RedACT

RANSOMNEWS DISCLOSURE & ACTIVITY TRACKING

REPORT MENSILE
MAGGIO 2025

real data. real threats. ***ransomNews.***

/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 e analizzata manualmente**, senza l'impiego 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

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

/use_conditions

/executive_summary

Nel mese di maggio sono state registrate **441 rivendicazioni** a livello globale.

HIGHLIGHTS

- **Italia**: sono stati rilevati **12 attacchi**, con **641.50GB** di dati pubblicati. La regione **Lombardia** si assesta al primo posto con una netta maggioranza di attacchi, mentre i settori più colpiti sono la manifattura di genere e la distribuzione farmaceutica.
- **Area NIS2** (UE): **100 attacchi** rilevati. I tre paesi più colpiti sono **Germania**, **Spagna** e **Italia.**
- **Globale**: i gruppi più attivi del mese sono PLAY, Qilin, akira e Safepay.

TREND TECNICI

- **Tecnica di accesso dominante**: *phishing* mirato e *credential stealing*
- **Evoluzione**: uso di GenAI, loader multistadio e LOLbins, malware FakeUpdate
- **Vettori persistenti:** servizi esposti, VPN non patchate, riutilizzo di credenziali

ANALISI DI CONTESTO

Le imprese hanno dovuto fronteggiare un nuovo picco di ransomware e campagne DDoS ancora attive contro **telecomunicazioni** e **PA**, agevolate da *spear-phishing* e configurazioni SPF/DKIM/DMARC carenti.

settori più colpiti

manifattura e **distribuzione**

phishing e **credential stealing** ancora **dominanti**

gruppi emergenti in attività maggio

5

/breakdown_italy

Si sono registrati, per questo mese, **12 attacchi**, con una predominanza nell'area geografica del **Nord Italia** (ben 10 attacchi).
Seguono il **Centro Italia** con 1 attacco ed il **Sud Italia**, comprese le **isole**, anch'essi con 1 solo attacco (*fonti aggregate, elaborazione ransomNews*).

attacchi registrati

12

area geografica

Nord

dati pubblicati

641.50GB

settore principale

manifattura

Tabella riepilogativa delle **rivendicazioni confermate** su territorio italiano nel mese di maggio 2025.
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
Studio Vaiani Commercialisti	INCRansom	Crema (CR)	-	-
LUBIAM Moda Uomo SPA	Sarcoma	Mantova	-	5
T.consult SRL	Nova	Curtatone (MN)	10.00 GB	-
Comune di Pisa	Nova	Pisa	100.00 GB	-
Stiga SPA	IMNCrew	Castelfranco V.to (TV)	180.00 GB	-
Antea Luce SRL	Arcus	Savignano Rubicone (FC)	-	1
SAMA SRL	KillSec	Montichiari (BS)	-	1
Novaria SRL	KillSec	Como	-	1
Qualitas Commercialisti	Direwolf	Lecco	350.00 GB	-
Alliance Healthcare SPA	DATACARRY	Lavagna (GE)	-	-

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

/breakdown_italy

VITTIMA	GRUPPO	LOCALIZZAZIONE	DATI	NOTE
DM Barone SPA	Devman*	Modica (RG)	-	-
Termignoni SPA	akira	Predosa (AL)	1.50 GB	-

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

* il gruppo **Devman** non è attualmente inserito nel monitoraggio attivo; tracciamo unicamente le rivendicazioni che riguardano target italiani.

