WIZSEC
Bitcoin Security Specialists

July 27, 2017

Breaking open the MtGox case, part 1

Earlier today news broke of an arrest in Greece of a Russian national suspected of running a large-scale money laundering operation focused on Bitcoin. The man has since been publicly identified as Alexander Vinnik, 38, and over $4 billion USD is said to have been trafficked through the operation since 2011.

We won't beat around the bush with it: Vinnik is our chief suspect for involvement in the MtGox theft (or the laundering of the proceeds thereof). This is the result of years of patient work, and these findings were surely independently uncovered by other investigators as well. Everyone who worked on the case have patiently kept quiet while forwarding findings to law enforcement, so as not to tip suspects off and to maximize the chances of arrests.

With such an arrest actually happening, we think today might — finally — be the day when we can begin talking about what we've actually been doing all this time and what we found. Thank you for your patience.

Summary

We're going to split this into a couple of different posts, as our full findings cover a wider range of topics, and for this post we'll just very quickly summarize the main BTC theft and its connection to Vinnik:

- In September 2011, the MtGox hot wallet private keys were stolen, in a case of a simple copied wallet.dat file. This gave the hacker access to a sizable number of bitcoins immediately, but also were able to spend the incoming trickle of bitcoins deposited to any of the addresses contained.
- Over time, the hacker regularly emptied out whatever coins they could spend using the compromised keys, and sent them to wallet(s) controlled by Vinnik. This went on for long periods, but also had breaks — a prominent second phase of thefts happened later in 2012 and 2013.
- By mid 2013 when the funds spendable from the compromised keys had slowed to a near halt, the thief had taken out about 630,000 BTC from MtGox.
- In addition, the shared keypool of the wallet.dat file lead to address reuse, which confused MtGox's systems into mistakenly interpreting some of the thief's spending as deposits, crediting multiple user accounts with large sums of BTC and causing MtGox's numbers to go further out of balance by about 40,000 BTC. The majority of these funds were hurriedly withdrawn by their recipients rather than being reported.
- After the coins entered Vinnik's wallets, most were moved to BTC-e and presumably sold off or laundered (BTC-e money codes were a popular choice). In total some 300,000 BTC ended up on BTC-e, while other coins were deposited to other exchanges, including MtGox itself.
- Some of the funds moved to BTC-e seem to have moved straight to internal storage rather than customer deposit addresses, hinting at a relationship between Vinnik and BTC-e.
- The stolen MtGox coins were not the only stolen coins handled by Vinnik; coins stolen from **Bitcoinica**, **Bitfloor** and several other thefts from back in 2011 and 2012 were all laundered through the same wallets.
- Moving coins back onto MtGox was what let us identify Vinnik, as the MtGox accounts he used could be linked to his online identity "**WME**". As WME, Vinnik had

Labels

- MtGox (7)
- CoinLab (1)

Blog Archive

- ► 2021 (3)
- ► 2020 (1)
- ► 2019 (5)
- ► 2018 (1)
- ▼ 2017 (2)
  - ▼ July (2)
    - Breaking open the MtGox case, part 1
    - Comments on the Mark Karpelès trial
- ► 2015 (2)

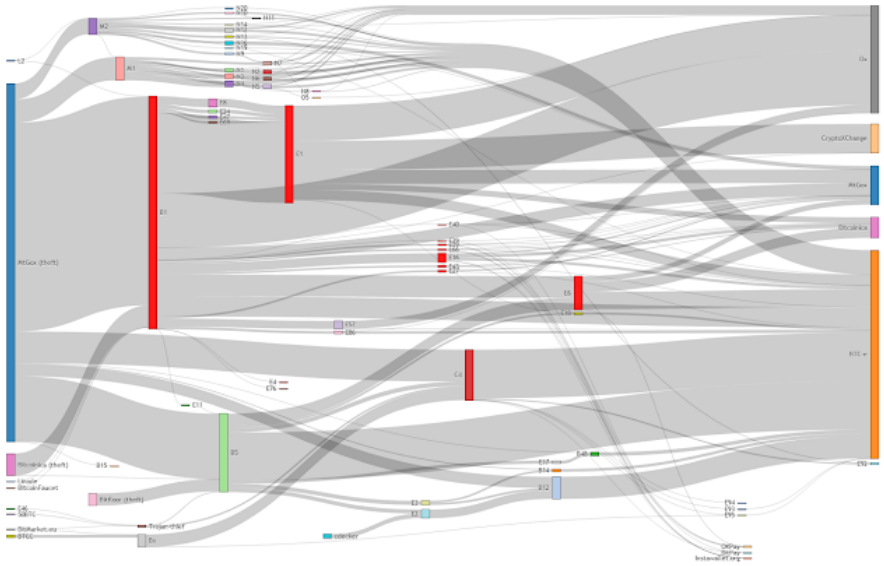
previously made a public outcry that coins had been confiscated from him (the coins in question coming from Bitcoinica).

- There were other thefts and incidents explaining other missing funds from MtGox. More on that in later posts.

There will be follow-up posts fleshing out the details of this post as well, for now we are keeping it short simply to stay close to the announcement of the arrest.

Coin flow

Having identified the actual transactions for the bulk of the stolen MtGox bitcoins, we traced them and clustered all addresses involved, quickly finding that other stolen coins were making their way into the same wallets. Below is a summarized illustration highlighting the theft coin flow of September 2011 onwards:



(The top area of the graph includes clusters unrelated to Vinnik, and appear to be part of a different theft.)

As some coins were deposited back to MtGox, we could identify which accounts were used to receive them; two in particular were of interest, and were possible to link to the online identity "WME". (Clusters who directly used these MtGox accounts are highlighted in red.) WME has been active since a long time back, often advertising "cheap coins" on the BitcoinTalk forums and wanting to trade exchange money codes. BTC-e publicly vouched for him, saying that "[we] know WME very well".

WME was involved with an incident involving stolen Bitcoinica funds (visible in the graph above), which provided yet another strong indicator that we had identified the right man, seemingly the main money launderer behind the MtGox heist. This incident also ended up revealing the name "Alexander Vinnik", though we didn't at the time think it was his real name, having seen many aliases. Today's arrest suggests it was real after all

To be clear, this investigation turned up evidence to identify Vinnik not as a hacker/thief but as a money launderer; his arrest news also suggests this is what he is being suspected for. He may have merely bought cheap coins from thieves and offered a laundering service. He is, however, a crucial piece of the puzzle, as he will have likely known who he was dealing with and laundering for, and so represents a major breakthrough in the case. We assume that law enforcement will now be taking the appropriate next steps to pursue all the remaining angles and hopefully identify the other individuals involved as well.

Next

We're currently preparing more material for disclosure, so for more information on the MtGox theft, and all the other aspects of the MtGox case that we didn't have time to cover in this post, stay tuned and check back again soon.