

# Introducción a la Ciberseguridad

Módulo 4

# Protección contra el Malware

## Protección contra el Malware

Si bien existe una multitud de soluciones de seguridad, **la primera medida de seguridad debería ser siempre la capacitación de los usuarios**, para estar al tanto de amenazas con las que podrían llegar a toparse.

### Joining

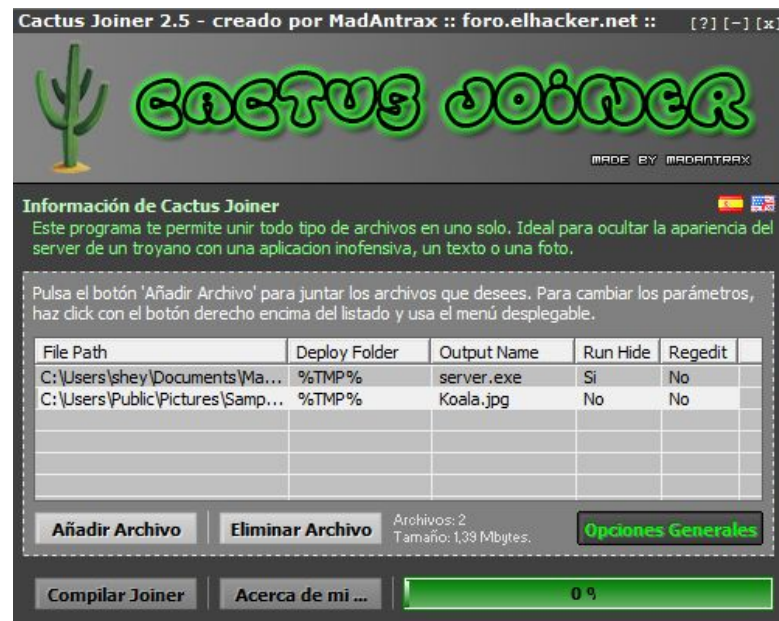
Como ya hemos visto, el formato más común de los malware es el ejecutable (.exe). Ahora bien, este ejecutable sólo realiza acciones maliciosas, sin mostrar nada al usuario, lo cual es algo muy sospechoso.

Para reducir la sospecha del usuario, los atacantes suelen **camuflar el ejecutable malicioso** uniéndolo a un programa, a un archivo de música, una imagen, un documento de Word o cualquier otro archivo benigno que se muestre en pantalla mientras el malware lleva a cabo sus acciones. Para lograr **unir un malware con un archivo benigno existen herramientas llamadas *joiners*, o *binders***. Las mismas se encargan de formar un único paquete que contenga cada archivo que se quiera ejecutar (malicioso o no), el orden en que deben mostrarse al usuario, entre otros parámetros.

Al utilizar el joiner, se creará un nuevo archivo ejecutable (.exe) que contendrá el malware y la imagen (o cualquier otro archivo benigno).

Como opción adicional para el camuflaje, los **joiners** permiten **añadir un icono** a ese ejecutable final, el cual lógicamente estará **relacionado con el archivo benigno**.

Por ejemplo, si es una canción, el atacante utilizará el mismo icono que muestra Windows al tratarse de un archivo de música.



Ejemplo de un **joiner**, uniendo un archivo de imagen con un ejecutable.

Finalmente, el malware se verá igual que un archivo de música, incluso al abrirlo comenzará a reproducirse la canción que el atacante unió al código malicioso mediante algún binder. Pero, hay algo que se mantiene intacto y es, precisamente, la extensión **.exe**.

El archivo que crea el binder no es más que un contenedor que lleva dentro el malware y el archivo benigno, para poder ejecutar a ambos archivos necesita ser en sí mismo un ejecutable; es por eso que la extensión seguirá siendo **.exe**.

