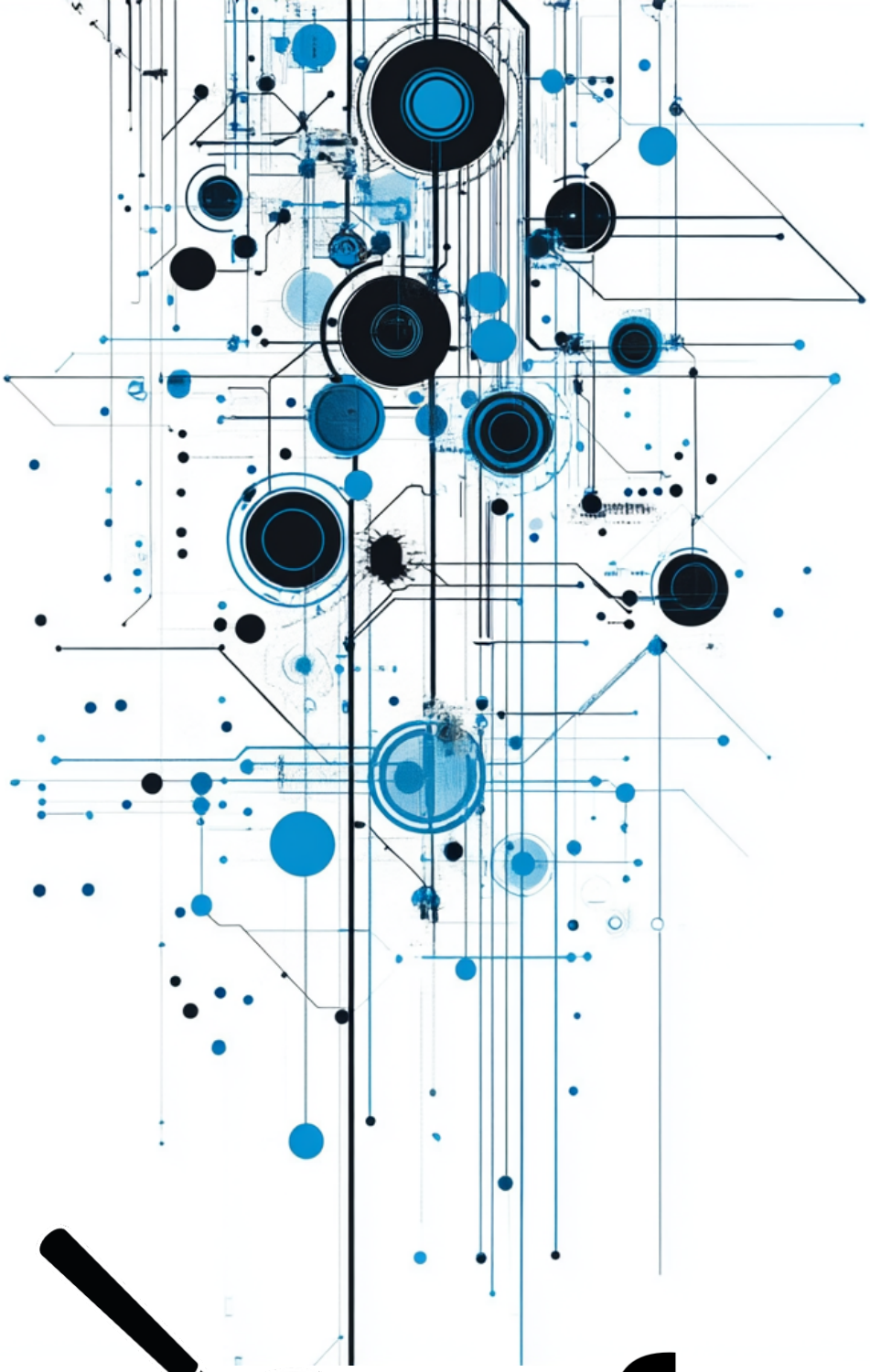


ransomfeed

ADVANCED **DATADRIVEN** CYBERNEWS

RECAP MENSILE
SETTEMBRE 2024

ver. glitch256_u01 - 13 ottobre 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, ci trovate inoltre sui canali social:

- linkedin.com/company/ransomfeed
- x.com/ransomfeed
- t.me/RansomFeedNews
- bsky.app/profile/ransomfeed.rfeed.it
- facebook.com/ransomfeed
- reddit.com/r/Ransomfeed

Focus Italia 🇮🇹

Nel mese di **settembre 2024** la piattaforma ha rilevato un totale di **9 attacchi**, localizzati prevalentemente nel **nord Italia**.

Questa concentrazione nelle aree economicamente avanzate del Paese può essere vista come un indicatore della **maggiore densità di imprese**, del più **alto livello di sviluppo** tecnologico e della **diffusione più capillare** della digitalizzazione.

