¿Qué es un virus informático?

Piensa en lo que te sucede cuando tienes la gripe: sales de casa sin abrigarte, te subes a un tren abarrotado de gente infectada o le das un lametón al pomo equivocado y ¡zas!

De repente, tus ojos están inyectados en sangre, sientes como si te estuvieran abrasando vivo y estás hecho un guiñapo.

Los virus informáticos actúan igual. Si tienes la mala suerte de pillar uno (tampoco te tortures si te pasa, porque son sumamente comunes), estate preparado, ya que causará estragos en el disco duro: reducción del rendimiento del PC, corrupción o destrucción de archivos y muchas otras cosas.

Una definición de «virus informático» al estilo de la Wikipedia

¿Buscas una definición sencilla? Aquí tienes:

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.

En definitiva, son altamente contagiosos.

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 (malicious software, 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 el PC.

Spyware: con ejemplos como los registradores de pulsaciones, 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 duro 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 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 del PC (¿te acuerdas de esa bandeja?).

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.

Menuda vacuna.

¿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 el 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 el PC con malware, lo cual, muchas veces, tiene consecuencias devastadoras para los archivos, el disco duro 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.

Usa tu linda cabecita: Cómo prevenir posibles infecciones

Aparte de contar con un antivirus que detecte y elimine los virus, te estarás haciendo un gran favor si sigues unas normas adecuadas de higiene digital y aplicas los siguientes consejos básicos sobre seguridad en Internet:

No hagas clic en todos los vínculos que te envíen tus amigos en las redes sociales, y mucho menos si el mensaje es solo un vínculo sin contexto o si no parece haber sido escrito por ellos. Las cuentas de Facebook de los internautas se piratean y se utilizan para propagar virus y malware. Cuando tengas dudas, escribe directamente al amigo en cuestión y pregúntale si es él quien te ha enviado el vínculo. Con frecuencia, la respuesta es «¡¿Qué?! ¡No!».

No abras ningún archivo adjunto de correo si no estás seguro al 100 % de lo que es. Los ciberdelincuentes suelen sacar provecho de tu curiosidad natural para propagar virus: te dicen que has ganado algo, pero no has participado en ningún concurso; o te envían un «itinerario de vuelo», pero no tienes pensando irte de viaje a ningún sitio. Al final abres el archivo adjunto para ver de qué se trata y, hala, ya estás infectado. Así que no lo hagas.

No caigas en la trampa de mensajes como «¡Su PC está infectado!» y otras ventanas alarmantes de este tipo que aparezcan de repente y no procedan directamente de tu antivirus. Existen muchas posibilidades de que se trate de un señuelo para que descargues un antivirus falso y robarte dinero, infectar el equipo con malware o ambas opciones. Cuando nuestro antivirus atrapa algo, te avisamos de la buena acción con mensajes discretos, ya está. No te pedimos que descargues nada más ni que pagues dinero.

No actives las macros en Microsoft Office. Hace unos años, te habría aconsejado que desactivaras las macros, pero Microsoft ya lo hace de forma predeterminada. Esto quiere decir que los ciberdelincuentes intentan engañarte para que las actives con todo tipo de tejemanejes y advertencias falsas cuando recibes un correo electrónico infectado. No caigas en la trampa.

Pero, en serio, ponte un antivirus ya.

Fuente: https://www.avg.com/es/signal/what-is-a-computer-virus