Guía de ciberataques

ATAQUES A LAS CONEXIONES # 2

Todo lo que debes saber a nivel usuario

Instituto Nacional de Cancerología-ESE
Colombia
Por el control del cáncer

OBJETIVOS DE LOS CIBERATAQUES Y SUS CONSECUENCIAS PARA EL USUARIO

Los ciberdelincuentes se encuentran siempre al acecho de nuevas formas con las que atacarnos a los usuarios **aprovechándose de nuestro desconocimiento o vulnerabilidades en nuestras defensas.**
Sus objetivos son muchos **y pueden tener** *distintas consecuencias para el usuario.*

3

Ataques a las conexiones

Los ataques a las conexiones inalámbricas *son muy comunes, y los ciberdelincuentes se sirven de diversos software y herramientas con las que saltarse las medidas de seguridad* **e infectar o tomar control de nuestros dispositivos.**

Generalmente, este tipo de ataques se basan en interponerse en el *intercambio de información entre nosotros y el servicio web, para monitorizar y robar* **datos personales, bancarios, contraseñas, etc.**

TIPOS DE CIBERATAQUES

3 Ataques a las conexiones

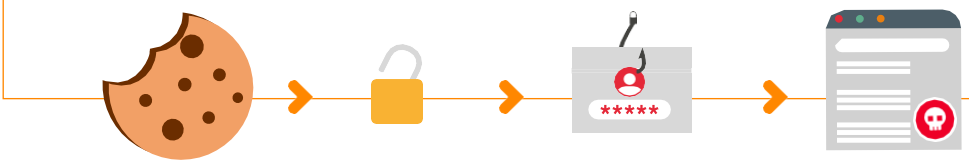
Ataques a Cookies

¿Cómo funciona?

Las *cookies* ***se envían entre el servidor de la web y nuestro equipo*****, sin embargo, en páginas con protocolos** *http*, **este intercambio puede llegar a ser visible para los ciberdelincuentes.**

Los ataques a las *cookies* ***consisten en el robo o modificación de la información almacenada en una cookie.***

Las *cookies* ***son pequeños ficheros que contienen información de las páginas webs que hemos visitado*****, así como otros datos de navegación, como pueden ser los anuncios vistos, el idioma, la zona horaria, si hemos proporcionado una dirección de correo electrónico, etc.** ***Su función es ayudarnos a navegar de forma más rápida, recordando esta información para no tener que volver a procesarla.***



¿Cómo se propaga/infecta/extiende?

Los atacantes se sirven de diferentes técnicas y *malware*, **así como de la falta de protocolos de cifrado que protejan la información intercambiada entre nosotros y el servidor web (***http***).**

¿Cuál es su objetivo?

Debido a la información almacenada en las *cookies*, **este tipo de ataques tienen como objetivo:**

- **El robo de identidad y credenciales.**
- **Obtener información personal sin nuestra autorización.**
- **Modificar datos.**

TIPOS DE CIBERATAQUES

3 Ataques a las conexiones

¿Cómo me protejo?

Además de una correcta configuración de las *cookies* desde nuestro navegador favorito, es recomendable seguir estas pautas:

- ***Mantener actualizado el navegador*, así como los complementos o plugins instalados. Verifica siempre que las páginas web tengan el candado y la palabra HTTPS**
- ***Eliminar cada cierto tiempo los datos de navegación*, como las *cookies*, el historial y el caché.**
- ***Revisar detenidamente las notificaciones o mensajes* que aparezcan al acceder a una web *antes de aceptarlos*.**
- ***A la hora de intercambiar información sensible o datos confidenciales* o muy personales, es mejor *utilizar el modo incógnito del navegador* .**
- ***No guardar las contraseñas dentro del navegador* y utilizar gestores de contraseñas en su lugar.**

Dentro de los ataques a las *cookies*, existen dos tipos con sus particularidades:

- ***Robo de cookies:* Aprovechando la falta de seguridad en los protocolos *http*, los atacantes son capaces de recibir una *cookie* perteneciente a un intercambio entre nosotros y el servidor. Con ello, el atacante puede llegar a identificarse como la víctima en la web o acceder a datos sensibles.**
- ***Envenenamiento de cookies:* Sirviéndose de la misma vulnerabilidad, el atacante puede llegar a modificar el valor recogido en la *cookie*. Por ejemplo, para modificar el precio que hemos pagado por un artículo en una tienda online.**

Por qué borrar las cookies del navegador

Entre cookies y privacidad

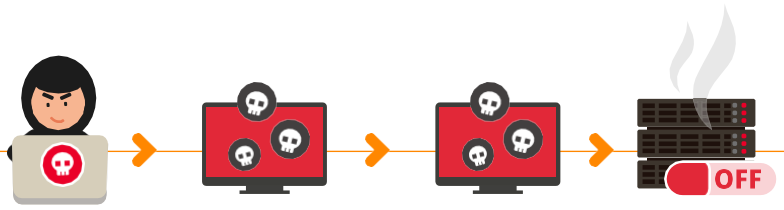
TIPOS DE CIBERATAQUES

3 Ataques a las conexiones

Ataque DDoS

¿Cómo funciona?

DDoS son las siglas en inglés de "Ataque distribuido denegación de servicio" y *consiste en atacar un servidor web al mismo tiempo desde muchos equipos diferentes para que deje de funcionar* **al no poder soportar tantas peticiones.**



¿Cómo se propaga/infecta/extiende?

El ataque como tal no se propaga, sino que el ciberdelincuente o los ciberdelincuentes lanzan un ataque desde diversos dispositivos infectados. De hecho, la propagación se lleva a cabo a partir de otro tipo de ataques con los que infectar dispositivos e ir aumentando la potencia del ataque.

¿Cuál es su objetivo?

Su objetivo es provocar la caída de la web. Dependiendo del servicio y del tiempo que permanezca caído, las consecuencias pueden ser mayores.

Los afectados por un ataque DDOS son principalmente los servicios web, es decir, los objetivos de los atacantes. Las consecuencias son una pérdida de reputación, suspensión del servicio, así como pérdidas económicas, además de las consecuencias de una brecha en su seguridad, como el robo de datos.

Para nosotros, los usuarios, las principales consecuencias son el no poder acceder a dicho servicio al estar caído debido al ataque. Sin embargo, también podemos ser cómplices del ataque sin saberlo, si nuestros equipos han sido infectados para formarte parte de una *Botnet*, **por ejemplo.**

TIPOS DE CIBERATAQUES

3 Ataques a las conexiones

Redes trampa | Spoofing | Ataques a Cookies | **Ataques DDoS** | Inyección SQL | Escaneo de puertos | Man in the middle | Sniffing

¿Cómo me protejo?

Como usuarios, si tenemos un servicio web, existen distintas técnicas de protección contra este tipo de ataque:

- *Monitorización continua:* **Existen herramientas para analizar la actividad del sitio web y detectar posibles ataques DDOS antes de que se conviertan en un problema. El** *firewall* **puede ayudarnos a detectar posibles intrusos o una actividad fuera de lo normal.**
- *Proveedor fiable:* **Elegir un proveedor que nos ofrezca garantías, como un servicio de prevención o una infraestructura sólida para aguantar un intento de ataque tipo DDOS.**
- *Actualizaciones:* **Las actualizaciones de seguridad nos protegerán de posibles vulnerabilidades en el** *software*.
- *Conexión sólida:* **Un buen ancho de banda nos ayudará a reducir los efectos de un ataque DDOS y a reponernos antes.**
- *Reducir la superficie afectada:* **Una solución muy útil es limitar la infraestructura de nuestro servicio web que pueda ser atacada, por ejemplo, no publicar servicios directamente a internet, ni exponer a internet servidores de bases de datos.**

¿Qué son los ataques DoS y DDoS?