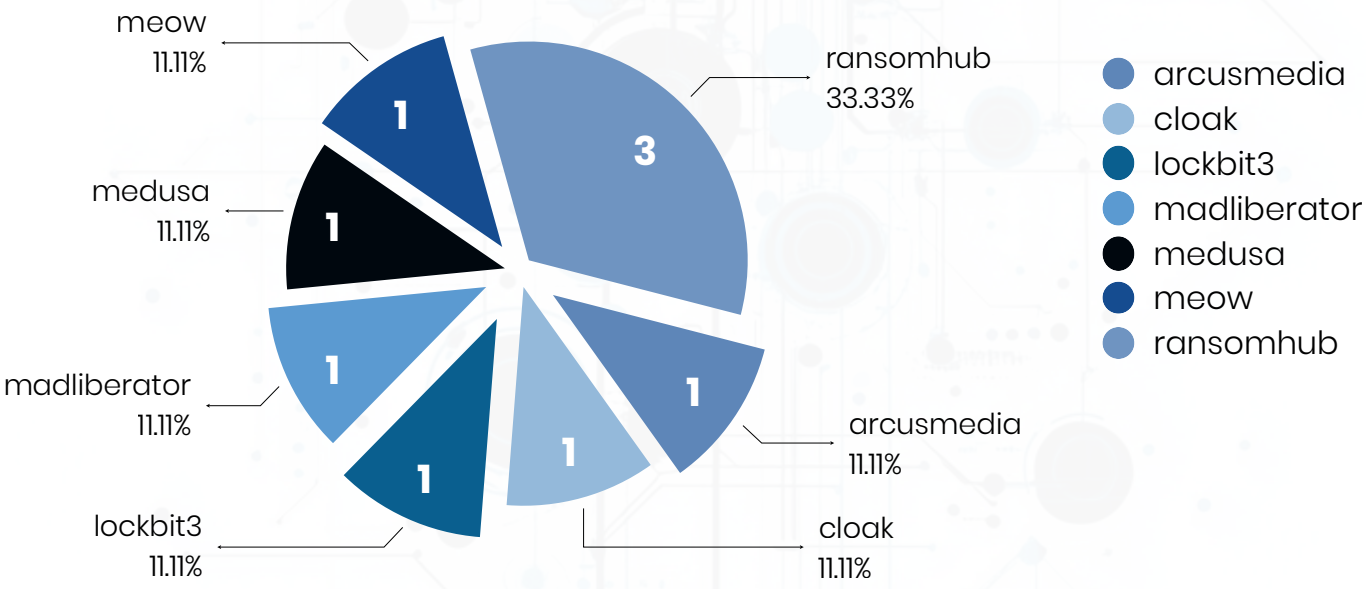
Il **totale dei dati pubblicati** ammonta a **514.40 GB**.

ID	GRUPPO	VITTIMA	DATI PUBBLICATI	LOCALIZZAZIONE
17225	ransomhub	Poker SPA	7.00 GB	Settimo Torinese (TO)
17292	madliberator	CTE Lift SPA	*	Rovereto (TN)
17300	meow	Nocciole Marchisio SPA	**	Cortemilia (CN)
17326	ransomhub	Università degli studi Genova	18.00 GB	Genova
17397	medusa	Tecnolog SRL	439.40 GB	Parma
17405	arcusmedia	Gino Giglio Generation SPA	***	Nola (NA)
17413	ransomhub	La Futura SRL	50.00 GB	Bondeno (FE)
17499	lockbit3	Yesmoke SRL	*	Settimo Torinese (TO)
17613	cloak	Te**********.net	***	-

** la quantità dei dati è sconosciuta*
*** i dati sono in vendita*
**** la rivendicazione è stata rimossa dal sito*

fonte: Ransomfeed, dati settembre 2024

Rispetto al mese di **settembre 2023**, quando gli attacchi rivendicati verso target italiani sono stati **13**, si osserva un **decremento del 30.77%**.



fonte: Ransomfeed, dati settembre 2024

Ogni attacco comporta inevitabilmente **costi rilevanti**: oltre al danno diretto alle prestazioni causato da un ransomware, che si traduce immediatamente in una significativa **perdita economica** (il pagamento del riscatto, l'interruzione delle attività, i costi per la riparazione e il ripristino dei sistemi compromessi), è fondamentale tenere in considerazione anche le **ricadute sociali**, come il danno alla **reputazione** e la perdita di fiducia da parte di clienti e fornitori.

Il **settore terziario industriale** è il più colpito 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 settembre 2024

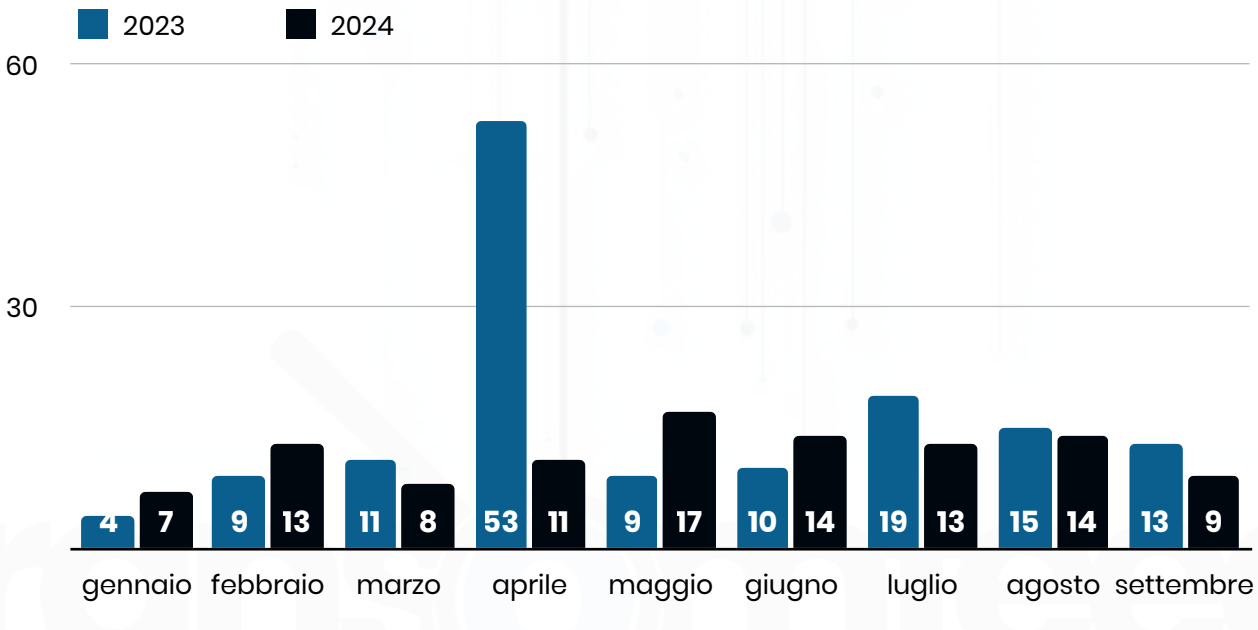
Nella tabella seguente, riportiamo il numero totale di rivendicazioni per ciascun mese e la **quantità complessiva provvisoria** di dati pubblicati dai diversi gruppi ransomware.

