

How To Track Malware Infrastructure - Identifying MatanBuchus Domains Through Hardcoded Certificate Values

By Matthew

Published: 2024-04-04 · Archived: 2026-04-05 21:28:22 UTC

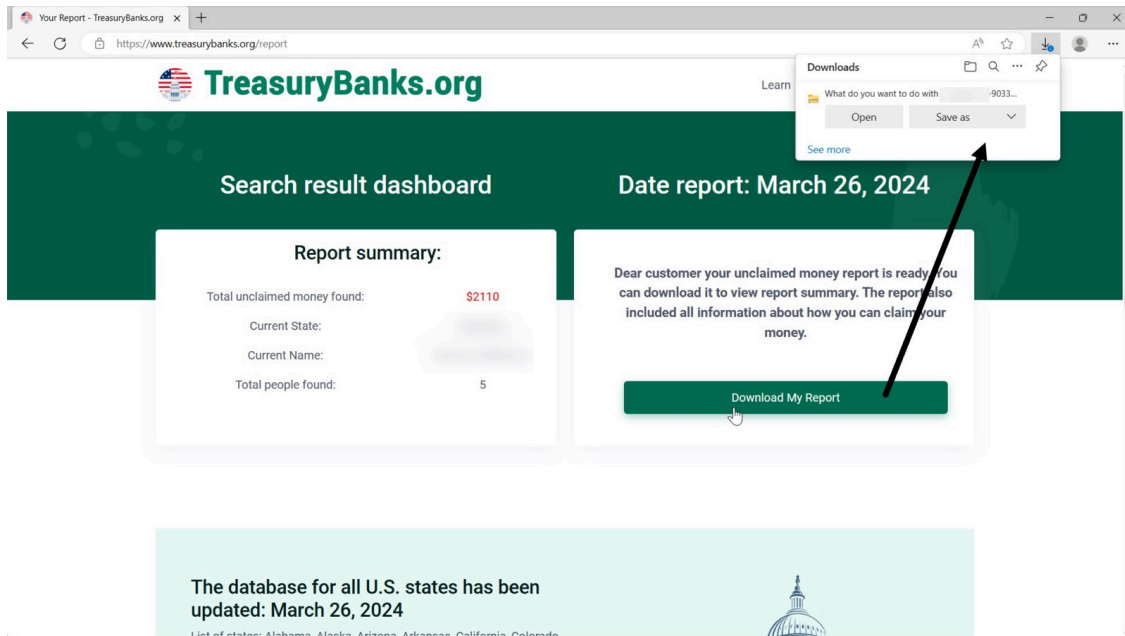
In this blog we will identify 6 malicious domains that are likely hosting MatanBuchus malware. We will identify these domains through the usage of hardcoded subdomains in the TLS Certificate of the initial shared domain.

After leveraging the hardcoded subdomains, we will leverage registration dates and certificate providers to hone in on our final results. Ultimately this will produce 6 domains sharing the same financial theme that was shared in the initial intel.

Initial Intelligence

This post is based on initial intelligence shared by [@unit42_intel](#) in an original post [here](#).

In this post, Unit42 shared details of a `treasurybanks[.]org` domain used in malicious ads targeting users looking for funds recovery services.

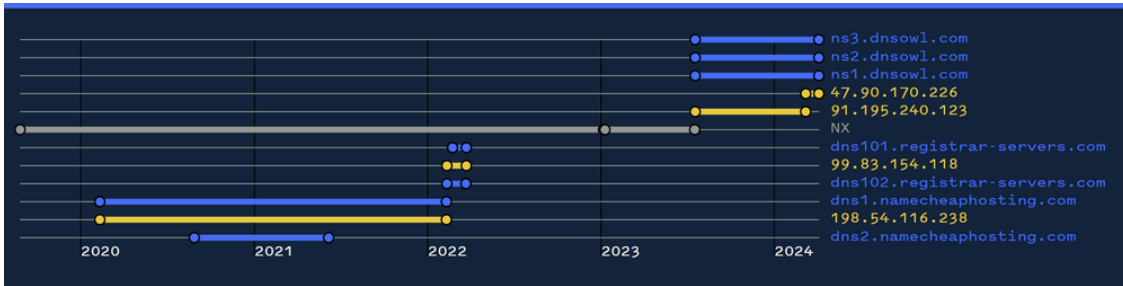


Review of First Historical Address

Since the initial indicator was a domain and not an IP address, we can use a passive dns tool like Validin to review indicators and history about the domain.

Our first step here is to look for historical IP resolutions which may point to similar domains hosted on the same servers.

Leveraging Valadin for the [initial search](#), we can see that the domain has recently resolved to 47.90.170[.]226 and 91.195.240[.]123



Our next step was to review the historical records for these IP addresses and determine if they resolved to any similar-looking domains in a similar time period.

Reviewing the most recent resolved IP address of 47.90.170[.]226, there are 19 domains that have been associated with this address. The most recent 5 domains are the original treasurybanks[.]org and the subdomains www, get, download, file .

