NewScientist.com

NEWS | EXPLORE BY SUBJECT | LAST WORD | SUBSCRIBE | BLOGS | VIDEO | SEARCH | ARCHIVE | RSS

Email attack could kill servers

Click to Print

14:29 06 April 2004
NewScientist.com news service
Will Knight

A crafty way of knocking out any email server using a few carefully constructed emails has been identified by a team of computer security experts.

The trick involves sending forged emails that contain thousands of incorrect addresses in the "copy to" fields that are normally used to send duplicate messages.

It was discovered by Stefan Frei, who maintains the computer security site Techzoom, along with Ivo Silvestri, an independent security researcher, and Gunter Ollmann of the UK-based company NGSSoftware. They sent forged messages to the largest email servers on the internet, and found they could force huge quantities of unwanted email to pour into another mail server of their choice.

The exploit depends on finding a server configured to return an email plus its attachments to each incorrect address. But this can be tested by sending just a single message.

The next step is to forge an email so it appears to come from the mail server that is to be the target of the attack. This is also relatively simple trick. Finally, the forged email, complete with the thousands of incorrect addresses is sent. The resulting avalanche of "bounced" messages sent to the target server would almost certainly cause it to crash, and leave its users without access to their mail.

"With one 10 kilobyte email I could then send 100 megabytes back to a server of my choosing," says Gunter Ollmann, one of the researchers who identified the potential attack.

Fortune 500

The researchers tested the email servers of all Fortune 500 companies and found that 30 per cent could be used to launch this type of attack.

All email is sent across the internet using the Simple Mail Transfer Protocol (SMTP), which stipulates that a notification should be sent whenever a message with a bad address is received. There are numerous different types of email server, however, which can all be configured in various ways.

Ollmann adds that using an insecure email server to send the initial messages would make the attack virtually untraceable. "You can pretty much do it anonymously," he told **New Scientist**.

It should be fairly simple to reconfigure mail servers so that they are no longer vulnerable to this attack, but Ollmann notes that is up to each company to take this step:

"They all need to take a look at their mailing architecture," he says. "It only takes two or of these companies for the attack to work."

Related Articles

New hacking tool hijacks file-sharing networks
http://www.newscientist.com/article.ns?id=dn4799
19 March 2004

Microsoft should weather zombie PC attack
http://www.newscientist.com/article.ns?id=dn4629
2 February 2004

mart routing could stop distributed net attacks
http://www.newscientist.com/article.ns?id=dn2973
25 October 2003

Weblinks

NGSSoftware
http://www.ngssoftware.com

Simple Mail Transfer Protocol
http://www.ietf.org/rfc/rfc0821.txt

Mailbomb paper, Techzoom
http://www.techzoom.net/paper-mailbomb.asp?id=mailbomb

Close this window

Printed on Wed Mar 12 08:44:54 GMT 2008