Bots and botnets: An overview of characteristics, detection and challenges

CONFERENCE PAPER · JANUARY 2012

DOI: 10.1109/ICCSCE.2012.6487169

3 AUTHORS:

Meisam Eslahi
Universiti Teknologi MARA
6 PUBLICATIONS **11** CITATIONS
SEE PROFILE

Rosli Salleh
University of Malaya
60 PUBLICATIONS **164** CITATIONS
SEE PROFILE

Nor Badrul Anuar
University of Malaya
90 PUBLICATIONS **467** CITATIONS
SEE PROFILE

2012 IEEE International Conference on Control System, Computing and Engineering, 23 - 25 Nov. 2012, Penang, Malaysia

Bots and Botnets: An Overview of Characteristics, Detection and Challenges

Meisam Eslahi
Security Research Group (SECReg)
University of Malaya, 50603
Kuala Lumpur, Malaysia.
Email: meisam_eslahi@um.edu.my

Rosli Salleh
Security Research Group (SECReg)
University of Malaya, 50603
Kuala Lumpur, Malaysia.
Email: rosli_salleh@um.edu.my

Nor Badrul Anuar
Security Research Group (SECReg)
University of Malaya, 50603
Kuala Lumpur, Malaysia.
Email: badrul@um.edu.my

Abstract—**Recently, botnets have become the biggest threat to cyber security and have been used as an infrastructure to carry out nearly every type of cyber attack. They have a dynamic and flexible nature and the botmasters, who control them, update the bots and change their codes from day to day to avoid the current detection methods. In this paper, we present an overview of botnets' characteristics along with their malicious activities. We also review the current botnet detection methods in addition to their advantages and disadvantages. Finally we discuss the new generation of botnets on cloud and mobile environments.**

Keywords—Cyber Security; Survey;Botnets; Cloud Botnets; Mobile Botnets.

I. INTRODUCTION

The convenience and speed of digital communications have become an integral part of home computer use, as well as every other aspect of use from education to business and research. While high-speed computer networking and the Internet have brought great convenience, a number of security challenges have also emerged with these technologies. Amongst different computer network security threats like viruses and worms, botnets have become the most dangerous [1,2].

A bot, originating from the term 'robot', is an application that can perform and repeat a particular task faster than a human. When a large number of bots spread to several computers and connect to each other through the Internet, they form a group called a botnet, which is a network of bots. A botnet comes from three main elements - the bots, the command and control (C&C) servers, and the botmasters. A bot is designed to infect targets (e.g. computers or mobiles), and make them a part of a botnet without their owners' knowledge under the control of a person, known as the botmaster. The botmaster sends orders to all the bots on infected targets and controls the entire botnet through the Internet and the C&C servers [3]. The botmasters try to get control of these targets and carry out their malicious activities.

In a review of the different types of malicious activities perpetrated by botnets, it is found that they are not only dangerous threats to computer networks and the Internet, but also used as an infrastructure to carry out other types of threats and attacks (e.g. DDOS) [1]. Therefore, the detection of botnets has become a challenging issue in the field of computer network security. This paper aims to provide an overview on botnets and their characteristics along with current detection methods and challenges. The rest of this paper is organised as follows:

Section II presents the botnet characteristics such as their lifecycle, different types of command and control mechanisms, and a set of attacks and malicious activities posed by them. The existing botnet detection methods are considered in Section III. The new generations of botnets are discussed in Section IV. Section V discusses current challenges along with some suggestions. Finally, Section VI gives the overall conclusion of this paper.

II. CHARACTERISTICS OF BOTNET

A. Botnet Lifecycle and Botmaster Activities

Botnets can come in different sizes or structures but, in general, they go through the same stages in their lifecycle [4,5]. Figure 1 depicts the general view of a botnet lifecycle.

