Colby-Sawyer College

Antivirus Product Comparison:
A real-world 'does it work' test

November 2004

By: Scott Brown
Information Security Analyst
Colby-Sawyer College

Antivirus Programs: Testing For A Solution

For many years, I read testing results from industry standard antivirus testing companies, countless pages of information, and I tried to make heads or tails of it. When I finished, I still pondered the question that brought me to read them in the first place. What antivirus program was best for my school?

Working as an Information Security Analyst at Colby-Sawyer College in New London, New Hampshire, I have the opportunity to see all sorts of malware.

Students want to explore all that the Internet has to offer. The problem is that the Internet is not always the best place to be curious. As a result, I've seen malware infections as high as 8,000 viruses on one computer. I was able to use my unique situation to acquire 10 zero day viruses/trojans and 2 exploits in one night. These could all be considered zero day infections, as most were not detected by antivirus software but all were confirmed by two or more companies after submission.

I chose to test these threats with 13 of the most popular antivirus programs available in the US, because I have seen these specific threats destroy a computer and render it useless both on and off the Internet. These threats are not self-propagating, which is what a true virus is.

Propagation is unnecessary when many of these infections are packaged with popular games or peer-to peer programs or on a web page that gets 10, 000 hits a day. In fact, Kazaa was the number one searched word on Yahoo last year. In any case, most of these infections were far more complicated and time consuming to remove and had worse effects than even the dreaded Sasser worm.

So why wouldn't every antivirus program detect and remove these infections? A technician from one of the antivirus programs tested explained to me that, although many of the samples I sent him

Most Popular Anitvirus Software Packages

Company	Product	Price
Sophos	Ant-virus v3.86.2	Single user license n/a
Network Associates	McAfee Virusscan 9.0	$39.99
Computer Associates	eTrust Anti-Virus 7.1	$29.95
Kaspersky Labs	Ant-Virus Personal 5.0	$41.50
Trend Micro	PC-Cillin Internet Security 2005	$49.95 (incl. Fire Wall)
Panda Software	Titanium Anti-Virus 2004	$49.95 With True prevent
Frisk Software	F-Prot Anti-virus for windows v3.15b	$29
Symantec	Norton Antivirus 2005	$49.95
F-secure	F-Secure Antivirus 2005	$64
Bit Defender	Bit Defender v8 standard	$44.95
Eset	NOD32 v2	$39
Norman	Virus Control v5	$63.74
RAV	GeCad	$29

were trojans and did create a back door into a computer or installed some sort of malicious code that would eventually completely disable a computer, they are primarily used to propagate spyware rather than virus-like activity. Until these infections are actually being used for virus-like activity or for reasons other than bombarding your computer with spyware, their company will not detect these infections. The technician went on to tell me that one spyware company in the UK was bold enough to take legal action against this antivirus company and sue under the pretense that their software does not self propagate and therefore does not meet the legal requirements of a virus. Detection by an antivirus company would most surely lead to bad press for these and other companies developing similar software. In my opinion, they are riding the fine line of the law, skirting legality by saying their programs do not self propagate and therefore are not viruses. It is important to note that another reason these companies avoid being sued is that they are just one program. One illicit malware program does not always destroy your computer, but when that piece of malware downloads other malware that downloads other malware, etc., it usually does destroy a computer. And that's what these products do.

I have not seen a virus that I cannot disable after a short time; however, I often spend several hours on a computer trying to remove spyware. With a few exceptions, people who have viruses usually don't know they are infected; that is seldom the case with spyware. The problem is that these malicious programs are technically not spyware either; they are a combination of spyware and a virus or trojan. As such, they weren't detected by any of the spyware programs I tested either, creating kind of a grey area. Without these programs removed, reinfection of your computer will keep occurring.

In one case, I experienced a computer with over 300 processes running; it took over 20 minutes to get the task manager up. In the information security age, antivirus programs that do not detect these spyware/virus crossbreeds simply won't cut it. Users need a complete antivirus solution combined with a good spyware solution with real time protection such as Pest Patrol or Spy Sweeper. Older programs tend not to address trojans for spyware. Pest Patrol reports over 1,000 new pests every month. ESET found over 400 new virus or trojans in the week of testing, while some of the traditional antivirus companies found as few as nine infections. See my results and you tell me where the real threat is.

