window.respimage && window.respimage({ elements: [document.images[document.images.length - 1]] });

Subject: SPAM

SPAM or UBE is a matter of little account for edv2g customers. Just a few samples per week remind users of the existence of unwanted advertisements and other harmless or even harmful varieties of electronic mail.

But there are rumours about installations out there where mailboxes are overfilled with offers for pills, dubious business opportunities, notifications about wins and so on.

What has proven as 'must' or 'useful' for deviding wanted and unwanted mail?

From the conceptional view we should differentiate between filtering of mails that are already delivered into mailboxes and not accepting suspicious mails for delivery:

Client side filtering

Manually trained mail user agents (MUA, "mail programm") do this almost perfectly (see bayes classifier) if they are trained with good and bad examples sufficently. Almost all current mail programs (e.g. Microsoft® Outlook® or Outlook Express®, Thunderbird™ and others) contain this function out of the box or there are addons available which add this capability.

Besides the fact that the mailbox becomes less crowded and thus less confusing the risk of a malware infection of the PC is lowered. There exists mail content that will infect a computer if the mail is only shown. So users should use a setup of the mail program in which the first view of the mail only show sender, recipient and subject but not the content of the mail. A SPAM senders standard technique is to check if a mail is shown to or read by the user. This can done by embedding visible or invisible images that the mail program must fetch from the internet. If the address of such an image is engineered in a way that allows to track whom that mail was sent to the SPAM sender can increase the value of mail addresses he is using by focusing on valid recipients.

And if a mail address is proven as valid and SPAM to this address as being read it can be sold to other spammers for higher prices. So don't be surprised that you will receive more and more SPAM if you have

a look at each incoming mail, espsecially if you don't suppress the loading of images from the internet.

Client side filtering helps the mail recipient: the SPAM ist sorted "automagically" into a SPAM folder and false sorted candidates can be found easily. But the spammer has the success of delivered SPAM. And each mail containing malicious code in an end users mailbox is always a risk.

SPAM filter and classifier on the internal mail server

are not really better than client side filtering because of the same problems. They only help as it is not so easy for the user to click on such a dangerous mail.

Therefore it is much better to check when receiving a mail if the sending system is a valid sender. If the sending system cannot prove to be a well configured mail server then no mail is accepted for further delivery. As a side effect the amount of "undeliverable" notices will lower. Because of such messages only have to be sent if a mail was accepted once for further transport.

SPAM filter as part of the firewall

A typical scenario for a company is using a mail gateway (where every incoming email is checked for viruses and malware) and as a second system the mail server with all user mailboxes in the internal network. If this gateway system does not immediately check if a given user (from user@domain.tld) exists it must accept all mails for the domain of this company. If later when trying to forward this mail to the internal server the latter will find non existing user names a error message will be send. Possibly to a innocent person whose mail adress was abused as sender address for SPAM. Those mysterious error mesages are called backscatter. But an unknown user error message could also result from a typo from the sender. So an information to the sender telling that his mail could not be delivered is very useful in this case.

SPAM sender abuse in many cases infected PC of home users and send messages directly from those PCs. These sending PCs must contact a mail server to reach a recipient and simple strategies will contact the mail server for the target domain directly. If this server rejects mails for unknown users those mails are not sent at all and also no "unknown user" messages will flood the internet. So this check for existence of the user is mandatory.

The next "must" is to check the sending system against one or more realtime black lists (RBL). The IP address of the sending system is checked against a database if it is known (or maybe only suspicious because of the address ranges of home users are not intended to send mails directly to target mailservers) as a SPAM source. If the contacting system is found on such a list no mail will be accepted.

Another very useful technique is greylisting. In short you can say: a real mail server will make a second attempt if the system he wants to deliver mail to says "I have a temporary problem."

Sometimes reverse DNS and HELO checks cause trouble with incorrect configured mail servers. In those cases usually whitelist entries on the gateway will help, besides contacting the administrator and motivate him to fix his configuration.

Other techniques like SPF or DKIM are not wide spread so far and will thus not significantly reduce the amount of unwanted mails.

If you find this article useful but you have further questions or suggestions please contact us. The needed data you find in the footer of this page.