TIC07 EL MALWARE

1 Introducción.

2 Evolución del malware.

3 Tipos de malware.

4 Formas de contraer malware.

5 Protección contra el malware.

6 Los antivirus y antiespías.

1. INTRODUCCION

Se denomina **malware** (software malicioso) al software específicamente diseñado para llevar a cabo acciones no deseadas (como infiltrase o dañar un ordenador o sistema informático) sin el consentimiento explicito del usuario.

Existen muchos tipos de malware: virus, gusanos, troyanos, adware, keyloggers, dialers, rootkits, spyware, ransomware, rogueware, etc. que se diseñan con diferentes fines. Algunos tipos de malware se diseñan con ánimo de lucro, otros son destructivos y su misión es alterar programas y archivos, otros hacen que un equipo sea controlado y explotado con fines ilícitos (envío de correo electrónico, almacenar pornografía, ataques a otros equipos o almacenar datos de actividades ilegales), etc.

Aunque el malware se puede diseñar para cualquier sistema operativo, la mayoría del malware que se diseña en la actualidad es para plataformas Windows (>99%). Linux, MacOS y otros sistemas operativos cuentan con especímenes de malware en menor medida. También existen ejemplares de malware para Android, Symbian e iOS, diseñados para infectar dispositivos y teléfonos móviles.

El malware puede contraerse de diferentes maneras: descarga de archivos desde páginas Web, correo electrónico, por vulnerabilidades del software, etc.

En cuanto a las medidas que se pueden tomar para prevenir infecciones, se pueden citar: utilización de programas antivirus, actualización del sistema operativo, navegador Web y resto de aplicaciones, utilización de cuentas de usuario restringido, etc.

Nota: No hay que confundir el malware o código malicioso con el software defectuoso, que es el que incluye código con errores o bugs de forma no intencionada. El software defectuoso es software con errores de programación.

2. EVOLUCION DEL MALWARE

Los primeros virus fueron creados por programadores que tenían como objetivo experimentar y demostrar su destreza como programadores. No existían fines económicos. Hoy en día existe todo un negocio alrededor del malware y hay verdaderas mafias detrás del mismo.

El malware puede diseñarse con diferentes fines. Por un lado, se puede diseñar con el objetivo de darse a conocer. También existe malware que se diseña con el objetivo de causar daño o pérdida de datos, llevando a cabo actos vandálicos, tales como como destruir archivos o corromper el sistema escribiendo datos inválidos. No obstante, dado el gran aumento de los usuarios de Internet, actualmente el malware se diseña para obtener beneficios, existiendo un gran negocio alrededor de él. Hoy en día, gran parte del malware que se diseña, tiene como objetivo acceder a un equipo para tomar su control (ordenador zombi) para su uso en el mercado negro (enviar spam, alojar datos ilegales como pornografía infantil, ataques DDoS como forma de extorsión, etc.).

La siguiente tabla puede servir como ejemplo para hacernos una idea de como ha ido evolucionando el malware:

1987-1999	Virus clásicos, los creadores no tenían ánimo de lucro, motivación intelectual y protagonismo.
2000-2004	Explosión de los gusanos en Internet, propagación por correo electrónico, aparición de las botnets.
2005-2009	Claro ánimo de lucro, profesionalización del malware, explosión de troyanos bancarios y programas espías.
2010-2011	Casos avanzados de ataques dirigidos, espionaje industrial y gubernamental, ataque a infraestructuras críticas, proliferación de infecciones en dispositivos móviles.

3. TIPOS DE MALWARE

El malware es aquel software que tiene como propósito explícito infiltrarse o dañar un equipo informático.

El malware se puede clasificar de acuerdo a las siguientes categorías:

- **Virus informáticos**: son programas que se instalan en el ordenador sin conocimiento del usuario. Se autoreplican e infectan otros programas. Su fin es propagarse a otros equipos y ejecutar las acciones para las que fueros diseñados. Estas acciones pueden ir desde pequeñas bromas, pasando por la ralentización o apagado del sistema, hasta la destrucción total de los discos duros.
- **Gusanos informáticos (worms)**: es un tipo de virus que se replica mediante copias de sí mismo, pero no infecta a otros programas. Su finalidad es multiplicarse e infectar todos los nodos de una red de ordenadores. No suelen implicar la destrucción de archivos, pero si si ralentizan el funcionamiento de los ordenadores y de toda la red. Suelen acompañar a un correo malicioso y muchos tienen la capacidad de enviarse automáticamente a todos los contactos de la agenda de correo.
- **Troyanos**: un troyano es un programa disfrazado como algo atractivo o inofensivo que invita al usuario a ejecutarlo. Puede ser una pequeña aplicación escondida en otros programas de utilidades, fondos de pantalla, imágenes, etc. No se replican ni infectan a otros programas de forma automática e indiscriminada. Su fin no es destruir información, sino disponer de una entrada a nuestro ordenador para que otro usuario o aplicación recopile información del mismo o incluso tome el control absoluto de nuestro equipo de forma remota. Se transmiten a través de software y medios como la Web, el correo electrónico, los chats o los servidores ftp.
- **Espias (spyware)**: Son programas que se instalan en el equipo sin conocimiento del usuario. Su objetivo es alterar el correcto funcionamiento del equipo (impiden acceder a determinadas páginas Web, muestran continuamente ventanas emergentes en nuestro navegador, etc.) o recopilar información del usuario. La información recopilada es

