Encrypted Chat Apps Doubling as Illegal Marketplaces

nortonlifelock.com/blogs/research-group/chat-apps-illegal-marketplaces

Encrypted chat apps are gaining popularity worldwide due to their central premise of not sending user data to tech giants.

Some popular examples include WhatsApp, Telegram and Signal. These apps have also been adopted by businesses to securely communicate directly to their users. Additionally, these apps have been instrumental to subverting authoritarian regimes. For example, Telegram has been used by pro-democracy dissidents to organize protests in Hong Kong, and communicate amongst themselves in Russia, Belarus, Thailand, and Iran.

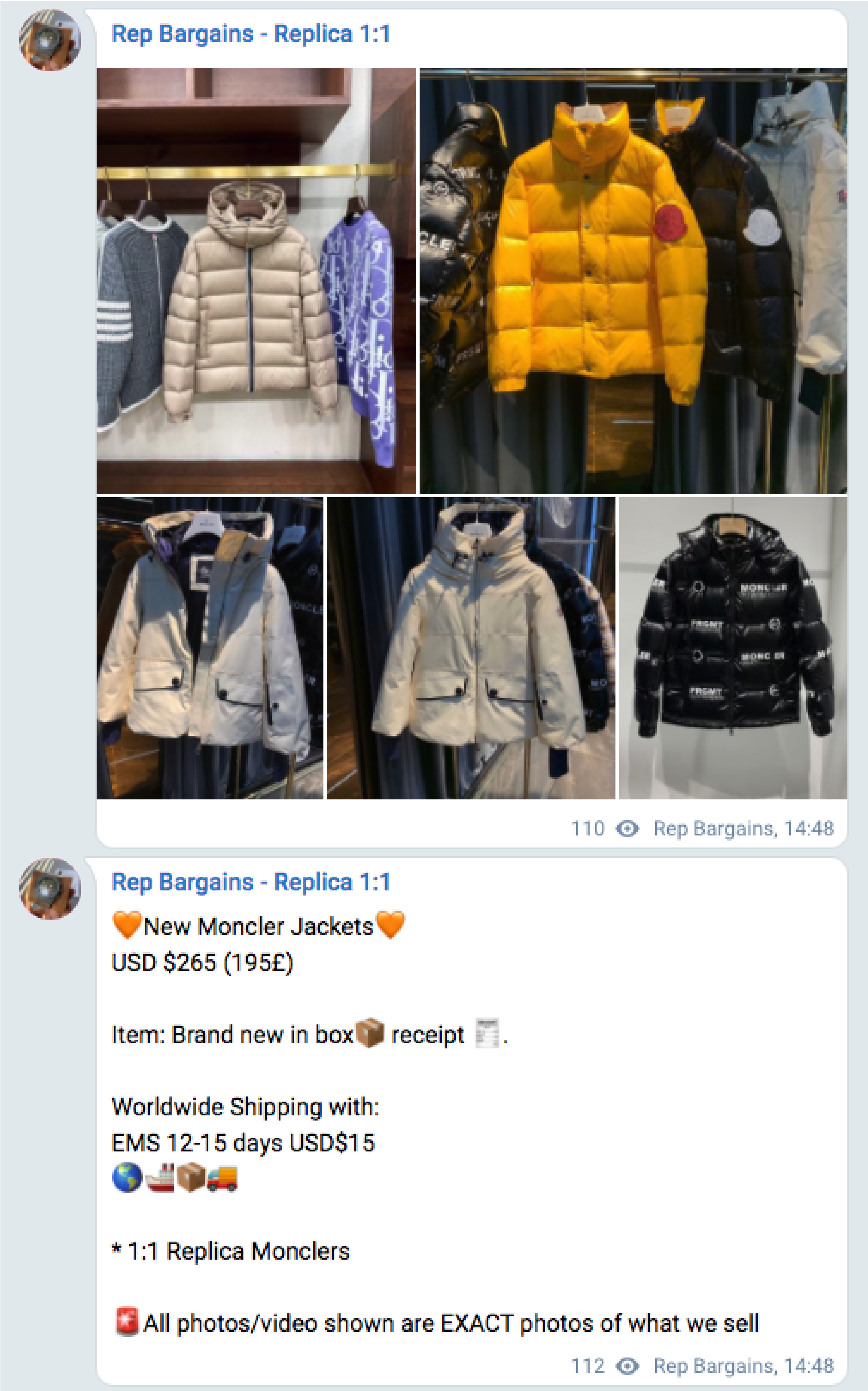
However, we've found that encrypted chat apps are also being used by criminals to sell illegal goods. Because content moderation is, by design, nearly impossible on these apps[1], they allow for an easy vector for dealers of illicit goods to communicate directly to customers without fear of law enforcement involvement. One example of this is Telegram, which provides especially strong anonymity protections, which are useful for dissidents, but can also be leveraged by criminals attempting to obscure their identities.

In our analysis, we found a wide variety of illegal goods are being sold on Telegram, including people's personally identifiable information (PII), likely stolen gift cards, fake documents, pirated software, and tools to facilitate cybercrime such as distributed denial-ofservice (DDoS) infrastructure. In recent months, we have also found several accounts dedicated to selling “COVID-19 vaccines,” targeting users in a variety of countries including the United States, China, India, Malaysia, and Russia.

Cybercriminals sell illegal goods for a variety of reasons. Sometimes, the goods are fake or counterfeit, leading to easy profits. In other cases, cybercriminals are trying to launder credit cards, or stolen gift cards, into money they can use.

Counterfeit Goods

Counterfeit goods are a popular product on Telegram. We found many accounts and groups dedicated to selling a wide variety of counterfeit goods, including luxury watches and purses, designer clothes, and high-end electronics. For example, you can find a counterfeit Rolex for as little as $69 USD.


Rep Bargains - Replica 1:1

110 👁 Rep Bargains, 14:48

Rep Bargains - Replica 1:1

🧡New Moncler Jackets🧡
USD $265 (195£)

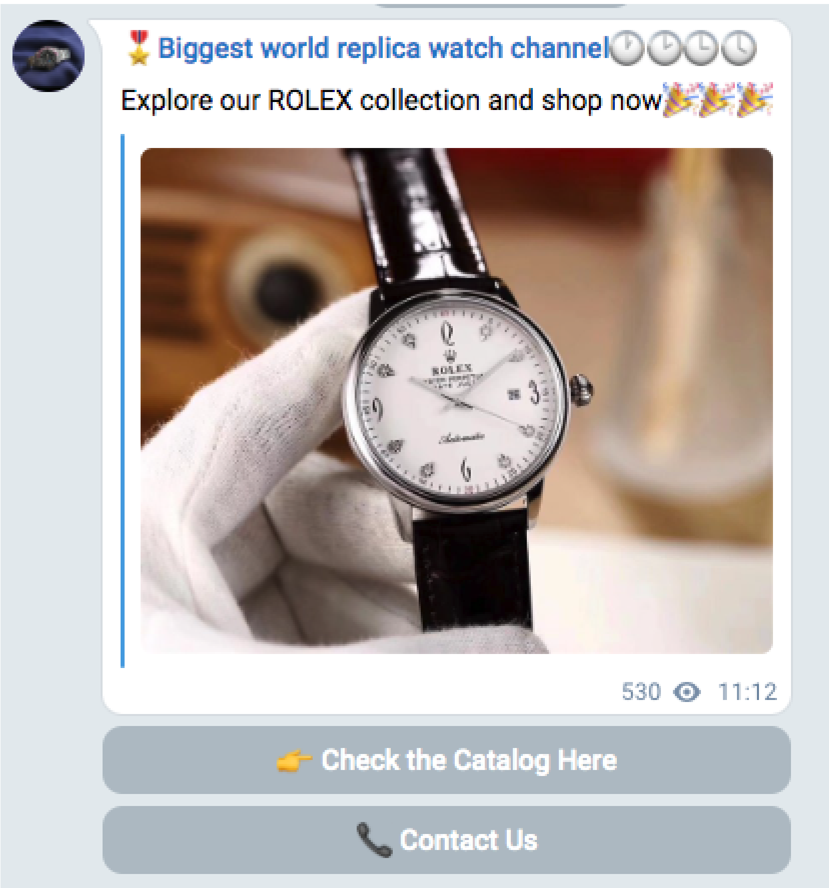
Item: Brand new in box📦 receipt 🧾.