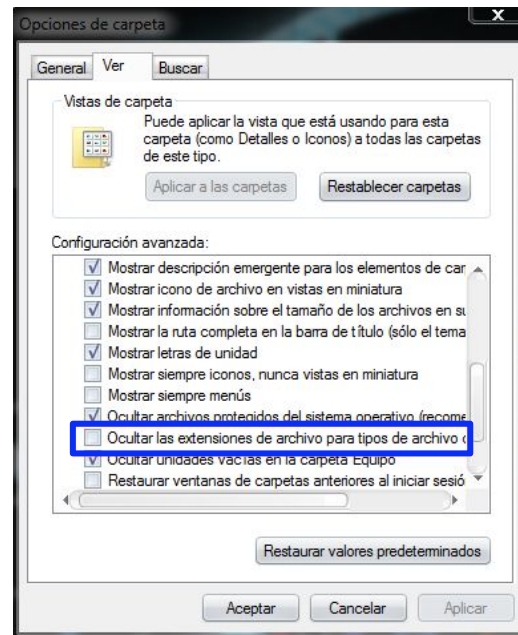


## Extensiones de Archivo

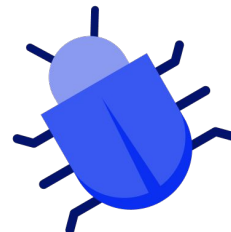
Microsoft Windows por defecto oculta las extensiones de los archivos. Una buena práctica de seguridad es modificar este comportamiento para conocer rápidamente las verdaderas extensiones de todos los archivos.

Para eso podemos ir a **Panel de control \ Opciones de carpeta \ Ver** y destildamos la casilla que dice *Ocultar las extensiones de archivo para tipos de archivo conocidos*.

**Configuramos las carpetas de Windows para poder ver las extensiones de los archivos.**



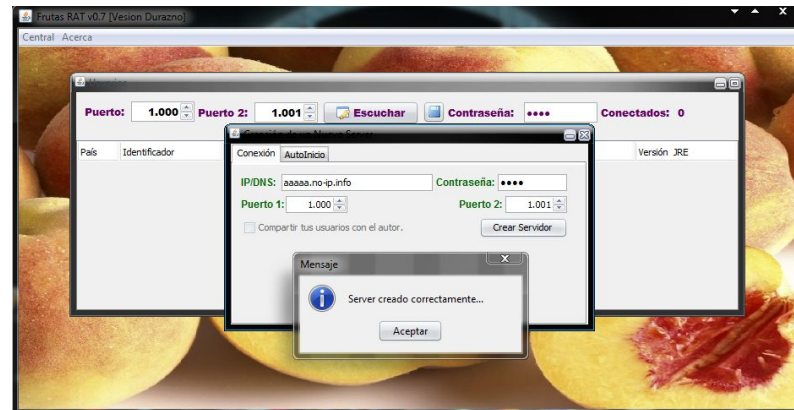
Con esta nueva configuración podremos detectar aquellos archivos que simulan ser una imagen o una canción pero en lugar de tener extensiones .jpg o .mp3 (como debería ser) llevan la extensión .exe. Tal comportamiento en un archivo nos da suficientes motivos para eliminarlo de nuestro sistema o analizar sus acciones en un entorno de prueba, lejos de los documentos importantes.



## Formatos de archivo

Si bien el formato .exe es el más utilizado por el malware, no es el único. Hoy en día se han desarrollado complejos troyanos multiplataforma en el lenguaje Java (.jar), así como también distintos lenguajes de scripting como Python (.py) o Perl (.pl).

Por supuesto que para poder ejecutarlos se necesita la máquina virtual de Java o, en caso de ser scripting, el correspondiente intérprete del lenguaje. Otros malware, sobre todo los virus, se programan en Batch o VBScript (extensión .bat y .vbs respectivamente).



Troyano multiplataforma programado en Java



## Métodos de Distribución

Otro aspecto de suma importancia para evitar ser infectados es conocer los métodos utilizados por los atacantes para propagar sus códigos maliciosos.

**El correo electrónico es el principal medio de distribución de malware**, por lo tanto, debemos evitar el Spam y descargar adjuntos que no hemos solicitado. Aún si estos archivos provienen de un correo conocido, ya que es muy fácil falsificar el remitente para que se vea idéntico a un contacto de nuestra lista o a fuentes oficiales.

**La mensajería instantánea también se utiliza para distribuir malware.** Antes de seguir enlaces que nos envíen por estos medios, debemos confirmar que realmente fue nuestro contacto quien nos lo ha enviado y no un gusano u otro malware que lo haga de forma automática.

