Botne and Botnet Detection Survey

Manar Y. Ahmad **Maisireem A. Kamal**

College of Computer Sciences and Mathematics
University of Mosul, Mosul, Iraq

Received on: 02/10/2012 **Accepted on: 30/01/2013**

ABSTRACT

Among the various forms of malware, Botnets are emerging as the most serious threat, Botnets, remotely controlled by the attackers, and whose members are located in homes, schools, businesses, and governments around the world.

This paper is a survey about Botnet and how Botnet is detected. The survey clarifies Botnet history, Botnet lifecycle, Botnet detection techniques, and proposed software has ability to detect (koobface) Botnet which attacks facebook website.

Keywords : Botne, Botnet Detection, Botnet detection techniques, (koobface) Botnet

دراسة حول الكشف عن Botne و Botnet

منار يونس كشمولة **ميس الريم عضيد**

كلية علوم الحاسبات والرياضيات

جامعة الموصل، الموصل، العراق

تاريخ استلام البحث: 2012/10/02 **تاريخ قبول البحث: 2013/01/30**

الملخص

بين أشكال مختلفة من البرمجيات الخبيثة ومضارها على مستخدمي شبكة الانترنيت، فان الـ Botnet يعتبر أكثرها خطر أو تهديدا للمستخدمين حيث يتم التحكم بحواسيب المستخدمين عن بعد من قبل المهاجمين، والهجمات تقع على مستخدمي شبكة الانترنيت في المنازل والمدارس والشركات والحكومات في جميع أنحاء العالم.

يقدم البحث دراسة مستفيضة حول الـ Botnet والـ Bot وكيف يتم الكشف عنها في شبكات الانترنيت وتتضمن تاريخ الـ Botnet، دورة حياة الـ Botnet، تقنيات كشف الـ Botnet، ودراسة تقنيات كشف الـ Botnet ، وأخيرا اقتراح تصميم نظام لكشف Botnet (koobface) الذي يقوم بمهاجمة مستخدمي الموقع الالكتروني FACEBOOK.

الكلمات المفتاحية: Botne، كشف Botnet ، تقنيات كشف Botnet ، Botnet (koobface).

1. Introduction

The computer and Internet age have ushered in a new breed of criminals who use technology for fraud and abuse. These computer hackers steal information from both individuals and businesses by penetrating firewalls, intercepting data during transmission, attacking unprotected home wireless networks, and other means [1].

Hackers have traditionally created computer viruses more for status and bragging rights than for financial gain. ''But now hackers are mixing with fraudsters and organized crime rings'' and ''viruses are being used illegally for financial gain, and they are becoming part of the modern criminal's toolbox.'' Criminals will use variations of viruses to take over multiple computers, often all over the world, and turn them into ''zombies.'' This results in a Botnet, a large-scale network that criminals can control remotely and use for malicious purposes [1]

Botnets (or, networks of zombies) are recognized as one of the most serious security threats today [2]. Botnets are nowadays one of the most serious threats to cybersecurity. The term Botnet is used to define a network of infected machines, called bots, which are under the control of a human operator commonly known as Botmaster. The term Botnet denotes a network of compromised end hosts (bots) under the remote command of a botmaster [3]. Once a Botnet has been constructed, these bots are controlled autonomously and automatically, in some cases to perform some illicit monetary activities [4].

Bots are used to carry out a wide variety of malicious and harmful actions against systems and services: DoS attacks, spam distribution, phishing and click fraud, among others [5]. As an example of the relevance of Botnets deployment, the (Federal Bureau of Investigation) FBI has recently uncovered more than $20 million in economic losses in the USA. In one case, a victim confirmed damages of nearly $20,000 due to denial of service attacks committed from Botnets (FBI, 2007) [6 and 7].

