[Poison Tap]
Final Project

[Eonshik Kim]

[CS 658]

[Rafat Elsharef]

[May 17, 2019]

Overview

In this project, I am going to install Poison tap on Raspberry Pi Zero, and I will try to see that I could hack my laptop (Mac) by using it. I will write about the result that hacking is successful or not and explain how to protect a computer from this tool.

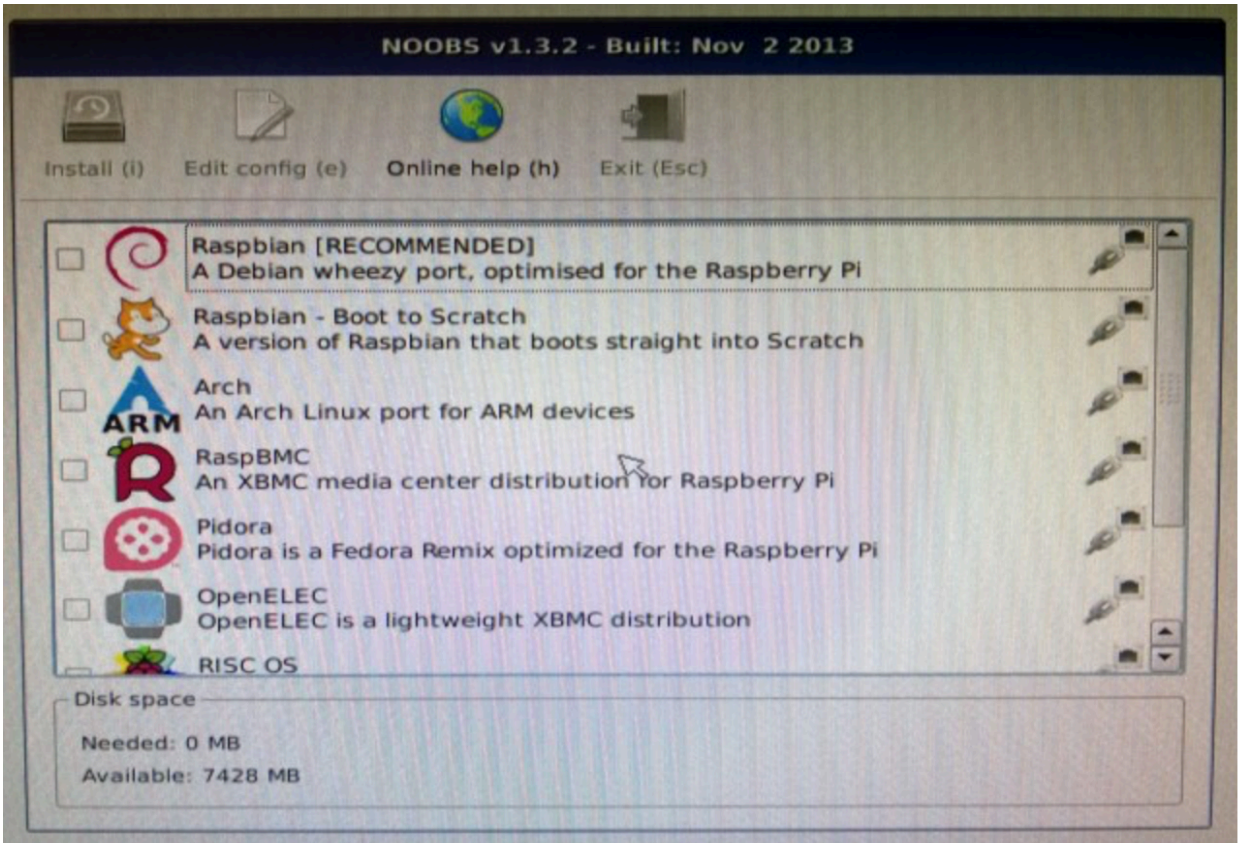
What is Poison Tap?

Poison Tap is the USB hacking tool that exploiter can install web backdoor on the locked computer over USB. This tool is made by Sami Kamkar in 2016. It's a simple tool by using node.js. An attacker can install Poison Tap on Raspberry Pi Zero. Then, the attacker connects the Raspberry Pi on the target computer over USB. Once, it connects, it emulates an Ethernet device over USB and hijacks all internet traffic from the machine. It siphons and stores all HTTP cookies and sessions include all the log of search history.

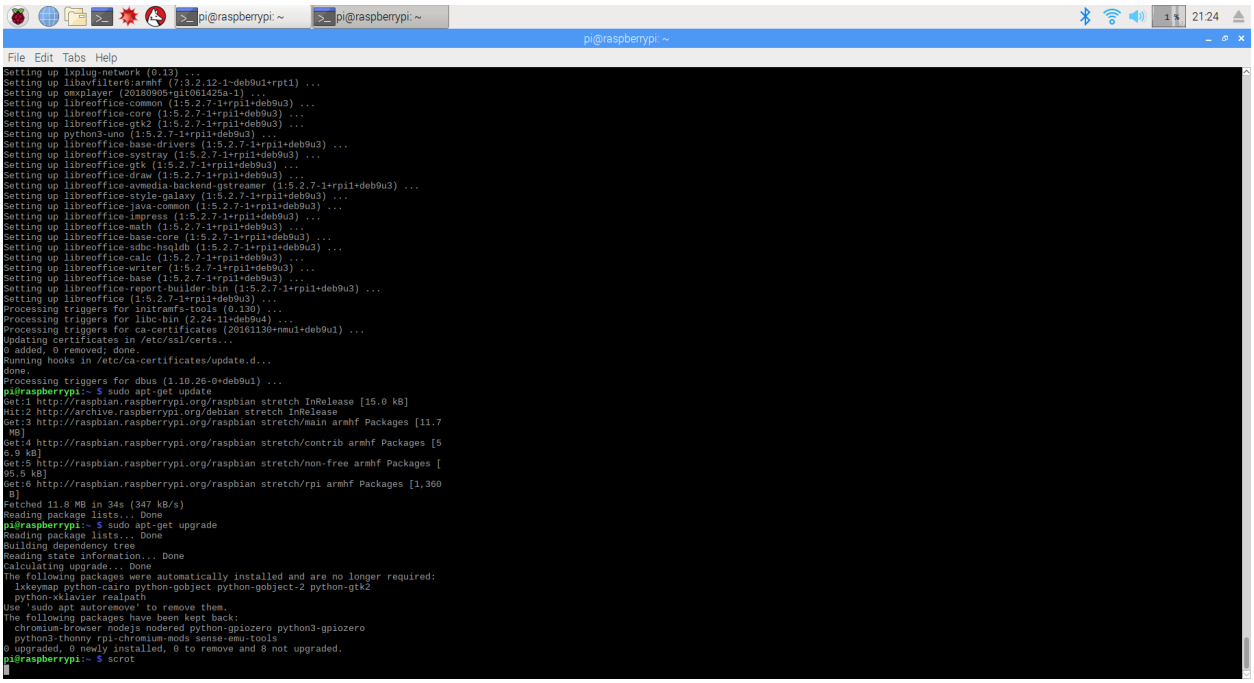
What do I need?

