United States District Court

NORTHERN DISTRICT OF GEORGIA

UNITED STATES OF AMERICA

v.

ROMAN VITALYEVICH OSTAPENKO

CRIMINAL COMPLAINT
Case Number: 1:24-MJ-0961

UNDER SEAL

(HSD)

HSD

I, the undersigned complainant being duly sworn, state the following is true and correct to the best of my knowledge and belief.

1. Beginning on or about October 18, 2018, and continuing until on or about November 27, 2023, in the Northern District of Georgia and elsewhere, the defendant, ROMAN VITALYEVICH OSTAPENKO, did knowingly combine, conspire, confederate, agree, and have a tacit understanding with others known and unknown to commit an offense against the United States in violation of Title 18, United States Code, Section 1956, that is:

   a. to knowingly conduct and attempt to conduct financial transactions affecting interstate commerce and foreign commerce, which transactions involved the proceeds of specified unlawful activities—that is, wire fraud, in violation of Title 18, United States Code Section 1343, illegal transactions with an access device, in violation of Title 18, United States Code 1029(a)(5), intentional damage to a protected computer, in violation of Title 18, United States Code, Section 1030(a)(5)(A), and extortion by threatening to obtain information from a protected computer and by demanding money and other thing of value in relation to damage to a protected computer, in violation of Title 18, United States Code, Sections 1030(a)(7)(B) and (a)(7)(C)— knowing that the transactions were designed in whole and in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of said specified unlawful activities, and that while conducting and attempting to conduct such financial transactions, knew that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i).

The manner and means used to accomplish the objectives of the conspiracy included, among others, the following: defendant OSTAPENKO and others known and unknown operated, promoted, and used Blender.io and Sinbad.io virtual currency mixing services for Bitcoin on the internet. The virtual currency mixing services were accessible to users across the world, including users located in the Northern District of Georgia, via the internet. The virtual currency mixing services were used to launder funds obtained through ransomware, virtual currency theft, and other crimes.

All in violation of Title 18, United States Code, Section 1956(h).

2. Beginning on or about October 18, 2018, and continuing until on or about April 2022, in the Northern District of Georgia and elsewhere, the defendant, ROMAN VITALYEVICH OSTAPENKO, aided and abetted by others known and unknown, knowingly conducted, controlled, managed, supervised, directed, and owned all and part of an unlicensed money transmitting business affecting interstate and foreign commerce, to wit, Blender.io, while failing to comply with the money transmitting business registration requirements under Section 5330 of Title 31, United States Code, and regulations prescribed under such section, and otherwise involving the transportation and transmission of funds that defendant OSTAPENKO, and others known and unknown, knew to have been derived from a criminal offense and intended to be used to promote and support unlawful activity, to wit, defendant OSTAPENKO, and others known and unknown, used Blender.io to transmit millions of dollars by means of virtual currency transactions, including funds known to defendant OSTAPENKO, and others known and unknown, to have been derived from a criminal offense and intended to be used to promote and support unlawful activity, without registering Blender.io as a money transmitting business under federal law, in violation of Title 18, United States Code, Section 1960 and Section 2.

3. Beginning on or about October 13, 2022, and continuing until on or about November 27, 2023, in the Northern District of Georgia and elsewhere, the defendant, ROMAN VITALYEVICH OSTAPENKO, aided and abetted by others unknown, knowingly conducted, controlled, managed, supervised, directed, and owned all and part of an unlicensed money transmitting business affecting interstate and foreign commerce, to wit, Sinbad.io, while failing to comply with the money transmitting business registration requirements under Section 5330 of Title 31, United States Code, and regulations prescribed under such section, and otherwise involving the transportation and transmission of funds that defendant OSTAPENKO, and others unknown, knew to have been derived from a criminal offense and intended to be used to promote and support unlawful activity, to wit, the defendant OSTAPENKO, and others unknown, used Sinbad.io to transmit millions of dollars by means of virtual currency transactions, including funds known to defendant OSTAPENKO and others unknown to have been derived from a criminal offense and intended to be used to promote and support unlawful activity, without registering Sinbad.io as a money transmitting business under federal law, in violation of Title 18, United States Code, Section 1960 and Section 2.

I further state that I am a(n) FBI Special Agent and that this complaint is based on the following facts:

PLEASE SEE ATTACHED AFFIDAVIT

Continued on the attached sheet and made a part hereof. Yes

Signature of Complainant
Jacob T. Smart

Based upon this complaint, this Court finds that there is probable cause to believe that an offense has been committed and that the defendant has committed it. Sworn to before me, and subscribed in my presence

November 1, 2024 at Atlanta, Georgia
Date City and State

LINDA T. WALKER
UNITED STATES MAGISTRATE JUDGE Linda T. Walker
Name and Title of Judicial Officer Signature of Judicial Officer
AUSA S. Kaushal

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Jacob Smart, hereby depose and state as follows under penalty of perjury:

INTRODUCTION

1. The FBI is investigating the operators of the Blender.io and Sinbad.io virtual currency mixing services, which offered money laundering services, including to criminals, across the world. The operators of these services include ROMAN VITALYEVICH OSTAPENKO (OSTAPENKO) and others.

2. I make this affidavit in support of a criminal complaint for ROMAN VITALYEVICH OSTAPENKO for his role in conspiring to operate of Blender.io and Sinbad.io. Blender.io was publicly accessible from on or about October 18, 2018 until on or about April 2022, and Sinbad.io was publicly accessible from on or about October 13, 2022 until on or about November 27, 2023. . Ostapenko conspired with others to knowingly conduct financial transaction through Blender.io and Sinbad.io involving proceeds of specified unlawful activities—including wire fraud (18 U.S.C. § 1343) (see paragraphs 61-63, *infra*), illegal transactions with an access device (18 U.S.C. § 1029(a)(5)) (same), intentional damage to a protected computer (18 U.S.C. § 1030(a)(5)(A) (see paragraphs 58-60, *infra*), and extortion by threatening to obtain information from a protected computer and by demanding money or other things of value in relation to damage to a protected computer (18 U.S.C. §§ 1030(a)(7)(B), (a)(7)(C)) (same)—knowing that the transactions were designed in whole and in part to conceal and disguise the nature, location, ownership, and control of the proceeds of said specified unlawful activities, and that while conducting those transactions, knowing that the property involved in the transactions represented the proceeds of some form of unlawful

activity (in violation of 18 U.S.C. § 1956(a)(1)(B)(i)). Additionally, Ostapenko, aided and abetted by others, operated Blender.io and Sinbad.io to transmit millions of dollars by means of virtual currency transactions without registering either virtual currency mixing service under federal law. Based on my training and experience and the facts set forth in this Affidavit, there is probable cause to believe that OSTAPENKO has violated Title 18, United States Code, Sections 1956(h) (money laundering conspiracy) by conspiring to operate Blender.io and Sinbad.io, and twice violated Title 18, United States Code, Section 1960 (unlicensed money transmitting business), for his operation of Blender.io and Sinbad.io., respectively.

AGENT BACKGROUND

3. I am a Special Agent of the Federal Bureau of Investigation ("FBI") and have been since April 11, 2021. As a Special Agent, I received extensive training on investigation of violations of federal statutes and I have conducted numerous federal investigations. In many of those investigations, I have gathered facts necessary for probable cause for search, seizure, and arrest warrants, and I have executed numerous warrants in my tenure. I have received advanced training in computer investigations, digital forensics, and cybersecurity principles. I also have extensive experience and training in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of search warrants, and various other criminal laws and procedures.

4. The facts and information contained in this Affidavit are based upon my personal knowledge of the investigation, information conveyed to me by other U.S. government employees, and my personal review of records, documents, and other

physical evidence obtained during this investigation. This Affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

TECHNICAL TERMS

5. From my training and experience investigating virtual currency transactions and crimes involving the use of virtual currency, I know the following:

a. Virtual Currency: Virtual currencies are digital representations of value that, like traditional coin and paper currency, function as a medium of exchange (i.e., they can be digitally traded or transferred, and can be used for payment or investment purposes). Virtual currencies are a type of digital asset separate and distinct from digital representations of traditional currencies, securities, and other traditional financial assets. The exchange value of a particular virtual currency generally is based on agreement or trust among its community of users. Some virtual currencies have equivalent values in real currency or can act as a substitute for real currency, while others are specific to particular virtual domains (e.g., online gaming communities) and generally cannot be exchanged for real currency. Cryptocurrencies, like Bitcoin and Ether, are types of virtual currencies, which rely on cryptography for security. Cryptocurrencies typically lack a central administrator to issue the currency and maintain payment ledgers. Instead, cryptocurrencies use algorithms, a distributed ledger known as a blockchain, and a network of peer-to-peer users to maintain an accurate system of payments and receipts.

b. Virtual Currency Address: A virtual currency address is an alphanumeric string that designates the virtual location on a blockchain where virtual currency can be sent and received. A virtual currency address is associated with a virtual currency wallet.

c. Blockchain: A blockchain is a digital ledger run by a decentralized network of computers referred to as "nodes." Each node runs software that maintains an immutable and historical record of every transaction utilizing that blockchain's technology. Many digital assets, including virtual currencies, publicly record all of their transactions on a blockchain, including all of the known balances for each virtual currency address on the blockchain. Blockchains consist of blocks of cryptographically signed transactions, and blocks are added to the previous block after validation and after undergoing a consensus decision to expose and resist tampering or manipulation of the data. There are many different blockchains used by many different virtual currencies. For example, Bitcoin in its native state exists on the Bitcoin blockchain, while Ether (or "ETH") exists in its native state on the Ethereum network.

d. Cluster: A cluster is a collection or grouping of virtual currency addresses identified through blockchain analysis as being controlled by a common user or entity.

e. Private Key: A private key is a cryptographic key that is uniquely associated with an entity and not made public. In the blockchain and virtual currency context, virtual currency addresses are controlled using a unique corresponding private key, the equivalent of a password, which is needed to access the funds associated with the address. Only the holder of an address's private key can authorize a transfer of virtual currency from that address to another address.

f. Virtual Currency Exchanges: A virtual currency exchange ("VCE"), also called a cryptocurrency exchange, is a platform used to buy and sell virtual currencies. VCEs allow users to exchange their virtual currency for other virtual currencies or fiat currency, and vice versa. Many VCEs also store their customers' virtual currency addresses in hosted wallets. VCEs can be centralized (i.e., an entity or organization that facilitates virtual currency trading between parties on a large scale and often resembles traditional asset exchanges like stock exchanges) or decentralized (i.e., a peer-to-peer marketplace where transactions occur directly between parties).

g. Virtual Currency Wallet: A virtual currency wallet (e.g., a hardware wallet, software wallet, or paper wallet) stores a user's public and private keys, allowing a user to send and receive virtual currency stored on the blockchain. Multiple virtual currency addresses can be controlled by one wallet. A hardware wallet is a physical, removable device that stores a user's private keys and can be connected to a computer when a user wishes to use the keys stored on the wallet for virtual currency transactions. Hardware wallets can be secured with PIN codes and passphrases and can be backed up or regenerated with a recovery phrase. Trezor and Ledger are some examples of the types of hardware wallets on the market. A hosted wallet, also known as a custodial wallet, is a virtual currency wallet through which a third party, e.g., a virtual currency exchange, holds a user's private keys. The third party maintains the hosted wallet on its platform akin to how a bank maintains a bank account for a customer, allowing the customer to authorize virtual currency transactions involving the hosted wallet only by logging into/engaging with the third party's platform.

