

ADRIÁN LÓPEZ FERNANDEZ

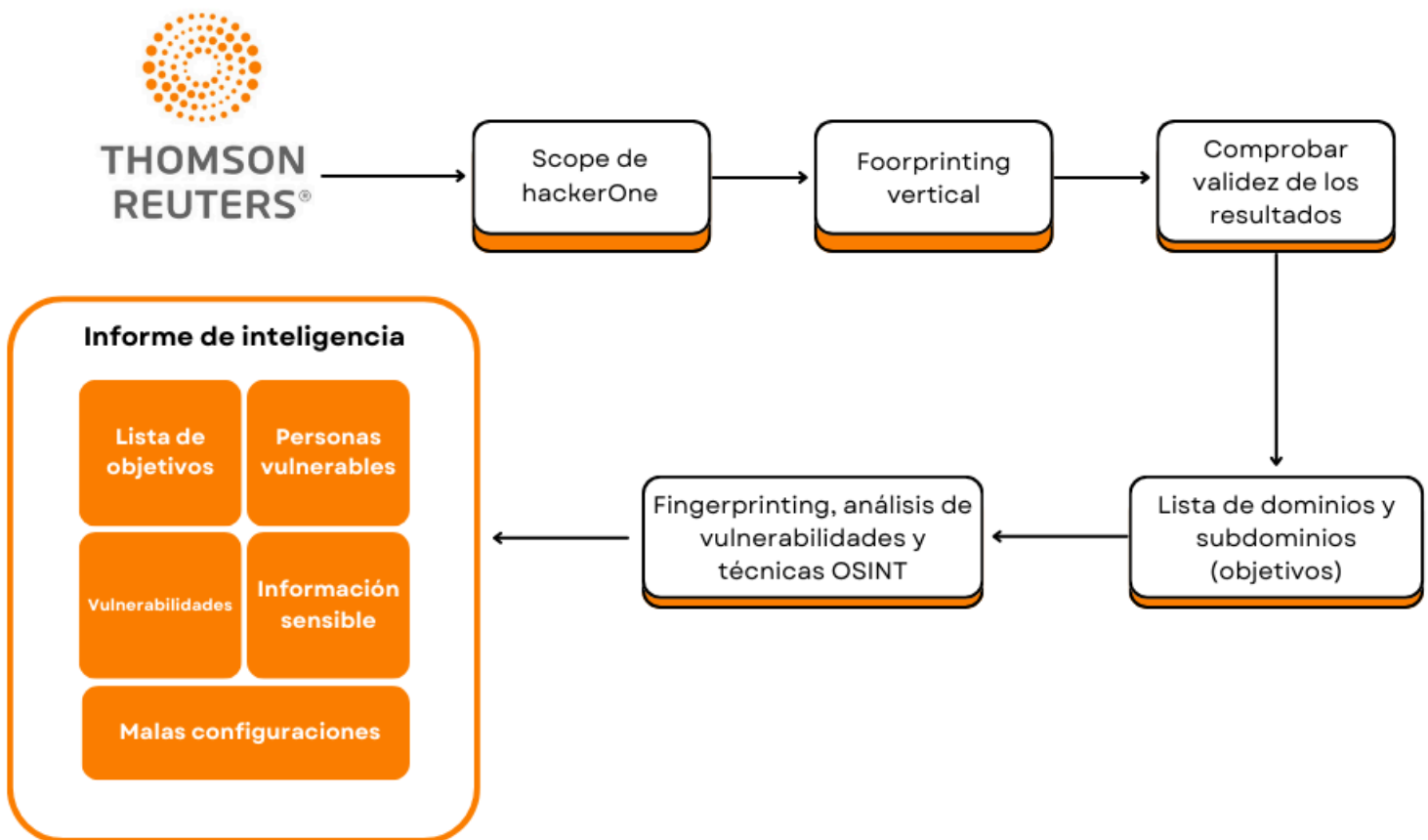
RECOPILACIÓN DE INFORMACIÓN

09 de marzo de 2025

ÍNDICE

DIAGRAMA DE FLUJO	3
SCOPE	4
FOOTPRINTING	5
DNS BRUTE FORCE	7
GOOGLE ANALYTICS	8
TLS PROBING	9
WEB SCRAPING	10
CERTIFICATE TRANSPARENCY LOGS	11
ARCHIVOS WEB/CACHÉ	12
CONCATENANDO PERMUTACIONES Y AGRUPANDO DOMINIOS	13
FINGERPRINTING	15
ESCANEANDO PUERTOS Y DETECTANDO SERVICIOS	15
IDENTIFICANDO TECNOLOGÍAS WEB	17
IDENTIFICANDO POSIBLES WAFS	20
DESCUBRIENDO CONTENIDO	21
ANÁLISIS DE VULNERABILIDADES	22
ANÁLISIS ESTÁNDAR	22
ANÁLISIS WEB	24
ANÁLISIS SSL/TLS	26
ANÁLISIS DE SERVIDORES DE CORREO	27
DETECCIÓN DE SUBDOMAIN TAKEOVER	28
OSINT	29
ENCONTRANDO CORREOS ELECTRÓNICOS Y USUARIOS	29
BÚSQUEDA DE METADATOS	31
REDES SOCIALES	32
CONCLUSIÓN	34

DIAGRAMA DE FLUJO



SCOPE

El presente informe documenta la fase de **Information Gathering** realizada sobre el dominio ***.thomsonreuters.com**, seleccionado dentro del programa de **Bug Bounty de Thomson Reuters en HackerOne**. Este dominio ha sido incluido en **scope**, permitiendo la exploración y análisis dentro de los límites establecidos por la compañía.

Para la recopilación de información se han empleado **técnicas avanzadas de reconocimiento**, incluyendo:

- **Footprinting vertical**: Identificación y enumeración de subdominios en scope.
- **Fingerprinting**: Análisis de tecnologías, frameworks y servicios utilizados por la infraestructura objetivo.
- **OSINT (Open Source Intelligence)**: Recolección de datos públicos sobre la empresa, empleados, posibles brechas de seguridad y correlación con información filtrada en bases de datos de terceros.

El objetivo principal de esta fase es obtener la **máxima cantidad de información posible** sobre los activos digitales de **Thomson Reuters**, identificando **vectores de ataque potenciales** y estableciendo una base sólida para futuras pruebas de seguridad.

[Download Burp Suite Project Configuration File](#) [Download CSV](#) [View changes](#) (Last updated on Septe

Asset name ↑	Type ↑	Coverage ↑	Max. severity ↓	Bounty ↑	Last update ↑	Resolved Reports ⓘ ↑
*.reuters.com	Wildcard	In scope	Critical	Ineligible	Sep 21, 2023	20 (3%)
*.thomsonreuters.com	Wildcard	In scope	Critical	Ineligible	May 15, 2023	592 (91%)

FOOTPRINTING

Se ha procedido a reunir datos sobre el objetivo antes de un posible ataque.

Para ello se ha comenzado consultando el **ASN de la empresa** y conocer los rangos de IPs que maneja, una vez encontrado el ASN se ha procedido a confirmar con una IP dentro del rango y la herramienta **Whois**, algo clave en esta etapa, utilizada para obtener **información sobre registros de dominios**, incluyendo **propietarios, direcciones IP o servidores DNS**.

Result	Type	
AS8802	ASN	Thomson Reuters (Professional) UK Ltd
AS7178	ASN	Thomson Reuters (Legal) Inc.
AS63521	ASN	Thomson Reuters - Hong Kong
AS5622	ASN	Thomson Reuters (Professional) UK Ltd
AS40319	ASN	Thomson Reuters U.S. LLC
AS399616	ASN	Thomson Reuters U.S. LLC
AS398934	ASN	Thomson Reuters U.S. LLC
AS398928	ASN	Thomson Reuters U.S. LLC
AS35528	ASN	Thomson Reuters (Professional) UK Ltd
AS32975	ASN	Thomson Reuters Holdings Inc
AS29506	ASN	Thomson Reuters (Professional) UK Ltd
AS27633	ASN	Thomson Reuters Holdings Inc
AS262335	ASN	THOMSON REUTERS BRASIL CONTEUDO E TECNOLOGIA LTDA
AS23109	ASN	Thomson Reuters U.S. LLC
AS21931	ASN	Thomson Reuters U.S. LLC
AS20480	ASN	Thomson Reuters U.S. LLC

[AS Info](#)
[Graph v4](#)
[Prefixes v4](#)
[Peers v4](#)
[Whois](#)
[RDAP](#)
[IRR](#)
[Traceroute](#)

Prefix	
155.46.211.0/24	<input checked="" type="checkbox"/> Thomson Reuters U.S. LLC

Showing 1-1 of 1

Otros ASN han quedado descartados por ser antiguos y no estar relacionados con la actividad principal y el país en el que tiene sede la empresa.

