VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Diciembre 2014

Boletín mensual de seguridad para usuarios de computadoras

OUCH!

En esta edición...

¿Qué es un antivirus?

Resumen

Un antivirus es un programa de seguridad que se instala en la computadora o dispositivo móvil para protegerlo de infecciones por malware. El término “malware” es una frase utilizada para cualquier tipo de software malintencionado, como virus, gusanos, troyanos o spyware. De hecho, el término malware proviene de la combinación de las palabras malicioso y software. Si el equipo ha sido infectado por malware, un atacante cibernético puede capturar todas las pulsaciones de teclas, robar tus documentos o utilizar tu computadora para atacar a otros. Contrariamente a lo que algunas personas creen, cualquier sistema operativo, incluyendo Mac OS X y Linux, puede ser infectado.

Editor Invitado

Jake Williams es fundador de Rendition Infosec (**www.renditioninfosec.com**) y es instructor y autor certificado de cursos del SANS. Su cuenta de Twitter es **@MalwareJake** y escribe en su blog **malwarejake.blogspot.com**.

Puedes comprar el software antivirus como una solución independiente aunque a menudo se incluye como parte de un paquete de seguridad. El problema es que el antivirus ya no puede seguir el ritmo de los atacantes cibernéticos, quienes constantemente desarrollan y liberan nuevos tipos de malware. Hay tantas nuevas versiones cada día, que no hay un solo programa antivirus que pueda detectarlos y protegerte contra todos ellos. Es por esto que es importante que entiendas que mientras el antivirus te ayudará a proteger tu equipo, no puede detectar o detener todo tipo de malware. Para entender mejor por qué, vamos a ver cómo trabajan algunos de estos programas.

Cómo funciona un antivirus

A grandes rasgos, hay dos formas de que un software antivirus identifique el malware: detección de firmas y detección de comportamiento. La detección por firma funciona como el sistema inmune humano. Se analiza el equipo en busca de características o “firmas” de programas maliciosos identificables. Para ello hace uso de un diccionario de malware conocido, si hay algo en la computadora que coincide con un patrón en el diccionario, el programa intenta neutralizarlo. Al igual que el sistema inmunológico humano, el enfoque del diccionario requiere actualizaciones (como vacunas contra la gripe) para proteger contra las nuevas cepas de malware. Un antivirus sólo puede proteger contra lo que reconoce como nocivo. El problema con los atacantes cibernéticos es que están desarrollando nuevo malware tan rápido, que los desarrolladores de antivirus no pueden mantener el ritmo. Como resultado, no importa qué tan actualizados estén sus antivirus, siempre hay alguna nueva variante de malware que potencialmente puede pasar por alto su software.

¿Qué es un antivirus?

Con la detección de comportamiento, el antivirus no trata de identificar malware conocido pero monitorea el comportamiento de software instalado en tu computadora. Cuando un programa actúa sospechosamente, como tratando de acceder a un archivo protegido o modificar otro programa, el software antivirus basado en comportamiento hace notar la actividad sospechosa y te advierte de ello. Este enfoque proporciona protección contra nuevos tipos de malware que aún no existen en los diccionarios. El problema con este enfoque es que puede generar falsas advertencias. Tú como usuario puedes sentirte inseguro sobre lo que debes permitir o no permitir y con el tiempo, llegar a ser insensibles a todas esas advertencias. Puedes tener la tentación de hacer clic en "Aceptar" en cada aviso, dejando tu computadora abierta a un ataque o una infección. Además, en el momento en que se detecta el comportamiento, el malware probablemente ya se ejecutó en tu máquina y podrías ignorar qué acciones tomó antes de que el software antivirus lo identificara.

Aunque el antivirus es parte importante de tu seguridad, no le es posible detectar o detener todos los ataques. En última instancia, tú es la mejor defensa, no sólo la tecnología.

El antivirus es una parte importante para la seguridad de tu equipo y de los dispositivos móviles, siempre que sea posible, se recomienda instalarlo y utilizarlo constantemente. Sin embargo, el punto clave a recordar es que, independientemente de cómo funciona tu antivirus, probablemente nunca te protegerá de todo tipo de malware. En última instancia, tú y no sólo la tecnología, eres la mejor defensa contra los atacantes cibernéticos de hoy en día.

Consejos sobre antivirus

1. Obtén el software antivirus sólo de fuentes conocidas y de proveedores de confianza. Es una táctica común de los atacantes cibernéticos distribuir programas antivirus falsos que en realidad son malware.
2. Asegúrate de tener la última versión de tu software antivirus instalado, paga la suscripción anual para activarla y revisa que tu antivirus está configurado para actualizarse automáticamente. Si el equipo ha sido desconectado o apagado por un tiempo, tu software antivirus tendrá que actualizarse a sí mismo cuando lo enciendas de nuevo o cuando vuelvas a conectarte a Internet. No pospongas estos cambios.
3. Asegúrate de que tu antivirus escanea automáticamente los medios de comunicación portátiles (tales como memorias USB) y asegúrate de que la protección en tiempo real esté activada.
4. Presta atención a las advertencias que aparecen en pantalla y a las alertas generadas por el software antivirus. La mayoría de las alertas incluyen la opción de obtener más información o una recomendación sobre qué hacer a continuación. Si recibes una alerta en un equipo de trabajo, asegúrate de ponerte en contacto con la persona adecuada para que te apoye (soporte técnico).

¿Qué es un antivirus?

5. No desactives o desinstales tu software antivirus por creer que se está ralentizando tu computadora, que está bloqueando un sitio web o que te impide instalar una aplicación o programa. Hacerlo te expondrá a un riesgo innecesario y podría dar lugar a un incidente de seguridad grave. Si persisten los problemas en tu equipo para el trabajo, ponte en contacto con el servicio de soporte técnico. Si los problemas persisten en tu computadora personal, trata de ponerte en contacto con el proveedor del antivirus, visita su sitio web para obtener más información o la sustitución de tu antivirus por otro producto.
6. No instales varios programas antivirus en el ordenador al mismo tiempo. Si lo haces, lo más probable es que ambos programas entren en conflicto uno con otro, esto provocaría la reducción de la seguridad.
7. Aprende a reconocer las señales de advertencia que tu software antivirus produce. Atacantes cibernéticos pueden crear sitios web maliciosos que publican avisos de antivirus falsos muy realistas que ofrecen “arreglar” tu computadora. Al hacer clic en estos enlaces o botones, realmente podrías dañar tu equipo.

Conoce más

Suscríbete al boletín mensual de conciencia sobre seguridad OUCH!, consulta los archivos OUCH! y aprende más acerca de las soluciones de seguridad SANS visitando: http://www.securingthehuman.org

Versión en español

UNAM-CERT, Equipo de Respuesta a Incidentes de Seguridad de la Información en México reconocido ante FIRST, es una referencia en la materia en este país.
Sitio web: http://www.seguridad.unam.mx
Síguelo en Twitter @unamcert

Recursos

Comparación de productos antivirus:	http://www.av-test.org/es/
Ingeniería social:	http://www.securingthehuman.org/ouch/2014#november2014
Ataques de phishing:	http://www.securingthehuman.org/ouch/2013#february2013
Me hackearon ¿Ahora?:	http://www.securingthehuman.org/ouch/2014#may2014

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traducción al español por: Jazmín López

