Ethereum Threat Actors Part 3 — Phishings/Scams using Smart Contracts

QuoScient GmbH

Apr 3 · 4 min read

Executive Summary

In part three of our mini-series (see part #1 & part #2) describing **how cybercrime actors are using the Ethereum blockchain for fraudulent means**, we analyze a phishing tactic that used a smart contract address. Interestingly, this smart contract is not unique and the exact same closed-source bytecode is used in more than 130 thousand smart contracts.

In this blogpost, we provide a quick analysis of the closed-source bytecode inside those smart contracts. We will also explain the process to find similar contracts and how to leverage this information to find the cryptocurrency exchange behind them.

Phishing on Forums/Telegram.

The focus of our analysis is based on observed phishing attempts related to the smart contract account 0x70305B080eFc49eB5DFb9bdA78Aea516c398f804.

Based on our observations the account owner is targetting forums and private channels (such as Telegram) discussing low value cryptocurrency tokens. For example, multiple scam messages were observed on forums related to Crypterium (CRPT), Envion (EVN) and Substratum (SUB).

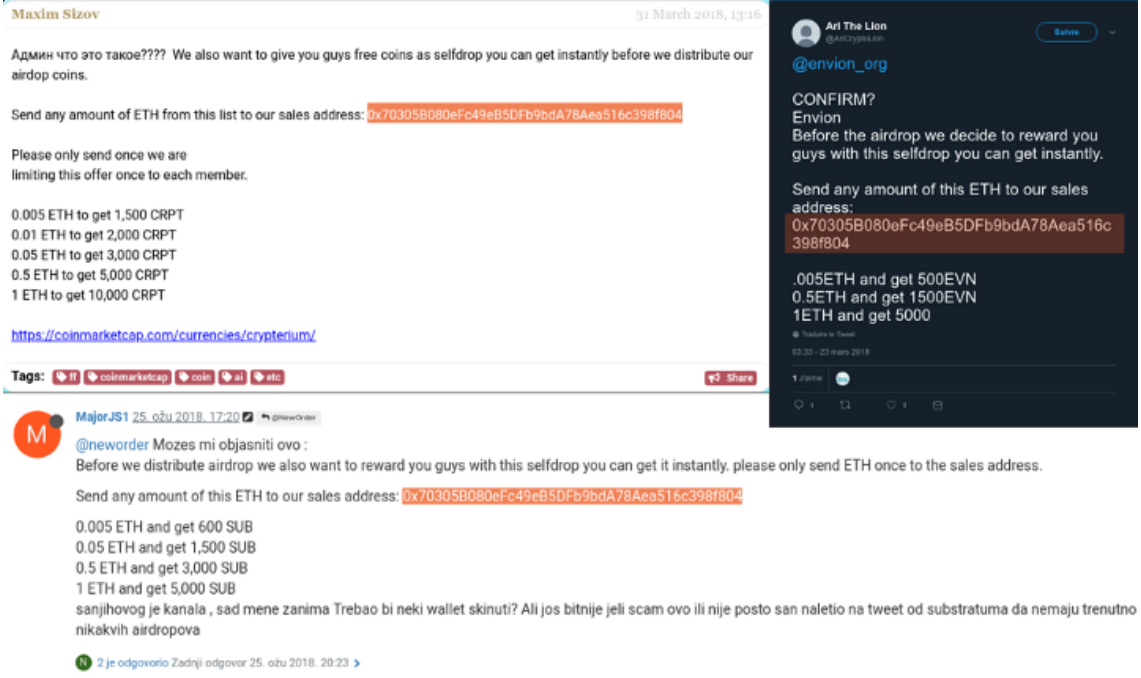


Image 1: Different scam messages posted by the actor and listing the same Ethereum addresses on various discussion forums.

In the above forums, the actor is enticing the users to make Ethereum payments to the address in question in order to receive awards. Based on the various languages used in the spam messages, the author speaks English, Croatian and Russian. Although, it is unclear if the author is fluent in the observed languages. One moderator of etherscan.io also found the same scam message on a private (fake) channel on Telegram.

