Lahocine José Ait Aliourdellah Bravo

SAD UT-2 T-0
Recopilación Pasiva de Información utilizando Google Hacking y Shodan

ÍNDICE

Búsqueda en Google

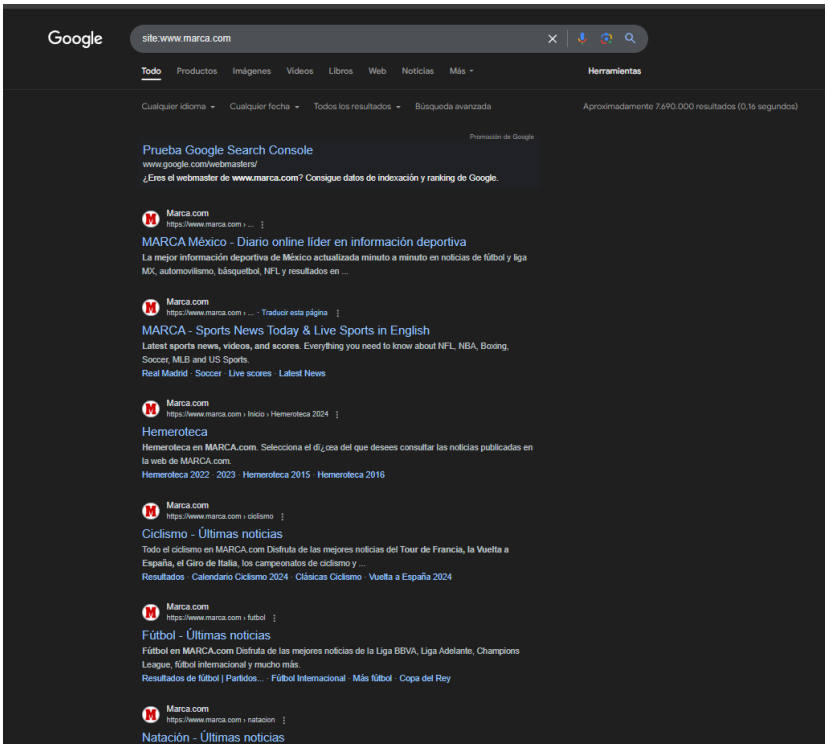
Indexación Completa del Sitio Web

Comando: “site:www.marca.com”.

Descripción: Esta búsqueda devuelve todas las páginas indexadas del sitio web de Marca.

Resultados Obtenidos: Aproximadamente 7.690.000 resultados. Los resultados incluyen una amplia gama de contenido:

- Noticias de diferentes deportes (fútbol, baloncesto, tenis, entre otros).
- Artículos de análisis y opinión.
- Estadísticas y datos sobre equipos y competiciones.
- Últimas noticias.



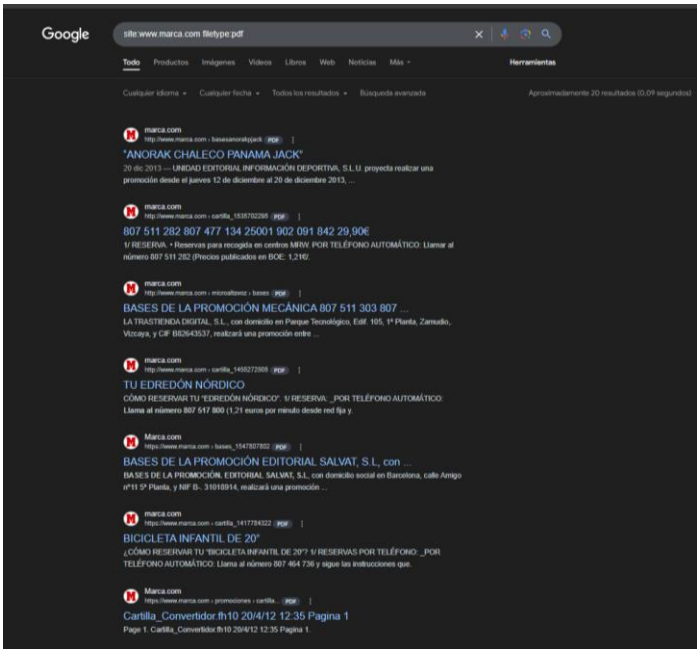
Documentos PDF Disponibles en el Sitio

Comando: “site:www.marca.com filetype:pdf”.

Descripción: Este comando se centra en documentos PDF alojados en el sitio web de Marca.

Resultados Obtenidos: Aproximadamente 20 documentos en formato PDF, entre los que destacan:

- Bases de promociones.



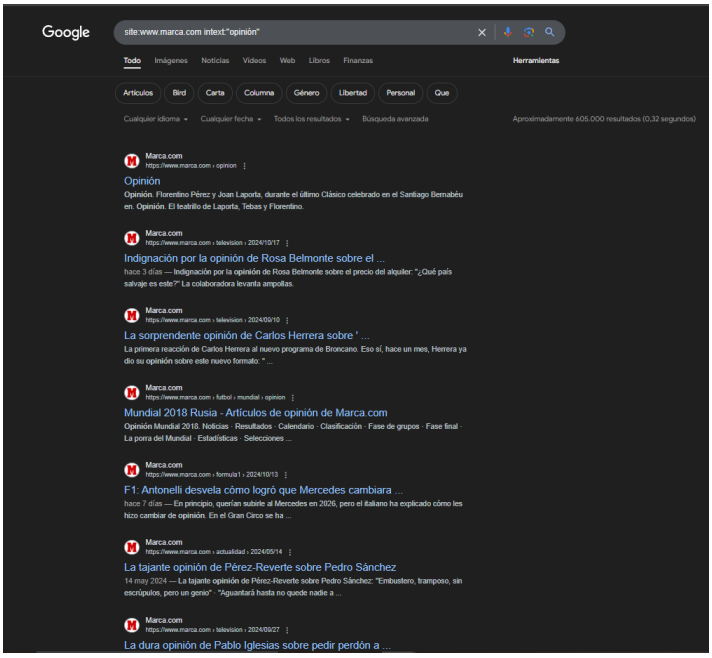
Artículos con “Opiniones”

Comando: “site:www.marca.com intext:"opinión” “.

Descripción: Este comando devuelve todas las páginas del sitio web de Marca que contienen la palabra "opinión" en el cuerpo del texto.

