RedACT

RANSOMNEWS DISCLOSURE & ACTIVITY TRACKING

REPORT MENSILE
GENNAIO 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 **9 attacchi**; segue il **Centro con 2 attacchi**, mentre **Sud e Isole**, questo mese, non hanno subito alcun attacco (*fonti aggregate, **elaborazione ransomNews***).

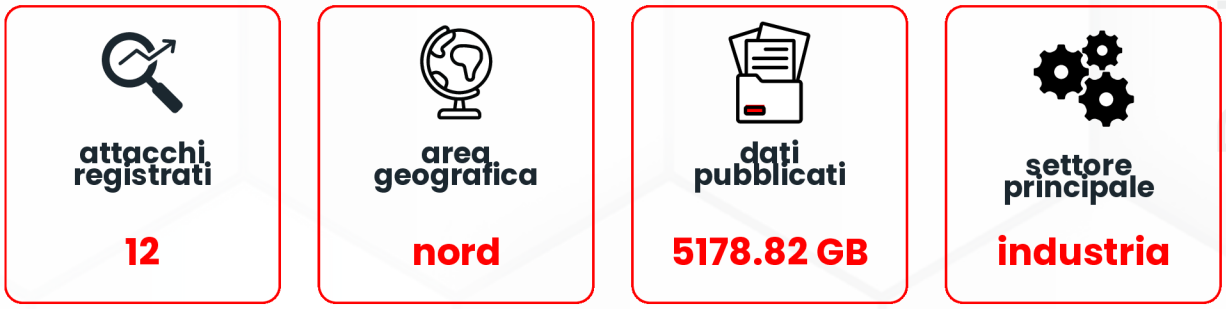


Tabella riepilogativa delle **rivendicazioni confermate** su territorio italiano nel mese di riferimento.
I dati includono il nome della vittima, il gruppo autore, la localizzazione geografica, la quantità dei **dati pubblicati** (come dichiarato dall'attaccante) e le note a riguardo.

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

VITTIMA	GRUPPO	LOCALIZZAZIONE	DATI	NOTE
Ascom SPA	8base	Formigine (MO)	156.40 GB	-
Corob SPA	Hunters	San Felice sul Panaro (MO)	430.00 GB	-
Conad Società Cooperativa	Lynx	Bologna	119.32 GB	-
Boart & Wire SRL	Sarcoma	Fara Vicentino (VI)	17.00 GB	-
BSE Group	RansomHub	Gavardo (BS)	108.00 GB	-
Volt Infrastructure SRL	Everest	Roma	-	5
Lynx SPA	Morpheus	Milano	-	5
Divimast SRL	akira	Brescia	400.00 GB	-
GE******COM**	Cloak	-	-	-
Eltek Group SPA	FOG	Casale Monferrato (AL)	-	5
Studio Dati Aziendali SAS	DragonForce	Poviglio (RE)	135.00 GB	⚠️
Eltek Group SPA	Qilin	Roma	339.00 GB	-

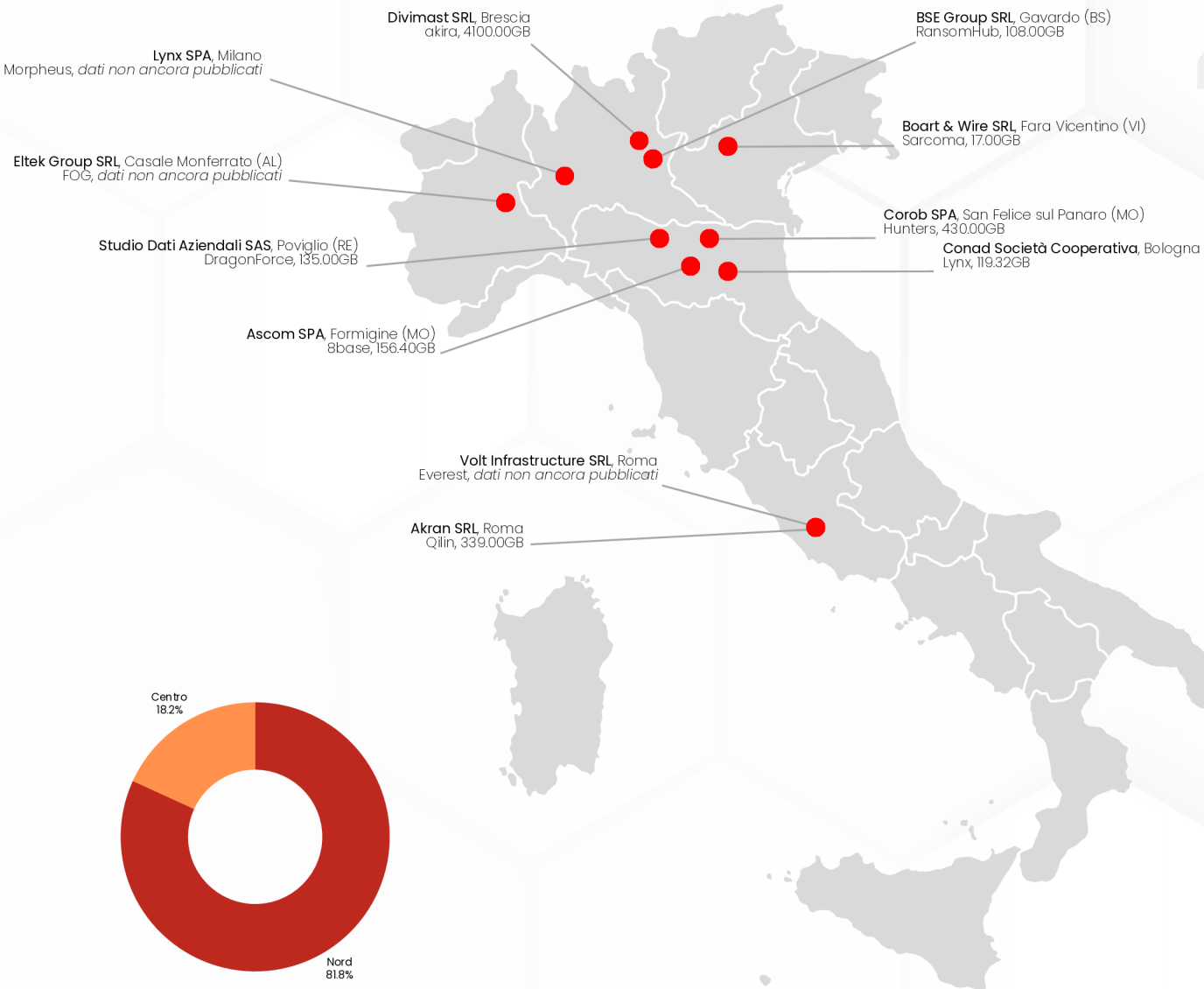
[1] quantità dei dati sconosciuta | [2] dati in vendita | [3] rivendicazione rimossa dal DLS
[4] deadline pubblicazione posticipata | [5] dati non ancora pubblicati

