RedACT

RANSOMNEWS DISCLOSURE & ACTIVITY TRACKING

REPORT MENSILE
FEBBRAIO 2025

/about

Il report mensile **RedACT** di **ransomNews** offre un'ampia panoramica sulla scena ransomware internazionale, basandosi su dati raccolti, **verificati e analizzati** con un approccio rigoroso. Il nostro obiettivo è presentare le informazioni in forma compatta e accessibile, per fornire una **visione chiara** dell'evoluzione delle minacce cyber.

Crediamo che una pubblicazione mensile sia essenziale per comprendere come le vulnerabilità **possano influenzare qualsiasi azienda**, indipendentemente dal settore o dalla dimensione, aiutando così a **migliorare la consapevolezza** e la resilienza nel security loop.

/data_compile

I dati presenti nel report mensile di **RedACT** sono stati raccolti attraverso **aggregatori e fonti OSINT**.
Ogni rivendicazione viene **verificata ed elaborata manualmente**, senza alcun utilizzo di automazioni per il sorting o la categorizzazione. Ogni analisi è frutto di un attento lavoro di intelligence basato su OSINT e SOCMINT, con un focus particolare sulle rivendicazioni che coinvolgono l'Italia.

Le fonti vengono selezionate e controllate con la massima accuratezza per garantire un'**informazione affidabile e contestualizzata**.

Tutti i dati sono presentati "*as is*", ovvero come raccolti dalle fonti, senza modifiche o interpretazioni oltre quelle strettamente necessarie per la loro analisi e la gestione, come la corretta localizzazione e la rimozione di rivendicazioni duplicate.

/follow_us

