# Recognizing P2P Botnets Characteristic Through TCP Distinctive Behaviour

Raihana Syahirah Abdullah, Mohd Zaki Mas’ud, Mohd Faizal Abdollah, Shahrin Sahib, Robiah Yusof
Faculty of Information and Communication Technology
Universiti Teknikal Malaysia Melaka,
Hang Tuah Jaya, 76100 Durian Tunggal, Melaka.

Email: rasyahb@gmail.com, {zaki.masud, faizalabdollah, shahrinsahib, robiah}@utem.edu.my

***Abstract*— Botnet has been identified as one of the most emerging threats to the Internet users. It has been attracted much attention and gives a big threat in network security. Through the year a number of Botnet variants have been introduced and the most lethal variants are known as peer-to-peer (P2P) botnets which able to camouflaging itself as the benign P2P application. This evolution of Botnet variants has made it harder to detect and shut down. Alike any network connection, p2p similarly using TCP to initialize the communication between two parties. Based on this reason, this paper investigates the network traffic characteristics of normal P2P connection and P2P botnets through the TCP connection initialize or received between the bot to the bot master. The proposed mechanism detects and classifies the P2P botnet TCP connection behaviour from the normal P2P network traffic. This can be used for early warning of P2P botnet activities in the network and prevention mechanism.**

***Keywords-P2P, Botnets, P2P Botnets, TCP***

## 1.0 INTRODUCTION

Nowadays people are heavily dependent on the Internet, however the advancement of the services offered by the Internet has 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 objective of the exploitation is certainly motivated by financial and political objectives. This global Internet threat is cause by collection of compromised computer or Botnet, remotely control by a perpetrator that can be located anywhere across the globe. Its distributed behaviour has made them a launching platform for several cyber-attack.

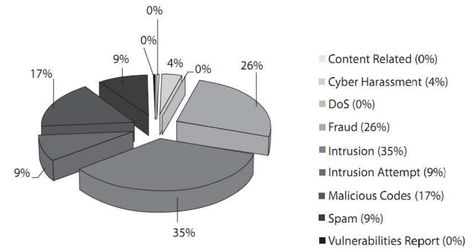


Figure 1: Percentage of Security Incidents Quarter 2 2010 from eSecurity MyCERT [1, 2]

The threat of Botnet is still at large and there is a need to address this problem. According to Malaysian Computer Emergency Response Team (MyCERT) in Quarter 2 2010 they have handled 277 reports related to mali cious code activities, this represent 17% out of the total number of security incidents [1, 2], this is illustrated in figure 1. Some of the malicious code security incidents handled is active botnets controllers, hosting of malware or malware configuration files on compromised machines and malware infections to computers.

The combination of the botnet with current technology such as IRC, HTTP and peer to peer (P2P) has made them silently organize their tactic hidden 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.

However, P2P still initialize their connection through TCP connection and thus there are still opportunities to classify the P2P botnet behaviour using the anomalies detection approach. This research focuses on how the P2P botnets can be detected with analysing abnormal characteristic changes in network traffic behaviour. This study only focuses on the TCP connection and is a part of ongoing research on studying the behaviour of P2P botnets.

This paper is organized as follows. Section 2 provides details background on the fast attack detection, P2P botnets and TCP flag parameters that is use to indicate malicious activity. Section 3 elaborates the methodologies and testbed use in segregating the P2P normal and P2P botnets network traffic. The findings and analysis are presented in Section 4. Finally, Section 5 concludes and discusses further directions of this work.

## 2.0 BACKGROUND

This paper presented an approach to detect and classifies P2P botnet activity through TCP distinctive behaviour. This preliminary study has an objective to find an early indication of botnet activities within the organization network so that any auxiliary connection between the bot and the botmaster can be prevented. Early detection of any malicious activity is crucial in defending the network from any additional damage, the concept of early detection is explained in the next subsection.

### A. Fast Attack Detection

According to [3], an attack to a network infrastructure consist of 5 phases, which are reconnaissance, scanning, gaining access, maintaining access and covering tracks. The first two phases is an initial stage of an attack and it does involve scanning and probing network traffic for information on the vulnerabilities of the targeted machine. Faizal et. al [4] has classified this initial stage into fast and slow attack, according to the research the fast attack detection is essential in order to eliminate the following action of an attack. The research proposed a new approach in detecting fast attack using a threshold value. The threshold value is obtained using observation and experimental technique.

The Threshold value is then verified using statistical control process approach in which it then can be used to diffrentiate the normal and abnormal behavior in a network traffic. Based on this, this research is aim to find the significance attribute from the network traffic that can be used to generate a treshold value which can differentiate a normal P2P activity and abnormal P2P activity.

