



Kaspersky Anti-Virus

Detecting spyware & other non-viral
potentially hostile programs



Contents

INTRODUCTION	3
1. DETECTING POTENTIALLY HOSTILE PROGRAMS	4
2. SPYWARE.....	6
3. MALWARE-RELATED 'RISKWARE' PROGRAMS	8
4. MALWARE-RELATED 'PORNWARE' PROGRAMS	10
5. ADWARE	10
6. OTHER MALWARE-RELATED PROGRAMS	11
TECHNOLOGY INTEGRATION.....	12
REFERENCES:	12

Introduction

The Kaspersky® anti-virus engine – the heart of all Kaspersky anti-virus product family, delivers a unique combination of technologies necessary to successfully find and remove all kinds of malicious objects, or ‘malware’. The engine is designed to successfully detect any program that is deliberately created to perform an unauthorized, often harmful, action. This includes not only viruses, worms, Trojans, but also malware-related programs such as spyware, adware, pornware applications, etc.

Virus detection capabilities of the Kaspersky Anti-Virus engine are reviewed in more detail in separate documents¹ available at Kaspersky Lab. This document focuses on additional outstanding capabilities of the Kaspersky anti-virus engine to detect non-viral categories of malware, such as spyware, adware, pornware and other types of undesired content.²

1. Detecting potentially hostile programs

During the last few years there has been a growth in the number of potentially hostile malware-related programs that can be used by criminals to attack users or hijack their machines for malicious purposes. This includes spyware, adware and malware-related 'riskware' and 'pornware' applications. Such programs are not referred to viruses and can not be defined as malware *per se*. In fact, they may be legitimate applications. But their potential for misuse by hackers and other cyber criminals means that users increasingly see them as undesirable applications and need the means to identify them.

Detection of potentially hostile programs is especially important for enterprises, since such applications can bring significant security and legal risks. This includes the following:

- Financial losses that result from theft of confidential corporate information.
- Reduced computer performance and lower employee productivity.
- Increased risk of legal liability.
- Increased remote access costs.

Kaspersky Lab has a long history in detecting and removing Trojan spyware programs. This goes back to 1996 when Kaspersky Lab included detection and removal for the first AOL password stealing Trojans. Today Kaspersky anti-virus products can boast a consistent track record in independent tests for detection of Trojans and other malware³.

Results over Backdoors, Trojans and other malware detection

Kaspersky Lab	99.2%
Symantec	94.5%
McAfee	90.5%
NOD32	90.0%
Dr.Web	87.1%
H+BEDV	86.1%
BitDefender	82.8%
TrendMicro, F-Prot	81.4%
Avast	76.2%
RAV	75.2%
AVG	70.0%
Sophos	67.4%



February, 2005

www.av-comparatives.org

Kaspersky Lab delivers exceptional levels of detection for malicious and potentially hostile programs, as indicated in a spyware detection test conducted by the German magazine *Computer Bild* in July 2005.

Although Kaspersky Anti-Virus Personal 5.0 is not a spyware-only solution, it was included in the test for comparative purposes. In spite of this, the program had the highest spyware detection rate, detecting over 90% of spyware in the test - and was consequently ranked first. The review noted that detection rates for other malicious programs (Trojans, backdoors,

keyloggers and browser hijackers) were even higher at 99%. The review concluded that Kaspersky Anti-Virus 5.0 with Maintenance Pack 3 not only provides advanced protection from viruses, but also excellent protection against spyware.

Results over Spyware protection

Kaspersky Anti-Virus	92.65%
Webroot, Spy Sweeper	84.15%
CA, E-Trust Pest Patrol	73.27%
Lavasoft, Ad-Aware SE	51.77%
BHV, Spionage-Abwehr	43.1%
Emsi Software, A-Squared	43.1%
Spybot Search & Destroy	38.03%
Tenebril, Spy Catcher	33.47%



Spyware

July, 2005

www.computerbild.de

In addition, Kaspersky Anti-Virus Personal recently passed certification tests carried out on the Microsoft Windows XP platform by the international research center West Coast Labs in its 'Spyware' protection category, and now holds the Spyware Checkmark certificate.⁴

The Kaspersky anti-virus engine delivers protection from viruses, worms and Trojans by default, using its standard databases. This includes malicious, Trojan spyware programs [including Backdoor Trojans and Trojan Spies, Trojan Proxies and Trojan Notifiers]. However, protection from other malware-related programs is provided through the extended databases. The following diagram shows the different categories of program and how Kaspersky Lab provides protection from them.

