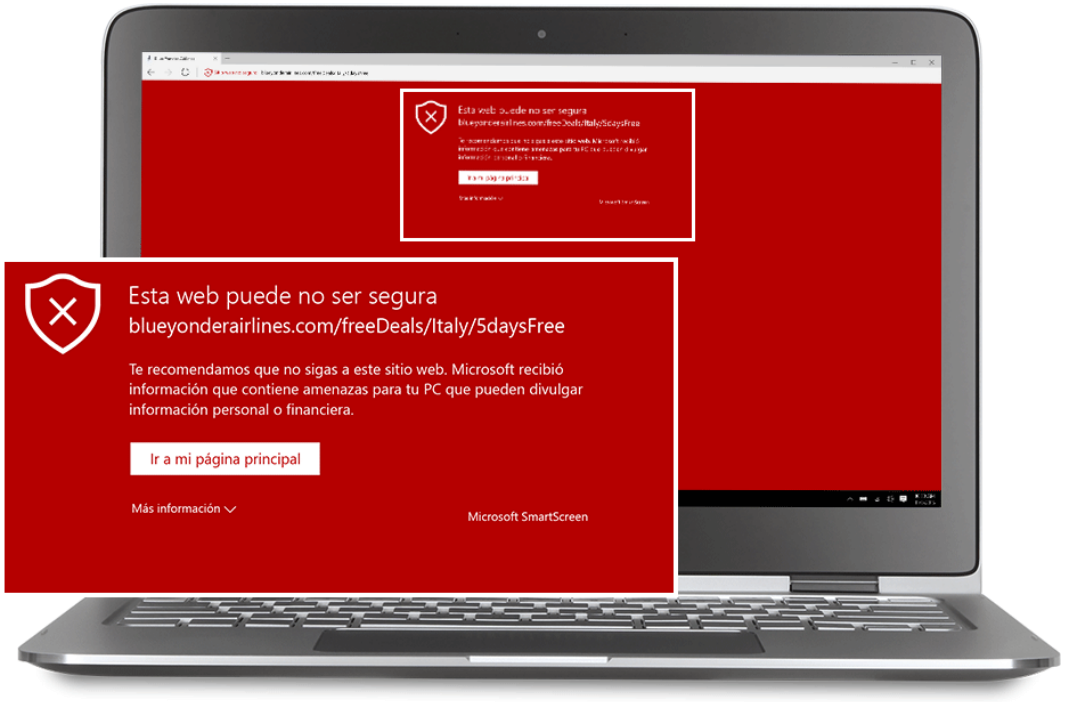
Infórmate

EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA

Instituto Politécnico Nacional
"La Técnica al Servicio de la Patria"

Amenazas Web



Las amenazas basadas en la web (o amenazas en línea) son programas malware que atacan cuando usas Internet. Estas amenazas basadas en navegador incluyen diversos programas de software malicioso diseñados para infectar las computadoras de las víctimas.

La principal herramienta de estas infecciones basadas en navegador es el paquete de exploits, que brinda a los cibercriminales una ruta para infectar computadoras que:

- No tienen un producto de seguridad instalado.
- Contienen un sistema operativo o aplicación de uso común que es vulnerable, porque el usuario no ha instalado las actualizaciones más recientes o el proveedor del software aún no ha publicado un nuevo parche

Aplicaciones y sistemas operativos atacados por las amenazas en línea

Los cibercriminales aprovechan prácticamente cualquier vulnerabilidad (dentro de un sistema operativo o aplicación) para ejecutar un ataque basado en exploit. Sin embargo, la mayoría de los cibercriminales desarrolla amenazas web dirigidas deliberadamente a los sistemas operativos y aplicaciones más comunes, como:

Java Como Java está instalado en más de 3000 millones de dispositivos (que se ejecutan en diversos sistemas operativos), se pueden crear exploits para aprovechar vulnerabilidades Java específicas en varias plataformas o sistemas operativos diferentes.	**Adobe Reader** Adobe Reader ha sido blanco de muchos ataques y Adobe ha implementado herramientas para proteger el programa contra la actividad de exploits, de manera que resulte más difícil crear exploits para la aplicación. Sin embargo, Adobe Reader ha seguido siendo un blanco habitual durante los últimos 18 meses.
Windows e Internet Explorer Los exploits activos siguen dirigiéndose a las vulnerabilidades que se detectaron allá por 2010, incluidas MS10-042 en el Centro de soporte técnico y la ayuda de Windows, y MS04-028, que se asocia a la manipulación incorrecta de archivos JPEG.	**Android** Los cibercriminales usan exploits para obtener privilegios de raíz y lograr el control prácticamente completo del dispositivo objetivo.

Millones de ataques web cada día

En 2012, la cantidad de ataques basados en navegador ascendió a 1 595 587 670. En promedio, eso significa que los productos Kaspersky Lab protegieron a los usuarios contra amenazas web más de 4,3 millones de veces cada día.

Los expertos en seguridad de Internet de Kaspersky han identificado los programas de software maliciosos más activos involucrados en amenazas web. La lista incluye los siguientes tipos de amenazas en línea:

- **Sitios web maliciosos**
  Kaspersky identifica estos sitios web mediante métodos de detección heurísticos basados en la nube. La mayoría de las detecciones de URL maliciosas se dirigen a sitios web que contienen exploits.

- **Scripts maliciosos**
  Los hackers inyectan scripts maliciosos en el código de sitios web legítimos que han visto su seguridad comprometida. Estos scripts se usan para realizar ataques en tránsito, en los cuales los visitantes del sitio web son redirigidos, sin ser conscientes de ellos, a recursos en línea maliciosos.

- **Scripts y archivos PE ejecutables**
  Por regla general: ○ Descargan e inician otros programas de software malicioso ○ Portan una carga que roba datos de cuentas de banca en línea y redes sociales o sustraen credenciales y datos de usuario de cuentas de otros servicios.

- **Descargadores de troyanos**
  Estos virus troyanos distribuyen diversos programas maliciosos a las computadoras de los usuarios.

- **Exploits y paquetes de exploits**
  Los exploits atacan vulnerabilidades y tratan de burlar la atención del software de seguridad de Internet.

- **Programas adware**
  A menudo, se instala simultáneamente adware cuando el usuario comienza a descargar un programa freeware o shareware.

Fuente:https://latam.kaspersky.com/resource-center/threats/web