Worldwide Shipping with:
EMS 12-15 days USD$15
🌎🚢📦🚚

* 1:1 Replica Monclers

🚨All photos/video shown are EXACT photos of what we sell

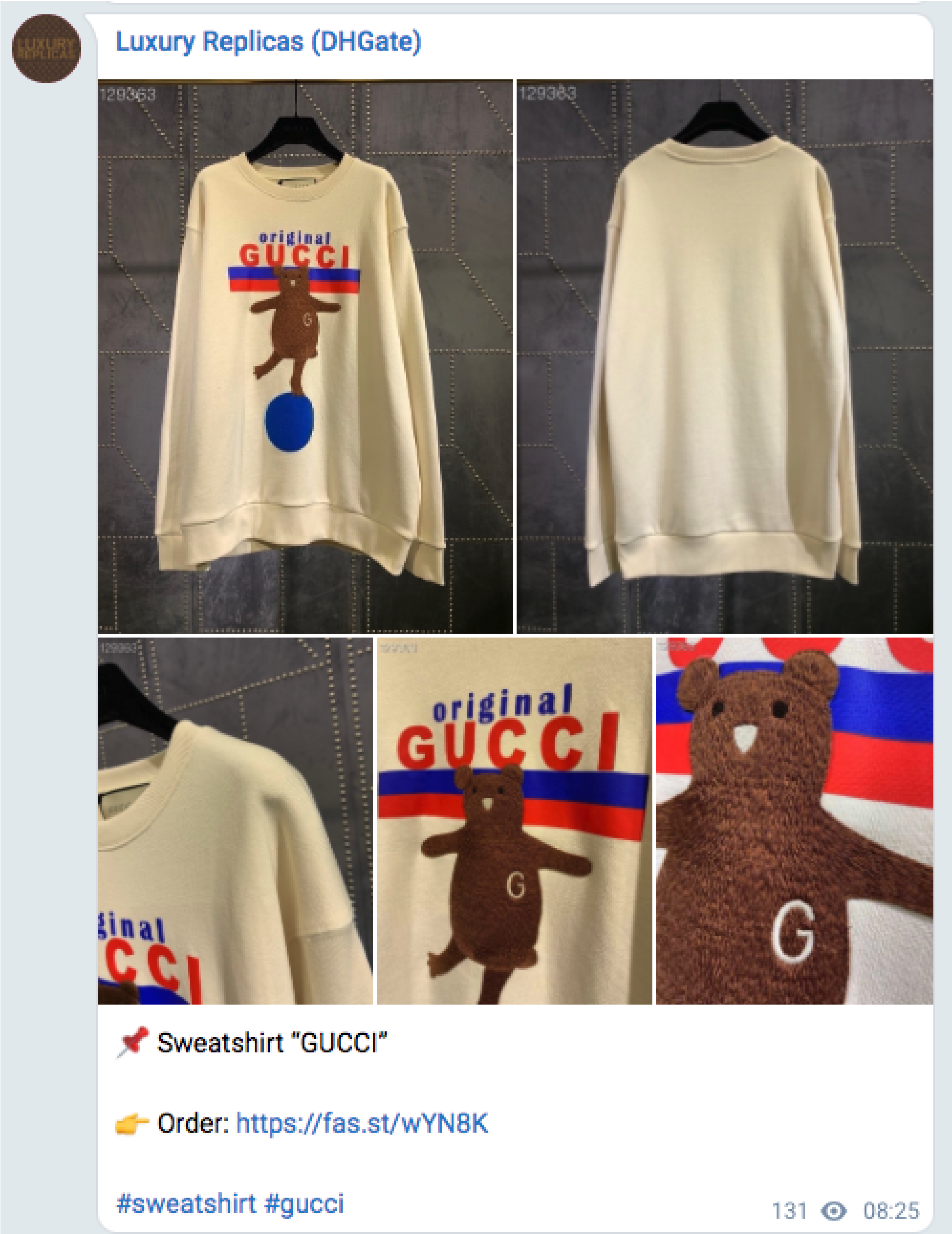
112 👁 Rep Bargains, 14:48



🎖️ Biggest world replica watch channel🕐🕑🕒🕓

Explore our ROLEX collection and shop now🎉🎉🎉

530 👁 11:12



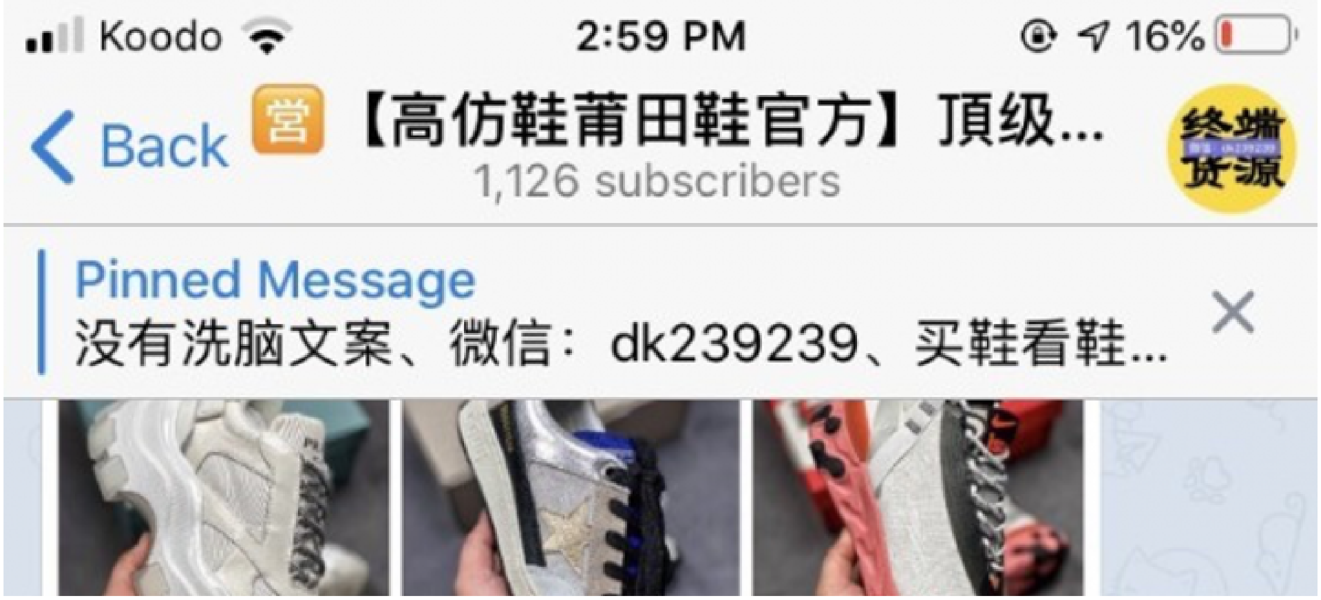
Luxury Replicas (DHGate)

