



Smart contract blockchain analysis

Intelligence input

- The following cryptocurrency address has been identified as high risk in a SAR/STR: 0x861449915F34aF0848D082785FE406b0B9f367D2
- Find the context for the assessment of high risk
 - What criminality is the address linked with?
 - What cryptocurrency protocols/networks is the address present on?
 - Can you identify any other addresses linked to this criminality?



The screenshot shows the BscScan website interface. At the top, there's a search bar and navigation menu. The main content area displays the address `0x861449915f34af0848d082785fe406b0b9f367d2`. A warning banner states: "This address is reported to be involved in kidnapping case in Russia." Below this, there's an overview section showing a balance of 0 BNB and a value of \$0.00. A 'More Info' section indicates that the name tag is not available. At the bottom, a table of transactions is visible, with the first entry showing a transfer of 0.048225795 BNB to a 'Kidnapper 3' address.

Txn Hash	Method	Block	Date Time (UTC)	From	To	Value	[Txn Fee]
0x05ee7307bee580f09...	Transfer	16399392	2022-03-26 16:04:24	0x861449915f34af0848d...	Kidnapper 3	0.048225795 BNB	0.000105
0x0010e1419ed125926...	Transfer	16399378	2022-03-26 16:03:42	0x861449915f34af0848d...	BUSD-T Stablecoin	0 BNB	0.00018035
0xad18474e1763a4177...	Transfer	15104878	2022-02-09 12:27:04	0x861449915f34af0848d...	BUSD-T Stablecoin	0 BNB	0.00018035

<https://bscscan.com/address/0x861449915f34af0848d082785fe406b0b9f367d2#token txns>

https://twitter.com/mah_twittar/status/1444088020483952646

The screenshot shows a Twitter thread. The main tweet is from user @mah_twittar, posted on Oct 2, 2021, at 12:53 AM. The text of the tweet reads: "Hello everyone. You won't believe how happy I am that I can tell this. I must be dead but born again!". The tweet has 1,071 retweets, 455 quote tweets, and 4,410 likes. Below the main tweet, there are several replies. One reply from @mah_twittar says: "The thing I will mention may look gross and I sincerely regret for this but I was just kidnapped a few days ago and strangled to death." Another reply from @mah_twittar says: "I will add some details into this because the story about how I resurrected in that condition and came home is a story for a movie." A third reply from @mah_twittar says: "This is the look of my second birth. And the one of a man who sold the flat for \$80k in 2020 to get onboarded and ride it up to 0.5mil. I now have \$33k left for my second living but I am still happy that I was given to live this life." The thread also includes a profile picture of a man. On the right side of the screenshot, there are sections for 'Relevant people' (listing @mah_twittar), 'What's happening' (with news snippets about Finland-Russia border and Fortnite), and 'Trending' (with topics like Bellingham and Metro Lifestyle).

001 on Twitter: "Hello everyone. You won't believe how happy I am that I can tell this. I must be dead but born again!" / Twitter

Blockchain analysis

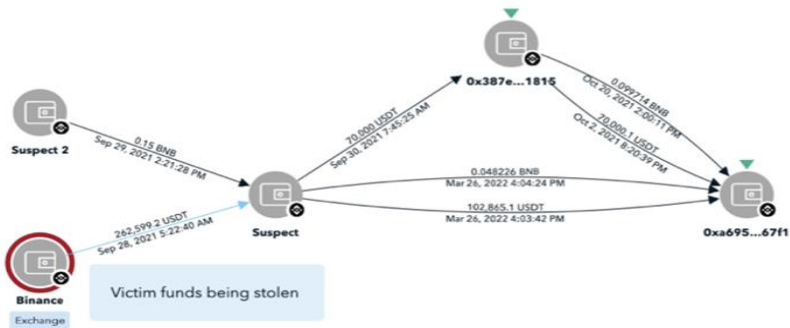
- Go to TRM and plot out the initial suspect address
- What immediate opportunities present themselves?
- What does this tell us in respect of the address outlined to focus on?
- From the transfers tab plot the transactions you believe are relevant



