2009 Third International Conference on Emerging Security Information, Systems and Technologies

A Survey of Botnet and Botnet Detection

Maryam Feily
National Advanced IPv6 Center of Excellence (NAv6)
IMPACT Research Team
Universiti Sains Malaysia (USM)
Penang, Malaysia
maryam@nav6.org

Alireza Shahrestani
Faculty of Computer Science and Information Technology
University of Malaya (UM), NAv6
IMPACT Research Team
Kuala Lumpur, Malaysia
shahrestani@nav6.org

Sureswaran Ramadass
National Advanced IPv6 Center of Excellence (NAv6)
IMPACT Research Team
Universiti Sains Malaysia (USM)
Penang, Malaysia
sures@nav6.org

Abstract— **Among the various forms of malware, botnets are emerging as the most serious threat against cyber-security as they provide a distributed platform for several illegal activities such as launching distributed denial of service attacks against critical targets, malware dissemination, phishing, and click fraud. The defining characteristic of botnets is the use of command and control channels through which they can be updated and directed. Recently, botnet detection has been an interesting research topic related to cyber-threat and cyber-crime prevention. This paper is a survey of botnet and botnet detection. The survey clarifies botnet phenomenon and discusses botnet detection techniques. This survey classifies botnet detection techniques into four classes: signature-based, anomaly-based, DNS-based, and mining-base. It summarizes botnet detection techniques in each class and provides a brief comparison of botnet detection techniques.**

Keywords: *Botnet; Botnet Detection; Cyber-security;*

I. INTRODUCTION

According to explanation in [1, 2], malicious botnet is a network of compromised computers called "Bots" under the remote control of a human operator called "Botmaster". The term "Bot" is derived from the word "Robot"; and similar to robots, bots are designed to perform some predefined functions in automated way. In other words, the individual bots are software programs that run on a host computer allowing the botmaster to control host actions remotely [1, 2].

Botnets pose a significant and growing threat against cyber-security as they provide a distributed platform for many cyber-crimes such as Distributed Denial of Service (DDoS) attacks against critical targets, malware dissemination, phishing, and click fraud[3,4]. 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.

In this survey, botnet phenomenon will be clarified and advances in botnet detection techniques will be discussed. This survey classifies botnet detection approaches into four classes: signature-based, anomaly-based, DNS-based, and mining-based. Furthermore, it summarizes botnet detection techniques in each class and provides a brief comparison of these techniques. The remainder of the paper is organized as follows: Section II describes botnet phenomenon. In this section, botnet characteristics and botnet life-cycle are explained to provide better understanding of botnet technology. Section III discusses botnet detection and tracking. In this section four classes of botnet detection approaches including signature-based, anomaly-based, DNS-based, and mining-based are discussed respectively. Section IV provides a brief comparison of botnet detection techniques. The survey concludes in Section V.

II. 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, e-bussiness extortion, performing click fraud, and identity theft [3,4].

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 [2, 5]. This characteristic makes botnet an attractive tool for cyber-criminals, and in fact poses a great threat against cyber-security. In order to provide better understanding of botnet phenomenon, botnet characteristics and botnet life-cycle will be explained respectively.

978-0-7695-3668-2/09 $25.00 © 2009 IEEE
DOI 10.1109/SECURWARE.2009.48

IEEE computer society

A. 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 [4,6,7].According to measurement studies in [2] 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 [2, 4, 5, 6, 7].

According to their command and control architecture, botnets can be classified as IRC-based, HTTP-based, DNS-based or Peer to Peer (P2P) botnets [8]. P2P botnets use the recent P2P protocol to avoid single point of failure. Moreover, P2P botnets are harder to locate, shutdown, monitor, and hijack [9, 10]. However, according to the analysis in [2] the most prevalent botnets are based on Internet Relay Chat (IRC) protocol [11] 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 [2, 12].

B. Botnet Life-cycle

A typical botnet can be created and maintained in five phases including: initial infection, secondary injection, connection, malicious command and control, update and maintenance. This life-cycle is depicted in Fig. 1.

