ADVANCED **DATADRIVEN** CYBERNEWS

RECAP MENSILE
MARZO 2024

ver. glitch256_u07 - 08 aprile 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 🇮🇹

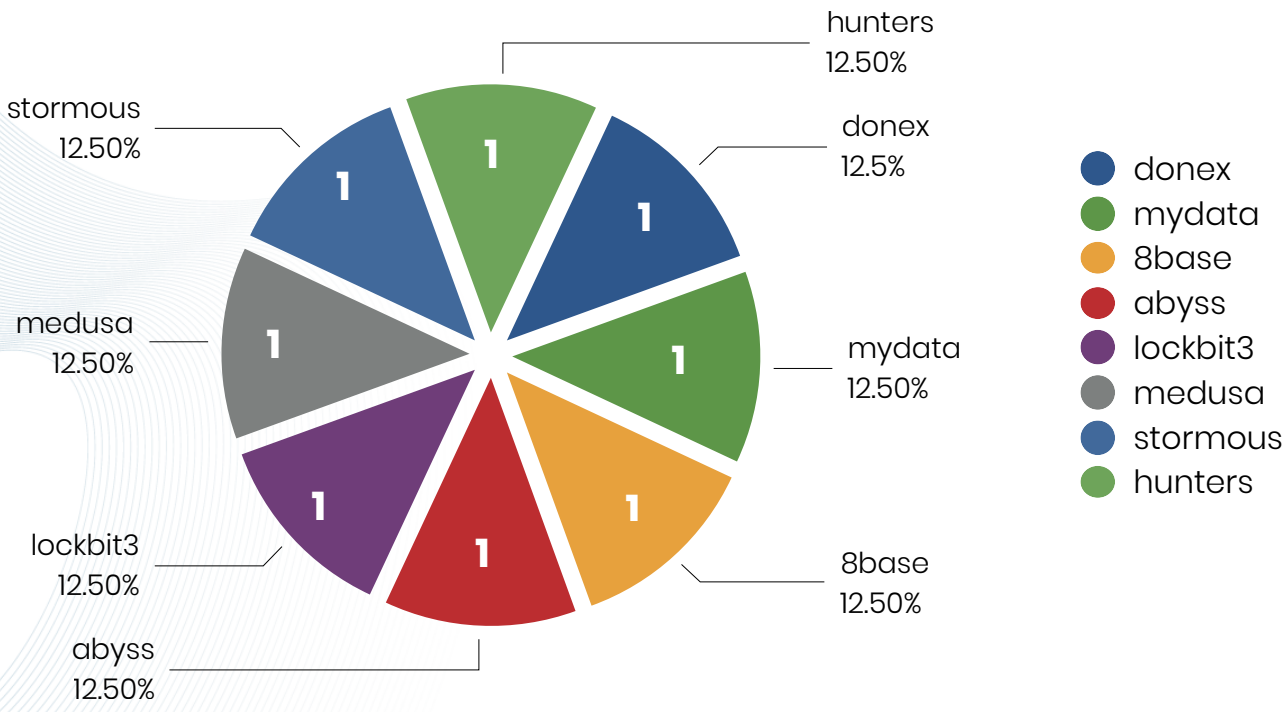
A **marzo 2024** la piattaforma ha registrato un totale di **8 attacchi**, per la maggior parte localizzati nel **Nord Italia** (**5 attacchi**).

Il **totale dei dati pubblicati** ammonta a 585.90 GB.

