Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.
CONSEJERÍA DE ECONOMÍA, INNOVACIÓN, CIENCIA Y EMPLEO

AndalucíaCERT
CENTRO DE SEGURIDAD TIC

Informe de divulgación
Investigación de código dañino

Tipo de documento:	*Informe*
Autor del documento:	*AndalucíaCERT*
Código del Documento:	*CERT-IF-4160-130930*
Edición:	*0*
Categoría	*Público*
Fecha de elaboración:	*30/09/2013*
N° de Páginas	*1 de 16*

1 TABLA DE CONTENIDOS

2 OBJETO

El objeto de este documento es proporcionar al personal de la Junta de Andalucía una serie de técnicas y herramientas para la detección de malware en sistemas Windows.

3 ALCANCE

Este documento va destinado al personal técnico de la Junta de Andalucía.

4 INTRODUCCIÓN

Uno de los focos principales de agresiones que pueden sufrir las organizaciones proviene de la ejecución de código dañino. Actualmente, la variedad de tipos de ataque identificados, requiere proveer al profesional de diferentes procedimientos a la hora de acometer un análisis con la solvencia adecuada.

Tradicionalmente, la adquisición de una solución antivirus ha sido contemplada como la estrategia seguida por una entidad para luchar contra el contenido dañino. Sin embargo, se ha constatado en muchas ocasiones que esta medida no siempre es suficiente. Una solución puede ser realmente efectiva ante determinado tipo de malware y no tanto frente a otros. Por ejemplo, no es lo mismo una código malicioso tipo rootkit, que un gusano, un troyano o cualquier otra categoría de código dañino.

Este documento proporciona una metodología para la detección de código dañino, dando así mecanismos y procedimientos orientados a su investigación. Para ello se describirán e identificarán aplicaciones y mecanismos técnicos, con los cuales llevar a efecto tareas que permitan identificar correctamente contenido dañino.

Esta guía recoge las tareas que deberán ser efectuadas para detectar contenido dañino en entornos Microsoft y poder obtener el ejecutable/fuente origen del código dañino. Determinadas operaciones serán diferentes entre sistemas anteriores o posteriores a Windows Vista. Esto es debido, fundamentalmente, a los cambios internos en el nivel de seguridad que se establecen con los sistemas operativos más modernos, y que exigen comportamientos diferenciales, incluso para las aplicaciones de seguridad.

La información recogida en el presente documento está basada en el informe desarrollado por el CCN-CERT denominado “PROCEDIMIENTO DE SEGURIDAD DE LAS TIC (CCN-STIC-912), PROCEDIMIENTO DE INVESTIGACIÓN DE CÓDIGO DAÑINO ”.

5 TIPOS DE ANÁLISIS

Dos tipos de análisis se pueden realizar sobre un sistema con objeto de realizar una detección pormenorizada: ACTIVO o PASIVO:

- **Activo** → Tiene como premisa la identificación de contenido dañino mientras el sistema operativo se encuentra ejecutándose.

- **Pasivo** → Se llevará a cabo sin que el sistema operativo de la máquina afectada se encuentre activo, y se utilizará para ello recursos que en modo Live-CD que permitirán acceder al equipo y realizar un análisis antimalware en el sistema.

La razón de emplear dos métodos tan diferentes se debe, principalmente, a que existen muchas circunstancias que hacen que uno u otro no sean funcionales bajo determinados escenarios. Por ejemplo, un análisis en activo con soluciones antivirus puede verse afectado por mecanismos empleados por aplicaciones dañinas para ocultarse y/o protegerse frente a la acción de los sistemas antimalware. Un análisis activo permite detectar presencias anómalas, pero puede que no permita una eliminación rápida de las aplicaciones dañinas. Un análisis pasivo pudiera no ser efectivo en sistemas que presentaran un mecanismo de cifrado para sus discos, imposibilitando así cualquier acceso que no implique el arranque del propio sistema.

Los dos tipos de análisis pueden llegar a combinarse si las condiciones del entorno lo permiten. Los resultados evidentemente no tienen por qué ser equivalentes, aunque sí complementarios. El uso de uno u otro dependerá fundamentalmente de la situación o sospecha que pueda llegar a tenerse de la posible presencia malware.

6 ACTIVIDADES PRE-ANÁLISIS: COPIA DE DISCO

A la hora de enfrentarse a cualquiera de los dos análisis, el primer paso que se ha de realizar es una copia de seguridad del disco duro que se va a analizar. Será necesario disponer de un Live-CD (CD autoarrancable) de cualquiera de las diferentes distribuciones Linux disponibles públicamente en Internet, que permita la utilización de una herramienta para la creación, copia o eliminación de datos (por ejemplo, "dd"). Luego podremos seguir los siguientes pasos para realizar la copia de seguridad:

1. Arrancar el sistema desde un Live-CD.

2. Asegurarnos de que no haya particiones "montadas" del disco duro que se desea copiar.

3. Montar el disco que almacenará la copia.

4. Si este disco ha sido usado anteriormente será recomendable realizar un borrado previo para evitar una posible contaminación de datos anteriores.

