INVESTIGATIVE
INTELLIGENCE REPORT

Project Name:

XODUS FINANCE

ASSURE DEFI™
THE VERIFICATION GOLD STANDARD

Project Name:

XODUS FINANCE

Project Name: **Xodus Finance**
Ticker: **$XOD**

Token Contract Address:
0x34F3d6Cccc8ddd1E2c7055591b110a81237af55B
Pair Address: **N/A (Token had not launched yet)**

Website: **https://xodus.finance**
Socials: **Deleted**
Dextools link: **N/A (Token had not launched yet)**

Date Investigation Was Opened:
4/16/22

Nature of scam:
Stolen Contract Ownership, Theft of Project Funds

CONTACT INFORMATION FOR LAW ENFORCEMENT TO OBTAIN KYC & IDENTITY DETAIL INFORMATION ON FILE WITH ASSURE DEFI:

Direct Contact
Email: chapo@assureteam.io
Twitter DM: www.twitter.com/el_crypto_chapo/
Telegram DM: https://t.me/el_crypto_chapo/

Mailing Address
Assure DeFi LLC
c/o United States Corporation Agents, Inc
411 Wolf Ledges Parkway, Suite 201
Akron, OH 44311

Potential Injured Parties:
< 400

Estimate Funds Stolen:
~$146,000

Last Known Location of Funds:

$120k currently still sitting in contract
$26k (DAI) has been withdrawn to self-custody wallets

***See details below in BlockChain Forensics/Funds Tracing Section of Report.**

BACKGROUND INFORMATION

Project pre-sale started on 4/15/2022.

According to the Xodus team (who have been actively communicating with Assure DeFi since the incident occurred):

A contracted developer has acted maliciously by building a backdoor in the contract that allowed him to transfer ownership of the pre-sale contract half way through their 2nd presale round. The rogue developer transferred the contract ownership, which gave him access to all the of the funds which had been raised via the presale. Subsequently, there has been $26K taken out of the contract using the emergency withdraw function & distributed to multiple self-custody wallets.

BLOCKCHAIN FORENSICS

The timeline of events given by the Xodus team:

There were 2 presales, the 1st one had an issue with the whitelist which meant that many people with whitelist were unable to buy. Therefore they advised users to purchase through their public sale which was at an increased cost. Therefore they had the developer create a new presale 2 contract. You can see the date the developer deployed it here.

https://ftmscan.com/tx/0x6ebe60a04fd2db6c7ebd2d4d81b9083065a815bd0e0a2debbe64b8e745c41836

The developer then restored all the whitelist addresses with the correct allocation for when they connect to the dapp, they would see the correct amount of tokens they would receive on launch.

0x94a15b435a77791e9b...	Transfer Ownersh...	35232666	16 days 18 hrs ago	0xcb376baaf5216f392f1...
0xfa288987628b9b7cfb7...	Restore Info	35231015	16 days 19 hrs ago	0xcb376baaf5216f392f1...
0xaafe87d1c31d170f18fb...	Restore Info	35231015	16 days 19 hrs ago	0xcb376baaf5216f392f1...
0xdd5e4d3352abac6d59...	Restore Info	35231010	16 days 19 hrs ago	0xcb376baaf5216f392f1...
0x21065eee8a5fdba8f70...	Restore Info	35230999	16 days 19 hrs ago	0xcb376baaf5216f392f1...
0xb046949f13b5f2b7238...	Restore Info	35230991	16 days 19 hrs ago	0xcb376baaf5216f392f1...
0x73ca986b63b813237d...	Restore Info	35230987	16 days 19 hrs ago	0xcb376baaf5216f392f1...
0x7e37a90671b8d3df8f6...	Restore Info	35230981	16 days 19 hrs ago	0xcb376baaf5216f392f1...
0xd4fd953985619e18ee6...	Restore Info	35230974	16 days 19 hrs ago	0xcb376baaf5216f392f1...
0x6814aa18bdf9efcb289...	Restore Info	35230969	16 days 19 hrs ago	0xcb376baaf5216f392f1...
0xfba866807b289eb3529...	Restore Info	35230962	16 days 19 hrs ago	0xcb376baaf5216f392f1...
0xe8d0373d58ff2fd1f576...	Restore Info	35230957	16 days 19 hrs ago	0xcb376baaf5216f392f1...
0x9df701d37694c350f64...	Restore Info	35230952	16 days 19 hrs ago	0xcb376baaf5216f392f1...
0xfa954b0ae6de59c2e3d...	Toggle Whitelist	35230947	16 days 19 hrs ago	0xcb376baaf5216f392f1...
0x6ebe60a04fd2db6c7eb...	0x60806040	35230914	16 days 19 hrs ago	0xcb376baaf5216f392f1...

CONTINUED

After all the information was restored the dev transferred the ownership to team member Kana, who then performed two operations in the contract. Setting presale launch date and start presale. At this point, he owned the smart contract and was not touched for 11days after this.

These actions can be seen here:

https://ftmscan.com/tx/0x94a15b435a77791e9b64edc0c15619a0eac0bd85dc1c6cf478b9a44c69912e

https://ftmscan.com/tx/0x563e097fbfe1410a570d89bd3b6aa2afae966b8050bac4158ae71dae553fb42d

https://ftmscan.com/tx/0x922c59d5f7e192dd4c162626fa5b14e323a7c8858cdae4530060a1ef759d0c28

When pre-sale round 2 launched on **4/15/2022**, it appeared to be working as planned and there were no issues initially.

