Malware

Mikel Egaña Aranguren

mikel-egana-aranguren.github.io

mikel.egana@ehu.eus

Universidad del País Vasco
Euskal Herriko Unibertsitatea
BILBOKO INGENIARITZA ESKOLA
ESCUELA DE INGENIERÍA DE BILBAO

Malware

https://doi.org/10.5281/zenodo.4302267

https://github.com/mikel-egana-aranguren/EHU-SGSSI-01

Definiciones

Malware: un programa que provoca daños y pérdidas a otros programas o a un usuario

Tipos de malware clásicos: Virus, gusanos, troyanos, bombas lógicas, etc.

Tipos de malware de nueva aparición: Spyware, backdoors, keyloggers, rootkits, exploits, etc.

Definiciones

Los tipos de malware no siempre están perfectamente diferenciados

Se suelen usar palabras genéricas (virus, troyano, etc.) sin prestar atención a sus características

Virus

Programa informático con capacidad de modificar ficheros, borrar datos, duplicarse y diseminarse

Virus

Chernobyl (Hay mas de 30 variantes):

- Creado en 1998 en Taiwan
- Infecta archivos ejecutables en sistemas Windows 9x
- Residente en memoria, se activa en una fecha determinada
- Sobreescribe documentos, formatea el MBR (Master Boot Record)
- Flashea la BIOS dejando el PC inservible

Gusanos

Programa informático cuyo principal objetivo es la reproducción

La principal diferencia con los virus es que no infecta otros ficheros

Gusanos

Netsky:

- Se propaga por redes de correo o P2P. Una vez infectado un ordenador, se autodistribuye a todos los contactos que encuentre
- Falsifica la dirección del remitente
- Hay que ejecutar el fichero para infectarse

Gusanos

I love U (2000)

Se recibía un correo con una "carta de amor" adjunta

La carta era una macro VBS que al abrirla reenviaba el gusano a todos los contactos

Instalaba un virus que borraba ficheros y ocultaba otros

Infectó a 50 millones de máquinas en una semana

Gusanos

Sasser (2004)

Se aprovecha de un agujero de seguridad de algunas versiones de Windows

(XP entre ellas)

No necesita interacción por parte del usuario para infectarse

Crea un servidor FTP para que otras máquinas se conecten y se infecten

Provoca reinicios no deseados

Gusanos

WannaCry (2017)

Se aprovecha de una vulnerabilidad de Windows para la que Microsoft había lanzado el parche de seguridad meses antes

Puede llegar al equipo en un fichero engañoso

Una vez ejecutado se propaga por toda la red

Cifra los contenidos del PC y exige un rescate para descifrarlos

(**Ransomware**)

Troyanos

Aplicación en apariencia inofensiva, pero que realmente tiene una funcionalidad oculta (El caballo de Troya)

No infecta otros ficheros, ni se reproduce o disemina

Troyanos

AIDS: En 1989, se distribuyen 10.000 copias de un programa de información sobre el SIDA

En las condiciones de uso se advertía de que romper la licencia tendría graves consecuencias para el ordenador

Al alcanzar un número determinado de ejecuciones, cifraba el contenido del disco duro

Para obtener la clave había que pagar (**Ransomware**)

Bombas lógicas

Aplicación latente en el ordenador hasta que se produce una circunstancia que la activa

Bombas lógicas

Viernes 13 (también conocido como Jerusalem)

Infecta los ficheros .com y .exe

Cuando llega un viernes 13, borra todos los ficheros infectados

Conmemora la creación del estado de Israel un viernes 13

Backdoors

Puerta trasera, permite acceso y control remoto del sistema sin una autentificación legítima

Backdoors

Backdoor BackOrifice

Consta de aplicación cliente y aplicación servidor

Al instalar la aplicación servidor, se obtiene control total sobre el ordenador

Lectura y escritura de archivos, ejecutar aplicaciones, reiniciar el sistema, visualizar la pantalla, manejar el ratón y teclado de la víctima, robar contraseñas, etc.

Más tipos de malware

Spyware: Recolecta y envía información privada sin el consentimiento y/o conocimiento del usuario

Keylogger: Captura las teclas pulsadas por el usuario, permitiendo obtener datos sensibles como contraseñas

Adware: Muestra anuncios o abre páginas webs no solicitadas

Más tipos de malware

Coinminer: Usa la potencia del equipo para minar criptomonedas sin conocimiento del usuario

Tipos de malware

Actualmente el malware no suele pertenecer a una única categoría, si no que presenta aspectos de varias

Por ejemplo Emotet (Ataque en 2019):

- Virus polimórfico
- Gusano que se distribuye por correo electrónico
- Incluye función keylogger
- Troyano que roba credenciales bancarias

Tipos de malware

Se suelen catalogar por su característica principal

Por ejemplo Lamin.B es un virus con una puerta trasera:

- Virus polimórfico que infecta ejecutables de Windows
- Gusano que se distribuye por redes locales
- Incluye función keylogger
- Backdoor que permite control remoto de la máquina

Tipos de malware

Zeus

- Troyano que genera una botnet (Red de ordenadores infectados y controlados por alguien ajeno)
- Controla los accesos a entidades bancarias
- Clona las webs y envía los datos al controlador
- Precursor de muchos de los troyanos financieros actuales

Tipos de malware

SpyEye

- Evolución de Zeus
- Plataforma “de pago” para el robo de datos bancarios

Nomenclatura de malware

Como convención (No obligatoria) sigue la siguiente estructura: Prefijo + Nombre + Variante + Sufijo (Establecida por Computer Antivirus Research Organization)

Nomenclatura de malware

Por ejemplo **W32/Klez.H@MM**

- Prefijo **W32**: Afecta a sistemas Windows de 32 bits
- Nombre **Klez**: Nombre para identificarlo
- Variante **H**: Existen otras 7 anteriores (a,b,c,d, ...)
- Sufijo **@MM**: Gusano de propagación masiva por correo electrónico

Nomenclatura de malware

Los pefijos más comunes:

- **W32**: Windows 32bit
- **W95**: Windows 9X/Me
- **WM**: Virus de macro de Word
- **XM**: Virus de macro de Excel
- **Worm**: Gusano
- **Troj**: Troyano
- **Bck**: backdoor

Malware en dispositivos móviles

¿Por qué se ataca más a Android?

Mayor cantidad de objetivos posibles

Código abierto (más fácil buscar fallos)

Personalización del SO de cada compañía (posibilidad de nuevas vulnerabilidades)

Menor control en Google Play

Malware en dispositivos móviles

¿Cómo evitarlo?

Instalar aplicaciones "conocidas"

Evitar aplicaciones fuera de la tienda oficial

Revisar los permisos y denegar los que no les corresponden

Mantener el SO actualizado

Instalar una aplicación antimalware

Fases de un virus

1.- Llegada al sistema (siempre desde el exterior), introducido voluntaria o involuntariamente

2.- Instalación (Infección): Se produce al ejecutar el código del virus por primera vez

Instalación de un virus

Añadidura: El código del virus se añade al final del archivo a infectar. El tamaño del archivo infectado crece

Inserción: El código del virus se reparte en huecos "libres" dentro del código del archivo infectado. El tamaño del archivo infectado no varía. Su creación no es trivial

Instalación de un virus

Reorientación: En el archivo a infectar se instala sólo una pequeña parte del código del virus. El resto está distribuido por el sistema. Al ejecutarse el virus se recompone y cumple su función

Sustitución: El virus sustituye directamente el código del archivo a infectar

Fases de un virus

3.- Activación y control del sistema:

- Acción directa: Se ejecuta el virus cada vez que se ejecute el fichero infectado
- Acción indirecta: el virus está residente en memoria y se ejecuta de manera regular

4.- Ocultamiento: A los ojos del usuario y del antivirus

Ocultación de un virus

Dispersión: el virus se divide y oculta sus partes

- Marca los ficheros como ocultos
- Se almacena en sectores libres del disco y los marca como defectuosos
- Se almacena en formatos que el sistema operativo no es capaz de leer

Ocultación de un virus

Compresión: el virus comprime el programa infectado y se instala en el sitio que queda libre para no modificar su tamaño

Camuflaje: el virus engaña al sistema operativo y al antivirus cuando comprueban los atributos de los ficheros (tamaño, fecha de modificación, etc.)

Ocultación de un virus

Sobrepasamiento: El virus actúa directamente sobre las rutinas de los servicios del sistema, engañando al antivirus que comprueba los servicios del sistema

Autocifrado: El virus se encripta y desencripta según lo necesite usando una clave distinta en cada ocasión. De este modo, el antivirus no puede acceder al contenido del virus y detectarlo

Ocultación de un virus

Polimorfismo: El virus cambia de forma (e incluso de comportamiento) cada vez que se propaga

Blindaje: Evita que el virus pueda ser desensamblado y por lo tanto se pueda acceder a su código

Fases de un virus

5.- Reproducción: Crear copias del virus en otros ficheros

- Búsqueda de uno o varios huéspedes
- Comprobación de que los huéspedes no han sido previamente infectados
- Recomposición del virus
- Copia en el programa huésped

Fases de un virus

6.- Manifestación: el virus lleva a cabo sus acciones, pueden ser más o menos dañinas:

... desde "jugar" con la interfaz (Virus Cascade)

... hasta estropear hardware (Chernobyl)

... o usar criptografía asimétrica para cifrar contenidos (Criptovirología)

Técnicas antivirus

Detección por cadena o firma: Se analiza el código del virus buscando una cadena representativa que lo diferencie de cualquier otro

