Intelligence On Chain

Investigation Report - Anonymised. For Education purposes only
Completed by JP

RESEARCH ★ INVESTIGATIONS ★

Blockchain	Avalanche
Transaction Hash	https://snowtrace.io/tx/0xead749051dca91fd8b80016a72d629bbbe60e7ac5231ad4add39720c4333cb93
Victim Address	0x80ea59690d1e903f5ecf732e7b311856cdb8c113
Attacker Address	0xb7F1c4c7bD985B1F034Bb166f92e3d93D2DA91bd
Date of Exploit	2022-05-17 08:23 (UTC)- 298 AVAX stolen worth $10,233 at the time

1. Introduction - Intelligence On Chain

Established in January 2022, Intelligence On Chain, commenced operations as a provider of impartial research on DeFi projects. Presently, we offer professional inquiries to our clients and members, complemented with educational material that seeks to enhance decision-making processes based on risk assessment. Please note that our investigation services do not provide any assurances regarding the recovery of funds. Our comprehensive service entails a written report that details the exploit's trajectory and the current location of funds at the time of issuance.

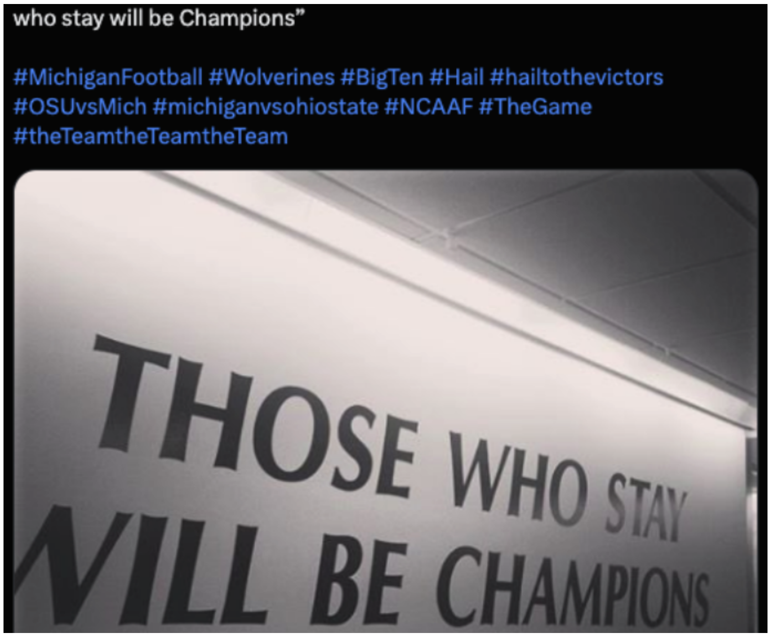
Visit intelligenceonchain.com for more information

2. Suspect Details - Anonymised

The Suspect is a developer at AnonymisedAddress.com. Here are some of his details:

Discord Name: **Anonymised**
Twitter: **Anonymised**
Twitter ID: **Anonymised**
Suspended Reddit: **Anonymised**
Github Repository: **Anonymised**
Github: **Anonymised**
Unconfirmed: Snapchat: **Anonymised**

Tweet provides some form of association with Michigan

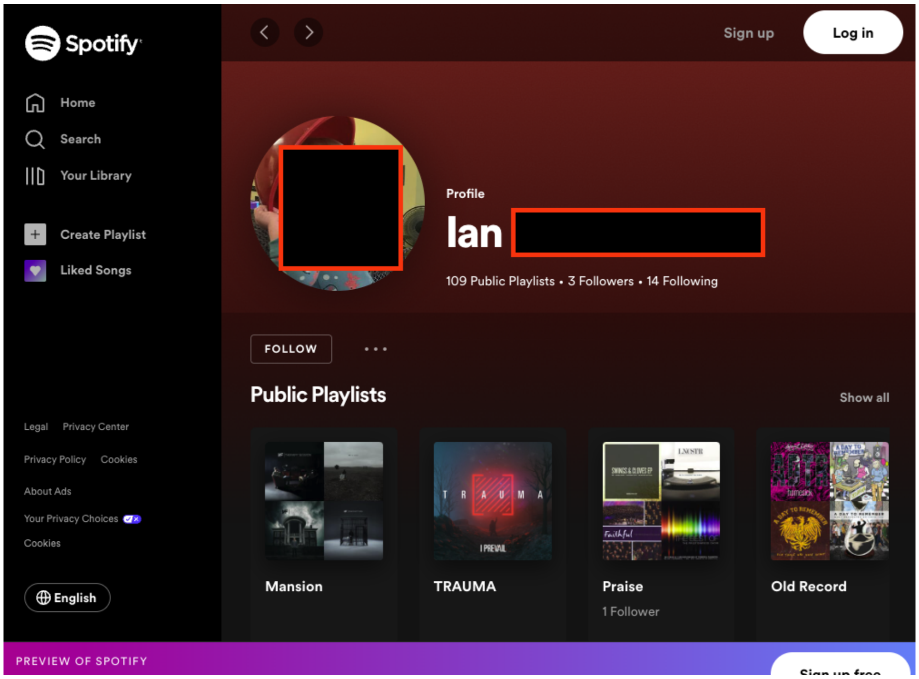


who stay will be Champions”

#MichiganFootball #Wolverines #BigTen #Hail #hailtothevictors #OSUvsMich #michiganvsohiostate #NCAAF #TheGame #theTeamtheTeamtheTeam

Anonymised - This spotify was linked to **Anonymised** account. We used it to look for further information (its archived so it can’t be deleted). The information retrieved here was a full name including a middle name!

Be cautious - Was this Spotify account the actual suspect’s account of a friends?? Be open minded and don’t disclose any information publicly until you are absolutely sure



[redacted]

Profile

Ian [redacted]

109 Public Playlists • 3 Followers • 14 Following

Public Playlists

Mansion

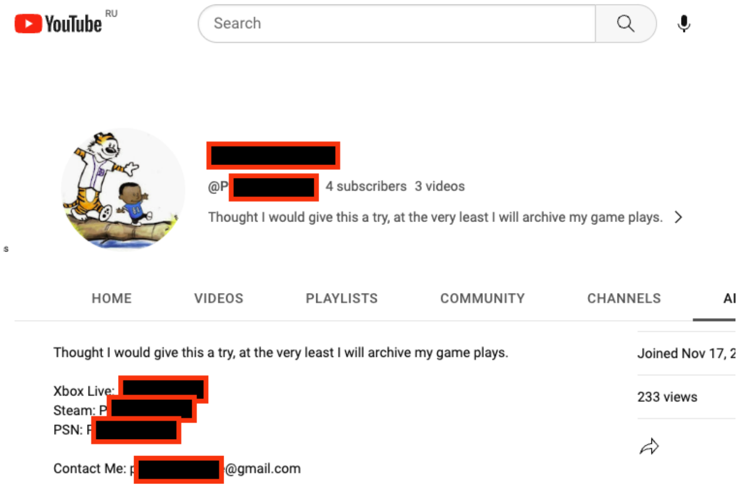
TRAUMA

Praise
1 Follower

Old Record

Having then searched for this person, we identified another online persona or alias, closely associated with the individual. You'll see this represented as @Pum******

Anonymised Youtube Channel - Reveals a **link to an email!**



[redacted]

@P[redacted] 4 subscribers 3 videos

Thought I would give this a try, at the very least I will archive my game plays.

Thought I would give this a try, at the very least I will archive my game plays.

