



ZEROFOX[®]

Your Intelligence Digest

**It's a Digital World.
Engage Securely.**

Automated Telegram Service Provides Network Access To Paying Members

New and untested threat actor “barf” announced an automated Telegram service that provides paying members with network access to various targets worldwide on the predominantly Russian language Deep Web forum “XSS.” Most network access deals are typically conducted manually, giving vendors more time to negotiate and potentially scam would-be buyers. The service offers remote desktop access (RDP) access with user and administrator-level rights to approximately ten different target networks per month, including individual and corporate instances.

The actor noted the same RDP accesses would be shared among all members of the group. While some peers expressed concern over this, the majority supported the service, stating that most network access brokers sell the same network access bundles to multiple buyers anyway, despite claims the deals are exclusive.

The subscription fee for the service was \$100 USD per month. The group was limited to 35 members.

Original post from threat actor "barf" announcing an automated Telegram service that provides paying members with network access to various targets worldwide

Automated Telegram Service Provides Network Access To Paying Members (Cont.)


barf
Premium
Premium

Sign up: 03.02.2023
Messages: 2
Reaction: 0

Today at 01:24

A unique product that allows you to save money. For only [\\$ 100 per month](#) you will receive a subscription to the channel, which publishes a constantly updated [catalog of rDP from pentest*](#)

1 In the list you will find access of any kind - [admin / user, server / home OS, as well as with domains](#) **

1 You no longer need to wait for a response to purchase access. If you need 10 or more accesses per month - this option is great for you and will clearly recoup your investment.

1 The number of places is limited - [there are 35 seats](#)

1 left **At the end of February, 500\$*****

will be drawn ***the list ~once a week, for your convenience, is checked for valid for a new one + part of the material has already been minted for rights and as*

***the list has already been sorted by country*

\$ 500 will be received by a random user who [subscribed from a](#)

[→](#) bot to a bot

More Supply Than Demand For Access Deals Involving WordPress Accounts

In mid-February 2023, well-regarded threat actor “punktir” cancelled an auction for administrator access to 10,500 compromised WordPress accounts, citing a lack of interest from potential buyers, on the predominantly Russian language Deep Web forum Exploit. This likely indicates the number of access deals involving WordPress accounts across the criminal underground far exceeds the current demand from attackers.

For years, threat actors have targeted websites built on WordPress to perform various cyber-attacks, including:

- Website defacement
- Phishing/spamming
- URL hijacking
- Malware distribution
- Stealing the personally identifiable information (PII) of victims

The actor originally listed the access for auction in mid-January 2023, with a starting bid of \$3,250 USD, a minimum bid of \$250 USD and an instant purchase price of \$5,250 USD. The actor eventually decreased the price before cancelling the auction.

Original post from threat actor "punktir" cancelling an auction for administrator access to 10,500 compromised WordPress accounts due to lack of interest from potential buyers

More Supply Than Demand For Access Deals Involving WordPress Accounts (Cont.)



10500 wp-admin accounts with rights

By Punktir, January 15 in Auctions

Punktir

megabyte



Seller



65 posts

Joined

02/18/21 (ID: 114266)

Activity

вирусология / malware

Posted January 15

the winner will receive 10500 valid wordpress accounts with administrator rights, without duplicates
verification with your database on my side is available, work is available through the guarantor at your expense

start 3250\$ (0.3 per admin panel)

step 250\$

flash 5250\$ (0.5 for admin)

