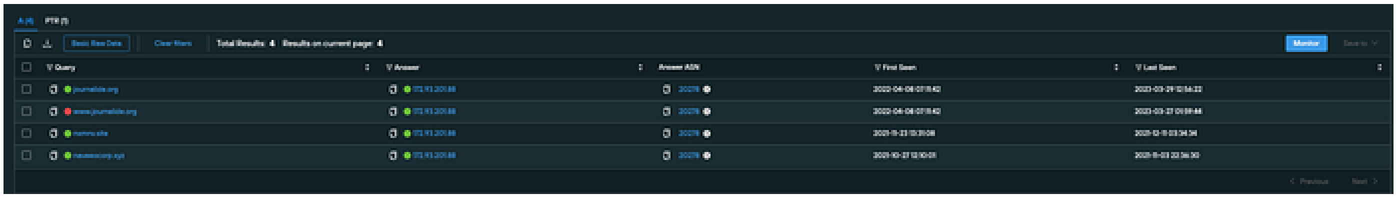
DPRK UNC3782

medium.com/@meeswicky1100/dprk-unc3782-d66329e5c071

Mees van Wickeren

November 9, 2025



Total Results: 4 Results on current page: 4

Query	Answer	Answer ASN	First Seen	Last Seen
journalide.org	172.93.201.88	20278	2022-04-08 07:11:42	2023-03-29 12:56:22
www.journalide.org	172.93.201.88	20278	2022-04-08 07:11:42	2023-03-27 01:59:44
nxmnv.site	172.93.201.88	20278	2021-11-23 10:35:08	2021-12-11 03:34:34
nauseascorp.xyz	172.93.201.88	20278	2021-10-27 12:10:01	2021-11-03 22:36:30

Executive summary

UNC3782 has targeted Naver Corp through hundreds of Naver typosquat phishing domains throughout 2021 and up until the end of 2022. In late 2022, UNC3782 briefly created some cryptocurrency domains, marking the first time UNC3782 had created different domains compared to their previous TTPs. The cryptocurrency-themed domains are live as of today and are believed to target NFT and Cryptocurrency holders We have discovered 19 unique email addresses that we believe are part of UNC3782 campaigns and we found 1983 unique hostnames. The extensive targeting of Naver CORP, cryptocurrency websites, and the overlap that Mandiant has seen with the DPRK APT43 (Kimsuky) makes UNC3782 a very interesting cluster. It remains unclear whether UNC3782 is APT43.

Background

In a blog from Mandiant from April 2023 named *"3CX Software Supply Chain Compromise Initiated by a Prior Software Supply Chain Compromise; Suspected North Korean Actor Responsible*are some interesting indicators shared which are attributed to UNC4736 and UNC3782.

2022–04–08`journalide[.]org`UNC4736

2021-11-26`nxmnv[.]site`UNC3782

Table 2: Resolutions for IP 172.93.201[.]88

In my research, I will uncover unreported domains, IP addresses, and emails from UNC3782.

Tool Usage

- Silent Push Platform
- Python scripts to pull data from Silent Push API

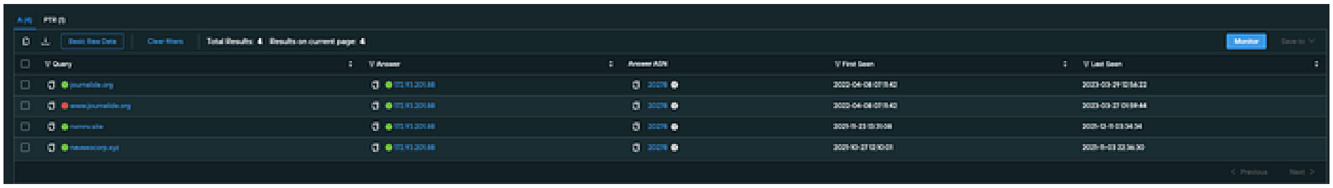
- Virtual safe environment

The rabbit hole

Before we dive into the pivots, I want to share some of my **research experiences**. It’s always a surprise: will you constantly hit **dead ends**, or stumble upon a **massive rabbit hole** that yields tons of indicators over time? Luckily, this time we’ve found the latter. **Enjoy the read!**

First Pivots on late 2021 Indicators

By traveling to the dedicated ip which is mentioned in the Mandiant report we see another domain naveeocorp[.]xy z that was observed in the same period of the domain `nxmnv[.]site`

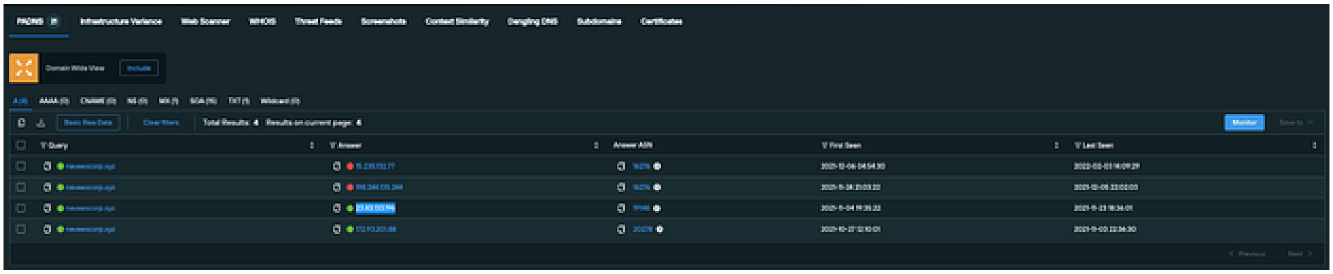


Total Results: 4 Results on current page: 4

Query	Answer	Answer ASN	First Seen	Last Seen
journalide.org	172.93.201.88	20278	2022-04-08 07:11:42	2023-03-29 12:56:22
www.journalide.org	172.93.201.88	20278	2022-04-08 07:11:42	2023-03-27 01:59:44
nxmnv.site	172.93.201.88	20278	2021-11-23 13:31:08	2021-12-11 03:34:34
naveeocorp.xyz	172.93.201.88	20278	2021-10-27 12:10:01	2021-11-03 22:36:30

https://explore.silentpush.com/enrichment/ipv4/172.93.201.88

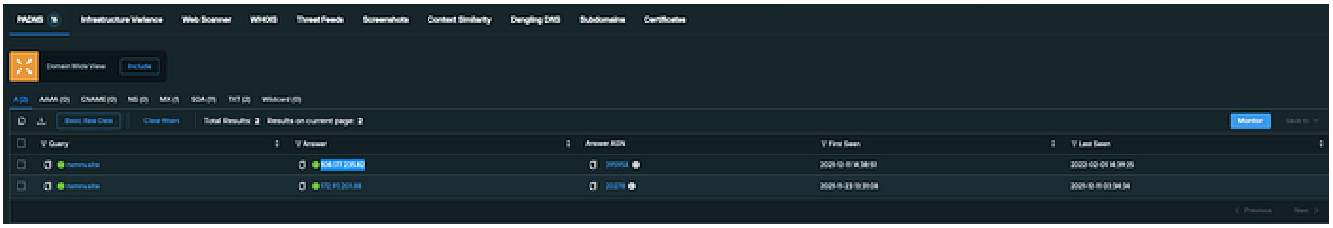
Looking up all A-records of both domains we can uncover new IPs 23.83.133[.]196 and 108.177.235[.]82



Total Results: 4 Results on current page: 4

Query	Answer	Answer ASN	First Seen	Last Seen
naveeocorp.xyz	15.235.132.77	16276	2021-12-06 04:54:30	2022-02-03 14:09:29
naveeocorp.xyz	198.244.135.244	16276	2021-11-24 21:03:22	2021-12-06 22:02:03
naveeocorp.xyz	23.83.133.196	19148	2021-11-04 19:35:22	2021-11-23 18:36:01
naveeocorp.xyz	172.93.201.88	20278	2021-10-27 12:10:01	2021-11-03 22:36:30

https://explore.silentpush.com/enrichment/domain/naveeocorp.xyz

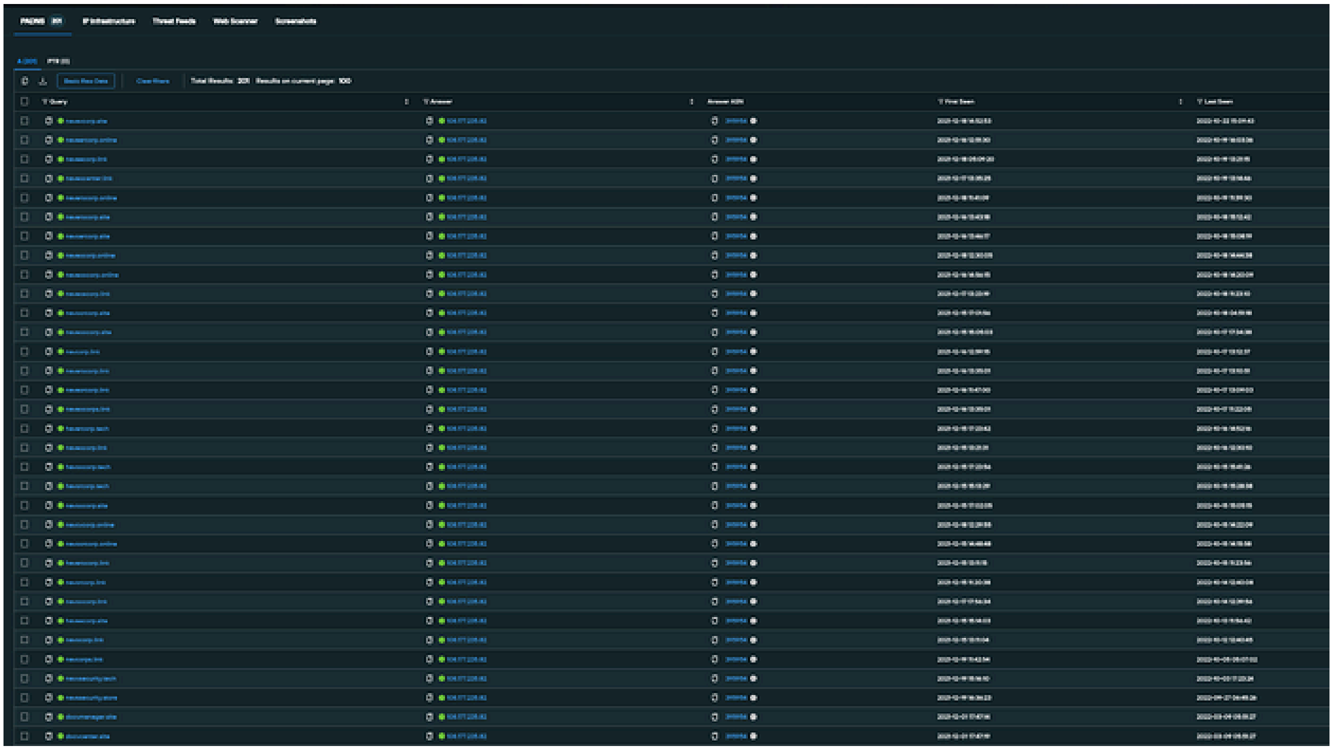


Total Results: 2 Results on current page: 2

Query	Answer	Answer ASN	First Seen	Last Seen
nxmnv.site	108.177.235.82	395954	2021-12-11 14:38:51	2022-02-01 14:39:25
nxmnv.site	172.93.201.88	20278	2021-11-23 13:31:08	2021-12-11 03:34:34

