Prashant S. Gosavi, Amit A. Dange, Dr. B. B. Meshram / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 3, Issue 2, March -April 2013, pp.1695-1701

Critical Infrastructure and Botnet

***Prashant S. Gosavi, **Amit A. Dange, **Dr. B. B. Meshram**
*M. Tech CE VJTI, Mumbai
**M. Tech CE VJTI, Mumbai
***H.O.D, Dept. of CE VJTI, Mumbai

Abstract

Critical infrastructures are those services which serve as the life line of nation. As the technology develops these services are becoming more and more interdependent and depends on information flow in between them and thus become a potential target for cyber attacks. At the center of most of the cyber attacks are collection of compromised host, or botnets. Botnets is group of compromised computers controlled remotely by attackers for various network attacks such DDoS etc. This paper review what critical infrastructure is, their interdependency and the threat that botnet posses to them. This paper also reviews the botnet life cycle, communication topologies and ways to detect and countermeasure the botnet.

Keywords — Critical Infrastructure, Botnet, Botnet Detection

I. INTRODUCTION

"*Leveraging the power of several thousand bots, it is viable to take down almost any website or network instantly. Even in unskilled hands, it should be obvious that botnets are a loaded and powerful weapon.*"[1]

Quotes like above in the articles and research papers have raised the profile of bots and botnets which have infected thousands of computers across the world.

And the incident like DDoS attack on numerous Estonian websites, which is basically flooding attacks by botnets, and the detection of Stuxnet worm in July 2010 [2], which attempts to take control of critical physical infrastructure and connects to command and control server for updates, has shown the abilities of the botnets to bear against any potential targets.

The financial systems operating 24/7 linking intermediaries globally, power plants and electrical grids, gas and oil distribution pipelines, water treatment systems, oil and chemical refineries, transportation systems, and even essential military communications all rely on an interdependent network of information systems that connect and increasingly control the operations of other critical infrastructures, they have become the potential targets for botnets.

Therefore in this paper, we seek to assess the threat that botnets pose to the critical national infrastructure. The paper is arranged as follows: Section II will describe the critical national infrastructure and its importance, Section III reviews botnet life cycle, topologies, types, type of targets and attacks and C&C channel. Section IV describes the recent trends botnet detection technique. Section V concludes the paper.

II. CRITICAL NATIONAL INFRASTRUCTURE

A. What is CNI?

The word infrastructure which is defined as "organizational structures or basic foundations and framework", gets new meaning in the report of PCCIP to the US President in October 1997 which define infrastructure as:

"a network of independent, mostly privately-owned, man-made systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services." [3]

In this report, the Commission narrowly focused on eight critical infrastructures "whose incapacity or destruction would have a debilitating impact on our defense and economic security". These eight are telecommunications, electric power systems, natural gas and oil, banking and finance, transportation, water supply systems, government services, and emergency services. The definition is later broadened by the Critical Infrastructure Assurance Office (CIAO) as:

"the framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of governments at all levels, and society as a whole."[3]

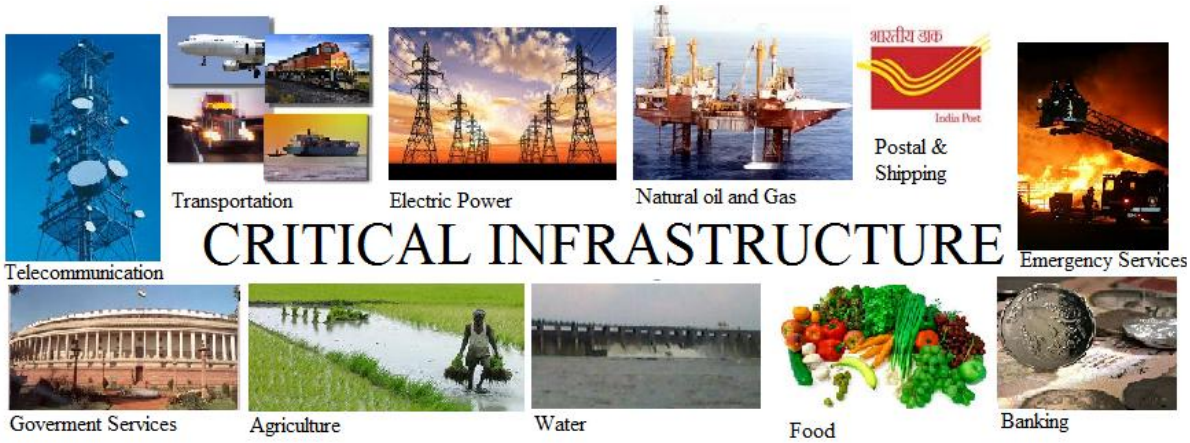

Figure 1: Critical National Infrastructure

In addition to the above eight critical infrastructure there are some more areas which can be considered as critical such as food, health etc. this critical infrastructure are shown in figure 1.

