



ZEROFOX[®]

Your Intelligence Digest

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

Actor Claims Russian Forum ‘Exploit’ Acquired By Security Service Of Ukraine

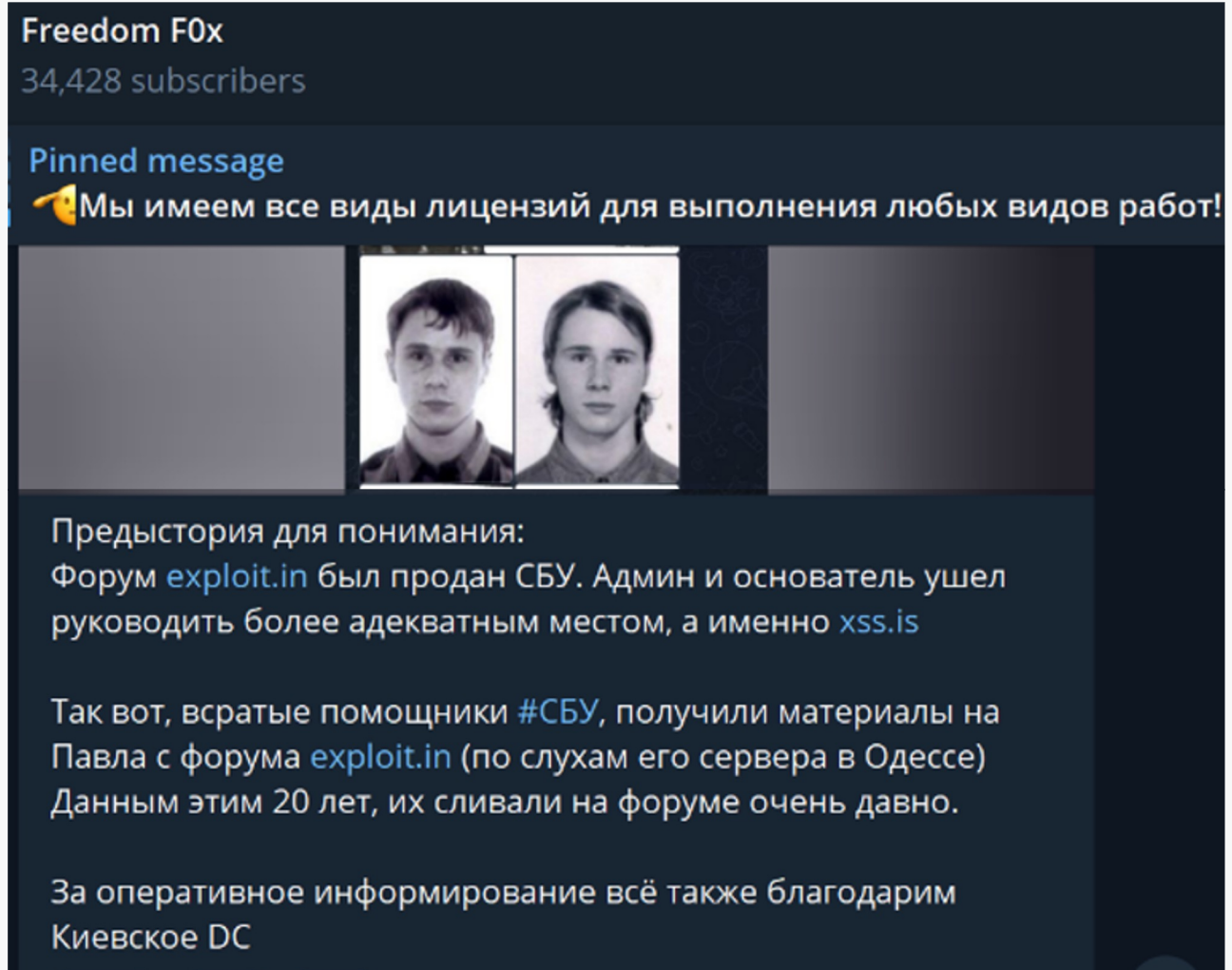
On October 31, 2022, the administrator of the well-regarded Russian language Telegram channel “Freedom F0x” announced the Security Service of Ukraine (also known as the SBU) has acquired the widely popular predominantly Russian language Deep and Dark Web forum exploit[.]in. ZeroFox researchers assess that pro-Russian threat actors will migrate to competing predominantly Russian language forum XSS to continue their operations.

The administrator of the “Freedom F0x” channel, who claims to have an insider at the SBU, said the agency likely has the real identity of at least one former “Exploit” administrator. The SBU will also possess the user information of various high-profile threat actors, including ransomware operators and network access brokers.

ZeroFox researchers assess the distinctions between pro-Russian and pro-Ukrainian threat actors will likely continue to grow on the criminal underground as the war between the two countries lingers.

