

Re: System32.exe XP? is this a virus

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2003-04/2927.html

From: Taj (*tajno1_at_yahoo.co.uk*)

Date: 04/25/03

Date: Fri, 25 Apr 2003 05:51:56 -0700

Ok Doug! Did all that you said – went to the norton website but decided to just use your cleaning tool (nice site!). ok then i turned off system restore and then put it back on.

now after all that – has that virus left my computer for good? no left over files?

another thing what damage does it do (antivirus sites are vague) and now that i used you cleaning tool – has all the damage been repaired?

>-----Original Message-----

>*This is not a Windows file. The command to run it is a left over remnant*

>*from a virus.*

>

><http://securityresponse.symantec.com/avcenter/venc/data/w32.kwbot.c.worm.html>

>

>*For automated removal of the remnants of this virus, see www.dougknox.com,*

>*Win XP Fixes, Clean KWBOT.Worm Registry Entries.*

>

>--

>*Doug Knox, MS-MVP Windows XP/ Windows Smart Display*

>*Win 95/98/Me/XP Tweaks and Fixes*

><http://www.dougknox.com>

>-----

>*Associate Expert*

>*ExpertZone –*

><http://www.microsoft.com/windowsxp/expertzone>

>-----

>*Please reply only to the newsgroup so all may benefit.*

>*Unsolicited e-mail is not answered.*

>

microsoft.public.windowsxp.security_admin: Re: System32.exe XP? is this a virus

>"Taj" <tajno1@yahoo.co.uk> wrote in message
>news:042a01c30ac6\$15dc0910\$a101280a@phx.gbl...
>> lol! thanks again Earl. What are the chances! lol
>>
>> okay so if i go to that reg clear place u said then the
>> message will sop popping up at startup?
>>
>> >-----Original Message-----
>> >
>> >"Taj" <tajno1@yahoo.co.uk> wrote in message
>> >news:033d01c30ac0\$3915e280\$a301280a@phx.gbl...
>> >> Previous post i wrote:
>> >>
>> >> "When starting the PC to the desktop screen a
message
>> box
>> >> titled "C:\WINDOWS\System32\system32.exe" appears
>> saying:
>> >>
>> >> "Windows cannot find 'C:\WINDOWS\System32
>> \system32.exe'.
>> >> Make sure you typed the name correctly, and then try
>> >> again. To search for a file, click the Strt button,
and
>> >> then click Search."
>> >>
>> >> I then have the option of clicking "OK". This occurs
>> >> everytime at start up now even though i don't
remember
>> >> making a search for that file and i don't reme,ber
>> >> deleting it at anypoint."
>> >>
>> >> Well a guy named Earl said this may be
>> >> a "W95.Smoker.Worm@mm" virus. I have some questions:
>> >>
>> >> 1)Reputable antivirus sites say this type of virus
uses
>> >> the system32.exe file to start itself. I have been
told
>> >> XP doesn't have a system32.exe file. Does this mean
i
>> >> have the virus or not since the key file for the
virus
>> to
>> >> work isnt on XP. I think this virus was meant for
>> >> previous windows that had the system32.exe file.
>> >>
>> >> 2)There are many similar but DIFFERNT viruses like
this
>> >> with different methods of removal involving the
>> Registry

Re: System32.exe XP? is this a virus

>> >> *Keys. Since im not even sure if i have the virus
>> should i
>> >> bother to follow the antivirus removal instructions.
>> >>
>> >> 3)If i should go through with removal– how do i
choose
>> >> which type of virus i have. since the virus has not
>> >> executed properly (no system32.exe file–hence the
>> reason
>> >> for the message at startup), i cannot tell what the
>> >> symptoms are . If i cant see the symptoms i cant
>> identify
>> >> what virus type i have, therefore i dont know how to
>> >> remove it. HOWEVER like i say, there seems to be no
>> >> symptoms other than this startup message box which
>> >> implies the virus hasnt actually executed yet , in
>> which
>> >> case....
>> >>
>> >> 4) is there a way to remove the message that i
recieve
>> at
>> >> startup
>> >>
>> >> PHEW ! thanks for reading this far! lets see whos
the
>> >> first to understand this one.....
>> >>
>> >> Taj
>> >
>> >The guy named Earl say that worms and virus often give
>> themselves
>> >names similar to authentic Windows files to discourage
>> people from
>> >deleting them or they place them in a different folder
>> from the
>> >authentic file with the same name. Some of the
favorite
>> names have
>> >"system" or "32" somewhere in the name. One worm is
>> called
>> >"Iexplorer.Exe" while the authentic file is
>> called "Iexplore.Exe."
>> >Many people would have deleted the authentic file and
>> kept the fake
>> >if they could.
>> >
>> >You can go to
>> <http://www.vtoy.fi/jv16/shtml/software.shtml> and
>> >download RegCleaner 4.3 which makes it easier to
remove*

microsoft.public.windowsxp.security_admin: Re: System32.exe XP? is this a virus

>> *lines in the*
>> >*Registry. It also backs up the delete in case you*
make
>> *a mistake.*
>> >
>> >--
>> >*Earl F. Parrish*
>> >
>> >.
>> >
>
>
>.
>