ransomfeed

ADVANCED **DATADRIVEN** CYBERNEWS

RECAP MENSILE

DICEMBRE 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 dicembre 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.

- Le modifiche alla piattaforma per il mese di dicembre 2025 hanno riguardato principalmente miglioramenti lato backend sul pannello di amministrazione di Ransomfeed.

Focus Italia 🇮🇹

Nel mese di **dicembre 2025** la piattaforma ha rilevato un totale di **20 attacchi**.
Si fa notare che il mese di dicembre 2025 vede un incremento del 100% rispetto allo stesso periodo dell'anno precedente (dicembre 2024: 10 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

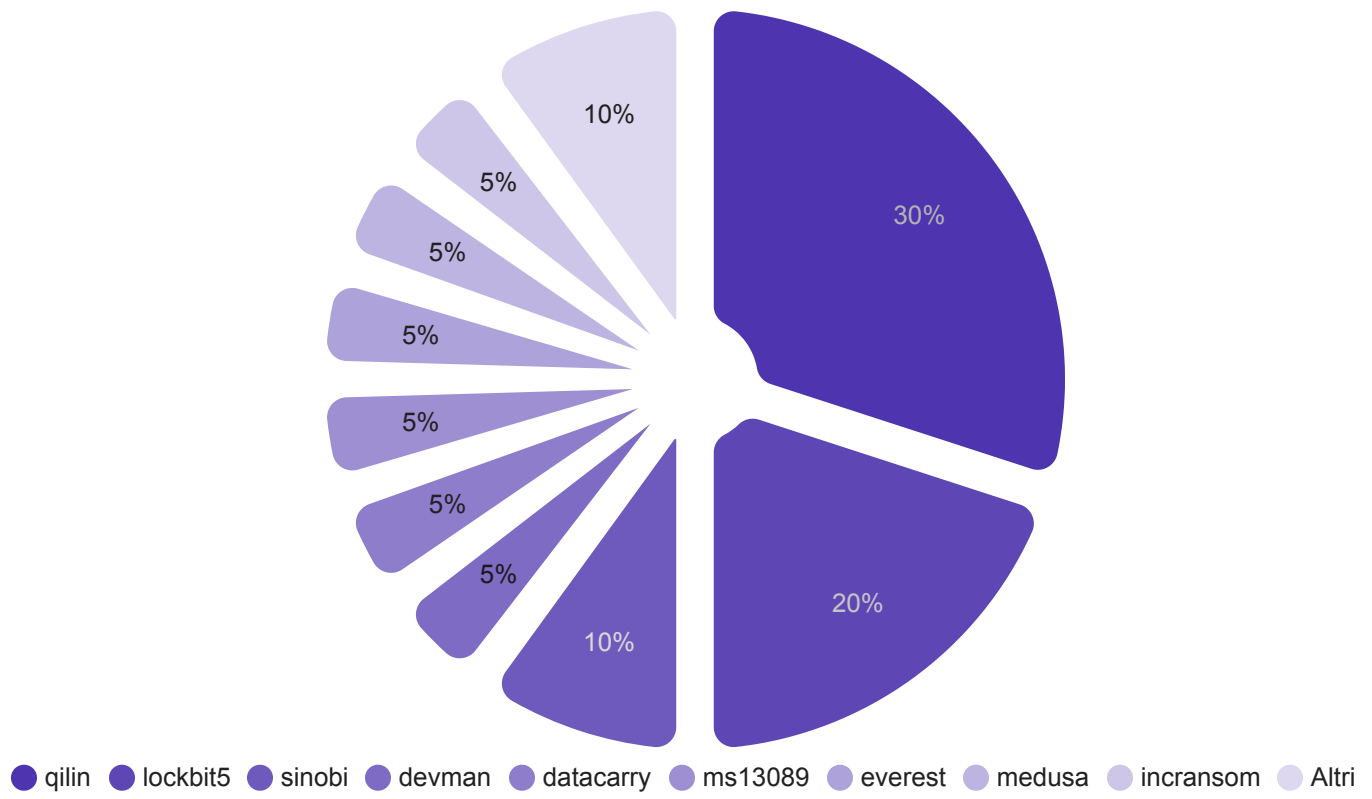
Vittime Italia	Totale GB pubblicati
20	419,82

	ID	GRUPPO	VITTIMA	DATI PUBBLICATI GB
1.	27572	devman	m*tt**ca**r**.**.it	0
2.	27593	qilin	Saca Industrie SpA	0
3.	27695	datacarry	Camomilla	0.1
4.	27735	lockbit5	milanoristorazione.it	171
5.	27740	lockbit5	iscot.it	12
6.	27744	lockbit5	comune.balmuccia.vc.it	85
7.	27886	qilin	Cdf	0
8.	28006	ms13089	dgpcommercialisti.it (Italy, Reggio Emilia)	0
9.	28044	sinobi	AIRCOND S.R.L.	0
10.	28050	everest	ELC Electroconsult SpA	0
11.	28108	sinobi	FHIABA	0
12.	28123	medusa	Callipo Group	66.62
13.	28188	incransom	Talarico	0
14.	28195	qilin	GIV SRL	63
15.	28217	qilin	Callipo Group	0
16.	28238	qilin	daispa.it	0
17.	28322	lockbit5	savantivibranti.com	22.1
18.	28363	chaos	VEPLASTIC	0
19.	28376	safepay	studioelad.it	0
20.	28402	qilin	SEACSUB S.p.a.	0