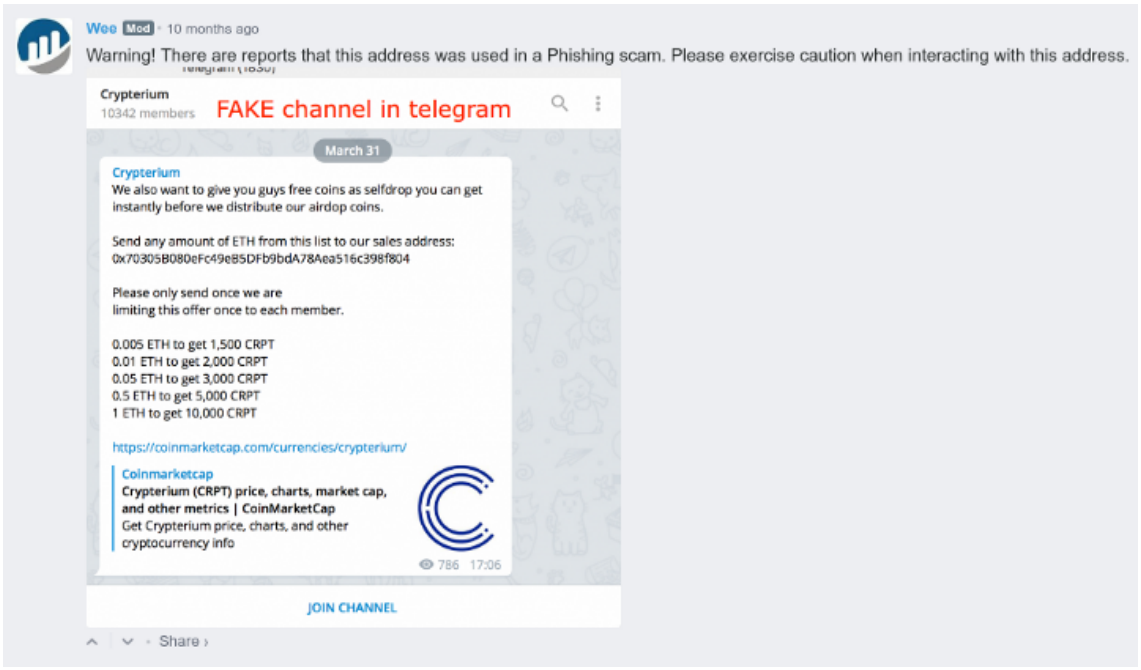


Image 2: Scams over a private Telegram group about Crypterium token

At the time of writing, this address has received a total of **457 transactions**, with **roughly 350 ETH** received (**USD 82 thousand**). While the address has been flagged for malicious phishing activity, it is unknown how many of the transactions were the result of this scam."

Quick analysis of the Smart contract Bytecode

The bytecode of the smart contract can be found in the "Code" tab on etherscan.io or by using the getCode method available in the Ethereum JS library web3js.

In order to reverse the bytecode, we used our open-source tool Octopus to generate the control flow graph (CFG) of the smart contract.