WHOIS Information for 155.46.211.20

```
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#

NetRange:      155.46.96.0 - 155.46.255.255
CIDR:          155.46.128.0/17, 155.46.96.0/19
NetName:       TLR-155-46-0-0-1
NetHandle:     NET-155-46-96-0-1
Parent:        NET155 (NET-155-0-0-0-0)
NetType:       Direct Allocation
OriginAS:
Organization:  Thomson Reuters U.S. LLC (TRU-11)
RegDate:       1994-08-26
Updated:       2022-08-10
Comment:       -----BEGIN CERTIFICATE-----
MIID7jCCAtYCCQDokKbIEaeQIjANBgkqhkiG9w0BAQsFADCBuDElMAkGA1UEBhMCVVMxEjAQBgNVBAgMCU1pbm5lc290YTEOMAwGA1UEBwwFRWFnYW4xJTJhBgNVBAoM
-----END CERTIFICATE-----
Ref:           https://rdap.arin.net/registry/ip/155.46.96.0

OrgName:       Thomson Reuters U.S. LLC
OrgId:         TRU-11
Address:       One Station Place
Address:       Metro Center
City:          Stamford
StateProv:     CT
PostalCode:    06902
Country:       US
RegDate:       2012-09-12
Updated:       2014-12-03
Ref:           https://rdap.arin.net/registry/entity/TRU-11
```

Ya en consola, se ha confirmado con el comando:

whois -h whois.radb.net -- '-i origin AS398934' | grep -Eo '([0-9.]{4}){4}/[0-9]+' | uniq

```
(kali㉿kali)-[~]
$ whois -h whois.radb.net -- '-i origin AS398934' | grep -Eo '([0-9.]{4}){4}/[0-9]+' | uniq
155.46.211.0/24
```

Se ha adjuntado el archivo *whois.txt* resultante junto con este informe.

Ahora sí, se procede a realizar un footprinting vertical mediante diferentes técnicas.

DNS BRUTE FORCE:

Se ha empezado intentando **averiguar el mayor número posible de subdominios** con un ataque de fuerza bruta de peticiones DNS y la herramienta **shuffledns**.

Para evitar saturar el servidor DNS local se le ha proporcionado una lista de servidores DNS diferentes que se han validado previamente con **dnsvalidator** y que shuffledns irá intercalando con las peticiones dns de la lista que se le proporciona.

Después de realizar el comando `shuffledns -mode bruteforce -d thomsonreuters.com -w $HOME/recopilacion/lists/domains.txt -r $HOME/reuters/resolvers.txt -silent > shuffledns.txt`

Ha encontrado los siguientes subdominios:

```

$ cat shuffledns.txt
auth.thomsonreuters.com
gl.thomsonreuters.com
app.thomsonreuters.com
www.thomsonreuters.com
innovation.thomsonreuters.com
legal.thomsonreuters.com
einstein.thomsonreuters.com
tracking.thomsonreuters.com
lms.thomsonreuters.com
newsletter.thomsonreuters.com
corporate.thomsonreuters.com
test.thomsonreuters.com
pr.thomsonreuters.com
redirect.thomsonreuters.com
store.thomsonreuters.com
maintenance.thomsonreuters.com
search.thomsonreuters.com
partner.thomsonreuters.com
jobs.thomsonreuters.com
es.thomsonreuters.com
partners.thomsonreuters.com
site.thomsonreuters.com
jp.thomsonreuters.com
cl.thomsonreuters.com
marketplace.thomsonreuters.com
cdp.thomsonreuters.com
sso.thomsonreuters.com
au.thomsonreuters.com
cs.thomsonreuters.com
www.cs.thomsonreuters.com
training.thomsonreuters.com
api.thomsonreuters.com
share.thomsonreuters.com
developer.thomsonreuters.com
developers.thomsonreuters.com
graphics.thomsonreuters.com
apple.thomsonreuters.com
hr.thomsonreuters.com
event.thomsonreuters.com
images.thomsonreuters.com

```

Se podrían destacar algunos subdominios interesantes como `auth.thomsonreuters.com` o `sso.thomsonreuters.com` **para realizar un inicio de sesión único**.

GOOGLE ANALYTICS:

Una vez hecho esto, se ha intentado la técnica para extraer subdominios **a través del ID de Google Analytics** del dominio principal, buscando que coincida en diferentes subdominios y así encontrar nuevos objetivos.

Para ello, se ha utilizado la herramienta **Analytics Relationships** y el comando *analyticsrelationships --url https://www.thomsonreuters.com/*

Desafortunadamente, parece que el objetivo no utiliza Google Analytics:

```
(kali@kali)~[~/reuters]
$ analyticsrelationships --url https://www.thomsonreuters.com/
/usr/bin/analyticsrelationships:34: SyntaxWarning: invalid escape sequence '\d'
pattern = "UA-\d+-\d+"
/usr/bin/analyticsrelationships:47: SyntaxWarning: invalid escape sequence '\.'
pattern = "(www\.googletagmanager\.com/ns\.html?id=[A-Z0-9\-\_]+)"
/usr/bin/analyticsrelationships:49: SyntaxWarning: invalid escape sequence '\d'
pattern3 = "UA-\d+-\d+"
/usr/bin/analyticsrelationships:78: SyntaxWarning: invalid escape sequence '\-'
pattern = "/relationships/[a-z0-9\-\_\.\_]+\.[a-z]+"

UA-ID
DOMAINS

> Get related domains / subdomains by looking at Google Analytics IDs
> Python version
> By @JosueEncinar

[+] Analyzing url: https://www.thomsonreuters.com/
[-] Tagmanager URL not found

(kali@kali)~[~/reuters]
$
```


TLS PROBING:

A continuación se ha intentado la técnica de TLS Probing para encontrar más subdominios a través del **certificado SSL/TLS**, que en ocasiones puede contener dominios o subdominios que pertenecen a la organización.

Para ello se ha utilizado la herramienta **Cero** con el siguiente comando:

```
cero -d thomsonreuters.com | grep 'thomsonreuters.com' > cero.txt
```

En este caso tampoco ha habido suerte ya que el certificado TLS solamente ha devuelto dominios de segundo nivel (SLD) y no subdominios, por lo que estaría fuera del Scope inicial.

```
(kali㉿kali)-[~/reuters]
$ cero -d thomsonreuters.com | grep 'thomsonreuters.com' > cero.txt

(kali㉿kali)-[~/reuters]
$ cat cero.txt
thomsonreuters.com
thomsonreuters.com.au
thomsonreuters.com.br
thomsonreuters.com.hk
thomsonreuters.com.my
thomsonreuters.com.pe
thomsonreuters.com.sg

(kali㉿kali)-[~/reuters]
$
```

WEB SCRAPING:

Después se ha pasado a la técnica de Web Scraping con la herramienta **Katana**, en la que se extrae información visitando el objetivo y **recopilando todos los enlaces y directorios**, para así **encontrar referencias** a otros subdominios en el código HTML de la web, en los enlaces internos o en **archivos de configuración públicos** como robots.txt o sitemap.xml

Para ello se ha utilizado el siguiente comando:

```
echo thomsonreuters.com | katana -jc -o katanaoutput.txt -kf robotstxt,sitemapxml
```