- A Raspberry Pi zero
- 16GB SD card
- A micro USB cable
- Monitor for Raspberry Pi
- Target computer
- Raspbian
- Poison Tap git

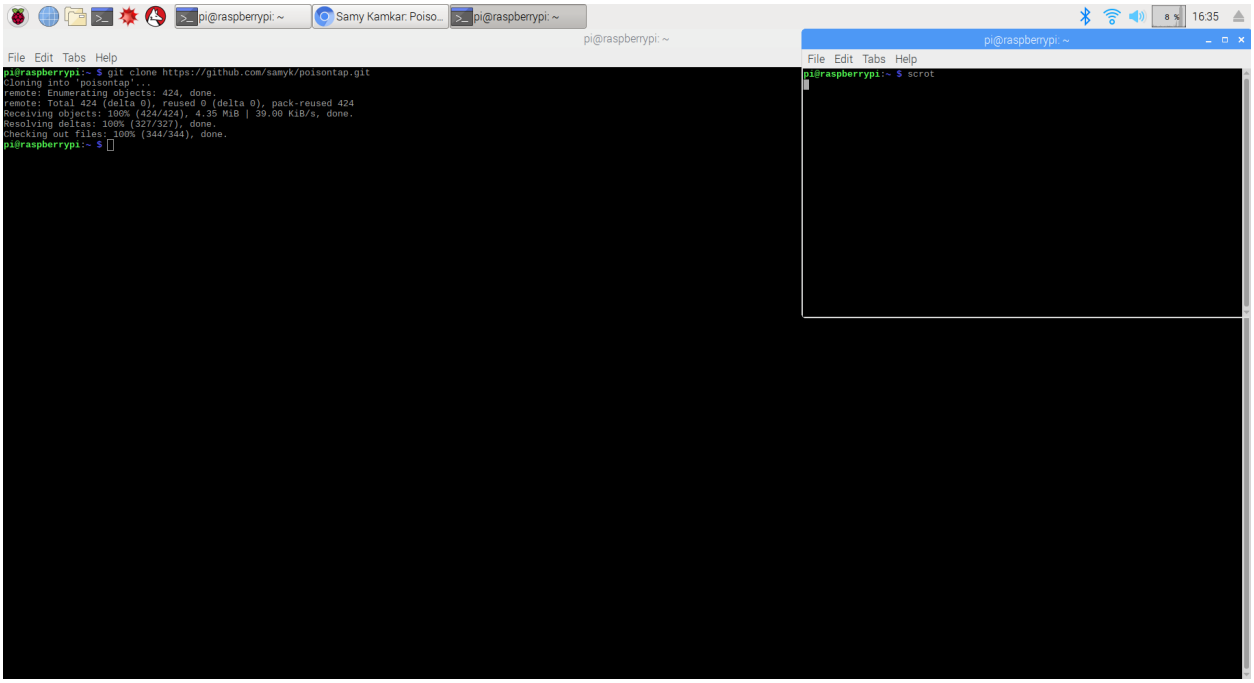
How to install Poison Tap?



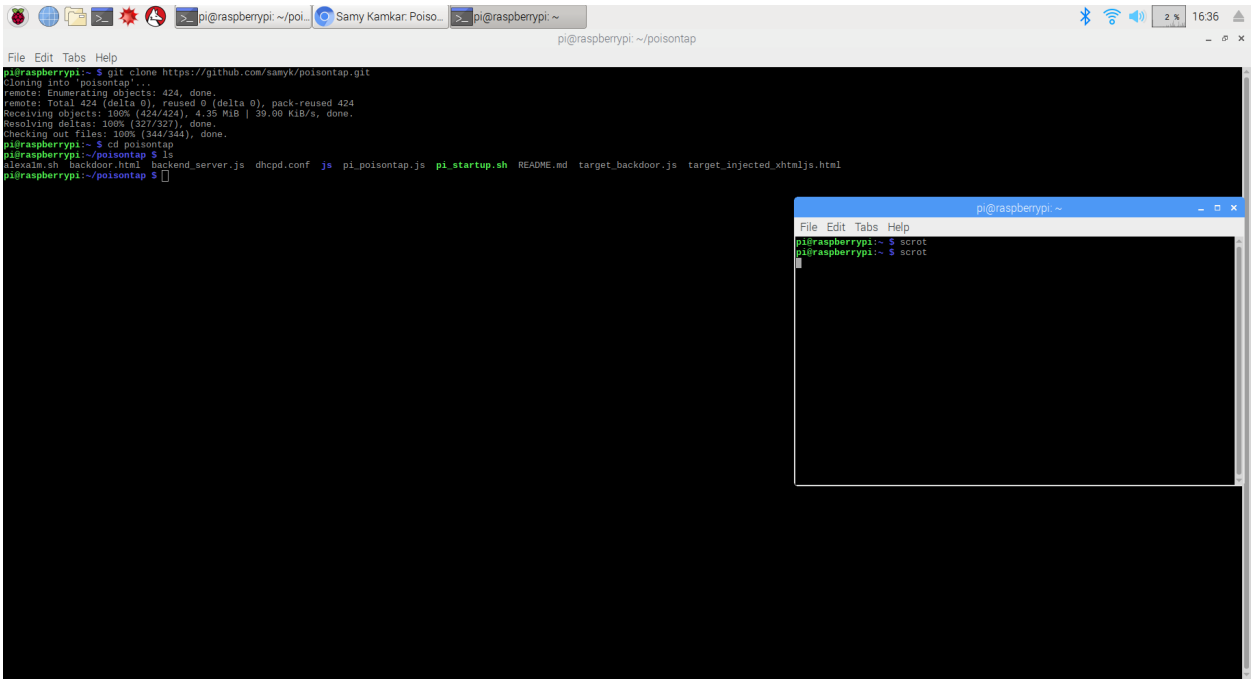
I installed the Raspbian on my Raspberry Pi Zero first.



