Universidad de Oviedo

Departamento de Informática

Campus de Gijón

Malware y Anti-Malware

Presentación

Daniel F. García

Concepto y tipos de malware

Definición

Malware es cualquier software que impide el funcionamiento normal del computador y que generalmente se ejecuta sin el consentimiento del usuario

Malware es una Contracción o Acrónimo de "**Mal**icious Soft**ware**"

Tipos

Tipos de Malware →
- Virus
- Puertas traseras (*Backdoors, Trapdoors*)
- Troyanos (*Trojans*)
- Gusanos (*Worms*)
- Bombas lógicas o de tiempo (*Time/Logic bombs*)
- Spyware, Adware, Stealware

Estado

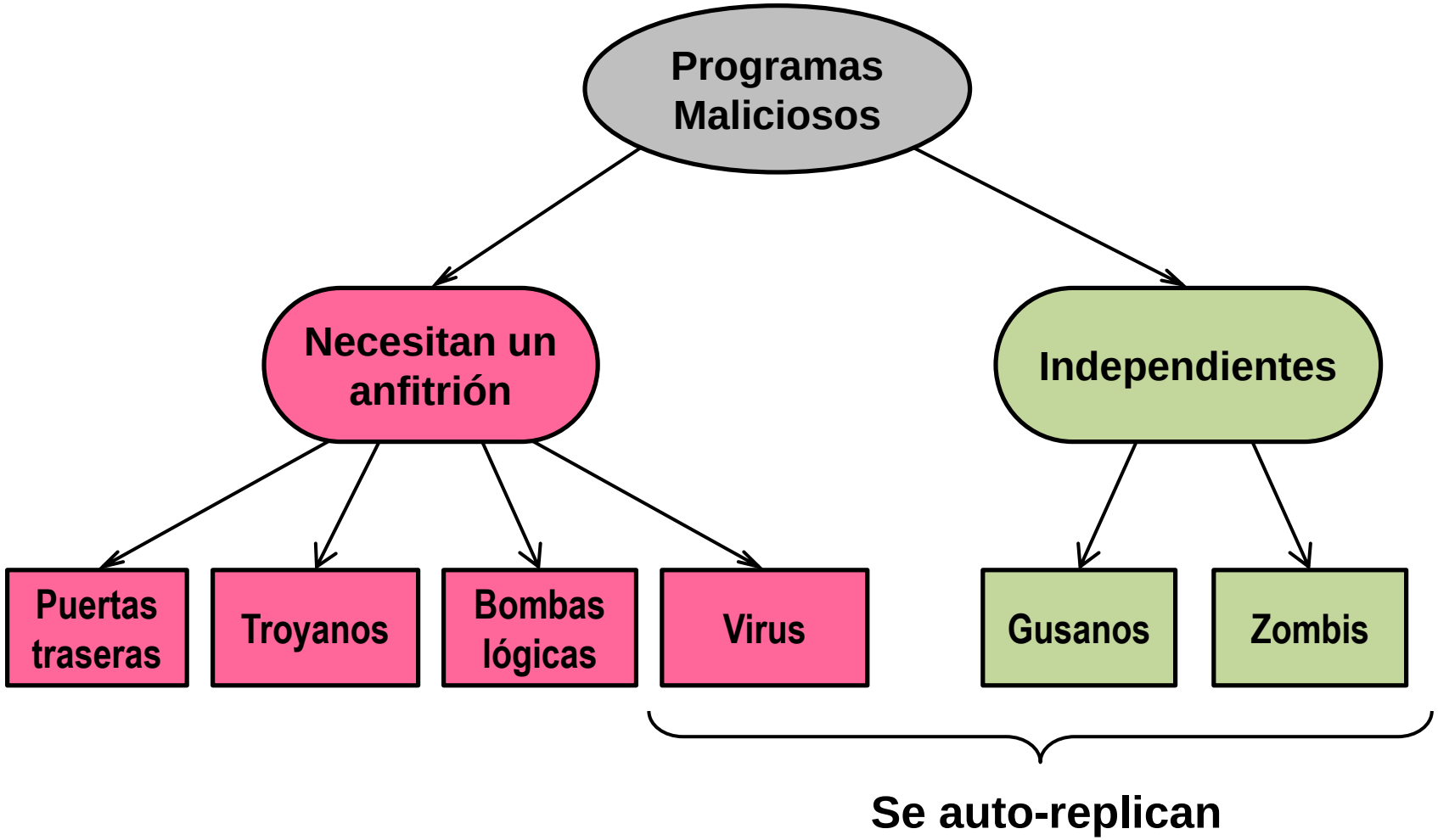
Cuando un malware comienza a infectar un gran número de equipos se dice que está "*in the wild*"
Un malware que reside en las colecciones de los investigadores se dice que está "*in the zoo virus*"

