Guía de ciberataques



Todo lo que debes saber a nivel usuario

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017
OSI Oficina de Seguridad del Internauta

Índice

Objetivos de los ciberataques y sus consecuencias para el usuario 03

Tipos de ciberataques

1 Ataques a contraseñas 04
1.1. Fuerza bruta 05
1.2. Ataque por diccionario 06

2 Ataques por ingeniería social 07
2.1. Phishing, Vishing y Smishing 08
2.2. Baiting o Gancho 10
2.3. Shoulder surfing o mirando por encima del hombro 11
2.4. Dumpster Diving o rebuscando en la basura 12
2.5. Spam o correo no deseado 13
2.6. Fraudes online 14

3 Ataques a las conexiones 15
3.1 Redes trampa (Wifi falsas) 16
3.2. Spoofing o suplantación 17
3.2.1 IP Spoofing 18
3.2.2 Web Spoofing 19
3.2.3 Email Spoofing 20
3.2.4 DNS Spoofing 21
3.3. Ataques a Cookies 22
3.4. Ataques DDoS 24
3.5. Inyección SQL 26
3.6. Escaneo de puertos 27
3.7. Man in the middle o ataque de intermediario 28
3.8. Sniffing 29

4 Ataques por malware 30
4.1. Virus 31
4.2. Adware o anuncios maliciosos 32
4.3. Spyware o software espía 33
4.4. Troyanos 34
4.4.1. Backdoors 35
4.4.2. Keyloggers 36
4.4.3. Stealers 37
4.4.4. Ransomware 38
4.5. Gusano 39
4.6. Rootkit 40
4.7. Botnets o redes zombi 41
4.9. Rogueware o el falso antivirus 42
4.10. Criptojacking 43
4.11. Apps maliciosas 44

Medidas de protección 45

Licencia de contenidos:
"La presente publicación pertenece al Instituto Nacional de Ciberseguridad (INCIBE) y está bajo una licencia Reconocimiento-No comercial-CompartirIgual 4.0 Internacional de Creative Commons. Por esta razón está permitido copiar, distribuir y comunicar públicamente esta obra bajo las condiciones siguientes:
• Reconocimiento. El contenido de esta publicación se puede reproducir total o parcialmente por terceros, citando su procedencia y haciendo referencia expresa a INCIBE y al servicio de la Oficina de Seguridad del Internauta (OSI) y sus sitios web: https://www.incibe.es y https://www.osi.es. Dicho reconocimiento no podrá en ningún caso sugerir que INCIBE presta apoyo a dicho tercero o apoya el uso que hace de su obra.
• Uso No Comercial. El material original y los trabajos derivados pueden ser distribuidos, copiados y exhibidos mientras su uso no tenga fines comerciales.
• Compartir Igual. Si altera o transforma esta obra, o genera una obra derivada, sólo puede distribuirla bajo esta misma licencia.
Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones pueden no aplicarse si se obtiene el permiso de INCIBE como titular de los derechos de autor.
Texto completo de la licencia: https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es_ES

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.***



1

Ataques a contraseñas

Los ciberdelincuentes se sirven de ***diversas técnicas y herramientas con las que atacar a nuestras credenciales***. Los usuarios no siempre les dificultamos esta tarea, y solemos caer en malas prácticas que ponen en peligro nuestra seguridad:

- Utilizar ***la misma contraseña para distintos servicios***.
- Utilizar ***contraseñas débiles, fáciles de recordar*** y de atacar
- Utilizar ***información personal a modo de contraseñas***, como la fecha de nacimiento.
- ***Apuntarlas en notas*** o archivos sin cifrar.
- ***Guardar las contraseñas*** en webs o ***en el navegador.***
- Y, finalmente, ***hacer uso de patrones sencillos***, como utilizar la primera letra en mayúscula, seguida de 4 o 5 en minúscula y añadir 1 o 2 números o un carácter especial. Estos patrones acaban por popularizarse, facilitando aún más la tarea a los ciberdelincuentes.



TIPOS DE CIBERATAQUES

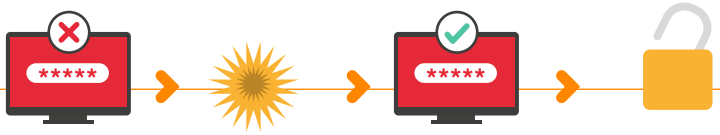
1 Ataques a contraseñas

Fuerza bruta | *Ataque por diccionario*

Fuerza bruta

¿Cómo funciona?

Consiste en adivinar nuestra contraseña a base de ensayo y error. Los atacantes comienzan probando diferentes combinaciones con nuestros datos personales, en caso de conocerlos por otras vías. Luego, continúan haciendo combinaciones de palabras al azar, conjugando nombres, letras y números, hasta que dan con el patrón correcto.



¿Cuál es su objetivo?

El objetivo de los ciberdelincuentes siempre será conseguir la información almacenada en nuestras cuentas.
Dependiendo de si se trata de un correo electrónico, con el que obtener datos personales y contactos; una red social, con la que poder suplantar nuestra identidad; o datos bancarios, con los que llevar a cabo transferencias a su cuenta o realizar compras sin nuestro consentimiento, el atacante hará uso de esta información para su propio beneficio.

¿Cómo me protejo?

Como protección, ***es fundamental evitar caer en los errores anteriores y mejorar la seguridad de las cuentas utilizando contraseñas robustas***. Además, ***es conveniente aplicar el factor de autenticación múltiple***, siempre que el servicio lo permita, y utilizar gestores de contraseñas

Aprende a gestionar tus contraseñas

El factor de autenticación doble y múltiple

Una contraseña fácil, ¿pero cuántas cuentas comprometidas?

TIPOS DE CIBERATAQUES

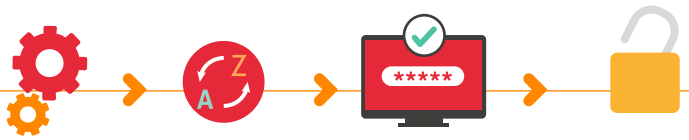
1 Ataques a contraseñas

Fuerza bruta | ***Ataque por diccionario***

Ataque por diccionario

¿Cómo funciona?

Los ciberdelincuentes ***utilizan un software que, de forma automática, trata de averiguar nuestra contraseña***. Para ello, realiza diferentes comprobaciones, empezando con letras simples como "a", "AA" o "AAA" y, progresivamente, va cambiando a palabras más complejas.



¿Cuál es su objetivo?

El objetivo de los ciberdelincuentes siempre será conseguir con la información almacenada en nuestras cuentas. Dependiendo de si se trata de un correo electrónico, con el que obtener datos personales y contactos, una red social, con la que poder suplantar nuestra identidad, o datos bancarios con los que llevar a cabo transferencias a su cuenta o realizar compras sin nuestro consentimiento, el atacante hará uso de esta información para su propio beneficio.

¿Cómo me protejo?

Como protección, ***es fundamental evitar caer en los errores anteriores y mejorar la seguridad de las cuentas utilizando contraseñas robustas***. Además, es conveniente aplicar el factor de autenticación múltiple, siempre que el servicio lo permita, y utilizar gestores de contraseñas.