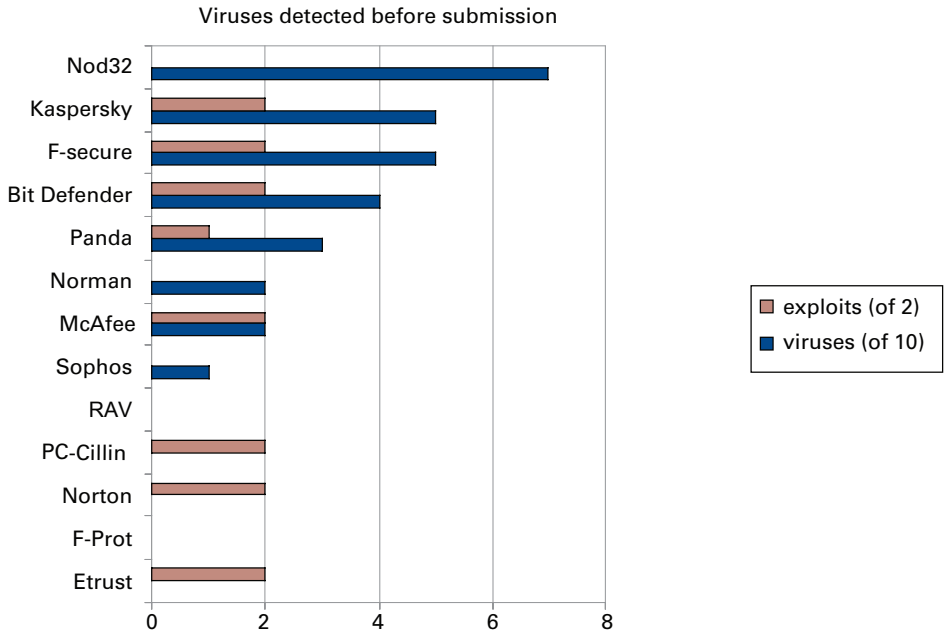
The Tests

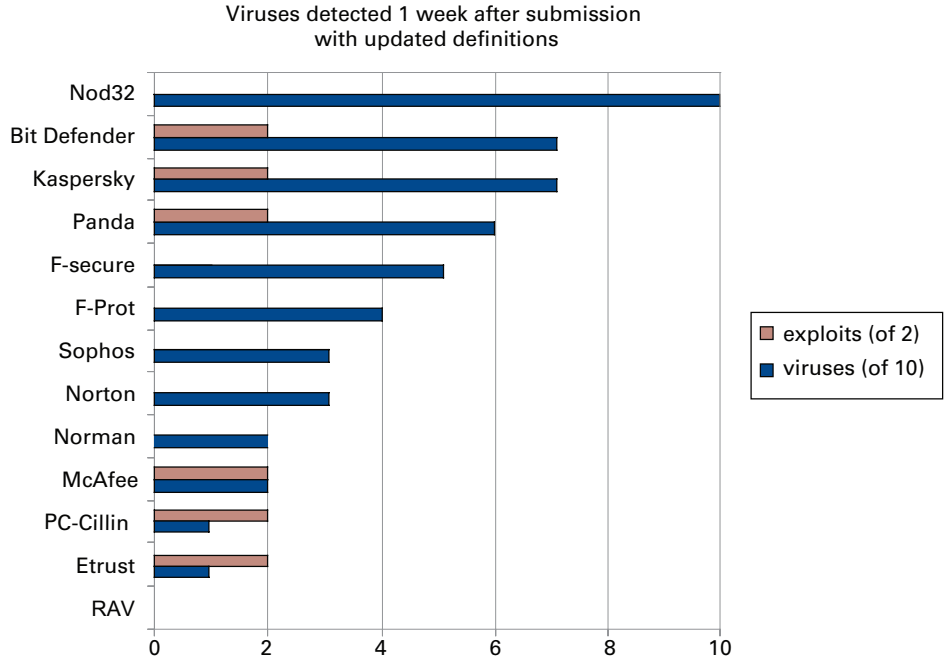
A few notes about my testing. I reviewed 13 different antivirus programs, testing them on a fully patched Microsoft Windows® XP Pro SP2 virtual machine (VMware) with the latest version and definitions from the antivirus company's web site. Only products assumed by me to be available to consumers in the US (or at least I thought they were, previous to testing) were tested. I did not read any manuals. Like most of you, I want to install my antivirus product, know that I am immediately protected and continue on with my chosen activity.