5. Realizar la copia de seguridad.

También existen herramientas para Windows que permiten realizar la copia del disco, pero dado que éstas deben emplearse con el sistema en ejecución, es posible que el código dañino enmascarase su presencia, modificase en algún sentido la copia o no permitiese copiar determinadas partes del disco. Se puede hacer uso de múltiples herramientas existentes en Internet, de las cuales se citan las siguientes:

- ODIN (http://odin-win.sourceforge.net/)
- DiskImage (http://www.dubaron.com/diskimage/)
- WinDD (http://windd.sourceforge.net/)
- NFGDump (http://nfgdump.sourceforge.net/)

7 ANÁLISIS ACTIVO

Este procedimiento presenta como objetivo fundamental identificar con el sistema operativo ejecutándose, la presencia de un malware, así como el tipo de actividad que éste estuviera realizando. Es conveniente aislar el equipo del resto de elementos de la organización. Aunque para ello el primer impulso pasaría por quitar el cable de red del equipo, hay que tener presente que muchas aplicaciones dañinas se muestran y actúan cuando existe presencia de red, algo vital para determinados procesos dentro de este tipo de análisis.

En resumen, el procedimiento aquí desarrollado presenta los siguientes objetivos:

- Determinar la presencia de elementos ocultos que no se muestran ni al usuario ni a la aplicaciones instaladas en el equipo.
- Determinar actividades de aplicaciones que intentan enviar información a través de la red.
- Detectar la presencia de actividades enfocadas a interceptar y modificar las operaciones del usuario (como puede ser recuperar lo que el usuario se encuentra escribiendo en el teclado).
- Determinar la alteración del sistema operativo por parte de una aplicación con contenido dañino.

7.1 DETECCIÓN DE ROOTKIT

La familia de rootkits contempla el conjunto de aplicaciones dañinas encaminadas a modificar el entorno del sistema operativo con fines diferentes a los convencionales. El objetivo fundamental consiste en la **ocultación de información a usuarios, aplicaciones y al propio sistema operativo**. Un rootkit se coloca entre la comunicación del hardware del equipo afectado y el propio sistema operativo, por lo que cualquier acción que hace el sistema operativo puede ser interceptada.

La identificación de un rootkit se hace esencial en una primera instancia para un análisis activo, porque este tipo de aplicaciones son utilizadas para ocultar la presencia y actividad de otras aplicaciones dañinas. Si el rootkit se encuentra activo, los demás procedimientos podrían ser infructuosos al quedar oculta la actividad dañina.

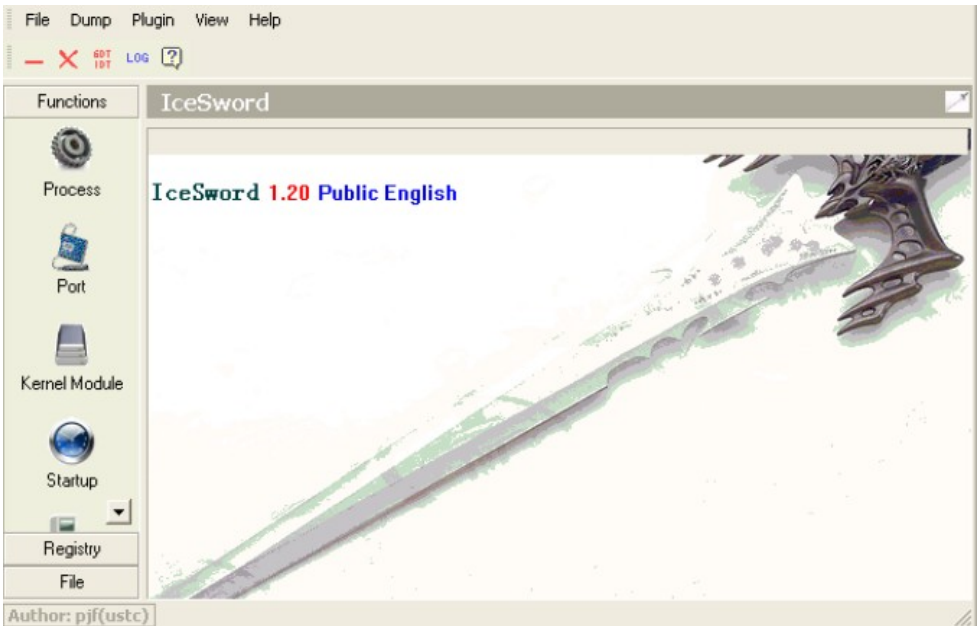
Las aplicaciones antirootkit operan fundamentalmente comparando y comprobando la información que reciben y que procesan las aplicaciones instaladas y el propio kernel del sistema. De esta forma, pueden evaluar y mostrar las discrepancias existentes, evidenciando la existencia de elementos ocultos en el sistema.