B. Interdependency

All this infrastructures are interdependent in one or more way. Basically these infrastructures are considered to be geographic, physical, logical and cyber interdependent [3]. An infrastructure has cyber interdependency if its state depends on information transmitted through the information infrastructure.

The cyber interdependency is the result of pervasive computerization and automation of infrastructures over the last several decades. This interdependency has increased the risks due to the complexity of the integrated infrastructures. Disruption in one part of the infrastructure spread out through the system and has effects on other sectors. Figure 2 shows the high level interdependency among several sectors.

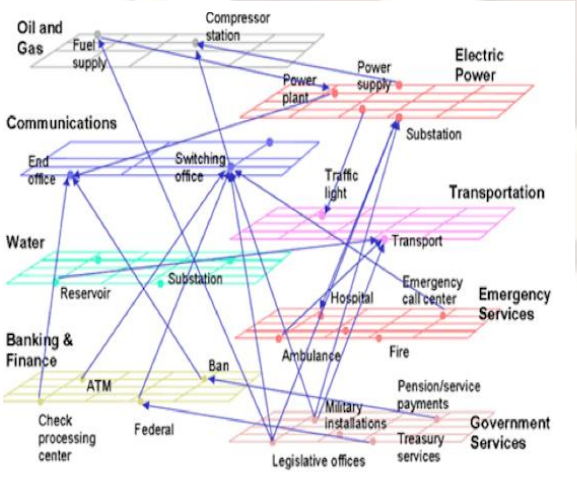

Figure 2: Critical Infrastructure Interdependency [4]

one critical infrastructure can easily propagate across all other dependent infrastructures. For example, loss of service from the electric power infrastructure would directly affect the oil infrastructure. The oil infrastructure relies heavily on the electric power infrastructure for power, in order to run pumping stations, control systems and for storage. If this function was not available the result would be disastrous. The oil infrastructure, as a result, could not produce fuels and lubricants which are required by the transportation infrastructure, natural gas, telecommunications, water and the electric power infrastructure. This is an illustration of the impact infrastructure failure could have on the other dependent infrastructures.

Section III BOTNET

A *botnet* is the melding of many threats into one. The typical botnet consists of a bot server and one or more bot clients. Botnets with hundreds or a few thousands of bot clients (called zombies or drones) are considered small botnets. In this typical botnet, the botherder communicates with bot clients using an IRC channel on a remote command and control (C&C) server. In step 1, the new bot client joins a pre designated IRC channel on an IRC server and listens for commands. In step 2, the botherder sends a message to the IRC server for each client to retrieve. In step 3, the clients retrieve the commands via the IRC channel and perform the commands. In step 4, the bot clients perform the commands. In step 5, the bot client reports the results of executing the command.

A. Command and Control Server

The most important part of a botnet is the so-called command-and-control infrastructure (C&C). This infrastructure consists of the bots and a control entity that can be either centralized or distributed (defined later in the paper). The control entity or Bot-Master communicates to bots through C&C channel, which sends commands to bots and stolen information to the Bot-Master. The C&C infrastructure typically serves as the only way to control bots within this infrastructure in order to

operate efficiently. Therefore, the architecture of the C&C infrastructure determines robustness, stability and reaction time.

B. Life Cycle of Botnet

A typical botnet can be created and maintained in five phases including: initial infection, secondary injection, connection, malicious command and control, update and maintenance [5].

