NEUTRINO

Bancor Security Breach

Tracing stolen ETH, BNT, NPXS

17/07/2018

Bancor Security Breach

Tracing stolen ETH, BNT, NPXS

INTRO

Bancor is a "decentralized liquidity network that allows you to hold any token and convert it to any other token in the network, with no counter party"[1]. On Jul. 9th, 12:56 CEST, the official Twitter account of the decentralized exchange Bancor released a statement announcing that earlier in the morning they suffered a security breach, simultaneously reassuring the users that no personal wallet was compromised.

Almost ten hours later another tweet was published by Bancor, providing more insights on the attack: a few minutes after 00:00 UTC, an attacker compromised "a wallet used to upgrade some smart contracts"[2] and used it to steal 24,984 ETH, 229,356,644 NPXS and 3,200,000 BNT from Bancor controlled smart contracts and wallets.

Thanks to XFlow, our cross-chain analysis platform, we managed to follow both the ETH and the token flows over the different hops on the Ethereum blockchain and clearly identified the services involved in the laundering process.

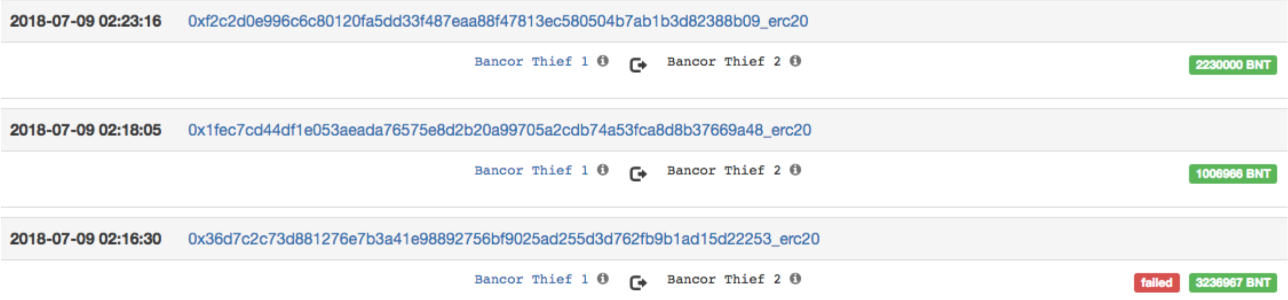
ETHEREUM

The stolen ethers were moved from Bancor smart contract and other Bancor accounts to address 0x33ed22f4b6b05f8a5faac4701550d52286bd735a, before being moved at 2:25 UTC to the main attacker's address: 0x5337a05cc6bcc36b9e70a4b2f81d4c7287aa742e. This address forwarded the stolen ethers and an additional 549 ETH coming from other sources to 0x8ddfdf60aaffe05c623ba193a186abd1f8024946, where they are still waiting to be spent.

We are currently monitoring all these addresses in order to spot future movements of the stolen ethers and any possible additional activity.

BANCOR TOKENS

Bancor Token (BNT) is the token underpinning the Bancor exchange system. As previously mentioned, several BNT were also stolen during the breach and were moved to 0x33ed...735a ("Bancor Thief 1"), before being transferred to 0x5337...742e ("Bancor Thief 2") in two different transactions at 2:18 and 2:23 UTC. Fun fact: a couple of minutes before, the attacker tried to move all the BNT in one transaction but failed to calculate precisely the total amount by just 1 BNT, causing the failure of the transaction.



2018-07-09 02:23:16 0xf2c2d0e996c6c80120fa5dd33f487eaa88f47813ec580504b7ab1b3d82388b09_erc20
Bancor Thief 1 → Bancor Thief 2 2230000 BNT

2018-07-09 02:18:05 0x1fec7cd44df1e053aeada76575e8d2b20a99705a2cdb74a53fca8d8b37669a48_erc20
Bancor Thief 1 → Bancor Thief 2 1006966 BNT

2018-07-09 02:16:30 0x36d7c2c73d881276e7b3a41e98892756bf9025ad255d3d762fb9b1ad15d22253_erc20
Bancor Thief 1 → Bancor Thief 2 failed 3236967 BNT

[1] https://about.bancor.network/network/

[2] https://twitter.com/Bancor/status/1016420621666963457

The attacker started laundering the BNT tokens first, probably knowing that Bancor would be able to freeze them once the breach was detected. The process started at 2:21 UTC, a few minutes after completing the first transactions

Three additional addresses received BNT from Bancor Thief 1, in order to speed up the token laundering:

- 0x57d279660ef1e86c2e505c31e6527a1a970a1123, received 500,000 BNT
- 0xf74f540c536d0153c80e84e516c88e0c996532dc, received 70,000 BNT
- 0x5e9c2d41a5332a25738e42c63ac827c05ae508b7, received 80,000 BNT

All these four accounts then proceeded to move the BNT towards two different well-known exchanges. A few hours later the Bancor team reacted, freezing the vast majority of the stolen tokens: at 8:16 UTC, 2,576,931 BNT were retaken from Bancor Thief 1 with transaction 0xf9c27cd018781d53ce1208dfd0eb5293bd679af6ffd26be5bf8fdb9c4d8f0491, while just a few minutes after, at 8:40 UTC, 460,292 BNT were frozen from 0x57d27…23at with transaction 0x6ca0c8fef18bd059f253338ac4e658e717bed9a74e8cca6f854ddded171b2037.

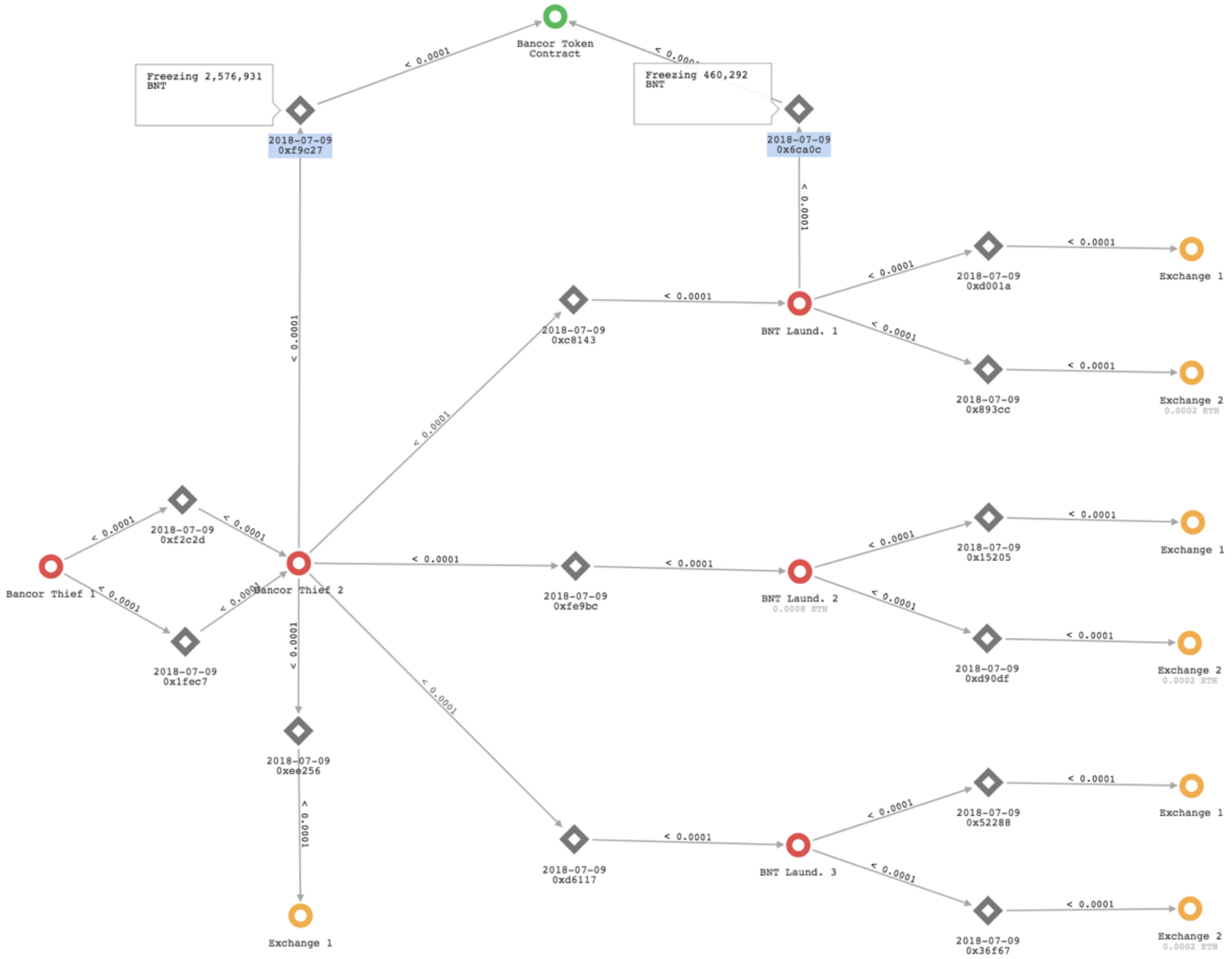
Thanks to the prompt reaction of the Bancor team, the attacker was able to launder only 199,744 BNT through two different exchanges:

- 28,145 BNT went through “Exchange 1”
- 171,599 BNT went through “Exchange 2”

Graph 1 below represents the laundering scheme previously described[3].