La identificación de rootkit cambia en función del sistema operativo al que hay que realizar el análisis. Por lo tanto, se exponen a continuación las herramientas que podrán utilizarse y el tipo de análisis a efectuar para sistemas anteriores y posteriores a Windows Vista.

7.1.1 SISTEMAS PREVIOS A WINDOWS VISTA

Estos sistemas presentan menos características de protección frente a código dañino, fundamentalmente de la familia de rootkits. Por lo tanto, la actividad de este tipo de malware en un sistema como Microsoft Windows XP o Microsoft Windows 2003 puede ser factible, actuando de forma combinada con cualquier tipo de aplicación dañina.

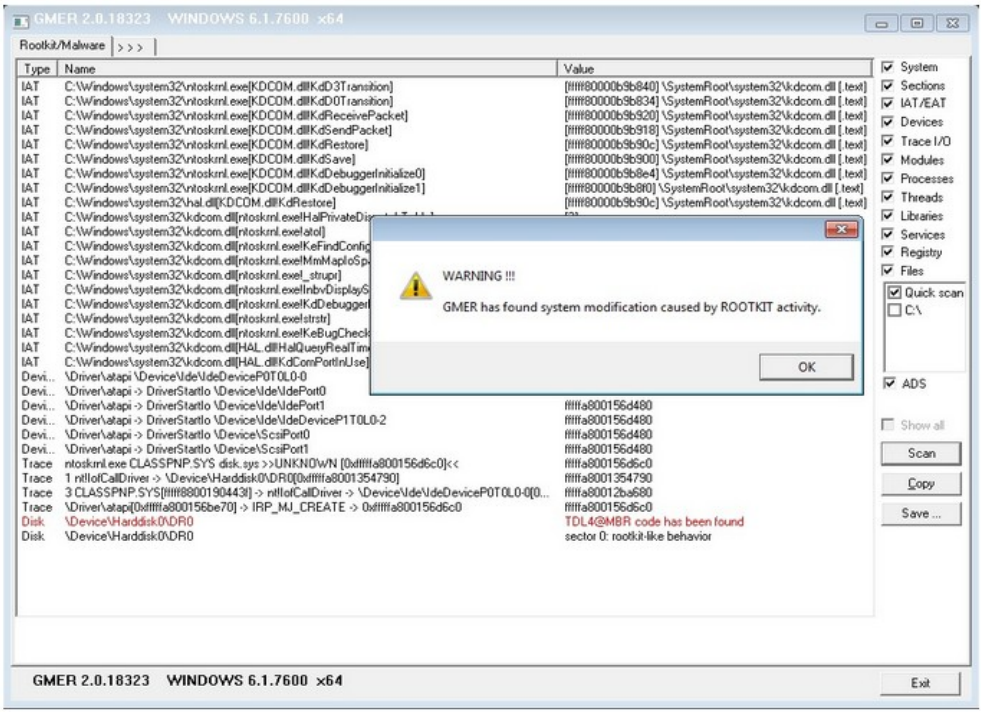
Aunque existen muchas aplicaciones que detectan actividades anómalas de este tipo de malware, por su versatilidad, facilidad de uso e información que proporciona destacamos la aplicación IceSword.



7.1.2 SISTEMAS WINDOWS VISTA O POSTERIORES

Las mejoras en los aspectos de seguridad de los nuevos sistemas operativos hicieron más compleja la actividad dañina de los rootkit. Sin embargo, a día de hoy, aunque en menor medida, se sigue pudiendo detectar la presencia de aplicaciones de este tipo (fundamentalmente para sistemas de 32 bits).

El número de aplicaciones de detección antirootkit para sistemas Windows Vista o posteriores es mucho menor y son más complejas para su apreciación que las de los sistemas previos. En esta guía, por su potencia se recomienda el uso de la aplicación **Gmer**.



7.1.3 OTRAS HERRAMIENTAS

- **RootkitRevealer**: Herramienta para detectar rootkits en sistemas Windows XP y Windows Server 2003.
  - http://technet.microsoft.com/es-es/sysinternals/bb897445.aspx
  - Realiza una búsqueda en el registro y las llamadas al sistema buscando posibles diferencias que puedan indicar la presencia de un rootkit (en nivel usuario o nivel kernel).

7.2 DETECCIÓN DE ADS

Algunas aplicaciones dañinas, como RAT's y Spywares, aprovechan funcionalidades del sistema para ocultarse. Entre ellas, una de las más comunes consiste en hacer uso de la funcionalidad **Alternate Data Streams** (ADS) para ocultar su presencia. El ADS es una característica propia del sistema de ficheros NTFS y también de otros sistemas operativos no Microsoft. Esta característica permite guardar flujos alternativos de datos. En esencia, incorporar ficheros dentro de otros ficheros.

