



# Determining the Attack Surface

By: Ryan Stewart

## Introduction:

Traditional threat intelligence models are **facing limitations** 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.

#### Co-Hosted

There are 19 domains hosted on 213.170.41.173 (AS16203 NCG Banco). [Show All →](#)

[View API →](#)

<a href="#">abanca.com</a>	<a href="#">queninguenbaileso.com</a>	<a href="#">abanca.net</a>
<a href="#">bancoetcheverria.eu</a>	<a href="#">hipotecamaricarmen.com</a>	<a href="#">bancoetcheverria.es</a>
<a href="#">bancaelectronica-abanca.com</a>	<a href="#">abanca.me</a>	<a href="#">factoriadeolasabanca.es</a>
<a href="#">imposiblesenti.com</a>	<a href="#">hipotecamaricarmen.es</a>	<a href="#">abanca.mobi</a>
<a href="#">imposiblesenti.es</a>	<a href="#">banca-e.eu</a>	<a href="#">hipotecamaricarmen.net</a>
<a href="#">bancae.com</a>	<a href="#">abanca-usa.info</a>	<a href="#">abanca-usa.org</a>
<a href="#">imposiblesenti.gal</a>		

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 →](#)

<a href="#">banesco.com</a>	<a href="#">banesco.com.pa</a>	<a href="#">bizum.es</a>
<a href="#">fbmpa.es</a>	<a href="#">cuentasclaras.es</a>	<a href="#">mundiario.com</a>
<a href="#">rcelta.es</a>	<a href="#">rcdeportivo.es</a>	<a href="#">scdmilagrosa.com</a>
<a href="#">aerosantiago.es</a>	<a href="#">museoconserva.com</a>	<a href="#">clubfluviallugo.com</a>
<a href="#">anunciantes.com</a>	<a href="#">ismsforum.es</a>	<a href="#">fexdega.com</a>
<a href="#">hipotecamultiproducto.es</a>	<a href="#">banesco.com.cw</a>	<a href="#">clubvigo.com</a>
<a href="#">travesiaanadocostaserena.es</a>	<a href="#">rompetino.org</a>	<a href="#">spaniardsfc.co.uk</a>
<a href="#">fexdega.es</a>	<a href="#">carrilanasesteiro.com</a>	<a href="#">cristalizaservicios.es</a>

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 →](#)

<a href="#">twitter.com</a>	<a href="#">facebook.com</a>	<a href="#">linkedin.com</a>
<a href="#">instagram.com</a>	<a href="#">cuentasclaras.es</a>	<a href="#">tusitiodecompras.es</a>
<a href="#">escogecasa.es</a>	<a href="#">uie.edu</a>	<a href="#">youtube.com</a>
<a href="#">abancacorporacionbancaria.com</a>	<a href="#">abancaserfin.com</a>	<a href="#">abancausa.com</a>
<a href="#">abanca.pt</a>	<a href="#">unepfi.org</a>	<a href="#">unpri.org</a>

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

## Redirects

There are 36 domains which redirect to [abanca.com](#). [Show All →](#)

[View API →](#)

<a href="#">calculadorahipoteca.es</a>	<a href="#">osteusgastosaraia.com</a>	<a href="#">abanca.mobi</a>
<a href="#">advancepayment.eu</a>	<a href="#">hipotecamaricarmen.es</a>	<a href="#">factoriadeolasabanca.es</a>
<a href="#">imposiblesenti.gal</a>	<a href="#">abancafactoriadeolas.gal</a>	<a href="#">abancausa.org</a>
<a href="#">tusgastosaraya.com</a>	<a href="#">bankoa.es</a>	<a href="#">advancepayment.es</a>
<a href="#">wbanca.es</a>	<a href="#">abancafactoriadeolas.es</a>	<a href="#">bancocaixageral.es</a>
<a href="#">abancausa.us</a>	<a href="#">abanca.me</a>	<a href="#">anticipodepagos.eu</a>
<a href="#">hipotecamaricarmen.net</a>	<a href="#">imposiblesinti.com</a>	<a href="#">bancaeletronica-abanca.com</a>
<a href="#">imposiblesenti.com</a>	<a href="#">abanca-usa.org</a>	<a href="#">bancoetcheverria.es</a>

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.



