
Cyber Attack in IoT on the rise

- Observing attacks in IoT using IoT POT -

Koji Nakao

Distinguished Researcher – NICT

Guest Professor – Yokohama National University

Adviser – KDDI

2017/1/24

Thingbots: The Future of Botnets in the Internet of Things

February 20, 2016 | By Paul Sabanal



The Internet of Things (IoT) is upon us. Everything from home appliances, watches, even children's toys are being connected online. It is projected that by the year 2020, there will be more than 25 billion devices



IoT Home Routers Botnet Leveraged in Large DDoS Attack

f t i SucuriSecurity | sucuri.net

Home Router Botnet Leveraged in Large DDoS Attack

Cyber attacks in IoT on the rise

Is your refrigerator ready to be part of a massive spam-sending botnet?

Ars unravels the report that hackers have commandeered 100,000 smart devices

by Dan Goodin - Jan 18, 2014 5:25am JST



Internet of Things security concerns boost in IoT services

by

News roundup: As Internet of Things concerns

RISK ASSESSMENT / SECURITY & HACKTIVISM

rise reality, one vendor is quick to combat the risks. Plus: 1% of users are at risk; Target pays up; Apple devices are the most secure in the enterprise.

“Internet of Things” is the new Windows XP —malware’s favorite target

Devices attacked our honeypot during Jan-June 2016

600,000+ IPs

500+ device types

†inferred by telnet and web responses



Categories of Inferred Infected devices (2016.9)

- Surveillance camera

- IP camera
- DVR



- Network devices

- Router, Gateway
- Modem, bridges
- WIFI routers
- Network mobile storage
- Security appliances



- Telephone

- VoIP Gateways
- IP Phone
- GSM Routers
- Analog phone adapters



- Infrastructures

- Parking management system
- LED display controller



Devices are inferred by telnet/web banners

- Control system

- Solid state recorder
- Sensors
- Building control system (bacnet)



- Home/individuals

- Web cam, Video recorders
- Home automation GW
- Solar Energy Control System
- Energy demand monitoring system



- Broadcasting

- Media broadcasting
- Digital voice recorder
- Video codec
- Set-top-box,



- Etc

- Heat pump
- Fire alert system
- Medical device (MRI)
- Fingerprint scanner



ROUTE CAUSES OF THE MASS- INFECTION

Telnet

Telnet

From Wikipedia, the free encyclopedia

Not to be confused with [Telenet](#).



This article **needs additional citations for [verification](#)**. Please help [improve this article](#) by [adding citations to reliable sources](#). Unsourced material may be challenged and removed.

(April 2014) ([Learn how and when to remove this template message](#))

Telnet is an [application layer](#) protocol used on the [Internet](#) or [local area networks](#) to provide a bidirectional interactive text-oriented communication facility using a virtual [terminal](#) connection. User data is interspersed [in-band](#) with Telnet control information in an 8-bit [byte oriented](#) data connection over the [Transmission Control Protocol](#) (TCP).

Telnet was developed in 1969 beginning with [RFC 15](#)^{[[↗](#)]}, extended in [RFC 854](#)^{[[↗](#)]}, and standardized as [Internet Engineering Task Force](#) (IETF) Internet Standard [STD 8](#), one of the first Internet standards.

Historically, Telnet provided access to a [command-line interface](#) (usually, of an [operating system](#)) on a remote host, including most network equipment and [operating systems](#) with a configuration utility (including systems based on [Windows NT](#)).^{[[clarification needed](#)]}

However, because of serious security concerns when using Telnet over an open network such as the Internet, its use for this purpose has waned significantly in favor of [SSH](#).

They are everywhere in Internet

B[redacted]5328 Broadband Router

ope[redacted]i.3.0.dm800se

Net[redacted]r login:

TL-[redacted]40N login:

[redacted]20-VoIP-AG login:

BC[redacted]328 xDSL Router

B[redacted]5328 ADSL Router

Router [redacted] User Access Verification

[redacted]800se.login:

[redacted]dvs.login:

adv[redacted]s login:

[redacted]vision login:

[redacted]x00 login:

Air[redacted]v2 login:

ope[redacted]4 et4x00

With default/weak id and password

```
[shogo@www9058up ~]$ telnet x.x.243.13
Trying x.x.243.13...
Connected to x.x.243.13.
Escape character is '^]'.

