

Fighting the Botnet Menace

While Internet users are generally acquainted with words like virus, spam, Trojans, etc., — the widely known forms of Internet Threats, the word botnet is still a vague term for many. However, as Internet becomes a way of life with rising usage, it is important for users to take that first step towards addressing the rising menace of botnets by being aware of what they are and the precautionary measures to be taken against them. Botnet has emerged as the biggest attack platform and its pervasiveness provides it with a capacity to steal data with impunity and bring down huge networks.

What are Botnets?

The word **bot** used for a compromised computer is actually an abbreviation of the word Robot and a network of such computers, the numbers of which may run into millions, is called botnet. Botnets, thus are networks of compromised computers that can be remotely controlled by an attacker and are the commonest attack platforms today.

These bots are created through malicious software programs, installed on unsuspecting computers of individuals and businesses. The malicious programs, also commonly known as rootkits, control these computers and are installed using other carrier software programs, such as viruses worms, Trojans and spams. Rootkits often modify parts of the operating system while installing themselves as drivers. The software is then controlled by a single command center called a "bot herder." This individual or individuals originate the bots and control them remotely.

The purpose of botnets is to provide a launching pad for either spam attacks or virus outbreaks. Apart from this, the information stored in the computer is also compromised by the botnet while concealing the true identity of the attacker. While doing so, a large number of users come in the attack ambit given the vastness and automation of the bot network.

The Immensity of Botnet Threats

Common industry knowledge estimates that more than 6 million infected computers worldwide are connected to a botnet and most owners of infected computers do not even know that their machines have been compromised. According to recent findings by an IT security company, top botnets are capable of sending more than 100 billion spam per day. Also, over the years, botnet capability has increased substantially to the point of blurring the lines between traditional categories of malware. In fact, Botnets can be compared to an army engaged in an attack on the network while Internet threats like viruses, worms, Trojans, Spam etc., are mere ammunition fired by the botnet army.

Talking about botnets, so far the Storm worm is widely known as the world's most, dangerous botnet. However, security experts say there's an up-and-comer called Nugache that could far exceed its capabilities in causing security breaches. Nugache was first sighted about two years ago as a worm designed to work with chat protocols. Hackers allegedly belonging to the notorious Russian Business Network online criminal mob, gave **Nugache** a facelift, copying many of the successful attributes of Storm, such as encryption, a rootkit and the ability to spread as web-borne malware. Nugache is now also peer-to-peer controlled. This puts it under a more decentralized command-and-control structure that makes it difficult to take down the botnet it can construct once it infects desktop machines. Business and consumers need to be aware that Nugache could attempt to compromise their desktop machines in various ways, particularly through Web-based drive-by downloads. One way it has been seen spreading is through URLs embedded by attackers in blogs.

Financial Gain: Cause of Botnet Proliferation

In the past, the rise of botnets was attributed to show off value in demonstrating the programming prowess that gave the programmers their ticket to fame. But today, a whole industry of criminal gangs operates around the

globe for financial gains through the use of botnets. It is a full-fledged industry out there. Financial gain is the motivation behind the origin of botnets. This also gives them enough financial muscle to develop new capabilities in the task of botnet code making in an organized and professional manner using highly skilled human resources. This makes the task of securing networks against this threat much more difficult.

