MYBTGWALLET SCAM

The dark side of the fork

powered by NEUTRINO

Intro

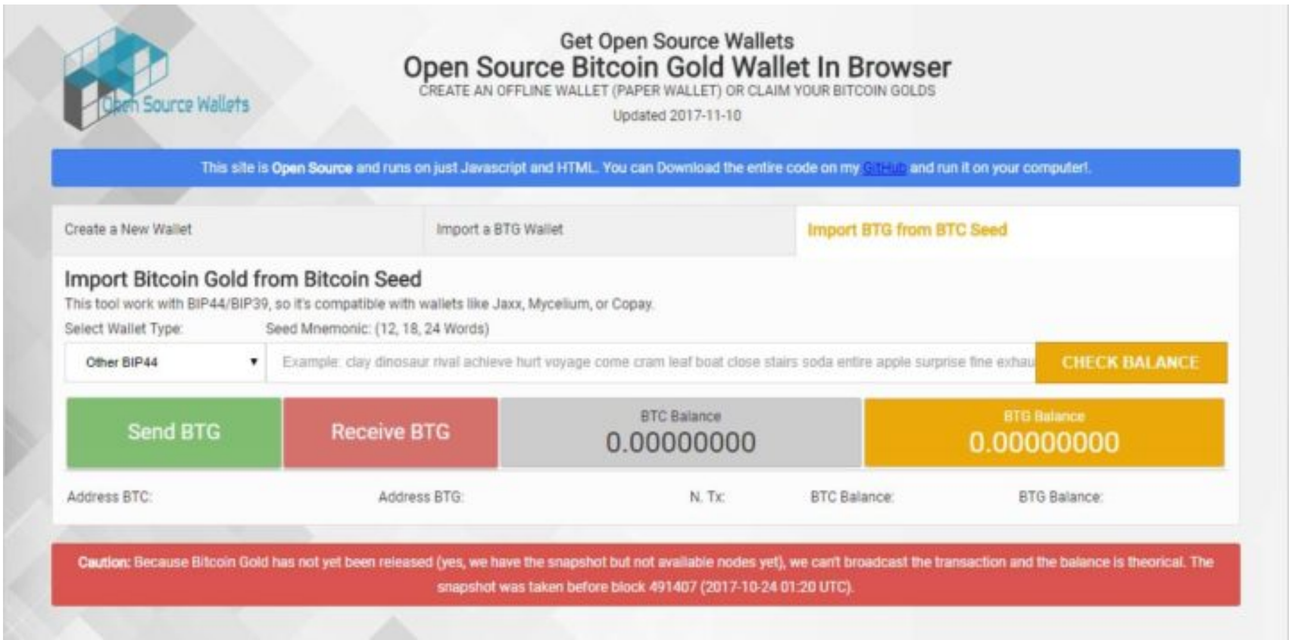
After Bitcoin Cash fork on Aug. 1st, Bitcoin was involved in two other forks between October and November: before the so disputed Segwit2x announced fork, on Oct. 24th a new crypto was launched.

Bitcoin Gold was a new greedy chance for Bitcoin owners to earn some free money: importing mnemonic seeds or private keys belonging to a BTC wallet in a BTG one they had the opportunity to redeem their free BTG.

This was possible through local BTG clients or through some web services such as MyBTGWallet.com, a website listed directly on BTG official webpage. This particular case turned in a scam that stole an impressive number of Bitcoin from "unexperienced" users.

The Scam Site

MyBTGWallet scam worked in a very simple way: users imported the mnemonic seed of their BTC wallet on the scam page providing in this way the scammer with the private keys needed to steal the balance of bitcoin still on the wallet and any other cryptocurrencies stored on the same wallet (e.g. Ethereum or Litecoin in case it was a multicurrency wallet).



Get Open Source Wallets

Open Source Bitcoin Gold Wallet In Browser

CREATE AN OFFLINE WALLET (PAPER WALLET) OR CLAIM YOUR BITCOIN GOLDS

Updated 2017-11-10

This site is **Open Source** and runs on just Javascript and HTML. You can Download the entire code on my GitHub and run it on your computer!.

