Research Journal of Information Technology

ISSN 1815-7432

Academic
Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 6 (3): 135-153, 2014
ISSN 1815-7432 / DOI: 10.3923/rjit.2014.135.153

Understanding the Threats of Botnets Detection: A Wide Scale Survey

Raihana Syahirah Abdullah, Nur Azman Abu, M.A. Faizal and Zul Azri Muhamad Noh
Faculty of Information and Communication Technology, Universiti Teknikal Malaysia, Hang Tuah Jaya, 76100, Durian Tunggal, Melaka, Malaysia

Corresponding Author: Raihana Syahirah Abdullah, Faculty of Information and Communication Technology, Universiti Teknikal Malaysia, Hang Tuah Jaya, 76100, Durian Tunggal, Melaka, Malaysia

ABSTRACT

A growing number of botnets threats recently has grown to the level of world wide concerns. This dangerous phenomenon emerges drastically and offers undefined capability to attack the global internet security never seen before. As time evolves, the incremental numbers of botnets attack have been recorded with types of variants such as peer-to-peer (P2P) have been discovered. Attentively, botnets attack nowadays is typically declared as an advance malware due to its ability to smokescreen itself as a benign P2P application which make it difficult to detect and shut down and also easily to escape itself. Alarming on this crisis, many studies propose on detection, prevention and mitigation techniques as the precaution action. Hence, this study addresses in-depth review on a wild scale for botnets detection techniques. Technically, the survey classifies the detection techniques into five categories based on its anomaly, signature, DNS, data mining and hybrid technique. To enrich the level of understandings on the strategy, this study also highlights the importance of such characteristics as type of technique, approach, response time, type of botnets, detection parameter, metric and variants. In addition, this study offers detail discussion about botnets detection techniques which is beneficial for botnets investigation and helpful to other researches for immediate references.

Key words: Botnet, P2P botnet, IDS, botnet detection techniques, advance malware, advance persistent threats

INTRODUCTION

The evolution of information technology has extremely changed our generation's life style. Nowadays, this greatest invention gives big influence to human life covering simplest activities such as buying the grocery to the biggest issues of developing the regional economic or fighting for the global peace. Due to over dependence of human towards the usage of internet, the life style has not only lead to infinite excitement and amenities but also exposing users to unpredictable criminals. The virtual threat has not only attacked towards individual but also critically larger communities such as countries or a continent. In reality, the cyber criminals are capable of launching a sudden attack to any network infrastructures only by isolating the hosts depending on their interests such financial institution or political bodies. Technically, an internet threat occurs when a group of compromised computers or botnets have been controlled by a mastermind from an unknown location around the globe through the domination of distributed behaviour to launch a cyber-attack.

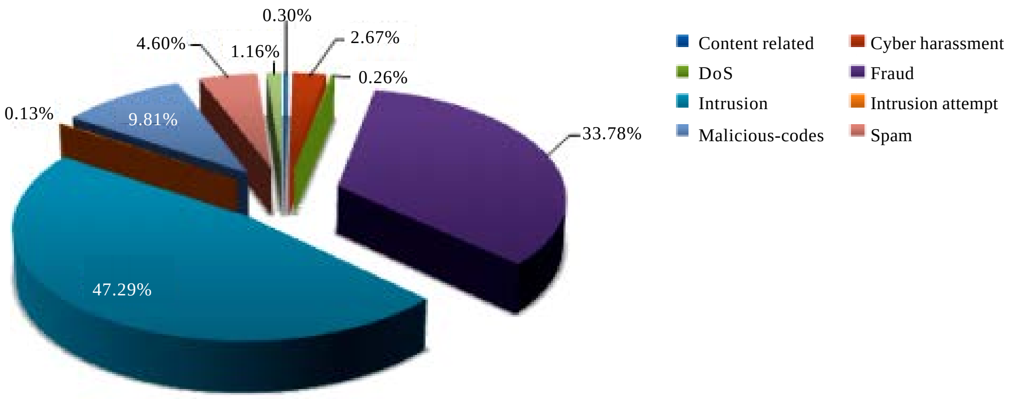
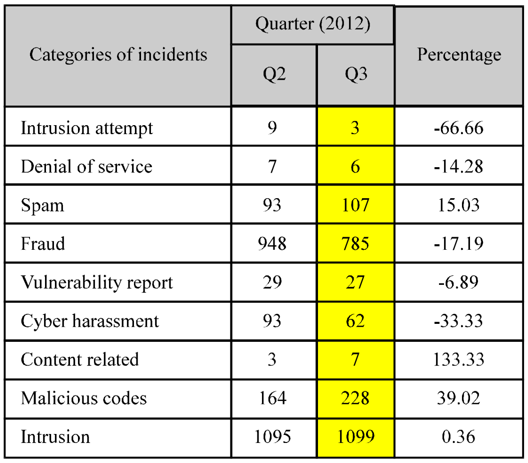


Fig. 1: Percentage of security incidents quarter3 2012 from MyCERT (Cyber Security Malaysia, 2012a, b)



Categories of incidents	Quarter (2012)		Percentage
	Q2	Q3	
Intrusion attempt	9	3	-66.66
Denial of service	7	6	-14.28
Spam	93	107	15.03
Fraud	948	785	-17.19
Vulnerability report	29	27	-6.89
Cyber harassment	93	62	-33.33
Content related	3	7	133.33
Malicious codes	164	228	39.02
Intrusion	1095	1099	0.36

Fig. 2: Comparison of incidents between Q2 and Q3 2012 (Cyber Security Malaysia, 2012a, b)

The increasingly prevalent threat from botnets should be taken seriously with appropriate actions needed to address the problems. According to Malaysian Computer Emergency Response Team (MyCERT) in Quarter3 2012, they have handled 228 reports related to malicious code activities that represent 39.02% out of the total number of security incidents (Cyber Security Malaysia, 2012a, b) as illustrated in Fig. 1.

Comparatively, two set of different data for Q2 and Q3 emphasized in Fig. 2 marked the incremental number of malicious code in 2012. Some of the malicious code security incidents handled was related to active botnets controllers, hosting of malware or malware configuration files on compromised machines and malware infections to computers.

