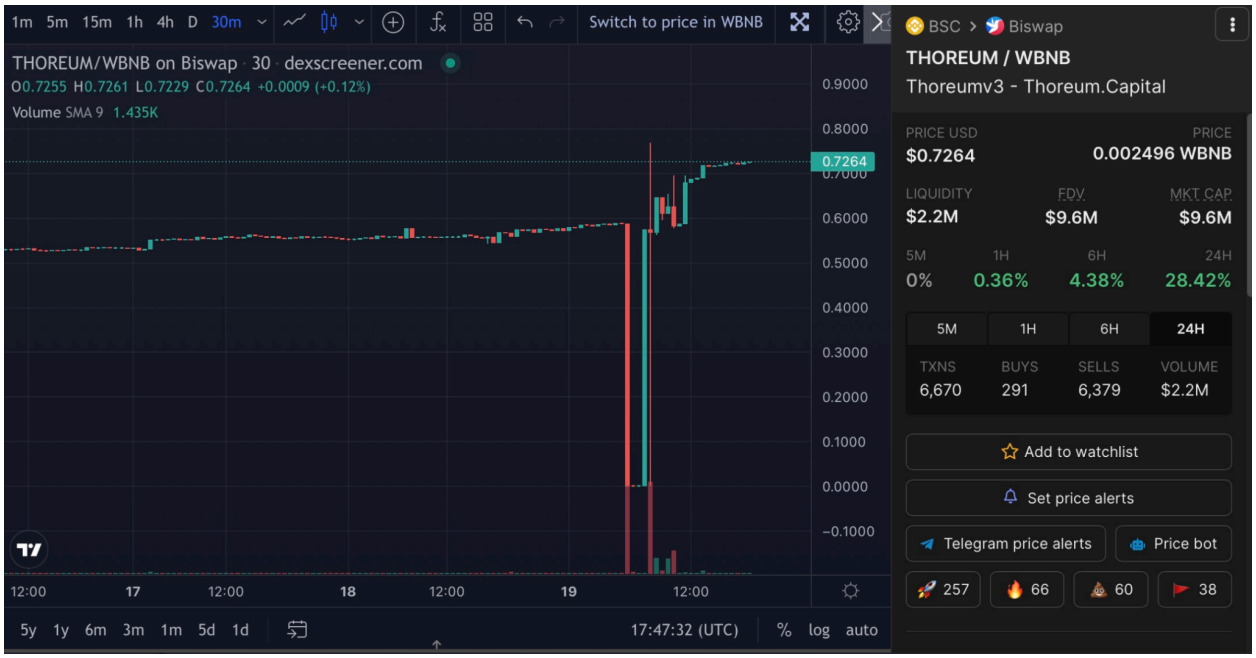
Thoreum Attack Investigation

DateTime: 02/10/2023
Author: Nicolas Melendez



Description

Thoreum was exploited on 01/19/2023 approximately 4:51 AM +UTC on the Binance Smart Chain. Thoreum a day before updated their contract but unfortunately it had a bug in the transfer function: if a wallet transfers funds to itself, the amount of tokens in the wallet would be increased by as much as the sent amount. An Attacker discovered the bug and created an exploiting contract that deposited BNB to gain WBNB, then it swap WBNB for Thoreum tokens and used the transfer function bug to mint more doing the transfer to itself. After having a great amount of Thoreum it converted it to WBNB, after that to the native BNB to do the money laundering with tornado cash.

- **Attack Category:** Bug exploit
- **Losses in USD:** 691.929 USD

Additional Details

- Thoreum contracts are not open source
- There are no audits over the Thoreum contracts v4
- 1 day took someone to find the bug
- Assets (BNB) drained in 34 minutes.

- Official Thoreum twitter post-mortem says that the bug was introduced Jan-18-2023 07:01:05 AM +UTC but the last contract proxy upgrade alert before the attack was fired at Jan-19-2023 03:19:33 AM +UTC

Indicators

List of all the indicators associated with the attack

Indicator	Type	Chain	Notes
0x1Ae2Dc57399B2f4597366C5Bf4fE39859c006F99	Attacker EOA	BSC	Attack address that deploy the attack contract
0x7d1E1901226E0ba389BfB1281EDE859e6E48CC3d	Attacker Contract	BSC	Attacker contract that exploits the vulnerability
0x1285FE345523F00AB1A66ACD18d9E23D18D2e35c	Attacker EOA	BSC	Attack Address for money laundering
0xce1b3e5087e8215876af976032382dd338cf8401	Thoreum Contract	BSC	Thoreum Proxy Contract

Timeline

Attack Timeline of Block Explorer Tx (color coded red) and Forta Alerts (color coded green)

DataTime in UTC	Link	Stage	Notes
Jan-19-2023 03:19:33 +UTC	https://bscscan.com/tx/0x5a1788e1fbd582d1b89dc23fdf6cb7600c5ab07e4156b37cc3a6da27d5aa0349	Various	Last contract upgrade before the attack.
Jan-19-2023 03:19:33 +UTC	https://explorer.forta.network/alert/0x050520d716e10738765e57afbedbb8cdc8b479093c9e83ca889a37db0ff15c6e	Various	Alert: **OZ-GNOSIS-EVENTS** Thoreum Upgrades a Contract with a bug in the transfer function
Jan-19-2023 04:19:39	https://bscscan.com/t	Funding	Address gets 3.13