Cuando el antivirus detecta esa cadena, determina que hay infección

EICAR Anti Malware test file:

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

Detección por cadena o firma

Es la técnica más extendida entre los antivirus

Permite identificar el malware de forma concreta

No detecta nuevos virus ni modificaciones

Filosofía reactiva, requiere actualización continua

Si el virus se encripta, no se puede encontrar la cadena

Técnicas antivirus

Detección por localización y nombre de archivo: Se buscan archivos concretos que generan los virus

Si existe ese fichero, el antivirus determina que hay infección

No detecta nuevos virus ni modificaciones

Filosofía reactiva, requiere actualización continua

Técnicas antivirus

Detección heurística: Se analiza el código para buscar conjuntos de instrucciones y comportamientos habituales del malware

No necesita de actualizaciones tan constantes

Capacidad para detectar malware nuevo

Más propenso a falsos positivos

Penalización en el rendimiento en los análisis

No detecta malware con características nuevas

Técnicas antivirus

Detección por comportamiento: En vez de analizar el código, comprueba las acciones que intentan llevar a cabo las aplicaciones, e identifican las que puedan ser potencialmente peligrosas

No necesita de actualizaciones tan constantes

Capacidad para detectar malware nuevo

Más propenso a falsos positivos

Penalización en el rendimiento del sistema

No detecta malware con características nuevas

Técnicas antivirus

Detección por emulación: Las aplicaciones se ejecutan en un entorno informático simulado (sandbox), para evaluar el grado de peligrosidad

No necesita de actualizaciones tan constantes

Capacidad para detectar malware nuevo

Más propenso a falsos positivos

Especial penalización en el rendimiento en los análisis (mayor que en el caso del análisis heurístico de código)

No detecta malware con características nuevas

Otras tecnicas antivirus

Chequeo de integridad: Comprobar la integridad de los archivos contra una base de datos (checksums, hash, ...)

Debe partir de un archivo limpio

Fáciles de burlar (spoofing)

Otras tecnicas antivirus

Control de acceso: Sólo se pueden ejecutar las aplicaciones permitidas por el administrador, con determinados privilegios y según perfil

Difíciles de administrar, sobre todo en ambientes heterogéneos, y poco práctico para usuarios particulares

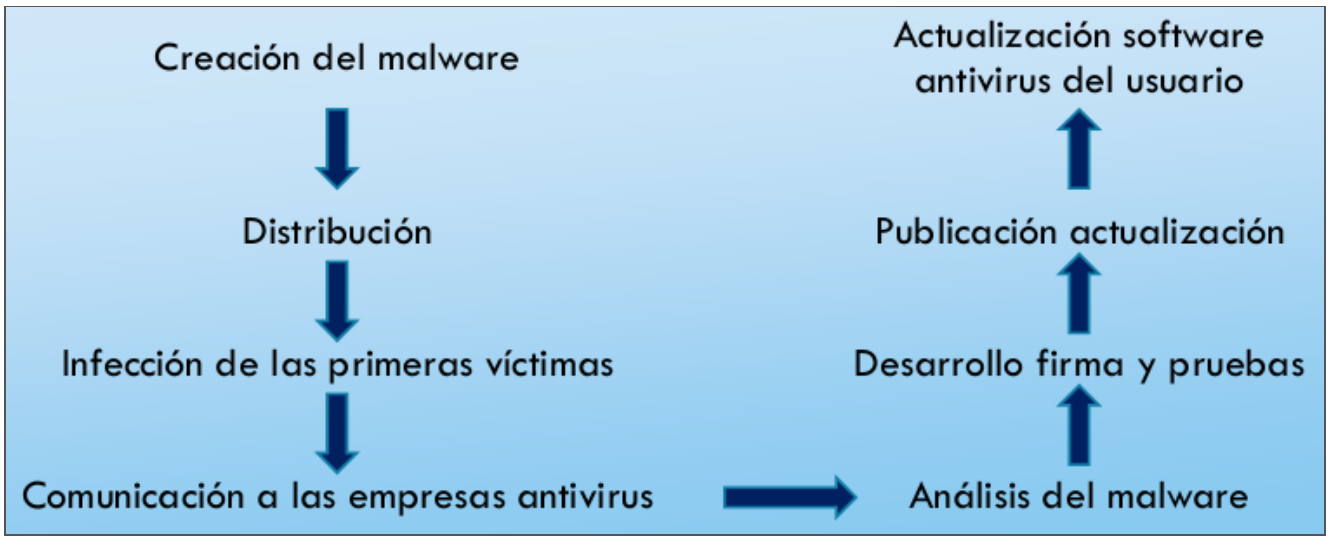
Limitaciones técnicas antivirus

Facilidad de burlar los métodos de detección

Esquema reactivo, solución a posteriori

Ventana vulnerable, no protegen a tiempo

Ventana vulnerable



Limitaciones técnicas antivirus

Falsa sensación de seguridad AV (perimetrales, locales)

Protocolos que no pueden ser analizados (HTTPS, ...)