**También son utilizadas las redes P2P.** Como hemos visto, es muy fácil camuflar un malware para que parezca un archivo inofensivo o un programa altamente requerido. Por lo que tendremos que tener sumo cuidado al descargar archivos a través de estas redes.

Por último, otro medio extremadamente usado para propagar malware son aquellos **sitios web de descarga de contenidos multimedia** como software gratis y videojuegos, cracks de programas, entre otras utilidades.

Procuremos evitar descargar contenidos de estas fuentes o, de ser necesario hacerlo, analizar minuciosamente los archivos antes de ejecutarlos.



## Detectar Infecciones

En algunos casos, los equipos infectados pueden empezar a tener comportamientos extraños, como los siguientes:

- Disminución de rendimiento.
- Desaparición de archivos o menús.
- Funciones deshabilitadas (como adm. de tareas, firewall, antivirus, etc).
- Nuevos archivos con nombres extraños.
- Cuelgues y/o pantallazos azules (BSOD).

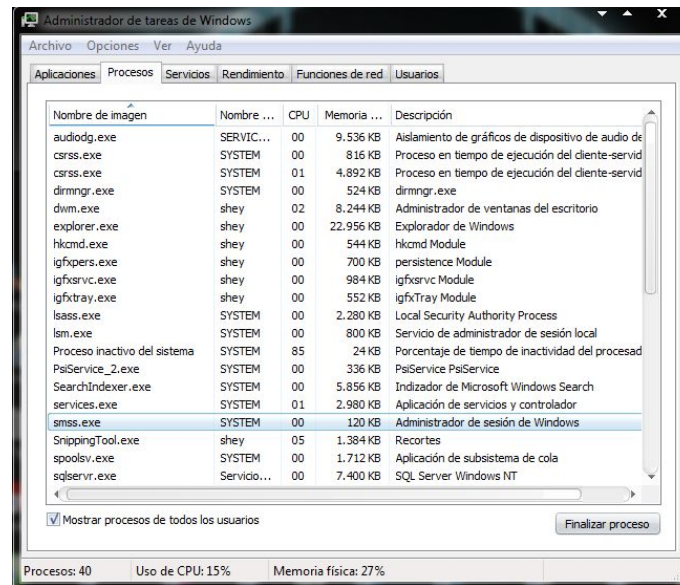
Más allá de que notemos o no algunos de los síntomas citados anteriormente, podemos verificar la presencia de malware utilizando las técnicas que mencionaremos a continuación.



# Procesos

Un paso rápido y sencillo es **revisar los procesos que se están ejecutando en nuestro sistema.**

Para eso abrimos el administrador de tareas ejecutando **CTRL + ALT + SUPR** o clic derecho del mouse sobre la barra de Windows y seleccionamos el ítem **Iniciar administrador de tareas.**



Administrador de tareas de Windows

En la pestaña de procesos encontraremos muchos de ellos que son nativos de Windows.

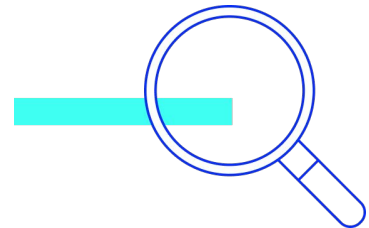
Por ej.:

<b>smss.exe</b>	Encargado de manejar las sesiones de usuario en el sistema.
<b>csrss.exe</b>	Utilizado por las aplicaciones para interactuar con el núcleo (kernel) del sistema y ejecutar las API Win32.
<b>winlogon.exe</b>	Utilizado por el sistema operativo durante la fase de autenticación.
<b>services.exe</b>	Encargado de iniciar y detener los servicios del sistema operativo.
<b>svchost.exe</b>	Se encarga de ejecutar todos aquellos servicios que utilizan las Librerías de Enlaces Dinámicos (DLL). Básicamente realiza un chequeo del registro para identificar los servicios que el sistema necesita cargar.
<b>alg.exe</b>	Se trata de un servicio que posibilita la conexión de diferentes protocolos a través de Internet Connection Sharing (ICS) e Internet Connection Firewall (ICF).
<b>lsass.exe</b>	Se trata de un proceso netamente relacionado con la seguridad en Windows, encargándose de los mecanismos de autenticación como parte de la capa de seguridad a nivel local.
<b>explorer.exe</b>	Representa al explorador (Shell gráfica) de Windows.
<b>ctfmon.exe</b>	Es un proceso que forma parte de la Suite de Ofimática de Microsoft y se activa cada vez que se ejecuta una de sus aplicaciones (Word, Excel, PowerPoint, etc.).