Resultados Obtenidos: Se obtuvieron aproximadamente 605.000 resultados, lo que revela una cantidad considerable de artículos que contienen la palabra “opinión”. Los temas incluyen:

- Opiniones sobre el desempeño de jugadores y equipos en competiciones como La Liga y la Champions League.
- Opiniones sobre política.
- Opiniones de famosos de temas deportivos.

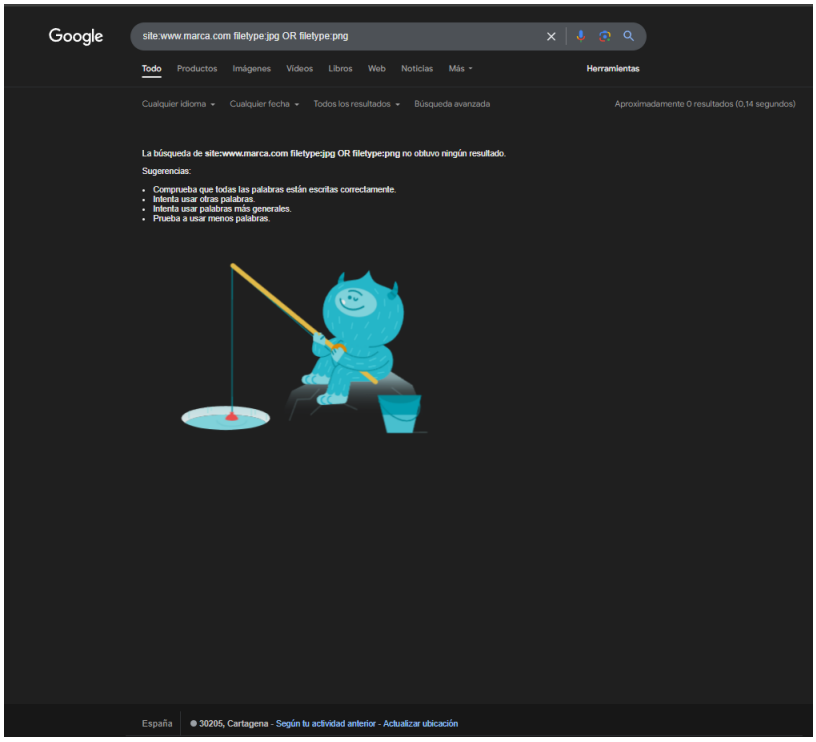


Búsqueda de Imágenes en Formato JPG o PNG

Comando: “site:www.marca.com filetype:jpg OR filetype:png”.

Descripción: Este comando filtra imágenes en formato JPG o PNG que se encuentra en el sitio web de Marca.

Resultados Obtenidos: No obtuvimos resultados al intentar buscar imágenes de Marca. Al intentar abrir una imagen, se redirige a la URL https://phantom-marca.unidadeditorial.es/. Esto se debe a que Marca utiliza una Red de Distribución de Contenido (CDN) para alojar y gestionar sus imágenes, lo que mejora la velocidad de carga y protege el contenido contra el uso no autorizado. Por esta razón, las imágenes de Marca no pueden ser indexadas por Google.



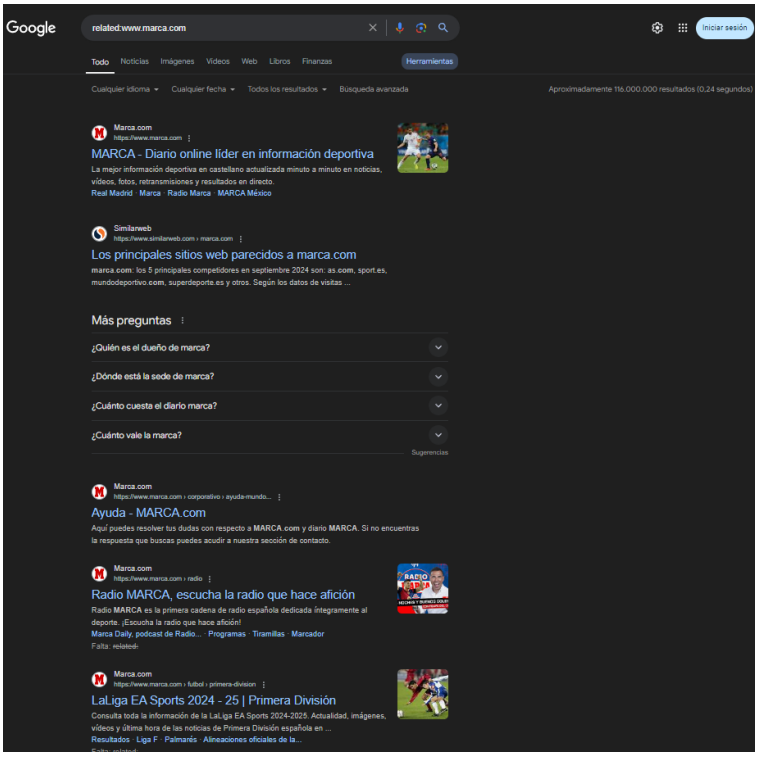
Sitios Web Relacionados con Marca

Comando: “related:www.marca.com”.

Descripción: Esta búsqueda es para identificar sitios web similares o relacionados con Marca.

Resultados Obtenidos: Aproximadamente 116.000.000 resultados. La búsqueda devolvió sitios web como:

- as.com
- mundodeportivo.com
- sport.es



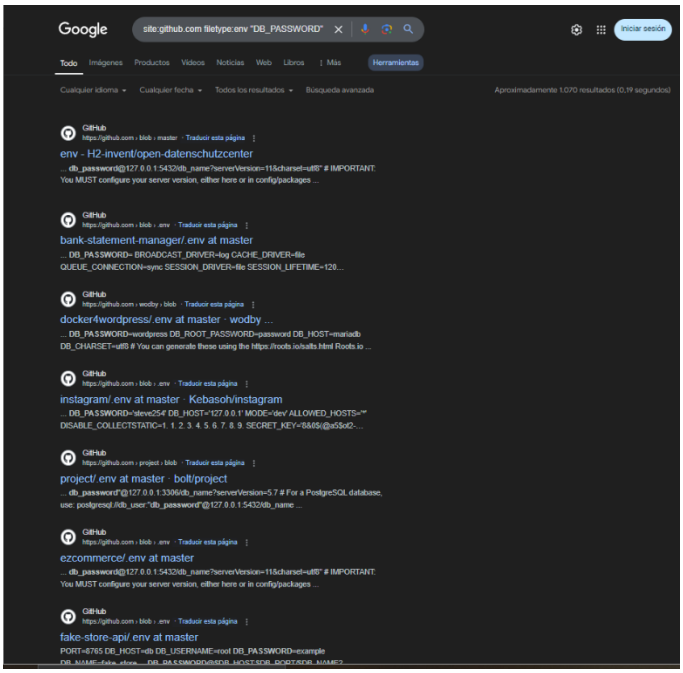
Google Dorks

Buscar archivos de configuración expuestos

Comando: “site:github.com filetype:env "DB_PASSWORD" ”

