Virus informáticos

Los virus informáticos son tan antiguos como las computadoras personales. Desde inicios de los ochenta, estas amenazas empezaron a invadir los equipos de cómputo, se propagaron y crearon problemas hasta convertirse en verdaderos dolores de cabeza para los usuarios. Al principio, simplemente enviaban mensajes en pantalla o consumían recursos del sistema; sin embargo, el grado de sofisticación y daño que pueden generar en la actualidad ha llamado profundamente la atención de empresas especializadas que dedican gran parte de sus esfuerzos en detectar, controlar y eliminar este *malware*.

En su definición más simple, un virus informático es un programa que tiene la característica de crear copias de sí mismo, pero siempre dependiendo de un archivo (*host program*) para poder ejercer su acción viral; aunque los programas que se autorreplican ya existían décadas atrás (en 1959 el matemático Leonel S. Penrose publica el artículo "Self Reproducing machines", donde describe programas capaces de activarse, autorreproducirse y hacer cambios de sí mismos), no es sino hasta 1983 cuando el término "virus" es propuesto por el ingeniero Fred Cohen. Su estrategia de propagación es similar a la de un virus biológico, es decir, el código viral requiere insertarse sobre el contenido de un archivo que al ejecutarse también activa dicho código, y aunque estrictamente hablando un virus es inocuo en un archivo de datos, cuando es abierto por un editor o *software* de aplicación podría ejecutar una secuencia de instrucciones implícitas en él que activen su acción viral.

Cabe señalar que desde hace algunos años la creación de virus fue disminuyendo, lo que dio lugar a los gusanos (*worms*), programas que crean copias de sí mismos (por eso también suelen llamarlos virus), pero sin depender de archivos para poder ejecutarse, lo que los hace todavía más complejos y peligrosos. Generalmente se propagan a través de la red (*Internet worms*), el correo electrónico (*email worms*) o ambos (*multivector worms*), generando efectos dañinos en clientes, servidores o ancho de banda.

Existe una lista interminable de problemas que los virus son capaces de provocar, por ejemplo, deteriorar, destruir o eliminar archivos de datos o incluso bases de datos, borrar y modificar archivos ejecutables, bloquear el arranque del sistema operativo, saturar la memoria principal con datos inservibles, consumir espacio del disco duro, alterar el funcionamiento del *software* de aplicación, crear tráfico inútil en la red, robar información confidencial, en incluso controlar y dañar *hardware*.

Las principales sospechas de la existencia de un virus en nuestros equipos son por lo general lentitud repentina y exagerada en la ejecución de programas de aplicación o al iniciar la carga del sistema operativo (encender la computadora), bloqueo constante del equipo, problemas para acceder a las unidades de almacenamiento (disco duro, memorias *flash*), impresión anormalmente errática o imposibilidad de imprimir documentos, identificación de nombres de archivo con caracteres especiales (secuencias de números o signos: $, &, /, *, !) muy largos, localización de archivos con tamaños exageradamente grandes o despliegue de mensajes poco usuales.

Así pues, para evitar contaminarse de algún virus informático es fundamental seguir las siguientes recomendaciones:

Instalar y actualizar el antivirus. Existe en el mercado una gran variedad de programas dedicados al monitoreo, la detección y la eliminación de virus informáticos. Empresas como Symantec, Kaspersky, Panda, McAfee, Avira o Sophos son solo algunos ejemplos; sin embargo, la variedad de sistemas antivirus es mucho mayor. Casi todos extienden su detección no solo a la presencia de virus, sino también al malware en general (*spam*, *spyware*, *adware*, etc.), de los cuales unos son más efectivos que otros. Además de instalar el antivirus, es indispensable mantenerlo actualizado. Kaspersky asegura detectar más de 315 00 archivos maliciosos cada día, y si en nuestros equipos omitimos actualizarlo, en poco tiempo tendremos una computadora vulnerable o infectada.

Mantener actualizado el sistema operativo. Muchos usuarios desactivan indebidamente las actualizaciones automáticas del sistema operativo sin pensar que estas pueden resolver problemas de vulnerabilidad o instalar parches que eviten conflictos futuros, ya sea con el *software* de aplicación o con los mismos antivirus.

Verificar que los dispositivos externos, como discos duros o memorias *flash*, no contengan código malicioso. Siempre que se conecte un dispositivo de almacenamiento (incluso teléfonos celulares o cámaras fotográficas) es necesario someterlo a una revisión a través de un antivirus. Esto evitará que el malware se transfiera del dispositivo al disco duro de la computadora y ejerza su acción expansiva.

Ser muy cuidadoso e intuitivo al revisar el correo electrónico. Aunque sigue vigente la recomendación de no abrir correos electrónicos de usuarios desconocidos, algunos correos infectados llegan de usuarios claramente identificados. En tales casos, la intuición permitirá saber si fue el remitente original quien envió el mensaje o es producto de un *malware*. La descripción del asunto, el contenido del mensaje o el idioma en que fue escrito son señales importantes para esta verificación.

Los virus informáticos pueden causarnos verdaderos dolores de cabeza; sin embargo, si

se toman en cuenta las medidas de seguridad adecuadas, esta amenaza, aunque latente, reducirá el riesgo de contagio y la consecuente pérdida de tiempo e información.

REFERENCIAS

- Chien, E. (2002). *Blended attacks exploits, vulnerabilities and buffer-overflow techniques in computer viruses*, Symantec. Tomado de http://www.symantec.com/avcenter/reference/blended.attacks.pdf
- Kaspersky (2013). Number of the year. Tomado de http://www.kaspersky.com/about/news/virus/2013/number-of-the-year
- Mell, P. (2005). *Guide to malware incident prevention and handling*, National Institute of Standards and Technology. Tomado de http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf
- Nachenberg, C. (2000). *The Evolving Virus Threat*, Symantec Corporation. Tomado de http://csrc.nist.gov/nissc/2000/proceedings/papers/019.pdf
- Souppaya, M. (2013). *Guide to malware incident prevention and handling for desktops and laptops*, National Institute of Standards and Technology. Tomado de http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf.

Dónde encontrar más información:

- https://www.us-cert.gov/publications/virus-basics.
- http://www.symantec.com/avcenter/reference/worm.vs.virus.pdf.
- http://www.symantec.com/avcenter/reference/striker.pdf.
- http://www.symantec.com/avcenter/reference/virus.and.vulnerability.pdf.
- http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.
- https://www.cs.columbia.edu/~smb/classes/f07/l19.pdf.
- http://www.history.navy.mil/library/online/computerattack.htm.
- http://www.emis.de/journals/IJOPCM/files/IJOPCM(vol.1.2.3.S.08).pdf.
- http://www.cs.toronto.edu/~gdahl/papers/malwareRandomProjections_icassp2013.pdf.
- http://usa.kaspersky.com/internet-security-center/threats/malware-classifications#.VDR0ORZ0wdU.
- http://www.sans.org/reading-room/whitepapers/incident/malware-101-viruses-32848.
- http://www.pcadvisor.co.uk/test-centre/security/3263332/best-antivirus-for-pc-laptop/.