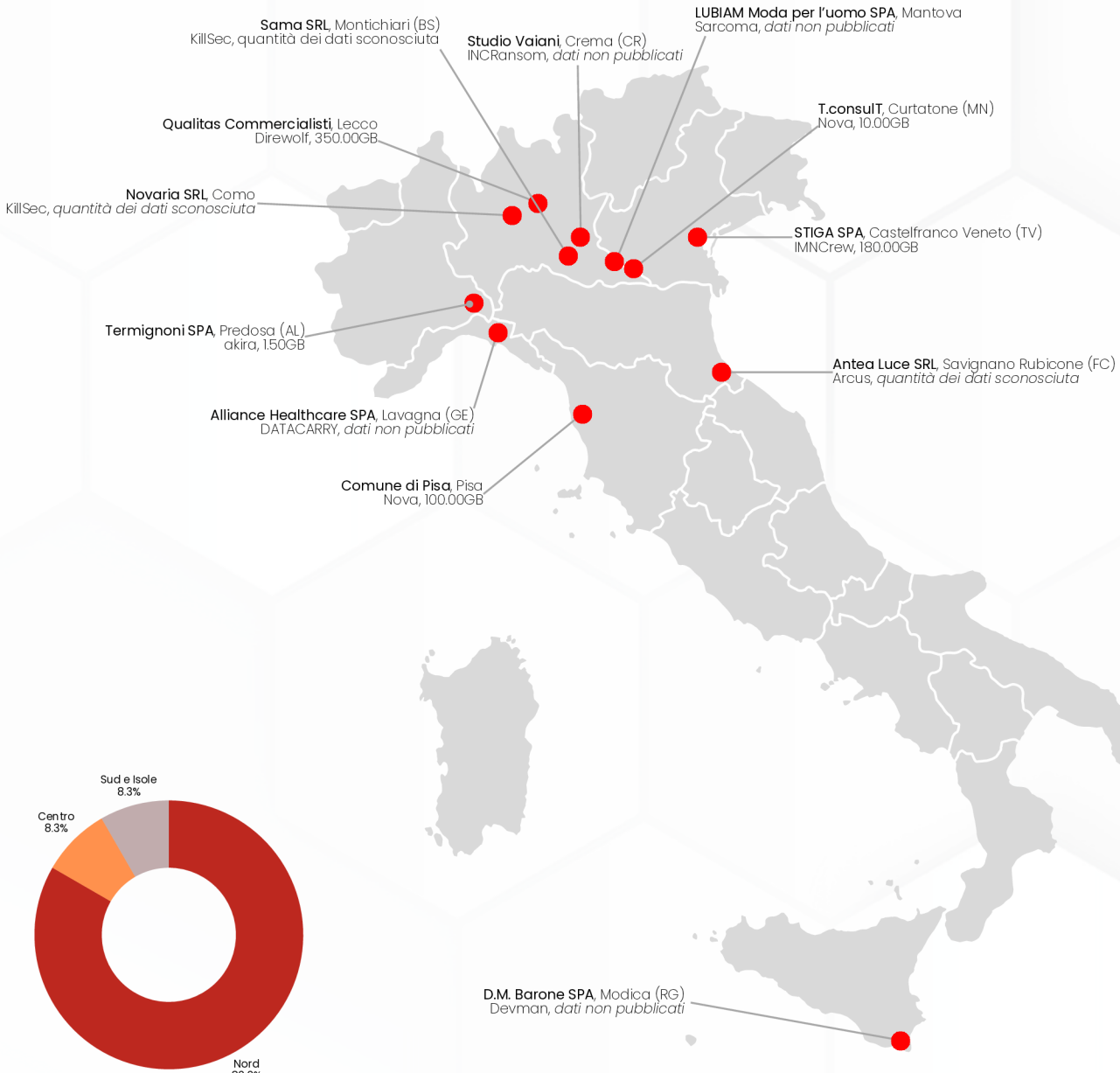
MESE	DATI (GB)	TREND	NOTE
✓ Gennaio	5178.82	—	
✓ Febbraio	1561.80	▼	
✓ Marzo	2553.90	▲	
✓ Aprile	2685.47	▲	1 target rimosso dal DLS
✓ Maggio	641.50	▼	
Giugno			
Luglio			
Agosto			
Settembre			
Ottobre			
Novembre			
Dicembre			

Totale generale dati esfiltrati dichiarati e pubblicati, in Italia: **12621.49 GB**

Nota: *il totale globale dei dati esfiltrati è basato sulle informazioni disponibili al momento della pubblicazione. Potrà subire variazioni nei mesi successivi in caso di aggiornamenti o rilevamenti retroattivi.*

/breakdown_italy_map

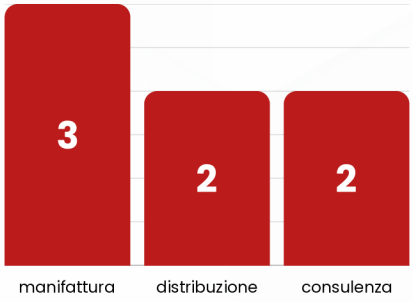
Visualizzazione geografica degli attacchi ransomware **confermati** sul territorio italiano. La mappa mostra la distribuzione regionale degli incidenti registrati nel mese, con indicazione del volume di dati pubblicati (dichiarati) per ciascuna rivendicazione.



Focus regionale

La regione più colpita è la **Lombardia**, che conta ben 6 attacchi.

Seguono Piemonte, Veneto, Emilia Romagna, Liguria, Toscana e Sicilia.