## Domain Information

Domain:	abanca.com
Registrar:	Acens Technologies, S.L.U.
Registered On:	1998-09-01
Expires On:	2024-08-31
Updated On:	2017-05-23
Status:	ok
Name Servers:	ns-cor.net.mundo-r.com ns.mundo-r.com ns2.abanca.com



## Registrant Contact

Organization:	ABANCA
State:	A Coruna
Country:	ES

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](http://viewdns.info) for this.

[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:

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.
abancabanker.com	2021-03-21	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 ) <a href="#">used by 2 domains</a>	NCG Banco (ES )	<a href="#">AS16203</a>	
NS Record	IP Address	Provider	ASN
ns.mundo-r.com <a href="#">used by 3,639 domains</a>	212.51.33.73 (ES )	R Cable y Telecablos Telecomunicaciones, S.A.U. (ES )	<a href="#">AS12334</a>
ns-cor.net.mundo-r.com <a href="#">used by 3,639 domains</a>	212.51.33.106 (ES )	R Cable y Telecablos Telecomunicaciones, S.A.U. (ES )	<a href="#">AS12334</a>
ns2.abanca.com <a href="#">used by 98 domains</a>	213.170.41.11 (ES )	NCG Banco (ES )	<a href="#">AS16203</a>
MX Record	IP Address	Provider	ASN
cluster8.eu.messagelabs.com (pref: 10) <a href="#">used by 11,744 domains</a>	85.158.142.211 (GB ) 85.158.142.216 (GB ) 195.245.230.195 (GB ) 195.245.230.198 (GB ) 195.245.231.66 (GB ) 195.245.231.71 (GB )	Amazon.com, Inc. (US ) Amazon.com, Inc. (US )	<a href="#">AS16509</a> <a href="#">AS16509</a> <a href="#">AS16509</a> <a href="#">AS16509</a> <a href="#">AS16509</a> <a href="#">AS16509</a>
cluster8a.eu.messagelabs.com (pref: 20)	46.137.95.199 (IE )	Amazon.com, Inc. (US )	<a href="#">AS16509</a>

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

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.**

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

## 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](https://securitytrails.com/list/apex_domain/abanca.com)

Domain	Rank	Hosting Provider	Mail Provider
abanca.com	1,234,565	A Coruna	<ul style="list-style-type: none"> <li>• MessageLabs Limited</li> <li>• Google LLC</li> <li>• Amazon.com, Inc.</li> </ul>
entradas.abanca.com	3,609,706	Galicia - Spain	-
corporacionbancaria.abanca.com	6,543,176	-	-
bancaelectronica.abanca.com	9,398,416	A Coruna	-
rsite.lb.abanca.com		Galicia - Spain	-
sai.lb.abanca.com		A Coruna	-

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.

```
> python3 sublist3r.py -d abanca.com



# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for abanca.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 106
www.abanca.com
3ds.abanca.com
3dsdes.abanca.com
```

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.

```
> assetfinder -subs-only abanca.com
kbmic1.abanca.com
static1.abanca.com
kbmis1.abanca.com
extranet2.abanca.com
ecdnsdmzaps5.abanca.com
bancaelectronica.abanca.com
corporacionbancaria.abanca.com
viaja.abanca.com
epasarela.abanca.com
sima.abanca.com
ra.abanca.com
alavuelta.abanca.com
beisuiza.abanca.com
b2b.abanca.com
netclub.abanca.com
dynamic.abanca.com
static.abanca.com
```

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.

```
> cat domains.txt | httpx -o websites.txt

    _/ /_ / / / / _\ | / /_
   /_ / \ / _/_ / / \ | /
  / / / / / / / / / / | |
 / / / / \ / \ / . / / / / | |
      / /          v1.1.5

      projectdiscovery.io

Use with caution. You are responsible for your actions.
Developers assume no liability and are not responsible for any misuse or damage.
http://calendar.abanca.com
https://developers-accountspt.lb.abanca.com
https://developers-accounts.lb.abanca.com
https://drag.abanca.com
https://admon.lb.abanca.com
https://acalendar.lb.abanca.com
https://comunicacion.lb.abanca.com
https://broker.lb.abanca.com
```

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/https 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.