📌 Sweatshirt “GUCCI”

👉 Order: https://fas.st/wYN8K

#sweatshirt #gucci

131 👁 08:25

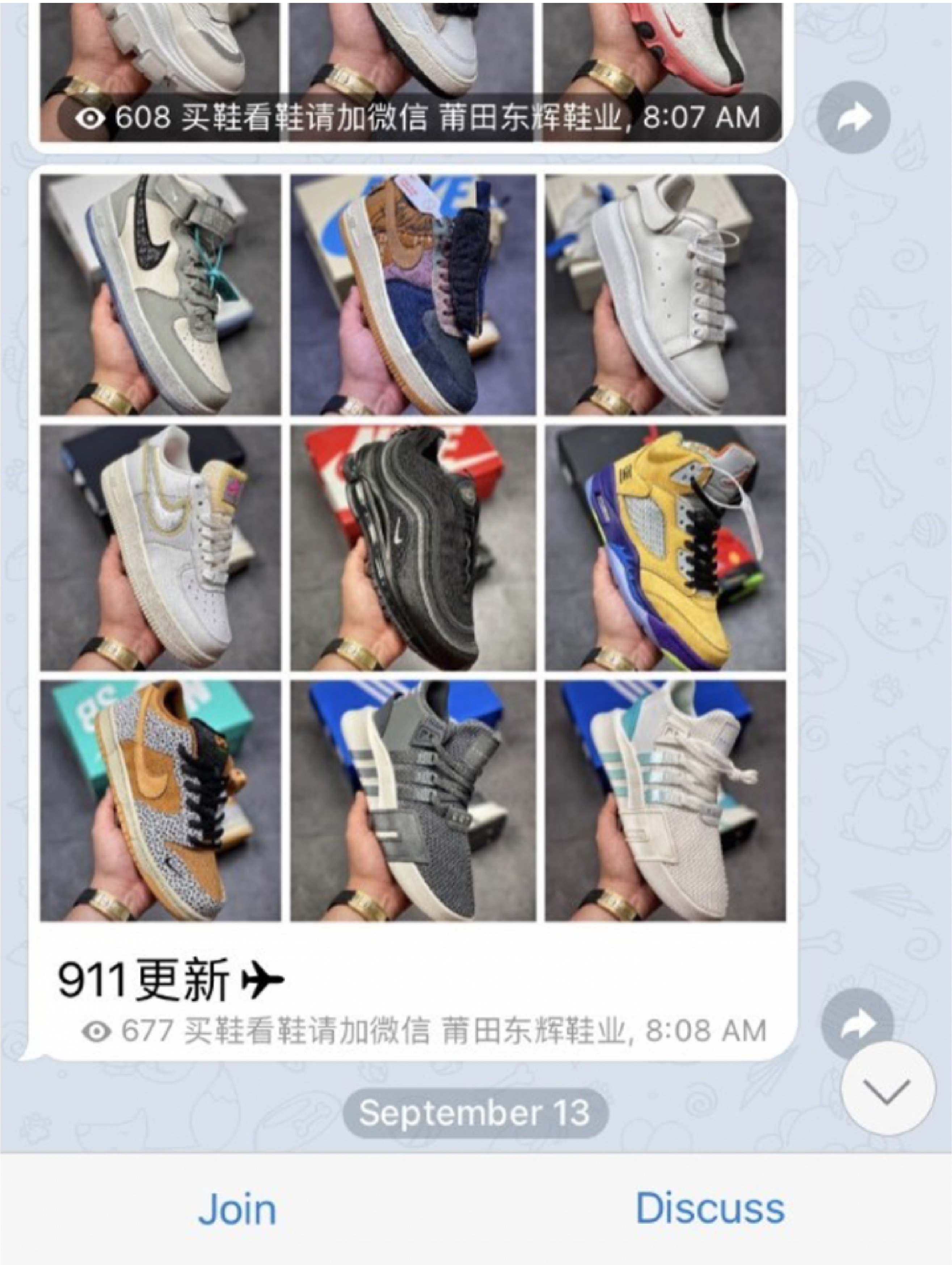


【高仿鞋莆田鞋官方】頂级...

1,126 subscribers

Pinned Message

没有洗脑文案、微信：dk239239、买鞋看鞋...



608 买鞋看鞋请加微信 莆田东辉鞋业, 8:07 AM

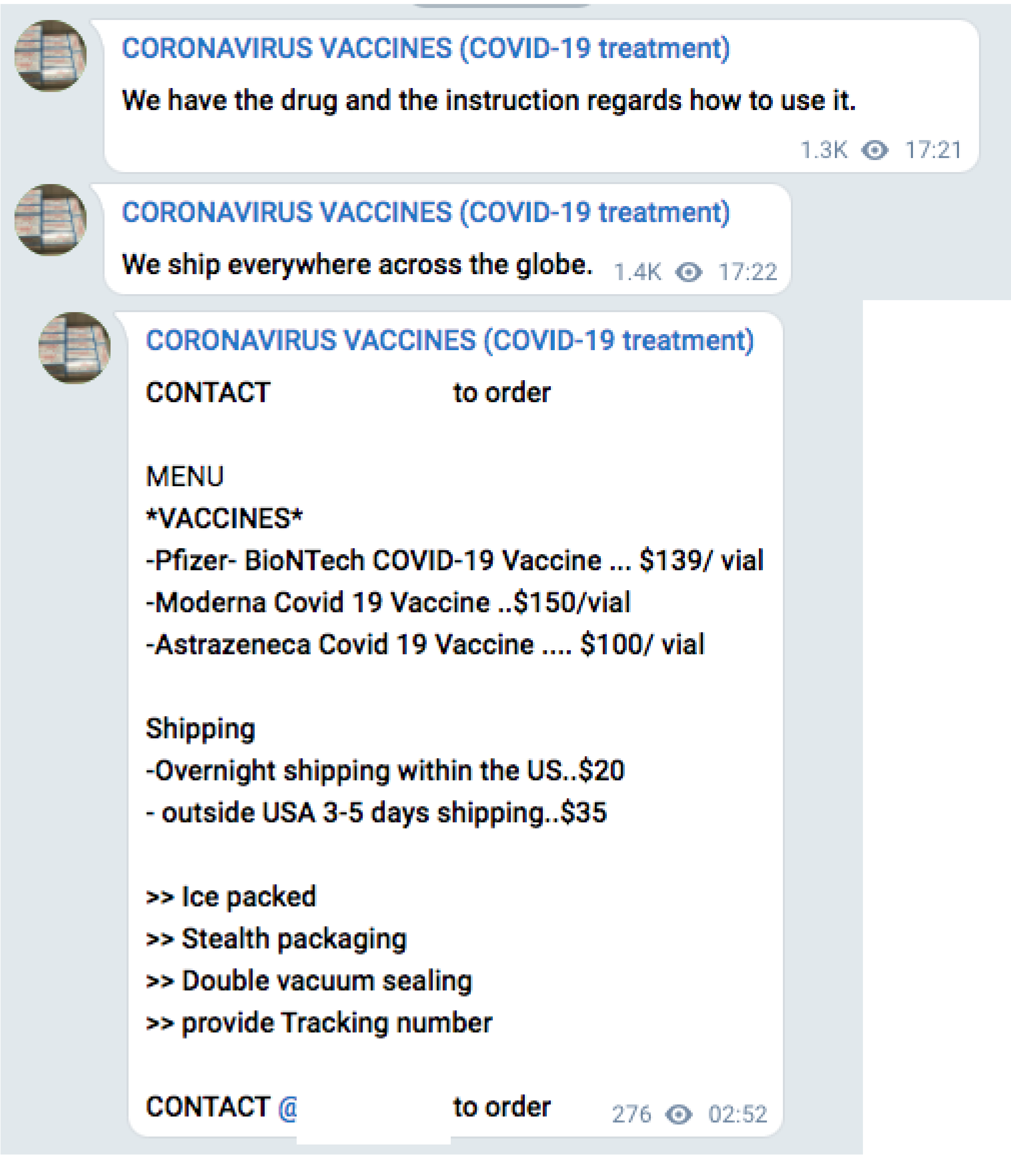
911更新 ✈

677 买鞋看鞋请加微信 莆田东辉鞋业, 8:08 AM

September 13

COVID-19 Vaccines

In recent months, with people anxious to receive a COVID-19 vaccine, criminals have attempted to take advantage of this stress by selling what they claim are COVID-19 vaccines.



