Sample Crypto Forensics Report for:
Ann E. Target

Date: January 1, 2023
Potential Cryptocurrency Scam
Authored By: Dev E. Loper

Overview/Executive summary

MacNerd Enterprises carried out an extensive forensics investigation on behalf of client, Ann E. Target. The investigation centered primarily on a compromised Ethereum wallet address provided by the client. The client met someone online and conducted crypto exchanges on OnBon (OnBonap.vip). The client suspected they were being scammed after additional money was requested to withdraw funds. Client provided us with the wallet address as well as the suspected scammer's wallet.

1. April 2022, client was contacted via Facebook by an individual who claims to be named Mike Bars, the suspect.
2. Soon after, they began communicating on WhatsApp and developing a catfish-established trust relationship.
3. After introducing client to cryptocurrency, suspect lured client into using the scam site OnBonap.vip.
4. Client expressed concerns and intially did not trust OnBon, but after being convinced and reassured by the suspect that CoinZoom simply changed their name, client proceeded with investing.
5. Under the suspect's guidance, client set up a crypto wallet and made exchanges on OnBonap.vip. Ultimately, these exchanges led to a total investment of approximately $1.3 million USD by the client.
6. Over the course of several months, client's account displayed a return of $5,295,890.54 USD.
7. On October 4, 2022, client attempted a withdrawal of $100,000 USD from the exchange account on the OnBanap.vip platform. Upon reaching out, client was informed that a "Platform Fee" of 12% of the account balance needed to be paid before funds could be released.
8. Client was further informed that this Platform Fee could not be paid by the existing funds in the exchange account and was provided a different wallet address for payment.

Website Recon Findings

1.1 Scope

The website that the client was instructed to use was OnBonap.vip. Below are the websites we scanned and did recon on.

https://www.OnBonap.vip/#/pages/tabBar/home/home

https://www.OnBonap.vip/#/pages/personal/login/login

We ran a series of IP lookups, DNS searches, reverse searches, and website scanning tools. We found that their website is being hosted by Amazon AWS. Here are the Ips that we found associated with the scamming website:

XX.84.37.100
XX.84.37.80
XX.85.61.105
XX.249.98.75
XX.249.98.96
XX.249.98.54
XX.249.98.72
XX.155.202.125
XX.155.202.9
XX.155.202.30
XX.155.202.98

All Ips are confirmed to be associated with Amazon's AWS services and the DNS host name is under "Namecheap, Inc". All reverse DNS lookups point to cloudfront.net servers. The findings/geo locations for the above IP addresses are in the next section.

We observed from one of our scans that the debug messages were written in Chinese.

1.2 Login & Home Geo location

Addresses XX.84.37.100 && XX.84.37.80 were found within the network tab when inspecting the page. Geolocation for these Ip's:

- United States, Newark New Jersey. ISP: Amazon.com INC
- United States, Newark New Jersey. ISP/Organization AMAZON-02
- United States Washington Seattle: ISP/Organization Amazon Technologies

Using https://www.iplocation.net/ POST methods from the home page were addressed to: XX.85.61.105
Geolocation for this address:

- United States, Newark New Jersey. ISP: Amazon.com INC
- United States, Virginia, Ashburn ISP: Amazon.com Using AWS
- United States Washington Seattle: ISP/Organization AMAZON-02

Using https://iplocation.com/ gave the location for Ip's XX.84.37.100**,** XX.84.37.80:

- Organization: Amazon CloudFront
- Location: Wichita Kansas

1.3 DNS

The DNS host provider is "Namecheap, Inc."

DNS lookup:

- Tool used: https://mxtoolbox.com/
- Common Name: OnBonap.vip
- Issuer: Amazon
  - Serial: 1234567890XYZ123
- Expires: 12 months
- Valid From: 8/3/2022
- Valid To: 9/2/2023
- Refer to screenshot DNS_Lookup1 for full reference.