The screenshot shows a browser window with the URL <https://soy.abanca.com/>. The page content includes the ABANCA logo, a blue hand icon, and the text "1 Bienvenid@". On the right, the Wappalyzer extension interface is overlaid. It has tabs for "TECHNOLOGIES" (selected) and "MORE INFO". An "Export" button is also present. The "TECHNOLOGIES" section lists the following detected components:

Category	Technology	Version	Icon
İçerik Yönetim Sistemi	WordPress	5.4.2	WordPress icon
Veritabanı	MySQL		MySQL icon
Analitik	Google Analytics		Google Analytics icon
Etiket Yöneticisi	Google Tag Manager		Google Tag Manager icon
Blog	WordPress	5.4.2	WordPress icon
JavaScript Kütüphaneleri	jQuery Migrate	1.4.1	jQuery Migrate icon
Yazı Tipi	jQuery	1.12.4	jQuery icon
Twitter Emoji (Twemoji)	Twitter Emoji (Twemoji)		Twitter emoji icon
Cookie compliance	OneTrust		OneTrust icon
Google Font API	Google Font API		Google Font API icon

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. “Whatrungs”, “BuiltWith” and “**Whatcms**” applications can be used as an alternative to the **Wappalyzer** tool.

The screenshot shows a browser window for <https://www.abanca.com/es/>. The main content area displays a banner with the Spanish text "Los bancos son como son hasta que tú los haces de otra manera". To the right, the Whatrungs extension interface is overlaid, showing technical details:

What runs abanca.com?	
Analytics	Web Server
Google Analytics UA	Nginx 1.10.2
Tag Managers	Javascript Frameworks
Google Tag Manager	Modernizr
	RequireJS
	jQuery 1.11.2

At the bottom right of the extension interface is the "whatrungs" logo.

The screenshot shows a browser window for <https://www.abanca.com/es/>. The main content area displays a banner with the Spanish text "Cada vez que llega un nuevo cliente, nosotros plantamos un árbol." Below it, a sub-banner says "Los bancos son como son hasta que tú los haces de otra manera." A blue button at the bottom says "Te lo contamos »". To the right, the BuiltWith extension interface is overlaid, showing sections for Analytics and Tracking, Adobe Dynamic Tag Management, and Everest Technologies.

**Analytics and Tracking**

- Omniture SiteCatalyst
- Omniture SiteCatalyst Usage Statistics · Download List of All Websites using Omniture SiteCatalyst
- Omniture SiteCatalyst provides your website with actionable, real-time intelligence regarding online strategies and marketing initiatives.
- Marketing Automation

**Adobe Dynamic Tag Management**

- Adobe Dynamic Tag Management Usage Statistics · Download List of All Websites using Adobe Dynamic Tag Management
- Satellite puts an end to tag and technology management, letting marketers and analysts manage their tools. Previously known as Search Discovery Satellite now Adobe DTM.
- Tag Management