bsky.app/profile/**ransomnews.online**
linkedin.com/company/**ransomnews**
github.com/**ransomnews**
x.com/**ransomnews**

/use_conditions

/breakdown_italy

La distribuzione geografica evidenzia una **concentrazione nelle regioni del Nord Italia**, con **6 attacchi**; segue il **Centro con 2 attacchi**, poi **Sud e Isole con 3 attacchi** (*fonti aggregate, elaborazione ransomNews*).

attacchi registrati

11

area geografica

nord

dati pubblicati

1561.80 GB

settore principale

industria

Tabella riepilogativa delle **rivendicazioni confermate** su territorio italiano nel mese di riferimento.
I dati includono il nome della vittima, il gruppo autore, la localizzazione geografica, la quantità dei **dati pubblicati** (come dichiarato dall'attaccante) e le note a riguardo.

Le informazioni sono **verificate** e **aggiornate** sulla base delle fonti aggregate OSINT ed elaborate dal team di ransomNews.

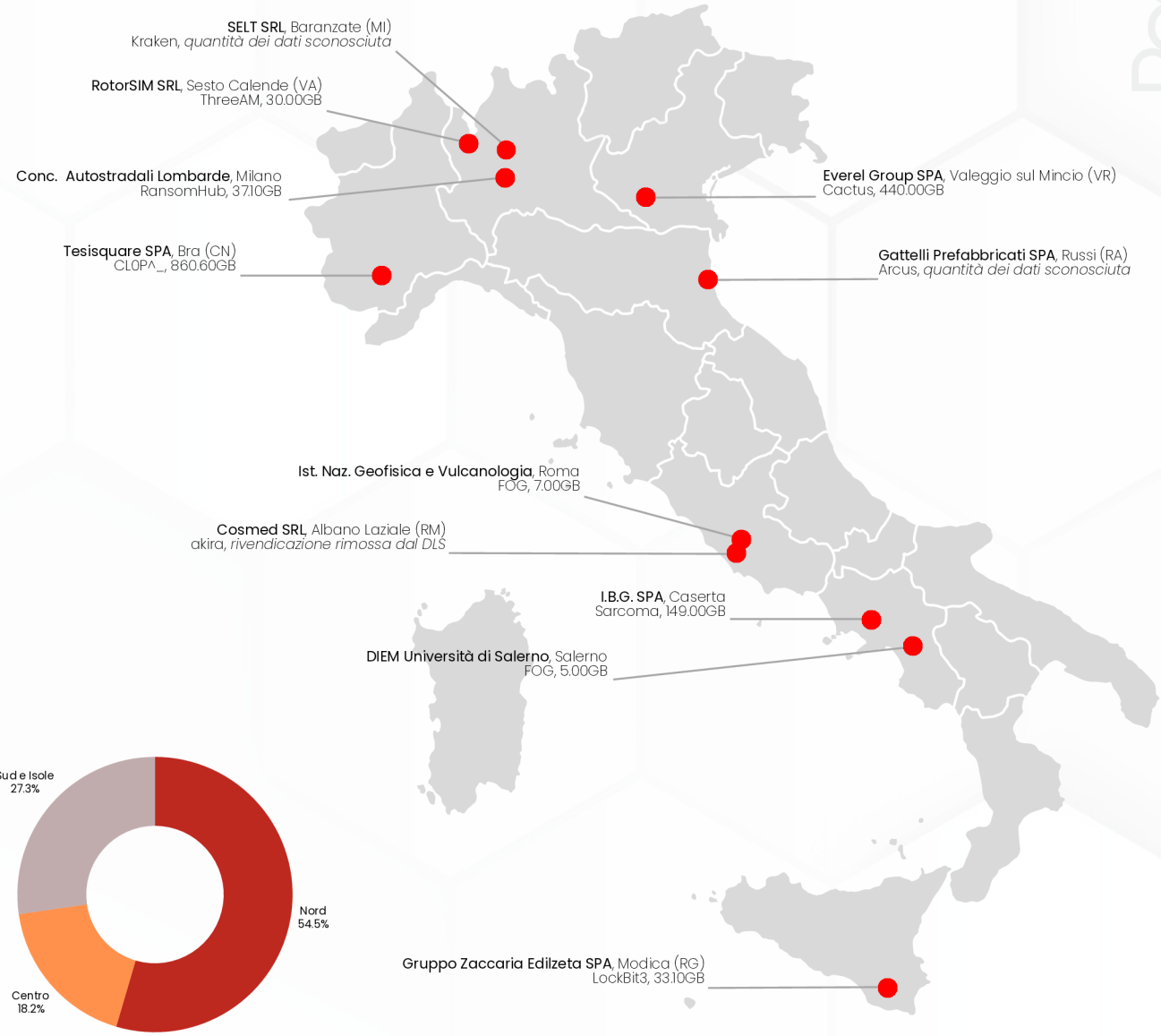
VITTIMA	GRUPPO	LOCALIZZAZIONE	DATI	NOTE
Gattelli Prefabbricati SPA	Arcus	Russi (RA)	-	1
Gruppo Zaccaria Edilzeta SPA	LockBit3	Modica (RG)	33.00 GB	-
DIEM Università di Salerno	FOG	Salerno	5.00 GB	-
I.B.G. SPA	Sarcoma	Caserta	149.00 GB	-
Ist. Geofisica e Vulcanologia	FOG	Roma	7.00 GB	-
RotorSIM SRL	ThreeAM	Sesto Calende (VA)	30.00 GB	⚠️
Conc. Austostradali Lombarde	RansomHub	Milano	37.10 GB	-
Cosmed SRL	akira	Albano Laziale (RM)	-	3
SELT SRL	kraken	Baranzate (MI)	-	1
Tesisquare SPA	CL0P^_	Bra (CN)	860.60 GB	-
Everel Group SPA	Cactus	Valeggio sul Mincio (VR)	440.00 GB	-

