TEMA 4. SOFTWARE ANTIMALWARE

É fundamental identificar que recursos e elementos necesitan protección así como coñecer os mecanismos ou ferramentas que podemos empregar para procurar a súa protección .

.

1. Software malicioso

Gracias al desarrollo de las comunicaciones y al creciente uso de la informática en la mayoría de los ámbitos de la sociedad, los sistemas de información se han convertido en objetivo de todo tipo de ataques y son sin duda el principal foco de amenazas. Por esta razón es fundamental identificar qué recursos y elementos necesitan protección así como conocer los mecanismos o herramientas que podemos emplear para procurar su protección.

Con el nombre de **software malicioso** o **malware** agrupamos clásicamente a los virus, gusanos, troyanos y en general todos los tipos de programas que han sido desarrollados para acceder a ordenadores sin autorización, y producir efectos no deseados. Estos efectos se producen algunas veces sin que nos demos cuenta en el acto.

En sus comienzos, la motivación principal para los creadores de virus era la del **reconocimiento público**. Cuanta más relevancia tuviera el virus, más reconocimiento obtenía su creador. Por este motivo, las acciones a realizar por el virus debían ser visibles por el usuario y suficientemente dañinas como para tener relevancia, por ejemplo, eliminar ficheros importantes, modificar los caracteres de escritura, formatear el disco duro, etc.

Sin embargo, la evolución de las tecnologías de la comunicación y su penetración en casi todos los aspectos de la vida diaria ha sido vista por los ciberdelincuentes como un negocio muy lucrativo. Los creadores de virus han pasado a tener una **motivación económica**, por lo que actualmente son grupos mucho más organizados que desarrollan los códigos maliciosos con la intención de que pasen lo más desapercibidos posible, y dispongan de más tiempo para desarrollar sus actividades maliciosas.

Hay varias formas en las que el creador del programa malicioso puede obtener un beneficio económico, las más comunes son:

- **Robar información sensible** del ordenador infectado, como datos personales, contraseñas, credenciales de acceso a diferentes entidades, mail, banca online, etc.
- Crear una **red de ordenadores infectados**, generalmente llamada **red zombi o botnet**, para que el atacante pueda manipularlos todos simultáneamente y vender estos servicios a entidades que puedan realizar acciones poco legítimas como el **envío de spam, de**

mensajes de phishing, acceder a cuentas bancarias, realizar ataques de denegación de servicio, etc.

- Vender falsas **soluciones de seguridad** (rogueware) que no realizan las acciones que afirman hacer, por ejemplo, falsos antivirus que muestran mensajes con publicidad informando de que el ordenador está infectado cuando en realidad no es así, la infección que tiene el usuario es el falso antivirus.
- **Cifrar el contenido** de los ficheros del ordenador y solicitar un rescate económico al usuario del equipo para recuperar la información, como hacen los criptovirus.

2. Clasificación del malware

Los distintos códigos maliciosos que existen pueden clasificarse en función de diferentes criterios, los más comunes son:

- **Virus**: de su analogía con los virus reales ya que infectan otros archivos, es decir, solo pueden existir en un equipo dentro de otro fichero, generalmente son ejecutables: .exe, .src, o en versiones antiguas .com, .bat. También pueden infectar otros archivos, por ejemplo un virus de macro infectará programas que utilicen macros, como los productos Office. Los virus infectan a un sistema cuando se ejecuta el fichero infectado.
- **Gusano**: característica principal es realizar el máximo número de copias posible de sí mismos para facilitar su propagación. Se suelen propagar por los siguientes métodos: correo electrónico, archivos falsos descargados de redes de compartición de ficheros (P2P), mensajería instantánea, etc.
- **Troyano**: código malicioso con capacidad de crear una puerta trasera o backdoor, que permita la administración remota a un usuario no autorizado. Pueden llegar al sistema de diferentes formas, las más comunes son: descargado por otro programa malicioso, al visitar una página web maliciosa, dentro de otro programa que simula ser inofensivo, etc.

Debido a la gran cantidad y diversidad de códigos maliciosos que existen, que muchos de ellos realizan varias acciones y se pueden agrupar en varios apartados a la vez, existen varias clasificaciones genéricas que engloban varios tipos de códigos maliciosos son las siguientes:

- **Ladrones de información** (infostealers): Agrupa todos los tipos de códigos maliciosos que roban información del equipo infectado, son los capturadores de pulsaciones de teclado (**keyloggers**), espías de hábitos de uso e información de usuario (spyware), y más específicos, los ladrones de contraseñas (PWstealer).
- **Código delictivo** (crimeware): Hace referencia a todos los programas que realizan una acción delictiva en el equipo, básicamente con fines lucrativos. Engloba a los ladrones de información de contraseñas bancarias (phishing) que mediante mensajes de correo electrónico no deseado o spam con clickers redireccionan al usuario a falsas páginas bancarias. Dentro de este ámbito encontramos otro tipo de estafas electrónicas (scam) como la venta de falsas herramientas de seguridad (rogueware).

