Determining the Attack Surface

By: Ryan Stewart

Introduction:

Traditional threat intelligence models are **facing limitation**s in today's rapidly evolving cybersecurity landscape. The introduction of the External Attack Surface concept has underscored these shortcomings, prompting a paradigm shift in threat intelligence. **Extended Threat Intelligence (XTI)** has emerged as a popular alternative, distinct from classical intelligence models. XTI focuses on creating an attack surface unique to an organization, providing a **targeted** perspective for intelligence generation. This approach empowers organizations with enhanced visibility, uncovering **overlooked endpoints** or **subdomains** and enabling a **comprehensive** inventory of assets for precise defense strategies.

Determining the Attack Surface:

When creating the attack surface, domains, subdomains, websites, login pages, CMS applications, technologies used on websites, IP addresses, IP blocks, DNS records, C-level employee mails, network applications, operating systems, bin numbers, and swift codes, and SSL certificates will be included. We will determine all these by proceeding through the main domain, which was provided to us by the organization as per the scenario.

1. Domains:

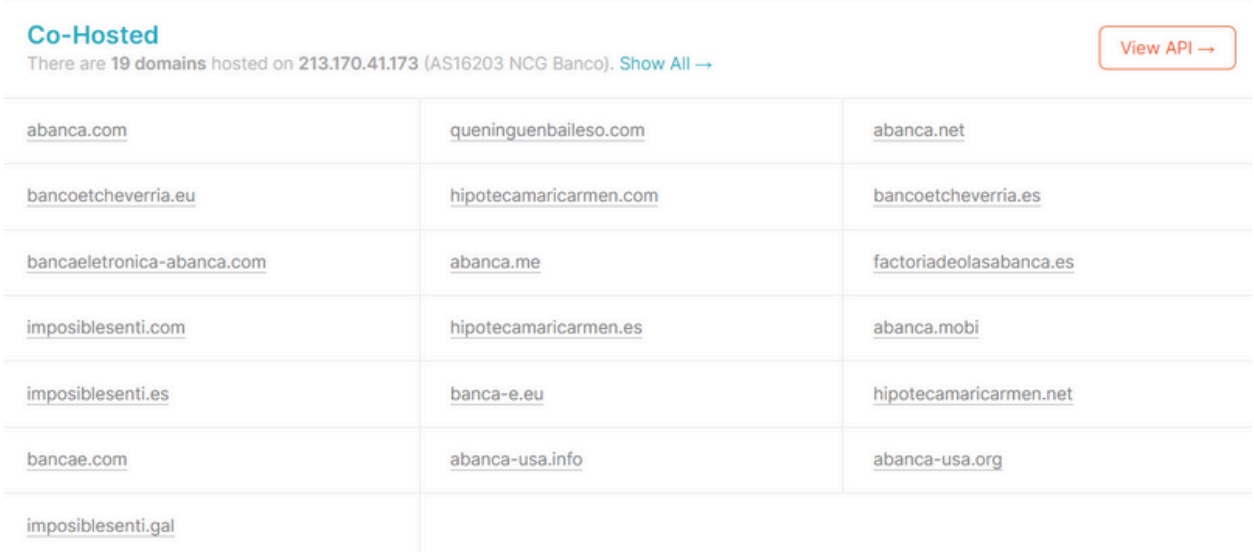
- The only information that will be given to us in the first place will be the primary domain of the organization, such as abanca.com.(**Main domain**)

- Utilize **host.io** to identify related domains, considering redirects, co-hosted domains, backlinks, and domain information from **whois records.**

- Verify potential domains through reverse whois lookups and DNS record examinations.

- Assess domains hosted on organization-specific nameservers, adding them to the inventory post-verification.

In order to find other domains of the company, we can find domains that provide redirects to the main domain. **We can use the host.io service for this.** Host.io will provide us with all the domains hosted on the same IP, the domains hosting the relevant domain within the website, and other domains hosted by the relevant domain within the website, apart from other domains that provide redirection to the relevant domain. **Not all** domains obtained may belong to the organization. We can decide which domains belong to the organization and which ones don't by checking the **whois outputs** of the domains or by looking at their content.



When we search the **abanca.com** domain on host.io, we can also see other domains hosted on the same IP address in the **"Co-Hosted"** section.

Backlinks

There are **249 domains** which backlink to **abanca.com**. Show All →

View API →

banesco.com	banesco.com.pa	bizum.es
fbmpa.es	cuentasclaras.es	mundiario.com
rccelta.es	rcdeportivo.es	scdmilagrosa.com
aerosantiago.es	museoconserva.com	clubfluviallugo.com
anunciantes.com	ismsforum.es	fexdega.com
hipotecamultiproducto.es	banesco.com.cw	clubvigo.com
travesiaanadocostaserena.es	rompetino.org	spaniardsfc.co.uk
fexdega.es	carrilanasesteiro.com	cristalizaservicios.es

In a subsection, we can view other domains that contain our relevant domain, and after making the necessary verifications, we can include these domains in our asset list.

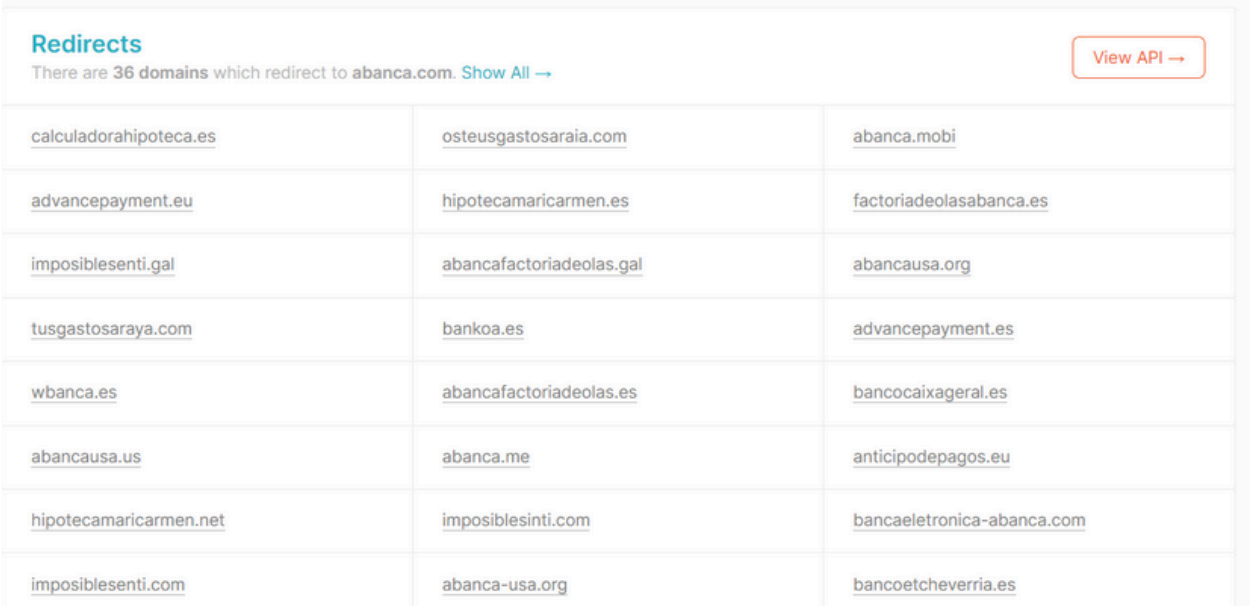
Links to

There are **15 domains** which **abanca.com** links to.

View API →

twitter.com	facebook.com	linkedin.com
instagram.com	cuentasclaras.es	tusitiodecompras.es
escogecasa.es	uie.edu	youtube.com
abancacorporacionbancaria.com	abancaserfin.com	abancausa.com
abanca.pt	unepfi.org	unpri.org

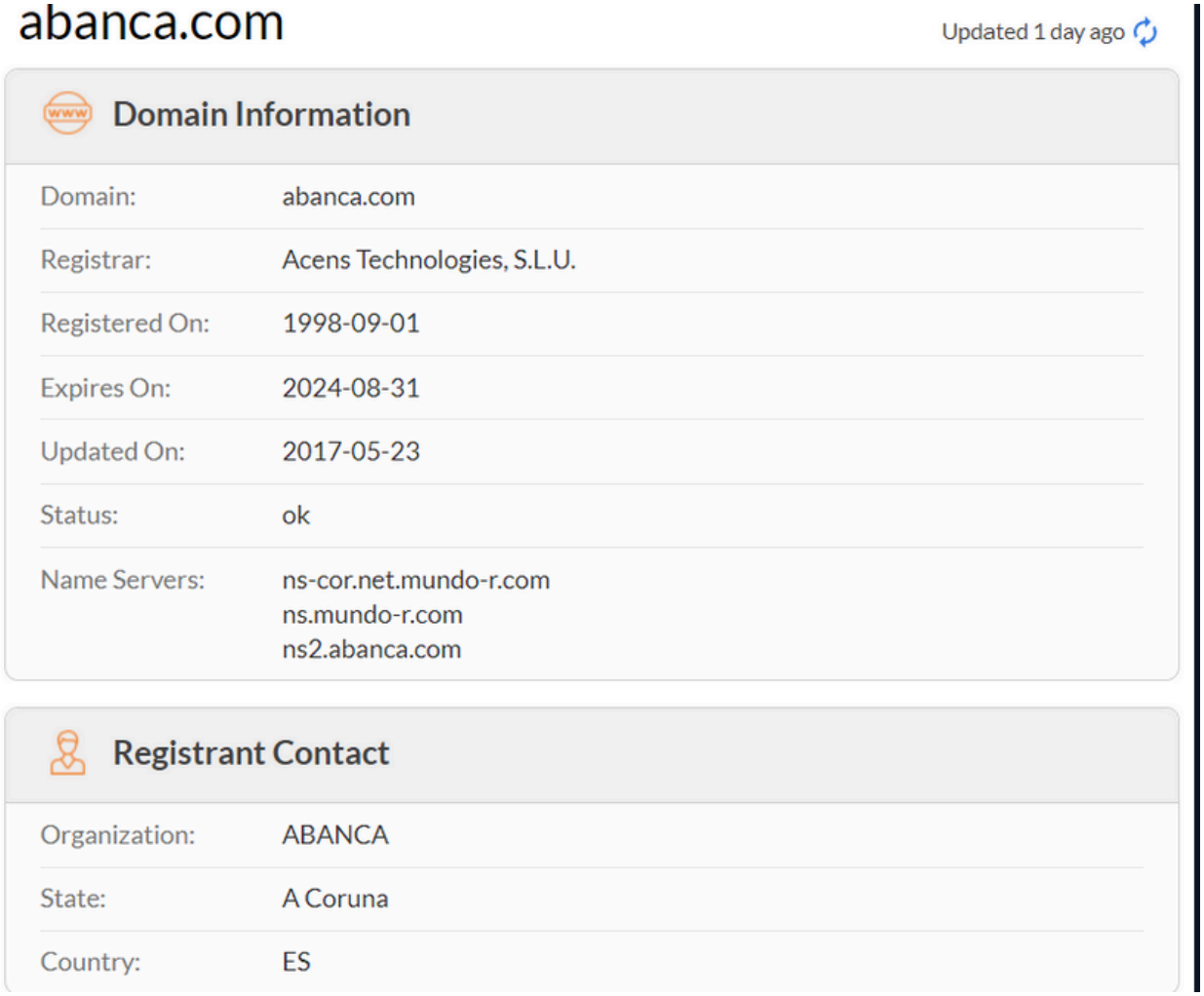
In the **"Links to"** section, we can view other domains that our domain hosts within the website.