### B. P2P Network & Application

The main interpretation of Peer-to-Peer (P2P) is that nodes are able to direct exchange resources and services between themselves. However, a more encompassing definition has been suggested is P2P is a class of applications that takes advantage of resources – storage, cycles, content, human presence that available at the edges of the Internet [5]. There are many protocols available for P2P networks, each differing in the way nodes first join the network and the role they later play in passing traffic along. Some popular protocols are BitTorrent, WASTE and Kademia [6]. In recent years, there has been a rise of research efforts to design P2P networks and its applications. From the observation and survey made to the recent P2P applications, it is found that the top 10 most popular P2P applications grouped by the file sharing applications category are BitTorrent, uTorrent, Vuze, BitComet, Tixati, Deluge, LimeWire, FrostWire, e-Mule and Ares Galaxy. the available,

### C. Botnets

Nowadays, the most serious manifestation of advanced malware is Botnets [7]. Botnets are a very real and quickly evolving problem that is still not well understood or studied. Botnets 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 [8]. The C&C controlling the bots are mostly malicious in nature and can be illegally controls the computing resources. The malicious behaviours of botnets create widespread security analysis and safety issues that propagating cyber crime. According to SearchSecurity.com website, a report from Russian-based Kaspersky Labs, botnets currently pose the biggest threat to the Internet and a report from Symantec came to a similar conclusion [9, 10].

### D. P2P Botnets

P2P botnets 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 botnets [11]. P2P botnets 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 botnets 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 figure 2.

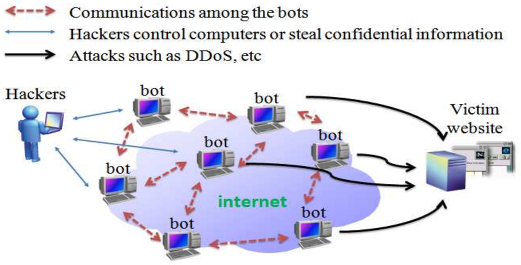

Communications among the bots
Hackers control computers or steal confidential information
Attacks such as DDoS, etc
Hackers
bot
bot
bot
bot
bot
bot
bot
internet
Victim website

Figure 2: P2P Botnets Operation [12]

### E. TCP Protocol

Transmission Control Protocol (TCP) is responsible for transferring data from one system to another. The main function of TCP is dividing the data into pieces and labels them with sequence numbers for proper data delivery on a network. According to Clarke G. E. [13], there are 8 flags; FIN, SYN, RST, PSH, ACK, URG, ECE, CWR in TCP flag. Basically, these flags have decimal numbers and description as Table 1.

Table 1: TCP Flag & Control Section

| TCP Flags Bit | Control Sections | Corresponding Decimal | Description |
|---|---|---|---|
| 8 | CWR | 128 | Indicate that the congestion window has been reduced |
| 7 | ECE | 64 | Indicate that a CE notification was received |
| 6 | URG | 32 | Indicates that urgent pointer is valid that often caused by an interrupt |
| 5 | ACK | 16 | Indicates the value in acknowledgement is valid |
| 4 | PSH | 8 | Tells the receiver to pass on the data as soon as possible |
| 3 | RST | 4 | Immediately end a TCP connection |
| 2 | SYN | 2 | Initiate a TCP connection |
| 1 | FIN | 1 | Gracefully end a TCP connection |

In line with that, Ezzeldin H. [14] has covered out the TCP Flag combination that probably performs to attack the network by an illegal attacker. A list of TCP Flag combination parameters that needs to give attention are:

a) TCP SYN (Half Open) Scan (tcp.flags==2)
b) TCP SYN/ACK Scan (tcp.flags==18)
c) TCP FIN Scan (tcp.flags==1)
d) TCP XMAS Scan (tcp.flags==41)
e) TCP NULL Scan (tcp.flags==0)

These parameters are an indicator that a malicious activity is luring in the network. This paper utilizes this parameter in differentiating a normal P2P and abnormal P2P.

## 3.0 IMPLEMENTATION

This section will describe the methodology and the testbed environment used in this study.

### *A. Proposed Framework*

The framework used in this study is P2P Botnets Detection Framework that depicted in Figure 4 which involves five main phases: P2P Network Traffic, Filtering, Traffic Monitoring, Malicious Activity Detector and Analyzer [15].

