

White Paper

The Contemporary Anti-Virus Industry and Its Problems

by Eugene Kaspersky
Head of Research & Development

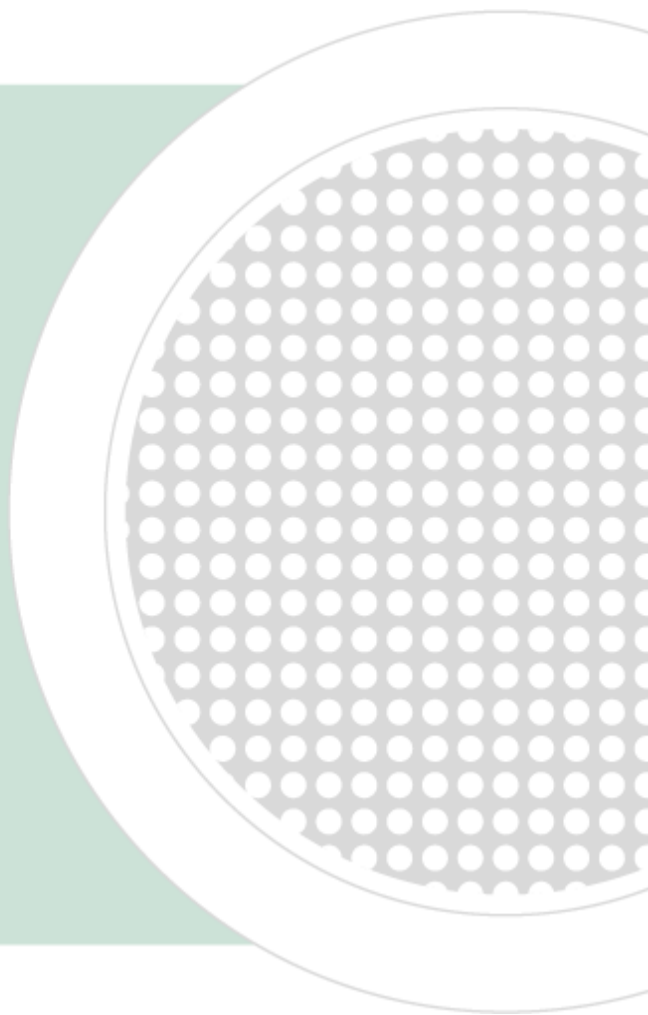


Table of Contents



The Broadening Scope of Virus Threats.....	1
The Anti-Virus Industry and Its Players	2
Problems Faced by the Anti-Virus Industry.....	4
The Feverish “Virus Arms Race”	5
The Lag in Anti-Virus Updates.....	6
Deleting Malicious Code from Compromised Machines	6
Managing Resource Usage.....	6
Incompatibility Between Anti-Virus Programs	7
New Technologies vs. Traditional Solutions	7
The Limits of Comparative Testing.....	9
Arming Yourself with Information.....	10

The Broadening Scope of Virus Threats

The Internet today is a breeding ground for criminal activity. Home users, small and medium businesses, international corporations and governmental bodies all suffer from constant attacks by viruses and Trojans – the reason why is a topic of continual discussion. In any case, it is clear that the Internet is a fertile environment for criminals seeking to profit from malicious programs that:

- steal personal and corporate bank account information;
- steal credit card numbers;
- conduct DDoS attacks, with the instigators then demanding money to stop the attacks (a cyber racket);
- create networks of Trojan proxy servers that can be used to send spam and for other commercial gain;
- create “zombie” networks that can be exploited in multiple ways;
- create programs that download and install adware on victims’ machines; and
- install Trojan dialers that repeatedly call pay services.

It's difficult to say exactly how widespread this criminal activity is. There are dozens, if not hundreds, of hacker groups and individual hackers active in the computer underground. According to the law enforcement agencies of most computerized countries, the number of hackers belonging to groups is estimated in the thousands. Over the last few years, several dozen hackers and hacker groups have been arrested, and the total number of arrests has topped several hundred. However, this doesn't seem to have had any real effect on the number of active viruses and Trojans.

