ISSN 1828-6003
Vol. 8 N. 12
December 2013

International Review on Computers and Software (IRECOS)

Contents:

(continued on inside back cover)

Praise Worthy Prize

International Review on Computers and Software (IRECOS)

The ***International Review on Computers and Software (IRECOS)*** is a publication of the **Praise Worthy Prize S.r.l..**
The Review is published monthly, appearing on the last day of every month.

Published and Printed in Italy by **Praise Worthy Prize S.r.l.,** Naples, December 31, 2013.

Praise Worthy Prize

International Review on Computers and Software (I.RE.CO.S.), Vol. 8, N. 12
ISSN 1828-6003 December 2013

Analysis and Improvement Design on P2P Botnets Detection Framework

Raihana Syahirah Abdullah[1], Faizal M. A.[2], Zul Azri Muhamad Noh[3], Robiah Yusof[4]

Abstract – *Developing the P2P botnets detection framework is crucial when we trying to fight against P2P botnets. Poor detection method can lead to a failure of P2P botnets detection. Thus, it needs to be accurately functioned well. This paper reviews and evaluates various current frameworks of P2P botnets detection and analyzing the existing gaps to make improvement of P2P botnets detection framework. Based on a review that conducted manually, we report our findings and analysis has been done on different frameworks concern on P2P botnets detection. Consequently, the gap and motivations found from this reviews are discussed. Then, the P2P botnets detection framework architecture has been proposed with the new improvement been reinforced by hybrid detection technique, hybrid analyzer and in-depth hybrid analysis. Future directions of this review are to develop the P2P botnets detection system that has capability in high detection accuracy and efficiency*.

Keywords: *P2P Botnets, P2P Botnets Detection, P2P Botnets Framework, P2P Botnets Detection Criteria*

I. Introduction

Nowadays, the most serious manifestation of advanced malware is Botnet [1]. Botnet is a very real and quickly evolving problem that is still not well understood or studied.

Botnet is a collection of computers that have 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 [2]. The combination of the Botnet which blended with current technology such as IRC, HTTP and peer to peer (P2P) have made them silently organizes their hidden tactic in a benign application.

Several researches have been done to detect IRC and HTTP Botnet via network monitoring analysis and most of their activity is easy to annihilate as each of the bot are connecting to a central command and control server. Yet, the P2P is a bit harder to detect as it command and control centre are distributed same as the P2P leeches that share files over the Internet. P2P Botnet is one of the most recent phenomenon's where Cyber defence desperately needs new Computational Intelligence (CI) techniques because traditional methods of intrusion detection are being foiled by P2P Botnet [1]. P2P Botnet implies that every compromised machine in the swarm acts as a peer for the others.

In order to find the solution against the attack of the future P2P botnets, it is important to understand on how the current P2P botnets was detected by using the existing detection framework and what are the strength and weaknesses for every detection framework.

It was supported by Sundaram [3] in his paper has highlighted the importance of building a security mechanism for preventing any intrusion from hacker so that we can take action and improve the system security.

For that reason, this paper reviews the existing P2P framework then the improvement on P2P botnets detection framework architecture is proposed.

II. Related Work

II.1. P2P Botnets Detection Framework

In general, a framework is an integrated set of components that collaborate to provide a reusable architecture for related applications [4]. In line with that, a framework is a real or conceptual structure intended to serve as a support or guide for the something that expands the structure into something useful [5].

The framework often a layered structure indicating what kind of programs can or should be built and how they would interrelate. It is not only to be able to rapidly develop any application or system.

Rather, it is able to use an architectural style to inherit all its advantages which are modularity, anticipation of change, abstraction, low coupling and high cohesion [6].

That, in turn, allows us to develop more quickly because the style put us constraints and we have some predefined configurations of component arrangement.

We can also achieve faster development by means of using proven patterns and reusing framework components. P2P botnets are an emerging phenomenon that has already made a big impact [7].

Manuscript received and revised November 2013, accepted December 2013

P2P botnets detection research has been explored since P2P botnets become as the threats to the world. The earlier detection on P2P botnets contributes to the success of P2P security. The P2P botnets detection needs a crucial specification before their implementations.

Thus, it need a framework to illustrate and explains the modules, terminologies and procedure steps as an important part to make the detection. Most of the earlier studies related with P2P botnets have their own framework in order to explain the detection chronology as [8]-[14]. In fact, the existence of framework facilitates the task on P2P botnets detection.

Thus, inconclusive here the significance of constructing the framework is identified as noble part of recognize the P2P botnets attacks.

II.2. Review of the P2P Botnets Detection Framework

This section presents a review of seven types of P2P botnets detection framework that have been used as navigation on the P2P botnets detection process.

Additionally, a review on the terminologies of the developed frameworks is also presented.

