

Re: Attacked by Spyware and Adware

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2004-05/1050.html>

From: Steven L Umbach (*n9rou_at_nospam-comcast.net*)

Date: 05/19/04

Date: Wed, 19 May 2004 00:16:05 GMT

You should ONLY go to the Windows Update site <http://v4.windowsupdate.microsoft.com/en/default.asp> to download critical updates and never follow anything from a popup or email attachment. What happened to your computer – who knows without examining it with some utilities.

The best solution is to back up your data including you profile under documents and settings and then format your hard drive and do a clean installation that will involve installing a service pack again first and then all critical updates. You should not connect any computer to the internet for any reason including updates unless you have firewall protection first. After rebuilding your computer and installing a virus protection program with latest updates, you would want to scan your backed up data media before copying to your new installation.

If you want to try and salvage your current installation, you can visit one of the websites that will scan for viruses and try a free tool like Stinger from McAfee that will scan for many recent well known viruses. The links below may be helpful. ---
Steve

<http://www.microsoft.com/security/protect/>

<http://vil.nai.com/vil/stinger/>

<http://security.symantec.com/sscv6/default.asp?productid=symhome&langid=ie&venid=sym>

<http://securityadmin.info/faq.asp#virustoc> tips from the FAQ.

"Poor Guy" <anonymous@discussions.microsoft.com> wrote in message

news:86059279-5DB6-405F-865A-C7238635B745@microsoft.com...

> *I have started to encounter spyware and adware attacks since last weekend. During the course of the incidents, I managed to get the online virus support from Microsoft (I clicked on the toolbar). However, I believe the so-called online virus support was a fake one cos' I could never find the site afterward. The technician taught me the step as stipulated in the attachment of this message. After a few attempts the computer is still in the same situation. I tried to clear the things by spyware removers but again, it did not work. Here I have 3 questions:*

>

> *1. What did the hacker do to my computer?*

> *2. Should the attached instruction be a fake one? What had been done to my computer?*

> *3. How can I resolve the situation?*

>

> *Thks!!!*

>

>

> *Attachment:*

> *{Erik M.}Instructions for patching and cleaning vulnerable Windows 2000 and Windows XP systems.*

>

> *To prevent LSASS.EXE from shutting down the machine during the cleaning process on Windows 2000 and Windows XP:*

> *Please do not perform step one until directed to! If you do you will loose the chat agent!*

> *Unplug the network cable from the machine, or if the machine dials up to the Internet through a modem, do not establish a connection to the Internet yet (or if connected, disconnect).*

> *i. This step is important as it will prevent a local copy of the worm from targeting the local machine while performing the remaining steps and crashing the local copy of LSASS.EXE.*

>

>

> *This work around involves creating a read-only file named 'dcpromo.log' in the "%systemroot%\debug" directory and applies to both Windows 2000 and Windows XP. Creating this read-only file will prevent the vulnerability used by this worm from crashing the LSASS.EXE process on ALL operating systems by preventing the vulnerable code from being executed.*

> *NOTE: %systemroot% is the variable that contains the name of the Windows installation directory. For example if Windows was installed to the "c:\winnt" directory the following command will create a file called dcpromo.log in the c:\winnt\debug directory.*

>

> *The following commands must be typed in a command prompt (i.e. cmd.exe) exactly as they are written below.*

> *i. To start a command shell, click Start and then click run and type 'cmd.exe' and press enter.*

> *ii. Type the following command:*

> *echo dcpromo >%systemroot%\debug\dcpromo.log*

>

> *For this workaround to work properly you MUST make the file read-only by typing the following command:*

> *attrib +R %systemroot%\debug\dcpromo.log*

> *{poor guy}should I disconnect from the net when I perform the procedures*

> *{Erik M.}After creating the read-only dcpromo.log you can plug the network cable back in or dial out to the Internet and you must download and install the MS04-011 patch from the MS04-011 download link for the affected machines operating system before cleaning the system. If the system is cleaned before the patch is installed it is possible that the system could get re-infected prior to installing the patch.*

> *Here is the URL for the bulletin which contains the links to the download location for each patch: <http://www.microsoft.com/technet/security/bulletin/ms04-011.msp>*

> *If the machine is acting sluggish or the Internet connection is slow you should use Task Manager to kill the following processes and then try downloading the patch again:*

> *i. Kill any process ending with '_up.exe' (i.e. 12345_up.exe)*

- > ii. Kill any process starting with 'avserv' (i.e. avserve.exe, avserve2.exe)
- > iii. Kill any process starting with 'skynetave' (i.e. skynetave.exe)
- > iv. Kill hkey.exe
- > v. Kill msiwin84.exe
- > vi. Kill wmiprvsw.exe
- > 1. Note there is a legitimate system process called 'wmiprvse.exe' that does NOT need to be killed.
- > Allow the system to reboot after the patch is installed.
- >
- > Run the Sasser cleaner tool from the following URL:
- > For the on-line ActiveX control based version of the cleaner you can run it directly from the following URL:
<http://www.microsoft.com/security/incident/sasser.asp>
- > For the stand-alone download version of the cleaner you can download it from the following URL:
<http://www.microsoft.com/downloads/details.aspx?FamilyId=76C6DE7E-1B6B-4FC3-90D4-9FA42D14CC17&dis>
- > i. NOTE: If the machine is acting sluggish again or the Internet connection is slow, you should once again kill the processes outlined in step 3b above.
- > {Erik M.}Determine if the machine has been infected with a variant of the Agobot worm which can also get on the machine using the same method as the Sasser worm.
- > To do this run a full antivirus scan of your machine after ensuring your antivirus signatures are up to date.
- > If you DO NOT have an antivirus product installed you can visit HouseCall from TrendMicro to perform a free scan using the following URL:
<http://housecall.trendmicro.com/>
- >
- > Please visit the Protect Your PC web site for more information on how to stay secure: <http://www.microsoft.com/security/protect/default.asp>
- > {Erik M.}For the first couple steps, yes, you should disconnect.
- > {Poor guy}thks mite!! sorry to bother u again
- > {Erik M.}Not a problem, good luck.