PANDA CLOUD EMAIL PROTECTION

Simply... Evolution

HOW TO PREVENT SPAM AND MALWARE IN MAIL MOST EFFECTIVELY

PANDA CLOUD OFFICE PROTECTION

PANDA CLOUD EMAIL PROTECTION

PANDA CLOUD INTERNET PROTECTION

PANDA SECURITY | 20 Aniversario 1990-2010

Index

1. Battling the increase in malware

It managers are working hard to combat the increasing volume of malware attacks on their enterprises. These attacks are also becoming progressively more sophisticated. As a result, the risks of them causing damage to the business are greater than ever before. The majority of threats that reach an organization do so through the mail server. There are several reasons for this trend:

- The enterprise's mail service is the most frequently used communication channel across the Internet.
- An email is easy to access and manipulate.
- The SMTP mail protocol is simple and can be emulated by any Internet user.
- Many confidential company communications are still transmitted using email.
- Firewall-type corporate security devices do not filter SMTP traffic which reaches email servers.
- Mail directories often include highly sensitive corporate information, such as organizational charts, key functions, directories with strategic information, etc.
- The mail service is a channel for mass infection, via worms and Trojans that replicate in each target, using infected computers and reading mail lists in the host computer.

A targeted attack on the mail server of a company can have serious or even fatal economic consequences. As a result, companies need their mail servers to be completely protected against all forms of attack. Enterprises are using a variety of layered protection strategies to defend themselves against possible infections from any kind of malware and other threats. But most of the solutions fall short of providing complete protection to the enterprise.

Another important element in email security is the reaction time against new, unknown infections. The 'risk window' is the time between the appearance of a new threat and the release of the first signatures file to detect it. A clear example is the MyDoom virus, which in just a few hours infected millions of computers worldwide. To reduce this exposure, enterprises need the ability to isolate these new outbreaks quickly, to prevent the occurrence of infections in the corporate IT infrastructure.

2. Addressing the surplus of spam

Email has become an indispensable tool in business management and even in personal relations, all but replacing traditional means of communication. But as with any widely implemented tool, it is susceptible to being used deliberately in ways that are detrimental to the users of the mail service.

One such malign use of email services is spam. Mass mailing has proven to be a powerful, low-cost marketing tool. Spammers are able to get very quick returns, receiving payment for the number of mails that they send across the Internet. This has caused an avalanche in the development of this type of mail, reaching exorbitant figures in some countries. According to the Messaging Anti-Abuse Working Group (MAAWG), 82-87% of all incoming email is currently categorized as spam or 'abusive email'.[1]

Spam is a nuisance at a personal level, as it has to be handled (opened, read, deleted) and clearly has a huge financial impact, due to the costs of processing large volumes of useless mail by the company. All of the time used by employees (users, IT administrators, etc.) as well as the use of server and communication resources also represent significant costs. In addition, spam slows down communication systems. When the mail server is forced to process large volumes of junk email, it is clearly detrimental to its ability to process useful mail. Unfortunately, spam is growing in frequency every year, with an increasing number of spammers generating ever more junk mail. This means there is a growing need for tools that can effectively filter and eliminate this type of mail.

The quality of an anti-spam system is measured by its preciseness and speed in diagnosing what is and what isn't spam. For this reason, the parameter of false positives (useful mail classified as spam) is used. Bear in mind that the criteria for classifying mail as spam is not without subjectivity, and therefore the mail recipient's criteria must be considered. Eliminating spam with severe criteria (high anti-spam levels) could have more negative than positive consequences, as the number of false positives could increase.

Therefore, an effective filtering technique should offer high levels of spam rejection, combined with low levels of false positives. This factor is critical, as users are naturally sensitive to having potentially useful mail eliminated. To prevent such undesired consequences and simultaneously block a high percentage of spam, it is important to keep filtering criteria automatically up-to-date and receive information about new origins of spam quickly from as many sources as possible. All of these factors illustrate that corporate anti-spam management is not a simple task and requires a comprehensive process to reach acceptable quality levels.