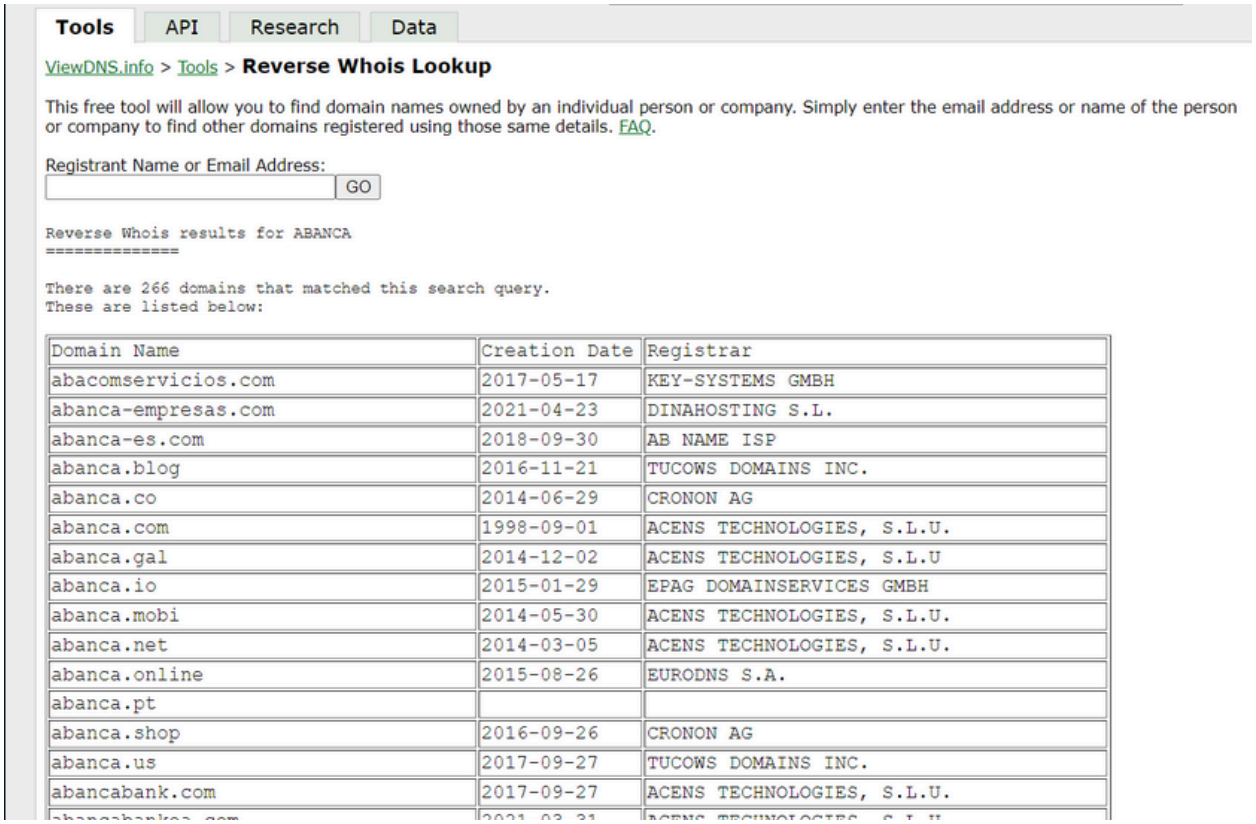
In the **Redirects** section, we can view other domains directed to our domain.

Since the number of domains displayed on the screen is limited, we can obtain all domains via the API by **becoming a member.**

As a secondary method, we can find similar information in whois records of the primary domain we are working on by performing a **Reverse whois lookup** (Reverse by Org Name, reverse by Registrant Mail, etc.) for certain information.



For example, when we look at the **whois information** of the abanca.com domain, we see that the organization section contains the name of the company. We will be able to see all other domains registered under this organization name when we reverse the organization name. We will use the reverse whois tool at viewdns.info for this.



Tools | API | Research | Data

ViewDNS.info > Tools > **Reverse Whois Lookup**

This free tool will allow you to find domain names owned by an individual person or company. Simply enter the email address or name of the person or company to find other domains registered using those same details. FAQ.

Registrant Name or Email Address:

GO

Reverse Whois results for ABANCA

There are 266 domains that matched this search query.
These are listed below:

Domain Name	Creation Date	Registrar
abacomservicios.com	2017-05-17	KEY-SYSTEMS GMBH
abanca-empresas.com	2021-04-23	DINAHOSTING S.L.
abanca-es.com	2018-09-30	AB NAME ISP
abanca.blog	2016-11-21	TUCOWS DOMAINS INC.
abanca.co	2014-06-29	CRONON AG
abanca.com	1998-09-01	ACENS TECHNOLOGIES, S.L.U.
abanca.gal	2014-12-02	ACENS TECHNOLOGIES, S.L.U
abanca.io	2015-01-29	EPAG DOMAINSERVICES GMBH
abanca.mobi	2014-05-30	ACENS TECHNOLOGIES, S.L.U.
abanca.net	2014-03-05	ACENS TECHNOLOGIES, S.L.U.
abanca.online	2015-08-26	EURODNS S.A.
abanca.pt		
abanca.shop	2016-09-26	CRONON AG
abanca.us	2017-09-27	TUCOWS DOMAINS INC.
abancabank.com	2017-09-27	ACENS TECHNOLOGIES, S.L.U.

266 domains containing this name were displayed when we searched "ABANCA" in the search section. These domains are potentially our domains. *After we verify each one, we can add it to our inventory.*

A / AAAA Record	Provider	ASN
213.170.41.173 (ES) used by 2 domains	NCG Banco (ES)	AS16203

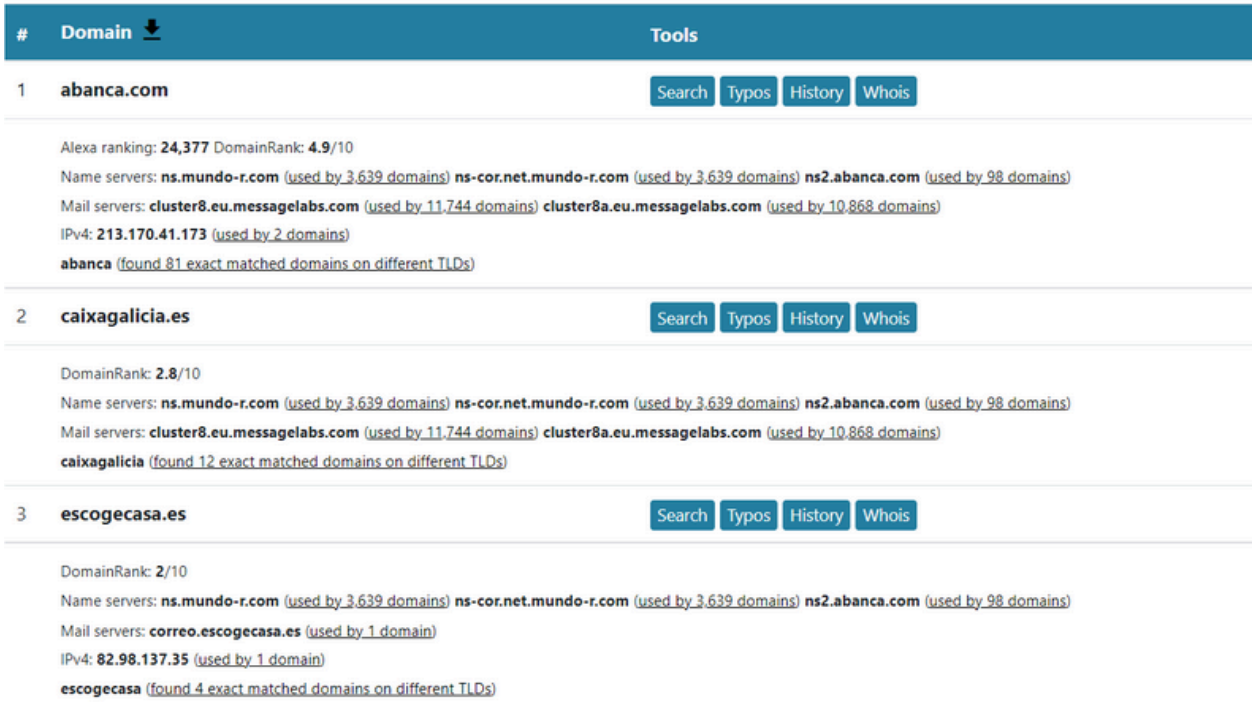
NS Record	IP Address	Provider	ASN
ns.mundo-r.com used by 3,639 domains	212.51.33.73 (ES)	R Cable y Telecable Telecomunicaciones, S.A.U. (ES)	AS12334
ns-cor.net.mundo-r.com used by 3,639 domains	212.51.33.106 (ES)	R Cable y Telecable Telecomunicaciones, S.A.U. (ES)	AS12334
ns2.abanca.com used by 98 domains	213.170.41.11 (ES)	NCG Banco (ES)	AS16203

MX Record	IP Address	Provider	ASN
cluster8.eu.messagelabs.com (pref: 10) used by 11,744 domains	85.158.142.211 (GB)	Amazon.com, Inc. (US)	AS16509
	85.158.142.216 (GB)	Amazon.com, Inc. (US)	AS16509
	195.245.230.195 (GB)	Amazon.com, Inc. (US)	AS16509
	195.245.230.198 (GB)	Amazon.com, Inc. (US)	AS16509
	195.245.231.66 (GB)	Amazon.com, Inc. (US)	AS16509
	195.245.231.71 (GB)	Amazon.com, Inc. (US)	AS16509
cluster8a.eu.messagelabs.com (pref: 20)	46.137.95.199 (IE)	Amazon.com, Inc. (US)	AS16509

Alternatively, we can use the whoxy.com tool to do the same check. With this tool, we can reverse whois in 4 categories with the help of this tool.

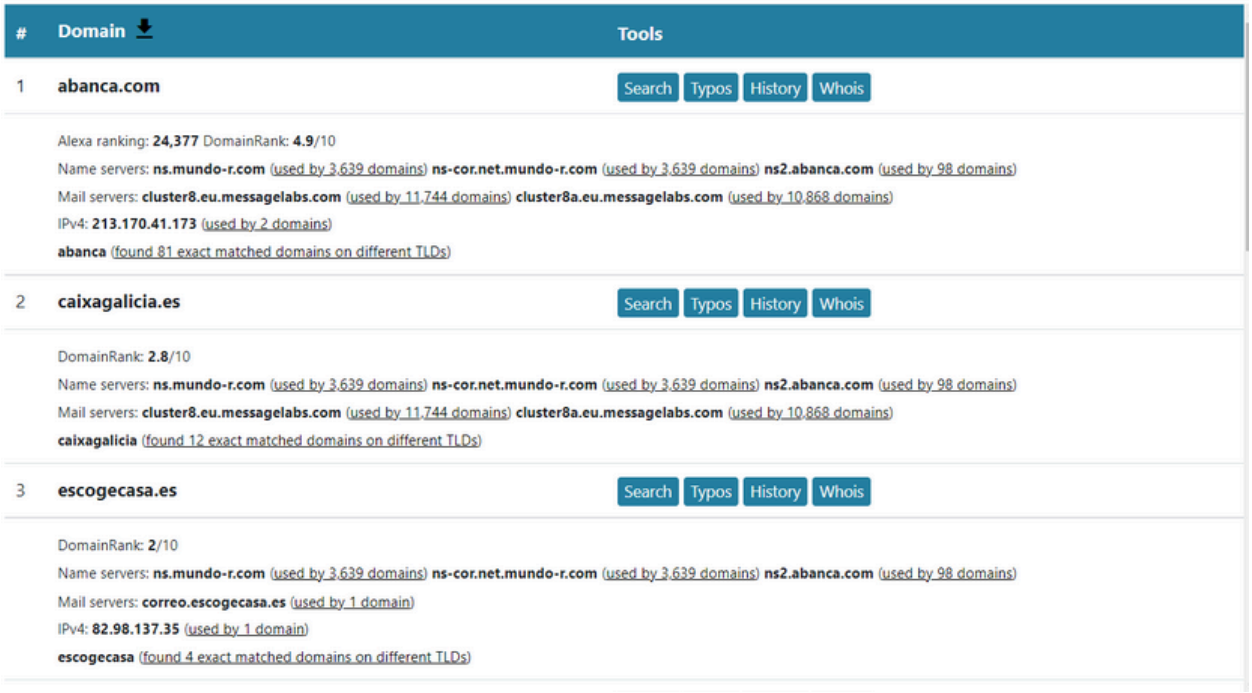
As a third method, we can examine the DNS records of the relevant domain and reach other domains using the same DNS records, **check these domains and add them to our inventory after verification.**

We can check the DNS records with the “**dig**” command on the command line or we can use the tools that work online on the internet. In this example, we are viewing DNS records using the **dnslytics.com** tool. In order to discover potential domains, we need to reverse records that are managed by the organization. For example, a shared nameserver belonging to any hosting company hosts too many domains, and these domains mostly do not belong to us. Therefore, it is useful to examine the records of the mail server or **nameserver** that **belongs to the organization.** In this example, the **ns2.abanca.com** record stands out. When the related nameserver is reversed on the same tool, it shows that **98 other domains** are hosted on this nameserver.



