



ZEROFOX[®]

Your Intelligence Digest

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

Automated Telegram Service Generates Falsified Documents

Untested threat actor “mimic_bot” advertised an automated Telegram service that generates falsified documents, dubbed “mimic drawing bot,” on the predominantly Russian language Deep Web forum “Exploit.” The service can make various documents in minutes, including:

- Passports
- Driver’s licenses
- Various statements
- Utility bills

The actor claims they can also add readable barcodes to any document for a fee. They specified the documents do not contain metadata, increasing the anonymity of the user.

Prices for the documents range from \$10 USD to \$18 USD.

ZeroFox researchers assess this service will likely lead to an increase in fraud cases worldwide because it streamlines the process of forging documents from different countries, including the U.S., U.K., and Russia.

Original post from threat actor “mimic_bot” advertising an automated Telegram service that generates falsified documents, dubbed “mimic drawing bot”

Telegram Service Generates Falsified Documents (Cont.)

 **DOCUMENT GENERATOR BOT AND MIMIC MANUAL RENDERING**
By mimic_bot, Wednesday at 04:58 PM in [Other] - everything else

Follow 1

Start new topic

Reply to this topic

mimic_bot

byte



Paid registration

2 posts

Posted Wednesday at 04:58 PM

HELLO! GLAD TO WORK FOR YOU ON THIS FORUM!
Ourmimicdrawing bot will make any of your verif easy and fast! Don't wait for the pollsters for hours— do it yourself!

Prices for the generation of any documents\$ 2 (generation speedfrom 1 minute to 5)
In this case, you geta product of the highest qualitywith cleanedEXIFdata! (Free USA PASSPORT or FEMALE 25 age SELFIE WITH USA PASSPORT)
AllMRZreads like in the original!
Generation of barcodes2\$(up to 1 minute)
The available barcodes are indistinguishable from the original!!!

Report post

Actor Selling Web Injects Compatible With Android Banking Malware

Untested threat actor “schwarze_puppen” advertised a collection of 465 web injects compatible with an unspecified Android banking malware on the predominantly Russian language Dark Web forum “RAMP.” This is significant because there are currently a limited number of credible threat actors publicly brokering web injects that target financial institutions on the Russian underground.

A skilled threat actor can likely use these injects to compromise the accounts of different banking or online payment processing service customers. Such attacks typically allow threat actors to bypass multi-factor authentication to authorize fraudulent transactions or steal personally identifiable information (PII) from victims.

ZeroFox researchers assess the actor is likely credible because they have received positive feedback from at least one well-regarded peer on the forum.

465 injects for Android Banking Trojan

schwarze_puppen · Wednesday at 6:24 PM

Forums > Market \ 市场 > Malware \ 恶意软件



schwarze_puppen

Sep 9, 2022

Messages	2
Reaction score	0
Points	1

Wednesday at 6:24 PM

Приветствую всех !

За всей информацией об инжектах обращайтесь в лс, установка инжектов на ваш Android Botnets.

