

# Informe OSINT

## **LEDGER SAS**

Billetera fría para criptomonedas,

## Contenido

<b>FINALIDAD DEL DOCUMENTO .....</b>	<b>3</b>
<b>INFORMACION DEL OBJETO .....</b>	<b>3</b>
<b>INTRODUCCION .....</b>	<b>3</b>
<b>WEB DEL OBJETO .....</b>	<b>4</b>
<b>APARICION EN MEDIOS .....</b>	<b>4</b>
<b>INFORMACIONES GENERALES.....</b>	<b>5</b>
<b>REDES SOCIALES.....</b>	<b>5</b>
<b>INFORMACION ADMINISTRATIVA.....</b>	<b>6</b>
<b>INFORMACION FISCAL.....</b>	<b>6</b>
<b>DATOS ECONOMICOS .....</b>	<b>6</b>
<b>INFORMACION TECNICA .....</b>	<b>6</b>
<b>DIRECCIONES IP Y DOMINIO (INFORMACION SOBRE EL DOMINIO).....</b>	<b>6</b>
<b>SUBDOMINIOS.....</b>	<b>8</b>
<b>HOSTING.....</b>	<b>8</b>
<b>SERVIDOR.....</b>	<b>10</b>
<i>Tecnologías de alojamiento web.....</i>	<i>10</i>
<i>Servidor.....</i>	<i>13</i>
<i>Puertos.....</i>	<i>14</i>
<i>Vulnerabilidades y cabeceras de seguridad.....</i>	<i>16</i>
<b>INFORMACION CORPORATIVA.....</b>	<b>21</b>
<b>EQUIPO CORPORATIVO. ....</b>	<b>21</b>
<b>EMAILS CORPORATIVOS, EXTRAIDOS DE LA HERRAMIENTA SPIDERFOOT. ....</b>	<b>21</b>
<b>METADATOS .....</b>	<b>24</b>
<b>RECOMENDACIONES.....</b>	<b>33</b>

## FINALIDAD DEL DOCUMENTO

Este documento se crea con la finalidad de recopilar datos de forma no agresiva ya que no hay posibilidad de testear los equipos informáticos encontrados tanto física como remotamente en busca de posibles vulnerabilidades por lo que se procede a recabar datos en fuentes de información públicas a través de herramientas disponibles para este fin, el principal objetivo de este documento es dar una visión integral de la compañía y generar recomendaciones en base al análisis realizado. El objeto de búsqueda es la empresa LEDGER SAS, blockchain dedicado al resguardo de criptomonedas en billeteras frías a través de dispositivos sin necesidad de que estos estén conectados a la red.

## INFORMACION DEL OBJETO

### INTRODUCCION

Definida la finalidad de este documento, para esta primera fase del informe, se realiza un trabajo de busqueda y analisis de la empresa mediante tecnicas de OSINT ( Open Source Intelligence) similares a las que un atacante pudiera emplear para la recoleccion de informacion sensible que pudiera comprometer la seguridad de la empresa.

Cabe aclarar que los datos que se exponen en este documento se han obtenido netamente de motores publicos de busqueda, es decir, informacion presente y abierta al publico, pero estas han sido recabadas parcialmente en fuentes basicas de busqueda como ser, pagina web, google, redes sociales y firefox, y los datos mas especificos se recopilaron a traves herramientas profesionales que permiten un analisis mas profundo de ciertas areas que son importantes de analizar, como ser el de seguridad informatica y seguridad de la informacion. A continuacion listamos estas herramientas para referencia:

- WHOIS:
- SUBLIST3R:
- NMAP:
- PING
- PING
- DNSENUM
- THE HARVESTER
- SHODAN:
- METAGOOFIL
- BUILTWITH
- DNSDUMPSTER
- YANDEX
- OMNISCI
- SPIDERFOOT
- SHERLOCK
- MALTEGO
- IEE DATAPORT
- MITRE
- NIST

Este informe si bien no refleja de testeos ni ataques agresivos, permite divisar y hallar información sensible o vulnerabilidades superficiales.

El tipo de analisis empleado es semipasivo, teniendo en cuenta el descubrimiento de servidores y otros datos mas confidenciales como correos electronicos, se intentaron transferencias de datos a otros servidores, analisis de la web corporativa. Etc.

## WEB DEL OBJETO

LEDGER SAS, blockchain que comercializar dispositivos de almacenamiento de criptomonedas en billeteras frias posee una web corporativa en distintos idiomas.

<https://www.ledger.com/>

## APARICION EN MEDIOS

Estas son algunas de la apariciones de Ledger en los medios.

Las fuentes citadas a continuacion fueron recopiladas por la herramienta YANDEX: una fuente de busqueda en Rusia, y las demas fueron obtenidas de google.

<https://yandex.com/search/?text=ledger.com+news+&lr=20994>

Vulnerabilidad

<https://news.bitcoin.com/ledger-wallet-customer-data-leak-invokes-threats-phishing-scams-user-allegedly-loses-life-savings/>

Informaciones generales acerca de Ledger

<https://crypt-mining.net/news/proekty-ot-ledger>

Vulnerabilidad

<https://mining-cryptocurrency.ru/ledger-uyazvimost-kotoraya-mozhet-privesti-k-potere-btc/>

Perfil de la empresa

<https://www.bloomberg.com/profile/company/1238082D:FP>

Noticias destacadas

<https://www.ledger.com/in-the-news>

Noticias

<https://iota-news.com/ledger-price-increase-order-before-january-3rd-2022/>

Informacion de producto

<https://buybitcoinworldwide.com/wallets/ledger-nano-x/>

Noticias

<https://es.cointelegraph.com/news/nearly-12-000-eth-were-staked-through-ledger-live-in-just-14-days>

Noticias

<https://observatorioblockchain.com/web3/ledger-presenta-stax-el-smartphone-para-comercializar-valor-digital-en-la-web3/>

## INFORMACIONES GENERALES

La fuente es publica y se denomina

<https://www.societe.com/societe/ledger-529991119.html>

Fecha de creacion de la empresa: 01-01-2011

Forma juridica: Sociedad Anonima.

Nombre comercial: LEDGER.

Contacto: 08 90 10 93 04 y correo medial@edger.com

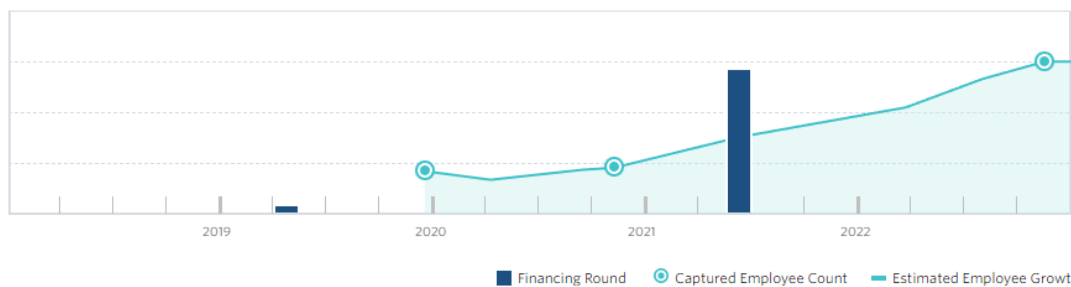
Direccion: 1 RUE DU MAIL 75002 PARÍS. FRANCIA

Actividad: Programacion informatica.

Sedes: París, Vierzon, Nueva York, Zúrich y Singapur.

Empleados: alrededor de 800 personas. Fuente: <https://pitchbook.com/>

### Ledger Timeline



Presidente: Pascal Gauthier.

## REDES SOCIALES

Los datos recopilados sobre redes sociales fueron obtenidos de herramientas variadas como: builtwith, sherlock y OMNISCI .

A continuacion se detallan las principales redes sociales de LEDGER, no obstante en un documento ANEXO se expone la totalidad.

Facebook: <https://www.facebook.com/LEDGER>

Fiverr: <https://www.fiverr.com/LEDGER>

Giphy: <https://giphy.com/LEDGER>

GitHub: <https://www.github.com/LEDGER>

GitLab: <https://gitlab.com/LEDGER>

Gitee: <https://gitee.com/LEDGER>

Instagram: <https://www.instagram.com/LEDGER>

Minecraft: <https://api.mojang.com/users/profiles/minecraft/LEDGER>

Myspace: <https://myspace.com/LEDGER>

Slack: <https://LEDGER.slack.com>

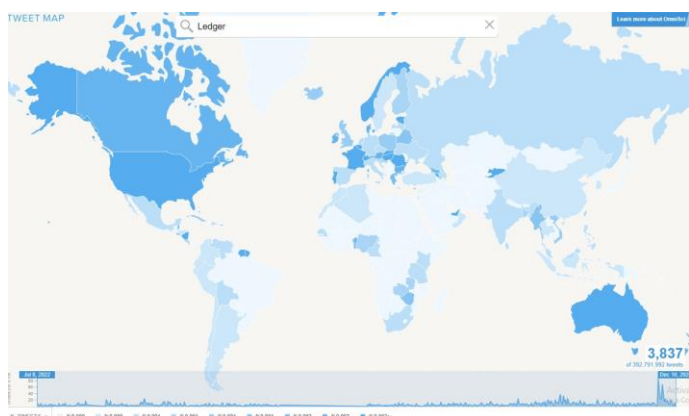
Telegram: <https://t.me/LEDGER>

Twitter: <https://twitter.com/LEDGER>

Youtube Channel: <https://www.youtube.com/c/LEDGER>

Linkedin: <https://www.linkedin.com/company/ledgerhq>

Se procede a analizar las publicaciones en una de las redes sociales que posee ledger, en este caso twitter y se puede divisar en el screen a continuacion el numero de publicaciones y de donde provienen geograficamente ,



## INFORMACION ADMINISTRATIVA

### INFORMACION FISCAL

Numero sirena: 529991119

Numero SIRET (fiscal): 52999111900056

Numero de valor agregado: FR03529991119

Numero RCS: París B 529 991 119

### DATOS ECONOMICOS

Capital social: 1.451.028 euros

Ultima oferta: \$ 100.000.000

Total de patentes: 17

Ventas: mas de \$ 400.000.000

## INFORMACION TECNICA

### DIRECCIONES IP Y DOMINIO (INFORMACION SOBRE EL DOMINIO)

Esta informacion fue obtenida a traves de la herramienta WHOIS en Kali Linux y corroborada con la herramienta dig y dnsenum y la plataforma DNSDUMPSTER.