Chronologically, this wide survey conducts the botnets detection techniques that will be clarified as concentrate in basis of type of technique, approach, response time, type of botnets, metric, type of variant and their parameters. All the studies that have been taken into accounts have been reviewed using the same characteristic.

Concerning on further discussion related to the particular studies, it is obligatory to know some of the key terms about botnets. Also, it is important to realize the causes and effects of botnets in the real world situation. Hence, this section discussed the key terms of botnets and P2P botnets to enhance the knowledge and understanding on the related topics.

Botnet: Internet security nowadays has been threatened by dangerous advanced malwares or botnets (Zeidanloo *et al*., 2010a). In recent years, an attack via botnets has increased drastically due to its real nature which remains incomprehensible though lots of studies have been done. Theoretically, botnets is a collection of computers which is infected by malicious software and become bots, drones or zombies which assimilate into a collective by centralized Command and Control (C and C) infrastructure (Mielke and Chen, 2008). The C and C manipulates the bots to illegally control the computing resources. When the overpowering incident is successful, the botnets shall exploits and recruits the computer to be the army of cyber attack via spamming, fake websites, DDoS attacks, viruses, worms, backdoors, information harvesting phishing and scams (Mielke and Chen, 2008). The behaviour of botnets can maliciously expose the secretive elements of security and safety which can easily propagate the number of cyber crimes.

Referring to SearchSecurity.com website, a report from Russian-based Kaspersky Labs reveals that botnets currently pose serious threat to the internet security. At the same time, a report from Symantec comes to the same conclusion (http://searchsecurity.techtarget.com; Westervelt, 2009). In addition, a report on the emerging cyber threat 2011 presented at the Georgia Tech Information Security Center (GTISC) at Security Summit 2010 had listed the botnets as one of the emerging threat in the year 2011 (GTISC, 2011). One of the cases mentioned by the report is the Mariposa botnets that are capable of stealing financial credential in which the center also reported almost 800,000 financial crimes involve personal computers.

IRC, HTTP and P2P Botnet: The integration of botnets and current technology such as IRC, HTTP and Peer to Peer (P2P) has increased the immunity of being detected and allowed them to silently organize their black mission into several benign applications. Many researches has embarked on detecting IRC and HTTP botnets through network monitoring analysis. Most of the botnets activities can be easily destroyed once the bots get connected to the central command and control server. Yet, the P2P is harder to be detected as its command and control centre are distributed similarly to the P2P leeches which share files over the internet.

P2P botnets currently is one of the critical phenomena where the Cyber defence is in needs of new Computational Intelligence (CI) techniques since existing methods of intrusion detection have been foiled by P2P botnets (Estrada and Nakao, 2010). Taking a consideration on this endeavour into current perspectives, this study uses the anomaly detection that is able to differentiate between normal network traffic and abnormal network traffic characteristics. An inappropriate and ineffective detection technique may not able to detect the P2P botnets due to its unique ability and special characteristic. Due to inconsistency characteristics of P2P botnets, advanced knowledge about malicious software and its characteristic is needed to create new rules for monitoring its behaviours. The chronology of the P2P botnets operation has been illustrated in Fig. 3.

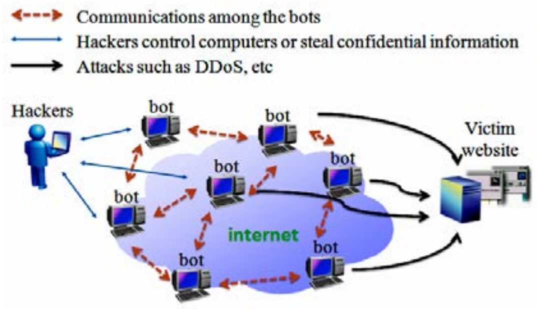

Communications among the bots
Hackers control computers or steal confidential information
Attacks such as DDoS, etc
Hackers
bot
bot
bot
bot
bot
bot
bot
internet
Victim website

Fig. 3: P2P botnet operation (Liao and Chang, 2010)

CLASSIFICATION OF BOTNET DETECTION TECHNIQUES

Botnets detection technique is a technique used to detect or identify the botnets activities. Previous researches have proposed several different solutions to solve the botnets attacks. Basically, botnets detection techniques divided into two approaches which are based on honeynet and Intrusion Detection System (IDS). At the early stage informal studies, the botnets attack were detected by setting up honeynet (Bacher *et al*., 2008; Baecher *et al*., 2006; Freiling *et al*., 2005; Provos, 2004). Many researchers have set up honeynet to analyze bots, learning tools, tactics and motives of botmaster (Jeong *et al*., 2011). However, honeynet is only effective in understanding the botnets characteristic but ineffective in detecting bots infection all the times. The weaknesses of the honeynet encourages the researchers to turn to IDS techniques that is more practical in identifying the existence of botnets. Generally, botnets detection in IDS can be categorized into anomaly-based, signature-based and hybrid-based detection techniques (Zeidanloo *et al*., 2010a; Robiah *et al*., 2009; Feily *et al*., 2009; Zeidanloo *et al*., 2010b; Rahim and Bin Muhaya, 2010; Li *et al*., 2009; Garcia-Teodoro *et al*., 2009; Zeidanloo and Manaf, 2010; Jeong *et al*., 2011; Wurzinger *et al*., 2009).

Based on previous collective works, the characteristics of each technique can be overviewed by referring to Fig. 4.

Anomaly-based detection: Anomaly-based detection is a sub-technique under the group of behaviour-based detection. The anomaly-based detection may then be divided into four types, namely, DNS, data mining, host and network. These techniques are able to detect botnets based on several network traffic anomalies such as high network latency, high volume traffic, traffic on unusual ports and unusual system behaviour that can indicates any presence of malicious bots in the network (Zeidanloo *et al*., 2010a; Garcia-Teodoro *et al*., 2009; Zeidanloo and Manaf, 2010; Saha and Gairola, 2005). Overall, it focuses on normal behaviour to overcome undetected unknown attack. The anomaly-based technique is capable of detecting the unknown botnets and attacks. Unfortunately, it produces a high false positive alarm rate.

DNS-based: The DNS-based detection technique can been performed by doing the DNS monitoring and checking on DNS traffic anomalies. In order to perform this technique successfully, it requires the DNS information generated by a botnets (Feily *et al*., 2009). Normally, bots send the DNS queries to access bots servers. It is useful since bots can later use the DNS to identify the address of botmaster.