A. P2P-based Detection Framework

As shown in Fig. 1, [8] provides a general detection framework focuses on P2P-based, HTTP-based and IRC-based. Developed as detection framework, it has been designed to make the detection using Artificial Immune System (AIS). Due to solving various P2P botnets problems security, AIS utilizes as a method that effectively can detect the malicious activities in P2P part.

Moreover, they are calculating Delay Time (Td) in IRC part which is a time frame between sending IRC NICK command and IRC JOIN command.

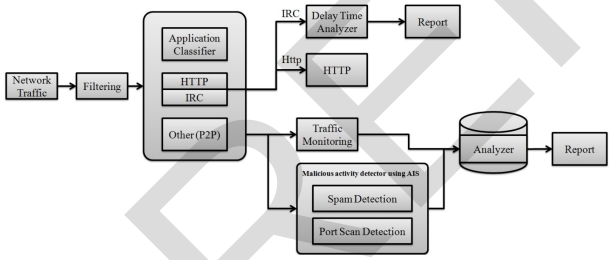

Fig. 1. P2P-based Detection Framework [8]

However, the framework passively concern on network traffic and does not rely with mined data. It is also not require any botnet specific information to make the detection. One major drawback of this framework is that the effect of different flow interval durations were not presented tend to accuracy approach is unknown.

Nevertheless, the framework fails to reveal bot server and it is has been focused on application OSI layer detection.

B. C&C Protocol-Independent Detection Framework

Yuanyuan et al. [9] have proposed a C&C protocol-independent detection framework to address the approaches function at the both level. They had considered both of the coordination within a botnet and the malicious behavior each bot exhibits at the host level and analysis on packet's payload. Subsequently, they had presented this framework that combines host-and-network level information for making detection decisions. In host-level, they employed a supervised learning algorithm or the support vector machine (SVM) to quantify its suspicion level.

Meanwhile, in network-level, they only do analysis on NetFlow data by takes the flow records direct from the router as input and generate the clustering results. Then, the data from both level were correlated by assigning the relationship between related multiple data using correlation engine.

With reference to Fig. 2, they do not have any filtering agent lead the direct network flow and host data to the analyzer. As a result, the high identification accuracy occurs in payload inspection. Although this framework can detect the real-time detection, it fails to feasible for offline detection. Another limitation with this approach is that its scalability since the approach requires runtime host-level analyzers.

Additionally, the network-analyzer looks for trigger-action patterns among hosts that may delay bots coordinated actions through waiting for random period of time.

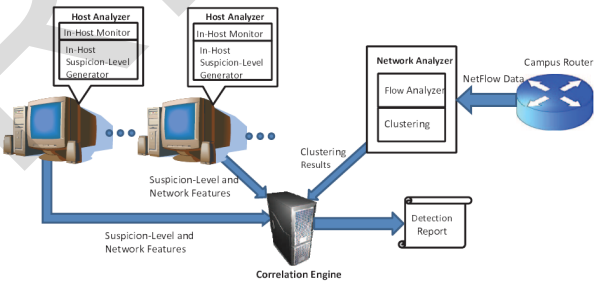

Fig. 2. C&C Protocol-Independent Detection Framework [9]

C. Botnets Detection Approach Architecture

Arshad et al. [10] have demonstrated a fully anomaly-based approach with only concern on network level to their framework as depicted in Fig. 3. Their detection systems are clusters bots with similar netflows and attacks in different time windows.

Then, they had performed the correlation process to identify bot infected hosts. It also finds behavior similarity of hosts in different properties such through netflow information.

However, one significant weakness that needs to be further enhanced is it fails to reveal bot server. They also claim that this framework has detected in real-world traces including normal traffic and several real-world botnet traces.

However, the framework does not feasible with offline detection alike as [9]. Although this framework has high detection accuracy and provides low false positive alarm, it becomes ineffective against the new P2P-based botnets.

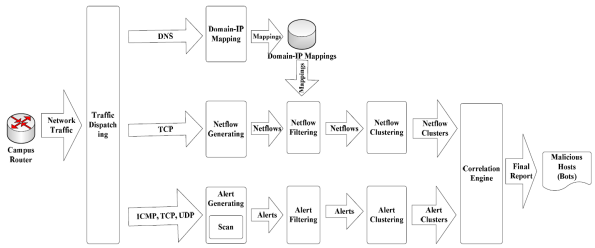

Fig. 3. Botnets Detection Approach Architecture [10]

D. General P2P Botnets Detection Framework

Chunyong and Ghorbani [11] have proposed the general P2P botnets detection framework based on association between common P2P network behaviors and host behaviors. With refer to Fig. 4, this framework have monitoring, filtering and correlation module.

At first, the monitoring had been done through both levels. Then, the detection will do filtering to classify the protocol used. At last, the framework constructed the correlation between network behaviors and host behaviors.

