Virus Informáticos

Un virus informático es un programa o fragmento de código diseñado para provocar daños en un equipo corrompiendo archivos del sistema, despilfarrando recursos, destruyendo datos o alterando el funcionamiento normal de otra forma.

Los virus se diferencian de otros tipos de malware en que se replican automáticamente, es decir, son capaces de copiarse de un archivo o un PC a otro sin el consentimiento del usuario.

Virus, malware, troyanos... ¿cuál es la diferencia?

No todo el software que ataca un PC es un virus. Los virus informáticos son solo una de tantas clases de malware (**mal**icious soft**ware**, software malicioso). A continuación, describimos otras clases muy comunes también:

- **Troyanos**: igual que el viejo caballo de madera infestado de atacantes del que toma su nombre, este malware simula ser software legítimo inocuo o se introduce en él a fin de engañar al usuario para abrir la puerta a otros tipos de malware que infectan la PC.
- **Spyware**: este tipo de malware tiene el objeto de espiar a los usuarios, guardar sus contraseñas, datos de tarjetas de crédito, otros datos personales y patrones de comportamiento en línea para después enviarlo todo al artífice que lo programó.
- **Gusanos**: este tipo de malware ataca redes enteras de dispositivos saltando de un PC a otro.
- **Ransomware**: esta variedad de malware secuestra archivos (y, a veces, el disco rígido entero), los cifra y exige dinero a la víctima a cambio de una clave de descifrado (que puede funcionar o no, pero lo más probable es que no).
- **Adware**: este tipo de malware, increíblemente irritante, inunda las pantallas de las víctimas de anuncios no deseados y crea vulnerabilidades de seguridad para que otra clase de malware se pueda introducir subrepticiamente.

Resumiendo, los virus son tan solo uno de los varios tipos de malware que existen. En sentido estricto, los troyanos, el ransomware, etc., no son virus informáticos, aunque muchas personas utilizan el término «virus» para simplificar al referirse al malware en general.

¿Por qué la gente crea virus y cuál es su función?

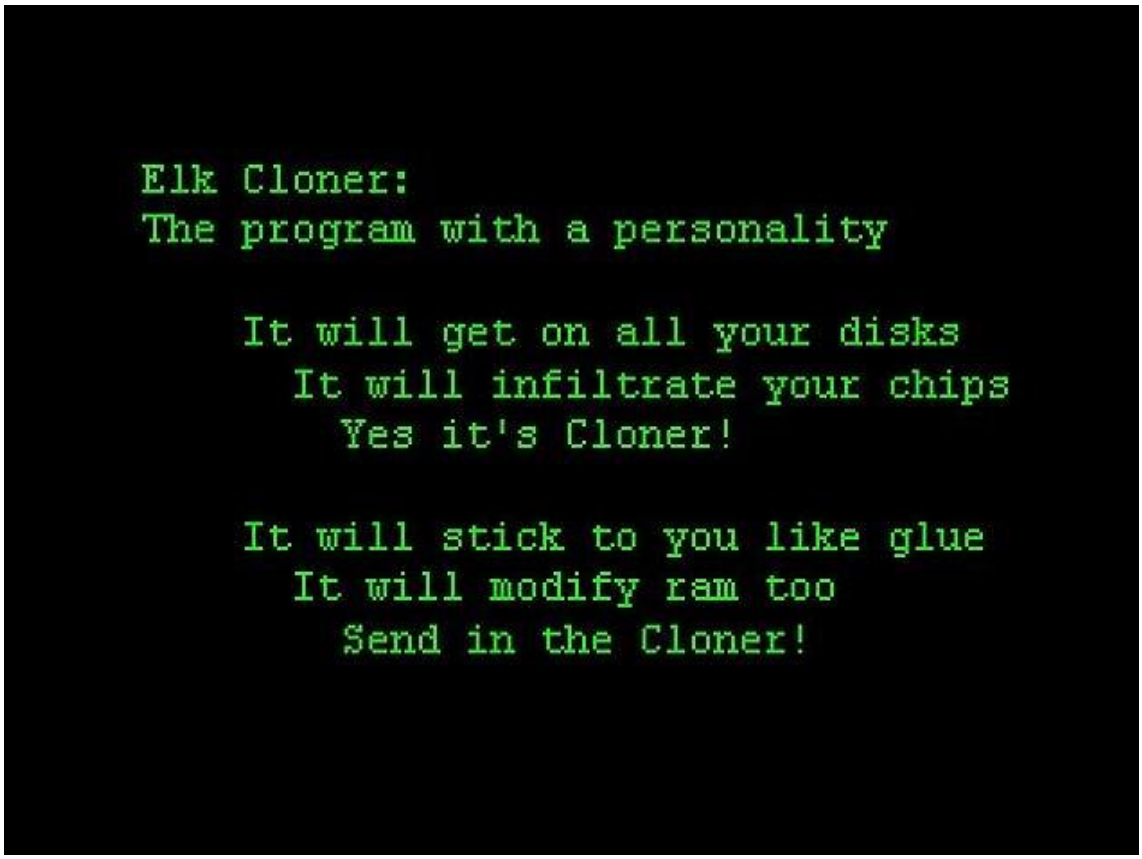
A diferencia de los biológicos, los virus informáticos no existen espontáneamente. Se fabrican, a menudo con mucho esmero, para atacar intencionadamente equipos, sistemas y redes.