1) Infection and Propagation: The lifecycle of a botnet begins with the infection process where the botmasters use different methods and techniques to infect new targets

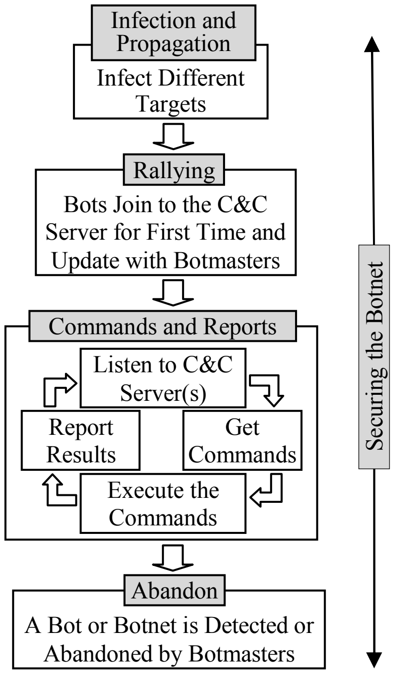
Infection and Propagation
Infect Different Targets
Rallying
Bots Join to the C&C Server for First Time and Update with Botmasters
Commands and Reports
Listen to C&C Server(s)
Report Results
Get Commands
Execute the Commands
Abandon
A Bot or Botnet is Detected or Abandoned by Botmasters
Securing the Botnet

Figure1: A Botnet Lifecycle Schema

(e.g. computers, mobile devices) and convert them into bots [6]. Infected codes attached to spam emails or instant messages, malicious URLs, P2P file sharing networks and even other botnets can be listed as sample of vectors to propagate the bots in target devices [5]. The most common targets of botmasters are less-monitored computers with high-bandwidth connectivity, university servers and home computers. In general, botmasters take advantage of those who have low awareness or lack of knowledge of network security to gain unauthorised access to their devices and keep their bots alive for a long time without being detected [7].

2) Rallying: This refers to the first time that bots connect to the C&C server to show the botmaster that it has already established a zombie, successfully [8]. In addition, the bots receive updates with essential information such as the list of relative C&C server's IP address [9].

3) Commands and Reports: During this stage, the bots listen to the C&C servers or connect to them periodically to get new commands from the botmaster. A new command, when detected by the bots, is treated as an order; they execute the order and the results are reported to the C&C server; the bots then wait for new commands [4,6].

4) Abandon: When a bot is no longer usable (e.g. its bandwidth is too low) or the botmaster decides that the particular bot is no longer suitable, it may be abandoned by the botmaster. In case any single bot is disabled the botnet is still available. A botnet is entirely destroyed when all its bots are detected or abandoned or when the C&C Servers are detected and blocked [4,7].

5) Securing the Botnet: The constant effort to keep the entire botnet secure is one of the important issues in a botnet lifecycle. Botnets and bots have a dynamic and flexible nature. They are continuously being updated and their codes change from day to day. Moreover, botmasters are always trying different techniques to protect their bots from existing detection solutions [10].

B. Command and Control (C&C) Mechanism

The Command and Control mechanism creates an interface between the bots, C&C servers and the botmasters to transmit data among them. It is crucial for botmasters to establish a fool-proof connection between themselves, C&C servers and the infected computers [3]. There are three types of botnet command and control architectures - centralised, decentralised, and Hybrid - based on the way the communication is implemented [6]. Figure 2 illustrates the differences between centralised and decentralised C&C mechanisms.

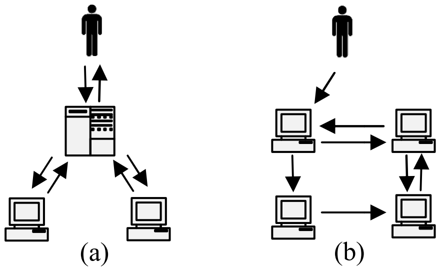

Figure 2: (a) Centralised (b) Decentralised Mechanisms

1) Centralised C&C: In the centralised command and control approach, the zombies or bots are connected to the central C&C server to get commands and updates. Depending on the settings, a C&C server may provide some services to register the available bots and this will make it possible to track their activities. Certainly, a botmaster must be connected to the C&C server to have control of the bots and distribute its commands and tasks [8,11]. However the centralised models come with a single point of failure, they are the most common type of botnets as they use simple steps to create and manage the bots and the response is fast [12]. The centralised C&C mechanism is divided into IRC and HTTP types based on the communication protocols they use to establish their connection.

