Chapter 56
A Survey on P2P Botnet Detection

Kyoung-Soo Han and Eul Gyu Im

Abstract Recently cyber-attacks in Internet using botnets have been increased. Also, crimes involved in monetary profits through cyber-attacks have been continuously increased. Attackers can use P2P botnets to launch various attacks such as Distributed Denial of Service (DDoS), malware propagation, and so on. For this reason, P2P botnet detection techniques have been studied. This paper is a survey of P2P botnet detection, and describes about the general type of P2P botnets and detection methods.

Keywords P2P botnet · Botnet detection

56.1 Introduction

Attacks using botnets in Internet have been significantly increased. The botnet is a type of network that consists of PCs which are infected with malware such like worms [1]. Botmasters can launch various cyber-attacks like Distributed Denial of Service (DDoS), malware propagation, and so on using P2P botnet. In this paper, we describe a general type of P2P botnets and detection methods.

K.-S. Han
Department of Electronics Computer Engineering, Hanyang University,
17, Haengdang-dong, Seongdong-gu, Seoul 133-791 South Korea

E. G. Im (✉)
Division of Computer Science and Engineering, Hanyang University,
17, Haengdang-dong, Seongdong-gu, Seoul 133-791 South Korea
e-mail: imeg@hanyang.ac.kr

K. J. Kim and S. J. Ahn (eds.), *Proceedings of the International Conference on IT Convergence and Security 2011*, Lecture Notes in Electrical Engineering 120,
DOI: 10.1007/978-94-007-2911-7_56, © Springer Science+Business Media B.V. 2012

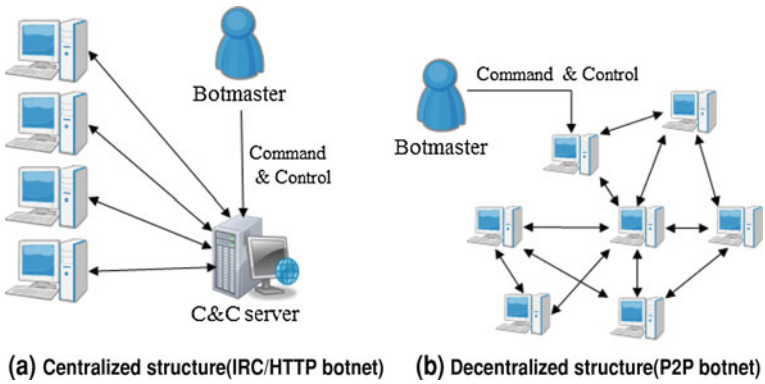

Fig. 56.1 The structure s of the botnet

56.2 P2P Botnet

Botmasters configure a computer network that can be controlled without exposing themselves for obtaining monetary profits. That is, botmasters infects so many vulnerable PCs using malware such like worms in order to freely control such PCs. And then the infected PCs are to be configured as a network. The network configured by these infected PCs is called a botnet, in which botmasters launch various attacks by transmitting commands to the infected PCs in this botnet [2, 3].

The botnet can be classified into IRC, HTTP, and P2P botnet according to used protocols. The IRC and HTTP botnets have a centralized structure as shown in Fig. 56.1a and the P2P botnet has a decentralized structure as shown in Fig. 56.1b. The P2P botnet was introduced in early 2007 and it has a decentralized structure differed from other existing botnets. Especially, the major characteristic of the P2P botnet is that all peers can play a role of the C&C server, because each bot-infected PC is connected by a P2P protocol. Therefore, botmasters have started to use botnets without single point failure, using decentralized P2P structure [4, 5]. Actually, it is hard to break, because the scale of the P2P botnets can be maintained and/or expanded by performing communications with bot-infected PCs that are largely distributed using the P2P protocol and that leads to configure a larger network.

56.3 P2P Botnet Detection Methods

Bot peers of the P2P botnet attempt the communication with the other bot peers as many as possible. Accordingly, the large amount of traffic is generated, because those bot peers find the other peers and exchange the information continuously

[6, 7]. Therefore, the techniques for detecting the P2P botnet based on these traffic features had been studied.

56.3.1 Data Mining

Liu et al. [8] proposed a method for detection using the network streams analysis and data mining techniques. The proposed method filters the streams of P2P botnet based on characteristics of paroxysm and distribution which can be discovered in P2P botnet. Also it find the peer sets according to the cohesion in a P2P network, then distinguish P2P botnet by comparing with the common botnets' behaviors of the each peer in P2P network.

