Pivoting through a Sea of indicators to spot Turtles

blog.strikeready.com/blog/pivoting-through-a-sea-of-indicators-to-spot-turtles/

December 27, 2023

December 27, 2023 by StrikeReady Labs 10 minutes

Sea Turtle is a threat group that tends to swim under the radar, but recently the Ministry of Justice in Greece, PWC, and others before them, published reports containing infrastructure currently in use. It was once believed that when an IP or domain was outed publicly, that an actor, especially a well-resourced one, would burn it down. In this blog we'll pull on threads to show that isn't always the case.

Sea Turtle, like most threat groups, leverages traditional malware for access, but also has used complex DNS hijacking techniques that were covered well in the above blogs. Many of the spoofed domains below would be of interest to those focused on domestic Turkish issues.

This analysis will focus on four major concepts in infrastructure pivoting.

1. Passive or Active DNS pivoting

   There is no perfect answer to the question "what domains are sitting on an IP?". Data vendors try to answer this question for analysts in a variety of ways, the most common being passive or active DNS, where the vendor collects responses for DNS requests, either by sniffing resolver traffic, by reading resolver logs, or by actively doing forward record lookups of domains

2. SSL certificate tracking

   Observing SSL certificates can often broaden a set of suspect infra, either by direct movement (seeing a cert from server A move to server B), or by tracking specific attributes of certs over time.

   Additionally, it would not be uncommon to see domains in certs for which you don't have a passive/active DNS record. An actor may prep their server and add a cert before making their campaign live.

3. Matching server response content to find similar infra

   For instance, a particular HTTP response header, the fuzzy hash of body content, or the way a server responds when you throw particular data at it. Many folks scan the internet with a 5 byte ASCII string "Gh0st", in order to see if the server they're talking to will respond like a Gh0st RAT server.

4. Discovering malware samples that are related to your original set, by looking for domain/ip overlaps, or by looking for static content with YARA that you don't expect to be in many unrelated samples

When tracking a threat actor, an analyst develops a confidence for whether a particular indicator belongs in her dataset or not. This confidence is based on examining artifacts over time, and with an eye towards which technical links are of what quality. Servers often change ownership, 'A' records can be forged when a c2 isn't operational, and supposed "uniqueness" may not be so unique upon further review. Sea Turtle leverages a multitude of these techniques which aggravate an investigation

Perhaps in an effort to provide a veil of legitimacy, or to improve a general "risk score" of their domain, this actor frequently points (or parks) their domain at large cloud providers, such as amazon/akamai/google. However, when the domain is used operationally, they typically leverage dedicated providers such as BLNWX, MVPS, Choopa, or the like.

Throughout their campaigns, they acquire domains (or leverage ddns) that look legitimate, such as systemctl.network, *.sslname.com, netssh.net, and serverssl.net. "serverssl" and "netssh" have nothing in common from a top level infrastructure perspective, but if you notice similar looking domains on a low density server, and see them move to IPs with the same provider, you can start to piece together lower quality sources of data.

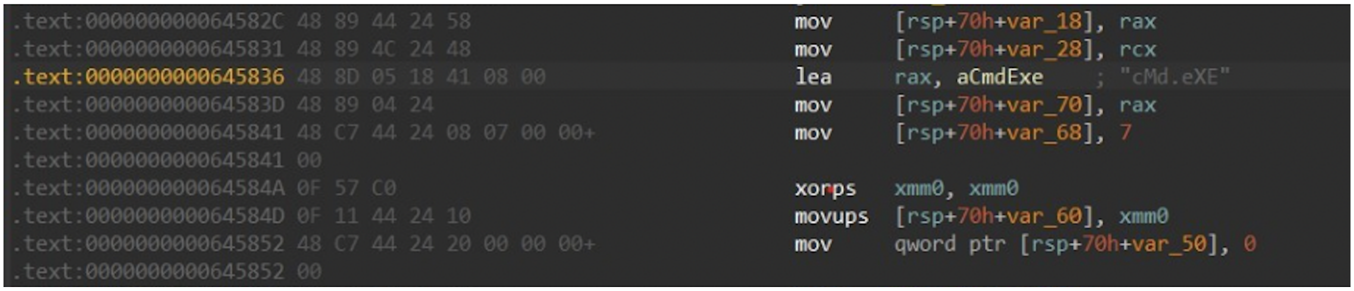
In the first pivot, we can do simple network or yara based pivot to find samples that are similar to the PWC or Greek DOJ report. The high-fidelity IoCs are collated in a github link at the end of the post, but we provide our reasoning in each table.

