12-2022

THE OBSERVATION OF SMART CAMERA SECURITY

Shun-Hsin Wang

THE OBSERVATION OF SMART CAMERA SECURITY

A Project

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirements for the Degree

Master of Science

in

Information Systems and Technology:

Cyber Security

by

Shun-Hsin Wang

December 2022

THE OBSERVATION OF SMART CAMERA SECURITY

A Project

Presented to the

Faculty of

California State University,

San Bernardino

---

by

Shun-Hsin Wang

December 2022

Approved by:

Dr. William Butler, Committee Chair

Dr. Conrad Shayo, Committee Member, Department Chair, Information Systems and Decision Sciences

ABSTRACT

At present, as the Internet of Thing (IoT) is increasingly widely used in human life, how to protect IoT devices from Malware attack has become an inevitable problem. This project is an analysis of two malwares and how they impact the Internet of Thing (IoT), especially the smart cameras common in people's life and used in the enterprise. The analysis looks at the vulnerabilities of smart cameras and how Mirai malware and Persirai malware take advantage to these vulnerabilities to attack smart cameras within the network through the simulation process. Through the simulation, although both malwares were implemented using different methods, they all see smart cameras as bots that lead to a similar impact. In this analysis, the simulation process was set up to find ways to prevent smart cameras from being infected by malware. The scanning part found the target, the report part saw how malware gained access to their target and the control part examined how malware controls infected smart cameras to launch an attack. This analysis also looks at Cyber Kill Chain framework to examine how it could be when applied to the smart cameras and malicious software attack. The Cyber Kill Chain framework was used to break down the cyberattacks and aided in providing ways to prevent both malwares at every step. The framework shows that the user plays a huge role in preventing smart cameras from malware attack. The more knowledge and awareness users have, the safer the environment for their smart cameras.

ACKNOWLEDGEMENTS

I would like to thank my parents and my friends for their support and encouragement through the process of this project.

Also, I would like to thank Professors William Butler and Conrad Shayo for guiding me to finish this project.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE:

INTRODUCTION

Project Motivation

At present, as networks have become an indivisible part of human beings' lives, the Internet of Things (IoT) has become a new noun, generalizing all the devices that install software or other techniques to send data, receive instructions, or both through the Internet. Benefiting from cheap computer chips and high-bandwidth telecommunications, there are ten billion devices that interact with the Internet. IoT is not only things people use every day, such as cars and smart furniture, but it is also used in industries such as the automotive industry and transportation. Among all the IoT devices, smart cameras are used the most in human life. Smart cameras can collect data via sensors and supply user demand based on this collected data. The collected data can be used to predict when the machine needs to be serviced or to improve the residence's efficiency and security.

With the increasing significance of IoT, the issues of security are unignorable. Josh (2022) said, "IoT is a network of connected smart devices supplying rich data, but it can also be a security nightmare" (p.1). We can always hear that there is no 100% safe way for security, and neither does IoT. As one cyber-attack, malware and ransomware, which are malicious software designed to gain access to control or damage devices, have become critical issues.

According to Lance Whitney (2021), the survey from NordPass shows that only 33% of users changed the default password on their devices (paras. 2). Without changing the default password can lead to serious problems, especially with smart appliances. The NCC group and Global Cyber Alliance (GCA) implemented an experiment to analyze how many attempts hackers try to hack into the environment they create with many smart appliances. It turns out over 12,000 cyber-attacks happened within one week.

With IoT technology getting mature, increasingly smart home appliances are in modern homes. The smart home is composed of several equipment with various functions. The same characteristic and the goal of the smart home is that they are all connected to IoT, and they are created to make human life more convenient, more comfortable, and simpler. Smart homes enable users to control remotely, all the devices could be accessed through the app or the factory program. However, the more connected the house is, the higher opportunity the hacker could interpose our life and cause the lost. People continuously suffer the attack from hackers to invade their smart home IoTs to gain the information then control their devices. The attack might not cause huge damage, but it still be a problem for users to be concerned about. So far, over 42% of Americans are using smart appliances but half of them have no methods to protect their devices (Douglas Broom, 2021).

This project will investigate the security of smart cameras by comparing two different kinds of malware. The word malware is the abbreviation of malicious

software. Malware is software that can be used by an attacker to damage their target devices. There are five types of malwares can compromise smart cameras' security which are Virus, Worms, Spyware, Ransomware and bots. In recent years, Mirai malware is the most widely known, developed by Paras Jha and Josiah White in 2016. At first, Mirai malware is created to attack their college but end up being replicated and changed by other cyber-criminal because of leaking the code to the Internet. Different than other malware, Mirai malware targets on the smart home devices such as smart camera and the home router to make these devices become remotely control bots so the hacker could launch the distributed denial of service (DDoS) on the Linux operation system which is the system the most IoT devices run.

Another malware that was discovered in 2017, this backdoor open source is called Persirai malware. Persirai malware was able to attack more than 1000 Internet Protocol (IP) cameras based on various Original Equipment Manufacturer (OEM). According to the latest research, Persirai has already replaced Mirai as the most common malware attack. Trend Micro has found that the amount of IP camera infected by Persirai is two times than Mirai. Like other malware, Persirai uses Universal Plug and Play (UPnP) protocol to infect IP camera and no matter how strong the password is, it can still inject the instruction to control the device.

Both malwares mentioned above are used to attack the smart camera which is used the most in smart homes. Thus, studying this attacking program is

important to improve smart camera security so the customer's living environment will not be in danger and people will not worry about their privacy being leaked. This project is tried to analyze these two malwares and supply the method based on the vulnerabilities of smart cameras.

Problem Statement

When we passed by the street, we could figure out that many families have installed smart cameras to check the activity in and around their houses. People are gradually installing smart cameras rather than traditional Wi-Fi cameras. However, the Porch study in 2019 shows that only 43% of the interviewees owned smart cameras because people are concerned about their security. People are not willing to sacrifice their privacy for installing devices that are not 100% secure. After the emergence of VPN services and more transparent privacy policies needed from technology companies, an increased number of families are beginning to implement smart cameras in their home (Jason Cohen, 2019, p.1). By 2021, the global smart home market size was USD 6.42 billion, and it is continuously rising. As more people are having smart cameras now, the awareness about smart camera security in both individuals and institutions is a lingering problem.

This project will attempt to answer the following questions:

- What vulnerabilities might the smart camera have?

- How Mirai malware and Persirai malware take advantage to these vulnerabilities and how can they be prevented?

Based on that awareness of existing problems about smart cameras and it is growing significantly in the market. This culminating experience project is organized as follows: Chapter 2 will describe a review of the literature to contextualize my research in the existing inquiry of smart camera security. Chapter 3 will provide methods to answer the project questions. Chapter 4 will provide the analysis data on the simulation process defined within Chapter 3 then figure out which are the ways to against Mirai and Persirai malware attack. Based on the result analysis, Chapter 5 is composed of a summary of the research and the limitations of this project. This project is not supplying the best method to against both Mirai malware and Persirai malware but putting an effort to figure out some ways to prevent smart cameras from infecting by both malwares in each step.

CHAPTER TWO:

REVIEW OF LITERATURE

What Is Smart Camera?

The word smart camera dates back to 1975, when Belbachir first published it. In 1976, a smart camera was defined as a camera that could process its pictures before recording them (HRL Laboratories,1976). Unlike traditional cameras which are mainly composed of an image sensor, and then process images to make the decision through an external PC that will take place too much, a smart camera is an individual image processing system that not only records and collects data but also extracts specific information from the application to make the ideal decisions that are used in the automated system by integrating image sensor and CPU functions to the camera which enables the smart camera to simple the vision system and process image without using external PC. Besides, the smart camera requires less space by supporting a localized pass/fail decision system, I/O part rejection and network management system. Figure 1 shows the general parts of a smart camera.

