Principales ciberataques

Troyano de puerta trasera

Programas que permiten hacerse con el control de computadoras ajenas sin el permiso de los usuarios. Se esconden dentro de programas legítimos para engañar a los usuarios y que los ejecuten.

Secuestrador de navegadores

Cambian la página de inicio y el motor de búsqueda predeterminados de los navegadores web sin el permiso de los usuarios. Una vez secuestrado el navegador, puede ser difícil volver a cambiar la página de inicio.

Filtración de datos

Divulgación no autorizada de información que puede deberse a robos o fugas de datos. Se producen cuando la información confidencial no se protege adecuadamente, al hacerla pública o compartirla con terceros.

Ataque de denegación de servicio

DDoS, por sus siglas en inglés. Impide que los usuarios accedan a un equipo o un sitio web, debido a una sobrecarga de solicitudes de acceso, por redes de bots o bloqueo de un servicio o página web.

Descarga automática

La descarga de un programa malicioso que infecta a una computadora cuando se visita un sitio web.

Gusano de internet

Programa malicioso que se duplica en internet o redes locales; pueden propagarse por su cuenta.

Malware

Genérico para referirse a virus, gusanos, troyanos y programas espía.

Parches

Complementos de software diseñados para corregir defectos, incluidas vulnerabilidades de seguridad, en sistemas operativos y aplicaciones.

Suplantación de identidades

Proceso mediante el cual los ciber intrusos engañan a los usuarios para que revelen información privada. Los usuarios reciben correos electrónicos que simulan provenir de una institución de confianza.

Ransomware

Programas que impiden acceder a los archivos o a los equipos personales hasta que se paga un rescate.

Ingeniería social

Métodos para engañar a las personas para que realicen determinadas acciones, como abrir páginas web maliciosas o ejecutar archivos adjuntos.

Spear phishing

En español “pesca con arpón”, es un ataque selectivo de suplantación de identidad en el que se utilizan mensajes de correo electrónico falsos con el fin de convencer a las personas de una empresa a que revelen información sensible o credenciales.

Spyware

Son utilizados por ciber intrusos y anunciantes para recolectar información privada de los usuarios sin permiso. Suelen introducirse en los equipos al visitar determinados sitios web. Algunos muestran ventanas para que el usuario descargue programas de manera automática.

Troyano

Programas maliciosos que se hacen pasar por software que finge realizar una actividad cuando en realidad llevan a cabo otra distinta sin el conocimiento del usuario.