Revealing the Criterion on Botnet Detection Technique

Raihana Syahirah Abdullah [1], Mohd Faizal Abdollah[2], Zul Azri Muhamad Noh[3], Mohd Zaki Mas'ud[4], Siti Rahayu Selamat[5], Robiah Yusof[6]

**[1] Faculty of Information and Communication Technology
Universiti Teknikal Malaysia Melaka,
Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia**

**[2 3 4 5 6] Faculty of Information and Communication Technology
Universiti Teknikal Malaysia Melaka,
Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia**

Abstract

Botnet have already made a big impact that need much attention as one of the most emergent threats to the Internet security. More worst when the peer-to-peer (P2P) botnets take the inspiration and underlying P2P technology to exchange files making botnets much harder to detect and shut down. It make botnets are the biggest threat to internet stability and security. Hence, Botnet detection and prevention has been an interesting research topic to be highlighted. Various types of techniques have been proposed for detection, prevention and mitigation for Botnet attack. Thus, this paper addresses the current trend of Botnet detection techniques and identifies the significant criteria in each technique. Several existing techniques are analyzing from 45 various researches and the capability criteria of Botnet detection techniques have been reviewed. The comparative analysis of these techniques have been shown on the selected detection criteria including; unknown Botnet detection, protocol and structure independent, low false positive, low cost, low risk, encrypted bot detection, real-world detection, not require prior knowledge and reveal bot servers and C&C migration.

Keywords: *Botnet, P2P Botnet, IDS, Botnet Detection Criterion*

1. Introduction

Nowadays people are heavily dependent on the Internet, however the advancement of the services offered by the Internet had exposed user to various threat. Cyber criminals are now capable of launching sophisticated attack toward the network infrastructure via several globally remote hosts and the purpose of the exploitation is certainly motivated by financial and political objectives. The global Botnet infections as reported by McAfee threats stated overall messaging Botnet growth jumped up sharply from April 2011 to Mac 2012 as depicted in Fig. 1.

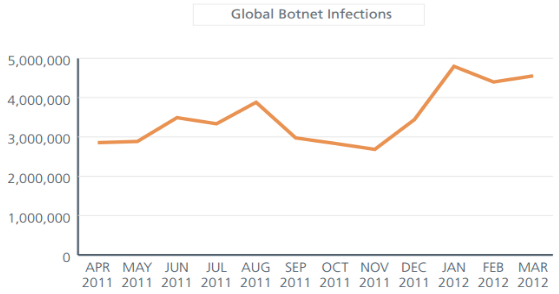

Fig. 1: Global Botnet Infections from McAfee Threat [1]

Meanwhile, according to Malaysian Computer Emergency Response Team (MyCERT) in Quarter 3 2012 they have handled 228 reports related to malicious code activities, this represent 39.02% out of the total number of security incidents [2], statistically illustrated in Fig. 2. Some of the malicious code security incidents handled is active Botnet controllers, hosting of malware or malware configuration files on compromised machines and malware infections to computers.

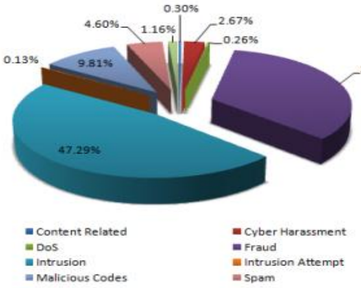

Fig. 2: Percentage of Security Incidents Quarter 3 2012 from eSecurity MyCERT in Malaysia [2]

The rapidly Botnet growth has given the bad impact and requires continuous effort to ensure the Botnet detection techniques is comprehensive enough. Hence, the selected criterion has been proposed as a basic for the success of the Botnet detection. This paper has provides the comparison of Botnet detection based on the criterions including; unknown Botnet detection, protocol and structure independent, low false positive, low cost, low risk, encrypted bot detection, real-time/real-world detection, not require prior knowledge and reveal bot servers and C&C migration. In order to increase the detection rate, the use of these criterion is indispensable.

The rest of paper is organized as follows. Section 2 provides details background on Botnet and selected criterion. Section 3 present the classification of Botnet detection techniques. In this section, five categories of Botnet detection techniques including anomaly-based, signature-based, DNS-based, data mining based, and hybrid-based are discussed respectively. The related work with comprehensive comparison in each detection criteria of Botnet detection technique are presented in Section 4. Finally, Section 5 concludes and discusses further directions of this work.