Una contraseña fácil, ¿pero cuántas cuentas comprometidas?

El factor de autenticación doble y múltiple

2

Ataques por ingeniería social

Los ataques por ingeniería social ***se basan en un conjunto de técnicas dirigidas a nosotros, los usuarios, con el objetivo de conseguir que revelemos información personal o permita al atacante tomar control de nuestros dispositivos***. Existen distintos tipos de ataques ***basados en el engaño y la manipulación,*** aunque sus consecuencias pueden variar mucho, ya que suelen utilizarse como paso previo a un ataque por *malware*.



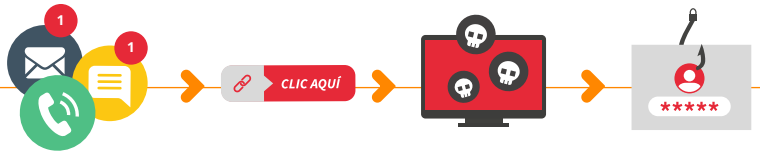
TIPOS DE CIBERATAQUES

2 Ataques por ingeniería social

Phishing, Vishing y Smishing

¿Cómo funciona?

Se tratan de tres ***ataques basados en ingeniería social muy similares en su ejecución***. De forma general, el ciberdelincuente ***enviará un mensaje suplantando a una entidad legítima***, como puede ser un banco, una red social, un servicio técnico o una entidad pública, con la que nos sintamos confiados, ***para lograr su objetivo***. Estos mensajes suelen ser de carácter urgente o atractivo, para evitar que apliquen el sentido común y se lo piensen dos veces.



Phishing

Suele emplearse el correo electrónico, redes sociales o aplicaciones de mensajería instantánea.

Vishing

Se lleva a cabo mediante llamadas de teléfono.

Smishing

El canal utilizado son los SMS.

En ocasiones, traen consigo un enlace a una web fraudulenta, que ha podido ser suplantada, fingiendo ser un enlace legítimo, o bien se trata de un ***archivo adjunto malicioso para infectarnos con malware.***

Cuando se trata de un ataque dirigido a una persona en concreto, se conoce como Spear phishing. Esta modalidad centra en una persona específica las técnicas de manipulación, recabando información sobre ella previamente para maximizar las probabilidades de éxito a la hora de hacerse con su información o dinero

TIPOS DE CIBERATAQUES

2 Ataques por ingeniería social

Phishing, Vishing y Smishing | *Baiting o Gancho* | *Shoulder surfing* | *Dumpster Diving* | *Spam* | *Fraudes online*

¿Cómo se propaga/infecta/extiende?

El principal medio de propagación es el correo electrónico donde, fingiendo ser una entidad de confianza, el atacante lanza un cebo. Generalmente suele ser un mensaje urgente o una promoción muy atractiva, para motivarnos a hacer clic en el enlace o archivo adjunto, o a compartir los datos que el atacante pide en su mensaje.

¿Cuál es su objetivo?

Su objetivo es obtener datos personales y/o bancarios de los usuarios, haciéndonos creer que los estamos compartido con alguien de confianza. También pueden utilizar esta técnica para que descarguemos *malware* con el que infectar y/o tomar control del dispositivo.

¿Cómo me protejo?

El principal consejo es ser precavido y leer el mensaje detenidamente, especialmente si se trata de entidades con peticiones urgentes, promociones o chollos demasiado atractivos.

Además, otras pautas que podemos seguir para evitar ser víctima de un *phishing* son:

- ***Detectar errores gramaticales en el mensaje***. Y, si se trata de un asunto urgente o acerca de una promoción muy atractiva, es muy probable que se trate de un fraude.
- ***Revisar que el enlace coincide con la dirección a la que apunta***. Y, en cualquier caso, debemos ingresar la url nosotros directamente en el navegador, sin copiar y pegar.
- ***Comprobar el remitente del mensaje***, o asegurarnos de que se trata de un teléfono legítimo.
- ***No descargar ningún archivo adjunto y analizarlo previamente con el antivirus***. En caso de *vishing*, no debemos descargar ningún archivo que nos haya solicitado el atacante, ni ceder el control de nuestro equipo por medio de algún *software* de control remoto.
- ***No contestar nunca al mensaje*** y eliminarlo.

Conoce a fondo qué es el phishing

SMISHING suplantando al BBVA para estafar a usuarios

¿Sabías que el 95% de las incidencias en ciberseguridad se deben a errores humanos?

TIPOS DE CIBERATAQUES

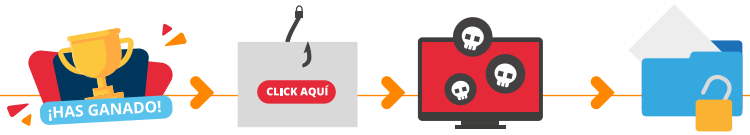
2 Ataques por ingeniería social

*Phishing, Vishing y Smishing | | **Baiting o Gancho** | Shoulder surfing | Dumpster Diving | Spam | Fraudes online*

Baiting o Gancho

¿Cómo funciona?

El *Baiting*, también conocido como "cebo", se sirve de un medio físico y de nuestra curiosidad o avaricia. ***Utilizando un cebo,*** los atacantes ***consiguen que infectemos nuestros equipos o compartamos información personal.***



¿Cómo se propaga/infecta/extiende?

El medio más utilizado son los dispositivos USB infectados que los atacantes colocan en sitios estratégicos, como lugares públicos con mucha afluencia de personas o en la entrada de las empresas. Otro método consiste en utilizar anuncios y webs con las que promocionar concursos y premios que nos incitan a compartir nuestros datos o descargar software malicioso.

¿Cuál es su objetivo?

Conseguir que los usuarios conectemos estos dispositivos infectados en nuestros equipos para ejecutar *malware* con el que robar nuestros datos personales y/o tomar control del equipo, infectar la red y llegar al resto de dispositivos.

¿Cómo me protejo?

La mejor defensa para este tipo de ataques ***es evitar conectar dispositivos desconocidos de almacenamiento externo o con conexión USB a nuestros equipos***. Además, debemos ***mantener nuestro sistema actualizado y las herramientas de protección, como el antivirus, activadas y actualizadas.*** Finalmente, como en todos los ataques por ingeniería social, debemos desconfiar de cualquier promoción demasiado atractiva, o de promesas que provengan de webs o mensajes poco fiables.

¿Sabías que el 95% de las incidencias en ciberseguridad se deben a errores humanos?

Prueba de detección de ingeniería social

TIPOS DE CIBERATAQUES

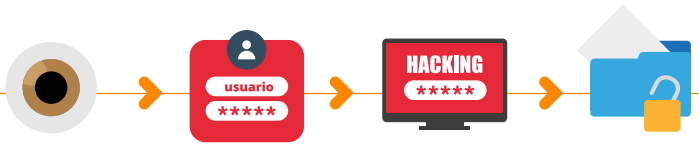
2 Ataques por ingeniería social

*Phishing, Vishing y Smishing | | Baiting o Gancho | **Shoulder surfing** | Dumpster Diving | Spam | Fraudes online*

Shoulder surfing

¿Cómo funciona?