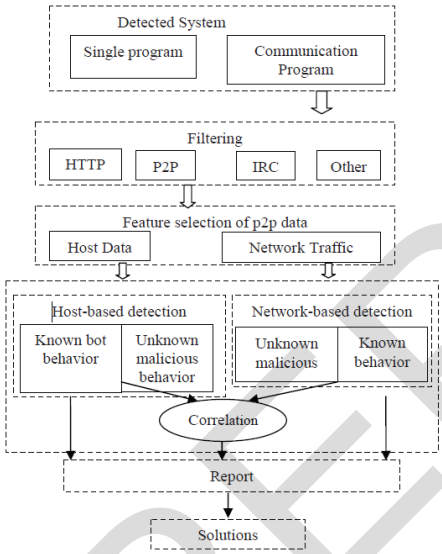

Fig. 4. General P2P Botnets Detection Framework [11]

Their result shows that the framework has better accuracy and has ability to detect some unknown P2P bots. Yet, they make no attempt and do not take into account to mining the data at first. Moreover, the framework has tended to focus only on application layer.

Another limitation is they need to deal with some problems especially in data encryptions and route selection. However, the main weakness of this framework is the failure to address the evaluation tests and results as reference to other researchers.

E. P2P Botnets Detection System

This framework [12] has focused on single detection method which is network-level detection. It able to identify stealthy P2P botnets even when malicious activities may not be observable.

At first, the framework identifies all hosts that have been engaged in P2P communications. Then, they derive statistical fingerprints to differentiate between P2P normal and P2P botnets. It can be a most comprehensive and complex detection for them.

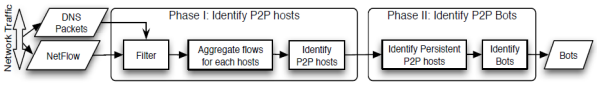

Fig. 5. P2P Botnets Detection System [12]

They claim that their experimental evaluation based on real-world data play a key role to achieve high detection accuracy with a low false positive rate.

However, it still cannot reveal the bot servers in real world as [8], [12]. Then, the analysis tends to overlook on transport and application layer. It also does not require any botnet specific information to make the detection.

F. P2P Detection Framework

The P2P detection framework proposed by [13] provides the ability that coined the framework with combination of host and network level. They are highlights on the real time detection similar to [9], [10]. At last, they also make the correlation between host and network analysis. In particular, they include the algorithm on P2P node identification, P2P network clustering, K-means P2P clustering, P2P botnet detection and correlation algorithm. However, they only depend on hybrid analyzer to make the whole detection. Apart from that, this framework is considered as simple and they are hardly to be efficient detection. By not including the crucial of filtering module, the payload inspection becomes high identification accuracy. The main drawback is they just provide the algorithm that appear failure to evaluate and validate the result from the detection as [8].

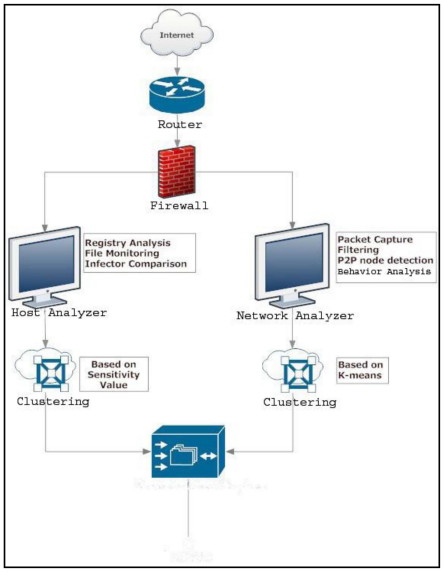

Fig. 6. P2P Detection Framework [13]

G. IPS-Based P2P Botnets Detection

Li et al. [14] have proposed a framework for P2P detection that includes a set of Irregular Phased Similarity (IPS) module.

The module has been produced by perception that the traffic generated by a P2P bot has phased similar patterns which occur at irregular intervals.

As similar to [8], [11] [12] and [14], this framework just cover on network level and focus on application layer. They have reported that this framework has capability to efficiency identify unknown P2P botnets.

However, it is only effective on detection against Storm and Waledac botnets. It proved that this framework become ineffective against the new P2P-based botnets detection.

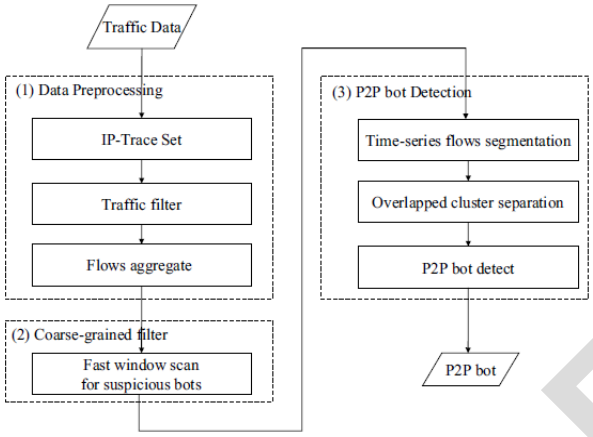

Fig. 7. IPS-Based P2P Botnets Detection [14]

Afterwards, to date, various terminologies are used to describe similar modules involved in P2P Botnets Detection Framework which can cause confusion in understanding the whole activity involved in the P2P Botnets Detection Framework.