CORONAVIRUS VACCINES (COVID-19 treatment)

We have the drug and the instruction regards how to use it.

1.3K 👁 17:21

CORONAVIRUS VACCINES (COVID-19 treatment)

We ship everywhere across the globe. 1.4K 👁 17:22

CORONAVIRUS VACCINES (COVID-19 treatment)

CONTACT [redacted] to order

MENU
VACCINES
-Pfizer- BioNTech COVID-19 Vaccine ... $139/ vial
-Moderna Covid 19 Vaccine ..$150/vial
-Astrazeneca Covid 19 Vaccine .... $100/ vial

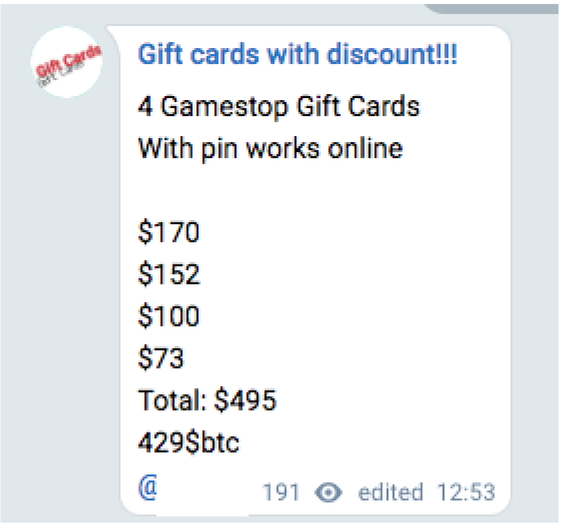
Shipping
-Overnight shipping within the US..$20
- outside USA 3-5 days shipping..$35

>> Ice packed
>> Stealth packaging
>> Double vacuum sealing
>> provide Tracking number

CONTACT @[redacted] to order 276 👁 02:52

Gift Cards

Cybercriminals often launder ill-gotten gains such as stolen credit cards through the purchase and sale of gift cards. Other times, the gift cards are stolen directly through either a password leak or via vulnerabilities in the gift card provider’s website. Those gift cards are then sold at heavily discounted prices.



Gift cards with discount!!!

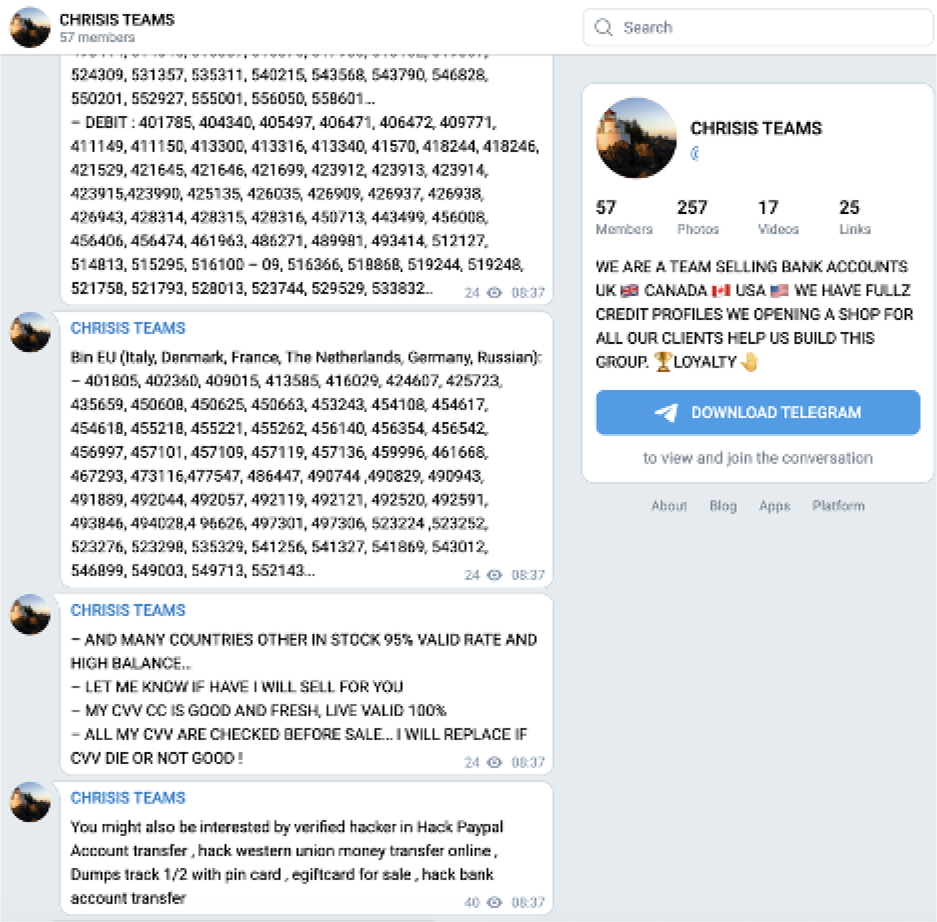
4 Gamestop Gift Cards
With pin works online

$170
$152
$100
$73
Total: $495
429$btc

@ 191 edited 12:53

Fake Documents and Personal Information

Another popular genre of illicit goods on Telegram are fake documents and personal information. Fueled by major data breaches such as the one at Experian, data brokers have amassed a shocking amount of personal information including social security numbers, addresses, phone number, bank account numbers, and more.



CHRISIS TEAMS
57 members

524309, 531357, 535311, 540215, 543568, 543790, 546828, 550201, 552927, 555001, 556050, 558601...
– DEBIT : 401785, 404340, 405497, 406471, 406472, 409771, 411149, 411150, 413300, 413316, 413340, 41570, 418244, 418246, 421529, 421645, 421646, 421699, 423912, 423913, 423914, 423915,423990, 425135, 426035, 426909, 426937, 426938, 426943, 428314, 428315, 428316, 450713, 443499, 456008, 456406, 456474, 461963, 486271, 489981, 493414, 512127, 514813, 515295, 516100 – 09, 516366, 518868, 519244, 519248, 521758, 521793, 528013, 523744, 529529, 533832..

24 08:37

CHRISIS TEAMS

Bin EU (Italy, Denmark, France, The Netherlands, Germany, Russian):
– 401805, 402360, 409015, 413585, 416029, 424607, 425723, 435659, 450608, 450625, 450663, 453243, 454108, 454617, 454618, 455218, 455221, 455262, 456140, 456354, 456542, 456997, 457101, 457109, 457119, 457136, 459996, 461668, 467293, 473116,477547, 486447, 490744 ,490829, 490943, 491889, 492044, 492057, 492119, 492121, 492520, 492591, 493846, 494028,4 96626, 497301, 497306, 523224 ,523252, 523276, 523298, 535329, 541256, 541327, 541869, 543012, 546899, 549003, 549713, 552143...

