Interview with ENISA expert Pascal Manzano around the third ENISA Anti-Spam Measures Survey "What Are the Measures Used by European Providers to Reduce the Amount of Spam Received by Their Customers?

ENISA Security Policy Expert Pascal Manzano is the editor of the recently launched ENISA report on spam.

You did this report now, the third about spamming. Do you see any differences compared to your previous surveys on spam?
One of the most prominent conclusions is that little has changed over the last two years. Most measures are applied by similar proportions of providers to what was observed in 2007.

Although the level of involvement in filtering spam has been high during the last few years, since ENISA started looking at spam, more and more providers are now involved in the process of making their customers' PCs safer. The ISPs have changed their view when it comes to blocking customers. This was previously seen as something that had a high cost and the view has now changed to this being seen as value adding. The providers today also encourage their customers to send in spam abuse reports, in order for them to take action against spam. These are some of the differences compared to the previous reports on spam.

Are people aware of their computers sending out spam?
No until they are blocked by their provider, typically the user cannot enter the internet anymore, since being stuck in the walled garden or quarantine. When the user has downloaded cleaning software, anti-virus, and cleaned his or her computer the internet can again be accessed. In other words, they are aware of the problems with sending out spam and also involved in the process of

cleaning their computers. In some countries, like Finland, this is mandatory and providers in other countries are now using the technique as well. One benefit of this security technique being mandatory is that the providers are not risking losing their customers.

Are there any of the technical measures that are more important in spam detection and prevention?
The most efficient and most used technique to prevent spam is blocklisting. At the same time, many of the providers say that it is not easy for them to get out of those lists. As one of the recommendations from ENISA say in the report, the blocklist managers need to ensure that it is easy to remove a server or domain from a blocklist when spam problems have been rectified. With so many different blocklists in use, collaborative efforts to share data on servers that should be removed from blocklists would help to address the problem. Wider use of whitelists could help in this effort. There are some providers that are against the use of whitelists at all.

When it comes to preventing spam, one of the most efficient of the measures is managing the blocking of "port 25", the port used to send email.

Less than 5 % of the e-mails are delivered. Does that mean that 95 % of all e-mails are spam?
Yes, and in fact the amount of spam is actually larger than this. Even if only 5 % of the emails reach peoples email inboxes, there are still some spam mails inside.

Is there any indication that the amount of spam will decrease?
It cannot grow indefinitely but the amount of spam is still increasing. Ten years ago it was around 75 % of all traffic, five years ago it was 85 % and now it is 95 %. The reason for this is that the spamming works. The spammers are making money.

Could you give some information on what the best practices in fighting spam are in the future?
We are currently working on limiting the amount of spam received, but we are not working on the root cause of spam. One important thing in dealing with spam is the awareness raising among the end users. ENISA is doing part of this job but ENISA cannot succeed in this job without help from the providers' organisations, the end user organisations, ISPs, national regulatory authorities etc. One important aspect when it comes raising awareness of spam is language. ENISA cannot contribute with information in all languages, but we can send information in English to the member states, which can then translate the information and use it where the citizens are looking for information regarding spam.

In some countries, such as Greece and the Netherlands, the national data protection agencies have asked ENISA to help providers adopt best practices in fighting spam.

Are there any collaborations working together to fight spam?
One collaboration that I can mention is when ETIS (The Global IT Association for Telecommunications) contacted its members, who decided to work together to fight spam. The group was successful in developing technical measures and reporting to and building trust among each other. By working together they managed to reduce the amount of spam sent between them by 50 %.

Another example is ECO, the German Providers Association that has two projects in place. One project to collect information about the spam sent and the other project is a whitelist they are working on. There is also a project in France called signal-spam, where every French citizen is invited to inform about the spam that they are receiving.

For report:
http://www.enisa.europa.eu/act/res/other-areas/anti-spam-measures

For press release:
http://www.enisa.europa.eu/media/press-releases/spam-survey-2009-the-fight-against-spam

For slides:
http://www.enisa.europa.eu/act/res/other-areas/anti-spam-measures/studies/spam-slides

For further details, contact:
Pascal Manzano, Expert Network Security Policy, ENISA, tel: +30 2810 391366
Ulf Bergstrom, Spokesman, ENISA
press@enisa.europa.eu, Mobile: +30 6948 460143