

Chapter 4

Network Forensics – Detection and Mitigation of Botnet Malicious Code via Darknet

R. Azrina, R. Othman, Normaziah A. Aziz, M. ZulHazmi, M. Khazin, J. Dewakunjari

Department of Computer Science, Kulliyyah of ICT, International Islamic University Malaysia

P.O. Box 10,50728 Kuala Lumpur, Malaysia

E-mail: razrina.rothman@jaring.my, naa@iium.edu.my

Computer malwares are major threats that always find a way to penetrate the network, posing threats to the confidentiality, integrity and the availability of data. Network-borne malwares penetrate networks by exploiting vulnerabilities in networks and systems. IT administrators in campus wide network continue to look for security control solutions to reduce exposure and magnitude of potential threats. However, with multi-user computers and distributed systems, the campus wide network often becomes a breeding ground for botnets. We present our work that applies the network forensic techniques via Darknet implementation for passive detection of malware infected computers; primarily botnets, in a campus wide network. Verification activities were conducted on the infected hosts. This work analyses the effectiveness of network forensics capability and the accurate detection of malicious traffic. An accurate detection of malware-infected host enables enforcement of security policies through isolation of hosts and eventually will enhance network performance. Alongside presenting various aspects of our work, some recommendation are proposed for preventive measurements to avoid further propagation of bots and network-borne malwares within campus wide network.

4.1 Introduction

Network is now pervasive and a critical entity in our every day working and learning environment. Despite increasing devices being connected to the TCP/IP network such as mobile phones, GPS, and iPads, personal computers are current main targets of exploits, primarily for malware and bot infection and propagation. The infection of personal computers with malware can compromise confidentiality, integrity and availability of information as well as take up unnecessary bandwidth.

Network forensics is the use of scientifically proven techniques to collect, fuse, identify, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response to orrecovery from these activities [1]. In order to capture network activities for analysis, a sensor is deployed in the network. The type of sensor and its location in the network influence the traffic being captured. Darknet [2] sensor is one of the available methods that is used and described in this chapter.

Network forensics can detect mainly two types of malwares – worms and botnet. Worm is a kind of malware that propagates via network; by network scanning and self-replicating email. Botnet is a collection of software robots, or in short termed ‘bots’, that run autonomously and automatically. The term *botnet* [3, 4] can also be used to refer to any group of bots, such as IRC bots (Internet Relay Chat bots). In general, botnet refers to a collection of compromised computers, or *Zombie* computers that receive instructions from command and control (C&C) servers. The command-and-control can take place via IRC server or a specific channel on a public IRC network, http, DNS and peer-to-peer application. The communication is encrypted for stealth and protection against detection and intrusion into the botnet network.

The chapter discusses on network forensics via implementation of Darknet and the sensors as an effort to detect computers that are infected with bots in campus wide network. A more interactive system implementation involving capturing of malware is outside the scope of this work.

The rest of the chapter is arranged as follows: Section 4.2 describes the background of the work, Section 4.3, presents the motivation for this work along with the related works. Section 4.4 talks about our approach used in carrying out this project. Section 4.5 presents the acquired results of our research implementation. We also discuss the possible countermeasures and recommend some steps to deal with the issues. And finally, Section 4.6 concludes the paper with some remarks about the outcome of the work.

4.2 Background

The key mechanism for bot propagation is via worm behaviour, which is network borne. It is noted that bots may also spread via email spam, web page drive-by affect and mo-

bile storage media. Botnets usually gain new victims through network scanning to detect available vulnerable systems and remotely exploiting the vulnerabilities of systems and applications running on networked host. Botnets borrow infection strategies from several classes of malware, including self-replicating worms and e-mail viruses, among others [5]. Once infected; a script (known as *shell code*) is executed which connects to another bot at a specified location which hosts malware binaries and fetches the actual bot binary. Upon completion of the download, the bot binary installs itself to the target machine so that it starts automatically each time the victim is rebooted. Figure 4.1 illustrates the botnet's lifecycle [6].

