

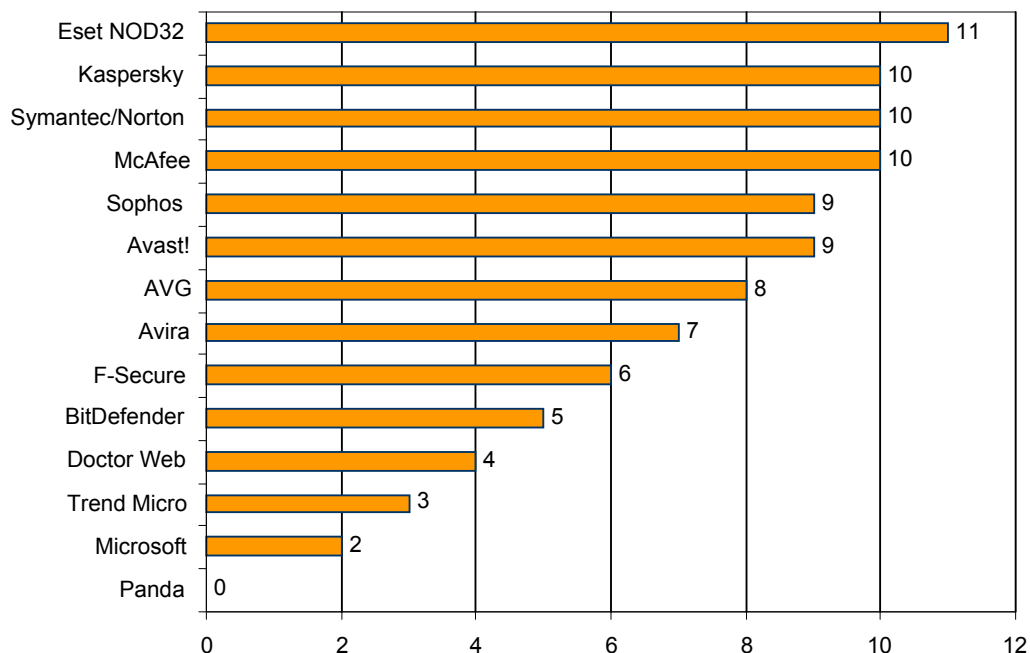
Variety is the Key to Testing

To confirm the advantages of their products antivirus developers often refer to the results of different independent tests. You can find them on various web sites and in promotional materials. But sometimes users do not understand what exactly has been tested or how. The aim of this article is to shed light on the tests performed by different research labs, to compare the antivirus products subjected to testing, and to develop a general integrated assessment of antivirus programs based on the test results. I would like to note that the article will only include a comparison of the most popular antivirus solutions in Russia, i.e., Kaspersky Anti-Virus, Symantec/Norton, Doctor Web, Eset Nod32, Trend Micro, McAfee, Panda, Sophos, BitDefender, F-Secure, Avira, Avast!, AVG, and Microsoft. Less familiar products such as G-DATA AVK, F-Prot Anti-Virus and AEC TrustPort will not be considered. So, let us begin our “research”.

Patriarchs of testing, isn't it time to retire?

The British magazine Virus Bulletin was the first to test antivirus products back in 1998. Their test is based on the WildList collection of malicious programs. To pass the test it is necessary to detect all the viruses from this collection, as well as avoiding false positives while scanning the “clean” files in the collection. Testing is performed several times a year on different operating systems. The products which successfully pass the test are awarded the VB100% award. Below is the list of companies whose antivirus products were awarded the VB100% in 2006-2007.

Number of successful VB100% tests (2006-2007)