Por defecto, los ficheros que hacen uso de las característica de ADS no son mostrados a través de las aplicaciones que incorpora el sistema. Sin embargo, pueden ser invocados sin ningún problema. Esta acción permitirá que el código dañino pueda ocultarse a la vista del usuario.

La identificación de ficheros tipo ADS puede realizarse con las siguientes aplicaciones:

- **LADS**
  - http://www.heysoft.de/en/software/lads.php?lang=EN
- **ADSspy**
  http://www.bleepingcomputer.com/download/ads-spy/

En caso de detectar la presencia de un ADS debe realizarse una búsqueda de los ficheros en el registro del sistema para identificar así qué mecanismo es utilizado por el sistema para cargarlo cuando el equipo reinicia.

Es posible que se encuentren algunos archivos ocultos mediante ADS y no se pueden analizar porque se encuentran bloqueados por el sistema. En caso de querer analizar estos ficheros bloqueados, será necesario iniciar con otro sistema operativo (por ejemplo, con el disco conectado en otro sistema) y realizar entonces el análisis. Estos ficheros ya no se encontrarán bloqueados puesto que el sistema operativo activo no hará uso de ellos.

7.3 DETECCIÓN DE ANOMALÍAS EN MEMORIA

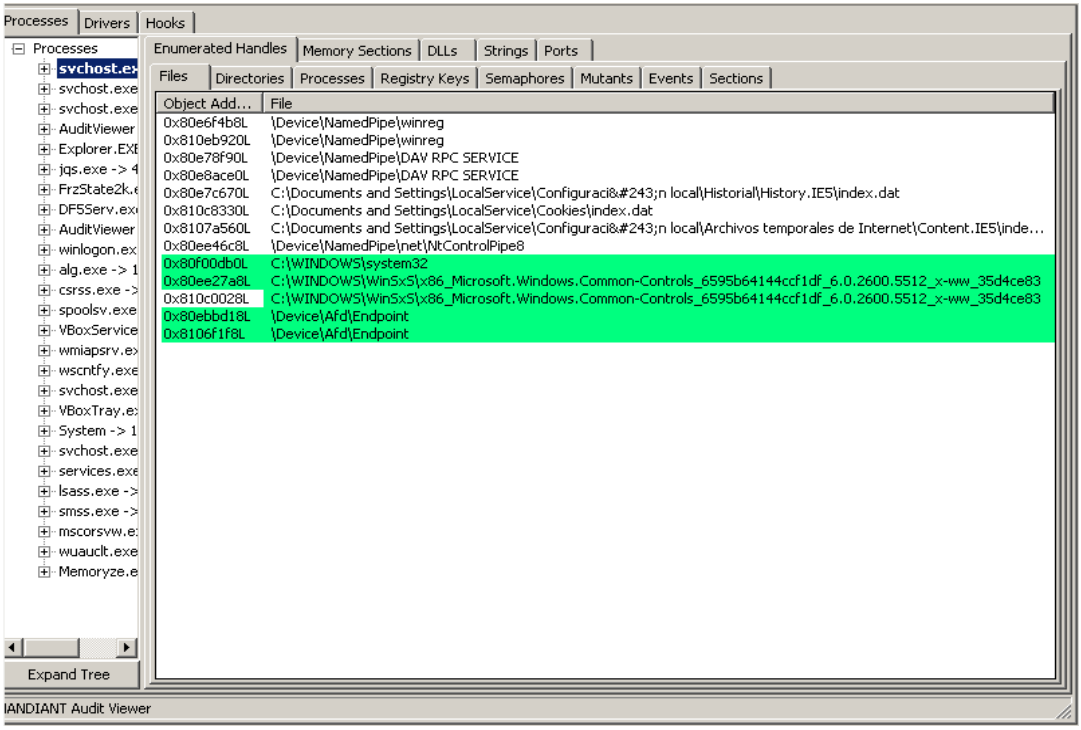
Otro tipo de análisis que se puede llevar a cabo en el equipo es la exploración de la memoria en busca de procesos ocultos, drivers de kernel desconocidos o hooks (interceptadores) en las llamadas del sistema, todas ellas operaciones típicas realizadas por contenido dañino. Para la exploración de la memoria se puede hacer uso de la herramienta **Mandiant Memoryze**, descargable de la página web:

- http://www.mandiant.com/assets/Memoryze.zip

Para poder usar esta herramienta y visualizar el contenido del análisis realizado por Memoryze es necesario hacer uso de una segunda, de nombre **AuditViewer**, otra herramienta de Mandiant descargable y gratuita de la página web:

- http://www.mandiant.com/assets/AuditViewer.zip

Esta herramienta permite listar todo los procesos activos, junto con sus identificadores y todos los ficheros/subprocesos que estos mantengan abiertos, así como identificar los drivers del kernel cargados y los posibles hooks existentes en el sistema (acciones del usuario interceptadas por una aplicación). Es interesante destacar que Memoryze es capaz de trabajar tanto en un sistema que se está ejecutando, como en un fichero de volcado de memoria.



