

Ransomware Incident Investigation and Cryptocurrency Tracking with OSINT

About Us

- Kelvin WONG, aka Forensics Ninja and independent researcher
- Dr. Zetta KE, Assistant Professor of Information System at SMU
- Anthony LAI, Founder of VXRL and Review Board members of BH Asia, experienced pentester / incident responder
- Alan HO, Co-founder of VXRL and experienced pentester / incident responder

Real Case Study

- Ransomware Incident
- Cryptocurrency Tracing

Background

- Company's Servers and Network Storage were compromised.
- All files was encrypted and backup was encrypted too.
- Attacker demanded 1.5 BTC.
- Our IR Team investigated the incident.

Ransom Note

"All your files are encrypted and cannot be recovered."

All your documents have been uploaded and compromised

COMPANY INFO:

- Company: [REDACTED]
- Website: [http://\[REDACTED\]](http://[REDACTED])
- Address: Country Hong Kong [REDACTED], Hong Kong
Phone [REDACTED]

-What data was received:

Contracts, financial documents, HR documents, client information, etc.
Over 500GB of confidential information.

-What will become of you:

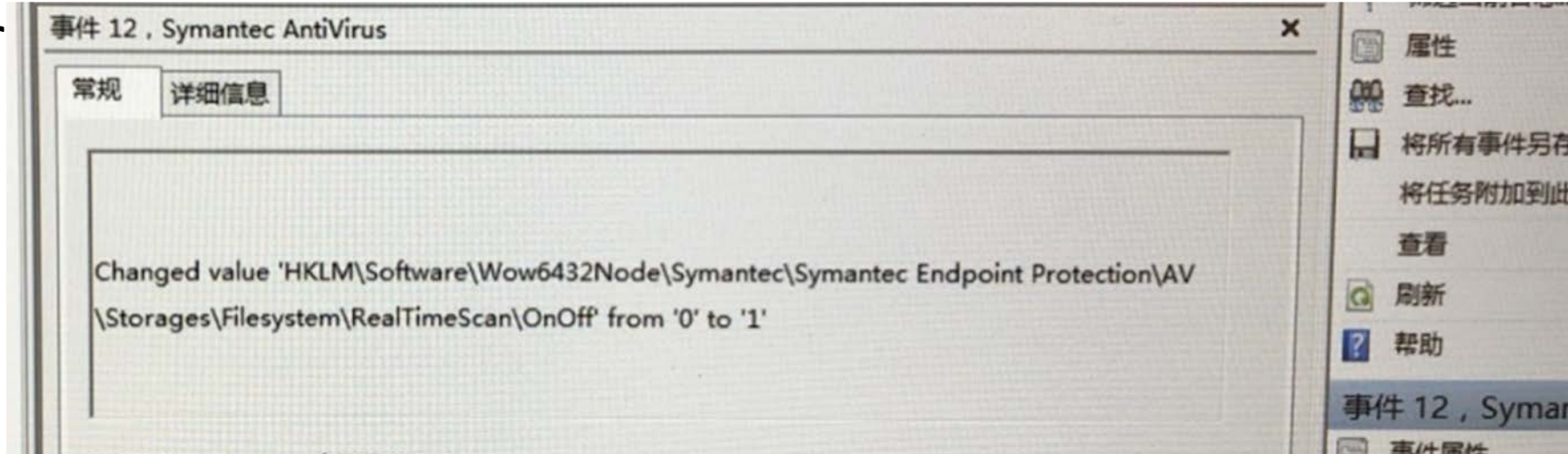
You have 72 hours to get in touch with us, if during this time you do not contact us, all your information will be published in our blog.
Anyone can access it. We will inform the client, employees, and merge your information with other hacker groups.
You will receive multiple lawsuits, suffer huge financial losses, and lose your reputation.

