By Zeljka Zorz, Net-Security.org

Every day, approximately 89.5 billion unsolicited messages (i.e. spam) are sent by computers that have been compromised and are part of a botnet.

Botnets - apart from inundating out inboxes with spam - can also be used for ulterior purposes such as executing DDoS attacks or hosting websites, so understanding the ˝modus operandi˝ and size behind the well-known names is a good idea.

Message Labs` list of top 10 botnets in 2009 reads like this:

Rustock

Rustock frequently sends spam at full capacity for short periods, and then ceases its activity often for days at a time. Between August and September 2009, it controlled between 1.3 million to 2 million bots.

Rustock had accounted for approximately 10-20% of all spam for much of the year, but by the end of 2009 it had increased its dominance and stabilized its output to approximately 18% of all spam. By the end of 2009, Rustock was mostly sending pharmaceutical and medical spam.

Cutwail

Cutwail consisted of 1 million to 1.5 million bots throughout the year, and was responsible for 17% of all spam.

It was responsible for the surge in Bredolab malware, spoofed greetings card emails containing malicious hyperlinks, phishing activities, pharmaceutical spam and spam peddling counterfeit watches.

Bagle

Bagle has finished the year with somewhere in between 600,000 and 800,000 bots under its belt. By the end of 2009, Bagle was responsible for approximately 16% of global spam, and the spam in question was almost exclusively pharmaceutical or medical.

Bobax (aka Kraken)

Bobax has an estimated 80,000 to 120,000 bots at its disposal, and throughout the year it increased the rate at which each bot was sending spam. Finishing the year by positioning itself in the 4th place by being responsible for 13% of spam, Bobax returned to its pre-McColo spam levels. The spam it sends out is mostly related to counterfeit fashion accessories and watches.

Grum

Grum was busiest between June and September, when it was sending more spam than any other botnet (20% of all spam). The number of bots it controls ranges from 600,000 to 800,000, and they are charged with sending out mostly pharmaceutical spam.

Maazben
A newcomer among botnets, Maazben made it`s first appearance in March. By the end of 2009, it controlled 200,000-300,000 bots. Responsible for 2% of all spam, it cornered the market on French and German language casino related and gambling spam.

Festi
Another newcomer, Festi emerged in August 2009 - by the end of the year, it controlled approximately 100,000-200,000 bots which send out counterfeit watch and fake fashion accessories spam.

Mega-D
At the beginning of 2009, Mega-D was the main spamming botnet and emerged after the McColo closure as the most active botnet, comprising of an estimated 300,000-500,000 bots. However, as the year progressed, Mega-D seemed to be seriously hemorrhaging bots, its estimated size plummeted to less than 100,000 bots.

In January, it was responsible for 58.3% of all spam, but it was almost eradicated on 4 November as the result of community action to disrupt the botnet, and it`s output fell drastically. It returned on 13 November using a different collection of bots, sending between 4-5% of spam, mostly pharmaceutical and some phishing activity.

Xarvester
Believed to be designed and operated by the owners of the defunct Srizbi botnet, Xarvester was closely watched and there was a lot of activity aimed at suppressing its operation.

In January it controlled 500,000-800,000 bots, but by the end of the year it had only 20,000-36,000 bots - less than 1% percent of all spam was sent by them (mostly pharmaceutical and medical).

Gheg
Gheg was at its peak in January, when it controlled 150,000 to 200,000 bots following the closure of McColo. At the end of 2009 it had less than 100,000 bots and was linked to approximately 0.5% of all spam - mostly Russian language dating spam, and medical spam in French, German and English.

Donbot
Somewhat of a ˝riches-to-rags˝ turn of events happened to Donbot. It appeared in the wake of the McColo closure and had a boom during the first quarter of 2009 - it controlled an estimated 800,000 to 1.2 million bots.

But, by the end of the year the number of bots fell to 100,000-150,000, so it effectively failed to enter the top 10 list - think of this as a honorable mention due to its huge impact it had at the beginning of the year.

Its spam contained links to profiles on social networking and micro-blogging websites, related to “make-money-working-at-home” type spam messages.