Warnings about junk mail deluge

The amount of spam circulating online could be about to undergo a massive increase, say experts.

Anti-spam group Spamhaus is warning about a novel virus which hides the origins of junk mail. The program makes spam look like it is being sent by legitimate mail servers making it hard to spot and filter out. Spamhaus said that if the problem went unchecked real e-mail messages could get drowned by the sheer amount of junk being sent.

Before now many spammers have recruited home PCs to act as anonymous e-mail relays in an attempt to hide the origins of their junk mail. The PCs are recruited using viruses and worms that compromise machines via known vulnerabilities or by tricking people into opening an attachment infected with the malicious program. Once compromised the machines start to pump out junk mail on behalf of spammers. Spamhaus helps to block junk messages from these machines by collecting and circulating blacklists of net addresses known to harbour infected machines. But the novel worm spotted recently by Spamhaus routes junk via the mail servers of the net service firm that infected machines used to get online in the first place. In this way the junk mail gets a net address that looks legitimate. As blocking all mail from net firms just to catch the spam is impractical, Spamhaus is worried that the technique will give junk mailers the ability to spam with little fear of being spotted and stopped. Steve Linford, director of Spamhaus, predicted that if a lot of spammers exploit this technique it could trigger the failure of the net's e-mail sending infrastructure. David Stanley, UK managing director of filtering firm Ciphertrust, said the new technique was the next logical step for spammers. "They are adding to their armoury," he said. The amount of spam in circulation was still growing, said Mr Stanley, but he did not think that the appearance of this trick would mean e-mail meltdown. But Kevin Hogan, senior manager at Symantec security response, said such warnings were premature. "If something like this mean the end of e-mail then e-mail would have stopped two-three years ago," said Mr Hogan. While the technique of routing mail via mail servers of net service firms might cause problems for those that use blacklists and block lists it did not mean that other techniques for stopping spam lost their efficacy too. Mr Hogan said 90% of the junk mail filtered by Symantec subsidiary Brightmail was spotted using techniques that did not rely on looking at net addresses. For instance, said Mr Hogan, filtering out e-mail messages that contain a web link can stop about 75% of spam.