

Re: Jan II: might be fixed! [WAS: Can't type in IE 6 or OE on Win XP Home PC}

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.inetexplorer.ie6.browser/2004-07/7878.htm>

From: Tony (*none_at_none.com*)

Date: 07/30/04

Date: Thu, 29 Jul 2004 21:38:00 -0400

Okay. Sorry it took so long to get back to you. I've been distracted by real work! As you do not want me to insert responses I will have to respond here point by point. In addition, I will top post to be consistent with your response methods.

Updates to both programs installed

Ad-aware reconfiguration confirmed

I have never kept a Windows configuration with files Hidden, so that is not an issue. In any event, both programs were run in Safe mode. Both found the same stuff I listed below (as when they were run in a regular instance).

I ran RAV and Panda. They both found old stuff in Zip files that were in a Deleted Items folder from an email account I haven't used since 2002. On an F: drive. Before jumping on that, I'll say that I don't open anything I get in an attachment unless I already know what it is (i.e., I'm expecting it).

Yes, that is the HijackThis thread. As indicated earlier, I don't operate my system with Hidden Files, so it was run in Show mode. It was not run in Safe Mode. I can do that.

I really don't remember which toolbar I had pop up in my Browser. All I remember is that I first deleted its entry from the Run key in the Registry, and then ran every correction tool I had. It went away.

I appreciate what you wrote about AV updating (I use McAfee). I run a fairly controlled computing environment at home. Only myself and my wife. My wife uses it only for email and browsing. I use it for that and work and digital imaging. Neither of us spends a whole lot of time looking for weird new stuff on the Web. Neither one of us even bother to look at mail if we don't know who it came from (even the ones from Microsoft Security from a few months ago :>). I also don't install random stuff for no reason. My system runs 24/7 on a cable modem behind a switch with NAT and SPI, and with XP Pro's firewall enabled. I also use another software firewall (Conseal PC

Firewall). With my AV updating weekly I have not had any attack on my system since the toolbar incident (which is not a virus, per se). If you go strictly by the definition of a virus I have no recollection of the last time my system was affected. And yes I have run any number of on-line firewall testers. My system comes up as Stealthy or Invisible.

I have listed my problem in the past in another thread. The reason why I jumped in on Steve's is that it seemed like there was some action in his thread that might help. Try this one

http://groups.google.com/groups?q=type+group:*ie6*+author:Tony&hl=en&lr=lang_en&ie=UTF-8&c2coff=1&selm

watch out for the overlap.

I will try your 2-4 steps listed below again (1 is already taken care of), and see what comes up.

"PA Bear" <PABear@mvps.org> wrote in message
news:ONrIGH7cEHA.1656@TK2MSFTNGP09.phx.gbl...

> *Please:*

>

> - *confirm that you've sought updates for Ad-aware and Spybot before
> using them each time;*

>

> - *confirm you are running Spybot v1.3;*

>

> - *confirm that you've reconfigured Ad-aware per*

> <http://aumha.org/forum/viewtopic.php?t=5877>;

>

> - *confirm that you've run both Ad-aware and Spybot in Safe Mode after
> first having enabled "Show Hidden Files";*

>

> - *confirm that you've updated virus definitions (manually, if
> necessary), enabled "Show Hidden Files" and ran a full system scan with
your*

> *AV app;*

>

> - *confirm that you've run at least two (2) of the free online scans*

> *found listed at <http://aumha.org/secure.php#freeav> (NB: one of them *must**
> *be Panda's!)*

