ransomfeed

ADVANCED **DATADRIVEN** CYBERNEWS

RECAP MENSILE

NOVEMBRE 2025

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.

Il recap mensile

Lo storico **report quadrimestrale** è momentaneamente sospeso per difficoltà di aggiornamento costante. Questo dunque resta per ora l'unico documento di reportistica diffuso dalla piattaforma. Riteniamo fondamentale offrire un riassunto più frequente delle vittime e della gravità degli incidenti informatici, insieme a molti altri dati statistici, che continueranno a essere disponibili sulla piattaforma.

I nostri contatti

La piattaforma è sempre accessibile al sito ransomfeed.it, ci trovate inoltre sui canali social:

- 🟩 linkedin.com/company/ransomfeed
- 🟩 x.com/ransomfeednews
- 🟩 t.me/RansomFeedNews
- 🟩 bsky.app/profile/ransomfeed.rfeed.it
- 🟩 facebook.com/ransomfeed
- 🟩 https://poliversity.it/@ransomfeed

ChangeLog novembre 2025

Ransomfeed è in continua evoluzione, nello specifico ci sono piccoli cambiamenti o migliorie che vengono sviluppati di continuo nei giorni. Normalmente se ne richiama l'attenzione nei nostri canali social, ma qui si fa un sommario per raggruppare gli ultimi cambiamenti e novità introdotte.

- Nel mese di riferimento non sono state registrate modifiche al core della piattaforma

Focus Italia 🇮🇹

Nel mese di **novembre 2025** la piattaforma ha rilevato un totale di **11 attacchi**.
Si fa notare che il mese di novembre 2025 vede una flessione del 35% rispetto allo stesso periodo dell'anno precedente (novembre 2024: 17 rivendicazioni).

Il dettaglio sui dati pubblicati è soggetto a costanti aggiornamenti e integrazioni (molti dati qui a 0, vedranno una pubblicazione nei prossimi giorni o settimane), per avere dati correttamente aggiornati seguirne l'andamento su ransomfeed.it

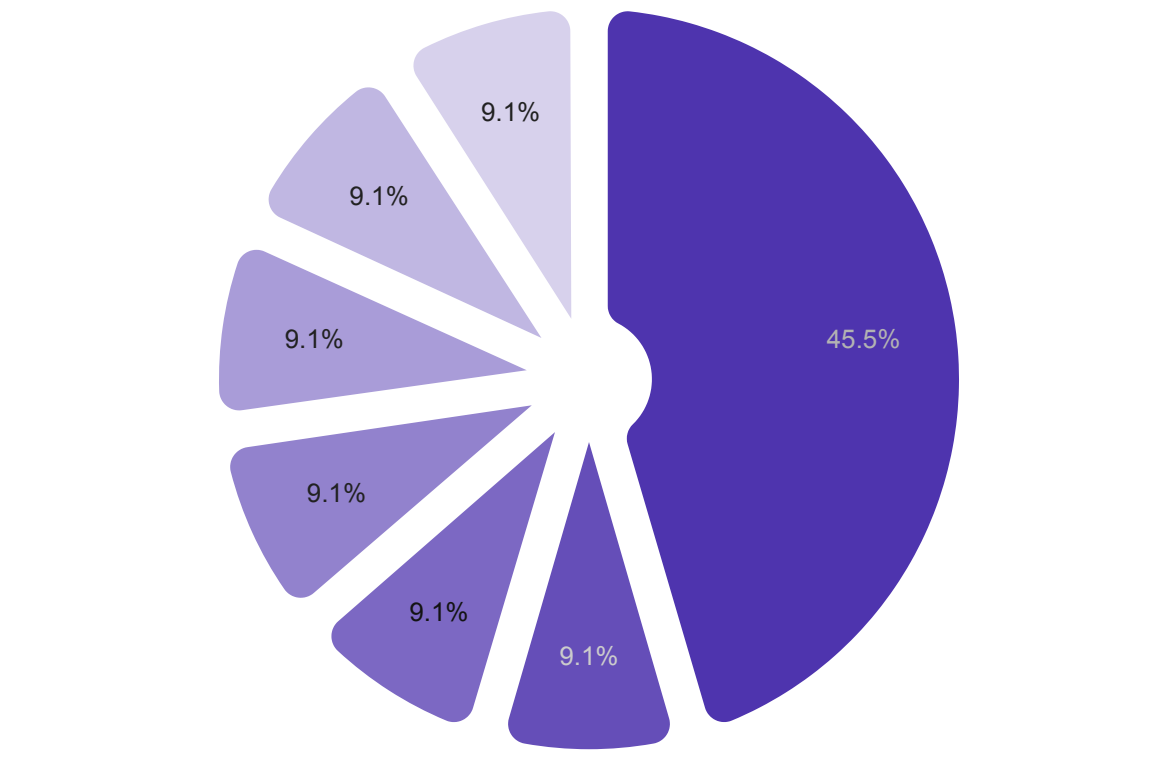
Vittime Italia	Totale GB pubblicati
11	1.801,24

	ID ▲	GRUPPO	VITTIMA	DATI PUBBLICATI GB
1.	26940	qilin	Studio Corvo Parma	42
2.	26973	dragonforce	Ponzini S.p.A.	314.24
3.	27008	everest	SIAD	1059
4.	27038	ransomhouse	Fulgar S.p.A.	0
5.	27056	incransom	galileo.it	286
6.	27074	qilin	Viabizzuno	0
7.	27148	qilin	FREEDL GROUP s.r.l.	100
8.	27205	safepay	istitutocomprensivo-cavaglia.edu.it	0
9.	27401	thegentlemen	Talarico	0
10.	27539	qilin	Battaglioli	0
11.	27542	qilin	ILCA Targhe s.r.l.	0