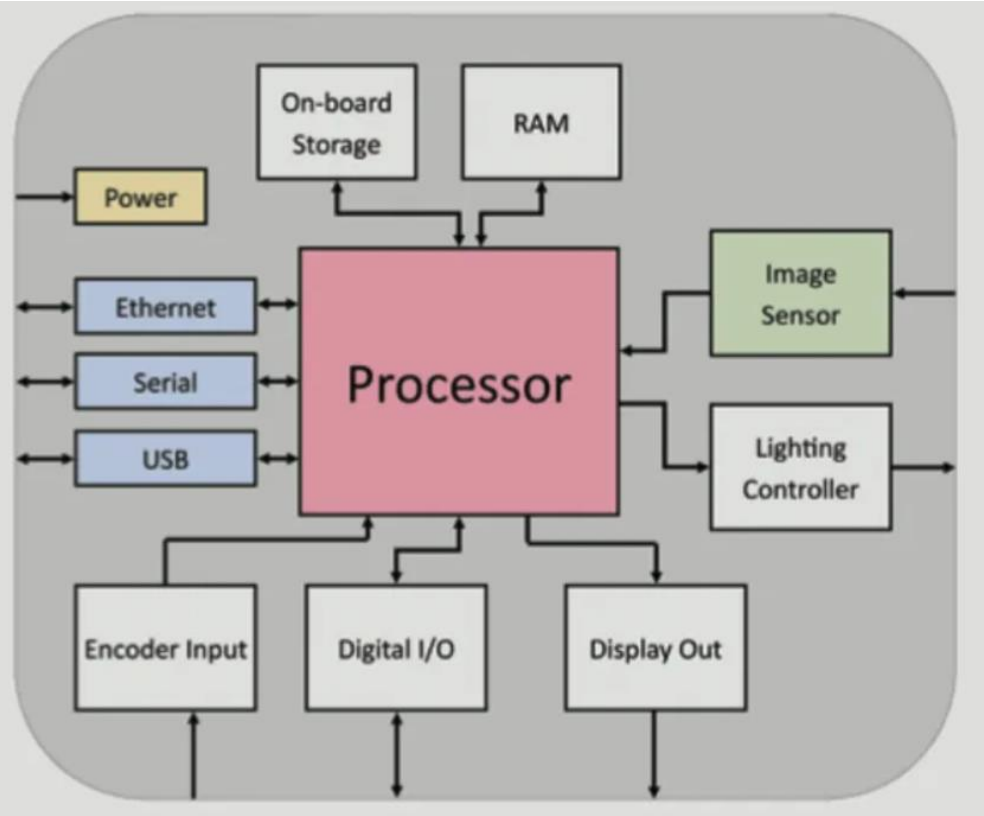


Figure 1. Parts in Smart Camera (Tech Briefs, 2014)

Attacks to the Smart Camera

Hackers usually take advantage of the weakest part of smart cameras which is called vulnerability to exposure and leads to severe damage such as the customer privacy might be explored through the internet. People may believe they are picking up a bargain wireless camera that can bring a sense of security, when in fact they could be unwittingly inviting hackers into their home or workplace (Kate Bevan, 2020). Since smart cameras are connecting to Wi-Fi to transfer and receive data, they are more likely to become a target, especially the

smart cameras do not support SSL/TLS encryption. Hackers are able to hack into the camera to access the video stream to monitor the victim's home, change the password or discover the victim's exact location. Below are some common attacks on smart cameras:

Man-In-The-Middle Attacks (MitM)

The MitM attack is when the attacker locates himself between the user and the application to pretend that the communication is normal. The goal of this attack is to obtain personal information so the attacker could achieve identification theft or change the password. According to a study in 2019, smart cameras store information such as MAC address and IP address to Address Resolution Protocol (ARP) table. The MitM attackers gain information by receiving the reply from ARP tables and then forwarding it to themselves. Figure 2 is an example of a MitM attack.

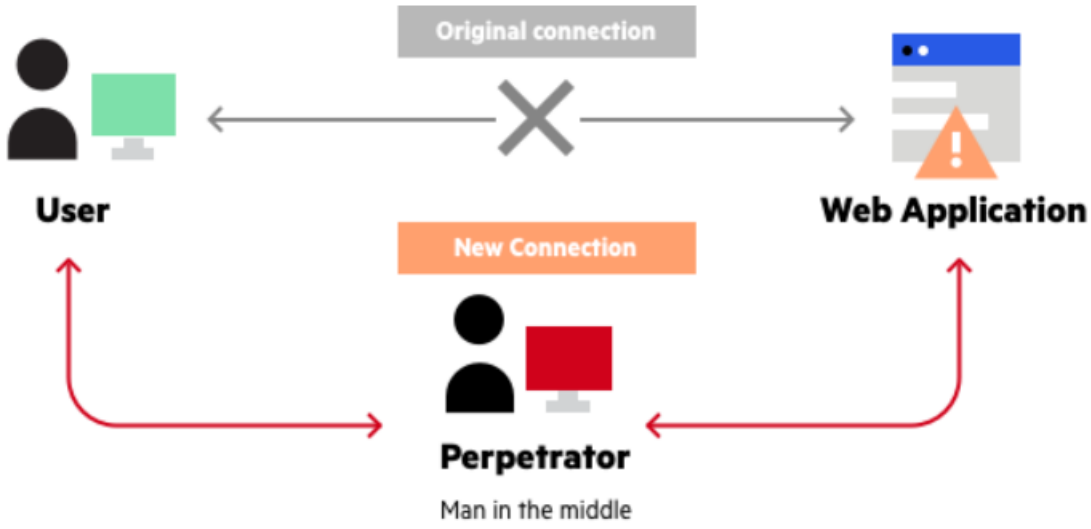


Figure 2. MitM Attack (Imperva, 2020)

Distributed Denial of Service (DDoS) Attack

Like other IoT devices, smart cameras rely on the Internet to operate. The high-speed and high-bandwidth connection required by smart cameras provide the best environment to launch a DDoS attack. The DDoS attack is to infect the devices through an HTTP flood attack and a SYN flood attack. The infected devices will turn into botnets and then send the request to the target server until the server overloads and denial the service. The attacker usually attacks smart camera by Brute-force password cracking as a breach to explore other devices connect to the same network to make these devices become the botnet.

Exploiting Password and Social Engineering

People usually use their birth date password or keep using a password such as “admin” when they install the smart cameras. Without a strong password, it will become the most vulnerable issue for smart cameras that

enable attackers to gain access then attack. Even if the user uses the system from a famous company, their password could be still leaked by a careless company employee who suffers from social engineering so the attacker can gain access to the database to get their username and then guess the password.

Mirai Malware Review

The Mirai malware, a self-propagating worm, was developed by Paras Jha and Josiah White, who are the founder of the DDoS mitigation service company, in 2016. At first, the Mirai malware was created to provide the DDoS protection for Minecraft servers. However, after the open-resource code was published on the website, the code was advanced by cyber-criminal. According to the report by OVH, the largest hosting vendor in Europe, the Mirai attacks have exceeded 1 TB which is the largest public record, and these attacks were carried out via small IoT devices such as smart cameras (Cloudflare, 2017). As previously mentioned, Mirai malware will infect the smart camera and other devices running on Linux to make them become the botnet to launch DDoS attack. The Mirai malware's structure and activity can be divided into 4 steps. The better understanding how Mirai malware's the greater against methods could be provide. The list of the 4 steps, figure 3, are Scan, Report, Enslaved and Control.

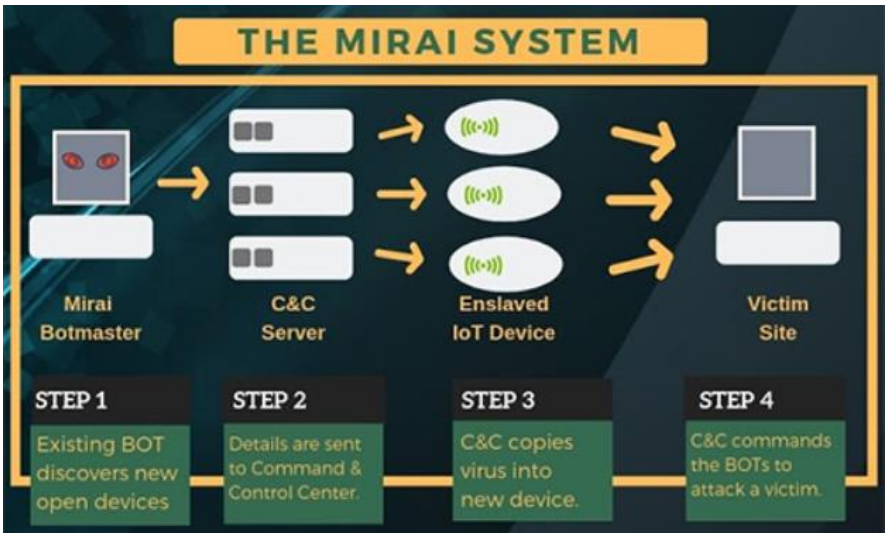


Figure 3. Mirai malware Attack Step (attify, 2019)

Step 1: Scan

The first step for Mirai malware is to continuously scan the publicly accessible devices without password protect or using the default password and the IP of IoT devices by sending TCP SYN probe to pseudo-random IPv4 addresses on telnet TCP ports 23 and 2323 through Internet. Once the Mirai malware discover the attackable device, it will conduct brute-force login by using the combination of several default password from 62 credentials list which include most of the default passwords by IoT vendors.