ID	GRUPPO	VITTIMA	DATI PUBBLICATI	LOCALIZZAZIONE
13632	donex	ELSAP SPA	48.00 GB	Milano
13653	mydata	Consorzio Innova	225.00 GB	Bologna
13683	8base	Federchimica	63.90 GB	Milano
13726	abyss	IAM Design	78.00 GB	Vicenza
13755	lockbit3	Bergmeister SRL	dati pubblicati *	Varna (BZ)
13765	medusa	Autorità Portuale Mar Tirreno	dati pubblicati *	Livorno
13778	stormous	PagineSì SPA	170.00 GB	Terni
13788	hunters	Panzeri e Cattaneo Notai	nessuna informazione	Galbiate (LC)

** i dati esfiltrati sono stati pubblicati, tuttavia non è stato possibile stabilirne la quantità*

Rispetto al mese di **marzo 2023**, in cui gli attacchi rivendicati contro target italiani erano **11**, si osserva un **decremento del 27.27%**.



fonte: Ransomfeed, dati marzo 2024

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

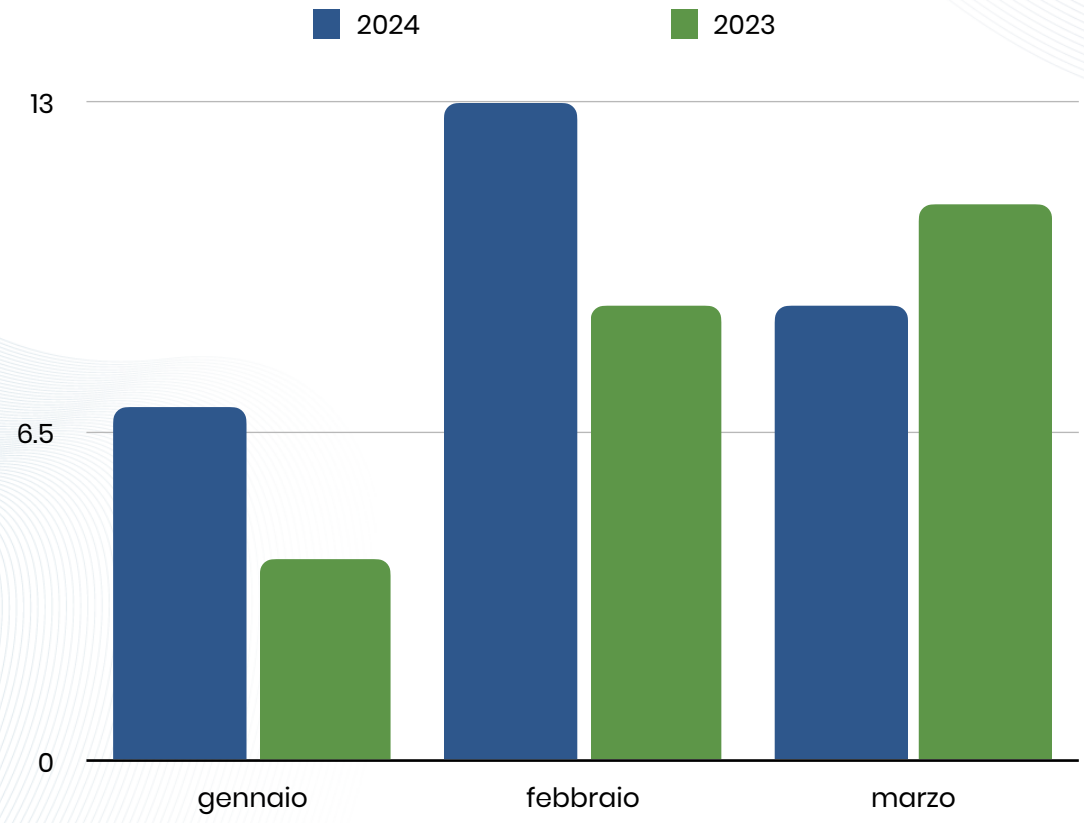
Nel trimestre, il totale dei dati:

- **esfiltrati dichiarati** ammonta a **2980.20 GB**
- **pubblicati** ammonta a **2036.20 GB**

