Informe

Por: Mateo Carusotti

Informe Gerencial:

Tras el análisis con diversas técnicas aplicadas en los dominios de la organización Opera.com, se puede concluir que Opera aloja sus servicios en la nube, utilizando plataformas como Amazon y Cloudflare, lo que delega gran parte de la responsabilidad de seguridad a estos proveedores. No se han detectado dispositivos expuestos a internet que puedan ser vulnerables.

Los distintos puertos que tienen abiertos para establecer una conexión son puertos dedicados a la web, como el puerto 80 o el 443. Mientras que los demás puertos que se pueden ver como establecidos están filtrados, es decir, bloqueados por algún firewall o solo permiten la conexión desde IPs específicas configuradas.

En cuanto a filtraciones de información, no se han identificado incidentes recientes, y los problemas anteriores han sido mitigados. Sus servidores web emplean tecnologías comunes como Apache y Nginx en versiones actualizadas, lo que minimiza el riesgo de vulnerabilidades conocidas.

La principal vulnerabilidad detectada es la facilidad con la que se puede obtener información sobre empleados y exempleados. A través de herramientas básicas, es posible extraer direcciones de correo electrónico y, con ellas, deducir nombres de usuario asociados.

Se observó un único sitio de login que no utiliza una conexión segura, lo cual representa un riesgo significativo, especialmente porque este sitio también es utilizado por empleados.

En conclusión, la organización Opera mantiene un buen nivel de seguridad siempre que continúe actualizando sus recursos y proteja adecuadamente los datos personales de sus empleados.

Informe Técnico:

Para el análisis de subdominios, utilicé herramientas como:

- Con esta herramienta obtenemos una gran cantidad de dominios que se desprenden de opera.com. Para el análisis de los demás anexos, tomaré solo algunos, basándome en los que la organización ofrece para escanear.

```
sublist3r -d opera.com.
```

No se encontró información de dispositivos conectados dentro de los dominios o bloques IP:

- Se utilizó el buscador Shodan, de donde solo se pudo obtener los hosts web de los diferentes dominios, sin encontrar dispositivos como cámaras, impresoras, etc.
- Se utilizó Nmap para el escaneo de dispositivos en diversos puertos, con:

  ```
  nmap -sS dominio.com
  ```

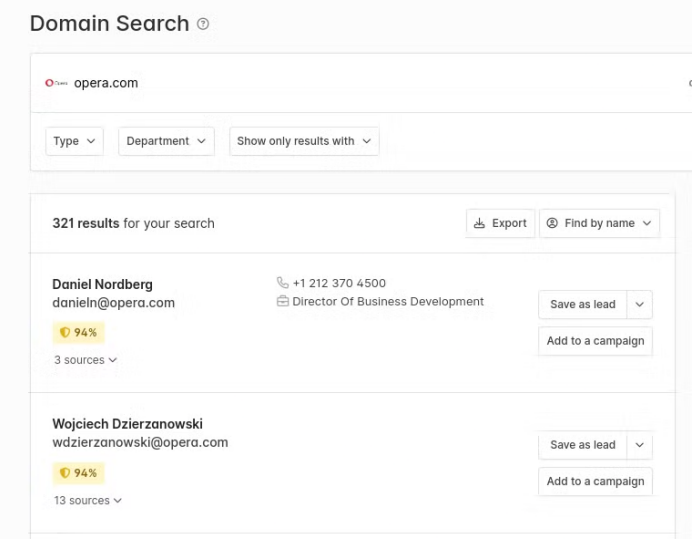
  Pero los datos que retorna son solo de servicios web.

Para el análisis de emails, utilicé herramientas como:

- TheHarvester para obtener, entre varios datos, correos electrónicos según el dominio

  ```
  theHarvester -d dominio.com -b all.
  ```

- Con la herramienta web Hunter.io, buscando por dominio se obtienen correos electrónicos dentro del dominio.



Para el análisis de nombres de usuario asociados a los correos electrónicos, utilicé:

- Google Hacking, con la búsqueda `intext:"*@dominio.com"`.
- Hunter.io, donde al buscar dominios y obtener correos electrónicos, en ocasiones también retorna nombres de los usuarios asociados.
- LinkedIn, plataforma donde podemos buscar los correos electrónicos encontrados y ver el nombre de la persona que los posee.