En el screen de abajo se puede notar toda la informacion relacionada con el dominio, registro, empresa que registra el dominio, la localizacion geografica, el mail y telefonos de contacto en caso necesario, toda la

demas informacion ha sido redactada privadamente lo cual es bueno para no exponer informacion sensible.

#### Informacion de Dominio: herramienta WHOIS, kali linux

```
Domain Name: ledger.com
Registry Domain ID: 1225774_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.gandi.net
Registrar URL: http://www.gandi.net
Updated Date: 2022-08-18T01:10:19Z
Creation Date: 1994-09-19T02:00:00Z
Registrar Registration Expiration Date: 2023-09-18T04:00:00Z
Registrar: GANDI SAS
Registrar IANA ID: 81
Registrar Abuse Contact Email: abuse@support.gandi.net
Registrar Abuse Contact Phone: +33.170377661
Reseller: Ledger
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransfer
Domain Status:
Domain Status:
Domain Status:
Domain Status:
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Ledger
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Ile-de-France
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: FR
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext:
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext:
Registrant Email: 0b9c159f73485c46b8f2a7aa3b5574f2-7097036@contact.gandi.net
Registry Admin ID: REDACTED FOR PRIVACY
```

#### Informacion IP: herramienta dig, Kali linux

```
;; ANSWER SECTION:
www.ledger.com.      216      IN      A       104.18.35.20
www.ledger.com.      216      IN      A       172.64.152.236

;; AUTHORITY SECTION:
ledger.com.          81165    IN      NS      jessica.ns.cloudflare.com.
ledger.com.          81165    IN      NS      jason.ns.cloudflare.com.

;; ADDITIONAL SECTION:
jason.ns.cloudflare.com. 50566    IN      A       172.64.33.179
jason.ns.cloudflare.com. 50566    IN      A       173.245.59.179
jason.ns.cloudflare.com. 50566    IN      A       108.162.193.179
jason.ns.cloudflare.com. 50566    IN      AAAA    2a06:98c1:50::ac40:21b3
jason.ns.cloudflare.com. 50566    IN      AAAA    2606:4700:58::adf5:3bb3
jason.ns.cloudflare.com. 50566    IN      AAAA    2803:f800:50::6ca2:c1b3
jessica.ns.cloudflare.com. 18751    IN      A       173.245.58.171
jessica.ns.cloudflare.com. 18751    IN      A       108.162.192.171
jessica.ns.cloudflare.com. 18751    IN      A       172.64.32.171
jessica.ns.cloudflare.com. 18751    IN      AAAA    2606:4700:50::adf5:3aab
jessica.ns.cloudflare.com. 18751    IN      AAAA    2803:f800:50::6ca2:c0ab
jessica.ns.cloudflare.com. 18751    IN      AAAA    2a06:98c1:50::ac40:20ab

;; Query time: 16 msec
;; SERVER: 192.168.100.1#53(192.168.100.1) (UDP)
;; WHEN: Sat Dec 10 02:52:26 CET 2022
;; MSG SIZE rcvd: 395
```



Se hallaron dos IPS principales a traves de dig, en el punto 4.3 exponemos los hosts hallados, sus localizaciones e IPs.

## SUBDOMINIOS

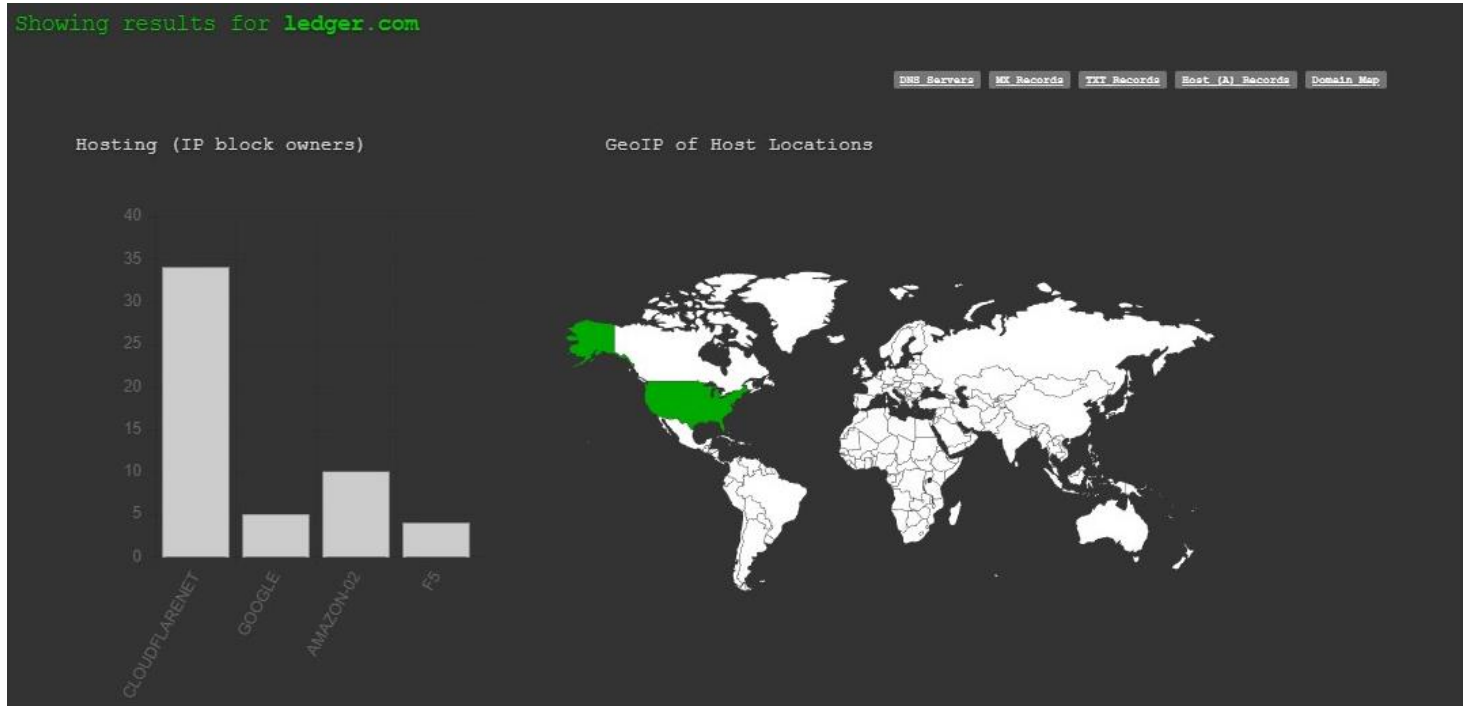
Los subdominios han sido obtenidos con la herramienta Sublist3r en KALI LINUX

En total se hallaron y fueron corroborados los 16 subdominios en el momento de realización de la búsqueda.

```
[~] Total Unique Subdomains Found: 16
www.ledger.com
affiliate.ledger.com
blog.ledger.com
developers.ledger.com
donjon.ledger.com
enterprise.ledger.com
get-connect.ledger.com
go.ledger.com
links.ledger.com
download.live.ledger.com
market.ledger.com
privacy-request.ledger.com
shop.ledger.com
speculos.ledger.com
status.ledger.com
support.ledger.com
```

## HOSTING

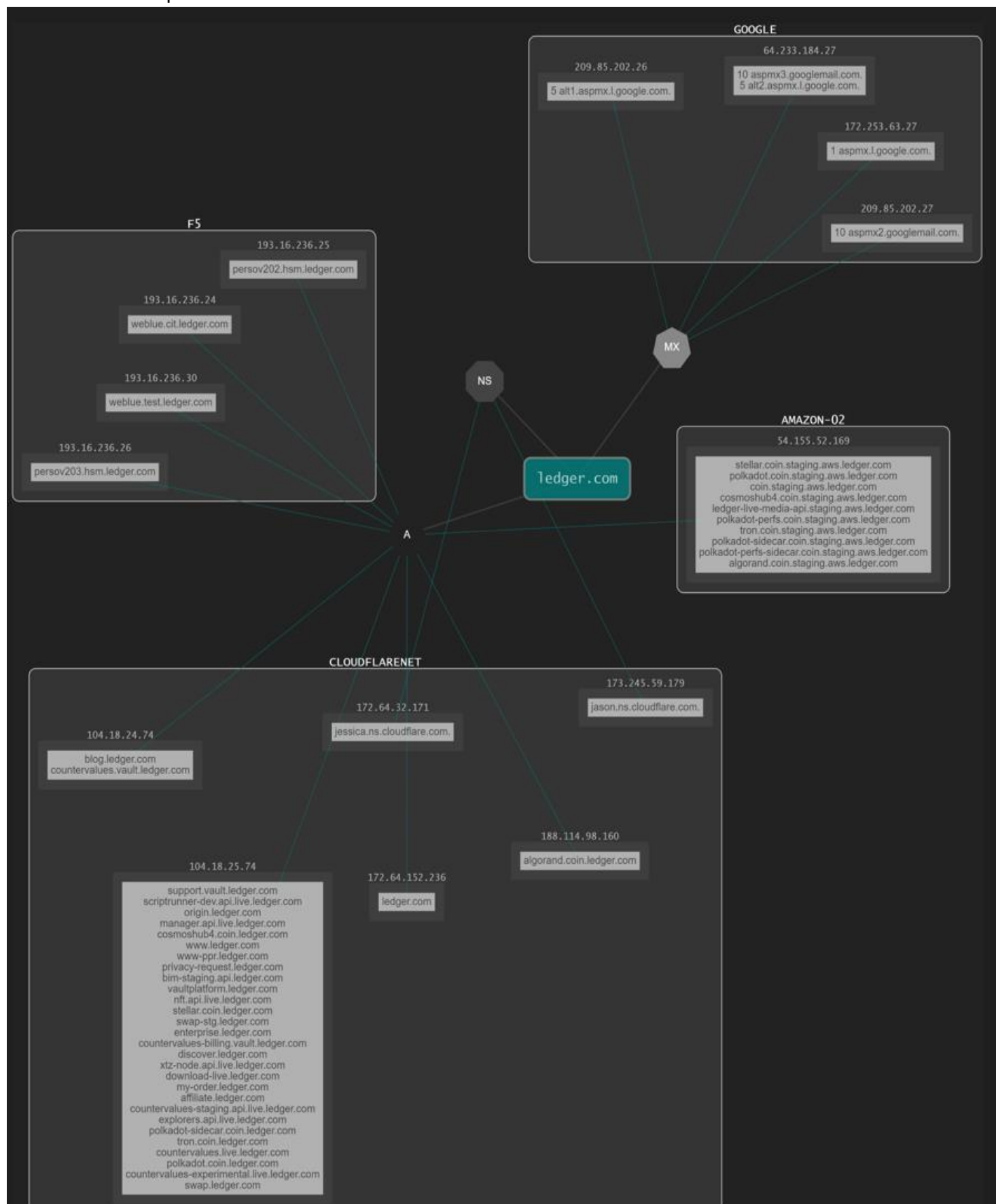
A continuacion se presenta el mapa de localizacion de los hosts y sus propietarios.