Step 2: Report

Once Mirai malware discovers the devices that is attackable, it will report the IP and related information of target devices to the command & control (C&C). When Mirai malware successfully infects the camera, it will camouflage itself by

using a pseudo-random alphanumeric string as the process name which turns out it will not exist when the system reboots.

Step 3: Enslaved

After Mirai malware infect the IoT devices, these cameras will become the bot. The Mirai malware will remove other malware that already exist in the infected devices to make sure it is safe and make sure that the bots stay in the botnet securely. All the activities are executed no matter if the user agrees or disagrees. These bots are waiting for any command from C&C and keep scanning for other vulnerable devices.

Step 4: Control

The infected cameras could be remotely controlled by C&C and keep searching for other vulnerable. The hacker could control these bots to launch DDoS attacks such as HTTP flooding, UDP flooding and TCP flooding to the target devices decided by C&C. Since most of the smart home devices still do not have comprehensive network security, it will be easy for Mirai malware to attack smart cameras and other smart home appliances.

Mirai malware is extremely dangerous as it launches the DDoS attack to cause lot of damage not only in smart home environment but also business. The botnet could be spread all over the world, always attacking without user knowing, which makes Mirai malware more difficult to defend. Figure 4 shows the geographic distribution of the infected devices by Mirai malware (Brian Krebs, 2017). Another thing that makes Mirai malware tricky is that programmers must

put a lot of endeavor into detecting a device to make sure whether it is infected or not, as common symptoms of an infected device such a slow network connection or lower performance of equipment might not appear.

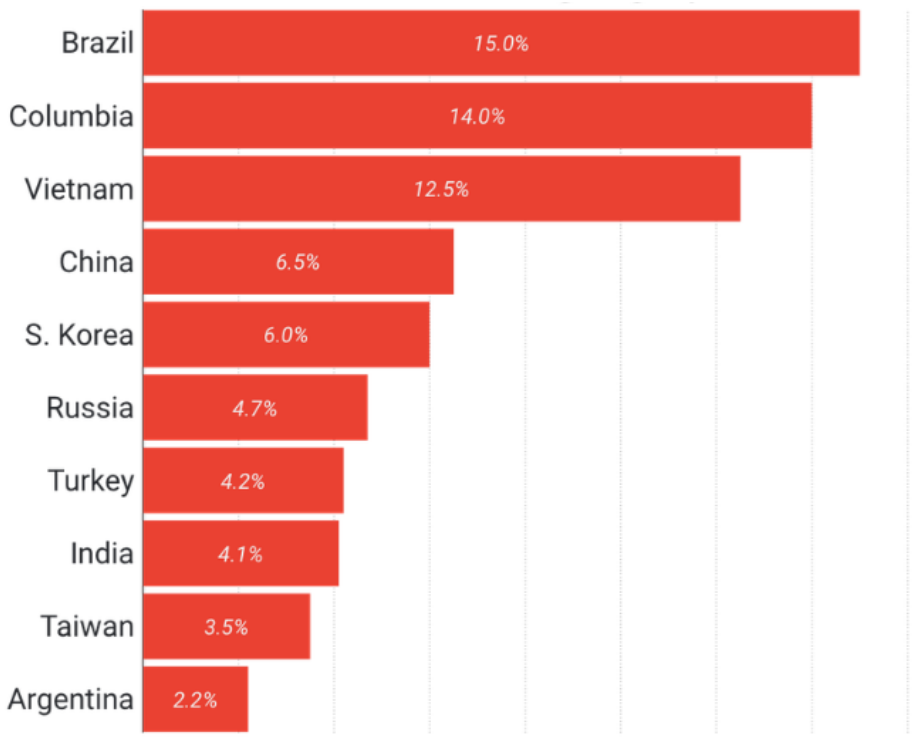


Figure 4. Geographic Distribution of Infected Devices (Cloudflare, 2017)

Persirai Malware Review

The Persirai Malware, an attack that targets Internet-based smart camera using UPnP protocol, was discovered by Trend Micro in 2017. Benefiting from the open-resource code of Mirai malware, hackers are able to change the code then launch the attack. Targeting over 1,000 Internet Protocol (IP) Camera models based on various Original Equipment Manufacturer (OEM) products (Tim

Yeh, 2017), the amount of smart camera infected by Persirai malware is two times more than Mirai malware and over 20% of the infected cameras are in China (Pierluigi Paganini, 2017). Table 1 shows the amounts of infected cameras in each country. Based on the vulnerabilities of the smart cameras, Persirai exploit them so the hackers could access the smart cameras by injecting commands and connecting them to the server remotely. There are three steps, as figure 5, for Persirai to infect the smart camera or other IoT devices. The steps are divided into Scan and Access, Inject and Install, and Control.

Table 1. Infected Smart Cameras in each Country (Trend Micro, 2017)

Country	Percentage
China	20.30%
Thailand	11.60%
United States	8.84%
Hong Kong	4.66%
Mexico	3.44%
United Kingdom	3.40%
Japan	3.33%
others	34.65%

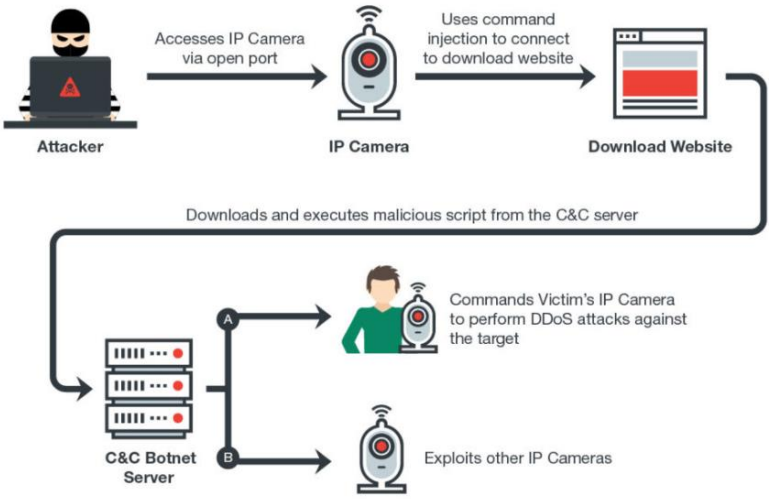


Figure 5. Progress of Persirai Infection (Trend Micro,2017)

Step 1: Scan and Access

The attackers scan for the vulnerabilities of smart cameras through TCP port 81. Once targeted the smart camera, Persirai would start to gain access to management Web interface by using UPnP protocol which is supported by most of the smart cameras and allow it to remotely control. UPnP protocol allows devices to open the port on the router so these devices will become the server, as a highly visible target for malware.

Step 2: Inject and Install

Once Persirai gain the access of the management Web interface, the attacker can inject the commands to force the smart cameras connect to the Iran download site for downloading and installing the malicious script which is called shell. After executing the script, Persirai will drop the installation file to hide it, so

the user will not even know their devices have already been infected. Also, Persirai protects the infected smart cameras from other malware. Although Persirai could be stopped by restarting the smart camera, smart cameras could still be easily infected again.

Step 3: Control

In this step, the infected smart camera will report to C&C server which is set at Iran. The C&C server uses these infected cameras as a bot and keeps scanning through the Internet to search for other vulnerable devices. The attacker used to exploit a zero-day vulnerability to gain the password from the user file through these controlled cameras. Also, attackers will start launching the UDP DDoS attack through SSDP packets which is the core protocol of UPnP.

A large number of these attacks were caused by using the default password in the device interface (Tim Yeh, Dove Chiu, and Kenney Lu, 2017). Since Persirai attacks start from scanning through the Internet to gain access to the vulnerable smart cameras, these default passwords which are public on Internet enable attackers to take advantage of it. The user should not only understand what smart devices are connecting to Wi-Fi and change the password to against Persirai but also stop using UPnP on their server if necessary so their Internet port would not open through UPnP by the devices in the interior network without their awareness. The manufacturer also shares the responsibility against Persirai by providing the latest version of these cameras or

IoT devices and always patch the vulnerabilities once they discover them as soon as possible.

Cyber Kill Chain (CKC) Review

The Cyber Kill Chain (CKC), which was created by Lockheed Martin in 2011, is a cybersecurity model to trace and describe each step of cyber-attack. The CKC also helps the operator to understand how attackers take advantage of the vulnerability of IoT devices. The military adopted the concept of “Kill Chain” to describe the actions used by an adversary to attack and destroy a target (Bianca Soare, 2022, p.1). Similarity to the concept of military, going through the seven steps of the CKC benefit the security team to set up the methods or precaution within each step so the security team can strengthen their incident response, cyber-defense capability and analysis capability to prevent the continuously cyber threat. In addition, reversing the attack gives the security team an opportunity to figure out and analyze new technology to launch the attack from adversary.

