Anti-spam protection in the network perimeter

The information contained in this document represents the current views of Panda Security on the issues discussed herein as of the date of publication. This document is for informational purposes only. Panda Security makes no warranties, expressed or implied, in this document.

Anti-spam protection in the network perimeter

TABLES

1 Introduction

The term “malware” can be defined as: any program, document or message, which is liable to be detrimental to the users of IT systems. Viruses therefore only form part of an ever-increasing group of other IT hazards in which spam, dialers or spyware are included.

At present, spam (or any unsolicited mail) is one of the greatest Internet dangers, chiefly because it can cause damage at very different levels.

1.1 Objectives

To learn about the characteristics of unsolicited mail or spam, the best means of prevention and the techniques applied by GateDefender Performa to minimize the impact of this type of communication in business productivity.

1.2 Audience

- IT users
- Mail administrators
- Network administrators
- Security experts
- CTOs (Chief Technology Officer)
- CIOs (Chief Information Officer)

2 What is spam?

The word "spam" comes from a gag in a comedy series in which all of the dishes in a restaurant include a brand of canned luncheon meat called spam as the main ingredient. By way of comparison, this term started being used to describe the huge number of unwanted messages received by any e-mail account.

Although it is not typical, spam may contain viruses or other malicious codes, or e-mail addresses which lead to Web pages equipped to download programs in an unauthorized manner. This was presumably the method used by the famous worm, "Sobig.F" that was granted the title "the fastest spreading virus in computer history."

3 Why is it necessary to worry about spam?

On the one hand, the damage caused by this kind of malware can be economically quantified by the hours of work wasted each day all over the world—not from the task of reading spam messages but from simply eliminating them. Just imagine a corporate network with 500 workstations where 10 messages of this kind are received every day.

If five minutes are wasted every day as a result of these messages, it is easy to calculate the huge number of hours lost by each worker due to spam each year. In addition, if the content is sufficiently attractive to entice the user to read the content, or connect to a Web site indicated by the text, the time wasted increases exponentially.

3.1 Economic impact

Spam has a negative influence on companies' results by:

3.1.1 Lowering staff productivity

Companies lose productivity when their employees waste time downloading and deleting unwanted mail instead of tending to their normal duties. The cost may vary according to the cost/hour of each employee, but considering that detecting and deleting junk mail takes approximately 10 seconds, for a company with a headcount of 1,000 employees where users receive approximately 100 unwanted e-mails per month, this would take 3½ hours yearly, which amounts to a cost of more than $70,000.

3.1.2 Heavier administration workload

Network and mail administrators, together with technical support professionals, must spend their time and effort giving advice and providing end users with tools to tackle this kind of malware.

3.1.3 Increased use of network resources

The volume of e-mail spam is directly proportional to the cost of the IT resources dealing with it. Therefore, if 3/5 of a company's incoming mail is spam, this means that 3/5 of the e-mail servers, LAN bandwidth and the devices dealing with security copies are being used to process and store junk mail.

3.1.4 Security risks

The weakest part of a security system is the human component. Spammers cannot directly access employees' desktops to steal passwords and gain access to confidential information. However, they can trick users into opening messages or attached files containing viruses or malicious codes, thereby generating a security hole in the entire company.

3.1.5 Legal risks

Many unwanted e-mails contain offensive, sexual or violent content that does not comply with the organization's code of ethics. Furthermore, if measures are not taken to block this type of content, the company could face legal action from trade unions and workers for not providing a respectable work environment.

3.2 Quantitative studies

These days, e-mail is the number one communication exchange preferred by companies and individuals. Virtually all large companies listed on the Stock Market use these systems and according to recent studies, up to 60% of the intellectual capital of a company may be found electronically within their mail systems.

It therefore comes as no surprise that according to figures recently quoted in the Spamfilter Review in 2004, **31 million e-mail messages are sent** everyday worldwide and 40 % of them, **12.4 million messages are undesired**.

