Tipos de malware y cómo puedes eliminarlos

Descubre qué tipos de software malicioso pueden atacar tu dispositivo y cómo protegerlo de ellos.

1. Ciberseguridad
2. Ataques informáticos
3. Tipos de malware y cómo puedes eliminarlos

Índice

02/11/2021

Un *malware* es todo **programa o código malicioso que ataca un dispositivo electrónico**, desde ordenadores a móviles o tabletas, con el objetivo de **dañar su sistema**, provocar un **mal funcionamiento del mismo** o **robar la información** alojada en él. Puede venir oculto en:

2. **Enlaces en SMS** que solicitan descargar aplicaciones o archivos.
3. **Aplicaciones no oficiales** que han sido infectadas con este software.
4. **Publicidad maliciosa** enmascarada en páginas web ilegítimas.
5. **Actualizaciones de software solicitadas** para ver ciertos contenidos en páginas web.

En caso de que el dispositivo electrónico se vea infectado con un *malware*, pueden detectarse **ciertas anomalías**, tales como:

- El dispositivo **no funciona con la fluidez** habitual.
- El sistema **se bloquea** con frecuencia.
- Se **reduce el espacio disponible en el disco duro**.
- Se **instalan programas desconocidos** para el usuario.
- Aparecen **extensiones y herramientas** en el navegador **que no se han descargado previamente**.
- **Cambia la página de inicio** del mismo.
- Se reciben **mensajes de error** desconocidos con asiduidad.
- **Deja de funcionar correctamente** el antivirus.

¿Cuáles son los principales objetivos que persiguen estos programas maliciosos?

- **Robo de información**: son muchos los tipos de malware que tienen como objetivo conseguir información personal del usuario (contraseñas, cuentas bancarias o medios de pago) para venderla o utilizarla posteriormente, con el fin de cometer fraude o extorsión. Entre ellos se encuentran:
  - ***Troyano***: se presenta como un programa útil para el usuario, por lo que habitualmente lo descarga e instala sin miedo. Una vez en el sistema, ofrece acceso remoto y no autorizado al hacker al dispositivo ya infectado.
  - ***Spyware***: software espía que se instala en el equipo del usuario cuando descarga un fichero adjunto infectado o instala algún programa que contiene este software camuflado. Recopila información privada de los usuarios y la envía a terceros.
  - ***Keylogger***: es una aplicación que registra las teclas que pulsa el usuario en su equipo, sin su permiso ni conocimiento, y después envía la información a terceros.
- **Secuestro de información (*ransomware*)**: es un tipo de malware que bloquea el acceso a la información almacenada en el equipo del usuario, cifrándola. Tras ello, los delincuentes solicitan el pago de un importe para que el usuario pueda recuperar dicha información. El miedo a perderla hace que las víctimas paguen este rescate, con resultados muy diversos, por lo que es totalmente desaconsejable ceder ante este tipo de extorsiones.
- **Fines publicitarios**: menos peligroso, pero muy molesto, es el denominado malware publicitario o *adware*, un software que muestra anuncios no deseados en la pantalla del usuario, habitualmente a través de su navegador o de su cuenta de correo. También lo hace mediante ventanas emergentes o *pop-ups*.

Seguro BBVA Allianz Cyber

BBVA ayuda a sus clientes pymes y autónomos a proteger sus negocios de las ciberamenazas existentes en la red con herramientas como el seguro BBVA Allianz Cyber.

El seguro proporciona coberturas preventivas para incrementar la seguridad de la información de la empresa, así como asistencia legal, informática y de peritos informáticos en caso de pérdida o robo de datos y coberturas de daños propios como la pérdida de beneficios por paralización del negocio. Además, presta el apoyo y asesoramiento de un equipo de especialistas en caso de reclamaciones por violación de datos, perjuicios por actos en medios o sanciones de protección de datos.

Tipos de pharming

Existen tres versiones:

- *Ataque al archivo host del ordenador (o pharming local)*

Requiere la instalación del virus o troyano en el ordenador. El objetivo es modificar dicho archivo y reconducir, con ello, el rumbo del tráfico a un sitio web malicioso de su elección (en el que se lleva a

Tipos de pharming

Existen tres versiones:

- *Ataque al archivo host del ordenador (o pharming local)*

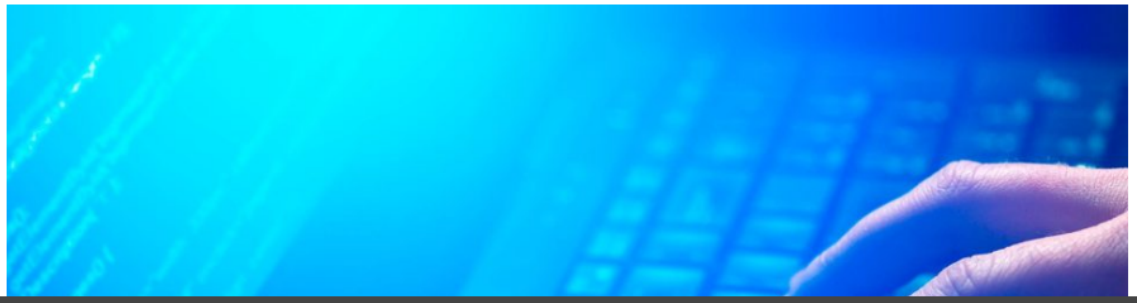
Requiere la instalación del virus o troyano en el ordenador. El objetivo es modificar dicho archivo y reconducir, con ello, el rumbo del tráfico a un sitio web malicioso de su elección (en el que se lleva a cabo el robo de datos sensibles).

