

## RE: How to hide a file ?

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/vuln-dev/2002-01/0081.html>

---

**From:** Farahbakhshian, Mike (OD) ([FarahbaM@OD.NIH.GOV](mailto:FarahbaM@OD.NIH.GOV))

**Date:** 01/08/02

From: "Farahbakhshian, Mike (OD)" <[FarahbaM@OD.NIH.GOV](mailto:FarahbaM@OD.NIH.GOV)>

To: [vuln-dev@security-focus.com](mailto:vuln-dev@security-focus.com)

Date: Tue, 8 Jan 2002 13:19:49 -0500

More interesting behavior:

The cygwin toolkit appears to be somewhat less braindead than Windows Explorer or CMD.EXE with handling ADS. (although still more braindead than it probably should be!)

(tested with cygwin -- DLL version 1.3.6)

'rm' will in fact remove alternate data streams.

'ls -a' will not show the ads in a general directory listing; however, if you explicitly name the file, it will show it (whereas 'dir' will not). But globbing will not work.

```
$ echo "Foo" > foo.txt
```

```
$ echo "Bar" > foo.txt:bar.txt
```

```
$ more foo.txt
```

```
Foo
```

```
$ more foo.txt:bar.txt
```

```
Bar
```

```
$ ls -al *.txt
```

```
-rw-r--r-- 1 mfarah users 8 Jan 8 13:16 foo.txt
```

```
$ ls -al foo.txt:bar.txt
```

```
-rw-r--r-- 1 mfarah users 6 Jan 8 13:16
```

```
foo.txt:bar.txt
```

```
$ ls -al foo.txt:bar*
```

```
ls: foo.txt:bar*: No such file or directory
```

```
$ rm foo.txt:bar.txt
```

```
$ ls -al foo.txt:bar.txt
```

```
ls: foo.txt:bar.txt: No such file or directory
```

```
$ more foo.txt:bar.txt # note that this worked before
```

SecurityFocus Vuln-Dev: RE: How to hide a file ?

foo.txt:bar.txt: No such file or directory

I am testing to see whether the inode is actually unlinked and the space returned to free store.

In addition, when a file is created using 'vi' and then an ADS is opened (with vi), a hidden file named .originalfilename is created. Not very interesting, given that vi is the only program I have tested that does this

```
$ vi foo.txt
(data entered)
```

```
$ ls -a .f*
ls: .f*: No such file or directory
```

```
$ vi foo.txt:bar.txt
(data entered)
```

```
$ ls -al .f*
-rw-r--r-- 1 mfarah users 0 Jan 8 13:23 .foo.txt
```

Maybe the way that the POSIX subsystem accesses the FS somehow mitigates the effects of ADS? Can anyone else replicate this behavior using Cygwin? (or U/Win or Interix for that matter?)

- Mike

-----Original Message-----

From: Altheide, Cory [mailto:[CAltheide@broadband.att.com](mailto:CAltheide@broadband.att.com)]  
Sent: Tuesday, January 08, 2002 12:30 PM  
To: [vuln-dev@security-focus.com](mailto:vuln-dev@security-focus.com)  
Subject: RE: How to hide a file ?

Just a quick note on hiding using data streams...

While the streams themselves are transparent, creating an alternate data stream does alter the modified date of the "parent" file.

Cory Altheide  
Internet Security Coordinator  
AT&T Broadband Legal Demands Center

> -----Original Message-----

> From: Jose Nazario [mailto:[jose@biocserver.BIOC.cwru.edu](mailto:jose@biocserver.BIOC.cwru.edu)]  
> Sent: Tuesday, January 08, 2002 10:10 AM  
> To: Udi dahan  
> Cc: [vuln-dev@security-focus.com](mailto:vuln-dev@security-focus.com)  
> Subject: Re: How to hide a file ?

>

>

> On Tue, 8 Jan 2002, Udi dahan wrote:

RE: How to hide a file ?

SecurityFocus Vuln-Dev: RE: How to hide a file ?

>  
> > *I was wondering if there's a way to hide a file under windows 2000*  
> > *server, so that it will not be seen when using "show hidden file",*  
> > *"show all files" and so on. I want to hide a file but I want to be*  
> > *able to run the file only when I know exactly where it is*  
> > *and what is*  
> > *the file name.*  
>  
> *use the file streams. h carvey has written some nice documentation on*  
> *this:*  
> <http://patriot.net/~carvdawg/perl.html>  
> [http://www.chi-publishing.com/isb/backissues/ISB\\_2001/ISB0601/](http://www.chi-publishing.com/isb/backissues/ISB_2001/ISB0601/ISB0601HC.pdf)  
> [ISB0601HC.pdf](http://www.chi-publishing.com/isb/backissues/ISB_2001/ISB0601/ISB0601HC.pdf)  
>  
> *an additional discussion is available on:*  
> <http://rr.sans.org/win/ADS.php>  
>  
> *enjoy,*  
>  
>  
> \_\_\_\_\_  
> *jose nazario*  
> [jose@cwru.edu](mailto:jose@cwru.edu)  
> *PGP: 89 B0 81 DA 5B FD 7E 00 99 C3 B2 CD*  
> *48 A0 07 80*  
> *PGP key ID 0xFD37F4E5*  
> *(pgp.mit.edu)*  
>  
>  
>

- 
- **Previous message:** [H C: "Re: How to hide a file ?"](#)
  - **Maybe in reply to:** [Udi dahan: "How to hide a file ?"](#)
  - **Next in thread:** [Altheide, Cory: "RE: How to hide a file ?"](#)
  - **Messages sorted by:** [\[ date \] \[ thread \] \[ subject \] \[ author \] \[ attachment \]](#)