Mirai botnet

Abhinav Narain

December 7, 2016

1 Mirai Activity and Results

1.1 Breakdown of Activity

The following activity is performed by Mirai bot.

1. Sets up some certain data structures, and kills a previous instance is running.
2. Connects to CNC server after resolving the IP address using a DNS packet to DNS server
3. *fork()* to do a SYN scan for a range of IP addresses by transmitting TCP syn frames using RAW sockets
4. Run an infinite loop waiting for SYN responses for further conducting a TELNET login
5. Wait for attacks from a CNC server and *fork()* to launch an attack for a period of time – one of which is a UDP flood attack conducted for 5 seconds 1

1.2 Expected Output of EMI

- Step 2 above should produce an EMI on spectrogram corresponding to SYN packets transmitted in bulk to certain subnets.
- Step 4 should show EMI on spectrogram corresponding to UDP flooding

1.3 Lenovo laptop

I did the experiments by running Mirai bot on the laptop.

1.4 Raspberry Pi

I did the experiments with Raspberry Pi as the client. As with previous experiments of UDP blasts and computation, I was not able to see change in EMI. There are possibly two reasons for it.

- It uses the USB power-supply 2. I am not clear about how the conversion of power supply takes place.
- The change in power consumed by Raspberry Pi might not be significant. I don't think this should be the case. A busy loop should have changed the noise profile in our previous experiments and also showed some change in noise on powerline when Mirai was executed.

2 Setup

The setup was first made in Virtual environment and then ported to actual machines on a private network in lab.

- Linux Box DNS server
- Linux Box CNC server
- Rasperry Pi - client

3 Attack from CNC

The 1 shows the CNC server Mirai interface over localhost. One attack was conducted – UDP flood attack for 5 seconds.

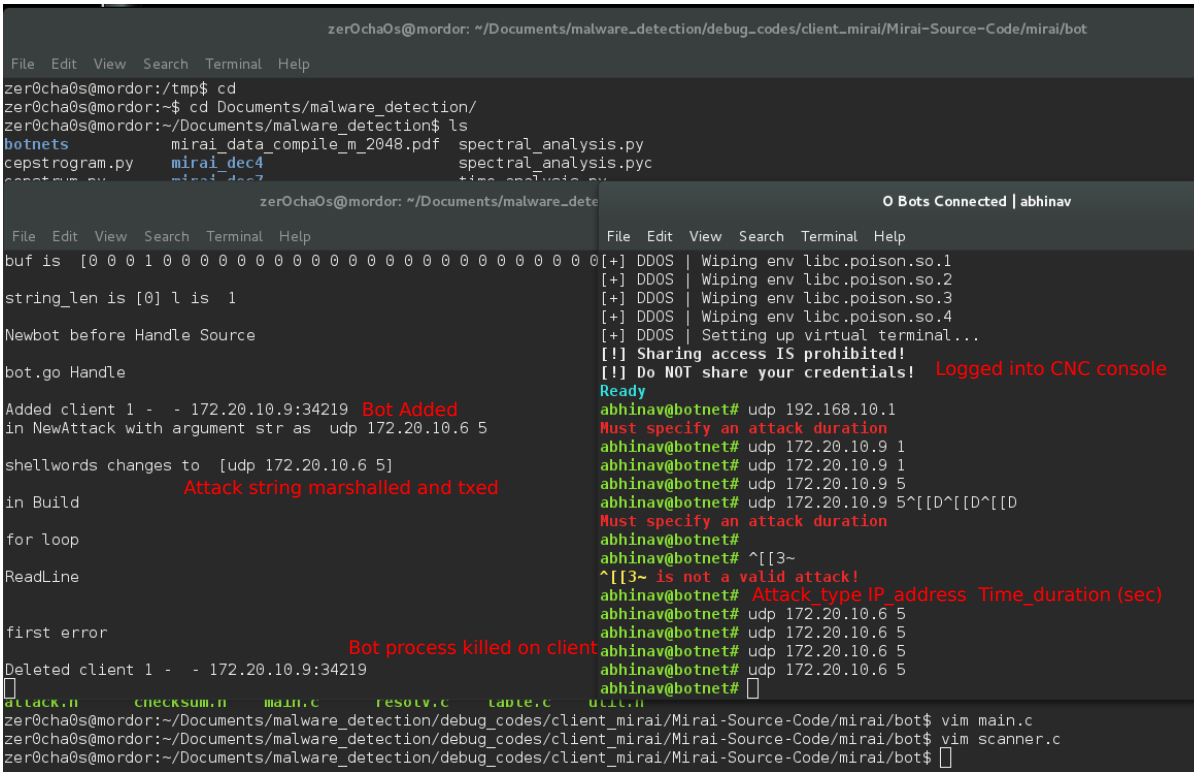

Figure 1: Attack issued on CNC window. UDP flood for 5 seconds

Figure 2: USB to powerline converter adapter for Raspberry Pi