ransomfeed

ADVANCED **DATADRIVEN** CYBERNEWS

# RECAP MENSILE

# LUGLIO 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 luglio 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.

- Implementazione **RQL** (Ransomfeed Query Language): *bottone giallo di fianco a motore di ricerca tradizionale* - una sintassi che permetti ricerche avanzate con un grande numero di parametri, lasciando la libertà all'utente di estrarre i dati che interessano in quella specifica ricerca. Le ricerche effettuate contengono un link univoco, che si può copiare e salvare per accessi futuri, o condividere con altri per mostrare i medesimi risultati ad altri utenti.

- **Gestione notifiche**: *icona campanellina in alto a destra* - migliorata l'usabilità con notifiche più recenti in alto nel menu e di colore giallo; icona con badge numerico su campanellina nella prima settimana di introduzione di una (o più) nuova notifica; introdotto pulsante "MOSTRA TUTTE" con archivio notifiche completo.

- **OpenCTI connector**: pubblicata prima versione del connector con codice scaricabile da link Gitea (dentro sezione *Feeds*); si sta lavorando per integrazione dentro il progetto ufficiale di OpenCTI di modo che diventi un connector ufficiale.

- **API pubbliche**: introdotta nuova versione delle API (nulla cambia in termini di endpoint da utilizzare), nuove funzioni e nuovi endpoint, tutti ben rappresentati nella documentazione per API da *icona gialla (nuvola) su topbar* del progetto.

- **Pagina RSS**: razionalizzata la pagina dei feed che ora offre all'utente tutte le possibilità di connessione che la piattaforma offre, riportando collegamenti per i classici feed RSS2.0, le API pubbliche e il connector OpenCTI.

- **Sezione News**: introdotta nuova funzione con rassegne giornaliere su mondo cyber/ransomware/databreach, visionabile in titoli, oppure consultabile nel dettaglio di ogni news con link alla fonte originale. Il flusso delle notizie è diffuso anche mediante feed RSS specifico (separato da quello delle rivendicazioni ransomware).

- **Ampliamento Forum**: il forum di discussione aumenta di grandezza e offre maggiori subforum sui quali intervenire. All'interno anche ricerche e analisi specifiche (spesso con IoC utili). Ogni news della rassegna diventa un thread su cui poter discutere, così come anche tutti gli articoli del Network di Dario Fadda (insicurezzadigitale.com - ziobudda.org - spcnet.it).

## Focus Italia 🇮🇹

Nel mese di **luglio 2025** la piattaforma ha rilevato un totale di **21 attacchi**.
Si fa notare che il mese di luglio 2025 vede un **incremento del 61,54%** rispetto allo stesso periodo dell'anno precedente (luglio 2024: 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

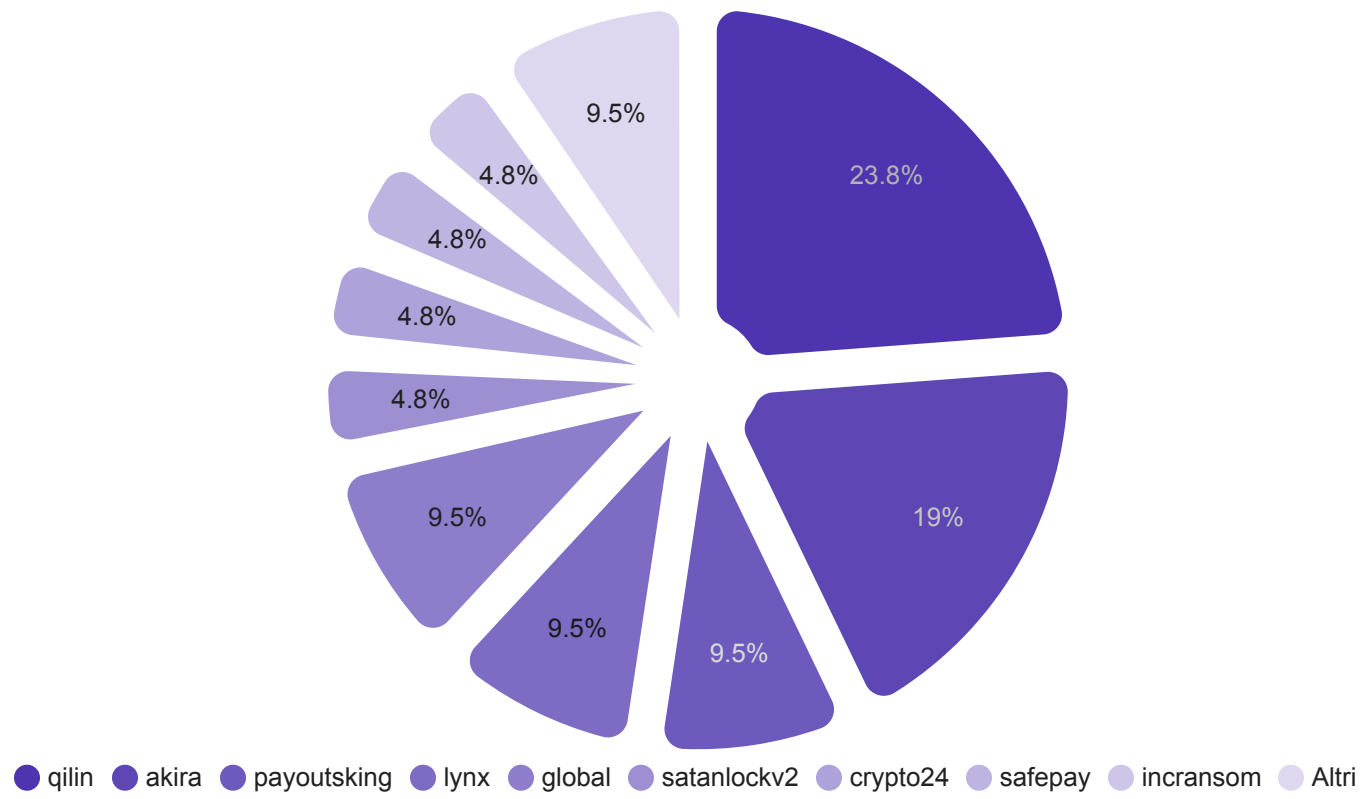
| Vittime Italia | Totale GB pubblicati |
|---|---|
| 21 | 5.316,61 |