The spam problem is widespread among Internet users, given that approximately 60% of the target audience (e-mail users), have received inappropriate messages or messages with sexual content. (1)

(1 Source: USA Today.)

The figures regarding the percentage of junk mail varied, depending on their sources as shown by **Table 1 - Mail vs. junk**, but it seems clear that turning a blind eye to spam is no longer an option for companies, especially when only 5% are capable of blocking these messages effectively (90% success rate)[2].

Source	Percentage of junk mail
Gartner Group	25
AOL	33
Brightmail	50

Table 1 - Mail vs. Junk

The continually growing amounts of spam and junk mail made 85 % of companies consider spam to be a serious problem and 90% are evaluating anti-spam solutions.

([2] Source: Gartner Group.)

4 How to fight against spam?

4.1 Preventive measures

The best way to fight spam is to avoid being its target. The following is a list of the actions most often targeted by spam:

- Sending messages to **newsgroups**
- Giving your e-mail address to an **online stores**
- Subscribing to an **Internet service** that requests an e-mail address
- Sending an e-mail requesting to unsubscribe from a spam distribution list because unfortunately, this is almost exclusively used to confirm the validity of the new e-mail address
- Subscribing to or participate in a **mail distribution** list
- Online **chatting**
- Posting e-mail addresses on **Web pages** that are automatically extracted by robots who search for chains using the @ sign

Furthermore, spammers may buy mailing lists of recipients' e-mail addresses. This kind of practice seriously damages the reputations of companies that carry out online marketing campaigns without the permission of the addressee.

Users can opt to be included (opt-in) in permission marketing programs (i.e. they give authorization to receive promotional mail), or choose to be excluded from all types of advertising campaigns (opt-out) through Robinson lists, for example.

Another mechanism traditionally used by spammers is to randomly generate e-mail aliases using common words and names such as support, sales or first names. Afterwards, these aliases are combined with domains registered in the NIC in order to obtain valid e-mail addresses.

The next step involves checking which of the thousands of generated addresses are valid. The most advanced spammers attach links to tiny images in their Web pages which are almost impossible to detect at first sight. When addressees download and examine the HTML content of their mail, their mail client then requests the image from the server, which generates an automatic process of e-mail address validation in the database targeted by the spam.

It is therefore advisable to disable the preview pane in mail so they are not notified that the address is valid, even before opening the message.

4.2 Corrective measures

4.2.1 When is it the right moment?

The right moment is now! Everyone can start fighting against the spam that invades work centers and personal e-mail accounts by strictly applying the following rules:

- Never reply to an unwanted e-mail under any circumstances.
- Do not acquire any products from promotions advertised by this kind of mail. This will encourage spammers to send more mail, since their aim is to use e-mail for economic benefit. According to ComputerWorld, one out of every 400 promotional spam recipients ends up purchasing the product or service advertised.
- Do not get taken in by chain mail. This kind of mail bombardment is spam and spammers subsequently use the list of addresses that appears in these chain letters.
- Do not launch an electronic attack on the spammer’s e-mail account because the address that appears in this type of mail has probably been stolen or does not even exist.

4.2.2 Legal actions

Legal actions against spam have a limited effect because if legislation is enforced opposing this type of practice, spammers can simply move their operations to an ISP located in a country which does not have any legislation on the matter, or illegally tap into the computers of innocent people using hacking tools and launch the spam from there.

4.3 Conclusion

As you can see, all actions involve educating end users why they do not need to waste time on these unnecessary tasks. A perimeter barrier is needed that does not require user intervention and that can filter most of the spam messages that reach corporate network users every day.

5 The GateDefender Performa anti-spam solution

Panda GateDefender Performa provides the most powerful corporate anti-spam protection, as its preventive protection against spam is implemented in the perimeter, preventing spam from even getting inside the corporate network.

5.1 Layered protection

Spam can cause significant damage to companies. On the one hand, the growing number of spam messages reaching companies every day is saturating corporate mail servers. Alternatively, the distribution of this junk mail to different recipients leads to an increase in the volume of network traffic, using costly resources that could be used for more profitable purposes. Furthermore, users waste valuable time opening, reading and/or deleting these messages.