1. http://www.maawg.org/about/MAAWG20072Q_Metrics_Report.pdf

3. The mail server – A critical vulnerability

Email traffic is based on the SMTP protocol, which offers little or no reliable safeguards when it comes to exchanging information over the Internet between two nodes. In addition, it is a protocol that is easily emulated, and it is possible to generate SMTP traffic for exchanging information across the protocol from an Internet node (a simple PC) without the intention to send mail but rather to saturate a server.

Corporate firewalls cannot block mail traffic, since email is a fundamental source of the company's communication. For this reason, spammers know it is the ideal channel for sending all types of viruses and malware (spyware, hoaxes, phishing, etc.) to the unsuspecting enterprise. The following sections will examine some of the attack scenarios that could be clearly detrimental to users of a mail service.

3.1 Denial of Service (DoS) Attacks

An attack on a mail server can involve massive sending of connection requests to the server. This means that large communication volumes are generated (frequently from different sources) without even an email being sent. The server can respond in several different ways:

- Option A: Not respond to communication requests aimed at addresses not registered in the mail server.
- Option B: Respond with an error message to the sender.
- Option C: Return a message that the server is busy.

Option A means the application of 3.2 a policy that will block malicious mail, but also to potentially useful mail in which the sender has, for example, made an error on typing the address.

Option B means that for each time the SMTP protocol is started, the email server will be interrogated for an address and it will answer the requesting node as to whether or not it exists in the domain. This is the most common way in which mail servers work today, as it offers a reasonable degree of certainty about the reception of the message. However this is a typical hackers' tactic (DHA) to know all real mail addresses existing in the network in order to be used later for spamming attacks.

Option C occurs in special circumstances, either because the mail server is saturated or because it has been adopted as a tactic to respond to an identified attack. The objective of DoS attacks is clear: slow down the email server, and, if possible, render it inoperative with the corresponding financial consequences.

3.2 Directory Harvest Attacks (DHA)

DHA is a technique used by hackers to capture the mail directories of the targeted organization. They do this with software that generates random email addresses, using feasible combinations (common names, positions, department names, etc.).

By mass-mailing to these types of addresses and using a trial and error technique, hackers can capture not just email addresses, but also sensitive information such as organizational structure, drives with restricted information, etc. The consequences that this could have are easy to imagine, and could even rise to expensive legal liability on the part of the targeted company if negligence in data-processing procedures can be proven.

3.3 Phishing

This term describes how malicious users pass themselves off as someone else (normally a company) in order to obtain confidential information from the recipient of the 'phishing email'. Typically phishers send emails that appear to come from a bank or financial institution and under some pretext or other, ask the recipient for confidential information, such as account access codes. Spoofing of the third-party Web page (which victims are led to through a link in the email) is sometimes highly accurate. This deceitful practice has a high level of success, with often devastating financial consequences.

4. Levels of protection for the mail service

Mail security can be provided at several different network levels:

- **Mail security in the PC.** This is not an effective solution from an administrative point of view for eliminating spam or combating denial of service or directory attacks. Moreover, spam filtering may not effectively meet the criteria of 'high rejection of spam and few false positives' and is at users' discretion.

- **Security in the Mail Server.** All unwanted mail traffic passes through the network to reach the email server, meaning that there is already a processing overload on other network devices. Awareness of attack types and origins is limited to the experience of the client's network administrator. Moreover, the mail server is also burdened with additional workloads.

- **Specific Security Hardware at the Gateway.** This method resolves the overload in the communication resources, eliminating the processing load on the network. However the hardware needs a specific regular administration to be updated according to the new attacking techniques.

- **Network Security through Managed Services.** This method provides an effective solution to all of the previous problems:

  - Spam is eliminated outside of the client's network, without using their resources.

  - DHA or DoS attacks do not target the mail server.

  - Additional processing load on the client's network devices is eliminated.

  - No additional Hardware investments are required.

  - Always up to date information to rapidly respond to new attacks is provided at the network level.

5. Achieving network security through managed services

The most reliable solution for achieving network and mail security is by leveraging a managed service. In this model, security measures are applied through a mail filter system in a node outside of the client's network. To do this, all traffic from the client's mail domain is redirected to the filter system by modifying the MX file[2] in the client's domain name system (DNS). From that point on, mail addressed to the client's domain is first sent to the managed services provider's filter platform. This platform processes and scans all mail with one or more antivirus and anti-spam engines. Optionally, it also filters the content following criteria based on words, file types, or image types.