Another figure, which can only be guessed at, is the total cash flow generated by the computer underground. Published sources estimate that, between 2004 and 2005, hackers either stole or scammed several hundred million dollars. As the vast majority of cyber criminals have not been arrested or imprisoned, we can assume that the annual gross is probably billions of dollars (This may well exceed the annual revenues of anti-virus companies. See below for relevant figures).

The total damage done to the world economy by the activity of virus writers, hackers and spammers has recently exceeded tens of billions of dollars annually, and this figure continues to grow. Research conducted by Computer Economics puts total 2004 losses at close to \$18 billion, with a trend towards a 30 - 40% annual growth rate.

The total damage done to the world economy by the activity of virus writers, hackers and spammers has recently exceeded tens of billions of dollars annually, and this figure continues to grow.

Let's take a look the world of cyber threats:

- Virus writers and hackers are creating and distributing viruses and Trojans for many reasons.
- End users' machines and networks are under constant threat of hacker attacks, and they may also often fall victim to coordinated attacks.
- Police and law enforcement bodies throughout the world are only partially successful in investigating and prosecuting cyber crimes.
- Anti-virus companies create software to counteract cyber threats.

There has been a great deal written about viruses and hackers, as well as about those who hunt them down - there have even been Hollywood films on the subject. The developers and vendors of anti-virus solutions use their web sites to publicize their achievements. However, there isn't much information about the problems faced by the anti-virus industry. This white paper aims to address this topic and, to some extent, rectify the imbalance.

The Anti-Virus Industry and Its Players

Let's take a look at the companies manufacturing standard solutions that protect against computer viruses (We'll discuss dedicated solutions and tools later in the white paper). "Standard solutions" include software for desktops, file servers, mail servers and the perimeters of corporate networks.

The total market for standard solutions was estimated at \$2.7 billion in 2003 and \$3.3 billion in 2004, with \$3.8 billion being predicted for 2005 (All information in this section is taken from IDC, 2005). All anti-virus manufacturers are divided into three groups: industry leaders, second tier companies and others (i.e., those which have minimal effect, if any, on the anti-virus landscape).

The industry leaders include Symantec, McAfee (NAI) and Trend Micro.

Company	Annual Revenue, \$M	
	2003	2004
Symantec	1098	1364
McAfee (NAI)	577	597
Trend Micro	382	508

These three companies occupy leading positions in all markets, with a few exceptions. Symantec and NAI (McAfee) are North American organizations. Trend Micro, which dominates the Japanese market, was originally a Taiwanese company that was floated on the Japanese stock market and is currently headquartered in the U.S.

The second tier includes companies with significantly lower revenues than the leading three. However, these companies still have annual revenues of tens of millions of dollars:

Company	Annual Revenue, \$M	
	2003	2004
Sophos (UK)	97	116
Panda Software (Spain)	65	104
Computer Associates (US)	61	74
F-Secure (Finland)	36	51
Norman (Norway)	23	31
AhnLab (South Korea)	21	28
*Panda Software is a private company. Financial information is not audited.		

Kaspersky Lab, based in Russia, is also included in this group. However, the company does not disclose financial information.

The majority of second-tier companies have a significant presence in their respective domestic markets, but a relatively small presence in foreign markets. For instance, Sophos is most successful in the UK, Panda in Spain, F-Secure in Scandinavian countries, etc.

The third group includes several dozen anti-virus companies. The best-known companies and products include:

- Alwil - Awast (Czech Republic)
- Arcabit - MKS (Poland)
- Doctor Web - DrWeb (Russia)
- ESET - NOD32 (Slovakia)
- Frisk Software - F-Prot (Iceland)
- GriSoft - AVG (Czech Republic)
- H+BEDV - AntiVir (Germany)
- Hauri - VI Robot (South Korea)
- SoftWin - BitDefender (Romania)
- VirusBuster - VirusBuster (Hungary)

The third group also includes UNA and Stop! (both Ukraine), Rising and KingSoft (both China), and others.