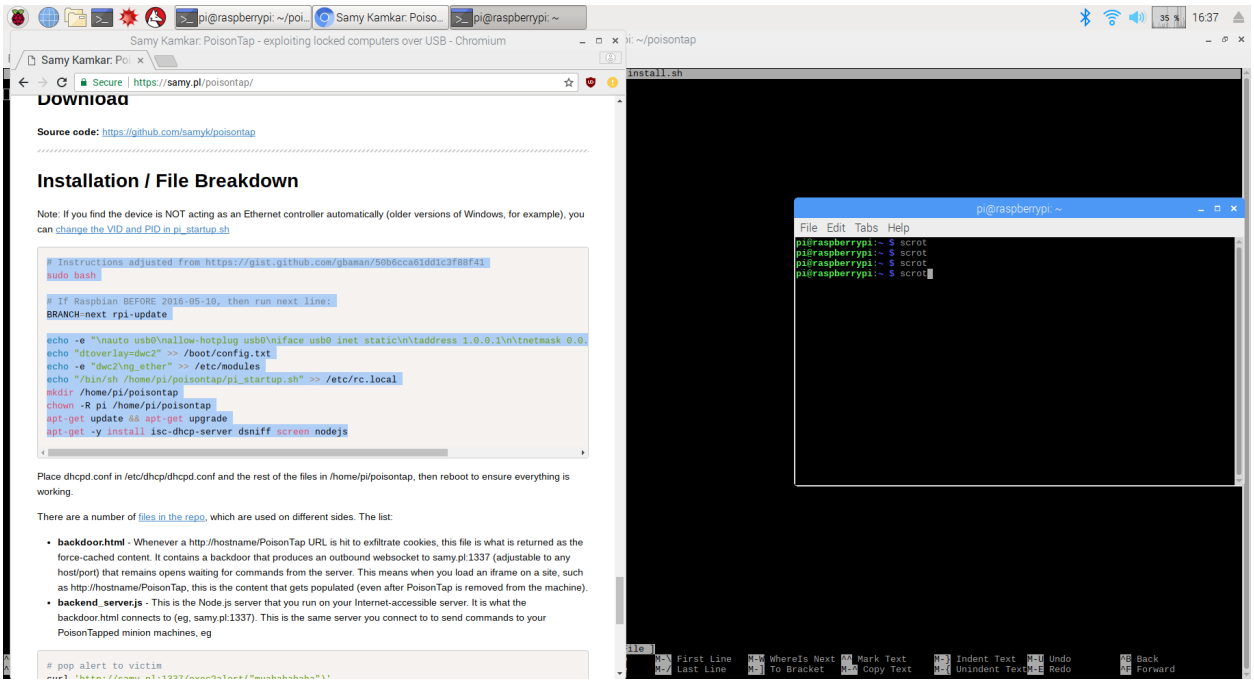
I needed to update the Raspbian as the latest version. I used the command “sudo apt-get update” and sudo apt-get upgrade”.



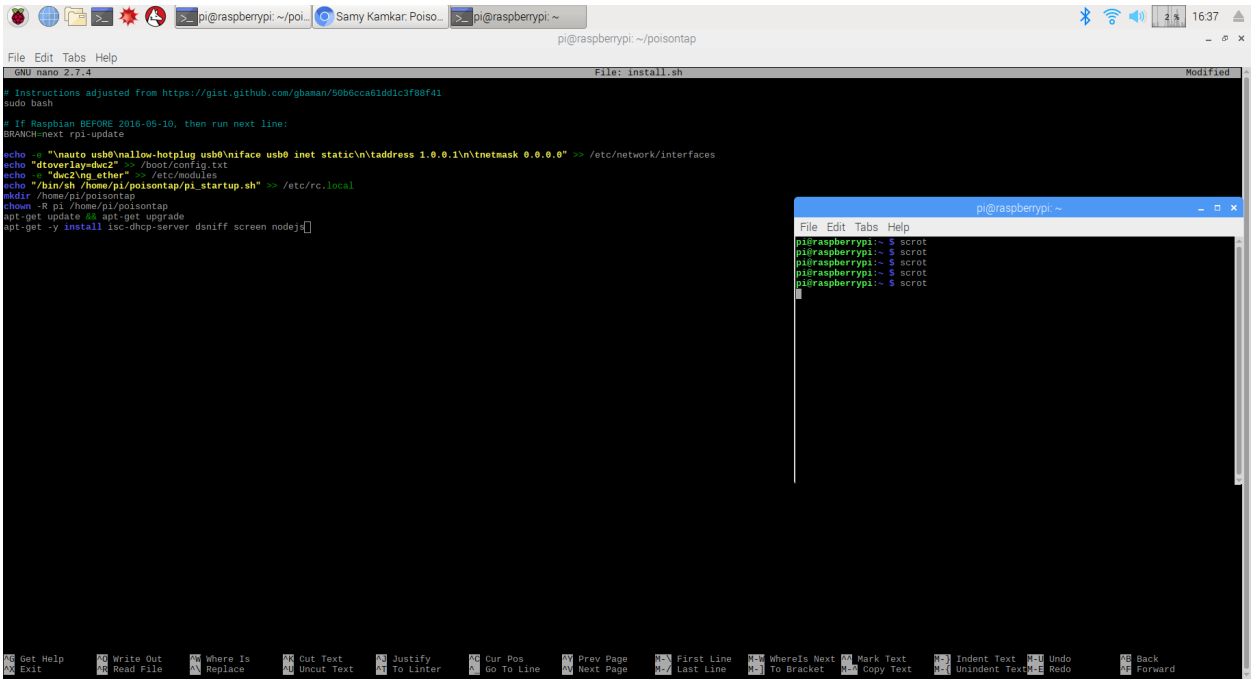
Then, I cloned the git by typing “git clone https://github.com/samyk/poisontap.git”.



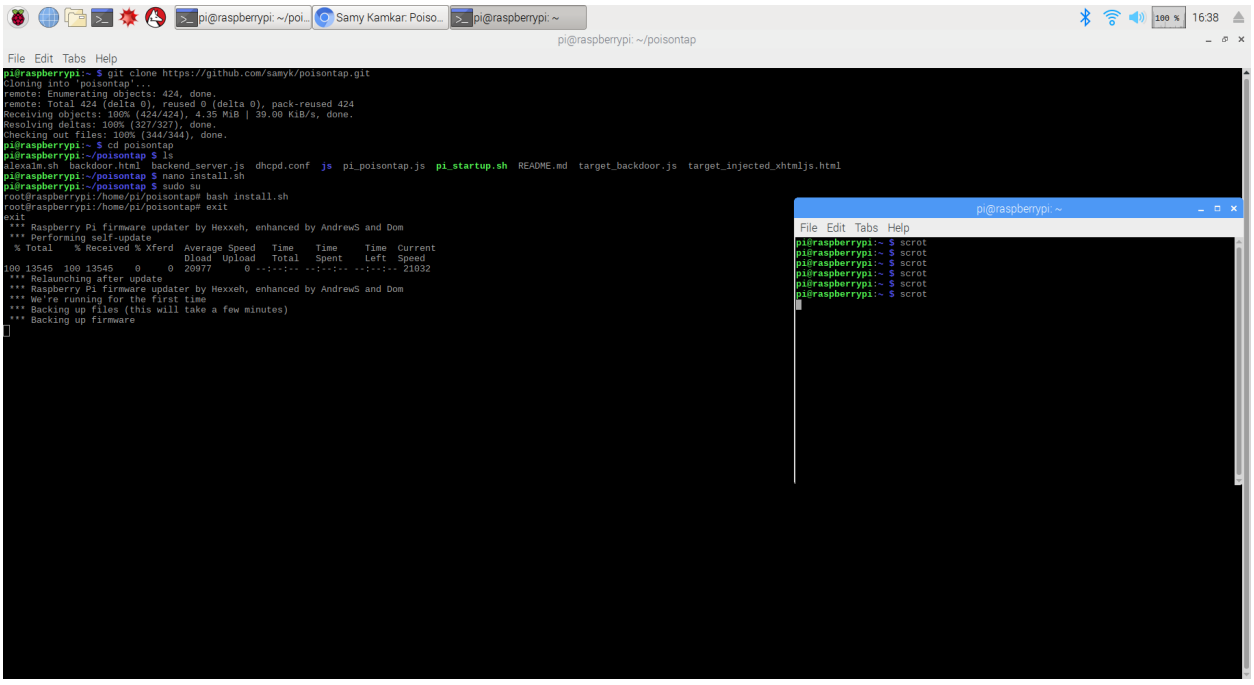
Then, I typed “cd poisontap” to change the directory to the “poisontap” folder. Once, I typed “ls” I was able to see the files in the “poisontap” folder. After that, I typed “nano install.sh” to create the new file.



