



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

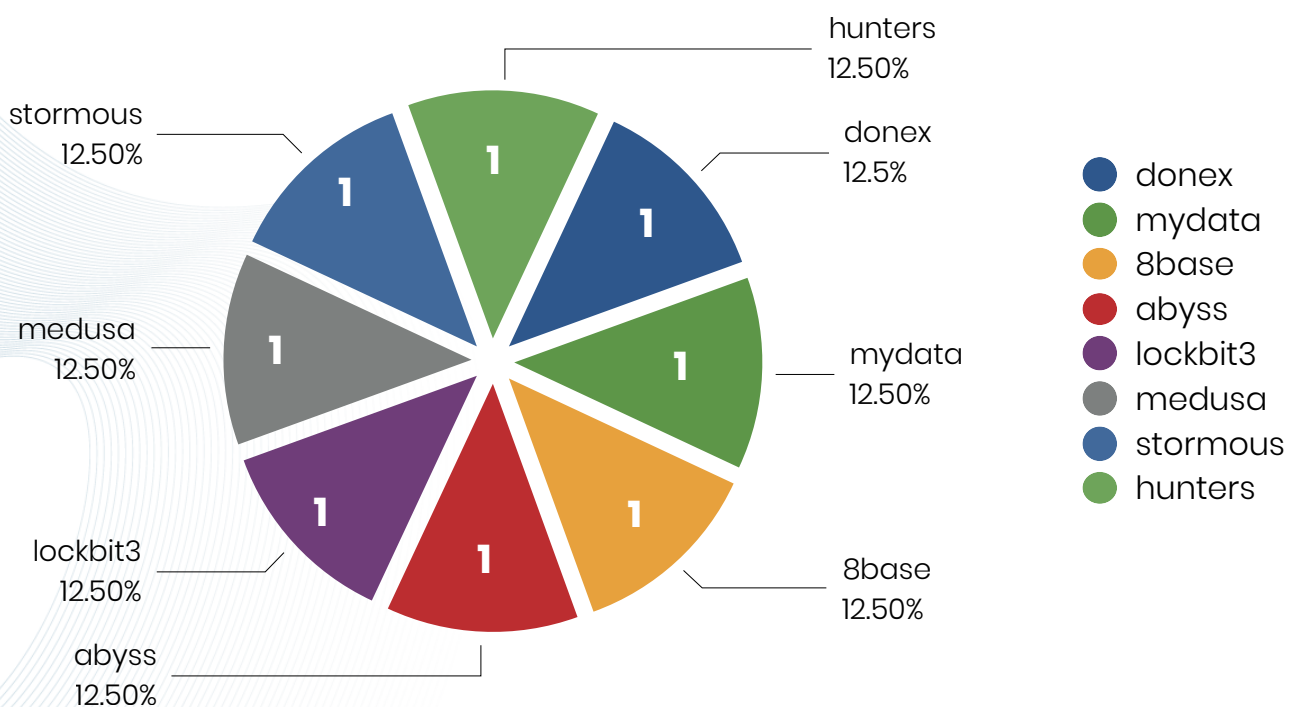
A **marzo 2024** la piattaforma ha registrato un totale di **8 attacchi**, per la maggior parte localizzati nel **Nord Italia (5 attacchi)**.

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.