Una vez hecho esto se ha procedido a limpiar el fichero resultante con unfurl, borrando duplicados y dejando únicamente los subdominios únicos:

```
cat katanaoutput.txt | unfurl --unique domains > katana.txt
```

```
(kali@kali)-[~/reuters]
$ cat katana.txt
www.thomsonreuters.com
store.legal.thomsonreuters.com
tax.thomsonreuters.com
legal.thomsonreuters.com
jobs.thomsonreuters.com
cs.thomsonreuters.com
community.thomsonreuters.com
store.tax.thomsonreuters.com
developers.thomsonreuters.com
training.thomsonreuters.com
author-prod-ams.ewp.thomsonreuters.com
blogs.thomsonreuters.com
signon.thomsonreuters.com
onepass.thomsonreuters.com
legalprof.thomsonreuters.com
corporate.thomsonreuters.com
myaccount.thomsonreuters.com
checkpointaccount.tax.thomsonreuters.com
annual-report.thomsonreuters.com
event.thomsonreuters.com
info.legalsolutions.thomsonreuters.com
us.practicallaw.thomsonreuters.com
ir.thomsonreuters.com
onesourceuniversity.thomsonreuters.com
uk.practicallaw.thomsonreuters.com
checkpointlearning.thomsonreuters.com
innovation.thomsonreuters.com
legalsolutions.thomsonreuters.com
developerportal.thomsonreuters.com
africa.thomsonreuters.com
mena.thomsonreuters.com
thomsonreuters.com
financial.thomsonreuters.com
dmi.thomsonreuters.com
risk.thomsonreuters.com
mifidii.thomsonreuters.com
mypaysolutions.thomsonreuters.com
investors.thomsonreuters.com
```

CERTIFICATE TRANSPARENCY LOGS:

También se ha utilizado la técnica de Certificate Transparency Logs, cuando una empresa adquiere un certificado SSL/TLS para su dominio, este se registra en **Transparency Logs (CT Logs)**. Estos **registros son públicos** y permiten encontrar subdominios que han sido asegurados con HTTPS gracias a esta técnica.

Para encontrar subdominios a través de esta manera se ha utilizado la herramienta **CTFR** y el siguiente comando:

```
ctfr -d thomsonreuters.com > ctfrtodos.txt
```

Y después se ha limpiado el archivo resultante para eliminar duplicados y aislar subdominios con:

```
cat ctfrtodos.txt | unfurl --unique domains > ctfr.txt
```

```
(kali@kali)-[~/reuters]
$ cat ctfr.txt
rs.cp.thomsonreuters.com
thomsonreuters.com
imapop.qcmail.thomsonreuters.com
mmail.qcmail.thomsonreuters.com
OfficeWebQC.thomsonreuters.com
outlook.qcmail.thomsonreuters.com
webmail.qcmail.thomsonreuters.com
thesharecloud.thomsonreuters.com
*.thomsonreuters.com
sa-uk.practicallaw.thomsonreuters.com
a.uk.practicallaw.thomsonreuters.com
sa-au.practicallaw.thomsonreuters.com
a.concourse.thomsonreuters.com
a-ediscoverypoint.thomsonreuters.com
proview.thomsonreuters.com
sa-businessintelligence.thomsonreuters.com
sa-concourse.thomsonreuters.com
sa-dataprivacyadvisor.thomsonreuters.com
sa-drafting.thomsonreuters.com
sa-ediscoverypoint.thomsonreuters.com
sa-proview.thomsonreuters.com
sa-discoverysphere.thomsonreuters.com
ca-concourse.thomsonreuters.com
ia-concourse.thomsonreuters.com
ja-concourse.thomsonreuters.com
admin.researchinview.thomsonreuters.com
bath.researchinview.thomsonreuters.com
gatech.researchinview.thomsonreuters.com
huddersfield.researchinview.thomsonreuters.com
institution-a.researchinview.thomsonreuters.com
institution-b.researchinview.thomsonreuters.com
institution-c.researchinview.thomsonreuters.com
institution-d.researchinview.thomsonreuters.com
institution-e.researchinview.thomsonreuters.com
osu.researchinview.thomsonreuters.com
qub.researchinview.thomsonreuters.com
researchinview.thomsonreuters.com
```

ARCHIVOS WEB / CACHE:

También se ha probado una técnica de **footprinting vertical pasivo**, que recopila URLs de páginas como **Wayback Machine**, **URLScan** o **Common Crawl** y que han estado activas en algún momento de la vida del dominio que se está escaneando.

Para ello se ha utilizado la herramienta **GetAllUrls** y el siguiente comando:

```
gau --threads 5 thomsonreuters.com -o gauoutput.txt
```

Y una vez hecho esto, como de costumbre, se ha procedido a limpiar la lista resultante:

```
cat gauoutput.txt | unfurl --unique domains > gau.txt
```

```
(kali㉿kali)-[~/reuters]
$ cat gau.txt
thomsonreuters.com
montana.support.legalsolutions.thomsonreuters.com
5992.aws.thomsonreuters.com
www.thomsonreuters.com
secure.insights.thomsonreuters.com
regintel-content.thomsonreuters.com
images.productnotice.thomsonreuters.com
ppe.fingfx.thomsonreuters.com
accelus.thomsonreuters.com
training.thomsonreuters.com
store.tax.thomsonreuters.com
aig-learning.thomsonreuters.com
anzlaw.thomsonreuters.com
email.researchops.thomsonreuters.com
careers.thomsonreuters.com
sp-tracking-secure.thomsonreuters.com
images.thomsonreuters.com
livenotestream.thomsonreuters.com
legal.thomsonreuters.com
cs.thomsonreuters.com
content-5714791550287872.analytics.thomsonreuters.com
content-5721662265491456.analytics.thomsonreuters.com
content.pendo-cobalt.thomsonreuters.com
community.thomsonreuters.com
cocounsel.thomsonreuters.com
ewp.thomsonreuters.com
sp-tracking.thomsonreuters.com
hello.legal.thomsonreuters.com
dfsae.thomsonreuters.com
sftp.content.thomsonreuters.com
store.legal.thomsonreuters.com
legalsolutions.thomsonreuters.com
myaccount.thomsonreuters.com
answers.legalprof.thomsonreuters.com
ca.practicallaw.thomsonreuters.com
ontariocourts.casecenter.thomsonreuters.com
netdemo.legaltracker.thomsonreuters.com
```

CONCATENANDO PERMUTACIONES Y AGRUPANDO DOMINIOS:

Una vez recopilado el máximo de subdominios posible, se han concatenado todos los resultados y **se han generado permutaciones**.

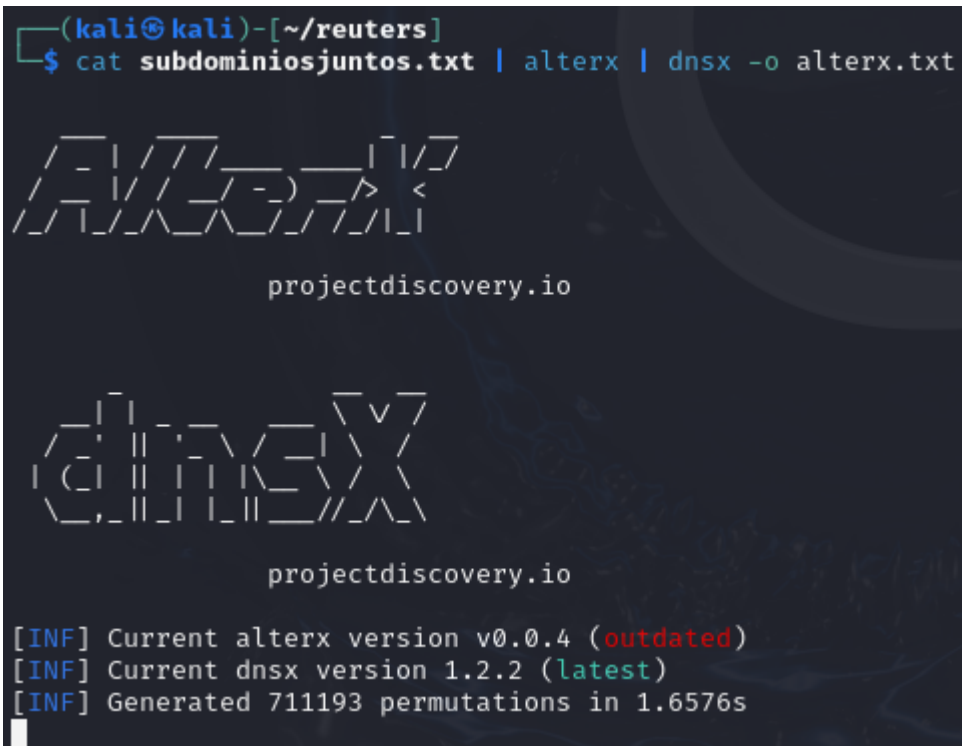
Para ello, **se han combinado los ficheros resultantes** de todas las técnicas anteriores en un único archivo:

```
cat cero.txt ctfr.txt gau.txt katana.txt shuffledns.txt > subdominiosjuntos.txt
```