	MALICIOUS SOFTWARE	POTENTIALLY HOSTILE SOFTWARE
STANDARD DATABASES	Viruses Worms Trojans [including Trojan Spyware]	
EXTENDED DATABASES		Non-Trojan Spyware <ul style="list-style-type: none"> • Adware • Riskware Pornware <ul style="list-style-type: none"> • Dialers • Downloaders Riskware <ul style="list-style-type: none"> • Takes many forms

2. Spyware

In a recent survey of more than 600 North American businesses, IDC lists spyware as the fourth greatest threat to a company's enterprise network security and estimates that 67% of all computers [mostly consumer] have some form of spyware installed⁵.



'Spyware', as the name suggests, is software designed to gather data from a computer and forward it to a third party without the consent or knowledge of the computer's owner. This includes monitoring key strokes, collecting confidential information [passwords, credit card numbers, PIN numbers, etc.], harvesting e-mail addresses or tracking browsing habits. There's a further by-product, of course: spyware inevitably affects network performance, slowing down the system and thus affecting the whole business process.

Some security vendors use the word spyware as an umbrella term to include a wide range of malware-related programs, including Trojan Spies, non-Trojan spyware, adware, 'riskware' and 'pornware'. It's certainly true that some of these different applications share some specific characteristics. Many adware utilities collect and forward information about individual machines and users: this may include IP address, browsing habits, frequently visited web sites, search engine queries and other information that can be used to design a new advertising campaign.

However, at Kaspersky Lab we consider them to be distinct categories of malware-related programs, based largely on the intent of the author or master of the program. So while it's true that spyware and adware may gather data from a computer and forward it to a third party without the consent or knowledge of the computer's owner, each has a different purpose: the aim of a Trojan Spy is to steal financial and other information, while adware is designed to advertise or promote goods or services. The net result for the user may be the same, but the intent is different.

Unfortunately, spyware is something of a grey area. There's no industry standard definition of the term. And while it may be tempting to think of all spyware programs as malicious, it's not that simple. For example, some remote administration tools have the ability to monitor user activity. Such utilities are legitimate in themselves, so they can not simply be flagged as Trojans without risking shouts of protest from the developer of the application, needlessly irritating both the user and developer of these utilities. On the other hand, such tools can be put to misuse by cyber criminals: dropped onto a user's machine by a Trojan Downloader and 'hijacked' by the author or master of the Trojan. It's no surprise, therefore, that demand to include detection for such applications has grown over the last year or so.

The decision to add detection of a program is not always a simple one. Remember that a legitimate remote administration tool and a backdoor Trojan share similar functionality. So how do we decide whether to detect it or not? One key difference is that spyware programs seldom reveal their presence. They may arrive as part of some other package, perhaps a freeware program. Or they may be dropped silently onto the system by a Trojan Dropper or Trojan Downloader. Either way, they install silently and run in the background, hidden from view. Even if the owner of the computer

becomes aware of their presence, such programs don't de-install automatically, as legitimate applications do.

As stated above, if a program with spyware capability is clearly malicious [if, using our definition above, it has been deliberately created to perform an unauthorized, often harmful, action] Kaspersky Lab includes detection in its standard databases.

This is true for a range of different Trojans.