- *Ataque al servidor DNS (o Drive-By pharming)*

Tras sortear los firewalls o rúters, se infecta este servidor (encargado de traducir los nombres de las distintas webs tomando como referencia la IP), enviando a los usuarios que acceden a ellas a una dirección falsa elegida por el hacker.

- *Ataque a las vulneraciones del servidor DNS (o DNS poisoning)*

Como variante de la anterior, su objetivo son las brechas que puedan tener los servidores DNS en relación a su caché de direcciones. Su complejidad hace que sea la más peligrosa de las 3 aunque, hoy en día, es la menos habitual, ya que los proveedores de Internet han corregido los fallos que pudiese haber.



Pharming contra phishing: ¿qué los diferencia?

A pesar de tener la misma meta, la forma de realizar el ataque es diferente. Mientras el *phishing emplea un cebo* (sms, correo electrónico, etc.) con el que atraer al usuario a una web en la que *robarle sus datos, el pharming le ataca directamente, accediendo a su ordenador (bien al hosts o al servidor DNS*) y enviándole directamente a la web en la que se le sustraerá la información (en lugar de darle la opción de clicar, o no, en un enlace).

Combatir el pharming, ¿es posible?

Un ataque de pharming es difícil de detectar si se realiza bien, por lo que es mejor prevenirlo. Para ello, existen una serie de medidas básicas a adoptar:

- *Comprobar que la url es correcta* (se corresponde con la que accedes habitualmente). Si detectas qu no es la misma, puedes estar ante una copia.
- *Revisar que incluye la 's'* tras el 'http' (visualizando 'https').
- *Evaluar bien la página antes de empezar a navegar por ella* (su aspecto es el de siempre). Hay que vigilar tanto sus componentes como los distintos enlaces que incluya.
- *No pulsar en enlaces ni descargar archivos* que no parezcan seguros.
- *Visualizar las notificaciones del antivirus* o el navegador. Si indican que la página no es segura, lo mejor es no entrar y buscar una opción alternativa.
- *Contar con un buen software de seguridad* y hacerlo, si es posible, en su versión de pago (y no la gratuita, más limitada). También se pueden encontrar opciones ad hoc para este tipo de vulneraciones, más adecuadas a la hora de evitar el robo de información delicada.

La creciente preocupación de los ciudadanos por el coronavirus está siendo aprovechada por los ciberdelincuentes para realizar estafas electrónicas y obtener información privada de los usuarios.

Los tipos de ciberataques que están ejecutando para llevar a cabo estos delitos son, principalmente:

- El *phishing:* correos electrónicos en los que suplantan a un organismo oficial e intentan redirigir al usuario, a través de un enlace, a una página web falsa para que introduzca en ella sus datos personales y/o bancarios. También pueden contener un archivo adjunto que ha sido infectado con software malicioso.
- El *smishing:* el modus operandi es el mismo, pero los canales utilizados son el SMS y las herramientas de mensajería instantánea como WhatsApp.

Ten precaución y mantente en alerta si recibes alguno de los siguientes correos electrónicos o mensajes fraudulentos relacionados con el coronavirus que están circulando durante estos días por la Red:

1. Mensaje de *WhatsApp suplantando al Ministerio de Sanidad* con algunas recomendaciones para hacer frente a la nueva enfermedad. El texto va encabezado por el titular *'ALERTA POR CORONAVIRUS. Mensaje urgente del Ministerio de Sanidad'* y va acompañado de un enlace que redirige a los usuarios a una *página web falsa de venta de mascarillas.*
2. Correo electrónico en el que suplantan al *departamento interno de la empresa* y en el que invitan a descargar un PDF, infectado con malware, con el *protocolo que la compañía ha activado para enfermedades contagiosas.*
3. Correo electrónico de la *Organización Mundial de la Salud* (OMS) que incluye un botón para descargar las medidas de seguridad (escrito en inglés, **Safety measures**). El email aparece firmado por la supuesta doctora Stella Chungong.
4. Correo electrónico del *Centro para el Control y la Prevención de Enfermedades* (CDC) con remitente *CDC-Covid19@cdc.gov* en el que se informa del avance del coronavirus y se solicitan donaciones a través de bitcoins. El correo, redactado en inglés, está firmado por la Division of eHealth Marketing. También suplantando al CDC está circulando otro correo con un archivo adjunto malicioso que supuestamente contiene las últimas estadísticas sobre contagios.
5. También han sido detectados diversos mapas online que muestran el número de infectados por el coronavirus en cada uno de los países. *Las páginas web y aplicaciones que los albergan contienen software espía y malware* y han sido diseñadas para infectar los dispositivos de los