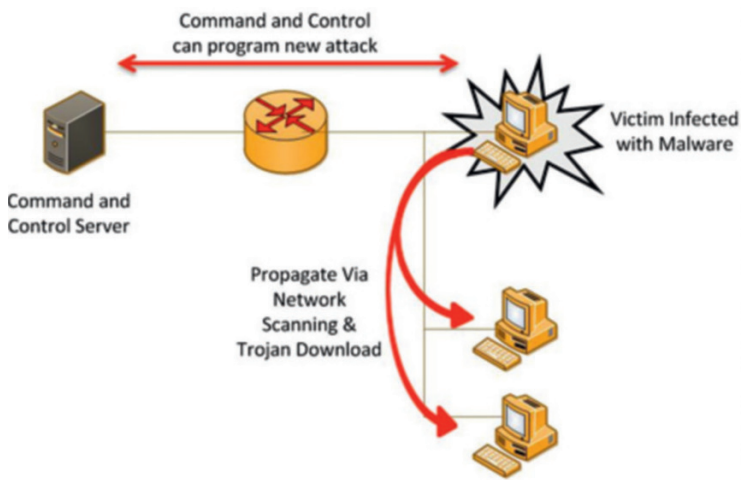


Fig. 4.1 Lifecycle of Botnet

4.3 Motivation and Related Works

Industry analysts estimate that about 5% to 10% of all PCs are infected with sophisticated, remotely controlled malware. The current defences of layering firewall, Intrusion Prevention System (IPS) and anti-virus are ineffective in stopping advanced malware, zero-day and targeted attacks once it enters into the network [7]. Network Intrusion Detection System (NIDS) conducts passive has evolved into IPS, and the detection technique, very much depends on the signature had matched a known exploit or having to know the vulner-

abilities. Both these aspects require a challenging effort in keeping up with the exponential growth of exploit signature and vulnerabilities.

A similar approach of using darknet for detection of botnet was used by researchers in the John Hopkins University. Their work involved measuring botnet traffic, in the size of hundreds to thousands. Their findings revealed botnets are a major contributor to the overall unwanted traffic on the Internet. They confirmed that although the scan generated by botnet are primarily to recruit new victims, the behavior is markedly different from autonomous malware, worms, because of its manual orchestration. They also discovered that IRC remain to be the dominant protocol for C&C communication [8].

A lot of the work done has been to quantify the size of botnets, the growth, and their behavior. In the context of our work, the main objective is to apply darknet technique to accurately detect bots and network-borne malware and eventually confirm via live forensics the type of infection on the affected hosts in a campus wide network. As such the darknet is ideally deployed in a LAN environment to enable verification of hosts to be conducted. This will also provide insight on the effectiveness of security controls within the campus wide network and the computers in defending against bot and network-borne malware. The specific objectives of this project are to: a) passively identify infected computers in the network; b) analyse the types of botnets that are infecting the computers in the campus; c) identify the attack vector or how the bot penetrated into the host or computer, if possible; d) identify the source of the bot or malware, if possible; e) provide recommendations on countermeasures against future attacks.

4.4 Our Approach and Implementation

Monitoring all traffic within a large-scale network to track compromised computer client and malicious traffic requires a lot of resources; Intruder Detection System (IDS) (with packet processing capability to carry out packet capture and analysis) as well as large capacity of storage. Once the data are captured, there is an issue on the preserving of confidentiality of the information, which may contain legitimate traffic with sensitive information such as passwords.