Descripción: Este comando busca específicamente archivos con la extensión .env en GitHub que contengan la cadena "DB_PASSWORD". Los archivos .env suelen almacenar configuraciones sensibles para aplicaciones, incluyendo credenciales de bases de datos.

Resultados Obtenidos: Aproximadamente 1.070 resultados. Después de realizar una búsqueda exhaustiva con este comando, he encontrado varios archivos de configuración en diferentes repositorios que contienen la palabra "DB_PASSWORD". Esto indica que GitHub ha implementado medidas efectivas para prevenir la exposición de datos críticos, reflejando las buenas prácticas de seguridad de los desarrolladores al manejar información sensible.

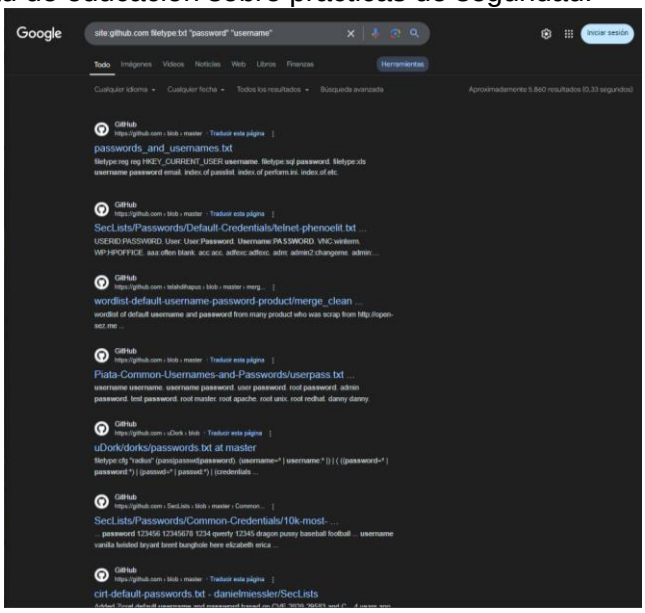


Buscar contraseñas en archivos de texto

Comando: “site:github.com filetype:txt "password" "username" ”

Descripción: Este comando busca archivos ".txt" en GitHub que contengan las palabras "password" y "username". Es común que los desarrolladores dejen credenciales en archivos de texto por error, lo que puede resultar en la exposición de información sensible.

Resultados Obtenidos: Aproximadamente 5.860 resultados. En esta búsqueda, encontré varios archivos que incluían listas de credenciales de acceso, algunas de las cuales estaban claramente destinadas a ser utilizadas en entornos de desarrollo. Sin embargo, también se encontraron ejemplos de archivos que parecían ser pruebas de concepto o documentación, lo que indica que no todos los desarrolladores son conscientes de los riesgos de compartir este tipo de información públicamente. Esto resalta la necesidad de educación sobre prácticas de seguridad.

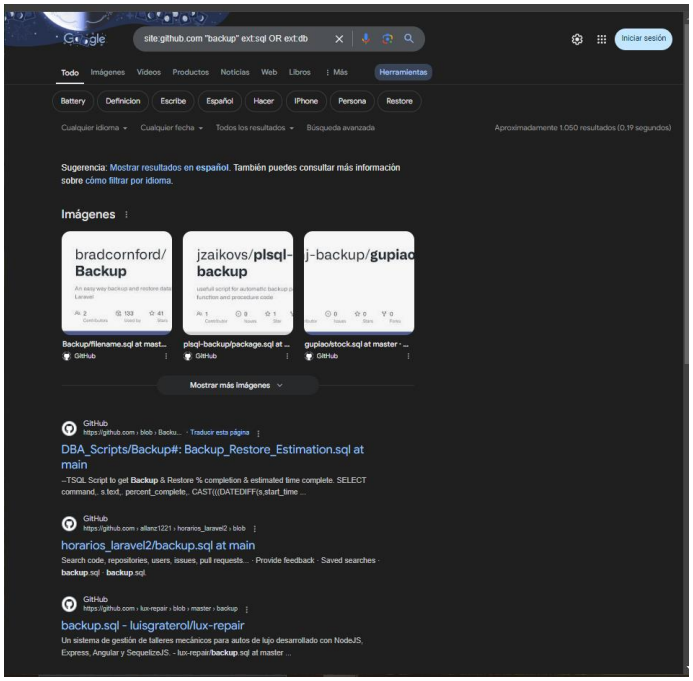


Buscar archivos de respaldo

Comando: “site:github.com "backup" ext:sql OR ext:db”

Descripción: Este comando busca archivos con las extensiones “sql”y “db” en GitHub que contengan la palabra "backup". Los archivos de respaldo son copias de bases de datos que pueden incluir información sensible, como datos de usuarios y configuraciones de la base de datos. Si estos archivos son accesibles públicamente, pueden ser utilizados por atacantes para comprometer la seguridad de los sistemas.

Resultados Obtenidos: Aproximadamente 1.050 resultados. En esta búsqueda, encontré varios scripts relacionados con la gestión de bases de datos. Un ejemplo destacado es un script T-SQL que recopila y organiza las rutas de archivos de datos, archivos de registro y ubicaciones de copias de seguridad en SQL Server. Esto sugiere que muchos administradores están compartiendo herramientas útiles para facilitar la administración de bases de datos.



Búsqueda en Shodan

Servidores FTP

Búsqueda: “port:21”

Descripción: Esta búsqueda mostrará dispositivos que tienen el puerto 21 (FTP) abierto.

