

# ransomfeed

ADVANCED **DATADRIVEN** CYBERNEWS

## RECAP MENSILE **AGOSTO 2024**

ver. glitch256\_u03 - 23 settembre 2024

## Il progetto Ransomfeed

**Ransomfeed.it** è un servizio di monitoraggio continuo dei gruppi ransomware; utilizzando l'attività di scraping, ovvero l'estrazione di dati da più siti web per mezzo di programmi software e la successiva strutturazione degli stessi, la piattaforma memorizza le rivendicazioni in un **feed RSS permanente**.

L'intero servizio di monitoraggio è **gratuito e di libera consultazione**, raccoglie e analizza costantemente i dati relativi agli attacchi a livello internazionale.







La piattaforma è in grado di rilevare in modo efficace e tempestivo tutte le rivendicazioni pubblicate dai gruppi, mettendo i dati a disposizione di chiunque desideri comprendere l'entità e l'evoluzione degli attacchi informatici.

## Il recap mensile

Abbiamo deciso di affiancare al nostro **report quadrimestrale** anche un recap mensile, con una particolare attenzione agli **attacchi italiani**. Riteniamo fondamentale offrire un riassunto più frequente delle vittime e della gravità degli incidenti informatici, insieme a molti altri dati statistici, che continueranno a essere disponibili sulla piattaforma.

## I nostri contatti

La piattaforma è sempre accessibile al sito [ransomfeed.it](https://ransomfeed.it), ci trovate inoltre sui canali social:

-  [linkedin.com/company/ransomfeed](https://www.linkedin.com/company/ransomfeed)
-  [x.com/ransomfeed](https://x.com/ransomfeed)
-  [t.me/RansomFeedNews](https://t.me/RansomFeedNews)
-  [bsky.app/profile/ransomfeed.rfeed.it](https://bsky.app/profile/ransomfeed.rfeed.it)
-  [facebook.com/ransomfeed](https://facebook.com/ransomfeed)
-  [reddit.com/r/Ransomfeed](https://reddit.com/r/Ransomfeed)

## Focus Italia

Nel mese di **agosto 2024** la piattaforma ha registrato un totale di **14 attacchi**, concentrati principalmente nel **nord Italia**.

La **maggiore concentrazione** di attacchi nel nord del paese, in aree economicamente sviluppate, può essere interpretata come un indicatore di una maggiore **densità di imprese**, un alto livello di **sviluppo tecnologico** e una diffusione più ampia della **digitalizzazione**.

Il **totale dei dati pubblicati** ammonta a **1098.85 GB**.

ID	GRUPPO	VITTIMA	DATI PUBBLICATI	LOCALIZZAZIONE
16674	hunters	ENEA Italy	219.90 GB	Roma
16831	helldown	Albatross SRL	23.00 GB	Porto Cervo (SS)
16834	helldown	Azienda Trasporti Pubblici	65.00 GB	Sassari
16860	blacksuit	For Rec SPA	236.00 GB	Sta Giustina (PD)
16882	ciphbit	F.D. SRL	*	Palermo
16890	ransomhub	ISNART	10.00 GB	Roma
16898	hunters	BTS Biogas	**	Brunico (BZ)
16911	ciphbit	KEIOS Consulting SRL	167.40 GB	Roma
16928	stormous	Teleco SRL	33.00 GB	Roma
16941	hunters	Ferraro Group SRL	210.00 GB	Ariano Irpino (AV)
16979	ciphbit	Luigi Convertini	134.55 GB	Martina Franca (TA)
17035	bianlian	Studio Notarile Isolabella	***	Milano
17092	meow	Finlogic SPA	***	Bollate (MI)
17207	meow	Caseificio Alta Val Sesia	***	Piode (VC)

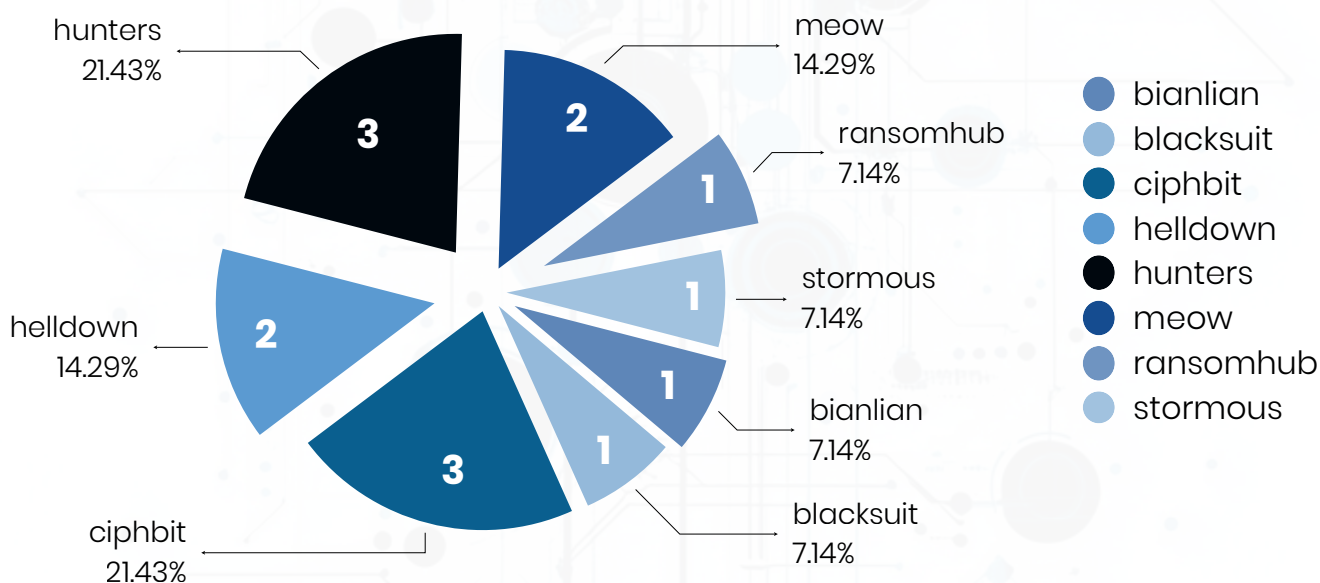
\* la quantità dei dati è sconosciuta

\*\* la rivendicazione è stata rimossa dal DLS

\*\*\* i dati non sono stati pubblicati

fonte: Ransomfeed, dati agosto 2024

Rispetto al mese di **agosto 2023**, quando gli attacchi rivendicati verso target italiani sono stati **15**, si osserva un **decremento del 6.66%**.