DNS lookup for: https://www.OnBonap.vip/#/pages/tabBar/home/home

- Tool Used: https://www.whatismyip.com/dns-lookup/
- IPs: XX.249.98.75
  - XX.249.98.96
  - XX.249.98.54
  - XX.249.98.72
- Location: Miami, Florida: 33010
- Host: Amazon.com Inc
- Domain amazon.com

- Network speed: T1

Running https://www.OnBonap.vip/ through DNS lookup:

- 18.155.202.125
- 18.155.202.9
- 18.155.202.30
- 18.155.202.98

All IPs are hosted by Amazon.com, Inc

Transaction Findings

Below are the findings gathered from following some of the transactions out from our clients wallet address: (address redacted)

We followed two transactions. Both transactions ended at Binance 14. It is clear that most of the accounts that the funds traveled through are involved in scams/illegal activity of some sort. Many of them have the label “poor reputation” and have been reported in numerous scamming activities. A good majority of them also participate in transactions with a scam token called ERC-20 TOKEN* . This token seems to be a mimic/copy of the actual token ERC-20 perhaps created with the intent to further scam victims. All transactions involving ERC-20 TOKEN* were flagged by etherscan.io.

Two addresses within the transaction flow had direct dealings with contracts labeled Fake_Phishing8133 and Fake_Phishing2894. While Fake_Phising2894 has been closed since late 2021, Fake_Phising8133 is still active and making transactions. All transactions within these contracts are dealing with ERC-20 TOKEN* . Our conclusion based on the evidence is that the client was the victim of a crypto scamming scheme.

Evidence

One of the first accounts that our client's wallet interacted with already had a "warning" message attached to it. We followed the transaction involving address (address redacted) from the client's wallet. Many of the accounts that it routed the token through were also tagged with an "untrustworthy/warnings". Deeper in the transaction flow, a large majority of the wallets were documented as having previously dealt in a token called ERC-20 TOKEN* . This token was found to be used in many phishing/scamming incidents.

The LooksRare: Deployer sent a majority of the ERC tokens to the addresses associated with (address redacted). The transactions within LooksRare are extremely odd as there are thousands of transactions all occurring at the same time and for the same amount of 800 units.

Address (address redacted) has a different contract and amount for its transaction. The contract is Arbitrum: Bridge and the amount is for 738 units. The Arbitrum Bridge page on Etherscan also has a message warning users about its poor reputation.

(Address redacted) has a contract Tether: USDT Stablecoin for the token amount of 6,000 units. One transaction stood out: an ERC-20 in the amount of 6,330,000,000. This ERC token does not have any warnings placed on it. All the other ERC transactions associated with the phishing addresses could be mimic accounts of this specific token as their names only vary by one * character.

The transactions originating from address (address redacted) end in two transactions to Binance 14 through accounts (address redacted) & (address redacted).

The former's last transaction was this outbound to Binance, but the latter still has transactions occurring to this day. When following this specific branch, the other accounts usually split up the amounts transferred. This account always sends to Binance exactly the amount it receives. We strongly recommend monitoring this account.

The other account we followed was (address redacted)
Specifically, this Tether: USDT transaction (address redacted) has an entire transaction history with (address redacted) and the token ERC-20 TOKEN*. Some of the transactions are in the trillions.

Findings Conclusion

Our findings indicate the clear presence of a scam/phishing attack. Just going 3 to 4 addresses deep withing the transactions, the number of addresses that were tagged with “warning” messages kept increasing. The fact that there are so many of them, with some being still active and some going back to last year indicate that these accounts and scams have most likely taken many victims. While these accounts are extremely useful to the scammers, a heavy part plays in the communication these scammers have with their victims. The result of basic internet searches of OnBonap.vip indicates that the website cannot be trusted and is, in fact, a scam.

Supplementary Information / Transactions

Ethereum Transactions – Client ETH wallet
Date Range: 08/02/22 – 09/29/22
(address redacted)

Exchanges under Tether Contract address: Tether USD
(address redacted)

Sender: (address redacted)

- Block No: 1234567
- Amount: $123,356.78
- Token Value: 123,456.7891
- Gas Value:
- Hash: (address redacted)
- Receiver: (address redacted)
- Timestamp: 08-04-2022 07:17:00

A complete report would provide all wallet addresses, tokens and exchanges investigated with specific details like the above.

End of Report