RedACT

RANSOMNEWS DISCLOSURE & ACTIVITY TRACKING

REPORT MENSILE
APRILE 2025

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

/about

Il report mensile Red**ACT** 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 Red**ACT** 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

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

/use_conditions

/executive_summary

Nel mese di aprile sono state registrate **508 rivendicazioni** a livello globale.

HIGHLIGHTS

- **Italia**: 20 attacchi rilevati, con **2685.47GB** di dati pubblicati. **Lombardia**, Piemonte e Toscana si assestano al primo posto come le regioni più colpite; il settore maggiormente impattato è quello dell'**industria**, seguito dalla **manifattura** e dall'**alimentare**.
- **Area NIS2** (UE): **95 attacchi** rilevati. I tre paesi più colpiti sono **Germania**, **Italia** e **Spagna**.
- **Globale**: i gruppi più attivi del mese sono **akira** e **Qilin**. Nuovi attori come BERT, Gunra e IMNcrew si fregiano di tecniche avanzate e modelli offensivi non convenzionali.

TREND TECNICI

- **Tecnica di accesso dominante**: *phishing* mirato e *credential stealing*
- **Evoluzione**: uso crescente di strumenti AI per migliorare il social engineering
- **Vettori persistenti:** servizi esposti, supply chain & hub, password deboli

ANALISI DI CONTESTO

Il panorama mostra una **crescente specializzazione** e distribuzione dei gruppi. L'Italia resta altamente esposta a causa della densità industriale e dell'interconnessione infrastrutturale.

dati pubblicati
vs marzo
+5.15%

phishing e
credential stealing
ancora
dominanti

gruppi emergenti
in attività da aprile
5

/breakdown_italy

La distribuzione geografica mostra una netta **concentrazione nelle regioni del Nord Italia**, con **12 attacchi**; segue il **Centro con 5 attacchi**, poi **Sud e Isole** con **2 attacco** (*fonti aggregate, **elaborazione ransomNews***) - non viene considerata la rivendicazione di Cloak, in quanto non identificata

attacchi registrati

20

area geografica

nord

dati pubblicati

2685.47GB

settore principale

industria

Tabella riepilogativa delle **rivendicazioni confermate** su territorio italiano nel mese di aprile 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
Grandi Molini Italiani SPA	akira	Rovigo	-	1
Prima Power	akira	Torino	-	1
Sistel SRL	Nightspire	Torino	500.00 GB	-
Baucenter SNC	Qilin	Bolzano	4.00 GB	-
Telecontrol Vigilanza SRL	RansomHouse	Rivoli (TO)	-	-
Asolo Dolce SPA	akira	Asolo (TV)	-	1
TIME SRL	akira	Lucca	-	1
Gruppo C.R. SPA	Sarcoma	Roma	255.00 GB	-
Service Trade SPA	DragonForce	Milano	89.87 GB	-
Govoni Giuseppe e Daniele SAS	Qilin	S. Matteo Decima (BO)	55.00 GB	-
Lamberti SPA	akira	Vicenza	-	1

[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
TRALFO SRL	Sarcoma	Rosciano (PE)	34.00 GB	-
Tutto Per l'Ufficio SRL	LockBit3	Massa (MC)	107.60 GB	-
Bindi SPA	akira	Arezzo	-	1
Lemi Group SRL	INCRansom	Casalbuttano (CR)	80.00 GB	-
Farmo Res SRL	Lynx	Cervia (RA)	300.00 GB	-
MDB SRL	Rhysida	Fossacesia (CH)	1260.00 GB	-
Klinger Italy SRL	Gunra	Rho (MI)	-	1
DFL SRL	Qilin	Sala Consilina (SA)	-	3
target senza nome	Cloak	-	-	3

