
# Análisis de OSINT aplicado a la detección de amenazas y vulnerabilidades en las organizaciones

Trabajo Final presentado para obtener el grado de Especialista en Redes y Seguridad

**Universidad Nacional de La Plata**
**Facultad de Informática**

**Tesista**
*Lic. Eduardo Fabián Tossolini*
**Director**
*Mg. Nicolas Macia*
**Co-Director**
Lic. Francisco Javier Díaz

La Plata, Argentina. Año 2021

# Índice

# Resumen

Actualmente, la información y los activos que las organizaciones exponen a Internet muchas veces ponen en riesgo a las mismas por presentar configuraciones incorrectas, malas prácticas o vulnerabilidades conocidas sin parchear, estas debilidades pueden llegar a ser utilizadas por actores maliciosos para filtrar y exhibir información sensible entre otras acciones.

El presente trabajo muestra la importancia de la utilización de OSINT en el monitoreo y evaluación de los activos de una organización para la detección de amenazas y vulnerabilidades con el propósito de mostrar a los equipos que gestionan la seguridad de la información, tácticas, técnicas y procedimientos que puedan ser utilizados de manera proactiva en la detección y gestión de incidentes.

# Introducción

Los avances en las tecnologías de la información y la presencia de las organizaciones en Internet requieren la gestión continua de la seguridad de la información a través de evaluaciones y monitoreos de sus infraestructuras y servicios. Existen muchos ejemplos que lo demuestran, la evolución constante de las amenazas, el descubrimiento continuo de vulnerabilidades, el aumento de ciberataques y la oferta creciente del cibercrimen como servicio son algunos de ellos.

La utilización de Inteligencia de Fuentes Abiertas (OSINT por sus siglas en inglés Open Source Intelligence) proporciona tácticas, técnicas y herramientas para un uso proactivo en la detección de incidentes.

La inmensa cantidad y variedad de fuentes abiertas disponibles permite adquirir conocimiento de la información que se recopila, analiza y relaciona. El conocimiento adquirido posiciona mejor a las defensas frente a las diferentes amenazas y mejora la visibilidad de las vulnerabilidades que afectan a una organización.

El uso de OSINT en la evaluación de estos riesgos de manera rutinaria puede mejorar la postura de seguridad de las organizaciones, para descubrir vulnerabilidades, mitigar riesgos y establecer políticas de seguridad firmes.

# Objetivos

## Objetivo General

El objetivo general del trabajo es presentar un análisis de OSINT para su utilización en la detección de amenazas y vulnerabilidades y mostrar tácticas, técnicas y procedimientos que pueden ser utilizados para la detección y gestión de incidentes por los equipos de seguridad de la información en las organizaciones.

## Objetivos Específicos

Para llevar a cabo el objetivo planteado se definen los siguientes objetivos específicos:

- Analizar las amenazas y vulnerabilidades más significativas que afectan a las organizaciones.
- Analizar diferentes fuentes de información que pueden ser utilizadas como fuente de inteligencia de amenazas.
- Analizar recursos OSINT disponibles para la detección proactiva de distintas amenazas y vulnerabilidades en una organización.
- Investigar el uso de OSINT para mejorar la capacidad de defensa de una organización.

# Motivación y Estado del Arte

OSINT ha adquirido especial importancia en la actualidad debido a la enorme cantidad de datos expuestos de las personas y las organizaciones en Internet, puede ser utilizado en diferentes ámbitos con distintos objetivos. Por ejemplo, las fuerzas policiales pueden usar OSINT para evaluar posibles relaciones entre las personas investigadas o el periodismo de investigación, para dar con información complementaria que por algún descuido está a la vista de todos.

OSINT incluye información muy variada utilizada para diferentes propósitos. Permite acceder a información relacionada con personas, organizaciones, dispositivos, servicios, organismos, infraestructuras y estados entre otros. Información que se puede obtener de redes sociales como Facebook, Twitter, Instagram, Linkedin o YouTube, de buscadores como Google, Bing, Yahoo o Shodan, denominado el buscador de las cosas, que brinda información de diferentes equipos, como servidores, cámaras, routers, impresoras y distintos dispositivos conectados a Internet.

OSINT también puede ser utilizado para acceder a servicios como “robtex.com”, “netcraft.com”, “centralops.net” o “ipneighbour.com” y obtener información de un dominio o dirección IP. También permite conseguir información de servidores de C&C (command and control servers), una forma de nombrar a los servidores de botnets, la información son listas de reglas de software, como las de Snort o Feeds de información donde se incluyen listas de IP y dominios que deben ser bloqueados para mitigar una determinada vulnerabilidad. Estos son algunos ejemplos de fuentes de información abiertas que forman parte de OSINT y pueden ser utilizados con distintos fines.

En seguridad de la información, OSINT es una temática actual a la cual se hace referencia y se aplica tanto para uso ofensivo como defensivo buscando garantizar la seguridad de las personas y las organizaciones.

Actualmente, las diferentes técnicas, métodos y herramientas de OSINT continúan evolucionando. Conocer las distintas herramientas, métodos y poseer los conocimientos adecuados para obtener los mejores resultados es el punto clave para la utilización y aplicación de OSINT. La búsqueda y vinculación de la información adquiere importancia relevante para las organizaciones, a tal punto que las mismas afectan a dichos procesos a profesionales en OSINT que cuenten con conocimientos para el análisis de altos volúmenes de información.

Diferentes investigaciones, demuestran el interés en la temática OSINT, por ejemplo la Universidad de Lisboa en el año 2018 propone un enfoque automatizado para la detección de amenazas de la red utilizando IDS basados en el conocimiento de OSINT [1].

En el mismo sentido la Universidad de Coimbra, Portugal, presenta en el año 2019 un análisis sobre problemas de seguridad encontrados en PCOM, un protocolo SCADA poco explorado, donde se utiliza OSINT para proporcionar información de las funciones centrales de PCOM [2].

# Capítulo 1 – Vulnerabilidades y Amenazas en las Organizaciones

## Introducción

Las nuevas tecnologías de la información están presentes diariamente en diferentes ámbitos de nuestras vidas brindando solución y soporte para poder realizar diferentes actividades. Muchas veces estas soluciones están enfocadas a cuestiones específicas, sin tener una visión amplia de todo el escenario que acompaña a la misma. En el ámbito de la seguridad de la información esta realidad está presente en la aparición continua de fallas que vuelven vulnerables a los sistemas.
"X-Force Incident Response" e "Intelligence Service (IRIS)", en su reporte "X-Force Threat Intelligence Index 2020" exponen que en el año 2019 se registró un aumento de registros expuestos mayor al 200 % que en el año anterior, los mismos afectaron a más de 8,5 mil millones de ellos [3]. El 86 % de los mismos pudieron ser accedidos a causa de servidores mal configurados, bases de datos inseguras, copias de seguridad no aseguradas correctamente y dispositivos de almacenamiento presentes en segmentos de red abiertos conectados a Internet.
El crecimiento de Internet ha cambiado la forma en que las organizaciones utilizan las tecnologías de la información. Las redes sociales, la computación en la nube, la ubicuidad que brindan los dispositivos móviles son parte de este nuevo escenario utilizado por las mismas en busca de nuevas oportunidades de negocios, reducción de costos y una mayor eficiencia.
Desde el punto de vista de la seguridad de la información estas nuevas oportunidades y la manera en que las organizaciones y sus integrantes hacen uso de la tecnología han provocado que se exponga una inmensa cantidad de información en línea. Esta gran exposición lleva muchas veces a dejar visibles datos sensibles que pueden ser utilizados por actores maliciosos para vulnerar los sistemas, interrumpir servicios o filtrar información. En relación a lo anterior, OSINT puede ser utilizado para mitigar estos riesgos y amenazas [4].

## Vulnerabilidades

El Instituto Nacional de Ciberseguridad (INCIBE) en su blog define una vulnerabilidad como una debilidad o falla en un sistema de información, lo que permite que un actor malicioso pueda comprometer los atributos básicos de la información, integridad, disponibilidad y confidencialidad [5].

En relación a lo anterior Mitre Corporation en el sitio web donde publica y mantiene la lista de Vulnerabilidades y exposiciones comunes, por sus siglas en inglés CVE, define una Vulnerabilidad en seguridad de la información como un error en el software que un actor malicioso puede utilizar para obtener acceso a un sistema o red [6].
En línea con lo anterior podemos definir una vulnerabilidad como una debilidad o falla en un activo, que puede ser aprovechada por un actor malicioso.

## Tipos de Vulnerabilidades

En la Figura 1 se observa la clasificación de vulnerabilidades según su tipo publicada por “CVE Details” en su sitio web (https://www.cvedetails.com/), donde se listan trece tipos diferentes con los totales de vulnerabilidades de cada tipo reportadas desde el año 1999.

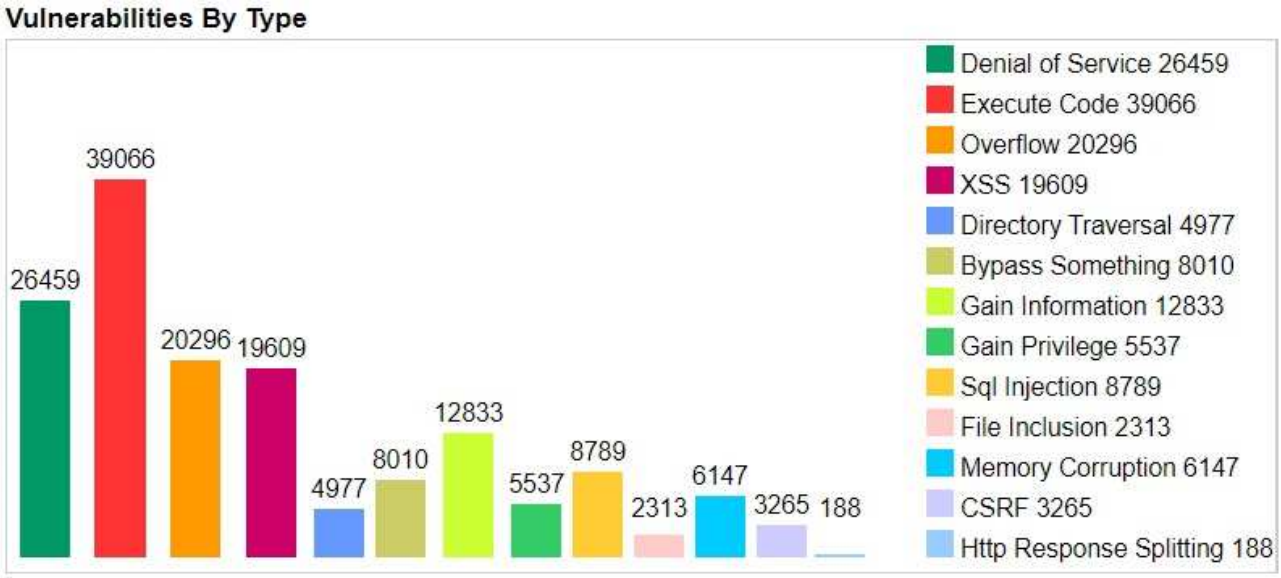



Figura 1: Clasificación de Vulnerabilidades por tipo de CVE Details

**Denegación de servicios (Denial of Service)**: esta vulnerabilidad permite que un actor malicioso provoque en un sistema, servicio o recurso la pérdida de conectividad del mismo o de un tercero dejándolo inaccesible para los usuarios.
**Ejecución de código (Execute Code)**: esta vulnerabilidad permite que un actor malicioso pueda inyectar código y ejecutar comandos en un sistema.
**Desbordamiento (Overflow)**: esta vulnerabilidad puede provocar que un sistema sea bloqueado o que cree un punto de acceso para un actor malicioso.
**Secuencia de comando en sitios cruzados (XSS)**: esta vulnerabilidad permite que un actor malicioso pueda inyectar script, en páginas web que visita el usuario.

**Cruce de directorio (Directory traversal)**: esta vulnerabilidad permite que un actor malicioso pueda acceder a directorios sin validación o control suficiente.
**Evitar control y autenticación (Bypass Something)**: esta vulnerabilidad permite que un actor malicioso pueda eludir los mecanismos de autenticación y control.
**Obtención de información (Gain Information)**: esta vulnerabilidad permite que un actor malicioso pueda tener acceso a información confidencial, como la contenida en el registro del sistema operativo Windows.
**Obtener privilegios (Gain Privilege)**: esta vulnerabilidad permite que un actor malicioso pueda obtener privilegios distintos a los que originalmente tenía, logrando acceso a donde no se le permitía.
**Inyección SQL (SQL Injection)**: esta vulnerabilidad permite que un actor malicioso introduzca sentencias SQL para saltar la validación de las operaciones que se realizan sobre una base de datos.
**Inclusión de archivos (File Inclusion)**: esta vulnerabilidad permite que un actor malicioso incluya archivos en una aplicación web, es provocada por errores de programación en páginas dinámicas.
**Corrupción de memoria (Memory Corruption)**: esta vulnerabilidad permite que un actor malicioso pueda ejecutar código en una aplicación, es provocada por errores de programación que modifican el contenido de alguna ubicación de memoria.
**Falsificación de solicitud entre sitios (CSRF)**: esta vulnerabilidad permite que un actor malicioso pueda obtener datos sensibles de un usuario a través de solicitudes falsas cuando este interactúa con una página web.
**División de respuesta HTTP (Http Response Splitting)**: esta vulnerabilidad permite que un actor malicioso pueda realizar una serie de acciones que pueden comprometer a una aplicación web, es provocada por errores de programación que no realizan un tratamiento adecuado de limpieza de los valores de entrada.

## Vulnerabilidades, métricas y puntuación

Las vulnerabilidades identificadas en Tecnologías de Información reciben un puntaje que se asigna de acuerdo a la gravedad de la misma y es tomado del “Common Vulnerability Score System” (CVSS), el cual permite cuantificar la criticidad de las mismas [7]. El CVSS es administrado por el “Foro Global de Equipos de Seguridad y Respuesta a Incidentes” (FIRST), una organización sin fines de lucro.
La versión actual del CVSS es la 3.1 y de forma similar a sus versiones anteriores utiliza una ecuación predefinida para calcular el puntaje que se asigna a la vulnerabilidad.
El CVSS se forma con tres grupos de métricas, base, temporal y ambiental. A su vez cada una de ellas incluye un conjunto de métricas como se muestra en la figura 2.

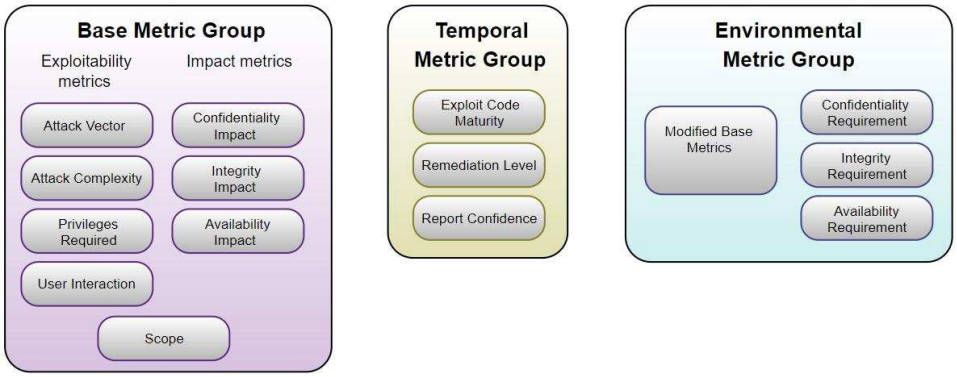



Figura 2: Grupos de Métricas CVSS

**Métricas del grupo base**: son las características específicas de una vulnerabilidad que se mantienen constantes a lo largo del tiempo. Están compuestas por las métricas de explotabilidad y de impacto.

**Métricas del grupo temporal**: son las características de una vulnerabilidad que pueden cambiar a lo largo del tiempo.

**Métricas del grupo ambiental**: son las características relevantes y únicas asociadas al entorno de un usuario en particular.

La Figura 3 ilustra la ecuación base y las métricas que se utilizan para el cálculo de la puntuación que se asigna a las vulnerabilidades. Los valores van desde 0.0 a 10. Al primer valor que se obtiene de la ecuación base, que incluye las métricas de explotación e impacto, se lo puede depurar incorporando las métricas temporales y ambientales que permiten presentar con mayor precisión la gravedad de una vulnerabilidad. Al valor numérico CVSS que se asigna a la vulnerabilidad se suma una cadena denominada “vector string” como se muestra en la figura 3 [7].

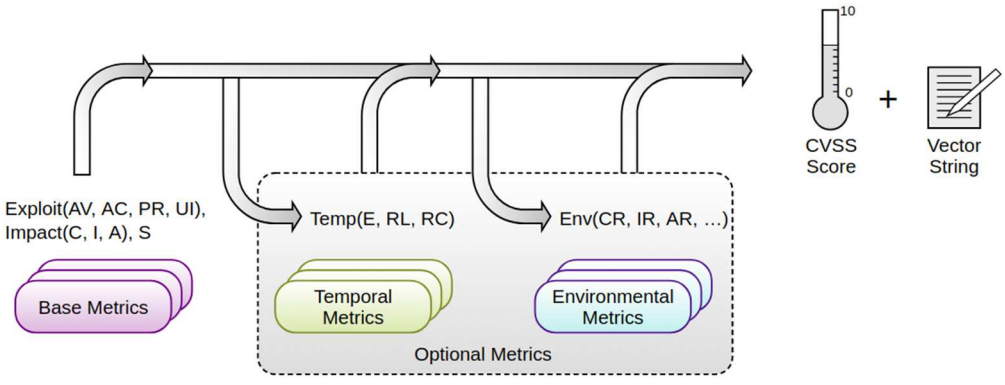



Figura 3: Métricas y ecuaciones CVSS

La puntuación numérica básica, temporal y ambiental permite calificar de forma cualitativa la gravedad de una vulnerabilidad. La Figura 4 muestra la escala de calificación de gravedad cualitativa.

| Clasificación | Puntaje CVSS |
|---|---|
| Ninguno | 0.0 |
| Bajo | 0,1 - 3,9 |
| Medio | 4.0 - 6.9 |
| Elevado | 7,0 - 8,9 |
| Crítico | 9,0 - 10,0 |

Figura 4: Escala de calificación de gravedad cualitativa

## Vulnerabilidades de severidad elevada y crítica

En los últimos años muchas vulnerabilidades han sido reportadas como graves o críticas.
El Boletín de seguridad de Microsoft MS17-010 del 14 de marzo del 2017, hace referencia a una serie de vulnerabilidades encontradas en Microsoft Server Message Block 1.0 (SMBv1) [8]. La lista asociada a este boletín incluye el CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146 y CVE-2017-0148, entre otros. Los CVE mencionados recibieron un puntaje CVSS de 8.1 [9]. Los problemas reportados en SMBv1 fueron aprovechados tiempo después por diferentes versiones de Ramsomware como Petya y WannaCry que utilizaron estas vulnerabilidades y un código de explotación conocido como “EternalBlue” para ejecutar código de forma arbitraria en las computadoras infectadas.
Una vulnerabilidad muy utilizada por actores maliciosos es la identificada como CVE-2017-11882 que afecta a Microsoft Office 2007, 2010 Service Pack 3, 2013 Service Pack 2 y 2016 Service Pack 1 y que permite la ejecución de código arbitrario en el contexto de la memoria del usuario, denominada también como “Vulnerabilidad de corrupción de memoria de Microsoft Office”, la cual recibió un puntaje CVSS de 7.8 [10].
Otra vulnerabilidad grave es la identificada como CVE-2017-0199 que afecta a los productos Microsoft Office 2007 Service Pack 3, 2010 Service Pack 2, 2013 Service Pack 1, Microsoft Office 2016, Microsoft Windows Vista SP2, Windows Server 2008 SP2, Windows 7 SP1, Windows 8.1. Esta vulnerabilidad también se denomina “Vulnerabilidad de ejecución remota de código en Microsoft Office/WordPad con la API de Windows”, la cual recibió un puntaje CVSS de 7.8 [11].
Por último la vulnerabilidad identificada como CVE-2017-8759 que afecta a Microsoft .NET Framework 2.0, 3.5, 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2 y 4.7. Esta vulnerabilidad también se denomina “Vulnerabilidad de ejecución remota de código en .NET Framework”, la cual recibió un puntaje CVSS de 7.8 [12].

Con un puntaje máximo CVSS de 10.0 asignado podemos mencionar el identificador CVE-2017-5638 que hace referencia a una vulnerabilidad en Apache Struts 2 2.3.x y Apache Struts 2 2.5.x, presente en versiones anteriores a la 2.3.32 y a la 2.5.10.1 que permite ejecutar comandos de forma remota utilizando un contenido especialmente diseñado [13].

Otra vulnerabilidad para destacar con puntaje crítico es el identificador CVE-2019-0708 que hace referencia a una vulnerabilidad que permite la ejecución remota de código utilizando los servicios "Remote Desktop Protocol" (RDP) o Servicio de Escritorio Remoto conocido anteriormente como Servicio de Terminal Server, la cual recibió un puntaje CVSS de 9.8 [14].

Algunas de las vulnerabilidades mencionadas se encuentran aún presentes en las organizaciones y aprovechadas por actores de amenazas.

En la Figura 5 perteneciente al reporte "X-Force Threat Intelligence Index 2020" se presentan vulnerabilidades aprovechadas por actores de amenazas durante el año 2019 que se reportaron dos años antes y continuaron siendo utilizadas por los actores de amenazas, informe que evidencia la falta de aplicación de los parches o un atraso en la solución de las mismas en las organizaciones [3].

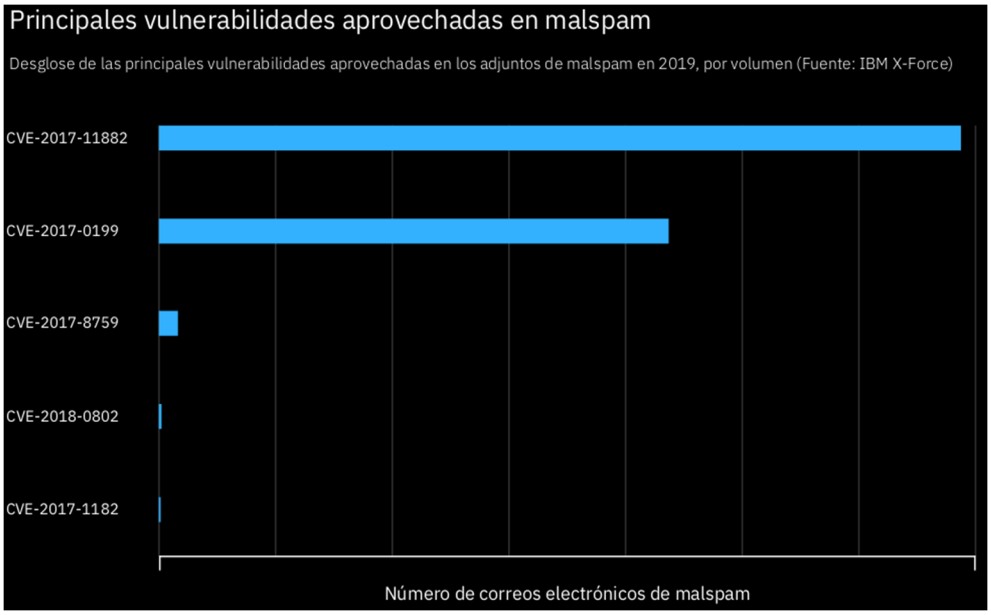



Figura 5: Principales vulnerabilidades aprovechadas en malspam

Los diez CVE Web más críticos reportados por la comunidad "Detectify Crowdsource" durante el año 2020 son [15]:

El identificador CVE-2020-12720, es una vulnerabilidad de inyección SQL encontrada en vBulletin, un software utilizado para crear y administrar sitios web, tiene un CVSS 9.8 y la misma permite a un actor malicioso realizar un ataque Remote Code Execution (RCE) llegando a restablecer la clave del administrador.

El identificador CVE-2020-5902, es una vulnerabilidad que afecta al software F5 BIG-IP, tiene un CVSS de 9.8 y la misma permite la ejecución de comandos y lectura de archivos, lo que podría ser utilizado por un actor malicioso no autenticado para realizar un ataque de Path transversal y lograr acceso a puntos sensibles del sistema pudiendo ejecutar código arbitrario en el mismo.
El identificador CVE-2020-15506, es una vulnerabilidad que afecta al software Mobile Iron Core versión 10.6, tiene un CVSS de 9.8, OWASP top 10 “Autenticación rota”, lo que permite a un actor malicioso omitir la autenticación y obtener acceso a los servicios y el panel de administración.
Los identificadores CVE-2020-14882, CVE-2020-14750 y CVE-2020-2551, son vulnerabilidades que afectan a los productos Oracle WebLogic Server, tienen un CVSS de 9.8 y permiten a un actor malicioso ejecutar comandos arbitrarios enviando una solicitud al servidor. El CVE-2020-2551, afecta a las versiones 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 y 12.2.1.4.0 de Oracle WebLogic Server de Oracle Fusion Middleware.
El identificador CVE-2020-17530, es una vulnerabilidad que afecta a Apache Struts en su versión 2.5.25 o anterior y permite la ejecución remota de código lo cual puede ser utilizado por un actor malicioso para ejecutar comandos en el servidor, tiene un CVSS de 9.8.
El identificador CVE-2020-13379, es una vulnerabilidad que afecta a Grafana, una herramienta Open Source para visualización de datos, tiene un CVSS de 8.2 y el error reportado permite a cualquier usuario no autenticado enviar solicitudes HTTP a cualquier URL y devolver el resultado a un cliente, debido a una vulnerabilidad de falsificación de solicitud en la función del avatar de Grafana.
El identificador CVE-2020-1147, es una vulnerabilidad que afecta a .NET Framework, Microsoft SharePoint y Visual Studio, tiene un CVSS de 7.8 y se encuentra en el proceso de la deserializacion de la entrada del contenido XML que permite a un actor malicioso realizar Remote Code Execution (RCE).
La reportada en el décimo lugar es el identificador CVE-2020-8209, es una vulnerabilidad que afecta a Citrix XenMobile Server 10.12 anterior a RP2, Citrix XenMobile Server 10.11 anterior a RP4, Citrix XenMobile Server 10.10 anterior a RP6 y Citrix XwnMobile Server anterior a 10.9 RP5, tiene un CVSS de 7.5 y permite que un actor maliciosos descargue archivos de forma arbitraria del servidor y realice Remote Code Execution (RCE).

## Evaluación de Vulnerabilidades

Como se mencionó anteriormente el descubrimiento de nuevas vulnerabilidades es continuo. Frente a este escenario una buena práctica es contar con un programa de gestión de vulnerabilidades asociado a controles que permitan probar y garantizar la efectividad del mismo en una organización, teniendo en cuenta que este tipo de evaluaciones pueden identificar vulnerabilidades conocidas aun sin parchear y configuraciones por defecto entre otras malas prácticas. La evaluación de

vulnerabilidades permite la revisión de los sistemas y sus parches para confirmar la existencia de las mismas frente a falsos positivos, permitiendo además a las organizaciones conocer cómo se ve la superficie que exponen.

En el mismo sentido resulta fundamental crear conciencia de seguridad en el personal para mitigar debilidades en el factor humano implementando programas de formación en seguridad con el objetivo de establecer una cultura de seguridad en los integrantes que forman parte de las organizaciones.

## Amenazas

El Instituto Nacional de Ciberseguridad (INCIBE) en su blog define una Amenaza a toda acción que aprovecha una vulnerabilidad para atentar contra un sistema de información [5].

También podemos definir una amenaza como una violación potencial de la seguridad en donde la misma busca sacar ventaja de vulnerabilidades y malas prácticas.

En la Figura 6 se presentan las principales amenazas consideradas por ENISA (European Union Agency For Cybersecurity) en su informe denominado “ENISA Threat Landscape 2020 - List of top 15 threats” [16].


Figura 6: List of top 15 threats ENISA 2020

## Principales Amenazas

Una clasificación de las principales amenazas es la presentada por ENISA en su lista, clasificándolas de la siguiente manera:

**1 - Malware**. Este tipo de amenaza la integra software malicioso del tipo virus, gusanos, spyware, ransomware, cripto mineros y otros, tienen como objetivo robo de información, corrupción de datos, espionaje e interrupción de servicios, entre otros. Este tipo de amenaza también presentes como "Malware as a service" (MaaS) son ofrecidos como Tool Kits. Otra variante muy poderosa de este tipo de amenazas es el denominado Malware sin archivo ejecutable, donde el actor malicioso una vez que logra inyectar código en un host utiliza herramientas propias del sistema como por ejemplo "Windows Managment Instrumentation (WMI) o PowerShell para ganar persistencia a través del registro o el programador de tareas del Sistema Operativo.

En la Figura 7 se muestran los porcentajes de eventos sin archivos detectados por Norton durante el primer semestre del 2019.

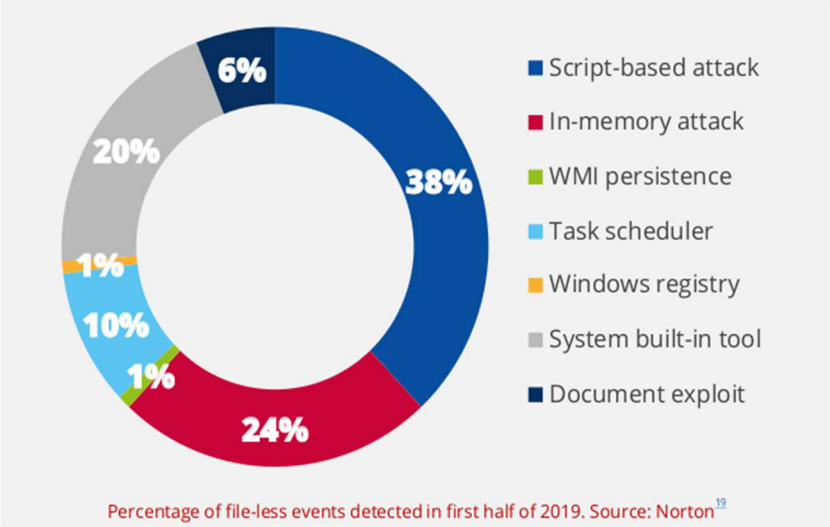



Figura 7: Eventos sin archivos - List of top 15 threats ENISA 2020

En la Figura 7 se observa que los ataques basados en script tienen la mayor incidencia en este tipo de amenazas con el 38%, seguido por los ataques en memoria con el 24%, herramientas incorporadas en el sistema con el 20%, programador de tareas 10%, exploit de documentos con el 6 % y el resto con el 1%.

**2 - Ataques basados en web (Web Based Attacks)**. Este tipo de amenazas incluyen la utilización de URLs y script maliciosos para redirigir al usuario a un sitio determinado, provocar la descarga de Malware o inyectar código en sitios web legítimos para robar credenciales entre otras acciones posibles. Forman parte de las mismas los vectores denominados como "Drive by Downloads", "Formjacking ", "Malicious URL" y "Watering hole attacks", que incluyen técnicas como inyección

SQL, manipulación de parámetros, secuencia de comandos entre sitios, path transversal y fuerza bruta como parte de los mismos.

