IBM Introduces New Weapons in the Fight against Spam

March 22 2005

IBM today introduced new anti-spam technology to help companies reduce the cost and security risks associated with spam and make existing spam filtering solutions more effective.
Dealing with spam is costing businesses a significant amount of time, money and system resources. In addition to loss of workforce productivity, spam has become a vehicle for identity theft and propagating viruses and worms that can be devastating to company reputations and IT systems.

Developed by IBM and dubbed FairUCE ("Fair use of Unsolicited Commercial Email"), the new technology helps filter and block spam by analyzing the domain identity of an email -- using built-in identity management capabilities at the network level. FairUCE is able to establish the legitimacy of an e-mail message by linking it back to its origin -- thereby establishing a relationship between an e-mail domain, e-mail address and the computer from which is was sent. Since IP addresses are fixed and cannot be changed, FairUCE can identify if the messages are arriving from a zombie computer, bot device or legitimate email server. Unlike spam filters, which identify spam by scanning the content of every email message entering the network, FairUCE blocks and eliminates spam from spammers who assume false identities to hide who they really are.

The new solution effectively minimizes the growing threats of phishing and spoofing - tactics used to trick people into disclosing information that can lead to identity theft. Content filtering also heavily taxes IT

systems, siphoning off bandwidth used for business needs. IBM's new FairUCE spam technology can help customers identify potentially harmful traffic much earlier -- before it affects their networks.

The February IBM Global Business Security Index -- the monthly report that measures the global security threat landscape -- found that spam has actually decreased from 83.11 percent in January to 76.3 percent in February -- a decrease of seven percent.(1) Despite the decrease, spam continues to be a major headache and tax on IT staffs worldwide.

"Spam has become a high priority security issue for businesses today," said Stuart McIrvine, director of corporate security strategy, IBM. "By creating a multi-layered defense that proactively repels spam at its source, companies can get ahead of spammers and malicious hackers who are always looking for new ways of penetrating IT systems through email."

Highlights from IBM's Global Business Security Index report for February 2005:

-- Spam -- during February, IBM Security Intelligence Services found that 1 in every 1.3 (or 76.0 per cent) emails was identified and intercepted as spam, and 1 in every 46.1 (or 2.2 per cent) emails was stopped for carrying a virus, trojan or other malicious content.

-- Microsoft vulnerabilities -- on February 8, Microsoft announced a number of vulnerabilities in Windows, Internet Explorer, and other applications. One of the most serious vulnerabilities announced was in the Server Message Block (SMB) protocol used by most Windows systems. To exploit the vulnerability, an attacker could trick the user into visiting a malicious URL or could also send malicious SMB traffic to vulnerable systems. IBM recommends businesses use patches to fix the vulnerabilities.

-- Malware outbreaks -- in February, a new variant of MyDoom and a new strain of malware -- Poxdar -- appeared. MyDoom spreads via email, while Poxdar seeks to exploit a number of Microsoft Windows vulnerabilities. IBM recommends that businesses update antivirus signatures and solutions to address these variants.