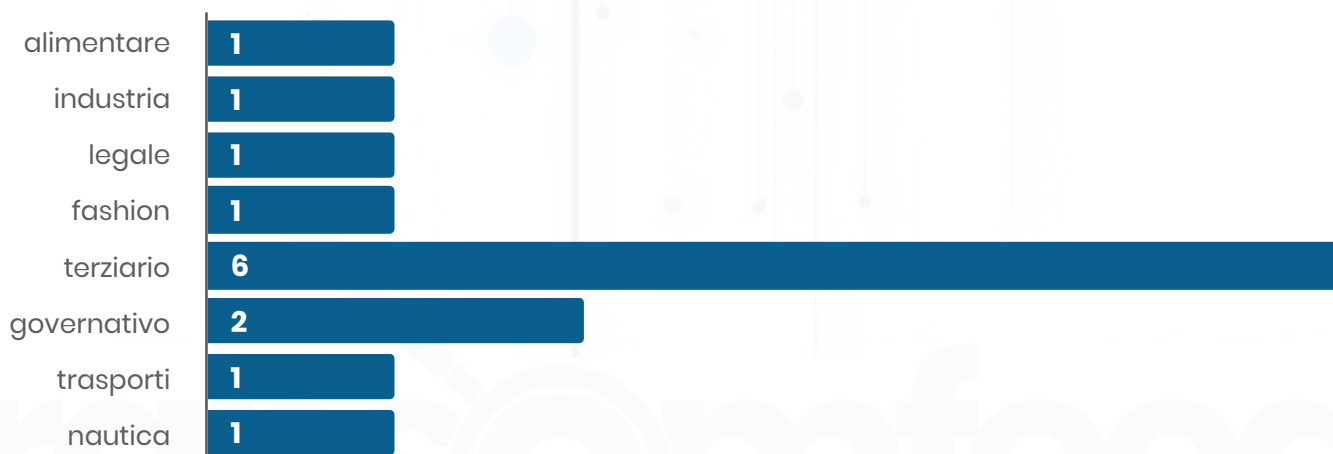


fonte: Ransomfeed, dati agosto 2024

In generale, ogni attacco comporta una serie di **costi significativi**: oltre all'impatto sulle *performance* causato da un *ransomware*, che evidenzia immediatamente una notevole perdita economica (tra il pagamento del riscatto, l'interruzione della produzione o dei servizi e le spese per riparare e ripristinare i sistemi compromessi), si devono considerare anche le **conseguenze sociali** in termini di reputazione e fiducia.

**Industria** e settore **governativo** sono i settori più colpiti dagli attacchi, per la maggior parte utilizzando **phishing**, **social engineering** ed **exploits** di vulnerabilità note.

Da notare che, in alcuni casi, la carenza di sicurezza in aziende **"hub"** si ripercuote su diverse realtà collegate.



fonte: Ransomfeed, dati agosto 2024

Nella tabella seguente, riportiamo il numero totale di rivendicazioni per ciascun mese e la **quantità complessiva provvisoria** di dati pubblicati dai diversi gruppi ransomware.

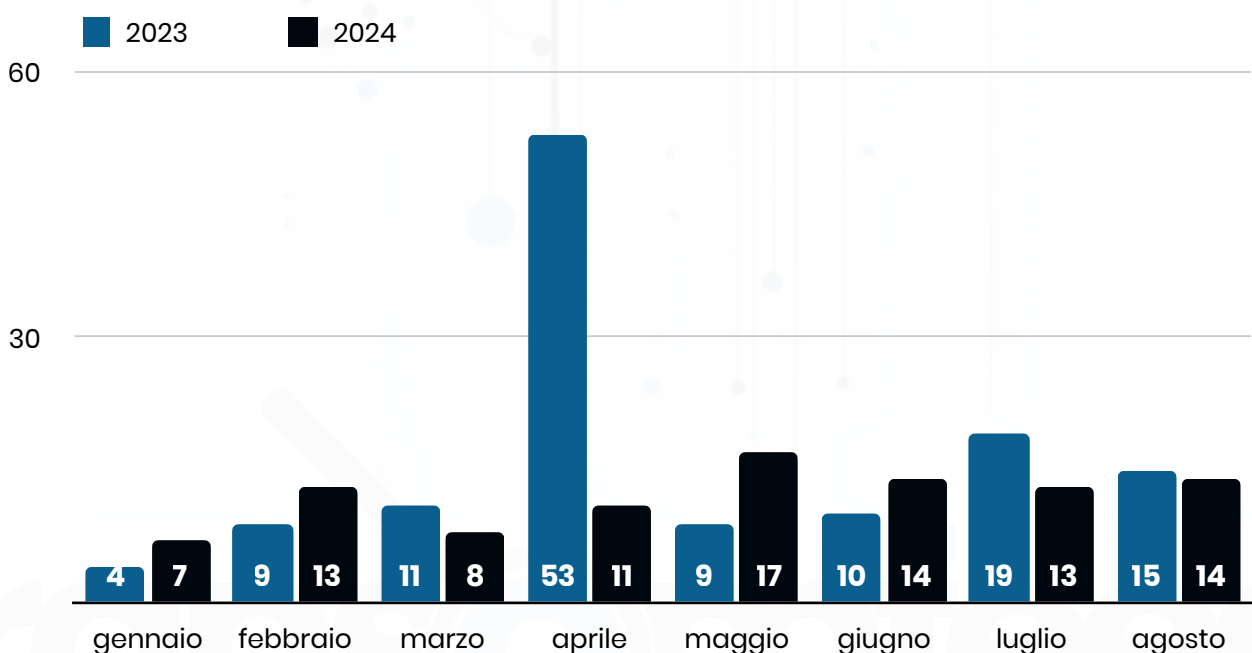
Nel mese di **agosto 2024**, il totale dei dati:

- **esfiltrati dichiarati** ammonta a **2577.95 GB**
- **pubblicati** ammonta a **1098.85 GB**

MESE	RIVENDICAZIONI	DATI DICHIARATI	DATI PUBBLICATI
gennaio	7	599.70 GB	599.70 GB
febbraio	13	1814.10 GB	1092.10 GB
marzo	8	924.10 GB	924.10 GB
aprile	11	2725.90 GB	2624.33 GB
maggio	17	6029.10 GB	4429.10 GB
giugno	14	3026.66 GB	3026.66 GB
luglio	13	3570.71 GB	3559.71 GB*
agosto	14	2577.95 GB	1098.85 GB
<b>totale</b>	<b>97</b>	<b>21268.22 GB</b>	<b>17354.55 GB</b>

\* quantità aggiornata, rispetto al mese precedente

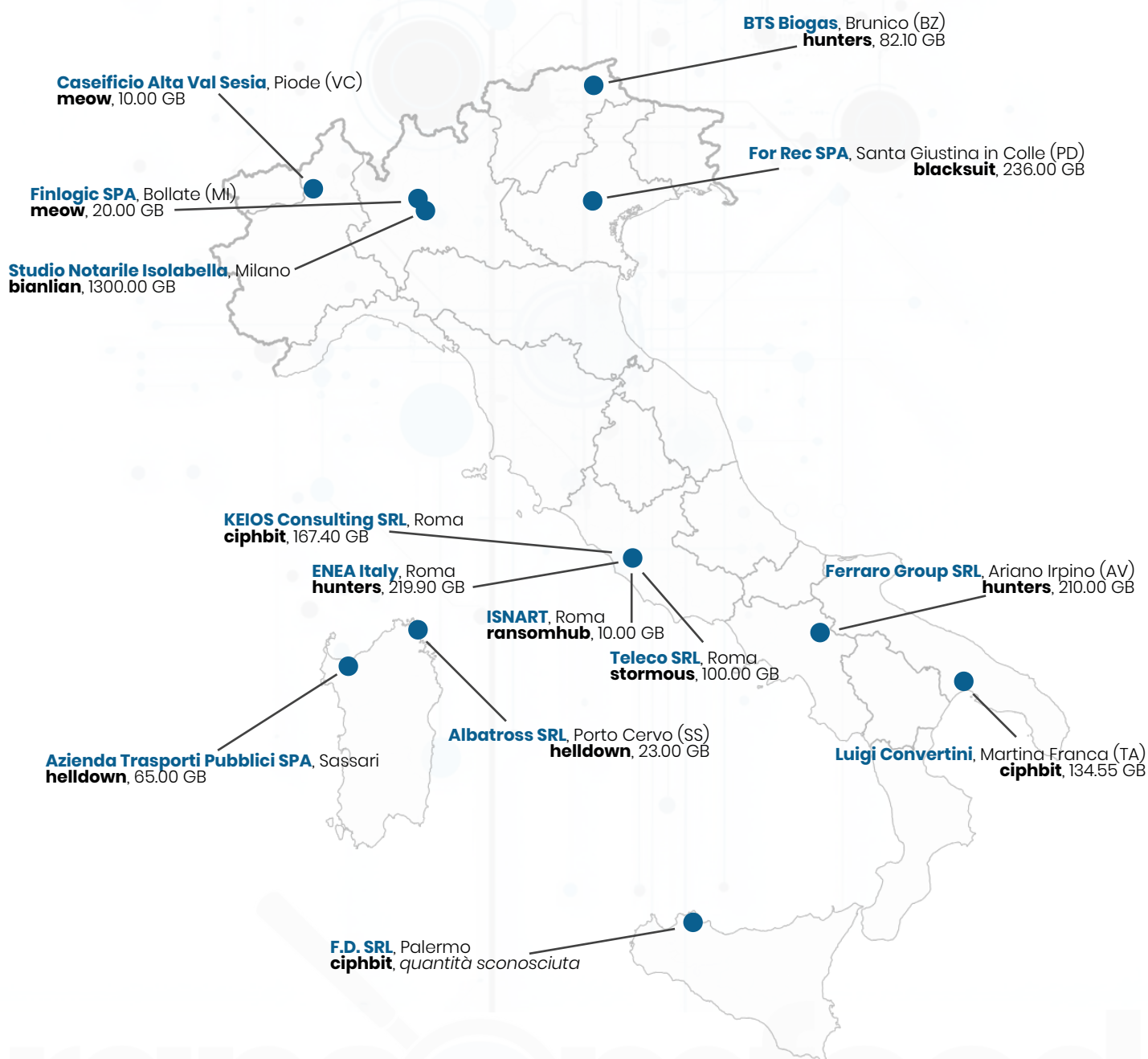
Comparando i dati degli attacchi con quelli dei **primi otto mesi del 2023** (130 attacchi) si osserva un **decremento del 25.38%**.



fonte: Ransomfeed, dati agosto 2024

Con riferimento al mese di **agosto 2024**, la mappatura degli attacchi ransomware sul territorio evidenzia, ancora una volta, una significativa concentrazione nel **nord** del paese con **5 attacchi**, seguiti da **4 attacchi** al **centro**, **2 attacchi** nel **meridione** e **3 attacchi** nelle **isole**.

