Guía de ciberataques

ATAQUES A LAS CONEXIONES #1

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*

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

Redes trampa

¿Cómo funciona?

La creación de redes wifi falsas es una práctica muy utilizada por los ciberdelincuentes. ***Consiste en la creación de una red wifi gemela a otra legítima y segura*****, con un** ***nombre igual o muy similar a la original*****, que crean utilizando** *software* **y** *hardware*. **Luego, la configuran con los mismos parámetros que la original, esperando que nos conectemos a esta.**

¿Cómo se propaga/infecta/extiende?

Este tipo de ataques suelen darse en lugares con una red wifi pública, con gran afluencia de usuarios. De modo que su red falsa pueda pasar desapercibida y engañe al mayor número de víctimas posible.

¿Cuál es su objetivo?

El objetivo es conseguir robar nuestros datos cuando accedamos a nuestra cuenta bancaria, redes sociales o correo electrónico, pensando que estamos llevando a cabo una conexión segura. Además, el ciberdelincuente puede llegar a tomar control sobre nuestra navegación, accediendo a determinadas webs fraudulentas o muy similares a la original preparadas para el engaño o para la infección por *malware*.

¿Cómo me protejo?

La mejor forma de prevenir este ataque es aprendiendo a identificar las redes wifi falsas:

- ***El primer indicativo es que existan dos redes con nombres iguales o muy similares*****. O, por ejemplo, que añadan la palabra "gratis".**
- ***Si las webs a las que accedes tras conectarte solo utilizan el protocolo http*****, detén tu actividad y desconéctate.**
- ***Es probable que estas redes estén abiertas*** **o que permitan introducir cualquier contraseña.** *Otra medida preventiva es desconectar la función del dispositivo móvil para conectarse automáticamente a redes abiertas.* **Finalmente, como protección, no es recomendable utilizar este tipo de redes cuando vamos a intercambiar información sensible, como nuestros datos bancarios. En caso de necesidad, podemos recurrir a la VPN institucional .**

Te explicamos qué es una VPN y para qué se usa

¡Conexión gratis a la vista! ¿Conecto mi móvil?

TIPOS DE CIBERATAQUES

3 Ataques a las conexiones

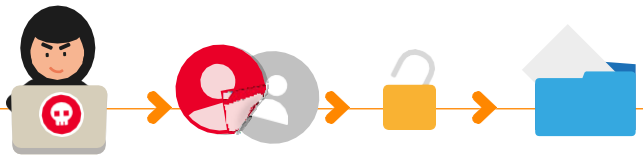
Spoofing

¿Cómo funciona?

Consiste en el *empleo de técnicas de hacking de forma maliciosa para suplantar nuestra identidad*, **la de una web o una entidad. Se basa en tres partes: el atacante, la víctima y el sistema o entidad virtual que va a ser falsificado.**

El objetivo **de los atacantes es, mediante esta suplantación,** *disponer de un acceso a nuestros datos*. **Según el tipo de** *Spoofing*, **la suplantación y el engaño se llevarán a cabo de forma distinta.**

Como protección, **es fundamental que nos mantengamos alerta y sigamos las recomendaciones para** *una navegación segura*.



TIPOS DE CIBERATAQUES

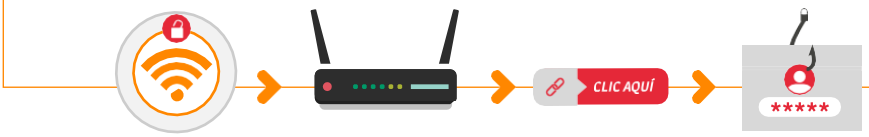
3 Ataques a las conexiones

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

IP Spoofing

¿Cómo funciona?

El ciberdelincuente *consigue falsear su dirección IP y hacerla pasar por una dirección de red distinta*. **De este modo, consigue saltarse las restricciones de los controles de seguridad de red, y por ejemplo, hacernos llegar un paquete con** *malware*.



¿Cómo se propaga/infecta/extiende?

La falsificación de la dirección IP del atacante se consigue mediante *software* **especial desarrollado a propósito para esta función.**

¿Cuál es su objetivo?

Uno de los objetivos de este tipo de ataque es obtener acceso a redes que sirven para autenticar a los usuarios o que aplican permisos en función de la dirección IP de origen para saltarse restricciones y robar credenciales.
Suele utilizarse para preparar ataques de mayor complejidad por lo que, si consigue infectarnos, podría tomar control de nuestros dispositivos para llevar a cabo un ataque de denegación de servicio.

¿Cómo me protejo?

En casa es recomendable *llevar a cabo un filtrado de las direcciones IP para controlar las conexiones entrantes*. **Para ello, es necesario acceder a la configuración del router, ir al apartado Seguridad y acceder al** *Firewall*. **Desde aquí, es posible filtrar las direcciones IP aplicando normas y reglas de filtrado a los paquetes que entren al router. Dentro del Instituto, se cuentan con controles de acceso a la red (NAC) y de firewall que detectan y evitan este tipo de ataques.**

Tu router, tu castillo. Medidas básicas para su protección

Spoofing o el robo de identidades, ¡qué no te engañen!

