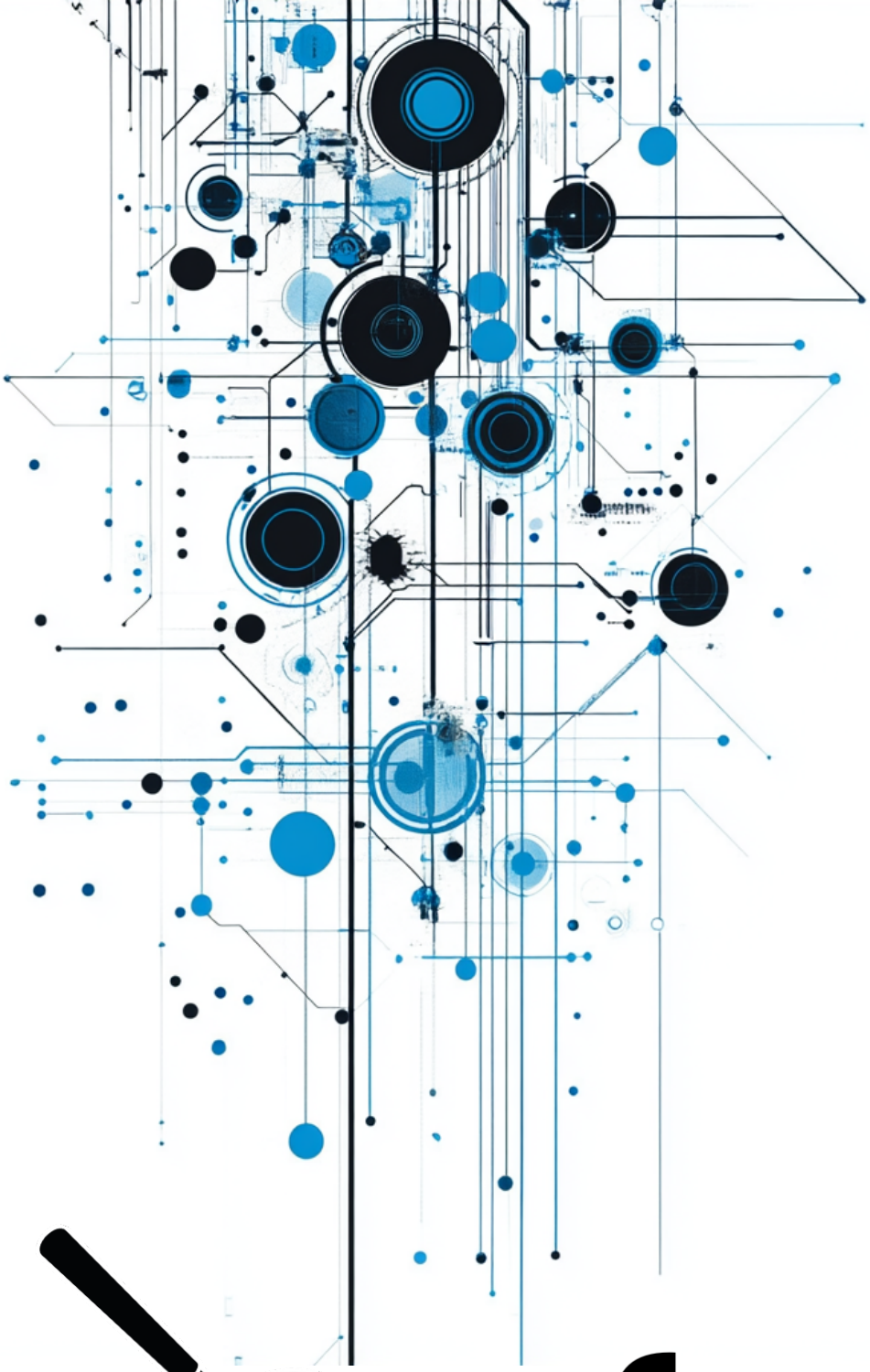


ransomfeed

ADVANCED **DATADRIVEN** CYBERNEWS

REPORT QUADRIMESTRALE
III-4M 2024

ver. r01 - 15 febbraio 2025

INDICE

Mentre il mondo si prepara a convivere con l'Intelligenza Artificiale e le sue implicazioni a tutti i livelli, il ransomware continua a diffondersi giornalmente, con le tecniche classiche ormai ben consolidate e per le quali ancora si è scarsamente imparato a convivere.

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 **terzo quadrimestre del 2024**, con un focus specifico sulle attività di monitoraggio condotte tramite la piattaforma OSINT **Ransomfeed**.

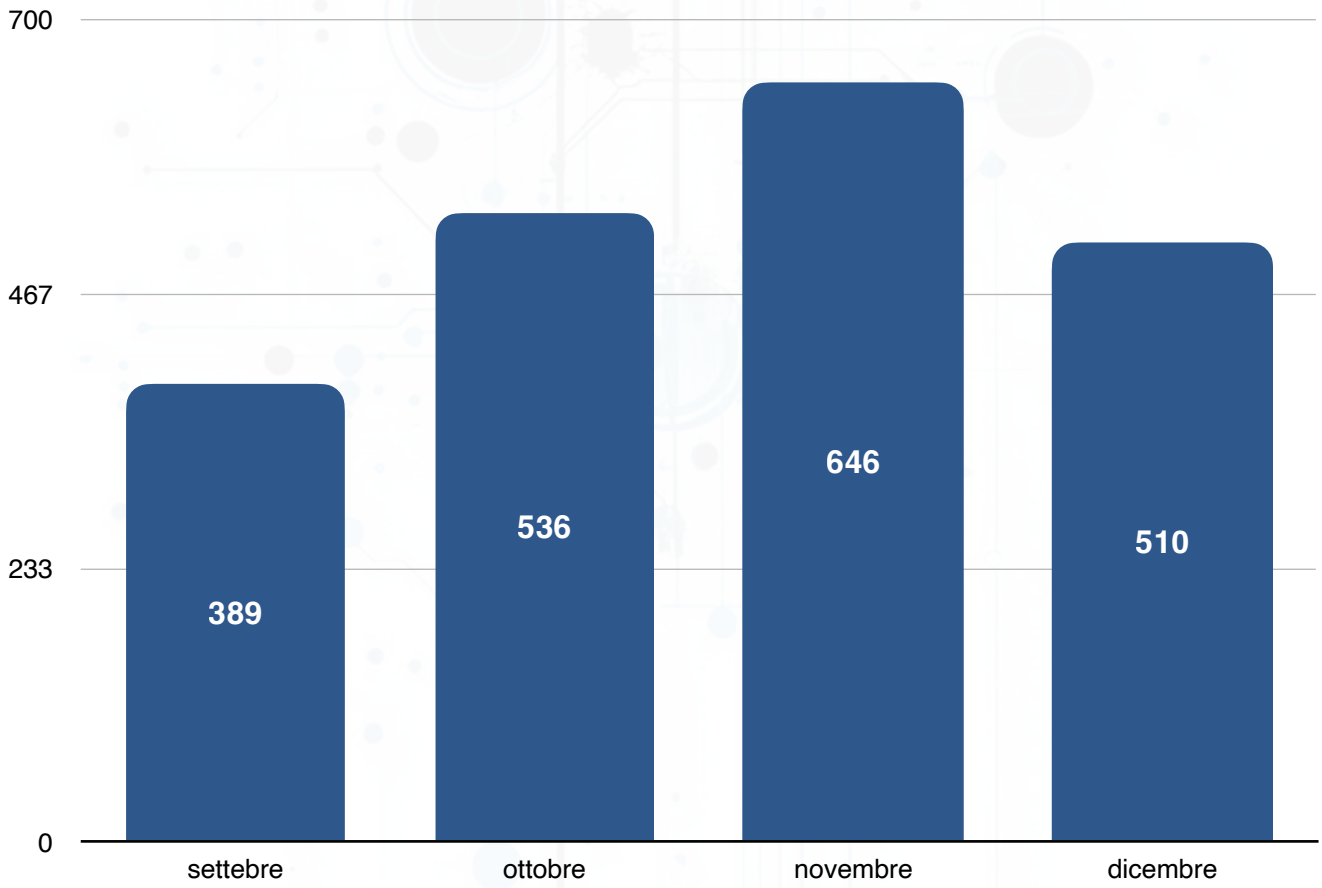
Durante il periodo in esame, sono stati tracciati **235 gruppi criminali** attivi a livello globale e monitorati **504 server** utilizzati per attacchi ransomware, registrando un totale di **2.081 rivendicazioni**, di cui **49 in Italia**.

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 **terzo quadrimestre 2024**, offrendo prima una panoramica globale e poi un'analisi specifica per l'Italia.

Novembre 2024 è stato il mese più colpito, con **646 attacchi**, seguito da **ottobre con 536**, **dicembre con 510** e **settembre con 389**. Come emerge, il numero di attacchi è abbastanza altalenante nei mesi e non presenta una crescita progressiva o un andamento regolare.

