I.J. Engineering and Manufacturing, **2012,1, 22-26**
Published Online February 2012 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijem.2012.01.04

Available online at http://www.mecs-press.net/ijem

The Detection of Intrusion Through P2P Botnet Based on the Analysis of Successful Connection Rate and Average Packet

LIU Jian-bo

Network Center, Shandong University of Fiance, Jinan, 250014, China

Abstract

Through the research on the mechanism of the P2P botnet, this paper proposes a algorithm of intrusion detection by P2P botnet based on the analysis of successful **c**onnection **r**ate. According to the flow, it gets a data collection including three vectors, such as source IP, destination IP and package size, does dynamic analysis of the successful connection rate and average packet. Through the comparison with the methods between the traditional network and normal P2P,this paper provides intuitive figures in which we could locate the position of intrusion by P2P botnet accurately, therefore the algorithm could provide the gist for detecting the intrusion in time.

Index Terms: intrusion;P2P botnet; successful connection rate ;flow; average packet; clustering

1. Introduction

Hacker attacks by botnet is one of major problems of the security fields. With wide application of P2P technology, as well as the existence defects of the traditional botnet based on IRC protocol, some new attacks of botnet program began to use P2P protocol, with which they could construct their commands and control mechanisms more anonymously. Different from the attacks by IRC protocol botnet, this kind of attack does not exist center control point. For example, when some attack bots are discovered, the whole botnet net will not be affected, the attack among the network still exists, so this type of attack by P2P botnet is more latent and threatening.

2. Academic Research Situations

Because of the personalized difference of the intrusion by P2P botnet, there isn't a general detection method now, but with continuous development of P2P botnet in recent years, it is an important research topic that how to construct effective detection method to locate the intrusion by P2P botnet. Through the virus of binary code for

* Corresponding author.
E-mail address: liujb@sdfi.edu.cn

disassembly Holz Thorsten analyzed the zombie virus propagation mechanism, malicious behavior and control channel encryption method etc, thus realized the tracking, detection and duplication of the intrusion . HuangShaoYin of Fudan university proposed a multiphase flow model based on P2P botnet flow to locate the same type of attack, which focused on multiple flow of a Bot node produced when it makes communications with lots of remote nodes. Similar to this method, the method presented in this paper is also based on the test of network flow.

3. Data Capture and preprocessing

Through the analysis of different P2P protocols, it is found that almost all the P2P protocols establish contact via TCP. Therefore, the method could filter the TCP flow from the whole flow firstly, which could be grasped by NetFlow. According to the type of packets, the paper could get indexical data acquisition including three vectors such as destination address, source address and packet size (average packet size), which are stored in the database and analyze the botnet based on the algorithm of connection rate detection, by which we could find out the intrusion in the whole network.

4. Algorithm Based on Connection Rate

4.1. Algorithm Overview

In P2P botnet, each node tries to establish links to some infected hosts from its initialization, but destination IP is often static or stochastic dynamic designated. Either way, because of the instability of P2P botnet, the node will last for related links; however its successful rate is not high. According to this characteristic, the algorithm to detection the intrusion can be described mainly by the rate of successful connection, in which the Variables are defined as follows:

Definition 1. SenPackIPCount: The number of different destination IP address in SYN packets send by nodes

Definition 2. RecPackIPCount: The number of different destination IP address in SYN packets received by nodes.

Based on the above two definitions, we can calculate the nodes' rate of successful connection in a certain period(the sliding time window defined in the algorithm):

ConRate= SenPackIPCount/ RecPackIPCount.

4.2. Implementation of the Algorithm

Firstly, for I=1 to RecordCound ,the paper calculates SenPackIPCount and RecPackIPCount (RecordCount is the number of database records) and queries the SrcIp and DstIp by SQL statements respectively. Secondly, the algorithm could gain statistical outcome of different IP addresses and respective numbers, which are stored into the arrays such as SrcIp[j], SenPackIPCoun[j],DstIp[j] and RecPackIPCount[j].

The program could be achieved through Visual C++ based on the above algorithm, with the reasonable definition of time sliding window (flow capture period),it could calculate the rate of successful connection of each node, which could be the orientation purposes for the analysis of intrusion by P2P botnet.

5. Test and verify

5.1. The analysis of the rate of successful connection

In the experiments, in order to find the distinction of successful connection rates between P2P botnet and traditional flow,this paper builds three different environments, such as P2P botnet, traditional network and P2P network, and studied three connecting rates. The data could be grasped from the mirror port of switch. The sliding time window is defined as 50 seconds. The follow figure shows the successful connection rates of three environments.

