CMSC 414 Final Project: Mirai Botnet

By: Suraj Ilavala, Ankur Patel, and Daniel Ruiz

Background

- Mirai Botnet was created 21 year old Paras Jha and 20 year old Josiah White who co-founded Protraf Solutions.
- Mirai Botnet attacks IoT Devices that contain ARC processors.
    - The ARC processor is a compressed version of a Linux Machine
- After turning devices into bots and a botnet is created; then the botnet is used to carry out a DDoS attacks

Project Objectives

- Understand the Mirai Botnet
- Understand IoT vulnerabilities
- Infect a another device or a Virtual machine with Mirai Botnet
- Use the bot and botmaster attack a IoT device
- Gain access to IoT device

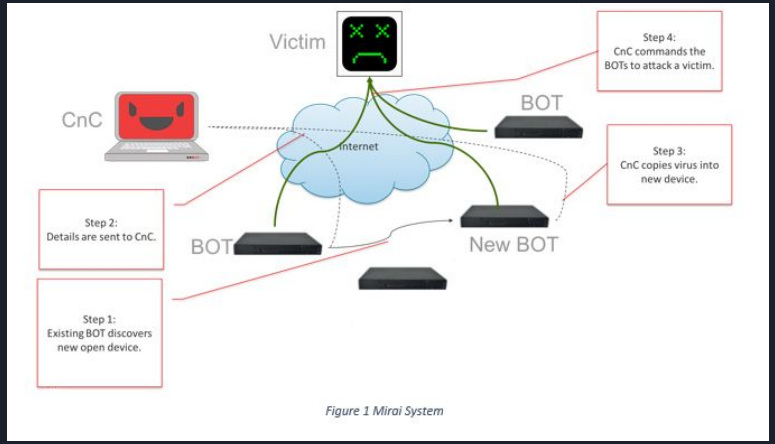
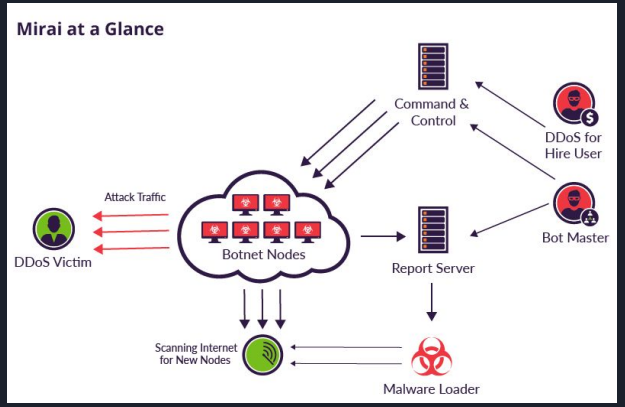
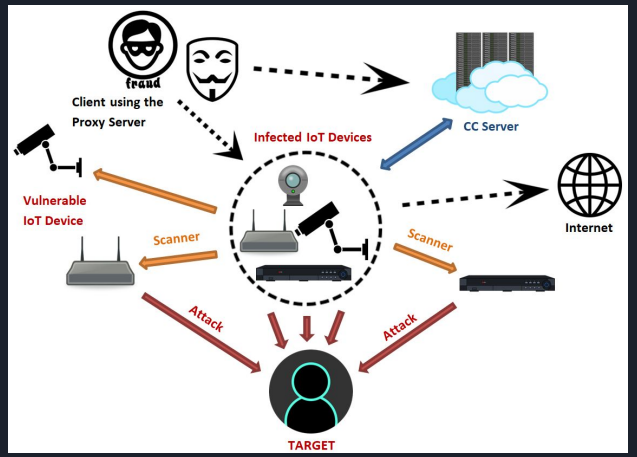