hash	extracted indicator for pivot	filename from VT
01b8a91f3d4446f2bdd22c85b225dfd2f619951e8f33178c3185dbf7543845df	xss[.]codes	Skype.exe
01d1b63eace6383428e42c48f3d1e13e643e8a8f70d4af5d4ee6f47a0522e300	xss[.]codes	Skype.exe
0dda7e987104867695be561a8008d3282252e05c611c247eae62c7b798be0e24	139.162.137[.]240/man.php	**3_Members_of_the_Committ**
13171d3b1acf5ffbae47777cae03d5d6cb96d2d9b76fe4491bf547b2e309fb52	xss[.]codes	Skype.exe

hash	extracted indicator for pivot	filename from VT
1de46a62f53dbf3b4668bfa7fe63c022c541d8651f776fa5fd8060f21036e63a	213.252.246[.]79/Chrome.exe 213.252.246[.]79/main.php?s=	SkypeApp.exe
487bb8f6c0b6691d3575eee3faa8bfc73ddebe0d1052c02b636cc0a394ed384d	update.qnetau[.]net/syw.php? 213.252.247[.]10	
528fd0b183dd1ca2d109af1714d1ee89d3244c37451203b7b14e951742e16741	cn.sslname[.]com	System.exe
702108f50f953aff3c2b345c2604e9fa614cb86d8299c209065b41878fd4f66b	xss[.]codes	Skype.exe
71bbcd06a4a28f1f33a998928bfe6d78aa7a56fe068c61556f41e2586809a470	xss[.]codes	(potential test xlsm)
85ee62d57a17221e52325020b4d6f587f68fb321723be7ed794503b40bd989f7	ns2[.]me/1p.php	Skype.exe
86b13a1058dd7f41742dfb192252ac9449724c5c0a675c031602bd9f36dd49b5	X-Auth-43245-S-20	[kauditd]
94e7fff8d4abccca0080004a497153ce04f74f7507b52ca092462e22d84f0f8a	ns2[.]me/ip.php?s= 213.252.247[.]10	SkypeApp.exe
aebc8acd17e247c8892e6a8226be4dbf2af3848bdcc1cc1536d1f8487bed55a4	net3[.]me/man.php “hello martin”	Skype.exe
b0307e523e5893f2a865b0abea91cb4fb2e9d86fc71e33adaf63c8878fac2748	cn.sslname[.]com	SkypeApp.exe
be4590c31e8385a67394f7d49147a0b97cff07da6ff771614d3d3ed9ad2cd49f	ns2[.]me/1p.php?s=	Skype.exe
d7d699f04463e86abc85ec029953ea7d558fd385a5e73ce0cc0d9cd0dbebd41e	cMd.eXE, “hello hgroup”	
d7f53836227dde351def7c1a5e9dd03c3a49bdc4eec6342136795038aa6d415d	ope[.]ftp[.]sh xss[.]codes	xlsm
ef1af0acb25dc88b223c7b6a6be48d35a64665bb372cf8b7674cacd5818f7ff3	ns2[.]me/ip.php?s=	Update.exe
f5e0edca8a63eb45054039104f509ef0e66fc2e67637614a0f386803506cbac1	update.qnetau[.]net/syw.php?s=	mpam-fe.exe
f8cb77919f411db6eaeea8f0c8394239ad38222fe15abc024362771f611c360f	net3[.]me/b/kdd net3[.]me/b/socat	upxa.sh

