

ATTRACTHOR

Thank You for buying AttracThor, 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.

1.65

What is it ?

AttracThor is a tiny device that can help you check if your Home WiFi network is vulnerable for Evil Twin Attacks. It's small size helps to deploy the attack in just a few seconds with no additional overwhelming hassle of configuring operating systems and additional hardware.

Thanks to the 5V MicroUSB power supply it can be powered with pretty much everything, starting from Power Banks, through Solar panels, USB from your laptop or with a small modification with a dedicated battery shield.

Instead of spending time on setting up your dedicated operating system image, configure the automated pen-testing attack on your network, just take one (or more) AttracThors, plug in and start investigating.

Once configured your AttracThor 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 loss.

So how does it work?

First: Evil Twin

*"An **evil twin** is a fraudulent [Wi-Fi](#) access point that appears to be legitimate but is set up to eavesdrop on wireless communications..."*

*"This type of attack may be used to **steal the passwords** of unsuspecting users, either by monitoring their connections or by **phishing**, which involves setting up a fraudulent web site and luring people there."*

Second: Deauth attack

"The attacker conducts a deauthentication attack to the target client, disconnecting it from its current network, thus allowing the client to automatically connect to the Evil twin access point."

This is exactly what AttractThor does - and can help you understand if your WiFi users are vulnerable for this attack.

Now that we know what above are, let's have a quick look into the process of how AttracThor works to capture WiFi Credentials of target Access Point.

1. You first select the target
2. Then you enable options and you're done.
3. Once configured, it will periodically check for clients connected to target access point by sniffing the wireless data around looking after the traffic through selected AP.

This is scheduled every minute but if we have a user already connected to AttracThor - we don't want to disturb him, so we skip looking for STA's (clients connected to target AP).

4. Additionally we host a new access point, the same channel and the same name as the one we're attacking - the only difference is that we disable encryption - opening our access point to everyone.
5. We also have a web server running hosting Captive web page - which you can customise to fit your needs and be more convincing to your victims.
6. We also have our DNS server started so that all domain names are resolved and pointing to our AttracThor. When he types `www.google.com` in the browser - it transfers him to our Captive web page.
7. Now, when we have a list of STA's (clients connected to target AP) we know who can we target for deauth attack. Thanks to this part clients that are on the list start to have massive difficulties using internet, AttracThor will flood them with DEAUTH packets sourcing from target AP and devices will break their connections to the Access

Point we're attacking.

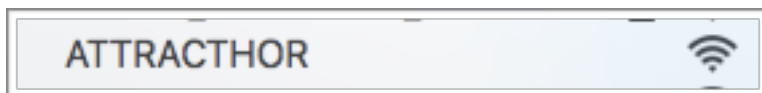
In the end we get these clients disconnected from their legit Access Point.

8. When the victim gets dropped from his Access Point, he will notice that immediately as the internet will stop work. His next step is go and reconnect, he clicks on the name of his Access Point - but this time it's AttracThor and he is immediately transferred to our Captive portal.
9. The captive portal tells i.e: his router has rebooted and he needs to provide a WiFi password to reconnect.
10. He puts the credentials
11. AttracThor verifies provided password by connecting to target AccessPoint and if successful, stores the provided password and shuts down OR
12. It will validate the passwords provided with every boot.

Start

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

AttracThor will start blinking blue with it's built in led. Look for "ATTRACTHOR" WiFi Access Point and connect.



After connecting, head to: <http://192.168.4.1/setup>

Default login: **razor**

Default password: **admin**

You can change this in the setup panel, but don't forget it - the only way to restore it is to flash the device with firmware.

This is the main setup page for AttracThor, let's split it into few things to help you understand what is happening.

```
This is AttracThor 40f52029a1f7 version 1.65
(c) Razor 2020 - hack the planet
```

```
Device ID..: 40f52029a1f7
ChipID.....: 2728439
Free Space.: 2879.15 KB
Version....: [1.65]
Reboot.....: [now]
Reset.....: [now]
Password...: [admin]
```

This is AttracThor 40f52029d061 version 1.65

A simple header telling you the version and ID of the device.

```
Device ID..: 40f52029d061
ChipID.....: 2740321
Free Space.: 2878.66 KB
Version....: [1.6]
Reboot.....: [now]
Reset.....: [now]
```

Basic device operation, you can **Upgrade**, **Reboot** or **Reset** to defaults.

