RedACT

RANSOMNEWS DISCLOSURE & ACTIVITY TRACKING

REPORT MENSILE
GIUGNO 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**@**ransomnews.online

/use_conditions

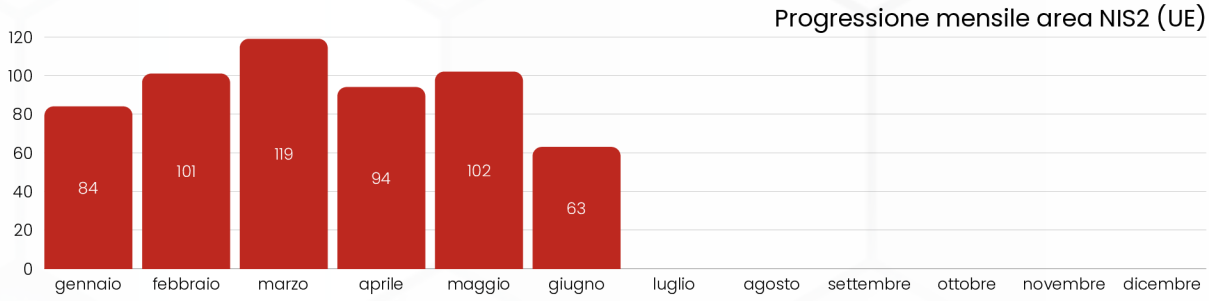
/executive_summary

Nel mese di **giugno 2025** sono state registrate **482 rivendicazioni** a livello globale.

HIGHLIGHTS

- **Italia**: rilevati **11 attacchi**, con **619.90GB** di dati pubblicati. La regione **Lombardia**, di nuovo, si assesta al primo posto con una netta maggioranza di vittime. I settori più colpiti sono la **manifattura** di genere, la **consulenza** e la **sanità**.
- **Area NIS2** (UE): **63 attacchi** rilevati. I tre paesi più colpiti sono **Germania**, **Spagna** e **Italia**.
- **Globale**: i gruppi più attivi del mese sono **Qilin**, **PLAY** e **akira**.

Progressione mensile area NIS2 (UE)



TREND TECNICI

- **Tecnica di accesso dominante**: *phishing* mirato e *credential stealing*
- **Evoluzione**: uso di GenAI, malware FakeUpdate
- **Vettori persistenti:** servizi esposti, riutilizzo di credenziali, vulnerabilità note

ANALISI DI CONTESTO

Il **phishing BEC** mantiene un ritmo costante: *email spoofing* e *typosquatting* colpiscono in particolare **istituti bancari** e grandi **aziende di consulenza**, sfruttando lacune persistenti nell'implementazione di SPF/DKIM/DMARC e scarsa formazione degli utenti.

RISK ASSESSMENT

Gli incidenti registrati, a livello globale, mostrano una chiara polarizzazione: attacchi ad alto impatto nel **sanitario** e attacchi più diffusi ma a impatto medio in ambito **bancario** e **manifatturiero**.

EVENTO	TTPs	SETTORE	RISCHIO	IMPATTO
Phishing BEC	email spoofing, credential theft	bancario	medio	alto
Stealer-as-a-Service	loader, infostealer (Redline, Raccoon)	PMI/manifattura	alto	medio
DDoS mirati	Botnet-as-a-Service (IoT)	PA	basso	medio

/breakdown_italy

Si sono registrati, per questo mese, **11 attacchi**, con una netta predominanza nell'area geografica del **Nord Italia** (ben 8 attacchi).

Segue il **Centro Italia** con 3 attacchi; **Sud Italia** e **isole** non registrano, questo mese, alcun attacco (*fonti aggregate, elaborazione ransomNews*).

attacchi registrati

11

area geografica

nord

dati pubblicati

619.90GB

settore principale

consulenza

Tabella riepilogativa delle **rivendicazioni confermate** su territorio italiano nel mese di giugno 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
PPM Industries SPA	Sarcoma	Brembate di Sopra (BG)	228.00	-
RECYCLA SPA	akira	Maniago (PN)	0.00	5
Farmacisti Più Rinaldi SPA	akira	Udine	15.00	-
Girva International Broker SRL	Qilin	Milano	0.00	5
Dugoni Facility Management SCRL	Qilin	Mantova	0.00	5
BioAlleva SRL	Qilin	Vallese di Oppeano (VR)	0.00	5
Susta SRL	Qilin	Castellalto (TE)	300.00	-
Fratellanza Popolare Valle del Mugnone	Qilin	Caldine (FI)	0.00	5
Studio Verna Società Professionale	akira	Roma	6.50	-
Tiscali SPA (Tessellis SPA / Dr. Montagna)	WorldLeaks	Brescia	58.40	-
Meleam SPA	akira	Roma	12.00	-

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

👉 i dati pubblicati nella rivendicazione **Tiscali SPA** sono in realtà appartenenti all'attività di Dr. Montagna.

/breakdown_italy

Nel primo semestre 2025, il volume di dati esfiltrati e pubblicati da gruppi ransomware in Italia ha raggiunto **13241.39 GB**, distribuiti su sei mesi di attività documentata.