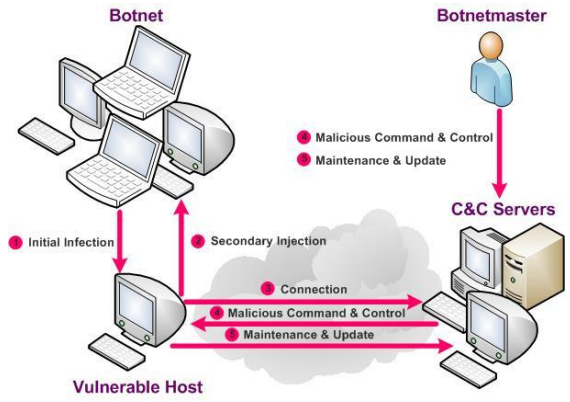

Figure. 1. A Typical Botnet Life-cycle

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. The bot application starts automatically each time the zombie is rebooted [2, 8, 13].

In connection phase, the bot program establishes a command and control (C&C) channel, and connects the zombie to the command and control (C&C) server. Upon the establishment of C&C channel, the zombie becomes a part of attacker's botnet army. After connection phase, the actual botnet command and control activities will be started. The botmaster uses the C&C channel to disseminate commands to his bot army. Bot programs receive and execute commands sent by botmaster. The C&C channel enables the botmaster to remotely control the action of large number of bots to conduct various illicit activities [8, 13].

Last phase is to maintain bots lively and updated. In this phase, bots are commanded to download an updated binary. Bot controllers may need to update their botnets for several reasons. For instance, they may need to update the bot binary to evade detection techniques, or they may intend to add new functionality to their bot army. Moreover, 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 [2, 8, 14, 15]. Botmasters try to keep their botnets invisible and portable by using Dynamic DNS (DDNS) [16] which is a resolution service that facilitates frequent updates and changes in server locations. In case authorities disrupt a C&C server at a certain IP address, the botmaster can easily set up another C&C server instance with the same name at a different IP address. IP address changes in C&C servers propagate almost immediately to bots due short time-to-live (TTL) values for the domain names set by DDNS providers. Consequently, bots will migrate to the new C&C server location and will stay alive [14, 15, 17].

III. BOTNET DETECTION

Despite the long presence of malicious botnets, only few formal studies have examined the botnet problem. To date, just very little is known about botnet malicious behavior. The Honeynet project [4] was one of the pioneering informal studies of the botnet problem. However, efforts are in progress to quantify the botnet problem, detect the presence of botnets, and design defenses against attacks by botnets.

Botnet detection and tracking has been a major research topic in recent years. Different solutions have been proposed in academia. There are mainly two approaches for botnt detection and tracking [8]. One approach is based on setting up honeynets. For instance, solutions in [4, 18] have been initial honeynet-based solutions. In addition, many papers [2, 6, 7, 13, 19, 20, 21, 22, 23] discussed how to use honeynets for botnet tracking and measurement. However, honeynets are

mostly useful to understand botnet technology and characteristics, but do not necessarily detect bot infection.

The other approach for botnet detection is based on passive network traffic monitoring and analysis. Botnet detection techniques based on passive traffic monitoring have been useful to identify the existence of botnets. These techniques can be classified as being signature-based, anomaly-based, DNS-based, and mining-based that will be described and summarized in this section respectively.

A. Signature-based Detection

Knowledge of useful signatures and behavior of existing botnets is useful for botnet detection. For example, Snort [24] is an open source intrusion detection system (IDS) that monitors network traffic to find signs of intrusion. Like most IDS systems, Snort is configured with a set of rules or signatures to log traffic which is deemed suspicious [24]. However, signature-based detection techniques can be used for detection of known botnets. Thus, this solution is not useful for unknown bots.

B. Anomaly-based Detection

Anomaly-based detection techniques attempt to detect botnets based on several network traffic anomalies such as high network latency, high volumes of traffic, traffic on unusual ports, and unusual system behavior that could indicate presence of malicious bots in the network [1].

Although anomaly detection techniques solve the problem of detecting unknown botnets, problems with anomaly detection can include detection of an IRC network that may be a botnet but has not been used yet for attacks, hence there are no anomalies. To solve this, Binkley and Singh [25] proposed an effective algorithm that combines TCP-based anomaly detection with IRC tokenization and IRC message statistics to create a system that can clearly detect client botnets. This algorithm can also reveal bot servers [25]. However, Binkley's approach could be easily defeated by simply using a trivial cipher to encode the IRC commands.