Se puede notar que según lo arrojado por la herramienta DNSDUMPSTER los propietarios de los hosts se encuentra en territorio Americano, específicamente Estados Unidos y Alaska y son CLOUDFLARE, GOOGLE, AMAZON Y F5, esto fue corroborado con otras herramientas.

Abajo se muestra un resumen de los hosts hallados por DNSDUMPSTER y corroborados con TheHarvester, otra herramienta que halla host relacionados con un dominio.



Observacion: para mayor referencia acerca de localización, ir al documento anexo.

## SERVIDOR

### *Tecnologias de alojamiento web*

La informacion acerca de tecnologia de alojamiento web utilizada por LEDGER fueron obtenidas a través de la herramienta Builtwith. A efectos de simplicidad solo se citaran algunos ítems MAS IMPORTANTES, para más información visitar la página de abajo donde se puede hallar las fechas de inicio y actualización además de mas información sobre las herramientas.

<https://builtwith.com/detailed/ledger.com>

- Analiticks and tracking
  - Google Optimize 360
  - Google analytics
  - Bing Universal Event Tracking
  - Reddit Conversion Tracking
  - Twitter Website Universal Tag
  - Hubspot
  - LinkedIn Insights
  - Google conversation tracking
  - Facebook pixel
  - Yahoo web analytics
  - Yaandex metrika
  - Salesforce audience studio
  - Comscore
  - Omniture sizecatalyst y otros
- Widgets
  - Onetrust
  - Octanom
  - Font awesome
  - Googl font api
  - Contact form
  - US privacy user signal mechanism
  - Centercode
  - Wordpress plugins
  - reCAPTCHA
  - cookie notice
  - drift
  - zopim
  - visual composer
  - wunderground y otros
- Languages

Para todos los lenguajes de utilizo HREF LANG

- Ecommerce

## Shopify

- Frameworks
  - Ruby on Rails Token
  - Bug Bounty
  - Facebook Domain Verification
  - Organization Schema
  - Schema
  - Ruby on Rails
  - PHP
  - Unicon
  - WordPress Theme
  - ASP.NET
  - Shockwave Flash Embed
- Content delivery network
  - Cloudflare
  - UNPKG
  - CDN JS
  - BootstrapCDN
  - jsDelivr
  - CloudFront
  - AJAX Libraries API
  - GStatic Google Static Content
  - Yahoo Image CDN
- Pagos
  - Paypal
  - Maestro
  - Mastercard
  - Visa
  - Euro
  - Entre otros
- Librería javascript
  - JQuery
  - handlebars
  - lightbox
  - corejs
  - intersection observer
  - web font loader
  - clipboard.js
  - google hosted web font loader y muchos mas
- web hosting providers
  - Cloudflare hosting
  - Amazon
  - Shopify hosted

- Linode
- Email hosted provided
- Zendesk
- MailJet
- SPF
- Google Apps for Business
- Apple iCloud Mail
- DMARC
- Name Server
- 10 to 14 ccTLD Redirects
- Cloudflare DNS
- Amazon Route 53
- 3 to 9 ccTLD Redirects
- SSL Certificates
- LetsEncrypt
- Cloudflare SSL
- SSL by Default
- Amazon SSL
- GlobalSign
- Comodo PositiveSSL
- Comodo SSL
- Web Servers
- Varnish
- nginx
- IIS 7
- IIS
- IPv6
- Live Writer Support
- RSS
- Atom
- Pingback Support
- Associated Press Hosted Content
- Document Encoding
- UTF-8
- Cloudflare CDN
- Google Webmaster
- MSN/Bing Webmaster
- Content Delivery Network

## Servidor

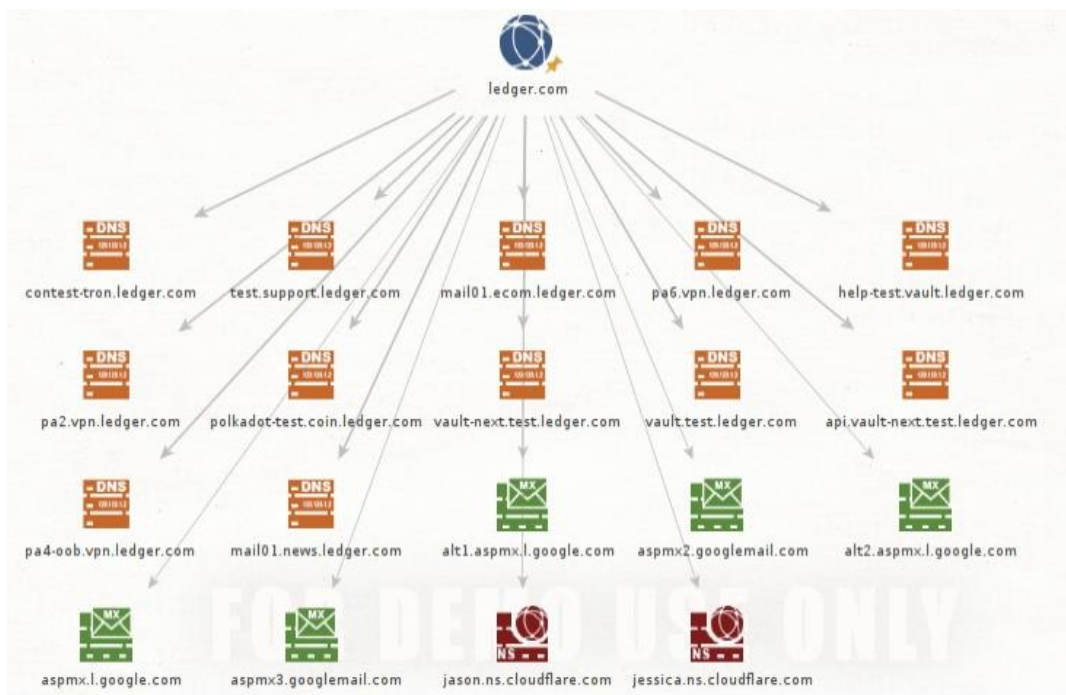
Se ha utilizado la herramienta o comando dnsenum a traves de kali linux para hallar los servidores relacionados con el dominio ledger.com

El resultado se expone a continuacion:

```
Host's addresses:
ledger.com. 104.18.25.74: icmp_seq=8 ttl=52 time=7.25 ms
ledger.com. 104.18.25.74: icmp_seq=9 ttl=52 time=6.11 ms
64 bytes from 104.18.25.74: icmp_seq=7 ttl=52 time=5.78 ms
ledger.com. 104.18.25.74: icmp_seq=8 ttl=52 time=7.25 ms
ledger.com. 104.18.25.74: icmp_seq=9 ttl=52 time=6.11 ms
64 bytes from 104.18.25.74: icmp_seq=10 ttl=52 time=5.36 ms
104.18.25.74: icmp_seq=11 ttl=52 time=5.81 ms
Wildcard test:
good
64 bytes from 104.18.25.74: icmp_seq=14 ttl=52 time=6.12 ms
64 bytes from 104.18.25.74: icmp_seq=15 ttl=52 time=3.94 ms
64 bytes from 104.18.25.74: icmp_seq=16 ttl=52 time=5.29 ms
Name Servers:
jason.ns.cloudflare.com. 148057 IN A 172.64.33.179
jason.ns.cloudflare.com. 148057 IN A 173.245.59.179
jason.ns.cloudflare.com. 148057 IN A 108.162.193.179
jessica.ns.cloudflare.com. 69649 IN A 172.64.32.171
jessica.ns.cloudflare.com. 69649 IN A 173.245.58.171
jessica.ns.cloudflare.com. 69649 IN A 108.162.192.171
64 bytes from 104.18.25.74: icmp_seq=20 ttl=52 time=8.12 ms
64 bytes from 104.18.25.74: icmp_seq=21 ttl=52 time=7.09 ms
Mail (MX) Servers:
aspmx.l.google.com. 241 IN A 64.233.186.27
aspmx2.googlemail.com. 242 IN A 64.233.184.26
aspmx3.googlemail.com. 242 IN A 142.250.27.27
alt1.aspmx.l.google.com. 241 IN A 64.233.184.26
alt2.aspmx.l.google.com. 241 IN A 142.250.27.26
64 bytes from 104.18.25.74: icmp_seq=26 ttl=52 time=5.29 ms
64 bytes from 104.18.25.74: icmp_seq=27 ttl=52 time=5.29 ms
```

Se hallaron varios servidores con los nombres de jessica y jason quienes asumimos controlan estos servidores, y adicionalmente nos arroja el mail de los servidores.