Trend generale:

- **gennaio** si apre con un picco anomalo (oltre 5 TB), segno di backlog o pubblicazioni cumulative di fine 2024
- **febbraio** segna un forte calo, con valori ridotti di oltre il 70%
- **marzo** e **aprile** mostrano una ripresa, anche se meno esplosiva, indicando che attori quali akira, Hunters e PLAY, hanno mantenuto una costanza di operazioni
- **maggio** e **giugno** riportano un ulteriore declino, stabilizzando l'attività su volumi inferiori a 1 TB/mese - una fase di apparente "*quiet period*" dopo ondate intense di leak

Questo andamento suggerisce un raffreddamento della scena italiana dopo i primi mesi dell'anno, probabilmente dovuto a:

- maggiore pressione investigativa (operazioni *Endgame*, *Duck Hunt*)
- rotazione o dissoluzione di gruppi attivi nel Q1
- saturazione dei target medio-piccoli
- una transizione verso campagne meno eclatanti ma più mirate

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	619.90	▼	
Luglio			
Agosto			
Settembre			
Ottobre			
Novembre			
Dicembre			

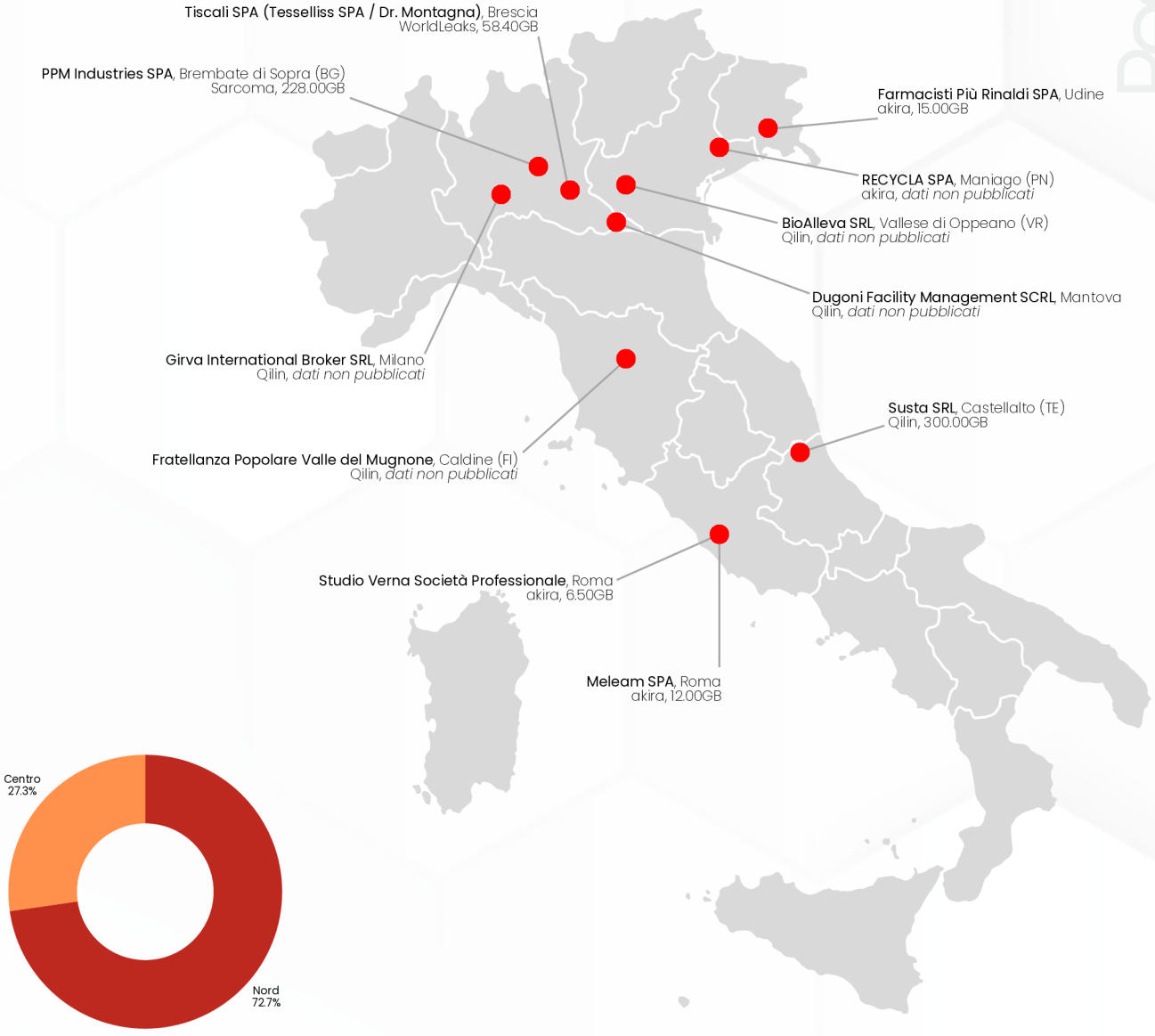
Totale generale dati esfiltrati dichiarati e pubblicati, in Italia: **13241.39 GB**

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 totalizza 5 attacchi.

Seguono Friuli Venezia Giulia, Veneto, Abruzzo, Toscana e Lazio.