The CKC is composed of seven steps to analyze the cyber-attack and assist in preparing a defense. The steps of the CKC, figure 6, are Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control (C2), and action on Objectives.

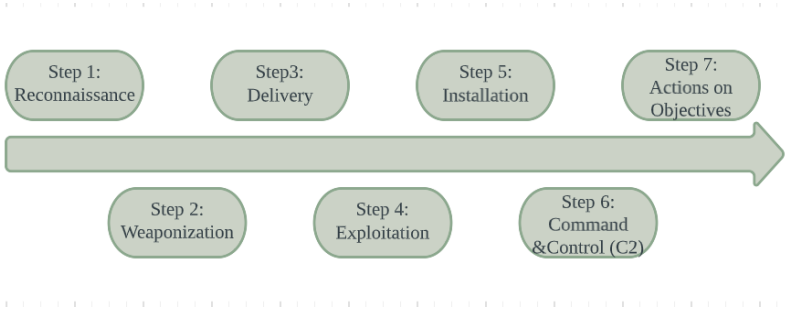


Figure 6. Cyber Kill Chain Steps

Step 1: Reconnaissance

Like traditional war, the first step all the attackers take for the attack is to search for the potential target and discover the vulnerabilities of the device they want to attack. The reconnaissance step also involves scanning the existing interface and new interface of target. During this step, attackers usually use several tools to collect information. Some kinds of tools might be:

- Port Scanner: Nmap, Angry IP scanner, TCP port scanner
- Packet Sniffer: Wireshark, SolarWinds deep packet inspection tool
- Cloud Service

Step 2: Weaponization

The weaponization happened after attackers gather enough information of target the generate one or several ways to launch an attack. The weaponization could be building new malicious software or modifying the existing malware. This step is still seen as preparation of attack. Once the malicious software is created, the several ways like Man-in-the-middle attacks, SQL injection attacks, social engineering or careless employees will be used to invade the target.

Step 3: Delivery

The delivery phase can be seen as the start of the attack. After gathering enough information and gaining access to the target from the previous two steps, the attacker will connect them to victim to deliver the malicious software. The most common way for attackers to deliver the malware is through sending phishing email or sending the link to victims and tempting them to click the link. Some attackers might conduct social engineering to increase the success rate of deliver their malicious software. The delivery phase could be the first chance for defenders to protect their assets by training how to identify the phishing email and how to deal with social engineering.

Step 4: Exploitation

In exploitation phase, the expected payload from attacker has already been delivered and the malicious code is working within the target system. During this step, attackers also take advantage of the vulnerabilities they gain from step 1. Sometimes the target is not attacked directly by the attacker, but through exploiting the vulnerabilities of the system or the device the attacker is able to arrive at their goal to launch the attack. The exploitation step is another opportunity for defenders to fight against the malicious software that is already operating within the system. Through proper training, the technical staff should have several ways to identify the existing malicious software and eliminate it.

Step 5: Installation

Once the hacker gain access to the target, they will start to install the malicious software or other application to the system to seek persistence. In installation step, attackers usually install the backdoor for consistence access so if there is any future information interested by attackers, the backdoor will enable them to gain access to the system and leak the information without going through again the previous steps. The defender can block installed backdoors by periodically detecting them in logs to check for unusual login time or unusual data movement.

Step 6: Command and Control (C2)

In C2 phase, hackers are able to communicate to the system through the malicious software they installed in step 5. Adversary can also control the device or system remotely to launch the attack. The adversary might do some work to maintain their control of the target system and keep scanning for the new interface. It will be too late for defenders to figure out the information is leaking within this phase because they have already lost control of the system or devices. However, the defender should cut off the communication between the adversary and the malicious software and eliminate it once discovered.

Step 7: Action on Objectives

This is the last step in CKC. The intruders already achieved their original goal. Within this step, various kinds of attack will be launched depending on adversary and what information they desire to leak. The classification of cyber-

attack might be Malware Attack, SQL Injection Attack, Man-in-the-middle attacks, Denial-of-Service Attack, and Cryptojacking.

The CKC is an analysis tool that can divide the attack into several parts and enable the defender to look at the detail in each step so the defender or the security team can have a greater understand to the attack then set up a proper mitigation plan to control the attack until eliminate it. Also, defender must remember that the time is the most essential thing to defect the malicious software while conducting CKC steps because the adversary will continue establishing the best way to infect the target until the defender identify it then eliminate it. By conducting CKC when the attack occurrs, the defender will figure out the mitigating control within each step and then know where the control should be implemented to break the chain.

CHAPTER THREE:

METHODOLOGY

Project Purpose

The purpose of this project to analyze Mirai malware and Persirai malware among all distinct kinds of malware is even though the creator of Mirai malware has already been caught and the Persirai creator is still unknown, attackers are still able to take advantage of both malware's open-source code to create their own variant malware to attack smart camera or other IoT devices. Defending against both Mirai and Persirai malware is a huge challenge because people never know when the attack will be launched, and the impact range can narrow down to a smart home environment and zoom to the large company. Both are targets of attackers. Although there are already some methods to protect against malwares, the point of this project is not to evaluate or examine the efficacy. The main purpose of this project is to go through the steps of how these two malwares infect smart cameras and try to provide methods against them then see which the best way is to defend.

Procedure

The process of knowing how Mirai malware and Persirai malware take advantage to vulnerabilities of smart cameras in smart home environment will be

done by going through the steps both malwares infect smart cameras. By following the malware's attack step-by-step, the goal is to analyze the steps of the attack and try to figure out the methods to against the attack in each step. Once figured out the method that can be used to patch vulnerabilities of smart cameras, it will be analyzed and resulted in data to see if it is available to prevent the malware attack.

The Malware

The two malwares will be analyzed separately. The four steps of the Mirai malware attack will be simulated then the three steps of Persirai malware attack will be imitated. This project will put efforts to run these two malwares by going through each step as making them look like the real-world attack.

The Environment: Wi-Fi

Since most of the smart cameras are operating wireless, wireless network security is becoming a critical issue in business and home. Smart cameras connect and communicate through Wi-Fi still have the risk. Although the wireless network has an internet access security system such as firewall to block people who desire to access without signing up, the attackers could still scan the network and take advantage of the leaking data by infecting the devices connect to Wi-Fi. To prevent the leaking data, Wired Equivalent Privacy (WEP) was created in 1997 by using 10 or 26 hexadecimal digits for its key recognize as a part of 802.11 standard. The only goal for WEP is to protect the data stolen from hackers. WEP used to be widely used and was the top choice for users.

However, WEP was not as effective as people expect when facing massive cyber-attacks, so people end up using Wi-Fi Access (WPA) to replace WEP. WPA solved the security defect WEP had and was encrypted using a pre-shared key and Temporal Key Integrity Protocol (TKIP). So far, people are using WPA2 as an upgraded version of WPA by using advanced encryption standard (AES) which the U.S government approves. It is expected to protect the family network by applying on most the devices and Wi-fi routers to encrypt the Wi-fi flow. However, the interface of WPA2 is still at considerable risk of attack which is also a problem from WPA. The lack of methods to prevent leaking data provides the ideal environment for hackers to scan through Wi-Fi for vulnerable devices.

The Simulation Process

By going through the simulation process of malware attack, we should figure out some vulnerabilities of smart cameras and then find some methods to prevent so we can answer the question posed in problem statement. The three steps are scan through the network, report, and control and launch attack.

Step 1: Scan Through the Network

This step will scan through the Network to look for the IP of the smart cameras and the vulnerable cameras connecting to the Internet through ports 23 and 81 to simulate how Mirai malware and Persirai malware really do in the real world. Once figure out the location of the cameras, this project will supply the lists

of the usually used default password for both malware to login to the smart camera and then go to the next step.

Step 2: Report

After gaining access to smart cameras, this step will supply some code or data to show how these malware uses infected cameras for reporting to C&C and what they will execute to download the script to the infected cameras. Also, this step tries to look at how both malwares prevent the infected cameras from other malware.

Step 3: Control and Launch Attack

In this step we will look at what command will be provided by C&C and provide the data of how the infected smart cameras launch DDoS attacks such as HTTP flooding, UDP flooding and TCP flooding. It should provide details of the data needed to figure out the ways to protect against malware.

CHAPTER FOUR:

DATA COLLECTION AND MALWARE ANALYSIS

This chapter will go through the simulation process. Also, the simulation process is just trying to simulate the attack as much as possible and see what can be found. No devices will be infected by DDoS attack and no damage will be caused through the process based on the legal and ethical considerations.