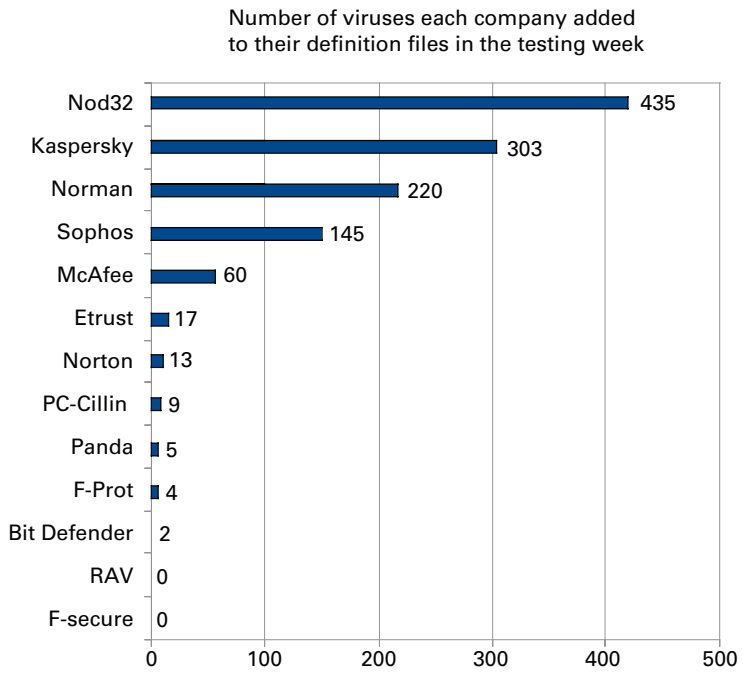
Products were all tested on the same day and then exactly one week later.

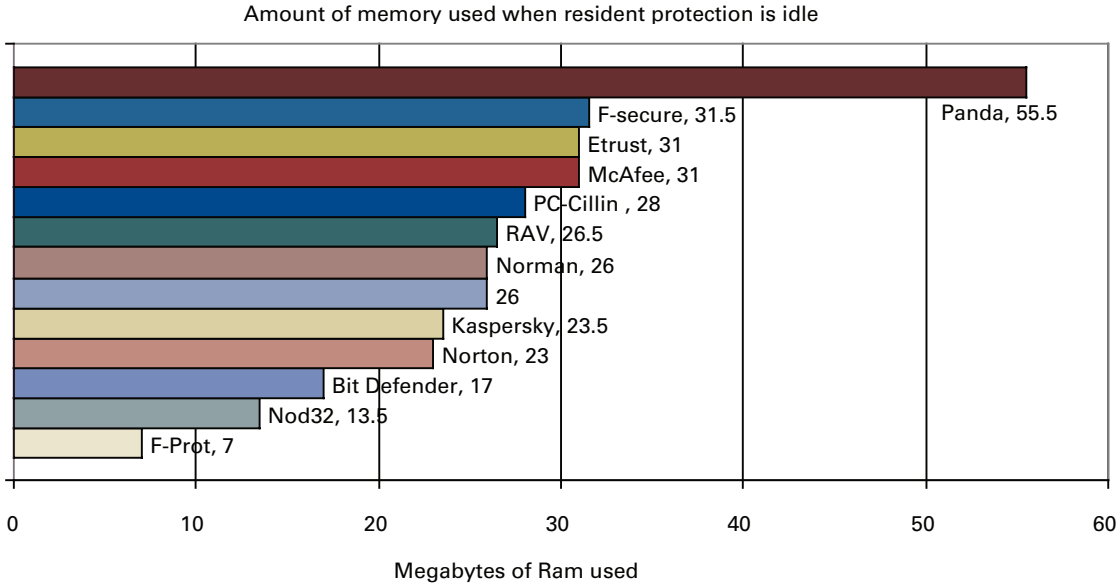
To test the antivirus companies for their responsiveness, each company was sent the 10 zero day viruses and two exploits that they had been previously unaware of, emailed to them that same day using a distribution list. Exactly one week later, I updated all antivirus definitions and retested. Note that some of these viruses were detected by many of the antivirus companies as unknown infections with the use of heuristics (refer to the "Viruses detected before submission" and "Viruses detected 1 week after submission with updated definitions" charts in this paper).

