

Re: Backdoor.Lateda.C

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2005-05/0372.html>

From: David H. Lipman (*DLipman~nospam~_at_Verizon.Net*)

Date: 05/26/05

Date: Thu, 26 May 2005 09:13:14 -0400

From: "shuckie69" <shuckie69@discussions.microsoft.com>

| Hi David

|

| Just wanted to let you know that I think I have resolved the problem. I
| managed to connect the PC to the internet via my router using a USB wireless
| adapter and ran a variety of anti-virus scans. AntiVir detected and deleted
| a couple of worms, and ZoneAlarm was stopping c:\windows\system32\winsci.exe
| from connecting to the internet. According to the log it tried to connect
| almost 1000 times in just a few minutes! I ran online scans at
| www.antivirus.com, www.symantec.com and www.mcafee.com. The last one
| detected a worm which was actually this winsci.exe file. I deleted the file
| and I'm no longer getting the connection message re. l33t.freeshellz.org.
| Apart from some minor spyware repeated scans haven't revealed any further
| worms/viruses/trojans (touchwood!).

|

| Many thanks for your help and advice, I will let you know if the problem
| re-occurs when I return the PC to my friends this evening.

|

* I strongly urge you to still perform the following based upon the information you provided. *

Dump the contents of the IE Temporary Internet Folder cache (TIF)

Start --> Settings --> Control Panel --> Internet Options --> Delete Files

Dump the contents of the Mozilla FireFox Cache { if you use FireFox }

Tools --> Options --> Privacy --> Cache --> Clear

Download CLEAN.EXE from the URL --

<http://www.ik-cs.com/programs/virttools/clean.exe>

It is a self-extracting ZIP file that contains the Kixtart Script Interpreter

{ <http://kixtart.org> Kixtart is CareWare } three batch files, two Kixtart scripts, two Link (.lnk) files and a PDF instruction file.

GETFILES.BAT -- For downloading (FTP) the files needed to run the McAfee Command Line Scanner. You may have to disable your FireWall or allow FTP.EXE to go through your FireWall

microsoft.public.security.virus: Re: Backdoor.Lateda.C

to allow the FTP utility to download the needed files

CLEAN.BAT -- For running within Windows after running c:\mcafee\GetFiles.BAT. If you choose

to scan again at a future date, run this batch file. It will automatically check the date of the McAfee DAT files and if it is a couple of days old, it will download (FTP) the latest signature files and install them before performing the scan.

DOSCLEAN.BAT -- For use on a Win9x/ME PC or on a Win2K/WinXP PC that is using FAT32 after you have booted from an Emergency Boot Disk or DOS disk and have already executed; c:\mcafee\GetFiles.BAT from within Windows. DOS disk boot images can be obtained from; <http://www.bootdisk.com/bootdisk.htm>

I need you to perform the following...

Execute; CLEAN.EXE
Choose; Unzip
Choose; Close

Execute; c:\mcafee\GetFiles.BAT
{ or Double-click on 'GetFiles Link' in c:\mcafee }

Reboot the PC into Safe Mode [F8 key during boot]

Shutdown as many applications as possible !

It would also help for you to read - "How to perform a clean boot in Windows XP"
<http://support.microsoft.com/kb/310353>

Execute; c:\mcafee\CLEAN.BAT
{ or Double-click on 'Clean Link' in c:\mcafee }

A final report in HTML format called C:\mcafee\ScanReport.HTML will be generated. At the end of the scan, it will be displayed in your browser (Opera, FireFox or Internet Explorer). It is suggested that you move the report out of c:\mcafee before performing another scan. It would be a good idea to scan in Safe Mode and in Normal Mode and save a copy of the HTML report for each session.

* * * Please report back your results * * *

--

Dave
<http://www.claymania.com/removal-trojan-adware.html>
<http://www.ik-cs.com/got-a-virus.htm>