2. Background

In order to construct further discussion and details, it is necessarily to know some key terms about Botnet. Also, it is important to realize the cause and effect of Botnet in the real world situation. This section discuss the key terms about Botnet and P2P Botnet to compose a better understanding about it.

2.1 Botnet

Nowadays, the most serious manifestation of advanced malware is Botnet [3]. Botnet are very real and quickly evolving problem that is still not well understood or studied. Botnet is a collection of computer that has been infected by malicious software and become bots, drones, or zombies, which have been assimilated into a greater collective through a centralized command and control (C&C) infrastructure [4]. The C&C controlling the bots are mostly malicious in nature and can be illegally controls the computing resources. Botnet had exploit and recruit computer to become army for cyber attack and it can be used for spamming, fake websites, DDoS attacks, viruses, worms, backdoors, information harvesting phishing and scams [4]. The malicious behaviours of Botnet create widespread security analysis and safety issues that propagating cyber crime.

According to SearchSecurity.com website, a report from Russian-based Kaspersky Labs, Botnet currently pose the biggest threat to the Internet and support by a report from Symantec came to a similar conclusion [5, 6]. In addition, a report on the emerging cyber threat 2011 presented at the Georgia Tech Information Security Center (GTISC) Security Summit 2010 has also listed Botnet as one of the emerging threat in the year 2011 [7]. Among of the cases had mentioned in the report is the Mariposa Botnet that can steal financial credential where they found that almost 800,000 financial related information was found inside the operator's home computers.

2.2 IRC, HTTP and P2P Botnet

The combination of the Botnet with current technology such as IRC, HTTP and peer to peer (P2P) has made them silently organize their hidden tactic in a benign application. Several researches has been done to detect IRC and HTTP Botnet through network monitoring analysis and most of their activity is easy to annihilate as each of the bot are connecting to a central command and control server. Yet, the P2P is a bit harder to detect as it command and control centre are distributed same as the P2P leeches that share files over the Internet.

P2P Botnet are one of the most recent phenomenon's where Cyber defence needs new Computational Intelligence (CI) techniques because traditional methods of intrusion detection are being foiled by P2P Botnet [8]. P2P Botnet imply that every compromised machine in the swarm acts as a peer for the others. This study use the anomaly detection which differentiate normal network traffic and abnormal network traffic characteristic. However, misuse detection is insufficient for P2P Botnet detection and classification because it requires advance knowledge on specific characteristics of the malicious software in order to create rules that can be used to monitor the characteristics. The operation of the P2P Botnet operation is depicted in Fig. 3.

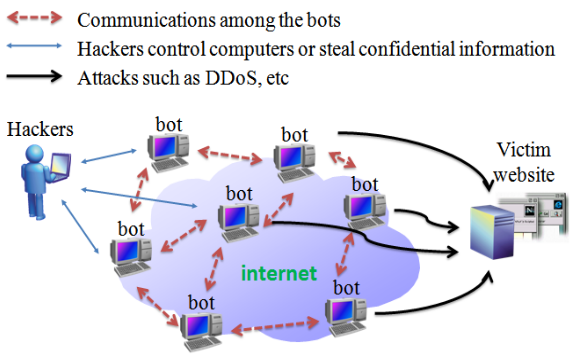
Communications among the bots
Hackers control computers or steal confidential information
Attacks such as DDoS, etc
Hackers
bot
bot
bot
bot
bot
internet
bot
bot
Victim website

Fig. 3: P2P Botnet Operation [9]

3. Classification of Botnet Detection Techniques

Botnet detection technique is the technique used to detect or identify the Botnet activities. The previous research has proposed the different solutions to solve the Botnet attack. Initially, Botnet detection technique mainly divided into two approaches which are honeynet-based and Intrusion Detection System (IDS) based.

The earlier informal studies about the Botnet attack is based on setting up honeynet [10][11][12][13]. Most of researchers setting up honeynet to analyze bots, learn tools, tactics and motives of botmaster [21]. However, honeynet is only good for understanding Botnet characteristic and technology but cannot detect bot infection all the times. This situation make the researchers turned to IDS techniques that more useful to identify the existence of Botnet. In general, Botnet detection in IDS technique can be categorized into anomaly-based, signature-based and hybrid-based detection [3][14][15][16][17][18][19][20][21][59].