2022-09-22 12:41 0x86144...367d2 -DRAFT

Graph Library

Actions



Help



Last edit was a few seconds ago



July

August
04, 2021

September

October

November
04, 2021

December

January

February
01, 2022

March

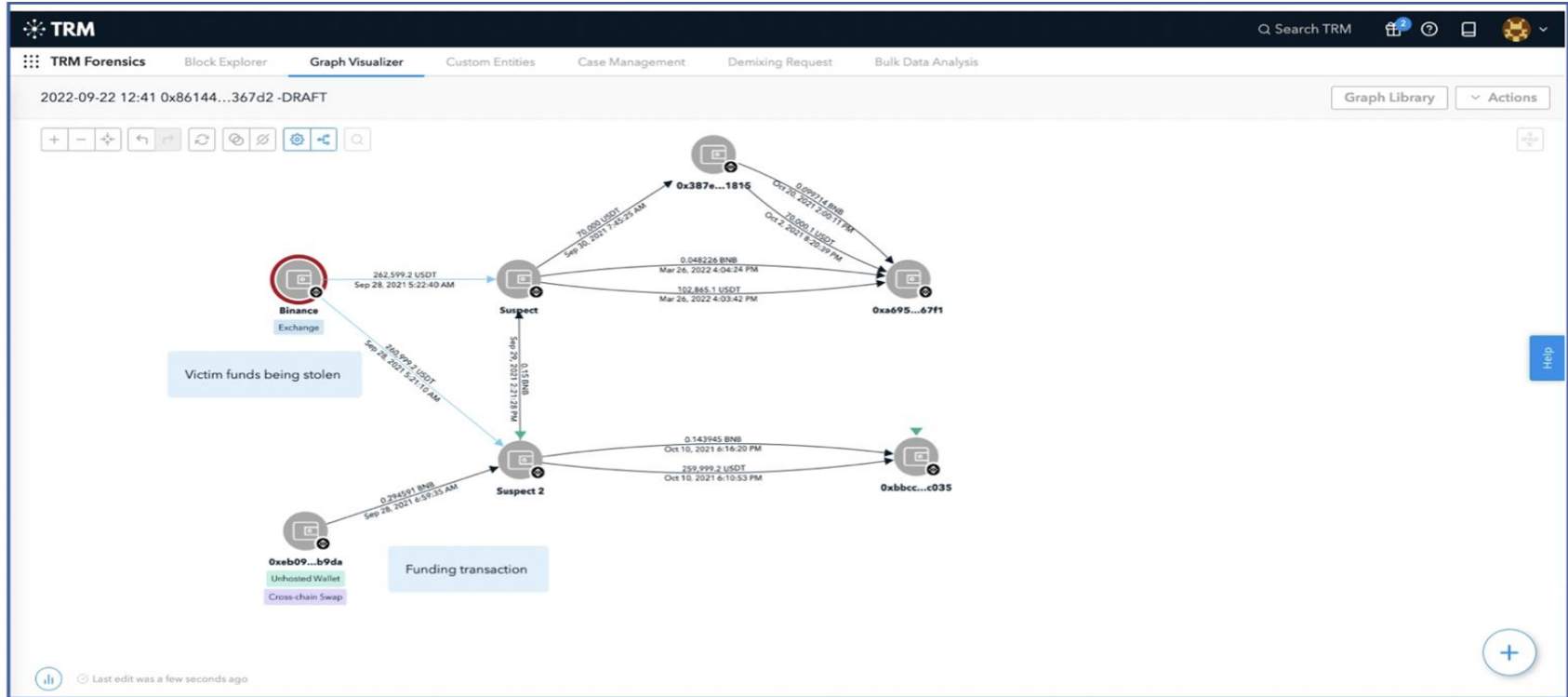
April


May
04, 2022

June

Blockchain analysis cont.

- Do the same for suspect address 2
- Why is the initial deposit of BNB worth reviewing?