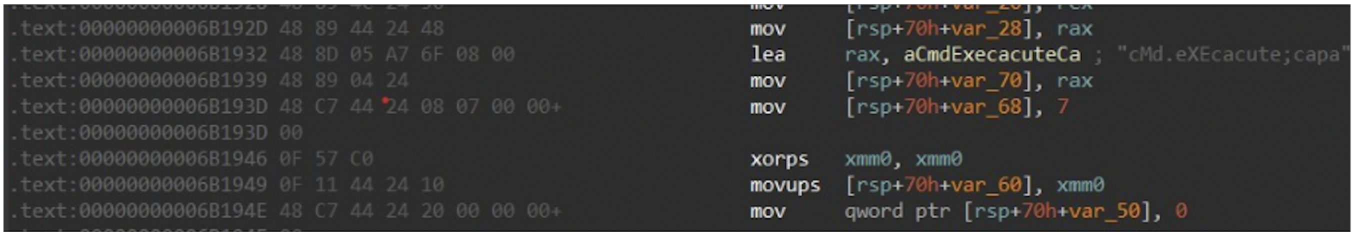
Figure 1: Publicly available ST samples

Standalone string matches, after unpacking, remains an easy pivot to expand a dataset. Although these are not definitive pivot points, Sea Turtle does leverage a number of strange capitalizations and “shout-outs” to unknown persons, that can be combined to cast a net.



```
.text:000000000064582C 48 89 44 24 58                mov     [rsp+70h+var_18], rax
.text:0000000000645831 48 89 4C 24 48                mov     [rsp+70h+var_28], rcx
.text:0000000000645836 48 8D 05 18 41 08 00          lea     rax, aCmdExe    ; "cMd.eXE"
.text:000000000064583D 48 89 04 24                   mov     [rsp+70h+var_70], rax
.text:0000000000645841 48 C7 44 24 08 07 00 00+      mov     [rsp+70h+var_68], 7
.text:0000000000645841 00
.text:000000000064584A 0F 57 C0                      xorps   xmm0, xmm0
.text:000000000064584D 0F 11 44 24 10                movups  [rsp+70h+var_60], xmm0
.text:0000000000645852 48 C7 44 24 20 00 00 00+      mov     qword ptr [rsp+70h+var_50], 0
.text:0000000000645852 00
```

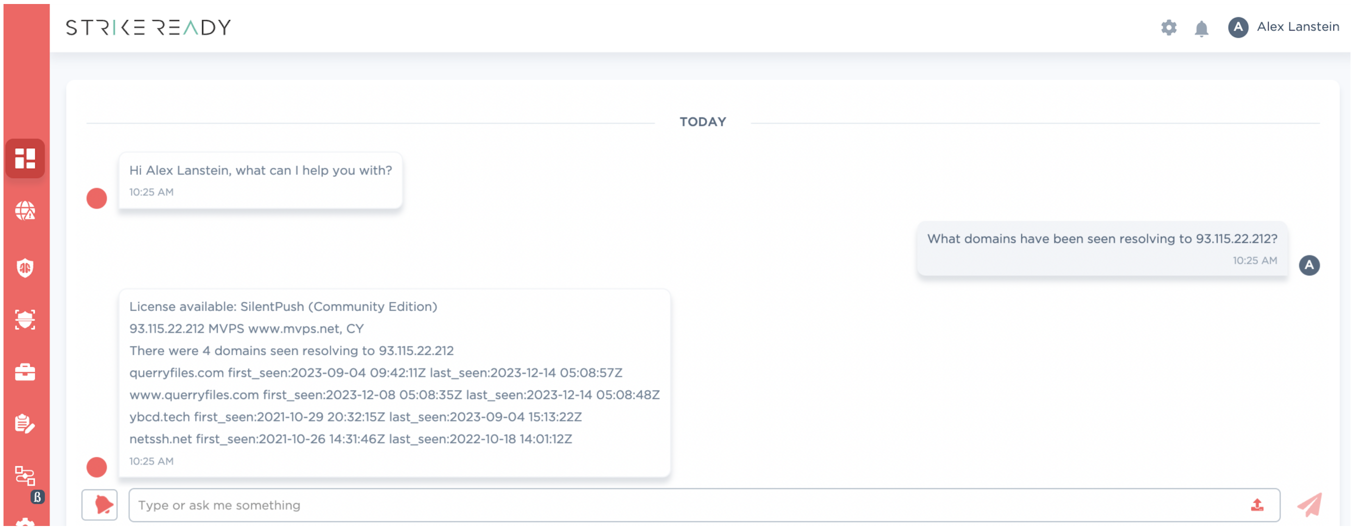
Figure 2: obligatory IDA of d7d699f04463e86abc85ec029953ea7d558fd385a5e73ce0cc0d9cd0dbebd41e



```
.text:00000000006B192D 48 89 44 24 48                    mov     [rsp+70h+var_28], rax
.text:00000000006B1932 48 8D 05 A7 6F 08 00              lea     rax, aCmdExecacuteCa ; "cMd.eXEcacute;capa"
.text:00000000006B1939 48 89 04 24                       mov     [rsp+70h+var_70], rax
.text:00000000006B193D 48 C7 44 24 08 07 00 00+          mov     [rsp+70h+var_68], 7
.text:00000000006B193D 00
.text:00000000006B1946 0F 57 C0                          xorps   xmm0, xmm0
.text:00000000006B1949 0F 11 44 24 10                    movups  [rsp+70h+var_60], xmm0
.text:00000000006B194E 48 C7 44 24 20 00 00 00+          mov     qword ptr [rsp+70h+var_50], 0
```

