INCIDENT REPORT FOR THEFT OF VIRTUAL ASSETS

[redacted]

CRYPTEGRIDY LTD Kemp House 160 City Road, EC1V 2NX

Investigator:	[redacted]
	CrypTegridy LTD
	Kemp House 160 City Road, EC1V 2NX
Subject:	Blockchain Incident Report
Offence:	Money Laundering, Fraud, Theft, organized crime activities
Accused:	Owner of OrbitGTM-pros.com "Actor" [redacted] "Actor" [redacted] "Actor" [redacted] "Actor" [redacted]
Date of Request:	21/07/2022
Date of Conclusion:	10/08/2022
Report commissioned by:	[redacted] – [redacted]

Contents Page

10. All exhibits in printed .pdf

Background to the Case

OrbitGTM operates as a fraudulent broker service and trading platform. The bad actors started by setting up an [redacted] German bank account. Then they had the victim send assets in EUR from their personal and business accounts. Then the actors would connect to the victims device via "AnyDesk" and send the assets to various bank accounts around Europe. The actors convinced the victim to set up a [redacted] account and defrauded them of virtual assets for various services that were fake or fraudulent. When trying to withdraw the assets from the OrbitGTM platform there were always paywalls to overcome to gain access to assets which never gets released.

1. Scope of the report

The scope of this report is limited to:

	Included in report
1	Investigation of publicly available information of accused.
2	Collection of evidence related to the investigation.
3	Proof of ownership of stolen assets.
4	Tracking and tracing of stolen assets to withdrawal address.
5	Investigation of stolen BTC virtual asset on the Bitcoin blockchain.

2. Entities and evidence exhibits

[redacted] is referred to as the "victim".

The owner of orbitgtm-pros.com, the various "actors" related, [redacted] and [redacted] referred to as the "accused".

All exhibits with the prefix "OG" are related to the "accused".

All exhibits with the prefix "HN" are related to the "victim".

All exhibits with the prefix "CT" are constructed by the "investigator".

All blockchain wallet addresses and transaction hashes will be abbreviated to 7 digits, full addresses and transaction hashes can be referred to in the exhibits.

	Exhibits submitted	
OG1	Email regarding the transfer of 15000 EUR	29 June 2021 11-57.eml
OG2	Email – showing test withdrawal	04 June 2021 10-52.eml
OG3	Email – showing use of "anydesk"	23 July 2021 11-26.eml
OG4	Email – not to mention OrbitGTM	09 July 2021 13-29.eml
OG5	Email – request for money	05 August 2021 14-08.eml
OG6	Email – new fake investment options	09 August 2021 16-58.eml
OG7	Email – introducing "Actor" [redacted]	12 August 2021 18-10.eml
OG8	Email – confirmation off 100000 EUR transfer	26 October 2021 12-14.eml
OG9	Email – sign up to [redacted]	21 October 2021 09-43.eml

OG10	Email – mentions company loan from OrbitGTM	09 December 2021 11-40.eml
OG11	Email – problems start	27 January 2022 14-20.eml
OG12	Email – problems start	27. January 2022 12-01.eml
OG13	Email – service payment request	02 February 2022 13-46.eml
OG14	Email – problems with contractor and [redacted] bank	04 February 2022 10-10.eml
OG15	Email – OrbitGTM is a dealership that provides you with access to market assets via various contractors	04 February 2022 13-51.eml
OG16	Email – invoice to be paid to reopen account for withdrawals	18 February 2022 12-54.eml
OG17	Email – request for withdrawal after paying invoice	23 February 2022 10-26.eml
OG18	Email – final correspondence from "actors" claiming they will prepare the amounts to be available	23 February 2022 12-08.eml
OG19	Email – "victim" sending multiple emails requesting withdrawal	25 February 2022 12-20.eml
OG20	Email – "victim" attempts to contact [redacted]	01 March 2022 12-32.eml
OG21	Invoice for brokerage commission and fees	UPGR_BSIS.pdf
HN1	[redacted] pdf bank statement	[redacted] statement-2021-07.pdf
HN2	[redacted] pdf bank statement	[redacted] statement-2021-08.pdf
HN3	[redacted] pdf bank statement	[redacted] statement-2021-09.pdf
HN4	[redacted] pdf bank statement	[redacted] statement-2021-10.pdf
HN5	[redacted] pdf bank statement	[redacted] statement-2021-11.pdf
HN6	[redacted] pdf bank statement	[redacted] statement-2021-12.pdf
HN7	[redacted] pdf bank statement	[redacted] statement-2022-01.pdf
HN8	[redacted] pdf bank statement	[redacted] statement-2022-02.pdf
HN9	[redacted] pdf bank statement	[redacted] statement-2022-04.pdf
HN10	[redacted] pdf bank statement	[redacted] statement-2022-05.pdf
HN11	[redacted] pdf bank statement	[redacted] statement-2022-06.pdf
HN12	[redacted] pdf bank statement	[redacted] statement-2022-07.pdf
HN13	Email – [redacted] Bitcoin purchase confirmation	25.01.2022 - Bank Transfer - Fwd_ BTC purchase request confirmed.eml
HN14	Email – [redacted] withdrawal confirmation	04.11.2021 - Bitcoin - BTC withdrawal request confirmed.eml
HN15	[redacted] fiat transactions	fiat_transactions_record_20220801_182311.csv
HN16	[redacted] crypto transaction records	crypto_transactions_record_20220801_182637.csv
CT1	[redacted] IBAN -BIC details	[redacted] - IBAN info.docx
CT2	[redacted] Companies House details	[redacted] companies house.pdf
CT3	Flow chart of BTC transfers	OrbitGTM Investment Broker Fraud.png
CT4	Tracing of assets to centralized exchange	Tracking of assets reported as stolen.xslx

