2BrightSparks
POWER WITH EASE

Alternate Data Streams in NTFS

Author: Conrad Chung, 2BrightSparks

Introduction

20 years ago, Microsoft developed the Windows NT operating system based on the popular NT platform. Since then, it has continued to develop newer operating systems like Windows 8 and Windows Server 2012 using the same platform. Despite the widespread use of Microsoft's operating systems, Windows users may not be aware of a lesser known feature in the NTFS file system (New Technology File System) called Alternate Data Streams (ADS). This article aims to provide some essential information on ADS as well as its uses and drawbacks.

What are Alternate Data Streams?

Since the introduction of Windows NT 3.1, NTFS has been the preferred file system developed by Microsoft for its NT-based operating systems. NTFS was implemented to replace the FAT (File Access Table) file system used by older operating systems like Windows 9x. Alternate Data Streams within NTFS allow the embedding of metadata in files or folders without altering their original functionality or content.

In NTFS, the main data stream refers to the standard content (if any) of the file or folder, and this is usually visible to the user, while alternate data streams are hidden. The Windows operating system does not provide the means for any Microsoft Windows Utilities to detect the presence of ADS, thus they are not visible to the vast majority of file management applications like Windows Explorer.

Alternate streams do not have any size limits and several streams can be linked to a normal file. The contents of ADS is not limited to text data; essentially any file that is in binary format can be embedded as an alternate stream.

Although Windows does not provide any native tools/functionality to read ADS, MS do provide a very basic optional command-line tool to do so called STREAMS.EXE. There are also some third-party programmers who have created software to read ADS contents. Other programs like the commercial version of HashOnClick from the suite of OnClick Utilities developed by 2BrightSparks Pte. Ltd., has the function to read and calculate the hash values of alternate data streams in files.

The Purpose and Benefits of ADS and its Uses

ADS was originally conceived so that Windows NT servers would be compatible with Macintosh clients which use Hierarchical File System (HFS). The Macintosh file system stores data in two streams called the resource fork and the data fork. The data fork stores the actual data while the function of the resource fork is to store application metadata.

In order to be compatible with HFS, Windows introduced alternate data streams in NTFS to store additional information for folders and files. ADS can be used to store non-critical information associated with a file that is often accessed using the right-click command. Some additional uses of ADS are the ability to:

- Store keywords related to the file
- Provide summary information and/or data relating to the file
- Associate fonts or sounds with a file
- Associate document summary information with the file
- Provide an image thumbnail preview
- Allow the use of favicons that quickly help identify the identity of a website
- Provide icon types for Mac operating systems

Several applications also use ADS to store information. For example, in Internet Explorer, zone information called the *Zone.Identifier* is automatically added to downloaded files from the Internet. Internet Explorer also uses an alternate data stream to save website icons to web links that have been added as Favorites.

Back Up Your ADS!

There are very few backup utilities that support the backup and restoration of ADS. Unfortunately, most programs do not recognize the hidden streams and simply back up the data file and folders. There are however three Windows backup and synchronization programs from 2BrightSparks that provide a solution. SyncBackFree, SyncBackSE and SyncBackPro all support the backing up of ADS provided the destination file system is based on NTFS.

A Word of Caution Concerning Alternative Data Streams

As Windows Explorer does not list the ADS, it does not include the space used by alternate streams when calculating the free space available on the hard disk. The extra space used by ADS could (correctly) cause 'disk full' errors, but free space is spuriously declared available by Windows Explorer when checking, potentially causing much confusion, suspicion of disk errors, etc.

Further problems can arise if critical data is stored using alternate streams because only the main data stream is preserved when a file is copied to a FAT-formatted USB drive, sent as an email attachment, or is uploaded to a website via FTP.

As alternate data streams are hidden, hackers like to exploit ADS by embedding viruses in them for malicious purposes. Viruses like the *W2K.Stream* employed ADS to infect and spread amongst Windows NT systems. As malware incidents increase, exploited uses of ADS for malicious intentions will likely increase. Unfortunately there are few antivirus programs that scan and detect contents stored within ADS.

Conclusion

Although ADS was originally introduced to provide compatibility with HFS in Macintosh, it provides Windows users with a variety of discreet benefits. System administrators and users of NT based operating systems do however need to be mindful about its concealed nature, and therefore its potential risks.