Capítulo 4.
SOFTWARE ANTIMALWARE

Autor: Jesús Costas Santos

SW ANTIMALWARE

Índice de contenidos

- 4.1. SOFTWARE MALICIOSO
- 4.2. CLASIFICACIÓN DEL MALWARE
  - 4.2.1. Métodos de infección
- 4.3. PROTECCIÓN Y DESINFECCIÓN
  - 4.3.1. Clasificación del software antimalware
  - 4.3.2. La mejor herramienta antimalware

SW ANTIMALWARE

4.1. SOFTWARE MALICIOSO

- **Software malicioso** o **malware:** clásicamente virus, gusanos, troyanos y todo tipos de programas para acceder a ordenadores **sin autorización**, y producir efectos no deseados.
- **En sus comienzos**, motivación creadores de **virus** era **reconocimiento público**.
- + relevancia + más reconocimiento obtenía su creador. Las acciones a realizar por el virus debían ser visibles por el usuario y suficientemente dañinas.
- **Actualmente: malware como negocio muy lucrativo**. Los creadores de virus han pasado a tener una **motivación económica.**

SW ANTIMALWARE

4.1. SOFTWARE MALICIOSO

- **¿Cómo obtener un beneficio económico?:**
  - **Robar información sensible:** datos personales, credenciales, etc.
  - Crear **una red de ordenadores infectados**, red zombi o *botnet*, el atacante puede manipularlos todos simultáneamente y vender servicios: envío de *spam*, mensajes de *phishing*, acceder a cuentas bancarias, realizar DoS, etc.
  - Vender **falsas soluciones de seguridad** (*rogueware*).
  - Cifrar el contenido de ficheros y solicitar **rescate** económico.

SW ANTIMALWARE

4.2. CLASIFICACIÓN DEL MALWARE

- Clásica:
  - **Virus**: analogía con virus reales ya que infectan otros archivos. Infectan a un sistema cuando se ejecuta el fichero infectado.
  - **Gusano**: realizar el máximo número de copias posible de sí mismos para facilitar su propagación.
  - **Troyano**: código malicioso con capacidad de crear una puerta trasera o *backdoor*, que permita la administración remota a un usuario no autorizado.

SW ANTIMALWARE

4.2. CLASIFICACIÓN DEL MALWARE

- **Clasificaciones genéricas** que engloban varios tipos de códigos maliciosos:
  - **Ladrones de información** (*infostealers*). Roban información del equipo infectado, capturadores de pulsaciones de teclado (*keyloggers*), espías de hábitos de uso e información de usuario (*spyware*), y ladrones de contraseñas (*PWstealer*).
  - **Código delictivo** (*crimeware*). Acción delictiva en el equipo, fines lucrativos. Ladrones de información de contraseñas bancarias (*phishing*) propagados por *spam* con *clickers* a falsas páginas bancarias. Estafas electrónicas (*scam*), venta de falsas herramientas de seguridad (*rogueware*).
  - *Greyware* (o *grayware*). Acción que no es dañina, solo molesta o no deseable. Visualización de publicidad no deseada (*adware*), espías (*spyware*) información de costumbres del usuario para publicidad, bromas (*joke*) y bulos (*hoax*).

SW ANTIMALWARE

Índice de contenidos

- 4.1. SOFTWARE MALICIOSO
- 4.2. CLASIFICACIÓN DEL MALWARE
  - 4.2.1. Métodos de infección
- 4.3. PROTECCIÓN Y DESINFECCIÓN
  - 4.3.1. Clasificación del software antimalware
  - 4.3.2. La mejor herramienta antimalware

SW ANTIMALWARE

4.2.1. Métodos de infección

- ¿Cómo llega al ordenador el *malware* y cómo prevenirlos? Prevenir la infección resulta relativamente fácil **conociéndolas**:
  - **Explotando una vulnerabilidad**: desarrolladores de malware aprovechan vulnerabilidades de versiones de sistema operativo o programa para tomar el control. Solución actualizar versiones periódicamente.
  - **Ingeniería social**: técnicas de abuso de confianza hacer que el usuario realice determinada acción, fraudulenta o busca un beneficio económico.
  - **Por un archivo malicioso**: forma habitual: archivos adjuntos en spam, ejecución de aplicaciones web, archivos de descargas P2P, generadores de claves y *cracks* de software pirata, etc.
  - **Dispositivos extraíbles**: gusanos dejar copias en dispositivos extraíbles, con ejecución automática cuando el dispositivo se conecta a un ordenador, pueda ejecutarse e infectar el nuevo equipo, y a nuevos dispositivos.
  - *Cookies* **maliciosas**: pequeños ficheros de texto en carpetas temporales del navegador al visitar páginas web; almacenan información monitorizan y registran las actividades del usuario en Internet con fines maliciosos.