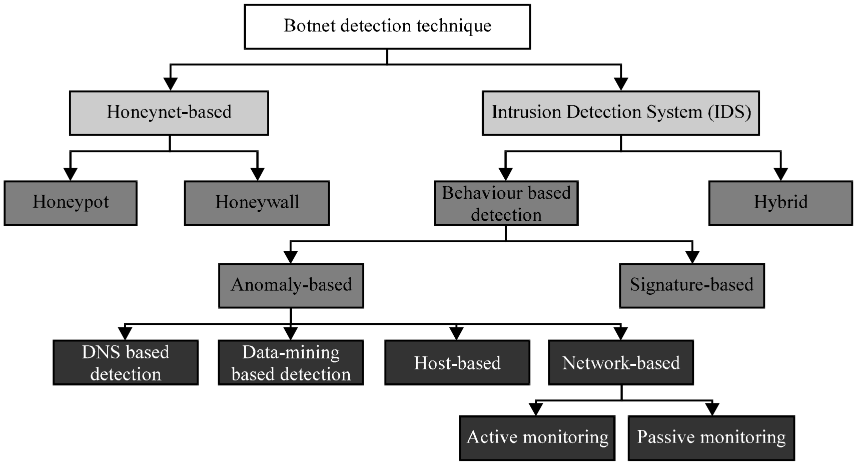


Fig. 4: Botnet detection technique

Data mining-based: The data miming-based detection technique is able to improve the level of accuracy for detection method (Jeong *et al*., 2011). It is an effective technique for botnets detection since it can be used efficiently to detect botnets C and C traffic by using machine learning, classification and clustering approach.

Host-based: The host-based approach functions via monitoring the network traffic for any indication of the bots infecting machines (Wurzinger *et al*., 2009). The host is being infected when bots has been activated by making some changes on system registry and system files (Jeong *et al*., 2011). Botnets then re-create a series of systems and library calls in initiating the attacks.

Network-based: The network-based approach is more appropriate on monitoring the network traffic in (Jeong *et al*., 2011; Wurzinger *et al*., 2009):

- Detecting the individual bots by checking the traffic patterns or content that can reveal the command and control (C and C) server or malicious in bots-related activities
- Analyzing the traffic that indicates two or more hosts with similar patterns as bots react the same function. Monitoring in network-based can be done either in active or passive mode

Signature-based detection: Similar to anomaly-based technique, the signature-based detection technique also is a part of behaviour-based detection. This technique learns and gains knowledge from the signatures or behaviours from existing botnets (Feily *et al*., 2009; Zeidanloo *et al*., 2010b). This solution is useful for detecting on well-known botnets accurately but the unknown bots. Moreover, signature-based solution can perform immediate detection and zero possibility towards fake or false positive. It also requires less amount of system resource to perform the detection process.

Hybrid-based detection: In hybrid-based detection technique, two or more IDS techniques are combined. For instance, it can be the combination of DNS-based with anomaly-based, signature-based with anomaly-based or data mining-based with anomaly-based technique. For

Table 1: Related reviews involving botnets detection techniques from previous studies

Detection technique	Study review reference No.
Anomaly-based	Zeidanloo and Manaf (2010), Binkley and Singh (2006), Karasaridis *et al*. (2007), Stinson and Mitchell (2007), Gu *et al*. (2007), Gu *et al*. (2008a, b), Strayer *et al*. (2008), Liu *et al*. (2008), Guofei *et al*. (2009), Villamarin-Salomon and Brustoloni (2009), Wei *et al*. (2009), Chang and Daniels (2009), Zang *et al*. (2010), Al-Hammadi and Aickelin (2010), Arshad *et al*. (2011), Kristoff (2004), Dagon (2005), Choi *et al*. (2007), Villamarin-Salomon and Brustoloni (2008), Choi *et al*. (2009), Masud *et al*. (2008a, b), Nivargi *et al*. (2009), Liao and Chang (2010), Zhang *et al*. (2011), Yu *et al*. (2010)
Signature-based	Goebel and Holz (2007), Xie *et al*. (2008), Wang *et al*. (2009), Behal *et al*. (2010), Rieck *et al*. (2010), Schonewille and van Helmond (2006)
Hybrid-based	Gu *et al*. (2008a), Strayer *et al*. (2008), Goebel and Holz (2007), Kristoff (2004), Dagon (2005), Ramachandran *et al*. (2006), Choi *et al*. (2007), Villamarin-Salomon and Brustoloni (2008), Masud *et al*. (2008a), Yu *et al*. (2010)

signature-based, DNS-based and data mining-based, they have equal capability whereby they are able to detect known attacked but fail to detect any unknown attacks. Alternatively, the anomaly-based by chance bring extra capabilities for detecting the unknown attack compares to other techniques. Referring to the analysis by (Robiah *et al*., 2009), the combination of IDS techniques will improve the weakness and complement each other in contributing to better performance.

As a summary, 44 researchers who perform various botnets detection techniques have been reviewed. Table 1 shows the related reviews involving botnets detection techniques from previous researches.

DISCUSSION ON COMPARISON OF BOTNET DETECTION TECHNIQUES

The botnets detection and prevention nowadays catches some major interest in the topic to be explored as these issues are on current demands. This security topic is increasingly prevalent to national and global security risk. Various types of techniques have been proposed related to detection, prevention and mitigation of botnets attacks. Technically, botnets detection technique is a complicated task, whereby, the detection procedures can only be possibly performed when the botnets are communicating within a large scale of network. The botnets may hides itself when it attacks a small network. Hence, this section provides a brief comparison on botnets detection techniques. The comparisons have been made regardless to the type of techniques, approaches, response time, type of botnets, metrics, type of variants and their parameters. The summarization of the comparisons are described in Table 2.