It is important to understand the involvement of activities in each module so that the improvement P2P Botnets Detection Framework with the appropriate and relevant module can be developed. The terminology used by [8]-[14] are analyzed and it is summarized in Table below.

There are eleven different terminologies used to describe the module in the P2P Botnets Detection Framework: ***Monitoring, Filtering, Classifier, Pre-processing,*** *Mined Data, Analysis Approach, Activity Detector, Host Analyzer, Network Analyzer, Correlation* and *Parameterization.*

However, some of the modules such as *Pre-Processing* and *Mined Data* have similar functions due to the same objectives to prepare a good data and producing the valid and reliable models.

Overall, there are several work related to make the detection on P2P botnets. Yet, most of these works are still immature and have drawbacks particularly for improvise the technique. Thus, there are still had some of room improvements to develop an improved technique for P2P botnets detection.

TABLE I
GENERAL TERMINOLOGY TO DESCRIBE THE MODULE IN P2P BOTNETS DETECTION FRAMEWORK

No.	Component	Description
1.	Monitoring	Monitor and packet capturing to gather the data
2.	Filtering	Process to take selectively control the flow of data from network packet
3.	Classifier	To classify protocol used
4.	Pre-processing	All attributes are assigned with meaningful values
5.	Mined Data	Prepare a good data that will produce the valid and reliable models
6.	Analysis Approach	Involved of three type of detection technique analysis approach; static, dynamic and hybrid
7.	Activity Detector	Involved of detection technique on anomaly-based, signature-based, specification-based or hybrid
8.	Host Analyzer	To analyze host data
9.	Network Analyzer	To analyze network packet
10.	Correlation	This process indicates the extent to which two or more variables fluctuate together
11.	Parameterization	To verify selected parameter used

III. Discussion

The reviewed session has proved that there are several P2P detection systems have been done in network security field which is very beneficial to both side of industries and users. It is a valuable works that every research struggled and useful knowledge to fight against security problem in real network environment.

Technically, there are lots of Botnets detection systems towards IRC and HTTP-based. However, the studies for P2P-based detection and prevention are still limited. Also, by reviewing the previous studies, this research has found some room for improvements that related to P2P-based which directly contributes to security field. From that, we have conducted a review on seven (7) types of P2P botnets detection framework that have been developed for P2P botnets detection. These P2P botnets detection frameworks are [8]-[14].

Based on our review and as shown in Table II, we have found that most of P2P botnets detection frameworks are implemented on combination of modules that has similar functions and it can be clarified by referring Table II. From the results in Table II, we also found that each researcher will choose to implement *Monitoring, Filtering, Pre-processing, Mined Data, Dynamic Analysis Approach* and *Network Analyzer* module since the total number of occurrence has the value of 5 and above. Yet, this is the due to the facts that this module is implemented by all the researchers and it is needed to be maintained in implementation of P2P Botnets detection because it functions still necessary and important. However, one of the obvious findings from this study is that majority of the researchers do not choose the *Classifier Module* and *Correlation Module* as a favorite module to develop their framework. It is due on their capability and function has been replaced by the other module that has the same significant value to the

detection. The *Classifier Module* has been used to classify protocol used and the module has been replaced by *Filtering Module* since the module does the same duties. Meanwhile, the *Correlation Module* had been exchange by the rest of detection techniques which have equivalent task.

Through the analysis that had been in our previous study [15] has reveal the criterion on successful botnets detection as depicted in Table III. The specified criterion is responsible in making the significant on P2P botnets detection. These criterions can measure how far a framework and technique can be applied and reliable in real situation. These criterions can also help researchers analyse the advantages and limitations of such a technique in distinguishing among other techniques.

Furthermore, these criterion considered as an indicator for effectively and efficiency of the technique.

Consequently, this review also utilizes this criterion in distinguishing among other techniques. So, we has covered out the seven criterion which are including unknown botnet detection, protocol and structure independent, low false positive, encrypted bot detection, no require prior knowledge and reveal bot servers or C&C migration.

