Far East Journal of Electronics and Communications
100 *Proceedings of SHANNON* - 3rd *Int. Conf. Comp. Sci.*, 2016
© 2016 Pushpa Publishing House, Allahabad, India
http://dx.doi.org/10.17654/ECSV3PII16307
Special Volume 3, Part II, 2016, Pages 307-317 **ISSN: 0973-7006**

DYNAMIC STRATEGY FOR BOTNET DETECTION USING BBA

Sanjeev Kumar Dwivedi[1], **Om Prakash**[1], **Surendra Kumar Keshari**[1] **and K. Muthumanickam**[2]

[1]Department of Information Technology
Krishna Institute of Engineering and Technology
Ghaziabad, India

[2]Department of Computer Science and Engineering
Pondicherry Engineering College
Pondicherry, India

Abstract

Apart from well known malwares viruses, worms and Trojan houses; there is less familiar threat known as the botnet. The term botnet (network of bots) is a combination of two words: bot (victim host) and net (network). In relation of botnet taxonomy bot is referred as a victim host which is under the control of the attacker called BotMaster (or Botherder). These botnets are frequently used for many cyber attacks and crimes, and they are root causes for several illegal activities like click fraud, DDOS, etc. Botnets operate under the command and control infrastructure (C & C) which makes botnets functioning unique giving serious problems in defending from this malware. Botnets become more elaborate and efficient. Their use is growing at an exponential rate. Although botnets showed their existence several years ago, it became an interesting area for research only recently. Various types of technique are proposed for detection

---

Conference held during April 8-9, 2016 at Lovely Professional University, Punjab, India.
Guest Editor: G. Geetha; Division of Research and Development, Lovely Professional University, Punjab, India.

and prevention from botnet attacks. Current detection models deal with only a limited set of bots behavior and thus are not able to resolve protocol independent and architecture independent (PI & AI) problem, and autoupdation mechanism used by the botnet. The proposed model addresses these problems along with the detection of advanced botnets. In this paper, we have taken up a survey report for detection of hybrid botnets.

Introduction

Malware includes viruses, worms, Trojan horses, spyware that gather information about a computer user and access to a system without permission. It can appear in the form of scripts, active content, code, or other softwares. Malware programs are divided into two classes: the first one consisting of viruses, Trojan horses, logic bombs, trapdoors (requiring a host program) and the second one consisting of worms, zombie (independent programs). Botnet has become the most serious security threats on the current internet infrastructure. A botnet (BotNetwork) is an interconnected collection of compromised infected computer (bots) which is remotely controlled by its originator (called BotMaster or Botherder) under a common and control infrastructure [1]. Bot is a new type of malware which is designed for malicious activity. The term bot is derived from the word robot which is used to describe sets of scripts designed to perform predefined functions. After the bot code has been installed into a computer, the computer becomes a bot. Here all the bots are under the control of BotMaster. So, if a bot exists in computer, then it is not harmful until it receives command from BotMaster. After receiving the command from BotMaster, it is dangerous for the system. These bots are not self-propagate from one system/network to other systems/networks. They are in an idle state. After receiving the commands from BotMaster, they propagate from one system/network to other systems/networks and thus enter into malicious activities [2].

Due to existence of C & C infrastructure, botnet differs from other types of malware. So, if we are able to detect the location of C & C, then botnet can be detected and prevented from cyber-attacks. But this also depends on which type of communication protocols are used by botnets. Based on the architecture, botnets are classified into three categories: Centralized, Decentralised and Hybrid Botnets. Centralized mechanisms are used by many botnet architectures. This is a client-server architecture. HTTP (Agobot, SDbot) and IRC (Zeus bot) are the two common protocols used by this architecture. In a decentralized architecture of botnets, any victim host acts as a client and a server. Strom botnet is an example of decentralized (P2P) architecture. The hybrid architecture is a combination of both centralized and decentralized architectures [2, 3, 8].

Botmaster provides following services to its bots:

1. Rich network connectivity.
2. Control traffic dispersion.
3. Individual encryption.
4. Easy recovery and monitoring by BotMaster.

Table 1 shows different classifications of botnet based on their topological structures and some of their comparison parameters.

Table 1. Comparison of command and control topologies

S. No.	Topology	Design complexity	Delectability	Message latency	Survivability
1.	Centralized	Low	Medium	Low	Low
2.	Decentralized	Medium	Low	Medium	Medium
3.	Hybrid	Low	High	High	High

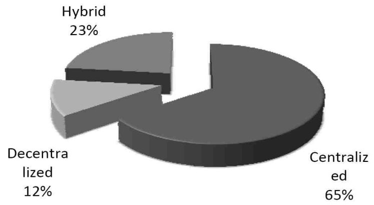

Figure 1. Distribution of different types of architectures.