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

- **esfiltrati dichiarati** ammonta a **623.40 GB**
- **pubblicati** ammonta a **514.40 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	2398.85 GB
settembre	9	623.40 GB	514.40 GB
totale	**106**	**22665.02 GB**	**19168.95 GB**

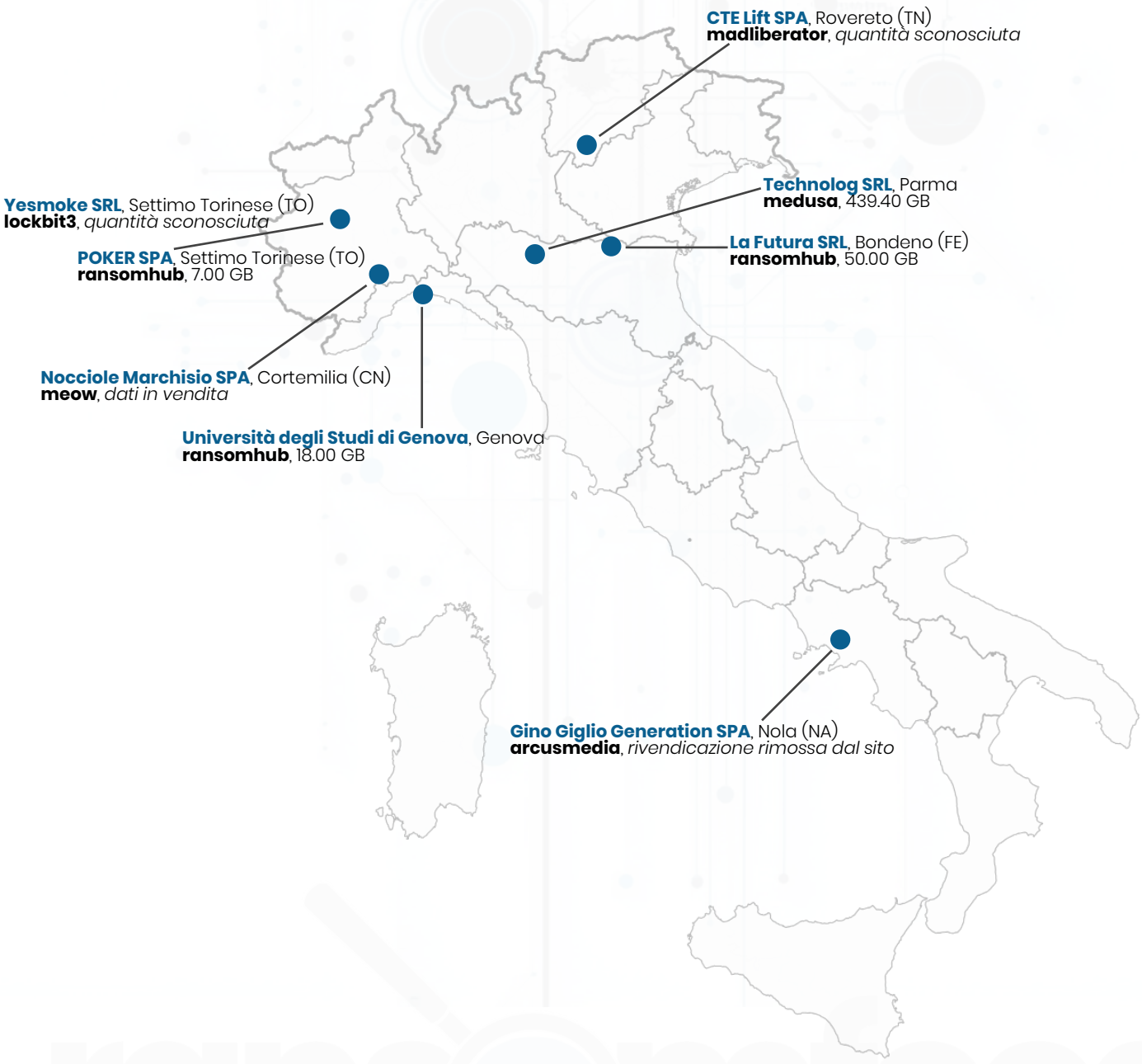
Comparando i dati degli attacchi con quelli dei **primi nove mesi del 2023** (**143** attacchi) si osserva un **decremento del 25.87%**.



fonte: Ransomfeed, dati settembre 2024

Con riferimento al mese di **settembre 2024**, la mappatura degli attacchi ransomware sul territorio evidenzia, ancora una volta, una significativa concentrazione nel **nord** del paese con **4 attacchi**, seguiti da **3 attacchi** al **centro**, **1 attacco** nel **meridione**.
Di un attacco (TE **** .NET di cloak) non siamo riusciti a identificare la localizzazione.