Import Bitcoin Gold from Bitcoin Seed

This tool work with BIP44/BIP39, so it's compatible with wallets like Jaxx, Mycelium, or Copay.

Select Wallet Type: Other BIP44

Seed Mnemonic: (12, 18, 24 Words) Example: clay dinosaur rival achieve hurt voyage come cram leaf boat close stairs soda entire apple surprise fine exhau

BTC Balance 0.00000000

BTG Balance 0.00000000

Caution: Because Bitcoin Gold has not yet been released (yes, we have the snapshot but not available nodes yet), we can't broadcast the transaction and the balance is theorical. The snapshot was taken before block 491407 (2017-10-24 01:20 UTC).

MyBTGWallet page

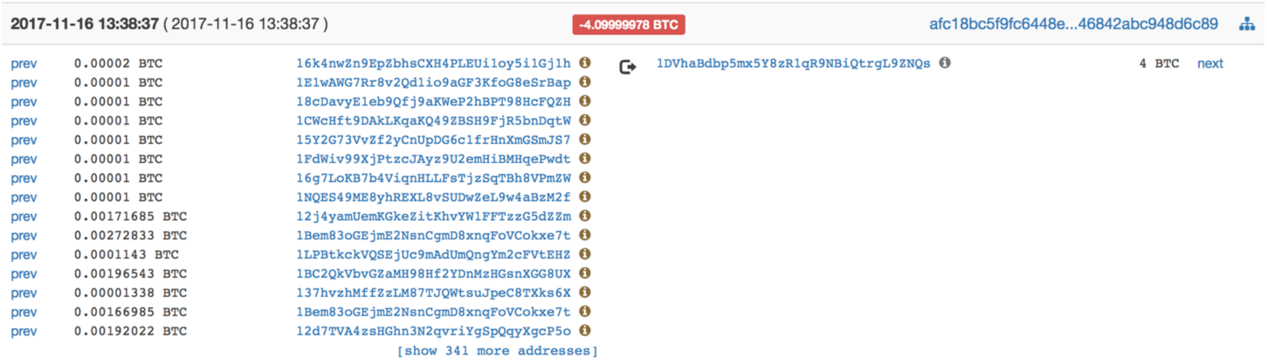
The site used a clever trick to save the mnemonic seed into the cookies of the browser and then siphoned the cookies via a google tracking javascript having this way access to all seeds checked on the website.

The numbers

The website was used by many bitcoin holders after the fork happened. The scammers progressively moved the stolen funds to other bitcoin addresses. Thanks to open source intelligence activities, we were able to create the clusters of the stolen bitcoin and determine that the number of compromised addresses is almost 4500. The aggregated balance of those addresses is almost 400 Bitcoins (equal to 3.3 million Euros at current change rate).

It is not easy to determine the number of victims since the mnemonic seed give you access to all the addresses in the wallet. But with some analysis on the patterns we found that the modus operandi of the stealer changed over time.

During the first days, he imported all the private keys in a single wallet and created some transactions with high number of inputs (the stolen keys) such as:



```
2017-11-16 13:38:37 ( 2017-11-16 13:38:37 )          -4.09999978 BTC          afc18bc5f9fc6448e...46842abc948d6c89

prev   0.00002 BTC      16k4nwZn9EpZbhsCXH4PLEUiloy5ilGjlh   1DVhaBdbp5mx5Y8zR1qR9NBiQtrgL9ZNQs   4 BTC   next
prev   0.00001 BTC      1E1wAWG7Rr8v2Qd1io9aGF3KfoG8eSrBap
prev   0.00001 BTC      18cDavyE1eb9Qfj9aKWeP2hBPT98HcFQZH
prev   0.00001 BTC      1CWcHft9DAkLKqaKQ49ZBSH9FjR5bnDqtW
prev   0.00001 BTC      15Y2G73VvZf2yCnUpDG6c1frHnXmGSmJS7
prev   0.00001 BTC      1FdWiv99XjPtzcJAyz9U2emHiBMHqePwdt
prev   0.00001 BTC      16g7LoKB7b4ViqnHLLFsTjzSqTBh8VPmZW
prev   0.00001 BTC      1NQES49ME8yhREXL8vSUDwZeL9w4aBzM2f
prev   0.00171685 BTC   12j4yamUemKGkeZitKhvYW1FFTzzG5dZZm
prev   0.00272833 BTC   1Bem83oGEjmE2NsnCgmD8xnqFoVCokxe7t
prev   0.0001143 BTC    1LPBtkckVQSEjUc9mAdUmQngYm2cFVtEHZ
prev   0.00196543 BTC   1BC2QkVbvGZaMH98Hf2YDnMzHGsnXGG8UX
prev   0.00001338 BTC   137hvzhMffZzLM87TJQWtsuJpeC8TXks6X
prev   0.00166985 BTC   1Bem83oGEjmE2NsnCgmD8xnqFoVCokxe7t
prev   0.00192022 BTC   12d7TVA4zsHGhn3N2qvriYgSpQqyXgcP5o
                                  [show 341 more addresses]
```