Remember doing upgrades over WiFi will require strong stable signal.

Target section allows you to select the Target AP you want to attack, but also upload Captive web page you want to display through newly introduced File Manager.

```
[TARGET]-----  
Captive.....: [preview] /captive.htm  
File Manager: [open]  
Network.....: [select]
```

AttracThor comes with a default Captive Web Page, feel free to **preview** if needed or **upload** if you want your own page.

With the version 1.65 a File Manager was added to make it easier for you to upload more than one page and **set** the one you want to display when users connect.

Here is an example of my captive page files:

```
Free Space.: 2865.67 KB  
Go back.....: now  
Upload.....: now
```

```
[FILES]-----  
- [Delete] [Set] /test.html  
- [Delete] [Set] /zebra.png
```

Click on the file manager **open** to start uploading web pages, remember about the very limited size of the internal File System!

Click **set** to use selected file as the one served for Captive portal.

Once ready with Captive page, **select** a target now.

You should be presented with a list of AP around.

Select	SSID	BSSID	Channel	RSSI	Encryption	Chance
select	AAAA	aaa	1	-69	OPEN	62%
select	BBBB	bbb	1	-78	WPA / WPA2 / PSK	44%
select	CCCC	ccc	5	-74	WPA2 / PSK	52%
select	RAZOR_LAB	ddd	6	-62	WPA2 / PSK	76%
select	EEEE	eee	6	-25	WPA / WPA2 / PSK	100%
select	FFFF	fff	7	-90	WPA2 / PSK	20%
select	GGGG	ggg	7	-89	WPA2 / PSK	22%
select	HHHH	hhh	7	-85	WPA / WPA2 / PSK	30%
select	IIII	iii	9	-66	WPA2 / PSK	68%
select	JJJJ	jjj	10	-91	WPA / WPA2 / PSK	18%
select	KKKK	kkk	11	-78	WPA / WPA2 / PSK	44%

Pay attention to the **Chance** column. It's a calc of the RSSI. The less chance % your target has, the distant it is. In WiFi the range is very very important.

As with every WiFi attack, the range and signal strength is top on the list of important things to consider, so the chance is calculated on the RSSI levels. Definitely look more after the yellow / green ones than the red ones.

Select your target, i'll choose RAZOR_LAB - my lab. Once selected, you will be redirected to main page.

```
[TARGET]-----  
Captive.....: [upload] [preview]  
Network...: [RAZOR_LAB/aa:bb:cc:dd:ee:ff]
```

This is how the Target section will look like after me selecting the victim AP. Again, pay attention to Captive web page.

Captive Web page is very important. Treat it seriously, when your users connect to AttracThor, this is what will be presented to them. The more friendly it is to their current setup (router their using i.e) the more convincing it is for them to provide You password. AttracThor comes with the default Captive Web Page.

There are two variables you can use on the Captive page:

%SSID% - will provide target access point 'name'

%BSSID% - will provide target access point mac address.

Follow below form example to pass the user input for processing:

```
<form action='/userinput' method='get'>  
<input type='password' name='password' minlength='5' required  
autofocus>  
<input type=submit value='Log in'>  
</form>
```


[OPTIONS]-----

Deauth Attack...: [no]
Beacon Mist.....: [no]
Broadcast.....: [no]
HearbeatBlink...: [no]
InputValidation: [no]
BootValidation.: [no]
AutoReboot.....: [no]

Once your target is selected you can start working on enabling options. In default, all are set to NO.

Deauth Attack...: [no] - Enable deauthentication attack, which will cause target STA's to drop connection forcing them to reconnect. You don't have to spend cycles with Atthor on DEAUTHing, switch this off if you want to have a dedicated deauther like Repeller.

Beacon Mist.....: [no] - Enable beacon flood, so users have our EvilTwin flooding their WiFi survey list.

Broadcast.....: [no] - Enable status broadcasting to AttracThor sister software

HearbeatBlink...: [no] - Blink every 10 seconds

InputValidation: [no] - Once user provides Password, enable immediate validation by connecting to targetted network and checking if password is valid.