Economical profits are also usually behind the design and development of Botnets by botmasters. They can reportedly make large sums of money by marketing their technical services. One example of that is Jeanson Ancheta, a 21-years-old hacker member of a group called the "Botmaster Underground". He received more than $100,000 from different Internet advertising companies using his Botnet with more than 400,000 vulnerable PCs [6 and 7]

To understand the scope and thus, the threat Botnets represent, let us point out that Vinton Cerf, one of the "fathers of the Internet", estimated that between 100 million and 150 million of the 600 million hosts on the Internet were part of a Botnet [6 and 8]. This represents a 16–25% of the total of computers connected to the Internet [6 and 8].

As a consequence of the impact of Botnets, the research community is increasing its interest in this field. The number of publications on Botnets has exponentially grown in the last decade, from only a few in earliest 2000 to several hundreds in the last year. Taxonomies on Botnets have been proposed. They all seem to put their focus on the different aspects of Botnets, like architecture, communication protocols, detection techniques, etc., presenting a separate taxonomy for every one of these aspects. Due to this fact, despite these taxonomies allow to understand certain aspects of Botnets, it is difficult to get a complete vision of the problem from them. Botnet detection has been a major research topic in recent years. Researchers have proposed several approaches for Botnet detection to combat Botnet threat against cyber-security [6].

For this reason, there is a need to contribute a deep analysis that deal with the Botnet problem from a global perspective. In this paper, we provide a survey of current Botnet technology and defense by exploring the intersection between existing Botnet research, the Botnet life-cycle begins with the conception of the Botnet, and has the final objective of carrying out a certain attack.

The remaining part of the paper is organized as follows: Section 2 explains a Botnet history and trends, section 3 describes motives and economics, section 4 describes a botnet phenomenon, and botnet characteristics are explained in section 5, Botnet life-cycle is explained to provide better understanding of Botnet technology in section 6. Section 7 states botnet classification, sections 8 and 9 discuss Botnet type and detection technique. Finally, in section 10, we summarize our survey and suggest future directions.

2. Botnet History and Trends

Internet Relay Chat (IRC) was invented in August of 1988 by Jarkko Oikarinen of the University of Oulu, Finland. This protocol provides a platform that allows data dissemination among large number of end users by supporting multiple forms of communication (point-to-point, point to multi-points, etc.) [3 and 4]. As the IRC protocol developed, administering busy channels, such as handling tedious 24-hours-a-day requests from users, becomes time consuming. Bot, or robot, was then created as the benign assistant to IRC channel management.

In 1989, Greg Lindahl, an IRC server operator, created the benevolent bot called GM which would play a game of Hunt the Wumpus with IRC users. Starting from this simple example, bots have evolved from being code that helps a single user to code that manages and runs IRC operations on local host as well as code that provides services for other users. Bots gradually have been developed into a comprehensive tool which operates as an IRC channel operator, for example, Eggdrop was written in 1993 to assist channel operators. In time, IRC bots with more nefarious purposes emerged when some IRC servers and bots began offering the capability to make OS shell available which permits users to run commands on the IRC host. By the late 1990s, massive amount of trojan-infected computers tended to be grouped together and remotely controlled by a botmaster connected to an IRC server [3, 4].

Version 2.1 of the SubSeven Trojan, released in June 1999, included the typical malicious functions, (such as stealing password, logging keystrokes, and hiding its identity), and provided a significant new feature that permits the SubSeven server to be remotely controlled via an IRC channel. This link, between trojan server and IRC channels, set stage for all malicious Botnets to come [3, 4].

In 2005, over a four month span of Botnet research conducted by the Honeynet Project, over a million computers were observed as members of Botnets [4].

For over a decade, IRC based Botnets were predominant among all the other existing ones. However, as the Botnet detection escalates, Botnets have also evolved. In terms of protocol, more and more Botnets start to implement HTTP and Fast Flux network based on DNS servers; topology wise, instead of the traditional single server centralized structure, more sophisticated structures, such as a group of IRC servers with inter links between each other or a Hybrid P2P system, have been implemented [4].

