



How to combat spyware in corporate environments

The information contained in this document represents the current view of Panda Software International, S.L. on the issues discussed herein as of the date of publication. This document is for informational purposes only. Panda Software International, S.L. makes no warranties, express or implied, in this document.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise) or for any purpose, without the express written permission of Panda Software International, S.L.

Panda Software International, S.L. may have patents, patent applications, trademarks, copyrights or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Panda Software International, S.L. the furnishing of this document does not give you any license to these patents, trademarks, copyrights or other intellectual property.



CONTENT

HOW TO COMBAT SPYWARE IN CORPORATE ENVIRONMENTS	4
Target	4
Executive summary	4
THE SPYWARE PROBLEM	5
Spyware in organizations	5
Adware in organizations	5
CLASSIFYING SPYWARE	6
Types of spyware	7
THE HISTORY OF SPYWARE	8
The future of spyware and adware	10
THE ECONOMIC THREAT OF SPYWARE	10
Associated risks	13
THE PANDA SOFTWARE APPROACH TO THE SPYWARE PROBLEM	14
Alternatives	14
APPENDIX A. TERMS AND ABBREVIATIONS	17
Acronyms	17
Glossary of terms	17
ANEXO B. PANDA SOFTWARE EN EL MUNDO	18



Tables and graphs

- ActiveX Control for installing Gator from Internet Explorer _____ 9
- Growth of spyware / adware (up to Feb. 2003 – Pest Patrol) _____ 10
- Growth of spyware in the Internet (The Economist) _____ 11
- IDC survey of the greatest security threats in corporate networks _____ 12
- CNet survey of the biggest scourge of the Internet. _____ 12
- What are the main problems you find when using the Internet? _____ 13



HOW TO COMBAT SPYWARE IN CORPORATE ENVIRONMENTS

Target

This document is aimed at people in charge of any aspect of IT security in large companies.

Executive summary

Spyware and adware are no longer just a threat to home user and as well as increasing their capacity to get into computers, they have also increased their area of action to the **corporate environment**. In fact, some spyware can even obtain information about email messages, passwords and even credit card details ...

Spyware downloaded to companies can **steal confidential information**, reduce the **performance of the IT infrastructure**, due to the resources used by non work-related activity and **loss of employee productivity**, who have to deal with changes to system settings and unwanted advertisements.

Even though tools are available for protecting home users, according to Gartner "The use of consumer grade tools is no substitute for a **managed solution**, no matter how effective the tool."

Panda Software offers a range of **solutions adapted** to needs of each type of client, from home users, through ActiveScan Pro and Platinum Internet Security 2005, which according to the **PC Magazine** "it was more successful in cleaning and blocking spyware than any of the other suites were," to corporate environments with **BusinesSecure** and **EnterpriSecure** with **TruPrevent™ Technologies**, capable of providing **complete centralized protection for every network layer**: workstations, laptops and server, and combine preventive techniques - **TruPrevent™** and reactive techniques - filters and signatures - to achieve effective **detection and disinfection** of spyware, however they try to get into the organization.

THE SPYWARE PROBLEM



Spyware in organizations

Spyware are deceitful programs that perform certain activities in the PC without appropriate user authorization for their installation. Spyware can collect personal information and/or change the Internet browser configuration, among other types of behavior.

Spyware is developed by companies looking for financial gains using unorthodox methods. Information collected by spyware is used by the companies themselves or sold to third parties. This type of information is extremely useful, as it can be used to generate specific profiles that can then be targeted with personalized advertising, usually as spam messages. For example, an employee that regularly visits financial news website will receive spam about buying and selling shares.

Spyware is very similar to adware in terms of its design, but **compromises the security** of companies and the information it transfers. Spyware is installed on computers in the same way as adware. They can get into computers when the user or a Trojan downloads files from the Internet or can be bundled with freeware. Once installed, these programs can register browsing habits, activity of the computer, information sent via email, etc.

This type of **confidential information** is constantly sent out via the Internet by spyware. Even though the privacy policy of advertising companies claims that they do not collect personal or confidential data in order to protect the identification of the user, computers with these programs installed can leak corporate information, as well as **using corporate resources**.

Adware in organizations

Adware comes from the abbreviation of the words Advertising Software, in other words programs that show adverts. Adware is software that shows advertising, using any type of method: pop-ups, banners, changes in the home page or search engine, etc. The advertising is linked to products and/or services offered by the creators or third parties.

Adware is run as a background task and is generally **transparent** to the user, except when they **browse the Internet**. The symptoms of adware include modifying banners displayed in the browser, changing the **start page** to redirect traffic to a certain advertiser, adding **toolbars** to the browser or displaying **pop-up windows** that degrade employee activity.