[1] quantità dei dati sconosciuta | [2] dati in vendita | [3] rivendicazione rimossa dal DLS | [4] deadline pubblicazione posticipata

⚠️ l'attacco è stato rivendicato nominalmente a Leonardo SPA, tuttavia i dati risultano appartenere a RotorSIM SRL

/breakdown_italy_map

Visualizzazione geografica degli attacchi ransomware **confermati** sul territorio italiano. La mappa mostra la distribuzione regionale degli incidenti registrati nel mese, con indicazione del volume di dati pubblicati (dichiarati) per ciascuna rivendicazione.



Focus regionale

Con 3 attacchi confermati, la **Regione Lombardia** si attesta come l'area più colpita del mese.

La provincia di **Milano** risulta la più esposta.

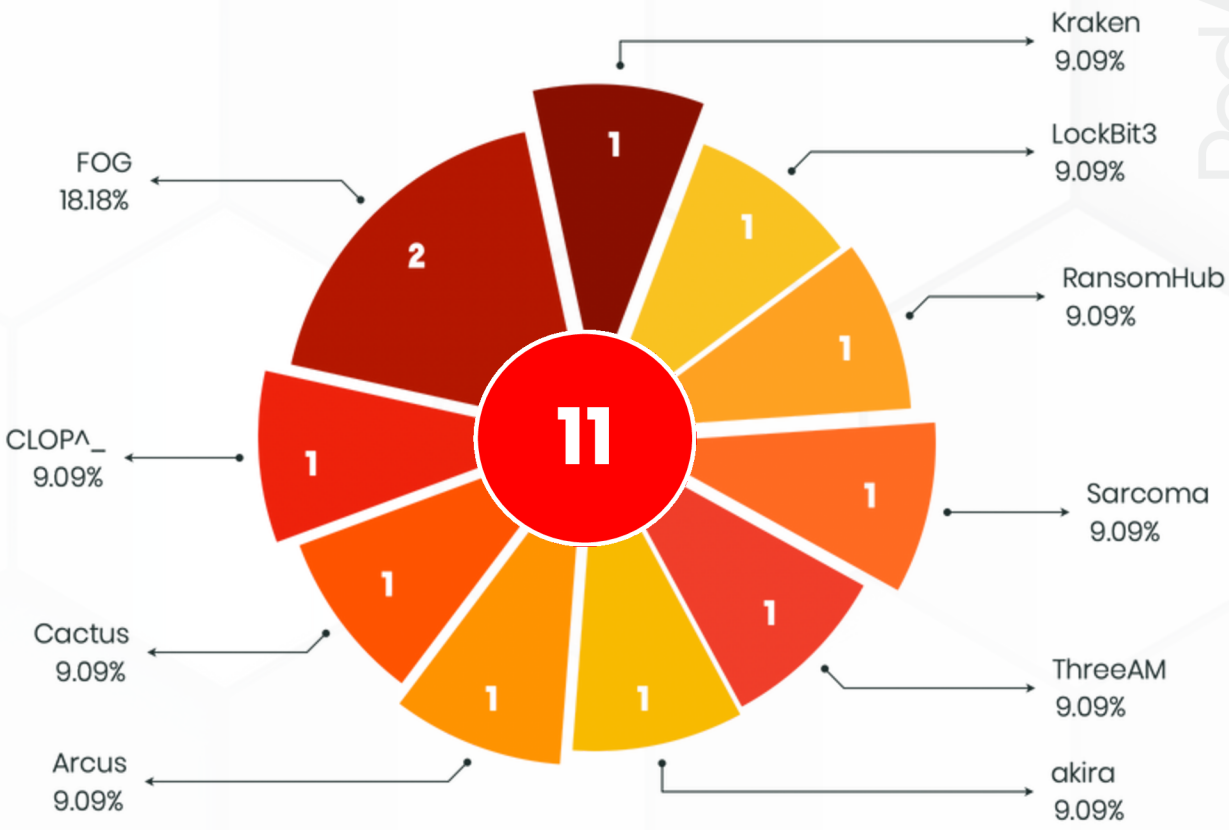
Dati esfiltrati

Il volume dei dati pubblicati per la regione è di **67.10GB**.

Viene **escluso dal calcolo** l'attacco a SELT SISTEMI SRL (in cui la quantità dei dati è sconosciuta).

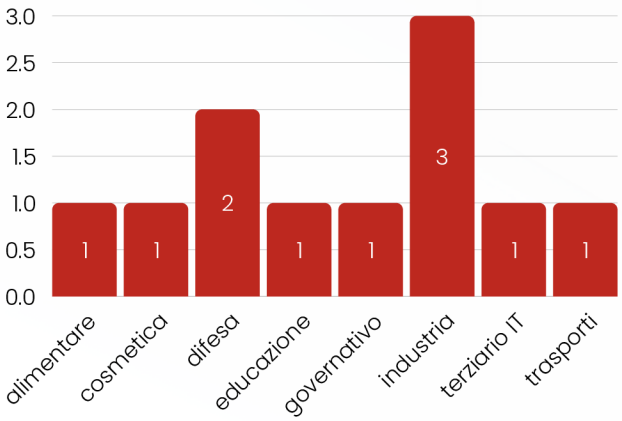
/breakdown_italy_groups

Sono **10 i gruppi** che hanno rivendicato almeno un attacco contro target italiani. Ancora una volta, si conferma una distribuzione frammentata delle attività ransomware (*fonti aggregate,* ***elaborazione ransomNews***).



Tra i **settori più colpiti**, fin dal 2024, troviamo l'industria manifatturiera, la PA, il settore sanitario e il comparto IT.

Per il mese di febbraio, in Italia, gli attacchi hanno interessato i seguenti settori:



La **concentrazione** di attacchi in aree industriali del **Nord Italia** evidenzia un'esposizione elevata delle PMI con **supply chain** interconnesse.

In molti casi, l'accesso iniziale è avvenuto tramite servizi esposti in rete o account compromessi da **campagne di phishing**.

La ripetizione di attacchi in specifiche province suggerisce la presenza di **vettori** persistenti **non ancora mitigati**.

Da notare che alcuni gruppi hanno iniziato a integrare strumenti basati su **intelligenza artificiale** per potenziare le campagne di social engineering e di phishing, rendendole ancora più credibili e personalizzate.