#	Domain	Tools
1	**abanca.com**	Search Typos History Whois
	Alexa ranking: **24,377** DomainRank: **4.9**/10 Name servers: **ns.mundo-r.com** (used by 3,639 domains) **ns-cor.net.mundo-r.com** (used by 3,639 domains) **ns2.abanca.com** (used by 98 domains) Mail servers: **cluster8.eu.messagelabs.com** (used by 11,744 domains) **cluster8a.eu.messagelabs.com** (used by 10,868 domains) IPv4: **213.170.41.173** (used by 2 domains) **abanca** (found 81 exact matched domains on different TLDs)	
2	**caixagalicia.es**	Search Typos History Whois
	DomainRank: **2.8**/10 Name servers: **ns.mundo-r.com** (used by 3,639 domains) **ns-cor.net.mundo-r.com** (used by 3,639 domains) **ns2.abanca.com** (used by 98 domains) Mail servers: **cluster8.eu.messagelabs.com** (used by 11,744 domains) **cluster8a.eu.messagelabs.com** (used by 10,868 domains) **caixagalicia** (found 12 exact matched domains on different TLDs)	
3	**escogecasa.es**	Search Typos History Whois
	DomainRank: **2**/10 Name servers: **ns.mundo-r.com** (used by 3,639 domains) **ns-cor.net.mundo-r.com** (used by 3,639 domains) **ns2.abanca.com** (used by 98 domains) Mail servers: **correo.escogecasa.es** (used by 1 domain) IPv4: **82.98.137.35** (used by 1 domain) **escogecasa** (found 4 exact matched domains on different TLDs)	

All the domains that are listed here are potentially our own, as they are hosted on our own nameserver. **After performing the verification, we can add them to our inventory.**



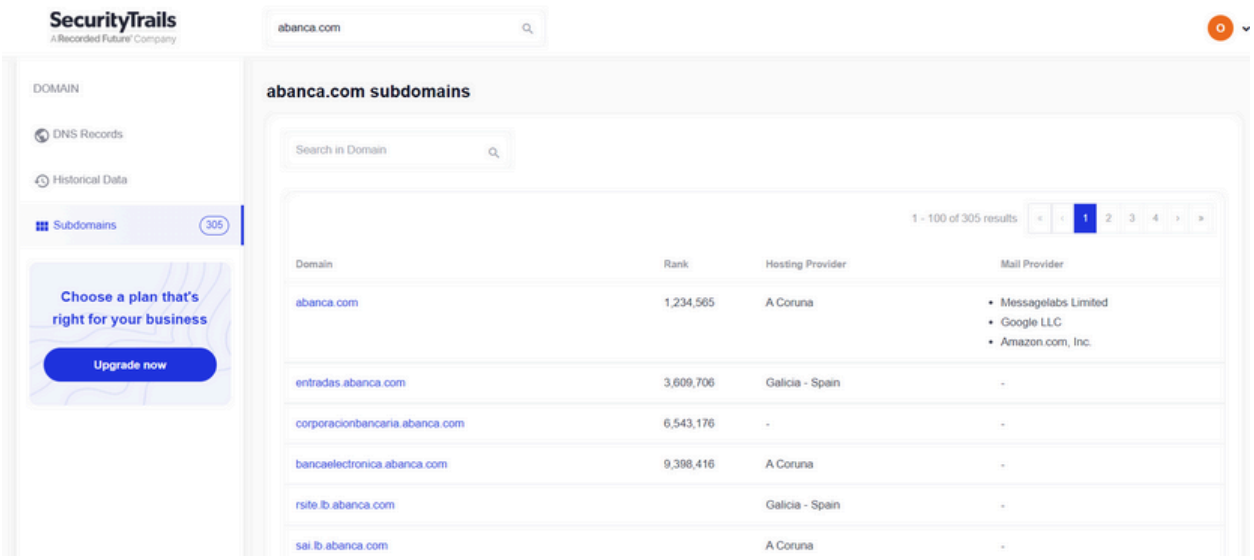
2. Subdomains:

- Employ tools like SecurityTrails, Aquatone, Sublist3r, and Assetfinder for comprehensive subdomain discovery.
- Aggregate data from multiple sources to compile an extensive list of subdomains.

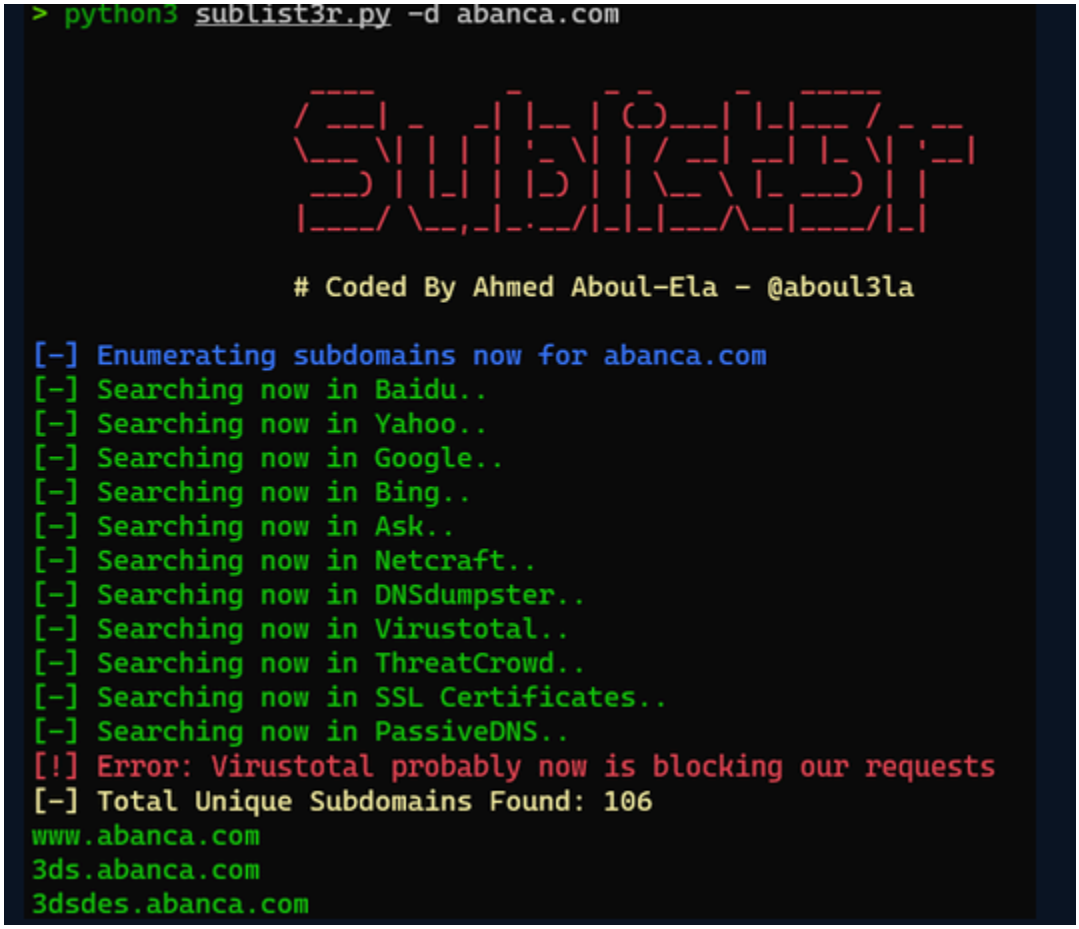
There are many tools that are available online or on the command line to find subdomains. We will now use 4 of them. These tools are SecurityTrails, Aquatone, Sublist3r, and Assetfinder.

SecurityTrails can be used on the command line via the hacktrails tool or API or queries can be made from the visual interface. It produces high-quality output.

https://securitytrails.com/list/apex_domain/abanca.com



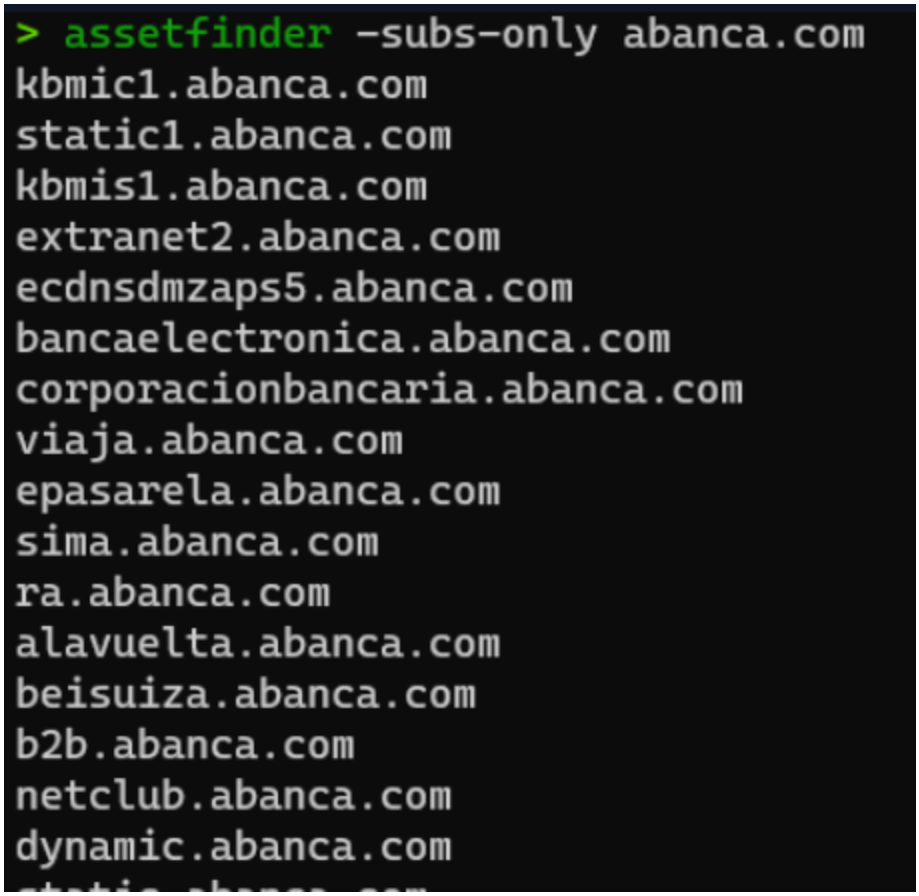
Secondly, the **Sublist3r tool** runs on the command line and finds and outputs findings from multiple sources. It is run with the command in the screenshot.



Thirdly, "**Aquatone**" collects data and produces output by querying from multiple sources, just like the **Sublist3r tool.** If you enter the necessary API keys in the configuration files for the resources that require API keys, the number of subdomains it finds will increase. **Aquatone** can check the activity **status** of the **subdomains** it finds with the help of the scan module it contains, and it can check whether there is a takeover vulnerability on the subdomains it finds with the help of the takeover module it has.

```
> aquatone-discover -d abanca.com
                                __
  ____ _____ ___  ______ _/ /_____  ____  ___
 / __ `/ __ `/ / / / __ `/ __/ __ \/ __ \/ _ \
/ /_/ / /_/ / /_/ / /_/ / /_/ /_/ / / / /  __/
\__,_/\__, /\__,_/\__,_/\__/\____/_/ /_/\___/
        /_/  discover v0.5.0 - by @michenriksen

Identifying nameservers for abanca.com... Done
Using nameservers:

 - 212.51.33.73
 - 213.170.41.11
 - 212.51.33.106

Checking for wildcard DNS... Done

Running collector: Wayback Machine... Done (61 hosts)
Running collector: VirusTotal... Skipped
 -> Key 'virustotal' has not been set
Running collector: Threat Crowd... Done (101 hosts)
Running collector: Shodan... Skipped
 -> Key 'shodan' has not been set
Running collector: Riddler... Skipped
 -> Key 'riddler_username' has not been set
Running collector: PublicWWW... Done (0 hosts)
Running collector: PTRArchive... Done (0 hosts)
Running collector: PassiveTotal... Skipped
 -> Key 'passivetotal_key' has not been set
```

Finally, with the “**assetfinder**” tool, you can query subdomains and obtain data from many sources.

