

How to stop a Conficker infection

1. PATCH – Verify the MS08-067 patch was applied. Make sure to patch images, too. An unpatched image is still vulnerable and will often be forgotten. However, patching this one vulnerability is only one of the ways Conficker spreads. It is possible to be fully patched and still get this infection on your systems.
2. If possible, use Group Policy settings to stop Conficker from spreading. Microsoft has a great document at <http://support.microsoft.com/kb/962007> that describes exactly how to do this.
3. Turn off AutoRun functionality for removable media. <http://support.microsoft.com/kb/962007> is the best and most comprehensive page describing how to do this. This feature had a bug and Microsoft released a patch in late August, 2009 <http://www.microsoft.com/technet/security/advisory/967940.mspx> that must be applied to correctly disable AutoRun functionality. (KB 953252 and 967715 also discuss the patch. Applying any of these 3 enable correct functionality). <http://support.microsoft.com/kb/962007> is the page that describes exactly what needs to be done. As a caution, while turning off AutoRun does NOT break any application, it does require the user to browse the file system of the media to find any executables. The newer patches give you the option of turning off for all removable media, including CD drives.

As an added precaution, proactively create an autorun.inf FOLDER on any thumb drive you find. We used to recommend creating a file and mark the file as read-only, but we have found at least one variant that can overwrite this file. This may be able to keep drives from being reinfected.

4. Update and VERIFY that your Anti-Virus (AV) application is operating. Do NOT trust the Windows Security Center to alert you that your AV application is not functioning. Some infections have been known to spoof the operation of the AV to Windows Security Center. Make sure that your AV software scans and disinfects removable media. Skipping this step will result in reinfection of your systems. Conficker has been out long enough any reputable AV software should detect and clean it. If your AV is not detecting the infection, download the Microsoft Malicious Software Removal Tool (MSRT) from <http://www.microsoft.com/security/malwareremove/default.mspx>.

Make sure your AV is actively scanning AND disinfecting removable media. We have seen organizations get all of their systems cleaned up and one student/faculty/staff member brings in an infected thumb drive and the dance starts all over again. It is also imperative that your patrons understand they must protect/disinfect home systems. Thumb drives are excellent SneakerNet devices to bring infections like this back and forth from home to work.

5. Use unique, secure passwords on administrative accounts (especially the local administrator account). DO NOT LOGIN TO A SUSPECTED CONFICKER INFECTED MACHINE WITH A DOMAIN ADMINISTRATOR ACCOUNT. Conficker can also spread from computer to computer if the same administrative password is used on all systems or if a user is a domain admin and has access to all workstations. Conficker impersonates the current, logged-on account to access other domain systems and infections spread like wildfire.
6. Turn off the Server Service (at least temporarily). This is a DRASTIC measure and WILL break functionality, especially on servers. However, for many sites, this is the only way to stop the infection from spreading, especially if someone has logged into an infected system as a Domain Administrator. <http://support.microsoft.com/kb/962007#Manualsteps> gives detailed steps of how to do this.