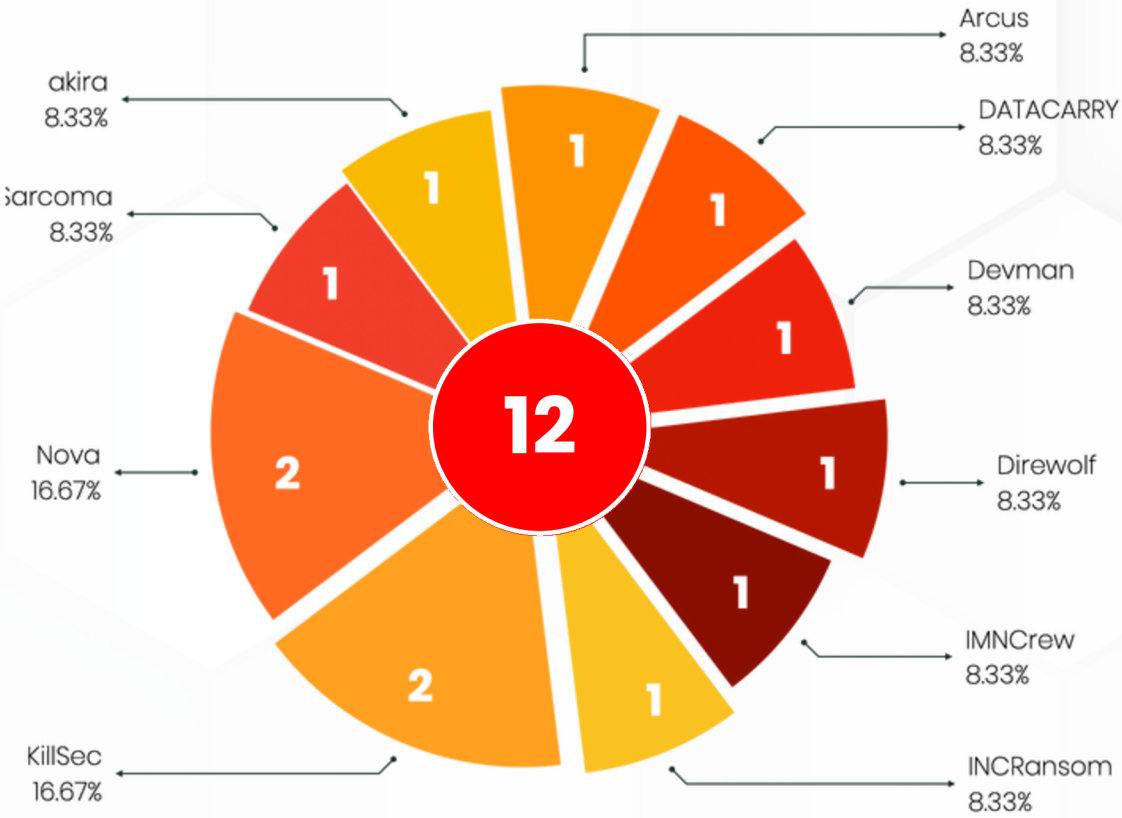
Dati esfiltrati

Il volume dei dati pubblicati per la regione Lombardia ammonta a **360.00GB**.

Nonostante la capillarità degli attacchi, il quantitativo dei dati è basso.

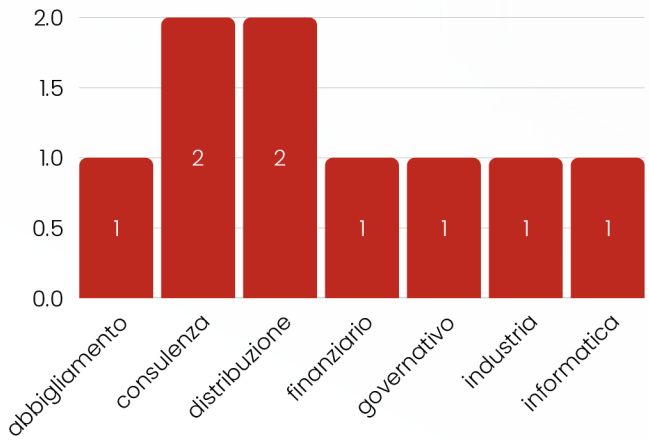
/breakdown_italy_groups

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 **maggio**, in Italia, gli attacchi hanno interessato i seguenti settori:



La concentrazione di attacchi nelle aree industriali del **Nord Italia** continua a mettere in luce le **vulnerabilità delle imprese** attive in settori ad alta interconnessione logistica e digitale.

A maggio, l'intrusione iniziale ha avuto origine principalmente da **servizi esposti in rete** o da **credenziali compromesse**, spesso raccolte tramite campagne di **phishing** mirato.

La ricorrenza degli attacchi in queste aree è dovuta alla persistenza di **vettori non ancora neutralizzati**, riconducibili a criticità strutturali.

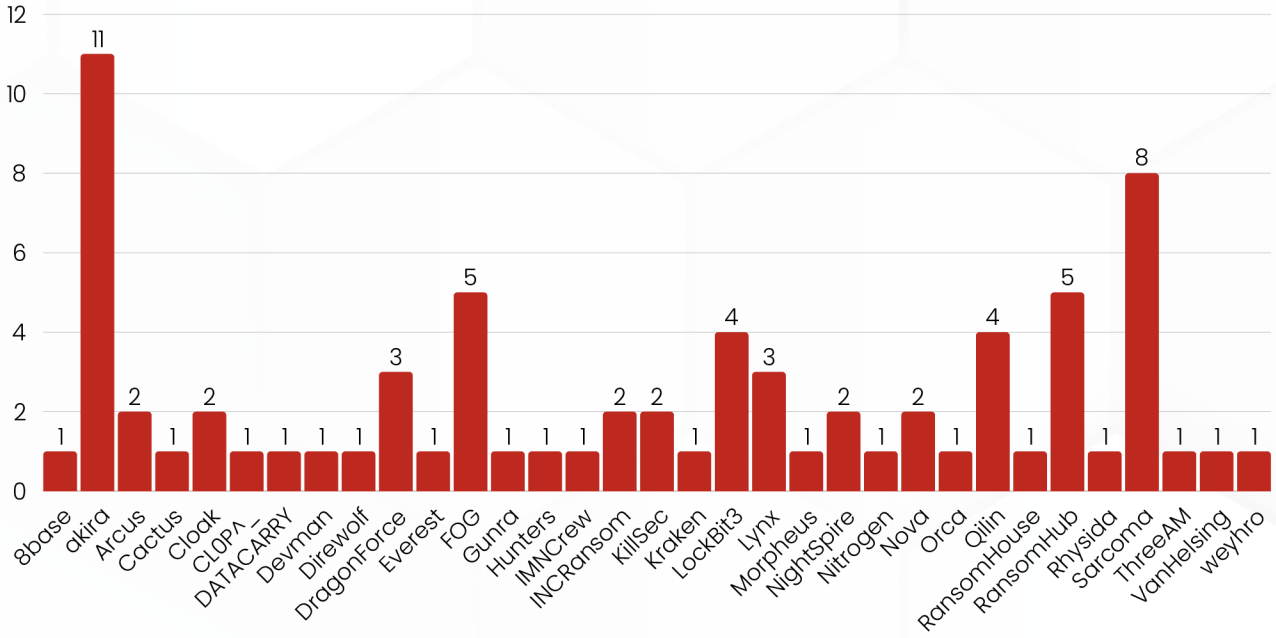
Parallelamente, si osserva una crescente adozione di strumenti basati su **intelligenza artificiale**, utilizzati per raffinare ancor più le tecniche di **social engineering** e aumentare la precisione delle campagne di compromissione.

