Researchers Kneecap 'Pushdo' Spam Botnet

Published: 2010-08-27 · Archived: 2026-04-05 20:36:08 UTC

Security researchers have dealt a mighty blow to a spam botnet known as **Pushdo**, a massive grouping of hacked PCs that until recently was responsible for sending more than 10 percent of all junk e-mail worldwide.

According to security firm **M86 Security Labs**, junk e-mail being relayed by Pushdo (a.k.a. Cutwail) tapered off from a torrent to a dribble over the past few days. M86 credits researchers at **LastLine Inc.**, a security firm made up of professors and graduate students from **University of California, Santa Barbara**, the **Vienna University of Technology** (Austria), **Eurecom** (France), and **Ruhr-University Bochum** (Germany).

LastLine's **Thorsten Holz** said his group identified 30 Internet servers used to control the Pushdo/Cutwail infrastructure, located at eight different hosting providers around the globe. Holz said Lastline contacted all hosting providers and worked with them to take down the machines, which lead to the takedown of nearly 20 of those control servers.

"Unfortunately, not all providers were responsive and thus several command & control servers are still online at this point," Holz wrote on the company's blog. "Nevertheless, this effort had an impact on Pushdo/Cutwail, which you can also see in new Anubis reports generated today by re-running the analysis: Many connection attempts fail and infected machines can not receive commands anymore."

It will be interesting to see whether this action has a lasting effect on the Pushdo/Cutwail botnet, which has rebounded from similar infrastructure attacks in the past. In January 2010, researchers at Neustar and several ISPs targeted the control servers for the Lethic botnet, another botnet that at the time was estimated to be responsible for relaying roughly one in ten spam e-mails. But just a month after that takedown, spam volumes from Lethic began recovering.

In May 2009, the Federal Trade Commission ordered the unplugging of a hosting provider in Northern California called **3FN**, which was at the time hosting a large number of Cutwail control servers. The 3FN takedown — a type of botnet assault that I like to call a "shun" — relies on ostracizing or immobilizing ISPs and hosting providers that repeatedly turn a blind eye to serious abuse on their networks.

This latest action by Lastline falls into the other major takedown category, a group of tactics best described as "stuns," wherein researchers target a botnet's control infrastructure in a coordinated takedown. I discuss both of these tactics in the latest *McAfee Security Journal*, available at this link.
