RedACT

RANSOMNEWS DISCLOSURE & ACTIVITY TRACKING

REPORT MENSILE
MARZO 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

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

/use_conditions

/executive_summary

Nel mese di marzo sono state registrate **648 rivendicazioni** a livello globale.

HIGHLIGHTS

- **Italia**: 19 attacchi confermati, con **2553.90GB** di dati pubblicati. Il **Veneto** si conferma la regione più colpita, con una netta prevalenza del settore **terziario/IT**.
- **Area NIS2** (UE): **119 attacchi** rilevati. I tre paesi più colpiti sono Germania (39), Francia (16) e Italia (19).
- **Globale**: i gruppi più attivi sono **RansomHub**, **akira** e **FOG**. Nuovi attori come Frag, Crazyhunters e SECP0 introducono tecniche avanzate e modelli operativi non convenzionali.

TREND TECNICI

- **Tecnica di accesso dominante**: phishing mirato con allegati malevoli
- **Evoluzione**: uso crescente di strumenti AI per migliorare il social engineering
- **Vettori persistenti:** servizi esposti, credenziali compromesse, supply chain

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. La frammentazione dei threat actors rende la prevenzione più complessa.

dati pubblicati
vs febbraio
+63.5%

phishing e
vulnerabilità
ancora
dominanti

gruppi emergenti
in attività da marzo
9

/breakdown_italy

La distribuzione geografica mostra una netta **concentrazione nelle regioni del Nord Italia**, con **13 attacchi**; segue il **Centro con 5 attacchi**, poi **Sud e Isole** con **nessun attacco** (*fonti aggregate, **elaborazione ransomNews***) - nel conteggio viene esclusa la rivendicazione "senza nome".

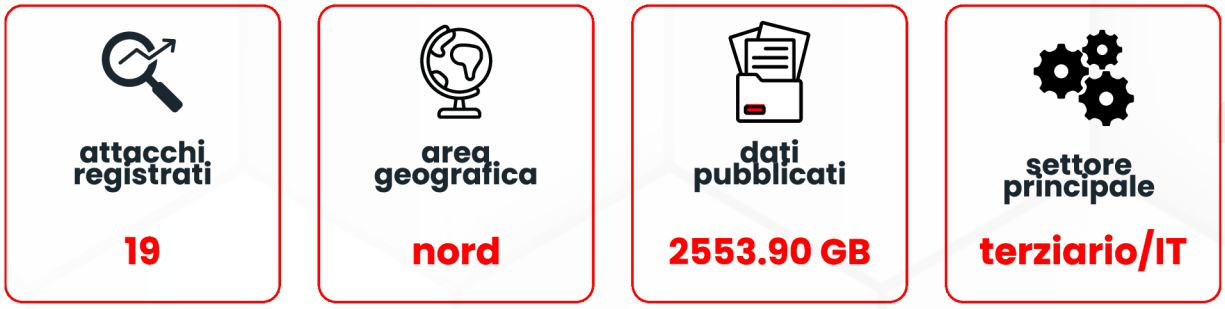


Tabella riepilogativa delle **rivendicazioni confermate** su territorio italiano nel mese di riferimento.
I dati includono il nome della vittima, il gruppo autore, la localizzazione geografica, la quantità dei **dati pubblicati** (come dichiarato dall'attaccante) e le note a riguardo.

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

VITTIMA	GRUPPO	LOCALIZZAZIONE	DATI	NOTE
Cogesi SRL	LockBit3	Guidonia Montecelio (RM)	272.90 GB	-
Fantin Group SRL	akira	Istrana (TV)	-	5
piùadrenalina SG&B SRL	akira	Cairano S. Marco (TV)	-	5
Bizcode SRL	FOG	Acquafredda (BS)	54.50 GB	-
Engicam SRL	FOG	Scandicci (FI)	59.00 GB	-
Fragola SPA	weyhro	Assisi (PG)	-	1
Sirius SRL	Nitrogen	Torino	542.00 GB	-
target senza nome	Sarcoma	-	-	3
Trycon SRL	Lynx	Dueville (VC)	8.00 GB	-
Casale del Giglio SA SRL	Orca	Le Ferriere (LT)	253.00 GB	-
MESS Sales SRL	Sarcoma	Genova	36.00 GB	-

[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
Terre Cortesi Moncaro SC	DragonForce	Montecarotto (AN)	193.50 GB	-
Exemplar SRL	RansomHub	Torino	846.00 GB	-
Studio Vallone	VanHelsing	Monza (MB)	-	5
SolidWorld Group SPA	RansomHub	Treviso	103.00 GB	-
Bio-Clima SRL	LockBit3	Bernareggio (MB)	-	5
Bassi Gianfranco SRL	RansomHub	Mirandola (MO)	-	3
Geass SRL	Sarcoma	Pozzuolo del Friuli (UD)	156.00 GB	-
Omci SPA	Nightspire	Castelfranco Emilia (MO)	30.00 GB	-