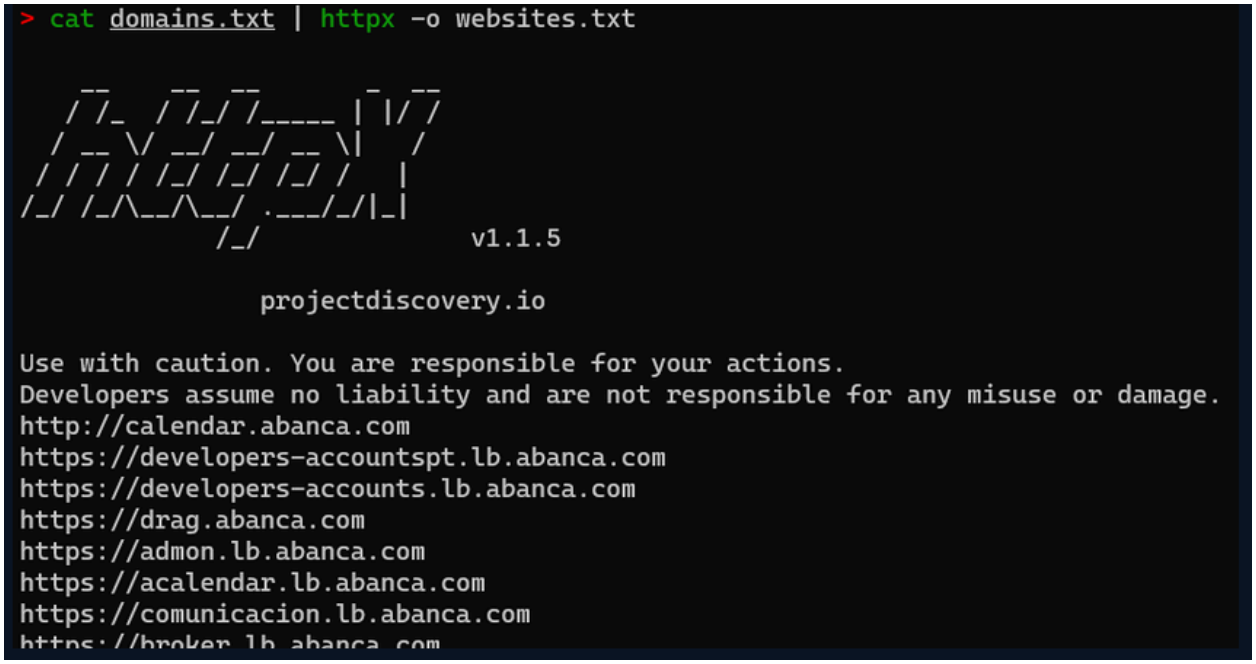


One of the **most important** points when searching for a subdomain is to get as much data from as many sources as possible. After collecting and bringing all the data together, we will have a fairly large list of subdomains.

3. Websites

- Send requests to domains and subdomains to identify active websites using tools like httpx or httprobe.
- Capture login pages by scripting the detection process, focusing on indicators like keywords, form tags, and expressions.

In order to find the websites, we need to send requests to the domains and subdomains we find. We obtain our active websites by examining the domains or subdomains that respond to our **HTTP/HTTPS** requests.



As you can see in the above screenshot, when we list all of our domains and scan them on the "**httpx** " tool, it will list all the domains that respond to our http/http requests. As an alternative to "httpx" tool you can also use "**httprobe**" tool which is a tool that will meet your needs with similar functions.

Login Pages

Detecting websites with login screens poses a unique challenge that goes beyond conventional methods. Manually inspecting each website for login screens and compiling a list is a **labor-intensive** and **time-consuming** task. However, this process can be streamlined using simple scripts, particularly leveraging the "**python**" language due to its extensive libraries. With just a few lines of code, we can efficiently identify login pages by sending requests to websites and analyzing the content of the returned responses using the requests and BeautifulSoup libraries in Python.

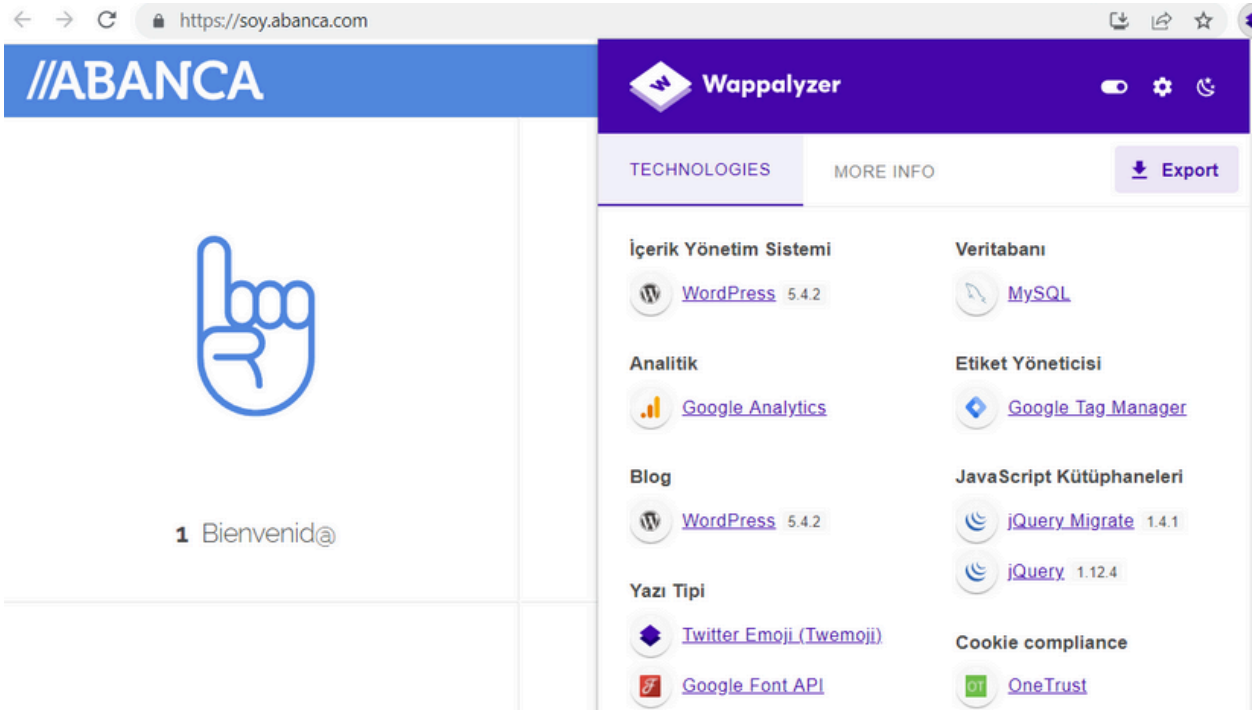
To initiate this process, it is essential to examine the underlying code of the login page and identify specific indicators that provide clues about the presence of a login page. The following sample questions serve as a guide to determine whether a page is a login page:

1. Is the word "Login" or its equivalent phrase in any language present on the page?
2. Do form tags exist on the page?
3. Are expressions such as "Username" or "Password" found in the placeholder section of the input fields on the page?
4. Are there occurrences of "Login" or similar expressions in the title or header of the page?

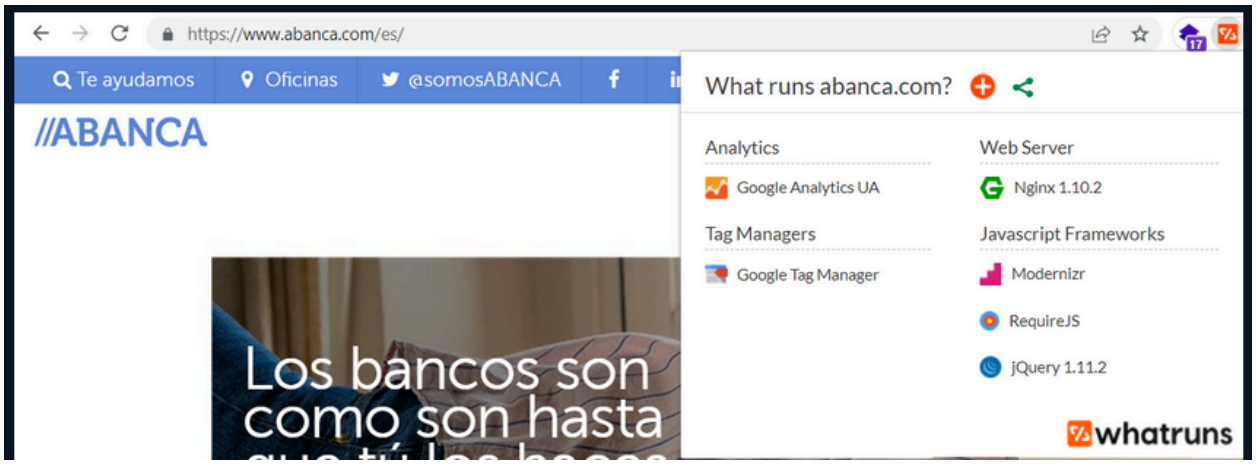
By systematically addressing these questions and leveraging the insights obtained from the indicators, we can effectively automate the detection of login pages, saving considerable time and resources. This approach ensures a more efficient and accurate identification process compared to manual inspection, contributing to a streamlined and effective threat intelligence workflow.

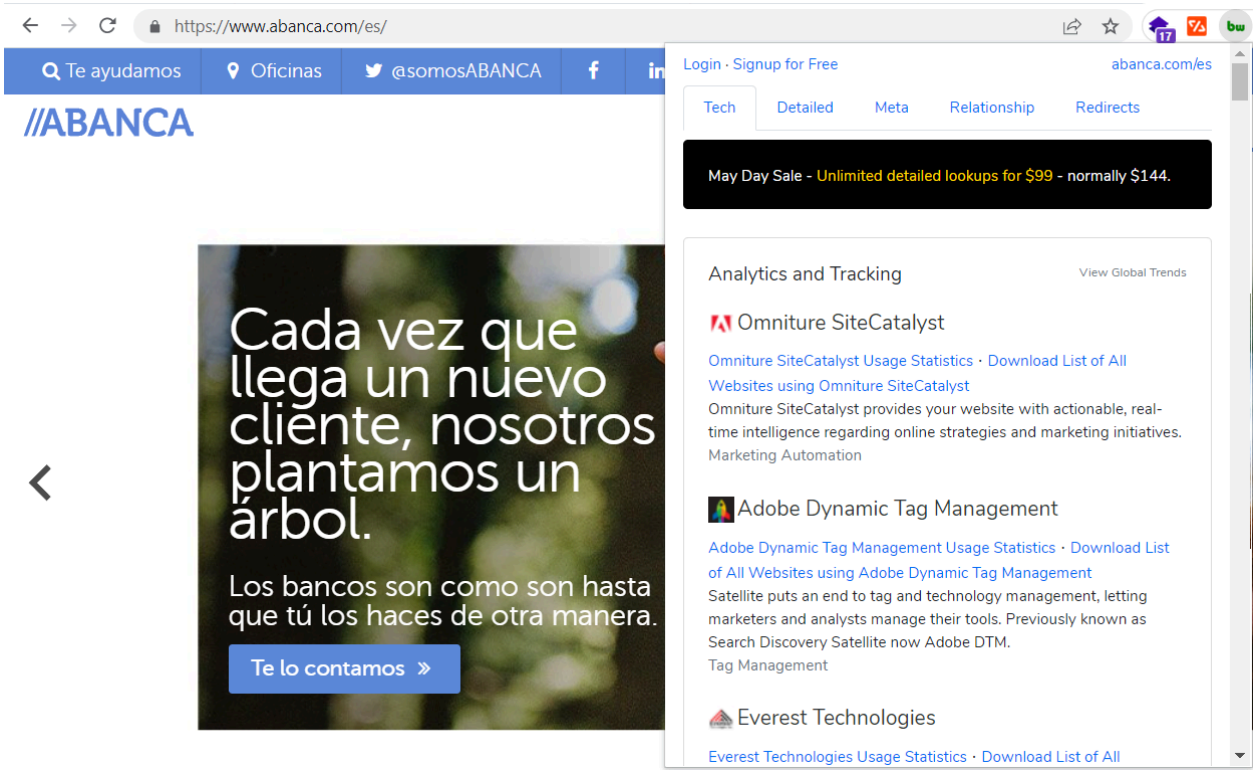
4. Technologies Used on Websites:

The technologies used on the websites we detect will make an important contribution to us, especially in terms of vulnerability intelligence. For example, after we determine the CMS and the version used on a website, we can take quick action on the remediation if there is any matching vulnerability found in the product and the version used on the website in the CVEs we pull from our intelligence sources. There are multiple tools and manual methods to detect the technologies used on the websites. We will use **https://soy.abanca.com/**, one of the websites we have identified for testing purposes. First of all, we install the "**Wappalyzer**" tool (https://chrome.google.com/webstore/detail/wappalyzer-technology-pro/gppongmhjkpfnbhagpmjfkannfbllamg) in our browser in the Chrome Web Store. After opening soy.abanca.com on our browser, we click on the "Wappalyzer" tool icon in the upper right corner, the application gives us as much as it detects in terms of the technologies used on the page.