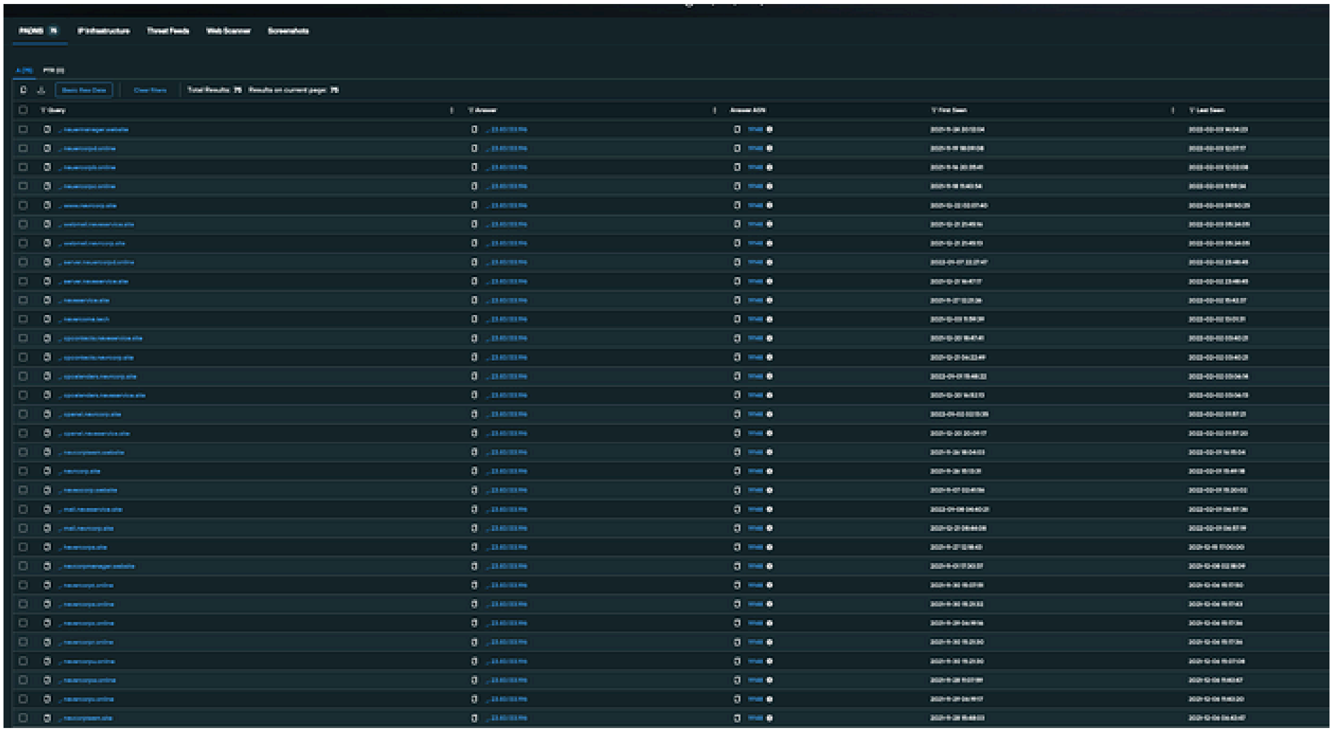
https://explore.silentpush.com/enrichment/domain/nxmnv.site

108.177.235[.]82 reveals 201 A-records in the same period of time that UNC3782 shifted the domain from 172.93.201[.]88 over. Tons of the domains are typosquats of NAVER Corp. Since the Domains are this many, I will parse all of them in Appendix A: First Pivots



https://explore.silentpush.com/enrichment/ipv4/108.177.235.82

Repeating the same process for the other dedicated IP again reveals tons of NAVER Corp phishing domains



https://explore.silentpush.com/enrichment/ipv4/23.83.133.196

OPsec mistakes in the WHOIS

Actors often make mistakes while registering a domain. Well we found 271 hostnames which are listed in Appendix A. We just quickly chucked these hostnames in two WHOIS queries to lookup in the WHOIS datasource from Silent Push. Query 1 and Query 2

Appendix B will include the full results and here I will highlight the interesting findings here below.

```
                                                 // :                // :                      // :
// :              // :               // :           // :
```

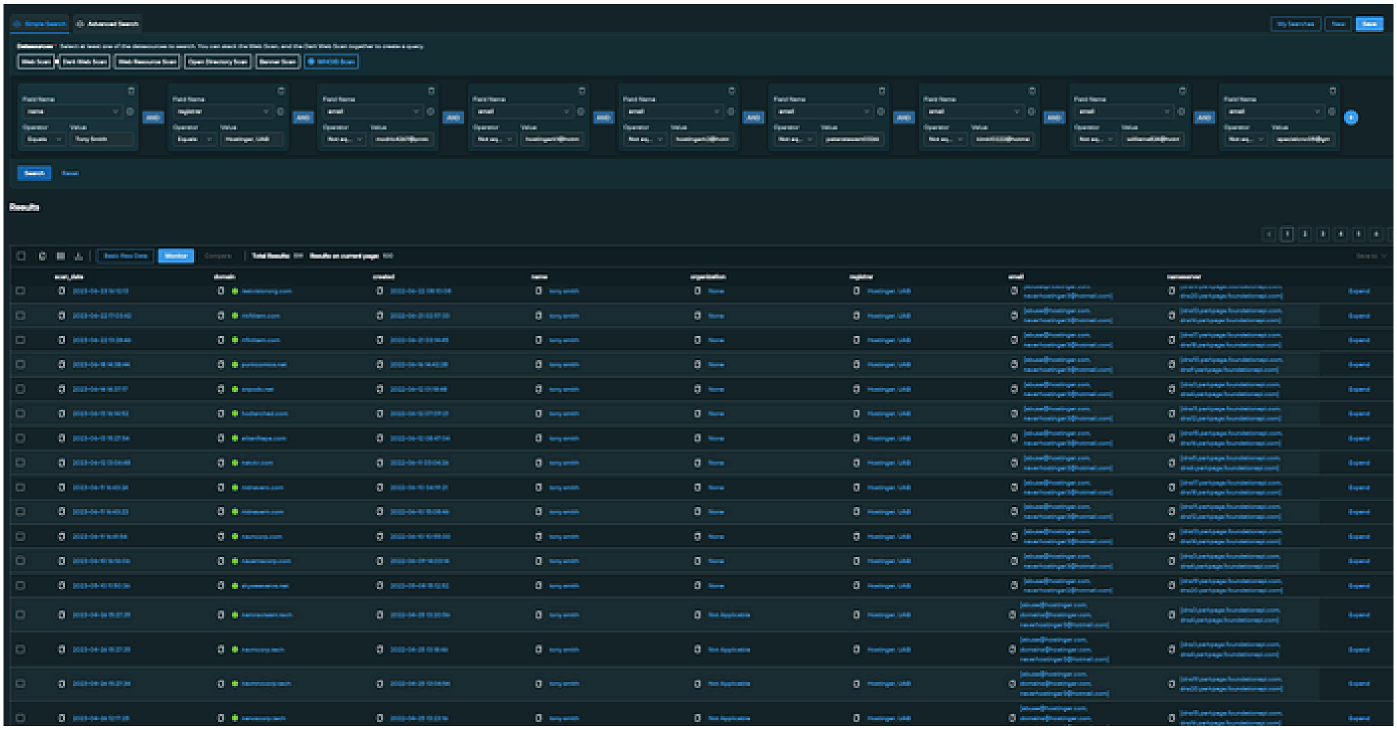
We have discovered 7 unique emails in the WHOIS that we believe are dedicated to UNC3782. Further more 3 interesting values were found in the ‘name’ value field. First of Tony smith. Why is this interesting? Well it is interesting since it has been used several times so there is a pattern there. Also there are two different emails hostingerk1[@]hotmail[.]com and hostingerk2[@]hotmail[.]com which indicate that their might be a third and fourth. Before we dive into this pattern lets first go into the other two interesting values.

