CHAPTER 4

Mass-Mailing Based Threats

Revised: July 22, 2009, OL-10610-03

Introduction

This chapter introduces the concept of mass-mailing based threats and how to protect against them using the SCE.

Mass-Mailing Based Threats

The Mass-Mailing based threat detection module is based on monitoring SMTP session rates for individual subscribers. It uses the SCE platform's subscriber-awareness and can work in subscriber-aware or anonymous subscribers mode.

SMTP is a protocol used for sending email; an excess rate of such sessions from an individual subscriber is usually indicative of malicious activity involving sending email: either mail-based viruses or spam-zombie activity.

Configuration of Mass-Mailing Detection

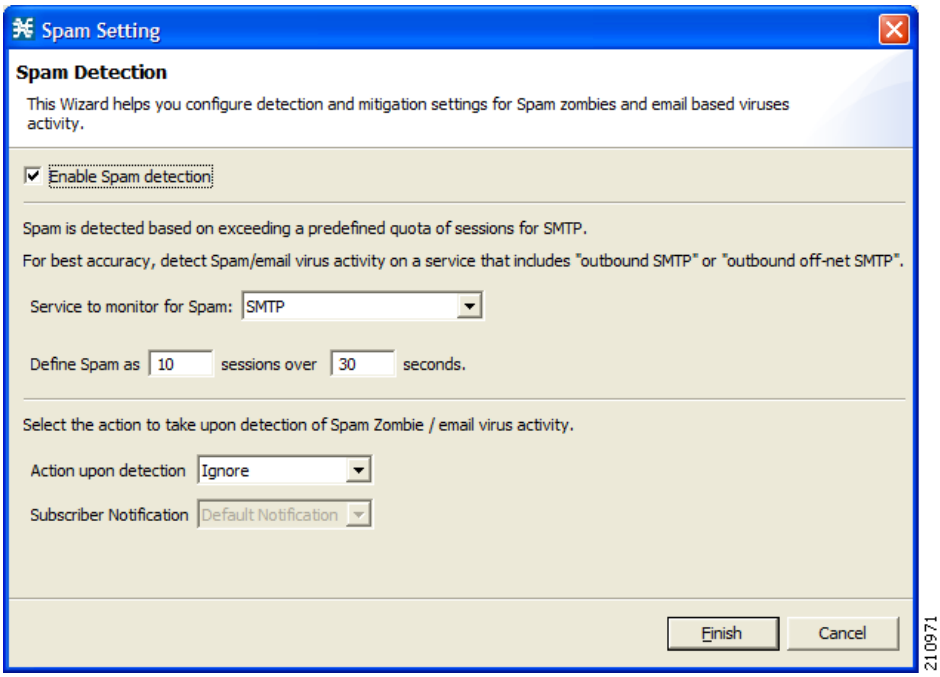
Mass mailing detection is based on a subscriber breaching a predefined SMTP session quota.

In order for the functionality to work, the system must be configured to subscriber-aware or anonymous subscribers mode. This allows the SCE platform to accurately count the number of SMTP sessions generated by each subscriber (Figure 4-1).

Configuration is based on the following stages:

- Configuring the service for detection—The user should configure the appropriate service, which should have been built before this stage, for mass-mailing detection. It is common to use a service that includes only the SMTP protocol. Refinements can be made to narrow down the scope of detection and to potentially reduce the detection threshold.
  - "Outbound SMTP"—To account for only SMTP sessions generated by a subscriber. SMTP should not normally be seen as an inbound protocol because a subscriber is not expected to run an SMTP server on their own premises. Inbound SMTP connections may represent other kinds of malicious activity. To build such a service, a user should include the "outbound" attribute in the service definition.
  - "OffNet SMTP"—SMTP that is not targeted to a subscriber's "home SMTP server". Normal email clients send email through a home SMTP server, which later relays the email to wherever needed. Limiting the service to offNet can avoid accounting for "legitimate" sessions; and so forth, sessions that subscribers conduct with the SMTP server of their ISP. One caveat is that prominent non-ISP email providers such as Google and Yahoo! etc. have started providing an SMTP based service either for a fee, or free of charge, OffNet is no longer a suitable differentiator between "legitimate" and "non-legitimate" activity. To build such a service, a user should include an SMTP server list in the "onNet" service definition, which turns the rest of SMTP into "offNet".
  - A combination of the two.
- Define the quota to be used for indicating anomalous email activity. The quota is defined as a number of sessions for a given period—number of sessions and period length are both configurable. It is suggested that the user should base the values for these fields on some baseline monitoring of subscriber activity. See Monitoring Mass Mailing Activity, page 4-3.
- Define the action to be taken upon detecting Mass-Mailing activity. The action to be taken can be:
  - Block—SMTP or the more granular service over which detection is done is blocked once the quota is breached. The blocking is removed once the quota monitoring period ends. For example, for a 10 sessions / 60 seconds limit, blocking will be applied after 10 sessions occur within the quota period (quota period is started at an arbitrary point), and be removed once the quota period ends.
  - Notify—Redirect the subscriber browsing sessions to a captive portal presenting a message from the operator. This is done using "subscriber notification".
  - A combination of the two.

Figure 4-1 Spam Setting Window



Monitoring Mass Mailing Activity

Mass mailing activity can be monitored based on information processed and stored in the CM database.

The most suitable report for detecting mass mailing activity by subscribers is the “top subscribers by sessions” report. This report is generated for the service and is used for mass-email detection (SMTP or a more granular service if it was defined). The report would highlight the IDs of subscribers most likely to be involved in mass mailing activity.

Figure 4-2 Top Subscribers Report