sandvine®

Intelligent Broadband Networks

Trend analysis: Spam trojans and their impact on broadband service providers

Sandvine Incorporated, June 2004

OVERVIEW: The majority of spam – as much as 80 per cent of all unsolicited marketing messages sent -- now emanates from residential ISP networks and home user PCs. This is due to the proliferation of spam trojans, bits of surreptitious malware code embedded in residential subscriber PCs by worms and spyware programs.

Worm attacks are growing in frequency because they provide a fast means of infecting a vast number of computers with spam trojans in a very short period of time. It's no surprise that many service providers report an upsurge in spam traffic immediately following a worm attack. Worms can credibly be seen as the delivery mechanism for unsolicited mass-market direct email campaigns.

The trend to automating spam by hijacking home user machines has become a significant threat to service provider business models, imposing unplanned costs, disrupting service and making them targets for large ISPs who see their smaller networks as sources of malicious traffic.

Spam is now a problem for everyone who uses or provides Internet access: ISP networks, enterprise customers and end users. In all cases the spam problem is unlikely to abate without active intervention by internet service providers.

DEFINING THE PROBLEM: Spam trojans exploit vulnerabilities created by worms to bypass normal email routing and use SMTP to drop spam messages directly into end user machines.

IMPACTS: In practical terms this means large volumes of spam traffic getting past outbound spam filters and "gumming up" email servers on the inbound side. Most spam filters succeed in identifying only 90 per cent of spam – a level of effectiveness that can be overcome by the massive volume of messages spam Trojans are capable of generating.

This mushrooming volume of email is forcing ISPs to purchase additional email servers to accommodate spam-induced traffic and avoid service degradations. Anti-spam software must then be purchased and installed on each.

For small to medium sized ISPs, the proliferation of spam sent via spam trojans is also drawing the unwanted attentions of large service providers, who are coming to see smaller providers as sources of spam and other malicious traffic. Antagonisms have begun to surface and at least one major service provider is issuing 'cease & desist' letters to smaller ISP competitors, warning that their entire domain could be blacklisted if the spam emanating from their networks is not addressed.

SOLUTIONS: A multi-layered approach to the spam problem is required. While spam filters on both mail servers and end user machines should continue as one line of defense against unsolicited email, the sheer volume of email traffic generated by spam trojans means additional defenses must be added to ISP network infrastructure.

Traditional spam filtering techniques based on the content of messages must be augmented with techniques that recognize the unique behaviour of spam trojans on the network and take appropriate action to stop spam traffic from leaving a host network, or black-holing it – if and when it arrives from another.

For more information on spam and its impact on broadband service providers, please visit www.sandvine.com, or send an email to info@sandvine.com.