Hay decenas de miles de malware identificados pero solo unos pocos son preocupantes → "*wild list*"

Niveles de amenaza

Ninguna → Malware que funciona mal o son bromas pesadas (*hoax*)
Baja → Malware que requiere de la acción humana para propagarse
Media → Malware que se auto-propaga lentamente y hace pocos o ningún daño
Alta → Malware que se auto-propaga rápidamente o hace daños considerables

Una clasificación del malware



Virus

Definición

Un virus es un malware que se ejecuta en un computador sin el consentimiento del usuario para producir daños y tiene la capacidad de hacer copias de si mismo para propagarse

Los virus suelen añadir su código a otros programas (los infectan) para facilitar su propagación

Componentes básicos de un virus

1) Un mecanismo de replicación
2) Una tarea que se ejecuta en un computador para dañarlo
3) Un disparador (*trigger*) diseñado para activar la replicación y/o la tarea

Estos tres componentes pueden tomar multitud de formas y comportarse de diversas maneras

Los **virus polimórficos** son aquellos que cambian su forma al infectar un nuevo sistema

Virus: Fases de operación

1. **Fase latente (*dormant phase*)**
   - El virus está inactivo y será activado por algún evento futuro
   - No todos los virus tienen esta fase

2. **Fase de propagación (*propagation phase*)**
   - El virus se copia a si mismo en otros ejecutables, zonas del sistema o discos
   - A esta fase se la denomina comúnmente como fase de infección
   - Al copiarse puede mutar (cambiar de forma)

3. **Fase de activación (*triggering phase*)**
   - El virus se activa para realizar la función para la que fue diseñado
   - La activación puede ser provocada por una gran variedad de eventos

4. **Fase de ejecución (*execution phase*)**
   - El virus realiza su función, dañina o no

Virus: Estructura de un ejecutable

Virus genérico

```
    program V :=

{goto main;
    1234567;

    subroutine infect-executable :=
        {loop:
        file := get-random-executable-file;
        if (first-line-of-file = 1234567)
           then goto loop
           else prepend V to file; }

    subroutine do-damage :=
        {whatever damage is to be done}

    subroutine trigger-pulled :=
        {return true if some condition holds}

main:   main-program :=
        {infect-executable;
        if trigger-pulled then do-damage;
        goto next;}

next:

}
```

La detección es fácil: el programa infectado es mas largo que el programa original