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

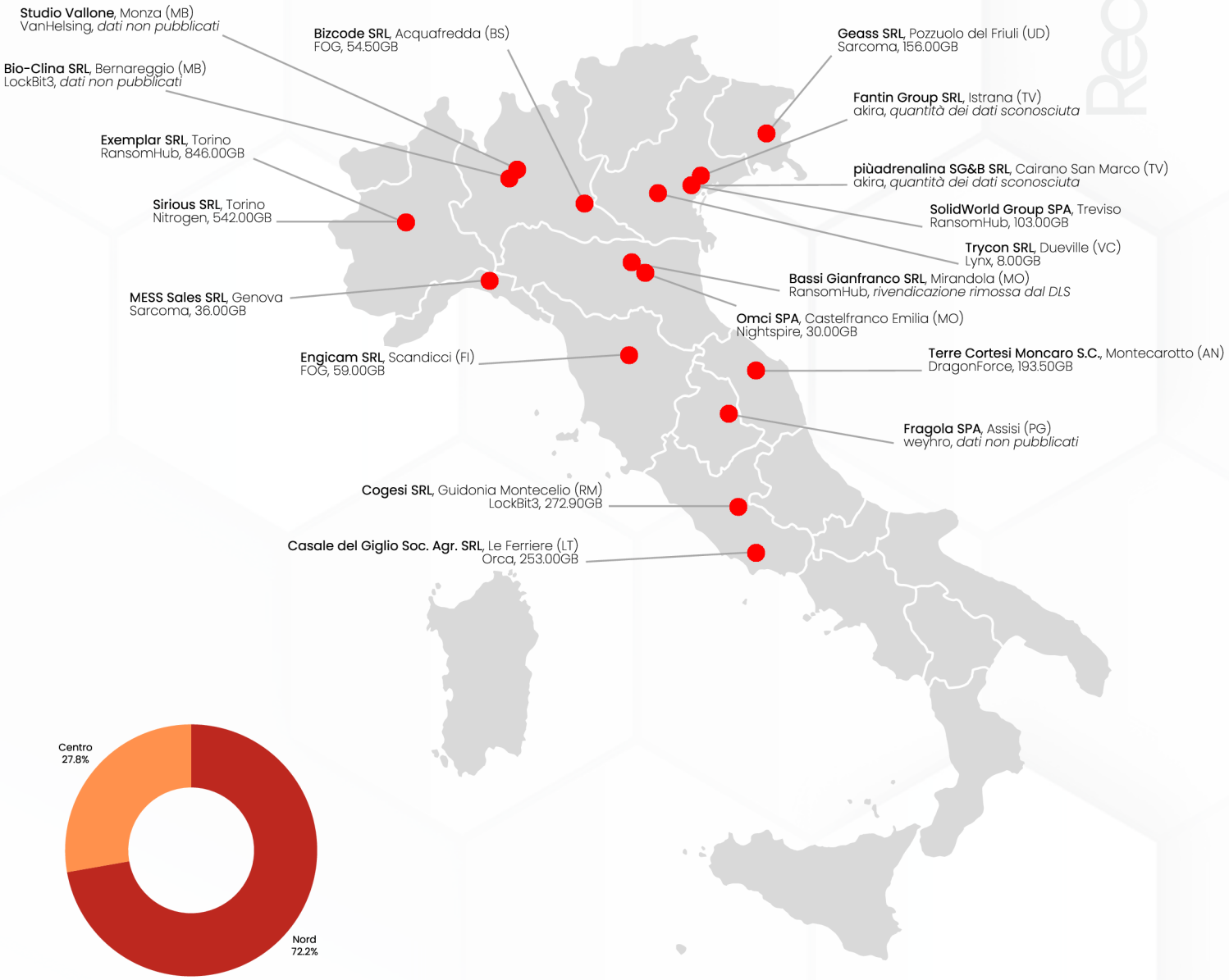
MESE	DATI (GB)	TREND	NOTE
✓ Gennaio	5178.82	—	
✓ Febbraio	1561.80	▼	
✓ Marzo	2553.90	▲	
Aprile			
Maggio			
Giugno			
Luglio			
Agosto			
Settembre			
Ottobre			
Novembre			
Dicembre			

Totale dati esfiltrati pubblicati: **9294.52 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 ritrovamenti retroattivi.*

/breakdown_italy_map

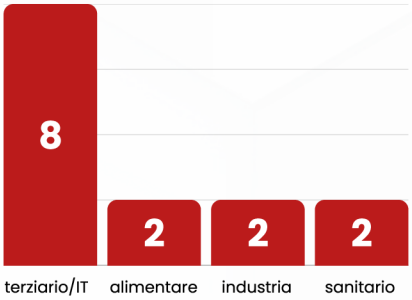
Visualizzazione geografica degli attacchi ransomware **confermati** sul territorio italiano. La mappa mostra la distribuzione regionale degli incidenti registrati nel mese, con indicazione del volume di dati pubblicati (dichiarati) per ciascuna rivendicazione.



Focus regionale

Con **4** attacchi confermati, la **Regione Veneto** si attesta come l'area più colpita nel mese di marzo.

È la provincia di **Treviso** a risultare più esposta, segue **Vicenza** (1 attacco).



