Seguridad y Alta Disponibilidad

TEMA 4

Software Antimalware

ICSE

OBJETIVOS DEL TEMA 4

- Comprender qué es el software malicioso y sus posibles fuentes
- Conocer los riesgos y la toma de precauciones en operaciones informáticas
- Identificar las nuevas posibilidades y riesgos de Internet y redes sociales
- Analizar las distintas herramientas de seguridad antimalware existentes

ICSE

SOFTWARE ANTIMALWARE

DEFINICIÓN

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.

ICSE

OBJETIVOS DEL MALWARE

- **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.

ICSE

OBJETIVOS DEL MALWARE

- 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 esta 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 economico al usuario del equipo para recuperar la información, como hacen los criptovirus.

ICSE

CLASIFICACIÓN DEL MALWARE

Códigos maliciosos más comunes

- **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.

ICSE

CLASIFICACIÓN DEL MALWARE

Códigos maliciosos más comunes

- **Gusano:** característica principal es realizar el máximo numero 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 mas comunes son: descargado por otro programa malicioso, al visitar una pagina web maliciosa, dentro de otro programa que simula ser inofensivo, etc.

ICSE

MÉTODOS DE INFECCIÓN

- **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.

ICSE

MÉTODOS DE INFECCIÓN

- **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 si 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.

ICSE

MÉTODOS DE INFECCIÓN

- ***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.

ICSE

KEYLOGGER

DEFINICIÓN

Los **keyloggers** son un tipo de herramienta que permite el robo de contraseñas. Este tipo de malware tiene como misión **registrar todas las teclas** que pulsamos en el teclado.

De esta forma, cada vez que iniciamos sesión en un servicio como correo electrónico, páginas, aplicaciones web o escritorio, el programa mantendrá un historial del contenido que insertamos por teclado, a menudo incluyendo claves de acceso y el nombres de usuario. Esta información se podrá usar posteniormente en ataque de diccionario.

ICSE

KEYLOGGER

RECOMENDACIONES

- Realizar escaneos periódicos antimalware
- Controlar accesos físicos (puertos red y terminales físicas)
- Limitar los privilegios de las cuentas de usuario

ICSE

PROTECCIÓN Y DESINFECCIÓN DE SISTEMAS

- Mantente informado sobre las novedades y alertas de seguridad.
- Mantén actualizado tu equipo, tanto el SO como cualquier aplicación 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.).

ICSE

PROTECCIÓN Y DESINFECCIÓN DE SISTEMAS

- 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 SO 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.

ICSE

PROTECCIÓN Y DESINFECCIÓN DE SISTEMAS

- Realizar periódicamente escaneo de puertos, test de velocidad y de las conexiones de red para analizar si las aplicaciones que las emplean son autorizadas.
- No fiarte de todas las herramientas *antimalware* que puedes descargarte a través de Internet de forma gratuita o las que te alertan que tu sistema esta 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*.

ICSE

CLASIFICACIÓN DE SOFTWARE ANTIMALWARE

- **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 mas aplicaciones web que permiten, mediante la instalación de *plugins* en el navegador, analizar nuestro sistema de archivos completo.

- **Antivirus portable:** no requieren instalación en nuestro sistema, se ejecutan directamente desde el sistema de ficheros y consumen una pequeña cantidad de recursos.

ICSE

CLASIFICACIÓN DE SOFTWARE ANTIMALWARE

- **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.

ICSE

OTRAS HERRAMIENTAS ESPECÍFICAS

- **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, que enlaces de esas paginas se consideran peligrosos y cual es el motivo. Existen varios tipos de analizadores en función de como se accede al servido: 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.

ICSE

CONFIGURACION DE ANÁLISIS ANTIMALWARE

En los sistemas operativos es necesario realizar tareas de monitorización y control exhaustivas para detectar anomalías y modificaciones no deseadas.

Sistema Windows Defender: hconjunto de herramientas software que incluyen las distribuciones de Windows. Nos permiten controlar y detectar modificaciones en nuestro sistema de ficheros, incluyendo tanto modificaciones de archivos como descargas. Se recomienda inspecciones periódicas y análisis de las variaciones que se produzcan.

