# Técnicas de implementación de malware

Los cibercriminales a menudo explotan cualquier vulnerabilidad que existe dentro del sistema operativo (SO) 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 introducirse en el equipo de la víctima y ejecutarse.

## ¿Qué es una vulnerabilidad?

Una vulnerabilidad es, en efecto, un error en el código o lógica de operación dentro del SO o el software de aplicaciones. Como los sistemas operativos y las aplicaciones de hoy en día son muy complejos e incluyen muchas funciones, es difícil que el equipo de desarrollo de un proveedor cree software que no contenga ningún error.

Lamentablemente, sobran los creadores de virus y cibercriminales listos para dedicar esfuerzos considerables para investigar cómo se pueden beneficiar de la explotación de alguna vulnerabilidad, antes de que sea reparada por el proveedor que emite un 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 (SO)**
  CodeRed, Sasser, Slammer y Lovesan (Blaster) son ejemplos de gusanos que explotaban las vulnerabilidades del SO Windows, donde los gusanos Ramen y Slapper penetraban las computadoras a través de las vulnerabilidades en el SO Linux y algunas aplicaciones Linux.

## Cómo explotar las vulnerabilidades del navegador de Internet

Hace poco, la distribución de un código malicioso a través de páginas web se ha vuelto una de las técnicas de implementación de malware más populares. Un archivo infectado y un programa de script (que explotan la vulnerabilidad del navegador) se colocan 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. A fin de infectar la mayor cantidad posible de máquinas, el creador de malware usará 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, en donde los motores de búsqueda procesan el texto colocado en una página infectada y luego el enlace a la página se incluye en las listas de resultados de búsqueda.

## Allanar la ruta para infecciones de virus troyano

Los cibercriminales también usarán troyanos pequeños diseñados para descargar y ejecutar virus troyanos más grandes. El virus troyano pequeño ingresará a la computadora del usuario (por ejemplo, a través de una vulnerabilidad) y luego descargará e instalará otros componentes maliciosos desde Internet. Muchos de los troyanos cambiarán la configuración del navegador (a la opción menos segura) a fin de facilitar que otros troyanos se descarguen.

## Los desarrolladores de software y los proveedores de antivirus responden a los desafíos

Lamentablemente, el período 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 crea desafíos tanto para los proveedores de software como para las empresas antivirus:

- Los proveedores de SO y aplicaciones tienen que rectificar su error de inmediato, al desarrollar un parche de software, probarlo y distribuirlo a los usuarios.
- Los proveedores de antivirus deben trabajar rápidamente para lanzar una solución que detecte y bloquee los archivos, los paquetes de red o cualquier otro elemento usado para explotar la vulnerabilidad.