Información:

- Resultados totales: 8.479.960 de dispositivos con el puerto 21 abierto. Esto muestra la magnitud de servidores FTP expuestos en Internet, lo que puede ser útil para administradores de redes, investigadores de seguridad o incluso hackers.

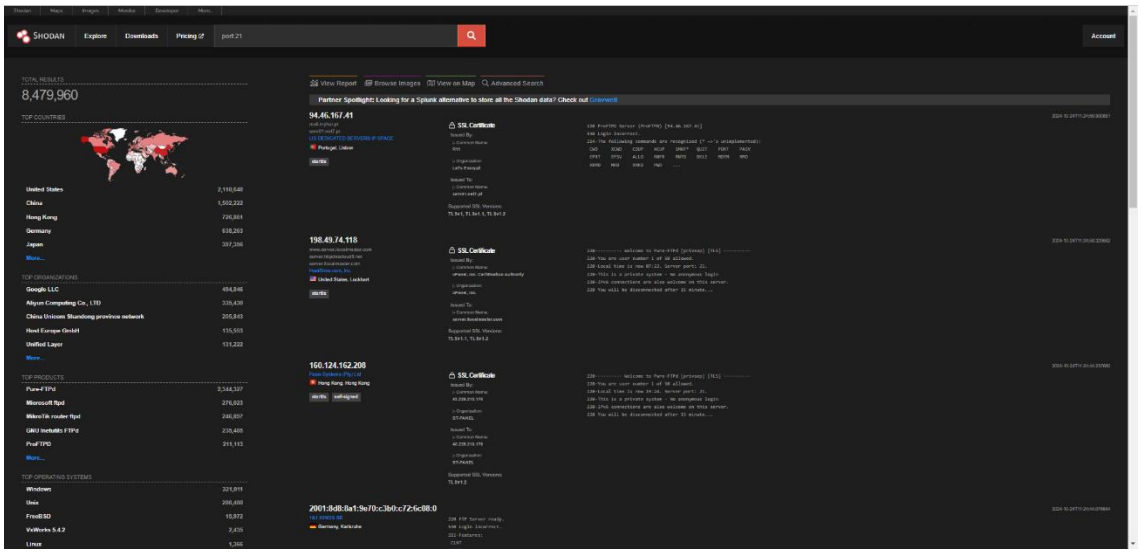
- IPs: 94.46.167.41, 198.49.74.118, 160.124.162.208, 2001:8d8:8a1:9e70:c3b0:c72:6c08:0.
Estas son direcciones IP de dispositivos que tienen el puerto 21 accesible en Internet.

- Principales países: Estados Unidos (2.110.648), Porcelana (1.502.222), Hong Kong (726.881), Alemania (638.263), Japón (397.356).
Estos países son los que tienen la mayor cantidad de servidores FTP expuestos en Internet. El gran número de servidores en Estados Unidos y China es especialmente relevante, ya que son dos de los países con mayores infraestructuras tecnológicas.

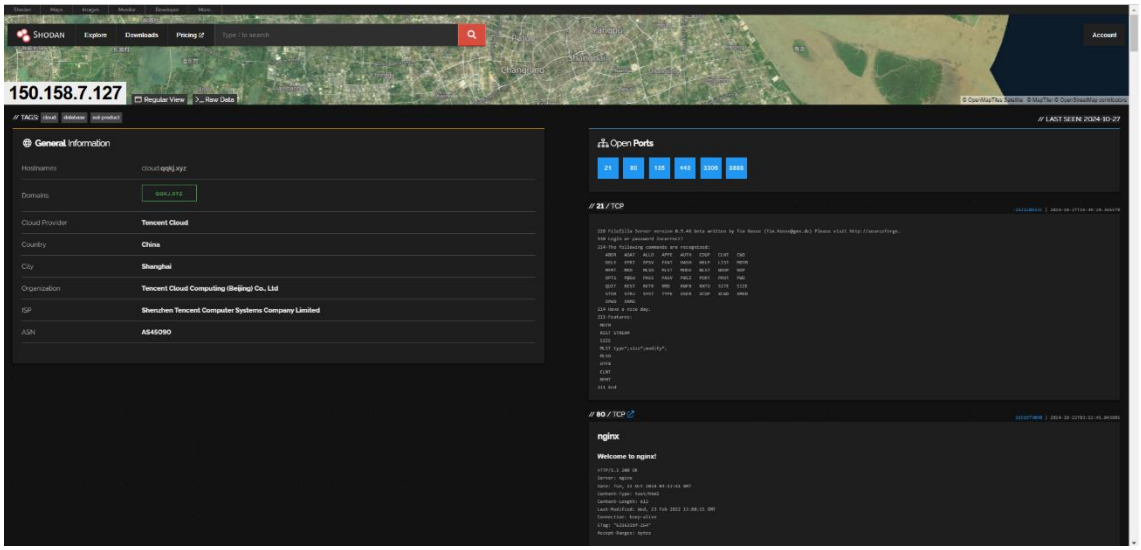
- Organizaciones principales: Google LLC (494.846), Aliyun Computing Co (335.430), Red de la provincia de China Unicom Shandong (205.843), Host Europe GmbH (135.553), Capa unificada (131.222).
Estas organizaciones tienen servidores FTP expuestos, lo cual podría ser una oportunidad para realizar auditorías de seguridad o identificar vulnerabilidades.

- Productos destacados: Pure-FTPd (2.344.327), Microsoft ftpd (276.023), MikroTik router ftpd (246.897), GNU Inetutils FTPd (235.485), ProFTPD (211.113).
Estos son los tipos de software de servidor FTP más comunes que se encuentran en los dispositivos expuestos.

- Sistemas operativos más usados: Windows (321.011), Unix (286.480), FreeBSD (15.972), VxWorks 5.4.2 (2.435), Linux (1.366).