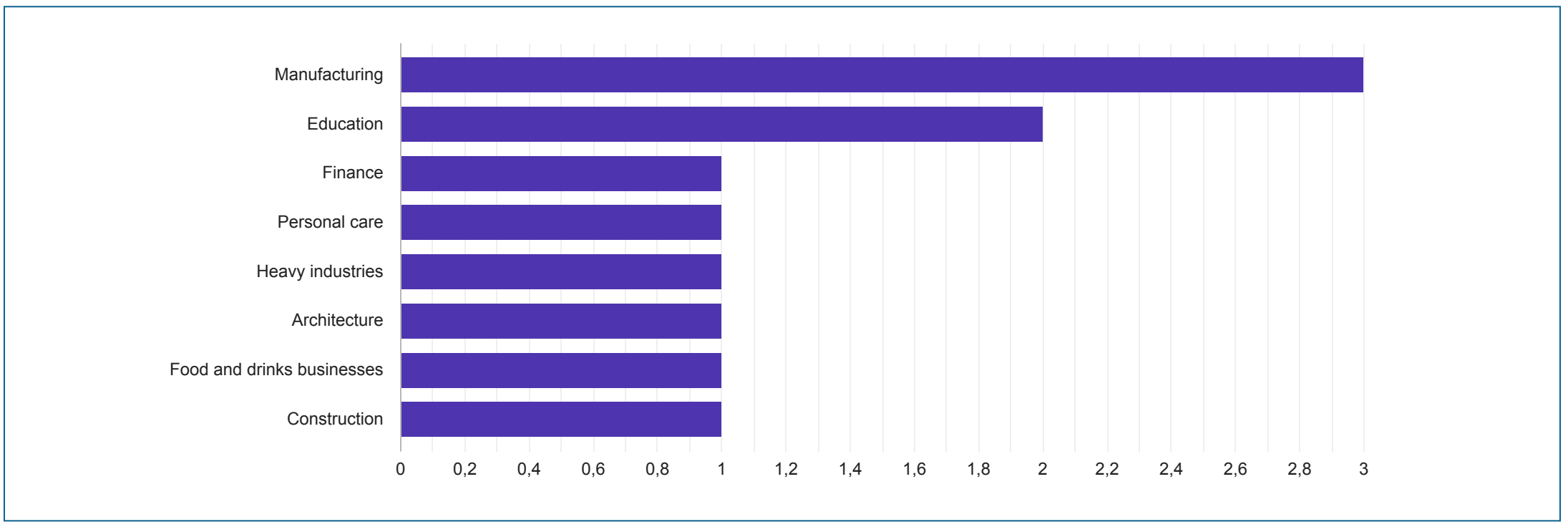
Gruppi criminali
focus Italia

Il grafico e la tabella qui sotto riportano i dati dei gruppi criminali coinvolti negli attacchi ransomware verso target italiani, nel mese di **novembre 2025**.
Mentre invece in fondo si trova la distribuzione dei settori economici.

	GRUPPO	VITTIME
1.	qilin	5
2.	dragonforce	1
3.	everest	1
4.	ransomhouse	1
5.	incransom	1
6.	safepay	1
7.	thegentlemen	1



Settori economici
focus Italia



Ransomware Story

Come il ransomware ha messo in ginocchio il gigante giapponese Asahi

Asahi è diventato il caso-scuola di novembre 2025: un singolo attacco ransomware ha fermato la birra più famosa del Giappone, costretto un colosso industriale al ritorno a carta e fax e messo a rischio i dati di quasi 2 milioni di persone. È l'episodio che meglio racconta come il ransomware oggi sia capace di colpire insieme disponibilità operativa, supply chain e privacy, trasformando un "incidente IT" in una crisi nazionale dei consumi.

Dal "system failure" alla crisi della birra

Il 29 settembre 2025 Asahi rileva un'anomalia nei sistemi del data center giapponese e parla inizialmente di "system failure" che impatta ordini, spedizioni e call center. Nel giro di poche ore l'azienda è costretta ad ammettere un attacco ransomware che blocca la produzione in diversi stabilimenti domestici e rende impossibile gestire ordini e spedizioni via canali digitali.

Il risultato è tangibile sugli scaffali: i retailer e le catene di convenience store (7-Eleven, FamilyMart, Lawson) iniziano a segnalare carenze di Asahi Super Dry e altre bevande, mentre il produttore posticipa il lancio di 12 nuovi prodotti per l'impossibilità di orchestrare correttamente logistica e promozioni. L'impatto resta confinato al Giappone sul piano operativo, ma la vicenda diventa rapidamente globale perché Asahi controlla anche brand europei come Peroni e la community internazionale della sicurezza segue il caso come ennesimo esempio di ransomware "a catena del freddo".

Qilin, quattro ore di vantaggio e 27 GB di dati

Nel giro di pochi giorni il gruppo ransomware Qilin rivendica l'operazione, sostenendo di aver sottratto 27 GB di dati prima della cifratura e minacciando la pubblicazione sul proprio leak site. Secondo le ricostruzioni tecniche, gli attaccanti entrano da apparati di rete compromessi in un sito separato, si muovono lateralmente verso il data center principale e, nello stesso giorno, distribuiscono il payload di cifratura su più server e PC connessi.

Il dettaglio più interessante per chi si occupa di difesa è la finestra temporale: Asahi dichiara di aver isolato il data center entro quattro ore dalla scoperta, ma le analisi forensi mostrano che gli aggressori avevano già stabilito persistenza, esfiltrato i dati e avviato il processo di cifratura. È una dinamica che conferma quanto la "golden hour" del ransomware sia stata compressa: quando l'incidente diventa visibile ai team interni, spesso la fase di data theft è già conclusa e la negoziazione si gioca su un doppio ricatto (ripristino + non pubblicazione).

Dalla fabbrica al fax: impatto operativo

Sul piano OT/operativo l'attacco azzera di fatto i flussi digitali di ordine, spedizione e customer service in Giappone, costringendo Asahi a un rollback manuale fatto di telefono, fax e ordini scritti a mano. In alcuni stabilimenti la produzione riparte gradualmente, ma senza i sistemi di orchestrazione automatica la capacità resta limitata e l'azienda non riesce a stimare con precisione i tempi per il pieno ripristino.
Per contenere l'incidente Asahi isola il data center colpito, ingaggia esperti esterni e notifica le autorità, mentre comunica a partner e retailer l'impossibilità di evadere gli ordini secondo le normali finestre SLA. La complessità dell'evento è tale che l'azienda decide di rinviare parte della reportistica finanziaria al 2026, segno che la dimensione cyber è ormai profondamente intrecciata con disclosure di bilancio e aspettative degli investitori.

