

Beware Conficker worm come April 1
Tue Mar 24, 2009 6:21PM EDT

In an event that hits the computer world only once every few years, security experts are racing against time to mitigate the impact of a bit of malware which is set to wreak havoc on a hard-coded date. As is often the case, that date is [April 1](#).

Malware creators love to target April Fool's Day with their wares, and the latest worm, called Conficker C, could be one of the most damaging attacks we've seen in years.

Conficker first bubbled up in late 2008 and began [making headlines in January](#) as known infections topped 9 million computers. Now in its third variant, Conficker C, the worm has grown incredibly complicated, powerful, and virulent... though no one is quite sure exactly what it will do when D-Day arrives.

Thanks in part to a [quarter-million-dollar bounty](#) on the head of the writer of the worm, offered by Microsoft, security researchers are aggressively digging into the worm's code as they attempt to engineer a cure or find the writer before the deadline. What's known so far is that on April 1, all infected computers will come under the control of a master machine located somewhere across the web, at which point anything's possible. Will the zombie machines become denial of service attack pawns, steal personal information, wipe hard drives, or simply manifest more traditional malware pop-ups and extortion-like come-ons designed to sell you phony security software? No one knows.

Conficker is clever in the way it hides its tracks because it uses an enormous number of URLs to communicate with HQ. The first version of Conficker used just 250 addresses each day -- which security researchers and ICANN simply bought and/or disabled -- but Conficker C will up the ante to 50,000 addresses a day when it goes active, a number which simply can't be tracked and disabled by hand.

At this point, you should be extra vigilant about protecting your PC: Patch Windows completely through Windows Update and update your anti-malware software as well. Make sure your antivirus software is actually running too, as Conficker may have disabled it.

Microsoft also offers a [free online safety scan](#) here, which should be able to detect all Conficker versions.

=====

Our friends at Hard Drive Computers offer the following advice regarding this computer virus.

1. Virus Protection Software

Make sure that your program is up to date and keep it current.

2. Computer scan

Follow your virus computers program to initiate a complete virus scan of your computer.

3. Control Panel / Firewall

Click on the start button of your computer, then click the button titled CONTROL PANEL. When the panel has opened look for the button titled: Firewall. Click on this button and insure that your fire wall is ON.

4. Microsoft Download.

Being that it appears that Microsoft has taken this threat very seriously, as a matter of fact they have placed a bounty of \$250,000.00 for information leading to the creator(s) of the virus program known as Conficker. They have also made available on their web site a download to reduce the potential damage to computers using their software.

Be aware that if you download using high speed internet (or DSL) that it will take approximately one hour to complete. Of course if you are using dial up services it will be considerably longer. This Microsoft download site can be reached at the following link:

<http://www.update.microsoft.com/windowsupdate/v6/default.aspx?ln=en-us>

So plan on at least an hour (DSL) or possibly overnight (Dial up internet service) for the Microsoft download and update to finish.

5. Email Scanner

Make sure that this feature is enabled on your virus program.