Free Antivirus Software for Home Use v5.0

1. Summary for the impatient

- Avast: Recommended
- AVG: Acceptable
- Avira: Recommended
- ClamWin: Not recommended
- Comodo: Recommended
- CyberDefender Early Detection Center: Not recommended
- Drivesentry: Not recommended
- Moon Secure Antivirus: Not recommended
- PC Tools: Not recommended
- Spyware Terminator: Acceptable with cautions

2. Introduction

If you're using Windows, you'd be foolish not to have anti-virus software. At work you have an IT department to take care of it and pay for it. But home users are on their own. However, you don't need to spend lots of money to get good anti-virus software. In fact, you don't have to spend any money at all.

There are at least 10 anti-virus programs free for home use you can choose from. Three of them are also free for business use too. If you don't like those, sometimes your Internet Service Provider will provide you with commercial antivirus software at no charge. Regardless of the price or source, which one do you choose?

I used to believe the answer was simple, just pick one and keep it updated. I was wrong. There are many factors to look at. Three of the most important ones are cost, how much of a PITA the software is, and last, but hardly least, how well does it work. As one antivirus tester put it (http://blog.untangle.com/?p=95), “Open source antivirus hasn’t gotten a fair shake, and all the meanwhile some commercial vendors escape with selling products so poor it should be considered a scam to sell them...”

I set out to prove him right. I wanted to show that two open source antivirus products, Moon Secure and Clam, are just as good as any commercial antivirus. And

since I was at it, why not test some other free products that would be of interest to HAL-PC members too? In the end, things didn't go quite like I expected.

As a note, I will use the terms virus and malware pretty much interchangably. All the antivirus products I'm aware of don't just detect viruses any more. They detect viruses, trojans, worms, spyware, and rootkits, aka malware. Or at least they try to. A 2007 research study by Panda Labs found that about 23% of infected machines had active and up-to-date antivirus software (http://cli.gs/930J3L).

3. The Criteria

Which products to test? That was the question I faced. Considering this is all self funded, the free products jumped right to the front of the line. I started searching the net for a complete list of all the antivirus products out there. I didn't expect the list to be that big. In the end, I found 55, and I'm still not sure I found them all. There is no one, complete list that I could find.

Out of those 55, how many are free for at least home use? Most HAL-PC members have home computers to protect, and except for us Linux SIG members, the vast majority those computers are running Windows. So I limited my search to at least free for home use and Windows, which gave me 10 candidates.

4. Licensing Issues

The next step was to check out the license terms for each of the 10 finalists. It's not unknown for software manufacturers to stick rather onerous terms in licensing agreements, including no benchmarks being published without their say-so.

While it's true that such terms might very well be declared unconscionable by almost every judge in America, it's just not worth the money to fight it out in court. Better to learn about it early, and pass that product by. With that in mind, I started reading the End User Licensing Agreements (EULA). When I woke from my legalise induced coma, two contenters eliminated themselves. No testing was done on these products.

> *CyberDefender Early Detection Center* (http://www.cyberdefender.com/antivirus-products/products.html): Not recommended. The free version is ad supported and the license agreement includes a clause that you must agree to a software audit at any time at the company's discretion. While free, there are other choices in this list that don't make you see ads or agree to audits.

Drivesentry (http://www.drivesentry.com/): Not recommended. After 30 days, the free version of their software does not automatically update. You must remember to do this by hand every day. As with CyberDefender, there are less annoying choices in this list. OK, technically this isn't a licensing issue, but it's such a big drawback I can not recommend it.

Be warned that nasty terms and tricks are not limited to just these two. For instance, in my research I turned up this quote:

> ...McAfee, Symantec and Microsoft (with Windows Live OneCare) all set your credit card up for automatic renewals when you purchase their security software on-line. The gripe is that you can't opt out of this during the purchase. OneCare is the most difficult of the three to opt out of. In fact, you can't. Instead you must must cancel your subscription altogether by calling 866-663-2273...

5. Gathering the malware

Now that the field was down to 8, it was time to find some malware to throw against them and see how the various products did.

In my line of work, I'm sometimes called upon to clean infected computers. This gave me a perfect opportunity to gather, real, in-the-wild, samples. I have friends and associates that also do cleaning from time to time, and they gave me additional samples.