1. Backdoor Trojans and Trojan Spies are designed to steal confidential financial data. Dozens of new variants appear every week, often different in both form and function. Some are simple keystroke loggers that use e-mail to send the captured information to the author or controller of the Trojan. The more elaborate among them provide complete control over victim machines, sending whole data streams to remote servers and receiving further commands from these servers. Victim machines are frequently combined into so-called 'bot' networks, used for the wholesale collection of personal data [passwords, PIN numbers, etc.], to distribute spam e-mail or to launch DDoS [Distributed Denial of Service] attacks.
2. Trojan Proxies install and launch a proxy server on the victim machine [sometimes making use of system vulnerabilities] without the user's knowledge. They then open a port on the victim machine, allowing it to send and receive e-mail: turning the victim machines into an army of spam-spewing 'zombies'.
3. Trojan Notifiers are used to confirm to the master that a machine has been successfully attacked. They typically return information about the victim machine [IP address, open ports, e-mail address] and relay this to the master.
4. PSW Trojans are designed search system files for passwords or Internet access telephone numbers, which are then relayed to an e-mail address coded into the body of the Trojan for retrieval by the 'master'. PSW Trojans also steal other types of information, including system information, IP, address, registration details or online games passwords. The numerous AOL password stealers, which began to appear in the mid-1990s, belong to this group of Trojans.

N.B.: If an application has spyware capability, but isn't malicious by design, detection is added to the extended databases!

Thus Kaspersky Lab protects against ALL spyware. This includes programs deliberately written to access a user's machine without authorization, as well as legitimate applications that have the potential to be misused by cyber criminals. They both share the same technical capability [hence the common category of 'spyware']. However, Kaspersky Lab groups them differently based on the underlying intent of the programmer that created them. Malicious spyware is detected using standard databases; potentially hostile spyware is detected using extended databases.

The use of spyware programs to steal confidential data is symptomatic of a key change in the nature of the threat landscape: its increasing criminalization. And it's clear that this trend will continue as long as it proves successful for the writers of malicious code and those who pay them to create code that can be used to make money illegally. As part of the

transition from cyber vandalism to cyber crime, hackers are focusing more on how they can cover their tracks more effectively, thus maximizing their 'investment'. One way of doing this is by using a rootkit to conceal changes made to the victim machine. Rootkits, which originated in the Unix world, are being used more and more by the authors of Trojans and quasi-legal spyware, to try and prevent detection of their programs. A rootkit is a collection of programs used by a hacker to evade detection while trying to gain unauthorized access to a computer. This is done either by replacing system files or libraries, or by installing a kernel module. The hacker installs the rootkit after obtaining user-level access: typically this is done by cracking a password or by exploiting a vulnerability. This is then used to gather other user IDs until the hacker gains root access to the system.

Detection of rootkits will be further enhanced in Kaspersky Anti-Virus 6: this will include detection of unknown rootkits and restoration of registry settings.

The use of spyware programs to steal confidential data is symptomatic of a key change in the nature of the threat landscape: its increasing commercialization. And it's clear that this trend will continue as long as it proves successful for the writers of malicious code and those who pay them to create code that can be used to make money illegally.

3. Malware-related 'riskware' programs

There are other ways, in addition to spyware, to infiltrate computers. In fact, the computer underground has shown remarkable versatility in 'hijacking' legitimate applications and using them for their own ends. That's what 'riskware' is: any legal program that hackers use to penetrate computers. This makes it tricky to define, because there is no way to predict what types of software might fall into this category: it depends on inventiveness of the computer underground. The intent of the cyber criminals is the key to defining this category of software. Once cyber criminals have identified software that they can misuse, they can download it to a victim machine without the knowledge or consent of the owner and control the victim machine without triggering anti-virus solutions or other security software. Legal software skillfully used for illegal purposes can be extremely difficult to detect.



Here are some of the types of software that can currently be used in this way. Remember that it's not an exhaustive list. The important thing in defining riskware is not the type of program, but the malicious intent of the cyber criminal making use of it.

1. Dialers, as their name suggests, are programs designed to automatically dial a specific telephone number using the computer's modem. They do no direct harm to the machine on which they're installed. But they can have a serious financial impact on the owner of the computer. Although there are legitimate dialers, many are used by web site owners to instruct the host machine to call pay-to-view sites: more often than not pornographic sites. Obviously, the resulting large telephone bill makes dialers unwelcome 'guests' in the eyes of computer and network owners. There are two varieties of dialer, Trojan dialers and legitimate dialers.