- IRC-based: IRC or Internet Relay Chat is a system that is used by computer users to communicate online or chat in real-time mode. This method was used in the first generation of bots in which the botmasters used the IRC server and the relevant channels to distribute their commands [13]. Each bot connects to the IRC server and channel that has been selected by a botmaster and waits for commands. In this setup, the botmaster establishes real-time communication with all the connected bots and controls them. The IRC bots follow the *PUSH* approach which means that when an IRC bot connects to a selected channel, it remains in the connect mode [11].
- HTTP-based: The HTTP command and control is a new technique that allows the botmasters to control their bots by using the HTTP protocol [13]. In this technique, the bots use a specific URL or IP address defined by the botmaster, to connect to a specific web server, which plays a C&C server role. Unlike the *PUSH* approach used by the IRC-based bots, the HTTP bots adopt the *PULL* approach. They do not remain in the connect mode after they have established connection to the C&C server for first time. In the *PULL* approach, the botmasters publish the commands on certain web servers and the bots periodically visit those web servers to update themselves or get new commands. This process continues at regular intervals defined by the botmasters [1,14].

2) Decentralised C&C: The decentralised command and control architecture is based on the peer-to-peer (P2P) network model. In this model, an infected computer acts as a bot and as a C&C server at the same time [15]. In fact in P2P botnets, instead of having a central C&C server, each bot acts as a server to transmit the commands to its neighbouring bots. The botmaster sends commands to one or more bots, and the bots that receive the commands deliver them to other bots. This process is repeated by each bot which receives a new command. Unlike the centralised botnets; creating and managing P2P botnets involves complex procedures and requires a high level of expertise [6,14].

3) Hybrid C&C: As discussed above, each C&C mechanism comes with a set of advantages and disadvantages with respect to the ease of use and management and difficulty of detection and abandonment. In order to take the advantages of each C&C

model the different protocols and architectures are used to form a hybrid approach. For instance, HTTP2P botnets [15] communicate with HTTP protocol to evade firewalls over a P2P structure to eliminate the central C&C servers' traditional drawbacks. The hybrid approach is not limited to the use of certain services or architectures; in fact botmasters can use any applicable protocols to implement this model. For example, the AHP2P [16] is an advanced hybrid P2P botnet which use the web2.0 technology to hide its communications into social websites.

C. Botnets Malicious Activities

Botnets range in size from a large botnet having thousands of bots (large-scale botnets) to a small botnet having hundreds or lesser number of bots (small-scale botnets). Regardless of their size, which has a direct link to their complexity and purpose, botnets are mainly created to carry out malicious activities in computer networks [5]. They are not only a dangerous threat to computer networks and the Internet, but are also involved in other types of threats and attacks [17]. Some examples of these attacks are listed as follows:

1) DDOS: This is the distributed form of denial of service or DOS attack that is carried out by sending a large number of UDP packets, ICMP requests, or TCP sync floods which is aimed at using the resources of particular servers and forcing them to shut down. As botmasters control botnets, they can carry out this type of attack from thousands of different places by sending a particular command to the bots in the infected computers in the same botnet [3,12].

2) Spamming: Spam refers to unsolicited messages, which have the same content but are sent in high volume over different mediums like email, Instant Messenger, comments on blog or news groups [18]. Based on Kaspersky lab report [19] around 85% of spam activities are generated by botnets. Therefore botnets can be considered as the main platform to collecting different email addresses from infected computers and generate and send spam messages. Each bot can send an average of three spam emails or fake messages per second. Thus Koobface botnet [20] with 2.9 million infected computers can generate more than 8 million fake messages per second.

3) Thieving Personal Information: While the theft of personal information has always been considered as one of the most notable Internet threats, Zeus botnet alone infected nearly 3.5 million computers and attempted to steal sensitive information [20]. Botmasters use the botnets to steal information and use them for their own benefit. They can set a trigger to bots and make them scan websites where important information is entered [17]. In addition, other applications such as key-loggers are spread by bots to obtain important information like personal passwords and financial data like online banking [21].