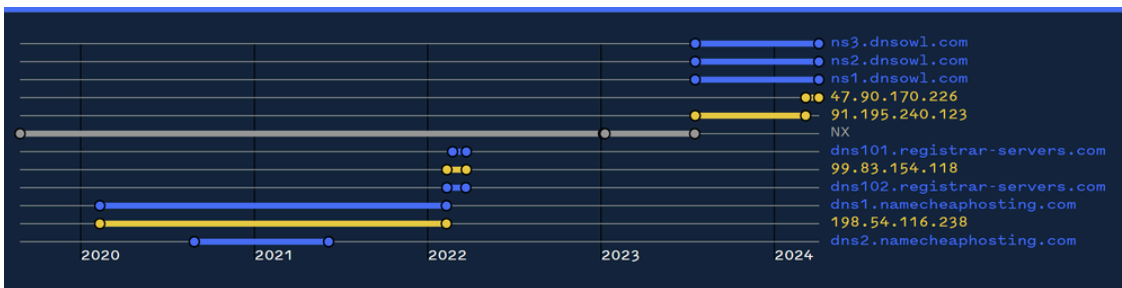
The other domains here are from a much older time period and do not show any indications of being related to treasurybanks[.]org, so we decided to ignore these and come back later if other searches did not yield results.



Review of Second Historical Address

The second most recent resolved IP address for treasurybanks[.]org is 91.195.240[.]123 .

We can again pivot and investigate this IP address for similar domain records that may point us to similar sites.



The address 91.195.240[.]123 has a huge number of past records, indicating that it is likely a proxy or some kind of "middle" infrastructure shared amongst thousands of other sites.

Reviewing the historical records did not yield any useful results.

91.195.240.123

AS 47846 (SEDO-AS)

0 Low 0 Med 1 High

Reputation OSINT (4) Resolutions (5000+) Subdomains DNS Records (109) Host Connections (5000+) Host Responses (5064) CT Stream (0)

TABLE VIEW TIMELINE VIEW

Key	Type	Value	First Seen	Last Seen
91.195.240.123 AS 47846	A	rppwe.club	2023-05-24	2024-04-03
91.195.240.123 AS 47846	A	kkkwe.club	2023-05-24	2024-04-03
91.195.240.123 AS 47846	A	vbkwe.club	2023-06-01	2024-04-03

Reviewing the historical DNS records also did not yield any results for similar sites.

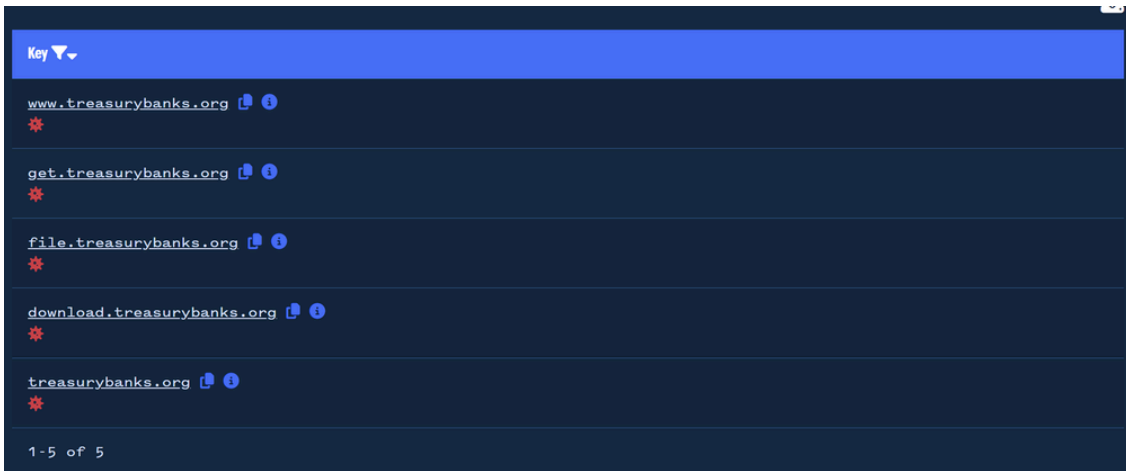
Reputation OSINT (4) Resolutions (5000+) Subdomains DNS Records (109) Host Connections (5000+) Host Responses (5064) CT Stream (0)

TABLE VIEW TIMELINE VIEW

Key	Type	Value	First Seen	Last Seen
91.195.240.123	HTTPS_FOR	whited.shop	2023-08-03	2023-08-03
91.195.240.123	HTTPS_FOR	www.fairysselection.com	2023-07-20	2023-08-03
91.195.240.123	HTTPS_FOR	m.sagatee.com	2023-08-03	2023-08-03
91.195.240.123	HTTPS_FOR	hg2023.one	2023-08-03	2023-08-03
91.195.240.123	HTTPS_FOR	boomzap.top	2023-07-27	2023-07-27
91.195.240.123	HTTPS_FOR	www.vgame02.top	2023-07-27	2023-07-27

Finding a First Pivot Point

Attempts to pivot on the historical IP records did not yield any meaningful results, so we decided to return to the interesting subdomains that we observed on the initial `treasurybanks[.]org`.



If we inspect the Certificate history for the `treasurybanks[.]org` domain, we can see that these subdomains are hardcoded into the Certificate (this is in contrast to a typical wildcard certificate with something like `*.treasurybanks[.]org`)

Since the subdomains are hardcoded, we decided to use them as a pivot point.

Of additional note here, is that the certificate leverages GeoTrust and was registered on `2024-03-06`. This information we can leverage as additional pivot points later.

