Chapter 16
Malware Threat in Internet of Things and Its Mitigation Analysis

Shingo Yamaguchi
Yamaguchi University, Japan

Brij Gupta
National Institute of Technology Kurukshetra, India

ABSTRACT

This chapter introduces malware's threat in the internet of things (IoT) and then analyzes the mitigation methods against the threat. In September 2016, Brian Krebs' web site "Krebs on Security" came under a massive distributed denial of service (DDoS) attack. It reached twice the size of the largest attack in history. This attack was caused by a new type of malware called Mirai. Mirai primarily targets IoT devices such as security cameras and wireless routers. IoT devices have some properties which make them malware attack's targets such as large volume, pervasiveness, and high vulnerability. As a result, a DDoS attack launched by infected IoT devices tends to become massive and disruptive. Thus, the threat of Mirai is an extremely important issue. Mirai has been attracting a great deal of attention since its birth. This resulted in a lot of information related to IoT malware. Most of them came from not academia but industry represented by antivirus software makers. This chapter summarizes such information.

INTRODUCTION

In September 2016, Brian Krebs' web site "Krebs on Security" came under a massive DDoS attack (Krebs, 2016). This attack was caused by a new type of malware called Mirai. Mirai primarily targets IoT devices such as security cameras and wireless routers. This is because IoT devices feature large volume, pervasiveness, and high vulnerability (Kolias, Kambourakis, Stavrou, &Voas, 2017). As a result, a DDoS attack raised from infected IoT devices tends to become massive and disruptive. Thus, the threat of Mirai is an extremely important issue.

DOI: 10.4018/978-1-5225-9742-1.ch016

This chapter introduces malware's threat in IoT and then analyzes the mitigation methods against the threat. It consists of two parts. In the former part, we describe Mirai's threat, attack, mechanism, and mitigation methods. In the beginning, we trace the history from Mirai's birth. Next, we illustrate the mechanism of Mirai's infection and attack. Against the threat, there are some mitigation methods such as rebooting infected devices and using an IoT worm called as Hajime which blocks Mirai. In the latter part, we present a mathematical model of the infection phenomenon of Mirai. We regard the infection phenomenon as a multi-agent system and express it with agent-oriented Petri net called as Petri nets in a Petri net (PN^2 for short). Intuitively, a PN^2 is a Petri net in which each token is a Petri net again. PN^2 is not only as a graphical and mathematical modeling tool but also useful as a simulation tool. We reflect the mitigation methods into the PN^2 model and evaluate the methods of the model. We illustrate the dynamic behavior of the mitigation methods with the simulation of the model. We finally conclude this chapter by summarizing our key points and give future research directions.

MALWARE IN INTERNET OF THINGS: MIRAI

Threat and Attack

Mirai (means "future" in Japanese) is a malware which changes IoT devices into malicious bots and creates the network of bots called botnet. The botnets can be used to perform large-scale network attacks typified by DDoS attacks. We shall trace Mirai's history to show its threat and attack.

- **Discovery (August 31, 2016):** A malware research group MalwareMustDie reported the discovery of Mirai. See [MalwareMustDie. (2016)].
- **Early Major Attacks (September 2016):** The first attack came on September 18, 2016. It targeted a French cloud hosting company OVH [Bonderud, D. (2016)]. At about the same time as the first attack, another attack fell on Brian Krebs' website "Krebs on Security" [Krebs, B. (2016)]. It reached 620 Gbps that means twice the size of the largest attack in history. In addition, a United States Domain Name System provider Dyn was exposed to attacks on October 21, 2016 [York, K. (2016)]. Major internet services such as Amazon and Twitter were made unavailable. These massive and disruptive attacks and threats made Mirai well-known.
- **Source Code Released (September 30, 2016):** The author of Mirai "Anna-senpai" posted the source code of Mirai on Hack Forums as open source [Statt, N. (2016)]. Later, it was removed by the administrator of Hack Forums. For the academic purpose, it has also been archived to Github: https://github.com/jgamblin/Mirai-Source-Code.
- **Variant (December 2017):** The released source code enabled anyone not only to implement Mirai but also to evolve Mirai into new variants. In December 2017 researchers discovered a variant of Mirai called "Satori" [360 netlab. (2017)]. Satori has higher infectivity than Mirai by using vulnerabilities in IoT devices. In the following month, a variant of Satori called "Okiru" was found. Okiru becomes able to target more architectures like ARC [Arzamendi, P., Bing, M. & Soluk, K. (2018)]. Following Satori and Okiru, more than ten variants of Mirai have been discovered. That number of variants will continue to increase.