CT5	OrbitGTM reconnaissance	OrbitlGTM Recon.docx
CT6	Transfers between wallet addresses	Connection transfers of bc1q7cyrfmck2ffu2ud3rn5l5a8yv6f0chkp0zpemf to 1EXTEeZZEoFvc8qASpFXpyhBKxjFUuojV6.xlsx
CT7	Transfers between wallet addresses	Connection transfers of 1EXTEeZZEoFvc8qASpFXpyhBKxjFUuojV6 to 1AS5SVLLjCvrcLkPAMPtFWkkYV52B6pzGj.xlsx
CT8	Transfers between wallet addresses	Connection transfers of 1EXTEeZZEoFvc8qASpFXpyhBKxjFUuojV6 to 1NvQiipvSyxLVGHzHZvb9wR86ehzoT6TyC.xlsx
CT9	Transfers between wallet addresses	Connection transfers of 1EXTEeZZEoFvc8qASpFXpyhBKxjFUuojV6 to 18fuPg464LjER2bcz8KYWsibbo1K14gkMa.xlsx
CT10	Transfers between wallet addresses	Connection transfers of 18fuPg464LjER2bcz8KYWsibbo1K14gkMa to 3KPsEHC47uYT9gsmYYb6vbVHVJUPv6G2Je.xlsx
CT11	Transfers between wallet addresses	Connection transfers of 1NvQiipvSyxLVGHzHZvb9wR86ehzoT6TyC to 3KPsEHC47uYT9gsmYYb6vbVHVJUPv6G2Je.xlsx
CT12	Transfers between wallet addresses	Connection transfers of 1AS5SVLLjCvrcLkPAMPtFWkkYV52B6pzGj to 3KPsEHC47uYT9gsmYYb6vbVHVJUPv6G2Je.xlsx
CT13	Transfers between wallet addresses	Connection transfers of 1AS5SVLLjCvrcLkPAMPtFWkkYV52B6pzGj to 32L1aAb2hawK56x65dfxYu5DKjkFC6hpJA.xlsx
CT14	Transfers between wallet addresses	Connection transfers of 3KPsEHC47uYT9gsmYYb6vbVHVJUPv6G2Je to 1L15W6b9vkxV81xW5HDtmMBycrdiettHEL.xlsx
CT15	Transfers between wallet addresses	Connection transfers of 3KPsEHC47uYT9gsmYYb6vbVHVJUPv6G2Je to 1L1xSXttdsBAPVjVfyoyCg3RZbdHinT5G5.xlsx
CT16	Transfers between wallet addresses	Connection transfers of 32L1aAb2hawK56x65dfxYu5DKjkFC6hpJA to 1L1xSXttdsBAPVjVfyoyCg3RZbdHinT5G5.xlsx

Further information required relative to the investigation

1	Information relating to the ownership of the following telephone numbers: [redacted]
2	Information from ddos-guard.net relating to the ownership of the domain OrbitGTM-pros.com
3	Questioning of [redacted] the director of [redacted] of which OrbitGTM is a trading name for possible association to crimes
4	Questioning of [redacted] the director of [redacted] a company registered in England and Wales for possible association to crimes
5	The German Bank [redacted] should be investigated for being potentially complicate due to relaxed due diligence done
6	Report should be sent to law enforcement in all relevant jusridictions
7	Further investigation required into the Crypto Conduct Authority and its association

8	Information from alleged exchange [redacted] relating to the ownership of the account where received transfers by address '1L15W6b..' are sent transfers by address '3KPsEHC..' for further investigation by law enforcement
9	Information from alleged exchange [redacted] relating to the ownership of the account where received transfers by address '1L1xSXt..' are sent transfers by addresses '32L1aAb..' and '3KPsEHC..' for further investigation by law enforcement

3. Evidence searched for

Evidence was collected from the victim including correspondence emails, bank statements, virtual asset proof of ownership. Evidence was gathered on publicly available data relating to OrbitGTM and then subsequently [redacted] as the registered business name of the trading name OrbitGTM.