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

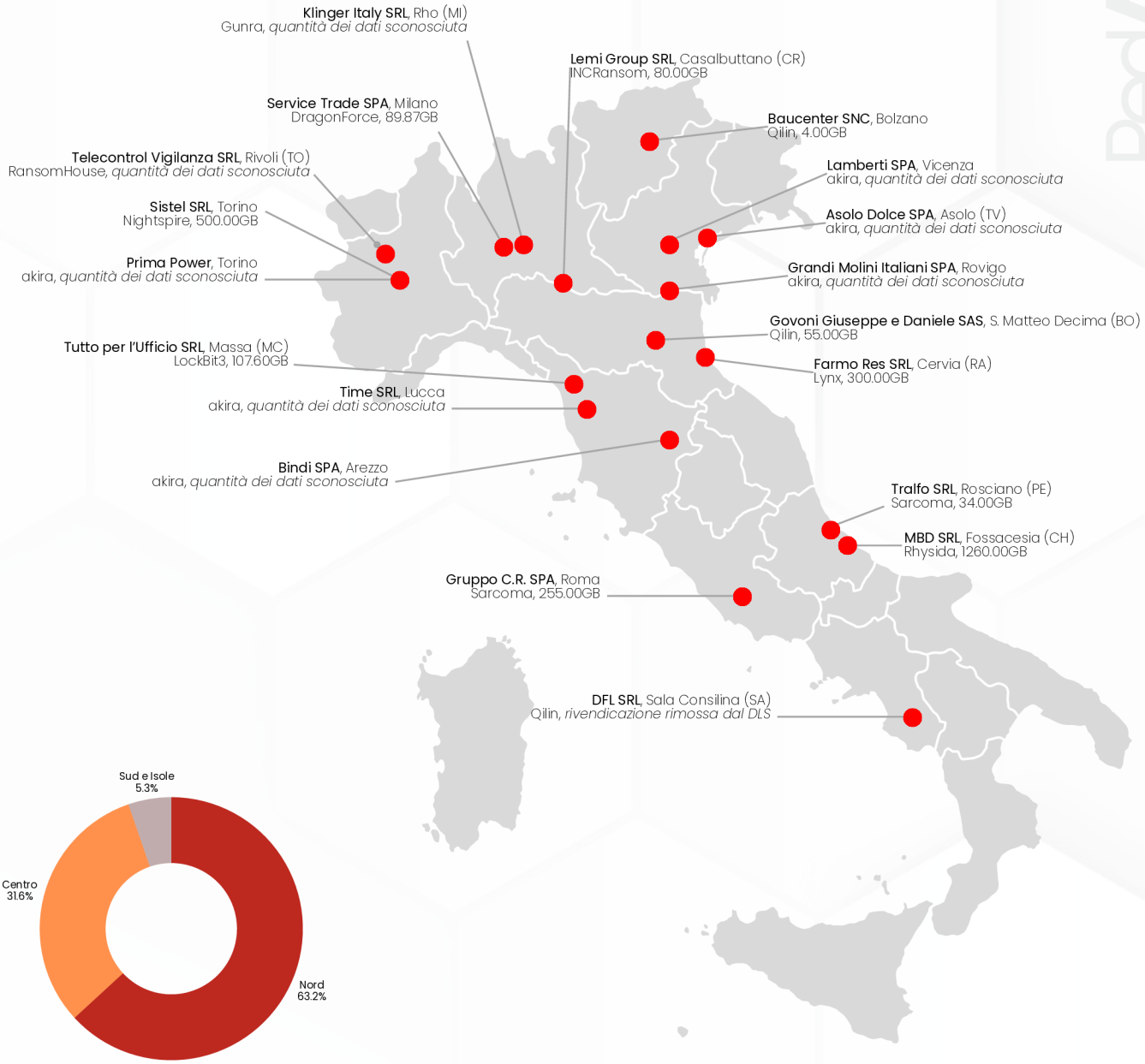
MESE	DATI (GB)	TREND	NOTE
✓ Gennaio	5178.82	–	
✓ Febbraio	1561.80	▼	
✓ Marzo	2553.90	▲	
✓ Aprile	2685.47	▲	1 target non ancora identificato
Maggio			
Giugno			
Luglio			
Agosto			
Settembre			
Ottobre			
Novembre			
Dicembre			

Totale globale dati esfiltrati dichiarati e pubblicati: **11979.99 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

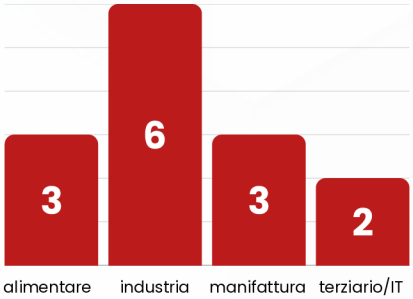
Visualizzazione geografica degli attacchi ransomware **confermati** sul territorio italiano. La mappa mostra la distribuzione regionale degli incidenti registrati nel mese, con indicazione del volume di dati pubblicati (dichiarati) per ciascuna rivendicazione.



Focus regionale

Le regioni più colpite nel mese di aprile sono la **Lombardia**, il **Piemonte**, il **Veneto** e la **Toscana**.

Seguono Emilia Romagna, Abruzzo, Alto Adige, Campania e Lazio.