**3 - Phishing**. Este tipo de amenaza incluye mensajes de correo electrónico con enlaces maliciosos o archivos adjuntos utilizando técnicas de ingeniería social para engañar al usuario con la intención de lograr que abra el contenido adjunto o ejecute un enlace incluido intencionalmente en el cuerpo del mensaje. Spear phishing es una de las técnicas más utilizadas por los actores maliciosos para obtener acceso inicial, combinado con una gran variedad de tácticas de ingeniería social.

**4 - Ataques a aplicaciones web (Web Application Attacks)**. Este tipo de amenaza incluye la inyección SQL, abuso de la API de PHP 7 y autenticación fallida, entre otras técnicas. El Open Web Application Security Project (OWASP) mantiene una lista de los 10 errores más relevantes en aplicaciones web, los cuales pueden ser utilizados por los actores de amenazas.

En la Figura 8 se presentan los principales vectores en relación a las amenazas contra las aplicaciones web.

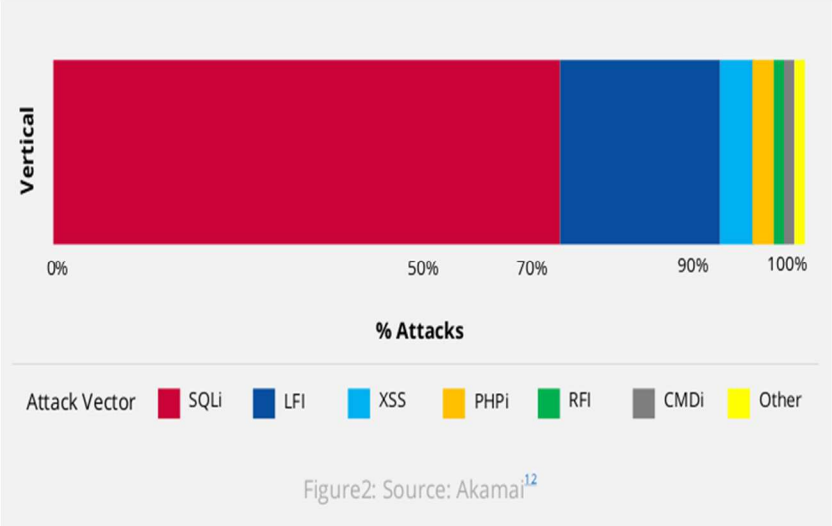



Figura 8: Vectores de ataque a aplicaciones web - List of top 15 threats ENISA 2020

En la Figura 8 se observa que el principal vector es la inyección SQL (SQLi), seguido por la inclusión local de archivos (LFI), ejecución de comandos en sitios cruzados (XSS), PHPi, inclusión remota de archivos (RFI) y otros.

**5 - Spam**. El spam es considerado una amenaza cuando es utilizado como un vector de ataque basado en el envío masivo de mensajes que no han sido solicitados. A veces se confunde el spam con las campañas de phishing lo cual se diferencia del spam al ser dirigida y hacer uso de la ingeniería social. La Figura 9 muestra los orígenes más significativos de las campañas de Spam.

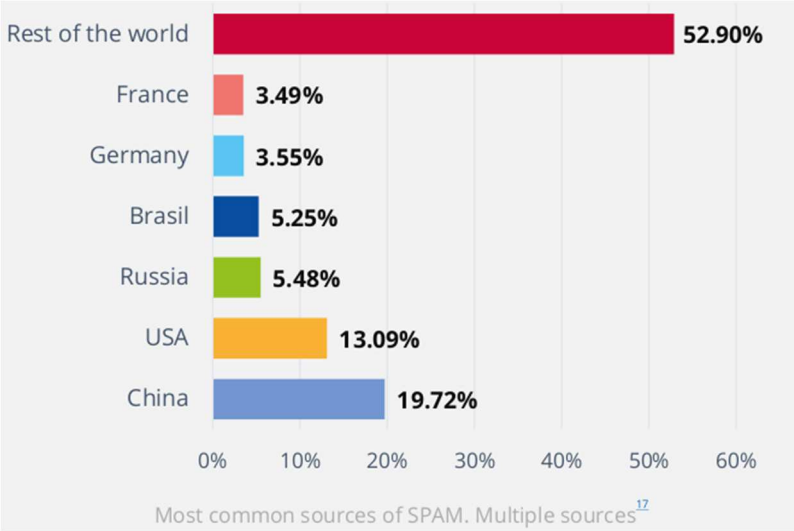



Figura 9: Orígenes del Spam - List of top 15 threats ENISA 2020

En la Figura 9 se observa que China tiene el mayor porcentaje de campañas de distribución de spam con un 19,72%, seguido de USA con el 13,09%, Rusia 5,48%, Brasil con el 5,25%, Alemania con el 3,55%, Francia con el 3,49% y el resto con el 52,90%.

**6 - Denegación de servicio distribuida (DDoS)**. Este tipo de amenaza sobrecarga el tráfico hasta interrumpir servicios. El gran aumento de dispositivos conectados y el crecimiento de IoT entre otros, son aprovechados por los actores de amenazas y utilizados para DDoS a través de la actividad de las Botnets, grupo de dispositivos infectados y controlados por un actor malicioso de forma remota, entre otros. Los principales ataques DDoS utilizan el envío masivo de paquetes SYN (SYN Flood). El protocolo de descubrimiento dinámico de servicios web (WS-Discovery), utilizado principalmente en dispositivos IoT. La utilización de UDP para amplificación, falsificando IP y host del remitente y DDoS multi-vector, técnica en la cual los actores de amenazas utilizan automatización y diferentes capas como aplicación y red con HTTP Flood, DNS Flood y  Amplificación con UDP entre otras. La Figura 10 muestra la distribución por tipo de ataques de DDoS.

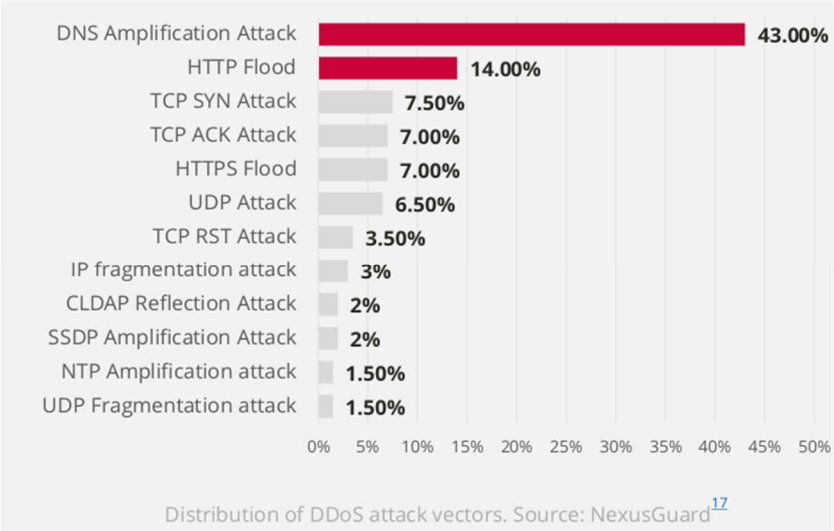



Figura 10: Distribución de vectores de ataques DDoS - List of top 15 threats ENISA 2020

En la Figura 10 se observa que el principal vector de ataque de DDoS según “List of top 15 threats ENISA 2020” es la amplificación de DNS con el 43,00%, seguido de la inundación HTTP con el 14,00%, TCP SYNC con el 7,50%, TCP ACK y HTTPS Flood con el 7,00%, ataques basados en UDP con el 6,50%, TCP RST con el 3,50%, fragmentación IP con el 3%, reflexión CLDAP y amplificación SSDP con el 2% y amplificación NTP junto a fragmentación UDP con el 1,50%.

**DDoS basados en UDP**. Por su estructura UDP es un protocolo no orientado a conexión donde no se valida la dirección IP origen:

- En él no hay “handshake” (Intercambio de información privada).
- Los segmentos son independientes.
- A cada mensaje de la aplicación le corresponde un segmento.

Estas características de UDP han llevado a que algunos protocolos de la capa de aplicación sean utilizados como vector de ataque. A continuación se describen algunos de los protocolos utilizados en ataques basados en UDP [17]:

- **DNS (Domain Name System)**: El sistema de nombres de dominio es un conjunto de protocolos y servicios que permiten resolver nombres de dominios a direcciones IP. Utiliza por defecto el puerto 53, se encapsula en UDP y ocasionalmente en TCP. La alerta (TA13-088A) indica que el proyecto “Open DNS Resolver Project” sostiene que de los 27 millones de resolutores DNS conocidos en Internet, cerca de 25 millones representan un riesgo de ser utilizados en un ataque [18]. DNS puede ser utilizado para realizar DDoS mediante la utilización de servidores abiertos con acceso público. Los actores de amenazas pueden enviar solicitudes a un servidor DNS recursivo abierto usando la técnica conocida como suplantación de IP, la cual consiste en crear paquetes con la dirección IP de origen falsa para ocultar la identidad del emisor y enviar solicitudes falsas a un servidor con la dirección IP de origen alterada, reemplazada por la dirección IP del objetivo. Las solicitudes falsas

buscan obtener la mayor cantidad de información posible de una zona para lograr un mayor efecto de amplificación en la respuesta.

- **NTP (Network Time Protocol)**: El protocolo de tiempo de red utiliza por defecto el puerto 123 UDP, permite realizar consultas a un servidor mediante el comando “monlist”, este comando se encuentra habilitado por defecto en servidores NTP con versiones anteriores a la 4.2.7. Los actores de amenazas abusan de servidores NTP vulnerables enviando solicitudes “get monlist” con la dirección origen modificada y en reemplazo introducen la dirección de la víctima. Ha sido utilizado para ataques de amplificación y reflexión usando la técnica conocida como suplantación de IP, logrando factores de amplificación hasta 200 veces mayor con un tráfico estimado de 300 Gbps como los registrados contra CloudFlare y Spamhaus [19]. La consulta a un servidor vulnerable crea una lista con las 600 últimas direcciones IP que se conectaron al mismo y la envía a la víctima [20].
- **CLDAP (Connection-less Lightweight Directory Access Protocol)**: El protocolo ligero de acceso a directorios sin conexión es la alternativa a LDAP de Microsoft, definido originalmente en el RFC 1798 y luego reemplazado por la RFC 3352. CLDAP utiliza UDP a diferencia de LDAP que lo hace sobre TCP, ambos en el puerto por defecto 389. Los actores de amenazas pueden abusar de CLDAP para DDoS mediante reflexión utilizando la técnica conocida como suplantación de IP.

  En 2016 el centro de operaciones de seguridad (SOC) de Akamai identificó las primeras operaciones utilizando este método de amplificación y reflexión. En febrero de 2020 Amazon Web Services fue el objetivo de un ataque que utilizó servidores CLDAP, el mismo alcanzó un máximo de 2.3 Tbps y tuvo una duración de tres días transformándose en uno de los mayores ataques de DDoS conocidos hasta el momento.
- **Memcached**: es un sistema distribuido utilizado en servidores, permite guardar datos en memoria RAM con el objetivo de acelerar las respuestas. Utilizado por servicios de Internet como Facebook, Twitter y Youtube entre otros.

  En los últimos años Memcached ha sido utilizado como vector de ataque en diferentes incidentes. Informes publicados en el blog de Akamai expresan que los actores de amenazas han abusado de las funcionalidades del sistema enviando tráfico UDP a través del puerto 11211 y obteniendo paquetes UDP de respuesta con una longitud de 1.400,- bytes con factores de amplificación cercanos a 1 Gbps por reflector [21].

  La Figura 11 muestra el número de servidores Memcached listados por Shodan en 2018, año en que se registraron ataques de gran magnitud como el realizado contra GitHub con picos de tráfico entrante de 1.35 Terabits por segundo (Tbps) en el primer ataque y de 1.7 Tbps en el segundo [22] [23].


Figura 11: Servidores Memcached listados por Shodan en 2018

- **WS-Discovery (Web Services Dynamic Discovery)**: El protocolo de descubrimiento dinámico de servicios web es utilizado para localizar servicios de red y facilitar el descubrimiento y la conectividad, por defecto utiliza el puerto 3702 TCP y UDP y la dirección IP de multidifusión 239.255.255.250.

  WS-Discovery está presente en una amplia variedad de productos como impresoras, cámaras CCTV y DVR entre otros. Destinado a brindar funciones similares a otras tecnologías implementadas en hardware de consumo como Simple Service Discovery Protocol (SSDP) y Universal Plug and Play (UPnP) también utilizadas en ataques DDoS a causa de implementaciones deficientes.

  La debilidad radica en la posibilidad de falsificar las solicitudes sobre UDP, sin estado, logrando que se envíen respuestas a un objetivo consumiendo grandes cantidades de ancho de banda. Los dispositivos IoT mal implementados son de uso común en este tipo de ataques DDoS.

  En 2019 el centro de operaciones de seguridad (SOC) de Akamai identificó un vector de ataque que utiliza un método de amplificación y reflexión que abusa del descubrimiento dinámico de servicios web (WSD). Informes publicados en el blog de Akamai sitúan a WSD en el cuarto lugar en la tabla de clasificación de ataques DDoS debido a su elevado factor de amplificación reflejado [24].
- **Chargen (Character Generator Protocol)**: El protocolo generador de caracteres fue diseñado para fines de prueba y medición, definido en la RFC 864. Utiliza el puerto 19 TCP o UDP, sobre UDP el servidor devuelve un datagrama con un número aleatorio de caracteres (de 0 a 512) cada vez que recibe un datagrama desde el host [25]. Chargen con un factor de amplificación de ancho de banda de 358,8 en caso de estar habilitado puede ser usado para ataques de DDoS.

- **QOTD (Quote of the Day)**: El protocolo de “Cita o frase del día” pertenece al grupo de protocolos de comunicaciones de Internet. Permite al administrador de un sistema establecer un mensaje o frase del día, por defecto utiliza el puerto 17 [26]. QOTD con un factor de amplificación de ancho de banda de 140,3 en caso de estar habilitado puede ser usado para ataques de DDoS.
- **SSDP (Simple Service Discovery Protocol)**: El protocolo de descubrimiento de servicios es utilizado para el descubrimiento de dispositivos UPnP en una red. Utiliza por defecto el puerto 1900 UDP en unicast o multicast. SSDP con un factor de amplificación de ancho de banda de 30,8 en caso de estar habilitado puede ser usado para ataques de DDoS.

**Proyección de DDoS:** La Figura 12 muestra las predicción de Cisco relacionada con la evolución de los ataques de DDoS hacia el año 2023, en la misma se muestra un incremento proyectado de 7.9 millones en 2018 a 15.4 millones para 2023 [27].

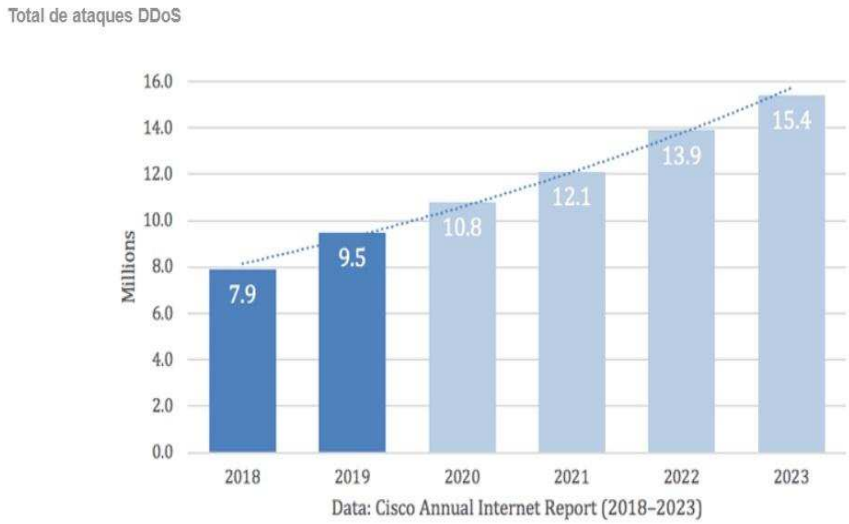



Figura 12: Proyecciones de Cisco en ataques DDos para 2023

DDoS es un vector tradicional utilizado para intentar quebrantar la disponibilidad de servicios y recursos en línea con el propósito de afectar el normal funcionamiento de los mismos, aun así su detección temprana constituye un desafío crítico para las organizaciones debido al abuso continuo de nuevas tecnologías utilizadas por los actores de amenazas.

La velocidad en la detección y respuesta es un factor clave para mitigar los ataques y frustrar a los actores de amenazas que utilizan esta estrategia volumétrica. En este contexto resulta de vital importancia la implementación de soluciones de seguridad proactivas.

**7 - Robo de identidad (Identity Theft)**. Este tipo de amenaza ha sido reportada en los últimos tiempos con incidentes relacionados a distinto tipo de entidades como el sucedido en marzo de 2019 con la violación de datos de los clientes de Capital One, el incidente relacionado al servicio Mixcloud en el cual se comprometieron 20 millones de cuentas, la violación de datos de usuarios

de Uber en noviembre de 2019 y el robo de 9 millones de registros personales de clientes de EasyJet son algunos ejemplos.

En la Figura 11 se muestran los pasos que se llevan a cabo para realizar la estafa fiscal conocida como “Dirty Dozen” que ocurre contra el Servicio de Impuestos Internos en Estados Unidos donde se utiliza el robo de identidad.

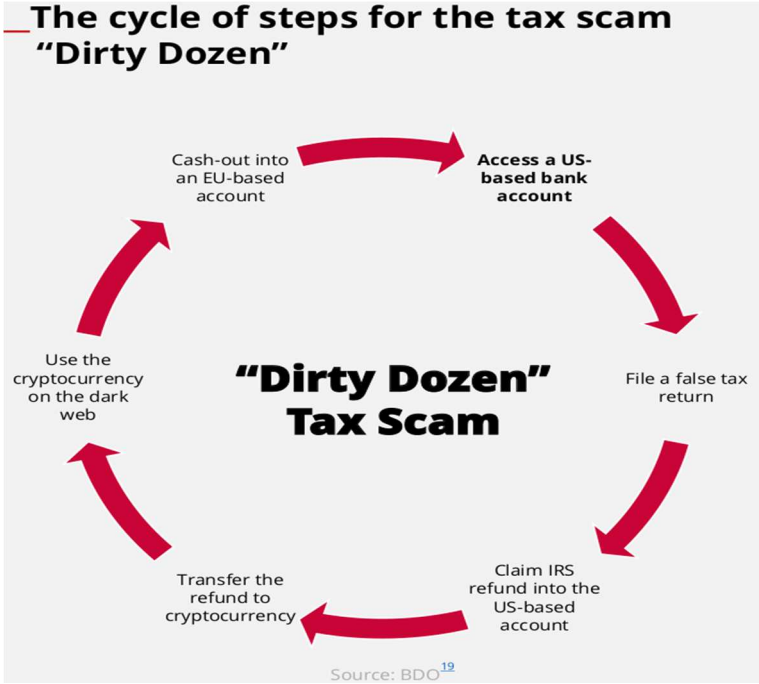



Figura 11: El ciclo de la estafa “Dirty Dozen” - List of top 15 threats ENISA 2020

Para acceder a datos personales y lograr la suplantación los actores de amenazas utilizan diferentes vectores y técnicas como el uso de URL de Phising, Spear Phising, la nube como interfaz de captura para datos de los clientes, la suplantación de marca y tarjetas de regalo troyanisadas utilizadas como correo electrónico comercial entre otras.

**8 - Filtración de datos (Data Breach)**. Este tipo de amenaza busca el acceso sin autorización a un sistema de información y generalmente con intenciones maliciosas, también puede ser provocada por errores humanos no intencionales que ocurren durante la configuración e implementación de algún servicio o sistema. Según estudios una organización demora en promedio 206 días para detectar una violación de datos y el impacto financiero que provoca puede permanecer durante dos años.

En la Figura 12 se muestran los diferentes tipos de datos expuestos a causa de las filtraciones.

| Type of data | 2019 | 2018 | 2017 |
|---|---|---|---|
| E-mail | 70 | 44 | 32 |
| Password | 64 | 39 | 27 |
| Name | 23 | 37 | 41 |
| Miscellaneous | 18 | 19 | 15 |
| Social security number | 11 | 22 | 27 |
| Credit card | 11 | 16 | 19 |
| Address | 11 | 22 | 30 |
| Account | 10 | 7 | 4 |
| Unknown | 8 | 13 | 18 |
| Date of birth | 8 | 13 | 12 |
| Medical | 5 | 9 | 7 |
| Financial | 5 | 13 | 19 |

Source: Cyber Risk Analytics[8]

Figura 12: Tipos de datos expuestos por filtraciones - List of top 15 threats ENISA 2020

En la Figura 12 se observa que los datos relacionados al correo y las contraseñas son los más expuestos en las filtraciones durante los años 2017, 2018 y 2019.

Esta amenaza incluye filtraciones en sistemas de bases de datos que pueden exponer información ya sea por estar mal configurados o presentar vulnerabilidades. A continuación se describen algunos ejemplos de estos sistemas con diferentes problemáticas:

- **MongoDB**: es un sistema de base de datos orientado a documentos, basado en colecciones de documentos Json, permite manejar grandes volúmenes de datos con gran velocidad y escalabilidad. Este sistema tiene productos gratuitos y de pago, en su producto gratuito no posee seguridad de forma predeterminada y acepta conexiones externas a la red local en el puerto 27017, por lo cual requiere configuraciones de seguridad adicionales para evitar que el sistema quede expuesto a posibles acciones maliciosas [28].
- **Elasticsearch**: es un sistema que permite indexar grandes volúmenes de datos y luego hacer consultas sobre los mismos a través de una interfaz REST recibiendo y enviando los datos en formato Json. No admite la autenticación de forma predeterminada y no restringe el acceso a los datos, por lo cual requiere configuraciones de seguridad adicionales si se va a exponer a Internet de manera tal de bloquear los accesos y realizar controles de seguridad de forma periódica [29].
- **DB2**: este sistema en sus versiones para Unix, Linux y Windows puede exponer información y permitir que se envíe información de forma arbitraria al Fast Communications Manager (FCM) y provocar la denegación de servicios del servidor. En configuraciones single node el sistema no es vulnerable, pero sí lo es cuando la base de datos está particionada en diferentes nodos y utiliza FCM para la comunicación entre los mismos en el puerto 523 [30].

**9 - Amenaza interna (Insider Threat)**. Este tipo de amenaza puede provocar incidentes por acciones que realizan personas o grupos pertenecientes a una organización. Existen patrones relacionados con las mismas, de los cuales podemos mencionar el “Uso indebido de privilegios”, además el mal uso de la información por desconocimiento o descuido puede provocar un incidente. Las amenazas internas se pueden clasificar según su objetivo en:

1. Empleados que realizan un manejo inadecuado de la información o violan las políticas de uso, por ejemplo instalando aplicaciones sin autorización.
2. Empleados que roban información para terceros.
3. Empleados descontentos que buscan causar un daño en la organización.
4. Empleados malintencionados que abusan de los privilegios para beneficio personal.
5. Terceros con acceso a información de una organización que realizan un uso indebido de la misma, accesos malintencionados o abuso de un activo.

La Figura 13 muestra los activos de IT vulnerables a amenazas internas.

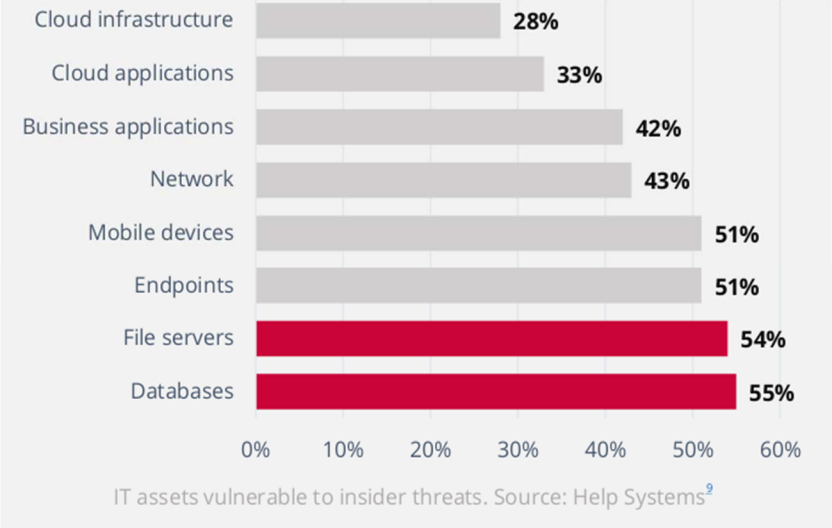



Figura 13: Activos vulnerables a las amenazas internas - List of top 15 threats ENISA 2020

En la Figura 13 se observa que los activos de IT más afectados por las amenazas internas son las bases de datos con el 55%, seguidas por los servidores de archivos con el 54%, EndPoints y dispositivos móviles con el 51%, las redes de datos con el 43%, las aplicaciones de negocio con el 42% y las aplicaciones e infraestructura en la nube con el 33% y 28% respectivamente.

En la Figura 14 se muestran las áreas donde las amenazas internas tienen mayor impacto en las organizaciones.

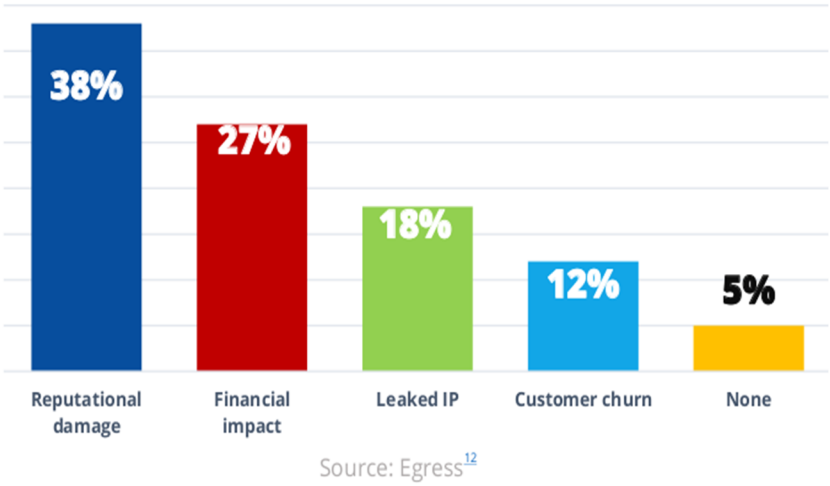



Figura 14: Áreas más afectadas por amenazas internas - List of top 15 threats ENISA 2020

En la Figura 14 se observa que el daño a la reputación es donde los incidentes provocados por amenazas internas causan mayor impacto con un 38%, seguido por el impacto financiero con el 27%, filtrado IP con el 18%, pérdida de clientes con el 12% y otros con el 5%.

**10 - Botnets**. Este tipo de amenaza puede provocar denegación de servicios, operaciones de fraude electrónico, minería de criptomonedas, distribución de ransomware y otros.

Son dispositivos infectados con malware que conforman una red, son controlados de forma remota y pueden operar de forma sincronizada y automatizada.

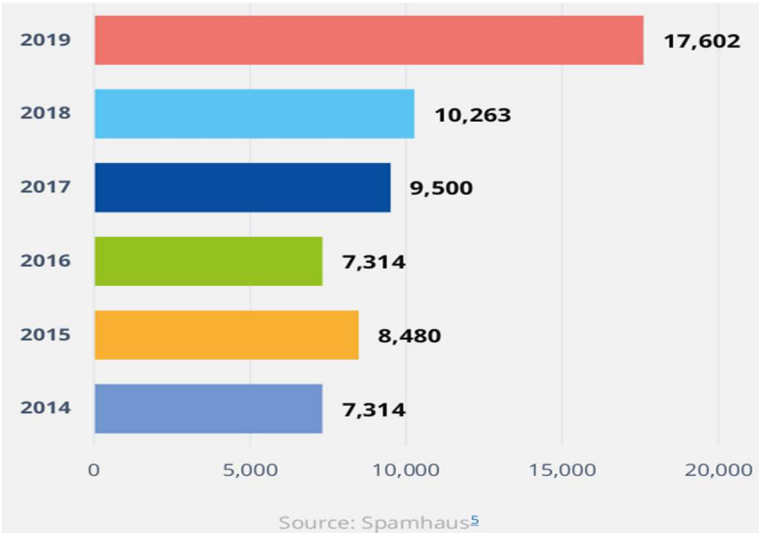



Figura 15: Servidores C2 de Botnet entre 2014 y 2019 - List of top 15 threats ENISA 2020

En la figura 15 se presenta el número de servidores C2 de Botnet observados entre 2014 y 2019 donde se ve un aumento creciente de esta amenaza particularmente a partir del año 2017.

**11 - Manipulación física, daño, robo y pérdida (Physical manipulation/ damage/ theft/ loss)**. Este tipo de amenaza involucra toda posible violación a la seguridad física en las organizaciones,

Algunos ejemplos de este tipo de amenaza son:

- La rotura de cajeros automáticos usando explosivos, mecanismos para captura de tarjetas, trampa de efectivo o elementos contundentes para dañarlos y lograr acceso al dinero.
- La conexión de dispositivos USB, denominados “USB Killer” para obtener una puerta trasera para acceso a un sistema.

**12 - Filtración de Información (Information Leakage)**. Este tipo de amenaza puede comprometer la confidencialidad, disponibilidad o integridad de la información de una organización, muchas veces son causadas por integrantes de la organización o por errores en los procesos de la misma.