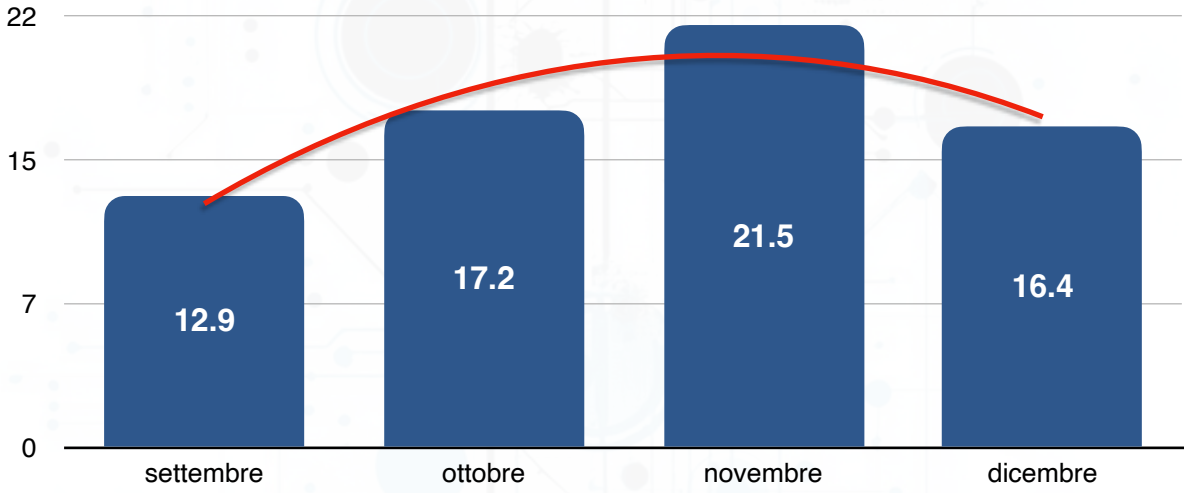


attacchi suddivisi per mese, fonte Ransomfeed.it

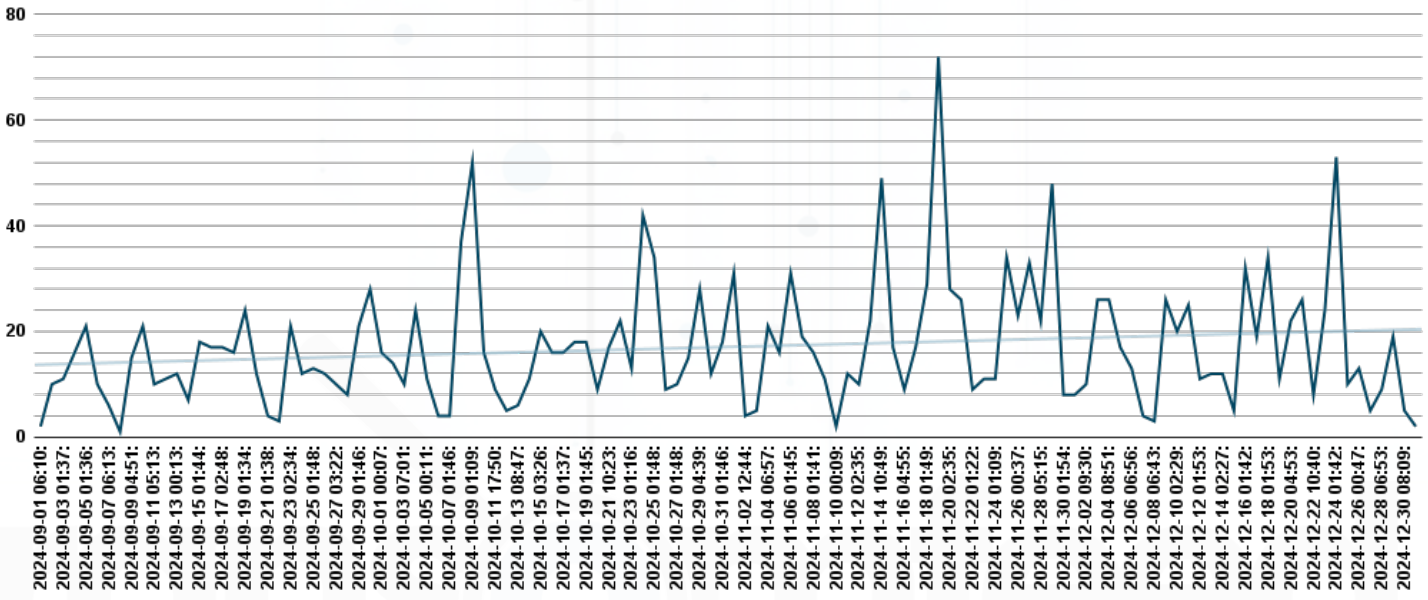
Il **19 novembre** si è registrato il **picco di attività ransomware** del quadrimestre, con ben **72 attacchi** rivendicati in un solo giorno, segno della capacità dei gruppi criminali di sfruttare rapidamente le vulnerabilità digitali. Questo incremento mette in evidenza l'urgenza di colmare le lacune nella sicurezza informatica e di rafforzare le difese contro minacce in continua crescita.

Al contrario, il giorno dell'**8 settembre** si è distinto come il **meno colpito**, con una sola rivendicazione. 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 in crescita di 17 attacchi giornalieri** (il quadrimestre precedente era di 11) 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.



media giornaliera suddivisa per mesi, fonte Ransomfeed.it



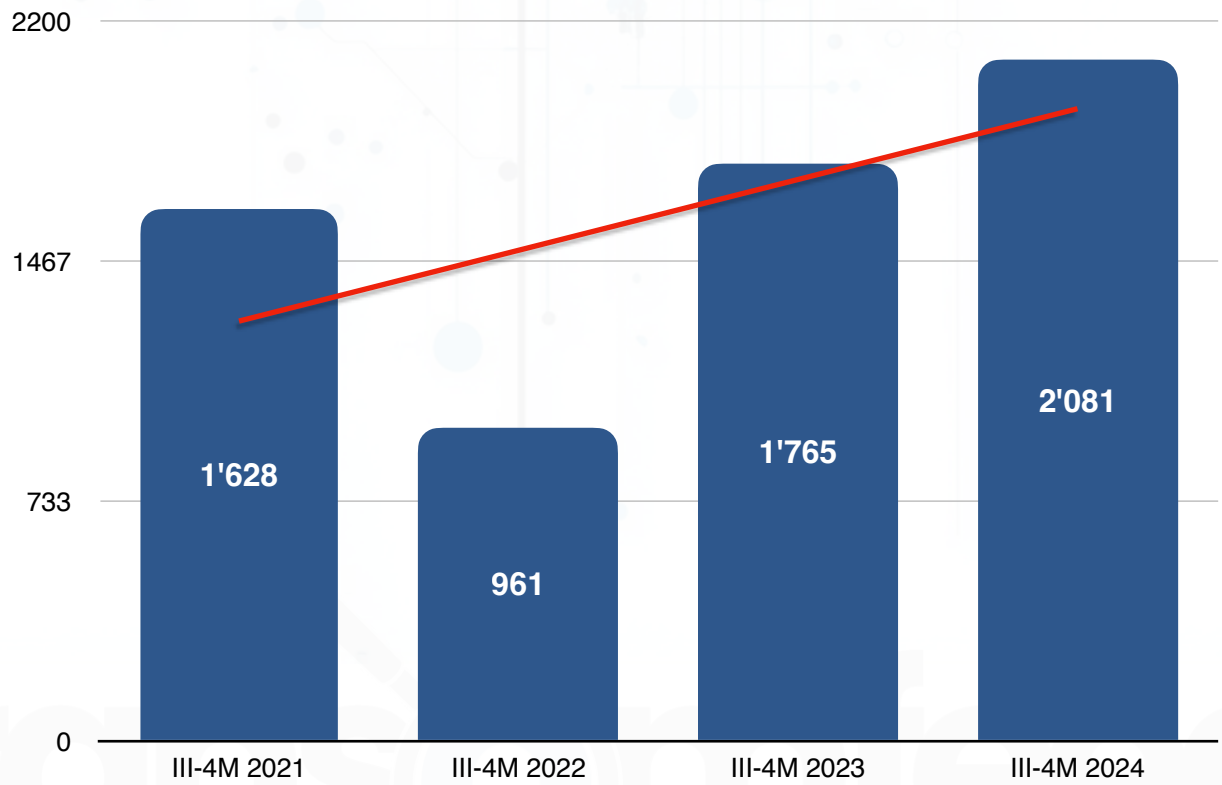
Quadrimestri a confronto

Per contestualizzare i dati della Panoramica, è stato condotto un **confronto** tra il terzo quadrimestre 2024 e i dati dei terzi 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 terzo quadrimestre del 2024 appare significativa e, rispetto agli anni precedenti, il 2024 ha superato il 2023 con un **aumento dell'17.9%**, mentre il confronto con il 2022 evidenzia un **incremento** impressionante del **116.54%**.

