

Re: A2 found "traces"

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2007-04/msg00214.html

- *From:* "Jeff" <jeff@xxxxxxxx>
 - *Date:* Tue, 17 Apr 2007 09:25:34 -0400
-

"Poprivet" <poprivet@xxxxxxxxxxxxxxxxxxxx> wrote in message
<news:u4uT03pfHHA.4652@xxxxxxxxxxxxxxxxxxxxxxxx>

Jeff wrote:

Hi
Sometimes a little knowledge is dangerous!

For years I have used both Ad-Aware and Spybot (in addition to a firewall and ZA free. Recently I downloaded and installed "A2 Squared Anti-Malware" and it discovered on my wife's PC the following 2 items. I've checked their website but have to say I am still not sure whether to delete them or ignore them.

The 2 items are:

- 1) Trace.Directory.Spyware.MateWatcher (Trace: C:\Worksetup)
- 2) Trace.Registry.MyWay
(Trace: Value: HKLM\Software\Microsoft\Windows\CurrentVersion\App Management\ARP Cache\MyWay Speedbar Uninstall --> Changed)
(Trace: Value: HKLM\Software\Microsoft\Windows\CurrentVersion\App Management\ARP Cache\MyWay Speedbar Uninstall --> ShowInfoCache)

That indication is telling you that a change was made to your Registry.

Can I safely delete these or are they false alarms?

Concerning C:\Worksetup, the PC may have come with MS Works but that was removed years ago. She now uses MS Office.

Concerning MyWay Speedbar, I have no idea what that is and she certainly does not have it installed that she knows of.

Re: A2 found "traces"

That seems to be malware; see here:

[http://www.scumware.com/apps/scumware.php?action::view_article/article_id::1063294991/topic::Scumware.](http://www.scumware.com/apps/scumware.php?action::view_article/article_id::1063294991/topic::Scumware)

and here:

<http://help.myway.com/features/speedbar.html>

And:

<http://www.pchell.com/support/mywebsearch.shtml>

Aha! I AM familiar with some of the things in that last link! That infestation is hard to get rid of! It leaves chaff all over the system and a lot of them can recreate themselves.

So apparently at one time at least, the machine WAS infested with it, but whether it still is or not, I can't say. I think the top link I gave you would be the best way to check for its existance.

HOW you get such stuff is, you actually ask for it, without knowing it.

You find a neat little app that promises say, to make it easy to put a smiley anywhere you want to, in an email, a Word file, whatever, so you download it. But what they do NOT tell you is that, for the next several days/weeks and periodically, you will be continually downloading more and more pieces of spyware, a little bit at a time and usually quick enough so you won't notice the extra time the modem data lights are on. Now, since you actually did ask for the original program, they claim it's not spyware because you intentionally downloaded it. But what they didn't tell you was about all the spyware that came along with it.

This makes it worth a few minutes of effort to get rid of it or at least be sure it's not still there.

If it IS still installed, or parts of it, deleting won't get rid of it.

It'll just keep on recreating itself where it needs it.

Fortunately, it's not going to damage your data or drives if I've identified it correctly, but there is a lot of spyware activity going on.

I don't know about Spybot, but I –thought– Adaware had done a fix to catch that; maybe they removed it. Have you updated Adaware and Spybot? If not, do so and rerun the scans; this isn't new stuff although it might be a new incarnation.

GAIN, one of the companies involved in the spyware, sued a few people over it being detected as spyware and that scared some others into not listing it. You can see one of the stories about it here, which includes links to the versions I think you have toward the bottom:

<http://en.wikipedia.org/wiki/E-wallet>

and this one mentions some (not all inclusive) filenames you can check for to see if it's on your system:

<http://www3.ca.com/securityadvisor/pest/pest.aspx?id=453088629>

And this one claims to have a free scanner for it:

<http://www.pctools.com/mrc/infections/id/GAIN.Weatherscope/>

Feel free to come back with further questions: I've cleaned that crap off of two machines so far.

Re: A2 found "traces"

Re: A2 found "traces"

HTH
Pop`

PS The GAIN and Gator web sites both used to claim to have a "remover" for the software, but it didn't remove it; it simply put it to sleep so you didn't know it was there. Check their sites if you wish, but take anything they say with a grain of salt.

Appreciate any advice.

Jeff

I've never heard of any of those, so ... where they come from is beyond me.

You can probably delete them. But ...

Instead of deleting them, you could try renaming them by adding OLD say, to the end of their filenames or any change you can easily remember, then Restart and see what happens. If nothing goes wrong, they are probably OK to delete. If it does go wrong, put them back. They don't should like they would be anything to stop you from booting, but even if hthey did, you'd still be able to use Safe Mode to rename them back.

If you suspect these of being malware, deleting them isn't really the right way to get rid of htem as it may not remove the actual malware engine.

In addition, you should stay away from software you know nothing about; stick with names that are respected in the industry. A lot of "protection" software can be just the opposite.

Thank you for all the advice and information. Yes I do keep Ad-aware SE and Spybot updated and they say I am clean. I must have removed the malware engine long ago. but they left these traces of their having been there. I also allowed A2 to remove these "traces" and re-ran everything and it seems I am clean on all the utilities.

I must have been infected at one time in the past and these were traces of evidence of that, but they are now gone.

Thank you.

Jeff

.

Re: A2 found "traces"