4. List of Criminal Offence

The criminal offences facing the accused are:

Money Laundering, Fraud, Theft, organized crime activities.

5. Breach

Use of social engineering to convince the victim to invest assets into a fake platform and then payment was needed in order to release assets for withdrawal. No assets were ever returned to the victim.

6. Investigation details

I started the investigation by examining the evidence collected from the victim and focused on the transfers into and out of the [redacted] bank account (exhibits HN1-12) and email correspondence to verify the claim of fraud and found lots of data relating to transfers to various bank accounts around Europe including Bulgaria, Spain, Poland, and Lithuania and the United Kingdom. The total transferred to the European banks was 211000 EUR (exhibit CT1). There was one deposit from what the victim claimed was an OrbitGTM platform "test" withdrawal (exhibit OG2) when in fact the transfer into the [redacted] bank account was form a company registered in England and Wales [redacted] (exhibit CT2). The victim claims that the IBAN numbers and related details were input by the accused using "AnyDesk" (exhibit OG3). The accused asked the victim not to mention "OrbitGTM" if any banks were to call (exhibit OG4). In October 2021 the victim was introduced to virtual assets by way of a 7.5% bonus on the amount deposited (exhibit OG9), all further transactions were deposits to [redacted] (exhibit HN15) and then to a private wallet on the Bitcoin blockchain (exhibits HN13, HN14).

When it came to trying to withdraw assets in January 2022 there were problems withdrawing (exhibits OG11, OG12). The accused went on to say that "OrbitGTM is a dealership that provides you with access to market assets via various contractors" and that the problems lied with these contractors and the previously recommended bank [redacted] (exhibits OG14, OG15). On February 18th 2022 the accused sent another email with an Invoice for brokerage commission and fees to the value of $77,187.29 (exhibits OG16, OG21) before assets could be withdrawn from the OrbitGTM platform. This amount was paid using Bitcoin on February 21st 2022 and was sent to wallet address '1EXTEeZ..' from the victims [redacted] account.

These Bitcoin transfers can be followed on a public blockchain explorer like blockchain.com using a transaction hash like the ones in the crypto transactions record exported from [redacted] (exhibit HN16). Analyzing the blockchain data I could determine a total amount of Bitcoin sent to the fraudulent service provider is 9.7340268 BTC and a total value at the times of purchase is 369800.24

EUR. In this case the stolen virtual assets were transferred from the wallet address '1EXTEeZ..' to '18fuPg4..', '1NvQiip..' and '1AS5SVL..' in order to mix the stolen virtual assets with other virtual assets accumulated by other means. The virtual assets were then transferred to two more wallet addresses '3KPsEHC..' and '32L1aAb..' in order to be mixed again with virtual assets accumulated by other means. The virtual assets are then transferred to withdrawal addresses '1L15W6b..' and '1L1xSXt..' allegedly controlled buy the centralized exchange [redacted] (exhibit CT3, CT4).

Reconnaissance was done on the domain and associated links. The IP address for orbitgtm-pros.com is (185.178.208.152), the hosting provider is ddos-guard.net. OrbitGTM is a trading name of [redacted] a company registered in Dominica. Orbit GTM joined the Crypto Conduct Authority on 02.07.21, membership active. Various phone numbers, addresses and email addresses linked to OrbitGTM (exhibit CT5).

7. Conclusion

- The victim has been defrauded of 211000.00 EUR and 9.7340268 BTC (369800.24 EUR) total value 580800.24 EUR by the accused
- I was able to track and trace the virtual assets to the alleged exchange [redacted] which implements a Know-Your-Customer and Anti-Money-Laundering Policies
- The virtual assets were mixed with other obtained virtual assets and transferred through various wallet addresses and deposited into the withdrawal addresses '1L15W6b..' and '1L1xSXt..' controlled by alleged exchange [redacted]
- Further investigation by law enforcement is required to reveal the identities of the accused from the possible sources
- From the analysis of a available evidence and is likely a large well organized group in overall control and is to be taken very seriously

8. Generated Material

- Microsoft word document of [redacted] IBAN -BIC details related to the case
- Printed pdf from Companies House [redacted] company details
- Flow chart of stolen virtual assets image presented in .png format
- Microsoft excel document of assets traced to centralized exchange
- Microsoft excel document of OrbitGTM reconnaissance
- Ten Microsoft excel documents of Transfers between wallet addresses (exhibits CT6-CT15)
- PDF printouts of all exhibits

9. **Glossary**

Address

A digital destination used to send and receive cryptocurrency funds. Cryptocurrency wallets can contain many addresses inside. Addresses vary depending on the specific blockchain it live on.

