

# Bits and Bytes

Arkansas' Premier Computer Club

November 2007  
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](http://www.bvcompclub.org)

E-mail: [jrc@bvcc.arcoxmail.com](mailto:jrc@bvcc.arcoxmail.com)

---

The following article was provided by Paul Buckner, Buckner Computer Service

### Beware of Spyware

You have undoubtedly heard of Spyware by now, and probably have Spybot Search and Destroy or Ad Aware installed to help deal with the threat(s) it poses. According to F-Secure, Spyware is defined as: Software that performs actions such as creating unsolicited pop-ups, hijacks home/search pages, or redirects browsing results.

Although that definition is correct, the lines between Spyware, adware, viruses and Trojans are blurring badly. Many who wrote viruses have found employment using their skills to write Spyware programs. As you have probably heard by now, Spyware often times comes packaged with free software in the hopes that you will download the potentially fun or helpful program, and unknowingly infect your computer. This kind of software is usually advertised by popup ad or banner ad on a website, or by spam, etc.

Recently, Spyware writers have begun using Trojan and worm software to compromise your computer. This is where the lines blur, because these aren't tactics traditionally used by Spyware. This 'strain' uses flaws in Microsoft Windows (like many viruses) to get onto your computer, along with popup ads, etc. Once your machine is infected, it will slow down and you will receive many, many more popups, some of them impersonating real alerts from Microsoft Windows.

These Popups in turn often advertise software that will supposedly remove Spyware, viruses, speed up your computer or clean your registry, all for a fee. Once you have downloaded and installed the software, the Spyware infection may or may not be removed, but many of the popups remain. The horrible fact is, you have actually paid to have the Spyware removed by the people who put it there in the first place.

These programs are weak pretenders bent on infecting your machine and then blackmailing you into having the infection removed. It is no different than someone stealing something from you and then selling it back. Unfortunately, in many cases the infection is either not removed, or is in fact replaced by other Spyware. People often pay between \$20.00 and \$60.00 to these charlatans.

Now, to be certain everyone understands, companies like Microsoft, Norton, McAfee, Grisoft (AVG), BitDefender, Ad Aware, and Spybot Search and Destroy, and other well known products, do not deliberately infect your machine with anything.

So, in conclusion, if you are receiving any of these symptoms, be aware that fraud may be at your doorstep, and quickly move to eliminate these popups with antispymware programs such as Ad Aware, or Spybot. If you are already well in their grasp, you may need to resort to outside help, but I hope that this article serves as warning of a change in how Spyware programmers are targeting unsuspecting PC users.

---

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.

No Club meeting in December. Have a happy holiday and we will see you in January.

People are always asking about the free antivirus programs; AntiVir, Avast!, and AVG. While the following article did not state which version of the program (commercial or free) was tested, I

think the results speak well for the companies that make these products.

# AV-Test.org Reports Stats from Antivirus Roundup

05.22.07

by Larry Seltzer

AV-Test.org, an independent testing group at the Otto-von-Guericke-University (Magdeburg, Germany), tested 29 anti-malware products with a very large set of files (606,901 to be specific). The goal was to test detection capabilities only, not cleaning. Products were set with their most aggressive detection options, such as using all heuristics and testing inside archives.

In the test set were:

- 68,864 backdoors
- 407,487 Trojan Horses
- 47,891 bots (zombies)
- 82,659 worms

Some of the results:

- The best product, WebWasher, detected 99.83 percent, but this is a gateway product. The best desktop product, at 99.56 percent, is AVK 2007.
- The worst product, Computer Associates's eTrust-VET, detected 62.12 percent.
- The average product detected 86.95 percent, the median 90.97 percent.

All products were last updated on Friday, May 18th, prior to the test. Only current malware was used, meaning all samples were seen in the last 12 months. Only Win32 malware, not 16-bit Windows or DOS, was used, and all malware had to be functional, as opposed to corrupted or benign samples.

Here is the full data set:

This information obtained from the following Web site.

<http://www.pcmag.com/article2/0,1895,2135092,00.asp>

Program	# Detected	Detection %
WebWasher	605,846	99.83%
AVK 2007	604,255	99.56%
AntiVir	603,408	99.42%
F-Secure	594,333	97.93%
Symantec	593,355	97.77%
Kaspersky	592,606	97.64%
Fortinet	589,028	97.06%
Avast!	584,574	96.32%
AVG	583,541	96.15%
Rising	582,772	96.02%
BitDefender	580,700	95.68%
Norman	574,476	94.66%
Ikarus	561,607	92.54%
Panda	558,899	92.09%
Trend Micro	552,107	90.97%
Nod32	536,043	88.32%
McAfee	529,680	87.28%
Dr Web	520,959	85.84%
F-Prot	517,491	85.27%
VBA32	498,264	82.10%
Sophos	496,135	81.75%
eSafe	495,074	81.57%
Microsoft	488,942	80.56%
Ewido	456,660	75.24%
VirusBuster	441,341	72.72%
Command	414,036	68.22%
ClamAV	387,276	63.81%
QuickHeal	382,557	63.03%
eTrust-VET	376,983	62.12%