In 2009, Conficker - arguably the most influential and sophisticated Botnets - has appeared. Conficker has implemented the DNS as the C&C protocol and a P2P C&C structure [4].

3. Motives And Economics

About 600 million computers are connected to the internet, of these computers 100-150 million are part of one or several Botnets. One Botnet alone was discovered to consist of about 1.5 million computers, when three Dutch botmasters were arrested for extorting a US company [15]. To illustrate the resources exploited by Botnets, a single Botnet was at one point using 15% of Yahoo’s search capacity to create random e-mails to get past spam filters. According to an FBI projection, cybercrime robs U.S businesses for $67.2 billion a year. That amount of money is good motivation for doing any crime [9].

Message Labs reports that Botnets are responsible for distributing 87.9% of all spams and there is an increase of 2.9% from the second quarter of 2009 and most of these spam emails come from the Botnets. In addition, the attacker can use phishing e-mails to expand his Botnets [10].

Jeremy Jaynes, one of the top ten spammers in the world, allegedly made 750 000 dollars a month from spamming people, with offers ranging from fake goods to pornography. His email schemes had given him a total income of 24 million dollars. Considering that there is little risk of ever getting caught, combined with the possibility of high profit, there is no surprise that scams on the internet has exploded. In fact, according to US treasury advisor Valerie McNiven, last year proceeds from cyber crime were greater than proceeds from sale of illegal drugs [9].

As of January 2007, Google's Vinton Cerf estimated that up to 150 million computers (about 25% of all Internet hosts) could be infected with bot software [11].

Botnets are motivated by financial profit. Organized crime groups often use them as a source of income, either by hiring "freelance" botmasters or by having their own members create Botnets. As a result, network security professionals are up against motivated, well-financed organizations that can often hire some of the best minds in computers and network security. This is especially true in countries such as Russia, Romania, and other Eastern European nations, where there is an abundance of IT talent at the high school and university level, but legitimate IT job prospects are very limited. In such an environment, criminal organizations easily recruit recent graduates by offering far better opportunities than the legitimate job market. One infamous example of such a crime organization is the Russian Business Network (RBN), a Russian Internet service provider (ISP) that openly supports criminal activity. They are responsible for the Storm Worm (Peacomm), the March 2007 DDoS attacks on Estonia, and a high-profile attack on the Bank of India in August 2007, along with many other attacks. It might not be immediately obvious how a collection of computers can be used to cause havoc and produce large profits[11].

Other motivation reasons are:

1. Data regarding bots is rarely available. This is due to the fact that the Botnet data can contain sensitive information. As a result, making this data publicly available can be dangerous [10].
2. Botnets pose a severe threat to Internet security. For example, an army of several thousand bots can exhaust the bandwidth of a large number of systems or networks. An attacker can use the Botnet to perform malicious activities. These activities include performing any attacking behavior which will be explained in the next sections [10].
3. During the past few years, there was an exponential growth of using Botnets to perform large number of malicious activities ranging from Internet Relay Chat (IRC) bots and Peer-to-Peer (P2P) bots ,Mcafee also reports that they have observed fourteen million new bots in the second quarter of the year 2009, in comparison to nearly twelve million new bots in the first quarter in the same year which is approximately an increase of more than 150,000 new bots every day as shown.

4. Botnet Phenomenon

Botnets are emerging as the most significant threat facing online ecosystems and computing assets. Malicious Botnets are distributed computing platforms predominantly used for illegal activities such as launching Distributed Denial of Service (DDoS) attacks, sending spam, trojan and phishing emails, illegally distributing pirated media and software, force distribution, stealing information and computing resource, ebussiness extortion, performing click fraud, and identity theft [5].

The high light value of Botnets is the ability to provide anonymity through the use of a multi-tier command and control (C&C) architecture. Moreover, the individual bots are not physically owned by the botmaster, and may be located in several locations spanning the globe. Differences in time zones, languages, and laws make it difficult to track malicious.