A parte de estos datos se intentaron hacer pruebas de transferencias o copias de datos de un servidor a otro, los cuales fallaron por lo que esto es positivo y no hay posibilidad de realizar este proceso, tambien probamos hacerlo por fuerza bruta y el resultado fue el mismo.



## Puertos

Se emplearon dos herramientas shodan y nmap en KALI LINUX para filtrar los puertos abiertos con las IPS halladas anteriormente y abajo exponemos los resultados.

Observacion: la variacion entre los puertos es debido a que fueron hechos en momentos diferentes.

## NMAP

```
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-10 02:45 CET
Nmap scan report for 104.18.25.74 / red_team
Host is up (0.037s latency).
Not shown: 989 filtered tcp ports (no-response)
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
119/tcp   open  nntp
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
8080/tcp   open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 117.61 seconds
```

```
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-10 19:05 CET
Nmap scan report for jason.ns.cloudflare.com (173.245.59.179)
Host is up (0.0064s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT      STATE SERVICE
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
119/tcp   open  nntp
143/tcp   open  imap
443/tcp   open  https
563/tcp   open  snews
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 86.06 seconds
```

## SHODAN

```
104.18.25.74
Hostnames:      navyarmyccurewards.com;sni.cloudflaressl.com
City:           San Francisco
Country:        United States
Organization:   Cloudflare, Inc.
Updated:        2022-12-10T04:51:56.757692
Number of open ports: 9

Ports:
  80/tcp
  443/tcp
    └─ SSL Versions: -SSLv2, -SSLv3, -TLSv1, -TLSv1.1, TLSv1.2, TLSv1.3
  2052/tcp
  2082/tcp
  2083/tcp
  2086/tcp
  2087/tcp
  8080/tcp CloudFlare
  8880/tcp
```

```
173.245.59.179
Hostnames:      jason.ns.cloudflare.com
City:           San Francisco
Country:        United States
Organization:   Cloudflare, Inc.
Updated:        2022-12-06T14:22:41.003690
Number of open ports: 5

Ports:
  53/tcp
  80/tcp CloudFlare
  443/tcp CloudFlare
  2082/tcp
  2086/tcp
```



Los puertos abiertos constantemente se pueden corroborar son el 80, puerto utilizado para la navegacion web en forma no segura, el 443 que es el puerto de navegaci3n web m1s seguro. y el 8080 un puerto que normalmente deberia estar abierto.

### *Vulnerabilidades y cabeceras de seguridad.*

Este documento compila datos de la empresa Ledger SAS, por lo que se ha realizado algunas pruebas superficiales con herramientas para probar su seguridad y en un segundo punto hemos investigado en fuentes abiertas publicas algunas de las vulnerabilidades y ataques que han sufrido.

### DNSENUM,

Esta herramienta permiti3 realizar una prueba de copia de datos de un servidor a otro, el cual fallo en una primera etapa, y luego se realiza este mismo ataque con fuerza bruta, este ultimo tambien fallo.

Referirse al screen a continuacion:

#### Trying Zone Transfers and getting Bind Versions:

```
Trying Zone Transfer for ledger.com on jason.ns.cloudflare.com ...  
AXFR record query failed: FORMERR
```

```
Trying Zone Transfer for ledger.com on jessica.ns.cloudflare.com ...  
AXFR record query failed: FORMERR
```

#### Brute forcing with /usr/share/dnsenum/dns.txt:

```
*.ledger.com A record query failed: NXDOMAIN  
1003.ledger.com A record query failed: NXDOMAIN  
1025.ledger.com A record query failed: NXDOMAIN  
1027.ledger.com A record query failed: NXDOMAIN  
1029.ledger.com A record query failed: NXDOMAIN  
1037.ledger.com A record query failed: NXDOMAIN  
1044.ledger.com A record query failed: NXDOMAIN  
1066.ledger.com A record query failed: NXDOMAIN  
1070.ledger.com A record query failed: NXDOMAIN  
1071.ledger.com A record query failed: NXDOMAIN  
1075.ledger.com A record query failed: NXDOMAIN  
1082.ledger.com A record query failed: NXDOMAIN  
1088.ledger.com A record query failed: NXDOMAIN  
11.ledger.com A record query failed: NXDOMAIN  
1106.ledger.com A record query failed: NXDOMAIN  
1107.ledger.com A record query failed: NXDOMAIN  
1108.ledger.com A record query failed: NXDOMAIN  
1114.ledger.com A record query failed: NXDOMAIN  
1115.ledger.com A record query failed: NXDOMAIN  
1116.ledger.com A record query failed: NXDOMAIN  
112sos.ledger.com A record query failed: NXDOMAIN  
1167.ledger.com A record query failed: NXDOMAIN
```

PING,

Se utiliza la herramienta ping en kali linux para el analisis de ataques a traves de la red y cuanto mayor es el tiempo de espera, puede indicar problemas de seguridad. Se realizo la prueba, y el tiempo de espera era largo por lo que se procede a realizar un analisis mas profundo de la red.

```
ping 104.18.25.74
PING 104.18.25.74 (104.18.25.74) 56(84) bytes of data.
64 bytes from 104.18.25.74: icmp_seq=1 ttl=52 time=5.07 ms
64 bytes from 104.18.25.74: icmp_seq=2 ttl=52 time=4.95 ms
64 bytes from 104.18.25.74: icmp_seq=3 ttl=52 time=4.75 ms
64 bytes from 104.18.25.74: icmp_seq=4 ttl=52 time=5.11 ms
64 bytes from 104.18.25.74: icmp_seq=5 ttl=52 time=7.25 ms
64 bytes from 104.18.25.74: icmp_seq=6 ttl=52 time=6.11 ms
64 bytes from 104.18.25.74: icmp_seq=7 ttl=52 time=5.78 ms
64 bytes from 104.18.25.74: icmp_seq=8 ttl=52 time=4.26 ms
64 bytes from 104.18.25.74: icmp_seq=9 ttl=52 time=6.24 ms
64 bytes from 104.18.25.74: icmp_seq=10 ttl=52 time=5.36 ms
64 bytes from 104.18.25.74: icmp_seq=11 ttl=52 time=5.81 ms
64 bytes from 104.18.25.74: icmp_seq=12 ttl=52 time=4.38 ms
64 bytes from 104.18.25.74: icmp_seq=13 ttl=52 time=4.69 ms
64 bytes from 104.18.25.74: icmp_seq=14 ttl=52 time=6.12 ms
64 bytes from 104.18.25.74: icmp_seq=15 ttl=52 time=3.94 ms
64 bytes from 104.18.25.74: icmp_seq=16 ttl=52 time=5.29 ms
64 bytes from 104.18.25.74: icmp_seq=17 ttl=52 time=6.67 ms
64 bytes from 104.18.25.74: icmp_seq=18 ttl=52 time=5.39 ms
64 bytes from 104.18.25.74: icmp_seq=19 ttl=52 time=4.53 ms
64 bytes from 104.18.25.74: icmp_seq=20 ttl=52 time=9.14 ms
64 bytes from 104.18.25.74: icmp_seq=21 ttl=52 time=11.6 ms
64 bytes from 104.18.25.74: icmp_seq=22 ttl=52 time=11.6 ms
64 bytes from 104.18.25.74: icmp_seq=23 ttl=52 time=10.9 ms
64 bytes from 104.18.25.74: icmp_seq=24 ttl=52 time=7.71 ms
64 bytes from 104.18.25.74: icmp_seq=25 ttl=52 time=9.44 ms
64 bytes from 104.18.25.74: icmp_seq=26 ttl=52 time=8.12 ms
64 bytes from 104.18.25.74: icmp_seq=27 ttl=52 time=9.69 ms
64 bytes from 104.18.25.74: icmp_seq=28 ttl=52 time=9.67 ms
64 bytes from 104.18.25.74: icmp_seq=29 ttl=52 time=6.30 ms
64 bytes from 104.18.25.74: icmp_seq=30 ttl=52 time=8.95 ms
64 bytes from 104.18.25.74: icmp_seq=31 ttl=52 time=11.3 ms
64 bytes from 104.18.25.74: icmp_seq=32 ttl=52 time=9.26 ms
```

Wpdoctor.es

Esta es una herramienta de analisis de red y cabeceras de seguridad de una pagina. Para mayor referencia sobre el analisis a continuacion ir a

































<https://www.wpdoctor.es/analisis/?url=https:%2F%2Fwww.ledger.com%2F#testSRV>


- En wordpress se dio una puntuacion de 52/100, esto debido a que no se detecto ningun plugging de cache, motivo por el cual la pagina no responde rapido, recordemos que este tiempo de respuesta por parte de la pagina es muy importante ya que aunque los dispositivos no requieren de conexión mientras almacenan las criptomonedas, si lo requieren cuando se realizan transacciones con estas.


 Detección de caché

- El servidor obtuvo 71/100, la velocidad de respuesta de la pagina es de 200 lo cual significa que la pagina carga correctamente, es decir no hay redirecciones ni problemas relacionados.

- También se detecto que la ip es de un país extranjero, esto ya lo vimos anteriormente, ya que si buscamos las ips halladas como servidor estas pertenecen a EEUU, abajo una constancia, fuente : DNSSUMPSTER.

