ADVANCED **DATADRIVEN** CYBERNEWS

RECAP MENSILE
MAGGIO 2024

ver. glitch256_u05 - 25 giugno 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 classico **report quadrimestrale**, anche un recap mensile, con una particolare attenzione agli attacchi italiani. Crediamo sia importante fornire, in un segmento di tempo meno ampio, un riassunto di quelle che sono state le vittime degli attacchi e la loro portata, insieme ad altri dati statistici - sempre 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/rising

Focus Italia 🇮🇹

Nel mese di **maggio 2024** la piattaforma ha registrato un totale di **17 attacchi**, per la maggior parte localizzati nel **nord Italia**.

Il **totale dei dati pubblicati** ammonta a **4429.10 GB**.

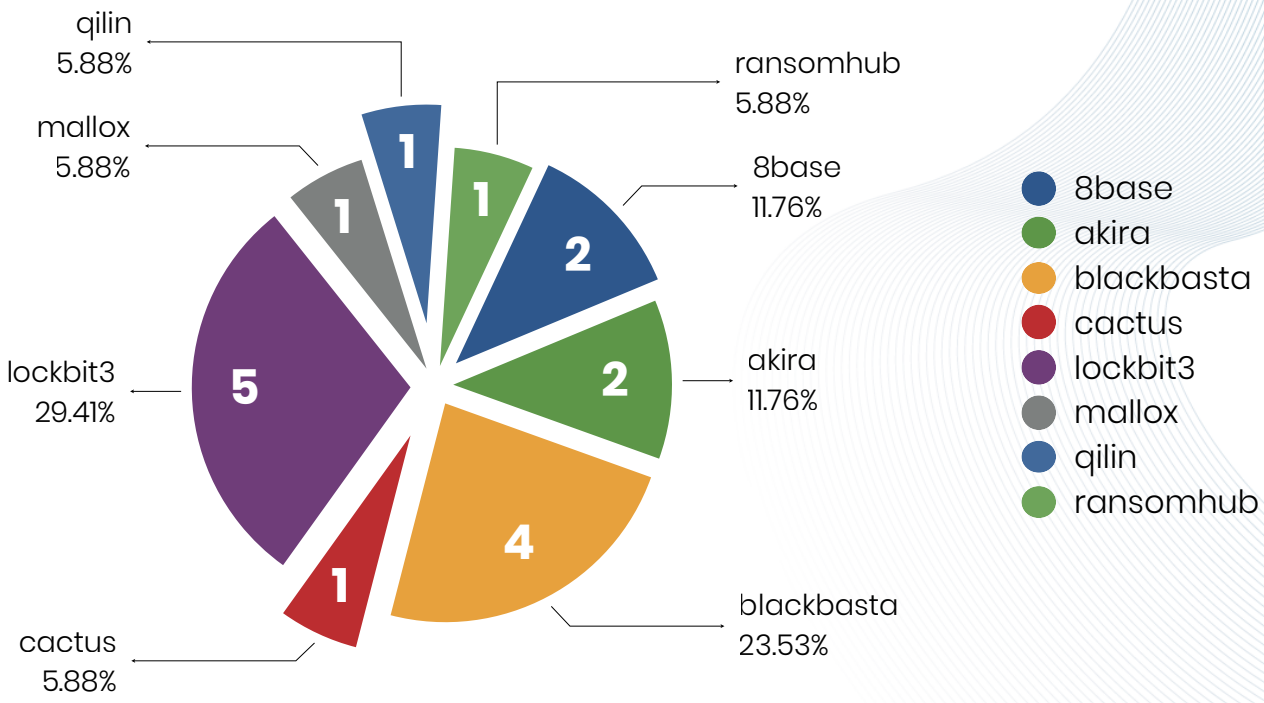
ID	GRUPPO	VITTIMA	DATI PUBBLICATI	LOCALIZZAZIONE
15159	blackbasta	T.E.A. SPA		Mantova
15161	blackbasta	Synlab Italia		Monza
15163	blackbasta	GAI SPA		Ceresole d'Alba
15293	lockbit3	Agencavi Systems		Rodano
15297	lockbit3	Giovanni Randi SPA		Faenza
15300	lockbit3	Orsini Group Div. Imballaggi		Roma
15312	lockbit3	Interfashion Intermoda SPA		Rimini
15400	8base	Costa Edutainment SPA		Ceriale
15402	8base	Brovedani Group		S. Vito Tagliamento
15426	akira	Bruno Generators		Grottaminarda
15458	qilin	FIAB SPA		Vicchio
15506	lockbit3	Università di Siena		Siena
15527	blackbasta	MF Group		Monzuno
15602	mallox	Assist Informatica *	non disponibili	non disponibile
15631	ransomhub	SIAED SPA **		Roma
15668	akira	MagicLand SPA		Valmontone
15680	cactus	Dollmar SPA		Caleppio di Settala

fonte: Ransomfeed, dati maggio 2024

** la rivendicazione è stata rimossa dal DLS del gruppo mallox. La localizzazione del target non era disponibile; avendo riscontrato un caso di omonimia e, in assenza di altri indizi, non abbiamo potuto inserire una località certa.*

*** la rivendicazione è stata rimossa dal DLS del gruppo ransomhub e, di conseguenza, i dati non risultano pubblicati.*

Rispetto al mese di **maggio 2023**, in cui gli attacchi rivendicati contro target italiani sono stati **9**, si osserva un **incremento del 88.88%**.



fonte: Ransomfeed, dati maggio 2024

Nella tabella successiva, evidenziamo la totalità delle rivendicazioni per mesi e la relativa **quantità totale provvisoria dei dati pubblicati** dai gruppi ransomware.

