ransomfeed

ADVANCED **DATADRIVEN** CYBERNEWS

RECAP MENSILE

FEBBRAIO 2026

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

Focus Italia 🇮🇹

Nel mese di **febbraio 2026** la piattaforma ha rilevato un totale di **21 attacchi**.
Si fa notare che il mese di gennaio 2026 vede un incremento del 62% rispetto allo stesso periodo dell'anno precedente (febbraio 2025: 13 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

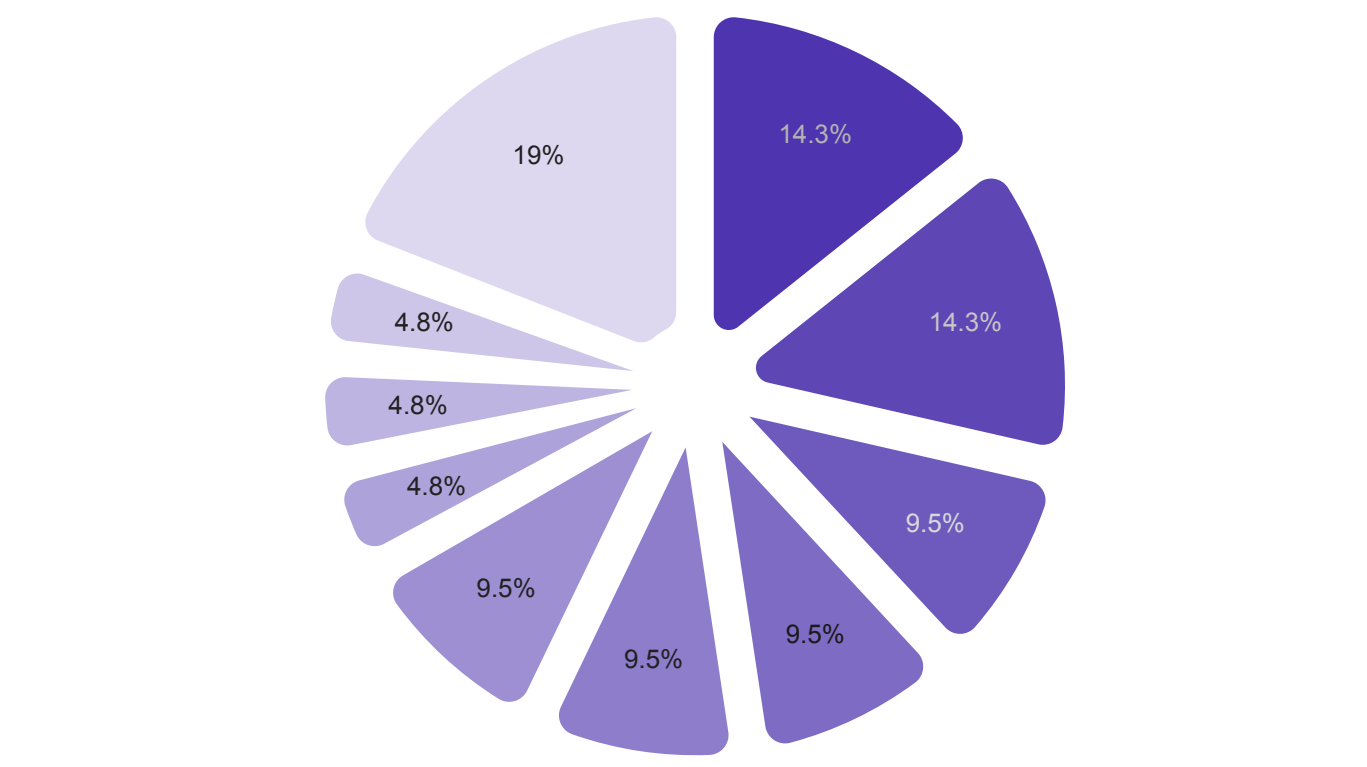
Vittime Italia	Totale GB pubblicati
21	794,35

	ID ▲	GRUPPO	VITTIMA	DATI PUBBLICATI GB
1.	29296	akira	Ferretti Construction	97.84
2.	29312	medusa	Comune di Battipaglia	94.08
3.	29483	thegentlemen	Silvi SRL	0
4.	29485	qilin	Parente Fireworks	0
5.	29504	clop	LABINF.IT	6.29
6.	29519	lockbit5	autoservizilocatelli.it	21.8
7.	29686	spacebears	Siem Srl	0
8.	29740	nightspire	A.T.I di Zuinisi srl	10
9.	29747	incransom	Bitgo	0
10.	29763	akira	Icat Food SpA	0
11.	29767	dragonforce	wiproferretto.com	302
12.	29770	akira	iSMA CONTROLLI	1.2
13.	29773	qilin	Casartigiani	0
14.	29820	tengu	femar.it	145
15.	29827	spacebears	Elgon Cosmetic	9.5
16.	29868	qilin	ABAR S.p.A.	0
17.	29914	thegentlemen	Seac	0
18.	30019	nightspire	OFFICINE FRATELLI AMADORI snc	12
19.	30035	tengu	martec.it	67.04
20.	30097	vect	keliweb	0
21.	30426	payload	Easy Servizi SRL	27.6