In 2007, Karasaridis *et al.* [12] presented an algorithm for detection and characterization of botnets using passive analysis based on flow data in transport layer. This algorithm can detect encrypted botnet communications. It helps to quantify size of botnets, identify and characterize their activities without joining the botnet [12]. Recently, Gu *et al.* have proposed Botsniffer [26] that uses network-based anomaly detection to identify botnet C&C channels in a local area network. Botsniffer is based on observation that bots within the same botnet will likely demonstrate very strong synchronization in their responses and activities. Hence, it employs several correlation analysis algorithms to detect spatial-temporal correlation in network traffic with a very low false positive rate [26].

C. DNS-based Detection

DNS-based detection techniques are based on particular DNS information generated by a botnet. DNS-based detection techniques are similar to anomaly detection techniques as similar anomaly detection algorithms are applied on DNS traffic. As mentioned in Section II, bots typically initiate connection with C&C server to get commands. In order to access the C&C server bots perform DNS queries to locate the respective C&C server that is typically hosted by a DDNS provider. Thus, it is possible to detect botnet DNS traffic by DNS monitoring and detect DNS traffic anomalies [15, 17].

In 2005, Dagon [27] proposed a mechanism to identify botnet C&C servers by detecting domain names with abnormally high or temporally concentrated DDNS query rates. This technique is similar to the approach proposed by Kristoff [28] in 2004. However, both techniques have the same weakness and could easily be evaded by using faked DNS queries. Furthermore, according to the evaluation in [17], this technique generates many false positives due to misclassification of legitimate and popular domains that use DNS with short time-to-live (TTL).

An alternative approach was proposed by Schonewille and Van Helmond [29] in 2006. This approach was based on abnormally recurring NXDOMAIN reply rates. In order to classify anomalous reply rates, they use the algorithms similar to those Dagon used for classifying analogous query rates. According to their observation DDNS responses indicating name error (NXDOMAIN) often correspond to botnet C&C servers that have been shut down by authorities. Hosts that repeatedly issue such queries may be infected with a bot and they may have the vulnerability to enable similar infection. According to [17], this approach is very effective to detect several suspicious domain names and there may be less false positive because NXDOMAIN replies are more likely to refer to DDNS than to other names. Ramachandran *et al.* [30] proposed a set of techniques and heuristics to identify botnets using passive analysis of DNS-based Black-hole List (DNSBL) lookup traffic. This technique addresses the possibility of performing counter-intelligence that help us to detect DNSBL reconnaissance activity, whereby botmasters themselves must perform lookups against the DNSBL to determine their bots' blacklist status. The goal in developing these models and heuristics is to distinguish DNSBL queries issued by botmasters from legitimate DNSBL traffic to identify likely bots. These heuristics could be used to detect reconnaissance activities in real-time and allows for active countermeasures. As botmasters usually perform reconnaissance lookups prior to the use of bots in an attack, this DNSBL counter-intelligence can be used for early warning to boost responses. Moreover, this detection technique does not require direct communication with any component of the botnet, and does not disrupt the botnet's activity. They have presented the first study that uses direct analysis of DNSBL logs to infer other types of network behaviour. However, this technique runs the risk of false positives due to active countermeasures such as reconnaissance poisoning. In addition, this approach cannot detect distributed reconnaissance.

In 2007, Choi *et al.* [15] proposed an anomaly-based botnet detection mechanism by monitoring group activities in DNS traffic, which form a group activity in DNS queries simultaneously sent by distributed bots. They have defined unique features of DNS traffic as group activity to distinguish botnet DNS queries from legitimate DNS queries. Since DNS

traffic appears in several stages of botnet life-cycle, it is possible to detect botnet by using the group activity property of botnet DNS traffic. They also developed a mechanism that enables to detect C&C server migration. This anomaly-based botnet detection mechanism is more robust than the previous approaches and can detect botnet regardless of the type of bot and botnet by looking at their group activities in DNS traffic. Furthermore, it can detect botnets with encrypted channels since it uses the information of IP headers. Nevertheless, the main drawback of this approach is the high processing time required for monitoring huge scale of network.

Other proposals in [22, 23] are also based on DNS monitoring. However, they are mostly useful for botnet tracking and measurement to understand botnet technology and characteristics, but do not necessarily detect bot infection.

