Find us on facebook Follow us on twitter

AV-TEST The Independent IT-Security Institute Magdeburg Germany

A New AV-TEST Study: Dangerous Spam E-Mails

Spam – More Dangerous than Ever Before

By using botnets, spammers are able to send millions of spam e-mails every day. The test institute AV-TEST from the German city of Magdeburg recently carried out an 18-month-long study in which it collected and evaluated over half a million spam e-mails before coming to the conclusion that the risk posed by spam is higher than ever.

Markus Selinger

The hype concerning the issue of spam has calmed down. Although they are still annoying, people have now gotten used to receiving spam e-mails. Nevertheless, it is precisely this situation that makes such e-mails even more dangerous. In an 18-month-long study carried out between August 2011 and February 2013, the AV-TEST laboratory collected and analysed over half a million e-mails classified as spam. The results of the study are sobering: every third spam e-mail containing an attachment is infected with malware. Other e-mails use a different technique by attempting to attract users to visit infected websites.

The worst finding revealed by the study, however, is the fact that 25 percent of all spambots are located in offices, even those in Germany!

Over 500,000 Spam E-Mails in the Laboratory Analysis

AV-TEST investigated a total of 550,000 e-mails that had been classified as spam prior to the analysis. Nearly 14,000 of these e-mails were infected, which corresponds to approx. 2.5 percent of the total number of e-mails analysed.

The institute used 90 monitored e-mail accounts to collect the spam e-mails for the study. Some of these addresses were published in forums and competition entries, which was like a kick-off point and resulted in the sending of dozens of e-mails to the accounts every day just a short while later.

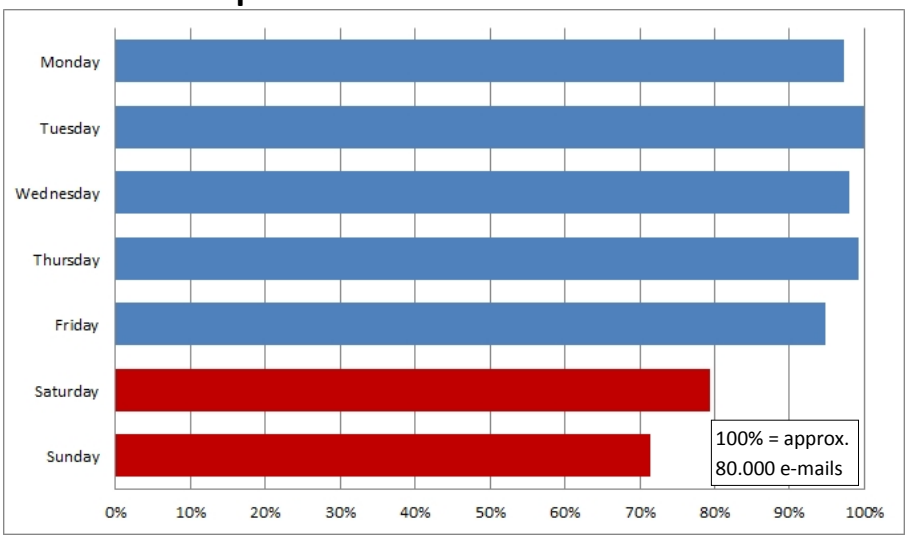
A Multitude of Infected Attachments

A good 30,000 of the 550,000 spam e-mails analysed in the study contained an attachment and over 10,000 of these attachments, namely slightly more than 30 percent, were infected with malicious malware. 400,000 of the e-mails contained website addresses (URLs) alongside their content text. Nearly 1 percent of the links found in these mails with URLs led users directly to

For more information, please visit
www.av-test.org

You can always find the latest information concerning this test and other studies, as well as up-to-date statistics on spam and malware, on the AV-TEST GmbH website.

25 Percent of Spambots Are Located in Offices



The study recorded the spam e-mails received every weekday. The maximum number of spam e-mails received in one day was around 80,000. The results showed that the number of spam e-mails sent remained consistent from Monday to Friday before significantly decreasing at the weekend. This proves that these PCs are located in offices, where they are switched off at the weekend. 25% of the botnet PCs that send spam e-mails can therefore be traced back to offices, even those located in Germany!

15 percent of these were actually infected with malware. Attachments in e-mails sent from India, on the other hand, had an infection rate of 78 percent during the study, closely followed by e-mails with attachments from Vietnam with a rate of 77 percent.

Half of the 30,000 spam e-mails with attachments recorded in the study came from the USA, China, India and even Germany. The spam containing attachments from Germany, was, however, less dangerous with only 10 percent of the e-mails containing malware on the side.

