

## Re: Malicious startup programs

**Source:** <http://www.derkeiler.com/Newsgroups/alt.computer.security/2005-01/0124.html>

---

**From:** Sasquatch (*none\_at\_thistime.com*)

**Date:** 01/05/05

Date: Wed, 05 Jan 2005 03:00:50 GMT

Do like Jim suggested. Kill the process and then get rid of the file Xej7.exe. Be forewarned though, that many of these nasties are set to auto download/repair themselves if you should remove their key files. Ensure you dump all temp files as well as checking the following keys in the registry:

Start-->Run-->Regedit

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\Run

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\RunOnce

Delete anything that may reference Xej7.exe

Download and use Spybot Search and Destroy \*\*\*AND\*\*\* Ad Aware. Both find things the other misses.

Once accomplished, stop using IE and start using Mozilla Firefox.

"tvfun" <tvfun@sbcglobal.net> wrote in message

news:PvlCd.4817\$092.777@newssvr31.news.prodigy.com...

> A malicious program keeps re-inserting itself in my start-up list.

>

> I've "Startup Control Panel 2.8 by Mike Lin" which conveniently displays

> startup items in a tabbed interface.

>

> The following is a real bugger.

>

> In HKLM/Run I have an item named '4GDY2MI296K6CX' with path

> C:\WINDOWS\SYSTEM\Xej7.exe

>

> If tried to uncheck it but doing that resulted in it creating a duplicate

> entry immediately with the other one checked! Trying to uncheck the other

> one resulted in an error message "There is already and enabled/disabled

> entry with the same name..." and a simple OK button. Hit OK and the second

> duplicated entry remains checked.

>

> I cannot delete Xej7.exe because it is "in use"

>

> I've had this problem repeatedly. Last time I finally rebooted in safe mode,

alt.computer.security: Re: Malicious startup programs

- > *made sure nothing extra was loaded and deleted Xej7.exe (actually a*
- > *precursor), removed all entries from startup and searched windows registry*
- > *for it and deleted anything that was connected to it.*
- >
- > *Within a day or so it returned. Not the same name but something like it. I*
- > *think it was named 'AOzdf.exe'. I could tell was the same thing because it*
- > *acted the same.*
- >
- > *It looks like something is lurking somewere on my system and it checks to*
- > *see if it's exe is there and in startup and if not creates it and adds it*
- > *to*
- > *the start up list. Question is how do I find it.*
- >
- > *In other words something created/wrote Xej7.exe and set it up to load at*
- > *startup. That something is lurking somewhere on my system. This exe gets*
- > *recreated even if I disconnect the wire to the internet.*
- >
- > *I have Spy Bot Search and Destroy and Add Aware and run them on a*
- > *schedule.*
- > *I have anti virus software. All of this has failed to get rid of the*
- > *problem I describe.*
- >
- > *The key is to find what is creating the 'Xej7.exe' and getting rid of*
- > *that.*
- >
- > *Any ideas on how to diagnose this.*
- >
- >