Para el análisis de las personas más relevantes de la organización, utilicé:

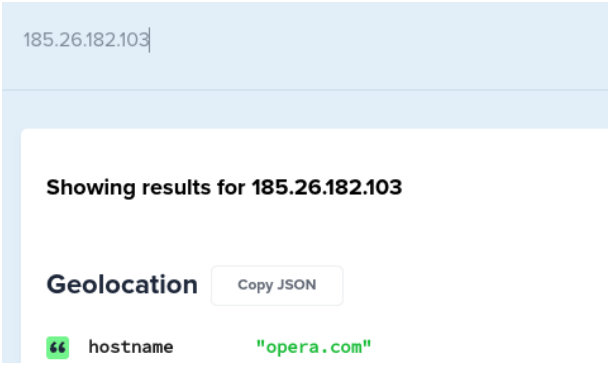
- LinkedIn, buscando según la organización y puestos jerárquicos como CEO, CTO, etc., y averigüé los nombres de estos.

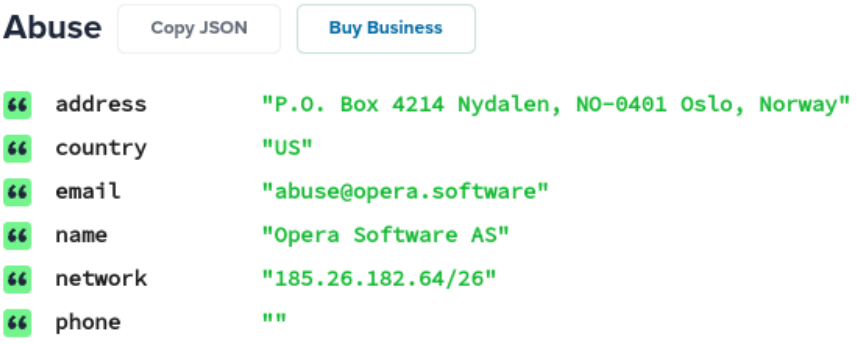
Para el análisis de reportes, utilicé las herramientas:

- Whois, donde se puede obtener varios datos del dominio, entre ellos canales de reportes

```
whois dominio.com.
```

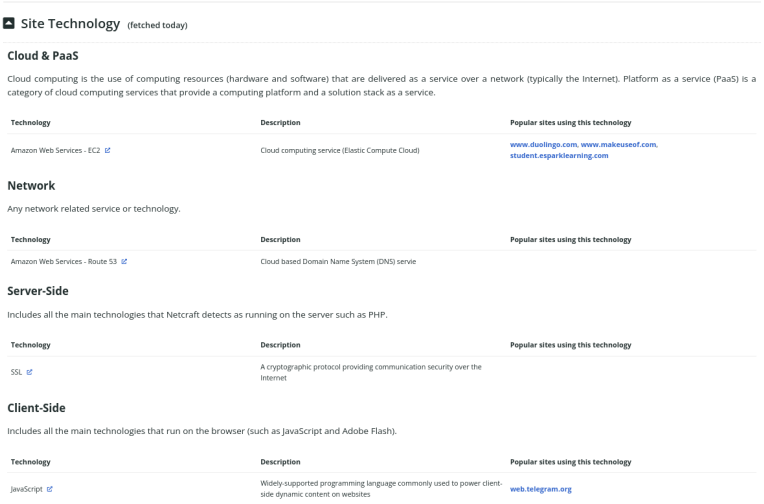
- En el sitio web ipinfo.io, se pueden ingresar IPs de dominios para también obtener datos, entre ellos los canales de reportes.





Para el análisis del software utilizado, utilicé las herramientas:

- Netcraft, donde podemos ingresar dominios y obtener información de las tecnologías que utilizan para distintas partes, como Client Side, Server Side, etc.



Site Technology (fetched today)

Cloud & PaaS

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). Platform as a service (PaaS) is a category of cloud computing services that provide a computing platform and a solution stack as a service.

Technology	Description	Popular sites using this technology
Amazon Web Services - EC2	Cloud computing service (Elastic Compute Cloud)	www.duolingo.com, www.makeuseof.com, student.esparklearning.com

Network

Any network related service or technology.