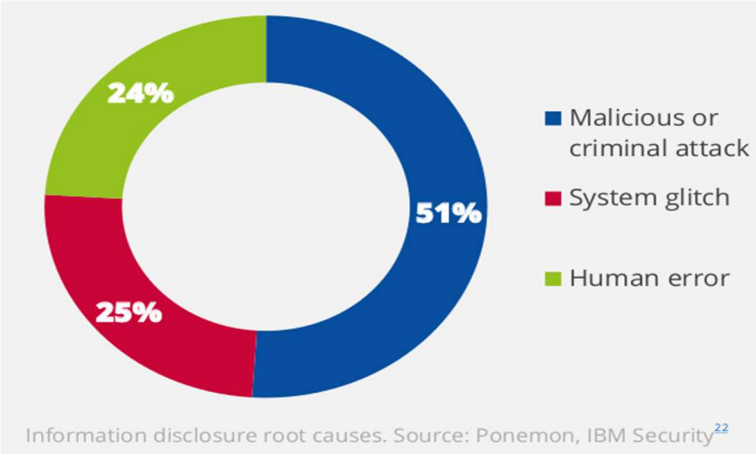
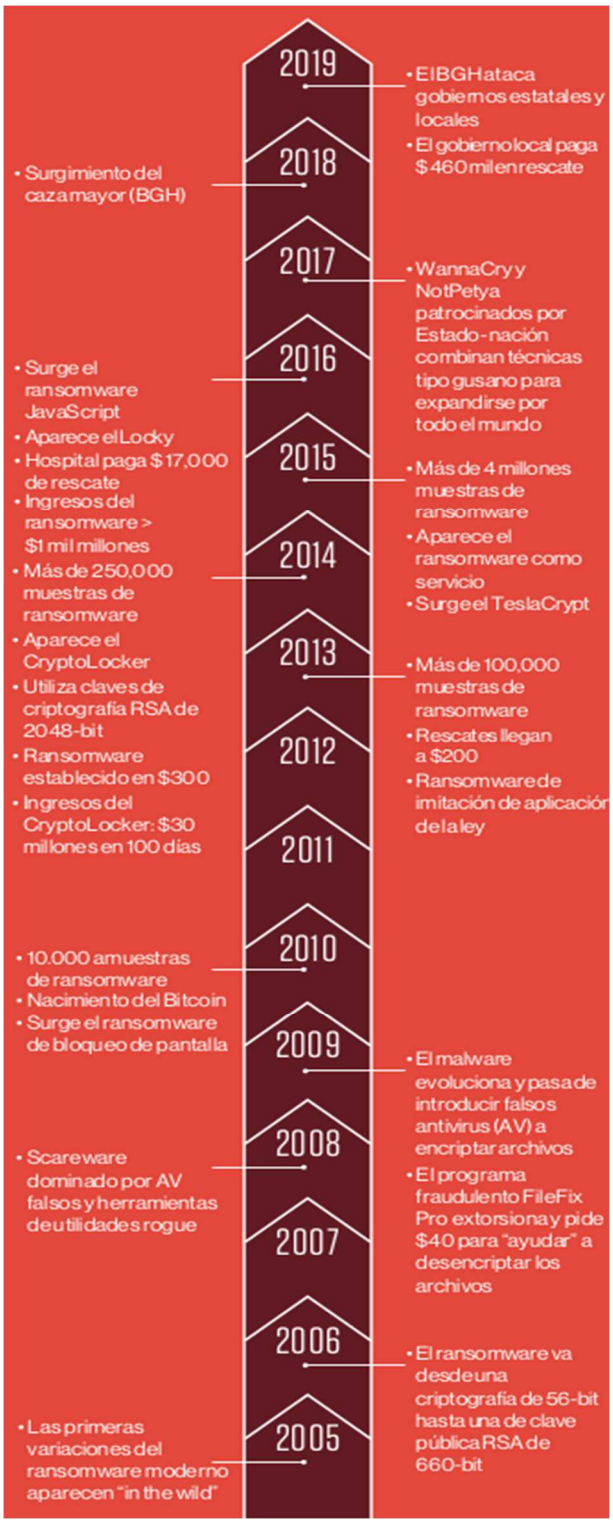



Figura 16: Principales causas de divulgación de información - List of top 15 threats ENISA 2020

En la Figura 16 se muestran los porcentajes de las principales causas de divulgación de información donde los ataques maliciosos ocupan el 51%, seguido por fallas del sistema con el 25% y los errores humanos con el 24%. El vector principal para provocar este tipo de incidentes son los mismos integrantes de las organizaciones, personas con acceso a información relevante interesada en exfiltrar la misma para un tercero, otros vectores también utilizados son vulnerabilidades sin resolver, errores humanos y configuraciones incorrectas entre otros.

**13 - Ransomware**. Esta es una amenaza creciente que ha generado incidentes que llegaron a paralizar ciudades. Pasaron de ser incidentes al azar a ser dirigidos a grandes organizaciones combinando tácticas, técnicas y procedimientos (TTPs). Los vectores más utilizados por esta amenaza incluyen los correos electrónicos de phising, los pop-ups de páginas web, el uso de vulnerabilidades conocidas como las explotadas en SMB, RDP y el denominado Ransomware sin archivos. Para protegerse es primordial que las organizaciones realicen copias de seguridad y las protejan en un entorno seguro y separado, mantengan los sistemas actualizados y parcheados, capaciten regularmente a los usuarios finales y cuenten con un plan de respuesta a incidentes.

En la Figura 17 se muestra una tabla con la evolución del Ransomware y las variantes de mayor impacto a lo largo del tiempo presentado por “Crowdstrike” en su reporte denominado “La evolución del ransomware” [31].




Evolución del Ransomware moderno

Ransomware de mayor impacto

Figura 17: Ransomware, evolución y variantes - “Crowdstrike - La evolución del ransomware”

**14 - Espionaje cibernético (Cyber espionage)**. De acuerdo a informes recientes es una amenaza en crecimiento que afecta a los sectores industriales, infraestructuras críticas, gobiernos, empresas de energía, telecomunicaciones, hospitales y bancos entre otros, se centra en la filtración de secretos comerciales e información estratégica.

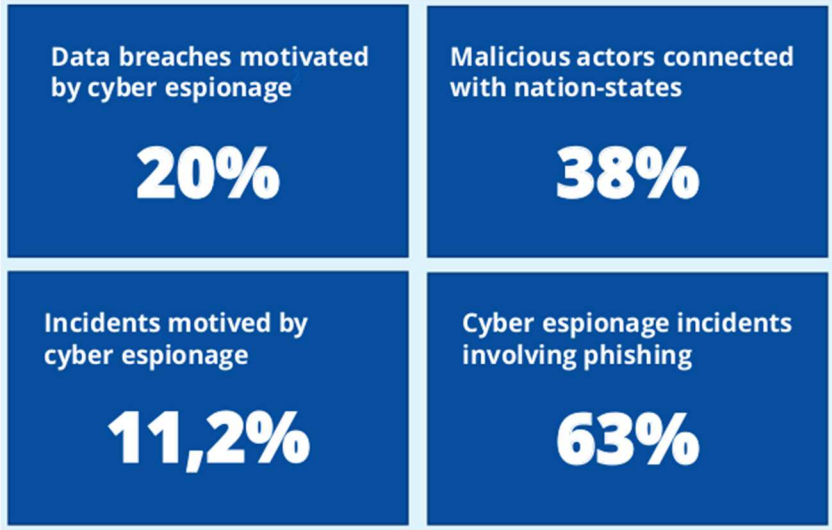



Figura 18: Incidentes que involucran al Espionaje cibernético - List of top 15 threats ENISA 2020

En la Figura 18 se presentan los porcentajes de distintos incidentes relacionados con la amenaza del espionaje cibernético. El mayor porcentaje es ocupado por los incidentes de ciberespionaje que incluyen phishing con un 63%, seguido por los provocados por actores maliciosos vinculados a estados con un 38%, violaciones de datos motivadas por el ciberespionaje con el 20% y otros incidentes motivados por el ciberespionaje con el 11,2%,

**15 - Cryptojacking**. Esta amenaza consiste en el uso no autorizado de un recurso para minar criptomonedas, también se lo denomina “Cryptomining” y los recursos que pueden ser utilizados incluyen computadoras y teléfonos móviles, aunque una tendencia creciente muestra que los actores de amenazas están cada vez más interesados en las infraestructuras en la nube. Los actores de amenazas también utilizan la criptominería basada en archivos combinada con diferentes tipos de malware y herramientas adicionales para extraer información de los recursos infectados.

Los vectores utilizados por esta amenaza incluyen entrega de malware con capacidades de criptojaking, infección de sitios web, distribución a través de redes sociales, tiendas de aplicaciones, aplicaciones para móviles, Kits de explotación, publicidad maliciosa y medios extraíbles entre otros.

En la Figura 19 se listan diferentes variantes de Malware de criptominería.

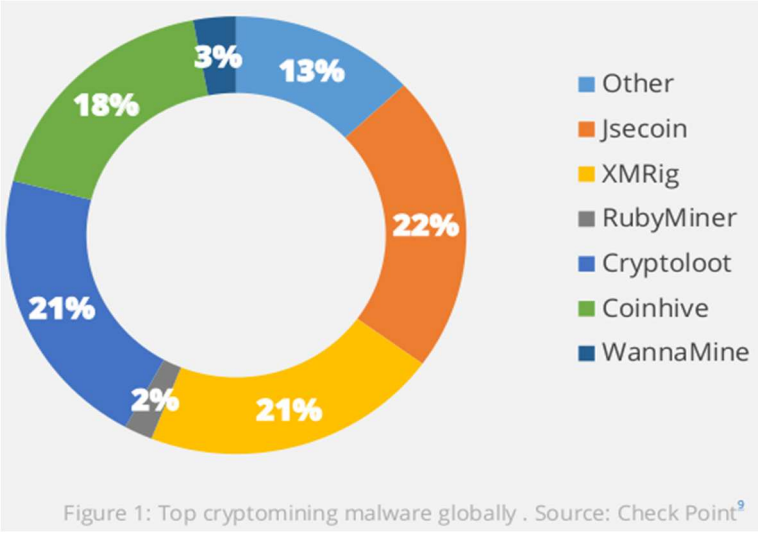



Figura 19: Malware de criptomineria a nivel mundial - List of top 15 threats ENISA 2020

En la Figura 19 se presentan los porcentajes ocupados por las variantes de mayor impacto de malware de criptomineria donde Jsecoin ocupa el 22%, seguido por Cryptoloot y XMRig con el 21%, Coinhive con el 18%, WannaMine con el 3%, RubyMiner el 2% y otras variantes con el 13%.

## Tácticas y técnicas del adversario

Las diferentes tácticas, técnicas y procedimientos (TTP), que utilizan los actores de amenazas, han sido reunidas, clasificadas, descritas y publicadas por “Mitre Corporation” en una base de conocimiento conformada por tres matrices denominada, “MITRE ATT&CK” [32].

- Matriz para empresas, actualmente describe 14 tácticas con sus respectivas técnicas y sub técnicas conformadas por más de trescientas de ellas.

- Matriz para dispositivos móviles Android y iOS describe 14 tácticas y más de un centenar de técnicas y sub técnicas.

- Matriz para sistemas de control industrial describe 11 tácticas con sus respectivas técnicas.

## MITRE ATT&CK: Matriz Empresarial

De las tres matrices mencionadas, a los efectos del presente trabajo se analiza la Matriz para empresas la cual describe técnicas y sub técnicas incluidas en la táctica de Reconocimiento que utilizan recursos OSINT. En la Figura 20 se presenta la “Matriz ATT&CK para empresas”.

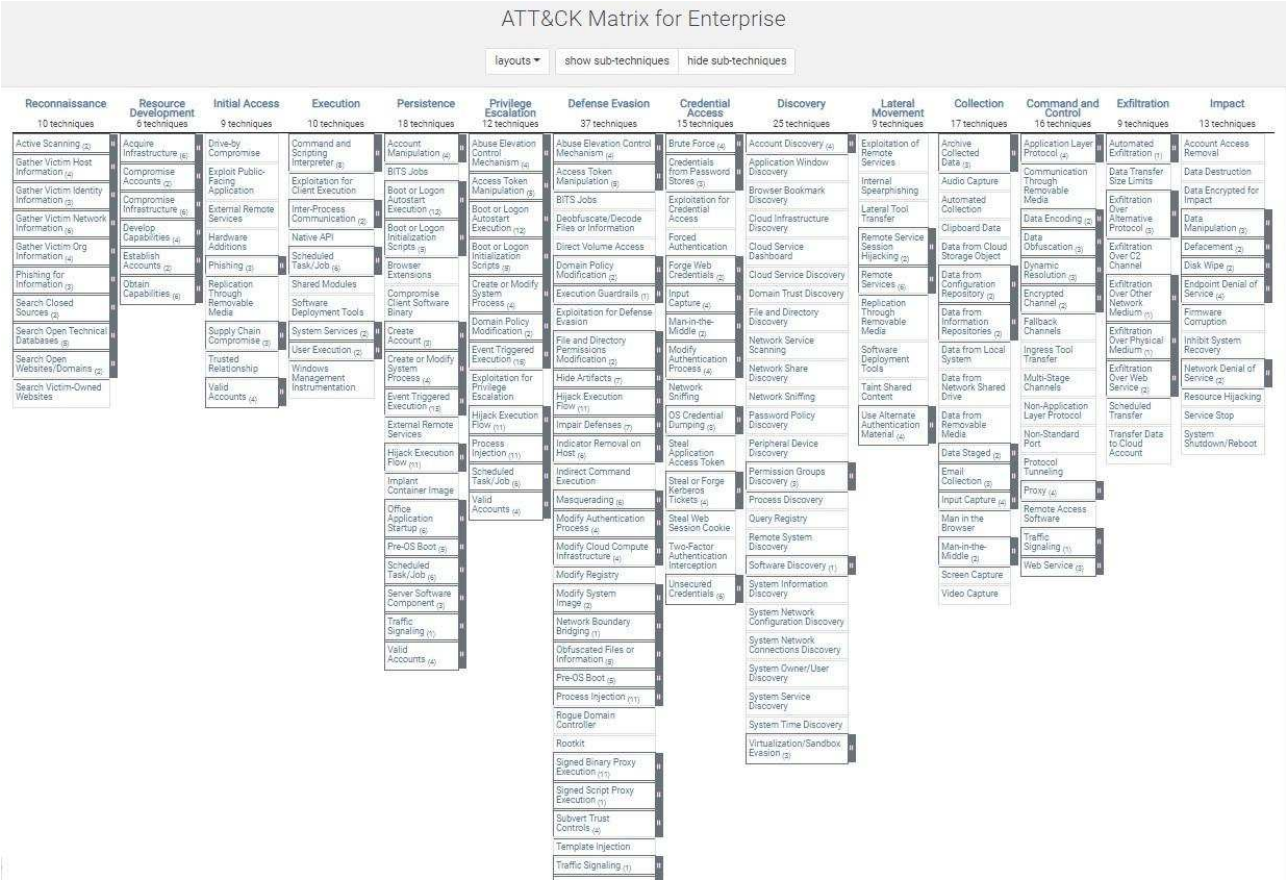



Figura 20: Matriz ATT&CK para empresas

La matriz describe el comportamiento y las acciones de los actores de amenazas durante las distintas fases de un ataque, permite modelar el comportamiento de estos para ser utilizado en la emulación de adversarios, por ejemplo para verificar las defensas de una organización frente a diferentes técnicas en distintas fases o por un equipo de defensa para detectar comportamientos adversos, también puede ser utilizada para probar herramientas de monitoreo, para probar la capacidad de un SOC para detectar, analizar y responder a las intrusiones, es decir puede ser utilizado por los equipos defensivos, los equipos ofensivos y los analistas de seguridad.

La matriz constituye una base documentada y fundamentada sobre amenazas que puede ser utilizada como modelo en los procesos de recolección de inteligencia para implementar defensas basadas en dicha inteligencia. Además verificar que las defensas funcionan y aplicar una mejora continua a las mismas, sin perder de vista que no representa una lista rígida a seguir de los

procedimientos que deben considerarse. Los actores de amenazas evolucionan constantemente en sus tácticas, técnicas y procedimientos y la matriz describe el comportamiento conocido de los mismos.

Los procedimientos que utilizan OSINT se ubican dentro de la Táctica denominada Reconocimiento, la cual actualmente describe 10 técnicas con sus respectivas sub técnicas o procedimientos, que se emplean para recolección de información y descubrimiento. Algunas de ellas son [32]:

- **Recopilar información de la identidad de la víctima**, identificada con el ID T1589. Actualmente cuenta con tres sub técnicas, T1589.001, T1589.002, T1589.003. Mediante esta técnica un actor de amenaza puede obtener nombres de empleados, direcciones de correos, credenciales, vínculos familiares y círculo de amistad entre otras. La obtención la puede lograr mediante observación en redes sociales, sitios web propiedad del objetivo, envío de correos de Phishing o mensajes donde se utilizan técnicas de ingeniería social para hacerse pasar por una fuente en la cual el objetivo confía.
- **Recopilar información de la red de la víctima**, identificada con el ID T1590. Actualmente cuenta con seis sub técnicas, T1590.001 a T1590.006. Mediante esta técnica un actor de amenaza puede obtener nombres y datos administrativos de dominios, direcciones IP, tecnologías utilizadas en la infraestructura de red, servicios disponibles, información de proveedores y dispositivos de seguridad entre otros. La obtención la puede lograr mediante técnicas de escaneo, análisis de tráfico de red, búsquedas de dominios, búsqueda en bases de datos abiertas o aprovechándose de relaciones de confianza que el objetivo tiene con otras organizaciones.
- **Recopilar información de la organización**, identificada con el ID T1591. Actualmente cuenta con cuatro sub técnicas, T1591.001 a T1591.004. Mediante esta técnica un actor de amenaza puede obtener información para determinar la ubicación física del objetivo, identificar roles, funciones y responsabilidades de los empleados más importantes, obtener los nombres de las áreas o departamentos de la organización, obtener datos de las operaciones comerciales y el ritmo empresarial vinculado a las horas y días de trabajo entre otros. La obtención la puede lograr mediante la recopilación de datos en redes sociales, sitios web propiedad del objetivo o mediante el acceso a relaciones de confianza del objetivo entre otros.
- **Buscar dominios y sitios web abiertos**, identificada con el ID T1593. Actualmente cuenta con dos sub técnicas, T1593.001 y T1593.002. Mediante esta técnica un actor de amenaza puede obtener información del objetivo utilizando motores de búsqueda con técnicas de piratería y búsquedas avanzadas en sitios webs, dominios accesibles, redes sociales y sitios con información comercial del objetivo entre otros.

- **Buscar sitios web propiedad de la víctima**, identificada con el ID T1594. Mediante esta técnica un actor de amenaza puede buscar información en el sitio web propiedad del objetivo que le permitan obtener datos de contacto, ubicación y datos comerciales entre otros.
- **Buscar bases de datos técnicas abiertas**, identificada con el ID T1596. Actualmente cuenta con cinco sub técnicas, T1596.001 a T1596.005. Mediante esta técnica un actor de amenaza puede obtener información del objetivo realizando búsquedas en bases de datos técnicas y repositorios disponibles en línea como los registros de dominios y certificados, APIs públicas y colecciones de datos de red recopilados mediante análisis del tráfico y escaneos.

Las TTP mencionadas son las encuadradas en el contenido del presente trabajo y describen sólo una mínima parte del total de técnicas presentes en la Matriz ATT&CK para empresas.

# Capítulo 2 - Inteligencia de Fuentes Abiertas (OSINT)

## Introducción

El concepto inteligencia de fuentes abiertas se refiere al conocimiento que se puede generar mediante un proceso de búsqueda, análisis y recolección de información que está accesible públicamente. OSINT (por sus siglas en inglés Open Source Intelligence) es el término utilizado para referirse al mismo.
El departamento de Defensa de los Estados Unidos (DoD), define OSINT de la siguiente manera:

> *"La inteligencia de fuentes abiertas (OSINT) es una inteligencia que se produce a partir de información disponible públicamente y se obtiene, utiliza y difunde de manera oportuna a una audiencia adecuada con el fin de responder un requisito de inteligencia específico" [33]*

El uso de OSINT ha tomado gran impulso e importancia facilitado por el crecimiento exponencial de Internet y las posibilidades para el desarrollo de investigaciones que ofrece a profesionales de diferentes áreas como la seguridad informática, las fuerzas del orden, el periodismo y la publicidad entre otros [34].
Los datos abiertos proporcionan una valiosa fuente a la que se puede acceder de forma legal y ética para extraer información y definir estrategias de inteligencia. Algunas características relevantes que las distinguen de otras formas de inteligencia es su carácter y posibilidad de acceso público y fácil, siempre disponibles independientemente de su ubicación, con la posibilidad de ser utilizadas por diferentes usuarios en cualquier contexto, solo se requiere conocimiento y herramientas para recolectar y analizar fuentes OSINT de manera correcta. Solo Google en 1998 disponía de 26 millones de páginas, cifra que ha crecido a mil millones para el año 2000 [35]. Informes publicados por IDC (International Data Corporation) estiman un crecimiento de 175 zettabytes de datos para el año 2025, de los 33 zettabytes existentes en 2018 [36]. En el mismo sentido Cisco estima una acumulación de tráfico IP de 4.8 zettabytes por año para el 2022 con 4.800 millones de usuarios conectados a Internet [37]. Estas cifras permiten tener una representación de la inmensa cantidad de datos que están disponibles en la red.

# Buscadores

Un buscador es un software automatizado que escanea continuamente los sitios web mediante un rastreador o crawler para indexar su contenido y almacenarlo en bases de datos masivas.
Según la plataforma de datos Live Stats en agosto de 2019 ya existían más de 1.700 millones de páginas web. La cifra mencionada representa un número abrumador en cuanto a su crecimiento, considerando que solo diez años atrás había algo más de 200 millones según Live Stats.

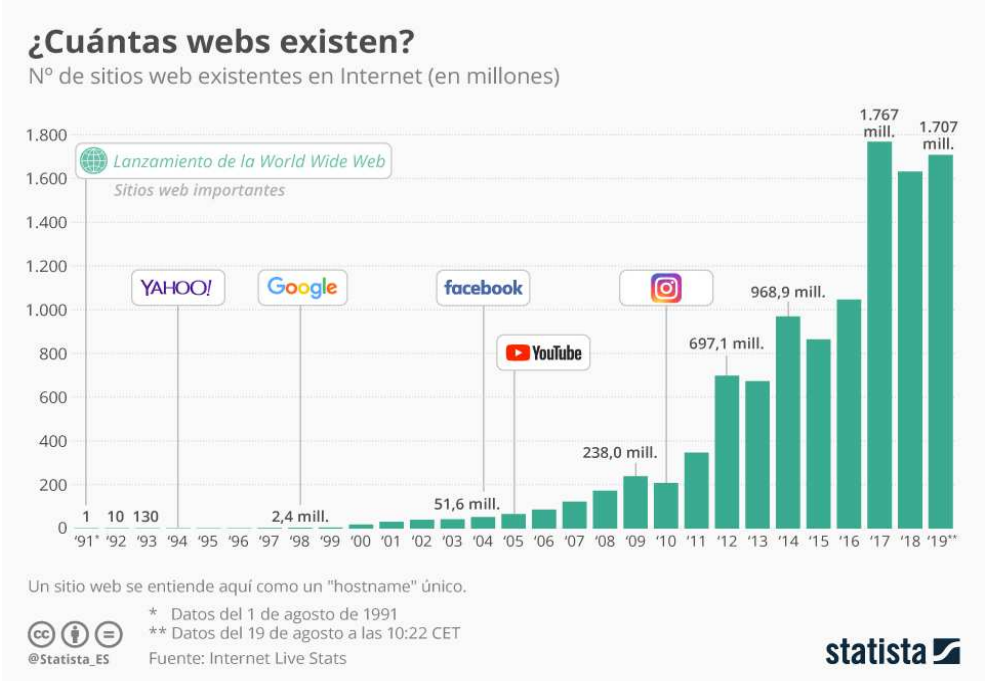



Figura 21: Sitios Web existentes en Internet en 2019

La Figura 21 muestra el crecimiento en cantidad de sitios web existentes en Internet en una línea de tiempo que va desde el lanzamiento de la World Wide Web hasta el año 2019 expresado en millones [38]. En la misma se destacan el surgimiento de diferentes redes sociales y buscadores como Yahoo, Google, Facebook, Youtube e Instagram, donde los buscadores se han convertido en uno de los recursos más importantes de Internet para la utilización de OSINT. Existe una amplia variedad de los cuales se analizaran los más utilizados por las características que ofrecen para buscar y analizar fuentes abiertas.

## Google

Google es considerado el buscador más importante en cuanto a su tamaño y uso, posee una interfaz web muy sencilla pero muy poderosa, que permite realizar búsquedas básicas como así también

consultas avanzadas mediante la utilización de operadores y caracteres comodines de forma combinada. Las búsquedas más simples que podemos realizar con Google consisten en ingresar una palabra, una frase encerrada entre comillas o una URL en el campo de texto del buscador, mediante el cual Google nos permite ingresar el término o los términos a buscar. La Figura 22 muestra la página principal de Google con el campo donde se ingresa el contenido a buscar.

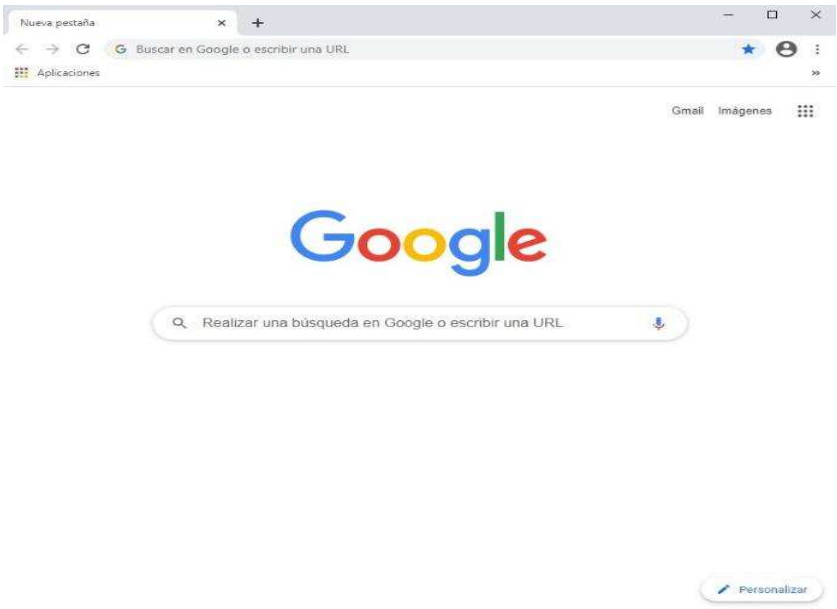



Figura 22: Página principal de Google

Las palabras y las frases también se pueden combinar con símbolos y operadores avanzados que proporciona el buscador. Los operadores más básicos que se utilizan para realizar consultas avanzadas son los operadores booleanos AND, OR y NOT, que permiten separar las distintas partes de una consulta.

El operador AND es equivalente a dejar un espacio entre dos palabras o entre dos frases encerradas entre comillas. El operador OR es equivalente al símbolo (|) y permite ampliar la búsqueda. El operador NOT es equivalente al símbolo (-) antes de una palabra sin dejar espacio entre el símbolo y la palabra, esto permite forzar la exclusión de la misma en la búsqueda.

Además se puede utilizar el símbolo (+) antes de una palabra sin dejar espacio entre el símbolo y la palabra para forzar la inclusión de la misma en la búsqueda y el símbolo (~) antes de la palabra sin dejar espacio entre el símbolo y la palabra para buscar una palabra y sinónimos de la misma.

Este buscador puede ser utilizado para el descubrimiento de una gran variedad de recursos realizando diferentes consultas que utilicen combinaciones de operadores avanzados. Los operadores avanzados de Google permiten diseñar consultas que delimitan los resultados de la búsqueda y su sintaxis básica es: **operador:término de búsqueda**.

En la Tabla 1 se describen los operadores avanzados más significativos [39].

| Operador | Descripción |
|---|---|
| site | Permite buscar un sitio o dominio específico. Se puede combinar con otros operadores. |
| inurl | Permite buscar cadenas en la URL de una página. Se puede combinar con otros operadores. |
| intitle | Permite buscar cadenas en el título de una página. Se puede combinar con otros operadores. |
| intext | Permite buscar cadenas en el contenido de una página. Se puede combinar con otros operadores. |
| allinurl | Permite buscar cadenas en la URL de una página, similar a inurl, pero en este caso la coincidencia debe ser exacta. |
| allintitle | Permite buscar cadenas en el título de una página, similar a intitle, pero en este caso la coincidencia debe ser exacta. |
| allintext | Permite buscar cadenas en el contenido de una página, similar a intext, pero en este caso la coincidencia debe ser exacta. |
| filetype | Permite buscar archivos según la extensión del mismo. Se puede combinar con otros operadores. |
| link | Permite buscar enlaces a un sitio o URL. |
| inanchor | Permite buscar cadenas en el contenido de la descripción de una página. Se puede combinar con otros operadores. |
| cache | Permite mostrar la copia de una página, que Google tiene en cache. |
| related | Permite buscar sitios o URL relacionadas con una dada. |
| info | Muestra información de una página. |

Tabla 1: Operadores avanzados de Google

## Google Dorks

Los diferentes operadores descriptos anteriormente, combinados con distintas expresiones son utilizados para la evaluación de una gran variedad de recursos en línea. A estas expresiones de búsqueda se las denomina Google Dorks y se encuentran en Google Hacking Data Base, también conocida como GHDB, disponible en https://www.exploit-db.com/google-hacking-database. Actualmente la GHDB no solo incluye búsquedas para el motor de Google sino también para otros motores de búsqueda y repositorios como el de Bing y GitHub como herramienta OSINT para realizar las consultas con los Google Dorks.

Google indexa el contenido de los sitios web y si no se bloquea de forma explícita la información sensible, la misma puede quedar expuesta públicamente. Las búsquedas con Dorks pueden mostrar información sensible relacionada con diferentes tipos de archivos conteniendo nombres de usuarios, contraseñas, información personal, listas de correo, páginas de inicio de sesión, software inseguro, directorios sensibles, mensajes de error, cámaras web, impresoras y otros dispositivos en línea entre otros.

Algunos ejemplos básicos de búsquedas son:

- Búsqueda de listados de directorios:
  intitle:index of
  intitle:index of “parent directory”
- Búsqueda de directorios sensibles:
  intitle:index of /Backup
  intitle:index of /admin
  intitle:index of /logs
- Búsqueda de archivos sensibles:
  filetype:xls password|contraseña|user|username|
  filetype:sql “MySQL dump”

Los operadores avanzados pueden ser utilizados por quien gestiona la seguridad de la información en una organización para realizar de forma activa y frecuente operaciones proactivas de prueba de vulnerabilidad sobre los sitios web de la misma para evaluar el nivel de exposición de los activos.

## Bing

Bing es un buscador que proporciona una serie de símbolos y palabras claves similares a los símbolos y operadores de Google para realizar búsquedas avanzadas. La Figura 23 muestra la página principal de Bing.