DNS Servers		
jason.ns.cloudflare.com.      	173.245.59.179 jason.ns.cloudflare.com	CLOUDFLARENET United States
jessica.ns.cloudflare.com.      	108.162.192.171 jessica.ns.cloudflare.com	CLOUDFLARENET United States
MX Records ** This is where email for the domain goes...		
1 aspmx.l.google.com.    	142.250.31.26 bj-in-f26.1e100.net	GOOGLE United States
10 aspmx2.googlemail.com.    	209.85.202.27 dg-in-f27.1e100.net	GOOGLE United States
10 aspmx3.googlemail.com.    	64.233.184.26 wa-in-f26.1e100.net	GOOGLE United States
5 alt1.aspmx.l.google.com.    	209.85.202.26 dg-in-f26.1e100.net	GOOGLE United States
5 alt2.aspmx.l.google.com.    	64.233.184.26 wa-in-f26.1e100.net	GOOGLE United States

 País

 US






La IP del servidor es de un país extranjero.

En cuanto a uno de los puntos mas importantes en seguridad, califico a la pagina en 61/100, esto porque esta herramienta detecto que **El fichero wp-config.php es accesible desde el exterior**, lo cual permite la intromision de un atacante que pueda aprovecharse de esta vulnerabilidad.

 wp-config.php protegido


KO

También se detecto que se puede acceder al servidor con un USER-AGENT malicioso, lo cual hace vulnerable a ataques. Destacar que en muchas noticias se refirio que Ledger es vulnerable al tipo de ataque man in the middle.

	Cabecera Content-Security-Policy
	Cabecera X-Content-Type
	Cabecera X-Frame
	Cabecera XSS
	

Otras falencias detectadas fueron las carencias de cabeceras, las cuales deben implementarse y a parte de ellos deben configurarse correctamente o podrian dañar la web.

Por otro lado, la web posee certificacion SSL

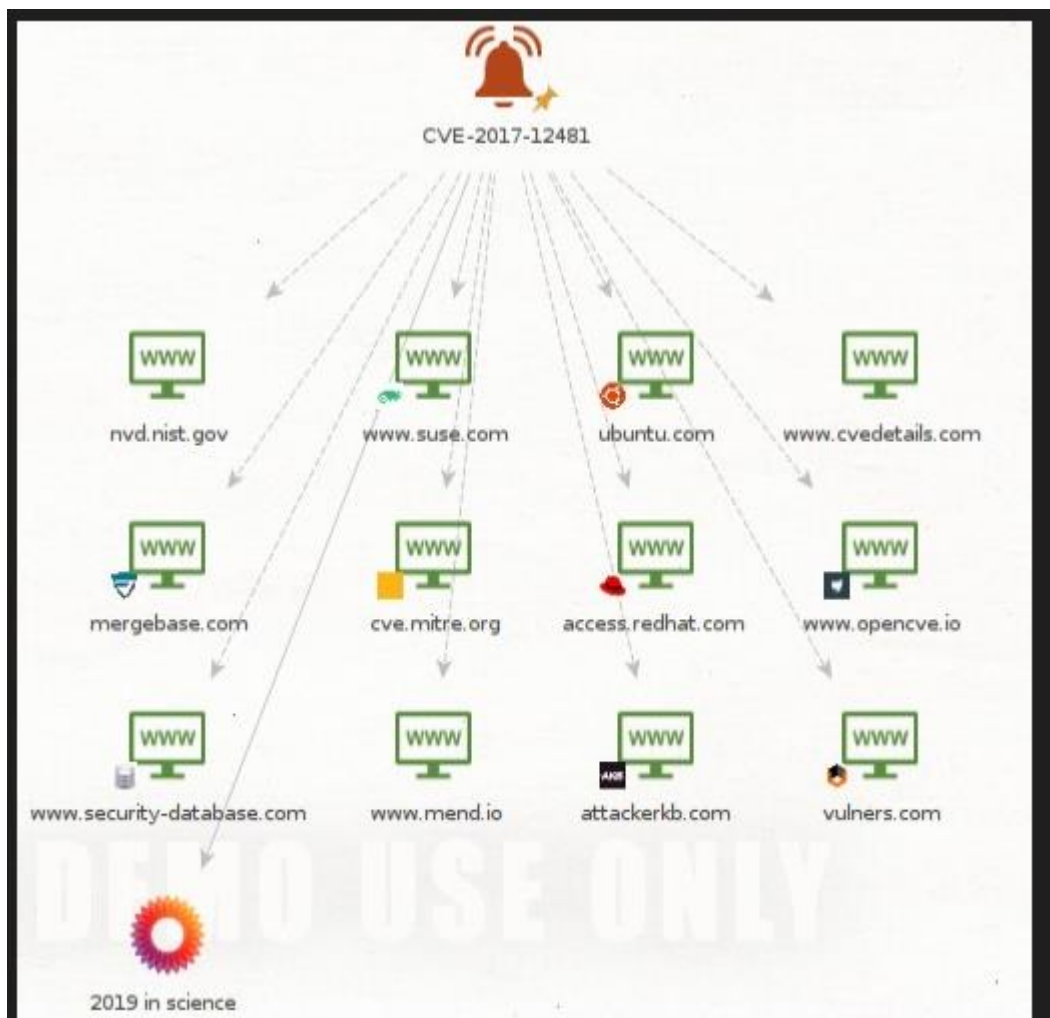
	<b>Certificado SSL</b>	Se ha detectado un certificado SSL instalado. Datos del certificado: Country=US , Organization=Cloudflare, Inc.,CommonName=Cloudflare, Inc., Subject=ledger.com <b>Expedido:</b> Jun 27 00:00:00 2022 GMT <b>Caduca:</b> Jun 26 23:59:59 2023 GMT
---	------------------------	---

Otras falencias descubiertas no tienen relacion con la seguridad informatica, sino mas bien con SEO o marketing, como que el google analytics no esta funcionando por ende es necesaria la verificacion ya que esta herramienta permite el conteo de visitantes, etc.

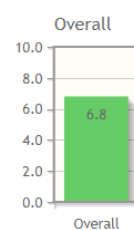
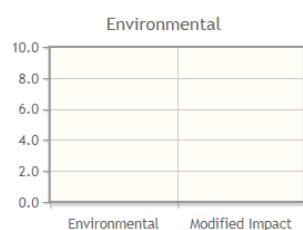
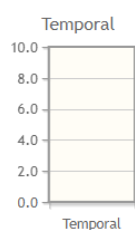
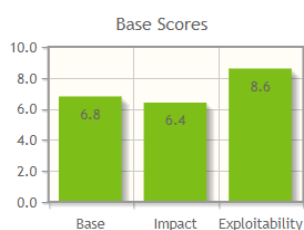
Se realizo una breve investigacion en google para conocer algunas vulnerabilidades detectadas y hallamos la 2017-12481. La función find\_option en option.cc en Ledger 3.1.1 permite a los atacantes remotos provocar una denegación de servicio (desbordamiento de búfer basado en la pila y bloqueo de la aplicación) o posiblemente tener otro impacto no especificado a través de un archivo manipulado.

Se realizo una busqueda en maltego para averiguar mas acerca de esta vulnerabilidad





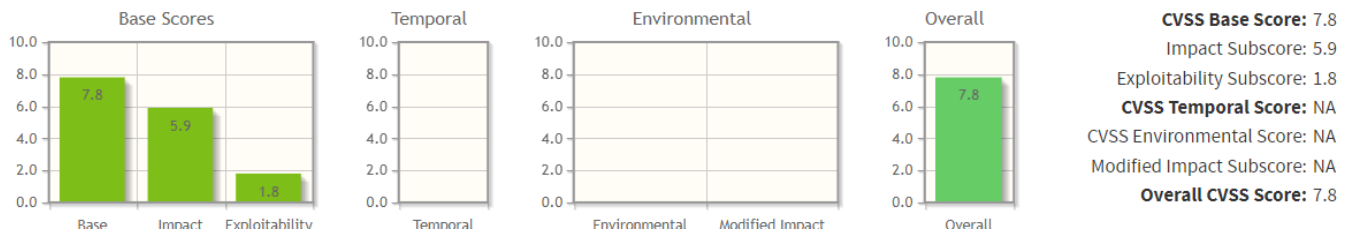
Se realiza la búsqueda en la primera de las opciones nvd.nist.gov y se descubre que esta vulnerabilidad posee dos versiones, la primera versión 2.0, la cual tiene un puntaje base de 6.8, esto porque si bien el atacante puede realizar el ataque a través de la red, el acceso es de complejidad media, pero no requiere autenticación para el ingreso, La confidencialidad, integridad y disponibilidad de la información están comprometidas parcialmente.



**CVSS Base Score: 6.8**  
 Impact Subscore: 6.4  
 Exploitability Subscore: 8.6  
**CVSS Temporal Score: NA**  
 CVSS Environmental Score: NA  
 Modified Impact Subscore: NA  
**Overall CVSS Score: 6.8**

La versión 3.x en cambio posee un puntaje de base más alto, de 7.8 puntos.

El ataque debe ser realizado localmente, la complejidad de acceso para el atacante es baja, no requiere privilegios para acceso, es decir no necesita autorización, pero requiere interacción con el usuario. Caso el atacante llegara a concretar su objetivo La confidencialidad, integridad y disponibilidad de la información se verían altamente comprometidas.



Una vez analizado esto, y hurgando un poco mas se encuentra el articulo de un investigador de criptodivisas descubrio una vulnerabilidad que permite el robo de bitcoins. El investigador señala que cuando un usuario se encuentra realizando operaciones con cualquier criptomoneda el atacante puede extraer bitcoins (moneda virtual). Según señala cuando un usuario realiza transacciones la clave publica como su funcionalidad para firmar estan expuestas por lo que se hace posible el robo de bitcoins, entonces el usuario se encuentra operando y sin darse cuenta sufre un robo.