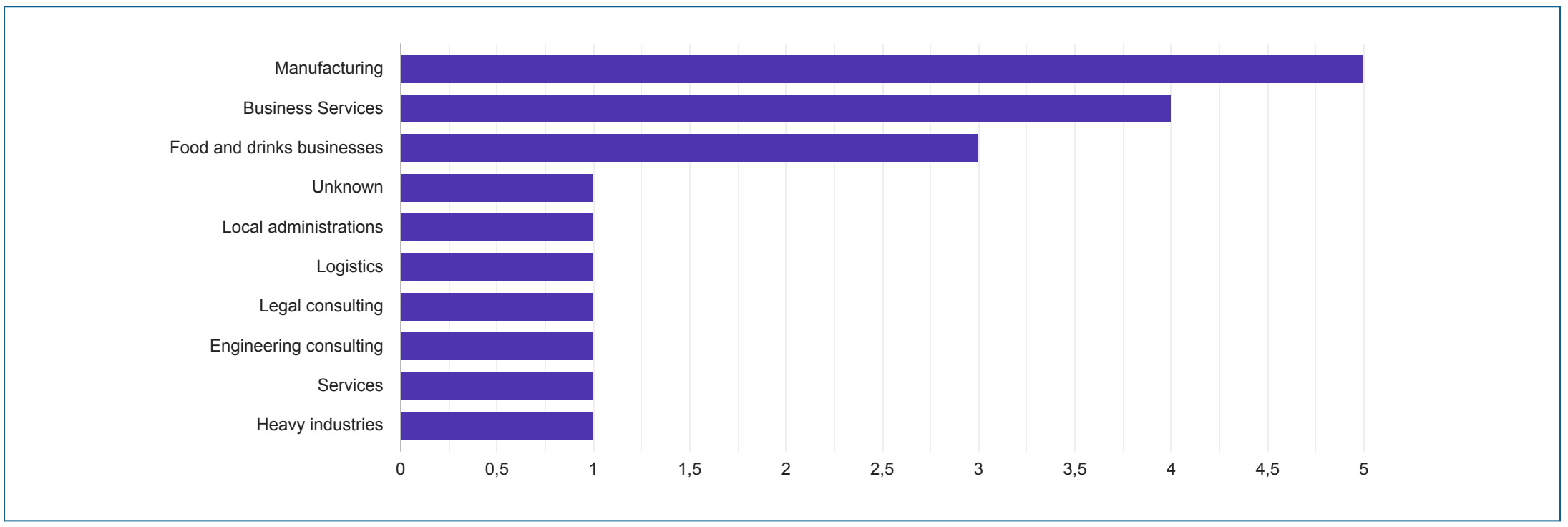
Gruppi criminali
focus Italia

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

	GRUPPO	VITTIME
1.	qilin	6
2.	lockbit5	4
3.	sinobi	2
4.	devman	1
5.	datacarry	1
6.	ms13089	1
7.	everest	1
8.	medusa	1
9.	incransom	1
1…	chaos	1
1…	safepay	1



Settori economici
focus Italia



Ransomware Story

Dicembre 2025: dalle tubature esplose ai campus paralizzati, il mese in cui il rischio è diventato "Fisico"

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.

Se novembre ci aveva insegnato che il ransomware può fermare la produzione di birra, dicembre 2025 ha alzato la posta in gioco, dimostrando che gli attacchi informatici possono avere conseguenze cinetiche e distruttive sulle infrastrutture vitali, pur continuando a dissanguare i dati di milioni di cittadini attraverso vulnerabilità note. Il mese si chiude con una lezione severa: il rischio cyber non è più confinato ai server, ma scorre letteralmente nelle tubature delle nostre città e nei corridoi delle nostre università.

Il caso Tureby Alkestrup: quando il cyberattacco rompe le tubature

L'incidente più allarmante del mese è avvenuto in Danimarca, dove un attacco informatico ha superato la barriera digitale per causare danni fisici. L'acquedotto di Tureby Alkestrup è stato colpito da un attacco distruttivo attribuito al gruppo filo-russo Z-Pentest.
L'impatto fisico: a differenza dei classici blocchi amministrativi, questo attacco ha provocato lo scoppio di tubature, lasciando intere famiglie senz'acqua.
Il significato: l'intelligence danese ha classificato l'evento come parte di una più ampia "guerra ibrida". Non si è trattato solo di estorsione, ma di sabotaggio mirato per destabilizzare la vita quotidiana dei civili. Questo segna un pericoloso precedente per la sicurezza delle utility europee nel 2026.

L'onda lunga di Cl0p: l'assedio alle Università

Mentre la Danimarca affrontava la crisi idrica, negli Stati Uniti il sindacato ransomware Cl0p continuava a sfruttare spietatamente le vulnerabilità di Oracle E-Business Suite (EBS), una campagna iniziata nei mesi precedenti ma esplosa in gravità a dicembre.
Le vittime: l'Università di Phoenix ha subito un colpo devastante, con il furto di dati sensibili (personali e finanziari) appartenenti a quasi 3,5 milioni di studenti, personale e fornitori. Anche l'Università della Pennsylvania è caduta vittima dello stesso schema, con esfiltrazione di dati confermata.
La tattica: Cl0p ha confermato la sua strategia di "data-theft-only" (solo furto dati), sfruttando falle di sicurezza in piattaforme terze per colpire su vasta scala senza necessariamente criptare l'intera rete, ma causando danni reputazionali immensi.

