



ZEROFOX[®]

Your Intelligence Digest

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

Russian Forum 'Exploit' Requiring Users To Enable Multi-Factor Authentication

The administrator of the Russian language Deep Web forum "Exploit" has announced that all users will soon be required to enable multi-factor authentication (2FA) on their accounts. The forum is implementing the change because an increasing number of threat actors are compromising Deep and Dark Web forum accounts, likely to avoid having to pay registration fees or to scam their peers.

The forum's competitor, "XSS," has also made changes recently to deter fraud, mandating that all forum users make transactions via an automated escrow service.

"Exploit" users have until December 20, 2022 to enable 2FA, or their accounts will be disabled.

A

Обязательная двух-факторная авторизация!

By admin, November 17 in About Exploit.IN Site and Forum

Follow 1

Start new topic

admin

<forum.status>

●●●●●●●●

A

Admin

1168

6915 posts

Joined

02/18/05 (ID: 1)

Activity

другое / other

Deposit

0.001001 B

Posted November 17

Report post

Всем привет!

В связи с участвовавшими случаями кражи почт привязанных к аккаунтам форума, двух-факторная авторизация теперь становится обязательной.

До 20 декабря все участники форума должны включить 2FA самостоятельно.

Учетки без двух-факторной авторизации подлежат деактивации.

Восстановление аккаунта при утере ключа 2FA - не возможно.

Для включения 2FA, перейдите в [настройки аккаунта](#) > [Безопасность аккаунта](#)

Следуйте инструкциям.

Сохраните свой код 2FA и не теряйте его!

Browsers:

- Устанавливаем расширение

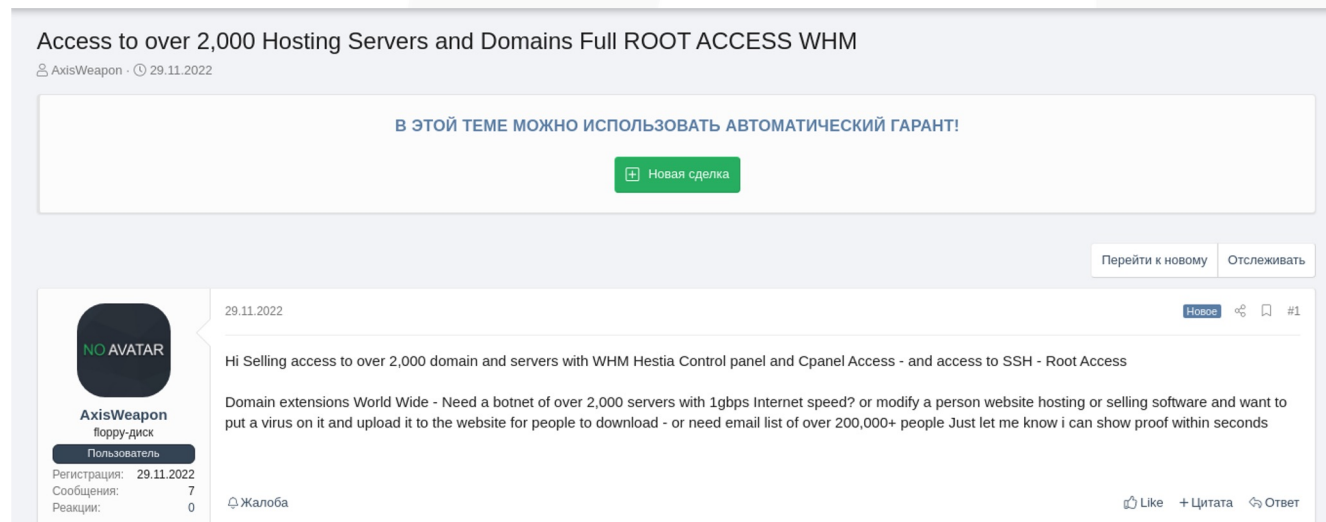
для firefox <https://addons.mozilla.org/en-GB/firefox/addon/auth-helper> (Source code <https://github.com/Authenticator-Extension/Authenticator>)