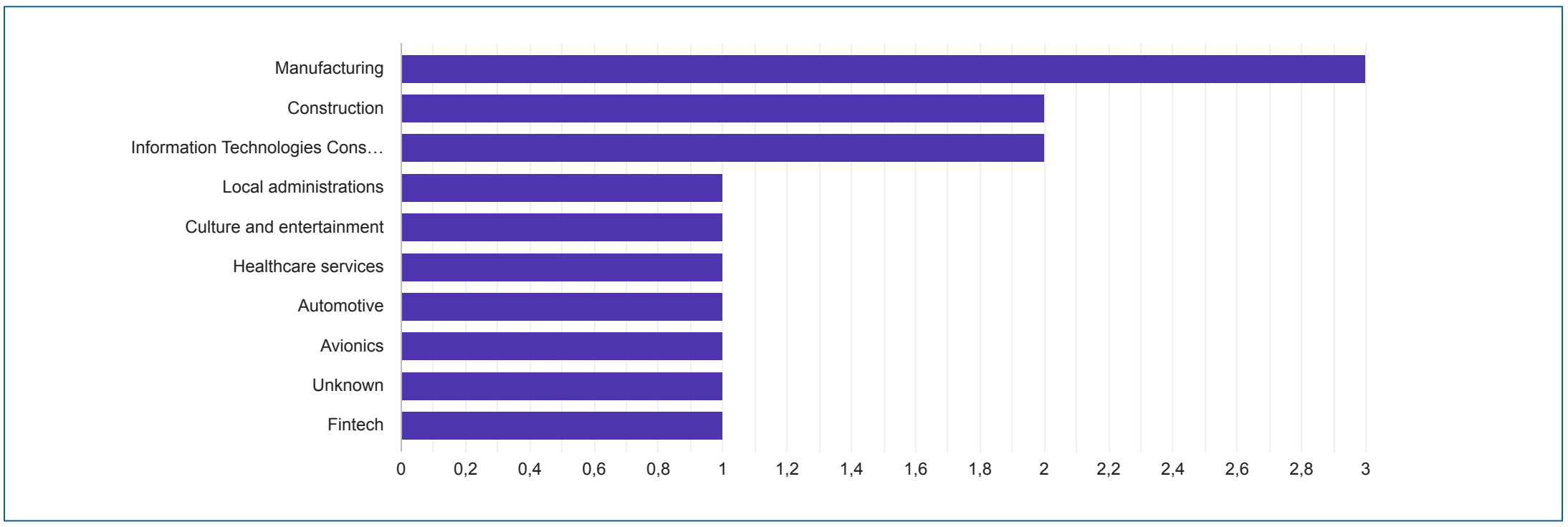
Gruppi criminali
focus Italia

Il grafico e la tabella qui sotto riportano i dati dei gruppi criminali coinvolti negli attacchi ransomware verso target italiani, nel mese di **febbraio 2026**.
Mentre invece in fondo si trova la distribuzione dei settori economici.

	GRUPPO	VITTIME
1.	akira	3
2.	qilin	3
3.	thegentlemen	2
4.	spacebears	2
5.	nightspire	2
6.	tengu	2
7.	medusa	1
8.	clop	1
9.	lockbit5	1
1…	incransom	1
1…	dragonforce	1
1…	vect	1



Settori economici
focus Italia



Ransomware Story

BridgePay, ransomware blocca i pagamenti e costringe i commercianti al contante

Nel febbraio 2026 il ransomware ha trovato uno dei suoi bersagli più efficaci: non un singolo ufficio, non una rete periferica, ma il cuore silenzioso dei pagamenti digitali. BridgePay, fornitore statunitense di servizi di pagamento, è stata colpita da un attacco che ha trasformato in poche ore una compromissione tecnica in una crisi operativa capace di propagarsi ben oltre il perimetro dell'azienda. È in casi come questo che il ransomware mostra la sua natura più contemporanea: non più soltanto minaccia di cifratura e richiesta di riscatto, ma strumento di interruzione sistemica, capace di incidere sulla continuità di servizi essenziali e sul funzionamento quotidiano di clienti, esercenti e amministrazioni.

Le prime segnalazioni emerse all'inizio del mese hanno descritto un'interruzione ampia e improvvisa. BridgePay ha parlato di una "system-wide service disruption", formula che, nel linguaggio spesso asciutto degli incident response team, equivale a dire che il danno non era confinato a un singolo ambiente o a una funzione accessoria, ma investiva l'architettura centrale della piattaforma. A essere coinvolti, secondo le ricostruzioni successive, sarebbero stati i componenti fondamentali del servizio: gateway, virtual terminal, API, hosted payment pages e reporting tool. In un settore come quello dei pagamenti, dove ogni tassello è parte di una catena molto più ampia, il blocco di questi elementi equivale a interrompere il flusso stesso delle transazioni.

L'impatto dell'incidente è stato immediato e tangibile. Per molti clienti di BridgePay, il problema non si è presentato come una notifica tecnica, ma come un servizio che semplicemente smetteva di funzionare. Diversi commercianti e soggetti che dipendevano dall'infrastruttura hanno dovuto gestire temporaneamente i pagamenti in contanti; alcuni enti pubblici e realtà collegate hanno segnalato l'impossibilità di processare le transazioni online o con carta. È questa la dimensione più eloquente del caso: quando un payment processor si ferma, il ransomware non produce solo un danno informatico, ma altera il ritmo di una porzione concreta dell'economia.

La vicenda BridgePay è particolarmente utile perché racconta bene la trasformazione del ransomware in minaccia infrastrutturale. Non si tratta più soltanto di un gruppo criminale che cifra dati per ottenere denaro, ma di un attacco che colpisce un punto di concentrazione, sapendo che da lì può propagare il proprio effetto su una platea molto più ampia della sola vittima primaria. BridgePay, infatti, operava come nodo di integrazione per soggetti diversi, inclusi enti pubblici, utility, imprese e merchant, e proprio questa interconnessione ha amplificato le conseguenze dell'attacco. Il fermo della piattaforma non ha soltanto creato un problema interno: ha messo in pausa transazioni, portali di pagamento e flussi operativi di organizzazioni terze, mostrando quanto fragile possa essere la catena quando un fornitore centrale viene compromesso.

Dal punto di vista tecnico, l'ipotesi di lavoro più plausibile è quella di una compromissione iniziale tramite account, con successiva disattivazione dei servizi da parte dell'attaccante e richiesta di riscatto. Alcune fonti hanno parlato di file cifrati e di un contesto compatibile con una classica operazione ransomware, mentre BridgePay ha cercato di rassicurare il pubblico dichiarando che non vi erano evidenze di compromissione dei dati delle carte e che i dati eventualmente raggiunti risultavano cifrati, senza segni di esposizione utilizzabile. Anche questo dettaglio è importante: nel caso BridgePay, il danno più grave non sembra essere stato il leak immediato, ma l'indisponibilità del servizio e la pressione esercitata sulla vittima attraverso il blocco dei sistemi.