I should note that homes with teenagers were great sources of malware samples. Parents, don't let your teenagers on your computer if you have information on there that you wouldn't want a criminal to have. The teenagers aren't quite as web-savvy as they would like to believe.

As soon as I got the malware, I would then run it against the remaining antivirus products, being sure to update them first, and recorded which ones missed it. In a several cases, the samples were false positives - the antivirus said it was malware, but it was not – and I recorded those as misses too.

After I ran my tests, I submited the samples to those vendors that missed them, in hopes of preventing someone else from getting infected. In the process, I learned two dishearting facts about the antivirus world.

1. Antivirus companies don't like to share. A sample submitted to one will not be passed around as a rule. Clam is one exception, and the developers of Clam claim the sharing is pretty much all one-way. The side effect of this is the

time it takes an antivirus product to start detecting new malware can vary considerably. This lack of sharing also means the same malware will have many different names, making researching it that much harder.

2. Protection comes slow. I would keep the samples around and test again over the next few days. None of the companies ever gave any acknowledgement that the sample submitted was malware and a new signature had been added. Testing against the updates was the only way to see when they added my samples to their databases. The shortest update time I observed was 3 days, with some samples taking 2 weeks to get added.

I suspect the slow update times were a combination of several factors. First, none of my samples got much press coverage. I'm certain mainstream media talking about a particular piece of malware would speed up the definitions. It is also reasonable to assume the number of submissions of a particular piece of malware has an impact on how quickly a signature is added.

Another part of the problem is one of sheer numbers. There are many, many more malware writers than antivirus signature writers. The defenders are simply overwhelmed. Each sample has to be checked to be sure it is malware, then a signature has to be created, then checked to make sure said signature doesn't create a big false positive problem. All this takes time.

6. The Results

None of the remaining contenders had a perfect score. None. Everyone missed something, which is more than a little disheartening. In fact, I had two samples that appeared to be zero day malware that over 40 different scanners missed. So much for the vaunted heuristics engines many vendors tout.

Still, some caught most of the samples, while others did poorly. Remember that 23% statistic from Panda Labs. It's quite believable based on my results. It's not enough to have active and up-to-date antivirus. You have to have active and up-to-date GOOD antivirus.

Unfortunately, GOOD is hard to determine. All test results, not just mine, are snapshots of history. Today's top performer could easily become tomorrow's dog, and vice-versa, and even top performers can have bad periods. It is important to reguarly evaluate your antivirus solution, regardless of what it is. Don't just rely on fancy marketing or a recommendation from someone who knows a lot about computers. This especially includes salesmen at the big electronics stores.

My testing has come down to eight products I would put in three different categories. The finalists are: Avast, AVG, Avira, ClamWin, Comodo, Moon Secure, PC Tools Antivirus, and Spyware Terminator. Of these, there are three categories: Standard, Host Intrusion, and Manual Scanning.

6.1. Standard

Most antivirus programs fall into the Standard category. They have a database of signatures for malware that they check against, both manually and with an on-access real-time scanner. Many also have a heuristics engine that will attempt (key word: attempt) to figure out if a program has the characteristics of malware even without a signature.

The heuristics engines are something of a mixed blessing. While they give you a chance to block malware there is no signature for, they also tend to flag perfectly harmless, and sometimes important, programs and files as malware. Heuristics engines have resulted in critical system files being removed, disabling the computer. It happened before and will likely happen again.

Overall, programs in the standard category require very little user interaction. They run on auto-pilot 95+% of the time. Of the final seven, Avast, AVG, Avira, and PC Tools Antivirus are in the standard category. Moon Secure is also in the standard category, but as explained below, was excluded very early in the testing.

> *Avast* (http://www.avast.com/): Recommended. Its detection scores are tied with AVG and are very good. It beat Avira in the speed tests, but not by a significant amount. This software requires registration to keep working after 60 days, but the registration is only once every 14 months, so that's not very annoying. Avast's biggest problem IMHO is its interface. It has the strangest, least user friendly interface of all seven. The interface is modeled after an audio media player. I would be lost using it without the tool tips. Fortunately, you don't have deal with it often. Avast also tends to be chatty, making use of your speakers to notify you of certain events.
>
> *AVG* (http://free.avg.com/): Acceptable. Of the four standard programs, it is part of a three way tie for best detection rates. Its interface is pretty simple to use when needed, and it's free. No mandatory registration or pop-up ads like Avast or Avira. It has one big flaw though, it's s--l--o--w. AVG finished dead last in the speed tests. You will notice when it is running its full disk scans, which, by default, are run every day.