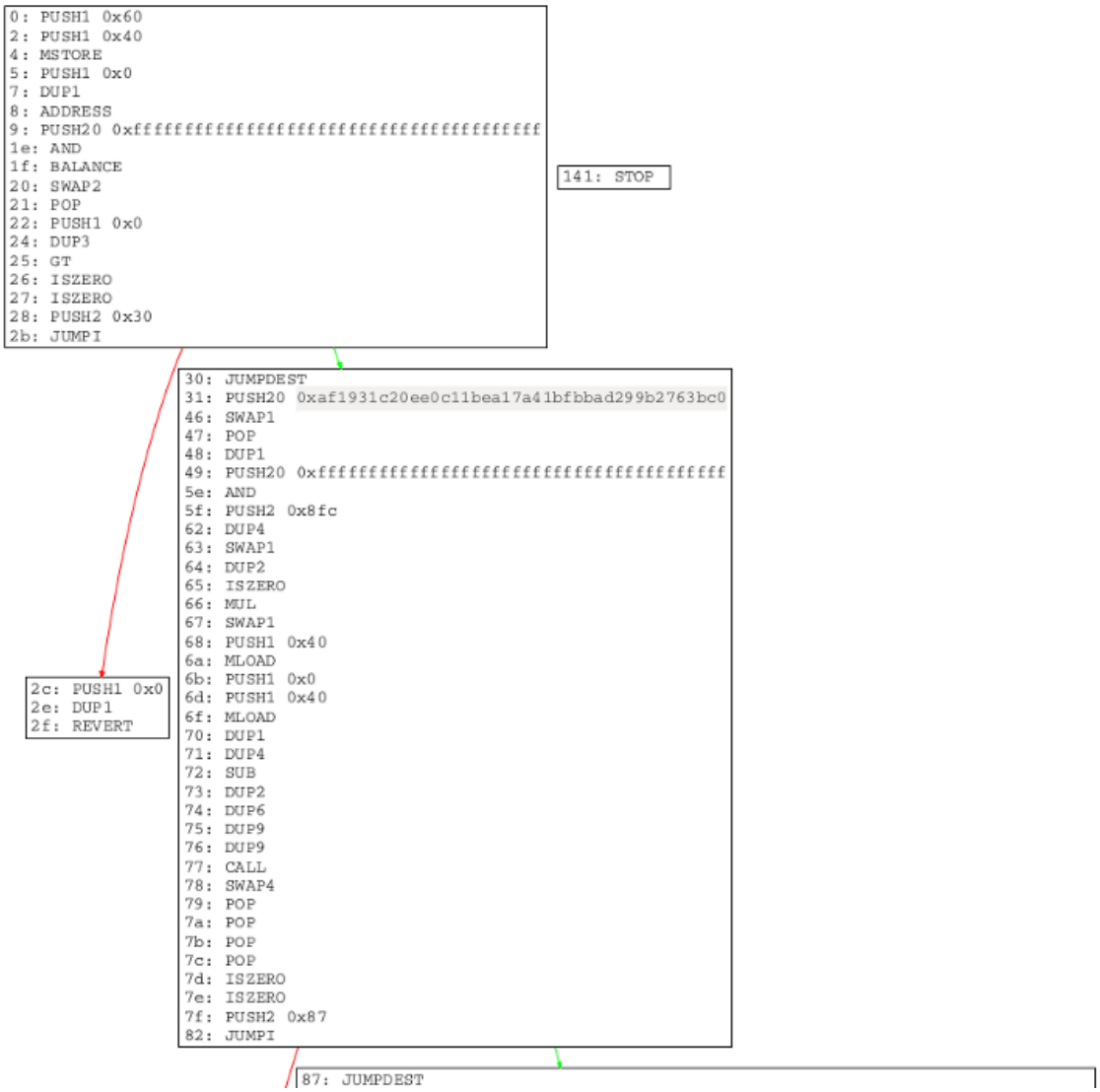