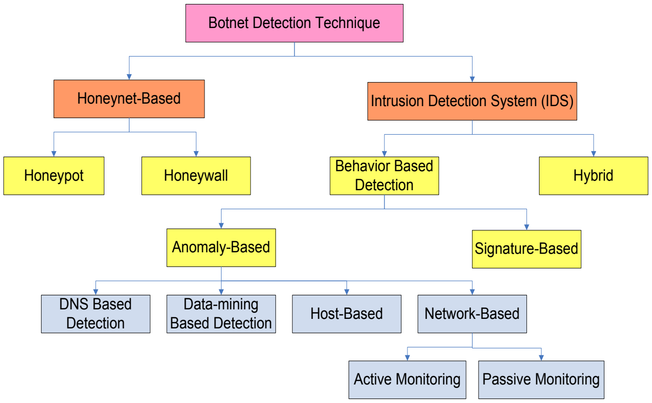

Fig. 4: Botnet Detection Technique

Based on previous worked, the characteristics of each techniques are as follows.

3.1 Anomaly-based Detection

Anomaly-based detection technique is a part of behaviour-based detection. The anomaly-based is divided into DNS-based, data mining-based, host-based and network-based. This techniques attempt to detect Botnet based on several network traffic anomalies such as high network latency, high volumes of traffic, traffic on unusual ports and unusual system behaviour that could indicate presence of malicious bots in the network [3][19][20][22]. Means, it have focuses on normal behaviour to overcome undetected unknown attack. Thus, the anomaly-based technique is capable to detect the unknown Botnet and novel attacks. Unfortunately, it produces a high false positive alarm.

3.1.1 DNS-based

The DNS-based detection technique has been done by doing the DNS monitoring and DNS traffic anomalies. In order to make this technique successful, it demands for the DNS information that generated by a Botnet [15]. Usually, bots send DNS queries to access bot servers. It is helpful as bot used DNS to find the address of botmaster. At once, the carry out of DNS queries will help to locate in particular bot server.

3.1.2 Data Mining-based

The data mining-based detection techniques was proposed to improve the accuracy [21]. It is one effective technique for Botnet detection since it can be used efficiently to detect Botnet C&C traffic by using machine learning, classification and clustering approach.

3.1.3 Host-based

The host-based approach will monitor the network traffic for indications of bot-infected machines [59]. The host become worse when bot had been activated lead the changes on system registry and system files [21]. Then, the Botnet makes a series of systems and library calls.

3.1.4 Network-based

Meanwhile, the network-based approach [21] [59] more focus on monitoring network traffic in; (i) detection of individuals bots by checking for traffic patterns or content that can reveal the command and control (C&C) server or malicious in bot-related activities, and (ii) analyzing the traffic that indicate two or more hosts behave similar patterns as bot to react in the same function. Monitoring in network-based can be done either in active or passive mode.

3.2 Signature-based Detection

Similarly to anomaly-based techniques, signature-based detection technique also as a part of behaviour-based detection. This techniques learn and gain knowledge of useful signatures or behaviours from existing Botnet [15][16]. This solution is useful for detection on known Botnet accurately rather than the unknown bots. In addition, signature-based can make immediate detection and impossibility of false positive. It require less amount of system resource to make the detection.

3.3 Hybrid-based Detection

In hybrid-based detection technique, two or more IDS techniques were combined. It can be the combination of DNS-based with anomaly-based, signature-based with anomaly-based or data mining-based with anomaly-based technique. Due to signature-based, DNS-based and data mining-based that have same capability where it is only able to detect known attack but cannot detect unknown attack. Instead, anomaly-based has this extra capabilities to detect unknown attack compare to other technique. Based on analysis by [14], the combination of IDS technique will complement each other weaknesses.

In summary, the 45 researchers of various Botnet detection techniques have been reviewed. Table 1shows the related literature review in Botnet detection techniques.

Table 1: Related Literature Review in Botnet Detection Techniques

Detection Technique	***Paper Review Reference No.***
Anomaly-based	[20], [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33], [34], [35], [36], [37], [44], [45], [48], [49], [50], [51], [52], [53], [54], [55], [62]
Signature-based	[38], [39], [40], [41], [42], [43], [46]
Hybrid-based	[28], [29], [39], [44], [45], [47], [48], [49], [51], [62]

4. Proposed Criterion for Botnet Detection Techniques

The Botnet detection and prevention have been an interesting research topic to be highlighted. Various type of techniques have been proposed for detection, prevention and mitigation for Botnet attacks. Botnet detection techniques is not an easy task. Technically, the detection of Botnet only can be done when Botnet are communicate in a large scale of network. This section provides a comprehensive comparison of Botnet detection techniques. The comparison has been made regardless to the detection criteria. The comparison is summarized as Table 2 in Appendix-A.

