ransomfeed

ADVANCED **DATADRIVEN** CYBERNEWS

RECAP MENSILE

GENNAIO 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

ChangeLog gennaio 2026

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.

- Migliorati script di scraping per velocizzarne il processo con nuove fonti di enrichment.

- Sistemazione GUI per riquadro "Dataset italiani", con implementazione anno 2026.

Focus Italia 🇮🇹

Nel mese di **gennaio 2026** la piattaforma ha rilevato un totale di **20 attacchi**.
Si fa notare che il mese di gennaio 2026 vede un incremento del 185% rispetto allo stesso periodo dell'anno precedente (gennaio 2025: 7 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

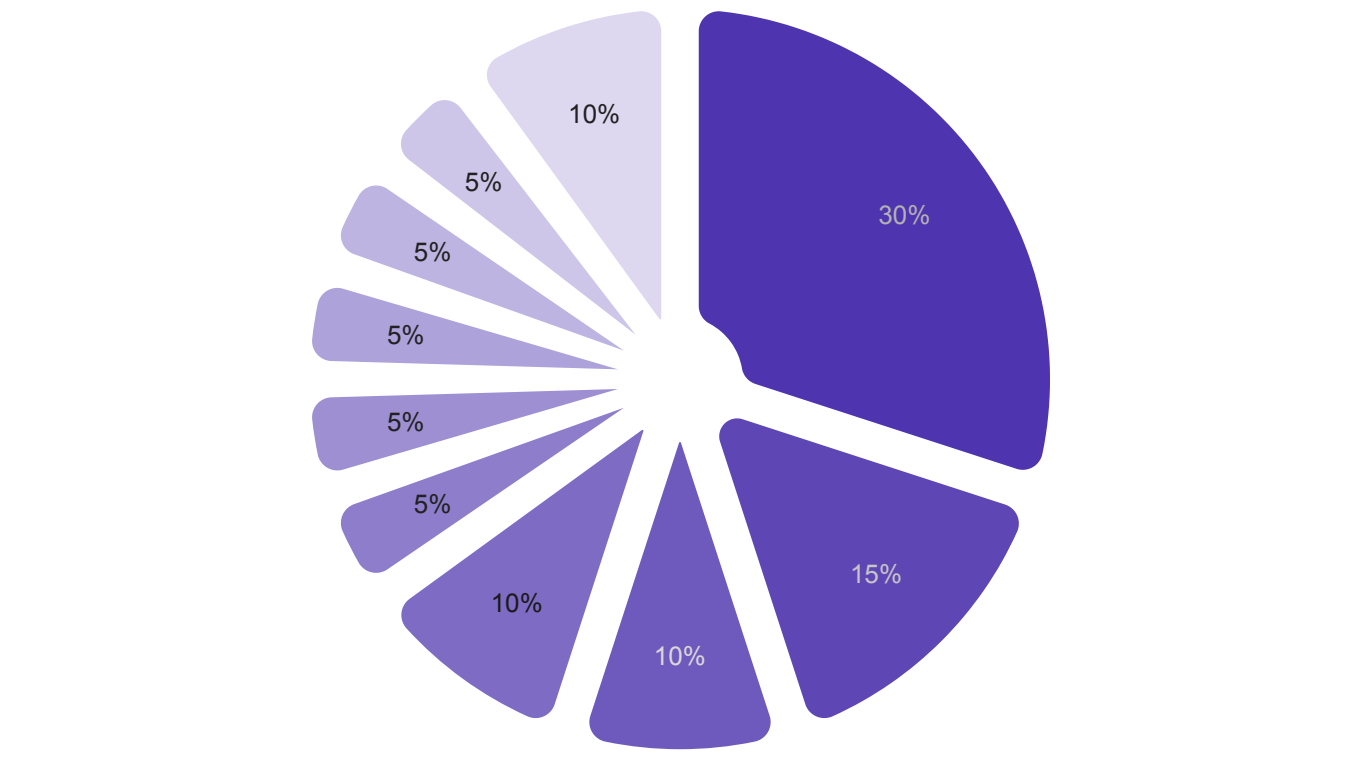
Vittime Italia	Totale GB pubblicati
20	1.908,57

	ID ▲	GRUPPO	VITTIMA	DATI PUBBLICATI GB
1.	28451	qilin	Csv Group	0
2.	28537	nova	Saplog Group	202.55
3.	28539	brotherhood	Italgrafica Sistemi	6
4.	28560	akira	Labeltex Group	3.22
5.	28574	qilin	The Cressi	0
6.	28584	qilin	Softlab SpA	0
7.	28594	clop	MUTTI-PARMA.COM	0
8.	28677	incransom	stimgroup	0
9.	28709	anubis	Adriatic Port Authority	184.68
10.	28766	qilin	Fluorsid Spa	0
11.	28770	qilin	Colacem	0
12.	28777	lockbit5	depotnapoli.com	0
13.	28794	qilin	Casadei	0
14.	28821	thegentlemen	San Carlo Gruppo Alimentare	0
15.	28829	sarcoma	MecMatica	74
16.	28854	thegentlemen	Sita Sud	0
17.	28879	lockbit5	frandent.it	0
18.	28963	clop	RSTRT.IT	1358.12
19.	28979	safepay	lcpublishinggroup.com	0
20.	29214	clop	AUGUSTEA.COM	80