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

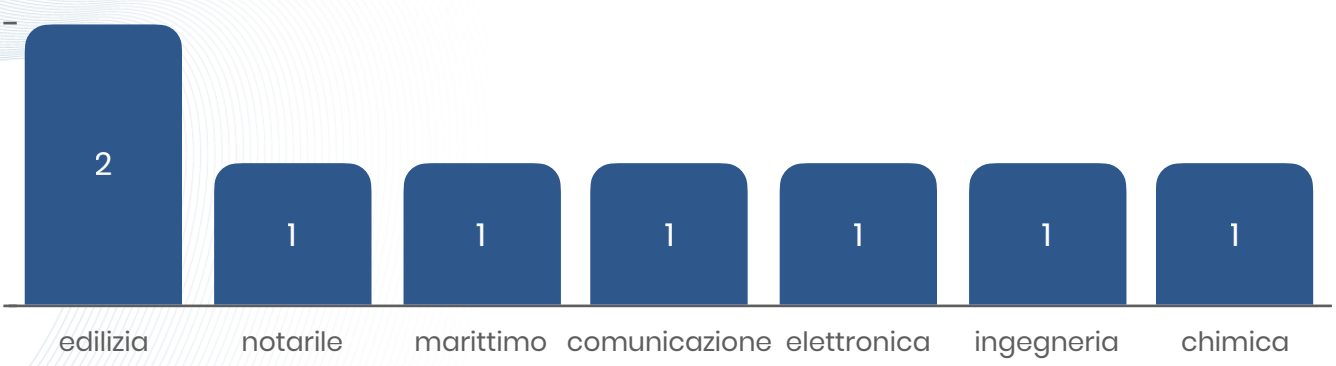
MESE	RIVENDICAZIONI	DATI DICHIARATI	DATI PUBBLICATI
gennaio	7	599.70 GB	599.70 GB
febbraio	13	1794.60 GB	850.60 GB
marzo	8	585.90 GB	585.90 GB
totale	**28**	**2980.20 GB**	**2036.20 GB**

Comparato con il **trimestre dell'anno precedente**, in cui gli attacchi rivendicati verso target italiani erano **24**, si osserva un **incremento del 16.66%**.



fonte: Ransomfeed, dati marzo 2024

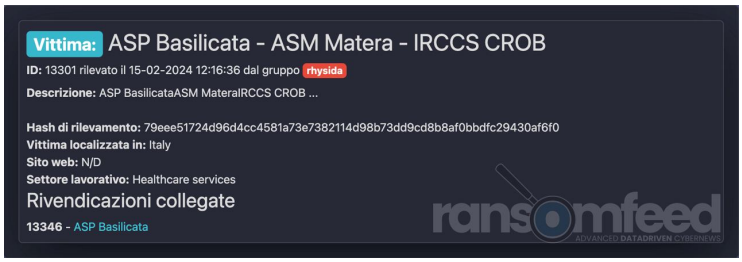
La **mappatura** degli attacchi ransomware sul territorio evidenzia, ancora una volta, una significativa **concentrazione nel nord** del Paese (5 attacchi), a seguire il **centro** (3 attacchi), in regioni economicamente sviluppate e industrializzate.

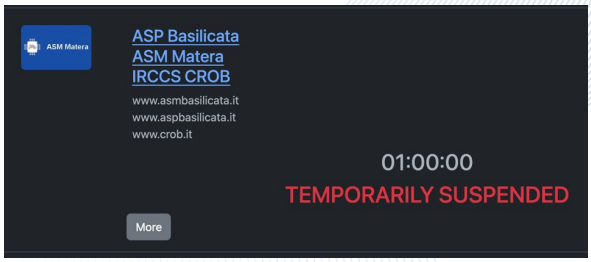


fonte: Ransomfeed, dati marzo 2024

🚨 Aggiornamenti

Per quanto riguarda il **caso Rhysida** e le **aziende sanitarie della Basilicata** (attacco rivendicato il 15 febbraio), permane lo stallo. Il countdown per la pubblicazione dei dati è stato sospeso il 26 febbraio e, nel mese di marzo, **non si sono evidenziate novità** in merito.

