

MALWARE: una docena de programas maliciosos

Por Joel Walsh* © 2005

Parece que tan pronto como se siente seguro prendiendo su computadora oye en las noticias acerca de una nueva clase de amenaza de la seguridad en Internet. Generalmente, la amenaza de la seguridad es alguna clase de malware (aunque, sin duda, el término "amenaza de la seguridad" ayuda a vender más periódicos).

¿Qué es malware? Malware es exactamente lo que su nombre indica: mal (significa malo, en sentido de maligno o malicioso antes que sólo pobremente hecho) + ware (de software). Más específicamente, malware es software que no da ningún beneficio al dueño de la computadora, e incluso puede dañarlo, así que es únicamente un parásito.

LAS DIFERENTES CARAS DEL MALWARE

Según Wikipedia, hay de hecho once diferentes tipos de malware, y aún más subtipos de cada uno.

1. Virus. El malware que más aparece en las noticias, incluso su abuela sabe lo que es. Usted probablemente ya ha oído abundantemente acerca de por qué esta clase de software es malo para usted, así que no hay necesidad de insistir con este punto.

2. Gusanos. Una leve variación del virus. La diferencia entre virus y gusanos es que los virus se esconden dentro de los archivos de los programas verdaderos (por ejemplo, los macros en Word o el VBScript en muchas otras aplicaciones de Microsoft), mientras que los gusanos no infectan un archivo o programa, sino que son programas en sí mismo.

3. Wabbits. Sea honesto: ¿ha oído alguna vez sobre wabbits? (fuera de las tiras de Warner Bros.) Según Wikipedia, wabbits es de hecho raro, y no es difícil ver por qué: no hacen nada para esparcirse a otras máquinas. Un wabbit, como los virus, se replica pero no tiene instrucciones para mandar correos electrónicos o para pasar por una red de la computadora para infectar a otras máquinas. El menos ambicioso de todos los malware, se concentra simplemente en devastar totalmente una sola máquina.

4. Troyanos. Discutiblemente, la clase más peligrosa de malware, por lo menos desde un punto de vista social. Mientras los troyanos raramente destruyen las computadoras o los archivos, eso es sólo porque tienen objetivos más grandes: su información financiera, sus recursos de sistema de computadora, y a veces incluso ataques masivos de negación de servicio lanzados al tener millares de computadoras tratando de conectarse a un servidor Web todas al mismo tiempo.

5. Spyware. En otro caso de nombrar creativamente a un software, spyware es software que lo espía a usted, a menudo, rastreando sus actividades en Internet para mostrarle anuncios. (Sí, es posible ser tanto adware como spyware al mismo tiempo.)

6. Backdoors. Los Backdoors son similares a los troyanos o los gusanos, pero hacen algo diferente: abren una "puerta trasera" en la computadora, proporcionando una conexión de red para piratas informáticos o para que entren otros malware, o para que se envíen virus o spam desde allí.

7. Exploits. Los Exploits atacan vulnerabilidades específicas de seguridad. ¿Usted sabe cómo Microsoft está siempre anunciando nuevas actualizaciones para su sistema operativo? A menudo, las actualizaciones tratan realmente de cerrar un agujero de seguridad señalado por un nuevo exploit descubierto.

8. Rootkit. El malware que más probablemente tenga un toque humano, los rootkits son instalados por crackeadores (piratas informáticos malos) en las computadoras de otras personas. El rootkit se diseña para camuflarse como un proceso propio de sistema, para mantenerse sin ser vistos. Es el más difícil de detectar de todos los malwares y por lo tanto de remover; muchos expertos recomiendan limpiar completamente su disco duro y volver a instalar todo de nuevo.

9. Keyloggers. No hay premio para quien adivina lo que hace este software: sí, guarda las teclas pulsadas, es decir, lo que usted escribe en la máquina. Típicamente, este tipo de malware (opuesto a los keyloggers instalados deliberadamente por sus dueños para diagnosticar los problemas de las computadora) están almacenando información sensible tal como las contraseñas y detalles financieros.

10. Marcadores o Dialers. Marcan números de teléfono desde el módem de la computadora. Como los keyloggers, ellos son malware sólo si usted no los quiere. Los Dialers suelen marcar números telefónicos con tasas costosas, a menudo localizados en países pequeños lejos de la computadora que llama; o, llaman a la máquina de un pirata informático para transmitir datos robados.

11. Inyectores de URL. Este software "inyecta" una URL dada en lugar de los enlaces que usted está por visitar en su navegador. Generalmente, el URL inyectado es un enlace afiliado a un URL objetivo. Un enlace afiliado es un enlace especial utilizado para rastrear el tráfico que un afiliado (el anunciante) ha mandado al sitio Web original, para que este sitio Web pueda pagar las comisiones sobre las ventas generadas por ese tráfico.

12. Adware. El menos peligroso y más lucrativo de los malware (lucrativo para sus distribuidores, por supuesto). Los Adware despliegan anuncios publicitarios en su computadora. La definición de Wikipedia de malware no da al adware su propia categoría aunque comúnmente se los llame malware. Como notas en Wikipedia, los adware son, a menudo, un subconjunto de spyware. La implicación es que si el usuario escoge permitir un adware en su máquina, no es realmente malware, que es el argumento que la mayoría de las compañías de los adware aducen. En la realidad, sin embargo, la elección de instalar un adware es generalmente una farsa legal que implica la colocación de una mención del adware en algún lugar del material de instalación, y a menudo, sólo en el acuerdo de licencia, que casi nadie lee.

¿Está preparado para desafiar a estos 12 malos? No vaya sólo. Cerciórese de que tiene, por lo menos, un antivirus y un antispyware.

* Joel Walsh escribe para spyware-refuge.com sobre eliminación de malware: eliminador de malware