Nonostante la **frequenza maggiore** di attacchi ransomware nel nord e centro Italia, le misure di sicurezza adottate restano insufficienti. Molte imprese, oggi, **non investono** a sufficienza in misure di sicurezza informatica, esponendosi a rischi sempre più elevati.



fonte: Ransomfeed, dati agosto 2024

## 📍 Aggiornamenti

Lo **Studio Legale Associato Isolabella**, vittima del gruppo criminale **bianlian**, ha subito un'esfiltrazione di 1.3 TB di dati. Alla data di uscita di questo report, i dati non sono stati ancora pubblicati dai threat actors.

**Vittima:** Studio Legale Associato Isolabella

ID: 17035 rilevato il 24-08-2024 08:49:58 dal gruppo **bianlian**


**Descrizione:** Studio Legale Associato Isolabella is a company that operates in the Law Firms & Legal Services industry.

**Hash di rilevamento:** c56a3598c0cb770e26dae02b298d1a19dcd2fa867696a02ee88a44d254dddada

**Vittima localizzata in:** Italy

**Sito web:** N/D

**Settore lavorativo:** Attorney



## BianLian

Work with us: targets' providers, software engineers, pentesters, journalists.

Tox: `AMNDQF5HOCIFEDANFORDIADOCIFDCI BFWH B7NMAUWHI FT7BANKFJOMAGCELPKCECH`

Email: `disruptive@isolabellmail.org`

## # Studio Legale Associato Isolabella

Studio Legale Associato Isolabella is a company that operates in the Law Firms & Legal Services industry.

*Founder:* Lodovico Isolabella

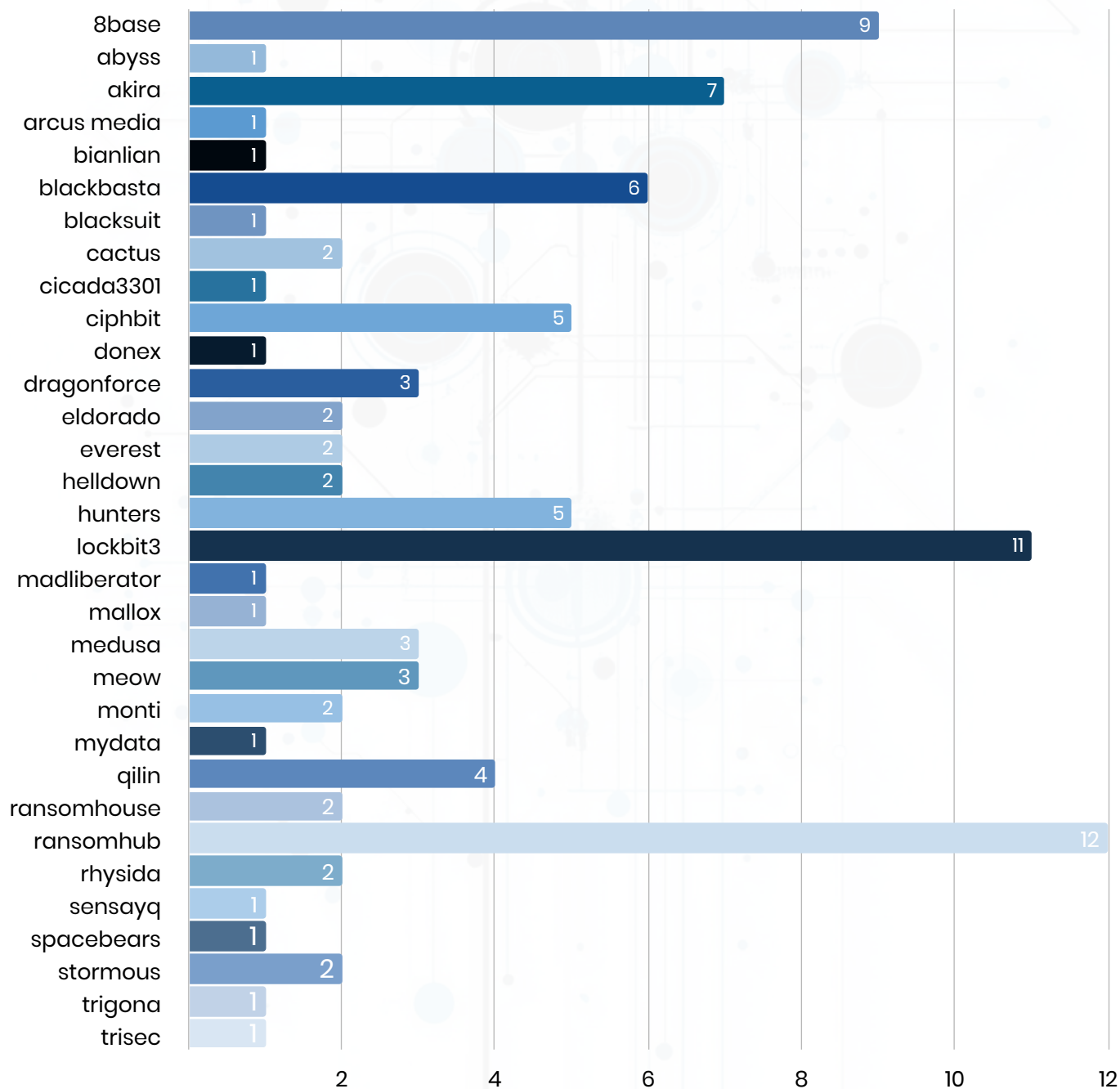
Business Email: `Lodovico.Isolabella@isolabella.it`

La scelta dei criminali di non comunicare la pubblicazione dei dati esfiltrati si riconduce, innanzitutto, al **massimizzare il profitto** tramite l'estorsione: il silenzio sulla pubblicazione dei dati permette di mantenere la pressione sulla vittima, aumentando le possibilità che questa decida di pagare il riscatto per evitare la divulgazione.

