European Journal of Scientific Research
ISSN 1450-216X / 1450-202X Vol. 118 No 1 January, 2014, pp.75-85
http://www.europeanjournalofscientificresearch.com

Tracing the P2P Botnets Behaviours via Hybrid Analysis Approach

Raihana Syahirah Abdullah
Faculty of Information and Communication Technology Universiti Teknikal Malaysia Melaka Hang Tuah Jaya, 76100 Durian Tunggal, Melaka
E-mail: rasyahb@gmail.com

Faizal M.A
Faculty of Information and Communication Technology Universiti Teknikal Malaysia Melaka Hang Tuah Jaya, 76100 Durian Tunggal, Melaka
E-mail: faizalabdollah@utem.edu.my

Zul Azri Muhamad Noh
Faculty of Information and Communication Technology Universiti Teknikal Malaysia Melaka Hang Tuah Jaya, 76100 Durian Tunggal, Melaka
E-mail: zulazri@utem.edu.my

Abstract

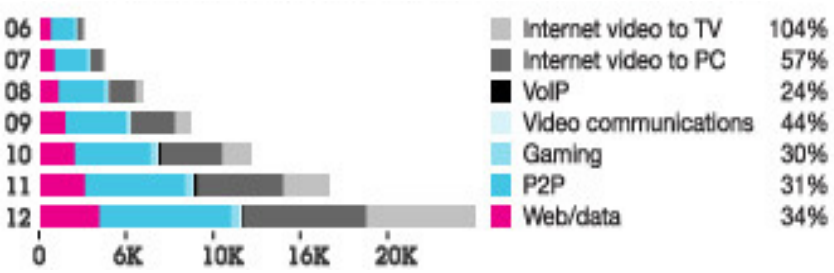
P2P botnets has become central issue that threatens global network security. The unification of botnets and P2P technology make it more powerful and complicated to detect. P2P botnets generally known with abnormal traffic behaviours may highly impact the networks operation, network security and cause financial losses. In order to detect these P2P botnets, a highly-profile investigation on flow analysis is necessary. We consider hybrid analysis approach that integrate both static analysis and dynamic analysis approach. The hybrid analysis will be used in profiling the P2P behaviours and characteristics. Then, the findings of analysis results will contributes on P2P botnets behaviour pattern that will be used in constructing the general model of P2P botnets behaviour. Through the findings, this paper proposes a general P2P botnets behaviour model. The proposed model will be beneficial to further work on P2P botnets detection techniques.

Keywords: P2P Botnets, P2P Security, P2P Botnets Hybrid Analysis, Static Analysis, Dynamic Analysis, IDS

I. Introduction

The applications of P2P network become more valuable when meet the business demand and personal needs. P2P technology offers direct access to information and services with lowest cost, saving time and optimization of Internet usage to user. Moreover, most peer is a PC owned and controlled by users. According to [1], P2P technology minimizes the workload on servers and maximizes overall network performance. P2P also has been seen as one of internet traffic trends as illustrated in figure 1 that become interesting and exciting applications where its builds a direct link between users. Currently, there are several applications that uses P2P as a backbone includes P2P online shopping (Smart Peer), P2P software agents (Consilient), P2P collaboration (Groove Networks, Ikimbo), P2P file sharing (Freenet) and P2P music files (Morpheus).

Figure 1: Global Internet Traffic Trends 2006-2012[2]



However, P2P technology itself is not 100% safe whereby it is exposing to intrusion attemption. Recently, P2P network raises serious concerns with malicious activity occurs in the P2P application that known as P2P botnets. P2P botnets initially begin with injection codes by malicious bots called as botnets. As highlighted by Kindsight [3], botnets were major issues throughout 2012 with 4 of the top 5 threats being bot-related infections and almost 50% of infected home networks having a botnets issue. Then, P2P botnets used the motivation of P2P technology to inject their vulnerable codes together with exchanging files. P2P botnets are exists in centralized and distributed communication and become as benign application. The malicious code activities in P2P botnets subsequently make it resilient, more complicated and robust to detect. Attacker have been used P2P networks for transmission of botnets codes and recruited other bots. Each infected bots is capable to communicate to other bots by receiving and passing on commands, updates and download codes to the other bots. Therefore, the cyber defense critically demand a new Computational Intelligence (CI) techniques to tracking the P2P botnets since the traditional methods of intrusion detection are already being foiled by P2P botnets [3].