D. *Mining-based Detection*

One effective technique for botnet detection is to identify botnet C&C traffic. However, botnet C&C traffic is difficult to detect. In fact, since botnets utilize normal protocols for C&C communications, the traffic is similar to normal traffic. Moreover, the C&C traffic is not high volume and does not cause high network latency. Therefore, anomaly-based techniques are not useful to identify botnet C&C traffic. Several data mining techniques including machine learning, classification, and clustering can be used efficiently to detect botnet C&C traffic.

Geobl and Holz [31] proposed Rishi in 2007. Rishi is mainly based on passive traffic monitoring for unusual or suspicious IRC nicknames, IRC servers, and uncommon server ports. They use n-gram analysis and a scoring system to detect bots that use uncommon communication channels, which are commonly not detected by classical intrusion detection systems [31]. However, this approach is quite limited, in that IRC nickname can be changed to resemble normal host. In addition, this method cannot detect encrypted communication as well as non-IRC botnets.

In 2008, Strayer *et al.* [32] proposed a network-based solution using machine learning techniques for detecting botnet traffic. They showed that evidence of botnet command and control activity can be extracted from flow characteristic using passive traffic analysis. They adopt a two stage process which first distinguish IRC flows, and then identify botnet C&C traffic from normal IRC flows [32]. Although these techniques are effective to detect some botnets, they are specific to IRC-based botnets. Moreover, for accurate analysis and detection these techniques require access to payload content. Thus, it cannot detect encrypted C&C traffic.

Masud *et al.* [33] proposed robust and effective flow-based botnet traffic detection by mining multiple log files. They introduce multiple log correlation for C&C traffic detection. They classify an entire flow to identify botnet C&C traffic. This method does not impose any restriction on the botnet communication protocol and is therefore applicable to non-IRC botnets. Furthermore, this method does not require access to payload content. Hence, it is effective even if the C&C payload is encrypted or is not available [33].

Botminer [34] is the most recent approach which applies data mining techniques for botnet C&C traffic detection. Botminer is an improvement of Botsniffer [26]. It clusters similar communication traffic and similar malicious traffic. Then, it performs cross cluster correlation to identify the hosts that share both similar communication patterns and similar malicious activity patterns. Botminer is an advanced botnet detection tool which is independent of botnet protocol and structure. Botminer can detect real-world botnets including IRC-based, HTTP-based, and P2P botnets with a very low false positive rate [34].

IV. COMPARISON OF BOTNET DETECTION TECHNIQUES

This section provides a brief comparison of botnet detection techniques. We have compared botnet detection approaches based on key features including: ability to detect unknown bots, capability of botnet detection regardless of botnet protocol and structure, and botnets with encrypted C&C channels, real-time detection, and accuracy. This comparison is summarized in Table 1.

As Shown in this table, signature-based techniques can only detect known botnets, whereas the other classes are able to detect unknown bots. However, there are few botnet

TABLE 1. COMPARISON OF BOTNET DETECTION TECHNIQUES

	Detection Approach	*Unknown Bot Detection*	*Protocol& Structure Independent*	*Encrypted Bot Detection*	*Real-time Detection*	*Low False Positive*
Signature-based	**[24]**	×	×	×	×	×
Anomaly-based	**[25]**	√	×	×	×	×
	[12]	√	×	√	×	√
	[26]	√	×	√	×	√
DNS-based	**[27]**	√	×	√	×	×
	[28]	√	×	√	×	×
	[29]	√	×	√	×	√
	[30]	√	×	√	√	×
	[15]	√	√	√	×	√
Mining-based	**[31]**	√	×	×	×	×
	[32]	√	×	×	×	×
	[33]	√	√	√	×	√
	[34]	√	√	√	×	√

detection techniques [15, 33, 34] that can detect botnet regardless of botnet protocol and structure. These techniques will be effective even though botmasters change their C&C communication protocol and structure. On the other hand, detection techniques that require access to C&C payloads [24, 25, 31, 32] are less effective as botmasters tend to use encrypted channels for C&C communications. Among all detection techniques, the only approach that allows real-time detection is a DNS-based detection which uses DNSBL counter-intelligence to detect reconnaissance in real-time. However, active countermeasures run the risk of false positives. The most recent botnet detection techniques [33, 34] based on data mining as well as DNS-based botnet detection approach in [15] provide promising tradeoff. These methods are independent of botnet protocol and structure. Moreover, they are effective to detect encrypted C&C botnet communication. In overall, these techniques can detect real-world botnets regardless of botnet protocol and structure with a very low false positive rate.