The majority of companies in this group do not disclose any financial information. However, some estimates state that this group's annual revenues are around \$10 million per organization.

The information above provides a market share breakdown for a number of anti-virus companies. However, companies offering products based on licensed technologies aren't included. Examples include G-Data (a German company with an anti-virus solution based on that from Kaspersky Lab), SoftWin technologies and Microsoft (which offers a multi-engine solution developed by Sybari).

There are also some non-standard types of anti-virus protection, some of which are relatively specialized. These include systems that delete any potential threat from corporate email messages (i.e., the end user receives only messages without executable attachments or HTML scripts), systems that launch the web browser within a virtual machine, and others. There are also some programs that are fairly similar to anti-virus solutions, such as software that protects against DDoS attacks and patch management software. However, none of these can be considered fully functional anti-virus products.

Problems Faced by the Anti-Virus Industry

What problems does the anti-virus industry face, aside from the typical headaches encountered by any manufacturer of consumer goods? To many, it might seem that anti-virus solutions are standard consumer products, with one solution barely differing from the next. As just another consumer product, an anti-virus solution would be selected by consumers based simply on its design, its marketing or and/or other non-technical characteristics.

Unfortunately (or perhaps fortunately) this is not the case. Users often chose an anti-virus solution for its technical characteristics, which can differ widely between products. In addition to evaluating a product's overall level of protection, users often focus on whether or not a specific product protects against a specific type of cyber threat.

The better an anti-virus solution is at protecting against all types of malicious programs, the more satisfied users and system administrators will be. The hard truth is that it only takes a single virus to do a lot of damage, compromising personal data, passwords and other sensitive information. Given this, users should look critically at the level of protection offered by an anti-virus solution, so they can make an informed choice that will provide an optimal level of security.

Let's say that anti-virus solution X detects 50% of all viruses currently circulating on the Internet, and products Y and Z detect 90% and 99.9%

The hard truth is that it only takes a single virus to do a lot of damage, compromising personal data, passwords and other sensitive information.

respectively. N number of attacks will result either in the computer's integrity being maintained or in the system becoming infected. If the computer is attacked 10 times, then the likelihood of product X failing to detect a malicious program is virtually guaranteed; product Y is more than likely to fail to detect the culprit; and, in the case of product Z, the danger is almost infinitesimal.

Unfortunately, there are relatively few products available that offer even close to 100% protection. The majority of products are unable to guarantee even 90% protection. This is the largest problem encountered by the anti-virus industry today.

Many products marketed as “anti-virus solutions” shouldn't really be called this at all.

The Feverish “Virus Arms Race”

The number and variety of malicious programs is increasing every year. Many anti-virus companies are simply unable to cope with the onslaught and are therefore losing the “virus arms race.” Unfortunately, this means that increasing numbers of anti-virus users become exposed to a growing population of malicious programs. Consequently, many products marketed as “anti-virus solutions” shouldn't really be called this at all.

It wasn't long ago that an anti-virus solution didn't need to protect systems against every new virus and Trojan, as early versions of malicious programs were often unable to penetrate a user's computer. Most were written by adolescent cyber vandals, who sought either to show off their coding skills or to satisfy their curiosity. Users therefore only needed protection against the few “in-the-wild” viruses that could actually penetrate target machines.

Today, more than 75% of malicious programs are created by the criminal computer underground - most all seeking to infect computers via the Internet. The number of new viruses and Trojans is now increasing by a few hundred every day. The Kaspersky Virus Lab currently receives between 200 and 300 new samples a day.

