Navegación segura (II): Ataques comunes al navegador

Introducción de código malicioso en el equipo del usuario (y víctima) a través de una vulnerabilidad del navegador:

- mediante anuncios,
- mediante engaños de ingeniería social (por ejemplo, phishing),
- a través de sitio web legítimo previamente infectado.

Inclusión de código malicioso en formularios o en la misma ruta de navegación para que se ejecuten en el propio navegador del usuario (cuando éste introduce datos en blogs, foros, redes sociales,…)

Descarga y ejecución de ficheros de fuentes no confiables (por ejemplo, cuando se visitan sitios no oficiales para descargar software, imágenes u otros documentos maliciosos)

Uso de extensiones y plugin maliciosos (originalmente diseñados para añadir o modificar funcionalidades)

Interceptación y manipulación de las comunicaciones entre el navegador (el cliente) del usuario y el servidor web (por ejemplo, mediante falsos Puntos de Acceso Wifi de conexión a una Wifi suplantada)

Navegación segura (II): Recomendaciones de seguridad

Verifique que su navegador, así como plugin, extensiones y cualquier otro elemento que utilice, están actualizados correctamente. (los atacantes conocerán la versión y tipo del navegador y de los plugin para posteriormente lanzar exploits a medida)

No haga clic en enlaces sospechosos; por ejemplo, los recibidos por medio del correo electrónico.

Desinstale o deshabilite aquellas extensiones que hubiera instalado en algún momento para una cierta tarea y que ya no le son de utilidad; en caso contrario, estará aumentando su superficie de exposición de forma innecesaria

Aunque los navegadores ofrecen la posibilidad de almacenar las credenciales de acceso a los diferentes sitios web para comodidad del usuario, esto está desaconsejado ya que, si el equipo es comprometido, es relativamente sencillo acceder a dichas credenciales. Además, si el equipo es compartido de forma no segura, es trivial acceder a las credenciales

Revise las opciones de seguridad y privacidad de su navegador. Actualmente los navegadores disponen de medidas tan interesantes como: no aceptar cookies de terceros, bloquear pop-ups, evitar la sincronización de contraseñas, evitar el autocompletado, borrar los ficheros temporales y cookies al cerrar el navegador, bloquear la geolocalización, filtrar ActiveX, etc.

El usuario no debe almacenar las sesiones asociadas a servicios web que manejen información sensible o crítica en el equipo y, además, debe cerrar las mismas una vez que finalice su navegación.