Viruses Detected






Number of viruses each company added
to their definition files in the testing week
Nod32
Kaspersky
Norman
Sophos
McAfee
Etrust
Norton
PC-Cillin
Panda
F-Prot
Bit Defender
RAV
F-secure
435
303
220
145
60
17
13
9
5
4
2
0
0
0
100
200
300
400
500


Amount of memory used when resident protection is idle
Panda, 55.5
F-secure, 31.5
Etrust, 31
McAfee, 31
PC-Cillin , 28
RAV, 26.5
Norman, 26
26
Kaspersky, 23.5
Norton, 23
Bit Defender, 17
Nod32, 13.5
F-Prot, 7
0
10
20
30
40
50
60
Megabytes of Ram used

The following "does it work" section is taken from Virus Bulletin, one of the world's best antivirus testing labs, relied on by many professionals. This is what inspired me to do this testing, find some viruses that eluded detection and send them in to the antivirus software companies. Like the quote says, you need to be able to detect most of the viruses found in real life, including trojans.

Does it work?

How do you determine whether antivirus software works? The main purpose of antivirus software is to identify and block viruses and trojans that are circulating in the wild. It doesn't matter which virus software can recognize "the most" viruses, or whether it detects all viruses in a test collection consisting mostly of non-functional viruses, viruses that haven't been in circulation for years, or artificial viruses that were created solely for testing purposes. Neither does it matter how many copies the software has sold or how many companies are relying on its protection. Antivirus software only works if it can deal with real-life viruses that make their way into your inbox, your browser, or your network right now.

Virus Bulletin magazine is a technical journal on developments in the field of computer viruses and anti-virus products. VB tests antivirus software on a monthly basis and awards products that detect all "in the wild" viruses during both on-demand and on-access scanning in certain Virus Bulletin tests with its VB100% award. More details on what this award is all about can be found at: http://www.virusbtn.com/vb100/about/100procedure.xml.

Total of each company's success rate on any given product or OS to date* as tested by Virus Bulletin (10/2004)

Name	Tests	Pass	Fail	Success ratio %
ESET/NOD32	31	28	3	90.32%
Trend Micro	31	25	6	80.65%
Symantec	31	25	6	80.65%
Sophos	36	25	11	69.44%
Norman	35	24	11	68.57%
eTrust	28	18	10	64.29%
Kaspersky	36	23	13	63.89%
F-secure	27	15	12	55.56%
McAfee	33	16	17	48.48%
bit defender	10	4	6	40.00%
Frisk/f-prot	28	11	17	39.29%
Panda	4	1	3	25.00%
RAV	25	6	19	24.00%

*testing was done only with propagating viruses, not other types of malware

Conclusion:

After an extensive internal test of nearly every antivirus product on the market for higher education, I concluded that NOD32 is the best antivirus product on the market. Kaspkersky is my second choice.

Both are top notch. In the testing, NOD32 excelled in speed and low use of resources, while Kaspersky did a better job with archives but detected fewer overall. It is worth noting that NOD32 has US support. A real person answers the phone and the company offers close to 24/7 email support, where Kaspersky has no support in the US. They do, however, have a US reseller. (Note: as of recently, Kaspersky has an office in the US.)

bit defender and Panda were next in line. However, Panda was one of the most resource intensive products tested. All four of these products deal with downloader trojans, droppers and a wide variety of malware and would be helpful in this fast-growing epidemic.

College students are becoming increasingly technologically savvy, spending a significant amount of time daily exploring the Internet, reading and sending email and downloading potentially risky files. Starting with the fall 2005 semester, Colby-Sawyer College will require all computers that plug into a campus network connection to have NOD32 antivirus protection.

