Attacks begin on net address flaw

Attack code that exploits flaws in the net's addressing system are starting to circulate online, say security experts.

The code could be a boon to phishing gangs who redirect web users to fake bank sites and steal login details.

In light of the news net firms are being urged to apply a fix for the loop-hole before attacks by hi-tech criminals become widespread.

Net security groups say there is anecdotal evidence that small scale attacks are already happening.

Address list

"We are in a lot of trouble," said security guru Dan Kaminsky who found the flaw in the net's Domain Name System (DNS) in March 2008.

"This attack is very good," he said. "This attack is being weaponised out in the field. Everyone needs to patch, please."

The DNS acts as the net's address system and helps computers translate the website names people use, such as bbc.co.uk, into the numerical equivalents preferred by machines.

If exploited the flaw would allow malicious hackers to direct people to fake sites even if that user typed in the correct address for the place they wanted to visit.

Now security researchers have come up with two separate methods for attacking the flaw.

The code used in the attacks has been added to a popular testing tool called Metasploit used by both good and bad hackers alike to find weaknesses in computer systems.

The attack code was developed following the accidental leaking of the bug Mr Kaminsky discovered. Initially he had planned to release more information in October.

After being discovered in March, information about it was shared with large net organisations such as Cisco, Google, Yahoo and Microsoft to give them chance to produce patches and fixes.

Now net supply firms are being urged to get on with the job of updating their systems so customers are not left at risk.