| | ID | GRUPPO | VITTIMA | DATI PUBBLICATI GB |
|---|---|---|---|---|
| 1. | 24336 | satanlockv2 | studionotarile.com | 0 |
| 2. | 24364 | qilin | Ridewill SRL | 0 |
| 3. | 24380 | payoutsking | Silent Gliss Italia | 414 |
| 4. | 24387 | payoutsking | Rhea Vendors Group SpA | 1740.8 |
| 5. | 24403 | qilin | volpatoindustrie.it | 110 |
| 6. | 24427 | lynx | Confartigianato Imprese | 0 |
| 7. | 24439 | lynx | nactarome.eu | 0 |
| 8. | 24440 | akira | Wispone | 0 |
| 9. | 24499 | qilin | VM Racing | 0 |
| 10. | 24517 | akira | Mazzoleni | 2.61 |
| 11. | 24540 | crypto24 | Larimart S.P.A | 2.2 |
| 12. | 24541 | akira | Acetificio Andrea Milano | 47 |
| 13. | 24553 | safepay | accademia.it | 0 |
| 14. | 24606 | akira | Studio Associato Callatroni Bianchi | 0 |
| 15. | 24682 | incransom | www.labiennale.org | 0 |
| 16. | 24708 | global | lafavoritaservice.it | 0 |
| 17. | 24720 | global | Rete Toscana Classica | 0 |
| 18. | 24754 | worldleaks | ACEA SpA | 2969 |
| 19. | 24793 | J | restiani.com | 31 |
| 20. | 24796 | qilin | STE Energy S.r.l. | 0 |
| 21. | 24797 | qilin | Consorzio di Bonifica Adige Po | 0 |

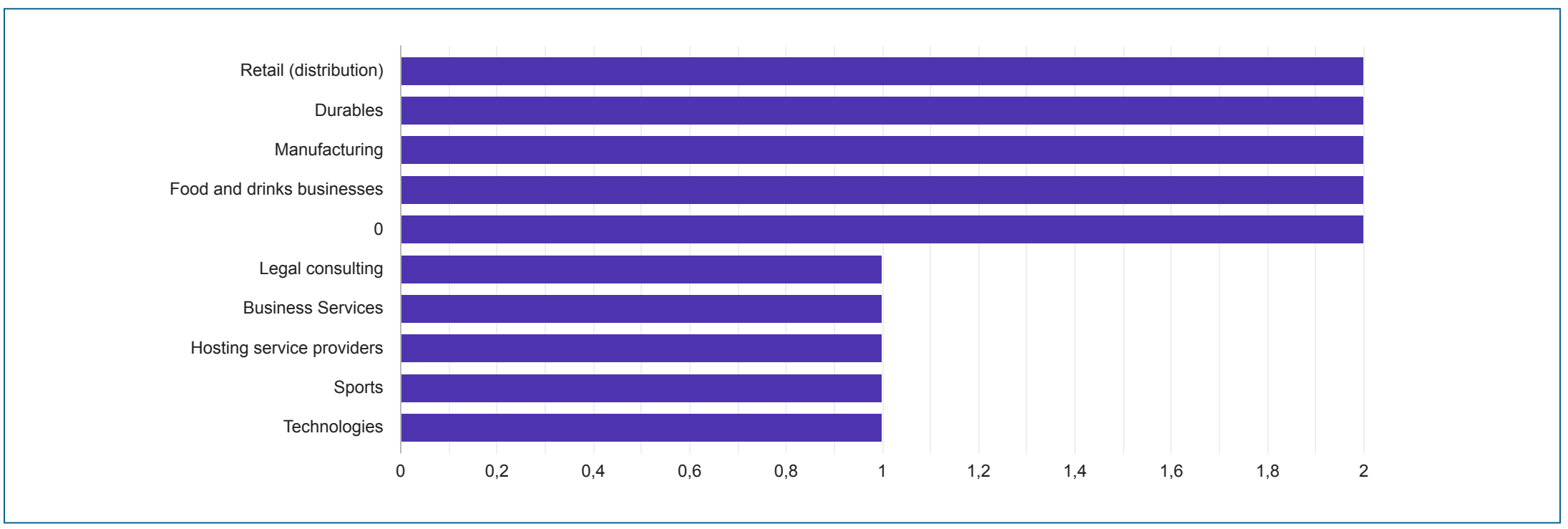
## Gruppi criminali
**focus Italia**

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

| | GRUPPO | VITTIME |
|---|---|---|
| 1. | qilin | 5 |
| 2. | akira | 4 |
| 3. | payoutsking | 2 |
| 4. | lynx | 2 |
| 5. | global | 2 |
| 6. | satanlockv2 | 1 |
| 7. | crypto24 | 1 |
| 8. | safepay | 1 |
| 9. | incransom | 1 |
| 1… | worldleaks | 1 |
| 1… | J | 1 |