Kaspersky receives sample viruses from several sources, including honeypots (dedicated machines used to collect malicious files on the Internet), users of infected machines, local network administrators and ISPs – as well as from other anti-virus companies. Despite market segmentation in the anti-virus industry, anti-virus companies often collaborate with one another. If a new worm that propagates quickly is detected by one anti-virus company, the company usually informs its competitors almost immediately. The majority of anti-virus companies exchange virus samples at least once a month. They also exchange information at dedicated professional gatherings.

When a new virus or Trojan is detected in the wild, either on the Internet or on an infected computer, it's likely that hundreds or thousands of other

computers on the Internet are already infected. If the latest “beastie” is a network worm, then the number of victims could be in the millions. Consequently, anti-virus companies must be able to release rapid updates to anti-virus databases, and these updates must include protection against all of the newest viruses and Trojans.

The Lag in Anti-Virus Updates

Today, malicious programs propagate so quickly that anti-virus companies must release updates as quickly as possible to minimize the amount of time that users will potentially be at risk. Unfortunately, many anti-virus companies are unable to do this, and users often receive updates only after their computers are already infected.

Let's assume that a virus manages to penetrate a target machine, and the user's anti-virus solution doesn't detect any suspicious activity – perhaps because of the quality of the solution itself or because the user has not downloaded the latest updates. While the user may eventually acquire an update that detects the virus, the update may not necessarily defeat the virus. To get rid of the virus once and for all, the infected files have to be carefully deleted from the machine.

Deleting Malicious Code from Compromised Machines

The third problem faced by the anti-virus industry is deleting malicious code from compromised machines. Viruses and Trojans are often designed to evade detection and/or to penetrate a system so deeply that deleting them is a complex task. Unfortunately, some anti-virus programs are unable to delete malicious code and restore modified data without causing further problems.

An additional issue is that all software consumes system resources, and anti-virus programs are no exception. To protect the computer, the anti-virus program has to perform certain actions, such as opening and reading files and archives. The more thoroughly a file is checked, the more resources are required by an anti-virus solution. In this way, the anti-virus solution is similar to a security door: the thicker the door is, the more protection it will offer; however, the heavier the door is, the more difficult it is to open and close. Therefore, anti-virus solutions are constantly challenged to balance program speed against level of protection.

Managing Resource Usage

The issue of resource usage is almost insoluble. Experience shows that anti-virus solutions that offer rapid scanning are heavily flawed, letting viruses and

Today, malicious programs propagate so quickly that anti-virus companies must release updates as quickly as possible to minimize the amount of time that users will potentially be at risk.

Trojans through like water through a sieve. However, anti-virus programs that run slowly do not necessarily offer effective protection.

To scan files on-the-fly and provide constant protection for the computer, an anti-virus solution must penetrate relatively deeply into the kernel of the system. It will always penetrate the same levels. Technically speaking, to successfully scan intercepted files, network packets and other potentially dangerous objects, the anti-virus program has to install interceptors of system events deep inside the protected system and transmit the results to the anti-virus engine.

However, sometimes it's simply not possible to install two interceptors in a necessary kernel level of the operating system. The result is incompatibility between the anti-virus monitors (which function constantly), as the second anti-virus will either be unable to intercept system events, or the attempt to duplicate the interception mechanism will lead to system crash.

Incompatibility Between Anti-Virus Programs

Incompatibility between anti-virus programs is an issue because, in the vast majority of cases, installing two anti-virus programs from different vendors on one machine (i.e., for increased protection) is technically impossible, as the two programs will disrupt each other's functioning.

People often think that anti-virus companies act like toddlers snatching at each other's toys, and that the incompatibility issue is the result of unfair competition designed to squeeze other manufacturers out of the market. While unfair and unethical competition does occur, it is not the norm. On the contrary, developers make every effort they can to ensure that their product does not conflict with other popular software (including anti-virus solutions).

New Technologies vs. Traditional Solutions

From time to time, anti-virus companies pursue quintessentially new technologies in their quest to develop a universal panacea that addresses the above problems in a single stroke.