Es una ***técnica mediante la que el ciberdelincuente consigue información*** de nosotros, como usuarios concretos, ***mirando "por encima del hombro" desde una posición cercana,*** mientras que utilizamos los dispositivos sin darnos cuenta.



¿Cómo se propaga/infecta/extiende?

No dispone de un medio de propagación, pero es habitual darse en lugares públicos, como cafeterías o centros comerciales, y en transportes, mientras utilizamos nuestro equipo, o en cajeros automáticos.

¿Cuál es su objetivo?

El objetivo es, como en otros ataques por ingeniería social, el robo de información: documentos confidenciales, credenciales, contactos, códigos de desbloqueo, etc.

¿Cómo me protejo?

La opción más segura es evitar que terceros tengan visión de nuestra actividad y, en sitios públicos, eludir compartir información personal o acceder a nuestras cuentas. ***También se recomienda utilizar gestores de contraseñas y la verificación en dos pasos*** para añadir una capa extra de seguridad a las credenciales.

Finalmente, ***debemos cerciorarnos de que no hay terceras personas observando nuestro dispositivo, especialmente a la hora de ingresar datos personales.*** Podemos utilizar medidas físicas, como los ***filtros "anti-espía"***. Se trata de una lámina fina que podemos colocar sobre la pantalla de nuestro dispositivo para evitar que terceros puedan ver su contenido desde distintos ángulos.

Técnicas de ingeniería social: ¿Cómo consiguen engañarnos?

El ciclo de la Ingeniería Social. ¿Cómo preparan los ciberdelincuentes un ataque de Ingeniería Social?

TIPOS DE CIBERATAQUES

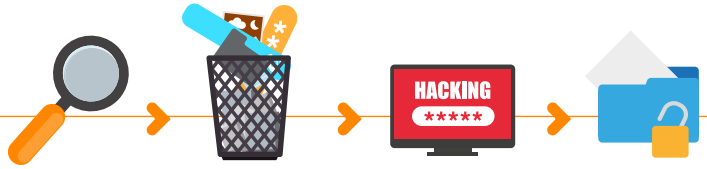
2 Ataques por ingeniería social

*Phishing, Vishing y Smishing | | Baiting o Gancho | Shoulder surfing | **Dumpster Diving** | Spam | Fraudes online*

Dumpster Diving

¿Cómo funciona?

En ciberseguridad, ***se conoce como el proceso de "buscar en nuestra basura" para obtener información útil sobre nuestra persona o nuestra empresa*** que luego pueda utilizarse contra nosotros para otro tipo de ataques.



¿Cómo se propaga/infecta/extiende?

No dispone de un medio de propagación, pero está dirigido principalmente a grandes organizaciones o a individuos en concreto de los que se pueda obtener información sensible. El usuario afectado podría haber tirado a la basura documentos importantes o información personal muy valiosa para un atacante.

¿Cuál es su objetivo?

Su objetivo son documentos, anotaciones y demás información sensible que hayan podido tirar a la basura por descuido, como números de tarjetas de crédito, contactos, anotaciones con credenciales, etc.

También buscan dispositivos electrónicos desechados a los que acceder y sacar toda la información que no haya sido borrada correctamente.

¿Cómo me protejo?

La única medida de protección que debemos seguir es ***la eliminación segura de información***. Desde una trituradora de papel para el formato físico, hasta seguir los pasos para la eliminación segura de información digital.

Técnicas de ingeniería social: ¿Cómo consiguen engañarnos?

¿Sabías que 2 de cada 5 dispositivos vendidos contienen información personal?

TIPOS DE CIBERATAQUES

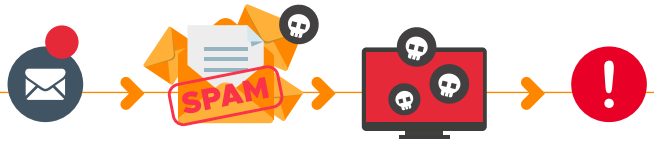
2 Ataques por ingeniería social

*Phishing, Vishing y Smishing | | Baiting o Gancho | Shoulder surfing | Dumpster Diving | **Spam** | Fraudes online*

Spam

¿Cómo funciona?

Consiste en el ***envío de grandes cantidades de mensajes o envíos publicitarios a través de Internet sin haber sido solicitados***, es decir, ***se trata de mensajes no deseados***. La mayoría tienen una finalidad comercial, aunque puede haberlos que contengan algún tipo de *malware*.



¿Cómo se propaga/infecta/extiende?

El canal más utilizado sigue siendo el correo electrónico, pero se sirve de cualquier medio de Internet que permita el envío de mensajes, como las aplicaciones de mensajería instantánea o las redes sociales.

¿Cuál es su objetivo?

Los objetivos son muy variados. Desde el envío masivo de mensajes publicitarios, hasta maximizar las opciones de éxito de un ataque de tipo *phishing* a una gran población, o tratar de infectar el mayor número posible de equipos mediante *malware*.

¿Cómo me protejo?

La recomendación es ***nunca utilizar la cuenta de correo electrónico principal para registrarnos en ofertas o promociones por Internet***. Además, es fundamental configurar el filtro anti*Spam* para evitar la recepción de este tipo de mensajes. Otros medios, como las redes sociales, también cuentan con medidas de protección similares pero lo mejor es ignorar y eliminar este tipo de mensajes.

- *Mis contactos están recibiendo spam y el remitente soy yo ¿por qué?*
- *Filtros de correo antispam: para qué sirven y cómo configurarlos*

TIPOS DE CIBERATAQUES

2 Ataques por ingeniería social

*Phishing, Vishing y Smishing | | Baiting o Gancho | Shoulder surfing | Dumpster Diving | Spam | **Fraudes online***

¿Cómo funciona?

La ingeniería social es utilizada frecuentemente para llevar a cabo todo tipo de fraudes y estafas online con las que engañarnos a los usuarios para que revelemos nuestros datos personales, o con las que obtener un beneficio económico a nuestra costa.

Existen una gran variedad de fraudes, y sus objetivos y medidas de protección pueden variar de un tipo a otro. ***Para aprender a identificarlos y a actuar ante ellos, la OSI pone a nuestra disposición una guía para aprender a identificar fraudes online***, donde se incluye: falsos préstamos, tiendas online fraudulentas, falsos alquileres, falso soporte técnico, sextorsión y muchos otros.



Guía para aprender a identificar fraudes online

Ponle freno a los fraudes y bulos con buenas prácticas

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

¿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 conecte 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 una VPN.

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

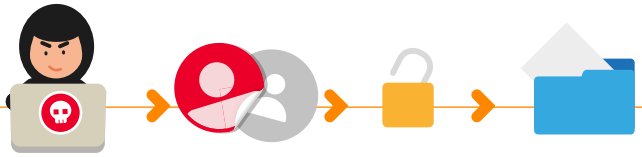
Spoofing

¿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***.



