Anti-spam technology: securing business correspondence

Mass mailings (spam) are a serious problem not just because of the time it takes to sort through email but also because they are often a source of malicious content. For instance, the Duqu Trojan, one of the most notorious cyber weapons to date, infected computers by exploiting a system vulnerability after recipients opened what appeared to be a harmless text document. Active use is also made of spear phishing, email scams that target specific individuals or groups to penetrate an organization's IT infrastructure. This type of attack was used in the Hellsing APT.

Unwanted correspondence is a serious problem for business. This is reflected in the results of the IT Security Risks Survey, with 64% of companies describing spam as their number one external threat over the last 12 months. Kaspersky Lab experts have also found that the proportion of spam averaged 56.4% of total email traffic in the first half of 2015.

The fact that more than half of all email traffic is spam, and given the ingenuity of fraudsters, it is essential to use security solutions that can effectively combat this threat.

Kaspersky Lab's approach to effective detection of new spam mailings with minimum false positives is based on a combination of content analysis (linguistic, graphic and signature), message and attachment attributes, and default filtering rules (black- and whitelists) with a cloud infrastructure.

Urgent Detection System

The Urgent Detection System 2 (UDS2) is integrated in the Kaspersky Security Network (KSN) and allows the immediate exchange of information about spam messages between the product installed on the customer's computer and a database of threats in KSN.

When a suspicious email is received, the client software sends the message characteristics – so-called signatures (lexical and graphic) – to the cloud database. The cloud database analyses the signatures for any matches and the client receives a verdict about whether or not the email is spam. It is important to note that the actual content of the email is not sent to the server and cannot be restored using the signatures. This ensures the complete confidentiality of email correspondence.

If a fraudster spoofs the sender address and uses domain names of well-known organizations (example@google.com, example@apple.com, etc.) in a spam mailing, the anti-spam technology will detect it using protocols that confirm the authenticity of an email. These protocols are based on comparisons of a number of typical features present in mass mailings (e.g., the mailing is sent from an IP address that does not belong to the range of IP addresses used by the organization that supposedly sent the message).

In the past, adding new signatures to the database required input from an analyst. UDS2 now uses a new approach to creating message signatures. The fact is, a single signature for each email makes it impossible to block new spam mailings whose content has been slightly modified. That is why UDS2 uses a new type of signature – 'shingles'. A shingle is a unique checksum that makes it possible to detect traces of the original text even if the spammers have changed some of the parameters (e.g., the insertion of special symbols).

An important difference between UDS2 and other signature-based systems is that it does not require a 100% shingles match to make a detection. As a result, even a modified version of a spam mailing will be blocked by the cloud system based on an existing shingle without the need for an analyst to review the message or to manually create a signature for the detected spam message.

Another advantage of the system is that information about new shingles is transmitted to client devices via urgent updates from Kaspersky Security Network. This provides users with protection within minutes of a new spam mailing appearing on the Internet.

Content Reputation

The UDS2-based Content Reputation technology filters suspicious or unwanted emails on the basis of their reputation. This is similar to the mechanism used for detecting suspicious programs based on their behavior on other users' devices (Kaspersky File Advisor).

The automated Content Reputation system of blocking messages, as well as UDS2, is based on work with shingles but is not limited to the verdicts "spam" or "not spam". If a number of shingles and email characteristics (e.g., the reputation of the server or the domain IP address from which it was sent) are suspicious, the system sends the email to "quarantine" so that a more detailed inspection can be made (e.g., similar emails from other Kaspersky Lab clients).

This sort of 'fuzzy' match between a new spam mailing and known spam messages enables suspicious emails to be added to the local blacklist before one of the thousands of recipients are deceived by the fraudsters.

Technology of delaying suspicious messages (quarantine)

Detecting some types of unwanted correspondence requires processing in the Kaspersky Security Network cloud service. For example, operations such as searching the database for a particular message characteristic or accessing external services require more time than is permissible within the time interval of a single online request. Quarantine technology allows the email to be placed in temporary storage with the option of re-scanning; if the verdict "spam" is issued, the email will be automatically blocked. This method is effective in cases where spam mailings are distributed within minutes.

Advantages of the anti-spam technology in Kaspersky Lab products

- The use of UDS2 and Content Reputation cloud technologies significantly reduces the response time to new spam mailings. The lists of shingles are updated and available for anti-spam solutions in real time.
- The technologies determine the sender's reputation based on analysis of the IP addresses and/or the domain the message was sent from and does not require

manual input by the spam analyst, which also speeds up the blocking of unwanted correspondence.

- Automated analysis of the web resources used in the content of spam mailings (e.g., analysis of data from the domain name registrar, frequency of URL use in mass mailings, etc.) allows spammer web resources to be blacklisted quickly.
- Each Kaspersky Lab user that has agreed to send information on cyber threats to the Kaspersky Security Network is also an anonymous source of information about new spam messages. All this together with the protocol for urgent delivery of updates to users reduces the response time to emerging email threats to just a few seconds.
- As well as "spam" or "legitimate email" verdicts, anti-spam can mark emails belonging to mass mailings, or sent by popular email platforms as “massmail”. The user can utilize this marker to separate private and business correspondence from advertising mass mailings and notifications.

Anti-spam technology is integrated in the following products:

For business

- Kaspersky for Linux Mail Server
- Kaspersky Security for Mail Gateway
- Kaspersky Security for Microsoft Exchange Servers
- Kaspersky Anti-Spam SDK

For home users

- Kaspersky Total Security – Multi-Device
- Kaspersky Internet Security – Multi-Device
- Kaspersky Internet Security