How to get to our page

1. Download Tor browser - <https://www.torproject.org/>
2. Install Tor browser
3. Open link in Tor browser
4. [midasbkic5eyf\[REDACTED\]pmsb2qgux7diqbpa4up4rtdad.onion/link.php?id=rDxy7vEiFx2H\[REDACTED\]](http://midasbkic5eyf[REDACTED]pmsb2qgux7diqbpa4up4rtdad.onion/link.php?id=rDxy7vEiFx2H[REDACTED])
5. Follow the instructions on this page

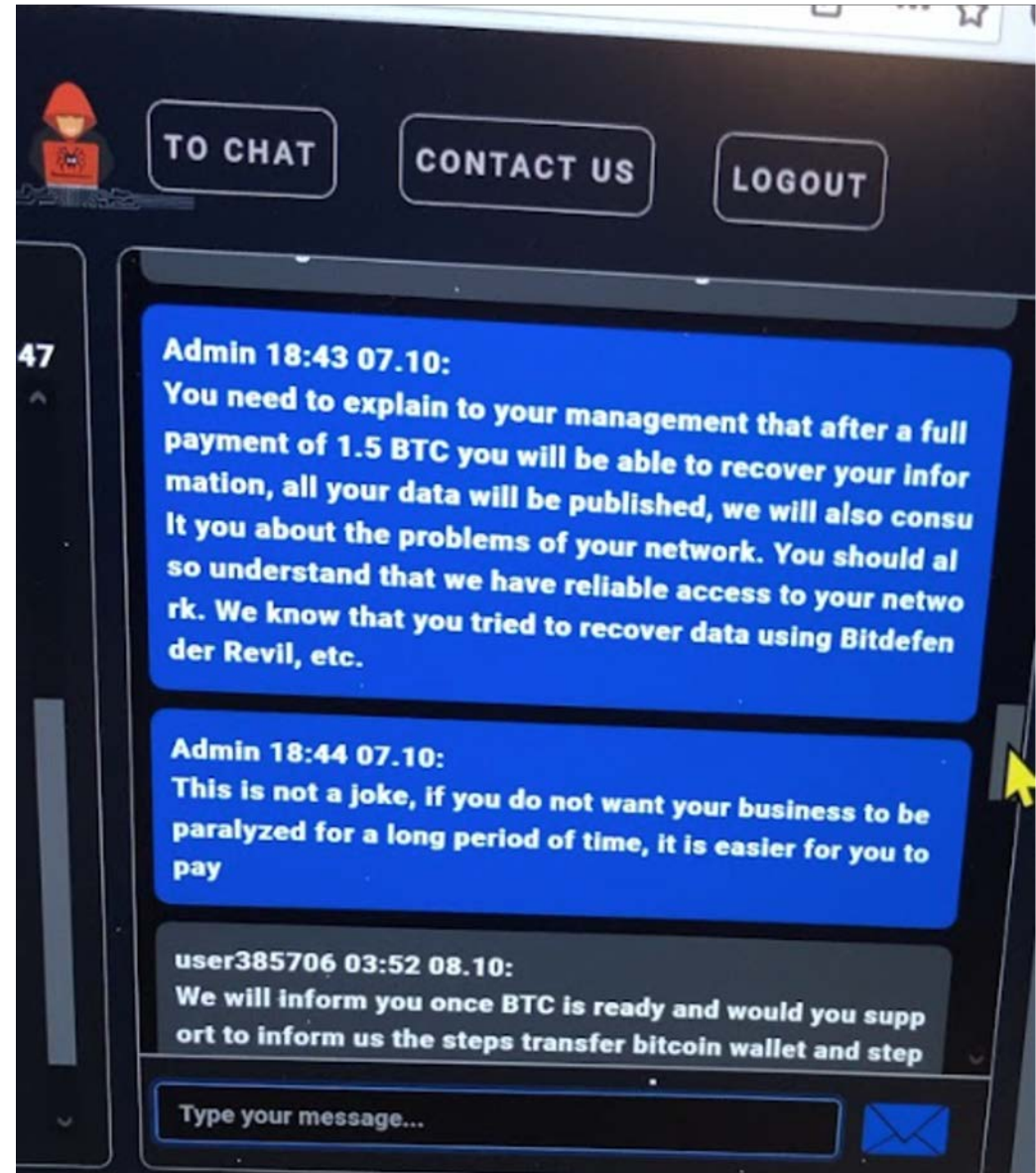
Incident Response

- Attacker preformed Eternal Blue MS17-010 (remote code execution) against the exchange server, then attacker RDP to a desktop in HR department which mapped drives from network storage
- From Windows Event Log, we found that the Attacker disabled Anti-vir



Incident Response

- On the other hand, since there were no backup at all, management from victim company decided to pay the ransom, our IR team negotiated with the Attacker in the chatroom
- Eventually 1.5BTC was agreed.