## Settori economici
**focus Italia**

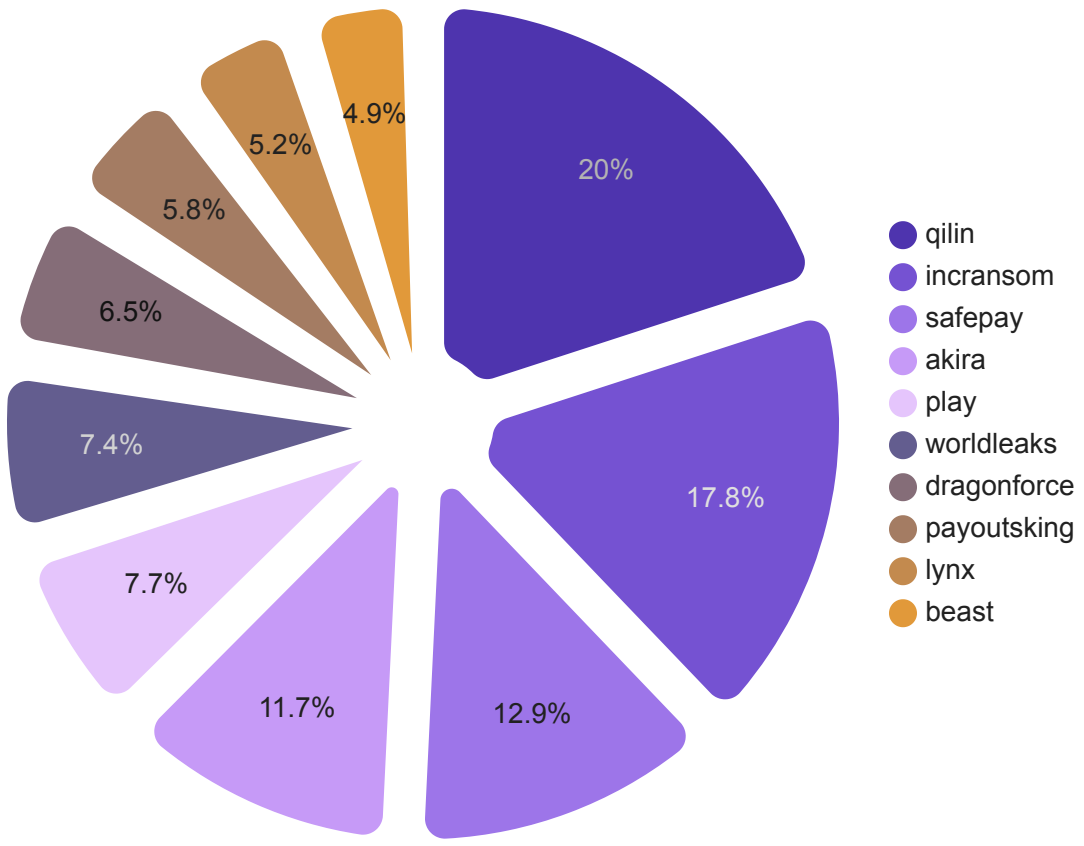


## Scena internazionale 🌐

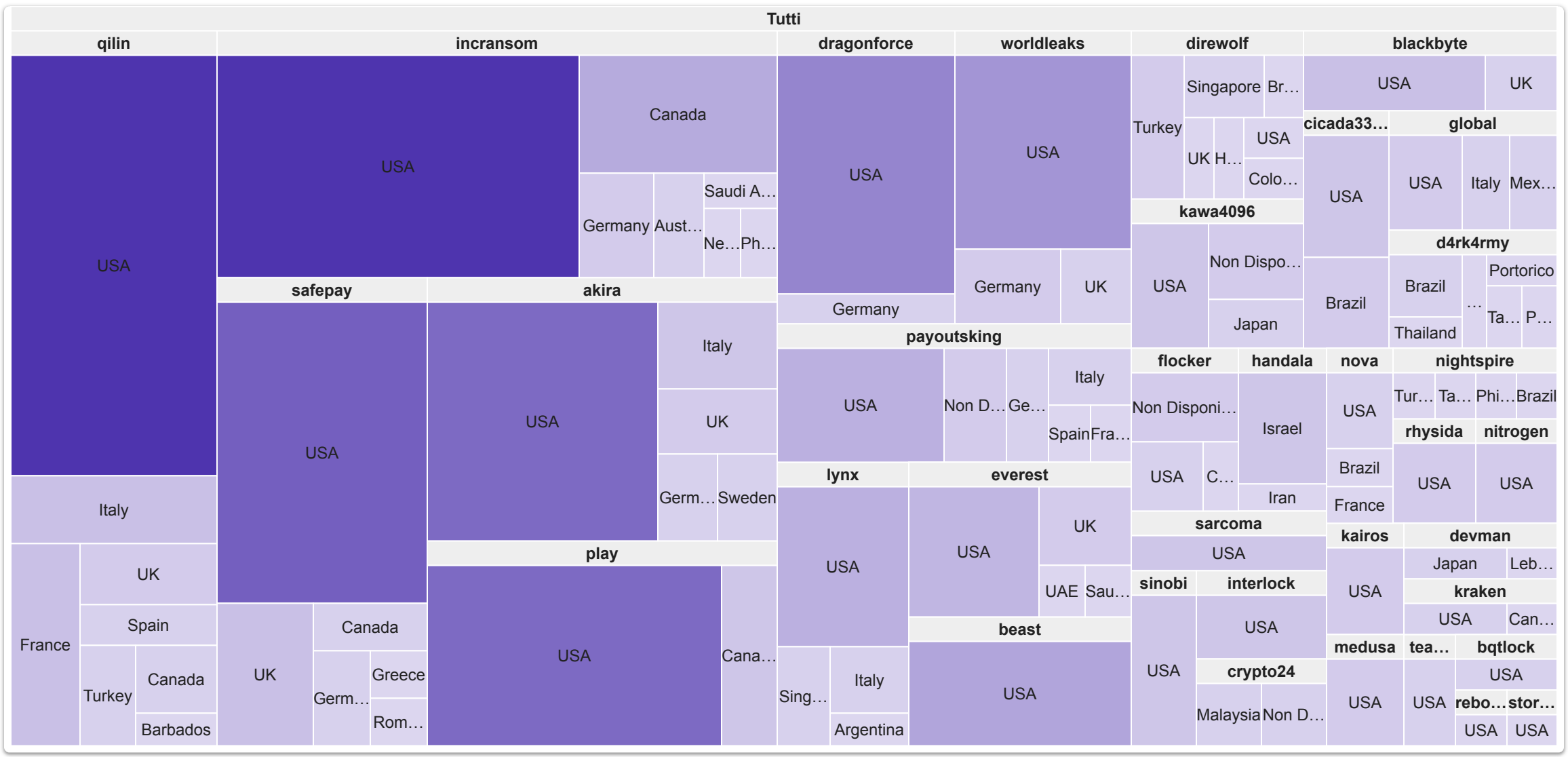
| Vittime | Gruppi attivi | Paesi colpiti |
|---|---|---|
| 506 | 47 | 61 |

