

Re: Alternate Data Streams

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2003-11/3731.html

From: Sarge (*GiveMeTwenty_at_bootcamp.invalid*)

Date: 11/19/03

Date: 19 Nov 2003 22:04:29 GMT

"Daniel L. Belton" <abuse@spam.gov> wrote in
news:9DLub.30859\$oC5.733@clmboh1-nws5.columbus.rr.com:

> *Know of any Windows apps that put an ADS in your Windows\System32
> folder with .exe filenames?*

Can't say that I do. You might want to ask over at alt.comp.virus and/or
alt.comp.anti-virus, there are some pretty knowledgeable folks posting
in those groups. You mentioned that you're running Kaspersky resident.
Didn't that catch the trojan as it was being written to disk?

>> *Not that I know of. Other freeware tools you can use in addition to*

>> *Streams are Crucial ADS*

>> (<http://www.crucialsecurity.com/downloads.html>) and LADS

>> (http://www.heysoft.de/Frames/f_sw_la_en.htm).

>

> *I have those two, and they are good at finding and displaying the*

> *ADS... Just not good at removing them. I want a way to disable it since*

> *it's not needed and leaves a big security hole open.*

The easiest way I've found to delete ADS is with the shell extensions
available at:

http://www.giac.org/practical/GCWN/Ryan_Means_GCWN.zip

There's one that'll add a "Streams" property sheet from where you can
extract or delete an ADS, and another that'll add a "Streams Size"
column to Windows Explorer. Read the white paper first:

http://www.giac.org/practical/GCWN/Ryan_Means_GCWN.pdf