Anti-spam protection has become essential for companies. Panda Security offers different levels of solutions to protect against spam.

The classification of e-mail as spam is a very controversial topic, as there are messages that could be considered spam by some companies but not by others. In this case, mechanisms are needed to detect and separate the messages that are on the borderline between spam and not spam, giving rise to the concept of classifying messages as “probably spam.”

Each workstation can be protected by a solution that is especially designed for this purpose. This software identifies spam and prevents the user from wasting valuable time reading the message in order to discover that it is useless.

Mail servers can also be protected, preventing, to a large extent, junk mail from circulating around the network.

Finally, the network perimeter can be protected with GateDefender Performa. By doing this, junk messages are blocked before they even enter the network, taking the load off corporate mail servers and optimizing internal network traffic.

5.2 Intelligent anti-spam filtering

Panda GateDefender Performa determines if a message is spam, while using multiple techniques (rules, heuristic, Bayesian, lists, machine learning, etc.), with over 300,000 algorithms to reduce false positives (a false positive is classifying a message as spam when it is not).

Each message is scanned in detail, using a combination of anti-spam techniques to optimize spam detection. The spam signature file is constantly growing as new spam messages are detected worldwide. GateDefender Performa automatically updates this file every 90 minutes, unnoticeably to the user.

By thoroughly scanning every received message, the protection is optimized and false positives are reduced to a minimum.

All the messages received are classified as 'Spam,' 'Probably Spam' or 'Not Spam.'

5.3 Functioning

The Panda GateDefender Performa anti-spam series incorporates four scan engines to automatically scan potential spam e-mails. The message passes through all four engines in order to classify it as spam, probably spam or not spam.

These four engines are:

• **SpamBulk** - Compares the message with an internal list of known spam messages that have previously been sent out in bulk.
• S**pamRepute** - Checks if the sender is in the internal list of known spammers.
• **SpamContent** - Scans the content of the message, checking the style, design, language and text, breaking it down into minimum pieces in order to detect key words, even if the words are not an exact match (FREE= F – R –E – E).
• **SpamTricks** - Checks if the message contains technical tricks usually used by spammers. GateDefender Performa can detect:

• Tactics spammers use to reduce the cost of sending large volumes of information (image-only messages, HTML obfuscation, etc.).
• Tactics spammers use to get past spam filters.

After passing through the four spam engines, a percentage is obtained that determines whether the message is definitely spam, close to being spam or probably spam, or a normal message that cannot be classified as spam or probably spam.

Both the training and the feeding of data on new spam messages or spammers are done remotely and are updated every 90 minutes without user intervention.

The system administrator can define the sensitivity level of the scan, choosing high, medium or low, so the solution adjusts to the precise needs of each company.

A scan with a high sensitivity level will detect a larger number of spam messages, but the number of false positives will also increase. A scan with a low sensitivity level will do the opposite; it will classify few messages as spam, but it will not return any false positives.

Apart from the automatic scan that GateDefender Performa always carries out, the administrator can manually define a “white list” of trusted senders whose messages will never be classified as spam.

The administrator can also define a “blacklist” of sender whose messages will always be classified as spam, without needing to scan them.

The senders can be included in the white list and the blacklist:

- By the e-mail address of the sender of the message
- By the domain of the sender of the message
- By the source IP address

The administrator can choose from the following actions to take with a message classified as spam or probably spam:

- Flag the message subject so that the recipient can easily identify it as junk mail
- Block the message so that it does not reach the recipient. This option is available for spam received via SMTP
- The message can also be forwarded to a spam mailbox for subsequent administration

The actions to take on messages classified as spam and classified as probably spam are defined separately, as they could be different.

