Gusano

Gusanos informáticos

Entre los diversos códigos malignos, los gusanos informáticos han logrado conquistar la primera plaza por méritos propios. Aunque teóricamente no son dañinos por sí mismos, afectan de tal manera a las infraestructuras de soporte de Internet que son capaces de hacer caer los sitios Web más potentes. Conozca cómo se comportan estos temibles enemigos.

Los diccionarios de informática definen un gusano como un código maligno cuya principal misión es reenviarse a sí mismo. Por ello, los gusanos son códigos víricos que, en principio, no afectan a la información de los sistemas que contagian, aunque sí consumen amplios recursos de los mismos y los utilizan como lanzadera para infectar a otros equipos.

A diferencia de la mayoría de los virus, los gusanos se propagan por sí mismos, sin modificar u ocultarse bajo otros programas. Así mismo, y por su propia definición, no destruyen información, al menos de forma directa. Pero claro, estas definiciones se aplican a los gusanos como tales; algunos códigos de malware son principalmente gusanos, pero pueden contener otras propiedades características de los virus.

El mayor efecto de los actuales gusanos es su capacidad para saturar e incluso bloquear por exceso de tráfico a los sitios Web. Incluso si están adecuadamente protegidos por un antivirus actualizado. Y precisamente cuando tienen protección aumenta la sobrecarga, debido a los procesos necesarios para analizar e intentar la eliminación de una cascada de correos en los que se detecta la infección.

Salvo algunos sistemas especializados de protección, los antivirus convencionales intentarán eliminar la parte vírica y dejar el resto; que en general no es nada útil, sino la simple pantalla bajo la que se oculta el gusano. Pero esto conlleva más trabajo que simplemente eliminar un mensaje, cuya única "información" es … un gusano.

En caso de mensajes salientes, también algunos sistemas cuentan con optimización, ya que son capaces de analizar y eliminar, o incluso destruir totalmente, un grupo de correos de una sola operación. Así, por ejemplo, el clásico mensaje de gusano, que se envía a toda la libreta de direcciones del sistema infectado, no necesitará ser procesado de forma individual, tantas veces como remitentes, sino que será analizado una sola vez, detectado como un envío múltiple y eliminado en su núcleo, en lugar de hacerlo sobre las copias individuales.

Este tipo de enfoque facilita que los gusanos no sobrecarguen a los sistemas de protección y que éstos, a su vez, no sean la causa de la caída o saturación de los sistemas informáticos. Historia

Melissa tuvo el dudoso honor de ser el primero de su especie, al menos con distribución masiva. En el mes de marzo cumplió tres años este gusano que inauguró una nueva era de infecciones. Melissa era un virus de macro para Word, su forma de activación, con característica de gusano,

dado que se enviaba a los 50 primeros elementos de la lista de contactos Outlook del sistema infectado.

El sistema de difusión es realmente simple. Sólo hay que insertar el gusano en un sistema, infectarlo, y dejar que se active. El gusano utilizará la libreta de direcciones y se enviará a N sistemas, que a su vez multiplicarán el efecto al mandarlo a cada uno de los elementos de cada uno de los sistemas atacados.

Haga cuentas: si el primer sistema tiene 50 nombres en su lista, y cada uno de éstos por su parte tiene 50 nombres que su vez …, en apenas tres o cuatro pasos, los números adquieren cantidades realmente astronómicas. Aunque algunos de éstos tengan la protección suficiente (pongamos la mitad) y detengan la infección, el resto se expandirá de forma exponencial a lo largo del mundo. Esta acción de multiplicación es su efecto más importante. Melissa fue el precursor de toda una nueva generación de gusanos de este tipo, que posteriormente fue seguida por otros elementos tan conocidos y dañinos como "I Love you", Hybris, Kournikova, CodeRed o Sircam.

Remitente conocido

Una de las características de este tipo de códigos es, precisamente por su forma de infección, que están enmascarados en un email que nos llega de una fuente bien conocida. Alguien con quien mantenemos correspondencia, o, al menos, que el remitente la mantiene con nosotros. Así que su procedencia no resulta en absoluto sospechosa.

Esto es parte de la ingeniería social en que se basan la mayoría de códigos víricos y malignos. En lugar de confiar simplemente en conocer el remitente de un mensaje, compruebe que dispone de un antivirus eficaz y permanentemente actualizado.