Mirai Malware Analysis

The Mirai malware simulation analysis is a three steps process based on the simulation step provide in chapter 3. The three steps of the simulation are scan the network, report, and control and launch the attack.

- Tools: Angry IP scanner, Nmap
- OS system: Microsoft Windows
- IP address: 192.168.4.104
- Scanning network range: 192.168.4.0/24

Step 1: Scan the Network

The first step hackers will take is to scan the network to see if there's any open port so they can look for the attackable smart camera or the devices which are not protected by strong password. Normally, Mirai malware scan through the

Internet but not only the specific Local Area Network (LAN). In this simulation, however, the scanning network range is narrowed down to 192.168.4.1~ 192.168.4.255 based on typing “ipconfig” in command prompt in Microsoft Windows. Showing by figure 7, the device which is used to scan the network is connecting to the Wireless LAN.

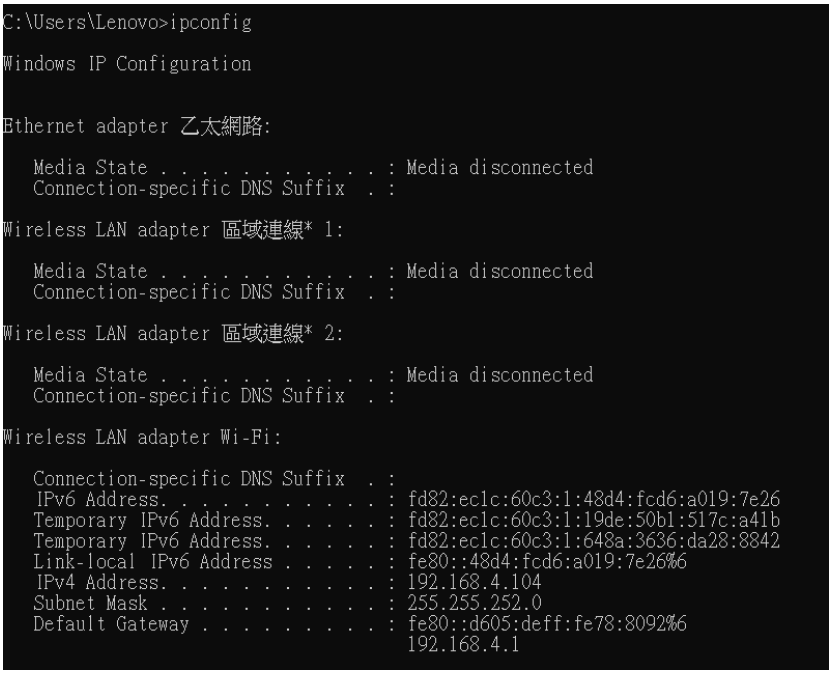


Figure 7. IPconfig Command

Nmap will be implemented in this step. Nmap is a free network security scanner used in this step for network discovery and scanning for the open port. After determining the range of network, type “nmap -open 192.168.4.0/24” in the command line to show all the open ports on this network. See figure 8.

Figure 8. Open Ports on Network

As Mirai malware do which is mentioned in chapter 2, the telnet TCP ports 23 and 2323 is scanned through Internet by typing “nmap -p23 192.168.4.0/24” and “nmap -p2323 192.168.4.0/24”. See figure 9 and figure 10. It shows the port state, the MAC address and the name of the devices connecting to the network. Table 2 shows the meaning of the state.

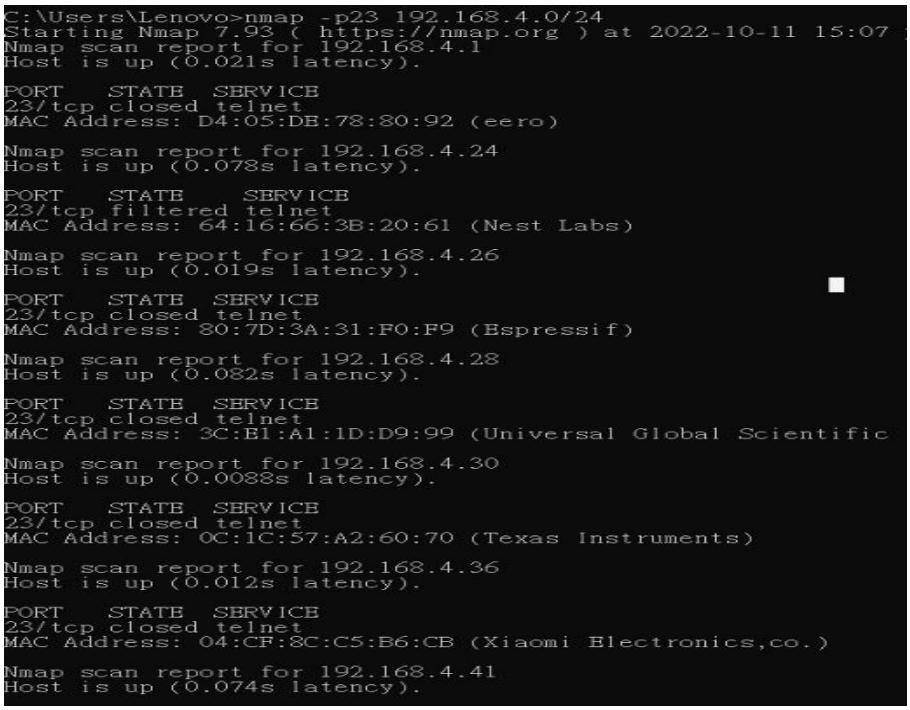


Figure 9. Port 23

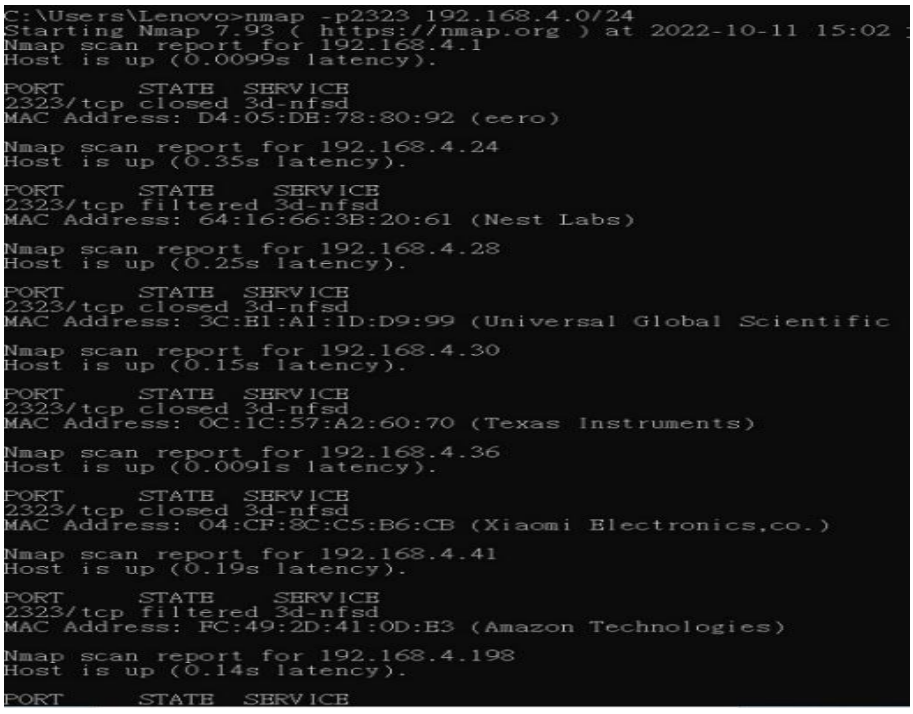


Figure 10. Port 2323

Table 2. State of the Ports

State	Description
Open	The port responds to TCP/UDP requests
Closed	There is no listening service for connection
Filtered	Nmap cannot detect whether the port is open or closed due to the firewall blocking the port.

Another network scanner is Angry IP scanner. Like Nmap, after typing IP range then click “start”, Angry IP scanner shows the IP address, ping, host name and port in the define range. See figure 11.