TABLE II
ANALYSIS OF MODULES INVOLVED IN P2P BOTNETS DETECTION FRAMEWORK
(MODULE FOUND=√, MODULE NOT FOUND=X, S=STATIC, D=DYNAMIC, H=HYBRID, SI=SIGNATURE-BASED, A=ANOMALY-BASED, DM=DATA MINING-BASED)

Researchers/ Components	Monitoring	Filtering	Classifier	Pre-processing	Mined Data	Analysis Approach			Activity detector				Host Analyzer	Network Analyzer	Correlation	Parameterization
						S	D	H	SI	A	dM	H				
P2P-based Detection Framework	√	√	√	X	X	X	√	X	X	√	X	X	X	√	X	HTTP, IRC, P2P
C&C Protocol-Independent Detection Framework	√	X	X	√	√	X	√	X	X	√	X	X	√	√	X	HTTP, IRC, P2P
Botnets Detection Approach Architecture	√	√	X	√	√	X	√	X	X	√	X	X	X	√	√	HTTP, IRC
General P2P Botnets Detection Framework	√	√	X	X	X	X	√	X	√	X	X	X	√	√	√	HTTP, IRC, P2P
P2P Botnets Detection System	√	√	X	√	√	X	√	X	X	X	√	X	X	√	X	P2P
P2P Detection Framework	√	X	X	√	√	X	√	X	X	X	√	X	√	√	√	P2P
IPS-Based P2P Botnets Detection	√	√	X	√	√	X	√	X	X	X	√	X	X	√	X	P2P
Improvement of P2P Botnets Detection	√	√	**X**	√	√	√	√	√	√	√	√	√	√	√	**X**	**P2P**
Total No. of Occurrences (√)	7	5	1	5	5	0	7	0	1	3	3	0	3	7	3	HTTP=4, IRC=4, P2P=6

TABLE III
P2P BOTNETS DETECTION CRITERION

Researchers/Components	Unknown Botnet Detection	Protocol and Structure Independent	Low False Positive	Encrypted Bot Detection	Not Require Prior Knowledge	Reveal Bot Servers and C&C Migration
P2P-based Detection Framework [8]	√				√	
C&C Protocol-Independent Detection Framework [9]		√	√			√
Botnets Detection Approach Architecture [10]			√		√	
General P2P Botnets Detection Framework [11]	√					
P2P Botnets Detection System [12]			√		√	
P2P Detection Framework [13]	√				√	
IPS-Based P2P Botnets Detection [14]	√					
Improvement of P2P Botnets Detection	√	√	√	√	√	√

In this comprehensive review on a P2P detection framework, we found that there are significant associations between the criterion and the selection of each of the terminologies. In the other words, a relationship exists between these criterions with the selected terminologies.

This view is supported by Zeidanloo and Eternad [8] used a network-based anomaly detection to identify IRC, HTTP and P2P-based botnets. Despite it not require prior knowledge, [8] suffers from the effect of different flow interval durations was not presented and the accuracy approach is unknown. Elsewhere, Chunyong and Ghorbani [9] and [8] are not mined the data due they depend wholly on classifier module to cluster the data. However, they are successful in detection on unknown botnets attack.

Meanwhile, Yuanyuan et al. [10], Chunyong and Ghorbani [13] and Muthumanickam and Ilavarasan [13] performed the combined of host and network analyzer with directly trigger action to detection reports in real time detection. Nevertheless, Yuanyuan et al. [10] and Muthumanickam and Ilavarasan [13] do not provide filtering module because the lack on payload inspection may occur high identification accuracy. The direct network flow and host log analysis provided by [13], make it do not feasible for offline detection. Then, Arshad et al. [12] and Junjie et al. [11] utilized the passive monitoring concern on network traffic.

However, their detection has consistently shown that it is not required prior knowledge and draws our attention to the real time detection. Li et al [14] also conducted a single detection methods where are network-based analyzer.

This detection system become ineffective against the new P2P-based botnets infected detection since the detection only done in Storm, Waledac and Skype application.

Hence, by reviewing the previous studies, most of them target to detect in network-based level [8], [11], [12], [14] rather than host-based level [9], [10], [13].

Besides that, majority researchers used dynamic analysis [8]-[14] rather than static analysis. Means, the analysis only had been done during or after program execution. This situation lead researcher capable to detect malicious behavior and activity during or after program is running [16]. In addition, no research has been found using hybrid analysis that combined static and dynamic analysis. The research to date has tended to focus on anomaly-based detection rather than others technique to tackle the problem on unknown botnets detection with low level false positives alarm [10], [12].

As the appropriate detection system, majority of previous work had done with mined data in ensuring a good data preparation by remove outliers as a key to producing valid and reliable framework [10]-[14].

Statistically, a major problem with the current framework is it cannot reveal the bot servers and C&C migration due they not compromise with protocol and structure independent. So far, only the [10] can trace the bot servers. Then, the research works has focus more on network layer and application layer [8], [9], [13], [14] due the layer will be fully visible the full picture of P2P botnets infections. Compares to the above framework detections, our work are not constrained by single detection technique and does not require the learning of data label to detection. Moreover, our approach offers more robustness because it does not rely on one single detection analyzer whether in host analyzer or network analyzer. So far, all the previous detection systems have their own drawbacks and the improvement needs to be carried out. Toward enhancing the previous framework, this develop framework architecture has provide better improvement since the detection are made by doing the hybrid analysis, hybrid technique and combination of host analyzer and network analyzer compared with previous works that not have the hybrid analysis and hybrid techniques. Only several researches do the hybrid analyzer [9], [10], [13], compare with the rest do the single level detection [8], [11], [12], [14].