>

> - *post the URL for the forum thread where you posted your HijackThis
log*

> *(and if they didn't have you enable "Show Hidden Files" and run HT in Safe*

> *Mode, do so and post back to the thread. (You may reference this IE6*

> *Browser thread and my post.)*

>

> *[Is this it?... <http://forums.spywareinfo.com/index.php?showtopic=8784>]*

>

>>> *Do you or did you have any ["free" toolbars] installed?*

>>>

> > *[At] one time yes.*
>
> *What was it?*
>
> > *Spybot found ...5 DSO Exploits*
>
> *Assuming your homepage and default Search choices are what you want them to*
> *be and are working properly, you may consider these DSO exploits a known and*
> *much-discussed bug. You may configure Spybot to ignore them in further*
> *scans.*
>
> > *...I have my full [AV scan] set to once per week*
>
> *That scenario is simply insufficient anymore, Tony. Configure your AV to*
> *seek definitions at least once a day (Some IT pros have chosen hourly!),*
> *at*
> *a time when the machine is booted up and connected to the 'net. Then*
> *configure it to run a full system scan about five minutes or so after*
> *seeking and installing updates, also daily.*
>
> > *In all the time I've been looking here (and other IE*
> > *newsgroups) I've only seen my exact problem posted three times*
>
> *Tony, I've read, re-read, reviewed and re-reviewed [Quiet, Jan! <wink>]*
> *all*
> *of your posts in the original thread (<http://snipurl.com/81fo>) and here.*
> *You have never stated "your exact problem" in either thread. You only*
> *made*
> *a "Me, too" reply to OP Steve's post. Please do not consider this an*
> *attack*
> *on you. The fact that you didn't clearly state *your* problem (and what*
> *you'd done so far to solve it) is what caused me to "lurk in the*
> *background"*
> *for the past month. I suspect others who may have been able to help also*
> *chose to ignore this thread (and the original) for the very same reason*
> *(though Jan's done an admirable job so far and kudos to her for jumping*
> *into*
> *the fray).*
>
> > *I would appreciate getting some insight as to why you are so sure it's*
> > *malware of some kind...*
>
> *The inability to type in IE text boxes (and in OE) was one of the very*
> *first*
> *"hijackings" we saw, dating back to December 2002 IIRC. It was caused*
> *(then) by a still-nasty, still around POS called Xupiter. There are so*
> *many*
> *new types of hijackware, new variants of known ones, and exploits used to*
> *install them, that we simply cannot keep up with them all (which is proolly*

> *the intent of the a**holes who're writing and foisting this stuff on mostly unsuspecting users).*

>

> *I respectfully suggest you (1) enable "Show Hidden Files" (and leave it that way), (2) update virus definitions and run a full system scan in Safe Mode,*

> *(3) update & run Ad-aware and Spybot (in that order and per all of the above) once again, then (4) update and run HijackThis again (in Safe Mode),*

> *saving your log.*

>

> *Then go to <http://forums.aumha.org> and Register. Sign in and post your new log to a new thread in <http://forum.aumha.org/viewforum.php?f=30>. Some of the best hijackware mavens are working there, including MVPs Mike Burgess (WinHelp2002 in <http://forums.spywareinfo.com/index.php?showtopic=8784>), Siljaline, and the inimitable TonyKlein. Again, you may reference this thread in your post.*

>

> *Please do *not* insert your replies inline, it's simply too confusing.*

>

> *Please do not change the subject of a thread; doing so disassociates your post and replies to it from the original thread.*

>

> *Please include all of the previous message in your replies.*

> --

> *HTH – Please Reply to This Thread*

>

> *~Robear Dyer (PA Bear)*

> *MS MVP–Windows (IE/OE), AH–VSOP*

>

> *AumHa Forums*

> *<http://forum.aumha.org>*

>

> *Protect Your PC*

> *<http://www.microsoft.com/security/protect>*

>

> *Tony wrote:*

> > *As there are many points here, I will respond with inserted comments...*

> >

> > *"PA Bear" <PABear@mvps.org> wrote in message*

> > *news:%23FPTwRucEHA.3476@tk2msftngp13.phx.gbl...*

> > > *Hi, Tony. I've been following this thread since it began earlier this month. Reinstalling IE won't make a bit of difference if malware is still present on your machine (and your problem is 99.9% certain to be malware-related, a recent CoolWebSearch variant, most likely).*

> > >

> > > *IE Tools>Internet Options>General>Accessibility> Is anything enabled here? Did you enable it?*