Xbox Live: [redacted]
Steam: P[redacted]
PSN: P[redacted]

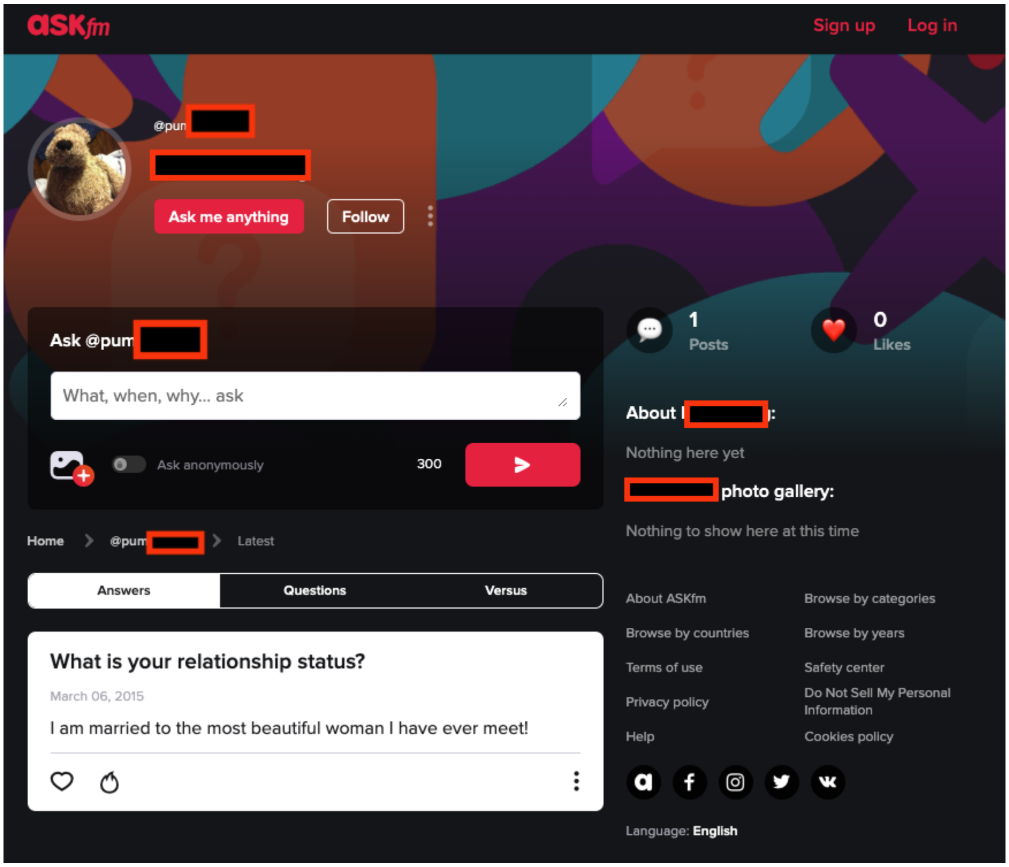
Contact Me: p[redacted]@gmail.com

Joined Nov 17, 2

233 views

Anonymised Xbox Gamer Pass

Anonymised Ask FM - Revealed a **link to a name!**



@pun[redacted]

[redacted]

Ask @pum[redacted]

What, when, why... ask

1 Posts

0 Likes

About [redacted]:

Nothing here yet

[redacted] photo gallery:

Nothing to show here at this time

Home > @pum[redacted] > Latest

What is your relationship status?

March 06, 2015

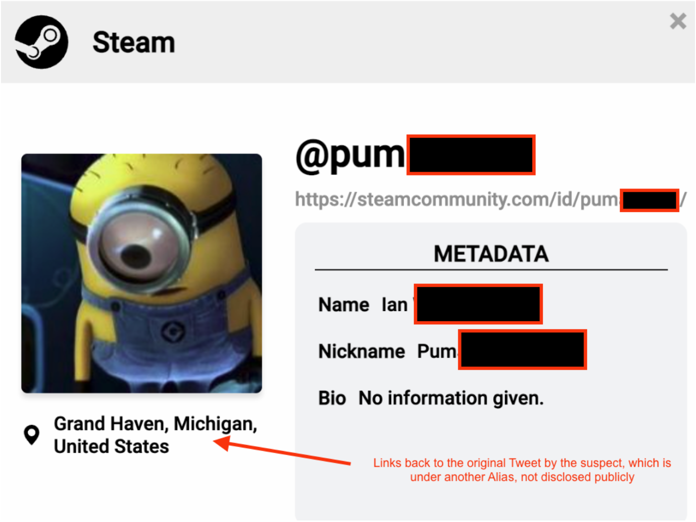
I am married to the most beautiful woman I have ever meet!

Language: English

Anonymised - Instagram Account that shows the link between Full Name, Alias and provides images of the suspect.

NOTE: As a sleuth, you can never be sure that your understanding of the context is accurate. For example, The Spotify account that was linked to the suspect's Discord account, may have been a friend or family's Spotify account. Therefore your role is to gather as much information as possible and hand it over to the authorities!

Anonymised Steam - Links to Grand Haven, Michigan - Important because this links this person, alias to the other alias used on Discord! In other words, we're starting to connect the dots



@pum[redacted]

https://steamcommunity.com/id/pum[redacted]/

METADATA

Name Ian [redacted]

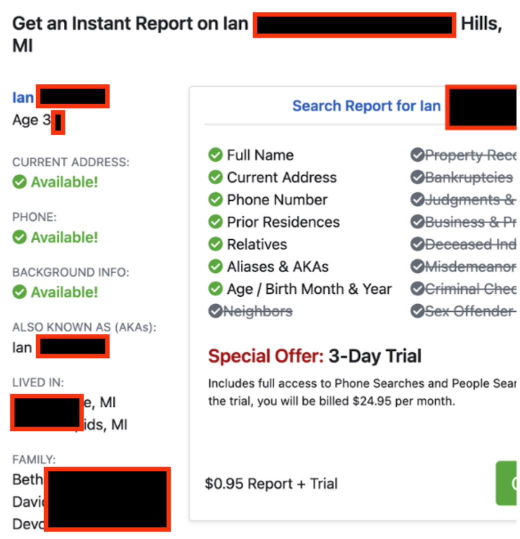
Nickname Pum[redacted]

Bio No information given.

Grand Haven, Michigan, United States

Links back to the original Tweet by the suspect, which is under another Alias, not disclosed publicly

Once we have connected the dots, we can then go looking for personal information that can be provided to law enforcement, enabling them to cross-reference these names and aliases to centralised accounts that we find during our on-chain sleuthing.



Get an Instant Report on Ian [redacted] Hills, MI

Ian [redacted]
Age 3[redacted]

CURRENT ADDRESS:
✓ Available!

PHONE:
✓ Available!

BACKGROUND INFO:
✓ Available!

