Virus informáticos

Equipo editorial, Etecé ⋮⋮ 27/6/2016

4 min. de lectura

Te explicamos qué son los virus informáticos y cuáles son sus características. Además, cómo se propagan y cómo protegerse de ellos.

Los virus informáticos son piezas de software programadas con fines dañinos.

¿Qué son los virus informáticos?

Los virus informáticos **son programas informáticos (**software**) diseñados para esparcirse en las computadoras ajenas** y ocasionar daños, robar datos o sabotear su funcionamiento. Normalmente, la "infección" de la computadora y la ejecución del virus se llevan a cabo de manera automática, sin la autorización expresa del usuario.

A este tipo de programas **se los conoce como "virus" porque su comportamiento es similar al de los virus biológicos**: ingresan secretamente en un sistema informático e introducen un conjunto de instrucciones específicas en el código de ciertos archivos. De esta manera, el sistema, al ejecutarlos, activa también la programación del virus.

Las acciones de los virus en una computadora infectada pueden ser muy distintas y tener objetivos diferentes. Entre ellos, el robo de información personal de importancia (claves de seguridad, datos de acceso y contraseñas, por ejemplo), la difusión de publicidad invasiva y no autorizada por el usuario, el sabotaje del funcionamiento regular del sistema o incluso la entrega del control a terceros de manera remota y clandestina.

¿Son lo mismo los virus y el *malware*?

En la jerga informática, los virus son una de las formas del *malware* o software malintencionado. Sin embargo, se suele utilizar el término *malware* para referir a otros programas menos peligrosos, aunque no inofensivos, que se dedican a bombardear al usuario con publicidad, conducirlo automáticamente hacia páginas web específicas o hacerlo caer en ofertas engañosas o portales peligrosos.

- Ver además: Software libre

Características de los virus informáticos

Los virus informáticos pueden ser muy distintos en sus efectos y métodos de infección, pero en general comparten las siguientes características:

- Son piezas de software programadas de manera clandestina y con fines dañinos e ilegales.
- Suelen ser programas livianos, breves, de código simple, pero encriptado.
- Ejecutan acciones no autorizadas por el usuario, como robar datos, consumir recursos o sabotear el funcionamiento del sistema.
- Se transmiten de una computadora a otra a través de distintos medios y procedimientos, como discos infectados o redes informáticas.
- Algunos cuentan con mecanismos de camuflaje para evitar ser detectados por el usuario o por el software antivirus.
- Pueden ser resistentes al formateo de la memoria de la computadora.
- En algunos casos, facilitan la infección de la computadora por otros softwares maliciosos, actuando con ellos de manera conjunta.

Tipos de virus informáticos

Existe una enorme variedad de virus informáticos. Normalmente, se los clasifica de acuerdo a sus mecanismos de transmisión y a los efectos que surten dentro de los sistemas infectados.

Según sus mecanismos de transmisión

Según sus mecanismos de transmisión, es posible clasificar los virus informáticos en dos categorías esenciales: los virus residentes y los no residentes.

- **Virus residentes**. Son aquellos que se alojan en la memoria RAM de la computadora, por lo que se ejecutan cada vez que se inicia el sistema y pueden infectar al instante cualquier aplicación que ejecute el usuario.
- **Virus no residentes o de acción directa**. Son aquellos que no se alojan en la memoria RAM, sino que se encuentran contenidos en un archivo específico dentro del sistema. Actúan únicamente cuando ese archivo es ejecutado; el resto del tiempo permanecen ocultos.

Según sus efectos en el sistema infectado

En cuanto a sus dinámicas y efectos en el sistema infectado, es posible clasificar los virus informáticos en los siguientes tipos:

- **Virus de sobreescritura**. Son programas maliciosos que afectan un archivo determinado y proceden a sobreescribir su código, haciéndolo completamente inservible. Muchas veces estos virus inscriben mensajes o contenido al azar en el interior de los archivos infectados.
- **Virus en lotes (*batch*)**. Son conjuntos de instrucciones específicas contenidas en un fichero de lenguaje script. Al ejecutarse, fuerzan al sistema a realizar determinadas acciones, como abrir carpetas específicas, apagar la computadora o simplemente agotar en vano sus recursos disponibles.
- **Virus de red y de secuencias de comandos web**. Son programas que atacan el navegador web y otras herramientas vinculadas con las redes informáticas, para afectar la conectividad de la computadora, capturar parte de la información que se carga o descarga del sistema, o bien debilitar los sistemas de seguridad para facilitar la infiltración de *hackers* y programas malintencionados. A los virus que hacen esto último se los conoce como “troyanos”.
- **Virus del sector de arranque (*boot*)**. Son programas que atacan los sectores específicos de la memoria que permiten el inicio del sistema. De este modo, al iniciar la computadora, sus códigos se ejecutan y producen sus efectos dañinos.
- **Virus de macros**. Son programas que atacan directamente las tareas automáticas del software de aplicación de escritorio, como los paquetes de Microsoft Office. Este tipo de programas se ejecutan al abrir los documentos infectados y borran o alteran la información que contienen.