7.4 DETECCIÓN DE HOOKS EN EL SISTEMA

Determinados tipos de aplicaciones tienen la capacidad de interactuar con las acciones del usuario. Escribir, copiar un texto o navegar por Internet son acciones que pueden desembocar en que una aplicación distinta del sistema proceda a almacenar la información o bien enviarla a través de internet. Esta interceptación de las acciones del sistema se denomina hook.

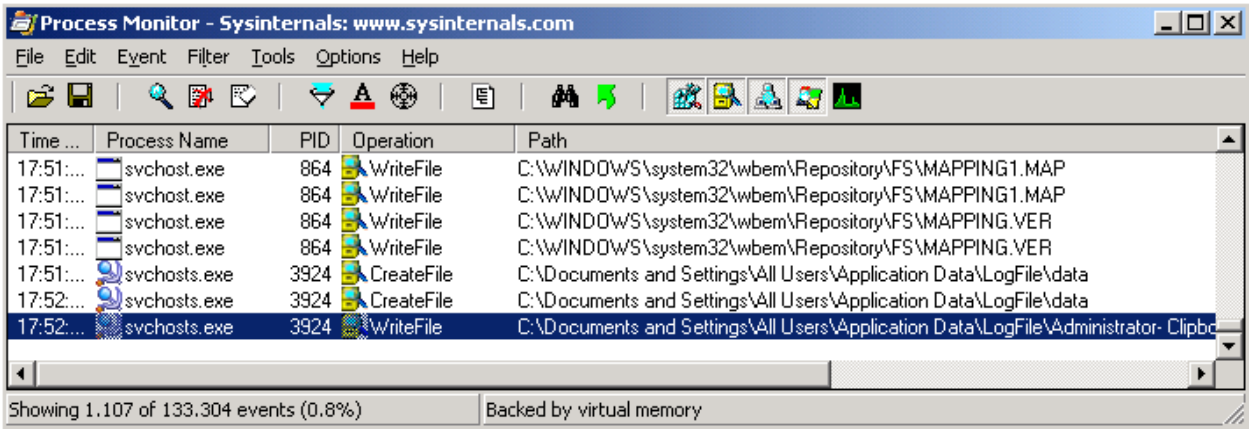
El objetivo en esta parte del procedimiento consiste en desencadenar acciones que permitan identificar la presencia de aplicaciones que analizan el comportamiento del usuario. Para ello puede utilizarse tanto la aplicación **Memoryze** que se acaba de ver en la sección anterior, como otras aplicaciones como por ejemplo la aplicación **Process Monitor**, descargable de la siguiente dirección:

- http://technet.microsoft.com/es-es/sysinternals/bb896645.aspx

Esta aplicación registra las acciones que realizan las aplicaciones:

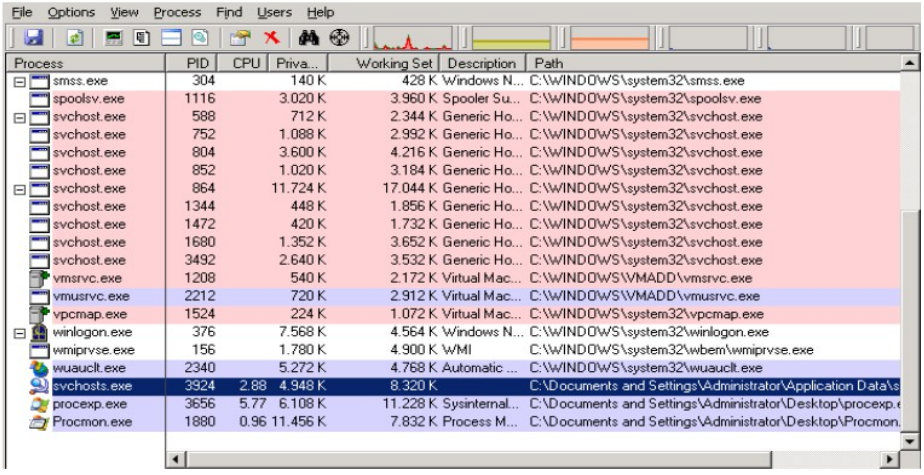
- Actividad con ficheros y carpetas.
- Actividad con el registro.