Figure 3: b0307e523e5893f2a865b0abea91cb4fb2e9d86fc71e33adaf63c8878fac2748

In our next pivot, we'll examine Passive/Active DNS datasets, to try to find infrastructure "one hop" away.



Hi Alex Lanstein, what can I help you with?
10:25 AM

What domains have been seen resolving to 93.115.22.212?
10:25 AM

License available: SilentPush (Community Edition)
93.115.22.212 MVPS www.mvps.net, CY
There were 4 domains seen resolving to 93.115.22.212
querryfiles.com first_seen:2023-09-04 09:42:11Z last_seen:2023-12-14 05:08:57Z
www.querryfiles.com first_seen:2023-12-08 05:08:35Z last_seen:2023-12-14 05:08:48Z
ybcd.tech first_seen:2021-10-29 20:32:15Z last_seen:2023-09-04 15:13:22Z
netssh.net first_seen:2021-10-26 14:31:46Z last_seen:2022-10-18 14:01:12Z
10:25 AM

Figure 4: PADNS coming to CARA in Q1 '24

old artifact	pivot point	new	notes
ai-connector.splendor[.]org	161.35.32[.]185	ai-connector.splendos[.]org	note "splendor->splendos"
querryfiles[.]com	93.115.22[.]212	netssh[.]net	
ai-connector.goldchekin[.]com	168.100.10[.]187	ono.technewsir[.]gq	possibly a "technews iran" spoof. however, like most pivoting these days, this is one hop away from a crypto cluster

Figure 5: PADNS pivots leads to more artifacts

Sea Turtle has been known to spoof news-related websites, and PWC highlighted three: alhurra[.]online, al-marsad[.]co, anfturkce[.]news. Examining their infra, some of the IPs or domains throw a 426 response seen below. A 426 error is "caused when a client is attempting to upgrade a connection to a newer version of a protocol, but the server is refusing to do so." Despite this being a valid and common response code, when scanning the internet for that header/string, only ~25 results are returned with that exact context, and many appear to be interesting.

```
HTTP/1.1 426 Upgrade Required
Date: Sat, 23 Dec 2023 22:09:37 GMT
Content-Type: application/json
Content-Length: 29
Connection: keep-alive
Server: Apache

{"detail":"Upgrade Required"}
```

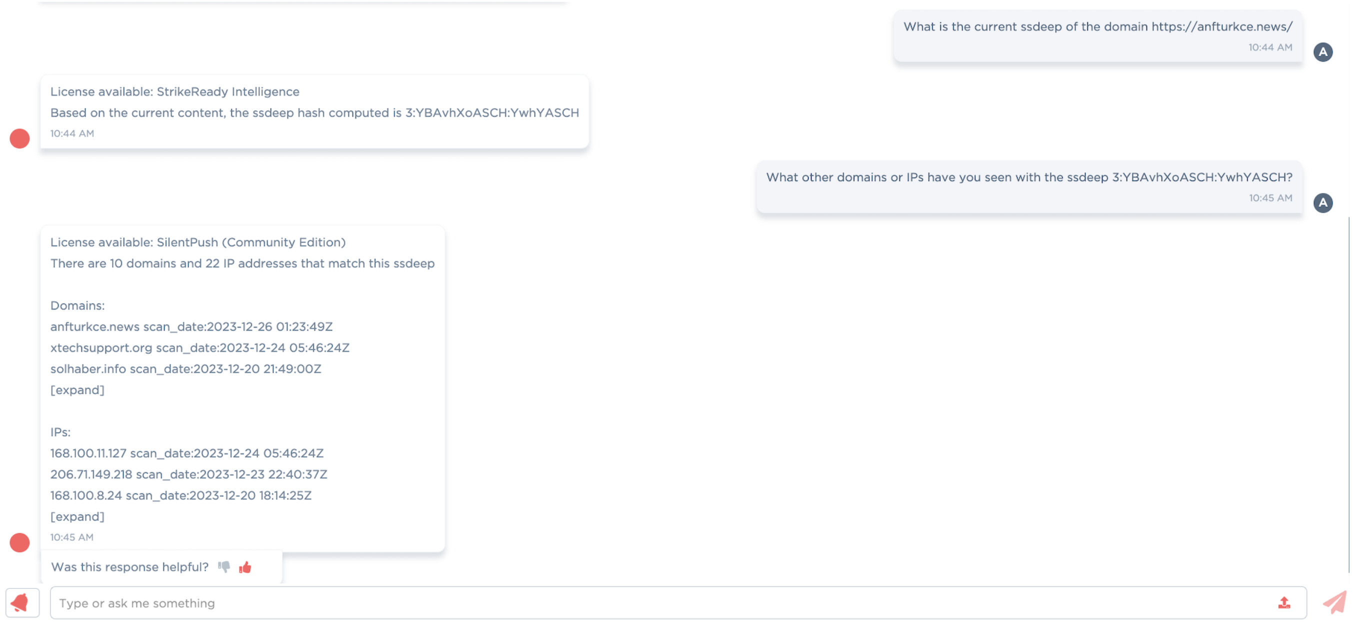
Figure 6: Specific "426" server output from suspicious servers