4) Illegal Hosting, Sale or Rent Services: A computer or server with a large storage and a high-bandwidth connection to the Internet can become a target for a botmaster to gain control and use for file sharing and illegal hosting. Botnet programs and hosting services are available for sale or rent for the malicious purposes in any required duration. One of the intentions of these services is to place further barriers and gaps between their customers and law enforcement [18,22].

5) Click Fraud and Adware: One of the main differences between botnets and other Internet threats is that a botnet can be used to make money by click frauding. Botmasters can earn a lot of money by using their bots to click on open websites that pay a small sum of money for each visit to the website or for each click on the advertisement. Pop-up advertisements can also be downloaded, installed or displayed by bots to force a user to visit particular websites [18].

In addition to the attacks discussed above, botnets can be used to spread different types of computer threats in the form of viruses, Trojans, backdoors, worms, etc. This means that botnets are not only a threat, but also a platform for the distribution of other malwares.

III. Botnet Detection

There are several methods and techniques that have been used to track botnet activities and detect them such as signature-based detection, honeypots, analysing the DNS traffic and behavioural analysis (e.g. active and passive) as follows:

A. Detection by Signature

Signature refers to the known patterns or characteristics of threats from intruders into computer systems. By analysing and comparing these patterns or characteristics, it is possible to distinguish the malicious activities from the normal ones. A few studies proposed the signature-based botnet detection method [23,24]. However, detection by signature is rarely used for botnet detection because this method cannot identify new behaviour, patterns or characteristics. This method is based on a simple comparison of collected information with the predefined characteristics of existing bots. Thus, this method is good for detecting well-known bots, but less significant for detecting new and zero-day bots [3].

B. Honeypot and Honeynet

Honeypots are tools that are used as traps to collect the bots' information and activities and analyses them in order to detect botnets. The information can be used to understand more about bots' behaviour or the intentions of the botmasters [25]. There are two types of Honeypots: low-interaction honeypots and high-interaction honeypots [26]. The main difference between them is the level of access rights to system resources, services, and functions [27]. Low-interaction honeypots are deployed with a limited interaction between computers and botmasters. Therefore they may not be completely compromised and the collected information may not be sufficient for analysis to detect botnets. In order to provide more information, the high-interaction honeypots emulate the real system and services which allow botmasters to have more control. Although this approach is able to provide useful information for botnet detection, the botmasters can gain full control of the computers in which the high-interaction honeypot is installed. Moreover recently, botmasters use many techniques to detect and avoid the honeypots [25,28].

C. Detection by DNS Traffic Monitoring

The use of honeypots provides useful botnet traffic but it provides less information about DNS query. Monitoring and analyzing the DNS traffic generated by bots and their differences with normal DNS queries has been used as a technique to detect botnets [9]. These methods are no longer effective as the new generation of botnets have been designed to generate a minimum number of DNS queries. Moreover, the process of analysing DNS traffic is very complex [1,10]. Finally, the DNS analysing technique is unable to provide information on botnet propagation and the way they infect the targets [6].

D. Behavioural Analysis Detection

In order to provide an effective approach to analyse and detect botnets, a behavioural analysis is proposed by some studies. This method looks out for abnormal patterns in network traffic and not at the content of the information being transmitted [29]. One of the main advantages of this technique is the ability to detect unknown botnet threats [30]. The behavioural analysis comes in different forms as follows:

1) Attack Behaviour Analysis: In this method, the characteristics and behaviour of attacks are examined more than other issues such as the bots' behaviour [6]. The main disadvantage of this method lies in the fact that it is only applicable after a botnet is already propagated, established and the attack is started. Moreover, this method adopted an active behaviour analysis which interferes with the normal communication which makes it possible for the botmaster to be aware about the observation and detection process [28].

2) Operational Behaviour Analysis: Unlike the method mentioned above, operational behaviour analysis focuses on bots' characteristics, C&C servers and communication methods, botmaster behaviour and intentions. Therefore, a number of studies on botnet detection have adopted behavioural analysis by collecting the network traffic for a specific period (i.e. passive approach) and analyse them in order to identify any evidence of bot and botnet activities [6].