È un passaggio che vale molto, anche sul piano narrativo. L'immagine classica del ransomware come furto di dati e minaccia di pubblicazione è ormai solo una parte della storia. Sempre più spesso, ciò che pesa davvero è la capacità di paralizzare l'operatività, di interrompere il normale ciclo del business e di costringere l'organizzazione a lavorare in condizioni degradate. BridgePay è un esempio limpido di questa evoluzione: il ransomware ha colpito il punto in cui tecnologia e funzione economica coincidono, facendo emergere una vulnerabilità che non è solo informatica, ma sistemica.

La risposta all'incidente ha coinvolto non soltanto i team interni di sicurezza e i professionisti della forense digitale, ma anche le autorità federali statunitensi, tra cui FBI e Secret Service. La presenza di questi attori sottolinea il profilo dell'evento, che non è apparso come un semplice incidente isolato, ma come un caso abbastanza serio da richiedere coordinamento esterno e attività di contenimento più ampie. Eppure, come spesso accade in episodi di questo tipo, la fase più delicata non è quella dell'allarme iniziale, ma quella meno visibile del recupero: bonifica degli ambienti, ricostruzione fidata dei sistemi, verifica dell'assenza di persistenze, riallineamento dell'infrastruttura e ripristino graduale delle funzioni più sensibili.

La durata stessa del disservizio ha finito per raccontare molto della complessità del caso. Alcune analisi di settore hanno indicato che il ripristino completo richiese settimane, segnalando quanto sia costoso, in termini di tempo e risorse, tornare a una condizione operativa normale dopo un attacco che colpisce un'infrastruttura così centrale. Ed è qui che BridgePay diventa un caso particolarmente adatto a un report mensile sul ransomware: perché mostra, in modo netto, il passaggio dal livello tecnico al livello strategico. L'attacco non ha solo "compromesso" un'azienda; ha imposto una revisione forzata delle sue dipendenze, della sua resilienza e della sua capacità di garantire continuità ai clienti.

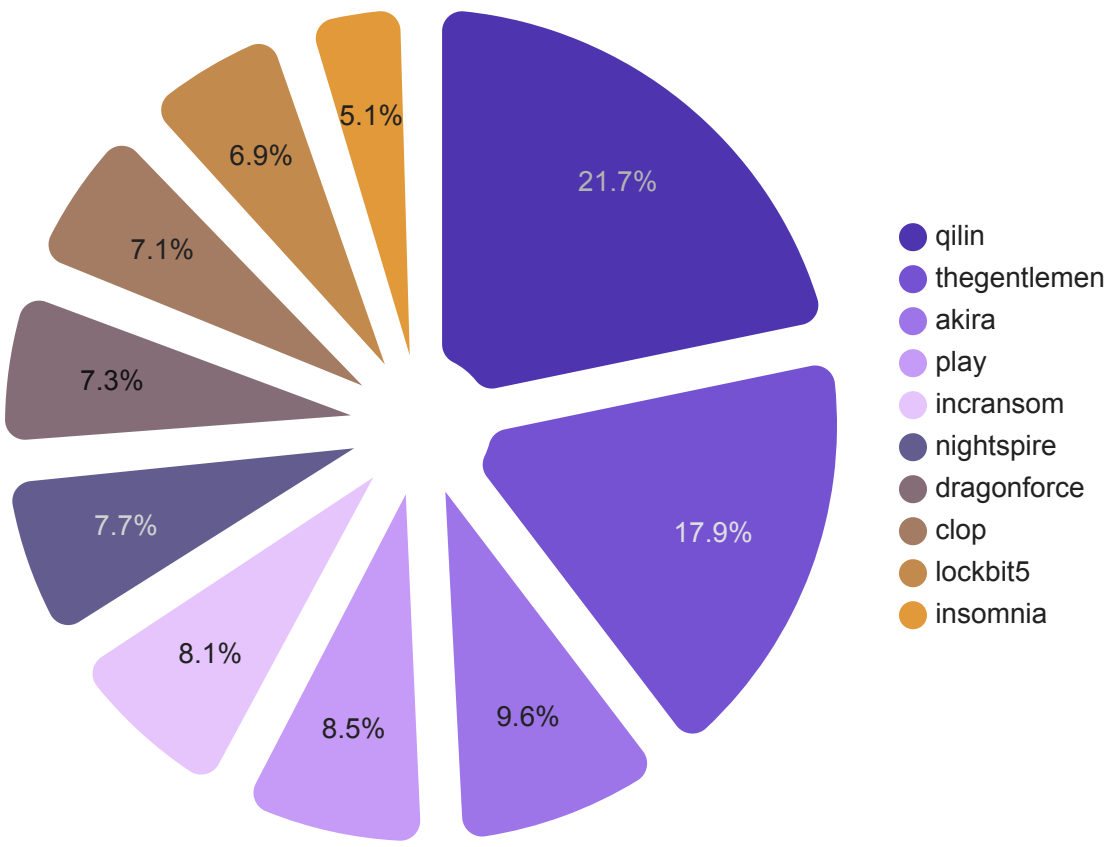
C'è infine un'ultima lezione, forse la più importante. BridgePay ricorda che la resilienza nei pagamenti digitali non può essere intesa come semplice ridondanza infrastrutturale. Serve segmentazione, serve controllo degli account privilegiati, serve osservabilità continua sui punti di ingresso e soprattutto serve la capacità di ripristinare davvero, non solo di riaccendere i sistemi. Quando un operatore di questo tipo cade, il danno non resta confinato a una dashboard o a un SOC alert: si riflette nei negozi, nei portali di pagamento, nei servizi pubblici, nei flussi economici che ogni giorno presuppongono che quella piattaforma funzioni senza attrito. E proprio per questo BridgePay resta uno dei casi più significativi del mese: perché ha mostrato quanto il ransomware, oggi, sia capace di colpire la parte invisibile ma essenziale dell'economia digitale.