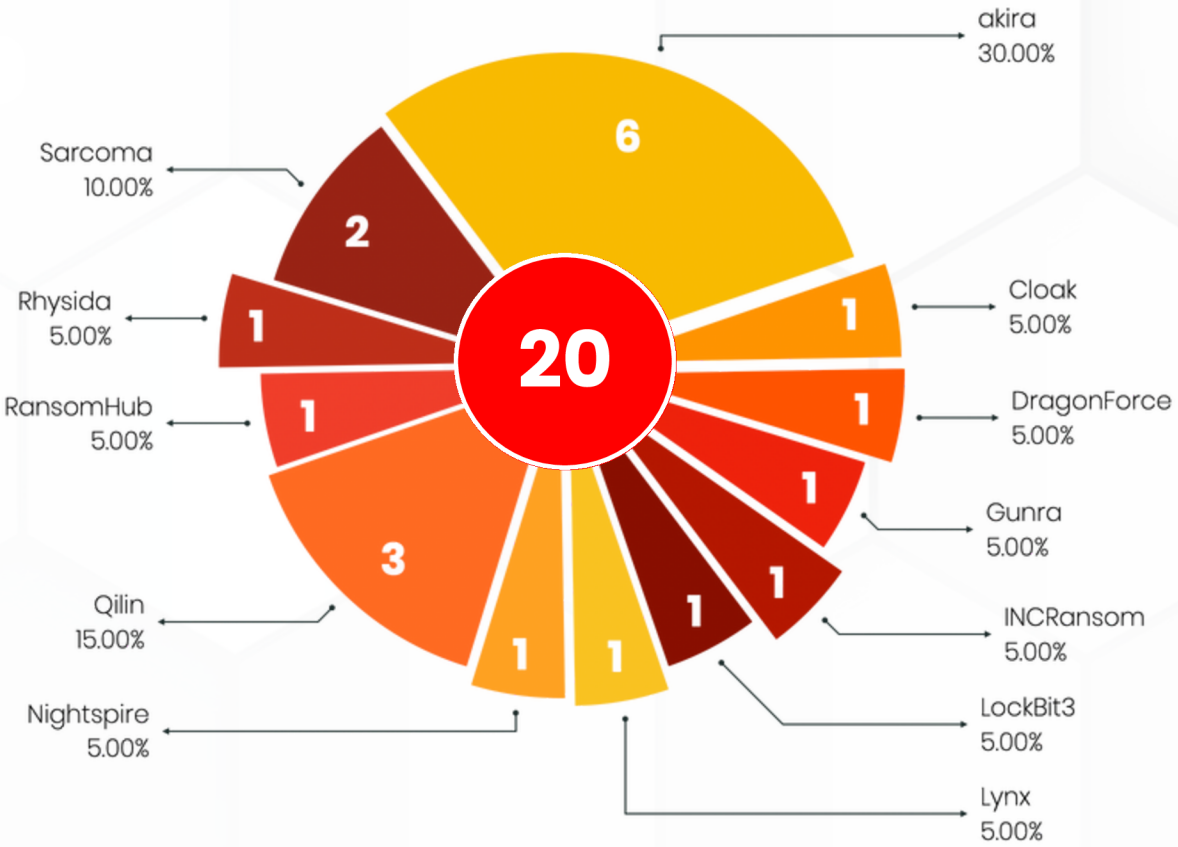
Dati esfiltrati

Il volume dei dati pubblicati per le quattro regioni è di **827.18GB**.

Viene esclusa dal calcolo la rivendicazione del gruppo Cloak - al momento non identificata.

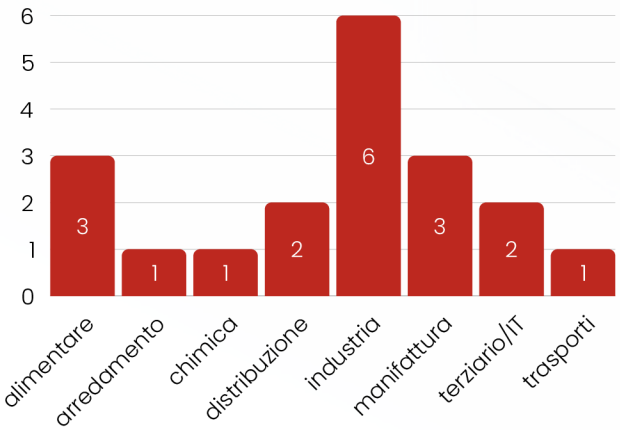
/breakdown_italy_groups

Sono **11 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 marzo, in Italia, gli attacchi hanno interessato i seguenti settori:



L'elevata concentrazione di attacchi nelle aree industriali del **Nord Italia** evidenzia la fragilità delle aziende operanti in settori a forte interconnessione **logistica e digitale**.

Ad aprile, l'accesso iniziale è avvenuto prevalentemente tramite servizi **e accessi esposti** online e/o **credenziali compromesse**, ottenute, per lo più, attraverso **campagne di phishing** mirato.

La **reiterazione** degli attacchi in **specifiche province** e **regioni**, suggerisce la presenza di vettori persistenti non ancora mitigati, potenzialmente **legati a vulnerabilità strutturali**.

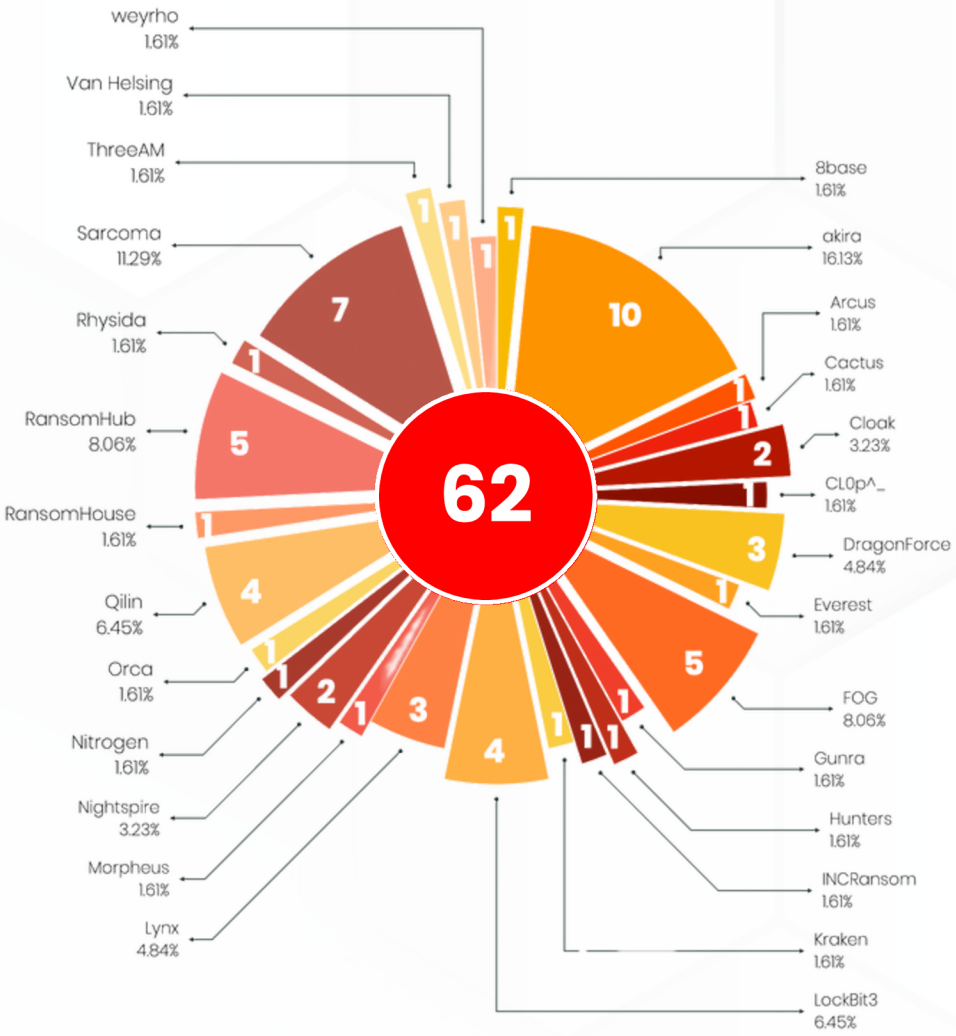
Emergono inoltre segnali di un utilizzo crescente di strumenti **basati su AI** per potenziare il **social engineering** e raffinare le tecniche di compromissione, rendendo gli attacchi più efficaci e mirati.