Un'altra ragione è che, spesso, i criminali preferiscono **vendere i dati esfiltrati sul dark web**, poiché pubblicarli ne ridurrebbe il valore economico. Tenere nascosta l'esfiltrazione consente anche di evitare un'attenzione immediata da parte delle autorità o degli esperti di sicurezza informatica, riducendo il rischio di essere individuati.

Infine, mantenere segreta l'esfiltrazione permette di sfruttare ulteriormente le informazioni rubate, usando i dati per compromettere altre organizzazioni.

Questo uno spaccato dei **97 attacchi**, suddivisi per gruppo criminale (per un totale di **32 gruppi**) nei primi otto mesi del 2024.






























fonte: Ransomfeed, dati agosto 2024



## Focus paesi UE direttiva NIS2

Nel mese corrente, i **Paesi UE** hanno subito un totale di **74 attacchi**.  
I tre paesi **più colpiti** sono: Italia (14), Francia (12) e Germania (9).

 <b>Austria</b> , 3 (4.05%)	 <b>Germania</b> , 9 (12.16%)	 <b>Polonia</b> , 5 (6.75%)
 <b>Belgio</b> , 3 (4.05%)	 <b>Grecia</b> , 1 (1.35%)	 <b>Portogallo</b> , 1 (1.35%)
 <b>Bulgaria</b> , 0 (0%)	 <b>Irlanda</b> , 3 (4.05%)	 <b>Rep. Ceca</b> , 1 (1.35%)
 <b>Cipro</b> , 2 (2.70%)	 <b>Italia</b> , 14 (18.90%)	 <b>Romania</b> , 2 (2.70%)
 <b>Croazia</b> , 0 (0%)	 <b>Lettonia</b> , 0 (0%)	 <b>Slovacchia</b> , 0 (0%)
 <b>Danimarca</b> , 4 (5.40%)	 <b>Lituania</b> , 0 (0%)	 <b>Slovenia</b> , 0 (0%)
 <b>Estonia</b> , 0 (0%)	 <b>Lussemburgo</b> , 0 (0%)	 <b>Spagna</b> , 7 (9.46%)
 <b>Finlandia</b> , 0 (0%)	 <b>Malta</b> , 0 (0%)	 <b>Svezia</b> , 3 (4.05%)
 <b>Francia</b> , 12 (16.21%)	 <b>Paesi Bassi</b> , 4 (5.40%)	 <b>Ungheria</b> , 0 (0%)

fonte: Ransomfeed, dati agosto 2024

## NIS2 in breve

**Network and Information Security Directive** è la seconda iterazione della Direttiva sulle reti e i sistemi informativi; mira a stabilire un livello più elevato di resilienza informatica all'interno delle organizzazioni dell'Unione Europea, in particolare per gli operatori di infrastrutture critiche e servizi essenziali.

La direttiva mira a potenziare la sicurezza informatica in generale, richiedendo a ogni Stato membro dell'UE di essere preparato ad affrontare un'eventuale minaccia informatica con un **Computer Security Incident Response Team** (CSIRT) e un'autorità nazionale competente per le reti e i sistemi informativi.

Aumentando la collaborazione tra gli Stati membri con la creazione di un gruppo di cooperazione per lo scambio d'informazioni, atto anche a promuovere una cultura della sicurezza informatica e applicare le migliori pratiche in materia di difesa.

Più informazioni:

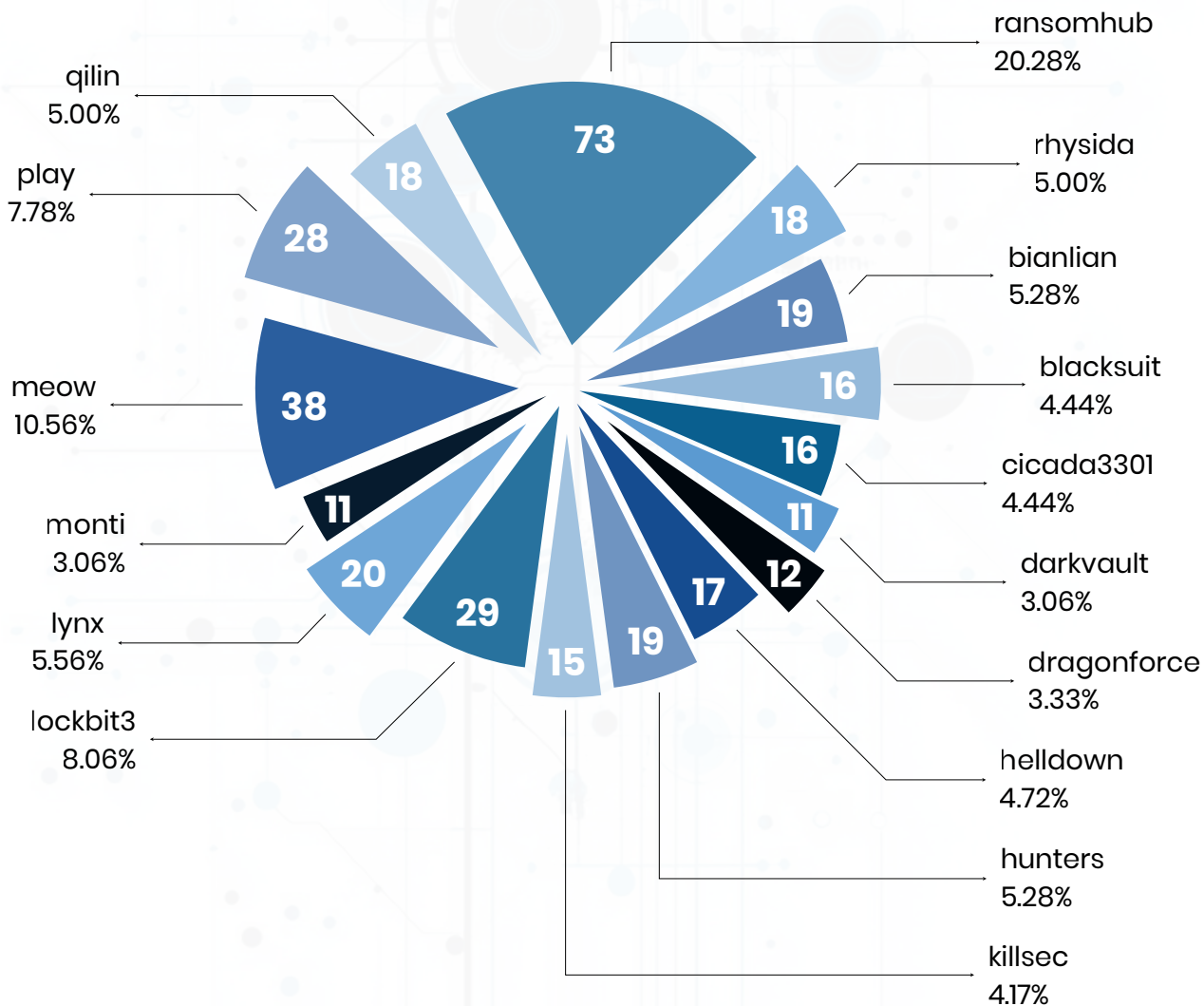
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555>