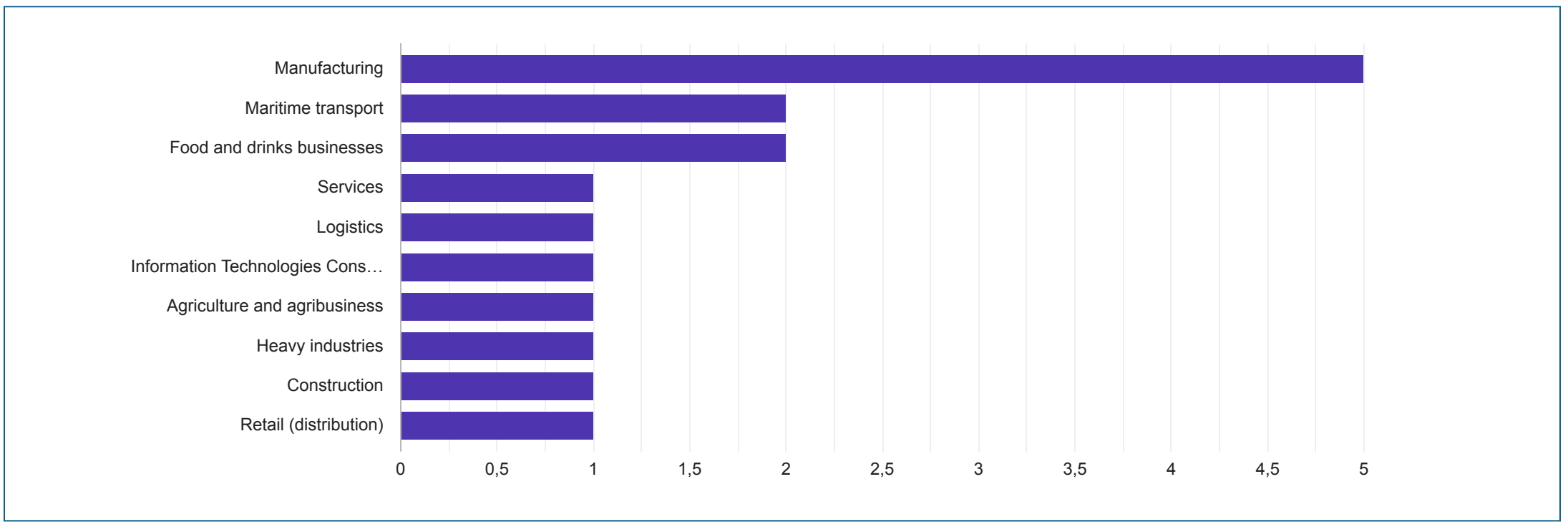
Gruppi criminali
focus Italia

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

	GRUPPO	VITTIME
1.	qilin	6
2.	clop	3
3.	lockbit5	2
4.	thegentlemen	2
5.	nova	1
6.	brotherhood	1
7.	akira	1
8.	incransom	1
9.	anubis	1
1…	sarcoma	1
1…	safepay	1



Settori economici
focus Italia



Ransomware Story

L’episodio SoundCloud di fine 2025 è una classica storia di “non-ransomware che si comporta come un’estorsione”, perfetta per leggere le dinamiche moderne del cyber-ricatto tra scraping, API deboli e pressione reputazionale, più che cifratura dei dati.

Dal 403 Forbidden alla piena esposizione

Quando a metà dicembre 2025 una parte degli utenti SoundCloud inizia a vedere un laconico 403 Forbidden – soprattutto passando da VPN – il problema viene trattato, almeno in apparenza, come un guasto tecnico di piattaforma.
Dietro quella schermata si nasconde in realtà l’attivazione delle procedure di incident response: il team di sicurezza ha appena individuato attività “non autorizzata” su una dashboard di servizio interna, un pannello amministrativo che non dovrebbe mai essere toccato da mani esterne.
SoundCloud conferma l’incidente il 15 dicembre, parlando inizialmente di accesso limitato a dati “coerenti con le informazioni già pubbliche dei profili”. Per qualche giorno la narrativa rimane quella rassicurante: niente password, niente carte di credito, solo ciò che in teoria chiunque potrebbe vedere sul profilo pubblico di un creator.

Come si costruisce un data-set da 29,8 milioni di account

La vera portata del caso emerge settimane dopo, quando Have I Been Pwned (HIBP) indicizza il breach: 29,8 milioni di account coinvolti, circa il 20% della base utenti SoundCloud, con 30 milioni di indirizzi email univoci mappati ai profili pubblici.
Parliamo di un’operazione di de-anonimizzazione su larga scala: l’intrusione alla dashboard interna consente agli attaccanti di correlare email – normalmente non esposte – con username, nome visualizzato, avatar, conteggi di follower/following, statistiche di profilo e, in alcuni casi, il Paese.
Tecnicamente non è necessario compromettere milioni di endpoint, né bucare il core dell’applicazione: basta ottenere accesso a un’interfaccia amministrativa privilegiata o a un’API scarsamente protetta, allineandosi perfettamente con scenari MITRE ATT&CK di abuso di account validi (T1078) e debole autenticazione di servizi interni. Una volta dentro, lo scraping è questione di automazione: query ripetute, estrazione di blocchi di dati, consolidamento in un archivio unico da quasi 30 milioni di righe.
Il dato forse più inquietante per chi fa threat intelligence è un altro: secondo Troy Hunt, circa il 67% degli indirizzi email presenti in questo dump era già finito in HIBP per breach precedenti.Non è solo “un altro incidente”: è l’ennesimo tassello in una catena di esposizioni che va a costruire profili sempre più completi, predittivi e monetizzabili.

Estorsione senza cifratura: la pressione si sposta sul brand

A gennaio 2026 il dataset viene usato per quello che, a tutti gli effetti, è un tentativo di estorsione: gli attaccanti contattano SoundCloud chiedendo denaro per evitare la pubblicazione del dump.
La logica è quella ben nota del double extortion del ransomware, ma senza componente di cifratura: niente file bloccati, solo la minaccia reputazionale e legale derivante dalla diffusione del data-set.
Quando la trattativa fallisce, il database viene pubblicato online nelle settimane successive. Nel frattempo, gli attori mettono in campo tattiche di fastidio organizzato: campagne di email flooding contro utenti, dipendenti e partner, per aumentare la pressione e il costo operativo della gestione crisi.
È qui che il confine tra “data breach” classico ed ecosistema ransomware si fa sottile: gli stessi gruppi che orchestrano campagne di cifratura vera e propria hanno capito da tempo che non serve sempre bloccare i sistemi per ottenere leva negoziale. Un pannello interno poco difeso, una massa critica di dati personali e un brand globale con un’utenza fortemente esposta al phishing bastano per costruire una storia di estorsione credibile.

