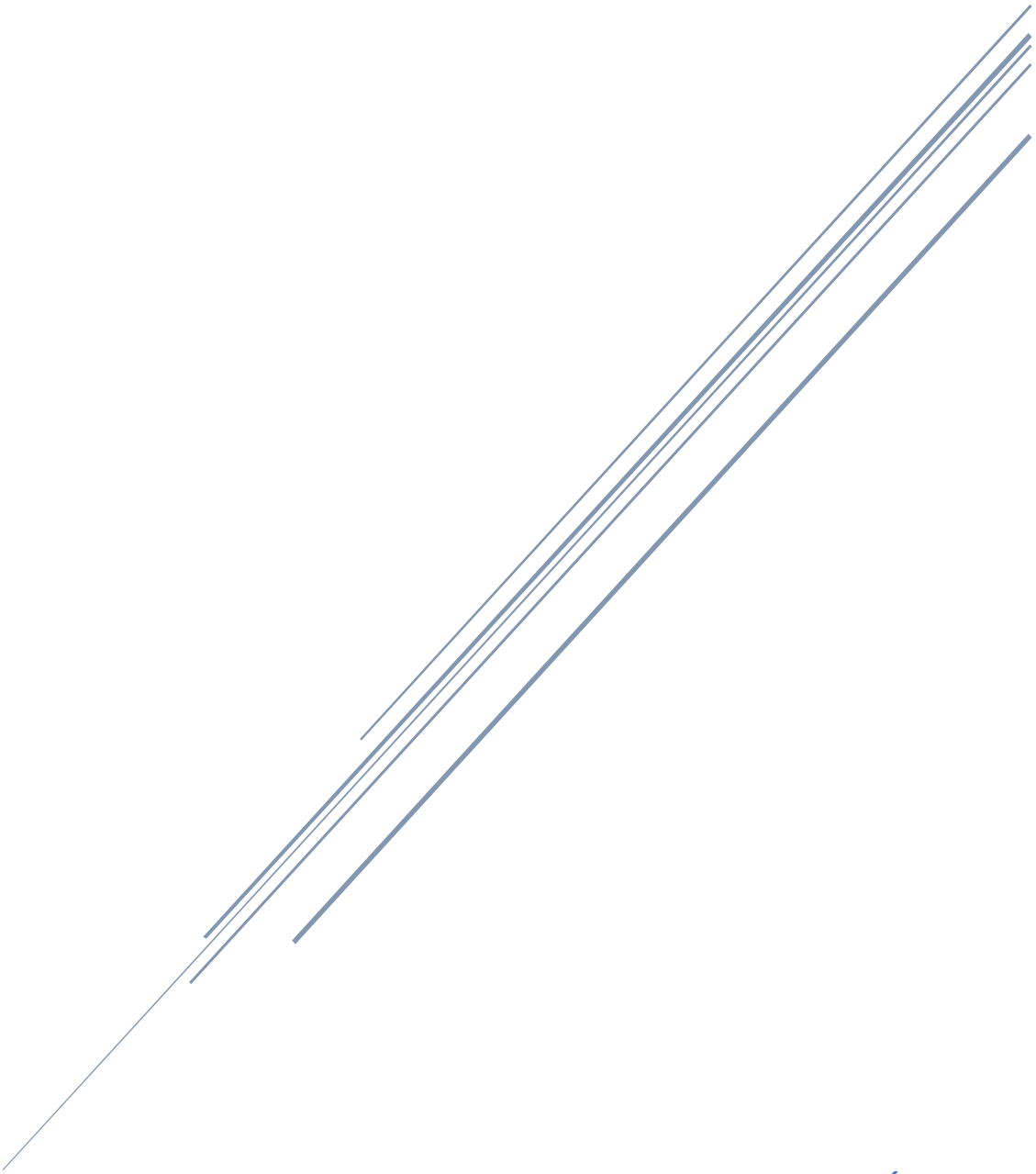
Detección de IP maliciosas

Técnicas de investigación



El Hacker Ético
elhackeretico.com

ÍNDICE

1

¿Cómo investigar direcciones IP sospechosas?

¿Qué es una dirección IP?

La dirección IP es una identificación asignada a cada dispositivo conectado a Internet. Está constituida por números y es única.