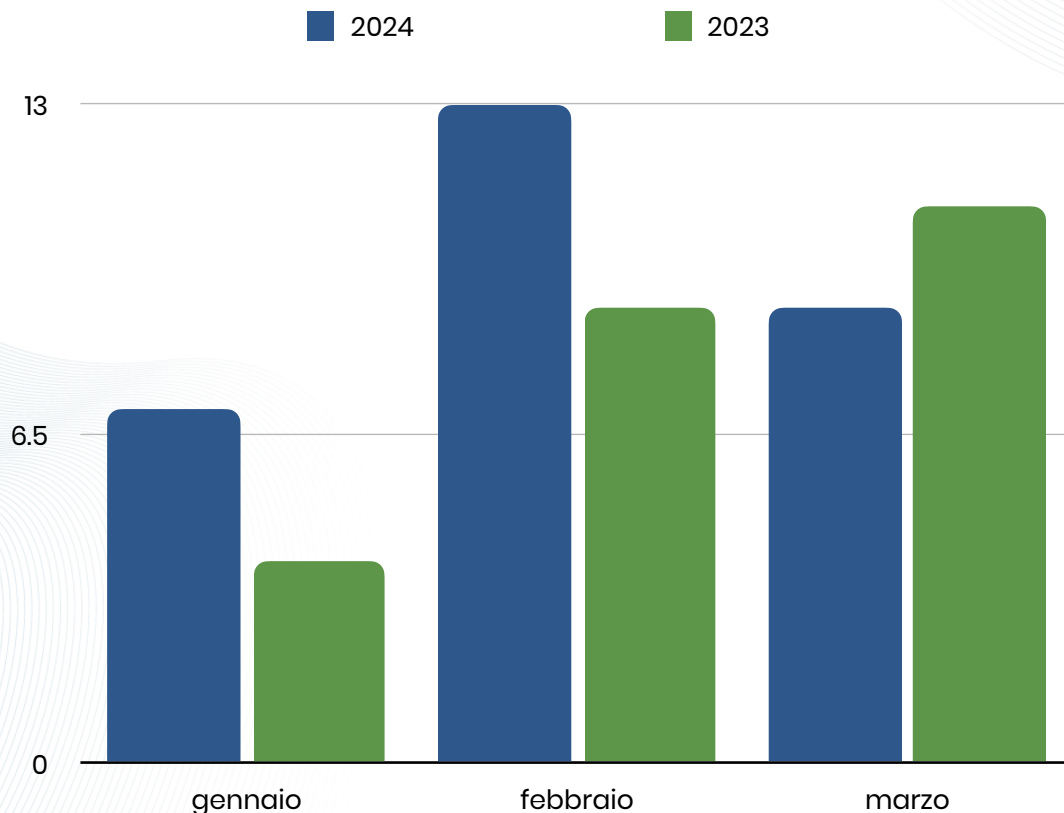
Nel trimestre, il totale dei dati:

- **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

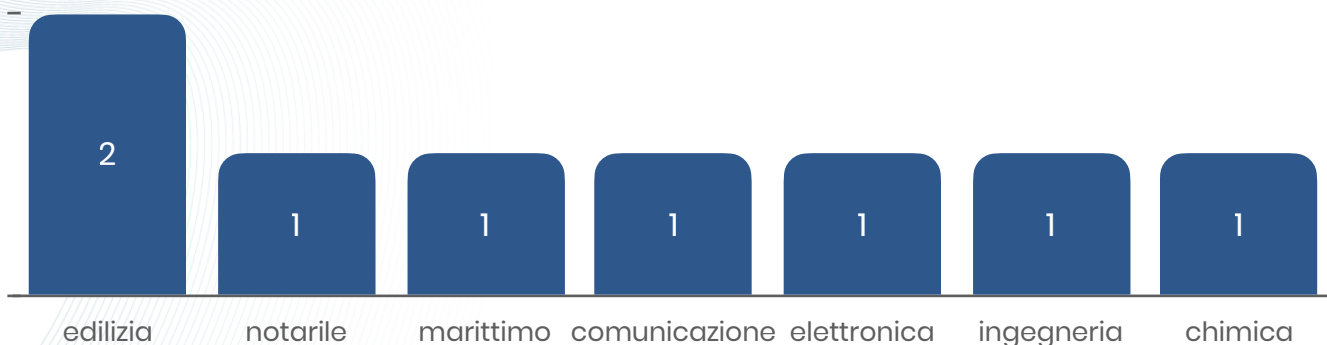
Comparato con il **trimestre dell'anno precedente**, in cui gli attacchi rivendicati verso target italiani erano **24**, si osserva un **incremento del 16.66%**.