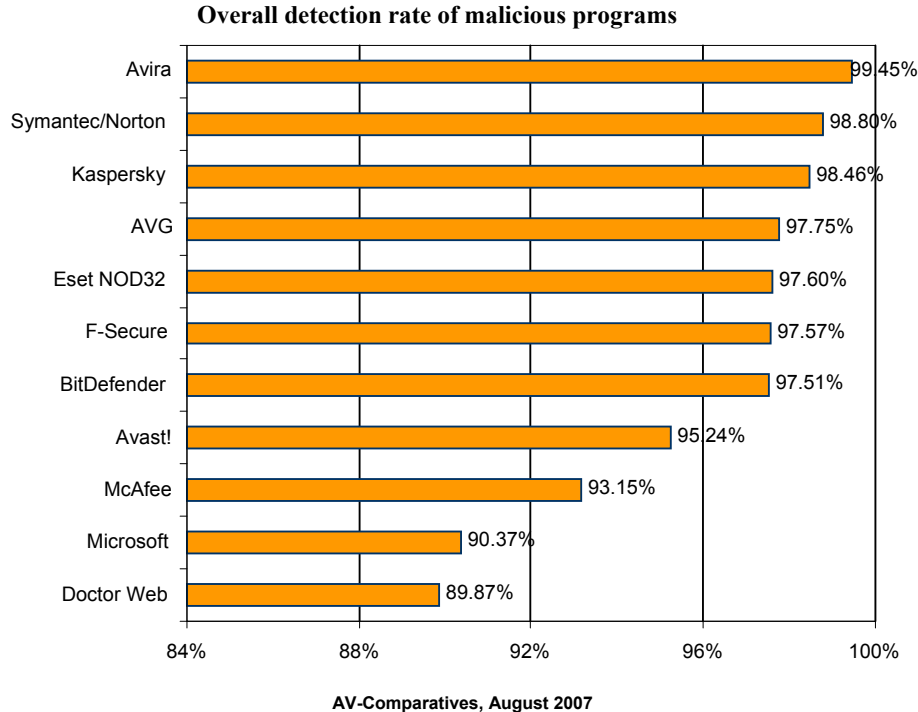
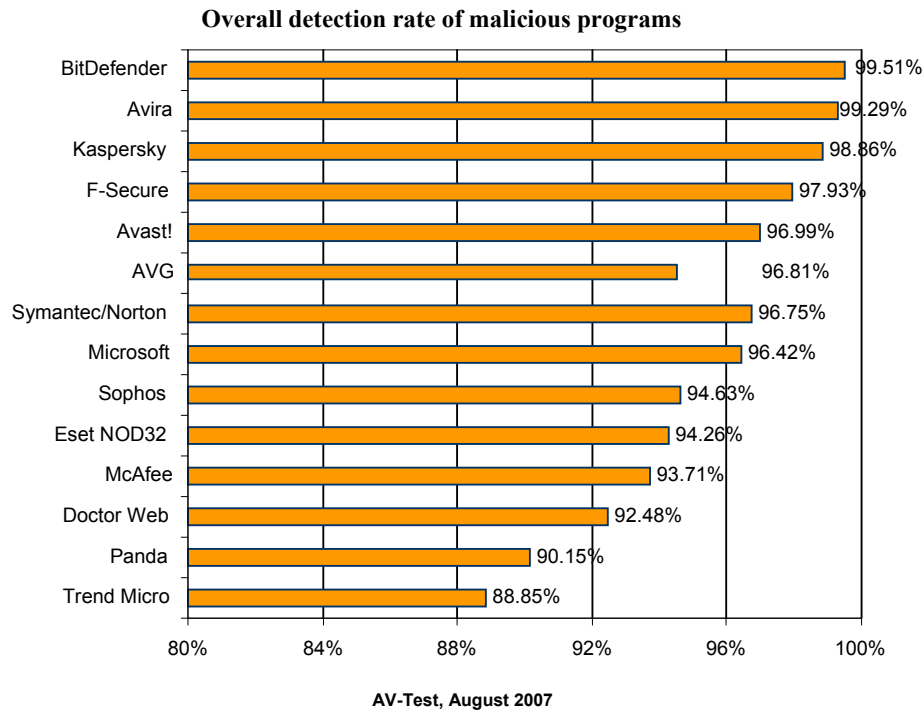
Virus Bulletin, October, 2007

Virus Bulletin may be the oldest antivirus tester, but its patriarch status does not protect it from critics within the antivirus community. For example, at the Virus Bulletin Conference in September in Vienna Andreas Marks, a renowned expert from the AV-Test Lab at Magdeburg University, presented a report entitled The WildList is Dead, Long Live the WildList!. In his report he stresses that all tests based on the WildList collection, including VB100%, have a number of drawbacks because of the content of the collection. First of all, the WildList collection only includes viruses and worms for the Windows platform. Other types of malicious programs (Trojans, Backdoors) and malicious programs for other platforms are not considered. Secondly, the WildList collection contains quite a small number of malicious programs and is updated rather slowly – only a few dozen new viruses are added to the collection per month, while the AV-Test collection is replenished with tens and even hundreds of thousands of new malicious programs.

