi ransomware, guidando le strategie di protezione e mitigazione delle aziende e delle istituzioni.

I gruppi criminali più attivi

Anche per il secondo quadrimestre 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 **ransomhub** si è attestato come il **più attivo in Italia** durante questo periodo, con il **15% degli attacchi totali**.

Diventano così **quattro i grandi player** criminali del quadrimestre in Italia: oltre a ransomhub, troviamo **lockbit3**, **blackbasta** e **akira**.



fonte Ransomfeed.it

Conclusione

Complessivamente, sono stati **monitorati 208 gruppi** criminali operanti a livello globale, con **1747 rivendicazioni ransomware**, di cui **58 in Italia**.

In sintesi:

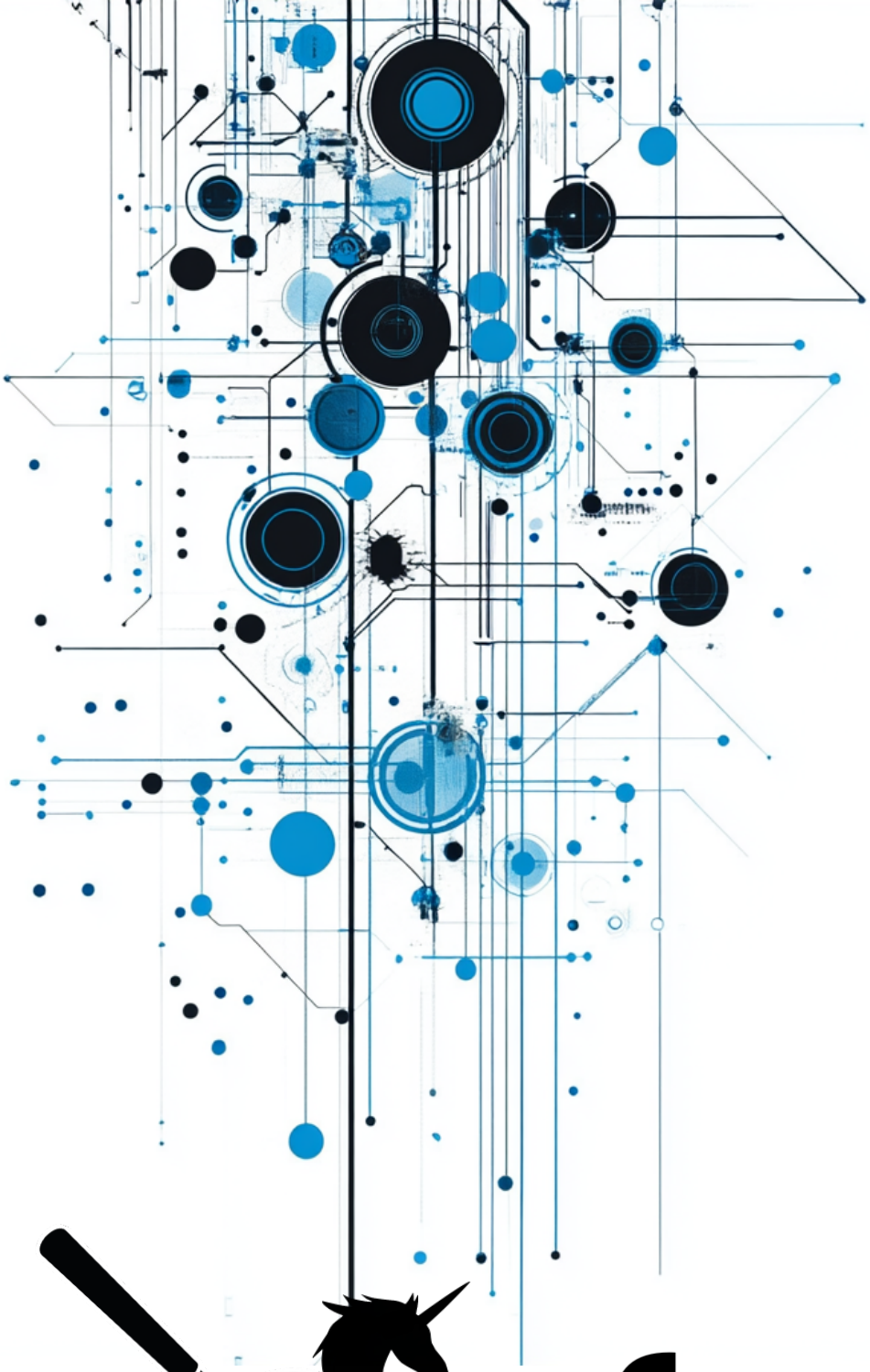
- sono stati **monitorati 208 gruppi** criminali, per un **totale di 1.747 rivendicazioni globali** e **58 in Italia**;
- i settori più colpiti sono stati l'**industria** e la **consulenza**, ma anche servizi, produzione, salute per una fetta pari al **56% del mercato ransomware**;
- le **organizzazioni governative** si sono posizionate al **12° posto** per attacchi rivendicati.

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

REPORT QUADRIMESTRALE
II-4M 2024