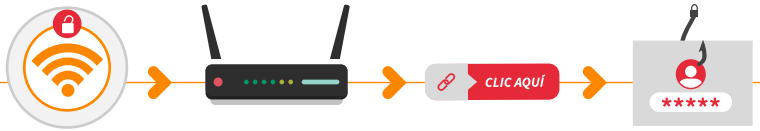
TIPOS DE CIBERATAQUES

3 Ataques a las conexiones

IP Spoofing

¿Cómo funciona?

El ciberdelincuente ***consigue falsear su dirección IP y hacerla pasar por una dirección distinta***. De este modo, consigue saltarse las restricciones del router del servidor o del nuestro 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 ataques DDoS 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?

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.

Una configuración segura del router protegerá el sistema de este y otros tipos de ataque.

Tu router, tu castillo. Medidas básicas para su protección

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

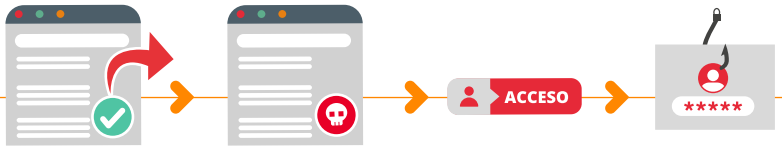
TIPOS DE CIBERATAQUES

3 Ataques a las conexiones

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 *https* ni certificados digitales 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?

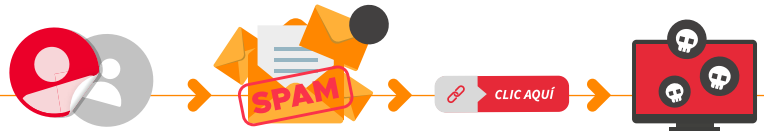
Tiendas online fraudulentas

TIPOS DE CIBERATAQUES

3 Ataques a las conexiones

¿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 bulos 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 nos descarguemos *malware* en su equipo.

¿Cómo me protejo?

Utilizar firma digital o cifrado a la hora de enviar *Emails* nos permitirá autenticar los mensajes y prevenir suplantaciones. Si la organización con la que nos comunicamos dispone de firma digital, también será más sencillo identificar este tipo de ataques.
Finalmente, ***analizando el contenido como si de un phishing se tratase, bastará para identificar el engaño.***

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

Cómo identificar un correo electrónico malicioso

TIPOS DE CIBERATAQUES

3 Ataques a las conexiones

¿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 router. 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 la DNS (*Domain Name System*), es decir, la tecnología utilizada para conocer la dirección IP del servidor donde está alojado el dominio al que queremos acceder.

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



¿Cómo se propaga/infecta/extiende?

Sirviéndose de la escasez de medidas de seguridad en nuestro router, así como de *malware* especializado, el atacante consigue acceder a la configuración del router 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 blindar la seguridad del router,*** restringiendo las conexiones remotas, cambiando las contraseñas por defecto, además de seguir las pautas para identificar webs fraudulentas.

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

TIPOS DE CIBERATAQUES

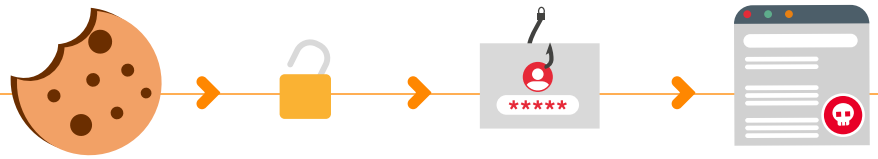
3 Ataques a las conexiones

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. Y siempre descargarlos desde sitios oficiales.
- ***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***.
- ***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

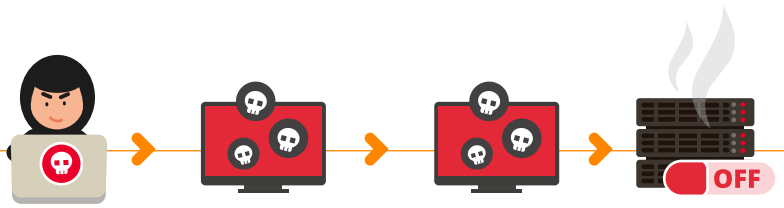
TIPOS DE CIBERATAQUES

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

¿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.
- ***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, redirigiendo el tráfico directo de Internet.



¿Qué son los ataques DoS y DDoS?

Qué es una botnet o una red zombi de ordenadores

TIPOS DE CIBERATAQUES

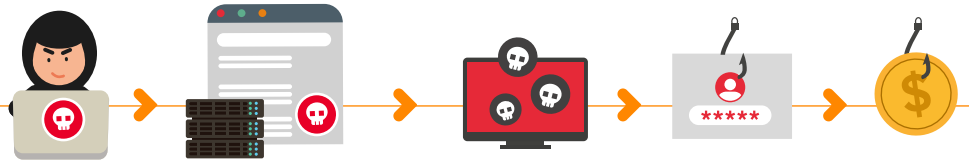
3 Ataques a las conexiones

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

Escaneo de puertos

¿Cómo funciona?

El ataque de escaneo de puertos, o *portscan*, ***es el proceso en el que se analiza automáticamente los puertos 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 de un router.

¿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 router tiene 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*

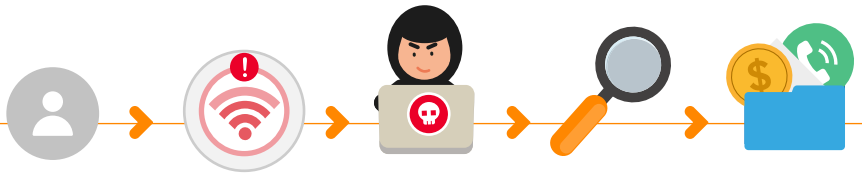
TIPOS DE CIBERATAQUES

3 Ataques a las conexiones

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 monitoriza 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 nuestro dispositivo y software instalado actualizado a su última versión,*** utilizar aplicaciones de cifrado y 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 *https* y certificado digital y conectarse a redes wifi por medio de una VPN si es necesaria la conexión a Internet.

Man in the middle. Toda tu actividad al descubierto

TIPOS DE CIBERATAQUES

3 Ataques a las conexiones

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?

Existen herramientas de protección antimalware que 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 desconocidos, etc.

Compartir Wifi ¿Si o No?
WhatsApp ya cifra las comunicaciones

4

Ataques por malware

Los ataques por *malware* se sirven de programas maliciosos cuya funcionalidad ***consiste en llevar a cabo acciones dañinas en un sistema informático y contra nuestra privacidad.*** Generalmente, buscan robar información, causar daños en el equipo, obtener un beneficio económico a nuestra costa o tomar el control de su equipo.

Dependiendo del *modus operandi*, y de la forma de infección, existen distintas categorías de *malware*. ***Las medidas de protección***, por el contrario, ***son muy similares para todos ellos y se basan en mantener activas y actualizadas las herramientas de protección antimalware.***



TIPOS DE CIBERATAQUES

4 Ataques por malware

Virus | Adware | Spyware | Troyanos | Gusano | Rootkit | Botnets | Rogueware | Criptojacking | Apps maliciosas

Virus

¿Cómo funciona?