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.

Vittima: ASP Basilicata - ASM Matera - IRCCS CROB
 ID: 13301 rilevato il 15-02-2024 12:16:36 dal gruppo **rhysida**
 Descrizione: ASP BasilicataASM MateraIRCCS CROB ...
 Hash di rilevamento: 79eee51724d96d4cc4581a73e7382114d98b73dd9cd8b8af0bbdfc29430af6f0
 Vittima localizzata in: Italy
 Sito web: N/D
 Settore lavorativo: Healthcare services
 Rivendicazioni collegate
 13346 - ASP Basilicata



ASP Basilicata
ASM Matera
IRCCS CROB
 www.asmbasilicata.it
 www.aspbasilicata.it
 www.crob.it

01:00:00
TEMPORARILY SUSPENDED

More

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**.


Federchimica Published
 Comment: 13/02/2024 P:00001: 13.03.2024 View: 8491
 Federchimica is the National Federation of the Chemical Industry. Currently, almost 1400 companies, for a total of almost 90,000 employees, join Federchimica, grouped into 17 sector Associations, in turn divided into 41 product groups. Federchimica is part of Confindustria and, in Europe, of CEFIC, European Chemical Industries Council and ECEG
 www.federchimica.it

Comment:
 Were uploaded to the servers:
 Invoices
 Receipts
 Accounting documents
 Personal data
 Certificates
 Employment contracts
 A huge amount of confidential information
 Confidentiality agreements
 Personal files
 Other

https://github.com/8base/8base
EXPIRED

Vittima: Federchimica
 ID: 13683 rilevato il 12-03-2024 04:14:26 dal gruppo **8base**
 Descrizione: Federchimica is the National Federation of the Chemical Industry. Currently, almost 1400 companies, for a total of almost 90,000 employees, join Federchimica, grouped into 17 sector Associations, in turn divided into 41 product groups. Federchimica is part of Confindustria and, in Europe, of CEFIC, European Chemical Industries Council and ECEGwww.federchimica.it

Hash di rilevamento: 16993cdca785f05dc83b5afbec049c3830d0e70e9555a8da61f714b9c3e8dbf1
Vittima localizzata in: Italy
Sito web: N/D
Settore lavorativo: Heavy industries



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**.

MEDUSA BLOG

PUBLISHED


Autorità di Sistema Portuale del Mar Tirreno Settentrionale It

Autorità di Sistema Portuale del Mar Tirreno Settentrionale It is a non-economic state body that exclusively manages the territories and assets of maritime state property under its jurisdiction. The office is located at: Scali Rosciano 6/7 57123 Livorno Italy

2024-03-16 20:48:42 2518

Vittima: Autorità di Sistema Portuale del Mar Tirreno Settentrionale It
 ID: 13765 rilevato il 17-03-2024 08:40:56 dal gruppo **medusa**
 Descrizione: Autorità di Sistema Portuale del Mar Tirreno Settentrionale it is a non-economic state body that exclusively manages the territories and assets of maritime state property under its jurisdiction. The office is located at: Scali Rosciano 6/7 57123 Livorno Italy

Hash di rilevamento: 622524d1105144f4dd57667a925717f3dc54a78af3d115a2a17cd3aa89089c00
Vittima localizzata in: Italy
Sito web: https://www.portaltotirreno.it
Settore lavorativo: Maritime transport