Figure 2: Top 20 of Home Network Infections and High Level Threats [3]

Position	Name	Threat Level	% of Total	Last Quarter
1	Botnet.ZeroAccess2	High	20.19%	2
2	Spyware.MyWebSearchToolbar	Moderate	9.94%	4
3	Adware.GameVance	Moderate	6.75%	3
4	Backdoor.TDSS	High	5.93%	5
5	Trackware.Binder	High	5.41%	7
6	Downloader.Agent.TK	High	4.75%	11
7	Hijacker.StartPage.KS	Moderate	4.58%	9
8	Adware.MarketScore	Moderate	3.31%	8
9	Botnet.Alureon.A	High	2.54%	10
10	BankingTrojan.Zeus	High	2.37%	13
11	Backdoor.Hupigon.FI	High	2.23%	16
12	Botnet.ZeroAccess1	High	2.13%	1
13	Virus.Sality.AT	High	1.60%	-
14	Hijacker.MyWebSearch	Moderate	1.55%	12
15	ScareWare.FakeXPA	High	1.44%	-
16	MAC.Bot.Flashback.K/I	High	1.28%	15
17	Spyware.SBU-Hotbar	Moderate	1.10%	17
18	Trojan.Alureon/TDL/TDSS	High	0.89%	-
19	Adware.MediaFinder	Moderate	0.71%	-
20	Trojan.Medfos.A	High	0.59%	14

In August 2011, P2P botnets detected by Karpersky Lab experts now has the most conservative count where nearly 40,000 different public IP address [4]. At the end of the month, Kaspersky Lab detected 35 unique malicious programs loaded in targeted system. In line with that, the Karpersky Security Bulletin 2012 [4] has declared that botnets as the most interesting practice by cybercriminals in launching mass attacks for direct financial gain. Subsequently, regarding the statistics issued by Kindsight security lab malware report [3] claimed that the P2P botnets vied for the top spot on the top 20 home network infections and high level threats as depicted in figure 2. The situation becomes more

frightening when P2P botnets expected to be more resilient in 2013 as continuing to be a major problem despite takedown attempts.

The P2P botnets growth has given the bad impact to the real world. The awareness of risks in P2P botnets enables it to seriously take down with any prevention and detection scheme. The prevention and detection scheme requires essential information that mainly concentrated on P2P behaviors and characteristics. To address these issues, we investigate and observe the behavioral pattern of P2P botnets. Hence, we propose a hybrid approach to analyze and profiling the whole P2P Botnet activities and events in order to recognize the behaviour and characteristics of P2P botnets. Since hybrid is a new generic model that complement each other weaknesses and applied for solving various problems in the field of information security, we used this approach in capturing P2P behaviours and characteristics. The hybrid analysis approach is derived from the combination of static analysis approach and dynamic analysis approach.

The remainder of paper is organized as follows. In Section II, we provide details related work on the P2P botnets, its behavior and also the hybrid analysis approach that are used to indicate malicious activities and events. Section III will describe the methodology used to conduct the analysis approach. Then Section IV discusses the findings of our analysis and the proposed general P2P botnets behavior model together with entire components. Finally, the conclusion of the paper is concluded in Section V.

II. Related Work

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

A. P2P Botnets

The combination of botnets with P2P technology have made them silently organizes their hidden tactic in a benign application. Yet, this blended technology known as P2P botnets. The P2P leeches and exchanges files over the Internet make it harder to detect as it command and control centre are distributed [5]. P2P botnets engage every compromised machine acts as a peer for the others. Presentation by Charles has claimed that the P2P botnets C&C server as a new generation of botnets with encrypted communication [6].

To date, the way to help our computers from being compromised by P2P botnets, the appropriate action come only by installation of antivirus, keep on updating the software, use a strong passwords and do not give the personal information on non secure web pages. But, with a more advanced P2P botnets introduced, the signature and codes are rapidly changing make it more difficult to track down unless the signature is continuous updated. This situation make the users not solely depending on antivirus company and acquire more trust for better developed on prevention and detection scheme to get over the P2P botnets threat. This situation was agreed by [7] when researchers highlighted the importance of building the improvement on security mechanism. Thus, there are needs of sophisticated of anti P2P botnets detection in a real network environment.