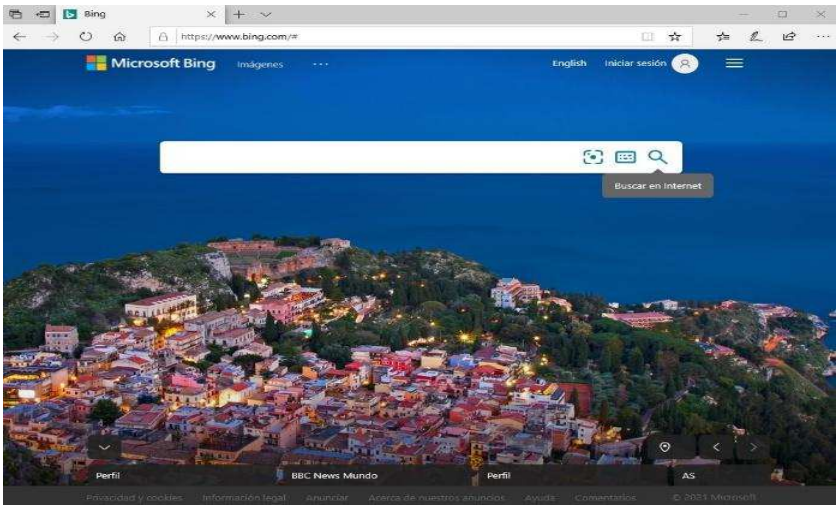



Figura 23: Página principal de Bing

En la Tabla 2 se describen los símbolos y operadores básicos que ofrece Bing [40].

| Símbolo | Descripción |
|---|---|
| + | Busca páginas que contengan los términos que preceden al símbolo. |
| " " | Busca páginas que contengan las palabras o frase exacta encerrada entre las comillas. |
| AND o & | Busca páginas que contengan todos los términos o frases unidas por el símbolo. |
| NOT o - | Excluye de la búsqueda las páginas que contengan el término o frase que precede al símbolo. |
| OR o \| | Busca páginas que contengan alguno de los términos o frases separadas por el símbolo. |

Tabla 2: Operadores básicos de Bing

Bing también cuenta con palabras claves para búsquedas avanzadas. En la Tabla 3 se describen los operadores avanzados de Bing [41].

| Palabra clave | Descripción |
|---|---|
| Contains | Busca sitios con vínculos a los tipos de archivos que se especifique.<br>Ejemplo: ***contains:wma*** |
| Ext | Busca páginas con una extensión específica.<br>Ejemplo: ***ext:docx*** |
| Filetype | Busca páginas creadas con un tipo de archivo específico.<br>Ejemplo: ***filetype:pdf*** |
| inanchor, inbody, intitle | Busca páginas que contengan el término especificado en los metadatos, como el delimitador, el cuerpo o el título.<br>Ejemplo: ***inanchor:msn inbody:espacios inbody:magog***<br>En el ejemplo dado se buscan páginas que contengan "msn" en el delimitador y los términos "espacios" y "magog" en el cuerpo. |
| Ip | Busca los sitios alojados en la dirección IP dada.<br>Ejemplo: ***IP:207.46.249.252*** |
| Language | Busca páginas en el idioma especificado.<br>Ejemplo: para buscar páginas sobre OSINT en español se ingresa ***"OSINT" language:es*** |
| loc o location | Busca páginas web de un país o región específica. Se debe ingresar el código de país o región después de la palabra clave. Se pueden combinar búsquedas utilizando el operador lógico OR. |

| | |
|---|---|
| | Ejemplo: para ver páginas sobre Argentina o España se ingresa ***loc:AR OR loc:ES*** |
| Prefer | Enfatiza un término u operador de búsqueda centrando los resultados en él.<br>Ejemplo: para buscar resultados sobre fútbol correspondientes a un club, se debe ingresar fútbol ***prefer:River Plate*** |
| Site | Busca páginas de un sitio especificado y páginas que contengan una palabra de búsqueda específica. Se puede utilizar para buscar dominios de nivel superior y directorios que no contengan más de dos niveles. Se pueden combinar búsquedas utilizando el operador lógico OR<br>Ejemplo: ***site:unsitio.com OR site:otrositio.com*** |
| Feed | Busca fuentes RSS o Atom en el sitio dado con el término especificado.<br>Ejemplo: para buscar fuentes sobre fútbol, se debe ingresar ***feed:futbol*** |
| Hasfeed | Busca páginas que contengan una fuente RSS o Atom en un sitio dado con el término especificado.<br>Ejemplo: para buscar páginas con fuentes RSS o Atom en el sitio de Cnn, se debe ingresar ***site:cnn.com hasfeed:futbol*** |
| url | Permite comprobar si el índice de Bing incluye el dominio o dirección especificada.<br>Ejemplo: para comprobar que el dominio de Microsoft está en el índice, se debe ingresar ***url:microsoft.com*** |

Tabla 3: Operadores avanzados de Bing

## Shodan

Shodan es una plataforma desarrollada por John Matherly que cuenta con un motor de búsqueda, una API y una serie de herramientas como la CLI (Command-line interface). El motor de búsqueda de Shodan permite localizar dispositivos conectados a Internet, a diferencia de Google y Bing que buscan páginas o sitios web, Shodan busca equipos con un determinado software o con una determinada versión de un tipo específico del mismo, también permite la búsqueda de servicios que responden a puertos como el 21 (FTP), 22 (SSH), 23 (TELNET), 25 (SMTP), 80 (HTTP), 161 (SNMP), 443 (HTTPS), 3389 (RDP), 5900 (VNC), entre otros. La Figura 24 muestra la página principal de Shodan.

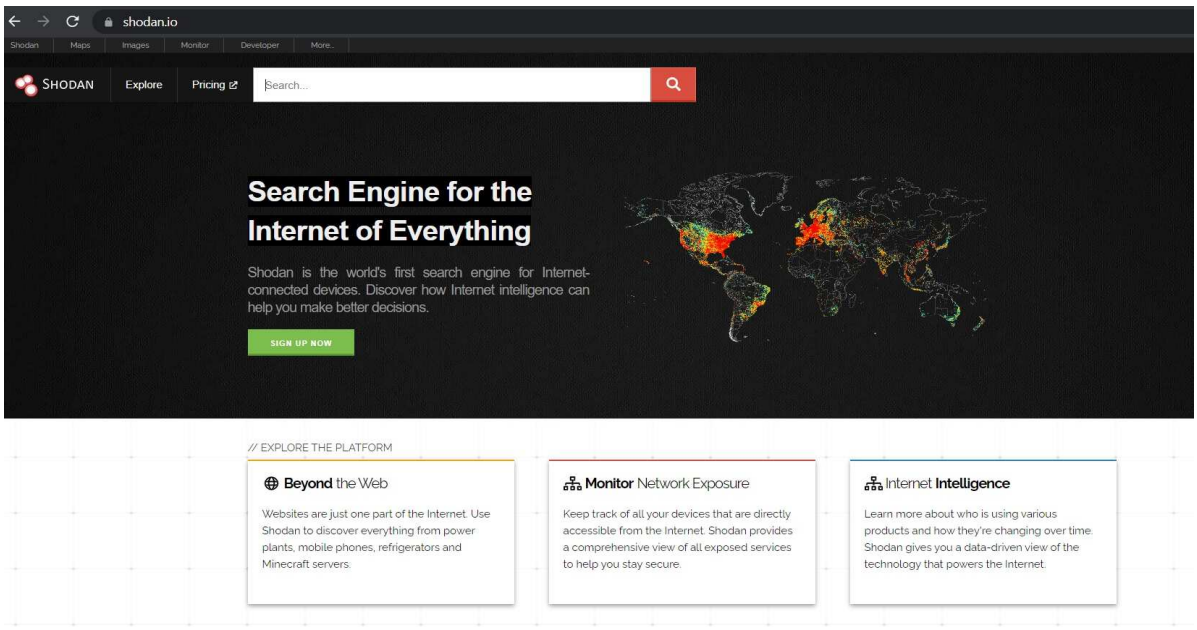



Figura 24: Página principal de Shodan

Este buscador puede indexar una gran variedad de dispositivos por ejemplo webcams, routers, firewalls, impresoras, sistemas de circuito cerrado (CCTV), sistemas de control industrial, dispositivos IoT y muchos más.

Shodan logra indexar diferentes dispositivos y servicios utilizando la información contenida en el banner, unidad básica de datos recopilada por Shodan con información textual que describe el servicio presente en los mismos [42].

La Tabla 4 muestra dos ejemplos de banner, el primero muestra un banner de un dispositivo que ejecuta un servidor web nginx en su versión 1.1.19 y el segundo muestra el banner de un sistema de control industrial Siemens.

| | |
|---|---|
| HHTTP/1.1 200 OK<br>Server: nginx/1.1.19<br>Date: Sat, 03 Oct 2015 06:09:24 GMT<br>Content-Type: text/html; charset=utf-8<br>Content-Length: 6466<br>Connection: keep-alive | Copyright: Original Siemens Equipment<br>PLC name: S7_Turbine<br>Module type: CPU 313C<br>Unknown (129): Boot Loader A<br>Module: 6ES7 313-5BG04-0AB0 v.0.3<br>Basic Firmware: v.3.3.8<br>Module name: CPU 313C<br>Serial number of module: S Q-D9U083642013<br>Plant identification:<br>Basic Hardware: 6ES7 313-5BG04-0AB0 v.0.3 |
| Banner servidor nginx | Banner sistema industrial siemens |

Tabla 4: Ejemplos de Banners

En los ejemplos se puede observar cómo difieren los banners dependiendo del tipo de dispositivo, software y versión que ejecuta el mismo.

Las búsquedas más simples que podemos realizar con Shodan consisten en ingresar una frase en el campo de texto del buscador y que devuelva como resultado los banners que incluyen la frase ingresada. También cuenta con filtros de búsqueda con los cuales se puede obtener la información básica del banner y realizar búsquedas en función de los metadatos de un dispositivo o servicio. El formato para ingresar un filtro es:

**nombre del filtro:valor**

A continuación en la Tabla 5 se describen los filtros generales más utilizados para realizar búsquedas con la interfaz web de Shodan presentada en la figura 24.

| Filtro | Descripción |
|---|---|
| City | Permite buscar los dispositivos localizados en la ciudad especificada.<br>Ejemplo: city:Rosario |
| Country | Permite buscar los dispositivos localizados en el país especificado según su código ISO.<br>Ejemplo: country:AR |
| Os | Permite buscar dispositivos con el sistema operativo especificado. |
| Port | Permite buscar dispositivos con el puerto especificado abierto. |
| Hostname | Permite buscar por el nombre de host del dispositivo. |
| Org | Permite buscar por el nombre de la organización. |
| Ip | Permite buscar por la ip especificada. |
| Net | Permite buscar por un rango de red en notación CIDR.<br>Ejemplo: 200.5.2.0/24 |
| Asn | Permite buscar por el número de sistema autónomo especificado. |
| Product | Permite buscar por el nombre del producto especificado, presente el banner. |
| Versión | Permite buscar por la versión del producto especificado. |
| Vuln | Permite buscar por el CVE ID de una vulnerabilidad especificada. |

Tabla 5: Filtros de Shodan

Otro elemento que proporciona Shodan es la CLI (Command-line interface), una herramienta externa que se puede instalar localmente y permite obtener datos de la API utilizando comandos. En la Tabla 6 se describen los comandos más utilizados.

| Comando | Descripción |
|---|---|
| Search | Permite buscar, obtener y visualizar datos en la terminal. |
| Download | Permite descargar los resultados de una búsqueda en un archivo JSON. |
| Parse | Permite filtrar los datos descargados en el archivo JSON. |
| Convert | Permite convertir el archivo JSON descargado a un formato de archivo diferente. |
| Host | Permite obtener información de un host. |
| Scan | Permite realizar escaneos de red. |
| Alert | Permite crear alertas de red para monitoreo |

Tabla 6: Comandos de la CLI de Shodan

## Censys

Censys es un motor de búsqueda desarrollado por los creadores de Zmap. Originalmente surgió como un proyecto de investigación en la Universidad de Michigan. Actualmente es dirigido por un equipo de profesionales académicos y de la industria de redes y seguridad [43]. Cuenta con un repositorio donde se publican instantáneas diarias de los escaneos. El mismo es administrado por el grupo de “Stanford Empirical Security Research Group”, perteneciente a “scans.io”, el repositorio de datos de investigación de Internet de la Universidad de Stanford [44].

Censys permite realizar búsquedas de dispositivos IPv4, escaneo de 2329 puertos, la detección de 36 protocolos, sitios web y almacena millones de certificados en su repositorio entre otros [43]. Se puede interactuar con Censys a través de su página web, su API o mediante la descarga de las instantáneas en formato Json.

Censys en su página web proporciona diferentes posibilidades de búsquedas, estas son:

- IPv4 Hosts: permite realizar búsquedas sobre hosts utilizando filtros.
- Websites: permite realizar búsquedas sobre websites y enumerar puertos abiertos, subdominios y otros.
- Certificates: permite realizar búsquedas sobre certificados para generar reportes o informes de interés.

Censys al igual que Shodan proporciona una serie de herramientas que aportan inteligencia a los datos dentro de las que podemos mencionar mapas para geolocalización, metadatos, reportes y Apis para desarrolladores.

Una opción para trabajar con Censys es mediante el uso de consultas estructuradas que admiten operadores lógicos. Los siguientes ejemplos ilustran dos consultas que hacen uso de los mismos.

Búsqueda de servidores Apache, puerto 80 utilizando un número de AS (Autonomous System) determinado:

(services.port: 80) and services.software.product=`apache` and autonomous_system.asn:5692

Búsqueda de servidores Apache, puerto 80 utilizando un prefijo de red determinado:

(services.port: 80) and services.software.product=`apache` and ip:163.10.0.0/16

Herramientas como Censys o Shodan permiten tener una visión de los activos que la organización expone a Internet y evaluar riesgos asociados a ello. Representan una fuente útil para tener visibilidad de la información que un actor malicioso puede estar recopilando de la organización.

## Redes sociales

En líneas generales se define como red social a una plataforma que permite la conexión y comunicación de personas por algún interés común, amistad o parentesco. Actualmente los sitios de redes sociales permiten a los usuarios comunicarse, socializar, jugar, comprar, vender o buscar información. La mayoría de las personas tienen una o más cuentas en las redes sociales como Facebook, YouTube, Twitter, Instagram o LinkedIn.

La Figura 25 muestra la cantidad de usuarios activos en las diferentes redes sociales lo que las convierte en valiosos recursos OSINT, estudio realizado por “Digital 2020 Global Digital Overview” de Weare Social y Hootsuite [45].

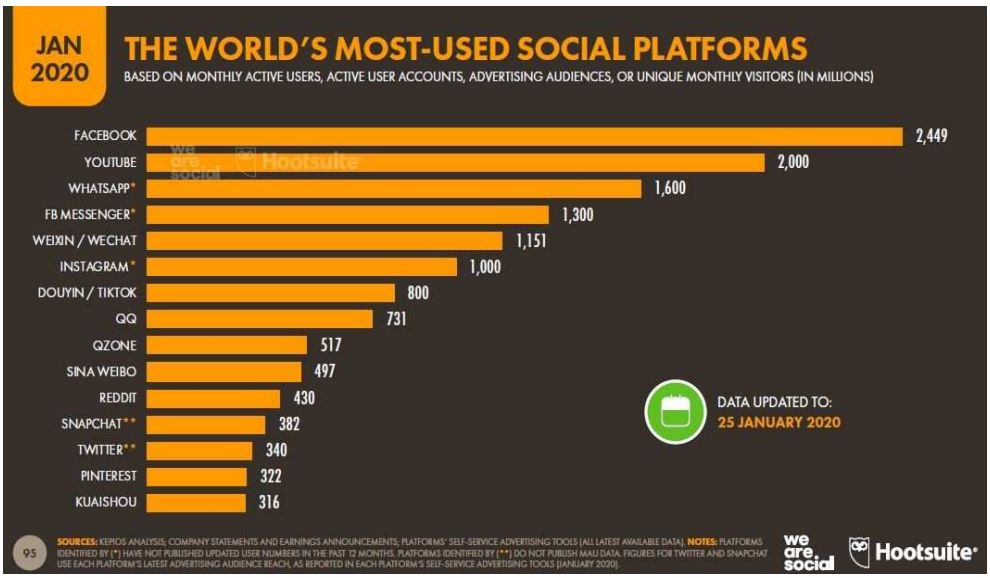



Figura 25: Cantidad de usuarios en las Redes Sociales

Los millones de usuarios que forman parte de estas redes generan volúmenes de datos gigantescos propiciado por la capacidad que ofrecen las mismas para publicar, difundir contenido e interactuar entre los usuarios. Las características antes mencionadas han convertido a estas plataformas en grandes fuentes de información, gran parte de la cual está publicada sin restricciones y es visible públicamente, lo que representa un grave riesgo para la privacidad.

Por lo antes mencionado las redes sociales son una gran fuente de extracción de datos.

Existe una gran variedad de ellas, de las cuales se estudian las más utilizadas y las que ofrecen posibilidades adicionales para buscar y analizar información.

## Facebook

Facebook es la red social más popular, cuenta con más de 2 mil millones de usuarios, permite la publicación e intercambio de mensajes de texto, imágenes, videos y transmisión en vivo, entre otros. Para crear una cuenta en Facebook se debe proporcionar el correo electrónico, fecha de nacimiento y género. Además, después de crear y activar su cuenta el usuario puede continuar agregando información relacionada a su formación, empleo, lugar de residencia, relaciones, celular, sitio web, dirección, creencias religiosas, ideología política, pasatiempos y mucho más.

Toda la información mencionada que los usuarios registran en Facebook representa una fuente de información muy valiosa para cualquier investigación OSINT. Un aspecto fundamental que la convierte en valiosa para cualquier investigación son los escasos controles de privacidad que los usuarios establecen sobre el acceso a la información personal que publican en la red social.

Facebook ha desarrollado un mecanismo de búsqueda propio para simplificar la localización de diferente tipo de contenido. Cuenta con un motor de búsqueda semántico avanzado, denominado

“Graph Search”, que permite búsquedas utilizando palabras claves y frases en inglés natural. Se debe tener en cuenta que se necesita tener configurada la cuenta en idioma inglés para poder utilizar “Graph Search”.

## Linkedin

Linkedin desde 2016 propiedad de Microsoft es la mayor red social de profesionales a nivel mundial tiene más de 756 millones de usuarios distribuidos en más de 200 países [46]. En esta red se puede acceder a una cuenta gratuita o de pago mensual y crear un perfil profesional o de empresa.
El propósito de esta red es conectar a profesionales con empresas u otros profesionales, no solo por motivos laborales sino también para promocionar productos, servicios o encontrar ideas para negocios.
La red permite a los usuarios acceder a una sección propia de empleos donde las empresas publican las oportunidades laborales y a las empresas buscar determinados perfiles para contactarlos y proponerles una entrevista.
Linkedin permite buscar por nombre y apellido, empresa, cargo e idioma entre otros filtros. También permite el uso de operadores avanzados como NOT para excluir una palabra o frase específica, OR para incluir una o más palabras en la búsqueda, AND para incluir dos o más palabras juntas en la búsqueda.
En investigaciones OSINT, Linkedin es uno de los primeros lugares para buscar personas relacionadas a una profesión o empresa específica, conocer su historial de trabajo, experiencia y habilidades. En relación a las empresas en la sección de empleos se puede encontrar gran cantidad de información relacionada a las tecnologías que utilizan. Plataformas, nombres de productos, versiones de los mismos y servicios que utilizan entre otros. Las Figuras 26, 27, 28 y 29 representan ejemplos de esta problemática.

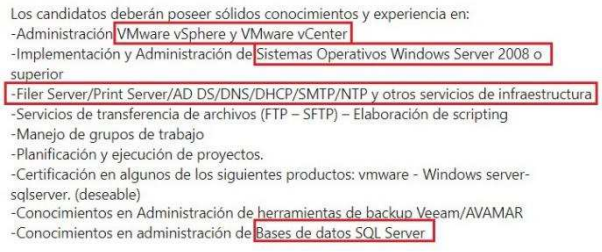

Los candidatos deberán poseer sólidos conocimientos y experiencia en:
-Administración VMware vSphere y VMware vCenter
-Implementación y Administración de Sistemas Operativos Windows Server 2008 o superior
-Filer Server/Print Server/AD DS/DNS/DHCP/SMTP/NTP y otros servicios de infraestructura
-Servicios de transferencia de archivos (FTP – SFTP) – Elaboración de scripting
-Manejo de grupos de trabajo
-Planificación y ejecución de proyectos.
-Certificación en algunos de los siguientes productos: vmware - Windows server-sqlserver. (deseable)
-Conocimientos en Administración de herramientas de backup Veeam/AVAMAR
-Conocimientos en administración de Bases de datos SQL Server

Figura 26: Anuncio Linkedin

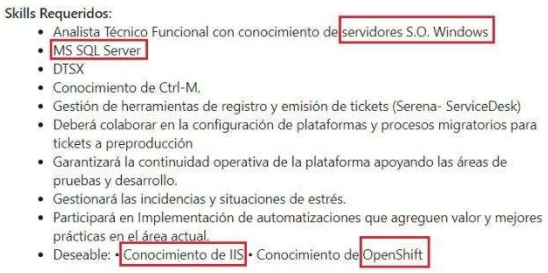

**Skills Requeridos:**
- Analista Técnico Funcional con conocimiento de servidores S.O. Windows
- MS SQL Server
- DTSX
- Conocimiento de Ctrl-M.
- Gestión de herramientas de registro y emisión de tickets (Serena- ServiceDesk)
- Deberá colaborar en la configuración de plataformas y procesos migratorios para tickets a preproducción
- Garantizará la continuidad operativa de la plataforma apoyando las áreas de pruebas y desarrollo.
- Gestionará las incidencias y situaciones de estrés.
- Participará en Implementación de automatizaciones que agreguen valor y mejores prácticas en el área actual.
- Deseable: • Conocimiento de IIS • Conocimiento de OpenShift

Figura 27: Anuncio Linkedin


Figura 28: Anuncio Linkedin

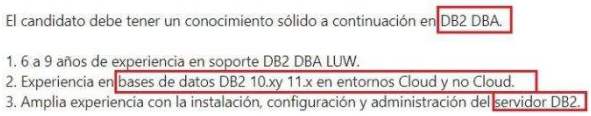



Figura 29: Anuncio Linkedin

La información expuesta puede ser utilizada por un actor de amenazas para una enumeración inicial sobre una organización.

## Twitter

Twitter es una red social de microblogging que cuenta con más de 330 millones de usuarios. Inició sus actividades en 2006. Inicialmente permitía a sus usuarios publicar tweets con una longitud máxima de 140 caracteres. Esta limitación fue ampliada en 2017 extendiendo a 280 caracteres la longitud máxima de los tweets. Los usuarios pueden incluir en ellos texto, fotos, videos cortos y enlaces. Principalmente Twitter se utiliza para construir comunidades en línea y conectar personas con intereses comunes para lo cual utiliza lo que se conoce como “hashtags”.

Twitter no exige el uso de nombres reales para registrarse, proceso donde el usuario debe proveer un número de teléfono o dirección de correo electrónico para poder activar una cuenta.

Twitter utiliza un identificador de nombre para referirse a un usuario. El identificador comienza con el signo @ y es precedido por caracteres alfanuméricos. Se utiliza para enviar mensajes privados o hacer referencia a un usuario en tweets públicos. Twitter permite seguir perfiles públicos y recibir notificaciones de los cambios y actualizaciones que ese perfil realice. Por sus características Twitter no brinda tanta información de las personas como por ejemplo Facebook o Linkedin. La información OSINT más buscada en Twitter de sus usuarios corresponde a intereses políticos, personales, religiosos, amistades, lugares frecuentados y geolocalización entre otros.

Twitter cuenta con operadores de búsqueda avanzada similares a los de Google, algunos de ellos se describen a continuación en la Tabla 7 [47].

| Operador | Descripción |
|---|---|
| "" | Permite buscar frases o palabras. Devuelve coincidencias exactas con los términos incluidos entre las comillas dobles.<br>Ejemplo: "fuentes OSINT" |
| OR y AND | Permiten buscar coincidencias por más de un término.<br>Ejemplo: OSINT OR “fuentes abiertas” o OSINT AND tweet |
| - | Permite excluir palabras o frases. |
| # | Permite buscar tweets con un hashtag específico.<br>Ejemplo: #OSINT |

| | |
|---|---|
| from:cuenta tema | Permite buscar los tweets enviados desde una cuenta, filtrando por temas.<br>Ejemplo: from:eftossolini OSINT |
| to: from: | Permite buscar los tweets dirigidos a la cuenta en to: que provienen de la cuenta en from: |
| lang: | Permite buscar los tweets de un idioma determinado.<br>Ejemplo: lang:es |
| since: until: | Permite buscar los tweets entre dos fechas indicadas y asociados por ejemplo a una palabra.<br>Ejemplo: since:2020-10-10 until:2021-01-01 OSINT |
| near: within | Permite buscar los tweets enviados desde una ubicación específica.<br>Ejemplo: near:rosario within:50km |
| filter:videos | Permite buscar tweets que contengan videos asociados a una palabra o hashtag.<br>Ejemplo: OSINT filter:videos |
| filter:media | Permite buscar tweets que contengan imágenes o videos asociados a una palabra o hashtag.<br>Ejemplo: OSINT filter:media |

Tabla 7: Operadores de búsqueda avanzada de Twitter

Twitter también cuenta con una página de búsqueda avanzada mediante la cual se pueden configurar diferentes filtros y obtener los mejores resultados en las búsquedas.

La figura 30 muestra la interfaz de búsqueda avanzada de Twitter.

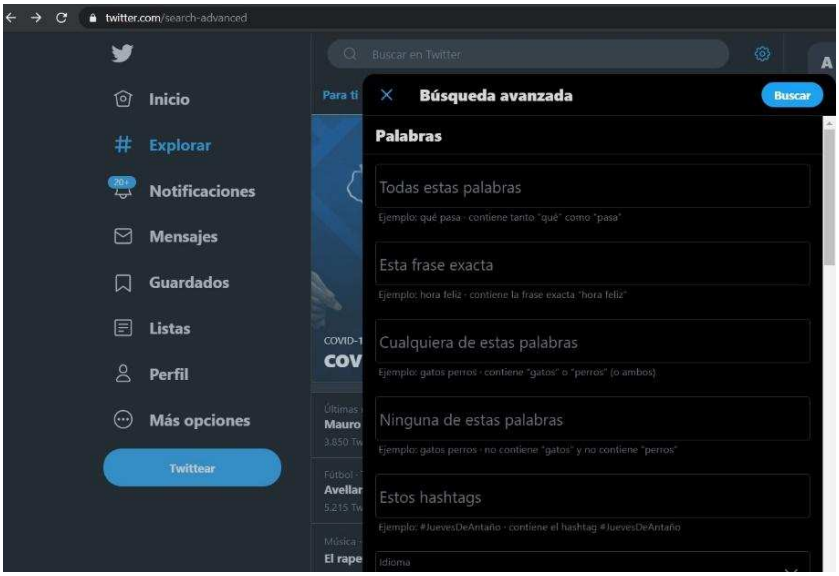



Figura 30: Página de búsqueda avanzada de Twitter

# Otras fuentes y recursos OSINT

Las fuentes abiertas disponibles son muy variadas y permiten recuperar distintos tipos de datos que pueden ser utilizados con diferentes propósitos. Abarcan la información disponible en redes sociales, sitios webs, repositorios de diferentes tipos de archivos como archivos de imagen, texto, videos o código, apis de servicios, blogs, foros, feeds y bases de datos entre otros, estos son algunos ejemplos de fuentes de información que forman parte de OSINT.

Existen listados y repositorios que reúnen cientos de enlaces y herramientas como el disponible en el sitio web de Michael Bazzell (inteltechniques.com) o el de Julián GL (ciberpatrulla.com) entre otros. A continuación, como referencia se mencionan algunas de ellas encuadradas en el marco del presente trabajo.

**Robtex** (www.robtex.com): este recurso permite obtener información pública relacionada a direcciones IP, nombres de dominio, nombres de host y sistemas autónomos entre otros. Realizar búsqueda de DNS inversa de direcciones IP, registros MX (servidores de correo) y NS (servidor de nombres).

**Netcraft** (www.netcraft.com): fundada por Mike Prettejohn dispone en su web de herramientas para obtener informes de un dominio o IP y búsquedas DNS entre otras.

Tanto Robtex como Netcraft permiten realizar búsqueda de información en múltiples bases de datos y obtener información técnica, de contacto, fecha de registro, vencimiento y todo lo asociado a los datos de registro del dominio de una organización. Permiten visualizar qué información técnica y administrativa de una organización se encuentra registrada y es accesible públicamente.

**Have I Been Pwned** (haveibeenpwned.com): este recurso permite verificar si una cuenta de correo electrónico está dentro de alguna base de datos cuya información ha sido filtrada y expuesta.

**PhishTank** (www.phishtank.com): este recurso almacena en su base de datos información de miles de sitios que fueron comprometidos para realizar ataques de phishing. Esta base de datos es mantenida y actualizada por la comunidad. Permite informar sobre un sitio sospechoso para que el mismo sea analizado y también brinda a las organizaciones la posibilidad de consultar y verificar si un sitio de la misma ha sido denunciado como fraudulento o reportado para alojar ataques de phishing.

**Spamhaus** (www.spamhaus.org): este recurso permite verificar direcciones IP, dominios y bloques de red que estén asociados a operaciones de distribución de Spam. Spamhaus brinda a las organizaciones la posibilidad de consultar su “Blocklist” también conocida como DNSBL, una gran base de datos con información relacionada con el origen del correo electrónico que permite saber si el mismo cumple con las políticas de Spamhaus para la aceptación del correo entrante.

**Reglas de Snort**: el NIDS (Network Intrusion Detection System) Snort es un software de código abierto que utiliza un conjunto de reglas y un motor de detección para analizar tráfico y encontrar amenazas en función de las reglas configuradas.

Snort se puede utilizar en línea para analizar el tráfico y dispone de dos conjuntos de reglas:

- Conjunto de reglas de la comunidad: son desarrolladas por la comunidad de Snort, controladas por Cisco Talos y están disponibles de manera gratuita para su descarga y utilización.
- Conjunto de reglas de suscriptor de Snort: son desarrolladas, controladas y aprobadas por Cisco Talos y distribuidas para los suscriptores de Snort.

Las reglas de Snort antes mencionadas permiten, por ejemplo, detectar actividad asociada a una botnet: PCs de nuestra organización comunicándose con servidores de comando y control (C&C servers). Esta información podría ser utilizada como fuente de información.

# Capítulo 3 - OSINT aplicado a la detección de vulnerabilidades y amenazas en las organizaciones

## Introducción

Gran parte de los incidentes de seguridad comienzan con una fase de reconocimiento y recolección de información. Los actores de amenazas pueden recopilar datos personales como nombres de los integrantes de una organización, área en la cual trabaja, cargo, correos electrónicos, información de la red de la organización, rangos de direcciones IP, nombres de dominios, subdominios, servidores de DNS, servidores de correo, datos administrativos, errores de configuración, vulnerabilidades y malas prácticas entre otros. La información que recopilan es expuesta en Internet y accesible a través de redes sociales, sitios web de las organizaciones, bases de datos abiertas con información técnica, buscadores, filtraciones de datos en línea y más.
Una gran parte del reconocimiento se realiza de forma pasiva utilizando diferentes técnicas y herramientas OSINT.
Los profesionales responsables de la seguridad de la información en las organizaciones pueden utilizar estas técnicas para trazar un perfil de la exposición que la organización tiene en Internet y realizar una detección temprana de vulnerabilidades, configuraciones incorrectas y malas prácticas.
A continuación, encuadrado en el contenido del actual trabajo se presenta un análisis de diferentes problemáticas y ejemplos de estas.

## Listado de directorios del servidor web

En esta sección se orienta el análisis de OSINT a la detección de listados de directorios en servidores web, se utilizan para dicho análisis operadores avanzados de Google. El listado de directorios representa una debilidad en la configuración de seguridad de un servidor web. Poder listar el contenido de directorios, subdirectorios y navegar a través de estos, puede dar lugar a fuga de información al permitir descargar o editar el contenido de los mismos. Un actor malicioso puede aprovecharse de esta debilidad para encontrar y descargar información sensible como archivos con nombres de usuario y claves o backups de bases de datos, entre otros. Se debe evitar que desde un navegador se pueda listar y acceder al contenido de directorios y subdirectorios.

La búsqueda de “Listados de directorios” sobre un dominio se puede realizar utilizando el operador “site” para restringir la misma a un dominio determinado y combinar por ejemplo con el operador “intitle” y la frase “Index of”. La Figura 31 muestra los numerosos resultados que devuelve el buscador Google con la consulta “**site:.ar intitle:index of**” la cual restringe su búsqueda a los dominios “.ar”.

