Práctica de laboratorio: Anatomía del malware

Objetivos

Investigar y analizar malware.

Aspectos básicos / Escenario

El malware, o software malicioso, hace referencia a diversos programas de software malicioso que se pueden utilizar para causar daños en sistemas informáticos, robar datos y eludir medidas de seguridad. El malware también puede atacar infraestructura crítica, deshabilitar servicios de emergencia, hacer que las líneas de ensamble fabriquen productos defectuosos, deshabilitar generadores eléctricos e interrumpir servicios de transporte. Los expertos en seguridad estiman que se lanzan más de un millón de amenazas de malware nuevas por día. Los laboratorios de amenazas de McAfee revelaron que en el año 2019 se descubrieron nuevos tipos de técnicas de ransomware, mediante la exposición de miles de millones de cuentas a través de enormes extracciones de datos, una cantidad significante de explotación web en HTTP, defectos en el sistema operativo Windows, Microssoft Office, y en el sistema iOS de Apple, además de ataques continuos en dispositivos IoT (Internet of Things) personales. Encontremos la versión más actual del reporte mediante una búsqueda web de "McAfee Labs Threats Report".

Nota: Puede utilizar el navegador web de la máquina virtual instalada en una práctica de laboratorio anterior para investigar problemas relacionados con la seguridad. Si utilizan la máquina virtual, pueden impedir que se instale malware en su computadora.

Recursos necesarios

- Computadora personal o dispositivo móvil con acceso a internet

Instrucciones

Realizar una búsqueda de malware reciente en internet

a. Utilizar su motor de búsqueda favorito para buscar malware reciente. Durante la búsqueda, elijan cuatro ejemplos de malware, uno de cada tipo de malware diferente, y prepárense para debatir detalles de qué hacen, cómo se transmiten y el impacto que causan.

   Entre algunos de los ejemplos de malware podemos incluir los siguientes: Ransomware, Troyanos, Hoax, Adware, Malware, PUP, Exploit, Exploit Kit, etc. Realizar la búsqueda de los ejemplos de malware utilizando los siguientes términos.

   - McAfee Threat Center Threat Landscape Dashboard
   - Malwarebytes Labs Threat Center (Top 10 Malware)
   - Securityweek.com > virus-threats > virus-malware
   - Technewsworld.com > security > malware

b. Leer la información sobre el malware encontrado en la búsqueda realizada en el anterior paso, escoger uno de ellos y escribir un pequeño resumen explicando qué hace el malware, como funciona, como se transmite y cuáles son sus efectos.