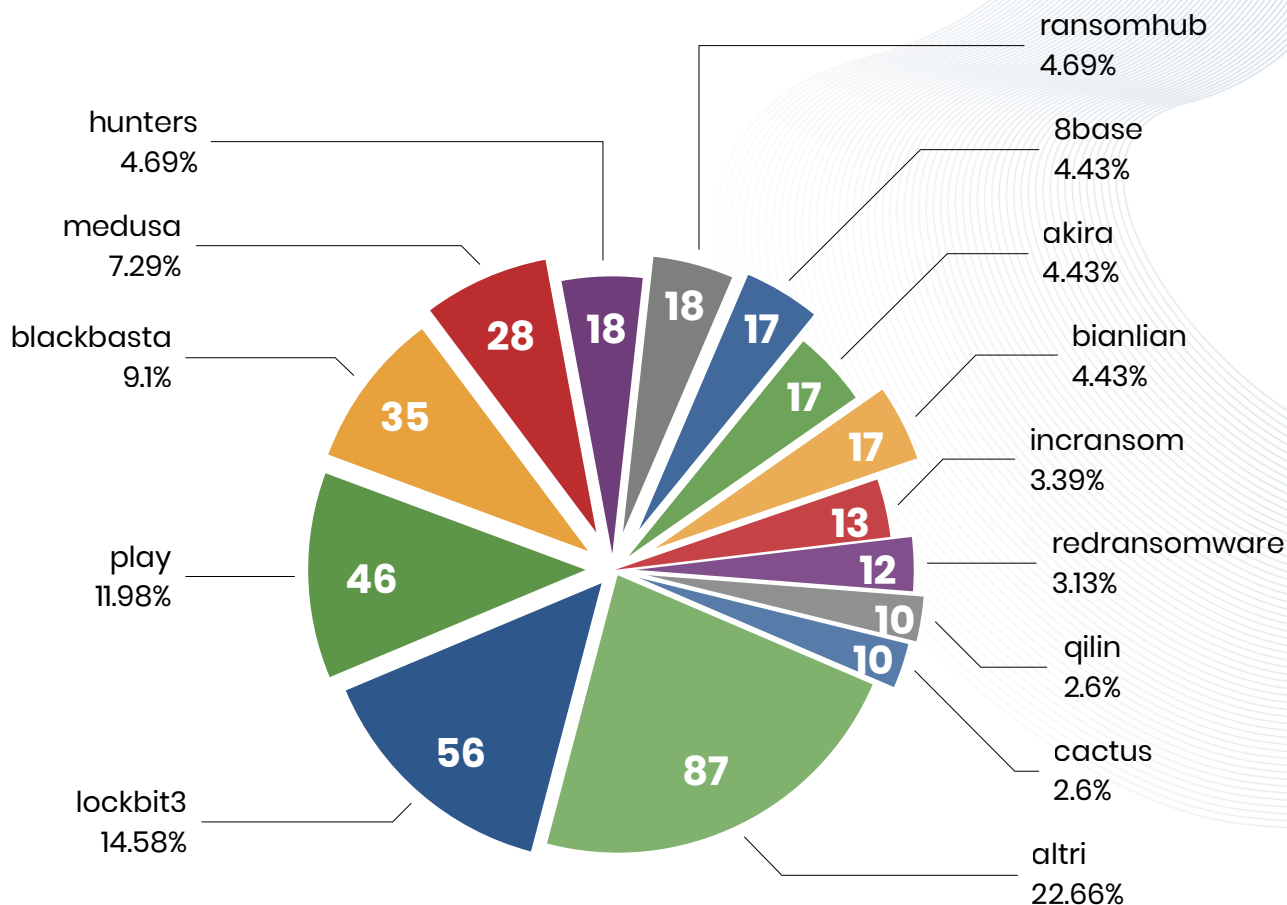


Ad oggi, sui siti web di entrambe le vittime, **non risulta pubblicato** alcun comunicato ufficiale relativo all'attacco subito.