As shown in the Table 2, most of researchers use the anomaly-based technique to detect botnets. Then, several researches are using DNS, signature and data mining-based techniques. Otherwise, there are only few researchers using the hybrid-based as technique for detecting the botnets. The hybrid-based technique widely used by the integration of anomaly-based with other techniques including; DNS-based with anomaly-based (Kristoff, 2004; Dagon, 2005; Choi *et al*., 2007; Villamarin-Salomon and Brustoloni, 2008), data mining-based with anomaly-based (Gu *et al*., 2008b; Strayer *et al*., 2008; Masud *et al*., 2008a; Yu *et al*., 2010) and signature-based with data mining-based (Goebel and Holz, 2007). Through the detection, normal behaviour of system will be protected while the malicious of botnets will continuously detect based on traffic anomalies. Still, some of the handful researchers apply ancillary techniques to strengthen their

Table 2: Botnets detection techniques

	Detection technique					Approach		Response time		Type of botnet			Metric				
Author/Technique and year	Anomaly based	Signature based	DNS based	Data mining based	Others	Host based	Network based	Active monitoring	Passive monitoring	IRC	HTTP	P2P	Efficiency	Effectiveness	Robustness	Detection parameter	Variant
Binkley and Singh (2006)	√						√		√	√						IRC tokenization, IRC message statistics	
Karasaridis *et al.* (2007)	√								√	√						IRC service ports	
BotSwat Stinson and Mitchell (2007)	√					√										Remote control behavior	
BotHunter Gu *et al.*, (2007)	√				adding SCADE and SLADE		√		√					√		Whole process of Botnet infection (life cycle bots)	
BotSniffer Gu *et al.* (2008a)	√						√		√	√	√					Spatial temporal correlates traffic in space and time	
BotMiner Gu *et al.* (2008b)	√			√			√		√	√	√	√	X			Used unsupervised X-mean clustering	Nugache, Stormworm
Strayer *et al.* (2008)	√			√	Machine learning technique		√		√	√						IRC flow analysis (packet inter-arrival time and packet size)	
BotTracer Li *et al.* (2009)					virtual machine technology	√				√	√	√					Agobot, Forbot, Jrbot, Sdbot, Reptilebot, Rxbot, Graybird, Nugache

Table 2: Continue

	Detection technique					Approach		Response time		Type of botnet			Metric				
Author/Technique and year	Anomaly based	Signature based	DNS based	Data mining based	Others	Host based	Network based	Active monitoring	Passive monitoring	IRC	HTTP	P2P	Efficiency	Effectiveness	Robustness	Detection parameter	Variant
BotProbe Guofei *et al.* (2009)	√				hypothesis testing		√	√		√						Network session in IRC chatting	
Bayesian Bot Villamarin-Salomon and Brustoloni, 2009)	√						√			√	√					A and CNAME queries and answers	Backdoor, NetWorm Bobax
Automati-cally Discovery Wei *et al.* (2009)	√						√									Payload signature	
P2P Botnet Detection (Chang and Daniels, 2009)	√				Statistical test							√				P2P protocol and non-P2P protocol	Nugache
SbotMiner Yu *et al.* (2010)	√ √			√			√		√	√	√	√				Used Matrix-based	ClickBot.A
Choi *et al.* (2007)					Clustering and Monitoring				√	√	√	√				Similar pattern as Source IP (SIP) address, destination IP (DIP) address, Source Port (SPORT), Destination Port (DPORT), Duration (Dr), Protocol (Pr), Packet Arrival Time (PAT), No. of packets (np) and No. of bytes (nb)	Stormworm Bobax

Table 2: Continue

	Detection technique					Approach		Response time		Type of botnet			Metric				
Author/Technique and year	Anomaly based	Signature based	DNS based	Data mining based	Others	Host based	Network based	Active monitoring	Passive monitoring	IRC	HTTP	P2P	Efficiency	Effectiveness	Robustness	Detection parameter	Variant
Zang *et al.* (2010)	√					√	√			√	√	√				Similar behavior between host in network flow	IRC-Rbot, IRC-Spybot, HTTP-Bobax, Storm and Waledac
Al-Hammadi and Aickelin (2010)	√				correlation algorithm							√				Specified time window	Peacomm (Storm)
Arshad *et al.* (2011)	√				correlation algorithm					√	√			√		Similar netflow and time window	IRC-Sdbot, IRC-Spybot,
HTTP-Bot																	
Snort (http://www.snort.org)		√															
Schonewille and van Helmond (2006)	√													√		NXDOMAIN reply rates	
Rishi (Goebel and Holz, 2007)		√		√	n-grep tools, n-gram analysis, scoring system								√	√	√	Odd IRC nickname, IRC server, uncommon server port, suspicious string in URLs	Trojan. Zlob.Gen
AutoRE (Xie *et al.*, 2008)		√									√					Spam payload and spam server traffic	Spam Botnet (MSN, HTML)
Wang *et al.* (2009)		√								√						Similarity nickname in same channel	SXBot
N-EDPS		√								√	√	√				Feasibility of	Conficker A

Table 2: Continue

	Detection technique					Approach		Response time		Type of botnet			Metric				
Author/Technique and year	Anomaly based	Signature based	DNS based	Data mining based	Others	Host based	Network based	Active monitoring	Passive monitoring	IRC	HTTP	P2P	Efficiency	Effectiveness	Robustness	Detection parameter	Variant
Behal *et al.* (2010)																outbound traffic	and B, HotBar, Pakes, Cutwail, Pushdo, Kobeka, Storm/ Peed, GTBotBotzi
lla Rieck *et al.* (2010)		√			Automatic signature inference					√	√	√				Malware binaries	Hupigon (HTTP), Storm (P2P), Banload (FTP)
Kristoff (2004))	√		√													Intense DDNS query rate	
Dagon (2005)	√		√				√		√	√						DNS Queries rate, DDNS	
Ramachandran (2006)		√	√		Perform counter-intelligence		√		√				X			DNSBL recoinassance activity	
Choi *et al.* (2007)	√		√				√		√	√		√	√		√	DNS Queries, RR record, IP headers	Agobot
Villamarin-Salomon and Brustoloni (2009)	√		√														
BotGAD Choi *et al.* (2009)			√														
Masud *et al.* (2008b)	√			√	Temporal correlation technique		√		√	√	√			√	√	Multiple log files	SdBot, Rbot
Liao and Chang (2010)				√										√		Stream data classification	