/breakdown_italy_groups

Nella tabella, il numero delle **vittime italiane** accertate per ogni gruppo, a partire **dal 1° gennaio 2025**, per un totale di **62 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	Everest, 1	Lynx, 3	RansomHub, 5
akira, 10	FOG, 5	Morpheus, 1	Rhysida, 1
Arcus, 1	Gunra, 1	Nightspire, 2	Sarcoma, 7
Cactus, 1	Hunters, 1	Nitrogen, 1	ThreeAM, 1
Cloak, 2	INCRansom, 1	Orca, 1	VanHelsing, 1
CL0P^_, 1	Kraken, 1	Qilin, 4	weyhro, 1
DragonForce, 3	LockBit3, 4	RansomHouse, 1	

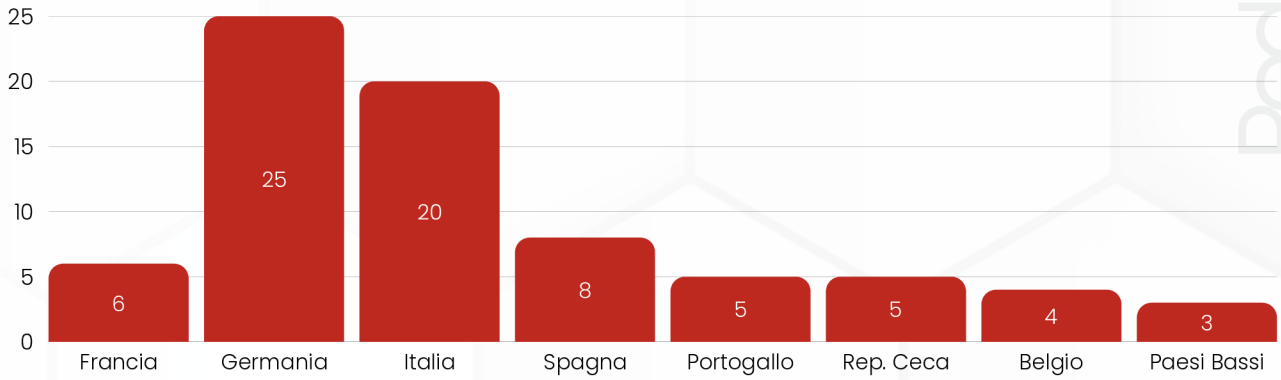


📌La **concentrazione anomala** di attacchi in regioni solitamente a basso impatto di incidenti (Abruzzo in primo luogo) evidenzia un **possibile shift strategico nei target**.

La ricorrenza in aree limitrofe suggerisce l'esistenza di un **potenziale hub infrastrutturale** o logistico condiviso, utilizzato come **vettore per espandere l'attacco** a catena su realtà connesse.

/breakdown_europe_nis2

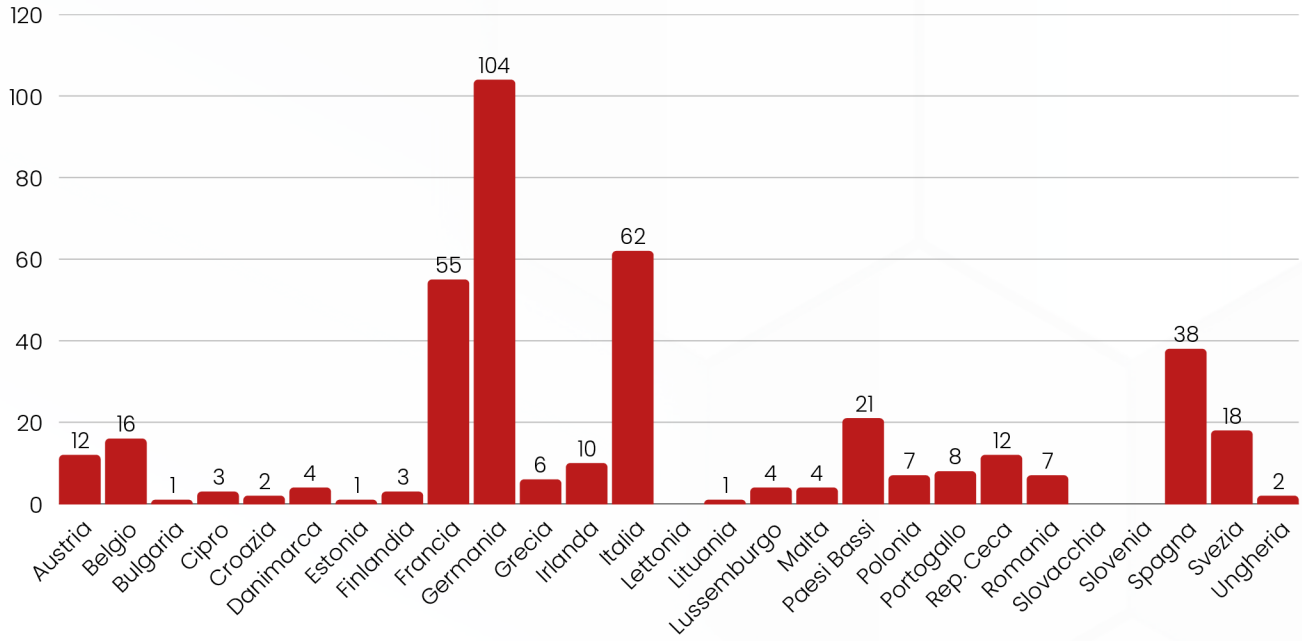
Nel mese di **aprile 2025**, i Paesi UE che adottano le normative della **Direttiva NIS2** hanno subito un totale di **95 attacchi**.
I più colpiti sono stati **Germania**, **Italia** e **Spagna** (*fonti aggregate, **elaborazione ransomNews***).