La nuova frontiera tecnica: caccia agli Hypervisor

Dicembre ha anche evidenziato un cambiamento tecnico critico nelle tattiche ransomware. I ricercatori hanno notato un picco negli attacchi mirati agli hypervisor (le piattaforme che gestiscono le macchine virtuali). Se nella prima metà del 2025 gli hypervisor erano coinvolti solo nel 3% degli attacchi, a fine anno questa cifra è salita al 25%. Gruppi come Akira stanno prendendo di mira queste infrastrutture per criptare centinaia di server virtuali in un colpo solo, rendendo il ripristino estremamente complesso.

Cosa ci portiamo nel 2026?

Dicembre 2025 ci lascia con tre avvertimenti chiari:
Proteggere l'OT (Operational Technology): il caso danese dimostra che i firewall non proteggono solo i dati, ma l'integrità fisica delle infrastrutture pubbliche.
Patching di terze parti: la vulnerabilità di Oracle EBS ha continuato a mietere vittime per settimane. La velocità di reazione alle patch critiche (come quelle rilasciate d'urgenza a fine anno per MongoDB e Fortinet) è l'unica difesa contro campagne massive.
L'estorsione senza fine: con gruppi come ShinyHunters che hanno ricattato aziende come PornHub sottraendo dati di 200 milioni di utenti, il modello di business criminale si sta spostando sempre più verso l'estorsione pura basata sulla sensibilità dei dati rubati.

DragonForce vs NK Technologies: il cartel RaaS scala in fine 2025

Timeline dell'attacco
Il 29 dicembre, DragonForce ha claimed l'attacco su suo leak site, annunciando cifratura completa e esfiltrazione di dati sensibili da nktechnologies.com, con minaccia di dump pubblico entro breve se non contattati via Tor o Tox. La victim profile – MSP con esposizione a dati IP, credenziali e PII – si allinea a target high-value per chain attacks su supply chain tech. Ransom note specifica warnings anti-forensic: no rename file, no reboot, contacts solo su canali anonimi, con timer per negoziazione.

Accesso iniziale e TTPs
Scattered Spider Affiliate Scattered Spider (aka 0ktapus/UNC3944) ha fornito initial access via vishing avanzato o MFA fatigue su employee NK Tech, pattern consolidato da retail UK (apr-mag 2025) a telco USA. Exploit include SIM swap per MFA bypass, social engineering su helpdesk, e OSINT da LinkedIn/DomainTools per recon mirato.MITRE mapping: T1190 (Supply Chain), T1566 (Phishing), T1621 (MFA Monitoring).
Post-accesso, handoff rapido al RaaS core per escalation.

Post-exploit e encrypt chain
Post-breach, deployment di BYOVD (Bring Your Own Vulnerable Driver) per kill AV/EDR (es. vuln drivers come in SimpleHelp CVE-2025-XXXX), lateral movement via Cobalt Strike-like beacons, e esfil su C2 Proton66-geoloc Russia. Encryptor deriva da leaked Conti/LockBit 3.0 source: obfuscated binary con anti-analysis (string encoding, API hashing), multi-thread encrypt % based on file size/ext (.docx, .sql prioritari), e multi-extortion (leak + DDoS threat). Forensics rivela custom ransom note w/ leak site countdown e revenue share basso (20%) per attrarre affiliate low-skill.

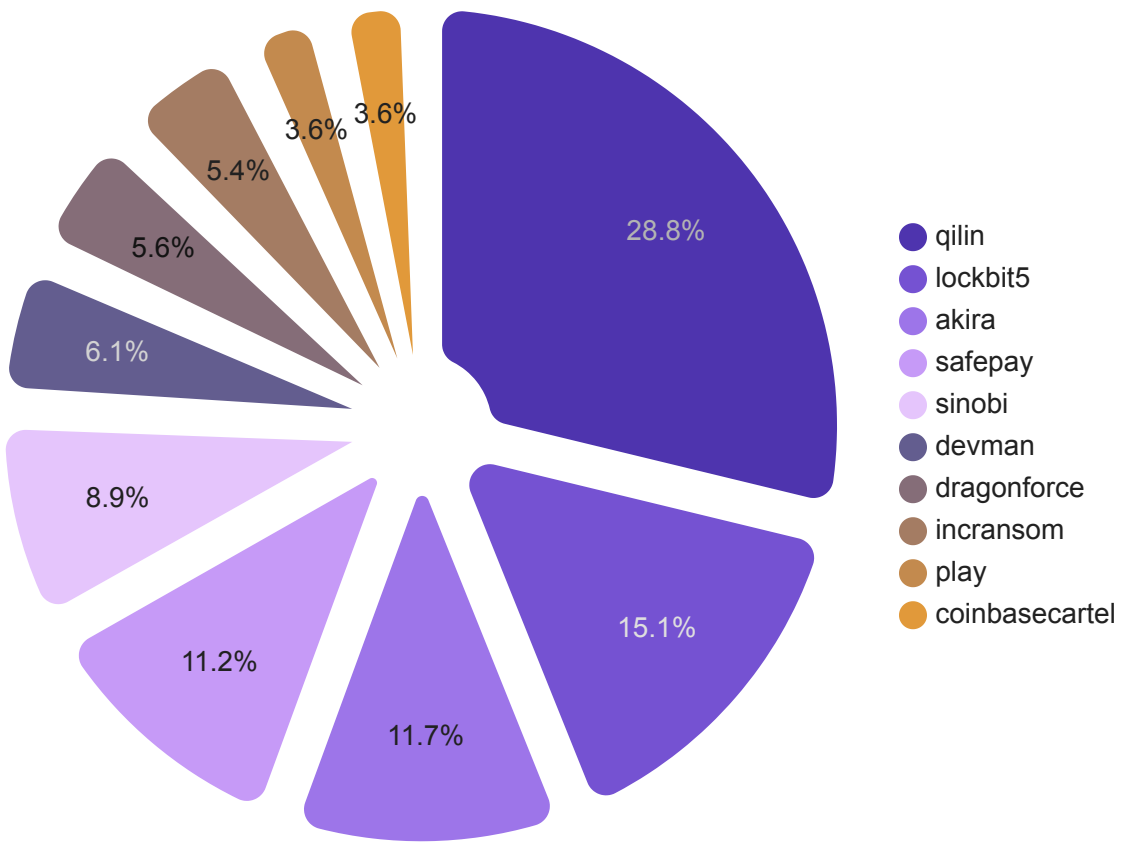
Evoluzione cartel dicembre 2025
Dicembre segna picco DragonForce post-rebranding: >200 victims totali, white-label kits (binaries, notes, infra RansomBay), e alleanza Scattered Spider per initial access broker. Trend contestualizzato da FinCEN (21B$ estorti 2022-24) e MITRE Top 25 CWE (Out-of-bounds Write, Deserialization), con focus su RaaS industrializzazione: dev kit, revenue share, servizi premium (C2-as-service). Differenza da LockBit: più agile, meno leak site drama, ma hybrid extortion scalabile su MSP chain risks.

