

unwanted
end-user e-mail
quarantine access

white paper

Bandwidth saving
virus
outbreak
protection

E-MAIL SECURITY

- > UNWANTED E-MAIL
- > END-USER
QUARANTINE
ACCESS
- > BANDWIDTH SAVING
- > VIRUS OUTBREAK
PROTECTION



Guidelines on how to tackle SPAM issues

PREFACE

The purpose of this document is to inform the reader about SPAM. SPAM is a widespread problem and every e-mail user, sooner or later, is faced with it. This document explains what SPAM is, how it continues to exist and what it costs to your company. Furthermore in this document you'll find information about the different technologies that have been developed to combat this SPAM-problem and how you can implement them into your corporate network.

Quentris

Rue de la fusée 60 Raketstraat
1130 Bruxelles

T 32 2 727 14 11

F 32 2 727 15 00

info@quentris.com

www.quentris.com



INTRODUCTION

Recent publications in the media (VRTnieuws.net, De Morgen, Sunday Times,...) confirm that SPAM¹ is still a big problem. Some sources even report that during certain periods more than 9 out of 10 electronic messages are unwanted. Just like other digital threats, the abusers are also increasingly more inventive in how to get their SPAM to the user, which makes it a constant struggle for network administrators to protect their end users from it as much as possible.

WHAT IS SPAM?

Whenever we talk about SPAM we mean unwanted electronic messages that are sent in bulk. Generally the message offers products that are probably fake and for which the transaction is generally illegal. Other types of SPAM messages are trying to influence the stock market or offering illegal services. The e-mail addresses from which the messages are sent are almost always non-existent; moreover the addresses to which the messages are sent are obtained without the knowledge or permission of their owner, which is illegal.

WHY SPAM CONTINUES TO EXIST?

In spite of the fact that most people are not interested in the services or products that are offered in this manner, there is still a small minority who can be influenced this way. Because the cost of sending SPAM is extremely low (all a SPAMMER² needs is an Internet connection and a list of addresses), this is still an extremely profitable business.

WHAT SPAM COSTS YOUR COMPANY?

For this example we'll use a medium-sized company with 100 employees who use e-mail, where each employee receives on average 25 SPAM message per working day. The time required to detect and remove a SPAM message will on average take an estimated 5 seconds. It follows that 5 seconds multiplied by 25 messages times 100 employees equals 12 500 seconds. This comes to approximately 210 minutes, or 3.5 hours of lost productivity per working day. If we assume an average staffing cost of €60 000 per year this comes to 44% (3.5/8 hours) of €60 000 or €26 400.

We have not included in this: the time it takes for the network administrators to provide support for accidentally deleted mails, the bandwidth that is unnecessarily wasted and the extra storage capacity that your mail server needs to support the overload of unwanted mail.

¹ In this document we concentrate on SPAM by means of e-mail messages. The term SPAM also applies to unwanted electronic messages that are disseminated through chat channels, usenets, SMS or other digital communication channels.

² By spammer we mean the person who sends the unwanted mail.



HOW SPAMMERS OPERATE

STEP 1: SEARCHING FOR E-MAIL ADDRESSES

One of the oldest techniques for collecting e-mail addresses is by means of a script, or so-called “bot” that scans websites, newsgroups and other online media for e-mail addresses. This method is quite simple but is reasonably time-intensive and you run the risk of also gathering out-of-date information and addresses that are no longer valid.

Another method is the “brute force” attack, where you try to retrieve e-mail addresses automatically by sending mail to various combinations of many common first and family names in combination with known domain names. But this method is also very time-intensive and unnecessarily wastes the spammer’s bandwidth. Other contemporary methods are much more sophisticated and consist of viruses or worms, just think of the JS.Yamanner@m³, whose aim is to track down an existing user’s address book and upload it to a public website or FTP server, as a result of which the spammers are certain to have reasonably accurate contact data.

STEP 2: SENDING THE MESSAGE

The next challenge for the spammers is naturally getting the messages sent. It seems simple to start up a mail server on a normal home Internet connection and start sending mail, but it is not as easy as that. It is relatively simple to determine the origin (IP address) of a mail, the spammer must therefore find a method to conceal or distribute it. One of the options is to try and compromise some company’s mail server, we generally call this an “open relay” server, another option is to make use of so-called “botnets”. “Botnets” are clusters of end-user PCs that are infected with an unnoticed piece of software that carries out certain actions on command; one of those actions can be sending SPAM, another can be carrying out “Denial of Service” attacks.

STEP 3: SMUGGLING THE MESSAGE IN

Since SPAM is generally really not wanted, most destinations already have a solution to make an automatic selection. Initially these solutions consisted of a sort of digital dictionary that searched for certain undesirable words in the mail, an example of this is the word Viagra or medicine. The disadvantage of this is of course that there is a lot of administration involved in making the specific dictionaries for your business.

Y First Thing Or To get round these dictionaries, they started using camouflage techniques. Just liek
ut for HOT NEWS! I cn wrte thiz sentens kmpletely wrng but u cn still reed it, we get the phenomenon
of V\$i@gra. This is also known as leech speak. The latest development is so-called
ate: MONDAY, image SPAM, here the spammer puts the text messages in a photograph or drawing
: QUANTUM that is sent with a nonsense but readable text. To prevent an anti-spam provider
Price: \$3.12 simply recognizing these drawings, the drawing is different for every destination.
NOW!