+UTC	x/0x9396731b5a00db45d46abf0f090662f71b22ed05c40fb64d3fb523c50e5364f3		BNB from fixed float CEX
Jan-19-2023 04:19:39 +UTC	https://explorer.forta.network/alert/0x18a228038867edfa9c9902780d89f08ef529656a8fe7c821f0dcbf6fa50df66e	Funding	Alert: **CEX-FUNDING-1** Address gets 3.21 BNB from fixed float CEX
Jan-19-2023 04:19:39 +UTC	https://bscscan.com/tx/0x9396731b5a00db45d46abf0f090662f71b22ed05c40fb64d3fb523c50e5364f3	Funding	Address gets 1.98 BNB from fixed float CEX
Jan-19-2023 04:30:04 +UTC	https://explorer.forta.network/alert/0x267a394df66c3d1860ee8cc6c0a6cc2a143e81120a1263677ed007d3affcb6cf	Funding	Alert **CEX-FUNDING-1** Address gets 1.98 BNB from fixed float CEX
Jan-19-2023 04:51:17 +UTC	https://bscscan.com/tx/0xfe6284a4a156a77d3b71de485cccebb06349666fb09f0a42e95c4a689dce64ab	Preparation	The attacker creates the exploit contract
Jan-19-2023 04:51:17 +UTC	https://explorer.forta.network/alert/0xeeb6f094f84e662b3f2cac91087dc17e48744d15dd09c5db41df6c4c862cee0f	Preparation	Alert: **SUSPICIOUS-CONTRACT-CREATION** Forta bot using ML detects that the contract may be malicious
Jan-19-2023 05:01:47 +UTC	https://bscscan.com/tx/0x5058c820fa0bb0daff2bd1b30151cf84c618dffe123546223b7089c8c2e18331	Exploitation	First Attack of 36
Jan-19- 2023 05:01:50 +UTC	https://explorer.forta.network/alert/0xd75bccb35ab336d47079d348f758a2ac1884f650bc5f220846f42e260e449553	Exploitation	Alert: **ASSET-DRAINED** Attack contract accumulates thoreum token

			First of consecutive 10
Jan-19-2023 05:10:11 +UTC	https://bscscan.com/tx/0xcd79a278fec119526290435aa46ea6b68a1e0fc3ac5a0208b6660a736b653b2a	Money Laundering	Attacker preparing the laundering is converting WBNB to BNB
Jan-19-2023 05:13:23 +UTC	https://bscscan.com/tx/0xb3b11704cf158dd5bc1f2a331872e9b8bf3cafa1cd686f4c212405b4ec225a5c	Money Laundering	Attacker first deposit in Tornado cash: 100 BNB. one of many (51)
Jan-19-2023 05:45:41 AM +UTC	https://bscscan.com/tx/0xc5654ee55cdf40728be4d4d6754d146f183a7b704099b607054fd010be8ee5cf	Money Laundering	Attacker address withdraw 100 BNB from tornado cash
Jan-19-2023 05:45:41 AM +UTC	https://explorer.forta.network/alert/0x1d405cd85f1c97d5106f5715ef689eafd1fa4673f4db3f78715a76d0b99290fa	Money Laundering	Alert: **FUNDING-TORNADO-CASH-HIGH** Attacker address get 100 BNB from tornado cash

References

Reference	**Relevance**
https://twitter.com/ThoreumFinance/status/1616138674173014016	Thoreum Twitter thread explaining with detail how the attack happened
https://medium.com/neptune-mutual/thoreum-finance-smart-contract-vulnerability-1fc18068d18c	Neptune mutual explaining the Thoreum smart contract attack
https://quillaudits.medium.com/decoding-thoreum-finance-exploit-quillaudits-199f090e9bac	Decoding Thoreum Finance Exploit | QuillAudits

New Detection Bot Ideas

- Bot idea: A bot that detects if a self transfer increases the balance of the wallet.
    a. Identify ERC20 transfers from & to same wallet (self)
    b. Check change in the balance
    c. Alert if the balance increases

Detection Bot Improvement Suggestions

BotId	**Bot Title**	**Issue**	**Improvement**	**Link to Github Issue**
0x186f424224eac9f0dc178e32d1af7be39506333783eec9463edd247dc8df8058	Funding Laundering Detector	Bot Didn't detect the deposit in tornado cash	Bot should detect the deposit in tornado cash	https://github.com/venglov/Funding-Laundering-Detector/issues/6
0xc5654ee55cdf40728be4d4d6754d146f183a7b704099b607054fd010be8ee5cf	Tornado Cash FundingInfo Severity	Bot doesn't have addresses in the metadata.	Bot should have the address receiving funds in the metadata.	No github