Classifying spyware



According to Dell Computer Corporate, "...The term spyware refers to software that gathers personal information from your computer, sometimes **without your knowledge**. The information is often used for advertising purposes. Spyware may cause your computer to **slow down** or encounter errors. Spyware has also been known to cause unwanted pop-up advertisements, an inability to connect to the Internet, and problems printing."

"Spyware applications can be bundled as a **hidden component of freeware or shareware** programs that can be downloaded from the Internet. Once installed, spyware can monitor your activity on the Internet and transmit that information to a third party."

Junk programs and pop-up windows can even make the **computer impossible to use**, to the point that it needs to be reformatted in order to recover normal functioning. However, the most serious problem is, without a doubt, the way in which some companies try to persuade users to install this type of software. Even though many claim they do not contain spyware, their privacy policies give them the **right to transfer and store all types of personal information** they consider necessary and to **install any type of software** they want on the computer, without the user's permission.

There are even anti-spyware programs that detect spyware that does not exist in order to boost sales and seem better than competitors and companies that **design software for eliminating spyware** which is actually spyware itself. The only way to avoid these situations is to carefully read the **EULA** (End User License Agreement) for the product before installing it and install products that the anti-spyware software allows to be installed. If this is not the case, a large part of your activity could be collected by these programs and used to generate personalized campaigns without your permission.



Types of spyware

There is a wide range of software and applications of all kinds that can be classified as spyware or adware. In this section, we will look at the applications, the most sophisticated of which are even capable of capturing screenshots from Webcams.

For Panda Software, spyware is a type of malware. Apart from being annoying to the user, spyware causes a variety of effects in the PC, ranging from performance degradation to a violation of personal privacy.

Panda Software defines adware as programs that display advertising through pop-ups, banners, changing the start page of the Internet browser, etc. Adware can be installed with the user's authorization and full awareness, but this is not always the case. If it is installed with the user's knowledge and consent, this is categorized and detected as adware in Panda. If it is installed without the user's authorization or knowledge, it is categorized as spyware in Panda.

The following types of threats fall within the spyware category:

- **Tracking software** or Trackware: are programs that carry out inventories of the applications installed, tracking user itineraries etc. Consequently, they save all searches performed in the search engine which they position as the home page, or introduce keyloggers, which record all keystrokes made.
 - **Tracking Cookies:** a type of Tracking Software are Tracking Cookies. Cookies are small text files used by servers and Web browsers to store and recover information on visitors. However, there is a type of malicious cookie called Tracking Cookie which is normally used by spyware to collect information. These are detected as cookies in Panda.
- **Spybot or spy Trojans:** there is a large variety of spy Trojans, each of which is increasingly dangerous and all of which are designed to steal sensitive information. These Trojans are programmed to act automatically and activate themselves or carry out certain actions after receiving the relevant orders from their creators. Some of them specialize in obtaining financial data, while others look for codes for the fraudulent use of pirate software. They concentrate on the theft of user names and passwords from systems as well as access credentials to web or mail services. These are detected as Trojans in Panda.

With respect to their behavior once installed, they can be termed as Hijackers when they modify user information, such as the home page and browser engine, altering the results of searches carried out etc.

And, according to the way they activate themselves, we can differentiate between:

- **BHO (Browser Helper Object):** are browser plug-ins like Google, eBay, Yahoo or the Acrobat Reader plug-in that allows users to view a PDF document in the browser is a BHO (Browser Helper Object). They are normally loaded when clicking on a link in a malicious page visited, and will be executed every time the browser is opened. They may be visible like browser tool bars or remain hidden while they perform a series of operations unknown to the user.
- Other forms of activation that coincide are those used by viruses and Trojans.



Other manufacturers include some of the types of malicious software that Panda Software classifies as malware under the category of spyware. These include threats against which Panda Software has been protecting its clients for many years, and which don't perform the same actions in systems:

- **Keyloggers:** keyloggers are a kind of behavior associated with a virus, worm or Trojan, rather than a type of threat. This behavior involves logging exactly what a user enters on a keyboard and saving it in a file which can then be sent to a third party without the user's knowledge or consent. BugBear.B, for example, is a worm that behaves in a similar way.
- **Dialers:** These are programs that can, without the user knowing, disconnect their telephone connection (which allows access to the Internet, by dialing a certain telephone number) and redial another such as a premium-rate number. Dialers only affect users with modem or dial-up Internet connections. If the user with a modem is affected by a dialer, they will experience a notable increase in their telephone bill.

The history of spyware

It wasn't that long ago when the first spyware programs emerged. Two of the most famous are Gator and BargainBuddy, widely spread applications that are still highly active. In fact, it would be difficult to find an experienced Internet user that hasn't at one time or other felt the effects of one of them.

