Tax Relief from Spam

Dan Griffin, 2007-16-03

There have been some interesting email threads flying around internally over the past week discussing spam and how people must deal with it. You likely know that we formed a partnership with Secure Computing that resulted in a product offering called the Message Security Module (MSM) that can be licensed on a BIG-IP. The announcement is located here.

The email threads were related to MSM and discussed how long mail had to be retained and what constituted actually receiving a message which, in turn, leads to it having to be retained.

Companies are increasingly facing requirements to store email for longer periods of time. There is a huge amount of resources wasted on storing and backing up spam messages that have absolutely nothing to do with business. Once you've received the message, you need to deal with it - even if it is spam and that costs both time and money. Intel is currently facing a challenge to come up with old emails and I'm sure system administrators everywhere hate getting the request "we need to find all email associated with _____". If spam is eliminated from what had to be retained in the first place, at least there would be less to sift through.

We're hearing of organizations even backing up the spam that their spam gateways process. The end users don't see it hit their inbox but the internal systems still have to deal with it and that just doesn't seem right.

Typical anti-spam devices must receive, parse, scan and then evaluate a message in order for them to determine what to do with it (nicely put, Ken). Blocking spam by never allowing the message to be received in the first place seems to be a very good way to negate all taxes that downstream systems have placed on them due to spam - lower load on the network, less load on the anti-spam gateways, less storage required, less bandwidth for data backup, etc. With MSM, email from known bad senders is blocked before the message is ever received.

MSM basically works this way:

1. Send mail (SMTP) request is made from the Internet to BIG-IP running MSM
2. We do a query to Secure Computing's TrustedSource reputation database
3. TrustedSource replies with a reputation score for the sender
4. We either terminate the SMTP connection before the sender is able to send the message or pass it through based on the reputation score and the thresholds configured.
5. Done

Since the spam message is never actually received, other systems don't have to deal with it and thereby enjoy "Tax Relief" from the burden that spam would otherwise place on them.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com