This detection criteria is responsible for the success of the Botnet detection. The specified criterion has made based on the actual goals of significant Botnet detection. The level of detection rate in the botnet detection technique can be measured by these criterions. These criterions can measure how far a technique can be applied and practiced in real situation. These criterions can also help researchers analyze the advantages and limitations of such a technique in distinguishing among other techniques.

Furthermore, these criterion considered as an indicator for effectively and efficiency of the technique. Therefore, this paper utilizes this criterion in differentiating among other techniques. There are some researchers who evaluate the Botnet detection technique using some of this criterion. In line with that, [15] has covered out the five similar criterion from nine criterion as listed below. A list of nine detection criteria as description below:

Table 3: Detection Criteria

Criterion	***Description***
Unknown Botnet Detection	Indicates the detection on new intrusion and novel attack
Protocol and Structure Independent	Indicates the identification of botnet C&C traffic even though botmasters change their C&C communication protocol and structure
Low False Positive	Indicates the value on low rate of false positive alarm
Low Cost	Indicates the exploration in a simple way
Low Risk	Indicates the performing detection in passive mode monitoring
Encrypted Bot Detection	Indicates the detection on encrypted C&C botnet communication
Real-Time/Real-World Detection	Indicates the real situation of network traces detection by turn into active mode
Not Require Prior Knowledge	Indicates that it does not require any Botnet specific information to make the detection
Reveal Bot Servers and C&C Migration	Indicates that it can discover the bot servers respectively

As shown in table 2, most of researchers used the anomaly-based technique to make detection on unknown Botnet [20][23][24][25][26][27][28][29][30][31][32][33][34][35] [36][37][62] while the signature-based techniques can only detect on known Botnet [38][39][40][41][42][43][46]. This indicates that the detection of Botnet attempts to estimate the normal behaviour of system to be protected and the detection of Botnet have been made based on traffic anomalies. Thus, the detection will cover on the current and future Botnet.

Nevertheless, there are some of Botnet detection techniques [26][28][48][51] that can detect Botnet in spite of its protocol and structure independent. These techniques will be effective even though botmasters have changed their C&C communication protocol and structure [15]. Among all detection techniques, only a few of Botnet detection technique [23][48][60] can reveal Botnet servers and C&C migration. Taking down the bot C&C server allows the Botnet attacks can be thwarted directly from its beginning with gain access and shutdown the central component.

On the other hand, most of researchers [23][24][25][27][28][31][34][37][39][40][43][46][48][51][59] produce a very low false positive rate in simple and realistic scenarios. Meanwhile, sometimes a low cost technique [23][26][27][28][29][39][40] can be as effective way although explored in a simple way. The researchers also uses a low risk approach in their detection techniques [23][26][27][28][29][39][40] by performing detection in passive mode monitoring. Consequently, this situations will not allowing detection occurs in real network traces.

In overall, these techniques [24][27][28][44][45][46][47][48][51][59] currently have simply detects encrypted C&C Botnet communication. The encryption will immediately make content signature useless where sequentially make detection analysis at the difficult task. Recently, most of Botnet detection techniques [28][34][35][37][47][50][55][57][58][59] allows real-time or real-world detection. However, the analyses for detection have done in a passive mode before it can really be tested in a real scenario that provides active countermeasures. This is due to active countermeasures run the risk of false positives [15].

Moreover, there are several techniques [20][27][28][36][37][53][55][57] that attempt to distinguish from other similar works by implementing a technique that not need prior knowledge of Botnet detection such as Botnet signature. In the other word, it does not require any Botnet specific information to make the detection. As a result, these technique have choose the anomaly-based and data mining-based as their approaches.

According to the briefly comparison, the only Botnet detection technique in [48] can detect real-world Botnet irrespective of Botnet protocol and structure that reveal the bot C&C server and encrypted Botnet with a very low false positive rate which similar claimed by [15]. However, the developing techniques based on Hybrid-SA, the combination of signature-based with anomaly-based detection technique proposed by [14] has been comprehensive approach to fight against Botnet threat in the real world situation. It is because the combination of this two techniques have complement each other in deal with known and unknown Botnet including detection on encrypted bot, reduce false positive and negative alert, real-world detection and reveal the bot C&C servers.