Qué es una botnet o una red zombi de ordenadores

TIPOS DE CIBERATAQUES

3 Ataques a las conexiones

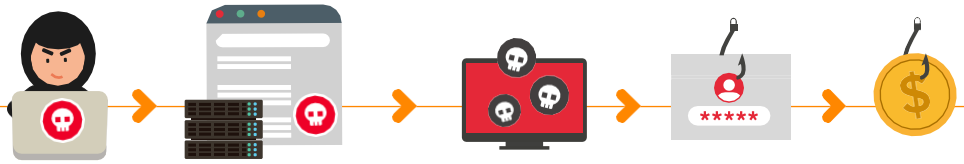
Redes trampa | Spoofing | Ataques a Cookies | Ataques DDoS | **Inyección SQL** | Escaneo de puertos | Man in the middle | Sniffing

Inyección SQL

¿Cómo funciona?

Las páginas webs suelen estar vinculadas a bases de datos, basadas en un lenguaje de programación conocido como SQL. **Este tipo de ataque permite a los ciberdelincuentes insertar líneas de código SQL maliciosas en la propia aplicación web, obteniendo acceso parcial o completo a los datos, pudiendo ser monitorizados, modificados o robados por el atacante.**

SQL es un lenguaje de programación utilizado para interactuar con bases de datos. Los ciberdelincuentes *atacan a una aplicación web basada en este tipo de lenguaje, comprometiendo la base de datos mediante líneas de código malicioso.*



¿Cómo se propaga/infecta/extiende?

Los atacantes inyectan líneas de código SQL malicioso en la base de datos de las aplicaciones web. Para ello, se sirven de cualquier canal de entrada para enviar comandos maliciosos, como elementos *input*, **cadenas de consulta,** *cookies* **y archivos.**

¿Cuál es su objetivo?

El objetivo del atacante es tener acceso a los datos sensibles recogidos en la base de dato del servicio o aplicación web para robarlos o para destruirlos.

¿Cómo me protejo?

Como usuarios, *no podemos hacer mucho para prevenir este tipo de ataques, pues depende de la seguridad implantada por el servicio web.*

En el caso de los desarrolladores web, es fundamental que sigan las recomendaciones basadas en el diseño seguro y en el desarrollo de código seguro, que priorice la privacidad de las comunicaciones y la protección de nuestros datos.

Entre cookies y privacidad

Botnet: Asprox

TIPOS DE CIBERATAQUES

3 Ataques a las conexiones

Redes trampa | Spoofing | Ataques a Cookies | Ataques DDoS | **Inyección SQL** | Escaneo de puertos | Man in the middle | Sniffing

Escaneo de puertos

¿Cómo funciona?

El ataque de escaneo de puertos, o *portscan*, *es el proceso en el que se analiza* **automáticamente los puertos lógicos** *de una máquina conectada a la red* **con la finalidad de analizar los puertos** e *identificar cuáles están abiertos, cerrados o cuentan con algún protocolo de seguridad.*

¿Cómo se propaga/infecta/extiende?

Los ciberdelincuentes se sirven de varios programas con los que escanear los puertos usados por un firewall empresarial o un router de hogar .

¿Cuál es su objetivo?

En este tipo de ataques, el objetivo suele ser el robo de nuestra información, como credenciales o datos bancarios, pero también ofrecen una entrada para controlar dispositivos conectados a una red.

¿Cómo me protejo?

Como medida de protección, *el firewall empresarial o Router en casa tienen el papel protagonista a la hora de proteger los sistemas de la mayoría de los ataques a las conexiones.*

Es fundamental configurarlo correctamente, *controlar las conexiones* **entrantes y los dispositivos conectados por medio de un filtrado MAC, mantener el** *firewall* **activado y controlar los puertos que tenemos abiertos. Y, como cualquier dispositivo, mantenerlo actualizado para protegerlo de posibles brechas de seguridad.**