Si fa notare che il mese di luglio 2025 vede un incremento del **25%** rispetto allo stesso periodo dell'anno precedente (luglio 2024: 405 rivendicazioni).

### TOP 10 gruppi criminali

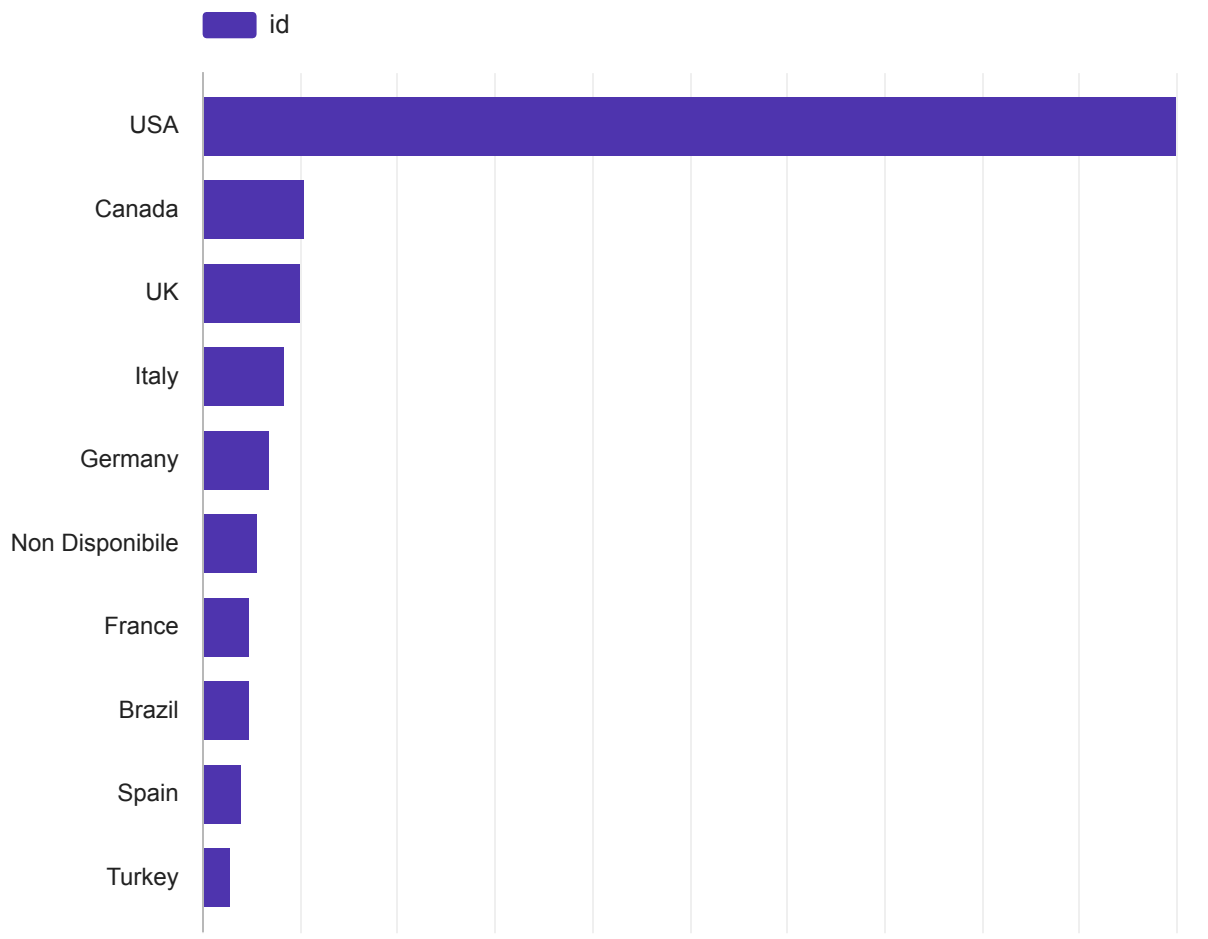



| | GRUPPO | VITTIME |
|---|---|---|
| 1. | qilin | 65 |
| 2. | incransom | 58 |
| 3. | safepay | 42 |
| 4. | akira | 38 |
| 5. | play | 25 |
| 6. | worldleaks | 24 |
| 7. | dragonforce | 21 |
| 8. | payoutsking | 19 |
| 9. | lynx | 17 |
| 10. | beast | 16 |
| 11. | global | 14 |
| 12. | everest | 13 |
| 13. | direwolf | 12 |
| 14. | kawa4096 | 10 |
| 15. | devman | 9 |
| 16. | blackbyte | 9 |
| 17. | crypto24 | 9 |
| 18. | cicada3301 | 8 |
| 19. | arcusmedia | 8 |
| 20. | nightspire | 7 |
| 21. | Altri | 82 |