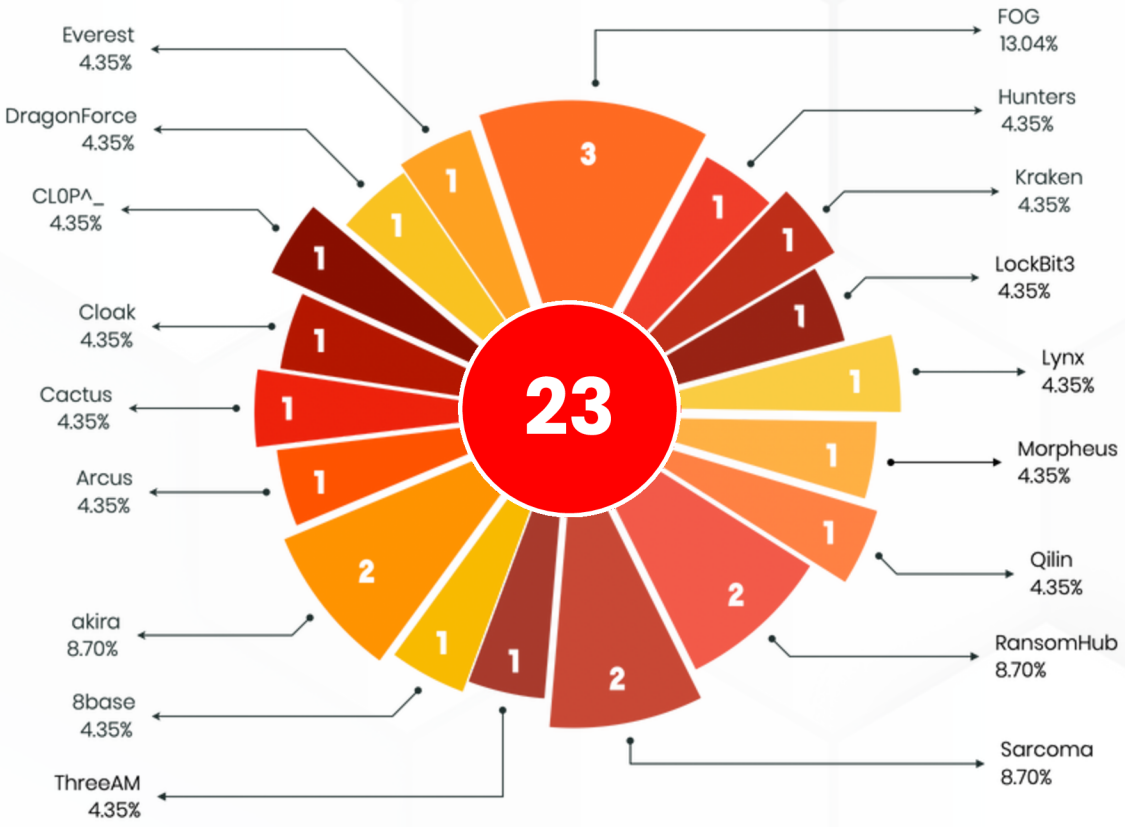
Questo tipo di attacchi rappresenta una minaccia in rapida evoluzione.

/breakdown_italy_groups

Nella tabella, il numero delle **vittime italiane** accertate per ogni gruppo, a partire **dal 1° gennaio 2025**, per un totale di **23 rivendicazioni** (*elaborazione ransomNews*).

In **colore rosso**, i gruppi che, nel corso dell'anno, sono diventati **inattivi** (per scioglimento, arresto di componenti, sequestro delle infrastrutture, ...).

8base, 1	CL0P^_, 1	Kraken, 1	RansomHub, 2
akira, 2	DragonForce, 1	LockBit3, 1	Sarcoma, 2
Arcus, 1	Everest, 1	Lynx, 1	ThreeAM, 1
Cactus, 1	FOG, 3	Morpheus, 1	
Cloak, 1	Hunters, 1	Qilin, 1	



📌 Le **tecniche di attacco** osservate nei casi analizzati rivelano un'evoluzione costante degli strumenti e delle modalità operative adottate dai gruppi criminali. L'accesso iniziale avviene spesso tramite **phishing altamente mirato**, con email costruite ad hoc e **allegati malevoli** che sfruttano vulnerabilità note nei software utilizzati.

Un'altra via di compromissione molto diffusa riguarda i servizi esposti su internet, come **VPN** non aggiornate o **ambienti RDP** (*Remote Desktop Protocol*) mal configurati, che rappresentano un punto di ingresso privilegiato.

In diversi casi, l'accesso iniziale viene **venduto sul dark web** da broker specializzati, che operano in coordinamento con gruppi attivi.
Una volta dentro la rete, gli attaccanti si muovono lateralmente sfruttando strumenti legittimi (*Living off the Land*), **raccolgono credenziali** ed **esfiltrano i dati** prima di procedere alla cifratura e alla pubblicazione nei propri DLS.