V. CONCLUSION

Botnets pose a significant and growing threat against cyber-security as they provide a key platform for many cyber-crimes such as Distributed Denial of Service (DDoS) attacks against critical targets, malware dissemination, phishing, and click fraud. Despite the long presence of malicious botnets, only few formal studies have examined the botnet problem and botnet research is still in its infancy. This paper surveys botnet and botnet detection.

As mentioned in this paper, 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. Diversity of botnets protocols and structures makes botnet detection a very challenging task. In this survey botnet detection techniques based on passive network traffic monitoring are classified into four classes including signature-based, anomaly-based, DNS-based, and mining-base. Signature-based techniques can only detect known botnets, whereas the other classes are able to detect unknown bots.

However, most of the current botnet detection techniques work only on specific botnet C&C communication protocols and structures. Consequently, as botnets change their C&C communication architecture, these methods will be ineffective. According to our comparison, the most recent botnet detection techniques [33, 34] based on data mining as well as DNS-based botnet detection approach in [15] can detect real-world botnets regardless of botnet protocol and structure with a very low false positive rate. Hence, developing techniques based on data mining and DNS traffic for botnet C&C traffic detection has been the most promising approach to combat botnet threat against online ecosystems and computer assets.

REFERENCES

[1] B. Saha and A, Gairola, "Botnet: An overview," *CERT-In White PaperCIWP-2005-05*, 2005.

[2] M. Rajab, J. Zarfoss, F. Monrose, and A. Terzis, "A multifaceted approach to understanding the botnet phenomenon," in *Proc. 6th ACM SIGCOMM Conference on Internet Measurement (IMC'06)*, 2006, pp. 41–52.

[3] N. Ianelli, A. Hackworth, "Botnets as a vehicle for online crime," *CERT Request for Comments (RFC) 170*0, December 2005.

[4] Honeynet Project and Research Alliance. Know your enemy: Tracking Botnets, March 2005. See http://www. honeynet.org/papers/bots/.

[5] G. Schaffer, "Worms and Viruses and Botnets, Oh My! : Rational Responses to Emerging Internet Threats", *IEEE Security & Privacy*, 2006.

[6] E. Cooke, F. Jahanian, and D. McPherson, "The zombie roundup: Understanding, detecting, and disrupting botnets," in *Proc. Steps to Reducing Unwanted Traffic on the Internet Workshop (SRUTI'05)*, 2005, pp. 39-44.

[7] A. Ramachandran and N. Feamster, "Understanding the network-level behavior of spammers," in *Proc. ACM SIGCOMM*, 2006.

[8] Z. Zhu, G. Lu, Y. Chen, Z. J. Fu, P.Roberts, K. Han, "Botnet Research Survey," in *Proc. 32nd Annual IEEE International Conference on Computer Software and Applications (COMPSAC '08),* 2008, pp.967-972.

[9] J. B. Grizzard, V. Sharma, C. Nunnery, B. B. Kang, and D. Dagon, "Peer-to-peer botnets: Overview and case study," in *Proc. 1st Workshop on Hot Topics in understanding Botnets*, 2007.

[10] P. Wang, S. Sparks, and C. C. Zou, "An advanced hybrid peer-to-peer botnet," in *Proc. 1st Workshop on Hot Topics in understanding Botnets*, 2007.

[11] C. Kalt, "Internet Relay Chat: Client Protocol," *Request for Comments (RFC) 2812 (Informational),* April 2000.

[12] A. Karasaridis, B. Rexroad, and D. Hoeflin, "Wide-scale botnet detection and characterization," in *Proc. 1st Workshop on Hot Topics in Understanding Botnets*, 2007.

[13] K. K. R. Choo, "Zombies and Botnets," Trends and issues in crime and criminal justice, no. 333, Australian Institute of Criminology, Canberra, March 2007.

[14] D. Dagon, G. Gu , C.P. Lee, W. Lee, "A Taxonomy of Botnet Structures," in *Proc. 23rd Annual Computer Security Applications Conference (ACSAC 2007)*, 2007, pp. 325-339.