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 (che sembrava registrare un crollo degli attacchi) e il 2024** indica un'**escalation particolarmente preoccupante** negli ultimi due anni. Il crollo del 2022 dunque non viene confermato nel tempo, ma purtroppo velocemente recuperato

In sintesi, l'analisi storica offre un altro 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. Ransomfeed mette a disposizione tutte le esportazioni di dati in maniera open, nella sua piattaforma online, utili proprio ad analisi di questo tipo.



fonte Ransomfeed.it

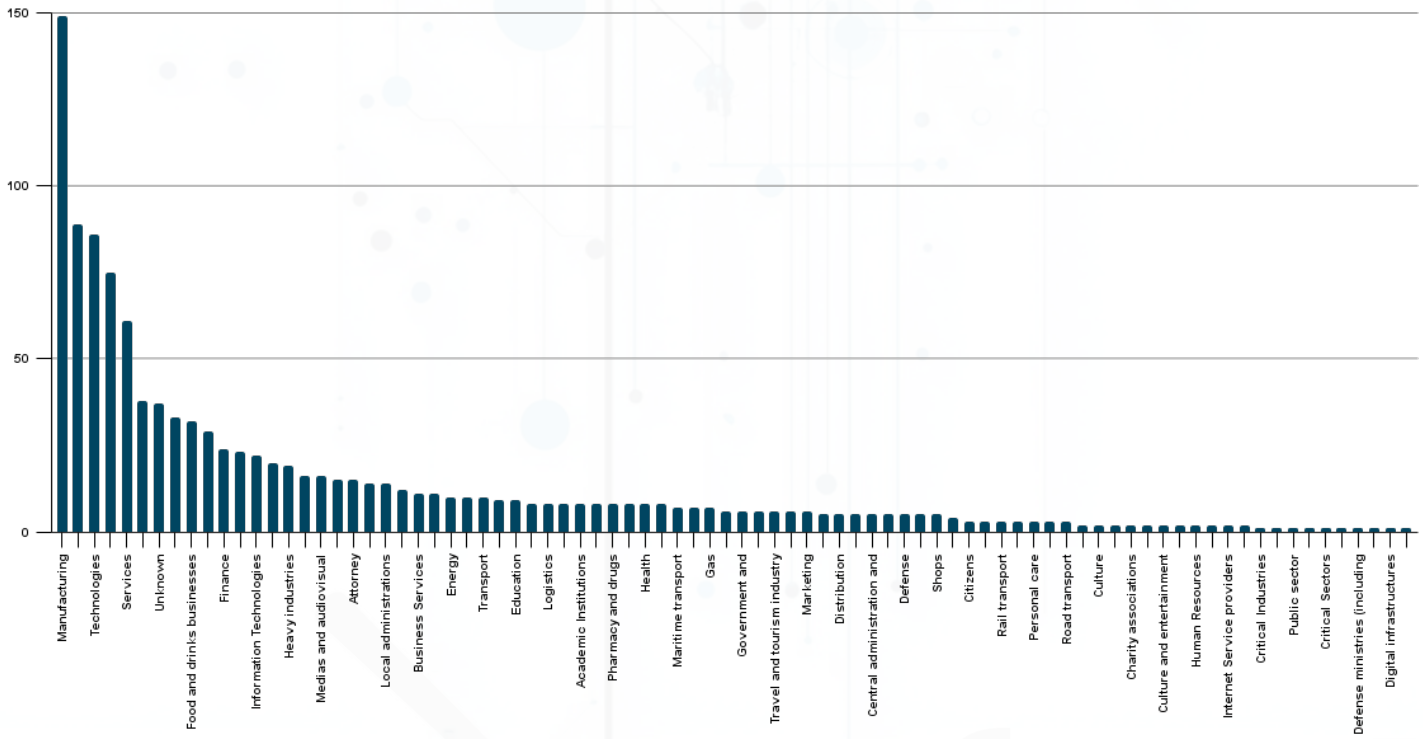
Distribuzione del ransomware nei settori lavorativi

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 che come vediamo rispetto ai precedenti report, restano quasi sempre invariate, a rappresentare il **55% del totale** degli attacchi:

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



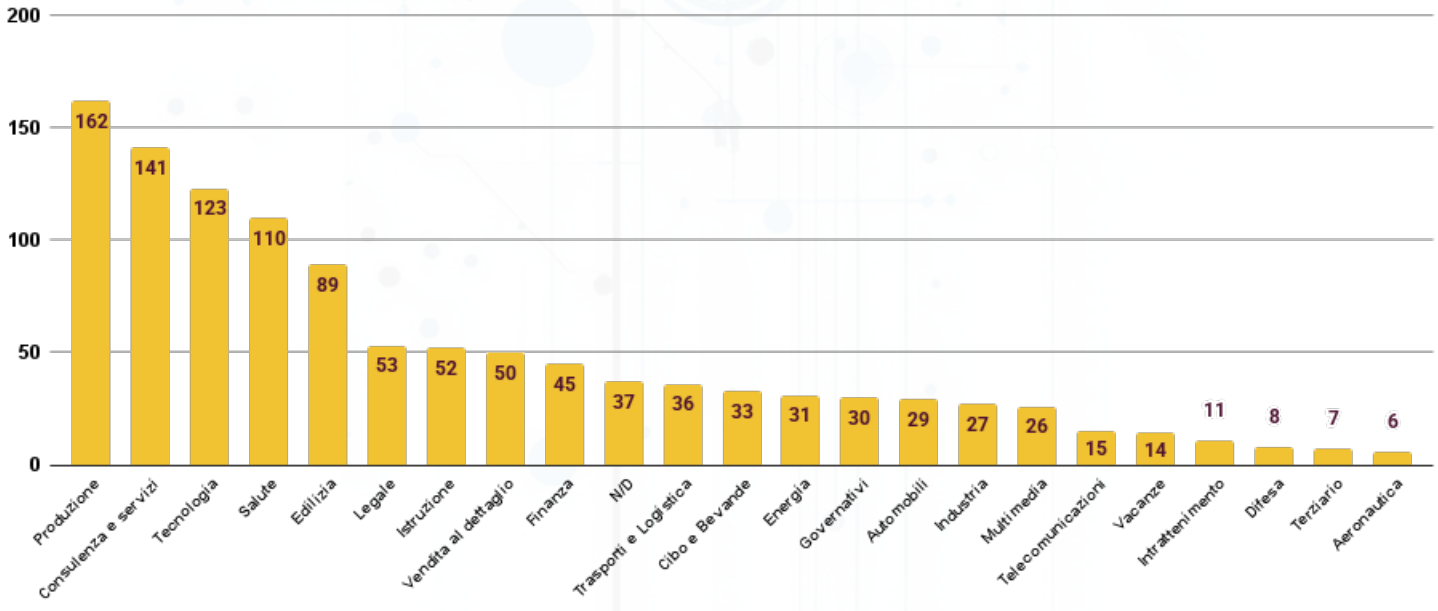
fonte Ransomfeed.it

Le **organizzazioni governative** occupano la **quattordicesima posizione** tra le categorie che impattano sulla sicurezza nazionale, con **30 attacchi** rivendicati nel periodo analizzato; un decremento rispetto al quadrimestre precedente. Il **settore dell'istruzione**, significativo anche per la sicurezza nazionale, si colloca al **settimo posto con 52 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**.

Nel settore educativo 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**.



