Software Malicioso

Informática General

Contenidos

Software Malicioso

Es un software que tiene como objetivo dañar un ordenador o infiltrarse en él, sin el conocimiento de su propietario. Las finalidades son muy diversas encontrándonos desde un Troyano hasta un Spyware.

- Adware
- Backdoor
- Bomba Fork
- Bomba Lógica
- Bots
- Caballo de Troya (Troyano)
- Cryptovirus

Software Malicioso

- Exploit
- Pharming
- Phishing
- Rootkit
- Spam
- Spyware
- Virus
- Worms (gusanos)

Software Malicioso

Adware

- Software que muestra publicidad en el equipo sin permiso.
- Suele venir acompañando a software gratuitos.
- En ocasiones recogen información del usuario sin su permiso y la mandan a terceros.

Backdoor (Puerta Trasera)

- Software que permite el acceso a un equipo. Incluido en el propio software, porque así lo quiso el desarrollador.
- Dos tipos de puertas traseras:
  - Son manualmente insertadas dentro de otro software.
  - Se ejecuta como procedimiento de inicialización del sistema.

Software Malicioso

Bomba Fork

- Se replica velozmente dentro de un equipo.
- Termina saturando la memoria RAM y capacidad de procesamiento.
- Su ataque se basa en la Denegación de Servicio (DoS) atacando servidores o a la red de computadores.

Bomba Lógica

- Permanece oculta hasta que se da una serie de condiciones.
- Tras cumplirse dicha ejecución, se produce una serie de acciones perjudiciales.

Software Malicioso

Bots

- Programas que se encargan de hacer funciones rutinarias en el equipo que pueden **ser perjudiciales o no**.
- Destacar **AVBOT**, robot creado por Emilio José Rodríguez Posada (alumno de la UCA) para detectar actos vandálicos en Wikipedia España.
- Entre las posibles acciones de un bot perjudicial:
  - Crear cuentas de e-mail o cuentas de usuario.
  - Realizar acciones enviadas desde otra máquina remota.
  - Crear y expandir spam en redes sociales.

Caballo de Troya (Troyano)

- Software dañino disfrazado o incluido en un software legítimo.
- No tiene capacidad para replicarse.
- Se encubre detrás de otro software para dañar e infectar.

Software Malicioso

Cryptovirus

- Busca y cifra los archivos del registro del disco infectado.
- Su fin es solicitar dinero para poder descifrar los archivos.

Exploit

- Ataca una vulnerabilidad particular de un sistema operativo o un programa.
- No siempre son malos, en ocasiones son creados por expertos en seguridad informática para demostrar la existencia de vulnerabilidades en un sistema.

Software Malicioso

Pharming

- Suplanta al DNS para conducir a páginas webs falsas, alterando las tablas del propio equipo.
- Imitando webs bancarias roban información de cuentas corrientes.

Phishing

- Técnica que se basa en el envío de e-mail o direcciones de webs, cuyo fin es estafar.
- Con imitaciones de webs o e-mail pretenden conseguir los datos de cuentas bancarias.
- Para engañar al usuario utilizan:
  - El miedo (si no entras en tu cuenta, esta será cerrada).
  - Lo cotidiano (con botones y mensajes de las webs originales).
  - Confianza (avisando de la existencia de webs fraudulentas).

Software Malicioso

Rootkit

- Herramienta o grupo de ellas que se encargan de ocultar o esconder otros programas, procesos, archivos...
- Esto le permitirá al intruso meterse en nuestro sistema y realizar acciones sobre él.

Spam

- También conocidos como e-mails basura.
- Usados por grandes empresas para mandar publicidad.
- Actualmente:
  - La mayoría de los servidores de correo electrónico tienen filtros.
  - Además existe una legislación contra el spam.

Software Malicioso

Spyware

- Aplicaciones que se dedican a recopilar información del sistema en el que se encuentran instaladas.
- Rara vez el usuario es consciente de ello.
- Normalmente trabajan y contaminan sistemas como lo hacen los caballos de Troya.

Virus

- Código ejecutable que infecta otros programas para propagarse, y que al activarse realiza algún tipo de acción no autorizada (normalmente dañina).
- Los virus pueden reemplazar ficheros o ejecutables, destruir datos o simplemente ser molestos.

Software Malicioso

Virus (cont.)

- Infecta al equipo reemplazando archivos ejecutables por otros ya infectados.
- Un virus se propaga por nuestro equipo infectando al resto de ficheros, pero no duplicándose a sí mismo.
- Un virus puede propagarse por la red.