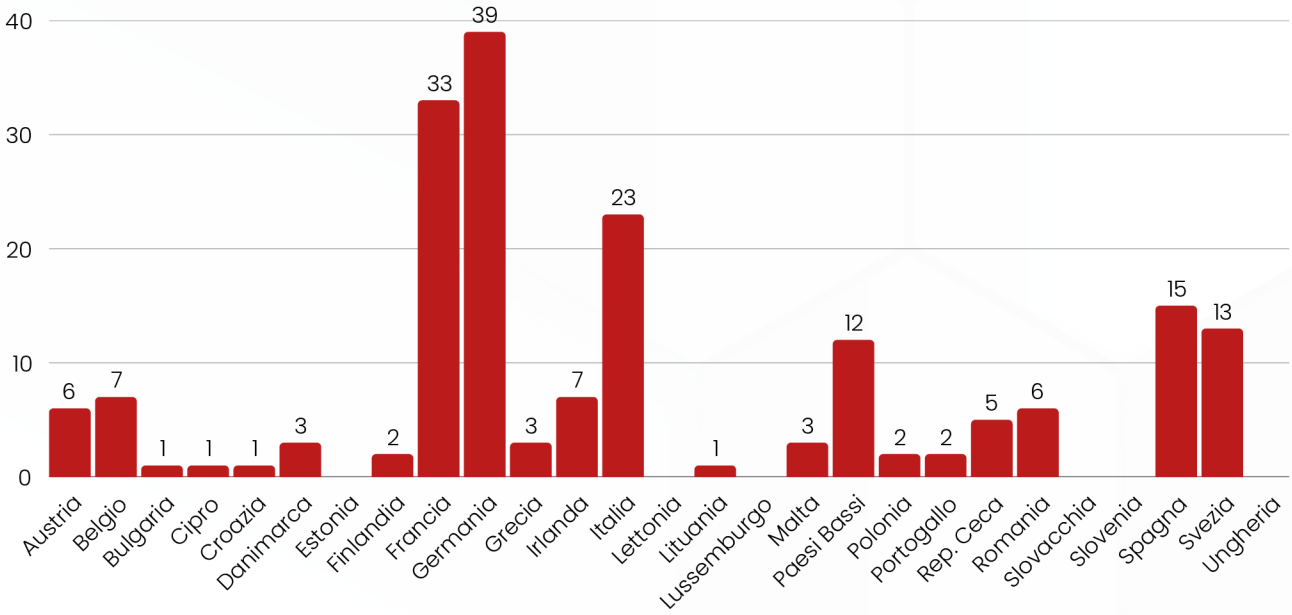
/breakdown_europe_nis2

Nel mese di **febbraio 2025**, i Paesi UE che adottano le normative della **Direttiva NIS2** hanno subito un totale di **101 attacchi**.
I più colpiti sono stati **Germania**, **Francia** e **Italia** (*fonti aggregate, **elaborazione ransomNews***).

- Austria, 2
- Belgio, 3
- Bulgaria, 1
- Cipro, 0
- Croazia, 0
- Danimarca, 1
- Estonia, 0
- Finlandia, 0
- Francia, 15
- Germania, 25
- Grecia, 3
- Irlanda, 6
- Italia, 11
- Lettonia, 0
- Lituania, 0
- Lussemburgo, 0
- Malta, 2
- Paesi Bassi, 8
- Polonia, 1
- Portogallo, 0
- Rep. Ceca, 2
- Romania, 5
- Slovacchia, 0
- Slovenia, 0
- Spagna, 7
- Svezia, 9
- Ungheria, 0

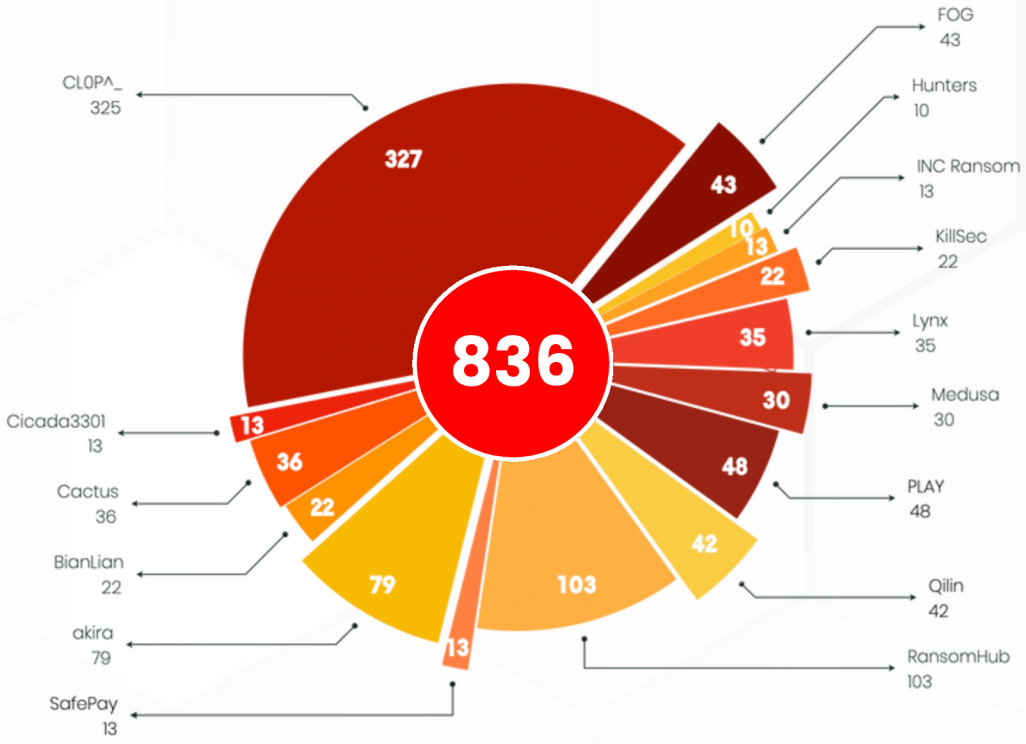
Distribuzione degli incidenti ransomware rilevati **per ciascun paese** membro, sulla base delle rivendicazioni confermate, a partire **dal 1° gennaio 2025,** per un totale di **185 attacchi.**

L'obiettivo è evidenziare il livello di esposizione delle nazioni coinvolte nel nuovo quadro normativo europeo.



/breakdown_world

951 sono le **rivendicazioni tracciate**, da fonti aggregate, per il mese corrente. Nel grafico sono riportati i gruppi che hanno totalizzato **più di 10 attacchi**: **15 gruppi**, per un **totale di 836 attacchi** (*elaborazione ransomNews*).



Nota: l'imponente quantità delle rivendicazioni pubblicate da **CL0P^_** nel mese corrente è, per la quasi totalità, da imputare allo sfruttamento della vulnerabilità **CLEO**.