Scena internazionale 🌐

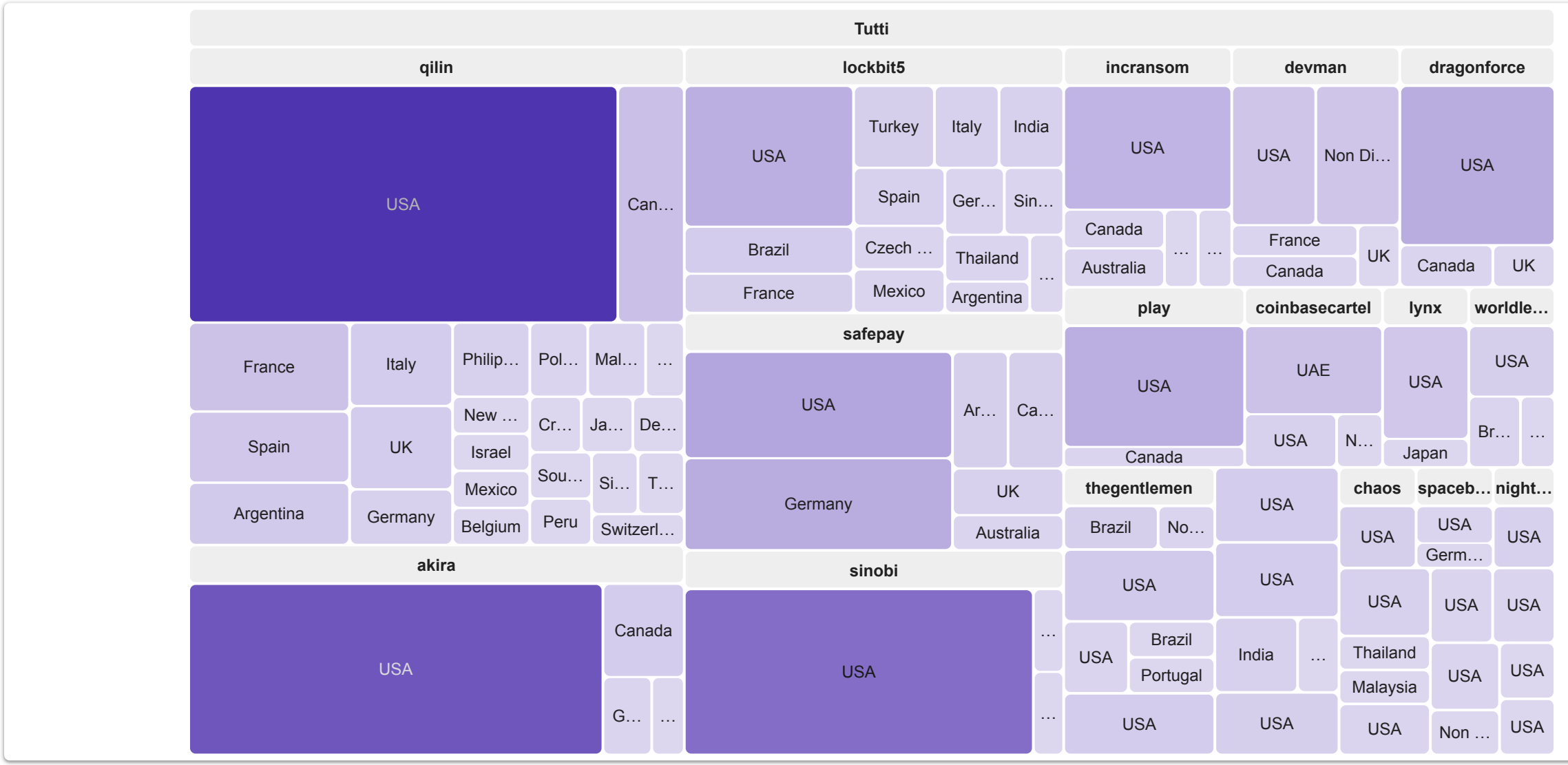
Vittime	Gruppi attivi	Paesi colpiti
817	53	69

Si fa notare che il mese di dicembre 2025 vede un incremento del **68,8%** rispetto allo stesso periodo dell'anno precedente (dicembre 2024: 484 rivendicazioni).