Table 2: Continue

	Detection technique					Approach		Response time		Type of botnet			Metric				
Author/Technique and year	Anomaly based	Signature based	DNS based	Data mining based	Others	Host based	Network based	Active monitoring	Passive monitoring	IRC	HTTP	P2P	Efficiency	Effectiveness	Robustness	Detection parameter	Variant
Nivargi *et al.* (2009)				√	Machine learning technique					√						Botnet binaries, IRC log	
Liao and Chang (2010)				√	J48, NaiveBayes, BayesNet							√				Host and gateway P2P	
Trojan.Peacomm Zhang *et al.* (2011)				√	Statistical traffic finger-prints, flow clustering							√		√		P2P stealthy and application (BitTorrent, LimeWire, eMule, Ares, Skype)	Storm, Waledac
SLINGbot Jackson *et al.* (2009)										√	√	√					IRC bot, tiny P2P bot, Kademlia bot, hierarchical kademlia bot
Canary Detector Chandrashekar *et al.* (2009)						√										Destination address	
BLOBOT Dini and La Porta (2009)					Tool detect Botnet					√	√					Single user detection	Black Energy/ DdoS Bot, Dbotv31, GT-Spam, Msn AIOHacks

Table 2: Continue

	Detection technique					Approach		Response time		Type of botnet			Metric				
Author/Technique and year	Anomaly based	Signature based	DNS based	Data mining based	Others	Host based	Network based	Active monitoring	Passive monitoring	IRC	HTTP	P2P	Efficiency	Effectiveness	Robustness	Detection parameter	Variant
Wurzinger *et al.* (2009)					Apply CPD algorithm and CUSUM					√	√	√		√		(i) No. of packets, (ii) No. of different machines contacted, (iii) No. of binary bytes in network stream, (iv) No. of different IP's contacted, (v) No. of different ports contacted, (vi) No. of non-ASCII bytes in payload, (vii) No. of UDP packets, (viii) No. of HTTP packets (port 80), (ix) No. of SMTP packets	Kraken, Storm

Table 2: Continue

	Detection technique					Approach		Response time		Type of botnet			Metric				
Author/Technique and year	Anomaly based	Signature based	DNS based	Data mining based	Others	Host based	Network based	Active monitoring	Passive monitoring	IRC	HTTP	P2P	Efficiency	Effectiveness	Robustness	Detection parameter	Variant
Law *et al.* (2010)					Forensic investiga -tion	√				√	√					Digital traces and physical memory	
BotGrep Nagaraja *et al.* (2010)					Sybil attack							√				Communic-ation graph	
Kuwabara *et al.* (2010)					Heuristic technique											Behavior of download and port scan	IRC Bot, MyBot, PoeBot, Rbot, Allaple, Bobax, Virut, Buzus, Agent, Autorun, Swtymlal
Rostami *et al.* (2011)					Root kits capabili-ties							√				Node profiling	TDSS Black Energy
P2P Firewall Koo *et al.* (2011)											√					Degree of periodic repeatability, freedom and standard deviation	
Bot-Magnifier Stringhini *et al.* (2011)												√				Seed pools and transaction log	Lethic, Rustock, Cutwail, MegaD, Waledac

study such as using statistical test and traffic fingerprints, temporal and correlation algorithm, automatic signature inference, heuristic technique, machine learning and virtual machine technology.

According to Zang *et al.* (2010), among all of detection techniques, the integration of host-based and network-based as IDS approach is capable to finding the similarity of behaviour between hosts in network flow. This technique is practically effective for host and network environments. Looking into different angle of study, researchers also concentrates on passive monitoring besides active monitoring. Passive traffic monitoring is useful and effective in identifying the existence of botnets. In earlier stage, botnets have performed as traditional botnets such IRC-bots (Binkley and Singh, 2006; Karasaridis *et al.*, 2007; Strayer *et al.*, 2008; Guofei *et al.*, 2009; Arshad *et al.*, 2011; Goebel and Holz, 2007; Wang *et al.*, 2009; Nivargi *et al.*, 2009) and HTTP-bots (Villamarin-Salomon and Brustoloni, 2009; Arshad *et al.*, 2011; Xie *et al.*, 2008; Rieck *et al.*, 2010; Dini and La Porta, 2009; Yu *et al.*, 2010; Koo *et al.*, 2011). Recently, most of the botnets detection techniques including (Zeidanloo and Manaf, 2010; Chang and Daniels, 2009; Zang *et al.*, 2010; Al-Hammadi and Aickelin, 2010; Behal *et al.*, 2010; Rieck *et al.*, 2010; Liao and Chang, 2010; Zhang *et al.*, 2011; Jackson *et al.*, 2009; Wurzinger *et al.*, 2009; Nagaraja *et al.*, 2010; Rostami *et al.*, 2011; Stringhini *et al.*, 2011) have concentrated on P2P-bots which make it too robust and complicated to be detected because it has the flexibility to transform itself into a benign application.

From the literature review, many researchers prefer to choose the parameters on normal five tuples from TCP connection (Zeidanloo and Manaf, 2010; Karasaridis *et al.*, 2007; Goebel and Holz, 2007; Chandrashekar *et al.*, 2009; Wurzinger *et al.*, 2009). The five tuples are the source IP address, destination IP address, source port number, destination port number and protocol in use. For DNS-based technique, researchers are selecting the behaviours in DNS as their detection parameter such as DNS Resource Record (A, CNAME and RR) (Villamarin-Salomon and Brustoloni, 2009; Choi *et al.*, 2007; Villamarin-Salomon and Brustoloni, 2008), DNS query (Dagon, 2005; Choi *et al.*, 2007; Choi *et al.*, 2009), DDNS query rate (Kristoff, 2004), NXDOMAIN reply rates (Schonewille and van Helmond, 2006) and DNSBL reconnaissance activity (Ramachandran *et al.*, 2006). Also, the common parameters that have been used by researchers who are dealing with IRC-bot are IRC port, IRC packet size, network session in IRC chatting, odd IRC nickname and IRC server (Binkley and Singh, 2006; Karasaridis *et al.*, 2007; Guofei *et al.*, 2009; Goebel and Holz, 2007; Wang *et al.*, 2009). At the same time, some researchers prefer to use the unsupervised X-mean clustering, matrix-based, specified time window, malware and botnets binaries, TTL values, digital traces, communication graph, node profiling and P2P application as their detection parameters.