⚠️ l'attacco è stato rivendicato nominalmente a **Benassi Immobiliare SAS** (Ca' del Bosco Sopra, Reggio Emilia), tuttavia i dati risultano appartenere a **Studio Dati Aziendali SAS**

/breakdown_italy_map

Visualizzazione geografica degli attacchi ransomware **confermati** sul territorio italiano.

nota: la rivendicazione **GE******COM** di Cloak non è identificabile, viene quindi **esclusa dalla rappresentazione** sulla mappa.

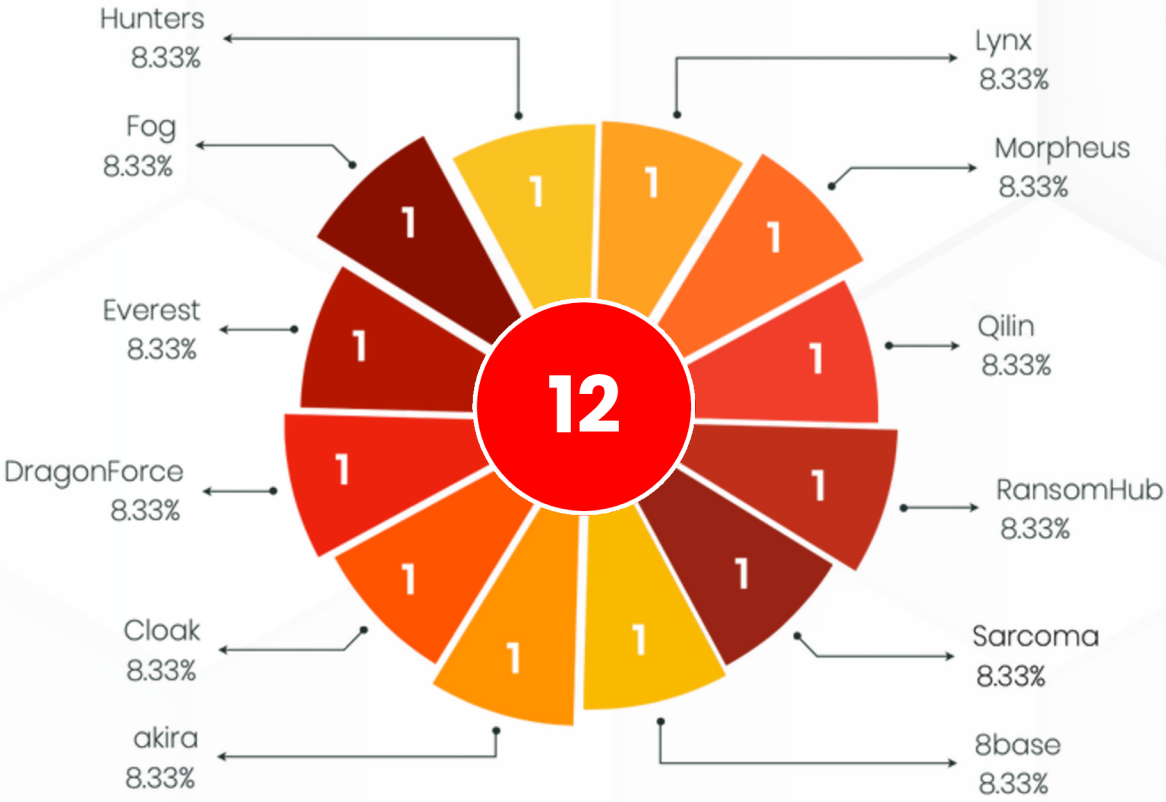


Nel mese di gennaio 2025 si sono registrati **4 attacchi in Emilia Romagna**, aumentando il numero delle vittime nella regione.
La concentrazione di aziende colpite - in particolare nelle province di **Reggio Emilia**, di **Bologna** e **Modena** - risulta essere quantomeno singolare, se consideriamo gli attacchi registrati anche nei mesi di ottobre (3), novembre (3) e dicembre (2) dello scorso anno (*fonti aggregate, **elaborazione ransomNews***).

