Expos - IoTPOT: Analyzing the Rise of IoT Compromises

Name Surname
Matr.: XXXX XXX XXXXX
eMail: XXXXXX.XXXXXX@ruhr-uni-bochum.de

Based on the Paper **IoTPOT: Analyzing the Rise of IoT Compromises** *I will analyze how attacks that target IoT devices generally work. By using a honeypot and sandbox the authors managed to capture and analyze some Telnet-based attacks against various IoT devices running on different CPU architectures. Based on the observation, that the authors of the paper made, I will analyze and explain the basic attack pattern against IoT devices.*
In the end I will try to give some solutions and countermeasures for users and manufacturer on how to detect and prevent attacks to motivate further reading and research.

1 Introduction

Since years, Internet of Things (IoT) devices are getting more and more embedded in everyday life. Almost daily there are new *Smart-Devices* such as: connected fridges, smart toasters, routers, connected weather stations, etc. and most of them are connected to the internet. Smart-Devices bring forth some more or less useful features, such as monitoring the energy consumption of your fridge while the door is open, displaying the weather forecast on your toaster or none recognizable function such as to be connected to the internet to receive updates for your coffee machine.

But it is known that many of these IoT devices are vulnerable to simple intrusion attempts, for example, using weak or even default passwords. Once compromised, these IoT devices become part of an botnet, online DDoS service or some other hazardous service.

IoT devices are an attractive playground, compared to PCs, since they are 24/7 online, have no antivirus installed and can be compromised with an relatively easy attack pattern, giving attackers easy access to powerful shells (such as Busy-Box). Seeing these trends, I believe that IoT devices are an important new area of security research.

In this paper, I will investigate how the authors managed to trick real attackers in to trying to attack their honeypot and there analyze their attacks. To do so, I will explain how their honeypot is set up and what measures they took to be able to capture a variety of different attacks aiming against different CPU architectures and devices.

After explaining how they managed to capture the malware samples, my focus will be on how the actual intrusion and malware works. I will analyze and explain in detail how and why the attacker did certain steps during the attack by comparing attack patterns and results with each other.

It is sometimes hard to detect an attack and even harder to prevent them without some effort. It is up to the manufacturer to develop higher security standards and make it harder for attackers to misuse the IoT device, but also a matter of considering the actual need of such devices in everyday life. Motivated by this, I will try to give a short introduction to solutions for manufacturer and users on how to detect and prevent these attacks, trying to motivate further research and reading.

Following is the summary of my contributions:

1. I will give a brief introduction to IoT devices and their functions.

2. Going into detail on how an attack on IoT devices works in general.

3. Showing what devastating options an attacker has with a network of compromised IoT devices.

4. Finishing with giving a brief overview on how to detect and prevent attacks to motivate further reading and research.

2 Working method

During this paper I will work with several different sources such as books, other papers and online research. I plan on writing this paper in English and giving the presentation in German. My goal is to give an insight to IoT and their threats when compromised and motivate to further research and reading about IoT in general.