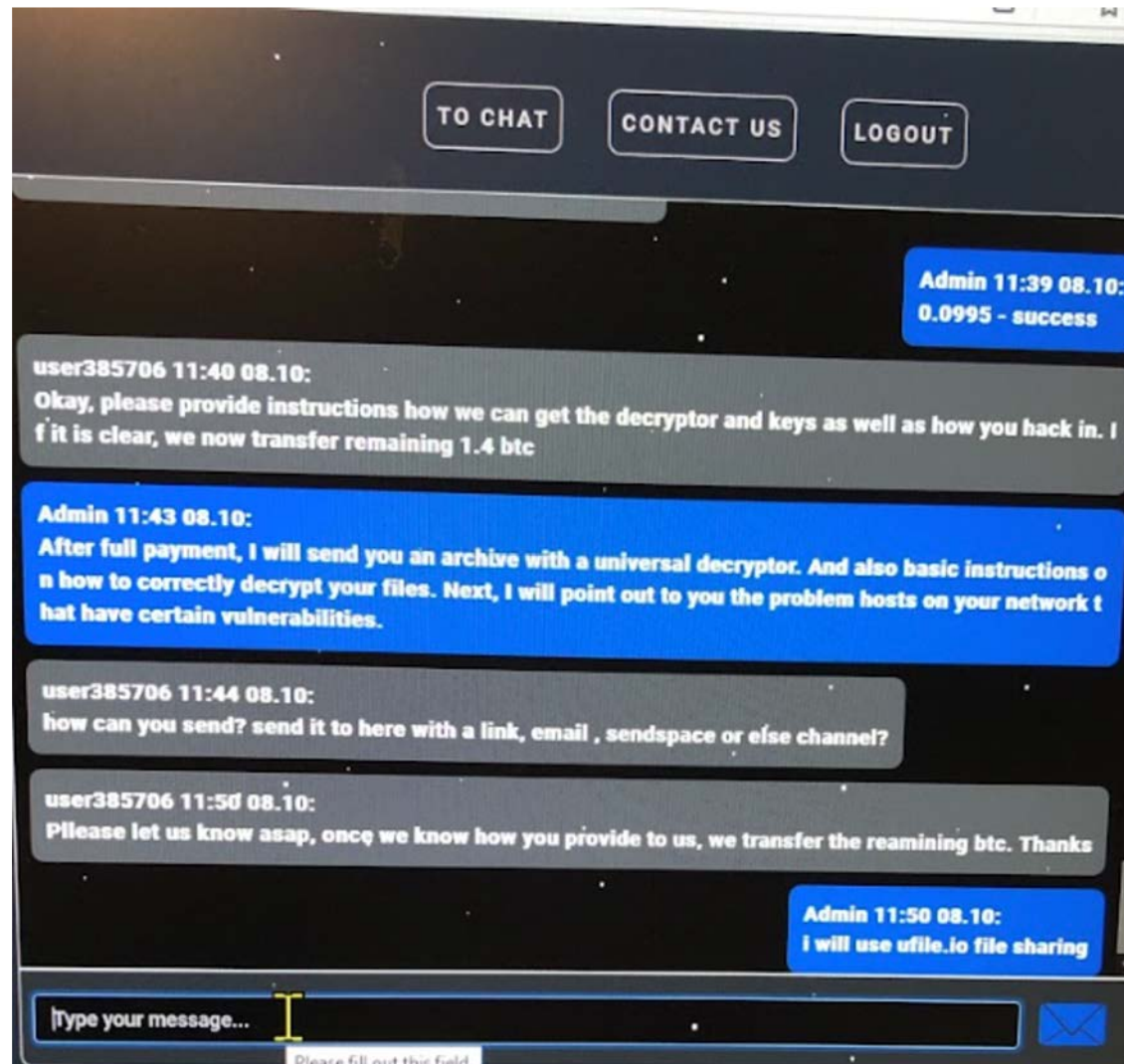


Incident Response

- The following tasks were done
 - To stop further potential attacker, we recommended the company to block any incoming network traffic and compile an inventory list.
 - New firewall and policies were deployed to block malicious traffic

Incident Response

- Paying the Ransom



Negotiation (extracted)

Admin 09:31 08.10:

Use this wallet for a transaction, after full payment you will receive a decryptor and all instructions

Admin 09:31 08.10:

bc1qhlapvqs5nd2mzvvd9s8x4cssnsvlele622ykxe 1.5BTC

user385706 11:38 08.10:

please check the wallet, we have transferred 0.0995 btc.