enviada a servidores de Internet que son gestionados por compañías de publicidad. La información es utilizada para enviarnos spam o correo basura. Los ordenadores infectados con spyware tienen ralentizada su conexión con Internet.

- **dialers**: son programas que se instalan en el ordenador y utilizan el módem del usuario (cuando éste se conecta a Internet a través de una conexión de acceso telefónico) para realizar llamadas telefónicas de alto coste incrementando la factura telefónica. Si la conexión a Internet se realiza mediante un router ADSL se evita este problema.
- **Adware**: son programas que muestran publicidad no deseada por el usuario de forma intrusiva (sin consentimiento del usuario) e inesperada, normalmente en forma de ventanas emergentes (pop-up).
- **Spam (correo basura)**: consiste en el envío de correo electrónico publicitario de forma masiva a cualquier dirección de correo electrónico existente. Su fin es vender sus productos. Los principales perjuicios son la saturación de los servidores de correo y la ocultación de otros correos maliciosos.
- **pharming**: consiste en la suplantación de páginas Web por parte de un servidor local que está instalado en el equipo sin que el usuario lo sepa. La suplantación suele utilizarse para obtener datos bancarios de los usuarios y cometer delitos económicos.
- **Phishing (pesca de datos)**: consiste en obtener información confidencial de los usuarios de banca electrónica mediante el envío de correos electrónicos que solicitan dicha información. Esta estafa se disimula dando al correo el aspecto oficial de nuestro banco y usando la misma imagen corporativa.
- **keyloggers**: un keylogger es un programa que captura las pulsaciones del teclado. Su misión es espiar lo que el usuario escribe y almacenarlo para enviarlo posteriormente al creador del programa. La mayoría se utilizan para recopilar claves de acceso, números de tarjetas de crédito (para realizar pagos fraudulentos) y cualquier otra información sensible.
- **rootkits**: utilizan técnicas que modifican el sistema operativo del usuario para que el malware permanezca oculto ante el usuario y las aplicaciones de seguridad. Algunas de estas técnicas pueden ser: evitar que un proceso malicioso aparezca en la lista de procesos del sistema, impedir que los archivos se muestren en el explorador de

archivos, etc.

- **ransomware**: es un tipo de malware cuyo fin es el chantaje. Puede ser una aplicación que cifra documentos y cualquier otro tipo de archivos (imágenes, etc.). y luego pide al usuario que pague un rescate si quiere la clave que permite acceder a los originales.
- **rogueware**: se trata de un falso antivirus. Su misión es hace creer al usuario que su sistema está infectado para cobrarle por la supuesta desinfección.
- **Puerta trasera (Backdoor)**: una puerta trasera permite evadir los procedimientos normales de autenticación al conectarse a una computadora y permite al atacante conectarse y controlar la máquina infectada. Mediante un virus, un gusano de Internet o un troyano, se puede instalar una puerta trasera en el equipo y permitir así un acceso remoto más fácil en el futuro.
- **Bot**: es un tipo de malware que infecta a los sistemas convirtiéndolos en "zombies" que conforman una botnet (red de bots). Las botnets son redes de ordenadores controladas de forma remota por un individuo que los utiliza para el envío masivo de spam o para lanzar ataques contra organizaciones afectando a su ancho de banda e impidiendo así su correcto funcionamiento, lo cual utiliza como forma de extorsión.
- **Crimeware**: es un tipo de malware que se utiliza para cometer fraudes y delitos financieros. Puede ser, por ejemplo, un troyano que roba las claves de acceso del usuario a la banca electrónica, de forma que el atacante puede realizar transferencias en nombre del usuario.
- **Drive-by download**: son sitios Web que instalan spyware o programas que dan información de los equipos sin conocimiento del usuario. La infección se produce al descargar y ejecutar algún fichero malicioso que se descarga sin el consentimiento del usuario (al visitar un sitio Web en el que alguien ha instalado algún script malicioso aprovechando alguna vulnerabilidad del mismo, al ejecutar un fichero adjunto recibido por correo electrónico - por ejemplo un pdf con código malicioso -, al entrar en una ventana emergente o pop-up que muestra un mensaje de error, etc.). Sin saberlo, el usuario consiente la descarga del software e instala spyware o programas que dan información del equipo sin su conocimiento.
- etc.