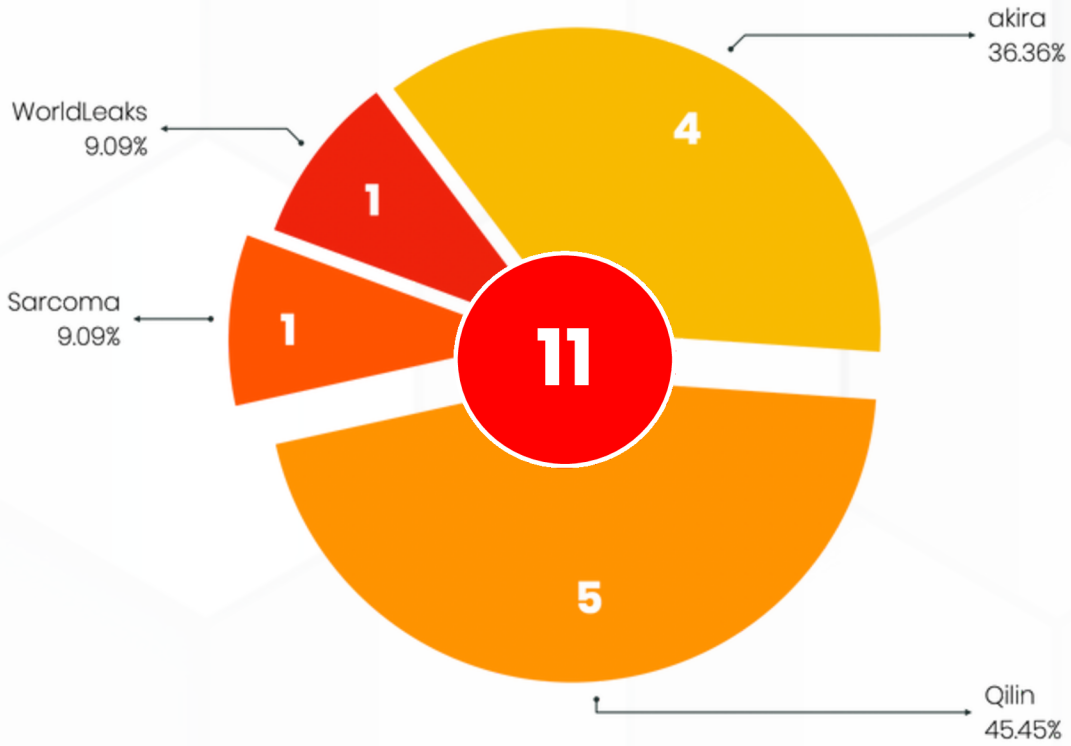
Dati esfiltrati

Il volume dei dati pubblicati per la regione Lombardia ammonta a **307.90GB**.

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

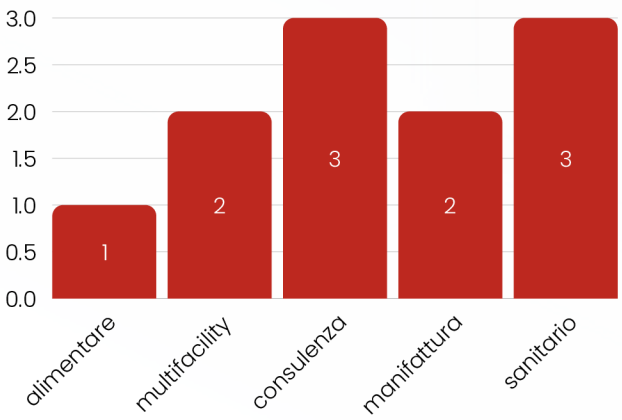
/breakdown_italy_groups

Sono **4 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 **giugno**, in Italia, gli attacchi hanno interessato i seguenti settori:



La pressione sugli ecosistemi industriali del **Nord Italia** si è ulteriormente intensificata a giugno, con attacchi che colpiscono in particolare le **filiere manifatturiere** e logistiche, dove l'elevata interconnessione digitale continua a rappresentare un punto di debolezza.

Le **intrusioni iniziali** restano legate in gran parte a **servizi esposti** e a **credenziali sottratte** tramite campagne di **phishing mirato**; tuttavia, cresce l'uso di **accessi RDP** e **VPN** rivenduti nei marketplace underground.

Si registra **un'accelerazione** nell'impiego di strumenti basati su **intelligenza artificiale generativa**, sfruttati per rendere più convincenti le campagne di *social engineering*, simulare in modo credibile identità digitali e aumentare, in maniera esponenziale, la probabilità di successo delle compromissioni.