Gator is a good example to take to explain how spyware works. This program takes the form of an application offering users some kind of free service, often a system for **storing passwords** so that users will be able to recover them easily should they forget them. The application is installed via a window that appears asking for authorization from the user, if they accept then the spyware will be installed along with the application. This then displays **unsolicited advertising** and snoops on the user's Internet connections. Worst of all, had the user paid close attention to the terms for installing Gator, they would have read that they were being asked for permission to install the spyware.

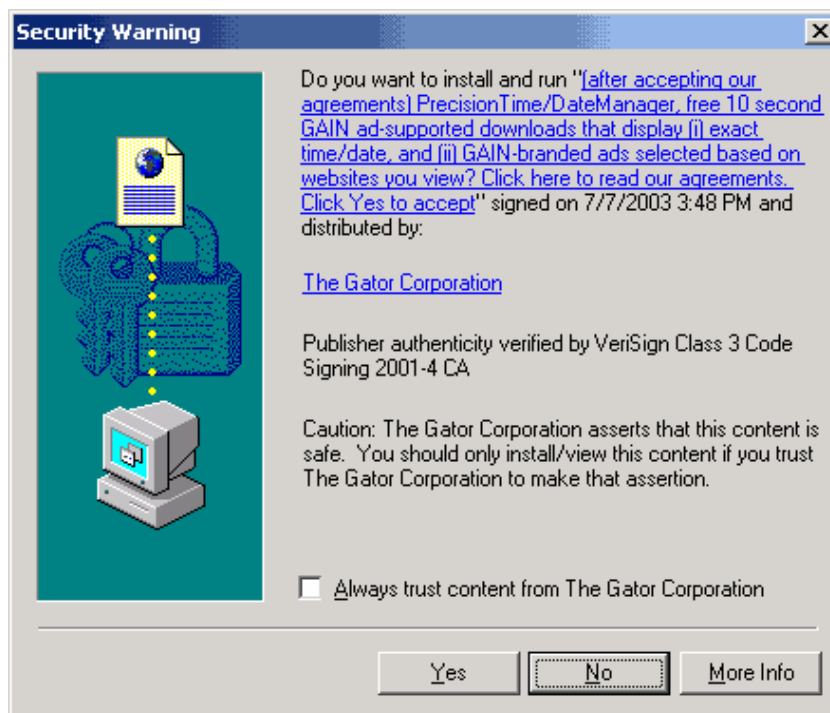


Figure 1 – ActiveX Control for installing Gator from Internet Explorer

It is more usual for spy programs to be installed secretly. Sometimes it is downloaded automatically on viewing a certain web page and accepting the installation of an ActiveX control; on other occasions it is installed on the system alongside another program.

The future of spyware and adware

Just as with any other Internet threat, spyware is evolving towards even more sophisticated programs, capable of carrying out ever more complex actions and becoming increasingly difficult to detect and remove. At the same time, the creators of this type of malware are determined to see their creations spread as widely as possible to reap the benefits as quickly as possible. As spyware is often relatively large, it is not easy to spread these applications through channels such as email. For this reason there is an increase in the number of **computer viruses** -which are easier to propagate quickly- designed to download spyware onto the computers they infect. This has the added advantage for the culprits that one virus can insert multiple spy programs on a single computer.

THE ECONOMIC THREAT OF SPYWARE

Spyware collects confidential user data that could then be sold to marketing companies for advertising purposes. The same happens with adware, which earns a significant income from companies willing to pay to get their advertisements viewed, whether the user has requested it or not.

This software has become an epidemic. A study of 1 million computers by the ISP Earthlink shows that in the US **28 programs** of this kind were detected on each PC, reaching a total of 29.5 million installations. Webroot also offers statistics, which are lower but still worrying: an average of **2 spyware applications per computer**.

While most spyware is adware-related and relatively harmless, the study detected over **300,000** more serious System Monitors and Trojans. This figure shows how real a threat identity or system corruption is for users.

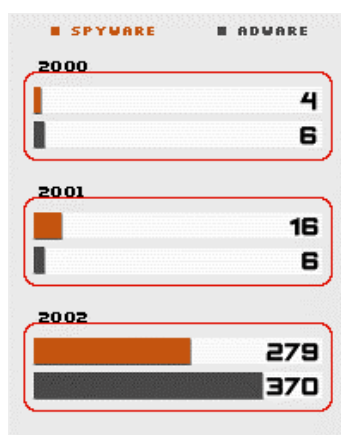


Figure 2 – Growth of spyware / adware (up to Feb. 2003 – Pest Patrol)

Some PC vendors, for instance, blame spyware for the rise in calls to **tech support**. For example, Dell executives said spyware accounted for **15 percent** of its support calls, a dramatic increase from 2003's 2 percent.