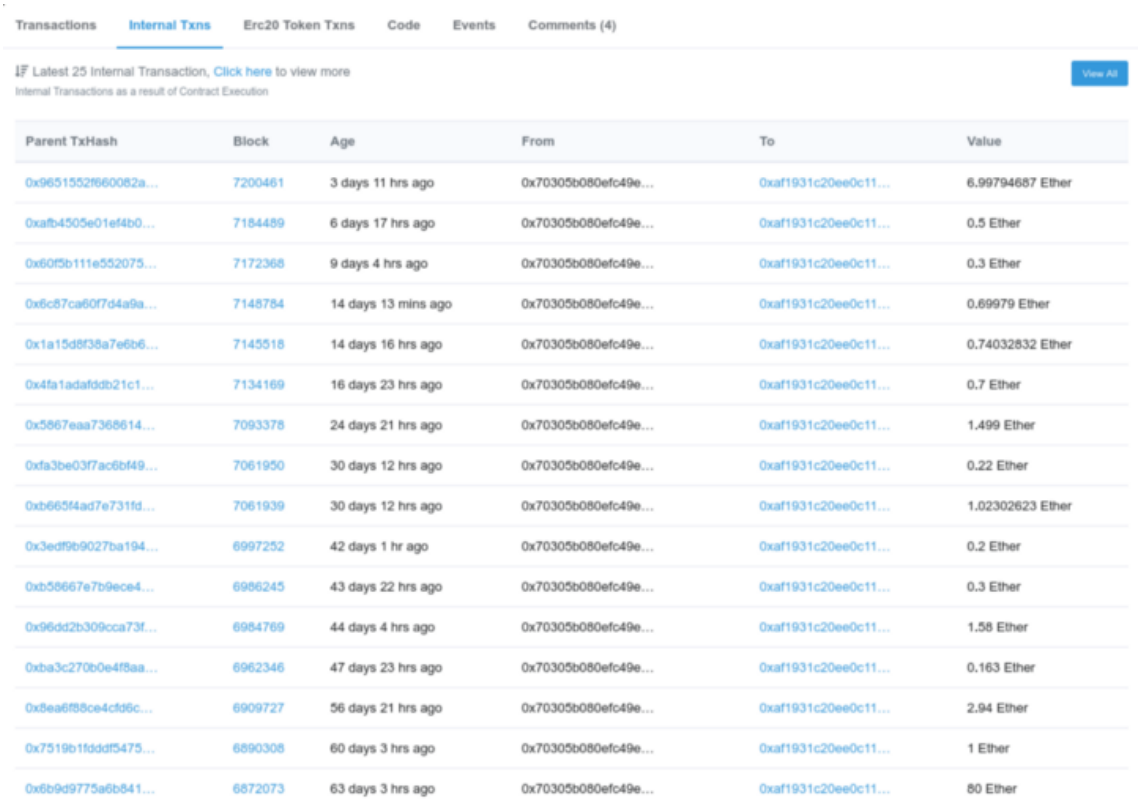