Tu router, tu castillo. Medidas básicas para su protección

Te refrescamos cómo proteger la red wifi de casa

TIPOS DE CIBERATAQUES

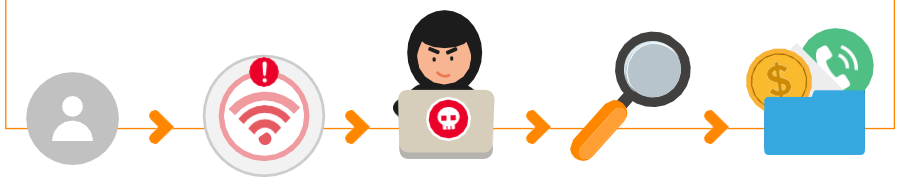
3 *Ataques a las conexiones*

*Redes trampa | Spoofing | Ataques a Cookies | Ataques DDoS | **Inyección SQL** | Escaneo de puertos | Man in the middle | Sniffing*

Man in the middle

¿Cómo funciona?

Este tipo de ataque requiere que *el atacante se sitúe entre nosotros y el servidor con el que nos estamos comunicando.*



¿Cómo se propaga/infecta/extiende?

Suelen ser habituales en redes públicas o en redes wifi falsas localizadas en sitios públicos, como centros comerciales, aeropuertos u hoteles. El atacante consigue monitorizar la actividad online dentro de la red infectada.

¿Cuál es su objetivo?

Su objetivo es interceptar, leer o manipular los datos intercambiados, como mensajes, credenciales, transferencias económicas, etc. Generalmente, el atacante monitorea nuestra actividad online y registra la información que más le interese.

¿Cómo me protejo?

La primera norma es no conectarse a redes públicas. **Además,** *es recomendable mantener nuestros dispositivos y software instalado actualizado a su última versión,* **utilizar aplicaciones de cifrado, disponer de contraseñas robustas y, si es posible, añadir una capa extra de seguridad con la verificación en dos pasos. Finalmente, aplicar buenas prácticas de navegación segura, como acceder solo a webs con certificado digital** *https* **y conectarse a redes wifi por medio de la VPN institucional si es necesaria la conexión a Internet.**

Man in the middle. Toda tu actividad al descubierto

TIPOS DE CIBERATAQUES

3 *Ataques a las conexiones*

*Redes trampa | Spoofing | Ataques a Cookies | Ataques DDoS | **Inyección SQL** | Escaneo de puertos | Man in the middle | Sniffing*

Sniffing

¿Cómo funciona?

Se trata de una *técnica utilizada para escuchar todo lo que ocurre dentro de una red*. **Los atacantes utilizan herramientas de** *hacking*, **conocidas como** *sniffers*, **de forma malintencionada para monitorizar el tráfico de una red.**

¿Cómo se propaga/infecta/extiende?

Los *sniffers* **no son virus y, por ello, no pueden reproducirse por sí mismos y deben ser controlados por terceras personas. Pueden ser instalados como cualquier otro programa con o sin nuestro consentimiento.**

¿Cuál es su objetivo?

Mediante el uso de diferentes herramientas, los atacantes buscan capturar, interpretar y robar paquetes de datos lanzados por la red, para analizarlos y hacerse con nuestros datos.

¿Cómo me protejo?

***Las herramientas de protección de Antivirus y antimalware pueden detectar y eliminar los sniffers instalados en un equipo*. Sin embargo, dado que no son considerados como** *malware*, **no siempre son detectados y deben ser eliminados de forma manual.**

Para evitarlo, se deben seguir todas las pautas para prevenir la descarga de *software* **malicioso cuando navegamos por la red, como no descargar adjuntos sospechosos, no navegar por webs fraudulentas, así como evitar conectar dispositivos USB, y solicitar apoyo a a la mesa de ayuda para realizar cualquier instalación en el equipo.**

Compartir Wif i ¿Si o No?

WhatsApp ya cifra las comunicaciones

Fuente:

INCIBE - https://www.incibe.es

Instituto Nacional de Ciberseguridad (INCIBE), publicación de INCIBE bajo una licencia Reconocimiento Internacional de Creative Commons 4.0-No comercial-CompartirIgual. Texto completo de la licencia: https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es_ES

OSI - Servicio de la Oficina de Seguridad del Internauta (OSI) - https://www.osi.es.