

Atomic Computer Solutions, LLC
111 Allison Lane
Vernon, Vermont 05354

ADMINISTRATIVE OFFICES
TEL: (802) 254-6120

Virus Alert

January 23, 2009

The Conficker Worm

Target: All users of Windows XP and Windows Vista.

A new worm called Conficker, sometimes referred to as **Downadup**, has generated a lot of interest. Current users of Symantec's Norton security products or McAfee security products are protected. Users who lack protection should purchase a copy of either Norton Security or McAfee Security. Both products will detect and remove this worm. If you already own one of these products, you should update your products virus library immediately.

What does the Conficker worm do?

The Conficker worm mostly spreads across networks. If it finds a vulnerable computer, it turns off the automatic backup service, deletes previous restore points, disables some security services, blocks access to a number of security web sites and opens infected machines to receive additional programs from the malware's creator. The worm then tries to spread itself to other computers on the same network.

How does the worm infect a computer?

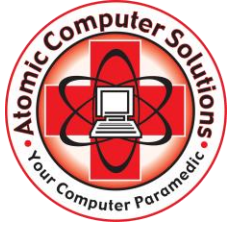
The worm tries to take advantage of a problem with Windows (a vulnerability) called MS08-067 to quietly install itself. Users who automatically receive updates from Microsoft are already protected from this. The worm also tries to spread by copying itself into shared folders on networks and by infecting USB devices such as memory sticks.

Who is at risk?

Users who's computers are not configured to receive patches and updates from Microsoft and who are not running an up to date antivirus product.

What to do if you are infected

1. Disable System Restore (Windows Me/XP).
2. Update the virus definitions.
3. Run a full system scan.
4. Delete any values added to the registry.



Atomic Computer Solutions, LLC

111 Allison Lane
Vernon, Vermont 05354

ADMINISTRATIVE OFFICES

TEL: (802) 254-6120

Advice to Stay Safe from the Conficker Worm:

1. Run a good security suite.
2. Keep your computer updated with the latest patches. If you don't know how to do this, have someone help you set your system to update itself.
3. Don't use "free" security scans that pop up on many web sites. All too often these are fake, using scare tactics to try to get you to purchase their "full" service. In many cases these are actually infecting you while they run.
4. Turn off the "autorun" feature that will automatically run programs found on memory sticks and other USB devices.
5. Be smart with your passwords. This includes
 1. Change your passwords periodically
 2. Use complex passwords – no simple names or words, use special characters and numbers
 3. Using a separate, longer password for each site that has sensitive personal information or access to your bank accounts or credit cards.
 4. Use a passwords management system such as Identity Safe to track your passwords and to fill out forms automatically.
 5. Run a trustworthy security system such as McAfee Security, Norton Internet Security, Norton Antivirus or Norton 360.

FAQ

Q: Am I safe if I don't go to questionable web sites?

A: No. The Conficker worm seeks out computers on the same network. You can be in a coffee shop, an airport or in the office and the worm will quietly try to attach to your computer and run itself.

Q: How do I know if I am infected?

A: The best way to know if you are infected is to run a good antivirus product. Symptoms that may indicate you are infected include your being blocked from accessing the web sites of most security companies,

Q: Can't I just run free antivirus software?

A: Yes, but they're not thorough or comprehensive. While some of the legitimate free antivirus products aren't bad at detecting viruses in files, they only provide basic protection, in general they are weak at detecting modern threats such as drive-by-downloads, malicious web sites and intrusion attempts. Worse, the internet is overflowing with fake free security scanners that



Atomic Computer Solutions, LLC
111 Allison Lane
Vernon, Vermont 05354

ADMINISTRATIVE OFFICES
TEL: (802) 254-6120

actually infect your computer. Fake scanners such as “Antivirus 2008” or “Antivirus 2009” are difficult to identify and have plagued hundreds of thousands of users around the world.