Trojan dialers are installed without the knowledge or consent of the user and dial pay-to view sites automatically. Legitimate dialers, on the other hand, inform the user of what calls are being made, and how much the calls will cost. Such dialers can be de-installed using standard procedures. However, they may still be regarded as malicious because the initial installation occurs without the consent of the user, even if they offer the user a chance to decide what action to take later.

2. Downloaders may be malicious, like the many Trojan Downloaders that exist. However, even legal downloading utilities can be dangerous, since they are usually programmed to function in the background, without direct intervention from the user. Moreover, it's easy for a hacker to substitute links to infected resources for safe download sites, causing malware to be downloaded to the victim machine without the user's knowledge.
3. FTP servers are utilities that can be used to gain remote access to files. Once installed on a system by a hacker, it is possible for the hacker to download files from the victim machine automatically, and also to track activity on the victim computer.
4. Proxy servers were originally developed to secure internal networks by separating internal addresses from external users. However, hackers use them to connect anonymously to the Internet: the address of the proxy server is substituted for the hacker's real address.
5. Telnet servers were developed to provide remote access to resources on other machines. Hackers use them to gain full access to victim machines.
6. Web servers provide access to web pages that are located in a defined area of the file system. They are used by hackers to gain full access to the victim machine file system.
7. IRC clients provide access to IRC channels. Many IRC clients, especially mIRC, incorporate powerful script languages that automate the IRC client. This functionality can be exploited to write Trojans and IRC worms. When installing a Trojan IRC program on a victim machine, hackers will often also surreptitiously install an IRC client as well.
8. Monitors are legal utilities that monitor computer and user activity and a number of commercial utilities of this nature exist. Normally information on user activity is saved to disk or sent to a specified e-mail address. However, monitoring programs only differ from Trojan spy programs in not masking their presence in the system and that fact that it's possible to de-install them.
9. PSW tools are used to restore lost passwords. They normally display information about the password on screen or save it to disk. When used by a hacker, this information will be sent to the remote attacker.
10. Remote administration tools are legitimate utilities that allow a network administrator to directly control machines under their supervision. Of course, the same tools provide a hacker with the same full control over victim machines.

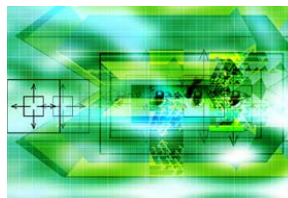
11. Crackers are programs used by hackers to hack different kinds of software. They don't normally have any adverse effect on installed software, being used just to remove copy and/or key protection in protected programs.

12. Bad jokes and hoaxes are programs that do not cause any direct damage to a machine. They typically display fake warnings or alerts about purported damage that has been, or will be, done to the machine. This may include, messages telling users that drives have been re-formatted, that a virus has been found, or that symptoms of infection have been detected. The possibilities are limited only by the so-called 'sense of humor' of the author of the joke or hoax.

Once again, it's important to stress that this is not an exhaustive list and there are other free and commercial programs that may be used by hackers for malicious purposes. Their intent is the key to understanding this category.

4. Malware-related 'pornware' programs

'Pornware' is a generic term used by Kaspersky Lab to group together malware-related programs that either use the computer's modem to connect to pornographic pay-to-view services, or download pornographic content from the web, without the consent of the user.



Such programs may be used legitimately, to provide access to various adult services on the Internet. That's why they are not detected using the standard databases. However, they are open to misuse by cyber criminals. So the extended databases provide detection for the growing numbers of users who need protection from such applications.

This category is clearly related to the dialers outlined above, but refers to those programs designed to access pornographic content specifically.

5. Adware

Adware programs [also referred to as 'AdvWare', 'SpyWare' or 'Browser Hijackers'] are designed to launch advertisements on infected machines and/or to re-direct search engine results to promotional web sites. Adware does not usually show itself in the system in any other way: there are no icons in the system tray and no mention of the files in the program list. Adware seldom comes with any de-installation procedures: unfortunately, attempts to manually remove adware may cause the original carrier program to malfunction.



Adware reached epidemic proportions between 2000 and 2004, for two reasons. First, the widespread use of computers in developed countries made Internet marketing the most inexpensive and effective channel for reaching

reach extensive audiences. Second, spam was declared illegal in many countries, leading spammers to change their methods. If anti-adware laws are also passed in the future, electronic marketing will undergo further changes.

