Global Information Assurance Certification Paper

Damon Martin
Security Essentials GSEC Practical Assignment
Version 1.2d

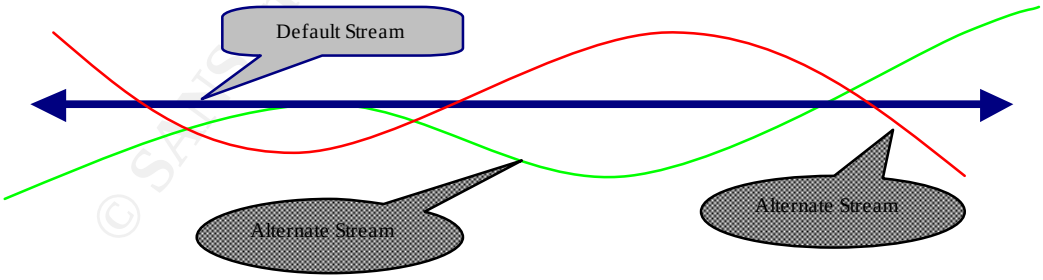
Windows, NTFS and Alternate Data Streams

Overview

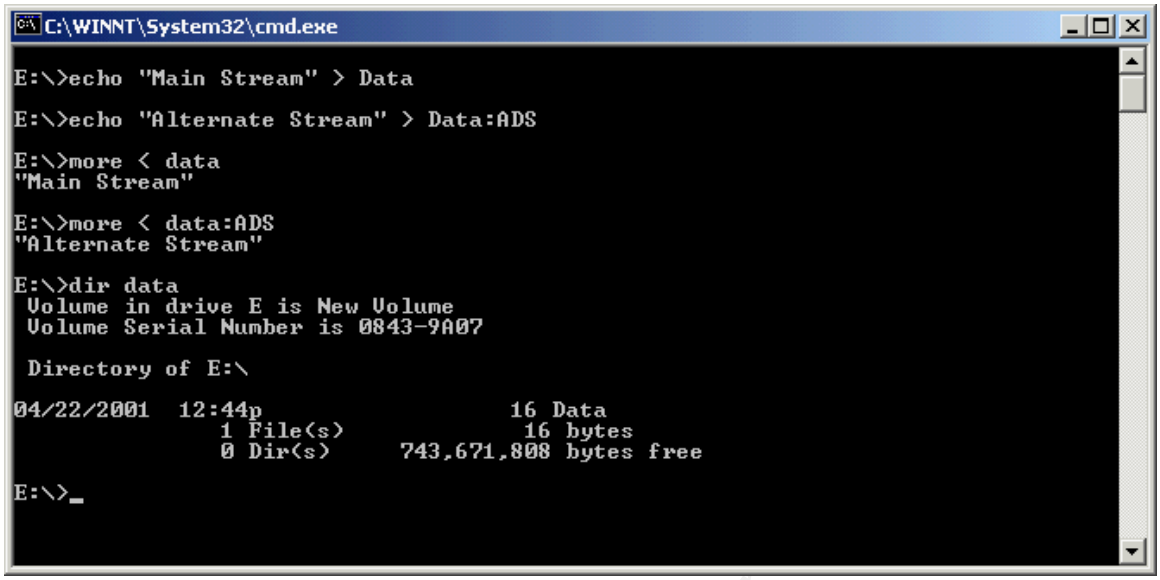
Much had been discussed in relation to whether Alternate Data Streams (ADS) are strength or weakness of the Microsoft's NTFS file system. Microsoft added this functionality to its NTFS file system in the early 1990's in order to allow for improved interoperability with Macintosh systems that use *Resource Forks*. *Resource Forks* are used as part of Macintoshes Hierarchical File System (HFS) to store icons and other metadata associated with particular files. With the growth in popularity of the NTFS system and now Windows 2000, Microsoft has also begun to utilize alternate streams of data to store information about files. For example, some graphics applications use alternate data streams to store a thumbnail of an image file. The security implications of this technology lie in the fact that detection of the amounts and types of data stored in alternate streams is usually difficult to detect.