La seconda ondata: quasi 2 milioni di identità esposte

Se a ottobre la narrativa è ancora centrata sul blocco della produzione, tra fine novembre e inizio dicembre arriva la seconda onda: Asahi comunica che i dati personali di circa 1,5–1,9 milioni di persone possono essere stati compromessi. Nelle cifre rientrano circa 1,5 milioni di clienti che avevano contattato i customer service, oltre 100 mila tra dipendenti attuali ed ex, 168 mila familiari di dipendenti e oltre 100 mila contatti esterni come partner commerciali o destinatari di comunicazioni formali.
Il data set comprende nomi, recapiti, date di nascita e altre informazioni personali, mentre l'azienda ribadisce che i dati di pagamento non risultano coinvolti.

Questo però non riduce il livello di rischio: combinazioni di anagrafiche e contatti sono perfette per campagne di phishing mirato, frodi di identità e reset malevoli di account basati su domande di sicurezza o procedure di recupero.

Perché Asahi è il “case study” del 2025
Nel contesto giapponese, la polizia nazionale registra nel primo semestre 2025 un numero di incidenti ransomware in linea con i massimi storici, con una crescente percezione che le aziende del Paese rappresentino target appetibili per difese ancora immature e una certa propensione a negoziare. Asahi diventa il simbolo di questa tendenza perché incarna tutto quello che un moderno attacco ransomware può scatenare: stop della supply chain, shortage di prodotto, data breach di massa, ritardi finanziari e crisi reputazionale del marchio più iconico del mercato locale.

Il caso è un’illustrazione concreta di tre messaggi chiave:
- la **perimetrazione** classica non basta se il punto d’ingresso è un apparato di rete periferico gestito in modo debole;
- la resilienza operativa richiede piani B realmente testati tra IT e OT, altrimenti il ritorno a carta e fax è più una resa che un esercizio di continuità;
- senza telemetria profonda e capacità di detection precoce, le “quattro ore di risposta” rischiano di arrivare quando il danno – tecnico, operativo e di dati – è già pienamente compiuto.

In altre parole, Asahi non è solo la storia della birra che manca dagli scaffali: è il promemoria mensile, per ogni board, che il ransomware del 2025 è una minaccia sistemica, capace di mettere in crisi allo stesso tempo produzione, fiducia dei clienti e trasparenza verso il mercato.

Fonti:

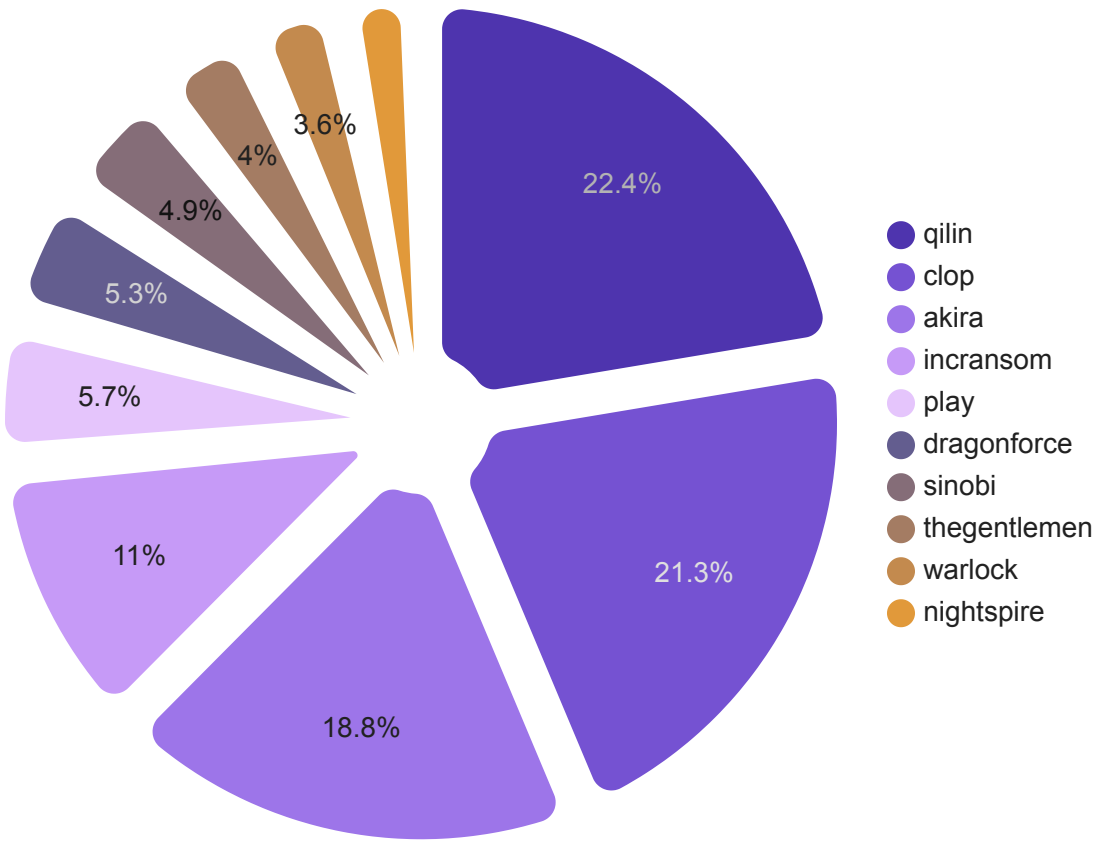
https://www.bbc.com/news/articles/cly64g5y744o
https://www.rescana.com/post/asahi-group-holdings-ransomware-attack-2025-digital-order-system-disrupted-nationwide-beer-shortag
https://breached.company/asahi-group-holdings-breach-investigation-reveals-1-9-million-affected-as-qilin-ransomware-dominates-2025-attack-landscape/
https://www.cnn.com/2025/09/30/asia/japan-asahi-cyberattack-production-halt-intl-hnk
https://www.bbc.com/news/articles/ce86n44178no
https://securityaffairs.com/185126/data-breach/asahi-says-crooks-stole-data-of-approximately-2m-customers-and-employees.html
https://www.nbcnews.com/world/asia/japan-cyberattack-shortage-asahi-beer-rcna235352
https://www.asahigroup-holdings.com/en/newsroom/detail/20251003-0204.html
https://www.independent.co.uk/asia/japan/japan-asahi-beer-cyberattack-data-leak-b2836220.html
https://www.reuters.com/technology/japans-beer-giant-asahi-group-cannot-resume-production-after-cyberattack-2025-09-30/
https://sg.news.yahoo.com/hackers-halt-production-japan-biggest-061340305.html
https://www.rescana.com/post/asahi-group-holdings-ransomware-attack-qilin-breach-disrupts-japanese-operations-and-exposes-1-5-mi
https://www.theregister.com/2025/11/27/asahi_ransomware_numbers/
https://industrialcyber.co/ransomware/qilin-hackers-claim-responsibility-for-asahi-cyberattack-allege-theft-of-27-gb-of-data-amid-ongoing-investigation/
https://shieldworkz.com/reports/decoding-the-asahi-brewery-ransomware-attack
https://www.reuters.com/world/asia-pacific/cybercriminals-claim-hack-japans-asahi-group-2025-10-07/
https://cybersecurefox.com/en/asahi-ransomware-attack-data-breach-japan/
https://www.bbc.com/news/articles/c0rpwk51qxro
https://www.bitdefender.com/en-us/blog/hotforsecurity/asahi-cyber-attack-spirals-into-massive-data-breach-impacting-almost-2-million-people
https://www.youtube.com/watch?v=CbNqbOt8bdc