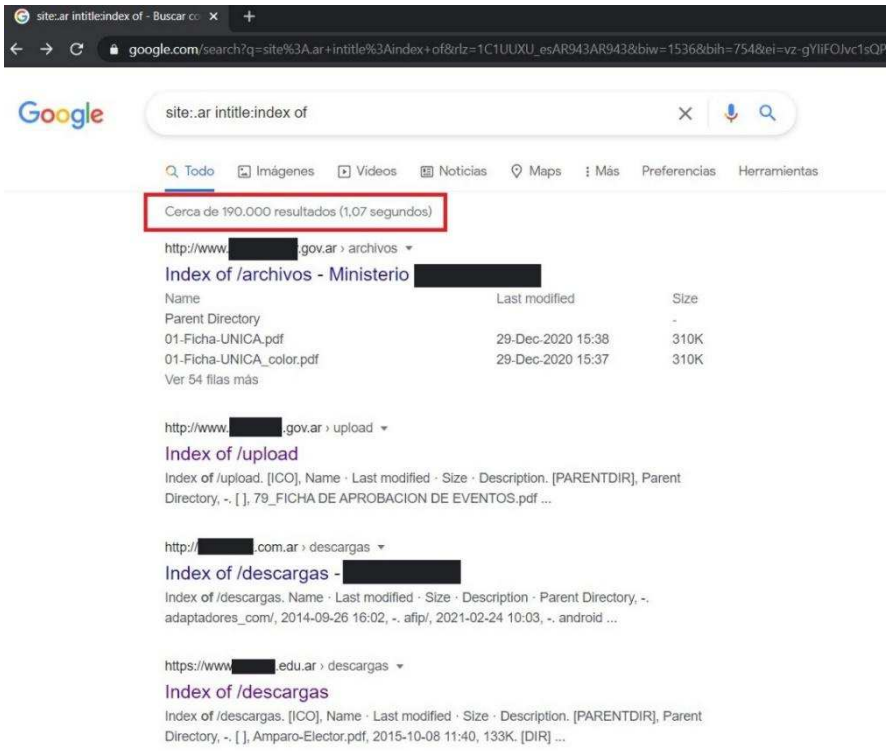



Figura 31: Búsqueda básica para localizar listados de directorios

En la Figura 32 se observa un listado de directorios que permite visualizar uno de los enlaces que devuelve Google en la consulta mostrada en la figura 31.

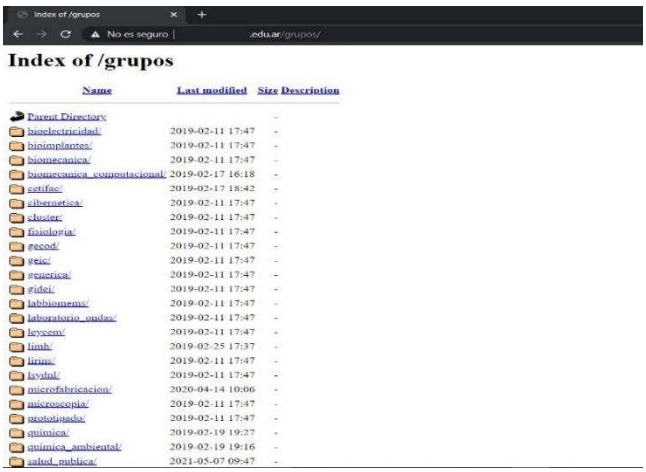



Figura 32: Listado de directorios accesible desde enlace de Google

Como parte del análisis de listado de directorios, se pueden realizar búsquedas orientadas a descubrir directorios específicos que permitan ser listados desde el navegador. La siguiente búsqueda se realiza para descubrir directorios con el nombre “backup” que permitan ser listado por el navegador. La Figura 33 muestra los resultados devueltos por el buscador utilizando la consulta “**site:.ar intitle:index of /backup**”.

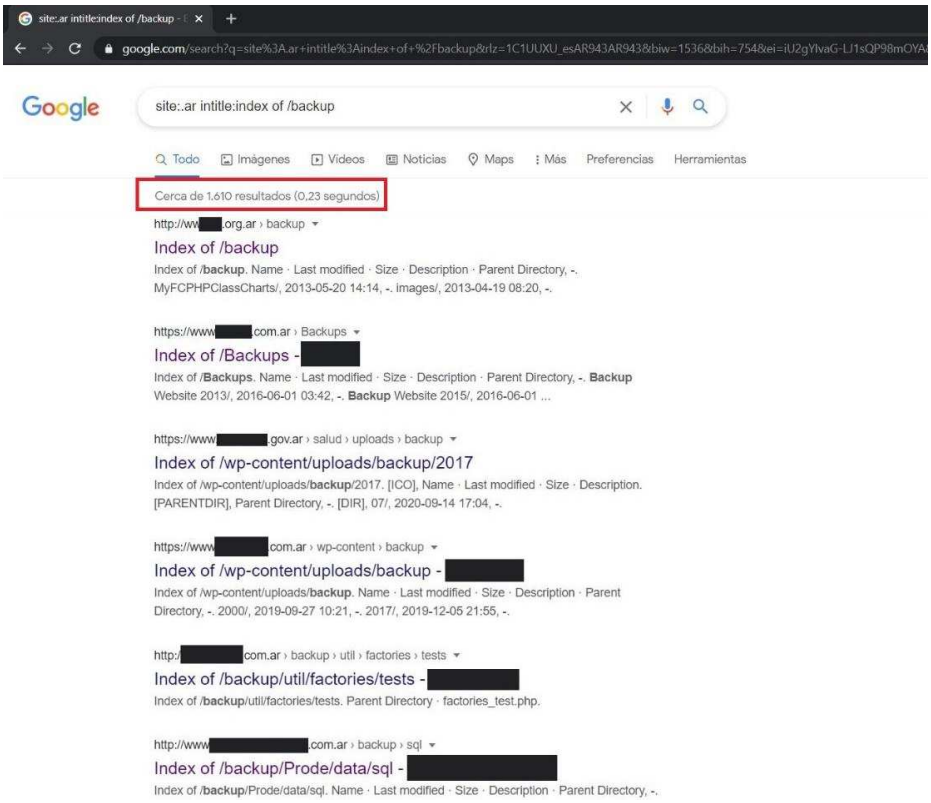



Figura 33: Búsqueda de directorio específico “backup”

En las Figuras 34, 35, 36 y 37 se observan listados de directorios accesibles desde los enlaces devueltos por el buscador en la consulta mostrada en la figura 33.

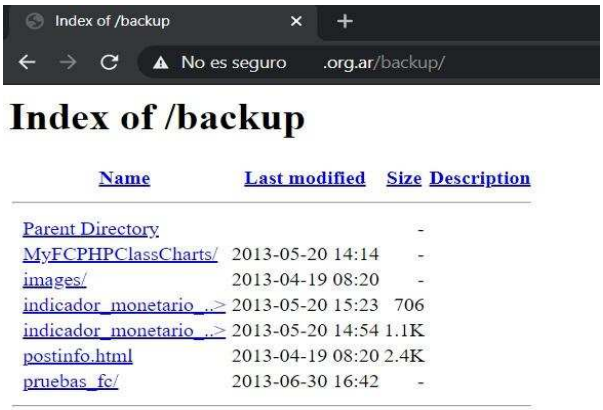



Figura 34

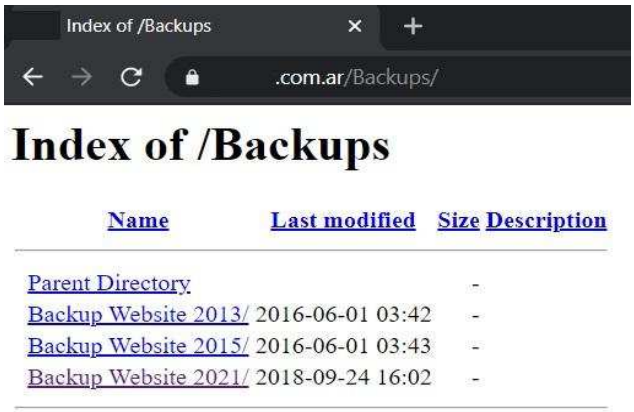



Figura 35

Figura 34 y 35: Búsqueda de directorio específico “backup”

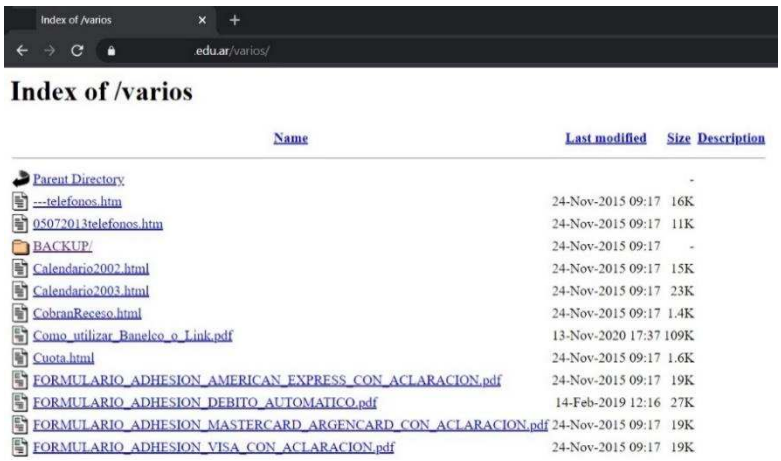



Figura 36

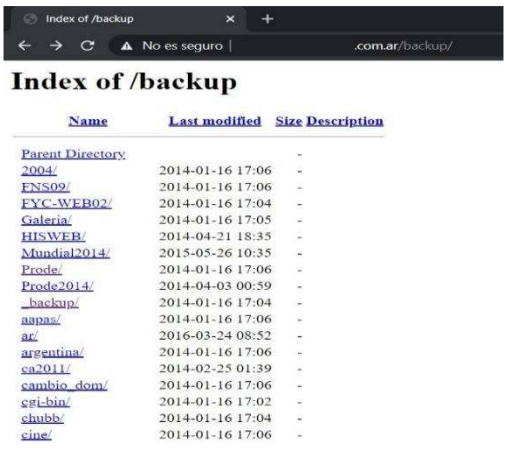



Figura 37

Figura 36 y 37: Búsqueda de directorio específico “backup”

Como parte de las búsquedas de directorios específicos que pueden contener información sensible, también se pueden buscar por ejemplo los directorios “admin” y “httpd” entre otros.

# Listado de archivos

Los servidores que tienen una configuración de seguridad débil y permiten listar sus directorios también pueden permitir listar diferentes tipos de archivos. Se puede realizar una búsqueda utilizando operadores avanzados de Google para buscar archivos “xls” que contengan “usuario” y “contraseña”. La Figura 38 muestra los resultados devueltos por el buscador utilizando la consulta “**site:.ar filetype:xls +usuario +contraseña**”.

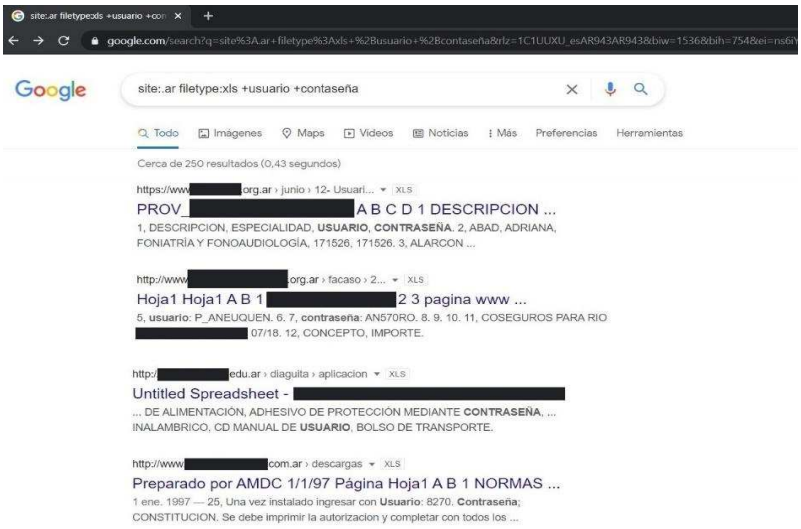



Figura 38: Búsqueda de archivos “xls” con usuario y contraseña

En la segunda búsqueda de listado de archivos se buscan archivos de bases de datos del tipo “sql”. Las Figuras 39 y 40 muestran los resultados devueltos por el buscador utilizando la consulta “**site:.ar filetype:sql**” y “**site:.ar filetype:sql intext:insert into `usuarios`**”.

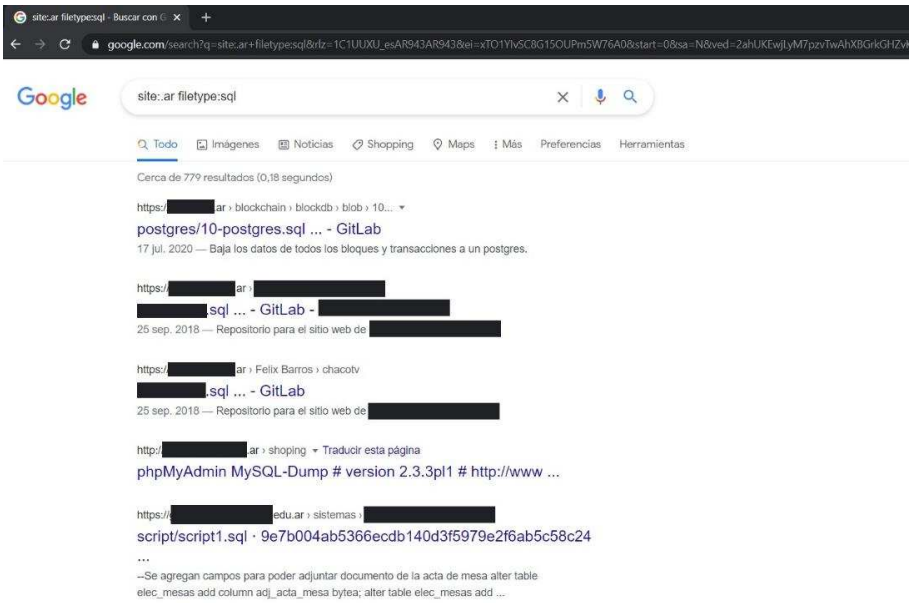



Figura 39: Búsqueda de archivos sql. Consulta: **site:.ar filetype:sql**

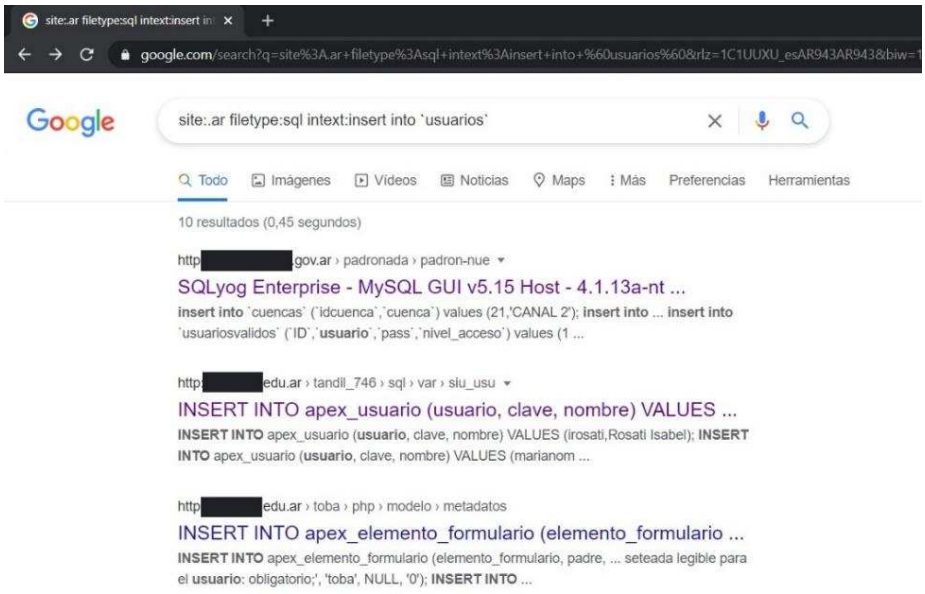



Figura 40: Búsqueda de archivos sql. Consulta: **site:.ar filetype:sql intext:insert into `usuarios`**

En la Figura 41 se observa un archivo sql accesible desde uno de los enlaces que devuelve Google en la consulta mostrada en la figura 39.

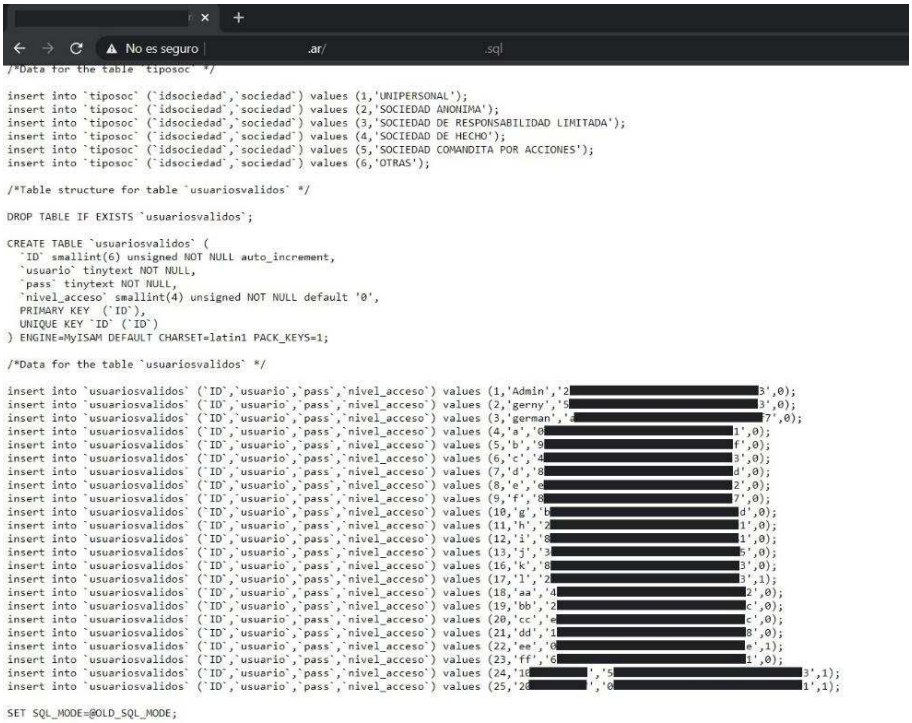



Figura 41: Archivo sql accesible desde enlace de Google

Como parte de las búsquedas de archivos específicos que pueden contener información sensible, también es posible listar archivos de logs. La Figura 42 muestra los resultados devueltos por el buscador utilizando la consulta "**site:.ar filetype:log intext:usuario**".

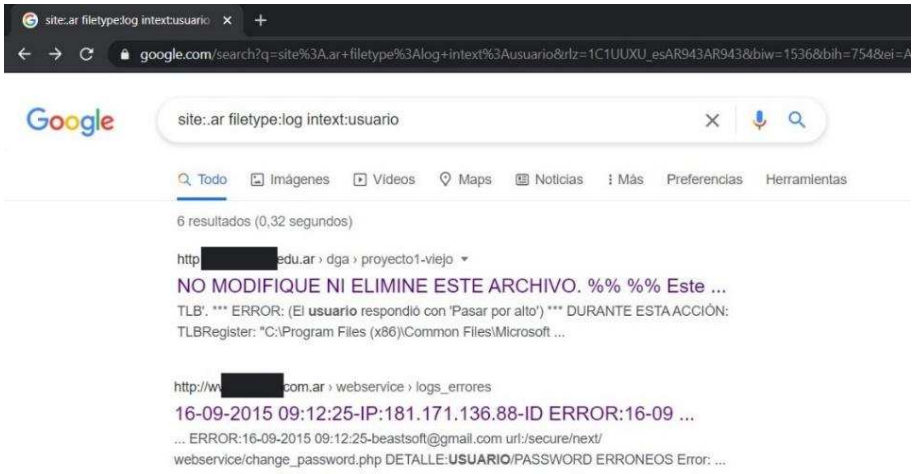



Figura 42: Búsqueda de archivos log.

Como se observa en los ejemplos anteriores es posible obtener a través de consultas con operadores avanzados diferentes tipos de archivos que pueden contener información sensible como usuarios y contraseñas entre otros.

# Inicios de sesión inseguros

En esta sección las búsquedas se orientan al descubrimiento de páginas de inicio de sesión sobre conexiones no seguras. Los inicios de sesión sobre el protocolo “http” pueden exponer información sensible debido a la falta de cifrado en la conexión. Un actor malicioso puede interceptar las comunicaciones poniendo en riesgo la seguridad de la misma. Algunas de las combinaciones usadas son: “**site:.ar inurl:http://webmail**”, “**site:.ar inurl:http:// login**” y “**site:.ar inurl:http://intranet**”, las consultas realizadas devuelven numerosos resultados, parte de ellos encuadrados con el objetivo de las mismas. Las Figuras 43, 44, 45 y 46 muestran ejemplos de estos resultados positivos donde se observan páginas de inicio de sesión sobre “http”.

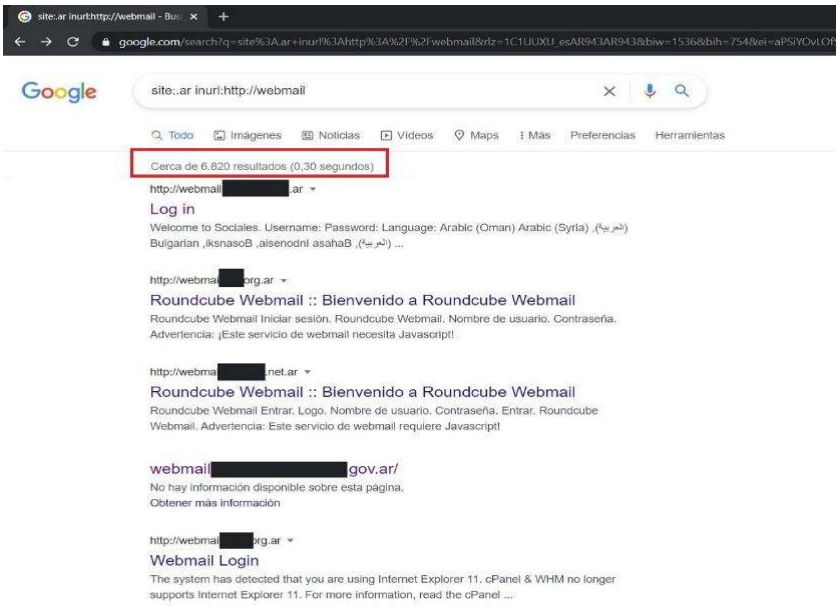



Figura 43: Búsqueda de webmail. Consulta: site:.ar inurl:http://webmail

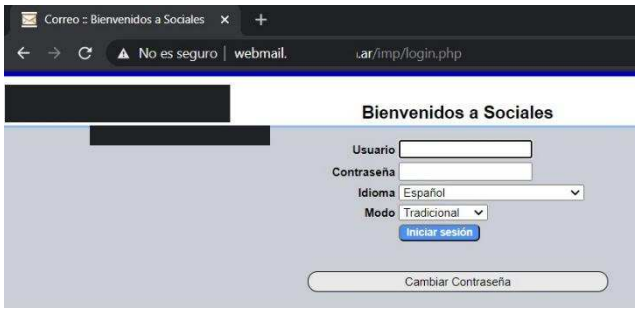



Figura 44: Login webmail sobre “http”

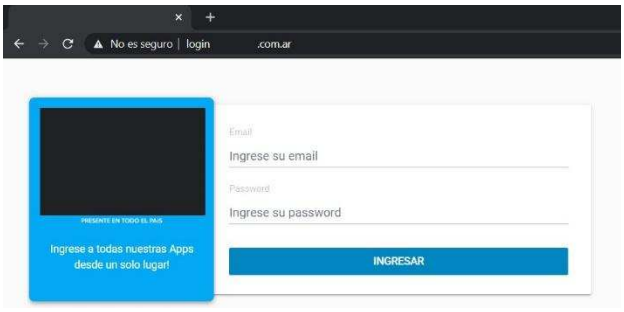



Figura 45: Login aplicación web sobre “http”

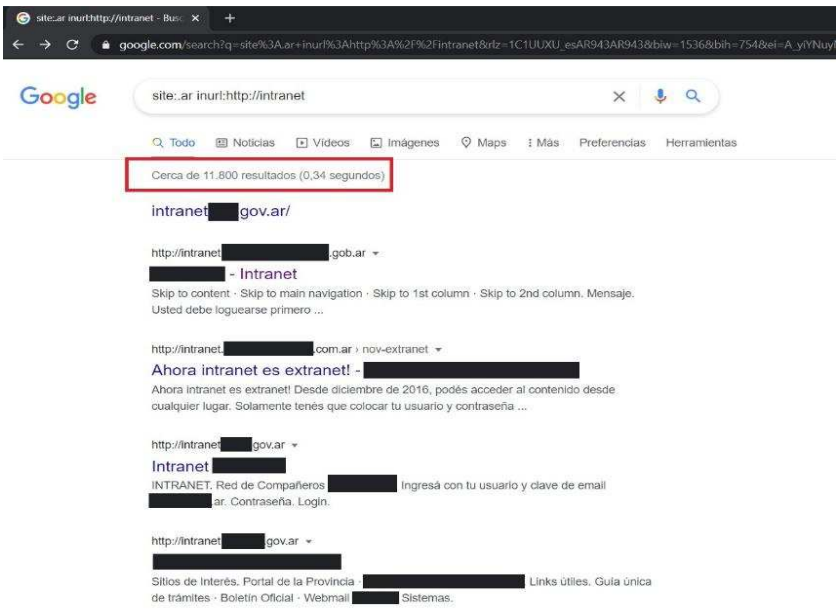



Figura 46: Búsqueda de intranet. Consulta: site:.ar inurl:http://intranet

Los inicios de sesión sobre el protocolo “http” pueden agravar la debilidad si quien se conecta para iniciar la sesión lo hace desde una conexión WiFi pública.

## Gestores de bases de datos expuestos

En esta sección se analiza  la exposición de páginas de inicio de sesión que correspondan a herramientas para la administración de bases de datos. La Figura 47 muestra los resultados devueltos por el buscador utilizando la consulta “**site:.ar inurl:/phpmyadmin/**”, en este caso se obtienen numerosos resultados, parte de ellos encuadrados en la consulta realizada y también son devueltos falsos positivos.

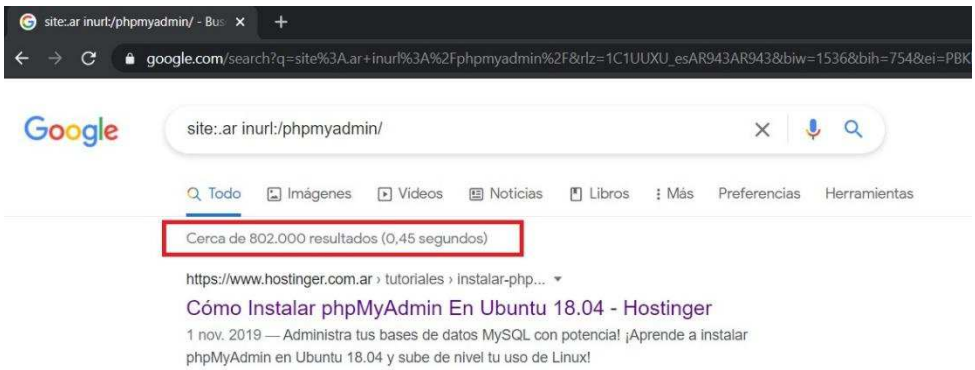



Figura 47: Búsqueda del gestor phpMyAdmin

En las Figuras 48 y 49 se muestran inicios de sesión perteneciente a distintos accesos a phpMyAdmin, accesibles desde los enlaces devueltos por el buscador en la consulta mostrada en la figura 47.

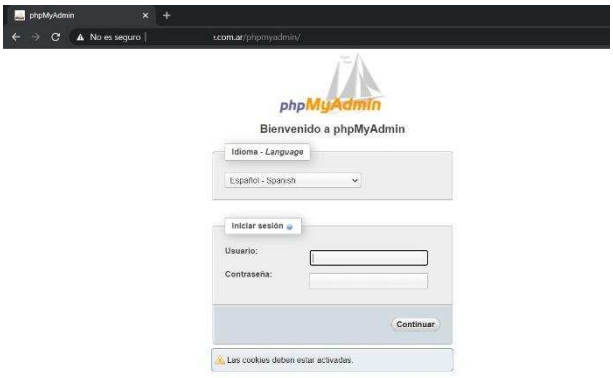



Figura 48: Inicio de sesión a phpMyAdmin

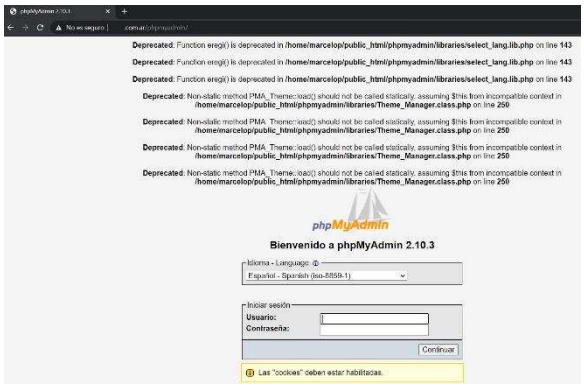



Figura 49: Inicio de sesión a phpMyAdmin

La herramienta “phpMyAdmin” permite la administración del servidor de bases de datos “MySQL”, la debilidad radica en la visibilidad desde internet de la interfaz de acceso a la administración de la base de datos lo que permite que un actor malicioso intente un ataque de fuerza bruta.

El análisis de gestores de bases de datos expuestos puede incluir entre otros los utilizados por la base de datos PostgreSQL. La Figura 50 muestra los resultados devueltos por el buscador a otra consulta en busca de sistemas de gestión de bases de datos, en este caso utilizando la consulta “**site:.ar inurl:/phppgadmin/**”, para localizar una herramienta para la administración de bases de datos PostgreSQL.

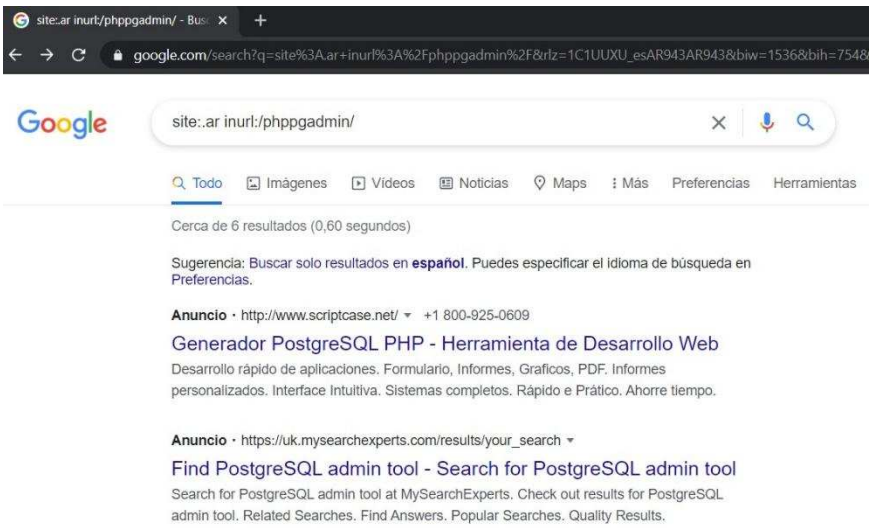



Figura 50: Búsqueda del gestor phpPgAdmin

En las Figuras 51 y 52 se muestran inicios de sesión pertenecientes a distintos accesos a phpPgAdmin accesibles desde los enlaces devueltos por el buscador en la consulta mostrada en la figura 50.

