ISSN 1828-6003
Vol. 8 N. 11
November 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, November 30, 2013.

Praise Worthy Prize

International Review on Computers and Software (I.RE.CO.S.), Vol. 8, N. 11
ISSN 1828-6003 *November 2013*

New Discovery of P2P Botnets Attack Pattern within Host-and-Network Atmosphere

Raihana Syahirah Abdullah, Faizal M. A., Zul Azri Muhamad Noh

Abstract – *The attacks of advanced P2P botnets become critical threats to the Internet security. Nowadays, powerful botnets creates to make this botnets stronger and immune from any prevention techniques. Hence, studies of attack pattern required on detecting and restructuring the security of the network that has been attacked. This paper proposes a new generalization of P2P botnets attack pattern that conducted within host and network atmosphere. In each attack steps, the investigation of P2P botnets has been conducted to identify the characteristics and the behaviors. Then, detailed analyses on infected files have been conducted that cover both of host log and network log in different OSI layer via hybrid analyzer. This P2P botnets hybrid analyzer can be abstracted to form P2P botnets attack patterns. In advances, this paper verifies the new discovery attack pattern has achieved new level of accuracy and efficiency. Furthermore, this P2P botnets attack pattern will beneficial to the P2P botnets detection and computer forensic investigation.*

Keywords: *P2P Botnets, P2P Botnets Attack Pattern, Botmaster Attack, P2P Botnets Host-Log, P2P Botnets Network Traffic*

I. Introduction

The dangerous attacked of P2P botnets continuously occur and this circumstances have been manipulated through the P2P applications which helping the botnets spreading easily in the network. Historically, P2P botnets such as Storm and Nugache are the first generation of botnets that have been detected in attacking the network [1]-[28]. Second generation of P2P botnes such as Peacomn [1] and Trojan [2] discover which recreates to conquer the weaknesses of the traditional botnets. For the followed botnets batch, powerful botnets with robust and stronger profile created to attack the network and paralyzed the security defend. The botnets have spreading unnoticeable through the recruitment and exploitation of the other computers known as bots or zombies make them become the army for cyber-attacks. It also offers the distribution on quickly exploiting the operating system make the vulnerability occur in a single host.

These critical situations require emergency action to detect the P2P botnets injection either in the network-level or host-level. In order to address with future P2P botnets attack, the deeper understanding towards the way of the current P2P botnets infection being propagates. Hence, this paper proposes the new of P2P botnets attack pattern within host and network atmosphere in response to the demand of network community. Technically, researches have selecting two scenarios: P2P botnets host-log scenario and P2P botnets network traffic scenario. This new attack pattern will be stressed on the P2P behaviors and characteristics of Botmaster attack on host-log (system log, application log and security log) and P2P network activity (tcpdump log and full payload captured data).

II. Related Work

As far as our knowledge, there are no previous studies have been conducted which focus on the attack pattern such the problem in this paper.

There a numerous of journals in network forensic studies such [1], [2], [3], [4].

II.1. P2P Botnets Infected Files

The P2P botnets currently becomes a central issue for the P2P network traffic. The earlier detection of P2P botnets may give benefits for security purpose. According to researcher, [3] claimed that network security demand advances and new Computational Intelligence (CI) techniques where the conventional detection and prevention had being defeated by the powerful P2P botnets.

Recently, more attention being paid to the emergence of botnets in P2P computing networks. It has been agreed by Yousof and Aickelin [4] when the researches discussed the new botnets capable to use the P2P protocols which potentially becoming the threat to the Internet security. This situation is exacerbated by limitation of non-centralized server to shut down and trace the losing bots, that gave an extra advantages over the traditional centralizes botnets.

Manuscript received and revised October 2013, accepted November 2013

Moreover, the P2P botnets potentially to make the economic losses incurred as online based transactions were disrupted. P2P Botnets spreads by doing complete life cycle in their attack steps: Scan, Exploits, C&C Connection and Impact/Effect stage as described in [6][7][8].

They are recruiting bots to attack the host by instructing them to exploit in files system, registry files and log system. Then, they also infected the whole network by suspicious port, suspicious IP address and launched such attack; DDoS, viruses, worms, spam, phishing and scams, information harvesting and etc. [9].

Adding on concern, Dan L. et al [5] predicted that there will be a new kind of P2P botnets basing on special designed P2P protocol in several years. By considering of this factor, currently it is highly required for the researchers to be able to differentiate the requirements and characteristics between the P2P normal and P2P botnets, identifying the new feature of the P2P botnets, investigating the infection steps, and analyze the impact of P2P infections.