h. Virtual Currency Mixers: Virtual currency mixers (also known as tumblers or mixing services) are services that allow users, for a fee, to send virtual currency to designated recipients in a manner designed to conceal and obfuscate the source of the virtual currency. These services are sometimes used by state-sponsored and criminal actors as a money laundering tool.

i. Stablecoins: Stablecoins are a type of virtual currency whose value is pegged to a commodity's price, such as gold, or to a fiat currency, such as the U.S. dollar, or to a different virtual currency. For example, USDT is a stablecoin pegged to the U.S. dollar. Stablecoins achieve their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives.

j. Peel Chains: A peel chain occurs when virtual currency sitting at one address is sent through a series of transactions in which a slightly smaller amount of virtual currency is transferred to a new address each time. In each transaction, some quantity of virtual currency "peels off" the chain to another address (frequently, to be deposited into a virtual currency exchange), and the remaining balance is transferred to the next address in the peel chain. Intermediate addresses are often part of a single wallet and are created automatically to receive the leftover change that results from certain transactions. Peel chains are often used as a technique to launder large amounts of virtual currency.

k. Blockchain Analysis: Law enforcement can trace transactions on blockchains to determine which virtual currency addresses are sending and receiving particular virtual currency. This analysis can be invaluable to criminal investigations for many reasons, including that it may enable law enforcement to uncover transactions involving illicit funds and to identify the person(s) behind those transactions. To conduct blockchain analysis, law enforcement officers use reputable, free, open-source blockchain explorers, as well as commercial tools and services. These commercial tools are offered by different blockchain-analysis companies. Through numerous unrelated investigations, law enforcement has found the information associated with these tools to be reliable.

l. Blockchain Bridge: A bridge protocol, also known as a cross-chain bridge, is a software application that enables the direct transfer of assets/value across different blockchains (e.g., from the Bitcoin blockchain to the Ethereum network). When a bridge protocol user initiates a transaction from one blockchain to another, the user specifies the number of coins or tokens (i.e., the value) that the user would like to send from the originating blockchain to the destination blockchain. There are typically two ways that bridge protocols accomplish this transfer of value. The first way is through "locking" and then "releasing" coins or tokens. If a user is dealing with a lock-and-release style bridge protocol, then the bridge will lock (or hold) coins/tokens on the originating blockchain. Once those coins/tokens are locked, the bridge protocol will release from its liquidity pool coins/tokens of an equivalent value on the destination blockchain. If a user would like to go back from the destination blockchain to the originating blockchain, then the bridge protocol will use the same lock and release mechanism. The second way is through "locking" and "minting/burning" coins or tokens.

If a user is dealing with a lock-and-mint/burn style bridge protocol, then the bridge will lock coins/tokens on the originating blockchain and then mint (or create) coins/tokens of an equivalent value on the destination blockchain. If a user would like to go back from the destination blockchain to the originating blockchain, then the bridge protocol will burn (or destroy) the representative coins/tokens on the destination chain and release the initial value back to the user on the originating blockchain. Bridge protocols are either unidirectional (i.e., only allow for the transfer of value to specific blockchains) or are bidirectional (i.e., allow for the transfer of value back and forth across blockchains).

PROBABLE CAUSE

Overview

6. The FBI is investigating the operators of the Blender.io and Sinbad.io virtual currency mixing services, which offered money laundering services, including to criminals, all over the world. Based on the evidence collected and information analyzed as part of the FBI's investigation, the operators of these services include OSTAPENKO and others. This affidavit covers the following matters:

a. Paragraphs 8 through 19 describe the virtual currency mixer services Blender.io and Sinbad.io, explain what a virtual currency mixer service is, and outline the evidence that shows that Sinbad.io was a continuation of Blender.io that began operation after Blender.io ceased operation in April 2022. Aside from similarities in appearance and operation, the FBI determined that Bitcoin from Blender.io was transferred from a Bitcoin cluster associated with Blender.io to Sinbad.io.

b. Paragraphs 20 through 23 describe efforts of Blender.io's operators to advertise the service on internet forums discussing virtual currency, including its concealment and obfuscation functions.

c. Paragraphs 24 through 27 describe some of Ostapenko's role in advertising Blender.io and assisting in funding Sinbad.io. Specifically, the FBI believes that Ostapenko or a co-conspirator, using the alias "rn3rd," paid for advertising for Blender.io's non-custodial virtual currency wallet application, Blenderwallet,io, and moved virtual currency from a virtual currency address he controlled to a virtual currency address that was used to facilitate the transfer of funds from Blender.io to Sinbad.io after Blender.io ceased operation and to purchase the domain name "Sinbad.io".

d. Paragraphs 28 through 44 describe Ostapenko's connection to the Russian company Smart Code Group, his status as the CEO of that company, and Smart Code Group's role as the suspected developers of Blender.io (based on evidence of the existence of references to a source code repository for Smart Code Group that was found on a Blender.io server). These paragraphs also describe how network infrastructure (and payments for the infrastructure) show that the individuals that purchased and maintained network infrastructure used to operate Sinbad.io are the same individuals that developed and maintained source code for Blender.io.

e. Paragraphs 45 through 53 explain the financial connection between virtual currency accounts for rn3rd, cyberbiber, and asaventura; the FBI's belief that the cyberbiber and asaventura virtual currency accounts belong to

Ostapenko; and the financial connection between the virtual currency account for asaventura and the Blender.io mixing service.

f. Paragraph 54 describes a bitcoin transaction identified through review of data produced pursuant to a search warrant for Ostapenko's email accounts, revealing a "test mixer" transaction on or about 12 days before Blender.io was publicly advertised.

g. Paragraphs 55 through 57 explain how funds flowed from Blender.io to Sinbad.io after Blender.io ceased operations, and how some of these funds also went to a virtual currency address believed to be controlled by Ostapenko.

h. Paragraphs 58 through 64 describe how Blender.io and Sinbad.io were used to launder criminal proceeds, including proceeds that were stolen or fraudulently obtained from victims located in the Northern District of Georgia.

i. Paragraphs 65 through 71 explain how Blender.io and Sinbad.io acted as unlicensed money transmitting businesses.

j. Paragraphs 72 and 73 describe how Sinbad.io ceased operations and was sanctioned by OFAC in November 2023.

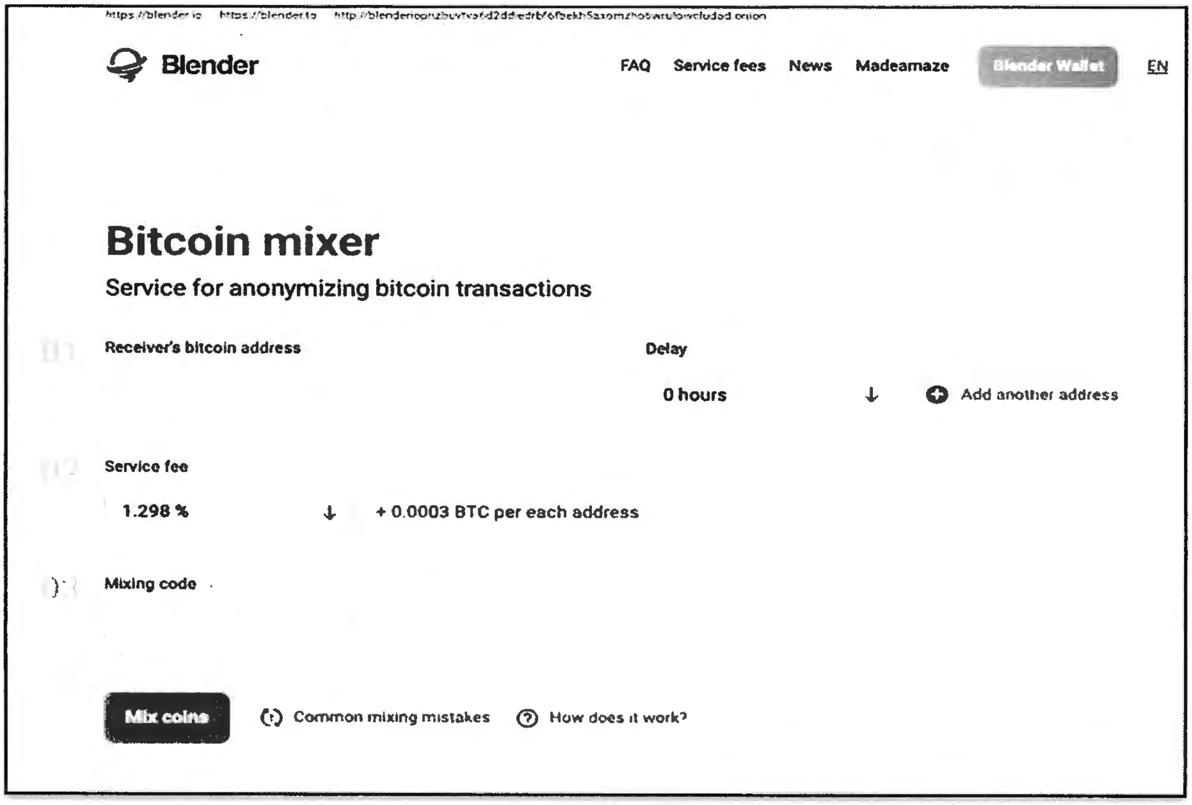
7. Based on the information presented in this affidavit, I believe that Ostapenko and his co-conspirators operate businesses entities, such as the Smart Code Group, that create source code to support the operation of virtual currency mixers that launder criminal proceeds.

A. Similarities and Connections Between Blender.io and Sinbad.io

8. Blender.io was a virtual currency mixing service that operated from at least October 18, 2018, until at least April 2022. According to the U.S. Treasury Department, over $500 million worth of virtual currency moved through the service. On May 6, 2022, the Treasury Department's Office of Foreign Assets Control ("OFAC") sanctioned Blender.io, citing its use by the Democratic People's Republic of Korea ("DPRK") to support malicious cyber activities and money-laundering of stolen virtual currency.[1]

9. The Blender.io website is no longer in operation; however, a portion of the website was captured by Archive.org, a non-profit, public digital library that automatically collects information on public websites using web crawlers. An FBI special agent accessed Archive.org to view an image of Blender.io's website that was captured on March 27, 2022. Below is a portion of that image:

[1] *See* "U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats," https://home.treasury.gov/news/press-releases/jy0768.



https://blender.io https://blender.to http://blenderioonzbuvtva6d2ddedrb6fbekh5axomzhotwrufowcluded.onion

Blender

FAQ Service fees News Madeamaze Blender Wallet EN

Bitcoin mixer

Service for anonymizing bitcoin transactions

Receiver's bitcoin address

Delay

0 hours

Add another address

Service fee

1.298 %

+ 0.0003 BTC per each address

Mixing code

Mix coins

Common mixing mistakes

How does it work?