	Reggio Emilia	Modena	Bologna	Parma	Rimini
settembre 2024	0	0	0	1	0
ottobre 2024	1	0	1	0	1
novembre 2024	1	0	1	0	1
dicembre 2024	1	0	1	0	0
gennaio 2025	1	2	1	0	0

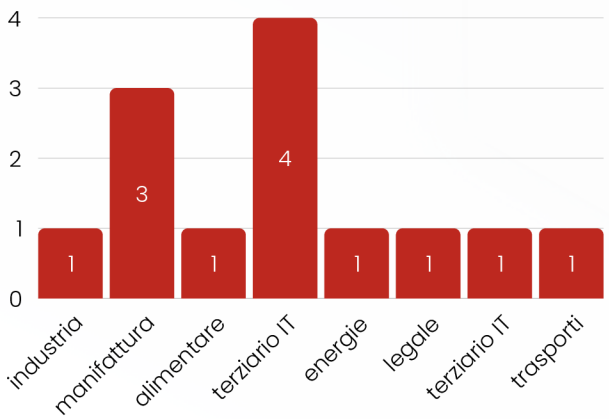
/breakdown_italy_groups

Sono **12 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 gennaio, in Italia, gli attacchi hanno interessato i seguenti settori:



È importante sottolineare, ancora una volta, che le **vie d'accesso preferenziali** derivano **dall'inadeguatezza** delle misure di sicurezza adottate dalle organizzazioni.

Tra i principali fattori di rischio si segnalano **vulnerabilità note non patchate**, **credenziali** archiviate **in chiaro** su sistemi non protetti o accessibili via cloud, e l'**assenza di pratiche basilari** di sicurezza, come l'autenticazione a più fattori.

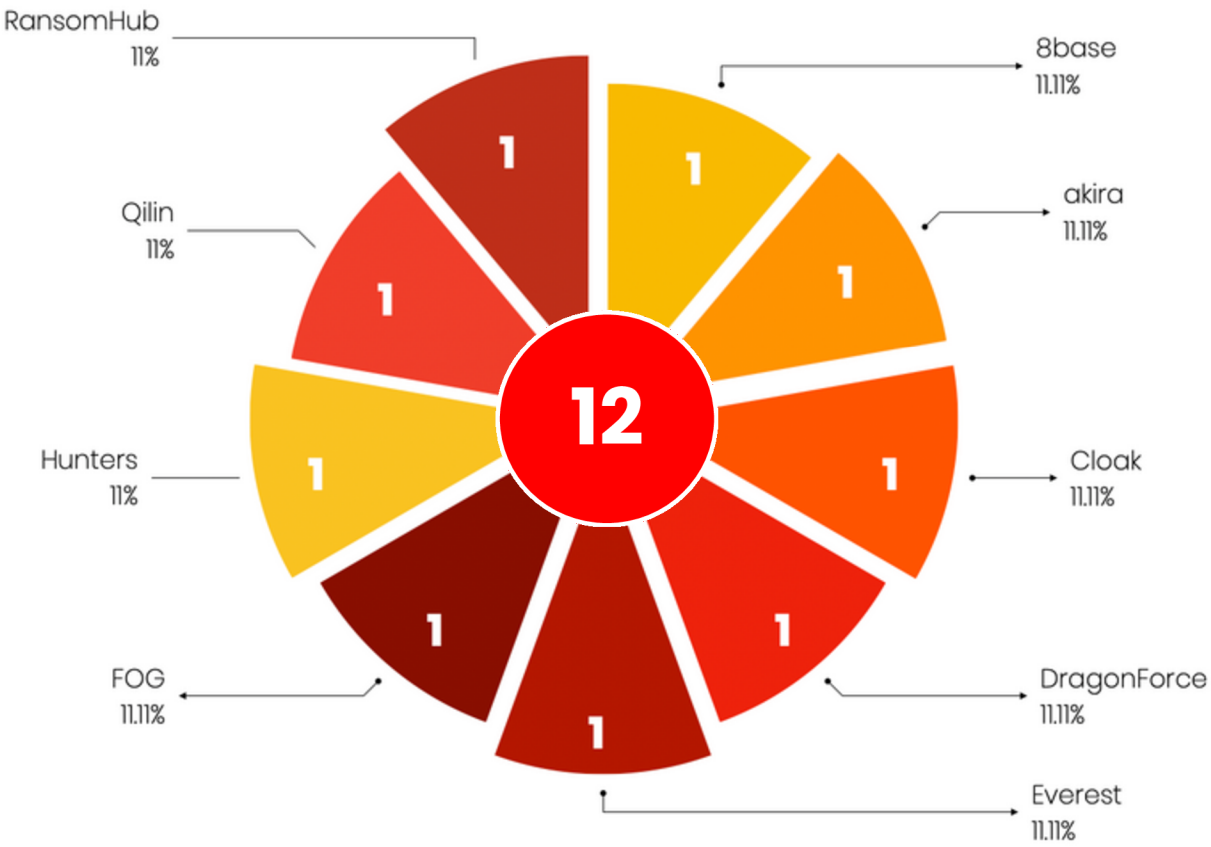
A questi si aggiungono nuove tecniche di attacco, tra cui l'**uso di IA** per **campagne di phishing mirate**, l'abuso dei **protocolli RDP**, troppo spesso mal configurati, e la compromissione **della supply chain** (fonte **ENISA**).