The values “Kil Nyeon Kim” and “junseog son” sound very Korean. I am not a fluent Korean translator, so I will leave this mystery to other experts :). Let’s see what we can find more…

Filter what you know to keep oversight

By creating a WHOIS query finding any WHOIS Record with the value name ‘Tony Smith’ and registrar Hostinger and excluding what we already know which is the 7 emails. We are able to discover many more Naver Corp domains that we believe are associated to UNC3782

Query: datasource = “whois” AND name = “Tony Smith” AND registrar = “Hostinger, UAB” AND email != “modric4267[@]protonmail[.]com” AND email != “hostingerk1[@]hotmail[.]com” AND email != “hostingerk2[@]hotmail[.]com” AND email != “peterstewart0326[@]gmail[.]com” AND email != “kimkl0222[@]hotmail[.]com” AND email != “williama824[@]hotmail[.]com” AND email != “specialcnc05[@]gmail[.]com”



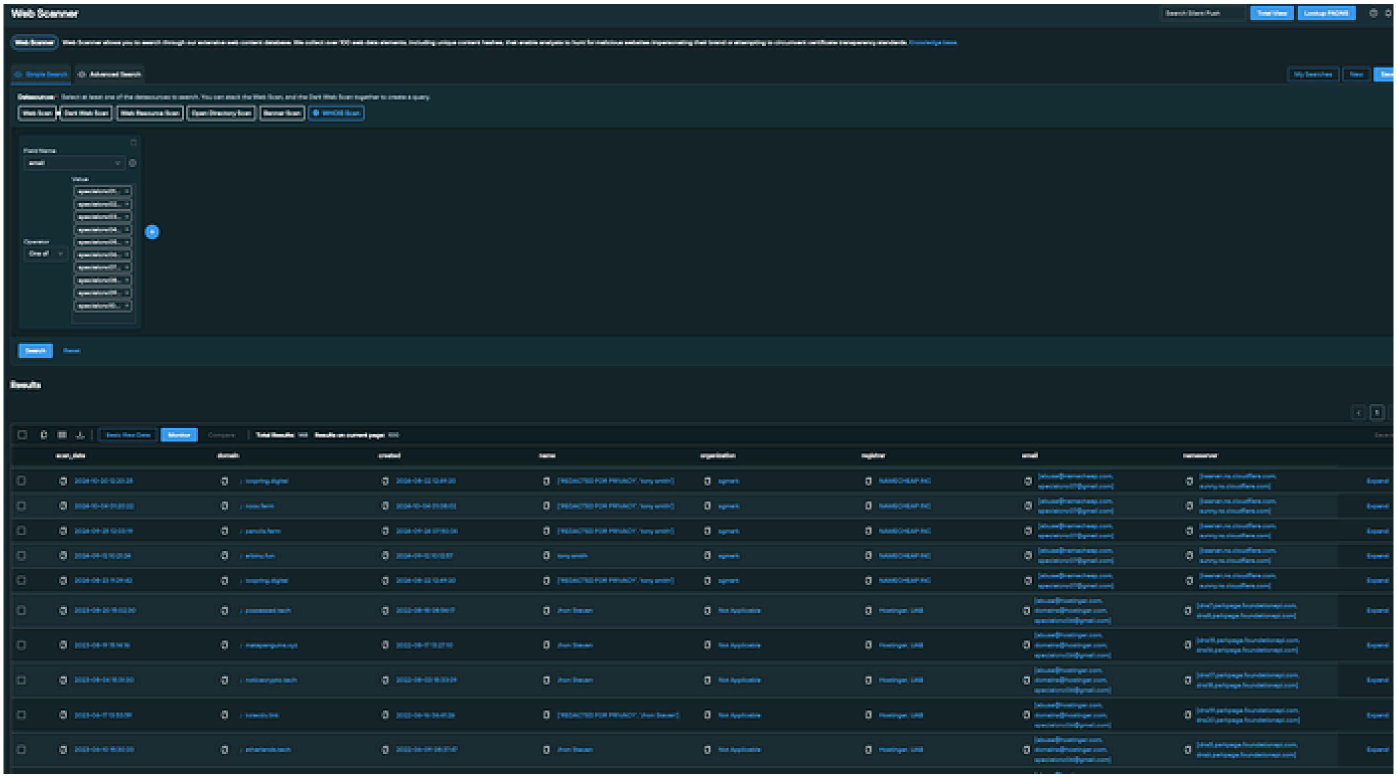
This find the following domains more and as we suspected there is clearly a number pattern in those emails. For example we found emails specialcnc05 and specialcnc07, but where is 6?

mynfthostinger1[@]hotmail[.]com
naverhostinger1[@]hotmail[.]com
naverhostinger2[@]hotmail[.]com
naverhostinger3[@]hotmail[.]com
specialcnc07[@]gmail[.]com
tony42671[@]hotmail[.]com

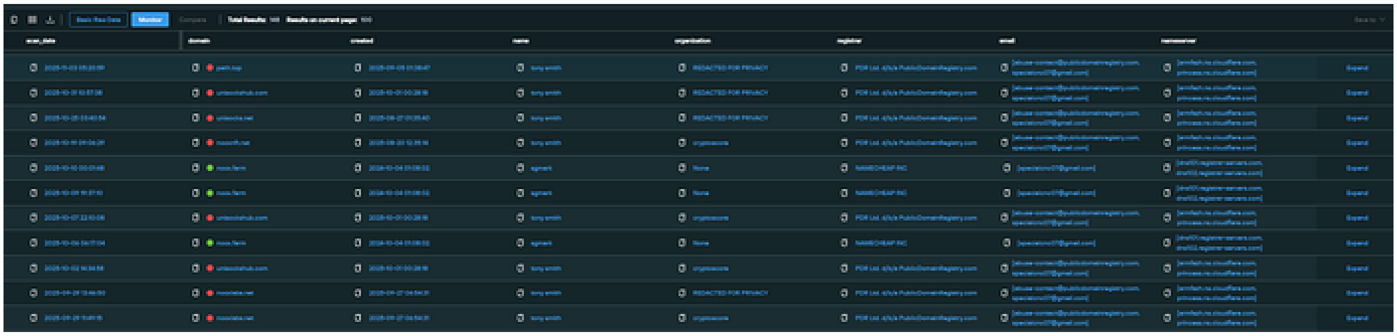
Lets hunt for even more!

Lazy email registration?

We did a check across all number email patterns and discovered one more email specialcnc06[@]gmail[.]com



More importantly. The email specialcnc07 has several domains found to be registered in September and October of 2025.



We will dive into the live websites here shortly, but before we do, we will be pulling all domains found and will cross correlate with PADNS data from Silent Push and see which dedicated IPs are (historically) in use and which subdomains are associated with the domains.

First off I will pull all domains found in Silent Push WHOIS records based of any domain found with the 14 unique email addresses that we found

Query datasource = “whois” AND email = [“hostingerk1[@]hotmail[.]com”, “hostingerk2[@]hotmail[.]com”, “kimkl0222[@]hotmail[.]com”, “modric4267[@]protonmail[.]com”, “mynfthostinger1[@]hotmail[.]com”, “naverhostinger1[@]hotmail[.]com”, “naverhostinger2[@]hotmail[.]com”, “naverhostinger3[@]hotmail[.]com”, “peterstewart0326[@]gmail[.]com”, “specialcnc05[@]gmail[.]com”, “specialcnc06[@]gmail[.]com”, “specialcnc07[@]gmail[.]com”, “tony42671[@]hotmail[.]com”, “williama824[@]hotmail[.]com”]

This resulted in 500 unique domains exactly, and several were found to be registered in 2025. The data can be found in Appendix B: WHOIS data from 14 unique emails, organized by date.

Script for more

By combining Appendix A and B we have 687 domains that we want to lookup for Subdomains and to find IPs that have any of these domains found in the last 8 days. **Keep in mind that ownership of the domain may have changed over time, so checking the WHOIS records and any information that indicates an ownership change could have occurred is important.**

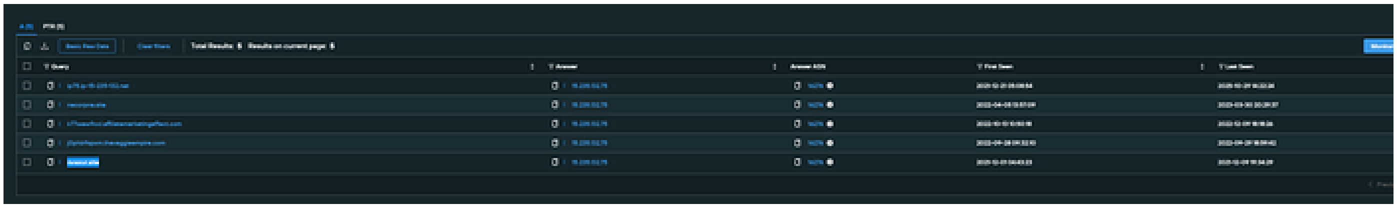
HOSTNAMES AND IPs LAST SEEN IN THE LAST 8 DAYS (since 2025–10–31–2025–11–08 (today)):

```
============================================================
fz9buhqmal[.]pencils[.]farm -> IPs: 172[.]236[.]126[.]142, 172[.]236[.]126[.]145, 172[.]236[.]126[.]225, 172[.]236[.]126[.]234
m[.]noox[.]farm -> IPs: 172[.]236[.]126[.]142, 172[.]236[.]126[.]145, 172[.]236[.]126[.]225, 172[.]236[.]126[.]234
noox[.]farm -> IPs: 172[.]236[.]126[.]142, 172[.]236[.]126[.]145, 172[.]236[.]126[.]225, 172[.]236[.]126[.]234
nooxdao[.]net -> IPs: 188[.]114[.]96[.]3, 188[.]114[.]96[.]4, 188[.]114[.]97[.]3, 188[.]114[.]97[.]4
nooxdao[.]top -> IPs: 104[.]21[.]7[.]194, 172[.]67[.]187[.]252
nooxlabs[.]net -> IPs: 104[.]21[.]52[.]18, 172[.]67[.]194[.]73
nooxnft[.]net -> IPs: 104[.]21[.]82[.]51, 172[.]67[.]153[.]143
pencils[.]farm -> IPs: 172[.]236[.]126[.]142, 172[.]236[.]126[.]145, 172[.]236[.]126[.]225, 172[.]236[.]126[.]234
peth[.]top -> IPs: 104[.]21[.]70[.]235, 172[.]67[.]168[.]192
pooleth[.]top -> IPs: 104[.]21[.]40[.]31, 172[.]67[.]174[.]224
unisocks[.]net -> IPs: 104[.]21[.]19[.]35, 172[.]67[.]184[.]241
unisockshub[.]com -> IPs: 104[.]21[.]10[.]119, 172[.]67[.]163[.]32, 188[.]114[.]96[.]0, 188[.]114[.]96[.]3, 188[.]114[.]96[.]4, 188[.]114[.]97[.]0, 188[.]114[.]97[.]3, 188[.]114[.]97[.]4
vwg9epio2y[.]pencils[.]farm -> IPs: 172[.]236[.]126[.]142, 172[.]236[.]126[.]145, 172[.]236[.]126[.]225, 172[.]236[.]126[.]234
wildcard[.]noox[.]farm -> IPs: 172[.]236[.]126[.]142, 172[.]236[.]126[.]145, 172[.]236[.]126[.]225, 172[.]236[.]126[.]234
www[.]noox[.]farm -> IPs: 172[.]236[.]126[.]142, 172[.]236[.]126[.]145, 172[.]236[.]126[.]225, 172[.]236[.]126[.]234
www[.]nooxdao[.]net -> IPs: 188[.]114[.]96[.]3, 188[.]114[.]97[.]3
www[.]pencils[.]farm -> IPs: 172[.]236[.]126[.]142, 172[.]236[.]126[.]145, 172[.]236[.]126[.]225, 172[.]236[.]126[.]234
```

```
www[.]peth[.]top -> IPs: 104[.]21[.]70[.]235, 172[.]67[.]168[.]192
www[.]unisockshub[.]com -> IPs: 188[.]114[.]96[.]3, 188[.]114[.]97[.]3
==============================================================
```