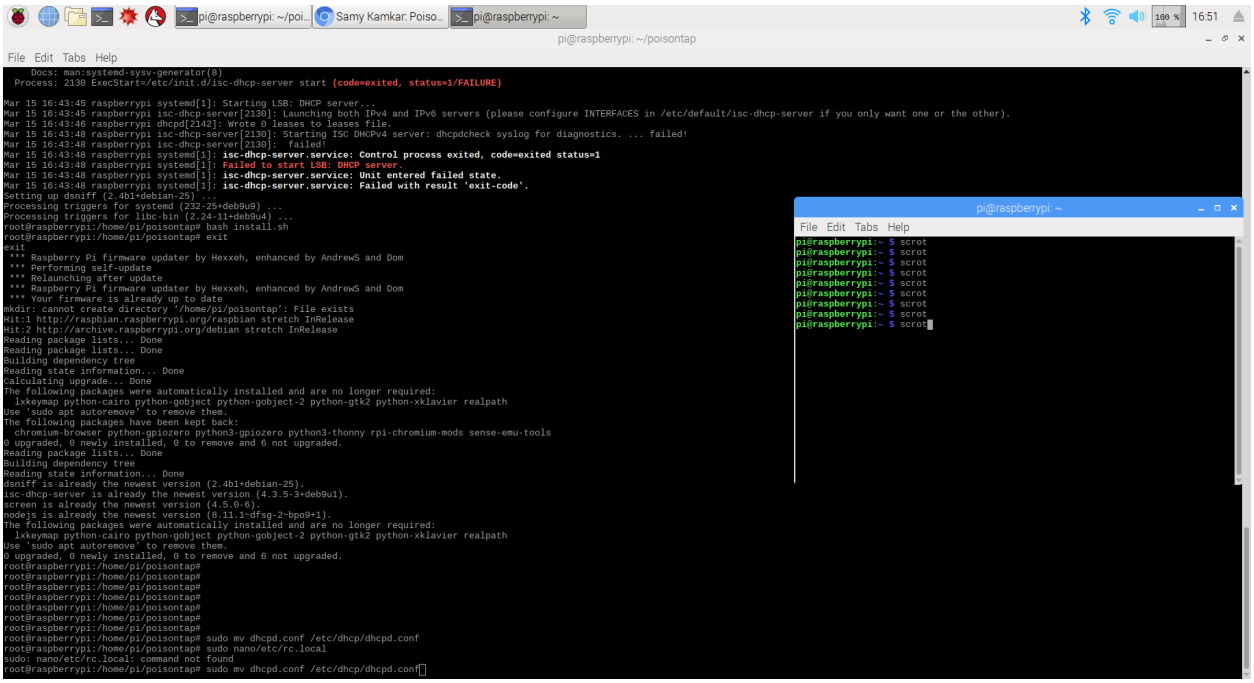
I copied the installation code from “http://samy.pl/poisontap/



Then, I pasted it on install.sh. After that, I typed “ctrl + x” to save the file.

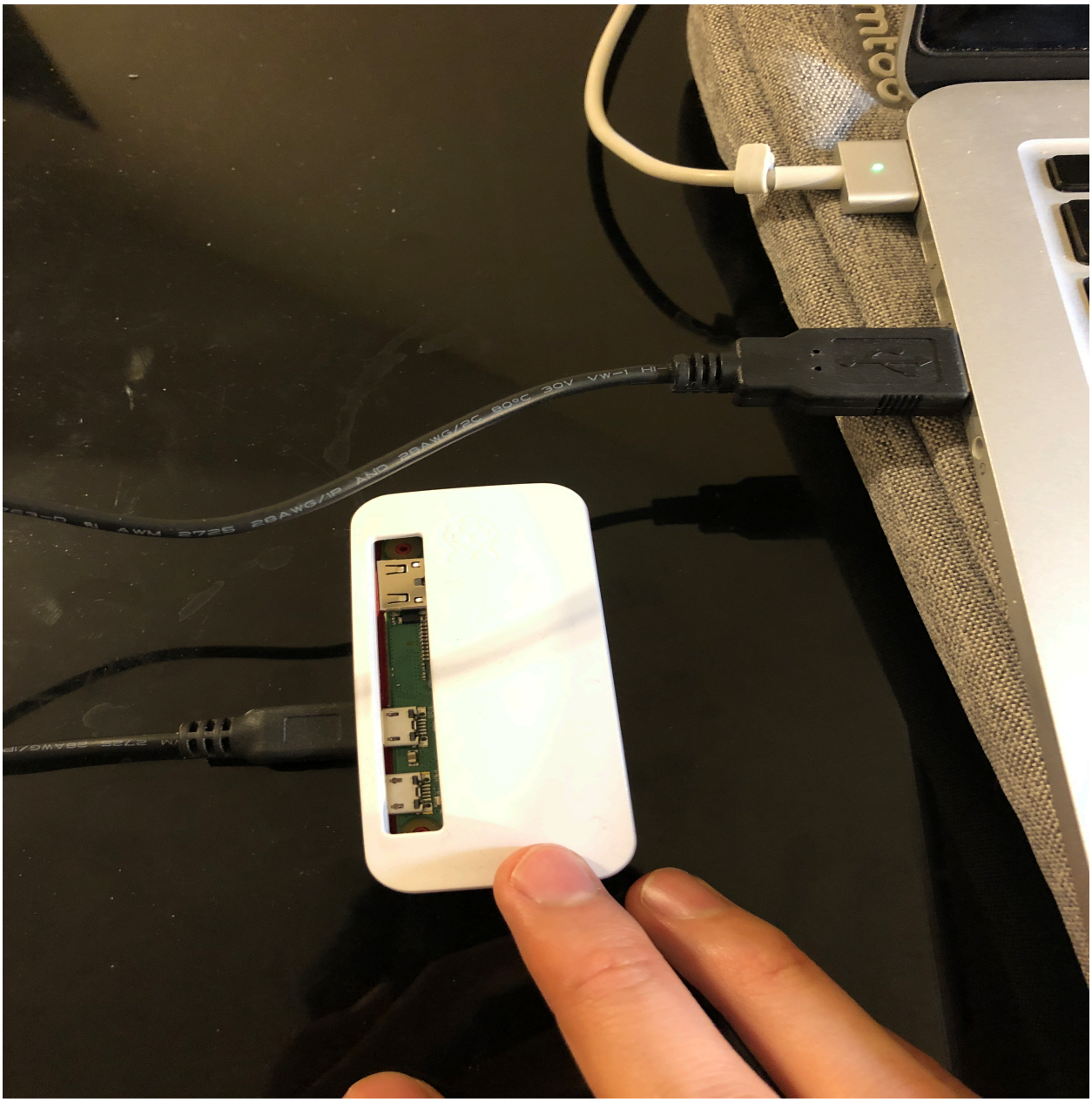


I used the command “sudo su” and “bash install.sh” to process the installation for Poison Tap.