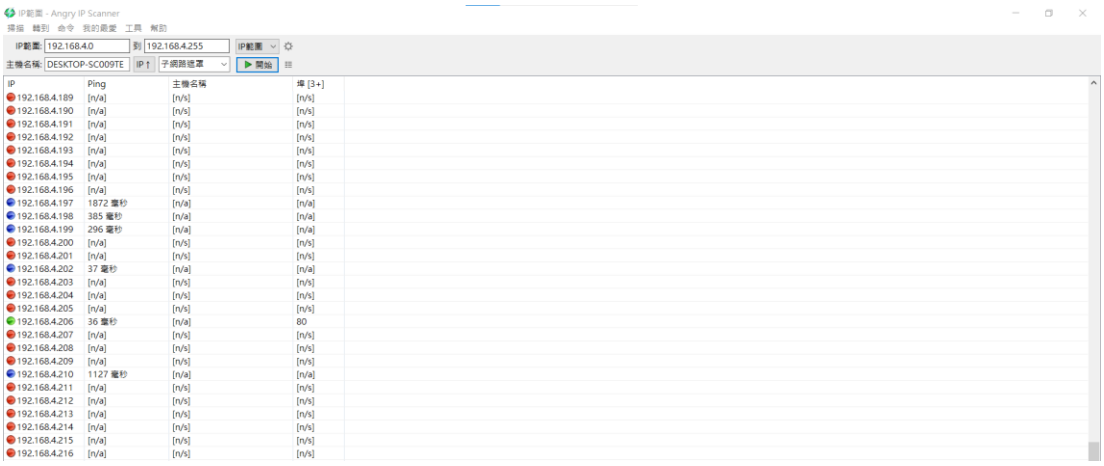


Figure 11. Angry IP Scanner

Once Mirai malware discovers the attackable smart camera or other devices by scanning the network, it will start attempting to gain the access. According to the Imperva Incapsula security team, Mirai malware executes brute-force login to guess the password of discovered smart cameras (Ben, Igal, Dima, 2016). Table 3 is the combination of username and password the attacker might use to conduct brute force login. After gaining access to smart cameras, the infected smart camera will go to the next step.

Table 3. List of Password Combination

Username	Password
Root	Admin
Root	Default
Root	12345678
User	Admin1234
admin	Password
admin	88888888

Step 2: Report

After successfully access to smart cameras, Mirai malware send the detail of smart cameras to C&C so the attacker can select the victim IP address and the attack time. C&C is a control center of infected smart cameras which controls the devices to launch DDoS attack and keep receiving the details from the new

infected devices. Mirai malware will delete the existed services running on the infected smart cameras and install the script so the infected cameras will not be infected again by other malware such as worms and Trojans. Figure 12 shows a part of open-source code from Sourcegraph to kill the process running on the port 23.

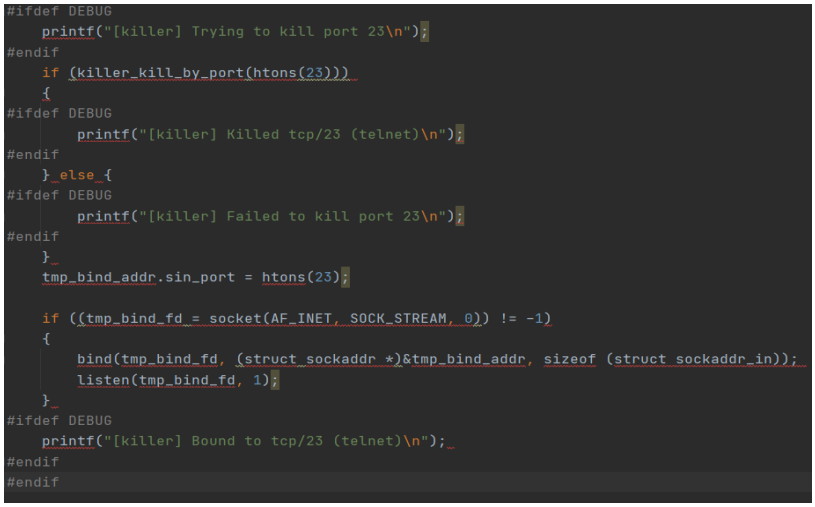


Figure 12. Kill Process Code (Sourcegraph, 2016)

Step 3: Control and Launch Attack

In this step, the infected smart cameras are called bots. These bots are waiting for the commands from C&C to launch the DDoS attack such as HTTP flooding, TCP/UDP flooding and other attacks on OSI application layer. These botnets are not just waiting for commands to launch but keeping scanning the Network as step 1 do then go step 2 to keep looping until Mirai malware is eliminated from smart cameras.

Step 1: Scan the Network

Same as the simulation process Mirai malware went, Persirai malware scan through the Internet and scan for the vulnerable smart cameras through TCP port 81. In this step, the scanning network range is still limited at 192.168.4.1~ 192.168.4.255, see figure 6 Ipconfig Command. Since hackers usually use Persirai malware to attack smart cameras and other IoT devices by UPnP which uses UDP 1900 and all used TCP, we scan the open port, please see figure 8 above, TCP port 81 and UDP 1900 by using the command from Nmap.

The telnet TCP ports 81 and UDP 1900 are scanned through the Internet by typing “nmap -p81 192.168.4.0/24” and “nmap -p U:1900 192.168.4.0/24”. See figure 13 and figure 14. The UDP 1900 scanning, see figure 13, shows the MAC address and the name of the devices connecting to the network as TCP port scanning, the only difference is that it does not show the port state. However, in UDP scanning, the port will be seen as open if the device responds to the request.

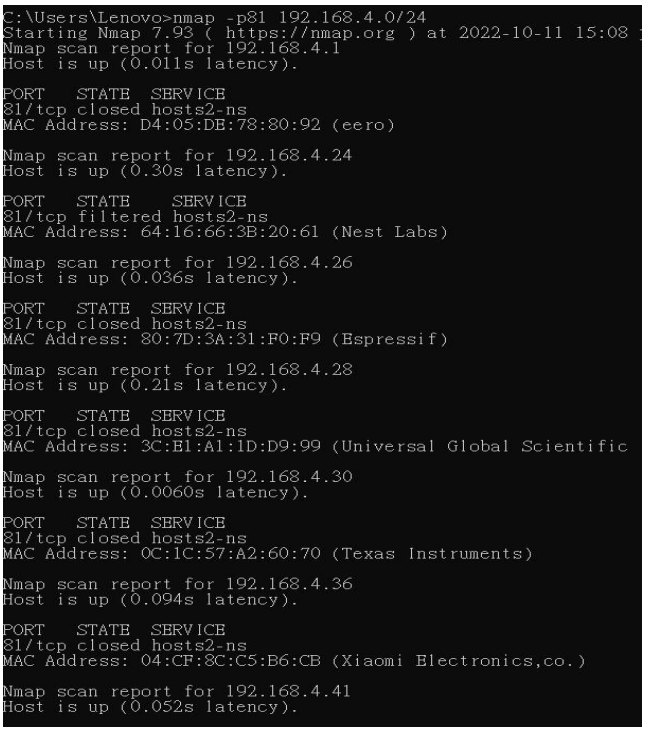


Figure 13. Port 81

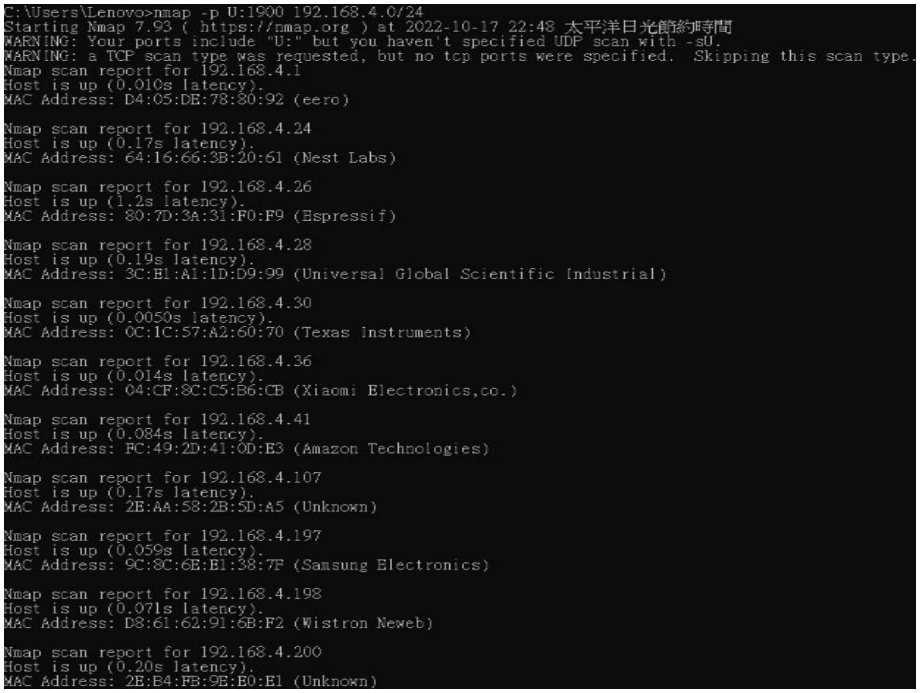


Figure 14. UDP 1900

After scanning for vulnerable smart cameras, Persirai would start gaining access to management Web interface. To gain access to management Web interface, the first need is to get the router's IP address. The IP address can be known by typing ipconfig in command line as figure 6 shows. Once access the management Web interface, see figure 15, the attacker will start applying the password combination, like table 3, to login the web management then go to next step.