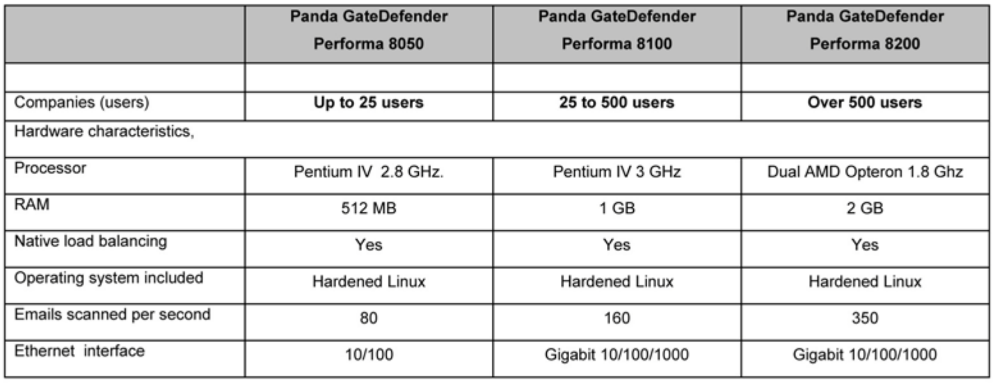
Scalability

The new Panda GateDefender Performa is a high-performance, integrated and dedicated perimeter protection solution that combines hardware and software for maximum ease of use. It protects clients against spam, detecting and blocking junk mail to prevent it from entering the network and spreading, before it is detected by other security systems.

Since it is an integrated solution, the hardware and software are designed to provide optimum functioning. This perimeter protection safeguards the network at the Internet gateway, freeing the rest of the computers from risks and workload. Because it is dedicated protection, it guarantees maximum performance in all the tasks it is configured to perform.

It offers gateway protection, designed to be implemented simply in any network, without interfering with network performance or productivity, and without degrading performance of critical systems like firewalls and application or Web servers.

Three models are available, so the solution adapts to the needs of all small, mid-sized and large companies (up to 40,000 workstations), adjusting scan capacity to the overall volume of network traffic.



	Panda GateDefender Performa 8050	Panda GateDefender Performa 8100	Panda GateDefender Performa 8200
Companies (users)	**Up to 25 users**	**25 to 500 users**	**Over 500 users**
Hardware characteristics,			
Processor	Pentium IV 2.8 GHz.	Pentium IV 3 GHz	Dual AMD Opteron 1.8 Ghz
RAM	512 MB	1 GB	2 GB
Native load balancing	Yes	Yes	Yes
Operating system included	Hardened Linux	Hardened Linux	Hardened Linux
Emails scanned per second	80	160	350
Ethernet interface	10/100	Gigabit 10/100/1000	Gigabit 10/100/1000

Table 2: Model comparative

6 Main benefits of GateDefender Performa

The main advantages of the new version of GateDefender Performa are the efficiency, wide functionalities, ease of use (‘plug-in and forget’) and high performance and scalability.

Complete protection: It scans the three most widely used mail protocols: SMTP, POP3 and IMAP4.

High performance, transparent to users: Panda GateDefender Performa takes over the workload of the traditional anti-spam protection, optimizing use of the network resources. It guarantees excellent performance and the highest scanning capability in its class. It can scan up to 350 messages per second (SMTP traffic) completely unnoticeably to corporate network users.

Auto-updates: The updates to the system are programmed by default to be carried out automatically every hour and a half. This means that Panda GateDefender Performa will be the most up-to-date protection across the network.

Simple administration - Plug-in and forget: Panda GateDefender Performa is designed to be implemented simply on any network, with no need for redirecting network traffic. GateDefender Performa proactively sends all relevant information about the anti-spam activity to the administrator. It is managed remotely and securely through a simple and intuitive Web console.

Low cost of ownership: By preventing saturation of network resources and loss of productivity, Panda GateDefender Performa offers higher resource management capabilities.

All of this (along with its 'plug-in and forget' operation, requiring minimum administrator intervention) results in low cost of ownership of Panda GateDefender Performa.