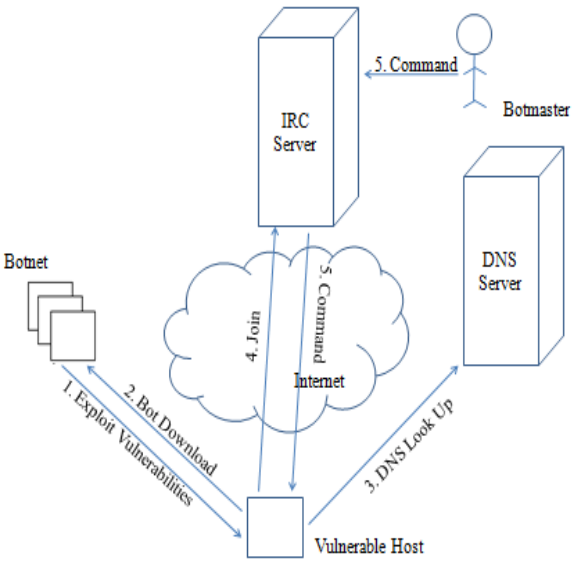

Figure 3: Botnet Life Cycle

During the initial phase, the attacker, scans a target machine for known vulnerabilities, and infect victim machines through different exploitation methods. After initial infection, in secondary injection phase, the infected hosts execute a script known as shell-code. The shell code fetches the image of the actual bot binary form the specific location via FTP, HTTP or P2P. Once the bot program is installed the victim computers turns to a Zombie. In connection phase, the bot program establishes the connection with C&C server. Upon establishment of C&C channel, the zombie becomes part of attacker's botnet army. Now actual botnet activity is started i.e. malicious command and control phase. Bot programs receive and execute commands sent by Bot-Master. The C&C channel enables the botmasters to remotely control the action of large number of bots to conduct various illicit activities. In Update and Maintenance phase, bots are commanded to be lively and updated. So any new Solution to find and control is detected than control center can update it with new strategies or may add new functionalities. Sometimes the updated binary move the bots to a different C&C server. This process is called server migration and it is very useful for botmasters to keep their botnet alive.

C. Botnet Topologies

The botnet topologies can be categorized into two types depending on the C&C channel: Centralized and Decentralized model.

1. Centralized C&C Architecture: In a centralized C&C infrastructure, all bots establish their communication channel with one, or a few single connection points as illustrated in the figure 4. These are usually command-and-control servers, under the control of the botmasters. Because all bots connect to these servers, botmasters are able to communicate with the bots simultaneously and can issue commands to all the bots that are both online and connected to the botnet. This offers low reaction times and a good means of coordination. Direct feedback enables easy monitoring of the botnet status for the botmasters and gives information about fundamental properties, such as the number of active bots or their global distribution.

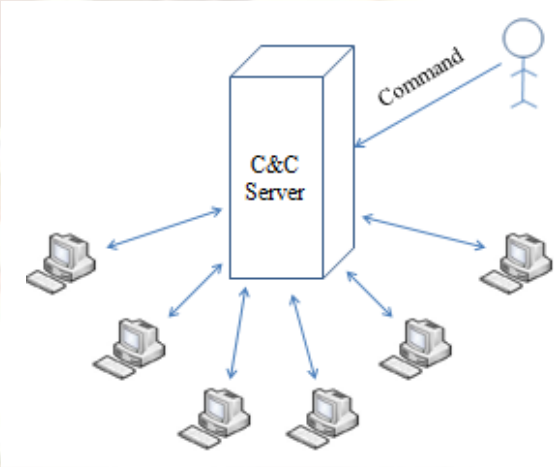

Figure 4: Centralized Architecture

a) Bots based on IRC: The IRC protocol serves as important technology for botnet control and enables a centralized communication model. One important property of this protocol is that the number of potential participants within one channel is technically not limited. This allows the collection of many bots in one such channel and the ability to command them in parallel. Additional one-to-one communication is possible between bot and the botmaster. Because the IRC protocol is text-based, it is easy to implement and customize. In the context of botnets, these properties offer a robust, well-established and easy-to-implement approach to commanding a botnet. Some famous IRC based botnet are Agobot, SDBot, Spybot, and GTBot [6].

b) Bots based on HTTP: A well-known standard used throughout the internet is the Hypertext Transfer Protocol (HTTP). HTTP is the protocol most commonly used for the delivery of data over the internet. Because of these important features, HTTP is available in nearly every network connected to the internet and is rarely filtered. This

is especially interesting for botnet operators, because it makes the protocol viable as a command-and-control protocol. Some HTTP based botnet are Bobax, ClickBot, Rustock and Blackenergy aswll.