At once, it will help for other researchers to have a better understanding of this P2P botnets for strive them to make the P2P botnets detection.

II.2. Definition of Attack Pattern

Theoretically, researches [10] define the attack pattern as systematic defenses of the attack goals and strategies to counter the botnets attacked. This statement is parallel with Hoglund and McGraw [11] that claimed an attack pattern is determined as the steps in a generic attack.

However, Moore et. al. [12] refreshing the idea of attack pattern more detail by defining the term as the attack steps, attack goal, pre-conditions and post-conditions of an attack. Afterward, Barnum and Sethi [13] pointed out the attack pattern is a method that caused exploitation against software used by attackers.

Thus, it inconclusive here that the attack pattern can be defined as the defenses mechanism to recognize potential of botnets attacks.

Several studies from [14], [15], [16], [17] provide the overview of P2P botnets focuses on the architecture and description about their purpose in their activities. The overview is only concern on traditional P2P botnets which are Waledac, Storm, Nugache, Slapper, Sinit and Kraken. Meanwhile, [18] and [19] highlighted the related mechanism in the P2P botnets such command mechanism, control mechanism, propagation mechanism, attack mechanism and survivability mechanism. However, full picture of P2P botnets infections still not clearly defined.

Subsequently, the study of P2P botnets in [20] conclusively carried out the comparison between Storm and Nugache. In their comparison, [20] isolates six features consists of P2P-protocol, C&C protocol, boots-table, routing-table, predecessor-table and successor-table. Based on the previous study, most of studies concentrated on the full concept of P2P botnets itself and general structure that associated to the development of architecture rather than drown in deep to the root of botnets problem.

Moreover, the investigation of analyzing the whole P2P botnets network activity has more concentrated on network-level rather than P2P botnets activity occurred in host-level.

Unfortunately, all the studies are insufficient for helping us to detect and prevent the attacks whereby P2P botnets nowadays getting smarter in doing their mission. P2P botnets are not only attacking the network-level but also the host-level. As the emergency reaction, this paper discovers the new P2P botnets attack pattern that focuses on both of host-level and network-level.

III. Methodology

The methodology of overall analysis process illustrated in Fig. 1 started by performing analysis in each of P2P botnets infected file.

The hybrid analysis approach discover two level of analysis: host-based analysis and network-based analysis whereby the analysis conducts at every single host log and network packet captured purposely to differentiate either the payload is malicious or spam.

Also, the analysis checked either it is remotely control for vulnerabilities, or it is follows unusual conventions with respect to normal P2P botnets. This hybrid analysis depicted in Fig. 1 is performed by considering two levels; host-level and network-level environments in inheritance of our previous study [21].

At host-level, the host logs were analysed by the characteristics on file system monitoring, registry and log monitoring.

Whereas, in the network-level, the characteristics on the full-payload from network packet were examined.

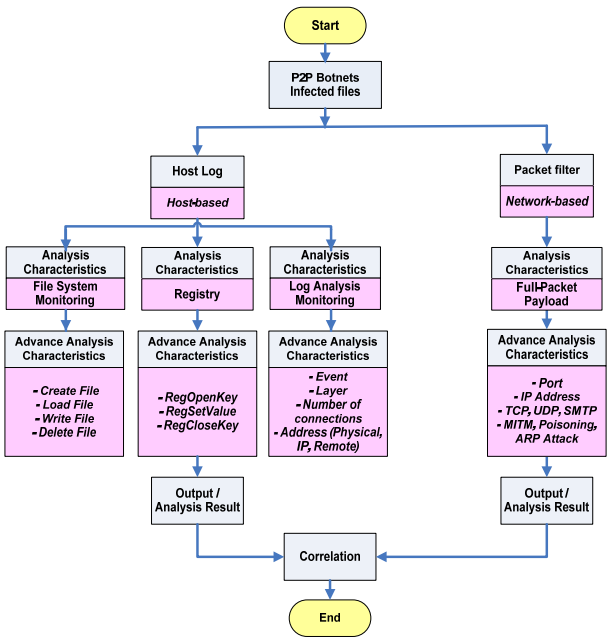

Fig. 1. Hybrid Analysis Process [19]

IV. Testbed Experiment Approach

The testbed experiment of P2P botnets as depicted in Fig. 2 involves of four main stages: Testbed Environment Setup, P2P Botnets Attack Activation, P2P Botnets Dataset Collection and P2P Botnets Hybrid Analysis.

The details are discussed as following sub section.