Original post from the administrator of the well-regarded Russian language Telegram channel "Freedom F0x" announcing the Security Service of Ukraine has acquired the widely popular predominantly Russian language Deep and Dark Web forum exploit[.]in

Actor Claims 'Exploit' Acquired By Security Service Of Ukraine (Cont.)



Source Code For Twitter Account Generator Advertised

Untested threat actor “ericluho” advertised the source code for a Twitter account generator on the predominantly Russian language Deep Web forum “Exploit”. The actor claims the generator can create thousands of Twitter accounts themed around NFTs per hour. This indicates a threat actor can almost certainly use these accounts for phishing or spam campaigns aimed at would-be NFT investors. The actor specified the generator is written in Golang. They claim the resulting accounts will not be shadowbanned, a term that means Twitter will not prevent other Twitter users from viewing the fake accounts.

The actor charged \$3,500 USD for the source code.

ZeroFox researchers assess the sale of this source code will likely lead to a wide variety of spam campaigns on Twitter because a skilled threat actor can almost certainly change or modify the code to generate different types of accounts based on the target.



ericluho
kilobyte



Paid registration
33 posts
Joined
05/07/22 (ID: 130103)
Activity
кодинг / coder

Selling Twitter Account Generator

By ericluho, October 17 in [Social networks] - accounts, groups, hacking, mailing

Posted October 17

Selling twitter account gen, features :

- Written in golang
- Can make thousands of accounts per hour
- Accounts with nft profile pics
- Purely request Based
- Accounts aren't shadowbanned
- Full src

Accounts can be used to spam on twitter ect...

Price : 3.5k\$

MM accepted

Contact me on telegram : @monerobandit

Multifunctional Malware With Ransomware Capabilities Alleged

Untested threat actor “MicrosoftUpdateForXP” advertised a multifunctional malware, dubbed “KAWAS,” with distributed denial-of-service (DDoS), stealer, and ransomware capabilities on the English language Dark Web forum “CryptBB”. ZeroFox researchers assess a deal involving this malware would likely lead to the formation of new ransomware gangs, since the malware allows threat actors to quickly create and execute their own ransomware campaigns and assign user roles to team members via web panel. Additional features of the malware include:

- Works on systems running Windows, Linux, or macOS
- Deploys obfuscated agents (AKA modules)
- Will not be detected as malicious by most antivirus products
- Does not have software dependencies
- Avoids virtualization and analysis environments

Additionally, the actor specified the Windows version of the malware will maintain persistence even after a system reboot.

The actor is currently working on new features for the malware, including:

- Ransom negotiation portal
- Wiper agent that would allow a threat actor to erase the storage on a compromised machine

The actor charged \$499 USD for a lifetime license.

ZeroFox cannot rule out the possibility this offer is a scam because the actor lacks credibility on the forum and the asking price is very low compared to other malware with similar functionality.

Original post from
threat actor
"MicrosoftUpdateForXP"
advertising a
multifunctional
malware, dubbed
"KAWAS," with
distributed denial-of-
service (DDoS), stealer,
and ransomware
capabilities

Multifunctional Malware With Ransomware Capabilities (Cont.)

KAWAS Botnet | Cross Platform, Modular, Ransomware | Native



MicrosoftUpdateForXP •
Junior
Member

11-05-2022, 08:08 PM

Welcome to KAWAS Botnet!

When you need stealth to conduct your business use KAWAS!
Real-time encrypted communication with your agents.
Harvest information, Deploy ransomware (no fee, you own it 100%), Modular via Plugin System, Truly Cross Platform.
KAWAS is lightweight and super-fast to setup.

SCREENSHOTS
https://anonfiles.com/6egao6G5y7/kawas-promo_zip

Actor Selling Administrator Access To 23,000 Compromised WordPress Websites

Moderately credible threat actor “Punktir” advertised an auction for administrator access to 23,000 compromised WordPress websites on the predominantly Russian language Deep Web forum “Exploit”. It is virtually certain a skilled threat actor can leverage these sites for fraudulent operations, including:

- Stealing PII
- Spamming
- Mining cryptocurrency
- URL hijacking

The starting bid for the auction is \$5,000 USD, with a minimum bid of \$500 USD and an instant purchase price of \$11,500 USD.

ZeroFox researchers assess the actor likely exploited a new or unpatched vulnerability in WordPress to compromise the websites, since the bundle contains access to such a high volume of sites.



Punktir
kilobyte

23000 wp-admin accounts with rights
By Punktir, 13 hours ago in Auctions



Punktir
kilobyte

Paid registration
46 posts
Joined
02/18/21 (ID: 114266)
Activity
вирусология / malware

Posted 13 hours ago

the winner will receive 23000 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 5000\$ (0.21 per admin panel)
step 500\$
flash 11500\$ (0.5 for admin)

telegram for communication @wctrlshift

+ Quote