In overall, these techniques currently are capable of detecting the traditional and current variants such as IRC-bots (Agobot, Sdbot, Rxbot, Spybot, Mybot), HTTP-bot (Bobax a.k.a Kraken, Waledac, Kademlia, Cutwail, MegaD, Rustock) and P2P-bot (StormWorm a.k.a Peacomm, Nugache). Discussing on enrichment of knowledge, this study explore a potential room of improvements on investigating and detecting current and upcoming botnets. In addition, there should be an appropriate metric to measure the botnets detection techniques concerning their efficiency, effectiveness or robustness as claimed by (Wang *et al.*, 2010) in detecting the botnets in a real-world.

Regarding to the comparisons that have been done in this study on current botnets detection techniques being used by researchers are (Gu *et al.*, 2008a; Strayer *et al.*, 2008; Goebel and Holz, 2007; Kristoff, 2004; Dagon, 2005; Choi *et al.*, 2007; Villamarin-Salomon and Brustoloni, 2008; Masud *et al.*, 2008a; Yu *et al.*, 2010) technically based on hybrid-based which integrates the host-based and network-based (Zang *et al.*, 2010). The integration of host-based and network-based enhances the ability of discovering the real-world botnets as detected on IRC-bots, HTTP-bots and P2P-bots with selected parameters. Hence, the development of hybrid-based technique through the combination of host and network has being most promising approaches to control and eradicate the botnets threat in the real world atmosphere.

CONCLUSION

In this study, we have reviewed and summarized the distinctive approaches on existing botnets detection techniques. Then, the comparison among botnets detection techniques by type of techniques, approaches, response time, type of botnets, metric, type of variants and parameters have been done. Thus, the comparative analysis of botnets detection techniques has been presented through these factors. Analytically, this study is a preliminary work on botnets detection. Hence, this study contributes to the ideas of developing a new botnets detection technique by finding the gap among the existing botnets detection techniques.

ACKNOWLEDGMENT

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) in encouraging the authors to publish this paper. This work was supported by the MoE of Malaysia under Grants FRGS/2012/FTMK/SG05/03/1/F00141.

REFERENCES

Al-Hammadi, Y. and U. Aickelin, 2010. Behavioural correlation for detecting P2P bots. Proceedings of the 2nd International Conference on Future Networks, January 22-24, 2010, Sanya, Hainan, China, pp: 323-327.

Arshad, S., M. Abbaspour, M. Kharrazi and H. Sanatkar, 2011. An anomaly-based botnet detection approach for identifying stealthy botnets. Proceedings of the IEEE International Conference on Computer Applications and Industrial Electronics, December 4-7, 2011, Penang, Malaysia, pp: 564-569.

Baecher, P., M. Koetter, T. Holz, M. Dornseif and F. Freiling, 2006. The nepenthes platform: An efficient approach to collect malware. Proceedings of the 9th International Symposium on Recent Advances in Intrusion Detection, September 20-22, 2006, Hamburg, Germany, pp: 165-184.

Bacher, P., T. Holz, M. Kotter and G. Wicherski, 2008. Know your enemy: Tracking botnet. The Honeynet Project and Research Alliance. October 8, 2008. http://www.honeynet.org/papers/bots/.

Behal, S., A.S. Brar and K. Kumar, 2010. Signature-based botnet detection and prevention. Proceedings of the International Symposium on Computer Engineering and Technology, March 19-20, 2010, Mandi Gobindgarh, Punjab, India, pp: 1-6.

Binkley, J.R. and S. Singh, 2006. An algorithm for anomaly-based botnet detection. Proceeding of the 2nd USENIX Workshop on Steps to Reducing Unwanted Traffic on the Internet, July 7, 2006, San Jose, CA., USA., pp: 43-48.

Chandrashekar, J., S. Orrin, C. Livadas and E.M. Schooler, 2009. The dark cloud: Understanding and defending against botnets and stealthy malware. Intel Technol. J., 13: 130-147.

Chang, S. and T.E. Daniels, 2009. P2P botnet detection using behavior clustering and statistical tests. Proceedings of the 2nd ACM Workshop on Security and Artificial Intelligence, November 9-13, 2009, Chicago, IL., USA., pp: 23-30.

Choi, H., H. Lee and H. Kim, 2009. BotGAD: Detecting botnets by capturing group activities in network traffic. Proceedings of the 4th International Conference on Communication System Software and Middleware, June 15-19, 2009, Dublin, Ireland,.

Choi, H., H. Lee, H. Lee and H. Kim, 2007. Botnet detection by monitoring group activities in DNS traffic. Proceedings of the 7th IEEE International Conference on Computer and Information Technology, October 16-19, 2007, Aizu-Wakamatsu, Fukushima, pp: 715-720.

Cyber Security Malaysia, 2012a. MyCert 2nd quarter 2012 summary report. e-Security, Vol. 31 (Q2/2012), Cyber Security Malaysia. http://www.cybersafe.my/pdf/bulletin/vol31-Q212.pdf.

Cyber Security Malaysia, 2012b. MyCert 3rd quarter 2012 summary report. e-Security, Vol. 32 (Q3/2012), Cyber Security Malaysia. http://www.cybersafe.my/pdf/bulletin/vol32-Q312.pdf.

Dagon, D., 2005. Botnet detection and response: The network is the infection. Proceedings of the 1st DNS-OARC Workshop, July 25-26, 2005, Santa Clara, CA., USA.

Dini, G. and I.S. La Porta, 2009. BLOBOT: BLOcking BOTs at the doorstep. Proceedings of the 4th International Multi-Conference on Computing in the Global Information Technology, August 23-29, 2009, Gare de Cannes-La Bocca, France, pp: 181-185.

Estrada, V.C. and A. Nakao, 2010. A survey on the use of traffic traces to battle internet threats. Proceedings of the 3rd International Conference on Knowledge Discovery and Data Mining, January 9-10, 2010, Phuket, Thailand, pp: 601-604.

Feily, M., A. Shahrestani and S. Ramadass, 2009. A survey of botnet and botnet detection. Proceedings of the 3rd International Conference on Emerging Security Information, Systems and Technologies, June 18-23, 2009, Glyfada, Athens, Greece, pp: 268-273.