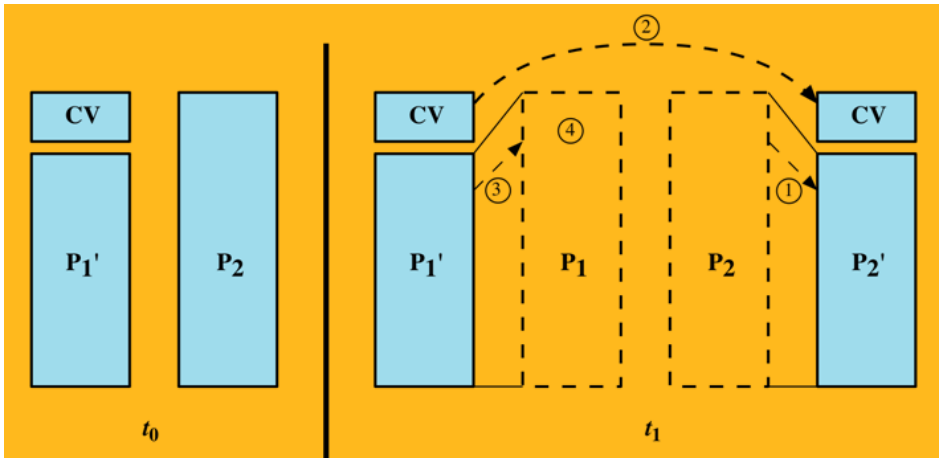
Virus compresor

```
    program CV :=

{goto main;
    01234567;

    subroutine infect-executable :=
          {loop:
               file := get-random-executable-file;
          if (first-line-of-file = 01234567) then goto loop;
        (1)    compress file;
        (2)    prepend CV to file;
        }

main:   main-program :=
          {if ask-permission then infect-executable;
        (3)    uncompress rest-of-file;
        (4)    run uncompressed file;}
        }
```



Stallings – Computer Security

Tipos de Virus 1

Se clasifican los virus en función del tipo de programa que infectan

Virus de sector de arranque

Se instala en (infecta a) el primer sector de una unidad de disco

El primer sector contiene el programa de arranque y la tabla de particiones de la unidad

Al arrancar el computador lo primero que se carga en memoria y se ejecuta es el virus

Luego el virus ejecuta el programa de arranque que ha sido guardado en otro sector de la unidad

Se propagan copiándose en disquetes (obsoleto) o lápices USB → Mecanismo lento

Virus de archivo ejecutable

Se instala en (infecta a) un archivo ejecutable que actúa como portador

Al ejecutar el programa del archivo (.exe, .com, .sys, .dll) también se ejecuta el virus

El virus debe diseñarse para cada tipo de ejecutable (para cada sistema operativo)

Tipos de virus 2

Virus de macro

Se instala en (infecta a) documentos (Word, Excel)

Los virus de macro son **multiplataforma** → Pueden afectar a cualquier plataforma donde se pueda utilizar Word, Excel, etc., como Windows, Mac, …

Ejemplo: Macro-Virus de MS-Word

Dentro de un documento de Word se almacenan macros para automatizar tareas repetitivas

Existen macros que se ejecutan de forma automática, al abrir un documento (*Auto-Open*), al cerrar un documento (*Auto-Close*) y en otros casos (*Auto-Save*)

Generalmente, los virus de macro utilizan las macros automáticas que se ejecutan cuando se abre el documento y graban la macro infectada en la plantilla NORMAL.DOT que contiene las macros comunes a todos los documentos (esta es la fase de infección del sistema)

Desde la plantilla NORMAL.DOT la macro infectada pasa a cualquier documento que se abra Al guardar el documento éste queda infectado (esta es la fase de propagación del virus)

El virus se propaga a otros sistemas que reciben documentos infectados por e-mail, lápiz USB ...

Tipos de virus 3

Virus de correo electrónico

Se instala en (infecta a) el programa de correo electrónico de un sistema

Generalmente, se replica enviándose a si mismo a las direcciones de correo electrónico almacenadas en la libreta de direcciones del programa de correo

Se suele diferenciar entre los que envían correo de forma masiva y lentamente (porque suponen niveles de amenaza distintos)

Los virus de envió masivo de correo (*mass mailers*) tratan de:
- Saturar las carpetas de correo de los usuarios
- Colapsar a los servidores de correo electrónico

Ej. Virus Melissa (1999)

Es un virus de Macro de MS-Word que envía 50 e-mails a las 50 primeras direcciones que encuentra en outlook adjuntando un fichero Word infectado

Puertas traseras

Definición

Una puerta trasera en un sistema/aplicación es un mecanismo que permite **eludir el proceso normal de autenticación** para acceder al sistema/aplicación