B. P2P Botnets Behaviour

Most of studies have reveals the behaviours concentrated on survey and literature of the P2P botnets. They are collected the common trends and characteristics of P2P botnets from the traditional P2P variants. Zang et al [8] and Leder et al. [9] conduct a review on several P2P variants to fine the flow of classification and encounter with offensive approach. Works done by Junfeng et al [10] have come out with a complete comparison between P2P variants on several features. The study makes the comparison on Storm and Nugache as P2P variants. Only two studies focused in some technical study approach on a P2P variant. They

were studies by Donghong et al [4] and Chao et al. [11] that designed the mechanism to differentiate the P2P variants. The mechanisms are involved the command, control, infections, propagation, exploits, attack and survivability mechanism. With the selected P2P variants, they have illustrates the characterization and summarization on the particular P2P variants. These studies continually contributed much in considering the evolution of P2P botnets behaviours in general conceptual.

Furthermore, the general concept will help the researcher to have better understanding about P2P variants on how the P2P botnets will infect the host and network. This can be done by analyzing the P2P botnets itself by doing a reverse engineering. The reverse engineering analysis consists of two main approach which are static analysis and dynamic analysis. The integrated of analysis recognized as hybrid analysis will discovers the P2P behaviours and characteristics that give beneficial on understanding of P2P botnets in order to develop an effective P2P botnets detection techniques.

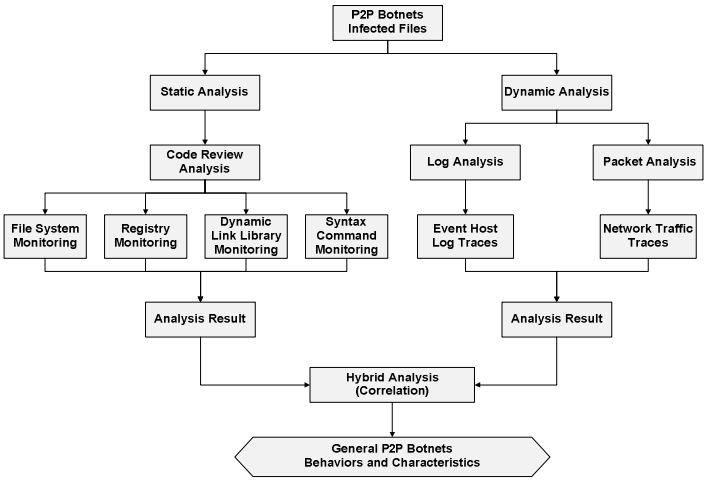
C. Hybrid Analysis Approach

In hybrid analysis approach, two of analysis approaches were combined. It is the combination of static analysis and dynamic analysis approach. Due to static analysis, it has capability to detect malicious activity before the programs been executed. This allow the raw codes of infected files can be revealed and give initial perceptions to administrator before the entire analysis is performed. Instead, dynamic analysis by chance has the ability to detect the malicious activity during and after the programs executed. The dynamic analysis essentially completes the whole analysis on fully diverse logs and network packet in a good manner. Based on analysis by [12], the combination of hybrid analysis approach has given an implication that there are complement each other weaknesses.

III. Methodology

This paper investigates several P2P botnets infected files using hybrid analysis approach. As depicted in figure 3, the hybrid analysis approach discover with two level of analysis which are static and dynamic analysis. For final hybrid analysis result, these two types of analysis approach are correlated.

Figure 3: Proposed P2P Botnets Hybrid Analysis Approach



At static analysis, analysis is done on file system, registry, dynamic link library and syntax command monitoring. This static analysis had been done in reviewing the real codes of infected files to reveal and study their true characteristics. The P2P botnets generally will create and load their code file and make the dramatic changes in registry in order to exploits the host. Then, it attempt to inject the code by execute the dynamic link library (*.dll)* and generate it to stack overflow status. Then, every single of P2P infected files was captured by their own syntax command where it will correspondent to botnets server. The important of code review