- **Virus de enlace o directorio**. Son programas malintencionados que sustituyen las direcciones de almacenamiento de los archivos de un programa, de modo que se los ejecute sin notarlo. Suelen tener extensiones .exe o .com y sus efectos pueden ser muy diversos.
- **Virus polimórficos**. Son programas maliciosos que cifran o alteran su código con cada copia o infección que realizan. Por esta razón, resulta muy difícil reconocerlos y erradicarlos.
- **Virus secuestradores (*hijackers*)**. Son programas que controlan los navegadores de internet, ya sea para dirigirlos a páginas web específicas y desencadenar secuencias de acciones (como descargas de otros archivos dañinos), o bien para impedir el acceso a otras páginas (como antivirus en línea).
- **Virus del teclado (*keyloggers*)**. Son programas maliciosos que registran cada una de las teclas que se presionan en el teclado de la computadora y comparten la información sensible con terceros que pueden sacar provecho de ello.
- **Virus de extorsión (*ransomware*)**. Son programas que amenazan con capturar información sensible del sistema, archivos valiosos y otras acciones similares, a menos que el usuario realice un pago a terceros.
- **Virus zombies**. Son programas que toman el control de la computadora y se lo entregan a un actor desconocido, quien puede no solo acceder a la información contenida en ella, sino también llevar a cabo operaciones en línea.
- **Virus FAT**. Son programas malintencionados que corrompen o confunden sectores críticos de la tabla de asignación de archivos (FAT, por sus siglas en inglés), impidiéndole al sistema operar de manera normal.

¿Cómo se propagan los virus informáticos?

Un virus informático no es más que un conjunto de instrucciones que, al ejecutarse en un sistema, se replican a sí mismas en varios de sus archivos y procesos, con el fin de alcanzar asimismo otros sistemas.

En décadas pasadas, los virus se transmitían de un sistema a otro exclusivamente a través de discos infectados, por lo que bastaba con una revisión mediante un software antivirus para detectarlos y a menudo eliminarlos. Hoy en día, el panorama es más complicado, debido a la cantidad de información que se maneja a través de internet.

Las maneras más usuales de contraer un virus informático son:

- Instalar software pirata o clandestino en la computadora.
- Ejecutar archivos descargados de internet o recibidos en correos electrónicos cuando se desconoce su función y proveniencia.
- Conceder permisos a portales de internet y programas de ejecución en línea sin saber qué son ni qué propósito tienen.
- Aceptar envíos de paquetes de software de terceros, especialmente si se trata de desconocidos.
- Visitar páginas web de contenido dudoso.
- Utilizar soportes físicos de información (como pendrives y discos duros portátiles) para recibir archivos provenientes de computadoras infectadas.

¿Cómo protegerse de los virus informáticos?

La mejor defensa contra los virus informáticos radica en la prevención, es decir, en **exponerse lo menos posible a las fuentes de infección**. A ello debe sumarse la utilización de un programa antivirus, que supervise las interacciones del sistema y lo proteja de la intrusión de virus, *malware* y *hackers*.

Por otro lado, es buena idea **realizar tareas de mantenimiento regular que minimicen el daño causado** por este tipo de programas nocivos. Por ejemplo, hacer copias frecuentes de seguridad, utilizar siempre software original, mantener actualizados los programas antivirus y disponer de los pormenores de la configuración del equipo, incluyendo sus parámetros técnicos, por si acaso hiciera falta restablecer el sistema a su configuración de fábrica.

Historia de los virus informáticos

Los orígenes de los virus informáticos **se remontan a mediados del siglo XX**, cuando la computación daba sus primeros pasos en firme. En 1949, el matemático húngaro-estadounidense John von Neumann (1903-1957) dictó una serie de conferencias en la Universidad de Illinois sobre lo que llamó "autómatas autorreplicantes", programas informáticos que podían copiarse a sí mismos de manera invasiva, es decir, virus informáticos.

En ese momento, **se inauguró un nuevo tema de estudio, conocido hoy en día como la "virología informática"**. Entre 1960 y 1972, hubo diferentes experiencias de producción de virus informáticos en laboratorios, con fines académicos. Uno de ellos fue "Creeper", una pieza de software que se transmitía por ARPANET (el precursor de internet) y que mostraba a los usuarios el mensaje "*I'm the creeper: catch me if you can*" (algo así como: "Soy el acechador: atrápame si puedes").

Diez años después, **apareció el primer virus informático no experimental**. "Elk Cloner", un virus de arranque programado por el informático Rich Skrenta (1967-), en ese entonces estudiante de secundaria, infectó millones de unidades de la serie Apple II de Macintosh. A raíz de este incidente, se creó en 1984 el término "virus informático" y se hizo patente la necesidad de contar con algún tipo de defensa en contra del software malicioso.

En 1986, apareció otro virus importante, "Brain", desarrollado como un castigo para los usuarios de IBM que usaran cierto software ilegal. Y en 1988 fue el turno del "gusano Morris", un virus que ocasionó varias caídas en los servidores de correo electrónico. Su desarrollador, Robert Tappan Morris (1965-), fue el primer procesado en Estados Unidos por la Ley de Fraude y Abuso Informático.

A partir de entonces, el software malintencionado no paró de proliferar y diversificarse en distintas familias de programas, y a la par lo hicieron las distintas empresas de software antivirus.