24 08:37

CHRISIS TEAMS

– AND MANY COUNTRIES OTHER IN STOCK 95% VALID RATE AND HIGH BALANCE..
– LET ME KNOW IF HAVE I WILL SELL FOR YOU
– MY CVV CC IS GOOD AND FRESH, LIVE VALID 100%
– ALL MY CVV ARE CHECKED BEFORE SALE.. I WILL REPLACE IF CVV DIE OR NOT GOOD !

24 08:37

CHRISIS TEAMS

You might also be interested by verified hacker in Hack Paypal Account transfer , hack western union money transfer online , Dumps track 1/2 with pin card , egiftcard for sale , hack bank account transfer

40 08:37

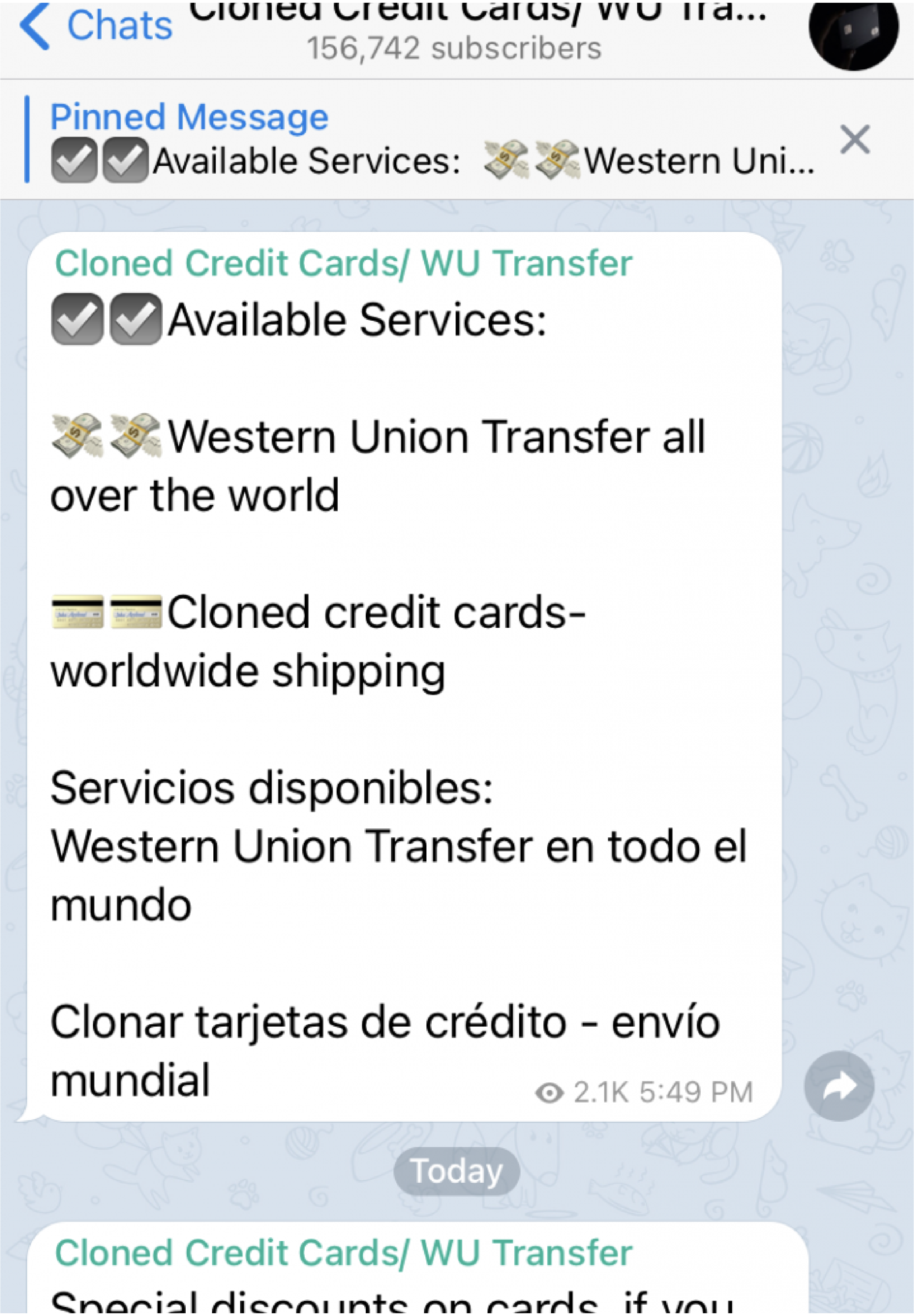
CHRISIS TEAMS
@

57	257	17	25
Members	Photos	Videos	Links

WE ARE A TEAM SELLING BANK ACCOUNTS UK 🇬🇧 CANADA 🇨🇦 USA 🇺🇸 WE HAVE FULLZ CREDIT PROFILES WE OPENING A SHOP FOR ALL OUR CLIENTS HELP US BUILD THIS GROUP. 🏆LOYALTY 👋

DOWNLOAD TELEGRAM
to view and join the conversation
About
Blog
Apps
Platform

Koodo
4:22 PM
49%
Cloned Credit Cards/ WU Tra



< Chats
Cloned Credit Cards/ WU Tra...
156,742 subscribers
Pinned Message
☑️☑️Available Services: 💸💸Western Uni...

Cloned Credit Cards/ WU Transfer

☑️☑️Available Services:

💸💸Western Union Transfer all over the world

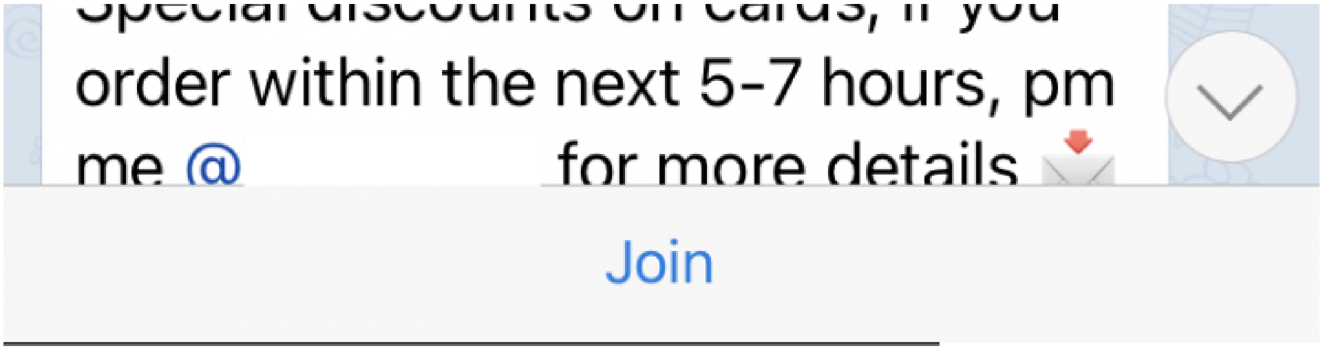
💳💳Cloned credit cards- worldwide shipping

