Proposal: Block virus e-mail instead of quarantine and notify

Summary

During the seven-day period starting April 26, 2004, the SMTP.UCLA.EDU cluster processed over nine million e-mail messages. Of these, slightly less than half a million were quarantined due to a viral infection. Each message quarantined generated a notice to the e-mail recipient informing of the quarantine. 99.1% of these messages were not acted upon. Of those notices acted upon, 99.8% were of no substantive value. Only a single message of the half million messages quarantined during this period was retrieved from the quarantine and had value to the message recipient. The process of providing access to this single message produced hundreds of thousands of e-mail notices and requires additional servers above the number needed simply to reject infected e-mail.

Current practice

When SMTP.UCLA.EDU identifies an infected e-mail message, the message is quarantined, and a virus notification message is generated. The notification is sent to the message’s intended recipient, and for UCLA recipients, the notification provides instructions on how to retrieve the infected message from the quarantine area.

Proposed practice

When SMTP.UCLA.EDU identifies an infected e-mail message, the message will be rejected with an error indication return code. E-mail messages would no longer be quarantined and stored for later retrieval.

Costs

This proposal can be implemented with no capital costs, and minimal engineering and operations staff time. Support costs for the Bruin OnLine Help Desk are expected to be measurably reduced.

Impact

Blocking infected messages at the submission stage will result in fewer resource demands on the SMTP.UCLA.EDU cluster. This will increase the useful lifetime of these servers, and slow the cluster’s rate of growth. Performance levels will improve. Instead of notifying the recipients of an infected e-mail, the sender of such an e-mail will be notified of the delivery failure by normal SMTP error processing. Valid e-mail could be blocked. Today, the quarantine process mitigates this issue by making blocked messages available; this mitigation would no longer occur.
Rationale

Between 2004/04/26 at 00:00 and 2004/05/02 at 00:00 (1 week), 9,040,477 messages were scanned by the SMTP.UCLA.EDU cluster. Of that number, 493,818 were blocked due to viral content. Of those blocked, 442 (0.9%) were later retrieved from the quarantine area. Of the 442 messages retrieved, all but one message were generated by variants of Netsky, Bagle, Dumaru, Mimail, Sefex, Klez, Sober, or MyDoom. Those viruses are all mass mailing infections and represent junk mail. The one message (0.2% of those retrieved / 0.002% of the total blocked / 0.00001% of the total scanned) that may have potentially had value was infected with W97/Thus, which is a word macro virus.

Given the exceptionally low rate at which messages are retrieved from the quarantine area, and the miniscule chance that such retrieval might result in a valid message being returned, the maintenance of the notification and quarantine process is of questionable value.

In addition, most of the notifications being produced are the result of mass mailing infections, and should properly be considered internally generated spam. Removal of these annoying messages would likely be well received by the campus community as a spam reduction measure.