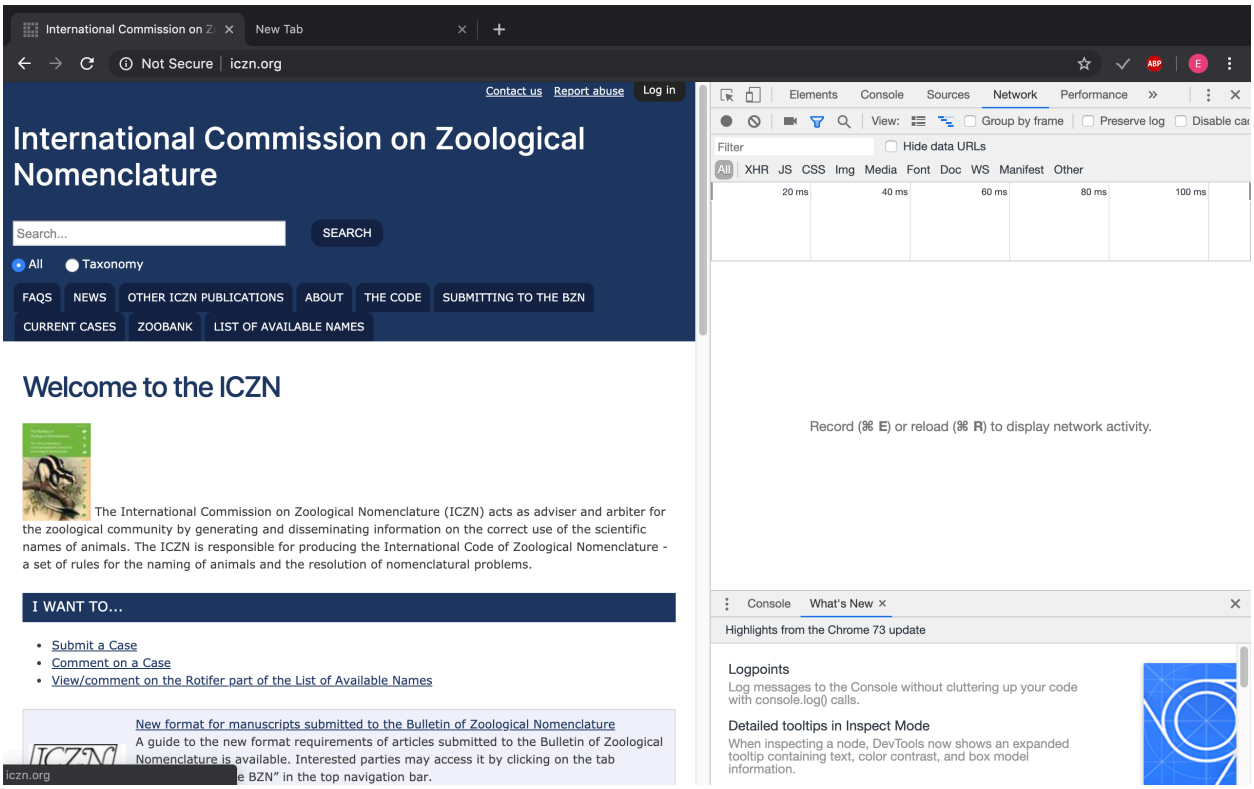


After the installation was finished, I typed “sudo mv dhcpd.conf/etc/dhcp/dhcpd.conf” to move the config file. Poison Tap was ready to use at this point.