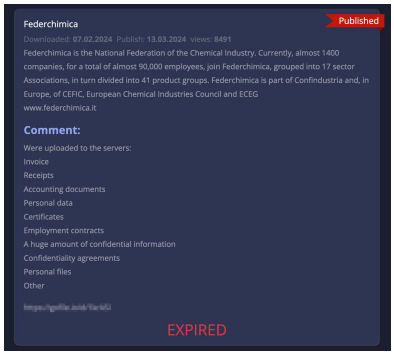




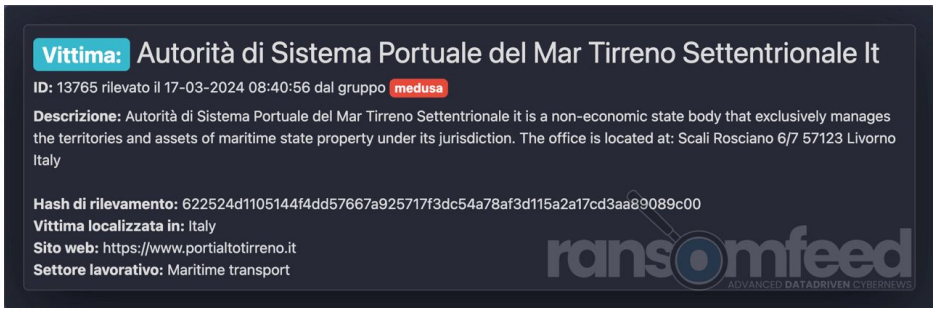
📰 In evidenza

Degli attacchi pubblicati nel mese di marzo, vogliamo mettere in risalto due rivendicazioni.

La prima riguarda **Federchimica Confindustria** (rivendicata da 8base) per cui sono stati **pubblicati 63.90 GB**.



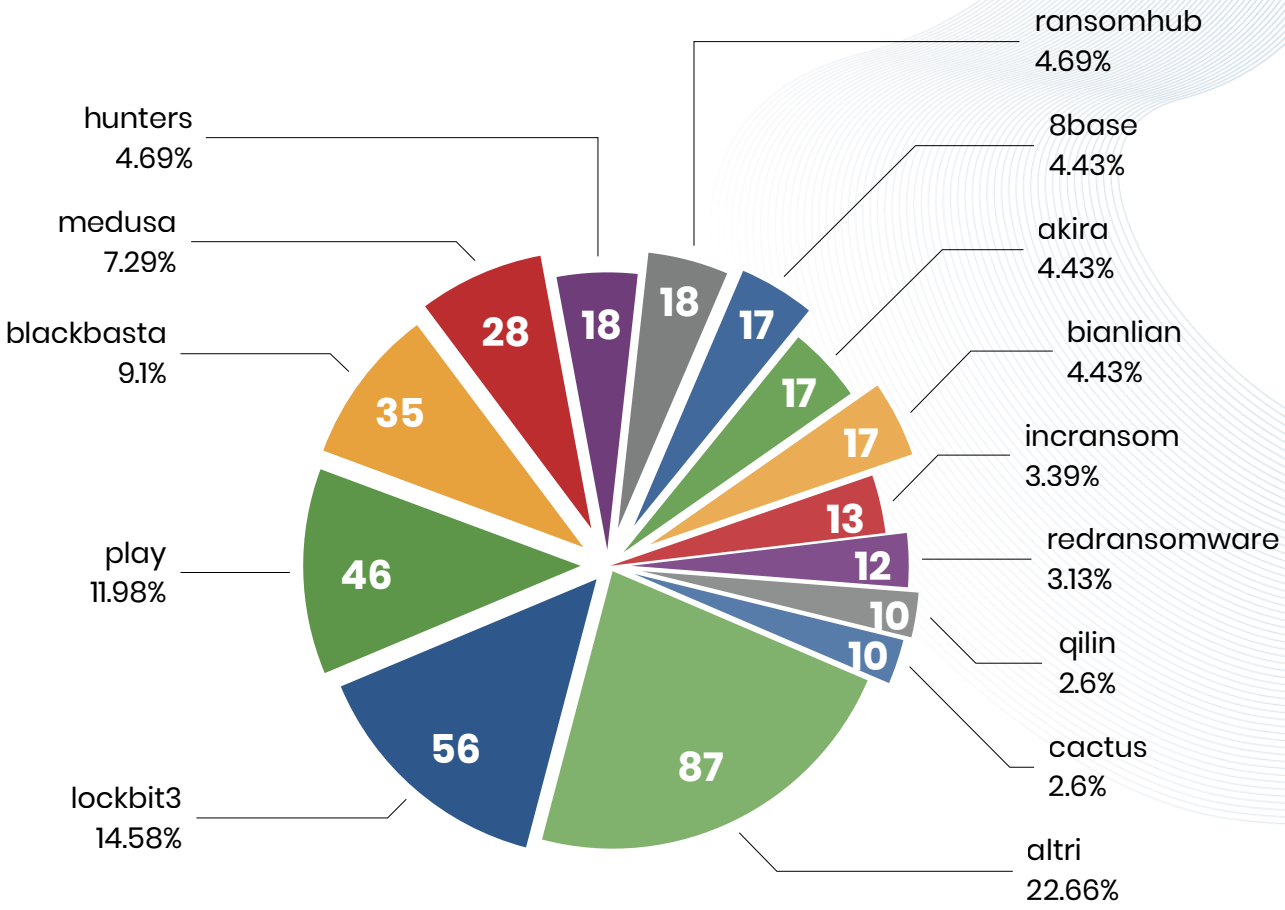
La seconda (rivendicata da medusa) riguarda l'**Autorità Portuale del Mar Tirreno Settentrionale**, i cui dati sono stati pubblicati, ma non è stato possibile **determinarne la quantità**.