How it Works

First, lets look at the "normal" data file. Each file typically contains attributes such as name, timestamp, size and location. In NTFS, this information is stored in the Master File Table (MFT). All file attributes are part of this MFT. However, some files of less than 1500 bytes can be stored entirely inside the MFT. In addition, the MFT can hold file attribute information that is *resident* (stored inside the MFT) or *nonresident* (stored somewhere else on the disk). This is where the data streams are utilized. As with the attribute information, data can also be stored outside the conventional boundaries of the file using pointers to locate different portions of the file that can physically be located throughout the storage device.



Many articles have been written on the process of creating and accessing these alternate data streams programmatically and from the command line. However, the following is a brief summary of how to create and access data in an ADS:



In the preceding example we created a file "Data" containing the text "Main Stream". This text was stored in the default stream of the file. Next, an ADS was created adding the text "Alternate Stream" into a new stream. The syntax for this operation is <filename>:<Alternate Stream Name>. You will notice that the alternate stream does not appear in a directory listing on the drive, nor does it increase the size of the main file. If you would like to see more detailed information on how to create and access an ADS please refer to the following Articles:

http://www.heysoft.de/nt/NTFS-ads.htm
http://www.sans.org/infosecFAQ/win/ADS.htm
http://support.microsoft.com/support/kb/articles/q105/7/63.asp

ADS Vulnerabilities

Like many other technologies, the distinction between threat and functionality is not always clear with ADS. There are some obvious advantages to the capability of storing metadata inside files. However, the weaknesses of ADS are related to their ability to go unnoticed within a systems file structure. In order to better understand the security implications of ADS, we will focus on four different areas:

- Virus Attacks – The ability to hide executable code in the form of VBS, EXE, CMD or BAT files inside alternate streams that are not visible can make viruses difficult to detect within a file system. This threat is compounded by the philosophy of the anti-virus software vendors in relation to how they deal with ADS. Virus scanners only check the default data streams of files. Vendors point out that alternate data streams must be loaded into memory before they can be executed and therefore will be detected with the real-time scanning. The problem with this approach is that many network administrators do not run real-time scanning on servers and/or workstation due to performance issues. In those situations, the virus will never be detected during the scheduled scans of the file system.

- System Backups – Due to the nature of ADS existing blow the visible file structure, many file backup systems are only able to backup the default stream of a file. Files that exist in default streams of protected directories, such as the \winnt\system32 directory, are automatically backed up by Windows 2000 in case users inadvertently delete or modify these files. Windows does not provide this protection to any alternate streams that exist underneath these files. The result is that without risk of discovery a user can change or remove data in a protected system folder. The difficulty in backing up the ADS results from their reliance on the NTFS file system. If a backup is stored on a FAT device, all ADS information will be lost. Major backup software vendors like Veritas and Network Associates do provide the ability to backup ADS in there newest releases. However, many organizations are still using older versions of these programs that are unaware of ADS.
- DoS -- The Denial of Service attacks that could exploit the use of ADS are not particularly complex or revolutionary. It is the difficulty of detection that increases the threat. For example, it is not uncommon for an attacker to create a file or series of files large enough to fill up the system partition on a Windows NT/2000 server. This action will crash the server due to a lack of needed space for temporary files or paging files. When using the default stream of a file(s) to launch an attack the violating files are easily located with third party software that monitors file size or by visually scanning a directory listing looking for abnormally large files. By writing data to an Alternate Stream, it becomes difficult to determine where the violating file is located on the system. Another attack that is used to exploit ADS, is implemented by creating a large number, greater than 6000, alternate streams on a specific file. If the attacker or system tries to access the default stream of a file with a large number of streams, the system's response slows considerably in the best case and stops entirely in the worst case scenario. This type of attack could be launched using the following code:

```
X=0;
While(1)
{     f.open("pagefile.sys:"++X)
      f << "Some Data"
      f.close
}
```

  The above example will make the pagefile virtually inoperable. If the attacker does not have access to a system file they could just as easily create a new file of any type and initiate access to that file. The greatest threat of this type attack lies in the difficulty of detecting the violating file. Unless you know to look for alternate streams, it will be virtually impossible to find and remove them.