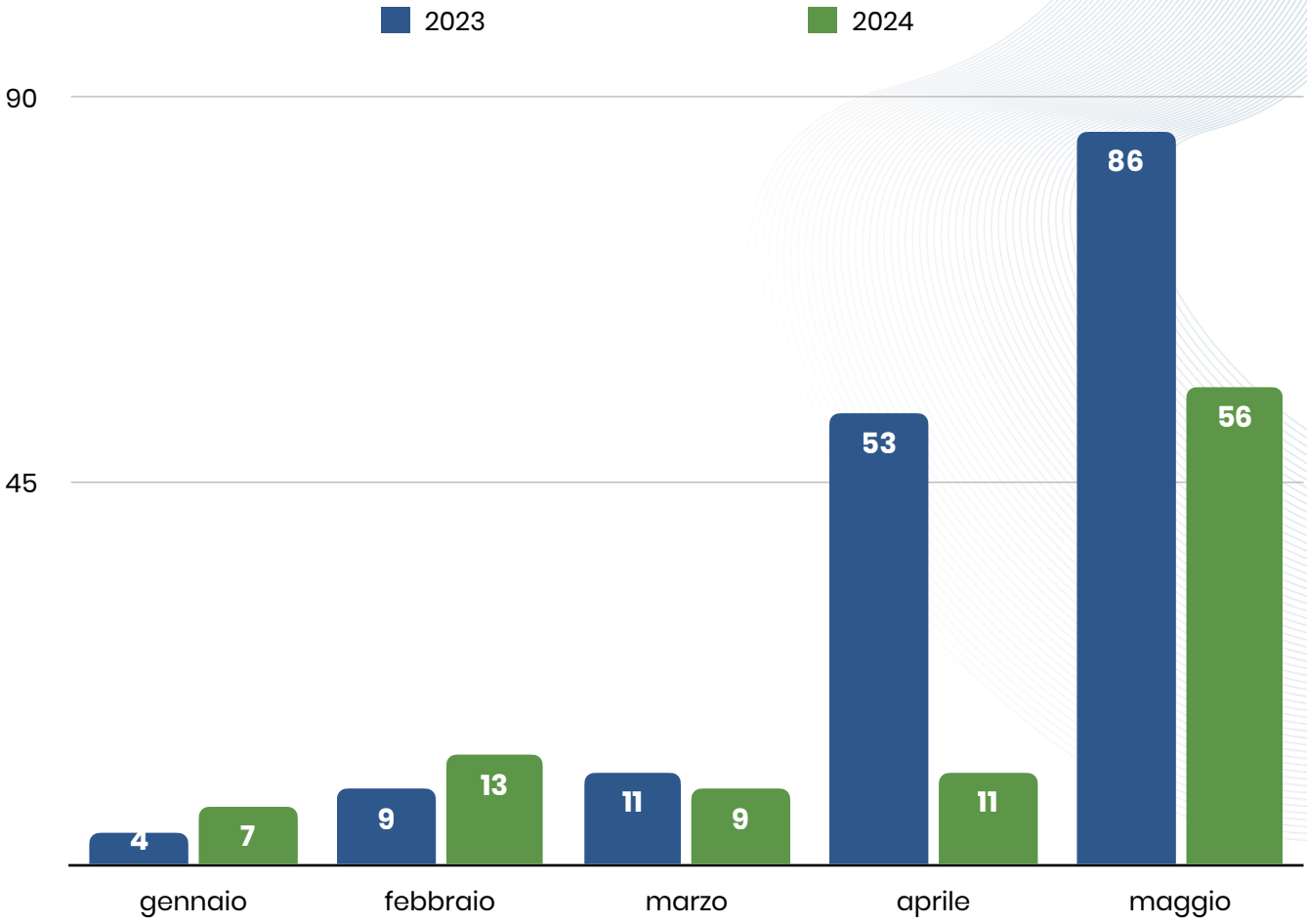
Nei primi cinque mesi dell'anno, il totale dei dati:

- **esfiltrati dichiarati** ammonta a **12092.20 GB**
- **pubblicati** ammonta a **9669.33 GB**

MESE	RIVENDICAZIONI	DATI DICHIARATI	DATI PUBBLICATI
gennaio	7	599.70 GB	599.70 GB
febbraio	13	1814.10 GB	1842.10 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
totale	**56**	**12092.90 GB**	**9669.33 GB**

Nel prossimo recap riporteremo le quantità dei dati aggiornate, se disponibili.