Methods Used by Botnets to Steal Information, Cause Damage

- **DDOS** - Often botnets are used for Distributed Denial-of-Service – DDOS - attacks. A DDoS attack is an attack on a computer system or network that causes a loss of service to users. Typically, it is due to the loss of network connectivity and services by consuming the bandwidth of the victim network or overloading the computational resources of the victim system.
- **Spamming** - Bots often are used for activities like spamming. With the help of a botnet and thousands of bots, an attacker is able to send massive amounts of bulk email, that is spam. Some bots also implement a special function to harvest email-addresses.
- **Phishing** - In addition, bots can be used to send phishing mails. Since phishing with the use of social engineering tricks can be used to deceive users into divulging sensitive personal information such as usernames, passwords, account IDs, ATM PINs, credit card details and social security numbers, botnets with their extensive network cause immense damage to users through misuse of their information asset.
- **Sniffing Traffic** - Bots can also use a packet sniffer used to retrieve sensitive information like usernames and passwords. But the sniffed data can also contain other interesting information. If a machine is compromised more than once and is also a member of more than one botnet, the packet sniffing allows gathering the key information of the other botnet. Thus it is possible to "steal" another botnet.
- **Keylogging** - Most bots with the help of a keylogger, very easily retrieve sensitive information. For example, if one is using the Internet for financial transactions, it can steal the password and account number used online. And to think that this keylogger runs on thousands of compromised machines in parallel! One can imagine how quickly such accounts can be harvested.
- **Conduits to new Malware** - In most cases, botnets are used to spread new bots. This is very easy since all bots implement mechanisms to download and execute a file via HTTP or FTP. In fact, it is very easy to spread an email virus using a botnet. A botnet with 10,000 hosts, which acts as the start base for the mail virus allows very fast spreading and thus causes more harm.
- **Mass Identity Theft** - Fake emails ("phishing mails") that pretend to be legitimate (such as fake payment gateway or banking emails) ask their targeted users to go online and submit their private information. These fake emails are generated and sent by bots via their spamming mechanism. These same bots can also host multiple fake websites pretending to be genuine banking or financial websites, and harvest personal information. Just as quickly as one of these fake sites is shut down, another one can pop up.

Why User Education/Awareness is Important

The rise of botnets is directly proportionate to the users becoming both victims and participants due to a poor understanding of network and computer security and lack of awareness and education campaigns. User education and precautionary measures is the key to comprehensive security as the user is the final layer in defending the network. According to industry sources, findings suggest that SMTP email, is responsible for the propagation of almost 75% of all malware, which means people are still clicking on software they get in emails and the spammers are well aware of this.

Findings in corporate settings, which use comprehensive security solutions, point out that organizations that train users performed significantly better than those relying mainly on technical controls

User Education: Integral to Cyberoam Solution

Cyberoam has been providing security to corporations across the world and is one of the leading vendors in the security industry. A Botnet is a blended threat, which Cyberoam tackles at multiple levels through web content filtering and gateway anti-virus checks and scanning of web mail traffic. Similarly, its gateway anti-spyware

scans web and mail traffic while gateway anti-spam scans mail traffic for spam and malware laced mails. This is combined with the functionality of virus outbreak detection against mail-based zero-day outbreaks.

Apart from this, educating users and defining the user threat quotient based on a user's surfing practices are two equally important parameters that Cyberoam engages in providing protection to the network. For example, each time a site is blocked, Cyberoam displays a customized message, stating the reason for blocking the site, eg., "the site is a known phishing URL that directs the user to malicious replica website". Cyberoam thus believes that user education goes a long way in providing security.

Precautions and Measures to Home Users against Botnets

- **Update:** Update your computer's operating system and Internet applications as this will close many of the vulnerabilities used by botnets to infect a computer. Modern up-to-date virus scanners will come handy in detecting botnet agents running on the computer.
- **Use caution against attachments:** Desist from opening attachments or web links in e-mail or instant messages, even if the sender's name is familiar unless you are expecting it or know what it contains.
- **Be alert if connection is unusually slow:** Botnets generate a lot of traffic slowing down the network and Internet connection. Investigate the computer if a large amount of network activity is noticed at an unnatural time. If the Internet connection appears slow, but a lot of data is being transferred, the computer is probably being used in an attack.
- **Enable Firewalls:** Firewalls are effective in controlling access to the botnet control servers, but require some effort to configure correctly. It's especially important to run a firewall if you have a broadband connection. Most common operating system software comes with a built-in firewall, but you may have to enable it.
- **Disconnect from the Internet when not using it:** Leaving your Internet connection on and unprotected is just like leaving your front door wide open. Hackers just can't get into your computer when it's disconnected from the Internet
- **Inspect your "sent items" file or "outgoing" mailbox:** If you find unknown messages in your out box, it's a sign that your computer may be infected with spyware, and may be part of a botnet.



Toll Free Numbers

USA : +1-877-777-0368

India : +1-800-301-00013

APAC/MEA : +1-877-777-0368

Europe : +44-808-120-3958

Copyright © 1999 - 2008 Elitcore Technologies Ltd. All rights reserved.
Cyberoam and Cyberman logo are registered trademarks of Elitcore Technologies Ltd. Although Elitcore has attempted to provide accurate information, Elitcore assumes no responsibility for accuracy or completeness of information neither is this a legally binding representation. Elitcore has the right to change, modify, amend or otherwise revise the publication without notice. PL-30-00453-000001

