Collaborative Behavior Visualization and Its Detection by Observing Darknet Traffic*

Satoru Akimoto, Yoshiaki Hori, and Kouichi Sakurai

Graduate School of Information Science and Electrical Engineering, Kyushu University, Fukuoka, Japan
Institute of Systems, Information Technologies and Nanotechnologies, Fukuoka, Japan
akimoto@itslab.inf.kyushu-u.ac.jp, hori@inf.kyushu-u.ac.jp, sakurai@csce.kyushu-u.ac.jp

Abstract. Recently, we have a problem about an attack generated by a botnet which consists of a group of compromised computers called bots. An attacker called botmaster controls it and a botnet invokes an attack such as scanning and DDoS attack. In this paper, we use the 3D-visualization to investigate the change of attack according to the darknet traffic. As a result, we discover the attack in which several source IP addresses transmit packets to a single destination within a short period of time. In addition, we find that the packet size and the destination port number are identical on its attack. Furthermore, we propose the method to detect this attack called behavior of collaborative attack. In our proposal, we focus on the number of source IP addresses which transmit packets to the single destination. We detected this packet and the rate of packet with the same packet size and destination port number occupied about 90% of the set unit of extracted packet.

Keywords: darknet, collaborative behavior, botnet, 3D-visualization, cybersecurity.

1 Introduction

Threats which use the Internet include some examples such as personal and confidential information disclosure, leading to malware distribution site, infection by malware download. It is related to an institutional platform of an attack. These threats utilize a collaborative attack basement called a botnet.

1.1 Motivation

We have a problem in terms of an attack generated by a botnet which consists of a network of compromised computers. An attacker known as a botmaster infects

* This work was partially supported by Proactive Response Against Cyber-attacks Through International Collaborative Exchange (PRACTICE), Ministry of Internal Affairs and Communications, Japan.
Collaborative Behavior Visualization and Its Detection

many machines with virus. These infected machines, known as bots, receive the command for an attack from the botmaster and invoke scanning attack and DDoS (Distributed Denial of Service) attack and sending spam mails and so on [1]. These command are passed typically through an agency server which is called C&C server using a command and control (C&C) channel. In short, the C&C server is utilized to control the botnet for the botmaster. The botnet is usually located in a remote area. A number of security companies have pointed out the problem related to the number of bots and the scale of botnet [2] [3]. Therefore, it is important to detect the botnet to prevent expansion of the further damage.

On one hand, tendency of the attack is changing with the improvement and complication of the malware [4]. In concrete terms, the attacker attempts to hide from a network observer by decreasing the number of packets which the single source IP address (s-IP) transmits such as slow scan [5] and low-rate DDoS attack [6]. Slow scan evades detection by increasing the time between probes from more than one s-IP [5]. Low-rate DDoS attack is an intelligent attack as the attacker can send attack packets to the target server at a sufficiently low rate to elude detection [6]. An attack, which several s-IPs transmit packets collaboratively like scan and DDoS attack, is related to the behavior of botnet.

In this research, we propose a detection scheme to find collaborative behavior of which the many sources that send a packet to a specific target such as destination IP address (d-IP) or a destination port number in a short time. We apply our method to network traffic in order to reach darknet sensors. We think most of the traffic is related to malicious activities such as vulnerability scan by attackers.

1.2 Related Work

Kim et al. provide the change-point detection based on the characteristic of the packet, IP address and port number [7]. An attack shows an abnormal value by adding the weight to them and compares the attack with normal statement. Thus, we can detect it using this detection method. Their target is to detect the scan attack and TCP SYN Flood attack.

Treurniet also provides the detection scheme using the above characteristic and the session information based on an action of the communication protocols such as TCP and UDP [5]. He defines the state machine according to the session information such as TCP, UDP, and ICMP. He finds the last transition destination of the state machine on the session information for the traffic data. After that, he detects an attack and judges its type based on the number of s-IPs, d-IPs and port numbers. We can detect various attacks by using the characteristic of the session information. His target is to detect the scan, DoS, DDoS, and backscatter. Moreover, this detection method has succeeded in the detection of the slow scan attack with a long interval.

Eto et al. have developed the Network Incident analysis Center for Tactical Emergency Response also known as nicter [8]. They detect the threat of various security which occurs on the network using nicter and derive it’s effective