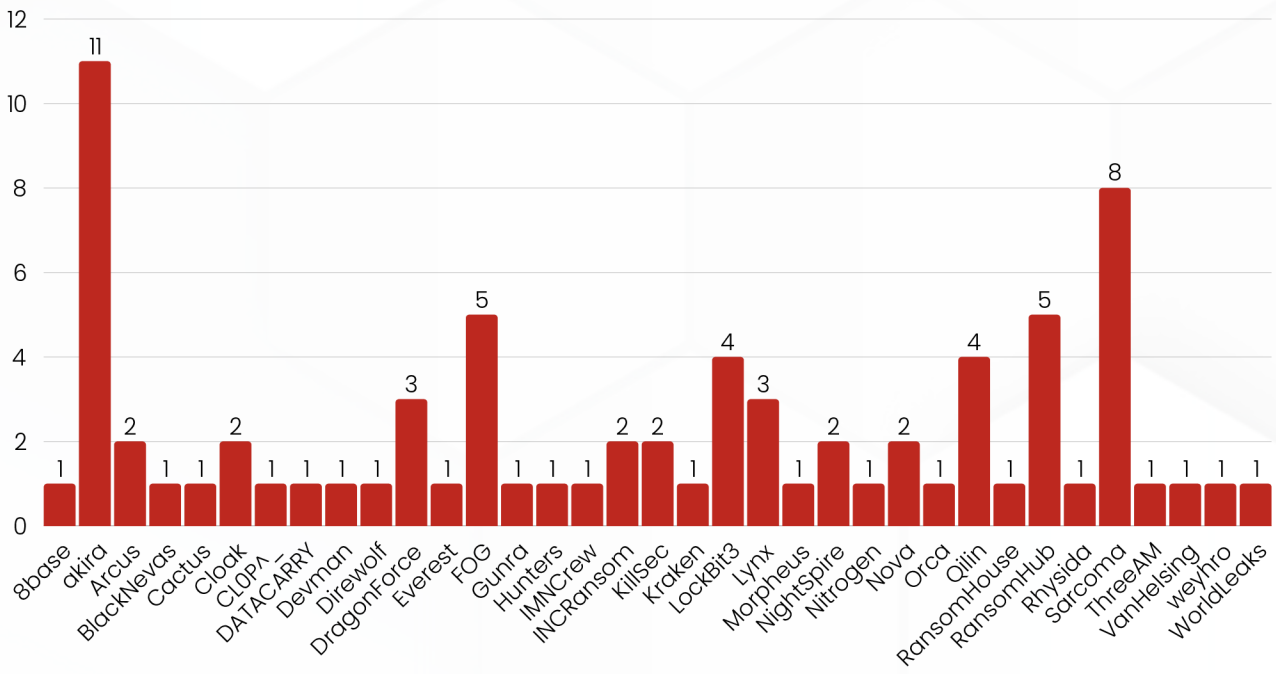
/breakdown_italy_groups

Nella tabella, il numero delle **vittime italiane** accertate per ogni gruppo, a partire **dal 1° gennaio 2025**, per un totale di **86 rivendicazioni** divise fra **35 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	Direwolf, 1	Kraken, 1	RansomHouse, 1
akira, 15	DragonForce, 3	LockBit3, 4	RansomHub, 5
Arcus, 2	Everest, 1	Lynx, 3	Rhysida, 1
BlackNevas*, 1	FOG, 5	Morpheus, 1	Sarcoma, 9
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	WorldLeaks, 1
Devman, 1	KillSec, 2	Qilin, 9	

Rispetto al **primo semestre** del **2024**, si registra un incremento degli attacchi: **+16 rivendicazioni**, corrispondenti ad un **incremento del +22.86%.**



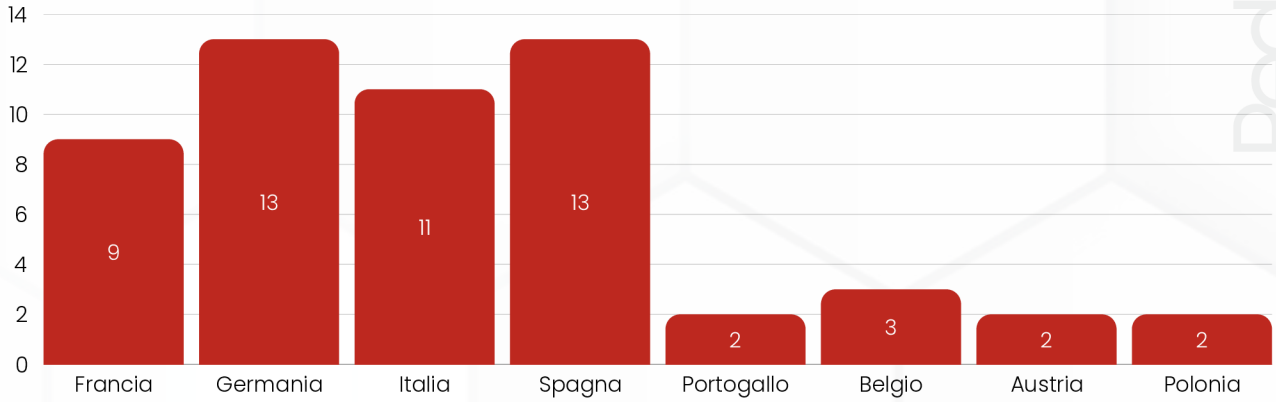
📌 **akira** - il gruppo, emerso nel 2023, si è rapidamente imposto con un modello RaaS colpendo soprattutto i settori **sanitario** e **industriale**. Le sue intrusioni iniziano spesso **tramite phishing mirato** o **sfruttando vulnerabilità in VPN e RDP**, seguite da movimento laterale con strumenti come PsExec e WMI.

L'analisi OSINT e SOCMINT condotta da ransomNews mostra come akira **non sia legato a grandi cartelli** come Conti o REvil, ma si muova in un ecosistema criminale interconnesso, con scambi di exploit e tool sui forum underground e un uso regolare di **RAT** (Remcos, NanoCore), **Mimikatz** e **Rclone**.

Questo contenuto esclusivo è disponibile solo sul nostro sito, nella sezione **HUB**.