/breakdown_italy_groups

Nella tabella, il numero delle **vittime italiane accertate** per ogni gruppo, a partire **dal 1° gennaio 2025**, per un totale di **12 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	FOG, 1	RansomHub, 1
akira, 1	Hunters, 1	Sarcoma, 1
Cloak, 1	Lynx, 1	
DragonForce, 1	Morpheus, 1	
Everest, 1	Qilin, 1	



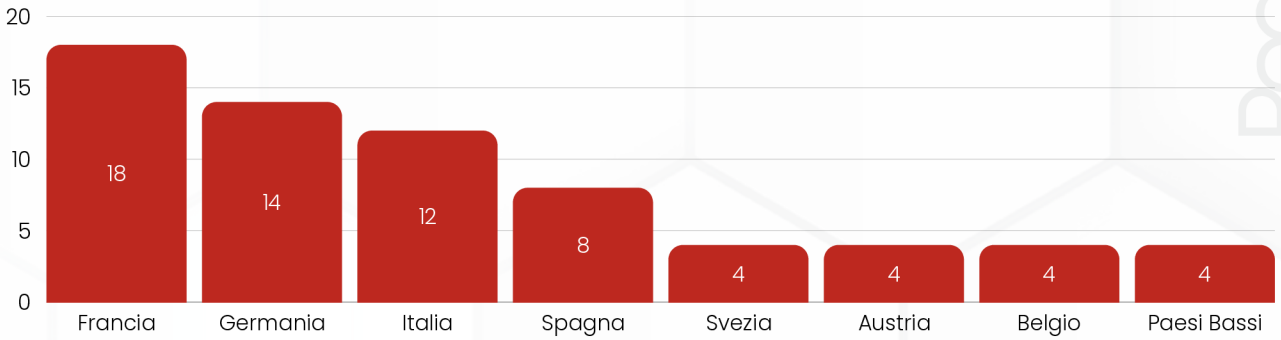
📌 Le **tecniche di attacco** osservate nei casi analizzati evidenziano un'evoluzione costante delle modalità operative adottate dai gruppi criminali. L'accesso iniziale avviene frequentemente attraverso lo **sfruttamento di credenziali esposte**, reperite tramite **data breach**, **repository pubblici** o **forum del dark web**, che consentono agli attaccanti di accedere direttamente ai sistemi aziendali senza dover ricorrere a tecniche di social engineering.

Un'altra modalità di compromissione molto diffusa riguarda l'abuso di **sistemi non patchati,** in particolare server e applicazioni esposti a internet che presentano vulnerabilità note ma non ancora corrette, diventando così facili bersagli per exploit automatizzati o mirati.

In diversi casi, l'accesso iniziale **viene acquistato sul dark web** da broker specializzati, che collaborano con gruppi criminali strutturati. Una volta ottenuto l'accesso, gli attaccanti si muovono lateralmente sfruttando strumenti legittimi (*Living off the Land*), raccolgono ulteriori credenziali ed **esfiltrano dati sensibili** prima di procedere alla cifratura e alla pubblicazione all'interno dei propri DLS.