Attori e contesto criminale

Diverse fonti collegano l’operazione al gruppo ShinyHunters, già noto per campagne di furto dati e ricatto su larga scala, inclusi tentativi recenti contro ambienti SSO di colossi come Okta, Microsoft e Google.
Se confermato, il collegamento rafforza l’idea di un threat actor specializzato nella monetizzazione di grandi data-set, capace di muoversi indifferentemente tra dark web, marketplace di credential e tecniche di pressione diretta sulle vittime corporate.
In questo quadro SoundCloud non è un obiettivo isolato, ma un tassello: un’enorme piattaforma consumer, con un pubblico giovane, creativo e spesso già esposto ad altre compromissioni, ideale per campagne successive di phishing, account takeover e truffe mirate.

Impatti reali: dalla privacy al phishing industriale

Un argomento ricorrente nelle prime fasi di incidenti come questo è la minimizzazione: “sono solo dati pubblici”.
Ma aggregare e correlare informazioni “pubbliche” cambia radicalmente il profilo di rischio: l’email collegata all’handle SoundCloud, associata a follower/following e Paese, diventa materia prima perfetta per phishing mirato, impersonation, scam creativi e campagne di social engineering di massa.

Esempi plausibili, alla portata di qualunque spammer che scarichi il dump:
- Email di phishing che imitano notifiche SoundCloud (“nuovo commento”, “violazione copyright”, “problema con la monetizzazione”), con riferimenti reali a username e metriche per sembrare legittime.
- Tentativi di takeover tramite reset password su altri servizi, sapendo che la stessa email è ricorrente in più piattaforme già compromesse.
- Campagne di scam rivolte specificamente a creator con molti follower – visibili nel dump – a cui proporre finti accordi commerciali o richieste di pagamento.

Per la piattaforma, l’impatto si traduce in ondate di segnalazioni, possibile aumento del churn, costi investigativi e legali, oltre al danno d’immagine per un servizio che vive sulla fiducia della community.
Per gli utenti, il rischio non è tanto l’account SoundCloud in sé, quanto l’aumento di superficie di attacco nella loro vita digitale complessiva, in un ecosistema dove – lo mostra il 67% di indirizzi ricorrenti – la maggior parte è già stata “pwned” altrove.

Lezioni per chi difende: API, dashboard e threat model

Per un lettore esperto, il caso SoundCloud è un laboratorio di lezioni pratiche più che l’ennesimo numero da aggiungere alle statistiche dei breach.

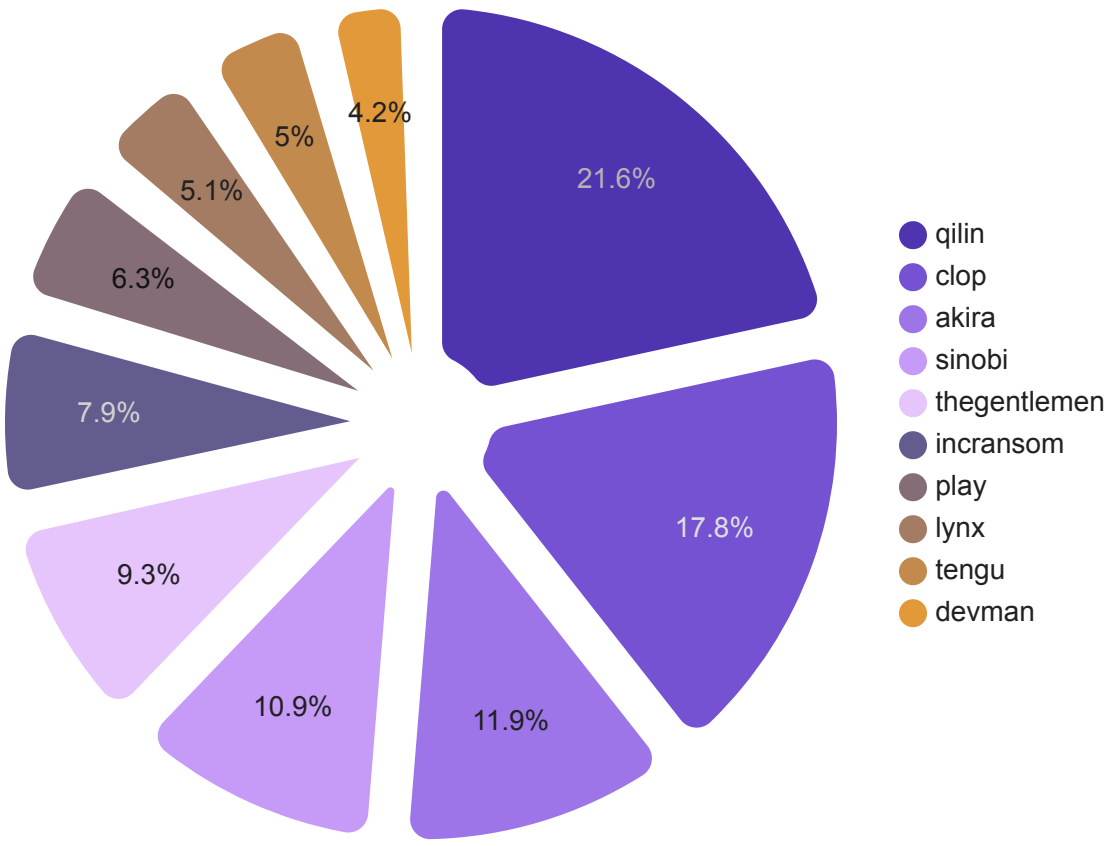
Alcuni punti chiave:
- Perimetro interno come “nuovo esterno”: dashboard di servizio e interfacce amministrative vanno progettate assumendo che possano essere raggiunte e sondate da un attaccante, con hardening, MFA forte, bastion host, logging aggressivo e riduzione radicale della superficie esposta.
- API e autenticazione: debolezze nell’autenticazione o autorizzazione di API interne – o credenziali di dipendenti poco protette – trasformano servizi pensati per uso operativo in potenti strumenti di estrazione dati.
- Data minimization anche lato pannelli: se una dashboard non ha motivo di mostrare 1:1 email + profilo pubblico per 30 milioni di account, quella correlazione non dovrebbe esistere o dovrebbe essere dietro ulteriori barriere di accesso.
- Prepararsi all’estorsione “senza ransomware”: i playbook di risposta devono contemplare scenari di ricatto basati solo su stolen data, inclusa la gestione della comunicazione pubblica, le valutazioni legali su eventuali pagamenti e l’uso proattivo di servizi come HIBP per notifiche mirate.

