Advanced Science and Technology Letters
Vol.140 (GST 2016), pp.260-263
http://dx.doi.org/10.14257/astl.2016.140.50

Intelligent Detecting Technique of APT Attack

Sun-Myung Hwang[1], Seong-Uk Park[1], Jung-Tae Kim[2]

[1] Daejeon University, Computer Engineering Dept., 62,Daehak-ro, Dong-gu, Daejeon, Korea , sunhwang@dju.kr, pppforte@gmail.com
[2] Electronics & Telecommunications Research Institute, 161,Gajeong-dong Yuseong-gu, Daejeon, Korea , jungtae_kim@etri.re.kr

Abstract. As the Social and Financial damages caused by APT attack are increased, the technical solution against APT attack is required. However, it is difficult to protect APT attack with existing security equipment. We implemented a testbed can collect attacker's data and analyze behavior of them. In this paper, we propose an intelligent technique to analyze pattern and behavior using Net Flow data, and generate test data based on scenarios to detect anomaly.

Keywords: APT, DDOS, Netflow, Intelligent Detecting

1 Introduction

Nowadays, DDoS (Distributed denial of service) attacks on web sites reward attackers financially or politically because our life tightly depends on web services such as on-line banking, e-mail, and e-commerce. One of DDoS attacks to web servers is called APT flood attack which is becoming more serious. As the social and financial damages caused by APT attack such as cyber terror are increased, the technical solution against APT attack is needed.

Most existing techniques are running on the application layer because these attack packets use legitimates HTTP-GET request and malicious requests.

We propose a practical detection technique against APT attack based on the access behavior of inline objects in a webpage using Net Flow.

2 APT Attack

In general, APT attack has the characteristics such as advanced, persistent and threat. The stage of APT attack is as fallows;

a. Advance Preparation
b. Internal Network Intrusion
c. Internal Activity
d. Goal Achievement

ISSN: 2287-1233 ASTL

Therefore, various event information on host network and legacy node have to analyze and detect the anomaly cased of attacker on netflow against advanced APT attack.

2 Construction of Test Bed

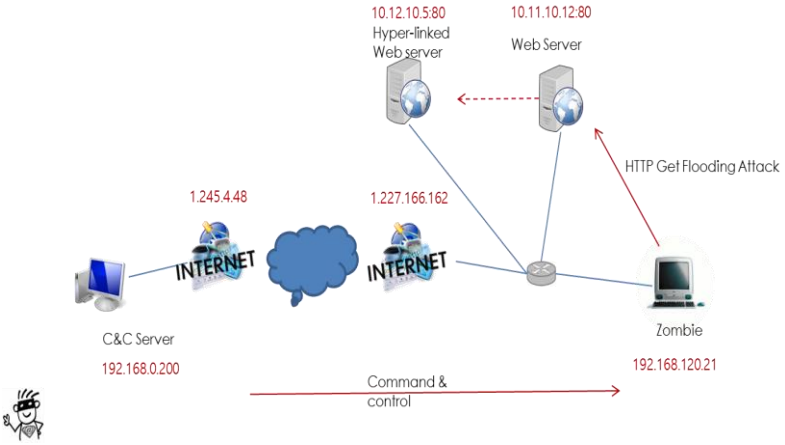

Fig. 1. Test bed

We constructed the test environment contains Netbot in Figure 1

The Test bed can test which occurs various APT attacks based on possible scenarios.

The C&C server has a separate IP network, attacking the web server by using one C&C server and one zombie PC. These series of attacks are configured to collect flows on the network using Netflow.

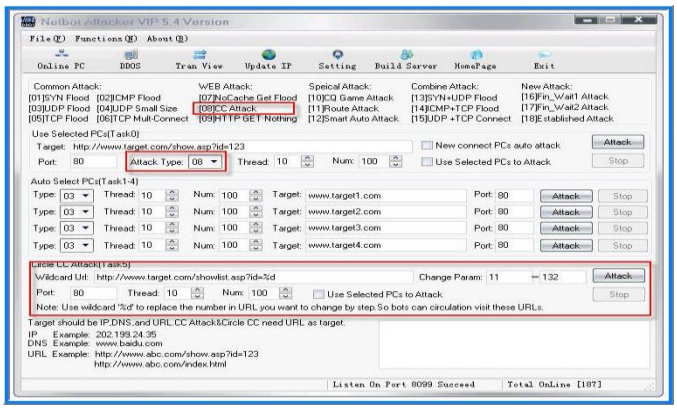

Fig. 2. xDoS Flow Analysis based on the Netbot Attacker

The Netbot attacker in Figure 2 is a remote control program that uses DDoS attack to the other side using a zombie PC. You can instruct 21 attack methods such as 'http-get flood' attack method with the designated ip to the zombie pc created by virus in advance.