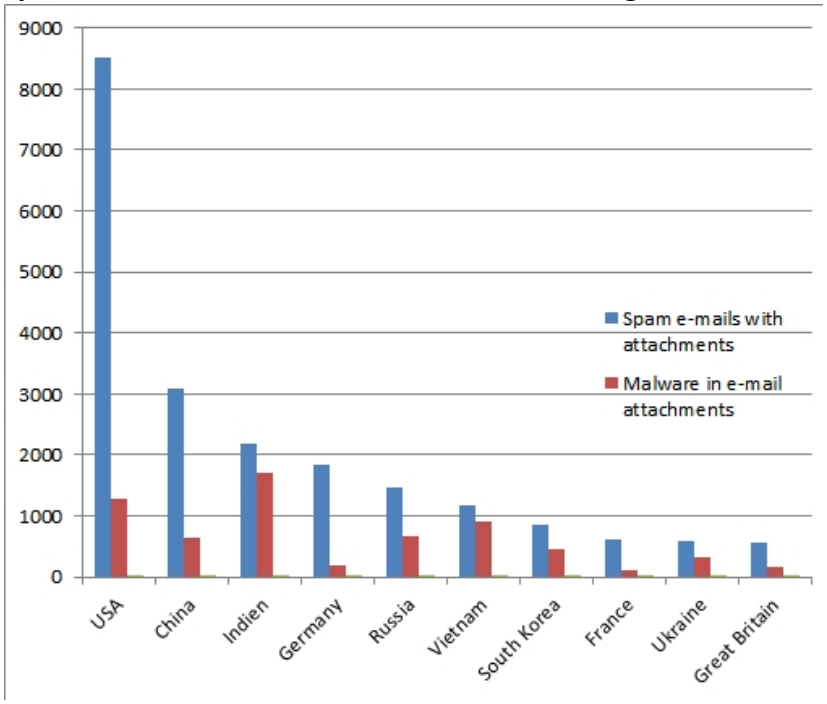
websites infected with malware, while the others were mostly fraudulent offers for counterfeit products such as pharmaceuticals.

The majority of the infected e-mail attachments involved the classic examples used for spam attacks, namely zip files, HTML documents and executable EXE, COM, SCR, BAT or PIF files. PDF files and images also continue to be used as popular infected objects. The study proved that almost all spam e-mails containing zip files are infected. This also applies to executable files such as EXE or PIF files, while over 80 percent of the HTML documents attached to spam e-mails in the study were infected.

Indian Spam Is Always Dangerous

Although most of the spam e-mails containing attachments analysed in the study came from the USA, only

Spam E-Mails with Attachments Sorted According to Countries



Although the USA was the country of origin of most of the spam e-mails with attachments recorded in the study, these messages contained fewer dangerous elements than those from other countries. Virtually all of the mails sent from India or Vietnam contained malware on the side, while only 10 percent of the e-mails with attachments sent from Germany were infected.

25 Percent of Spambots Are Located in Offices

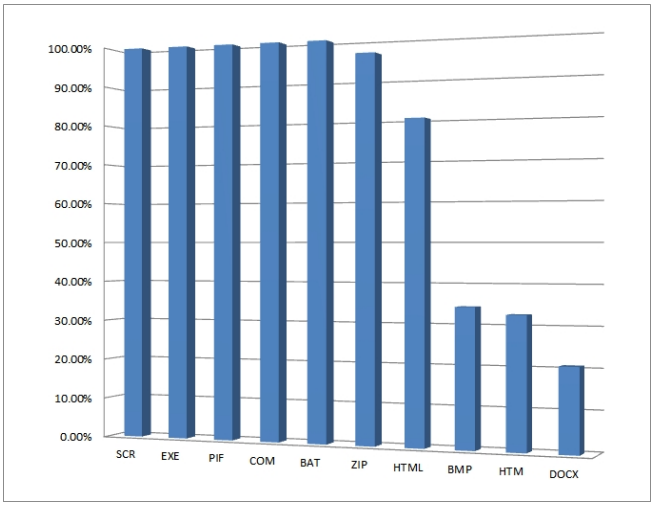
The study recorded the number of spam e-mails received on each day of the week and then carried out a final analysis after a period of 18 months. The results of the test showed that the amount of spam sent remained extremely consistent from Monday to Friday before reducing to 25 percent at the weekend, namely on Saturday and Sunday. The study therefore proves that 25 percent of all spambots are located in offices, where they are switched off at the weekend. The amount of spam sent then increases straight away on the Monday after the weekend.

The analysis of the spam e-mails according to the months in which they were received did not reveal any specific focuses. It only showed that the highest infection rate among the e-mails sent was recorded in July and August, but this did not indicate any sort of pattern.

Botnets – Active & Malicious

Virtually all spam e-mails are sent via PCs that are inconspicuously remotely controlled by botnets. The e-mails therefore always have different sender IPs, which makes it difficult for providers to identify suspicious messages according to their IP addresses.

The Top Ten Infected E-Mail Attachments



The study recorded a total of 30 different file types used as e-mail attachments. In the case of the top five file types, all spam e-mails containing an executable file are infected with malware.

When PCs infected by controlling Trojans are used, the infection remains perfidiously inconspicuous to their users. After all, these users should not be able to notice that somebody else is using their computer to send e-mails. The size of different botnets also ranges significantly. The networks deactivated in recent years contained a total of between 1 and 10 million controlled PCs. Although these computers were never all online at the same time, it only takes a few hundred thousand PCs to be able to send a multitude of spam e-mails in a very short time.

"Am I part of a botnet?" – Online Checks for Your PC!

The German Federal Office for Information Security has set up the website www.botfrei.de (different languages) in cooperation with the Association of the German Internet Industry. This website contains a multitude of links to manufacturer sites that can be used to check whether PCs belong to a botnet.

Anti-Virus Software Protection

Using an up-to-date protection program on a computer virtually excludes the possibility that a malicious botnet can take control of the PC. Such protection programs are able to prevent this risk by using their scanners to identify rootkits and Trojans, the two favourite tools used by botnet operators. You can read about the latest tests to be carried out on the best protection programs for free at any time by visiting www.av-test.org

Find us on facebook Follow us on twitter

Magdeburg, Germany, 11th April 2013
Author: Markus Selinger

Please contact the team at AV-TEST GmbH if you have any questions.
E-mail: presse@av-test.de
Tel.: +49 (0)391 6075460
Website: www.av-test.org