Y después se utiliza **alterx** para generar las permutaciones junto con **dnsx** para comprobar que dicho subdominios son **válidos**:

alterx ha probado 711193 y dnsx encuentra 257 válidas.

```
(kali㉿kali)-[~/reuters]
$ cat subdominiosjuntos.txt | alterx | dnsx -o alterx.txt
```



```
projectdiscovery.io

projectdiscovery.io

[INF] Current alterx version v0.0.4 (outdated)
[INF] Current dnsx version 1.2.2 (latest)
[INF] Generated 711193 permutations in 1.6576s
```

```
242 www.abacus.thomsonreuters.com
243 www.cs.thomsonreuters.com
244 www.developers.thomsonreuters.com
245 www.lawschool.thomsonreuters.com
246 www.onesourceuniversity.thomsonreuters.com
247 www.roadmap.thomsonreuters.com
248 www.trainingtools.thomsonreuters.com
249 www.thomsonreuters.com.tr
250 www.thomsonreuters.com.hk
251 www.thomsonreuters.com.au
252 www.thomsonreuters.com.ar
253 www.thomsonreuters.com
254 www.thomsonreuters.com.pe
255 www.thomsonreuters.com.br
256 www.thomsonreuters.com.sg
257 www.thomsonreuters.com.my
258
```

Finalmente se ha generado un archivo que combina los subdominios encontrados con las técnicas anteriores junto a las permutaciones validadas.

Para filtrar todos los subdominios que se encuentran dentro del Scope que se pide, se ha procedido a usar el siguiente comando:

```
cat subdominiosfinal.txt dnsx.txt | grep -P '^[^\.]+\.(thomsonreuters\.com)$' >
subdominios_filtrados.txt
```

De esta manera se ha dejado en un archivo todos los subdominios *.thomsonreuters.com que entran en scope, eliminando la estructura *.*.thomsonreuters y *.thomsonreuters.com.* que quedan fuera de scope.

FINGERPRINTING

Normalmente se asocia a las técnicas de identificación de un objetivo. Se extrae información más concreta del objetivo: las tecnologías que utiliza en un sistema, sistema operativo, puertos abiertos...

ESCANEANDO PUERTOS Y DETECTANDO SERVICIOS:

Una vez realizado el footprinting vertical se ha continuado con el fingerprinting, usando la herramienta **HTTPX**, que se ha encargado de **determinar qué subdominios de la lista filtrada están vivos y son accesibles**, con el siguiente comando:

```
cat subdominios_filtrados.txt | httpx -silent > subdominios_vivos.txt
```

Teniendo la lista de subdominios válidos y que se encuentran online, se ha procedido a utilizar **masscan** y **nmap** para **escanear los puertos y servicios en dichos subdominios y así encontrar posibles vulnerabilidades**.

Para adaptar el archivo de subdominios_vivos.txt a nmap y eliminar los prefijos, se ha utilizado el comando:

```
cat subdominios_vivos.txt | unfurl --unique domains > subdominiosfinal.txt
```

Y para dicho archivo se han convertido los subdominios en IPs para utilizar en masscan y sacar los resultados a un archivo que se adjunta a este documento:

```
sudo masscan -p80,443,22,21,25,53 -iL subdominiosfinal_ips.txt -oL resultados.txt
```

Para así ya, realizar el escaneo de nmap al dominio principal:

```
sudo nmap -sS -Pn -sV -sC -O -vv --open --reason --min-hostgroup 16 --min-rate 100  
--max-parallelism=10 -F -iL subdominios_vivos.txt -oN nmap.txt
```

```

PORT      STATE SERVICE      REASON      VERSION
53/tcp    open  domain      syn-ack ttl 64  dnsmasq 2.78
| dns-nsid:
|_ bind.version: dnsmasq-2.78
80/tcp    open  http-proxy   syn-ack ttl 239 F5 BIG-IP load balancer http proxy
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: BigIP
|_ http-open-proxy: Potentially OPEN proxy.
|_ Methods supported: CONNECTION
|_ http-title: Did not follow redirect to http://www.thomsonreuters.com/
443/tcp   open  ssl/http-proxy syn-ack ttl 239 F5 BIG-IP load balancer http proxy
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS

```

Y se ha exportado a un archivo nmap.txt que se adjunta al github en el que se presenta este informe.

Algunos hallazgos destacables en los servicios:

dnsmasq 2.78 → Posibles vulnerabilidades de DNS spoofing.

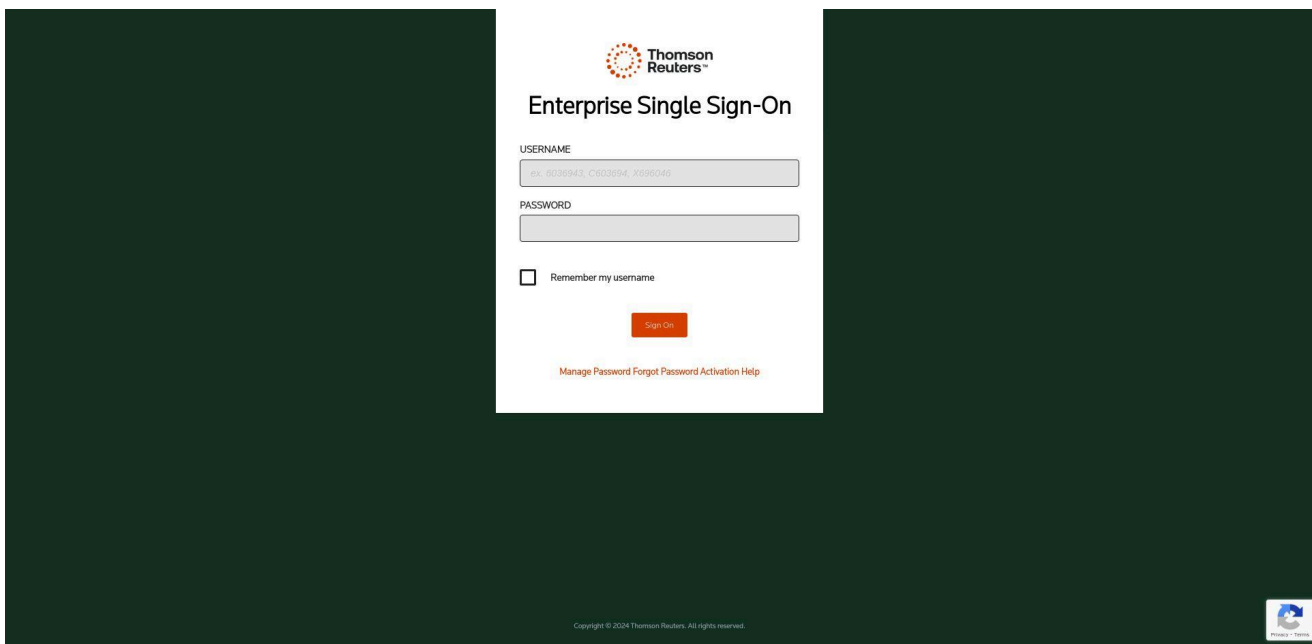
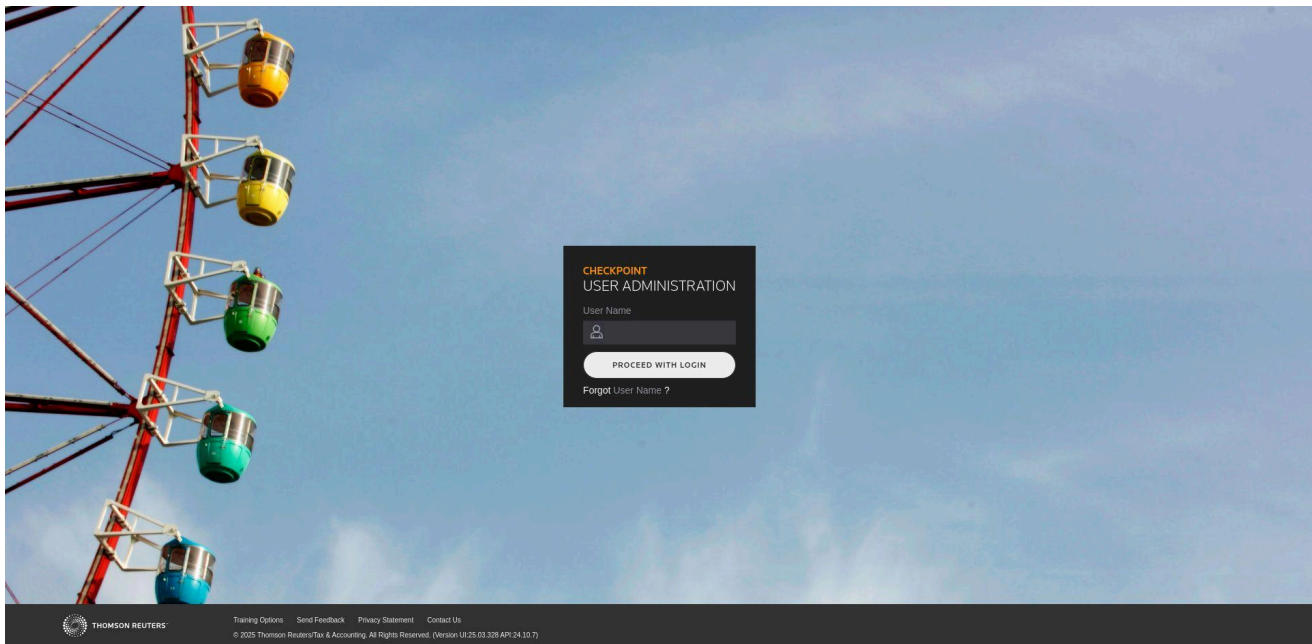
Microsoft HTTPAPI/IIS 10.0 → TRACE habilitado, posible riesgo XST.