Liao et al. [5] proposed a method that used data mining techniques to analyze network behavior based on network traffic monitoring at the gateway. In order to perform the data mining, it used J48 algorithm, Naïve Bayes and WEKA which is the freeware used as an academic purpose. As a result, it could discover the flow of the P2P botnet among the mixed flows.

56.3.2 Machine Learning

Saad et al. [9] proposed a method to characterize and detect P2P botnets using network traffic behavior analysis and machine learning. It performed the network traffic analysis in order to classify the various traffic types. In addition, the method used packet information such as payload size, the number of packets, duplicated packet length and port numbers to make traffic feature sets. As a result, it could detect the P2P botnet in command and control phase before the P2P botnet launch the attacks.

56.3.3 Network Behavior and Traffic Analysis

Noh et al. [6] proposed a method for modeling multi-phased flows of P2P botnet traffic. It includes flow grouping, flow compression and flow modeling. The flow grouping clusters the TCP/UDP connection and measures similarity of each flow. The flow compression is performed in the flow grouping and then, transition matrix is organized in the flow modeling step. Finally, the detection engine detects the P2P botnet traffic by using the similarity calculated from the flow models.

Gu et al. [10] proposed BotMiner which is a botnet detection framework that is independent of the protocol and structure of botnets. It clustered hosts that have similar pattern of communication and behavior and then it performed cross correlation across each cluster. If host has both behaviors, the host is detected as a bot.

Zhang et al. [11] proposed a P2P botnet detection system that can identify the stealthy P2P botnets. It identified all hosts which are communicating using P2P protocol in the monitored network. And then, it derived the statistical fingerprints about the P2P communication traffic which were generated by infected hosts. These obtained statistical fingerprints of P2P botnet can be used to distinguish between the normal P2P network and P2P bots.

56.4 Conclusion

Botnets have become a most serious threat in Internet. Since the attacks using the botnets are continuously increased, the various techniques for detecting the botnetss had being studied.

In this paper, we described a general type of P2P botnets and summarized about the P2P botnet detection methods. Most of the proposed methods captured and analyzed network traffic and then each method applied data mining and/or machine running in order to detect P2P botnets, respectively.

Acknowledgments This work was supported by the Mid-career Researcher Program of the NRF grant funded by the MEST (NRF 2010-1179-000).

References

1. Freiling F, Holz T, Wicherski G (2005) Botnet tracking: exploring a root-cause methodology to prevent distributed denial-of-service attacks. In: Proceedings of the 10th European symposium on research in computer security. pp 319–335
2. Zhu Z, Lu G, Chen Y, Fu ZJ, Roberts P, Han K (2008) Botnet research survey. In: Proceedings of the 32nd annual IEEE international conference on computer software and applications. pp 967–972
3. Choi H, Lee H, Lee H, Kim H (2007) Botnet detection by monitoring group activities in DNS traffic. In: Proceedings of the 7th IEEE international conference on computer and information technology. pp 715–720
4. Ha DT, Yan G, Eidenbenz S, Ngo HQ (2009) On the effectiveness of structural detection and defense against P2P-based botnets. In: Proceedings of the 39th annual IEEEIIFIP international conference on dependable systems and networks, pp 297–306
5. Liao W, Chang C (2010) Peer to peer botnet detection using data mining scheme. In: Proceedings of the international conference on internet technology and applications, pp 1–4
6. Noh SK, Oh JH, Lee JS, Noh BN, Jeong HC (2009) "Detecting P2P botnets using a multi-phased flow model. In: Proceedings of the 3rd international conference on digital society IEEE, pp 247–253
7. Han KS, Lim KH, Im EG (2009) The Traffic Analysis of P2P-based Storm Botnet using Honeynet. J KIISC 19(4):51–61
8. Liu D, Li Y, Hu Y, Liang Z (2010) A P2P-botnet detection model and algorithms based on network streams analysis. In: Proceedings of the international conference on future information technology and management engineering, pp 55–58

9. Saad S, Traore I, Ghorbani A, Sayed B, Zhao D, Lu W, elix J, Hakimian P (2011) "Detecting P2P botnets through network behavior analysis and machine learning. In: Proceedings of the 9th annual international conference on privacy, security and trust, pp 174–180
10. Gu G, Perdisci R, Zhang J, Lee W (2008) BotMiner: clustering Analysis of network traffic for protocol- and structure-independent botnet detection. In: Proceedings of the 17th conference on security symposium, pp 139–154
11. Zhang J, Perdisci R, Lee W, Sarfraz U, Luo X (2011) Detecting stealthy P2P botnets using statistical traffic fingerprints. In: IEEE/IFIP 41st international conference on dependable systems and networks, pp 121–132