**Everest Technologies**

- Everest Technologies Usage Statistics · Download List of All

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

# What CMS Is This Site Using?

Currently detecting 1279 website powering technologies

<https://soy.abanca.com/>

 Detect CMS

JSON

✓ Success

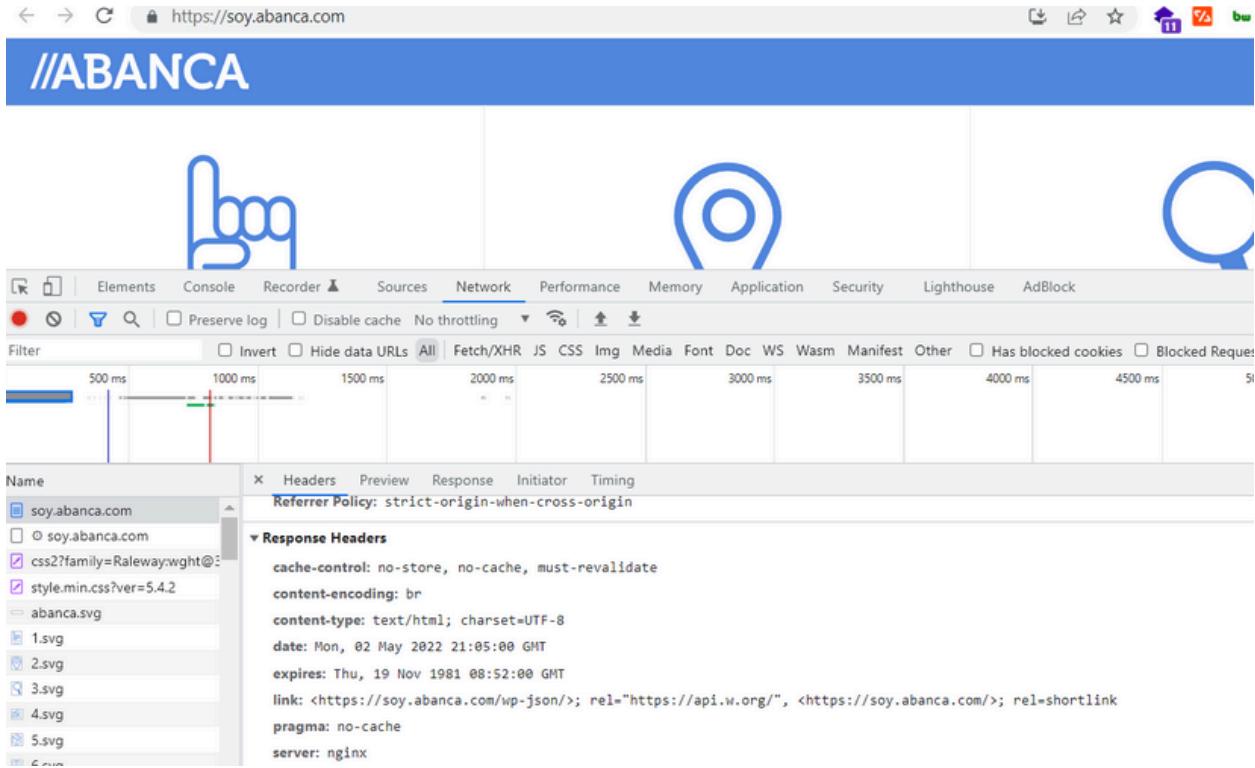
soy.abanca.com uses		
Category	Software	Version
Blog, CMS	WordPress	5.4.2
Programming Language	PHP	
Database	MySQL	
Web Server	Nginx	

Unlike other tools, “**Whatcms**” is an online tool and it is available at [whatcms.org](http://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

```
105 <link rel='stylesheet' id='client_name-css' href='https://soy.abanca.com/wp-content/themes/abanca/assets/css/main.css?ver=5.4.2' type='text/css' media='all' />
106 <script type='text/javascript' /* <![CDATA[ */
107 var superpwa_sw = {"url": "\/superpwa-sw.js"};
108 /* ]]> */
109 </script>
110 <script type='text/javascript' src='https://soy.abanca.com/wp-content/plugins/super-progressive-web-apps/public/js/register-sw.js'></script>
111 <script type='text/javascript' src='https://soy.abanca.com/wp-includes/js/wp-embed.min.js?ver=5.4.2'></script>
112 <script type='text/javascript' src='https://soy.abanca.com/wp-includes/js/jquery/jquery.js?ver=1.12.4-wp'></script>
113 <script type='text/javascript' src='https://soy.abanca.com/wp-includes/js/jquery-migrate.min.js?ver=1.4.1'></script>
114 <script type='text/javascript' src='https://soy.abanca.com/wp-content/themes/abanca/assets/js/lib.js?ver=5.4.2'></script>
115 <script type='text/javascript' src='https://soy.abanca.com/wp-content/themes/abanca/assets/js/site.js?ver=5.4.2'></script>
116 </body>
117 </html>
```

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.

SHODAN | Maps | Images | Monitor | Developer | More... |

SHODAN | Explore | Downloads | Pricing | org:"Abanca" |

TOTAL RESULTS  
282

TOP PORTS

PORT	COUNT
443	179
80	89
8443	4
21	3
22	2

[More...](#)

TOP PRODUCTS

PRODUCT	COUNT
Apache httpd	148
nginx	19
Microsoft ftpd	2

**Web Page Blocked** 2023-05-02T21

213.170.41.01  
ABANCA Corporación  
Bancaria, S.A. (NCG BANCO)  
Spain, Madrid

HTTP/1.1 503 Service Unavailable  
Content-Type: text/html; charset=UTF-8  
Content-Length: 953  
Connection: close  
PSP: CP="CAO PSA OUR"  
Expires: Thu, 01 Jan 1970 00:00:00 GMT  
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0  
Pragma: no-cache