IV. New Generation of Botnets

Botnets have been operating on traditional network infrastructures and their most common targets are computers and computer networks, but they have always been evolved by their high technical botmasters to keep pace with new technologies. Recently, a new generation of botnets is moving to new infrastructures as follows:

A. Cloud Botnets

Botmasters realize that instead of spending a long time infecting different targets, they can rent a cloud service (e.g. by stolen credit cards) to build their botnet over cloud. Along high computational capabilities of clouds, they can be built in minutes and unlike the normal infected computers they are always ready to use. Moreover, while the bots on infected computers have to prevent unusual or suspicious use of the computer resources, which expose their presence, the resources of infected clouds can be fully employed by botmasters [31].

B. Mobile Botnets

With the immense use of mobile devices and the Internet, botnets migrate to mobile infrastructures. Accordingly the new generations of C&C models are designed based on mobile technologies such as SMS/MMS and Bluetooth [17]. Nowadays, mobile devices and more particularly Smartphones are well emerged with the Internet and become efficient enough to provide environments which attract botmasters [8]. Moreover, mobile devices are not well protected compared to computer and computer networks and their users pay less attention to security updates [12]. Although there has been only anticipation of the existence of botnets in mobile devices, the first official report on mobile botnets has been released by Damballa technology research lab [32]. Based on this report, 40,000 infected mobile devices have been communicating through cyber criminal command and control servers for the first six months of 2011.

V. Current Challenges and suggestions

This section discusses the current botnet detection challenges that need to be addressed. It also highlights the main issues along with a number of suggestions for future studies.

A. General Botnet Detection Challenges

Botnets have several characteristics (e.g. developed by skillful developers, dynamic nature, and high flexibility) that make them difficult to analyse and detect. They are distributed very fast and the botmasters are always trying different techniques to protect their bots from existing detection solutions [10].

1) Changing Techniques and Environments: As noted by MacAfee research lab, in nearly every detection algorithms the success has been short-lived because the botmasters keep changing their techniques and operational environments. In addition, the McAfee research labs predicted that the cyber community will face more widely-distributed and more resilient botnets, which are difficult to detect [33].

Suggestion: To be well prepared for future botnet attacks, the researchers should keep studying advanced techniques and infrastructures (e.g. cloud and mobile) that could be used by botmasters. Therefore, the research on botnet detection and especially in new generations is an open area for more research.

2) Small-Scale and Single Bot Detection: As noted by Bailey *et al.* [6], a wide range of current botnet detection methods are designed based on analysing the cooperative behaviours posed by bots from the same botnet. These techniques are more effective in large-scale botnet detection where there are high numbers of bots (i.e. infected targets) in a botnet, hence, the detection of small-scale botnets and single bots can still considered as a challenge [11].

Suggestion: Early detection of botnet activities is an important issue because its further propagation and damages can be responded and prevented [34]. Therefore, detection of single bots and botnets with a small number of members is required to be addressed to detect and prevent a botnet in the early days of its lifecycle.

3) Botnet Response, Prevention and Mitigation: To the best of our knowledge, the current studies on botnets are mostly discussed on detection only. Therefore, response, prevention and mitigation are open fields for further studies.

Suggestion: More studies on botnet infection and propagation systems are needed to design prevention and mitigation approaches. In addition any other methods like detection of single bots can help to detect them in the early stages and respond to them fast.

B. HTTP-based Botnet Detection Challenges

Botmasters use HTTP protocol to hide their activities among the normal web flows and easily avoid current detection methods like firewalls. Because of the wide range of HTTP services used, unlike the IRC and P2P, it is not easy to block this service [13]. Moreover, this service is commonly used by normal applications and services in the Internet, thus, detection of the HTTP botnets with low rate of false alarms (e.g. false negative and false positive) has become a notable challenge [3].