Block

An entry of the cryptocurrency transactions that have been made in a certain time frame. A new block is validated approximately every 10 minutes on the Bitcoin network and becomes part of the blockchain. The blockchain is a sequence of connected data blocks.

Block Explorer

A website for viewing public blockchains and transaction information such as status and confirmation time. Blockchain.com and Etherscan.io are two examples of block explorers.

Bridge

Also known as a cross-chain bridge, a bridge allows the transfer of assets from one blockchain to another (e.g., Ethereum to Polygon). Bridges can be operated by a centralized entities or through the use of a smart contract to facilitate the transfer in a decentralized process.

Cluster

A collection of cryptocurrency addresses that various data sources has been identified to be controlled by one entity.

Cold Wallet

A type of wallet that is not connected to the internet. This is also referred to as cold storage.

Counterparty

The other party that participates in a cryptocurrency transaction.

Custodial Wallet

A type of wallet in which a company or organization holds cryptocurrency assets and private keys on behalf of their users.

DAO

Also known as a decentralized autonomous organization, a DAO is an entity with no centralized decision makers. Instead, DAOs consist of a group of people who come together for a specific purpose without any one group or entity having full control. DAOs are built and run on a blockchain through the use of smart contracts which defines the rules and protocols of the DAO.

Exposure

The relationship between addresses and other entities that is created through your transfers to and from other addresses. Exposure is an important component in measuring your risk levels.

Hosted Wallet

A wallet that resides on a third-party service, for example a centralized exchange. The third-party service may hold both the user's private and public keys.

Input

The cryptocurrency address from which funds were sent (the source of the coins in a single transaction). An input is also a reference to an output from a previous transaction.

Mining

The process by which transactions are validated and issued on the blockchain network. Miners receive a reward of cryptocurrency when they successfully add a block to the blockchain.

Mixing

Coin mixing could refer to any activity that involves the obfuscation of funds by substituting them with others. Coin mixing is commonly done by third party service providers for a fee. Multiple users assets are combined into one transaction and distributed. This can be done by hand for technically-proficient users. The user will take all of the information, craft it into a transaction, transfer to multiple addresses then collecting the assets in a wallet or service.

NFT

Also known as a non-fungible token, an NFT is unique code stored digitally on a blockchain. An NFT can only have one owner, and the owner is visible to everybody due to the public nature of blockchain technology. Users can purchase and sell NFTs using cryptocurrency on NFT marketplaces

Node

A participant in the blockchain network that verifies and stores transactions. There are numerous types of nodes that have different functions on varying blockchains.

Output

The cryptocurrency destination addresses for funds, i.e. where funds are being sent. There can be multiple inputs and outputs for a single transaction.

Private Key

A secret alphanumeric string that allows the user to access the funds at a single corresponding address. Wallets contain one or more private keys.

Private Wallet

A type of wallet that allows the user to manage their own addresses and private keys.

Public Key

An alphanumeric string that is used to derive an address. The public key is only publicly known if currency has been spent from its corresponding address.

Smart contract

Programs stored on a blockchain that run when predetermined conditions are met and verified. An example is a DEX (Decentralized Exchange) smart contract that facilitates the exchange of cryptocurrency between two people.

Transaction

A transaction consists of one or more fund transfers. On most blockchains a transaction comprises of a unique transaction ID (the transaction hash), inputs which are the source of the coins and outputs which are the destinations of the virtual assets.

Transaction Hash

Also known as a transaction ID, the transaction hash is a unique identifier of a transaction.

VASP

An acronym for Virtual Asset Service Provider.