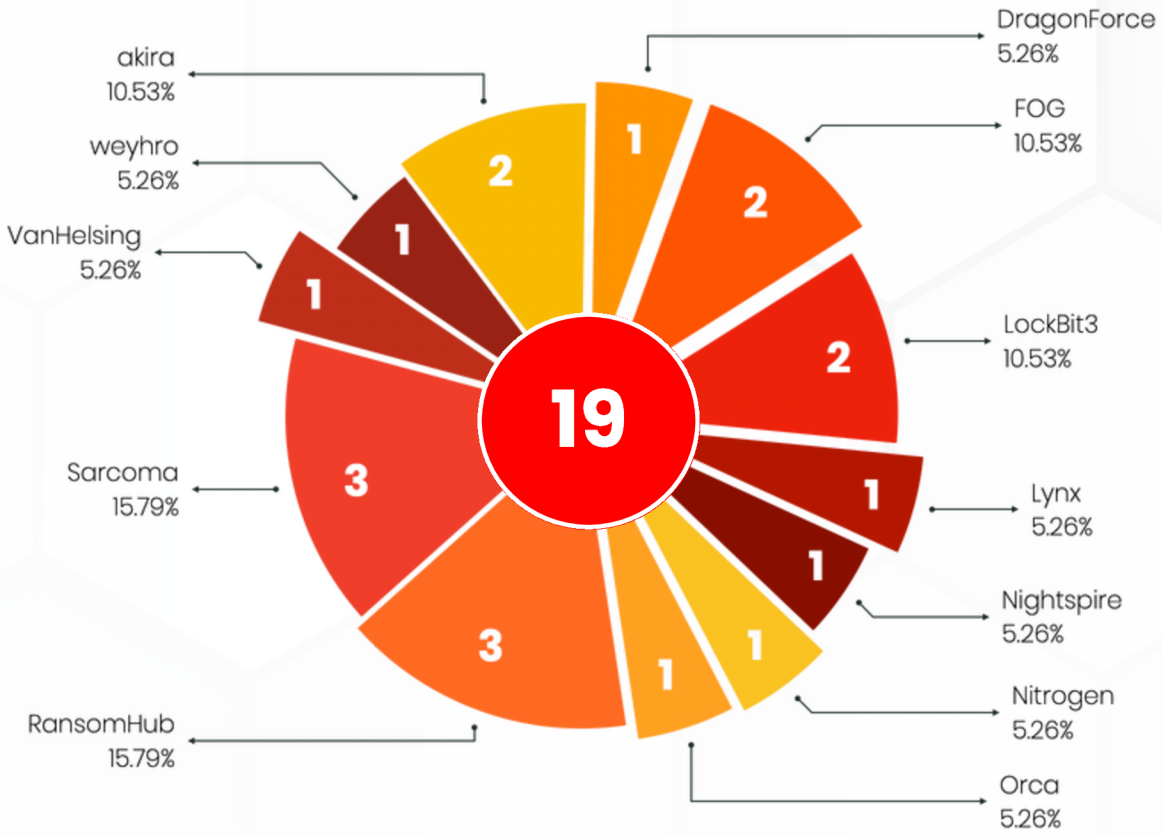
Dati esfiltrati

Il volume dei dati pubblicati per la regione è di **111.00GB**.

Vengono ad oggi **esclusi** dal calcolo gli attacchi a **Fantin Group** e **+adrenalina** (in cui la quantità dei dati non è stata pubblicata).

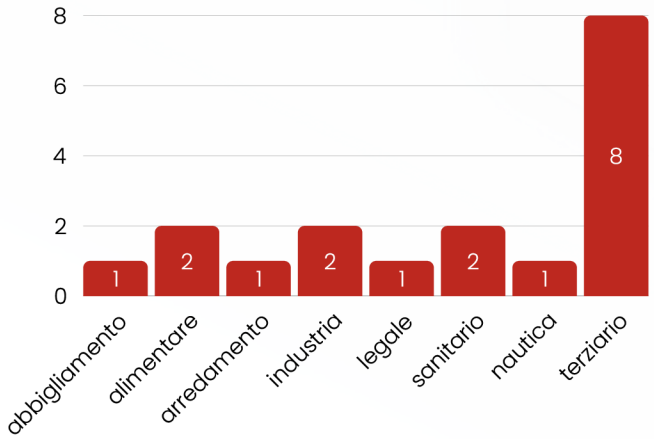
/breakdown_italy_groups

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



La frequenza degli attacchi nelle aree industriali del **Nord Italia** mette in luce la vulnerabilità delle aziende, in particolare quelle con **catene di fornitura fortemente interconnesse**.

Nella maggior parte dei casi, l'intrusione iniziale è avvenuta attraverso **servizi esposti online** o **account compromessi** a seguito di campagne di **phishing**.

La ricorrenza degli attacchi diretti in determinate province indica la presenza di **vettori di minaccia** persistenti non ancora neutralizzati.

È rilevante osservare come alcuni gruppi stiano adottando **strumenti basati sulle AI** per rafforzare le attività di **social engineering** e **phishing**, rendendole più sofisticate, credibili e **su misura**.

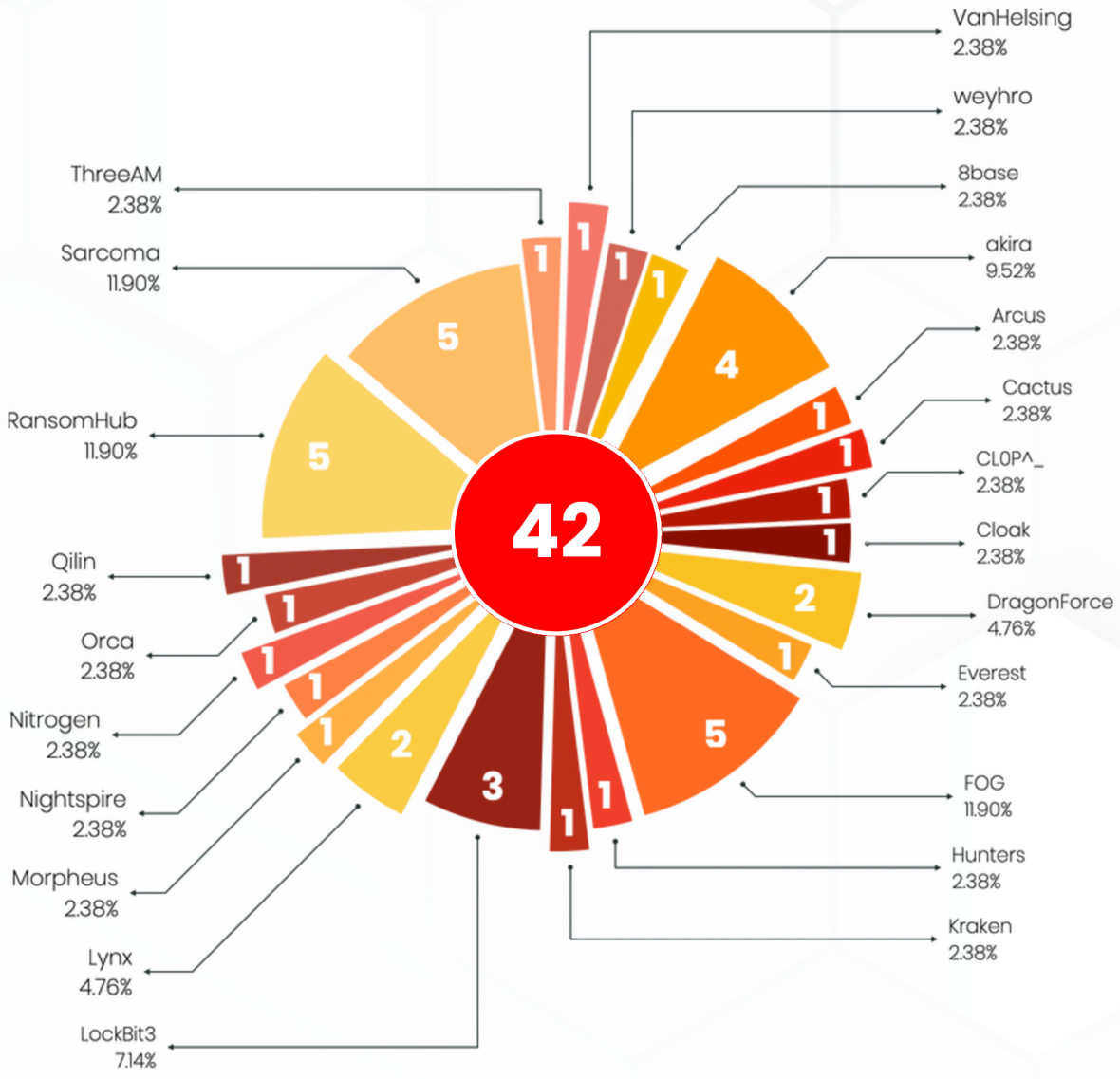
Questi attacchi rappresentano ancora una minaccia in rapida e costante evoluzione.