Admin 11:39 08.10:

0.0995 - success

user385706 11:40 08.10:

Okay, please provide instructions how we can get the decryptor and keys as well as how you hack in. If it is clear, we now transfer remaining 1.4 btc

Admin 11:43 08.10:

After full payment, I will send you an archive with a universal decryptor. And also basic instructions on how to correctly decrypt your files. Next, I will point out to you the problem hosts on your network that have certain vulnerabilities.

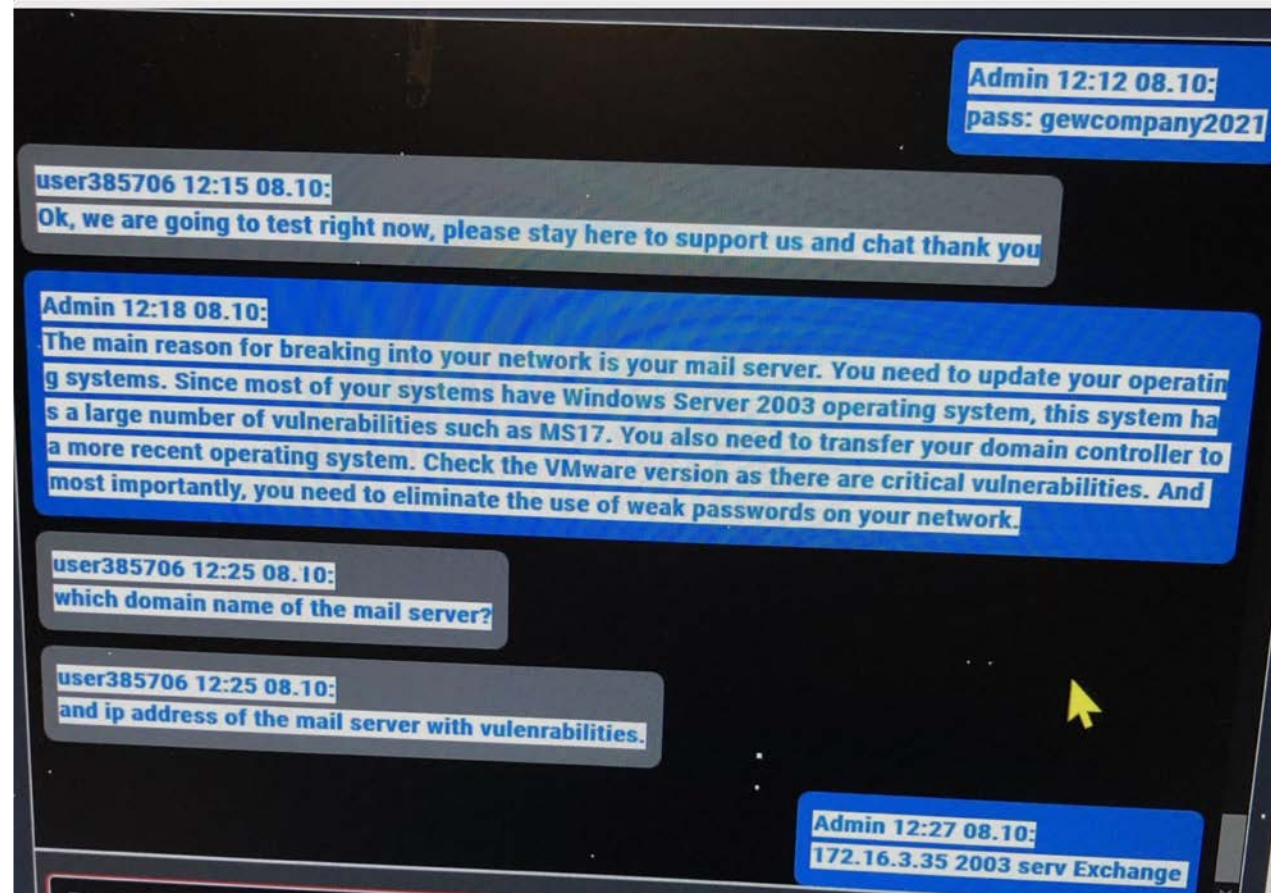
Bitcoin Wallet - bc1qhlapvqs5nd2mzvvd9s8x4cssnsvlele622ykxe

