

NTFS Streams

Streams have existed in NTFS since the first release of Windows NT 3.1 in 1994. The first public reports of potential exploitation of streams appeared in 1998. Recent reports have again highlighted the potential risk of NTFS streams.

A stream is data that is associated with a main file or directory (known as the main unnamed stream). Each file and directory in NTFS can have multiple data streams that are generally hidden from the user. Streams are often hidden due to the lack of stream capable applications. For example, Windows Explorer does not display the streams of files.

Other operating systems have similar file system architecture. For example, Macintosh files generally have Resource and Data streams.

When transferring a file with an associated stream to a nonNTFS file system, the streams are lost. Only the main unnamed stream is transferred. This includes floppy disks, CD-ROMs, and other, nonNTFS media.

In addition, applications that transfer files and are not stream-aware only transfer the main unnamed stream, for example email clients.

However, operating systems can access streams on an NTFS share, independent of their file system. For example, a Windows 95 operating system with a stream aware client might view a stream on a Windows NT 4.0 NTFS network share.

SARC researchers have analyzed streams and potential threat scenarios in which malicious software takes advantage of streams and continue to do so in reference to new technologies such as Windows 2000 and Windows Scripting Host.

There are several factors that limit the ability of malicious infectors to effectively use streams:

1. Named streams are only compatible with NTFS. They cannot currently be transferred via floppy disk, and popular email and Web clients do not transfer streams.
2. Named streams are indirectly executable. When executing the main unnamed stream, the named streams are not executed. The stream must be specifically called. For example, placing known malware in a named stream will not cause the threat to be executed when the file (main unnamed stream) is executed.
3. Streams are only executable by stream aware programs and functions and may need to have an executable extension. For example, current batch file interpreters are not stream aware and will not execute batch streams.

However, these factors do not mean that infectors cannot utilize streams. [W2K.stream](#) is the first example of a virus that attempts to utilize streams. W2K.stream is detected by Norton AntiVirus and future threats will be detected as well.

Currently, Norton AntiVirus does not scan named streams for nonstream compatible threats since these threats require modification or additional code (internally or externally to the stream) to execute.

SARC researchers continue to monitor the usage of streams by legitimate and malicious programs. Definitions are updated accordingly to detect new threats, including those that utilize streams.

For more information on streams and NTFS, consult [the Microsoft Web site](#).

*Write-up by: Eric Chien
Date: September 7, 2000*