Certificate

Common Name

```
treasurybanks.org
```

All Domains

```
treasurybanks.org  
download.treasurybanks.org  
file.treasurybanks.org  
get.treasurybanks.org  
www.treasurybanks.org
```

Not Before

```
2024-03-06T00:00Z
```

Not After

```
2025-03-05T23:59Z
```

Authority Info

```
http://cacerts.geotrust.com/GeoTrustTLRSACAG1.crt  
http://status.geotrust.com
```

Fingerprint

```
ef7f7cffa225fc49f2ea139b70dc59feb03ffa8c
```

Pivoting on Subdomains In TLS Certificates

We can now attempt to leverage the following indicators to identify new domains.

- Hardcoded subdomains (www, file, get, download)
- Use of GeoTrust for Certificate signing
- Registration dates around March 2024

To perform the initial search for hardcoded subdomains, we leveraged Censys to search certificates with hardcoded values beginning with the previously identified subdomains.



The initial results for this search returned 581 results. Many of which did not look anything like the original certificate for `treasurybanks[.]org`.

Certificates
Results: 581 Time: 6.34s

🌐 CN=dashboard.ensodata.com

🏠 Google Trust Services LLC GTS CA 1D4
📅 2024-04-03 – 2024-07-02

🌐 6gwk9.podb.incentable.com, admin.glorified.io, admin.luka.la, adminmeta.melzo.com, agilemapper.staging.roadbotics.com, airportwatcher.com, ankitsangwan.com, api.onroad.app, aplinder.com, apollo4u.demo.medeintegra.app, app.hupla.fr, app.nurmuhammad.com, app.v2.polyflow.co, argumentos.roda.dev, auth.zlnk.io, beta.admin.taj.upswing.global, bishops-see-connect.equiem.mobi, bittheory.io, clout.platformance.io, console.axwhite.com, cos4env.eu, d-vision.tokyo, dashboard.ensodata.com, development-agile-webapp.knolskape.io, dispatch.zomio.com, dlinks.meetlete.com, download.beespilot.app, editor-steamhub.idealabkids.com, egamebook.com, eraofnocode.com, exu1cpoa.org, feedback.mjcholdings.com.au, files.jupiterpi.de, fleet.gogpsgo.com, frenzyflowers.shop, fresh-accounts.hummingbirdtech.com, function.koalahospital.org.au, getelleratlet.se, gourmetgurugroup.com, greysonalloys.com, heist.fun, hello.idverse.com, herospace.app, instapack.eu, investment-accounting.resre.bm, ironheartindustries.com, jmclimousine.com, link.dovewallettest.com, link.rofl.nu, maherskitchen.com, pels.ramtinmovahed.com, reach-dev.me, referral.xrex.exchange, reports.rsamb.com, schutzmittelplattform.de, sharktankbreakdown.com, shouldhavebought.com, shraddha.rahulsawant.dev, shreyashkarandikar.com, skycast.gallichan.app, st6i2.podc.incentable.com, stage.svar.as, student.examind.io, taskflow.solutions, theopenborders.com, tiruppur.yazhdroptaxi.com, tobitobertson.com, tryingsg.com, u17r.com, vapelegends.ca, vbschools.playfuturetraders.com, ventonorteimoveis.com.br, wayz.app, web.bff.chat, wiziontech.com, wordoff.app, www.brmapp.net, www.coastcaritas.org, www.denellwong.com, www.donne-cosi.org, www.eerielabs.app, www.ellisarp.com, www.eraofnocode.com, www.gferrami.com, www.imiexpres.sk, www.linenbuild.com, www.lionandfox.co.uk, www.miralo.pl, www.niemeyer.wtf, www.ricomenu.es, www.rschemistry.com, www.ryseeng.com, www.spreadthevote.net, www.stevenscottbragg.com, www.techgicus.com, www.wobith.de, yekola-lingala.com, yuricholak.tech, zaharzagrava.com, zavadil.pro

However after scrolling slightly through the first page of results, we can see two certificates (`maxrecovery[.]org` and `myfundsrecovery[.]org`) that look extremely similar to our initial `treasurybanks[.]org`.

We can also note that both of these certificates are registered with GeoTrust and were registered in March 2024.

🌐 CN=maxrecovery.org

🏠 DigiCert Inc GeoTrust TLS RSA CA G1
📅 2024-03-27 – 2025-03-27

🌐 download.maxrecovery.org, file.maxrecovery.org, get.maxrecovery.org, maxrecovery.org, www.maxrecovery.org

🌐 CN=filedriveo.xyz

🏠 Let's Encrypt R3
📅 2024-03-26 – 2024-06-24

🌐 chamkhn.cfd, despdownload.shop, downldasdfsosofts.click, downldocflu.online, downldsmra.shop, downldtbsm.site, downloadespl.click, downloadharon.site, downloadsndi.site, filedriveo.xyz, getwithpremium.click, pcreafacz.click, premiumworks.click, roostfiles.click, www.chamkhn.cfd, www.despdownload.shop, www.downldasdfsosofts.click, www.downldocflu.online, www.downldsmra.shop, www.downldtbsm.site, www.downloadespl.click, www.downloadharon.site, www.downloadsndi.site, www.filedriveo.xyz, www.getwithpremium.click, www.pcreafacz.click, www.premiumworks.click, www.roostfiles.click, www.yiouce348.click, yiouce348.click

🌐 CN=myfundsrecovery.org

🏠 DigiCert Inc GeoTrust TLS RSA CA G1
📅 2024-03-25 – 2025-03-25

🌐 download.myfundsrecovery.org, file.myfundsrecovery.org, get.myfundsrecovery.org, myfundsrecovery.org, www.myfundsrecovery.org

Applying Filters On GeoTrust/Digicert

To hone in on the results, we can add a filter for DigiCert (owner of GeoTrust) certificates. This narrows us down to 15 related certificates.



