Anti-Spam

Contributed by Administrator
Tuesday, 14 November 2006

Spammers have long attempted to bypass anti-spam software by incorporating their sales pitch into an image, rather than sending it as plain text. When they first adopted this practice, they were able to evade simple content recognition tools. As image spamming grew in popularity, anti-spam vendors developed signatures designed to detect specific image spam messages. In doing so, the anti-spam software was able to reference these signatures and reject identical or nearly identical messages. However, spammers have now fired a new barrage of image spam using randomized images that appear identical to the human eye, yet appear to be entirely unique to most anti-spam software. Many of the changes to the images contained within spam messages are so subtle that they require a pixel-by-pixel examination of the image in order to detect the differences.

Image spam is junk email that replaces text with images as a means of fooling spam filters. Image delivery works by embedding code in an HTML message that links to an image file on the Web. Image spam is a larger drain on network resources than text spam because image files are larger than ASCII character strings. Larger files require more bandwidth and, as a consequence, cause greater degradation of transfer rates.

If the recipient's email program downloads images automatically, the image appears when the message is opened. The image itself may be a picture or drawing of alphanumeric characters that appears as text to the viewer, although it is processed as an image by the user's computer. Many spam filters, especially older or less sophisticated ones, rely upon certain text criteria on which to make judgments. Such filters typically watch for predetermined words in the subject lines of e-mail messages, suspicious word patterns and word frequency. Image spam is not stopped by such filters because it contains no words that can serve as the basis for blocking messages.