Técnicas de implementación de malware

Los cibercriminales explotan a menudo cualquier vulnerabilidad que existe dentro del sistema operativo o el software de aplicaciones que se está ejecutando en la computadora de la víctima, de manera que un gusano de red o virus troyano pueda ingresar en el equipo de la víctima y ejecutarse.

¿Qué es una vulnerabilidad?

Una vulnerabilidad es en realidad un error en el código o la lógica de operación del sistema operativo o del software de aplicaciones. Como los sistemas operativos y las aplicaciones de hoy en día son muy complejos e incluyen una gran cantidad de funciones, es difícil que el equipo de desarrollo de un proveedor cree software que no contenga ningún error.

Lamentablemente, no faltan creadores de virus y cibercriminales listos para dedicar esfuerzos considerables a investigar cómo aprovechar cualquier vulnerabilidad antes de que sea solucionada por el proveedor que publica el parche de software.

Entre las vulnerabilidades típicas se incluyen:

Vulnerabilidades de aplicaciones

Los gusanos de correo Nimda y Aliz explotaron las vulnerabilidades de Outlook de Microsoft. Cuando la víctima abría un mensaje infectado (o incluso colocaba el cursor sobre el mensaje en la ventana de vista previa), el archivo del gusano se ejecutaba.

Vulnerabilidades del sistema operativo

CodeRed, Sasser, Slammer y Lovesan (Blaster) son ejemplos de gusanos que aprovechaban las vulnerabilidades de Windows, mientras que gusanos Ramen y Slapper penetraban en las computadoras a través de las vulnerabilidades de Linux y algunas aplicaciones de esta plataforma.

Cómo explotar las vulnerabilidades del navegador de Internet

Recientemente, la distribución de código malicioso a través de páginas web se ha convertido en una de las técnicas de implementación de malware más populares. Se introducen un archivo infectado y un programa de script (que aprovechan la vulnerabilidad del navegador) en una página web. Cuando un usuario visita la página, el programa de script descarga el archivo infectado en la computadora del usuario a través de la vulnerabilidad del navegador y luego ejecuta el archivo. Con el objetivo de infectar la mayor cantidad posible de máquinas, el creador de malware usa varios métodos para atraer víctimas a la página web, entre ellos:

Enviar mensajes de spam que contengan la dirección de la página infectada.

Enviar mensajes a través de sistemas de mensajería instantánea.

A través de motores de búsqueda, que procesan el texto ingresado en una página infectada y luego el enlace a la página se incluye en las

listas de resultados de búsqueda.

Allanar el camino para infecciones de virus troyanos

Los cibercriminales también usan troyanos pequeños diseñados para descargar y ejecutar virus troyanos más grandes. El pequeño virus troyano ingresa en la computadora del usuario (por ejemplo, a través de una vulnerabilidad) y luego descarga e instala otros componentes maliciosos desde Internet. Muchos de los troyanos cambiarán la configuración del navegador (a la opción menos segura) para facilitar la descarga de otros troyanos.

Los desarrolladores de software y los proveedores de antivirus responden al desafío

Lamentablemente, el período que media entre la aparición de una nueva vulnerabilidad y el inicio de su explotación por parte de gusanos y troyanos tiende a ser cada vez más corto. Esto plantea desafíos tanto para los proveedores de software como para las empresas antivirus:

- Los proveedores de sistemas operativos y aplicaciones tienen que rectificar su error de inmediato, para lo cual necesitan desarrollar un parche de software, probarlo y distribuirlo entre los usuarios.
- Los proveedores de antivirus deben trabajar con rapidez para lanzar una solución capaz de detectar y bloquear los archivos, los paquetes de red o cualquier otro elemento usado para aprovechar la vulnerabilidad.

Tomado de https://latam.kaspersky.com/resource-center/threats/malware-implementation-techniques