Botnet Detection Techniques

Jihan Barazi Jihan-barazi@hotmail.com

Ahmad Jakalan ahmad@njnet.edu.cn

Wang XiaoWei xwwang@seu.edu.cn

ABSTRACT: *Botnet detection and response is currently an arms race. The bot-masters rapidly evolve their botnet propagation and command and control technologies to evade the latest detection and response techniques from security researchers. Researches in botnets in addition to botnet detection include also Tracking, Measurement, Prediction, and Countermeasure. In this study, we try to raise main points in the field of botnet detection techniques.*

Keywords: Botnet, Botnet detection, Network Security.

1. Introduction

A “bot” is a short for robot, or it is also called a Zombie. A computer infected with a malware, which allow the remote attacker to control the infected computer without the knowledge of the owner of the infected machine. **Botnet** is a network of compromised computers remotely controlled by its bot-herder, or bot-master under a common Command-and-Control (C&C) infrastructure. The main difference between botnet and worms is the use of common Command and Control channels to control the army of zombies infected by the botnet herder. In this paper, we investigate the techniques used by security researchers to detect botnets. Researchers classified these techniques into main two categories: Honeypot-based botnet detection and Network-based botnet detection, the former one depends on deploying a honeypot system to collect and analyze botnets, while the later depends on capturing network traffic and monitoring network behavior to detect botnet activity on the monitored network. Botnet detection and response is currently an arms race. The bot-masters rapidly evolve their botnet propagation and command and control technologies to evade the latest detection and response techniques from security researchers[1]. Researches in botnets in addition to botnet detection include also Tracking, Measurement, Prediction, and Countermeasure[2]. In this report, we will try to raise main points in the field of botnet detection techniques.

2. Honeypot-based botnet detection

A honeypot is an information system resource, which value lies in unauthorized or illicit use of that resource; they are vulnerable systems waiting for attacks. The idea behind this methodology is to lure in attackers such as automated malware and then study them in detail. Honeypots have proven to be very effective tools in learning more about Internet crime like botnets. There are two general types of honeypots:

The first one is *Low-interaction honeypots:* They emulate services or operating systems with a low

Received March, 14, Reviewed April 20 2014

level of interaction. Implementing this type of honeypots tends to be low risk, the main intention is to *capture harmful code samples*, and deployment and maintenance tend to be easy. A popular example of this kind of honeypots is *Nepenthes.* In our research published in our paper [3] we used the low-interaction honeypot “nepenthes” to detect botnets. A distributed framework of Nepenthes honeypots was built to collect as more as possible malware samples. The authors have optimized. The configuration of Nepenthes to improve the capture efficiency. Later, they have analyzed these samples firstly by features via antivirus scan, then by behavior via two different online sandboxes in different periods and multiple times for obtaining accurate behavior. The second type is *High-interaction honeypots* allowing the attacker to interact with a real system. The risk of deploying tends to be higher, so it is required to establish precautions and special provisions to prevent attacks against the system, more complex to setup and maintain. The main intention is to understand the attack scene, concerned that the attacks on the process, it requires a strong ability to interact with the attacker. The most common setup for this kind of honeypots is a *GenII Honeynet*. Many papers discussed how to use honeynets for botnet tracking and measurement. The Honeynet Project [4], for example, has done extensive work on capturing live bots and characterizing botnet activities, and a group of white-hat vigilantes is scouring the Internet looking for evidence of botnets. Honeynets are mostly useful to understand botnet technology and characteristics, but do not necessarily detect bot infection.

3. Network-based botnet detection

In their paper Wei Lu and Ali A. Ghorbani [5] proposed a new approach for detecting and characterizing botnets on a large-scale WiFi ISP network. They first classified the network traffic into different applications by using payload signatures and a novel clustering algorithm and then analyzing the specific IRC application community based on the temporal-frequent characteristics of flows that leads the differentiation of malicious IRC channels created by bots from normal IRC traffic generated by human beings. They evaluated their approach with over 160 million flows collected over five consecutive days on a large-scale network and results showed that the proposed approach successfully detects the botnet flows from over 160 million flows with a high detection rate and an acceptable low false alarm rate. In 2008 Gu et al [6] proposed ***BotSniffer*** which is an approach that uses network-based anomaly detection to identify botnet C&C channels in a local area network without any prior knowledge of signatures or C&C server addresses. This detection approach can identify both the C&C servers and infected hosts in the network. This approach is based on the observation that, because of the pre-programmed activities related to C&C, bots within the same botnet are likely to demonstrate spatial-temporal correlation and similarity. For example, they engage in coordinated communication, propagation, and attack and fraudulent activities. BotSniffer, can capture this spatial-temporal correlation in network traffic and utilize statistical algorithms to detect botnets with theoretical bounds on the false positive and false negative rates. BotSniffer was evaluated using many real-world network traces. The results showed that

BotSniffer can detect real-world botnets with high accuracy and has a very low false positive rate.