Scena internazionale 🌐

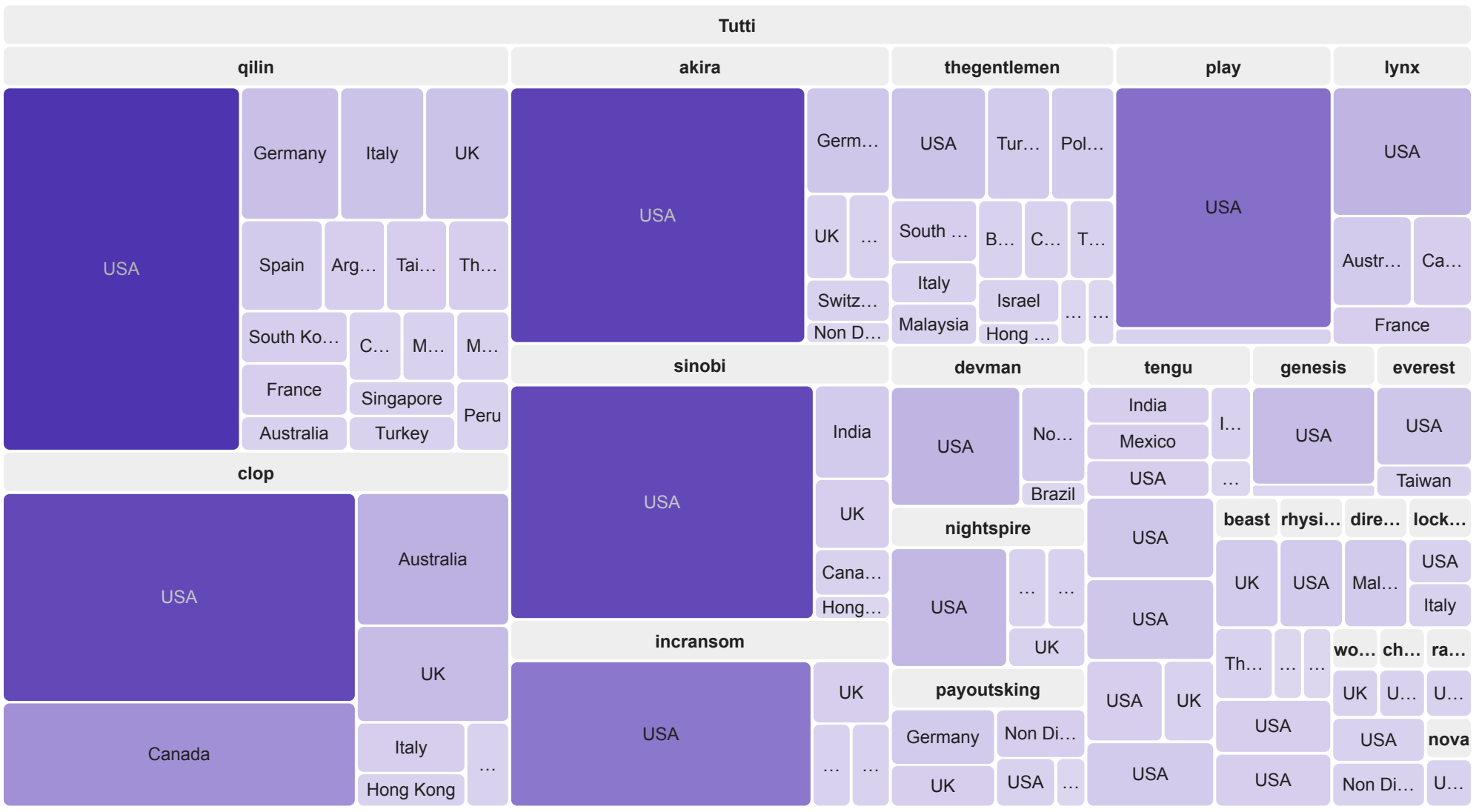
Vittime	Gruppi attivi	Paesi colpiti
692	49	69

Si fa notare che il mese di gennaio 2026 vede un incremento del **33,6%** rispetto allo stesso periodo dell'anno precedente (gennaio 2025: 518 rivendicazioni).