Figure 1 shows that the distribution of different types of botnet structures exists in a network. Some botnets use centralized architectures, while others use hybrid structures. Around 20% to 25% botnet structures are based on hybrid mechanisms which exist in a network.

Botnet life cycle (Figure 2):

Typically botnets create and maintain 4 phases:-

1st phase: BotMaster infects a victim host (after infection a victim host is called a bot) through compromise mechanisms, social engineering, etc.

2nd phase: Now, these infected hosts are connected to C & C server.

3rd phase: BotMaster sends command to C & C server and the C & C server replicates command to other victim hosts (bots), and in this process, id is repeated again and again in order to create troops of botnets (botnet army).

4th phase: Bots are regularly updated with the new business functionality through BotMaster and the C & C server.

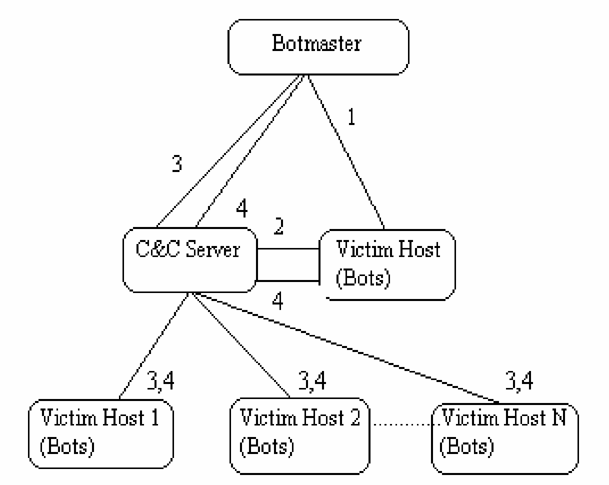

Figure 2. Botnet life cycle.

Some researches use behavior correlation algorithm/bot behavior algorithm (BBA) [10, 12] to detect bots from a network. These provide mathematical models for detecting bots. But by using above algorithm, we have to set threshold value for detecting bots for every experiment. So a proper detection technique is needed which may stabilize these parameters increasing the detection rate. Also, existing algorithm fails to address the problem like normal communication program and botnet communication program, PI & AI problem, etc.

There are several reasons for modeling the botnet detection model: first botnet uses command and control infrastructure for their communication which makes its functioning unique. Second botnet uses different-different types of topologies (centralized, decentralized, hybrid) for their connection with victim host, and third uses different-different types of protocols. Some botnets also use protocol independent and architecture independent platforms for their connection and communication. The proposed technique will work on three phases: data collection, filtering and botnet detection.

Background Material

Currently, many botnet detection techniques such as FCM (flow-correlation method) [12], VTM (visual threat monitor) [9], SMM (signature matching method) [13, 17] exist. There are two essential techniques for botnet detection: setting up honey-nets and passive monitoring network traffic [14, 15]. Many papers have already discussed about using honey-nets for botnet detection. Additionally, there are many ideas to analyze strategies and the type of command and control channels used by P2P botnet.

In [9], a visual thread monitor tool which is a graphical visualization method is used to improve the visibility of network traffic associated with invariant bot behaviors. The main advantage of VTM method is to easily visualize information to be processed. For users, it is easy to gain useful information about bot enabling to detect both known and unknown types of bots. But it visualizes only a limited set of invariant bot behavior (small size command, fast response time). Also, this method besides being unable to detect encrypted types of bots suffers from PI & AI problem.

Reference [10] suggests a mechanism called FCM. It is an IRC-based botnet detection mechanism applied flow correlation for grouping the same activities of same bots and identify both normal IRC and abnormal IRC behaviors.

In [5], a P2P botnet detection framework which is based on association between common P2P networks behaviors and host behaviors is suggested. This mechanism not only detects known P2P botnet with a high detection rate but also detects some unknown P2P malwares. This method deals with some problems such as data encryption, route selection and communication behaviors.

The impact of botnet to the computer world is discussed in [3 ,4]. They described several methods to create networks of bots, their control and communication techniques, the protocols used for communication and different types of possible attacks. They also discussed one of the botnet tracking tools, namely the honeypot to understand bots operation.

In [8], the structure of a hybrid P2P botnet is discussed. It is noted how the hybrid botnet differs from centralized and decentralized botnets, their update architectures, types of propagation schemes and network connectivity used by botnet.

Reference [6] suggests a P2P botnet detection based on network stream analysis. Their botnet detection strategy is based on three algorithms: P2P node detection, P2P node clustering and finally botnet detection. Before bots detection, the suggested strategy detects P2P nodes in a network. The suggested algorithm uses several parameters for bots detection and for every experiment adjusts these parameters and threshold values.