On the other hand, the above issues are not present in the Darknetimplementation. Darknet involves capturing and monitoring traffic communication to unused IP Addresses. Darknet is a portion of routed, allocated IP space in which no active services or servers reside. Any packet that enters a Darknet is by its presence aberrant because no legitimate

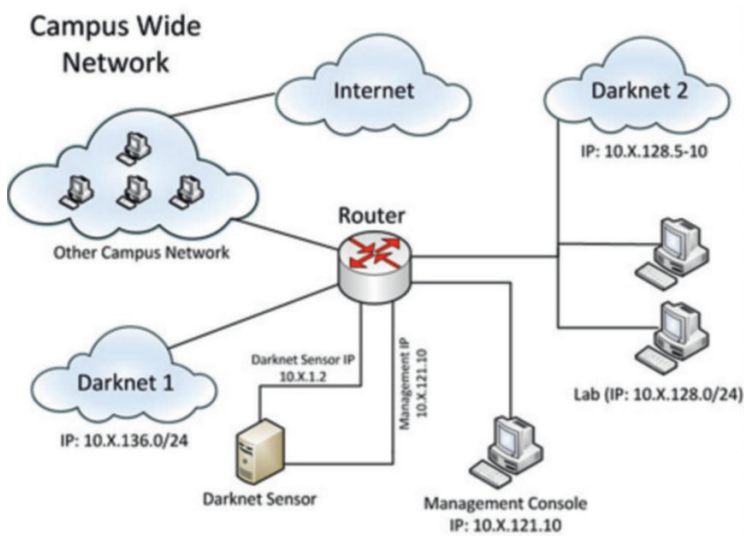


Fig. 4.2 Network diagram

packet should be sent to a Darknet. Such packets may have arrived by mistake or wrong configuration, but the majority of such types of packets are sent by malware.

Figure 4.2 demonstrates the network used for the implementation and analysis of this research. The network consists of two parts with a /24 mask. We chose to have one of the /24 network to be assigned to a Darknet 1, while another ten IP Address is assigned to Darknet 2. The Darknet 2 is part of IP range within a computing lab, that is used actively on daily basis. A sensor server is setup with 2 network interfaces, one to passively capture packets destined to the darknet, while the other network interface is used for administrative access to the sensor from the management console. In order to have any traffic destined to the Darknet, diverted to the sensor, the router needs to be configured to send all Darknet prefix traffic to the Darknet Sensor interface.

```

outer#conf t
router(config)# ip route 10.X.136.0 255.255.255.0 10.X.1.2
router(config)# ^Z
router# wr

```

The sensor requires a separate network interface for the management console access primarily to prevent poisoning the Darknet with legitimate traffic. The setup immediately

generated records showing network traffic activity entering the Darknet from various internal hosts. Further analysis was done on the infected computer to identify the type of malware as well as other security controls present in the system.

4.5 Experimental Results and Analysis

After appropriate configurations of all necessary parts of our network, data were collected from the Darknet throughout a one month period. This implementation produced very significant results. In this section, we will discuss in our findings.

Upon analysis of the data, a few anomalous network traffic communications can be observed on destination port 445 and ICMP.

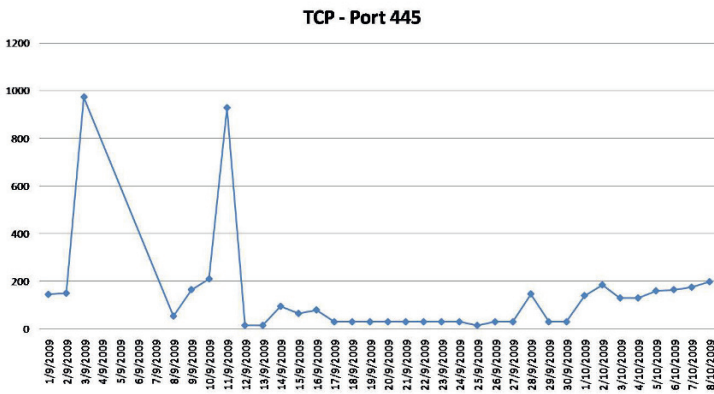


Fig. 4.3 Time series of SYN packets of port 445

Based on the data obtained at the sensor server, which can consists of any sniffer based technology such as tcpdump, all the ICMP communication sent to the Darknet are identified as echo requests. Figures 4.3 and 4.4 show the network communication to port 445 and ICMP. As shown in the Figure 4.3, the network activities were decreasing in the middle of the month which is due to the mid-semester break and other vacation period. Therefore, most computer clients were not active during those times. However, the network activities began to increase after the semester vacation.