Certificates
Results: 15 Time: 11.75s

- CN=Treasurybanks.org**
 - DigiCert Inc GeoTrust TLS RSA CA G1
 - 2024-03-06 – 2025-03-05
 - Treasurybanks.org, download.treasurybanks.org, file.treasurybanks.org, get.treasurybanks.org, www.treasurybanks.org

Some of these look exactly like our original domain, indicating that we are getting closer to desirable search results.

Certificates
Results: 15 Time: 11.75s

- CN=Treasurybanks.org**
 - DigiCert Inc GeoTrust TLS RSA CA G1
 - 2024-03-06 – 2025-03-05
 - Treasurybanks.org, download.treasurybanks.org, file.treasurybanks.org, get.treasurybanks.org, www.treasurybanks.org
- CN=astrologytop.com**
 - DigiCert Inc GeoTrust TLS RSA CA G1
 - 2024-02-09 – 2025-02-09
 - astrologytop.com, download.astrologytop.com, file.astrologytop.com, get.astrologytop.com, www.astrologytop.com
- CN=myfundsrecovery.org**
 - DigiCert Inc GeoTrust TLS RSA CA G1
 - 2024-03-25 – 2025-03-25
 - download.myfundsrecovery.org, file.myfundsrecovery.org, get.myfundsrecovery.org, myfundsrecovery.org, www.myfundsrecovery.org

However if we scroll down to the end of our 15 results, there are still multiple hits for certificates that don't look anything like our `treasurybanks[.]org`

We can also see that these certificates were registered years ago and are now expired, so we can leverage this to filter them out.

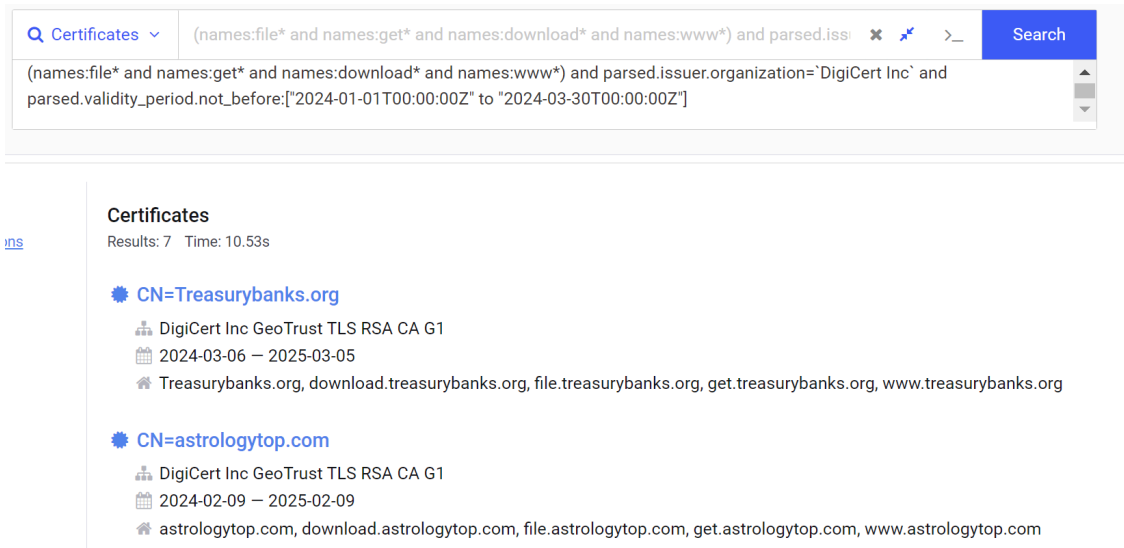
- C=US, ST=California, L=Campbell, O=CDNetworks Inc., CN=support15.cdnetworks.net**
 - DigiCert SHA2 High Assurance Server CA
 - 2019-11-14 – 2021-02-09
 - *.aquan.bizwill.net, *.aquan.eduwill.net, *.aquan.neungyule.com, *.aquan.studywill.net, *.babyjoyclub.com, *.bizwill.net, *.boyaa.com, *.boyaa.us, *.c.blog.so-net.ne.jp, *.c.blogs.so-net.ne.jp, *.dwa.cdnetworks.com, *.dwa.krhttpvod.cdnetworks.com, *.eduwill.net, *.giftcatalog.jp, *.gw-dev.jp, *.j-tabimono.com, *.jonahbass.com, *.kokorobiyori.net, *.kx88.com, *.kyods.com, *.lifree.com, *.mamypoko.com, *.meiyin.meitu.com, *.misumi.com.cn, *.moony.com, *.myseleca.jp, *.neungyule.com, *.pantherssl.com, *.rubanne.jp,

Applying Time-Based Filters

To filter out the 8 undesired results, we can either apply a filter to ignore expired certificates (`and not labels:expired`) or apply a new filter specifying that we only want results registered in 2024.