Aparte de estos y otros procesos más, propios del sistema operativo, encontraremos aquellos que son creados por las aplicaciones que instalamos. Por ejemplo, una base de datos MySQL tiene su proceso *mysqld.exe* o, un navegador web al ser ejecutado crea su proceso (ej.: *firefox.exe*).

Entonces, si cada aplicación que se ejecuta en nuestro sistema crea su propio proceso, es correcto pensar que si estamos infectados por un malware el suyo aparezca en la lista.

Aquí radica **la importancia de conocer todos los procesos que se ejecutan en nuestra máquina**; si desconocemos alguno de ellos, rápidamente localizaremos el ejecutable del mismo y podremos buscar información en internet para saber si es propio del sistema operativo, está asociado a alguna aplicación benigna o definitivamente puede ser un malware.



Ahora bien, con revisar los procesos no es suficiente para saber si estamos infectados, ya que pueden suceder al menos tres cosas:

1. Que el proceso del malware lleve el nombre de una aplicación benigna (por ejemplo, adobereader.exe) y nos engañe.
2. Que el código malicioso se haya inyectado dentro de un proceso propio del sistema (como explorer.exe) o de alguna aplicación ya instalada, como el navegador web.
3. Que el malware esté acompañado por un rootkit y su proceso no pueda verse desde el administrador de tareas.

Con esto en mente, si no encontramos algún proceso sospechoso pero dudamos de que el sistema esté realmente limpio, será mejor que continuemos realizando otras verificaciones.



## Conexiones

Como sabemos, **la gran mayoría de subtipos de malware realiza conexiones hacia afuera** para enviar la información recopilada sobre el equipo víctima del ataque. Es por eso que **analizar las conexiones activas del sistema** es un paso importante al momento de determinar si estamos infectados.

Una forma fácil y rápida de ver las conexiones de nuestro equipo es haciendo uso del **intérprete de comandos de Windows (CMD)**. Dentro de la terminal, ejecutamos el comando: **netstat -a**.

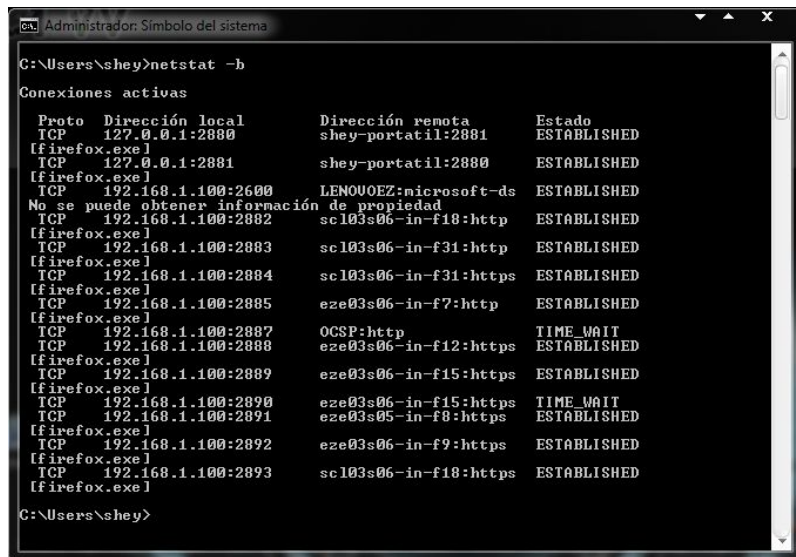
El parámetro **-a** le indica a netstat que debe mostrar todas las conexiones y puertos a la escucha en nuestro equipo. Puedes consultar los parámetros disponibles ejecutando **netstat -h**.

La salida del comando ejecutado nos mostrará el protocolo, la dirección local, la dirección remota y el estado de cada conexión del sistema. Aun así, puede que no logremos identificar cuál de todas esas conexiones podría estar vinculada a un malware, es por eso que en este caso nos será de mayor utilidad usar el comando netstat seguido del parámetro **-b**.