/breakdown_europe_nis2

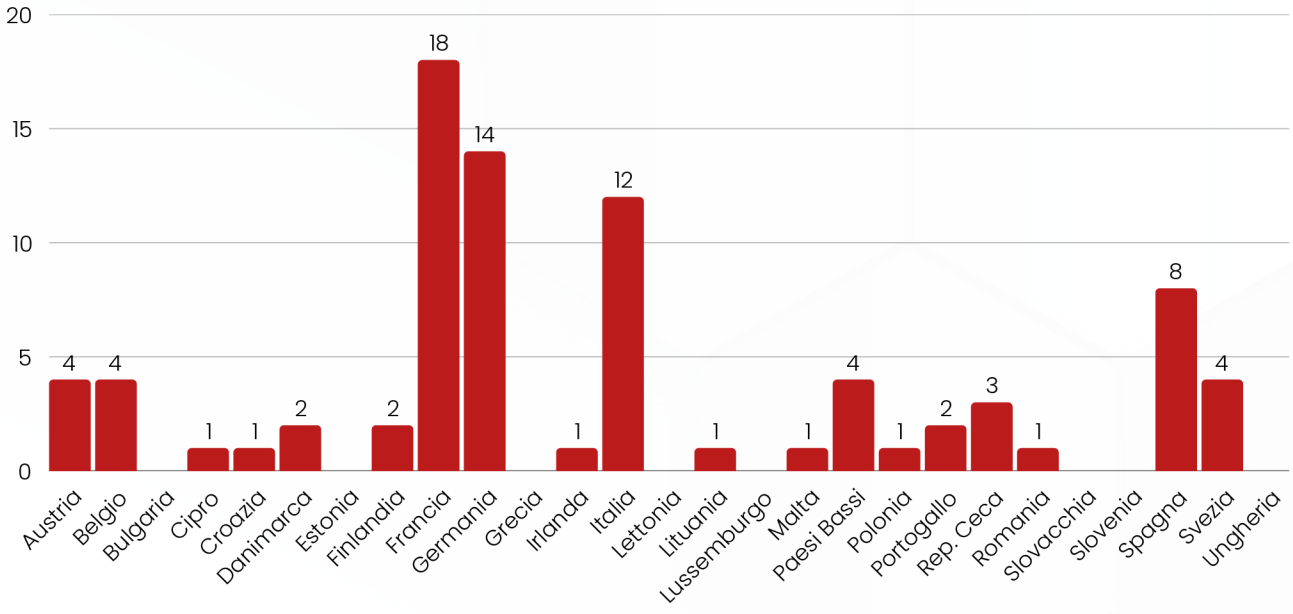
Nel mese di **gennaio 2025**, i Paesi UE che adottano le normative della **Direttiva NIS2** hanno subito un totale di **84 attacchi**.
I più colpiti sono stati **Francia**, **Germania** e **Italia** (*fonti aggregate, **elaborazione ransomNews***).



- **Austria**, 4
- **Belgio**, 4
- **Bulgaria**, 0
- **Cipro**, 1
- **Croazia**, 1
- **Danimarca**, 2
- **Estonia**, 0
- **Finlandia**, 2
- **Francia**, 18
- **Germania**, 14
- **Grecia**, 0
- **Irlanda**, 1
- **Italia**, 12
- **Lettonia**, 0
- **Lituania**, 1
- **Lussemburgo**, 0
- **Malta**, 1
- **Paesi Bassi**, 4
- **Polonia**, 1
- **Portogallo**, 2
- **Rep. Ceca**, 3
- **Romania**, 1
- **Slovacchia**, 0
- **Slovenia**, 0
- **Spagna**, 8
- **Svezia**, 4
- **Ungheria**, 0

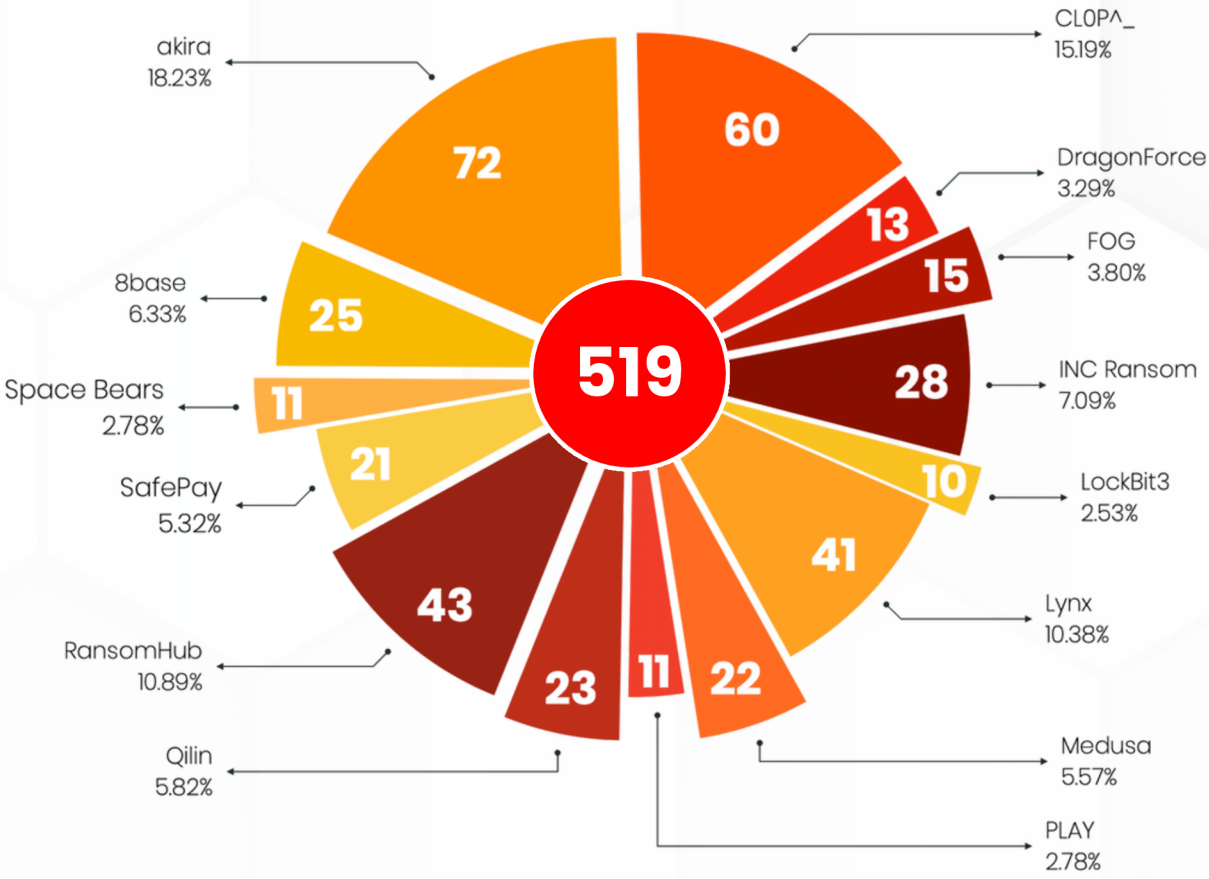
Distribuzione degli incidenti ransomware rilevati **per ciascun paese** membro, sulla base delle rivendicazioni confermate, a partire **dal 1° gennaio 2025,** per un totale di **185 attacchi.**