We chose to apply the second option, allowing only for certificates registered in 2024. We can see this applied to the `parsed.validity_period.not_before` field, specifying a date range of 2024-01-01 to 2024-03-30.

[After applying these filters](#) we are left with 7 results.

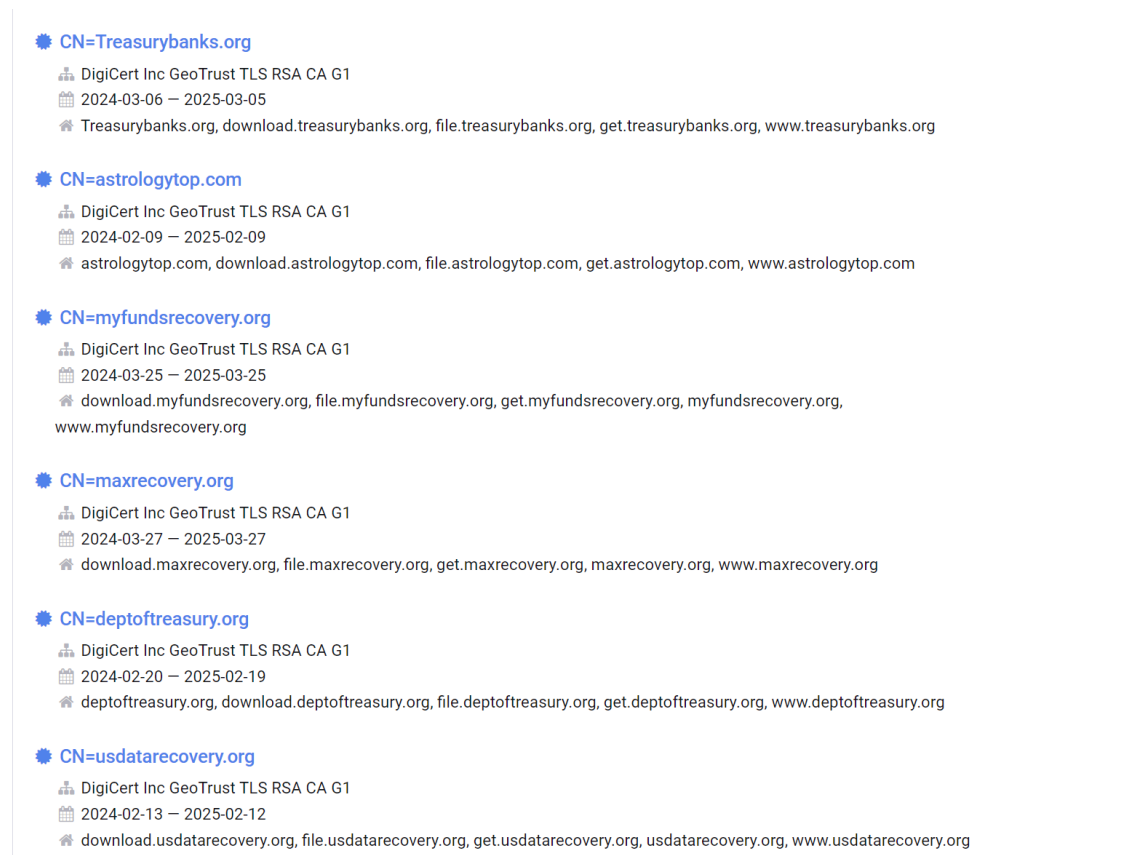


The screenshot shows a search interface with a query bar containing the following query: `(names:file* and names:get* and names:download* and names:www*) and parsed.issuer.organization='DigiCert Inc' and parsed.validity_period.not_before:['2024-01-01T00:00:00Z' to '2024-03-30T00:00:00Z']`. Below the query bar, the search results are displayed under the heading "Certificates". The results show two entries:

- CN=Treasurybanks.org**
 - DigiCert Inc GeoTrust TLS RSA CA G1
 - 2024-03-06 – 2025-03-05
 - Treasurybanks.org, download.treasurybanks.org, file.treasurybanks.org, get.treasurybanks.org, www.treasurybanks.org
- CN=astrologytop.com**
 - DigiCert Inc GeoTrust TLS RSA CA G1
 - 2024-02-09 – 2025-02-09
 - astrologytop.com, download.astrologytop.com, file.astrologytop.com, get.astrologytop.com, www.astrologytop.com

Of particular interest here, is that our final 7 results all

- follow the same subdomain structure
- Are registered in March 2024
- Mostly follow the same financial theme

