Steps for Welchia Worm Cure on Workstations
August 25, 2003
GV/WFL BOCES-EduTech

The following 5 steps have been designated by GV/WFL BOCES-EduTech for the effective removal of the Welchia virus and the securing of workstations from re-infection. It is important that they be performed in the order presented.

These steps also include a full scan for known viruses that may also be present.

Step 1. Install MicroSoft Windows Critical Updates for the appropriate Operating System.

Go to the Microsoft update website by clicking on Start and selecting MicroSoft Updates or click here.
http://v4.windowsupdate.microsoft.com/en/default.asp

Select - Scan for updates

Install Critical Updates by following the provided instructions.

Step 2. Update Virus Signatures on installed virus protection applications.

For InnoculateIT, click on the Realtime monitor icon in the tool bar at the lower left section of the screen.

The system will download the most recent virus signatures for the InnoculateIT engine.

When complete, you may close the window.

Step 3. Download and run the Stinger Anti-Virus software from McAfee.

See the complete instructions from Network Associates for downloading and running this fix at the following web site.

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

Follow the directions provided to remove a number of specific viruses including the Welchia worm. Be sure to read the special instructions provided for WindowsME/XP operating systems to disable the System Restore settings. These are located in a READ THIS FIRST link on step 3 of the Stinger instructions.

Step 4. Perform a full virus scan with the InnoculateIT software updated in Step 2.

Go to Start-Programs-“eTrust InnoculateIT”- “eTrust InnoculateIT”.

Be sure the Local Disk (C:) is checked.

Click on the green (Start Scan) triangle button.

The full scan will can take a while depending on how many files are on the drive.

Viruses found will be cured, renamed with an AVB extension, quarantined, or otherwise deleted. If a virus is identified that cannot be dealt with, contact the Help Desk for further assistance.

Step 5. Search for and delete files with .AVB extensions

Any viruses that have been isolated by renaming will have a file extension of .AVB. These files should be deleted.

Go to Start-Search-For Files or Folders...

Select “All Files or Folders”

Enter .AVB in the “All or part of the file name:” area and press enter.

If any .AVB files are identified, highlight them and delete them permanently by holding down the shift key while right clicking and selecting delete.