Denial of service is usually caused by people trying to cause problems for their victims or by misconfiguration of software. Mail bombing, distributed denial-of-service attacks, and list-subscription bombing are examples of the former. Mail storms caused by list administrators who allow automated out-of-office messages to be distributed by their list server are an example of the latter.

Here's another example.

I recently upgraded from MS-Outlook 2002 to Outlook 2003 on my main computer after trying the new version of Office 2003 that was installed on my university laptop. I found the new functionality in the much-reviled e-mail client helpful and worth the price of the upgrade.*

I have been using Cloudmark’s SpamNet service for over a year now and have been consistently pleased with its ability to snag junk mail efficiently. However, a couple of days ago I came back to my computer in the morning after having left Outlook loaded overnight and found my system doing such a huge amount of I/O that it was interfering with performance; everything was sluggish, including keyboard entry, mouse movements, menu response and so on.

At first I thought my defragmentation program might still be running, although normally it would stop immediately at the first sign of user activity. It wasn't. What I did find was 8,000 messages in my spam folder in Outlook. The list included hundreds of copies of several spam messages.

Now, getting one spam message is bad enough; getting hundreds of copies of the same spam message stored in my OUTLOOK.PST file is not my idea of fun. SpamNet was in fact still deleting apparently nonexistent spam. Any time I switched to the inbox the I/O would resume.

My best guess is that version 3.0 is unable to recognize that a message has been deleted, and so it continues to delete spam repeatedly. Since I normally flush deleted messages from my inbox just before switching out of that folder, I didn't notice the repeated spam messages until I left Outlook unattended overnight. By that point, there were enough deleted spam messages in the inbox to cause significant I/O; flushing those deleted messages immediately stopped the excessive I/O.

I went to the SpamNet support site and immediately found a thread in the user forum discussing this problem; some users had canceled their subscription for the product as a result of the bug.

My own workaround is to disable the automatic scan; one can run the scan on demand instead of automatically. Then I immediately purge deleted messages from the inbox to prevent them from being caught again.

According to CloudMark staff, the next update of SpamNet repairs this problem and it is due in mid-November.
Until then, I'll have to exercise some self-discipline to prevent further self-denial of service.

* Note: Dear Readers, PLEASE don’t flood me with attacks on Outlook. I’m aware of security issues but I do keep the product up to date, run an excellent firewall, have automatically-updated antivirus, and find the product a good choice for my needs. I really don’t have time for religious wars about e-mail clients.

* * *

A Master’s degree in the management of information assurance in 18 months of online study from Norwich University – see <http://www3.norwich.edu/msia> for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2004 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.