/breakdown_europe_nis2

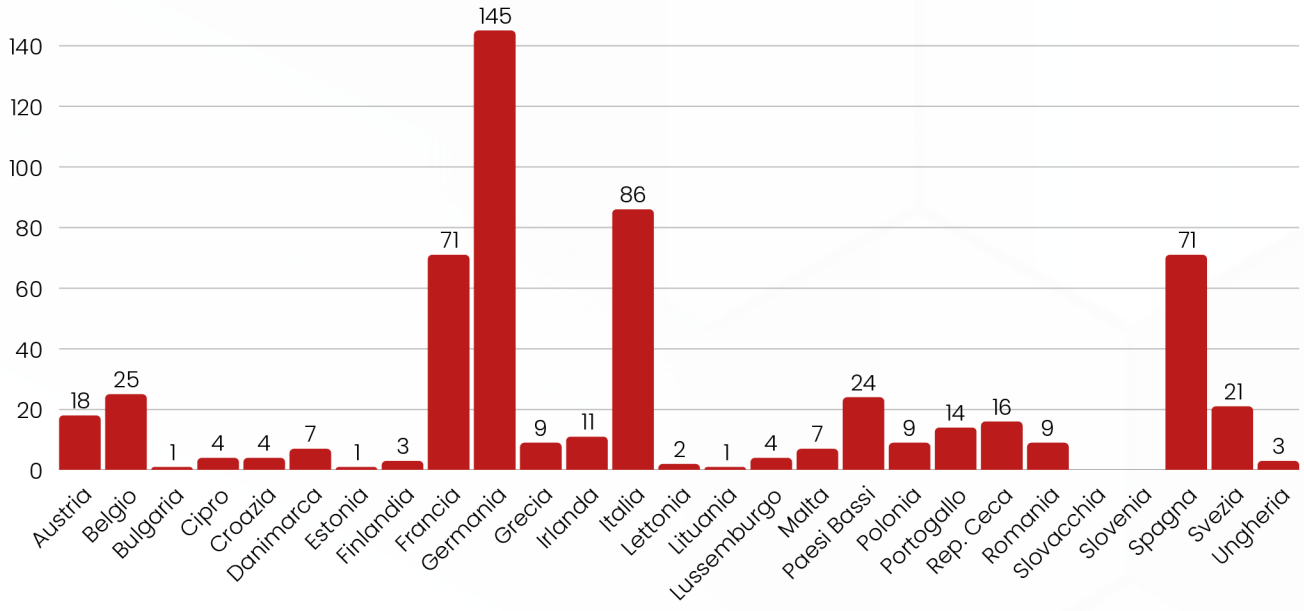
Nel mese di **giugno 2025**, i Paesi UE che adottano le normative della **Direttiva NIS2** hanno subito un totale di **63 attacchi**.
I più colpiti sono stati **Germania**, **Spagna** e **Italia** (*fonti aggregate, **elaborazione ransomNews***).



- Austria, 2
- Belgio, 3
- Bulgaria, 0
- Cipro, 0
- Croazia, 1
- Danimarca, 2
- Estonia, 0
- Finlandia, 0
- Francia, 9
- Germania, 13
- Grecia, 1
- Irlanda, 1
- Italia, 11
- Lettonia, 1
- Lituania, 0
- Lussemburgo, 0
- Malta, 0
- Paesi Bassi, 1
- Polonia, 2
- Portogallo, 2
- Rep. Ceca, 0
- Romania, 0
- Slovacchia, 0
- Slovenia, 0
- Spagna, 13
- Svezia, 1
- 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 **566 attacchi** *

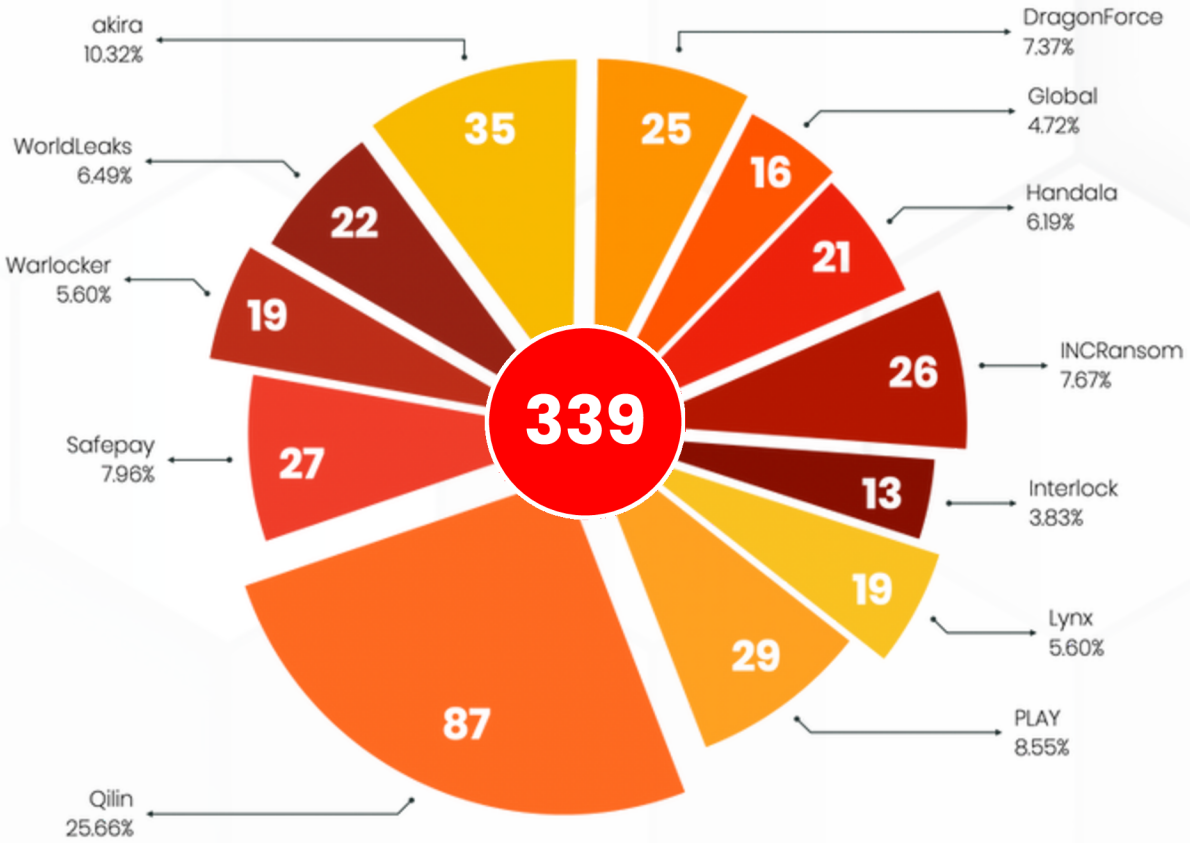
L'obiettivo è evidenziare il livello di esposizione delle nazioni coinvolte nel nuovo quadro normativo europeo.



