ADVANCED **DATADRIVEN** CYBERNEWS

RECAP MENSILE
APRILE 2024

ver. glitch256_u09 - 10 maggio 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.

Focus Italia 🇮🇹

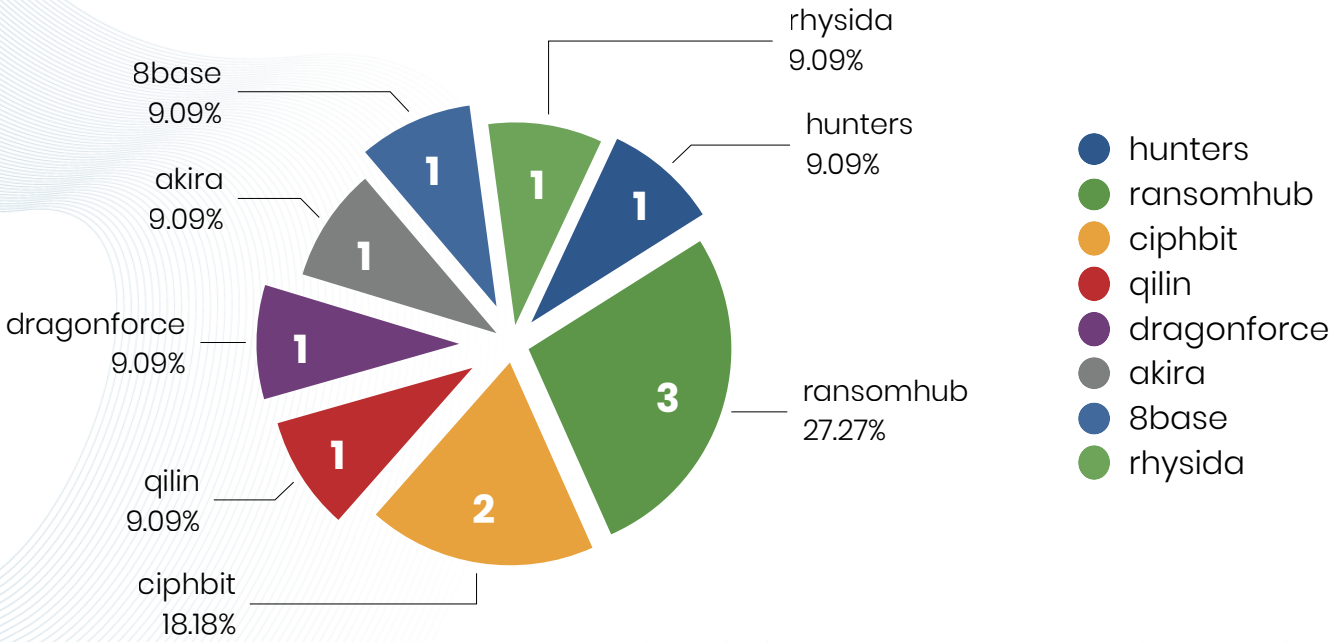
Nel mese di **aprile 2024** la piattaforma ha registrato un totale di **11 attacchi**, per la maggior parte localizzati nel **nord Italia**.

Il **totale dei dati pubblicati** ammonta a **2624.33 GB**.

ID	GRUPPO	VITTIMA	DATI PUBBLICATI	LOCALIZZAZIONE
14104	hunters	Olimpias (Benetton Group)	433.70 GB	Treviso
14138	ransomhub	Carrozzeria Aretusa SRL	90.00 GB	Milano
14144	ciphbit	Termoplastic SRL	28.26 GB	Pomezia
14162	ransomhub	Farmacia Ettore Florio	200.00 GB	Napoli
14168	qilin	Maccarinelli SRL	29.00 GB	Paitone
14170	ciphbit	Macuz & C. SNC	87.14 GB	Firenze
14198	dragonforce	New Concept Production SRL	19.23 GB	Imola
14317	akira	Studio Lambda SRL	non disponibili	Matera
14343	ransomhub	Mercatino SRL*	1500 GB	Verona
14932	8base	FEB31st	non disponibili	Brembilla
14979	rhysida	CDS Hotels**	237.00 GB	Lecce

** la rivendicazione è stata rimossa dal DLS del gruppo ransomhub e, con essa, anche i dati*
*** i dati pubblicati sono parziali rispetto ai dati esfiltrati dichiarati*

Rispetto ad **aprile 2023**, in cui gli attacchi rivendicati contro target italiani sono stati **53**, si osserva un **decremento del 79.25%**.



fonte: Ransomfeed, dati aprile 2024

Abbiamo evidenziato, nella tabella sottostante, la totalità delle rivendicazioni per mesi e la relativa **quantità totale provvisoria dei dati pubblicati** dai gruppi ransomware.

