

1 December 2008

By: Lucian Constantin, Web News Editor



Security researchers kept the Srizbi botnet under control
FireEye, Inc.

[Major Botnet Resurrection Partially Prevented](#)

Researchers have been fighting to keep the Srizbi botnet offline

Following the [recent takedown](#) of the notorious McColo ISP, the control servers of several major botnets have been knocked offline, rendering the armies of zombie PCs out of the reach of their owners. Researchers from the FireEye Malware Intelligence Lab have fought and succeeded to keep the largest of these botnets, Srizbi, inactive.

The McColo ISP was known for hosting the control servers of some of the biggest botnets responsible for the vast majority of the world's spam e-mails. These included Srizbi, Rustock, Pushdo, Mega-D, and others. After the shady hosting company had been depeered by their uplink providers, the spam levels worldwide plunged and kept to a low level. Security researchers remained skeptical, warning that it was very likely for the junk mail levels to go up again, if the botnet herders would relocate their infrastructure.

Such fears started to come true when McColo successfully [secured a new uplink](#) for a brief period of a few hours. Even this short time frame was enough for the cybercriminal gang behind Rustock to start pushing updates to the botnet and instruct them to use a control and command server hosted in Russia. Fortunately, due to limitations in the botnet design, which required every infected machine to connect to the control server, they did not succeed to update the entire botnet, since many of the compromised computers had not been switched on during the short period of uptime.

However, the Srizbi botnet, considered to be the largest in the world, had more complex backup instructions coded in exactly for such scenarios when the primary control servers went down. These consisted of an [algorithm](#) that generated 4 different random-looking and unique domain names every day, and instructed the infected computer to attempt to connect to them in cycles, until new updates were received.

After breaking the algorithm, the security experts from FireEye made significant efforts to keep ahead of the Srizbi owners and register those domain names every day for themselves, in order to prevent updates being served to the compromised systems. Such a task obviously required monetary resources, and the researchers eventually decided that they could not support the investment indefinitely and [stopped](#). As soon as that happened, the bot herders registered the new domain names, which they hosted on servers in Estonia, and started issuing updates.

The cybercriminals decided to test if the botnet was still functioning correctly, so their first move was to push a Russian-language spam template, which was obviously aimed at a limited number of users. Fortunately, before having a chance to install an English-language template, the servers were taken offline through a coordinated effort between FireEye and Estonian parties, which have yet to be named. The researchers note that a single control server located in Frankfurt is still active, so the threat has not been completely averted yet, but it has been temporarily contained.