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



/breakdown_world

519 sono le **rivendicazioni tracciate**, da fonti aggregate, per il mese corrente.
Nel grafico sono riportati i gruppi che hanno totalizzato **più di 10 attacchi**: **14 gruppi**, per un **totale di 395 attacchi** (*elaborazione ransomNews*).



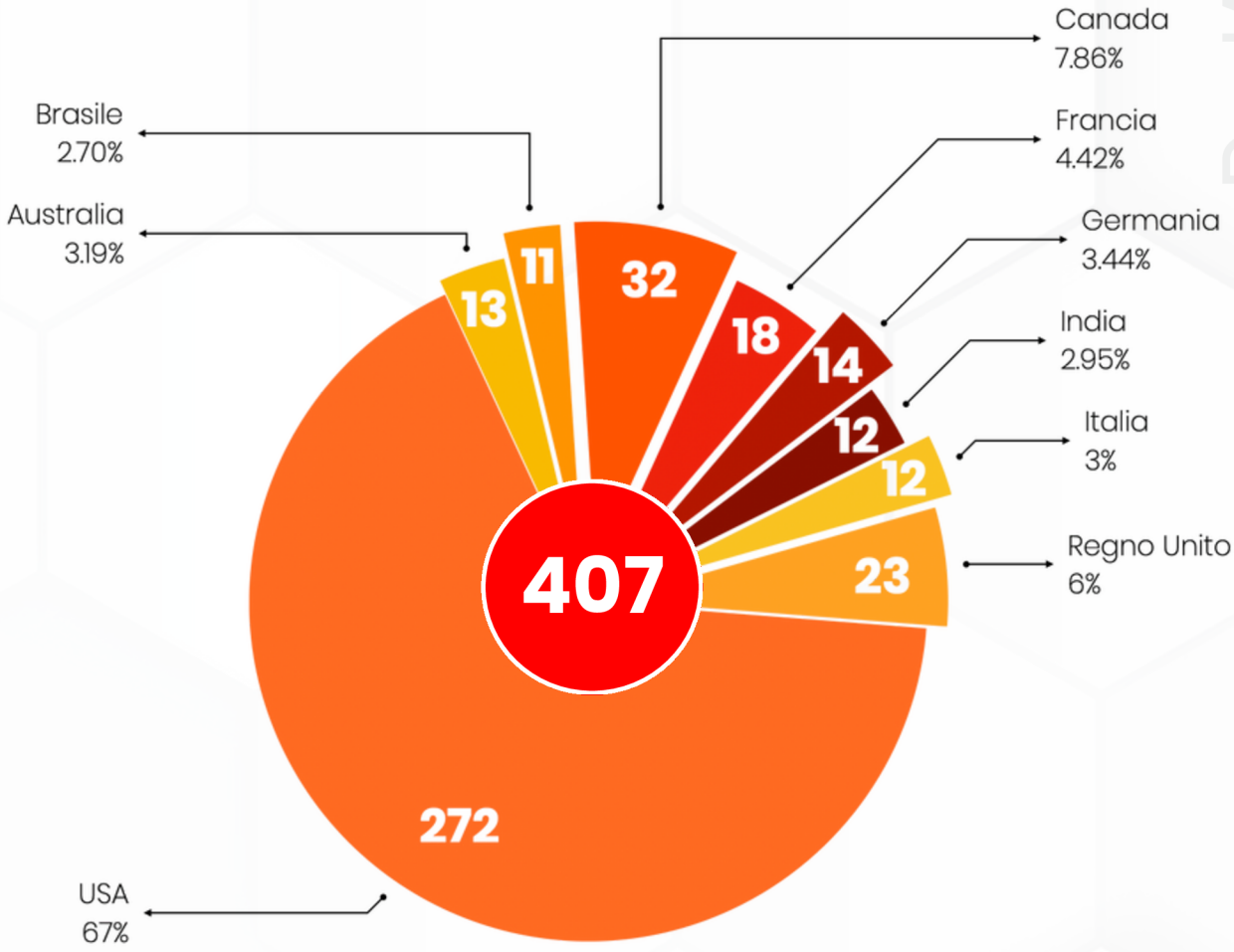
il **dataset** di gennaio 2025, con tutte le rivendicazioni è disponibile qui: **https://rnws.online/YyZGM**

29 invece sono i gruppi che hanno rivendicato **meno di 10 attacchi**, per un totale complessivo di **124 rivendicazioni** (*fonti aggregate, elaborazione ransomNews*).