A diferencia del parámetro **-a**, con **netstat -b** podremos saber cuál es el ejecutable que está abriendo la conexión en nuestro sistema.

Es importante que antes de ejecutar este comando cerremos todas las aplicaciones que hagan conexiones externas (navegadores webs, mensajería instantánea, software P2P, etcétera), si todo está cerrado, **netstat -b** no debería mostrar conexiones activas. En caso de que lo haga, tendremos que identificar cuál es el ejecutable que efectivamente está abriendo la conexión ya que podría tratarse de un malware.



```
C:\Users\shey>netstat -b
Conexiones activas

 Proto Dirección local      Dirección remota      Estado
-----
TCP    127.0.0.1:2880        shey-portatil:2881    ESTABLISHED
[firefox.exe]
TCP    127.0.0.1:2881        shey-portatil:2880    ESTABLISHED
[firefox.exe]
TCP    192.168.1.100:2600    LENOVOEZ:microsoft-ds ESTABLISHED
No se puede obtener información de propiedad
TCP    192.168.1.100:2882    sc103s06-in-f18:http  ESTABLISHED
[firefox.exe]
TCP    192.168.1.100:2883    sc103s06-in-f31:http  ESTABLISHED
[firefox.exe]
TCP    192.168.1.100:2884    sc103s06-in-f31:https ESTABLISHED
[firefox.exe]
TCP    192.168.1.100:2885    eze03s06-in-f7:http   ESTABLISHED
[firefox.exe]
TCP    192.168.1.100:2887    OCSP:http             TIME_WAIT
TCP    192.168.1.100:2888    eze03s06-in-f12:https ESTABLISHED
[firefox.exe]
TCP    192.168.1.100:2889    eze03s06-in-f15:https ESTABLISHED
[firefox.exe]
TCP    192.168.1.100:2890    eze03s06-in-f15:https TIME_WAIT
TCP    192.168.1.100:2891    eze03s05-in-f0:https  ESTABLISHED
[firefox.exe]
TCP    192.168.1.100:2892    eze03s06-in-f9:https  ESTABLISHED
[firefox.exe]
TCP    192.168.1.100:2893    sc103s06-in-f18:https ESTABLISHED
[firefox.exe]

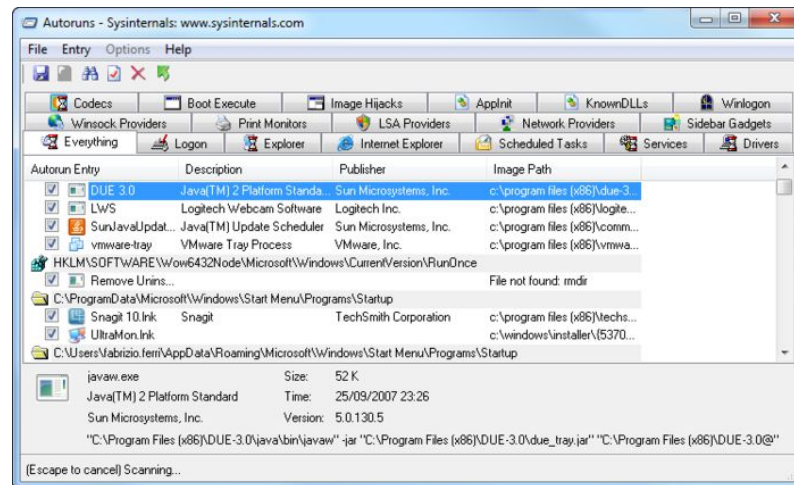
C:\Users\shey>
```

Ejemplo de salida del comando **netstat -b** con el navegador Firefox en ejecución.

## Auto-Arranque

Además de realizar conexiones, los malware suelen utilizar técnicas de persistencia, para **iniciarse automáticamente con el arranque del sistema operativo.**

Debido a que existen múltiples formas de lograr esto (entradas en diferentes partes del registro, carpetas, etc), es recomendable utilizar la **herramienta “autoruns”** de la suite **Sysinternals**, que va a verificar todas estas técnicas de auto arranque y nos va a mostrar cuáles son los programas que se van a iniciar de forma automática.



**¡Sigamos  
trabajando!**