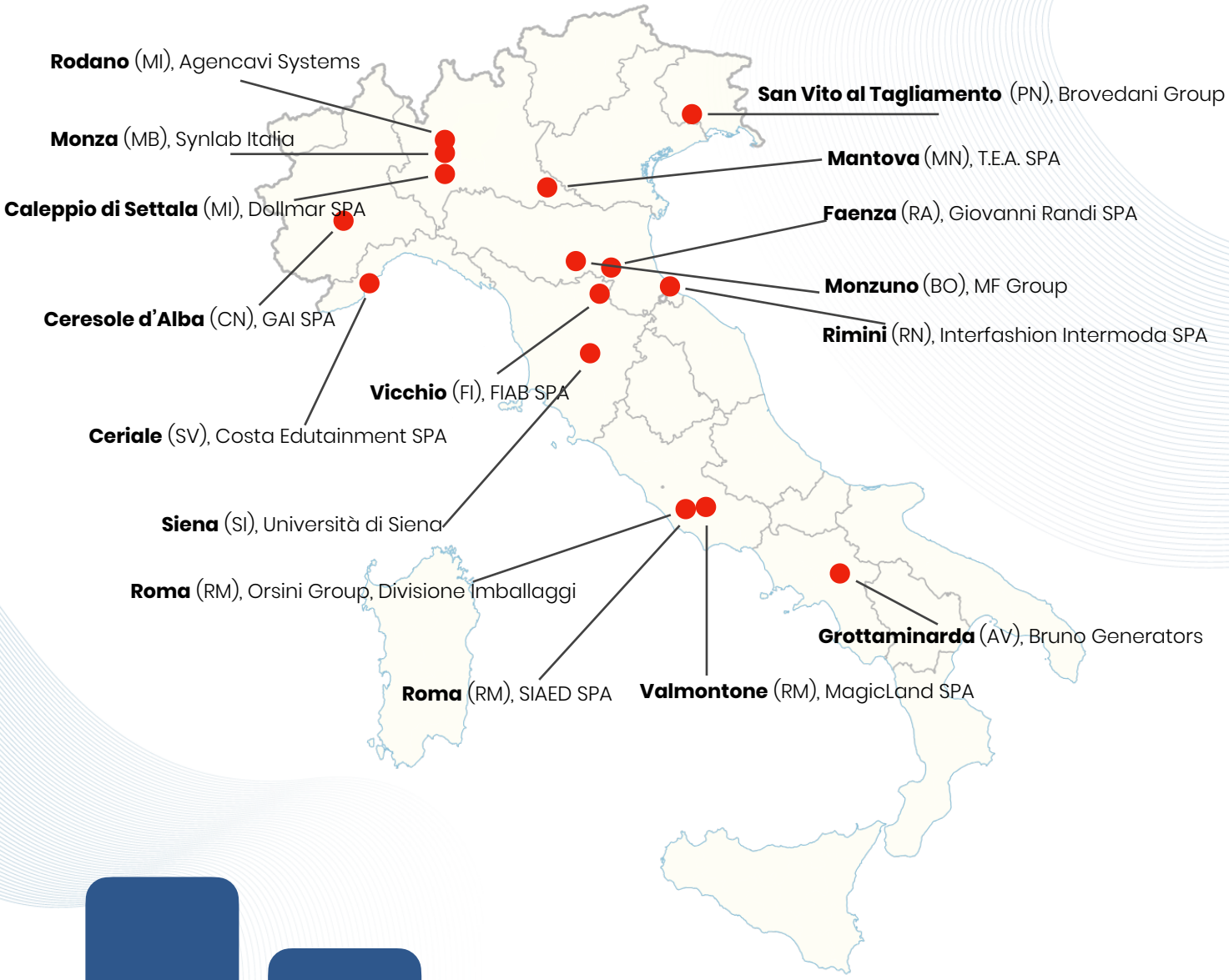
Comparando i dati con i **primi cinque mesi dell'anno precedente**, in cui gli attacchi rivendicati verso target italiani sono stati **86**, si osserva un **decremento del 34.88%**.

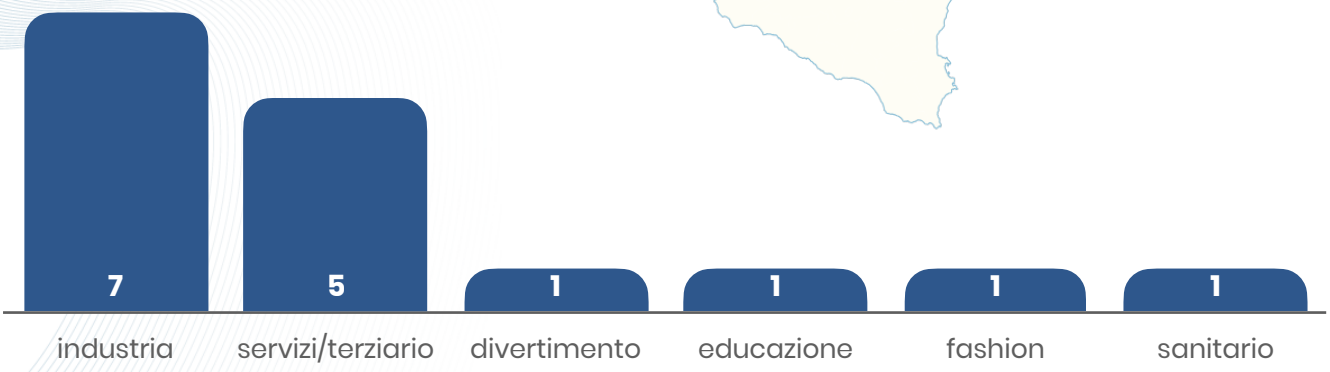


fonte: Ransomfeed, dati maggio 2024

Sempre con riferimento al mese di maggio, la **mappatura** degli attacchi ransomware sul territorio evidenzia, ancora una volta, una significativa **concentrazione nel nord** del Paese (11 attacchi), a seguire il **centro** (5 attacchi) ed infine il **sud** (1 attacco), in regioni economicamente sviluppate e industrializzate.