[15] H. Choi, H. Lee, H. Lee, and H. Kim, "Botnet Detection by Monitoring Group Activities in DNS Traffic," in *Proc. 7th IEEE International Conference on Computer and Information Technology (CIT 2007),* 2007, pp.715-720.

[16] P. Vixie, S. Thomson, Y. Rekhter, and J. Bound, "Dynamic updates in the domain name system(dns update)," 1997. http://www.faqs.org/rfcs/rfc2136.html/.

[17] R.Villamarin-Salomon and J.C. Brustoloni, "Identifying Botnets Using Anomaly Detection Techniques Applied to DNS Traffic," in *Proc. 5th IEEE Consumer Communications and Networking Conference (CCNC 2008)*, 2008, pp. 476-481.

[18] N. Provos, "A virtual honeypot framework," in *Proc. 13th USENIX Security Symposium*, 2004, pp. 1–14.

[19] M. Vrable, J. Ma, J. Chen, D. Moore, E.Vandekieft, A. C. Snoeren, G. M. Voelker, and S.Savage," Scalability, Fidelity and Containment in the Potemkin Virtual Honeyfarm," in *Proc. ACM SIGOPS Operating System Review*, vol. 39(5), pp. 148–162, 2005.

[20] F. Freiling, T. Holz, and G. Wicherski, "Botnet tracking: Exploring a root-cause methodology to prevent distributed denial-of-service attacks," in *Proc. 10th European Symposium on Research in Computer Security (ESORICS)*, vol. Lecture Notes in Computer Science 3676, September 2005, pp. 319–335.

[21] P. Barford and V. Yegneswaran, "*An Inside Look at Botnets*," ser. Advances in Information Security, Springer, 2006.

[22] D. Dagon, C. Zou, and W. Lee, "Modeling botnet propagation using time zones," in *Proc. 13th Network and Distributed System Security Symposium (NDSS'06)*, 2006.

[23] J. Oberheide, M. Karir, and Z.M. Mao, "Characterizing Dark DNS Behavior," in *Proc. 4th nternational Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, 2007.

[24] Snort IDS web page. http://www.snort.org, March 2006.

[25] J.R. Binkley and S.Singh, "An algorithm for anomaly-based botnet detection," in *Proc. USENIX Steps to Reducing Unwanted Traffic on the Internet Workshop (SRUTI'06)*, , 2006, pp 43–48.

[26] G. Gu, J. Zhang, and W. Lee, "Botsniffer: Detecting botnet command and control channels in network traffic," in *Proc. 15th Annual Network and distributed System Security Symposium (NDSS'08)*, 2008.

[27] D. Dagon, "Botnet Detection and Response, The Network is the Infection," in *OARC Workshop*, 2005.

[28] J. Kristoff, "Botnets," in *32nd Meeting of the North American Network Operators Group*, 2004.

[29] A. Schonewille and D.J. van Helmond. "The Domain Name Service as an IDS," Master's Project, University of Amsterdam, Netherlands, Feb 2006, http://staff.science.uva.nl/~delaat/snb-2005-2006/p12/report.pdf

[30] N. F. A. Ramachandran and D. Dagon, "Revealing botnet membership using dnsbl counter-intelligence," in *Proc. 2nd Workshop on Steps to Reducing Unwanted Traffic on the Internet (SRUTI '06)*, 2006.

[31] J. Goebel and T. Holz, "Rishi: Identify bot contaminated hosts by irc nickname evaluation," in *Proc. 1st Workshop on Hot Topics in Understanding Botnets*, 2007.

[32] W. Strayer, D. Lapsley, B. Walsh, and C. Livadas, *Botnet Detection Based on Network Behavior*, ser. Advances in Information Security. Springer, 2008, PP. 1-24.

[33] M. M. Masud, T. Al-khateeb, L. Khan, B. Thuraisingham, K. W. Hamlen, " Flow-based identification of botnet traffic by mining multiple log file," in *Proc. International Conference on Distributed Frameworks & Applications (DFMA),* Penang, Malaysia, 2008.

[34] G. Gu, R. Perdisci, J. Zhang, and W. Lee, "Botminer: Clustering analysis of network traffic for protocol- and structure independent botnet detection," *in Proc. 17th USENIX Security Symposium*, 2008.