Image 3: CFG of the 0x7030 smart contract bytecode on Octopus

This smart contract is really short, with only 365 bytes in size, 1 function, 5 basic blocks, and 110 EVM instructions. The most interesting part of the contract bytecode is the hardcoded address **0xaf1931c20ee0c11bea17a41bfbbad299b2763bc0**. This address is used as the second argument for the CALL (offset 0x77) instruction, meaning that every transaction to the 0x7030 contract will directly go through 0xaf1931c20ee0c11bea17a41bfbbad299b2763bc0.

This smart contract is a typical automated proxy that forwards every Ether received to the 0xAf1931c20ee0c11BEA17A41BfBbAd299B2763bc0 Ethereum address. We observe confirmation of this behavior by looking at the “Internal Txns” tab on etherscan.io.



Transactions | Internal Txns | Erc20 Token Txns | Code | Events | Comments (4)

Latest 25 Internal Transaction, Click here to view more

Internal Transactions as a result of Contract Execution

View All

Parent TxHash	Block	Age	From	To	Value
0x9651552f660082a...	7200461	3 days 11 hrs ago	0x70305b080efc49e...	0xaf1931c20ee0c11...	6.99794687 Ether
0xafb4505e01ef4b0...	7184489	6 days 17 hrs ago	0x70305b080efc49e...	0xaf1931c20ee0c11...	0.5 Ether
0x60f5b111e552075...	7172368	9 days 4 hrs ago	0x70305b080efc49e...	0xaf1931c20ee0c11...	0.3 Ether
0x6c87ca60f7d4a9a...	7148784	14 days 13 mins ago	0x70305b080efc49e...	0xaf1931c20ee0c11...	0.69979 Ether
0x1a15d8f38a7e6b6...	7145518	14 days 16 hrs ago	0x70305b080efc49e...	0xaf1931c20ee0c11...	0.74032832 Ether
0x4fa1adafddb21c1...	7134169	16 days 23 hrs ago	0x70305b080efc49e...	0xaf1931c20ee0c11...	0.7 Ether
0x5867eaa7368614...	7093378	24 days 21 hrs ago	0x70305b080efc49e...	0xaf1931c20ee0c11...	1.499 Ether
0xfa3be03f7ac6bf49...	7061950	30 days 12 hrs ago	0x70305b080efc49e...	0xaf1931c20ee0c11...	0.22 Ether
0xb665f4ad7e731fd...	7061939	30 days 12 hrs ago	0x70305b080efc49e...	0xaf1931c20ee0c11...	1.02302623 Ether
0x3edf9b9027ba194...	6997252	42 days 1 hr ago	0x70305b080efc49e...	0xaf1931c20ee0c11...	0.2 Ether
0xb58667e7b9ece4...	6986245	43 days 22 hrs ago	0x70305b080efc49e...	0xaf1931c20ee0c11...	0.3 Ether
0x96dd2b309cca73f...	6984769	44 days 4 hrs ago	0x70305b080efc49e...	0xaf1931c20ee0c11...	1.58 Ether
0xba3c270b0e4f8aa...	6962346	47 days 23 hrs ago	0x70305b080efc49e...	0xaf1931c20ee0c11...	0.163 Ether
0x8ea6f88ce4cfd6c...	6909727	56 days 21 hrs ago	0x70305b080efc49e...	0xaf1931c20ee0c11...	2.94 Ether
0x7519b1fdddf5475...	6890308	60 days 3 hrs ago	0x70305b080efc49e...	0xaf1931c20ee0c11...	1 Ether
0x6b9d9775a6b841...	6872073	63 days 3 hrs ago	0x70305b080efc49e...	0xaf1931c20ee0c11...	80 Ether

Image 4: Internal transactions between 0x7030 contract and 0xaf19 address on etherscan.io

Who is behind 0xAf1931c20ee0c11BEA17A41BfBbAd299B2763bc0?

After a relationship analysis of the 0xAf1931c20ee0c11BEA17A41BfBbAd299B2763bc0 transactions, we discovered that this address in controlled by the Luno.com cryptocurrency exchange.