<https://www.nis-2-directive.com>

[https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS\\_BRI\(2021\)689333\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf)

## Scena internazionale

Sono stati rilevati **446 attacchi** (su un totale, nei primi otto mesi, di 3165) evidenziando un **incremento del 10.40%** rispetto allo stesso periodo dell'anno precedente, quando gli attacchi rivendicati furono **404** (su un totale, nei primi otto mesi, di 3081).



**25**

gruppi con **meno di 10 attacchi** (per un totale di **86** rivendicazioni)

**cloak**, 8  
**incransom**, 7  
**akira**, 6  
**abyss**, 6  
**braincipher**, 6  
**cactus**, 5  
**medusa**, 4  
**eldorado**, 4  
**fog**, 4

**madliberator**, 3  
**apt73**, 3  
**ciphbit**, 3  
**danon**, 3  
**everest**, 3  
**metaencryptor**, 3  
**spacebears**, 3  
**ransomhouse**, 2  
**trinity**, 2

**flocker**, 2  
**handala**, 2  
**mydata**, 2  
**ransomexx**, 2  
**blackout**, 1  
**raworld**, 1  
**stormous**, 1

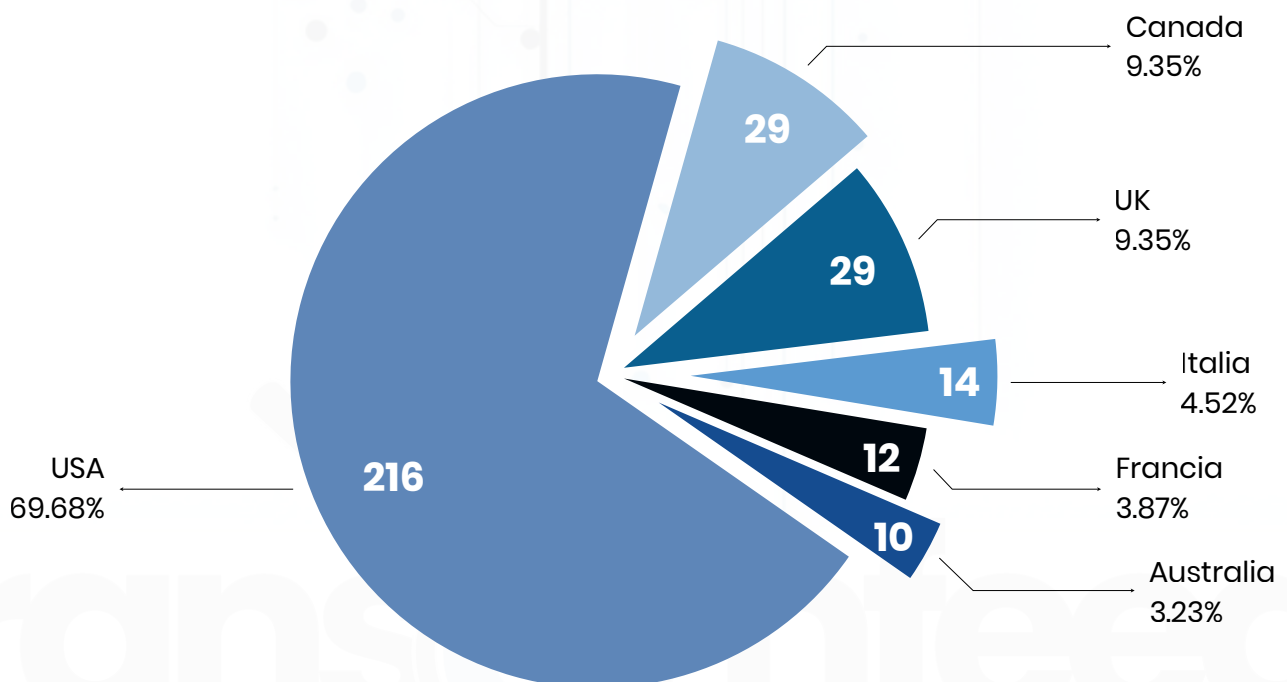
Anche a livello internazionale, pubblichiamo la tabella con il **numero totale delle rivendicazioni**, suddivise per mese, escludendo eventuali duplicati che potrebbero essere individuati nei mesi successivi.

MESE	RIVENDICAZIONI
gennaio	284
febbraio	373
marzo	382
aprile	379
maggio	557
giugno	339
luglio	405
agosto	446
<b>totale</b>	<b>3165</b>

Rispetto allo stesso periodo dell'anno precedente, in cui gli attacchi ammontavano a **3081**, si osserva un **incremento del 2.73%**.