**OTP Web App** 2023-05-02T20

213.170.41.15  
wch.abanca.com  
ABANCA Corporación  
Bancaria, S.A. (NCG BANCO)  
Spain, Madrid

HTTP/1.1 200 OK  
Date: Mon, 02 May 2022 20:53:01 GMT  
Server: Apache  
Content-Length: 10090  
Content-Type: text/html; charset=utf-8  
Pragma: no-cache  
Cache-Control: no-cache,max-age=0,must-revalidate

**SSL Certificate**

Issued By:  
- Common Name: DigiCert TLS RSA SHA256 CA1  
- Organization: DigiCert Inc  
Issued To:  
- Common Name: wch.abanca.com  
- Organization:

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.

**HURRICANE ELECTRIC**  
**INTERNET SERVICES**

[abanca.com](#)

**Quick Links**

- [BGP Toolkit Home](#)
- [BGP Prefix Report](#)
- [BGP Peer Report](#)
- [Exchange Report](#)
- [Bogon Routes](#)
- [World Report](#)
- [Multi Origin Routes](#)
- [DNS Report](#)
- [Top Host Report](#)
- [Internet Statistics](#)
- [Looking Glass](#)
- [Network Tools App](#)
- [Free IPv6 Tunnel](#)
- [IPv6 Certification](#)
- [IPv6 Progress](#)
- [Going Native](#)
- [Contact Us](#)

**DNS Info** **Website Info** **IP Info**

213.170.41.173 > 213.170.41.0/24 > AS16203 > NCG Banco  
 213.170.41.173 > 213.170.32.0/19 > AS12541 > EVOLUTIO CLOUD ENABLER S.A. UNIPERSONAL  
 213.170.41.173 > 213.170.32.0/19 > AS8903 > EVOLUTIO CLOUD ENABLER S.A. UNIPERSONAL

Updated 02 May 2022 13:21 PST © 2022 Hurricane Electric

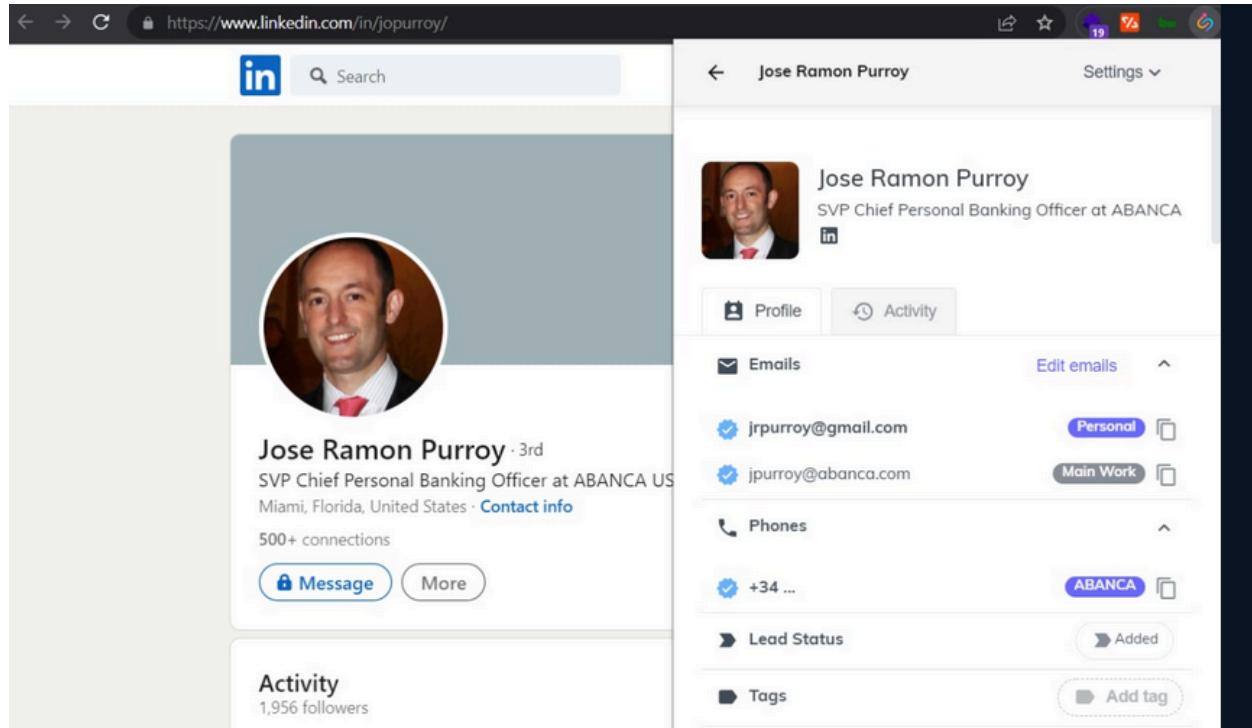
## 6. DNS Records:

- Monitor DNS records for detecting changes, using tools like Google's dig tool or [dnslytics.com](https://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**.

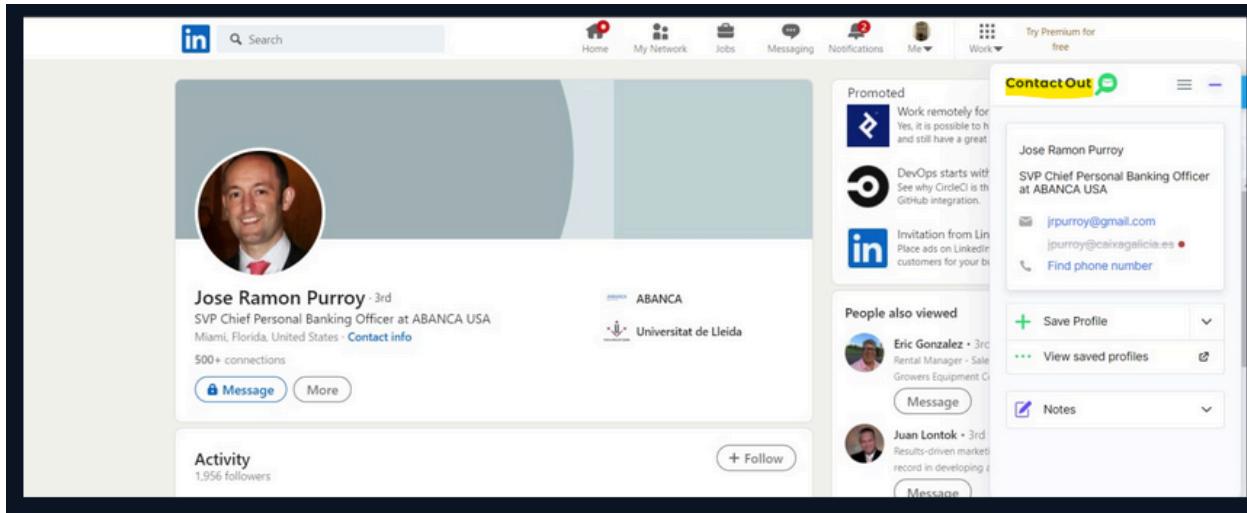
For senior executives, email compromises may result in disaster. The data that's transmitted within the mail traffic on a daily basis is crucial for the organization. Therefore, it is very important to monitor corporate email traffic as well as personal emails.



The screenshot shows a LinkedIn profile page for Jose Ramon Purroy. On the left, there is a sidebar with his profile picture, name, title (SVP Chief Personal Banking Officer at ABANCA US), location (Miami, Florida, United States), and connection count (500+). Below this are buttons for 'Message' and 'More'. On the right, the main profile page displays his name, title, and employer (ABANCA). It also shows sections for 'Emails' (listing two email addresses: jrpurroy@gmail.com and jrpurroy@abanca.com, with the latter marked as 'Main Work'), 'Phones' (listing a phone number starting with +34), 'Lead Status' (marked as 'Added'), and 'Tags' (with an 'Add tag' button). The URL in the browser bar is https://www.linkedin.com/in/jopurroy/.

The screenshot shows a LinkedIn profile for Jose Ramon Purroy. The profile includes his photo, title (SVP Chief Personal Banking Officer at ABANCA USA), location (Miami, Florida, United States), and connection count (500+). Buttons for 'Message' and 'More' are present. To the right, the RocketReach extension is overlaid, displaying additional information: Title (Vice President, Personal Banking Senior Executive), Location (Miami, Florida, United States), Company (ABANCA), and email addresses (jrpurroy@gmail.com, jrpurroy@abanca.com). A 'Add to List' button and a '+ Add All' button are also visible.