A solution offering proactive protection would make it possible to detect an emerging virus and delete it prior to the virus actually being created and appearing on the Internet. However, a “universal” solution is only effective against threats that act in accordance with constant, well-defined rules. Because computer viruses manifest from the intricate workings of hackers' minds, they are not subject to any fixed rules. Rather, viruses abide by sets of rules that constantly change in accordance with the goals of the computer underground.

People often think that anti-virus companies act like toddlers snatching at each other's toys, and that the incompatibility issue is the result of unfair competition designed to squeeze other manufacturers out of the market.

Consider the example of the behavior blocker, which competes with traditional anti-virus solutions. Behavior blockers and anti-virus solutions scan for viruses using two completely different approaches (that are not necessarily mutually exclusive). A traditional anti-virus solution detects infections by leveraging virus signatures, which it compares to files on the user's computer, checking for identical matches. A behavior blocker tracks applications as they launch and terminates any programs exhibiting signs of suspicious or known malicious behavior. Both methods have their advantages and disadvantages.

One benefit of an anti-virus signature scanner is that it detects all malicious code that it recognizes. However, it fails to detect malicious code that it hasn't encountered before. Another potential issue is the large size of anti-virus databases and the resources they consume. On the other hand, behavior blockers are able to detect even unknown malicious programs. However, these solutions tend to generate false positives, since today's viruses and Trojans behave so diversely that devising a single set of rules is simply impossible. Behavior blockers can therefore fail to detect some malicious programs, while periodically preventing legitimate applications from functioning.

Behavior blockers have another inherent disadvantage in that they are unable to combat conceptually new malicious programs. Imagine that Company X develops a behavioral anti-virus AVX that detects 100% of current malicious programs. As hackers continually invent new types of malicious programs, it becomes necessary to update the product's behavioral rules on a regular basis. At the end of the day, the behavior blocker essentially becomes a signature scanner that leverages behavioral signatures rather than pieces of code.

This conclusion also applies to the heuristic analyzer, another proactive protection method. As hackers learn that new technologies are preventing them from reaching their victims, they quickly invent new virus technologies to evade proactive detection - thereby rendering advanced heuristics and/or behavior blocking products ineffective.

“Reinvented” proactive technologies are therefore effective only for a relatively short length of time. Where junior hackers require a few weeks or a couple of months to get around proactive protection, professional hackers may need one or two days (or, in the worst cases, a few minutes or hours). This means that both behavior blockers and heuristic analyzers, however effective they may be, require constant development and updating. It should also be noted that adding new signatures to an anti-virus database takes a matter of minutes, whereas perfecting and testing proactive protection methods takes much longer. The result is that, in many cases, signature updates to anti-virus databases are far better than the average proactive protection solution. This theory continues to be proven with the spread of

In many cases, signature updates to anti-virus databases are far better than the average proactive protection solution.

new epidemics of email and network worms, spy programs and other types of malicious code.

Of course, this doesn't mean that proactive protection is useless. It functions well within specific boundaries and is capable of stopping a certain amount of malware (i.e., programs created by less experienced hackers and virus writers). For this reason, proactive protection solutions complement signature scanners, but they should not be relied upon to provide total protection.

The Limits of Comparative Testing

In their search for an effective anti-virus solution, many users review comparative test results from various sources. However, not many professional sources exist. Most IT publications conduct comparative tests of anti-virus solutions on a fairly regular basis, evaluating everything from a product's price to the quality of its technical support. However, these tests don't really prove the quality of the anti-virus function. To effectively evaluate an anti-virus product, a tester needs a fairly large virus collection as well as test stands and automated testing procedures. A dedicated group is usually required to thoroughly test anti-virus solutions - something that most IT publications don't have. Comparative tests conducted by IT publications therefore either leave much to be desired or rely on third-party experts who specialize in testing anti-virus products.