References [11, 13, 14] use signature matching, pattern matching, packet sampling approaches for botnet detection, but these techniques have low computational complexity and generate false alarms.

Discussion

Our literature review shows the current technologies for botnet detection based on flow correlation method [12] (FCM), visual threat monitor tool [9], (VTM), P2P bots behaviors method [10] (PBBM) realized only with a limited set of bots behavior which are unable to detect protocol and architecture independent botnets. The problems like attacks on payload, differentiation between normal communication programs and botnet communication program, deal with certain problems such as data encryption, route selection, and communication behaviors which are not completely solved by the existing system. Even though the existing approach is available for detection of centralized and decentralized botnets, which are described at both designed level as well as implementable level. The above mentioned problems are not yet fully solved. Only few researchers explained architecture independent botnet.

Figure 3 shows different types of intrusion detection system. It also depicts the various types of detection mechanisms available at both the host and the network-level. Many researchers use network-level botnet detection techniques which are mostly anomaly-based (either active or passive network monitoring) and signature-based [14, 15]. Some of the researchers address the combination of both host-level and network-level techniques [5].

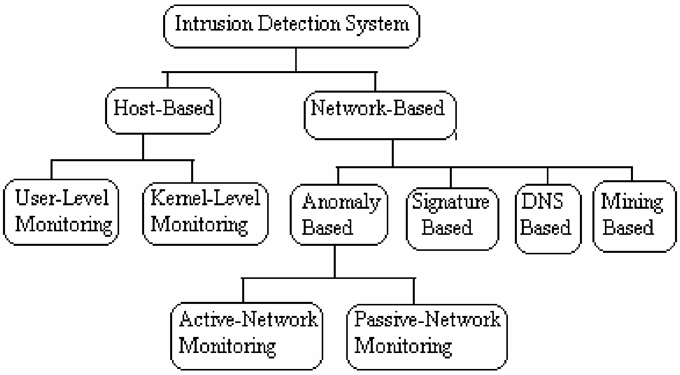

Figure 3. Classification of intrusion detection system.

Table 2 describes comparative study of various botnet detection approaches based on network traffic monitoring. Some of the network based methods detect only known and unknown bots; some detect known, unknown and encrypted bots. Many researchers used signature-based method [13] for botnet detection but this method detects only known bots and fails to detect unknown bots and encrypted bots.

Table 2. Comparative study of various network-based methods

S. No.	Network-based method	Known bot detection	Unknown bot detection	Encrypted bot detection	PI & AI problem
1	Mining-based [7]	Yes	Yes	No	No
2	VTM [9]	Yes	Yes	No	No
3	Signature-based [13, 17]	Yes	No	No	No
4	Anomaly-based [14, 16]	Yes	Yes	No	No
5	DNS-based [15]	Yes	Yes	Yes	No

Table 3. Comparative analysis from existing model with proposed model research directions

S. No.	Researchers	Tool/Algo./Module	PI & AI Prob.	Topology
1	Shahrestani et al. [9]	visual threat monitor tool (VTM)	No	Centralized
2	Hammadi and Aickelin[10]	P2P bots behaviors	No	Decentralized
3	Lin et al. [12]	flow correlation	No	Centralized
4	Munz and Carle [16]	Traditional packet inspection for classification of botnet	No	Decentralized
5	Wang et al. [17]	flow attributes, signature matching.	No	Decentralized
6	Sperotto et al. [18]	Packet sampling, pattern matching.	No	Centralized
7	Our work	Victim host behavior and Network-level analysis	Yes	Hybrid

Table 3 shows the comparative analysis of existing model with proposed model. The existing models are not covering the protocol independent and architecture independent (PT & AI problem) botnet detection problem. But our proposed model will avoid the PI & AI problem by introducing a new botnet detection model. The proposed algorithm is applicable for both centralized and decentralized botnets.

Research Directions

There is a need of a model which will detect both centralized and decentralized botnets in a network and their respective specificities.

- Idea for detecting botnet from a network is passively monitoring network traffic. Some work has been carried out in the past for detection of P2P botnets but they fail to address the problems like data encryption, communication behavior, etc.
- Current botnet detection models such as visual threat monitor tool (VTM), flow correlation method (FCM), etc. provide only a limited support for detecting the bots from a network. And these methods are available in either centralized or decentralized botnets, not in, hybrid botnets.
- If protocol independent and architecture independent problems are solved, detection rate will then be increased.

If network-level method is combined with host-level, then the success rate of botnet detection will be increased and this is applicable for both centralized and decentralized botnets.