La rivendicazione di **Assist Informatica** (ctf Ransomfeed) non è presente sulla mappa in quanto non è stato possibile localizzarla con il solo lavoro di OSINT; sul DLS di mallox non è più presente alcun riferimento all'attacco e non è stato possibile risalire all'esatto posizionamento geografico.

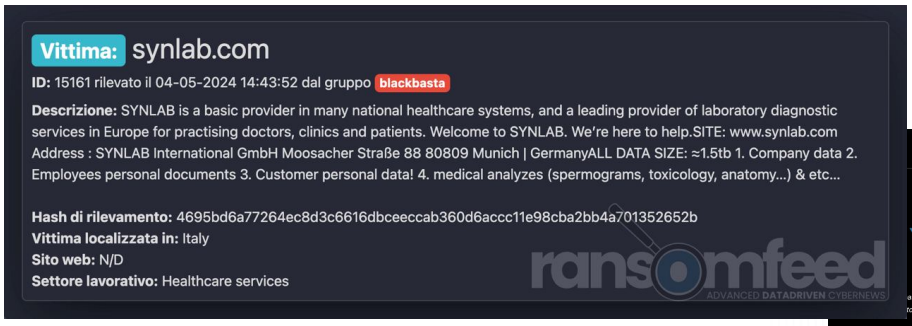


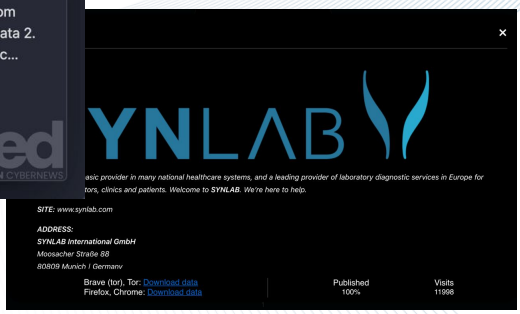


fonte: Ransomfeed, dati maggio 2024

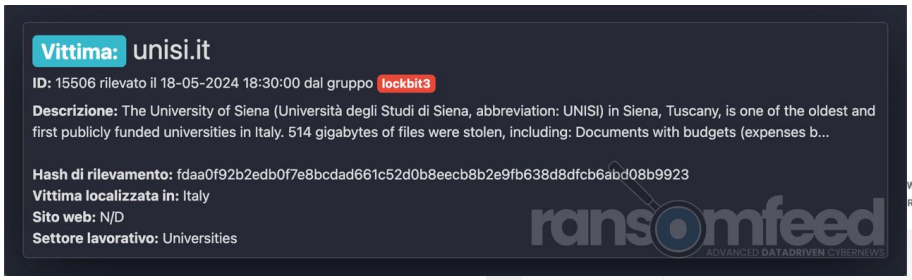
🚨 Aggiornamenti

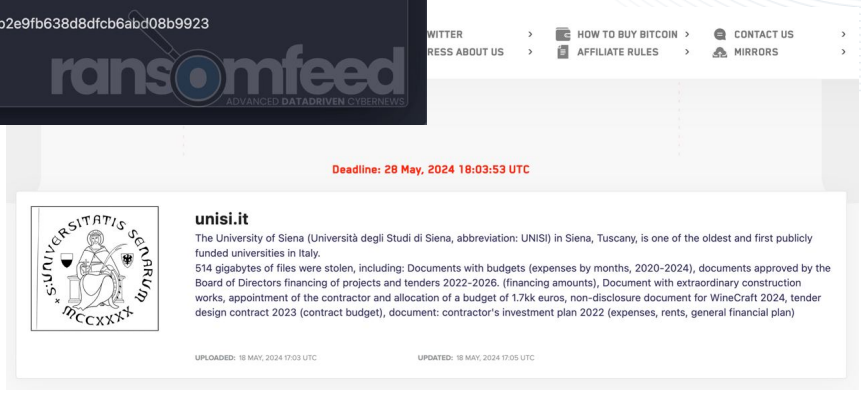
I dati di **Synlab Italia**, dopo il breach e la conseguente esfiltrazione del 18 aprile 2024 scorso, sono stati pubblicati in data 11 maggio. L'ammontare complessivo è di 1.5 TB.