Los virus se encuentran dentro de la categoría de *malware* y ***están diseñados para copiarse a sí mismos y propagarse a tantos dispositivos como les sea posible.***



¿Cómo se propaga/infecta/extiende?

Proliferan infectando aplicaciones, a través del correo electrónico u otros servicios web, y pueden transmitirse por medio de dispositivos extraíbles, como memorias USB o archivos adjuntos, incluso a través de conexiones de red.

¿Cuál es su objetivo?

Pueden llegar a modificar o eliminar los archivos almacenados en el equipo. Son capaces de dañar un sistema, eliminando o corrompiendo datos esenciales para su correcto funcionamiento.

¿Cómo me protejo?

La mejor protección ***es mantener activas y actualizadas las herramientas de protección, como el antivirus, y no descargar ningún archivo que pueda ser sospechoso*** o de origen poco fiable.

Principales tipos de virus y cómo protegernos frente a ellos

Ponte al día con los virus informáticos

TIPOS DE CIBERATAQUES

4 Ataques por malware

*Virus | **Adware** | Spyware | Troyanos | Gusano | Rootkit | Botnets | Rogueware | Criptojacking | Apps maliciosas*

Adware

¿Cómo funciona?

Se trata de un ***software malicioso*** diseñado ***para mostrarnos anuncios no deseados de forma masiva.***



¿Cómo se propaga/infecta/extiende?

Suelen instalarse junto a otros programas legítimos que, sin que nos percatemos, aceptamos y terminamos por instalar en el equipo.

¿Cuál es su objetivo?

Su objetivo es recopilar información sobre nuestra actividad y, de este modo, mostrarnos anuncios dirigidos.
Suelen suponer más una molestia y un incordio. Sin embargo, su instalación también puede suponer una bajada de rendimiento y un mal funcionamiento del dispositivo. Además, suelen servir de enlace a sitios web maliciosos.

¿Cómo me protejo?

Como protección, ***es fundamental evitar la descarga de aplicaciones de sitios no oficiales o el software pirata.*** También, se debe prestar atención a los pasos de la instalación para evitar seleccionar alguna casilla con la que instalar programas adicionales. Puede ser útil hacer clic en el botón de "Instalación Avanzada" u "Opciones de instalación".
Finalmente, otra recomendación es mantener las herramientas de protección debidamente actualizadas.

Principales tipos de virus y cómo protegernos frente a ellos
Qué es y cómo eliminar adware, spyware y bloatware

TIPOS DE CIBERATAQUES

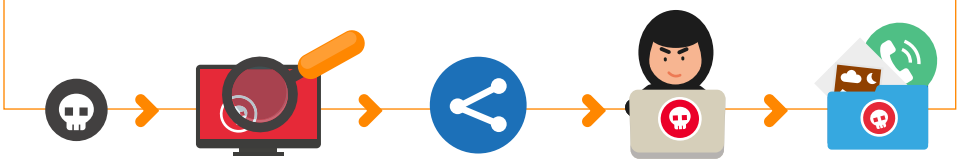
4 Ataques por malware

*Virus | Adware | **Spyware** | Troyanos | Gusano | Rootkit | Botnets | Rogueware | Criptojacking | Apps maliciosas*

Spyware

¿Cómo funciona?

Este *malware* ***se instala en nuestros equipos y comienza a recopilar información, supervisando toda su actividad para luego compartirlo con un usuario remoto.*** También es capaz de descargar otros *malware* e instalarlos en el equipo.



¿Cómo se propaga/infecta/extiende?

Al navegar por páginas webs no seguras, pueden aparecer mensajes en forma de anuncios o *pop-ups* que, al hacer clic, descarguen este tipo de *malware*. También es común que se ejecuten como programas adicionales durante la instalación de un *software*.

¿Cuál es su objetivo?

Una vez que el *malware* se instala en el dispositivo, puede llevar a cabo numerosas acciones, como controlar el dispositivo de forma remota, realizar capturas del contenido de aplicaciones y servicios como el correo electrónico o redes sociales.
También es capaz de registrar y capturar el historial de navegación y llevar a cabo grabaciones utilizando la cámara o el micrófono.

¿Cómo me protejo?

Descargar *software* desde el sitio oficial y prestar atención durante el proceso de instalación es fundamental. Además, ***es recomendable ignorar los anuncios y ventanas emergentes que aparezcan durante la navegación, y no hacer clic en archivos o enlaces que provengan de un sitio poco fiable.*** Finalmente, mantener el sistema y las herramientas de protección siempre activas y actualizadas minimizará los riesgos.

Principales tipos de virus y cómo protegernos frente a ellos
Qué es y cómo eliminar adware, spyware y bloatware

TIPOS DE CIBERATAQUES

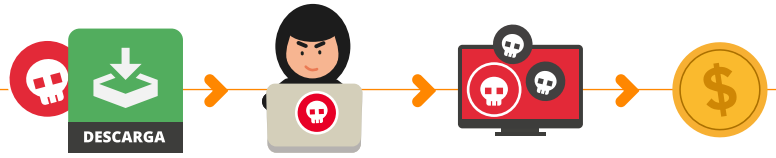
4 Ataques por malware

*Virus | Adware | Spyware | **Troyanos** | Gusano | Rootkit | Botnets | Rogueware | Criptojacking | Apps maliciosas*

Troyanos

¿Cómo funciona?

Los troyanos ***suelen camuflarse como un software legítimo para infectar nuestro equipo,*** o a través de ataques de ingeniería social.



¿Cómo se propaga/infecta/extiende?

A menudo, se propagan por medio de archivos adjuntos en correos electrónicos o desde páginas webs poco fiables, escondiéndose tras descargas de juegos, películas o aplicaciones no legítimas. Nosotros, confiados, no somos conscientes de que nuestros equipos han sido infectados hasta que es demasiado tarde.

¿Cuál es su objetivo?

La mayoría de los troyanos tienen como objetivo controlar nuestro equipo, robar los datos, introducir más *software* malicioso en el equipo y propagarse a otros dispositivos.

¿Cómo me protejo?

Las medidas de protección son comunes con otro tipo de *malware*, como ***mantener el equipo actualizado y las medidas de protección activadas (antivirus).*** También, evitar ejecutar archivos, *links* o utilizar dispositivos USB de dudosa procedencia.

Principales tipos de virus y cómo protegernos frente a ellos

Ponte al día con los virus informáticos

TIPOS DE CIBERATAQUES

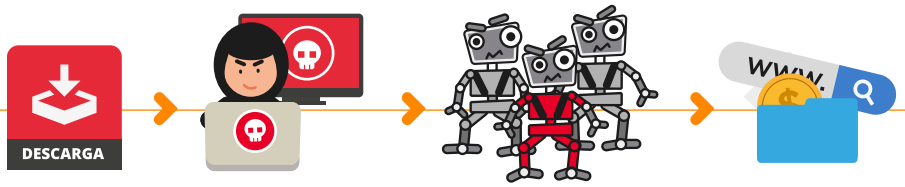
4 Ataques por malware

*Virus | Adware | Spyware | **Troyanos** | Gusano | Rootkit | Botnets | Rogueware | Criptojacking | Apps maliciosas*

Backdoors

¿Cómo funciona?