Exposición de información en encabezados HTTP. (Server: Microsoft-IIS/10.0, X-Powered-By: ASP.NET)

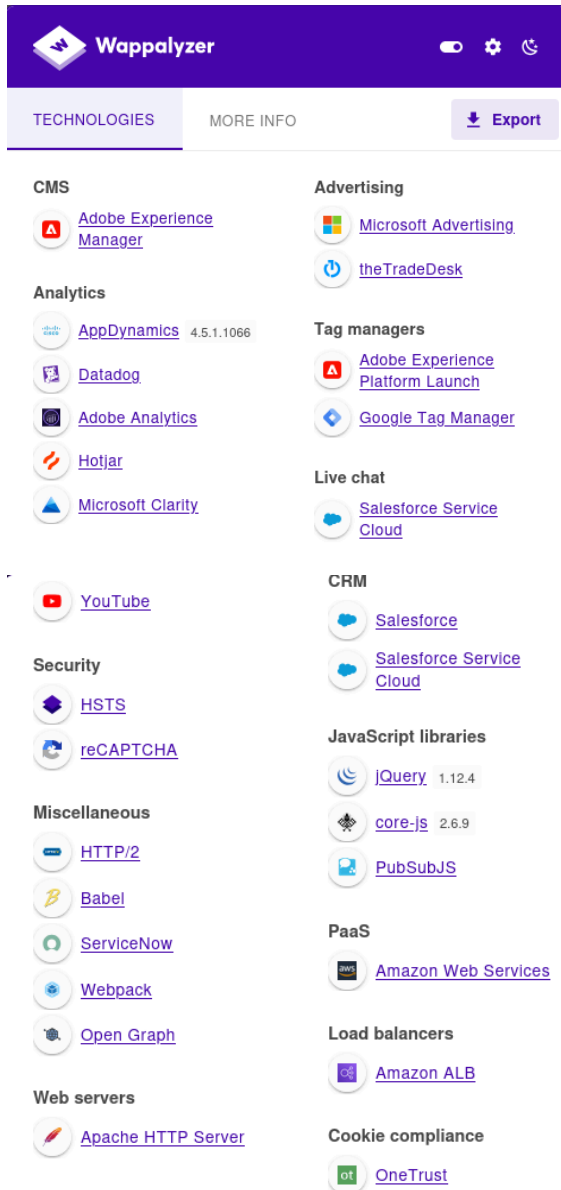
IDENTIFICANDO TECNOLOGÍAS WEB:

Una vez hecho esto se ha procedido a utilizar la herramienta **gowitness** para hacer **capturas de pantalla** de los sitios web, lo que facilita obtener una vista visual rápida de los sitios. Esto puede ser útil para identificar **tecnologías** y **características** visibles de las páginas web, como banners, frameworks, o **paneles de login en servicios internos o de administración**:





También se ha utilizado **Wappalyzer**, para detectar frameworks, servidores web, bibliotecas de JavaScript, lenguajes de programación...



Wappalyzer

TECHNOLOGIES MORE INFO Export

- CMS**
 - Adobe Experience Manager
- Advertising**
 - Microsoft Advertising
 - theTradeDesk
- Analytics**
 - AppDynamics 4.5.1.1066
 - Datadog
 - Adobe Analytics
 - Hotjar
 - Microsoft Clarity
- Tag managers**
 - Adobe Experience Platform Launch
 - Google Tag Manager
- Live chat**
 - Salesforce Service Cloud
- YouTube**
 - YouTube
- CRM**
 - Salesforce
 - Salesforce Service Cloud
- Security**
 - HSTS
 - reCAPTCHA
- JavaScript libraries**
 - jQuery 1.12.4
 - core-js 2.6.9
 - PubSubJS
- Miscellaneous**
 - HTTP/2
 - Babel
 - ServiceNow
 - Webpack
 - Open Graph
- PaaS**
 - Amazon Web Services
- Web servers**
 - Apache HTTP Server
- Load balancers**
 - Amazon ALB
- Cookie compliance**
 - OneTrust

En general, el sitio web de Thomson Reuters parece tener una infraestructura bastante robusta en cuanto a ciberseguridad. Está implementando prácticas como el uso de **HTTP/2**, **HSTS**, **AWS** para seguridad en la nube, y **reCAPTCHA** para protegerse contra ataques automatizados.

IDENTIFICANDO POSIBLES WAFs:

Para esta técnica de fingerprinting se ha utilizado **Wafwoof**, herramienta que permite identificar si los subdominios que se están escaneando están **protegidos por un firewall**, y focalizar a la hora de lanzar ataques.

Con el comando *wafw00f -i subdominiosfinal.txt* se ha establecido que **65 subdominios no tienen WAF que los proteja**.

Algunos subdominios sin WAF como onepass.thomsonreuters.com, passwordmanager.thomsonreuters.com o cs-user.thomsonreuters.com **podrían estar vinculados a servicios sensibles**.

Se adjunta el log de la herramienta junto a este informe.

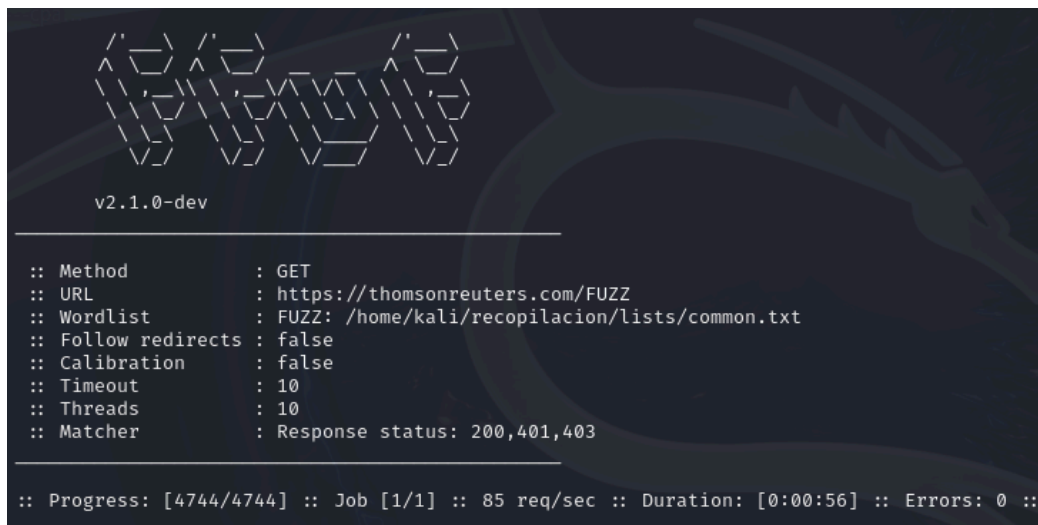
DESCUBRIENDO CONTENIDO:

Con esta técnica de **fuzzing** se ha realizado la búsqueda de directorios o ficheros a través de **diccionario**, que podrían proporcionar acceso a otros subdominios o información sensible.