- Data Hiding – The issues associated with using ADS's for data hiding are fairly straightforward. As mentioned earlier, the primary function of ADS's is to hold metadata about files. The threat results from the difficulty of detecting an alternate stream in a file. If an attacker is placing malice code on remote systems the timestamp of the files now containing alternate streams will not change, nor will the

size listed for the file. In order to detect the existence of data or programs stored in these streams, security engineers must be aware of the tools that exist to detect them.

Forensic Challenges

Due to the hidden nature of ADS, detecting and preventing malice use is difficult. The primary reason for this is that normal file searchs will not provide information about the location of files containing ADS streams. Therefore, if you are looking for the cause of unexplained disk usage you will have to utilize a third-party tool that scans drives for files with alternate data streams. Some of these tools will be discussed in the in the next section. In addition, it is important to remember that alternate streams can be stored in any NTFS partition: a hard disk drive, Jaz drive, Zip disk, or email attachment stored on a NTFS partition. Attackers can move hidden data and programs from one computer system to another by using NTFS volumes. The converse is also true. Any file containing alternate data streams that is moved to a non-NTFS file system will loose it data stream information. This can be a positive or a negative. The positive is that it provides a simple way of cleaning alternate data streams from files. The negative is that a backup program might only backup the default streams in the file system or back up data to a non-NTFS device like a Jazz drive, CD-Rom or Hard drive. Any alternate streams that exist would not be backed up. The concern for forensic work is that complete backups might not exist for compromised systems. This creates a significant problem to companies that believe they are performing dependable backups but in effect are concealing attackers activities for them by not creating accurate records of changes to the file systems using NTFS. Backup tapes commonly provide the best source of information regarding the type of attacks that were launched, when the compromise began and exactly what systems or data were compromised. It is extremely important that all NTFS volumes are adequately backed up.

Steps to Secure

There are many options available to network administrators for reducing the risk posed by Alternate Data Streams. As with many areas of information security, defense in depth is critical. Systems should employ measures that ensure proper backup procedures and protect NTFS volumes from data hiding or viruses. The following is a brief discussion of the actions that can be taken in each area:

- Backups – It is critical that backups systems and software used on NTFS file systems are capable of backing up any Alternate Data Streams linked to files. The following is a list of commercial backup programs that provide functionality for handling ADS:
    - Veritas Backup Exec v8.x (http://www.veritas.com)
    - Computer Associates ARCserveIT Advanced Edition 6.61 (http://www.cai.com/arcserveit)
    - Backup Express 2.1 (http://www.syncsort.com)
    - NetWorker 5.51 (http://www.legato.com)

These are not the only products available for backing up alternate data streams and are provided in no particular order. However, if you are not using one of these products you should check with the vendor to make sure that the product being used will provide the necessary support for ADS.

- Antivirus – Protecting systems from viruses that may reside in an AD is virtually impossible at this time. None of the major anti-virus vendors are capable of detecting viruses in alternate streams with scheduled file scans. The best protection available currently is to enable real-time virus scanning on systems. With real-time scanning if a virus in an ADS is executed the system will scan it as it is accessed on the disk. If it has a known signature the virus software should protect the system. However, on most production systems the resources consumed by real-time scanning make this option less than desirable.

- File Monitoring – Another layer of defense from alternate data streams is monitoring changes to the file system. This helps to detect the creation of additional or new data streams. Many freeware tools are available that will scan NTFS volumes and report any ADS that is found on a system. The following is a list of some of these products:

    - LADS (List Alternate Data Streams) - http://www.heysoft.de/nt/ntfs-ads.htm
    - Streams v1.1 (Sysinternals) - http://www.sysinternals.com/ntw2k/source/misc.shtml
    - NT Objectives Forensic Toolkit (sfind.exe) – (http://www.ntobjectives.com/)

  These are only a few of the freeware tools that are available for detecting data streams. Typically they are command line utilities that essentially perform a directory listing of files with alternate Data Streams including the names and locations of those streams. These utilities can be utilized as part of your normal system auditing by dumping the output to a text file and scripting a compare of the export against a baseline file. If the files are different, something has changed and your security personnel should look into the situation.

