Spam down but 'zombie' armies growing: McAfee

May 7 2009

"Cyber war!" flashes on the screen at an internet security conference. Hackers appear to be beefing up armies of "zombie" computers to recover from a major hit scored in the battle against spam email, according to software security firm McAfee.

Hackers appear to be beefing up armies of "zombie" computers to recover from a major hit scored in the battle against spam email, according to software security firm McAfee.

A McAfee report said that during the first three months of this year, nearly 12 million new computers were added to the ranks of machines infected with "malware" that lets cybercriminals use them to spew spam.

The ominous news came with word that the amount of spam dropped 20 percent during the same period, evidently as a result of the elimination

of a "McColo" spam-generating operation late last year.

The rate of spam email dropped from an average 153 billion daily last year to 100 billion a day in March, according to the McAfee report released Tuesday.

"Seems the bad guys are attempting to recover from last November?s takedown of a central spam-hosting ISP by rebuilding their army," researchers said in a McAfee Threats Report for the first quarter of 2009.

The United States unseated China as the country with the most "botnet-infected" computers, accounting for 18 percent of the world's "zombie machines" as compared with China's 13.4 percent, according to McAfee.

Australia "rocketed" to third place on the list with 6.3 percent of the world's zombie computers after not even being it into the Top 10 list at the end of last year.

"The Land Down Under is proving to be fertile ground for zombie recruiting," McAfee researchers wrote.

Despite the international nature of botnets, spammers seem to prefer sending the unwanted email from the United States, which McAfee said was the source of 35 percent of the messages as compared to 7.3 percent from second-place Brazil.

Cybercriminals are also increasingly rigging legitimate websites to sneak viruses onto visitors' computers, according to McAfee.

Threat researchers reported discovering in March more than 800 new versions of a Koobface virus tailored to attack users of hot social-networking website Facebook.

"Servers hosting legitimate content have increased in popularity with malware writers as a means for distributing malicious and illegal content," McAfee reported.

Cybercrooks have "deeply compromised" computers at key Russian and Eastern European corporations and government agencies, according to McAfee.

"The Internet knows no geographical boundaries," researchers said in the report. "It is now apparent that cybercriminals will attack any target of opportunity they can find."

Spam levels are the lowest the world has seen in two years, but are expected to rise.

"The question is not whether spam will return to previous levels, but rather when it will return," McAfee said. "There is data regarding new zombie and botnet creation that suggest the time may not be too far in the future."

(c) 2009 AFP