UDC 004.056

V.G. Abdullayev

ANAS, Institute of Control Systems, Azerbaijan State Oil Academy, Baku, Azerbaijan

BASIC METHODS AND RULES FOR EFFECTIVE COMBATING ADVERTISING MESSAGES

This article considers basic methods and rules for effective combating advertising messages. Methods of filtering e-mail messages on the server side were examined too. Options were proposed for countering ways to circumvent filtering methods and protection from advertisements.

Keywords: *spam, distribution of advertising messages, filtering methods.*

1. Introduction and literature review

Spam is advertising messages sent without consent of receiver, as well as messages with fraudulent purposes. Every year the quantity of Internet users is increasing: in 2011 and 2012 this figure was respectively 718 million and in 1.3 billion people [1]. This is related to many factors, including reduction of equipment prices (as a result the price for Internet access is going down), active use of tablets and smartphones by mobile internet users.

The share of spam in international internet traffic makes up about 80 % (figure for 2011) [2]. In 2012 the total quantity of detected and deleted messages was 65 billion [3]. According to statistics, the level of spam increased significantly by the end of 2012. At present the level of spam is more than 120 million comments daily.

The massive rise of unprotected web-sites, wiki and internet forums contributed to the spam increase. At the same time the spam senders started actively to use illegal methods, such as web-site hacking, infection of users' computers for creating botnets (network of infected computers used by hackers with the purpose of infliction of harm). Along with this, the significant rise was resulted from the increase of traffic from China – this was related with promotion of counterfeits of popular brands.

The rise of popularity of instant messages services and social networks led to increase of spam in these services. SMS messages are used for spam as well.

Losses caused by spam are huge: they are time, overload of the equipment and as a result – reducing operation time of the equipment. All these lead to the financial losses by both public and private institutions.

2. Problem definition

To consider rules and elaborate methods of protection from spam. Taking into account the annual increase of volumes and quantity of spam, as well as development of ways for circumvention of various protection methods, it is necessary constantly improve protection technique. Compliance with the simple rules will ensure the decrease of spam quantity. One also needs to take into consideration the spam published in comments at web-sites and forums. To elaborate counteractions of ways of circumvention of spam filters.

3. Rules for use of email addresses in Internet

One of the reliable methods, which, in principle, reduce the quantity of spam e-mails and make it more difficult for intruders to get email addresses, is adherence to the simple rules:

• Not to publish own email address on public sites in open form. Special symbols can be used to make it difficult to recognize the email address. It is also possible to use an address as a picture;

• Most users have accounts on social networks. And given the recent trend that sites frequently use authentication through a social network, in this case it is better to use a social networking account;

• Not to use the email address for registration on the little-known forums and sites;

• For registration on forums and sites, a special email address, or service for creating disposable addresses, for example http://mailinator.com/, can be used;

• Not to reply to spam or click on links from emails, including a link that provides unsubscribe from the mailing list. As a rule, these actions confirm the real address. Not to open attachments as well;

• It is advisable to disable the loading of images that are in the email, so user activity cannot be tracked;

• When receiving a link from an unknown person or contact that is in your contact list, but the link seems suspicious, it is better to avoid clicking on the link;

• It is necessary to create long names addresses, for example, which consists of a name and surname in order to exclude the method of selection of address by random address generators.

Following simple rules and caution will provide the partial protection against spam, as well as of a personal computer, which can be one of the nodes of the fraud network.

4. Ways to protect e-mail addresses and web-sites

In order to protect e-mail addresses that are posted on web-sites, there are various ways and rules that are implemented purely technical, or in compliance with elementary actions. Most important is a protection against bots (automated programs (scripts), intended to gather information or send messages.