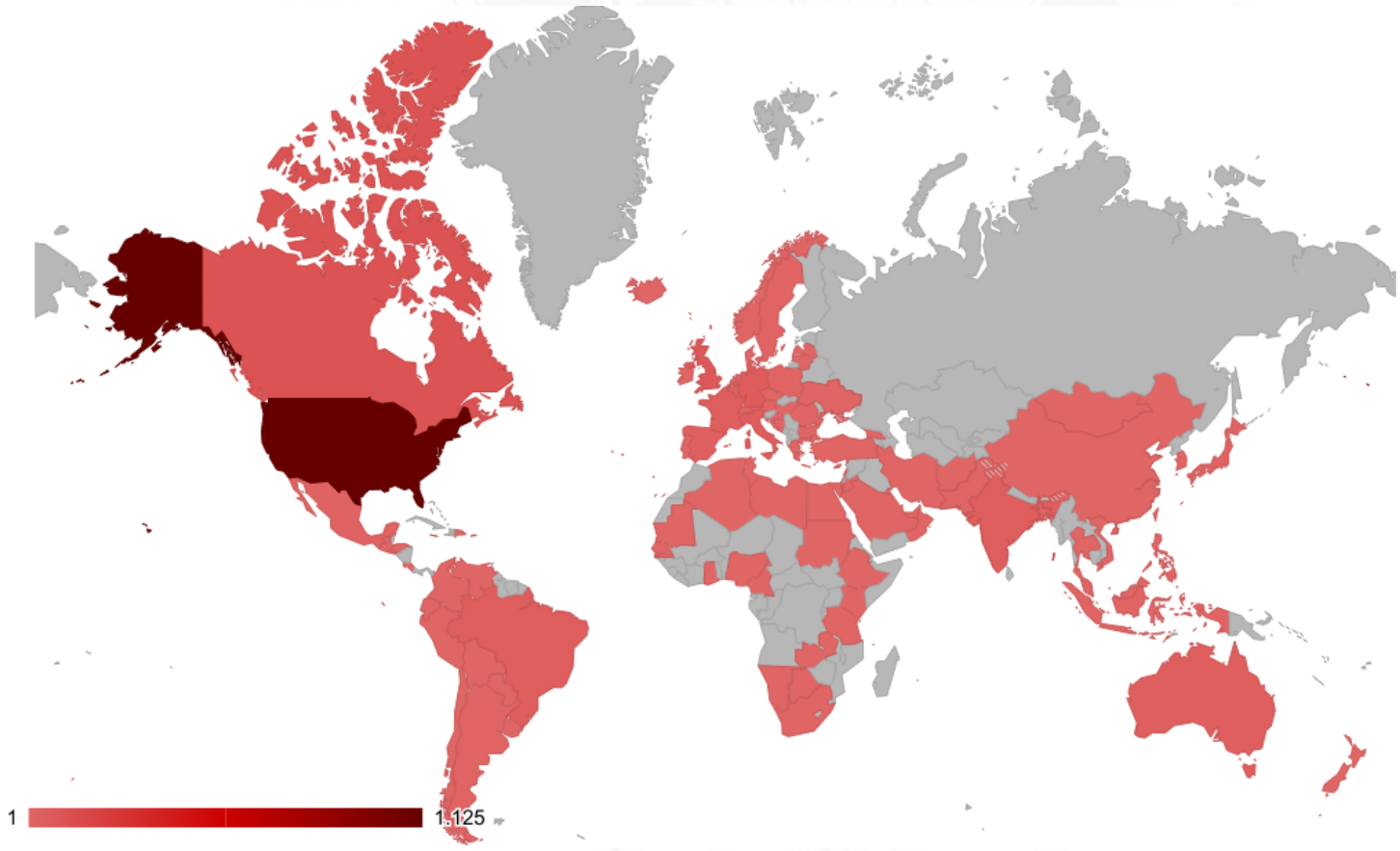
fonte Ransomfeed.it

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 da trend ormai consolidati, la **regione nord-occidentale del mondo** si conferma la **più colpita** dai gruppi criminali. anche se c'è un inizio di tendenza che vede il subentro di alcune regioni tropicali del sud-est asiatico.

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.

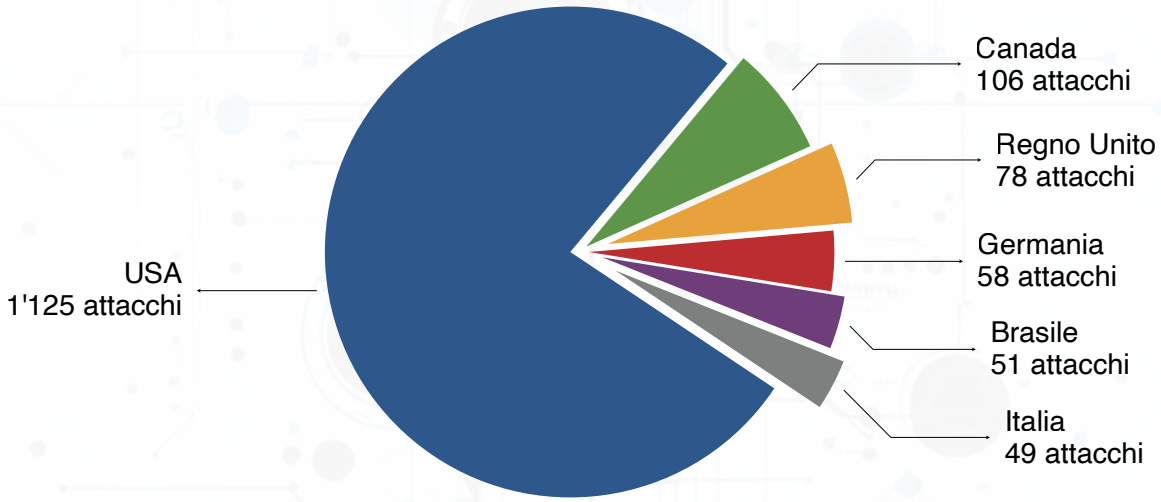
Gli **Stati Uniti** rappresentano una quota significativa degli attacchi, con il **54% del totale**, corrispondente a **1125 rivendicazioni**.

Seguono il **Canada, Regno Unito e Germania**, 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, 54.1%	**Emirati Arabi**, 0.6%	**Malesia**, 0.2%	**Kuwait**, 0.1%
Canada, 5.1%	**Svezia**, 0.6%	**Cile**, 0.2%	**Giamaica**, 0.1%
Regno Unito, 3.7%	**Taiwan**, 0.5%	**Bangladesh** 0.2%	**Cipro**, 0.1%
Germania, 2.8%	**Paesi Bassi**, 0.5%	**Hong Kong**, 0.2%	**Uruguay**, 0.1%
Brasile, 2.5%	**Indonesia**, 0.5%	**Sud Corea**, 0.2%	**Nigeria**, 0.1%
Italia, 2.4%	**Austria**, 0.5%	**Danimarca**, 0.2%	**Croazia**, 0.1%
India, 2.3%	**Rep. Ceca**, 0.4%	**Filippine**, 0.2%	**Namibia**, 0.1%
Francia, 2.2%	**Turchia**, 0.4%	**Pakistan**, 0.2%	**Rep. Dominicana**, 0.1%
Australia, 1.9%	**Sud Africa**, 0.4%	**Portogallo**, 0.2%	**Senegal**, 0.1%
Spagna, 1.6%	**Perù**, 0.4%	**Irlanda**, 0.2%	**Afganistan**, 0.1%
Israele, 1.3%	**Tailandia**, 0.3%	**Egitto**, 0.2%	**Guatemala**, 0.1%
Belgio, 1.1%	**Colombia**, 0.3%	**Lussemburgo**, 0.1%	**Bulgaria**, 0.1%
Non Disponibile, 0.9%	**Norvegia**, 0.3%	**Costa Rica**, 0.1%	**Bosnia**, 0.1%
Messico, 0.8%	**Portorico**, 0.3%	**Vietnam**, 0.1%	**Isole Vergini,** 0.1%
Giappone, 0.7%	**Nuova Zelanda**, 0.3%	**Bolivia**, 0.1%	**Iran**, 0.1%
Argentina, 0.6%	**Romania**, 0.3%	**Venezuela**, 0.1%	**Kenya**, 0.1%
Svizzera, 0.6%	**Grecia**, 0.3%	**Lituania**, 0.1%	**Georgia**, 0.1%
Singapore, 0.6%	**Cina**, 0.2%	**Tunisia**, 0.1%	**Ghana**, 0.1%
Polonia, 0.6%	**Oman**, 0.2%	**Libano**, 0.1%	**Finlandia**, 0.1%

fonte Ransomfeed.it

Nel **terzo quadrimestre** del 2024, l'**Italia** si posiziona al **sesto posto con 49 attacchi**, segnando un **decremento** rispetto ai periodi precedenti.



fonte Ransomfeed.it

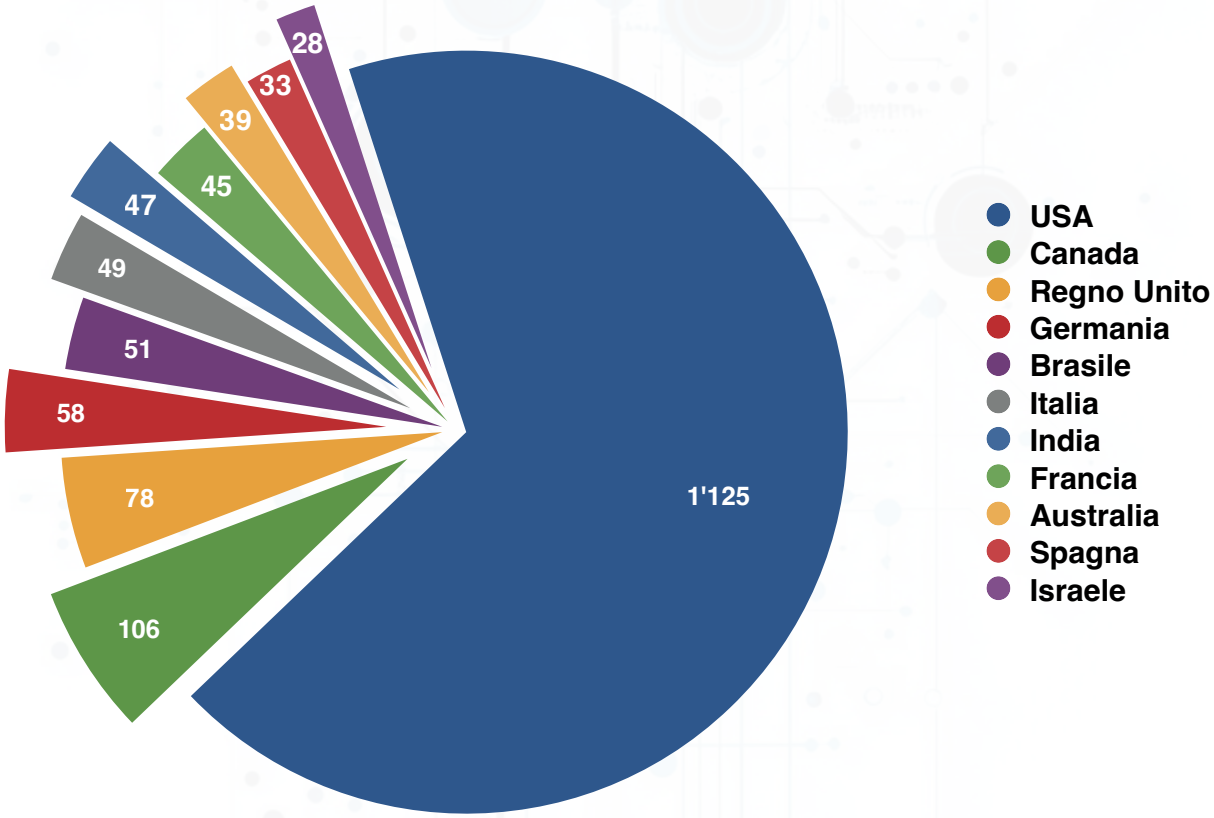
L'**impatto degli attacchi** ransomware sulle economie dei paesi colpiti è spesso devastante, comportando un **notevole dispendio di risorse** sia economiche sia umane. **Interruzioni della produttività** che durano giorni o settimane, **paralisi nelle operazioni** di approvvigionamento e nella gestione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

Gli aspetti economici e del pagamento dei riscatti sono la principale molla, che alimenta questi attacchi e del perché ancora non li si vede diminuire

Top 10

Anche nel **terzo 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, ..).