- **Austria**, 2
- **Belgio**, 4
- **Bulgaria**, 0
- **Cipro**, 1
- **Croazia**, 1
- **Danimarca**, 0
- **Estonia**, 1
- **Finlandia**, 0
- **Francia**, 6
- **Germania**, 25
- **Grecia**, 3
- **Irlanda**, 2
- **Italia**, 20
- **Lettonia**, 0
- **Lituania**, 0
- **Lussemburgo**, 3
- **Malta**, 0
- **Paesi Bassi**, 3
- **Polonia**, 2
- **Portogallo**, 5
- **Rep. Ceca**, 5
- **Romania**, 0
- **Slovacchia**, 0
- **Slovenia**, 0
- **Spagna**, 8
- **Svezia**, 3
- **Ungheria**, 1

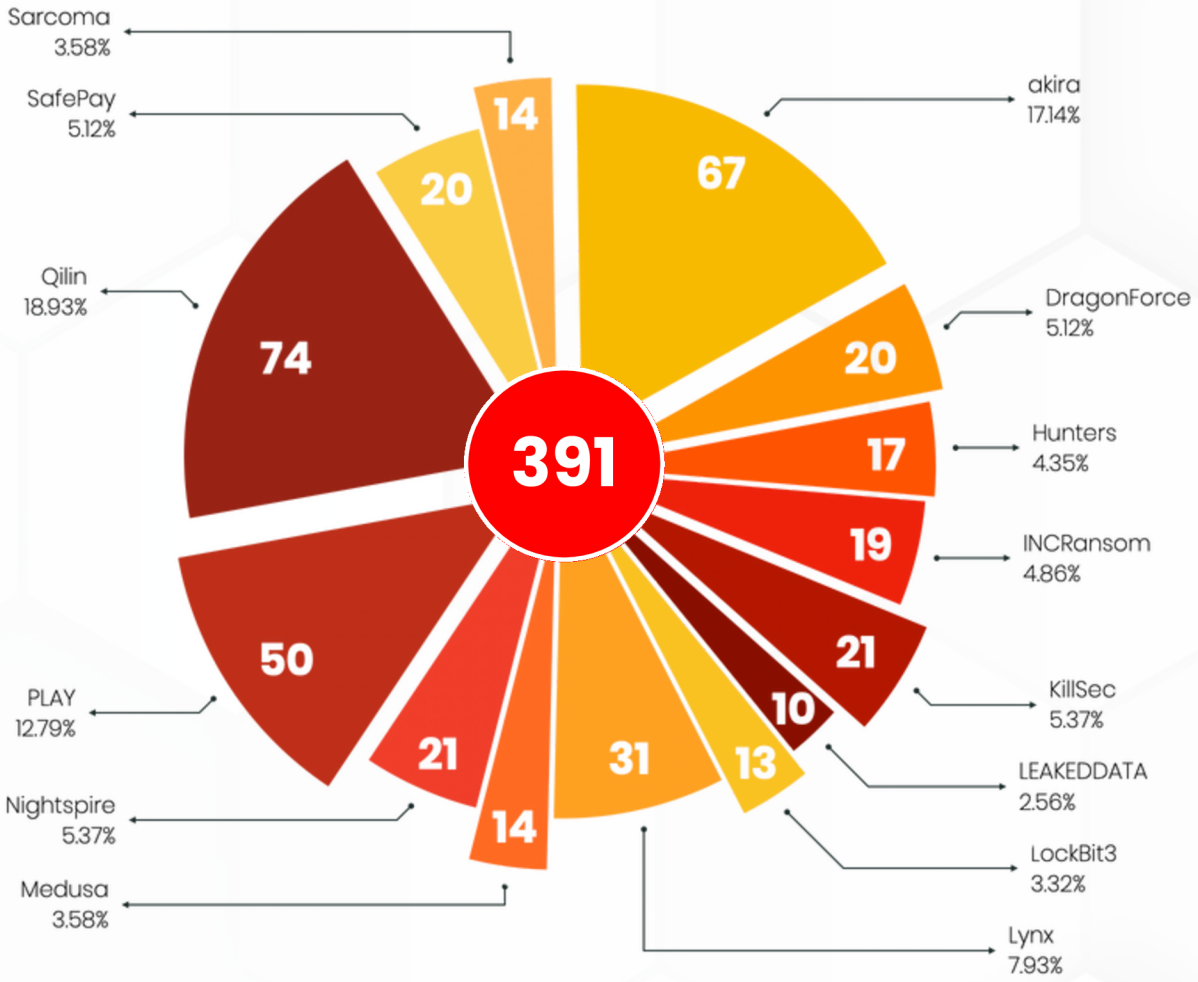
Distribuzione degli incidenti ransomware rilevati **per ciascun paese** membro, sulla base delle rivendicazioni confermate, a partire **dal 1° gennaio 2025,** per un totale di **401 attacchi.**

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



/breakdown_world

508 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 391 attacchi** (*elaborazione ransomNews*).