Botnet activities across international boundaries. This characteristic makes Botnet an attractive tool for cybercriminals, and, in fact, poses a great threat against cybersecurity [5].

5. Botnet Characteristics

Like the previous generations of viruses and worms, a bot is a self-propagating application that infects vulnerable hosts through exploit activities to expand their reach. Bot infection methods are similar to other classes of malware that recruit vulnerable systems by exploiting software vulnerabilities, trojan insertion, as well as social engineering techniques leading to download malicious bot code. According to measurement studies in [3 and 5] modern bots are equipped with several exploit vectors to improve opportunities for exploitation.

However, among the other classes of malware, the defining characteristic of Botnets is the use of command and control (C&C) channels through which they can be updated and directed. The multi-tier C&C architecture of Botnets provides anonymity for the botmaster. C&C channels can operate over a vide range of logical network topologies and use different communication protocols. Botnets are usually classified according to their command and control architecture [5].

According to the command and control architecture, Botnets can be classified as IRC-based, HTTP-based, DNSbased or Peer to Peer (P2P) Botnets. P2P Botnets use the recent P2P protocol to avoid single point of failure. Moreover, P2P Botnets are harder to locate, shutdown, monitor, and hijack. However, based on the analysis in [3 and 5] the most prevalent Botnets are based on Internet Relay Chat (IRC) protocol with a centralized command and control mechanism. IRC protocol was originally designed for large social chat rooms to allow for several forms of communication and data dissemination among large number of end-hosts. The great prevalence of IRC-based Botnets is due to the inherent flexibility and scalability of this protocol. Furthermore, there are several open-source implementations that enable botmasters to extend them according to their demands [3 and 5].

6. Botnet Life Cycle

During the initial infection phase, the attacker, scans a target subnet for known vulnerability, and infects 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 from the specific location via FTP, HTTP, or P2P. The bot binary installs itself on the target machine. Once the bot program is installed, the victim computer turns to a “Zombie” and runs the malicious code [4, 13 and 14]. The bot application starts automatically each time the zombie is rebooted.

The general life cycle of a Botnet, shown in Figure 1, contains four phases: initial infection, secondary injection, maintenance and update, and malicious activities [5, 12, 13 and 14].

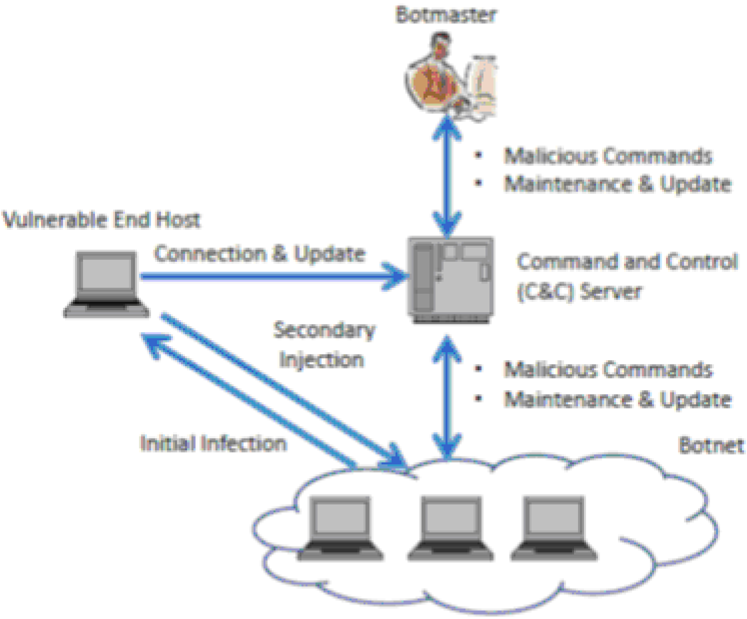


Figure 1. A General Botnet Life Cycle [5]

This material is based upon work supported by the National Science Foundation under Grant No. 0915552 and a Cisco Systems URP gift [4].