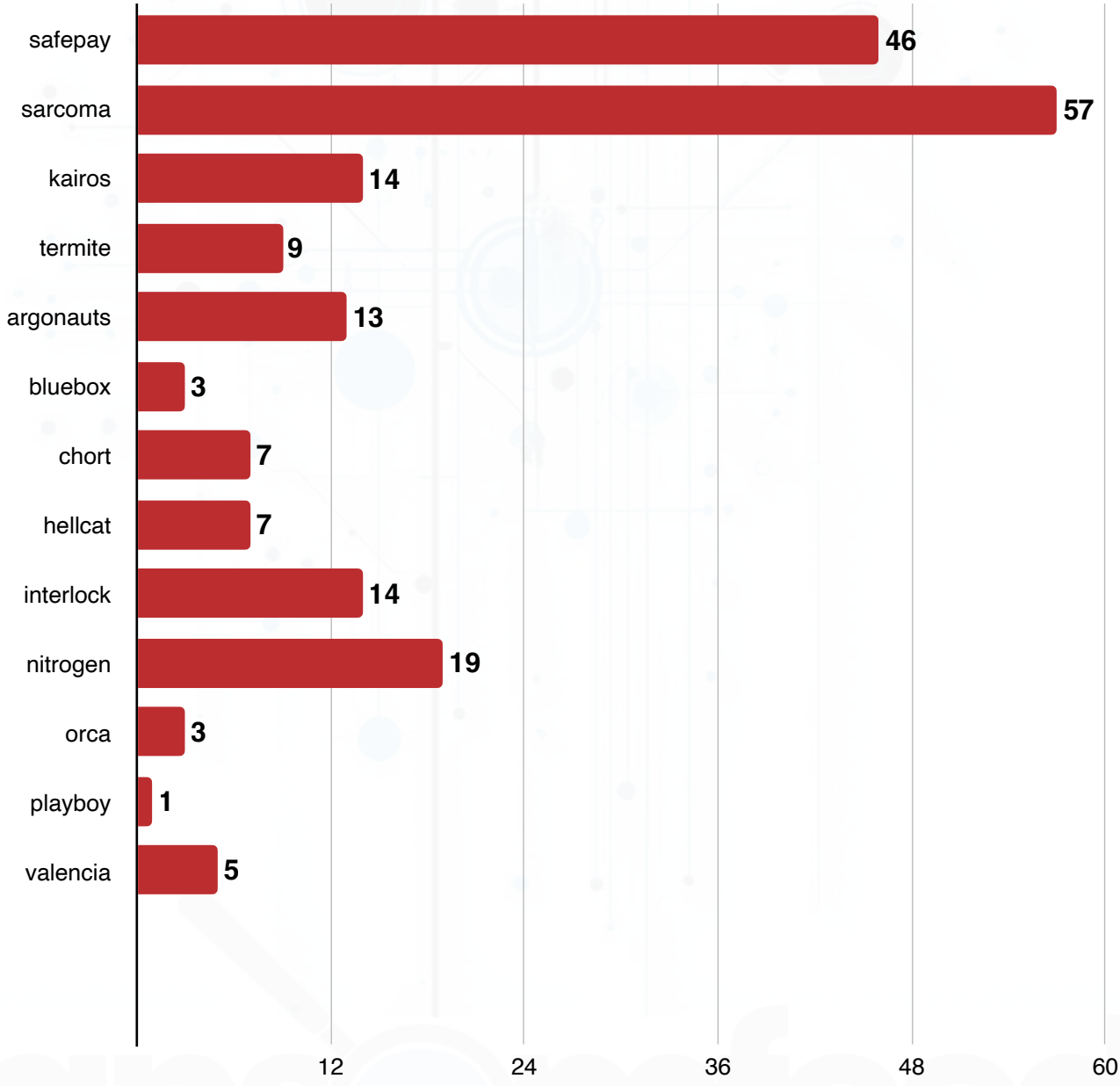
I criminali comprendono che **colpire aziende e istituzioni** americane può generare **ripercussioni a livello mondiale**, destabilizzando mercati e innescando effetti a catena in diverse industrie.

Nuovi gruppi criminali

Nel **terzo 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.

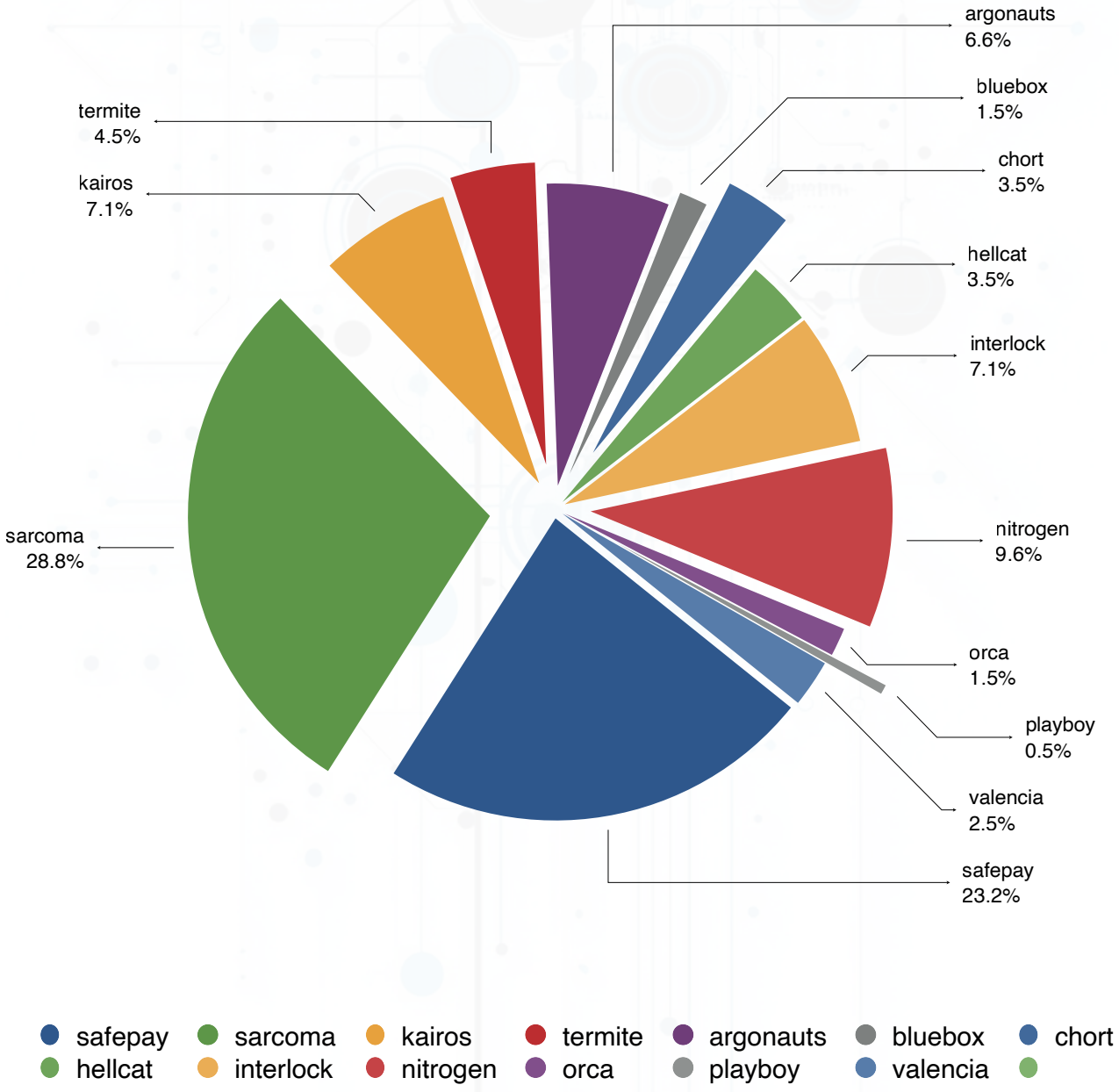
In totale, sono stati registrati **198 nuovi attacchi** ransomware rivendicati, provenienti da **13 gruppi criminali** distinti.