TOP 10 gruppi criminali

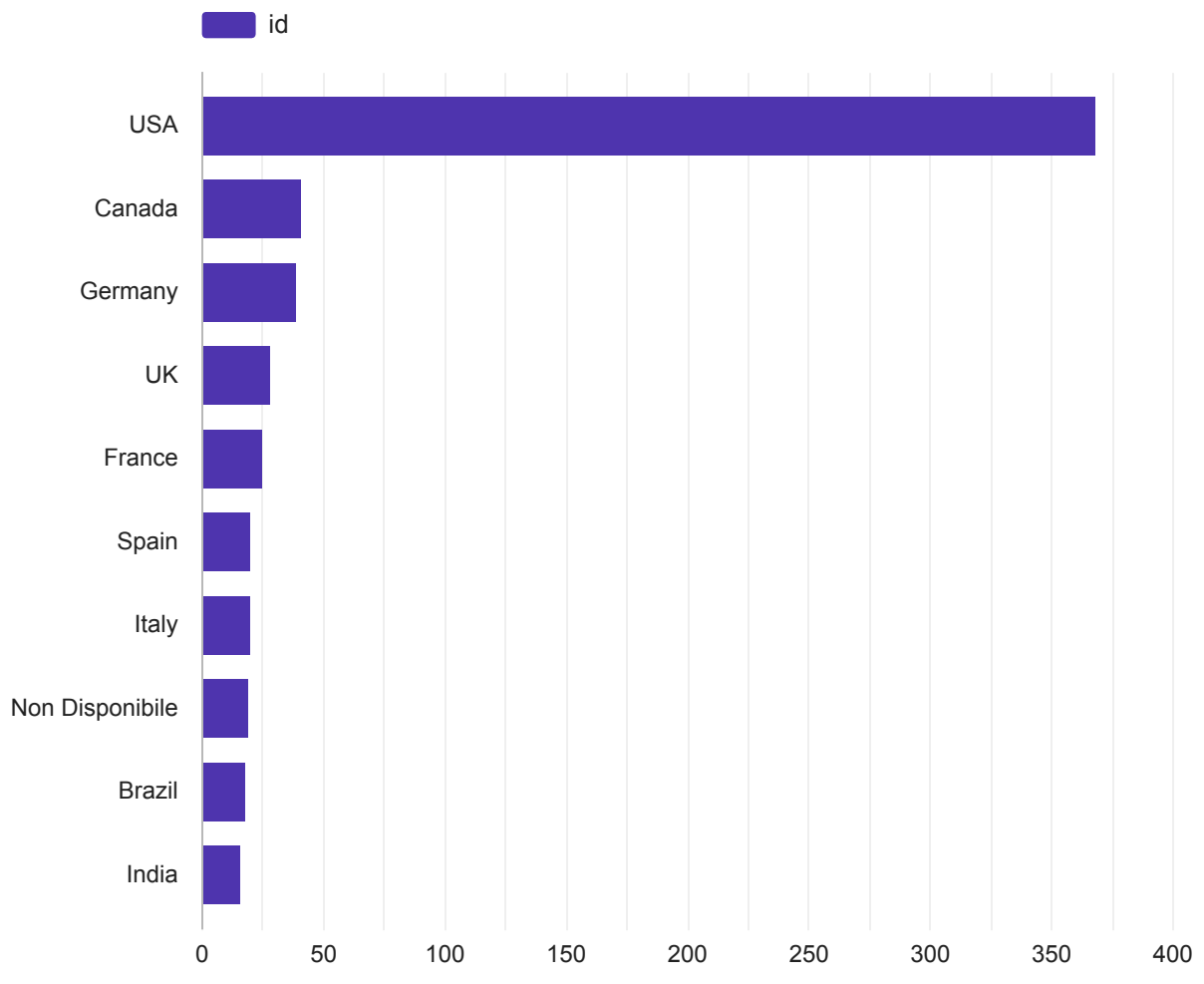


	GRUPPO	VITTIME
1.	qilin	175
2.	lockbit5	92
3.	akira	71
4.	safepay	68
5.	sinobi	54
6.	devman	37
7.	dragonforce	34
8.	incransom	33
9.	play	22
10.	coinbasecartel	22
11.	lynx	14
12.	worldleaks	13
13.	thegentlemen	13
14.	rhysida	11
15.	nova	11
16.	anubis	10
17.	everest	9
18.	ransomhouse	9
19.	genesis	8
20.	nightspire	8
21.	Altri	103