TOP 10 gruppi criminali

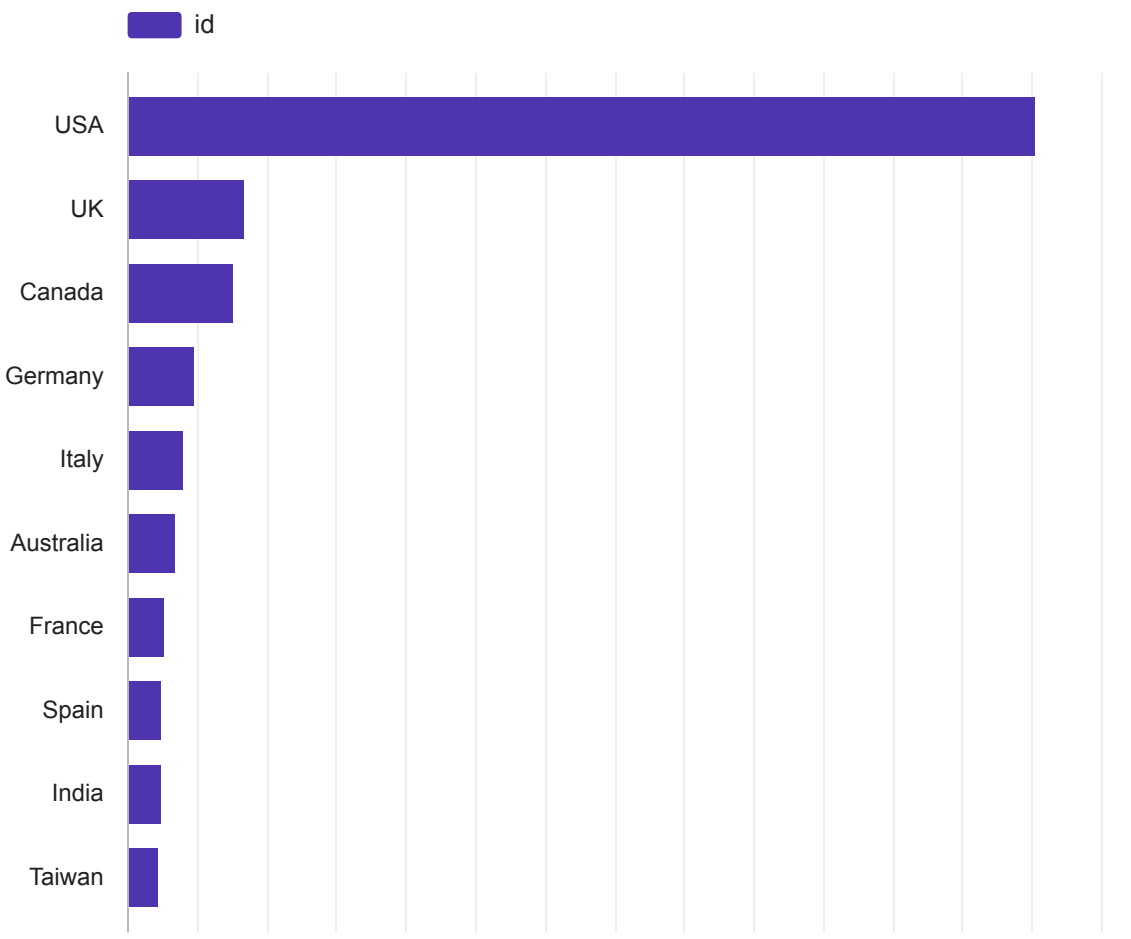


	GRUPPO	VITTIME
1.	qilin	109
2.	clop	90
3.	akira	60
4.	sinobi	55
5.	thegentlemen	47
6.	incransom	40
7.	play	32
8.	lynx	26
9.	tengu	25
10.	devman	21
11.	nightspire	18
12.	payoutsking	16
13.	everest	13
14.	direwolf	12
15.	genesis	11
16.	safepay	10
17.	dragonforce	9
18.	lockbit5	8
19.	coinbasecartel	7
20.	nova	6
21.	Altri	77