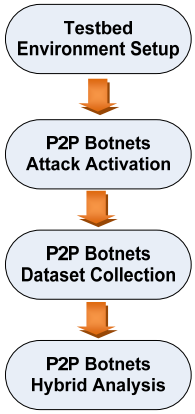

Fig. 2. Testbed Experiment Approach for P2P Botnets Analysis

IV.1. P2P Testbed Network Environment Setup

The network configuration that has been used for this experiment technically referring to the network simulation sequence steps proposed by MIT Lincoln Lab [22]. These simulation sequences practically modified using Linux and Windows XP to adapt with the testbed experiment. The experimental testbed lab was conducted to capture the P2P botnets activities under the controllable environment. Fig. 3 illustrated the network testbed logical design has been used in this research; in principally similar to the configuration used by Faizal [23]. The testbed design consists of one router, two switches, four personal computers/peers that placed with a fresh installation of Windows XP 32-bit and Linux, one NTP server and one server to performed the capturing packet process. In this experiment, each peer had installed by process explorer, process monitor and one of seven P2P botnets infected files which is provided by the MYCERT of CyberSecurity Malaysia. Among the P2P botnets variants tested on this testbed are Invalid Hash, Allaple, Palevo, Rbot, srvcp.exe, tnnbtib.exe and kido. Each of P2P botnets environment has run and been captured for 7 days long. The log files that have been selecting to be analyzed are system application and security log whose generate from the host-based level.

The full payload P2P network traffic as whole network traffic also has been captured to be analyzed indicates as network-level log. The whole network traffics are captured by *crontab* service.

IV.2. P2P Testbed Network Environment Setup

The P2P botnets attack is activated in this controlled environment to capture the activities and interaction between peers.

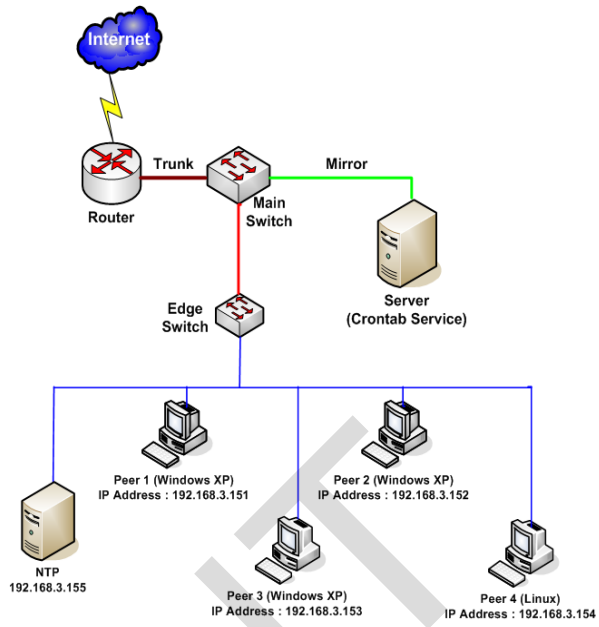

Fig. 3. P2P Testbed Environment

Each of P2P botnets infected files is activated in every single of scenarios. The variant is installed and activated for every peer: 192.168.3.151 – 192.168.3.155. This experiment was running unstoppable for 7 days long strictly without human interruption to obtain the P2P attack log and network traffic.

IV.3. P2P Botnets Dataset Collection

The data is collected at each peers and whole traffic. Each peer generates *system log, application log* and *security log*. The *crontab* service generates *tcpdump* network traffic. *Wireshark* and *tcpdump* have been used to verify the traffic between the host and network level.

IV.4. P2P Botnets Hybrid Analysis

At these stages, the researchers have combining both of static approach and dynamic approach for analyzing the botnets code before program executed and the effect after the program executed.

In this study, the hybrid analysis brought its strength that offers capability to identify the P2P botnets attack by observing specific attack pattern of P2P botnets attack that exists in host logs and network log at three different situations; before, during and after the attack launched.

This hybrid analysis is an input towards the attack pattern identification in proposed general P2P botnets attack pattern.

The P2P botnets attack designed for this study basically contain four phases as described in the previous section. The attack scenario implemented for host-log and network traffic analysis. In Figure 4, the scenario shown that the P2P botnets attack operated through full life cycle; Scan, Exploit, C&C Connection and Impact/Effect stage.

V. Attack Scenario

These P2P attacks at first stage do the scanning process and exploited all peers except the peer that installed with Linux OS.

Then, the P2P botnets organized attacks on host that continuously make a recurrence connection to C&C server. After the connection has been established with C&C server, we can see the impact/effect occur in every single host. At this stage, the hosts marked with *135, 139* and *445* officially successful being exploited by the Botmaster.