Otherwise, the difference between this improvement frameworks with others are the detection involve on the majority detection on OSI layer rely on Data Link Layer, Network Layer, Transport Layer and Application Layer.

The rest of previous studies only focus on Application Layer [9], [13], [14]. Thus, this research proposes a new framework for P2P Botnets detection within the improvement has been made in hybrid analysis, hybrid technique and combination of host analyzer and network analyzer. Then, this proposes framework will complement the entire of criterion listed in Table II.

The details of improvement P2P botnets detection framework architecture are defined as following section.

IV. Proposed Improvement of P2P Botnets Detection Framework Architecture and Component

In this research, the marriage of several P2P botnets detection systems and techniques has been done in order to improve the functionality and capability of detection system.

Technically, this framework has structured using the multi-layer detection systems which contain input and output layers and four hidden layers that represent the mined data, analyzer, analysis modules and detection tasks. Fig. 8 graphically visualizes the architecture of framework. The detail of each layer can be understood as followed.

A. Layer 1: Input Layer

First layer describes as the input layer that entail by *Monitoring Module*. In this layer, the dataset has gathered from host level and network level. The data has been labeling through capturing packet in a controlled environment called as P2P testbed network. The host logs categories have involved the system log, application log and security log. Meanwhile, the network log consists of full payload packet for P2P network traffic.

B. Layer 2: Mining Data Layer

Layer 2 describes as the mined data layer involve with *Filtering Module, Pre-processing Module* and *Mined-Data Module*. In this layer, filtering is a process to take selectively control the flow of data from network packet where it allows only useful data and unnecessary data will be taken from the raw data are applied to make the next process easy and smooth.

Then, it is set as a data mining that exclusively denote by pre-processing stage. Overall, the major task implicate in mining data layer are data reduction and data discretization that obtains reduced representation in analytical and numerical results.

C. Layer 3: Analyzer Layer

The third layer represents the analyzer layer. In this layer, the hybrid analyzer had been used as a combination of host-level and network-level denote as *Host Analyzer Module* and *Network Analyzer Module* similar as our preliminary analysis [17].

D. Layer 4: Analysis Layer

Layer 4 enlightens the *Hybrid Analysis Module* and *Attack Pattern Identification Module*. The in-depth analysis provides two levels of analysis approach which are static approach and dynamic approach.

E. Layer 5: Detection Layer

The layer fifth expresses the hybrid detection techniques layer indicate the *Signature Generation Module* and *Statistical Test Module*. The hybrid technique has using the combination on data mining-based, signature-based and anomaly-based techniques. It has encounter the attributes relate on behavior features either in host-level or network-level.

