evazor

Thank You for buying Evazor, before we start playing with the device please remember this is only for testing your own devices and educational purposes. I do not take responsibility for what you do with it.

Please check the legal regulations for your country to make sure you don't violate any laws. I don't take any responsibility for what you do with it.

What is it?

Evazor is a pocket size network recon device Once connected to a network over WiFi it will infiltrate to find out as much as possible about the devices.

It implements passive and active scanning scenarios including ARP Poisoning, Portscan, MITM Http User Agent sniffing, DHCP, MDNS and more to come.

All you need to do is plug it in and leave working while you can easily check it’s status by connecting to it’s Access Point and reviewing status page or downloading logs from it’s operations.

Once configured your Evazor will remember the settings and every-time you power it on it will know what to do, no need to reconfigure it after the power is lost.

Start

Start with mounting the antenna to the Evazor, be gentle, this is 3D Printed - don't break it ! When the antenna is in place, plug in a 5v MicroUSB cable and power it on.

Evazor will start blinking blue with it's built in led.

Look for "Evazor" WiFi Access Point and connect to it.

Once connected head to http://192.168.4.1/setup

and use default credentials (you can change them later):

Username: **razor**
Password: **admin**

Next you will be presented with Evazor's status and configuration page.

Evazor will stay in setup mode until you hit ‘start’ after choosing the target.

```
This is Evazor xxxxxxxxxx version 0.1
(c) Razor 202I - hack the planet

Device ID..: xxxxxxxxxx < your device unique ID
ChipID.....: 7161882
Free Space.: 2858.56/100 KB < free space on flash
Free Mem...: 23904/11000 KB < free heap memory
Life Ticker: 14
Version....: [0.1] < upgrade firmware
Reboot.....: [now] < reboot device
Reset......: [now] < reset all configs
Key........: [your_evazor_unique_key] < Never loose it
Web Passwd.: [_admin] < web panel password
My hostname: [_Evazor] < change the hostname of the device here
My SSID....: [_EVAZOR] < change the AP SSID of Evazor here
My Password: [_] < change the password to AP of Evazor
My STA MAC.: [_a4:b7:eb:d3:81:ed] < generate random STA Mac of evazor

[TARGET]--------------------------------------
Network.....: [select] < select the network to connect to
Network Pass: [set] < provide target network WiFi Password
Start.......: [start] < hit start once all configured properly

[LOGS]----------------------------------------
Review logfiles: [here] < see log files of the scans

[OPTIONS]-------------------------------------

Ping...........: [yes] < active ping scan
Portscan.......: [yes] < active port scan
ARP Poisoning..: [no] < mitm

[STATUS]--------------------------------------
Target.........: Disconnected < status of the target
Reconnections..: 0 < how many reconnections
Channel........: 1 < which channel evazor is operating on
Devices........: 0 < number of devices discovered
```

Quick Start

1. Start by providing a proper Key, otherwise Evazor will not start.

If you don't have your Key, contact me on Tindie - provide Order ID and Date of order.

```
Key........: [your_evazor_unique_key] < Never loose it
```

2. Change the Evazor AP name and setup AP password - so it's not public and open to everybody. This will be the AP you will connect to after leaving config mode.

```
My SSID....: [_EVAZOR] < change the AP SSID of Evazor here
My Password: [_] < change the password to AP of Evazor
```

3. Select target network

```
[TARGET]--------------------------------------
Network.....: [select] < click here
```

You will be shown results of the WiFi scan, choose the AP from the list - take into consideration their colors, which represent the RSSI (signal strength) to the Access Point.

```
Select      SSID  BSSID Channel     RSSI  Encryption  Chance
select      RAZOR EE:AA:BB:CC:DD:EE      -53   WPA2 / PSK  94%
```

Click "select" and provide a password to the selected network here:

```
[TARGET]--------------------------------------
Network.....: [RAZOR/EE:AA:BB:CC:DD:EE] [clear]
Network Pass: [set] < set target network WiFi Password
```

4. Once the network is selected go to options to enable scanning scenarios.I have enabled all active scenarios. This can be noisy but since I am connecting to my network, I can live with it ;)

```
[OPTIONS]-------------------------------------

Ping...........: [yes]
Portscan.......: [yes]
ARP Poisoning..: [yes]
```