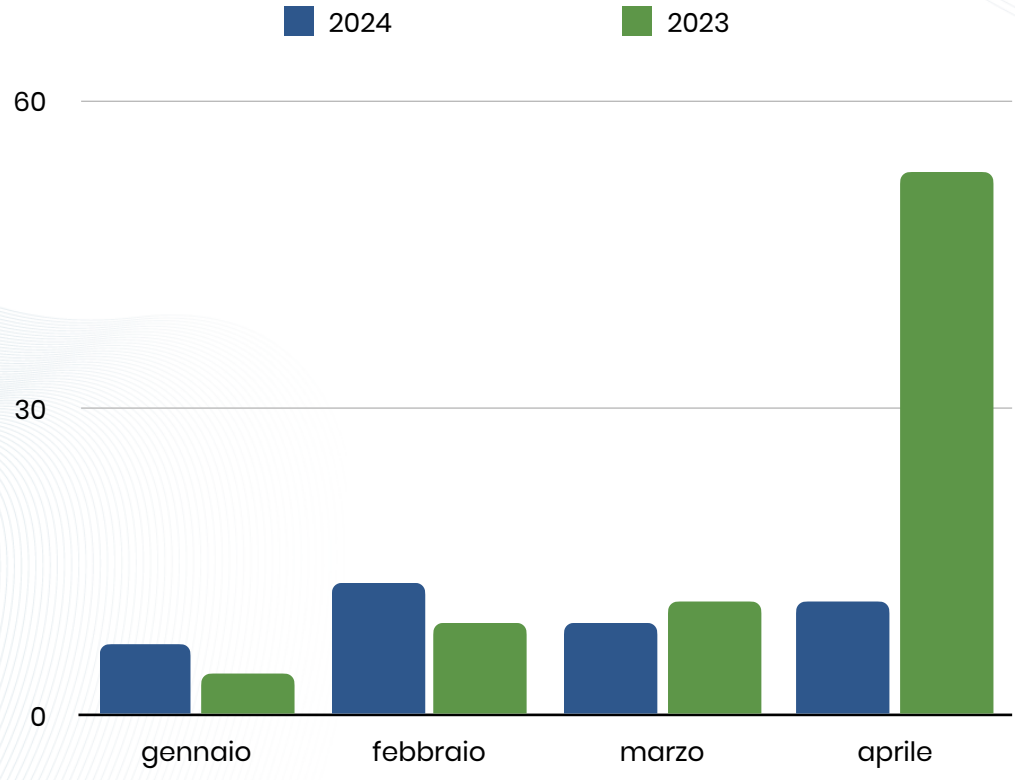
Nel quadrimestre, il totale dei dati:

- **esfiltrati dichiarati** ammonta a **6063.80 GB**
- **pubblicati** ammonta a **5240.23 GB**

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

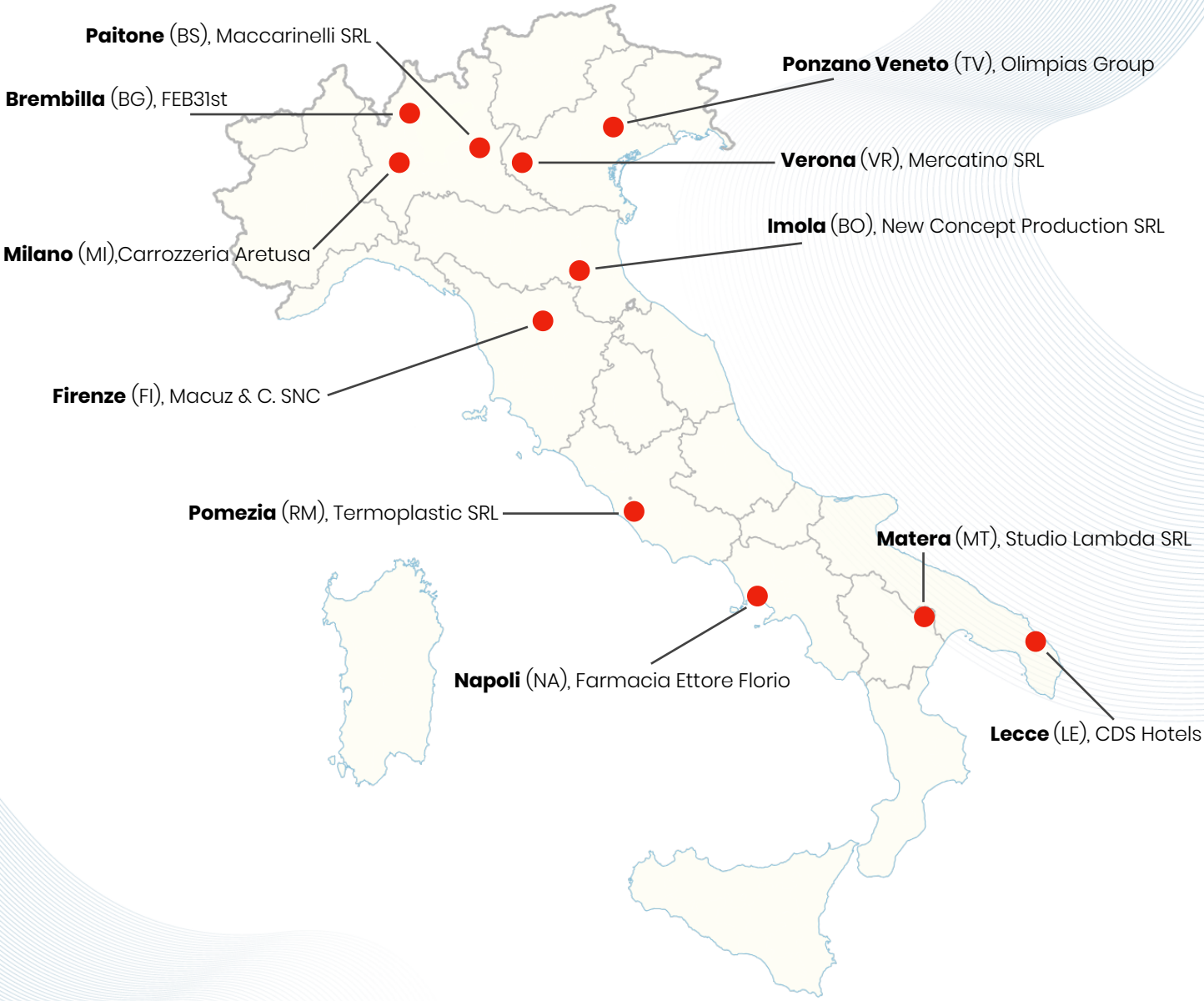
MESE	RIVENDICAZIONI	DATI DICHIARATI	DATI PUBBLICATI
gennaio	7	599.70 GB	599.70 GB
febbraio	13	1814.10 GB	1092.10 GB
marzo	8	924.10 GB	924.100 GB
aprile	11	2725.90 GB	2624.33 GB
totale	**39**	**6063.80 GB**	**5240.23 GB**