Figure 1 Mirai System

Approach

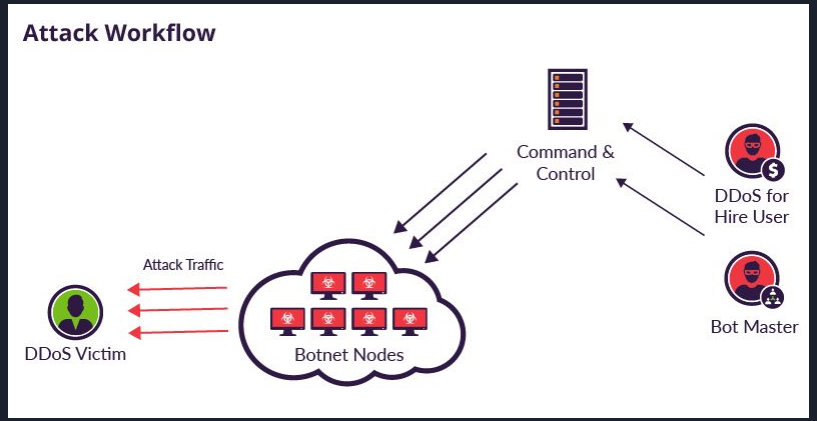
1. First find a vulnerable IoT device to practice on
2. Infect a vulnerable device with Mirai virus and turn it into a bot
3. Use the bot with the botmaster to attack IoT device.





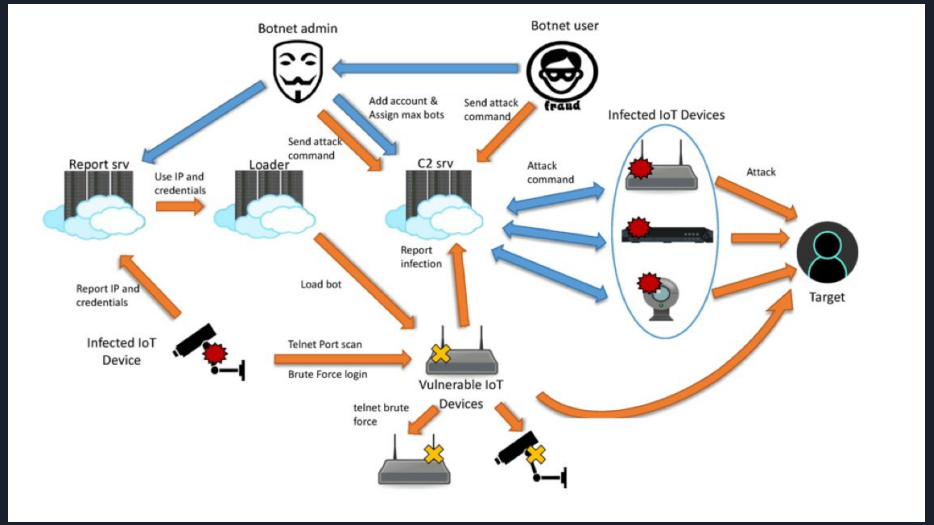
Tasks

1. Find a IoT device proxy that is vulnerable to Mirai Botnet
2. Enable a botmaster to control a botnet
3. Use the botnet to break into the IoT device



Implementation

1. Configure C&C server on Ubuntu image
2. Compile and distribute client file to victim machine
3. Establish ssh connection to victim
4. Execute scripts and modify local files from C&C



Evaluation

- Wireshark utilized for network analysis
- Capture shows evidence of ‘ssh’ connection and data transfer through respective port
- Attacker was able to view the contents of victim’s directory
- Victim’s “Downloads” directory was compromised, as shown in demo

Botnet was successful in establishing a connection with the victim and executing a remote attack on their system.

```
$ python server.py --host 192.168.226.135 --port 8080
```

Host

Source	Destination	Protocol	Length	Info
192.168.226.135	192.168.226.137	TCP	286	8080 → 33212 [PSH, ACK] Se
[illegible]	192.168.226.135	TCP	66	33212 → 8080 [ACK] Seq=1 A
192.168.226.137	[illegible]	TCP	326	33212 → 8080 [PSH, ACK] Se
192.168.226.135	192.168.226.137	TCP	66	8080 → 33212 [ACK] Seq=221
192.168.226.137	[illegible]	TCP	222	33212 → 8080 [PSH, ACK] Se

Victim

```
[osboxes @ /home/osboxes/Desktop/byob]>shell 0

Starting Reverse TCP Shell w/ Session 0...

[ 0 @ /home/osboxes/Downloads ]>ls

distUtils.py
```