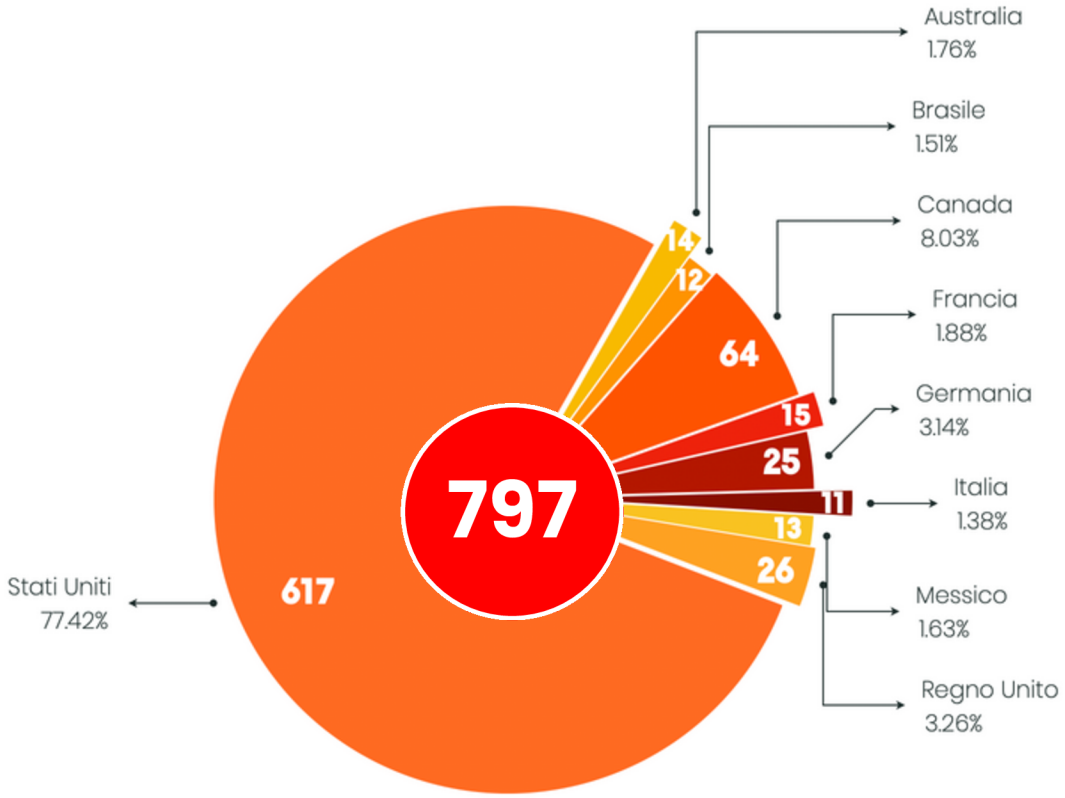
il **dataset** di febbraio 2025, con tutte le rivendicazioni è disponibile **qui**: **https://rnws.online/YyZGM**

33 invece sono i gruppi che hanno rivendicato **meno di 10 attacchi**, per un totale complessivo di **115 rivendicazioni** (*fonti aggregate, **elaborazione ransomNews***).

- 8base, 4
- Abyss, 6
- Anubis, 4
- Apos Security, 1
- APT73 / BASHE, 6
- Arcus, 5
- Brain Cipher, 2
- CiphBit, 1
- Cloak, 2
- DragonForce, 6
- EMBARGO, 3
- Everest, 2
- FSociety FLocker, 7
- Handala, 2
- HellCat, 1
- InterLock, 1
- Kairos, 5
- Kraken, 6
- Linkc, 1
- LockBit3, 7
- MedusaLocker, 2
- MONTI, 1
- Morpheus, 2
- RansomEXX, 2
- RansomHouse, 2
- Rhysida, 7
- Run Some Wares, 4
- Sarcoma, 7
- Space Bears, 3
- Stormous, 2
- Termite, 7
- ThreeAM, 3
- Underground, 1

/breakdown_world

Riportiamo nel grafico i paesi che, in questo mese, hanno subito **più di 10 attacchi**, su un totale di **66 paesi colpiti**. Si tratta di **9 paesi**, per complessive **797 rivendicazioni** (*fonti aggregate, **elaborazione ransomNews***).



Nota: il massiccio numero di attacchi verso i paesi, in particolare verso gli Stati Uniti e il Canada, è determinato in larga parte dalle rivendicazioni pubblicate da **CL0P^_**, a causa dello sfruttamento della vulnerabilità **CLEO**.

