



Article published on December 7th 2011 | [Computer](#)

Large botnets nowadays are in the hot seat due to the fact that law enforcement as well as security agencies are tracking and eliminating them one by one. In fact some of the major botnet operations have been ended and their operators are now behind bars. Because of the increase of crackdowns against them, some vile minds are directing their skills to different avenues. These avenues are multiplying in an alarming rate even with the increase of crackdowns against them and the reason is simple “because they are smaller and much harder to trace botnets. These kinds of botnets are cheaper and far easier to build and manage, and criminals know that large scale botnets will surely attract unwarranted attention.

Nowadays botnets have become more commoditized, sophisticated and automated; in fact, botnets are powerful weapons that can greatly affect our society, even if it is in the hands of a criminal with little computer expertise. And smaller botnets can steer clear of the law enforcement as security agencies radar, thus they have become numerous. The development of botnet technology is parallel to the technology in the Internet industry. The staggering truth is that latest versions of botnet kits can be purchased for just a couple of thousand bucks and it could lead into millions of illegal profit. Sometimes, there are free versions of such tools, which lead to some major concerns of experts and computer forensics in the security industry.

Botnet industry is one of the most sophisticated, yet scalable business in the black market. Some clients can employ the service of a botnet merchant for a certain 1 hour DDoS attack for a few dollars only. In fact, botnet rental comes with service agreements as well customized controls for their clients “making it appear as legitimate as regular business transactions.

Even if the security system of an industry is protected from becoming host to a botnet, it doesn't mean that it is safe from botnet attacks like DDoS. As the number of controlled botnets increase, the bandwidth needed to control them also increases. This year the largest ever recorded DDoS attack was 49 Gbps. That number alone could take out a lot of working sites and could possibly lead to serious damages.

The threats of botnets are always present wherever you may be in the globe, so what should your business do against them. Smaller businesses should first find a safer refuge for their important data; relocate them to extremely capable and highly maintained cloud applications providers “providers that offer safety and defense against DDoS attacks. It would be less expensive than maintaining it on your own. Larger companies must first assess the abilities and features of their chosen data or webhosting providers so that the important services are not ignored and become an open vulnerability against attacks. Of course all of these industries, whether small or large must have the assistance of security experts as well as individuals who have received computer forensics training.

Botnets are an all around tools and once a computer system has been infected with a bot, hackers can use it as a leverage to send spam, execute DDoS attacks and even host illegal contents. They can be used in some covert illegal activities like recording the keystrokes of a victim, steal the banking information of an individual. One of the most common botnet software is the Zeus and it is a creation as well as control software that is used to steal passwords as well as other credible information.

Somehow, almost half of bot variants made the same way as Zeus can be detected by regular antivirus programs. Years ago the Conficker botnet can be compared to a dangerous volcano, waiting to erupt any moment, but somehow it has been mitigated and stopped. So this implies that, botnets can still be eliminated, whether it is large or small and it all relies on the education and knowledge of individuals who are willing to work together to be able to eliminate the infection and also improve the cyber security of a network.

However, criminals do not need large botnets just to direct an attack to a particular enterprise; smaller botnets can deliver the job. Even cyber security experts and individuals who have completed computer forensic course always say that industries must treat small botnets the same as the large botnets.

Article Source:

<http://www.articleside.com/computer-articles/incoming-waves-of-small-botnets.htm> - [Article Side](#)

[Eccuni](#) - About Author:

The International Council of E-Commerce Consultants (EC-Council) is a member-based organization that certifies individuals in cybersecurity and e-commerce. It is the owner and developer of 20 security certifications. EC-Council has trained over 90,000 security professionals and certified more than 40,000 members. These certifications are recognized worldwide and have received endorsements from various government agencies. They also offer trainings in computer forensics.

More information about EC-Council is available at www.eccouncil.org, a [computer forensics](#), a [computer forensics training](#), a [computer forensic course](#)

Article Keywords:

Botnets, computer forensics, computer forensics training, computer forensic course, cyber security experts, law enforcement, Large botnets, security agencies, security industry, Botnet industry, black market, DDoS, webhosting providers, Zeus, antivirus pr

You can find more [free articles](#) on [Article Side](#). Sign up today and share your knowledge to the community! It is completely FREE!