/breakdown_world

482 sono le **rivendicazioni tracciate**, da fonti aggregate, per il mese corrente (comprensive di NIS2).

Nel grafico sono riportati i gruppi che hanno totalizzato **più di 10 attacchi**: **12 gruppi**, per un **totale di 339 attacchi** (*elaborazione ransomNews*).



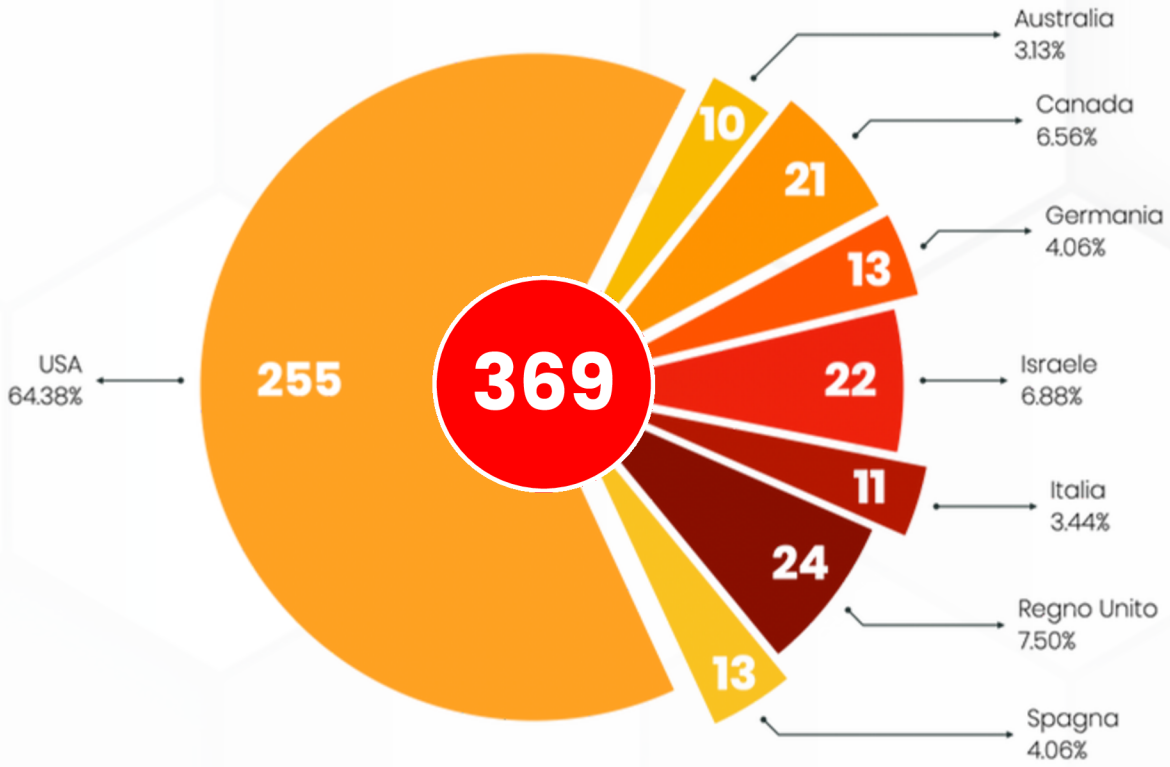
il **dataset** di giugno 2025, con tutte le rivendicazioni è disponibile su **ransomnews.online**

40 invece sono i gruppi che hanno rivendicato **meno di 10 attacchi**, per un totale complessivo di **143 rivendicazioni** (*fonti aggregate, elaborazione ransomNews*).

Anubis, 2
Apos, 2
Arkana, 2
BERT, 2
Blacklock, 8
BlackNevas, 2
Blacksuit, 1
CHAOS, 3
CL0P^_, 1
Cloak, 1
Crypto24, 5
DataCarry, 2
Direwolf, 8
EMBARGO, 2
Everest, 6
FRAG, 2
FSociety FLocker, 3
Gunra, 4
Hellcat, 2
IMNCrew, 1
J Group, 5
Kairos, 6
Kawa4096, 2
KillSec, 2
Kraken, 8
Medusa, 7
Metaencryptor, 2
Nightspire, 9
Nova, 4
PEAR, 6
RansomHouse, 2
Rhysida, 4
Sarcoma, 7
Silent, 1
SpaceBears, 3
Stormous, 4
TeamXXX, 8
ThreeAM, 2
Underground, 1
VALocker, 1

/breakdown_world

Nel grafico sono evidenziati gli **8 paesi** che, nel mese, hanno registrato **più di 10 attacchi**. Su un totale di **57 nazioni** colpite (inclusi i paesi NIS2), queste rappresentano **369 rivendicazioni** complessive (*fonti aggregate, **elaborazione ransomNews***).



