Advanced Science and Technology Letters
Vol.44 (Networking and Communication 2013), pp.18-21
http://dx.doi.org/10.14257/astl.2013.44.05

The Design for Detecting and Monitoring P2P Botnet

Yuhui Fan[1], Ning Xu[1]

[1]Department of Computer and Information Engineering, Huainan Normal University, Huainan, China
122336956@qq.com

Abstract. Through the research on the life cycle of P2P botnet host, integrated with offline and online modes, this paper proposes a new technique to analyse the captured export network flow, and to detect and monitor the P2P botnet hosts which are on initial stage, trance stage and attack stage, then make the identified P2P botnet hosts live in isolation. The solution can implement the detection of P2P botnet hosts more efficiently and precisely, and reduce the harm of the botnet.

Keywords: P2P; botnet; life cycle; SMTP; Spam

1 Introduction

The number of Chinese Internet users has reached 450 million, but CNCERT claimed the number of IP for botnet control server in 2010 was 13,782 in The 2010 China Internet Network Security Report [1]. Government departments, commercial institutions and common users suffered a lot from net theft, DDoS attack and a mass of spam caused by Botnet, which has been affecting seriously Internet security.

2 Correlational rationale

While the newly emerging botnet based on P2P protocol has different control nodes distribution throughout the net, which do no virtual harm to the whole net when one or several nodes destroyed. So botnet based on P2P protocol is more elusive and has more damage resistance than ever.

There are two ways to detect P2P botnet at present: one is off-line detection, the other is on-line detection. The former can distinguish the existing botnet during the detection but cannot take control measures immediately, while the later can detect the botnet instantly but is powerless to deal with the mass of net flow. In all, it is urgent to detect, distinguish and control botnets in the network study.

ISSN: 2287-1233 ASTL

3 Behavioural analysis of P2P botnet's survival features

The present detections of P2P botnets focus on the analysis of the botnet flow[2~5], thus they are distinguished from other P2P applications. After that, the infected hosts by botnets are recognized through off-line detection and on-line detection. We find the P2P botnets are grouped into initial stage, trance stage and attack stage according to network flow [6].

In the above analysis, the important features are:

(1)P2P botnet hosts produce many ICMP reports with low rate of successful linking during the initial stage; (2)P2P botnet hosts are linked to many nodes with the same communication traffic during the trance stage; (3)P2P botnet hosts produce too much SMTP contact with too much similar data package of destination address during the attack stage.

Above all, the features in (1), (2) can be extracted off-line to detect the address of P2P botnets hosts and the hosts can be monitored on-line. If behaviors like in (3) are spotted, the hosts can be stopped immediately.

4 Sign for detection of botnet hosts' behavior

This paper designs a detection of combining the off-line detection and on-line monitoring to minimize the impact from the P2P botnet hosts to other users.

(1) Design of the Off-line Detection

Detection of connection success rate

When P2P botnet hosts are linked the botnet nodes in the network, the connection success rate will be very low due to the firewall block, network address conversion or not-online hosts and so on. The connection success rate is obtained to tell the abnormal network of the hosts. If the rate is between 0 and 0.1, it shows the low connection between the source address and outside destination address, which can be caused by the suspected botnet hosts, as in [7,8].

Detection of similarity of communication traffic

Since P2P botnet hosts will keep the continuous contact with the botnet nodes to wait for the controller's commands after the linking, and P2P botnet hosts mostly are in this trance stage in its life cycle, there will be P2P botnet hosts behaviors like a great deal of nodes linking, similar communication traffic between nodes and little communication traffic. Markov chain then is employed to calculate the change in those status values, the result of which is compared to the normal network flow to tell whether there is the botnet host.

Feasibility of off-line detection

Since detection of similarity of communication traffic follows detection of connection successful rate, the detection range is greatly reduced, the speed increased and misreport ratio decreased. But those two detections are based on 2 sampling time, and are likely to fail to report.

(2)Design of On-line Monitoring

The suspected botnet hosts through the off-line detection in the address set are all in their initial stage and trance stage and do no harm to other hosts or network. There will be misreports if they are judged as botnet hosts. So the paper here suggests the on-line and continuous monitoring of the suspected hosts to precisely locate P2P botnet hosts. Once there is the harmful behavior, the suspected host will be stopped to minimize the harm.