Telegram: @skloveyou

Report

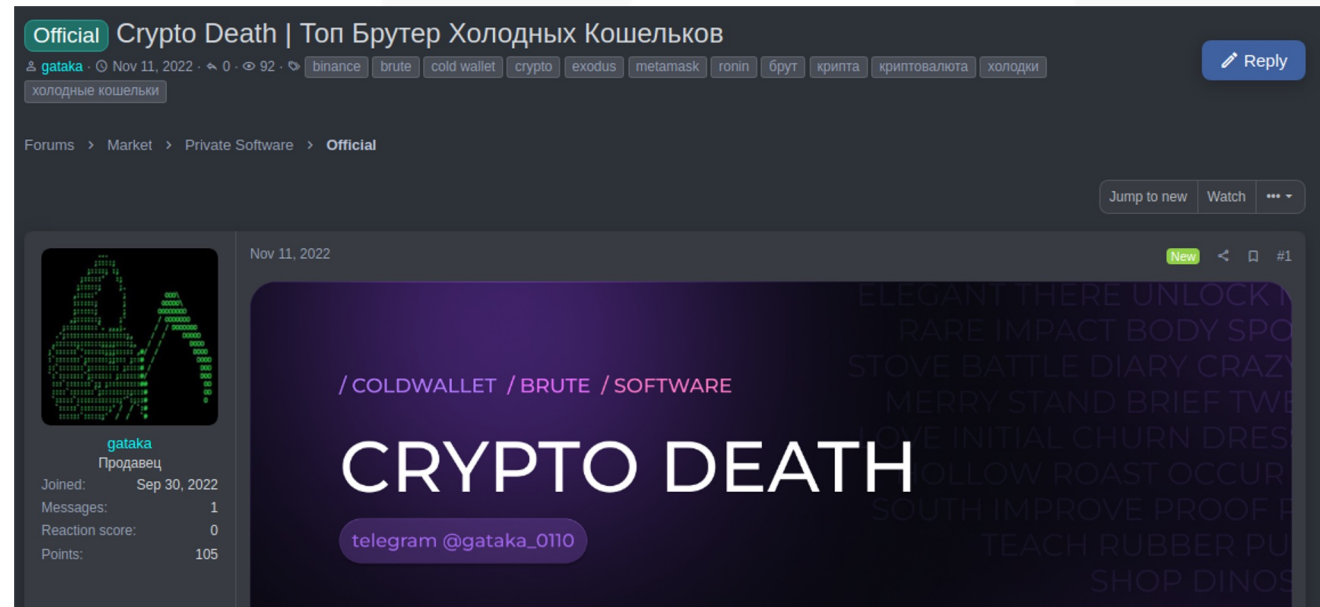
Tool Compromises Offline Cryptocurrency Wallets

Untested threat actor “gataka” advertised a tool to compromise offline cryptocurrency wallets, dubbed “Crypto Death,” on the predominantly Russian language Deep Web forum “BHF.” The tool leverages a custom list of compromised account credentials (AKA combolist) to determine the passwords and seed recovery phrases of more than 30 different cryptocurrency wallets, including:

- Metamask
- Ronin
- Exodus
- Electrum

The actor said the tool currently relies on the widely popular password cracker “Hashcat” to compromise some wallets. They plan to update the tool to be completely autonomous in the future.

The actor charged \$200 USD for a lifetime license.



XSS Moves To Make All Transactions Use Automated Forum Escrow Service

The predominantly Russian language forum XSS[.]is recently made a transition to make using the forum's escrow service, for facilitating deals, mandatory. The forum announced this as a new rule to cut down on the number of members who are scammed from peer threat actors looking to make a quick profit on naive users. The automated escrow service was originally introduced in 2021 and the mandate to use the forum's escrow service to facilitate deals came on the week of November 14th 2022. This service is unique as it allows users to conduct the escrow agreement on their own unlike some Deep and Dark web forums require a buyer and seller to manually conduct escrow via a forum administrator or moderator. This helps mitigate the small risk of using a forum administrator or moderator which can sometimes lead into larger scams where the forum administrators take an additional cut of the escrow fee or work in tandem with the would be scammer.

- One of the most recent cases of this occurred on the now defunct Deep Web English language forum RaidForums where the former forum administrator "Omnipotent" sold data to users under a different alias and operated as the escrow agent, in the same deal, with their administrator alias to maximize their profits.



Announcement of XSS that the use of the automated escrow service is mandatory.

Translation of the text is:

“Stop feeding the scammer! Use fully automated escrow. Refusing escrow = ban”

XSS Moves To Make All Transactions Use Automated Forum Escrow Service (Cont.)

[~/ XSS.is](#) [ЛЕНТА](#) [ПОЛЬЗОВАТЕЛИ](#) [FAQ](#) [РЕКЛАМА](#) [ГАРАНТ](#)

Хватит кормить юддэл! Работайте через ПОЛНОСТЬЮ автоматический гарант. Отказ от гаранта = бан. Тема поддержки тут.

 **DAILY UPDATES**

Обработка SEED фраз, логов и Private key
AudioX: Миксер + Обменник
Установка скрипта на ваши сайты

XSS.is (ex DaMaGeLaB)

UNDERGROUND

 Уязвимости web-приложений	Тем: 2.3K	Сообщений: 16.7K	 Symfony RCE help Вчера в 22:15 - xan0ph0sia
 Уязвимости сетей	Тем: 790	Сообщений: 7.6K	 трансмикро сар Сегодня в 05:35 - H10X
 Атаки на беспроводные сети	Тем: 191	Сообщений: 2K	 Проблемы с Калес 13 мес. назад - Woy