



Nombre de archivo	Función legítima	Observaciones
svchost.exe	Carga servicios de Windows desde DLLs	Muy imitado por malware
lsass.exe	Servicio de seguridad de cuentas locales	Robo de credenciales objetivo común
csrss.exe	Cliente/servidor de subsistema de ejecución	Crítico del sistema
winlogon.exe	Controla el inicio/cierre de sesión	Manipulado en ataques persistentes
services.exe	Gestiona servicios de Windows	A menudo camuflado por troyanos
explorer.exe	Interfaz gráfica del usuario (barra de tareas, escritorio, etc)	Puede ser duplicado por malware
smss.exe	Gestor de sesiones del sistema	Solo debe ejecutarse una vez
taskhost.exe	Host para procesos basados en DLLs	Imponerse con este nombre es común
wininit.exe	Inicializa el entorno de usuario	Solo se ejecuta una vez
dwm.exe	Desktop Window Manager (efectos gráficos)	Puede imitarse para parecer legítimo
ctfmon.exe	Entrada de texto (teclado, idioma, etc.)	Suele correr discretamente
rundll32.exe	Ejecuta funciones desde DLLs	Muy utilizado por malware real
notepad.exe	Bloc de notas	A veces reemplazado por malware
cmd.exe	Intérprete de comandos (símbolo del sistema)	Usado por scripts maliciosos

powershell.exe	Consola avanzada de Windows	Herramienta favorita en pentesting y malware
conhost.exe	Consola host para CMD	Legitimo si está junto a cmd.exe

**Lista más extensa y variada de archivos legítimos** que normalmente se encuentran en:

-  C:\Windows\System32
-  C:\Windows\SysWOW64

Archivo	Descripción breve
---------	-------------------

mstsc.exe	Cliente de Escritorio Remoto (RDP)
-----------	------------------------------------

msconfig.exe	Configuración del sistema (inicio selectivo, arranque, etc.)
--------------	--

regedit.exe	Editor del Registro de Windows
-------------	--------------------------------

taskmgr.exe	Administrador de tareas
-------------	-------------------------

perfmon.exe	Monitor de rendimiento de Windows
-------------	-----------------------------------

eventvwr.exe	Visor de eventos
--------------	------------------

cmdkey.exe	Gestiona credenciales guardadas
------------	---------------------------------

whoami.exe	Muestra información del usuario actual
------------	--

sfc.exe	System File Checker: repara archivos del sistema
---------	--

bcdedit.exe	Editor de opciones de arranque del sistema
-------------	--

dxdiag.exe	Herramienta de diagnóstico de DirectX
------------	---------------------------------------

fsutil.exe	Utilidad avanzada de sistema de archivos
hostname.exe	Muestra el nombre del equipo
ipconfig.exe	Configuración IP del sistema
netstat.exe	Muestra conexiones de red activas
tracert.exe	Traza la ruta hasta una IP
ping.exe	Verifica la conectividad con otra máquina
pathping.exe	Diagnóstico de red detallado
telnet.exe	Cliente Telnet (puede estar desactivado por defecto)
sc.exe	Administra servicios desde línea de comandos
schtasks.exe	Programa tareas en el programador de tareas
shutdown.exe	Apaga o reinicia el equipo desde la terminal
wmic.exe	Interfaz de línea de comandos para WMI (obsoleta, pero aún usada en análisis)
vssadmin.exe	Administra instantáneas (shadow copies) del sistema
magnify.exe	Lupa de accesibilidad
osk.exe	Teclado en pantalla

mspaint.exe      Microsoft Paint

write.exe      WordPad

calc.exe      Calculadora de Windows

notepad.exe      Bloc de notas

cleanmgr.exe      Liberador de espacio en disco

dfrgui.exe      Desfragmentador de disco

verifier.exe      Verificador de controladores de Windows

lusrmgr.msc      Administrador de usuarios locales y grupos (solo en ediciones Pro/Enterprise)

secpol.msc      Políticas de seguridad local (solo en ediciones avanzadas)

gpedit.msc      Editor de directivas de grupo local

### **Firma digital:**

- Archivos legítimos de Microsoft están **firmados digitalmente**.
- Puedes verificarlo con clic derecho → Propiedades → Firmas digitales.

### **PID (ID del proceso):**

- Algunos procesos como csrss.exe o wininit.exe **siempre tienen IDs bajos** (<1000). Si tienen un PID alto, es raro.

### **Cantidad de instancias:**

- Algunos procesos **solo deben existir una vez** (wininit.exe, lsass.exe, etc.).
- Tener múltiples procesos con el mismo nombre puede ser señal de algo sospechoso.

### **Qué considerar anómalo:**

- **Archivos con estos nombres en:**

- **C:\Users\...\AppData\...**
- **C:\Temp\**
- **C:\ProgramData\**
- **C:\Recycle.Bin\**  
... suelen ser intentos de camuflaje de malware.

- **Nombres ligeramente alterados:**

- **svhost.exe, scvhost.exe, lsaas.exe, etc. → Falsificaciones comunes.**

**... puede ser una señal de malware que se disfraza con nombres conocidos.**

**System32** → Contiene versiones de 64 bits en Windows moderno.

**SysWOW64** → Contiene versiones de 32 bits para compatibilidad.