10. Open-source websites, as well as Blender.io's advertisements on Bitcointalk.org, an online Bitcoin forum, describe the service. Based on my review of the open-source information, I understand that the service was designed to allow users to send the virtual currency Bitcoin (BTC) to the service, that Blender.io held the Bitcoin for a period of time designated by the user, and Blender.io then sent the Bitcoin at unpredictable intervals to up to eight new virtual currency wallet addresses. The time between transfers, the ratio of the amount transferred to each destination, and the number of destination virtual currency wallets served to obfuscate the linkage between the source and destination wallets. Blender.io received a fee for transferring the Bitcoin.

11. Blender.io ceased operations in or about April 2022. The virtual currency mixing service Sinbad.io began operating in or about October 2022. A blockchain

analytics company published analysis in which they indicate Sinbad.io is a rebranding of Blender.io.[2] The company's assessment noted the following to support its conclusion:

a. Prior to Sinbad.io's public launch, a service address on the Sinbad.io website received Bitcoin from a wallet believed to be controlled by the operator of Blender.io;

b. Blockchain analysis shows a wallet used to pay individuals who promoted Sinbad.io received funds from a suspected Blender.io wallet;

c. Blockchain analysis of early incoming transactions to Sinbad.io that originated from a suspected Blender.io wallet; and

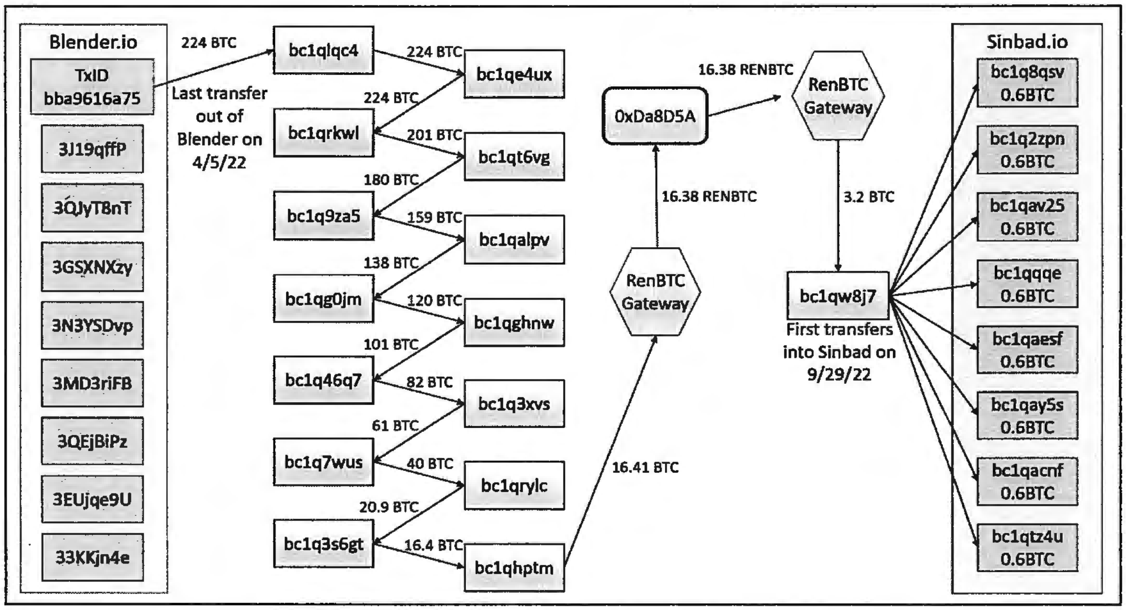
d. Similarities between Blender.io and Sinbad.io functionality, transaction delay, guarantee letters, website similarities, languages supported, and naming conventions.

12. FBI blockchain analysis identified a cluster attributed to Sinbad.io that received transfers on or about September 29, 2022, originating from a cluster that was attributed to Blender.io and contained several virtual currency addresses that were sanctioned by OFAC. The following diagram shows the flow of Bitcoin from a cluster attributed to Blender.io to a cluster attributed to Sinbad.io.[3] The virtual currency address beginning with 0xDa8D5A, which transferred funds from and back through the RenBTC

[2] *See, e.g.*, "Has a Sanctioned Bitcoin Mixer Been Resurrected to Aid North Korea's Lazarus Group?," https://hub.elliptic.co/analysis/has-a-sanctioned-bitcoin-mixer-been-resurrected-to-aid-north-korea-s-lazarus-group/.

[3] The tracing diagrams in this affidavit list the first eight characters of the identified addresses and the first several characters of transaction IDs ("TxIDs").

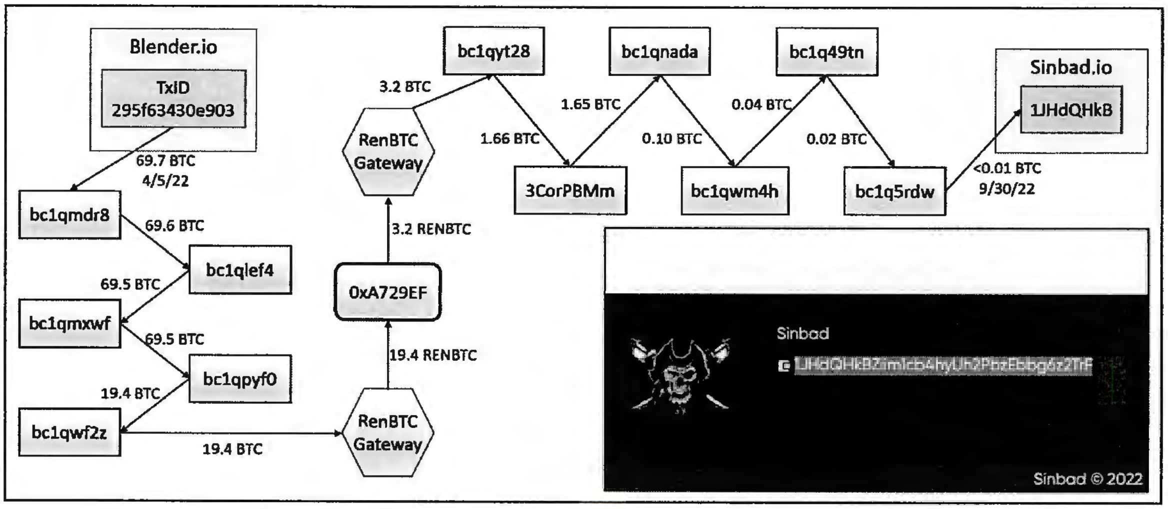
Gateway, received its initial funds from a virtual currency address believed to be controlled by Blender.io and Sinbad.io's operator(s).



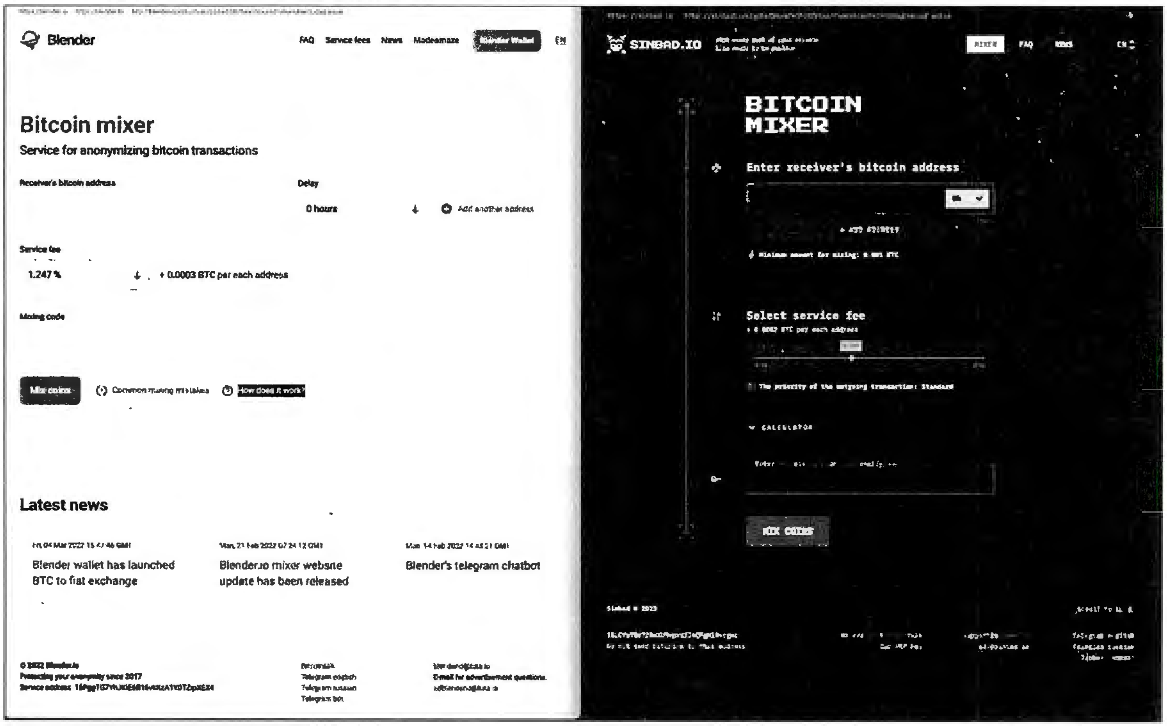
The transfer out of Blender.io on or about April 5, 2022, illustrated above, occurred the same day that the user "blenderio" posted a message to Bitcointalk.org stating that Blender.io was closed for maintenance and maintenance completion would be announced at a later date. The transferred funds moved through a peel chain," and then passed through the RenBridge (a blockchain bridge), which converted the funds from the Bitcoin blockchain to virtual currency on the Ethereum blockchain. Within hours, the funds were passed back through the RenBridge, to convert an equivalent amount of funds back to BTC on the Bitcoin blockchain. Based on my training and experience, I believe that this cross-blockchain transfer was likely made to obfuscate the origin of the funds because the conversion from BTC to the Ethereum blockchain back to BTC seemingly served no legitimate financial purpose (and resulted in a loss of the conversion fees).

13. As shown in the diagram below, the service address listed at the bottom of a November 6, 2022, version of the Sinbad.io website (obtained through Archive.org)

received funds from a virtual currency address attributed to Blender.io. The funds were received by the Sinbad.io service address prior to public announcements of the Sinbad.io service's existence.