Tra questi, **Sarcoma** si distingue come la cybergang **più attiva** del terzo quadrimestre, con il **28.8% 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

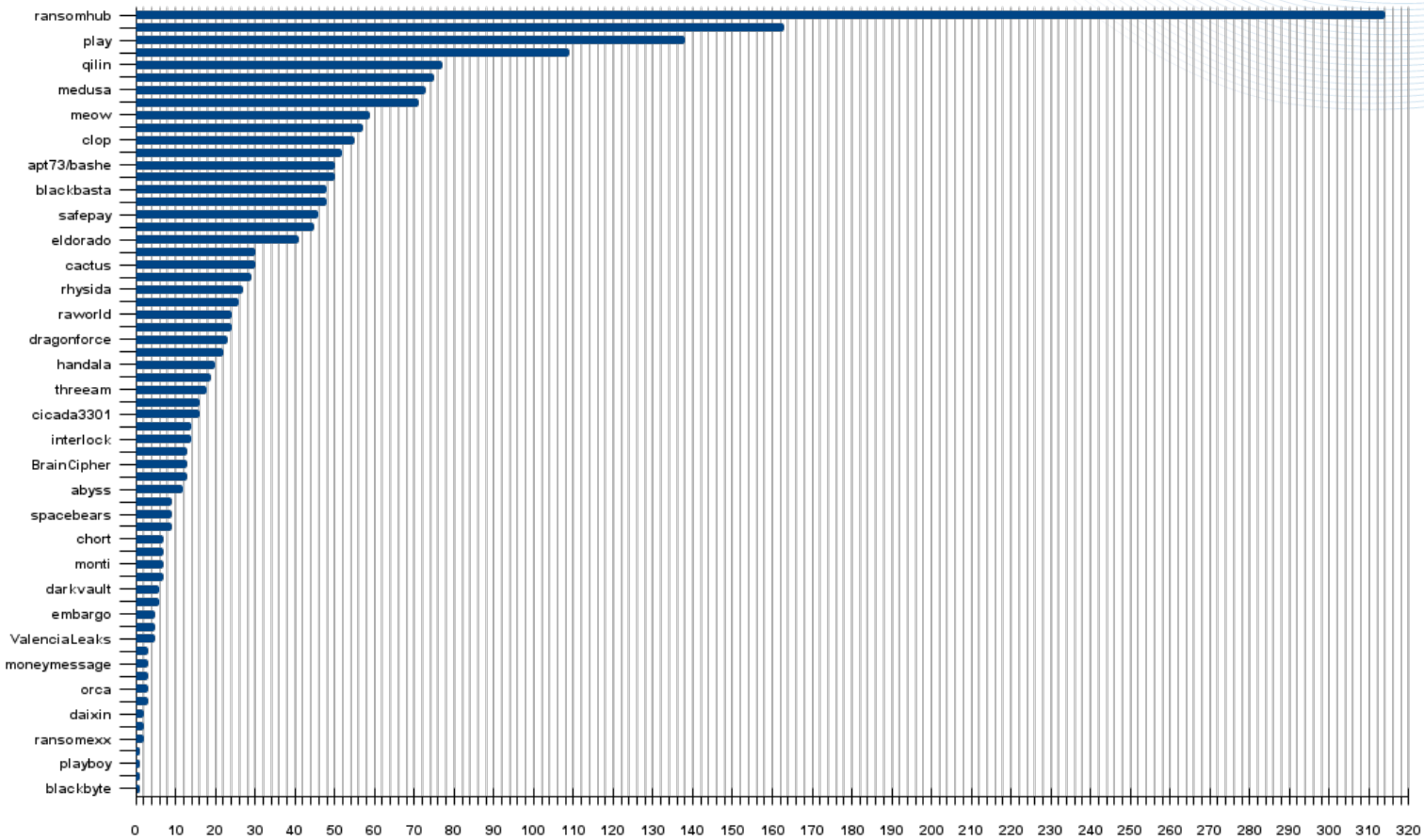
Le attività globali dei gruppi ransomware

Abbiamo analizzato i gruppi che hanno generato attività in questa fase conclusiva 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**, nel periodo in analisi sono necessarie le azioni di **otto gang** estremamente attive per rappresentare insieme il **50% degli attacchi totali** registrati. Una leadership meno netta del periodo precedente, che invece vedeva la metà degli attacchi ripartiti in soli 5 gruppi criminali.

- **ransomhub**: questa fase dell'anno lo vede leader indiscusso con il **15.1% degli attacchi**, in crescita rispetto al II-4M 2024
- **akira**: con il **7.8% degli attacchi**, si posiziona come il secondo gruppo più attivo
- **play**: responsabile del **6.6% degli attacchi**, al terzo posto
- **killsec**: con il **5.2% degli attacchi**
- **qilin**: registra al suo attivo il **3.7% degli attacchi**
- **hunters**: chiude il gruppo di testa con il **3.6% degli attacchi**
- **medusa**: chiude il gruppo di testa con il **3.5% degli attacchi**
- **fog**: chiude il gruppo di testa con il **3.4% degli attacchi**

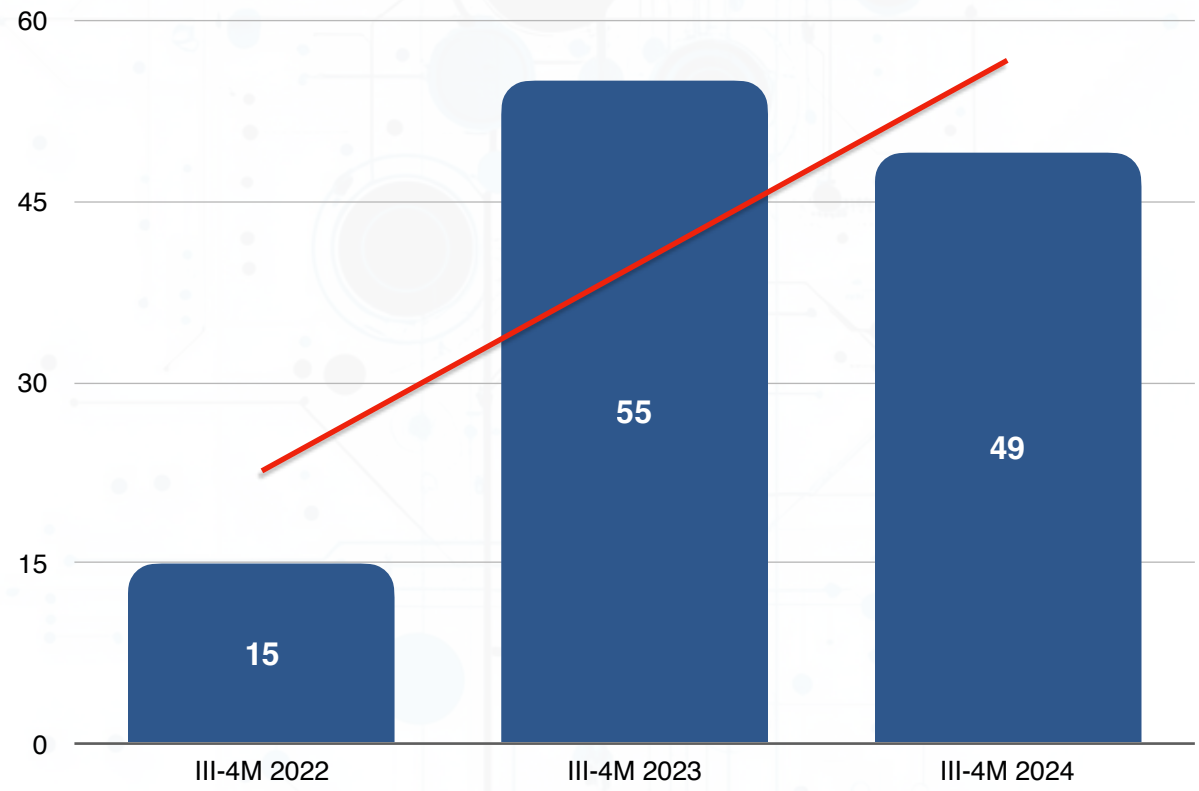
Gli altri gruppi non menzionati sono risultati **inattivi**, nel terzo quadrimestre del 2024, in alcuni casi può essere una sospensione temporanea delle attività, in altri casi è responsabilità di una riorganizzazione interna post law enforcement.



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 **49 attacchi**, equivalenti a poco meno 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 lieve decremento del 11% rispetto allo stesso periodo dell'anno precedente.
L'**incremento percentuale** degli attacchi dal 2022 al 2024 è **del 226%**.

