Don't fret about Conficker: Here's what to do

March 31 2009, By JORDAN ROBERTSON , AP Technology Writer

(AP) -- The Conficker worm, a nasty computer infection that has poisoned millions of PCs, will start ramping up its efforts Wednesday to use those machines for cybercrimes. It's unclear whether everyday PC users will even notice, but this is as good an excuse as any to make sure your computer is clean.

There are some easy ways to figure out whether a computer has the Conficker worm, and free tools available for getting rid of it.

One scary thing about Conficker is that it spreads without human involvement, moving from PC to PC by exploiting a security hole in Microsoft Corp.'s Windows operating system. The hole was fixed in October, but if your computer doesn't get automatic updates from Microsoft, you could be vulnerable.

Lots of computer worms disable antivirus software outright, which can be a tip-off that something is wrong. But Conficker doesn't do that. Instead, Conficker blocks infected PCs from accessing the antivirus vendors' and Microsoft's Web sites, so victims won't get automatic updates and can't download the Conficker removal tools that those companies have developed.

So see what Web sites you can visit. If you can navigate the Internet freely except for sites owned by Microsoft or antivirus vendors such as Symantec Corp., McAfee Inc. or F-Secure Corp., your PC might have Conficker or a similar bug.

Fixing the problem gets a little trickier.

The best remedy is to have a friend - whose computer is not infected - download a removal tool from Microsoft or one of the antivirus vendors. Then that person should e-mail the tool to you.

A list of the free Conficker removal programs is available on the Web site of the Conficker Working Group, an alliance of companies fighting the worm. The removal programs will take care of themselves, for the most part, scanning your system and purging the worm.

One thing to note: Conficker blocks infected machines from running removal tools with "Conficker" in the name. So users might have to change the name of the file (one you've saved the tool to your desktop, right-click on it and select "rename") before running it. The program's instructions will let you know if you need to do this. Many antivirus vendors have already changed the names in their removal tools - in some cases calling the file a misspelled variant of "Conficker" - to trick the worm into letting the program run.

Businesses have a bigger challenge, because Conficker has yet another method for evading detection. Once the worm is inside a machine, it applies its own version of the Microsoft patch that fixes the vulnerability Conficker exploited in the first place. So a business running a standard network scan, looking for unpatched machines, might come up empty-handed, even though some computers on the network are infected.

The scans need to take a deeper dive into the machines on the network - something an antivirus vendor's service should enable. For government agencies, contractors and operators of critical infrastructure, the Department of Homeland Security also has released a network-detection tool for Conficker.

On the Net:

List of Conficker removal programs:

http://www.confickerworkinggroup.org/wiki/pmwiki.php?nANY.RepairTools

Homeland Security's announcement of its detection tool:

http://tinyurl.com/c3petb