Scena internazionale 🌐

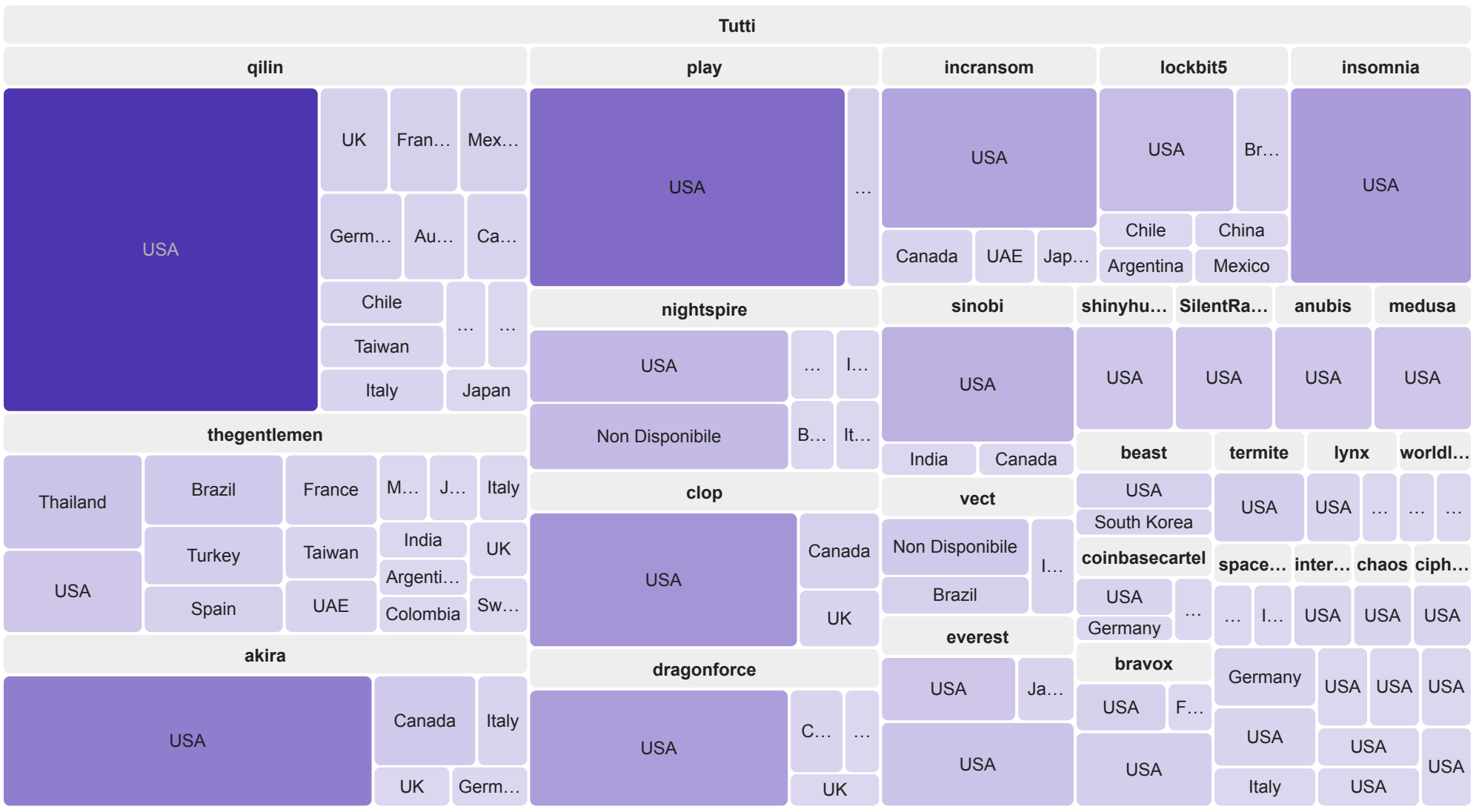
Vittime	Gruppi attivi	Paesi colpiti
715	50	68

Si fa notare che il mese di febbraio 2026 vede un decremento del **25%** rispetto allo stesso periodo dell'anno precedente (febbraio 2025: 955 rivendicazioni).