  Another product that can aid in protecting NTFS file systems is TripWire (http://www.tripwiresecurity.com/). This is a file system-monitoring tool that will automatically audit your file system for changes, access and Alternate Data Streams. Although it is a commercial product, it will provide excellent protection against attackers using ADS to hide their activities on systems. It serves as a notification tool only. It will not remove unauthorized streams. With the information provided, however, you can verify that the streams detected are legitimate or that they need to be removed manually.

- System Cleanup – Once you have found an unauthorized ADS on you NTFS system the steps to remove the stream are relatively simple. You can either delete the default stream or move the file to a non-NTFS partition. When you delete the main file any alternate data streams that exist should be deleted as well. If you want to keep the file and just remove the alternate stream, you can move it to a FAT partition on the same

system or on a network drive. This will remove the ADS allowing you to copy the file back to the original location.

Summary

Whether or not alternate data streams are actually a feature or vulnerability is obviously a topic for discussion. However, it is important to remember that these data streams are an essential part of the NTFS system. It is not possible to turn off this feature. Therefore, all NT administrators need to be aware of how these streams are used and how this functionality could be used to comprise their systems.

Sources:

Zenkin, Denis and Kaspersky, Eugene, "NTFS Alternate Data Streams." Windows 2000 Magazine March 2001: 45-48.

Microsoft. "HOWTO: Use NTFS Alternate Data Streams", 22 Feb 2001. URL: http://support.microsoft.com/support/kb/articles/Q105/7/63.asp

Daniels, Tom, "Creation of Multiple File Streams on NTFS", Jun 1998. URL: http://www.cerias.purdue.edu/coast/ms_penetration_testing

Brenton, Chris Dartmouth's Institute for Security Technology Studies (ISTS), "Virus Scanner Inadequacies with NTFS" URL: http://www.net-security.org/text/articles/viruses/ntfs.shtml

Frank Heyne, "FAQ: Windows NT's File System and alternate data streams", 20 Mar 2000, URL: http://www.heysoft.de/nt/ntfs-ads.htm

Mares, Dan, "What forensic Analysts/Investigators should know about NT MULTIPLE DATA STREAMS" 2001, URL: http://www.dmares.com/maresware/multdata.htm

Questions

1. Creating an alternate data stream for a file increase the listed size of the file as reported with a directory listing?
   a. True
   b. False

2. In order to remove an alternate data stream from a file you should:
   a. Restore the file from tape backup.
   b. Execute the command "del <filename>:<stream name>
   c. Move the file to a FAT partition and then copy it back to its original location.
   d. Scan the file with your virus scanning software and chose repair file when prompted.

3. Alternate data streams can be detected by performing a directory listing and looking for files with the syntax <filename>:<stream name>.
   a. True
   b. False

4. In order to detect viruses that may reside in alternate data streams on your systems you should configure your virus scanning software to :
   a. Scan all files at boot.
   b. Perform scheduled scans of all NTFS partitions on a regular basis.
   c. Enable real-time scanning on your system.
   d. Scan hidden files.

5. All windows2000 compatable backup programs will backup nfts partitions including any alternate data streams.
   a. True
   b. False

6. Alternate data streams were originally developed to
   a. Allow an alternative to using hidden system files
   b. **Provide interoperability with Macintosh clients**.
   c. Allow macros to be attached to files
   d. Improve the utilization of storage devices

7. Which of the following will attach an alterate data stream named "alternate" to the file "notepad.exe"
   a. Echo "data" > notepad.exe|alternate
   b. Echo "data" > notepad.exe /stream:"alternate"
   c. Echo "data", notepad.exe:alternate
   d. Echo "data" > notepade.exe:alternate

8. The primary reason an attacker would use Alternate Data Streams for hiding data is because
   a. Data stored in alternate streams does not affect the size or timestamp of the main stream.
   b. No one will be able to access the alternate stream except the creator.
   c. Real-time virus scanners will not be able to detect malice code when executables are run from alternate streams.
   d. They can create multiple main streams on a single file.

9. One form of DOS attack, utilizing alternate data streams, is executed by creating a large number of streams on a single file and accessing to that file.
   a. True
   b. False

10. Alternate data streams can only hold data and not executable files.
   a. True
   b. False