/breakdown_italy_groups

Nella tabella, il numero delle **vittime italiane** accertate per ogni gruppo, a partire **dal 1° gennaio 2025**, per un totale di **42 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	DragonForce, 2	Lynx, 2	RansomHub, 5
akira, 4	Everest, 1	Morpheus, 1	Sarcoma, 5
Arcus, 1	FOG, 5	Nightspire, 1	ThreeAM, 1
Cactus, 1	Hunters, 1	Nitrogen, 1	VanHelsing, 1
Cloak, 1	Kraken, 1	Orca, 1	weyhro, 1
CL0P^_, 1	LockBit3, 3	Qilin, 1	

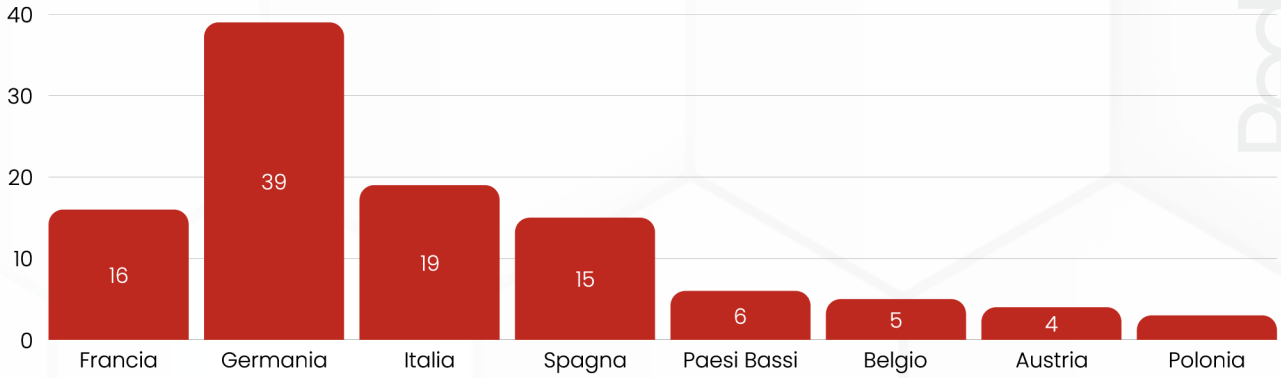


📌 Le analisi indicano un'**evoluzione costante nelle TTP** (*Tactics, Techniques, and Procedures*) dei gruppi criminali.

Il vettore d'ingresso più diffuso resta il **phishing mirato**, veicolato da email con allegati malevoli progettati ad hoc per eludere i controlli e sfruttare le vulnerabilità umane.

/breakdown_europe_nis2

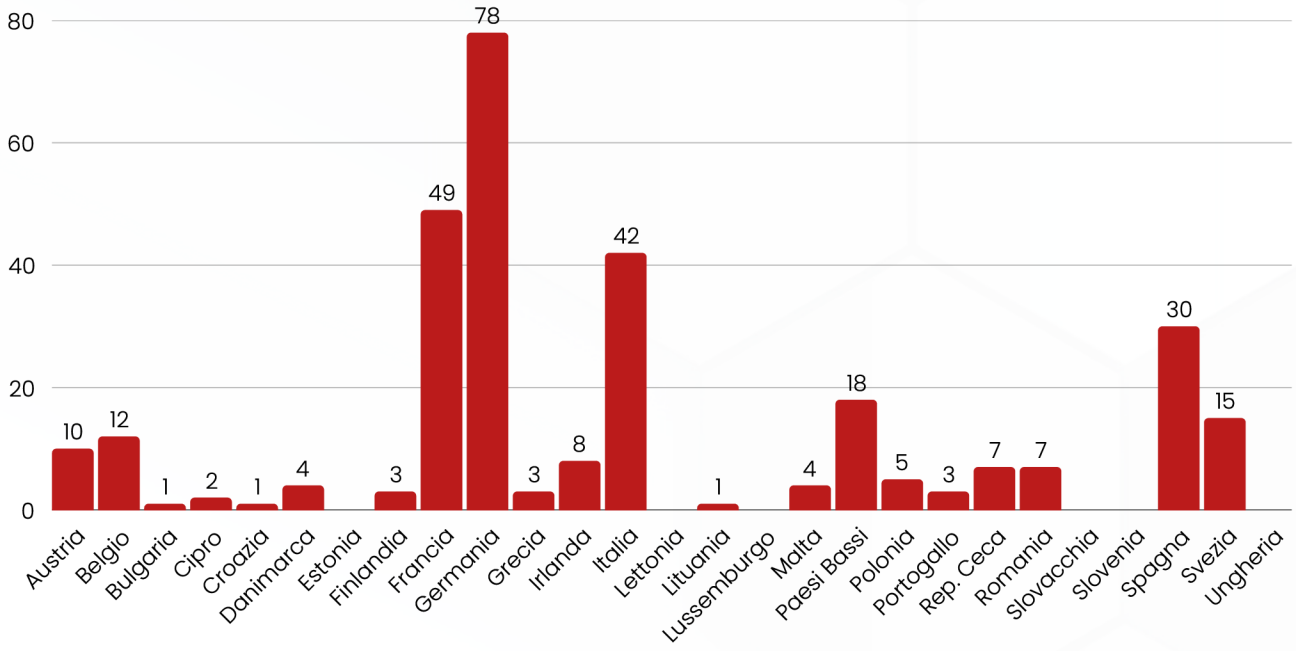
Nel mese di **marzo 2025**, i Paesi UE che adottano le normative della **Direttiva NIS2** hanno subito un totale di **119 attacchi**.
I più colpiti sono stati **Francia**, **Germania** e **Italia** (*fonti aggregate, **elaborazione ransomNews***).