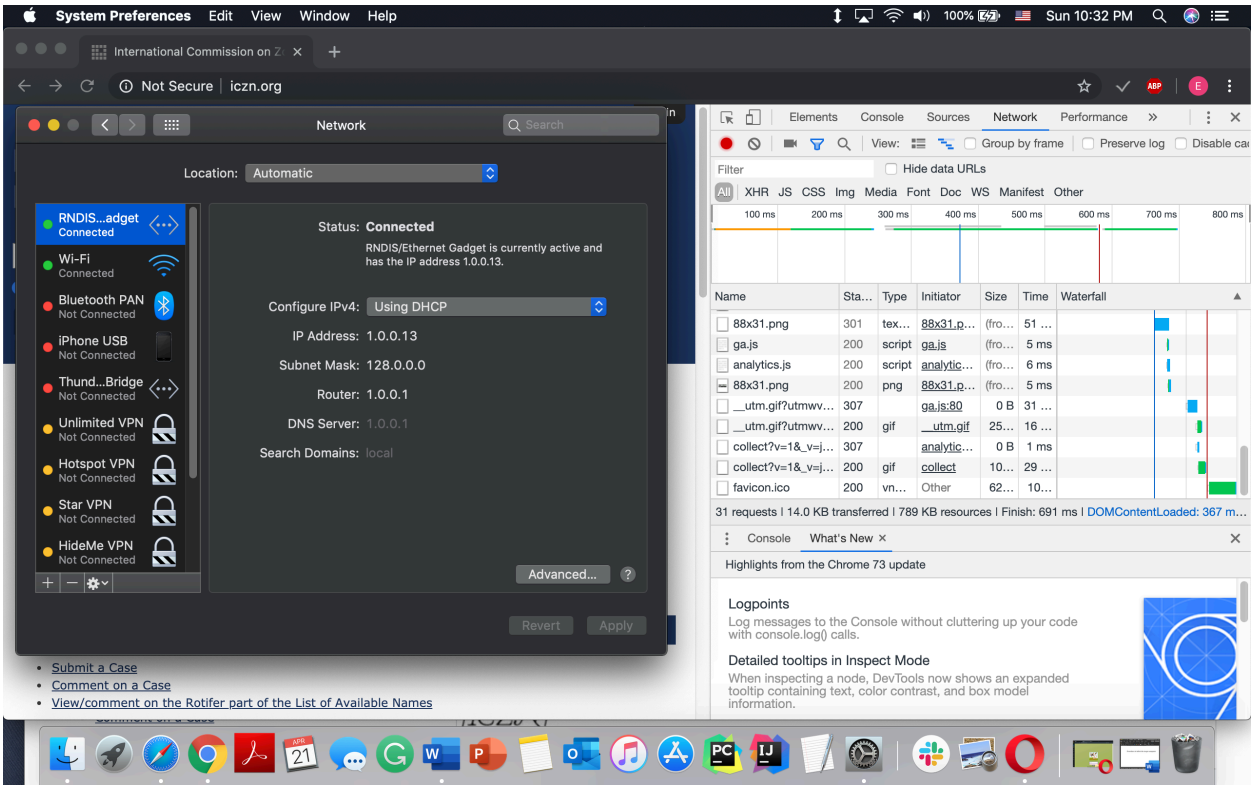
Procedure to infect the target computer



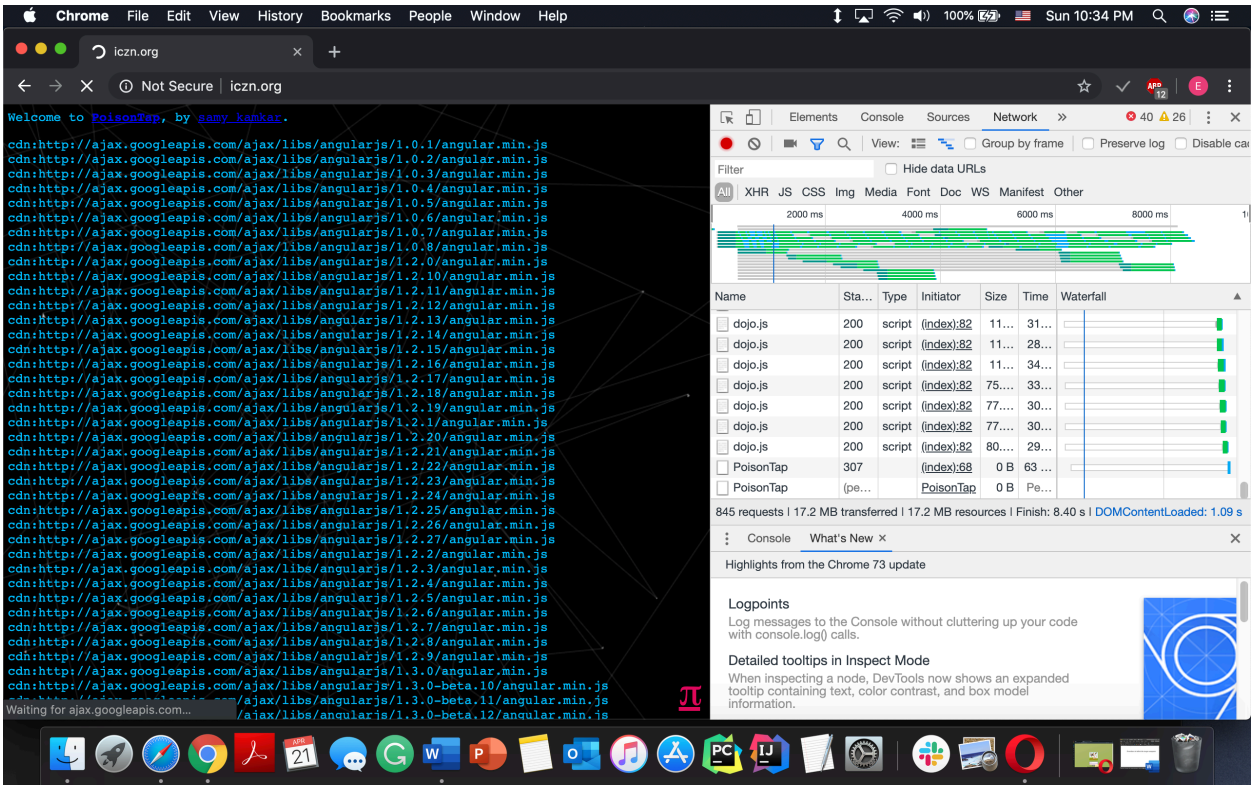
First, I plugged the Raspberry Pi zero into the target computer via USB.



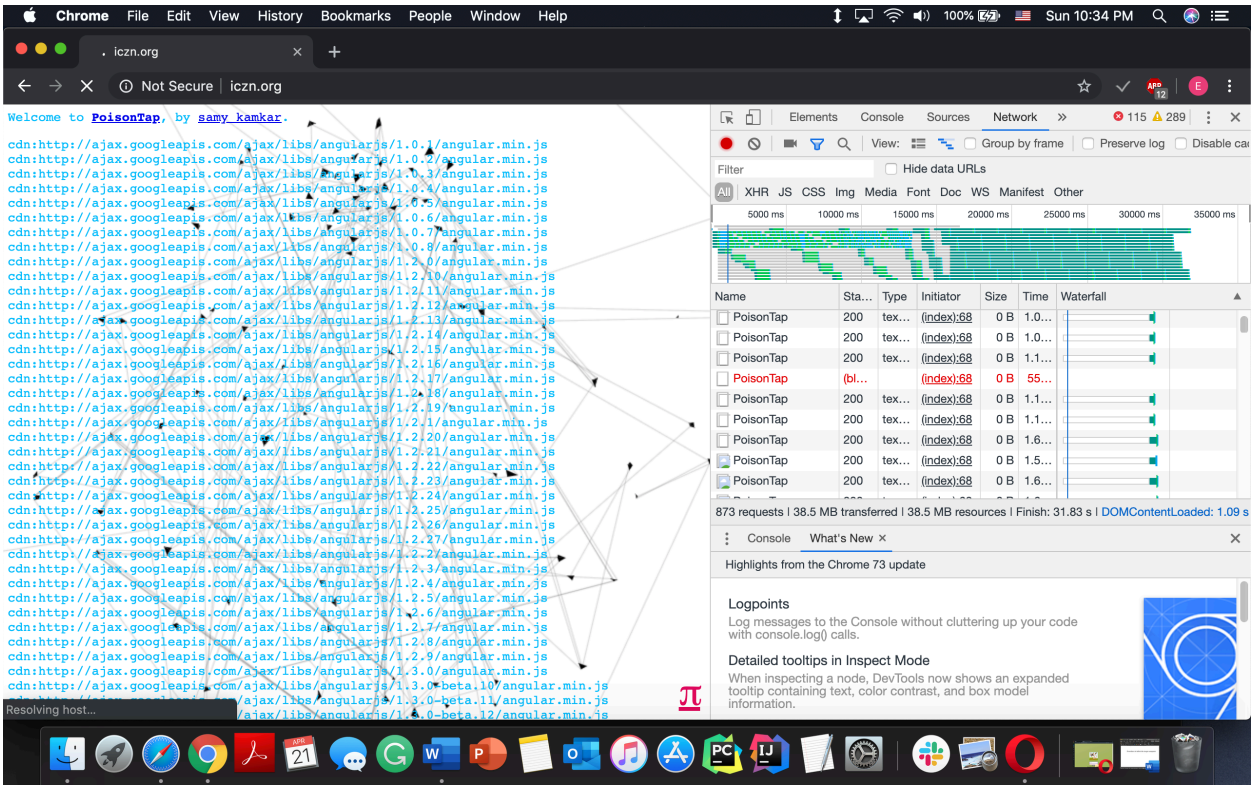
I prepared the HTTP website before I plug the Raspberry Pi zero into the target computer via USB. Poison Tap only works when HTTP website is on.



