

# The 10 most feared 'ghost computer' networks in the world

Statistics show that these 10 ghost computer networks (botnets) are controlling 5 million computers and distributing 135 billion spam every day - accounting for 80% of the current spam volume.

**Statistics show that these 10 ghost computer networks (botnets) are controlling 5 million computers and distributing 135 billion spam every day - accounting for 80% of the current spam volume.**

## Grum (Tedroo)



Grum is the future for spammy botnets. They work stealthily under the hidden mode of rootkits, infecting the AutoRun registry key to ensure that it is always activated. This botnet is currently receiving special attention from researchers. The number of Grum's distribution programs is currently 600,000 but it accounts for 25% of spam in a day, which spreads to 40 billion spams a day.

## Bobax (Kraken / Oderoor / Hacktool.spammer)

Bobax is a new botnet identified with respect to the previous Kraken famous botnet. Recently, Kraken was upgraded to Bobax by switching commands and controlling traffic to the HTTP protocol to make it difficult for users.

According to current statistics, Bobax's distribution program only accounts for 100,000 but it spreads to 27 billion spams a day, accounting for 15% of spam. Thus, it means that every minute it can generate 1400 spam.

## **Pushdo (Cutwail / PANDEX)**

The Botnet is a network of malicious computers infected by hackers who have control, and the victim is unaware.

Hackers will take advantage of exploiting "zombie computers" in their botnets to serve spam, infect malicious code . to profit. Started with the name Storm in 2007, Pushdo has so far grown quite strong and has generated about 19 billion spams a day and owns 500,000 "ghost computers" (controlled due to malicious code). .

Pushdo is a form of downloader malicious code that takes access to victim computers and downloads Cutwail spam software.

This botnet involves spam spills about pharmaceuticals, online casinos and includes phishing activities as well as links to sites containing malware.

## **Rustock (Costrat)**

Rustock was known in 2008 but was quickly eliminated when McColo's "spam-dispenser" was completely destroyed. After a period of quiet silence has returned and became one of the largest botnets with nearly 2 million "ghost computers" as tools for the purpose of attack.

Rustock is also known as spam that uses image files to bypass protection filters. Rustock regularly opens a series of spam litter advertising medical drugs or sends spam messages to Twitter's social network with spam amounting to about 17 billion per day.

## **Bagle (Beagle / Mitglieder / Lodeight)**

The botnet Bagle was born in 2004, but until two years ago, Bagle creators began to bring Bagle botnets to profitability. Currently Bagle has 500,000 "ghost computers" with the number of spam messages posted every day on the Internet at 14 billion.

## **Mega-D (Ozdok)**

In November 2009, researchers at FireEye broke the botnet with command lines as well as controlling domains before botnet owners. But then Mega-D was restructured to be able to continuously create new domain names to help its owners control their activities.

Among the top 10 botnets, Mega-D is the smallest botnet with only 50,000 members. Although the number of "slaves" is small, Mega-D can spread up to 11 billion spams a day. If you consider spam every minute, Mega-D is just behind Bobax.

## **Maazben**

Maazben was discovered and prevented from June 2009. Although Maazben has a number of "ghost computers" of 300,000, compared to other botnets, it provides a low amount of spam messages every day, reaching only 500 million messages.

## **Xarvester (Rlsloup / Pixoliz)**

Xarvester has been formed since McColo was terminated. Researchers discovered that Xarvester has similarities with the infamous botiz Srizbi.

The current statistics of Xarvester contain 60,000 "members" with spam spread throughout the Internet of about 2.5 billion per day.

### **Donbot (Buzus)**

This is one of the first botnets to use the service to shorten URL addresses, one of the best ways for them to hide malicious links in spam to trick users into clicking that malicious link. Donbot has about 100,000 "members" with a daily spam volume of around 800 million.

### **Gheg (Tofsee / Mondera)**

Three highlights of the 10th botnet are: 85% of spam from South Korea, Gheg is one of the few botnets that encrypts bandwidth traffic by commands and controls servers by connecting. not SSL compliant. The third thing is how Gheg chooses proxies to send spam or it can even send spam to the victim's computer via the Internet provider email server.

Gheg currently has 60,000 "ghost computers" with about 400 million spams scattered every day.

You finished reading the article "**The 10 most feared 'ghost computer' networks in the world**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.