Austria, 4	**Germania**, 39	**Polonia**, 3
Belgio, 5	**Grecia**, 0	**Portogallo**, 1
Bulgaria, 0	**Irlanda**, 1	**Rep. Ceca**, 2
Cipro, 1	**Italia**, 19	**Romania**, 1
Croazia, 0	**Lettonia**, 0	**Slovacchia**, 0
Danimarca, 1	**Lituania**, 0	**Slovenia**, 0
Estonia, 0	**Lussemburgo**, 0	**Spagna**, 15
Finlandia, 1	**Malta**, 1	**Svezia**, 2
Francia, 16	**Paesi Bassi**, 6	**Ungheria**, 1

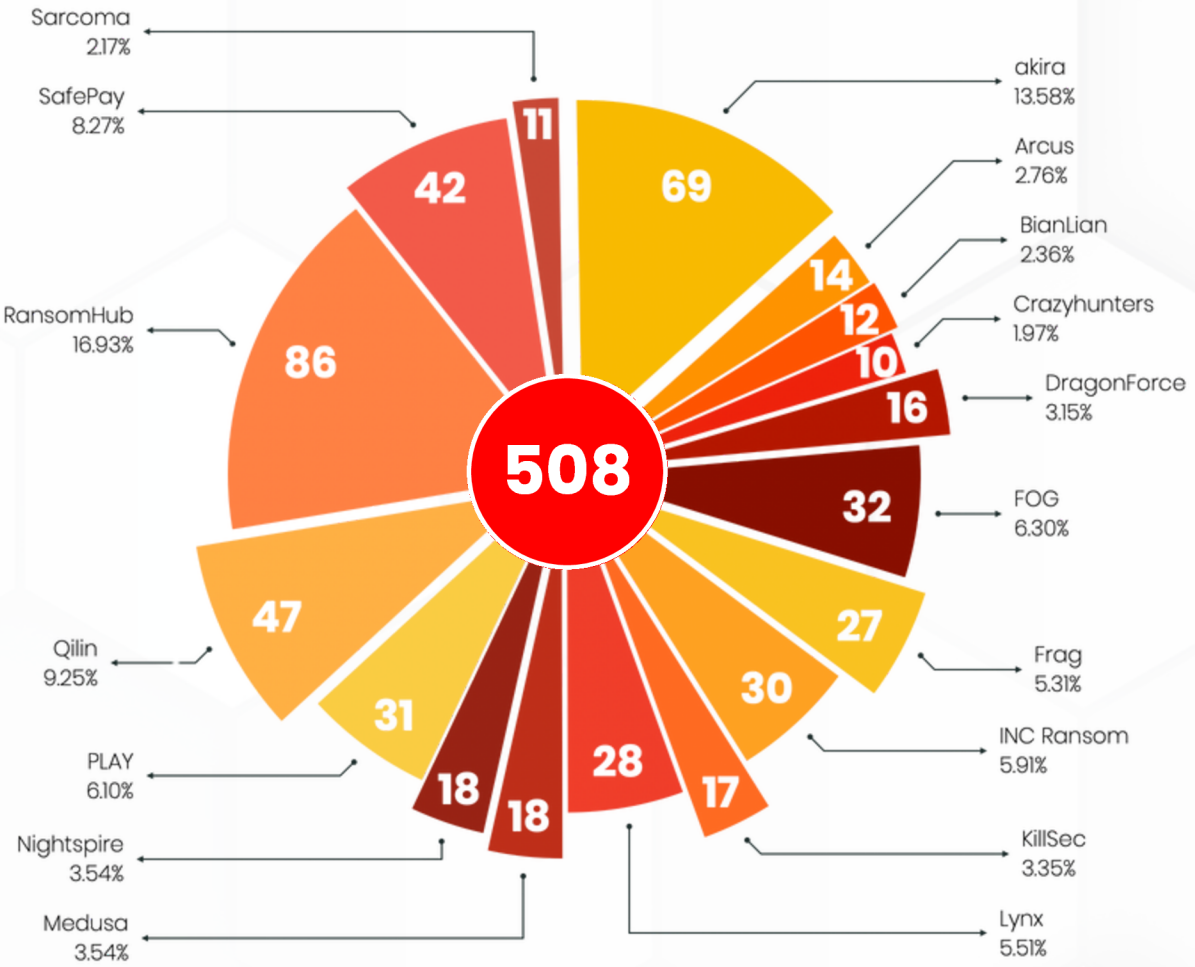
Distribuzione degli incidenti ransomware rilevati **per ciascun paese** membro, sulla base delle rivendicazioni confermate, a partire **dal 1° gennaio 2025,** per un totale di **304 attacchi.**

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



/breakdown_world

648 sono le **rivendicazioni tracciate**, da fonti aggregate, per il mese corrente.
Nel grafico sono riportati i gruppi che hanno totalizzato **più di 10 attacchi**: **17 gruppi**, per un **totale di 508 attacchi** (*elaborazione ransomNews*).



