УДК 004.492.3

DEVELOPMENT AND TESTING OF AN ALGORITHM FOR DETECTING MALICIOUS TRAFFIC USING THE MIRAI BOTNET AS AN EXAMPLE

Нгуен Д.К. (Университет ИТМО)
Научный руководитель – к.т.н., доцент Комаров И.И.
(Университет ИТМО)

In this work, we present an algorithm for detecting Mirai botnet by analyzes the network traffic comprehensively. The algorithm is based on 3 characteristics of Mirai botnet: port scanning, heartbeat communication between bots and C&C server, and DDOS attacks. This work focusses on improving the accuracy of detecting Mirai botnet.

Введение. The widespread adoption of Internet of Things has led to many security issues. Recently, there have been malware attacks on IoT devices, the most prominent one being that of Mirai. IoT devices such as IP cameras, DVRs and routers were compromised by the Mirai malware. With 100,000 Bots, Mirai DDOS attacks on service provider Dyn in October 2016 triggered the inaccessibility to hundreds of websites in Europe and North America. Recent studies to detect the Mirai botnet are not comprehensive but rely on just one characteristic of Mirai botnet: port scanning. Relying on only one factor to detect this type of botnet can lead to inaccurate results. In this work, we take a closer look at the structure of the botnet mirai, how it works and how it spreads infection. Besides, we propose an algorithm for detecting Mirai botnet by its network traffic. The developed algorithm will analyze captured traffic packets and will output all the bots according to port scanning activities, communication between bots and C&C server, and DDOS attacks.

Основная часть. Mirai is a malware that infects IoT devices that run on ARC processor, turning them into a network of remotely controlled bots. These bots will continuously scan TCP to port 23/2323 of IoT devices running on ARC processors on the Internet. If the default username-and-password combo is not changed, Mirai is able to log into the device and infect it with 62 possible factory default user-id and password combinations. Currently, Mirai is one of the most dangerous botnets and it has been used in some of the largest and most disruptive DDoS attacks. To build our Mirai system, we have used 1 ubuntu server machine for the server: port 23 for C&C server, port 48101 for report server, port 3306 for mysql server and port 80 for Wget & TFTP server; 3 ubuntu server machines as Mirai bots; 2 normal Ubuntu machines as Iot devices, 1 ubuntu server machine to run a website as the victim and 1 windows machine for attacker to connect to the server and to publish the commands. The developed algorithm is based on 3 characteristics of Mirai botnet: Port scanning, heartbeat communication between bots and C&C server (or so called command and control server), and DDOS attacks. We will use WireShark to capture the traffic. From here we can filter out the IoT traffic by the window size because IoT devices have small buffer size for TCP stack and therefore commonly has a smaller TCP window size. After handling network traffic with 3 characteristics, we will receive 3 blacklists. From these lists, we can conclude which IoT device is belong to Mirai botnet. To analyze the captured network traffics, we use the following criteria:

- Criteria for port scanning is TCP protocol and the destination port is 23/2323.
- Criteria for heartbeat communication is that every 60 seconds a heartbeat is sent from the bot to the C&C server. This heartbeat is based on TCP protocol and the destination port is 23.
- And to handle DDOS traffic, we will separate the traffic by protocol and flag (like TCP, UDP, HTTP or SYN, ACK, GET and so on) and analyze both incoming and outgoing traffic. Because IoT device connects to limited endpoints (mostly vendor cloud servers), so if the destination IP address is not the IP of cloud servers and the number of packets from 1 source IP address to 1 destination IP address in 1 second is greater than 5, then we can conclude that there was a DDOS attack and the type of attack is based on the protocol and the flag.

Выводы. In this work, we built a Mirai botnet system and created a dataset by capturing Mirai's traffic, developed a comprehensive algorithm for detecting this botnet and testing it with the dataset. Based on some tests with Mirai's dataset and some DDOS traffic samples from kb.mazebolt.com, the algorithm has worked well.

Нгуен Д.К. (автор) Подпись

Комаров И.И. (научный руководитель) Подпись