GUIAS DE SEGURIDAD UJA

Software malicioso (malware)

1. ¿Qué es el malware?

El término *malware* (también conocido como software malicioso o software malintencionado) hace referencia a todo tipo de programas diseñados específicamente para dañar un ordenador o una red o para obtener algún tipo de beneficio o hacer mal uso del mismo.

El malware en muchos casos se instala en nuestro ordenador sin nuestro conocimiento, generalmente a través de descargas o enlaces de carácter engañoso que simulan ser contenido en el que podríamos estar interesados. Una vez que el malware se ha instalado en el ordenador, las personas que tienen el control en muchas ocasiones pueden intentar acceder a nuestra información personal. A veces registran nuestras pulsaciones de teclas (*keylogging*) o controlan la actividad de nuestro equipo, pudiendo forzarlo a visitar determinados sitios web, enviar correos electrónicos o realizar otras acciones sin nuestro conocimiento. Los efectos del malware pueden ser tan inofensivos como una pequeña molestia o tan graves como un robo de identidad, con todo el perjuicio que ello nos puede causar.

Síntomas más habituales de infección:

- Aparición de barras de elementos adicionales en nuestro navegador web sin que nosotros las hayamos instalado conscientemente.
- Nuestra página de inicio cambia sin que nosotros lo indiquemos. Si la sustituimos por la correcta, vuelve a cambiar automáticamente.
- Cuando navegamos por Internet, determinadas páginas son redirigidas automáticamente a otras de dudoso contenido (pornografía, hacking, juegos on-line, páginas de acceso mediante pago...).
- El equipo se ralentiza y se cargan iconos desconocidos en la barra de Windows.

2. Tipos de malware y técnicas de infección más comunes

Los ejemplos de malware más habituales suelen ser los siguientes:

- **Virus:** tipo de malware cuya finalidad es la de alterar el funcionamiento normal de nuestro equipo, sin el permiso o el conocimiento del usuario.
- **Gusanos (*worms*):** programas informáticos malintencionados que se replican automáticamente, usando una red informática para enviar copias de sí mismos a otros ordenadores de la red, pudiendo causar un enorme efecto en muy poco tiempo.
- **Troyanos:** programas destructivos que se hace pasar por una aplicación legítima e inofensiva, pero por detrás y sin el conocimiento del usuario, roba información, daña el sistema o abre una puerta trasera para poder entrar al equipo de forma remota sin ser detectado.
- **Software espía (*spyware*):** software malintencionado que extrae información sobre los usuarios sin su conocimiento.
- **Software publicitario (*adware*):** cualquier paquete de software que reproduce, muestra o descarga anuncios en nuestro ordenador de forma automática y sin nuestro consentimiento.
- **Rogue software y Ransomware:** programas que hacen creer al usuario que su ordenador está infectado por algún tipo de virus o software malicioso, y fuerzan al usuario a pagar por un software malicioso que supuestamente elimina las infecciones.
- **Rootkits.** conjuntos de programas que modifican el sistema operativo de nuestro PC para permitir que el malware permanezca oculto al usuario.

2.1. ¿Cómo llega el malware hasta nuestro PC?

Existen gran variedad de formas por las que el malware puede llegar a un ordenador:

- **Explotando una vulnerabilidad** en cualquier programa que puede ser aprovechada para introducir programas maliciosos. Para prevenir infecciones por esta vía, se recomienda tener siempre actualizado el software en nuestro equipo.
- **Ingeniería social:** Las técnicas de ingeniería social apremian al usuario a que realice determinada acción, amenazándolo de diversas formas.
- **A través de un archivo malicioso** que puede llegar como adjunto de un mensaje, por redes P2P, como enlace a un fichero que se encuentre en Internet, a través de carpetas compartidas en las que el gusano haya dejado una copia de sí mismo, etc.
- **Dispositivos extraíbles (ej: llaves USB):** muchos gusanos suelen dejar copias de sí mismos en dispositivos extraíbles para que automáticamente, cuando el dispositivo se conecte a un ordenador, ejecutarse e infectar el nuevo equipo.

3. Cómo combatir el malware. Medidas prácticas

1. **Actualiza tu sistema operativo** con todos los parches más recientes y activa las actualizaciones automáticas si es posible.

2. **Instala periódicamente todas las actualizaciones del navegador** o elige navegadores que se actualizan de forma automática y transparente a la última versión. Instala únicamente extensiones en las que confíes.

3. **Ten mucho cuidado al hacer clic en un enlace o descargar un archivo.** Para proteger tu ordenador, descarga únicamente archivos de fuentes de confianza. Ten cuidado cuando accedas a sitios desconocidos. Si no estás seguro, sal del sitio y busca información sobre el software que se te pide que instales.

4. **Desconfía de cualquier elemento de un correo electrónico que parezca sospechoso.**

5. No abras archivos si no conoces su extensión o si recibes advertencias o mensajes del navegador web que no te resulten familiares.

6. **Al instalar software, presta especial atención a los mensajes que aparezcan y lee la letra pequeña.** También es recomendable buscar información sobre cualquier software desconocido antes de iniciar el proceso de instalación.

7. **Ten mucha precaución con las unidades USB.** Siempre ten la precaución de analizar la unidad externa con un buen software antivirus antes de abrir los archivos.

8. **No te fíes de las ventanas emergentes que te piden que descargues software.** Cierra la ventana y asegúrate de no hacer clic en ninguna zona de la ventana emergente.

9. **Ten cuidado con la descarga de ficheros desde redes P2P** (BitTorrent y similares). El software malintencionado se puede hacer pasar por un programa, un disco, una película o cualquier elemento conocido.

10. **Elimina el malware lo antes posible.** Existe una serie de programas específicos como Malwarebytes Anti-malware que te pueden resultar útiles.

4. Referencias en Internet

- Instituto Nacional de Ciberseguridad (INCIBE)
  http://www.incibe.es
- Oficina de Seguridad del Internauta (OSI)
  http://www.osi.es/
- CCN-CERT
  https://www.ccn-cert.cni.es/
- Guardia Civil - Grupo de Delitos Telemáticos:
  https://www.gdt.guardiacivil.es
- Policía Nacional – Brigada de Investigación Tecnológica
  http://www.policia.es/org_central/judicial/udef/bit_alertas.html
- Vídeos Intypedia: Lección 6 – Malware (con ejercicios)
  http://www.criptored.upm.es/intypedia/video.php?id=malware&lang=es
- InfoSpyware:
  http://www.infospyware.com/articulos/que-son-los-malwares
- Eset Security:
  http://www.eset-la.com/centro-amenazas/tipos-amenazas