Scena internazionale 🌐

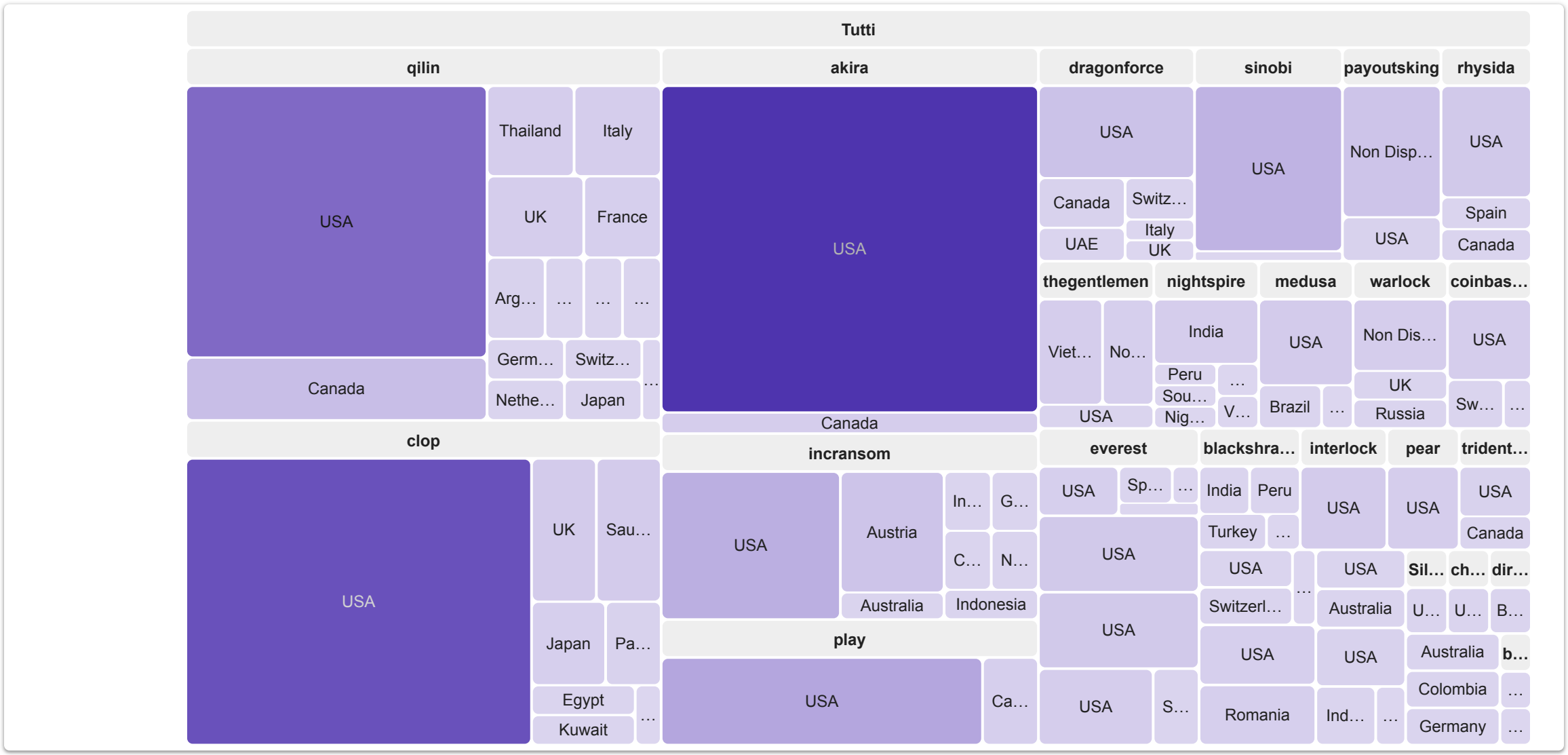
Vittime	Gruppi attivi	Paesi colpiti
693	53	69

Si fa notare che il mese di novembre 2025 vede un incremento del **7,40%** rispetto allo stesso periodo dell'anno precedente (novembre 2024: 645 rivendicazioni).

