Overview

W32/SirCam@MM is a virus that infects files of extension EXE, SCR, and OCX. (Note: This is McAfee’s name for it; your antiviral product may call it something else.) The SirCam virus enters your system as an e-mail attachment.

Once your machine is infected, the virus will infect all the executable files on your system and any network shares you have open. It will then scan your Windows address book and the contents of the Temporary Internet Files folder for e-mail addresses and send each of those addresses a randomly selected document from your hard disk and a copy of the virus. SirCam then scans the local network for machines with open Microsoft network shares, and infects those machines as well. Instructions for removal follow. For more information, see the McAfee Website at http://vil.nai.com/vil/virusSummary.asp?virus_k=99141.

There are a number of ways to remove SirCam. It’s easiest if you have Iowa State’s Micronet Scout installed, as you can use the SirCam remover in the Advanced area. The instructions for this method appear first in this handout. If you don’t have Scout installed but do have an Internet connection, go to section 2 “If You Don’t Have Scout, But Do Have an Internet Connection”. If you don’t have either, you need handout WVT 272 “Using the Emergency Disk”, which is available at the Solution Center, 195 Durham Center, or on the Web at http://www.ait.iastate.edu/pubs/wvt272/.

For instructions on how to get Scout, Iowa State’s utility for installing network software, you’ll need handout WNG 231 “Getting Network Software for Computers Running Windows”, which is available from the Solution Center, 195 Durham Center, or on the Web at http://www.ait.iastate.edu/pubs/wng231/.

1. If You Have Scout Installed

1. Close all open applications and windows.
2. From the Start Menu, click Programs, then Scout.
3. In the Scout window, click Configure.
4. In the Configuration window, click Advanced, OK, and then Done.
5. Back in the Scout window, click SirCam Remover.
6. In the new window, click Setup McAfee SirCam Remover.
7. A short message will appear in a dialog box. Read it and click OK.
8. When all of the files have been unpacked, a command prompt window will appear and your hard disk will be scanned for the SirCam virus.
9. When the scanner is finished, a window displaying the removal results will appear. After reading the report, click Continue.
10. Restart your machine.
11. From the Start Menu, click Programs, and then Scout.
12. In the Scout window, click Configure.
13. Click Current and then Done.

You should now have removed SirCam. If you have no virus protection on your machine, this is a good time to click the VirusScan (Antivirus) button in Scout and install McAfee VirusScan. You may remove the files in the C:\SCREMOVE folder; they are no longer needed.

2 If You Don’t Have Scout, But Do Have an Internet Connection

1. Start a command prompt. From the Start menu, click Run.
2. If you’re using Windows 95 or 98, enter COMMAND and press <Enter>. If you’re using Windows NT 4 or 2000, enter CMD and press <Enter>.
3. At the command prompt, type the commands:
   
   ```
   cd \\
   mkdir c:\scremove
   cd \scremove
   ftp ftp.sitelicensed.iastate.edu
   ```
4. The FTP server will ask for username and password. Enter your Iowa State Network-ID (the first part of your e-mail address) and password.
5. Type the following commands:
   
   ```
   cd scoutkit/win32
   binary
   get scrmove2.zip
   get unzip.exe
   ```
6. Disconnect from the FTP server. Type:
   
   ```
   bye
   ```
7. You’ll return to the Windows command prompt. Type:
   
   ```
   unzip scrmove2.zip
   remove
   ```
8. The last command starts a batch file, and several windows will open in sequence. The first windows will quickly open and close; the final window shows the results of scanning all the files on your hard disk; the scanning will take a long time.
9. When the scanner is finished, you’ll return to the command prompt. Close all windows and restart your machine.

Your computer should now be free of the SirCam virus. You may remove the files in the folder C:\SCREMOVE; they are no longer needed. If you have no virus protection on your machine, this would be a good time to install Micronet Scout and then use it to install McAfee VirusScan.