El que conoce la puerta trasera puede acceder al sistema/aplicación sin pasar por los controles normales de acceso y además intenta pasar inadvertido

La puerta trasera puede tomar la forma de { Un programa instalado / Un rootkit

Ejemplos

- Una puerta trasera en un sistema de login puede consistir en una combinación de usuario y contraseña codificados en el software de login
- Se puede insertar una puerta trasera en el núcleo de un SO: una función que al llamarla proporciona los privilegios de root
- Los programadores usan puertas traseras para acceder a las aplicaciones para depurarlas y testearlas, pero las puertas traseras son amenazas si se dejan en los programas de producción

Tipos

Puerta trasera **simétrica**: cualquiera que encuentre la puerta trasera puede usarla
Puerta trasera **asimétrica**: solo puede usarla el que la ha insertado (solo él conoce cierta información)

Troyanos

Definición

Un troyano es un código malicioso que permite la **ejecución de comandos** en el computador infectado **sin la autorización** del propietario del computador

El troyano se suele presentar al usuario del computador como un programa o herramienta muy útil y generalmente gratuita que contiene al troyano (por ejemplo un antivirus o un juego)

Funcionamiento

En principio, los troyanos no se replican a si mismos

El troyano puede realizar acciones dañinas directamente o instalar una puerta trasera para dar acceso (remoto generalmente) a un hacker para que realice manualmente las tareas dañinas:

- Borrar o renombrar archivos
- Cargar archivos
- Modificar el registro del SO
- Apagar o reiniciar el computador
- Robar contraseñas e información confidencial
- Registrar pulsaciones de teclas (*keystroke logging*)
- Anonimizar la navegación por Internet
- Deshabilitar antivirus, firewalls, etc., …

Ej. Troyano Zeus (2007)

Gusanos

Definición

Un gusano (*worm*) es un malware que **se replica** a si mismo y utiliza una red para **enviar copias** de si mismo a otros computadores sin necesitar la intervención del usuario

El proceso de auto-replicación puede ser indefinido o estar limitado por un temporizador interno

Funcionamiento

Los gusanos no necesitan introducirse en un programa, al contrario que los virus
Pero necesitan explotar alguna vulnerabilidad del SO para instalarse

Muchos gusanos han sido diseñados exclusivamente para propagarse
Pero algunos gusanos transportan una carga (*payload*) para hacer alguna tarea:

- Borrar archivos en el computador anfitrión
- Cifrar los archivos y extorsionar al usuario para descifrarlos
- Enviar documentos por e-mail
- Instalar una Puerta Trasera en el computador

Ej. WannaCry ransomware CryptoWorm (2017)

Ej. Stuxnet (2017) para PLCs

Así se crea una red de computadores controlados denominada botnet = red de ro**bot**s (zombis)
Generalmente las botnets se utilizan para enviar spam y realizar ataques de denegación de servicio

Ej. Zeus botnet (2007) basada en el troyano Zeus

Bombas lógicas o de tiempo

Definición

Una bomba de tiempo (o bomba lógica) es un malware que una vez instalado **permanece latente** hasta que es **activado por un evento** o circunstancia específica

La activación se puede producir en una fecha y hora concretas o bien cuando se ha acumulado un determinado número de arranques del sistema

¿Quién usa y por qué bombas de tiempo?

Muchos programadores descontentos han instalado bombas de tiempo en los sistemas de su empresa para tomar **represalias** contra la dirección

También se instalan bombas de tiempo para realizar **extorsiones**

Las empresas que venden software pueden instalar estas bombas que desactivan si cobran el software o las cuotas de mantenimiento en los plazos estipulados (Esta práctica es ilegal)

Los virus y los gusanos se pueden utilizar para instalar bombas de tiempo

Spyware

Definición

El término spyware se utiliza para describir cualquier software malicioso que **recopila información** sobre una persona u organización sin su conocimiento ni consentimiento

Típica información recopilada:

- La secuencia de teclas pulsadas por el usuario
- La lista de sitios web visitados por el usuario
- Las aplicaciones instaladas en el computador
- Información personal del usuario (ej.: números de tarjetas de crédito)