Cuando se lleve a cabo cualquier acción podremos visualizar todos los procesos que actúan asociadas a la misma. Por ejemplo podemos ver los procesos asociados a copiar un texto al portapapeles e imprimir pantalla:



Este procedimiento, aunque puede ser algo lento y confuso en la valoración de la información, permite identificar claramente situaciones anómalas donde las acciones de usuario son interceptadas y enviadas de forma externa. Para corroborar los resultados, las acciones deberán realizarse en varias ocasiones y observar cada vez los resultados dados por la aplicación de monitoreo. Una vez identificado el proceso dañino, puede conocerse la ruta de ejecución de la aplicación mediante la aplicación **Process Explorer**. Esta aplicación puede descargarse desde la siguiente URL:

- http://technet.microsoft.com/es-es/sysinternals/bb896653.aspx



Es posible que nos encontremos con que el proceso coincidiera con el nombre de una aplicación legítima. En este punto los ejecutables, ficheros y demás elementos identificados deben ser analizados con aplicaciones antivirus o bien analizarse mediante el procedimiento que se describirá en el apartado 10.

7.5 DETECCIÓN DE TRÁFICO DE RED ANÓMALO

Resulta muy habitual que la información recopilada por la aplicación dañina sea enviada a través de la red. Un comportamiento significativo de aplicaciones dañinas consiste precisamente en el envío de información o en establecer conexiones externas desde el sistema infectado.

Tienen como objetivo actualizarse, descargar otro software dañino en el sistema víctima, o generar un canal de comunicación que el atacante aprovecha para controlar el equipo infectado.

Este hecho permitirá que, dando los pasos adecuados, puedan conocerse:

- Qué procesos se encargan de realizar conectividad hacia Internet.
- Qué puertos de origen y destino intervienen en la comunicación.
- Qué dirección IP o nombre host de destino tiene la comunicación.
- Qué tipo de protocolos se emplean.
- Qué información se envía o descarga.

Habitualmente en estos procedimientos se emplea una herramienta de monitorización de tráfico (sniffer) para capturar el tráfico que se envía a Internet, pero esto puede encontrarse con varios problemas. El sniffer es capaz de identificar el puerto de origen, pero no la aplicación que genera la conexión. Además, el tráfico podría estar cifrado y por lo tanto no obtener información significativa del intercambio de datos. Por lo tanto, para que esta parte del procedimiento puede resultar eficaz, hay que combinar dos elementos: un identificador de conexiones internas y un sniffer de red.

Una aplicación que permite controlar los programas y conexiones internas es **PortReporter**. Ésta funciona como un servicio de Windows que guarda la actividad en una serie de ficheros de registros. Puede descargarse desde la siguiente URL:

- http://www.microsoft.com/en-us/download/details.aspx?id=9964

El sniffer a emplear puede ser Wireshark y se puede descargar desde la siguiente dirección URL.:

- http://www.wireshark.org/download.html

Debe establecerse una correlación entre las conversaciones recogidas en Wireshark y los datos registrados en PortReporter. De esta forma se obtiene una información detallada de todo lo concerniente al tráfico de red. Entre los objetivos a identificar están, entre otros:

- Intentos de conexión en la red interna a otros sistemas. Puede ser significativo de la presencia de gusanos de red.
- Conexiones a Internet desde programas identificables, que puede utilizar habitualmente el usuario, aunque no hayan sido lanzados por él en el momento del análisis: navegadores, programas de mensajería instantánea, aceleradores de descarga, etc. Esto puede indicar la presencia de troyanos o spyware que hubieran modificado el comportamiento de aplicaciones convencionales.
- Procesos o aplicaciones desconocidas que inician comunicación por la red o hacia Internet. Este hecho puede indicar la presencia de troyanos, gusanos, spyware o descargadores de virus.

Con objeto de limitar la información que se recoge y no interferir en el análisis que debe realizarse, es aconsejable, antes de iniciar la recogida de información, desactivar todos aquellos procesos que pudieran influir en el tráfico de red y que son identificados como no peligrosos:

- Parar los sistemas de actualizaciones del sistema operativo y otras aplicaciones convencionales.
- Cerrar todos los navegadores.
- Detener el antivirus y su proceso de actualización.
- Cerrar todas aquellas aplicaciones susceptibles de enviar tráfico: Outlook, etc.
- Desconectar unidades de red existentes en el equipo.

Tenemos que asegurarnos también que el sistema tiene acceso a Internet, ya que de lo contrario, los procesos maliciosos, no iniciarán las conexiones que queremos analizar. Hay que tener también presente que esta máquina se encuentra infectada, por lo tanto debe mantenerse en la medida de lo posible el máximo aislamiento del equipo de otros equipos de la red. Por ejemplo, puede conectarse el equipo para las pruebas en una red ADSL independiente del resto de la organización.

7.6 DETECCIÓN DE PROCESOS ANÓMALOS

Determinados tipos de malware pueden ser detectados por la presencia de procesos no identificativos, o bien que siendo éstos conocidos presentan parámetros anómalos, como pudiera ser la ruta de ejecución. Identificar procesos a priori no es una tarea simple, puesto que existe la posibilidad de camuflar procesos dañinos con nombres de aplicaciones del sistema. También determinados contenidos dañinos se ejecutan junto con procesos totalmente inocuos y del propio sistema.