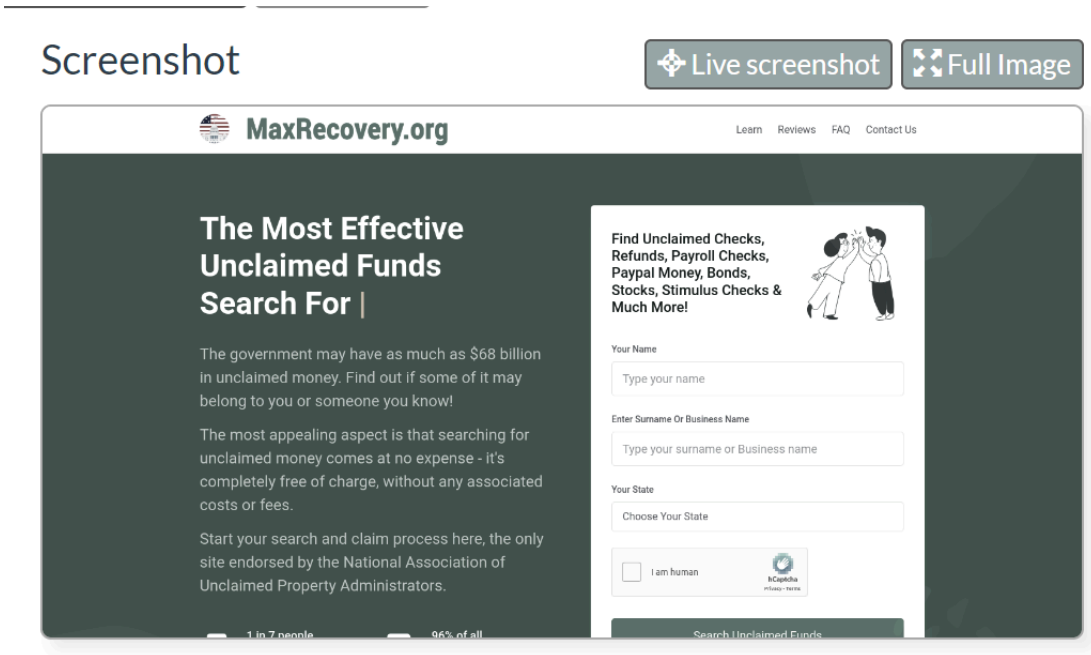


The screenshot shows a list of seven search results for certificates, each with a subdomain structure, issuer information, validity period, and associated domains:

- CN=Treasurybanks.org**
 - DigiCert Inc GeoTrust TLS RSA CA G1
 - 2024-03-06 – 2025-03-05
 - Treasurybanks.org, download.treasurybanks.org, file.treasurybanks.org, get.treasurybanks.org, www.treasurybanks.org
- CN=astrologytop.com**
 - DigiCert Inc GeoTrust TLS RSA CA G1
 - 2024-02-09 – 2025-02-09
 - astrologytop.com, download.astrologytop.com, file.astrologytop.com, get.astrologytop.com, www.astrologytop.com
- CN=myfundsrecovery.org**
 - DigiCert Inc GeoTrust TLS RSA CA G1
 - 2024-03-25 – 2025-03-25
 - download.myfundsrecovery.org, file.myfundsrecovery.org, get.myfundsrecovery.org, myfundsrecovery.org, www.myfundsrecovery.org
- CN=maxrecovery.org**
 - DigiCert Inc GeoTrust TLS RSA CA G1
 - 2024-03-27 – 2025-03-27
 - download.maxrecovery.org, file.maxrecovery.org, get.maxrecovery.org, maxrecovery.org, www.maxrecovery.org
- CN=deptoftreasury.org**
 - DigiCert Inc GeoTrust TLS RSA CA G1
 - 2024-02-20 – 2025-02-19
 - deptoftreasury.org, download.deptoftreasury.org, file.deptoftreasury.org, get.deptoftreasury.org, www.deptoftreasury.org
- CN=usdatarecovery.org**
 - DigiCert Inc GeoTrust TLS RSA CA G1
 - 2024-02-13 – 2025-02-12
 - download.usdatarecovery.org, file.usdatarecovery.org, get.usdatarecovery.org, usdatarecovery.org, www.usdatarecovery.org

Leveraging urlscan.io to search on these domains, we can see extremely similar structure to that initially reported by Unit42.

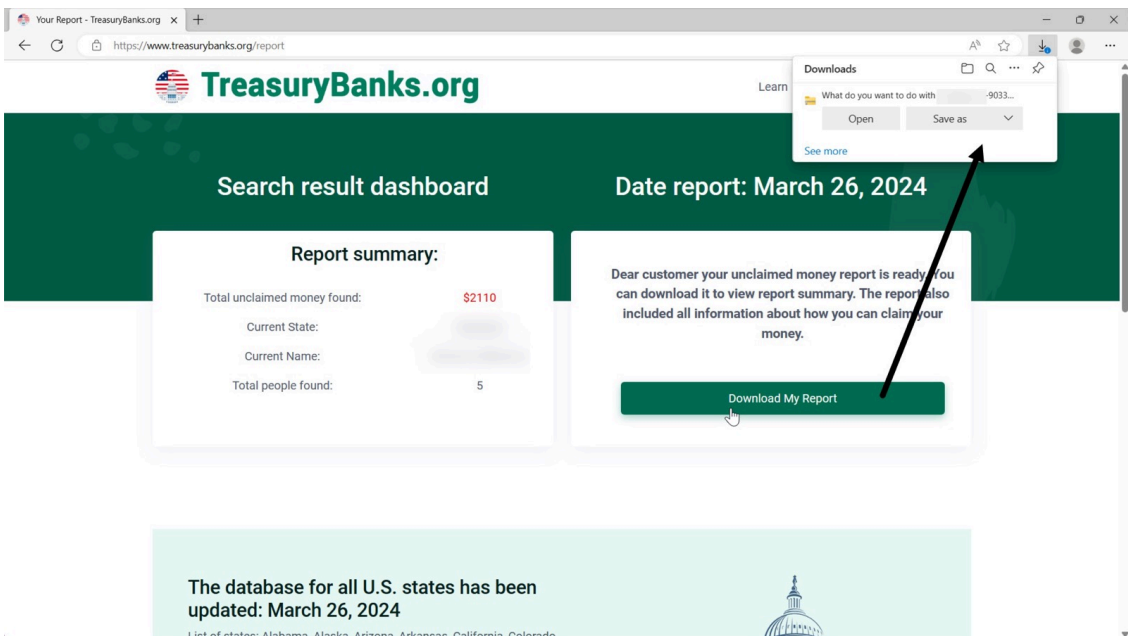
Here is a screenshot from our newly identified domain `maxrecovery[.]org`