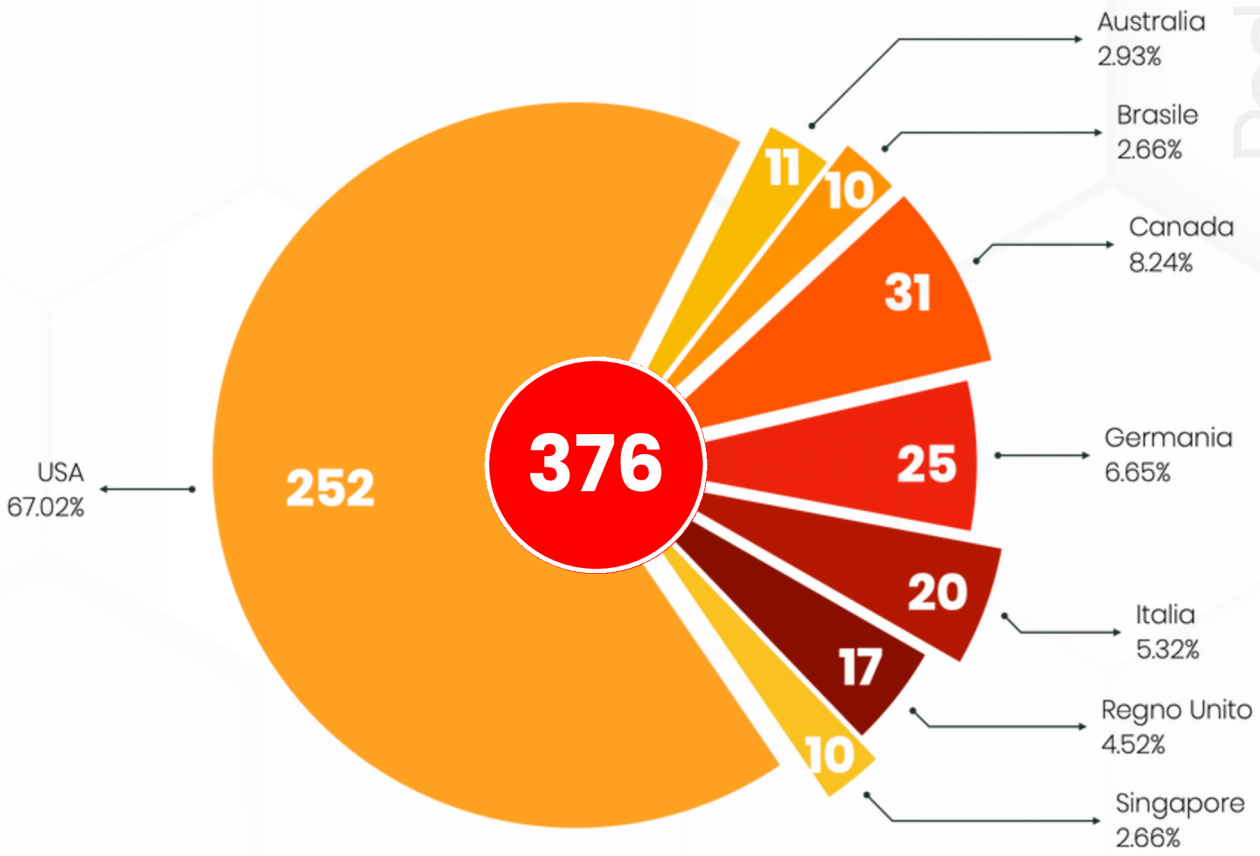
il **dataset** di aprile 2025, con **tutte le rivendicazioni** è disponibile **qui**: **https://rnws.online/YyZGM**

35 invece sono i gruppi che hanno rivendicato **meno di 10 attacchi**, per un totale complessivo di **117 rivendicazioni** (*fonti aggregate, elaborazione ransomNews*).

- Abyss, 1
- Anubis, 2
- BERT, 3
- Blacksuit, 3
- Brain Cipher, 1
- CHAOS, 4
- Cicada3301, 5
- CL0P^_, 1
- Cloak, 5
- Crypto24, 8
- Everest, 1
- Frag, 1
- FSociety FLocker, 1
- Gunra, 5
- HellCat, 6
- IMNCrew, 6
- InterLock, 7
- J Group, 3
- Kairos, 5
- Metaencryptor, 1
- MoneyMessage, 1
- Morpheus, 3
- Nitrogen, 4
- Nova, 1
- RALord, 9
- RansomHouse, 3
- RansomHub, 2
- Rhysida, 9
- Run Some Wares, 1
- Silent, 4
- Skira Team, 1
- Space Bears, 4
- Termite, 3
- Underground, 2
- VanHelsing, 1

/breakdown_world

Riportiamo nel grafico i paesi che, in questo mese, hanno subito **più di 10 attacchi**, su un totale di **58 paesi colpiti** (mondo e paesi NIS2). Si tratta di **8 paesi**, per complessive **376 rivendicazioni** (*fonti aggregate, **elaborazione ransomNews***).