Ad oggi, sui siti web di entrambe le vittime, **non risulta pubblicato** alcun comunicato ufficiale relativo all'attacco subìto.

Scena internazionale

Sono **384** gli attacchi ransomware rilevati a **marzo 2024**; rispetto allo stesso mese dell'anno precedente (**443 attacchi** rivendicati), rileviamo un **decremento del 13.32%**.



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

stormous, 9
blacksuit, 8
raworld, 6
dragonforce, 6
trigona, 6
killsec, 5
abyss, 5
alphv, 5
cloak, 5
donex, 5
snatch, 5
rhysida, 4
cl0p, 4
mallox, 3
donutleaks, 2
everest, 2
meow, 2
blackbyte, 1
mydata, 1
ransomexx, 1
threeam, 1
werewolves, 1

fonte: Ransomfeed, dati marzo 2024

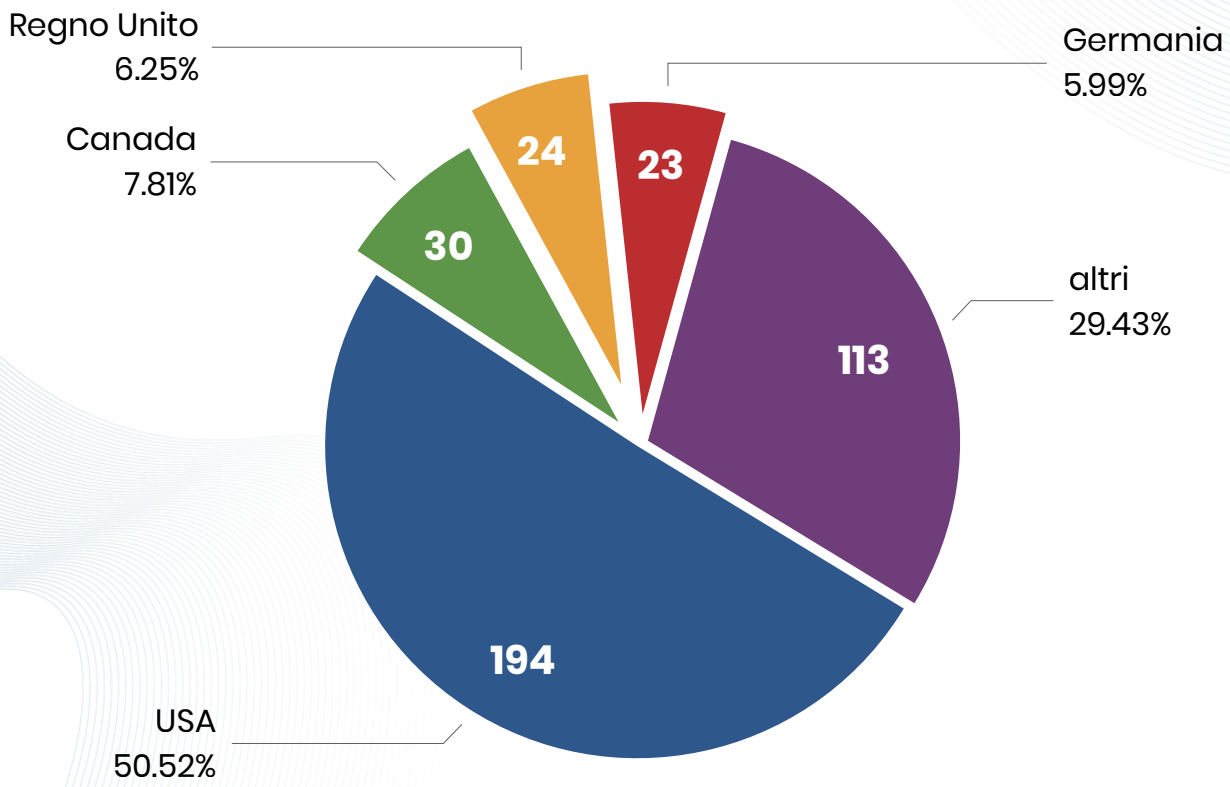
Anche per la scena internazionale, pubblichiamo la tabella con il numero totale delle rivendicazioni (al netto degli eventuali duplicati che potrebbero essere rilevati nei mesi successivi).

MESE	RIVENDICAZIONI
gennaio	284
febbraio	375 *
marzo	384
totale	**1043**

** dato aggiornato rispetto al report di febbraio 2024*

Comparato con il **trimestre dell'anno precedente**, in cui gli attacchi ammontavano a **842**, si osserva un **incremento del 23.99%**.

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



fonte: Ransomfeed, dati marzo 2024