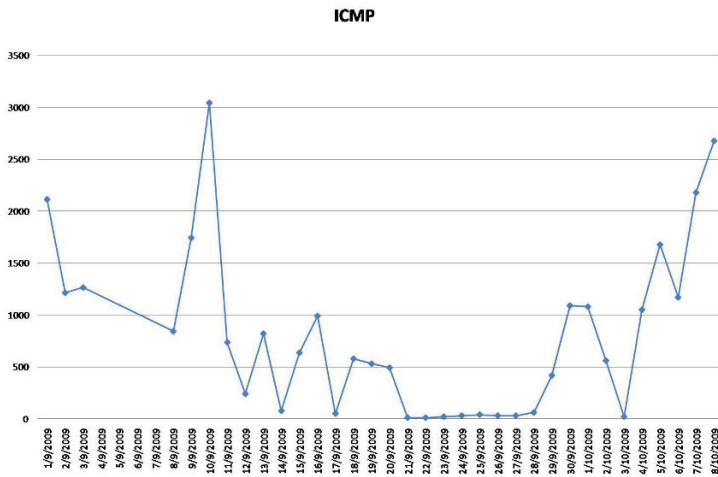
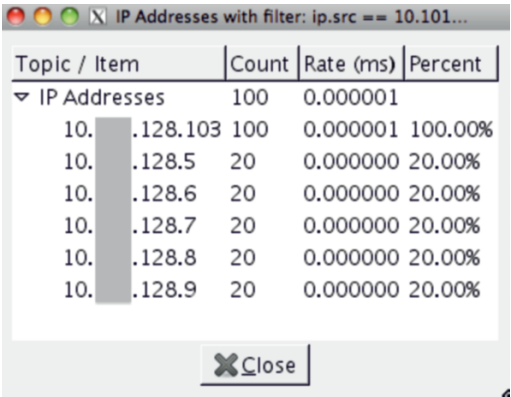


Fig. 4.4 Time series of incoming ICMP packet

Referring to the Figure 4.4, the ICMP traffic shows similar pattern as port 445 network activities, in which low network activities were observed in the middle of the month due to the fact that most of the computers remained turned off during the semester breaks. The network activities began to increase again after the semester breaks.

4.5.1 Further Analysis on Destination Port 445 Traffic

Destination port 445/TCP is commonly used and assigned for Microsoft-DS Active Directory and Windows shares. Thus, this port is to be used when the organization is using Microsoft Domain Service Active Directory and Windows File Sharing [9, 10]. However, all identified computer clients were not using Microsoft Domain Service Active Directory and had insignificant usage of Windows File Sharing. Each computer suspected to be infected with malwares sent 20 TCP SYN requests of size 64 bytes to each unique destination IP address as shown in Figure 4.5.



Topic / Item	Count	Rate (ms)	Percent
IP Addresses	100	0.000001	
10. .128.103	100	0.000001	100.00%
10. .128.5	20	0.000000	20.00%
10. .128.6	20	0.000000	20.00%
10. .128.7	20	0.000000	20.00%
10. .128.8	20	0.000000	20.00%
10. .128.9	20	0.000000	20.00%

Fig. 4.5 TCP/445 probes summary generated by host 10.x.128.103

4.5.2 Further Analysis on ICMP traffic

The ICMP echo requests (commonly known as “ping”) are used primarily for troubleshooting network connection. Most Internet gateways now block incoming echo requests in order to avoid Distributed Denial of Service (DDoS) [11] attacks. Historically, several malwares that propagate via ICMP echo request include Nachi worm [12]. The collected data indicate that each infected host generated only a single ping probe to each sequence of unique IP, as shown in Figure 4.6. This indicates ping sweep, not ping flood. Ping sweep would be relevant for the purpose of determining whether the host is alive or not.