Combining multiple artifacts such as the below can rule-in, or rule-out, indicators.

- Low global prevalence
- Timestamp overlaps, such as domain creation time or server ownership changes
- Historical scan non-overlaps (when was the first time this string appeared anywhere)

- Infrastructure similarly (registrars, hosting providers)
- Legitimate content or lack thereof, especially on domains with highly legitimate keywords where you would expect a domain to be actually used

In the case of our specific “Upgrade Required” string with the same headers, SilentPush reports the first time they saw it was 2023-09-21, and Censys reports a similarly narrow set of IPs.



What is the current ssdeep of the domain https://anfturkce.news/
10:44 AM

License available: StrikeReady Intelligence
Based on the current content, the ssdeep hash computed is 3:YBAvhXoASCH:YwhYASCH
10:44 AM

What other domains or IPs have you seen with the ssdeep 3:YBAvhXoASCH:YwhYASCH?
10:45 AM

License available: SilentPush (Community Edition)
There are 10 domains and 22 IP addresses that match this ssdeep

Domains:
anfturkce.news scan_date:2023-12-26 01:23:49Z
xtechsupport.org scan_date:2023-12-24 05:46:24Z
solhaber.info scan_date:2023-12-20 21:49:00Z
[expand]

IPs:
168.100.11.127 scan_date:2023-12-24 05:46:24Z
206.71.149.218 scan_date:2023-12-23 22:40:37Z
168.100.8.24 scan_date:2023-12-20 18:14:25Z
[expand]
10:45 AM

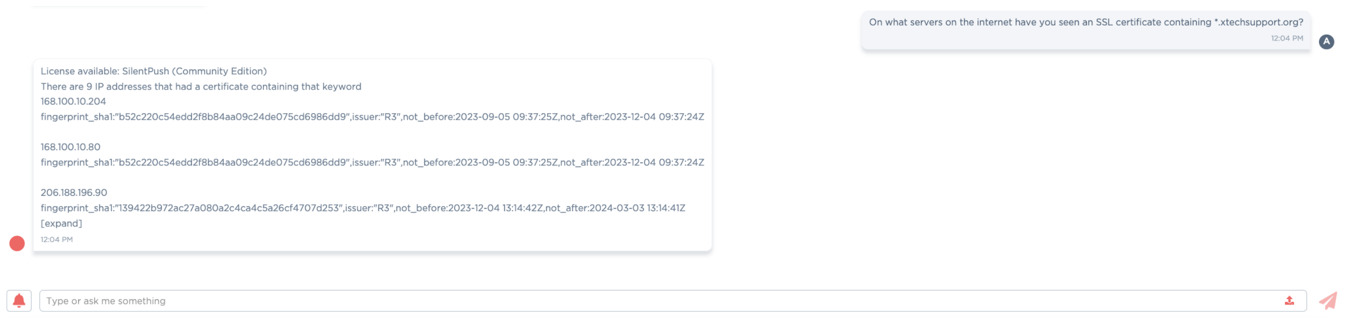
Figure 7: SSDEEP infrastructure scanning coming to CARA Q1 '24