A través de fuerza bruta con la herramienta **FFUF**, se han buscado **backups de bases de datos** en la web a través del comando:

```
ffuf -w ~/recopilacion/lists/common.txt -t 10 -mc 200,401,403 -u
https://thomsonreuters.com/FUZZ
```

La palabra fuzz en el comando permite elegir **dónde inyectar** las palabras elegidas en el diccionario.



```
v2.1.0-dev

:: Method      : GET
:: URL         : https://thomsonreuters.com/FUZZ
:: Wordlist     : FUZZ: /home/kali/recopilacion/lists/common.txt
:: Follow redirects : false
:: Calibration  : false
:: Timeout     : 10
:: Threads     : 10
:: Matcher     : Response status: 200,401,403

:: Progress: [4744/4744] :: Job [1/1] :: 85 req/sec :: Duration: [0:00:56] :: Errors: 0 ::
```

En este caso, después de ejecutar la herramienta **no se han detectado ficheros que puedan contener información sensible**.

ANÁLISIS DE VULNERABILIDADES

Una vez recopilada información del dominio y sus subdominios, se procede a realizar un análisis de posibles vulnerabilidades con diferentes técnicas:

ANÁLISIS ESTÁNDAR:

Para esta técnica se ha utilizado **Greenbone**, que es una herramienta utilizada para **detectar brechas de seguridad** en redes y sistemas. Ofrece **escaneos automatizados**, gestión de riesgos y una base de datos de vulnerabilidades actualizada.

Se ha procedido añadiendo la IP del dominio principal en el apartado de Assets y creando una nueva tarea para el escaneo.

New Target

Name Thomson Reuters

Comment

Hosts ☒ Manual thomsonreuters.com ☐ From file Browse... No file selected.

Exclude Hosts ☒ Manual ☐ From file Browse... No file selected.

Allow simultaneous scanning via multiple IPs ☒ Yes ☐ No

Port List All IANA assigned TCP ☐ *

Alive Test Scan Config Default ☐

Credentials for authenticated checks

SSH -- ☐ on port 22 ☐ *

SMB -- ☐ *

Cancel Save

En el reporte únicamente se ha encontrado una vulnerabilidad de severidad **Leve**:

TCP Timestamps Information Disclosure, el servidor de **thomsonreuters.com** implementa **marcas de tiempo TCP** (RFC1323/RFC7323), lo que permite a un atacante calcular el **uptime** del sistema y podría ayudar en ataques de fingerprinting, facilitando la identificación del sistema operativo y su estado.

<div>⏪ ⏩ 1 - 1 of 1 ⏪ ⏩</div>									
Status	Task	Severity	High	Medium	Low	Log	False Pos.	Actions	
Done	Thomson Reuters	2.6 (Low)	0	0	1	6	0	⚠️ ✕	
<div>Apply to page contents ▼ 📄 ✕</div>									
Vulnerability		🔧 Severity ▼	QoD	Host IP		Name		Location	
TCP Timestamps Information Disclosure		🔧 2.6 (Low)	80 %	155.46.172.255		thomsonreuters.com		general/tcp	

Summary

The remote host implements TCP timestamps and therefore allows to compute the uptime.

Detection Result

It was detected that the host implements RFC1323/RFC7323.

The following timestamps were retrieved with a delay of 1 seconds in-between:

Packet 1: 79562297

Packet 2: 79562404

Insight

The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Detection Method

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.

Details: [TCP Timestamps Information Disclosure OID: 1.3.6.1.4.1.25623.1.0.80091](#)

Version used: 2023-12-15T16:10:08Z

Affected Software/OS

TCP implementations that implement RFC1323/RFC7323.

Impact

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Una vez hecho esto, también se ha utilizado **Nuclei**, que permite realizar escaneos de vulnerabilidades con plantillas.

Se utiliza el comando **nuclei -u thomsonreuters.com** que genera un log que se adjunta junto con el informe.

Se pueden apreciar algunas potenciales vulnerabilidades leves, como la **Exposición del Tenant ID de Azure AD** en

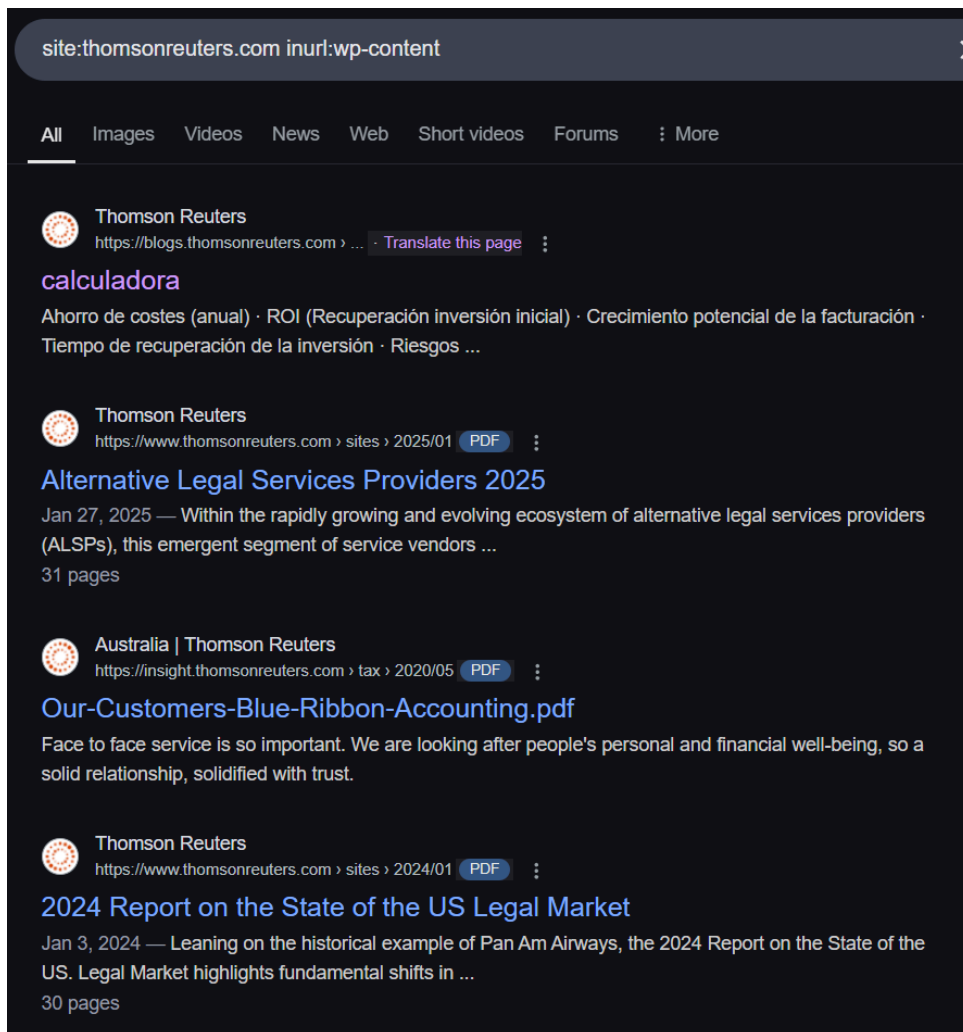
<https://login.microsoftonline.com:443/thomsonreuters.com/v2.0/.well-known/openid-configuration> que podría permitir ataques de enumeración de usuarios.

ANÁLISIS WEB:

Se ha realizado la siguiente búsqueda de google ([site:thomsonreuters.com inurl:wp-content](#)) para comprobar si el dominio objetivo tiene **subdominios que posean tecnología de Wordpress**.