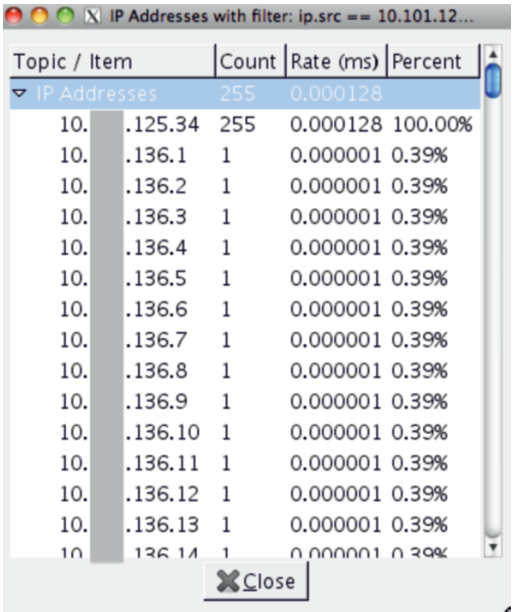


Fig. 4.6 Summary of ICMP Echo Request generated by host 10.x.125.34

4.5.3 Analysis of Suspected Client

Four of the suspected (infected) computers were selected for our analysis. The selection was mainly based on the ability to gain physical access to the computers within the duration of the project. Table 4.1 shows the information gathered pertaining to the suspected computers that were analyzed. One of the hosts had most recent updated antivirus signature, while three other hosts had the antivirus signature outdated, and in which one of them apparently has the license expired. All four hosts sampled, were running on Windows XP.

Table 4.1 Selected Computer System’s Information

Client No / System Info	Client 1	Client 2	Client 3	Client 4
Operating System	MS Windows XP SP 2	MS Windows XP SP 2	MS Windows XP SP 3	MS Windows XP SP 3
Antivirus Name and Signature Status	eScan - outdated	eScan - outdated	Avira - recently updated	Avira - outdated and license expired

Further analysis was conducted on each host via live forensics, using tools such as Sysinternals Suite [13] as well as other standard tools such as Netstat [14]. The investigation revealed that the hosts were not only infected with multiple malwares but also they were actively establishing connection to foreign hosts in the Internet. Based on the analysis of the reputation of the foreign hosts’ IP addresses, they were confirmed to be rated high risk and minimal risk, as well as reputed to be malicious C&C and Backdoor Trojan sites. The host running the antivirus with recently updated signature was found to be infected with the Conficker malware [15] as well as possibly Autoit malware [16], while the IP Address of the remote host in Hong Kong is reputed as High Risk. The acquired information is shown in Table 4.2.

Table 4.2 Suspected Client System’s Information 2

Client No	Client 1		Client 2	
Malware Detected	Conficker, Mabezat, IRC Trojan Backdoor		Conficker, Mabezat, IRC Trojan Backdoor, Trojan Dropper, Sality	
Foreign Addresses - Reputation	149.9.1.16	Minimal Risk - IRC Server (TrustedSource) C&C (Emerging Thread)	85.25.176.33	High Risk (TrustedSource)
			74.208.64.145	High Risk - Malicious Sites, Phishing (TrustedSource) IRC Trojan Backdoor (ThreatExpert)
			89.149.227.194	High Risk - Malicious Sites Sality Virus (ThreatExpert)
			87.106.24.200	High Risk - SmartFilter Category: Malicious Sites, Phishing (TrustedSource) IRC Trojan Backdoor (ThreatExpert)

Client No	Client 3		Client 4	
Malware Detected	Conficker, Autoit		Autoit	
Foreign Addresses with Bad Reputation	110.44.0.50	High Risk - Malicious Sites (TrustedSource)	204.12.222.155	Minimal Risk - Not Categorized (TrustedSource) Autoit (ThreadExpert)