```

```

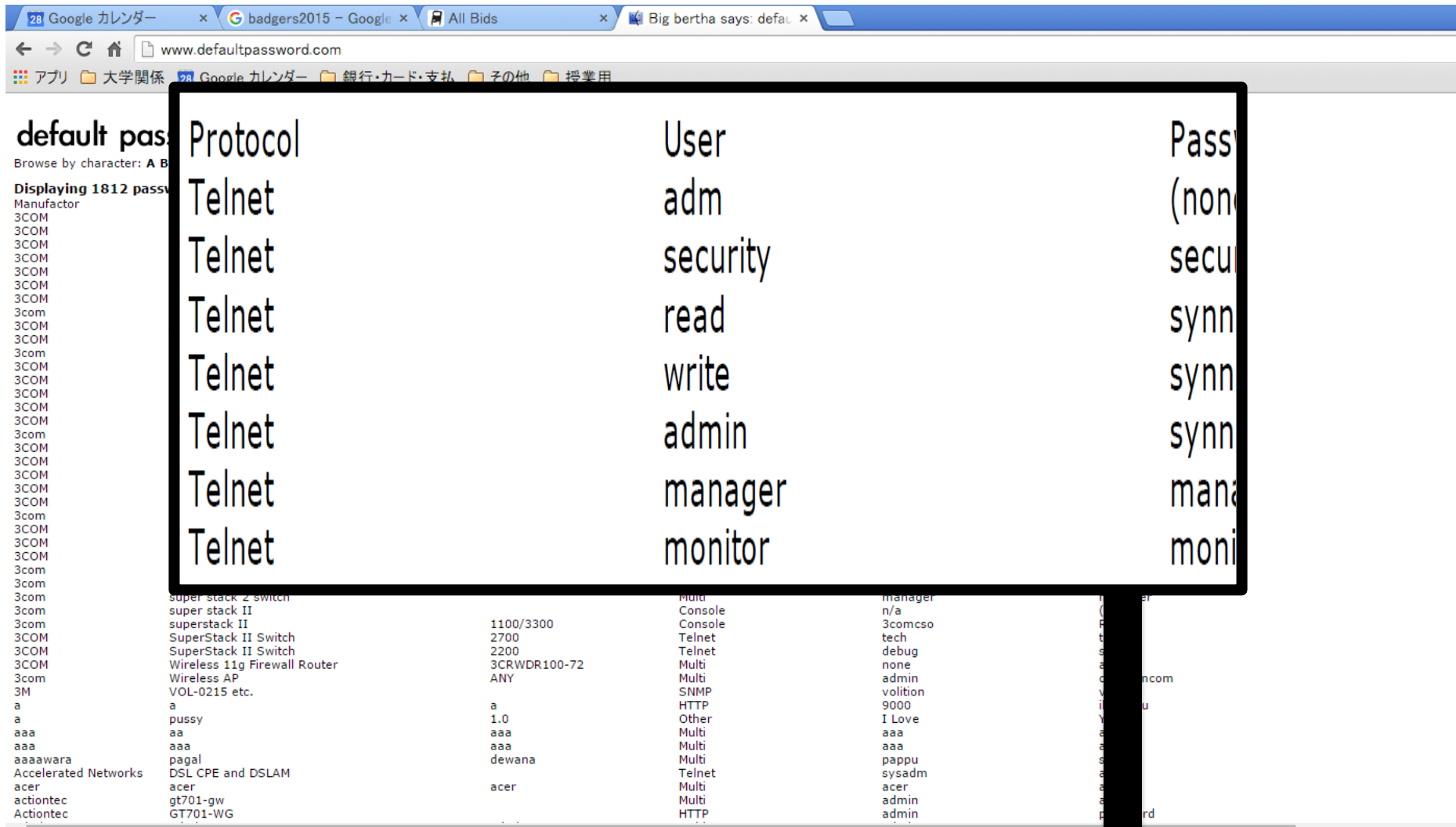
i.3.0.dm800s
e.login: root
Password: 12345

```

```
BusyBox v1.1.2 (2007.05.09-01:19+0000) Built-
in shell (ash)
Enter 'help' for a list of built-in commands.