Abyss, 2
Apos Security, 1
APT73 / BASHE, 6
BianLian, 1
Black Basta, 8
Cactus, 9
Cicada3301, 1
CiphBit, 1
Cloak, 8
DarkVault, 2
ElDorado, 6
EMBARGO, 1
Everest, 7
FSociety FLocker, 3
GD LockerSec, 5
Handala, 2
Hunters, 9
Kairos, 6
KillSec, 9
MedusaLocker, 1
Metaencryptor, 1
Money Message, 1
MONTI, 8
Morpheus, 3
RansomHouse, 1
Rhysida, 9
Sarcoma, 8
Termite, 2
ThreeAM, 3

/breakdown_world

Riportiamo nel grafico i paesi che, in questo mese, hanno subito **più di 10 attacchi**, su un totale di **60 paesi colpiti**. Si tratta di **9 paesi**, per complessive **407 rivendicazioni** (*fonti aggregate, **elaborazione ransomNews***).



Gli attacchi ai rimanenti **51 paesi**, per un totale di **112 rivendicazioni**, sono così suddivisi (*fonti aggregate, **elaborazione ransomNews***):

- Algeria, 1
- Argentina, 5
- Austria, 4
- Belgio, 4
- Cile, 2
- Cina, 3
- Colombia, 4
- Croazia, 1
- Cipro, 1
- Danimarca, 2
- Egitto, 2
- El Salvador, 1
- Emirati Arabi, 2
- Finlandia, 2
- Georgia, 1
- Giamaica, 1
- Giappone, 3
- Hong Kong, 1
- Indonesia, 2
- Irlanda, 1
- Israele, 2
- Kenya, 1
- Lituania, 1
- Malesia, 2
- Malta, 1
- Marocco, 1
- Messico, 4
- Paesi Bassi, 4
- Nigeria, 2
- Non Disponibile, 2
- Nuova Zelanda, 1
- Oman, 1
- Pakistan, 1
- Perù, 1
- Polonia, 1
- Portogallo, 2
- Portorico, 1
- Rep. Ceca, 3
- Rep. Dominicana, 2
- Romania, 1
- Singapore, 5
- Spagna, 8
- Svezia, 4
- Svizzera, 4
- Sud Africa, 1
- Tailandia, 5
- Taiwan, 2
- Turchia, 2
- Uruguay, 1
- Venezuela, 1
- Vietnam, 2

/breakdown_groups

Nella tabella, il numero delle vittime accertate per ogni gruppo ransomware a partire **dal 1° gennaio 2025**, per un totale di **519 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, 25
Abyss, 2
akira, 72
Apos Security, 1
APT73 / BASHE, 6
BianLian, 1
Black Basta, 8
Cactus, 9
Cicada3301, 1
CiphBit, 1
CL0P^_, 60
Cloak, 8
DarkVault, 2
DragonForce, 13
ElDorado, 6
EMBARGO, 1
Everest, 7
FSociety FLocker, 3
FOG, 15
GD LockerSec, 5
Handala, 2
Hunters, 9
INC Ransom, 28
Kairos, 4
KillSec, 9
LockBit3, 10
Lynx, 41
Medusa, 22
MedusaLocker, 1
MetaEncryptor, 1
MoneyMessage, 1
MONTI, 8
Morpheus, 3
PLAY, 11
Qilin, 23
RansomHouse, 1
RansomHub, 43
Rhysida, 9
SafePay, 21
Sarcoma, 8
Space Bears, 11
Termite, 2
ThreeAM, 3