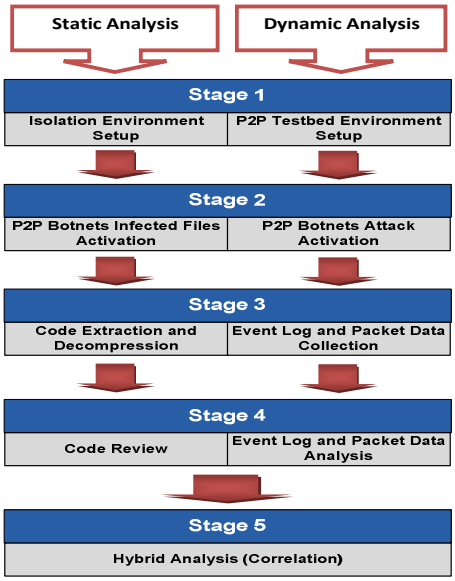
analysis is it can extract the information on system and application log on each of infected host includes the event status, process status, action status and more.

Subsequently, the dynamic analysis had been done on the event host log and network traffic dataset. The dataset has been collected by implementing the P2P testbed setup in a controlled environment. The event host log has captured by process monitor and process explorer in order to gather the information on local host. Meanwhile, the overall network traffic is captured by tcpdump service. Through this dataset, the P2P botnets behaviour and characteristic fully observed to ensure the interaction on the botnet server and the effect on each of infected files to real environment. After that, the combination of analysis result on static and dynamic analysis will be correlated together to construct the general behaviour of P2P botnets.

A. P2P Testbed Environment Setup

This analysis approach incorporates with two main components as a hybrid. This combination successfully complements each other in the real world of P2P Botnet traces. The hybrid analysis approach had been analyzed through the static analysis and dynamic analysis components. In this approach, five stages are applied to make the whole approach easier and smooth.According to our opinion, the static and dynamic analysis is divides into five different stages and shares one similar stage. The component for static analysis consists of isolation environment setup, P2P botnets infected files activation, code extraction and decompression and code review. Then, the components for dynamic analysis are P2Ptestbed environment setup, P2P botnets attack activation, event log and packet data collection and event log and packet data analysis. The last stage for both of analysis is correlates and mapped together to find the sequence of infections on identified P2P botnets. The P2P testbed environment setup is illustrates in figure 4 and will be discussed in details at following sub-section.

Figure 4: P2P Testbed Environment Analysis Design



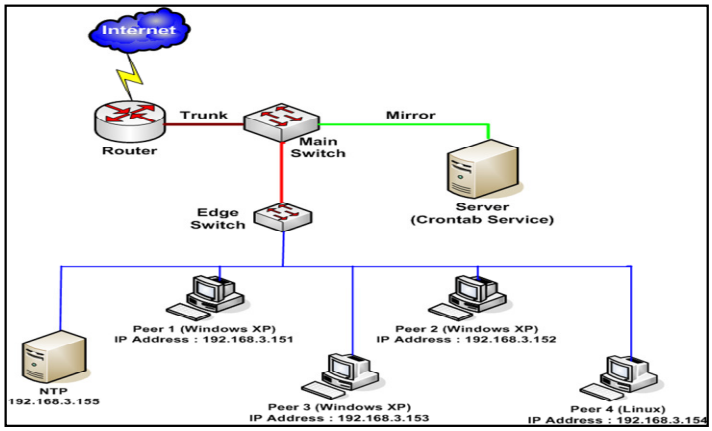
B. Static Analysis

The analysis has started with isolated the experimental setup in controlled environment. Then, every single of P2P botnets infected files were activated. At third stage, each of infected files in .exe were extracted using McAfee tools known as Bintext. Bintext is a small, fast and powerful text extractors that has capability to extract text from any kind of file. Moreover, we use UPX to make the decompression for implying any specimen code that was obfuscated in particular way. At last, the code is reviewed with gathered the specific information and behavior on each infected files including event status, process status, action status and connection status.

C. Dynamic Analysis

At first stage, the controlled environment has been implemented known as P2P testbed environment. The experimental testbed lab is conducted to capture the P2P Botnet activities with similar configuration have been used by Faizal [13]**.** The testbed used in this research consist of one router, two switches, four peer placed with a new installation of Windows XP 32-bit and Linux, one NTP server and one server to perform the capturing packet process. The activation has been done to launch the P2P botnets attack in the second stage. Afterwards, the event logs are collected by process explorer (procex) and process monitor (procmo) application provided by sys internal. Meanwhile, the network traffic was collected via tcpdump service using the crontab server. This event logs and network packet data will be analyzed through the next stage.