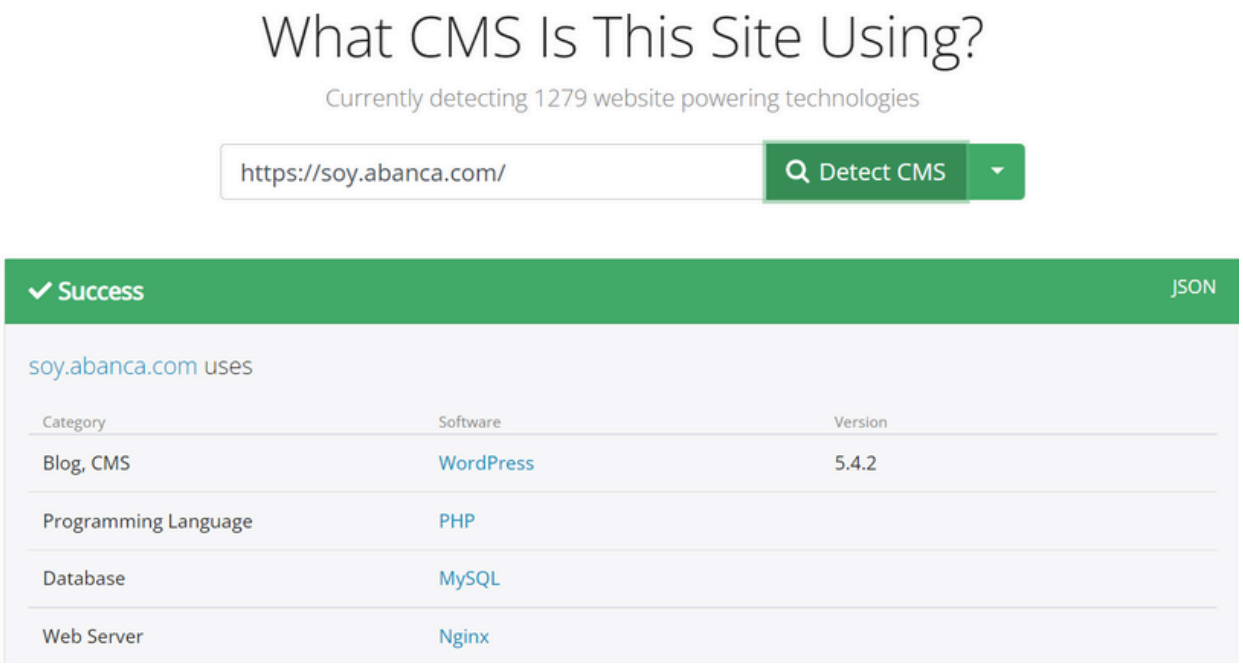


As you can see in the screenshot above, the content management system has listed all the information about the database and the libraries used as much as it can detect. “Whatruns”, “BuiltWith” and “**Whatcms**” applications can be used as an alternative to the **Wappalyzer** tool.





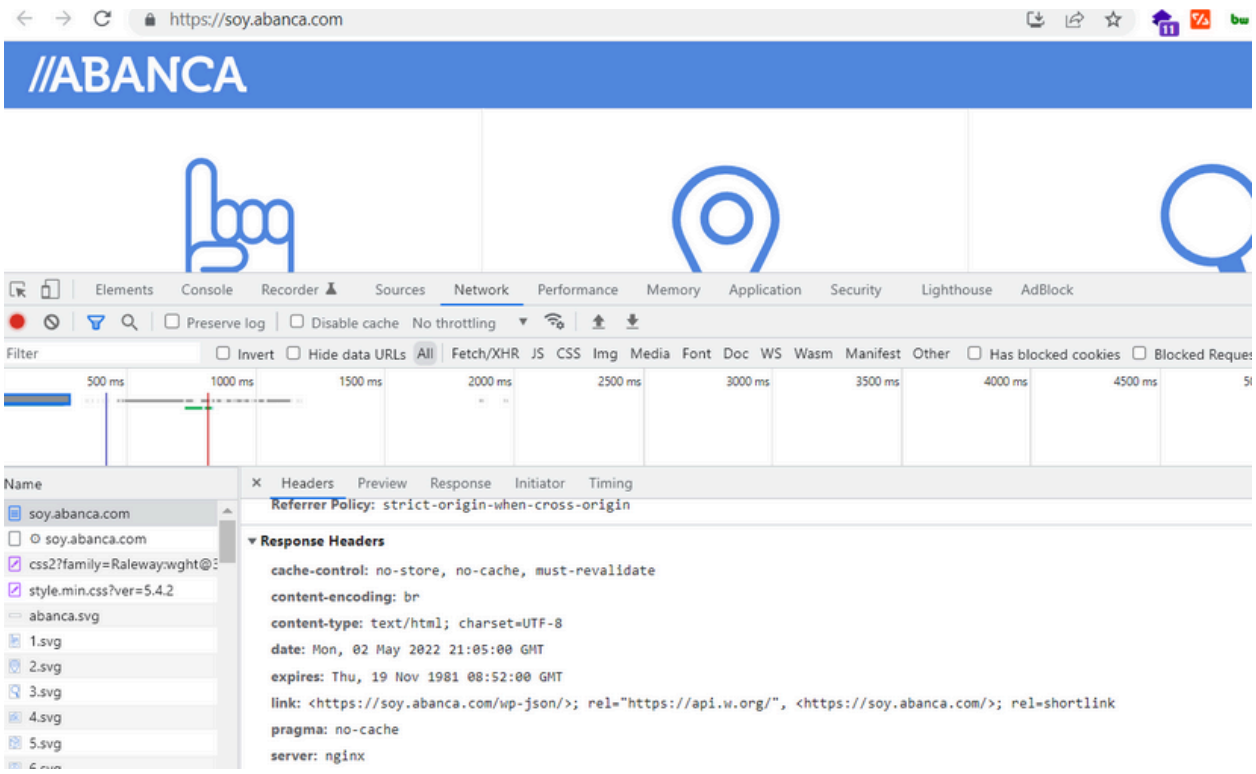
- The above screenshots show that “**Whatruns**” and “**BuiltWith**” tools are installed as browser add-ons and work just like “Wappalyzer” tool.



Unlike other tools, "**Whatcms**" is an online tool and it is available at **whatcms.org.** All you need to do is to enter the URL address you want to scan, and it will display the detections.

If you want to detect it **manually** rather than using a tool, you can examine the source code of the page and make a technology detection by viewing the **file paths** of the theme belonging to the content management system and the libraries given in the code, especially in the script tags

Another tool-independent method would be to examine the header of the response returned from the page from the **developer console**. We can display information about the technologies used on the page within the header of the returned responses.



5. IP Addresses and Blocks:

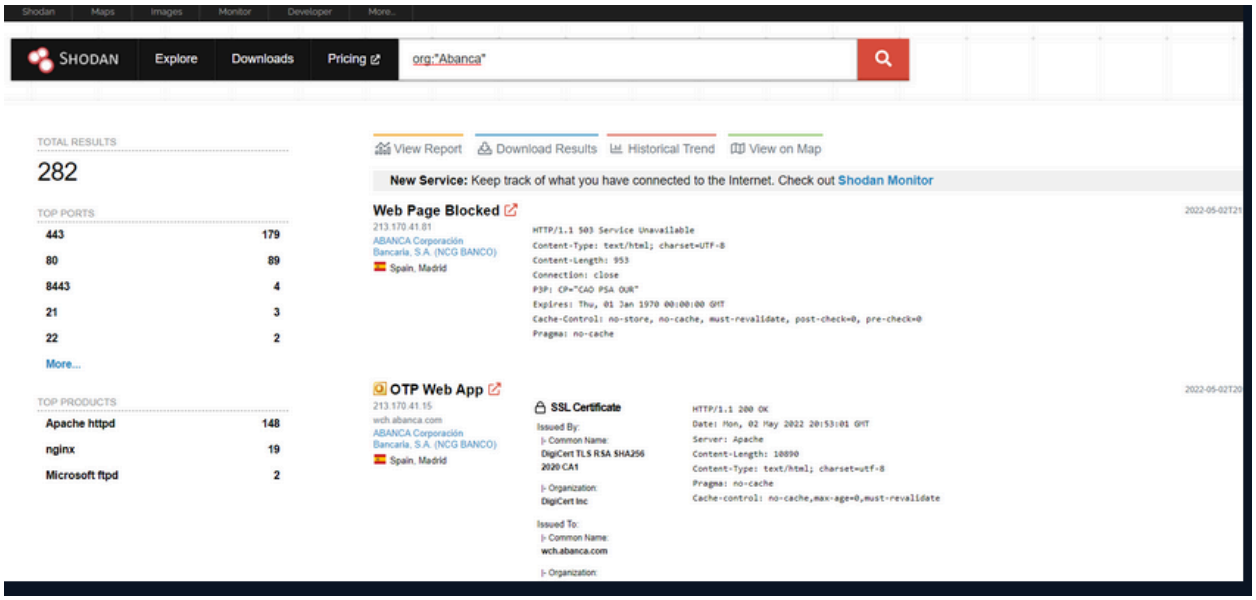
- Analyze IP addresses associated with domains and subdomains.
- Identify IP blocks through patterns and whois information, utilizing **Shodan** or similar tools for organization-specific IP searches.
- Use online tools to associate IP blocks and detect potential risks.

Since IP blocks contain mostly the IPs owned by the organization, the IPs with the **highest risk** are within these blocks. Therefore, follow-up of these is very important.

We can detect IP blocks by looking for patterns in the IP addresses we obtained from the domains and checking the whois information of consecutive IP addresses to understand whether they belong to the organization or not.

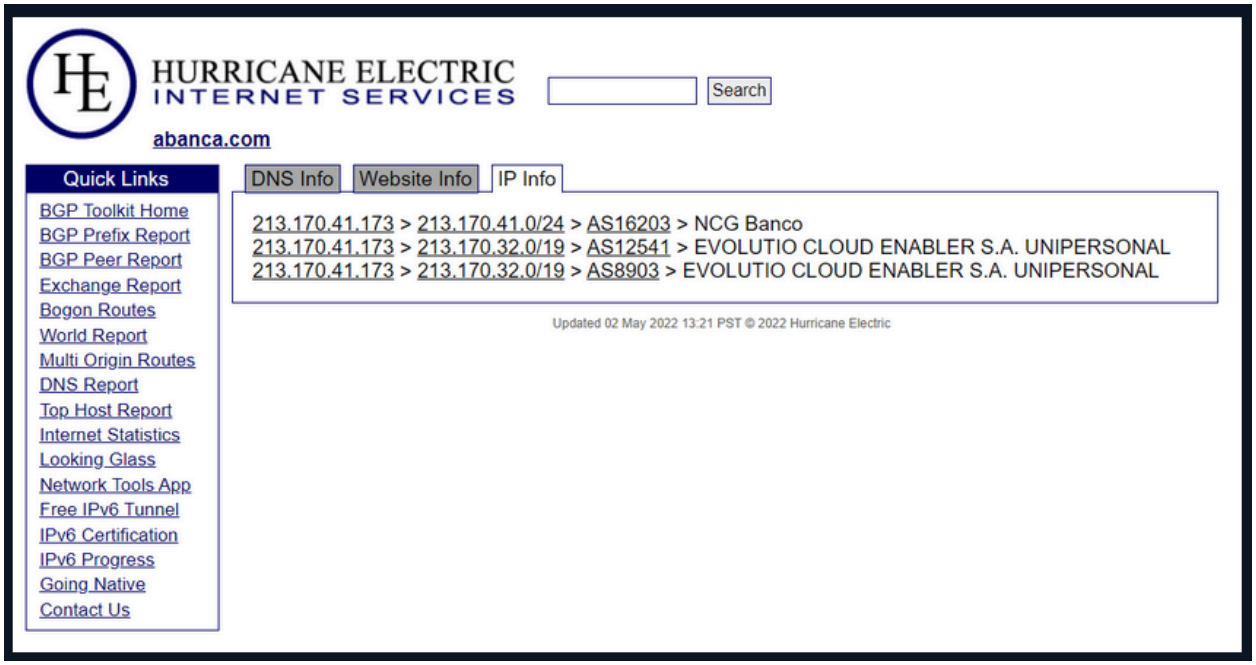
As a secondary method, we can search for the keywords of our organization by using the org parameter on Shodan. The org parameter is a search parameter used for the organization part of the IP addresses.