Transactions

- Test “0.1 Bitcoin” same bitcoin wallet address
- 1.4 Bitcoin
- Around 4-5 blocks (15 mins)
- URL ‘ufile.io’ from cloudflare > download decrypter
- Successful

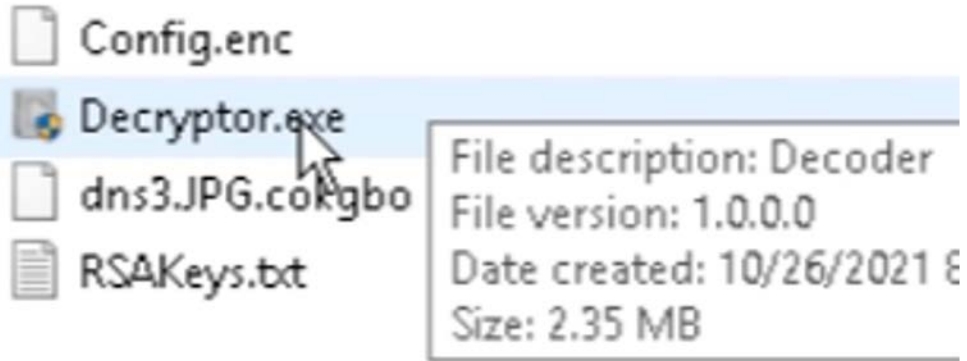
Incident Response

- After paying the ransom, attacker explained how they gained access to the network.

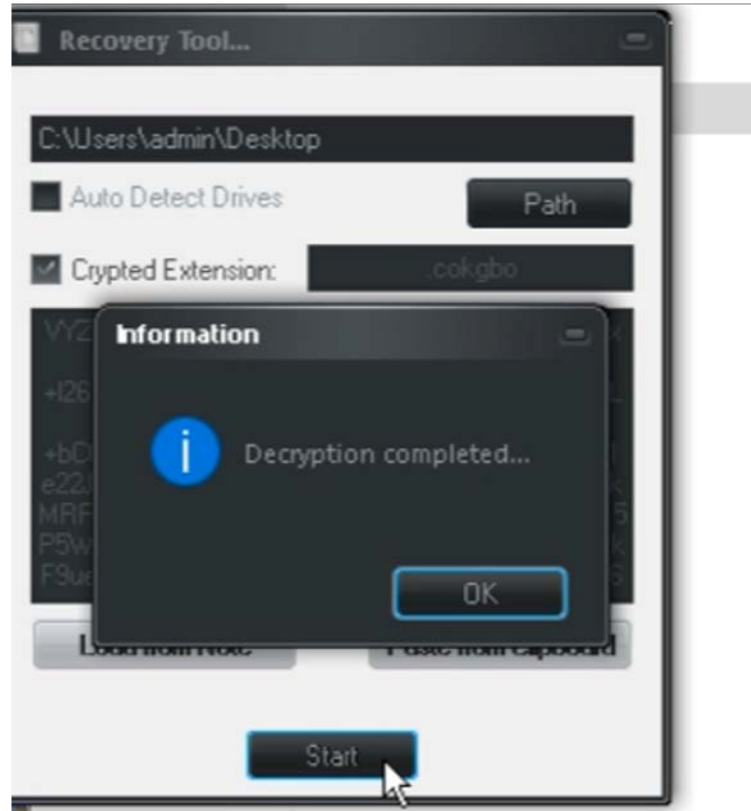


Incident Response

- Decryptor was sent to us, and we tested it. It could decrypt all the encrypted files successfully.