Signature-based has the ability to immediate detection and impossibility of false positives. But signature-based is only capable to be used for detection of well-known Botnet. More important, very similar bots with slightly different signature may be missed-out to be detected. However, the anomaly-based technique faced with the problem of detecting unknown Botnet through show existence of bots in the network. Anomaly-based technique also has the extra capabilities in terms of reducing false negative alert and detecting multistep attack [14]. Nevertheless, it cannot reduce the false positive alert which can only be reduced by using signature-based technique. Hence, this has given an implication that there are complement each other weaknesses.

5. Conclusions

In this study, the researchers have reviewed and summarized the different approaches for existing Botnet detection techniques. Then, researchers also make the comparison between Botnet detection techniques by detection criteria whereas unknown Botnet detection, protocol and structure independent, low false positive, low cost, low risk, encrypted bot detection, real-time/real-world detection, not require prior knowledge and reveal bot servers and C&C migration. Thus, the comparative analysis towards Botnet detection techniques have been presented by these factors. This research is preliminary worked for Botnet detection. This will contribute ideas in development of a new Botnet detection technique by finding the gap between this existing Botnet detection techniques.

Appendix

Appendix-A as Table 2 below.

Acknowledgments

The authors would like to express the appreciation to Inforslab Group of Universiti Teknikal Malaysia Melaka (UTeM) and MyBrain15 Programme by Ministry of Higher Education Malaysia (MoHE) for their invaluable supports either technically and financing in encouraging the authors to publish this paper.

References

[1] McAfee Threats Report: *First Quarter 2012*, [Online] Retrieved on June 2012 from http://www.mcafee.com/uk/resources/reports/rp-quarterly-threat-q1-2012.pdf

[2] eSecurity Cyber Security Malaysia, *MyCert 3rd Quarter 2012 Summary Report. Volume 32* [Online] Retrieved on January 2013 from http://www.cybersafe.my/pdf/bulletin/vol32-Q312.pdf

[3] Zeidanloo, H.R.; Shooshtari, M.J.Z.; Amoli, P.V.; Safari, M.; Zamani, M.; , "A taxonomy of Botnet detection techniques," *Computer Science and Information Technology*

(ICCSIT), 2010 3rd IEEE International Conference on , vol.2, no., pp.158-162, 9-11 July 2010

[4] Mielke, C.J.; Hsinchun Chen; , "Botnet, and the cybercriminal underground," *Intelligence and Security Informatics, 2008. ISI 2008. IEEE International Conference on* , vol., no., pp.206-211, 17-20 June 2008

[5] Anonymous (2008). *SearchSecurity.com*. [Online] Retrieved on January 2011 from http://searchsecurity.techtarget.com

[6] Westervelt R. (2009). *Conficker Botnet Ready to be Split, Sold SeachSecurity.com* [Online] Retrieved on February 2011 from http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1349282_mem1,00.html

[7] GEORGIA TECH INFORMATION SECURITY CENTER (GTISC). *Emerging Cyber Threat Report 2011*. Security Summit 2011

[8] Estrada, V.C.; Nakao, A.; , "A Survey on the Use of Traffic Traces to Battle Internet Threats," *Knowledge Discovery and Data Mining, 2010. WKDD '10. Third International Conference on* , vol., no., pp.601-604, 9-10 Jan. 2010

[9] Wen-Hwa Liao; Chia-Ching Chang; , "Peer to Peer Botnet Detection Using Data Mining Scheme," *Internet Technology and Applications, 2010 International Conference on* , vol., no., pp.1-4, 20-22 Aug. 2010

[10] Honeynet Project and Research Alliance: Know Your Enemy-Tracking Botnet [Online] Retrieved on June 2012 from http://www.honeynet.org/papers/bots

[11] Baecher, P., Koetter, M., et al.: The Nepenthes Platform: An Efficient Approach to Collect Maiware *Proceedings of International Symposium on Recent Advances in Intrusion Detection (RAID),* 2006.

[12] Freiling, F., Holz, T., and Wicherski, G.,: Botnet Tracking: Exploring a Root-cause Methodology to Prevent Denial of Service Attacks, *Proceedings of 10th European Symposium on Research in Computer Security (ESORICS)*, 2005.