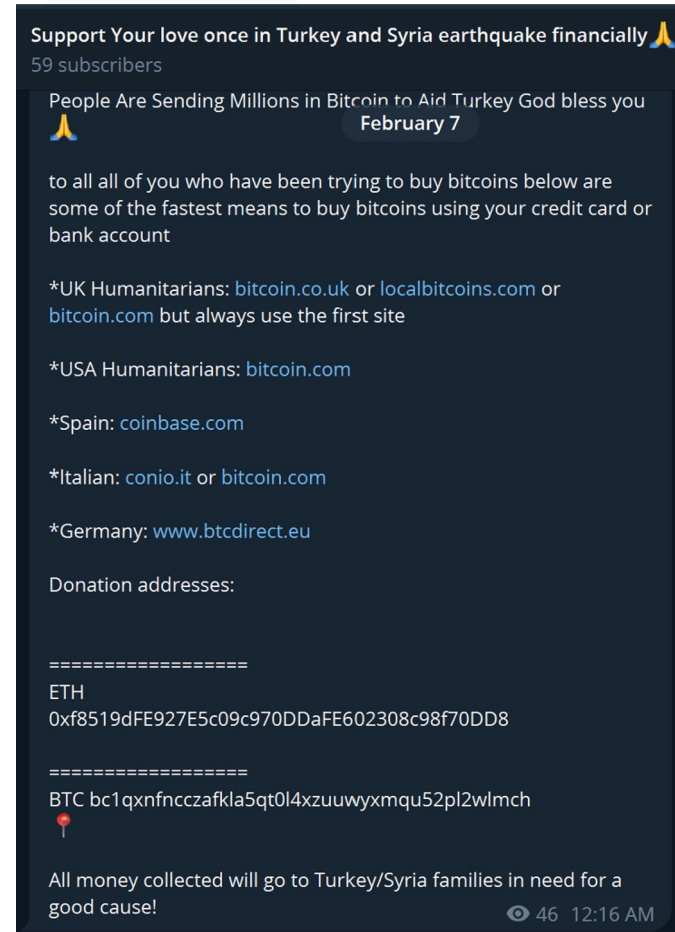
telegram for communication @wctrlshift

Scammers Looking To Profit From Recent Earthquakes In Turkey & Syria

In early February 2023, ZeroFox researchers identified new Telegram channels run by scammers looking to profit from the recent earthquakes in Turkey and Syria. One channel, “Support Your love once in Turkey and Syria earthquake financially,” is asking for Bitcoin donations for those affected. Specifically, the channel is soliciting for funds from the following countries:

- U.S.
- U.K.
- Spain
- Italy
- Germany

The administrator of the channel also shared a screenshot of what they claimed to be a successful payment transaction. It is virtually certain this was done to make the campaign look more legitimate to potential victims.



Service Scans Target Networks For Vulnerabilities Using Commercial Tools

New and untested threat actor “CINT” advertised a service that scans target networks for vulnerabilities on the predominantly Russian language Deep Web forum “XSS.” The service gives threat actors access to licensed copies of commercial penetration testing tools at heavily discounted rates, including:

- Metasploit Professional
- Invicti Enterprise
- Acunetix
- Burp Suite Enterprise

For an additional fee, the service team can also help threat actors set up their own command-and-control (C2) servers using Metasploit Professional, Cobalt Strike, or Brute Ratel. This would allow the actors to maintain communications with any compromised devices on a network.

Prices for the service started at \$35 USD per scan. It cost \$300 USD per month for unlimited scans.



CINT
HDD-drive

Пользователь

Регистрация: 01.01.2023
Сообщения: 25
Реакции: 1

Суббота в 17:42

CINT Scanner as a Service

How does SaaS work?
With our service you can scan websites and servers for vulnerabilities with premium tools quickly and at a cheap price. We can also help you set up your pentesting infrastructure.

Why CINT SaaS

Anonymity
With us you won't have to worry about anonymity, all it takes is a Monero payment and the scan will be made by completely untraceable servers for you.

Fast
No more boring hours setting up your vps, connecting to it thru tor, installing your tools and just then starting the scan. We manage all of it for you, you just have to wait for the scan result in the mail.

Security
We use official and up-to-date tooling so you won't risk infecting yourself or compromising the security of the penetration test by pirating the tools from non-trusted sources.

Cheap
We offer tens of thousands of dollars of tooling starting at just 35\$!

----- Note: single \$300 monthly subscription includes unlimited scans for all scanners.