

Re: RDRIV Virus

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2005-05/0056.html>

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

Date: 05/02/05

Date: Mon, 2 May 2005 13:48:08 -0400

From: "Michael Dudus" <MichaelDudus@discussions.microsoft.com>

| What I know about this virus:

|

| It's a denial of services virus that has done it's deed in my registry.

|

| It runs as a service

|

| It's picked up by trend and even when deleted, it's back after a reboot of my system.

|

| It's nasty.

|

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. If you are using Windows XP, you may have to disable the Windows XP FireWall 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...

microsoft.public.security.virus: Re: RDRIV Virus

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 }

I also suggest BHodemon: -- <http://www.definitivesolutions.com/bhodemon.htm>

--

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