TOP 10 gruppi criminali

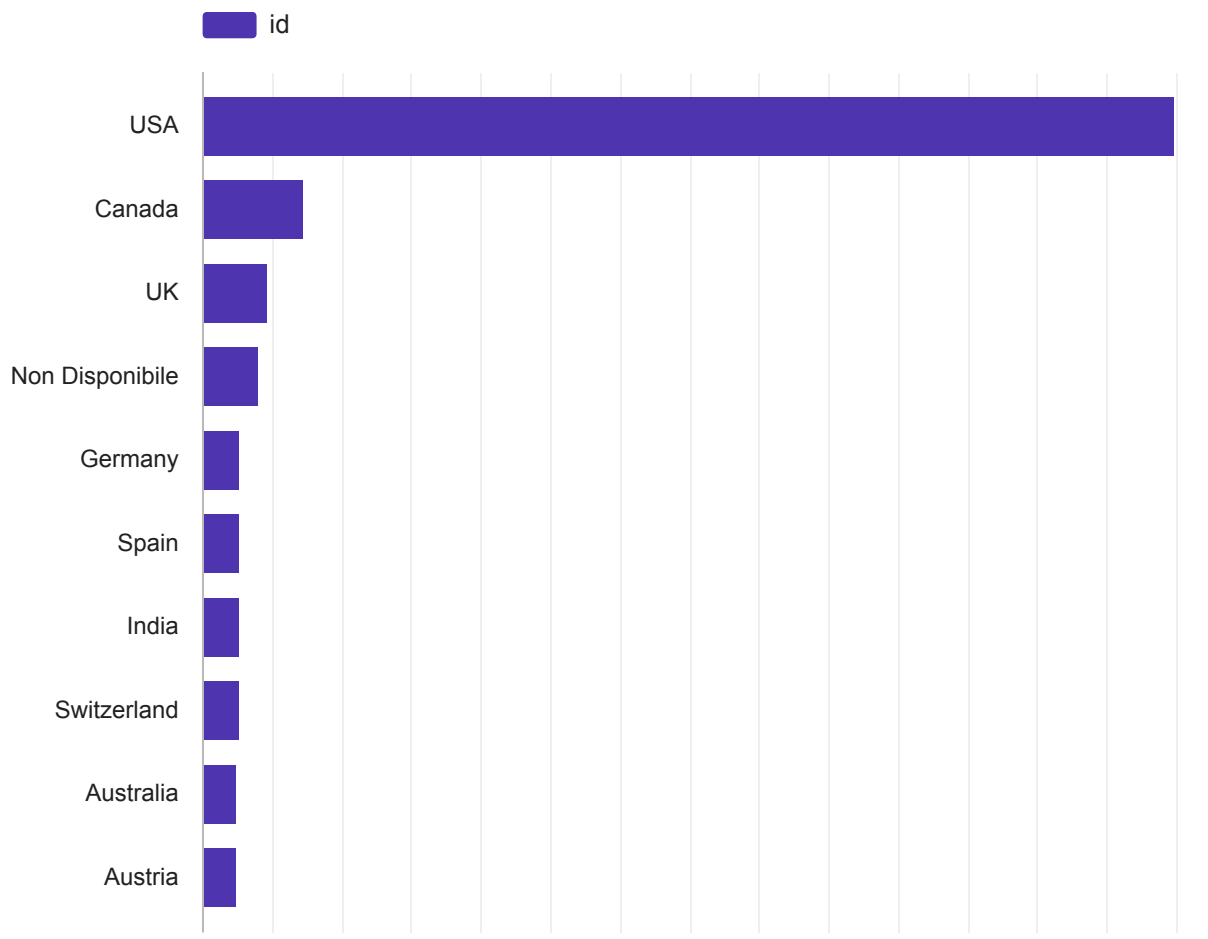


	GRUPPO	VITTIME
1.	qilin	106
2.	clop	101
3.	akira	89
4.	incransom	52
5.	play	27
6.	dragonforce	25
7.	sinobi	23
8.	thegentlemen	19
9.	warlock	17
10.	nightspire	15
11.	safepay	14
12.	payoutsking	13
13.	ransomhouse	13
14.	medusa	12
15.	rhysida	11
16.	devman	10
17.	worldleaks	10
18.	everest	10
19.	nova	10
20.	coinbasecartel	10
21.	Altri	106

