APLICACIONES SEGURIDAD- MALWARE

La seguridad informática está tomando muchísima importancia, así que en este curso no podía faltar un apartado dedicado a ella, y, particularmente, al llamado malware, que no es sino software diseñado para realizar acciones maliciosas en nuestros equipos informáticos. Empezaremos por ver los distintos tipos que hay y terminaremos comentando algunas herramientas para eliminarlo o, al menos, detectarlo.

Tipos de malware

•Virus: Un virus es un código malicioso que se adjunta a un archivo o programa y se propaga cuando el archivo infectado es ejecutado. Los virus pueden destruir archivos o causar problemas operativos en los sistemas infectados.

•Gusanos: Los gusanos son similares a los virus, pero tienen la capacidad de replicarse y propagarse automáticamente a través de redes sin necesidad de interacción humana. Pueden causar congestión de red y dañar sistemas al consumir recursos.

•Troyanos: Los troyanos se presentan como software legítimo para engañar a los usuarios y obtener acceso a sus sistemas. Una vez dentro, pueden robar información, instalar otros tipos de malware o crear puertas traseras para acceso no autorizado.

•Ransomware: Este tipo de malware cifra los archivos del usuario o bloquea el acceso al sistema, exigiendo un pago de rescate para restaurar el acceso. Es una amenaza persistente que puede causar pérdidas significativas de datos.

•Spyware: El spyware se instala en un dispositivo para espiar la actividad del usuario y robar información confidencial, como datos financieros y contraseñas. Puede ser difícil de detectar ya que opera de manera encubierta.

•Adware: El adware muestra anuncios no deseados en los dispositivos infectados. Aunque no siempre es dañino, puede ser intrusivo y afectar el rendimiento del sistema.

•Rootkits: Los rootkits están diseñados para ocultar la presencia de otros tipos de malware y permitir el acceso no autorizado al sistema. Son difíciles de detectar y eliminar, llegando a infectar el kernel del sistema o incluso firmware de dispositivos.

•Keyloggers: Este tipo de malware registra las pulsaciones de teclas del usuario para capturar información sensible, como contraseñas y datos de tarjetas de crédito.

•Botnets: Una botnet es una red de computadoras infectadas que son controladas de manera remota por un atacante. Las botnets se utilizan para realizar ataques coordinados, como ataques de denegación de servicio ().

Herramientas de Seguridad y Privacidad en Linux

•ClamAV: Motor antivirus de código abierto para detectar troyanos, virus, malware y spyware. Útil para escanear archivos y correos electrónicos en servidores Linux.

•Bleachbit: Además de limpiar el sistema, tiene opciones para eliminar datos de forma segura y evitar que puedan ser recuperados.

•Tor Browser: Navegador web basado en Firefox que permite navegar de forma anónima y eludir la censura. Útil para proteger la privacidad en línea.

•Chkrootkit. Herramienta utilizada para detectar rootkits en sistemas Linux. Es una utilidad ligera y fácil de usar que verifica la presencia de rootkits conocidos.

•Rkhunter: Similar a Chkrootkit, Rkhunter es un escáner de rootkits que verifica la integridad del sistema y busca rootkits, puertas traseras y exploits locales.

•Lynis: Herramienta de auditoría de seguridad que escanea sistemas Linux en busca de vulnerabilidades, problemas de configuración y malware.

•Linux Malware Detect (): Escáner de malware diseñado específicamente para detectar amenazas en entornos Linux, especialmente en servidores compartidos. Se puede integrar con ClamAV para mejorar el rendimiento y utiliza una base de datos de firmas actualizada para detectar malware.

•Kaspersky Virus Removal Tool (): Herramienta gratuita de Kaspersky para escanear sistemas Linux y Windows en busca de ciberamenazas conocidas. No ofrece monitoreo en tiempo real, pero es útil para escaneos periódicos.

Herramientas de Seguridad y Privacidad en Windows

Bitdefender: Antivirus premiado por su eficacia en la detección y eliminación de malware. Ofrece tanto soluciones gratuitas como de pago. Incorpora protección en tiempo real, análisis de comportamiento y un motor de detección avanzado que identifica amenazas conocidas y desconocidas.

•Windows Defender: El programa de seguridad nativo de Windows 11, que proporciona protección básica contra malware. Incluye protección antivirus y contra amenazas, con opciones para realizar análisis rápidos, completos y personalizados del sistema.

•Avast Antivirus: Antivirus gratuito que ofrece protección contra una amplia gama de amenazas de malware. En su versión de pago incremente sus prestaciones. Incorpora protección en tiempo real, análisis de red, y herramientas para eliminar malware y mejorar el rendimiento del sistema.

•Malwarebytes: Conocido por su capacidad para eliminar malware que otros programas pueden pasar por alto. Ofrece protección contra malware, ransomware y otras amenazas avanzadas, con un enfoque en la eliminación de infecciones existentes.

•Kaspersky Antivirus: Antivirus robusto que proporciona protección integral contra malware y otras amenazas de seguridad. Incorpora protección en tiempo real, análisis de vulnerabilidades y herramientas de seguridad adicionales, como un gestor de contraseñas y .