2. Decentralized C&C Architecture: In decentralized command-and-control architectures, loosely coupled links between the bots enable communication within the botnet and provide the basis for its organization. A common term for this class of botnets is peer-to-peer botnets, as this is the name of the corresponding network model. The knowledge about participating peers is distributed throughout the botnet itself. Consequently information about the whole botnet cannot be obtained directly, and commands have to be injected into one peer of the botnet. Usually, this is either realized over the communication protocol directly or via the update functionality. In the latter case, bots will exchange their revision number upon communication and, if these vary, the older bot is updated to the version of the new bot. The insertion of such updates and commands into the botnet usually happen from an arbitrary point, making localization of the botmaster almost impossible. This provides a high degree of anonymity. Figure 5 shows the simple design of peer-to-peer botnet as an example of decentralized C&C approach. SpamThru [6] botnet is one of the example botnet using peer-

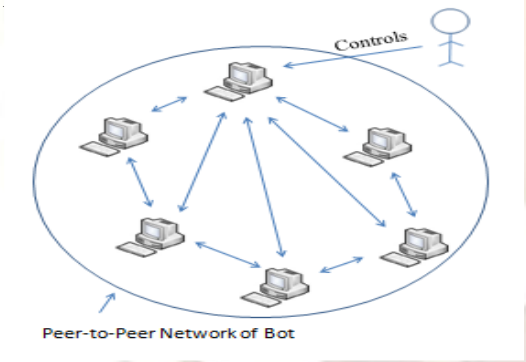

Figure 5: Decentralized Architecture

D. Threats of Botnet

Botnet possess different threats some of which are listed below:

1. Distributed Denial-of-Service Attacks: Often botnets are used for DDoS attacks. A DDoS attack is an attack on a computer system or network that causes a loss of service to users, typically the loss of network connectivity and services by consuming the bandwidth of the victim network or overloading the computational resources of the victim system. One example of such attack is DDoS attack on several websites of Estonia.

2. Spamming: With the help of a botnet and thousands of bots, an attacker is able to send massive amounts of bulk email (spam). Some bots also implement a special function to harvest email-addresses. In addition, this can of course also be used to send phishing-mails since phishing is a special case of spam.

3. Sniffing Traffic: Bots can also use a packet sniffer to watch for interesting clear-text data passing by a compromised machine. The sniffers are mostly used to retrieve sensitive information like usernames and passwords.

4. Key logger: Key logger can be used to steal the sensitive information. And if the filtering mechanism (such as information related to particular keyword like BillDesk) is used it can help in stealing sensitive data. And if it is used in parallel in several machines you can think how quickly these accounts will harvest.

5. Spreading new malware: Botnets can be used to spread the malware as most of the botnets have the capability to download the file using HTTP or FTP.

6. Click Fraud and Pay-Per-Install: Another way of using Botnet is through what is called as click fraud. First, the attacker sets up an account with an online advertiser, who pays for page visits or for additional advertising links by, for example, clicking on a banner. Second, the attacker uses the controlled bots to visit those pages and to generate clicks on the target banners. In this case, the attacker gains money directly from the advertising company, which in turn does not benefit from the traffic generated.

7. Mass Identity Theft: A major use of botnets, with the intention of gaining financial benefits, is for the automated extraction of user data and credentials from infected hosts. Key targets include passwords for various services. This technique is often called identity theft, because it enables botmasters to impersonate the victim, making further actions, like fraud, possible.

8. Manipulating online polls: With the bots under the control, the botmasters can easily manipulate the online polls. Since the bots have distinct IP address they will be as valuable as a vote cast by the real person.

E. Some Incidents of Botnets affecting Critical Infrastructure

- One of the major concerned incidents is successful DDoS attack in April 2007 in Estonia [2]. For around two weeks, several federal, banking, and news website were targets of concentrated DDoS attacks connected with botnet. These were considered to be the first politically motivated cyber attacks of this size. The DDoS attacks had a significant impact on the Estonian population.
- In 2009 and 2010, two espionage botnets were explored in depth, GhostNet [7] and the Shadow Network. The investigation of GhoshNet have led to the discovery of 1295 infected machines in 103 countries, with around 30% of the infected machines considered as “high-value” because they were situated in

government institutions. These included computers in various embassies, ministries, and commissions. Several network traces captured from these machines showed communications between infected hosts and IP addresses of C&C servers situated in China. Those traces proved the extraction of sensitive information.

- To Another example is the Stuxnet worm [2]. It contains many botnet features. After successful infection, the compromised host verifies internet connectivity and then tries to connect to possible C&C servers in order to send information about the system and ask for an update. Stuxnets features include routines that identify and attack only industrial systems containing a specifically defined configuration. It is therefore the first to target critical infrastructure.

IV BOTNET DETECTION TECHNIQUE

The botnet detection techniques can be categorized into Passive techniques and Active Techniques. The details about these techniques can be found in this section.