[13] Provos, N.,: A Virtual Honeypot Framework, *Proceeding 13th USENIX Security Symposium*, 2004

[14] Robiah Y, Siti Rahayu S., Mohd Zaki M., Shahrin S., Faizal M. A., Marliza R..: A New Generic Taxonomy on Hybrid Malware Detection Technique. *(IJCSIS) International Journal of Computer Science and Information Security*, Vol. 5, No. 1, 2009

[15] Feily, M., A. Shahrestani, et al.: A Survey of Botnet and Botnet Detection. *Third International Conference on Emerging Security Information, Systems and Technologies (SECURWARE)*, 2009.

[16] Zeidanloo, H. R., Hosseinpour, F. and Eternad, F.F.: New Approach for Detection of IRC and P2P Botnet. *International Journal of Computer and Electrical Engineering Vol. 2(No. 6): 1793-8163*, 2010

[17] Rahim, A., Muhaya, F.T., et al.: Discovering the Botnet Detection Techniques, 2010

[18] Chao, L., J. Wei, et al.: Botnet: Survey and Case Study. *Fourth International Conference on Innovative Computing, Information and Control (ICICIC)*, 2009.

[19] Garcia-Teodoro, P., J. Diaz-Verdejo, et al.: Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security 28: 18-28,* 2009

[20] Zeidanloo, H. R. a. A., A.B.: Botnet Detection by Monitoring Similar Communication Patterns. *(IJCSIS) International Journal of Computer Science and Information Security Vol. 7(No. 3): 36-45,* 2010

[21] Jeong, O. K., Kim, C., et al.: Botnet: Threats and Responses. *International Journal of Web Information Systems Vol. 7(Iss: 1): pp.6 - 17,* 2011

[22] Saha B. and Gairola A.: Botnet: An Overview. *CERT-In White Paper CIWP-2005-05*, 2005

[23] Binkley, J. R. and Singh, S.: An algorithm for anomaly-based Botnet detection, *Proceeding USENIX: Steps to Reducing Unwanted Traffic on the Internet Workshop (SRUTI)*, 2006

[24] Karasaridis, A., Rexroad, B., and Hoeflin, D.: Wide Scale Botnet Detection and Characeristics, *Proceeding 1st Workshop on Hot Topics in Understanding Botnet*, 2007

[25] Stinson, E. and Mitchell, J. C.; Characterizing Bots, Remote Control Behaviour, *Proceedings of the 4th GI International Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA)*, 2007

[26] Gu, G., Porras, P. et al.: BotHunter: Detecting Malware Infection throufh IDS-Driven Dialog Correlation, *Proceedings of the 16th USENIX Security Symposium, Boston*, 2007

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

[28] Guofei, G., P. Roberto, et al.: BotMiner: Clustering analysis of network traffic for protocol-and-structure-independent Botnet detection. *Proceedings of the 17th conference on Security symposium. San Jose, CA, USENIX Association,.* 2008

[29] Strayer, W., D. Lapsely, et al.: *Botnet Detection Based on Network Behavior Botnet Detection, Springer US. **36:** 1-24.*, 2008

[30] Liu, L., S. Chen, et al.: BotTracer: Execution-Based Bot-Like Malware Detection Information Security, *Springer Berlin /Heidelberg. **5222:** 97-113*, 2008

[31] Guofei, G., V. Yegneswaran, et al.: Active Botnet Probing to Identify Obscure Command and Control Channels. *Annual Computer Security Applications Conference (ACSAC)*, 2009.

[32] Ricardo, V., S. n, et al.: Bayesian bot detection based on DNS traffic similarity. *Proceedings of the 2009 ACM symposium on Applied Computing. Honolulu, Hawaii, ACM*, 2009

[33] Wei, L., T. Mahbod, et al.; Automatic discovery of Botnet communities on large-scale communication networks. *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security. Sydney, Australia, ACM*, 2009

[34] Su, C. and E. D. Thomas: P2P Botnet detection using behavior clustering and statistical tests. *Proceedings of the 2nd ACM workshop on Security and artificial intelligence. Chicago, Illinois, USA, ACM.*, 2009

[35] Yuanyuan, Z., H. Xin, et al.: Detection of Botnet using Combined Host-and Network-Level Information. *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2010.

[36] Al-Hammadi, Y. and U. Aickelin: Behavioural Correlation for Detecting P2P Bots. *Second International Conference on Future Networks (ICFN)*, 2010.