Figure 5: P2P Testbed Setup



D. Correlation

The principal step in correlation are finding and mapping together the P2P activities done from every infected file. The main concept of correlation phase indicates the extent to various behaviours and characteristics in both analyses: static analysis and dynamic analysis to be fluctuate together. In the above context of analysis, the revealing P2P botnets code that had found in static analysis will be mapped to the activity found in event log and network packet in dynamic analysis.

IV. Analysis and Finding

These two levels of hybrid analysis: static analysis and dynamic analysis are further investigates in this section. The hybrid analysis results will be used as a main key to outlining the P2P botnets behaviours and their characteristics. The capturing of P2P botnets behaviours and characteristics is assembled by information gathered by file, registry, dynamic link library, syntax command monitoring and the several of event log and network traffic data. Otherwise, the P2P Botnet variants tested on this testbed are Invalid Hash, Allaple, Palevo, Rbot, srvcp.exe, tnnbtib.exe and kido. The P2P Botnet infected files is provided by the MYCert of Cyber Security Malaysia. Each of P2P Botnet environment has run and been captured for 7 days long. The details of analysis and findings are discussed in following part.

A. Static Analysis

Static analysis has been enlighten the capabilities to detect the malicious activity before the programs files is running. The operation process involved in every P2P botnets infected files has thread create as its main process start. The information of P2P botnets infected files has discovered in four main components: file monitoring, registry monitoring, dynamic link library monitoring and syntax command monitoring as illustrated in figure 6.

Table 1 shows the list of operation process that occurred in the P2P botnets infected files. Operation process like *Create File, Load File, Write File* and *Delete File* are considered as dangerous event process that happen to allow the attacker replace the original files in operating systems. Here, we can see the attempting of malicious activity in trying creates an *.exe* file and delete essential files in system directory to exploits the victim host. Otherwise, the frequent changes in registry will be noticed as high possibility of malicious activity has arisen. The operation processes in registry that need to be addressed are *RegOpenKey, RegSetValue and RegCloseKey*. The *TCP/UDP Reconnect, TCP/UDP Disconnect, TCP/UDP Send* and *TCP/UDP Send* are indicates the TCP and UDP communication is luring in the network.

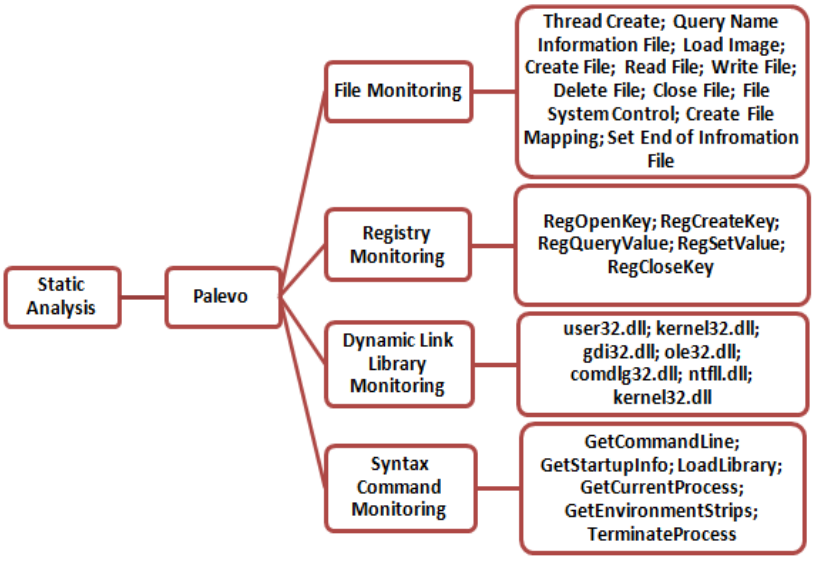
Table 1: Operation Process by P2P Botnets