Nel mese di agosto, gli **Stati Uniti** continuano a essere il paese più colpito, con **216 attacchi** su un **totale di 310**, rappresentando la maggioranza degli incidenti a livello globale.

























































Nel grafico sono considerati i paesi che hanno subito **più di 10 attacchi**.



fonte: Ransomfeed, dati agosto 2024

57

paesi con **meno di 10 attacchi** (per un totale di **136** rivendicazioni)

 <b>Germania</b> , 9	 <b>Cipro</b> , 2	 <b>Grecia</b> , 1
 <b>India</b> , 8	 <b>Guatemala</b> , 2	 <b>Hong Kong</b> , 1
 <b>Spagna</b> , 7	 <b>Libano</b> , 2	 <b>Indonesia</b> , 1
 <b>Brasile</b> , 6	 <b>Non Disponibile</b> , 2	 <b>Costa d'Avorio</b> , 1
 <b>Svizzera</b> , 6	 <b>Perù</b> , 2	 <b>Giamaica</b> , 1
 <b>Israele</b> , 6	 <b>Romania</b> , 2	 <b>Kenia</b> , 1
 <b>Sud Africa</b> , 6	 <b>Seychelles</b> , 2	 <b>Kuwait</b> , 1
 <b>Polonia</b> , 5	 <b>Corea del Sud</b> , 2	 <b>Norvegia</b> , 1
 <b>Messico</b> , 4	 <b>Venezuela</b> , 2	 <b>Pakistan</b> , 1
 <b>Paesi Bassi</b> , 4	 <b>Zimbabwe</b> , 2	 <b>Filippine</b> , 1
 <b>Danimarca</b> , 4	 <b>Repubblica Ceca</b> , 1	 <b>Portogallo</b> , 1
 <b>Belgio</b> , 3	 <b>Oman</b> , 1	 <b>Arabia Saudita</b> , 1
 <b>Malesia</b> , 3	 <b>Singapore</b> , 1	 <b>Timor Est</b> , 1
 <b>Nuova Zelanda</b> , 3	 <b>Taiwan</b> , 1	 <b>Turchia</b> , 1
 <b>Austria</b> , 3	 <b>Argentina</b> , 1	 <b>UAE</b> , 1
 <b>Irlanda</b> , 3	 <b>Cile</b> , 1	 <b>Uruguay</b> , 1
 <b>Svezia</b> , 3	 <b>Gibuti</b> , 1	 <b>Vietnam</b> , 1
 <b>Giappone</b> , 2	 <b>Rep. Dominicana</b> , 1	
 <b>Cina</b> , 2	 <b>Fiji</b> , 1	
 <b>Colombia</b> , 2	 <b>Ghana</b> , 1	

fonte: Ransomfeed, dati agosto 2024

Nel mese di **agosto 2024** abbiamo registrato in piattaforma **1 nuovo gruppo** ransomware. Precisiamo che l'entrata in piattaforma, e il successivo monitoraggio, non determinano la nascita effettiva di un nuovo gruppo.

<b>Helldown Leaks</b> (17 attacchi)	
-------------------------------------	--

fonte: Ransomfeed, dati agosto 2024

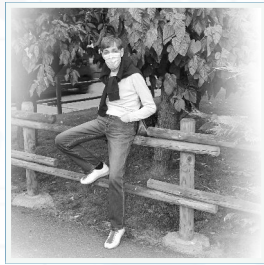
Riepiloghiamo, suddivisi per gruppi, gli attacchi registrati sulla piattaforma dal **1 gennaio** al **31 agosto 2024**; i **78 gruppi** hanno totalizzato **3165 attacchi**:

<b>Omega</b> , 1	<b>daixin</b> , 3	<b>lockbit3</b> , 493	<b>ransomwareblog</b> , 1
<b>8base</b> , 123	<b>danon</b> , 19	<b>lynx</b> , 22	<b>raworld</b> , 30
<b>abyss</b> , 29	<b>darkvault</b> , 45	<b>madliberator</b> , 11	<b>redransomware</b> , 16
<b>akira</b> , 152	<b>donex</b> , 5	<b>malekteam</b> , 3	<b>rhapsida</b> , 58
<b>alphv</b> , 53	<b>donutleak</b> , 10	<b>mallox</b> , 10	<b>sensayq</b> , 2
<b>apossecurity</b> , 4	<b>dragonforce</b> , 70	<b>medusa</b> , 138	<b>slug</b> , 1
<b>apt73</b> , 15	<b>dunghill leak</b> , 3	<b>meow</b> , 69	<b>snatch</b> , 15
<b>arcusmedia</b> , 26	<b>eldorado</b> , 19	<b>metaencryptor</b> , 9	<b>spacebears</b> , 31
<b>bianlian</b> , 123	<b>embargo</b> , 11	<b>moneymessage</b> , 3	<b>stormous</b> , 25
<b>blackbasta</b> , 135	<b>everest</b> , 25	<b>monti</b> , 25	<b>threeam</b> , 12
<b>blackbyte</b> , 3	<b>flocker</b> , 12	<b>mydata</b> , 13	<b>trigona</b> , 19
<b>blackout</b> , 7	<b>fog</b> , 16	<b>noname</b> , 3	<b>trinity</b> , 5
<b>blacksuit</b> , 93	<b>gookie</b> , 2	<b>play</b> , 217	<b>trisec</b> , 3
<b>braincipher</b> , 12	<b>handala</b> , 23	<b>pryx</b> , 2	<b>underground</b> , 17
<b>cactus</b> , 74	<b>helldown</b> , 17	<b>qilin</b> , 104	<b>unsafe</b> , 2
<b>cicada3301</b> , 26	<b>hunters</b> , 152	<b>qiulong</b> , 8	<b>vanir</b> , 3
<b>ciphbit</b> , 9	<b>incransom</b> , 111	<b>ransomcortex</b> , 4	<b>werewolves</b> , 3
<b>cloak</b> , 32	<b>insane</b> , 1	<b>ransomexx</b> , 13	<b>zerotolerance</b> , 1
<b>cl0p</b> , 19	<b>killsec</b> , 26	<b>ransomhouse</b> , 42	
<b>cuba</b> , 2	<b>knight</b> , 8	<b>ransomhub</b> , 217	