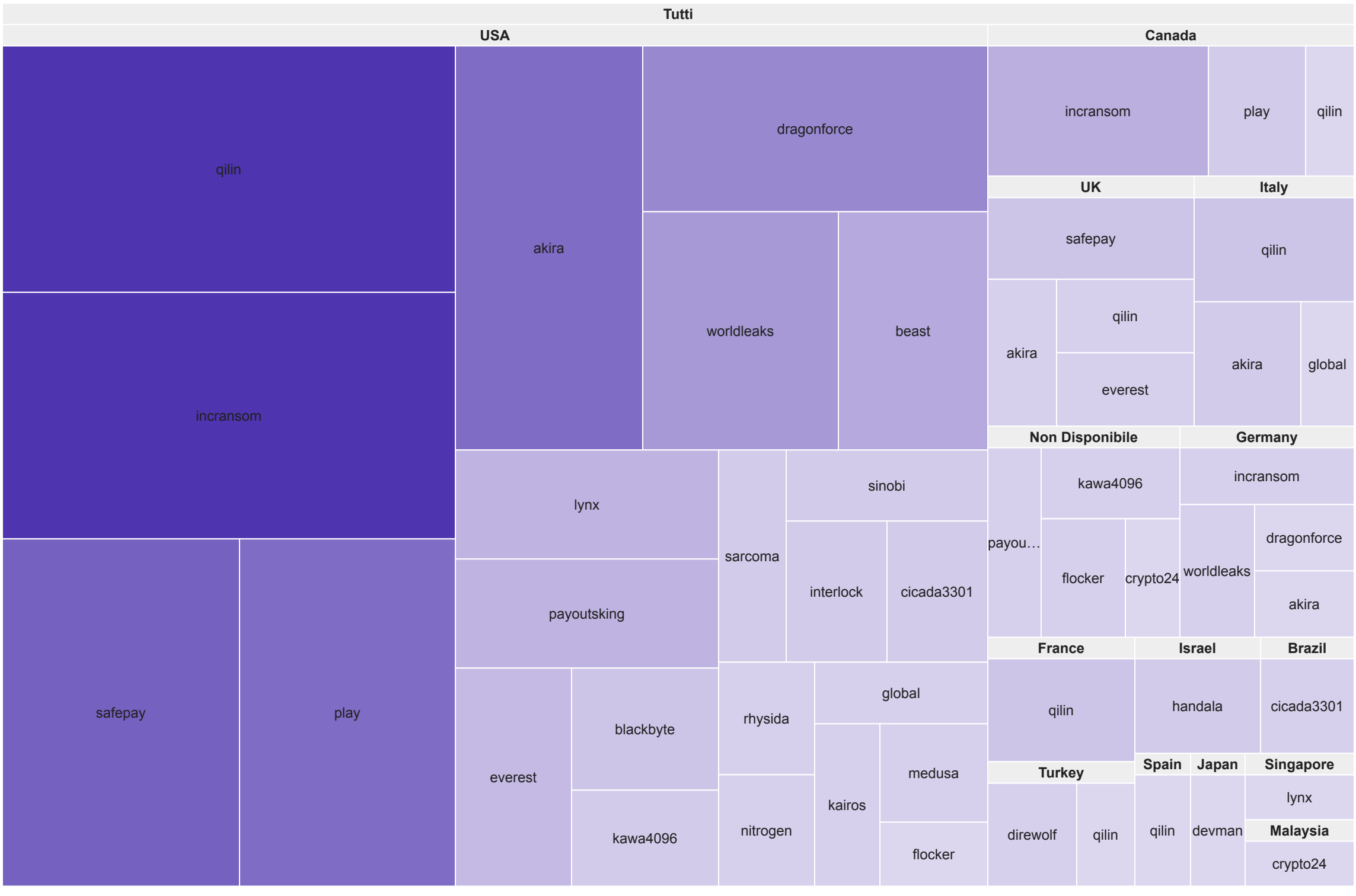


## Scena internazionale 🌐

TOP 10 Paesi colpiti

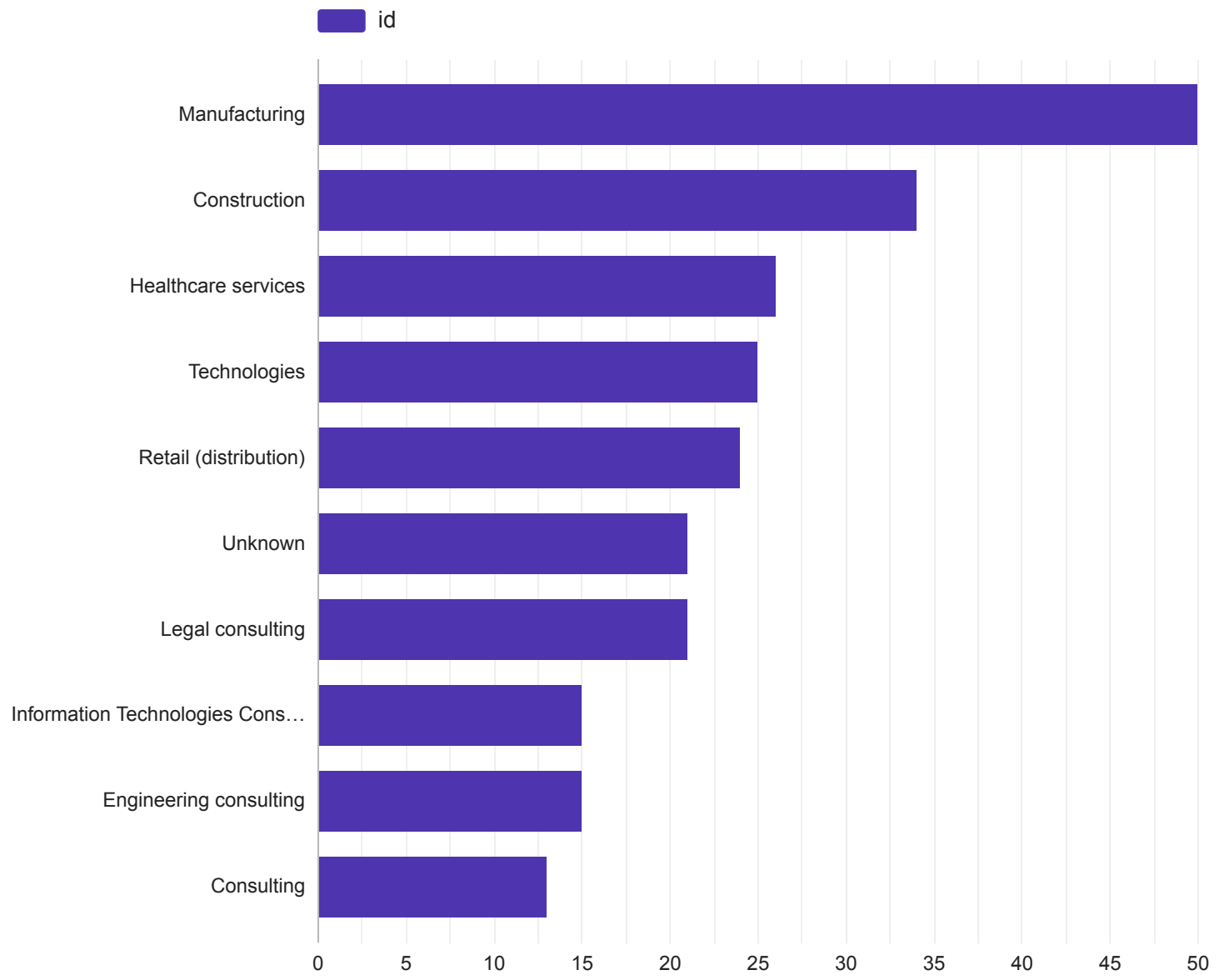



| | PAESE | VITTIME |
|---|---|---|
| 1. | USA | 249 |
| 2. | Canada | 26 |
| 3. | UK | 25 |
| 4. | Italy | 21 |
| 5. | Germany | 17 |
| 6. | Non Disponibile | 14 |
| 7. | France | 12 |
| 8. | Brazil | 12 |
| 9. | Spain | 9 |
| 10. | Turkey | 7 |
| 11. | Thailand | 7 |
| 12. | Japan | 6 |
| 13. | Singapore | 5 |
| 14. | Switzerland | 4 |
| 15. | Sweden | 4 |
| 16. | Mexico | 4 |
| 17. | Belgium | 4 |
| 18. | Israel | 4 |
| 19. | Australia | 4 |
| 20. | UAE | 4 |
| 21. | Altri | 66 |