14. Side-by-side images of the Blender.io and Sinbad.io websites are shown below.



Bitcoin mixer

Service for anonymizing bitcoin transactions

Receiver's bitcoin address

Delay

0 hours

Service fee

1.247 %

+ 0.0003 BTC per each address

Mixing code

Latest news

Fri, 04 Mar 2022 15:47:46 GMT

Blender wallet has launched BTC to fiat exchange

Mon, 21 Feb 2022 07:24:12 GMT

Blender.io mixer website update has been released

Mon, 14 Feb 2022 14:45:21 GMT

Blender's telegram chatbot

© 2022 Blender.io

Protecting your anonymity since 2017

Enter receiver's bitcoin address

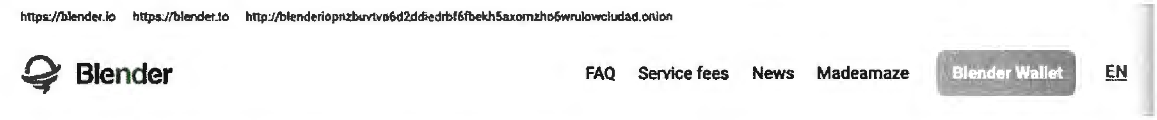
Select service fee

The priority of the outgoing transaction: Standard

15. A comparison of the two websites revealed several similarities in content and functionality:

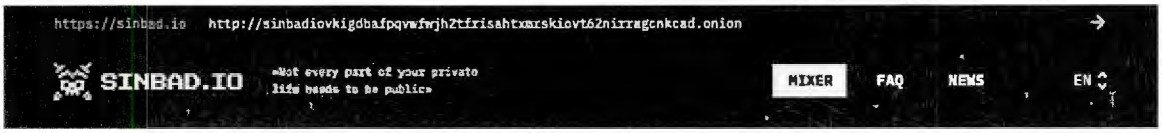
a. In the top banner, each site contains the name of the mixer, FAQ and NEWS hyperlinks, and a drop-down menu to allow for selection of English or Russian language. The banners also both contain the clearnet (a website that can be accessed through the public internet) and the Onion Routing ("Tor") website addresses (websites that can be accessed through using a Tor browser).[4]

[4] Tor, short for The Onion Router, is free and open-source software for enabling anonymous communication. It directs Internet traffic via a free, worldwide, volunteer



https://blender.io https://blender.to http://blenderiopnzbuvtva6d2ddiedrbf6fbekh5axomzho6wrulowcludad.onion

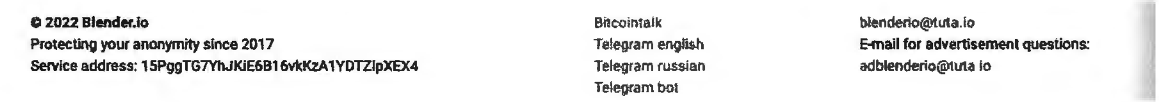
Blender FAQ Service fees News Madeamaze Blender Wallet EN



https://sinbad.io http://sinbadiovkigdbafpqvwfwjh2tfrisahtxmrskiovt62nirragcnkcad.onion

SINBAD.IO «Not every part of your private life needs to be public» MIXER FAQ NEWS EN

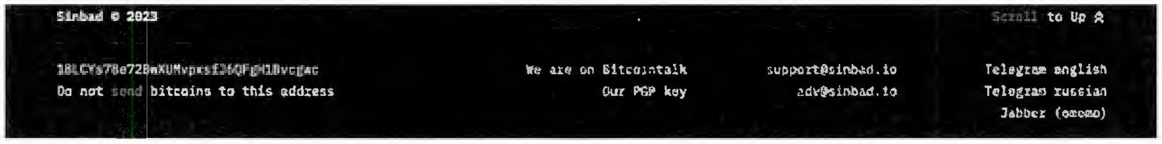
b. The footer of both websites contains a copyright marking, a service bitcoin address, a hyperlink to Bitcointalk.org, contact emails for the administrator/advertiser of the sites, and hyperlinks to Russian and English Telegram channels:



© 2022 Blender.io
Protecting your anonymity since 2017
Service address: 15PggTG7YhJKiE6B16vkKzA1YDTZlpXEX4

Bitcointalk
Telegram english
Telegram russian
Telegram bot

blenderio@tuta.io
E-mail for advertisement questions:
adblenderio@tuta io



Sinbad © 2023

18LCYs78e728wXUMvpxsfJ6QFgM1Bvcgac
Do not send bitcoins to this address

We are on Bitcointalk
Our PGP key

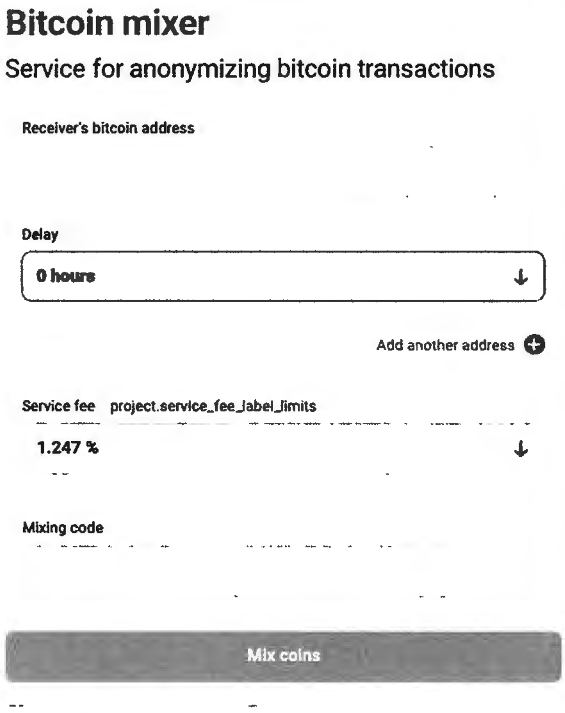
support@sinbad.io
adv@sinbad.io

Telegram english
Telegram russian
Jabber (omemo)

Scroll to Up

c. The layout of the user interaction fields is similar. Both websites have a field for "receiver's bitcoin address," a service fee selection option, and a mixing code field, which are similarly aligned from top to bottom in the same order. The receiver's Bitcoin address field has the option to add additional Bitcoin addresses:

overlay network that consists of more than seven thousand relays. Using Tor makes it more difficult to trace a user's Internet activity.



Bitcoin mixer

Service for anonymizing bitcoin transactions

Receiver's bitcoin address

Delay

0 hours

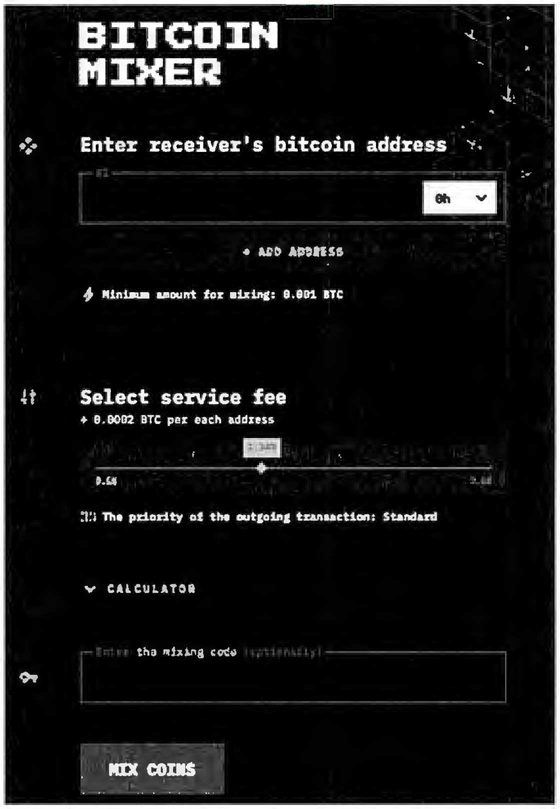
Add another address

Service fee project.service_fee_label_limits

1.247 %

Mixing code

Mix coins



BITCOIN MIXER

Enter receiver's bitcoin address

0h

+ ADD ADDRESS

Minimum amount for mixing: 0.001 BTC

Select service fee

+ 0.0002 BTC per each address

0.5%

The priority of the outgoing transaction: Standard

CALCULATOR

Enter the mixing code (optionally)

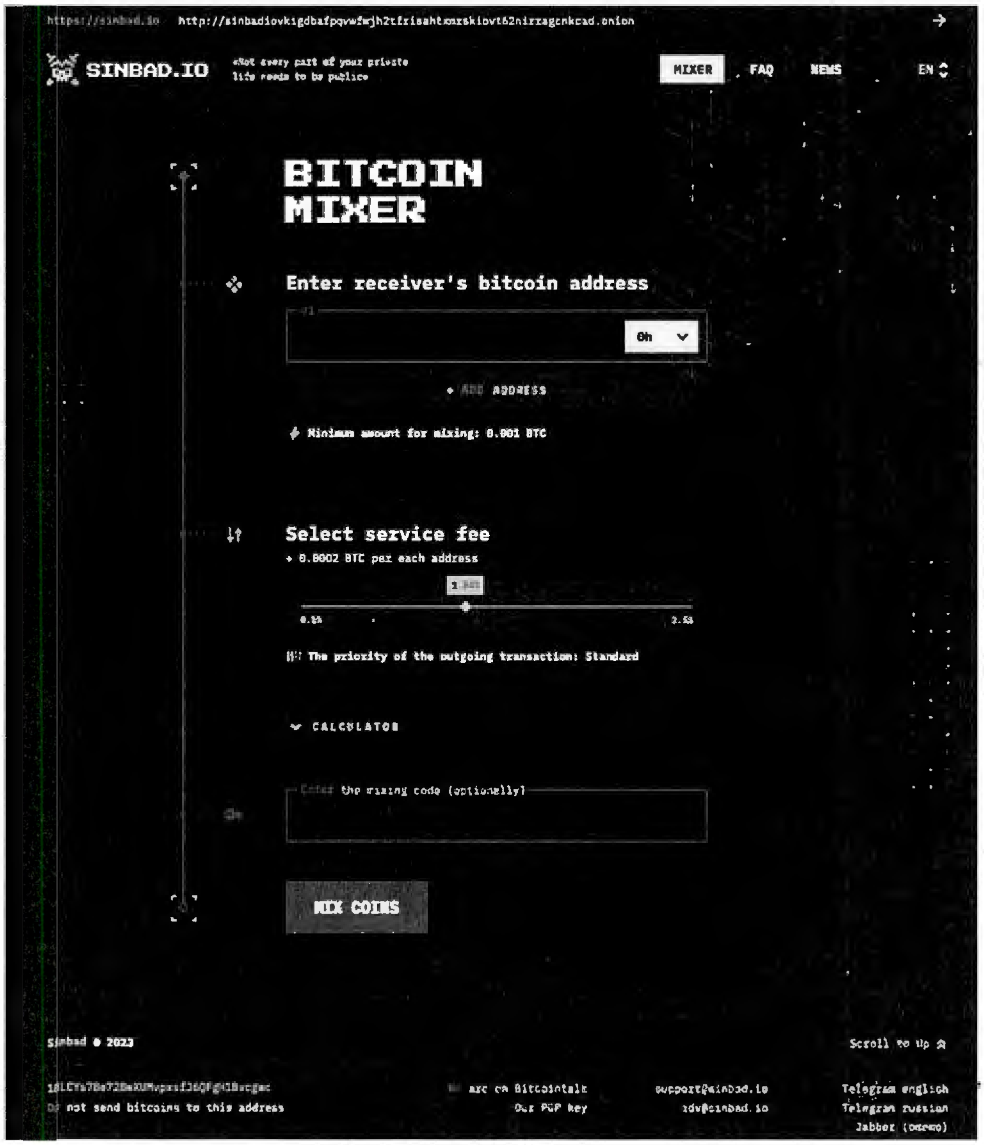
MIX COINS

d. Both websites allow the user to select a time range up to a maximum of seven days. The user can also select the user fee. According to the Sinbad.io site, the user fee paid determines the priority of outgoing transaction ranging from 0.5% (slow) to 2.5% (fast). Although I am unable to confirm the number of destination addresses Blender.io supported by viewing the option on the site, open-source research indicates that Blender.io supported eight output addresses when it was in operation, which is the same number of output addresses supported by Sinbad.io.[5]

[5] *See, e.g.*, "Blender Review – Is It Legit or Scam?," https://deepweblinks.live/blender-review/.

e. Both websites indicate a letter of guarantee is issued, and in both cases a letter of guarantee may be downloaded by the user. Open-source information on Blender.io obtained from https://deepweblinks.live/blender-review contained an image of the website that showed a download link. In the case of Sinbad.io, the instructions advise the user to download the guarantee letter.

