Informe OSINT

CONTENIDO

Versión	Fecha	Autor	Cambios
1.0	14/10/24	María Rodríguez	-
2	15/10/24	María Rodríguez	Eliminar numeración de portada Reducir índice Intercalar capturas de pantalla

1. Finalidad del documento

El presente informe tiene como objeto la recopilación, análisis y presentación de información obtenida de fuentes públicas y abiertas (principalmente, páginas web, redes sociales, bases de datos, etc.) para identificar amenazas potenciales y riesgos de ciberseguridad, y proponer una serie de recomendaciones para eliminar o mitigar dichos riesgos.

2. Información del objetivo

2.1 Introducción

Adarve Abogados es una firma que ofrece asesoramiento jurídico, legal y fiscal a empresas y particulares. Adarve destaca por su experiencia en resolución de conflictos societarios, contratación mercantil y reestructuración empresarial, con un enfoque especializado en derecho procesal, mercantil, inmobiliario, fiscal y laboral.

2.2 Apariciones destacadas en los medios

Entre los primeros resultados de noticias ofrecidos por Google News, destaca en primer lugar el compromiso de Adarve Abogados por la educación y la formación, asistiendo a la Universidad Complutense de Madrid en la creación de un Observatorio de Justicia Civil. También sobresale su relevancia global, colaborando con Yingke Law Firm y permitiendo la entrada de despachos chinos en España; o su participación en foros importantes como el Legal Management Forum.

2.3 Contacto y redes sociales

Página web: https://www.adarve.com/

Madrid (sede central)	Teléfono: +34 91 591 30 60 Correo electrónico: info@adarve.com Dirección: C/ Guzmán el Bueno, 133 – 28003
Barcelona	Dirección: Carrer de Roger de Lluria, 145 – entr. 2º - 08037
Sevilla	Dirección: Callejón de Capachuelos, 73 1ºF - 41710 Utrera, Sevilla
Valencia	Dirección: Avinguda de Carlet, 48 - 46250 L'Alcúdia, València
Santiago de Compostela	Dirección: Calle Enseñanza, 9 Bajos - 15703 Santiago de Compostela
Gran Canaria	Dirección: Calle Domingo J. Navarro, 1-4º Oficina 5 - 35002 Las Palmas, Gran Canaria
Málaga	Dirección: Calle Martínez, 2-4º Oficina 408 - 29005 Málaga

Redes sociales

LinkedIn: https://es.linkedin.com/company/adarve-corporaci-n-jur-dica
Instagram: https://www.instagram.com/adarveabogados/

3. Datos fiscales y económicos

Con páginas web como Infonif y Axesor se han obtenido los siguientes datos sobre la empresa fiscales y económicos:

NIF	B83854653
Antigüedad	21 años (23/12/2003)
Situación mercantil	Activa
Forma jurídica	Sociedad Limitada Profesional
Domicilio	C/ General Rodrigo 6, 4º, 28003 – Madrid
Sector	Consultoría empresarial y otros
Objeto social	Ejercicio en común de las actividades profesionales de abogado.
CNAE	6910 Actividades jurídicas
SIC	8111 Servicios legales
Tamaño de ventas	Microempresa
Últimas cuentas presentadas	31/01/2023

Imagen 1: Resultados de la búsqueda en Infonif de Adarve Abogados

INFORMACIÓN GENERAL DE ADARVE ABOGADOS SLP

Nombre:	**ADARVE ABOGADOS SLP**
Dirección:	C/ GENERAL RODRIGO, 6 4º. 28003, MADRID, MADRID Ver mapa Consultar si la empresa tiene delegaciones
Teléfono:	915913060 Consultar si la empresa tiene otros teléfonos
CIF:	B83854653
Forma jurídica:	SOCIEDAD LIMITADA PROFESIONAL
Constituida hace:	20 años, 9 meses y 13 dias
Objeto social:	LA SOCIEDAD TIENE COMO OBJETO EL EJERCICIO EN COMUN DE LAS ACTIVIDADES PROFESIONALES DE ABOGADO.-
CNAE:	6910 Actividades jurídicas
SIC:	8111 Servicios legales

Imagen 2: Resultados de la búsqueda en Axesor deAdarve Abogados

4. Información técnica

En este apartado se analizarán los aspectos técnicos del dominio y el servidor asociados. Esto proporciona una visión completa del entorno técnico y expone posibles puntos débiles o áreas de interés que pueden afectar la seguridad y el funcionamiento de la infraestructura analizada.

4.1. Direcciones IP

En este apartado se analizará la información relacionada con las direcciones IP asociadas al dominio de la empresa (https://www.adarve.com). Esta información es importante, ya que la dirección IP puede proporcionar datos sobre la localización geográfica del servidor, el proveedor de servicios de alojamiento y otros aspectos técnicos.

4.1.1. Dirección IP asociada al dominio:

La dirección IPv4 (A) púbica que corresponde al dominio es 84.246.209.97. Esta información fue obtenida de herramientas de kali como whois, host, dig, dnsenum y the Harvester; y las páginas web whois y webcheck.
El rango de IP del dominio (obtenido de dnsenum) es de clase C: 84.246.209.0/24.
Con la herramienta Sublist3r se analizaron posibles subdominios, no obteniendo ninguno.

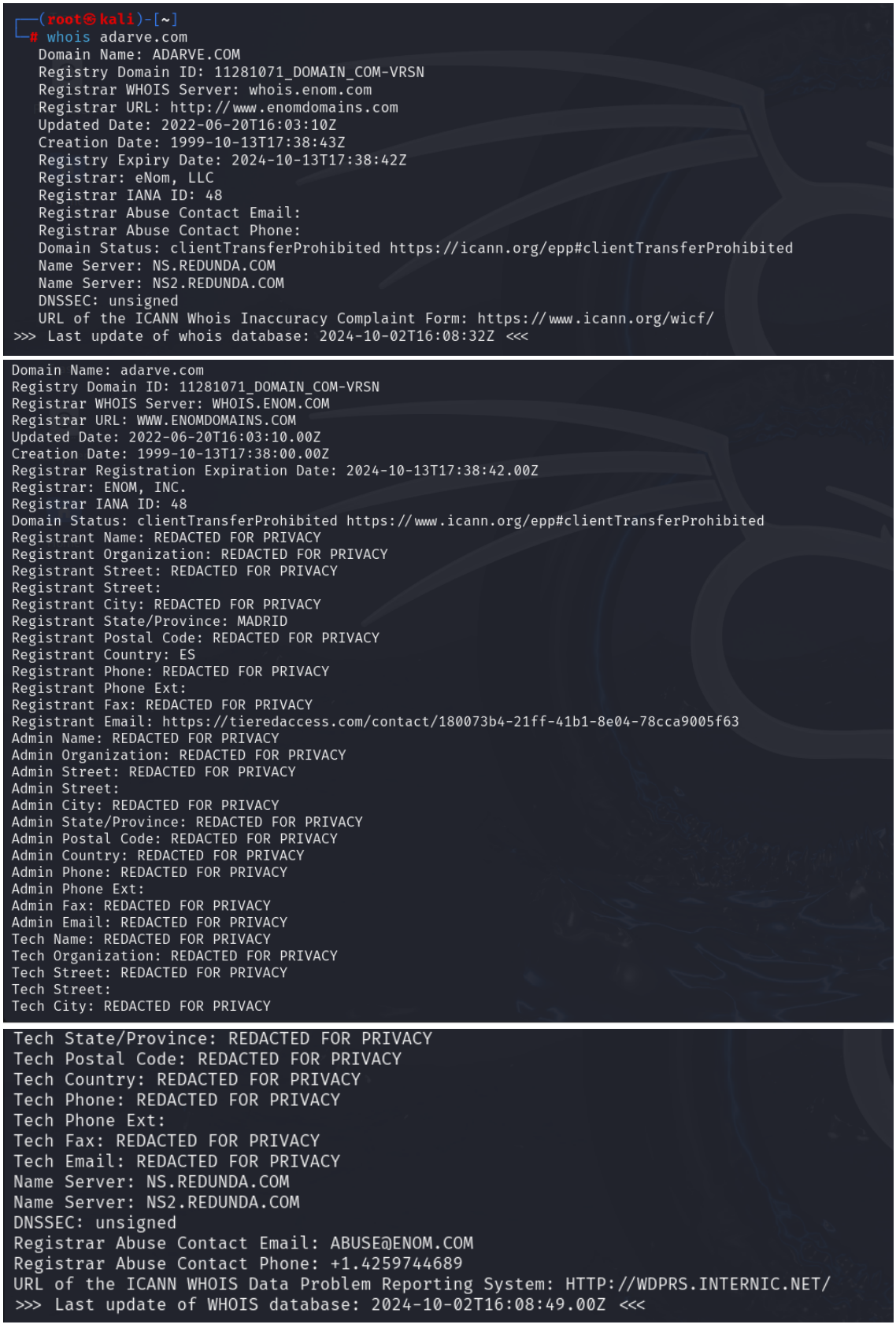

Imagen 3. Captura del resultado obtenido de la herramienta whois de kali.

```
┌──(root㉿kali)-[~]
└─# host adarve.com
adarve.com has address 84.246.209.97
adarve.com mail is handled by 0 adarve-com.mail.protection.outlook.com.
```

Imagen 4. Captura del resultado obtenido de la herramienta host de kali.

```
┌──(root㉿kali)-[~]
└─# dig adarve.com

; <<>> DiG 9.20.2-1-Debian <<>> adarve.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16196
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;adarve.com.                    IN      A

;; ANSWER SECTION:
adarve.com.             14400   IN      A       84.246.209.97

;; Query time: 12 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Wed Oct 02 18:11:06 CEST 2024
;; MSG SIZE  rcvd: 55
```

Imagen 5. Captura del resultado obtenido de la herramienta dig de kali.

```
┌──(root㉿kali)-[~]
└─# dnsenum adarve.com
dnsenum VERSION:1.3.1

-----   adarve.com   -----


Host's addresses:
__________________

adarve.com.                              14400    IN    A        84.246.209.97


Name Servers:
______________

ns2.redunda.com.                         5654     IN    A        84.246.209.5
ns.redunda.com.                          1378     IN    A        84.246.208.5


Mail (MX) Servers:
___________________

adarve-com.mail.protection.outlook.com.  10       IN    A        52.101.73.30
adarve-com.mail.protection.outlook.com.  10       IN    A        52.101.73.21
adarve-com.mail.protection.outlook.com.  10       IN    A        52.101.73.11
adarve-com.mail.protection.outlook.com.  10       IN    A        52.101.68.5


Trying Zone Transfers and getting Bind Versions:
_________________________________________________


Trying Zone Transfer for adarve.com on ns2.redunda.com ...
AXFR record query failed: REFUSED

Trying Zone Transfer for adarve.com on ns.redunda.com ...
AXFR record query failed: REFUSED
```