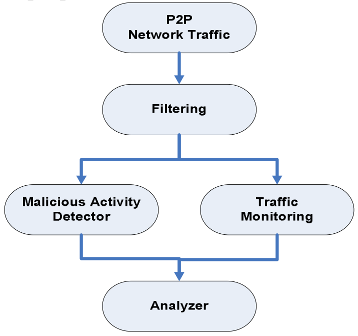


Figure 4**:** General P2P Botnet Detection Framework [15]

To improve the detection, the study also combined the general P2P botnet detection framework with the P2P botnet detection model proposed by L. Dan et al. [16] as depicted in figure 5. The model is divided into three sequent steps: detection of the P2P-nodes, clustering of P2P-nodes and detection of the botnets action. The output of the previous step is the input of the next step.

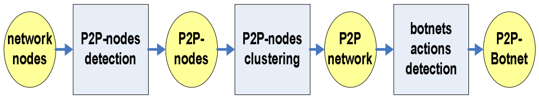


Figure 5: P2P botnet detection model

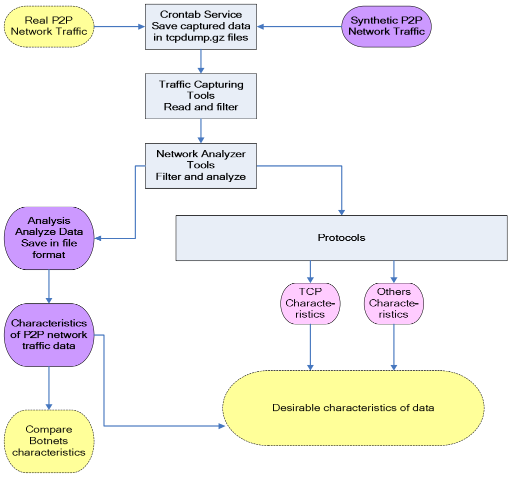


Figure 6: Modified P2P Botnet Detection Framework

The proposed framework for this study is depicted in figure 6. The modified framework has detailed out the filtering mechanism by differentiating the protocol used in the network traffic and comparison is made at the end of the experiment to detect and classifies the P2P botnet characteristics through TCP protocol. The framework started the experiment by setting up a network testbed to simulate a network environment running a normal P2P application and a network environment running a P2P application that has been effected with P2P botnet or called as abnormal P2P traffic. The captured dataset are labelled with P2P normal network traffic, top five P2P normal network traffic and P2P botnets malicious traffic.

In order to acquire the P2P normal network traffic, the updated antivirus is activated on each node to ensure there are no viruses and worms activities in the traffic. The captured dataset is then analyzed using a network analysing tools. The analysis is restricted only to TCP protocols. Once the normal traffic is captured the network testbed are then running infected P2P application and during this session the antivirus is deactivated. Both of the captured dataset is then compared to find the distinctive behaviour of P2P botnet.

### *B. Network Testbed Configurations*

Figure 7 illustrated the network testbed logical design used in this research; similar configuration has been used by Faizal [17]**.** The testbed used in this research consist of one router, two switches, six personal computers that placed with a fresh installation of Windows XP 32-bit and one server to performed the capturing packet process. Three different testbed environments have been run on the testbed and each environment run typically 12–120 hours long. The three network testbed environment implemented in the research are network environment with P2P normal configuration, network environment with Top six P2P normal configurations and network environment with P2P botnets configuration that run with ten P2P botnets infected files which is provided by the MYCERT of CyberSecurity Malaysia. Among the P2P botnet variants tested on this testbed are Conficker.B&C, Allaple, Palevo, Rbot and kido.

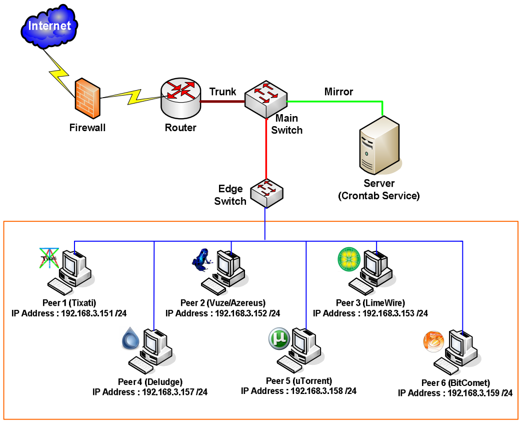

Internet
Firewall
Router
Trunk
Main Switch
Mirror
Server (Crontab Service)
Edge Switch
Peer 1 (Tixati) IP Address : 192.168.3.151 /24
Peer 2 (Vuze/Azereus) IP Address : 192.168.3.152 /24
Peer 3 (LimeWire) IP Address : 192.168.3.153 /24
Peer 4 (Deludge) IP Address : 192.168.3.157 /24
Peer 5 (uTorrent) IP Address : 192.168.3.158 /24
Peer 6 (BitComet) IP Address : 192.168.3.159 /24

Figure 7: Testbed Setup

## 4.0 ANALYSIS RESULT VALIDATION

The analysis approach discover the level of analysis in Data Link Layer in which the analysis is done on every single packet captured in order to distinguish whether its payload is malicious or spam, whether it corresponds to a remote check for vulnerabilities, or whether it follows unusual conventions with respect to flags and TCP options.