	Invalid Hash	**Allaple.L**	**RBot**	**Palevo**	**srvcp**	**tnnbtib**
Thread Create	√	√	√	√	√	√
Query Name Information File	√	√	√	√	√	√
Load Image	√	√	√	√	√	√
Create File	√	√	√	√	√	√
Read File	√	√	√	√		
Load File	√	√	√			
Write File			√	√		
Delete File			√	√		
Close File	√	√	√	√	√	√
RegOpenKey	√	√	√	√	√	
RegCreateKey		√		√	√	
RegQueryValue	√	√	√	√		
RegSetValue		√	√	√	√	
RegCloseKey	√	√	√	√	√	
File System Control	√	√	√	√		
Query Open					√	
Create File Mapping	√		√	√	√	
Set End Of Information File	√	√	√	√	√	
TCP/UDP Reconnect		√			√	√
TCP/UDP Disconnect		√			√	√
TCP/UDP Receive		√				
TCP/UDP Send		√				
Dynamic Link Library	√	√	√	√	√	√
Syntax Command	√	√	√	√	√	√

The most important part that torching an intention are stack overflow occurrence that generates by *dynamic link library* (*.dll*). In fact, a stack overflow is an undesirable condition which a particular P2P botnets tries to use more memory space than the call stack has available to inject their codes. As a result, the P2P botnets excessive demand for memory space to launch such attack and the host may crash immediately. Thus, the risk of P2P botnets exploits in a maximized situation. Besides that, each of P2P botnets has their own *syntax command* from bots server to instruct the recruit bots to do the malicious task such as steal any information in host and network.

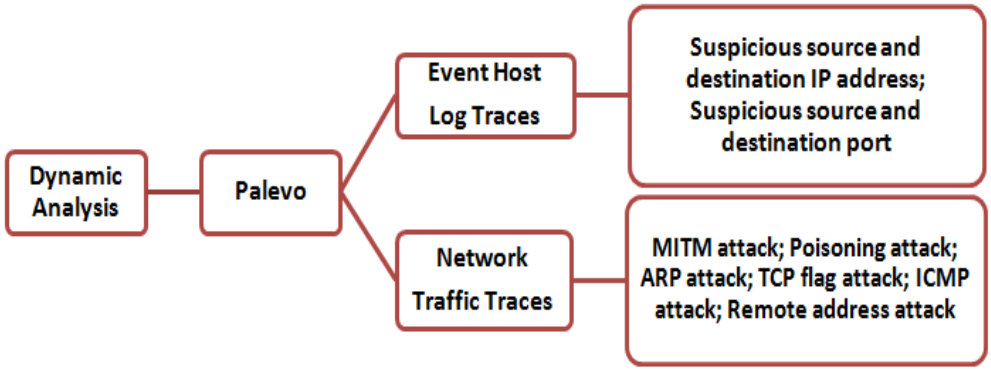
Actually, the in-depth reviewing of P2P botnets codes were revealed the details of behavior and characteristic. It can be demonstrated by an example on Palevo analysis as shown in figure 6. All of dangerous event process involved Create File, Write File and Delete File are occurred in this infected files to exploits the original directory files. Then, the significant registry which is RegOpenKey, RegSetValue and RegCloseKey also encompass make the host is expose in malicious activity. The dynamic link library become as stack overflow on user32.dll, kernel32.dll, gdi32.dll, ole32.dll, comdlg.dll and ntfll.dll. Other monitoring is syntax command as define in Figure are used by bot server to update, make connection and permit any command to launch various attack.

