Security companies on alert as scam e-mails plunge

January 14 2011, By Byron Acohido

E-mail spam has plunged by more than half since Christmas Day when the world's largest criminal spamming operation inexplicably shut down.

Even so, cyber-security experts have moved to high alert: They fear that top spamming groups might be shifting to sneakier, more lucrative online scams. "If the past is any indication, these guys will regroup," says Fred Touchette, senior analyst at messaging security firm AppRiver.

On Dec. 25, the Rustock botnet - the world's largest source of the unsolicited messages that inundate e-mail systems - went dark, followed by two smaller operations.

Spam is difficult to eradicate because it originates from networks of infected home PCs; the Rustock botnet used as many as 1.7 million PCs to send out e-mail ads for fake drugs.

The spam that anti-virus giant Symantec filters from the e-mail systems at large organizations plummeted to 47 billion per day, down from a daily average of 131 billion per day in 2010. Other e-mail security firms reported a similar drop-off.

On Monday, after a 16-day hiatus, Rustock began spreading spam again, though at a lower level. It's not clear what will happen next. E-mail spam has become simple to block. That makes it more costly to generate the volume of messages needed to saturate filters, says Mikko Hypponen, analyst at anti-virus firm F-Secure.

Yet Rustock and dozens of other large spamming networks remain pervasive and resilient. says Gunter Ollmann, vice president of research at security firm Damballa.

Cyber-gangs could repurpose infected PCs to bedevil consumers and companies by:

-Corrupting searches. Botnets can drive up the profile of sites that might show up in response to popular search queries. The ones promoted by the botnets can be set up to infect visitors' PCs with programs which can, for example, stealthily hijack cash from your online bank accounts.

-Accelerating click fraud. Botnets also can click on online ads that link to advertisers' Web pages. An ad network that distributes ads pays the crooks each time a PC clicks on an ad. "These are technically talented guys using their talents for badness," says Alex Cox at security firm NetWitness.

-Changing ad routing. A botnet operator can make sure that infected PCs only display ads from networks affiliated with the criminals. "We're in the eye of the hurricane, and we don't know what will happen next," Symantec engineer Martin Lee says.