

Surviving an Email Attack

It was every mail administrator's nightmare; spammers were forging valid email addresses at a site hosted by solutio.dk as return addresses on massive spam runs.

Today's spammer never uses their email address as the From: address of their spam, but many misguided systems administrators (and even some anti-spam software vendors) configure their systems to bounce detected spam messages back to the apparent sender of the spam. This can result in a site was getting hit with millions of forged, bounced spam messages per day.

This type of Denial of Service (DOS) attack is known as a "Joe Job" and there is little a site can do to proactively prevent this type of email attack. The attack on Solutio's customer actually resulted in almost 3,000,000 attempts to deliver bounced spam messages to innocent users at the site.

With a single CPU mail gateway, running conventional anti-spam software, the site could not hope to sort out the 10,000 real email messages from the 2,990,000 bogus messages and email delivery at the site was effectively halted.

Since Solutio was already using anti-spam software from Fort Systems Ltd. Brian Jensen, Solutio's owner turned to them for help salvaging his client's email. Fort Systems had just released BarricadeMX software, which uses a completely new approach to safely reduce the number of messages that a site accepts for processing.

Simply by installing BarricadeMX software on his existing email gateway, Brian was able to refuse the delivery of all of the bounced messages and spam and accept and process the actual email - all on the same single CPU server that had been swamped by millions of Daily connection attempts before the installation of BarricadeMX.

The new software from Fort Systems works because it can almost always determine if the sender of the message is a spammer just by examining the content of the short header of the email and the behavior of the sender during the delivery of the header. This early detection of spam results in a substantial reductions in load, bandwidth requirements and the processing time required for the average connection.

And the clients are reporting that almost no spam is getting through and there are virtually no false positives. If a message is rejected before acceptance, an error message is sent back to the sender letting them know that their email was rejected and who to contact if the message was rejected by mistake. This

rejection error can be safely sent during the delivery attempt because the actual sending server and the real sender of the message get the error message, not the bounced forged recipient!

The email gateway at Solutio.dk now routinely handles over 2,000 simultaneous incoming email connections while showing a negligible load on the system's CPU, memory and disk I/O. In fact the system is actually operating under less load and with better spam detection than before the DOS attack started.

Fort Systems Ltd. has made this BarricadeMX available at no charge for 30 to 60 days for sites that are under any type of DOS email attack. BarricadeMX currently runs on Red Hat, CentOS, SuSE, OpenBSD and FreeBSD Operating Systems and Microsoft and Mac OS X ports are planned.

For more information or help in surviving an email attack please contact info@fsl.com or visit www.fsl.com.

Release date:

December 11, 2007

Media Contact:

Robin Bains
Fort Systems Ltd.
robin@fsl.com
202 595-7760 (USA)