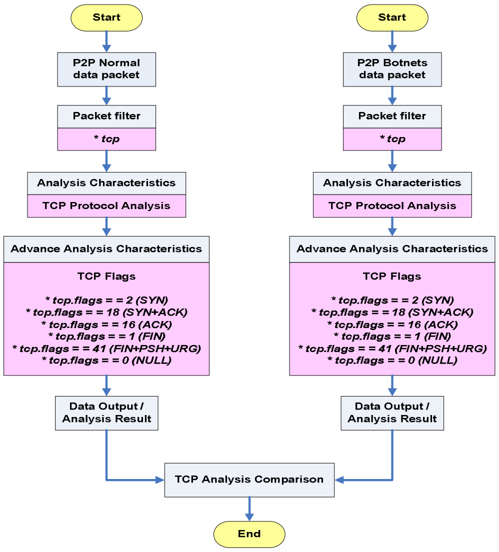


Figure 8: TCP Flag Analysis Process

### A. *TCP Flag Analysis Process*

The TCP analysis process illustrated in figure 8 started with the performing of analysis in both P2P normal and P2P botnets data packet. Each of data packets will be filtered based on TCP connection made by the host especially on TCP flags characteristics. Then the analysis result from each of data packets will be compared to distinguish between P2P normal and P2P botnets.

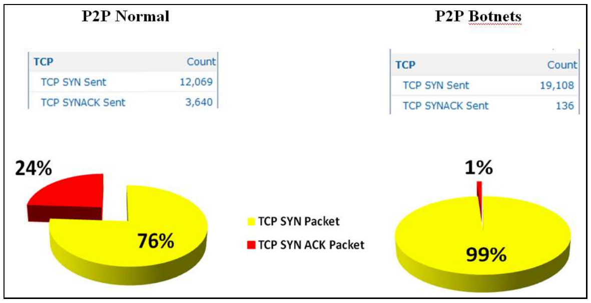
### B. *TCP Flag Analysis Result*

From the analysis it is found that there are significant different between a normal P2P traffic and abnormal P2P traffic. The details of the analysis are described in Table 2.

Table 2: Comparison of TCP Flag Analysis Result

| | |
|---|---|
| **(a) Comparison on TCP SYN (tcp.flags = = 2) and TCP SYN/ACK (tcp.flags = = 18)** | |
| **P2P Normal** | **P2P Botnets** |
| Even though, the TCP SYN flood attack occurred in P2P normal but it was not much compared to P2P botnets. | P2P botnets data captured was resulted TCP SYN flag (tcp.flags = = 2) filter shown the larger number of packet compared to the packet number in SYN/ACK (tcp.flags = = 18) filter. Happen when attackers send multiple SYN requests to victim server rather than SYN/ACK responses apply. DDoS attacks takes advantage of the half open state possibly scanning process. |
| **(b) Comparison on TCP FIN Scan (tcp.flags = = 1)** | |
| **P2P Normal** | **P2P Botnets** |
| Does not have TCP FIN Scan (tcp.flags = = 1). | Have a TCP FIN Scan (tcp.flags = = 1) to confuse the targets. Attackers use this approach because they know that many firewalls typically not necessary guard against FIN segments. |
| **(c) Comparison on TCP XMAS (tcp.flags = = 41)** | |
| **P2P Normal** | **P2P Botnets** |
| Does not have TCP XMAS Scan (tcp.flags = = 41). | Have a TCP XMAS Scan (tcp.flags = = 41). Combination of FIN+PSH+URG flags. P2P botnets will have a TCP XMAS Scan which is should never be seen on normal network. So if have a single XMAS flagged packet, then attacker might use this confusing to make scanning process and run malicious programs for any intended purposes. |
| **(d) Comparison on TCP NULL (tcp.flags = = 0)** | |
| Does not have TCP NULL Scan (tcp.flags = = 0). | Have a TCP NULL Scan (tcp.flags = = 0). Should never ever see an NULL packet on a normal network for any reason because it is illegal to have a packet with no flags set. If the TCP NULL Scan is retrieved means that attacker might use this illegal flags to run malicious programs for any intended purposes. - |