High scalability and load balancing: GateDefender Performa adapts perfectly to the needs of all small to large companies (up to 40,000 workstations), adjusting scan capacity to the overall volume of network traffic.

Its load balancing is completely automatic, allowing the workload to be shared across multiple units. The result is increased scalability and improved anti-virus performance for complete protection of your network perimeter.

***Detailed graphic reports and customizable alerts**: GateDefender Performa offers graphic statistics on the network traffic and system activity. It also offers comprehensive spam graphic reports, as well as customizable alerts and notifications.*

Besides, the chance to send all important events through the standard log format "Syslog" allows the administrator to analyze everything that is happening in the GateDefender Performa units with a standard analysis system which can monitor many network devices at the same time, in order to control all network elements. Similarly, all events produced in GateDefender Performa units are sent through SNMP protocol in order to allow centralized monitoring of all devices installed on the company network.

***Other options**: As well as the anti-spam protection, GateDefender Performa also offers other types of protection:*

Web filtering: The Web filtering module can restrict access to the Internet. It can filter traffic by undesirable Web content categories and lists of authorized and unauthorized Web pages. Each page is included in one of the Web categories available (59) and the domains included in each category are updated automatically. This controls the use of corporate network resources and blocks undesirable Web content, such as offensive, sexual or violent content, or content that simply shouldn't be accessed at work. It also allows a list of VIP user to be defined, to whom the control policies will not be applied.

Anti-malware protection: This prevents unknown viruses, worms or any other malicious code from getting into the company and saves network resources and bandwidth, blocking potentially dangerous content before it enters the network.

7 Technical details

Operating system and interception software

The software incorporated in GateDefender Performa is based on the GNU/Linux operating system, reinforced and optimized to offer maximum security and high performance. The operating system used in GateDefender Performa only includes the services and processes it needs to function correctly.

Panda GateDefender Performa acts as a transparent bridge between the Internet and the corporate network. This means that the traffic passes through transparently and the appliance intercepts the protocols it has been configured to scan.

Self-repair system:

Under extreme circumstances (excessive heat, etc.) damage could be caused to the Panda GateDefender Performa hardware, such as hard disk corruptions or physical errors in some partitions, etc.

To prevent system failures in these cases and to ensure continuous perimeter anti-virus services, Panda GateDefender Performa includes a system for controlling partitions or a self-repair system. When Panda GateDefender Performa starts, a control partitions starts up that determines which work partition will be used to run the anti-spam system.

If the self-repair system detects that the work partition has failed for any reason, the next work partition established will be started up. It also incorporates a process for restoring the partition that has failed in order to guarantee that it works in subsequent startups. The partitions are kept updated with the latest versions of the software, in order to make recovery as little traumatic as possible.

There are other perimeter solutions that promise high-availability using SCSI RAID disks. Panda Security believes that SCSI RAID disks are only necessary for storage servers that have to protect data and provide high-availability. However, SCSI RAID disks don’t offer any benefits in devices that are not geared to storing data, such as Panda GateDefender Performa or other appliances on the market. This is really just another marketing angle that does no more than add to the cost for the end-user and Panda Security would prefer to eliminate unnecessary costs. Panda GateDefender Performa offers high-availability by using tools like WatchDog and its Self-Repair system, as well as load balancing.

WatchDog: fault tolerance system

The motherboard of GateDefender Performa incorporates a system monitoring circuit to prevent the system from blocking or failing for long periods of time. The WatchDog system receives signals indicating that it is functioning correctly and if it does not receive this signal within a specific interval, WatchDog will completely reset the system from the motherboard, avoiding loss of network services for excessive periods of time.

Thanks to this fault tolerance system, Panda GateDefender Performa can automatically recover from service failures either in the applications or the operating system.

