

# Malware independiente del sistema operativo



Con excesiva frecuencia se habla de las desventajas del sistema operativo Windows, ya que tiene demasiados fallos de seguridad, que no se parchea adecuadamente, que no está orientado a la seguridad... hasta que el famoso Vista llegue por fin a los discos duros de los ordenadores, tendremos todavía mucho tiempo para protestar.

Sin embargo, la nueva dinámica empleada por el malware está empezando a hacerse independiente de los sistemas operativos de los ordenadores. Ya no importa si el usuario es doméstico o trabaja en una empresa, da igual que el administrador del sistema sea un vecino o el responsable de IT con varias carreras a sus espaldas.

Si hace unos cuantos años los códigos maliciosos estaban pensados para multiplicarse y llevar a cabo determinadas acciones (generalmente dañinas) en los ordenadores, hoy en día esa vía prácticamente ha desaparecido. Se busca el dinero de los usuarios, y para eso no hace falta ser un programador experto, basta con tener la malicia necesaria para engañar a los usuarios.

Hagamos un pequeño repaso a determinadas acciones que se han puesto en marcha para engañar a los usuarios. Veremos que ninguna de ellas depende en ninguna forma del sistema operativo utilizado, no del navegador, ni del lector de correo. Depende, única y exclusivamente, del usuario.

Si empezamos con los clásicos, no podemos olvidar a los famosos timos llamados "419". En estos timos un supuesto descendiente de un empresario, o presidente o general de un país africano dispone de una sustanciosa cantidad de dinero que, carambolas de la vida, está bloqueada en un banco y necesita de nuestra colaboración para poder hacerla en efectivo. El usuario que acepte entrar en este "juego" se verá inmerso en una sucesión de pagos de comisiones hasta que se aburra o se arruine.

Con menos solera que el "419" pero con igual frecuencia nos encontramos con los mensajes de estupendos premios de lotería. Un mensaje que aparentemente llega de una famosa lotería (o sin ser famosa, pero con visos de serlo), nos informa de que somos los ganadores de una elevada cantidad de dinero: generalmente, cientos de miles o millones de euros. Para recibir el premio, basta con llamar al agente de la lotería anunciado en el mensaje que nos hará llegar el premio. Eso sí, tras el pago de varias comisiones, como en el caso del "419", hasta que el usuario se da cuenta de que le están estafando.

¿Quién no ha recibido un mensaje de correo electrónico en el que le anuncian una mejora en el crédito que se está pagando por la casa? Estos mensajes no suelen ser ciertos (aunque quizá hay alguna empresa crediticia que sí ofrezca sus servicios mediante spam), el trasfondo económico reside en el número de teléfono que aparece en el mensaje. Existen micro-compañías de teléfonos que, por virtud de los acuerdos telefónicos con grandes operadores, pueden llegar a ganar mucho dinero con las llamadas que efectúan a esos números, además de los números con tarifas especiales.

# Malware independiente del sistema operativo



También podemos considerar ya clásico el phishing. Mensajes de correo electrónico que simulan ser enviados por una entidad bancaria solicitándonos confirmación de las claves de acceso a la banca electrónica, o los datos de nuestra tarjeta de crédito. Estos mensajes son cada vez más peligrosos, ya que si bien antes se simulaban páginas web falsas que tarde o temprano las empresas que los alojaban o los proveedores se encargaban de cerrar, en ocasiones se han encontrado mensajes HTML que incluyen los campos para rellenar con los datos del usuario, que son enviados directamente por correo electrónico al malhechor.

Estos mensajes de phishing no solo aparentan provenir de bancos, sino que en numerosas ocasiones se aprovechan de otros servicios relacionados con el dinero, como puede ser PayPal, o e-Bay. El procedimiento es siempre el mismo: un mensaje en el que se piden los datos “o se cancelarán las cuentas”.

