

Hackers attack heart of the net

Hackers have attempted to topple key parts of the internet's backbone, in one of the most significant attacks of recent years.

The target was servers that help to direct global internet traffic.

In the early hours of Tuesday three key servers were hit by a barrage of data in what is known as a distributed denial-of-service attack.

There is no evidence so far of damage, which experts are saying is testament to the robust nature of the internet.

Websites unreachable

The so-called root servers involved in the attack act as a kind of global address book for the internet by translating website name information into IP addresses to enable computers to visit particular sites.

The servers involved were each operated by a separate body - the US Defense Department, the net's oversight body ICANN (Internet Corporation for Assigned Names and Numbers) and UltraDNS, which manages traffic for websites ending in "org" and some other suffixes.

The most interesting element of this concerted attack is that the system demonstrated the benefits of being dispersed and interoperable. There was no one point of failure,

Paul Levins, Icann

"Last night we were seeing attacks which lasted for a couple of hours. There were probably hundreds of root server operators co-operating around the globe to make sure that the average user wouldn't notice," said Paul Levins, executive officer of Icann.

The fact that the attack remained invisible to users is being hailed as a success.

"The most interesting element of this concerted attack is that the system demonstrated the benefits of being dispersed and interoperable. There was no one point of failure," said Mr Levins.

The type of attack favoured in this case involves floods of data being sent to a machine in an effort to knock it over.

"A denial-of-service attack is a bit like fourteen fat men trying to get into an elevator - nothing can move," explained Graham Cluley, senior consultant at security firm Sophos.

If a part of the DNS system went down it would mean websites could be unreachable and e-mail undeliverable.

Research last year suggested that holes in the net's addressing system could leave 85% of the net vulnerable to take over if hackers combined simple attacks with denial-of-service attacks.

Mischief or money?

The fact that the attack remained invisible to users will be seen as evidence that the heart of the net can be kept healthy.

It was, said Mr Levin, too early to analyse exactly what happened or why; although there is speculation that zombie computers - the machines of innocent users which are recruited by hackers - were involved in the attack.

Whether the motive was mischief or money - in the form of blackmail - remains to be seen but Mr Cluley believes it is more likely to be the former.

"If money is involved there is a trail for investigators to follow. Attacking a target like this is just asking for trouble - like letting a huge bomb off in a building," he said.

Story from BBC NEWS:

<http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/6338261.stm>

Published: 2007/02/07 11:39:45 GMT

© BBC MMVII