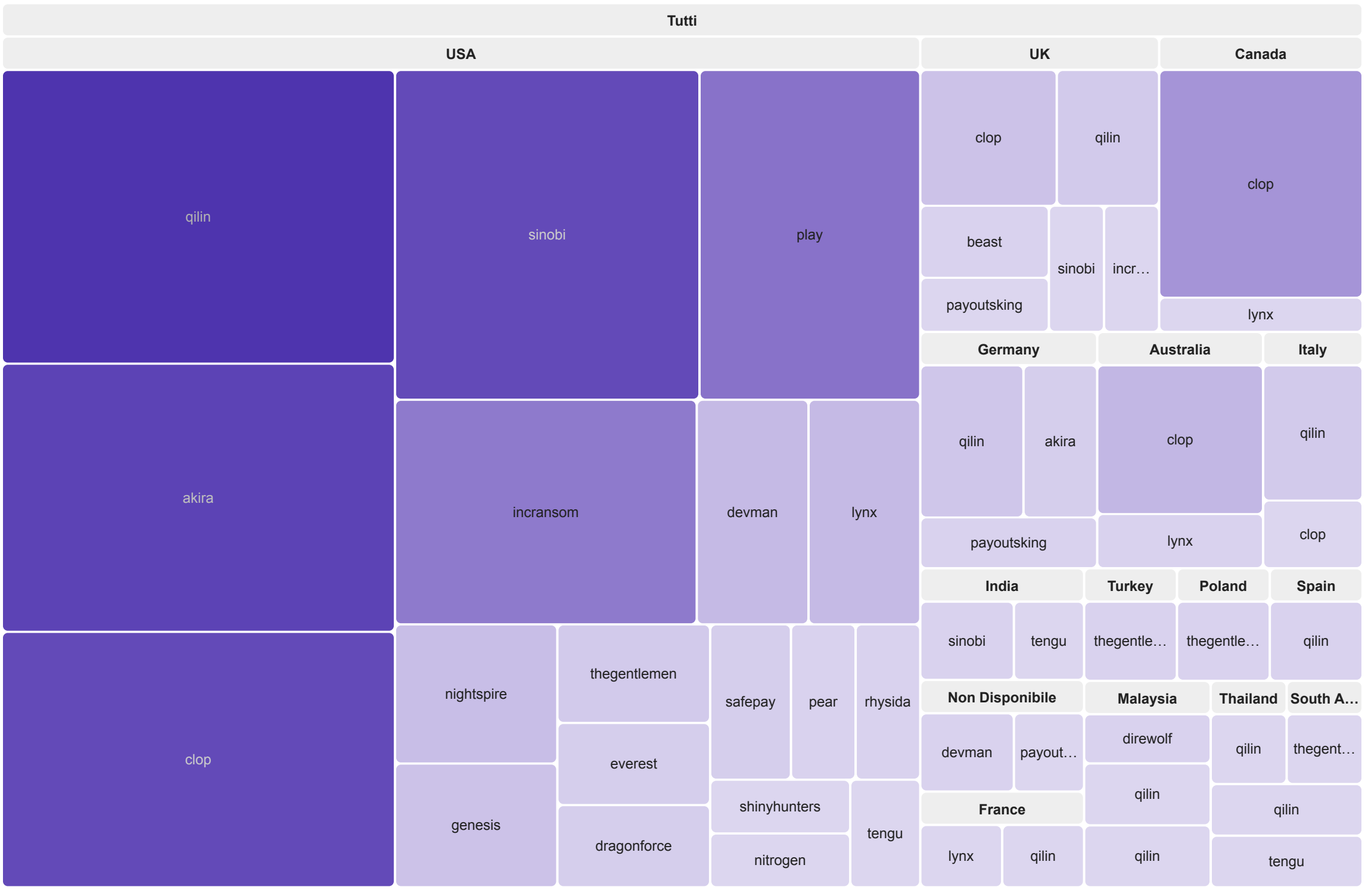


Scena internazionale 🌐

TOP 10 Paesi colpiti

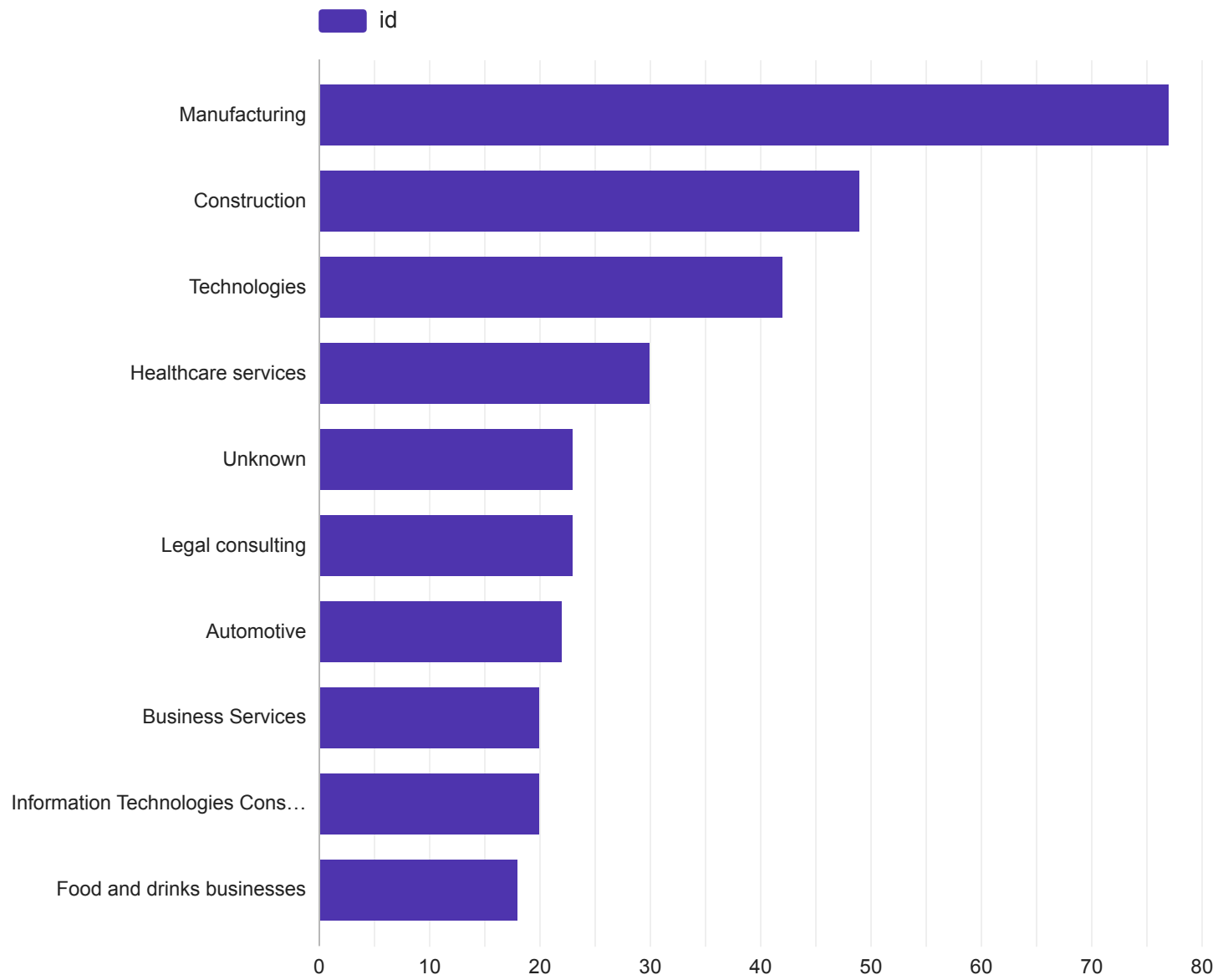


	PAESE	VITTIME
1.	USA	324
2.	UK	42
3.	Canada	38
4.	Germany	24
5.	Italy	20
6.	Australia	17
7.	France	13
8.	Spain	12
9.	India	12
10.	Taiwan	11
11.	Non Disponibile	11
12.	Thailand	10
13.	Brazil	9
14.	Turkey	8
15.	Malaysia	8
16.	Poland	8
17.	Mexico	7
18.	Hong Kong	6
19.	Israel	5
20.	Argentina	5
21.	Altri	98