Additional Comments and General Notes by Product

All antivirus companies in this research responded to the emails sent with virus information, indicating that I had the right email addresses.

My comments below are listed in order of best to worst, as determined by Virus Bulletin. You'll note that except for the ranking of NOD32 number one, their results don't match mine.

NOD32 by ESET

Web site: http://www.nod32.com
Local office: San Diego CA
File size: 7.2 MB
Support: (619) 437-7037, 6-3 PST, almost 24/7 email support

Comments: Very low resource overhead; the product is advertised as the fastest scanner in the world. The Internet module watches IP stack and intercepts viruses before they make it to your computer.

Great support, no automated answering menu, always a live person and never any wait times. Great heuristics; in fact the highest detection with the fewest false positives, as reported by independent testers. Independent tests say 85%, while ESET says they are at 91%. Automatic updates start immediately at logon or dial up. This was one of two products that caught viruses importing into my VMware session. After detection, I was no longer allowed to access those files. It is also worth noting that the last few big viruses that disabled the antivirus software did not disable NOD32.

One of the only complaints I have is related to the company's web site. It lacks a little information about viruses, only seeming to list the biggest ones.

This is an outstanding product, probably the best. These guys are definitely not marketing their product enough, as over the past nine years Virus Bulletin has awarded NOD32 more Virus Bulletin 100% awards than any other antivirus software available.

PC-cillin 2005 by Trend Micro

Web site: http://www.trendmicro.com
Local office: Cupertino, CA
File size: 38 MB (with fire wall, no evaluation version available; used what had been recently purchased, but soon abandoned by a colleague)
Support: (800) 864-6027 toll-free phone support (Mon – Fri 5 a.m. – 5 p.m. U.S. Pacific Time)

Comments: Nice pre scan on the install, says it can detect spyware. Unfortunately though, the program doesn't seem to detect much of anything, and even deletes an entire archive without asking, even if just one infected file is found.

Norton 2005 by Symantec

Web site: http://www.symantec.com
Local office: Waltham, MA
File size: 24 MB (almost that much in updates)
Support: Not available

Norton 2005 by Symantec (continued)

Comments: Limited support plan, very high resource usage after install, needs extensive updates and a reboot. Has a built-in pre scan during install. Detects spyware but not the trojans used to install them. Did not auto update; I had to do it manually and it required a reboot to be effective.

SOPHOS

Web site: http://www.sophos.com
Local office: Lynnfield, MA
File size: 14.5 MB
Support: 1-800-355-3220, 24 hour/7 days a week

Comments: This program offer few options; no manual update, no single user license, no way to unload from memory and it is fairly resource intensive. It locked up when extracting my zipped viruses, which made testing very hard. One surprise is that is doesn't appear to have an OD scan. It does, however, have an option to scan for Mac viruses.

When I called on a Saturday night, a technician answered the phone and was very helpful. He emailed me a nice script to help capture new viruses. The technician also stated that it is company policy that their company does not detect nor remove any spyware related infections.

This product has no manual update features. When I downloaded the new definitions dated November, it was only the third week in October.

Norman

Web site: http://www.norman.com
Local office: Fairfax, Virginia
File size: 12.5 MB
Support: 703-267-6109, 1-888-GO-NORMAN (888-466-6762)

Comments: No reboot required after install, but product is a little sluggish. Technician did return my phone call after leaving a message over the weekend.

eTrust by Computer Associates (formerly InoculateIT)

Web site: http://www3.ca.com/Solutions/Product.asp?ID=156
Local office: Islandia, NY
Support: (866) 422-2774
File size: 17.2 MB uncompressed, as this came on a CD provided by CA.

Comments: This program kept locking up and when I rebooted, the SP2 fire wall prompted me to allow eTrust to connect to the internet, but it didn't run right until I disabled the firewall completely. Support is not included and there is a $50 minimum charge.

eTrust has two different scan engines to choose from, although neither one of them found many viruses. The options were few to moderate. There was a lot of work to get this product to work, only to have it find just one new virus.

Their web page was difficult to navigate which is why I gave you a direct link to the product (these guys market a ton of solutions).

Must disable SP2 fire wall or manually set permissions to update.