Incident Response



Incident Response

- After the files were restored.
 - Offline storage was deployed to backup files once they're decrypted.
 - Exchange Server was migrated to cloud (Office 365)
 - Desktops were upgrade from Windows 7 or XP to Windows 10
 - Servers were upgraded from Windows Server 2012 to 2019

Ransomware Analysis

- Our team used any.run to execute analyze the ransomware

SHA256

49bc1609d070355ea87a98c1448af64ed692f77a2dbb9f7a9a8eda2903117b96

SHA1

5121af6c222c8198600844c516807a314527e04d

MD5

908eab61ebd2d5c7fd2b2f02c24de42a

Mitre ATT&CK Matrix


Tactics 6 | Techniques 18 | Events 336

All tactics
● Danger (18) ● Warning (147) ● Other ()

Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Collection	C & C	Exfiltration	Impact
	Command and Scripting Interpreter (2/5)	Boot or Logon Autostart Execution (1/9)	Boot or Logon Autostart Execution (1/9)	Indicator Removal on Host (1/5)		Query Registry 75 116					Data Encrypted for Impact 13
	Windows Command Shell 3	Registry Run Keys / Startup Folder 1	Registry Run Keys / Startup Folder 1	File Deletion 1		System Information Discovery 4 53					Service Stop 1 47
	PowerShell 1			Signed Binary Proxy Execution (1/11)							
	System Services (1/1)	Scheduled Task/Job (1/2)	Scheduled Task/Job (1/2)	Mshta 1		Software Discovery (0/1) 1					
	Service Execution 7	Scheduled Task 2	Scheduled Task 2	Virtualization/Sandbox Evasion (1/3)		System Service Discovery 7					
	Scheduled Task/Job (1/2)			Time Based Evasion 1		Virtualization/Sandbox Evasion (1/3)					
	Scheduled Task 2					Time Based Evasion 1					
	User Execution (1/2)										
	Malicious File 2										

CryptoCurrency Tracing (Commercial Tools)

- Chainanalysis
- CipherTrace



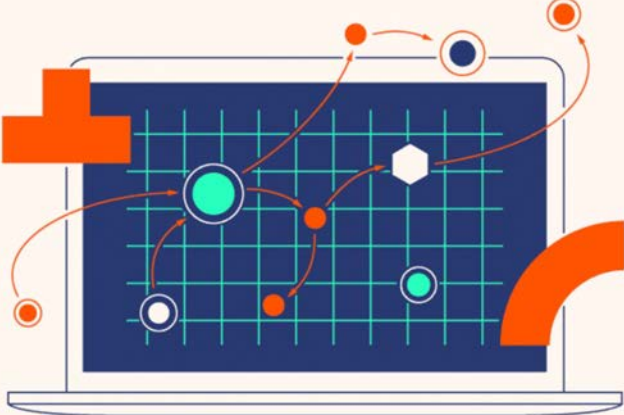
THE BLOCKCHAIN DATA PLATFORM

Empowering you to answer questions about blockchains

Our data platform powers investigation, compliance, and risk management tools that have been used to solve some of the world's most high-profile cyber criminal cases and grow consumer access to cryptocurrency safely.

Organization Type

Select... [Request a demo](#)



CipherTrace is hiring! See our [current job openings](#).