[37] Arshad, S., M. Abbaspour, et al.: An anomaly-based Botnet detection approach for identifying stealthy Botnet. *IEEE International Conference on Computer Applications and Industrial Electronics (ICCAIE)*, 2011

[38] Snort IDS [Online] Retrieved on January 2013 from http://www.snort.org

[39] Jan, G. and H. Thorsten.: Rishi: Identify bot contaminated hosts by IRC nickname evaluation. *Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnet. Cambridge, MA, USENIX Association*, 2007

[40] Yinglian, X., Y. Fang, et al.: Spamming Botnet: Signatures and Characteristics. *Proceedings of the ACM SIGCOMM Conference on Data Communication. Seattle, WA, USA*, 2008

[41] Wei, W., F. Binxing, et al.: A Novel Approach to Detect IRC-Based Botnet. *International Conference on Networks Security, Wireless Communications and Trusted Computing (NSWCTC)*, 2009.

[42] Behal, S., Brar, A.S., et al.: Signature-based Botnet Detection and Prevention, 2009

[43] Konrad, R., S. Guido, et al.: Botzilla: Detecting The "Phoning Home" Of Malicious Software. *Proceedings of the Symposium on Applied Computing. Sierre, Switzerland, ACM*, 2010

[44] Kristoff, J.: Botnet." *32nd Meeting of the North American Network Operators Group*, 2004

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

[46] Van Helmond, D.J., and Schonewille, A.: The Domain Name Service as an IDS, *Master Project University of Amsterdam, Netherlands*, 2006

[47] Ramachandran, A. Feamster, N. and Dagon, D.: Revealing Botnet membership using DNSBL counter-intelligence, *Proceedings of the 2nd Conference on Steps to Reducing Unwanted Traffic on the Internet (SRUTI), San Jose*, 2006

[48] Hyunsang, C., L. Hanwoo, et al.: Botnet Detection by Monitoring Group Activities in DNS Traffic. *7th IEEE International Conference on.Computer and Information Technology* (*CIT)*, 2007.

[49] Villamarin-Salomon, R. and J. C. Brustoloni.: Identifying Botnet Using Anomaly Detection Techniques Applied to DNS Traffic. *5th IEEE Consumer Communications and Networking Conference (CCNC)*, 2008.

[50] Hyunsang, C., L. Heejo, et al.: BotGAD: Detecting Botnet by capturing group activities in network traffic. *Proceedings of the Fourth International ICST Conference on Communication System Software and Middleware. Dublin, Ireland, ACM*, 2009

[51] Masud, M. M., T. Al-khateeb, et al.: Flow-based identification of Botnet traffic by mining multiple log files. *First International Conference on Distributed Framework and Applications*, 2008.

[52] Mohammad, M. M., G. Jing, et al.: Peer to peer Botnet detection for cyber-security: a data mining approach. *Proceedings of the 4th annual workshop on Cyber security and information intelligence research: Developing strategies to meet the cyber security and information intelligence challenges ahead. Oak Ridge, Tennessee, ACM*, 2008

[53] Nivargi, V., Bhaowal, M., et al.: Machine Learning Based Botnet Detection, 2009

[54] Wen-Hwa, L. and C. Chia-Ching: Peer to Peer Botnet Detection Using Data Mining Scheme. *International Conference on Internet Technology and Applications*, 2010

[55] Junjie, Z., R. Perdisci, et al.: Detecting Stealthy P2P Botnet Using Statistical Traffic Fingerprints. *IEEE/IFIP 41st International Conference on Dependable Systems & Networks (DSN)*, 2011

[56] Jackson, A. W., D. Lapsley, et al.: SLINGbot: A System for Live Investigation of Next Generation Botnet. *Conference for Homeland Security, Cybersecurity Applications & Technology (CATCH)*, 2009.

[57] Chandrashekar, J., Orrin, S., et al.: The Dark Cloud: Understanding and Defending against Botnet and Stealthy Malware. *Intel Technology Journal Vol. 13 (Issues 2)*, 2009

[58] Dini, G. and I. S. La Porta: BLOBOT: BLOcking BOTs at the Doorstep. *Fourth International Multi-Conference on Computing in the Global Information Technology (ICCGI)*, 2009.

[59] Wurzinger, P., L. Bilge, et al.: Automatically Generating Models for Botnet Detection Computer Security, *Springer Berlin / Heidelberg. 5789: 232-249*, 2009

[60] Law, F. Y. W., K. P. Chow, et al.: A Host-Based Approach to Botnet Investigation? Digital Forensics and Cyber Crime. *O. Akan, P. Bellavista, J. Caoet al, Springer Berlin Heidelberg.* ***31:*** *161-170*, 2010

[61] Nagaraja, S., Mittal, P., et al.: BotGrep: Finding P2P Bots with Structured Graph Analysis, 2010

[62] Fang, Y., X. Yinglian, et al.: SBotMiner: Large scale search bot detection. *Proceedings of the Third ACM International Conference On Web Search And Data Mining, New York, USA, ACM*, 2010

[63] Kuwabara, K., H. Kikuchi, et al. (2010). Heuristics for Detecting Botnet Coordinated Attacks. *International Conference on Availability, Reliability and Security (ARES)*, 2010.