A. Passive techniques

Passive Techniques are those where data is collected through observation without tampering with the environment. Therefore, these techniques are transparent and unknown to the botmasters. The different passive techniques are:

1. Packet Inspection

A Popular concept for increasing a networks security is to inspect the network data packets. The basic idea is to match various protocol fields, or the payload of a packet, against pre-defined patterns of abnormal or suspicious content. These patterns are also called detection signatures.

Blinkley and Singh [8], has used an anomaly based approach which gathers data by packet inspection. They developed an algorithm for detecting an IRC based botnet. There approach consists of two components: one for TCP and another for IRC. The TCP approach calculates the work weight for an IP address, which is define as ratio of TCP control packets to overall TCP packets. A value close to 1 is considered abnormal traffic. The second component consist of IRC tracking module that collects statistics about IRC channels on the one hand and the activity of distinct source IP addresses on the other. They correlated the data from both components to identify those IRC channels which were likely to be host-infected machines that appeared suspicious due to a high work weight.

2. DNS-Based Approaches

When a victim is successfully compromised, the bots connects to the C&C server for commands and updates. For this the C&C address has to be specified one way is to specify the fixed IP address and another one is specifying the domain name. Therefore, by identifying the malicious domain name the bot C&C server can be bring down.

H. Choi et al. [9], observed the behavior of bots and patterns for querying to DNS. They observe that bots tends to exhibit coordinated behavior as they called “group activity”. For example, migration of C&C server to new domain name results in simultaneous query for C&C domain name. They make the database for all DNS query and combining the DNS query for same domain names in a particular time interval to identify the malicious domain name.

3. Honeypots

A honeypot [10] is an intentionally vulnerable resource deployed in a network with the aim of soliciting attacks or even compromise by a malicious entity. The main reason for researching and developing honeypots is to discover new information about the practices and strategies used by creators of malware and hackers.

Li et al. [11] employed a combined darknet and honeynet, consisting of 2540 addresses from 10 continuous class C networks, and analyzed the incoming traffic for a year. After filtering the incoming traffic, they observed 43 global scan botnet events carried out by 63851 unique sender addresses. They discovered that 75% of all successful scanning events led to an attack with a malicious payload.

B. Active Techniques

The group of active measurement techniques contains approaches that involve interaction with the information sources being monitored. Although this enables the performance of deeper measurements, their application may leave traces that influence results, or include activities that can be observed by the botherder. This can cause reactions, such as a DDoS attack against the analyst or the introduction of changes to the botnet structure that will complicate measurements, even including migration of the service to evade monitoring.

1. Sink holing

Sink holing is a technical countermeasure to cutoff the control source from the botnet. One of the ways to do this is to change the malicious domain name with the trusted domain name controlled by the investigator as shown in the figure 6.

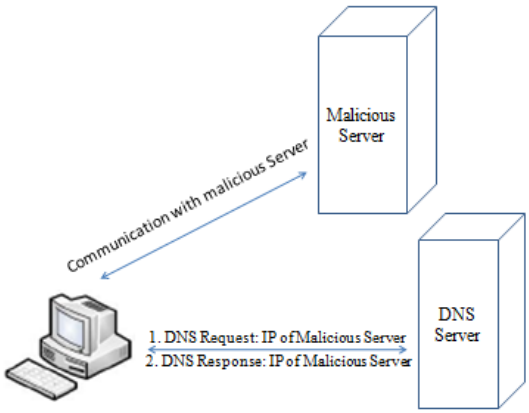

Figure 6(a): Normal Working

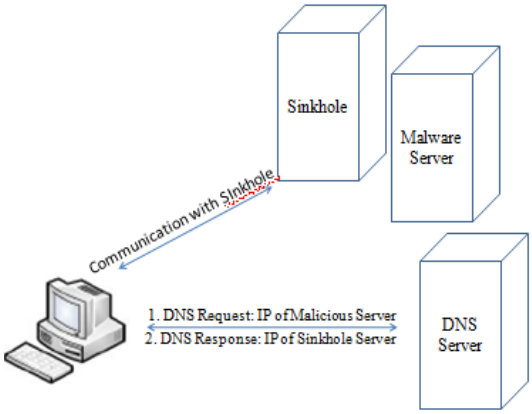

Figure 6(b): Normal Working

This approach is used in Dagaon et al. [12] experiment. When they detected a malicious domain name they contacted the DNS authority and with their help they forwarded the request for malicious domain name to their logging machine (sinkhole). And with this technique, they are able to retrieve 350000 infected hosts.