SW ANTIMALWARE

4.3. PROTECCIÓN Y DESINFECCIÓN

- **Recomendaciones de seguridad**:
  - Mantente informado sobre las novedades y alertas de seguridad.
  - Accede a servicios de Internet que ofrezcan seguridad (HTTPS) y en ordenadores de confianza y seguros.
  - Mantén actualizado tu equipo, sistema operativo y aplicaciones.
  - Haz copias de seguridad con cierta frecuencia, guárdalas en lugar y soporte seguro.
  - Utiliza software legal que suele ofrecer mayor garantía y soporte.
  - Utiliza contraseñas fuertes en todos los servicios.
  - Crea diferentes usuarios en tu sistema, cada uno de ellos con los permisos mínimos necesarios para poder realizar las acciones permitidas.
  - Utiliza herramientas de seguridad antimalware actualizadas periódicamente. Ojo rogueware.Analizar con varias herramientas, contraste *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.

SW ANTIMALWARE

4.3.1. Clasificación del software antimalware

- Herramientas *antimalware* + desarrolladas para entornos + utilizados por usuarios no experimentados y por tanto más vulnerables.
- Entornos Windows, aunque también archivos alojados en servidores GNU/Linux, y aplicaciones navegadores web: Mozilla Firefox.

SW ANTIMALWARE

4.3.1. Clasificación del software antimalware

- **Antivirus**: diseñado para detectar, bloquear y eliminar códigos maliciosos. Versiones de pago y gratuitas, distintas versiones probar productos de forma gratuita, y en ocasiones para poder desinfectar necesario comprar sus licencias. Variantes:
  - Antivirus de escritorio. Ej: Windows: Malwarebytes. GNU/Linux: ClamAV
  - Antivirus en línea: cada vez + utilizadas. Ej: Panda
  - Análisis de ficheros en línea. Ej: Hispasec.
  - Antivirus portable: no requieren instalación.
  - Antivirus Live: arrancable y ejecutable USB, CD o DVD. Ej:AVG
- **Otras herramientas** específicas destacamos:
  - Antispyware: herramientas de escritorio y en línea, que analizan nuestras conexiones de red, en busca de conexiones no autorizadas.
  - Herramientas de bloqueo web.

SW ANTIMALWARE

4.3.2. La mejor herramienta antimalware

- ¿Qué herramienta se ajusta mejor?.
- Empresas desarrolladoras *antimalware*: estudios en sus propias web.
- La tasa de detección varia de mes a mes, gran número de *malware* que se crea.
- Ningún antivirus es perfecto (no existe el 100% de detección).
- Estudios con más validez empresas o **laboratorios independientes**:
  - 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 solución detectan pero no corrigen el problema.

SW ANTIMALWARE

4.3.2. La mejor herramienta antimalware

- En estos casos es más efectivo un **control a fondo** de los procesos de arranque, y uso de las conexiones de red establecidas.
- Windows:
  - msconfig (control de procesos de arranque automático en inicio).
  - Suite de herramientas de control de procesos: Sysinternals.
  - Herramientas de control a fondo del sistema: empresa Trend Micro **herramienta HiJackThis.**
  - Comando netstat: control de conexiones de red.