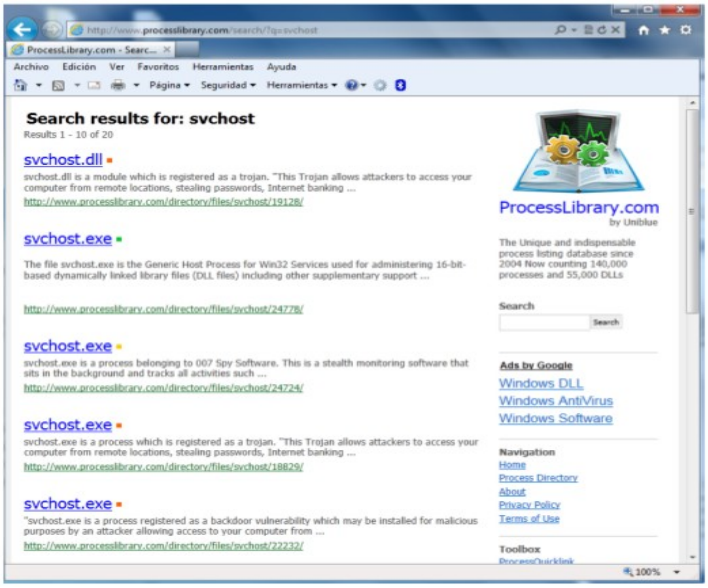
En este sentido pueden identificarse comportamientos anómalos en los procesos cuando:

- Existan procesos de navegadores u otras aplicaciones de uso convencional cuando no hayan sido ejecutados por el usuario.
- Existan procesos identificativos del sistema pero que se ejecutan en rutas diferentes de las convencionales.
- Existan procesos del sistema ejecutados con usuarios diferentes de los habituales.

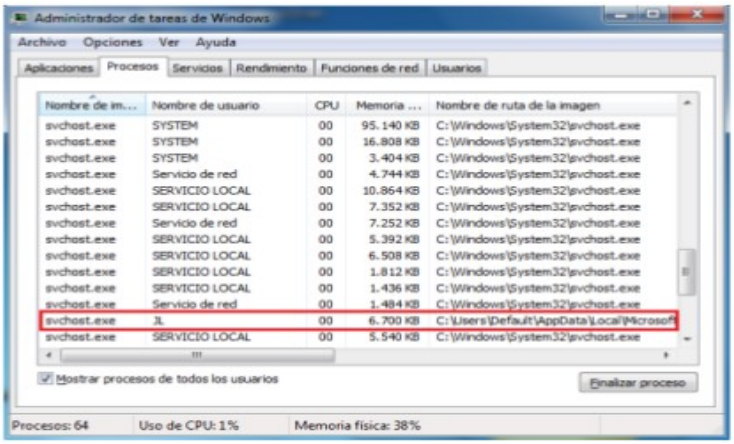
Para conseguir un conocimiento previo de los procesos activos en el sistema debemos primero identificarlos y consultar una base de datos como http://www.processlibrary.com para obtener información de cada uno de ellos. Para identificarlos podemos usar el Administrador de Tareas de los sistemas Windows, o el programa Process Hacker:

- http://processhacker.sourceforge.net

Es importante tener en cuenta a la hora de interpretar los resultados que existen múltiples posibles resultados para un mismo tipo de proceso. Existe la posibilidad de que un mismo proceso pueda tratarse de un proceso del sistema o de una aplicación dañina. Sólo el análisis en conjunto podría llegar a determinar que un determinado proceso es realmente dañino.



Un dato que nos puede resultar útil es identificar la ruta de ejecución del proceso. (mediante el uso de Process Explorer, por ejemplo). Un proceso que se ejecute en una ruta diferente de la habitual puede resultar sospechoso.



Todos los procesos identificables como potencialmente dañinos deberían ser analizados en un servicio online o local con objeto de determinar si son o no malware.

8 ANÁLISIS PASIVO

Muchos de los códigos dañinos de los que hoy en día pueden afectar a nuestros sistemas son sumamente sofisticados. Estos programas son capaces de desplegar sistemas de evasión de soluciones antimalware. Una forma de evitar que el código malicioso anule la detección, es mediante el análisis pasivo, de tal modo que el sistema operativo a analizar, no estará activo durante el análisis.

Un análisis pasivo es consiste en realizar un análisis totalmente neutro donde el sistema no se encuentre activo y buscar indicios de código dañino entre los ficheros de forma totalmente automatizada.

Para este tipo de análisis, los diferentes fabricantes de antivirus proponen soluciones antimalware implementadas sobre Live-CD (CD autoarrancable) que permitirán analizar un sistema.