2. Infiltration

The 'infiltration' of botnets can be divided into software-and hardware-based techniques. Software-based infiltration extends the ideas of the enumeration approaches. Instead of emulating or modifying the bot software on a controlled host with the intention of joining the botnet and measuring it internally, infiltration goes a step further and aims to take control of the botnet.

This usually requires as its starting point the reverse-engineering of the communication mechanisms used by the botnet. Such a precise analysis may lead to the identification of potential weaknesses. This procedure may be compared to a security audit or penetration-test of the botnet and its infrastructure. Knowledge obtained in the process can be exploited in further steps to achieve a commanding position inside the botnet. This may lead to the possibility of performing measurements or revealing information about infected hosts, or even the bothered.

The other approach, hardware-based infiltration, may be applied if an IP address belonging to a command-and-control server has been identified and a relationship to a data processing centre or hosting company can be established. By obtaining a connection to a mirror port on the suspected servers, the communication can be wiretapped and analyzed. This enables all traffic to and from the server to be monitored, which also allows information about number, location and other attributes of infected hosts to be gathered. The limitations of this approach are comparable to sink holing. For example, traffic encryption can reduce the number of usable attributes and therefore influence the accuracy of the measurements.

3. Peer-to-Peer Botnet Enumeration

Even though IRC and HTTP is prevalent technology for botnet control, other schemes have gained in importance. Another common approach used by botnets is to employ a peer-to-peer (P2P) based infrastructure. As explained in Section III Decentralized architecture section, information is not available at a central point in peer-to-peer network; the structure of the network can be exploited for measurement purposes. By repeatedly querying the peer about their neighbor peer list, we can obtain the exhaustive list of peer participating in the network. But before querying the peer for the neighborhood list we must participate in the network which requires reverse engineering of the communication protocol to become part of network.

V CONCLUSION

The power of the Internet, our growing dependence upon it, and the disruptive capability of cyber attackers now threaten national and international security. National critical infrastructures are now at risk not only during war, but also in times of peace.

Cyber security for critical infrastructures is an emerging area that requires extensive new research. This paper reviews botnet which has become a one of the biggest threat of network security and major contributor to unwanted network traffic.

In this paper, techniques used for botnet detection are reviewed. But as time passes new attack techniques are reviled and so we have to be ready for such type of attack and improve detection technique to that extend.

REFERENCES

[1] Paul Bacher, Thorsten Holz, Markus Kotter and Georg Wicherski, "Know your Enemy: Tracking Botnets", www.honeynet.org/papers/bots/

[2] Thomas M. Chen, "Stuxnet, the real start of cyber warfare?" IEEE Network, November/December 2010.
[3] Steven M. Rinaldi, James P. Peerenboom and Terrence K. Kelly, "Critical Infrastructure Interdependencies", IEEE Control Systems Magazine, 2001.
[4] David Korowica, "Financial System Supply Chain Cross contagion", http://www.feasta.org/wp-content/uploads/2012/06/Trade-Off1.pdf
[5] Maryam Feily, Alireza Shahrestani and Sureswaran Ramadass, "A Survey of Botnet and Botnet Detection", International Conference on Emerging Security Information, System and Technologies, IEEE 2009.
[6] Julian B. Grizzard, Vikram Sharma, Chris Nunnery, Brent Kang, David Dagon, "Peer-to-Peer Botnets: Overview and Case Study", HotBots'07 Proceedings of the first conference on Hot Topics in Understanding Botnets.
[7] Tracking GhostNet: Investigating a Cyber Espionage Network Information Warfare Monitor, 2009.
[8] Binkley, J.R., Singh, S., "An algorithm for anomaly-based botnet detection", In Proceedings of the 2nd conference on Steps to Reducing Unwanted Traffic on the Internet, 2006.
[9] Choi, H., Lee H., Kim H., "Botnet Detection by Monitoring Group Activities in DNS Traffic", In Proceeding of the 7th IEEE International Conference on Computer and Information Technology, 2007.
[10] Lance Spitzner, "Honeypots: Definitions and Value of Honeypots", www.tracking-hackers.com/papers/**honeypots**.html
[11] Zhichun Li, Anup Goyal, and Yan Chen, "Honeynet-based Botnet Scan Traffic Analysis", "Botnet Detection: Countering the Largest Security Threat," Springer 2007.
[12] Dagon, D., Zhou, C., Lee, W. "Modelling botnet propagatioin using time zones", In Proceedings of the 13th Annual Symposium on Network and Distributed System Security, 2006.