Freiling, F., T. Holz and G. Wicherski, 2005. Botnet tracking: Exploring a root-cause methodology to prevent distributed denial-of-service attacks. Proceedings of the 10th European Symposium on Research in Computer Security, September 12-14, 2005, Milan, Italy, pp: 319-335.

GTISC, 2011. Emerging cyber threat report 2011. Georgia Tech Information Security Center (GTISC). https://www.gtisc.gatech.edu/pdf/cyberThreatReport2011.pdf.

Garcia-Teodoro, P., J. Diaz-Verdejo, G. Macia-Fernandez and E. Vazquez, 2009. Anomaly-based network intrusion detection: Techniques, systems and challenges. Comput. Secur., 28: 18-28.

Goebel, J. and T. Holz, 2007. Rishi: Identify bot contaminated hosts by IRC nickname evaluation. Proceeding of the 1st USENIX Workshop on Hot Topics in Understanding Botnet, April 10, 2007, Cambridge, MA., USA., pp: 1-12.

Gu, G., P. Porras, V. Yegneswaran, M. Fong and W. Lee, 2007. BotHunter: Detecting malware infection through IDS-driven dialog correlation. Proceedings of the 16th USENIX Security Symposium, August 6-10, 2007, Boston, MA., USA.

Gu, G., J. Zhang and W. Lee, 2008a. BotSniffer: Detecting botnet command and control channels in network traffic. Proceedings of the 15th Annual Network and Distributed System Security Symposium, February 10-13, 2008, San Diego, CA., USA.

Gu, G., R. Perdisci, J. Zhang and W. Lee, 2008b. BotMiner: Clustering analysis of network traffic for protocol and structure-independent botnet detection. Proceedings of the 17th USENIX Security Symposium, July 28-August 1, 2008, USENIX Association, San Jose, CA., USA., pp: 139-154.

Guofei, G., V. Yegneswaran, P. Porras, J. Stoll and W. Lee, 2009. Active botnet probing to identify obscure command and control channels. Proceedings of the Annual Computer Security Applications Conference, December 7-11, 2009, Honolulu, HI., USA., pp: 241-253.

Jackson, A.W., D. Lapsley, C. Jones, M. Zatko, C. Golubitsky and W.T. Strayer, 2009. SLINGbot: A system for live investigation of next generation botnets. Proceedings of the Cybersecurity Applications and Technology Conference for Homeland Security, March 3-4, 2009, Washington, DC., USA., pp: 313-318.

Jeong, O.K., C. Kim, W. Kim and J. So, 2011. Botnets: Threats and responses. Int. J. Web Inform. Syst., 7: 6-17.

Karasaridis, A., B. Rexroad and D. Hoeflin, 2007. Wide-scale botnet detection and characterization. Proceeding of the 1st USENIX Workshop on Hot Topics in Understanding Botnet, April 10, 2007, Cambridge, MA., USA., pp: 1-8.

Koo, T.M., H.C. Chang and G.Q. Wei, 2011. Construction P2P firewall HTTP-botnet defense mechanism. Proceedings of the IEEE International Conference on Computer Science and Automation Engineering, June 10-12, 2011, Shanghai, pp: 33-39.

Kristoff, J., 2004. Botnets. Proceedings of the 32nd Meeting of the North American Network Operators Group, October 17-19, 2004, Reston, Virginia, USA..

Kuwabara, K., H. Kikuchi, M. Terada and M. Fujiwara, 2010. Heuristics for detecting botnet coordinated attacks. Proceedings of the International Conference on Availability, Reliability and Security, February 15-18, 2010, Krakow, Poland, pp: 603-607.

Law, F.Y. W., K.P. Chow, P.K.Y. Lai, H.K.S. Tse, 2010. A Host-Based Approach to Botnet Investigation? In: Digital Forensics and Cyber Crime: First International ICST Conference, ICDF2C 2009, Albany, NY, USA, September 30-October 2, 2009, Revised Selected Papers, Goel, S. (Ed.). Vol. 31. Springer, Berlin, Heidelberg, pp: 161-170.

Li, C., W. Jiang and X. Zou, 2009. Botnet: Survey and case study. Proceedings of the 4th International Conference on Innovative Computing, Information and Control, December 7-9, 2009, Kaohsiung, Taiwan, pp: 1184-1187.

Liao, W.H. and C.C. Chang, 2010. Peer to peer botnet detection using data mining scheme. Proceedings of the International Conference on Internet Technology and Applications, August 20-22, 2010, Wuhan, China, pp: 1-4.

Liu, L., S. Chen, G. Yan and Z. Zhang, 2008. BotTracer: Execution-based bot-like malware detection. Proceedings of the 11th International Conference on Information Security, September 15-18, 2008, Taipei, Taiwan, pp: 97-113.

Masud, M.M., J. Gao, L. Khan, J. Han and B. Thuraisingham, 2008a. 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, May 12-14, 2008, Oak Ridge, TN., USA.

Masud, M.M., T. Al-Khateeb, L. Khan, B. Thuraisingham and K.W. Hamlen, 2008b. Flow-based identification of botnet traffic by mining multiple log files. Proceedings of the 1st International Conference on Distributed Framework and Applications, October 21-22, 2008, Penang, Malaysia, pp: 200-206.

Mielke, C.J. and H. Chen, 2008. Botnets and the cybercriminal underground. Proceedings of the IEEE International Conference on Intelligence and Security Informatics, June 17-20, 2008, Taipei, Taiwan, pp: 206-211.

Nagaraja, S., P. Mittal, C.Y. Hong, M. Caesar and N. Borisov, 2010. BotGrep: Finding P2P bots with structured graph analysis. Proceedings of the USENIX Security Symposium, August 11-13, 2010, Washington, DC., USA., pp: 1-16.

Nivargi, V., M. Bhaowal and T. Lee, 2009. Machine learning based botnet detection. CS 229 Final Project Report. http://cs229.stanford.edu/proj2006/NivargiBhaowalLee-MachineLearningBasedBotnetDetection.pdf

Provos, N., 2004. A virtual honeypot framework. Proceedings of the 13th USENIX Security Symposium, August 9-13, 2004, San Diego, CA., USA.

