Guía de ciberataques

ATAQUES POR MALWARE # 12

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.*

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 antivirus y antimalware.

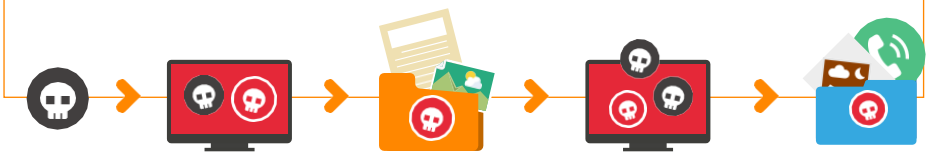
TIPOS DE CIBERATAQUES

4 Ataques por malware

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

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 lo 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 e incomodidad. Sin embargo, su instalación también puede suponer una pérdida de rendimiento del equipo o dispositivo 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 de 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 de antivirus debidamente actualizadas.**

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

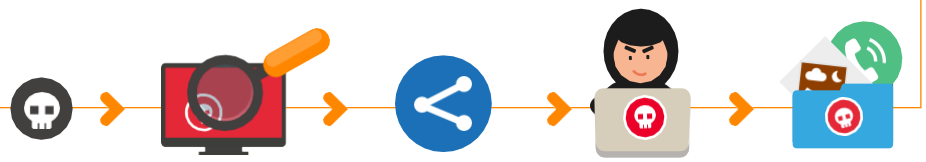
TIPOS DE CIBERATAQUES

4 Ataques por malware

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 del dispositivo.**

¿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 sitios poco fiables.*** **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

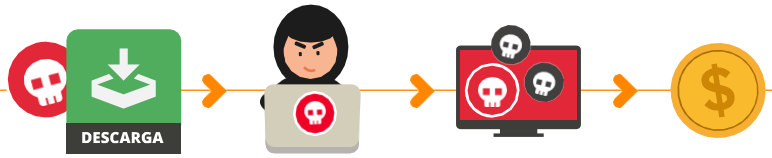
4 Ataques por malware

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 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 a través de la red.**

¿Cómo me protejo?

Las medidas de protección para contener infección por troyanos consisten en *mantener el equipo actualizado y las medidas de protección activadas (antivirus).* **También, evitar ejecutar** *archivos* **y** *links* **de dudosa procedencia, o utilizar dispositivos USB.**

Principales tipos de virus y cómo protegernos frente a ellos

Ponte al día con los virus informáticos

TIPOS DE CIBERATAQUES

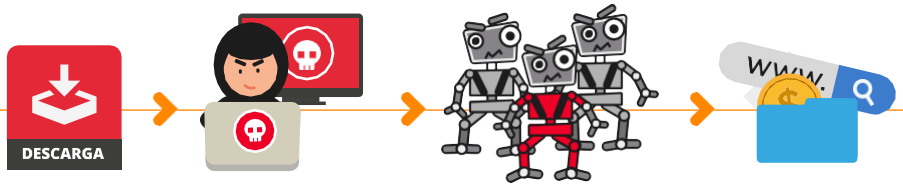
4 Ataques por malware

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 usando todos los dispositivos infectados (Red Zombie).
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* **y** *links* **de dudosa procedencia, o utilizar dispositivos USB.**

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 y links de dudosa procedencia, o utilizar dispositivos USB. Tampoco se debe permitir el acceso físico al equipo de cómputo para personas desconocidas o sin supervisión permanente. Revise periódicamente los conectores y puertos de su equipo y teclado, para descartar conexión de elementos extraños .

Principales tipos de virus y cómo protegernos frente a ellos
¿Sabías que el 90% de las contraseñas son vulnerables?

TIPOS DE CIBERATAQUES

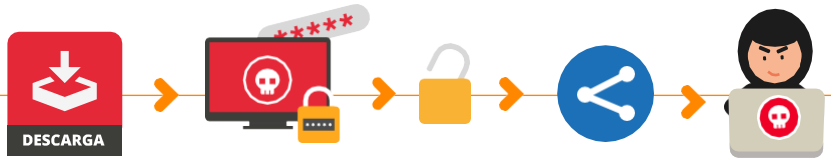
4 Ataques por malware

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 descargar películas y juegos, ejecutar archivos o** *links* **de dudosa procedencia, o utilizar dispositivos USB.**

Principales tipos de virus y cómo protegernos frente a ellos

Fuente:

INCIBE - https://www.incibe.es

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