Nonostante il **maggior numero di attacchi** ransomware nel **nord** e **centro** Italia, le misure di sicurezza adottate rimangono **inadeguate**. Molte aziende continuano a investire poco nella protezione informatica, aumentando così la **vulnerabilità a minacce** sempre più gravi.



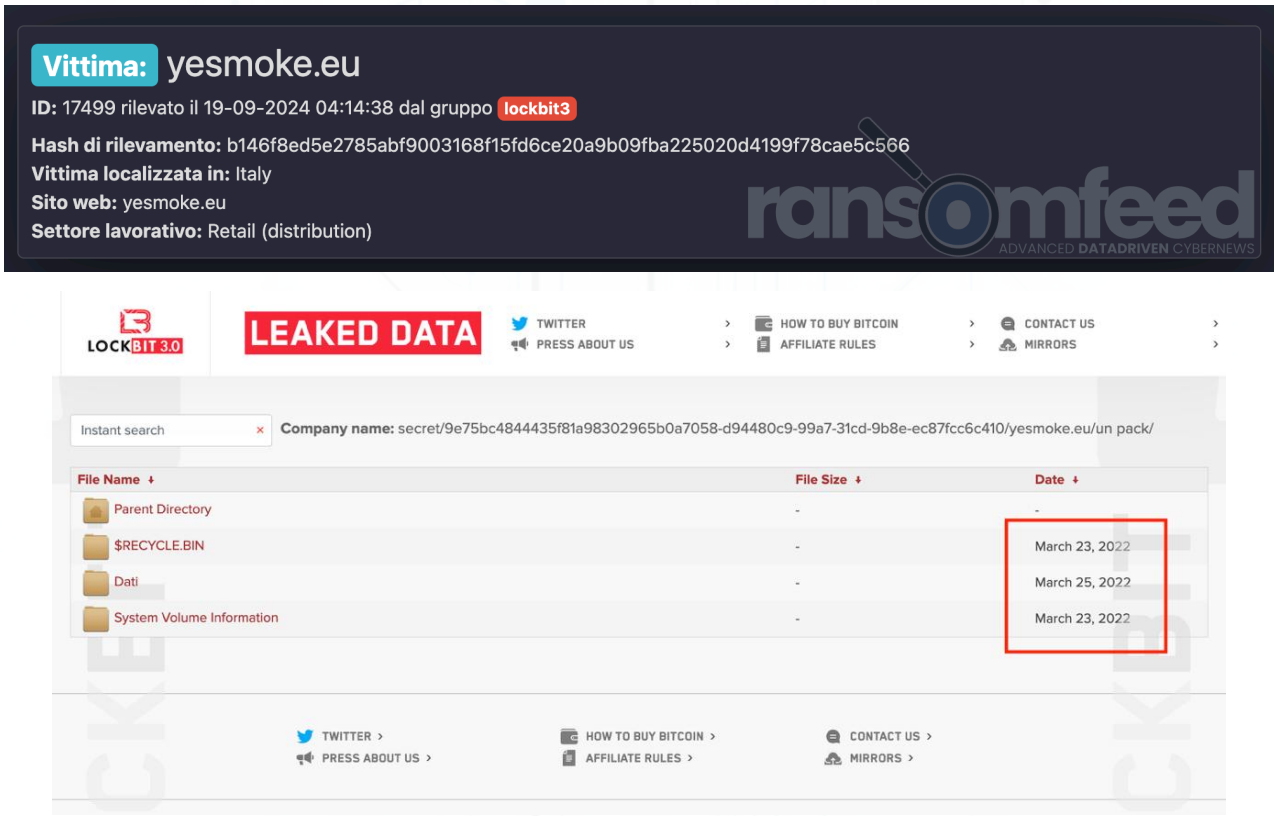
fonte: Ransomfeed, dati settembre 2024

Aggiornamenti

Studio Associato Isolabella: lo studio legale milanese ha subìto un attacco ransomware il 24 agosto scorso, da parte del gruppo criminale **bianlian**. I dati esfiltrati, 1.3TB, sono stati pubblicati il 26 settembre.

L'**Università degli Studi di Genova**, il 9 settembre, ha subìto un'esfiltrazione di dati da parte del gruppo **ransomhub**, poi pubblicati, di 18.00 GB.

Per quanto riguarda l'attacco a **Yesmoke SRL** registrato il 19 settembre, i dati pubblicati risalirebbero al 2022, quindi ancora sotto **lockbit2**.