```


Search for “default” “password” “list”



28 Google カレンダー x badgers2015 - Google x All Bids x Big bertha says: defau x

www.defaultpassword.com

default pas
Browse by character: A B
Displaying 1812 passw
Manufacturer

Manufacturer	Model	Protocol	User	Password
3COM		Telnet	adm	(non
3COM		Telnet	security	secu
3COM		Telnet	read	synn
3COM		Telnet	write	synn
3COM		Telnet	admin	synn
3COM		Telnet	manager	mana
3COM		Telnet	monitor	moni
Super stack 2 switch		Multi	manager	
super stack II		Console	n/a	
superstack II	1100/3300	Console	3comcso	
SuperStack II Switch	2700	Telnet	tech	
SuperStack II Switch	2200	Telnet	debug	
Wireless 11g Firewall Router	3CRWDR100-72	Multi	none	
Wireless AP	ANY	Multi	admin	incom
VOL-0215 etc.		SNMP	volition	
a	a	HTTP	9000	
pussy	1.0	Other	I Love	
aaa	aaa	Multi	aaa	
aaa	aaa	Multi	aaa	
aaaawara		Multi	pappu	
Accelerated Networks		Telnet	sysadm	
acer		Multi	acer	
actiontec	acer	Multi	admin	
Actiontec	gt701-gw	Multi	admin	
	GT701-WG	HTTP	admin	rd

Devices attacked our honeypot during Jan-June 2016

Those devices attacked us also run telnet and we believe it is via which they got infected

Two approaches to monitor attacks

- **Passive monitoring**

Prepare network to monitor attacks and wait

- Darknet monitoring
- Honeypot

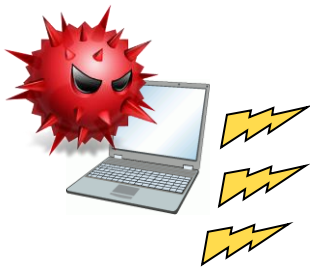
- **Active monitoring**

Search for device/vulnerability/backdoors

- Accessing Web, Telnet, FTP, etc to decide what devices they are
- Checking for backdoor ports
- Measuring clock skew for tracing individual devices

Darknet monitoring

Darknet: unused but routable IP address (es) or net blocks

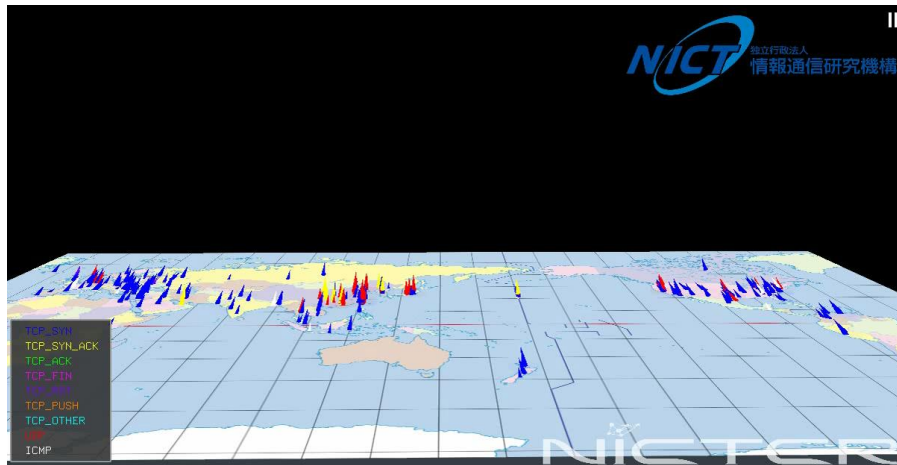


Many researchers/organization utilize darknet to monitor malicious activities like scanning, remote exploits, back scatters, etc

Scanning observation by nicter-Atlas

Recently, “scanning to Port 23 (telenet)” is getting larger!!

- Capturing packets through dark-net in real time basis.
- Color indicates the protocol types.



Atlas All view



Atlas only port23

Increases of telnet attacks

packets

7 TCP 宛先ポート別パケット数 Top 10

宛先ポート	パケット数	割合
23	2,699,639	45%
22	461,738	8%
80	348,077	6%
1433	208,460	3%
3306	199,372	3%
3389	151,868	3%
8080	145,657	2%
443	124,800	2%
9200	116,255	2%
25	94,901	2%