For instance when we search for org:“**Abanca**” it will list the IP addresses with the word Abanca in the organization section. By examining these IP addresses, we can look at their whois information and find out whether they belong to the organization and which block they belong to.



In addition to **Shodan**, alternatives such as **Binaryedge** and **Zoomeye** can be used.

Lastly, you can also detect blocks by using online tools that make IP block associations over bgp.he.net and similar domain or IP addresses.



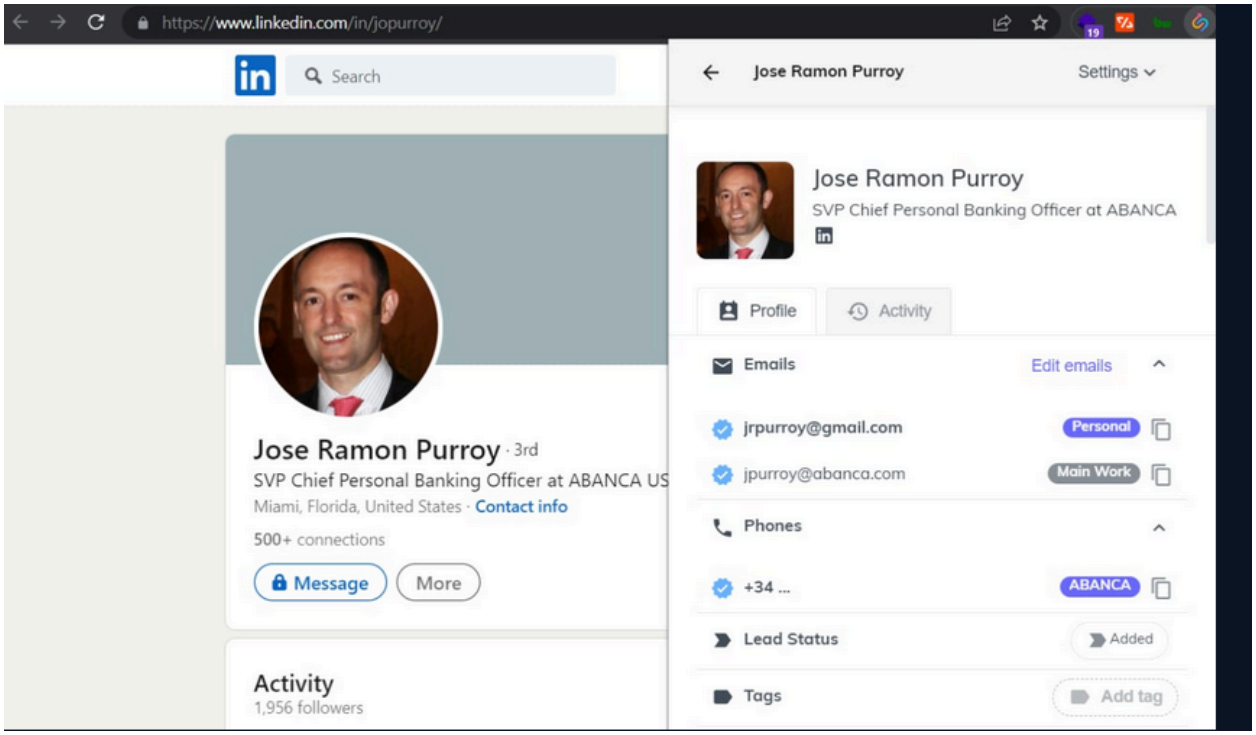
6. DNS Records:

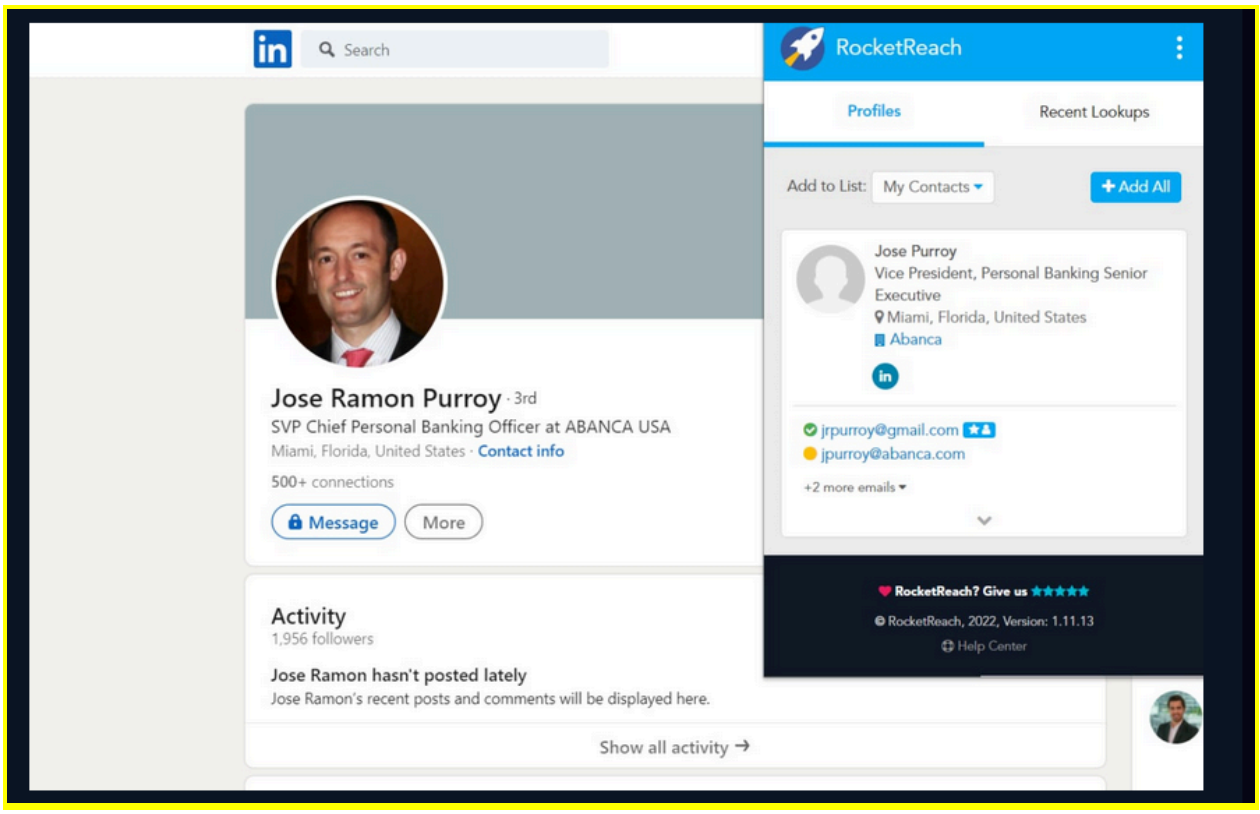
- Monitor DNS records for detecting changes, using tools like Google's dig tool or **dnslytics.com.**
- Access DNS records via the dig command for command-line users.

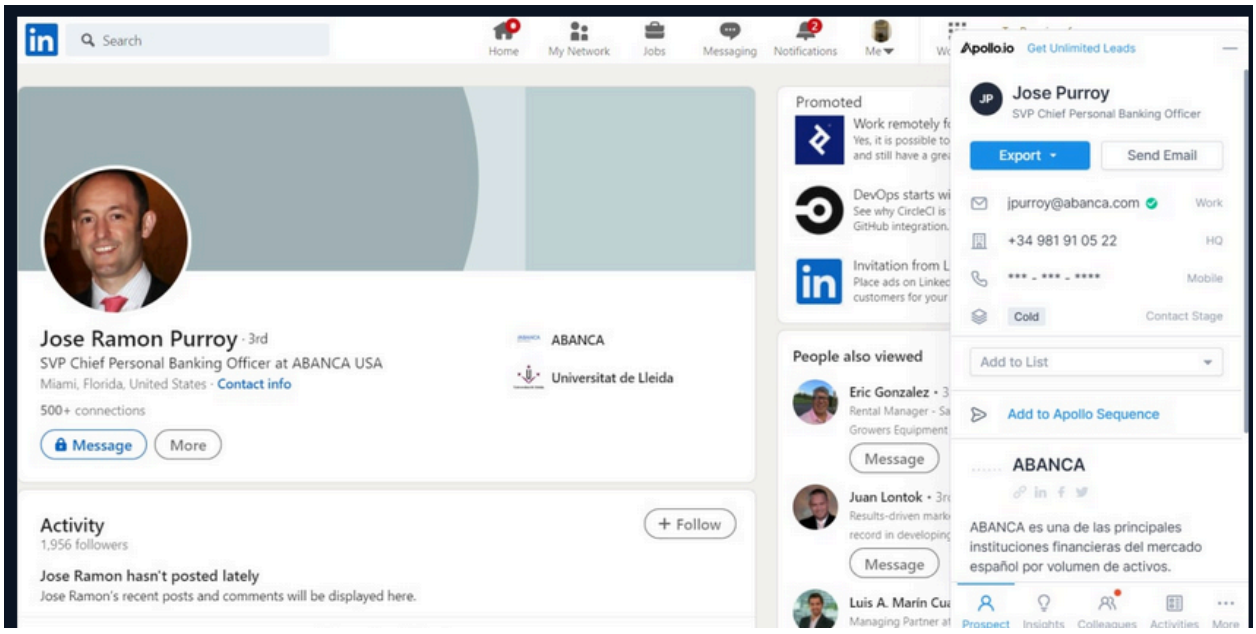
7. C-Level Employee Emails:

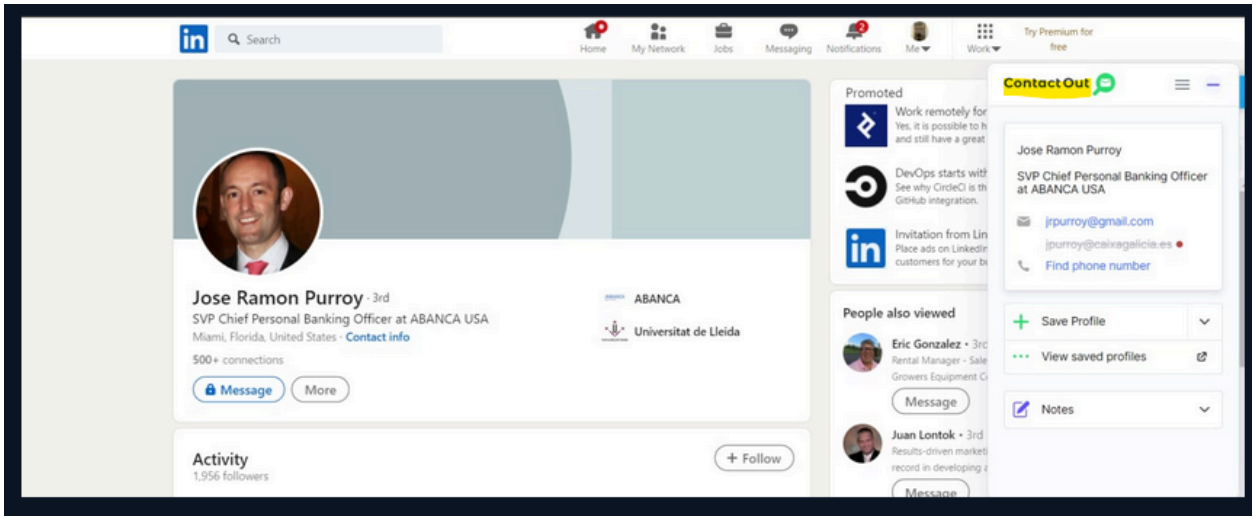
- Use tools like **SalesQL, RocketReach, Apollo**, and **ContactOut**, via a fake Linkedin account, to detect C-level employee emails.

For senior executives, email compromises may result in disaster. The data that's transmitted within the mail traffic on a daily basis is crucial for the organization. Therefore, it is very important to monitor corporate email traffic as well as personal emails.




