

## RE: How to hide a file ?

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/vuln-dev/2002-01/0126.html>

---

**From:** Vincent Tiu (AV-PH) ([Vincent\\_Tiu@support.trendmicro.com](mailto:Vincent_Tiu@support.trendmicro.com))

**Date:** 01/10/02

From: "Vincent Tiu (AV-PH)" <[Vincent\\_Tiu@support.trendmicro.com](mailto:Vincent_Tiu@support.trendmicro.com)>  
To: "'Young, Brandon'" <[Brandon.Young@Honeywell.com](mailto:Brandon.Young@Honeywell.com)>, 'H C' <[keydet89@yahoo.com](mailto:keydet89@yahoo.com)>  
Date: Thu, 10 Jan 2002 12:39:03 +0800

One way to transfer files with streams to another computer with NTFS is through the use of WinRAR. (haven't checked with other archivers, but definitely not a feature in WinZIP)

There's an option there to include the file streams within the archive so that it gets extracted with the streams intact.

Hope this helps.

Vincent Tiu  
Research & Development, AV Group  
TrendLabs, Philippines  
Trend Micro, Incorporated  
Web: <<http://www.antivirus.com/>>

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

From: Young, Brandon [mailto:[Brandon.Young@Honeywell.com](mailto:Brandon.Young@Honeywell.com)]  
Sent: Thursday, January 10, 2002 7:56 AM  
To: 'H C'  
Cc: '[vuln-dev@security-focus.com](mailto:vuln-dev@security-focus.com)'  
Subject: RE: How to hide a file ?

If I remember correctly from the earlier thread on this same topic you stated that this is only possible on NTFS and that if you were to move the ADS file to FAT that you would lose the files attached or something to that effect. The question I had was this. Would it be possible to take a file (test.txt) and bind multiple tools in ADS and the transfer the file via ftp on to another box, also is using NTFS, would the programs still accessible via the start command. I tested this with a Win2K box and NT4.0 and was unsuccessful. So were the results accurate? Is there no way to hide programs using ADS and transfer the file by normal means and still have them exist?

Brandon

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

From: H C [mailto:[keydet89@yahoo.com](mailto:keydet89@yahoo.com)]

Sent: Wednesday, January 09, 2002 9:51 AM

To: J. J. Horner

Cc: John Stauffacher; 'Matthew LaGrange'; [vuln-dev@security-focus.com](mailto:vuln-dev@security-focus.com)

Subject: Re: How to hide a file ?

- > *I know this may not be what we are really about,*
- > *being*
- > *more on the good side of the law than bad, but what*
- > *are the*
- > *potential uses for this?*

Well, I'm going to jump right in, knowing full well that this thread is going to end up generating a lot of theoretical, untested, undocumented stuff. My hope is that anything someone posts is done so in such a way as to be reproduceable, as it will help us all understand and therefore protect against the issue.

- > *I've seen discussions on how adses can be used to*
- > *hide a*
- > *large amount of data, making it unable to be viewed*
- > *using*
- > *the normal utilities while performing a DOS on the*
- > *server by*
- > *taking up all available space.*

Yes, a simple 'do...while(1)' that copies a file into successive ADSs will eventually fill up all of the usable space on the drive.

- > *I've seen discussions on how virus writers could use*
- > *an ads*
- > *to send a virus to a machine and make it hidden from*
- > *Antivirus*
- > *programs, then just execute it later. If*
- > *autoprotect is*
- > *enabled, preventing a lot of the malicious*
- > *activities, this*
- > *could have limited affects.*

Correct. The W2k.stream virus from Benny and Ratter of 29A didn't really 'use' ADSs, per se, in any malicious manner. And AutoProtect may work well enough for some A/V products to protect the system. But keep in mind that signature-based tools need to be

RE: How to hide a file ?

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

updated, so designing a new bit of malware, and using it in a truly stealthy manner, could work for quite a while. After all, isn't the reason that a lot of the current viruses and malware are detected so quickly is b/c they're so 'in your face' and 'noisy'?

- > *The barriers that I have seen:*
- >
- > *\* Running an ads is not as easy as typing the*
- > *pseudo-name.*
- > *\* An ads requires that the :realname.ext section be*
- > *part*
- > *of the filename. This makes them hard to hide and*
- > *hard*
- > *to transport with normal means: web, email,*
- > *napster, etc.*

Also keep in mind that:

(a) applications that only *\*read\** the file contents, such as graphics and multimedia viewers, don't usually execute any arbitrary data they find in, or associated with, the file.

(b) copying an ADS-laden file across a non-NTFS file system destroys the ADS.

So, at least for now, ADSs seem to be about as you put it...useful for file hiding and some limited executable storage. However, the issue really isn't the technology itself, but the human factor. Yes, we are discussing here, in a public forum, so maybe now more people will be aware of the issue. But not everyone who currently uses NT/2K, or who will be tomorrow, are aware of ADSs.

It's similar to the vulnerability issue. IIS's dir transversal exploit was patched in Nov '00, and sadmin/IIS (aka, poisonbox) was fairly wide ranging. So, the information was there and publicly available, but ignored. Code Red was similar...many folks, and even Microsoft to a degree, had been saying that 'best practices' includes removing/disabling unnecessary services or functionality. To me, script mappings in IIS constitute 'functionality', and if I don't have any pages ending in .ida or .idq on my web site, I'd disable the script mapping. Doing so would protect anyone from Code Red, w/o having to wait for an install a patch.

So, my point is...yeah some of us know about it. There are tools available to detect them. I've seen

RE: How to hide a file ?

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

screen captures of EnCase in which ADSs were used, and heard from forensics analysts who regularly look for ADSs. But does this mean that ADSs will never be used in an offensive manner? Not hardly. In fact, one would think that with more visibility, we're likely to see them more often in the future.

---

Do You Yahoo!?

Send FREE video emails in Yahoo! Mail!

<http://promo.yahoo.com/videomail/>

---

- **Previous message:** [Blue Boar: "Re: How to hide a file ?"](#)
- **Maybe in reply to:** [Udi dahan: "How to hide a file ?"](#)
- **Next in thread:** [Farahbakhshian, Mike \(OD\): "RE: How to hide a file ?"](#)
- **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)