Servicios disponibles:
Western Union Transfer en todo el mundo

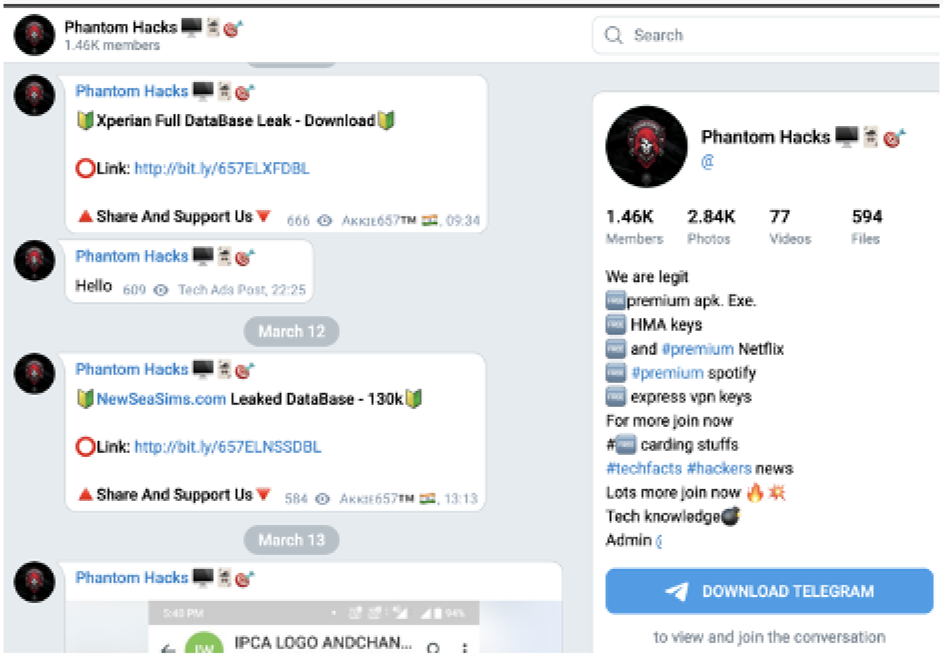
Clonar tarjetas de crédito - envío mundial

Cloned Credit Cards/ WU Transfer

Special discounts on cards, if you



Special discounts on cards, if you order within the next 5-7 hours, pm me @ [redacted] for more details 📩