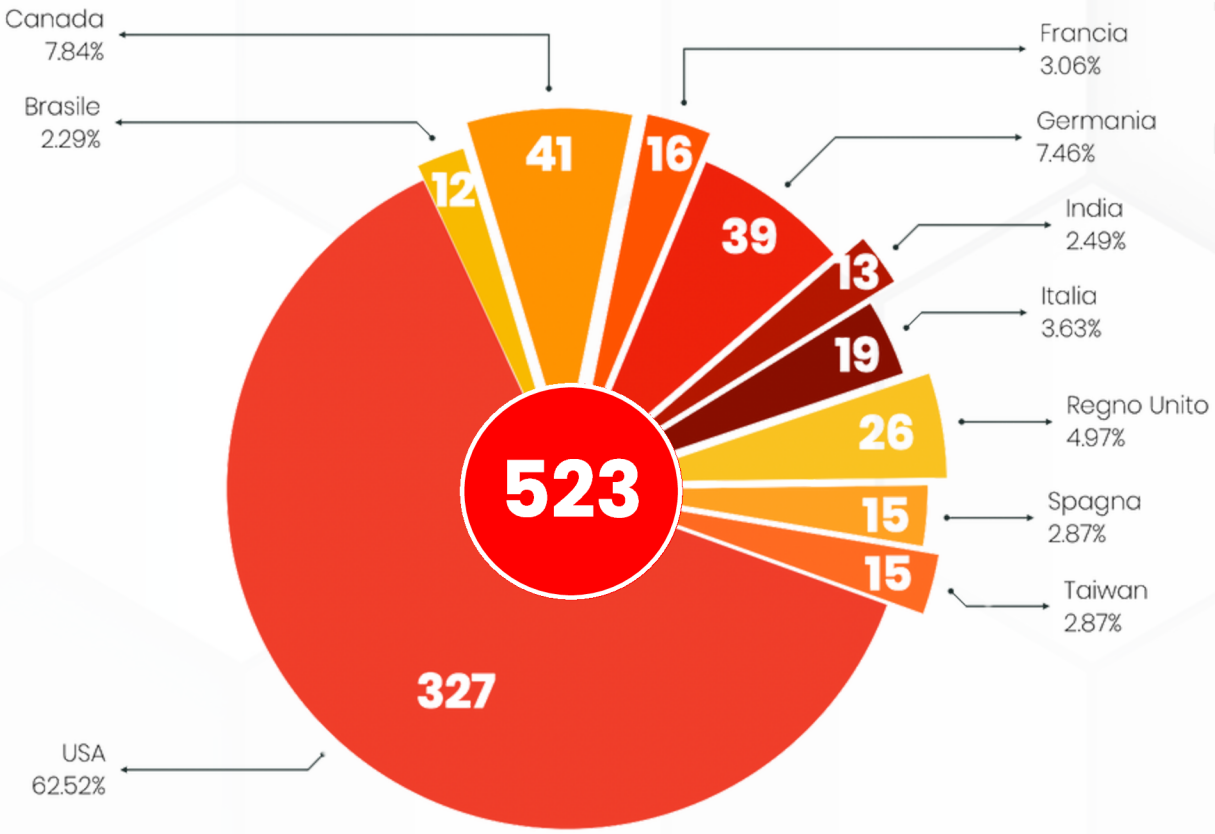
il **dataset** di marzo 2025, con **tutte le rivendicazioni** è disponibile **qui**: **https://rnws.online/YyZGM**

33 invece sono i gruppi che hanno rivendicato **meno di 10 attacchi**, per un totale complessivo di **140 rivendicazioni** (*fonti aggregate, elaborazione ransomNews*).

- **Abyss**, 3
- **Anubis**, 1
- **Apos Security**, 3
- **Arkana**, 2
- **Blackout**, 1
- **Blacksuite**, 2
- **Brain Cipher**, 1
- **Cactus**, 8
- **CHAOS**, 4
- **Cicada3301**, 2
- **CL0P^_**, 6
- **Cloak**, 5
- **Dunghill Leak**, 1
- **EMBARGO**, 2
- **FSociety FLocker**, 3
- **HellCat**, 5
- **Hunters**, 6
- **InterLock**, 6
- **Kairos**, 4
- **Kraken**, 1
- **LockBit3**, 5
- **MedusaLocker**, 1
- **MONTI**, 6
- **Nitrogen**, 2
- **Orca**, 1
- **RALord**, 5
- **RansomEXX**, 1
- **RansomHouse**, 3
- **Rhysida**, 8
- **SECP0**, 1
- **Skira Team**, 4
- **Space Bears**, 2
- **Stormous**, 3
- **Termite**, 1
- **ThreeAM**, 8
- **Trinity**, 7
- **VanHelsing**, 8
- **weyhro**, 8

/breakdown_world

Riportiamo nel grafico i paesi che, in questo mese, hanno subito **più di 10 attacchi**, su un totale di **64 paesi colpiti** (mondo e paesi NIS2). Si tratta di **10 paesi**, per complessive **523 rivendicazioni** (*fonti aggregate, **elaborazione ransomNews***).