TIPOS DE CIBERATAQUES

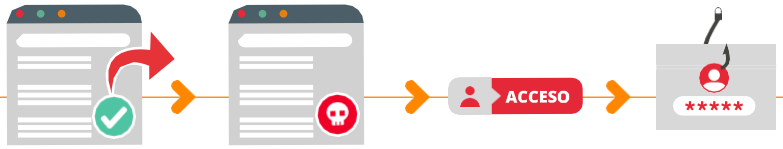
3 Ataques a las conexiones

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

Web Spoofing

¿Cómo funciona?

Consiste en la *suplantación de una página web real por otra falsa*. La web falsa es una copia del diseño de la original, llegando incluso a utilizar una URL muy similar. El atacante trata de hacernos creer que la web falsa es la original.



¿Cómo se propaga/infecta/extiende?

El atacante se sirve de otro tipo de ataques, como la ingeniería social o anuncios maliciosos, para intentar que accedamos al enlace de la web falsa pensando que se trata de la página web legítima.

¿Cuál es su objetivo?

El objetivo de falsificar una web no es otro que el de robar las credenciales o los datos que intercambiemos con dicho servicio. Generalmente, se utilizan para hacerse con nuestras credenciales al tratar de ingresarlos en la web falsa.

¿Cómo me protejo?

Al ser un *ataque que suele llegar en forma de enlace se debe revisar con mucho cuidado la URL para identificar diferencias con la original*. También habrá que desconfiar de las webs sin certificados digitales "https" y, en caso de tenerlo, comprobar que se trata de la web que dice ser.

Spoofing o el robo de identidades, ¡qué no te engañen!

¿Qué pasa si una página web no utiliza https?

Tiendas online fraudulentas

TIPOS DE CIBERATAQUES

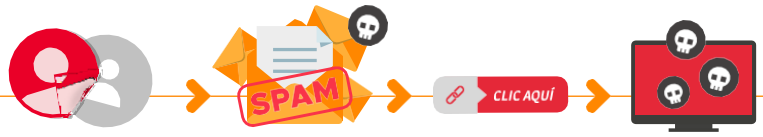
3 Ataques a las conexiones

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

Email Spoofing

¿Cómo funciona?

Consiste en *suplantar la dirección de correo de una persona o entidad de confianza*. **También suele ser usado para enviar de forma masiva correos de Spam o cadenas de estafas u otros fraudes.**



¿Cómo se propaga/infecta/extiende?

El atacante ha podido obtener el *Email* **suplantado a partir de otro tipo de ataques, como la ingeniería social. Además, es muy utilizado en otro tipo de ataques, como el** *phishing* **o el** *spam*, **para aumentar sus probabilidades de éxito.**

¿Cuál es su objetivo?

Su objetivo principal es conseguir información personal sirviéndose de la confianza que transmita la identidad suplantada o también engañarnos para conseguir que descarguemos *malware* **en nuestro equipo.**

¿Cómo me protejo?

Una suplantación de mail por una cuenta comprometida es difícil de detectar. Identifique solicitudes de información sospechosas, comportamientos o temas inusuales en el contenido del mail. *Reporte a mesa de ayuda de manera inmediata si fue víctima o sospecha de compromiso de su cuenta o de alguno de sus compañeros de trabajo.*

Spoofing o el robo de identidades, ¡qué no te engañen!

Cómo identificar un correo electrónico malicioso

TIPOS DE CIBERATAQUES

3 Ataques a las conexiones

DNS Spoofing

¿Cómo funciona?

A través de programas maliciosos específicos y aprovechándose de vulnerabilidades en las medidas de protección, los atacantes consiguen infectar y acceder a nuestro navegador web. **Así, cuando tratemos de acceder a una determinada web desde el navegador, este nos llevará a otra web elegida por el atacante. Para ello, los atacantes tienen que suplantar el nombre DNS (*Domain Name System*), es decir, la tecnología utilizada para nombrar los dominios y subdominios a los que queremos acceder.**

Aunque intentemos acceder a la URL correcta, el navegador nos redireccionará a la web fraudulenta, ya que el atacante habría modificado los DNS.

¿Cómo se propaga/infecta/extiende?

Sirviéndose de ataques de phishing , así como de *malware* especializado, el atacante consigue acceder al navegador web, o Router en el hogar para modificar los DNS.

¿Cuál es su objetivo?

El objetivo del atacante es modificar los DNS para redirigirnos cada vez que intentemos acceder a una página web, a una web fraudulenta preparada por el atacante.

¿Cómo me protejo?

***La mejor forma de prevenir* este ataque *es evitara abrir correos y sitios* web de dudosa reputación, restringir las conexiones remotas, usar contraseñas fuertes y cambiar las contraseñas por defecto, además de seguir las pautas para identificar webs fraudulentas.**

Spoofing o el robo de identidades, ¡qué no te engañen!

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.