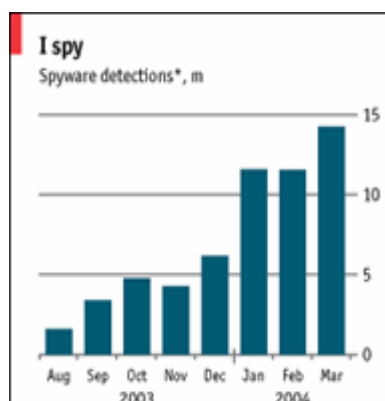


Figure 3 – Growth of spyware in the Internet (The Economist)

Although spyware initially target home users, it is gradually become a threat that administrators have to spend more time dealing with. According to a study compiled by Web@Work in 2004, **92 percent of companies** acknowledge a serious spyware problem. To respond to this situation, IDC estimates that **corporate investment** in this field will increase **2,500 percent** (305 million dollars) by 2008

The estimates of the percentage of computers affected by spyware vary depending on the source. These range from 4 percent of the IT infrastructure to 30 percent of corporate desktops¹, through 40-50 percent, estimated by EarthLink or 67 percent, estimated by IDC, and reaching 90 for computers with broadband connections².

The main companies that operate with these kinds of programs state that more than 100 million samples of their software is installed on PCs, whereas ClickZ Stats gives a total volume of **280 million** affected PCs. For example Claria revealed that their software resided on 40 million PCs, where as Avenue Media claimed they had 2 million infected machines, with an **annual income of around 3 dollars per infection per year**.

When comparing spyware to other Internet threats, interesting conclusions on the real impact of spyware are revealed. A study of over 600 organizations carried out by IDC in August 2004, spyware was the **4th greatest threat** to corporate security. If spyware is combined with spam, as CNet did in its online survey, it takes first place, exceeding even **viruses and hackers**.

¹ Web@Work, 2004.

² US National Cyber Security Alliance

What is the single greatest threat to your company's enterprise network security? IDC-aug04

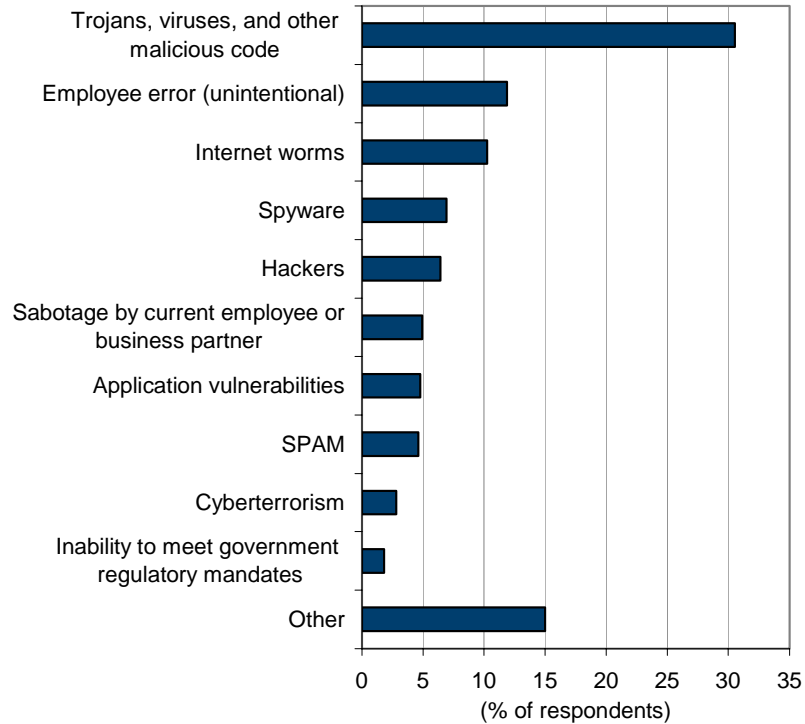


Figure 4 – IDC survey of the greatest security threats in corporate networks

What's the biggest scourge of the Internet?



Figure 5 - CNet survey of the biggest scourge of the Internet.

Data compiled by Panda ActiveScan Pro, the spyware / adware detection and disinfection tool, are no more hopeful, as the percentage of spyware / adware vs. virus / worms / Trojans detected by this online solution is 84 percent vs 16 percent. The number of PCs infected with the 7 most common spyware programs exceeds the total computers infected by any known virus, worm or Trojan.

If these issues are transferred the study carried out in the last quarter of 2004 by AIMC in Spain, the results are incredibly similar, despite the differences in the sample.