1) Initial Infection: A computer can be infected in different ways: Inadvertently execute malicious code, exploit system vulnerabilities, and access through engineered backdoors. Users may accidentally download and execute the malicious programs while viewing a Web Site, opening an attachment from an email, or clicking a link in an incoming instant message. Every released patch to update some of the most popular operating systems, such as Windows XP and Windows 7, is followed by a flurry of reverse engineering in the hacker community in order to exploit the problems that the most recent patch has fixed, because millions of users tend not to update their computer promptly and properly. Also, some ports, which are used for Remote Access or File Sharing services, are under constant scanning from other bots for vulnerabilities check, for example, port 135 - Microsoft Remote Procedure Call (RPC) service, and port 139 - Netbios File Sharing Service [3]. The term 'backdoor' denotes as the port which is forcefully opened by the malicious softwares, allows for remote connection and therefore gives up the administrative control of the compromised computer. Given the current circumstances, a vulnerable computer is usually infected by multiple malicious software programs. In order to take advantage of this fact, a list of ports has been routinely examined by a single malicious software for backdoors left by others, including port 2745 - backdoor of Bagle worm, and port 3410 - backdoor of Optix Pro remote access trojan [5, 13 and 14].

2) Secondary Injection: Although, a particular Botnet makes use of possible backdoors left by other Botnets, it does not mean that botmasters would like to have a common shared pool of bots. So, most communication and command protocols are Botnet-specifically designed. Intuitively, most of the source codes are confidential. Although some most popular Botnets have their source codes publicly available (e.g., Agobot, SDBot, and GT Bot), due to the complexity and modularity of the coding architecture, along with the constant evolvements of the Botnets, there are no standardized command and control functions [4].

Therefore, after the successful initial infection, the next step is to download and run the Botnet code in order to become a bot which is under control of a specific botmaster. This procedure can be processed by using Trivial File Tansfer Protocol (TFTP), File Transfer Protocol (FTP), HyperText Transfer Protocol (HTTP) or CSend [5, 13 and 14].

3) Maintenance and Update: The first two stages only contain communications between bots and targeted computer. After becoming a bot, the infected machine starts to 1) log into the command and control server and 2) create a protected session parsing and executing the topics in the channel. These two steps are processed periodically and require authentication. Before the botmaster authorizes certain malicious activities, such as Distributed Denial of Services (DDoS), it usually sends out an update command to the C&C server which in turn contacts the bots to give the botmaster an updated status feedback of the Botnet. These internet flows, especially the periodically log/listen sessions, are of great interest for Botnet detections, since the passive intrusion detection system (IDS) would like to recognize the suspicious patterns and disrupt the Botnet before the actual attacks take place [5, 13 and 14].

4) Malicious Activities: The aforementioned definition of Botnet indicates that Botnets are mostly used for criminally motivated activities, include Distributed Denial of Services, Click Fraudulence, Spamming, and Identity Theft [5, 13 and 14].

a) Distributed Denial of Services (DDoS), b) Click Fraudulence, c) Spamming, d) Identity Theft

7. Bot Classification

There is no industrial standard for bot classification. However, all noted sources use the same approach to classify bots. In general, this approach can be reduced to the following [16]:

- Bots are divided into two main groups “good” bots and “bad” ones or malware bots.
- According to the Honeynet.org group and to the main producers of antivirus software, malware bots can be divided into 9 main classes:
  1. Lisp IRC Bots
  2. Click bot or hitbot
  3. Agobot/Phatbot/Forbot/XtremBot
  4. SDBot/RBot/UrBot/UrXBot
  5. mIRC-based Bots - GT-Bots
  6. DSNX Bots
  7. Q8 Bots
  8. Kaiten
  9. Perl-based bots.