Scena internazionale 🌐

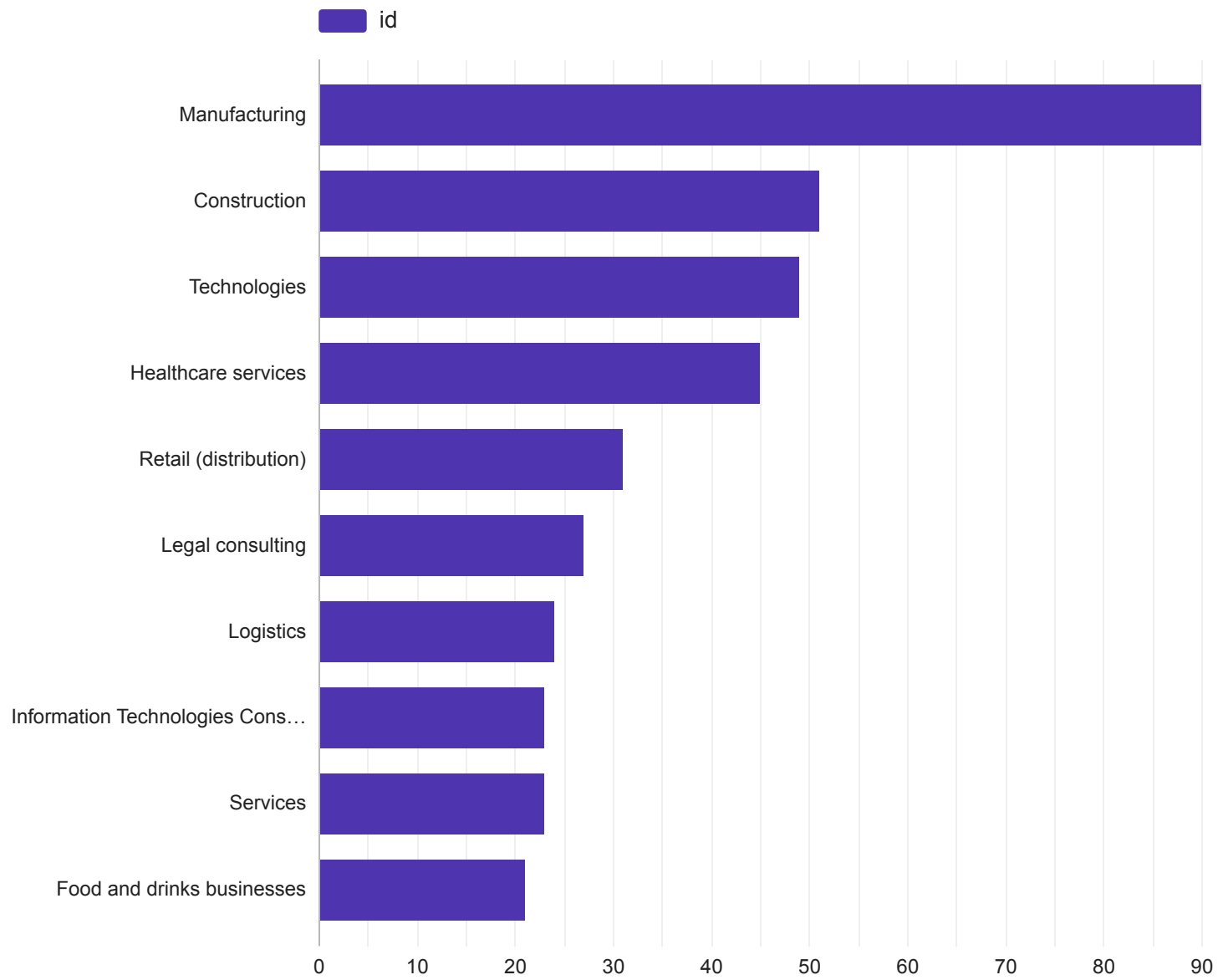
TOP 10 Paesi colpiti



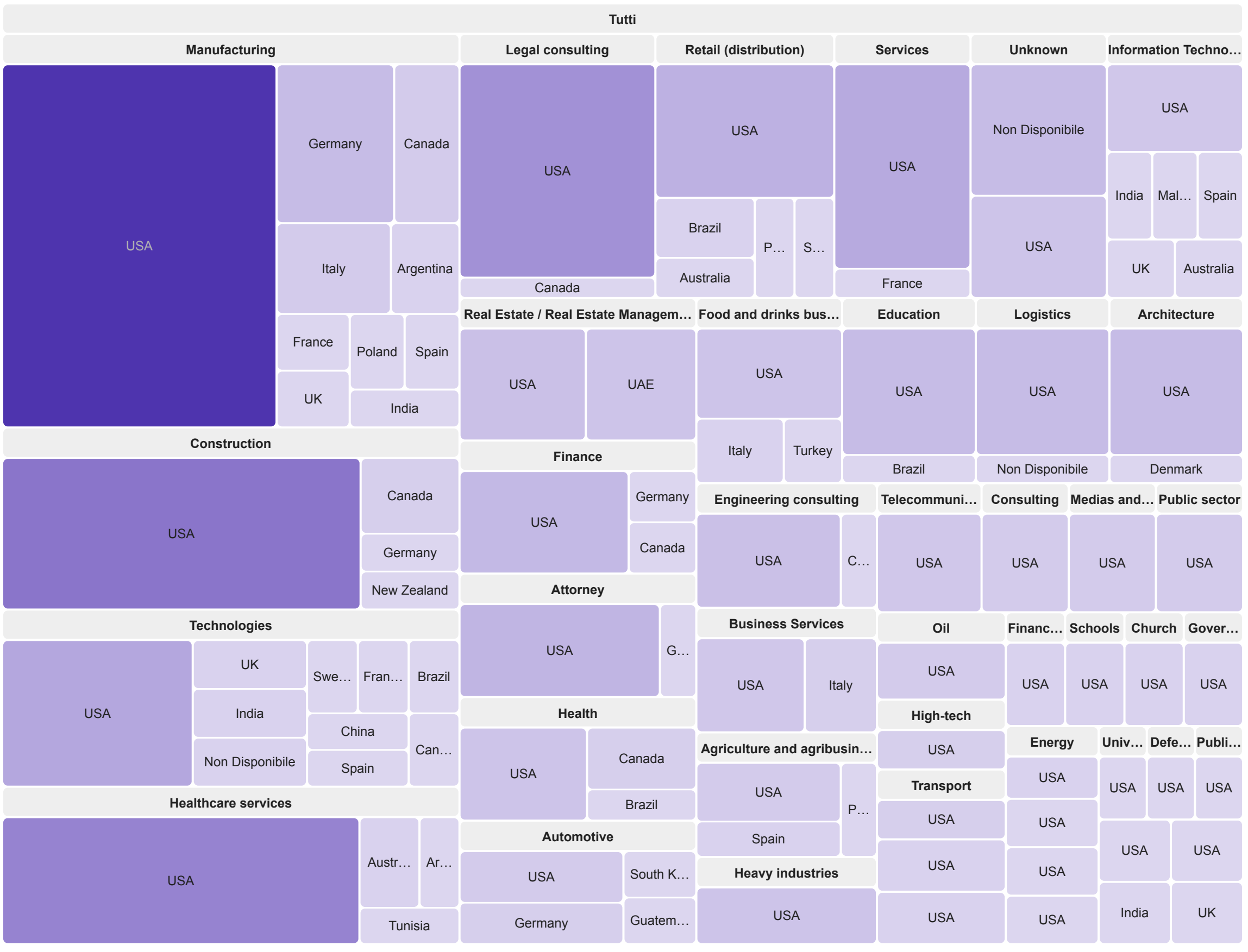
	PAESE	VITTIME
1.	USA	367
2.	Canada	41
3.	Germany	39
4.	UK	28
5.	France	25
6.	Spain	20
7.	Non Disponibile	19
8.	Italy	19
9.	Brazil	18
10.	India	16
11.	Argentina	14
12.	UAE	13
13.	Turkey	11
14.	Australia	10
15.	Japan	10
16.	Malaysia	9
17.	Thailand	9
18.	Philippines	7
19.	Poland	7
20.	Switzerland	7
21.	Altri	125