¿Pero para qué se usan los virus?

Para divertirse

Bueno, «divertirse». Burlarse usando software, «pintar» grafitis de código informático… Los primeros virus informáticos fueron obra, fundamentalmente, de programadores con ganas de reírse un rato, como el que quizás fuera el primero: el **virus Creeper**. Creeper, que significa «enredadera» y data de 1971, mostraba el mensaje «I'm the creeper, catch me if you can!» (Soy la enredadera, ¡atrápame si puedes!).

O el **virus Elk Cloner**, que recitaba una pequeña poesía:



O el **virus Ika-tako**, que sustituía los archivos y programas por imágenes de calamares.

O el **virus Stoned**, que mostraba arbitrariamente el texto «Your computer is stoned. Legalize marihuana!» (Tu PC está fumado. ¡Que legalicen la marihuana!) en la pantalla (y se quedaba congelado sin hacer nada más).

Y mi favorito: el virus que finge ser un mensaje de una empresa conocida de software **que ofrece un soporte para tazas gratis** si lo descargas e instalas; al hacerlo, abre la bandeja de CD.

Para hacer el mal

Tristemente, no todos los virus son tan adorables. Hazle caso al mayordomo de Batman: algunas personas simplemente desean ver el mundo en llamas, y los virus informáticos son una forma muy efectiva de extender el caos por todos los rincones.

Es el caso del **virus ILOVEYOU**, que destruyó los archivos de más de 50 millones de internautas de todo el planeta, impidió el encendido de los PC y copió las

contraseñas de los usuarios para enviarlas a sus creadores. En total, el valor de los daños que ocasionó ascendió a 9000 millones de dólares en el año 2000.

Hasta esta cantidad palidece en comparación con los 37 000 millones de dólares en pérdidas que provocó el **virus Sobig.F**, el cual detuvo el tráfico informático en Washington DC e impidió despegar a Air Canada durante un tiempo.

También está el **virus Mydoom**, que causó tal congestión cibernética que se cree que llegó a ralentizar el tráfico digital en un 10 % el día de su aparición.

Para... ¿hacer el bien?

Sí, existe una minúscula proporción de virus informáticos que son «buenos», como el virus Cruncher, que comprime todos los archivos que infecta y, en teoría, trata de ayudar ahorrando un espacio en disco muy valioso.