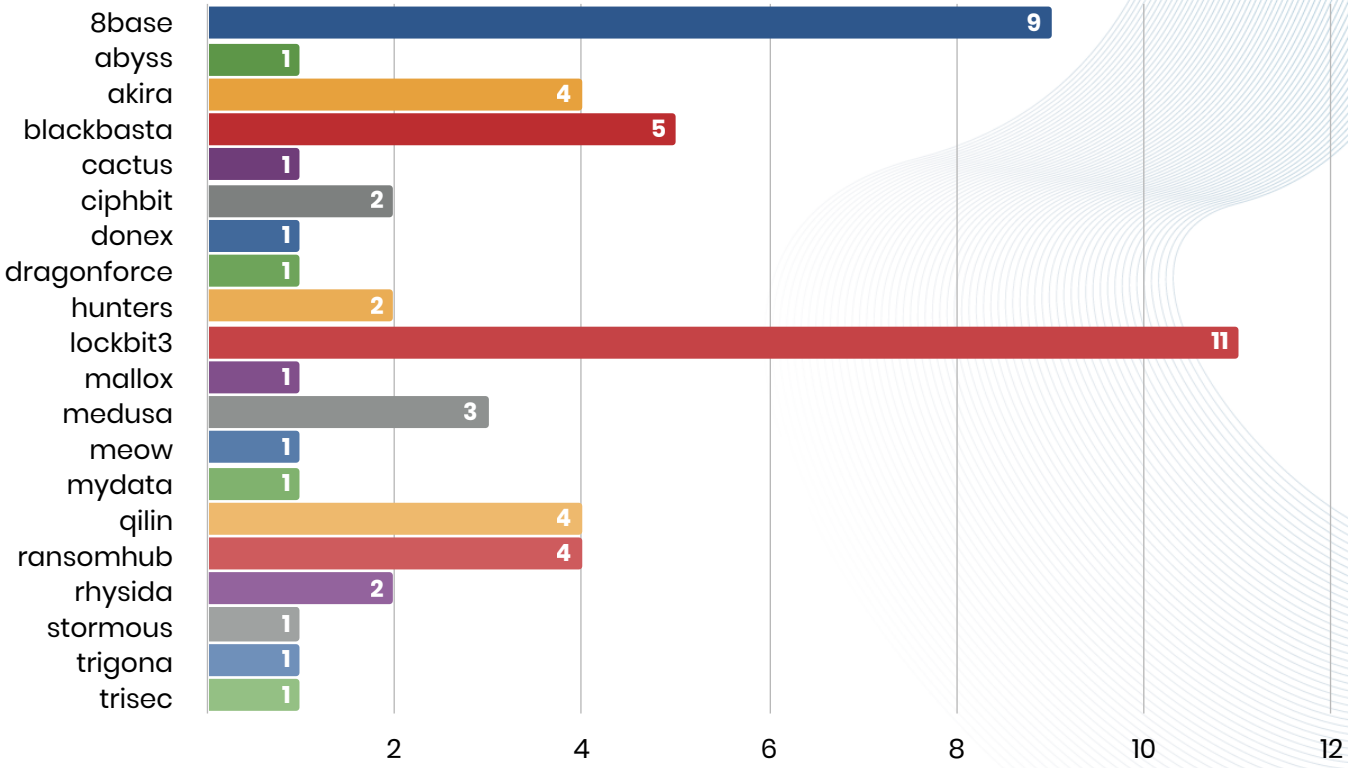
Anche l'**Università di Siena**, colpita dal gruppo **lockbit3** il 18 maggio, ha visto i propri dati pubblicati (**514 GB**); tuttavia sul DLS del threat actor, i dati interessati non risultano presenti. Nota positiva è stata la comunicazione trasparente e tempestiva verso gli utenti da parte dell'università.





Diamo conto della situazione di **SIAED SPA**: l'azienda ha subìto un breach con **esfiltrazione** di **1.6TB di dati**, il 27 maggio. Il gruppo criminale ransomhub ha successivamente rimosso la rivendicazione dal proprio DLS, si presume che il gruppo abbia pagato il riscatto.

Uno spaccato dei **56 attacchi**, suddivisi per gruppo criminale (per un totale di **20 gruppi**), **dal 1 gennaio fino al 31 maggio 2024**.