Phantom Hacks 🖥️📱🎯

🔰Xperian Full DataBase Leak - Download🔰

⭕Link: http://bit.ly/657ELXFDBL

🔺Share And Support Us🔻 666 👁 Akkie657™ 🇮🇳, 09:34

Phantom Hacks 🖥️📱🎯

Hello 609 👁 Tech Ads Post, 22:25

March 12

Phantom Hacks 🖥️📱🎯

🔰NewSeaSims.com Leaked DataBase - 130k🔰

⭕Link: http://bit.ly/657ELNSSDBL

🔺Share And Support Us🔻 584 👁 Akkie657™ 🇮🇳, 13:13

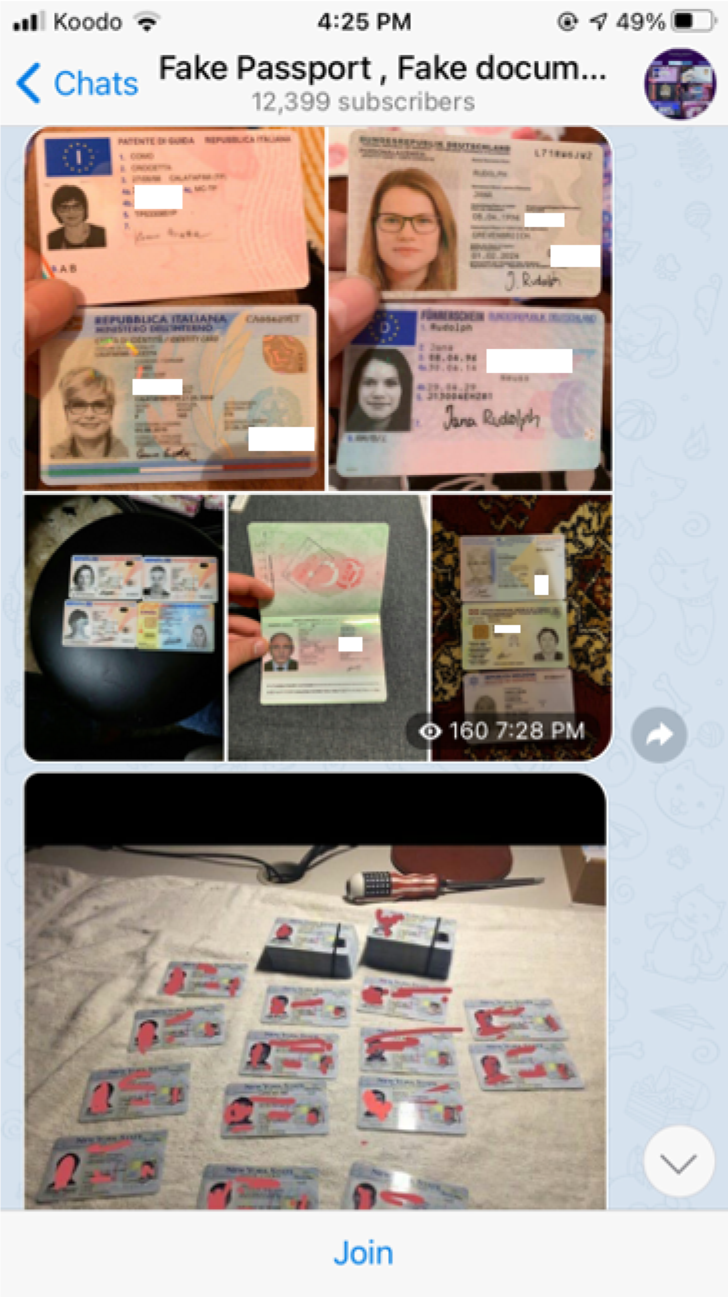
March 13

Phantom Hacks 🖥️📱🎯

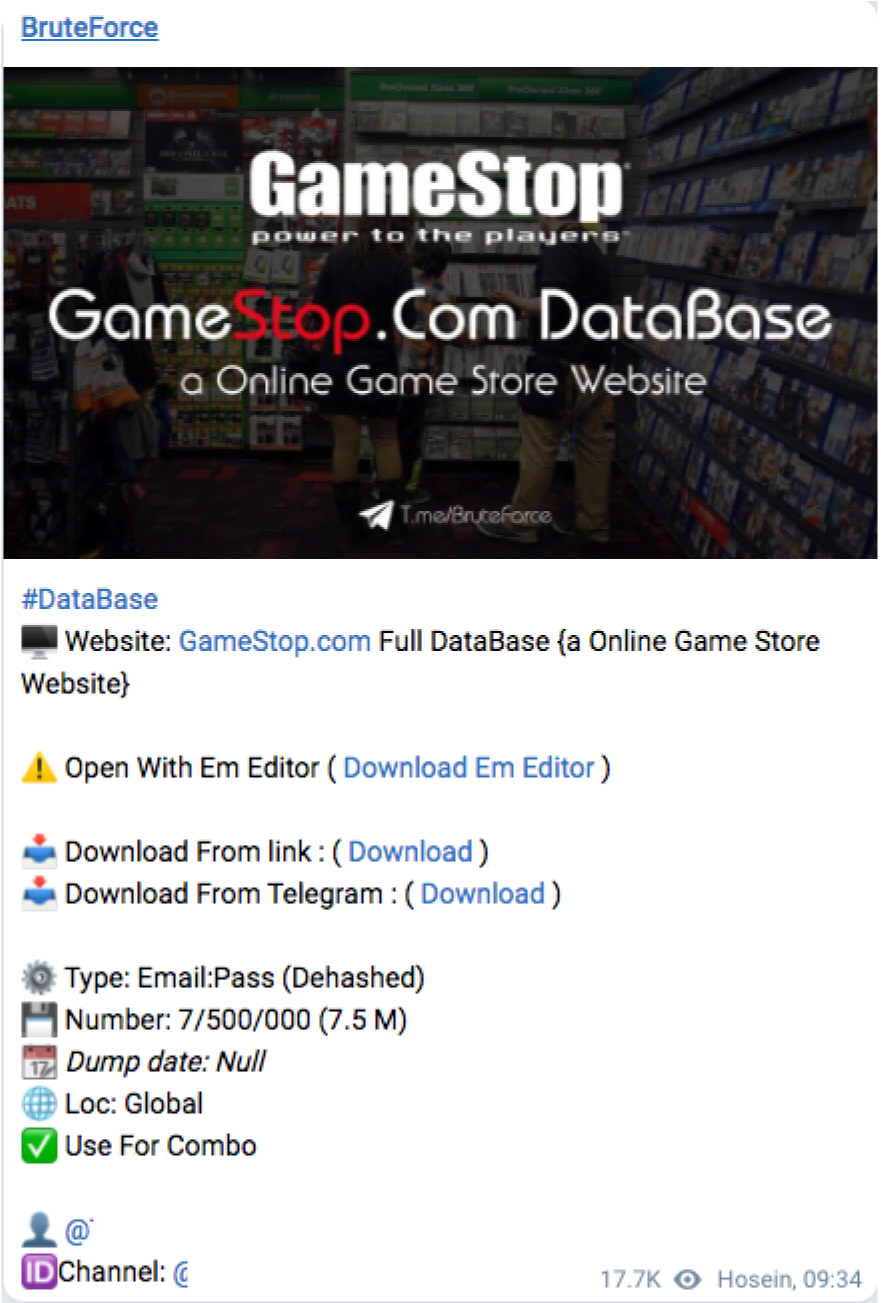
Phantom Hacks 🖥️📱🎯
@

1.46K	2.84K	77	594
Members	Photos	Videos	Files

We are legit
🆓premium apk. Exe.
🆓 HMA keys
🆓 and #premium Netflix
🆓 #premium spotify
🆓 express vpn keys
For more join now
#🆓 carding stuffs
#techfacts #hackers news
Lots more join now 🔥💥
Tech knowledge💣
Admin @



Some accounts even strategically market their items for sale to coincide with newsworthy events. We found a vendor offering hacked GameStop accounts around the time of that GameStop stock’s growth drew worldwide attention.



BruteForce

#DataBase
🖥 Website: GameStop.com Full DataBase {a Online Game Store Website}

⚠️ Open With Em Editor (Download Em Editor)

📥 Download From link : (Download)
📥 Download From Telegram : (Download)

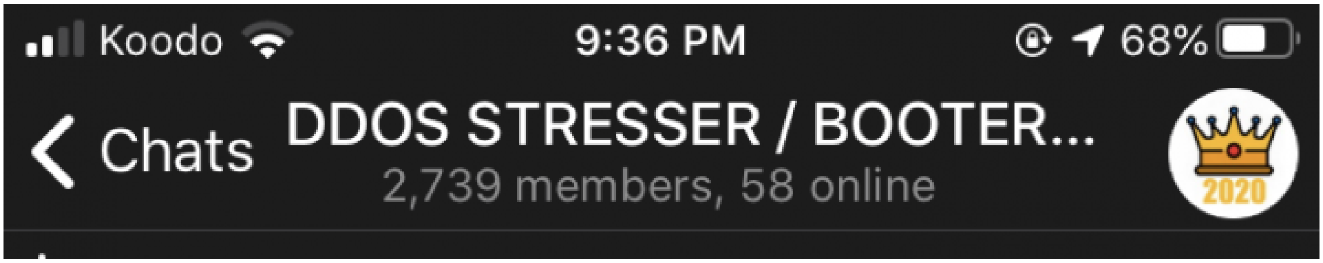
⚙️ Type: Email:Pass (Dehashed)
💾 Number: 7/500/000 (7.5 M)
📆 *Dump date: Null*
🌐 Loc: Global
✅ Use For Combo

👤 @
🆔Channel: @

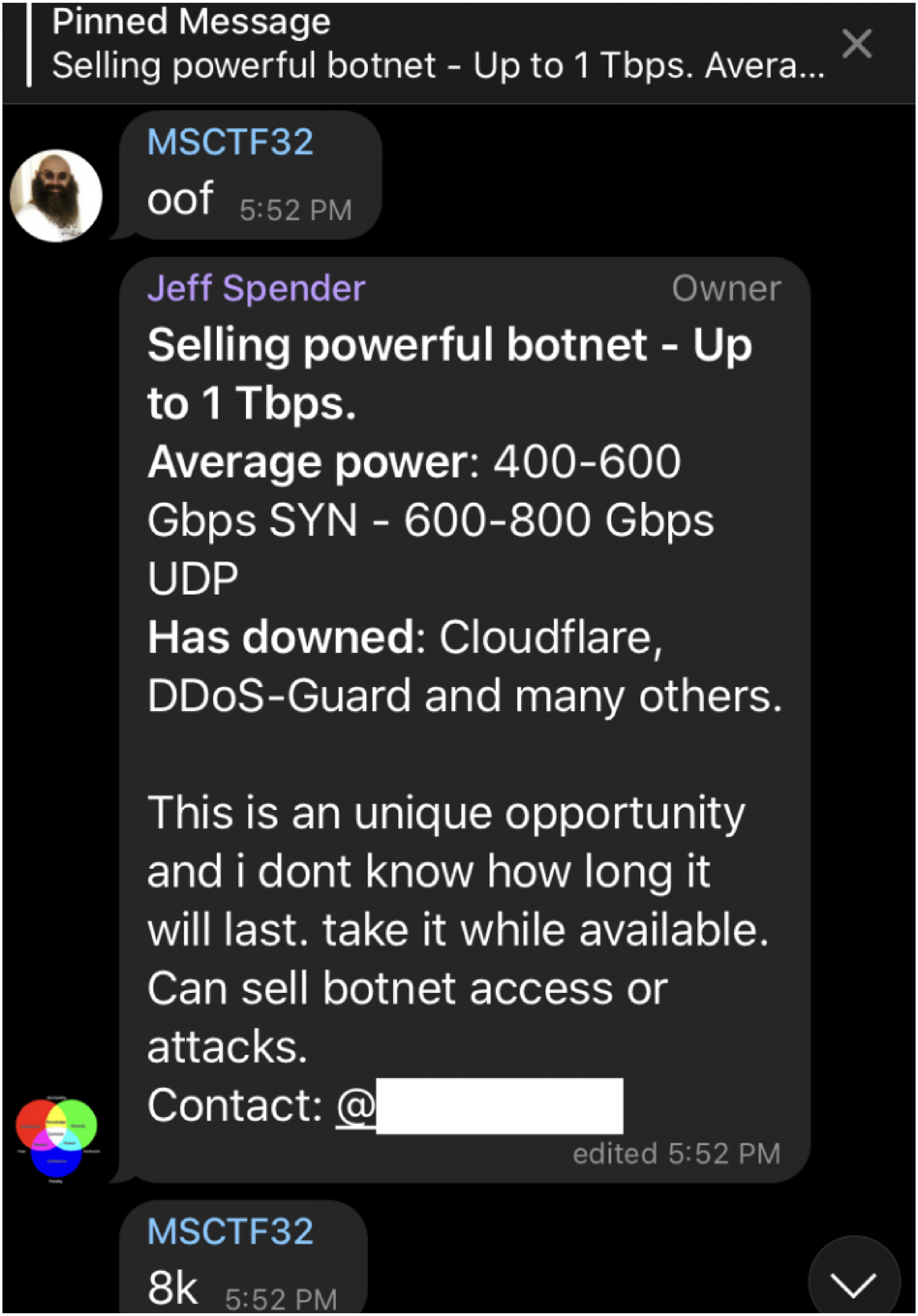
17.7K 👁 Hosein, 09:34

Tools to Facilitate Cyber-Crime

Interestingly, we observed that cybercriminals are also selling a variety of tools and services, including rental of DDoS infrastructure. We also found accounts marketing cheats for a variety of games, and services marketing themselves for users in India, Europe, Russia, the Arab world, and North America.