ALSO KNOWN AS (AKAs):
Ian [redacted]

LIVED IN:
[redacted]e, MI
ids, MI

FAMILY:
Beth [redacted]
Davi
Devo

Search Report for Ian [redacted]

✓ Full Name
✓ Current Address
✓ Phone Number
✓ Prior Residences
✓ Relatives
✓ Aliases & AKAs
✓ Age / Birth Month & Year
⊘ ~~Neighbors~~

⊘ ~~Property Reco~~
⊘ ~~Bankruptcies~~
⊘ ~~Judgments &~~
⊘ ~~Business & Pr~~
⊘ ~~Deceased Ind~~
⊘ ~~Misdemeanor~~
⊘ ~~Criminal Chec~~
⊘ ~~Sex Offender~~

Special Offer: 3-Day Trial

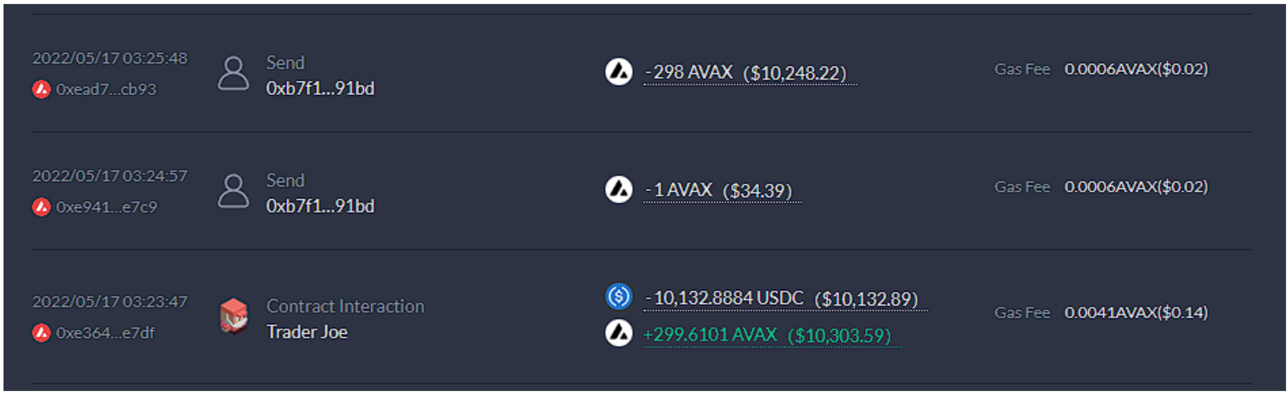
Includes full access to Phone Searches and People Sear
the trial, you will be billed $24.95 per month.

$0.95 Report + Trial

3. Events leading up to the theft

The image below shows activity happening within the victim's wallet. A swap from Avalanche's $AVAX token to 10,233 $USDC. Following that funds are sent out of the victim's wallet via a test transaction and then the remainder.

This screenshot shows DeBank and the visualisation of swaps and sends

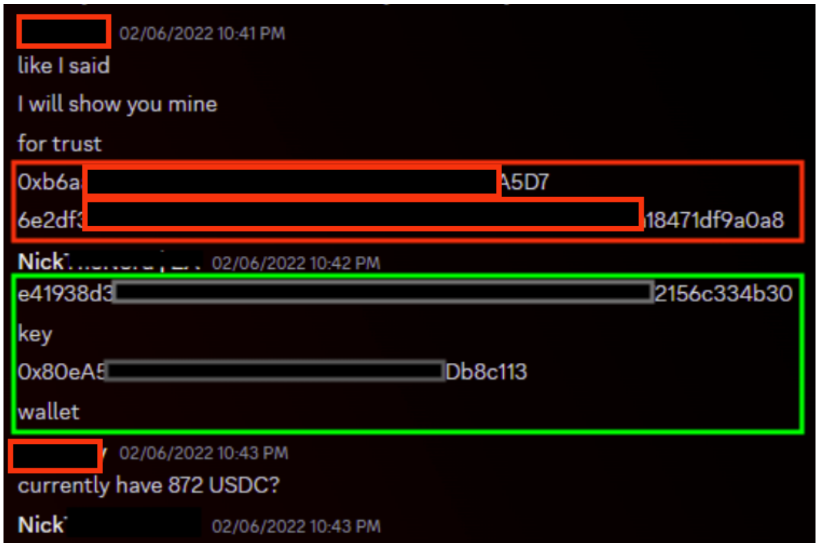


2022/05/17 03:25:48 0xead7...cb93	Send 0xb7f1...91bd	-298 AVAX ($10,248.22)	Gas Fee 0.0006AVAX($0.02)
2022/05/17 03:24:57 0xe941...e7c9	Send 0xb7f1...91bd	-1 AVAX ($34.39)	Gas Fee 0.0006AVAX($0.02)
2022/05/17 03:23:47 0xe364...e7df	Contract Interaction Trader Joe	-10,132.8884 USDC ($10,132.89) +299.6101 AVAX ($10,303.59)	Gas Fee 0.0041AVAX($0.14)

During this investigation, we will follow this money to determine its exit point from the blockchain, or to an account on a centralised exchange whereby, this report can be handed over to the authorities, by the victim, in order to obtain information about the account/s.

Prior to this theft happening on the 17th May, there was a chain of events that took place that may or may not explain what happened to the victim's wallet. It is during this investigation, that we will look for further evidence to build an accurate narrative either proving this theory is correct or incorrect.

Conversations between the Victim and Suspect:
On the 6th of February, the victim was persuaded to give up their private key to their wallet, essentially giving full control of that wallet to someone else, in this case, **Anonymised**


[redacted] 02/06/2022 10:41 PM
like I said
I will show you mine
for trust
0xb6a[redacted]A5D7
6e2df[redacted]18471df9a0a8
Nick[redacted] 02/06/2022 10:42 PM
e41938d3[redacted]2156c334b30
key
0x80eA5[redacted]Db8c113
wallet
[redacted] 02/06/2022 10:43 PM
currently have 872 USDC?
Nick[redacted] 02/06/2022 10:43 PM

As you can see, **Anonymised** fostered "trust" by providing his own private key, in order to persuade the victim that it is ok to share. The victim shared his private key on the 6th of February 2022 at 10:42pm local time.
This was shared one more time on 3rd of March at 14:41 local time, with **Anonymised**

4. Following the funds

We have drawn out the exploit using MetaSleuth. The link for the map is here: https://metasleuth.io/result/avalanche/0x782f924e420aA88A9318Bed827a9e1e210619f00?source=8785a374-75b0-44e8-a350-f491774fdeed which is valid until 19-10-2023

The three transactions that occur are (oldest to newest):

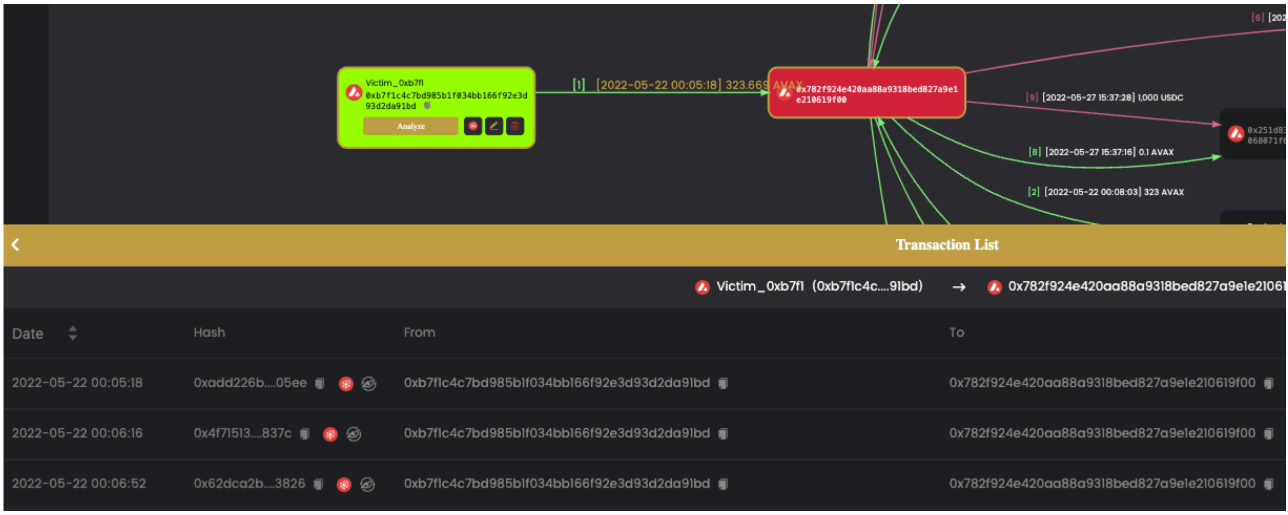
1. 0xadd226ba15818460f0cc941744d775aac09cdea39ff053e7045329a82c9b05ee
   a. 1 AVAX, tester transaction
2. 0x4f715137042c5662be4cddf0b324f06947e5cc195202d4f1889b7c79aeb1837c
   a. 322.66 AVAX, full amount
3. 0x62dca2b84a543e1bd08453284722a35a9202a90a64396417e60dd2cb5d343826

a. 0.009 AVAX to remove final amounts

After reviewing these transactions manually and looking at the call logs on Tenderly, we can confirm that no contracts were used in this theft. The 'call' was made from the wallet indicating that either the seed phrase, private key or the victim's device is compromised.