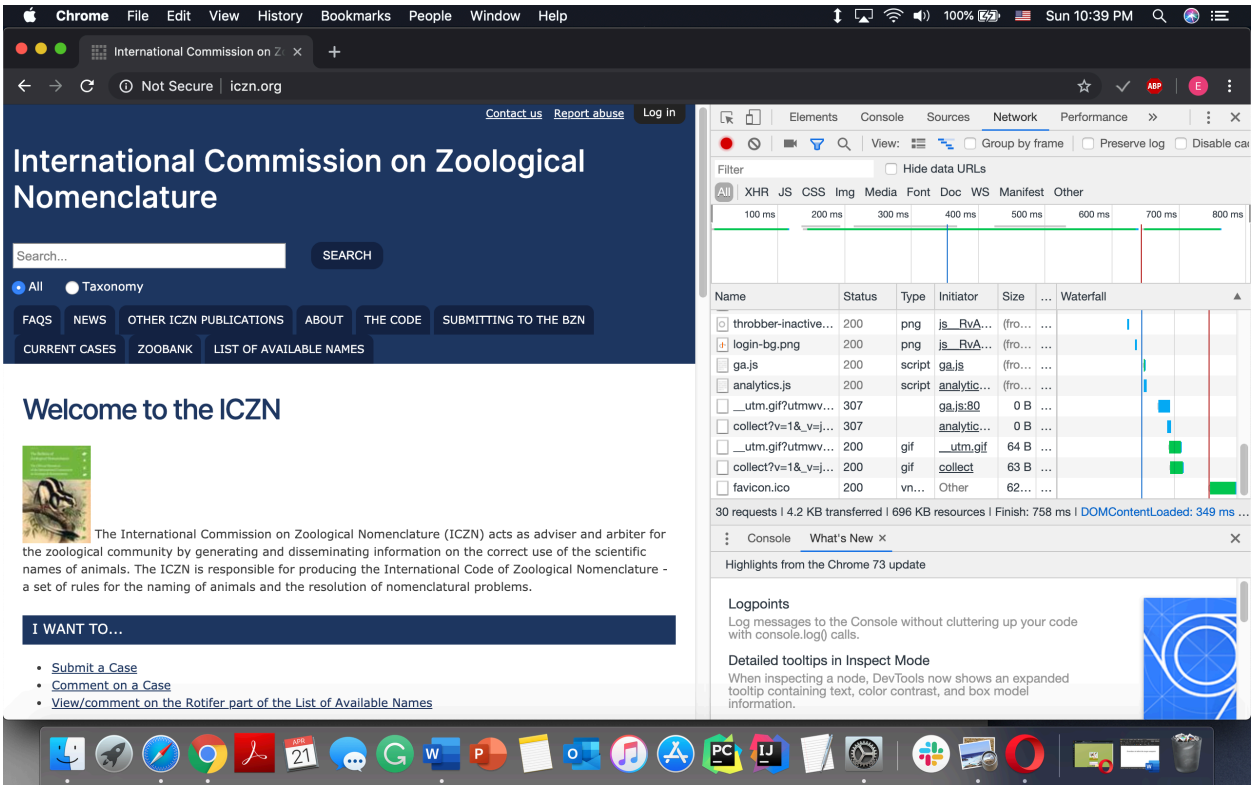
Once, I plugged in, the Poison Tap was disguised as RNDIS/Ethernet Gadget and connected as a DHCP. DHCP stands for Dynamic Host Configuration Protocol. It dynamically allocates IP addresses. Poison Tap responds to the DHCP request, and it provides the machine with an IP address. It provides entire IPv4 addresses from 0.0.0.0 to 255.255.255.255 rather than providing a small subnet.



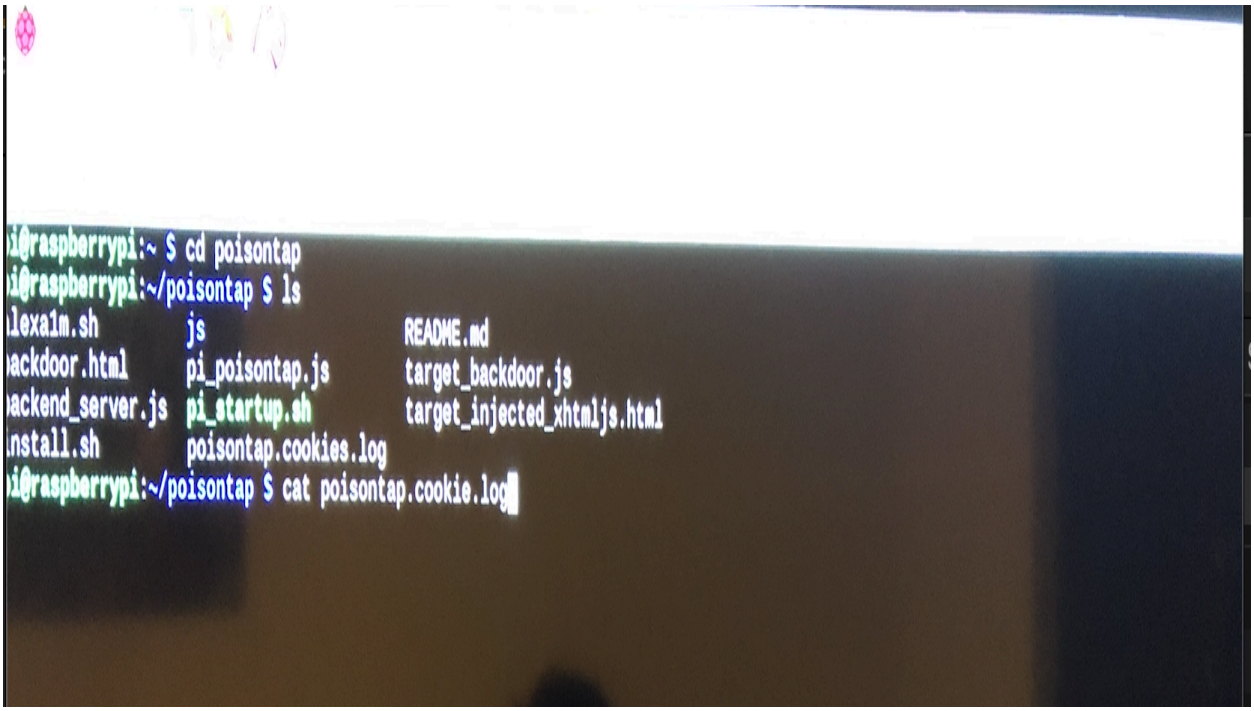
After about 30 seconds, when I redirected the HTTP page. I found that the cool screen was displayed.