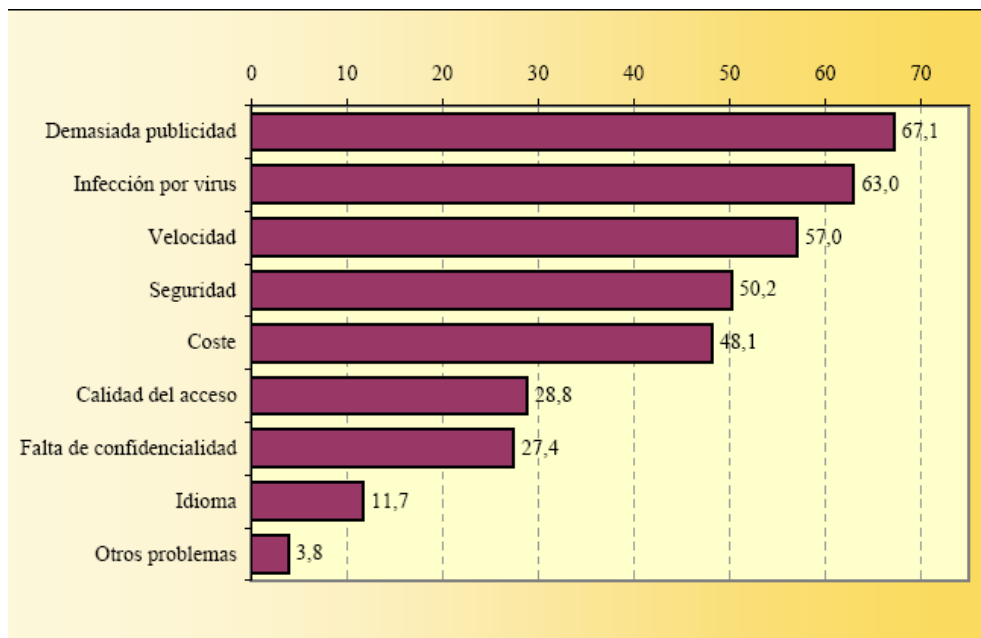


Figure 6 – What are the main problems you find when using the Internet?

Associated risks

The data described above shows that spyware and related threats introduce a significant security, confidentiality, and legal risk to the enterprise. As more corporate PCs get infected, the organization will encounter a greater number of problems, such as:

- Loss of confidential personal or corporate information
- Lower computer system performance
- More frequent system- and browser-related crashes
- Loss of network bandwidth
- Decreased employee productivity
- Higher risk of legal liability

With respect to the last concept, with HR 29, the U.S. Congress is attempting to set into law a distinction between adware and spyware. It will make it legal on the one hand to distribute software that shows you pop-up ads based on your browsing habits so long as that software asks for permission before it is installed and provides a mechanism for removing it.

This initiative, as well as those promoted in the states of California, New York, Iowa and Virginia, adhere to the principal of notifying, getting permission and providing mechanisms for removing it published by the European Commission in its privacy direct in 2002.



THE PANDA SOFTWARE APPROACH TO THE SPYWARE PROBLEM

As we add on more levels of protection, we succeed in maximizing the efficiency of the anti-spyware protection, not to mention the investment in the company's security systems. This **layered protection** will make it much more complicated for malware to penetrate the company and will therefore, **curb the risk** of infection. The greater the number of layers protected in the organization, the closer it will be in reaching the 100% security mark, by maximizing the efficiency of the security solutions.

Alternatives

There are many alternative ways of dealing with spyware and each has special characteristics, depending on the architecture selected:

- Specific programs on workstations
- Content filtering
- Multi-layered anti-malware protection

Specific programs on workstations

Programs designed to detect and eliminate spyware are **easy to use**, but all computers cannot be managed from a central console, which could lead to security holes.

What's more, some of the most popular free solutions do not include **permanent protection**, which **reduces their effectiveness**, when considering that according to Gartner, very few people carry out daily or frequent spyware scans, the need for permanent anti-spyware protection that avoids mistakes and theft of information between on-demand scans.

Content filtering

The **web content filtering module** in appliances or perimeter devices like Panda GateDefender 800 series prevent spyware from being downloaded when browsing the Internet. This avoids the user from downloading and installing this type of software by mistake, as it blocks access to web pages containing this type of software.

Unfortunately, the number of pages containing these types of programs is constantly growing and controlling the local sites is a huge task that cannot control all of the access points used by this software. What's more, the means used by spyware to get into companies are not limited to web services and therefore, another approach is needed in addition to the **complete protection** offered by perimeter content filtering tools.



Multi-layered anti-malware protection

The best solution to protect computers against spyware is to have an integrated security suite combining different technologies, both reactive and proactive. For corporate environments it is also necessary to have an integral strategy of layered protection, from gateways to endpoints.

Even though protection in servers can block the mass distribution of spyware across the network, by **filtering certain executable files** in the firewall or web server to prevent them from being downloaded, only the combination of client and server software can effective protection. Panda Software's solutions do this using a combination of **preventive and reactive techniques** to increase the protection offered to its clients.

Panda Software designed a layered protection architecture which allows the distribution and updating of anti-spyware solutions to all **points of the network**: workstations, file servers and Exchange and Domino mail, SMTP mail gateways and perimeter security servers, regardless of their physical location or technological platform: Windows, Novell or Linux.