The screenshot shows the same LinkedIn profile for Jose Ramon Purroy. The Apollo.io extension is overlaid on the right side. It includes a 'Promoted' section with a link to a blog post about remote work. Below it is a 'People also viewed' section showing profiles for Eric Gonzalez, Juan Lontok, and Luis A. Marin Cu. On the far right, there is a sidebar with contact information for Jose Purroy, including an 'Export' button, an 'Add to Apollo Sequence' button, and a summary of ABANCA's status as a leading financial institution in Spain. The Apollo.io logo and slogan 'Get Unlimited Leads' are also visible.



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

TOTAL RESULTS: 140

TOP PORTS:

Port	Count
443	89
80	44
8443	2
21	1
22	1

More...

TOP PRODUCTS:

Product	Count
Apache httpd	72
nginx	9
Microsoft ftpd	1

213.170.46.160

emercadohipotecario.abanca.com  
ABANCA Corporación Bancaria, S.A. (NCG BANCO)  
Spain, Madrid

Web Page Blocked

213.170.46.177  
ABANCA Corporación Bancaria, S.A. (NCG BANCO)  
Spain, Madrid

HTTP/1.1 503 Service Unavailable  
Content-Type: text/html; charset=UTF-8  
Content-Length: 954  
Connection: close  
P3P: CP="CAO PSA OUR"  
Expires: Thu, 01 Jan 1970 00:00:00 GHT  
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0  
Pragma: no-cache

SSL Certificate

HTTP/1.1 403 Forbidden  
Date: Fri, 06 May 2022 16:35:01 GHT  
Server: Apache  
Last-Modified: Wed, 20 May 2020 08:46:20 GHT  
ETag: "152be-5a6106e137162"  
Accept-Ranges: bytes  
Content-Length: 86718  
Content-Type: text/html; charset=utf-8

Issued To:  
- Common Name: emercadohipotecario.abanca.com

## 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
	<a href="#">400921</a>	SPAIN ↗	ABANCA CORPORACION BANCARIA, S.A. ✉	VISA ↗	DEBIT	PREPAID
	<a href="#">402456</a>	SPAIN ↗	ABANCA CORPORACION BANCARIA, S.A. ✉	VISA ↗	CREDIT	GOLD
	<a href="#">406308</a>	SPAIN ↗	ABANCA CORPORACION BANCARIA, S.A. ✉	VISA ↗	DEBIT	ELECTRON
	<a href="#">406670</a>	SPAIN ↗	ABANCA CORPORACION BANCARIA, S.A. ✉	VISA ↗	DEBIT	ELECTRON
	<a href="#">413266</a>	SPAIN ↗	ABANCA CORPORACION BANCARIA, S.A. ✉	VISA ↗	CREDIT	BUSINESS
	<a href="#">423601</a>	SPAIN ↗	ABANCA CORPORACION BANCARIA, S.A. ✉	VISA ↗	DEBIT	PREPAID
	<a href="#">427278</a>	SPAIN ↗	ABANCA CORPORACION BANCARIA, S.A. ✉	VISA ↗	CREDIT	CLASSIC
	<a href="#">440707</a>	SPAIN ↗	ABANCA CORPORACION BANCARIA, S.A. ✉	VISA ↗	CREDIT	CLASSIC
	<a href="#">444027</a>	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

What's the **SWIFT** code for ABANCA CORPORACION BANCARIA?

ABANCA CORPORACION  
BANCARIA, S.A.

 CAGLESMMXXX

Bank name  
ABANCA CORPORACION  
BANCARIA, S.A.