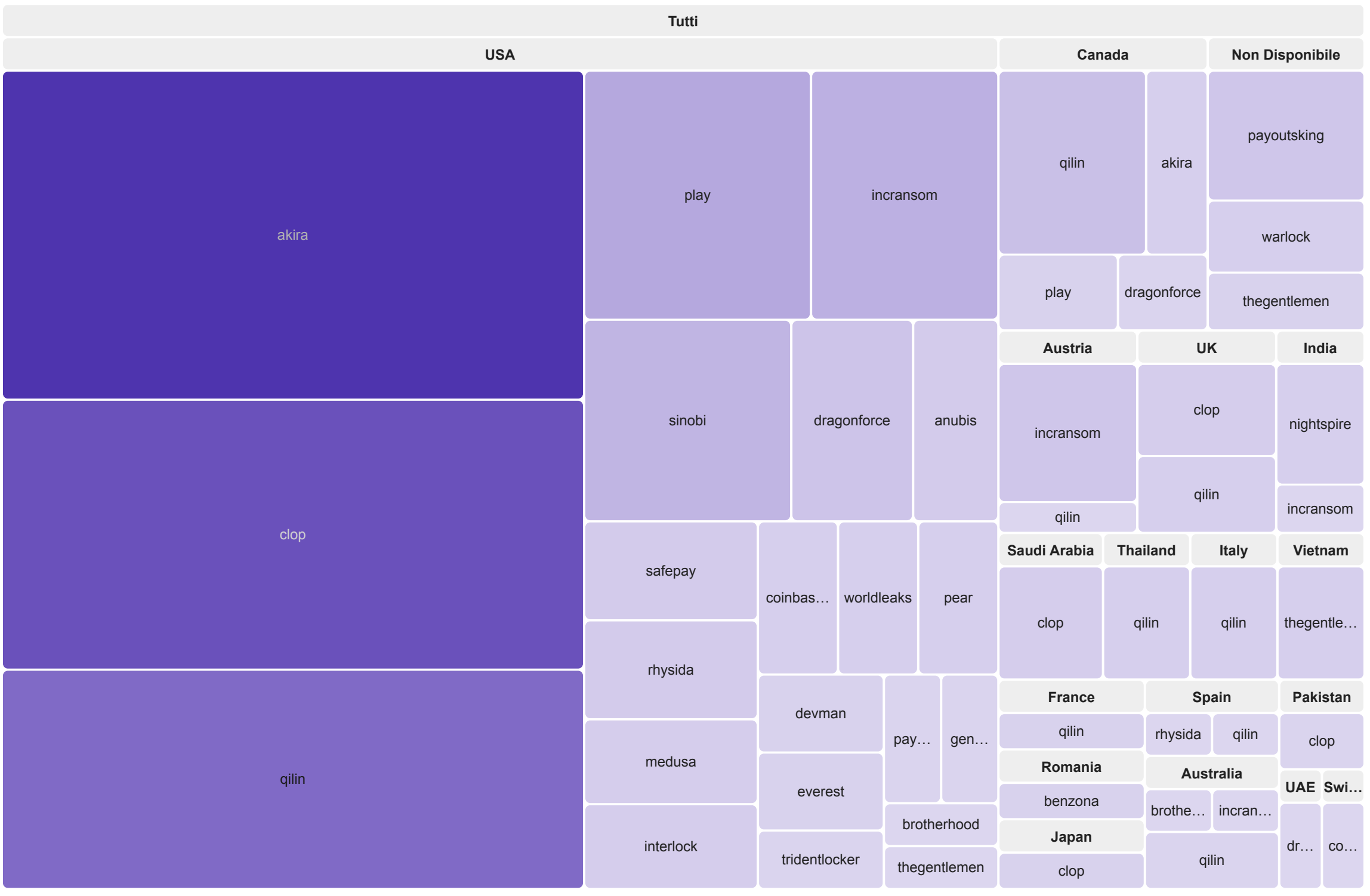


Scena internazionale 🌐

TOP 10 Paesi colpiti

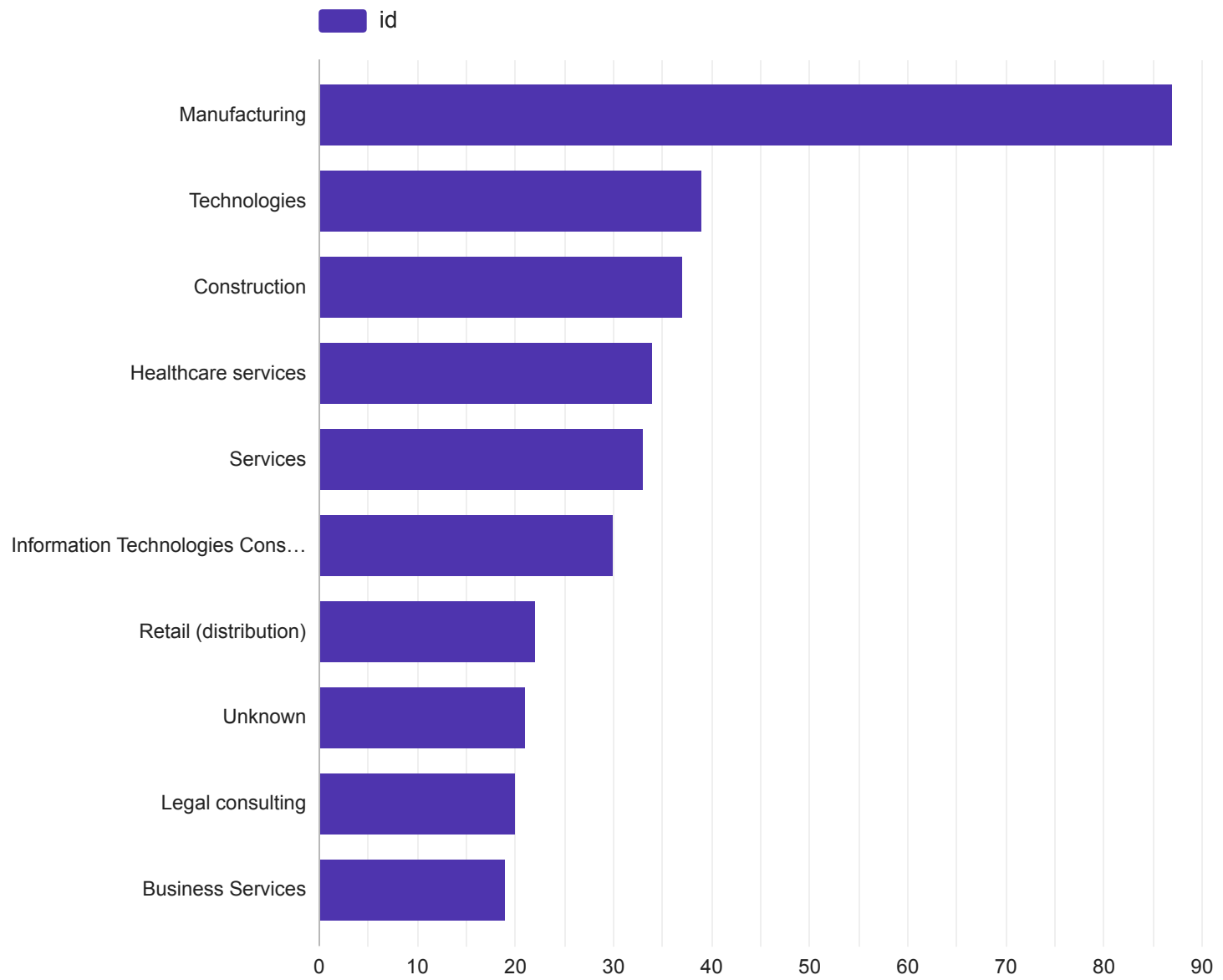


	PAESE	VITTIME
1.	USA	348
2.	Canada	36
3.	UK	23
4.	Non Disponibile	20
5.	Germany	13
6.	Spain	13
7.	India	13
8.	Switzerland	13
9.	Australia	12
10.	Austria	12
11.	Italy	11
12.	Mexico	10
13.	Thailand	10
14.	Brazil	10
15.	Vietnam	8
16.	Japan	8
17.	France	6
18.	UAE	6
19.	Saudi Arabia	6
20.	Colombia	6
21.	Altri	108