TOP 10 gruppi criminali

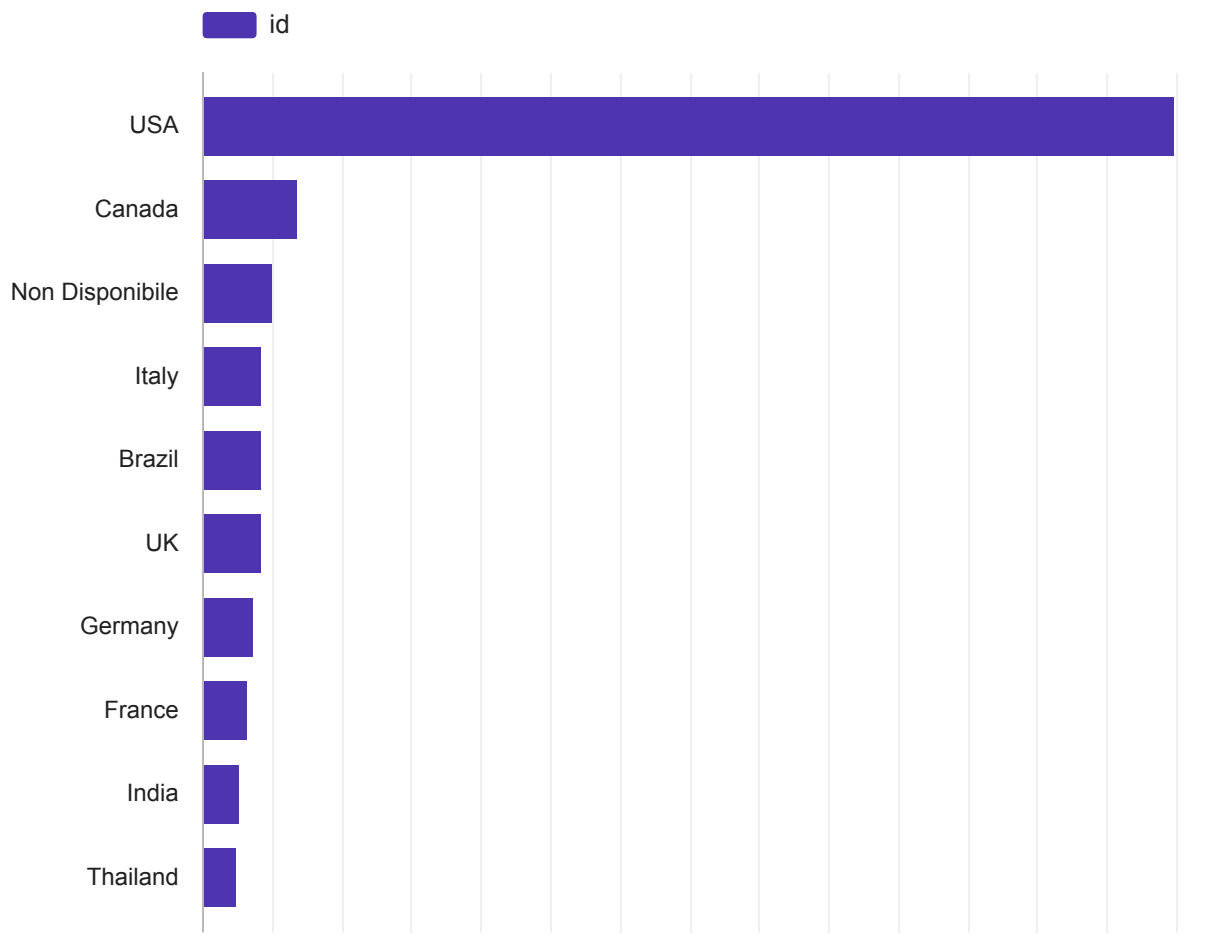


	GRUPPO	VITTIME
1.	qilin	107
2.	thegentlemen	88
3.	akira	47
4.	play	42
5.	incransom	40
6.	nightspire	38
7.	dragonforce	36
8.	clop	35
9.	lockbit5	34
10.	insomnia	25
11.	vect	19
12.	sinobi	18
13.	everest	10
14.	anubis	10
15.	coinbasecartel	10
16.	spacebears	10
17.	shinyhunters	9
18.	genesis	9
19.	lynx	9
20.	beast	9
21.	Altri	110

