Bits and Bytes

Arkansas' Premier Computer Club

April 2009
Don Hood, President

Bella Vista Computer Club - John Ruehle Center
Highlands Crossing Center, 1801 Forest Hills Blvd, Suite 120 Bella Vista, AR 72715-3016
Web site: www.bvcompclub.org
E-mail: jrc@bvcc.arcoxmail.com

With all the talk about the Conficker Worm it should have prompted some questions. Is my computer infected? How can I tell if my computer is infected or clean? What free programs can I use to check my computer? What free programs can I use to clean my computer if it is infected? Just because nothing happened on April 1 doesn't mean we're out of the woods. The folks that were smart enough to develop this program are also smart enough to realize that everyone was gunning for them on April 1. If anything is to become of this issue it will be five or six months from now when everything has quieted down. If you Google Conficker, you'll have access to over nine million articles on the issue. Since no one has time to read this many articles, how do you decide which ones to you should consider? One of the nice features of Google is that they present what they think are the most relevant articles in the first page. Most people that Google a topic don't look at more than the first five pages of results. That's going to narrow the search to about fifty articles. Next, look for articles from reputable web sites that you recognize like; PC World, Microsoft (to include TechNet), Snopes, Symantec, cnet, F-Secure, and ZDNet to name a few. Many of these companies are participant in an organization called the Conficker Working Group. Microsoft was instrumental in bringing together the global security community to combat this threat. Their web site address is www.confickerworking group.org/wiki/.

So what are the most obvious indications that your computer is infected? If you can't get updates from Microsoft or your antivirus provider, you're probably infected. At the top of the Conficker Working Group web site there is a really easy test to determine if your computer might be infected. If you determine your computer is infected the Conficker Working Group web site mentions a few of the sites that provide removal tools. Most of these web sites are antivirus program providers. Since Conficker blocks access to these types of web sites you need to use a workaround. You'll need to use a clean computer to download the removal tool and copy it to a CD or flash drive, then run the program from the CD or flash drive. Another option would be to attempt to log on to www.bdtools.net and download the removal tool (bd_rem_tool.zip) for a single PC. However, if you're one of those computer users that "just want to email", your dead in the water. To do any of this you need to know how to download programs from the Internet, move information around the computer, copy information to a CD or flash drive, and how to download and handle compressed files (.zip).

Your best defense against malicious programs like Conficker is to know what you need to do to keep your computer safe. It's much easier to use the free tools available to keep your computer safe then it is to recover from an infection that trashes your computer. Here's a list of things you need to do.

Make sure you're receiving all of the Microsoft updated that are appropriate for your computer.

Install a good antivirus program, make sure it's configured to provide maximum protection, and is updated every time you start your computer. Only one antivirus program. This means that if your computer came with a trial version of an antivirus program you elected to not use or didn't pay to continue to use after the trial period ended, you need to make sure that program has been uninstalled.

Install a number of spyware detection and removal programs and keep them up to date. If more than one of the programs you've elected to use includes an active monitoring feature, select the one you want to run in the background and turn off this feature in the remaining programs.

Use common sense and be careful what you click on when surfing the Internet and reading email. Those strange programs you find on your computer got there because the person running the mouse agreed to download them or visited a malicious web site that was designed to automatically install programs. Never open an email attachment unless you're absolutely positive it's safe. Know how to configure and use your email program so that you never open an unsolicited email message (spam).

Here are several relatively new free programs you might want to consider using.

Malwarebytes' Anti-Malware - A free program that can identify and remove malicious software from your computer. The address is www.malwarebytes.org

SUPERAntiSpyware - They offer a free version and a professional version ($29.95) with the option to purchase a lifetime subscription for $9.95. The address is www.superantispyware.com

Web of Trust (WOT) - This free program can help you stay away from risky web sites. Go to their site at www.mywot.com and watch the Demo.

Having read all of this, here's the good news. Conficker does not affect any Windows XP or Windows Vista operating system that has been kept up-to-date with all of the Windows patches and updates. Microsoft released a patch for the first variant of Conficker in October 2008. The update was KB958644

Having a problem with your computer? Having a problem doing something on the computer? Stop by one of the Open House Help Clinics we have at the John Ruehle Center and see if we can solve your problem. These clinics are from 10 a.m. to 1 p.m. on the first Saturday and the third Wednesday of the month. The clinics are open to the public so you can invite a friend or neighbor. There has been a significant increase in the number of people taking advantage of this service. If everyone arrives during the first hour there will probably be a wait