McAfee® TrustedSource™ is a global threat correlation engine and intelligence base of global messaging and communication behavior, including reputation volume, and trends, including email, web traffic and malware. Refer to <http://www.trustedsource.org/> ThreatExpert is an advanced automated threat analysis system designed to analyze and report the behavior of computer viruses, worms, trojans, adware, spyware, and other security-related risks in a fully automated mode. Refer to <http://www.threatexpert.com/>

Figure 4.7 illustrates how the botnets propagate within the campus wide network (based on the findings). The computer was confirmed to be infected with IRC Trojan backdoor and Conficker worm. They were scanning the LAN network for other vulnerable computers.

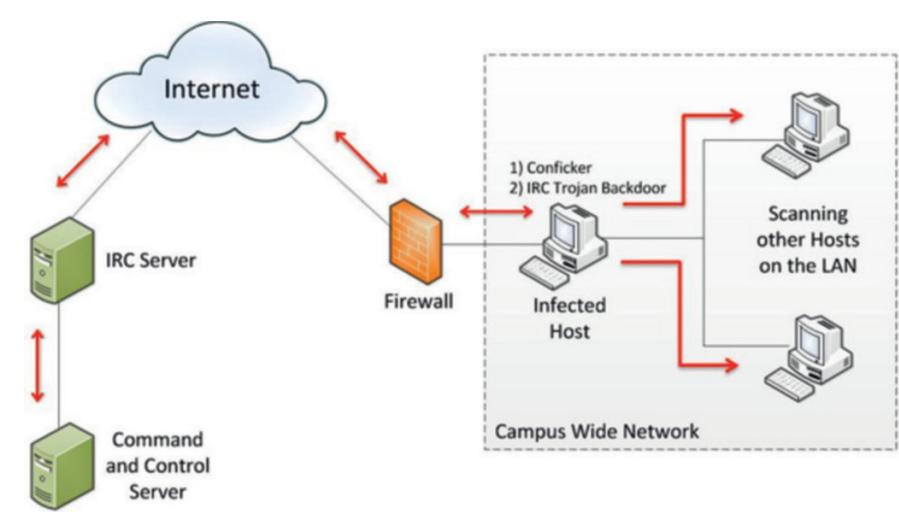


Fig. 4.7 Botnet attack on a campus network

Despite having perimeter defence which included the firewall, the infected hosts were able to establish outgoing connection to unauthorized external hosts, due to the lack for policy enforcement for outgoing traffic. The internal scanning activity generated by the infected host also caused unnecessary utilization of the bandwidth.

4.6 Future Work

There are several areas in which this research can contribute. In addressing operational level security, an organization requires sufficient skilled manpower to effectively apply enforcement measures at the system and network level. The use of remote management system will enable real-time alerts and integration to other application and systems that can enforce more restrictive policies. The Darknet can be integrated with Walled Garden method [17] to isolate the infected computer. The system can also be integrated with IPS to prevent unauthorized outgoing traffic from infected hosts. A graphical interface or dashboard can be integrated to provide visual status of malicious network activities. The use of Darknet is one practical solution, which requires low amount of resources to process the gathered data.

4.7 Concluding Remarks

The study identified a total of 31 computers suspected to be infected with malwares and 4 of them were proven to be infected by malwares; mainly Conficker which had caused high network traffic to destination port 445 and Autoit malware contributed high ICMP network traffic. This further confirms that high amount of ICMP traffic generally indicates a virus [18]. Using the Darknet, small amount of captured anomalous data were sufficient to elevate the attention to the problem. There was no need to sift through legitimate data to identify anomalous traffic.

Based on the analysis of our work, it can be concluded that the security controls at network and host level at certain segments of the network are insufficient and not effectively protecting the campus wide network from malware and bot propagation and infection. We present our recommendations to deal with this issue which we believe will be useful for similar settings.