Para realizar este análisis se proponen 2 soluciones distintas que pueden arrojar resultados diferentes:

- AVIRA Antivir Rescue System
  - http://www.avira.com/en/download/product/avira-antivir-rescue-system
- Kapersky Resuce Disk
  - http://support.kaspersky.com/faq/?qid=208282173

9 ANÁLISIS CON INDICADORES DE COMPROMISO (IOC)

Los indicadores de compromiso (Indicators of Comprimise - IOC), permiten describir las características técnicas de una amenaza conocida, o de una metodología de ataque, o cualquier otra evidencia de compromiso en un equipo por medio de las evidencias que deja en el propio equipo comprometido. Por ejemplo en función de los procesos, entradas de registro, servicios, ficheros descargados, etc. tras la infección.

Una opción para el uso de IOC's es OpenIOC. Se trata de un framework open-source desarrollado por Mandiant. Con él podremos describir de forma semántica el comportamiento de la amenaza por medio de ficheros XML y utilizar los mismos para buscar signos de infección en una máquina sin necesidad de llegar a realizar un análisis exhaustivo de la misma para identificar el tipo de amenaza:

- http://www.openioc.org/

10 ANÁLISIS EN ENTORNOS CONTROLADOS (SANDBOXING)

Mediante los métodos descritos anteriormente, ya deberíamos ser capaces de categorizar ciertos archivos de un sistema comprometido como sospechosos. Además de los análisis mediante sistemas antimalware, podemos hacer uso de los llamados "entornos controlados o **sandbox**".

Un entorno controlado es un entorno preparado especialmente para el análisis, aislado de cualquier otro equipo, y con capacidad de detectar actividades fuera de las habituales durante la ejecución de los ficheros sospechosos.

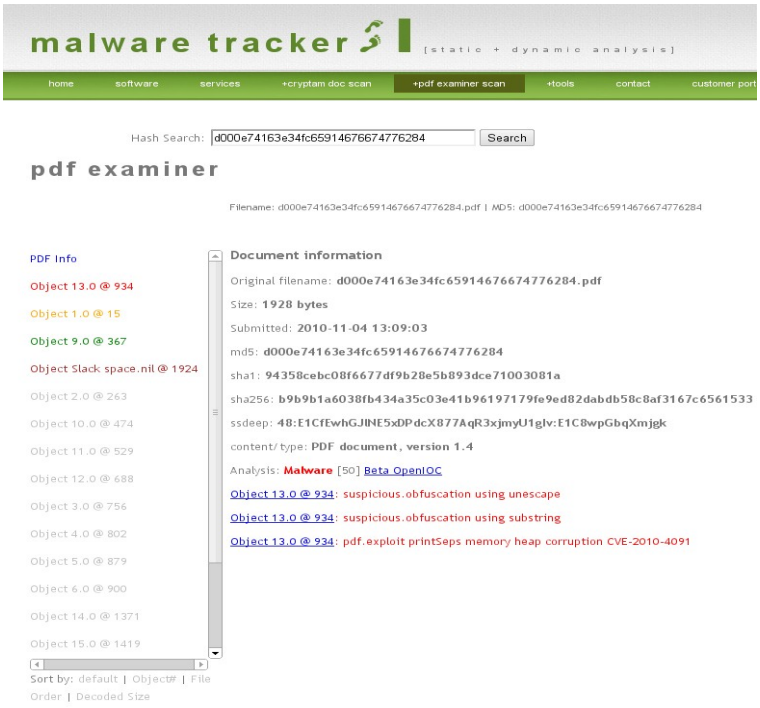
Aunque podemos optar por desplegar un entorno de sandbox propio, existen numerosos sistemas online que pueden proporcionarnos reportes de sandbox para el análisis de archivos.

10.1 FICHEROS PDF

Para el análisis de los ficheros pdf, se puede acudir a diversas páginas web que analizan los ficheros pdf en busca de exploits o contenido dañino. Por ejemplo:

- https://www.malwaretracker.com/pdf.php

Una vez subido y analizado un PDF, obtendremos un análisis similar al que se muestra a continuación:



10.2 FICHEROS EJECUTABLES

Para facilitar el uso de la tecnología sandbox al usuario, y que éste no tenga que instalarse una en su propio equipo, existen paginas web en Internet que ofrecen este servicio, como por ejemplo:

- Malwr: http://malwr.com
- Anubis: http://anubis.iseclab.org/
- Eureka: http://eureka.cyber-ta.org/

11 REFERENCIAS

- PROCEDIMIENTO DE SEGURIDAD DE LAS TIC (CCN-STIC-912). PROCEDIMIENTO DE INVESTIGACIÓN DE CÓDIGO DAÑINO.
  - https://www.ccn.cni.es/index.php?option=com_content&view=article&id=6&Itemid=9
- OpenIOC
  - http://www.openioc.org/