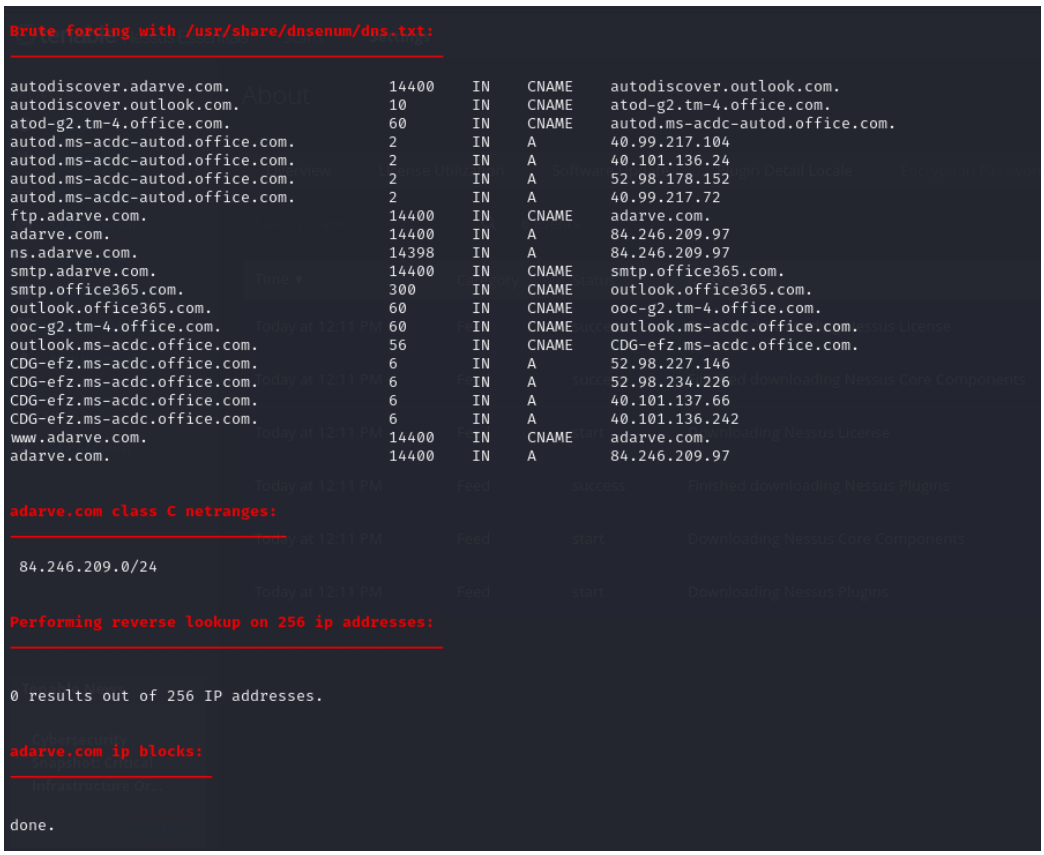

Imagen 6. Resultado obtenido con la herramienta Dnsenum

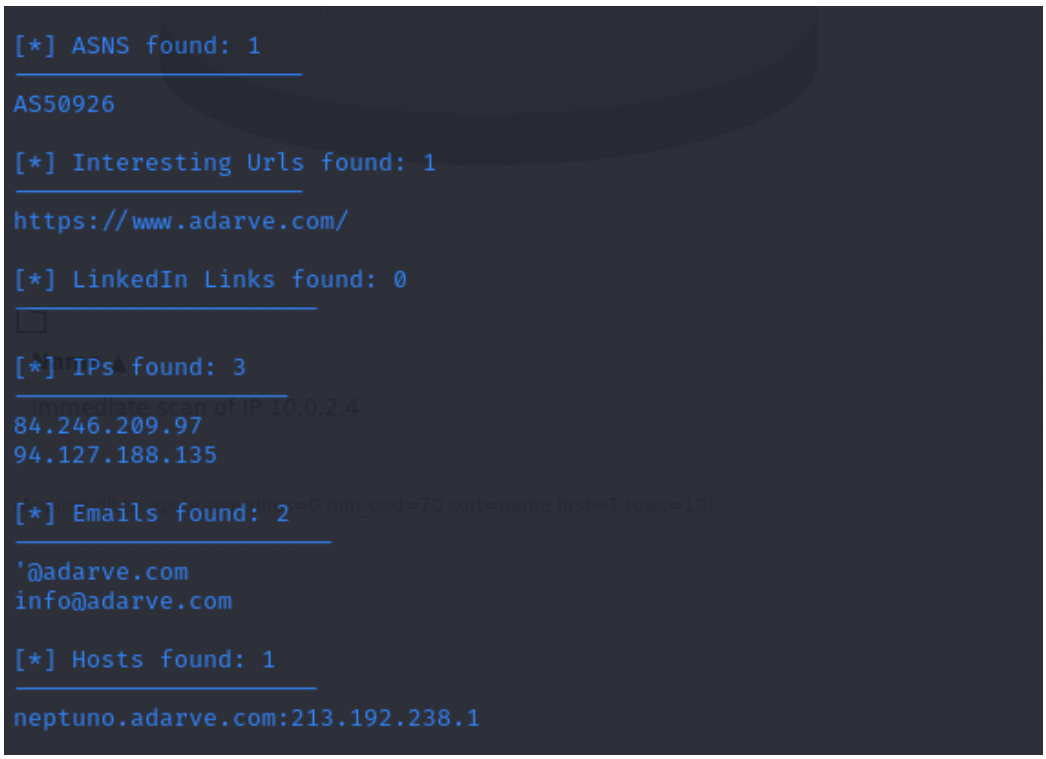

Imagen 7. Resultado obtenido con la herramienta theHarvester

Whois Record for Adarve.com

Domain Profile

Registrar	ENOM, INC. eNom, LLC IANA ID: 48 URL: WWW.ENOMDOMAINS.COM,http://www.enomdomains.com Whois Server: WHOIS.ENOM.COM abuse@enom.com (p) +1.4259744689
Registrar Status	clientTransferProhibited
Dates	9,121 days old Created on 1999-10-13 Expires on 2024-10-13 Updated on 2022-06-20
Name Servers	NS.REDUNDA.COM (has 8,392 domains) NS2.REDUNDA.COM (has 8,392 domains)
IP Address	84.246.209.97 - 96 other sites hosted on this server
IP Location	- Madrid - Madrid - Axarnet Comunicaciones S.l.
ASN	AS50926 AXARNET-AS AXARNET COMUNICACIONES, S.L., ES (registered Apr 22, 2010)
Domain Status	Registered And No Website

Imagen 8. Captura del resultado obtenido en la página https://whois.domaintools.com/

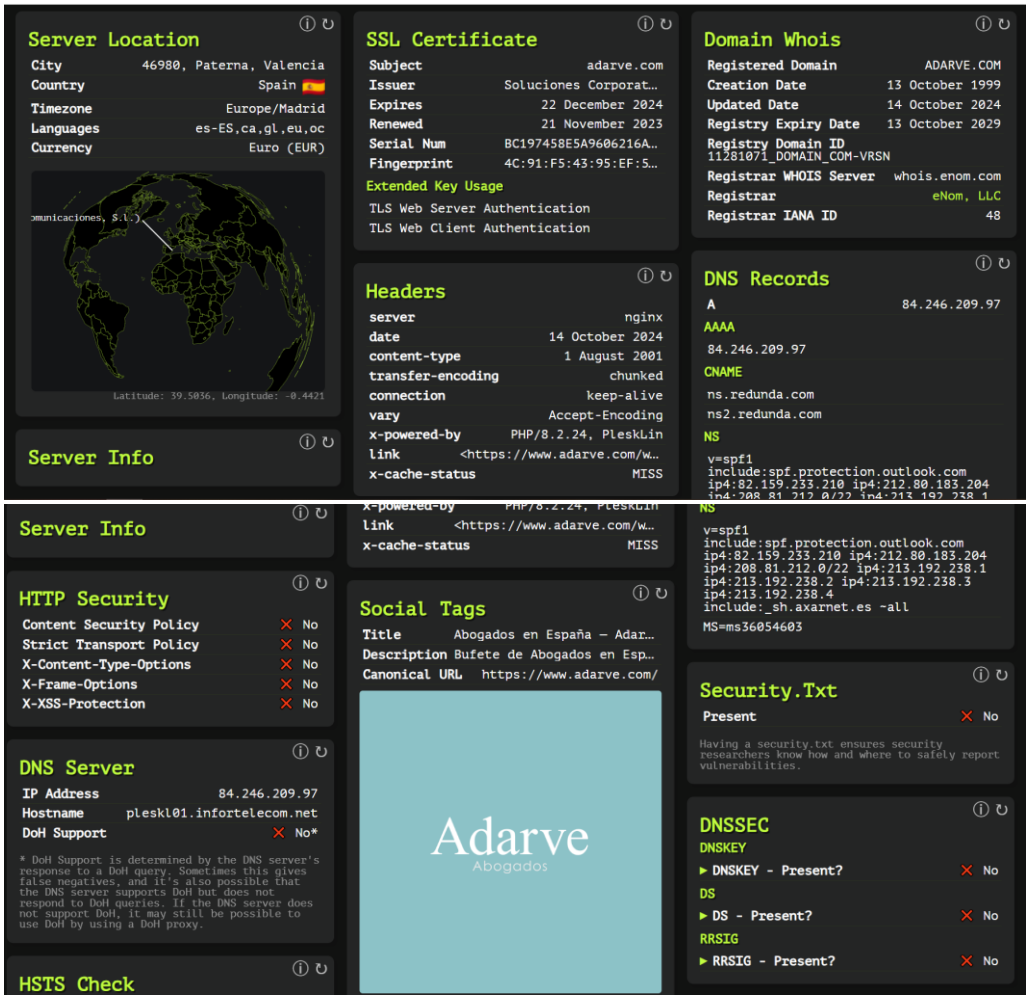

Imagen 9. Resultado obtenido de la página web WebCheck

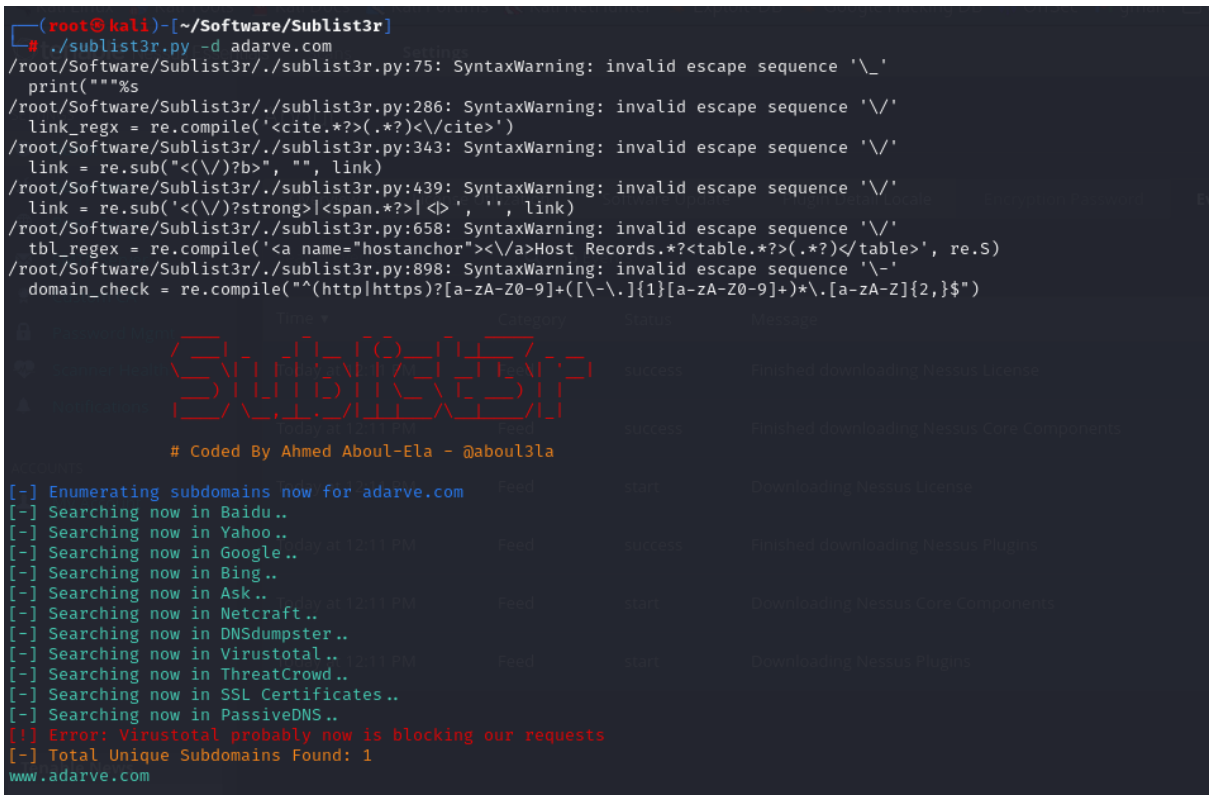

Imagen 10. Resultados obtenidos con la herramienta Sublister.

4.1.2. Información de registro del dominio

No se han obtenido datos del propietario del dominio, aunque sí algunos sobre el registro de este último. Estos han sido recopilados principalmente con la herramienta whois de kali.

URL del registrador	http://www.enomdomains.com
Registrador	eNom, INC.
Situación ID del Registrador (IANA)	48
Fecha de creación del dominio	19 de octubre de 1999
Fecha de caducidad del dominio	13 de octubre de 2024
Última fecha de actualización	20 de junio de 2024
Estado del dominio	clientTransferProhibited (ICANN EPP). Este estado indica que el dominio no puede ser transferido a otro registrador sin autorización explícita.

4.1.3. Proveedor del alojamiento (ASN) y ubicación del servidor

El servidor que aloja el dominio se encuentra físicamente ubicado en Paterna, Valencia (comprobado en webcheck y Shodan) y está gestionado por el proveedor de servicios de alojamiento Axarnet Comunicaciones S.L. El servicio está registrado desde el 22 de abril de 2010. AS50926 AXARNET-AS es el sistema autónomo (ASN) que gestiona el bloque de IP donde está alojado el servidor (ver imágenes 7 y 8).

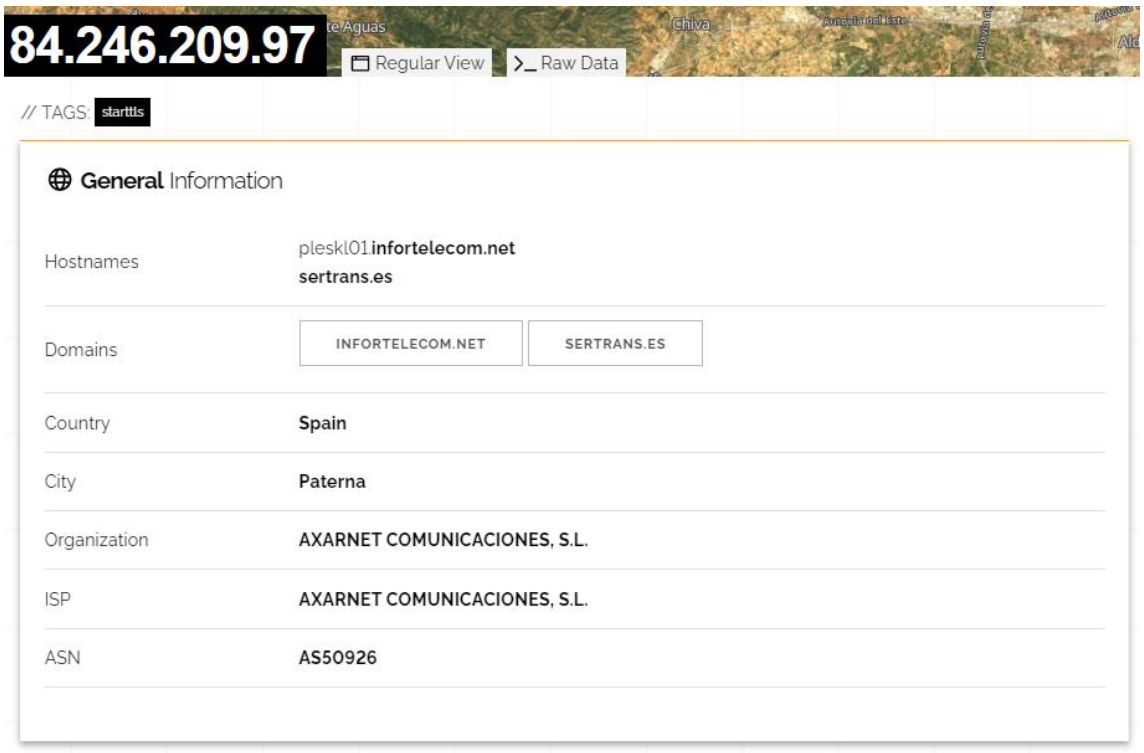

Imagen 11. Información general obtenida de Shodan

4.1.4. Certificado SSL

El dominio adarve.com está protegido por un certificado SSL emitido por una entidad de certificación (Soluciones Corporativas IP, S.L) el 21 de noviembre de 2023, y que vence el 22 de diciembre de 2024. Esto proporciona seguridad en las conexiones al sitio web.