Currently, the most experienced testers of anti-virus products are Andreas Marx (Germany <http://www.av-test.org>) and Andreas Clementi (Austria <http://www.av-comparatives.org>). These reports describe in detail the quality of detection of various types of malicious programs and the speed at which different anti-virus companies react to epidemics. In addition, the tests can be used to compare the characteristics of different anti-virus solutions. However, these tests are limited in that they only examine the two characteristics described above. They do not address issues regarding how an anti-virus solution cleans infected systems under real-life scenarios, how the solution reacts to infected web sites, the amount of resources it consumes, or the thoroughness with which it checks archives and installers.

Tests that provide in-depth, accurate pictures of how products react in typical situations barely exist. The one exception that we know of is the Test Lab at Moscow State University, which conducts tests using a fairly wide range of situations. However, their methodology still needs improvement, and the University's test lab is not yet known to the public at large.

Also notable are the tests conducted by VirusBulletin, an industry publication. However, VirusBulletin's tests are far from perfect, because its testing standards were developed in the mid-1990s and have barely changed since then. Anti-virus products are tested using a collection of files infected by ITW

Tests that provide in-depth, accurate pictures of how products react in typical situations barely exist.

viruses. The publication's VB100% award is given on the basis of the test results. However, the ITW collection only contains between two and three thousand files - fewer malicious programs than appear in the wild in the space of a single month. Therefore, a VB100% award doesn't necessarily mean that a product really provides protection against all types of malware. It simply means that the product copes well with VirusBulletin's ITW collection and nothing more.

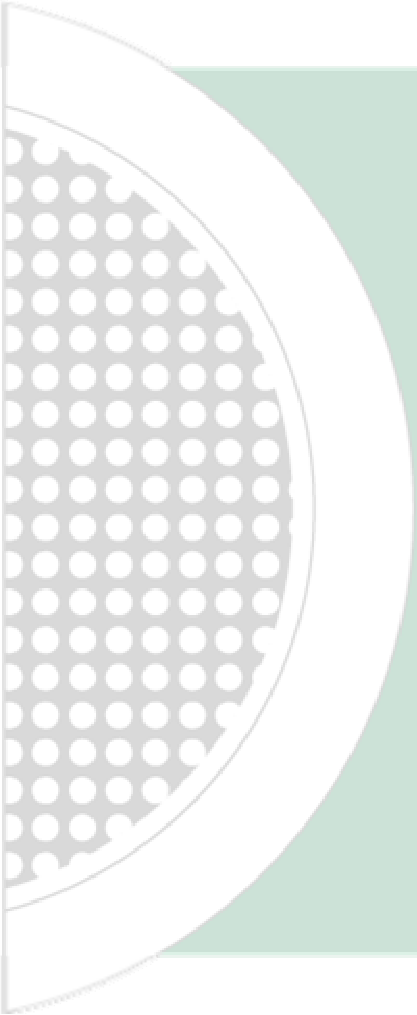
Arming Yourself with Information

You should now have a better understanding of the issues faced by the anti-virus industry and the factors to consider when selecting an anti-virus solution for your home computer or network. Any computer that is connected to the Internet can be safe or unsafe. Either way, arming yourself with information about virus risks and protective measures is critical to maintaining the integrity of your computer and the information it contains. Happy surfing!



Kaspersky Lab, Inc. • 300 Unicorn Park • Woburn, MA 01801
phone: (781) 503-1800 • fax: (781) 503-1818
www.kaspersky.com

About Us



At Kaspersky Lab, we produce and distribute information security solutions that protect our customers from IT threats and allow enterprises to manage risk. We provide security software products that protect information from all types of malware including viruses, hackers and spam for home users and enterprises and offer consulting services and technical support.

Founded in 1997, Kaspersky Lab is an international information security software vendor. Kaspersky Lab is headquartered in Moscow, Russia and has regional offices in the UK, France, Germany, the Netherlands, Poland, Japan, China, and the United States. Further expanding the company's reach is its large partner network comprising over 500 companies globally.

Learn more at www.kaspersky.com