fonte: Ransomfeed, dati maggio 2024

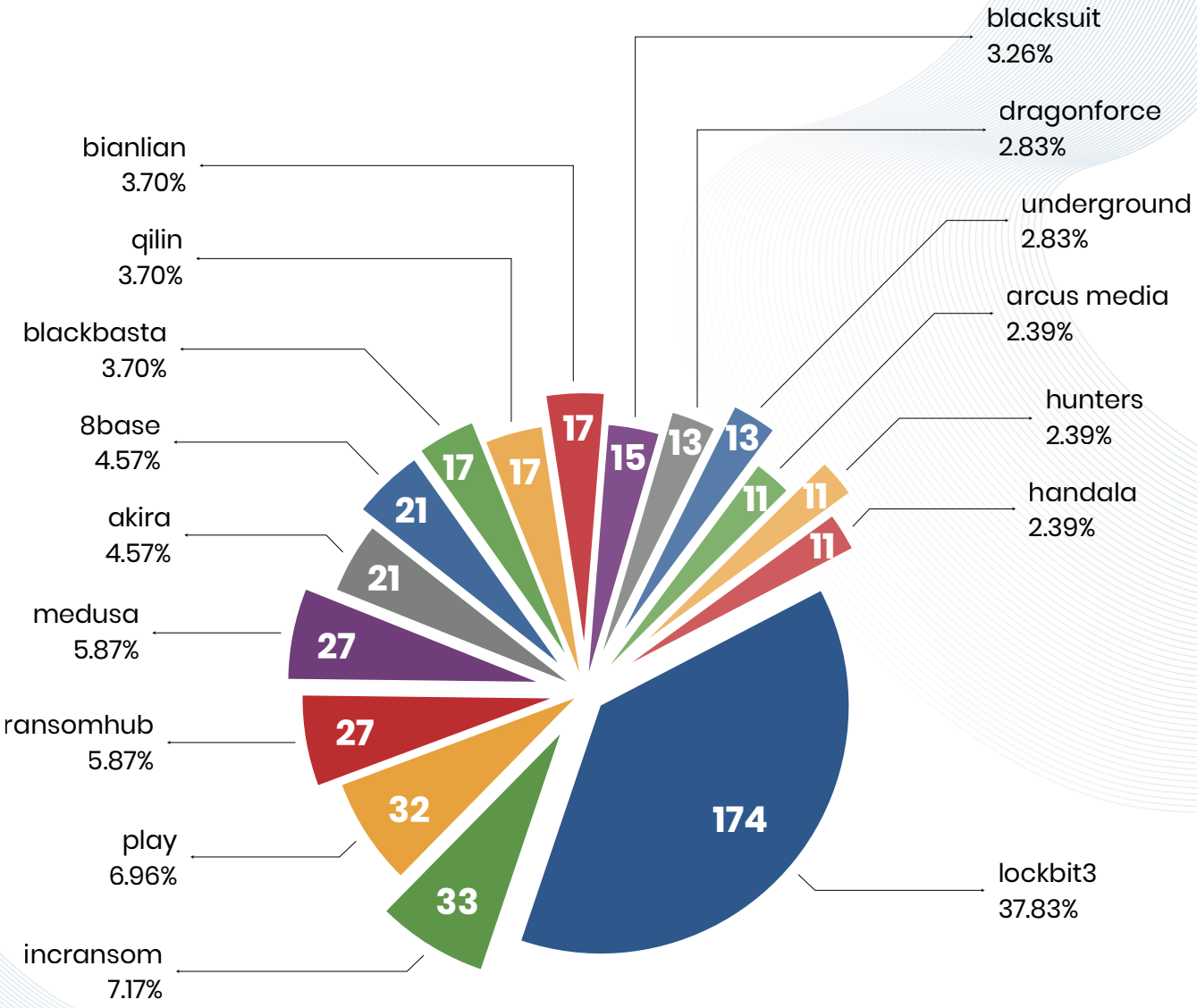
È chiaro che **lockbit3** sia, nel periodo considerato, il gruppo più attivo, con il numero più alto di attacchi (11), nonostante le operazioni delle forze dell'ordine abbiano più volte cercato di fermarli; non da meno **8base** (9 attacchi), con un trend consolidato.

I gruppi con un maggior numero di attacchi tendono a **dominare la scena ransomware** grazie alle loro risorse, competenze e reti consolidate; da non sottovalutare l'ondata di nuovi affiliati dopo l'uscita di ALPHV/BlackCat.

Si presume che lockbit3 abbia **aggiunto alla sua rete di affiliati** gruppi come *medusa*, *qilin*, *blackbasta* e molti dei loro sub-affiliati. Sul loro canale di comunicazione le rivendicazioni, così come le informazioni riguardanti alcuni dettagli degli attacchi, vengono costantemente ri-condivise.

Scena internazionale

Sono **558** gli attacchi rilevati nel mese di **maggio 2024**; rispetto allo stesso periodo dell'anno precedente (**411 attacchi** rivendicati), rileviamo un **incremento del 26.53%**.



27 gruppi con **meno di 10 attacchi** (per un totale di **87** rivendicazioni)

cactus, 7
clop, 7
everest, 6
rhysida, 6
danon, 5
ra world, 5
apt73, 4
metaencryptor, 4
flocker, 4
monti, 4
darkvault, 3
cloak, 3
embargo, 3
spacebears, 2
redransomware, 2
donutleak, 2
killsec, 2
snatch, 2
threeam, 2
mallox, 1
abyss, 1
moneymessage, 1
blackout, 1
meow, 1
qiulong, 1
ransomware, 1
zero tolerance, 1