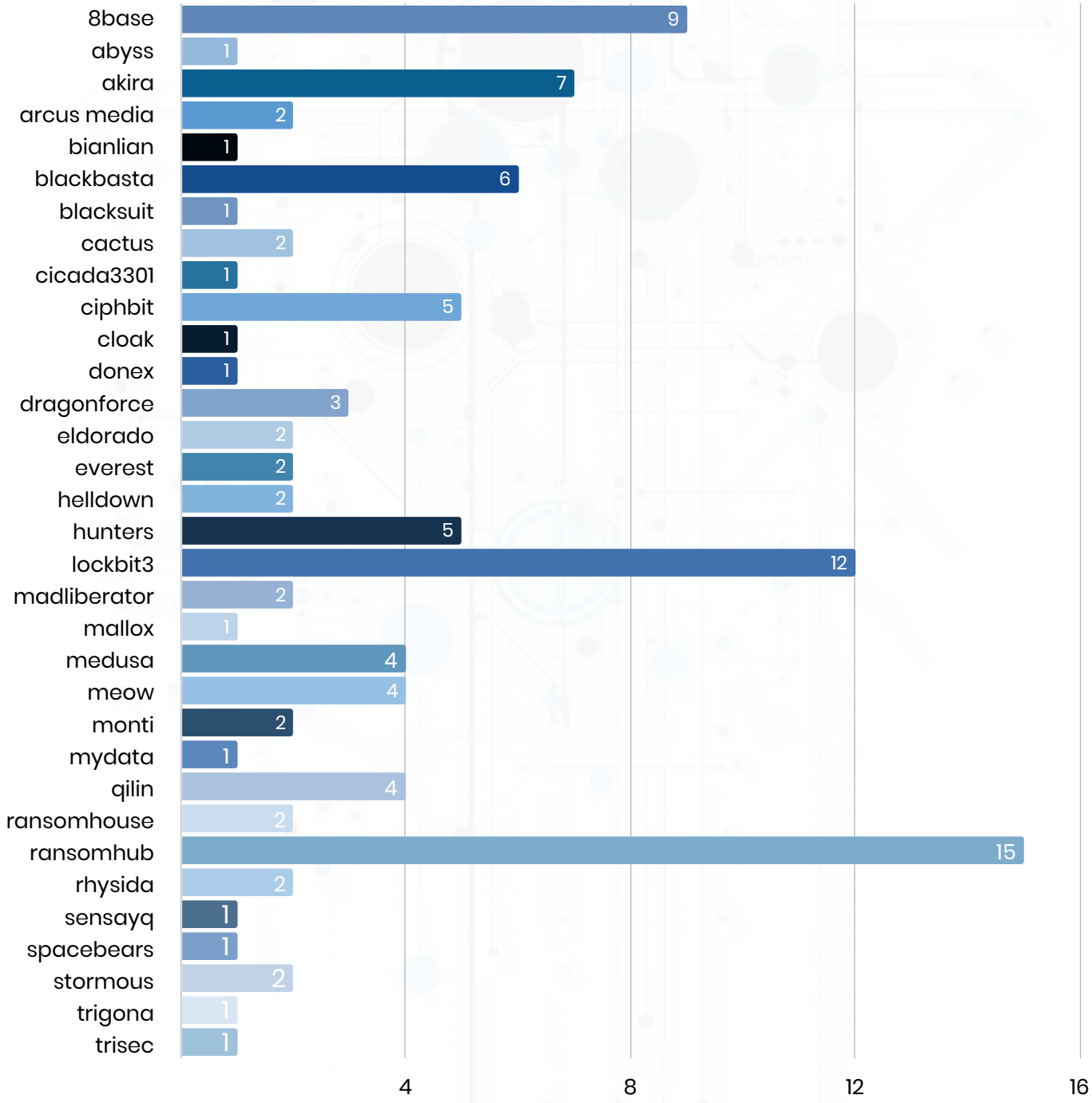


La scelta dei criminali di non comunicare la pubblicazione dei dati esfiltrati si riconduce, innanzitutto, al **massimizzare il profitto** tramite l'estorsione: il silenzio sulla pubblicazione dei dati permette di mantenere la pressione sulla vittima, aumentando le possibilità che questa decida di pagare 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 **106 attacchi**, suddivisi per gruppo criminale (per un totale di **33 gruppi**) **nei primi nove mesi** del 2024.



fonte: Ransomfeed, dati settembre 2024

Focus paesi UE direttiva NIS2 🇪🇺

Nel mese corrente, i **Paesi UE** hanno subito un totale di **56 attacchi.**
I paesi **più colpiti** sono: Spagna (10), Italia e Belgio (9) e Germania (7).

- **Austria**, 0 (0%)
- **Belgio**, 9 (16.07%)
- **Bulgaria**, 0 (0%)
- **Cipro**, 0 (0%)
- **Croazia**, 0 (0%)
- **Danimarca**, 2 (3.58%)
- **Estonia**, 0 (0%)
- **Finlandia**, 0 (0%)
- **Francia**, 4 (7.14%)
- **Germania**, 7 (12.50%)
- **Grecia**, 1 (1.78%)
- **Irlanda**, 0 (0%)
- **Italia**, 9 (16.07%)
- **Lettonia**, 0 (0%)
- **Lituania**, 1 (1.78%)
- **Lussemburgo**, 2 (3.58%)
- **Malta**, 0 (0%)
- **Paesi Bassi**, 1 (1.78%)
- **Polonia**, 2 (3.58%)
- **Portogallo**, 1 (1.78%)
- **Rep. Ceca**, 2 (3.58%)
- **Romania**, 1 (1.78%)
- **Slovacchia**, 0 (0%)
- **Slovenia**, 0 (0%)
- **Spagna**, 10 (17.86%)
- **Svezia**, 3 (5.36%)
- **Ungheria**, 1 (1.78%)