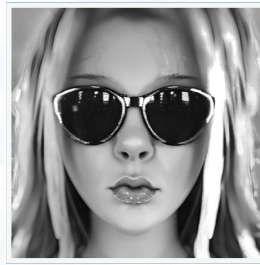
## Chi siamo



**Dario Fadda**  
co-founder  
dev maintainer



**Claudio Sono**  
co-founder  
OSINT maintainer



**Claudia Galingani Mongini**  
digital strategy  
OSINT, SOCMINT



**Matteo**  
backend developer  
frontend maintainer

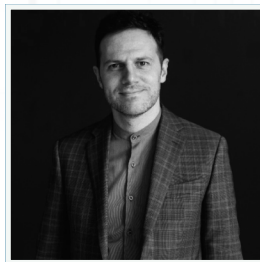


**Federico Fuga**  
backend developer  
frontend maintainer



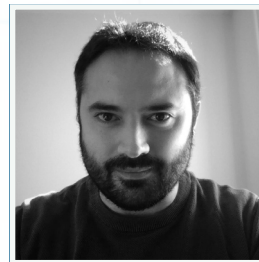
**Christian Bernieri**  
DPO

contributor  
privacy policy



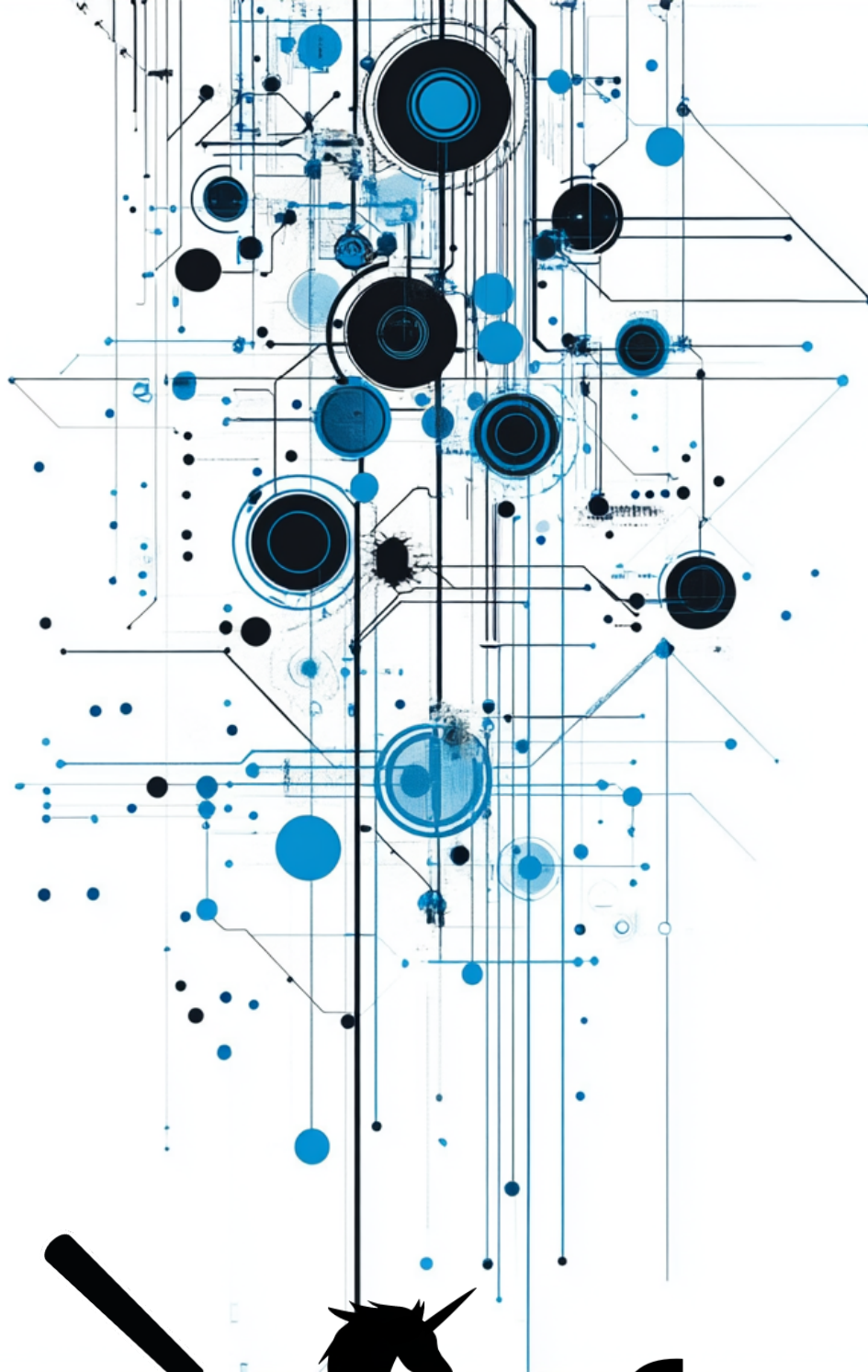
**Massimo Giaimo**  
Würth Phoenix

enrichment su settori  
lavorativi



**Edoardo Limone**  
consulente cyber

sostenitore e promotore  
del progetto



# ransomfeed

ADVANCED DATADRIVEN CYBERNEWS

RECAP MENSILE  
**AGOSTO 2024**

**/eof**