Panda provides a complete layered anti-malware protection strategy to combat malware or blended threats: **spyware, adware, dialers, virus, worms, Trojans, security vulnerabilities, spam, hoaxes** or other tools which are used by hackers and jeopardize the continuity of our business processes. For example, if spyware modified LSPs and was deleted manually by an inexperienced user, the computer could be left without an Internet connection. The Panda would restore this connection by simply scanning the computer.

This optimizes the effectiveness of the protection installed across the corporate network. It is necessary to cover the two vectors of a **bi-dimensional matrix**. On the one hand, installing anti-malware protection to safeguard the company from all types of threats, and on the other, applying this **protection in each network layer** to detect and resolve the problem in the entry-point before it spreads across the network.



The advantages of this strategy are obvious and are based on a philosophy that strives to optimize investment made in other security mechanisms:

- **Global centralized administration** of the anti-spyware policy along with the rest of the company's security policies.
- **Common administration, update and monitoring infrastructure**, reducing the **training time** needed by administrators to and optimizing **bandwidth and local resources** used to communicate with the administration console.
- **Automatic daily updates and permanent protection** for each network layer: laptops, workstations, mail servers and gateways, file and web servers or corporate firewalls, freeing the administrator from the time consuming task of carrying out on-demand scans.
- **Signature-based detection and disinfection mechanisms** that detect and disinfect known spyware. This is combined with the **preventative protection** provided by the **TruPrevent™ Technologies**, which have detected and blocked over 25 unknown spyware programs based on their **behavior** and include a **security policy** definition module to block exploits used by spyware to get into computers without the user realizing. This results in complete protection against these types of threats.

To sum up Panda Software's corporate solutions: **BusinesSecure** and **EnterpriSecure** with **TruPrevent™ Technologies** offer effective centralized protection³ against spyware in all network layers, reducing the risk of infection and transmission of confidential corporate information to third-parties.

³ Over 1500 traces and 500 spyware files eliminated.



APPENDIX A. TERMS AND ABBREVIATIONS

Acronyms

BHO – Browser Helper Object
CGI – Common Gateway Interface
EULA – End User License Agreement
FTP – File Transfer Protocol
RAT - Remote Access Tool

Glossary of terms

Update	Anti-spyware protection is constantly developing, resulting in more powerful versions, adapted to the new techniques used by spyware. For this reason, they incorporate a signature file. This file includes all of the characteristics of spyware programs, so that they can detect them and take the appropriate action. Incorporating the latest version of this file into the program is known as an update.
Cookies	Programs that track user Internet activity, registering the pages the user visits, the programs run, etc. without the user realizing.
Hijackers	The system that protects users against this type of malware is the anti-spyware protection. Scripts, ActiveX or programs in HTML pages that change the start and search pages of the browser, so that a certain page is opened by default. Sometimes the size of advertisements and banners that appear in Internet browser exceed the speed of the connection and can therefore, damage the user's browsing activity by using up all the bandwidth.
Protection against pop-up ads	In other cases, advertising can appear in pop-up windows when the user is browsing certain web pages can cause different problems: loss of productivity and time if many windows appear; which can even occupy the whole screen so that the user does not know how to close them. Protection against advertisements and y pop-ups blocks this type of malware, preventing them from being displayed.
RATs (Remote Access Tool)	Programs that are installed on the computer without the user knowing and allow remote control of the computer or access to confidential information.
Preventive protection	Capacity to prevent events using techniques that act before an event occurs.
Reactive protection	Protection system based on reacting to threats when they appear.
Software	Logical part of IT systems (programs, applications, information, etc.)
Spybots	Programs that are installed on the computer by other applications or installers of these applications without the user knowing. These collect information about the user's activity and habits and sends them to marketing companies via the Internet.
Spyware	Spyware refers to programs, ActiveX components or code embedded in email messages or web pages, designed to steal personal information from the user (Internet surfing habits, tastes, purchasing preferences, bank details, etc.) without them realizing or without having given their permission.
Traces	Files or Registry entries which applications use to store information about the activity of the application or its use.
WebBugs	Elements embedded in emails which are capable of sending personal user information to a predetermined server when the message is opened.