La información recopilada se vende a entidades interesadas en la publicidad
Y se combina con otra información de los usuarios para desarrollar perfiles que se venden

Funcionamiento

El spyware se instala de modo inadvertido al usuario (por ejemplo lo instala un virus) o bien lo instala el propio usuario al instalar una nueva herramienta que ya lo contiene

En general, el spyware no suele auto-replicarse (comportamiento contrario al de los virus y gusanos)
Pero es posible usar virus o gusanos como elementos de transporte y propagación

En general el uso de spyware **viola** leyes sobre la **privacidad** de la información y constituye un delito

Adware

Definición

El término adware se utiliza para describir cualquier software malicioso que descarga y visualiza **anuncios** automáticamente en un computador con o sin consentimiento del usuario

La palabra adware es una contracción de "*advertising-supported software*"

La mayoría del adware es también spyware porque los anuncios que muestra a los usuarios se basan en los datos obtenidos espiando a los propios usuarios

Hay programas que muestran anuncios como una alternativa a cobrar por su utilización (estos programas pueden considerarse adware pero no spyware)

Funcionamiento típico

Los WebSites grandes suelen solicitar información al usuario (incluso abrir una cuenta)

Cuando el usuario vuelve a visitar el WebSite, éste le envía una cookie con los datos

El WebSite indica que todo esto sirve para personalizar/mejorar el servicio

Pero el WebSite puede usar la información del usuario para añadir banners en ciertos instantes

Los propietarios del WebSite suelen publicar una política que asegura la privacidad de los usuarios

Contramedidas para virus

La contramedida fundamental es utilizar un programa “Anti Virus”

Fases básicas de funcionamiento de un antivirus:

1.- Detección

Una vez que ha ocurrido una infección → Determinar que efectivamente se ha producido y Localizar el programa infectado por el virus

2.- Identificación

Hay que identificar el virus específico que ha infectado al programa

3.- Eliminación

Hay que eliminar el virus del programa infectado y devolverlo a su estado original

Si la detección tiene éxito pero la identificación o la eliminación no son posibles …
Hay que borrar el programa infectado y recargar una versión limpia desde una copia de seguridad

Antivirus: Generación 1ª

Algunos autores distinguen 4 generaciones al menos

1ª Generación: escáneres sencillos

Estos escáneres **utilizan firmas** (*signatures*) para identificar a los virus

Una firma es cualquier secuencia de bits de un virus que puede usarse para identificar con precisión la presencia del virus en un archivo o en una zona de memoria

Hay diversas técnicas para seleccionar una firma (Ej: usando modelos de Markov)

La firma debe ser de suficiente **longitud** para evitar **falsas detecciones**
(Pero no siempre la firma más larga es la mejor)

Cada escáner utiliza un método para obtener las firmas y luego buscarlas
Un mismo virus tiene una firma distinta para cada antivirus

Estos escáneres **funcionan buscando** las firmas disponibles en archivos o en memoria

Problema: solo detectan los virus ya conocidos y que disponen de sus firmas

También se suele hablar de Definiciones de Virus (*virus definitions*) para referirse a la base de datos que contiene todas las firmas de virus utilizadas por un determinado antivirus

Antivirus: Generación 2ª

2ª Generación: escáneres heurísticos

Estos escáneres no buscan una firma específica para cada virus

Estos escáneres **utilizan reglas** heurísticas para buscar los virus

Una regla consiste en analizar bloques de código que frecuentemente están asociados con virus

Ej: Buscar el inicio del bucle de cifrado utilizado por un virus polimórfico y descubrir la clave
Con la clave, el escáner puede descifrar el virus e identificarlo

Estos escáneres **también comprueban la integridad** de los programas (archivos ejecutables)

Técnica: añadir una suma de comprobación (*checksum*) a cada programa

Si un virus infecta un programa sin cambiar la suma de comprobación
Cualquier comprobación posterior de integridad detectará la modificación del programa

PERO … El virus podría corregir la suma de comprobación tras infectar al programa

SOLUCIÓN: Calcular un hash del programa y cifrarlo con una clave separada del programa

Esto es simplemente firmar digitalmente el programa
Pero sin la clave … ¡el virus no podrá recalcular la firma!