TCP 宛先ポート別パケット数 Top 10

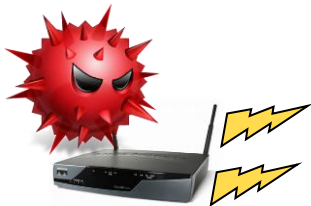
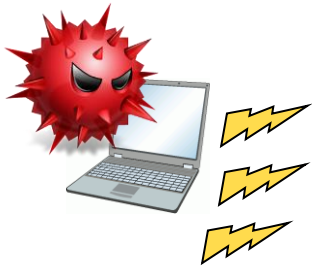
宛先ポート	パケット数	割合
23	11,727,894	65%
1433	791,485	4%
22	559,059	3%
3389	247,547	1%
80	247,159	1%
8080	184,132	1%
443	147,434	1%
3306	128,382	1%
4028	116,029	1%
54628	78,378	0%

1/1/2005 1/1/2006 1/1/2007 1/1/2008 1/1/2009

10 years observation of NICTER darknet (23/tcp only)

To monitor in depth

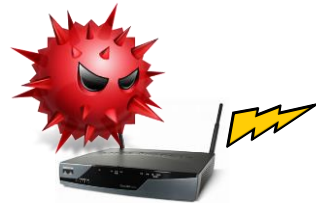
Darknet monitoring is simple and great to monitor wider networks but limited as it only gets the first packet of each attack.



Our system: IoT POT = IoT Honey Pot

We use decoy system (honeypot) to emulate vulnerable IoT devices to monitor the attacks in depth

Infected devices



Attacker's C2



Capture malware

IoT POT

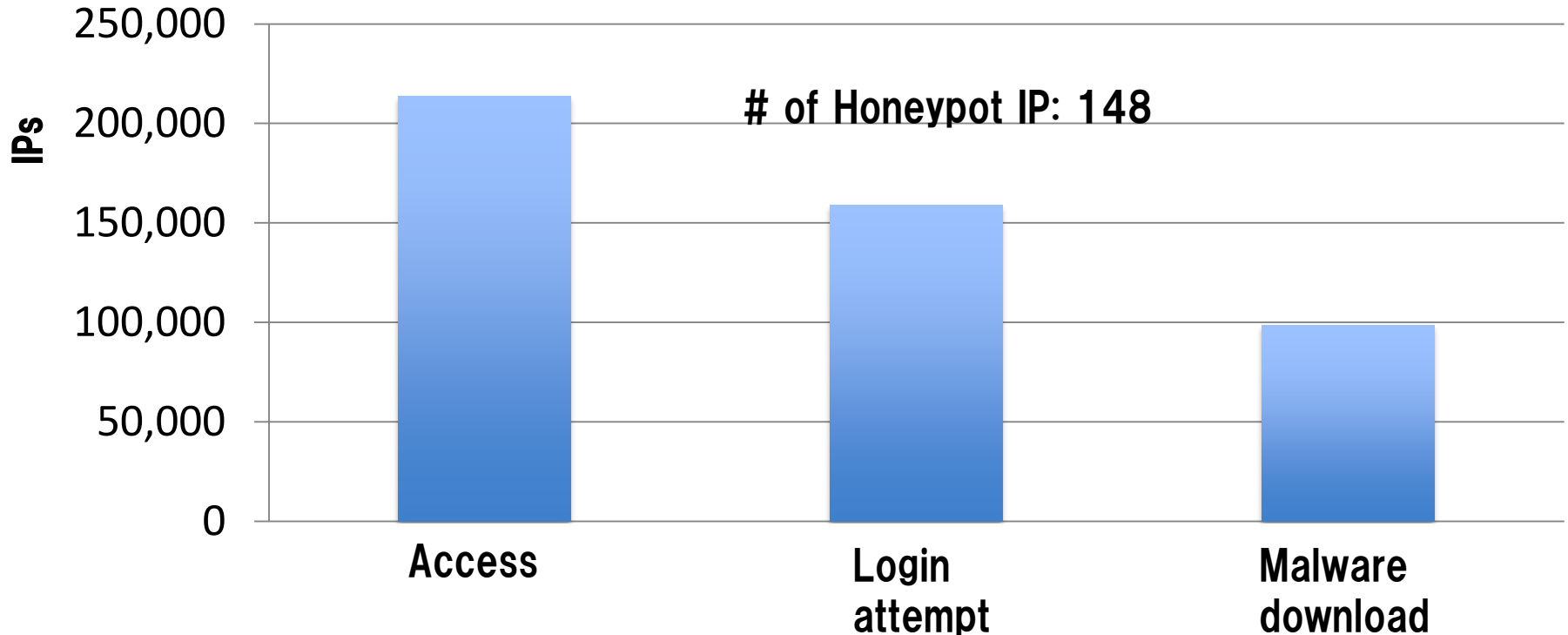


Sandbox

Analyze in depth

Observation result (last year)