1) Rate of False Alarms: A number of current detection methods are designed based on the fact that HTTP bots periodically connect to a particular command and control server to get commands and updates (i.e. PULL style) [11,13]. As observed in [1,14] some normal applications and services such as Gmail session (which periodically checks for new emails), auto updaters, HTTP based download managers, self-refresh pages and some browsers' toolbars can generate the same periodic pattern and increase false positive rates in the detection results.

Suggestion: Further studies must be conducted to design and propose new filter algorithms to reduce the amount of traffic (during the analysis process) by removing unwanted and useless data. Besides this, new classification algorithms are needed to distinguish normal web flows from bot generated flows. The review of the characteristics of different types of botnets shows that HTTP-based botnets have a set of attributes that make it difficult for them to be detected. On the other hand, the number of studies focusing on the detection of HTTP-based botnets is relatively low compared to the number of those on IRC-based and P2P botnets [1]. Therefore, further studies are needed in this area.

C. New Botnets Detection Challenges

Cloud and mobile infrastructures have recently become a new platform for botnet activities. Since, they have not been fully explored yet, further studies are needed to design a proper detection method based on their specific characteristics. However, clouds are dynamically monitored and protected by cloud service providers and botnets are easier to shutdown compared to other types [35]. On the other hand, mobile devices are not properly protected compared to computer and computer networks, and their users pay less attention to the security updates [12].

1) Mobile-Specific Characteristics and Resource Limitations: There are some mobile-specific characteristics that have differentiated mobile security management from that of computers such as mobility, strict personalisation, different types of connectivity, technology convergence, and variety of capabilities [2]. Besides this, the resource limitation of mobile devices like CPU, memory, and battery life make it difficult to implement existing botnet detection solutions discussed in this paper [17].

2) Lack of Central Security Management: In addition to the aforementioned characteristics, the main challenge with mobile security is the lack of central security management as it can track and monitor security threats and update the security policies on mobile devices accordingly [36]. Moreover, as discussed, the current detection methods mostly rely on analysing the similarity in the abnormal or malicious activities generated by the bots of the same botnet. [6]. As a matter of fact, in mobile devices, there is no centralised security management to record and analyse these similarities.

Suggestions: As suggested by Hua *et al.* [37], one possible solution is to design and develop special security managers (e.g. Honey Phones) based on mobile characteristics. However, in this solution and any other host-based model, the mobile limitations should still be considered. Therefore, central security management approach over network infrastructure (e.g. cloud) is proposed [38,39] as it minimises the complexity of computation on the mobile side, in addition to mobile resource consumption. Moreover, from a security point of view, a central management model can record a wide range of information of malicious activities on the same or different infected targets. It provides a rich dataset to enhance the forensics' capabilities and retrospective detection. Finally, different security analysis models and engines can be employed in central management servers in parallel and independent of clients' specifications and characteristics [38].

VI. Conclusion

This paper presents an overview of current state of bots and botnets. Unlike the other types of malwares, botnets are well organised and controlled by skilled botmasters. They employ various strategies to keep their bots safe and hidden as long as possible. Therefore, botnet detection is a big challenge in network security management. There are several methods and techniques that have been used to track botnet activities and detect them. Each of these methods comes with some advantages and disadvantages. In addition, these techniques are designed based on computers and computer networks' specifications and might not be fully applicable for new generations of botnets. Both mobile and cloud botnets have not been fully explored yet and therefore further studies are needed to design proper detection methods based on these environments' characteristics.

ACKNOWLEDGMENT

This work was supported in part by the University of Malaya and the Ministry of Higher Education, Malaysia, under Grant RG086-12ICT and FRGS FP034-2012A.

REFERENCES

[1] L. Jae-Seo, J. HyunCheol, P. Jun-Hyung, K. Minsoo, and N. Bong-Nam, "The Activity Analysis of Malicious HTTP-Based Botnets Using Degree of Periodic Repeatability," in *Proceedings of the International Conference on Security Technology (SECTECH)*, 2008, pp. 83-86.

[2] M. La Polla, F. Martinelli, and D. Sgandurra, "A Survey on Security for Mobile Devices," *IEEE Communications Surveys & Tutorials,* 2012, doi:10.1109/SURV.2012.013012.00028

[3] L. Chao, J. Wei, and Z. Xin, "Botnet: Survey and Case Study," in *Proceedings of the Fourth International Conference on Innovative Computing, Information and Control (ICICIC)*, 2009, pp. 1184-1187.