Consequently, these hosts has been infected and compromised by P2P botnets. On the other hand, these hosts also have been recruited as bots or zombies to become army for cyber-attack.

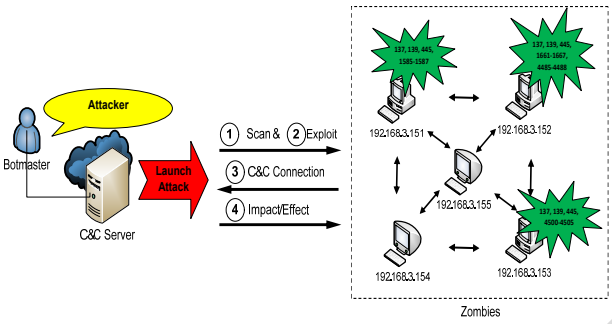

Fig. 4. P2P Botnets Attack Scenario

VI. Analysis and Findings

Based on the P2P attack scenario, various log and traffics from hosts and networks are analyzed to perform the attack pattern analysis.

The P2P attack scenario is further analyzed in this section. Analysis was done entirely on a complete life cycle of a P2P botnets that include Scan, Exploits, C & C Connection and Impact/Effect stage. P2P botnets life cycle is based on a study made by [6] [7] [8].

These findings then will be referred as the main guideline for develops this new P2P attack pattern. This new attack patterns consider host-level and network-level attack. The details of both levels are designated as follows.

VI.1. The P2P Botnets Attack Pattern Analysis at Host-Level

At the host-based, the experimental found that there was significant attack pattern in P2P botnets attack scenario.

The study is done by following the host-level analysis process flow as simplify in Fig. 5. Then, the summary of the P2P botnets host-based attack pattern shown in Table I. The existence of attacked pattern has been identified at the host log; *system log, application log* and *security log*.

As the continuity to this analysis, further discussion of the host-based attack pattern then elaborated.

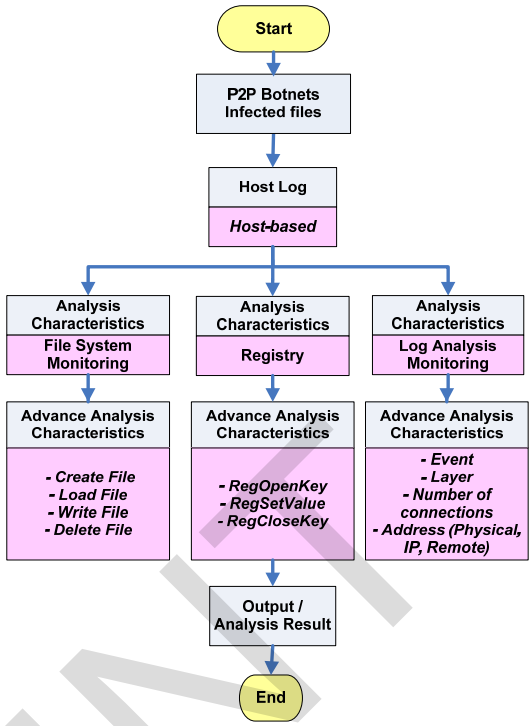

Fig. 5. Host-Level Analysis Process [19]

In this scenario, the *System Log* trace the P2P botnets attempt to create a fake process (*Event ID: 696)* shows that the P2P botnets have been operated in scanning process with proves the existence of event name. Consequently, the dramatic changes has occurs in registry system shown that the host system are partially exploited by P2P botnets.

Meanwhile, the data in *Security Log* appears as the vulnerable ports used by Botmaster to remotely control the host that allowing it to transmit the payload (botnets codes) as the ports open. Referring to the Table I, the attack pattern try to exploit the host by opening the vulnerable ports;139 Open TCP, 445 Open TCP and 137 Open UDP.

Furthermore, through the usage tools of *process explorer (procexp)* and *process monitoring (procmon)* have successfully reveal the scanning activity pattern which drove to the identification of behaviors and characteristics of P2P botnets in specific manner.

TABLE I
SUMMARY ON P2P BOTNETS ATTACK PATTERN FOR HOST-LEVEL

Level Analysis	Attack Steps	Host Log	Attributes
Host-based	Scan	System Log	Create File
			Load File
			Write File
	Exploit	System Log	RegOpenKey
			RegSetValue
			RegCloseKey
	C&C Connection	Security Log	139 Open TCP
			445 Open TCP
			137 Open UDP
	Impact/Effect	Security Log	Event ID: 696
			Event Name: xxxx.exe

Therefore, this discovery proved that the local host has been infected by P2P botnets and has high potential to launch such attack and re-infect to another host. After host was declared has being infected, the host technically considers as a stooges and possible to be an attacker to continually infecting other vulnerable hosts [24].