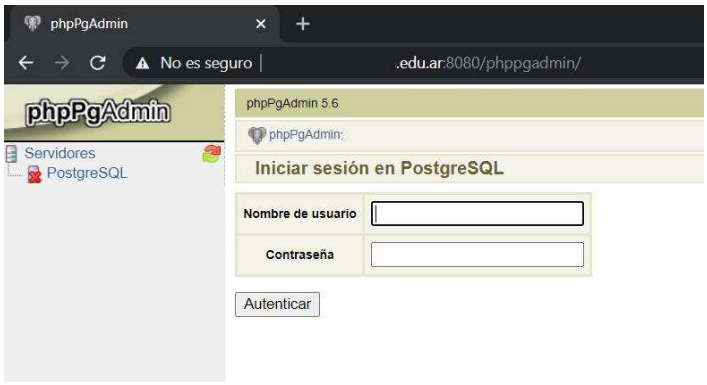



Figura 51: Inicio de sesión a phpPgAdmin


Figura 52: Inicio de sesión a phpPgAdmin

## Gestores de contenido inseguros

Como parte del análisis de inicios de sesión se pueden realizar búsquedas orientadas a descubrir accesos a gestores de contenidos como WordPress que cuenta con una interfaz de inicio de sesión al panel de administración. Utilizando la combinación de operadores avanzados de Google "**site:.ar inurl:/wp-admin**" se obtienen los siguientes resultados que se observan en la Figura 53.

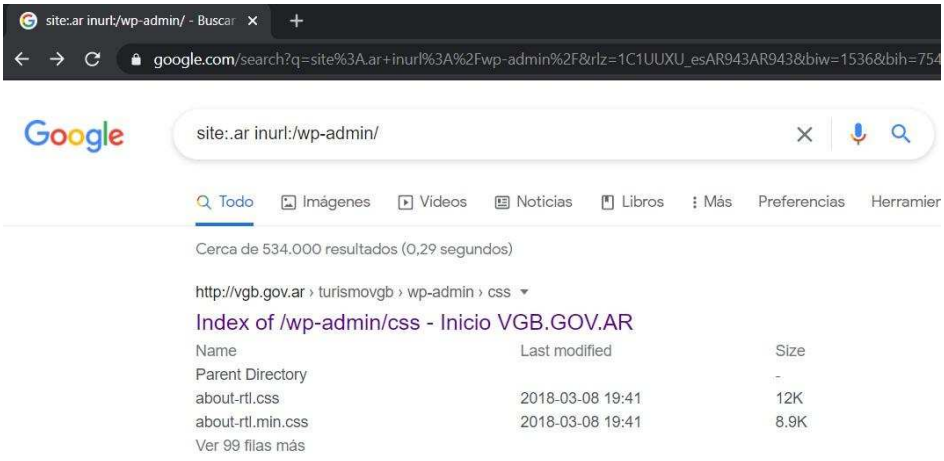



Figura 53: Búsqueda de inicio de sesión en WordPress

En las Figuras 54 y 55 se muestran inicios de sesión pertenecientes a distintos accesos a WordPress encontrados y accesibles desde los enlaces devueltos por el buscador en la consulta mostrada en la figura 53.

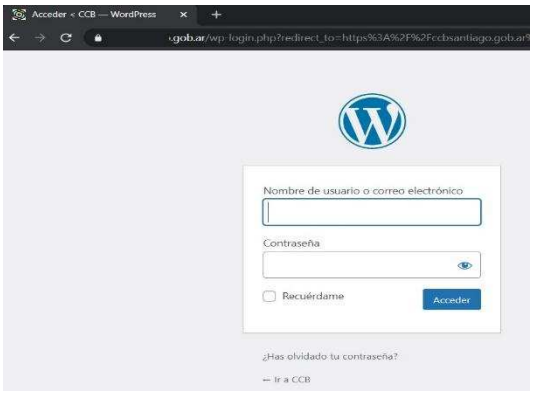



Figura 54: Inicio de sesión a WordPress

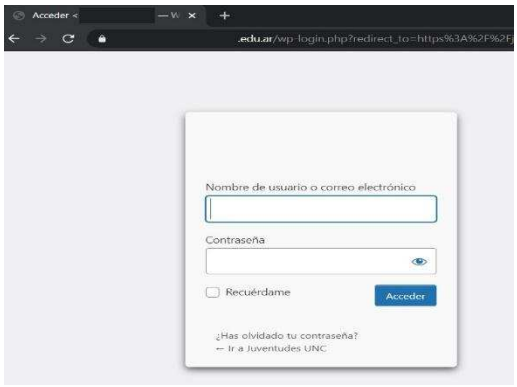



Figura 55: Inicio de sesión a WordPress

El gestor de contenido WordPress tiene numerosos reportes de vulnerabilidades, se puede analizar el código fuente de la página para ver las versiones del gestor utilizadas en los portales y posibles vulnerabilidades aún sin el parche aplicado. En la Figura 56 se observa la versión 5.3.2 del gestor de contenido que se logra visualizar en una página a través de la opción del navegador que permite ver el código fuente de la misma.

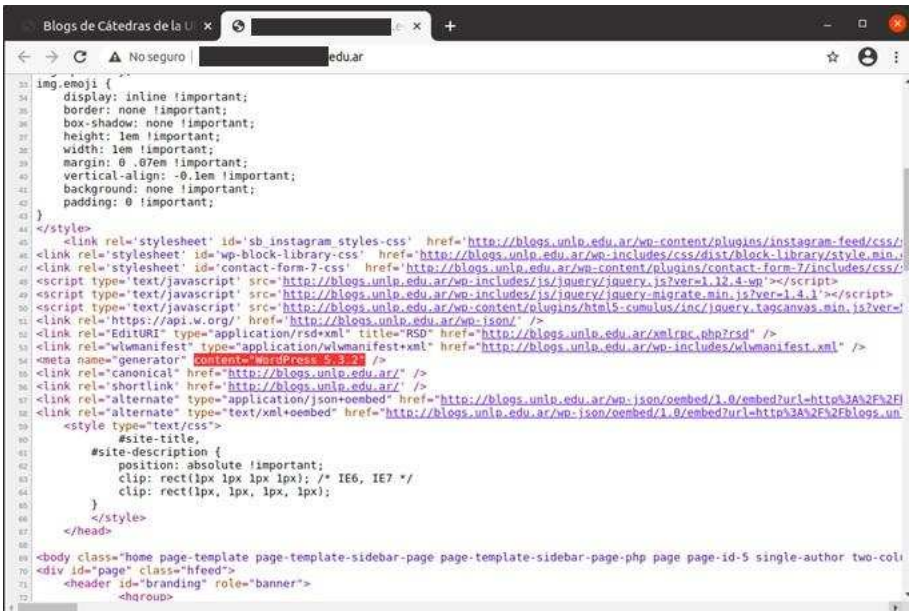



Figura 56: Código con la versión de WordPress

La versión 5.3.2 de WordPress tiene reportada múltiples vulnerabilidades [48]. Una de las más críticas es la del Plugin “Contact Form 7” [49]. Clasificada como CVE-2020-35489 y que afecta a la versión 5.3.1 y anteriores de dicho plugin. En base a la información antes mencionada, se busca la

versión del plugin activa en el sitio. En la Figura 57 y 58 se observa cómo se puede visualizar a través del código fuente de la página si WordPress tiene activo el plugin vulnerable [49].

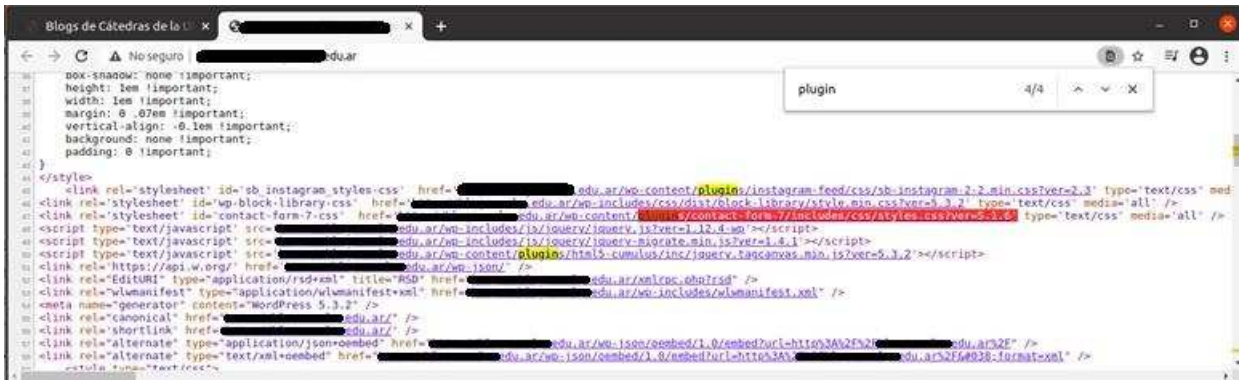



Figura 57: Código con la versión del Plugin


Figura 58: Código con la versión del Plugin

En la Figura 59 se muestra otro ejemplo donde se observa la versión 3.9.2 del gestor de contenido que se logra visualizar en la página observando el código desde el navegador.


Figura 59: Código con la versión de WordPress

Con la versión “Wordpress-3.9.2” obtenida, es posible consultar la lista CVE de vulnerabilidades de seguridad reportadas para dicha versión. La Figura 60 muestra el resultado obtenido en la consulta.

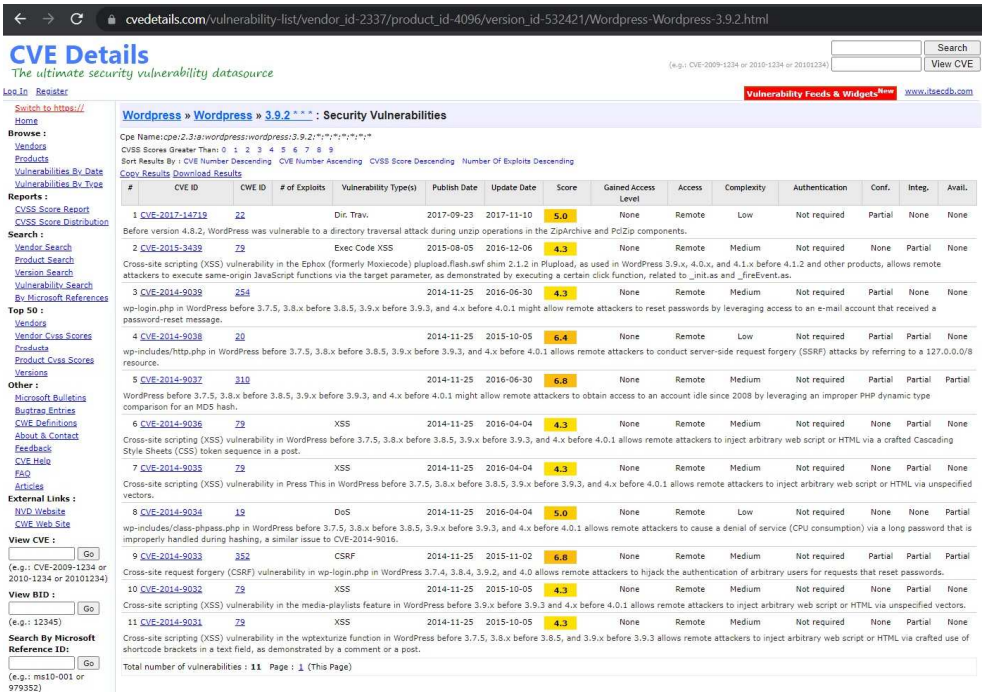



Figura 60: Lista CVE Details de vulnerabilidades en “WordPress 3.9.2”

La Figura 60 muestra un listado de once vulnerabilidades reportadas en la lista “CVE Details” para la versión 3.9.2 de “WordPress”.

# Dispositivos expuestos a Internet

En esta sección se utilizan recursos OSINT para analizar la exposición de dispositivos a Internet. Diferentes organizaciones, con el propósito de brindar conexión y permitir la gestión remota para mejorar los tiempos de respuesta y producción, habilitan servicios accesibles directamente desde Internet. Existen ocasiones en donde la tecnología utilizada, no fue pensada en su desarrollo para conectarse directamente a Internet y también aquellas donde las mismas han sido reportadas con diferentes vulnerabilidades. Estas situaciones representan un riesgo potencial para la organización que habilita algún servicio a través de ellas. Algunos ejemplos de esto último se ven en los sistemas de control industrial (ICS), donde muchos integran en el mismo hardware del dispositivo una interfaz web con un formulario de login que da acceso a la administración del dispositivo. En este sector se puede mencionar a los siguientes fabricantes como los más importantes [50]:

Siemens

ABB

Emerson process management

Rockwell automation

Schneider electric

Honeywell process solutions

Mitsubishi electric

Yokogawa electric

Omron automation

Danaher Industrial Ltd

Para buscar e identificar este tipo de dispositivos o servicios expuestos se pueden utilizar buscadores como Shodan o Censys.

La Figura 61 muestra los resultados que devuelve Shodan utilizando el filtro "**Schneider-WEB**" [51].

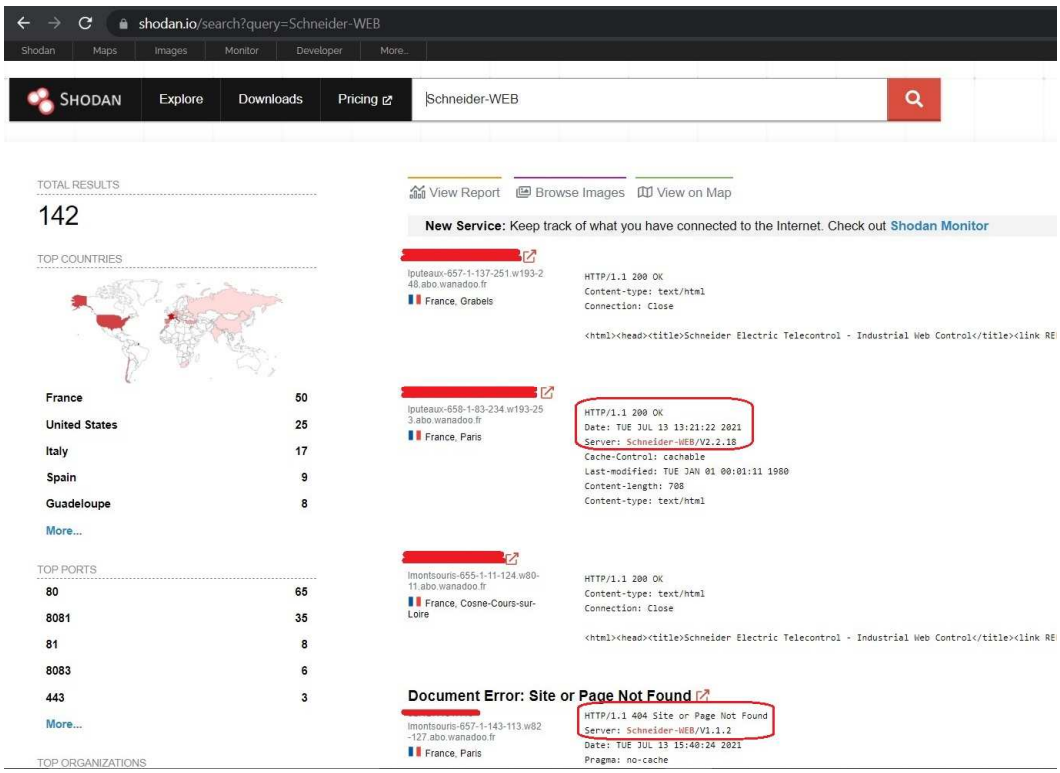



Figura 61: Búsqueda en Shodan filtro "Schneider-WEB"

En las Figuras 62, 63, 64 y 65 se observan inicios de sesión pertenecientes a los resultados mostrados por Shodan en la Figura 61 y accesibles desde los mismos.

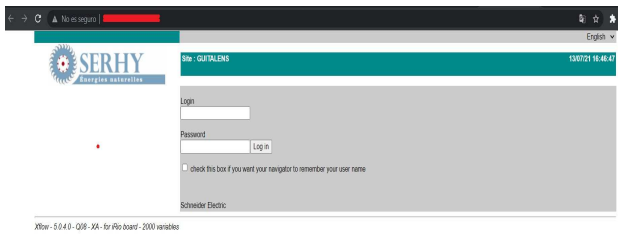



Figura 62


Figura 63

Figuras 62 y 63: Inicios de sesión accesibles desde enlaces de Shodan

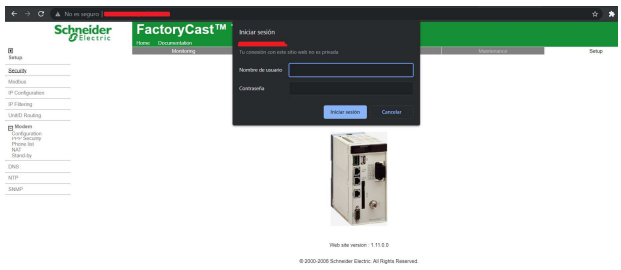



Figura 64

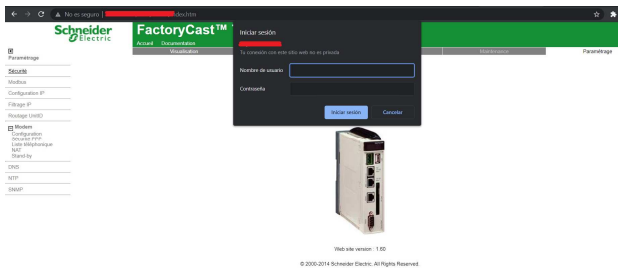



Figura 65

Figuras 64 y 65: Inicios de sesión accesibles desde enlaces de Shodan

La Figura 66 muestra los resultados que devuelve Shodan utilizando en este caso el filtro "**anti-web**" [51].

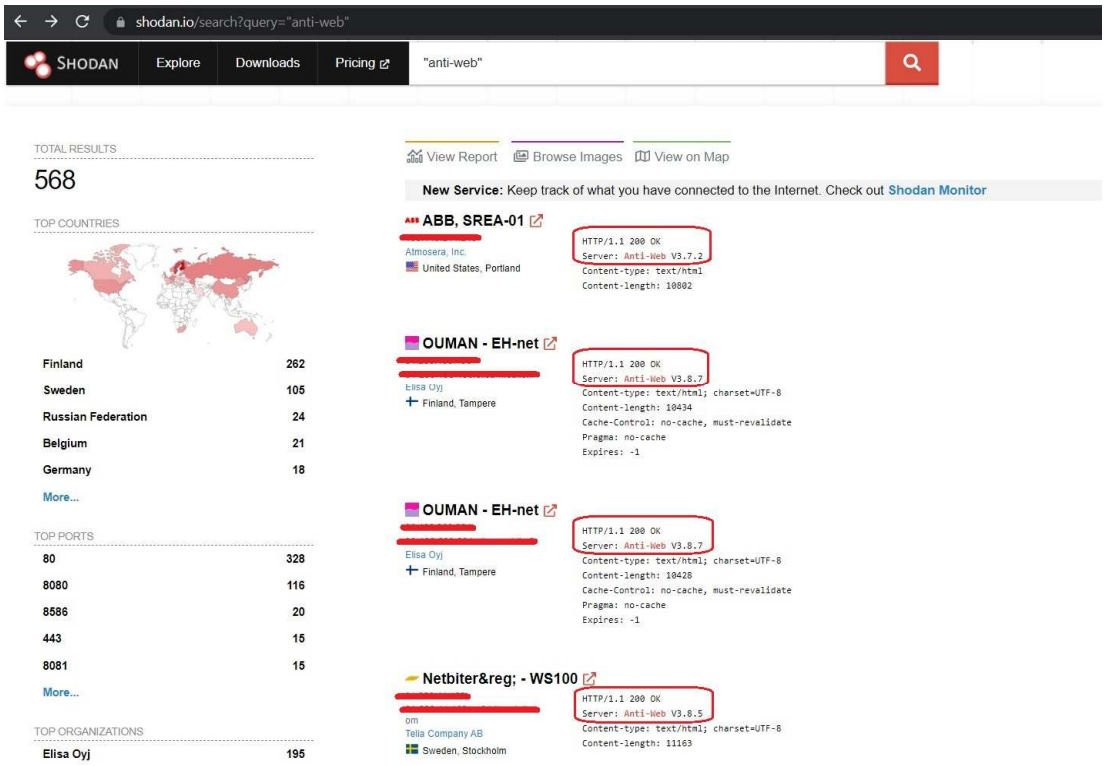



Figura 66: Búsqueda en Shodan filtro "anti-web"

En las Figuras 67, 68, 69 y 70 se observan inicios de sesión pertenecientes a los resultados mostrados por Shodan en la Figura 66 y accesibles desde los mismos.

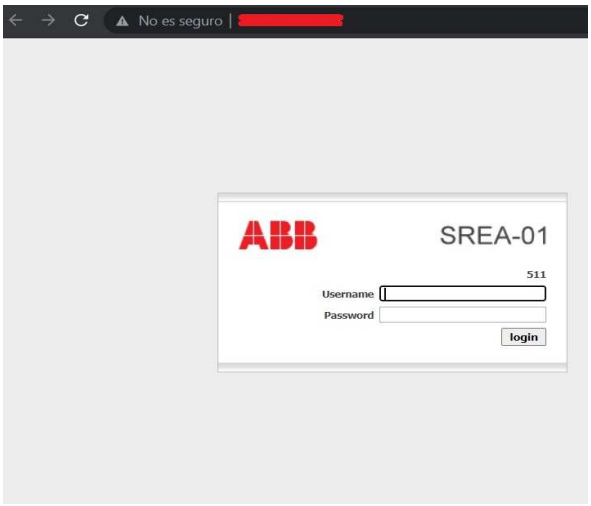



Figura 67


Figura 68

Figuras 67 y 68: Inicios de sesión accesibles desde enlaces de Shodan


Figura 69

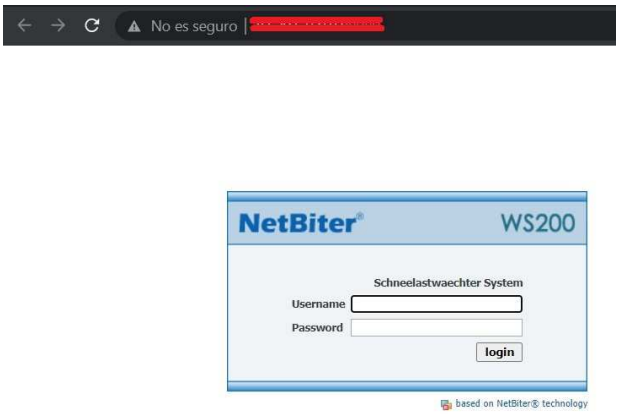



Figura 70

Figuras 69 y 70: Inicios de sesión accesibles desde enlaces de Shodan

En algunos casos estos dispositivos también están conectados a una terminal con servicio de escritorio remoto (RDP) habilitado lo cual da una doble vía a un actor de amenazas para intentar una acción maliciosa basada en fuerza bruta o diccionario. La figura 71 muestra uno de estos dispositivos con la interfaz web abierta en el puerto 8080 y un terminal con RDP habilitado en el puerto predeterminado 3389.

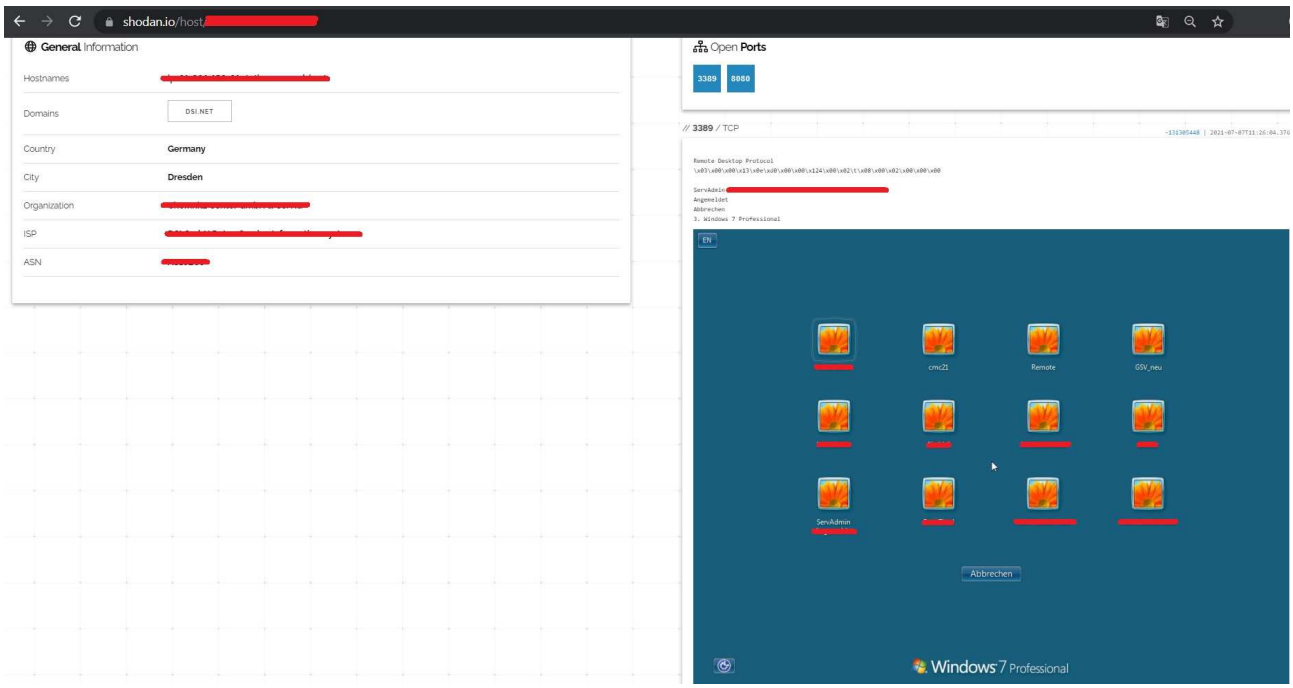



Figura 71: Información accesible desde enlaces de Shodan

# Detección de protocolos basados en UDP utilizados para DDoS

En esta sección se utilizan recursos OSINT para analizar la exposición de puertos conocidos a través de los cuales los actores maliciosos pueden abusar de protocolos y servicios basados en UDP. Para mayor información sobre ataques de amplificación basados en UDP en general se puede consultar la sección “Alerts” del “Cert-CISA” [17].

## DNS (Domain Name System)

Utilizando recursos OSINT como Shodan es posible realizar análisis en busca de servidores DNS con la recursividad habilitada.

La Figura 72 muestra los resultados obtenidos con Shodan utilizando el filtro **country:ar dns port:53 "Recursion: enabled"**

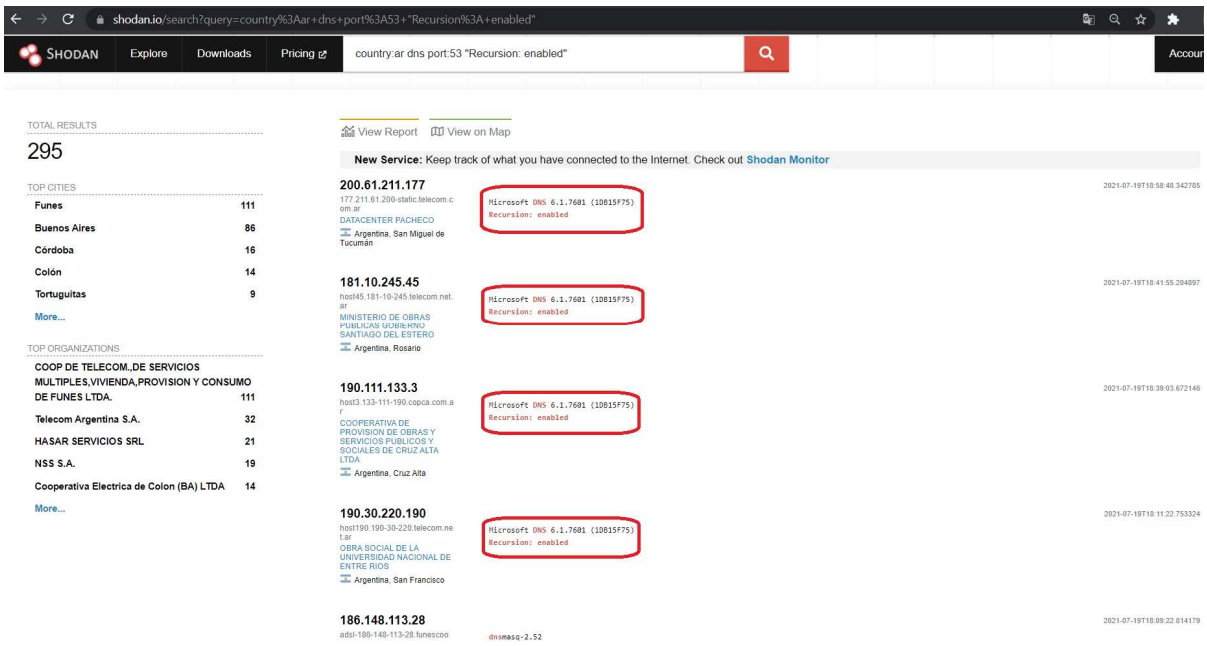



Figura 72: Dispositivos en el puerto 53 con “Recursión: enabled” mostrados por Shodan

Además se pueden mencionar como recursos OSINT disponibles para la detección de resolutores recursivos abiertos las siguientes herramientas de escaneo basadas en Web [18]:

- **DNSInspect**: este sitio ofrece una herramienta que permite ingresar el nombre de un dominio y testear los servidores DNS y de correo del mismo en busca de errores comunes. Disponible en: https://dnsinspect.com/
- **OpenResolver**: este sitio ofrece una herramienta que permite ingresar un dirección IP o el nombre de dominio del servidor que se quiere testear. Si el testeo devuelve el mensaje “open-resolver-detected”, entonces el servidor tiene un problema en su configuración. Disponible en: https://openresolver.com/

Utilizando “openresolver.com” se analizan dos de las IP encontradas por Shodan con "Recursión: enabled".

Las Figuras 73 y 74 muestran los resultados devueltos por esta herramienta a las consultas realizadas.

