

Test process

1. Attacker: In the first step, the attacker scans the MAC address of the target AP client. (MTK network card address)

system:Linux

```
CH 12 ][ Elapsed: 18 s ][ 2018-06-01 15:38
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
50:FA:84:6D:02:B8	-47	21	1 0	11	405	WPA2	CCMP	PSK	AAAA

BSSID	AP mac	STATION	MTK mac	PWR	Rate	Lost	Frames	Probe
50:FA:84:6D:02:B8	00:C0:CA:96:EC:F5			-41	0 - 1	0	6	

victim :The network card status at this time is normal.system: (win7)

The image shows two windows from a Windows 7 system. The left window is the Mediatek network utility, and the right window is the Windows Network Center showing wireless networks.

Mediatek Network Utility (Left Window):

- Network Name: AAAA
- Transfer Speed: 54.0 Mbps
- Channel: 11 (2462 MHz)
- IP Address: 192.168.1.102
- Subnet Mask: 255.255.255.0

Windows Network Center (Right Window):

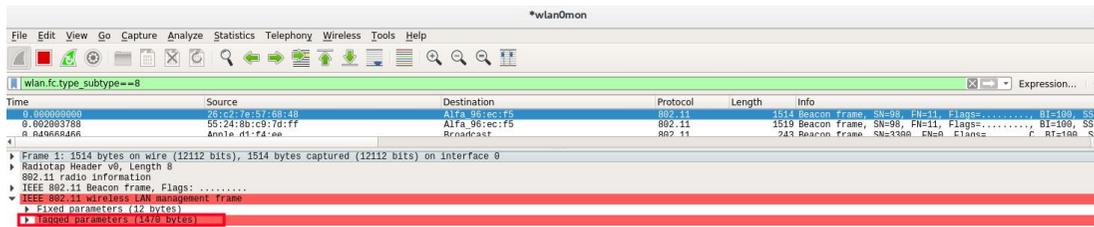
Network Name	SSID	Signal Strength	Security	Encryption	Authentication	Connection Status
12345679		6	b	g	n	100%
AAAA		11	b	g	n	100%
AD-LAB		6	b	g	n	100%
apple_iphone		6	b	g	n	100%
BEYOND		11	b	g	n	100%
ChinaNet-YdUz		3	b	g	n	78%
cosshare		11	b	g	n	73%
DIRECT-2e-HP M1...		3	g	n	n	94%
DIRECT-ec-HP M4...		11	g	n	n	68%
Network		6	b	g	n	100%
test		6	b	g	n	100%
TP-LINK_177CB4		1	b	g	n	100%
TPGuest_QianFang		1	b	g	n	57%
TstudioIP.v6		11	b	g	n	100%
U-CITY		6	b	g	n	100%

AP Information (Bottom of Right Window):

- Network Name: 12345679
- Physical Address: 38-37-8B-9B-29-3E
- Authentication Method: WPA-PSK...
- Encryption Method: AES

Attacker:Attacker sends malformed beacon frame system:(Linux)

Python xxx.py (payload)



Victim:Victims connected to the network are remotely attacked. System:(win7)

MEDIATEK

网络名称
传输速度 IP地址
频道 子网掩码

关于

版本

实用工具	5.0.9.19	日期	2015-05-06
驱动	5.1.25.0	日期	2015-11-19
SDK	1.1.18.19	日期	2015-03-14

物理地址 00-C0-CA-96-EC-F5

MEDIATEK (c) Copyright 2014, Mediatek Inc. All rights reserved.

无线网络

AAAA	11	b g o	100%
AD-LAB	6	b g o	100%
apple_iphone	6	b g o	100%
BEYOND	11	b g o	100%
DIRECT-2e-HP M1...	4	b g o	83%
DIRECT-ec-HP M4...	11	b g o	68%
DIRECT-f1-HP M27...	11	b g o	57%
Network	6	b g o	100%
NJTSP-2.4	11	b g o	47%
test	6	b g o	100%
TP-LINK_177CB4	1	b g o	100%
TStudio-PC	3	b g o a c	100%
U-CITY	6	b g o	100%
U-CITY	6	b g o	99%
U-CITY	1	b g o	73%

AP信息

网络名称	test	验证方法	WPA2-PSK
物理地址	38-37-8B-9B-29-3C	加密方法	AES

```

C:\windows\system32\cmd.exe
180.97.33.108 的回复: 字节=32 时间=43ms TTL=54
180.97.33.108 的回复: 字节=32 时间=143ms TTL=54
180.97.33.108 的回复: 字节=32 时间=151ms TTL=54
180.97.33.108 的回复: 字节=32 时间=52ms TTL=54
180.97.33.108 的回复: 字节=32 时间=175ms TTL=54
180.97.33.108 的回复: 字节=32 时间=416ms TTL=54
180.97.33.108 的回复: 字节=32 时间=1229ms TTL=54
180.97.33.108 的回复: 字节=32 时间=112ms TTL=54
180.97.33.108 的回复: 字节=32 时间=107ms TTL=54
180.97.33.108 的回复: 字节=32 时间=27ms TTL=54
180.97.33.108 的回复: 字节=32 时间=920ms TTL=54
180.97.33.108 的回复: 字节=32 时间=40ms TTL=54
180.97.33.108 的回复: 字节=32 时间=4ms TTL=54
180.97.33.108 的回复: 字节=32 时间=258ms TTL=54
180.97.33.108 的回复: 字节=32 时间=19ms TTL=54
180.97.33.108 的回复: 字节=32 时间=17ms TTL=54
180.97.33.108 的回复: 字节=32 时间=129ms TTL=54
180.97.33.108 的回复: 字节=32 时间=77ms TTL=54
180.97.33.108 的回复: 字节=32 时间=85ms TTL=54
180.97.33.108 的回复: 字节=32 时间=41ms TTL=54
请求超时。
180.97.33.108 的回复: 字节=32 时间=265ms TTL=54
180.97.33.108 的回复: 字节=32 时间=167ms TTL=54
请求超时。
请求超时。
请求超时。
请求超时。
请求超时。
请求超时。
请求超时。

```



The victim will be attacked as long as he can receive the malformed beacon frame!