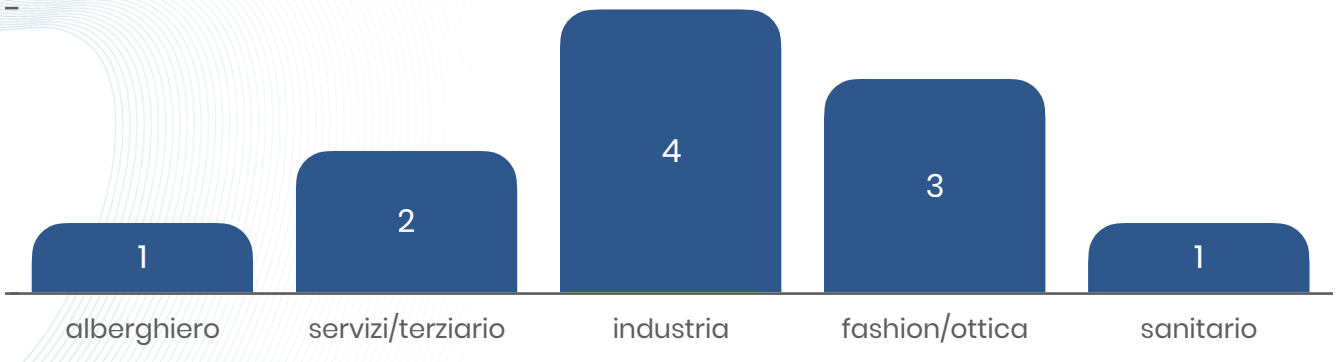
Comparato con il primo **quadrimestre dell'anno precedente**, in cui gli attacchi rivendicati verso target italiani erano **77**, si osserva un **decremento del 49.35%**.



fonte: Ransomfeed, dati aprile 2024

La **mappatura** degli attacchi ransomware sul territorio evidenzia, ancora una volta, una significativa **concentrazione nel nord** del Paese (5 attacchi), a seguire il **centro** (3 attacchi) ed infine il **sud** (3 attacchi), in regioni economicamente sviluppate e industrializzate.

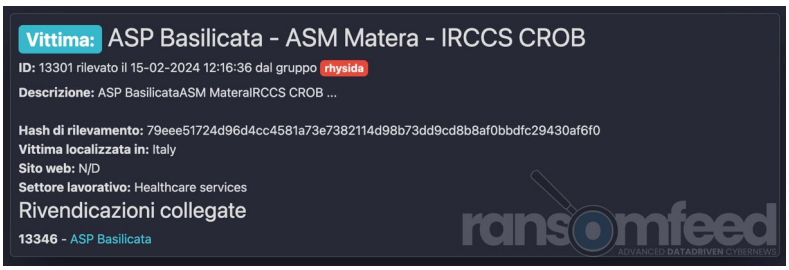


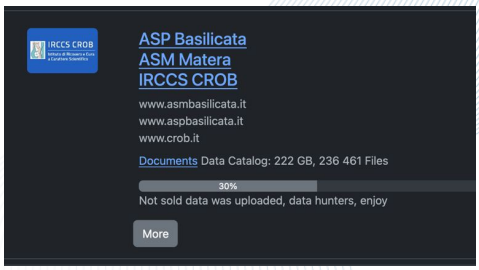


fonte: Ransomfeed, dati aprile 2024

🚨 Aggiornamenti

Torniamo sul **caso Rhysida** e le **aziende sanitarie della Basilicata**: il 25 aprile 2024, **conclusa la tornata elettorale regionale**, sono stati pubblicati **222.00 GB** di dati (rispetto ai **944.00 GB** esfiltrati dichiarati).