- **Greyware** (o grayware): Engloba todas las aplicaciones que realizan alguna acción que no es, al menos de forma directa, dañina, tan solo molesta o no deseable. Agrupa software de visualización de publicidad no deseada (adware), espías que solo roban información de costumbres del usuario para realizar campañas publicitarias (páginas por las que navegan, tiempo que navegan por Internet...), bromas (joke) y bulos (hoax).

Métodos de infección

Pero, ¿cómo llega al ordenador el malware y cómo prevenirlos? Existen gran variedad de formas por las que todo tipo de malware puede llegar a un ordenador; en la mayoría de los casos prevenir la infección resulta relativamente fácil conociéndolas:

- **Explotando una vulnerabilidad**: cualquier sistema operativo o programa de un sistema puede tener una vulnerabilidad que puede ser aprovechada para tomar el control, ejecutar comandos no deseados o introducir programas maliciosos en el ordenador.
- **Ingeniería social**: apoyado en técnicas de abuso de confianza para apremiar al usuario a que realice determinada acción, que en realidad es fraudulenta o busca un beneficio económico.
- **Por un archivo malicioso**: esta es la forma que tienen gran cantidad de malware de llegar al equipo: archivos adjuntos a través de correo no deseado o spam, ejecución de aplicaciones web, archivos de descargas P2P, generadores de claves y cracks de software pirata, etc.

- **Dispositivos extraíbles**: muchos gusanos suelen dejar copias de sí mismos en dispositivos extraíbles para que, mediante la ejecución automática que se realiza en la mayoría de los sistemas cuando el dispositivo se conecta a un ordenador, pueda ejecutarse e infectar el nuevo equipo, y a su vez, nuevos dispositivos que se conecten.
- **Cookies maliciosas:** las cookies son pequeños ficheros de texto que se crean en carpetas temporales del navegador al visitar páginas web; almacenan diversa información que, por lo general, facilitan la navegación del usuario. Las denominadas cookies maliciosas monitorizan y registran las actividades del usuario en Internet con fines maliciosos, por ejemplo capturar los datos de usuario y contraseña de acceso a determinadas páginas web o vender los hábitos de navegación a empresas de publicidad.

3. Protección y desinfección

Aunque, como se ha visto, existen gran cantidad de códigos maliciosos, es muy fácil prevenir el quedarse infectado por la mayoría de ellos y así poder utilizar el ordenador de forma segura, basta con seguir las recomendaciones de seguridad:

- **Mantente informado** sobre las novedades y alertas de seguridad.
- **Mantén actualizado tu equipo**, tanto el sistema operativo como cualquier aplicación que tengas instalada, sobre todo las herramientas antimalware ya que su base de datos de malware se actualiza en función del nuevo malware que se conoce diariamente.
- Haz **copias de seguridad** con cierta frecuencia, guárdalas en lugar y soporte seguro para evitar la pérdida de datos importantes.
- Utiliza **software legal** que suele ofrecer mayor garantía y soporte.
- Utiliza **contraseñas fuertes** en todos los servicios, para dificultar la suplantación de tu usuario (evita nombres, fechas, datos conocidos o deducibles, etc.).

- Crea diferentes usuarios en tu sistema, cada uno de ellos con los **permisos mínimos necesarios** para poder realizar las acciones permitidas. Utilizar la mayor parte del tiempo usuarios limitados que no puedan modificar la configuración del sistema operativo ni instalar aplicaciones.
- Utiliza **herramientas de seguridad** que te ayudan a proteger y reparar tu equipo frente a las amenazas de la red. Actualizar la base de datos de malware de nuestra herramienta antes de realizar cualquier análisis, ya que el malware muta y se transforma constantemente.
- Analizar nuestro sistema de ficheros con **varias herramientas**, ya que el hecho de que una herramienta no encuentre malware no significa que no nos encontremos infectados. Es bueno el contraste entre herramientas antimalware.
- Realizar periódicamente **escaneo de puertos, test de velocidad y de las conexiones de red** para analizar si las aplicaciones que las emplean son autorizadas. Veremos estos aspectos con más profundidad en el capítulo 6, relativo a redes.
- No debes fiarte de todas las herramientas antimalware que puedes descargarte a través de Internet de forma gratuita o las que te alertan que tu sistema está infectado, ya que algunas de ellas pueden contener **código malicioso**, publicidad engañosa, no ofrecer la protección prometida e incluso dar como resultado falsos positivos (FakeAV). Es el denominado rogueware.

Clasificación de software antimalware

En cuanto a las herramientas disponibles para realizar una correcta prevención y corrección son muy diversas según el frente que se desee atajar. Es importante resaltar que las herramientas antimalware se encuentran más desarrolladas para entornos más utilizados por usuarios no experimentados y por tanto más vulnerables, usualmente entornos Windows, aunque la realidad es cambiante y cada vez son mayor el número de infecciones en archivos alojados en servidores de archivos y de correo electrónico bajo GNU/Linux, y aplicaciones cada vez más usadas como Mozilla Firefox.

