

Re: Suspicious Icons on Desktop

Source: <http://www.derkeiler.com/Newsgroups/alt.computer.security/2006-05/msg00000.html>

- *From:* "David H. Lipman" <DLipman~nospam~@Verizon.Net>
 - *Date:* Sun, 30 Apr 2006 22:25:45 GMT
-

From: "Sam" <samnewsgrp71@REMOVE THISsbglobal.net>

| A neighbor just called me concerning two Icons on the desktop of her
| computer. It is a Dell Dimension 8400 with windows XP Pro (SP2 and with the
| latest MS Security Updates). She also has Symantec Norton Internet
| Security, NAV 2006, and Adaware SE Plus installed.

| The two icons appeared yesterday on her computer and unfortunately she
| clicked on the first one and her computer registry was supposedly scanned
| and found some errors in her computer and recommended something to the
| effect of purchasing a registry program. I had her accomplish a properties
| on the first Icon named "Registry Cleaner" and read me the entry for the
| Target, and it was as follows:

| <http://ad.double-click.net/clk;26983459;5531471>. The second Icon named
| Registry Cleaner, had for properties, Target: C:/Program Files/Registry
| Cleaner Trial/Regclean.exe. I also had her run Adaware and it found 18
| tracking cookies and she put them in quarantine. Her NAV 2006 and Adaware
| definitions were up to date.

| At this point, I am reluctant to recommend the deletion of the Icons on the
| desktop and the removal of the Registry Cleaner Trial folder in windows
| explorer since I don't know what she has on her computer. I also ran a
| Google search but did not find any applicable information. Any suggestions
| would be very much appreciated, Sam.

If neighbor is using any version of Sun Java that is prior to JRE Version 5.0,
then you are strongly urged to remove any/all versions that are prior to JRE
Version 5.0. There are vulnerabilities in them and they are actively being exploited.
It is possible that is how you got infected with malware.

Therefore, it is highly suggested that if there are any prior versions of Sun Java
to Version 5 on the PC that they be removed and Sun Java JRE Version 5.0 Update 6
be installed ASAP.

Simple check, look under...
C:\Program Files\Java

Re: Suspicious Icons on Desktop

The only folder under that folder should be the latest version...

C:\Program Files\Java\jre1.5.0_06

<http://www.java.com/en/download/manual.jsp>

For non-viral malware...

Please download, install and update the following software...

* SpyBot Search and Destroy v1.4

<http://security.kolla.de/>

<http://www.safer-networking.org/microsoft.en.html>

* SuperAntiSpyware

<http://www.superantispyware.com/superantispywarefreevspro.html>

After the software is updated, I suggest scanning the system in Safe Mode.

I also suggest downloading, installing and updating BHODemon for any Browser Helper Objects that may be on the PC.

* BHODemon

<http://www.majorgeeks.com/downloadget.php?id=3550&file=11&evp=245a87539eea8ed6904332b4b8b8442d>

For viral malware...

* 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.

Re: Suspicious Icons on Desktop

Re: Suspicious Icons on Desktop

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>

Additional Instructions:

http://pcdid.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>

.