Asignar esta dirección a cada dispositivo con conexión a Internet tiene dos propósitos: la identificación y el direccionamiento. Con la ayuda de las direcciones IP, se peude identificar el Host y/o la red y ubicar la ubicación del dispositivo.

La Autoridad de Números Asignados de Internet (IANA) administra las direcciones IPa nivel mundial y tiene cinco Registros de Internet Regionales distintos que administran diferentes regiones del mundo.

¿Qué significa IP sospechosa?

Hay IP buenas y hay IP "sospechosas". Esto depende de varios factores, que son los siguientes:

- Envío de SPAM
- Estar asociada a dispositivos que envían Malware
- Estar relacionado con Adware

Es importante detectar estas direcciones IP y bloquearlas antes de que puedan provocar daños en nuestros equipos.

¿Qué es la reputación de una dirección IP?

Una IP con un historial de actividades y relaciones no maliciosas, que no se ha asociado nunca con un comportamiento malicioso, nunca ha sido secuestrada por actores maliciosos y solo, está relacionada con dominios, ubicaciones y comportamientos "buenos", entonces está IP tendrá una buena reputación.

Por el contrario, si se observa que está IP aloja malware, está conectada a sitios de Phishing o realizar cualquier tipo de actividad maliciosa, entonces es probable que esta

IP represente un peligro para los usuarios de Internet. Todo esto afecta negativamente a la reputación de una dirección IP.

¿Por qué es importante la reputación de la IP?

Una reputación positiva significa que el dispositivo que se corresponde con esa dirección es una ubicación de confianza para la información y las comunicaciones por Internet.

Por ejemplo, una empresa desea enviar correos a sus clientes, la reputación de su IP puede afectar en gran medida al envío de estos emails. Si su sitio web es secuestrado o sus servidores se utilizan para enviar malware, la reputación de la IP se verá afectada hasta el punto de que sus correos no se considerarán de confianza, por los que estos se enviarán a la carpeta de correo no deseado.

¿Cómo se determina la reputación de una IP?

Hay una gran variedad de factores a considerar. Estos son algunos de los parámetros que se pueden utilizar para medir la reputación de la IP:

- Categoría de IP
- Antigüedad de la IP
- Historial de la IP
- Reputación del dominio
- Reputación de la URL asociada
- Presencia de archivos descargables o código
- Asociación con objetos maliciosos de Internet
- Ubicación del alojamiento
- Propietario del sitio web y/o la red
- Presencia en listas de permitidos o bloqueados

El análisis de esto genera una evaluación muy precisa del nivel de riesgo asociado con una dirección IP determinada.

Herramientas para realizar la evaluación.

En línea tenemos una serie de herramientas para realizar nuestras investigaciones. Algunas de las herramientas disponibles son las siguientes:

- AbuseIPDB: proporciona datos de reputación sobre la dirección IP o el nombre de host.
- BrightCloud URL/IP Lookup: presenta datos históricos de reputación sobre el sitio web.
- Email Blocklist Checker: verifica el nombre de dominio o la dirección IP en las listas de bloqueo de correo electrónico (se requiere dirección de correo electrónico, opta por marketing).
- IBM X-Force Exchange: proporciona datos históricos sobre IP, URL, etc.
- Hashdd: proporciona datos históricos sobre IP, URL, etc.
- IPQualityScore: presenta una clasificación de riesgo para la dirección IP
- PhishTank: busca la URL en su base de datos de sitios web de phishing conocidos
- PolySwarm: utiliza varios servicios para examinar el sitio web o buscar la URL
- Open Threat Exchange: presenta diversos datos de inteligencia de amenazas de AlienVault
- PassiveTotal: presenta DNS pasivo y otros datos de inteligencia de amenazas
- SecurityTrails: proporciona datos de dominio o sistema actuales e históricos
- Talos Reputation Lookup: presenta datos históricos de reputación sobre el sitio web
- Unmask Parasites: busca la URL en la base de datos de navegación segura de Google
- urlscan.io: examina la URL en tiempo real y muestra las solicitudes que emite para representar la página
- URLVoid e IPVoid: busca la URL o IP en varios servicios de listas negras
- VirusTotal: busca la URL en varias bases de datos de sitios maliciosos

4