## INFORMACION CORPORATIVA

### EQUIPO CORPORATIVO.

#### Equipo ejecutivo

- 1- **Presidente:** Pascal Gauthier
- 2- **CEO:** Eric Larcheveque
- 3- **Chief Financial Office :** Quentin Ricomard
- 4- **Chief Technology Officer & Chief Security office:** Charles Guillemet
- 5- **Chief Experience Office :** Ian Rogers
- 6- **Chief Information Security Officer:** Matt Johnson
- 7- **Global VP people:** Alexandre Blanc
- 8- **Head of ledger enterprise:** Alex Zinder
- 9- **General counser:** Antoine Tibault

#### Miembros de equipo contable

Nombre, representación, role

Name	Representing	Role
<a href="#">Cyril Bertrand</a>	<a href="#">XAnge</a>	Board Member
<a href="#">Dan Tapiero</a>	<a href="#">10T Holdings</a>	Board Member
Eric Larchevêque	Self	Co-Founder & Board Member
<a href="#">Fleur Pellerin</a>	<a href="#">Korelya Capital</a>	Board Member
Frederic Potter	<a href="#">Ledger</a>	Board Member

### EMAILS CORPORATIVOS, EXTRAIDOS DE LA HERRAMIENTA SPIDERFOOT.

Source	Data
ledger.com	aalexander@ledger.com

ledger.com	aalexander@ledger.com
ledger.com	agaquin@ledger.com
ledger.com	ajbauer@ledger.com
ledger.com	amackinnon@ledger.com
ledger.com	anestis@ledger.com
ledger.com	anestis@ledger.com
ledger.com	ariglian@ledger.com
ledger.com	aswanson@ledger.com
ledger.com	avaccaro@ledger.com
ledger.com	bfish@ledger.com
ledger.com	biznews@ledger.com
ledger.com	biznews@ledger.com
ledger.com	cburrell@ledger.com
ledger.com	cdowaliby@ledger.com
ledger.com	chazy@ledger.com
ledger.com	classads@ledger.com
ledger.com	cmaclean@ledger.com
ledger.com	cschiavone@ledger.com
ledger.com	dbarbuto@ledger.com
ledger.com	dbarbuto@ledger.com
ledger.com	dbraga@ledger.com
ledger.com	delivery@ledger.com
ledger.com	dtatz@ledger.com
ledger.com	dtatz@ledger.com
ledger.com	editpage@ledger.com
ledger.com	editpage@ledger.com
ledger.com	emchugh@ledger.com
ledger.com	ewilliams@ledger.com
ledger.com	features@ledger.com
ledger.com	fhanson@ledger.com
ledger.com	fhanson@ledger.com
ledger.com	gbotelho@ledger.com
ledger.com	glotan@ledger.com
www.ledger.com	info@www.ledger.com
ledger.com	iplatonova@ledger.com
ledger.com	jacksullivan@ledger.com
ledger.com	jbeare@ledger.com
ledger.com	jbrosseau@ledger.com
ledger.com	jchesto@ledger.com
ledger.com	jencarnacao@ledger.com
ledger.com	jfeinberg@ledger.com
ledger.com	jfeinberg@ledger.com
ledger.com	jfurbush@ledger.com
ledger.com	jjette@ledger.com
ledger.com	jmann@ledger.com
ledger.com	jorourke@ledger.com
ledger.com	jravitz@ledger.com
ledger.com	jwagner@ledger.com
ledger.com	jzaremba@ledger.com

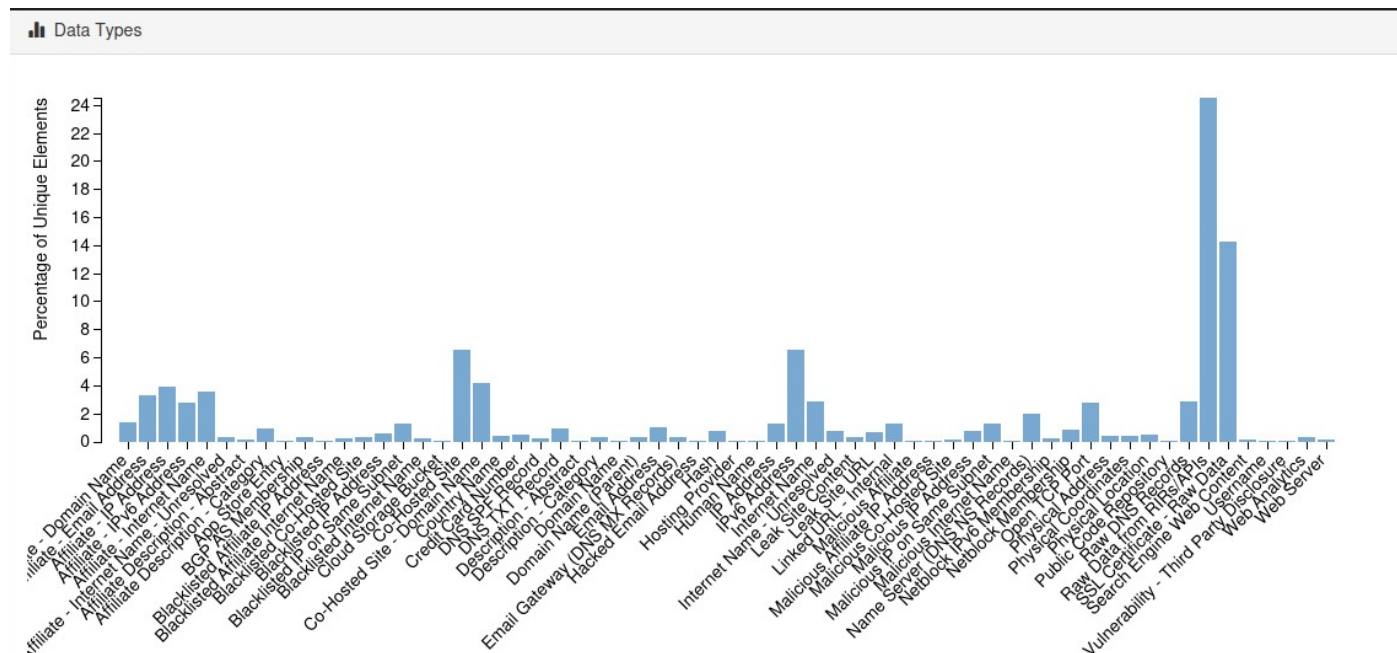
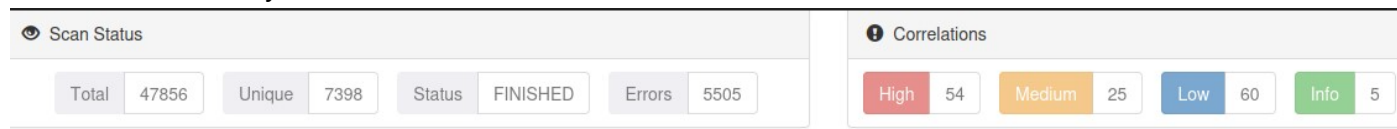


ledger.com	kenjohnson@ledger.com	
ledger.com	keschbacher@ledger.com	
ledger.com	kgoulart@ledger.com	
ledger.com	kjohnson@ledger.com	
ledger.com	ksutton@ledger.com	
ledger.com	lcampenella@ledger.com	
ledger.com	lditullio@ledger.com	
ledger.com	llambert@ledger.com	
ledger.com	llambert@ledger.com	
ledger.com	lshepherd@ledger.com	
ledger.com	lshepherd@ledger.com	
ledger.com	mikefine@ledger.com	
ledger.com	mloftus@ledger.com	
ledger.com	mloftus@ledger.com	
ledger.com	mtorpey@ledger.com	
ledger.com	mtorpey@ledger.com	
ledger.com	nesimpson@ledger.com	
ledger.com	newsroom@ledger.com	
ledger.com	nhoffman@ledger.com	
ledger.com	nornell@ledger.com	
ledger.com	nreardon@ledger.com	
ledger.com	nreardon@ledger.com	
ledger.com	obits@ledger.com	
ledger.com	pfelcis@ledger.com	
ledger.com	pronan@ledger.com	
ledger.com	rseto@ledger.com	
ledger.com	rseto@ledger.com	
ledger.com	sadams@ledger.com	
ledger.com	scheible@ledger.com	
ledger.com	scoffey@ledger.com	
ledger.com	sfedlizyn@ledger.com	
ledger.com	side@ledger.com	
ledger.com	sneo@ledger.com	
ledger.com	sports@ledger.com	
ledger.com	sreinert@ledger.com	
ledger.com	sscheible@ledger.com	
ledger.com	sschwartz@ledger.com	
ledger.com	sschwartz@ledger.com	hackeado
ledger.com	tbenner@ledger.com	
ledger.com	trace@ledger.com	
ledger.com	twenners@ledger.com	