fonte: Ransomfeed, dati settembre 2024

NIS2 in breve

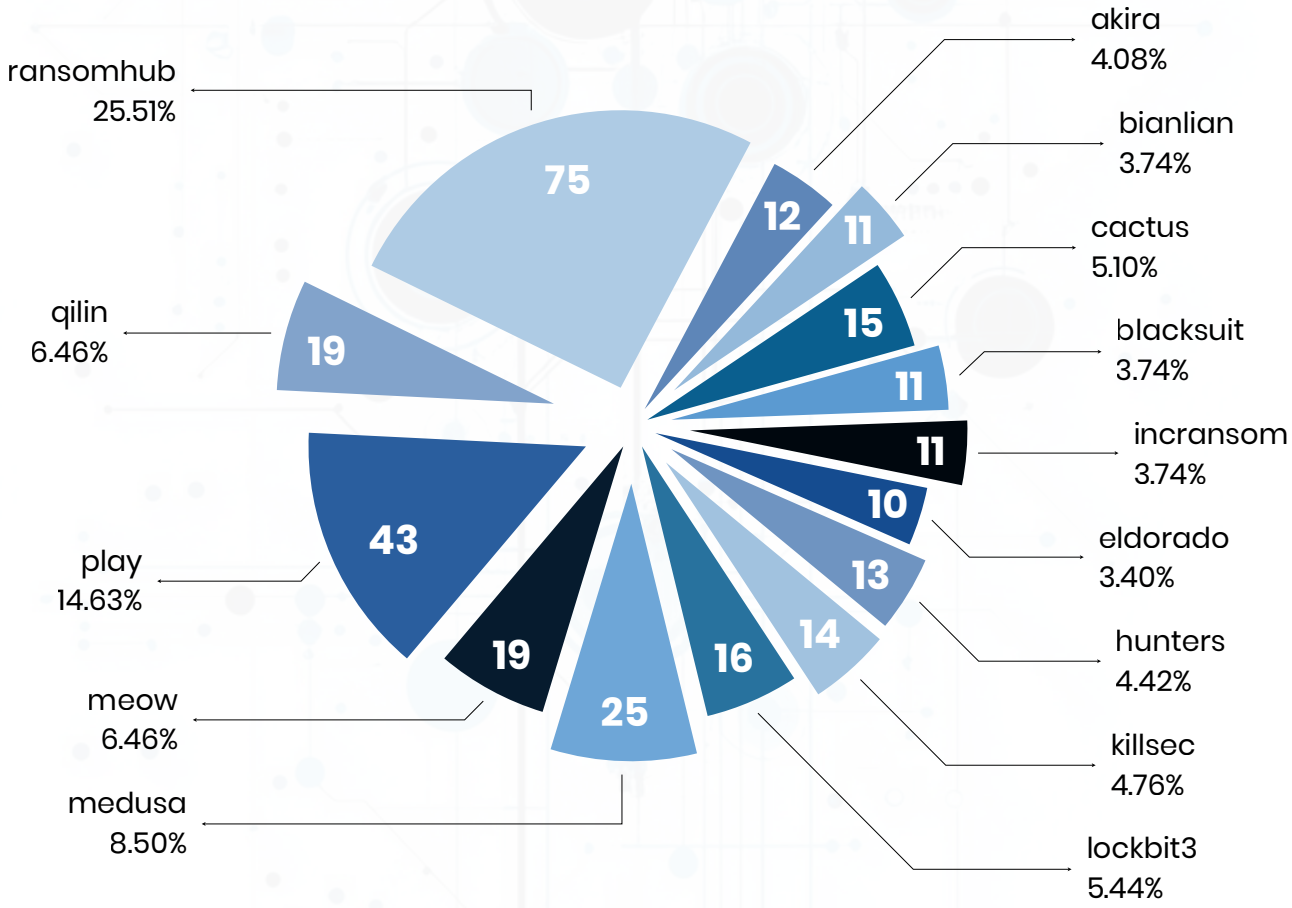
Network and Information Security Directive è la seconda iterazione della Direttiva sulle reti e i sistemi informativi; mira a stabilire un livello più elevato di resilienza informatica all'interno delle organizzazioni dell'Unione Europea, in particolare per gli operatori di infrastrutture critiche e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

Scena internazionale

Nel mese di settembre abbiamo registrato **389 attacchi**. Ne sono stati rilevati **3554** nei primi nove mesi dell'anno, evidenziando un **decremento del 15.06%** rispetto allo stesso periodo dell'anno precedente, quando gli attacchi rivendicati furono 458 su un totale di **3539 nei primi nove mesi**.



fonte: Ransomfeed, gruppi con più di 10 attacchi, dati settembre 2024

27 gruppi con **meno di 10 attacchi** (per un totale di **95** rivendicazioni)

rhysida, 9
arcusmedia, 9
threeam, 7
handala, 6
nitrogen, 6
lynks, 6
dragonforce, 6
cicada3301, 5
cloak, 5
fog, 5
valencialeaks, 5
abyss, 4
stormous, 3
trinity, 3
everest, 2
madliberator, 2
orca, 2
cl0p, 1
ransomhouse, 1
ciphbit, 1
blackbyte, 1
blackout, 1
braincipher, 1
embargo, 1
pryx, 1
ransomexx, 1
spacebears, 1