This is done by automatically changing the image or by introducing extra inconspicuous pixels. Spammers have known about this method for a while but it requires considerably more bandwidth. This has a greater impact on your corporate infrastructure because more image SPAM also means more disk space that you need on your mail server for temporary storage.

³ <http://www.frst.com/english/virus/2006/04507>



WHAT CAN YOU DO TO PREVENT SPAM

A simple tip could be: “Try not to leave your e-mail address in public places unnecessarily”, but since mail is one of the basic ingredients of the modern way of doing business, this isn’t really an option. For this reason there are various SPAM prevention solutions available on the market and each of these solutions has its advantages, depending on your needs. To give you an overview, we briefly outline the various technologies that an Anti-SPAM solution can include so that we can position them later in a corporate network.

TECHNOLOGY

KEYWORD FILTERING

“Keyword filtering” is a basic functionality that still survives from the initial development of anti-SPAM solutions. It offers the possibility of producing a list of standard words that will be blocked. Nowadays, a reliable anti-SPAM solution can no longer consist mainly of this technology, but it is still useful to have as a safety net for mails that would otherwise slip through.

WHITE & BLACK LISTS

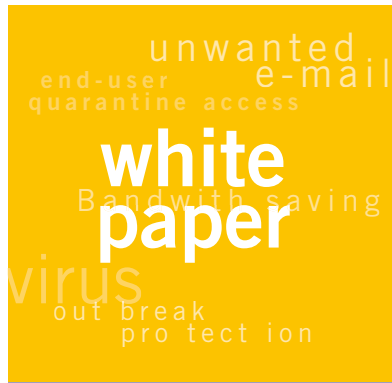
So-called “White lists” and “Black lists” give you the possibility of implementing positive and negative security. With positive security (white) you create a list of sources, these can be e-mail addresses or mail servers, that you always trust; they will then always be forwarded unchecked. Negative security (black) does exactly the opposite and gives you the possibility of filtering out known addresses, before they even enter the various security technologies.

PATTERN RECOGNITION

Pattern recognition is a technology that is analogous to “keyword filtering” but is much deeper and more complex. Here you don’t validate on certain known words, but you try to recognize patterns, just as happens in OCR recognition to be able to change scanned text or similar to the facial scanners that will be used to identify people. It is very important here, however, that you start with patterns that you have already seen before, the so-called “signature databases” that are offered by the makers of the anti-SPAM solution.

REPUTATION BASED

This solution is based entirely on the reputation of the mail server the message comes from. This is done by means of a database that contains all the IP addresses of known mail servers, together with their reputation. The reputation is dynamically updated by various anti-SPAM solutions. Whenever a new, unknown IP address is picked up as a sender, it is looked up in the database and the reputation of that address is used as the basis for determining the SPAM factor of the mail. If, for example, an unknown address is offered to the mail server, this will be given the reputation of medium because mail has never been sent from that address. When several anti-SPAM servers now make an enquiry about that same address in a very short time, its reputation will quickly become negative. On the other hand, if the requests for that address show a normal distribution, the address will quickly get a positive reputation.



REALTIME BLACKHOLE LIST (RBL)

This is a database that keeps track of which public legitimate mail servers are being misused by spammers. These mail servers are known as “open relays” or black holes.

RATE CONTROL

Using “Rate control” an administrator can specify how many mails can arrive at the same time from the same source, or in general how many mails can arrive at the same time. This is to reduce any overflow. Moreover it is useful to use the same technology for outgoing mail where, if a mail server has been compromised, it helps to prevent your own infrastructure from being negatively evaluated on the Internet by dynamic technologies such as RBL and “reputation classification”.

DENIAL OF SERVICE PROTECTION

Just as in “rate control” here the number of different connections is monitored, known patterns (behaviors) of DoS attacks seen earlier are taken into account and the communication is interrupted on the basis of that knowledge.

ANTI-SPOOFING

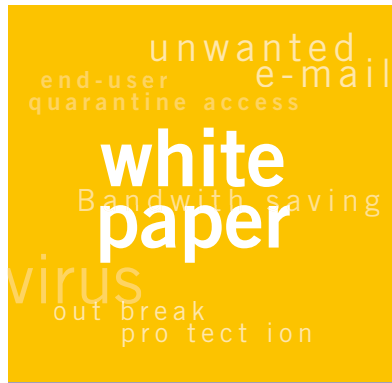
A technique once used a lot to get around security was to pretend to be the local mail server. Generally the restrictions on your own mail server are not as strict as those for mail servers on the Internet. “Anti-spoofing” prevents mail arriving via the Internet from looking like it comes from the internal mail server.

ANTIPHISHING

“Phishing” attacks try to extract certain data from the recipient. A very common example of this is a mail that asks you to update your bank details. The mail will look like it came from your bank and you are asked to click on a link to the website. The website itself does not belong to the bank but, just like the mail, looks real to the inattentive eye. The Anti-phishing technology will validate whether there is a connection between the contents of the mail and the sender of the mail, also taking the fact into account that most banks or other on-line service suppliers will not ask you to change your details by e-mail.