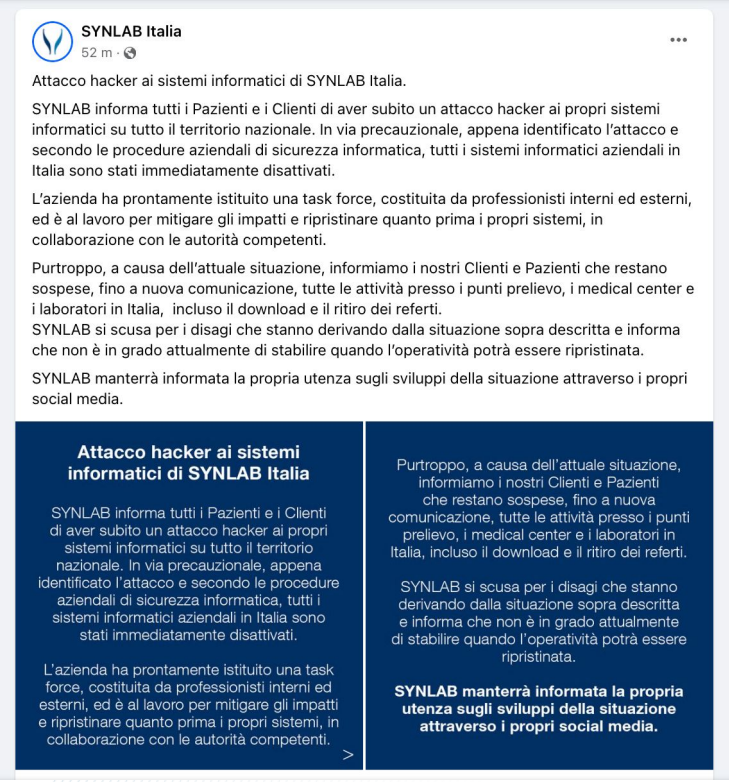




In evidenza

Il gruppo sanitario **Synlab Italia** ha subìto, in data 18 aprile 2024, un attacco di tipo ransomware; i loro sistemi, in tutta Italia, sono andati fuori uso, causando enormi disagi ai pazienti. Referti non disponibili per il download digitale e nemmeno ritirabili in formato cartaceo presso i punti prelievo.

Synlab, **impossibilitata ad accedere al mainframe**, ha comunicato la sospensione temporanea dei servizi con cartelli scritti a mano sulle serrande dei punti prelievo e con comunicati sui social media.


SYNLAB Italia
52 m ·

Attacco hacker ai sistemi informatici di SYNLAB Italia.

SYNLAB informa tutti i Pazienti e i Clienti di aver subito un attacco hacker ai propri sistemi informatici su tutto il territorio nazionale. In via precauzionale, appena identificato l'attacco e secondo le procedure aziendali di sicurezza informatica, tutti i sistemi informatici aziendali in Italia sono stati immediatamente disattivati.

L'azienda ha prontamente istituito una task force, costituita da professionisti interni ed esterni, ed è al lavoro per mitigare gli impatti e ripristinare quanto prima i propri sistemi, in collaborazione con le autorità competenti.

Purtroppo, a causa dell'attuale situazione, informiamo i nostri Clienti e Pazienti che restano sospese, fino a nuova comunicazione, tutte le attività presso i punti prelievo, i medical center e i laboratori in Italia, incluso il download e il ritiro dei referti.
SYNLAB si scusa per i disagi che stanno derivando dalla situazione sopra descritta e informa che non è in grado attualmente di stabilire quando l'operatività potrà essere ripristinata.

SYNLAB manterrà informata la propria utenza sugli sviluppi della situazione attraverso i propri social media.

Attacco hacker ai sistemi informatici di SYNLAB Italia

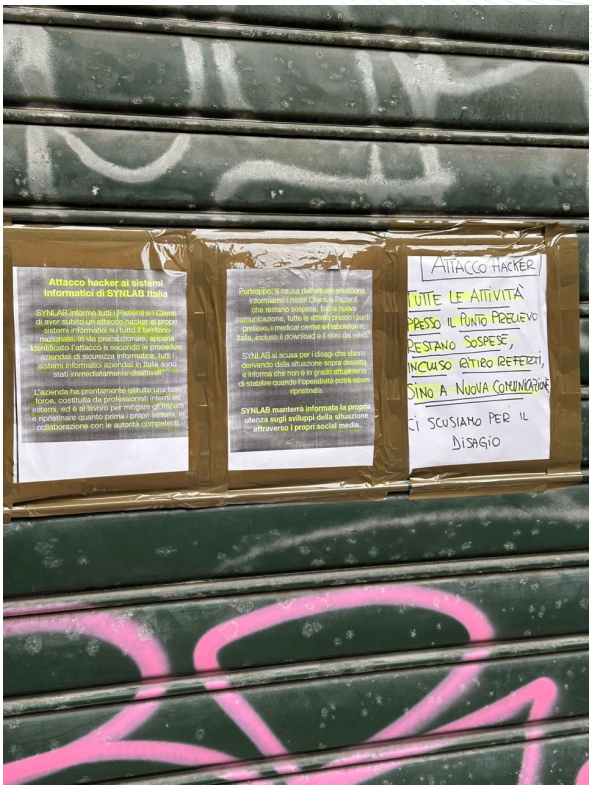
SYNLAB informa tutti i Pazienti e i Clienti di aver subito un attacco hacker ai propri sistemi informatici su tutto il territorio nazionale. In via precauzionale, appena identificato l'attacco e secondo le procedure aziendali di sicurezza informatica, tutti i sistemi informatici aziendali in Italia sono stati immediatamente disattivati.

L'azienda ha prontamente istituito una task force, costituita da professionisti interni ed esterni, ed è al lavoro per mitigare gli impatti e ripristinare quanto prima i propri sistemi, in collaborazione con le autorità competenti.

Purtroppo, a causa dell'attuale situazione, informiamo i nostri Clienti e Pazienti che restano sospese, fino a nuova comunicazione, tutte le attività presso i punti prelievo, i medical center e i laboratori in Italia, incluso il download e il ritiro dei referti.