Mail classified as spam can then be treated according to different policies. In a managed service environment, the client's domain administrator can establish his or her own policies or delegate this filtering configuration decision to the managed service provider. One possible policy is presented below:

- Mail which is clearly spam (e.g., sent by known spamming trojans) is immediately eliminated.
- Mail that fits the spam profile in high percentage is stored in quarantine. The recipient is then notified that they have 'probable spam', but they have a designated timeframe to read it before it is deleted.
- Mail that could cause a false positive can be marked in the mail header so it is dealt with by the email recipient.

A managed service also offers greater defense against denial of service and directory attacks. The experts managing the filter platform will detect anomalous behavior in domain traffic and can take countermeasures to fight against these attacks. For example, in the event of a DoS attack, the filter system can slow down the response to this address, nullifying the attack by increasing response times, and therefore the waiting time in the node carrying out the attack. This slowdown could block any type of response to certain addresses.

With a managed network service, large quantities of information can be quickly gathered about security attacks. This observatory-type strategy provides a clear advantage when it comes to the early detection of new threats. For example, a new phishing email may start to spread on the Internet purporting to be from an online bank and asking recipients to enter their account details. This sender's address is false and the Web page that the victim is redirected to appears to be that of the bank. A managed service will detect this new threat more rapidly and can employ security measures to ensure that no clients' domains are affected.

2. MX is short for 'mail exchange' record, an entry in a domain name database that identifies the mail server that is responsible for handling e-mails for that domain name.

6. Panda Cloud Email Protection

Panda Cloud Email Protection is a managed mail filter security service that guarantees clean, secure email delivery. Panda Cloud Email Protection provides four main functions: anti-malware, anti-spam, content filter, and mail continuity:

- Anti-Malware Protection – Using the most advanced preventive protection technologies, Panda Cloud Email Protection detects all types of known and unknown malware content in email. It detects both known viruses (through its signature engine) and new threats by incorporating the latest proactive technologies and direct handling of suspicious files by PandaLabs. This commitment is backed by an SLA guaranteeing that users will only receive 100% malware free email.

- Anti-Spam Protection – Panda Cloud Email Protection combines several anti-spam engines to achieve detection ratios over 98.5%, ensuring end users don't receive spam. What is more the false positive ratio is around 1 in 30,000, making Panda Managed Email Protection mail reach the highest efficiency level.

- Content Filtering – Lets clients define and enforce company security policies by establishing what attachments can be received and which should be blocked.

- Mail Continuity – Panda Cloud Email Protection prevents possible network failures from affecting business continuity. In the event of the failure of clients' servers or networks, mail will still be accessible for several days.

6.1 How Does It Work

Mail filtering takes place while messages are in transit on the Internet – before they can enter clients' networks. Panda Cloud Email Protection scans and takes action according to the criteria defined for each mailbox. If the mail is clean, it will be immediately sent to the recipient.

If suspicious behavior or a conflict with established policies is detected, the system will act accordingly – deleting the message or storing it in quarantine. The quarantine feature allows suspicious or invalid messages to be securely stored, and if necessary, viewed away from clients' systems.

Panda Cloud Email Protection is directly connected to the outstanding Panda's Collective Intelligence. This means that all new threats knowledge of PandaLabs is included – in real-time – in the platform transparently to users.

This fully customizable service provides 24x7 technical support The service also includes rapid analysis and support from PandaLabs, one of the most prestigious laboratories in the IT security sector.

Panda Cloud Email Protection delivers:

- **Maximum Data Security and Confidentiality** –Panda Cloud Email Protection employs the most rigorous measures to guarantee the security and confidentiality of clients' data and information. Mail scanning is performed with strict confidentiality, in line with ISO/17799 security policies, applying to both data management and physical security. It monitors both inbound and outbound mail to prevent inappropriate or confidential material from entering or leaving the company.

- **Straightforward Interface** – Domain administrators and mailbox users have access to Web consoles with a series of configuration options depending on their corresponding permissions. This console is highly intuitive and a user guide is available for any queries.