This only proves that the WildList collection is out of date and does not represent the real “virus” situation on the Internet. Consequently, according to Andreas Marks, tests based on the WildList collection are becoming less and less relevant. They are very good for the promotion of the products that pass them, but they do not indicate the real protection level of antivirus programs.

From the WildList to bigger collections

Independent research laboratories such as AV-Comparatives and AV-Tests do not only criticize; twice a year they test antivirus programs to assess their on-demand detection level. The collections used in their tests usually include up to a million malicious programs that are constantly being updated. The results of the tests can be found on the web sites of the labs (www.AV-Comparatives.org, www.AV-Test.org) and in computer magazines such as PC World, PC Welt, etc. The results of the August tests are given below.



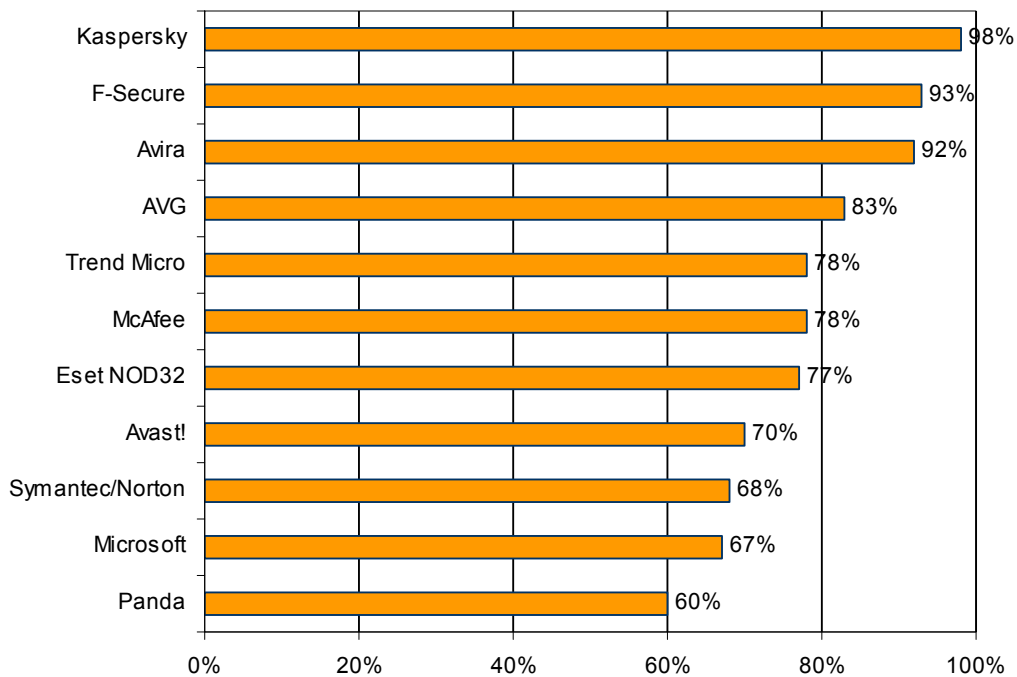
If we consider the most popular products on the Russian market, Kaspersky Lab and Symantec solutions rank among the three leaders. The third is Avira, but we will discuss it later in the chapter devoted to false positives.

Simulating user activities

The tests performed by the AV-Comparatives and AV-Test research laboratories, like any other tests, have their pros and cons. Among the advantages are the extensive collections of malicious programs which are used for testing. They include a wide range of all types of malicious malware. However, these collections do not only contain “fresh” malicious programs but relatively old ones collected over the last 6 months. In addition, these tests analyze the results of on-demand scanning of a hard disk, while in reality a user receives malicious files when downloading from the Internet or in email attachments. Even more importantly, these files must be detected the moment they are launched on the user’s computer.