Main theft transaction Tenderly link
Test transaction Tenderly link

The image below shows the 3 transactions in Metasleuth. The total amount stolen was 322.669 AVAX


Victim_0xb7f1
0xb7f1c4c7bd985b1f034bb166f92e3d93d2da91bd
Analyze
[1] [2022-05-22 00:05:18] 323.669 AVAX
0x782f924e420aa88a9318bed827a9e1e210619f00
[6] [202
[9] [2022-05-27 15:37:28] 1,000 USDC
[8] [2022-05-27 15:37:16] 0.1 AVAX
[2] [2022-05-22 00:08:03] 323 AVAX
0x251d8
068071f

Transaction List

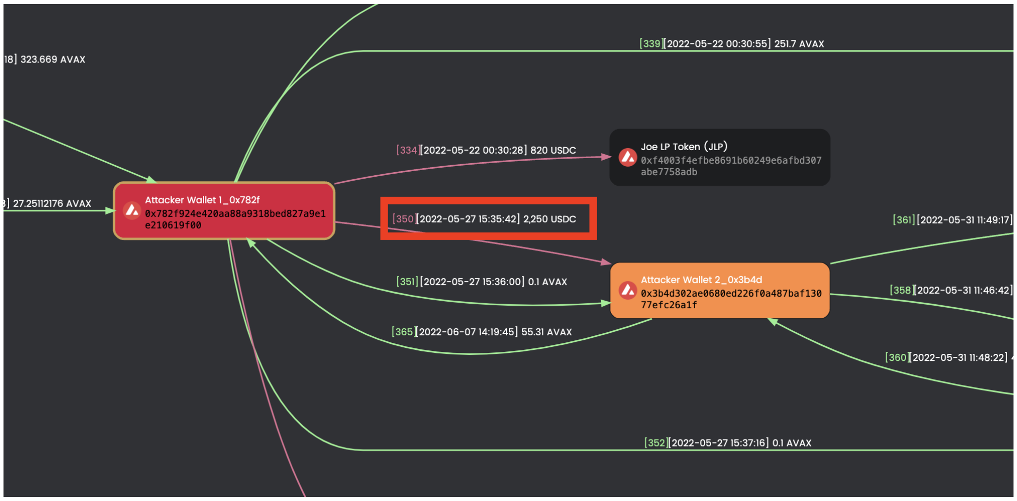
Victim_0xb7f1 (0xb7f1c4c....91bd) → 0x782f924e420aa88a9318bed827a9e1e21061

Date	Hash	From	To
2022-05-22 00:05:18	0xadd226b....05ee	0xb7f1c4c7bd985b1f034bb166f92e3d93d2da91bd	0x782f924e420aa88a9318bed827a9e1e210619f00
2022-05-22 00:06:16	0x4f71513....837c	0xb7f1c4c7bd985b1f034bb166f92e3d93d2da91bd	0x782f924e420aa88a9318bed827a9e1e210619f00
2022-05-22 00:06:52	0x62dca2b....3826	0xb7f1c4c7bd985b1f034bb166f92e3d93d2da91bd	0x782f924e420aa88a9318bed827a9e1e210619f00

All funds head to this wallet: 0x782f924e420aa88a9318bed827a9e1e210619f00 and from there, we're able to identify a number of swaps before heading out to a centralised exchange. Following receiving the funds, the attacker wallet then swaps the AVAX coins for USDC tokens. This is shown in this transaction.

From there 2,250 $USDC is sent to Attacker wallet 2, shown in these transactions:

- 0xe2ae519c23e0acc5204da129ceeb83e4053ff392cafa0236a15b95789c7f2d62
- 0x324977a8c04dae32bb9ee0d4c4ac4c83f3cccb94aa5186b272071317bd70641b
- 0x9b155cd30fcf6233866e4dee8ddaadb04da91afeba13482944eeb2674f8656f3
- 0x718ac3ecc9fb76884e52d4fa80924988debf0ae4d966293ae9d67f2628d88d1d
- 0xf16d42c08baf9dec1869289e24c90660d1aecbb5caf4244f1b20e5218384ab4a
-


18] 323.669 AVAX
[339][2022-05-22 00:30:55] 251.7 AVAX
[334][2022-05-22 00:30:28] 820 USDC
Joe LP Token (JLP)
0xf4003f4efbe8691b60249e6afbd307abe7758adb
3] 27.25112176 AVAX
Attacker Wallet 1_0x782f
0x782f924e420aa88a9318bed827a9e1e210619f00
[350][2022-05-27 15:35:42] 2,250 USDC
[361][2022-05-31 11:49:17]
[351][2022-05-27 15:36:00] 0.1 AVAX
Attacker Wallet 2_0x3b4d
0x3b4d302ae0680ed226f0a487baf13077efc26a1f
[358][2022-05-31 11:46:42]
[365][2022-06-07 14:19:45] 55.31 AVAX
[360][2022-05-31 11:48:22]
[352][2022-05-27 15:37:16] 0.1 AVAX

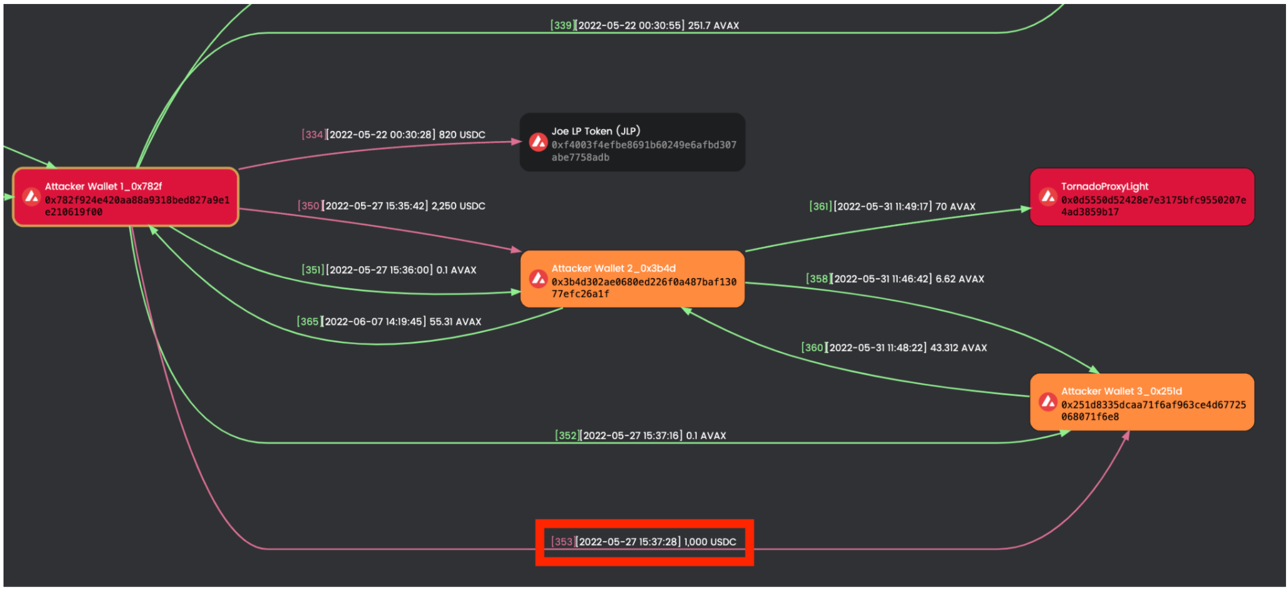
Some funds were then converted back to AVAX:

- 0x2ac425c874e47d8d061d335275d4d19a6b1c7b6b5891e706a8724fc84c650246
- 0xe98a30e81220cf6321c391619e3a95486ea06ccc38004743c20da30438588509

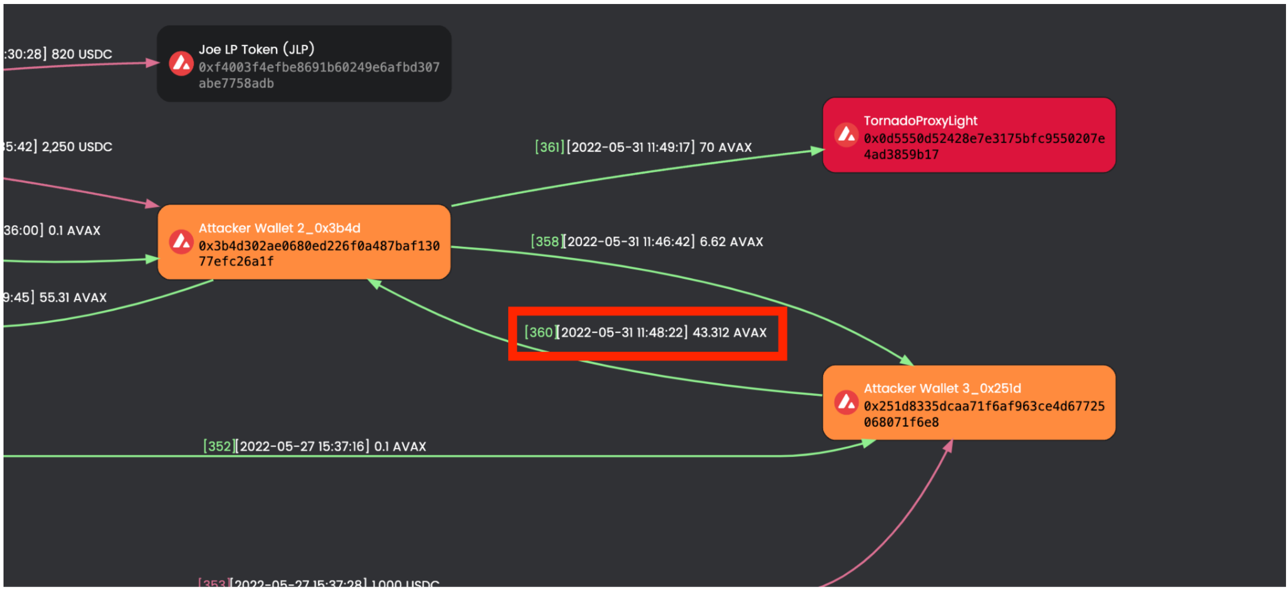
1000 $USDC was sent to Attacker Wallet 3:

- 0x17e22c2da0761114e1bcc638a396c4208305dab9c4aa5793f220a8c115a92ba6

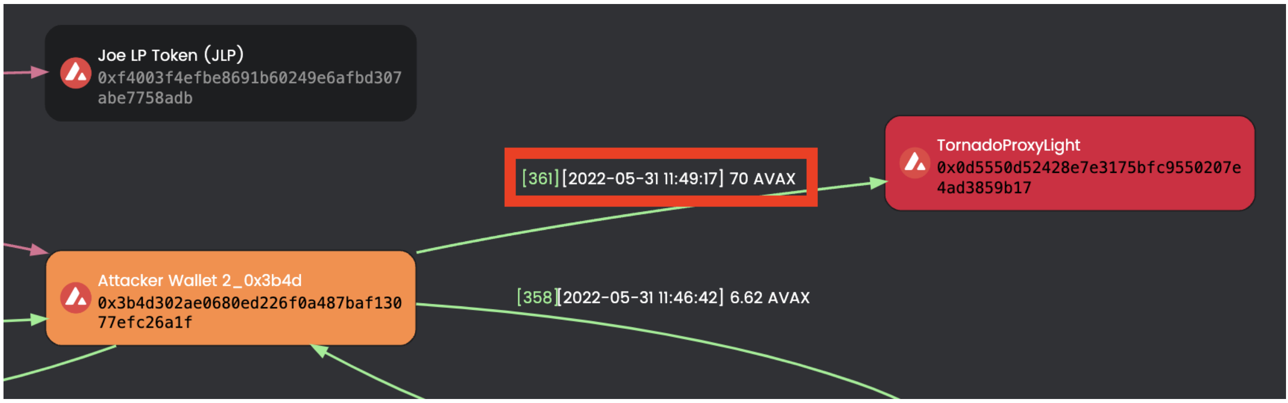
All of the above transactions are shown here


[339][2022-05-22 00:30:55] 251.7 AVAX
[334][2022-05-22 00:30:28] 820 USDC
Joe LP Token (JLP)
0xf4003f4efbe8691b60249e6afbd307abe7758adb
Attacker Wallet 1_0x782f
0x782f924e420aa88a9318bed827a9e1e210619f00
[350][2022-05-27 15:35:42] 2,250 USDC
[361][2022-05-31 11:49:17] 70 AVAX
TornadoProxyLight
0x0d5550d52428e7e3175bfc9550207e4ad3859b17
[351][2022-05-27 15:36:00] 0.1 AVAX
Attacker Wallet 2_0x3b4d
0x3b4d302ae0680ed226f0a487baf13077efc26a1f
[358][2022-05-31 11:46:42] 6.62 AVAX
[365][2022-06-07 14:19:45] 55.31 AVAX
[360][2022-05-31 11:48:22] 43.312 AVAX
Attacker Wallet 3_0x251d
0x251d8335dcaa71f6af963ce4d67725068071f6e8
[352][2022-05-27 15:37:16] 0.1 AVAX
[353][2022-05-27 15:37:28] 1,000 USDC

In Attack Wallet 3, all of the funds are eventually converted to AVAX and sent back to Attack Wallet 2 in this transaction. This is also shown in the diagram below