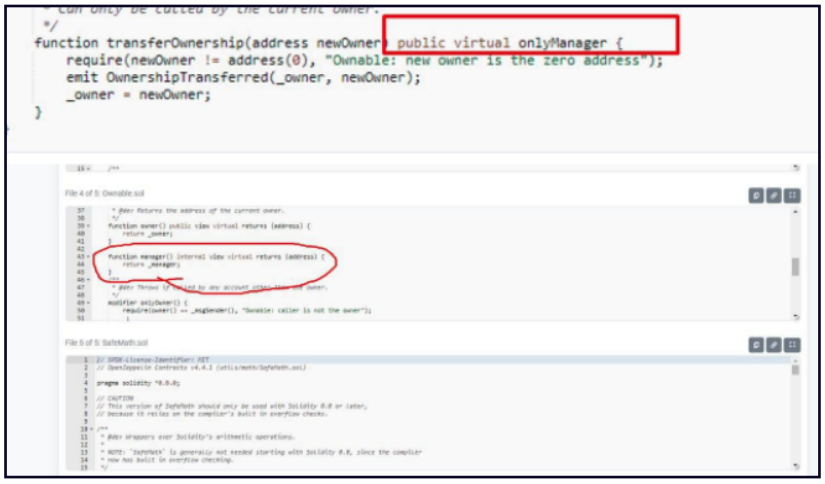
The next day however, Kana was asked to take funds out of p2 to begin launch marketing. When he called the contract it became clear that he no longer had control/ownership.

It was at this point that the team realized that someone transferred ownership (the original dev that deployed the contract).

Transfer of ownership TX:

https://ftmscan.com/tx/0x3d12e80dd4f04e033fc212e54d801ee115ffd3ce1326108a191a790f9635976c

At this time the Xodus team contacted an external developer to review the code and provide guidance. This code consultant explained that a backdoor had been built into the code. As shown in the screenshots below.



The code above can be viewed in full here:

https://ftmscan.com/address/0x34f3d6cccc8ddd1e2c7055591b110a81237af55b#code

CONTINUED

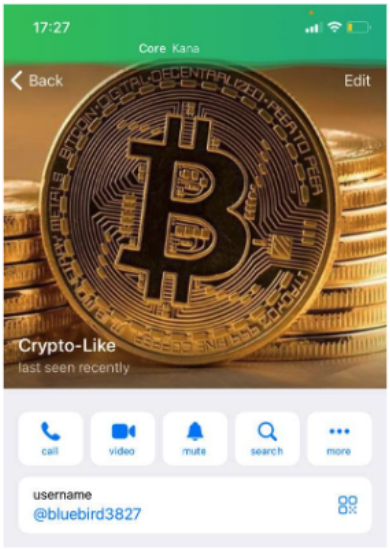
Members of the Xodus team then contacted the supposed rogue developer and asked for the ownership of the contract to be returned to them. A long conversation ensues without the dev agreeing and ultimately concludes with the alleged rogue dev deleting/changing his Telegram handle and exiting the group.

The individual who transferred ownership of the contract & currently is in control of the project funds goes by the pseudonym **Crypto-Like.**

He appears to be constantly changing his Telegram account in an attempt to avoid being tracked.

During the conversations with the team after the event, he was using the Telegram handle **@cryptolike0910.** This has since been deleted.

The most recent known active Telegram handle that he is using is **@bluebird3827** as can be seen in the below image.



Screenshots of the full conversation between the Xodus Finance team & the developer "Crypto-Like" can be found in

Appendix A: Telegram Conversation Record

Currently there is **120,746 DAI** remaining in the contract.
https://ftmscan.com/address/0x34F3d6Cccc8ddd1E2c7055591b110a81237af55B

26,000 DAI was transferred out via emergency withdraw
https://ftmscan.com/tx/0xe68f8cf65c54b182dff121dac90d4dd0c0c075d0eb93978401025b0a33f4e7b6

The **26,000 DAI** were withdrawn to the following address:
0x42404576b6be0484f1106d7945c1140080f03cf3

Since the initial withdraw, **20,000 DAI** have been transferred & bridged to multiple decentralized wallets in **5,000 DAI** increments.

SUMMARY/CONCLUSION

Based on the information gathered regarding the case, it appears that control of the contract was maliciously taken using backdoor code & a bad actor is now in current control of both the contract & the project funds which were raised.

Given the addresses used throughout the chain of transactions involved in moving the funds from the presale contract, it is believed that someone possessing the private keys of the project redistributed the funds from to himself.

There is no evidence that would suggest these funds are being used for legitimate purposes.

The team has made multiple attempts to contact the developer currently in control of the contract & funds via Telegram and although the message has been seen (2 blue ticks), he has not responded at this time.

RECOMMENDED ACTION ITEMS/NEXT STEPS FOR ADVERSELY AFFECTED PARTIES

- **Trying to recover funds by contacting the owner of the project.**
- **Trying to recover funds by using legal agencies/authorities**
- **Investors should contact authorities and make a formal complaint providing this report as an evidence package. File law enforcement reports with the following agencies:**

  Action Fraud
  https://reporting.actionfraud.police.uk/login

  The Financial Conduct Authority
  https://www.fca.org.uk/

  Federal Trade Commission
  http://www.reportfraud.ftc.gov/

  Commodity Futures Trading Commission
  http://www.cftc.gov/Complaint

  U.S. Securities and Exchange Commission
  https://www.sec.gov/tcr

NEXT STEPS FOR ASSURE

- **Assure will provide guidance on additional appropriate jurisdictions & agencies to which injured parties can file reports as applicable.**
- **Fully cooperate with law enforcement agencies upon official requests as received**

RESOURCES

If you have additional information related to this case, please submit via Assure DeFi's scam reporting form using the following link:

https://www.assuredefi.io/scam-reporting-form

Contact Assure DeFi directly via the following channels:

Twitter Direct Message:
www.twitter.com/assuredefi/
Email: chapo@assuredefi.io

ASSURE DEFI™

THE VERIFICATION **GOLD STANDARD**