Avira AntiVir (http://www.avira.com/en/pages/index.php): Recommended. Avira actually has the best detection rate of all seven programs. However, it also had the worst false positive rate of the seven programs (again, see Moon below for why seven and not eight). For this reason, I'd rate it a tie with AVG and Avast in the overall detection category. Speed wise it came in third, but the top three are so close most people won't notice a difference. The interface is good. This software has an optional registration. The free version of Avira does not include an email scanner. It does include a pop up ad for the paid version about once every one to two days, which stops me from giving it my top recommendation.

Moon Secure (http://www.moonsecure.com/): Not recommended. This software is free even for commercial use and uses the ClamAV engine. In early tests, it was missing stuff it should not. This is especially strange as some of the stuff it was missing **is** detected by ClamAV, upon which Moon is based. In addition, I have been able to confirm that it will not update if you enter any proxy settings in the program. For this reason, testing stopped early on Moon and it was dropped from testing. Hence, there are really only seven finalists.

PC Tools Antivirus (http://www.pctools.com/): Not recommended. While registration is optional, it is recommended. Otherwise your update download speed will be throttled. Of the four standard programs, it has the worst score in the detection tests, and is the second worst out of all seven overall. It's speed score (details below) was poor as well. While the interface is good, it doesn't make up for the other short comings.

6.2. Host Intrusion

The Host Intrusion programs are Standard category programs with an additional twist. They monitor access to certain critical files, folders, and registry keys. Any attempt by a program to access these is blocked and a pop-up message is issued. You, the user, can then chose to allow the action or continue to block it. Obviously, the user can exempt some programs from the auto-blocking.

Host Intrusion programs can warn you about attempted stealth installs even if the heuristics engine and the signature database fail. In my tests so far, none of the seven programs has a perfect score for the heuristics and signature detection, so the Host Intrusion programs can offer more security than those in the standard category.

However, this extra security comes at a price. While the Standard programs require almost no user interaction, the Host Intrusion programs can require a great deal of interaction. If you are the type of user who hates that sort of thing, go with one of the standard programs. If you are the user who has no idea how to determine what to block and what to allow, go with one of the standard programs.

Now don't get me wrong. The pop-ups do not occur every few minutes. All the pop-ups I've seen, with only a few exceptions, only occur when installing a new program or sometimes an update to a program. If you get a pop-up out of the blue and aren't installing something, odds are very good it's malware trying to infect you. The real difficulty usually occurs when some website tells you that you need a program they are offering you. Is it a legitimate program or malware? Unless it's Java, Flash, Shockwave, Silverlight, or Adobe Reader, the odds are good it's malware.

The pop-ups I found not caused by program installations were caused by the anti-piracy protection on some games. Teracopy also triggered a pop-up when I used it to change the default copy handler, but that was a one time occurence.

Two of the seven finalists are included in the Host Intrusion category: Comodo and Spyware Terminator.

> *Comodo Antivirus* (http://antivirus.comodo.com/): Recommended. This software is free even for commercial use. While the more complicated of the two Host Intrusion programs, it has a lot of nice features. One outstanding feature is threatcast. When a pop-up appears, Comodo will tell you how other Comodo users answered the question, although threatcast ratings are not available for every program. Usually, it is the more minor programs or malware that lack a threatcast rating. If there is no threatcast rating, the good course of action is to block. This will lead to an occasional incorrect answer, but you can always undo the block later. As far as detection, Comodo is in 4th place, although at least 3 malware programs it failed to detect by their signatures would have been stopped dead if you blocked it via the Host Intrusion. If you don't count those misses against Comodo, it is a four way tie for first place. Comodo finished first in the speed tests. Be warned, there is a learning curve for Comodo, but the protection offered once you climb that curve is probably the best of the group tested.
>
> *Spyware Terminator* (http://www.spywareterminator.com/): Acceptable with cautions. A third in the free even for business use category, this software was originally just anti-spyware. However, it includes the