[4] C. Schiller, J. Binkley, D. Harley, G. Evron, T. Bradley, C. Willems, and M. Cross, *Botnets: The Killer Web Application*, 1st ed. Syngress, 2007.

[5] N. Hachem, Y. Ben Mustapha, G. G. Granadillo, and H. Debar, "Botnets: Lifecycle and Taxonomy," in *Proceedings of the Conference on Network and Information Systems Security (SAR-SSI)*, 2011, pp. 1-8.

[6] M. Bailey, E. Cooke, F. Jahanian, X. Yunjing, and M. Karir, "A Survey of Botnet Technology and Defenses," in *Proceedings of the Cybersecurity Applications & Technology Conference for Homeland Security (CATCH)*, 2009, pp. 299-304.

[7] J. Govil, "Examining the Criminology of Bot Zoo," in *Proceedings of the 6th International Conference on Information, Communications & Signal Processing*, 2007, pp. 1-6.

[8] J. Kok and B. Kurz, "Analysis of the BotNet Ecosystem," in *Proceedings of the 10th Conference of Telecommunication, Media and Internet Techno-Economics (CTTE)*, 2011, pp. 1-10.

[9] H. Choi, H. Lee, and H. Kim, "BotGAD: Detecting Botnets by Capturing Group Activities in Network Traffic," in *Proceedings of the Fourth International ICST Conference*, 2009, pp. 1-8.

[10] J. Dae-il, C. Kang-yu, K. Minsoo, J. Hyun-chul, and N. Bong-Nam, "Evasion Technique and Detection of Malicious Botnet," in *Proceedings of the International Conference for Internet Technology and Secured Transactions (ICITST)*, 2010, pp. 1-5.

[11] G. Gu, R. Perdisci, J. Zhang, and W. Lee, "BotMiner: Clustering Analysis of Network Traffic for Protocol and Structure Independent Botnet Detection," in *Proceedings of the 17th Conference on Security Symposium*, San Jose: USA, 2008, pp. 139-154.

[12] E. Yuce, "A Literature Survey About Recent Botnet Trends," GÉANT Network, ULAKBIM,Turkey, Rep. JRA2 T4, 2012.

[13] K. Tung-Ming, C. Hung-Chang, and W. Guo-Quan, "Construction P2P Firewall HTTP-Botnet Defense Mechanism," in *Proceedings of the IEEE International Conference on Computer Science and Automation Engineering (CSAE)*, 2011, pp. 33-39.

[14] G. Gu, J. Zhang, and W. Lee, "BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic," in *Proceedings of the 15th Annual Network and Distributed System Security Symposium (NDSS)*, 2008.

[15] J. Dae-il, K. Minsoo, J. Hyun-chul, and N. Bong-Nam, "Analysis of HTTP2P Botnet: Case Study Waledac," in *Proceedings of the 9th IEEE International Conference on Communications (MICC)*, Malaysia, 2009, pp. 409-412.

[16] T. T. Lu, H. Y. Liao, and M. F. Chen, "An Advanced Hybrid P2P Botnet 2.0," *World Academy of Science, Engineering and Technology,* vol. 81, pp. 595-597, 2011.

[17] M. Chandramohan and H. Tan, "Detection of Mobile Malware in the Wild," *Computer,* vol. 45, pp. 65-71, 2012.

[18] C. Elliott, "Botnets: To What Extent Are They a Threat to Information Security?," *Information Security Technical Report,* vol. 15, pp. 79-103, 2010.

[19] V. Kamluk. (2009). *The Botnet Ecosystem* [Online]. Available: http://www.securelist.com/en/analysis/204792095/The_botnet_ecosystem

[20] E. Messmer. (2009). *America's 10 Most Wanted Botnets* [Online]. Available: http://www.networkworld.com/news/2009/072209-botnets.html?page=1

[21] B. Stone-Gross, M. Cova, B. Gilbert, R. Kemmerer, C. Kruegel, and G. Vigna, "Analysis of a Botnet Takeover," *Security & Privacy, IEEE,* vol. 9, pp. 64-72, 2011.