BAYESIAN (HEURISTICS) ALGORITHM

This method is based on mathematical algorithms, just as in “pattern recognition” you start with certain patterns that can occur and make a decision on that basis. The major difference here is that there is a set of keywords, concepts and syllables that are searched for in the mails. An exact pattern is not searched for, as in “signature databases”, but a correlation between the occurrences of the various patterns. The advantage is that there is no need for a permanently up-to-date database of known signatures, the algorithm also allows variations to be recognized and generally provides a self learning function. This means that the algorithm can be fine tuned by presenting the incorrectly classified mails again during a learning process in order to correct the qualification.



WHERE CAN YOU BEST IMPLEMENT AN ANTI-SPAM SOLUTION?

ON THE EXISTING MAIL SERVER

One of the options for locating the anti-SPAM solution is on the already existing mail server, which has a number of advantages. There are therefore solutions that, thanks to the direct link with the mail server, offer the possibility of automatically creating a separate folder in the user's mail folder in which the suspect mails are saved. This has the advantage that the administrator can adopt a policy where messages that are not 100% certain SPAM are placed in this folder and that the responsibility for the management of these messages is passed to the end-user. The major disadvantage of this solution is that the unwanted mail has already reached the internal network, that the mail server must have the extra processing power that is required for the anti-SPAM package and that provision must be made for the storage required for saving all the suspect mail.

GATEWAY

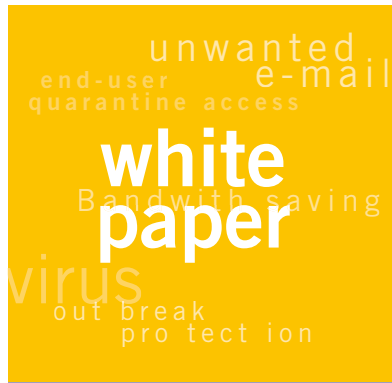
A second option is the so-called "gateway solution", where a separate "mail relay" is placed in the DMZ⁴ of the network. All incoming and outgoing mail can then be sent via this "relay" solution for validation.

This hardware ("appliance"), whether dedicated or not, can have one or more anti-virus solutions installed as well as extensive SPAM detection. The advantage here is that the processing power is removed from your internal mail server where the users will permanently work, in addition to which a good solution will also provide the possibility of clustering multiple hardware components. The advantage of the extra quarantine folders on the mail server is lost here; on the other hand a good solution will offer you the possibility of importing or recognizing the users automatically and creating a folder for them on the "gateway". They will then be informed at configurable intervals via mail which messages have been set-aside for them. Using a short summary and a link they can then choose which action they want to take on this mail (always delete, allow through temporarily or always allow through). In this way they can manage their own "black and white lists". In addition, the administrator keeps a clear overview of what is happening.

EDGE

Thanks to the fairly fast decision ability that the "reputation based" solution offers and its relative accuracy, we can see that there is a trend to implement this technology on the edge, or therefore on or immediately after the ISP router. This has the advantage that the components after it such as "firewalls", "mail relay" and mail servers do not have to be scaled to process this unwanted data. The combination of this functionality with the gateway solution discussed earlier ensures 99% accuracy in blocking SPAM. The enormous difference in this solution lies in the fact that the communication between the sending mail server and your mail server is already interrupted during the initial setup of the communication. This ensures that the SPAM never reaches your network, which then leads to a considerable bandwidth saving.

⁴ DMZ or "Demilitarized Zone" is a separate network between the internal network and the Internet, where the access between different networks is generally through a firewall.



About Quentris,

Quentris is the “competence center” of SUEZ Energy Services (SES) in Belgium in the field of communication technology. In close cooperation with other SES companies (Fabricom GTI, Axima services, Ineo Com in France, ...), Quentris offers solutions and services that are based on the integration and convergence of Data, Voice and Image technologies. We create complete solutions by integrating technologies of major ICT suppliers as Alcatel, Avaya, Cisco, Envoy, Microsoft and Nortel. Our activities focus on data cabling, wired and wireless networks, securing networks and business applications as IP telephony, Unified Communications, Contact Centres, CTI developments and Collaboration Tools. As an independent partner, Quentris is the new ICT alternative for the private and public sector. The majority of employees are specialized and certified engineers. Quentris has customers in Belgium and Europe.

Quentris

Rue de la fusée 60 Raketstraat
1130 Bruxelles

T 32 2 727 14 11

F 32 2 727 15 00

info@quentris.com

www.quentris.com

CONCLUSION

It is not simple to choose an anti-spam solution tailored for your company. The Quentris security engineers have therefore screened the products on the market today and made a selection of a limited number of solutions that meet the different requirements.

Thanks to many years of experience in the design, implementation and maintenance of voice, data and security solutions, Quentris is able to assist you in all the phases involved in an e-mail security solution. This includes helping to determine the best solution tailored for your company, the implementation and the routine maintenance that is necessary for staying safe.