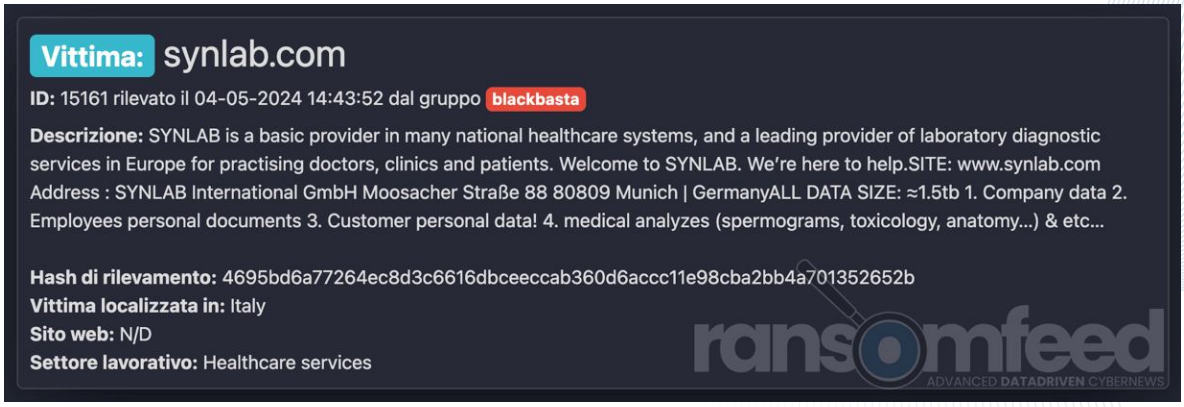
SYNLAB si scusa per i disagi che stanno derivando dalla situazione sopra descritta e informa che non è in grado attualmente di stabilire quando l'operatività potrà essere ripristinata.

SYNLAB manterrà informata la propria utenza sugli sviluppi della situazione attraverso i propri social media.



La situazione è risultata critica fin da subito, con l'assistenza impegnata a fornire supporto e nessuna certezza sullo stato dei dati.

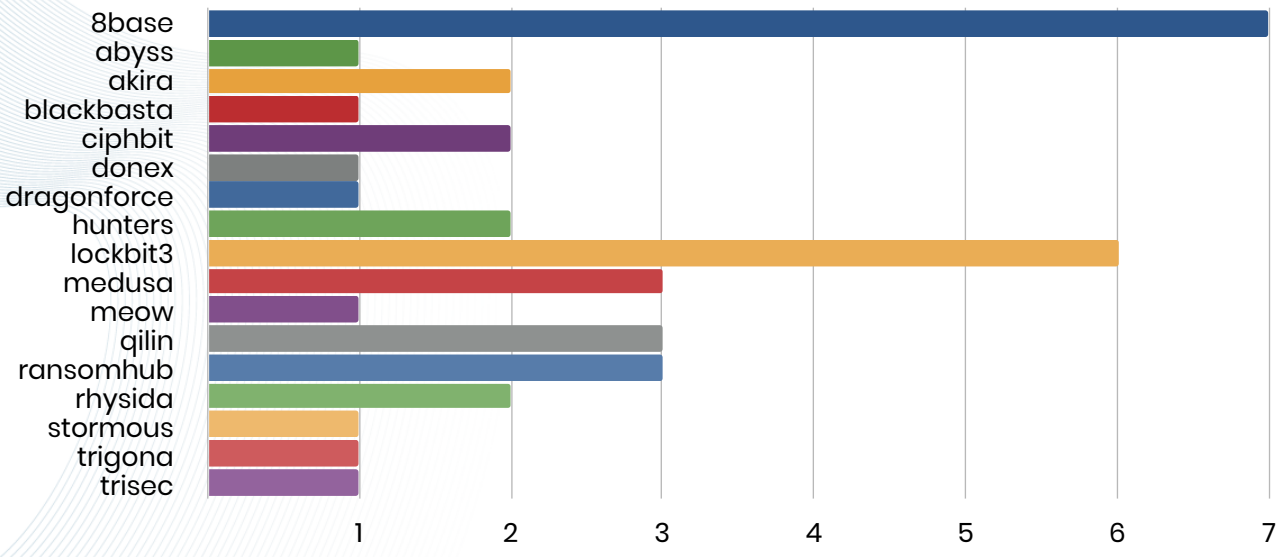
La rivendicazione del gruppo **blackbasta** è stata pubblicata il 4 maggio 2024, probabilmente dopo un principio di trattativa.



Inizialmente, alcune fonti avevano classificato l'attacco come tedesco, prendendo per buona la localizzazione sul *DLS* del gruppo criminale.
Dopo un'analisi approfondita, **abbiamo potuto appurare** che si trattava proprio dell'attacco italiano.

Molti sample forniti da blackbasta sono identificabili come **documenti d'identità** di persone italiane.
Tra i campioni anche **contratti** di varia natura, **cartelle cliniche** ed un directory tree che fa pensare ad un entry point localizzato nel sud Italia.