CIPHERTRACE

SOLUTIONS

BLOG

RESOURCES

ABOUT

PRODUCTS

DEMO

CONTACT

CipherTrace Inspector™

CipherTrace Armada™

CipherTrace Sentry™

CipherTrace Traveler™

Tracking Cryptocurrency with OSINT

- BlockChair Explorer
- BitQuery
- OXT.ME



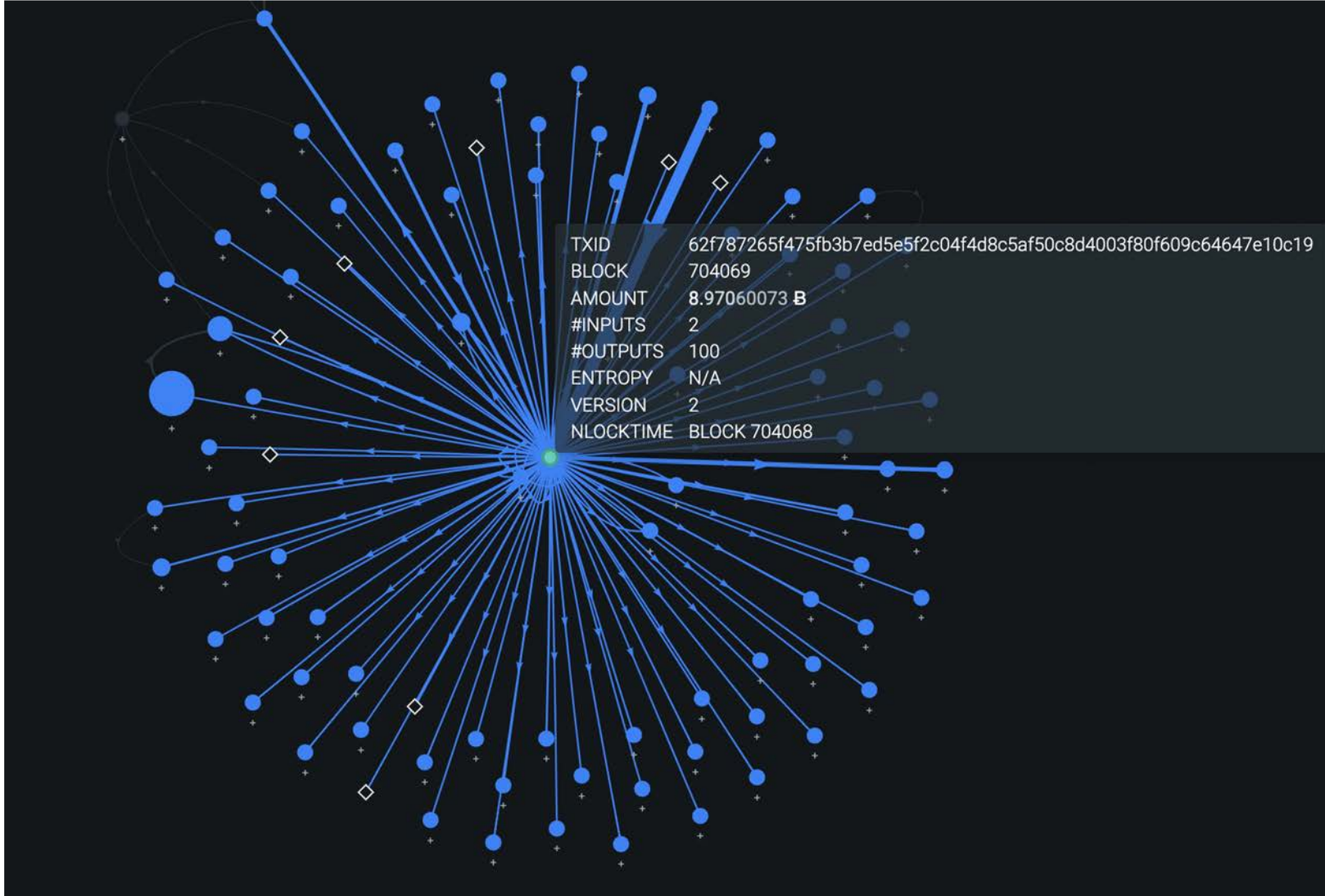
BlockChair Explorer



Address	bc1qhlapvqs5nd2mzvvd9s8x4cssnsvlele622ykxe 
Format	BECH32 (P2WPKH)
Transactions	3
Total Received	1.50000000 BTC
Total Sent	1.50000000 BTC
Final Balance	0.00000000 BTC