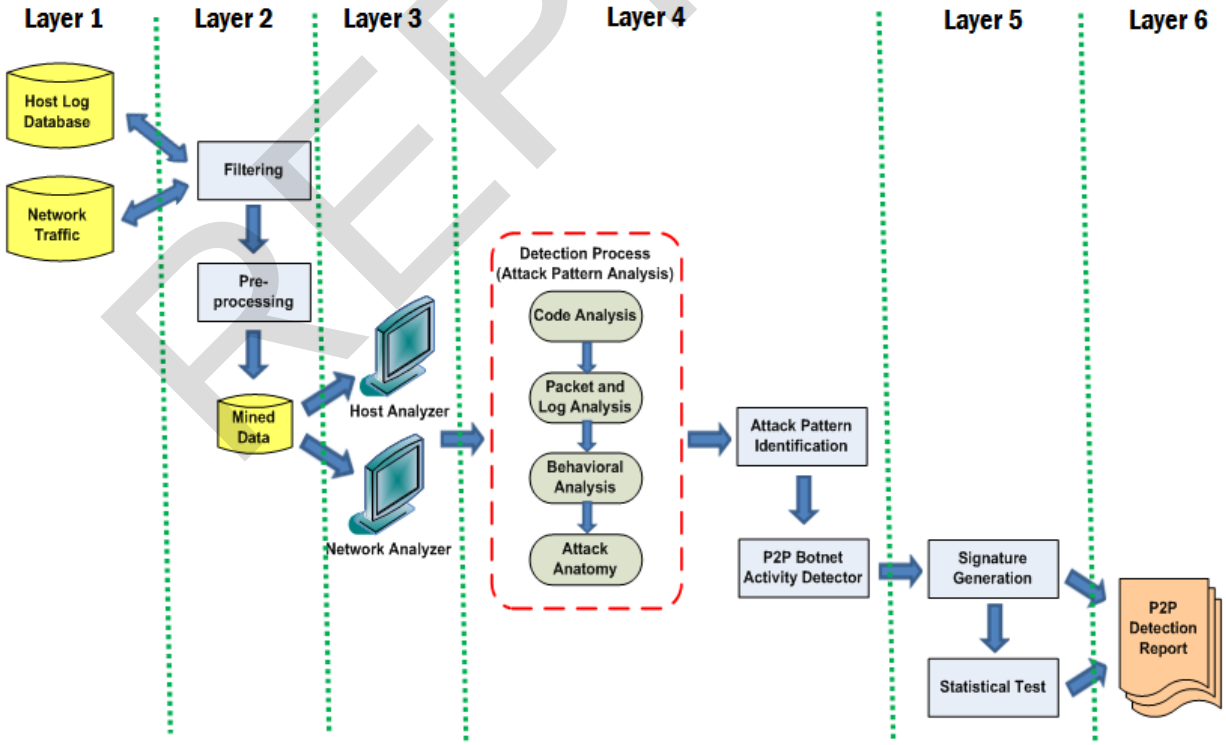

Fig. 8. Improvement of P2P Botnets Detection Framework Architecture

F. Layer 6: Output Layer

The final layer is describes the *P2P Detection Report Module* represents an individual output of P2P botnets detection system. The P2P detection system can be applied with standard detection method.

Our detection possibly raises the bar against botnets with make some of room improvements. In order to develop an enhanced P2P botnets framework, the improvement has been made on:

G. Hybrid Techniques – Combination of Mining Data, Signature-based and Anomaly-based Techniques

Technically, the signature-based technique is combined with anomaly-based technique which called hybrid technique. Then, the data has been mined based in pre-processing stage has incorporate with this hybrid technique. The hybrid technique introduces as improvement in P2P Botnets detection system.

This hybrid techniques used as the backbone in proposing the implementation of P2P Botnets detection system to modeling the intrusion report. The advantages of using the hybrid techniques is because it combination of IDS techniques offers inherent capabilities to complement each other weaknesses [18]. In the other word, hybrid has been choosing to advance their ability.

The implementation of hybrid technique used to have maximum accuracy, effectiveness and efficiency in detection rate evaluation

H. Combination of Host Analyzer and Network Analyzer

P2P Botnets have some unique characteristics and attacking behaviors that entirely different either in host or network level. The detection of P2P Botnets using host behaviors and networks behaviors has their own benefits and limitations. In host-based, the monitoring behaviors have done in a single host and the events occurring within that host for suspicious activity.

Meanwhile in network-based which monitors network traffic for particular network segments or devices will analyzes the network and application of protocol activity to identify suspicious activity [19].

If the detection is made at one level only probably it hardly provide reliable detection results. Thus, in order to detect bots more effectively, a combined host-based and network-based analysis is needed.

These combination levels of analysis are complement each other in finding malicious activity occur in the P2P network. This paper utilizes this combination of both approach simultaneously in differentiating a normal P2P and abnormal P2P behaviors. Thus, our framework considers both of level while making detection decisions.

I. Hybrid Analysis – Combination of static approach and dynamic approach

The analysis will consists of two levels of analysis approach which is static approach and dynamic approach. The use of both static and dynamic approaches remains as hybrid analysis approach which complements each other disadvantages [20].

Hence, static approach has capabilities to detect the malicious activity before the program is running or executed while the dynamic approach has the capabilities to detect the malicious activity during or after program execution.

J. Hybrid OSI Layer – Data Link Layer, Network layer, Transport Layer and Application Layer

The analysis has reveals the detection on imperative OSI layer [21] specifically in Data Link Layer (Layer 2), Network layer (Layer 3), Transport Layer (Layer 4) and Application Layer (Layer 7). This detection is vital to further analyzed.

Therefore, this research has proposed a new detection in improving the detection in P2P botnets with revealing their behaviors and characteristics. The real study on P2P Botnets detection will be compared to the previous systems. Both of the result will be compared. After that, this P2P detection will be developed whereas it is useful for security uses in future

V. Conclusion and Future Works

In this paper, the researchers have conducted the review of seven (7) currently P2P botnets detection framework to identify the gaps and problems that are still outstanding in enhanced the P2P botnets detection.

It is found in the previous section that there are several frameworks done in single method detection which are network-level. Only few frameworks combine the host-and-network level. Then, they are also focused on single detection technique rather than used the hybrid detection technique. Furthermore, almost none of the frameworks do the hybrid analysis consists of static and dynamic approaches to make the detection. Motivated from these, we have proposed the improvement in P2P botnets detection architecture framework by make enhancement in hybrid detection technique, hybrid analyzer and hybrid analysis. This improved P2P botnets detection framework is then extended to be further used in designing P2P botnets detection. The finding is essential for further research in P2P botnets detection and computer forensic investigation.