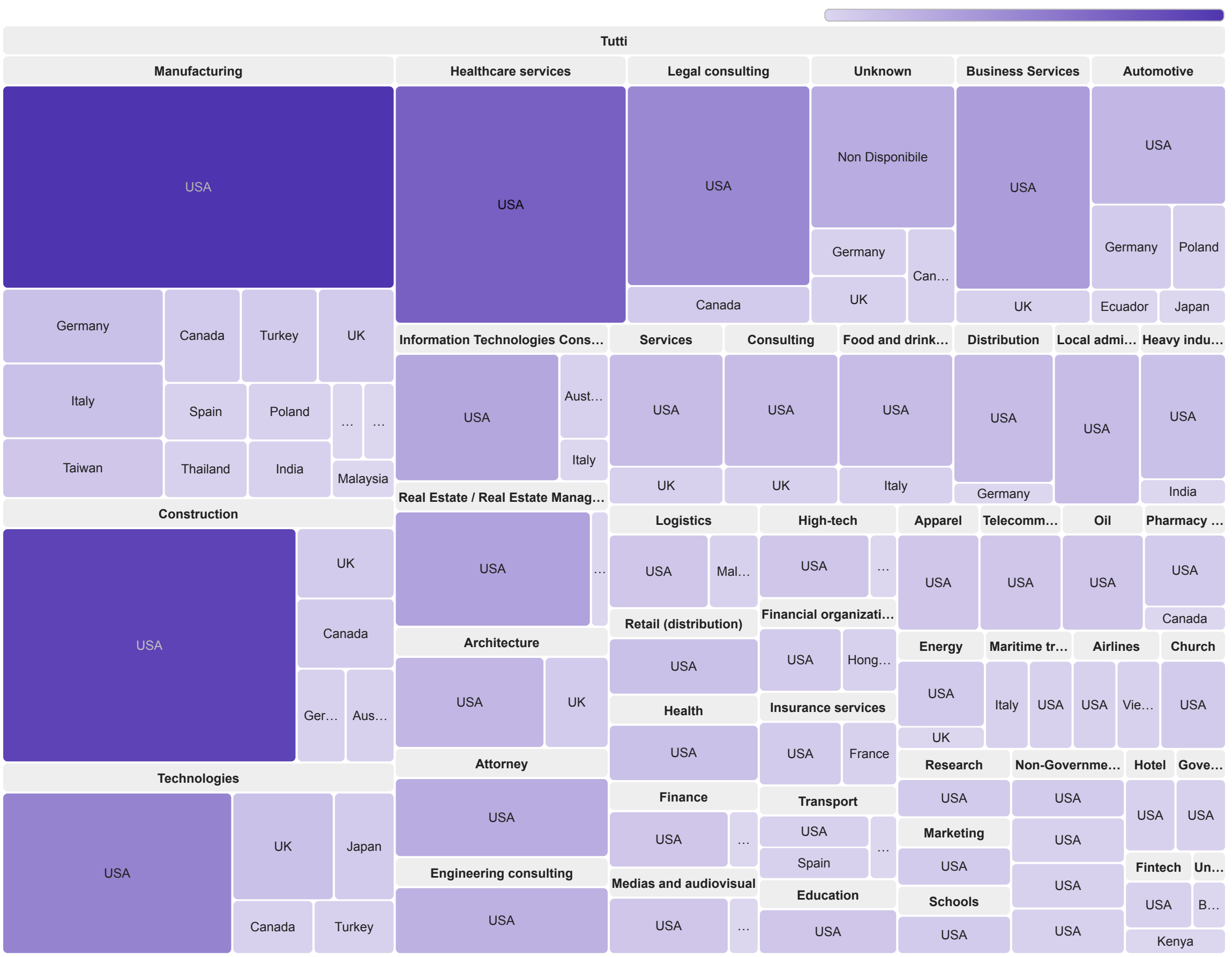


Scena internazionale 🌐

TOP 10 Settori economici



	SETTORE	VITTIME
1.	Manufacturing	77
2.	Construction	49
3.	Technologies	42
4.	Healthcare services	29
5.	Unknown	23
6.	Legal consulting	23
7.	Automotive	22
8.	Business Services	20
9.	Information Technologies Co…	20
10.	Food and drinks businesses	18
11.	Real Estate / Real Estate M…	15
12.	Engineering consulting	15
13.	Distribution	14
14.	Financial organizations	13
15.	Services	13
16.	Consulting	13
17.	Retail (distribution)	13
18.	Attorney	12
19.	Architecture	12
20.	Local administrations	11
21.	Altri	236



Vulnerabilità sfruttate dai gruppi ransomware a gennaio 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.

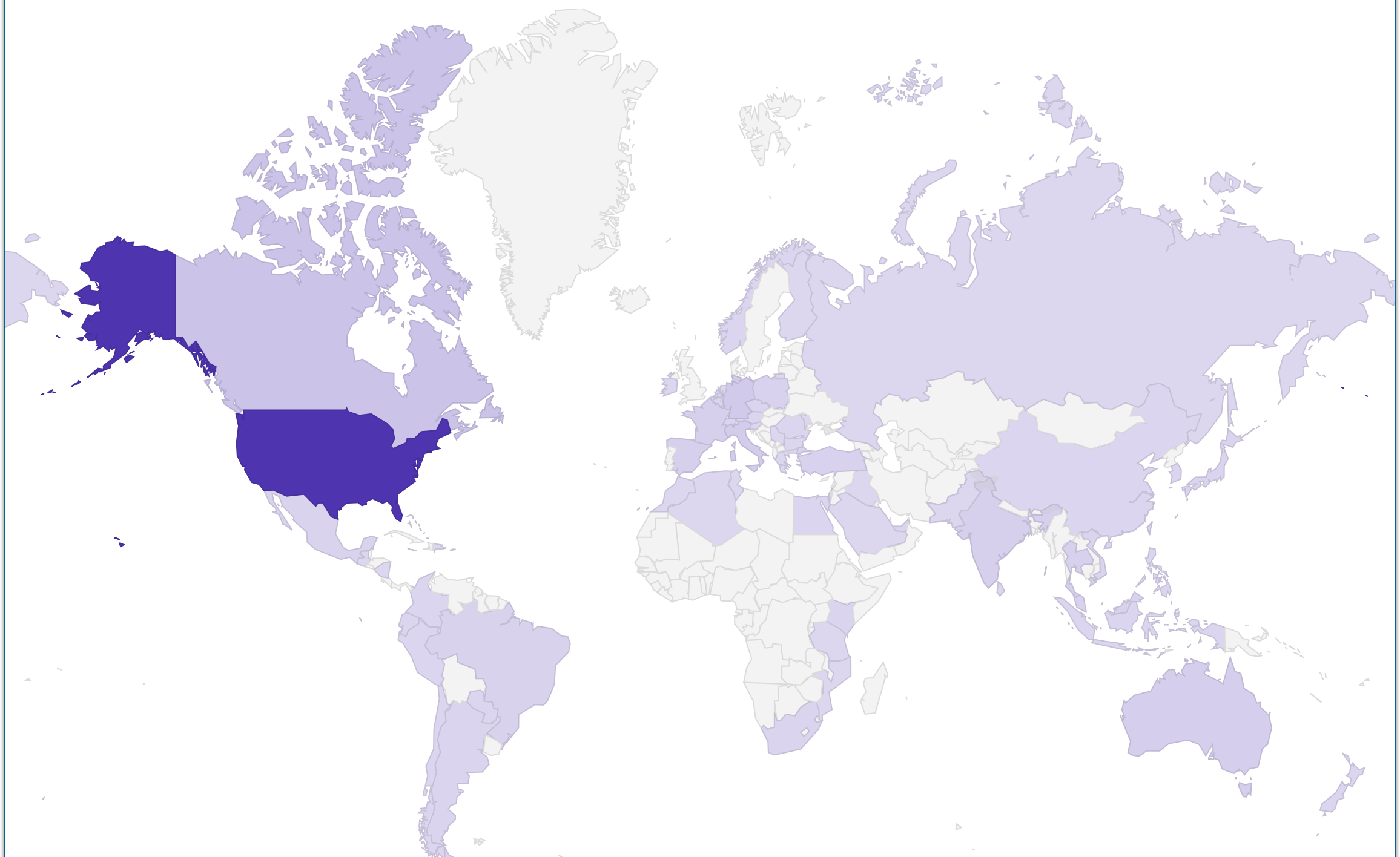
I threat actor hanno sfruttato attivamente queste falle in prodotti e sistemi operativi molto diffusi, prendendo di mira sia vulnerabilità nuovissime che falle note del passato.