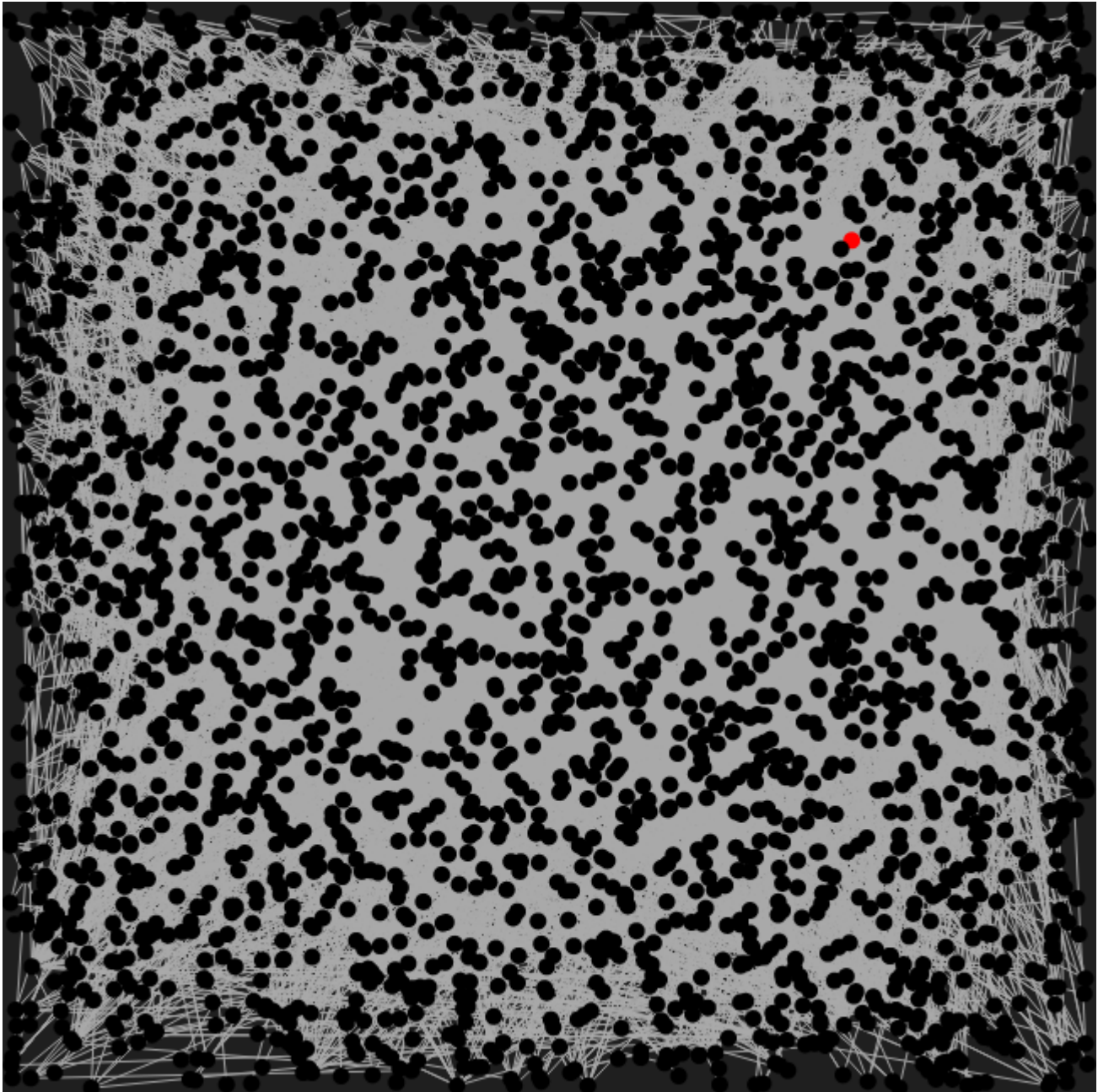
## METADATOS

Todos los datos expuestos a continuacion fueron generados por la herramienta spiderfoot, el cual escanea integralmente un objeto a traves de su dominio y lo hallado lo exponemos graficamente para su vision mas simple.

## Datos encontrados y analizados

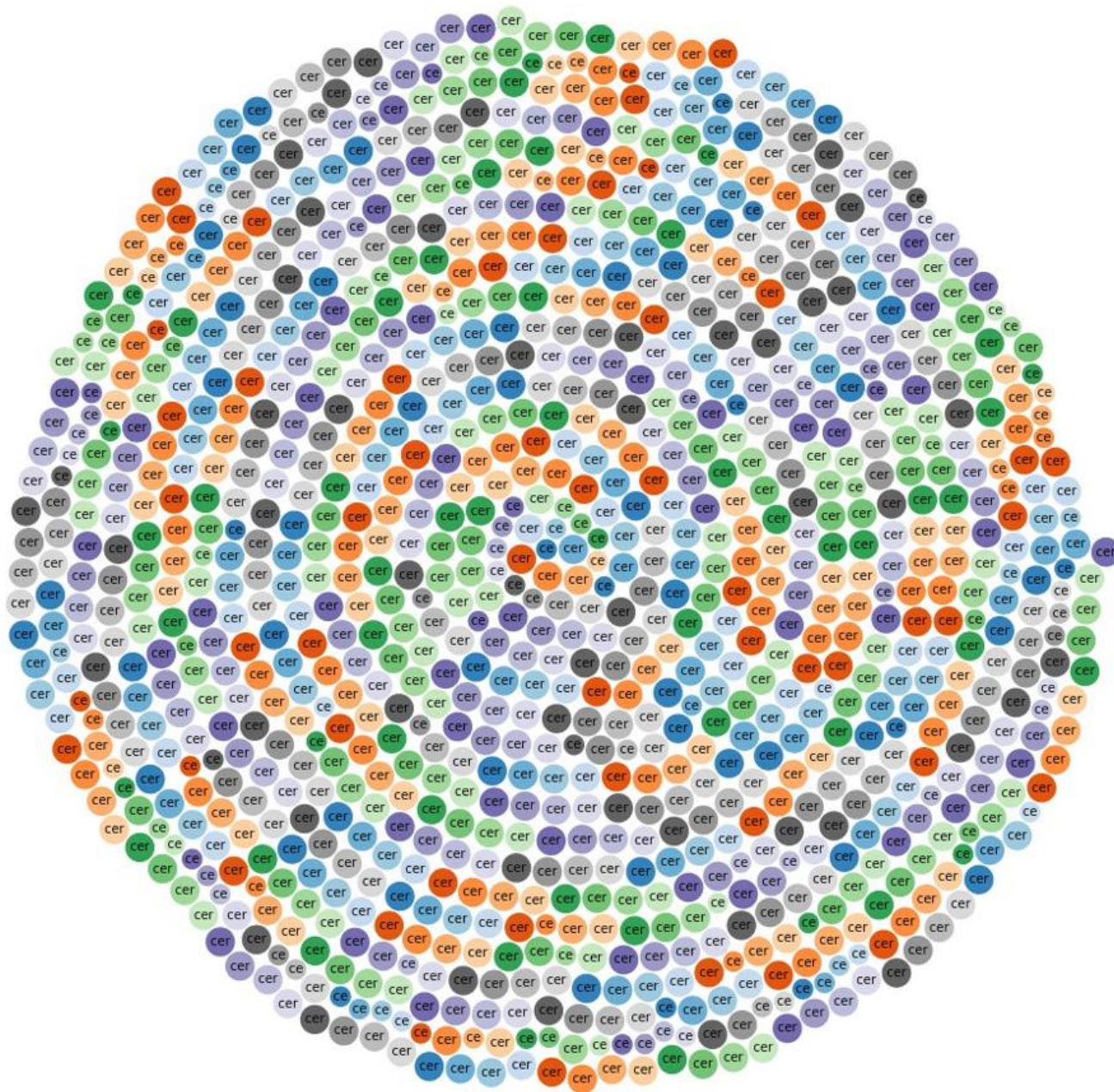


El siguiente grafico muestra la relacion del dominio (punto rojo) con todos los datos analizados, (punto negro)