Scena internazionale 🌐

TOP 10 Settori economici



	SETTORE	VITTIME
1.	Manufacturing	90
2.	Construction	51
3.	Technologies	49
4.	Healthcare services	44
5.	Retail (distribution)	31
6.	Legal consulting	27
7.	Logistics	24
8.	Information Technologies Co…	23
9.	Services	23
10.	Food and drinks businesses	21
11.	Automotive	21
12.	Agriculture and agribusiness	20
13.	Finance	20
14.	Real Estate / Real Estate M…	20
15.	Unknown	20
16.	Engineering consulting	18
17.	Health	18
18.	Attorney	18
19.	Education	17
20.	Business Services	16
21.	Altri	244



Vulnerabilità sfruttate dai gruppi ransomware a dicembre 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.

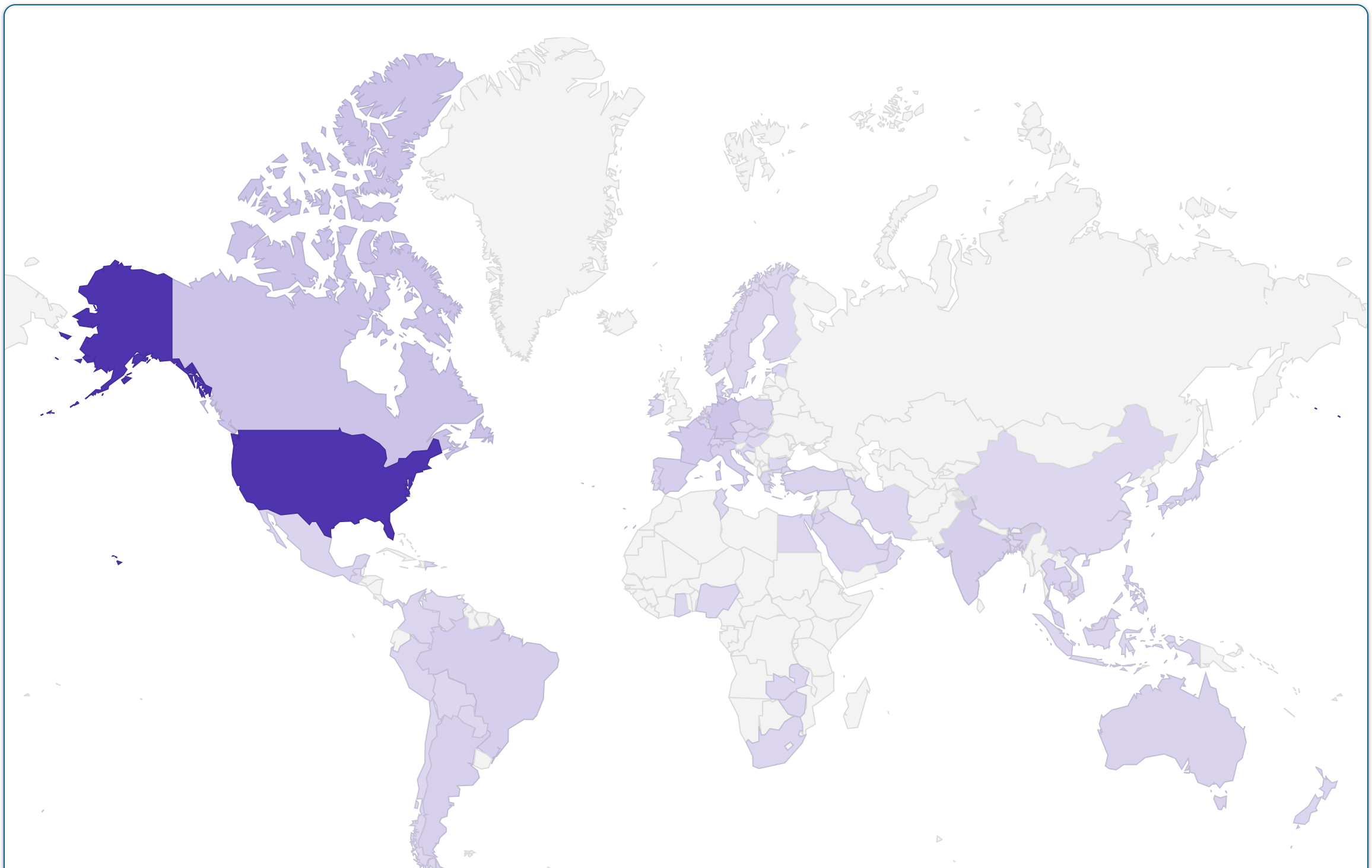
I threat actor hanno sfruttato attivamente queste falle in prodotti e sistemi operativi molto diffusi, prendendo di mira sia vulnerabilità nuovissime che falle note del passato.

