Botnet Defense System: Concept and Basic Strategy

Shingo Yamaguchi
Graduate School of Sciences and Technology for Innovation,
Yamaguchi University
2-16-1 Tokiwadai, Ube 755-8611, Japan
Email: shingo@yamaguchi-u.ac.jp

Abstract—This paper proposes a new kind of cybersecurity systems, named Botnet Defense System (BDS), which defends a network system against malicious botnets. The unique feature is that a BDS uses white-hat botnets to fight malicious botnets. The BDS monitors a network system. If detecting malicious botnets, it launches white-hat worms and constructs white-hat botnets in order to destroy the malicious botnets. A basic strategy is also proposed. The primary factor is the secondary infectivity of the white-hat worms. If it is high, the BDS only has to launch a few white-hat worms. Otherwise, it should launch as many white-hat worms as possible. The validity of the strategy was confirmed through simulation with agent-oriented Petri nets.

Keywords—Botnet, IoT, malware, Mirai, worm, Petri net

I. INTRODUCTION

In September 2016, Twitter, Amazon, and other major sites were knocked out by massive DDoS attacks [1]. Those attacks were brought about by a new kind of botnets called Mirai. The feature of Mirai is that its target is consumer IoT devices. IoT devices are characterized by the large volume, pervasiveness, and high vulnerability. Thus Mirai’s DDoS attacks tend to become massive and disruptive [2].

Some ways have been proposed to mitigate Mirai’s threat. In particular, a prospective way is to use a special worm called Hajime [3]. Hajime blocks ports that Mirai uses to infect IoT devices. It prevents Mirai from spreading. Yamaguchi proposed to extend Hajime to become white-hat by introducing lifespan [4] and secondary infectivity [5] (the ability to infect devices infected by Mirai). However, there is no discussion about how to dynamically put Hajime in response to Mirai’s infection situation. Molesky et al. [6] discussed some of the challenges to use white-hat worms from the viewpoints of individual, business and government. They proposed a perspective for utilizing worms through balancing them. However, they provided no more than qualitative concepts and have not evaluated them quantitatively.

In this paper, we propose a novel cybersecurity system, named Botnet Defense System (BDS), which uses white-hat botnets to defend an IoT system against malicious botnets. The concept of BDS is illustrated in Fig. 1. A BDS monitors an IoT network. If detecting malicious botnets, it analyzes the situation and plans a strategy to fight the malicious botnets. Based on the strategy, it launches white-hat worms and controls white-hat botnets in order to destroy the malicious botnets. In addition, we propose a basic strategy for launching white-hat worms. Then we evaluate the validity of the strategy through simulation with a kind of agent-oriented Petri nets called Petri nets in a Petri net (PN²) [7], [8].

II. WHITE-HAT WORMS

Hajime is a worm which has a similar capacity with Mirai except for DDoS capabilities. Once it infects an IoT device, it blocks ports which Mirai uses to infect the device. As a result, it protects the device against Mirai. However, Hajime can add new capabilities on the fly, so it is said to be gray-hat.

Yamaguchi [5] proposed to extend Hajime to become white-hat by introducing lifespan and secondary infectivity. The extended Hajime destructs itself when exhausting a designated lifespan. The secondary infectivity enables the extended Hajime to infect a device even if the device has already been infected by Mirai. He regarded a battle between Mirai and the extended Hajime as a multi-agent system and expressed it as a PN² model. The PN² model is executable. Figure 2 shows a state-transition of a PN² model. Figure 2 (a) shows an initial state. Each place (●) represents a node and has one device. Device device1 at place P1 is infected by Mirai. Device device2 at place P2 is normal. Device device3 at place P3 is infected by the extended Hajime. Each transition (○) represents action. Red transitions mean being executable. In , Mirai and Hajime are aiming to infect device2. Figure 2 (b) shows the state immediately after transition fired. Mirai produced a copy at P2 and the copy infected device2. Mirai cannot infect device3 because it is already infected by Hajime. In contrast, the extended Hajime has secondary infectivity, thus it can infect device2. Figure 2 (c) shows the state immediately after transition fired. The extended Hajime removed Hajime from P2 and infected device2 instead.

The effect of the extended Hajime through simulation with PN² has been confirmed. The extended Hajime reduced Mirai and most of them successfully destructed themselves. For the detail of its modeling and evaluation, refer to Refs. [5], [9].
III. BOTNET DEFENSE SYSTEM (BDS)

The number of IoT devices is growing explosively. For malicious botnets’ threat, there is a limit to vulnerability management depending on human-wave tactics. It is an urgent issue to improve defense ability dramatically. To solve this issue, we propose to use white-hat botnets to defend an IoT system against malicious botnets.

A. Concept

We first propose the concept of BDS. BDS is a cybersecurity system that defends a network system against malicious botnets. The unique feature is that a BDS uses white-hat botnets to fight malicious botnets. Figure 1 illustrates the concept of BDS. A BDS equips several different types of white-hat worms. The operation of BDS is as follows:

1. The BDS monitors a network system.
2. If detecting a malicious botnet, the BDS analyzes its situation and plans a strategy for fighting the malicious botnet with a white-hat botnet.
3. Based on the strategy, the BDS launches white-hat worms to construct the white-hat botnet.
4. The BDS commands and controls the constructed white-hat botnet to destroy the malicious botnet.

