1999 CERT Tech Tip: Email Bombing and Spamming

Original publication date: Apr 26, 1999

Revised: August 14, 2002

This document provides a general overview of problems associated with electronic mail bombing and email spamming. It includes information that will help you respond to and recover from this activity.

I. Description

Email bombing is characterized by abusers repeatedly sending an email message to a particular address at a specific victim site. In many instances, the messages will be large and constructed from meaningless data in an effort to consume additional system and network resources. Multiple accounts at the target site may be abused, increasing the denial of service impact.

Email spamming is a variant of bombing; it refers to sending email to hundreds or thousands of users (or to lists that expand to that many users). Email spamming can be made worse if recipients reply to the email, causing all the original addressees to receive the reply. It may also occur innocently, as a result of sending a message to mailing lists and not realizing that the list explodes to thousands of users, or as a result of a responder message (such as *va cation(1)*) that is setup incorrectly.

Email bombing/spamming may be combined with email spoofing (which alters the identity of the account sending the email), making it more difficult to determine who actually sent the email. For more details on email spoofing, see

http://www.cert.org/tech_tips/email_spoofing.html

II. Technical Issues

- If you provide email services to your user community, your users are vulnerable to email bombing and spamming.
- Email spamming is almost impossible to prevent because a user with a valid email address can spam any other valid email address, newsgroup, or bulletin-board service.
- When large amounts of email are directed to or through a single site, the site may suffer a denial of service through loss of network connectivity, system crashes, or failure of a service because of
  - overloading network connections
  - using all available system resources
  - filling the disk as a result of multiple postings and resulting syslog entries

III. What You Can Do

1. Detection
   If your system suddenly becomes sluggish (email is slow or doesn't appear to be sent or received), the reason may be that your mailer is trying to process a large number of messages.

1. Reaction
   a. Identify the source of the email bomb/spam and configure your router (or have your Network Service Provider configure the router) to prevent incoming packets from that address.
   Review email headers to determine the true origin of the email. Review the information related to the email bomb/spam following relevant policies and procedures of your organization.
   b. Follow up with the site(s) you identified in your review to alert them to the activity. Contact them to alert them to the activity.
   NOTE:

   When contacting these sites, keep in mind that the abuser may be trying to hide their identity.

   We would appreciate it if you sent a copy of your message to cert@cert.org; this facilitates our work on incidents and helps us relate ongoing intruder activities.

   If you have a CERT reference number (e.g., CERT#XXXXX) for this incident, please include it in the subject line of all messages related to this incident. (NOTE: The CERT/CC assigns this reference number, so if you do not have one, one will be assigned once we receive the incident report.)

To find site contact information, please refer to

http://www.cert.org/tech_tips/finding_site_contacts.html

c. Ensure you are up to date with the most current version of your email delivery software (sendmail, for example) and increase logging capabilities as necessary to detect or alert you to such activity.

1. Prevention
   Unfortunately, at this time, there is no way to prevent email bombing or spamming (other than disconnecting from the Internet), and it is impossible to predict the origin of the next attack. It is trivial to obtain access to large mailing lists or information resources that contain large volumes of email addresses that will provide destination email addresses for the spam.

   a. Develop in-house tools to help you recognize and respond to the email bombing/spamming and so minimize the impact of such activity. The tools should increase the logging capabilities as well as check for and alert you to incoming/outgoing messages that originate from the same user or same site in a very short span of time. Once you identify the activity, you can use other in-house tools to discard the messages from the offending users or sites.
   b. If your site uses a small number of email servers, you may want to configure your firewall to ensure that SMTP connections from outside your firewall can be made only to your central email hubs and to none of your other systems. Although this will not prevent an attack, it minimizes the number of machines available to an intruder for an SMTP-based attack (whether that attack is a email spam or an attempt to break into a host). It also means that should you wish to control incoming SMTP in a particular way (through filtering or another means), you have only a small number of systems--the main email hub and any backup email hubs--to configure. More information on filtering is available from

      http://www.cert.org/tech_tips/packet_filtering.html

   c. Consider configuring your mail handling system(s) to deliver email into filesystems that have per-user quotas enabled. Doing this can minimize the impact of an email bombing attack by limiting the damage to only the targeted accounts and not the entire system.
   d. Educate your users to call you about email bombing and spamming.
   e. Do not propagate the problem by forwarding (or replying to) spammed email.

IV. Additional Security Measures That You Can Take

1. If you have questions concerning legal issues, we encourage you to work with your legal counsel.
   U.S. sites interested in an investigation of this activity can contact the Federal Bureau of Investigation (FBI). Information about how the FBI investigates computer crimes can be found here

   http://www.cert.org/tech_tips/FBI_investigates_crime.html

   For information on finding and contacting your local FBI field office, see

   http://www.fbi.gov/contact/fo/fo.htm

   Non-U.S. sites may want to discuss the activity with their local law enforcement agency to determine the appropriate steps for pursuing an investigation.
2. For general security information, please see

   http://www.cert.org/

Revision History	
Apr 26, 1999	Converted to new web format
August 14, 2002	Updated to reflect more current information and resources