Another proposed framework by GU et al for Botnet detection was ***BotMiner*** [7] that is independent of communication protocols, structure and history knowledge of Botnet. It captures identical communication and malicious traffic, and performs cross cluster correlation to determine the bots that distribute communication and malicious activity patterns. BotMiner is implemented in a real-scenario and produce low false rate. An improvement to botminor was proposed by Yu et al called ***SBotMiner*** [8] to identify low rate traffic generated bots. SBotMiner focus on identifying groups of boats rather than capturing individual booths. SBotMiner is mainly consisting of two fundamental steps i.e. To identify the group activity that is different from history and by using Matrix based scheme to differentiate between human traffic and Botnet generated traffic. Bots within the same Botnet perform the same malicious activities by running the script issued from the master where as human traffic contains diversity. In 2010, Hossein Rouhani Zeidanloo et al [9] proposed a new general detection framework. This proposed framework is based on finding similar communication patterns and behaviors among the group of hosts that are performing at least one malicious activity. The point that distinguishes this proposed detection framework from many other similar works is that there is no need for prior knowledge of Botnets such as Botnet signature that means improvements in zero-day botnet detection.

4. Conclusion

Most of the current botnet detection techniques work only on specific botnet C&C communication protocols and structures. Consequently, as botnets change their C&C communication architecture, these methods will be ineffective[10]. The work done in the area of security against and removal of, Botnet Trojans has not been sufficient and each company continues to head towards their own discrete strategies. Amin Hossein Far et al [11] proposed a standardization in Botnet detection strategies within nodes and servers across security companies this is because that now security strategies vary greatly between companies. In addition to the needs for an integrated law and regulation accepted by all countries.

References

[1] W. Lee, C. Wang, and D. Dagon, *Botnet detection : countering the largest security threat*, New York ; London: Springer, 2008.

[2] C. X. FANG Bin-Xing, WANG Wei, “A Survey of Botnets,” 2011.

[3] A. Jakalan, G. Jian, and L. Shangdong, “DISTRIBUTED LOW-INTERACTION HONEYPOT SYSTEM TO DETECT BOTNETS,” *International Conference on Computer Engineering and Technology, 3rd (ICCET 2011)* 2011.

[4] “The Honeynet Project. Know Your Enemy : Learning about Security Threats. Addison-Wesley Professional; 2 edition (May 17, 2004), March 2004.

[5] L. Wei, and A. A. Ghorbani, “Botnets Detection Based on IRC-Community,” *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*, pp. 1-5, Nov. 30-Dec. 4, 2008.

[6] G. Gu, J. Zhang, and W. Lee, “BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic,” *In Proceedings of the 15th Annual Network and Distributed System Security Symposium (NDSS'08), San Diego, CA, Febrnary2008*, 2008.

[7] G. Gu, R. Perdisci, J. Zhang, and W. Lee, “BotMiner: clustering analysis of

network traffic for protocol- and structure-independent botnet detection," in Proceedings of the 17th conference on Security symposium, San Jose, CA, 2008, pp. 139-154.

[8] F. Yu, Y. Xie, and Q. Ke, "SBotMiner: large scale search bot detection," in Proceedings of the third ACM international conference on Web search and data mining, New York, New York, USA, 2010, pp. 421-430.

[9] H. R. Zeidanloo, A. B. Manaf, P. Vahdani, F. Tabatabaei, and M. Zamani, "Botnet Detection Based on Traffic Monitoring," *201O International Conference on Networking and Information Technology*, 2010.

[10] M. Feily, A. Shahrestani, and S. Ramadass, "A Survey of Botnet and Botnet Detection," pp. 268-273, 2009.

[11] H. J. Amin Hosseinian Far, Rouzbeh Ghazihesami, "Botnet Future Trend," 2010.

Jihan Barazi **R**eceived the B.S. degrees in Informatics Engineering from University of Aleppo, Syria in 2005. Now she is a Master Degree student in Southeast University, school of Computer Science and Engineering. Her research is in the field of honeypot and malware analysis.

Ahmad Jakalan Received the Master Degree in Computer Science from Southeast University, China. Now he is a PhD student in Southeast University, China. His research area is in Computer Networks Security.

Wang XiaoWei is an Associate Professor in the school of Computer Science and Engineering, Southeast University, China. Her Research Interests: computer architecture, embedded systems.