B. Basic Strategy

a) Observation: We observed the effect of white-hat worms against malicious botnets through simulation with PN². The white-hat worm is the extended Hajime with lifespan and secondary infectivity. In this simulation, we took a trivial strategy, i.e. We launch as many white-hat bots as possible. For example, let us consider an IoT network shown in Fig. 3. This network consists of 25 nodes, in which six nodes have been infected by Mirai. In this case, we put the white-hat worms on the other 19 nodes as shown in Fig. 4.
Fig. 3. An infection situation. 6 nodes of 25 have been infected by Mirai.

Fig. 4. A trivial strategy. Hajime was launched on all the nodes except Mirai bot’s nodes.

![Table I. Effect of White-Hat Worms. Each value shows the malicious bot node’s rate after 1,000 steps. The grayed cell means the value is getting worse.](image)

<table>
<thead>
<tr>
<th>Initial malicious bot node’s rate</th>
<th>White-hat worms’ secondary infectivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>72%</td>
<td>0%</td>
</tr>
<tr>
<td>48%</td>
<td>93%</td>
</tr>
<tr>
<td>24%</td>
<td>93%</td>
</tr>
</tbody>
</table>

We measured

Malicious bot node’s rate [%] = \[
\frac{\text{Number of bot nodes}}{\text{Total number of nodes}}\]

more, we investigated how much the initial number of white-hat worms affects the malicious bot node’s rate after 1,000 steps. We assumed the initial malicious bot node’s rate to be 24%. This means that the initial number of malicious bot nodes is 6 of 25. We measured the malicious bot node’s rate after 1,000 steps by varying the initial number of white-hat worms in 1, 3, 5, 11, 19 (full); and the possibility of secondary infection in 50, 75, 100%. The other parameters were set to the same as the previous simulation. Figure 5 shows the result. The horizontal axis shows the initial number of white-hat worms. The vertical axis shows the malicious bot node’s rate after 1,000 steps. When the possibility of secondary infection is 50%, the malicious bot node’s rate after 1,000 steps reduced gradually with the increase in the initial number of white-hat worms. This means that we should use as many white-hat bots as possible. On the other hand, when the possibility of secondary infection is 75% or more, the malicious bot node’s rate after 1,000 steps almost touched the bottom at 5 white-hat worms. This means that we only have to use 5 white-hat worms.
b) Proposal: Based on the above observation, we propose a basic strategy for BDS. The primary factor is the secondary infectivity of the white-hat bots.

Strategy 1 (Elitism Strategy): For an available white-hat worm, if its possibility of secondary infection is high, the BDS only has to launch a few white-hat bots. Otherwise, it should launch as many white-hat bots as possible.

For example, in the case of Fig. 3, the basic strategy indicates that we only have to launch the white-hat worm with high secondary infectivity to five nodes shown in Fig. 6.

IV. Evaluation

A BDS launches white-hat worms based on a given strategy. We evaluated the validity of the basic strategy proposed in the previous section. We measured the malicious bot node’s rate after 1,000 steps in the same way as the previous simulation. Figure 7 shows a screenshot of our simulation tool PN2Simulator during this simulation. Table II shows the result. The term “full” denotes the maximum number of white-hat

<table>
<thead>
<tr>
<th>Possibility of secondary infection</th>
<th>Initial malicious bot node’s rate</th>
<th>Number of white-hat worms</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a) 50%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>72%</td>
<td>31.1%</td>
<td>31.8%</td>
</tr>
<tr>
<td>48%</td>
<td>27.0%</td>
<td>32.8%</td>
</tr>
<tr>
<td>24%</td>
<td>18.2%</td>
<td>29.0%</td>
</tr>
<tr>
<td>(b) 75%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>72%</td>
<td>13.5%</td>
<td>11.5%</td>
</tr>
<tr>
<td>48%</td>
<td>12.5%</td>
<td>13.8%</td>
</tr>
<tr>
<td>24%</td>
<td>8.8%</td>
<td>10.8%</td>
</tr>
<tr>
<td>(c) 100%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>72%</td>
<td>1.1%</td>
<td>1.2%</td>
</tr>
<tr>
<td>48%</td>
<td>0.7%</td>
<td>1.8%</td>
</tr>
<tr>
<td>24%</td>
<td>0.4%</td>
<td>1.5%</td>
</tr>
</tbody>
</table>
worms to be put to non-bot nodes. Each value shows the mean for 1,000 trials. The highlighted cell shows the value obtained according to the strategy. When the possibility of secondary infection is 50%, the result of 5 worms differed from that of a full number. On the other hand, when the possibility of secondary infection is 75 or 100%, the result of 5 worms is almost the same as that of a full number. Thus we can say that our strategy is valid.

V. Conclusion

In this paper, we first proposed the concept of Botnet Defense System (BDS). A BDS monitors an IoT network. If detecting malicious botnets, it analyzes the situation and plans a strategy to fight the malicious botnets. Based on the strategy, it launches white-hat worms and controls white-hat botnets in order to destroy the malicious botnets. Next, we gave a basic strategy as Elitism Strategy. The primary factor is the secondary infectivity of the white-hat bots. For an available white-hat worm, if its possibility of secondary infection is high, the BDS only has to launch a few white-hat bots. Otherwise, it should launch as many white-hat bots as possible. Then we confirmed the validity of the proposed strategy through simulation with PN2.

In future work, we are going to propose a strategy for the command and control of the constructed white-hat botnets.

Acknowledgment

This work was supported by JSPS KAKENHI Grant Number JP19K11965.

References