BootValidation.: [no] - Enable validation of all passwords provided on every reboot of the device.

Both validation options require a proper signal strength to target AP. The more far you are (less signal strength) the longer it takes to validate the passwords. Default is: 15 seconds to validate password.

AutoReboot.....: [no] - Auto reboot every 24hrs (comes handy with BootValidation option enabled). Clears stats.

[STATUS]------
RSSI.....: 0
Channel.....: 0
Data packets...: 0
STA Known.....: 0
DNS Queries....: 0
Clients seen...: 0
Passwords.....: 0

Here things are simple.

RSSI - is the last known RSSI to the target AP.

Channel - channel we're currently at

Data Packets - number of data packets seen during last STA scan. The more there is, the more the network is used - briefly.

STA Known - how many STA's we've seen talking with target AP

DNS Queries - what DNS queries were made when clients connected to our ETwin

Clients Seen - List of clients seen connected to our EvilTwin

Passwords - you want more than 0 here !

Attacking

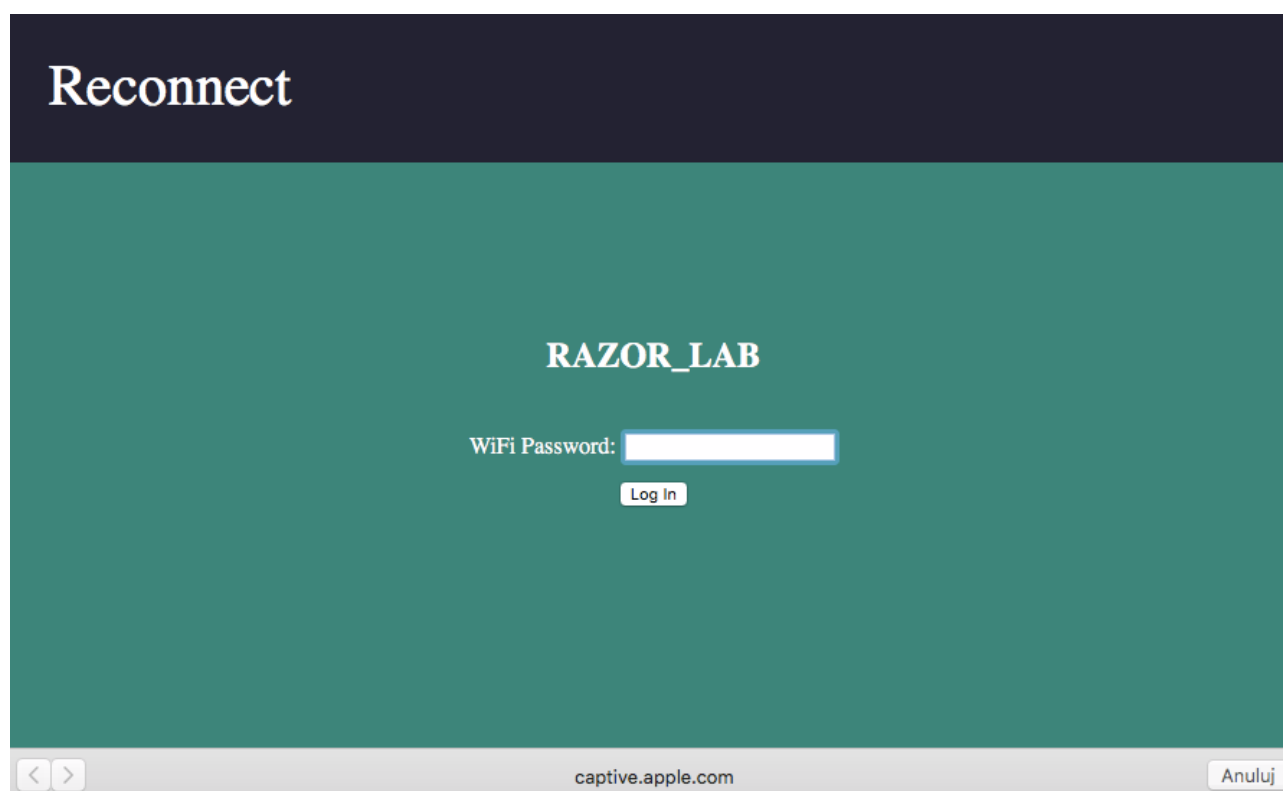
Attractor once configured will wait for 3 minutes to start attacking, or if you are connected - will wait until you drop to kick off.