SHODAN
Explore
Downloads
Pricing
port:21
Account
TOTAL RESULTS
8,479,960
TOP COUNTRIES
United States 2,110,648
China 1,502,222
Hong Kong 726,801
Germany 638,263
Japan 397,386
More...
TOP ORGANIZATIONS
Google LLC 494,846
Alicyun Computing Co., LTD 335,439
China Unicom Shandong province network 205,843
Hetzner Online GmbH 155,503
Unified Layer 131,222
More...
TOP PRODUCTS
Pure-FTPd 2,344,337
Microsoft ftpd 276,023
MikroTik router ftpd 246,807
GNU Inetutils FTPd 230,485
ProFTPD 211,113
More...
TOP OPERATING SYSTEMS
Windows 221,011
Unix 208,488
FreeBSD 10,972
VxWorks 5.4.2 2,435
Linux 1,366
View Report
Browse Images
View on Map
Advanced Search
Partner Spotlight: Looking for a Splunk alternative to store all the Shodan data? Check out Graylog9
94.46.167.41
SSL Certificate
198.49.74.118
SSL Certificate
160.124.162.208
SSL Certificate
2001:9d8:8a1:9e70:c3b0:c72:6c08:0

Resultado:



IP: 150.158.7.127
Esta es la dirección IP pública del servidor. Las IPs son únicas y permiten identificar dispositivos en Internet.

Nombres de host: cloud.qqkj.xyz
El "nombre de host" es un nombre asignado al servidor. En este caso, cloud.qqkj.xyz es el nombre que se utiliza para identificar al servidor en la red.

Dominios: QQKJ.XYZ
Es el dominio asociado con este servidor.

Proveedor de servicios en la nube: Tencent Cloud
El servidor está alojado en Tencent Cloud, que es un proveedor de servicios en la nube. Tencent es una importante empresa tecnológica de China, y su plataforma en la nube es utilizada por muchas organizaciones para alojar servidores y servicios.

País: China
El servidor está ubicado en China, lo que se puede deducir de la información de la IP y la infraestructura proporcionada por Tencent Cloud.

Ciudad: Shanghái
El servidor se encuentra en Shanghái, que es una de las principales ciudades tecnológicas de China y un importante centro para los servicios en la nube y la infraestructura de internet.

Organización: Tencent Cloud Computing (Beijing) Co., Ltd
La organización que gestiona este servidor es Tencent Cloud Computing (Beijing), que es una división de Tencent, responsable de sus servicios en la nube. Esto significa que el servidor es parte de la infraestructura de Tencent.

Proveedor de servicios de Internet: Shenzhen Tencent Computer Systems Company Limited
Este es el proveedor de servicios de Internet (ISP), que gestiona la conectividad del servidor a la red. En este caso, es también una entidad relacionada con Tencent, indicando que Tencent maneja no solo la infraestructura en la nube, sino también el acceso a Internet.

Número de serie: AS45090
Este es el número de serie del sistema autónomo (ASN), que se refiere a un identificador único asignado a una red de IPs controlada por una organización en particular. En este caso, AS45090 pertenece a Tencent. Los números AS son usados para identificar y enrutar las conexiones de Internet entre diferentes redes.

Puertos abiertos:
Estos son los puertos de red que están abiertos en el servidor y, por lo tanto, accesibles desde Internet. Los puertos abiertos permiten la comunicación con el servidor y, si no se gestionan adecuadamente, pueden ser puntos de acceso vulnerables.

21: FTP (File Transfer Protocol), usado para transferir archivos.
80: HTTP, puerto usado para tráfico web no cifrado.
135: RPC (Remote Procedure Call), usado principalmente por sistemas Windows.
443: HTTPS, puerto usado para tráfico web cifrado.
3306: MySQL, puerto usado para bases de datos MySQL.
8888: Usado comúnmente por aplicaciones web y servicios como Jupyter o servidores de desarrollo.

Software en ejecución: Nginx, Filezilla Server

Nginx es un servidor web de alto rendimiento utilizado para servir contenido web y gestionar la carga de tráfico.
Filezilla Server es un servidor FTP de código abierto, utilizado para la transferencia de archivos a través del protocolo FTP, lo que está relacionado con el puerto 21 abierto en este caso.

Última visita: 27/10/2024
Esto indica la última vez que el servidor fue escaneado o accedido a través de Shodan.

Cámaras IP

Búsqueda: “port:80 "webcam" country:US”

Descripción: Busca webcam que estén expuestas en el puerto 80 en los Estados Unidos.

Información:

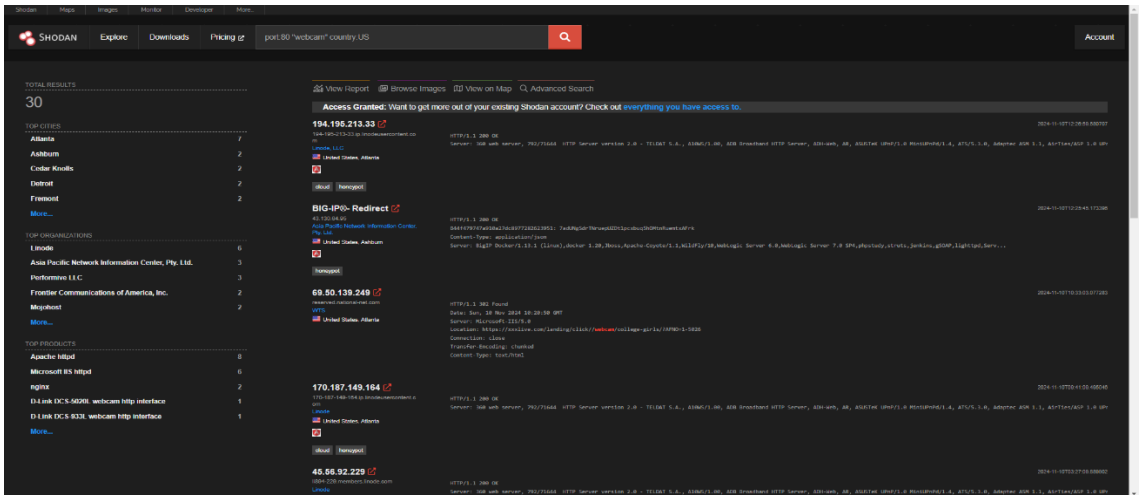
- Resultados totales: 30 que cumplen con los criterios de búsqueda. Esto significa que en Estados Unidos existen 30 cámaras que están expuestas públicamente en el puerto 80 y son detectables con esta búsqueda en Shodan.

- IPs: 194.195.213.33, 43.130.64.95, 69.50.139.249, 170.187.149.164.
Estas son las direcciones IP públicas que corresponden a las cámaras encontradas, lo que significa que estas cámaras están directamente accesibles desde internet en estas direcciones.

