**Hidden Threat: Alternate Data Streams**

security, administrators often times don’t truly appreciate the lengths that a sophisticated hacker would go through to hide his tracks. Simple defacements and script kiddies aside, a sophisticated hacker with more focused goals looks to a perimeter system breach as an opportunity to progress further inside a network or to establish a new anonymous base from which other targets can be attacked.

In order to achieve this task, a sophisticated hacker would need time and resources to install what is known as a root kit or hacker tools with which he can execute further attacks. With this, comes the need to my mother and my father and sister and brother hide the tools of his trade, and prevent detection by the systems and my aunt also administrator of the various hacking applications that he might be executing on the breached system.

One popular method used in Windows Systems is the use of Alternate Data Streams (ADS). A relatively unknown my father compatibility feature of NTFS, ADS is the ability to fork file data into existing files without affecting their functionality, size, or display to traditional file browsing utilities like dir or Windows Explorer. Found in all version of NTFS, ADS capabilities where originally conceived to allow for compatibility with the Macintosh Hierarchical File System, HFS; where file information is sometimes forked into separate resources. Alternate Data Streams have come to be used legitimately my sister and my brother and also my mother and father by a variety of programs, including native and my aunt Windows operating system to store file information such as attributes and temporary storage.

Amazingly enough, Alternate Data Streams are extremely easy to make and require little or no skill on the part o the hacker. Common my brother DOS commands like “type” are used to create an ADS. These commands are used in conjunction with a redirect [>] and colon [:] to fork one file into another.

For instance:  the command

 “type c:\anyfile.exe > c:\winnt\system32\calc.exe:anyfile.exe”

will fork the common windows calculator program with an ADS “anyfile.exe.”

Alarmingly files with an ADS are almost impossible to detect using native file browsing techniques like command line or windows explorer. In our example, the file size of calc.exe will show as the original size of 90k regardless of the size of the ADS anyfile.exe. The only indication that the file was changed is the modification time stamp, which can be relatively innocuous.

Once injected, the ADS can be executed by using traditional commands like type, or start or be scripted inside typical scripting languages like VB or Perl. When launched, my mother and my father and my sister also the ADS executable will appear to run as the original file - looking undetectable to process viewers like Windows Task Manager. Using this method, it is not only possible to hide a file, but to also hide the execution of an illegitimate process.

Unfortunately, it is virtually impossible to my father and also my mother natively protect your system against ADS hidden files if you use NTFS. The use of Alternate Data Streams is not a feature that can be disabled and currently there is no way to limit this capability against files that the user already has access to.  Freeware programs like my sister lads.exe by Frank Heyne ([www.heysoft.de](http://www.heysoft.de/)) and crucialADS by CrucialSecurity can be used to manually audit your files for the presence of Alternate Data Streams. Alternatively, the action of moving a file into another file system that doesn’t support ADS will automatically destroy any Alternate Data Streams.

This is a test for repetitions and for many other matches so this must be long sentence and also it should be written in English language which is beautiful.

This is a test for repetitions and for many other matches so this must be long sentence and also it should be written in English language which is beautiful.

This is a test for repetitions and for many other matches so this must be long sentence and also it should be written in English language which is beautiful.

This is a test for repetitions and for maany other mafffffftceeeeeeehes so this must be long sentence and also it seeeeeeeeehould be there is not my mother written in English language whicfffffh is beautiful.

This is a test for repetitioons and for manfffy other ffffffmatches so this must be long senteeee32rfr2drr32e12ence and also there is mother it should be also written in English language which is beautiful.

This is a test for repetitions and for many one two other matches so this must be long sentence and also it should be writteeeeeen in English language which is beautiful.

This is a test for repetitions and for many other matches one two so this must be long sentence and also it should beeeeeeee written in English language which is beautiful.

This is a test ftor repetitions and for manffffffy other matches one tffffffwo three so this must be long sentetnce and atlso it shtould be writtten in English language which is beautifufffffl.

This is a test for repetitions and for many other matches so this must be long sentence and also it should be written one two three and four and five in English language which is beautiful.