4. FORMAS DE CONTRAER EL MALWARE

Las formas más habituales de contraer malware son las siguientes:

- Descarga de archivos desde páginas Web.
- Correo electrónico:
  - Al abrir correos electrónicos de remitentes desconocidos sin antes analizarlos con un antivirus.
  - Archivos adjuntos en mensajes de correo electrónico.
- Vulnerabilidades del software.
- Utilización de dispositivos de almacenamiento compartido.
- Otros protocolos y aplicaciones de Internet
  - Mensajería instantánea.
  - Programas P2P.
  - Redes sociales.
- Navegar por Internet utilizando versiones obsoletas del sistema operativo, navegador y resto de aplicaciones.
- Etc.

5. PROTECCION CONTRA EL MALWARE

En cuanto a las medidas para prevenir infecciones o situaciones de riesgo, algunas de ellas pueden ser:

- Utilización de un programa antivirus actualizado.
- Instalación de cortafuegos (firewall).
- Actualización del sistema operativo, navegador Web y resto de aplicaciones (visor de pdf, complementos del navegador, paquetes ofimáticos, etc.).

- Utilización de cuentas de usuario: utilizar cuentas de usuario restringido frente al usuario administrador.
- Sentido común y uso responsable del equipo:
  - Evitar abrir correo no deseado y enlaces llamativos en las redes sociales
  - Evitar abrir documentos e instalar software de fuentes no confiables.
- Utilizar contraseñas seguras.
- Etc.

Como vimos anteriormente, el sistema operativo suele incorporar una serie de herramientas (herramientas de protección) que tienen como misión evitar que el sistema pueda ser infectado por virus o que determinados programas accedan al ordenador de forma oculta. Algunas de las herramientas de protección más comunes son las siguientes:

- **Cortafuegos** (Firewall): impide que usuarios sin autorización obtengan acceso al equipo a través de Internet o una red.
- **Actualizaciones automáticas**: busca e instala actualizaciones importantes periódicamente.
- **Configuración de seguridad de Internet**: esta herramienta permite analizar la configuración de seguridad del navegador y alerta al usuario si considera que los parámetros de seguridad están a un nivel más bajo del recomendado.
- **Control de cuentas de usuario**: permite crear cuentas independientes con diferentes privilegios para los diferentes usuarios de un ordenador. De esta manera, la mayoría de los programas se ejecutarán con permisos de usuario estándar, lo que limita el daño potencial que puede sufrir el equipo.
- **Antivirus**: los antivirus ayudan a proteger el equipo contra virus y otras amenazas a la seguridad.
- **Antiespías**: impiden que se instalen en nuestro ordenador determinados programas cuyo objetivo es alterar su correcto funcionamiento (impiden acceder a determinadas páginas Web, muestran continuamente ventanas emergentes en nuestro navegador,

etc.) o recopilar información del usuario.

Nota: Para evitar efectos indeseados en nuestros equipos es conveniente disponer de las herramientas anteriores y tenerlas activadas y correctamente configuradas.

6. LOS ANTIVIRUS Y ANTIESPIAS

Los antivirus son programas que ayudan a proteger el equipo contra virus y otras amenazas a la seguridad.

En cuanto a la efectividad de los antivirus hay que decir lo siguiente:

- Los antivirus no pueden proteger al 100% contra el malware, su efectividad es relativa.
- Aunque incorporan sistemas heurísticos, firmas genéricas y detecciones basadas en el comportamiento para intentar prevenir nuevos especímenes, en la mayoría de los casos siguen teniendo una respuesta reactiva (no efectiva hasta el estudio de una primera muestra del malware).
- Pese a sus limitaciones, es recomendable su uso para tratar de minimizar las infecciones.

Los programas antiespía impiden que se instalen en nuestro ordenador determinados programas cuyo objetivo es alterar su correcto funcionamiento (impiden acceder a determinadas páginas Web, muestran continuamente ventanas emergentes en nuestro navegador, etc.) o recopilar información del usuario.