[22] Cisco, "Cisco 2009 Midyear Security Report: An Update on Global Security Threats and Trends," Cisco Systems, Rep., 2009.

[23] J. Goebel and T. Holz, "Rishi: Identify Bot Contaminated Hosts by IRC Nickname Evaluation," in *Proceedings of the First Conference on Hot Topics in Understanding Botnets*, 2007, pp. 8-20.

[24] J. S. Bhatia, R. K. Sehgal, and S. Kumar, "Honeynet Based Botnet Detection Using Command Signatures," *Advances in Wireless, Mobile Networks and Applications,* vol. 154, pp. 69-78, 2011.

[25] P. Wang, L. Wu, R. Cunningham, and C. Zou, "Honeypot Detection in Advanced Botnet Attacks," *International Journal of Information and Computer Security,* vol. 4, pp. 30-51, 2010.

[26] W. Zanoramy, A. Zakaria, and M. L. M. Kiah, "A Review on Artificial Intelligence Techniques for Developing Intelligent Honeypot," in *Proceedings of the 3rd International Conference on Next Generation Information Technology (ICNIT)*, Seoul: Korea, 2012, pp. 696-701.

[27] N. Provos and T. Holz, *Virtual Honeypots: From Botnet Tracking to Intrusion Detection*, 1st ed. Addison Wesley Professional, 2007.

[28] A. K. Seewald and W. N. Gansterer, "On the Detection and Identification of Botnets," *Computers & Security,* vol. 29, pp. 45-58, 2010.

[29] M. Rehak, M. Pechoucek, M. Grill, J. Stiborek, K. Bartos, and P. Celeda, "Adaptive Multiagent System for Network Traffic Monitoring," *IEEE Intelligent Systems,* vol. 24, pp. 16-25, 2009.

[30] A. Caglayan, M. Toothaker, D. Drapeau, D. Burke, and G. Eaton, "Behavioral Analysis of Botnets for Threat Intelligence," *Information Systems and E-Business Management,* 2011, doi:10.1007/s10257-011-0171-7.

[31] K. P. Clark, M. Warnier, and F. M. T. Brazier, "BOTCLOUDS -The Future of Cloud-based Botnets?," in *Proceedings of the 1st International Conference on Cloud Computing and Services Science (CLOSER)*, 2011, pp. 597-603.

[32] Damballa, "First Half 2011 Advanced Threat Report," Damballa Lab, Rep., 2011.

[33] MacAfee, "Threat Predictions 2011," McAfee Lab, Rep., 2011.

[34] R. S. Abdullah, M. Z. Mas'ud, M. F. Abdollah, S. Sahib, and R. Yusof, "Recognizing P2P Botnets Characteristic Through TCP Distinctive Behaviour," International Journal of Computer Science and Information Security, vol. 9, pp. 7-11, 2011.

[35] Y. Chen, V. Paxson, and R. H. Katz. (2010). *What's New About Cloud Computing Security?* [PDF]. Available: http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.pdf

[36] A. Flo and A. Josang, "Consequences of Botnets Spreading to Mobile Devices," in *Proceedings of the 14th Nordic Conference on Secure IT Systems (NordSec)*, 2009, pp. 37-43.

[37] J. Hua and K. Sakurai, "A SMS-based Mobile Botnet Using Flooding Algorithm," in *Proceedings of the 5th International Conference on Information Security Theory and Practice*, Greece, 2011, pp. 264-279.

[38] J. Oberheide, E. Cooke, and F. Jahanian, "CloudAV: N-version Antivirus in the Network Cloud," in *Proceedings of the 17th Conference on Security Symposium*, San Jose:CA, 2008, pp. 91-106.

[39] G. Portokalidis, P. Homburg, K. Anagnostakis, and H. Bos, "Paranoid Android: Versatile Protection for Smartphones," in *Proceedings of the 26th Annual Computer Security Applications Conference*, Austin:TX, 2010, pp. 347-356.