What about the IPs before those 8 days? Well yeah those are either parking ips, sinkholes, shared hosting or dedicated hosting. The dedicated hosting IPs are the ones we want. In order to filter down on this we grab all IPs found with the previous script associated to the known domains. We lookup all IPs and only want the IPs that do not have 500 + A-records found. Sample below what this looks like:

```
python3 ip_lookup.py
[+] Starting concurrent PADNS enrichment process.
[+] Found 448 IP addresses. Using 10 workers.
[*] Done: Found 500 domains for 13.248.252.114
[*] Done: Found 500 domains for 13.248.158.159
[*] Done: Found 500 domains for 2.57.90.16
[*] Done: Found 104 domains for 5.196.104.158
[*] Done: Found 500 domains for 3.33.243.145
[*] Done: Found 500 domains for 13.248.151.237
[*] Done: Found 500 domains for 2.57.90.58
[*] Done: Found 137 domains for 15.235.33.18
[*] Done: Found 178 domains for 15.235.33.28
[*] Done: Found 5 domains for 15.235.132.75
```



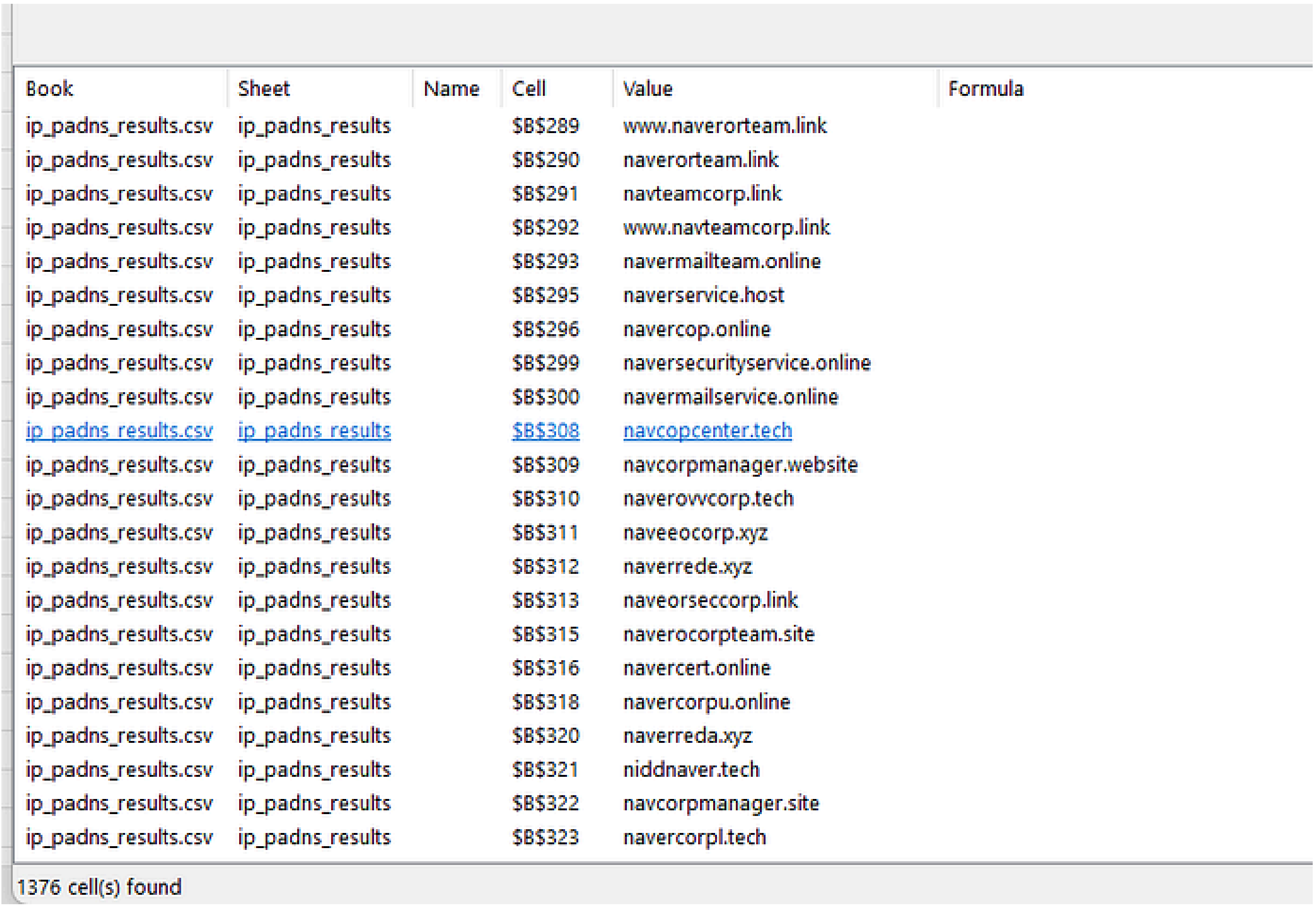
Total Results: 5 Results on current page: 5

Query	Answer	Answer ASN	First Seen	Last Seen
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

We discover 253 IPs overtime that we believe are dedicated IPs that have been in control of UNC3782. Running this script again with the 253 IPs we can find potential UNC3782 domains that were not caught with our WHOIS detection. Unfiltered we retrieve 6516 PADNS data. Of course this will include our indicators that we looked up in order to retrieve this data, though that means roughly 5800 records are potentially related.

```
[+] Writing 6516 records to ip_padns_results.csv…
[+] Process complete. Results saved successfully to ip_padns_results.csv.
```

Out of the 6516 records 1376 records have the value ‘nav’ found



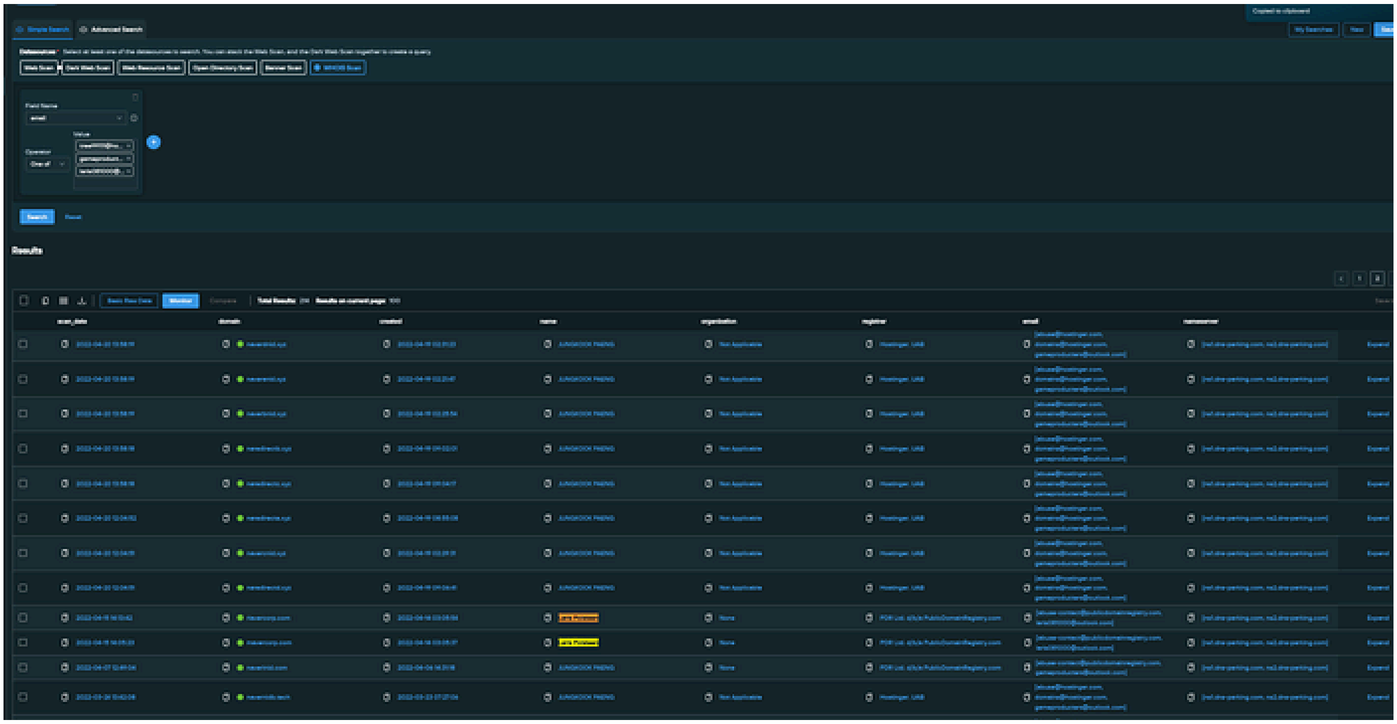
Book	Sheet	Name	Cell	Value	Formula
ip_padns_results.csv	ip_padns_results		B289	www.naverorteam.link	
ip_padns_results.csv	ip_padns_results		B290	naverorteam.link	
ip_padns_results.csv	ip_padns_results		B291	navteamcorp.link	
ip_padns_results.csv	ip_padns_results		B292	www.navteamcorp.link	
ip_padns_results.csv	ip_padns_results		B293	navermailteam.online	
ip_padns_results.csv	ip_padns_results		B295	naverservice.host	
ip_padns_results.csv	ip_padns_results		B296	navercop.online	
ip_padns_results.csv	ip_padns_results		B299	naversecurityservice.online	
ip_padns_results.csv	ip_padns_results		B300	navermailservice.online	
ip_padns_results.csv	ip_padns_results		B308	navcopcenter.tech	
ip_padns_results.csv	ip_padns_results		B309	navcorpmanager.website	
ip_padns_results.csv	ip_padns_results		B310	naverowcorp.tech	
ip_padns_results.csv	ip_padns_results		B311	naveeocorp.xyz	
ip_padns_results.csv	ip_padns_results		B312	naverrede.xyz	
ip_padns_results.csv	ip_padns_results		B313	naveorseccorp.link	
ip_padns_results.csv	ip_padns_results		B315	naverocorpteam.site	
ip_padns_results.csv	ip_padns_results		B316	navercert.online	
ip_padns_results.csv	ip_padns_results		B318	navercorpu.online	
ip_padns_results.csv	ip_padns_results		B320	naverreda.xyz	
ip_padns_results.csv	ip_padns_results		B321	niddnaver.tech	
ip_padns_results.csv	ip_padns_results		B322	navcorpmanager.site	
ip_padns_results.csv	ip_padns_results		B323	navercorpl.tech	