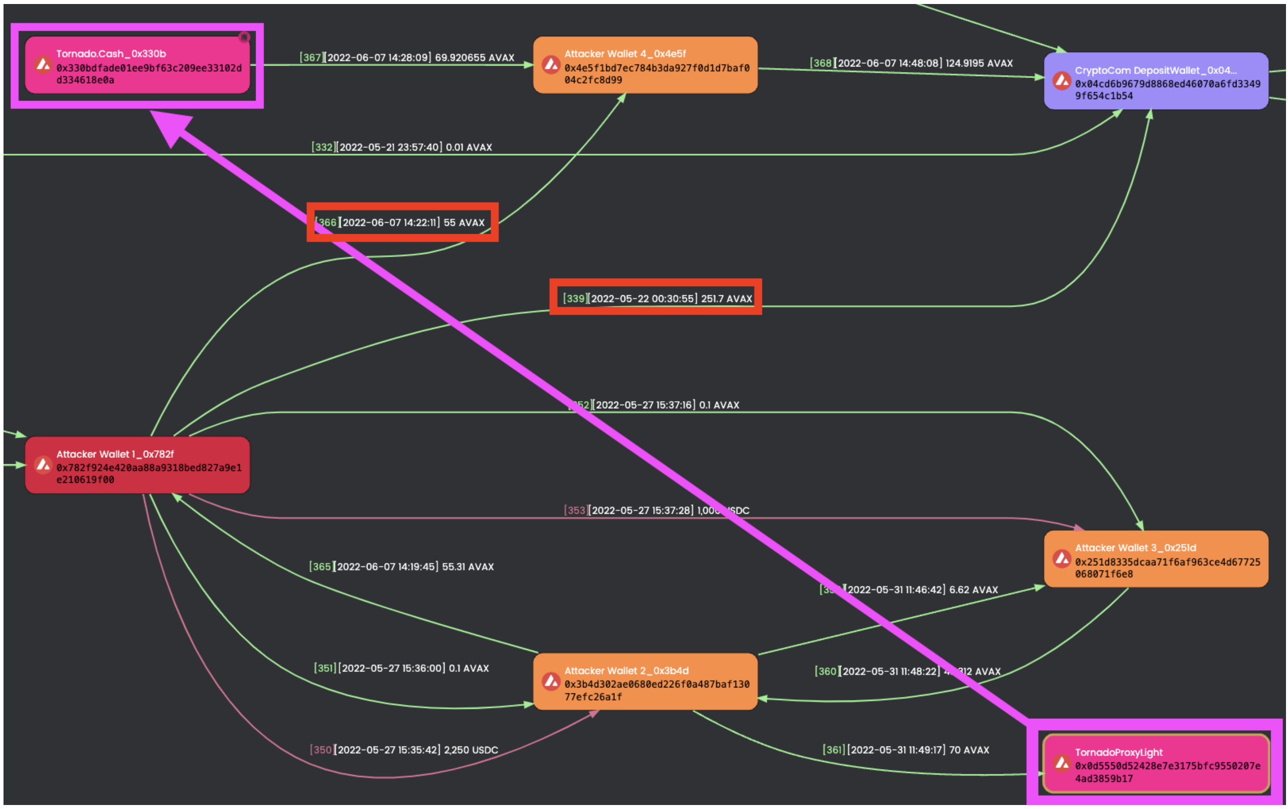

:30:28] 820 USDC
Joe LP Token (JLP)
0xf4003f4efbe8691b60249e6afbd307abe7758adb
5:42] 2,250 USDC
[361][2022-05-31 11:49:17] 70 AVAX
TornadoProxyLight
0x0d5550d52428e7e3175bfc9550207e4ad3859b17
36:00] 0.1 AVAX
Attacker Wallet 2_0x3b4d
0x3b4d302ae0680ed226f0a487baf13077efc26a1f
[358][2022-05-31 11:46:42] 6.62 AVAX
9:45] 55.31 AVAX
[360][2022-05-31 11:48:22] 43.312 AVAX
Attacker Wallet 3_0x251d
0x251d8335dcaa71f6af963ce4d67725068071f6e8
[352][2022-05-27 15:37:16] 0.1 AVAX
[353][2022-05-27 15:37:28] 1,000 USDC

In total, 70 AVAX was deposited to Tornado Cash shown here


Joe LP Token (JLP)
0xf4003f4efbe8691b60249e6afbd307abe7758adb
[361][2022-05-31 11:49:17] 70 AVAX
TornadoProxyLight
0x0d5550d52428e7e3175bfc9550207e4ad3859b17
Attacker Wallet 2_0x3b4d
0x3b4d302ae0680ed226f0a487baf13077efc26a1f
[358][2022-05-31 11:46:42] 6.62 AVAX

Tornado Cash is a mixer, allowing people to mix their funds with others' essentially reducing the risk of exposing where the funds are withdrawn to. Typically Tornado cash analysis isn't included in our basic investigations, however, the attacker made the mistake of withdrawing the funds to Attacker wallet 4, which is directly linked to both

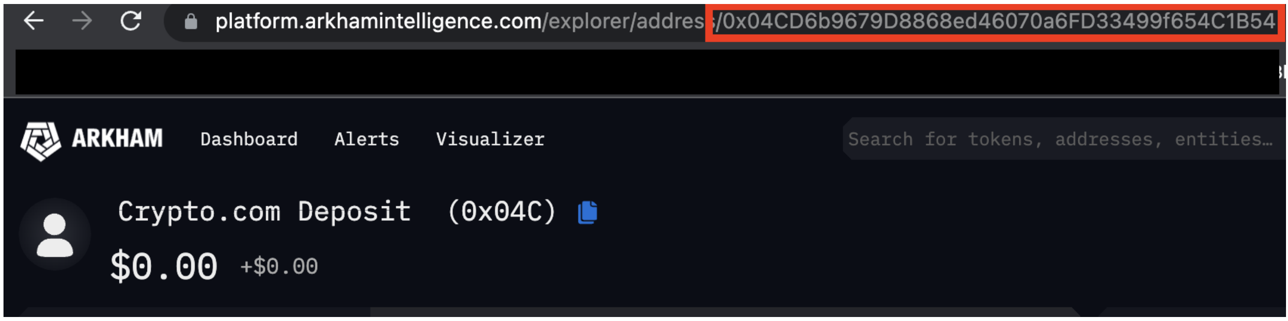
Attacker wallet 1 and Crypto.com.


Tornado.Cash_0x330b
0x330bdfade01ee9bf63c209ee33102dd334618e0a
[367][2022-06-07 14:28:09] 69.920655 AVAX
Attacker Wallet 4_0x4e5f
0x4e5f1bd7ec784b3da927f0d1d7baf004c2fc8d99
[368][2022-06-07 14:48:08] 124.9195 AVAX
CryptoCom DepositWallet_0x04...
0x04cd6b9679d8868ed46070a6fd33499f654c1b54
[332][2022-05-21 23:57:40] 0.01 AVAX
[366][2022-06-07 14:22:11] 55 AVAX
[339][2022-05-22 00:30:55] 251.7 AVAX
52][2022-05-27 15:37:16] 0.1 AVAX
Attacker Wallet 1_0x782f
0x782f924e420aa88a9318bed827a9e1e210619f00
[353][2022-05-27 15:37:28] 1,00 SDC
Attacker Wallet 3_0x251d
0x251d8335dcaa71f6af963ce4d67725068071f6e8
[365][2022-06-07 14:19:45] 55.31 AVAX
[2022-05-31 11:46:42] 6.62 AVAX
[351][2022-05-27 15:36:00] 0.1 AVAX
Attacker Wallet 2_0x3b4d
0x3b4d302ae0680ed226f0a487baf13077efc26a1f
[360][2022-05-31 11:48:22] 312 AVAX
[350][2022-05-27 15:35:42] 2,250 USDC
[361][2022-05-31 11:49:17] 70 AVAX
TornadoProxyLight
0x0d5550d52428e7e3175bfc9550207e4ad3859b17

One of the more important transactions is when Attacker Wallet 1 sends funds directly to Crypto.com Deposit wallet 0x04cd6, shown in the following transactions:

- 0x963d4ab91663e9da9c135bfe3489789ab2168b4d9a98669de872caf3f099f652
- 0x2c4f3b96d9378e7f246ccfea6092018e3f236f341a6298bce52a4294b1f2046a
- 0x5354d720c8f7fb2c84af8ae68cda8365af1564e8886bf1d2f6d7e0a9fc493c14
- 0xe4fe5ff6da4e6031dfa6fd79c05bd4b2fa1adff6ad5d4d717e6b9e261fe47394
- 0xf09cdcf77d962e4a2277d030d1a61a833f919a22785c15b67351b93f427ee0e9

251.7 AVAX was sent directly to Crypto.com Deposit wallet. This is indicated as a crypto.com wallet on Arkham Intelligence (shown below)



platform.arkhamintelligence.com/explorer/address/0x04CD6b9679D8868ed46070a6FD33499f654C1B54

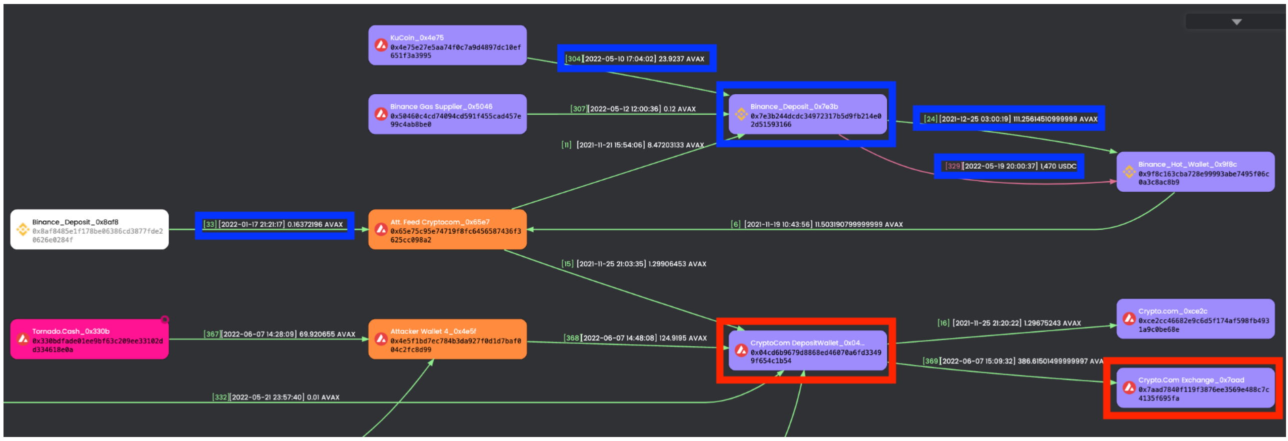
[redacted]

Crypto.com Deposit (0x04C)

$0.00 +$0.00

This investigation then opens up a number of different transactions and wallets which may lead to identification of the attacker. The map below shows the transactions we discussed prior in RED.

In BLUE, you will see the transactions and wallets that I will list below. Each one of them presents an opportunity to identify an account owner. The Orange wallet (at the top) identified as [Att. Feed Cryptocom]() is the wallet that feeds the crypto.com deposit address. This is crucial as it is the very first transaction to take place in that wallet and is likely to be the same person. All BLUE wallets are linked back to Att. Feed Cryptocom


KuCoin_0x4e75
0x4e75e27e5aa74f0c7a9d4897dc10ef651f3a3995
[304][2022-05-10 17:04:02] 23.9237 AVAX
Binance Gas Supplier_0x5046
0x50460c4cd74094cd591f455cad457e99c4ab8be0
[307][2022-05-12 12:00:36] 0.12 AVAX
[11] [2021-11-21 15:54:06] 8.47203133 AVAX
Binance_Deposit_0x7e3b
0x7e3b244dcdc34972317b5d9fb214e02d51593166
[24] [2021-12-25 03:00:19] 111.25614510999999 AVAX
[329][2022-05-19 20:00:37] 1,470 USDC
Binance_Hot_Wallet_0x9f8c
0x9f8c163cba728e99993abe7495f06c0a3c8ac8b9
Binance_Deposit_0x8af8
0x8af8485e1f178be06386cd3877fde20626e0284f
[33] [2022-01-17 21:21:17] 0.16372196 AVAX
Att. Feed Cryptocom_0x65e7
0x65e75c95e74719f8fc6456587436f3625cc098a2
[6] [2021-11-19 10:43:56] 11.503190799999999 AVAX
[15] [2021-11-25 21:03:35] 1.29906453 AVAX
Tornado.Cash_0x330b
0x330bdfade01ee9bf63c209ee33102dd334618e0a
[367][2022-06-07 14:28:09] 69.920655 AVAX
Attacker Wallet 4_0x4e5f
0x4e5f1bd7ec784b3da927f0d1d7baf004c2fc8d99
[368][2022-06-07 14:48:08] 124.9195 AVAX
CryptoCom DepositWallet_0x04...
0x04cd6b9679d8868ed46070a6fd33499f654c1b54
[16] [2021-11-25 21:20:22] 1.29675243 AVAX
Crypto.com_0xce2c
0xce2cc46682e9c6d5f174af598fb4931a9c0be68e
[369][2022-06-07 15:09:32] 386.61501499999997 AVA
Crypto.Com Exchange_0x7aad
0x7aad7840f119f3876ee3569e488c7c4135f695fa
[332][2022-05-21 23:57:40] 0.01 AVAX

5. Important Addresses and Transactions for Law Enforcement to request Subpoenas, in order to identify the attackers.

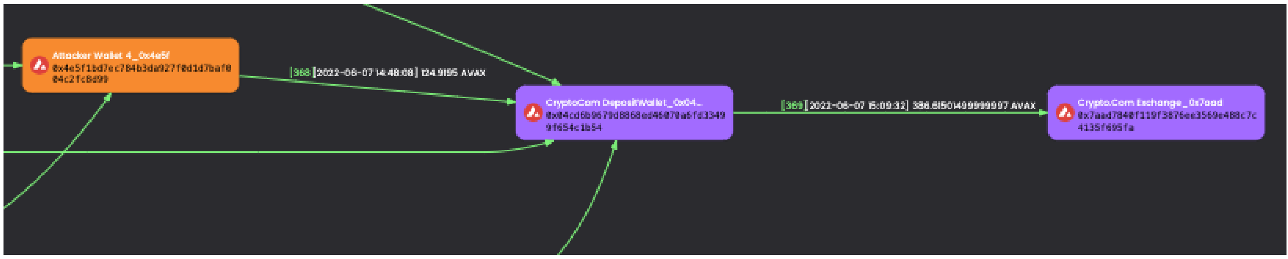
It is important to recognise that these accounts are attributed to the attacker. You must use the information obtained by Law Enforcement, from the centralised exchanges involved in order to compare them with the know team wallets of the suspected individual

Crypto.com
[Cryptocom DepositWallet_0x04_]() - 0x04cd6b9679d8868ed46070a6fd33499f654c1b54