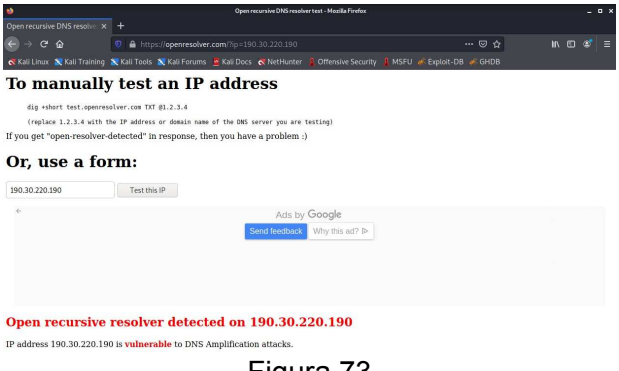



Figura 73

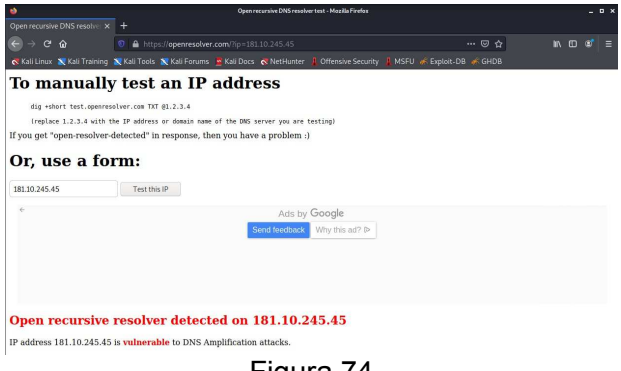


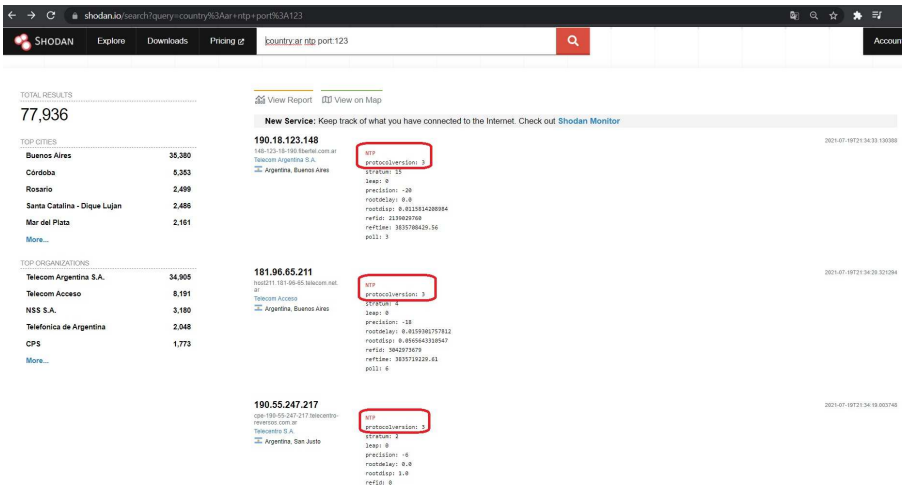

Figura 74

Figuras 73 y 74: resultado consultas a “openresolver.com”

Un servidor DNS recursivo solo debe responder consultas de clientes que se encuentren en su misma red y rechazar cualquier otra proveniente de una red externa.

## NTP (Network Time Protocol)

Utilizando Shodan es posible realizar búsquedas de dispositivos con el puerto 123 abierto, utilizado de forma predeterminada por NTP.
La Figura 75 muestra los resultados obtenidos con Shodan utilizando el filtro **country:ar ntp port:123**.




Figuras 75: Dispositivos en el puerto 123 mostrados por Shodan

Para determinar si el sistema es vulnerable se puede utilizar el comando “ntpdc monlist <ip>”, disponible en la mayoría de las distribuciones UNIX y Linux [52]. También se puede utilizar la herramienta local Nmap que incluye un script que permite obtener los datos del monitor de un servidor NTP con el siguiente comando [53]: “nmap -sU -pU:123 -Pn -n --script=ntp-monlist <ip>”

## Memcached

Utilizando Shodan se pueden listar servidores Memcached con el filtro “product:”Memcached””.
La Figura 76 muestra el número de servidores Memcached mostrados por Shodan. Se puede observar una reducción importante en el número de servidores que encuentra Shodan con respecto al año 2018 mostrado anteriormente, aunque continúa siendo alto.

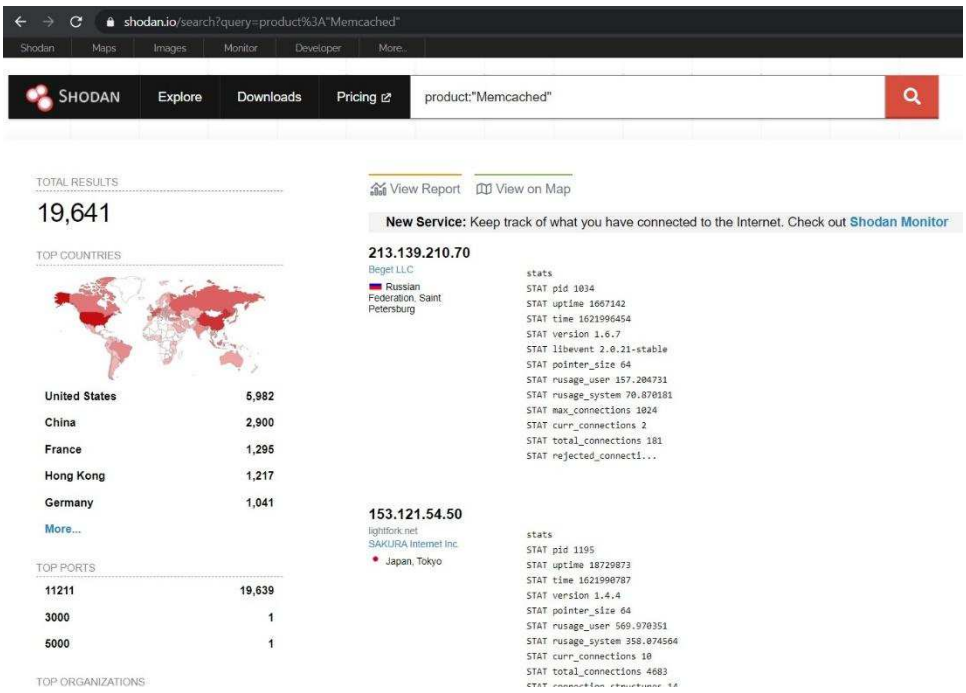



Figura 76: Servidores Memcached listados por Shodan

La Figura 77 muestra el resultado mostrado por Shodan en la búsqueda de servidores Memcached en Argentina aplicando el filtro "**country:ar product:"Memcached**".

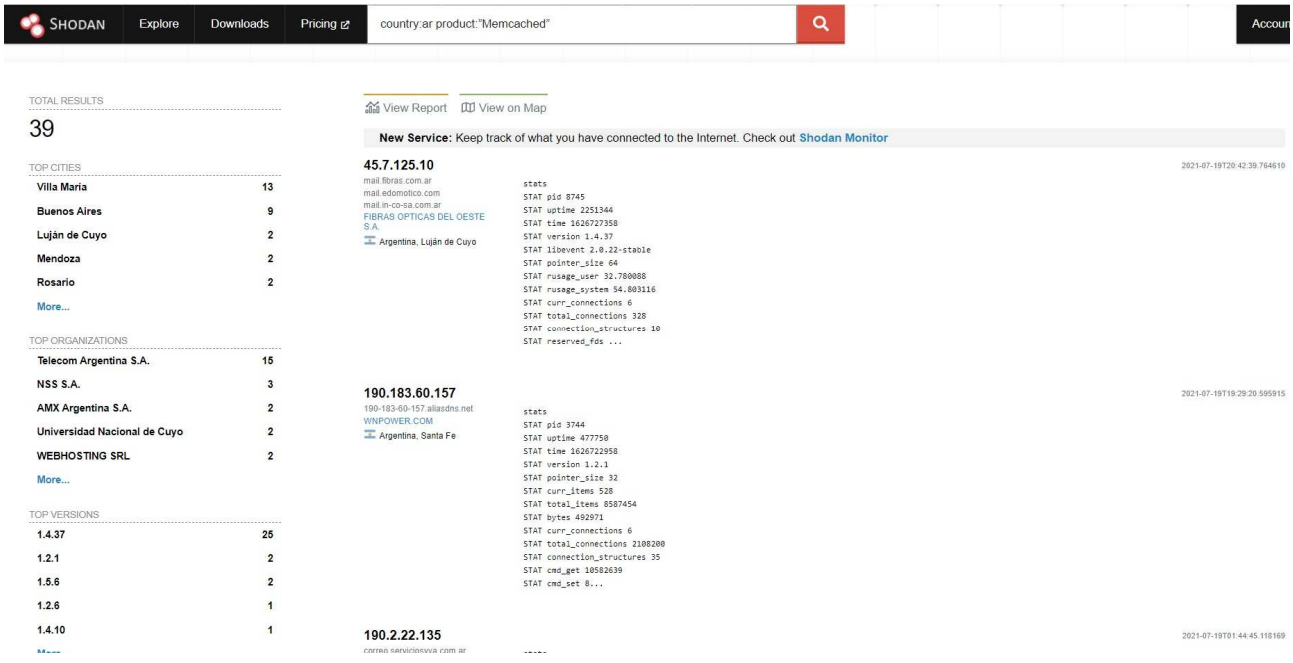



Figura 77: Servidores Memcached en Argentina mostrados por Shodan

Para mitigar y reducir al máximo posible las posibilidades de abuso de servidores memcached se recomiendan algunas de las siguientes acciones [54]:

- Reducir los servicios Memcached expuestos a Internet.
- Filtrar los puertos expuestos.
- Limitar la velocidad del tráfico entrante y saliente dirigido a los puertos expuestos.
- Deshabilitar UDP de forma predeterminada en el servicio de Memcached.

## WS-Discovery (WSD)

La Figura 78 muestra el resultado mostrado por Shodan en la búsqueda realizada utilizando el filtro "**country:ar port:3702**", puerto utilizado de forma predeterminada por WS-Discovery.

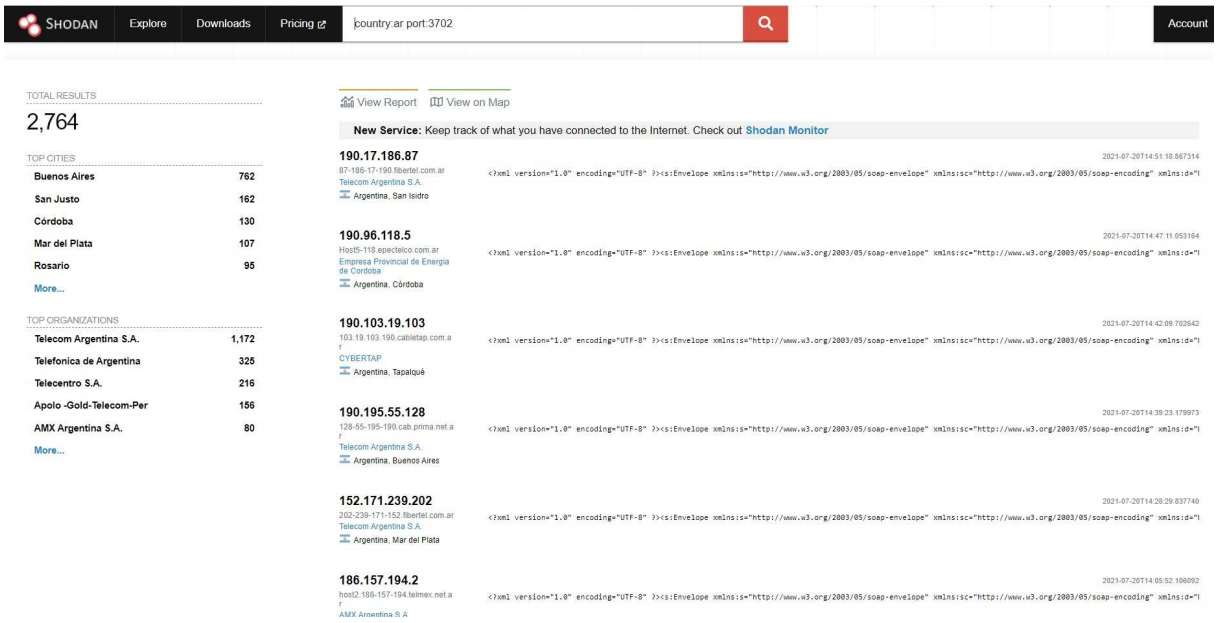



Figura 78: Dispositivos en el puerto 3702 mostrados por Shodan

Para mitigar un posible ataque al puerto UDP 3702 se recomienda contar con un proveedor de mitigación de DDoS que gestione ACL (Lista de control de acceso) y bloquee el tráfico ante un ataque o gestionar sus propias listas de acceso [24].

## Chargen

La Figura 79 muestra el resultado devuelto por Shodan en la búsqueda realizada utilizando el filtro "**country:ar port:19**", puerto utilizado de forma predeterminada por Chargen.

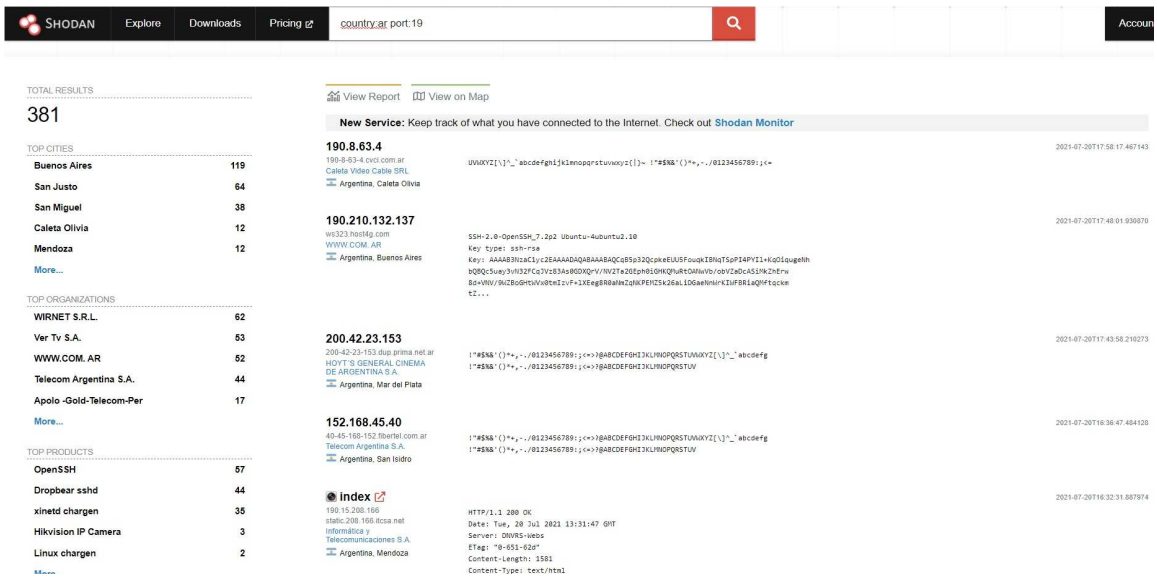



Figura 79: Dispositivos en el puerto 19 mostrados por Shodan

Para determinar si el sistema tiene Chargen habilitado se puede utilizar el siguiente comando “nc -u <ip> 19”, disponible en la mayoría de las distribuciones Linux en la herramienta “Netcat” [25]. Para mitigar un posible ataque al puerto UDP 19 se recomienda desactivar el servicio o bloquear el puerto de no utilizarse.

## QOTD

La Figura 80 muestra el resultado devuelto por Shodan en la búsqueda realizada utilizando el filtro “**country:ar port:17**”, puerto utilizado de forma predeterminada por QOTD.

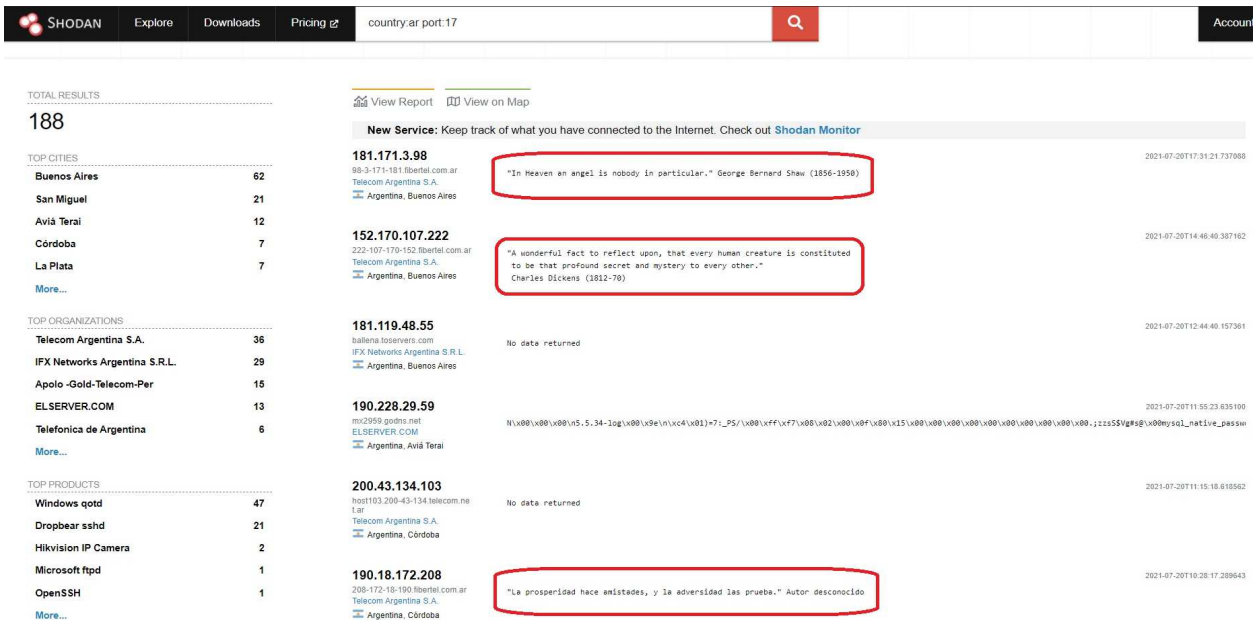



Figura 80: Dispositivos en el puerto 17 con diferentes frases mostrados por Shodan

Para determinar si el sistema tiene QOTD habilitado se puede utilizar el siguiente comando “nc -u <ip> 17”, disponible en la mayoría de las distribuciones Linux en la herramienta “Netcat” [26].
Para mitigar un posible ataque al puerto UDP 17 se recomienda desactivar el servicio o bloquear el puerto de no utilizarse o configurar el firewall para bloquear el tráfico TCP y UDP hacia el puerto 17.

## SSDP

La Figura 81 muestra el resultado devuelto por Shodan en la búsqueda realizada utilizando el filtro “**country:ar port:1900**”, puerto utilizado de forma predeterminada por SSDP.

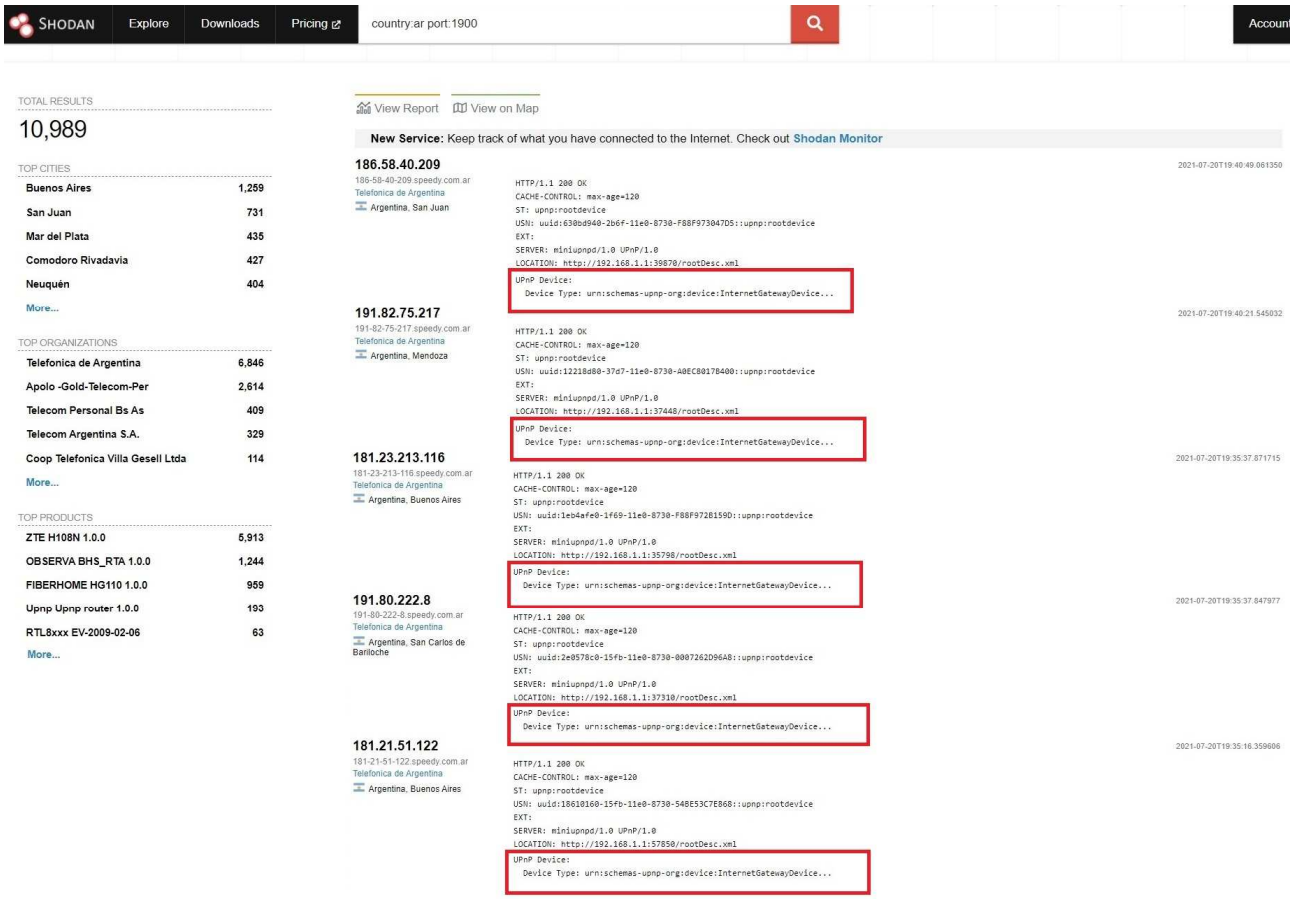



Figura 81: Dispositivos en el puerto 1900 mostrados por Shodan

Para determinar si el sistema tiene SSDP habilitado se puede emplear la herramienta local “tcpdump” disponible para Linux utilizando el siguiente comando “tcpdump -i any -n -Ss 0 -Xx host <ip>” [55].
Para mitigar un posible abuso de SSDP en el puerto UDP 1900 se recomienda desactivar el servicio o bloquear el puerto de no utilizarse, rechazar cualquier tráfico UDP con dirección falsificada (spoofed) o limitar solo el acceso desde la red interna hacia el puerto 1900.

# Protocolos y servicios vulnerables

Diferentes organizaciones, con el propósito de brindar conexión, compartir recursos o permitir la gestión remota para mejorar los tiempos de respuesta y producción, habilitan servicios accesibles directamente desde Internet como por ejemplo RDP (Remote Desktop Protocol), SMB (Server Message Block), Telnet y CWMP (Customer Premises Equipment Wan Management Protocol).

## RDP (Remote Desktop Protocol)

El protocolo de escritorio remoto utiliza por defecto el puerto TCP 3389 [56].
Utilizando recursos OSINT como Shodan se puede realizar un análisis en busca de servicios de escritorio remoto disponibles a través de RDP para su identificación.
La Figura 82 muestra los resultados obtenidos con Shodan utilizando el filtro "**country:ar port:3389,3388 "Remote Desktop Protocol"**"

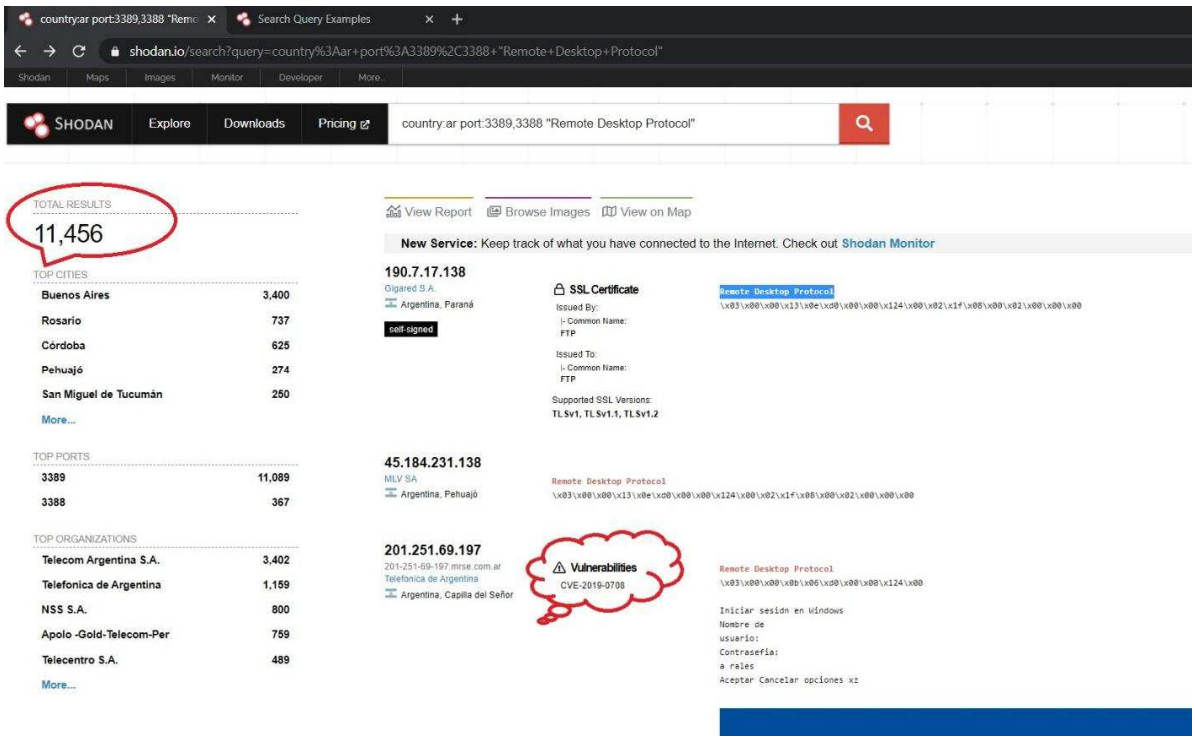



Figura 82: Dispositivos en los puertos 3388 y 3389 mostrados por Shodan

Para mitigar un posible abuso se recomienda bloquear todo acceso hacia los puertos que se encuentren configurados para el uso de RDP. En caso de ser necesario iniciar sesión a través de RDP, utilizar contraseñas fuertes, instalar y configurar doble factor de autenticación (2FA), aislar el host en un segmento diferente y mantener el sistema con las últimas actualizaciones y parches son solo algunos ejemplos de medidas que buscan asegurar el uso de RDP [57].

## SMB (Server Message Block)

El protocolo de bloques de mensajes del servidor utiliza por defecto el puerto 445 pero también se lo puede encontrar utilizando los puertos  TCP 139 y UDP 137 y 138 [58].
Utilizando recursos OSINT como Shodan se puede realizar un análisis en busca de  estos puertos abiertos.
La Figura 83 muestra los resultados obtenidos con Shodan utilizando el filtro "**country:ar port:445**"

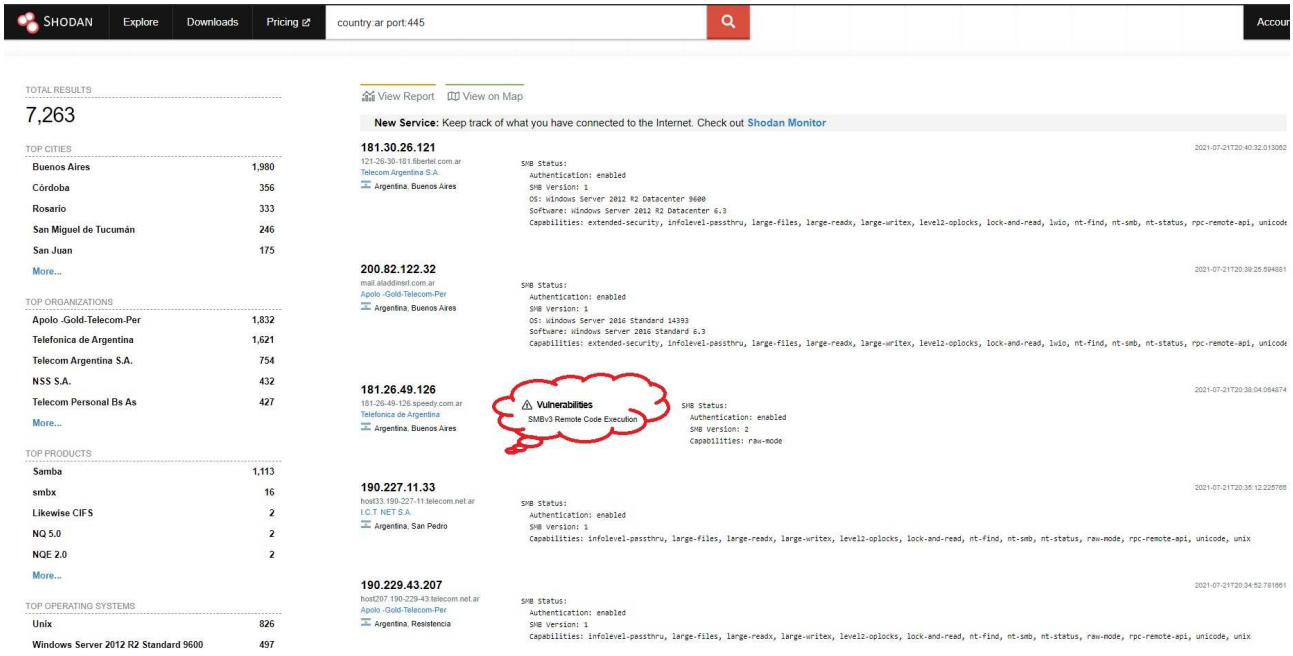



Figura 83: Dispositivos en el puerto 445 mostrados por Shodan

Para mitigar un posible abuso se recomienda bloquear todo acceso hacia los puertos que se encuentren configurados para el uso de SMB. Aplicar los parches de seguridad en Windows para solucionar los problemas asociados a SMB.