48 paesi con **meno di 10 attacchi** (per un totale di **113** rivendicazioni)

- **Italia**, 8
- **Spagna**, 7
- **Brasile**, 6
- **India**, 6
- **Australia**, 6
- **Cina**, 5
- **Messico**, 5
- **Svezia**, 5
- **Belgio**, 5
- **Indonesia**, 4
- **Giappone**, 3
- **Malesia**, 3
- **Paesi Bassi**, 3
- **Egitto**, 3
- **Nuova Zelanda**, 3
- **Polonia**, 3
- **Svizzera**, 3
- **UAE**, 2
- **Colombia**, 2
- **Peru**, 2
- **Sud Africa**, 2
- **Austria**, 1
- **Francia**, 1
- **Corea**, 1
- **Singapore**, 1
- **Argentina**, 1
- **Bangladesh**, 1
- **Bermuda**, 1
- **Bulgaria**, 1
- **Repubblica Ceca**, 1
- **Danimarca**, 1
- **Honduras**, 1
- **Hong Kong**, 1
- **Iran**, 1
- **Irlanda**, 1
- **Libano**, 1
- **Macedonia**,1
- **Namibia**, 1
- **Norvegia**, 1
- **Pakistan**, 1
- **Portogallo**, 1
- **Romania**, 1
- **Russia**, 1
- **Arabia Saudita**, 1
- **Slovacchia**, 1
- **Tailandia**, 1
- **Tunisia**, 1
- **Turchia**, 1

fonte: Ransomfeed, dati marzo 2024

👉🏻 Il caso: ALPHV/BlackCat

Il 3 marzo, dopo aver riscosso un pagamento di **22 milioni di dollari** da parte di OPTUM, operatore dietro **Change Healthcare**, vittima di attacco ransomware, ha chiuso definitivamente le proprie operazioni il gruppo ALPHV/BlackCat (con **53** rivendicazioni nel 2024).