Conclusion

Even though the detection models are available for detecting centralized and decentralized botnets, those techniques are not suitable for hybrid botnets and also do not focus on the protocol independent and architecture independent problem. Therefore, a new model for detecting the botnets has been proposed.

Existing passive network monitoring method is classified into DNS based, signature based, mining based and anomaly based detection techniques, among them signature based method detects only known bots and other method detects both unknown and known bots. Also, a proper detection technique is needed which not only detects known and unknown bots but also is able to detect encrypted bots. At the same time if bot programs are updated, existing network based method is not able to resolve this problem.

The proposed work can be implemented by using specified standards and the previous works for experiments. The experimental results of both the works are evaluated by parameters such as matching number of bot features, negative false and stability index, etc.

References

[1] Lei Zhang, Shui Yu, Di Wu and Paul Watters, A survey on latest botnet attack and defense, International Joint Conference of IEEE Trustcom-11/IEEE ICESS-11/FCST-11, 2011, pp. 53-60.

[2] Maryam Feily, Alireza Shahreshtani and Sureswaran Ramadas, A survey of botnet and botnet detection, IEEE in The Third Conference of Emerging Security Information, Systems and Technologies, 2009, pp. 79-84.

[3] Banday, M. T. Qadri and J. A. Shah, Study of botnet and their threats to internet security, sprouts: working papers on information system, 2009.
Available at: http://sprouts.aisnet.org/9-24.

[4] Niels Provos and Thorsten Holz, Virtual Honeypots: From Botnet Tracking to Intrusion Detection, See Chapter 11-Tracking Botnets. Publisher: Addison Wesley Professional, Publishing 16 June, 2007.

[5] Chunyong Yin and Ali A. Ghorbani, P2P Botnet Detection based on Association Between Common Network Behaviors and Host Behaviors, (2011), 5010-5012.

[6] Dan Liu, Yichao Li, Yue Hu and Zongwen Liang, A P2P botnet detection model and algorithm based on network stream analysis, IEEE Internat. Conference on Future Information Technology and Management Engineering, 2010, pp. 55-58.

[7] M. M. Masud, T. Al-Khateeb, L. Khan, B. Thuraisingham and K. W. Hamlen, Flow-based identification of botnet traffic by mining multiple log file, Proc. Int.

Conf. Distributed Frameworks and Applications, 2008, pp. 200-206.

[8] Ping Wang, Sherri Sparks and Cliff C. Zou, An advanced hybrid peer-to-peer botnet, IEEE Transaction on Dependable and Secure Computing 7(2) (2010), 113-127.

[9] Alireza Shahrestani, Maryam Feily Rodina Ahmad and Sureswaran Ramadass, Discovery of invariant bot behavior through visual network monitoring system, Fourth International Conference on Emerging Security Information, Systems and Technologies, 2010, pp. 182-188.

[10] Yousof Al Hammadi and Uwe Aickelin, Behavioral correlation for detecting P2P bots, Second International Conference on Future Networks, 2010, pp. 323-327. DOI 10.1109/ICFN2010.72.

[11] Hossein Rouhani Zeidanloo and Azizah bt Abdul Manaf, Botnet detection by monitoring similar communications patterns, International Journals of Computer Science and Information Security 7(3) (2010), 36-44.

[12] Hsiao-Chung Lin, Chia-Mei Chen and Jui-Yu Tzeng, Flow based botnet detection, IEEE Fourth International Conference on Innovative Computing, Information and Control, 2009, pp. 1538-1541.

[13] S. Zander, T. Nguyen and G. Armitage, P2P traffic identification based on the signature of key packets, IEEE Conference Local Computer Networks, 2010.

[14] Mohammed Abdul Qadeer and Mohammad Zahid, Network traffic analysis and intrusion detection using packet sniffer, Second International Conference on Communication Software and Networks, 2010, pp. 313-317.

[15] H. Choi, H. Lee, H. Lee and H. Kim, Botnet detection by monitoring group activities in DNS traffic, Proc. 7th IEEE Int. Conf. Computer and Information Technology (CIT 2007), IEEE Computer Society, 2007, pp. 715-720.

[16] G. Munz and G. Carle, Deep analysis of intending peer-to-peer botnet, 10th IEEE International Symposium on Integrated Network Management, 2009, pp. 1342-1347.

[17] Pinghui Wang, Xiaohong Guan and Tao Qin, P2P traffic identification based on the signature of key packets, IEEE Conference Local Computer Networks, 2009.

[18] Anna Sperotto, Gregor Schaffrath, Ramin Sadre and Cristian Morariu, An overview of IP flow-based intrusion detection, IEEE Communication Surveys and Tutorials, Third Quarter, 12(3) (2010), 343-356.