fonte: Ransomfeed, dati maggio 2024

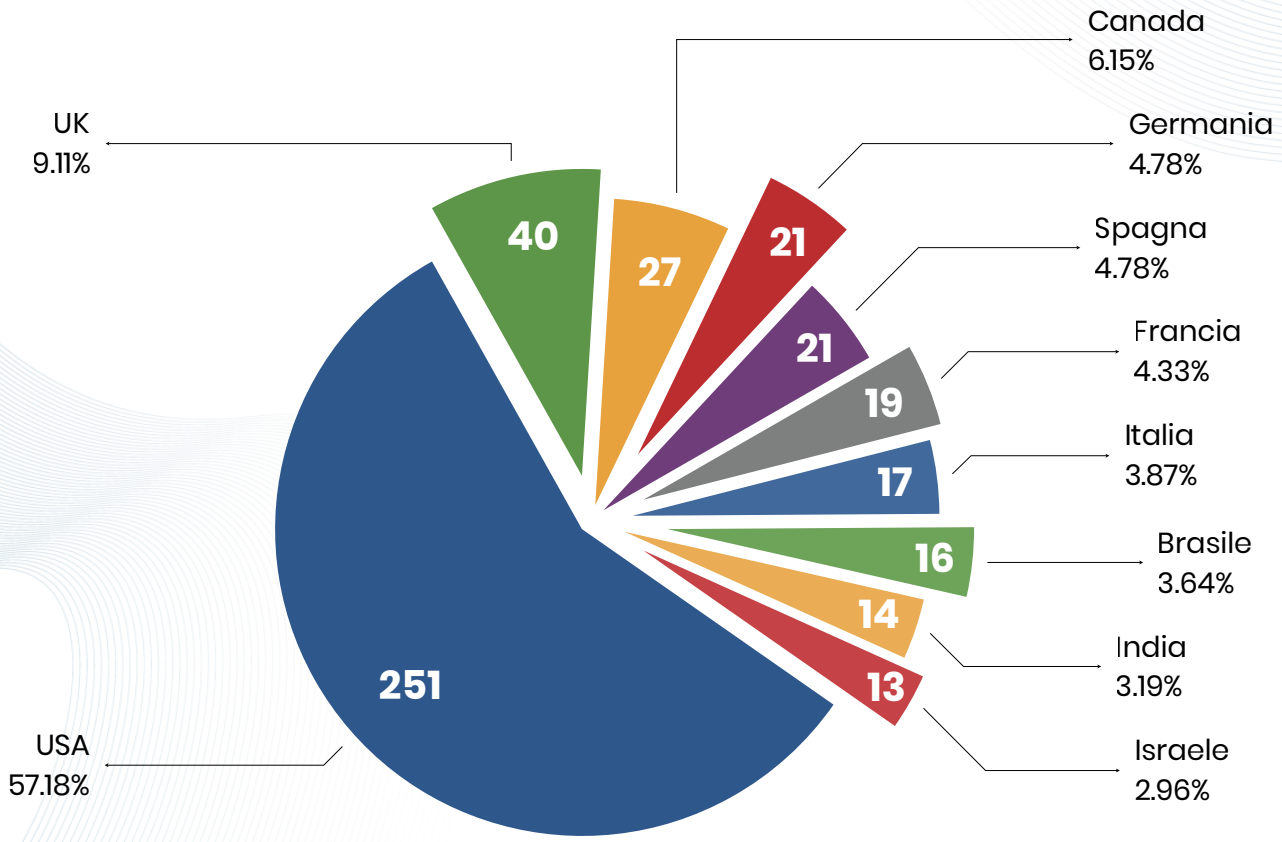
Anche per la scena internazionale, pubblichiamo la tabella con il numero **totale delle rivendicazioni** (al netto degli eventuali duplicati che potrebbero essere rilevati nei mesi successivi).

MESE	RIVENDICAZIONI
gennaio	284
febbraio	373
marzo	383
aprile	379 *
maggio	558
totale	**1977**

** dato aggiornato rispetto al report di aprile 2024*

Comparato con lo stesso **periodo dell'anno precedente**, in cui gli attacchi ammontavano a **1767**, si osserva un **incremento del 11.88%**.

Analizzando la distribuzione geografica, nel **mese di maggio** gli **Stati Uniti** risultano essere ancora la nazione più colpita con **251 attacchi**.



nel grafico sono considerati tutti i paesi che hanno subito più di 10 attacchi

54 paesi con **meno di 10 attacchi** (per un totale di **115** rivendicazioni)

- **UAE**, 8
- **Messico**, 8
- **Argentina**, 7
- **Belgio**, 7
- **Giappone**, 6
- **Colombia**, 4
- **Repubblica Ceca**, 4
- **Singapore**, 4
- **Svezia**, 3
- **Svizzera**, 3
- **Polonia**, 3
- **Cile**, 3
- **Irlanda**, 3
- **Non Disponibile**, 3
- **Australia**, 2
- **Corea del Sud**, 2
- **Taiwan**, 2
- **Turchia**, 2
- **Austria**, 2
- **Filippine**, 2
- **Sud Africa**, 2
- **Cina**, 2
- **Egitto**, 2
- **Indonesia**, 2
- **Slovacchia**, 2
- **Tailandia**, 2
- **Vietnam**, 2
- **Danimarca**, 1
- **Paesi Bassi**, 1
- **Portogallo**, 1
- **Croazia**, 1
- **Afganistan**, 1
- **Bahamas**, 1
- **Bangladesh**, 1
- **Costarica**, 1
- **Finlandia**, 1
- **Georgia**, 1
- **Iran**, 1
- **Costa d'Avorio**, 1
- **Kuwait**, 1
- **Namibia**, 1
- **Nepal**, 1
- **Nigeria**, 1
- **Norvegia**, 1
- **Perù**, 1
- **Portorico**, 1
- **Romania**, 1
- **St. Vincent e Grenadine**, 1
- **Arabia Saudita**, 1
- **Senegal**, 1
- **Serbia**, 1
- **Sri Lanka**, 1
- **Trinidad e Tobago**, 1
- **Isole Vergini**, 1