[64] Rostami, M. R., B. Shanmugam, et al.: Analysis and Detection of P2P Botnet Connections Based on Node Behaviour. *World Congress on Information and Communication Technologies (WICT)*, 2011

[65] Tung-Ming, K., C. Hung-Chang, et al.: Construction P2P firewall HTTP-Botnet defense mechanism. *IEEE International Conference on Computer Science and Automation Engineering (CSAE)*, 2011

[66] Stringhini, G., Holz, T., et al.: BOTMAGNIFIER: Locating Spambots on the Internet, 2011

[67] Wang, P., Aslam, B., et al.: Peer-to-Peer Botnet, 2010

Raihana Syahirah Abdullah She is currently a PhD student at Universiti Teknikal Malaysia Melaka. Her research area include Computer and Network Security.

Mohd Faizal Abdollah, Zul Azri Muhamad Noh, Mohd Zaki Mas'ud, Siti Rahayu Selamat and Robiah Yusof are currently a senior lecturer in Universiti Teknikal Malaysia Melaka. Their research area are IDS, Malware, Forensic and Network Security.

Appendix-A: Table 2 - Detection Criteria for Botnet Detection Techniques

Author/ Technique and Year	Detection Technique				Detection Criteria								
	Anomaly Based	Signature Based	DNS Based	Data Mining Based	Unknown Botnet Detection	Protocol and Structure Independent	Low False Positive	Low Cost	Low Risk	Encrypted Bot Detection	Real-Time/Real-World Detection	Not Require Prior Knowledge	Reveal Bot Servers and C&C Migration
Binkley & Singh (2006) [23]	√				X	X	√	√	√	X	X		√
Karasaridis (2007) [24]	√				√	X	√			√	X		
BotSwat (2007) [25]	√						√						
BotHunter (2007) [26]	√				√	√	X	√	√				
BotSniffer (2008) [27]	√				√	X	√	√	√	√	X	√	
BotMiner (2008) [28]	√			√	√	√	√	√	√	√	√	√	
Strayer et al. (2008) [29]	√			√	√	X	X	√	√	X	X		
BotTracer (2008) [30]													
BotProbe (2009) [31]	√						√						
Bayesian Bot (2009) [32]	√												
Automatically Discovery (2009) [33]	√												
P2P Botnet Detection (2009) [34]	√						√				√		
SBotMiner (2010) [62]	√			√									
Hossein et al. (2010) [20]	√											√	
Yuanyuan et al. (2010) [35]	√										√		
Al-Hammadi (2010) [36]	√											√	
Arshad et al. (2011) [37]	√						√				√	√	
Snort (2006) [38]		√			X	X	X			X	X		
VanHelmond (2006) [46]		√			√	X	√			√	X		
Rishi (2007) [39]		√		√	X	X	√	√	√	X	X		
AutoRE (2008) [40]		√			X	X	√	√	√				
Wang et al. (2009) [41]		√			X								
N-EDPS (2009) [42]		√			X								
Botzilla (2010) [43]		√			X		√						
Kristoff J. (2004) [44]	√		√		√	X	X			√	X		
Dagon D. (2005) [45]	√		√		√	X	X			√	X	X	
Ramachandran (2006) [47]		√	√		√	X	X		X	√	√		
Choi et al. (2007) [48]	√		√		√	√	√			√	X		√
Villamarin-Solomon et al. (2008) [49]	√		√										
BotGAD (2009) [50]			√		√						√		
Masud et al. (2008) [51]	√			√	√	√	√			√	X		
Mohammad et al. (2008) [52]				√									
Nivargi et al. (2009) [53]				√								√	
Liao & Chang (2010) [54]				√									
Junjie et al. (2011) [55]				√							√	√	
SLINGbot (2009) [56]													
Canary Detector (2009) [57]											√	√	
BLOBOT (2009) [58]											√		
Wurzinger et al. (2009) [59]							√			√	√		
Law (2010) [60]													√

Legend: Yes (√), No (X)