El certificado utiliza un algoritmo de firma SHA-256 con una clave pública RSA de 2048 bits, lo cual es un estándar seguro (ver imagen 12).

Imagen 12. Visor de certificado SSL del dominio www.adarve.com

4.2. Servidor

En este apartado se analizarán los distintos servidores asociados al dominio, incluyendo los servidores de nombres (DNS), de correo (MX), y los registros de nombre canónico (CNAME). También se evaluarán las tecnologías utilizadas por estos servidores, como el software de servidor web o de correo, y se realizará un análisis de los puertos abiertos y servicios activos. A continuación, se muestran un diagrama de relaciones de DNS y de la estructura de infraestructura de red.

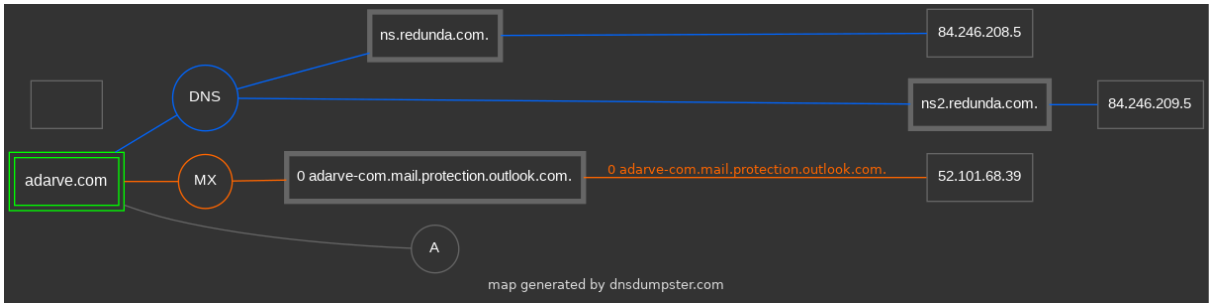

Imagen 13. Diagrama de relaciones de DNS obtenida de dnsdumpster.

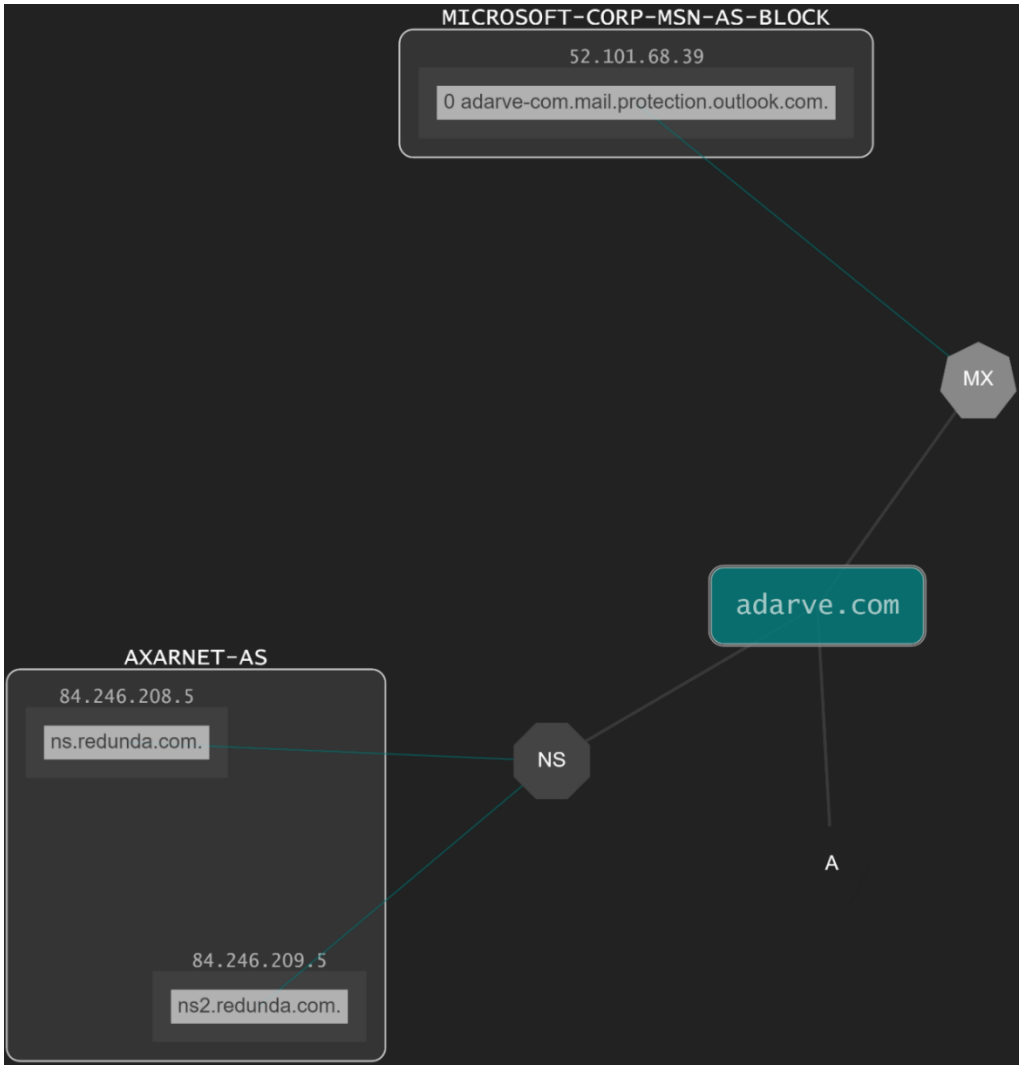

Imagen 14. Estructura de infraestructura de red

4.2.1. Servidores

Servidores de nombre (Name Servers)

Las consultas DNS para el dominio son gestionadas por dos servidores, ns.redunda.com y ns2.redunda.com. La dirección IP del primer servidor es 84.246.208.5. Está ubicado en España y es gestionado por AXARNET-AS. La dirección IP del segundo servidor es 84.246.209.5. Está ubicado también en España, y también es gestionado por la misma empresa.

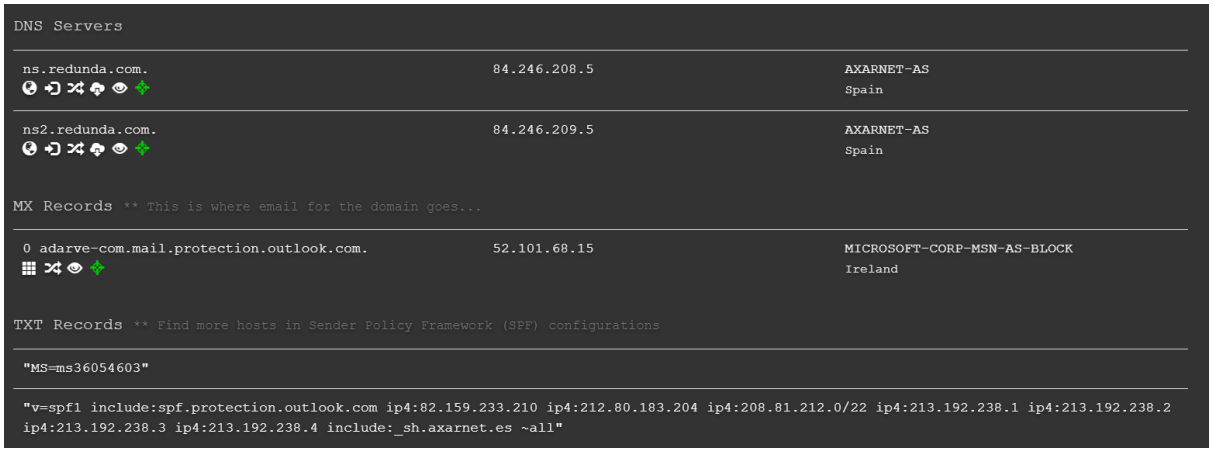

Imagen 15. Captura de los dominios de servidores obtenidos de dnsdumpster.com

Servidores de correo (MX Servers)

El servidor de correo para el dominio es 0 adarve-com.mail.protection.outlook.com, con la dirección IP 52.101.68.15. Se encuentra ubicado en Irlanda, y es gestionado por la empresa Microsoft Corp. MSN-AS-BLOCK. Con herramientas como dnsenum (ver imagen 6) y nslookup se han obtenido otras direcciones IP para los servidores de correo, como 52.101.73.30; 52.101.73.22; 52.101.73.21; 52.101.73.11; 52.101.68.5, 52.101.68.15, 52.101.68.16 y 52.101.68.32.

Con la herramienta theHarvester (ver imagen 7) también se encontró la IP 94.127.188.135. Haciendo una búsqueda inversa con nslookup, descubrimos que esta IP está asociada al host windu.hospedando.com, que parece ser un servicio de hosting.

Registros de nombre canónico (CNAME Records)

Realizando un ataque de fuerza bruta con dnsenum (ver imagen 6) se ha descubierto que varios subdominios de adarve.com están configurados como alias de otros dominios o servicios, muchos de los cuales están relacionados con Microsoft Office 365, lo que sugiere que esta organización utiliza la infraestructura de Microsoft para el correo electrónico y otros servicios.

Por ejemplo, autodiscover.adarve.com redirige a autodiscover.outlook.com, lo que indica que la empresa utiliza servicios de correo alojados en Outlook. Por otro lado, smtp.adarve.com redirige a smtp.office365.com, lo que apunta al uso de Office 365.

4.2.2. Tecnologías utilizadas

Con consultas a páginas web como Builtwith o Shodan se han podido recopilar las siguientes tecnologías utilizadas por el servidor:

Categoría	**Tecnología/descripción**
Tecnologías web y móviles	Lenguaje: PHP Sistema de gestión de contenidos (CMS): WordPress Ulkit Apple Mobile Web Clips Icon
Frameworks y librerías JavaScript	Prototype, RequireJS jQuery, jQuery Migrate 3.3.2 ProgressBar.js, Lightbox, Magnific Popup 5.4.1 Chart.js, amCharts parallax.js 5.4.1
Constructor de páginas	Elementor 3.14.0
Alojamiento y servidores	Infortelecom Hosting y Axarnet: proveedores de hosting con el servidor web ubicado en España Plesk: panel de control de hosting
Bases de datos	MySQL
Seguridad	SSL by Default: redirección automática a versión HTTPS para garantizar una conexión segura MrDomain: proveedor de certificado SSL reCAPTCHA: Sistema anti-bot de Google para proteger formularios
Correo y servicios en la nuble	Office 365
Idiomas y accesibilidad	Español/inglés HREF LANG WPML: Plugin multilingüe para WordPress
Ecommerce	Abicart: Plataforma de comercio electrónico
Generadores de formularios	Contact Form 7 5.7.5.1: Gestión de formularios de contacto en WordPress
SEO y Gestión de Contenidos	Yoast WordPress SEO Plugin: Optimización del contenido para motores de búsqueda Complianz: Suite de privacidad para WordPress (cumplimiento normativo como GDPR)
Seguimiento y análisis	Google Tag Manager: Sistema de gestión de etiquetas para análisis y seguimiento Global Site Tag: Seguimiento de conversiones/mediciones de Google Ads y DoubleClick CrUX Dataset: El sitio está en el top 10 millones y top 50 millones de sitios web según el tráfico
Widgets	Max Mega Menu 5.4.1: Plugin de menús para WordPress
Plugins de WordPress	Contact Form 7 5.7.5.1 WPML Max Mega Menu 5.4.1 Elementor 3.14.0

ADARVE.COM

Technology Profile | Detailed Profile | Meta Profile | Performance | Relationship | Redirect

Analytics and Tracking — View Global Trends

Global Site Tag

Global Site Tag Usage Statistics · Download List of All Websites using Global Site Tag

Google's primary tag for Google Measurement/Conversion Tracking, Adwords and DoubleClick.