old artifact	pivot point	new artifact	notes
“`Upgrade Required`”	192.153.57[.]31	nuceciwan[.]news solhaber[.]news loading-website[.]net	“Nûçe Ciwan” is an oft-targeted Turkish news source “Sol” is a Turkish newspaper. “haber” is Turkish for “news”
“`Upgrade Required`”	193.149.129[.]182	solhaber[.]info	“sol” is a Turkish newspaper
“`Upgrade Required`”	87.120.254[.]120	caglayandergisi[.]net	“Çağlayan Dergisi” is a Turkish blogger
“`Upgrade Required`”	93.123.12[.]151	infohaber[.]net	“haber” is Turkish for “news”
“`Upgrade Required`”	serverssl[.]net	206.71.149[.]112	146.70.157[.]28
“`Upgrade Required`”	168.100.9[.]203	exp-al-marsad[.]co (PTR)	not registered, although “Sl Marsad” is a human rights organization in the region
serverssl.net	95.179.130[.]232	mat-46.mehreganmobile[].ga iran-azad[.]cyou	These domains were seen pointing to .232 only before the “upgrade behavior” started. Additional overlaps show lure domains with Iranian dissidents, such as Mahsa Aminiw, but will not be included in the high confidence indicator list
loading-website.net	45.11.183[.]85		

Figure 8: Additional discovered Turkish-themed domains

Another common pivot is to look at what SSL certs have lived on an IP address – in a specific timeframe – to understand what domains may have pointed there that your PADNS collection missed, or to find a campaign that is not fully live yet. An “indicator of (potential) future attack”. An example of this is alarabiyaa[.]online, where there is no record of a forward resolution, but we can see a cert with that domain on one of our

“426” IPs, 206.166.251[.]163. The below table explores that technique.



On what servers on the internet have you seen an SSL certificate containing *.xtechsupport.org?
12:04 PM

```
License available: SilentPush (Community Edition)
There are 9 IP addresses that had a certificate containing that keyword
168.100.10.204
fingerprint_sha1:"b52c220c54edd2f8b84aa09c24de075cd6986dd9",issuer:"R3",not_before:2023-09-05 09:37:25Z,not_after:2023-12-04 09:37:24Z

168.100.10.80
fingerprint_sha1:"b52c220c54edd2f8b84aa09c24de075cd6986dd9",issuer:"R3",not_before:2023-09-05 09:37:25Z,not_after:2023-12-04 09:37:24Z

206.188.196.90
fingerprint_sha1:"139422b972ac27a080a2c4ca4c5a26cf4707d253",issuer:"R3",not_before:2023-12-04 13:14:42Z,not_after:2024-03-03 13:14:41Z
[expand]
12:04 PM
```

Figure 9: SSL cert scanning coming to CARA Q1 '24

old artifact	pivot point	new artifact	notes
206.166.251[.]163	426 + cert	www.alarabiyaa[.]online	A spoof of Al Arabiya, an Arabic language news organization
206.71.149[.]112	426 + cert	www.pictture[.]online	426 is the only link, provided for posterity. However, it was created a week apart from the above domain, both leveraging the ‘online’ tld
45.61.139[.]232	426 + cert	youtu[.]vc	426 is the only firm link, so provided for posterity. However both this and the ’tiktok’ leverage the obscure tld ‘.vc’.
64.190.113[.]216	426 + cert	tiktok[.]vc	426 is the only link, provided for posterity
206.188.196[.]228	426 + cert	techdateweb[.]com	426 is the only link, provided for posterity
206.71.149[.]218	426 + cert	libia[.]cc	426 is the only link, provided for posterity
192.153.57[.]78	426 + cert	amezon[.]pro	426 is the only link, provided for posterity

Figure 10: Additional potential infrastructure

It’s common for a domain to expire and point to an unrelated infra, but a well-formed certificate is an artifact that is generally intentionally created. For this reason, validity date ranges, along with domain creation timestamps, are useful data points when trying to timeline.

domain	domain creation time	not_before	not_after
nuceciwan[.]news	2022-11-26T11:23:56	2023-11-16 13:55:34	2024-02-14 13:55:33
solhaber[.]news	2023-11-24T07:00:00	2023-11-24 07:57:35	2024-02-22 07:57:34
loading-website[.]net	2023-01-19T07:00:00	2023-01-19 13:33:27	2023-04-19 13:33:26
solhaber[.]info	2023-11-10T07:00:00	2023-11-14 07:47:07	2024-02-12 07:47:06
caglayandergisi[.]net	2022-11-17T07:00:00	2023-08-24 12:52:02	2024-02-11 09:38:19
infohaber[.]net	2023-03-24T07:35:38	2023-08-04 18:08:37	2023-11-02 18:08:36
alarabiyaa[.]online	2023-11-13T21:52:21	2023-11-13 00:00:00	2024-02-11 23:59:59