Sin embargo, el sistema del phishing está empezando a ser demasiado conocido, y los “cibertimadores” ven que su mercado potencial disminuye drásticamente. Por ello han optado por otras técnicas más sutiles que el simple mensaje. Se están empezando a detectar mensajes en los que un supuesto comprador de un elemento en e-Bay protesta porque ya ha pagado por un objeto que no ha recibido. Si el usuario cae en la trampa, tiene la opción de contestar a este cliente descontento, pero para ello deberá introducir sus datos de usuario e-Bay, que automáticamente pasarán a manos del estafador.

Estos timos, sin embargo, necesitan de una pieza clave: la persona que se encarga de hacer de intermediario para recibir el dinero de los incautos. Para ello, nada mejor que un mensaje de correo electrónico anunciando un maravilloso empleo en el que basta con tener una cuenta bancaria para recibir dinero que luego hay que transferir a otra cuenta. Simple y sencillo. Pero esas transferencias recibidas no son más que los pagos que están haciendo los timados que hemos mencionado antes, y las transferencias emitidas lo son a las cuentas de los timadores. Al igual que las personas que intentan introducir drogas por las fronteras, se les conoce como “muleros”.

Todo esto está claro que son robos, timos, estafas, o como se le quiera llamar. Engañan a los usuarios y directamente le roban los datos o el dinero. Pero la sutileza está llegando a límites más altos. Se trata de mensajes en los que se sugiere comprar determinados valores bursátiles, ya que van a experimentar una subida próxima.

En este caso, no hay ninguna estafa. No hay un robo. Simplemente, la inocencia de los usuarios. El generador de estos mensajes sabe que no hay ninguna razón para que estas acciones suban en el mercado, simplemente busca un incremento artificial del valor de las acciones para poder vender las suyas.

Afortunadamente las empresas que se ven involucradas en estos mensajes nunca llegan a tener espectaculares alzas en el mercado, pero sí que podemos observar que el volumen negociado en estas compañías crece en unos días. Aunque el

# Malware independiente del sistema operativo



emisor del mensaje no consiga una elevada ganancia, sí que consigue deshacerse de unas acciones que por alguna razón le molestaban en su cartera de valores.

Y llegados a este punto, ¿cuáles de estos timos dependen de usar un sistema operativo u otro? Cualquier lector de correo electrónico nos mostrará el mensaje sin problema. No dependerá de si es Windows con la última actualización, ni de si el Linux está mejor o pero configurado. Dependerá única y exclusivamente del usuario que haga doble clic en el mensaje, de su credulidad y de su permisividad al engaño.

Si lo que realmente queremos es que los usuarios de una red corporativa estén protegidos contra las últimas amenazas, la solución no está en el sistema operativo ni en las actualizaciones de seguridad. La protección recae, por un lado, en la formación que reciba el usuario, y por otro, en los sistemas de protección instalados. Los sistemas de protección, tanto perimetral como en estaciones y servidores, tanto para Windows como para Linux, deben establecer una barrera auténtica para este tipo de timos y amenazas. No basta con confiar en el sistema operativo y en los usuarios. Uno poco va a hacer, y el otro, es muy probable que falle.

La clásica solución en sistemas tipo Linux, la asignación de distintos privilegios de manera que no se puedan ejecutar programas malignos en sistemas no autorizados puede suponer una pequeña limitación para todos estos tipos de engaños. El problema no está en un código ejecutable, sino en información engañosa al usuario.

La solución pasa, como siempre, por recurrir a las herramientas de seguridad, las suites que permiten tener en una sola aplicación todos los complementos necesarios para proteger a los usuarios. Desde el clásico antivirus hasta el firewall o la protección del correo electrónico, tanto para Windows como para Linux evitaremos que aunque el sistema sea seguro, los usuarios no lo sean.

**Fernando de la Cuadra**  
**Editor Técnico Internacional**  
Panda Software (<http://www.pandasoftware.com>)  
E-mail: [Fdelacuadra@pandasoftware.com](mailto:Fdelacuadra@pandasoftware.com)