- **Antivirus**: programa informático específicamente diseñado para detectar, bloquear y eliminar códigos maliciosos. Es una herramienta clásica que pretende ser un escudo de defensa en tiempo real para evitar ejecuciones de archivos o accesos a web maliciosas. Existen versiones de pago y gratuitas, los fabricantes suelen tener distintas versiones para que se puedan probar sus productos de forma gratuita, y en ocasiones para poder desinfectar el malware encontrado será necesario comprar sus licencias.

  Algunas de las variantes actuales que podemos encontrar son:

  - **Antivirus de escritorio:** instalado como una aplicación, permite el control antivirus en tiempo real o del sistema de archivos.
  - **Antivirus en línea:** cada vez se están desarrollando más aplicaciones web que permiten, mediante la instalación de plugins en el navegador, analizar nuestro sistema de archivos completo.

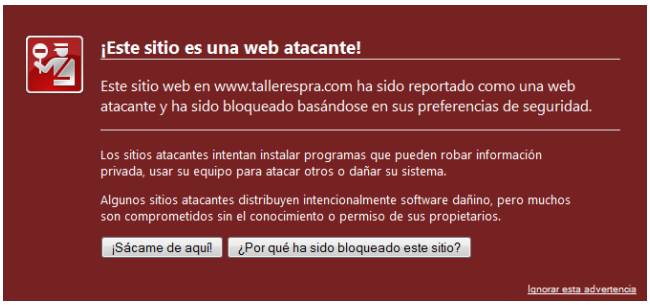
  - **Análisis de ficheros en línea:** servicio gratuito para análisis de ficheros sospechosos mediante el uso de múltiples motores antivirus, como complemento a

tu herramienta antivirus. De esta manera podrás comprobar si algún fichero sospechoso contiene o no algún tipo de código malicioso.

- **Antivirus portable:** no requieren instalación en nuestro sistema y consumen una pequeña cantidad de recursos.
- **Antivirus Live:** arrancable y ejecutable desde una unidad extraíble USB, CD o DVD. Permite analizar nuestro disco duro en caso de no poder arrancar nuestro sistema operativo tras haber quedado inutilizable por algún efecto de malware o no querer que arranque el sistema operativo por estar ya infectado y no poder desinfectarlo desde el mismo.

Entre otras herramientas específicas destacamos:

- **Antispyware**: el spyware, o programas espía, son aplicaciones que se dedican a recopilar información del sistema en el que se encuentran instaladas para luego enviarla a través de Internet, generalmente a alguna empresa de publicidad. Existen herramientas de escritorio y en línea, que analizan nuestras conexiones de red y aplicaciones que las emplean, en busca de conexiones no autorizadas.
- **Herramientas de bloqueo web:** nos informan de la peligrosidad de los sitios web que visitamos, en algunos casos, nos informan de forma detallada, qué enlaces de esas páginas se consideran peligrosos y cuál es el motivo. Existen varios tipos de analizadores en función de cómo se accede al servicio: los que realizan un análisis en línea, los que se descargan como una extensión/plugin de la barra del navegador y los que se instalan como una herramienta de escritorio.



A continuación vamos a realizar varias prácticas que permitan ver el espectro de herramientas fundamentales de escaneo antimalware.

La mejor herramienta antimalware

Conocer qué herramienta se ajusta mejor a mis necesidades en cuanto a consumo de recursos, opciones de escaneo, y cantidad de malware encontrado en test de prueba, no es fácil.

Muchas de las empresas desarrolladoras de software antimalware, muestran estudios en sus propias web demostrando que son mejor que la competencia, pero estos estudios pierden validez al ser conducidos por la propia empresa. También pierden validez los estudios conducidos por los propios usuarios (a pesar de que estos tengan buenos conocimientos de seguridad informática) debido a que generalmente la muestra de virus es muy pequeña o se pueden malinterpretar los resultados, por ejemplo contando la detección de un falso positivo como verdadera cuando no lo es y debería contarse como falsa.

También tenemos que tener en cuenta que la tasa de detección puede variar de mes a mes, debido al gran número de malware que se crea, y aunque la tasa de variaciones suele ser pequeña lo mejor es comparar un estudio con otro un poco más antiguo (meses, no años). Hay que recordar que ningún antivirus es perfecto (no existe el 100% de detección), y además, puede que un antivirus detecte un virus que otro antivirus no detectaría y viceversa.

Los estudios con más validez son los que son hechos por empresas o laboratorios independientes, entre las empresas más importantes y más precisas que realizan los estudios tenemos:

- **AV Comparatives** (http://www.av-comparatives.org).

- **AV-Test.org** (http://www.av-test.org).
- **ICSA Labs** (http://www.icsalabs.com).
- **Virus Bulletin** (http://www.virusbtn.com).
- **West Coast Labs** (http://westcoastlabs.org).

En ocasiones las herramientas antimalware no suponen una solución a una infección, ya que detectan posibles amenazas pero no corrigen el problema. En estos casos es más efectivo un **control a fondo** de los procesos de arranque, los que se encuentran en ejecución y otros archivos del sistema que hagan uso por ejemplo de las conexiones de red establecidas.

0. Índice