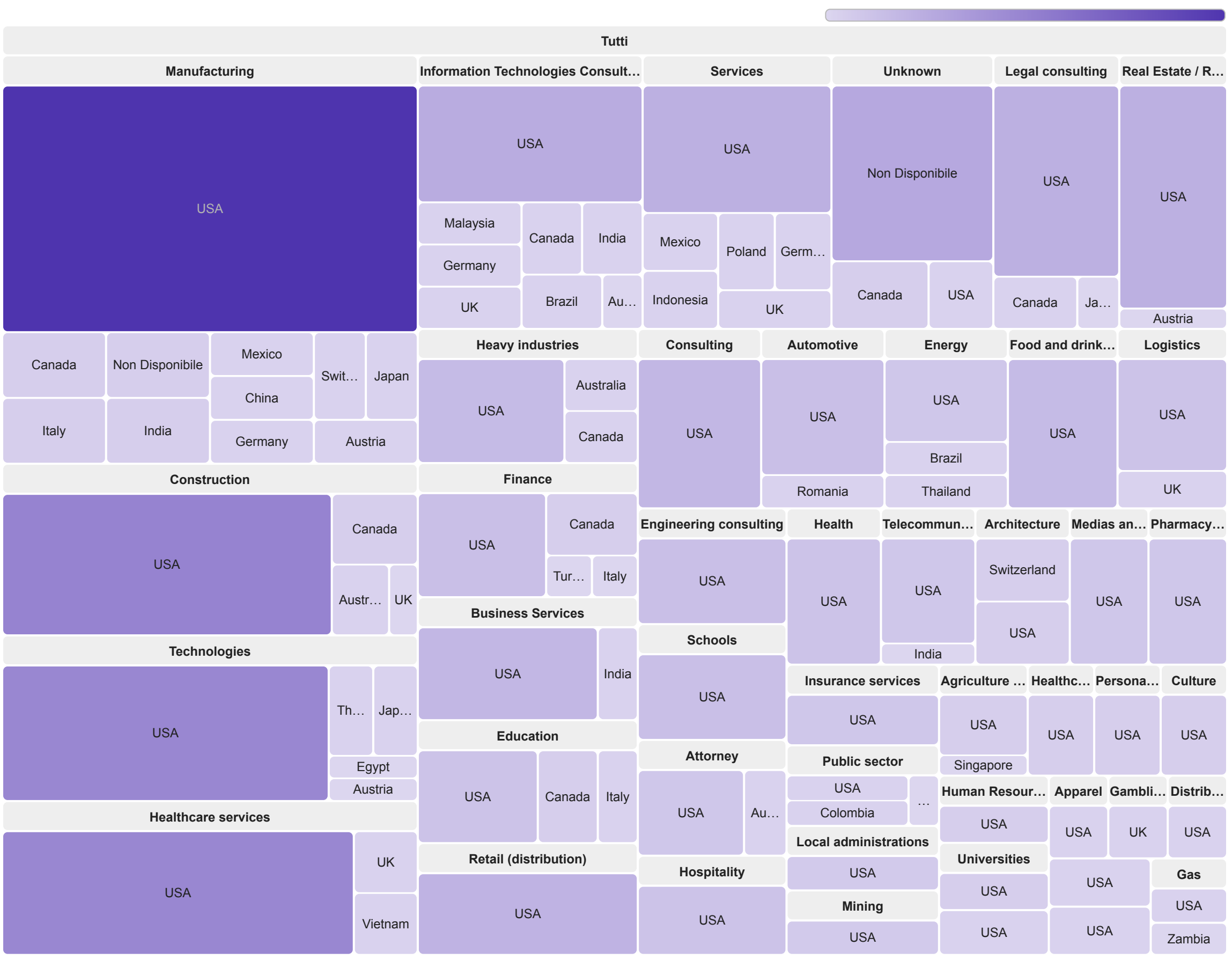


Scena internazionale 🌐

TOP 10 Settori economici



	SETTORE	VITTIME
1.	Manufacturing	87
2.	Technologies	39
3.	Construction	37
4.	Healthcare services	34
5.	Services	33
6.	Information Technologies Co…	30
7.	Retail (distribution)	22
8.	Unknown	21
9.	Legal consulting	20
10.	Business Services	19
11.	Heavy industries	17
12.	Finance	17
13.	Real Estate / Real Estate M…	16
14.	Automotive	16
15.	Food and drinks businesses	16
16.	Energy	15
17.	Logistics	14
18.	Consulting	14
19.	Education	12
20.	Engineering consulting	11
21.	Altri	202



Vulnerabilità sfruttate dai gruppi ransomware a novembre 2025

L'incremento degli attacchi ransomware osservato nel mese è stato alimentato da due fattori chiave: la continua scoperta di vulnerabilità IT critiche e l'elevato numero di asset esposti su Internet non ancora aggiornati.

I threat actor hanno sfruttato attivamente queste falle in prodotti e sistemi operativi molto diffusi, prendendo di mira sia vulnerabilità nuovissime che falle note del passato.

Questo scenario sottolinea l'importanza critica di un programma di patch management tempestivo e di una rigorosa gestione della superficie di attacco esposta online.

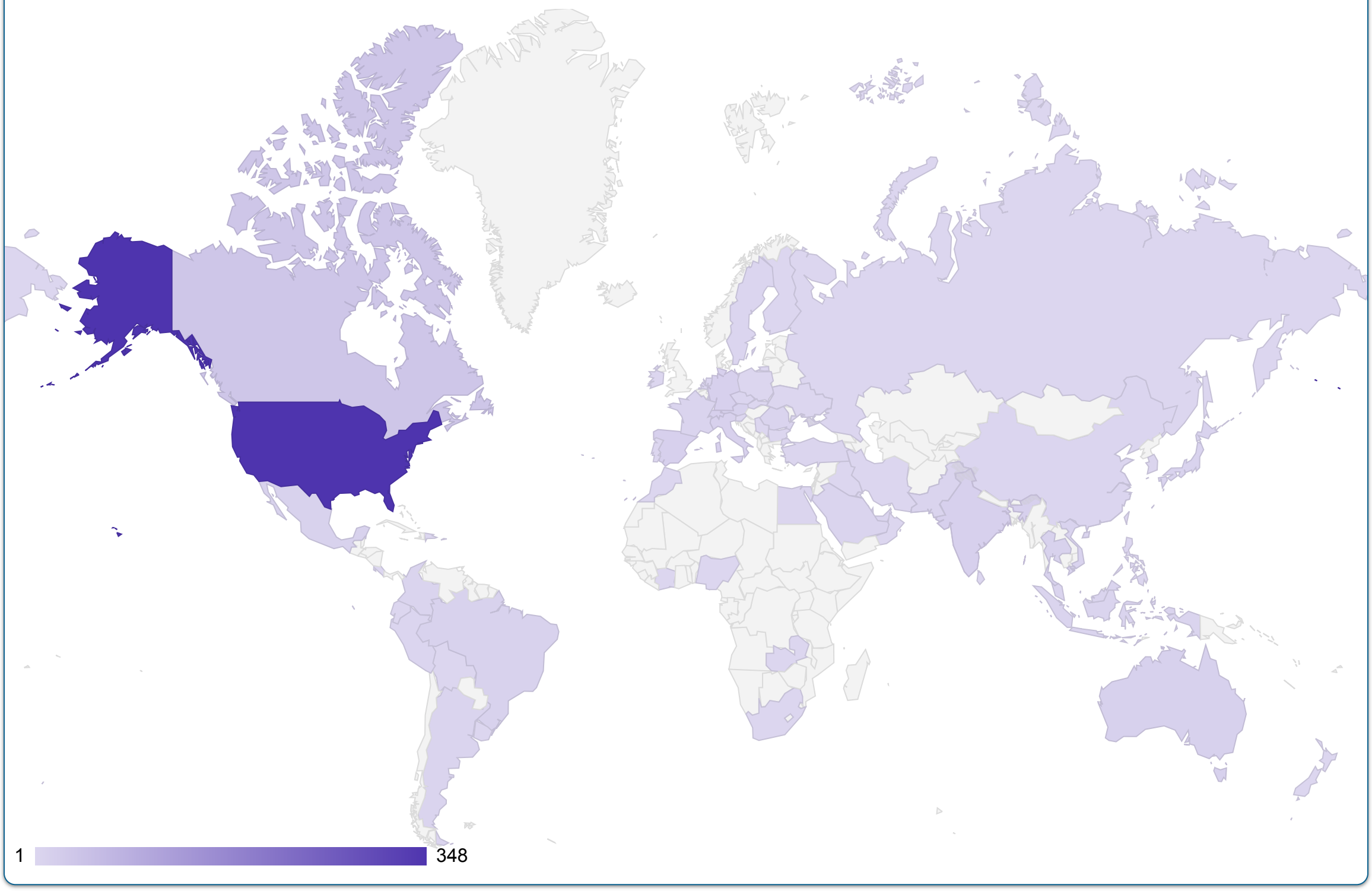
Tabella delle principali vulnerabilità sfruttate da ransomware (Novembre 2025)