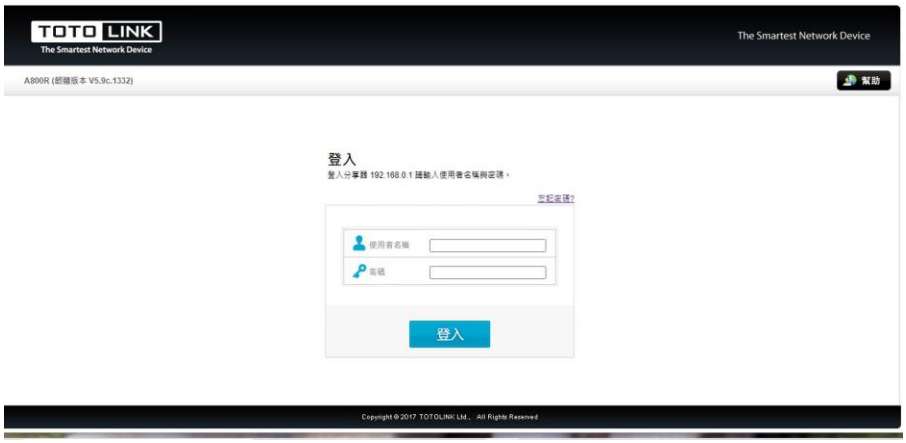


Figure 15. Management Web Interface

Step 2: Report

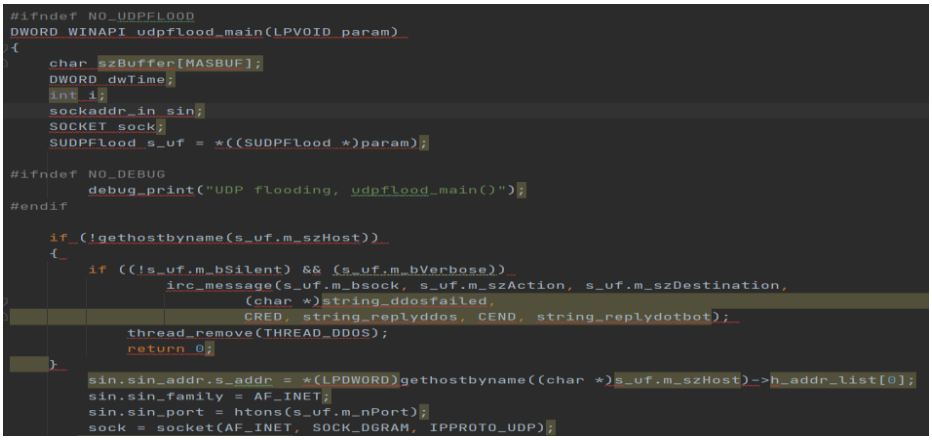
In this step, the Persirai has already logged in to the vulnerable smart camera web management. Persirai executes the code, figure 16, to script download site and waits for the respond. Once the infected smart cameras receive the response, the shell script, will be installed and conducted. The shell script will be deleted and hidden after installed. Like Mirai malware, Persirai also

report the details of infected smart cameras to C&C and prevent the infected smart cameras from attacking by other malware.

Figure 16. Script Download Request and Respond (Trend Micro, 2017)

Step 3: Control and Launch Attack

During this step, the infected smart cameras are also called bots. These bots are waiting for the commands from C&C to launch the UDP flooding DDoS attack. Due to most of smart cameras are conducting UPnP, these bots could easily discover the port of the router opened by these smart cameras, so these bots are able to scan and attack other vulnerable smart cameras through Network as step 1 do then go step 2 until Persirai malware is eliminated from smart cameras just like Mirai malware do. Figure 17 shows part of UDP flooding code from SourceGraph.



```
#ifndef NO_UDPFLOOD
DWORD WINAPI udpflood_main(LPVOID param)
{
    char szBuffer[MASBUF];
    DWORD dwTime;
    int i;
    sockaddr_in sin;
    SOCKET sock;
    SUDPFlood s_uf = *((SUDPFlood *)param);

#ifndef NO_DEBUG
        debug_print("UDP flooding, udpflood_main()");
#endif

    if (!gethostbyname(s_uf.m_szHost))
    {
        if ((!s_uf.m_bSilent) && (s_uf.m_bVerbose))
                irc_message(s_uf.m_bsock, s_uf.m_szAction, s_uf.m_szDestination,
                        (char *)string_ddosfailed,
                        CRED, string_replyddos, CEND, string_replydotbot);
            thread_remove(THREAD_DDOS);
            return 0;
    }
        sin.sin_addr.s_addr = *(LPDWORD)gethostbyname((char *)s_uf.m_szHost)->h_addr_list[0];
        sin.sin_family = AF_INET;
        sin.sin_port = htons(s_uf.m_nPort);
        sock = socket(AF_INET, SOCK_DGRAM, IPPROTO_UDP);
```

Figure 17. UDP Flooding (SourceGraph, 2017)

Combine Malware With CKC

By going through the simulation process of Mirai malware and Persirai malware, we can know how they work and combine the CKC to prevent the attack since the primary goal of both malwares is trying to enter the smart camera and to gain the access. The CKC gives seven steps as a framework to analyze and lower the risk of smart cameras suffering from malware attack. When looking at the Mirai malware and Persirai malware, we understand that the final goal of both malwares is to infect smart cameras then use them as bots to launch the attack. By figuring out the steps provided by CKC, we could identify some methods in each step to mitigate and prevent malware. Since the Mirai malware and Persirai malware are operating equivalent to infect, the mitigation methods could be used similarly. The seven steps of CKC could be divided into three parts. Phase 1 (Reconnaissance) through phase 4 (Exploitation) is the first

part which could be seen as scan the Network step in simulation process. Phase 5 (Installation) and phase 6 (C2) are the second part which is the report part in simulation process. Phase 7 (Actions on objectives) is the third part as control and launch the attack. The ways that can be provided to protect smart cameras from Mirai malware and Persirai malware will be focused on the first and second part.

In the first part, attackers scan through the network to see if there is any open port so they can gain access to smart cameras or other devices through these open ports. For normal smart cameras users to prevent Mirai malware and Persirai malware is to remember to check their network by using scanning tools to see what smart cameras or other devices are connecting to the network then see if there is any open port. Once the open port is figured out, the user should close it as soon as possible to lower the risk. Sometimes attackers might send phishing emails to victims with a link, when people click the link, the malicious malware will have the opportunity to invade the network to infect smart cameras. Not only the general user may be affected by phishing email, but companies also receive it. Without proper training, careless employees can be vulnerable to social engineering attack so attackers can deliver malware. Passwords are also an essential part of defending against malware, and once the smart camera or other device is installed, users should change their password but do not continue to use the default password. The structure of a strong password should be:

- Different from any previous passwords

- At least 12 characters long
- Include characters from at least 3 of the following 4 categories:
    - uppercase
    - lowercase
    - numbers
    - symbols
- Not be a single, recognizable word or your username. Passphrases are preferred

If users have been trained before or have related knowledge, they can still identify malware on their infected smart cameras and then eliminate it. However, most users are not trained enough to identify and eliminate by themselves. One of the ways is to cooperate with an outsourcing company to monitor their smart cameras so the malware could be identified by the outsourcing company and then eliminate it. Another way for general users is to be aware of their smart cameras, most of the smart cameras have a light on when it's operating and there is a microphone in it so users can speak through smart cameras. When people see the unusually flickering lights, the light is on when the user is not using it or there is a strange noise from smart cameras while not using, they should realize that their smart cameras might already be infected.

Within the second part, step 5 (Installation) and step 6 (C2) in CKC, attackers install the backdoor on the victim system so they can access their target camera anytime they want without going through previous CKC steps. The

only thing users and defenders need to do are to block the installation and sever the link between command and control. Once the attacker cannot send the command, the infected smart cameras will be no action which means that the defender successfully prevents the impact. The way to block the installation is to implement a Host-Based Intrusion Prevention System (HIPS) to examine every individual host and every event that occurs in a host for suspicious activities so that it can block common installation paths. The user should also audit the log of smart cameras regularly to identify if there is any suspicious file created.

Anti-Virus (AV) is another tool users and defenders should implement to their smart cameras or other IoT devices to provide real-time protection against malicious software, spyware, and phishing. The AV can cooperate with HIPS to protect smart cameras in a safer way. AV is available on the windows operating system or from third parties with lower cost.