/breakdown_italy_groups

Nella tabella, il numero delle **vittime italiane** accertate per ogni gruppo, a partire **dal 1° gennaio 2025**, per un totale di **74 rivendicazioni** divise fra 33 gruppi (*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	DragonForce, 3	LockBit3, 4	RansomHub, 5
akira, 11	Everest, 1	Lynx, 3	Rhysida, 1
Arcus, 2	FOG, 5	Morpheus, 1	Sarcoma, 8
Cactus, 1	Gunra, 1	Nightspire, 2	ThreeAM, 1
Cloak, 2	Hunters, 1	Nitrogen, 1	VanHelsing, 1
CL0P^_, 1	IMNCrew, 1	Nova, 2	weyhro, 1
DATACARRY, 1	INCRansom, 2	Orca, 1	
Devman, 1	KillSec, 2	Qilin, 4	
Direwolf, 1	Kraken, 1	RansomHouse, 1	



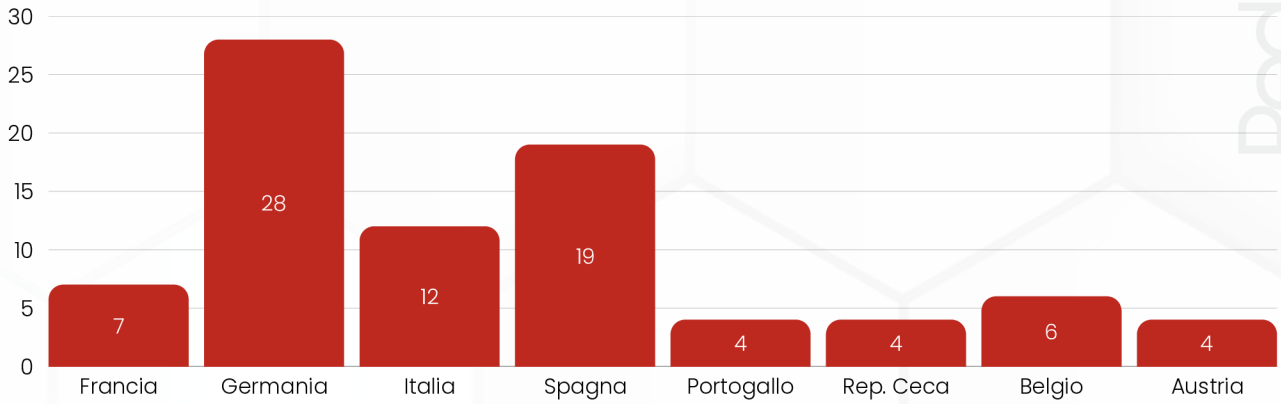
📌 **RansomHub**, sulla scena fin da febbraio 2024, si è rapidamente affermato come player di primo piano nel panorama ransomware, grazie a un modello RaaS altamente scalabile.
A marzo-aprile 2024 ha preso di mira grandi obiettivi come **Change Healthcare** (dopo l'exit scam di ALPHV/BlackCat) e **Christie's**, sfruttando campagne di **phishing mirato**, vulnerabilità come Netlogon/CVE-2020-1472, e uno schema affiliativo aggressivo che ha sfruttato affiliati defezionari proprio di ALPHV.

In pochi mesi (giugno 2024) ha rappresentato circa il 21% degli attacchi, superando LockBit come gruppo criminale dominante.

Tuttavia, tra aprile e maggio 2025 l'infrastruttura di RansomHub è andata offline, lasciando gli affiliati disorientati. Molti di loro sono migrati verso **Qilin** e **DragonForce**, quest'ultimo ha comunicato di aver inglobato parte dell'ecosistema di RansomHub e di aver iniziato una "*cyber turf war*" per acquisire totalmente i suoi asset criminali.