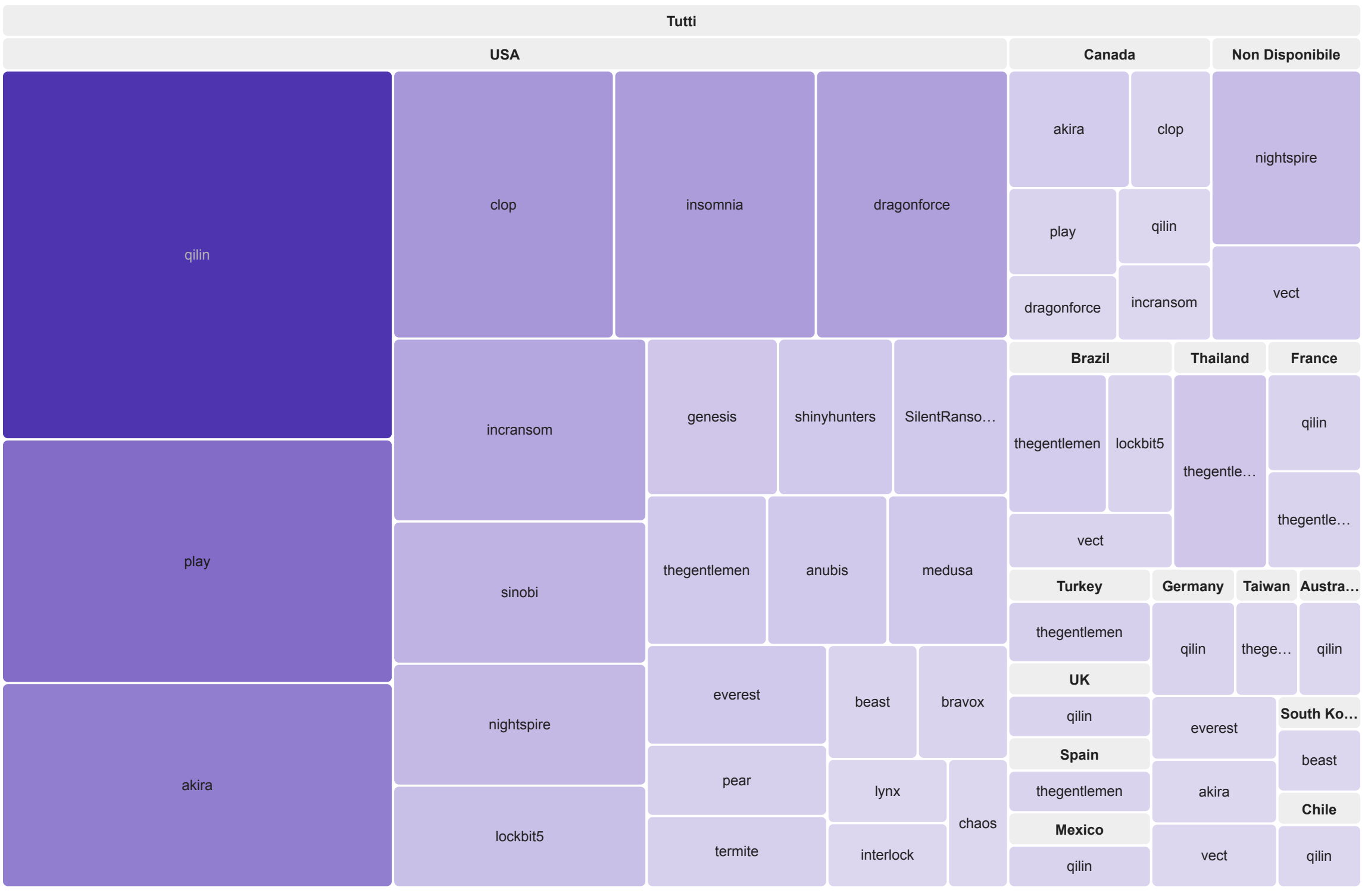


Scena internazionale 🌐

TOP 10 Paesi colpiti

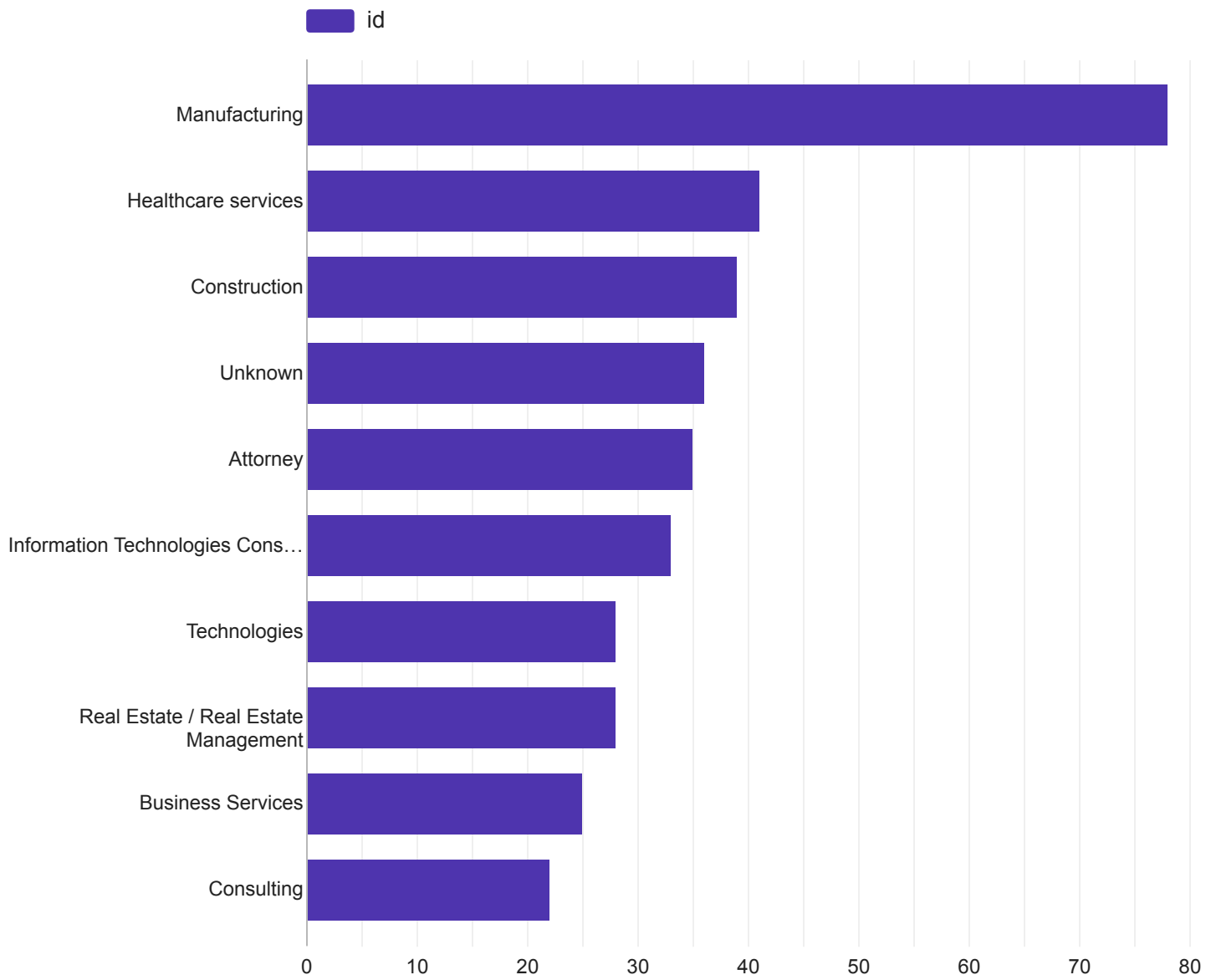


	PAESE	VITTIME
1.	USA	348
2.	Canada	34
3.	Non Disponibile	25
4.	Italy	21
5.	Brazil	21
6.	UK	21
7.	Germany	18
8.	France	16
9.	India	13
10.	Thailand	12
11.	Japan	11
12.	Mexico	11
13.	Spain	11
14.	Taiwan	10
15.	UAE	8
16.	Chile	7
17.	Switzerland	7
18.	Turkey	6
19.	Australia	6
20.	Argentina	6
21.	Altri	102