As well as WatchDog hardware, Panda GateDefender Performa also incorporates WatchDog software, which periodically monitors the status of all the processes that are running. If it detects that a process is not responding, WatchDog will try to recover it without needing to restart the system. If it cannot be recovered through the software, GateDefender

Performa will be completely restarted from the WatchDog hardware. Thanks to this fault tolerance software system Panda GateDefender Performa can recover automatically from service failures without needing to completely restart the system.

Load balancing

Load balancing allows the workload to be shared across multiple GateDefender Performa units, providing improved performance and higher availability. No additional hardware or software is needed to implement load balancing across multiple GateDefender Performa units and although it is highly advisable to use switches, these can also be connected through hubs.

One of the appliances will act as the master, with the rest acting as slaves. From the administration console, users can view all the appliances in the load balancing system and the mode each one is running in.

When several GateDefender Performa units are installed in parallel, they will automatically negotiate the role or mode of functioning of each one and whenever a new appliance is incorporated, the modes of functioning will be re-negotiated.

The master appliance implements a load balancing algorithm and redirects connections to the different slave appliances in order to balance the system workload. The master appliance will also scan connections and let clean traffic through.

Slave appliances will not let traffic through and will simply scan the connections redirected to them, returning clean traffic to the master appliance.

Summary & Conclusion

The negative impact of spam on companies' productivity is a proven fact, and the volume of unwanted e-mail is on the rise. As is nearly always the case, adopting **preventative measures** is actually more profitable than having to correct an undesirable situation which may increase the risk of damaging the reputation of the organization.

Although **legal protection** concerning these kinds of threats has made considerable progress over the past year, employees must be kept well informed when it comes to prevention and regarding which actions to take should they receive spam.

Manually dealing with spam in companies and using no other method is not an option. The same can be said for leaving the task of deciding which protection policies to adopt in the hands of each user. Although all members of the company should be involved in the fight against spam, someone—the e-mail or network administrator—must coordinate these efforts. This coordination task is much easier if the administrator has a tool like GateDefender Performa which allows the anti-spam protection to be installed, maintained and supervised without having to go from machine to machine to determine its level of protection.

APPENDIX A: PANDA SECURITY WORLDWIDE

Panda Headquarters Europe
Ronda de Poniente 19
Tres Cantos
28760 Madrid, Spain
Phone: +34 91 806 37 00
E-mail: info@pandasoftware.com

Panda Headquarters USA
230 N. Maryland, Suite 303
P.0. Box 10578
Glendale, CA 91209, USA
E- mail: usa@pandasoftware.com

Panda Software Argentina
Calle Roque Saenz Peña 1160, piso9b
Buenos Aires
Phone: +00 5n411 43823448
E-mail: argetina@pandasoftware.com

Panda Software Austria
Dr.-Detlev-Karsten-Rohwedder-Str. 19
47228 Duisburg
Phone: +49 20 65 9 87 654
Phone: +00 5411 43823448
E-mail: austria@pandasoftware.com

Panda Software Belgium
Mechelsesteenweg 311
1800 Vilvoorde
Phone: +32 2 756 08 80
E-mail: belgium@pandasoftware.com

Panda Software Bolivia
Calle Miguel de Cervantes Nro. 2725,
Sopocachi, La Paz
Phone: +591 2 411823
E-mail: bolivia@pandasoftware.com

Panda Software Brazil
Rua Dr Barcelar 173 Conjunto 114

Vila Clementino
04026-000 Sao Paulo – SP
Phone: +55 61 5082 4414
E-mail: brasil@pandasoftware.com
Panda Software Bulgaria
126, Tzar Boriss III Blvd.
office 111
1612 – Sofía-Bulgaria
Phone: +359 2 9556575
E-mail: bulgaria@pandasoftware.com

Panda Software Canada
1117 Ste Catherine O. Suite 920
Montreal Quebec H3B 1H9
Phone: +1 514 842 2288
E-mail: flourtau@pandasoftware.ca

Panda Software Chile
Mosqueto 428, oficina 502
6500426, Santiago
Phone: +56 2 639 7541
E-mail: chile@pandasoftware.com