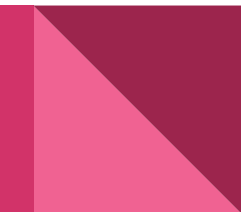
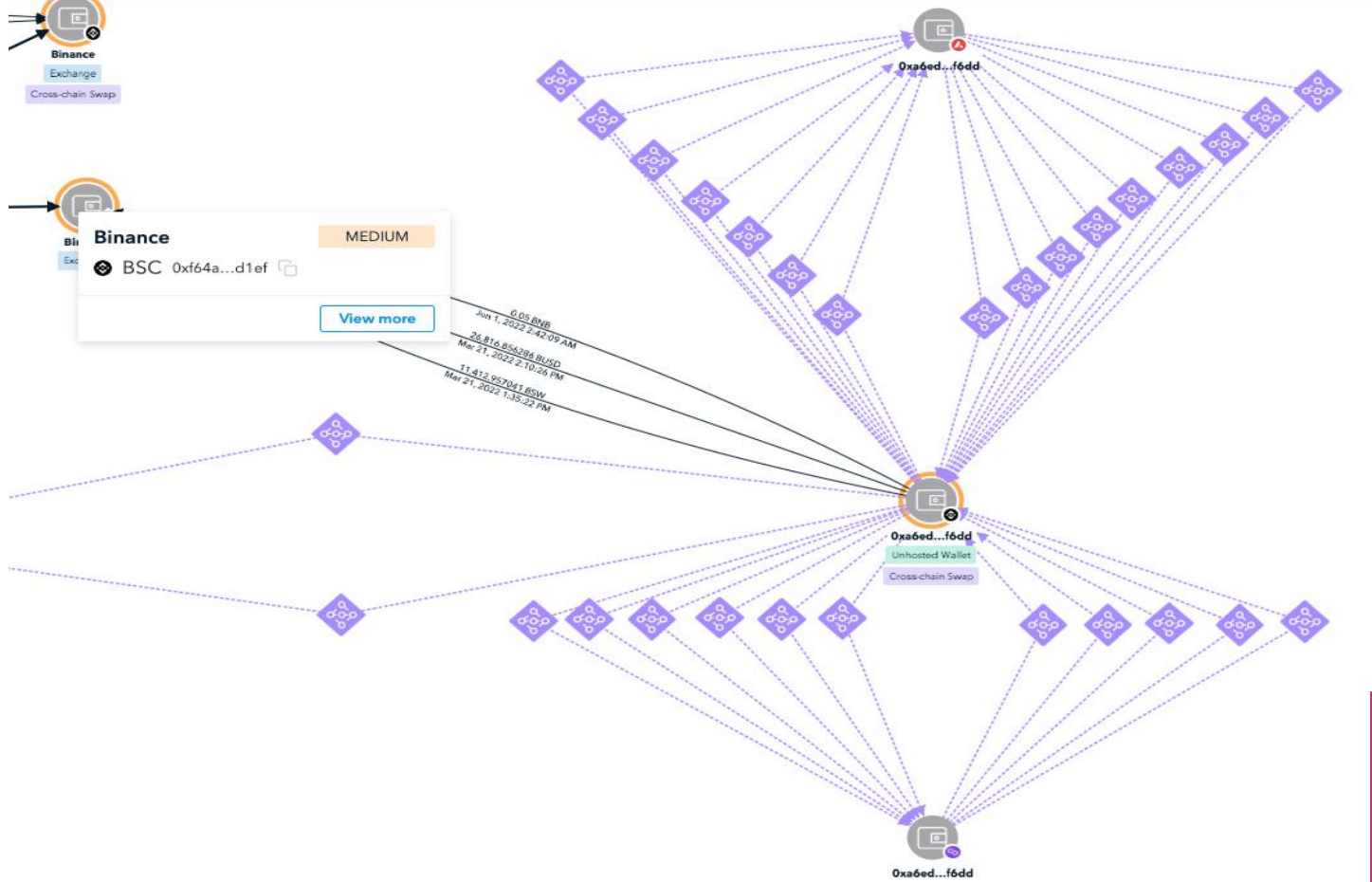
- Continue forward, what exchange are funds cashed out at?
 - Create a custom cluster for the addresses you believe are controlled by the suspect. Make sure you check which protocols the addresses have been active on.
 - 0xf64af01774ac8d0d0af933fc1fc1e0964531d1ef, would you consider any further tracing based on the incoming transactions detailed?
 - What further addresses would you add to your custom cluster?
- 


Binance
Exchange
Cross-chain Swap


Binance
Exchange

Binance MEDIUM
BSC 0xf64a...d1ef 
[View more](#)

6.05 BNB
Jun 1, 2022 2:42:09 AM
26,816,856,286 BUSD
Mar 21, 2022 2:10:26 PM
11,212,957,041 BSW
Mar 21, 2022 1:35:22 PM



Blockchain analysis cont.

- Search for and click on 0xa6ed50d06c420a3c540f9e4955772600f7c3f6dd in bscscan.com. Navigate to ERC-721 and review the NFT transactions. What NFT's are involved in these TX's?
 - Plot the address in TRM and map out some of the NFT transactions. What do you notice?
 - Now click on the Cross-chain Swap detail
 - Plot these transactions, what bridges are used by the entity? What protocols does the entity transact on?
 - On BSC protocol follow the most significant counterparty in respect of outgoing volume. Which exchange is used to cash out these funds?
 - On Polygon there is a transaction involving the Hop protocol, search for the address 0x76b22b8c1079a44f1211d867d68b1eda76a635a7 in counterparties. This is an address linked to the Hop Protocol. What do you notice?
 - Navigate to <https://explorer.hop.exchange/> and use the filters to search for 0xa6ed50d06c420a3c540f9e4955772600f7c3f6dd. See which of these transactions you can plot in TRM. What do you find?
 - On ETH the entity engages with Thorswap, what BNB address is associated with this? Search for the transactions on Etherscan and scroll "More details". Click to see more and then choose decode.
 - Plot the BNB address in TRM and identify any exchanges funds are sent to.
- 