Page Title

MaxRecovery.org | Search For Your Unclaimed money and Assets - It's Free | Trusted Authority in Unclaimed Property

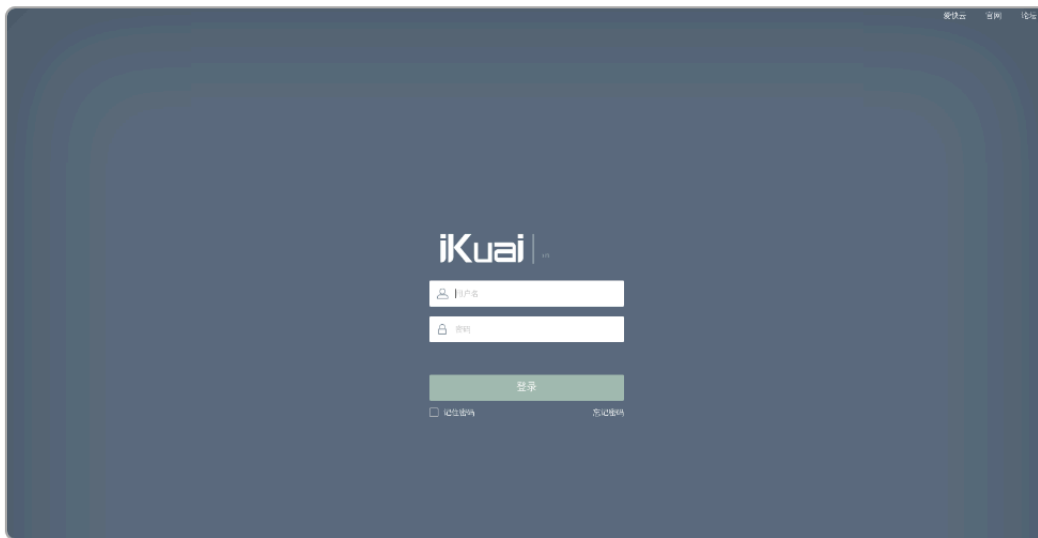
and here is a screenshot from the initial reported domain of `treasurybanks[.]org`



Astrologytop[.]com seems to be completely different and maybe a control panel or something completely different in nature.