VI.2. The P2P Botnets Attack Pattern Analysis at Network-Level

The network-level pattern technically extracted from full payload network traffic that captured the whole activity of P2P botnets. The study is done by following the network-level analysis process flow as depicts in Fig. 6. The pattern is analyzed in protocol used, suspicious port, suspicious IP address and attack that have been launched.

The P2P botnets attack pattern in network-level is summarized in Table II. Later, the summary is discussed in this section.

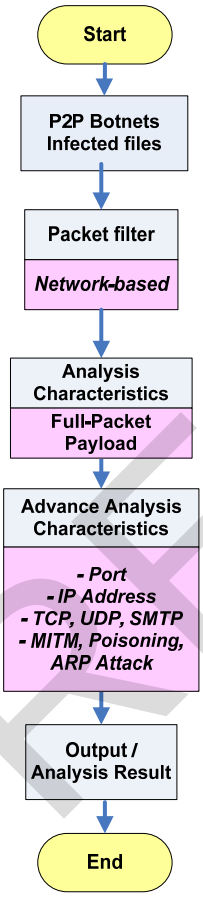

Fig. 6. Network-Level Analysis Process [19]

Referring to the Table II, this scenario shows the Botmaster start the exploitation with scanning the possible protocol to hijack their code into the network.

The P2P botnets makes the initial injection with launch the attack on TCP in order repeatedly send *echo request* and *echo reply* in ICMP state to make the connection.

The TCP flag combination that need to give attentions as an indicator to Botmaster performs network attack and P2P botnets activity is luring in the network are *TCP SYN (Half Open), TCP SYN/ACK, TCP FIN, TCP XMAS* and *TCP NULL* [25].

Thus, the TCP flag can utilize the P2P activity in differentiating a normal P2P and abnormal P2P. As mentioned in host-based level, the suspicious ports (139 Open TCP, 445 Open TCP and 137 Open UDP) were declaring as P2P botnets attack pattern for network-level that located in exploiting steps. These exploits allow the port open to the Botmaster inject their vulnerable codes. At once, the vulnerable open ports allow communication P2P botnets activities that permit all exploitation happen.

TABLE II
SUMMARY ON P2P BOTNETS ATTACK PATTERN FOR NETWORK-LEVEL

Level Analysis	Attack Steps	Network Log	Attributes
Network-based	Scan	Protocol	TCP Flag
			ICMP
	Exploit	Suspicious Port	139 Open TCP
			445 Open TCP
			137 Open UDP
	C&C Connection	Suspicious IP Address	Botnets/ C&C Website
	Impact/Effect	Launch Attack	ARP
			Poisoning
			MITM
			Other Attack : (i) Remote Address

C&C Connection attack step shows the P2P botnets initiate the connection to their server known as botnets website. The botnets website has been trace after capturing the source and destination of suspicious IP address. Hence, this attack pattern reveals the bots or C&C server where it then conquers the C&C server. Subsequently, the impact of P2P botnets to the network is proved by the series of attack that has been launched by Botmaster. This can be identified in Impact/Effect attack steps. The series of P2P botnets attack contained ARP attack, poisoning attack, MITM attack and the existence of remote address.

Through this study, a significant fingerprint found in network-level analysis by authenticate the existed pattern where the P2P botnets controlling the peer to download the botnets code via the vulnerable port where the IP address source is the peer and the IP address destination is the Botmaster.

Overall, on conducting the analysis, the researchers successfully recognized the attributes and behavior features for both host-level and network-level. The findings then useful for researchers to complete new P2P botnets attack pattern.

VII. Discovers New P2P Botnets Attack Pattern

This paper proposes the new of generalization for P2P botnets attack pattern for host-level and network-level.

The details discussion describes on following section.

VII.1. P2P Botnets Host-Level Pattern

The host–level pattern present a systematic description of dealing the attack goals and strategies for defending against the attack. Technically, the attack pattern brought potential assistance to the researchers for identified the Botmaster and bot server.

According to the data in Table I, a complete picture on overall attack pattern in host-level is illustrated in Figure 7. It indicate that the P2P botnets attack pattern at host-level used the ports (135, 139 and 445) to enable the scanning process operated illegally. From this illegal operation, a fake files will be created with new set of registry and transmit the event name.exe to exploit the *system log*. This situation initiates the P2P botnets code is execute to be downloaded by one single host. Then, the host infects the other peers and become as a bots or zombies.