/breakdown_europe_nis2

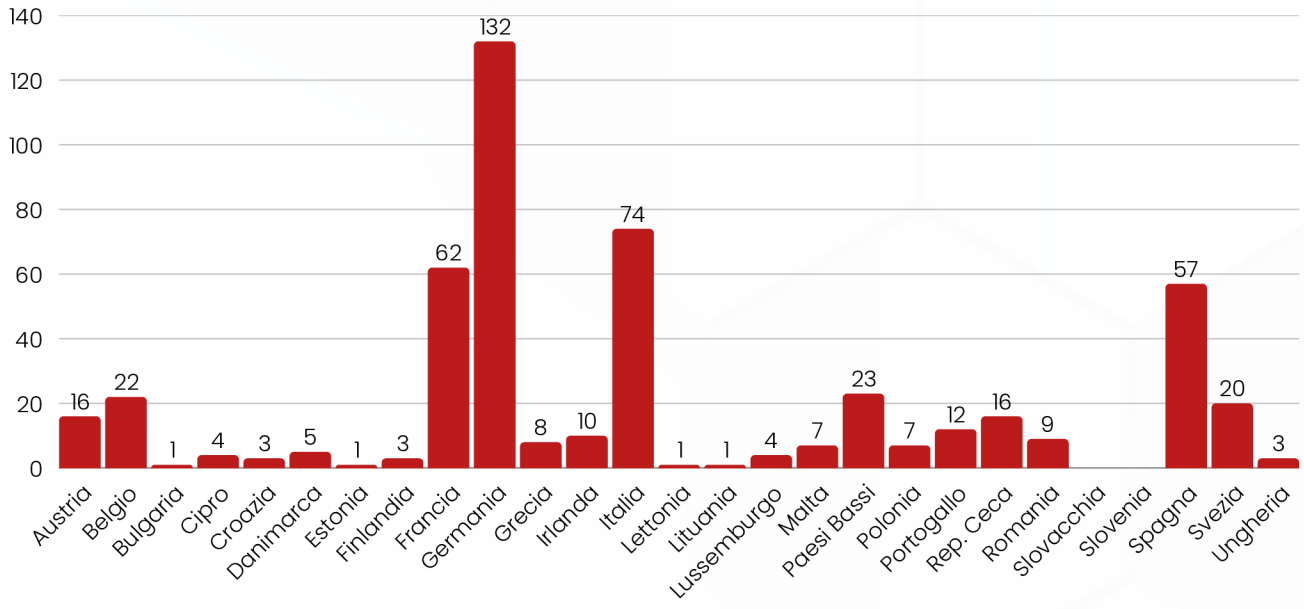
Nel mese di **maggio 2025**, i Paesi UE che adottano le normative della **Direttiva NIS2** hanno subito un totale di **100 attacchi**.
I più colpiti sono stati **Germania**, **Spagna** e **Italia** (*fonti aggregate, **elaborazione ransomNews***).



- **Austria**, 4
- **Belgio**, 6
- **Bulgaria**, 0
- **Cipro**, 1
- **Croazia**, 1
- **Danimarca**, 1
- **Estonia**, 0
- **Finlandia**, 0
- **Francia**, 7
- **Germania**, 28
- **Grecia**, 2
- **Irlanda**, 0
- **Italia**, 12
- **Lettonia**, 1
- **Lituania**, 0
- **Lussemburgo**, 0
- **Malta**, 3
- **Paesi Bassi**, 2
- **Polonia**, 0
- **Portogallo**, 4
- **Rep. Ceca**, 4
- **Romania**, 2
- **Slovacchia**, 0
- **Slovenia**, 0
- **Spagna**, 19
- **Svezia**, 2
- **Ungheria**, 1

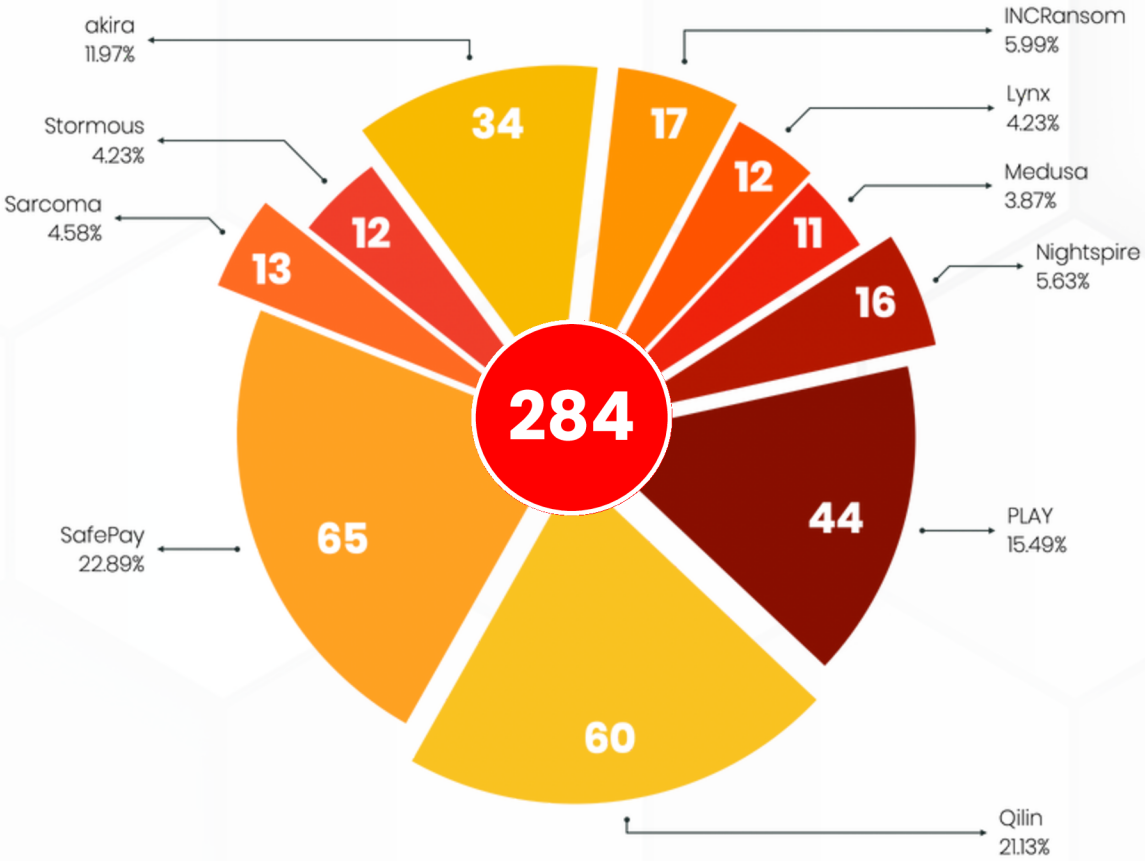
Distribuzione degli incidenti ransomware rilevati **per ciascun paese** membro, sulla base delle rivendicazioni confermate, a partire **dal 1° gennaio 2025,** per un totale di **501 attacchi.**