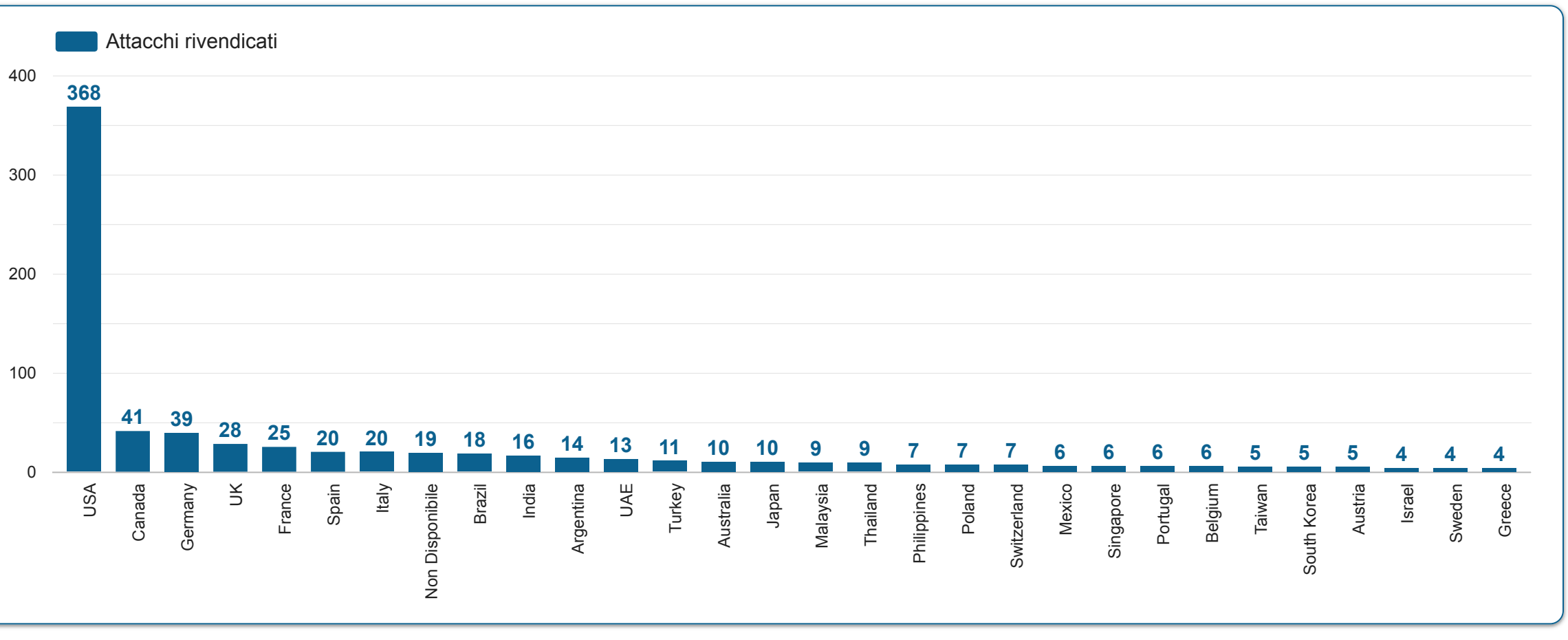
Questo scenario sottolinea l'importanza critica di un programma di patch management tempestivo e di una rigorosa gestione della superficie di attacco esposta online.

Tabella delle principali vulnerabilità sfruttate da ransomware (Dicembre 2025)

Prodotto/Sistema Vulnerabile	CVE	Tipologia di Vulnerabilità	Gruppo Ransomware Associato
Oracle E-Business Suite (EBS)	CVE-2025-61882*	Vulnerabilità Zero-day	Cl0p Ransomware Gang
Hypervisor (Infrastrutture Virtuali)	-	Compromissione ambienti virtuali	Akira Ransomware
Fortinet (FortiOS, FortiProxy)	CVE-2025-59718	Bypass dell'Autenticazione	-
MongoDB	CVE-2025-14847	Information Disclosure	-
WinRAR	CVE-2025-6218	Directory Traversal	APT-C-08
SmarterTools SmarterMail	CVE-2025-52691	Remote Code Execution (RCE)	-
OSGeo GeoServer	CVE-2025-58360	XML External Entity (XXE)	-
Array Networks AG VPN	CVE-2025-66644	Command Injection (RCE)	-
Apache Tika	CVE-2025-66516	XML External Entity (XXE)	-

La scena globale mese Dicembre 2025





ransomfeed

ADVANCED **DATADRIVEN** CYBERNEWS

RECAP MENSILE
DICEMBRE 2025

<eof>