4 Flow Analysis Tool and Result

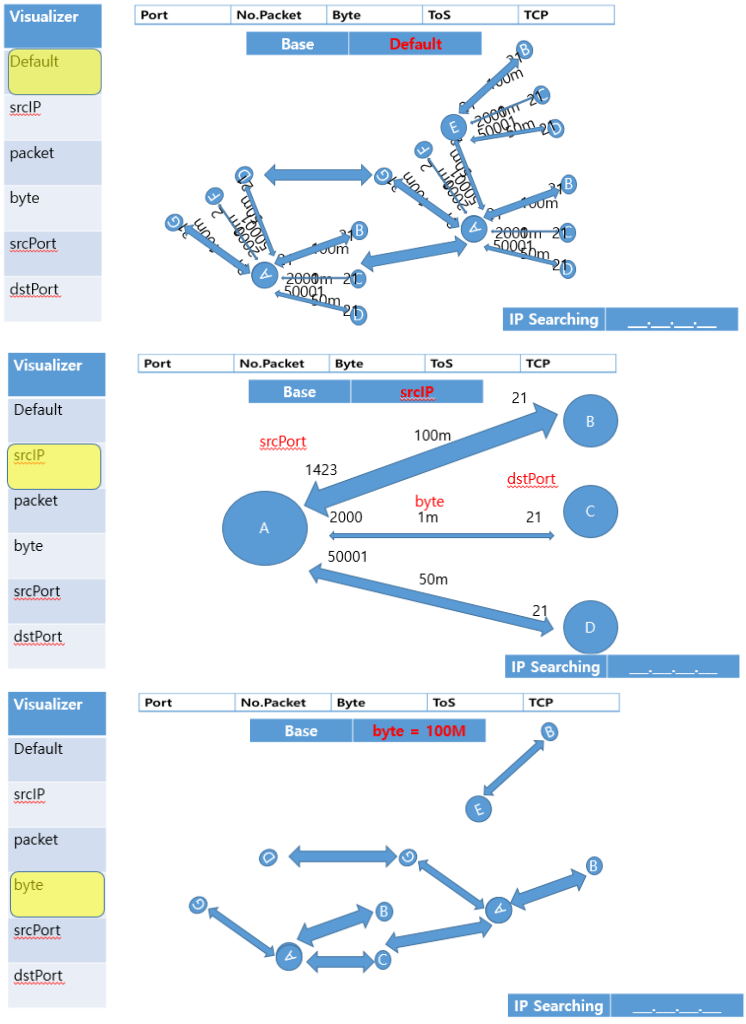

Fig. 3. Sample Image Flow Analysis Tool

In the default state, the entire flow data is displayed and the flow menu based on 'Source IP', 'Packet', 'Byte' etc. can be displayed through the detailed menu for Figure 3. Each arrow represents the byte size of each IP relationship and displays the correlation. It will also have a relationship with the specified IP or the ability to display more than a certain byte size.

5 Conclusions

In this paper, we propose a method to detect APT attacks based on network traffic flow information using Net Flow.

To do this, a test bed was constructed and a tool for analyzing source IP, packet, byte and source port / destination port based on the traffic quality was developed by test scenarios of simulation attack.

Acknowledgments. This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government (MSIP) (No. B0101-15-1293, Cyber-targeted attack recognition and traceback technology based on the long-term historic analysis of multi-source data).

References

1. Yatagai, T., Isohara, T., Sasase, I.: Detection of HTTP-GET flood Attack Based on Analysis of Page Access Behavior, Proceeding of IEEE Pacific Rim Conference, pp. 232-235, (2007)
2. Introduction to Cisco IOS NetFlow, http://cisco.com
3. Chwalinkski, P., Belavkin, R., Cheng, X.: Detection of Application Layer DDoS Attack with Clustering and Likelihood Analysis, Proceedings of Globecom, 2013.
4. NSHC, “3.20 South Korea Cyber Attack, Red Alert Research Report, “http://training.nshc.net/KOR/Document/virus/20130321_320CyberTerrorIncidentResponseReportbyRedAlert(EN).pdf, (2013)
5. Tankard, C.: Persistent threats and how to monitor and deter them, *Network security*, Vol. 2011, No. 8, pp. 16-19, Aug, (2011).