The similar activity happened on the network traffic log which pointed out to entire crafty evidence found on the host.

VII.2. P2P Botnets Network-Level Pattern

The P2P botnets network-level pattern uses to determine the process of network attacked by the Botmaster. From Fig. 8 depicted the detail of P2P botnets attack pattern in network-level which originally form from Table II. The figure portrayed the flow of P2P botnets trying to exploit the network by scan the appropriate protocol to find the vulnerable open port. The P2P botnets attempting to authenticate the pattern by using suspicious port and suspicious IP address.

Then, they are transmitting the various botnets codes through connecting with C&C or bot server. Immediately, when the host is infected by all king of techniques either worms, Trojan horse or viruses through botnets code, a Botmaster initiates to launch the attack. By the end of botnets attack, it would have a profound impact on network security.

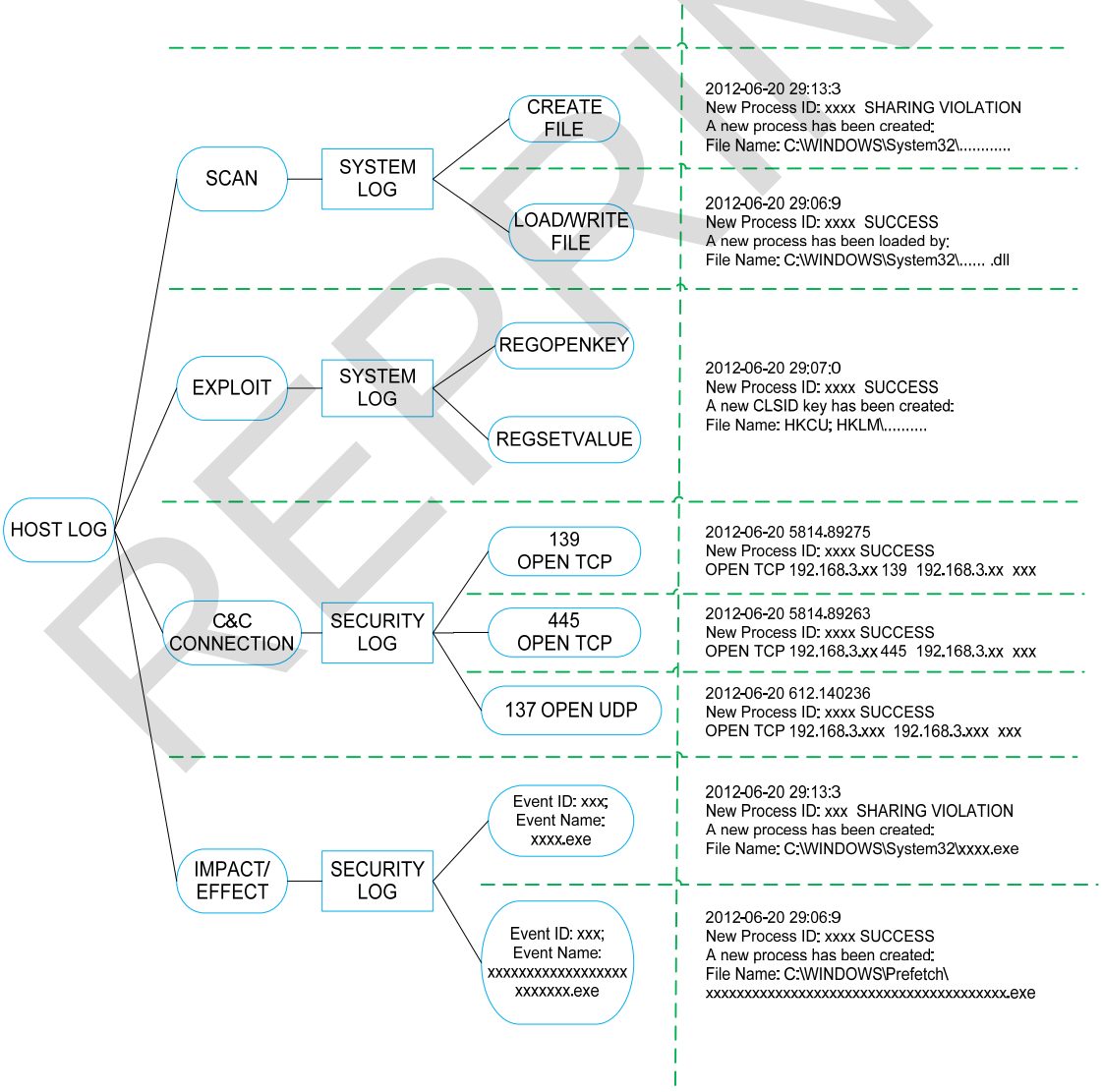

Fig. 7. Proposed General P2P Botnets Attack Pattern in Host-Level

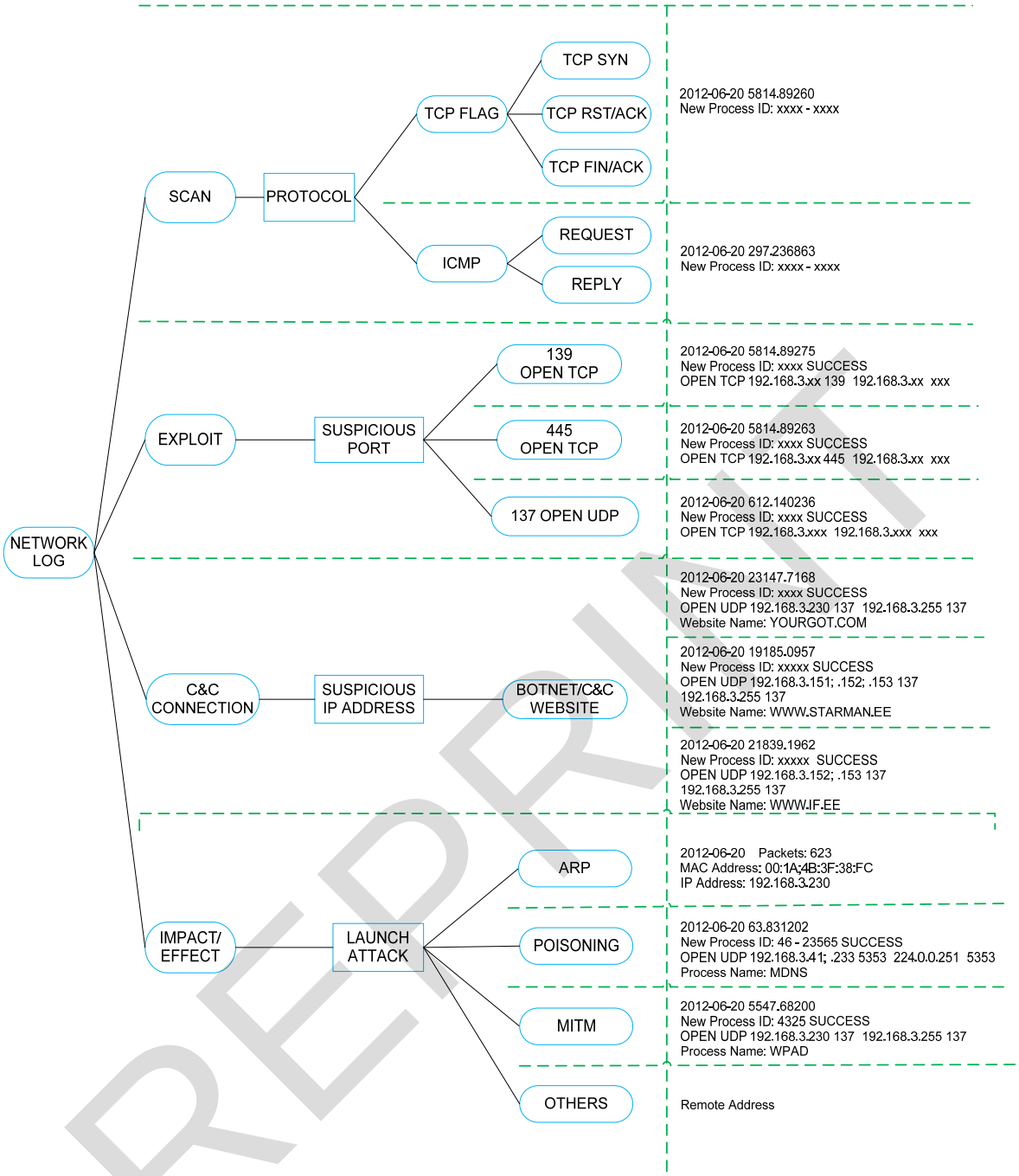

Fig. 8. Proposed General P2P Botnets Attack Pattern in Network-Level

VIII. Conclusion and Future Works

In this paper, researches have been conducted the analyses at the host logs data and network traffic data purposely to recognize the P2P botnets attack pattern for both host-level and network-level atmosphere. The discovery of attack patterns role as the alert alarm that helps administrator to detect the invisible attacker. The results used to propose new P2P botnets attack pattern that can be applied on host-level and network-level. Furthermore, this discovery will be extended to design an effective P2P botnets detection.