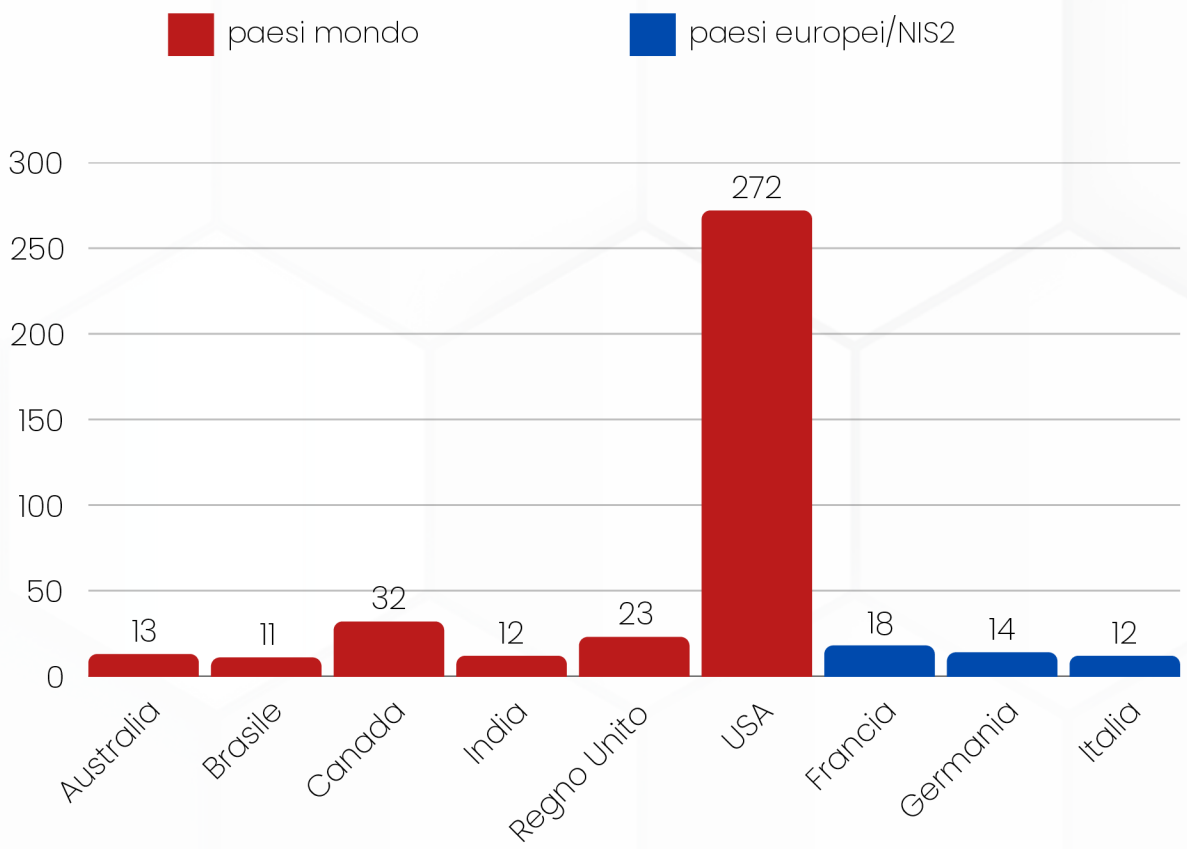
Il gruppo **CL0P^_** ha rivendicato, dal mese di **dicembre 2024**, attacchi contro aziende che utilizzano piattaforme di trasferimento file di **Cleo** (*Harmony, VLTrader, LexiCom*), sfruttando **due vulnerabilità 0day: CVE-2024-50623** e **CVE-2024-55956**
.
Queste falle, scoperte a ottobre, permettevano il caricamento e scaricamento di file **senza restrizioni,** portando all'**esecuzione di codice da remoto**. Una di esse veniva sfruttata per aprire una **reverse shell**, dando agli attaccanti accesso completo ai sistemi compromessi.

Riportiamo anche la distribuzione degli attacchi per ogni paese colpito, **dal 1° gennaio 2025**, ad *esclusione dei paesi europei/NIS2*, per un **totale di 435 attacchi** (*fonti aggregate, **elaborazione ransomNews***):

Algeria, 1
Argentina, 5
Australia, 13
Brasile, 11
Canada, 32
Cile, 2
Cina, 3
Colombia, 4
Egitto, 2
El Salvador, 1
Emirati Arabi, 2
Georgia, 1
Giamaica, 1
Giappone, 3
Hong Kong, 2
India, 12
Indonesia, 2
Israele, 2
Kenia, 1
Malesia, 2
Marocco, 4
Messico, 4
Nigeria, 2
Non Disponibile, 2
Nuova Zelanda, 1
Oman, 1
Pakistan, 1
Perù, 1
Portorico, 1
Regno Unito, 23
Rep. Dominicana, 2
Singapore, 5
Sud Africa, 1
Svizzera, 4
Tailandia, 5
Taiwan, 2
Turchia, 2
Uruguay, 1
USA, 272
Venezuela, 1
Vietnam, 2

/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 **gennaio 2025**:

- **Morpheus** (The Great Morpheus) - attivo probabilmente dalla fine di novembre 2024, il gruppo sembra utilizzare un payload molto simile a quello utilizzato da HellCat, il che indicherebbe un possibile builder condiviso.
- **GD LockerSec** - precedentemente noto come "*GhostSec-Devil*", il nome alluderebbe forse ad un potenziale collegamento con il gruppo GhostSec e il *GhostLocker ransomware*. Non esistono, al momento, prove certe a sostegno di questo collegamento.

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

/ransomware_price

Alla data odierna, secondo fonti aggregate, i due riscatti più alti pagati nel 2024 risultano essere:

- **CDK Global**, attaccato da **BlackSuit** a giugno, per **25 milioni di dollari** (387BTC)
- **Change Healthcare**, attaccato da **ALPHV/BlackCat** a febbraio, per **22 milioni di dollari**

/whois_core

@signorina37
Claudia Galingani Mongini

@sonoclaudio
Claudio Sono

@alekitto
Alessandro Chitolina

@fed
Federico Marsili

/whois_special

@garantepiracy
Christian Bernieri

RedACT

RANSOMNEWS DISCLOSURE & ACTIVITY TRACKING

/staysafe