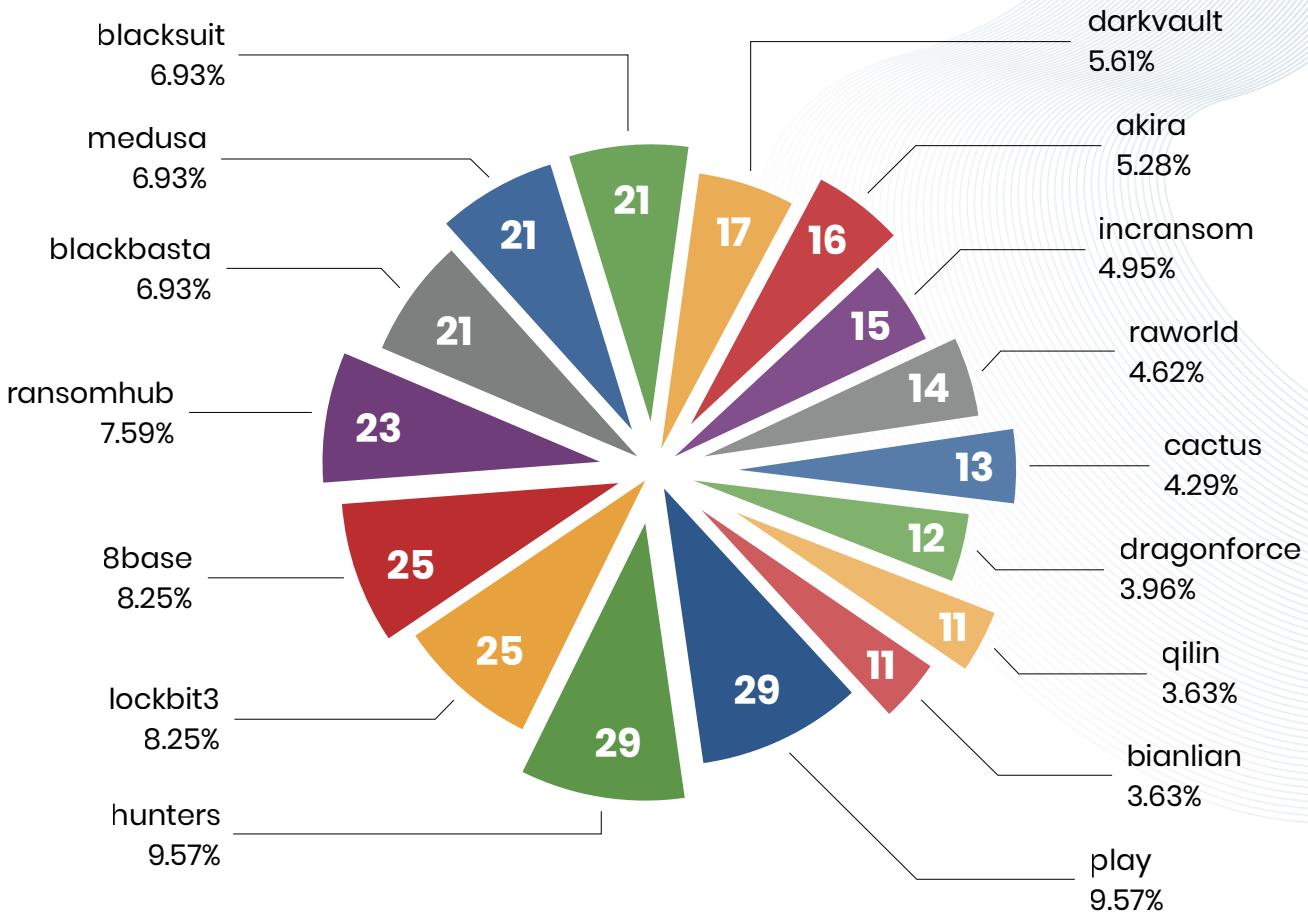
Una panoramica sui **39 attacchi italiani** dei primi quattro mesi dell'anno, per gruppo:



fonte: Ransomfeed, dati aprile 2024

Scena internazionale

Sono **380** gli attacchi ransomware rilevati nel mese di **aprile 2024**; rispetto allo stesso periodo dell'anno precedente (**514 attacchi** rivendicati), rileviamo un **decremento del 26.07%**.



nel grafico sono considerati tutti i gruppi con più di 10 attacchi

26 gruppi con **meno di 10 attacchi** (per un totale di **77** rivendicazioni)

cloak, 8
danon, 8
space bears, 8
rhysida, 6
qiulong, 6
ransomexx, 6
ransomhouse, 6
apos, 4
ciphbit, 4
apt73, 2
embargo, 2
gookie, 2
malek team, 2
mydata, 2
stormous, 1
everest, 1
snatch, 1
abyss, 1
blackout, 1
daixin, 1
dunghill, 1
killsec, 1
mallox, 1
redransomware, 1
threeam, 1

fonte: Ransomfeed, dati aprile 2024

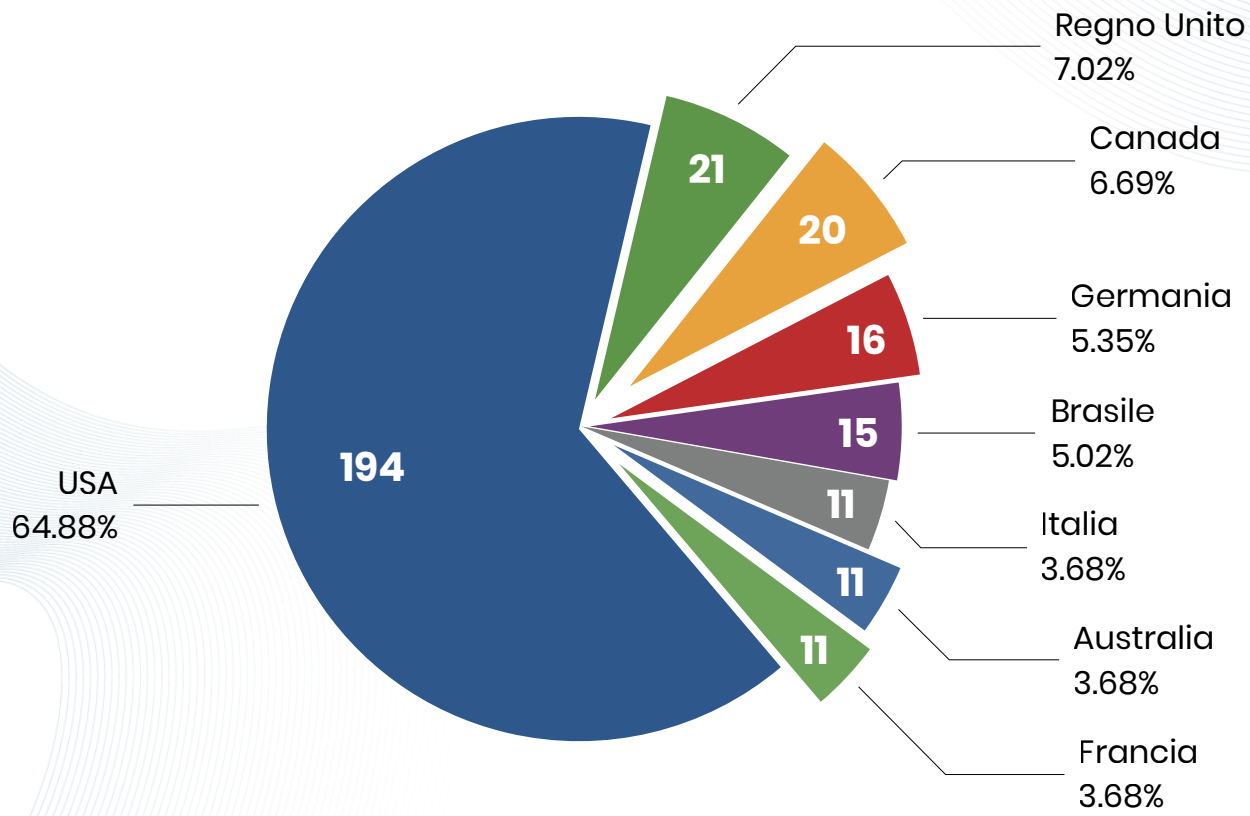
Anche per la scena internazionale, pubblichiamo la tabella con il numero totale delle rivendicazioni (al netto degli eventuali duplicati che potrebbero essere rilevati nei mesi successivi).