16. On October 27, 2023, an FBI special agent navigated to the Sinbad.io clearnet site and saved the image of the website shown below.



https://sinbad.io http://sinbadiovkigdbafpqvwfwjh2tfrisahtxmrskiovt62nirzagcnkcad.onion

SINBAD.IO «Not every part of your private life needs to be public»

BITCOIN MIXER

Enter receiver's bitcoin address

+ ADD ADDRESS

Minimum amount for mixing: 0.001 BTC

Select service fee

+ 0.0002 BTC per each address

The priority of the outgoing transaction: Standard

Enter the mixing code (optionally)

MIX COINS

Sinbad © 2023

18LCYs7Be72BeXUMvpxsfJ6QFgH1Bvcgac
Do not send bitcoins to this address

We are on Bitcointalk
Our PGP key

support@sinbad.io
adv@sinbad.io

Telegram english
Telegram russian
Jabber (omemo)

17. In the FAQ section, Sinbad.io describes a Bitcoin mixer as "a service that obfuscates your bitcoin transactions. It takes your bitcoins and sends you back the ones from the pool, which are premixed and not connected with you. Thus, it breaks the link between the transactions before and after mixing and makes it impossible to track the connection between the bitcoins that came into the mixer and went out."

18. Sinbad.io's FAQ section answers the question, "How to use the mixer properly?" It describes the process as follows:

a. "Enter one or several destination bitcoin addresses for receiving of new bitcoins."

b. "Specify the delay time and split the amount among destination addresses if there a few ones."

c. "Download the guarantee letter."

d. "Mixer gives you an address. Send your bitcoins to it."

19. FBI analysis approximates between $418.3 million and $616.2 million worth of Bitcoin moved through Sinbad.io since its inception, based on the value of the Bitcoin at the time of transactions.

B. Blender.io operators advertised concealment and obfuscation functions of the service on forums discussing virtual currency

20. When Blender.io first began operating, an advertisement for the service was posted on Bitcointalk.org. The advertisement was posted by a user with the username "blenderio" on or about October 18, 2018. The post described Blender.io's service, including three websites—two clearnet websites and one Tor site. The post noted that Blender.io had a "No Logs Policy" and that "[t]here's absolutely no log whatsoever, and whatever trace does exist of your transaction is deleted as soon as your transaction goes

through." The post also explained that no registration was required for users: "Blender.io doesn't require you to signup, register or provide any kind of detail except the receiving address! As there are no personal details asked for, there's no way your identity is compromised, or can be linked back to, because as far as blender.io goes they don't know who you are." The advertisement contained a contact email address for support, integration requests, and refunds: blenderio@tuta.io and a contact email address for advertisement questions: adblenderio@tuta.io.

21. On December 21, 2018, blenderio made a post entitled "iPhone X giveaway by the Blender team" that offered individuals a chance to win an iPhone X by advertising Blender.io on Bitcointalk.org, "liking" posts issued by blender_io on Twitter, and publishing reviews of Blender.io, among other things. The post also had a link to the twitter profile for Blender.io: blender_io. Records provided by Twitter show that the blender_io account was created on November 20, 2018, it was registered using the email address adblenderio@tuta.io, and the display name was blender.io. This account was registered to a Russian phone number and the Internet Protocol ("IP") address used to create the account belonged to a Russian internet service provider ("ISP").

22. The email account adblenderio@tuta.io was used to register an account with Bits.media. The account was created on January 14, 2019, with username "blender_io." Bits.media is a Russian-language, topic-based forum where, like Bitcointalk.org forum, users may post information. The blender_io account made a post on January 14, 2019, in Russian that used the same wording as the post made on Bitcointalk.org by user blenderio in October 2018.

23. From January 14, 2019, until July 7, 2021, the blender_io account on Bits.media made several posts. For example, on August 29, 2019, the blender_io account posted a message that, when translated to English, stated in part, "We have successfully completed the update of our beloved Blender.io," and described improvements, including longer mixing delays and "a random offset of a few minutes to the transaction appearing in the memory pool to make tracking transactions even more difficult."

C. The rn3rd account, linked to Blender.io and Sinbad.io's operator(s), was used to help fund Sinbad.io with funds from Blender.io, pay for an advertisement for a related application on a cyber-criminal forum, and purchase Sinbad.io's domain name.

24. As shown above in the figure from paragraph 12 of this affidavit, the virtual currency address starting with 0xDa8D5A was involved in the movement of funds from a cluster attributed to Blender.io to a cluster attributed to Sinbad.io. Based on FBI blockchain analysis, this 0xDa8D5A address received the initial funding to facilitate the movement of these funds from a virtual currency address starting 0xda6e62. The address 0xda6e62 was used for the first time on or about November 27, 2020; this initial transaction was a deposit of approximately 0.4815545 Ether from the virtual currency exchange company Any.Cash into 0xda6e62. Based on records provided by Any.Cash, this transaction was conducted by a user who registered for an account using the Telegram handle @rn3rd. The account was created on August 5, 2020, and was last used on April 5, 2022.

25. While in operation, the administrators of Blender.io advertised a linked virtual currency wallet service, Blenderwallet.io. In an April 5, 2022, post by blenderio on Bitcointalk.org, blenderio stated "Services blenderio and blenderwallet.io are closed

for maintenance … We apologize for the inconvenience, please do not worry, the services will be resumed in the near future."

26. Based on information collected from FBI databases, an account on a cyber-criminal forum using the email address blenderapp@tutanota.com made a payment to the forum for the placement of advertisements for the service Blenderwallet.io. The forum admin requested 10,000 USDT[6] be sent to the virtual currency address starting 0x8309F5FEee. On or about June 10, 2021, blenderapp@tutanota.com sent a message stating that the money had been sent and provided a transaction hash starting with 0xe30fa81a5d4bbe. Based on FBI blockchain analysis and records provided by Any.Cash, this transaction hash corresponds to a transfer of 10,000 USDT from the @rn3rd Any.Cash account to the virtual currency address starting 0x8309F5FEee.

27. The virtual currency address 0xda6e62 that received initial funding from the @rn3rd Any.Cash account was also responsible for moving funds that were used to purchase the Sinbad.io domain. On or about April 16, 2022, the 0xda6e62 virtual currency address sent approximately $40,400 worth of virtual currency on the Ethereum blockchain to an address beginning 0xf40fcC, which then converted these funds to Bitcoin on the Bitcoin blockchain. The converted Bitcoin was received by a virtual currency address beginning bc1q0vuhn8lfae on April 16, 2022. A portion of these funds was sent to an intermediary virtual currency address on April 25, 2022, where it remained until May 23, 2022, when a transfer worth approximately $20,000 was made from this

[6] USDT is the abbreviation for the virtual currency Tether. Tether is a stablecoin, a virtual currency with a value meant to be pegged to the U.S. dollar, meaning that generally one USDT equals approximately one U.S. dollar.

address to the domain registrar Namecheap. Based on records provided by Namecheap this transaction represented a deposit of $20,000 to a Namecheap account registered to a user who provided the name Yosha Worashen and the email address yowora@proton.me. On May 23, 2022, this account purchased the domains Sinbad.io and Sindbad.io. The price for the two domains was approximately $17,738.

D. The rn3rd account's connection to Ostapenko's company, Smart Code Group, and the company's link to multiple Ostapenko accounts.

28. Based on the records provided by Any.Cash, on November 5 and 8, 2021, the @rn3rd Any.Cash account made two transfers, totaling approximately 143,632 USDT, to a virtual currency address beginning 0x9f50831eE. Based on FBI blockchain analysis, this address belongs to the virtual currency exchange WhiteBIT. Based on records provided by WhiteBIT, the two transfers were an automated exchange of USDT to Euros. The resulting funds were sent via wire transfer to the recipient's bank account. The exchange order was placed by an individual with a Telegram messenger ID @WinnieTheeePooh, bank account number 40702978810000000769, identifier code TICSRUMMXXX, and entity name Smart Code Group. Based on open-source research, bank identifier code TICSRUMMXXX corresponds to Tinkoff Bank in Russia.

29. Open-source searches for "Smart Code Group" yielded a LinkedIn page for Roman Ostapenko, who was listed as the CEO of Smart Code Group. Based on records provided by LinkedIn, this account was registered by an individual who provided the name Roman Ostapenko, email address r.ostapenko@protonmail.com, and phone number +971 52 889 3678. Open-source searches for Roman Ostapenko returned information for a Russian LLC: "Смарт Код Групп" (this is a transliteration of the English spelling of Smart Code Group). This LLC was registered to an individual "Роман

Витальевич Остапенко" (this is the Russian Cyrillic spelling of the name Roman Vitalyevich Ostapenko). The LLC corporate filing information listed Ostapenko's contact email address as chief@scg.re and open-source research associated with this LLC lists Ostapenko's phone number as +79998496666.

30. Based on records provided by Google, a Google account exists tied to the phone number +971 52 889 3678. This phone number is associated with the email address rockguitars@gmail.com, which was registered by a user who provided the name "Roman Ostapenko (Cyberwolf)" and provided a recovery email address of cyberwolf@protonmail.ch. Based on records provided by Google, a Google account also exists tied to the phone number +79998296666. This phone number is associated with the email address baysell@gmail.com, which was registered by a user who provided the name "Roman Ost" and provided a recovery email address of zloiwolf@yandex.ru.

31. Based on records provided by the virtual currency exchange Binance, an account registered using the email address cyberwolf@protonmail.ch was created by a user providing the name Roman Ostapenko (the "Ostapenko Binance Account"). Know your customer (KYC) documents submitted by this user include a Russian passport under the name of Роман Витальевич Остапенко (again, this is the Russian Cyrillic spelling of the name Roman Vitalyevich Ostapenko).

E. Blender.io Servers Connected to Smart Code Group Email Domains

32. Beginning on or about April 5, 2022—the same date that the blenderio user on Bitcointalk.org claimed that Blender.io and Blenderwallet.io had been closed "for maintenance" and would return shortly—international law enforcement partners seized server infrastructure from a reseller of internet services. The seizure was made as part of

an investigation into online sales of narcotics and money laundering. The FBI received copies of hard drives seized during this operation. Later, FBI review of the servers indicated that some of the data pertained to Blender.io and the FBI determined that the servers seized included servers that had the source code for the Blender.io webpage and mixing functionality.