Una vez instalado en el sistema, permitirá al ciberdelincuente tomar el control del equipo de forma remota. Suelen utilizarse para infectar a varios dispositivos y formar una red zombi o *Botnet*.



¿Cómo se propaga/infecta/extiende?

A menudo, se propagan por medio de archivos adjuntos en correos electrónicos o desde páginas webs poco fiables, escondiéndose tras descargas de juegos, películas o aplicaciones no legítimas. Nosotros, confiados, no somos conscientes de que nuestros equipos han sido infectados hasta que es demasiado tarde.

En ocasiones, se aprovechan de vulnerabilidades específicas de los sistemas o de nuestra conexión.

¿Cuál es su objetivo?

Su objetivo es conseguir crear una puerta trasera en nuestro sistema con la que controlar el equipo poco a poco y, finalmente, robar información o perpetrar otro tipo de ataques.

Este tipo de *malware* tiene unas capacidades muy destructivas. Es capaz de monitorizar, registrar y compartir nuestra actividad con el atacante. Además, le permite crear, eliminar, editar y copiar cualquier archivo, así como ejecutar comandos y realizar modificaciones en el sistema.

¿Cómo me protejo?

Las medidas de protección son comunes con otro tipo de *malwares*, como ***mantener el equipo actualizado y las medidas de protección activadas (antivirus).*** También, evitar ejecutar archivos, *links* o utilizar dispositivos USB de dudosa procedencia.

Backdoor: MilkyDoor

IoT, el universo conectado

TIPOS DE CIBERATAQUES

4 Ataques por malware

*Virus | Adware | Spyware | **Troyanos** | Gusano | Rootkit | Botnets | Rogueware | Criptojacking | Apps maliciosas*

Keyloggers

¿Cómo funciona?

Los *Keyloggers* ***realizan un seguimiento y registran cada tecla que se pulsa en un equipo sin nuestro consentimiento.*** Pueden estar basados en un *software* o en un *hardware*, como por ejemplo un dispositivo USB.



¿Cómo se propaga/infecta/extiende?

A menudo, se propagan por medio de archivos adjuntos en correos electrónicos o desde páginas webs poco fiables, escondiéndose tras descargas de juegos, películas o aplicaciones no legítimas. Nosotros, confiados, no somos conscientes de que nuestros equipos han sido infectados hasta que es demasiado tarde.

En ocasiones, vienen ocultos en dispositivos USB que conectamos a nuestros equipos sin ser conscientes del peligro.

¿Cuál es su objetivo?

Su objetivo es monitorizar nuestra actividad y recoger datos que el atacante pueda utilizar para robar cuentas, información y perpetrar otro tipo de ataques.

Al ser capaz de interceptar y compartir todas las pulsaciones registradas en el teclado, la seguridad de nuestras cuentas puede ser fácilmente comprometida, así como otros datos sensibles, como los datos bancarios.

¿Cómo me protejo?

Las medidas de protección son comunes con otro tipo de *malware*, como ***mantener el equipo actualizado y las medidas de protección activadas (antivirus).*** También, evitar ejecutar archivos, *links* o utilizar dispositivos USB de dudosa procedencia.

Principales tipos de virus y cómo protegernos frente a ellos

¿Sabías que el 90% de las contraseñas son vulnerables?

TIPOS DE CIBERATAQUES

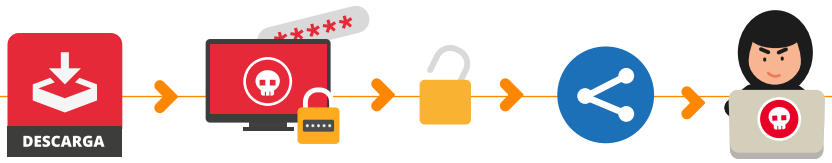
4 Ataques por malware

*Virus | Adware | Spyware | **Troyanos** | Gusano | Rootkit | Botnets | Rogueware | Criptojacking | Apps maliciosas*

Stealers

¿Cómo funciona?

Este tipo de troyano ***accede a la información privada almacenada en el equipo.*** Al ejecutarse, analiza los programas instalados y las credenciales almacenadas para luego, compartirlas con el atacante.



¿Cómo se propaga/infecta/extiende?

Se propaga por medio de archivos adjuntos en correos electrónicos o desde páginas webs poco fiables, escondiéndose tras descargas de juegos, películas o aplicaciones no legítimas.
No somos conscientes de que nuestros equipos han sido infectados hasta que es demasiado tarde.

¿Cuál es su objetivo?

Su objetivo es robar y compartir con el atacante todos los datos sensibles, como las contraseñas. Luego, el atacante podrá robar la información almacenada en las cuentas o suplantar la identidad de un usuario para perpetrar otro tipo de ataques.

¿Cómo me protejo?

Las medidas de protección son comunes con otro tipo de *malware*, como ***mantener el equipo actualizado y las medidas de protección activadas (antivirus).*** También, evitar ejecutar archivos, *links* o utilizar dispositivos USB de dudosa procedencia.

Principales tipos de virus y cómo protegernos frente a ellos

TIPOS DE CIBERATAQUES

4 Ataques por malware

*Virus | Adware | Spyware | **Troyanos** | Gusano | Rootkit | Botnets | Rogueware | Criptojacking | Apps maliciosas*

Ransomware

¿Cómo funciona?

Se trata de un tipo de *malware* que ***consigue tomar el control del dispositivo para cifrar el acceso al mismo y/o nuestros archivos o discos duros***. A cambio de recuperar el control y la información, nos exigirá el pago de un rescate.



¿Cómo se propaga/infecta/extiende?

A menudo, se propagan por medio de archivos adjuntos en correos electrónicos o desde páginas webs poco fiables, escondiéndose tras descargas de juegos, películas o aplicaciones no legítimas. No somos conscientes del ataque hasta que es demasiado tarde.

¿Cuál es su objetivo?

Una vez que el *malware* se ejecuta, poco a poco va cifrando todos los archivos y carpetas del dispositivo, impidiendo el acceso a ellos sin una clave. Una vez completada su tarea, el atacante nos envía otro correo con las instrucciones para el pago y el posterior envío de la clave para descifrar el equipo.

¿Cómo me protejo?

Las medidas de protección son comunes con otro tipo de *malware*, como ***mantener el equipo actualizado y las medidas de protección activadas (antivirus)***. También, evitar ejecutar archivos, *links* o utilizar dispositivos USB de dudosa procedencia.