He mixed all the stolen keys to avoid paying too much fee to create a huge number of transactions.

Then he started stealing directly from the mnemonic seed by creating new wallets each time and performing a transaction to empty the wallet without mixing it with other keys. The number of wallet emptied with the second method is roughly 70.

The number of addresses compromised with the first method (key mixing) is 3500. Given the average number of addresses per wallet and some analysis on the transaction history of the grouped addresses, we can estimate that the number of compromised wallet is 345.

Our final estimation is that the number of scammed victims is roughly 415.

The list of addresses used by the attacker is:

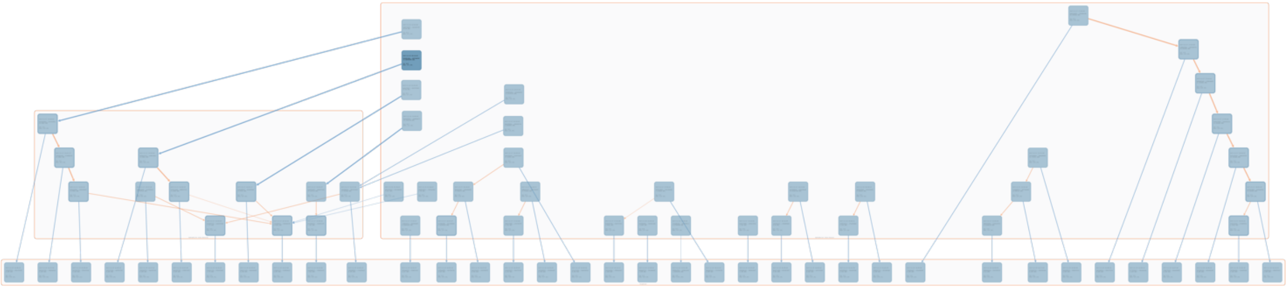
ADDRESS	INCOMING TXs	RECEIVED BTC
1DVhaBdbp5mx5Y8zR1qR9NBiQtrgL9ZNQs	13	70,56
13YKcoCqdCFE2MWCFcL4yfiHJB18Pu59V2	20	69,62
1NtSXE8C7MziWsEEDevgRf9F8RQBgrHPrV	1	60,09
19kbfqx16GejcJsemmRDHLJm3drdUuPS5y	4	24,52
14XHb7MHb22djAeXdmsTC78c2dsfvQdxKG	10	19,62
1ABE7aZRss1Ksiv8NEtXEr2t7VwpqXepNg	1	17,46
1K2YLVFbLQk73So5efapEM8YWm1iq995rK	1	16,03
1NJv7juV8LcLBo4egLvarkEVWskgjhY6NQ	28	14,94
1HGHVaApNto1cCeXzjb8jtufZ3X9wcz6wm	1	14,64
1EvRZhPf5g8X7XhVmTMyt9QeEpbZDWwkhL	4	12,23
1NjLL7b83eH1vP1qUy6uTEu2NUfyr41LmR	1	11,51
182csUn35VNv2j6ZPTgWUxzdagnbKfzf3R	1	10,02
13kyoLweKnxceaNDmxXxa68XCrYY2iHRAx	1	7,68
1KQE4uDuDRCUMQWHT5SyCV4NhjTbGJAuQB	1	7,47
1FkTQzxctFhvStd1mpbhrgaafEN5rhYFcy	1	5,78
1Nbc2ffuMZwLwTYKKkHR8zxUwTgfik33kD	1	4,99
19Wm3mZtB18SBJVY7YsM9ma5SCnaceEwMQ	1	4,47
1JEXyWny6uUrGLBndEfqAiWfmD8nKLnth3	1	4,47
15EYt3dmPwTtnoQ5w5cpE1Re4GTwv2kRAB	1	3,77
1FdaWJ71GVNFq1Yj7LSFXMv5YSLkVcLg2r	1	3,32
17xS2pyYoL9hH4Wx689fwnLeq2NbdtKvXh	1	3,23

