

# Re: W32/Backdoor.KPI

---

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2006-05/msg00203.html>

---

- *From:* "antioch" <[r.antiochdunkthis@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:r.antiochdunkthis@xxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Fri, 26 May 2006 01:19:25 +0100
- 

"David H. Lipman" <[DLipman~nospam~@Verizon.Net](mailto:DLipman~nospam~@Verizon.Net)> wrote in message [news:O2ZqEZFGHA.3456@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:O2ZqEZFGHA.3456@xxxxxxxxxxxxxxxxxxxxxxxx)

From: "antioch" <[r.antiochdunkthis@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:r.antiochdunkthis@xxxxxxxxxxxxxxxxxxxxxxxx)>

| Hello All  
| Just did my daily Netguard virus scan supplied by my ISP and up popped  
| this  
| virus W32/Backdoor.KPI.  
| Netguard reported that it could not be disinfected but was deleted so  
| did  
| another scan as per advice – nothing found.  
| Went into their site to see what it was and there was no trace of any  
| info  
| about it.  
| I also got a window entitled 'Windows file protection' This said;  
| "Files that are required by windows to run properly have been replaced  
| by  
| unrecognised versions. To maintain system stability windows must  
| restore  
| the original versions of these files.  
| Insert your WIN XP Home SP2 CD now.  
| I have a screen-shot of this window and the netguard warning.  
| If I insert the disk, does anyone know what I can expect. Will it  
| require  
| re-install of WIN XP or will the process just pick out what is required.  
| I thought it better to ask for advice first.  
| As it happens I had done a CD backup of personal stuff only an hour  
| before.  
| Rgds  
| Antioch  
|

Is Netguard AV an OEM product by RadialPoint ?

It sounds like this replaced a OS file with its own (like WININET.DLL).

The message you got is like running System File Chgecker to replace the

Re: W32/Backdoor.KPI

removed file.

If your OS is WinXP SP2 (as evidenced by the request to insert a WinXP SP2 CDROM) then you need to point it to a CDROM of WinXP SP2 or point it to an i386 folder that has been slip-streamed to SP2 level.

One can easily slip-stream a WinXP SP1 or WinXP Gold i386 folder. You would copy the i386 folder tree from the CDROM to the root of "C:" (c:\i386) then change the attributes of the folder from Read-Only to Read-Write.

Then you would download the SP2 update in EXE format (~265MB file)

<http://www.microsoft.com/downloads/details.aspx?FamilyID=049c9dbe-3b8e-4f30-8245-9e368d3cdb5a&D>

You would then execute;

```
WindowsXP-KB835935-SP2-ENU.exe -u -s:c:\
```

To slip-stream the c:\i386 folder to SP2 level.

Then you would go to the Registry and the following location...

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup

and change...

"SourcePath" from D:\ (or other location) to; c:\

This will tell the OS where the i386 folder is to be found, in the root of "C:"

Then if you run the System File Checker (SFC.EXE) it will automatically find the files needed and you won't get a 'Windows file protection' and "Insert your WIN XP Home SP2 CD now" type message.

--

Dave

<http://www.claymania.com/removal-trojan-adware.html>

<http://www.ik-cs.com/got-a-virus.htm>

Hello David

Glad to see you answered.

Yes it is by Radialpoint. The AV is free with my BB subscription with NTL Cable services.

I do have my own certified/authenticated/WGA'd etc WIN XP Home SP2 OEM

Re: W32/Backdoor.KPI

Re: W32/Backdoor.KPI

CDROM.

Now I assume this will take ME a while to do, it is early hours in the morning here in the UK, would it be OK to leave until morning, or am I going to find I will be unable to start in the morning and cause more grief for myself.

I still have that window to click on when I insert the disk.

I will leave the Q's there for the moment if I may, before I go further.

Antioch

.