Viruses and Worms Targeting Mobile Devices, Satellite Communications Anticipated in 2005

February 10 2005

IBM announced the results from its 2004 Global Business Security Index Report and provided an early look at potential security threats in 2005. Based on early indicators, a new and troubling trend this year may be the aggressive spread of viruses and worms to handheld devices, cell phones, wireless networks, and embedded computers, which include car and satellite communication systems.

IBM Global Business Security Index Report summarizes security threats in 2004 and provides trends for 2005. According to the report, there is a trend of spreading worms and viruses to mobile phones, PDAs, wireless networks, and embedded computers, such as satellite comunications systems and cars computers. Bluetooth and other wireless technologies provide new exposures for hackers to target.

Email worms and viruses wreaked havoc on corporate networks in 2004. Email worms such as Bagle, Netsky and Mydoom led the pack in the number of variants and overall impact. During the latter part of 2004, a growing number of viruses aimed at PDAs and other mobile devices, such as the Cabir worm, were released. It is likely that such worms will be used by copycats and may spur an epidemic of viruses aimed at mobile devices.

"After a year like 2004, many IT departments feel beaten down from combating viruses like Mydoom and Netsky," said Stuart McIrvine,

director of IBM's security strategy. "However, through sophisticated intelligence gathering and analysis, IBM can now identify and understand many of these risks. In addition, businesses and consumers can use this information to help them to not only anticipate these security risks, but more importantly, to prepare themselves to avoid a new breed of attacks in 2005."

IBM's Global Business Security Index report summarizes an early view of potential trends in 2005:

Mobile Devices - Mobile devices such as PDAs and cell phones are the new frontier for viruses, spam and other potential security threats. Bluetooth and other wireless technologies that connect mobile devices pose new exposures for hackers to target.

Identity Theft - There appears to be no end in sight for identity theft. Phishing attacks that use "spoofed" e-mails and fraudulent websites designed to deceive recipients into divulging personal information such as credit card numbers, account user names and passwords, social security numbers, etc. will likely continue to plague businesses and consumers.

Malware - Malicious software (known as "malware") writers are getting smarter and are employing basic software development practices to spread destructive software.
Instant Messaging - Botnets will likely move to instant messaging networks for command and control of infected systems.

VoIP - There will likely be an increase in the disruption of VoIP networks. In particular, eavesdropping and denial of service attacks carried out remotely against VoIP networks could provide significant damage for enterprise organizations.

The report summarizes the following assessment regarding 2004:

Viruses - Viruses are on the upswing, despite extensive efforts to contain them. The number of known viruses grew considerably in 2004.

Spam - Despite The CAN-SPAM Act, spam has continued to proliferate. It is estimated that a majority of all email traffic on the Internet is spam.

Phishing - Phishing continued to grow in 2004.

Natural Disasters - The tsunami that impacted three continents in the Indian Ocean ended a devastating year of natural disasters. Hurricanes in North America, typhoons in Asia and numerous other events around the world impacted lives and property. For corporations, the safety of their employees, their property, and IT environments is of serious concern. The events of 2004 highlight the need for all organizations to have a continuity and disaster recovery plan in place.

Digital Images - 2004 ushered in a new era of vulnerabilities that affected digital picture formats such as JPEG and BMP photos. Typically seen as benign files, hackers have discovered ways to embed malicious code in pictures in order to attack a number of different applications used to render images. Clicking on an infected image could set off a virus or worm without the user's knowledge.