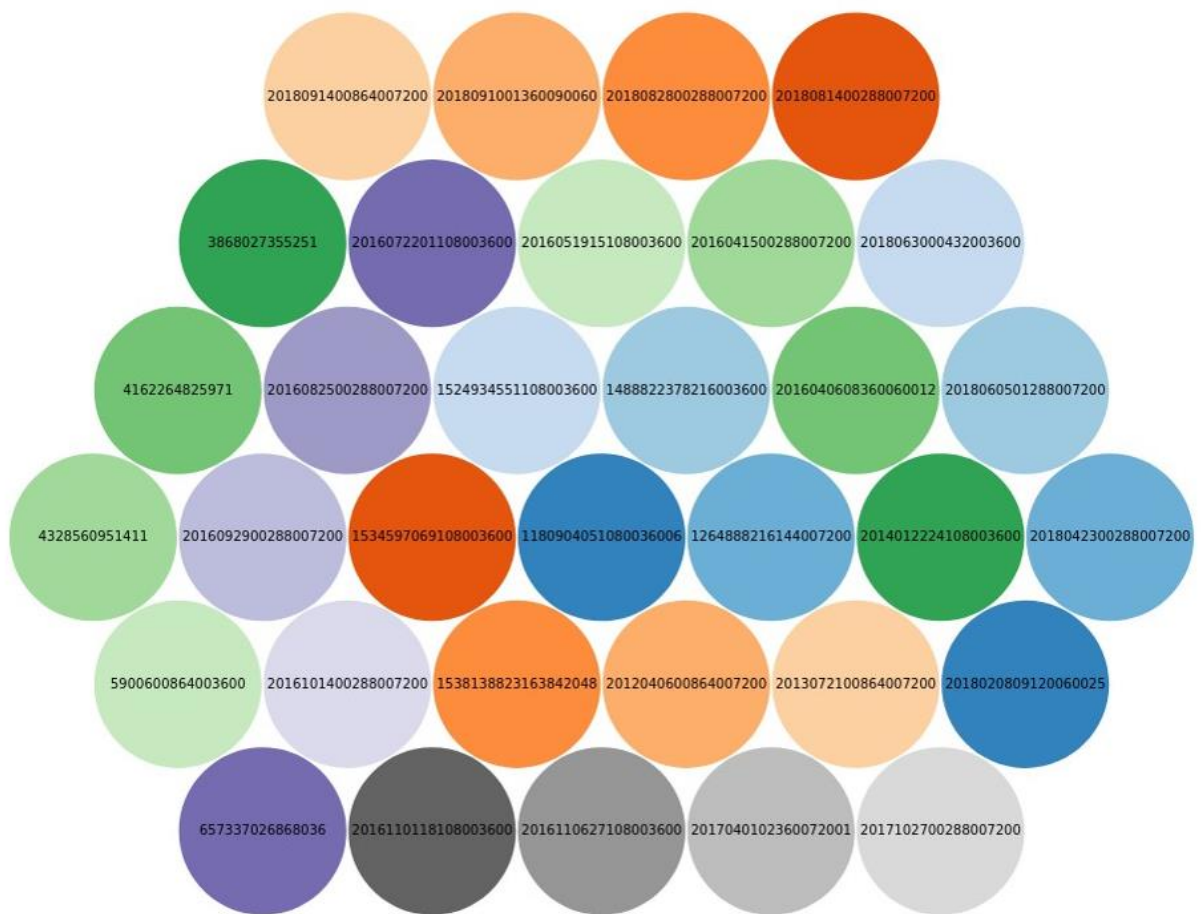




## Certificados SSL



## Numeros de tarjeta de credito hallados

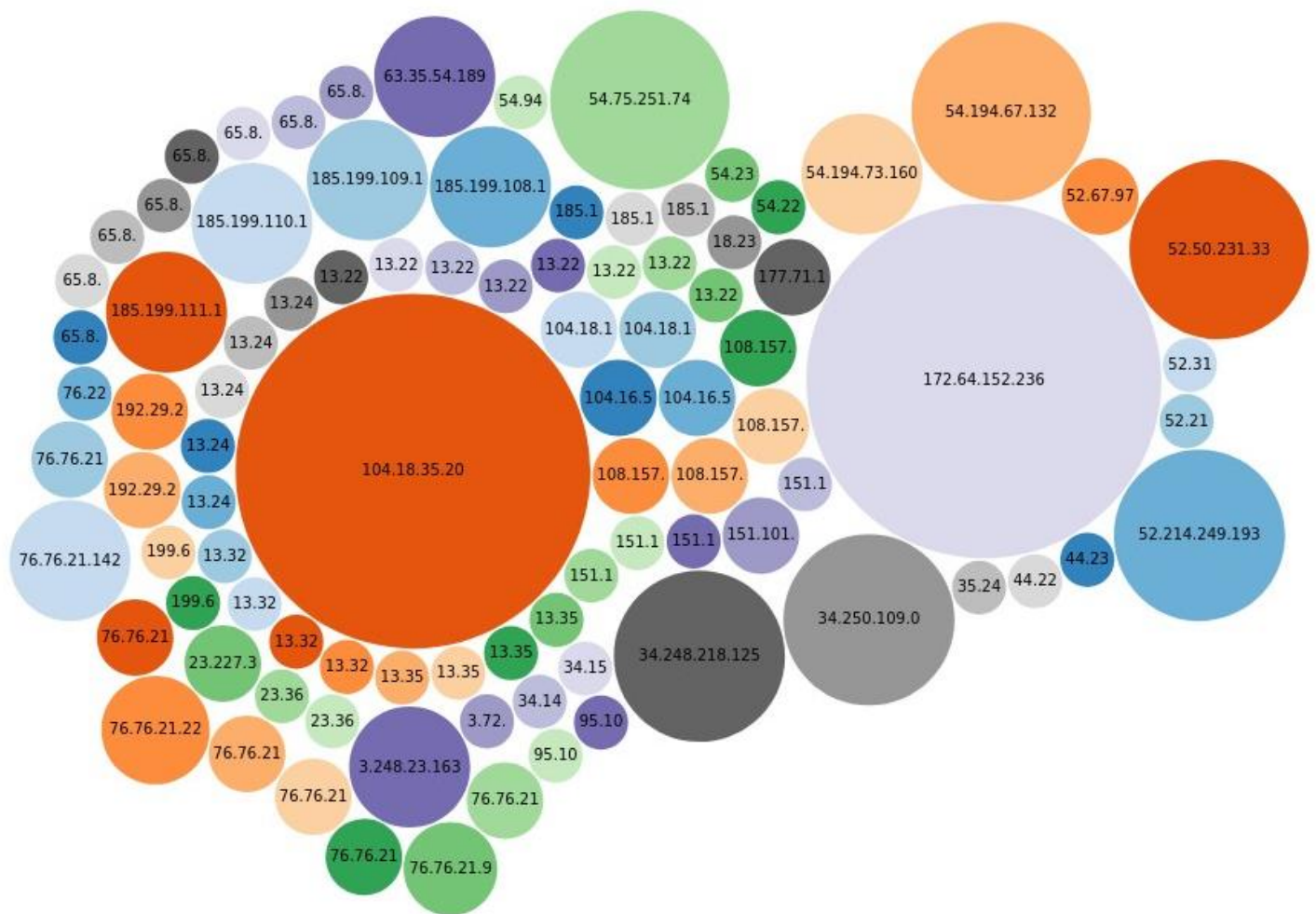




## Correos electronicos

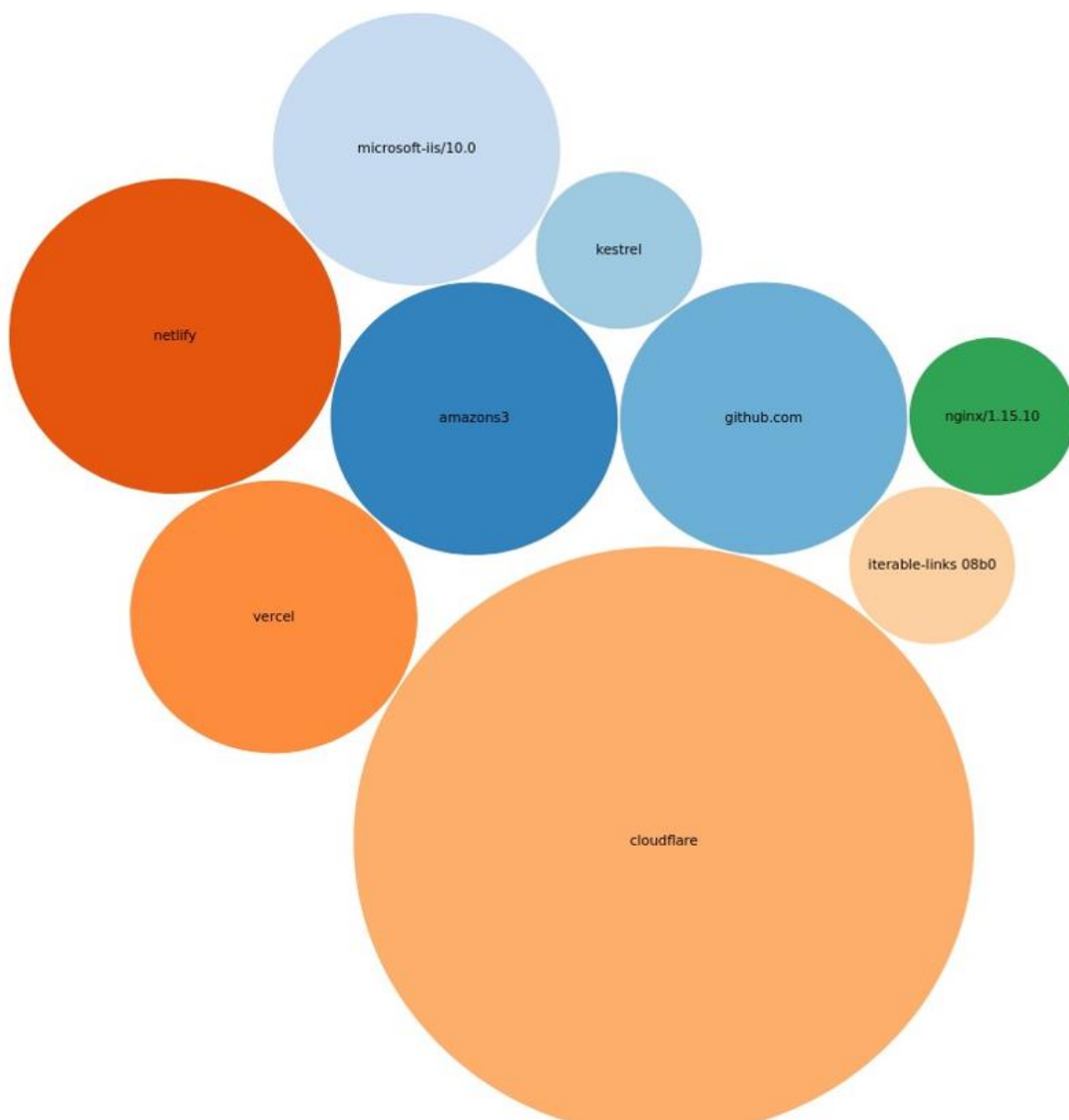


IPS address





## Web servers



IPS address maliciosos.



## IPS maliciosos en subnet



## RECOMENDACIONES

- 1- Se recomienda testeo de equipos informáticos para un análisis más integral,
- 2- La vulnerabilidad analizada por el investigador de criptomonedas no ha sido resuelta, se recomienda Ledger es un monedero de hardware que permite administrar las llaves y direcciones de distintas criptomonedas. Para asegurar los fondos de los usuarios, el equipo de desarrolladores tiene que idear un dispositivo donde cada aplicación de moneda se encuentra aislada una de la otra. Es decir, se puede tener acceso a direcciones de Ethereum, Bitcoin y Litecoin, pero cuando se abre una las otras se bloquean automáticamente.
- 3- Teniendo en cuenta que hay información sensible como números de tarjetas de crédito, correos electrónicos expuestos a ataques de ingeniería social se recomienda notificar a los posibles afectados por ataques como por ejemplo el phishing y de manera preventiva limpiar los metadatos de los documentos, publicados en internet o alojados en repositorios en la nube.
- 4- Con relación a lo anterior, se recomienda preventivamente el reseteo de contraseñas a la brevedad para evitar el robo de información a través de phishing, además de todas sus credenciales asociadas y eliminar información sensible o personal asociada a estos correos.
- 5- Se aconseja la práctica de campañas de concienciación sobre los riesgos derivados de la sobrexposición de información en redes sociales y otras plataformas de participación de información.
- 6- En el caso de que la página web asociada al registro sospechoso aún carezca de contenido, se recomienda la notificación inmediata al registrador, solicitando la eliminación del dominio. Se recomienda preventivamente la monitorización continuada de dominios, de cara a potenciales incidentes.
- 7- Se recomienda al Cliente filtrar la dirección de correo del remitente, actualizar sus firmas y/o la creación de alguna regla específica que permita el bloqueo de mensajes como este. Como medida reactiva caso el atacante haya logrado el acceso se aconseja la desactivación o eliminación de cuentas del usuario.
- 8- Se detectó la exposición de datos de tarjetas de crédito por lo que se recomienda la desactivación de las tarjetas y avisar a los usuarios afectados, se recomienda el análisis de dispositivos electrónicos y la retirada del contenido expuesto.