- **Customizable Definitions** – Panda Cloud Email Protection allows a high level of customization without detracting from its simplicity. Security policies can be established for user accounts, even allowing end users (if they have permissions) to configure their own spam white and black lists.

- **Quarantine Management** – PandaCloud Email Protection stores all spam or messages that could contain viruses in its own quarantine. This ensures that the end clients' servers are not saturated by spam, saving resources and storage capacity. Messages carrying viruses are stored in the system's quarantine for up to 5 days.

  However, known mass-mailing worms that spoof the sender's identity are deleted directly, although a record is kept in the log for statistical purposes. After the predetermined time in the quarantine, the message is automatically deleted. Attachments suspected of containing a virus and do not match known identifiers are sent to PandaLabs for detailed analyses. PandaLabs will take quick action either releasing it or confirming that it is infected.

- **Continuous Information about. Threats** – The service allows end clients to review the quarantine and receive a range of reports through the secure Web interface. These reports are customizable and provide continuous information about the mail traffic situation and any attacks that occur.

Panda Cloud Email Protection does not require initial investments in hardware technology, clients do not have to install complex and costly software, and it involves no maintenance costs. To use the system, clients only need to redirect their mail server to Panda's filter platform through a simple DNS redirection. The service is then available to clients within 24-hours.

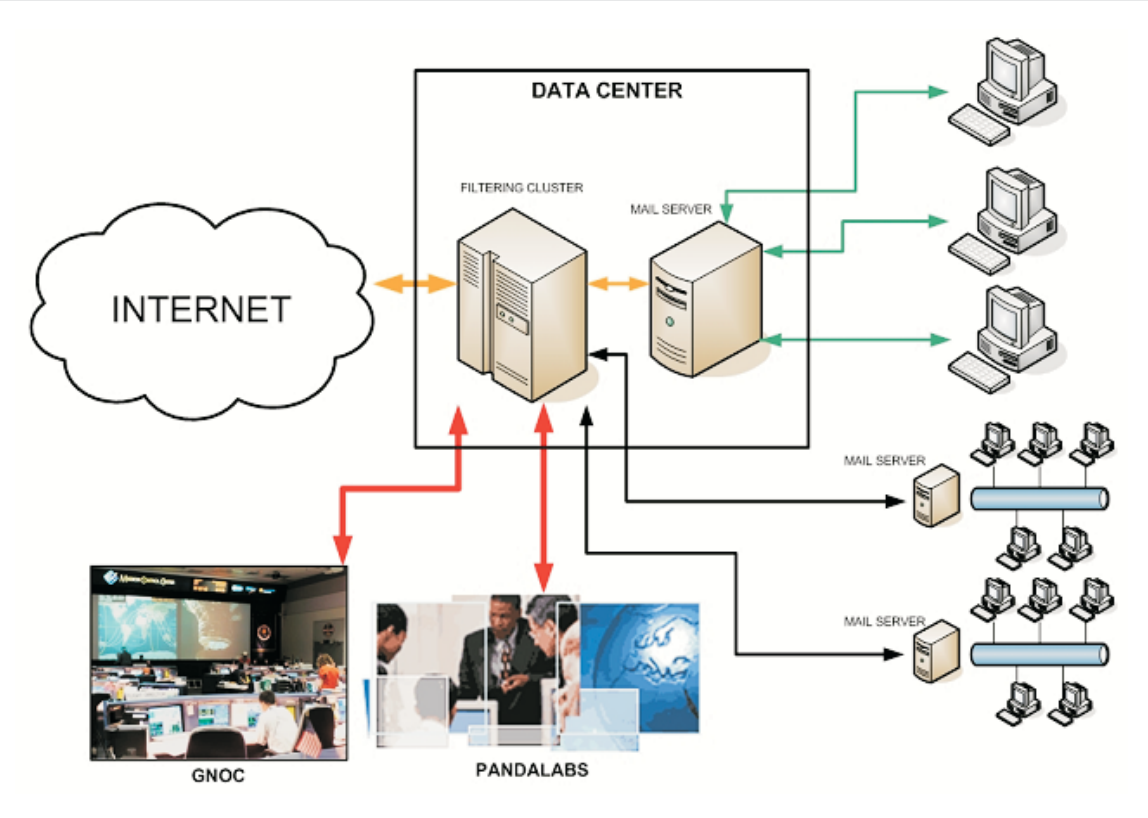

Figure 1: Panda Security Panda Cloud Email Protection filters all mail before sending it on to recipients or quarantining suspect emails.