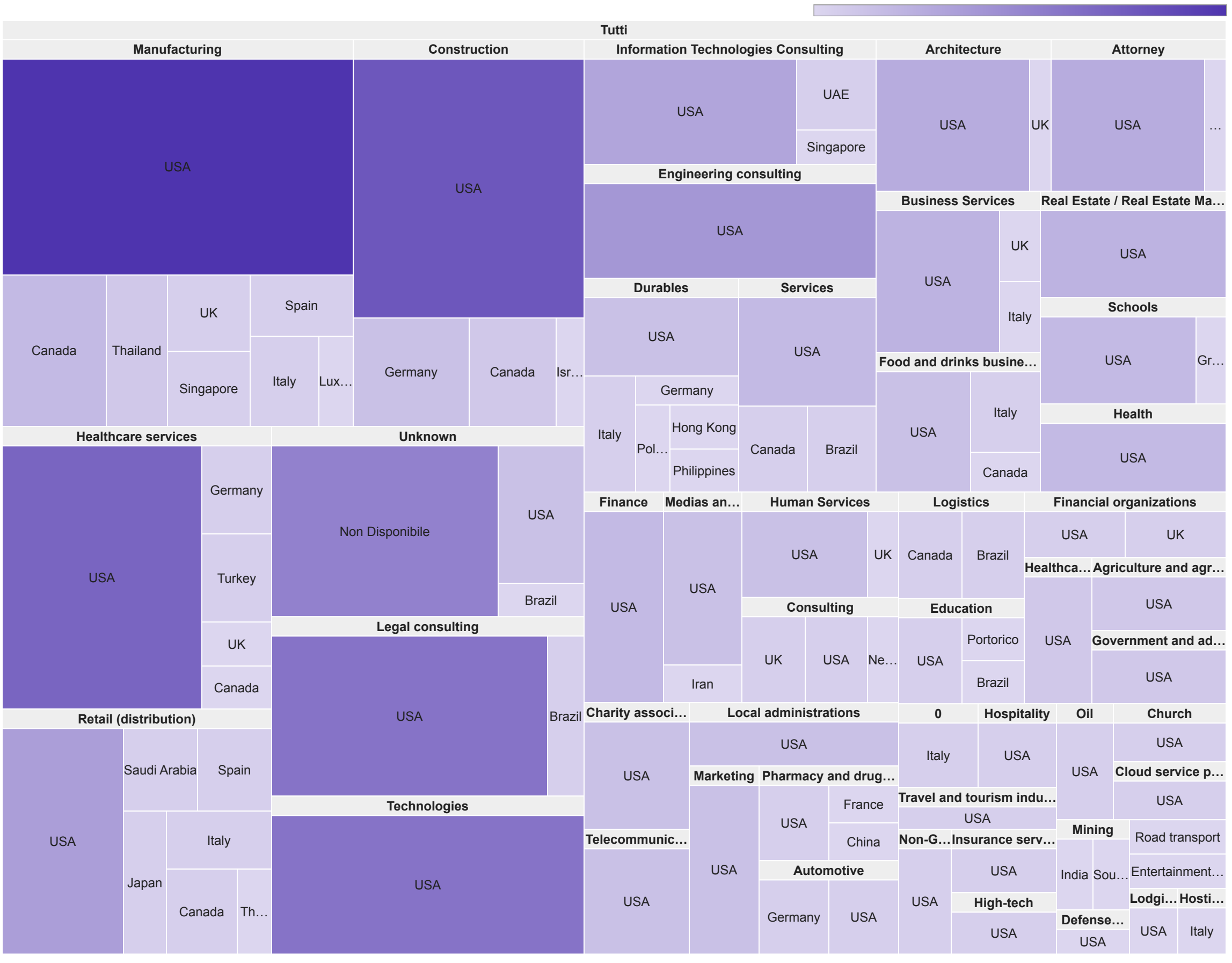


# Scena internazionale 🌐

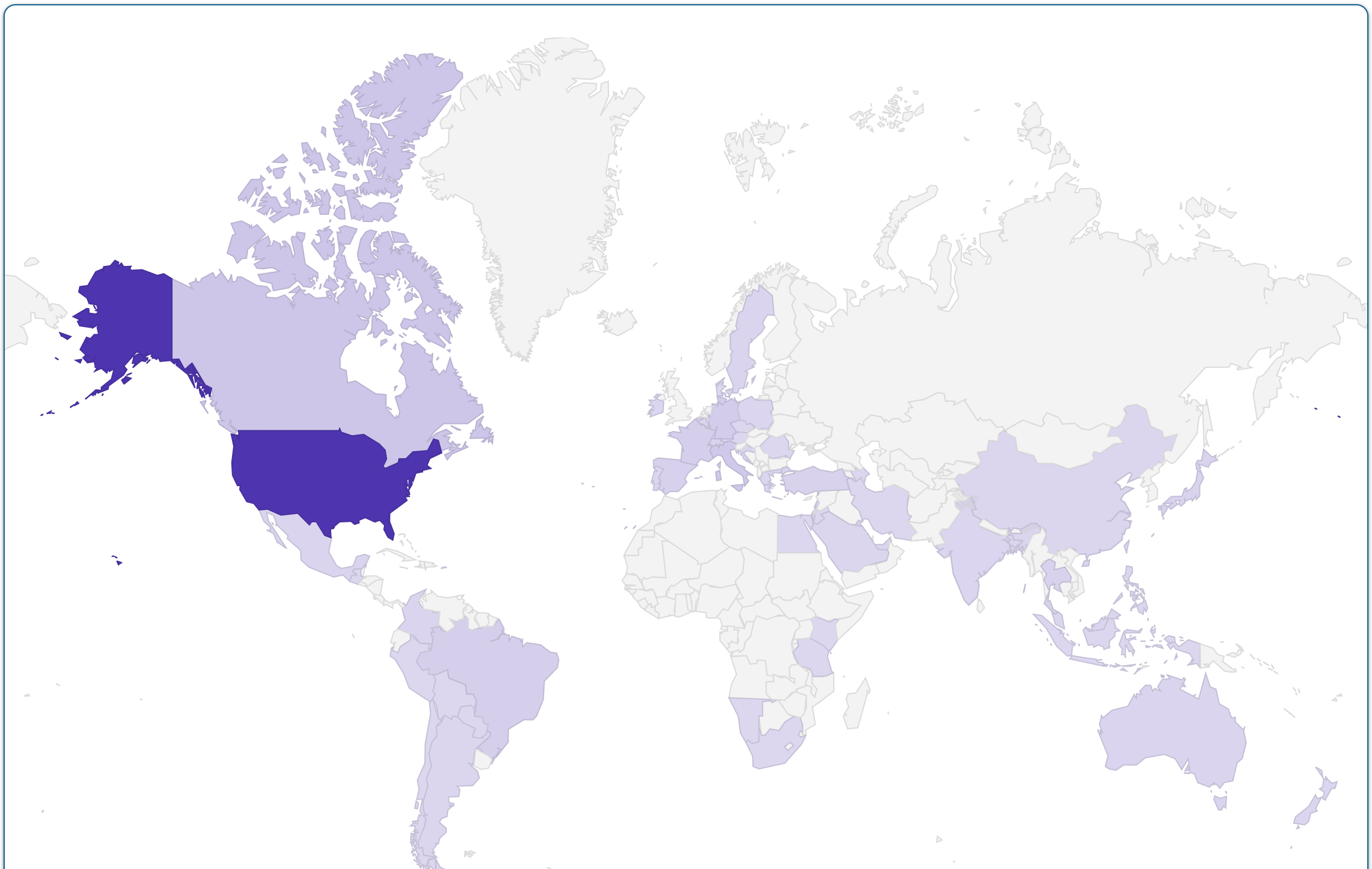
## TOP 10 Settori economici

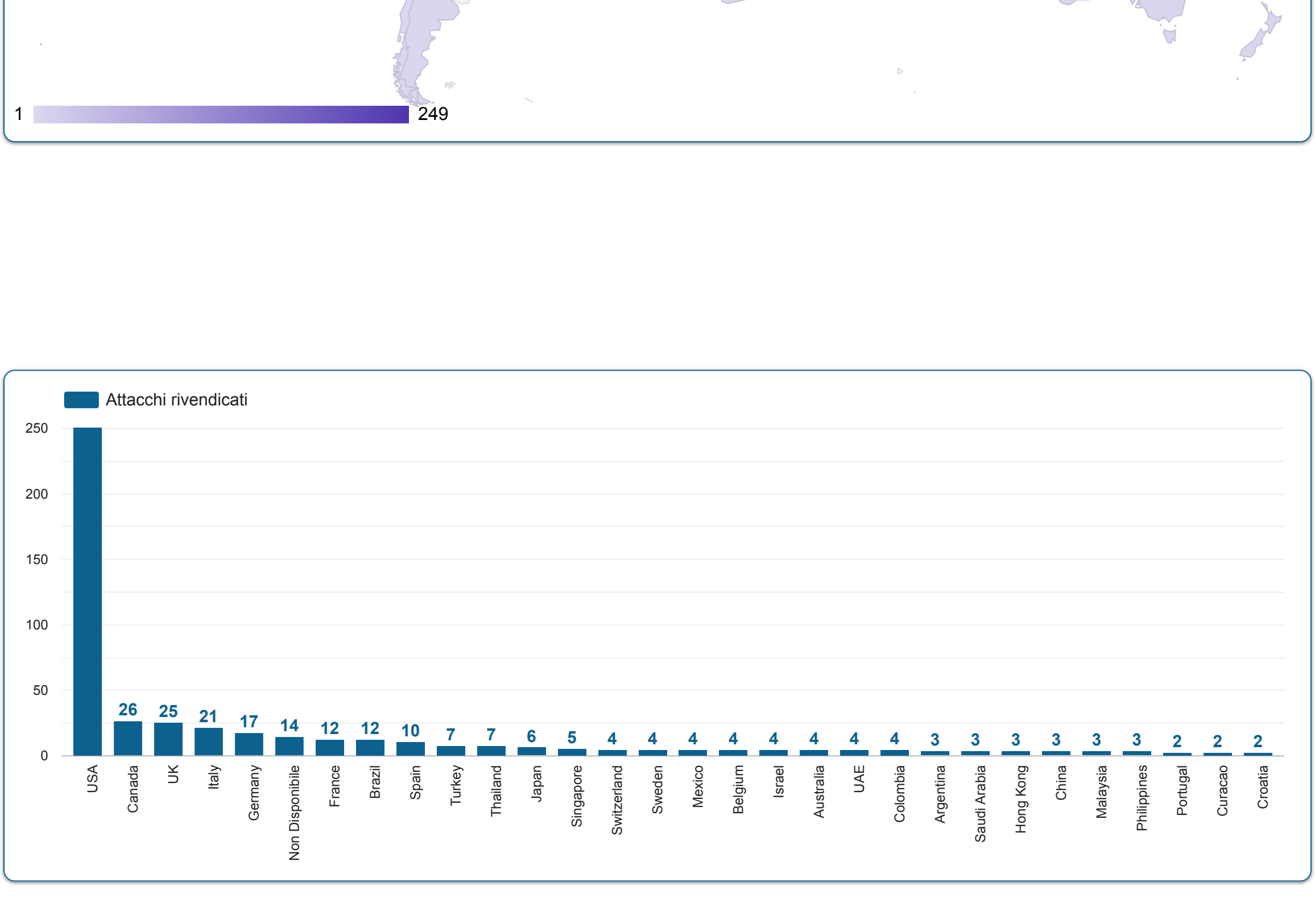



| | SETTORE | VITTIME |
|---|---|---|
| 1. | Manufacturing | 50 |
| 2. | Construction | 33 |
| 3. | Healthcare services | 26 |
| 4. | Technologies | 25 |
| 5. | Retail (distribution) | 24 |
| 6. | Unknown | 21 |
| 7. | Legal consulting | 21 |
| 8. | Information Technologies Co… | 15 |
| 9. | Engineering consulting | 15 |
| 10. | Consulting | 13 |
| 11. | Durables | 12 |
| 12. | Services | 12 |
| 13. | Business Services | 12 |
| 14. | Finance | 12 |
| 15. | Food and drinks businesses | 11 |
| 16. | Telecommunications | 10 |
| 17. | Attorney | 10 |
| 18. | Architecture | 10 |
| 19. | Automotive | 9 |
| 20. | Real Estate / Real Estate Ma… | 9 |
| 21. | Altri | 155 |



## La scena globale mese Luglio 2025



ransomfeed

ADVANCED **DATADRIVEN** CYBERNEWS

# RECAP MENSILE
## LUGLIO 2025

<eof>