After the BNT reached these two exchanges, we were able to discover that they were exchanged for BTC; thanks to Neutrino XFlow cross-chain capabilities, we managed to follow the money flow on the Bitcoin blockchain.

[3] In order to provide a readable graph, we decided not to represent all the transactions involved. Please consider that each diamond represents a transaction while circles are representing addresses.
Please note that the graph arrows are showing the amounts of ETH moved between the addresses. In case of token transfers, it represents only the cost of the contract call.



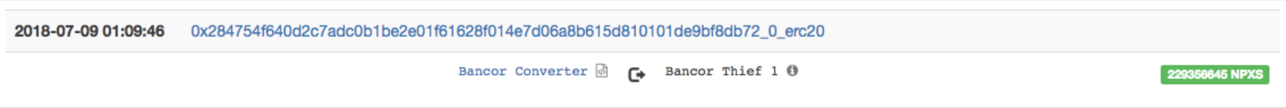
Graph 1 - Bancor tokens laundering process

In order not to compromise ongoing investigations, we decided to keep confidential the names of the entities involved in the laundering process, both on the Ethereum and the Bitcoin blockchains. For further details you can contact us at *info@neutrino.nu*.

PUNDI X TOKENS

According to its website tagline, Pundi X (NPXS) is an ERC20 token whose purpose is “empowering blockchain developers and token holders to sell cryptocurrency and services at any physical store in the world”.[4]

During the Bancor breach the attacker gained access to a smart contract that was responsible for the conversion of Pundi X tokens and was able to withdraw 229,356,644 NPXS in one transaction.



2018-07-09 01:09:46 0x284754f640d2c7adc0b1be2e01f61628f014e7d06a8b615d810101de9bf8db72_0_erc20

Bancor Converter → Bancor Thief 1 229356645 NPXS

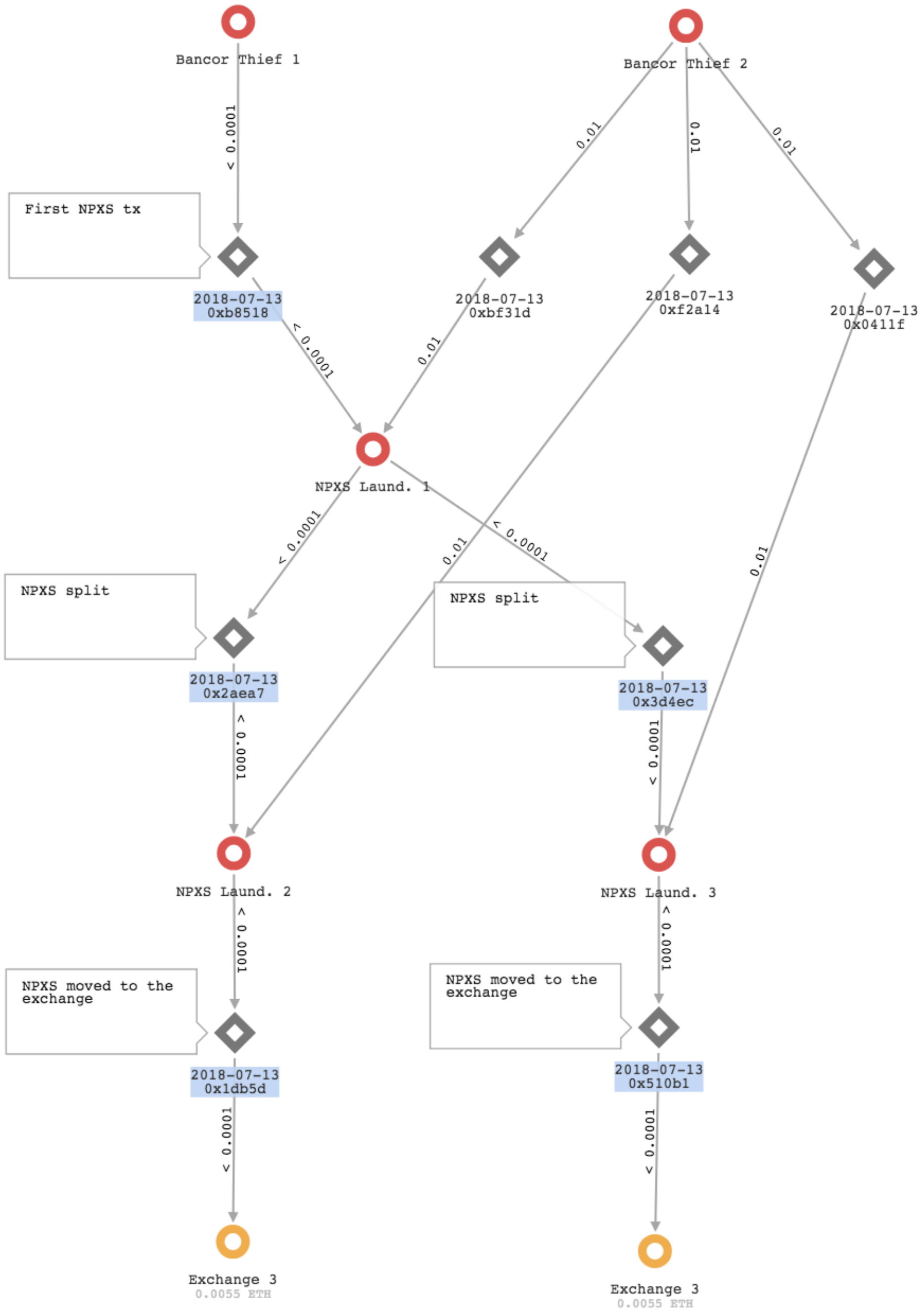
We followed the movements of the stolen NPXS through the laundering process set up by the attacker and clearly identified the involved addresses and the end point.