Panda Software China
Room 501, No.20, 421 Siping Rd.,
Shangai 200020
Phone: +86 21 6351 9020
E-mail: china@pandasoftware.com

Panda Software Colombia
Carrera 41 N.46-26 Itagui
Antioquia
Phone: + 57 4-3735588
E-mail: colombia@pandasoftware.com

Panda Software Costa Rica
Calle 25, Ave 6 y 8 #648
San José
Phone: 00 506 258 0100
E-mail: costarica@pandasoftware.com

Panda Software Denmark
Ny Vestergardsvej 15

DK 3500 – Værløse
Phone: +45 44 355 375
E-mail: denmark@pandasoftware.com

Panda Software Finland
P.O.BOX 636
33101 Tampere
Phone: +358 3 339 26 700
E-mail: finland@pandasoftware.com

Panda Software France
33 bis Boulevard Gambetta.
78300 Poissy
Phone: +33 1 30 06 15 15
E-mail: france@pandasoftware.com

Panda Software Germany
Dr.-Detlev-Karsten-Rohwedder-Str. 19
47228 Duisburg
Phone: +49 20 65 9 87 654
E-mail: germany@pandasoftware.com

Panda Software Greece
Botsari 12-14
18538 Pireaus
Phone: +30 1 04531201
E-mail: greece@pandasoftware.com

Panda Software Guatemala
Avenida Reforma 8-60 Zona 9
Edificio Galería Reforma, Torre 1 Oficina 1102
Ciudad de Guatemala
Phone: +502 385 6657
E-mail: guatemala@pandasoftware.com

Panda Software Hungary
Szugló utca 54
1145 Budapest
Phone: +36 1 469 70 97
E-mail: hungary@pandasoftware.com

Panda Software Israel
43 Hamelacha street, New Industrial Zone

42504 Natanya
Phone: +972 9 - 8859611
E-mail: israel@pandasoftware.com

Panda Software Italy
Viale E. Marelli 165
20099 Sesto S. Giovanni (Mi)
Phone: 02-24 20 22 08
E-mail: italy@pandasoftware.com
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
Panda Software Latvia
Merkela Street 1
1050 Riga
Phone: +371 7211636
E-mail: latvia@pandasoftware.com

Panda Software Lithuania
Žemaites g. 21
LT-2009 Vilnius -Lithuania
Phone: +370 5 2397833
E-mail: lithuania@pandasoftware.com

Panda Software Luxembourg
Mechelsesteenweg 311
1800 Vilvoorde
Phone: +32 2 756 08 80
E-mail: luxembourg@pandasoftware.com

Panda Software México
Tuxpan #39, Despacho 503
06760 México, D.F.
Phone: +52 5 2642127
E-mail: mexico@pandasoftware.com

Panda Software Netherlands
Fellenoord 23 – Postbus 2020
5600 CA Eindhoven
Phone: +31 40 233-3501

E-mail: netherlands@pandasoftware.com

Panda Software Norway
ViroSafe Norge AS
Midtbyen Park
Skolegt. 2
2315 HAMAR
Phone: 00 47 62 53 96 80
E-mail: norway@pandasoftware.com

Panda Software Paraguay
Eliseo Reclus 247 Calle Guido Spano,
República del Paraguay
Asunción
Phone: +00 595 21 607594
E-mail: paraguay@pandasoftware.com

Panda Software Peru
Calle Lord Cochrane 521
Miraflores – Lima 18 - Perú
Phone: 00 51 1 221 6001/ 221 0159
E-mail: peru@pandasoftware.com

Panda Software Poland
Ul. Wiktorska 63
02-587 Warszawa –Poland
Phone: +48 (22) 540 18 06
E-mail: poland@pandasoftware.com

Panda Software Portugal
Quinta da francelha - Edificio Sagres, 7B
2685-338 Prior Velho
Phone: + 351 219426800
E-mail: portugal@pandasoftware.com