One of the oldest British computer magazines PC Pro has attempted to overcome these problems. The publication used a collection of malicious programs detected in the traffic that passed through the server of the company MessageLabs two weeks before testing (MessageLabs offers services for the filtering of different types of traffic and its collection reflects the real-life distribution of computer infections throughout the Internet). Moreover, the PC Pro team did not only scan infected files but simulated user activities, e.g., email messages with infected files attached were downloaded to a computer with the installed antivirus program, or infected files were downloaded from the web server with the help of special scripts. These tests were very close to a real-life environment and this could not but influence the results – the detection level of most antivirus programs was significantly lower than in the on-demand tests performed by AV-Comparatives and AV-Test. The most important aspect of such tests is the response time of the antivirus developers to an outbreak of new malicious programs and the proactive mechanisms that they use for detecting them.

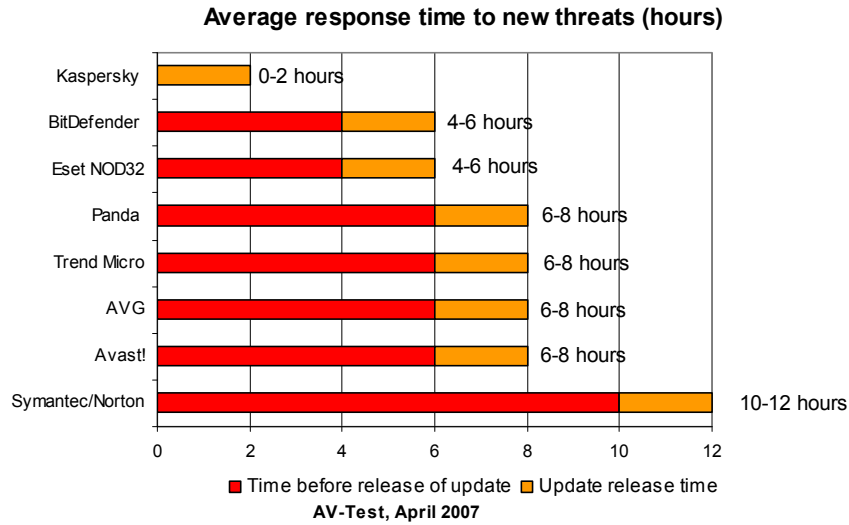
Detection of malicious software, simulating user activities



PC Pro, July 2007

Rapid response team

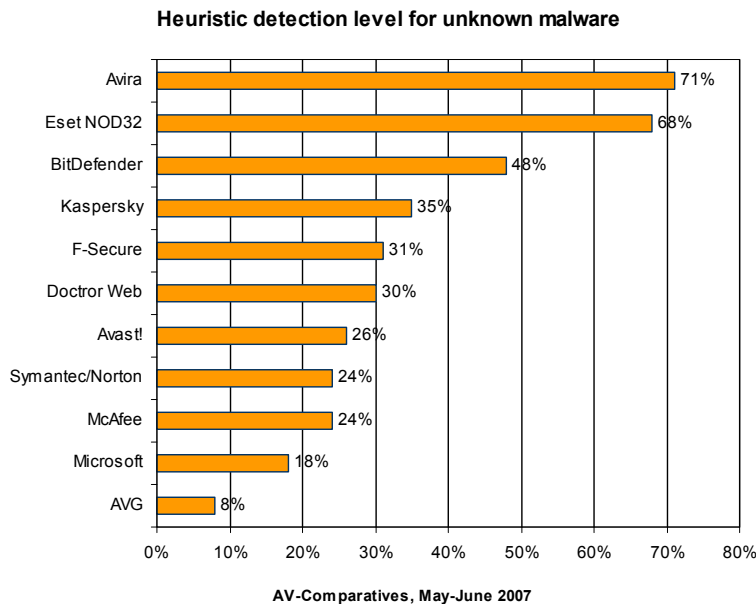
The new threat response time, i.e., the time antivirus vendors need to release an update with the signatures of new malicious programs is an important part of effective antivirus protection. The shorter the interval between updates, the shorter the period users remain unprotected. In April 2007, at the request of the US magazine PC World, the AV-Test team studied new threat response time and received the following results:



Knowing the unknown

Today's new malicious programs appear so quickly that antivirus laboratories hardly have time to respond. In this context an antivirus solution should be able to counteract not only known viruses but new threats which do not yet have signatures. Technologies used to detect unknown threats are called proactive protection. Proactive protection can be broken down into two basic technologies: heuristic analyzers, which detect malicious programs based on an analysis of their code, and behavior blockers, which block the activity of malicious programs based on their behavior.