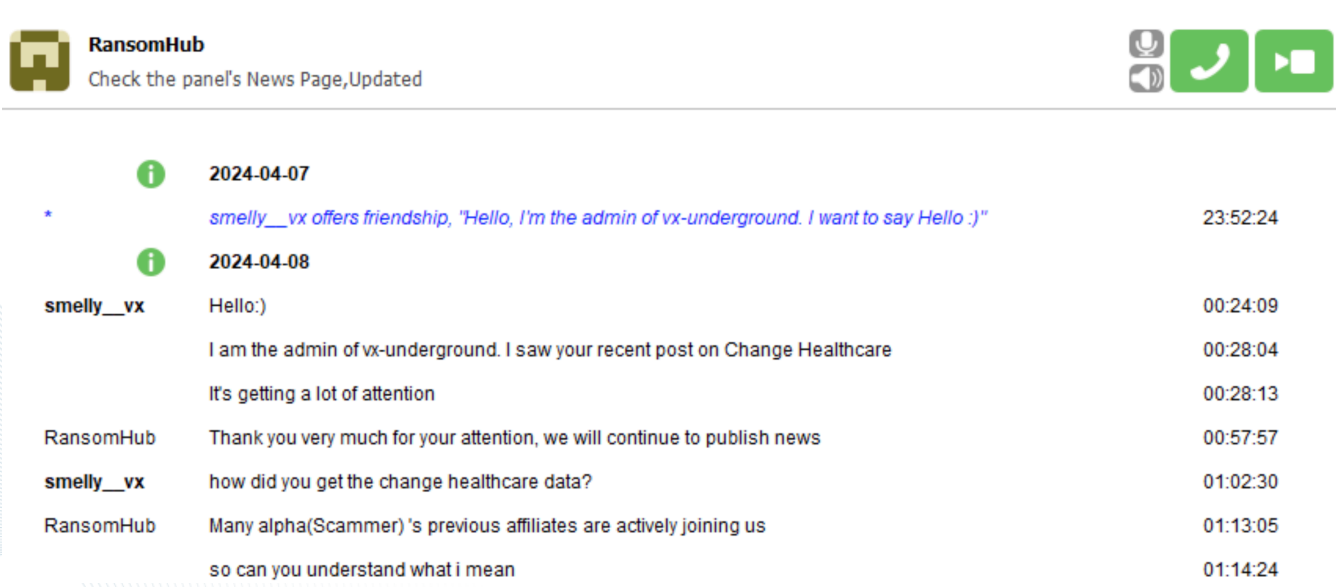
L'intera, controversa vicenda è descritta in un post **pubblicato su Ransomfeed**, raggiungibile a questo link: https://ransomfeed.it/index.php?page=blog&postID=02

L'8 aprile, mentre stavamo predisponendo il recap, il gruppo **Ransomhub** ha pubblicato una rivendicazione contro **Change Healthcare**.

Ci sono speculazioni su un possibile rebrand di ALPHV in Ransomhub, ma non abbiamo trovato alcuna evidenza.

Inoltre, che Ransomhub abbia acquistato, dall'ex affiliato di ALPHV, 4 TB di dati per poi tentare una seconda estorsione al gruppo OPTUM, ci sembra alquanto improbabile; maggiore, invece, la probabilità che l'ex affiliato di ALPHV abbia **raggiunto un accordo** con Ransomhub per dividersi un eventuale introito proveniente da una seconda estorsione.

La **conferma della nostra ipotesi** emerge da una chat tra un admin di Ransomhub e VX Underground.



fonte: VX Underground

ransomfeed

ADVANCED **DATADRIVEN** CYBERNEWS

RECAP MENSILE
MARZO 2024

/eof