Rahim, A. and F.T. Bin Muhaya, 2010. Discovering the botnet detection techniques. Proceedings of the International Conferences Security Technology, Disaster Recovery and Business Continuity, December 13-15, 2010, Jeju Island, South Korea, pp: 231-235.

Ramachandran, A., N. Feamster and D. Dagon, 2006. Revealing botnet membership using DNSBL counter-intelligence. Proceedings of the 2nd Conference on Steps to Reducing Unwanted Traffic on the Internet, July 7, 2006, San Jose, CA., USA., pp: 1-6.

Rieck, K., G. Schwenk, T. Limmer, T. Holz and P. Laskov, 2010. Botzilla: Detecting the phoning home of malicious software. Proceedings of the ACM Symposium on Applied Computing, March 22-26, 2010, Sierre, Switzerland, pp: 1978-1984.

Robiah, Y., S.S. Rahayu, M.M. Zaki, S. Shahrin, M.A. Faizal and R. Marliza, 2009. A new generic taxonomy on hybrid malware detection technique. Int. J. Comput. Sci. Inform. Secur., 5: 56-61.

Rostami, M.R., B. Shanmugam and N.B. Idris, 2011. Analysis and detection of P2P botnet connections based on node behaviour. Proceedings of the World Congress on Information and Communication Technologies, December 11-14, 2011, Mumbai, pp: 928-933.

Saha, B. and A. Gairola, 2005. Botnet: An overview. CERT-In White Paper, CIWP-2005-05, pp: 240.

Schonewille, A. and D.J. van Helmond, 2006. The domain name service as an IDS. Master Project University of Amsterdam, Netherlands, February, 2006.

Stinson, E. and J.C. Mitchell, 2007. Characterizing bots' remote control behavior. Proceedings of the 4th International Conference on Detection of Intrusions and Malware and Vulnerability Assessment, July 12-13, 2007, Lucerne, Switzerland, pp: 89-108.

Strayer, W.T., D. Lapsely, R. Walsh and C. Livadas, 2008. Botnet Detection based on Network Behavior. In: Botnet Detection: Countering the Largest Security Threat, Lee, W., C. Wang and D. Dagon (Eds.). Springer, New York, USA., ISBN-13: 9780387687667, pp: 1-24.

Stringhini, G., T. Holz, B. Stone-Gross, C. Kruegel and G. Vigna, 2011. BOTMAGNIFIER: Locating spambots on the internet. Proceedings of the 20th USENIX Conference on Security, August 8-12, 2011, USENIX Association Berkeley, CA., USA., pp: 28.

Villamarin-Salomon, R. and J.C. Brustoloni, 2008. Identifying botnets using anomaly detection techniques applied to DNS traffic. Proceedings of the 5th IEEE Consumer Communications and Networking Conference, January 10-12, 2008, Las Vegas, NV., USA., pp: 476-481.

Villamarin-Salomon, R. and J.C. Brustoloni, 2009. Bayesian bot detection based on DNS traffic similarity. Proceedings of the ACM Symposium on Applied Computing, March 8-12, 2009, Honolulu, HI., USA., pp: 2035-2041.

Wang, P., B. Aslam and C.C. Zou, 2010. Peer-to-Peer Botnet. In: Handbook of Information and Communication Security, Stavroulakis, P. and M. Stamp (Eds.). Springer, Berlin, Heidelberg, ISBN: 978-3-642-04116-7, pp: 335-350.

Wang, W., B. Fang, Z. Zhang and C. Li, 2009. A novel approach to detect IRC-based botnets. Proceedings of the International Conference on Networks Security, Wireless Communications and Trusted Computing, April 25-26, 2009, Wuhan, Hubei, China, pp: 408-411.

Wei, L., M. Tavallaee and A.A. Ghorbani, 2009. Automatic discovery of botnet communities on large-scale communication networks. Proceedings of the 4th International Symposium on Information, Computer and Communications Security, March 10-12, 2009, Sydney, Australia, pp: 1-10.

Westervelt, R., 2009. Conficker botnet ready to be split, sold. February 26, 2009. http://searchsecurity.techtarget.com/news/1349282/Conficker-botnet-ready-to-be-split-sold.

Wurzinger, P., L. Bilge, T. Holz, J. Goebel, C. Kruegel and E. Kirda, 2009. Automatically generating models for botnet detection. Proceedings of the 14th European Symposium on Research in Computer Security, September 21-23, 2009, Saint-Malo, France, pp: 232-249.

Xie, Y., F. Yu, K. Achan, R. Panigrahy, G. Hulten and I. Osipkov, 2008. Spamming botnets: Signatures and characteristics. Proceedings of the ACM SIGCOMM Conference on Data Communication, August 17-22, 2008, Seattle, WA., USA., pp: 171-182.

Yu, F., Y. Xie and Q. Ke, 2010. SBotMiner: Large scale search bot detection. Proceedings of the 3rd ACM International Conference on Web Search and Data Mining, February 3-6, 2010, New York, USA., pp: 421-430.

Zang, Y., X. Hu and K.G. Shin, 2010. Detection of botnets using combined host- and network-level information. Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks, June 28-July 1, 2010, Chicago, IL., USA., pp: 291-300.

Zeidanloo, H.R. and A.B.A. Manaf, 2010. Botnet detection by monitoring similar communication patterns. Int. J. Comput. Sci. Inform. Secur., 7: 36-45.

Zeidanloo, H.R., M.J.Z. Shooshtari, P.V. Amoli, M. Safari and M. Zamani, 2010a. A taxonomy of botnet detection techniques. Proceedings of the 3rd IEEE International Conference on Computer Science and Information Technology, Volume 2, July 9-11, 2010, Chengdu, China, pp: 158-162.

Zeidanloo, H.R., F. Hosseinpour and F.F. Etemad, 2010b. New approach for detection of IRC and P2P botnets. Int. J. Comput. Electr. Eng., 2: 1029-1038.

Zhang, J., R. Perdisci, W. Lee, U. Sarfraz and X. Luo, 2011. Detecting stealthy P2P botnets using statistical traffic fingerprints. Proceedings of the IEEE/IFIP 41st International Conference on Dependable Systems and Networks, June 27-30, 2011, Hong Kong, pp: 121-132.