Gli attacchi ai rimanenti **50 paesi** (mondo e paesi NIS2), per un totale generale di **132 rivendicazioni**, sono così suddivisi (*fonti aggregate, **elaborazione ransomNews***):

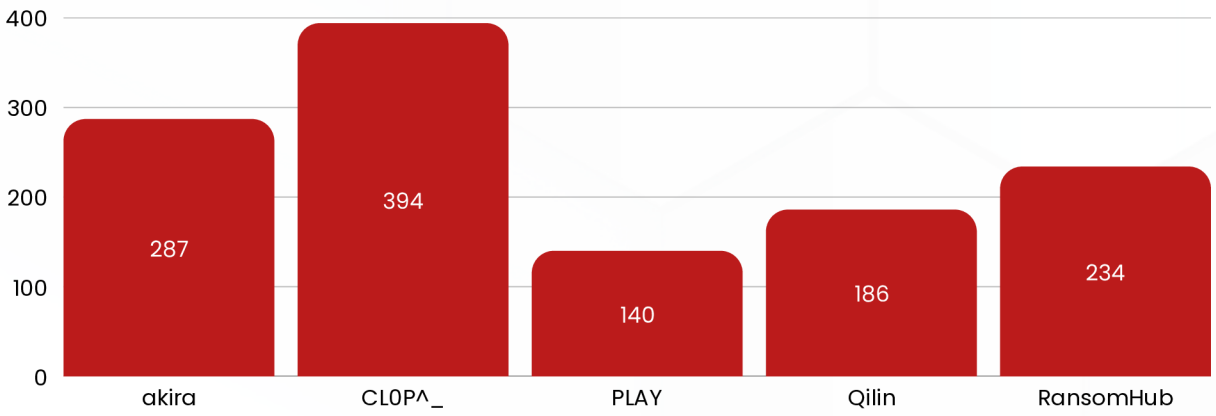
- Arabia Saudita, 3
- Argentina, 4
- Austria, 2
- Barhain, 1
- Barbados, 1
- Belgio, 4
- Bolivia, 1
- Cile, 3
- Cina, 3
- Cipro, 1
- Colombia, 1
- Corea del Sud, 1
- Costa Rica, 1
- Croazia, 1
- Egitto, 2
- Emirati Arabi, 2
- Estonia, 1
- Francia, 6
- Giamaica, 2
- Giappone, 4
- Giordania, 2
- Grecia, 3
- Irlanda, 2
- India, 6
- Indonesia, 3
- Lussemburgo, 3
- Malesia, 4
- Messico, 6
- Non Disponibile, 2
- Norvegia, 2
- Nuova Zelanda, 2
- Paesi Bassi, 3
- Pakistan, 1
- Panama, 1
- Perù, 2
- Polonia, 2
- Portogallo, 5
- Princ. Monaco, 1
- Rep. Ceca, 5
- Rep. Dominicana, 1
- Rep. Fiji, 1
- Spagna, 8
- Svezia, 3
- Svizzera, 7
- Tailandia, 1
- Taiwan, 7
- Tunisia, 1
- Turchia, 2
- Vietnam, 1
- 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 **2663 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, 287
Anubis, 7
Apos Security, 5
APT73 / BASHE, 12
Arcus, 19
Arkana, 2
BERT*, 3
BianLian, 35
Black Basta, 8
Blacklock, 6
Blackout, 1
Blacksuit, 5
Brain Cipher, 4
Cactus, 53
CHAOS, 8
Cicada3301, 21
CiphBit, 2
CL0P^_, 394
Cloak, 20
Crazyhunters, 10
Crypto24*, 8
DarkVault, 2
DragonForce, 55
Dunghill Leak, 1
EMBARGO, 6
Everest, 10
FOG, 90
Frag, 28
FSociety FLocker, 14
GD LockerSec, 5
Gunra*, 5
Handala, 4
HellCat, 12
Hunters, 42
IMNCrew*, 6
INCRansom, 90
InterLock, 14
J Group**, 13
Kairos, 20
KillSec, 69
Kraken, 7
LEAKEDDATA**, 37
Linkc, 1
LockBit3, 35
Lynx, 135
Medusa, 84
MedusaLocker, 4
Metaencryptor, 2
MoneyMessage, 2
MONTI, 15
Morpheus, 8
Nightspire, 39
Nitrogen, 6
Nova*, 1
Orca, 1
PLAY, 140
Qilin, 186
RALord, 14
RansomEXX, 3
RansomHouse, 9
RansomHub, 234
Rhysida, 33
Run Some Wares, 5
SafePay, 96
Sarcoma, 40
SECP0, 1
Silent*, 4
Skira Team, 5
Space Bears, 20
Stormous, 5
Termite, 13
ThreeAM, 14
Trinity, 7
Underground, 3
VanHelsing, 9
weyhro, 8



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

/breakdown_groups

Riportiamo di seguito la distribuzione degli attacchi per ogni paese colpito, **dal 1° gennaio 2025**, ad *esclusione dei paesi europei/NIS2*, per un **totale di 2262 attacchi** a **71 paesi** (*fonti aggregate, **elaborazione ransomNews***):