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



/breakdown_world

441 sono le **rivendicazioni tracciate**, da fonti aggregate, per il mese corrente. Nel grafico sono riportati i gruppi che hanno totalizzato **più di 10 attacchi**: **10 gruppi**, per un **totale** di **284 attacchi** (*elaborazione ransomNews*).



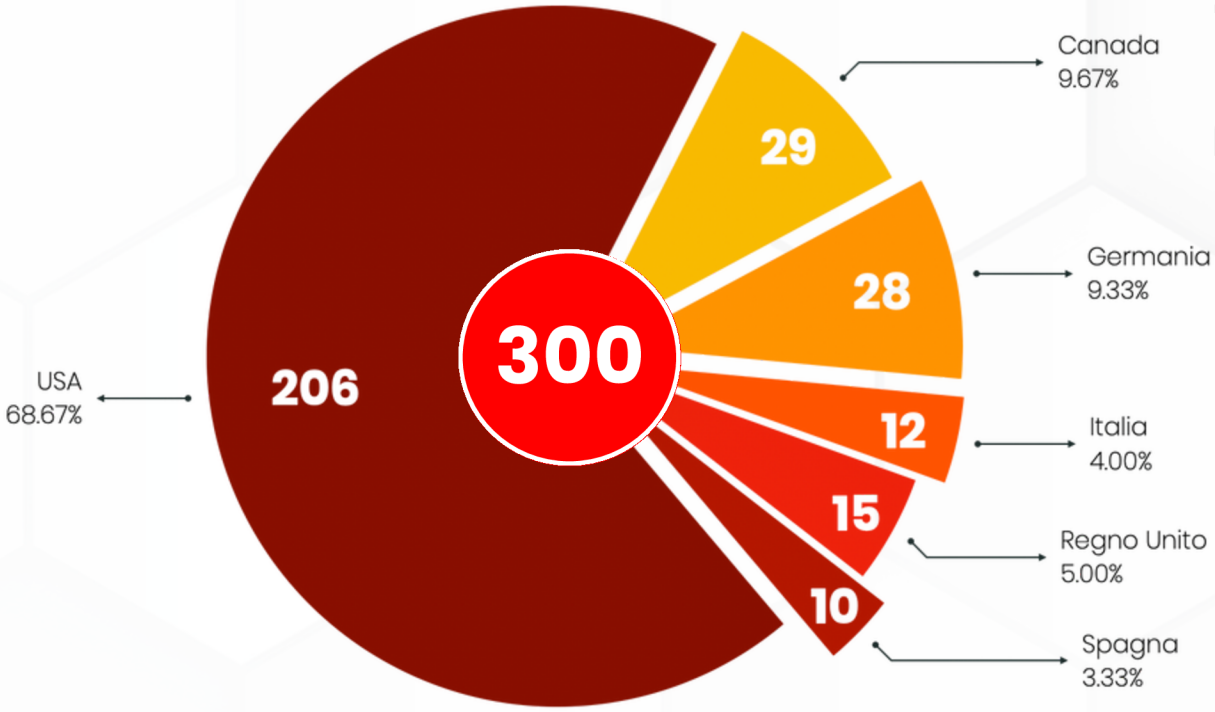
il **dataset** di maggio 2025, con **tutte le rivendicazioni** è disponibile su **ransomnews.online**

43 invece sono i gruppi che hanno rivendicato **meno di 10 attacchi**, per un totale complessivo di **157 rivendicazioni** (*fonti aggregate, elaborazione ransomNews*).

Apos, 3
Arcus, 8
Arkana, 2
BERT, 2
Blacklock, 6
Blacksuit, 3
Brain Cipher, 6
CHAOS, 1
CiphBit, 1
CL0P^_, 1
Cloak, 2
Crypto24, 2
DATACARRY, 9
Devman, 1
Direwolf, 8
DragonForce, 2
EMBARGO, 3
Everest, 9
FSociety FLocker, 1
Gunra, 6
Hunters, 5
IMNCrew, 2
InterLock, 6
J Group, 5
Kairos, 3
KillSec, 5
Kraken, 2
LockBit3, 5
Medusalocker, 2
MONTI, 2
Morpheus, 1
Nitrogen, 1
Nova, 5
Orca, 1
RansomHouse, 5
Rhysida, 9
Silent, 1
Skira Team, 1
SpaceBears, 5
Termite, 1
ThreeAM, 1
weyhro, 4
WorldLeaks, 9

/breakdown_world

Nel grafico sono evidenziati gli **6 paesi** che, nel mese, hanno registrato **più di 10 attacchi**. Su un totale di **57 nazioni** colpite (inclusi i paesi NIS2), queste rappresentano **300 rivendicazioni** complessive (*fonti aggregate, **elaborazione ransomNews***).