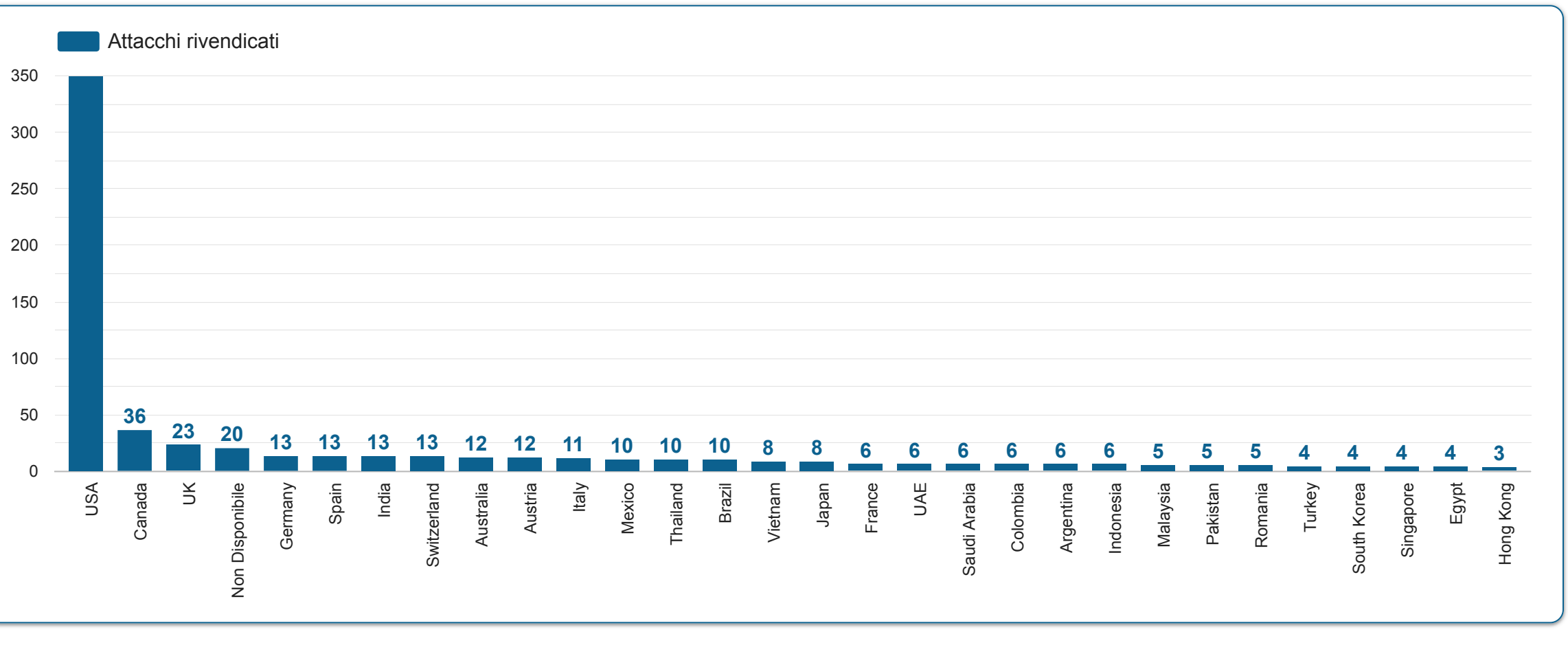
Prodotto/Sistema Vulnerabile	CVE	Tipologia di Vulnerabilità	Gruppo Ransomware Associato
Oracle E-Business Suite (EBS)	CVE-2025-61882	Vulnerabilità Zero-day	Cl0p
Syndicate Linux Kernel (netfilter/nf_tables)	CVE-2024-1086	Use-after-free (Escalation dei privilegi a livello root)	-
Gladinet Triofox	CVE-2025-12480	Controllo degli accessi improprio	UNC6485
Oracle Identity Manager (OIM)	CVE-2025-61757	RCE Pre-autenticazione	-
CentOS Web Panel (CWP)	CVE-2025-48703	Remote Command Injection	-
Microsoft Office & Windows	CVE-2025-60724	GDI+ heap overflow	-
N-Able N-Central	CVE-2025-9316 / CVE-2025-11700	Catena di attacco per bypass autenticazione e iniezione XML	-

- **Sfruttamento di vulnerabilità software**: il gruppo Cl0p è stato il più attivo del mese, sfruttando falle zero-day in Oracle E-Business Suite per colpire oltre 100 organizzazioni, tra cui nomi illustri come Logitech, The Washington Post e Cox Enterprises.
- **Sfruttamento di vulnerabilità di sistema**: è preoccupante notare come la vulnerabilità CVE-2024-1086, pur essendo nota da due anni e presente nella lista KEV di CISA, sia diventata una minaccia ransomware primaria solo in questo mese.

Molte delle vulnerabilità critiche di questo mese (come quelle in Triofox, OIM e CWP) permettono agli attaccanti di eseguire codice da remoto senza autenticazione, facilitando l'accesso iniziale alle reti aziendali

La scena globale mese Novembre 2025





ransomfeed

ADVANCED **DATADRIVEN** CYBERNEWS

RECAP MENSILE
NOVEMBRE 2025

<eof>