También merece la pena hablar del virus denominado **Linux.Wifatch**, que parece no hacer otra cosa que impedir que otros virus lleguen al router. Linux.Wifatch es un virus en sí mismo —infecta un dispositivo sin el consentimiento del usuario y coordina sus acciones mediante una red entre pares (P2P)—, pero, en vez de hacerte daño, actúa como guarda de seguridad.

(Aun así, existen maneras mucho mejores de proteger el router, y hasta los creadores de Linux.Wifatch dicen que no confiemos en este «guarda»).

Otros virus «bienintencionados» tienen el propósito de actuar como una vacuna en el sentido de que obligan a personas, compañías y gobiernos a reforzar las medidas de seguridad para que sean capaces de rechazar las amenazas genuinas.

Algunos creadores de virus alegan que hacen del mundo un lugar más seguro sacando a la luz la deficiencias y los fallos de seguridad que otros virus con intenciones verdaderamente malignas pueden explotar.

«¿Qué puede salir mal?», se pregunta uno en los diez primeros minutos de toda película de desastres en la que se produce alguna pandemia. Lo cierto es que los virus aplastan rápidamente las defensas que se supone que deben poner a prueba. Fijémonos en el **virus Code Red**, que, como en las películas de grandes desastres, atacó a la Casa Blanca (bueno, en realidad fue al servidor web de la Casa Blanca, pero aun así...) y produjo unos daños valorados en 2600 millones de dólares en todo el mundo.

¿Cómo se propagan los virus informáticos?

A continuación, describimos algunos de los medios habituales que usan los virus informáticos para infectar a sus víctimas:

Virus de correo electrónico

El correo electrónico es uno de los medios favoritos para transmitir los virus informáticos a cualquier parte. Estos virus se pueden «contraer» por correo electrónico:

- **Abriendo archivos adjuntos**. Con nombres habitualmente inofensivos (como «Su itinerario de vuelo»), son tipos de archivos de programa ejecutables (.com, .exe, .zip, .dll, .pif, .vbs, .js o .scr) o archivos de macro (.doc, .dot, .xls, .xlt, xlsm, .xsltm…).
- **Abriendo un correo con un mensaje infectado.** Hoy en día, impulsados por la proliferación de gráficos enriquecidos, colores y ornamentos, algunos virus se transmiten en el cuerpo HTML del propio correo. Muchos servicios de correo electrónico desactivan el HTML de forma predeterminada hasta que el usuario confirma que confía en el remitente.

Virus de mensajería instantánea

Los virus también se distribuyen por medio de la mensajería instantánea (MI). **Skype, Facebook Messenger, Windows Live Messenger** y otros servicios de MI se utilizan inadvertidamente para propagar virus a los contactos a través de vínculos infectados que se reciben en mensajes de chat.

Estos virus de mensajería instantánea y redes sociales se extienden rápidamente por todas partes porque es mucho más fácil conseguir que alguien haga clic en un vínculo incluido en un mensaje procedente de una persona en la que confía que en otro incluido en un correo que envía un desconocido.

Virus de intercambio de archivos

Los servicios que se usan para compartir archivos entre pares, como **Dropbox, SharePoint o ShareFile**, también se pueden utilizar para propagar virus. Estos servicios sincronizan archivos y carpetas con cualquier equipo asociado a una cuenta determinada, de modo que cuando alguien (involuntariamente o por cualquier otra causa) carga un archivo que contiene un virus en una cuenta de intercambio de archivos, dicho virus se descarga en el equipo de todos los usuarios que tengan acceso a esa carpeta compartida.

Algunos servicios de intercambio de archivos, como **Google Drive**, analizan los archivos cargados en busca de virus (aunque esto solo lo hace con los que pesan menos de 25 MB, lo que deja vía libre a los que propagan virus, que lo único que han de hacer es asegurarse de que los archivos infectados sean de un tamaño superior).

No obstante, casi todos los demás servicios no buscan virus en ningún archivo, así que es responsabilidad tuya garantizar tu protección contra las amenazas potenciales contenidas en el archivo que las otras personas vayan a descargar.