Gli attacchi ai rimanenti **49 paesi** (mondo e paesi NIS2), per un totale generale di **113 rivendicazioni**, sono così suddivisi (*fonti aggregate, **elaborazione ransomNews***):

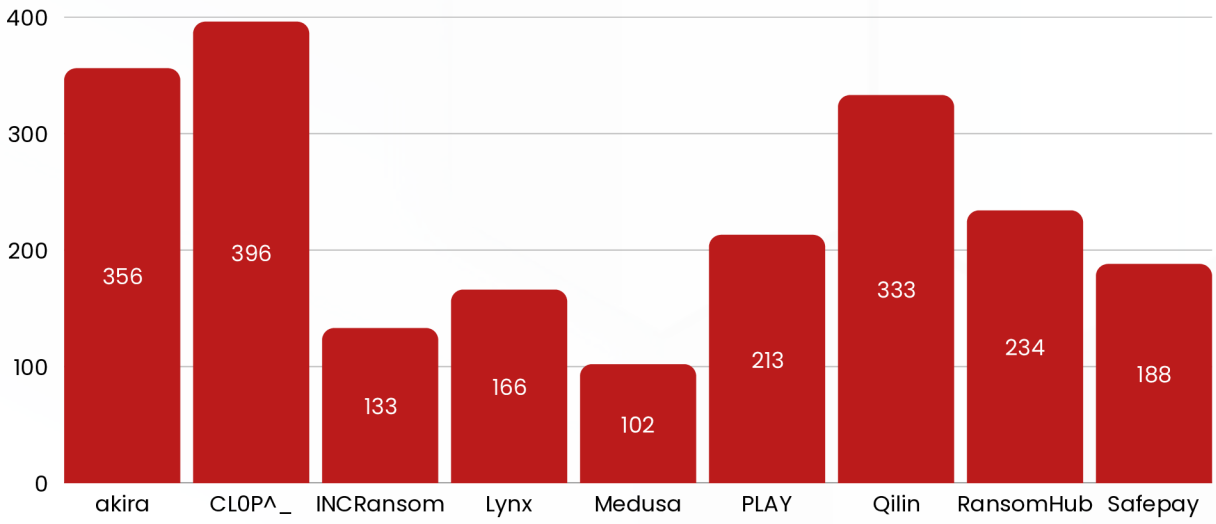
- Argentina, 3
- Austria, 2
- Azerbaijan, 1
- Bangladesh, 1
- Belgio, 3
- Brasile, 8
- Cambogia, 1
- Cile, 2
- Colombia, 5
- Corea del Sud, 1
- Croazia, 1
- Danimarca, 2
- Ecuador, 1
- Emirati Arabi, 3
- Filippine, 1
- Francia, 9
- Giappone, 1
- Haiti, 1
- Hong Kong, 2
- Grecia, 1
- India, 7
- Irlanda, 1
- Kuwait, 1
- Lettonia, 1
- Malesia, 1
- Marocco, 1
- Messico, 3
- Non Disponibile, 2
- Norvegia, 2
- Nuova Zelanda, 1
- Paesi Bassi, 1
- Panama, 1
- Perù, 4
- Polonia, 2
- Portogallo, 2
- Portorico, 1
- Regno di Tonga, 1
- Rep. Fiji, 1
- Rep. Mauritius, 1
- Rep. Dominicana, 1
- Serbia, 1
- Singapore, 4
- Sud Africa, 2
- Svezia, 1
- Svizzera, 4
- Tailandia, 6
- Taiwan, 4
- Turchia, 5
- 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 **3591 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, 356
Anubis, 9
Apos, 10
APT73 / BASHE, 12
Arcus, 27
Arkana, 6
BERT, 7
BianLian, 35
Black Basta, 8
Blacklock, 20
BlackNevas, 7
Blackout, 1
Blacksuit, 9
Brain Cipher, 10
Cactus, 53
CHAOS, 12
Cicada3301, 21
CiphBit, 3
CL0P^_, 396
Cloak, 23
Crazyhunters, 10
Crypto24, 15
DarkVault, 2
DataCarry, 11
Devman, 1
Direwolf, 16
DragonForce, 82
Dunghill Leak, 1
EMBARGO, 11
Everest, 25
FOG, 90
Frag, 30
FSociety FLocker, 18
GD LockerSec, 5
Global, 16
Gunra, 15
Handala, 25
HellCat, 14
Hunters, 47
IMNCrew, 9
INCRansom, 133
InterLock, 33
J Group, 23
Kairos, 29
Kawa4096, 2
KillSec, 76
Kraken, 17
LEAKEDDATA, 37
Linkc, 1
LockBit3, 40
Lynx, 166
Medusa, 102
MedusaLocker, 6
Metaencryptor, 4
MoneyMessage, 2
MONTI, 17
Morpheus, 9
Nightspire, 64
Nitrogen, 7
Nova, 10
Orca, 2
PEAR, 6
PLAY, 213
Qilin, 333
RALord, 14
RansomEXX, 3
RansomHouse, 16
RansomHub, 234
Rhysida, 46
Run Some Wares, 5
SafePay, 188
Sarcoma, 60
SECP0, 1
Silent, 6
Skira Team, 6
SpaceBears, 28
Stormous, 21
TeamXXX, 8
Termite, 14
ThreeAM, 17
Trinity, 7
Underground, 4
VanHelsing, 9
VA Locker, 1
Warlocker, 19
weyhro, 12
WorldLeaks, 31