Antivirus: Generación 3ª

3ª Generación: monitores de actividades

Estos antivirus son programas que residen en memoria e **identifican** a los virus **por** sus **acciones** (en vez de por su firma en un programa infectado)

Ventaja:

NO es necesario desarrollar una base de datos de firmas y heurísticas para muchos virus
Sólo hay que identificar el pequeño conjunto de acciones que indican un intento de infección

Estos antivirus reciben diversos nombres:

Trampas para actividades (*Activity Traps*)
Monitores de actividades/comportamientos (*Activity/Behavior Monitors*)
Bloqueadores de comportamientos (*Behavior-Blocking Software*)

Actividades típicas a monitorizar:

- Apertura, visualización, eliminación y modificación de **archivos**
- Formateo de unidades de **disco** y otras operaciones de disco irrecuperables
- Modificación de archivos **ejecutables** o macros
- Modificación de parámetros críticos del **sistema**, como la configuración de arranque
- Ejecución de comandos de **e-mail** o mensajería para enviar ejecutables
- Iniciación de **comunicaciones** por la red

Antivirus: Generación 4ª

4ª Generación: combinaciones

Estos antivirus utilizan conjuntamente las técnicas y métodos de las generaciones previas

Incluyen componentes para:

- Escanear archivos o memoria buscando firmas (definiciones) de virus
- Buscar virus en ejecutables usando heurísticos
- Comprobar la integridad de ejecutables verificando firmas digitales del código
- Monitorizar las actividades de los programas
- Controlar el acceso a funciones del sistema

Contramedidas para gusanos

Las técnicas para combatir a los gusanos son similares a las usadas para combatir a los virus

Cuando el gusano ya reside un computador se pueden usar las técnicas antivirus para detectarlo

Como la propagación de los gusanos genera una gran actividad en la red …
La monitorización de esa actividad es la base de la defensa contra los gusanos

Las técnicas de defensa contra los gusanos incluyen:

1) Filtrado de los escaneos de gusanos basado en firmas: Un filtro usa las firmas de los gusanos para prevenir los escaneos que entran o salen de una red o computador
2) Contención basada en filtros: Un filtro comprueba un mensaje para ver si contiene un gusano
3) Contención basada en la clasificación de la carga útil: Un filtro examina los paquetes para ver si contienen un gusano utilizando técnicas de detección de anomalías
4) Detección de escaneo mediante umbrales de aleatoriedad de rutas: Explota la aleatoriedad para elegir destinos a los que conectarse como una forma de detectar si un escáner esta funcionando
5) Limitación de frecuencia: Limita la frecuencia de escaneado desde un computador infectado
6) Frecuencia de parada: Bloquea inmediatamente el tráfico de salida cuando se supera un umbral en la frecuencia de conexiones de salida o en la diversidad de los intentos de conexión

Fabricantes de Anti-Malware

https://www.avast.com/

https://www.mcafee.com/

https://www.avg.com/
https://free.avg.com/

https://www.avira.com/

https://www.bitdefender.es/

https://www.trendmicro.com/

https://www.eset.com/

https://www.kaspersky.com/

https://www.pandasecurity.com/

https://es.norton.com/

https://www.broadcom.com/products/cyber-security

Cuestión

Los siguientes fragmentos de código muestran una secuencia de instrucciones de un virus y una versión metamórfica del virus.

Código original	Código metamórfico

`mov eax, 5`
`add eax, ebx`
`call [eax]`
	`mov eax, 5`
	`push ecx`
	`pop ecx`
	`add eax, ebx`
	`swap eax, ebx`
	`swap ebx, eax`
	`call [eax]`
	`nop`

Describe el efecto producido por el código metamórfico.