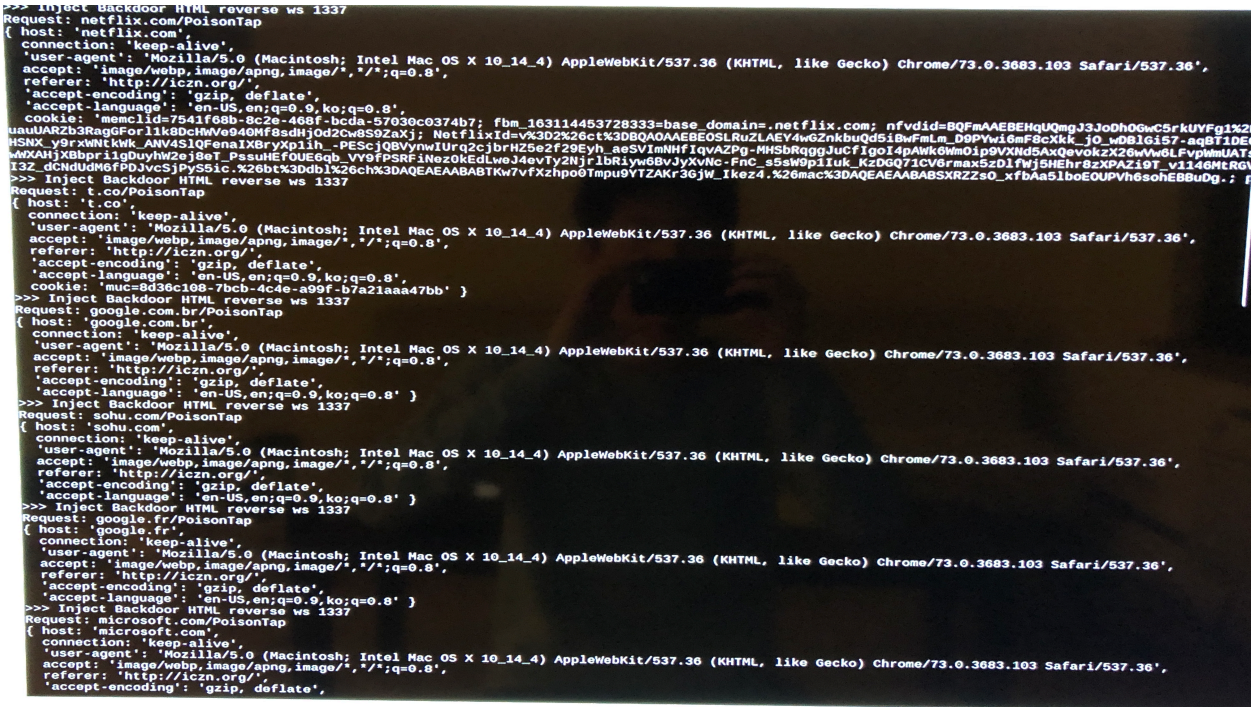
I was able to see that web backdoor was installed. All of the names of the files were changed to “PoisonTap”.



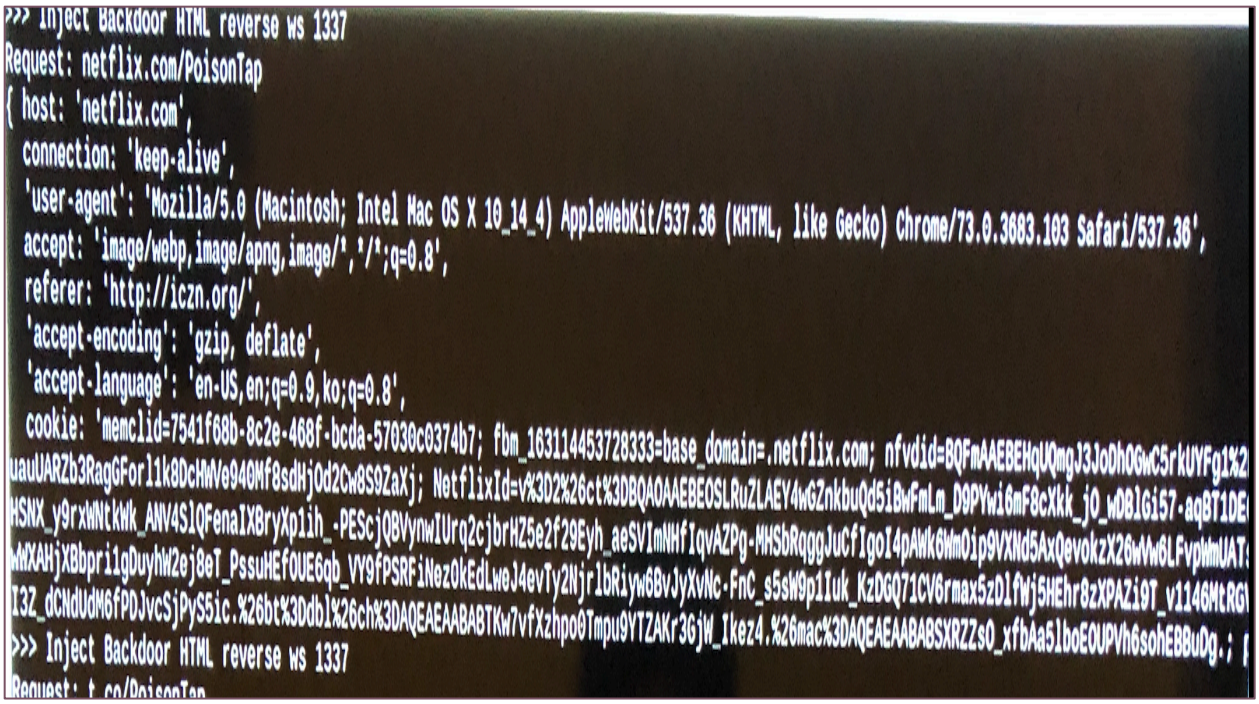
Once, I plugged it off. The screen was back to the normal page.



I booted Raspbian and I found that “poisiontap.cookies.log” was created. I saw the file by typing “cat poisontap.cookie.log”.



I could see lots of HTTP only cookies. I found the websites like Netflix.com and Microsoft.com that I entered before.



I zoomed in the cookie for Netflix. I could see that the referrer is http://iczn.org/. It's the website that I installed the web backdoor. I also found that Netflix uses HTTP only cookie to store the username instead of a secure cookie.

How to prevent?

From the website “Latest Hacking News”, “HTTP Only cookie is a flag added to cookies that tell the browser not to display the cookie through client-side scripts” (Latest Hacking News). Once, I exploit HTTP only cookies I could steal private information by using session hijacking. Session hijacking is the exploitation of a valid computer session. I will be able to log in without a password by using cookie and session hijacking. Of course, the website needs to be vulnerable from session hijacking. There are some methods to prevent getting hacked from Poison Tap.

1. You should never use the http only website for the startup page. Poison Tap only works if the http only website is opened.

2. You should delete the cookies for the browsers frequently. As deleting the cookies, it will also delete the web backdoor that Poiston Tap installed.

3. You should use only HTTPS websites - Cookies set with the "Secure" keyword will only be sent. Fortunately, most of websites are HTTPS(secure) now. However, you still need to be careful that some websites are still HTTP only.

Conclusion

In this project, I was able to install Poison tap on Raspberry Pi Zero, and I tried to see that I could hack my laptop (Mac) by using it. I was able steal the HTTP only cookies from my laptop even though the laptop was lock. I also explained the methods to protect a computer from this tool.

References

https://samy.pl/poisontap/

https://arstechnica.com/information-technology/2016/11/meet-poisontap-the-5-tool-that-ransacks-password-protected-computers/

https://www.security-sleuth.com/sleuth-blog/2017/3/6/installing-poison-tap-for-dummies-the-most-complete-guide

https://www.youtube.com/watch?v=Aatp5gCskvk

https://www.youtube.com/watch?v=B9EraHobheE

https://latesthackingnews.com/2017/07/03/what-is-httponly-cookie/