The result of the normal and abnormal P2P network traffic can be illustrated in form of pie chart as depicted in figure 9 and figure 10. Figure 9 shown that there are TCP SYN flood attack occurred in P2P normal but the number of occurrence is 23% higher if it is infected with P2P botnet. The same result is also shown in the Overall TCP Flags Percentage, the percentage of abnormal TCP connection is increasing to 39% higher in the abnormal P2P data traffic as illustrated in figure 10.



| TCP | Count |
|---|---|
| TCP SYN Sent | 12,069 |
| TCP SYNACK Sent | 3,640 |

| TCP | Count |
|---|---|
| TCP SYN Sent | 19,108 |
| TCP SYNACK Sent | 136 |

Figure 9: TCP SYN Flooding Percentage

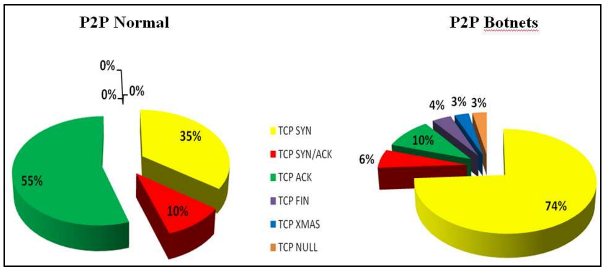


Figure 10: Overall TCP Flags Percentage

## 5.0 Conclusion and Future Work

This study presents a new approach to recognize P2P botnets. The proposed detection technique is based on TCP Flags combination in TCP FIN, TCP XMAS & TCP NULL. The study analyzed and validates a set of captured packet from a network testbed. The research also identifies the characteristics of P2P botnets, the P2P network principles, functions, capabilities and applications. In line with that, the P2P botnets files that are provided by CyberSecurity Malaysia that consist of Conficker.B, Kido, Allaple.L and Rbot variant are successfully detected.

This is an on going research on finding a new approach of detecting and classifying P2P botnet in the early stage of infections through anomalies detection. The significant different between the normal and abnormal P2P traffic from the testbed show it is possible to detect P2P botnet activities through TCP distinctive behaviour. In the near future we will look at the others network protocol such as UDP,and DNS.

## 6.0 References

[1] eSecurity Cyber Security Malaysia, *MyCert 2nd Quarter 2010 Summary Report. Volume 23* [Online] Retrieved on January 2011 from http://www.cybersecurity.my/data/content_files/12/725.pdf?.diff=1280302183

[2] eSecurity Cyber Security Malaysia, *MyCert 1st Quarter 2010 Summary Report. Volume 22* [Online] Retrieved on January 2011 from http://www.cybersecurity.my/data/content_files/12/692.pdf?.diff=1272440150

[3] Certified Ethical Hacker (CEH) Module, 2007.

[4] Faizal M. A., Mohd Zaki M., Shahrin S., Robiah Y, Siti Rahayu S., Nazrulazhar B.: Threshold Verification Technique for Network Intrusion Detection System. *(IJCSIS) International Journal of Computer Science and Information Security*, Vol. 2, No. 1, 2009

[5] Quang Hieu Vu, Mihai Lupu, Beng Chin Ooi, "Peer-to-Peer Computing: Principles and Application." *New York: Springer-Verlag*, 2010

[6] Grizzard J. B., *Peer-to-Peer Botnets: Overview and Case Study.* [Online] Retrieved on January 2011 from http://www.usenix.org/event/hotbots07/tech/full_papers/grizzard/grizzard.pdf

[7] 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

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

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

[10] 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

[11] 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

[12] 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

[13] Clarke G. E., "CCENT Certification All-In-One for Dummies." Indianapolis, USA: Wiley Publishing, 2011

[14] Ezzeldin H. (2010). *Penetration Testing: Scanning using Nmap Part I*[Online] Retrieved on Mac 2011 from http://haymanezzeldin.blogspot.com/2008/02/scanning-using-nmap-part-1.html

[15] Hossein R. Z. et al. (2010). "A Proposed Framework for P2P Botnet Detection.", *IACSIT International Journal of Engineering and Technology*, Vol.2, No.2, April 2010

[16] Dan Liu; Yichao Li; Yue Hu; Zongwen Liang; , "A P2P-Botnet detection model and algorithms based on network streams analysis," *Future Information Technology and Management Engineering (FITME), 2010 International Conference on* , vol.1, no., pp.55-58, 9-10 Oct. 2010

[17] Mohd Faizal Abdollah, "Fast Attack Detection Technique For Network Intrusion Detection System". Ph. D. Thesis. Universiti Teknikal Malaysia Melaka, Malaysia,2009