8. Types Of Botnets

There is a variety of Botnets causing the mass destruction. The three major categories depend on the type of command and control they are as follows:

- IRC Botnets: The IRC (Internet Relay Chat) protocol was initially designed for real-time Internet text messaging. The building ground of IRC is TCP/IP protocol. It works by making a central location and then all the required users (clients) connect to that central location; and that central location is called server; while anything except server is called client. the most vulnerable feature of an IRC is its server. The IRC channel operator is connected to this server. If the server is crashed due to some reason, then the connection of this operator would automatically die and another member from the same channel would automatically be assigned the server status [13 and 14].

- P2P Botnets: One of the main problems that botmasters face when implementing Botnets is losing control on their bots when using IRC protocols. Because the IRC network is a centralized structure, as a result, a Peer-to-Peer (P2P) command and control structure is used. Peer-to-Peer network is defined as a network in which the host in that network can act as a client and a server where there is no centralized point and any node can provide and retrieve information at the same time. Peer-to-Peer command and control structure has many advantages over the centralized structure. One of these advantages is that, it is hard to trace back or track the origin of the botmaster. In addition, if one bot is detected and shutdown, it will not affect other bots [13].
- HTTP Botnets: The most recent Botnet till date is HTTP Botnet. It works by exchanging web requests by using port 80. It sets up its communication with certain URL's using internet with an HTTP message. This HTTP message contains unique identifiers for the bots. The server under consideration will reply to these HTTP messages with further investigation commands (e.g. GET) [16]. In the HTTP-based, the botmaster informs the infected computers from the new list of commands to execute, updating the contents of a web page that bots are to periodically visit, which exposes the communication channel nodes as the access to this web-page is lots of times, and public [13 and14].

9. Botnet Detection Techniques [13]

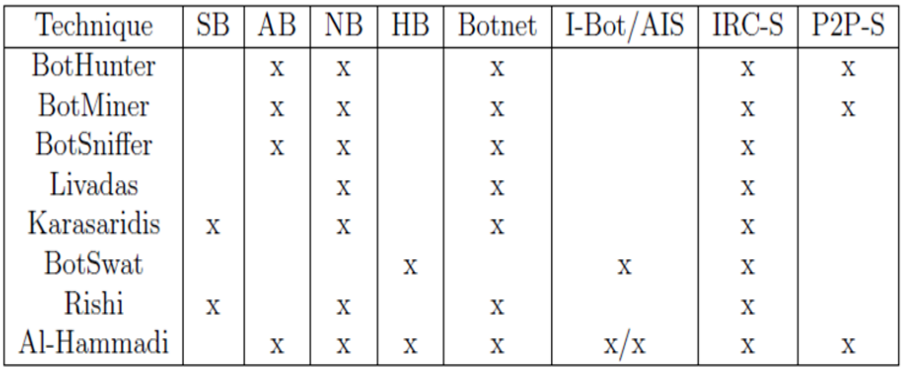
There are many techniques for Botnet detection. The summarized existing techniques and their features are stated below.

1-Botnet Taxonomy
2-Honeypots
3-Signature-based Detection
4-Anomaly Detection
5-Machine Learning

Table 1 summarized some of the existing Botnet/bots techniques and their specifications and features. Where:

- SB: Signature-Based Detection with network statistics
- AB: Anomaly-Based Detection with network statistics
- NB: Network-Based Detection
- HB: Host-Based Detection
- I-Bot: Individual Bot
- IRC-S: IRC Structure
- P2P-S: Peer to Peer Structure
- AIS: Use Artificial Immune System.

Table 1. Summarized some of the existing Botnet/bots techniques and their specifications and features [13].