Figure 11: Certificates for lookalike/spoof domains

At one point, the ‘426’ artifact was a curiosity, but we observed other commonalities. Many of the ‘426’ servers also contained a certificate for xtechsupport[.]org, and lived on infrastructure from a very small number of providers. Unlike the other domains discovered, ‘xtechsupport’ was registered through IHS, a Turkish domain registrar. There is no content publicly available about this domain.

IP	Provider	First matching scan for 426 response	426 code	xtechsupport cert

IP	Provider	First matching scan for 426 response	426 code	xtechsupport cert
168.100.10[.]119	BLNWX, US	2023-12-15	yes	yes
168.100.10[.]204	BLNWX, US		no	yes
168.100.10[.]80	BLNWX, US	2023-09-24	yes	yes
168.100.11[.]127	BLNWX, US	2023-11-02	yes	yes
168.100.8[.]103	BLNWX, US		no	yes
168.100.8[.]24	BLNWX, US	2023-10-11	yes	no
168.100.8[.]245	BLNWX, US	2023-12-01	yes	no
168.100.9[.]203	BLNWX, US	2023-10-26	yes	no
192.153.57[.]204	BLNWX, US		no	yes
192.153.57[.]31	BLNWX, US	2023-11-05	yes	yes
192.153.57[.]78	BLNWX, US	2023-11-19	yes	no
193.149.129[.]128	BLNWX, US		no	yes
193.149.129[.]182	BLNWX, US	2023-11-19	yes	no
193.149.189[.]94	BLNWX, US	2023-12-20	yes	no
195.85.114[.]106	BLNWX, US	2023-11-03	yes	no
206.166.251[.]161	BLNWX, US		yes	no
206.166.251[.]163	BLNWX, US	2023-12-03	yes	no
206.188.196[.]132	BLNWX, US	2023-12-19	yes	yes
206.188.196[.]228	BLNWX, US	2023-10-17	yes	no
206.188.196[.]90	BLNWX, US		no	yes
206.71.149[.]112	BLNWX, US	2023-12-03	yes	no
206.71.149[.]218	BLNWX, US	2023-12-23	yes	no
31.13.195[.]52	NETERRA-AS, BG	2023-11-10	yes	no
45.61.139[.]232	BLNWX, US	2023-10-05	yes	no
64.190.113[.]216	BLNWX, US	2023-12-06	yes	no
87.120.254[.]120	NETERRA-AS, BG	2023-12-07	yes	no
93.123.12[.]151	NETERRA-AS, BG	2023-09-21	yes	no
95.179.130[.]232	AS-CHOOPA, US	2023-10-27	yes	no

Figure 12: Servers currently responding with the specific ‘426’ error

At the end of an analysis exercise, it’s useful to do one last sweep through the collated indicator list, to look for commonalities that may have been missed. In the below table, armed with a higher confidence of “xtechsupport”, we’ll pivot once more.

initial artifact	pivot	new artifact	notes

initial artifact	pivot	new artifact	notes
xtechsupport[.]org	where else have we seen this cert, that was not on a previous indicator list?	168.100.10[.]204 168.100.8[.]103 192.153.57[.]204 206.188.196[.]90 193.149.129[.]128	Potentially interesting domains an additional hop away, but many at the same provider. Without stronger links, these artifacts have a lower confidence **168.100.8[.]103** infoviewdr[.]click, accepteddr[.]click **168.100.10[.]204** test.allsocial[.]site **168.100.8[.]24** appmetadata[.]co
xtechsupport[.]org	23be.xtechsupport[.]org	45.61.137[.]131	426 on 23be, but the domain only pointed to the IP on 12/14/23

Figure 13: Subsequent pivot from xtechsupport

For an easier to parse list of indicators, please visit our GitHub page.

Acknowledgements

The authors would like to thank the internal reviewers, as well as peer vendors, for their comments and corrections. Please get in touch if you have further corrections, or would like to collaborate on research in the future.

Additionally, we would like to thank Censys, Silent Push, and VirusTotal.