33. Based on analysis of the seized servers, one of the identified servers ("Blender Database Server") appears to have hosted Blender.io database information. This data includes tables of information that appear to represent transactions into and out of Blender.io. These tables include information about the virtual currency address to which funds were sent, transaction time and date information, transaction type, and other transactional information. A table describing the transaction type lists the options: "user request," "fee withdrawal," "reward withdrawal," "transfer," and "premixing." User request transactions appear to represent mixing requests initiated by users of the Blender.io mixing service. The overwhelming majority of the transactions in this table are in the user request category. Fee withdrawal and transfer transactions were not initiated by users of the mixing service, and these transactions were much less common. I believe in my training and experience that these fee withdrawal and transfer type transactions were initiated by the operators of the Blender.io mixing service and may represent actions such as the taking of profits and movement of funds for operating expenses.

34. Initial review of the Blender.io servers indicates that the developer(s) of Blender.io used a software called GitLab in the development of the service. GitLab is an open-source code repository and software development platform. GitLab includes version

control functionality, which allows users to track changes made to files. Each time a change is made to the file or code it is recorded as a unique "commit." These commits make up the history of when and how a file changed, and who changed it. Review of the GitLab logs for the Blender.io Server operating GitLab shows that multiple changes were made by users providing an email address at the email domain @scg.re—the same domain used in the Smart Code Group's LLC corporate record filings.

35. These changes include a change made on October 18, 2018, by a user who provided the name "Administrator" and the email address cto@scg.re, as well as multiple changes made by a user who provided the name "as" and the email address as@scg.re. Based on my knowledge and experience, I know that "CTO" is a commonly used acronym to describe the role of chief technical (or technology) officer within a company or organization. In addition to the commit made by the user providing the name "Administrator" and email address cto@scg.re, there were an additional approximately 451 commits made by a user who provided the name "cto." This user frequently provided the fictitious email you@example.com.

36. In multiple commits found in this GitLab log, an external URL is referenced. The URL, "gitlab.araxa.be," appears to represent an external server where a GitLab repository is being hosted.[7] For example:

[7] GitLab allows users to install and operate the software on private server(s) they control. This allows users to maintain control of their code and allows members of an organization to access the GitLab repository via a URL, which directs users to the server hosting the GitLab instance.

a. On March 30, 2019, Author: "cto <you@example.com>" recorded the commit "Merge branch 'develop' of gitlab.araxa.be:user/blender into develop"

b. On May 27, 2019, Author: "cto <you@example.com>" recorded the commit "Merge branch 'feature/#77_withdraw_unspents' of gitlab.araxa.be:user/blender into feature/#77_withdraw_unspents"

37. Based on analysis of the servers seized, a separate server was identified ("GitLab Server") that appears to have hosted the above-referenced GitLab repository. This server had a GitLab configuration file which included the configuration setting: "external_url: 'https://gitlab.araxa.be'." Based on documentation on GitLab's website,[8] this setting configures the URL by which users can reach the GitLab repository in question. This configuration file also included settings for email messages sent to or from the GitLab instance operating on this server.[9] The email address configured to receive incoming email for this GitLab instance was listed as "gitlab@scg.re." The email address configured to send outgoing email for this GitLab instance was listed as "git@eivindr.in."

38. Based on analysis of the GitLab Server, it appears that much of the data on the server was deleted after the seizure of this infrastructure began. When a file is

[8] GitLab, Configuration options, https://docs.gitlab.com/omnibus/settings/configuration.html.

[9] GitLab allows users to configure email addresses from which the application can send and receive email communications. The application can be configured to send automated email messages, such as notification email, and can also be configured to receive emails from users, allowing users to make changes by sending an email to a specified email address. *See* "Incoming email," https://docs.gitlab.com/ee/administration/incoming_email.html

deleted, most file systems simply mark the space on the hard drive where the data was maintained as available, but do not completely overwrite this data. This allows digital forensic investigators to review data on a server whose files have been deleted, although the context and structure of this data may be lost. Through review of this data, multiple references to scg.re were found, including the following email addresses ep@scg.re and is@scg.re.

39. As explained in paragraph 29 of this affidavit, the registration filing paperwork for Ostapenko's company, Smart Code Group, lists Ostapenko's email as chief@scg.re. Open-source research for the email address chief@scg.re indicates that the domain is no longer active, but as recently as April 1, 2022, this domain corresponded to a mail exchange server belonging to Zoho.com. According to their website, "Zoho Mail Suite is a business-focused email service provider where you can add your own domain and create a custom and unique—yourname@yourdomain.com—email address." Searches for "@scg.re" returned no other relevant results. Based on this context and my training and experience, I believe that the email domain @scg.re is a custom and unique email domain created for Ostapenko's business Smart Code Group, and that in fact "scg" is an abbreviation for Smart Code Group.

40. Based on this, I believe that the user(s) who made edits to the Blender.io source code providing email addresses at the @scg.re domain either are, or are associated with, Roman Ostapenko and his business.

F. The eivindr.in domain's links to Blender.io and Sinbad.io Infrastructure

41. In addition to finding @scg.re domains in the seized Gitlab Server data, as discussed in paragraph 38 of this Affidavit, multiple references to a "eivindr.in" domain

were also found, including as@eivindr.in and pooh@eivindr.in. In addition to these email addresses, the domain mail.eivindr.in was found in association with the IP address 198.199.124.37.

42. While it was operational, Sinbad.io's clearnet website used Cloudflare to provide a content delivery network and cloud security services.[10] Based on records provided by Cloudflare, as of March 2, 2023, two IP addresses were identified as the destination for internet traffic addressed to the Sinbad.io clearnet website: 65.21.185.112 and 65.108.241.248. These IP addresses were identified as belonging to Hetzner Finland, a server center based in Finland.

43. According to information provided by Hetzner Finland, these servers were sold to an Internet reseller service called Bithost.io ("Bithost"). Internet resellers rent and/or purchase servers and other internet infrastructure from large ISPs/server providers and sell them to end customers at a premium.

44. According to records provided by Bithost, the account that purchased the servers using IP addresses 65.21.185.112 and 65.108.241.248 purchased a server that was named "eivindr.in." The eivindr.in server was purchased on November 9, 2021, and was associated with the IP address 198.199.124.37. This is the same domain and IP address found in the GitLab Server described in paragraph 41. Based on this information, I believe that the individuals who purchased and maintained infrastructure used to operate

[10] Cloudflare provides services whereby its infrastructure acts as a mediator between a website's server and visitors, improving the speed and reliability of the website while also protecting from online threats.

Sinbad.io are the same individuals who developed and maintained the source code for Blender.io.

G. Additional Any.Cash accounts connected to Ostapenko and Blender.io

The "@cyberbiber"Any.Cash account

45. Based on blockchain analysis, a peel chain that made multiple deposits into the Ostapenko Binance Account also made deposits into an Any.Cash deposit address that, based on information provided by Any.Cash, was registered to a user operating the telegram moniker "@cyberbiber." The FBI's review of Ostapenko's Apple iCloud account pursuant to a search warrant issued on March 13, 2024, by a United States Magistrate Judge in the Northern District of Georgia revealed multiple screenshots of Telegram conversations in which the moniker @cyberbiber is a participant. Based on these images it appears that the individual who captured the images was the operator of the "@cyberbiber" moniker. Additionally, there is a bits.media forum profile account with the username Cyberbiber and email address cyberwolf@protonmail.ch. Cyberwolf@protonmail.ch is one of Ostapenko's email addresses, discussed *supra* in paragraphs 30 and 31 and *infra* in paragraph 51.

46. Based on blockchain analysis, a peel chain made multiple deposits, totaling approximately $143,000, into the "@rn3rd" Any.Cash account between July 3, 2021, and August 13, 2021. This same peel chain also made multiple deposits, totaling approximately $229,000, into the "@cyberbiber" Any.Cash account between July 7, 2021, and August 5, 2021.

47. Based on records provided by Binance, on November 17, 2021, the Ostapenko Binance Account sent 3,000,000 USDT to a virtual currency address

beginning 0x4BE231115cE. On February 9, 2022, this virtual currency address sent 50,000 USDT to the "@cyberbiber" Any.Cash account.

48. Based on this information and my knowledge and experience, I believe that Ostapenko controls the "@cyberbiber" Any.Cash account.

Any.Cash Account "@asaventura"

49. On February 26, 2022, the virtual currency address beginning 0x4BE231115cE sent 200,000 USDT to another Any.Cash deposit address that, based on records from Any.Cash, belongs to an account registered to a user operating the telegram moniker "@asaventura." This account was created on October 27, 2021, and was connected to a "GoogleAuth Token Title" of "roma.any". Based on my training and experience, I believe this refers to a two-factor authentication token,[11] like those provided by Google Authenticator and other two-factor authentication applications. Based on this information and my training and experience, I believe that the user of the "@asaventura" Any.Cash account was using two-factor authentication to access this account, and that this user provided the title "roma.any" in association with this two-factor authentication token.

[11] Two-factor authentication (2FA) is a security process that requires users to provide two different forms of identification to access a resource or data. This is in addition to the traditional username and password method. A 2FA software token, also known as a soft token, is a digital security token that generates a one-time passcode to verify a user's identity.

50. Based on records provided by Any.Cash, on October 27, 2021, 99,990 USDT was transferred from the "@cyberbiber" Any.Cash account to the "@asaventura" Any.Cash account. This transfer appears to be the first deposit into the "@asaventura" Any.Cash account.

51. The FBI's review of Ostapenko's Apple iCloud account pursuant to a search warrant revealed that the iCloud account contained a file that appeared to be an application configuration file for the application Authy. Based on their website, Authy is a free mobile app for two-factor authentication. Authy is owned by Twilio, a company based in San Francisco, California. This configuration file contains what appears to be information pertaining to two-factor authentication tokens for various websites/services. Many of these tokens are tied to Ostapenko's email addresses cyberwolf@protonmail.ch, baysell@gmail.com, and rockguitars@gmail.com. One of these token entries lists the token type as "GoogleAuthApp" and the name as "roma.any."

52. Based on this information and my knowledge and experience, I believe that Ostapenko controls/controlled the "@asaventura" Any.Cash account.

53. Blockchain analysis based on data from the Blender Database Server, first described in paragraph 33, shows that the "@asaventura" Any.Cash account received funds that moved through Blender.io.