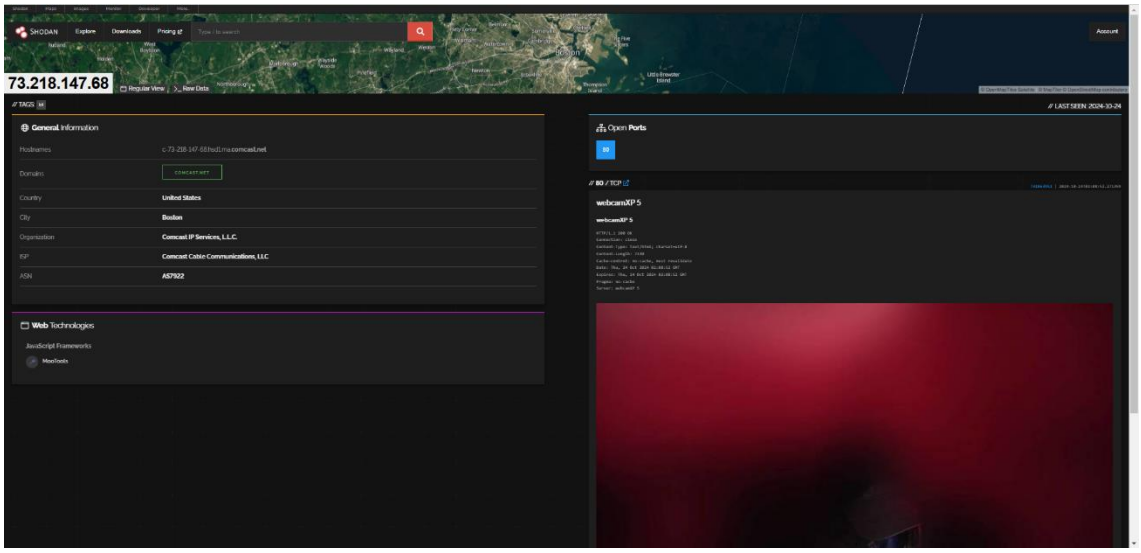
- Principales ciudades: Atlanta (7), Ashburn (2), Cedar Knolls (2), Detroit (2), Fremont (2).
Esto nos muestra que las cámaras están distribuidas por varias ciudades importantes en Estados Unidos, con Atlanta destacándose como la ciudad con el mayor número de cámaras expuestas.

- Organizaciones principales: Linode (6), Asia Pacific Network Information Center, Pty. Ltd. (3), Performive LLC (3), Frontier Communications of America, Inc. (2), Mojohost (2).
Estas organizaciones representan los proveedores de servicios de Internet o de infraestructura en la red que hospedan las cámaras IP, lo que indica que muchas de ellas están alojadas por empresas de telecomunicaciones o proveedores de hosting.

- Productos destacados: Apache httpd (8), Microsoft IIS httpd (6), nginx (2), D-Link DCS-5009L webcam http interface (1), D-Link DCS-5020L webcam http interface (1).
Esto revela que muchas de las cámaras expuestas utilizan servidores web estándar para gestionar el acceso HTTP y algunas de ellas son cámaras D-Link, un modelo de cámara IP popular.



Resultado:



IP: 73.218.147.68
Esta IP en particular pertenece a una red gestionada por Comcast, un proveedor de servicios de Internet (ISP) en Estados Unidos.

Nombre de host: c-73-218-147-68.hsd1.ma.comcast.net
En este caso, el nombre de host sugiere que el dispositivo está ubicado en una red gestionada por Comcast en Massachusetts (ma). El prefijo "hsd1" podría hacer referencia a una red residencial de banda ancha (high-speed data) de Comcast.

Dominio: comcast.net
El dominio asociado con esta IP es comcast.net, que confirma que el dispositivo está dentro de la infraestructura de Comcast, una de las principales empresas de telecomunicaciones de Estados Unidos. Esto implica que el dispositivo se conecta a Internet a través de la red de Comcast.

País: Estados Unidos
La dirección IP está ubicada en Estados Unidos, lo cual es consistente con el hecho de que está asociada con Comcast, una empresa que opera en ese país.

Ciudad: Boston
Según la información geográfica de la IP, el dispositivo está ubicado en Boston.

Organización: Comcast IP Services, LLC
El nombre de la organización asociada con esta IP es Comcast IP Services, LLC, lo cual indica que la organización que gestiona esta dirección IP es una división dentro de Comcast dedicada a la infraestructura de Internet.

ISP: Comcast Cable Communications, LLC
El ISP (Proveedor de Servicios de Internet) es Comcast Cable Communications, LLC, que es la división de Comcast encargada de ofrecer acceso a Internet de banda ancha y otros servicios de telecomunicaciones.

ASN: AS7922
El ASN (Autonomous System Number) AS7922 es un identificador único asignado a la red de Comcast. Este número se utiliza para identificar las redes en Internet y gestionar el enrutamiento del tráfico de datos entre diferentes redes. Este ASN pertenece a Comcast, lo que significa que la red que maneja esta IP es parte de la infraestructura de Comcast.

Puertos abiertos: 80/TCP
El puerto 80/TCP está abierto en el dispositivo, lo que permite la comunicación web a través del protocolo HTTP. Este puerto aloja el servicio webcamXP 5, un software utilizado para gestionar cámaras web IP. Esto significa que el dispositivo podría estar exponiendo públicamente una cámara o servicio de video en vivo, lo que representa un posible riesgo de seguridad si no está adecuadamente protegido.

Tecnologías web: JavaScript Framework: MooTools
El dispositivo o servicio web está utilizando el framework JavaScript MooTools, que es una biblioteca de JavaScript utilizada para crear aplicaciones web interactivas. El uso de MooTools sugiere que el sitio web o servicio asociado con este dispositivo tiene una interfaz web dinámica que utiliza JavaScript para mejorar la experiencia del usuario.

Última visita: 24/10/2024
Esto indica la última vez que el servidor fue escaneado o accedido a través de Shodan.

Dispositivos D-Link

Búsqueda: “org:"D-Link" port:80”

Descripción: Busca dispositivos de la organización D-Link que estén expuestos en el puerto 80, identificando cámaras IP, enrutadores y otros dispositivos que podrían estar mal configurados y accesibles públicamente.