On most web-sites or in blogs there are feedback forms for writing appeals, complaints, and comments to articles and so on. The most common and relatively reliable is the placement CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart – automated Turing text to determine differences - computer or human being) [4]. The basis of this method is giving such a task that can be solved only by a human being, for instance it can be curved images of characters or images of mathematical tasks (as a rule, addition) because automated scripts cannot recognize distorted text, while human beings do. Also, there are variants of modified examples such as to count the number of drawings depicting a certain way. At present there are sufficient ways to circumvent CAPTCHA:

• Creating a database of answers or obtaining database illegally. Some developers use existing database of tasks and responses, so tasks are not generated randomly. Therefore, attackers can manually create a database or download it. Countering way is not to create databases, and generate random tasks;

• Unqualified writing a script that will give the right answer at a certain compiling the query to the web-site. Solution - use ready scripts that have proven themselves as reliable, or appeal to professional performers;

• Automatic identification is possible in case a picture with tasks is not enough distorted or veiled, and in case of the use only one method of masking task. This all contributes to the development of a method of automatic recognition. Solution is to use various masking methods, which will vary randomly;

• Automatic selection of response options. The answer to the task is automatically selected. To protect against this method is blocking IP addresses or account for a certain time, if repeated, the full lock without restoring;

• Manual recognition. There are special services which use the human resources for recognition. This circumvention method is almost impossible to bypass. If track from what address or account these messages come, temporarily block and enter a specific time for the answer. As a rule, different data are used, so it necessary to moderate messages manually;

Additional methods of controlling unwanted messages can be banning anonymous comments, authorizing comments made only by registered users, or authorization through social networks. It can also be the use of reliable browser that provides a minimum number of problems in the system security, as well as the prohibition of direct publication of messages, permission to publish only after approval by an administrator.

In order to filter messages on web-sites, the filters for filtering messages based on keywords can be used. The principle of operation of such script is as follows: after the user sent a message, the script analyses it, and if the message contains the keywords or URL, which exists in the script database, the message will not be published and will be sent to the administrator for verification.

5. Methods of mail filtering on mail servers

Blacklisting, grey listing, displaying user rating, filtering messages based on the sender's domain, as well as on the keywords in the subject and body of the email can be used for filtering e-mail messages on the server.

There are the lists of blacklisted e-mail addresses and IP. This is the lists, which include data of users and systems that have been noted in sending spam or malicious messages. While receiving a new message the server automatically checks whether the user is listed in these databases. If they are mentioned there, such messages are automatically sent to the spam folder or deleted, depending on the system configuration. These lists are called DNSBL (DNS Black List). This method has lost its relevance due to the fact that spammers tend to use users' addresses and computers. And after entering their data in the above-mentioned lists, the users will not be able to send messages during a long time.

It is also possible to automatically filter (spam filters), both on the server and on the client side. One approach is to analyze content of the email (by keywords) and make decision depending on its content. One of the methods used here is a statistical analysis of the email content and Bayesian spam filtering method is usually used with that purpose. The essence of this method lies in the analysis of words in the body of the email in order to determine the possibility of its relation to spam, and then conclusions are made [5]. At the beginning of the use of this method, it is necessary to adjust the filter to identify spam. With the active and the correct adjusting the effectiveness of spam filtering can be increased to 95%, but for this constant adjusting is needed.

Recently grey listing has become a popular method. Its essence lies in the fact that during the first attempt to send an email, the server responds with an error. Spam software is not able to efficiently handle such kind of situations. Therefore, until they begin to resend, there will be a very high likelihood that they will be blacklisted. This method provides 90 % efficiency.

An additional protection against spam is to request PTR-record. The PTR-record connects IP-address with the domain name. Requesting a PTR, MTA will accept mail only in case of coincidence of the IP address with the domain name. Given that spam usually comes from the IP, which does not coincide with the domain name, the protection in this case is quite effective.

6. Additional methods of protection

The plug-ins for identifying signs of a mass mailing are built into e-mail servers. These modules calculate the checksum of the email and check it at servers of the services Razor and DCC. If the emails with the same checksums are found, there is a high probability that they are spam. The requirements to the sender's email are becoming stricter: checking domain name and return address, as well as IP address of the sending computer.

7. Alternative methods of protection

Every advertising message contains words and slogans that make up part of the advertising message, for instance "Buy", "Best offer" and so on. Having analyzed the e-mail message, except the message subject, it is possible to accurately determine whether the message is advertising one or not. This method is similar to the method used by the system of plagiarism recognition when parts of the message taken from other sources are sought.