5. Now it’s time to start, click here and Evazor will kick off providing basic details on your target network.

```
Start.......: [start]


Ready to roll
Target Selected: RAZOR
Target Password: hewehewehge

Disabling Setup mode, going to attack.
- Reconnect to: Internet from now on to connect to Evazor or
- Reboot to go back to setup again
```

After you start Evazor will drop it’s Config AP Name “EVAZOR” and (if configured) will change the name and enable encryption. Reconnect at any point in time to get the output of the scan, or restart it to enter setup mode again and download log files.

Recon Results

You can access results while Evazor is performing a scan - by connecting to the device and looking at the stats page:

```
[STATUS]--------------------------------------
Target.........: Connected <- connection status
RSSI...........: -35 (100%) <- RSSI
IP.............: 192.168.218.109 <- evazor IP
Netmask........: 255.255.255.0 <- netmask
DNS............: 192.168.0.1 <- dns ip
Gateway........: 192.168.218.1 <- gateway ip
Hostname.......: Router <- evazor hostname
Reconnections..: 2 <- how many reconnections
Channel........: 11 <- operating channel
Devices........: 32 <- Click here for recon results
```

Let's enter the recon results by clicking on “Devices 32”.

```
[01:02:03:04:05:06]
Interface...: 4
Hostname....:
MAC.........: 01:02:03:04:05:06
IP..........: 192.168.0.13
User Agent..:
MDNS........: 1
| _http
Open Ports..: 1 [rescan] <- hit here if you want to do portscan
again for this host

| 22 (SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.1 )
```

Neat, this device is having SSH version 2.0, let’s look more:

```
[02:03:04:05:06:07]
Interface...: 4
Hostname....:
MAC.........: 02:03:04:05:06:07
IP..........: 192.168.218.129
User Agent..:
MDNS........: 7
| 129
| HP DeskJet 3700 series [5C3644]
| _http
| _pdl-datastream
| _scanner
| _services
| _wfds-print
Open Ports..: 2 [rescan]
| 80 ()
| 443 ()
```

This guy is a printer, we can even spot the model from MDNS but also see 80 and 443 are open.

```
[AA:BB:CC:DD:EE:FF]
Interface...: 4
Hostname....:
MAC.........: AA:BB:CC:DD:EE:FF
IP..........: 192.168.218.71
User Agent..:
MDNS........: 3
| HIKVISION&CS-CV310-A0-1C2WFR&E31589019&ALARMREPORT
| _services
| _smart
Open Ports..: 0 [rescan]
```

HikVision IP Camera!

```
[ZZ:XX:CC:VV:BB:NN]
Interface...: 3
Hostname....:
MAC.........: ZZ:XX:CC:VV:BB:NN
IP..........: 10.0.1.3
User Agent..:
MDNS........: 0
Open Ports..: 3
            | 22 (SSH-2.0-dropbear_2011.54)
            | 80 ()
            | 443 ()
```

Another one on the network with few ports open, SSH running 2.0 - dropbear.

With ARP Poisoning we were able to track some User Agents too, check this out:

```
[EE:FF:GG:AA:BB:CC]
Interface...: 3
Hostname....: LaptopHAPEX
MAC.........: EE:FF:GG:AA:BB:CCF
IP..........: 192.168.4.3
User Agent..: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:89.0)
Gecko/20100101 Firefox/89.0
MDNS........: 2
| 0
| 192-168-4-3
Open Ports..: 0 [rescan]
```

Info

1. Due to very limited heap memory, Evazor will find out as many devices as it's memory allows for then stop. (Led will be on to mark memory limit). On many of my networks i was able to find out up to 50 devices - that's a lot!
   Once mem limit is hit, setup page will note that by marking red:

   Free Space.: 2852.67/100 KB
   Free Mem...: 7064/11000 KB

2. New s/w versions will be provided on Tindie product page
3. If you don't have the key, please contact me via Tindie page and provide:
   - Order ID
   - Order Date
4. Following ports are enabled by default for port scanning:
   21,22,23,139,80,443,25
   With future releases, you will be able to modify these.