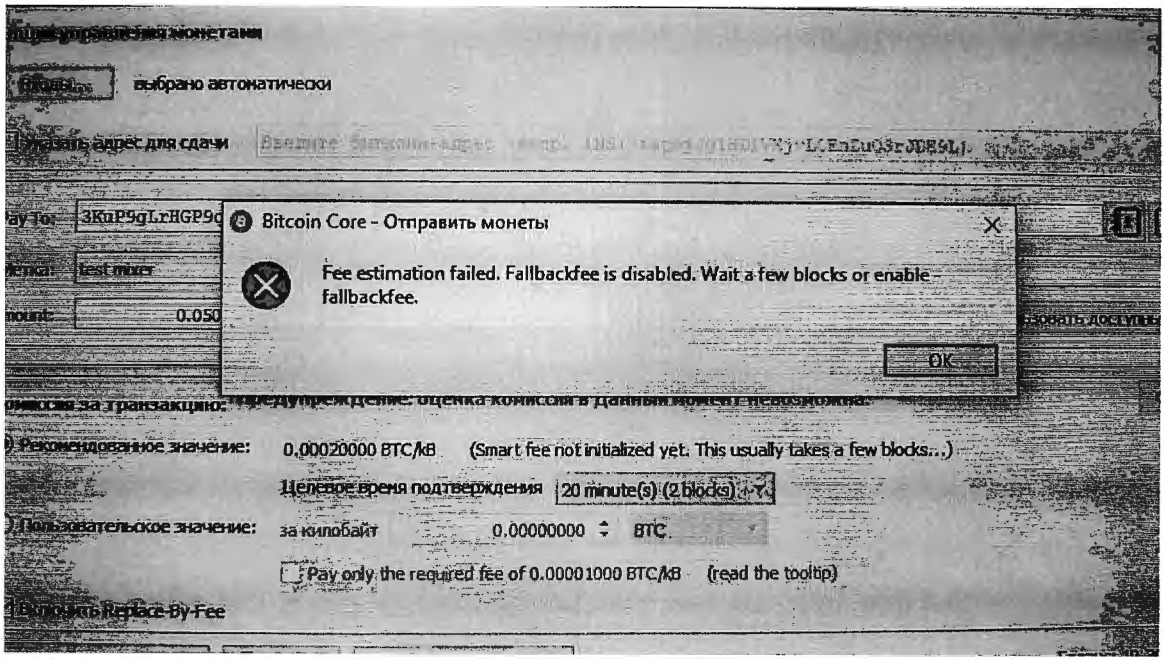
a. There is a database entry listed under ID number 74354 that lists the transaction type as "fee withdrawal." This entry lists the distribution address as bc1qckqzsj9e4th3065pnz9twtr4x7v9rshulecfss and lists a "created_at" timestamp of 2022-02-28 09:04:31. Based on blockchain analysis, the virtual currency address beginning bc1qckqzsj9e4th received approximately 6.05772792 Bitcoin on February 28, 2022, at approximately 9:25 AM. This address did not receive any other virtual currency before or after this transaction. Funds from this transaction moved through two intermediary virtual currency addresses as part of a peel chain before approximately 2.67950709 Bitcoin was deposited into the "@asaventura" Any.Cash account on March 1, 2022.

b. There is a database entry listed under ID number 53113 that lists the transaction type as "transfer." This entry lists the distribution address as bc1qpedyraevr0pgr9tsyslswchdampytflyavjs0v and lists a "created_at" timestamp of 2021-12-27 15:02:58. Based on blockchain analysis, the virtual currency address beginning bc1qpedyraevr received approximately 0.2696111 Bitcoin on December 27, 2021, at or about 15:07 UTC. This address did not receive any other virtual currency before or after this transaction. On February 1, 2022, this address sent approximately 0.17 Bitcoin to the "@asaventura" Any.Cash account. As part of this same transaction, approximately 0.09960261 Bitcoin was sent from the virtual currency address beginning bc1qpedyraevr to the virtual currency address beginning bc1qysre9ff0vwu. On February 2, 2022, the virtual currency address beginning bc1qysre9ff0vwu sent the entirety of this 0.09960261 Bitcoin to the "@asaventura" Any.Cash account.

H. Ostapenko's "test mixer" transaction twelve days before Blender.io was publicly advertised

54. Based on a review of data produced pursuant to a search warrant issued on May 10, 2024, by a United States Magistrate Judge in the Northern District of Georgia

for the email accounts rockguitars@gmail.com, baysell@gmail.com, and Ostapenko@helix.co, a photo that appears to be a screenshot from a computer was found in the rockguitars@gmail.com email account. A copy of this photo is included below.



управления монетами

Входы... выбрано автоматически

Указать адрес для сдачи [illegible] LCEnZuQ3rJD89Lj.

ay To: 3KuP9gLrHGP9c

етка: test mixer

nount: 0.050

Bitcoin Core - Отправить монеты

Fee estimation failed. Fallbackfee is disabled. Wait a few blocks or enable fallbackfee.

OK

зовать доступны

омиссия за транзакцию: Предупреждение: оценка комиссии в данный момент невозможна.

Рекомендованное значение: 0,00020000 BTC/kB (Smart fee not initialized yet. This usually takes a few blocks...)

Целевое время подтверждения 20 minute(s) (2 blocks)

Пользовательское значение: за килобайт 0,00000000 BTC

□ Pay only the required fee of 0.00001000 BTC/kB (read the tooltip)

Включить Replace-By-Fee

This photo appears to depict a bitcoin transaction. In the center of the photo there is logo and text field that says, "Bitcoin Core - Отправить монеты." Based on their website, Bitcoin Core "… is an open source project which maintains and releases Bitcoin client software called 'Bitcoin Core.' Bitcoin Core consists of both 'full-node' software for fully validating the blockchain as well as a bitcoin wallet." Отправить монеты is Russian Cyrillic, which in English translates to "Send Coins."[12] In this photo there is a section titled "Pay To" that lists a bitcoin address beginning 3KuP9gLrHGP9. There is only one address that begins with these characters that has registered transactions on the public Bitcoin blockchain. Below the "Pay To" field there is a field titled "Метка:",

[12] Based on open-source machine translation.

which is Russian Cyrillic that translates to "Label,"[13] with text entered, "test mixer." Below the "Метка:" field there is a field titled "mount:" which appears to be a truncation of the word "Amount." In that field the text entered is "0.050." The metadata for this photo shows a creation date of October 6, 2018. Based on blockchain analysis, the virtual currency address 3KuP9gLrHGP9 received a deposit of 0.05 bitcoin on October 6, 2018. This apparent test transaction occurred about 12 days before Blender.io was publicly advertised on Bitcointalk.

I. Blender.io Funds Move To Sinbad.io and an another Ostapenko-Connected/ Controlled Virtual Currency Address

55. When Blender.io ceased operations in April 2022, a large amount of funds was moved through a virtual currency wallet/mixing service called Wasabi Wallet. Based on Wasabi's website, "Wasabi is an open-source, non-custodial, privacy-focused Bitcoin wallet for desktop, that implements trustless coinjoin over the Tor anonymity network." On or about April 5, 2022, approximately 195 Bitcoin (worth approximately $9.1 million USD) was transferred from a cluster associated with Blender.io to a virtual currency address beginning bc1qdqt2q8e4gp.

56. On April 14, 2022, approximately 173 Bitcoin was transferred from the virtual currency address beginning bc1qdqt2q8e4gp to a cluster associated with Wasabi Wallet, and on the same date an additional approximately 22 Bitcoin was transferred through an intermediary address and into the same cluster associated with Wasabi Wallet. On or about April 16, 2022, a virtual currency address beginning bc1qvstxf86n received approximately 12.4 Bitcoin from this cluster associated with Wasabi Wallet. On or about

[13] Based on open-source machine translation.

April 17, 2022, this address sent approximately 12.1 Bitcoin through blockchain bridge RenBridge to be converted and sent to a virtual currency address beginning 0x3194bCA4Df56a on the Ethereum blockchain. Prior to this transaction, also on April 17, 2022, this address received its initial funding from the same 0xda6e62 virtual currency address described in Paragraphs 24 and 27 of this affidavit. On or about April 18, 2022, the 0x3194bCA4Df56a address transferred the entirety of the funds it received from the RenBridge transfer back through the RenBridge to convert these funds back into Bitcoin; this bitcoin was received at the virtual currency address beginning bc1qe0nd22wte3.

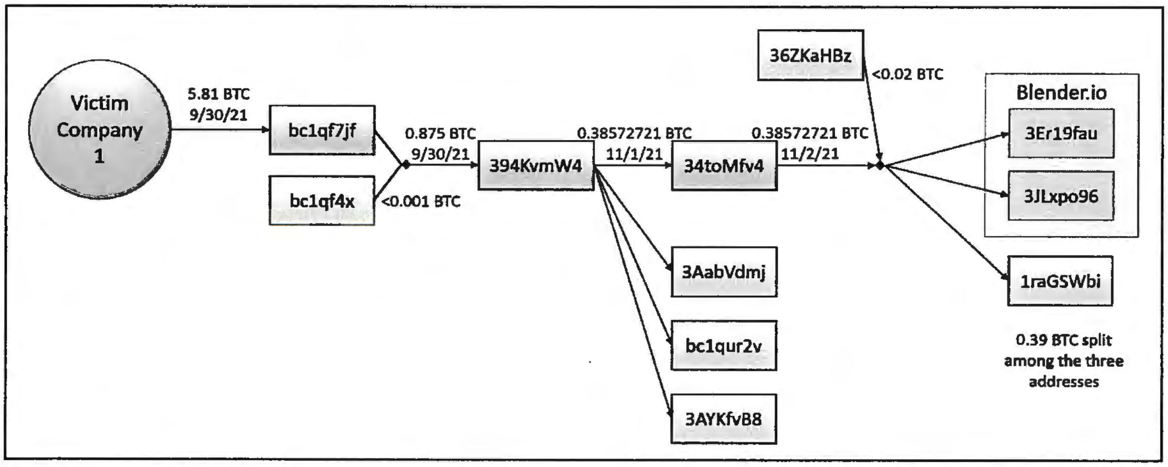
57. On or about December 1, 2022, the bc1qe0nd22wte3 address transferred the entirety of these funds out in a single transaction. Then, a large portion of these funds were sent to a series of addresses that appear to terminate at a cluster associated with Sinbad.io. Approximately $13,000 of the funds from bc1qe0nd22wte3 were sent to a virtual currency address starting bc1qr7lnv59wngre. Based on review of the returns from the search warrant described in paragraph 54 of this affidavit, the FBI identified a document containing a virtual currency recovery phrase. The FBI was later able to identify virtual currency addresses associated with this recovery phrase. One of these addresses was the bc1qr7lnv59wngre address. Based on this information, I believe that Ostapenko controlled the bc1qr7lnv59wngre address that received approximately $13,000 worth of virtual currency from the RenBridge transactions.

J. Blender.io and Sinbad.io Were Money Laundering Tools

58. On September 18, 2021, a company located in the Northern District of Georgia, (Victim Company 1) noticed that it was unable to access certain internal

computer systems and, upon investigation, learned its systems were encrypted with the Babuk ransomware variant. The Babuk ransomware variant is advertised as a Ransomware-as-a-Service and has been used by malicious actors to encrypt files on victims' computer networks. After a victim's files are encrypted, the malicious actors demand payment in exchange for the decryption key. If the victim fails to make the payment, the malicious actors publish the victim's data on the Babuk Tor site.

