Protecting yourself from Conficker

The Conficker worm (also known as Downup, Downadup and Kido) is probably the most prevalent computer worm on Janet and the Internet at this time. It's success can be attributed to it's use of a number of different vectors it uses to infect machines:

- Exploiting a vulnerability in Microsoft Windows to gain remote access
- Guessing user's login passwords
- Using the auto-run functionality in Microsoft Windows to trick the user into executing it

The worm then disables anti-virus software on the infected system, and attempts to download further instructions from a large number of domains. It is not known what the intended payload is, as the operator of the botnet has not yet attempted to send it any commands. The identity of the person or group operating the Conficker worm is also a mystery.

The worm is currently inactive and current threat from infection is minimal, but we believe that the huge number of infected hosts poses a potentially critical thread, and immediate action is required. If infected systems are ever activated, perhaps sending spam or participating in a denial of service attack, the impact on your network could cause massive problems.

- Tracing Conficker Reports [1]
- Detecting Conficker Infections [2]

Five Steps to protecting yourself from Conficker

1. Install the update for Microsoft Security Bulletin MS08-067
2. Block Windows LAN service ports when unnecessary
3. Enforce a strong password policy
4. Disable auto-run
5. Install correctly configured anti-virus software

Microsoft Security Bulletin MS08-067

All systems must be protected against the vulnerability outlined in this Microsoft Security Bulletin [3]. This was the initial way the worm spread. Centrally managed systems should have had the relevant patches and updates applied through your usual patch management procedures. You should issue instructions for staff and students to update their personal systems.

The system also needs to be reachable on port 445/tcp to be infected by this route. This is one of the ports used to support Windows LAN services such as NetBIOS [4]. The ports used by Windows LAN services must be blocked inbound and outbound at your network border. If you do need to access these ports over the Internet, exceptions can be made for particular

hosts. You may also need to consider blocking these ports at at internal divisions on your own network. Does a public wifi network need to be able to use this ports? Also remember that many desktop firewalls block access to these ports, but still allow access from systems on the local network.

Do not rely on patching or firewalling to provide complete protection. Installation of the update can fail, and firewalls provide no protection against infected across a local network. Also, neither method provides protection against other means of infection, so it cannot be the only step you take.

Dictionary attack against user accounts

Windows allows remote machines to list valid user names, a useful feature in some environments. The worm finds user accounts, and then attempts a simple dictionary attack against the passwords for this account. If successful, the worm can install itself.

The attack uses a simple and very small dictionary of common passwords but is surprisingly successful. You must enforce a strong password policy for your Windows domains [5], even a simple one is better than nothing. You should issue instructions for staff and students to make sure they chose secure passwords for their personal systems.

Auto-run, and tricking users into running the worm

Once a system is infected, the worm copies itself onto any available USB drives. When the drive is placed in a clean and unprotected system, the system will attempt to auto-run the worm, infecting itself. The worm also uses some clever tricks to try and convince the user to run the worm themselves.

Protect yourself against this method of infection by disabling auto-run [6], and ensuring your anti-virus software performs on-access scanning of USB media. Make sure that you correctly understand the operation of your anti-virus software and that if on-access scanning of USB drives is enabled. Often anti-virus installed, but incorrectly configured. It is unlikely that scheduled scans will provide much protection.

Links
[1] http://community.ja.net/library/janet-services-documentation/tracing-conficker-activity
[2] http://community.ja.net/library/janet-services-documentation/detecting-conficker-infections
[3] http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx
[4] http://community.ja.net/library/janet-services-documentation/blocking-lan-service-ports
[5] http://technet.microsoft.com/en-us/library/cc736605(WS.10).aspx
[6] http://www.us-cert.gov/cas/techalerts/TA09-020A.html