Figure 6: Palevo Operation Process in Static Analysis



B. Dynamic Analysis

Figure 7: Palevo Dynamic Analysis

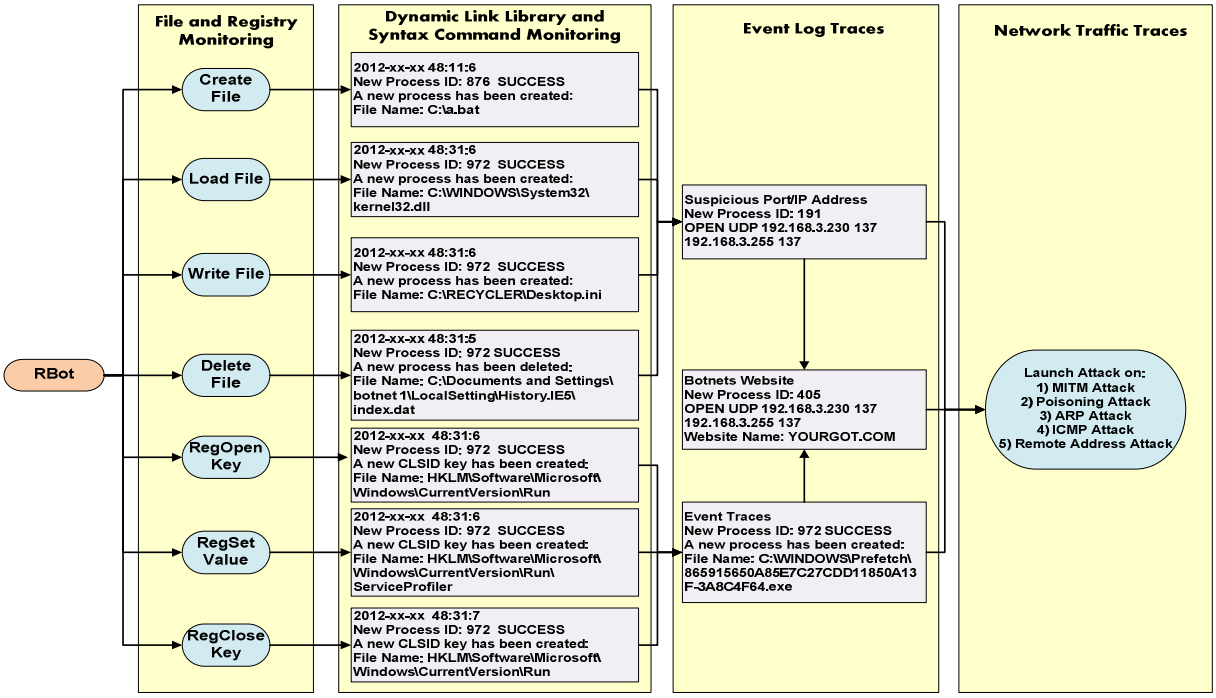


In dynamic approach, the capabilities are concern on the detection of malicious activity during or after program files execution. The P2P botnets activities are captured through the event host logs and whole network traffic. The Palevo dynamic analysis as depicted in figure 7 shows the P2P botnets attempting to contact the bots server by using vulnerable port and certain IP address as remote address. The Palevo make the connection via the bots server by receiving the command to launch a series of attack on MITM, poisoning, ARP, TCP flag and ICMP flooding attack. Yet, a similar analysis activities are also been done in Invalid Hash, Allaple.L, RBot, srvcp and tnnbtib.

C. Correlation

The recognition of P2P botnets activities has been constructed by accomplish on both of hybrid analysis which are static analysis and dynamic analysis. As discussed in previous section, this phase mapped the overall operation process with event log and network traffic traces. The correlation process contributed in creating the sequence of P2P botnets activity and event. Hence, the findings are beneficial for further purpose on build the general P2P botnets behaviour. Consequently, an overall correlation phase represent as a complete sequence of RBot activities and events are demonstrated in figure 8.

Figure 8: Correlation Process in RBot Summar



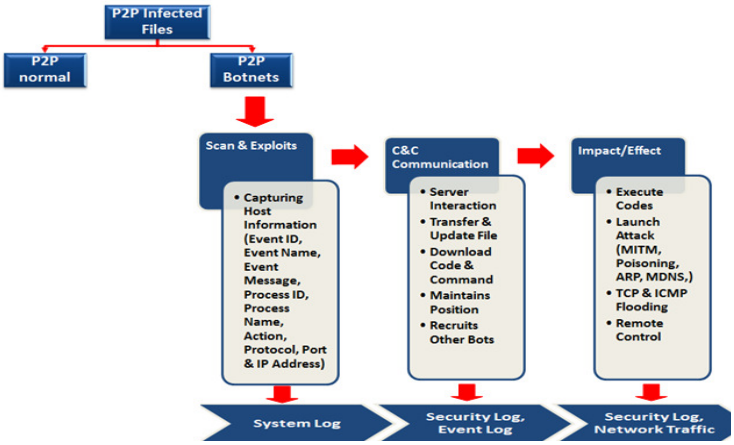
D. Proposed General P2P Botnets Behavior Model