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
rhytida, 4
cl0p, 4
mallox, 3

donutleaks, 2
everest, 2
meow, 2
blackbyte, 1
mydata, 1
ransomexx, 1
threeam, 1

werewolves, 1



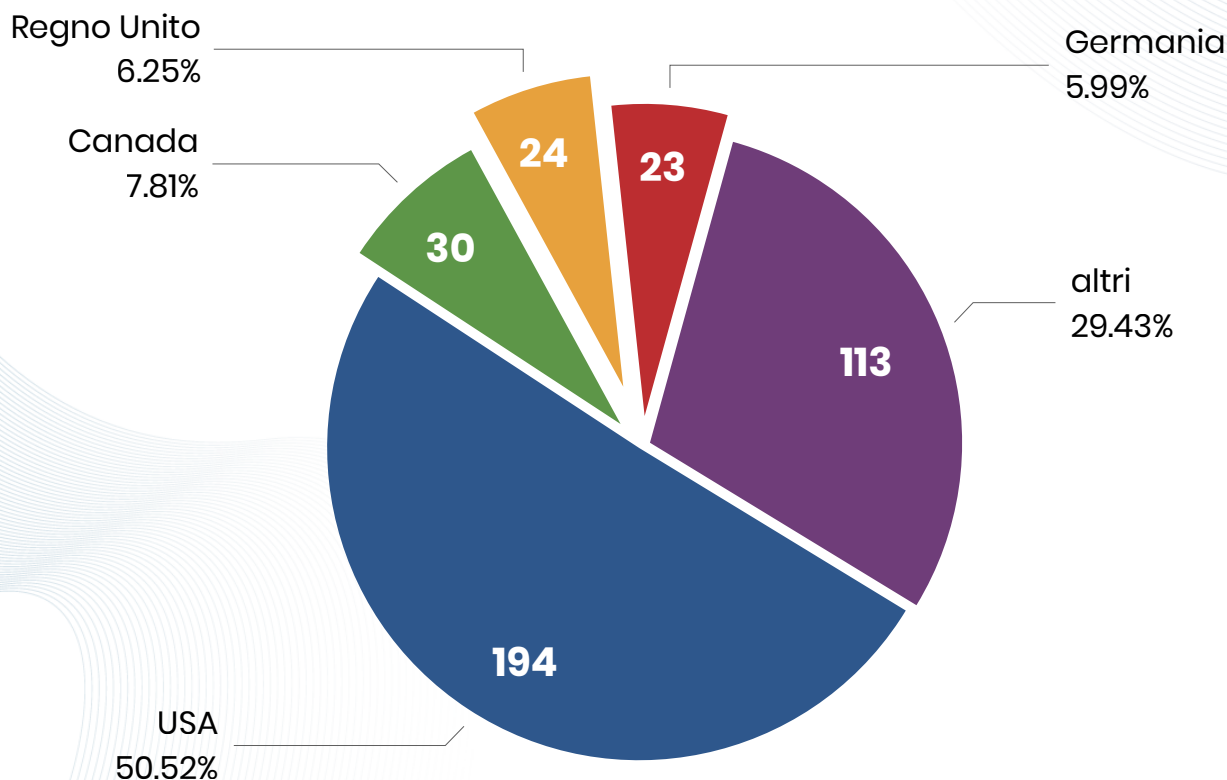
Anche per la scena internazionale, pubblichiamo la tabella con il numero totale delle rivendicazioni (al netto degli eventuali duplicati che potrebbero essere rilevati nei mesi successivi).

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



RansomHub

Check the panel's News Page, Updated



	2024-04-07	
*	<i>smelly__vx offers friendship, "Hello, I'm the admin of vx-underground. I want to say Hello :)"</i>	23:52:24
	2024-04-08	
smelly__vx	Hello:)	00:24:09
	I am the admin of vx-underground. I saw your recent post on Change Healthcare	00:28:04
	It's getting a lot of attention	00:28:13
RansomHub	Thank you very much for your attention, we will continue to publish news	00:57:57
smelly__vx	how did you get the change healthcare data?	01:02:30
RansomHub	Many alpha(Scammer)'s previous affiliates are actively joining us	01:13:05
	so can you understand what i mean	01:14:24

fonte: VX Underground



ransomfeed

ADVANCED DATADRIVEN CYBERNEWS

RECAP MENSILE MARZO 2024

/eof