59. The malicious actors demanded a $2.5 million ransom. Victim Company 1 negotiated a reduced ransom payment of $250,000. On or about September 30, 2021, the victim paid a ransom of approximately 5.81 BTC (worth approximately $253,000 at the time). As shown below, 0.3857272 BTC (approximately $24,000) of the victim's funds were then sent to a cluster attributed to Blender.io.



60. In or around February 2022, a series of internal chats among Conti ransomware actors[14] were publicly leaked online. In several chats, an actor known as

[14] *See* "Conti Ransomware," https://www.cisa.gov/news-events/alerts/2021/09/22/conti-ransomware ("In typical Conti ransomware attacks, malicious cyber actors steal files, encrypt servers and workstations, and demand a ransom payment").

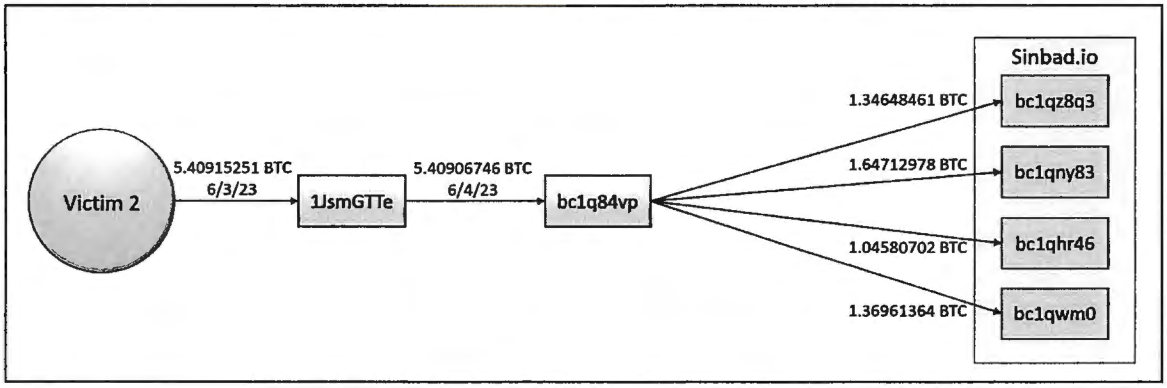
"reshaev" shared Bitcoin addresses belonging to him with other ransomware actors that were party to the chats. Performing blockchain analysis on reshaev's Bitcoin addresses showed that reshaev made transfers to addresses attributed to Blender.io between July 2020 and February 2021. The Bitcoin laundered through Blender.io corresponding to the reshaev addresses was valued at approximately $263,000 at the time. Additionally, other Bitcoin addresses attributed to reshaev by a commercially available Bitcoin tracing tool estimated that reshaev made approximately sixty transfers to addresses attributed to Blender.io. Those transfers were estimated at a total value of over $1 million at the time of the transfers.

61. In June 2023, a North Korean hacking group targeted virtual currency wallet software Atomic Wallet and stole more than $100 million in virtual currency.[15] This hack was widely publicized.[16] Blockchain analysis shows proceeds from the Atomic Wallet heist flowing into the Sinbad.io virtual currency mixer.

62. On or about June 2, 2023, a resident of the Northern District of Georgia (Victim 2) was a victim of the Atomic Wallet hack. Based on reporting by Victim 2, approximately 5.4 bitcoin (worth approximately $147,366 at the time of the theft) was transferred out of Victim 2's wallet without his knowledge or consent. Below is an illustration of the funds that flowed into a cluster attributed to Sinbad.io.

[15] *See* "FBI Identifies Cryptocurrency Funds Stolen by DPRK," https://www.fbi.gov/news/press-releases/fbi-identifies-cryptocurrency-funds-stolen-by-dprk.

[16] *See, e.g.*, "Atomic Wallet Was Breached by North Korean Hackers: Elliptic," https://www.coindesk.com/consensus-magazine/2023/06/06/atomic-wallet-was-breached-by-north-korean-hackers-elliptic/.



63. The flow of funds into Sinbad.io included virtual assets from addresses associated with malicious North Korean actors. This association, and North Korean hackers' use of Sinbad.io, was widely publicized and known, especially throughout the virtual currency community.[17]

64. The Sinbad.io mixing service was established and promoted on Bitcointalk.org after the United States issued sanctions against its predecessor service, Blender.io, for the unlawful laundering of funds. The sanctioning of Blender.io was also widely publicized in both mainstream and cryptocurrency-focused outlets, with many articles noting that Blender.io was the first virtual currency mixing service to be sanctioned by OFAC.[18]

[17] *See, e.g.*, "$35 million Atomic Wallet hacker funnels crypto to North Korea's favored mixer," https://www.elliptic.co/blog/analysis/35-million-atomic-wallet-hacker-funnels-crypto-to-north-korea-s-favored-mixer; "Atomic Wallet hacker sends crypto to mixer used by Lazarus Group: Elliptic," https://cointelegraph.com/news/atomic-wallet-hacker-sends-crypto-mixer-elliptic.

[18] *See, e.g.*, "U.S. adds cryptocurrency mixer Blender to sanctions list over alleged North Korea links," https://www.reuters.com/business/us-adds-virtual-currency-mixer-sanctions-list-over-north-koreas-cyber-activities-2022-05-06/;"US Officials Add North Korea-Linked Bitcoin Mixer, More BTC and ETH Addresses to Sanctions List," https://www.coindesk.com/policy/2022/05/06/us-treasury-department-sanctions-crypto-mixing-service/; "Crypto mixer sanctioned by US Treasury for role in Axie Infinity

K. Blender.io and Sinbad.io Operated as Unlicensed Money Transmitting Businesses

65. FBI analysis using commercially available blockchain analysis tools revealed that U.S.-based virtual currency exchanges and financial services companies sent and received millions of dollars in funds to and from Blender.io and Sinbad.io. The FBI found transactions involving Blender.io and multiple U.S.-based virtual currency exchanges and financial services companies, including: Coinbase.com, Kraken.com, Paxful.com, Crypto.com, Poloniex.com, Gemini.com, FTX.com, Binance.us, AthenaBitcoin.com, BitPay.com, Circle.com, FTX.us, PayPal.com, and Robinhood.com.[19] The FBI also found transactions involving Sinbad.io and various U.S.-based virtual currency exchanges and financial services companies, including Poloniex.com, Binance.us, Kraken.com, Crypto.com, Cash.app, Paxful.com, Coinbase.com, AthenaBitcoin.com, BitPay.com, Circle.com, Gemini.com, PayPal.com, Robinhood.com, FTX.com, and FTX.us.

66. The analysis distinguished between those funds directly sent to or received from the exchanges and funds that were indirectly sent or received. Funds that traversed one or more addresses between the clusters attributed to Blender.io or Sinbad.io before being received by an exchange are categorized as indirect exposure. Funds that flowed from the Blender.io or Sinbad.io cluster without intermediate addresses directly to an exchange are categorized as direct transfers. The chart below outlines approximate virtual

hack," https://cointelegraph.com/news/crypto-mixer-sanctioned-by-us-treasury-for-role-in-axie-infinity-hack.

[19] Note, not every listed exchange has claimed to have been exclusively U.S.-based or to provide services to U.S. users continuously since establishment.

currency exposure to U.S. exchanges based on this analysis. The chart lists the direct transfers and the total exposure (indirect exposure plus direct transfers) for the mixers:

Blender.io Exposure to U.S. Exchanges			
Direct Transfers		Total Exposure	
Received	Sent	Received	Sent
$1,627,000	$2,482,000	$52,090,000	$25,196,000
Sinbad.io Exposure to U.S. Exchanges			
Direct Transfers		Total Exposure	
Received	Sent	Received	Sent
$428,000	$124,000	$11,319,000	$1,732,000

67. Blender.io and Sinbad.io were available to users across the world, including in the Northern District of Georgia. From October 15, 2021, through December 13, 2021, a bitcoin wallet received approximately $1,210 in bitcoin from Blender.io via five transactions. On April 13, 2023, this same bitcoin wallet received approximately $320 in bitcoin from Sinbad.io. Based on information obtained by Hetzner Finland, it was determined that the April 13, 2023 mix, which was initiated from an IP address located in the Northern District of Georgia, requested the mixed funds to be transferred to the same bitcoin wallet.

68. On November 22, 2023, an undercover FBI special agent accessed Sinbad.io and submitted a mixing request. The undercover FBI agent requested a mix with no delay, fast priority, and output to an FBI-controlled wallet address. After submitting the mixing request, a guarantee letter was generated and downloaded by the agent. That letter stated:

> We hereby confirm that Sinbad has generated the address bc1qsentl6ngxl5p3rhzzm48uunv9a6r86kwen475x in order to transfer incoming amount (minus fee) to the following addresses: 100% to 1KoMGnhDifH2meUktSgAEMPZuc7LsTg9SJ after 0 hour(s). This service will

> be only available for all bitcoins received from Wed, 22 Nov 2023 21:20:04 GMT to Thu, 23 Nov 2023 21:20:04 GMT with minimum amount of 0.001 BTC per single transaction and maximum amount of 927.93828784 BTC total. Our fee is 2.5% + 0.0003 BTC for every target address. This letter is digitally signed by our main account: 18LCYs78e72BwXUMvpxsfJ6QFgH1Bvcgwc. Stay protected and thank you for using our service.

69. The agent transferred 0.0265 BTC, or approximately $1,000, from an FBI wallet address to the Sinbad.io service address specified for the mix. Immediately after the transaction had received 3 confirmations by the Bitcoin network, the FBI agent received 0.0255375 BTC to the specified FBI wallet address. The FBI agent was located in the Northern District of Georgia at the time of the transfer.

70. The letter of guarantee also stated the maximum mix allowed by the service at the time of the transfer was approximately 927 BTC, which is approximately $34 million. As previously outlined, Sinbad.io described its functionality as taking the user's Bitcoin and replacing it with Bitcoin that is premixed in the pool and unconnected to the user. This implies that Sinbad.io had at least 927 BTC. As such, I believe that at the time of the undercover transaction, Sinbad.io controlled a minimum of 927 BTC in its liquidity pool.

71. On November 30, 2023, the United States Treasury's Financial Crimes Enforcement Network (FinCEN) database for Money Service Businesses (MSBs) registrants was queried and no registration for Blender.io or Sinbad.io was found. An additional search of the database used by the Georgia Department of Banking and Finance for MSBs revealed no registration for Blender.io or Sinbad.io.

M. Sinbad.io goes offline in November 2023

72. On or about November 27, 2023, Sinbad.io became inaccessible due to law enforcement action by the FBI and international partners.

73. On or about November 30, 2023, OFAC sanctioned Sinbad.io, noting that it was a key money-laundering tool of the OFAC-designated Lazarus Group, a state-sponsored cyber hacking group of the DPRK. That same day, the Sinbad.io domain name was seized by the FBI and a webpage was put up on the domain name noting that the service was seized as part of a coordinated law enforcement action between the FBI and foreign law enforcement partners.

CONCLUSION

74. Based on the information in this Affidavit, I respectfully request that a complaint and arrest warrant be issued for OSTAPENKO for violations of Title 18, United States Code, Sections 1956(h) (money laundering conspiracy) and 1960 (unlicensed money transmitting business).