Gli attacchi ai rimanenti **54 paesi** (mondo e paesi NIS2), per un totale generale di **125 rivendicazioni**, sono così suddivisi (*fonti aggregate, **elaborazione ransomNews***):

- Antigua, 1
- Austria, 4
- Argentina, 6
- Australia, 9
- Bahamas, 1
- Belgio, 5
- Botswana, 1
- Cile, 2
- Cina, 3
- Cipro, 1
- Colombia, 4
- Corea del Sud, 2
- Costa Rica, 1
- Danimarca, 1
- Egitto, 2
- El Salvador, 1
- Emirati Arabi, 1
- Finlandia, 1
- Giamaica, 2
- Giappone, 6
- Hong Kong, 3
- Indonesia, 2
- Irlanda, 1
- Laos, 1
- Malesia, 3
- Malta, 1
- Messico, 4
- Nigeria, 1
- Non Disponibile, 3
- Norvegia, 2
- Nuova Zelanda, 1
- Paesi Bassi, 6
- Pakistan, 1
- Panama, 1
- Perù, 2
- Polonia, 3
- Portogallo, 1
- Portorico, 1
- Princ. Monaco, 1
- Rep. Ceca, 2
- Rep. Dominicana, 2
- Rep. Kiribati, 1
- Romania, 1
- Sri Lanka, 1
- Sud Africa, 2
- Svezia, 2
- Svizzera, 7
- Tailandia, 3
- Tanzania, 1
- Turchia, 3
- Ucraina, 1
- Ungheria, 1
- Uruguay, 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 **2118 rivendicazioni** (***elaborazione ransomNews***).

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

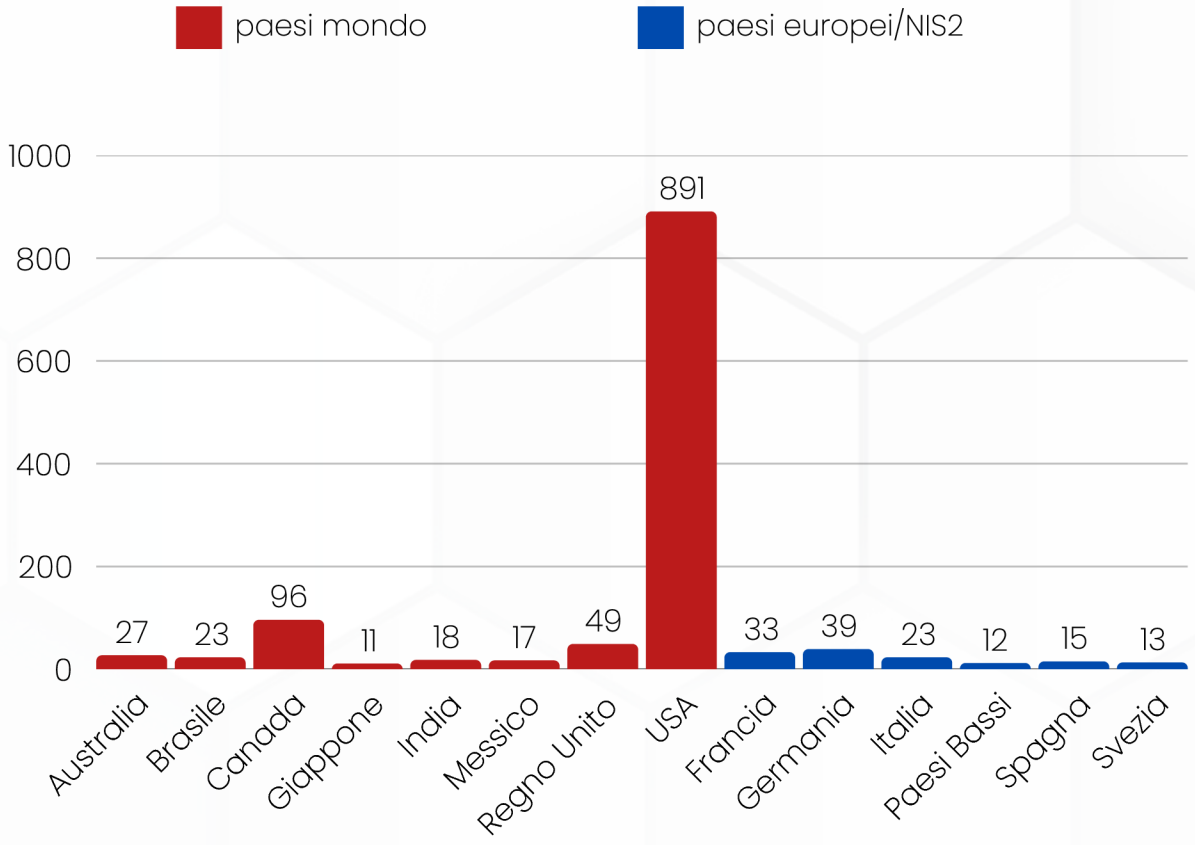
8base, 29
Abyss, 11
akira, 220
Anubis, 5
Apos Security, 5
APT73 / BASHE, 12
Arcus, 19
Arkana, 2
BianLian, 35
Black Basta, 8
Blacklock*, 6
Blackout, 1
Blacksuit, 2
Brain Cipher, 3
Cactus, 53
CHAOS, 4
Cicada3301, 16
CiphBit, 2
CL0P^_, 393
Cloak, 15
Crazyhunters, 10
DarkVault, 2
DragonForce, 35
Dunghill Leak, 1
EMBARGO, 6
Everest, 9
FOG, 90
Frag, 27
FSociety FLocker, 13
GD LockerSec, 5
Handala, 4
HellCat, 6
Hunters, 25
INCRansom, 71
InterLock, 7
Kairos, 15
KillSec, 48
Kraken, 7
Linkc, 1
LockBit3, 22
Lynx, 104
Medusa, 70
MedusaLocker, 4
Metaencryptor, 1
MoneyMessage, 1
MONTI, 15
Morpheus, 5
Nightspire, 18
Nitrogen, 2
Orca, 1
PLAY, 90
Qilin, 112
RALord, 5
RansomEXX, 3
RansomHouse, 6
RansomHub, 232
Rhysida, 24
Run Some Wares, 4
SafePay, 76
Sarcoma, 26
SECP0, 1
Skira Team, 4
Space Bears, 16
Stormous, 5
Termite, 10
ThreeAM, 14
Trinity, 7
Underground, 1
VanHelsing, 8
weyhro, 8