MESE	RIVENDICAZIONI
gennaio	284
febbraio	373
marzo	383 *
aprile	380
totale	**1420**

** dato aggiornato rispetto al report di marzo 2024*

Comparato con il primo **quadrimestre dell'anno precedente**, in cui gli attacchi ammontavano a **1356**, si osserva un **incremento del 4.72%**.

Analizzando la distribuzione geografica, nel **mese di aprile** gli **Stati Uniti** risultano essere ancora la nazione più colpita con **194 attacchi**.



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

41 paesi con **meno di 10 attacchi** (per un totale di **82** rivendicazioni)

- **Spagna**, 9
- **India**, 6
- **Paesi Bassi**, 6
- **Svizzera**, 5
- **Non Disponibile**, 4
- **Singapore**, 4
- **UAE**, 4
- **Taiwan**, 2
- **Belgio**, 2
- **El Salvador**, 2
- **Ungheria**, 2
- **Indonesia**, 2
- **Irlanda**, 2
- **Israele**, 2
- **Malesia**, 2
- **Norvegia**, 2
- **Sud Africa**, 2
- **Argentina**, 1
- **Colombia**, 1
- **Repubblica Ceca**, 1
- **Messico**, 1
- **Romania**, 1
- **Arabia Saudita**, 1
- **Austria**, 1
- **Bielorussia**, 1
- **Cina**, 1
- **Corea del Sud**, 1
- **Ecuador**, 1
- **Hong Kong**, 1
- **Giappone**, 1
- **Libia**, 1
- **Marocco**, 1
- **Oman**, 1
- **Pakistan**, 1
- **Polonia**, 1
- **Portorico**, 1
- **Palau**, 1
- **Seychelles**, 1
- **Sri Lanka**, 1
- **Svezia**, 1
- **Tailandia**, 1