CHAPTER FIVE:

DISCUSSION, CONCLUSION AND AREAS FOR FURTHER STUDY

Summary of Analysis

The analysis of Mirai malware and Persirai malware produced related results when applied to a simulation process in the small simple network and then combine with both malware to CKC. The network and malware were a constant part of the analysis when applied CKC. The simulation process provided for both malware showed that the focus of risk mitigation is the same concept for any smart camera user. The key similarity between the two malware simulations was scanning for the open port which is always ignored by the user. The open port is the break where both malwares can identify the target then try to gain access. Another key similarity between the two malware simulations was the password. Mirai malware applied brute force login to target smart cameras while Persirai used web management to login to the system and gain access. Both similarities show that the user is the most essential part in defending against malware. Attackers might use phishing techniques, malicious files, and social engineering to gain the user password or locate them in the target network. All malicious techniques are a major threat to a careless user. Common mitigation controls to protect smart cameras cannot be separated from the user, as they facilitate malware deployment within smart cameras.

What Vulnerabilities Might the Smart Camera Have?

While going through the simulation process, we know that the major vulnerabilities of smart cameras might have been the open ports and using default passwords or weak passwords themselves or on web management. While operating smart cameras, users must ensure all the ports are closed. Regularly scan through the network to check for the ports then check the log to see if there are any suspicious activities or download. Also, the name of the devices connected to the network helps hackers to identify their target. The other vulnerabilities are users, the lack of security knowledge could lead users to click on phishing emails and then cause their smart cameras to be infected. Another vulnerability for users is the lack of auditing. When malware reports to C&C and uses bots to launch an attack, there will be a record. Once users do not examine the log periodically for unusual activities, it would be the reason for attackers to use smart cameras as bots to launch attack such as MitM and DDoS.

How Mirai Malware and Persirai Malware Take Advantage to These Vulnerabilities and How Can They Be Prevented?

Mirai malware and Persirai malware take advantage of open port and weak or default password to gain access to the smart cameras. Besides, attackers launch MitM attacks to gather information and they use the infected smart cameras as bots to launch DDoS attacks. Attackers also use a phishing email to allure victims click the link to help spread malware. The ways to prevent Mirai malware and Persirai could be found by understanding how they work and

then combining with CKC. A strong password should be set and need to change every 6 months. In addition, the user should implement some mitigation software such as AV, HIPS and Patch. Users need to be aware of phishing emails since most of the malware is sent via email with a link. By not clicking the link in the email protect smart cameras, even the private network. Users could also find an outsourcing company to help them monitor their cameras. Be aware of the unusual sound or lights on smart cameras. Once figure out the infected cameras, cut the communication between cameras to the network to prevent a backdoor used by attackers to look through another target connect to the network.

Conclusion

This project made the analysis of two malware that usually attack smart cameras and built the simulation to see how attackers do in the real world to gain access to smart cameras and launch attacks. Then combine the simulation steps with CKC steps to figure out what methods can be applied to prevent or mitigate the malware attack. Although there is no best way to guarantee that it could 100% prevent smart cameras from infecting by Mirai malware and Persirai malware, what was learned is that several mitigation methods can be combined to improve the security of smart cameras and the user is an important part to defend malware. In conclusion, the more security knowledge the smart camera user has, the safer the smart cameras will be.

Future Work

Apart from Mirai malware and Persirai malware, malware attack is ubiquitous. The open-source code of these malware is still a threat to people because everyone can get it through the Network, and nobody knows when and where the new variant of malware will emerge. For future work, we still need to look at more variables and solutions to malware attacks since an increase in people is using smart cameras not only in their homes but in their companies. There is more knowledge to learn and more work to do for users to improve their cyber defense state.

REFERENCES

ADS security. (2020, April 30). Five Reason To Have Indoor Camera Installed at Home. ADS Security. https://adssecurity.com/five-reasons-to-have-indoor-cameras-installed-at-home/

AIA. (2017, December 19). Benefits of smart cameras in industrial settings. Control Engineering. https://www.controleng.com/articles/benefits-of-smart-cameras-in-industrial-settings/

Ali, Muhammad Hashir. (2022, January 30). Smart Home Security: Security and Vulnerabilities. Wevolver. https://www.wevolver.com/article/smart-home-security-security-and-vulnerabilities

Attify. (2019, January 30). How Mirai Botnet Hijacks Your IoT Devices. Attify. https://blog.attify.com/how-mirai-botnet-hijacks-your-devices/

Ben, Dima & Igal. (2016, October 26). Breaking Down Mirai: An IoT DDoS Botnet Analysis. Imperva. https://www.imperva.com/blog/malware-analysis-mirai-ddos-botnet/?redirect=Incapsula

Buxton, Oliver. (2022, August 17). What is the Mirai Botnet. Avaset Academy. https://www.avast.com/c-mirai

Chang, Ziv. (2019, July 30). Inside the Smart Home: IoT Device Threats and Attack Scenarios. Trend Micro. https://www.trendmicro.com/vinfo/fr/security/news/internet-of-things/inside-the-smart-home-iot-device-threats-and-attack-scenarios

Chiu, Dove, Lu, Kenney & Yeh, Tim. (2017, May 9). Persirai: New IoT Botnet Targets IP Cameras. Trend Micro. https://www.trendmicro.com/en_us/research/17/e/persirai-new-internet-things-iot-botnet-targets-ip-cameras.html

Cloudflare. (2017, December 14). Inside the infamous Mirai IoT Botnet: A Retrospective Analysis. https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/

Cybersecurity Exchange. (n.d.). The Cyber Kill Chain: The Seven Steps of a cyberattack. https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/

Dickson, Ben. (n.d.). The IoT ransomware threat is more serious than you think. IoT Security Foundation. https://www.iotsecurityfoundation.org/the-iot-ransomware-threat-is-more-serious-than-you-think/

Frunlinger, Josh. (2022, August 7). What is IoT? The Internet of thing explained. Networkworld. https://www.networkworld.com/article/3207535/what-is-iot-the-internet-of-things-explained.html

Hassan, Jahanzaib. (2017, May 10). New Persirai Malware infects tons of IP cameras. Hackread. https://www.hackread.com/persirai-malware-infects-tons-of-ip-cameras

Imperva. (n.d.). Man in the Middle Attack. https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/

Jones, Tanner. (2021, December 5). IoT Vulnerabilities: IP Cameras Most Insecure IoT device. Nerd For Tech. https://medium.com/nerd-for-tech/iot-vulnerabilities-ip-cameras-the-of-most-insecure-iot-device-b1dcf73d8b03

Laughlin, Andrew. (2022, November 9). How to stop your wireless security camera from being hacked. Which? https://www.which.co.uk/reviews/wireless-security-cameras/article/how-to-stop-your-wireless-security-camera-from-being-hacked-a61gJ5O2LAur

MYRA. (n.d.). What is Mirai. https://www.myrasecurity.com/en/what-is-mirai/rom

Netskope. (n.d.). What is the Cyber Security Kill Chain. https://www.netskope.com/security-defined/cyber-security-kill-chain

Roberts, Paul. (2017, May 9). Persirai Botnet: 120,000 Hacked Cameras Phoning Home to Iran. https://securityledger.com/2017/05/persirai-botnet-120000-hacked-cameras-phoning-home-to-iran/

Soare, Bianca. (2022, June 20). The Cyber Kill Chain (CKC) Explained. Heimdal. https://heimdalsecurity.com/blog/cyber-kill-chain-model/

Sourcegraph. (n.d.). https://sourcegraph.com/search

Tabona, Andrew. (2018, August 3). Scanning Open Ports in Windows: Part 3 (NMAP). TechTalk. https://techtalk.gfi.com/scanning-open-ports-in-windows-part-3-nmap/

Technology org. (2019, July 18). How Do Smart Camera Works. https://www.technology.org/2019/07/18/how-do-smart-cameras-work/

Tuohy, Jennifer Pattison. (2021, April 1). How Do Home Security Camera Works. U.S. news. https://www.usnews.com/360-reviews/services/security-cameras/how-do-security-cameras-work

Tuohy, Jennifer Pattison. (2021, October 13). Wired vs. Wireless Home Security Cameras. U.S. news. https://www.usnews.com/360-reviews/services/security-cameras/wired-vs-wireless

VALEO network. (n.d.). How is the IoT being impacted by malware. https://www.valeonetworks.com/how-is-the-internet-of-things-iot-being-impacted-by-malware/

Vedere Labs. (2022, June 1). R4IoT: When Ransomware Meets the Internet of Things. Forescout. https://www.forescout.com/blog/r4iot-when-ransomware-meets-the-internet-of-things/