Worms (gusanos)

- Los gusanos se propagan por la red y no dependen de archivos portadores para poder contaminar otros sistemas.
- Éstos pueden modificar el sistema operativo con el fin de autoejecutarse.
- El caso más conocido es el del gusano Blaster que se distribuyó por Internet rápidamente gracias a una vulnerabilidad del sistema operativo Windows.

Prevención

- La primera fase que un Ingeniero Informático debe afrontar es prevenir el riesgo.
- La prevención se puede realizar de diferentes formas:
  - A nivel de Software
  - A nivel de Usuario

Prevención

- Existen diferentes tipos de software especializados. Con ellos se podrá combatir de manera más adecuada el software malicioso.
- Tipo de software:
  - Antivirus
  - AntiSpam
  - Firewall
  - ...

Prevención

Antivirus

Software especializado en escanear, detectar y desinfectar diferentes tipos de virus.

- Ejemplo de Antivirus:
  - **Avast! Antivirus (Versiones para Linux)**
  - Panda Antivirus
  - AVG Antivirus
  - Norton Antivirus

Prevención

AntiSpam

Software encargado de detectar y evitar cualquier tipo de correo electrónico basura que intente entrar en el sistema.

- Ejemplo de AntiSpam:
  - **SpamBayes (GPL)**
  - ActionMail
  - Mailwasher
  - SpamFighter

Prevención

Firewall

Pared lógica y/o física que se sitúa entre los equipos que se desean proteger y el módem que nos dará acceso a Internet.

- Ejemplo de Firewall:
  - **Firewall PAPI (GPL)**
  - Ashampoo Firewall
  - Comodo Firewall Pro
  - Outpost Firewall

Prevención

También es importante realizar una prevención a nivel del usuario del sistema.

- Sobre el sistema operativo:
  - Limitar las acciones del usuario sobre el sistema.
  - Diferenciar entre usuarios habituales y administrador.
- Conocimiento del usuario.
  - Enseñar los peligros que supone Internet.
  - Enseñar cómo poder evitarlo y detectar un posible peligro.

Prevención

- Realizar periódicamente copias de seguridad
- No usar copias piratas de programas
- Activar los dispositivos de protección física en los discos
- Trabajar con privilegios de usuario normal
- No arrancar con discos no originales
- Activar las medidas de seguridad de las aplicaciones macro
- Conocer los nuevos códigos malignos

Diagnóstico

- El ordenador funciona lento y se bloquea
- Algunos programas no pueden ejecutarse
- Aumento de los sectores ocultos y menos RAM libre
- Cambios en los atributos de los ficheros y aparición de ficheros con el mismo nombre
- Excesiva actividad en los discos
- Sistema de arranque cambiado y aviso del antivirus
- Word nos pide guardar cambios que no hemos realizado

Forma de Actuar

Cuando un sistema ya está infectado por un software malicioso, ¿cómo debe actuar un Ingeniero para solucionarlo?:

1. Aislar el equipo (desconectándolo de la red). Si éste aún no ha infectado la red, el software malicioso quedará localizado a nivel local.
2. Identificar qué tipo de software malicioso nos ha atacado o infectado.
3. Una vez que sepamos a qué nos enfrentamos actuaremos en consecuencia:
   - Si es un virus, debemos desinfectar los archivos dañados y eliminar la raíz del virus.
   - Si es un spam, debemos reconfigurar el antispam enseñándole nuevas normas de filtrado.
   - ...

Ejemplos Reales

Desde hace años, existen una gran cantidad de ejemplos reales que han causado daño tanto a particulares como a grandes empresas e instituciones. Estos son algunos ejemplos:

- Brain, año 1986 - Virus
- ILoveYou, año 2000 - Gusano
- Code Red, año 2001 - Gusano
- SQL Slammer, año 2003 - Gusano
- Sasser, año 2004 - Gusano
- Sony RootKit, año 2005 - Rootkit
- Conficker, año 2008 - Gusano
- Stuxnet, año 2010 - Gusano

Referencias

- http://www.alerta-antivirus.es
- http://www.wikipedia.org
- http://www.securitybydefault.com/
- http://www.virustotal.com
- http://ddanchev.blogspot.com/
- http://www.securelist.com/
- http://vmyths.com/
- http://www.f-secure.com/weblog/
- http://www.f-secure.com/en_EMEA/security/security-lab/