Limitaciones de análisis en el perímetro (correo electrónico, web, etc.)

Formatos de empaquetado y compresión

Evolución y diversificación del malware

Defensa contra el malware

Origen de infecciones:

Abrir archivos legítimos (virus)

Abrir archivos no solicitados, adjuntos de correo, P2P, descargas (gusanos, troyanos)

Abrir archivos enviados por terceros intencionadamente (Ingeniería social) (troyanos, backdoors)

Defensa contra el malware

Origen de infecciones:

Configuración débil de nuestro sistema operativo (gusanos, virus, backdoors, ...)

Configuración débil de aplicaciones Internet (navegador, cliente de correo) (spyware, gusanos)

Vulnerabilidades del sistema operativo y aplicaciones Internet (gusanos, spyware, backdoors)

Defensa contra el malware

Visión habitual de la prevención

Defensa contra el malware

¿Contra qué origen de infección lucha cada uno?

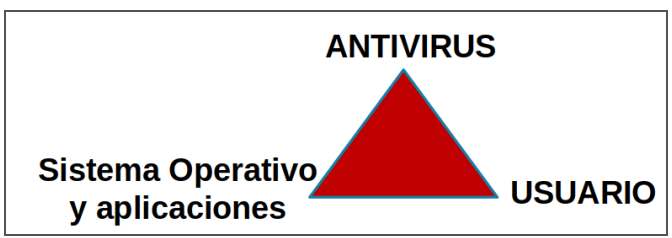
Antivirus: Abrir archivos legítimos

Usuario: Abrir archivos no solicitados, ingeniería social, configuración débil del S.O., configuración débil de aplicaciones Internet

Sistema Operativo y Aplicaciones: configuración débil del S.O., configuración débil de aplicaciones Internet, vulnerabilidades del S.O. y de aplicaciones

Defensa contra el malware

Si el antivirus es el que menos puede luchar, ¿Por qué es al que más importancia le damos? Hay que buscar el equilibrio



Defensa contra el malware

Educar / formar al usuario

Cultura de seguridad

Formatos potencialmente peligrosos

No abrir archivos no solicitados

No utilizar fuentes no confiables

Navegación segura

Política de passwords

Copias de seguridad

Defensa contra el malware

Respecto al S.O. y las aplicaciones Internet

Desactivar todos los servicios no necesarios

Aplicar actualizaciones automáticas (WSUS, SCCM)

Configuración segura navegador y correo

Políticas de uso de portátiles, memorias USB, acceso externo

Segmentación lógica redes

Políticas de privilegios según usuario y aplicaciones

Políticas de seguridad recursos compartidos

Defensa contra el malware

Respecto a las soluciones antivirus y antimalware

Uso de soluciones antivirus distintas y complementarias por capas (perímetro, servidor de archivos, host).

Firewall perimetrales y basados en hosts

Política de filtrado por contenidos

Política de acceso a la red (interna, externa)

Gestión centralizada seguridad

Auditorías y planes de contingencia/continuidad

Defensa contra el malware

Aplicaciones especialmente sensibles al malware

Aplicaciones de cliente de correo electrónico

Aplicaciones de escritorio

Aplicaciones de mensajería instantánea

Navegadores web

Aplicaciones P2P (eMule, torrent, etc.)

Defensa contra el malware

Bloqueo de aplicaciones no autorizadas: Permitir por defecto o bloquear por defecto

- Combatir virus
- Ejecutar sólo secuencias de comandos firmadas
- Asegurarse de que se instalan las aplicaciones autorizadas
- Bloquear equipos

Elegir un antivirus

Aspectos poco fiables

Marketing (protección 100%, detecta todos los virus conocidos y desconocidos, número 1, tecnología "supermegapotente",...)

Número de malware que dicen detectar (guerra de números, no es un dato cualitativo y no corresponde con la realidad)

“Consultores” (¿consultores o distribuidores?)

Premios y certificaciones

Comparativas (evaluación crítica, lectura de resultados)

Elegir un antivirus

Elementos a tener en cuenta

Recursos que consume, rendimiento y estabilidad

Facilidad de uso y posibilidades de configuración

Tipos de malware que cubre

Funciones proactivas

Actualizaciones y tiempos de respuesta

Elegir un antivirus

Elementos a tener en cuenta

Soporte

Puesto destacado en comparativas

Casuística de nuestros sistemas

Gestión centralizada, funciones corporativas

Elegir un antivirus

NINGUN SOFTWARE ANTIMALWARE ES PERFECTO

Lo mejor es usar una combinación de varios: Un antivirus, Un antiexploit, Un firewall, Un antispyware