Design of monitoring

Deng Guoqiang (Deng Guoqiang,2011) employs the sampling time expressed as To in the design[9]. SMTP flow data will be captured in every period. According to7-element data stream collection, the data flow number in the collection is counted. If the flow number is over 100, the host can be thought to be sending spam. The number of the same destination address with different source address in SMTP flow data should be counted, if the number is over 10, the source address of the hosts is the address of the same P2P botnet, and the source address should be put on blacklists too.

Confirmation of control of P2P botnet hosts

The host address in the blacklists can be confirmed as the member of P2P botnet, and the host can be blocked off at the network exports router. So the host cannot be linked to outer nets including botnets to decrease its danger.

Feasibility of on-line monitoring design

Since the above on-line monitoring is based on the suspected P2P botnet hosts collection, which is detected off-line, the monitoring is more targeted and its conclusion is more accurate. Yet, there may be the failure to report the P2P botnet hosts whose key feature is to send spam in the detection, but the chance of misreport is slim.

5 Simulation experiment

We use two networked PCs with 4G memory as an experimental platform. We install Vmware on PC A, and simulate 4 P2P zombie host, are A1, A2, A3, A4. The control program is installed on PC B, this PC is used to send control commands to the P2P bots. These hosts are connected to form network.

The first time, we mixed the sample data up with the normal network export traffic, and detected of mix data through off-line detection, then we got the suspected bot's IP address. The second time, we copied sample data three times and mixed up the normal network export traffic, then we got the suspected bots' IP address through off-line detection twice.

Through analysis of the experimental data, we draw an conclusion that enhancing sampling frequency will effectively decrease the misreport rate, and has an influence on the implementing effect of the whole scheme.

6. Acknowledgment

This research was supported by the Anhui provincial college and university Natural Science Foundation, China (No. KJ2012Z363, No.KJ2013Z302).

7. Conclusion

In all, the combination of the on-line monitoring and the off-line detection is helpful to detect P2P botnet hosts, and greatly relieves the load of detection platform. Off-line detection can be carried out by time period to obtain the blacklists of the suspected botnet hosts. On-line monitoring is supposed to capture and analyze the SMTP data traffic, which is a very small part of the protocol flow at the network outlet. So the monitoring can be implemented easily at the large outlet flow. Through the above analysis, the botnet hosts should be confirmed in the attack stage. There may be the failure to report the botnet hosts if they are not in the attack stage, but if the botnet hosts are stopped and separated in the attack stage, the danger of the botnet is lessened because botnet hosts mainly do harm to others in the attack stage.

References

[1] CNCERT/CC. CNCERT/CC Annual Report 2010. http://www.cert.org.cn/UserFiles/File/CNCERTAnnualReport2010v2.pdf
[2] Junjie Zhang, Perdisci R, Wenke Lee, Sarfraz U., Xiapu Luo. Detecting stealthy P2P botnets using statistical traffic fingerprints. Proc of the 41st Annual IEEE/IFIP International Conference on Dependable Systems and Networks Piscatawa:IEEE Press, 2011:121-132.
[3] Saad S., Traore I., Ghorbani A., Sayed B., Zhao D., Wei Lu, Felix J., Hakimian P. Detecting P2P botnets through network behavior analysis and maching learning. Proc of the 9th Annual International Conference on Privacy, Security and Trust Piscatawa:IEEE Press, 2011:174-180.
[4] Jian Kang, Jun-yao Zhang, Qiang Li, Zhou Li. Detecting new P2P botnet with multi-chart CUSUM. Proc of International Conference on Networks Security, Wireless Communications and Trusted Computing. Woshington D C:Computer Society, 2009:688-691.
[5] Gu Guofei, Perdisci R, Zhang Jun-jie. BotMiner: Clustering analysis of network traffic for protocol-and-sturcture-independent Botnet Detection[C] //Proc of the 17th USENIX Security Symposium. Berkeley:USENIX Association, 2008:139-154.
[6] CHAI Sheng, HU Liang, LIANG Bo. The P2P Botnet Online Detect Approach Research. Acta Electronica Sinica,2010,4:906~912
[7] Schoof R, Koning R. Detecting peer-to-peer botnets. System and Network Engineering. University of Amsterdam, 2007
[8] Liu Jianbo. Detection of P2P Botnet Based on Analysis of Flow. Computer & Digital Engineering, 2011.3:90:91
[9] DENG Guo-qiang, LI Zhi-tang, LI Dong, LI Zhan-chun. Design and implementation of a behavior based algorithm to detect spam zombie client. Journal of Guangxi University(Natural Science Edition), 2011,36:100-10

