

Realtime
publishers

"Leading the Conversation"

The Essentials Series

IT Compliance Volume II

sponsored by

SECURE[®]
COMPUTING

by Rebecca Herold

What Businesses Need to Know About Reputation-Based Messaging Technology

by Rebecca Herold, CIPP, CISSP, CISA, CISM, FLMI

March 2007

An Overview of Messaging Filtering

Email security and annoyances have been plaguing organizations since email left the mainframe and dumb-terminal-only view and started residing on distributed mail servers, communicating with anyone who wants to send messages from outside the enterprise network. One of the first types of malicious and annoying email messages that started to occur was spamming. It was soon followed by fraud schemes, then phishing. Security has been trying to keep up with all the new and clever ways to get around the protections that organizations implement to try and keep spam and related types of malicious messages from entering the enterprise network.

Some messaging filtering methods work better than others. Some worked fantastically well when first introduced, but then the evolution of spamming methods soon outdated the once wonderful spam fighter. When new message-filtering solutions are rolled out, the spammers adjust their spam delivery methods to defeat the filters. What messaging security methods have been used? Table 1 provides a brief overview.

Security Method	Description
Blacklist	A blacklist is a list of email addresses and Internet domains that identify that specific mailservers originate spam and so should disallow or delete all corresponding messages without any further analysis. Basically, if a sender or sender domain is on the blacklist, it is considered spam.
Whitelist	A whitelist is a list of email addresses or Internet domains from which messages will always be accepted. Anything not on the list is always rejected.
Content filtering	Filtering technologies compares the From field, and/or the Subject field, and/or the message body with a list of words or Internet domains known to be used by spammers. If there are matches from known spammers and spam messages, the domain and/or sender is put in the email client's blacklist and the filter then treats it as spam from that point forward.
Bayesian filtering	Generally, this technology allows a spam filter to "learn" the characteristics of spam using a statistical analysis of message length and the distribution of words present in a message. Messages are put through a Bayesian filter many times, and the administrator tunes it to determine what is spam and what is not to a typical 90 to 95% accuracy rate.

Security Method	Description
Heuristic detection	Heuristic analysis uses a rule-based approach to determining whether an email message is spam by using a type of analyzer engine. The engine works through a rule base, checking the message against criteria that indicates possible spam. It assigns points when it locates a match. If the total point score meets or exceeds a specified threshold score, the file is flagged as suspicious and processed accordingly.
Mail retrieval proxy	These programs insert themselves between the email client and the mail server from which the email is delivered. All the email passes through the mail retrieval proxy, which then filters for spam and either deletes the spam or marks it so that the email client can delete it after being inspected by the recipient.

Table 1: Messaging security methods.

There are problems with these typical types of filtering. One significant problem is with misclassification of the messages. Messages are often misclassified by:

- Flagging legitimate email as spam; a “false positive”
- Flagging spam as legitimate email; a “false negative”

These misclassifications have a significant cost to organizations. False negatives use valuable bandwidth and storage and degrade overall workforce productivity. False positives can result in lost business that results from lost orders and communications and perceived unresponsiveness. Newer and better methods for filtering were needed.

What Is Reputation-Based Technology?

In December 2005, the U.S. Federal Trade Commission (FTC) published “Effectiveness and Enforcement of the CAN-SPAM Act: A Report to Congress,” indicating spam has become more targeted and clever in the methods used to bypass the traditional filters. In the past few years, reputation-based technologies have emerged to improve upon message-filtering success.

Application of reputation technology is very similar to establishing credit scores at a bank. At a very high level, the local spam defense appliance creates a profile of all message sender activity on the Internet and then uses the profile to watch for deviations from expected behavior. The system uses global trusted sources in combination with knowledge about the enterprise to generate a reputation score based upon the behavior of the sending host. This score is then used to determine whether messages are good, are confirmed spam, or are suspicious.

 Some of the techniques incorporated into reputation-based technologies include:

- Anomaly detection
- Blacklists
- Bulk-mailing detection
- Content analysis
- Forgery detection
- Header analysis
- Malicious URL detection
- Spam honeypots
- Spam signatures
- User-reported spam
- Whitelists

Reputation-based technologies can broaden the context in which the message is evaluated, improving catch rate and accuracy. For example, effective reputation-based technologies can defend against the use of embedded URLs by reviewing multiple parameters to evaluate the reputation of the associated Web sites.

 [Http://www.TrustedSource.org](http://www.TrustedSource.org) is a very interesting site that allows anyone to check current and historical reputation and sending patterns of email senders as well as view analytical information such as country of origin, network ownership, and hosts for known senders within each domain. This site also shows global email and spam trends.

Features to Look for in a Reputation-Based Spam Filtering Solution

Be sure to check the capabilities of a reputation-based spam filtering solution before investing in one. To be most effective, a reputation-based solution should:

- Measure the behavior and traffic patterns of a Web site to assess its trustworthiness; this will provide improved protection against spam, viruses, phishing, and spyware threats
- Use as large a volume of reputation data as is possible
- Use high-quality reputation data; reputations should be correlated by most effectively aggregating global behavioral and pattern knowledge data
- Use highly accurate reputation data; without high accuracy, organizations will experience high numbers of misclassifications
- Integrate and correlate multiple signature- and content-based detection techniques; these multiple layers create a much richer and comprehensive knowledge database and will help to minimize the risks of misclassifications
- Allow for real-time updates to the knowledge base to provide the ability to stop as many brand new (zero-day) threats as possible before they can enter the enterprise network
- Block emails from known spam sources
- Block directory harvest attacks and bounced mail attacks
- Detect image spam
- Apply embedded URL reputation data to block emails with links to malicious Web sites