La búsqueda devuelve algunos resultados, como por ejemplo

<https://blogs.thomsonreuters.com/wp-content/services/spain-calculator/>



También se ha usado la herramienta **WPScan** para comprobar si dicho subdominio posee **plugins que puedan ser potencialmente explotados**.

wpscan --random-user-agent --ignore-main-redirect --url https://blogs.thomsonreuters.com > wpscan.txt

Se adjunta el archivo txt con el log resultante, a priori se han encontrado algunos datos interesantes como:

- **XML-RPC Habilitado**, que permite ejecutar acciones remotas en WordPress. Si está mal configurado, puede ser explotado para **ataques de fuerza bruta** o **DDoS** mediante pingbacks.
- **Versión de WordPress desactualizada** (WordPress 6.6.2, lanzada en septiembre de 2024) y que podría tener vulnerabilidades explotables.

ANÁLISIS SSL/TLS:

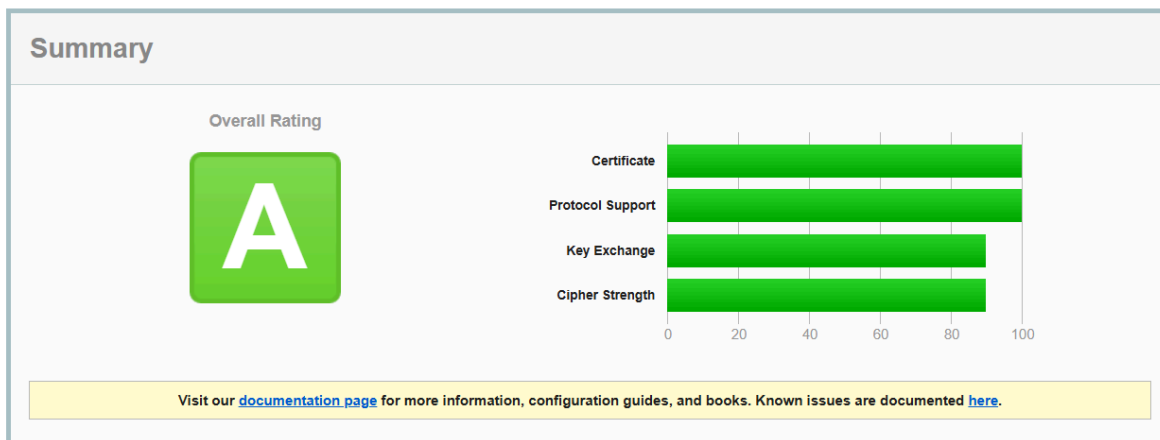
Con esta técnica se ha intentado encontrar si se usan **versiones obsoletas de TLS y SSL**, algoritmos de cifrado de claves obsoletos...

Para ello se ha utilizado una herramienta web **SSL Labs**, que otorga al dominio objetivo un rating de A y lo encuentra **segurizado** en términos generales.

SSL Report: thomsonreuters.com (155.46.172.255)

Assessed on: Sun, 09 Mar 2025 03:41:48 UTC | [Hide](#) | [Clear cache](#)

[Scan Another](#)



El único punto destacable sería la presencia de **algoritmos de cifrado débiles** en la versión de TLS 1.2, que podría permitir ataques **Man In The Middle** para atacantes que se encontrasen en la misma red local.

 **Cipher Suites**

# TLS 1.2 (suites in server-preferred order)				
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA)	FS		128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA)	FS		256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc0a8)	ECDH secp256r1 (eq. 3072 bits RSA)	FS		256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	WEAK	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	WEAK	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	WEAK	256

ANÁLISIS DE SERVIDORES DE CORREO:

En esta técnica se han intentado encontrar **configuraciones pobres** o inseguras en los mecanismos de seguridad **SPF**, **DKIM** y **DMARC** de los servidores de correo que permitan realizar **spoofing**.

El procedimiento se divide en dos partes: buscar vulnerabilidades en los registros DNS, e intentar enviar un correo malicioso.

Se ha utilizado la herramienta **spoofcheck**, con el siguiente comando: `python spoofcheck.py thomsonreuters.com`, de la que se ha recibido el siguiente resultado:

```
(kali@kali)-[~/spoofcheck]
$ python spoofcheck.py thomsonreuters.com
[*] Found SPF record:
[*] v=spf1 include:%{ir}%.%{v}%.%{d}.spf.has.pphosted.com ~all
[*] SPF record contains an All item: ~all
[*] Found DMARC record:
[*] v=DMARC1; p=reject; rua=mailto:dmarc_rua@emaildefense.proofpoint.com; ruf=mailto:dmarc_ruf@emaildefense.proofpoint.com
[-] DMARC policy set to reject
[*] Aggregate reports will be sent: mailto:dmarc_rua@emaildefense.proofpoint.com
[*] Forensics reports will be sent: mailto:dmarc_ruf@emaildefense.proofpoint.com
[-] Spoofing not possible for thomsonreuters.com
```

Con lo que se ha concluído que **el spoofing en este caso no sería posible**, ya que aunque el SPF está configurado con ~all (SoftFail) en lugar de -all (HardFail), lo que significa que aunque **los servidores no autorizados no deberían enviar correos en nombre del dominio**, los mensajes que no pasen la validación SPF **aún pueden ser entregados en la carpeta de spam** en algunos servidores de correo.

El DMARC está marcado como “reject”, lo que **impediría** que cualquier correo que no pase SPF o DKIM será rechazado directamente, evitando el spoofing.

DETECCIÓN DE SUBDOMAIN TAKEOVER:

Se ha utilizado esta técnica para comprobar si existen subdominios con registros **CNAME** que apuntan a servicios que ya **no están en uso** por la empresa objetivo, por lo que podrían ser **contratados por un atacante** y tomar el control del subdominio para publicar contenido malicioso o phishing.

Se ha utilizado la herramienta **Subzy** con el siguiente comando:

```
subzy run --targets ../reuters/subdominiosfinal.txt > subzy.txt
```

Generando un archivo de texto que se adjunta con este informe, y que revela que se detectaron **16 subdominios vulnerables** que apuntan a **Cargo Collective** y **UptimeRobot**, pero no tienen una instancia activa asociada, lo que permite que un atacante **reclame y controle** estos subdominios:

- app.thomsonreuters.com** → (Cargo Collective)
- corporate.thomsonreuters.com** → (Cargo Collective)
- gslink.thomsonreuters.com** → (Cargo Collective)
- gslink1.thomsonreuters.com** → (Cargo Collective)
- gslink2.thomsonreuters.com** → (Cargo Collective)
- hr.thomsonreuters.com** → (UptimeRobot)
- images.thomsonreuters.com** → (Cargo Collective)
- legalprof.thomsonreuters.com** → (Cargo Collective)
- legaltracker-highq.thomsonreuters.com** → (Cargo Collective)
- productnotice.thomsonreuters.com** → (Cargo Collective)
- risksolutions.thomsonreuters.com** → (Cargo Collective)
- sp-tracking.thomsonreuters.com** → (Cargo Collective)
- taxprof.thomsonreuters.com** → (Cargo Collective)
- tracking.thomsonreuters.com** → (Cargo Collective)
- trail.thomsonreuters.com** → (Cargo Collective)
- test.thomsonreuters.com** → (Cargo Collective)

OSINT

A través de técnicas de Open Source Intelligence es posible recopilar información pública sobre una empresa o sus empleados, como por ejemplo correos electrónicos, lo que podría permitir a atacantes realizar diversos tipos de ataques, por ejemplo, de phishing o de fuerza bruta.