Search
RocketReach
Profiles
Recent Lookups
Add to List: My Contacts
+ Add All
Jose Purroy
Vice President, Personal Banking Senior Executive
Miami, Florida, United States
Abanca
jrpurroy@gmail.com
jpurroy@abanca.com
+2 more emails
Jose Ramon Purroy · 3rd
SVP Chief Personal Banking Officer at ABANCA USA
Miami, Florida, United States · Contact info
500+ connections
Message
More
RocketReach? Give us
© RocketReach, 2022, Version: 1.11.13
Help Center
Activity
1,956 followers
Jose Ramon hasn't posted lately
Jose Ramon's recent posts and comments will be displayed here.
Show all activity →


Search
Home
My Network
Jobs
Messaging
Notifications
Me
Apollo.io
Get Unlimited Leads
Jose Purroy
SVP Chief Personal Banking Officer
Export
Send Email
jpurroy@abanca.com
Work
+34 981 91 05 22
HQ
Mobile
Cold
Contact Stage
Add to List
Add to Apollo Sequence
ABANCA
ABANCA es una de las principales instituciones financieras del mercado español por volumen de activos.
Jose Ramon Purroy · 3rd
SVP Chief Personal Banking Officer at ABANCA USA
Miami, Florida, United States · Contact info
500+ connections
Message
More
ABANCA
Universitat de Lleida
Activity
1,956 followers
+ Follow
Jose Ramon hasn't posted lately
Jose Ramon's recent posts and comments will be displayed here.
Promoted
People also viewed
Eric Gonzalez
Message
Juan Lontok
Message
Luis A. Marín
Prospect
Insights
Colleagues
Activities
More



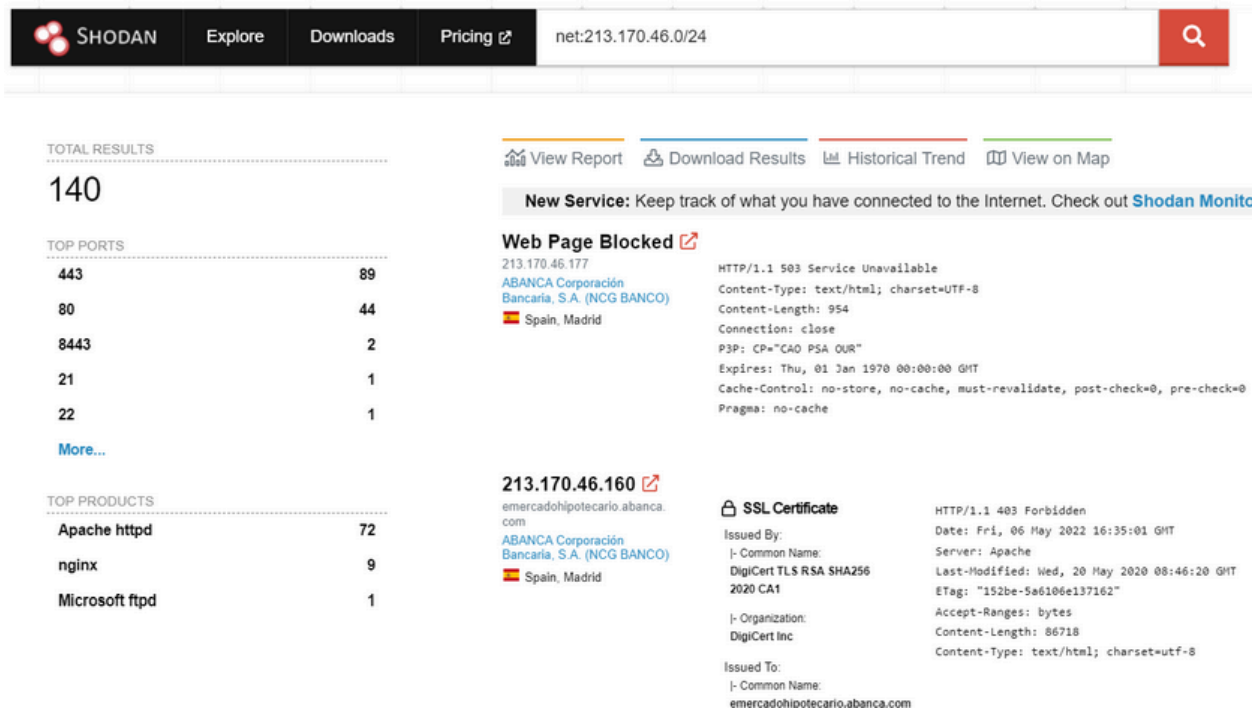
There are several tools that are frequently used to detect these e-mails. **We recommend using a fake Linkedin account and a fake email address when using the tools.** These tools work as chrome extensions. You can download the extensions from the Chrome Web Store or download them from their website and import them into chrome. These applications include **“SalesQL”, “RocketReach”, “Apollo”, and “ContactOut”.** All extensions work in the same logic.

- Basically, we just go to the person's Linkedin profile and click on the extension. **Extensions will list us the e-mail addresses they can detect.**

8. Network Applications and Operating Systems:

- Employ **passive** or **active scanning** via **Shodan** to collect information on network applications and operating systems.
- Utilize responses to open port requests for detection.

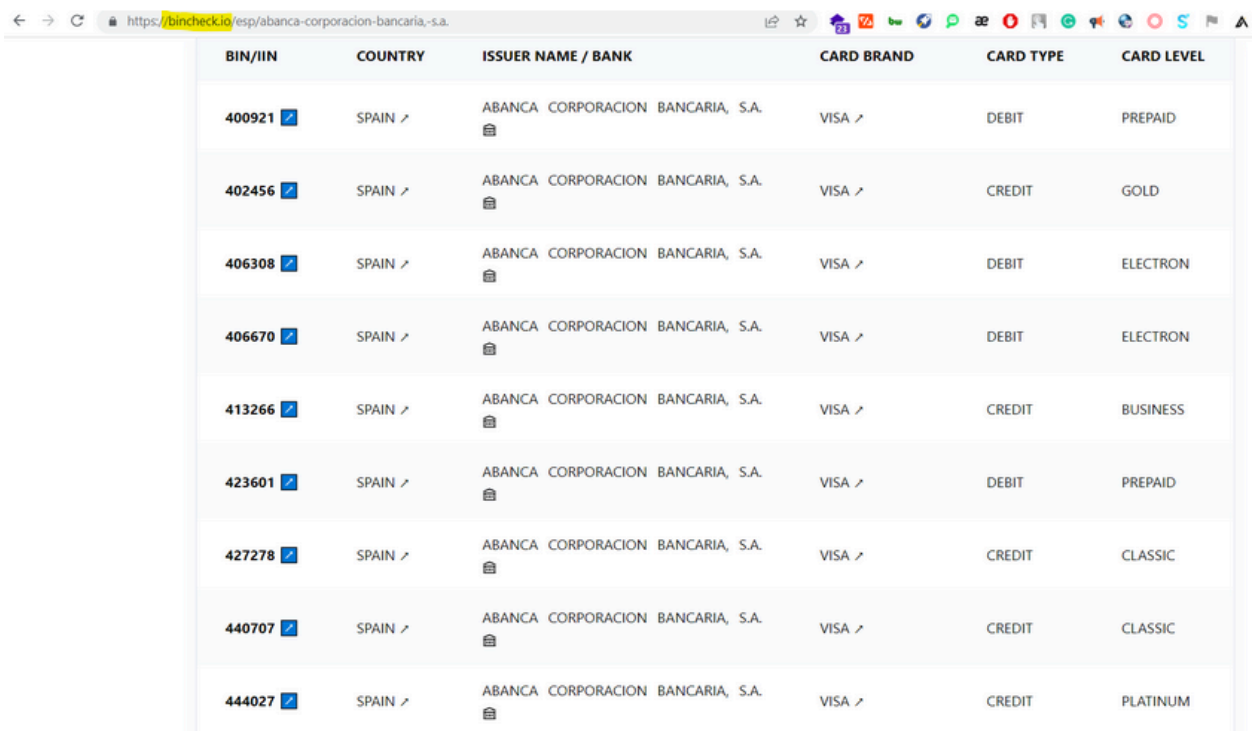
One of the most important steps for us to be able to track vulnerabilities actively or passively is to find all the applications and operating systems. All the methods mentioned in item 5 are also valid in this section. In addition, in this section, we can collect discovered services by querying our IP addresses via **shodan** with passive scanning or we can detect them via active scanning. Network applications and operating system detections can be made according to the responses to the requests we sent to the open ports of our previously removed IP addresses in our asset list



9. Bin Numbers and Swift Codes:

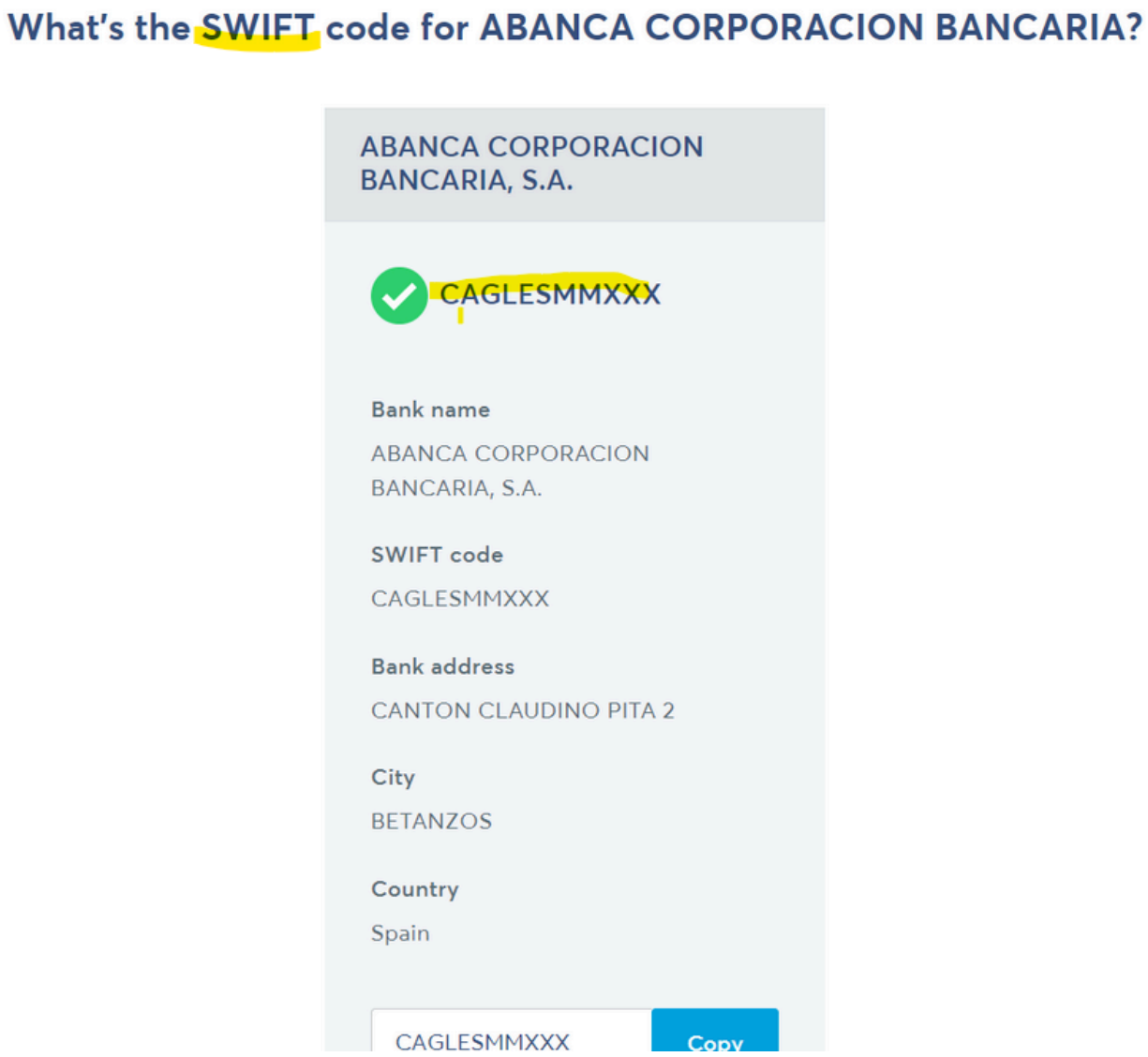
- Utilize public databases like bincheck.io, freebinchecker.com, and bintable.com for bin numbers.
- Explore sites like wise.com, bank.codes, and theswiftcodes.com for Swift codes.