Widgets — View Global Trends

Complianz

Complianz Usage Statistics · Download List of All Websites using Complianz

Privacy Suite for WordPress.

Privacy Compliance · WordPress Plugins

Slack

Slack Usage Statistics · Download List of All Websites using Slack

Messaging app for teams that makes working together simple and efficient.

Yoast Plugins

Yoast Plugins Usage Statistics · Download List of All Websites using Yoast Plugins

SEO based plugins from Yoast.

WordPress Plugins

Yoast WordPress SEO Plugin

Yoast WordPress SEO Plugin Usage Statistics · Download List of All Websites using Yoast WordPress SEO Plugin

Functionality that helps you optimize your pages content, images titles, meta descriptions and more.

Contact Form 7

Contact Form 7 Usage Statistics · Download List of All Websites using Contact Form 7

Specifically designed for wordpress blogs. Contact Form 7 can manage multiple contact forms, plus you can customize the form and the mail contents flexibly with simple markup.

Feedback Forms and Surveys

Sitelinks Search Box

Sitelinks Search Box Usage Statistics · Download List of All Websites using Sitelinks Search Box

With Google sitelinks search box, people can reach your content more quickly from search results.

Site Search

CrUX Dataset

CrUX Dataset Usage Statistics · Download List of All Websites using CrUX Dataset

CrUX is a data collection system that gathers information about how real users interact with websites. This website is included in the user experiences data gathered from Google Chrome and thus considered sufficiently popular on the Internet.

CrUX Top 10m

CrUX Top 10m Usage Statistics · Download List of All Websites using CrUX Top 10m

Relative measure of site popularity within the CrUX dataset, measured by the total number of navigations on the origin. This site is in the top 10 million.

CrUX Top 50m

CrUX Top 50m Usage Statistics · Download List of All Websites using CrUX Top 50m

Relative measure of site popularity within the CrUX dataset, measured by the total number of navigations on the origin. This site is in the top 50 million.

reCAPTCHA

reCAPTCHA Usage Statistics · Download List of All Websites using reCAPTCHA

Anti-bot CAPTCHA widget from Google.

CAPTCHA

Language

View Global Trends

Spanish

Spanish Usage Statistics · Download List of All Websites using Spanish

Website content is written in Spanish.

English HREF LANG

English HREF LANG Usage Statistics · Download List of All Websites using English HREF LANG

This webpage has alternate versions available in English via the use of the hreflang tag.

Frameworks

View Global Trends

PHP

PHP Usage Statistics · Download List of All Websites using PHP

PHP is a widely used general-purpose scripting language that is especially suited for Web development and can be embedded into HTML.

Organization Schema

Organization Schema Usage Statistics · Download List of All Websites using Organization Schema

Organization i.e. school, NGO, Corporation.

Schema

Mobile

View Global Trends

Apple Mobile Web Clips Icon

Apple Mobile Web Clips Icon Usage Statistics · Download List of All Websites using Apple Mobile Web Clips Icon

This page contains an icon for iPhone, iPad and iTouch devices.

Viewport Meta

Viewport Meta Usage Statistics · Download List of All Websites using Viewport Meta

This page uses the viewport meta tag which means the content may be optimized for mobile content.

IPhone / Mobile Compatible

IPhone / Mobile Compatible Usage Statistics · Download List of All Websites using IPhone / Mobile Compatible

The website contains code that allows the page to support IPhone / Mobile Content.

Content Management System

View Global Trends

WordPress

WordPress Usage Statistics · Download List of All Websites using WordPress

WordPress is a state-of-the-art semantic personal publishing platform with a focus on aesthetics, web standards, and usability.

Open Source · Blog

JavaScript Libraries and Functions

View Global Trends

UIkit

UIkit Usage Statistics · Download List of All Websites using UIkit

A lightweight and modular front-end framework for developing web interfaces.

Framework

Intersection Observer

Intersection Observer Usage Statistics · Download List of All Websites using Intersection Observer

API that can be used to understand the visibility and position of DOM elements relative to a containing element or to the top-level viewport.

Verified Link

View Global Trends

LinkedIn

LinkedIn Usage Statistics · Download List of All Websites using LinkedIn

The website mentions linkedin.com in some form.

Email Hosting Providers

View Global Trends

SPF

SPF Usage Statistics · Download List of All Websites using SPF

The Sender Policy Framework is an open standard specifying a technical method to prevent sender address forgery.

Office 365 Mail

Office 365 Mail Usage Statistics · Download List of All Websites using Office 365 Mail

Email sent from this domain has records showing Office 365 usage.

Business Email Hosting

Microsoft Exchange Online

Microsoft Exchange Online Usage Statistics · Download List of All Websites using Microsoft Exchange Online

A rich hosted Exchange environment for every user without having to manage a server.

Business Email Hosting

Microsoft Azure DNS

Microsoft Azure DNS Usage Statistics · Download List of All Websites using Microsoft Azure DNS

This domain is verified with Microsoft Azure.

Web Hosting Providers — View Global Trends

Infortelecom Hosting

Infortelecom Hosting Usage Statistics · Download List of All Websites using Infortelecom Hosting

Network infrastructure from Infortelecom Hosting based in Spain.

Spanish hosting

Axarnet

Axarnet Usage Statistics · Download List of All Websites using Axarnet

Axarnet offers web hosting, VPS, and backup services in Spain with 24/7 Spanish support. They also provide domain registration, WordPress hosting, and SSL certificates.

Spanish hosting

Spanish Server Location

Spanish Server Location Usage Statistics · Download List of All Websites using Spanish Server Location

The web server is located in Spain.

Server Location

SSL Certificates — View Global Trends

SSL by Default

SSL by Default Usage Statistics · Download List of All Websites using SSL by Default

The website redirects traffic to an HTTPS/SSL version by default.

MrDomain

MrDomain Usage Statistics · Download List of All Websites using MrDomain

SSL provider Soluciones Corporativas IP.

Web Servers — View Global Trends

nginx

nginx Usage Statistics · Download List of All Websites using nginx

nginx [engine x] is a HTTP server and mail proxy server written by Igor Sysoev.

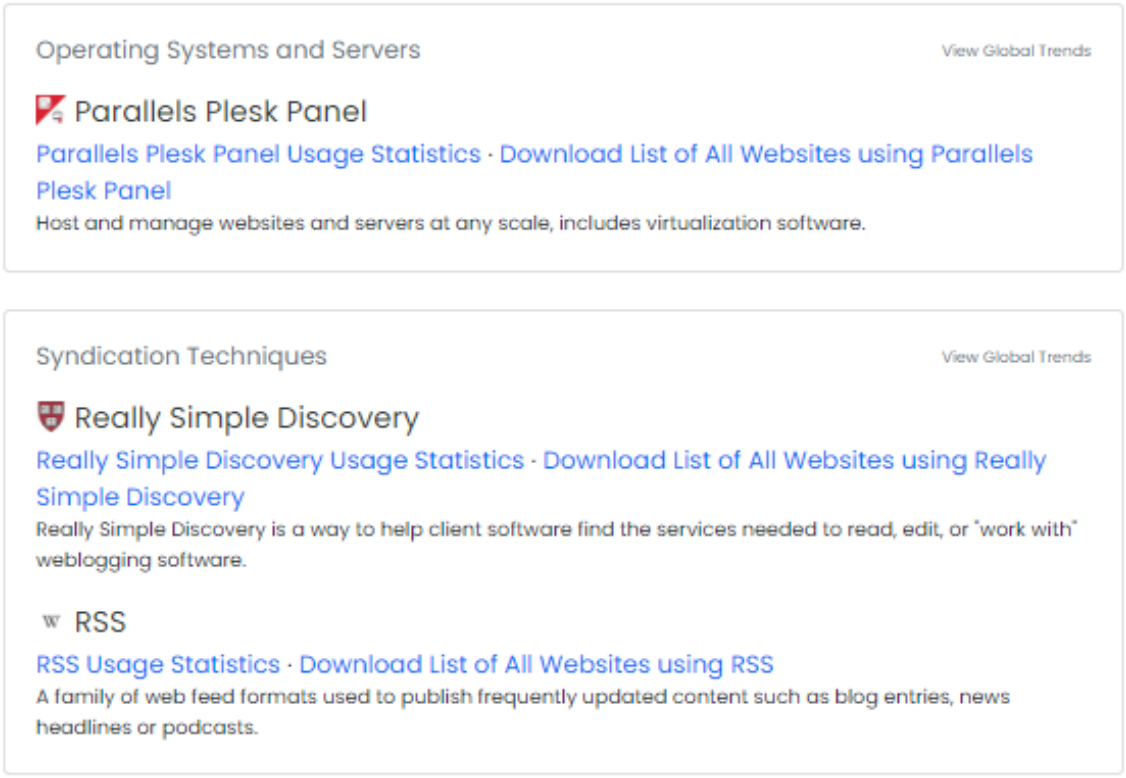

Imagen 16. Resultados de la búsqueda en Builtwith

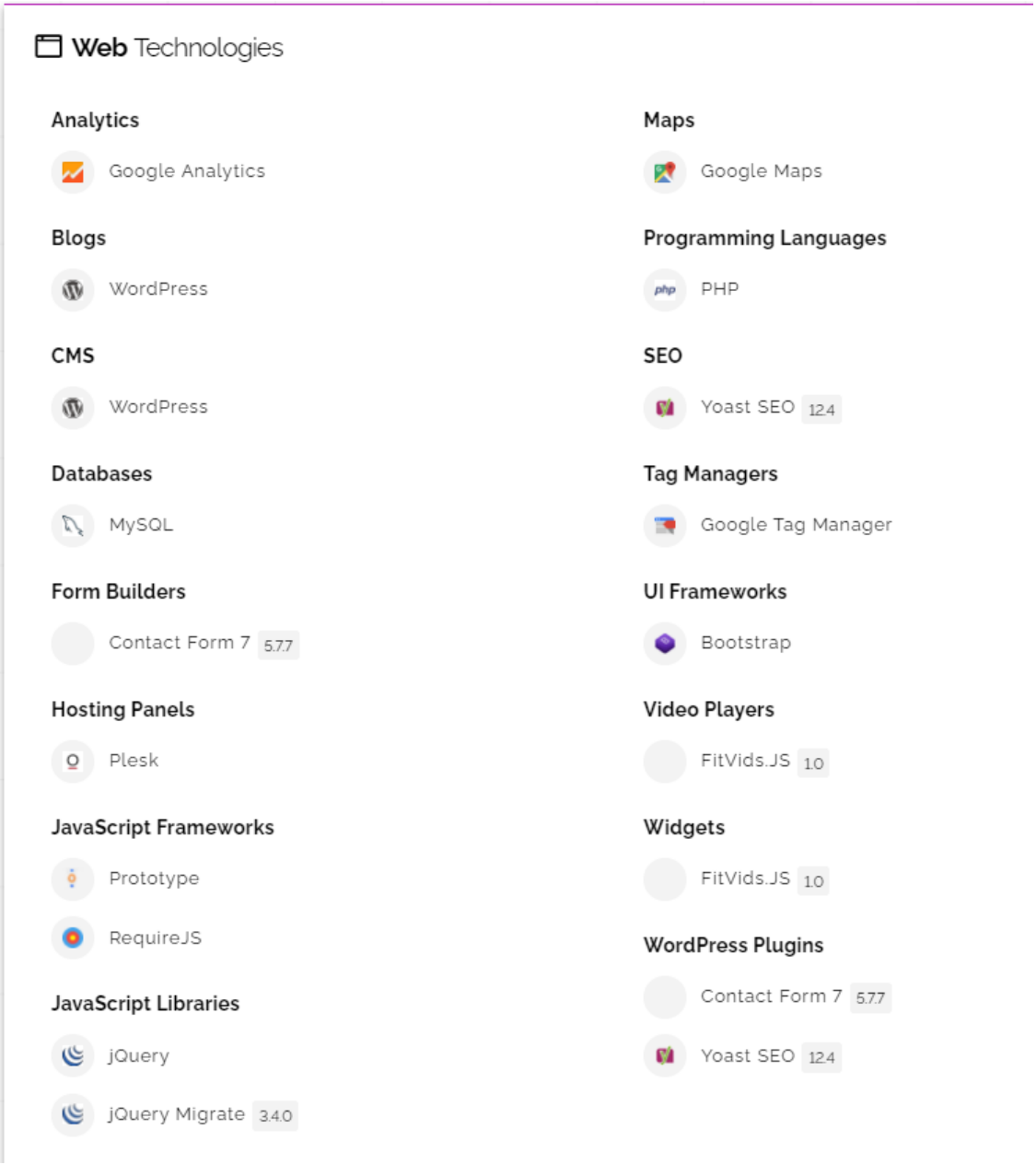

Imagen 17. Tecnologías web obtenidas en Shodan

4.2.3. Análisis de puertos y servicios

Con las herramientas Shodan y Censys se han descubierto 11 puertos abiertos en el servidor. A continuación, se analizarán los servicios prestados desde el punto de vista de la seguridad.