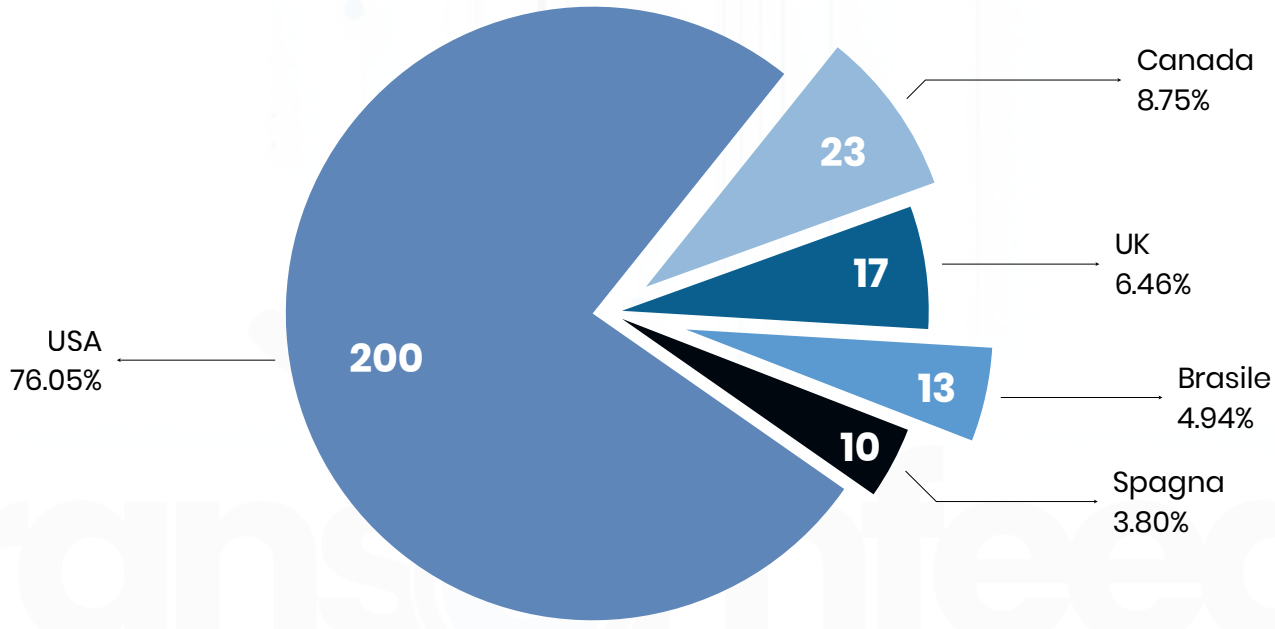
fonte: Ransomfeed, dati settembre 2024

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
settembre	389
totale	**3554**

Rispetto allo stesso periodo dell'anno precedente, in cui gli attacchi ammontavano a **3539**, si osserva un **incremento del 0.42%**.

Nel mese di settembre, gli **Stati Uniti** continuano a essere il paese più colpito, con **200 attacchi** su un **totale di 389**, rappresentando la maggioranza degli incidenti a livello globale. Nel grafico sono considerati i 5 paesi che hanno subito **più di 10 attacchi** (totale 263).



fonte: Ransomfeed, dati settembre 2024

52 paesi con **meno di 10 attacchi** (per un totale di **126** rivendicazioni)

- **Italia**, 9
- **Belgio**, 9
- **Israele**, 8
- **Germania**, 7
- **Australia**, 6
- **India**, 5
- **Giappone**, 5
- **Francia**, 4
- **Norvegia**, 4
- **Messico**, 4
- **Turchia**, 4
- **Svezia**, 3
- **Portorico**, 3
- **Tailandia**, 3
- **Colombia**, 2
- **Argentina**, 2
- **Cina**, 2
- **Danimarca**, 2
- **Indonesia**, 2
- **Filippine**, 2
- **Polonia**, 2
- **UAE**, 2
- **Repubblica Ceca**, 2
- **Lussemburgo**, 2
- **Malesia**, 2
- **Singapore**, 2
- **Svizzera**, 2
- **Taiwan**, 2
- **Bangladesh**, 1
- **Nuova Zelanda**, 1
- **Paesi Bassi**, 1
- **Romania**, 1
- **Arabia Saudita**, 1
- **Corea del Sud**, 1
- **Afganistan**, 1
- **Barbados**, 1
- **Camerun**, 1
- **Cile**, 1
- **Costa Rica**, 1
- **Grecia**, 1
- **Hong Kong**, 1
- **Ungheria**, 1
- **Libano**, 1
- **Lituania**, 1
- **Mauritius**, 1
- **Oman**, 1
- **Pakistan**, 1
- **Paraguay**, 1
- **Portogallo**, 1
- **Senegal**, 1
- **Tunisia**, 1
- **Vietnam**, 1

fonte: Ransomfeed, dati settembre 2024

Nel mese di **settembre 2024** abbiamo registrato in piattaforma **3 nuovi gruppi** ransomware. Precisiamo che l'entrata in piattaforma, e il successivo monitoraggio, non determinano la nascita effettiva di un nuovo gruppo.

Nitrogen (6 attacchi)	**Orca Ransomware** (2 attacchi)
Valencia Leaks (5 attacchi)	

fonte: Ransomfeed, dati settembre 2024

Riepiloghiamo, suddivisi per gruppi, gli attacchi registrati sulla piattaforma dal **1 gennaio** al **30 settembre 2024**; gli **81 gruppi** hanno totalizzato **3554 attacchi**:

0mega, 1
8base, 123
abyss, 33
akira, 164
alphv, 53
apossecurity, 4
apt73, 15
arcusmedia, 35
bianlian, 134
blackbasta, 135
blackbyte, 4
blackout, 8
blacksuit, 104
braincipher, 13
cactus, 89
cicada3301, 31
ciphbit, 10
cloak, 37
cl0p, 20
cuba, 2
daixin, 3
danon, 19
darkvault, 45
donex, 5
donutleak, 10
dragonforce, 76
dunghillleak, 3
eldorado, 29
embargo, 12
everest, 27
flocker, 12
fog, 21
gookie, 2
handala, 28
helldown, 17
hunters, 165
incransom, 122
insane, 1
killsec, 40
knight, 8
lockbit3, 509
lynx, 28
madliberator, 13
malekteam, 3
mallox, 10
medusa, 163
meow, 88
metaencryptor, 9
moneymessage, 3
monti, 25
mydata, 13
nitrogen, 6
noname, 3
orca, 2
play, 260
pryx, 3
qilin, 123
qiulong, 8
ransomcortex, 4
ransomexx, 14
ransomhouse, 43
ransomhub, 292
ransomwareblog, 1
raworld, 30
redransomware, 16
rhysida, 67
sensayq, 2
slug, 1
snatch, 15
spacebears, 32
stormous, 28
threeam, 19
trigona, 19
trinity, 8
trisec, 3
underground, 17
unsafe, 2
valencialeaks, 5
vanir, 3
werewolves, 3
zerotolerance, 1