ANEXO B. PANDA SOFTWARE EN EL MUNDO

<p>Panda Headquarters in Europe Ronda de Poniente 19 Tres Cantos 28760 Madrid, España Phone: +34 91 806 37 00 E-mail: info@pandasoftware.com</p>	<p>Panda Headquarters in USA 230 N. Maryland, Suite 303 P.O. Box 10578 Glendale, CA 91209, USA Phone: +00 1 818 543 6901 E-mail: usa@pandasoftware.com</p>
<p>Panda Software Germany Dr.-Detlev-Karsten-Rohwedder-Str. 19 47228 Duisburg Phone: +49 20 65 9 87 654 E-mail: germany@pandasoftware.com</p>	<p>Panda Software Saudi Arabia P.O.BOX # 2797, AL KHOBAR 31952, KSA Phone: + 966 3 897 9956 E-mail: saudiarabia@pandasoftware.com</p>
<p>Panda Software Argentina Calle Roque Saenz Peña 1160, piso9b Buenos Aires 1035 Phone: +00 5411 508 10500 E-mail: argentina@pandasoftware.com</p>	<p>Panda Software Austria Rennweg 98 Top 7 A – 1030 Wien Phone: +49 02065 987654 E-mail: austria@pandasoftware.com</p>
<p>Panda Software Belgium Mechelen Campus Schaliënhoevedreef 20d 2800 Mechelen Belgium Phone: +32 2 756 08 80 E-mail: belgium@pandasoftware.com</p>	<p>Panda Software Bolivia Calle Landaeta # 221, Edificio Gamarra 3er Piso La Paz – Bolivia Código postal 11433 Phone: +591 2 211 4777 E-mail: bolivia@pandasoftware.com</p>
<p>Panda Software Canada SECURE RDG CANADA INC 100 Allstate Parkway Suite 502 Markham, CANADA Phone: +1 (905) 479 2208 E-mail: canada@pandasoftware.com</p>	<p>Panda Software Bulgaria 26-28, Christo Stanishev str. Sofia 1225 BULGARIA Phone: +359 2 81 328 11 E-mail: bulgaria@pandasoftware.com</p>
<p>Panda Software China Room 1003,10F,Minfang Building, 593 Fuxing Road(M), 200020 Shanghai Phone: +86 21 2402 8800 +86 21 2402 8526 E-mail: china@pandasoftware.com</p>	<p>Panda Software Chile Mosqueto 459 ofic. 202 8320112, Santiago-Centro Chile Phone: +56 2 639 7541 E-mail: chile@pandasoftware.com</p>
<p>Panda Software South Korea 3Fl. SungWoo Bldg. 114-29 SamSung-Dong, KangNam-Gu, Seoul - Korea Phone: +82-2-555-8600 E-mail: korea@pandasoftware.com</p>	<p>Panda Software Colombia Carrera 41 N.46-26 Itagui Antioquia Phone: + 57 4-3735588 E-mail: colombia@pandasoftware.com</p>
<p>Panda Software Denmark Kirke Værløsevej 24, 1. sal, mf. DK 3500 – Værløse Phone: +45 60 218 738 E-mail: denmark@pandasoftware.com</p>	<p>Panda Software Costa Rica Calle 25, Ave 6 y 8 #648 San José Phone: 00 506 258 0100 E-mail: costarica@pandasoftware.com</p>



<p>Panda Software Slovakia Lublanska 1 83102 Bratislava Phone: +421 2 444 55 702 E-mail: slovakia@pandasoftware.com</p>	<p>Panda Software UAE Bldg-5 Office No. 5G-15 P O Box 41573 – Hamriyah Free Zone, Sharjah Phone: +971 (6-526.30.14) E-mail: UAE@pandasoftware.com</p>
<p>Panda Software Spain Ronda de Poniente 19 Tres Cantos 28760 Madrid Phone: 902 365 505 E-mail: info@pandasoftware.es</p>	<p>Panda Software Slovenia Stari trg 5A, SI-8210 Trebnje Phone: +386 7 34 61 020 E-mail: slovenia@pandasoftware.com</p>
<p>Panda Software Finland Hatanpään valtatie 8 33100 Tampere Postal address: P.O BOX 636. 33101 Tampere Phone: +358 3 339 26 700 E-mail: finland@pandasoftware.com</p>	<p>Panda Software USA 230 N. Maryland, Suite 303 P.O. Box 10578 Glendale, CA 91209, USA Phone: +00 1 818 543 6901 E-mail: usa@pandasoftware.com</p>
<p>Panda Software UK 5 Signet Court, Swanns Road Cambridge CB5 8LA Phone: +44 (0)870 444 5640 E-mail: uk@pandasoftware.com</p>	<p>Panda Software France 33 bis Boulevard Gambetta. 78300 Poissy Phone: +33 1 30 06 15 15 E-mail: france@pandasoftware.com</p>
<p>Panda Software Guatemala 5 Av. 5-55 Zona 14, Euro plaza Torre 1 Nivel 2. Ciudad de Guatemala Phone: +502 2386-8866/67/68 E-mail: guatemala@pandasoftware.com</p>	<p>Panda Software Greece 82 Zanni St. Piraeus, ZIP Code 18537 Phone: +30 2 10 4588 085 E-mail: greece@pandasoftware.com</p>
<p>Panda Software Hungary Szugló utca 54 1145 Budapest Phone: +36 1 469 70 97 E-mail: hungary@pandasoftware.com</p>	<p>Panda Software Netherlands Stephensonweg 14 4207 HB Gorinchem Phone: +31 183 699020 E-mail: netherlands@pandasoftware.com</p>
<p>Panda Software Israel 43 Hamelacha street, New Industrial Zone 42504 Natanya Phone: +972 9 – 8859611 E-mail: israel@pandasoftware.com</p>	<p>Panda Software India E-9, Connaught House Connaught Place New Delhi-110001 Phone: +91 11 2341 8199 E-mail: india@pandasoftware.com</p>
<p>Panda Software Japan Nakameguro GT Tower 7F, 2-1-1 Kamimeguro, Meguro-ku, Tokyo 153-0051 Phone: +81-3-6412-6020 E-mail: japan@pandasoftware.com</p>	<p>Panda Software Italy Viale E. Marelli 165 20099 Sesto S. Giovanni (Mi) Phone: 02-24 20 22 08 E-mail: italy@pandasoftware.com</p>
<p>Panda Software Lithuania Žemaitės st. 21, LT – 2009 Vilnius Phone: +370 5 2397833 E-mail: lithuania@pandasoftware.com</p>	<p>Panda Software Latvia Merkela Street 1 1050 Riga Phone: +371 7211636 E-mail: latvia@pandasoftware.com</p>