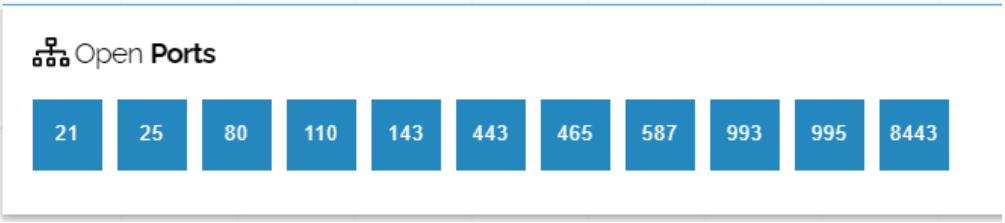

Imagen 18. Puertos abiertos obtenidos en Shodan

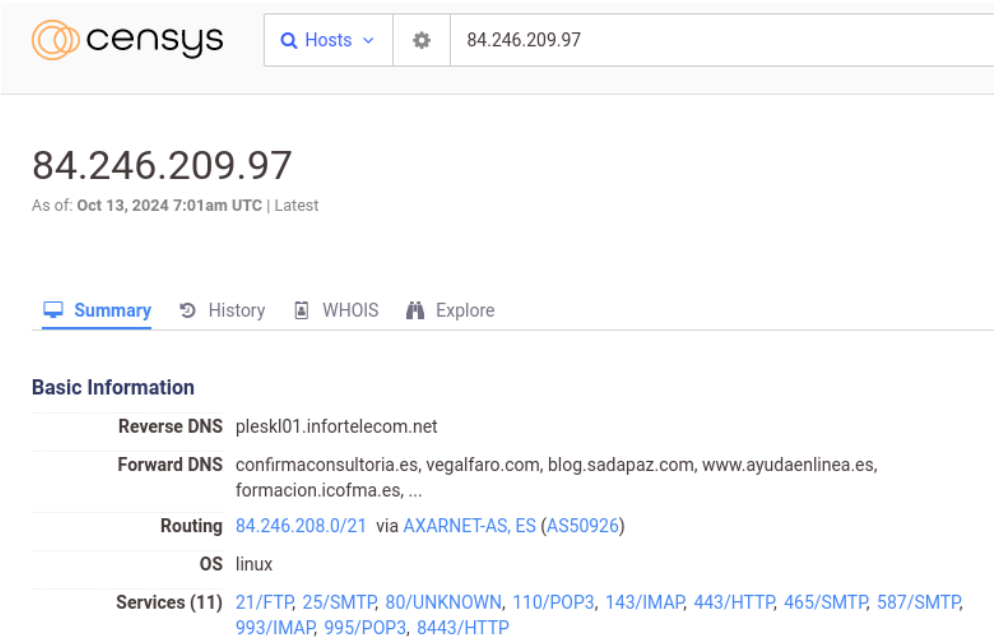

Imagen 19. Puertos abiertos obtenidos en Cenys

Primero se analizarán aquellos servicios que no agregan una capa de seguridad al protocolo con el que interactúan con el fin de proteger la integridad, confidencialidad y la autenticación:

Puerto	**Servicio**	**Protocolo**	**Cifrado**	**Información adicional**
21	FTP	TCP	Sí	Software: ProFTPD Project ProFTPD
25	SMTP	TCP	Sí	Software: Postfix
80	HTTP	TCP	No	Software: Red Hat Enterprise Linux
110	POP3	TCP	Sí	Software: Dovecot
143	IMAP	TCP	Sí	Software: Dovecot

Debajo se examinan los servicios que usan cifrado o medidas de seguridad adicionales:

Puerto	**Servicio**	**Protocolo**	**Información adicional**
443	HTTPS	TLS/SSL	Software: nginx No aparece versión de aplicación No permite realizar conexión anónima al servicio No contiene la cabecera Set-Cookie
465	SMTPS	TLS/SSL	Software: linux, Postfix No la ejecución del comando VRFY (250) o EXPN
587	SMTPS	TLS/SSL	Software: Postfix No la ejecución del comando VRFY (250) o EXPN
993	IMAPS	TLS/SSL	Software: linux, Dovecot
995	POP3S	TLS/SSL	Software: Dovecot
8443	HTTPS	TLS/SSL	Software: Parallels Plesk Panel, Parallels Plesk

4.2.4. Otras vulnerabilidades

Del examen con Shodan, Spiderfoot, y Pentest Tools (informe adjuntado al documento) se extrajeron las vulnerabilidades que se muestran en la tabla a continuación.
Por otro lado, del examen Spiderfoot, las categorías más relevantes extraídas son:

- Certificado SSL - Datos sin procesar
- Dominios similares
- Dominio similar - whois
- URL enlazada - Interna
- Afiliado - Dirección de correo electrónico
- Sitio coalojado
- Encabezados HTTP
- Datos brutos de RIRs/APIs
- Nombre humano

Vulnerabilidad/Riesgo	Nivel de impacto	Descripción	Afecta a
CVE-2024-4577	Crítico CVSS 9.8	El comportamiento "Best-Fit" en Windows se refiere a cómo ciertas configuraciones de código de página pueden hacer que el sistema reemplace caracteres al pasar comandos a la API Win32, resultando en interpretaciones incorrectas. Un usuario malicioso podría aprovechar esta vulnerabilidad para obtener acceso a scripts de PHP que deberían estar protegidos; o ejecutar código PHP no autorizado en el servidor.	PHP 8.3 (anteriores a 8.3.8) PHP 8.2 (anteriores a 8.2.20) PHP 8.1 (anteriores a 8.1.29) que se ejecutan en Windows con Apache y el módulo PHP-CGI
CVE-2013-2220	Alto CVSS 7.5	Desbordamiento de búfer que permite que un atacante remoto puede enviar un valor de longitud de Atributos Específicos de Proveedor (VSA) excesivamente grande al servidor. Esto puede causar una denegación de servicio (DoS) y en algunos casos, podría permitir al atacante ejecutar código arbitrario en el sistema afectado.	Sistemas que utilizan la extensión RADIUS de PHP
CVE-2024-5458	Medio CVSS 5.3	Se origina en un error de lógica en el código de PHP que afecta la forma en que las funciones de filtrado validan las URLs. Cuando se utilizan ciertas URLs que contienen información de usuario (es decir, nombre de usuario y contraseña), el filtro puede aceptar datos inválidos como válidos y procesarlos erróneamente. Esto podría	PHP versiones 8.1.* antes de 8.1.29, 8.2.* antes de 8.2.20, y 8.3.* antes de 8.3.8.

Vulnerabilidad/Riesgo	Nivel de impacto	Descripción	Afecta a
		llevar a problemas de seguridad, como la exposición de credenciales, o permitir a un atacante manipular la forma en que se gestionan las conexiones o la autenticación en una aplicación.	
CVE-2007-3205	Medio CVSS 5.0	Problema en la función parse_str() de PHP y sus extensiones Hardened-PHP y Suhosin. Se presenta cuando parse_str() es llamada sin un segundo parámetro, lo que permite que los nombres de las variables sean especificados directamente en la cadena de consulta. Los atacantes pueden manipular la cadena para sobreescribir variables arbitrarias en el ámbito global del script.	PHP, extensiones Hardened-PHP y Suhosin
Versión del software revelada en puertos abiertos	Medio	Revelar la versión de software puede facilitar ataques dirigidos basados en vulnerabilidades conocidas.	Servidores web y MX
Sitios web co-alojados considerados maliciosos	Medio	Varias páginas web alojadas en dominios como: gauss.es, hsnet.es, kitdigital.hsnet.es, hipodromolondonpub.hsnet.es, entre otros, han sido catalogadas como maliciosas por Comodo Secure DNS.	Sitios web co-alojados
Direcciones IP vinculadas a actividades maliciosas	Bajo	IP 15.197.142.173 y 3.33.152.147: Identificadas como maliciosas en múltiples fuentes (PhishStats y VoIP Blacklist). Estas direcciones están relacionadas con actividades de phishing y ataques VoIP.	Servidores asociados a esas IPs
Falta la cabecera de seguridad: Strict-Transport-Security (HSTS) - CWE-693	Bajo	La falta de esta cabecera permite a un atacante forzar a un usuario víctima a iniciar una conexión HTTP de texto claro con el servidor, lo que permite espiar el tráfico de red y extraer información sensible (por ejemplo, cookies de sesión).	Servidores web

Vulnerabilidad/Riesgo	Nivel de impacto	Descripción	Afecta a
Falta la cabecera de seguridad: Referrer-Policy - CWE-693	Bajo	Sin esta cabecera, los navegadores pueden enviar información de referencia completa (URL completa) a otros dominios. Esto podría incluir parámetros sensibles, tokens de sesión u otros datos que no deberían ser accesibles a terceros.	Servidores web
Falta la cabecera de seguridad: Content-Security-Policy - CWE-693	Bajo	Si la aplicación de destino es vulnerable a XSS, la falta de este encabezado hace que sea fácilmente explotable por los atacantes.	Aplicaciones web vulnerables
Falta la cabecera de seguridad: X-Content-Type-Options - CWE-693	Bajo	La falta de esta cabecera podría posibilitar ataques como Cross-Site Scripting o phishing en navegadores Internet Explorer.	Navegadores Internet Explorer
Archivo Robots.txt encontrado	Bajo	La existencia de un archivo robots.txt no supone ningún riesgo especial para la seguridad. Sin embargo, es importante tener en cuenta que añadir endpoints en él no debe considerarse una medida de seguridad. una medida de seguridad, ya que cualquiera puede acceder directamente a este archivo y leerlo.	Servidores web
Falta el archivo Security.txt	Bajo	No existe ningún riesgo particular en no tener un archivo security.txt para el servidor. Sin embargo, este archivo es importante porque ofrece un canal designado para informar de vulnerabilidades y problemas de seguridad.	Servidores web

Vulnerabilities

All ports | Latest

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

2024

CVE-2024-5458 falseIn PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, due to a code logic error, filtering functions such as filter_var when validating URLs (FILTER_VALIDATE_URL) for certain types of URLs the function will result in invalid user information (username + password part of URLs) being treated as valid user information. This may lead to the downstream code accepting invalid URLs as valid and parsing them incorrectly.

CVE-2024-4577 falseIn PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, when using Apache and PHP-CGI on Windows, if the system is set up to use certain code pages, Windows may use "Best-Fit" behavior to replace characters in command line given to Win32 API functions. PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc.

2013

CVE-2013-2220 7.5 Buffer overflow in the radius_get_vendor_attr function in the Radius extension before 1.2.7 for PHP allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a large Vendor Specific Attributes (VSA) length value.

2007

CVE-2007-3205 5.0 The parse_str function in (1) PHP, (2) Hardened-PHP, and (3) Suhosin, when called without a second parameter, might allow remote attackers to overwrite arbitrary variables by specifying variable names and values in the string to be parsed. NOTE: it is not clear whether this is a design limitation of the function or a bug in PHP, although it is likely to be regarded as a bug in Hardened-PHP and Suhosin.

Imagen 20. Vulnerabilidades obtenidas en Shodan

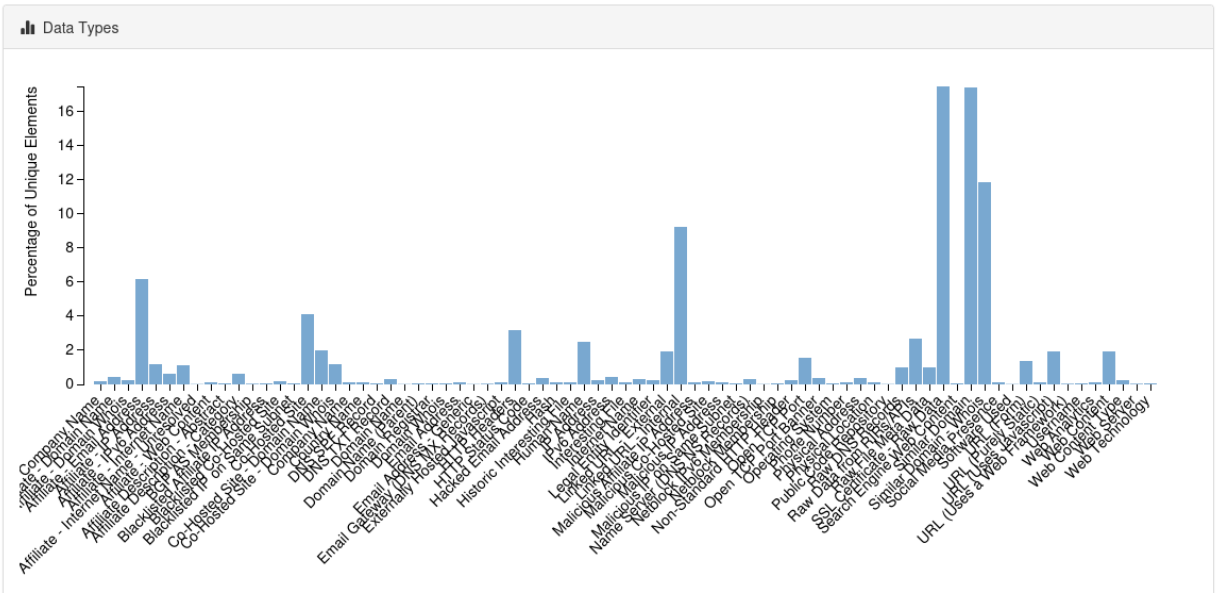

Imagen 21. Gráfico Spiderfoot

5. Información corporativa

5.1 Equipo directivo

Administradores, dirigentes y auditor de cuentas

Cargo vigente	**Apellidos y nombre**	**Nombramiento**
Presidente	García García, Juan José	24/02/2011
Vicepresidente	Cornejo Pablos, José Fernando	24/02/2011
Consejero delegado	García García, Juan José	24/02/2011
Consejero	Cabello Esteban, Francisco Javier	18/04/2016
Consejero	Gutiérrez del Álamo Gil, Ramón	24/02/2011
Consejero	Cornejo Pablos, José Fernando	24/02/2011
Consejero	García García, Juan José	24/02/2011
Secretario	Gutiérrez del Álamo Gil, Ramón	23/09/2013