Adware penetrates individual machines using one of two methods.

1. The adware component is built into freeware or shareware programs. In most cases, the adware is automatically de-activated if the software is purchased or registered by the user. Adware designed to download banners from the Internet usually includes ready-made components from other vendors. These adware utilities remain in the system even after the ad campaign is de-activated. Deleting such utilities while the campaign is still running can cause the carrier program to malfunction. Piggyback adware is an indirect charge for using free and shareware: the advertiser pays the ad agency, which pays the adware vendor or developer. Revenue from adware supports freeware and shareware developers, motivating them to write new versions and programs.
2. Adware is secretly downloaded onto the user's machine from infected web sites. In this case hacker utilities of various sorts are the technology of choice. These hacker utilities exploit vulnerabilities in Internet browsers or use Trojans [either Trojan Droppers or Trojan Downloaders] to pull down adware code. This category of adware is often referred to as 'Browser Hijackers', since such programs subvert the web browser in order to install software [in this case adware] without the knowledge or consent of the user. Browser Hijackers may change browser settings, re-direct incorrect or incomplete URLs, or change the default homepage. They may also re-direct searches to 'pay-to-view' [often pornographic] web sites.

The actual advertising materials themselves are usually delivered using one of the following methods:

- Downloaded adverts from web or FTP servers.
- Re-direction of search engine results to advertising sites. This might occur only if the web site requested by the user is unavailable for some reason.

Many adware utilities also collect and forward information about individual machines and users: this may include IP addresses, operating system and browser version numbers, lists of most visited web sites, search engine queries and other information that can be used to design a new advertising campaign.

6. Other malware-related programs

The Kaspersky Lab extended databases also provide detection for a wide variety of other non-viral, but potentially hostile programs. These include the following:

1. Programs known to cause system problems.
2. Key generators.
3. Credit card number generators.
4. Java classes.
5. Programs generating unexpected audio and video effects.
6. Security data collectors [gathering data about installed anti-virus and personal firewall programs].
7. Virus simulators.
8. Programs that have unusual form and content and may be malicious.

Technology integration

The use of an integrated security solution that includes protection from spyware and other malware-related programs has now become an essential part of a wider security strategy. One of the major plus points of the Kaspersky anti-virus engine, compared to other solutions available on the market, is that it provides advanced protection from spyware and other non-viral categories of malware without requiring customers to install two different scanning engines (one for anti-virus and one for spyware), without having to maintain and upgrade two different software programs and without having to install two different updaters and implement two different update routines for anti-virus and spyware signatures.

The extended databases to the Kaspersky anti-virus engine provide effective detection for non-viral, potentially hostile programs that can be misused by hackers and other cyber criminals. This includes adware and malware-related 'riskware' and 'pornware' applications, together with spyware programs that are not already detected as Trojans using the standard databases.

This capability, available in Kaspersky Lab anti-virus products, can also be seamlessly integrated into third-party products and business services. First-rate detection, flexible configuration and Kaspersky Lab's solid OEM business history have made the Kaspersky anti-virus engine the technology of choice for hundreds of business partners.

For more details about technology solutions and customized protection from malware-related programs, contact Kaspersky Project Division at [OEM@kaspersky.com](mailto: OEM@kaspersky.com). We are open to discuss all cooperation offers and will take into account the specifics of any business model.

The expertise of Kaspersky Lab virus researchers and our unmatched hourly updates, ensure not only quality detection, but a fast response to any new threat.

References:

¹ For more information about the engine, consult the whitepaper "Kaspersky Anti-Virus Engine. Base technology whitepaper".

² The latest information about potentially hostile programs and other malware types can be found in the Kaspersky Virus Encyclopaedia at <http://www.viruslist.com>

³ The tests include [Virus Test Center, University of Hamburg](#), [AV-Test GmbH](#), [AV-comparatives.org](#) & [Virus Bulletin](#). More information about test results is available at Kaspersky Project Division

⁴ Read more about Kaspersky Spyware Checkmark Certificate at <http://www.kaspersky.com/news?id=167585804>

⁵ [IDC](#), December 2004.