The laundering scheme is slightly convoluted: after stealing NPXS from different Bancor accounts, Bancor Thief 1 forwarded them to 29 different new addresses. Bancor Thief 2 funded these addresses with some ETH (usually 0.01 ETH per address) to cover the costs of future transaction fees.

Each of these 29 addresses subsequently split the received NPXS across two additional addresses that again received the 0.01 ethers from Bancor Thief 2 in order to pay the transaction fees. The final step is represented by the deposit of the split NPXS onto a known crypto-to-crypto exchange which operates without strong customer verification policies.

[4] Ranked 45 on CoinMarketCap as of July 18th, Pundi X were also targeted in the attack suffered in June by the Korean exchange Conrail: as a consequence of the security breach, almost $20 millions worth of NPXS were stolen together with other tokens and coins (Aston X, Dent, Tron) for a total of almost $37 millions.

The following graph is an example of the laundering process, with the ETH transactions that led the stolen coins from the thief's addresses to the known exchange.



Graph 2 - Pundi X tokens laundering process

All the stolen NPXS were laundered through this articulated mechanism and reached addresses belonging to "Exchange 3". As for the previous two exchanges, we were able to track the switches and to discover again that the stolen funds were withdrawn on the Bitcoin chain, where we are still following them thanks to XFlow cross-chain capabilities.

In order not to compromise ongoing investigations, we decided to keep confidential the names of the entities involved in the laundering process, both on the Ethereum and the Bitcoin blockchains. For further details you can contact us at *info@neutrino.nu*.

CONCLUSIONS

Despite the Bancor team being able to freeze and take back the vast majority of the stolen BNT, the breach was quite remunerative for the thief. The following table summarizes all the amounts involved in the theft and how they got laundered:

	ETHER	BANCOR	PUNDI X
Unspent	29,984		
Frozen		3,037,223	
Laundered		28,145 171,599	229,356,644
Laundered through		Exchange 1 Exchange 2	Exchange 3
Total stolen	**29,984**	**3,236,967**	**229,356,644**
Total USD	**~ 12,200,000**	**~ 600,000**	**~ 920,000**

In the last few months the number of attacks targeting crypto exchanges increased significantly, from the Japanese exchange Coincheck where hundreds of millions worth of NEM were stolen, to other relevant cases such as the breaches involving CoinSecure, Coinrail and BitHumb.

The Bancor breach is only the most recent in this wave of attacks, with the attacker being able to exfiltrate crypto assets in Ether, Bancor and PundiX, roughly equivalent to $14 millions.