The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Servers for 3rd-Largest Botnet Shut Down

By The Moscow Times

July 19, 2012

Servers in Russian and Ukraine, the final levers of the world's third-largest botnet responsible for 18 percent of all spam e-mail, have been shut down, killing the spam network known as Grum.

The six command-and-control servers in Ukraine and one in Russia were responsible for sending instructions to infected zombie computers, meaning that when the current spam template used by the zombie computers expires, they will find no new instructions and will cease sending spam, Atif Mushtaq, a senior staff scientist at internet security firm FireEye, said in a blog post.

"Grum's takedown resulted from the efforts of many individuals," wrote Mushtaq, who was instrumental in stopping the network. "This collaboration is sending a strong message to all spammers: 'Stop sending us spam. We don't need your cheap Viagra or fake Rolex. Do something else, work in a Subway or McDonald's, or sell hotdogs, but don't send us spam.'"

The first blow was dealt earlier this week when Dutch authorities took down two major servers in the Netherlands, leaving major servers in Panama and Russia.

After the Internet service provider for the Panama server shut it down, Mushtaq said he worked with several partners overnight to shut down the remaining server in Russia and six more that came online in Ukraine, finally succeeding after the servers' ISP Gazinvestproekt agreed to pull the plug at his request.

The 100,000-computer-strong spam network generated an estimated 18 billion unwanted messages per day, according to Mushtaq's blog.

Russia and Ukraine have long been seen as safe havens for illegal botnet activities, so the takedown of the servers was seen as a large success by the internet security community, technology site Arstechnica said.

Original url:
https://www.themoscowtimes.com/2012/07/19/servers-for-3rd-largest-botnet-shut-down-a16387