Bin numbers and **swift codes** are one of the **most important assets** to be monitored for matters such as the detection of stolen credit cards on the intelligence side, which are of particular interest to fraud teams in banks. We will use public databases designed for the detection of bin numbers and Swift codes. There is more than one database to find the bin numbers of an organization. Some of those are sites like “**bincheck.io**”, “**freebinchecker.com**”, “**bintable.com**”.



BIN/IIN	COUNTRY	ISSUER NAME / BANK	CARD BRAND	CARD TYPE	CARD LEVEL
400921	SPAIN	ABANCA CORPORACION BANCARIA, S.A.	VISA	DEBIT	PREPAID
402456	SPAIN	ABANCA CORPORACION BANCARIA, S.A.	VISA	CREDIT	GOLD
406308	SPAIN	ABANCA CORPORACION BANCARIA, S.A.	VISA	DEBIT	ELECTRON
406670	SPAIN	ABANCA CORPORACION BANCARIA, S.A.	VISA	DEBIT	ELECTRON
413266	SPAIN	ABANCA CORPORACION BANCARIA, S.A.	VISA	CREDIT	BUSINESS
423601	SPAIN	ABANCA CORPORACION BANCARIA, S.A.	VISA	DEBIT	PREPAID
427278	SPAIN	ABANCA CORPORACION BANCARIA, S.A.	VISA	CREDIT	CLASSIC
440707	SPAIN	ABANCA CORPORACION BANCARIA, S.A.	VISA	CREDIT	CLASSIC
444027	SPAIN	ABANCA CORPORACION BANCARIA, S.A.	VISA	CREDIT	PLATINUM

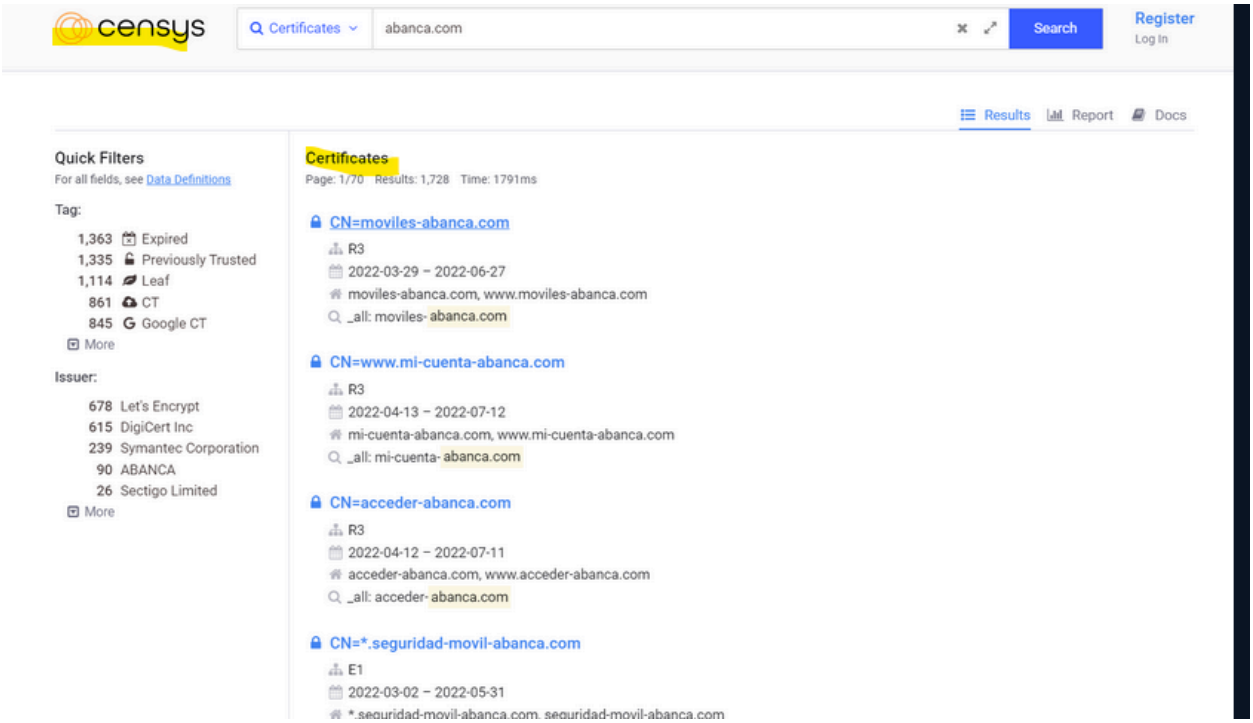
For example, we can list the bin numbers of Abanca on the bincheck.io site by filtering the country and the bank names, as seen above. Other databases work in a similar way. There are sites such as **“wise.com”, “bank.codes”, “theswiftcodes.com”** to detect Swift codes. We can also obtain swift codes by ma



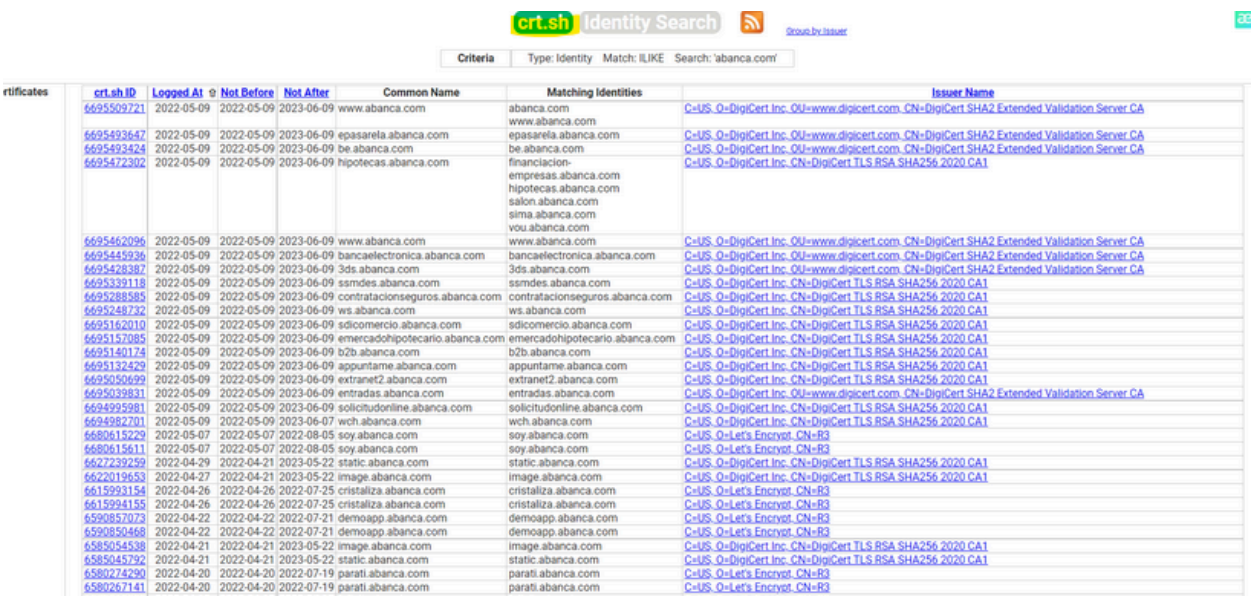
10. SSL Certificates:

- Use tools like Censys and crt.sh to efficiently collect SSL certificates associated with identified domains.

SSL certificates are one of the most important factors for **secure communication**. Therefore, we need to determine carefully if there is an SSL certificate on the domains we have detected and **add it to our asset list.** It is possible to collect SSL certificates manually on the site, but we prefer to use some tools to make it easier since this is a **time-consuming process.** The most common tools are "**Censys**" and "**crt.sh**".



For example, the above screenshot shows that we are able to list all the certificates that contain the **abanca.com domain on Censys.** We can also search for the abanca.com domain on crt.sh, and it lists all the certificates with abanca.com in it.



crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
6695509721	2022-05-09	2022-05-09	2023-06-09	www.abanca.com	abanca.com www.abanca.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 Extended Validation Server CA
6695493647	2022-05-09	2022-05-09	2023-06-09	epasarela.abanca.com	epasarela.abanca.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 Extended Validation Server CA
6695493424	2022-05-09	2022-05-09	2023-06-09	be.abanca.com	be.abanca.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 Extended Validation Server CA
6695472302	2022-05-09	2022-05-09	2023-06-09	hipotecas.abanca.com	financiacion-empresas.abanca.com hipotecas.abanca.com salon.abanca.com sima.abanca.com vou.abanca.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
6695462096	2022-05-09	2022-05-09	2023-06-09	www.abanca.com	www.abanca.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 Extended Validation Server CA
6695445936	2022-05-09	2022-05-09	2023-06-09	bancaelectronica.abanca.com	bancaelectronica.abanca.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 Extended Validation Server CA
6695428387	2022-05-09	2022-05-09	2023-06-09	3ds.abanca.com	3ds.abanca.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 Extended Validation Server CA
6695339118	2022-05-09	2022-05-09	2023-06-09	ssmdes.abanca.com	ssmdes.abanca.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
6695288585	2022-05-09	2022-05-09	2023-06-09	contratacionseguros.abanca.com	contratacionseguros.abanca.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
6695248732	2022-05-09	2022-05-09	2023-06-09	ws.abanca.com	ws.abanca.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
6695162010	2022-05-09	2022-05-09	2023-06-09	sdicomercio.abanca.com	sdicomercio.abanca.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
6695157085	2022-05-09	2022-05-09	2023-06-09	emercadohipotecario.abanca.com	emercadohipotecario.abanca.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
6695140174	2022-05-09	2022-05-09	2023-06-09	b2b.abanca.com	b2b.abanca.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
6695132429	2022-05-09	2022-05-09	2023-06-09	appuntame.abanca.com	appuntame.abanca.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
6695050699	2022-05-09	2022-05-09	2023-06-09	extranet2.abanca.com	extranet2.abanca.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
6695039831	2022-05-09	2022-05-09	2023-06-09	entradas.abanca.com	entradas.abanca.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 Extended Validation Server CA
6694995981	2022-05-09	2022-05-09	2023-06-09	solicitudonline.abanca.com	solicitudonline.abanca.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
6694982701	2022-05-09	2022-05-09	2023-06-07	wch.abanca.com	wch.abanca.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
6680615229	2022-05-07	2022-05-07	2022-08-05	soy.abanca.com	soy.abanca.com	C=US, O=Let's Encrypt, CN=R3
6680615611	2022-05-07	2022-05-07	2022-08-05	soy.abanca.com	soy.abanca.com	C=US, O=Let's Encrypt, CN=R3
6627239259	2022-04-29	2022-04-21	2023-05-22	static.abanca.com	static.abanca.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
6622019653	2022-04-27	2022-04-21	2023-05-22	image.abanca.com	image.abanca.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
6615993154	2022-04-26	2022-04-26	2022-07-25	cristaliza.abanca.com	cristaliza.abanca.com	C=US, O=Let's Encrypt, CN=R3
6615994155	2022-04-26	2022-04-26	2022-07-25	cristaliza.abanca.com	cristaliza.abanca.com	C=US, O=Let's Encrypt, CN=R3
6590857073	2022-04-22	2022-04-22	2022-07-21	demoapp.abanca.com	demoapp.abanca.com	C=US, O=Let's Encrypt, CN=R3
6590850468	2022-04-22	2022-04-22	2022-07-21	demoapp.abanca.com	demoapp.abanca.com	C=US, O=Let's Encrypt, CN=R3
6585054538	2022-04-21	2022-04-21	2023-05-22	image.abanca.com	image.abanca.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
6585045792	2022-04-21	2022-04-21	2023-05-22	static.abanca.com	static.abanca.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
6580274290	2022-04-20	2022-04-20	2022-07-19	parati.abanca.com	parati.abanca.com	C=US, O=Let's Encrypt, CN=R3
6580267141	2022-04-20	2022-04-20	2022-07-19	parati.abanca.com	parati.abanca.com	C=US, O=Let's Encrypt, CN=R3

We can collect the SSL certificates **quickly** and easily using these tools.

Conclusion:

Enhancing **threat intelligence** requires a **meticulous** analysis of the attack surface. By comprehensively assessing domains, subdomains, websites, technologies, IP addresses, and more, organizations can establish a **robust** defense strategy against potential threats. Regular monitoring and updates to the attack surface analysis contribute to a proactive and adaptive cybersecurity approach.