Cargos directivos

Cargo	Persona física/jurídica	Desde	Hasta
Consejero	Cabello Esteban Francisco Javier	18/04/2016	Actualidad
Secretario	Gutierrez Del Alamo Gil Ramon	23/09/2013	Actualidad
Consejero	Gutierrez Del Alamo Gil Ramon	14/02/2011	Actualidad
Presidente	Garcia Garcia Juan-Jose	14/02/2011	Actualidad
Consejero	Garcia Garcia Juan-Jose	14/02/2011	Actualidad
Con.Delegado	Garcia Garcia Juan-Jose	14/02/2011	Actualidad
Vicepresid.	Cornejo Pablos Jose Fernando	14/02/2011	Actualidad
Consejero	Cornejo Pablos Jose Fernando	14/02/2011	Actualidad

Imagen 22. Cargos directivos obtenidos de Libreborme

Directivos funcionales/ejecutivos

Cargo vigente	**Apellidos y nombre**
Gerente	Macipe Gómez, David
Director/Responsable financiero	Macipe Gómez, David

Accionistas

- García García, Juan José
- Cabello Esteban, Francisco Javier
- Gutiérrez del Álamo Gil, Ramón

5.2 Personal de la empresa

5.2.1 Datos personales

Cargo vigente	**Apellidos y nombre**
Letrados	Gutiérrez del Álamo, Ramón Cabello, Javier Calvo, Carlos Manuel Gutiérrez-Maturana, Luis Abelairas, Nuria Córdoba, Inmaculada Santamaría, Laura Alos, Esther Burón, Julia Camino, Gael
Director Plataforma de Recobro	Martín Canencia, Alfonso
Director General COO	Rodríguez, José Manuel
IT Tecnología	Josic, Rudi
Administración y Finanzas	Macipe, David
Consejera Académica	Peiteado, Pilar

5.2.2 Redes sociales

Haciendo una búsqueda en LinkedIn, vemos que hay 54 usuarios que actualmente trabajan para Adarve Abogados.

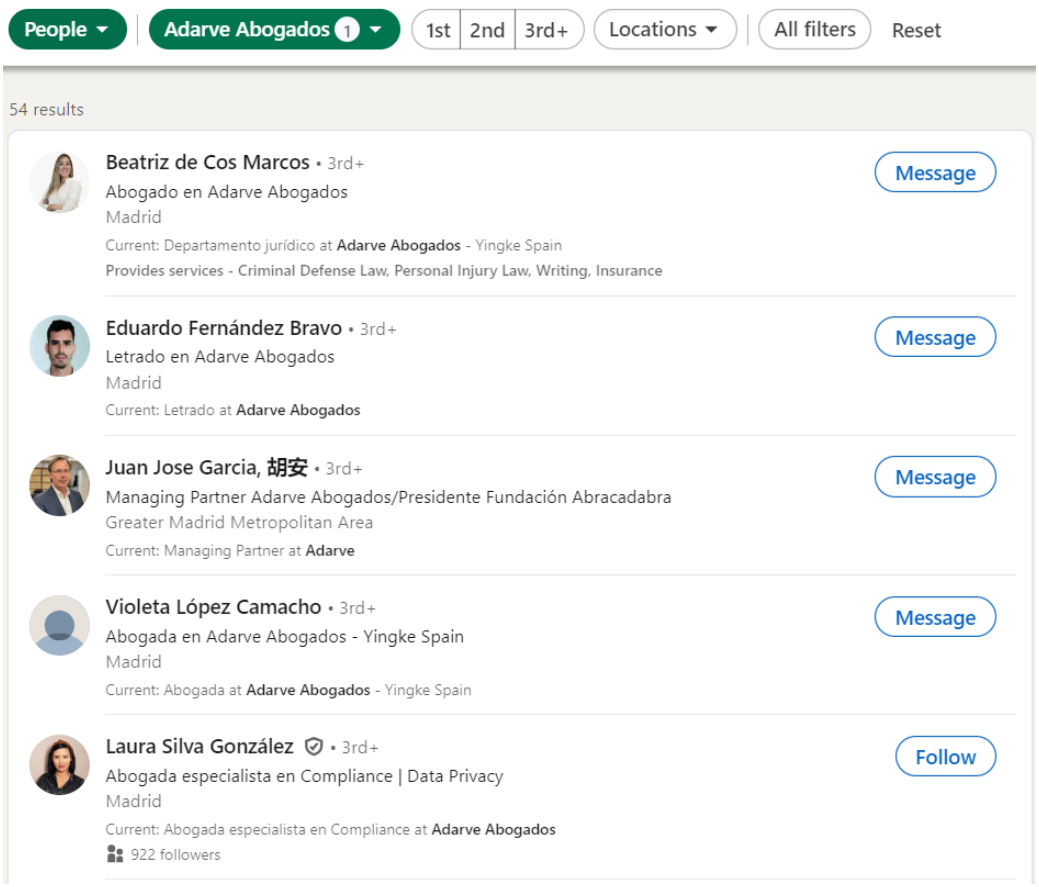

Imagen 23. Resultados de la búsqueda de empleados de Adarve Abogados en LinkedIn.

6. Otra información

6.1 Emails corporativos recopilados

Se encontraron los siguientes emails con una búsqueda en CrossLinked:

pol.panicot@adarve.com
jesus.fernandez@adarve.com
juan.an@adarve.com
david.gomez@adarve.com
isabel.alvarez@adarve.com
irene.martinez@adarve.com
elena.castillo@adarve.com
fernando.lozano@adarve.com
paula.camacho@adarve.com
santiago.londono@adarve.com
juanma.rubio@adarve.com
guillermo.albala@adarve.com
silvia.correal@adarve.com
javier.cabello@adarve.com
nelson.rendon@adarve.com
jose.garcia@adarve.com
luz.gomez@adarve.com
clara.gutierrez@adarve.com
paula.monroy@adarve.com
nuria.perez@adarve.com
andrea.martinez@adarve.com
edna.salazar@adarve.com
ramon.alamo@adarve.com
esther.zaragoza@adarve.com
adelaida.torres@adarve.com
alvaro.marco@adarve.com

```
┌──(root㉿kali)-[~/Software/crosslinked]
└─# python3 crosslinked.py -f '{first}.{last}@adarve.com' Adarve -o /root/Downloads/InformeOSINT/crosslinked_results.txt

    ____                     _     _           _
   / ___|_ __ ___  ___ ___| |   (_)_ __ | | _____  __| |
  | |   | '__/ _ \/ __/ __| |   | | '_ \| |/ / _ \/ _` |
  | |___| | | (_) \__ \__ \ |___| | | | |   <  __/ (_| |
   \____|_|  \___/|___/___/_____|_|_| |_|_|\_\___|\__,_|  @m8sec
                                                         v0.3.0

[*] Searching google, bing for valid employee names at "Adarve"
[*] 0   https://www.google.com/search?q=site:linkedin.com/in+"Adarve"&num=100&start=0 (429)
[!] None 200 response, exiting search (429)
[*] 20  http://www.bing.com/search?q="Adarve"+site:linkedin.com/in&first=0 (200)
[*] 26  http://www.bing.com/search?q="Adarve"+site:linkedin.com/in&first=20 (200)
[*] 36  http://www.bing.com/search?q="Adarve"+site:linkedin.com/in&first=26 (200)
[*] 45  http://www.bing.com/search?q="Adarve"+site:linkedin.com/in&first=36 (200)
[*] 45  http://www.bing.com/search?q="Adarve"+site:linkedin.com/in&first=45 (200)
[*] 55  http://www.bing.com/search?q="Adarve"+site:linkedin.com/in&first=45 (200)
[*] 65  http://www.bing.com/search?q="Adarve"+site:linkedin.com/in&first=55 (200)
[*] 65  http://www.bing.com/search?q="Adarve"+site:linkedin.com/in&first=65 (200)
[*] 65  http://www.bing.com/search?q="Adarve"+site:linkedin.com/in&first=65 (200)
[*] 65  http://www.bing.com/search?q="Adarve"+site:linkedin.com/in&first=65 (200)
[*] 74  http://www.bing.com/search?q="Adarve"+site:linkedin.com/in&first=65 (200)
[*] 74  http://www.bing.com/search?q="Adarve"+site:linkedin.com/in&first=74 (200)
[*] 74 names collected
[+] 63 unique names added to /root/Downloads/InformeOSINT/crosslinked_results.txt.txt!

┌──(root㉿kali)-[~/Software/crosslinked]
└─# /root/Downloads/InformeOSINT
```

```
┌──(root㉿kali)-[~/Downloads/InformeOSINT]
└─# cat crosslinked_results.txt.txt
pol.panicot@adarve.com
ver.*@adarve.com
antonio.adarve@adarve.com
etiquetas:euroinnova.comercialesfollowers:336@adarve.com
jesus.fernandez@adarve.com
etiquetas:madrid.(eoi)@adarve.com
juan.an@adarve.com
etiquetas:madrid.partner@adarve.com
david.gomez@adarve.com
etiquetas:madrid.for:adarvefollowers:335@adarve.com
jesus.adarve@adarve.com
etiquetas:madrid.ab@adarve.com
daniel.adarve@adarve.com
etiquetas:sevilla,.latam@adarve.com
isabel.alvarez@adarve.com
etiquetas:madrid.analystfollowers:432@adarve.com
irene.martinez@adarve.com
etiquetas:madrid,.intercultural@adarve.com
jose.adarve@adarve.com
etiquetas:project.s.l.@adarve.com
elena.castillo@adarve.com
fernando.lozano@adarve.com
lydia.adarve@adarve.com
ranier.mhpe@adarve.com
estefania.adarve@adarve.com
paula.camacho@adarve.com
santiago.londono@adarve.com
juanma.rubio@adarve.com
john.adarve@adarve.com
guillermo.albala@adarve.com
isabel.adarve@adarve.com
comercial.adarve@adarve.com
silvia.correal@adarve.com
angel.adarve@adarve.com
javier.cabello@adarve.com
pepe.adarve@adarve.com
laura.adarve@adarve.com
nelson.rendon@adarve.com
jose.garcia@adarve.com
enrique.adarve@adarve.com
luz.gomez@adarve.com
clara.gutierrez@adarve.com
paula.monroy@adarve.com
mario.adarve@adarve.com
javier.adarve@adarve.com
marcela.adarve@adarve.com
nuria.perez@adarve.com
mauricio.adarve@adarve.com
andrea.martinez@adarve.com
gloria.adarve@adarve.com
carlos.adarve@adarve.com
edna.salazar@adarve.com
ramon.alamo@adarve.com
adarve.seguros@adarve.com
esther.zaragoza@adarve.com
juan.adarve@adarve.com
ricardo.adarve@adarve.com
erin.adarve@adarve.com
adelaida.torres@adarve.com
sandra.adarve@adarve.com
patricia.adarve@adarve.com
luis.adarve@adarve.com
pedro.adarve@adarve.com
```

Imagen 24. Resultados de correos electrónicos obtenidos con CrossLinked

Tras una búsqueda con HaveIbeenPwned se comprueba que las direcciones de correo info@adarve.com, alvaro.marco@adarve.com y javier.cabello@adarve.com se encuentran en filtraciones de datos.