After going to attack mode the selected target AP is now cloned, and you can connect to it and swipe through the status page to see what's going on, let's open it.

I selected RAZOR_LAB as my target and i can see the cloned AP with no encryption, let's connect



Boom! i get Captive portal opened.



Don't close it, open the browser and head to: <http://192.168.4.1/setup> again, to see the stats.

[OPTIONS]-----

Enable Oled....: [no]
Deauth Attack...: [yes] (Yep enabled)
Beacon Mist....: [no]
Broadcast.....: [yes] (Yep enabled)
HearbeatBlink...: [no]
InputValidation: [no]
BootValidation.: [yes] (Yep enabled)
AutoReboot.....: [no191]

[STATUS]-----

RSSI.....: -72
Channel.....: 1
Data packets...: 9
STA Known.....: [2]
DNS Queries....: [1]
Clients seen...: [1]
Passwords.....: [0] [clear all]

No passwords yet, even though we see we have connected. Click on the number to see details.

Let's check a device that is connected to lab and see if it is hit with the death attack.



Perfect, unusable internet - that's what we need.

If you are looking close you can already see no WiFi on this screenshot, network went fully down for this device.

The user decides to reconnect as his network is down, scans the WiFis in range and he clicks the RAZOR_LAB - which is a cloned copy of our legit AP.



Boom! He gets Captive portal, and he logs in.



```
[STATUS]-----  
RSSI.....: -72  
Channel.....: 1  
Data packets...: 9  
STA Known.....: [2]  
DNS Queries....: [1]  
Clients seen...: [1]  
Passwords.....: [4/1] [clear all]
```

And here we've got it on our info page. Worth noticing, that there were few wrong passwords provided we store them as any input from the user is worth storing.

```
Passwords.....: [x/y]
```

x = Total number of passwords provided

y = Total number of passwords valid

clear all = Remove all stored passwords

Once clicked on passwords, you will be presented with the following self explanatory info:

- RAZOR_G E8:XX:XX:XX:XX:XX asdfasfa
- RAZOR_G E8:XX:XX:XX:XX:XX 124124124
- RAZOR_G E8:XX:XX:XX:XX:XX PoAOo123
- RAZOR_G E8:XX:XX:XX:XX:XX Majorca2055 valid

Things to remember

AttracThor can't guarantee a successful attack every-time you use it. It is impossible. Prominent WiFi attacks depend on various of things. Some of them are technical but majority of EvilTwin attack depend on the target audience.

Few of the tips worth remembering from AttracThor perspective:

Signal Strength/Distance to the target - I can't be seen if my signal is weak. It is also known, validation of passwords take longer when signal is weak. That's how important it is to be as close as possible to the target.

Coverage - The more of 'us' are here, the better coverage we have.

Data rate - The more users are connected to target AP the more deauths i can do and the more chances there are one of them will connect to me

Captive web page - I have to be convincing when asking user to put a password

Filesystem size - it's super small, this is a micro-controller so pay attention when uploading. Do not drop BIG files, things get faster when small sizes are served.

180 Seconds - This is the time after reboot - you have to access "ATTRACTHOR" in Setup mode, when target is selected - after this time, AttracThor will switch to attack mode. This is intentional, so that when a power is lost AttracThor will continue with attack after reboot. But only if Target is selected and password is not validated. When Password is known, it will stay in setup mode non stop.

Go Advanced, let your Sister talk

Playing with AttracThor web page for stats will become unfriendly after some time. Reconnecting between AttracThors, refreshing, getting caught in your own Captive Portals, having not enough signal to connect in really remote scenarios - will just not go.

Together with AttracThor comes handy tool called Evil Twin Sister - a simple command line utility to make looking after your AttracThors easy.