Screenshot

Live screenshot Full Image



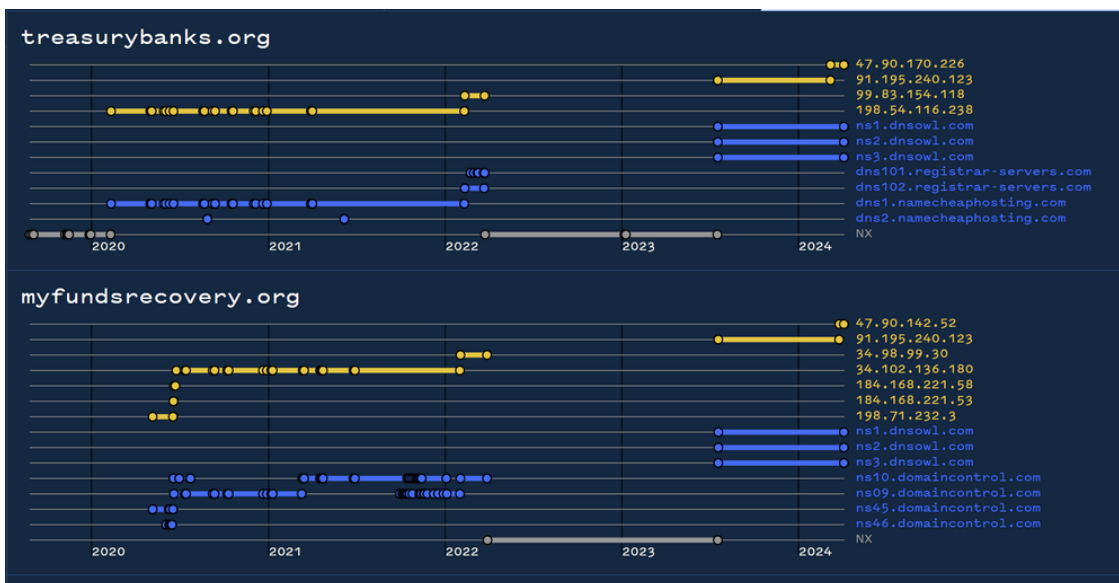
Page Title

登录

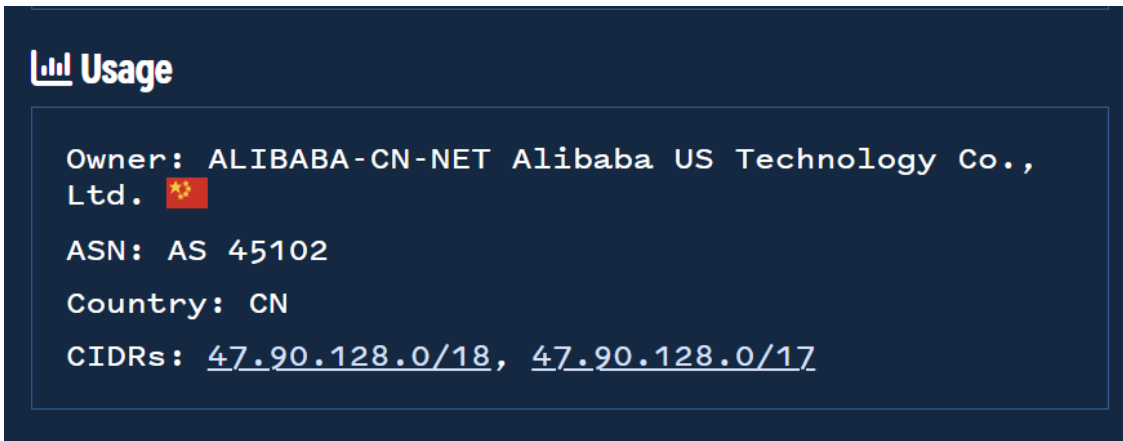
Bulk Review of Domain History

Returning to Validin with our new list of domains, we can perform a [bulk](#) search to look for commonalities.

This reveals that many of the results have previously resolved to `91.195.240[.]123`, demonstrating an additional link in their history.



We can also note that the most recent resolved addresses are different but all resolve to ranges owned by Alibaba. Indicating another commonality.



Usage

Owner: ALIBABA-CN-NET Alibaba US Technology Co., Ltd. 🇨🇳

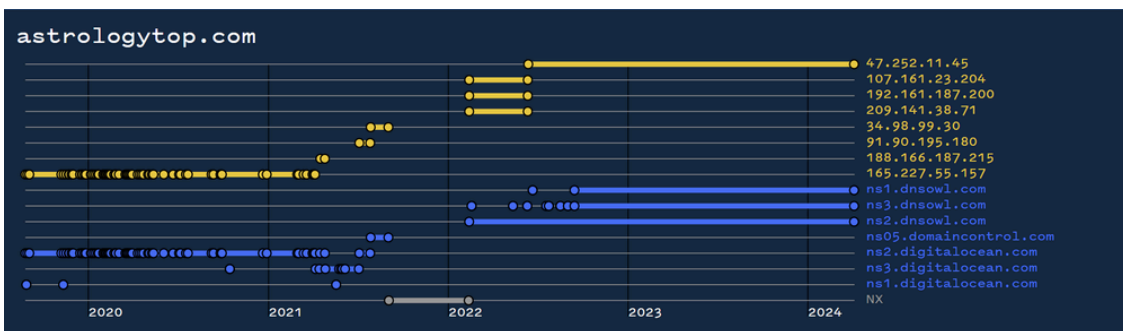
ASN: AS 45102

Country: CN

CIDRs: 47.90.128.0/18, 47.90.128.0/17

One slight exception to this pattern is the `astrologytop[.]com` domain, which currently resolves to an Alibaba IP but does not share the same history as the other domains.

We were unable to confirm for sure whether this domain was definitely related. However there are enough suspicious indicators to suggest that it might be.



Sign up for Embee Research

Malware Analysis and Threat Intelligence Research

No spam. Unsubscribe anytime.

Final Domains

- High Confidence
- treasurybanks[.]org
- myfundsrecovery[.]org
- maxrecovery[.]org
- deptoftreasury[.]org
- usdatarecovery[.]org

Lower Confidence

astrologytop[.]com

All Results

Treasurybanks[.]org

download[.]treasurybanks[.]org

file[.]treasurybanks[.]org

get[.]treasurybanks[.]org

www[.]treasurybanks[.]org

astrologytop[.]com

download[.]astrologytop[.]com

file[.]astrologytop[.]com

get[.]astrologytop[.]com

www[.]astrologytop[.]com

myfundsrecovery[.]org

download[.]myfundsrecovery[.]org

file[.]myfundsrecovery[.]org

get[.]myfundsrecovery[.]org

www[.]myfundsrecovery[.]org

maxrecovery[.]org

download[.]maxrecovery[.]org

file[.]maxrecovery[.]org

get[.]maxrecovery[.]org

www[.]maxrecovery[.]org

deptoftreasury[.]org

download[.]deptoftreasury[.]org

file[.]deptoftreasury[.]org

get[.]deptoftreasury[.]org

www[.]deptoftreasury[.]org

usdatarecovery[.]org

download[.]usdatarecovery[.]org

file[.]usdatarecovery[.]org

get[.]usdatarecovery[.]org

www[.]usdatarecovery[.]org

Source: <https://www.embeeresearch.io/tls-certificates-for-threat-intel-dns/>