Gli attacchi ai rimanenti **57 paesi**, per un totale di **154 rivendicazioni**, sono così suddivisi (*fonti aggregate, **elaborazione ransomNews***):

- **Arabia Saudita**, 2
- **Argentina**, 1
- **Austria**, 2
- **Bangladesh**, 1
- **Belgio**, 3
- **Bielorussia**, 1
- **Bulgaria**, 1
- **Cile**, 3
- **Cina**, 3
- **Colombia**, 3
- **Corea del Sud**, 1
- **Danimarca**, 1
- **Ecuador**, 3
- **Egitto**, 3
- **Emirati Arabi**, 1
- **Filippine**, 2
- **Ghana**, 1
- **Giamaica**, 2
- **Giappone**, 8
- **Grecia**, 3
- **Haiti**, 1
- **Hong Kong**, 1
- **India**, 6
- **Indonesia**, 5
- **Iraq**, 1
- **Irlanda**, 6
- **Israele**, 3
- **Malesia**, 3
- **Malta**, 2
- **Marocco**, 1
- **Namibia**, 1
- **Nigeria**, 1
- **Non Disponibile**, 5
- **Norvegia**, 3
- **Nuova Zelanda**, 4
- **Paesi Bassi**, 8
- **Pakistan**, 3
- **Panama**, 1
- **Perù**, 2
- **Polonia**, 1
- **Portogallo**, 2
- **Portorico**, 2
- **Rep. Ceca**, 2
- **Rep. Palau**, 1
- **Romania**, 5
- **Singapore**, 4
- **Spagna**, 7
- **Sud Africa**, 1
- **Svezia**, 9
- **Svizzera**, 4
- **Tailandia**, 2
- **Taiwan**, 7
- **Tanzania**, 1
- **Tunisia**, 1
- **Turchia**, 1
- **Vietnam**, 1
- **Zambia**, 1

/breakdown_groups

Nella tabella, il numero delle vittime accertate per ogni gruppo ransomware a partire **dal 1° gennaio 2025**, per un totale di **1470 rivendicazioni** (*elaborazione ransomNews*).

In colore rosso, i gruppi che, nel corso dell'anno, sono diventati **inattivi** (per scioglimento, arresto di componenti, sequestro delle infrastrutture, ...).

8base, 29
Abyss, 8
akira, 151
Anubis, 4
Apos Security, 2
APT73 / BASHE, 12
Arcus, 5
BianLian, 23
Black Basta, 8
Brain Cipher, 2
Cactus, 45
Cicada3301, 14
CiphBit, 2
Cloak, 10
CL0P^_, 387
DarkVault, 2
DragonForce, 19
ElDorado, 6
EMBARGO, 4
Everest, 9
FSociety FLocker, 10
FOG, 58
GD LockerSec, 5
Handala, 4
HellCat, 1
Hunters, 19
INC Ransom, 41
InterLock, 1
Kairos, 11
KillSec, 31
Kraken, 6
Linkc, 1
LockBit3, 17
Lynx, 76
Medusa, 52
MedusaLocker, 3
MetaEncryptor, 1
MoneyMessage, 1
MONTI, 9
Morpheus, 5
PLAY, 59
Qilin, 65
RansomEXX, 2
RansomHouse, 2
RansomHub, 146
Rhysida, 16
Run Some Wares, 4
SafePay, 34
Sarcoma, 15
Space Bears, 14
Stormous, 2
Termite, 9
ThreeAM, 6
Underground, 1

Mentre il gruppo **akira** sembra aver rinnovato la propria gestione, probabilmente trovando nuova linfa in affiliati vicini a gruppi un tempo rivali, dopo la pubblicazione dei chat logs, il gruppo **Black Basta** sembra essere entrato in un sonno profondo.

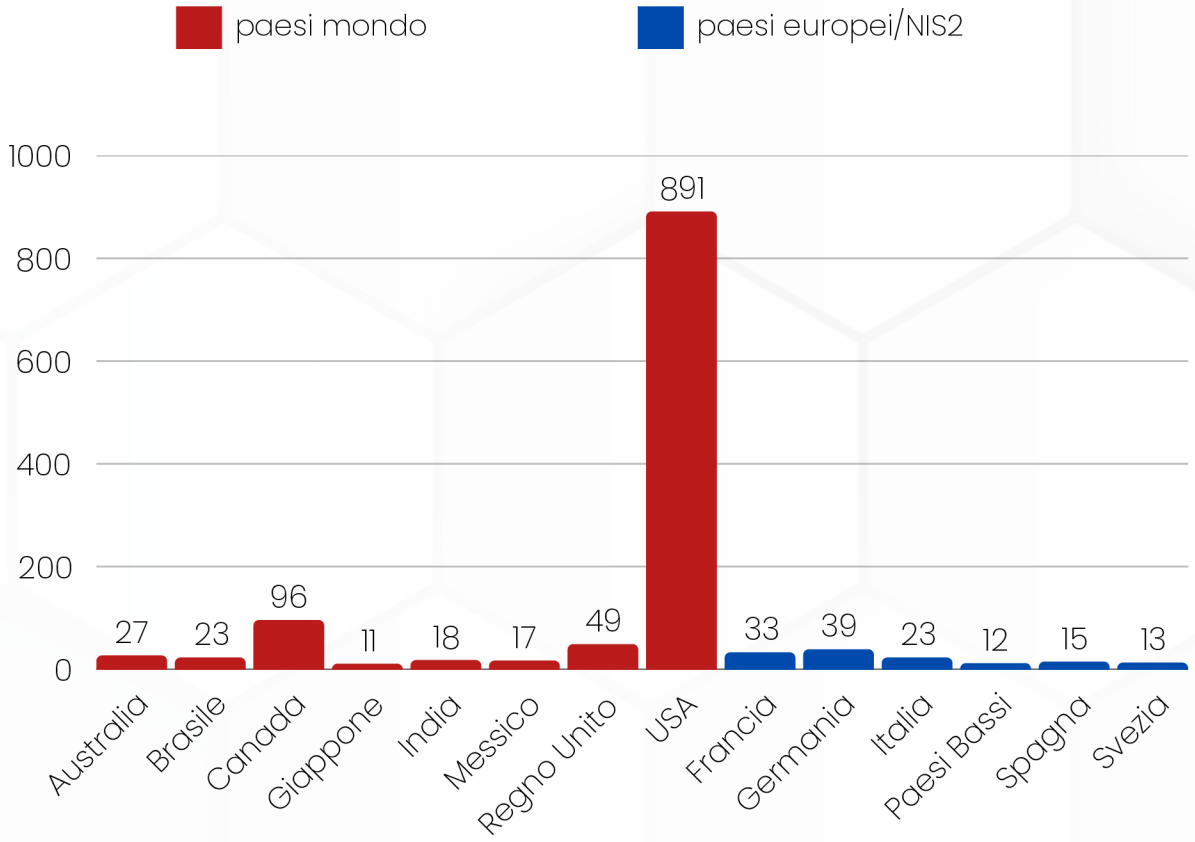
Da sempre forte di un modello di business solido e disciplinato, l'**esposizione della struttura interna** (e non solo), ha causato uno sbandamento ai vertici e una prolungata inattività.