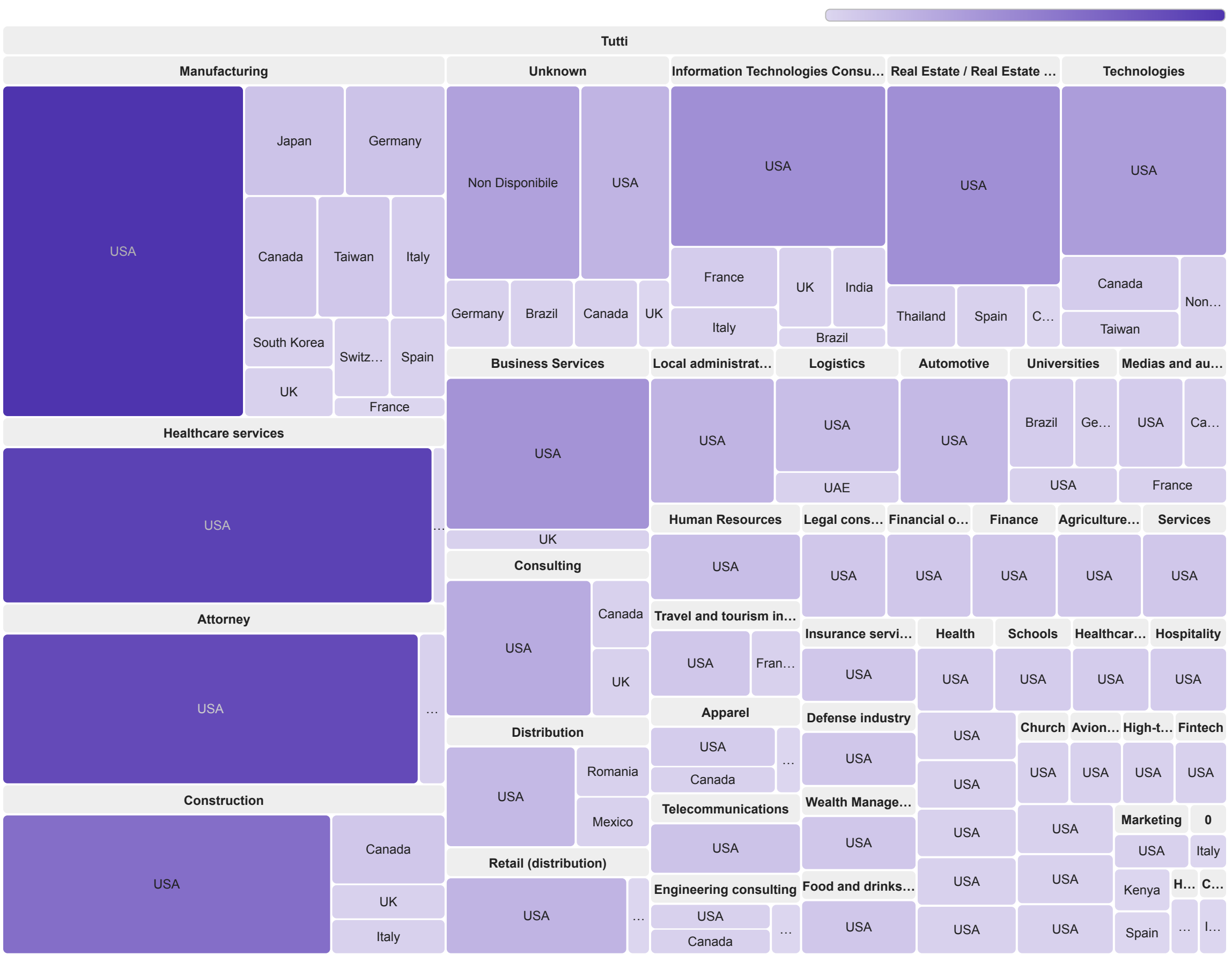


Scena internazionale 🌐

TOP 10 Settori economici



	SETTORE	VITTIME
1.	Manufacturing	78
2.	Healthcare services	41
3.	Construction	39
4.	Unknown	36
5.	Attorney	34
6.	Information Technologies Co…	33
7.	Technologies	28
8.	Real Estate / Real Estate M…	28
9.	Business Services	25
10.	Consulting	22
11.	Retail (distribution)	19
12.	Automotive	18
13.	Local administrations	14
14.	Logistics	13
15.	Distribution	13
16.	Food and drinks businesses	11
17.	Universities	10
18.	Apparel	10
19.	Engineering consulting	9
20.	Finance	8
21.	Altri	225



Vulnerabilità sfruttate dai gruppi ransomware a febbraio 2026

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.

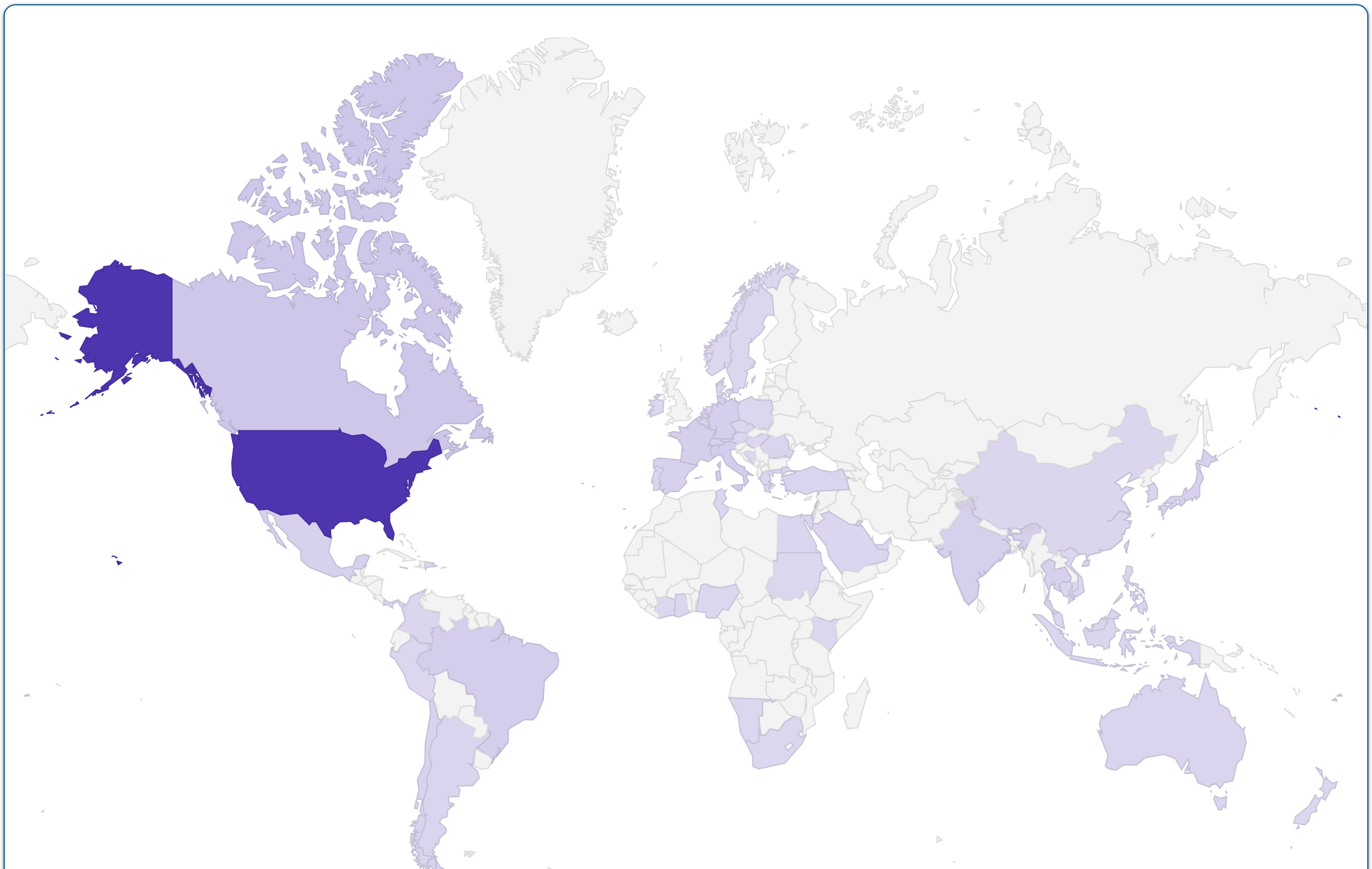
I threat actor hanno sfruttato attivamente queste falle in prodotti e sistemi operativi molto diffusi, prendendo di mira sia vulnerabilità nuovissime che falle note del passato.