- *Principales tipos de virus y cómo protegernos frente a ellos.*
- *El ransomware, cada vez más peligroso. Protégete.*

TIPOS DE CIBERATAQUES

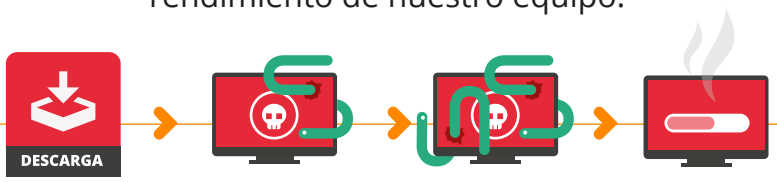
4 Ataques por malware

*Virus | Adware | Spyware | Troyanos | **Gusano** | Rootkit | Botnets | Rogueware | Criptojacking | Apps maliciosas*

Gusano

¿Cómo funciona?

Se trata de un tipo de *malware* que, ***una vez ejecutado en un sistema, puede modificar el código o las características de este.*** Generalmente, pasan inadvertidos hasta que su proceso de reproducción se hace evidente, produciendo consecuencias en el rendimiento de nuestro equipo.



¿Cómo se propaga/infecta/extiende?

Las formas más comunes son por medio de archivos adjuntos, las redes de intercambio de archivos y los enlaces a sitios web maliciosos. También pueden infectar otros dispositivos al conectar dispositivos USB infectados con el gusano.

¿Cuál es su objetivo?

El objetivo de un gusano informático no es otro que el de replicarse e infectar otros dispositivos. Una vez dentro, es capaz de realizar cambios en el sistema sin nuestra autorización.

La propagación de este tipo de *malware* supone un consumo de los recursos del sistema infectado. Puede traducirse en una disminución del rendimiento o una peor conexión al estar consumiendo parte de nuestro ancho de banda.

¿Cómo me protejo?

Las medidas de protección son comunes a otro tipo de ataques por *malware*. Se basan en ***mantener activos y actualizados los programas de protección, como el antivirus y el firewall, así como mantener nuestro sistema actualizado para evitar vulnerabilidades.***

Finalmente, es recomendable evitar la descargar de archivos maliciosos y navegar por sitios webs fraudulentos.

Principales tipos de virus y cómo protegernos frente a ellos

Infección masiva de ordenadores por el gusano Downadup (Conficker)

TIPOS DE CIBERATAQUES

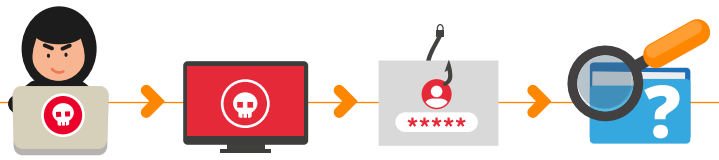
4 Ataques por malware

*Virus | Adware | Spyware | Troyanos | Gusano | **Rootkit** | Botnets | Rogueware | Criptojacking | Apps maliciosas*

Rootkit

¿Cómo funciona?

Un *Rootkit* es un ***conjunto de herramientas utilizadas por los ciberdelincuentes para acceder de forma ilícita a un sistema.*** Una vez dentro, se utilizarán para mantener al atacante con acceso al sistema y poder llevar a cabo otro tipo de ciberataques.



¿Cómo se propaga/infecta/extiende?

Del mismo modo que otros *malware*, es capaz de infectar otros dispositivos a través de archivos adjuntos maliciosos o descargas en sitios fraudulentos. También pueden ser instalados en nuestro sistema aprovechándose de alguna vulnerabilidad o tras conocer las credenciales de acceso.

¿Cuál es su objetivo?

Su propósito es la ocultación de elementos del sistema infectado, como archivos, procesos, credenciales, etc., de modo que no seamos capaces de encontrarlos.

¿Cómo me protejo?

Las medidas de protección son comunes a otro tipo de ataques por *malware*. Se basan en ***mantener activos y actualizados los programas de protección, como el antivirus y el firewall, así como mantener nuestro sistema actualizado para evitar vulnerabilidades.***
Finalmente, es recomendable evitar la descarga de archivos maliciosos y la utilización de contraseñas robustas.

- *No hace falta superpoderes para proteger los dispositivos*
- *Qué es y cómo eliminar adware, spyware y bloatware*

TIPOS DE CIBERATAQUES

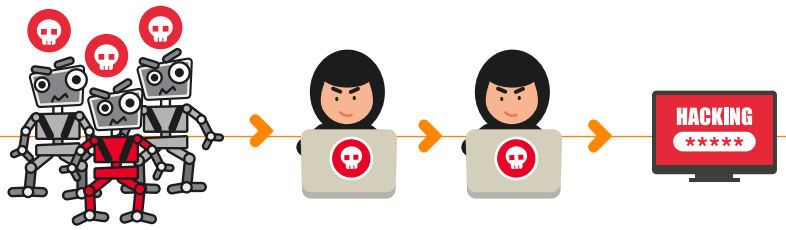
4 Ataques por malware

*Virus | Adware | Spyware | Troyanos | Gusano | Rootkit | **Botnets** | Rogueware | Criptojacking | Apps maliciosas*

Botnets

¿Cómo funciona?

Así se conoce a la ***red compuesta por diversos dispositivos infectados y controlados de forma remota por uno o varios ciberdelincuentes.***



¿Cómo se propaga/infecta/extiende?

Para infectar un equipo, los atacantes suelen recurrir a códigos maliciosos en páginas webs tras explotar una vulnerabilidad. Una vez que accedemos a la web, nuestro equipo queda infectado sin ser consciente de ello. También suelen recurrir al envío de archivos maliciosos a través de mensajes por Internet, como el correo electrónico.

¿Cuál es su objetivo?

El atacante busca controlar el mayor número de dispositivos posibles con los que llevar a cabo sus actividades ilícitas con la mayor probabilidad de éxito posible.

¿Cómo me protejo?

Las medidas de protección son comunes a otro tipo de ataques por *malware*. Se basan en ***mantener activos y actualizados los programas de protección, como el antivirus y el firewall, así como mantener nuestro sistema actualizado para evitar vulnerabilidades.***
Finalmente, es recomendable evitar la descarga de archivos maliciosos y la utilización de contraseñas robustas.

Principales tipos de virus y cómo protegernos frente a ellos

Qué es una botnet o una red zombi de ordenadores

TIPOS DE CIBERATAQUES

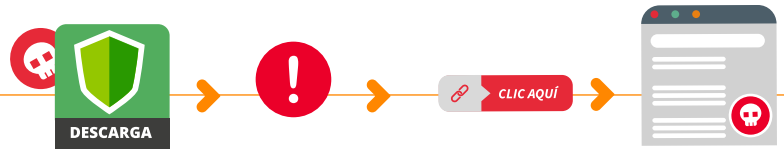
4 Ataques por malware

*Virus | Adware | Spyware | Troyanos | Gusano | Rootkit | Botnets | **Rogueware** | Criptojacking | Apps maliciosas*

Rogueware

¿Cómo funciona?

Se trata de un ***software malicioso que simula ser un antivirus o herramienta de seguridad*** y que nos alerta de un problema con nuestros dispositivos**.** Pueden alertar sobre la presencia de un *malware*, una amenaza o un problema que hay que corregir.
Rápidamente, ***nos invitará a hacer clic en un botón o enlace para descargar un supuesto software con el que solucionar el problema.***



¿Cómo se propaga/infecta/extiende?