Gli attacchi ai rimanenti **51 paesi** (mondo e paesi NIS2), per un totale generale di **132 rivendicazioni**, sono così suddivisi (*fonti aggregate, **elaborazione ransomNews***):

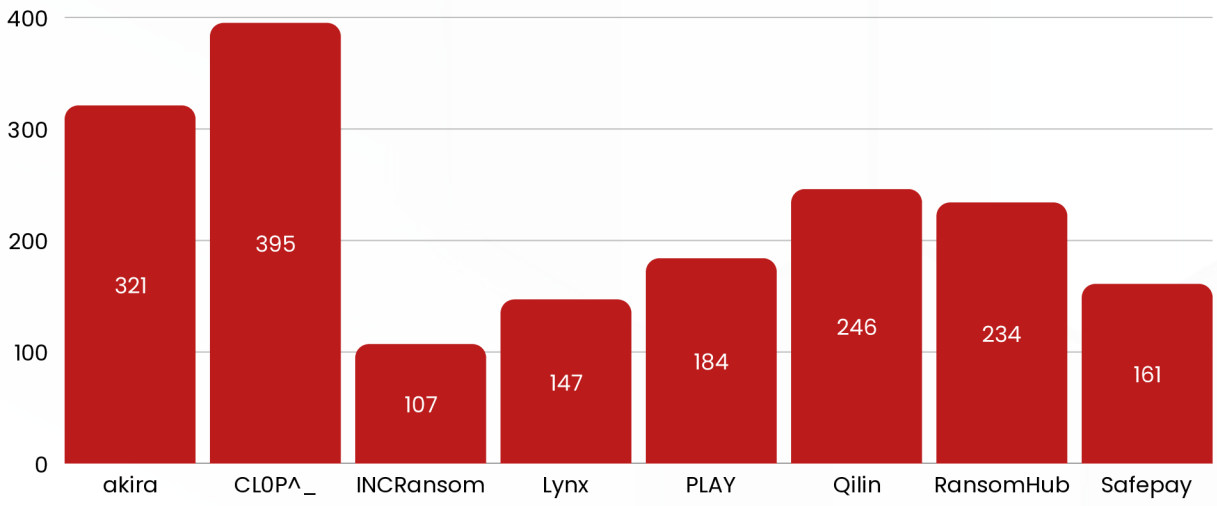
- Arabia Saudita, 2
- Argentina, 1
- Australia, 6
- Austria, 4
- Barhain, 1
- Barbados, 1
- Belgio, 6
- Bosnia Herzegovina, 1
- Botswana, 1
- Brasile, 8
- Camerun, 1
- Cina, 1
- Cipro, 1
- Colombia, 3
- Corea del Sud, 1
- Croazia, 1
- Danimarca, 1
- Ecuador, 1
- Egitto, 1
- El Salvador, 1
- Emirati Arabi, 6
- Filippine, 3
- Francia, 7
- Giappone, 8
- Grecia, 2
- India, 2
- Indonesia, 1
- Lettonia, 1
- Libano, 1
- Malesia, 3
- Malta, 3
- Messico, 1
- Norvegia, 3
- Paesi Bassi, 2
- Perù, 1
- Portogallo, 4
- Rep. Ceca, 4
- Rep. Dominicana, 1
- Rep. Maldive, 1
- Romania, 2
- Serbia, 1
- Singapore, 6
- Sud Africa, 3
- Sri Lanka, 2
- Svezia, 2
- Svizzera, 5
- Tailandia, 2
- Taiwan, 3
- Turchia, 4
- Venezuela, 4
- Ungheria, 1

/breakdown_groups

Nella tabella, il numero delle vittime accertate per ogni gruppo ransomware a partire dal 1° gennaio 2025, per un totale di **3104 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, 12
akira, 321
Anubis, 7
Apos, 8
APT73 / BASHE, 12
Arcus, 27
Arkana, 4
BERT, 5
BianLian, 35
Black Basta, 8
Blacklock, 12
Blackout, 1
Blacksuit, 8
Brain Cipher, 10
Cactus, 53
CHAOS, 9
Cicada3301, 21
CiphBit, 3
CL0P^_, 395
Cloak, 22
Crazyhunters, 10
Crypto24, 10
DarkVault, 2
DATACARRY, 9
Devman, 1
Direwolf, 8
DragonForce, 57
Dunghill Leak, 1
EMBARGO, 9
Everest, 19
FOG, 90
Frag, 28
FSociety FLocker, 15
GD LockerSec, 5
Gunra, 11
Handala, 4
HellCat, 12
Hunters, 47
IMNCrew, 8
INCRansom, 107
InterLock, 20
J Group, 18
Kairos, 23
KillSec, 74
Kraken, 9
LEAKEDDATA, 37
Linkc, 1
LockBit3, 40
Lynx, 147
Medusa, 95
MedusaLocker, 6
Metaencryptor, 2
MoneyMessage, 2
MONTI, 17
Morpheus, 9
Nightspire, 55
Nitrogen, 7
Nova, 6
Orca, 2
PLAY, 184
Qilin, 246
RALord, 14
RansomEXX, 3
RansomHouse, 14
RansomHub, 234
Rhysida, 42
Run Some Wares, 5
SafePay, 161
Sarcoma, 53
SECP0, 1
Silent, 5
Skira Team, 6
SpaceBears, 25
Stormous, 17
Termite, 14
ThreeAM, 15
Trinity, 7
Underground, 3
VanHelsing, 9
weyhro, 12
WorldLeaks, 9



gruppi con più di 100 attacchi, dal 1 gennaio 2025, *elaborazione ransomNews*

/breakdown_groups

Riportiamo nella tabella la distribuzione degli attacchi per ogni paese colpito, **dal 1° gennaio 2025**, ad *esclusione dei paesi europei/NIS2*, per un **totale di 2603 attacchi** a **76 paesi** (*fonti aggregate, **elaborazione ransomNews***):