1376 cell(s) found

I have filtered down on this large list of PADNS and I am left with 2746 PADNS records that I would attribute with a high confidence to be associated to UNC3782. This list is available under Appendix C: Script for more at:

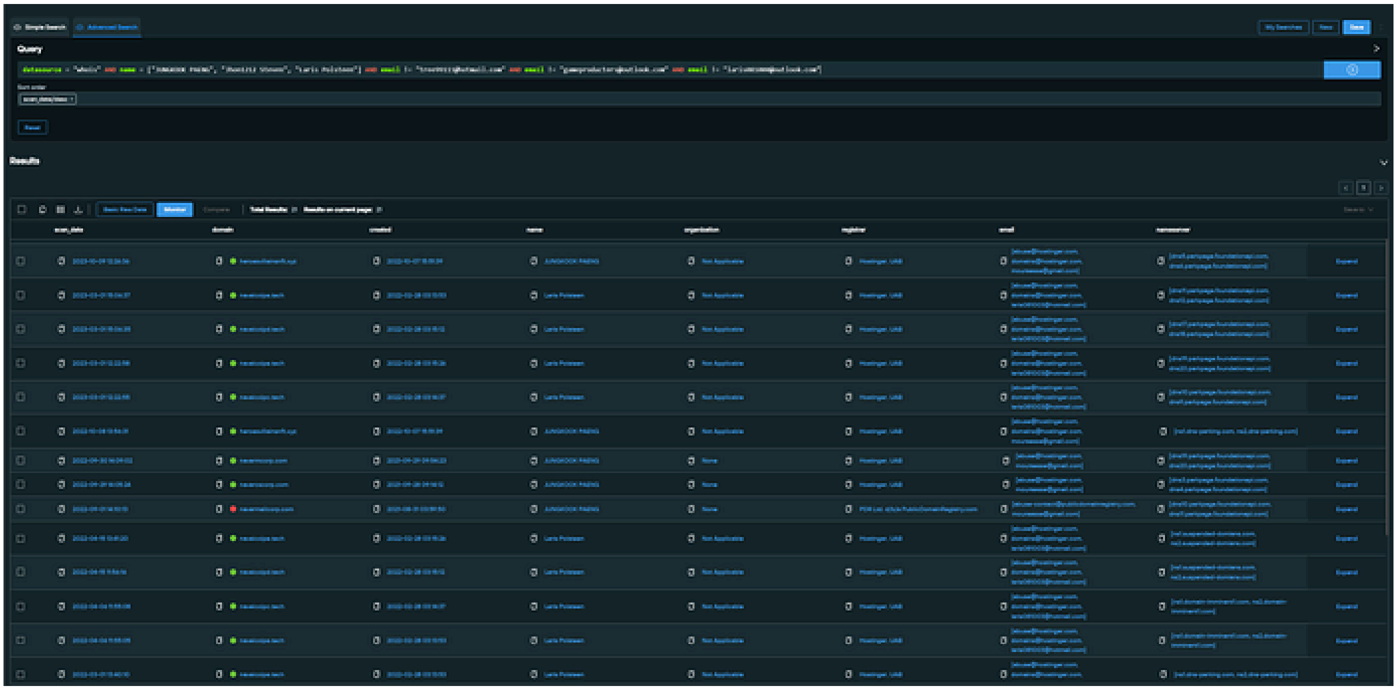
We did WHOIS lookups on all hostnames found and find three more emails: gameproducters[@]outlook[.]com, tree99111[@]hotmail[.]com and laris081000[@]outlook[.]com

Query: datasource = “whois” AND email = [“gameproducters[@]outlook[.]com”, “tree99111[@]hotmail[.]com”, “laris081000[@]outlook[.]com”]



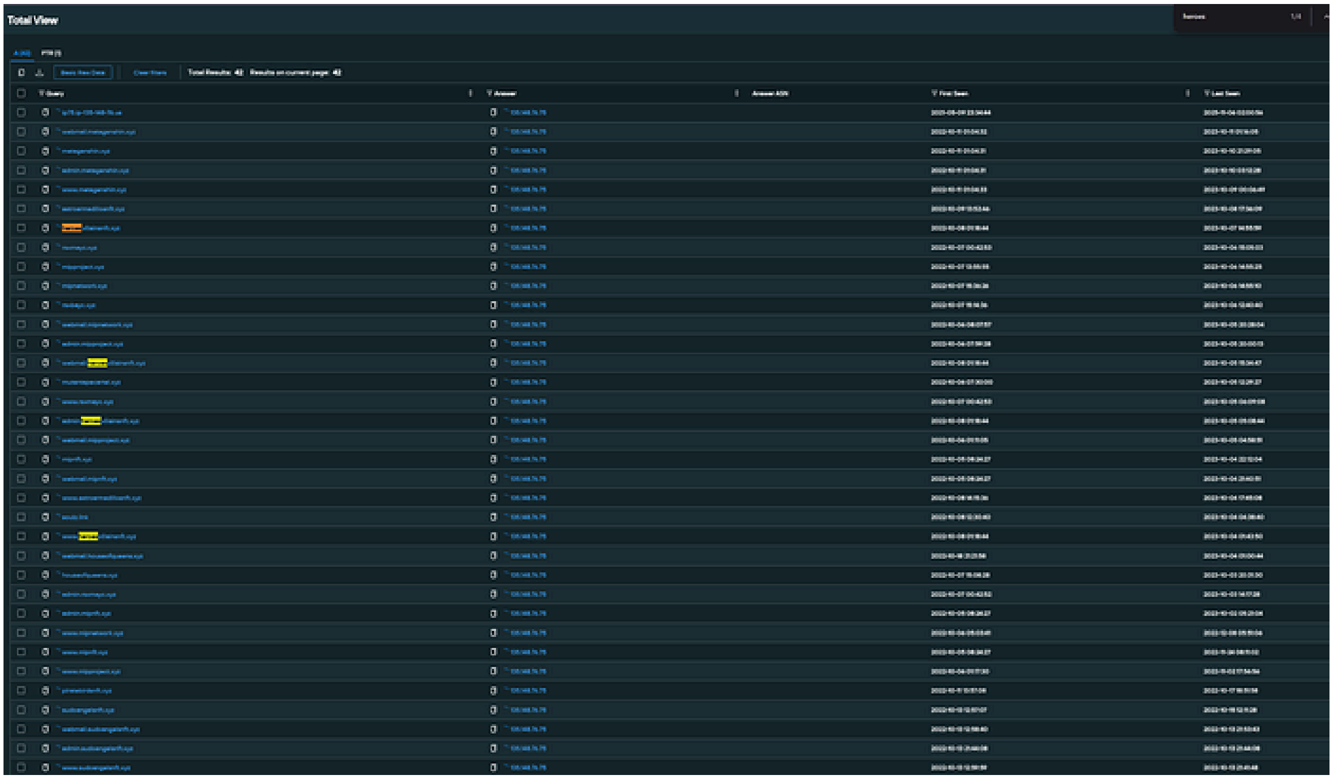
All emails have interesting name values which could potentially find more just like we did with the John Smith earlier. ‘John Steven’ was hitting False positives and nothing new, so we decided to filter this out

Query datasource = “whois” AND name = [“JUNGKOOK PAENG”, “Jhon1212 Steven”, “Laris Polsteen”] AND email != “tree99111[@]hotmail[.]com” AND email != “gameproducters[@]outlook[.]com” AND email != “laris081000[@]outlook[.]com”



The name value “Laris Polsteen” found from laris081000[@]outlook[.]com finds another email Laris08100**3**[@]**hotmail[.]com** which also had Naver phishing domains in the WHOIS data.

The name value “JUNGKOOK PAENG” finds another email mouraesse[@]gmail[.]com which registrered domains like navermailcorp[.]com. Also mouraesse[@]gmail[.]com was found to registrar a domain like: heroesvillainsnft[.]xyz This domain points to a dedicated ip that has historically have tons of NFT like domains seen in the PADNS data.



https://explore.silentpush.com/enrichment/ipv4/135.148.76.75

This leaves us with a 19 emails that we can attribute to be associated to UNC3782 campaigns.

