Software Engineering Institute
Carnegie Mellon University

W32/Blaster Recovery Tips

Accompanying CERT Advisory CA-2003-20

CERT Division

http://www.sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

This report was prepared for the

SEI Administrative Agent
AFLCMC/AZS
5 Eglin Street
Hanscom AFB, MA 01731-2100

DM17-0052

Table of Contents

1 Steps to recover from W32/Blaster

These instructions are designed for Windows XP. Under some circumstances, these instructions may not completely disable the worm or protect the system from re-infection. See Notes.

1. Physically disconnect the computer from the network (remove phone/network cable, wireless card).
2. Kill the worm process using Task Manager. Known variants of this worm may show up as "msblast.exe", "teekids.exe", or "penis32.exe".
   a. Press Ctrl-Alt-Delete key combination.
   b. Click "Task Manager" button.
   c. Select "Processes" tab.
   d. Highlight "msblast.exe".
   e. Click "End Process" button, answer "Yes" to warning dialog.
   f. Repeat previous two steps for "teekids.exe" and "penis32.exe".
3. Delete any files named "msblast.exe", "teekids.exe", or "penis32.exe" on the computer.
   a. Click "Start", "Search", and select "All files and folders".
   b. Search for "msblast.exe".
   c. Right-click each file and delete it.
   d. Repeat previous two steps for "teekids.exe" and "penis32.exe".
4. Enable Internet Connection Firewall (ICF).
   From Microsoft Knowledge Base Article 283673:
   a. In Control Panel, double-click Networking and Internet Connections, and then click Network Connections.
   b. Right-click the connection on which you would like to enable ICF, and then click Properties.
   c. On the Advanced tab, click the box to select the option to Protect my computer or network.
   d. If you want to enable the use of some applications and services through the firewall, you need to enable them by clicking the Settings button, and then selecting the programs, protocols, and services to be enabled for the ICF configuration.
5. (Optional) Disable DCOM.
   From MS03-026:
   a. Run Dcomcnfg.exe.
      If you are running Windows XP or Windows Server 2003 perform these additional steps:
      - Click on the Component Services node under Console Root.
      - Open the Computers sub-folder.

- For the local computer, right click on My Computer and choose Properties.
- For a remote computer, right click on the Computers folder and choose New then Computer. Enter the computer name. Right click on that computer name and choose Properties.

b. Choose the Default Properties tab.

c. Select (or clear) the Enable Distributed COM on this Computer check box.

d. If you will be setting more properties for the machine, click the Apply button to enable (or disable) DCOM. Otherwise, click OK to apply the changes and exit Dcomcnfg.exe.

6. Reboot your computer and reconnect to the network.
7. Install the patch from Windows Update or MS03-026.
   a. Using Internet Explorer, go to Windows Update and follow the instructions there to install any available patches.
   b. After installing the patch, reboot your computer.
8. Read and apply the clean up measures outlined in MS03-026.
   a. If you disabled DCOM in step 5, you will probably want to re-enable it.

2 Notes

- It is possible to stop the shutdown process by typing the following at a command prompt:
  ```
  shutdown -a
  ```
- If you are unable to run the Task Manager (step 2) or the Search function (step 3), type the following at a command prompt:
  ```
  taskkill.exe /im msblast.exe
  del %windir%\system32\msblast.exe
  ```
  Replace "msblast.exe" with other process/file names as necessary.
- You may not find the processes (step 2) and files (step 3) listed above, in which case your computer is not infected. If you are connected to the network, your computer may still be re-booting due to scan/attack traffic. If you do not find the processes and files, continue with step 4.
- The worm may exist as processes and files with names other than "msblast.exe", "teekids.exe", or "penis32.exe.".
- It may be necessary to disable System Restore in order to successfully delete worm files.
- Save yourself the trouble next time by blocking 135, 137, 138, 139, and 445 tcp and udp inbound and outbound. This will block most MS networking traffic. Leaving ICF enabled will stop unsolicited inbound network traffic. Unless it breaks something, leave ICF enabled.
- Another type of host-based or network firewall can be used to block 135/tcp.
- Use anti-virus software and maintain updated signatures. Many anti-virus vendors have developed removal tools for this worm.
- The worm is started by a registry key in HKLM\Software\Microsoft\Windows\CurrentVersion\Run. The key is typically named "windows auto update" or "Microsoft Inet xp.." and has a value of "msblast.exe", "teekids.exe", or "penis32.exe". If you are comfortable editing the registry, delete this key.
- Disabling DCOM may break things and may be unnecessary (assuming that the worm is completely disabled and ICF is enabled).
- It has been reported that AOL network connections do not display an option to use ICF.

3 More Information

- CERT Advisory CA-2003-20 <http://www.cert.org/advisories/CA-2003-20.html>
- Home Computer Security Guide <http://www.cert.org/homeusers/HomeComputerSecurity/>
- Anti-Virus Vendors <http://www.cert.org/other_sources/viruses.html#VI>
- Trend Micro WORM_MSBLAST.GEN < http://www.trendmicro.com/vinfo/virusency-clo/default5.asp?VName=WORM_MSBLAST.GEN>