Kaspersky

Web site: http://www.kaspersky.com
Local office: Russia (as of 2005 the company has an office in Woburn, MA)
File size: 13.7 MB
Support: Russian and English, 24 hours a day: 1- 800-803-2152 (although I never could get through)

Comments: No reboot required for install, nice, easy to use interface, nice options. This product comes in a pro version for the advanced user. Great archive scanner prompts user for password on locked files. Didn't update right away, but when I clicked on the update, it told me they were 7 days old and updated. By far the best web site with the most information and it offers an online scanner.

NOD32 and Kaspersky were the only programs that caught my viruses as I copied them into my VMware session and when I highlighted the file with the mouse without opening them. This is definitely one of the best products out there. I could not stop laughing as it squeals like a pig when viruses are detected.

F-Secure

Web site: http://www.f-secure.com
Local office: Finland
File size 25.1 MB
Support: +358 9 2520 5050, 8-6pm, CST,

Comments: Appears to be highly resource intensive; needed a reboot to get it to work properly but the program did not indicate that would be the case. Auto updated a week later with no interaction. Very fast scan, works nicely.

McAfee by Network Associates

Web site: http://www.mcafee.com/
Local office: Santa Clara, CA
File size: N/A (has online installer, hard to tell the size, but I would guess quite large)
Support: 1-800-338-8754

Comments: This is a great interface for someone who has no computer knowledge; it looks pretty easy to use, but offers very limited options. This program has quite a drain on resources (very slow.) It locked up the computer when unzipping my viruses. The interface encourages you to buy other security products, which seemed to me to be spyware-like tactics. Very slow scan speed when scanning a single file. It also scans about 35 extra system files, which make it agonizingly slow.

After sending the company several of the virus samples, MacAfee emailed back saying they were new viruses and they would update their definitions to capture them. A week later, they were still not detected.

When McAfee emailed the results back, they included an updated definition called extended.dat. However, with no instructions on what to do with it and after searching for an existing file by the same name with no results, I put it in the folder with the clean.dat and the scan.dat file, but it did not seem to make any difference, even after a reboot.

bit defender

Web site: http://www.bitdefender.com
Local office: Boca Raton, Fl
File size 8.6 MB
Support: 561-620-8815

Comments: Nice package, however the software offers few options and was semi resource intensive.

F-Prot by Frisk Software

Web site: http://www.f-prot.com/
Local office: Reykjavik, ICELAND
File size: 3.15 MB
Support: +354-540-7400 (did not have the US presence I thought it did and should not have been reviewed)

Comments: Small and fast install, extremely fast update (came with virus samples only a week old). However, it offered very limited options, and at the time of testing the definitions hadn't been updated in almost a month.

Panda

Web site: http://www.pandasoftware.com

Local office: Greendale, CA

File size: 20 MB

Support: (818) 543-6901

Comments: One of the slowest products tested, and it requires the most memory out of the programs tested, as you will know when it is installed. However, the program did perform fairly well, and the company was responsive to my emails.

RAV v8

Web site: http://www.ravantivirus.com/
Local office: Romania
File size: N/A
Support: Unknown

Comments: No reboot required. Packaging says it protects against all malware, 107,060 to be exact. Not sure the on demand scanner really scans anything; it always showed the same number of files after each scan. This product is temporarily unavailable for download, but I found it on their ftp server.

Their web page had the following announcement:

"**IMPORTANT ANNOUNCEMENT**: Due to the acquisition of RAV's IPR (Intellectual Property Rights) by Microsoft Corp., please be informed that starting with 3rd of September 2003, RAV AntiVirus direct sales (including the online e-store) have been **closed down**."

Updates are still available but seem to have no effect.

About the Author:

Scott Brown has been an Information Security Analyst with Colby-Sawyer College since 2004. Prior to joining the school, Scott had been running his own computer consulting business for nearly 20 years, specializing in building and repairing hardware and troubleshooting operating systems for small businesses. By the late 1990's he found himself doing more and more operating system and network troubleshooting. He's been working with malware since the beginning and is an individual that clearly understands viruses and other forms of malware.

Colby-Sawyer College is an independent and comprehensive liberal arts college located in scenic central New Hampshire.