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

/breakdown_attacks

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 3025 attacchi** a **81 paesi** (*fonti aggregate, **elaborazione ransomNews***):

- Algeria, 1
- Antigua Barbuda, 1
- Arabia Saudita, 7
- Argentina, 22
- Australia, 64
- Azerbaijan, 1
- Bahamas, 1
- Bahrain, 2
- Bangladesh, 2
- Barbados, 2
- Bielorussia, 1
- Bolivia, 1
- Bosnia Herzegovina, 1
- Botswana, 2
- Brasile, 62
- Cambogia, 1
- Camerun, 1
- Canada, 218
- Cile, 12
- Cina, 14
- Colombia, 20
- Corea del Sud, 6
- Costa Rica, 2
- Ecuador, 5
- Egitto, 10
- El Salvador, 3
- Emirati Arabi, 15
- Filippine, 6
- Georgia, 1
- Ghana, 1
- Giamaica, 7
- Giappone, 30
- Giordania, 2
- Haiti, 2
- Hong Kong, 7
- India, 48
- Indonesia, 13
- Iraq, 1
- Israele, 27
- Kenia, 1
- Kuwait, 1
- Laos, 1
- Libano, 1
- Malesia, 16
- Marocco, 3
- Messico, 31
- Namibia, 1
- Nigeria, 4
- Non Disponibile, 14
- Norvegia, 12
- Nuova Zelanda, 9
- Oman, 1
- Pakistan, 6
- Panama, 4
- Perù, 12
- Portorico, 5
- Prin. Monaco, 2
- Regno di Tonga, 1
- Regno Unito, 132
- Rep. Dominicana, 7
- Rep. Fiji, 2
- Rep. Kiribati, 1
- Rep. Maldive, 1
- Rep. Mauritius, 1
- Rep. Palau, 1
- Serbia, 2
- Singapore, 34
- Sud Africa, 9
- Sri Lanka, 3
- Svizzera, 31
- Tailandia, 19
- Taiwan, 38
- Tanzania, 2
- Tunisia, 2
- Turchia, 17
- Ucraina, 1
- Uruguay, 2
- USA, 1960
- Venezuela, 5
- Vietnam, 7
- Zambia, 1

/breakdown_groups_new

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

- **Global** - colpisce settori come consumer services, sanità, trasporti e business services, con impatto distribuito su scala mondiale.
  Caratteristiche operative: doppia estorsione, brokeraggio.
  Tattiche note: phishing, uso di infostealer, cancellazione di shadow copy.
  Tecnologie: phishing con domini riseup.

- **Kawa4096** - target variegati, colpisce settori come sanità, servizi finanziari, settore pubblico.
  Caratteristiche operative: criptazione multithread e attacchi network share.
  Tattiche note: cifratura, finestra di pagamento definita.
  Tecnologie: usa configurazioni embeddate e multithreading per efficienza.

- **PEAR** - colpisce servizi IT, pubblica amministrazione, healthcare, manufacturing.
  Caratteristiche operative: modello data broker senza cifratura.
  Tattiche note: estrazione silente dei dati; doppi attacchi.
  Tecnologie: leak site generico.

- **Satanlock** - breve carriera, ha compromesso circa 67organizzazioni..
  Caratteristiche operative: doppia estrazione.
  Tattiche note: violazioni senza encryption.
  Tecnologie: non dettagliate pubblicamente.

- **TeamXXX** - non ci sono dettagli tecnici specifici disponibili.
  Caratteristiche operative: non note al momento.
  Tattiche note: non note al momento.
  Tecnologie: non note al momento.

- **V.A. Locker/VA Locker** - attualmente pochi dettagli disponibili.
  Caratteristiche operative: attività sostenuta, impatto medio.
  Tattiche note: non note al momento.
  Tecnologie: non note al momento.

- **Warlock (Warlocker)** - targeting di IT, telecom, finanza, agricoltura.
  Caratteristiche operative: modello RaaS con affiliati, sfrutta exploit SharePoint.
  Tattiche note: exploit 0day SharePoint, ToolShell, PsExec/Mimikatz.
  Tecnologie: payload AK47 C2 framework (DNS e HTTP variant).

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

/DPO_commentary

Il malware è **opportunista**: teoricamente qualsiasi sistema informatico può essere compromesso, ma le azioni malevole si concentrano su bersagli vulnerabili per ottenere il massimo risultato con il minimo sforzo.

L'analisi dell'andamento degli eventi registrati permette di disegnare una mappa dei settori o degli ecosistemi più vulnerabili e, quindi, più colpiti.
L'**Italia spicca nella classifica**, specialmente leggendo i numeri alla luce della sua rilevanza economica o parametrando le cifre rispetto ad altri indicatori.

La stessa logica può essere applicata ai settori coinvolti: i più colpiti dimostrano **scarsa maturità** e, di conseguenza, **minor resistenza agli attacchi**.

Colpisce la presenza costante e significativa di **aziende di consulenza** e **servizi** che, quando vengono compromesse da *malware*, moltiplicano l'impatto e le conseguenze per il numero dei soggetti di cui trattano dati, i loro clienti, generando un numero di data breach impressionante.

/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.***