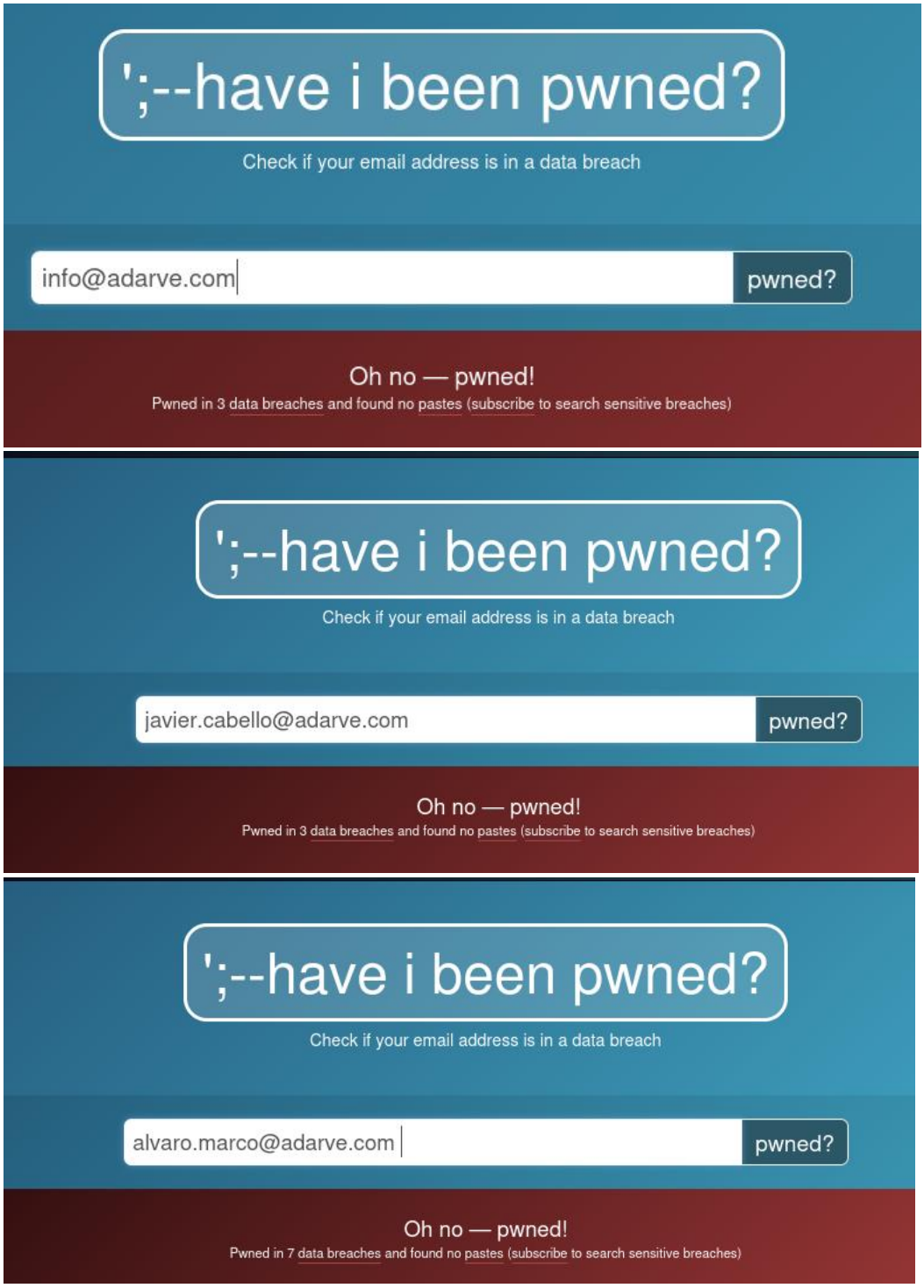

Imagen 25. Resultados de HaveIBeenPwned

Analizando los correos con Ghunt, no se encontraron suscripciones.

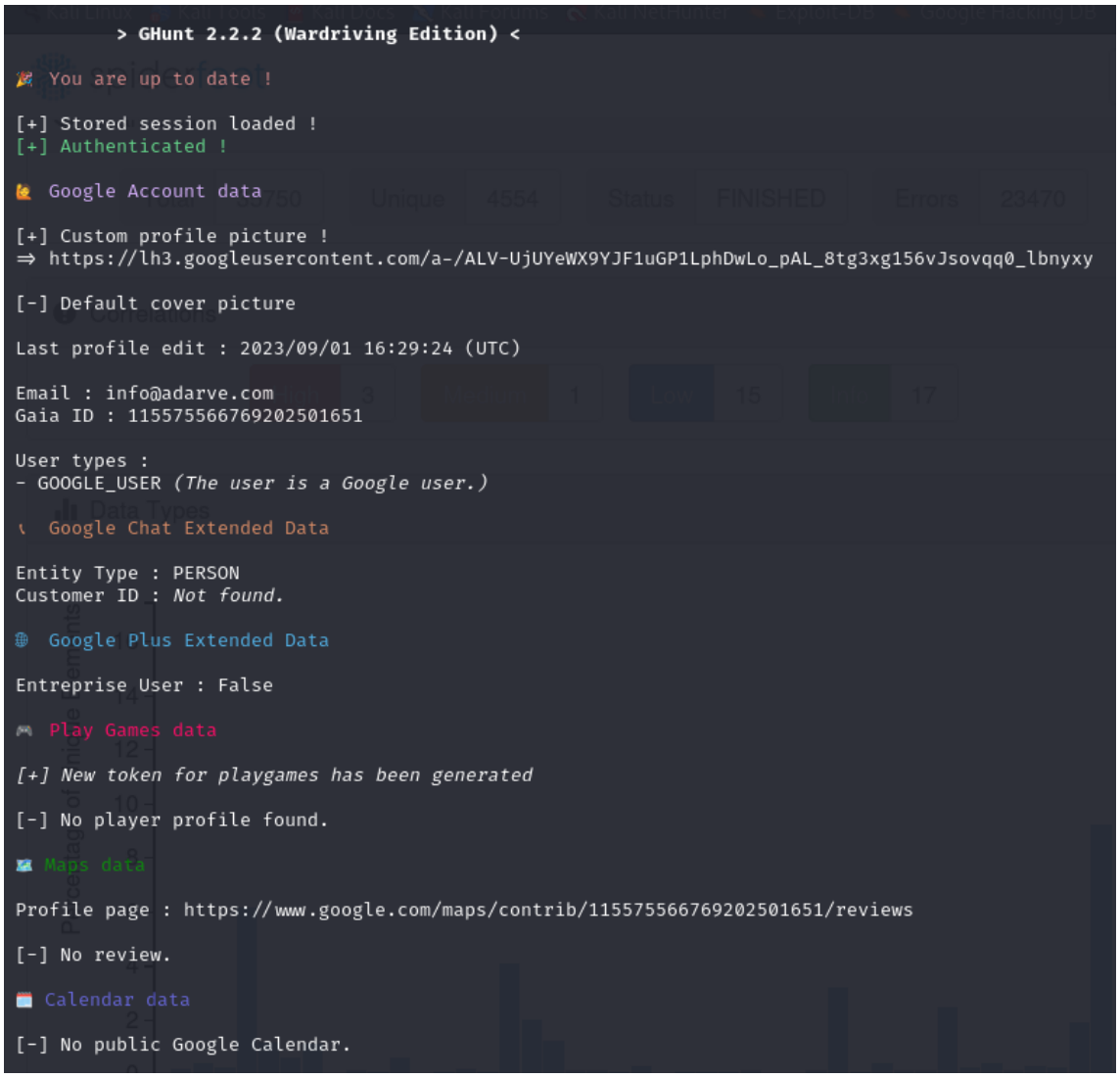

Imagen 26. Análisis de correos electrónicos con Ghunt.

6.2 Informe y gráfico Maltego

Se adjunta a este documento un informe elaborado con la herramienta Maltego, que recopila y analiza información sobre la presencia en la red de Adarve Abogados. Se adjunta también un gráfico de relaciones para mostrar cómo están conectados diferentes datos y entidades entre sí.

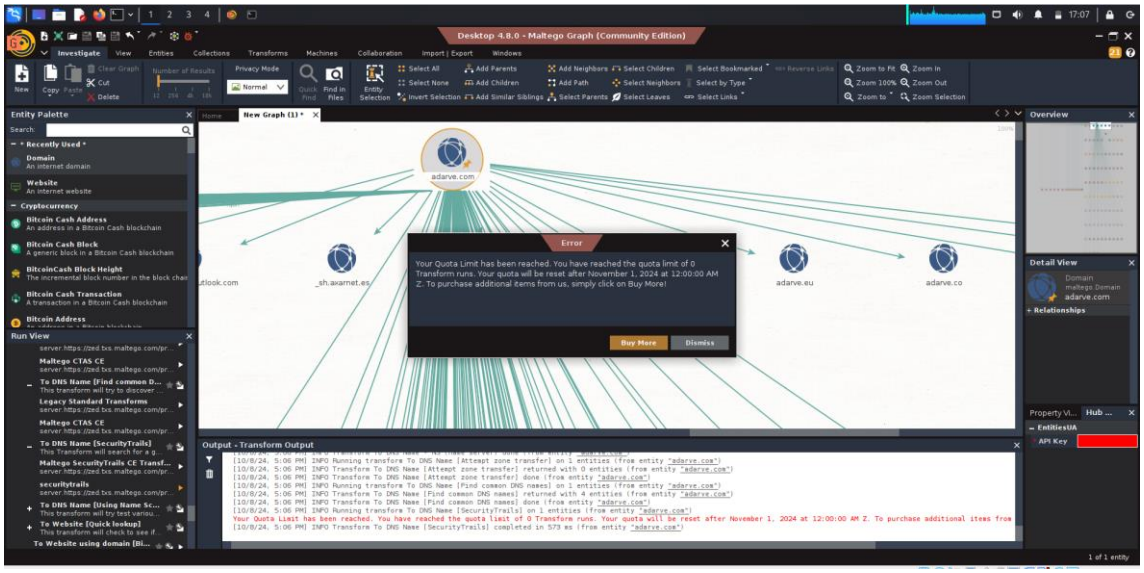

Imagen 27. Gráfico Maltego.

6.3 Metadatos

Con la herramienta metagoofil se consiguieron extraer dos documentos pdf de la página web de Adarve. Tras un análisis con exiftool, se comprobó que estos archivos no contienen metadatos relevantes/susceptibles.

```
┌──(root㉿kali)-[~]
└─# metagoofil -d adarve.com -t pdf
[*] Searching for 100 .pdf files and waiting 30.0 seconds between searches
^CTraceback (most recent call last):
```

Imagen 28. Búsqueda de archivos con metagoofil.

```
┌──(root㉿kali)-[~/Downloads/metagoofil_adarve/adarve_pdf]
└─# exiftool Adarve-021121-003.pdf
ExifTool Version Number         : 12.76
File Name                       : Adarve-021121-003.pdf
Directory                       : .
File Size                       : 1359 kB
File Modification Date/Time     : 2024:10:05 16:31:24+02:00
File Access Date/Time           : 2024:10:05 16:31:24+02:00
File Inode Change Date/Time     : 2024:10:05 16:31:24+02:00
File Permissions                : -rw-r--r--
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.4
Linearized                      : Yes
Language                        : es-ES
Tagged PDF                      : Yes
XMP Toolkit                     : Adobe XMP Core 5.6-c017 91.164464, 2020/06/15-10:20:05
Create Date                     : 2021:11:02 21:13:20+01:00
Metadata Date                   : 2021:11:04 14:26:04+01:00
Modify Date                     : 2021:11:04 14:26:04+01:00
Creator Tool                    : Adobe InDesign 16.4 (Macintosh)
Instance ID                     : uuid:e18adec0-0566-4fad-a23d-07d795390314
Original Document ID            : xmp.did:593b55cb-e7a5-4c0f-91a8-80cd28a28aab
Document ID                     : xmp.id:04f05784-9460-466a-b27f-278bd2ac8c84
Rendition Class                 : proof:pdf
Derived From Instance ID        : xmp.iid:d64f0eb4-9d0b-4f1e-a8c9-f0c0d6ebb9a3
Derived From Document ID        : xmp.did:cda5a6ee-31e6-433c-89b1-4d365eb50a3e
Derived From Original Document ID: xmp.did:593b55cb-e7a5-4c0f-91a8-80cd28a28aab
Derived From Rendition Class    : default
History Action                  : converted
History Parameters              : from application/x-indesign to application/pdf
History Software Agent          : Adobe InDesign 16.4 (Macintosh)
History Changed                 : /
History When                    : 2021:11:02 21:13:20+01:00
Format                          : application/pdf
Producer                        : Adobe PDF Library 16.0
Trapped                         : False
Page Count                      : 9
Creator                         : Adobe InDesign 16.4 (Macintosh)
```

```
┌──(root㉿kali)-[~/Downloads/metagoofil_adarve/adarve_pdf]
└─# exiftool Adarve-06_05.pdf
ExifTool Version Number         : 12.76
File Name                       : Adarve-06_05.pdf
Directory                       : .
File Size                       : 768 kB
File Modification Date/Time     : 2024:10:05 16:31:24+02:00
File Access Date/Time           : 2024:10:05 16:31:24+02:00
File Inode Change Date/Time     : 2024:10:05 16:31:24+02:00
File Permissions                : -rw-r--r--
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.4
Linearized                      : Yes
Language                        : es-ES
Tagged PDF                      : Yes
XMP Toolkit                     : Adobe XMP Core 7.1-c000 79.83fae64, 2022/02/15-08:07:32
Create Date                     : 2022:05:06 11:24:44+02:00
Metadata Date                   : 2022:05:06 11:24:46+02:00
Modify Date                     : 2022:05:06 11:24:46+02:00
Creator Tool                    : Adobe InDesign 17.2 (Macintosh)
Instance ID                     : uuid:05fdad07-74b6-0243-a071-46b775b01653
Original Document ID            : xmp.did:593b55cb-e7a5-4c0f-91a8-80cd28a28aab
Document ID                     : xmp.id:fc3ac22a-8a06-4301-b37b-69d4a7caffb1
Rendition Class                 : proof:pdf
Derived From Instance ID        : xmp.iid:9400ccdb-3a48-461b-92ef-01ae864e8891
Derived From Document ID        : xmp.did:2ac92cd5-8ab8-473d-9053-ad472ea927c8
Derived From Original Document ID: xmp.did:593b55cb-e7a5-4c0f-91a8-80cd28a28aab
Derived From Rendition Class    : default
History Action                  : converted
History Parameters              : from application/x-indesign to application/pdf
History Software Agent          : Adobe InDesign 17.2 (Macintosh)
History Changed                 : /
History When                    : 2022:05:06 11:24:44+02:00
Format                          : application/pdf
Producer                        : Adobe PDF Library 16.0.7
Trapped                         : False
Page Count                      : 7
Creator                         : Adobe InDesign 17.2 (Macintosh)
```

Imagen 29. Resultados de exiftools

6.4 Otra información

Tras una búsqueda en Pastebin, no se han encontrado menciones a la empresa.