Acknowledgments

This work was supported by the International Islamic University Malaysia particularly the Department of Computer Science and the university's central Information Technology Division. Credit goes to our Information Security Research Group (ISRG), Network Forensics team – Mohamed ZulHazmi, Dewakunjari J., Pengiran, A. Khaliq Ismail, KhairilFahmi, Ahmad Hassan and Mukmin for their determination and commitment in this research.

Bibliography

- [1] G. Palmer, A Road Map for Digital Forensic Research, DFRWS Technical Report, DTR-T001-01 Final, (Air Force Research Laboratory, Rome, New York, 2001).
- [2] Team Cymru, "The Darknet Project", Internet Security Research and Insight (2009). Available: <http://www.team-cymru.org/Services/darknets.html> [Last accessed: 1st November 2009].
- [3] Seewalda, A.K. and Gansterer, W.N., "On the detection and identification of botnets," *Computers & Security*, Volume 29, Issue 1, (Elsevier, February 2010), pp. 45–58.
- [4] Wang, P., Sparks, S., and Zou, C.C., "An Advanced Hybrid Peer-to-Peer Botnet," *IEEE Transactions on Dependable and Secure Computing*, Vol. 7, No. 2, (April-June 2010), pp. 113–127.
- [5] A.B. Moheeb, J. Zarfoss, M. Fabian, and T. Andres, "A Multifaceted Approach to Understanding the Botnet Phenomenon." In 6th ACM SIGCOMM conference on Internet measurement, (2006), pp. 41–52.
- [6] C. Jaideep, L. Carl, O. Steve, and S. Eve, "The Dark Cloud: Understanding and Defending against Botnets and Stealthy Malware", infoq.com, (Aug. 04, 2009). Available: www.infoq.com/.../intel-botnets-malware-security [Last accessed: Oct. 12, 2009].
- [7] Advanced Malware Exposed, Fire Eye Whitepaper, (FireEye Inc. California, 2011).
- [8] A.B. Moheeb, J. Zarfoss, M. Fabian, and T. Andres, "A Multifaceted Approach to Understanding the Botnet Phenomenon." In 6th ACM SIGCOMM conference on Internet measurement, (2006), p. 51.
- [9] Internet Assigned Numbers Authority (IANA), "Port Numbers," Internet Corporation for Assigned Names and Numbers(2009). Available: <http://www.iana.org/assignments/port-numbers> [Last accessed 13 November 2009].
- [10] "List of TCP and UDP port numbers" (2009). Available: http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers [Last accessed: 13th November 2009].
- [11] Sun, X., Torres, R., and Rao, S., "Preventing DDoS attacks on internet servers exploiting P2P systems," *Computer Networks*, Volume 54, Issue 15, Elsevier, (28 October 2010), pp. 2756–2774.
- [12] Cisco Security Notice: Nachi Worm Mitigation Recommendations, available at: <http://www.cisco.com/warp/public/707/cisco-sn-20030820-nachi.shtml> [Last accessed: 25th September, 2010]
- [13] Sysinternals Suite. <http://technet.microsoft.com/en-us/sysinternals/bb842062.aspx> [last accessed: 10th Sept 2010]
- [14] <http://www.netstat.net/> [Last accessed 5th Sept 2010]
- [15] Conficker Malware. <http://mtc.sri.com/Conficker/> [Last accessed 6th October 2010]

-
- [16] Autoit Malware. <http://www.threatexpert.com/report.aspx?md5=ef0c08d5d1ebc1f792a617580263a42c> [Last accessed 5th Sept 2010]
 - [17] MAAWG Best Practices for the Use of a Walled Garden, MAAWG Whitepaper (October, 2007).
 - [18] Skyway West, "Basic Security Requirements: ICMP Rate Limit," Skyway West Business Internet Services, (2009). Available: <http://www.skywaywest.com/support/basic-security-requirements.php> [Last accessed: 18 November 2009]