Figure 9: Basic P2P Botnets Behavior Model

The hybrid analysis result as described in previous section is utilized to construct the P2P botnets behaviour model. The basic P2P botnets behaviours model is another variation model as suited by the paper on multi-step model done by Robiah et. al [14]. Nevertheless, the paper only focuses on malware dynamic approach that concentrated on perspective of victim and attacker. Thus, an adaptation on new edition of P2P botnets has been proposed in this research called as a basic P2P botnets behaviour model. The proposed model consists of scan and exploits, C&C communication and impact/effect as shown in Figure. The details are:

1) Scan and Exploit - P2P botnets scan the vulnerable port and suspicious IP address. Then, it had exploited the victim host and network by capturing the private and confidential information.
2) C&C Communication - P2P botnets make the connection with C&C communication that known as bots server via P2P network to establish communication among bots
3) Impact/Effect - P2P botnets launch various attack to accomplish certain malicious task

Figure 10: General P2P Botnets Behavior Model



The comprehensive P2P botnets behavior model with suitable log to be monitored essentially illustrated in figure 10. The analysis had been done through a basic of P2P botnets life cycle involving Scan & Exploit, C&C Communication and Impact/Effect phase. At first, the Scan & Exploit phase will capturing the whole details information in system log including on event ID, event name, event message, process ID, process name, action, protocol, port and IP address. Subsequently, the server interaction with C&C Communication is establish in second phase to accomplish the task on transfer and update files, download codes and command, maintains the positions and recruits other bots as a member. The logs to be monitored in second phase are security log and event log. In a final phase which is Impact/Effect, the P2P botnets will executes code to launch malicious attack, flooding attack and remote control access. This malicious event is monitored on security log and network traffic log.

V. Conclusion and Future Directions

This paper presents the hybrid approach to analyze and classify the whole P2P Botnet activities and events in order to identify the behaviour and characteristics of P2P botnets. This research combines both of analysis approach: static approach and dynamic approach to get better understanding how the P2P botnets act in real P2P network environment. The hybrid analysis result is inherited to construct the General P2P Botnets Behaviour Model. This is an ongoing research in finding effective techniques to make the detection on P2P botnets. The further directions are essentially work on P2P 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) for their invaluable supports in encouraging the authors to publish this paper.

References

[1] Alfred Wai-Sing Loo: *Peer-to-Peer Computing: Building Supercomputers with Web Technologies,* Springer Publishings, 2007

[2] IBM Support Group: *Smarter Communication*, 2013

[3] Kindsight Security Lab, *Malware Report Q4 2012* [Online] Retrieved on July 2013 from http://www.kindsight.net/sites/default/files/ Kindsight_Security_Labs-Q412_Malware_Report-final.pdf

[4] Secure List: *Kaspersky Security Bulletin 2012. Cyber Weapons* [Online] Retrieved on August 2013 from http://www.securelist.com/en/analysis/ 204792257/Kaspersky_Security_Bulletin_2012_Cyber_Weapons

[5] Donghong, S., et al. *The New Architecture of P2P-Botnet. in Cybercrime and Trustworthy Computing Workshop (CTC), 2010 Second*. 2010

[6] Charles L. : *Malware Threats in our Cyber Infrastructure*, Swiss German University inYogyakarta Indonesia, 2013

[7] Sundaram, A. *An Introduction to Intrusion Detection*. ACM , 2 (4), 3-7, 1996.

[8] Zang, X., et al.: *Botnet Detection through Fine Flow Classification*. CSE Department Technical Report CSE11-001, 2011

[9] Leder et al.: *Proactive Botnet Countermeasures Approach,* 2009

[10] Junfeng et al. : *Descriptive Model of Peer-to-Peer Botnet Structure,* International Conference on Educational and Information Technology (ICEIT), 2010

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

[12] Robiah Y. et al.: *A New Generic Taxonomy on Hybrid Malware Detection Technique,* International Journal of Computer Science and Information Security Vol. 5, no. 1 56-61, 2009

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

[14] Robiah Y.; Rahayu, S.S., et al.: *New Multi-Step Worm Attack Model*, Journal of Computing, 2 (1), pp. 1-7, 2010