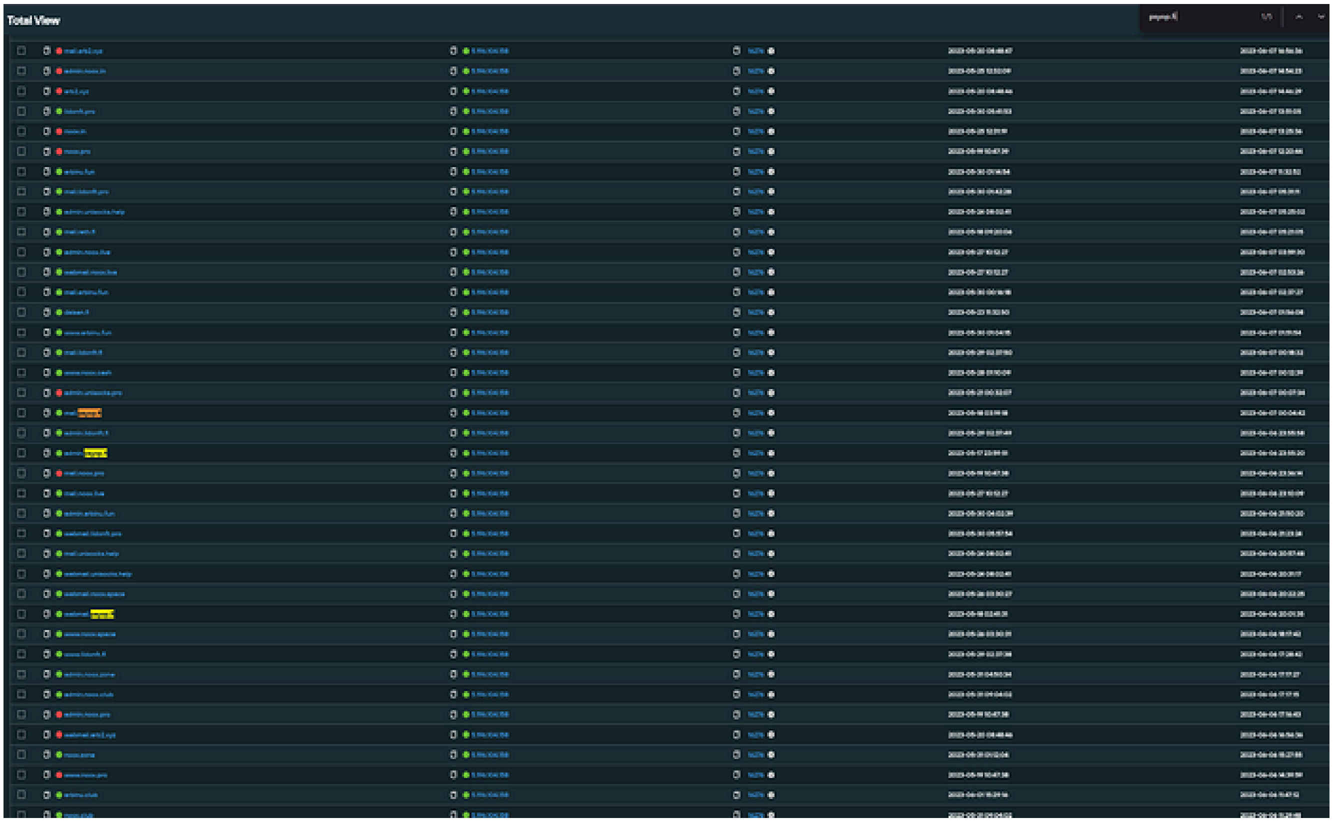
Laris081003[@]hotmail.com
gameproducters[@]outlook.com
hostingerk1[@]hotmail.com
hostingerk2[@]hotmail.com
kimkl0222[@]hotmail.com
laris081000[@]outlook.com
modric4267[@]protonmail.com
mouraesse[@]gmail.com
mynfthostinger1[@]hotmail.com
naverhostinger1[@]hotmail.com
naverhostinger2[@]hotmail.com
naverhostinger3[@]hotmail.com
peterstewart0326[@]gmail.com
specialcnc05[@]gmail.com
specialcnc06[@]gmail.com
specialcnc07[@]gmail.com

tony42671[@]hotmail.com
tree99111[@]hotmail.com
williama824[@]hotmail.com

We have not included the WHOIS results for the later 5 new emails found, but feel free to pull them yourself from the Silent Push platform.

Something out of the ordinary…

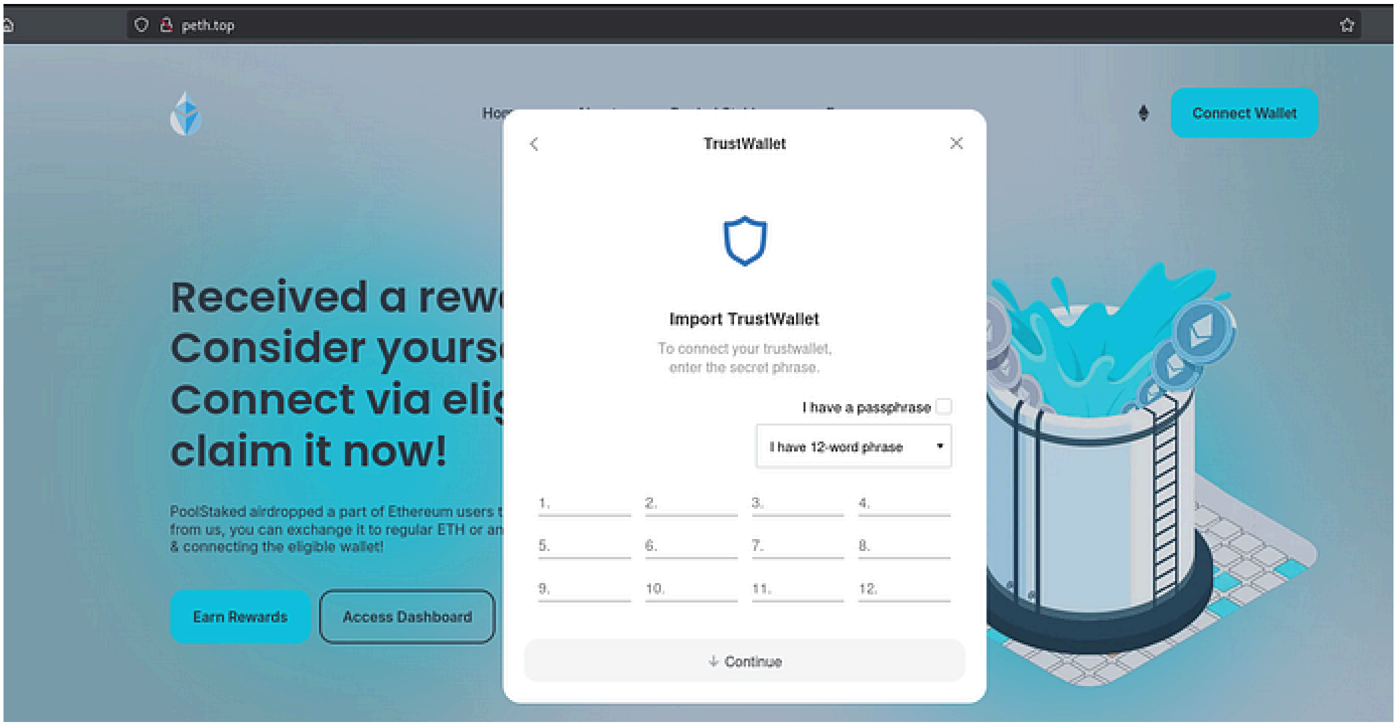
What stood out is that tons of the confirmed NFT domains connected to even bigger clusters with more Crypto related domains including domains with the TLD FI from Finland. One domain in particular stood out to me ‘psyops.fi’ which can be interpreted as Psychological operations (PSYOP) which is often part of military operations to convey selected information and indicators to audiences to influence their motives and objective reasoning, and ultimately the behavior of governments, organizations, groups, and large foreign powers.



https://explore.silentpush.com/enrichment/ipv4/5.196.104.158

Live crypto phishing sites

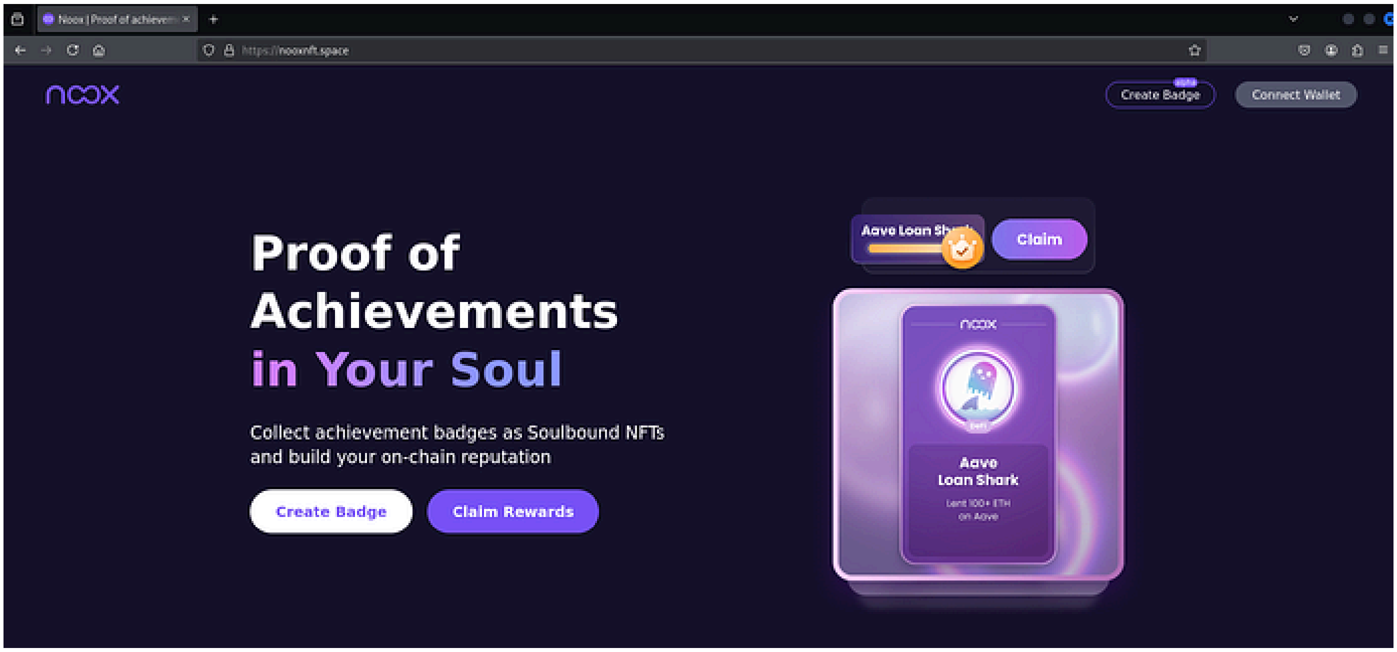
The websites all brand themselves in the crypto/NFT space and are suggesting the page visitor to claim their rewards. In order to do so the page visitor needs to connect their wallet. The connect wallet step requires the page visitor to fill in their **secret seed phrase** of their wallet. Well… if you do that you are not a page visitor anymore but a victim of a typical crypto wallet phishing site.