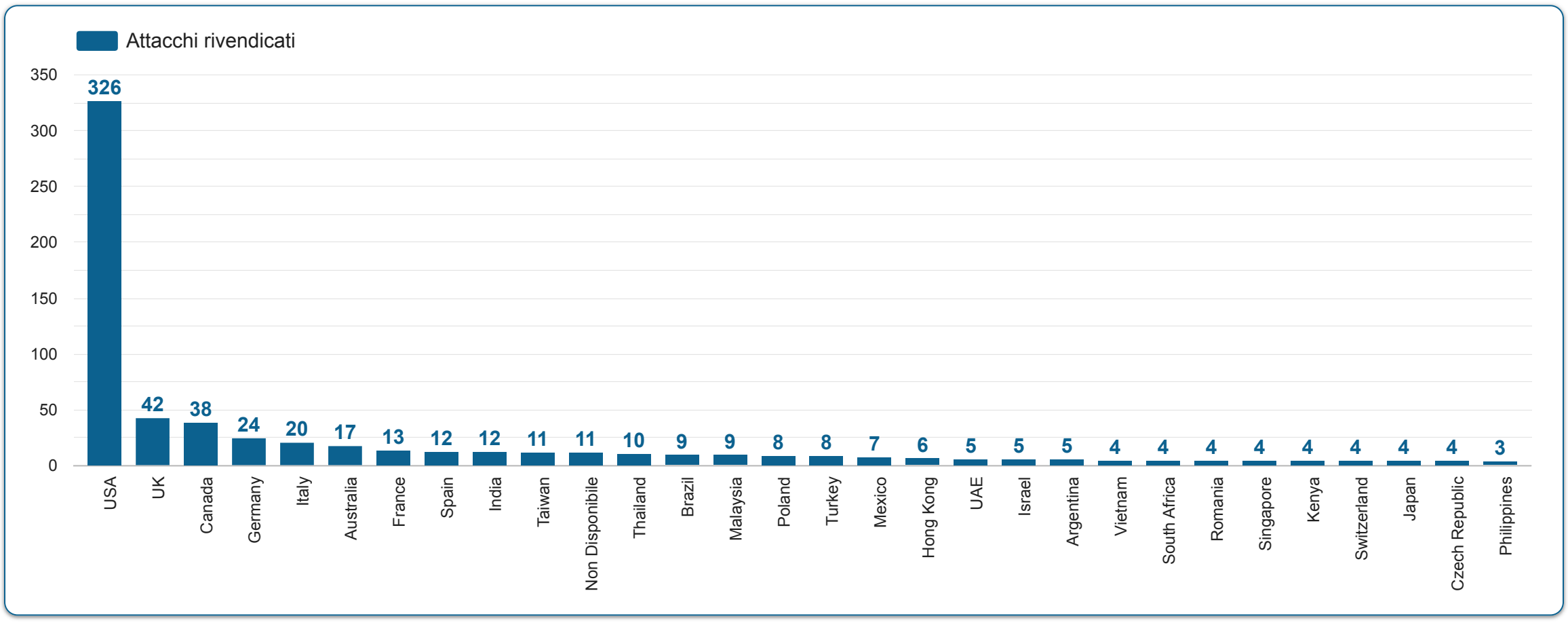
Questo scenario sottolinea l'importanza critica di un programma di patch management tempestivo e di una rigorosa gestione della superficie di attacco esposta online.

Tabella delle principali vulnerabilità sfruttate da ransomware (Gennaio 2026)

	Prodotto Vulnerabile	CVE	Tipologia Vulnerabilità	Gruppo Ransomware Associato
1.	Cisco Unified Communications Manager	CVE 2026 20274	Remote Code Execution	N/A
2.	D-Link DSL Router	CVE-2026-0625	Command Injection (RCE)	N/A
3.	Advanced Custom Fields WordPress Plugin	CVE 2025-7890	Privilege Escalation	N/A
4.	Microsoft Office	CVE 2025 38067	Remote Code Execution (Zero-Day)	N/A
5.	Fortinet FortiGate	CVE 2025 12825	Authentication Bypass / Unauthorized Access	N/A
6.	VMware Aria Suite (vRealize Operations, vRealize Log Insight)	CVE 2026 20860	Remote Code Execution	N/A
7.	vm2 NodeJS Library	CVE 2025 3421	Sandbox Escape / Remote Code Execution	N/A
8.	Zendesk	N/A	Account Hijacking	Sconosciuto
9.	SonicWall Cloud Backup	N/A	Unauthorized Access / Data Encryption	Sconosciuto
10.	SmarterMail Servers	N/A	Account Hijacking / Configuration Issues	Sconosciuto
11.	Chainlit AI Framework	CVE 2025 4697	Sandbox Escape	N/A
12.	eScan Update Server	N/A	Server Breach / Malicious Update Distribution	RATANKBA (Malware)
13.	Veeam Backup Server	CVE-2025-4549	Remote Code Execution	N/A
14.	Fortinet FortiGate	CVE-2020-12812	Bypass Two-Factor Authentication	N/A
15.	Fortinet FortiGate	N/A	Breach / Configuration Theft	Sconosciuto
16.	GitLab	CVE 2025 5678	Two-Factor Authentication Bypass / Denial of Service	N/A
17.	Trend Micro Apex Central Console	CVE 2025 6694	Remote Code Execution	N/A
18.	Veeam Backup Server	CVE-2025-4550	Remote Code Execution	N/A

La scena globale mese Gennaio 2026





ransomfeed

ADVANCED **DATADRIVEN** CYBERNEWS

RECAP MENSILE
GENNAIO 2026

<eof>