Riportiamo anche la distribuzione degli attacchi per ogni paese colpito, **dal 1° gennaio 2025**, ad *esclusione dei paesi europei/NIS2*, per un **totale di 1285 attacchi** (*fonti aggregate, **elaborazione ransomNews***):

Algeria, 1
Arabia Saudita, 2
Argentina, 6
Australia, 27
Bangladesh, 1
Bielorussia, 1
Brasile, 23
Canada, 96
Cile, 5
Cina, 8
Colombia, 6
Corea del Sud, 1
Ecuador, 3
Egitto, 5
El Salvador, 1
Emirati Arabi, 3
Filippine, 2
Georgia, 1
Ghana, 1
Giamaica, 3
Giappone, 11
Haiti, 1
Hong Kong, 2
India, 18
Indonesia, 7
Iraq, 1
Israele, 5
Kenia, 1
Malesia, 5
Marocco, 2
Messico, 17
Namibia, 1
Nigeria, 3
Non Disponibile, 7
Norvegia, 3
Nuova Zelanda, 5
Oman, 1
Pakistan, 4
Panama, 1
Perù, 3
Portorico, 3
Regno Unito, 49
Rep. Dominicana, 2
Rep. Palau, 1
Singapore, 9
Sud Africa, 2
Svizzera, 8
Tailandia, 7
Taiwan, 9
Tanzania, 1
Tunisia, 1
Turchia, 3
Uruguay, 1
USA, 891
Venezuela, 1
Vietnam, 3
Zambia, 1

/breakdown_groups_top

Nel grafico sono riportati i paesi che hanno subito **più attacchi** nel periodo di tempo considerato.



/breakdown_groups_new

Nuovi* gruppi in attività a **febbraio 2025**:

- **Anubis** - gruppo attivo probabilmente dalla metà/fine novembre 2024; al suo interno membri con pregressa esperienza nel mondo del ransomware e con una rete di affiliati piuttosto corposa. Il loro modello di RaaS, attualmente, garantisce l'accesso ad *Anubis Ransomware*, *Anubis Data Ransom* e *Access Monetization*. Predilige tattiche di double extortion.
- **Kraken** - il gruppo sfrutta tecniche e strumenti di *credential-dumping* come *Mimikatz*, *pwdump* e *hashdump*. Fino a metà agosto del 2024, ha lavorato nell'affinare tecniche di deployment, grazie al bundle nel Fallout Exploit Kit.
- **Linkc** - attivo fin da gennaio 2025, ha ufficializzato le attività nel mese di febbraio, dopo il riscatto di 15 milioni di dollari, chiesto alla prima vittima (il fornitore di servizi cloud H2O.ai).
- **Run Some Wares** - con un attivo di 4 target internazionali nel mese corrente, il gruppo opera prevalentemente con tattiche di simple e double extortion.

*vengono considerati i gruppi criminali di **nuova costituzione**, **rebrand** e gruppi **nuovamente in attività** dopo un lasso di tempo di almeno un anno.

/whois_core

@signorina37
Claudia Galingani Mongini

@sonoclaudio
Claudio Sono

@alekitto
Alessandro Chitolina

@fed
Federico Marsili

/whois_special

@garantepiracy
Christian Bernieri

U2VjdXJpdHkgSXMga2V5LCBCdXQgUmVtZW1iZXIgVG8gSGlkZSBZb3VyIEJhY2t1cA==

RedACT

RANSOMNEWS DISCLOSURE & ACTIVITY TRACKING

/staysafe