Received a rew
Consider yours
Connect via elig
claim it now!

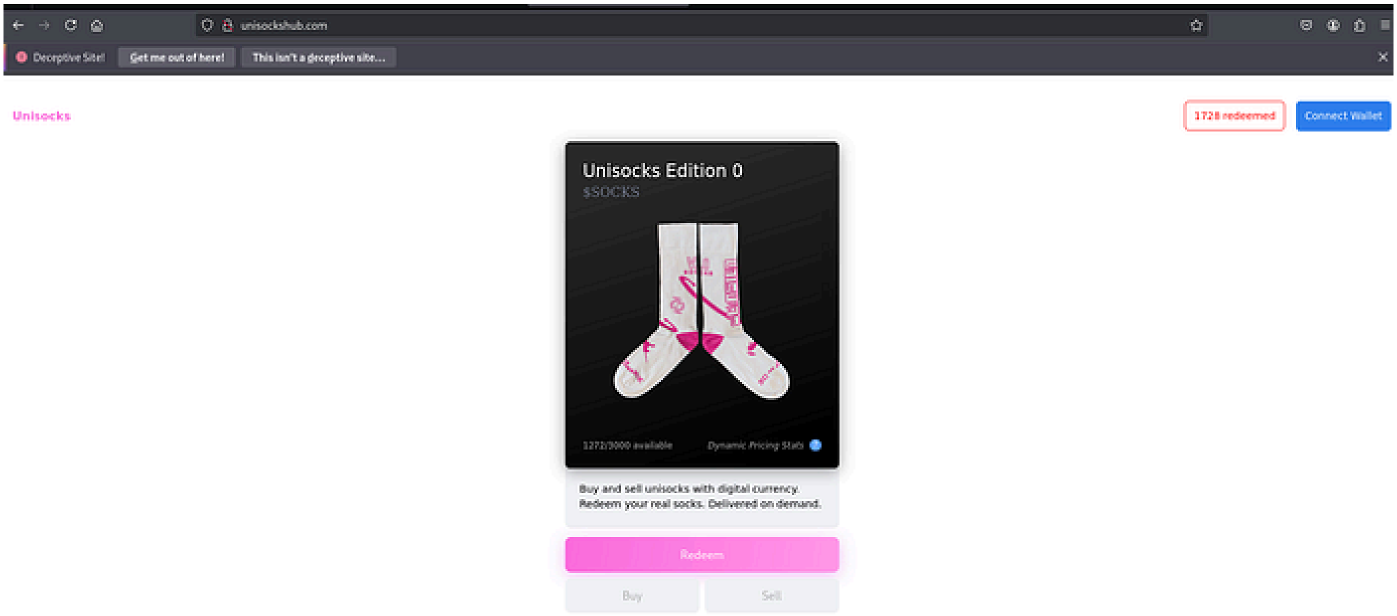
PoolStaked airdropped a part of Ethereum users t
from us, you can exchange it to regular ETH or an
& connecting the eligible wallet!

To connect your trustwallet, enter the secret phrase.



Proof of Achievements in Your Soul

Collect achievement badges as Soulbound NFTs and build your on-chain reputation

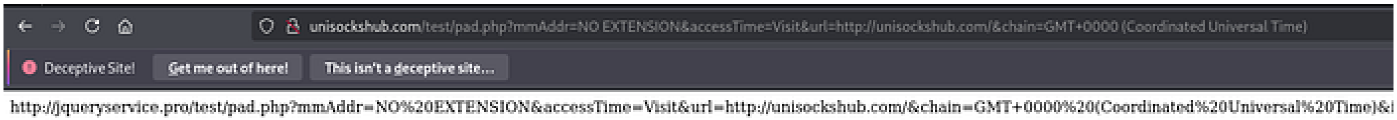


unisockshub.com

Buy and sell unisocks with digital currency.
Redeem your real socks. Delivered on demand.

Webresource datasource

The websites load in an interesting .php file with an interesting response.

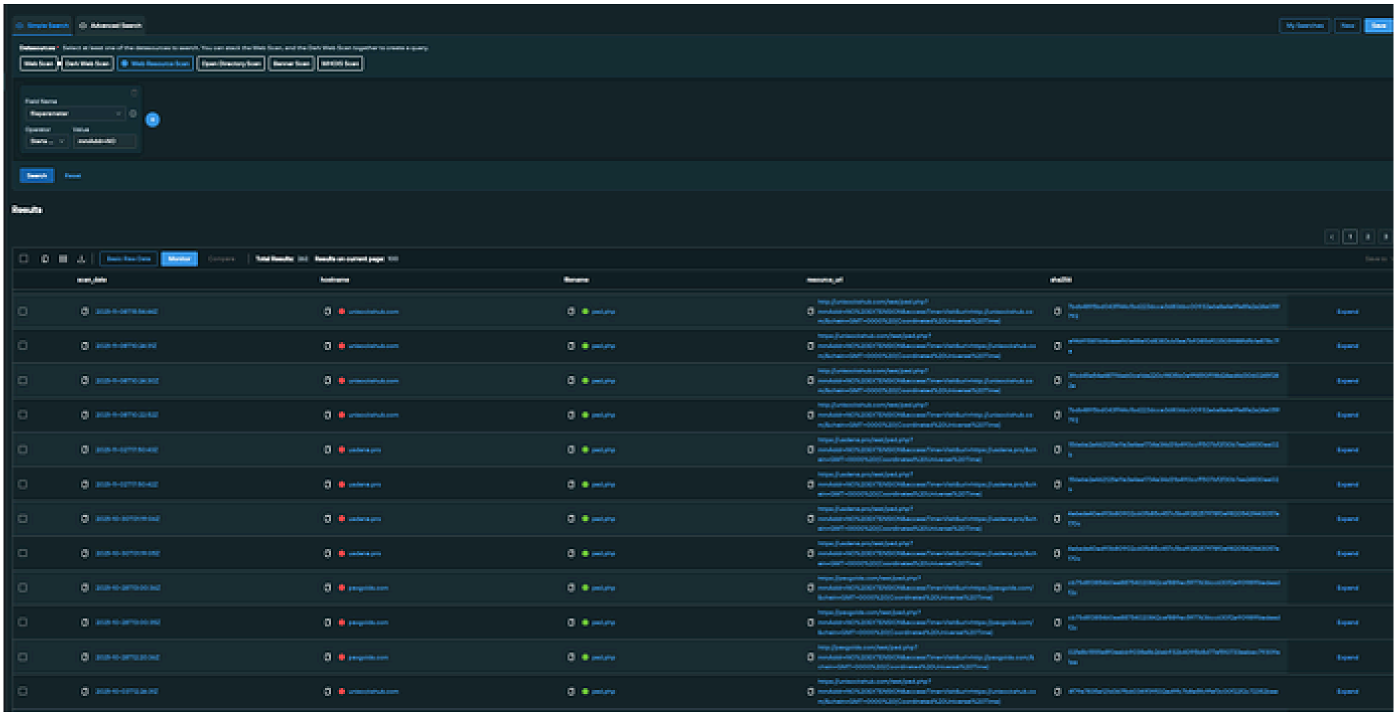


unisockshub.com/test/pad.php?mmAddr=NO EXTENSION&accessTime=Visit&url=http://unisockshub.com/&chain=GMT+0000 (Coordinated Universal Time)

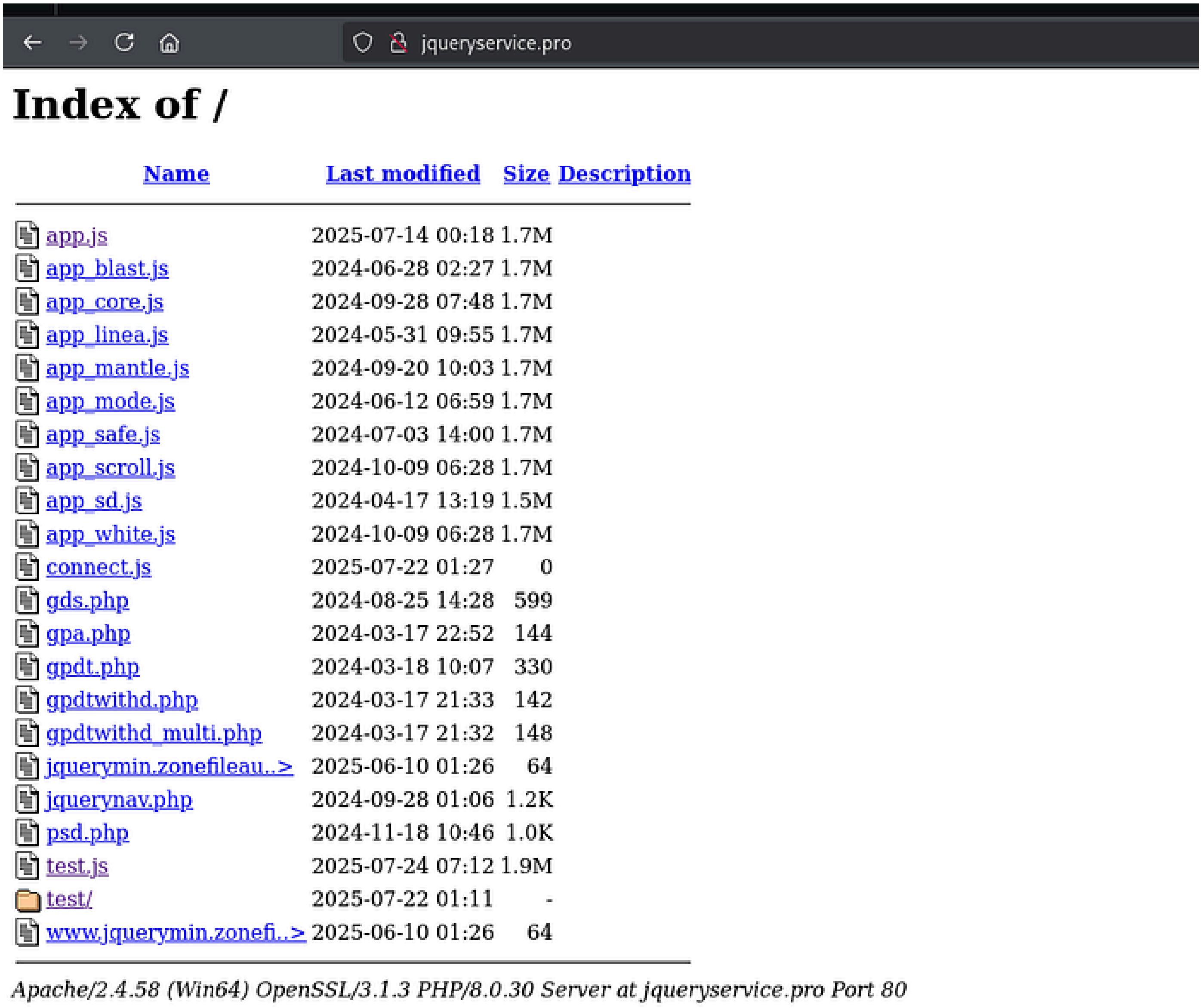
http://jqueryservice.pro/test/pad.php?mmAddr=NO%20EXTENSION&accessTime=Visit&url=http://unisockshub.com/&chain=GMT+0000%20(Coordinated%20Universal%20Time)&