ENCONTRANDO CORREOS ELECTRÓNICOS Y USUARIOS:

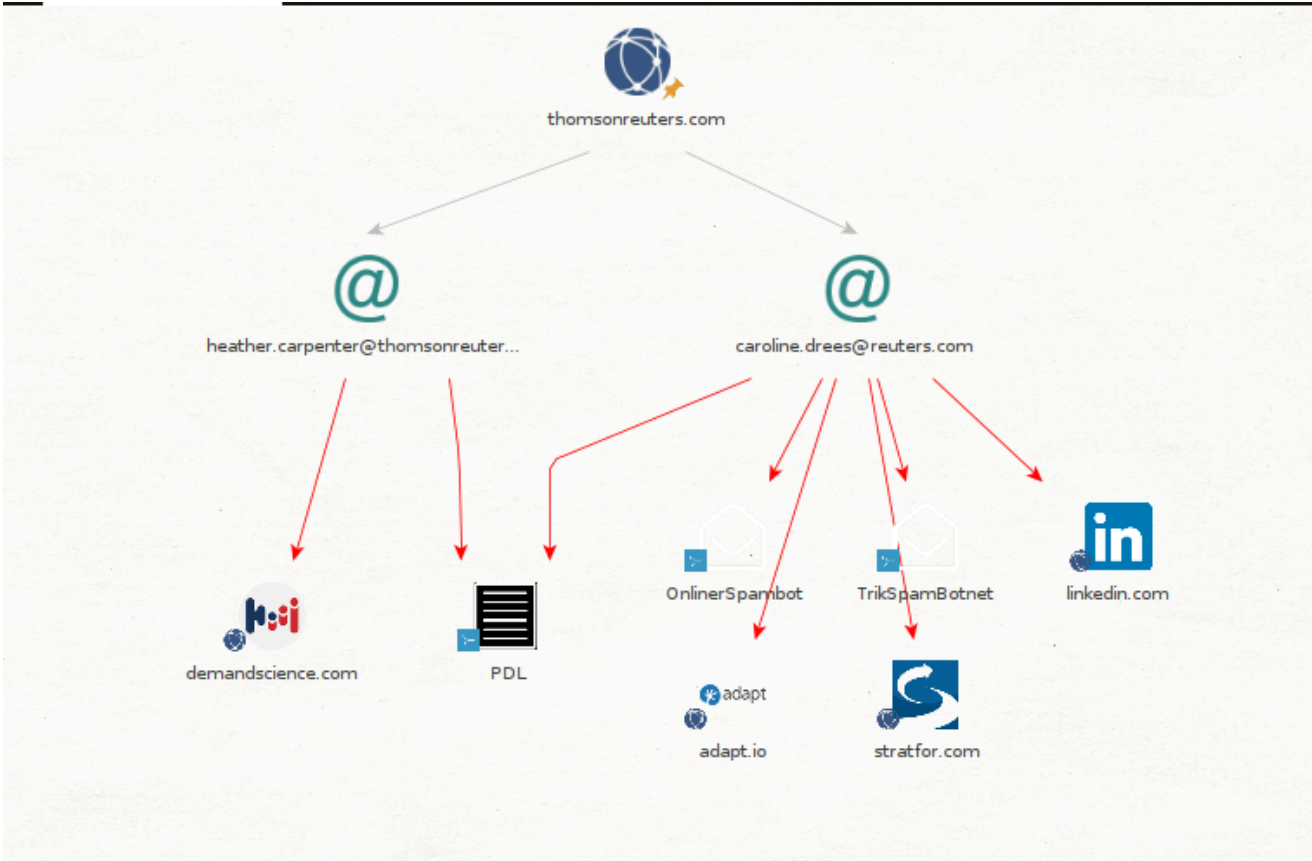
Utilizando **Maltego**, se ha ejecutado una **transformación de búsqueda** de direcciones de correo electrónico de empleados con éxito.

Dos correos de empleados destacan:

heather.carpenter@thomsonreuters.com

caroline.drees@reuters.com

Que además según la transformación de Haveibeenpwnd parecen **comprometidos en data breaches** de sitios como LinkedIn, demandscience, adapt.io, o stratfor, lo que podría permitir ataques de phishing o incluso un diccionario que pueda contener su contraseña filtrada.



También, a través de Spiderfoot se ha obtenido un **listado más amplio de direcciones de correo electrónico asociadas a la empresa**, el archivo se adjunta junto a este informe.

<input type="checkbox"/>	1750lisa.b.anderson@thomsonreuters.com	thomsonreuters.com	sfp_skymem
<input type="checkbox"/>	20olivia.rusu@thomsonreuters.com	thomsonreuters.com	sfp_skymem
<input type="checkbox"/>	22checkpointworldinfo@thomsonreuters.com	thomsonreuters.com	sfp_skymem
<input type="checkbox"/>	22jonathan.hilton@thomsonreuters.com	thomsonreuters.com	sfp_skymem

BÚSQUEDA DE METADATOS:

Se realiza a través de búsquedas en motores de búsqueda de ficheros que puedan contener **información útil en sus metadatos**.

Para ello se han realizado diversas búsquedas con site:thomsonreuters.com y probando diferentes tipos de archivo con [filetype: docx, xlsx, ppt...](#)

En este caso, a través de esta técnica se ha encontrado un documento docx interno genérico que no aporta ninguna información útil, pero al revisar los metadatos se ha obtenido un nuevo **nombre de un posible empleado** ([Mariana.Rene](#)) y el hash de una dirección de correo electrónico:

Mapa Completo de metadatos del archivo

Archivo: 1_AFN_AUT_Core_VER_16_03_15.docx	
Metadato	Valor
Application	Microsoft Office Word
ApplicationVersion	14.0000
Author	Mariana.Rene
Company	DIFC
CreationDate	2015-03-22T12:34:00Z
DocumentParts	Title 1
DocumentSecurity	0
EMAIL_OWNER_ADDRESS	sAAA2RgG6J6jCJ24kX+8L/RuC9exgbfkXIEYhjB8Kz6tPpQ=
Hyperlinks	false

REDES SOCIALES:

Se han utilizado técnicas de filtrado y búsqueda en redes sociales como LinkedIn para encontrar los **perfiles laborales de algunos de los empleados** cuyo correo había aparecido en las investigaciones anteriores, como por ejemplo Maltego o Spiderfoot.


En este caso se ha descubierto que el correo heather.carpenter@thomsonreuters.com redirige a la que es actualmente la **directora de comunicaciones** en Thomson Reuters, mientras que el correo caroline.drees@reuters.com pertenecía a una antigua empleada, que desempeñó el puesto de **Global Editor**.



Personas

1er

2º

3er y demás



Heather Carpenter  • 3er+
Senior Director, Communications, at Reuters
Long Beach, NY
 636 seguidores

Seguir

Ver todos los resultados de personas



Caroline Drees

Senior Director, Field Safety and Security at NPR

Washington, Distrito de Columbia, Estados Unidos · [Información de contacto](#)

Más de 500 contactos



Conectar

+ Seguir

Más



NPR



Yale University

Acerca de

Driven, experienced, multilingual manager and communicator with a track record of strong leadership in complex roles, difficult times and diverse regions. Strong budget, strategic, security, crisis, diversity and people management skills. German-U.S. dual national with bilingual native fluency.

Actividad

1.067 seguidores

Caroline Drees ha comentado en una publicación · 11 meses

I also fondly remember his disdain for "office ***** politics", and his quip that "if you've never been completely pissed, you've never learned to laugh at yourself."

[Mostrar todos los comentarios →](#)

Experiencia



Senior Director, Field Safety and Security, NPR

NPR · Jornada completa

nov. 2019 - actualidad · 5 años 5 meses

Washington, DC, United States



Reuters

11 años

- **Global Editor, Editorial Learning and Culture**

jun. 2017 - nov. 2019 · 2 años 6 meses


Washington D.C. Metro Area

As Global Editor, Editorial Learning and Culture, Caroline sets the agenda for the capabilities, skills development and training of our journalists. She is also in charge of diversity and inclusion at Reuters, from talent id ... ver más

- **Global Editor**

feb. 2016 - jun. 2017 · 1 año 5 meses

También se ha encontrado al **responsable de seguridad** actualmente en la empresa, que podría ser objetivo de ataques de **phishing** o **ingeniería social**:



Clyde Netto ✓ • 3er+
CISSP, MACS CP - Cyber Security | Director | CTSO | Governing Body Member - Melbourne CI...
Melbourne, VIC
Actual: Director (CTSO), Technology and Cyber Security - APAC, Middle East & Emerging Markets en Thomson Reuters - Playing the role of a CTO + **CISO**, provide strategic leadership and direction for the Technology...

[Conectar](#)

CONCLUSIÓN:

Entre los hallazgos más relevantes destacan:

- **Subdomain Takeover** en 16 subdominios, lo que permitiría a un atacante tomar control de ellos.
- **Exposición de información** en encabezados HTTP y servidores con configuraciones potencialmente explotables.
- **Correos electrónicos filtrados** de empleados en bases de datos comprometidas, lo que podría facilitar ataques de **phishing**.
- **Metadatos expuestos** en documentos públicos, revelando información sobre empleados.
- **Uso de TLS 1.2 con cifrados débiles**, lo que podría facilitar ataques Man-in-the-Middle en entornos específicos.

A pesar de contar con medidas de seguridad robustas, los hallazgos sugieren mejoras en la protección de subdominios, configuración de servidores y gestión de datos expuestos en la red.