Suspect Bitcoin Wallet - bc1qhlapvqs5nd2mzvvd9s8x4cssnsvlele622ykxe

OXT.ME

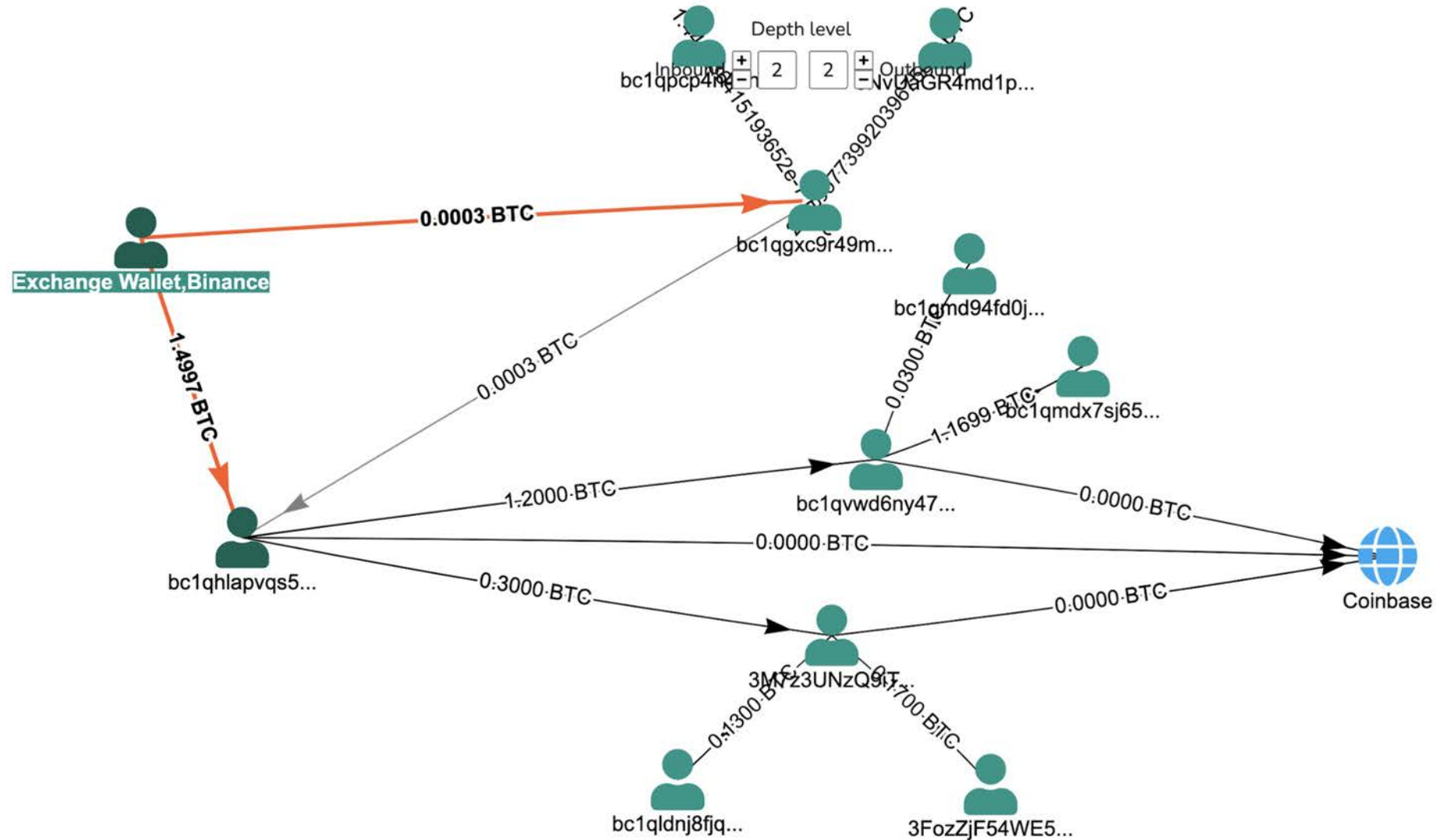


Use of OXT.me

TOOLS

-  - Display/hide transaction details
-  - Display/hide transaction and TXO details (fingerprint mode)
-  - Display/hide comments
-  - Display/hide marked transactions and TXOs
-  - Pause the graph animation
-  - Re-center the graph
-  - Reset the graph
-  - Clear the list of selected transactions (login required)
-  - Export selected transactions to CSV (login required)
-  - Export selected transactions to JSON (login required)
-  - Download a screenshot of the graph (login required)
-  - Bookmark the graph (login required)

Bitquery



Anonymous?

- Pseudo-Anonymity
- IP Address in RU
- Cash Out
- Big Data
- Know Your Customer (KYC)
- DeFi or CeFi

Thank You

Questions?

hello@vxrl.hk

www.vxrl.hk