7. The Collective Intelligence - A new security model

Panda Cloud Email Protection classifies the malware in real time based on the Collective Intelligence in order to provide the latest and most accurate viral knowledge. How does Collective Intelligence work?

Millions of computers running Panda Solutions all around the world are continuously sending information of possible malware events to PandaLabs. When a special event happens (a suspect file appears) it is sent to PandaLabs and classified as unknown by default. Another suspect file can appear then somewhere else and is sent to PandaLabs the same way.

Once in PandaLabs, both events and some others are sent to an automated Artificial Intelligence Process of correlation and classification that determines if it is malware or not. This process allows to define malware signatures in question of seconds. Only with very strange files there is a need of human intervention.

When a file is classified as a new malware it is included in Panda's signatures file and deployed to all Panda solutions in the world. If it is goodware it is also classified in order to avoid later suspect actions and flase positives.

Panda Cloud Email Protection is directly connected to PandaLabs and all new signatures are available in real time. The advantages of Collective Intelligence are notorious because:

- Intelligence resides in the Internet (Intelligence from the cloud).
- Panda has Global visibility of new threats.
- There is a Continuous Correlation work.
- Malware and goodware are classified automatically.
- All the process is totally Transparent for the user.

8. Benefits of using Panda Cloud Email Protection

Panda Cloud Email Protection provides users with an optimal cost-to-quality ratio by having constantly managed systems and reduced inbound traffic. By virtue of being a managed service, it offers maximum protection, since malware is increasingly complex and fast-changing. The solution delivers advantages only available through an external mail-cleaning system – benefits not possible with traditional mail server software or dedicated gateway devices.

Additional benefits included:

- **Increases users' productivity** eliminating spam and malware from the received messages with the biggest guarantee.
- **Offers Operating Cost reduction** due to the reduction of incidents caused by malware or spam, to be attended.
- **Eliminates any complexity** since management is by third parties and internal hardware infrastructure is eliminated.
- **Simplifies Risk Management** eliminating the mail as one of the most important threats origin.
- **Enables email Business Continuity** by keeping the emails during internal mail server failures and delivering them after the systems recovering.
- **Aids Regulatory Compliance** delivering virus free inbound and outbound mail transactions by contract and blocking damages due to involuntary spamming from inside the organization.

Through its use of Panda Security's Collective Intelligence and individual analysis of suspicious emails by PandaLabs, Panda Cloud Email Protection is able to offer 100% virus-free guarantee SLA. The system architecture offers load-balancing and redundancy, and is designed to offer maximum availability backed by 24x7 support to ensure an uninterrupted, clean email delivery service.

9. Conclusion

Spam and malware attacks are becoming increasingly sophisticated and targeted to specific objectives; therefore the risk of them causing extensive damage is greater than ever. The best technique for combating these threats is through a managed network service, given the high level of specialization that a third-party service provider can offer. Managed security systems for mail filtering are now the most effective and cost-effective methods for companies whose IT resources could be compromised by the threats transmitted via email.

Panda Cloud Email Protection provides the industry's most advanced security methodology for today's enterprises. It acts outside the client's network using redundant platforms and preventive detection systems that can resist attack and isolate new threats – even before they have been identified. It is an effective method because it does not require investment in specific systems. It reduces investments in communication infrastructure, and is offered at a predictable cost to the client.

With Panda Security's team of security experts managing mail protection, availability, and confidentiality – clients can redirect their valuable resources to focus on the enterprise's core business activities. For more information on Panda Cloud Email Protection, please visit www.pandasecurity.com.

PANDA SECURITY

EUROPE
Ronda de Poniente, 17
28760 Tres Cantos. Madrid. SPAIN

Phone: +34 91 806 37 00

USA
230 N. Maryland, Suite 303
P.O. Box 10578. Glendale, CA 91209 - USA

Phone: +1 (818) 5436 901

www.pandasecurity.com