Virus de descarga de software

Las infecciones de antivirus falsos son uno de los tipos más comunes de descargas de software que llevan virus. Los estafadores y ciberdelincuentes recurren a ventanas emergentes y anuncios con mensajes intimidatorios a fin de hacer creer a los usuarios que se ha detectado un virus inexistente en la PC, y los conminan a descargar su software «antivirus» para neutralizar la amenaza.

En lugar de quitarle los virus al equipo, este antivirus falso infecta la PC con malware, lo cual, muchas veces, tiene consecuencias devastadoras para los archivos, el disco rígido y la información personal de la víctima.

Software sin parchear vulnerable

Por último, uno de los medios más comunes (y que más a menudo se pasa por alto) de propagación de virus es el software sin parchear.

Se trata de programas y aplicaciones en los que no se han instalado las últimas actualizaciones de seguridad proporcionadas por el desarrollador con el objeto de tapar brechas de seguridad en el propio software.

El software sin parchear es motivo de grandes quebraderos de cabeza en lo que atañe a la ciberseguridad para negocios y organizaciones, pero dado que los delincuentes explotan vulnerabilidades en versiones desactualizadas de programas tan populares como **Adobe Reader, Java, Microsoft Windows** o **Microsoft Office**, los ciudadanos de a pie también corremos mucho riesgo de infección.

Tipos de virus informáticos

Aquí tenés la lista de los diversos tipos de virus informáticos que existen actualmente:

Virus de sector de arranque

El sector de arranque es la parte del disco rígido dla PC que carga el sistema operativo del equipo, por ejemplo, Microsoft Windows. Un virus de sector de arranque infecta el registro de arranque principal (MBR, por su sigla en inglés), es decir, que el virus se carga en la memoria del equipo durante el encendido.

Este tipo de virus solía propagarse, principalmente, a través de dispositivos conectables, como memorias USB, disquetes y CD-ROM. Con la evolución de la tecnología, los virus de sector de arranque son cada vez más infrecuentes y, en la actualidad, se distribuyen sobre todo como archivos adjuntos de correo.

Ejemplos de virus de sector de arranque:

- **Elk Cloner:** este virus de principios de los 80 se incorporó a un juego. Cuando se iniciaba el juego por 50 vez, el virus mostraba un poema en la pantalla.
- **Stoned:** la variedad inicial mostraba mensajes en pantalla a favor de la legalización de la marihuana. Su firma (que no el virus en sí) consiguió introducirse sigilosamente en la cadena de bloques de Bitcoin en 2014.
- **Parity Boot:** este, que es otro virus «vintage», fue el más prevalente en Alemania hasta 1996.
- **Brain:** considerado el primer virus informático para MS-DOS, lo crearon los hermanos pakistaníes Alvi en un intento por proteger su software médico de la infracción de derechos de autor. Un intento que, muy a su pesar, se les escapó de las manos rápidamente.
- **Michelangelo:** cada año, el 6 de marzo (día de nacimiento del artista Miguel Ángel) este virus cobraba vida y sobrescribía los 100 primeros sectores de un disco rígido con valores nulos, lo cual impedía que los usuarios habituales pudieran recuperar sus archivos.

Virus de acción directa

Estos virus están pensados para franquear equipos: se introducen, normalmente se propagan en archivos de un tipo concreto (suelen ser de extensión .com o .exe) y, cuando acaban, se borran automáticamente. Son el tipo más habitual de virus que existe y el más sencillo de crear, por lo que también es el más fácil de eliminar.

Ejemplos de virus de acción directa:

- **Win64.Rugrat:** este ejemplo temprano de virus de acción directa, también conocido como virus Rugrat, podía infectar todos los archivos ejecutables de 64 bits que hubiera en el directorio y los subdirectorios en que se ejecutara.
- **Virus Vienna:** este virus ostenta la distinción de ser el primero que un antivirus derrotó. Busca archivos .com y destruye algunos al intentar infectarlos.