Actor Selling Root Access To 2,000 Compromised Linux Web Servers

New and untested threat actor “AxisWeapon” advertised root access to more than 2,000 compromised Linux servers running Hestia Control Panel on the predominantly Russian language Deep Web forum “XSS.” In addition to the web panels, the actor said the servers can also be accessed via Secure Shell (SSH), a protocol designed for remote administration. A skilled threat actor can almost certainly utilize these web servers for various cyber-attacks, including:

- Botnet creation
- Spread additional malware
- Perform domain hijacking
- Leak sensitive data
- Launch phishing or spam campaigns

ZeroFox researchers assess the actor likely exploited a new vulnerability in Hestia because of the high number of servers available, indicating that more threat actors are successfully compromising Linux-based machines.



Actor Claims Data Outlines Cyber-Attacks Launched By Chinese Government

New and untested threat actor “WoyouLuma” advertised 613 MB of sensitive data outlining various cyber-attacks allegedly launched by the Chinese government against targets worldwide on the predominantly Russian language Deep Web forum “Exploit.” Compromised data includes:

- The real identities of more than 100 state-sponsored threat actors
- Information about various China-based companies that allegedly supported the attacks
- A list of the alleged targets
- Internal communications between the threat actors involved
- Evidence of corruption in the Wuhan policy agency

The actor charged \$10,000 USD per document or \$150,000 USD for the complete dataset. They also offered to sell the personally identifiable information (PII) of individual threat actors for \$1,000 USD per person.

ZeroFox researchers assess the announcement of this data likely indicates that there is a government insider leaking secrets about China’s cyber warfare operations because the actor claims the information was obtained firsthand from the Chinese Ministry of State Security.

Original post from threat actor "WoyouLuma" advertising 613 MB of sensitive data outlining various cyber-attacks allegedly launched by the Chinese government against targets worldwide

Actor Claims Data Outlines Cyber-Attacks Launched By China (Cont.)



Wuhan government hacking database for sale

By WoyouLuma, November 30 in [Other] - everything else

Follow 1

Start new topic

Reply to this topic

WoyouLuma

byte



Paid registration

0

4 posts

Joined

11/29/22 (ID: 139767)

Activity

дpyroe / other

Deposit

0.000281 ₿

Posted November 30

Report post

Recently obtained a database of sensitive information about cyber attacks organized by the Chinese government in Wuhan. I am just a middleman, acting as an agent for the seller who provides the database. At least from the samples I got, the data is real. Below is an example.

Data can be purchased by individual record, by category, or in bulk. If you are interested, please contact me to negotiate the wholesale price. If you buy the entire database, consider exclusive sales.

Brief introduction:

1. The identities of more than 100 hackers working for the Chinese government in Wuhan and officials of the National Security Bureau responsible for organizing and coordinating cyber attacks, including names, photos, ID numbers, phone numbers, and home addresses. (1000 USD per identity)
2. The names, addresses, and internal documents of companies supporting the Wuhan State Security Bureau's cyberattacks. (10000 USD)
3. Lists of hacked entities around the world from an internal confidential database. (10000 USD)
4. Internal WeChat and Mixun communications between hackers in Wuhan. Content included cyberattacks, dissatisfaction with superiors' corruption, complaints about low pay, long working hours, and restrictions on travel. It also includes dissatisfaction with the government's new crown epidemic prevention and Internet restrictions. (20000 USD)
5. Evidence of cronyism and corruption among senior National Security Bureau leaders in Wuhan. (10000 USD)

If you are interested in purchasing, please private chat or contact WoyouLuma@proton.me to get the payment address.

Intel Broker Leaks Sensitive Email Data Related To Iran

Well-regarded threat actor and established intel broker “Spectre” leaked the sensitive Outlook data of two Iranian Ministry of Foreign Affairs employees on their Telegram channel “Spectre’s Intel Repository” (AKA “intelrepo”). In addition to email messages, the leaked files likely contain other sensitive data, including calendar events and contacts. The actor claims they disclosed the files in support of the Iranian demonstrators protesting the current regime, specifically the morality police.

In November 2021, “Spectre” advertised another data leak related to the Saudi Arabian government on the now defunct English language Deep Web forum “RaidForums.” Similarly, the actor obtained the leak from the email inboxes of Saudi military officials.