## Telnet (Server Message Block)

El protocolo cliente-servidor Telnet permite el acceso remoto a un equipo y no utiliza ningún cifrado por lo que los datos que intercambian los equipos en la comunicación viajan en texto plano. Un actor malicioso puede capturar las credenciales utilizadas en una comunicación. Utiliza por defecto el puerto TCP 23 y  también se lo puede encontrar utilizando el puerto 2323 [59].
Utilizando Shodan se puede realizar un análisis en busca de dispositivos con el puerto 23 abierto.
La Figura 84 muestra los resultados obtenidos con Shodan utilizando el filtro "**country:ar port:23**"

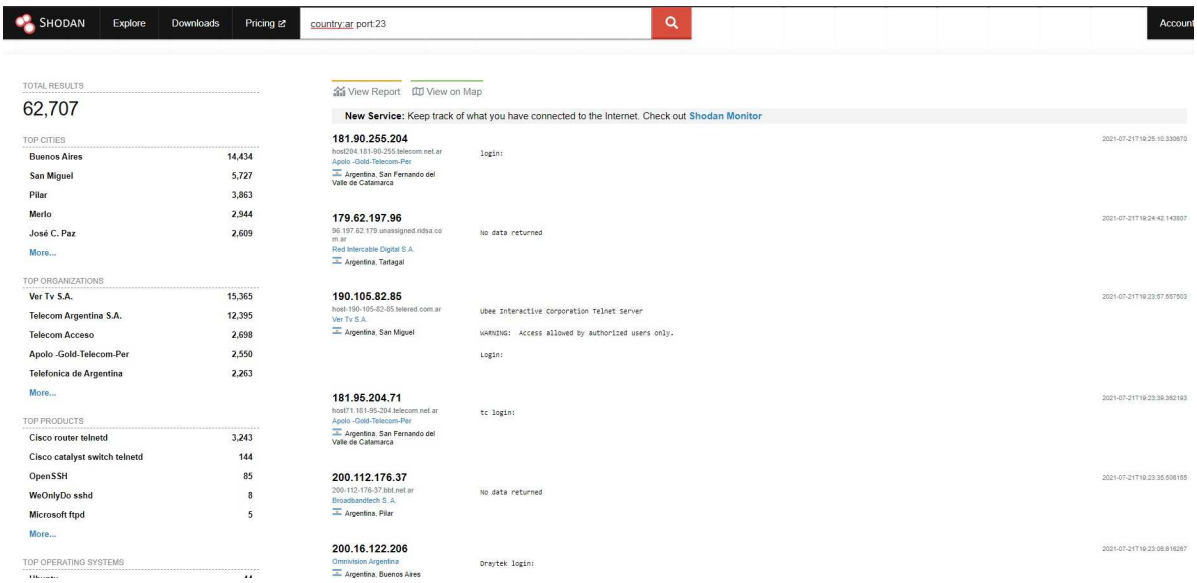



Figura 84: Dispositivos en el puerto 23 mostrados por Shodan

Para mitigar vulnerabilidades asociadas a Telnet se recomienda bloquear todo acceso hacia los puertos 23 y 2323 que se encuentren configurados para el uso de Telnet. Utilizar aplicaciones similares que utilicen cifrado para la transmisión de los datos intercambiados en la comunicación entre los hosts.

## CWMP (Customer Premises Wan Management Protocol)

El protocolo CWMP permite la administración remota de dispositivos de cliente como router, modems, gateway, decodificadores, cámaras, teléfonos VoIP y otros. Utiliza por defecto el puerto TCP 7547 y también se lo puede encontrar utilizando el puerto 30005 [60].
Utilizando Shodan se puede realizar un análisis en busca de dispositivos con el puerto 7547 abierto. La Figura 85 muestra los resultados obtenidos con Shodan utilizando el filtro "**country:ar port:7547**"

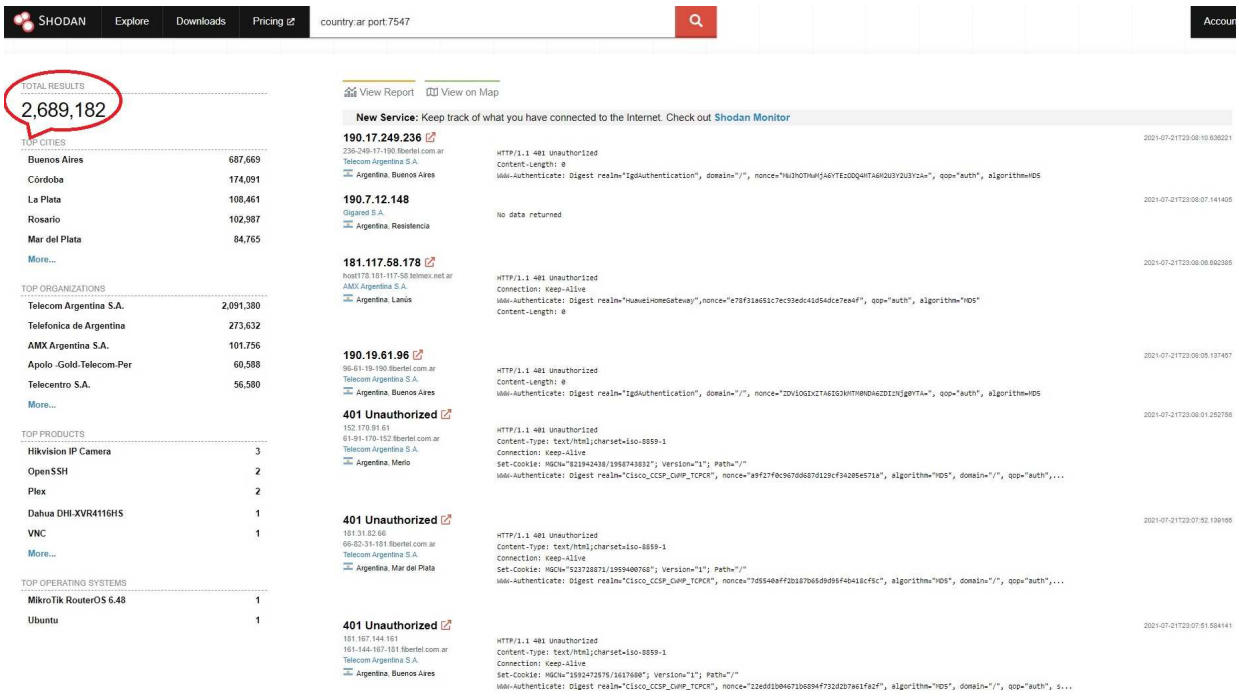
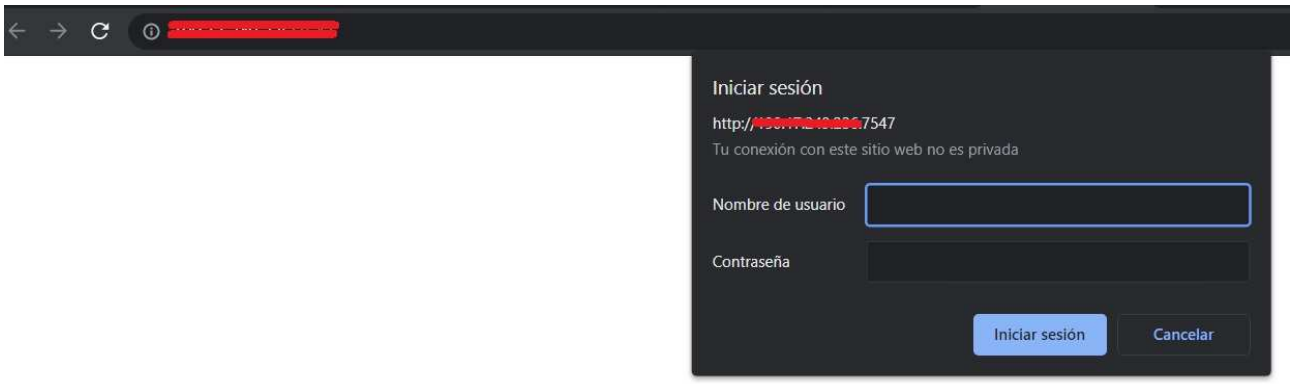



Figura 85: Dispositivos en el puerto 7547 mostrados por Shodan

En la Figura 86 se observa un inicio de sesión accesible desde uno de los resultados mostrados por Shodan en la Figura 85.




Figuras 86: Inicio de sesión accesibles desde enlace de Shodan

En muchos casos estos dispositivos exponen la interfaz de inicio de sesión a Internet con configuraciones por defecto o credenciales débiles lo cual da la posibilidad que un actor de amenazas utilizando estas vulnerabilidades intente una acción maliciosa basada en fuerza bruta o diccionario y tome el control del dispositivo.

# Bases de datos vulnerables

Utilizando Shodan con el filtro “**country:ar "database"**” el buscador enumera diferentes tecnologías de bases de datos.

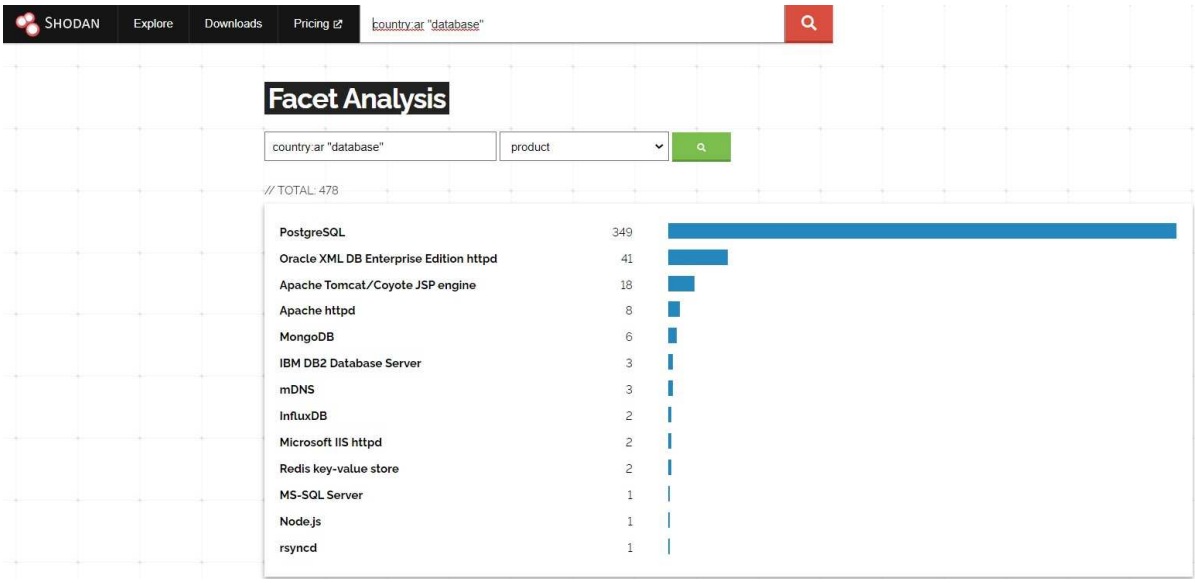



Figura 87: Bases de datos mostrada por Shodan

**MongoDB**: para buscar dispositivos con el puerto 27017 abierto donde MongoDB acepta conexiones externas a la red local se puede utilizar el filtro “**country:ar port:27017 "MongoDB"**” [28]. La Figura 88 muestra los resultados obtenidos con Shodan.

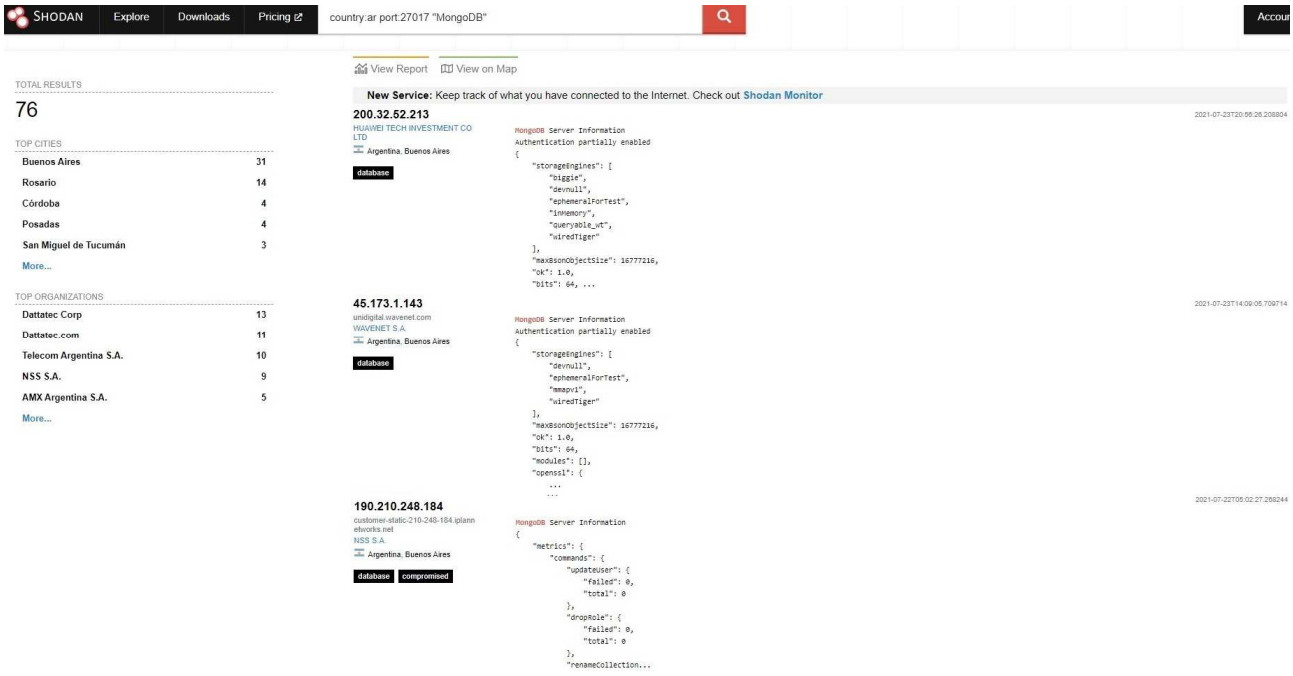



Figura 88: Dispositivos en el puerto 27017 mostrados por Shodan

Algunas acciones posibles para mitigar los riesgos son comprobar que la configuración de seguridad se encuentre configurada de manera correcta. Realizar backups frecuentemente. Mantener actualizada la base de datos a la última versión.

**Elasticsearch**: para buscar dispositivos con el puerto 9200 abierto donde Elasticsearch acepta conexiones por defecto se puede utilizar el filtro "**country:ar port:9200 "Elastic"**" [29]. La Figura 89 muestra los resultados obtenidos con Shodan.

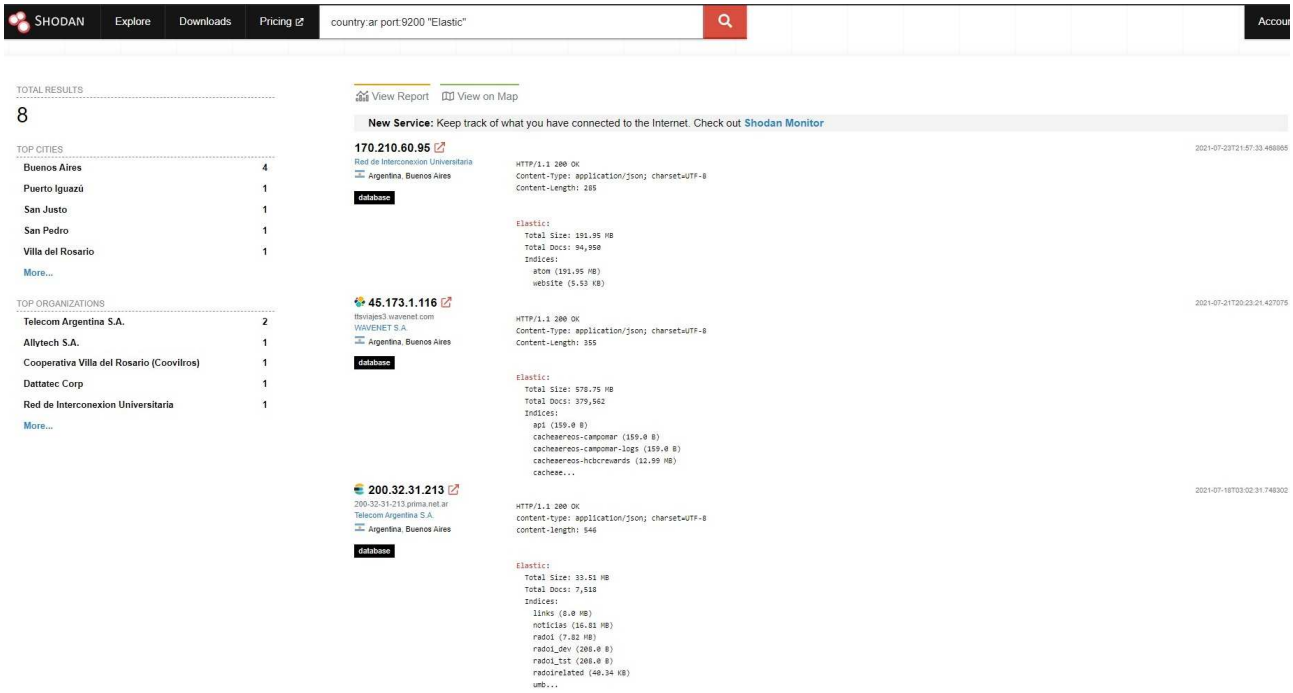



Figura 89: Dispositivos en el puerto 9200 mostrados por Shodan

Algunas medidas posibles para mitigar los riesgos son agregar autenticación a Elasticsearch, bloquear el puerto 9200, ubicarlo detrás de un Firewall, no correr Elasticsearch como root.

# Capítulo 4 – Conclusiones y Trabajos a futuro

## Conclusiones

En el desarrollo de este trabajo se mostró la gran cantidad de información que se puede extraer de los activos que las organizaciones exponen a Internet. Se puede recopilar información de una organización, una red, un dispositivo, bases de datos, servidores, dominios, sitios web, direcciones ip, servicios y puertos entre otros.

Es frecuente la utilización de vectores de ataque que explotan vulnerabilidades presentes en los activos de las organizaciones. En el desarrollo del trabajo se presentó la aplicación de tácticas, técnicas y procedimientos que hacen uso de fuentes abiertas y pueden ser utilizadas para la detección de vulnerabilidades y amenazas. También se presentaron vulnerabilidades de severidad alta o crítica y la existencia de estas en los activos de las organizaciones como un problema recurrente. En el mismo orden se describieron las amenazas más significativas que aprovechan estas debilidades.

Para finalizar, el uso de fuentes de datos abiertas puede brindar a los profesionales responsables de la seguridad de la información en una organización una mayor visibilidad de los activos expuestos que les permita mejorar las defensas y mitigar los riesgos en la búsqueda de una mejora continua de la postura de seguridad de la organización.

## Trabajos a Futuro

En el presente trabajo final el análisis de OSINT se enfocó en la utilización de tácticas, técnicas y procedimientos que hacen uso de diferentes buscadores y servicios. Los mismos permiten tener una imagen y visibilidad de los activos de una organización desde un posicionamiento externo a la misma.

Continuando con esta línea de investigación para trabajos futuros se identifica la utilización de fuentes OSINT en sistemas de correlación de eventos, gestión de incidentes y mecanismos de protección como los IDS. Estos sistemas y mecanismos de protección permiten obtener información de fuentes abiertas, identificar, analizar y gestionar eventos de seguridad desde un posicionamiento interno. Además posibilitan a los profesionales de la seguridad de la información divisar y contener incidentes asociados con amenazas a los activos de una organización.

# Bibliografía


**[1]** Ivo Vacas, Iberia Medeiros, Nuno Neves (2018) “Detecting Network Threats using OSINT Knowledge Based IDS”, 2018 14th European Dependable Computing Conference (EDCC), Iasi, 2018, pp. 128-135.

**[2]** Luis Rosa, Miguel Freitas, Sergey Mazo, Edmundo Monteiro, Tiago Cruz, Paulo Simoes, (2019) “A Comprehensive Security Analysis of a SCADA Protocol: From OSINT to Mitigation”, 2019 IEEE, disponible en:http://www.ieee.org/publications_standards/publications/rights/index.html

**[3]** X-Force, IBM (2020), “X-Force Threat Intelligence Index”, disponible en: https://www.ibm.com/security/data-breach/threat-intelligence

**[4]** Christopher Hobbs, Daniel Salisbury, Matthew Moran (2014) “Open Source Intelligence in the Twenty First Century”, Springer.

**[5]** Instituto Nacional de Ciberseguridad (INCIBE 2017), “Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?”, disponible en: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

**[6]** Common Vulnerabilities and Exposures (CVE), Mitre Corporation (2020), disponible en: https://www.cvedetails.com/cve-help.php

**[7]** Common Vulnerability Scoring System, FIRST (2020), “Common Vulnerability Scoring System v3.1: Specification Document“, disponible en: https://www.first.org/cvss/specification-document

**[8]** Microsoft Security Bulletin, Microsoft (2017), “Microsoft Security Bulletin MS17-010 – Critical”, disponible en: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

**[9]** National Vulnerability Database, National Institute of Standard and Technology (NIST), disponible en: https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=CVE-2017-0143&queryType=phrase&search_type=all

**[10]** National Vulnerability Database, National Institute of Standard and Technology (NIST), disponible en: https://nvd.nist.gov/vuln/detail/CVE-2017-11882

**[11]** National Vulnerability Database, National Institute of Standard and Technology (NIST), disponible en: https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=CVE-2017-0199&queryType=phrase&search_type=all

**[12]** National Vulnerability Database, National Institute of Standard and Technology (NIST), disponible en: https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=CVE-2017-8759&queryType=phrase&search_type=all

**[13]** National Vulnerability Database, National Institute of Standard and Technology (NIST), disponible en: https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=CVE-2017-5638&queryType=phrase&search_type=all

**[14]** National Vulnerability Database, National Institute of Standard and Technology (NIST), disponible en: https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=CVE-2019-0708&queryType=phrase&search_type=all

**[15]** Detectify blog, Detectify Crowdsource (2020), "Top 10 Most Critical CVEs Added in 2020", disponible en: https://blog.detectify.com/2020/12/30/top-10-critical-cves-added-in-2020/

**[16]** European Union Agency for Cybersecurity, (ENISA 2020), "ENISA Threat Landscape 2020 – List of top 15 threats", disponible en: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

**[17]** Cybersecurity & Infrastructure Security Agency, (CISA), "UDP-Based Amplification Attacks", disponible en: https://us-cert.cisa.gov/ncas/alerts/TA14-017A

**[18]** CISA, Us-Cert, Alert (TA13-088A) (2019) "DNS Amplification Attacks", disponible en: https://us-cert.cisa.gov/ncas/alerts/TA13-088A

**[19]** CS blog, Capital Software Blog (2020), "Cinco ataques DDoS más famosos", disponible en: https://capitalsoftware.com.ni/2020/08/05/cinco-ataques-ddos-mas-famosos-y-luego-algunos/#:~:text=El%2020%20de%20septiembre%20de,el%20mayor%20ataque%20jam%C3%A1s%20visto.

**[20]** EcuCERT-ARCOTEL, Centro de Respuesta a Incidentes Informaticos, disponible en: https://www.ecucert.gob.ec/wp-content/uploads/2021/07/Ficha-Tecnica-ntp-monitor.pdf

**[21]** Akamai blog, The akamai blog (2018), "Memcached UDP Reflection Attacks", disponible en: https://blogs.akamai.com/2018/02/memcached-udp-reflection-attacks.html

**[22]** Cloudflare blog, Cloudflare (2018), "Memcrashed - Major amplification attacks from UDP port 11211", disponible en: https://blog.cloudflare.com/memcrashed-major-amplification-attacks-from-port-11211/

**[23]** Eset WeLiveSecurity, "Los dos ataques DDoS más grandes de la historia se registraron en tan solo cuatro días de diferencia", disponible en: https://www.welivesecurity.com/la-es/2018/03/08/ataques-ddos-mas-grandes-historia-registraron-solo-cuatro-dias/

**[24]** Akamai blog, The akamai blog (2019), "New DDoS Vector Observed in the Wild: WSD attacks hitting 35/Gbps", disponible en: https://blogs.akamai.com/sitr/2019/09/new-ddos-vector-observed-in-the-wild-wsd-attacks-hitting-35gbps.html

**[25]** The Shadowserver Foundation, Chargen Service Scanning Project, disponible en: https://scan.shadowserver.org/chargen/

**[26]** The Shadowserver Foundation, Quote of the Day Service Scanning Project, disponible en: https://scan.shadowserver.org/qotd/

**[27]** Cisco, "Cisco Annual Internet Report (2018 – 2023)", disponible en: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

**[28]** The Shadowserver Foundation, Open MongoDb Report, disponible en: https://www.shadowserver.org/what-we-do/network-reporting/open-mongodb-report/

**[29]** The Shadowserver Foundation, Open Elasticsearch Report, disponible en: https://www.shadowserver.org/what-we-do/network-reporting/open-elasticsearch-report/

**[30]** IBM, "Boletín de seguridad: Vulnerabilidad de denegación de servicios en DB2", disponible en: https://www.ibm.com/support/pages/node/234369

**[31]** CrowdStrike, Resource Center, "La Evolución del Ransomware", disponible en: https://www.crowdstrike.com/resources/white-papers/la-evolucion-del-ransomware/

**[32]** Mitre corporation, "MITRE ATT&CK", disponible en: https://attack.mitre.org/

**[33]** Government Printing Office, "Public Law 109-163 109th Congress" August 25, 2017, disponible en: https://www.gpo.gov/fdsys/pkg/PLAW-109publ163/html/PLAW-109publ163.htm

**[34]** Asier Martinez, Incibe-Cert, Blog (2014) "OSINT – La información es poder", disponible en: https://www.incibe-cert.es/blog/osint-la-informacion-es-poder

**[35]** Jesse Alpert, Nissan Hajaj, Google Blog oficial (2008) "We knew the web was big", disponible en: https://googleblog.blogspot.com/2008/07/we-knew-web-was-big.html.

**[36]** Andy Patrizio, Network World (2018) "IDC:Expect 175 zettabytes of data worldwide by 2025", disponible en: https://www.networkworld.com/article/3325397/idc-expect-175-zettabytes-of-data-worldwide-by-2025.html

**[37]** Michael Cooney, Network World (2018) "Cisco predicts nearly 5 zettabytes of IP traffic per year by 2022", disponible en: https://www.networkworld.com/article/3323063/cisco-predicts-nearly-5-zettabytes-of-ip-traffic-per-year-by-2022.html

**[38]** Andrea Nuñez, TICbeat (2019) "¿Cuántas páginas web existen en el mundo en la actualidad?", disponible en: https://www.ticbeat.com/tecnologias/cuantas-paginas-web-existen-en-el-mundo-en-la-actualidad/#:~:text=A%20fecha%20del%2019%20de,puedes%20consultar%20a%20tiempo%20real.

**[39]** Johnny Long, Bill Gardner, Justin Brown (2016) "Google Hacking for Penetration Testers Third Edition", Elsevier.

**[40]** Bing Help, Microsoft (2020) "Palabras clave de búsqueda avanzada", disponible en: https://help.bing.microsoft.com/#apex/18/es/10002/-1

**[41]** Bing Help, Microsoft (2020) “Opciones de búsqueda avanzada”, disponible en: https://help.bing.microsoft.com/#apex/bing/es/10001/-1

**[42]** John Matherly, Shodan LLC (2016) “Complete Guide to Shodan”, Leanpub, disponible en: https://leanpub.com/shodan

**[43]** Censys Inc., “Censys”, disponible en: https://censys.io/

**[44]** Scan.io, “Repositorio de datos de investigación en Internet de Stanford”, disponible en: https://scans.io/

**[45]** Weare Social, Hootsuite (2020) “Digital 2020 Global Digital Overview”, disponible en: https://wearesocial.com/blog/2020/01/digital-2020-3-8-billion-people-use-social-media

**[46]** LinkedIn, Mayo 4, 2021, disponible en: https://about.linkedin.com/es-es?lr=1

**[47]** Yubal Fernandez, Xataca (2020) “Búsquedas avanzadas en Twitter”, disponible en: https://www.xataka.com/basics/busquedas-avanzadas-twitter-comandos-operadores-para-exprimirlas-al-maximo

**[48]** Acunetix support, Web Vulnerabilities index, “WordPress 5.3.x Multiple Vulnerabilities (5.3 – 5.3.2)”, disponible en: https://www.acunetix.com/vulnerabilities/web/wordpress-5-3-x-multiple-vulnerabilities-5-3-5-3-2/

**[49]** Eset WeLiveSecurity, “Vulnerabilidad severa en plugin Contact Form 7 permite tomar control de sitios WordPress”, disponible en: https://www.welivesecurity.com/la-es/2020/12/18/vulnerabilidad-severa-contact-form-7-wordpress/

**[50]** BTrending Top Most, “Top 10 Automation Companies in the World”, disponible en: http://www.trendingtopmost.com/worlds-popular-list-top-10/2017-2018-2019-2020-2021/business/best-automation-companies-world-largest-revenue/

**[51]** Blog de Samurai Blanco, “Accediendo a SCADAs Vulnerables”, disponible en: https://www.samuraiblanco.org/accediendo-scadas-vulnerables-parte-i/

**[52]** CISA, Us-Cert, Alert (TA14-013A) (2016) “NTP Amplification Attacks Using CVE-2013-5211”, disponible en: https://us-cert.cisa.gov/ncas/alerts/TA14-013A

**[53]** NMAP.ORG, NSEDoc, Scripts, ntp-monlist, “File ntp-monlist”, disponible en: https://nmap.org/nsedoc/scripts/ntp-monlist.html

**[54]** Senki blog, Scaling this thing we call the "Internet" – Barry's Security & Resiliency Blog (2018), “Memcached on port 11211 UDP & TCP being exploited”, disponible en: https://www.senki.org/memcached-on-port-11211-udp-tcp-being-exploited/

**[55]** EcuCERT-ARCOTEL, Centro de Respuesta a Incidentes Informaticos, disponible en: https://www.ecucert.gob.ec/wp-content/uploads/2021/07/Ficha-Tecnica-open-ssdp.pdf

**[56]** EcuCERT-ARCOTEL, Centro de Respuesta a Incidentes Informaticos, disponible en: https://www.ecucert.gob.ec/wp-content/uploads/2021/07/Ficha-Tecnica-Accessible-RDP.pdf

**[57]** Eset WeLiveSecurity, “Por qué desconectar RDP de Internet para evitar ser víctima de un ataque”, disponible en: https://www.welivesecurity.com/la-es/2019/12/23/por-que-desconectar-rdp-internet-evitar-victima-ataque/

**[58]** EcuCERT-ARCOTEL, Centro de Respuesta a Incidentes Informaticos, disponible en: https://www.ecucert.gob.ec/wp-content/uploads/2021/07/Ficha-Tecnica-Accesible-SMB.pdf

**[59]** EcuCERT-ARCOTEL, Centro de Respuesta a Incidentes Informaticos, disponible en: https://www.ecucert.gob.ec/wp-content/uploads/2021/07/Ficha-Tecnica-Accessible-Telnet.pdf

**[60]** EcuCERT-ARCOTEL, Centro de Respuesta a Incidentes Informaticos, disponible en: https://www.ecucert.gob.ec/wp-content/uploads/2021/07/Ficha-Tecnia-Accesible-CWMP.pdf