Virtual Asset

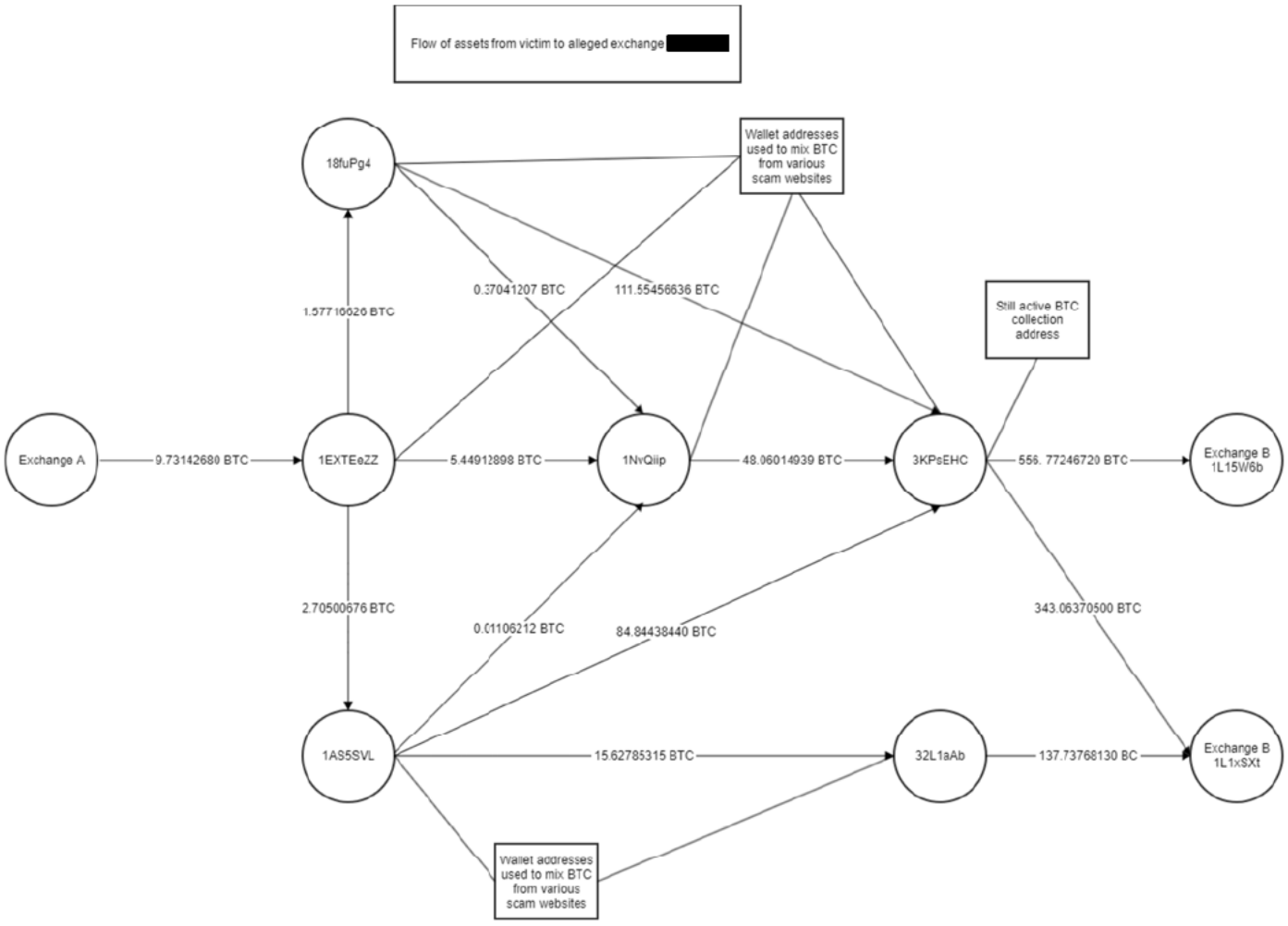
The type of cryptocurrency used in a transfer (Bitcoin, Ethereum, etc.). Can also refer to non-fungible representations of value (e.g. NFTs).

Wallet

A software program that generates and stores a user's addresses and private keys. It is used to send and receive cryptocurrency and monitor balances.

10. All exhibits printed in .pdf

Exhibit CT3


Flow of assets from victim to alleged exchange [redacted]
18fuPg4
Wallet addresses used to mix BTC from various scam websites
0.37041207 BTC
111.55456636 BTC
1.577 10026 BTC
Still active BTC collection address
Exchange A
9.73142680 BTC
1EXTEeZZ
5.44912898 BTC
1NvQiip
48.06014939 BTC
3KPsEHC
556. 77246720 BTC
Exchange B 1L15W6b
2.70500676 BTC
0.01106212 BTC
84.84438440 BTC
343.06370500 BTC
1AS5SVL
15.62785315 BTC
32L1aAb
137.73768130 BC
Exchange B 1L1xSXt
Wallet addresses used to mix BTC from various scam websites