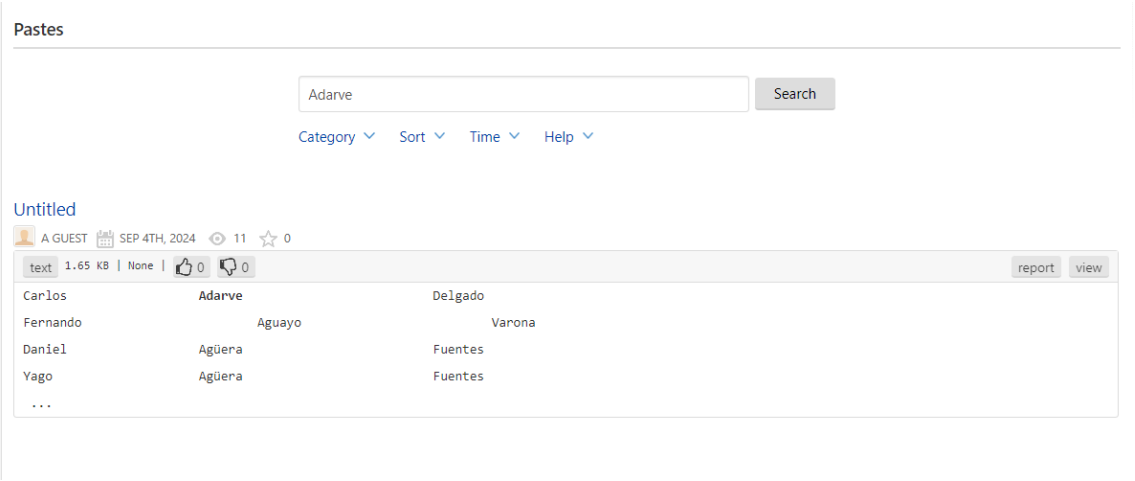

Imagen 30. Búsqueda en Pastebin

7. Recomendaciones

1. Vulneración Mec Seg: Vulnerabilidad CVE (parche existente): CVE-2024-4577 (CVSS 9.8 – Crítica)

Descripción:

Se detecta una vulnerabilidad sobre un activo del Cliente (con parche existente), publicada en el diccionario de vulnerabilidades CVE.

Recomendación:

- Se recomienda actualizar urgentemente el activo vulnerable a la última versión según indique el fabricante. Es decir, actualizar PHP a las últimas versiones que contienen los parches para CVE-2024-4577. El equipo de desarrollo de PHP ha publicado correcciones en el registro de cambios reciente para PHP 8 que abordan este problema. Se recomienda que la instalación de PHP esté actualizada a una de las siguientes versiones:
  - PHP 8.3.8 o posterior
  - PHP 8.2.20 o posterior
  - PHP 8.1.29 o posterior
- Si es posible, se aconseja configurar el servidor web para evitar ejecutar PHP en modo CGI. En su lugar, puede usarse PHP-FPM (Administrador de procesos FastCGI) o mod_php con Apache para lograr una mejor seguridad y rendimiento.

Acciones directas:

- Parcheo aplicaciones vulnerables
- Inventariado de activos
- Pentesting persistente
- Campañas de concienciación

2. Vulneración Mec Seg: Vulnerabilidad CVE (parche existente): CVE-2013-2220 (CVSS 7.5 – Alta)

Descripción:

Se detecta una vulnerabilidad sobre un activo del Cliente (con parche existente), publicada en el diccionario de vulnerabilidades CVE.

Recomendación:

- Se recomienda actualizar urgentemente el activo vulnerable a la última versión según indique el fabricante. Es decir, actualizar la extensión PHP Radius a la versión 1.2.7 o posterior. Esto se puede hacer normalmente a través del administrador de paquetes.
- Si no es posible realizar una actualización inmediata, se recomienda deshabilitar la extensión PHP Radius temporalmente hasta que se pueda aplicar una solución. Sin embargo, debe tenerse en cuenta que esto puede afectar cualquier funcionalidad que dependa de la autenticación RADIUS.

Acciones directas:

- Parcheo aplicaciones vulnerables
- Inventariado de activos
- Pentesting persistente

3. Vulneración Mec Seg: Vulnerabilidad CVE (parche existente): CVE-2024-5458 (CVSS 5.3 – Media)

Descripción:

Se detecta una vulnerabilidad sobre un activo del Cliente (con parche existente), publicada en el diccionario de vulnerabilidades CVE.

Recomendación:

- Se recomienda actualizar urgentemente el activo vulnerable a la última versión según indique el fabricante. Es decir, actualizar PHP a la versión 8.1.29, 8.2.20 o 8.3.8, según la versión instalada. Estas actualizaciones solucionan el error de lógica del código y garantizan la validación adecuada de la información del usuario dentro de las URL.
- Como solución temporal, los desarrolladores pueden validar manualmente la información del usuario dentro de las URL antes de pasarlas a la función filter_var. Esto se puede lograr implementando una lógica de validación personalizada o utilizando bibliotecas de análisis de URL alternativas que no sufran la misma vulnerabilidad. Debe tenerse en cuenta que esta solución alternativa debe ser temporal y se recomienda aplicar los parches oficiales lo antes posible.

Acciones directas:

- Parcheo aplicaciones vulnerables
- Inventariado de activos
- Pentesting persistente

4. Vulneración Mec Seg: Vulnerabilidad CVE (parche existente): CVE-2007-3205 (CVSS 5.0 – Media)

Descripción:

Se detecta una vulnerabilidad sobre un activo del Cliente (con parche existente), publicada en el diccionario de vulnerabilidades CVE.

Recomendación:

- Se recomienda actualizar urgentemente el activo vulnerable a la última versión según indique el fabricante. Si se utiliza Hardened-PHP o Suhosin, es recomendable actualizar también estos componentes a sus últimas versiones con parches de seguridad aplicados.
- Se recomienda también auditar el uso de parse_str, realizando una revisión del código para identificar todas las instancias donde se utiliza la función parse_str. Verificar que se esté utilizando correctamente, es decir, con un segundo parámetro que defina el array donde se deben almacenar las variables.
- Es aconsejable establecer una configuración segura de PHP, incluyendo la desactivación de funciones peligrosas y el uso de display_errors configurado en Off para evitar la exposición de información sensible.

Acciones directas:

- Parcheo aplicaciones vulnerables
- Inventariado de activos
- Pentesting persistente

5. Robo de credenciales

Descripción:

Se detectan credenciales relativos a un dominio interno o externo perteneciente a servicios corporativos (ej. SSO de la compañía) y/o servicios de uso personal (ej. gmail). En concreto, las credenciales de las cuentas info@adarve.com, alvaro.marco@adarve.com y javier.cabello@adarve.com

Recomendación:

- Se recomienda la modificación urgente de las contraseñas asociadas a las credenciales expuestas. Paralelamente se aconseja realizar un análisis de los equipos asociados a las credenciales comprometidas, revisando los logs de éstos de cara a identificar conexiones a IPs sospechosas. En la mayoría de los casos, la fuga de credenciales viene derivada de una infección en el equipo por algún tipo de Malware. Se recomienda también por lo tanto el escaneo de los PCs afectados (en este caso, estos pueden ser corporativos o de uso personal) de cara a identificar y eliminar cualquier tipo de recurso malicioso en el mismo.
- En el caso de que las credenciales expuestas correspondan a servicios personales utilizadas por empleados de la Organización (ej. gmail), se recomienda contactar con los usuarios afectados, con el propósito de comunicarles que sus credenciales personales han sido comprometidas. Por otra parte, existe un riesgo implícito derivado de ciertas

malas prácticas por parte de los usuarios al reutilizar sus contraseñas personales en cuentas corporativas (portales, cuentas de correo, etc.). Por lo tanto, se aconseja verificar con los usuarios afectados si éstos efectivamente usaban las mismas credenciales corporativas a las públicamente expuestas. En caso positivo proceder de igual forma al reseteo de las contraseñas corporativas.

- De forma preventiva se recomienda aplicar políticas de formación y concienciación, advirtiendo a los usuarios de los riesgos derivados de una mala gestión de contraseñas, enfatizando la importancia de utilizar contraseñas diferentes para aplicaciones profesionales y personales.

Acciones directas:

- Reseteo de contraseñas
- Revisar logs
- Análisis de equipos afectados
- Plan de formación y concienciación
- Notificación usuario afectado

6. Dominios sospechosos: Páginas web activas (phising)

Descripción:

Se identifica en internet el registro de un dominio con contenido malicioso (web similar a la oficial solicitando al usuario la introducción de sus credenciales) dirigido a confundir a los usuarios a través de la utilización no autorizada de recursos del Cliente para fines malintencionados (robo de credenciales, descarga de malware, etc.)

Recomendaciones:

- En el caso de que la web relativa al dominio sospechosa ya haya sido dotada de contenido, y éste represente un abuso explícito de la marca del Cliente (utilización de logo, marcas registradas, etc.), se recomienda la notificación de retirada de contenido a la plataforma que alberga el recurso malicioso en base al derecho del Cliente sobre su propiedad intelectual.
- Se aconseja además revisar los logs del firewall/proxy de cara a identificar accesos de los equipos de la Organización en la web maliciosa. De haberse producido, estos equipos podrían haber filtrado sus credenciales de acceso, por lo que resultaría esencial el reseteo de sus contraseñas, así como el análisis de los mismos en búsqueda de una posible infección.

Acciones directas:

- Notificación retirada contenido
- Revisión logs y accesos
- Reseteo de contraseñas equipos afectados

7. Dominios sospechosos: Sitios web co-alojados considerados maliciosos

Descripción:

Se identifican varias páginas web alojadas en dominios como gauss.es, hsnet.es, kitdigital.hsnet.es, hipodromolondonpub.hsnet.es, entre otros, que han sido catalogadas como maliciosas por Comodo Secure DNS. Estos sitios pueden estar involucrados en actividades maliciosas, como la distribución de malware, fraudes, o suplantación de identidad, lo que podría comprometer la seguridad de los usuarios y la reputación del Cliente.

Recomendaciones:

Se recomienda contactar a los proveedores de alojamiento que albergan los sitios web maliciosos identificados, solicitando la eliminación inmediata de los mismos, basándose en la información proporcionada por Comodo Secure DNS y cualquier evidencia que demuestre el uso indebido de la infraestructura del Cliente.

Realizar un análisis exhaustivo para determinar si los usuarios de la Organización han interactuado con estos dominios. Esto incluye la revisión de registros de acceso, así como la verificación de si se ha producido algún impacto en la seguridad de los sistemas internos.

Acciones directas:

- Contactar a los proveedores de hosting de los sitios identificados para solicitar la retirada de los contenidos maliciosos.
- Revisar los registros del firewall y proxy para identificar accesos desde la Organización a los dominios catalogados como maliciosos.
- Realizar un análisis de seguridad en los equipos que hayan accedido a los sitios maliciosos, buscando indicios de malware o brechas de seguridad.

8. Deficiencias en las configuraciones de seguridad

Descripción:

Se han identificado varias deficiencias en las configuraciones de seguridad de la aplicación web, que incluyen la falta de cabeceras de seguridad esenciales, un archivo robots.txt y la ausencia de un archivo security.txt. Estas deficiencias pueden exponer la aplicación a ataques y vulnerabilidades, así como dificultar la comunicación de seguridad.

Recomendaciones:

- Se recomienda implementar Cabeceras de Seguridad:
    - Strict-Transport-Security (HSTS) - CWE-693: Se recomienda habilitar la cabecera HSTS para obligar a los navegadores a utilizar conexiones HTTPS seguras. Esto previene ataques como el downgrade attack y garantiza que los usuarios siempre se conecten a través de HTTPS.
    - Referrer-Policy - CWE-693: Implementar una política de referencia adecuada que controle la información de referencia que se envía al navegar a otros sitios. Esto puede ayudar a proteger la privacidad de los usuarios.

  - Content-Security-Policy (CSP) - CWE-693: Establecer una política CSP que defina de manera clara qué recursos pueden ser cargados en la página. Esto ayuda a mitigar ataques de Cross-Site Scripting (XSS) y data injection.
  - X-Content-Type-Options - CWE-693: Habilitar esta cabecera con el valor nosniff para prevenir que los navegadores adivinen el tipo de contenido y ejecuten scripts maliciosos.
- Se recomienda revisar el contenido del archivo robots.txt para asegurarse de que no se permite el acceso a directorios o archivos sensibles. Es aconsejable que este archivo esté optimizado para evitar que los motores de búsqueda indexen recursos no deseados, como áreas de administración o datos confidenciales.
- Se recomienda la creación de un archivo security.txt en la raíz del dominio. Este archivo debe contener información sobre cómo los investigadores de seguridad pueden reportar vulnerabilidades, incluyendo detalles de contacto y políticas de respuesta a incidentes.

9. Software y tecnología de servidor encontrados

Descripción:
Un atacante podría utilizar esta información para montar ataques específicos contra el tipo de software y la versión identificados.

Recomendación:
Se recomienda eliminar la información que permite identificar plataforma de software, tecnología, servidor y sistema operativo: cabeceras del servidor HTTP, metainformación HTML, etc.