# The Joe Job DoS attack

By John Leyden
Published Tuesday 6th April 2004 17:30 GMT

A problem with the way that non-delivery notifications are sent by many mail servers could be exploited to launch "mail bomb" denial of service attacks.

Incorrectly configured mail servers may respond to mail delivery failure with as many non-delivery reports as there are undeliverable cc: and bcc: addresses contained in the original email. By forging the source of an email, hackers could bombard systems with spurious emails.

Security researchers have now demonstrated how easy it might be to turn such 'Joe Jobs (http://catb.org/~esr/jargon/html/J/joe-job.html)' into deliberate denial of service attacks.

Hackers could use badly set-up mail servers as multipliers (every bogus message could generate dozens) and flood any target email system or account.

Non-delivery notification emails generated by these systems often include a full copy of the original email sent in addition to any file attachments.

### Platform-independent DoS risk

The vulnerability is dependant on the *configuration* of SMTP servers, rather than software platform. Tests suggest the vulnerability works across the board, independent of mail server package or version.

Gunter Ollmann, professional services director at Next Generation Security Software (NGSSoftware), warns that the problem is easy to exploit. Ollmann, along with consultant Ivo Silvestri began looking at the problem on the instigation of Stefan Frei, a colleague who runs a number of Swiss webmail operations. These services were straining under the load ofbounced messages. Looking at how these messages were generated established the potential basis for deliberate attacks, rather than the accidental bombardment experienced by Frei's services.

Tests (http://www.techzoom.net/paper-mailbomb-details.asp) suggest that larger organisations tend to be more vulnerable to the "mail bombing" attack.

"This vulnerability appears to affect around 30 per cent of our main study group (the Fortune 500), and has significance to all essential email communications," Ollmann warns.

"We have proved that this vulnerability can be easily exploited and can be used to DoS almost any SMTP service on the Internet. By utilising multiple vulnerable STMP servers,

a distributed DoS is possible, and can be used to cause the loss of mail services (and in extreme cases all Internet connectivity) to any organisation."

### Action stations

The three researchers had originally intended to publish their analysis of the problem after the Easter break. But talk of the issue on a popular vulnerability discussion forum has prompted them to release their guidance (http://www.techzoom.net/mailbomb) ahead of schedule.

Ollmann isn't aware of any instances where the attack mechanism has been used in anger. But this is no reason for complacency.

Developers and mail administrators are urged to secure their SMTP mail services, as explained here (http://www.techzoom.net/paper-mailbomb.asp?id=mailbomb) (PDF). The fix is simple enough: don't send the attachment part of non-delivery receipt; and send one email in response to every mail failure, rather than one for every intended recipient. ®

### Related Stories

Sendmail suffers second major flaw (http://www.theregister.co.uk/2003/03/31/sendmail_suffers_second_major_flaw/)
Outlook Express becomes attack platform, of sorts (http://www.theregister.co.uk/2002/09/12/outlook_express_becomes_attack_platform/)
Beware the Habeas Joe Job (http://www.theregister.co.uk/2004/01/19/beware_the_habeas_joe_job/)