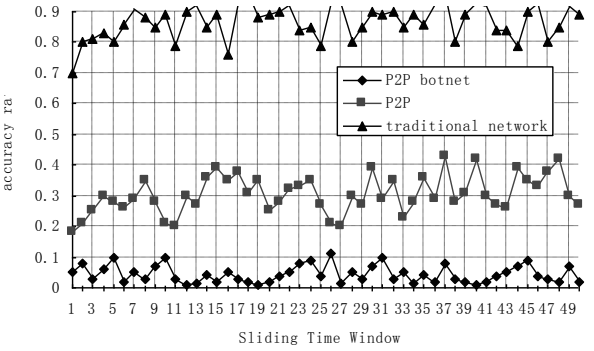

Fig. 1. The Connection Rates

It can be seen from the above figure that the traditional network has the highest connection rate, which is between 0.6 and 0.9, yet the rate of the normal P2P network is lower, which is between 0.2 to 0.5, and the rate of P2P botnet is relatively lower, which is between 0 and 0.1. It has inevitable connection with the operation mechanism of P2P botnet. In general, there are fixed (hard coded) and waiting peer points. For example, during peer initialization, Nugache usually attempts to make connection with 22 pre-assigned IP addresses, because these specified nodes are easy to be closed, the connection rate is much lower than normal network.

5.2. Clustering analysis of Average Packet

In order to analyze the intrusion fatherly, by the method of clustering, we do analysis of the average packet . There are many clustering algorithms to use, In the experiments, we made use of *k*-means, by which the experiments could get the change rule of average packets of different nets. Same as above, we need define reasonable sliding time window (10 seconds), the following figure shows the dynamic clustering outcome of the average packet.

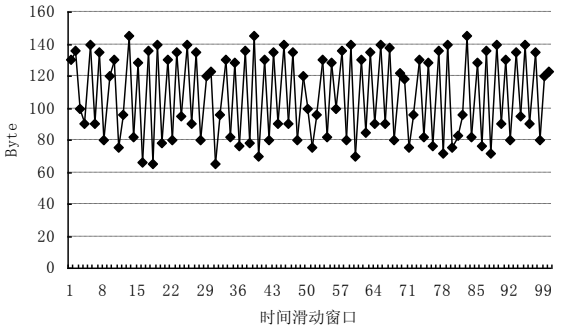

Fig. 2. Average packet of host 192.168.0.1

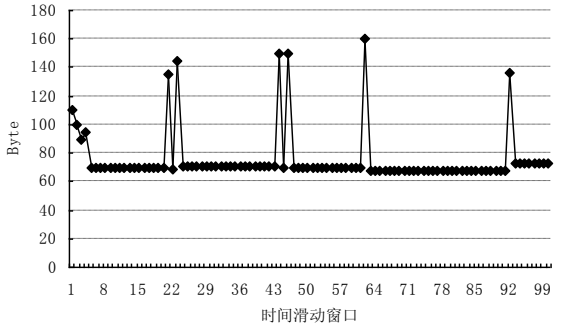

Fig. 3. Average packet of host 192.168.0.2

It can be seen from the above two figures that the average packet of host (192.168.0.1) has balanced movements, presents a center type of sine graphics, undulation and sudden flow is less, and the distribution is symmetrical, which explains that the packets are very active and the network in normal. Otherwise, host(192.168.1.2) maintains small packets for long time, and there are sudden flow phenomenon, which explains that there are coordinated attacks.

From the above analysis, we can see that the process of intrusion detection by P2P botnet could do as follows: Firstly locate the P2P botnet by the analysis of successful connection rate, in order to confirm the attack pot more accurately, we need do analysis toward its average packet .Only by these two processes, could we find out the intrusion by P2P botnet in time and reduce the loss by attack.

6. Conclusion

With the rapid development of technology of computer and network, hacker attacks by botnet turned more and more frequent and difficult to been found, which has caused great threat to the computer network . In view of technical characteristics and operation mechanism of P2P botnet, the automated detection mechanism could be established effectively to turn down its spread. This paper proposed a general detection method based on analysis of successful connection and average packet. The experimental results have shown that this method was

effective, and could be deployed to the core layer of exchange network to detect the intrusion by P2P botnet effectively.

References

[1] ZHANG Chen, WANG Liang, XIONG Wen-zhu. Technologies of P2P Botnet detection [J]. Journal of Computer Applications, 2010.30(6):117-118.
[2] WANG Tao,YU Shun-zheng. NovelM ethod for Detecting Centralized Botnet [J]. Journal ofChinese ComputerSystems, 2010.31(3):512-514.
[3] Zhang Xi Tang Heping. Study on Botnet Based on P2P [J]. Computer & Digital Engineering.2009.37(2):94-95
[4] YU Xiaocong,DONG Xiaomei1,YU Ge et al. Online Botnet Detection Technique [J].JGeomatics and Information Science of Wuhan University.2010.35(5):579-580.
[5] Karasaridis A, Rexroad B, Hoeflin D. Wide-scaleBotnet Detection and Characterization[C]. The 1stWorkshop on Hot Topics in UnderstandingBotnets,Cambridge,2007.
[6] AnagnostakisK G, Sidiroglou S, Akritidis P, et a.l Detecting tar-geted attacks using shadow honeypots[C]. In Proceedings of14thUSENIX Security Symposium, August2005,142-144.
[7] Wang P, Sparks S, Zou CC. An Advanced HybridPeer-to-Peer Botnet[C]. Proc. of the 1st Workshop on HotTopics in Understanding Botnets (HotBots 2007), Boston,2007
[8] ZHOU LINGYUN. VMM-based framework for P2P Botnets tracking and detection[C]//Proceedings of the 2009 International Confercence on Information Technology and Computer Science. Washing-ton, DC:IEEE Computer Society, 2009:174-175.