

Re: XP Home & hacktool

Source:

http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.help_and_support/2006-01/msg04979.htm

- *From:* "Tinman77865" <Tinman77865@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Sat, 28 Jan 2006 12:13:27 -0800
-

dont forget that if system restore is turned on that there is a copy of the virus in the restore point. yet another reason to rely on a good backup routine instead of the restore function.

"David H. Lipman" wrote:

> From: "Sandal" <Sandal@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
>
> | Today as I always do on a weekly basis I updated then ran Norton antivirus
> | and for the firsttime in a long time it said " Hack tool Virus" had been
> | found, it couldn't repair so gave me the option to quarantine it, which I've
> | done, but how do
> | I remove it or by quarantining have I done enough?
> |
> | When Norton found Hack Tool Virus it it was in C:\Documents and
> | Settings\Sandal\local settings\temporary internet
> | files\content.IE5\SDYRO1YJ\4[1].jpg, so I cleared my temporary internet
> | files, cookies and so on
> |
> | I also ran upto date Spybot. Adware, Microsoft-AntiSpy, it's found nothing.
> |
> | None of the above scans was done in safe mode, have I done enough, is the
> | infected file safe/removed or do I need to go further.
> |
>
> There are anti virus News Groups specifically for this type of discussion.
>
> microsoft.public.security.virus
> alt.comp.virus
> alt.comp.anti-virus
>
> Quarantining a file pulls the file out of the working OS and safely tucks the file away.
> The infector is rendered impotent while in quarantine. The objective is to determine if it
> is a False Positive declaration. If a file is falsely declared as an infector, it can be
> pulled out of quarantine and restored to its original location. If after time it is deemed
> the declaration was indeed correct, the quarantine can be dumped.
>
> MS anti spyware, SpyBot S&D and Ad-aware will not detect and handle a Symnatec detected

Re: XP Home & hacktool

- > Hacktool virus/Trojan. You would have to use another anti virus "On Demand" scanner for
- > verification. Either a locally installed one or an Online AV scanner.
- >
- > The following Multi AV Scanning Tool can be used in this role...
- >
- >
- > Download MULTI_AV.EXE from the URL ---
- > http://www.ik-cs.com/programs/virttools/Multi_AV.exe
- >
- > To use this utility, perform the following...
- > Execute; Multi_AV.exe { Note: You must use the default folder C:\AV-CLS }
- > Choose; Unzip
- > Choose; Close
- >
- > Execute; C:\AV-CLS\StartMenu.BAT
- > { or Double-click on 'Start Menu' in C:\AV-CLS }
- >
- > NOTE: You may have to disable your software FireWall or allow WGET.EXE to go through your
- > FireWall to allow it to download the needed AV vendor related files.
- >
- > C:\AV-CLS\StartMenu.BAT --- { or Double-click on 'Start Menu' in C:\AV-CLS }
- > This will bring up the initial menu of choices and should be executed in Normal Mode.
- > This way all the components can be downloaded from each AV vendor's web site.
- > The choices are; Sophos, Trend, McAfee, Kaspersky, Exit this menu and Reboot the PC.
- >
- > You can choose to go to each menu item and just download the needed files or you can
- > download the files and perform a scan in Normal Mode. Once you have downloaded the files
- > needed for each scanner you want to use, you should reboot the PC into Safe Mode [F8 key
- > during boot] and re-run the menu again and choose which scanner you want to run in Safe
- > Mode. It is suggested to run the scanners in both Safe Mode and Normal Mode.
- >
- > When the menu is displayed hitting 'H' or 'h' will bring up a more comprehensive PDF help
- > file. <http://www.ik-cs.com/multi-av.htm>
- >
- >
- > * * * Please report back your results * * *
- >
- > ---
- > Dave
- > <http://www.claymania.com/removal-trojan-adware.html>
- > <http://www.ik-cs.com/got-a-virus.htm>
- >
- >
- >
- .

• *Follow-Ups:*

◆ *Re: XP Home & hacktool*

◇ *From: David H. Lipman*

- **References:**

- ◆ **XP Home & hacktool**
 - ◇ From: Sandal
- ◆ **Re: XP Home & hacktool**
 - ◇ From: David H. Lipman

- Prev by Date: **I cannot delete cache which is building up**
- Next by Date: **Re: My speaker only plays through my mic port**
- Previous by thread: **Re: XP Home & hacktool**
- Next by thread: **Re: XP Home & hacktool**
- Index(es):
 - ◆ **Date**
 - ◆ **Thread**