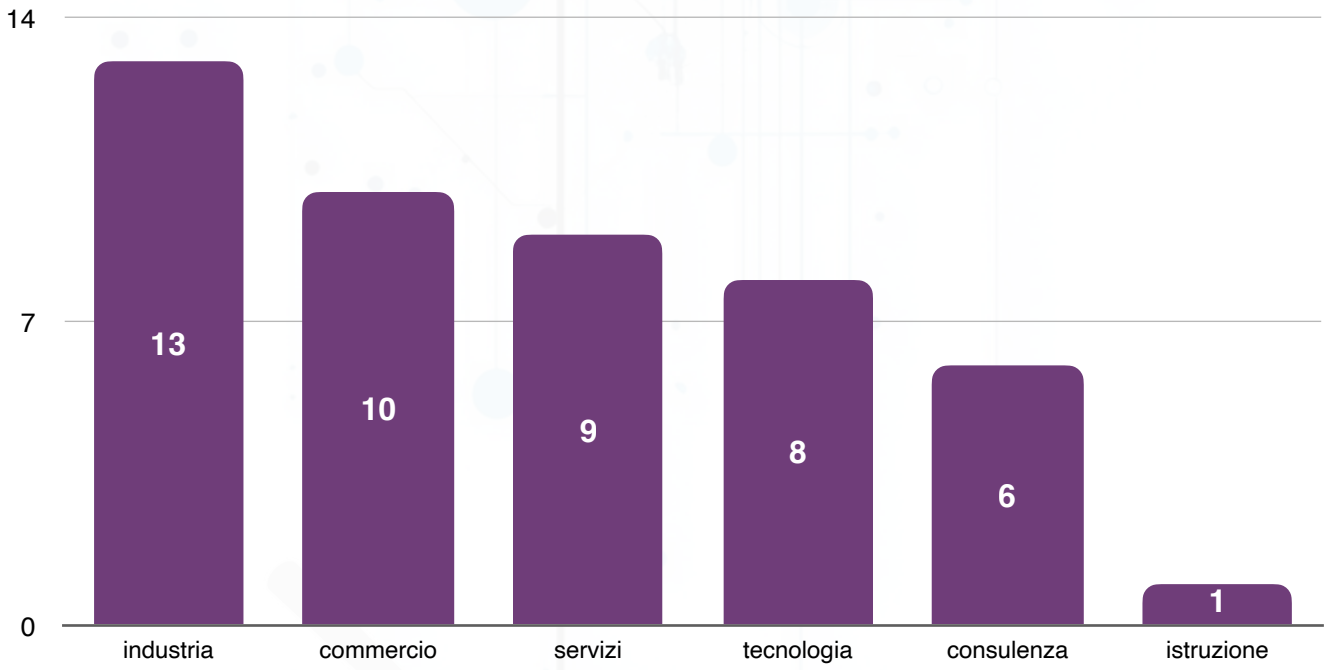
Confrontando questi dati con quelli globali, otteniamo una visione più completa del panorama delle minacce ransomware e delle tendenze emergenti. Inoltre, grazie a un'analisi specifica, possiamo estrarre **informazioni preziose** per valutare lo stato di salute delle aziende e delle istituzioni, nonché 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 terzo quadrimestre del 2024, questi settori hanno subito **rispettivamente 13** e **10 attacchi** ransomware. All'interno del **settore industriale**, le industrie **meccaniche**, **metallurgiche** ed **elettroniche** sono state particolarmente vulnerabili. Anche i **servizi**, hanno subito numerosi attacchi, facendo ricomprendere in questa categorie anche gli attacchi a società sportive di livello nazionale.

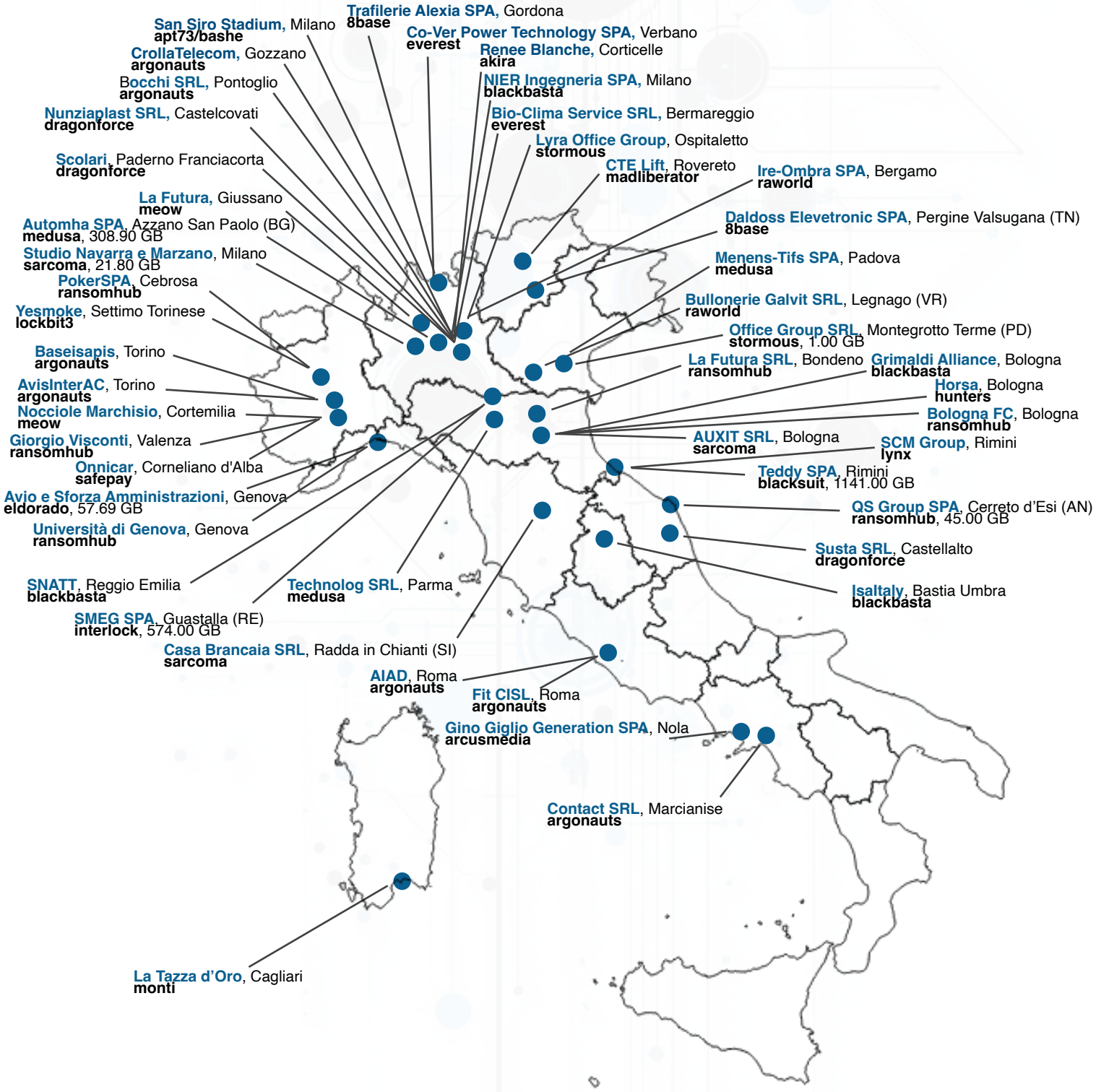
Seguono i settori della **tecnologia**, della **consulenza**, e **istruzione**, che insieme si spartiscono il restante 30% degli attacchi. È evidente che questi settori siano i più bersagliati a causa dell'elevato valore dei dati che gestiscono e della criticità delle loro operazioni, che li rende altamente suscettibili alle richieste di riscatto.

- 🏭 **industria**, 26.5%
- 🤝 **commercio**, 20.4%
- 🔌 **servizi**, 18.4%
- 🖥️ **tecnologia**, 16.3%
- 💼 **consulenza**, 12.2%
- 🏫 **istruzione**, 2.0%



fonte Ransomfeed.it

La distribuzione del ransomware nel territorio



fonte Ransomfeed.it

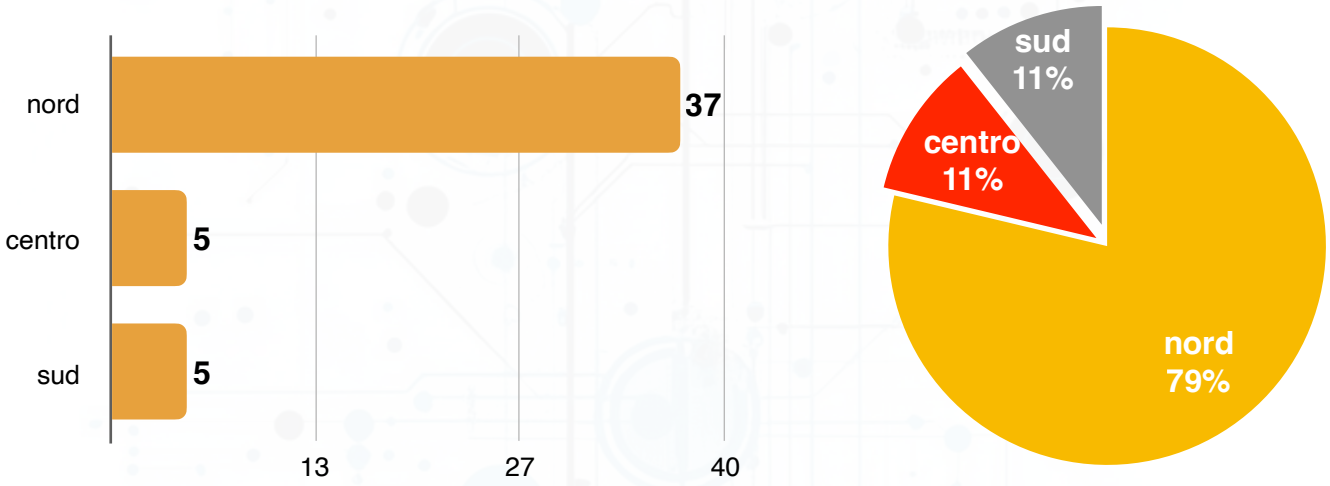
Grazie ai dati sulla **localizzazione** delle vittime raccolti su Ransomfeed, siamo stati in grado di creare una mappa che illustra la **distribuzione geografica degli attacchi** ransomware in Italia per il terzo quadrimestre del 2024.