Panda Software Puerto Rico /
Dominican Rep.
Av. Luis Muñoz Rivera 1058, Suite 1
Pto. Nuevo
Puerto Rico, 00920
Phone: +1 787 296 1139
E-mail: caribe@pandasoftware.com

Panda Software Russia
Tveritina 38/3
Ekaterinburg, 620026 Russia
Phone: +7 3432 78-31-27
E-mail: russia@pandasoftware.com

Panda Software Slovak Republic
Lublanska 1
83102 Bratislava
Phone: +421 2 444 55 702
E-mail: slovakia@pandasoftware.com

Panda Software Slovenia
Stari trg 5A,
SI-8210 Trebnje
Phone: +386 7 34 61 020
E-mail: slovenia@pandasoftware.com

Panda Software Spain
Ronda de Poniente 19
Tres Cantos
28760 Madrid
Phone: 902 365 505
E-mail: info@pandasoftware.es

Panda Software Sweden
P. O. Box 26026
100 41 Stockholm
Phone: +46 8-545 25030
E-mail: sweden@pandasoftware.com

Panda Software Switzerland
Route Champ-Colin, 10
1260 Nyon
Phone: +41 22 994 89 40
E-mail: switzerland@pandasoftware.com

Panda Software Thailand
192 Soi Laprao 107
Bangkapi, Bangkok 10240
Phone: 00 662 7311480
E-mail: thailand@pandasoftware.com

Panda Software Turkey
Darulaceze Cad
Karatas Sok. SNS Plaza Nº 6
80270 OKMEYDANI – ISTANBUL
Phone: 90 212 222 1520/90 212 210 2200
E-mail: turkey@pandasoftware.com

Panda Software United Arab Emirates
Bldg-5 Office No. 5G-15
P O Box 41573 – Hamriyah
Free Zone, Sharjah, United Arab Emirates
Phone: +971 (6-526.30.14)
E-mail: UAE@pandasoftware.com

Panda Software United Kingdom
5 Signet Court, Swanns Road
Cambridge CB5 8LA
Phone: +44 (0)870 444 5640
E-mail: uk@pandasoftware.com

Panda Software United States
230 N. Maryland, Suite 303
P.0. Box 10578
Glendale, CA 91209, USA
E- mail: usa@pandasoftware.com

Panda Software Uruguay
Jose Enrique Godó 1955
11200 Montevideo
Phone: +5982 4020673
E-mail: uruguay@pandasoftware.com
Panda Software Venezuela
Av. Libertador, C.C. Libertador, PH-7
Caracas
Phone: +5821 276188 60
E-mail: venezuela@pandasoftware.com

APPENDIX B. Glossary of terms.

Term Description:

Algorithm: Detailed sequence of actions to undertake in order to perform a task. Named after the Iranian mathematician Al-Khawarizmi.

Heuristic Scan: The method, strategy or technique used to easily resolve a problem. Within the IT sector, it is a technique used to detect viruses that are unknown at the time of the scan.

Hacking tools: A program that allows hackers to perform actions that pose security threats to other computers (spam, check of communication ports, attacks of denial of service -DoS-, etc.).

Malware: Programs, documents or messages liable to have negative effects on IT systems. MALicious softWARE.

Dialers : A program that can use the modem of computer without authorization.

Spam: Spam or junk mail involves receiving e-mails containing product advertising in an indiscriminate manner, from unwanted sources.

Spyware: Refers to programs, ActiveX components or code embedded in e-mails 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. Examples of spyware include:

WebBugs - Elements embedded in e-mails that are capable of sending personal user information to a predetermined server when the message is opened.

Cookies - Programs which monitor Internet surfing habits; programs which act without giving any warning, registering the web pages users visit, the programs they execute etc.

Virus: Programs that can get into computers and IT systems using many different means, and have annoying, dangerous or even destructive or irreparable effects.

APPENDIX C. Abbreviations and acronyms.

CIO – Chief Information Officer
CTO – Chief Technology Officer

ISP – Internet Service Provider
IT – Information Technology