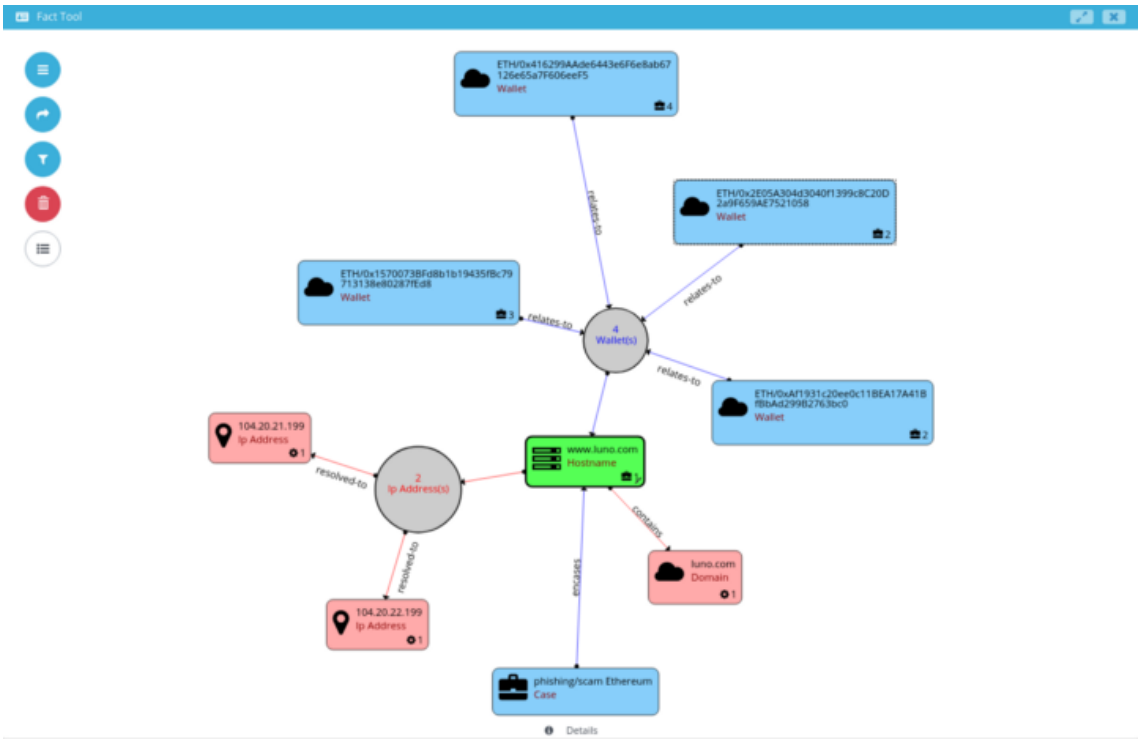


Image 5: Relationship graph using QuoLab

We determined the following role for each address:

- 0xAf1931c20ee0c11BEA17A41BfBbAd299B2763bc0: Luno user wallet receiver
- 0x416299aade6443e6f6e8ab67126e65a7f606eef5: Luno hot wallet
- 0x2E05A304d3040f1399c8C20D2a9F659AE7521058: Luno user wallet contract generator
- 0x1570073BFd8b1b19435fBc79713138e80287fEd8: Luno cold wallet

Similar Luno user wallets Used for Phishing

As we previously observed and explained in part #1 of this mini-series, you can use Google BigQuery to request and retrieve a complete list of all smart contracts, with a specific bytecode pattern, available on the Ethereum blockchain.