SW ANTIMALWARE

DIRECCIONES DE INTERÉS

- Blog con multitud de noticias y enlaces sobre seguridad informática:
  - http://www.inteco.es/Seguridad/Observatorio/BlogSeguridad
- CERT - INTECO – Centro de Respuesta a Incidentes de Seguridad. Instituto Nacional de Tecnologías de la Comunicación:
  - www.cert.inteco.es/
- Comparativas de software antivirus gratuitos:
  - http://www.descarga-antivirus.com/
- Web sobre software antimalware:
  - http://www.antivirusgratis.com.ar/
- Valida el nivel de seguridad y confiabilidad de las URL visitadas. McAfee:
  - www.siteadvisor.com

SW ANTIMALWARE

DIRECCIONES DE INTERÉS

- Listado con software malware y software antimalware falso (Rogue o Fakeavs)
  - www.Forospyware.com
- Artículo para prevenir y curar virus en el arranque de dispositivos USB.
  - www.cristalab.com/tips/como-eliminar-virus-autorun.inf-de-un-dispositivo-usb-c76436l/
- Historia del malware
  - http://www.pandasecurity.com/spain/homeusers/security-info/classic-malware/
- Web sobre software antimalware:
  - http://www.antivirusgratis.com.ar/
- Comprobar la confiabilidad de aplicaciones instaladas, mediante la revisión de la lista actualizada:
  - http://www.forospyware.com/t5.html

SW ANTIMALWARE

SOFTWARE

- Útiles gratuitos de seguridad informática categorizados, en CERT - INTECO – Centro de Respuesta a Incidentes de Seguridad. Instituto Nacional de Tecnologías de la Comunicación:
  - http://cert.inteco.es/software/Proteccion/utiles_gratuitos/
- Sección de software gratuito antimalware en Softonic:
  - http://www.softonic.com/s/malware
- **Revealer Keylogger:** Keylogger
  - http://www.logixoft.com/
- **ClamAv**, y su versión gráfica **Clamtk**: antivirus para entornos GNU/Linux.
  - http://es.clamwin.com/
- **AVG Rescue CD:** distribución arrancable desde USB y CD para análisis en modo Live de antimalware.
  - http://www.avg.com/ww-es/avg-rescue-cd
- **Sysinternals**: Paquete de herramientas de análisis a bajo nivel, del sistema operativo Windows.
  - http://technet.microsoft.com/es-es/sysinternals/default
- **HiJackThis**: Analizador de aplicaciones, servicios activos, cambios de configuración producidos por malware, en el sistema operativo Windows. Producto de Trend Micro.
  - free.antivirus.com/hijackthis/

SW ANTIMALWARE

SOFTWARE ANTIVIRUS

- AVG Anti-Virus 9.0
  - http://free.avg.com/ww-es/antivirus-gratis-avg
- Avast
  - http://www.avast.com/free-antivirus-download#tab4
- Avira
  - http://www.free-av.com/en/download/1/avira_antivir_personal__free_antivirus.html
- Microsoft *Security Essentials*
  - http://www.microsoft.com/Security_Essentials/
- Panda Cloud Antivirus
  - http://www.cloudantivirus.com/es/
- USB Vaccine USB
  - http://www.pandasecurity.com/spain/homeusers/downloads/usbvaccine/

SW ANTIMALWARE

SOFTWARE Antiespías-antimalware

- Malwarebytes
  - http://www.malwarebytes.org/mbam.php
- Spyware Terminator
  - http://www.spywareterminator.com/es/
- Ad-Aware.
  - http://www.lavasoft.com/products/ad_aware_free.php?t=overview
- Spybot
  - http://www.safer-networking.org/es/index.html
- Windows Defender
  - http://www.microsoft.com/downloads/details.aspx?displaylang=es&FamilyID=435bfce7-da2b-4a6a-afa4-f7f14e605a0d

SW ANTIMALWARE

NOTICIAS

- **Panda Security y Defence Intelligence ayudan al FBI a arrestar a cibercriminales – Hacker arrestado en Eslovenia:**
  - http://prensa.pandasecurity.com/2010/07/panda-security-y-defence-intelligence-ayudan-al-fbi-a-arrestar-a-cibercriminales-%E2%80%93-hacker-arrestado-en-eslovenia/
- **Artículo sobre la historia de los virus:**
  - http://www.nod32-la.com/tutorials/cronologia_de_los_virus_informaticos.pdf
- **Noticia "Madrid capital del SPAM" :**
  - http://www.csospain.es/Madrid,-capital-del-spam-/seccion-alertas/noticia-91980
- **Artículo sobre procesos legítimos del sistema operativo en sistemas Windows de ESET:**
  - http://blogs.eset-la.com/laboratorio/2009/05/07/procesos-legitimos-nativos-sistema-operativo-i/