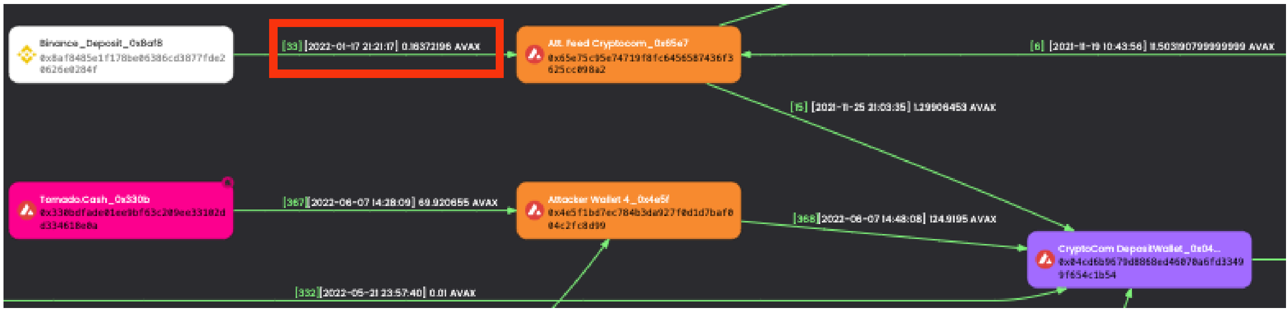
Exchange wallet: 0x7aad7840f119f3876ee3569e488c7c4135f695fa

Transactions to the Crypto.com exchange:

Tx1 (205.999475 AVAX):
https://snowtrace.io/tx/0xba62ac56d65ba31faf25b60849ff1498e70ab649a9b87865555ea4b4df7d74a2
Tx2 (0.009475 AVAX):
https://snowtrace.io/tx/0x922ad8e43224a5eb3187056f4fc2d22d81112069cccc52bf053b3f410607c0d1
Tx3 (27.199475 AVAX):
https://snowtrace.io/tx/0x21d9b883473081b151c2c46f89b0d13081d3134903f364630be9e26d7e4e3d6d
Tx4 (18.499475 AVAX):
https://snowtrace.io/tx/0xd7153bde74ca21827e63975cb830a91531755be2eb90e16acc3ed50ac89d773d
Tx5 (124.918975 AVAX):
https://snowtrace.io/tx/0x42b5c532be3398c0f3c558724dbae333a2c91a5f766e6c687b010e065360d286
Tx6 (9.98814 AVAX):
https://snowtrace.io/tx/0xff67cf5add0c26f9abe551093a49a17cf2bcc2a5b0f2029b6cb9bd842d871712

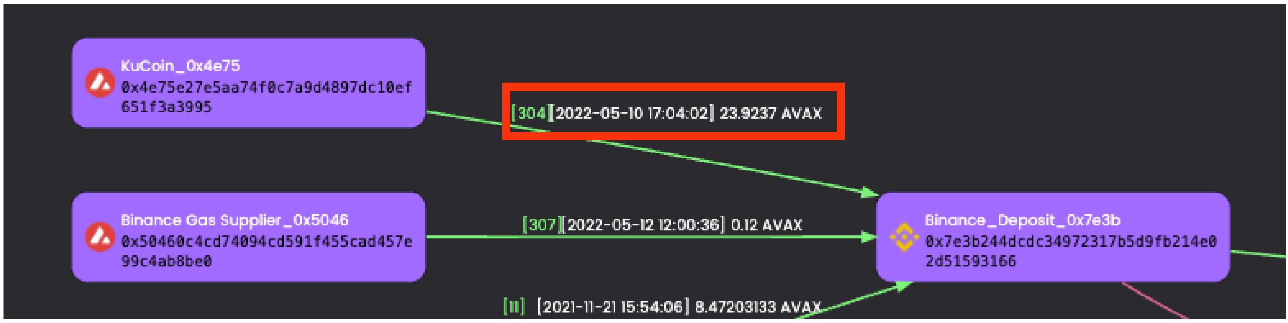

Attacker Wallet 4_0x4e5f
0x4e5f1bd7ec784b3da927f0d1d7baf004c2fc8d99
[368][2022-06-07 14:48:08] 124.9195 AVAX
CryptoCom DepositWallet_0x04...
0x04cd6b9579d8868ed46070a6fd33499f654c1b54
[369][2022-06-07 15:09:32] 386.6150149999997 AVAX
Crypto.Com Exchange_0x7aad
0x7aad7840f119f3876ee3569e488c7c4135f695fa

Binance Wallet to Feeder Wallet
Tx1 (0.16372196 AVAX):
https://snowtrace.io/tx/0xbb8c75e0fe6cc2eb889434918a76c165c95ee2e8695c6d099ce500050c74f7a4


Binance_Deposit_0x8af8
0x8af8485e1f178be06386cd3877fde2e626e0284f
[33] [2022-01-17 21:21:17] 0.18372196 AVAX
Alt. feed Cryptocom_0x65e7
0x65e75c95e74719f8fc6456587436f3625cc098a2
[6] [2021-11-19 10:43:56] 11.503190799999999 AVAX
[15] [2021-11-25 21:03:35] 1.29906453 AVAX
Tornado.Cash_0x330b
0x330bdfade01ee9bf63c209ee33102dd334618e0a
[367] [2022-06-07 14:28:09] 69.920655 AVAX
Attacker Wallet 4_0x4e5f
0x4e5f1bd7ec784b3da927f0d1d7baf004c2fc8d99
[368] [2022-06-07 14:48:08] 124.9195 AVAX
CryptoCom DepositWallet_0x04...
0x04cd6b9679d8858ed46078a6fd33499f654c1b54
[332] [2022-05-31 23:57:40] 0.01 AVAX

Binance Deposit Wallet -
https://snowtrace.io/address/0x7e3b244dcdc34972317b5d9fb214e02d51593166

Transaction from KuCoin to Binance Deposit Wallet
Tx1 (23.9237 AVAX):
https://snowtrace.io/tx/0x36a8eca38c3da010a6f0de4a00cecd19653d2b30108a1ccac23ea0a697fa5170


KuCoin_0x4e75
0x4e75e27e5aa74f0c7a9d4897dc10ef651f3a3995
[304] [2022-05-10 17:04:02] 23.9237 AVAX
Binance Gas Supplier_0x5046
0x50460c4cd74094cd591f455cad457e99c4ab8be0
[307] [2022-05-12 12:00:36] 0.12 AVAX
Binance_Deposit_0x7e3b
0x7e3b244dcdc34972317b5d9fb214e02d51593166
[11] [2021-11-21 15:54:06] 8.47203133 AVAX

Transactions from Binance Deposit Wallet to the Binance Hot Wallets *(NOTE: These happened in 2021 but are indirectly tied to the attacker wallet by other wallets with minimal transactions on them. These funds are not stolen from this victim)*
Tx1 (8.52023133 AVAX):
0xcc930ae2ca4e00abf16a5931983b5cc8b3f2eadd893dd280f5d93cfdbcb70af8
Tx2 (3.4994749 AVAX):
0x9b9af9f065f1262ba52ecde9fed8febf07a22fad60cf186e2b3af1084bb91eb7
Tx3 (2.3974749 AVAX):
0x8f5ba16da80bb5ae42e7493cc57acaf1c9408bd4ac34ef3852e30a820d966076
Tx4 (3.99827359 AVAX):
0xe8ef517f871493223d38c19d504d39586b3e7e5ebd5756ba954f5dfedc0c50f0
Tx5 (6.29829769 AVAX):
0x02aae72fb9cab5ba291a46e21158d29c44304be808bf3018bac1c498b9441778

Tx6 (62.62021984 AVAX):
0x53140951de1cbd1b3251d1cc3e17da53fc30c1acffed53a1cb690852d2c58e9a
Tx7 (23.92217286 AVAX):
0x6e786ba6ca08b3873fb6c751a4adaf0110939d13ea08b6e3ad07045a1aa97ee1

6. Contact Details

If you require further support from us, please contact us using the information below:

Twitter: https://twitter.com/Intell_on_Chain
Telegram: JP_IntelligenceOnChain
Discord: JP_IOC