DDOS STRESSER / BOOTER...
2,739 members, 58 online



Pinned Message
Selling powerful botnet - Up to 1 Tbps. Avera...

MSCTF32
oof 5:52 PM

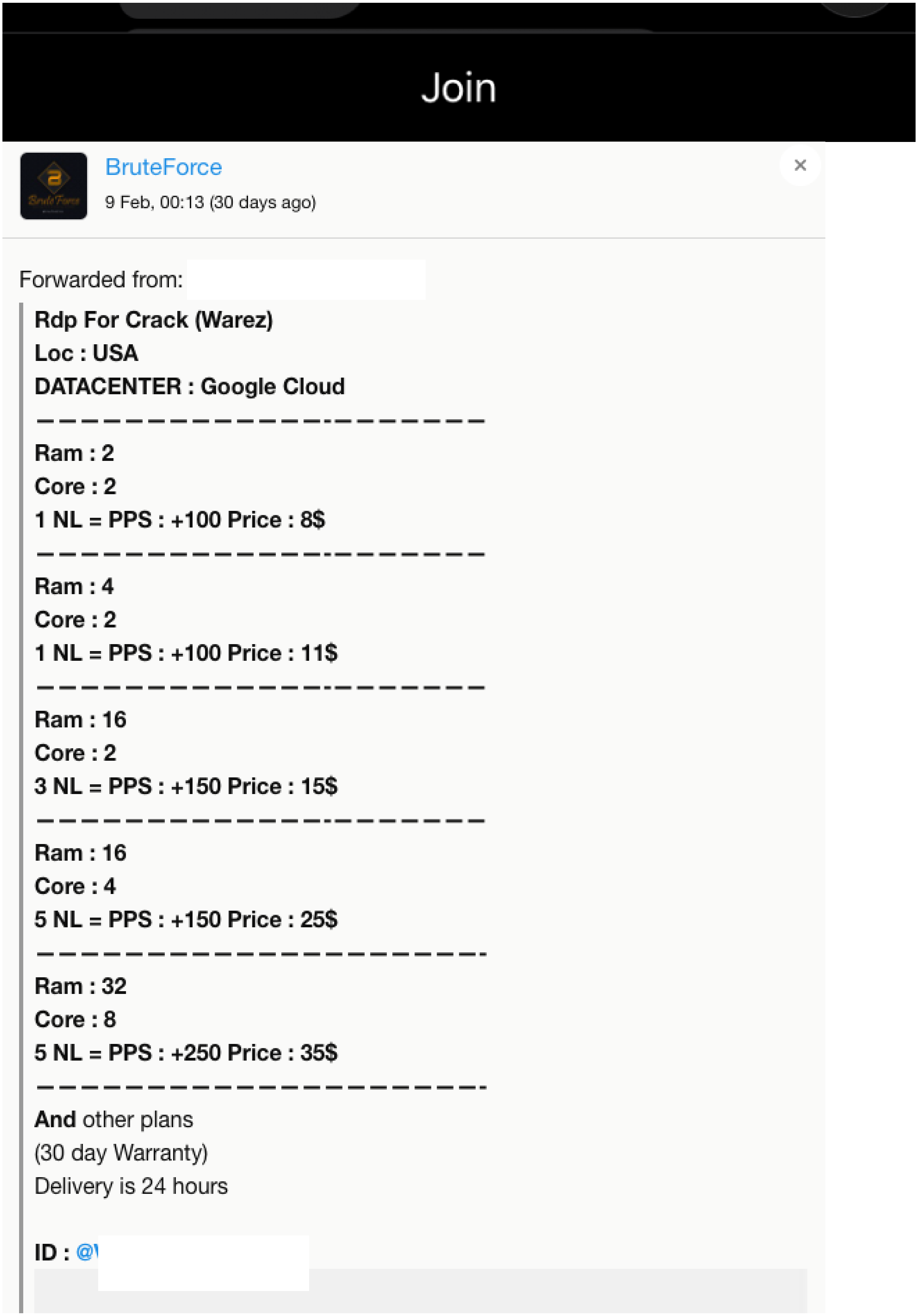
Jeff Spender Owner

Selling powerful botnet - Up to 1 Tbps.
Average power: 400-600 Gbps SYN - 600-800 Gbps UDP
Has downed: Cloudflare, DDoS-Guard and many others.

This is an unique opportunity and i dont know how long it will last. take it while available.
Can sell botnet access or attacks.
Contact: @[redacted]

edited 5:52 PM

MSCTF32
8k 5:52 PM



BruteForce
9 Feb, 00:13 (30 days ago)

Forwarded from: [redacted]

Rdp For Crack (Warez)
Loc : USA
DATACENTER : Google Cloud
——————————————————————
Ram : 2
Core : 2
1 NL = PPS : +100 Price : 8$
——————————————————————
Ram : 4
Core : 2
1 NL = PPS : +100 Price : 11$
——————————————————————
Ram : 16
Core : 2
3 NL = PPS : +150 Price : 15$
——————————————————————
Ram : 16
Core : 4
5 NL = PPS : +150 Price : 25$
——————————————————————
Ram : 32
Core : 8
5 NL = PPS : +250 Price : 35$
——————————————————————
And other plans
(30 day Warranty)
Delivery is 24 hours

ID : @[redacted]

Summary

Scammers, fraudsters and hucksters of illegal goods are usually ahead of the curve on the latest technologies to provide a good experience for their customers. Therefore, we often see these actors as early adopters of popular technologies (cybercriminals were also among the first to adopt cryptocurrencies such as BitCoin and Ethereum, which are now widely used by the general public for entirely legal purposes). This case is no different, and our research suggests that in the future, legitimate merchants may also adopt messaging apps and the peer-to-peer selling model they allow, similar to Telegram’s.

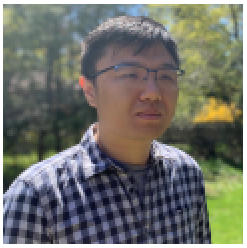
Innovations from Norton Labs are for research, evaluation, and consumer feedback purposes. NortonLifeLock does not give any warranties as to the suitability or usability of these prototypes and recommends safeguarding data and reviewing all terms and conditions before use.

About the Author

Daniel Kats

Senior Principal Researcher

Daniel earned his Masters at the University of Toronto Systems & Networking Group. His research involves building machine learning systems for security, and the subtle impact of those systems on the people who use them.



About the Author

David Zhuang

Software Engineer

David is a software engineer in Toronto working at NortonLifelock. He has eight years of experience with web development, DevOps with strong interest in security. In his spare time, David enjoys reading and translating.