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 **75% 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

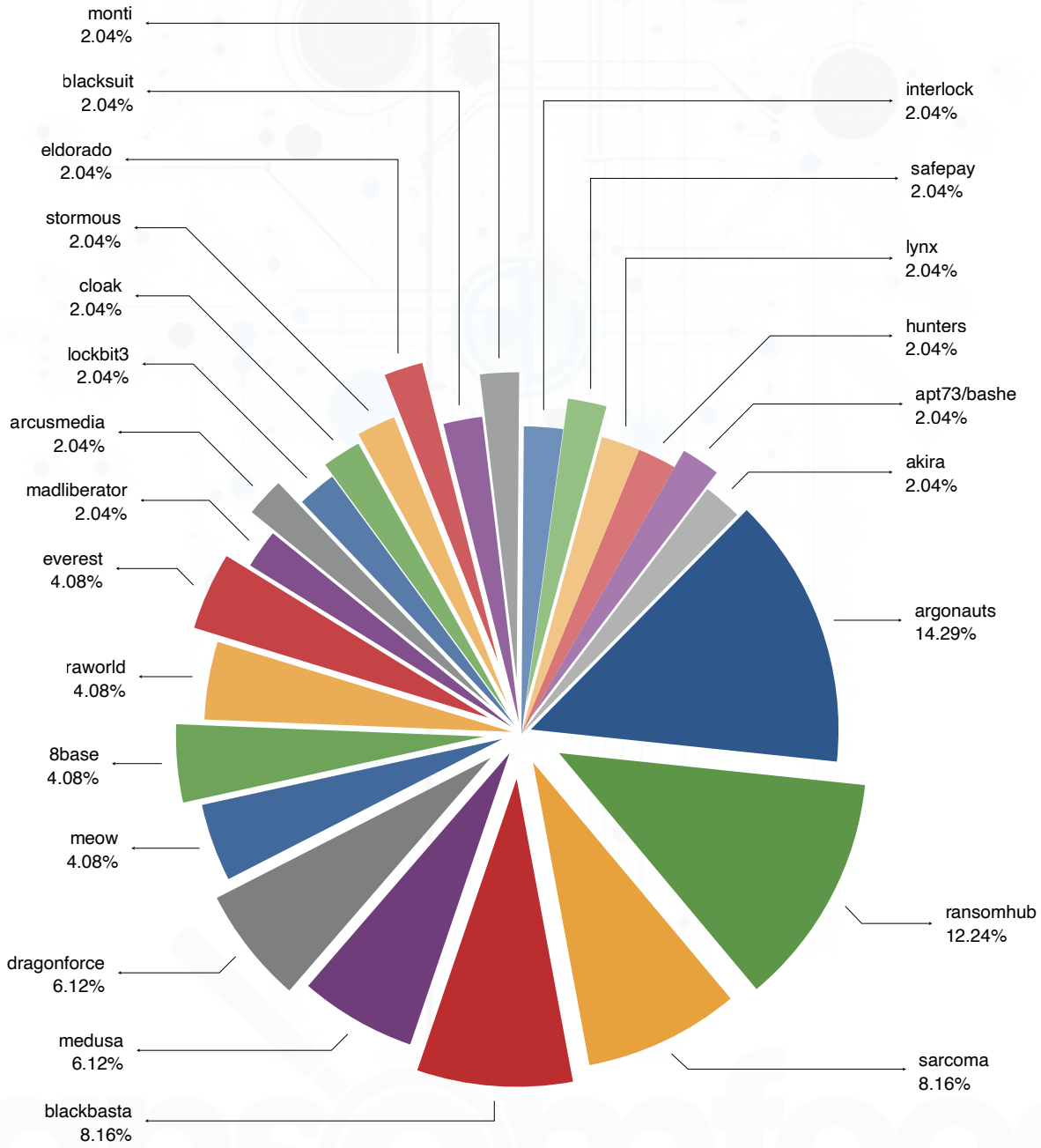
Il **confronto tra il sud e il nord Italia** rivela differenze significative.
Nel sud, la **densità industriale è minore**, con un'economia prevalentemente basata su agricoltura, pesca, turismo e industria leggera. Al contrario, il nord Italia vanta una **consolidata tradizione di sviluppo economico**,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

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 terzo 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 **argonauts** si è attestato come il secondo **più attivo in Italia** durante questo periodo, con il **14% degli attacchi totali**. Mentre invece il gruppo **ransomhub** che nel nazionale è il primo gruppi, in Italia diventa il secondo con il **12% degli attacchi**.

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



fonte Ransomfeed.it

Conclusione

Complessivamente, sono stati **monitorati 235 gruppi** criminali operanti a livello globale, con **2081 rivendicazioni ransomware**, di cui **49 in Italia**.

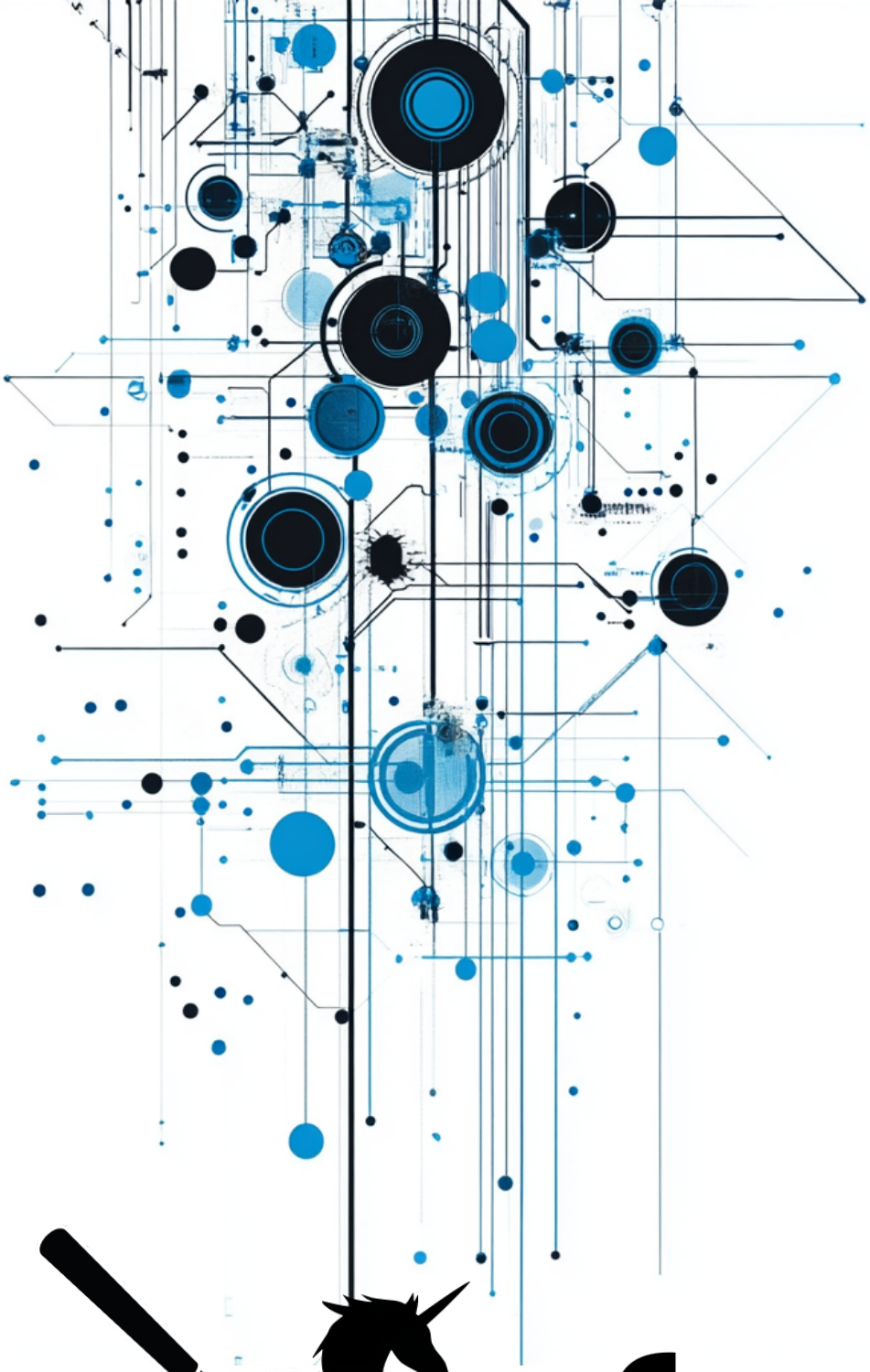
In sintesi:

- sono stati **monitorati 235 gruppi** criminali, per un **totale di 2.081 rivendicazioni globali** e **49 in Italia**;
- i settori più colpiti sono stati la **produzione**, **l'industria** e la **consulenza**, per una fetta pari al **38% del mercato ransomware**;
- le **organizzazioni governative** si sono posizionate al **14° 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**, lo si nota anche dal crescente rafforzamento delle frodi economiche a danni di cittadini. Ci sono **gap importanti** non colmati, che stanno aprendo la strada sempre più a rischi per tutti, dal semplice phishing, alle **frodi bancarie** viste di recente.

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.



ADVANCED **DATADRIVEN** CYBERNEWS

REPORT QUADRIMESTRALE
III-4M 2024