>>
>> *No and no.*
>>
>>> *IE Tools>Internet Options>Advanced>Browsing>Enable third party browser*
>>> *extentions (unchecked?)*
>>>
>> *Unchecked.*
>>
>>> *Do you or did you have any P2P file sharing apps installed? How about*
>>> *"free" toolbars?*
>>>
>> *No and at one time yes. Many months ago I had some add-on toolbar show*
up,
>> *but I got rid of it with the combination of tools listed here (I also*
>> *checked the Registry to make sure it was removed from the usual keys*
like
>> *Run and Run Once). Had not shown up since.*
>>
>>> *You piggy-backed onto a thread begun by another poster to which a*
>>> *talented MVP (Doug Varnau), familiar with hijackware, had responded.*
>>> *Did you see his post? You appear to have take only a few of his*
>>> *thorough and explicit suggestions.*
>>>
>> *While I only generically indicated what I did here, I did in fact follow*
>> *all of his suggestions.*
>>
>>>> *...I have been*
>>>> *through the entire mantra that the experts here suggest: AdAware,*
>>>> *Spybot, CWShredder, Virus Scan, Hijack This, etc. Not one thing was*
>>>> *found. I even did the mshtml.dll replacement. I was left twisting*
>>>> *in the wind. Apparently there's not a lot to suggest beyond the usual*
>>>> *things that seem to appear in this ng.*
>>>
>>> *Did you seek updates for CWShredder, Ad-aware and Spybot v1.3 before*
>>> *using them each & every time (even "right of the box" new), and run*
them
>>> *in that exact order? Have you updated and run them since 03 July-04?*
>>> *Have you enabled 'Show Hidden Files' before running them? Have you*
>>> *scanned with these tools in Safe Mode? Has Ad-aware been reconfigured*
>>> *for a full custom scan per <http://aumha.org/forum/viewtopic.php?t=5877?>*
>>>
>> *Yes.*
>>
>> *CWShredder just run. Came up completely clean.*
>>
>> *Adaware just run. 14 tracking cookies (all of which I recognize) and 5*
>> *redirected hosts file entries, which other sites indicate is sometimes*
>> *incorrectly identified by Adaware. BTW, I am using the hosts file from*
>> *<http://www.mvps.org/winhelp2002/>*
>>
>> *Spybot found the same tracking cookies as Adaware, and also 5 DSO*

> > *Exploits, of the form*
> >
> > *DSO Exploit: Data source object exploit (Registry change, fixed)*
> > *HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet*
> > *Settings\Zones\0\1004!=W=3*
> >
> > *As you can see from this example I fixed them.*
> >
> >> *Have you posted your HijackThis log to an appropriate forum for*
> >> *interpretation by the pros? HijackThis doesn't fix anything on its own*
> >> *and there's a fairly steep learning curve associated with knowing what*
> >> *the good and bad guys are. (If you have posted your log somewhere,*
> >> *please provide a link to the thread/forum.)*
> >>
> > *Yes. Nothing found.*
> >
> >> *Are your anti-virus application's definitions updated daily, followed*
by
> >> *a full system scan (also daily)? AFAIK, you haven't yet run a full*
> >> *system scan in Safe Mode (see*
> >> *<http://aumha.org/forum/viewtopic.php?t=5878>).*
> >
> > *Yes. Although I have my full scal set to once per week (hasn't found*
> > *anything in a long, long time).*
> >
> >> *Furthermore, you're missing several critical security updates at*
Windows
> >> *Update (though I wouldn't install updates until you get this malware*
> >> *problem sorted).*
> >>
> > *Yes, I know. I wanted to resolve this problem before doing this.*
> >
> > *I would appreciate getting some insight as to why you are so sure it's*
> > *malware of some kind. The posts on this NG which tend to be traced back*
to
> > *xxx-ware all seem to be things that many people are posting about (which*
> > *makes sense). In all the time I've been looking here (and other IE*
> > *newsgroups) I've only seen my exact problem posted three times... twice*
by
> > *me! Given that my indicated actions have made this problem go away (and*
> > *not come back even without any further CW / Ad / Spy etc efforts until I*
> > *just ran them again), why do you not conclude that in fact there may*
have
> > *been a combination of settings that may have been responsible for this?*
> > *(I'm not poking you with a stick, I'd like to know)*
>