fonte: Ransomfeed, dati settembre 2024

Chi siamo

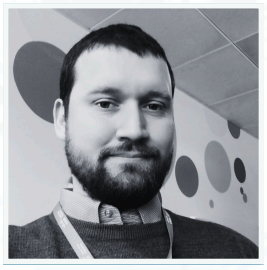
Dario Fadda
co-founder
dev maintainer

Claudio Sono
co-founder
OSINT maintainer

Claudia Galingani Mongini
digital strategy
OSINT, HUM/SOCMINT

Matteo
backend developer
frontend maintainer

Federico Fuga
backend developer
frontend maintainer



Federico Marsili
OSINT researcher

Alessandro Chitolina
full stack developer
solution architect

Christian Bernieri
DPO

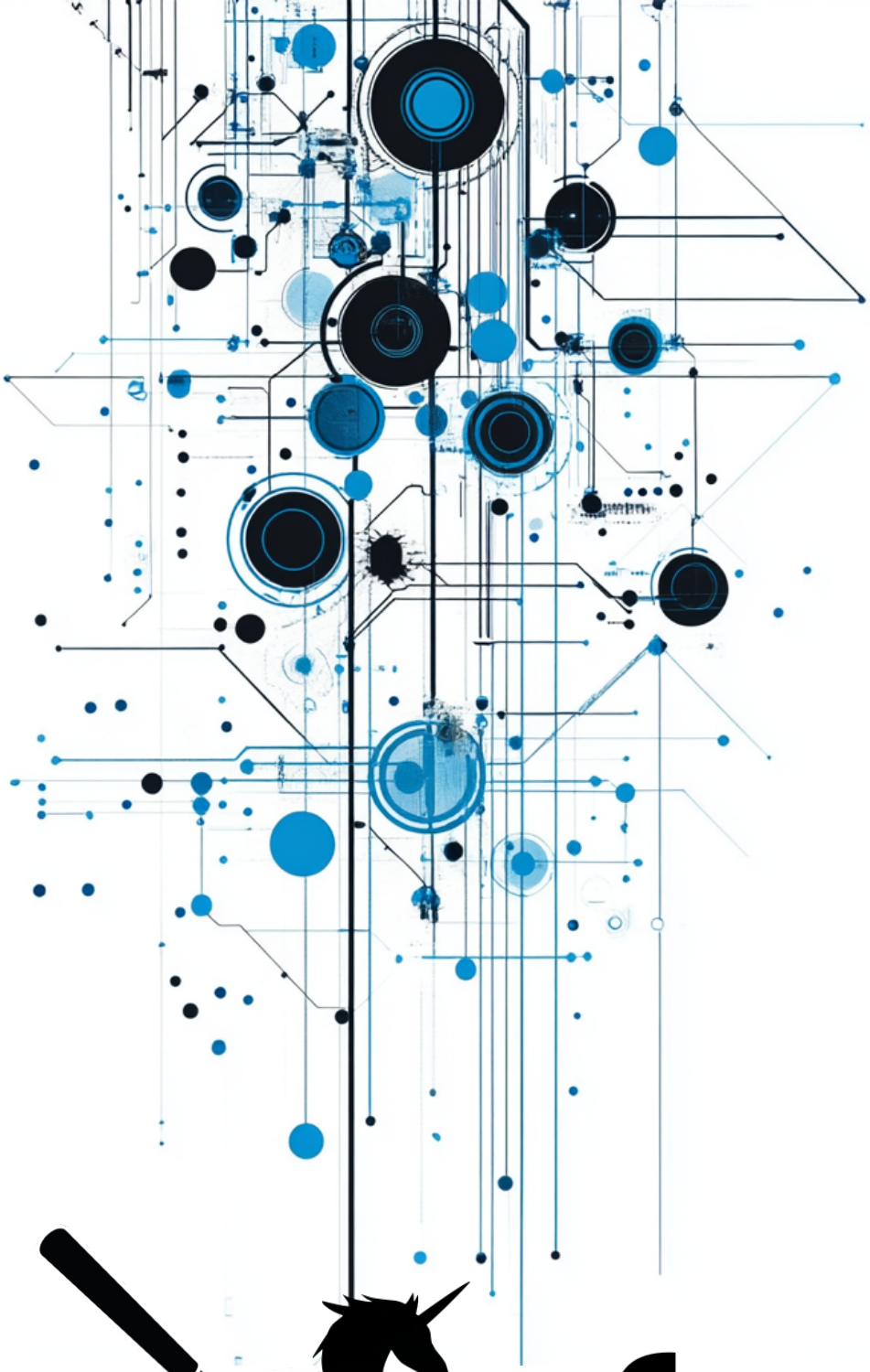
contributor
privacy policy

Massimo Giaimo
Würth Phoenix

enrichment su settori
lavorativi

Edoardo Limone
consulente cyber

sostenitore e promotore
del progetto



ransomfeed

ADVANCED **DATADRIVEN** CYBERNEWS

SETTEMBRE 2024

/eof