ICSE

LIMITAR EJECUCIONES EN ARRANQUE

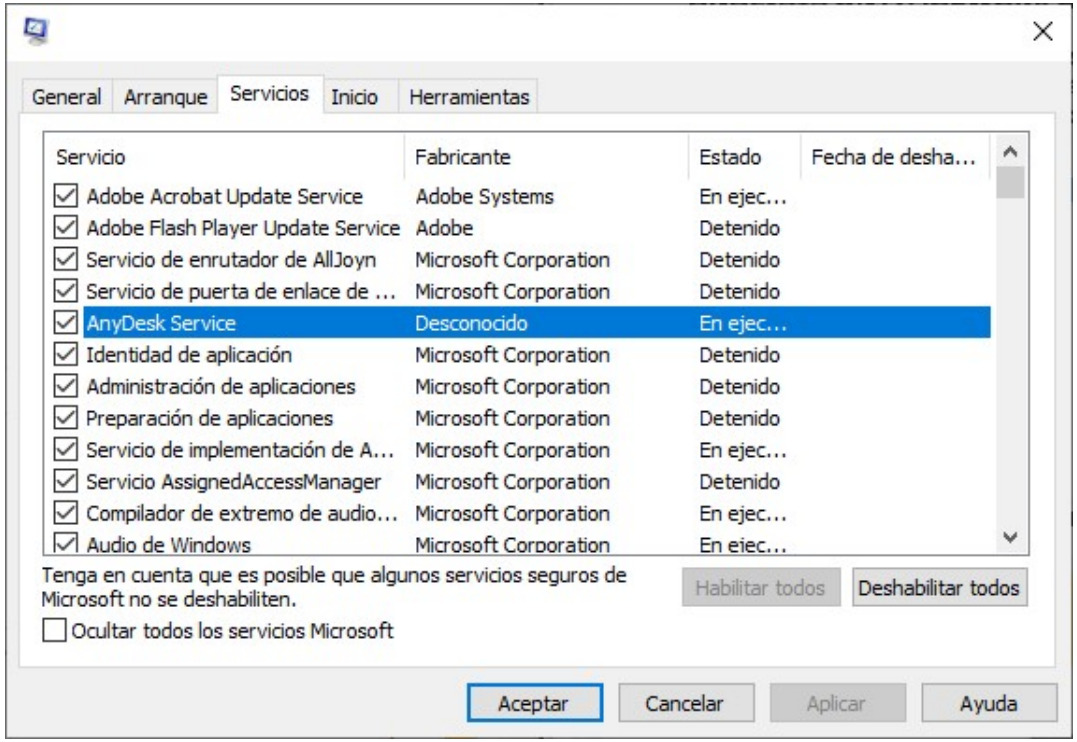
Las aplicaciones y servicios que en su instalación por defecto se configuran como aplicaciones de arranque presentan una vulnerabilidad para los sistemas, al convertirse estos en objetivos preferentes de infecciones de virus y modificaciones de los archivos con el fin de ejecutar malware en segundo plano.

Adicionalmente, tambien hay que tener en consideracion la recopilacion de informacion que realizan las aplicaciones, informandonos del rango y profundidad que pueden llegar a alcanzar antes de realizar su instalación y configuración.

ICSE

LIMITAR EJECUCIONES EN ARRANQUE

MS CONFIG en Windows: Los procesos de arranque en el sistema, mediante la ejecución de la herramienta msconfig.



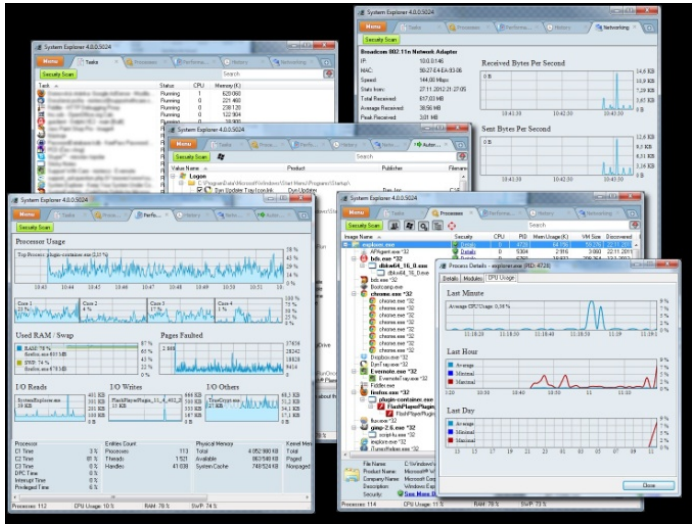
ICSE

ANÁLISIS ANTIMALWARE A FONDO

Los procesos en ejecución los podemos analizar mediante la herramienta: Autoruns y Process Explorer, en la suite de **herramientas Sysinternals**.

- ❑ Autoruns: Fabricante y ruta de ejecución del proceso.
- ❑ Process Explorer: muestra los vínculos entre cada proceso, el usuario que lanza el proceso, etc

System Explorer: Software con herramientas útiles para mantener el sistema bajo control. Rápido acceso a base de datos de archivos que lo ayuda a descubrir procesos indeseados o amenazas.



ICSE

Seguridad y Alta Disponibilidad

PRÓXIMO TEMA

Criptografía

ICSE