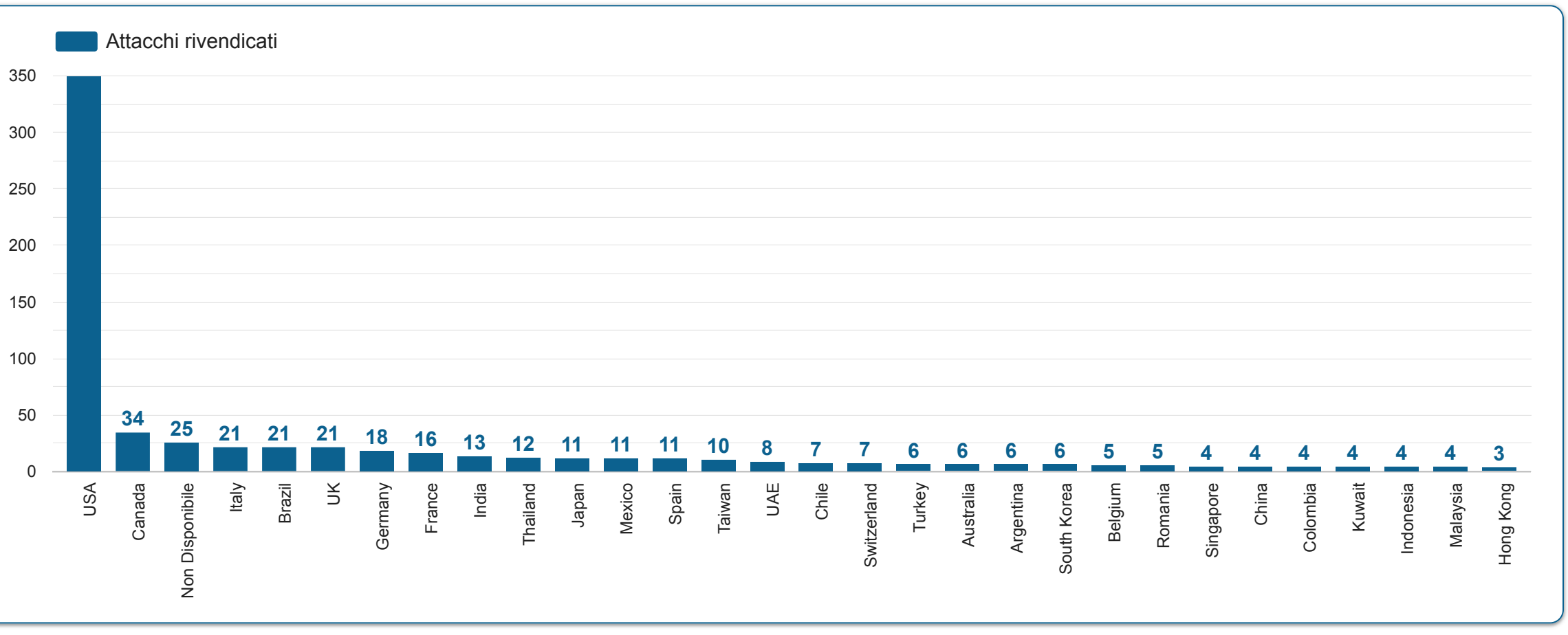
Questo scenario sottolinea l'importanza critica di un programma di patch management tempestivo e di una rigorosa gestione della superficie di attacco esposta online.

Tabella delle principali vulnerabilità sfruttate da ransomware (Febbraio 2026)

	Prodotto vulnerabile	CVE	Tipologia vulnerabilità	Gruppo Ransomware Associato
1.	n8n workflow automation platform	CVE-2025-68613	Environment escape / server takeover	Nessuno noto
2.	Zyxel router models	CVE-2025-7702	Remote code execution	Nessuno noto
3.	Windows 11 Notepad	CVE-2026-20841	Remote code execution	Nessuno noto
4.	WinRAR	CVE-2025-8088	Esecuzione di codice / initial access	Nessuno noto
5.	Visual Studio Code extension	CVE-2025-65715	File theft / local file access	Nessuno noto
6.	Visual Studio Code extension	CVE-2025-65716	Remote code execution	Nessuno noto
7.	Visual Studio Code extension	CVE-2025-65717	Remote code execution	Nessuno noto
8.	VMware ESXi	N/D nel link sorgente	Sandbox escape / compromissione hypervisor	Unknown
9.	SolarWinds Web Help Desk	CVE-2025-26399	Post-exploitation / accesso persistente	Nessuno noto
10.	SolarWinds Web Help Desk	CVE-2025-40551	Remote code execution	Nessuno noto
11.	SmarterMail	CVE-2026-24423	Remote code execution	Warlock Ransomware
12.	SmarterMail	CVE-2026-23760	Furto credenziali amministratore / compromissione server	Warlock Ransomware
13.	React Native Metro development server	CVE-2025-11953	Remote code execution	Nessuno noto
14.	Microsoft Office	CVE-2026-21509	Esecuzione di codice / malware delivery	Nessuno noto
15.	Honeywell CCTV models	CVE-2026-1670	Authentication bypass	Nessuno noto
16.	Grandstream VoIP phones	CVE-2026-21486	Eavesdropping / accesso interfacce interne	Nessuno noto
17.	GitLab	CVE-2021-39935	Autenticazione / accesso non autorizzato	Nessuno noto
18.	Dell RecoverPoint for Virtual Machines	CVE-2026-22769	"Zero-day	accesso non autorizzato"
19.	BeyondTrust Remote Support / Privileged Remote Access	N/D nel link sorgente	Remote code execution	Unknown

La scena globale mese Febbraio 2026





ransomfeed

ADVANCED **DATADRIVEN** CYBERNEWS

RECAP MENSILE
FEBBRAIO 2026

<eof>