The effectiveness of heuristic analysis has long been studied by the AV-Comparatives team under the guidance of Andreas Klementy. During tests antivirus programs with three-month-old signatures scan the latest virus collections. The antivirus program therefore has to be able to counteract malware that it has no knowledge of. The antivirus program scans a collection of malicious malware on a hard disk to test the effectiveness of the heuristic analysis. The other proactive technology – behavior blocker – is not enabled in these tests. The diagram shows that even the best heuristic analyzers can only produce a 70% detection level. Many of them, as we will see later, are prone to false positives while scanning clean files. This suggests that nowadays heuristic analysis as a proactive detection method can only be used in combination with the signature method.



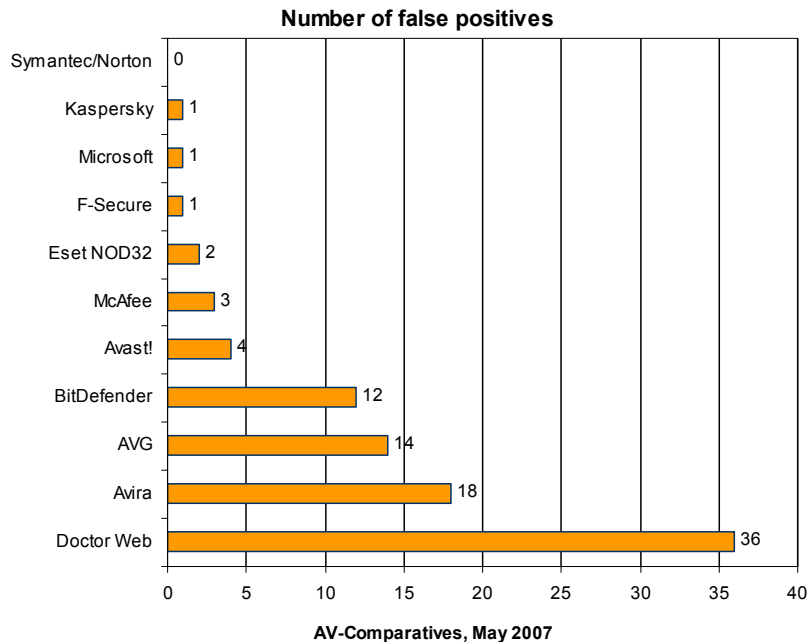
No comparative analyses have been performed for behavior blockers, the second type of proactive technology. First of all, in many antivirus programs (Doctor Web, NOD32, Avira and others) this feature is unavailable. Secondly, performing such tests is not as straightforward as scanning a disk with a collection of malicious programs. Testing the effectiveness of behavior blockers requires the downloading of malware on to a computer and observing how successfully the antivirus program blocks its activity. This process is time-consuming and very few researchers are capable of performing such tests. Only the results of several product tests performed by the AV-Comparatives team are available to the general public today. The antivirus programs that successfully detected and blocked hostile objects as they were launched on the computer were awarded the Proactive Protection Award. At the current time, the Kaspersky Anti-Virus solution with its proactive defense module and F-Secure's DeepGuard behavior technology have been awarded the Proactive Protection Award.

Protection technologies that detect malicious programs based on their behavior are gaining popularity and the lack of comparative analyses in this sphere is rather alarming. However, following the Virus Bulletin 2007 Conference held recently by the AV-Test research laboratory, where the issue attracted a lot of attention from antivirus developers, there is now hope that such testing will begin. The discussions resulted in new methods being devised to test antivirus products in terms of their capability to resist unknown threats. The details of the procedure will be presented in November at the Association of anti-Virus Asia Researchers Conference in Seoul.

