Guía de ciberataques

ATAQUES POR MALWARE # 22

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.*

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 una pantalla 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 a otro tipo de malware, como mantener el equipo actualizado y las medidas de protección activadas (antivirus). Mantenga siempre respaldada o sincronizada su información en la nube corporativa (One drive /Sharepoint). También, evite ejecutar archivos, links de dudosa procedencia o utilizar dispositivos USB. ¡NO PAGUE RESCATE!

Principales tipos de virus y cómo protegernos frente a ellos.

El ransomware, cada vez más peligroso. Protégete.

TIPOS DE CIBERATAQUES

4 Ataques por malware

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 de propagación son por medio de archivos adjuntos, carpetas compartidas locales, 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 el sistema operativo actualizado para evitar vulnerabilidades. Nunca cree y comparta archivos en carpetas compartidas locales. Finalmente, es recomendable evitar la descargar de archivos maliciosos, navegar por sitios webs fraudulentos, evite ejecutar archivos, links de dudosa procedencia o utilizar dispositivos USB

Principales tipos de virus y cómo protegernos frente a ellos

Infección masiva de ordenadores por el gusano Downadup (Conficker)

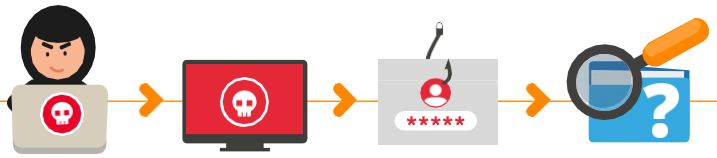
TIPOS DE CIBERATAQUES

4 Ataques por malware

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

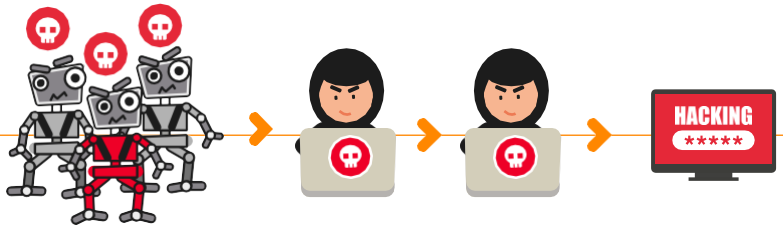
TIPOS DE CIBERATAQUES

4 Ataques por malware

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 o redes sociales.

¿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

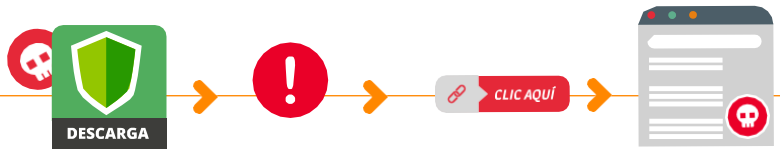
TIPOS DE CIBERATAQUES

4 Ataques por malware

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 o institucionales.* **Por otro lado, es fundamental que el sistema operativo y las herramientas de protección de nuestros dispositivos se encuentren debidamente actualizadas.**

4 de cada 10 falsos antivirus han sido creados este año

TIPOS DE CIBERATAQUES

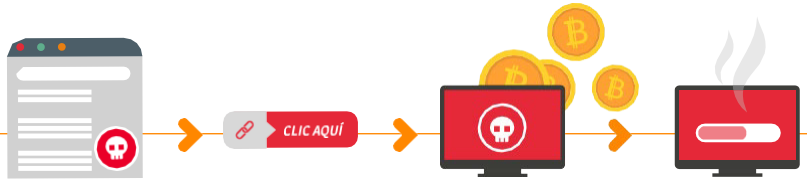
4 Ataques por malware

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 programas de* **Criptojacking**.

Criptomonedas: Entremos en materia

Mi PC se convirtió en una mina de bitcoins

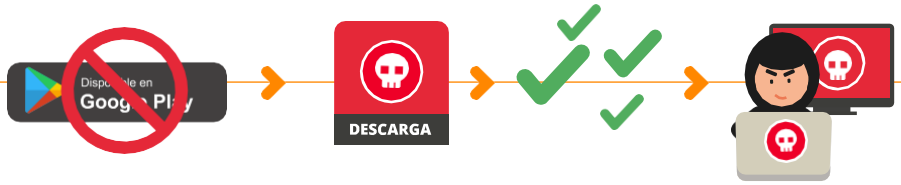
TIPOS DE CIBERATAQUES

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

Fuente:

INCIBE - https://www.incibe.es

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