But there are some weaknesses in this method. First of all, that during the adjustment of the system the operator will see others' messages while checking the system conformity. The second problem is the protection of confidential information, but in the case of the corporate sector it is not a key issue. The third one is spending additional resources for the information processing and thus the increase of costs.

Despite some disadvantages, this method can be an effective method of combating spam.

Conclusions

Taking into account the steady increase of spam, it can be concluded that this method of goods and services promotion make benefits to those who order it. Therefore it is not worth to expect the reduction of spam volumes in near future.

Following simple rules of behavior in the Internet will, as a rule, significantly reduce the volume of received mail. As a result, one can say that everything depends on users' behavior. And for them there is a choice: follow these rules or not.

CAPTCHA is quite effective and widely used method of combating spam. Statistics shows that about 200 million CAPTCHA were daily introduced in 2011 worldwide [6]. This method has proven itself in the feedback forms - comments, but it does not ensure the full filtration of advertising messages.

The use of special software and methods increases the efficiency of message filtering. But, as a rule, all methods require continuous improvement, because almost everyone, who is engaged in sending spam, improves ways of circumventing protection systems. It necessary to understand that demand creates offer. If entrepreneurs will further order sending spam, and users will respond to advertising messages, the demand will grow and the volume of spam will also increase.

One shouldn't forget about the legal aspects - in some countries there are laws on criminal liability for spamming. But the simple rules of behavior and the simultaneous use of effective methods of protection together will bring results and the amount of received spam will decrease. It is also desirable to continuously adjust systems to increase their efficiency.

The combination of the above-mentioned methods of protection will lead to a significant reduction in spam, and will also reduce the load on the server and network traffic, and will not take time of users.

List of references

1. Global smartphone sales to end users from 1st quarter 2009 to 3rd quarter 2014, by operating system (in million units) [Electronic resource] / The statistics portal. – Available at: http://www.statista.com/statistics/74592/quarterly- worldwide-smartphone-sales-by-operating-system-since-2009.

2. «МУСОРНАЯ СТАТИСТИКА» [Электронный ресурс] / Компьютеры и огротехника. – Режим доступа: http://www.computery.ru/news/news2010.php?nid=8302.

3. A Spammy Year in Review [Electronic resource]. – Available at: http://blog.akismet.com/2012/12/21/a-spammy-year-in-review.

4. Completely Automated Public Turing test to tell Computers and Humans Apart [Electronic resource] / Available at: http://ru.wikipedia.org/wiki/CAPTCHA.

5. Байесовская фильтрация спама [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/wiki/Байесовская_фильтрация_спама.

6. Welcome to the new TED.com [Electronic resource]. – Available at: http://www.ted.com/talks/lang/ru/luis_von_ahn_massive_scale_online_collaboration.html.

Поступила в редколлегию 1.04.2015

Рецензент: д-р техн. наук С.И. Юсифов, Азербайджанская Государственная Нефтяная Академия, Баку.

ОСНОВНІ МЕТОДИ ТА ПРАВИЛА ДЛЯ ЕФЕКТИВНОЇ БОРОТЬБИ З РЕКЛАМНИМИ ПОВІДОМЛЕННЯМИ

В.Г. Абдуллаєв

У даній статті розглянуті основні методи і правила для ефективної боротьби з рекламними повідомленнями. Також розглянуто методи фільтрації поштових повідомлень на стороні сервера. Запропоновані варіанти протидії способам обходу методів фільтрації і захисту від рекламних повідомлень.

Ключові слова: *спам, розсилання рекламних повідомлень, методи фільтрації.*

ОСНОВНЫЕ МЕТОДЫ И ПРАВИЛА ДЛЯ ЭФФЕКТИВНОЙ БОРЬБЫ С РЕКЛАМНЫМИ СООБЩЕНИЯМИ

В.Г. Абдуллаев

В данной статье рассмотрены основные методы и правила для эффективной борьбы с рекламными сообщениями. Также рассмотрены методы фильтрации почтовых сообщений на стороне сервера. Предложенные варианты противодействия способам обхода методов фильтрации и защиты от рекламных сообщений.

Ключевые слова: *спам, рассылка рекламных сообщений, методы фильтрации.*