We are able to fingerprint this very easily in the Silent Push platform by pivoting on the file parameter and this unfolds tons of records with the same file parameter string found

[Query](#) datasource = ["webresources"] AND fileparameter = "mmAddr=NO*"



jqueryservice[.]pro is believed to be a domain in control of UNC3782. Fortunately for us the server is configured as an open directory.



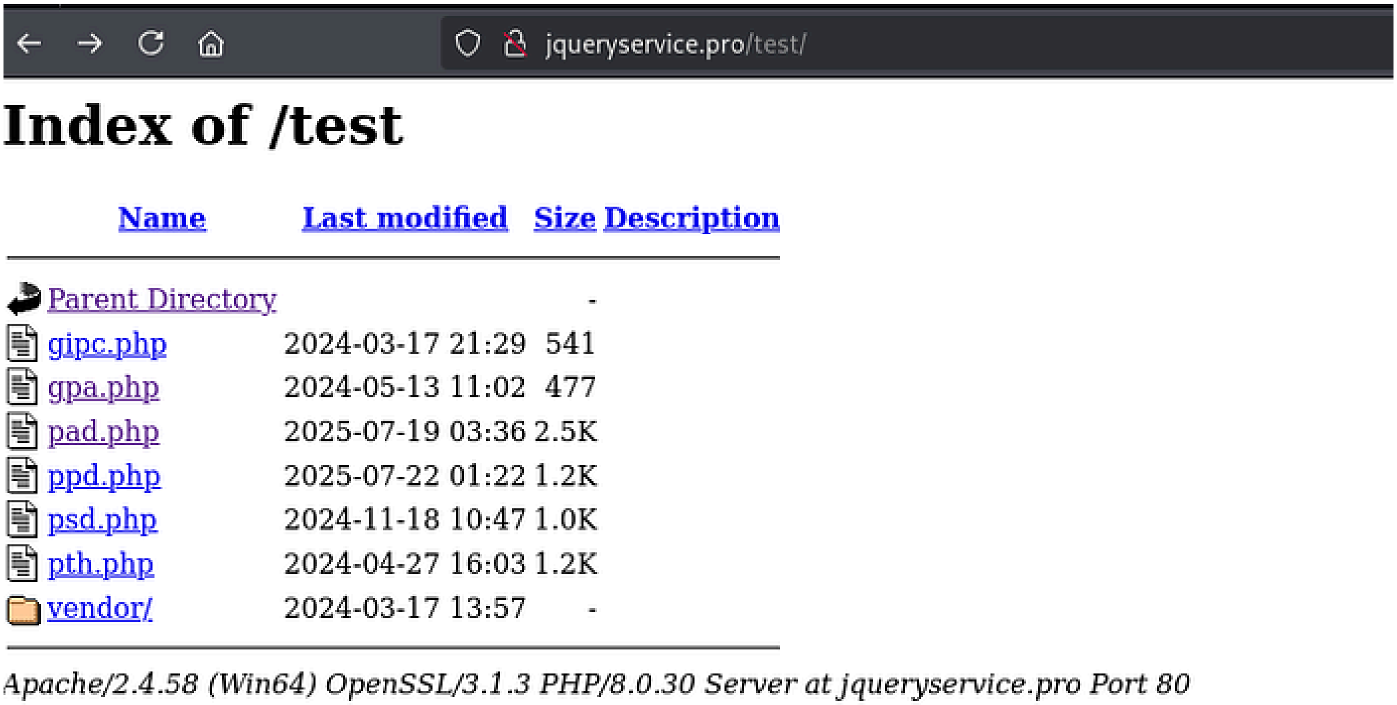
jqueryservice.pro

Index of /

Name	Last modified	Size	Description
app.js	2025-07-14 00:18	1.7M	
app_blast.js	2024-06-28 02:27	1.7M	
app_core.js	2024-09-28 07:48	1.7M	
app_linea.js	2024-05-31 09:55	1.7M	
app_mantle.js	2024-09-20 10:03	1.7M	
app_mode.js	2024-06-12 06:59	1.7M	
app_safe.js	2024-07-03 14:00	1.7M	
app_scroll.js	2024-10-09 06:28	1.7M	
app_sd.js	2024-04-17 13:19	1.5M	
app_white.js	2024-10-09 06:28	1.7M	
connect.js	2025-07-22 01:27	0	
gds.php	2024-08-25 14:28	599	
gpa.php	2024-03-17 22:52	144	
gpdt.php	2024-03-18 10:07	330	
gpdtwithd.php	2024-03-17 21:33	142	
gpdtwithd_multi.php	2024-03-17 21:32	148	
jquerymin.zonefileau..>	2025-06-10 01:26	64	
jquerynav.php	2024-09-28 01:06	1.2K	
psd.php	2024-11-18 10:46	1.0K	
test.js	2025-07-24 07:12	1.9M	
test/	2025-07-22 01:11	-	
www.jquerymin.zonefi..>	2025-06-10 01:26	64	

Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30 Server at jqueryservice.pro Port 80

app.js appears to be heavily obfuscated javascript.

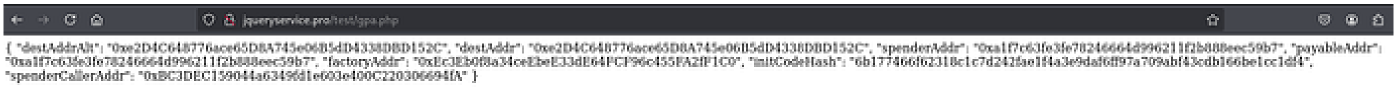


Index of /test

```
      Name          Last modified     Size Description
Parent Directory                        -
gipc.php          2024-03-17 21:29  541
gpa.php           2024-05-13 11:02  477
pad.php           2025-07-19 03:36 2.5K
ppd.php           2025-07-22 01:22 1.2K
psd.php           2024-11-18 10:47 1.0K
pth.php           2024-04-27 16:03 1.2K
vendor/           2024-03-17 13:57   -
```

Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30 Server at jqueryservice.pro Port 80

The gpa.php file reveals some interesting values as well.



{ "destAddrAlt": "0xe2D4C648776ace65D8A745e06B5dD4338DBD152C", "destAddr": "0xe2D4C648776ace65D8A745e06B5dD4338DBD152C", "spenderAddr": "0xa1f7c63fe3fe78246664d996211f2b888eec59b7", "payableAddr": "0xa1f7c63fe3fe78246664d996211f2b888eec59b7", "factoryAddr": "0xEc3Eb0f8a34ceEbeE33dE64FCF96c455FA2fF1C0", "initCodeHash": "6b177466f62318c1c7d242fae1f4a3e9daf6ff97a709abf43cdb166be1cc1df4", "spenderCallerAddr": "0xBC3DEC159044a6349fd1e603e400C220306694fA" }

{ “destAddrAlt”: “0xe2D4C648776ace65D8A745e06B5dD4338DBD152C”, “destAddr”: “0xe2D4C648776ace65D8A745e06B5dD4338DBD152C”, “spenderAddr”: “0xa1f7c63fe3fe78246664d996211f2b888eec59b7”, “payableAddr”: “0xa1f7c63fe3fe78246664d996211f2b888eec59b7”, “factoryAddr”: “0xEc3Eb0f8a34ceEbeE33dE64FCF96c455FA2fF1C0”, “initCodeHash”: “6b177466f62318c1c7d242fae1f4a3e9daf6ff97a709abf43cdb166be1cc1df4”, “spenderCallerAddr”: “0xBC3DEC159044a6349fd1e603e400C220306694fA” }

A vague twitter posts mentions the destAddr and mentions ‘STOLE MY NFT’
https://x.com/FrazierPharaoh/status/1837897175914741881

Analysing the code will require more time to figure out the full configuration of these websites. We suspect that these websites are purposed to drain people crypto wallets and steal NFTs. Since this will require more time I decided to keep this for a potential Part 2.

Final Word

Wow, you actually finished it! Seriously, thank you for reading this entire piece of research. Your time is appreciated, and I hope the journey through the data and findings was a valuable one for you. Curious what your thoughts are on this Campaign, feel free to comment or write to me on Medium / LinkedIN.

Appendixes

All appendixes can be found in my personal Github at
https://github.com/Meesvanwickeren/Threat_Intel/blob/main/DPRK_UNC3782_Indicators