Información:

- Resultados totales: 35 dispositivos de la marca D-Link expuestos en el puerto 80 en la red.

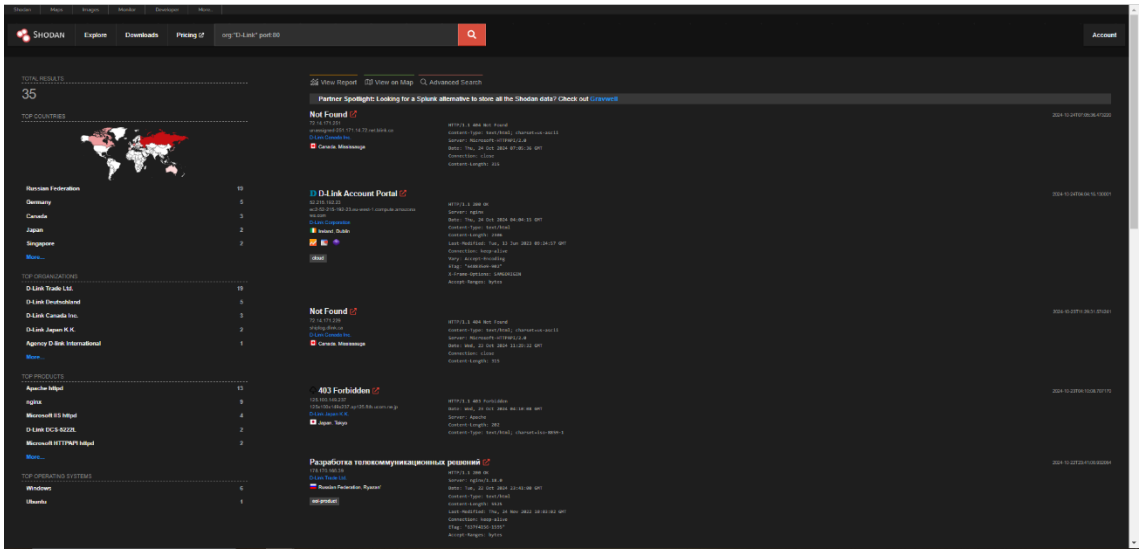
- IPs: 72.14.171.251, 52.215.192.23, 72.14.171.229, 125.100.149.237, 178.170.168.39
Estas son las direcciones IP públicas asociadas con los dispositivos de D-Link. Si estos dispositivos no están adecuadamente configurados, podrían ser accesibles desde cualquier lugar del mundo.

- Principales países: Federación Rusa (19), Alemania (5), Canadá (3), Japón (2), Singapur (2).
La mayoría de los dispositivos expuestos se encuentran en la Federación Rusa, lo que podría indicar que muchos dispositivos D-Link en este país están mal configurados o son accesibles sin seguridad adecuada.

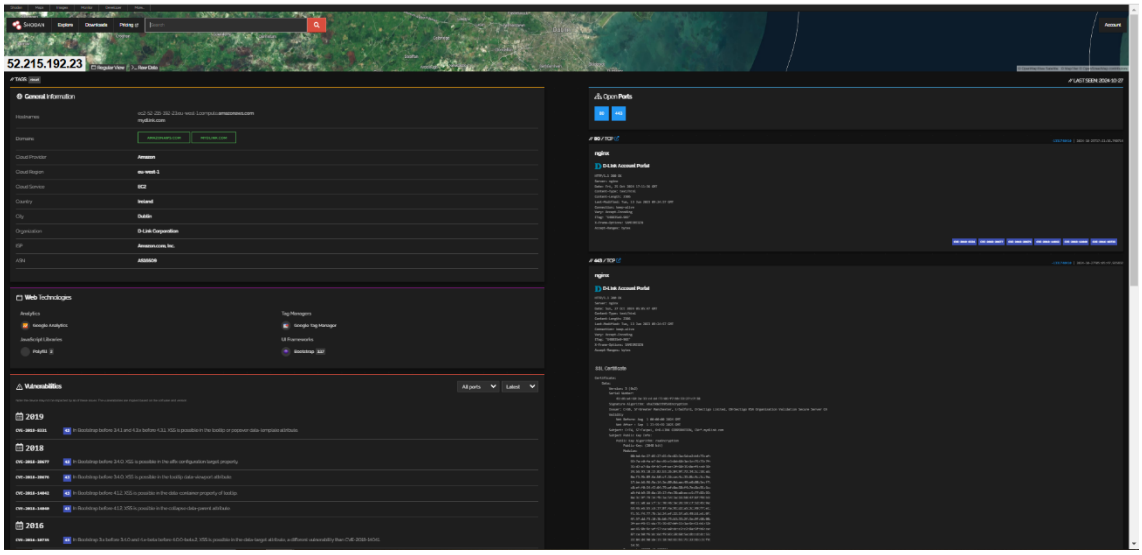
- Organizaciones principales: D-Link Trade Ltd. (19), D-Link Deutschland (5), D-Link Canada Inc. (3), D-Link Japan K.K. (2), Agency D-link International (1).
Estos dispositivos están gestionados por las filiales de D-Link en diversos países.

- Productos destacados: Apache httpd (13), nginx (9), Microsoft IIS httpd (4), D-Link DCS-5222L (2), Microsoft HTTPAPI httpd (2).
algunos dispositivos utilizan cámaras D-Link DCS-5222L, que son conocidas por ser cámaras IP.

- Sistemas operativos más usados: Windows (6), Ubuntu (1).



Resultado:



IP: 52.215.192.23
sta es la dirección IP pública de un dispositivo en la nube, ubicada en un servidor de Amazon Web Services (AWS).

Nombre de host: ec2-52-215-192-23.eu-west-1.compute.amazonaws.com
mydlink.com
El nombre de host indica que el dispositivo está en un servidor de Amazon EC2 en la región eu-west-1 (Irlanda). También está relacionado con mydlink.com, que pertenece a D-Link.

Dominio: amazonaws.com, mydlink.com
El dispositivo está asociado con los dominios amazonaws.com (proveedor de la nube) y mydlink.com (servicios de D-Link).

Proveedor de la nube: Amazon
El dispositivo está alojado en Amazon Web Services (AWS), una plataforma de nube popular que ofrece servicios de computación en la nube.

Región de la nube: eu-west-1
El dispositivo está ubicado en la región de AWS en Europa, específicamente en Irlanda (eu-west-1).