Technique	SB	AB	NB	HB	Botnet	I-Bot/AIS	IRC-S	P2P-S
BotHunter		x	x		x		x	x
BotMiner		x	x		x		x	x
BotSniffer		x	x		x		x	
Livadas			x		x		x	
Karasaridis	x		x		x		x	
BotSwat				x		x	x	
Rishi	x		x		x		x	
Al-Hammadi		x	x	x	x	x/x	x	x

10. Conclusion and Future Work

Botnet nowadays are one of the most dangerous threats for internet and computer networks, after understanding all Botnet features, Botnet types, and history, in this research, clear view points about Botnet are obtained in order to build a software as future work for detect a new bot which threats facebook called "koobface", and explains all its features and specifications to protect users of computer network and internet.

REFERENCES

[1] Martin T. Biegelman. 2009, "Identity Theft Handbook, Identity Theft Handbook Detection, Prevention, and Security ", John Wiley & Sons, INC.

[2] Guofei Gu, Junjie Zhang, and Wenke Lee. 2008, "BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic", 15th Annual Network &

[3] A. Rajab, J. Zarfoss, F. Monrose, and A. Terzis. 2006, "A multifaceted approach to nderstanding the Botnet phenomenon". In *Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement*, page 52. ACM, 2006.

[4] Xiaonan Zang, Athichart Tangpong, George Kesidis and David J. Miller,2011, "Botnet Detection Through Fine Flow Classification", This material is based upon work supported by the National Science Foundation under Grant No. 0915552 and a Cisco Systems URP gift.

[5] Maryam Feily, Alireza Shahrestani, Sureswaran Ramadass. 2009, "A Survey of Botnet and Botnet Detection", 2009 Third International Conference on Emerging Security Information, Systems and Technologies.

[6] R. A. Rodr´ıguez-G´omez, G. Maci´a-Fern´andez and P. Garc´ıa-Teodoro. 2011, Analysis Of Botnets Through Life-Cycle,SECRYPT 2011-International Conference on Security and Cryptography.

[7] Wilson, C. 2007, "Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress", Technical report, CRS Report for Congress.

[8] Weber, T. 2007, "Criminals ’may overwhelm the web’", Technical report, BBC News.

[9] Eirik Falk Georg Bergande, Jon Fjeldberg Smedsrud, 2011, "Using Honeypots to Analyze Bots and Botnets", Master of Science in Communication Technology, Norwegian University of Science and Technology, Department of Telematics.

[10] Yousof Ali Abdulla Al-Hammadi. 2010, "Behavioural Correlation for Malicious Bot Detection, Thesis submitted to The University of Nottingham, for the degree of Doctor of Philosophy, April 2010.

[11] John R. Vacca. 2010, "Network and System Security", Elsevier Inc.

[12] E. Cooke, F. Jahanian, and D. McPherson. 2005, "The zombie roundup: Understanding, detecting, and disrupting Botnets" . In Proceedings of the USENIX SRUTI Workshop, pages 39–44, 2005.

[13] Laheeb M. Ibrahim, Karam H. Thanoon, 2012, "A survey of Botnet crimeware life cycle", International Journal of Reasoning-based Intelligent systems., "for Intelligent Techniques and Constructive Approaches in Computing and Information Technology" based on CCIT" 2012 prceedings, 4-5 April/ 2012, Iraq, University of Anabr.

[14] Naseem F., shafqat M., et al, 2010, "A Survey of Botnet Technology and Detection", International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS Vol: 10 No: 01.

[15] Michael Bailey, Evan Cooke, Farnam Jahanian, Yunjing Xu, Ann Arbor, Manish Karir. 2009, "A Survey of Botnet Technology and Defenses", CATCH '09 Proceedings of the 2009 Cybersecurity Applications & Technology Conference for Homeland Security, Pages 299-304. IEEE Computer Society Washington, DC, USA, 2009.

[16] Website: Robert F. Erbacher, Adele Cutler, Pranab Banerjee, Jim Marshall, A Multi-Layered Approach to Botnet Detection, http://digital.cs.usu.edu/~erbacher/publications/BotnetArchitecture2.pdf