SWIFT code  
CAGLESMMXXX

Bank address  
CANTON CLAUDINO PITA 2

City  
BETANZOS

Country  
Spain

CAGLESMMXXX Copy

## 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**".

The screenshot shows the Censys search results for the domain `abanca.com`. The search bar at the top has "Certificates" selected and "abanca.com" entered. Below the search bar, there are filters for "Quick Filters" and "Tag". Under "Tag", there are several entries: 1,363 Expired, 1,335 Previously Trusted, 1,114 Leaf, 861 CT, 845 Google CT, and a "More" button. Under "Issuer", there are entries for Let's Encrypt, DigiCert Inc, Symantec Corporation, ABANCA, Sectigo Limited, and another "More" button. The main results section is titled "Certificates" and shows four entries:

- CN=mobiles-abanca.com**: Issued by R3, valid from 2022-03-29 to 2022-06-27, for `mobiles-abanca.com`, `www.mobiles-abanca.com`. Search terms: `_all: mobiles-abanca.com`.
- CN=www.mi-cuenta-abanca.com**: Issued by R3, valid from 2022-04-13 to 2022-07-12, for `mi-cuenta-abanca.com`, `www.mi-cuenta-abanca.com`. Search terms: `_all: mi-cuenta-abanca.com`.
- CN=acceder-abanca.com**: Issued by R3, valid from 2022-04-12 to 2022-07-11, for `acceder-abanca.com`, `www.acceder-abanca.com`. Search terms: `_all: acceder-abanca.com`.
- CN=\*.seguridad-movil-abanca.com**: Issued by E1, valid from 2022-03-02 to 2022-05-31, for `*.seguridad-movil-abanca.com`, `seguridad-movil-abanca.com`. Search terms: `_all: seguridad-movil-abanca.com`.

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.

The screenshot shows the crt.sh Identity Search results for the domain `abanca.com`. The search bar at the top has "Type: Identity Match: ILIKE Search: abanca.com". The results table has columns: crt.sh ID, Logged At, Not Before, Not After, Common Name, Matching Identities, and Issuer Name. The table contains many rows of certificate information, such as:

Common Name	Matching Identities	Issuer Name
<code>abanca.com</code>	<code>C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 Extended Validation Server CA</code>	
<code>epasarela.abanca.com</code>	<code>C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 Extended Validation Server CA</code>	
<code>finanzas.abanca.com</code>	<code>C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 Extended Validation Server CA</code>	
<code>empresas.abanca.com</code>	<code>C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1</code>	
<code>salon.abanca.com</code>	<code>C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1</code>	
<code>sima.abanca.com</code>	<code>C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1</code>	
<code>vou.abanca.com</code>	<code>C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1</code>	
<code>www.abanca.com</code>	<code>C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 Extended Validation Server CA</code>	
<code>bancatecnica.abanca.com</code>	<code>C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 Extended Validation Server CA</code>	
<code>3ds.abanca.com</code>	<code>C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 Extended Validation Server CA</code>	
<code>ssmdes.abanca.com</code>	<code>C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1</code>	
<code>contratacionseguros.abanca.com</code>	<code>C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1</code>	
<code>ws.abanca.com</code>	<code>C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1</code>	
<code>sdicomercio.abanca.com</code>	<code>C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1</code>	
<code>emergadolohopotecario.abanca.com</code>	<code>C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1</code>	
<code>b2b.abanca.com</code>	<code>C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1</code>	
<code>appuntame.abanca.com</code>	<code>C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1</code>	
<code>extranet2.abanca.com</code>	<code>C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1</code>	
<code>entradas.abanca.com</code>	<code>C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 Extended Validation Server CA</code>	
<code>solicitudonline.abanca.com</code>	<code>C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1</code>	
<code>wch.abanca.com</code>	<code>C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1</code>	
<code>soy.abanca.com</code>	<code>C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1</code>	
<code>soyabanca.com</code>	<code>C=US, O=Let's Encrypt, CN=R3</code>	
<code>static.abanca.com</code>	<code>C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1</code>	
<code>image.abanca.com</code>	<code>C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1</code>	
<code>crystaliza.abanca.com</code>	<code>C=US, O=Let's Encrypt, CN=R3</code>	
<code>crystaliza.abanca.com</code>	<code>C=US, O=Let's Encrypt, CN=R3</code>	
<code>demoapp.abanca.com</code>	<code>C=US, O=Let's Encrypt, CN=R3</code>	
<code>demoapp.abanca.com</code>	<code>C=US, O=Let's Encrypt, CN=R3</code>	
<code>image.abanca.com</code>	<code>C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1</code>	
<code>static.abanca.com</code>	<code>C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1</code>	
<code>parati.abanca.com</code>	<code>C=US, O=Let's Encrypt, CN=R3</code>	
<code>parati.abanca.com</code>	<code>C=US, O=Let's Encrypt, CN=R3</code>	

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.