False positives are worse than viruses

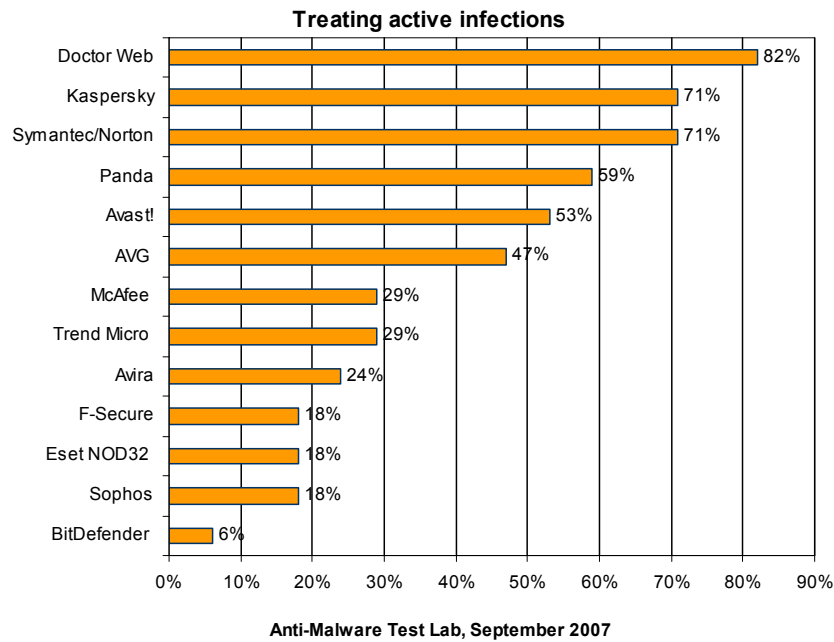
A high malware detection level is one of the most important features of an antivirus program. But just as important is the number of false positives. False positives can cause damage equivalent to a virus infection by blocking program operations, access to web sites, etc. Unfortunately, false positives are all too common. For example, after a database update in September 2007 the AVG antivirus program began to "recognize" Adobe Acrobat Reader 7.0.9 as the SHueur-JXW Trojan program. Another example in June 2007 involved the NOD32 antivirus program which informed users it had detected the Tivso.14a.gen Trojan program when faced with banners served by serving-sys.com on popular sites such as Yahoo, MySpace and other predominantly news-oriented portals.

As well as assessing the capabilities of antivirus programs to detect malicious malware, the AV-Comparatives research team tests for false positives in collections of clean files. As the diagram below shows, Dr. Web and Avira struggle most with false positives.



Treating the uncaught

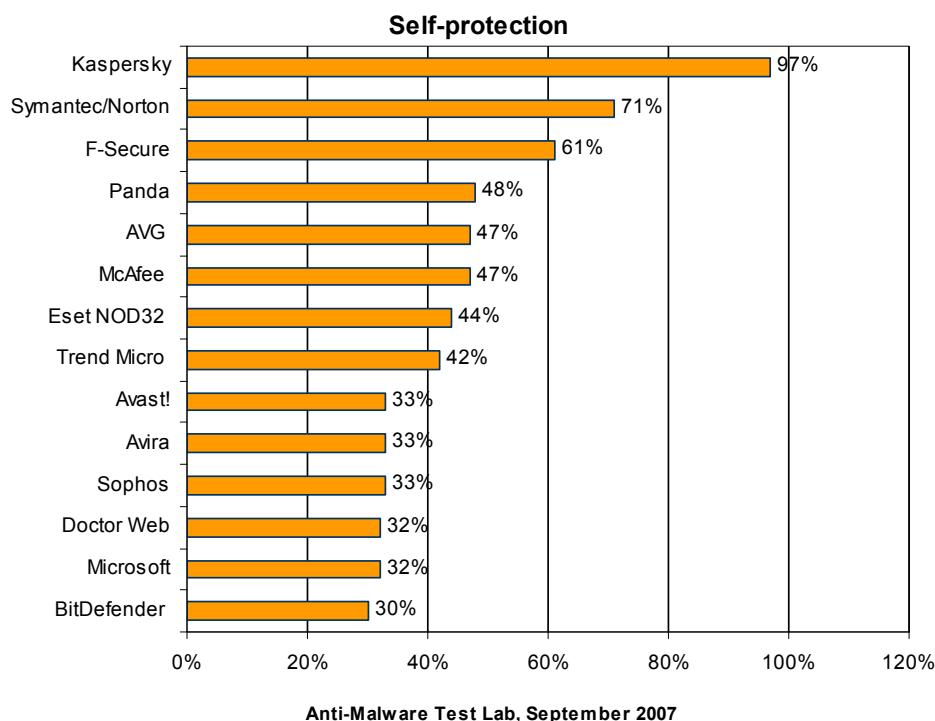
Unfortunately, no antivirus developer can guarantee 100% antivirus protection. From time to time users have to face a situation when malicious programs penetrate their computers and infect them. This happens either because no antivirus program is installed on the computer or because the installed program has failed to detect a malicious program using signatures or with the help of proactive methods. In this situation it is important to detect and to treat an active infection as soon as the signature database is updated. It is also necessary to understand that virus writers keep perfecting their software. Some malicious programs are very hard to remove from the computer because they use various methods to mask their presence in the system (including via rootkits) and to avoid detection and removal by antivirus programs. In addition, just detecting and to treating an infected file is not enough; it is also necessary to eliminate the changes made by a malicious program (for example, changes to the registry) and to restore operability of the system. I know only one group of researches which performs active infection treatment tests and that is the team at Anti-malware-test.com. Their last test was performed in September 2007 and the results are displayed in the diagram below.