- Algeria, 1
- Arabia Saudita, 5
- Antigua, 1
- Argentina, 18
- Australia, 48
- Bahamas, 1
- Bahrain, 1
- Bangladesh, 1
- Barbados, 1
- Bielorussia, 1
- Bolivia, 1
- Botswana, 1
- Brasile, 46
- Canada, 168
- Cile, 10
- Cina, 13
- Colombia, 12
- Corea del Sud, 4
- Costa Rica, 2
- Ecuador, 3
- Egitto, 9
- El Salvador, 2
- Emirati Arabi, 6
- Filippine, 2
- Georgia, 1
- Ghana, 1
- Giamaica, 7
- Giappone, 21
- Giordania, 2
- Haiti, 1
- Hong Kong, 5
- India, 38
- Indonesia, 12
- Iraq, 1
- Israele, 5
- Kenia, 1
- Laos, 1
- Malesia, 12
- Marocco, 2
- Messico, 27
- Namibia, 1
- Nigeria, 4
- Non Disponibile, 12
- Norvegia, 7
- Nuova Zelanda, 8
- Oman, 1
- Pakistan, 6
- Panama, 3
- Perù, 7
- Portorico, 4
- Prin. Monaco, 2
- Regno Unito, 92
- Rep. Dominicana, 5
- Rep. Fiji, 1
- Rep. Kiribati, 1
- Rep. Palau, 1
- Singapore, 24
- Sud Africa, 4
- Sri Lanka, 1
- Svizzera, 22
- Tailandia, 11
- Taiwan, 31
- Tanzania, 2
- Tunisia, 2
- Turchia, 8
- Ucraina, 1
- Uruguay, 2
- USA, 1498
- Venezuela, 1
- Vietnam, 5
- Zambia, 1

/breakdown_groups_new

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

- **BERT** - si è imposto come threat actor cross-platform grazie all'uso di **payload in ELF** per ambienti Linux, oltre a Windows; si distinguono per un uso avanzato di **tecniche anti-forensics** e payload personalizzati per ogni obiettivo.
- **Crypto24** - si riscontrano molte similitudini con altri threat actors come LockBit2 e LockBit3, ma con un focus più ampio sui **target asiatici**.
- **Gunra** - gruppo ransomware che sfrutta **tecniche anti-analisi** avanzate, con focus su sanità e ambiti ad alta esposizione mediatica; utilizza **codice offuscato** e protezione attiva contro strumenti forensi.
- **IMNCrew** - compare sulla scena alla fine di Marzo 2025 come semplice data broker ma si è evoluto rapidamente in operatore ransomware. Fa massiccio utilizzo di **script PowerShell veicolati tramite GPO** per la raccolta credenziali da browser e scansione della rete.
- **J Group** - costituito nel febbraio 2025, è un **data broker puro** che sfrutta strategie mirate verso settori IT e software house.
- **LEAKEDDATA** - gruppo che ha diviso i ricercatori, su vari livelli: spesso non esegue alcun tipo di crittografia, predilige esclusivamente l'esfiltrazione dei dati; si concentra su studi legali, assicurazioni e sanità con campagne di **callback phishing** e **vishing** per **installare RAT** su macchine target. Viene spesso associato al gruppo Silent per molte similitudini.

- **NOVA** - si tratta del **rebrand di RALord**, a sua volta rebrand di RaWorld.
- **Silent** - noto anche come **Luna Moth, Chatty Spider, UNC3753**, è attivo sin dal 2022, ma ha avuto una forte ripresa nel 2025 con campagne ad alto impatto di **social engineering avanzata** con contatti via telefono, simulazioni di help desk e induzione all'installazione di tool come Zoho Assist o AnyDesk.

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

****** gruppi emersi pubblicamente nel mese di **Maggio 2025**, tuttavia le rivendicazioni sono **documentate e attribuibili** al mese corrente

/DPO_commentary

I dati del mese non sono eclatanti, ma terrorizza il fatto che sia un **bollettino di guerra che si ripete senza tregua**.
La lotta sembra impari ed emergono **due tendenze opposte** che, in prospettiva, lasciano intravedere un peggioramento nei numeri:

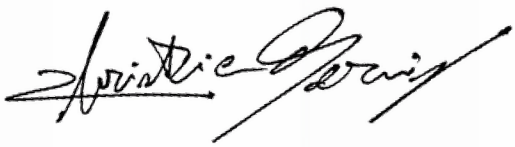
- I criminali informatici stanno **aumentando in numero** e stanno crescendo le loro capacità.
- Le vittime più numerose appartengono a **comparti con una minore maturità dei sistemi** di protezione: l'industria.

Le attività estorsive, tipiche del ransomware, sono molto remunerative e questo **attira persone competenti**, permette di migliorare le tecnologie utilizzate, aiuta a progettare attacchi complessi, sofisticati che richiedono tempo e risorse. Il nemico si rafforza ogni giorno e diventa sempre più aggressivo: non sono più script kiddie.

L'utilizzo delle **tecnologie basate su intelligenza artificiale** fa intravedere scenari direttamente connessi all'evoluzione di questi strumenti. Per difendersi è necessario far evolvere di pari passo sia le tecnologie che, soprattutto, le abilità delle persone nel riconoscere attività malevole.

L'industria è tradizionalmente **poco sviluppata** sotto il profilo della sicurezza informatica rispetto a settori con più alto contenuto tecnologico e, anche per questo, è il bersaglio ideale. Le data company devono proteggersi efficacemente sia per legge che per **tutelare il proprio know-how**.

L'industria tradizionale non è obbligata dalla legge a proteggere dati operativi (che non hanno natura personale). Tuttavia, **se i sistemi vengono violati**, possono comportare **gravi e prolungati blocchi** sia delle attività che delle filiere produttive.



/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.***