<p>Panda Software Malaysia Unit A-10-6, Megan Phileo Promenade, 189 Jalan Tun Razak, 50400 Kuala Lumpur Phone: +60 3 2163 2468 E-mail: malaysia@pandasoftware.com</p>	<p>Panda Software Luxemburg Mechelen Campus Schaliënhoevedreef 20d 2800 Mechelen Belgium Phone: +32 2 756 08 80 E-mail: luxembourg@pandasoftware.com</p>
<p>Panda Software Norway ViroSafe Norge AS Skogveien 41 2318 Hamar Phone: 00 47 62 53 96 80 E-mail: norway@pandasoftware.com</p>	<p>Panda Software Mexico Tuxpan 39# 104 y 105, 06760 México, D.F. Phone: +52 5 2642127 E-mail: mexico@pandasoftware.com</p>
<p>Panda Software Peru Calle Lord Cochrane 521 Miraflores – Lima 18 Phone: 00 51 1 221 6001/ 221 0159 E-mail: peru@pandasoftware.com</p>	<p>Panda Software Paraguay Eliseo Reclus 247 Calle Guido Spano Asunción Phone: +00 595 21 607594 E-mail: paraguay@pandasoftware.com</p>
<p>Panda Software Portugal Quinta da francelha - Edificio Sagres, 7B 2685-338 Prior Velho Phone: + 351 219426800 E-mail: portugal@pandasoftware.com</p>	<p>Panda Software Poland Ul. Wiktorska 63 02-587 Warszawa Phone: +48 (22) 540 18 06 E-mail: poland@pandasoftware.com</p>
<p>Panda Software Russia 64-47 Tokarey St., 620109 Yekaterinburg, Sverdlovsk region Phone: +7 3432 78-31-27 E-mail: russia@pandasoftware.com</p>	<p>Panda Software Puerto Rico / Rep. Dominicana Avenida Muñoz Rivera 1058 Edificio Fomento Corporativo Esquina Yale Río Piedras 00927 Puerto Rico Phone: +1 787 296 1139 E-mail: caribe@pandasoftware.com</p>
<p>Panda Software Sweden Industrivägen 7, S-171 48 Solna Phone: +46 8-545 25030 E-mail: sweeden@pandasoftware.com</p>	<p>Panda Software Singapore 10 Ubi Crescent, # 05-37 Ubi Techpark , Singapore 408564 Teléf:+ (65) 6742 2660 E-mail: singapore@pandasoftware.com</p>
<p>Panda Software Thailand 192 Soi Laprao 107 Bangkapi, Bangkok 10240 Phone: 00 662 7311480 E-mail: thailand@pandasoftware.com</p>	<p>Panda Software Switzerland Route Champ-Colin, 10 1260 Nyon Phone: +41 22 994 89 40 E-mail: switzerland@pandasoftware.com</p>
<p>Panda Software Uruguay Jose Enrique Godó 1955 11200 Montevideo Phone: +5982 4020673 E-mail: uruguay@pandasoftware.com</p>	<p>Panda Software Turkey Darulaceze Cad Karatas Sok. SNS Plaza N° 6 80270 OKMEYDANI – ISTANBUL Teléf.: 90 212 222 1520/90 212 210 2200 E-mail: turkey@pandasoftware.com</p>
	<p>Panda Software Venezuela Av. Libertador C.C. Libertador, PH-7 Caracas Phone: +(58 212) 700.7596 E-mail: venezuela@pandasoftware.com</p>