Self-protection

The battle between viruses and antivirus programs is becoming more and more like a personal feud with malware increasingly being developed to deliberately resist antivirus protection measures. Viruses now include algorithms to disable antivirus protection or disrupt operability. As a consequence, contemporary antivirus products need to be able to counteract such attacks, i.e., they need to have a self-protection function. This helps them to resist even the most complicated attacks, when malicious programs use a variety of methods to disable protection. The Anti-Malware Test Lab research team has performed a test to analyze the self-protection capabilities of different antivirus solutions.

The testing of the self-protection capabilities was conducted manually or by using specially developed utilities to imitate attacks. After each attack, the antivirus product was verified to ensure proper functioning (including individual modules, active processes, services and drivers).



Combined results

We have now discussed various approaches to testing antivirus programs. We have also described the parameters of antivirus programs that are usually tested. It is now clear that all antivirus solutions have their strengths and weaknesses. It is quite natural that in their promotional materials antivirus vendors name only those tests in which their products occupy the leading positions. For example, Kaspersky Lab stresses its response time to new threats, Eset focuses on its heuristic technologies, and Dr. Web emphasizes its advantages when treating active infections. But how can the end-user make the right choice?

This article aims to help the end-user make the right choice. The results of various tests have been used to provide the most comprehensive picture of the antivirus solutions. Obviously, the solution that the end-user chooses needs to be well-balanced and rank among the leaders for most of the tested parameters. For a fuller picture, the table below shows which ranking the different solutions got in the various tests, as well as a combined score that shows the average ranking for all the tests. The average is calculated only from those tests in which the product participated. As a result, the leaders are Kaspersky Lab, Avira, and Symantec.

Product Rankings for all Tests

	VB100% awards	Antivirus detection AV-Test	Antivirus detection, AV-Comparatives	Detection in real-life environment, PC Pro	New threat response time, AV-Test	Heuristic detection level, AV-Comparatives	False positives, AV-Comparatives	Treatment of active infection, Anti-Malware	Self-protection, Anti-Malware	Average
Kaspersky	2	3	3	1	1	4	2	2	1	2.11
Symantec /Norton	2	7	2	9	4	8	1	2	2	4.11
Avira	5	2	1	3	-	1	8	7	8	4.38
F-Secure	6	4	6	2	-	5	2	8	3	4.50
Eset NOD32	1	10	5	7	2	2	3	8	6	4.89
AVG	4	6	4	4	3	11	7	5	5	5.44
BitDefender	7	1	7	-	2	3	6	9	10	5.63
Avast!	3	5	8	8	3	7	5	4	8	5.67
McAfee	2	11	9	6	-	9	4	6	5	6.50
Sophos	3	9	-	-	-	-	-	8	8	6.67
Trend Micro	9	14	-	5	3	-	-	6	7	7.33
Panda	11	13	-	11	3	-	-	3	4	7.50
Doctor Web	8	12	11	-	-	6	9	1	9	8.00
Microsoft	10	8	10	10	-	10	2	-	9	8.43

**Average antivirus rating for all tests
(The lower the score, the higher the ranking)**