17vJdamgcjXJAiP7c9MytrReEamC7HaQ8v	1	3,13
1BNSvAQUj3GEMxAbLcJLXTBt6Q9tnF2qSX	6	2,88
1LwE8eKp5tN7JgFvexHmJXX5fZyxvsEXH6	2	1,48
17C4CQA6J34NpZkCv8CYvcngtfrqjrwdnT	1	0,90
1A43nfMEW3E73z3u7MCC67Yevdpjn6ws6c	12	0,84
1NKqAPqaHS3C9G7uXbtDFByjwbEfxnGpqk	1	0,76
15o9R2p4RCphQRPut7Di9YnovWdBihu37w	1	0,75
1159sXD6ivd8aLANQNstE1Wj8msBdbANEL	1	0,12
1kQDqNLd9s1s7FMhKJDkQiVQ2YL6LE2Fb	1	0,11
1J9HBhHxTt9cKaAkNstRgE4WqNYwYoAFvu	1	0,03

ChipMixer

As of Nov. 24th, 49 BTC have not been spent by the scammers but we have been able to recreate the spending patterns following the other money they moved.
So far, we have been able to determine that about 289 BTC have been moved to a notorious bitcoin mixer named ChipMixer[1].

In the graph below we can see the fraudster's wallets –the two big interacting orange boxes- sending all the bitcoins to ChipMixer – the box at the bottom-.

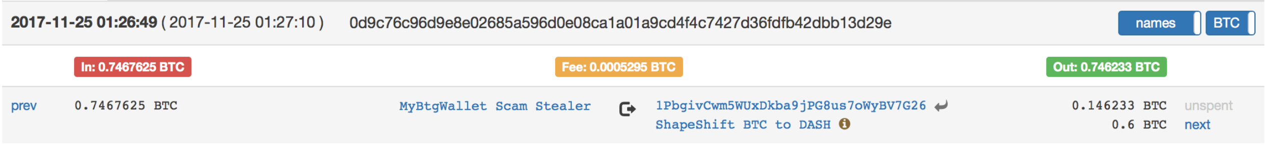


The spending pattern reveal that transactions to ChipMixer are never bigger than 10 BTC: the reason is that the mixer credits transaction under this value after just one confirmation, otherwise the user has to wait for six confirmations.

[1] https://chipmixer.com, ChipMixer became one of the leading mixing services after BitMixer shut down its operations. It appears to be online since May 2017 and one of the peculiarity is that Chipmixer is offering the users the possibility to mix bitcoins splitting them in many *chips.*

ShapeShift

On the Nov. 25th, 1.81 BTC were moved to ShapeShift shifting BTC to DASH (a privacy oriented cryptocyurrency). A total of 3 transactions were performed, one of them is depicted below:



2017-11-25 01:26:49 (2017-11-25 01:27:10) 0d9c76c96d9e8e02685a596d0e08ca1a01a9cd4f4c7427d36fdfb42dbb13d29e

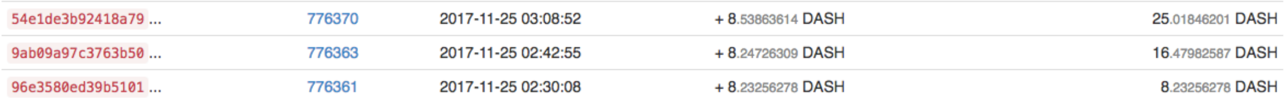
In: 0.7467625 BTC Fee: 0.0005295 BTC Out: 0.746233 BTC

prev	0.7467625 BTC	MyBtgWallet Scam Stealer	1PbgivCwm5WUxDkba9jPG8us7oWyBV7G26 ShapeShift BTC to DASH	0.146233 BTC 0.6 BTC	unspent next

The receiving address on the DASH blockchain is:

XpnqpQSDexV2msyowdPE1GY5PYTthABvng

The address received a total of 25 DASH from the three Shapeshift swaps.