Acknowledgements

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

References

[1] 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.

[2] Mielke, C.J.; Hsinchun Chen; , Botnet, and the cybercriminal underground, *Intelligence and Security Informatics, 2008. ISI 2008. IEEE International Conference on* , vol., no., pp.206-211, 17-20 June 2008.
[3] Sundaram, A. An Introduction to Intrusion Detection. ACM , 2 (4), 3-7, 1996.
[4] Sharon M. R. and Matthew R.: Reasons & Rigor: How Conceptual Frameworks Guide Research: *SAGE Publications,* 2011.
[5] Anonymous : "What is framework?" Retrieved on October 2013 from http://whatis.techtarget.com/definition/framework.
[6] Laura: "Why use framework?" Retrieved on October 2013 from http://www.asfusion.com/blog/entry/why-use-a-framework.
[7] Matthew Broersma: *Botnets getting harder to kill* [Online] Retrieved on February 2011 from http://pcworld.about.net/od/cyber crime/Botnets-getting-harder-tokill.htm .
[8] Zeidanloo, H. R., Hosseinpour, F. and Eternad, F.F.: New Approach for Detection of IRC and P2P Botnet. *International Journal of Computer and Electrical Engineering Vol. 2(No. 6): 1793-8163*, 2010.
[9] Yin, C. and Ghorbani, A.: P2P Botnet Detection Based on Association between Common Network Behaviors and Host Behaviors: IEEE, 2011.
[10] Yuanyuan, Z., H. Xin, et al.: Detection of Botnet using Combined Host-and Network-Level Information. *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2010.
[11] Junjie, Z., R. Perdisci, et al.: Detecting Stealthy P2PBotnet Using Statistical Traffic Fingerprints. *IEEE/IFIP 41st International Conference on Dependable Systems & Networks (DSN),* 2011.
[12] Arshad, S., M. Abbaspour, et al.: An anomaly-based Botnet detection approach for identifying stealthy Botnet. *IEEE International Conference on Computer Applications and Industrial Electronics (ICCAIE),* 2011.
[13] Muthumanickam, K. and Ilavarasan, E. : P2P Botnet Detection: Combined Host and Network-Level Analysis: IEEE, 2012.
[14] Li, H. et al.: P2P Botnet Detection based on Irregular Phased Similarity: IEEE, 2012.
[15] Raihana Syahirah Abdullah et al., "Revealing the Criterion on Botnet Detection Technique", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 2, No 3, March 2013, Pages 208-215.
[16] 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.
[17] Raihana Syahirah Abdullah et al., "Preliminary study of host and network-based analysis on P2P Botnet detection"; *TIME-E Confernece IEEE Bandung, Indonesia*: 2013.
[18] Robiah Y, Siti Rahayu S., Mohd Zaki M., Shahrin S., Faizal M. A., Marliza R..: A New Generic Taxonomy on Hybrid Malware Detection Technique. *(IJCSIS) International Journal of Computer Science and Information Security*, Vol. 5, No. 1, 2009.
[19] Sabahi, F. and Movaghar, A.: Intrusion Detection: A Survey. *The Third International Conference on System and Networks Communication,* 2008.
[20] Robiah Y., Siti Rahayu S., et. al.: An Improved Traditional Worm Attack Pattern: IEEE, 2010.
[21] Vivek A.: TCP/IP and Distributed System: *Firewall Media,* New Delhi, India, 2006.

Authors' Information

Raihana Syahirah Abdullah is currently a PhD student at Universiti Teknikal Malaysia Melaka. Her research area include computer and network security.
E-mail: rasyahb@gmail.com

Dr. **Mohd Faizal Abdollah** is currently a senior lecturer in Universiti Teknikal Malaysia Melaka. The research area are system communication computer cluster in IDS, malware, forensic and network security
E-mail: faizalabdollah@utem.edu.my

Dr. **Zul Azri Muhamad Noh** is currently a senior lecturer in Universiti Teknikal Malaysia Melaka. The current research interests include advanced networking and distributed system research cluster in quality of service (QoS), wireless LAN, packet scheduling algorithm, and multimedia communication.
E-mail: zulazri@utem.edu.my

Dr. **Robiah Yusof** is currently a head of system and computer communication department in Universiti Teknikal Malaysia Melaka. Her research area are network security, network administration and network management.
E-mail: robiah@utem.edu.my

International Review on Computers and Software
(IRECOS)

(continued from outside front cover)

(continued on outside back cover)

Abstracting and Indexing Information:

Cambridge Scientific Abstracts (CSA/CIG)
Academic Search Complete (EBSCO Information Services)
Elsevier Bibliographic Database - SCOPUS
Index Copernicus (Journal Master List): ***Impact Factor 6.14***

Autorizzazione del Tribunale di Napoli n. 59 del 30/06/2006

Praise Worthy Prize

1828-6003(201312)8:12;1-2