Riportiamo anche la distribuzione degli attacchi per ogni paese colpito, **dal 1° gennaio 2025**, ad *esclusione dei paesi europei/NIS2*, per un **totale di 1814 attacchi** (*fonti aggregate, **elaborazione ransomNews***):

Algeria, 1
Arabia Saudita, 2
Antigua, 1
Argentina, 12
Australia, 36
Bahamas, 1
Bangladesh, 1
Bielorussia, 1
Botswana, 1
Brasile, 35
Canada, 137
Cile, 7
Cina, 9
Colombia, 11
Corea del Sud, 3
Costa Rica, 1
Ecuador, 3
Egitto, 7
El Salvador, 2
Emirati Arabi, 4
Filippine, 2
Georgia, 1
Ghana, 1
Giamaica, 5
Giappone, 17
Haiti, 1
Hong Kong, 5
India, 31
Indonesia, 9
Iraq, 1
Israele, 5
Kenia, 1
Laos, 1
Malesia, 8
Marocco, 2
Messico, 21
Namibia, 1
Nigeria, 4
Non Disponibile, 10
Norvegia, 5
Nuova Zelanda, 6
Oman, 1
Pakistan, 5
Panama, 2
Perù, 5
Portorico, 4
Prin. Monaco, 1
Regno Unito, 75
Rep. Dominicana, 4
Rep. Kiribati, 1
Rep. Palau, 1
Singapore, 14
Sud Africa, 4
Sri Lanka, 1
Svizzera, 15
Tailandia, 10
Taiwan, 24
Tanzania, 2
Tunisia, 1
Turchia, 6
Ucraina, 1
Uruguay, 2
USA, 1218
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 **marzo 2025**:

- **Arkana** - adotta un modello di estorsione in tre fasi: *ransom*, *sale*, *leak*. Si distingue per tattiche di *doxxing* e una comunicazione aggressiva, inclusa la pubblicazione di un video musicale per intimidire le vittime. Le prove suggeriscono un'origine russa, sebbene non confermata
- **CHAOS** - il focus del gruppo è rivolto a settori come trasporti, logistica, chimica e assicurazioni negli Stati Uniti. È solito adottare tattiche di doppia estorsione
- **Crazyhunters** - concentra le sue attività su settori critici a Taiwan, tra cui sanità, istruzione e industria manifatturiera Circa l'80% del toolkit di Crazyhunter proviene da strumenti open source disponibili su GitHub, come il *Prince Ransomware Builder* e *ZammoCide*, adattati per le loro operazioni. Adotta tecniche *BYOVD* (Bring Your Own Vulnerable Driver) sfruttando driver legittimi ma vulnerabili e impiega strumenti come *SharpGPOAbuse* per manipolare oggetti di policy di gruppo (GPO), facilitando l'escalation dei privilegi e la diffusione del ransomware
- **Frag** - il gruppo si distingue per un'escalation rapida e sofisticata di attacchi, principalmente negli Stati Uniti, ma anche nei Paesi Bassi, Singapore e Canada. Frag sfrutta vulnerabilità note, come la CVE-2024-40711 in *Veeam Backup & Replication*, per ottenere l'accesso ai sistemi.

/breakdown_groups_new

- **Nightspire** - il gruppo mostra, fin da subito, segni di inesperienza nel settore, come l'uso di canali di comunicazione mainstream e una sicurezza operativa carente.Sfrutta vulnerabilità nei servizi esposti, come la CVE-2024-55591 in FortiOS, per ottenere accesso non autorizzato ai firewall FortiGate, e strumenti nativi di Windows come PsExec, WMI e RDP per muoversi lateralmente all'interno delle reti compromesse

- **SECP0** - si distingue per un approccio innovativo e piuttosto minaccioso nel panorama delle estorsioni: a differenza dei tradizionali gruppi ransomware, SECP0 adotta una strategia diversa. Scopre vulnerabilità critiche nei sistemi delle organizzazioni e minaccia di renderle pubbliche a meno che non venga pagato un riscatto. Si concentra sull'identificazione di vulnerabilità zero-day o non patchate nei sistemi delle vittime. Una volta individuate, minaccia di divulgarle pubblicamente, esponendo le organizzazioni a potenziali attacchi da parte di altri threat actors. L'assenza di malware o codice attivo consente al gruppo di eludere i sistemi di difesa tradizionali; adotta una tattica *extortionware*, minacciando di rivelare pubblicamente le vulnerabilità scoperte se non viene pagato un riscatto

- **Skira Team** - utilizza l'applicazione Session per le negoziazioni, garantendo un alto livello di anonimato; si focalizza sulla doppia estorsione, senza dettagli noti su strumenti o vulnerabilità specifiche sfruttate

- **VanHelsing** - vanta un modello di affiliazione accessibile e una compatibilità multipiattaforma, rappresentando una minaccia significativa per le aziende. O**pera come una piattaforma RaaS, consentendo a affiliati di lanciare attacchi ransomware in cambio di una quota dei proventi - a fronte di un deposito di $5.000 per la partecipazioni alle azioni criminali, che frutta loro l'80% dei pagamenti di riscatto.** Utilizza tecniche avanzate (WMI, script PowerShell, bootkits e DLL side-loading) per mantenere la persistenza e sfuggire al rilevamento

- **weyhro** - adotta un approccio focalizzato sull'estorsione dei dati senza l'uso di crittografia (pure extortion), implicando l'esfiltrazione di dati senza compromettere l'accesso ai sistemi tramite cifratura.

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

/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

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