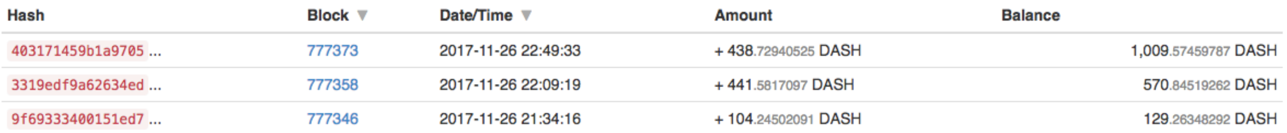


54e1de3b92418a79 ...	776370	2017-11-25 03:08:52	+ 8.53863614 DASH	25.01846201 DASH
9ab09a97c3763b50 ...	776363	2017-11-25 02:42:55	+ 8.24726309 DASH	16.47982587 DASH
96e3580ed39b5101 ...	776361	2017-11-25 02:30:08	+ 8.23256278 DASH	8.23256278 DASH

Wex

On Nov. 26th, 67 BTC were moved from the stealer wallet to Wex[2] with three transactions (7, 30, 30 BTC).

This exchange platform has a really poor KYC policy and, between other cryptos couples, it allows also to trade between BTC and DASH. It was easy to suppose how it was used by the scammer to swap again from these cryptos, so we performed a crossed-chain check and saw that the address used to receive Shapeshift transactions received three additional txs:



Hash	Block ▼	Date/Time ▼	Amount	Balance
403171459b1a9705 ...	777373	2017-11-26 22:49:33	+ 438.72940525 DASH	1,009.57459787 DASH
3319edf9a62634ed ...	777358	2017-11-26 22:09:19	+ 441.5817097 DASH	570.84519262 DASH
9f69333400151ed7 ...	777346	2017-11-26 21:34:16	+ 104.24502091 DASH	129.26348292 DASH

Given the Wex exchange rate at that time (between 0.066 and 0.067 DASH/BTC), it is clear how the received amounts match the 67 BTC moved on the exchange.

So, the fraudster cashed out on the same DASH address used to previously receive from Shapeshift.

[2] https://wex.nz, it is the new exchange born after the BTC-e seizure. As BTC-e only email address is requested to sign in.

Final Remarks

Since the mnemonic seed is the key derivation for all the past and future keys created by the wallet, the attacker still has full control of those wallets. Some of them are still receiving and spending bitcoins thinking that the new addresses are safe. We suggest to the victim of the scam to stop using the old seed and start from a completely new one.

This is just a first update on our research on the topic. Identifying the mixing service used by the attacker is just a preliminary step for tracking the bitcoin flows. Investigations regarding the output of mixed transaction are still in progress at the current date.

Neutrino S.r.l. An innovative startup founded in 2016 by a team with over ten years' experience in cyber security: a cyberlab dedicated to the research of innovative solutions to the new and complex challenges facing the security sector.

P-Flow, the first project developed by Neutrino, provides actionable insight on the blockchain and bitcoin network, offering to all of those interested in virtual currency, information which would otherwise not be accessible.

DISCLAIMER:
Please consider that the information contained into this report are confidential and are not intended for public disclosure, unless authorized or on a specific act from Neutrino representative.

Neutrino does not represent the information as being all-inclusive or to contain all information that may be desirable and **Neutrino is making no representations or warranties, express or implied, as to the accuracy or completeness of the information, and that Neutrino will have no liability with respect to any use or reliance upon any of the information.**

For more information: info@neutrino.nu