option to integrate the ClamAV engine, giving you anti-virus protection too (but see my Clam review below). Spyware Terminator is less complicated than Comodo, but also has fewer features. The detection rate is as bad as PC Tools, even with the optional Clam addition. However, Spyware Terminator can be used with other anti-virus products. At least one user in the forums has mentioned using it with Avast specifically, and it will probably work with any in the Standard Category. By itself, Spyware Terminator won't give you good protection, but it can enhance the protection given by one of the others. Spyware Terminator finished fourth in the speed tests, although the gap between 3rd and 4th is considerable.

6.3. Manual Scanning

There is only one entry in the Manual Scanning category: ClamWin. Manual Scanning does not offer any real time protection, and will only scan files when you explicitly ask it to. As such, any Manual Scanner should not be used for everyday desktop use.

ClamWin was included for three reasons. First, its database is used in other products, namely Spyware Terminator (optional) and Moon Secure. Second, the Linux version of Clam is often used on mail servers as a cheap, and supposedly effective, way to prevent the spread of malware via email. It is also used to check files in Windows shares stored on Linux file servers. The database used by the Windows version of Clam (ClamWin) is the exact same one used in the Linux version. Finally, I could find little in the way of tests done on Clam. The little evidence I found was all over the board, from perfect to poor.

I used the Windows version of Clam rather than the Linux version to keep the playing field as level as possible. All the other programs tested were run under Windows, so I needed to run Clam under Windows as well.

I actually got into testing because I wanted to do an article recommending Moon Secure, and by extension Clam. I hoped to give Clam a glowing recommendation. I wanted to give Clam a glowing recommendation. Sadly, I can not.

Clam has come in dead last in my signature tests. Further, it did poorly in the speed tests, with only AVG coming in worse. I found it interesting that Spyware Terminator, which can and did use the Clam database, as well as its own database during the speed tests, did better than ClamWin by itself. As for Clam's performance on Linux, my experience using it has led to an estimate of 8-10 minutes/per Gig of data. Not exactly a speed demon there either.

Therefore, I must put Clam in the Not Recommended category.

7. Speed Tests

The tests were all done under a virtual machine, running XP SP3 with 512 MB RAM. A test folder of exe's was assembled. Some of the exe files are installer programs and as such contain other files. Windows Explorer lists the directory as being 711 MB and containing 910 files. All times are from the program in question reporting how long it took. Each program was run three times and the results averaged (mean).

The programs are sorted from fastest to slowest. The reported objects are larger than 910 in many cases as some programs automatically scan the memory when called, while others include every file in an archive to bump up their numbers. All programs were run with their default settings.

Program	*Version*	*Reported Objects*	*Average Time (seconds)*
Comodo	3.10.102363531	947	53.67 sec
Avast	4.8.1351	1580	60.67 sec
Avira	9.0.0.407	2887	65.33 sec
Spyware Terminator	2.5.8.145	913	167.67 sec
PC Tools	6.0.0.19	910	193 sec
ClamWin	0.95.2	910	222.67 sec
AVG	8.5.374	5594	361 sec

One suggestion I've received about why AVG was so slow was the free version was crippled - the “price of free”. I re-ran the tests on the same hardware, against the same files. I can definitely state that the free version is not crippled. The commercial version, slightly later than the free version, had an average time of 348 secs, with 5594 objects reported.

8. Conclusion

Just having active and up-to-date antivirus is not enough. According to one December 2007 article (http://cli.gs/DN9na8), no product tested by the VB100 test has a perfect score. The best, NOD32, a commercial product, achieved only 94%, and I've seen complaints about their database not updating due to an "undocumented serious error" and the software nagging about sending suspicious files to the makers of NOD32.

You have to do your research when picking an antivirus product. Hopefully, I've opened your eyes to just how bad it is out there. Just one miss can cost thousands of dollars (http://cli.gs/Xz5U2v). Be careful, it's a jungle out there.

Now if you'll excuse me, I have to don my fire retardant suit, as there's a lot of flames headed my way.