Al igual que muchos otros *malware*, se propaga a través de archivos maliciosos que podríamos haber descargado a través de Internet, por ejemplo, al navegar por sitios webs poco fiables.

¿Cuál es su objetivo?

El objetivo del atacante es conseguir que hagamos clic en los enlaces que aparecen en las supuestas alertas de seguridad. Una vez hacemos clic, se descargará algún tipo de *malware*, o accederemos a una página web maliciosa.

¿Cómo me protejo?

Dado que el atacante requiere que hagamos clic en sus alertas, la mejor protección es aplicar el sentido común y confiar solo en las herramientas de seguridad legítimas.
Por otro lado, es fundamental que el sistema y las herramientas de protección se encuentren debidamente actualizadas.

4 de cada 10 falsos antivirus han sido creados este año

TIPOS DE CIBERATAQUES

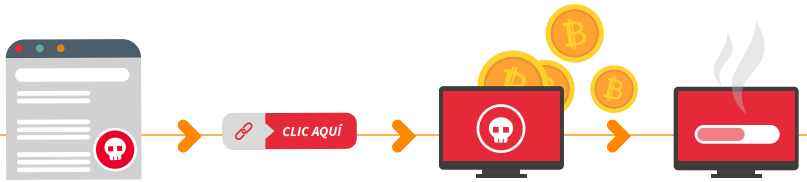
4 Ataques por malware

*Virus | Adware | Spyware | Troyanos | Gusano | Rootkit | Botnets | Rogueware | **Criptojacking** | Apps maliciosas*

Criptojacking

¿Cómo funciona?

El *Criptojacking* es una práctica por medio de la cual, los ciberdelincuentes ***utilizan nuestros dispositivos sin nuestro consentimiento para llevar a cabo "extracciones" de criptomonedas.*** Durante el proceso, utilizan los recursos del sistema.
Las criptomonedas son un tipo de divisa virtual muy popular desde hace varios años que puede utilizarse para pagar por Internet. Sin embargo, gracias a que permiten anonimizar las transacciones son muy utilizadas por los ciberdelincuentes como forma de pago en sus extorsiones.



¿Cómo se propaga/infecta/extiende?

Un equipo puede infectarse al descargarse este *malware* a través de un archivo malicioso o a través de páginas webs maliciosas que utilizan el ancho de banda de nuestra conexión para llevar a cabo los procesos de extracción.

¿Cuál es su objetivo?

No tiene interés en acceder a nuestros datos personales, sino en utilizar nuestros recursos para el minado de criptomonedas y obtener un beneficio económico.
La principal amenaza reside en el consumo de recursos que puede llegar a paralizar otros procesos e impedirnos utilizar con normalidad. Este consumo puede desembocar en el aumento de las facturas de luz o en la reducción de la vida útil del dispositivo.

¿Cómo me protejo?

La primera medida de protección es la instalación y actualización de un antivirus, así como llevar a cabo inspecciones regulares en busca de *malware*. Luego, es recomendable evitar la descarga de archivos maliciosos y la conexión a redes wifi públicas o a páginas webs poco fiables.
Finalmente, existen diversos complementos para el navegador que actúan como bloqueadores de scripts de *Criptojacking*.

Criptomonedas: Entremos en materia

Mi PC se convirtió en una mina de bitcoins

TIPOS DE CIBERATAQUES

4 Ataques por malware

Apps maliciosas

¿Cómo funciona?

Las *Apps* maliciosas ***se hacen pasar por aplicaciones legítimas o tratan de emular a otras aplicaciones de éxito.*** Una vez instaladas en el dispositivo, ***nos pedirán una serie de permisos abusivos o, por el contrario, harán un uso fraudulento de dichos permisos.***



¿Cómo se propaga/infecta/extiende?

Suelen estar disponibles para su descarga fuera de las tiendas oficiales de aplicaciones, aunque en ocasiones pueden saltarse los filtros de seguridad de estos sitios oficiales. Una vez instaladas, utilizarán los permisos concedidos para llevar a cabo su objetivo.

¿Cuál es su objetivo?

El objetivo de una *App* maliciosa es aprovecharse de los permisos concedidos para el robo de información y la toma de control del dispositivo. Las consecuencias son muy variadas y dependen del tipo de permiso que se conceda a la *App*. Pueden ir desde una reducción en el rendimiento del dispositivo o el robo de datos hasta la toma de control por parte del atacante debido a la concesión de permisos.

¿Cómo me protejo?

Como protección, ***lo primero si se sospecha de la instalación de una App maliciosa es desinstalarla del dispositivo.*** Para prevenir consecuencias más graves, es conveniente cifrar el dispositivo, así como hacer copias de seguridad de la información almacenada. Finalmente, es imprescindible descargar aplicaciones de los sitios oficiales, como **Google Play** o la **App Store**.

¡Ayuda! Instalé una app no fiable

Acepto o no lo acepto: revisando los permisos de las apps

MEDIDAS DE PROTECCIÓN

Proponemos el siguiente ***decálogo de buenas prácticas en ciberseguridad para mejorar la protección de los dispositivos y la seguridad de la información*** de los usuarios ***frente a los ciberataques***:



- ***Utiliza un antivirus*** para analizar todas las descargas y archivos sospechosos. Debes mantenerlo siempre actualizado y activo.
- ***Mantén el sistema operativo, navegador y aplicaciones siempre actualizadas*** a su última versión para evitar vulnerabilidades.
- ***Utiliza contraseñas robustas y diferentes*** para proteger todas tus cuentas. Si es posible, utiliza la verificación en dos pasos u otro factor de autenticación.
- ***Desconfía de los adjuntos sospechosos, enlaces o promociones demasiado atractivas.*** La mayoría de los fraudes se basan en ataques de ingeniería social que pueden ser detectados aplicando el sentido común.
- ***Ten cuidado por dónde navegas.*** Utiliza solo webs seguras con *https* y certificado digital y utiliza el modo incógnito cuando no quieras dejar rastro.
- ***Descarga solo de sitios oficiales*** aplicaciones o *software* legítimo para evitar acabar infectado por *malware*. En el caso de las aplicaciones, recuerda dar solo los permisos imprescindibles para su funcionamiento.
- ***Evita conectarte a redes wifi públicas o a conexiones inalámbricas desconocidas.*** Especialmente cuando vayas a intercambiar información sensible, como los datos bancarios. Y, en caso de que tengas que conectarte por una emergencia, trata de utilizar una VPN.
- ***No compartas tu información personal*** con cualquier desconocido ni la publiques o guardes en páginas o servicios webs no fiables.
- ***Haz copias de seguridad*** para minimizar el impacto de un posible ciberataque.

Recuerda que desde INCIBE, ponemos a tu disposición una línea telefónica gratuita de ayuda en ciberseguridad, 017.

017 TU AYUDA EN CIBERSEGURIDAD



TU AYUDA EN
CIBERSEGURIDAD

incibe_

017

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

017

OSI Oficina de Seguridad del Internauta