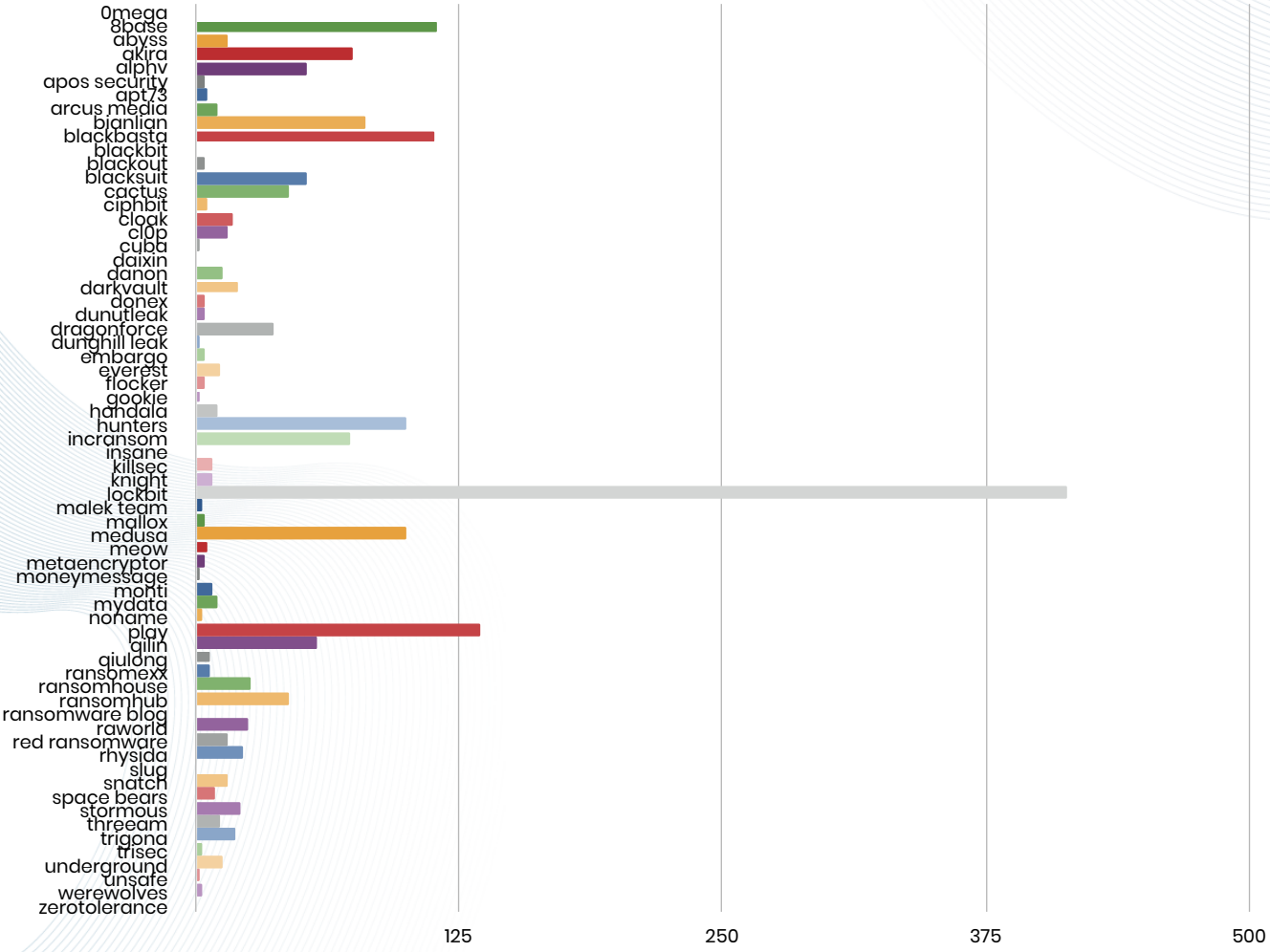
fonte: Ransomfeed, dati maggio 2024

Nel mese di **maggio 2024** abbiamo registrato in piattaforma **6 nuovi gruppi** ransomware; precisiamo che l'entrata in piattaforma e il successivo monitoraggio, non determinano la nascita effettiva di un nuovo gruppo.

Arcus Media	Ransomware Blog (Medusa Locker)
FSociety Locker	The Underground
Handala	Zero Tolerance

Infine, riepiloghiamo, suddivisi per gruppi, gli attacchi registrati sulla piattaforma dal **1 gennaio al 31 maggio 2024**; i **66 gruppi** hanno totalizzato **1977 attacchi**:

0mega, 1
8base, 115
abyss, 15
akira, 96
alphv, 53
apos security, 4
apt73, 6
arcus media, 11
bianlian, 81
blackbasta, 113
blackbit, 1
blackout, 4
blacksuit, 53
cactus, 44
ciphbit, 6
cloak, 18
cl0p, 16
cuba, 2
daixin, 1
danon, 13
darkvault, 20
donex, 5
donutleak, 5
dragonforce, 37
dunghill leak, 2
embargo, 5
everest, 12
flocker, 4
gookie, 2
handala, 11
hunters, 100
incransom, 74
insane, 1
killsec, 8
knight, 8
lockbit3, 413
malek team, 3
mallox, 5
medusa, 100
meow, 10
metaencyptor, 4
moneymessage, 2
monti, 8
mydata, 11
noname, 3
play, 135
qilin, 58
qiulong, 7
ransomexx, 7
ransomhouse, 26
ransomhub, 72
ransomware blog, 1
raworld, 25
red ransomware, 15
rhysida, 23
slug, 1
snatch, 15
space bears, 10
stormous, 22
threeam, 12
trigona, 19
trisec, 3
underground, 13
unsafe, 2
werewolves, 3
zerotolerance, 1



fonte: Ransomfeed, dati maggio 2024

ADVANCED **DATADRIVEN** CYBERNEWS

RECAP MENSILE
MAGGIO 2024

/eof