Technology	Description	Popular sites using this technology
Amazon Web Services - Route 53	Cloud based Domain Name System (DNS) servie	

Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites using this technology
SSL	A cryptographic protocol providing communication security over the Internet	

Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description	Popular sites using this technology
JavaScript	Widely-supported programming language commonly used to power client-side dynamic content on websites	web.telegram.org

Para la búsqueda de filtraciones realicé:

- Búsquedas en navegadores y sitios que suben contenido relacionado con filtraciones y brechas de seguridad.

Para el análisis de los bloques de IP de la organización, utilicé:

- ipinfo.io. Esta herramienta, al ingresar IPs de los dominios, nos brinda datos, entre ellos el bloque IP asociado a estas.

Para el análisis de los servidores de correo de la organización, utilicé:

- El comando dig para obtener esta información.

```
dig mx dominio.com
```

Para el análisis de los servidores DNS de los dominios de la organización, utilicé:

- El comando dig para obtener esta información.

```
dig ns dominio.com
```

- Para consultar la trasnferencia de zona hay que realizar estos pasos:
  1. Buscar que servidor primario

     ```
     dig soa dominio.com
     ```

  2. Con el servidor obtenido intentar la transferencia de zona

     ```
     dig axfr @servidor.primario dominio.com
     ```

Para el análisis de los servidores web utilice:

- Primero de los dominios que obtuve realice la siguente consulta

```
dig a dominio.com
```

- Luego con nmap bsuco que puertos tiene abiertos, en base a esto puedo saber si es un servidor web o no

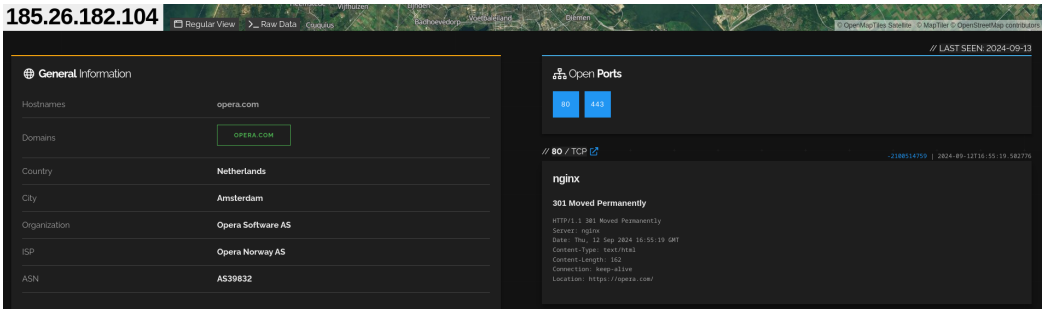
```
nmap -sS IP
```

Para encontrar servidores de otro tipo en este caso FTP utilice:

- Shodan con la busqueda `hostname:"ftp.opera.com"`

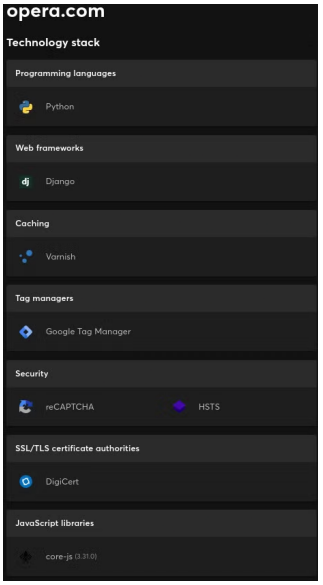
Para el análisis de las IPs de los puntos anteriores, utilicé:

- Shodan. Con este buscador, al ingresar las IPs seleccionadas, podemos analizar los puertos en los que están escuchando, además del protocolo que corre en estos y, en algunos casos, las versiones utilizadas.



Para el análisis de los proveedores de servicios, utilicé:

- Shodan. Similar al punto anterior, Shodan, al ingresar IPs o dominios, nos ofrece información sobre puertos y protocolos que corren en estos, además de brindarnos algunos servicios que utilizan.
- Wappalyzer. Esta herramienta web nos brinda información sobre las tecnologías que utilizan los dominios que ingresamos, incluyendo servicios.



Para el análisis de información adicional:

- Utilizando Shodan para analizar distintas IPs de recursos web de los dominios. Por ejemplo, en bugs.opera.com, la IP tiene un login que el navegador advierte como inseguro.