- Algeria, 1
- Antigua Barbuda, 1
- Arabia Saudita, 7
- Argentina, 19
- Australia, 54
- Bahamas, 1
- Bahrain, 2
- Bangladesh, 1
- Barbados, 2
- Bielorussia, 1
- Bolivia, 1
- Bosnia Herzegovina, 1
- Botswana, 2
- Brasile, 54
- Camerun, 1
- Canada, 197
- Cile, 10
- Cina, 15
- Colombia, 15
- Corea del Sud, 5
- Costa Rica, 2
- Ecuador, 4
- Egitto, 10
- El Salvador, 3
- Emirati Arabi, 12
- Filippine, 5
- Georgia, 1
- Ghana, 1
- Giamaica, 7
- Giappone, 29
- Giordania, 2
- Haiti, 1
- Hong Kong, 5
- India, 40
- Indonesia, 13
- Iraq, 1
- Israele, 5
- Kenia, 1
- Laos, 1
- Libano, 1
- Malesia, 15
- Marocco, 2
- Messico, 28
- Namibia, 1
- Nigeria, 4
- Non Disponibile, 12
- Norvegia, 10
- Nuova Zelanda, 8
- Oman, 1
- Pakistan, 6
- Panama, 3
- Perù, 8
- Portorico, 4
- Prin. Monaco, 2
- Regno Unito, 107
- Rep. Dominicana, 6
- Rep. Fiji, 1
- Rep. Kiribati, 1
- Rep. Maldive, 1
- Rep. Palau, 1
- Serbia, 1
- Singapore, 30
- Sud Africa, 7
- Sri Lanka, 3
- Svizzera, 27
- Tailandia, 13
- Taiwan, 34
- Tanzania, 2
- Tunisia, 2
- Turchia, 12
- Ucraina, 1
- Uruguay, 2
- USA, 1704
- Venezuela, 5
- Vietnam, 5
- Zambia, 1

/breakdown_groups_new

Nuovi gruppi* in attività nel mese di **maggio 2025**:

- **DATACARRY** - colpisce organizzazioni in settori consumer services, sanità, trasporti e business services, con focus globale.
  Caratteristiche operative: modello a doppia estorsione, brokeraggio dati.
  Tattiche note: phishing, infostealer, rimozione shadow copy, leak pubblico.
  Tecnologie: uso di email riseup, layout site stile desktop.

- **Direwolf** - attivo nei settori tech e industriale a livello globale.
  Caratteristiche operative: modello ransomware personalizzato, leak estorsivo.
  Tattiche note: cifratura, finestra di pagamento definita.
  Tecnologie: in Golang, packer UPX, mutex di esecuzione, terminazione servizi target.

- **J Group** - presunto gruppo data-leak.
  Caratteristiche operative: modello a sola pubblicazione dati.
  Tattiche note: estorsione via leak, senza cifratura nota.
  Tecnologie: leak site generico, assenza di elementi malware noti.

- **LEAKEDDATA** - gruppo focalizzato sulla diffusione di documenti trafugati.
  Caratteristiche operative: modello leak-only site.
  Tattiche note: pubblicazione dati sensibili, pressione reputazionale.
  Tecnologie: anonimizzazione backend, focus su file exposure.

- **WorldLeaks** - sospetto gruppo rebranded.
  Caratteristiche operative: modello di pubblicazione dati, nessuna cifratura.
  Tattiche note: estorsione tramite file exposure.
  Tecnologie: assenza di note tecniche confermate.

***** sono inclusi i gruppi di **nuova costituzione**, **rebrand** e i gruppi **riemersi** dopo oltre un anno di inattività

/DPO_commentary

Gli attacchi ransomware sono **particolarmente dannosi** quando il bersaglio è un **fornitore di servizi** che concentra su di sé il trattamento dei dati di diverse aziende.

Questo mese si caratterizza per la prevalente presenza di **società di consulenza e contabilità**: ciascuno dei clienti degli studi coinvolti ha subito un data breach e dovrà quasi certamente effettuare una autonoma notifica al Garante Privacy.

In questi casi, la vittima del ricatto ha due compiti: **informare il Garante** ed **informare ciascuno dei propri clienti**, a prescindere dalla valutazione di gravità dell'evento.

Purtroppo molti data breach vengono nascosti o taciuti e, di conseguenza, le persone coinvolte non vengono adeguatamente informate: **l'inconsapevolezza amplifica i rischi** e favorisce lo sfruttamento criminale dei dati esfiltrati.

/whois_core

@signorina37
Claudia Galingani Mongini

@sonoclaudio
Claudio Sono

@garantepiracy
Christian Bernieri

@fed
Federico Marsili

/thank_you

@alekitto
Alessandro Chitolina

U2VjdXJpdHkgSXMga2V5LCBCdXQgUmVtZW1iZXIgVG8gSGlkZSBZb3VyIEJhY2t1cA==

RedACT

RANSOMNEWS DISCLOSURE & ACTIVITY TRACKING

/staysafe

real data. real threats. ***ransomNews.***