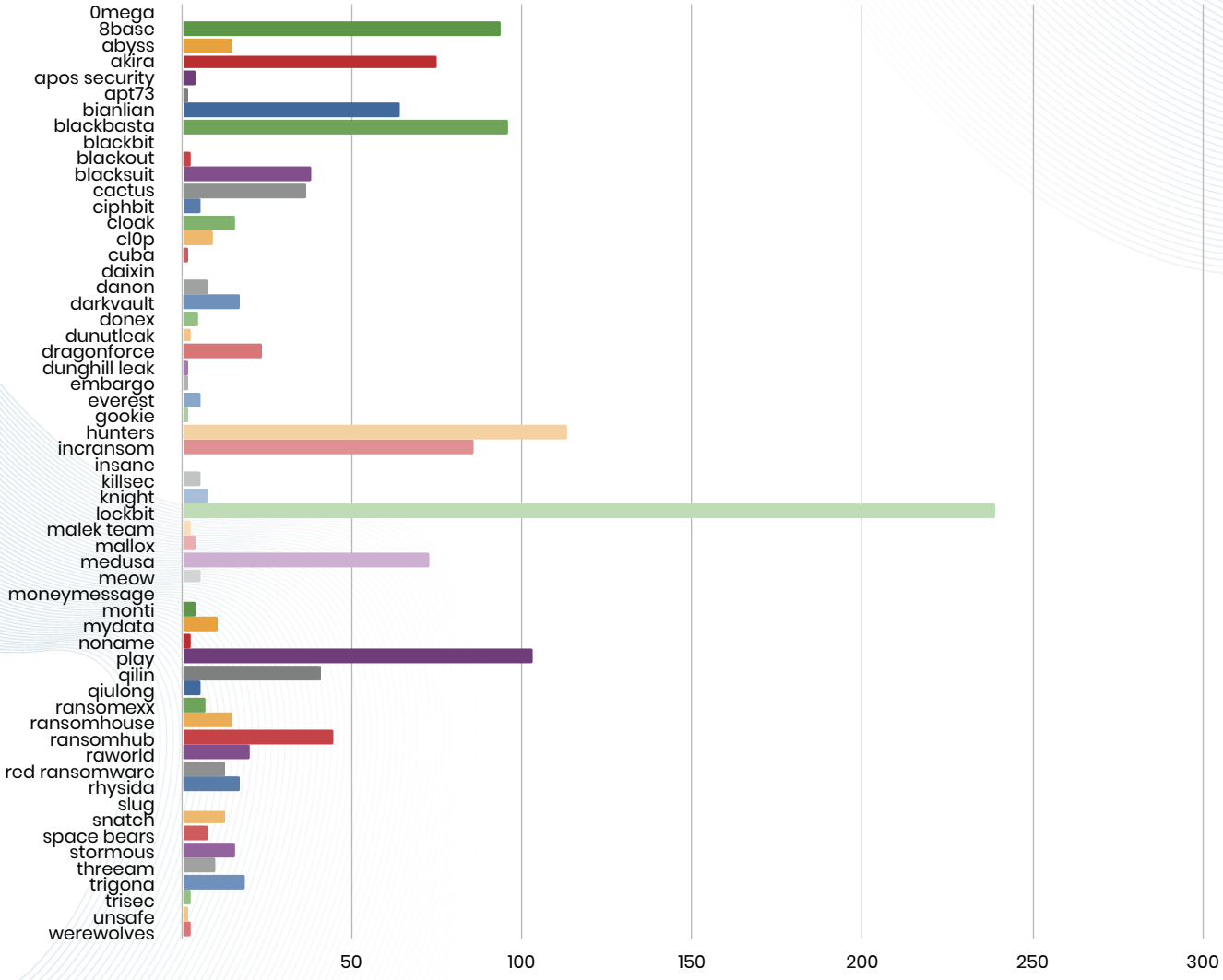
fonte: Ransomfeed, dati aprile 2024

Nei **primi quattro mesi del 2024** abbiamo registrato la nascita di **21 nuovi gruppi** ransomware:

APT73 (eraleig)	FSociety Locker	Ranstreet
Apos Security	Gookie	Ransomhub
Blackout	Insane	Red Ransomware
dAn0n	KillSec	SLUG
Dark Vault	Qiulong	Space Bears
donex	My Data	TriSec
embargo	Ransomblog Noname	Underground

Abbiamo raccolto gli attacchi monitorati dalla piattaforma dal **1° gennaio al 30 aprile 2024**; i **58 gruppi** hanno totalizzato **1420 attacchi**.

0mega, 1
8base, 94
abyss, 15
akira, 75
apos security, 4
apt73, 2
bianlian, 64
blackbasta, 96
blackbit, 1
blackout, 3
blacksuit, 38
cactus, 37
ciphbit, 6
cloak, 16
cl0p, 9
cuba, 2
daixin, 1
danon, 8
darkvault, 17
donex, 5
donutleak, 3
dragonforce, 24
dunghill leak, 2
embargo, 2
everest, 6
gookie, 2
hunters, 113
incransom, 86
insane, 1
killsec, 6
knight, 8
lockbit3, 239
malek team, 3
mallox, 4
medusa, 73
meow, 9
moneymessage, 1
monti, 4
mydata, 11
noname, 3
play, 103
qilin, 41
qiulong, 6
ransomexx, 7
ransomhouse, 15
ransomhub, 45
raworld, 20
red ransomware, 13
rhysida, 17
slug, 1
snatch, 13
space bears, 8
stormous, 16
threeam, 10
trigona, 19
trisec, 3
unsafe, 2
werewolves, 3



fonte: Ransomfeed, dati aprile 2024

👉🏻 Il caso: Change Healthcare

È nota la vicenda della struttura medica americana **Change Healthcare**: i loro sistemi sono stati violati dal gruppo criminale **ALPHV/BlackCat** all'inizio del mese di febbraio 2024 (sfruttando una vulnerabilità di Citrix, rivendicazione del 28 febbraio 2024 https://ransomfeed.it/index.php?page=post_details&id_post=13489), dopo la trattativa, la società madre **OPTUM** aveva pagato un riscatto di **22 milioni di dollari**.

Il gruppo criminale ha **incassato il riscatto** ma non ha mai corrisposto la fee al proprio affiliato, rimasto con **4TB di dati** in mano.
Il caso è stato reso pubblico dal portavoce dell'affiliato che ha denunciato ALPHV/BlackCat per **condotta scorretta** nei loro riguardi; si sono poi susseguite voci di un possibile rebrand e di movimenti all'interno della scena ransomware, tutto frutto di speculazioni senza alcun fondamento. ALPHV/BlackCat ha intascato i soldi ed è **sparito nel nulla**.
Ne abbiamo parlato su Ransomfeed, con un contenuto dedicato: https://ransomfeed.it/index.php?page=blog&postID=02.

L'8 aprile, mentre stavamo predisponendo il recap del mese di marzo, il gruppo criminale **Ransomhub** ha pubblicato sul proprio DLS la rivendicazione di Change Healthcare, minacciando la pubblicazione dei dati se non fosse avvenuto **un altro pagamento** (https://ransomfeed.it/index.php?page=post_details&id_post=14148).

Secondo un articolo pubblicato da **Bleeping Computer** (bleepingcomputer.com/news/security/change-healthcare-hacked-using-stolen-citrix-account-with-no-mfa), OPTUM avrebbe **ammesso di aver pagato** il riscatto, per proteggere i dati degli utenti, dopo la compromissione.
Successivamente, **Ransomhub ha rimosso la rivendicazione** di Change Healthcare dal proprio sito, dichiarando che un riscatto era stato pagato.

Oltre al pagamento del **doppio riscatto**, si stima che l'attacco informatico subìto dall'organizzazione sanitaria, abbia causato **danni finanziari per 872 milioni di dollari**.

ADVANCED **DATADRIVEN** CYBERNEWS

RECAP MENSILE
APRILE 2024

/eof