Virus residentes

A diferencia de los virus de acción directa descritos arriba, los virus residentes en memoria «acampan» en la memoria principal del equipo (RAM). Esto es muy malo, ya que pueden seguir funcionando incluso después de habernos deshecho del propagador original de la infección. Algunos actúan rápido, mientras que otros son de acción lenta y, por ello, más difíciles de detectar.

Ejemplos de virus residentes en memoria:

- **Virus Jerusalem (o Friday 13th, viernes 13):** después de lograr alcanzar la RAM y ocultarse en su interior, este virus eliminaba los programas del equipo los viernes 13 o aumentaba el tamaño de aquellos infectados hasta que eran demasiado grandes para ejecutarse.
- **Virus OneHalf:** este virus, también conocido como Freelove o Slovak Bomber, avanza lentamente por el disco rígido cifrando el contenido a su paso. Cuando va por la mitad (así como los días 4, 8, 10, 14, 18, 20, 24, 28 y 30 de cada mes), muestra el mensaje «Dis is one half. Press any key to continue…» (He llegado a la mitad. Pulsa cualquier tecla para continuar...).
- **Virus Magistr:** este virus tan destructivo se envía automáticamente por correo electrónico a tu lista de contactos, elimina archivos de forma alterna, se carga el CMOS y el BIOS, y termina dejándote mensajes insultantes para arrancar.

Virus multipartitos

Estos ultraversátiles virus duplican su capacidad de propagación infectando tanto los archivos como el espacio de arranque. De ese modo, incluso después de haber eliminado dla PC todos los archivos infectados satisfactoriamente, el virus aún permanece oculto en el sector de arranque, listo para atacar de nuevo. Y si limpias el sector de arranque, el virus lo vuelve a infectar saltando desde uno de los archivos infectados.

Ejemplos de virus multipartitos:

- **Virus Junkie:** este virus multipartito se transmitía en un archivo llamado HV-PSPTC.ZIP, supuestamente el juego de ordenador Pacific Strike. Pero no era tal.

- **Virus Tequila:** este evita los archivos que contienen las letras «v» y «sc» en el nombre, y muestra el mensaje «BEER and TEQUILA forever!» (¡Cerveza y tequila por siempre!).

- **Virus Invader:** este empieza bien reproduciendo una obra de Mozart, pero, al pulsar Ctrl+Alt+Supr para reiniciar, sobrescribe la primera línea del disco rígido con una copia del virus.

Virus polimórficos

Estos, los mutantes del mundo de los virus informáticos, cambian de forma con el propósito de evitar ser detectados sin perder sus capacidades de ataque básicas. Después de infectar los archivos, estos virus se replican automáticamente de una forma algo distinta, lo cual hace que sea muy difícil detectarlos y eliminarlos del todo.

Ejemplos de virus polimórficos:

- **Virus Satanbug:** a pesar de tener un nombre un tanto diabólico, este virus polimórfico no perjudica directamente a los archivos, pero a los analizadores de virus no les resulta tan fácil quitarlo dla PC, ya que tiene hasta nueve niveles de cifrado.
- **Virus VirLock:** mitad ransomware, mitad virus polimórfico, el virus Win32/VirLock cifra los archivos y pide un rescate, pero también cambia de aspecto cada vez que se propaga.

Virus de macro

Algunos virus se escriben en el lenguaje de las macros con la intención de insertarlos dentro de software que permita miniprogramas con macros, como Microsoft Word. Eso significa que la PC se puede infectar con virus contenidos en documentos de Word.

Ejemplos de virus de macro:

- **Melissa:** distribuido a través de archivos adjuntos de correo, cuando este virus infecta la PC, se abre camino hasta el cliente de correo Microsoft Outlook y se envía automáticamente a los 50 primeros contactos de la libreta de direcciones, algo que puede llegar a ralentizar o incluso desactivar por completo los servidores en una terrible reacción en cadena.