In a nutshell, this is a valuable finding that will be a knowledgeable material to the research of 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] J. B. Grizzard, V. Sharma, C. Nunnery, B. B. Kang, and D. Dagon: Peer-to-peer botnets: Overview and case study, Proc. 1st USENIX Workshop on Hot Topics in Understanding Botnets (HotBots '07), Cambridge, 2007.

[2] T. Holz, M. Steiner, F. Dahl, E. W. Biersack, and F. Freiling: Measurements and mitigation of peer-to-peer-based botnets: A case study on storm worm, Proc. 1st Usenix Workshop on Large-scale Exploits and Emergent Threats (LEET '08), San Francisco, 2008

[3] Langin C. et al. "A Self-Organizing Map and its Modeling for Discovering Malignant Network Traffic." Southern Illinois University, USA: IEEE, 2009

[4] Yousof A.H and Aickelin U.: 2011 – The Year of the Botnet, *IT Business Edge*, 2011

[5] Dan L. et al. (2010). "A P2P-Botnet Detection Model and Algorithms Based on Network Streams Analysis". *2010 International Conference on Future Information Technology and Management Training.* (pp. 55-58). China: IEEE

[6] Chandrashekar, J. et al: The Dark Cloud: Understanding and Defending against Botnets and Stealthy Malware. *Intel Technology Journal Vol.13 Issues 2,* 2009

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

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

[9] Mielke, C.J. and C. Hsinchun. Botnets, and the cybercriminal underground. in Intelligence and Security Informatics, 2008. ISI 2008. IEEE International Conference, 2008.

[10] Robiah Y., Siti Rahayu S., et. al.: An Improved Traditional Worm Attack Pattern: IEEE, 2010.

[11] Hoglund, G., & McGraw, G. (2004). Exploiting Software: How to Break Code. Boston, Massachussetts: Addison-Wesley/Pearson.

[12] P. Moore, A., J. Ellison, R., & C. Linger, R. (2001). Attack Modeling for Information Security and Survivability. (No. CMU/SEI-2001-TN-001.): Pittsburgh, Pennsylvania: Software Engineering Institute, Carnegie Mellon University.

[13] Barnum, S., & Sethi, A. (2006). Introduction to Attack Patterns. [Electronic Version]. Retrieved 18 April 2010.

[14] Dae-il, J., K. Minsoo, et al.: Analysis of HTTP2P Botnet: Case Study Waledac: *IEEE 9th Malaysia International Conference on Communications (MICC)*, 2009.

[15] Zeidanloo, H. R. and A. A. Manaf: Botnet Command and Control Mechanisms: Second International Conference on Computer and Electrical Engineering (ICCEE '09), 2009.

[16] Zang, X., Tangpong, A., et al.: Botnet Detection through Fine Flow Classification: *CSE Dept Technical Report CSE11-001*, 2011

[17] Leder, F., Werner, T. et al.: Proactive Botnet Countermeasures - An Offensive Approach, 2009

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

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

[20] Junfeng, D., J. Jian, et al.: Descriptive model of peer-to-peer Botnet structures: *International Conference on Educational and Information Technology (ICEIT)*, 2010.

[21] Raihana Syahirah Abdullah et al., "Preliminary study of host and network-based analysis on P2P Botnet detection"; *TIME-E Confernece IEEE Bandung, Indonesia*: 2013

[22] Lincoln Lab, M.,: 1999 DARPA Intrusion Detection Evaluation Plan, [Electronic Version]

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

[24] Braverman, M.: P2P Botnets: A Case Study from Microsoft's Perspective: *Virus Bulletin Conference*, 2005

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

[26] Hu, D., Luo, J., Feng, Y., Copyright protection in P2P networks using digital fingerprinting, (2011) *International Review on Computers and Software (IRECOS),* 6 (3), pp. 366-370.

[27] Pei, Y., Clustering identical sampling algorithm of mobile P2P networks from real-time data, (2012) *International Review on Computers and Software (IRECOS),* 7 (5), pp. 2401-2407.

[28] Alsous, E., Alsous, A., A botnet detection system using multiple classifiers strategy, (2012) *International Review on Computers and Software (IRECOS),* 7 (5), pp. 2022-2028.

Authors' information

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

PM 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

International Review on Computers and Software (IRECOS)

(continued from outside front 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

1828-6003(201311)8:11;1-6