Servicio en la nube: EC2
Este dispositivo es un servidor EC2 de Amazon, utilizado para ejecutar aplicaciones y servicios en la nube.

País: Irlanda
El servidor se encuentra en Irlanda, que es donde Amazon tiene centros de datos en la región eu-west-1.

Ciudad: Dublín
La ciudad donde se encuentra el servidor es Dublín, Irlanda, que es uno de los principales hubs de Amazon en Europa.

Organización: D-Link Corporation
El dispositivo está asociado con D-Link Corporation, una empresa que fabrica dispositivos de red, como cámaras IP y enrutadores.

ISP: Amazon.com, Inc.
El proveedor de servicios de Internet (ISP) es Amazon.com, Inc., ya que el dispositivo está alojado en sus servicios en la nube.

ASN: AS16509
El ASN (número de sistema autónomo) AS16509 está asociado con Amazon y se utiliza para gestionar el enrutamiento de tráfico de datos en sus redes.

Tecnologías web: Google Analytics, Google Tag Manager, Polyfill, Bootstrap
El sitio web o servicio asociado utiliza varias tecnologías, como Google Analytics (para análisis web), Google Tag Manager (para gestión de etiquetas), Polyfill (para compatibilidad de navegadores) y Bootstrap (un framework de diseño web).

Puertos abiertos: 80, 443
Los puertos 80 (HTTP) y 443 (HTTPS) están abiertos, lo que indica que el dispositivo permite tráfico web (páginas HTTP y seguras HTTPS).

Vulnerabilidades:

- CVE-2016-10735: En Bootstrap 3.x anterior a 3.4.0 y 4.x-beta anterior a 4.0.0-beta.2, es posible que se produzca XSS en el atributo data-target, una vulnerabilidad diferente a CVE-2018-14041.
Afecta a Bootstrap 3.x (hasta 3.4.0) **y** 4.x-beta (hasta 4.0.0-beta.2). Permite XSS a través del atributo data-target, lo que permite ejecutar código malicioso en los navegadores.

- CVE-2018-14040: En Bootstrap anterior a 4.1.2, XSS es posible en el atributo data-parent de colapso.
En Bootstrap anterior a 4.1.2**,** el atributo data-parent en menús plegables es vulnerable a XSS, permitiendo la ejecución de scripts maliciosos.

- CVE-2018-14042: En Bootstrap anterior a 4.1.2, XSS es posible en la propiedad del contenedor de datos de la información sobre herramientas.
En Bootstrap anterior a 4.1.2, el atributo data-container en tooltips puede ser manipulado para ejecutar XSS.

- CVE-2018-20676: En Bootstrap anterior a 3.4.0, XSS es posible en el atributo data-viewport de la información sobre herramientas.
En Bootstrap anterior a 3.4.0, el atributo data-viewport en tooltips permite XSS.

- CVE-2018-20677: En Bootstrap anterior a 3.4.0, XSS es posible en la propiedad de destino de configuración de afijo.
En Bootstrap anterior a 3.4.0, el atributo data-target en elementos fijados es vulnerable a XSS.

- CVE-2019-8331: En Bootstrap anterior a 3.4.1 y 4.3.x anterior a 4.3.1, XSS es posible en el atributo data-template de información sobre herramientas o ventana emergente.
En Bootstrap anterior a 3.4.1 **y** 4.3.x hasta 4.3.1, el atributo `data-template` en tooltips o popups permite XSS.

Todas estas vulnerabilidades permiten que un atacante inyecte scripts maliciosos en un sitio web, comprometiendo la seguridad de los usuarios.

Última visita: 27/10/2024
Esta es la fecha en que el dispositivo fue escaneado o accedido por la herramienta de escaneo Shodan.

Reflexión ética

Riesgos y Consecuencias de Utilizar Herramientas como Google Hacking y Shodan en Sistemas No Autorizados

Herramientas como Google Hacking y Shodan brindan la capacidad de realizar búsquedas avanzadas de información y detectar dispositivos expuestos en la red; aunque presentan beneficios para los expertos en seguridad cibernética., también entrañan ciertos riesgos potenciales. Estas herramientas resultan valiosas para los profesionales del ámbito de la seguridad informática; no obstante, pueden ser empleadas de forma maliciosa por hackers conocidos como “sombrero negro", quienes utilizan sus destrezas para comprometer sistemas de seguridad. El principal riesgo al utilizarlas sin autorización es la posible exposición de datos confidenciales; lo cual podría desembocar en interrupciones en servicios críticos y vulnerar la privacidad tanto de individuos como organizaciones.

Responsabilidades Éticas de un Hacker Ético

Desde un enfoque ético, un hacker ético debe obrar de manera íntegra y respetar la privacidad y la confidencialidad de la información que maneja. La ética en ciberseguridad dicta que cualquier descubrimiento de datos sensibles sea manejado cuidadosamente. Es fundamental no intentar identificar ni aprovechar vulnerabilidades en sistemas externos sin el consentimiento expreso del dueño; un hacker ético no busca comprometer la seguridad de un sistema si no cuenta previamente with the apropiada autorización adecuada. Por lo general se lleva a cabo este tipo de tarea en virtud de un contrato que establece los límites de las pruebas o a través de programas de “bug bounty", los cuales premian el descubrimiento de vulnerabilidades en situaciones reguladas.

Consecuencias Legales de Actuar sin Permiso

Acceder sin permiso previo al contenido de sistemas computarizados es considerado un actuar ilegal en la mayoría de las naciones y puede acarrear consecuencias que van desde multas hasta encarcelamiento efectivo como castigo por la transgresión cometida en forma de intentos de hacking o intrusión indebida que resaltan la necesidad imperativa de obrar siempre dentro de los márgenes legales establecidos.

El Rol del Hacker Ético en la Seguridad Digital

En este escenario particular resulta esencial el papel del hacker ético; su labor contribuye de forma significativa al fortalecimiento de la seguridad digital en general. Los hackers éticos emplean sus destrezas para resguardar en lugar de dañar y al hacerlo promueven un entorno más protegido para todos los usuarios. Por consiguiente, el respetar la privacidad, la responsabilidad ética y la conformidad a las normativas legales constituyen los fundamentos que orientan la práctica profesional en el campo de la seguridad informática.