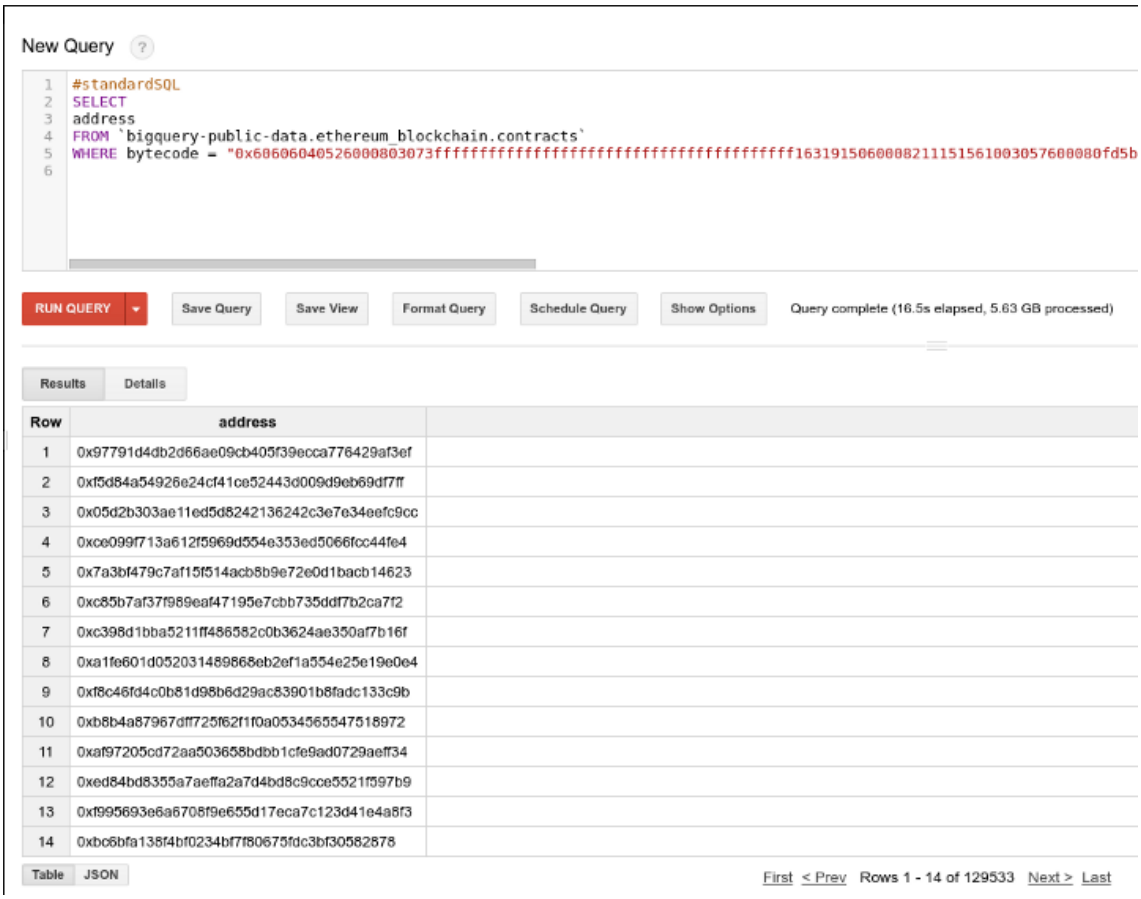


Image 6: Smart contracts with the exact same bytecode listed using Google BigQuery

The above query returns roughly **130k results**. After correlating this list of addresses with known phishing addresses tagged by Etherscan.io and EtherscamDB, we found eight similar Luno user wallets involved in phishing scams.

List of other Luno user wallet tagged as phishing/scam:

- 0x7355e49ba13082D3f83fD828Ee6FDA39738F1E55
- 0x1aBC65765FD0DF7D997635EBE3027384BCF7923E
- 0x82B36a7410796a3bD2a0B206abb402b899B0A388
- 0x42265e06267D5857CE0d28094A122f453EE66d37

- 0x0Da4eB121142879Db7cB4bCA6693c94154D07339
- 0xB7741854BDB50e086A85722f6E280CD0515B9230
- 0xBa663f63eE6eF36d8778615dB2b90679F605D8B4
- 0x6Ef982f9E7F09d4bF4a70398707c82970a6Dc31E

Conclusion

In total, Luno user wallets (0x7030 included) tagged as phishing/scam have received **678 ETH** i.e. **USD 190,000**. While it is possible additional Luno user wallets were used for phishing/scam purposes, this blog only focuses on the ones tagged by Etherscan.io and EtherscamDB.

Analysis and reversing of this smart contract was useful to understand its behavior and to determine if this smart contract was generic. Similar crypto-exchanges (like Bittrex) user smart contract can be found with the Solidity source code associated.

Additionally, you can check out our open source tool Octopus to analyze Ethereum transaction and reverse Ethereum Smart Contracts. Moreover, please also find our conference presentations about this subject in our QuoScient media center.

Feedback is as always welcome! Don't hesitate to use the comment section below!

Patrick Ventuzelo, Security Researcher at QuoScient

Twitter / Medium / LinkedIn

Indicators of Compromise

Ethereum addresses:

- 0x70305B080eFc49eB5DFb9bdA78Aea516c398f804

- 0x7355e49ba13082D3f83fD828Ee6FDA39738F1E55
- 0x1aBC65765FD0DF7D997635EBE3027384BCF7923E
- 0x82B36a7410796a3bD2a0B206abb402b899B0A388
- 0x42265e06267D5857CE0d28094A122f453EE66d37
- 0x0Da4eB121142879Db7cB4bCA6693c94154D07339
- 0xB7741854BDB50e086A85722f6E280CD0515B9230
- 0xBa663f63eE6eF36d8778615dB2b90679F605D8B4
- 0x6Ef982f9E7F09d4bF4a70398707c82970a6Dc31E