# ITS Technical Notes

## Windows Enterprise Announcement

**December 15, 2008 – AutoRun Viruses Present on ISU Campus**

An autorun virus has been a problem in at least three areas of the ISU campus. An autorun virus is present in the files used to automatically run an application (such as a software installer, selection menu, etc.) when a CD-ROM, USB key or drive, or other mountable file system is mounted on a computer. When the virus automatically runs, it infects the system and spreads by copying itself to other mountable devices it finds (including network drives) that it can write to). Autorun virus infections spread by mountable network drives and USB keys have been active at ISU recently. Apparently the military had gone so far as to block the usage of all USB mountable devices but has backed away from that more stringent policy.

Two important steps are needed to halt the spread of autorun viruses. First, a good antivirus package with up to date virus definition files is always mandatory. Second, OU admins are strongly advised to disable the autorun feature on ALL mounted drives for systems they manage. A good article from Microsoft on how to do this via group policy is here: http://support.microsoft.com/kb/953252 .

This topic was discussed at the last WinAdmin meeting (Dec 12, 2008). See the meeting notes at: http://tech.ait.iastate.edu/win2000/admin/WinAdmin.2008.12.12.pdf