With a single raspberry pi and monitor mode capable WiFi card (i.e Alfa) you can listen to your AttracThors talking to you from long distance.

First get your WiFi card into monitor mode with:

```
airmon-ng start wlan1
```

Then launch the Sister binary and let it go.

```
./atthor_sister wlan1mon
```

Recommended putting this into a screen ;-)

Sister talking

After you launch the binary, you immediately start to see your AttracThors performing.

Each and everyone one in range will broadcast encrypted packets via WiFi and you will see them coming.

All AttracThor statuses can be monitored from a single source, that's just handy.

```
BTWiFiSister by nodehastahPL 2020
Frameshift drive charging on wlan0m
Going full speed
2020/6/7 22:19:10 AttracThor 18288:4F44:f4 Awaiting setup
2020/6/7 22:19:11 AttracThor ec7:47:44:44 -74 RSSI 4 STA 0 Clients 0 Visitors 0 Passwords 44 Uptime 3 DR 80b MEM
2020/6/7 22:19:19 AttracThor 18f:47:44:44 Awaiting setup
2020/6/7 22:19:21 AttracThor 187:47:44:44 Awaiting setup
2020/6/7 22:19:27 AttracThor 1850:47:44:44 Awaiting setup
2020/6/7 22:19:33 AttracThor 187:47:44:44 Awaiting setup
2020/6/7 22:19:33 AttracThor 185:47:44:44 Awaiting setup
2020/6/7 22:19:35 AttracThor 187:47:44:44 Awaiting setup
2020/6/7 22:19:47 AttracThor 181:47:44:44 Awaiting setup
2020/6/7 22:19:51 AttracThor 84:xxyyzzwwaa TargetWIFI -76 RSSI 4 STA 0 Clients 0 Visitors 0 Passwords 8 Uptime 0 DR 8b MEM
2020/6/7 22:19:55 AttracThor 181:47:44:44 Awaiting setup
2020/6/7 22:19:59 AttracThor 187:47:44:44 Awaiting setup
2020/6/7 22:10:14 AttracThor 187:47:44:44 Awaiting setup
```

The most important message you should look at is the ones that include full details on the progress and status of your AttracThor(s).

```
2020/6/7 22:11:58 AttracThor 84xxyyzzwwaa TargetWIFI -76 RSSI 4 STA 0
Clients 0 Visitors 0 Passwords 11 Uptime 0 DR
```

Let's break this a little bit.

2020/6/7 22:11:58 AttracThor - Just a date and time the message was received

84xxyyzzwwaa - This is the MAC of AttracThor speaking

TargetWIFI - This is the Target Access Point SSID

-76 RSSI - This is the Relative Signal Strength Indicator for target AP

4 STA - This is the number of clients connected to the target AP

0 Clients - This is the number of clients connected to our AttracThor

0 Visitors - This is the number of our Captive Portal Visitors

0 Passwords - This is the number of passwords we have stored

11 Uptime - This is the uptime in minutes

0 DR - This is the 'Data Rate' of Target AP - how big is the traffic

Final words

Ok, if you got here - you should already know all to handle your AttracThor. Before we close out, few points below.

1. AttracThor is not a toy, it is created to help you check if your WiFi users are vulnerable for Evil Twin attack.

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.

2. All firmware updates and news will be shared on the Tindie product page

I am not hosting any dedicated web page for this product.

3. This is ESP8266 it has a very very limited memory, when updating Captive Portal - keep that in mind.

4. Device is a Wemos D1 Mini Pro - at any point in time, you can flash with whatever needed by just plugging a Usb cable.

5. You can use Serial Monitor to see what's happening on you AttracThor instead of using Web portal / Sister software

6. You cant contact me through the Tindie web page

7. This product is actively developed - be sure to check out the updates on Tindie

Hacking Atthor

AttracThor is based on Wemos D1 Mini Pro board. This makes it very easily expandable/customizable. There are many shields available on the market to customize AttracThor with new functionalities.

One of the best tested and well known expansion is adding the battery. There is a dedicated D1 Mini Battery Shield that you can use and move out from cables to mobile approach.

With the new upcoming releases of AttracThor version, there will be OLED support. Again, there is a dedicated OLED shield for D1 MINI. [Check]