Period: 2015/4/1 ~ 2015/7/31 (122days)



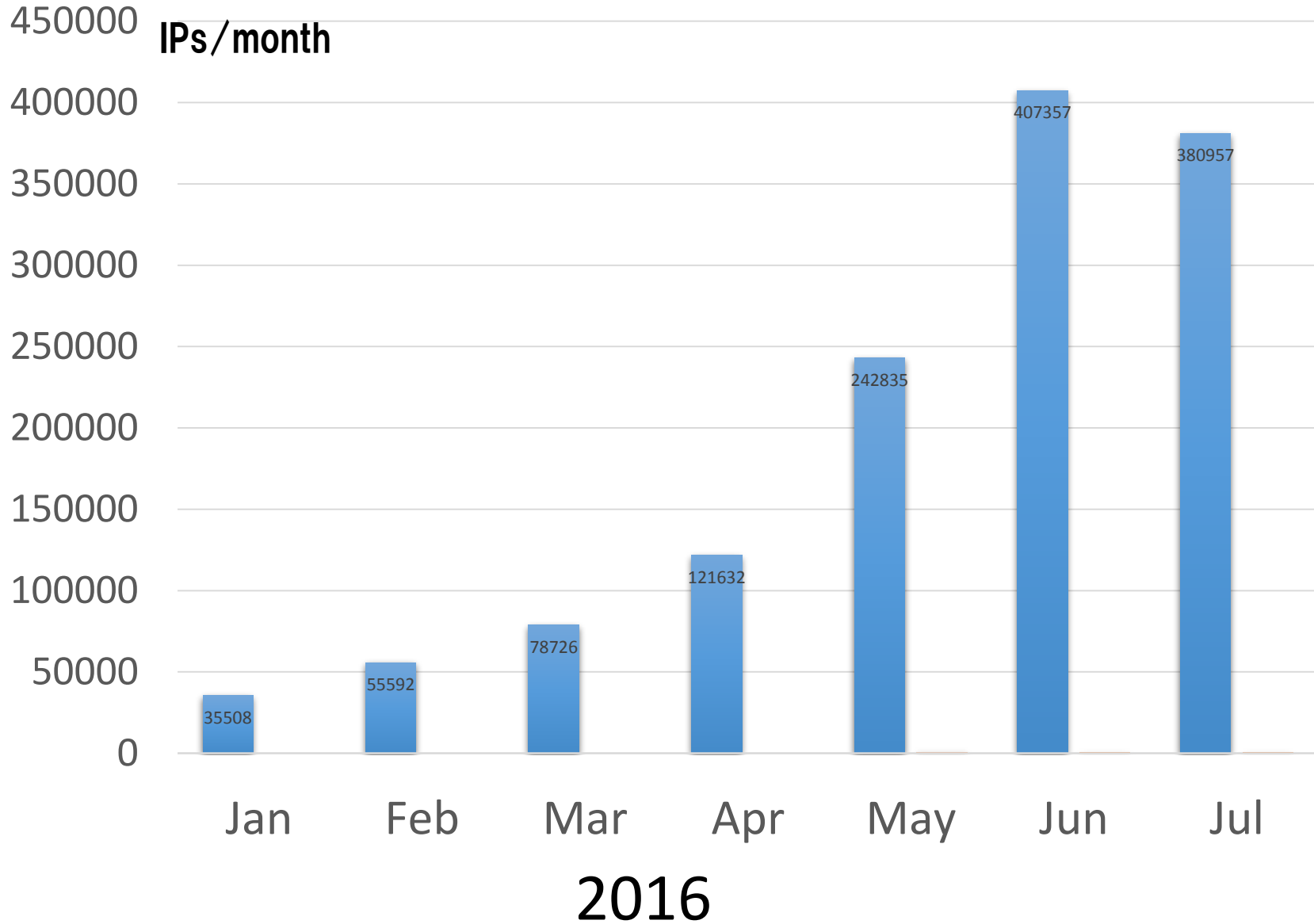
150,000 IPs attempted to login, 100,000 actually did send us malware binaries

Binaries with 11 different CPU architectures

93% of the binaries were new in VT (as of 2015/9/24)

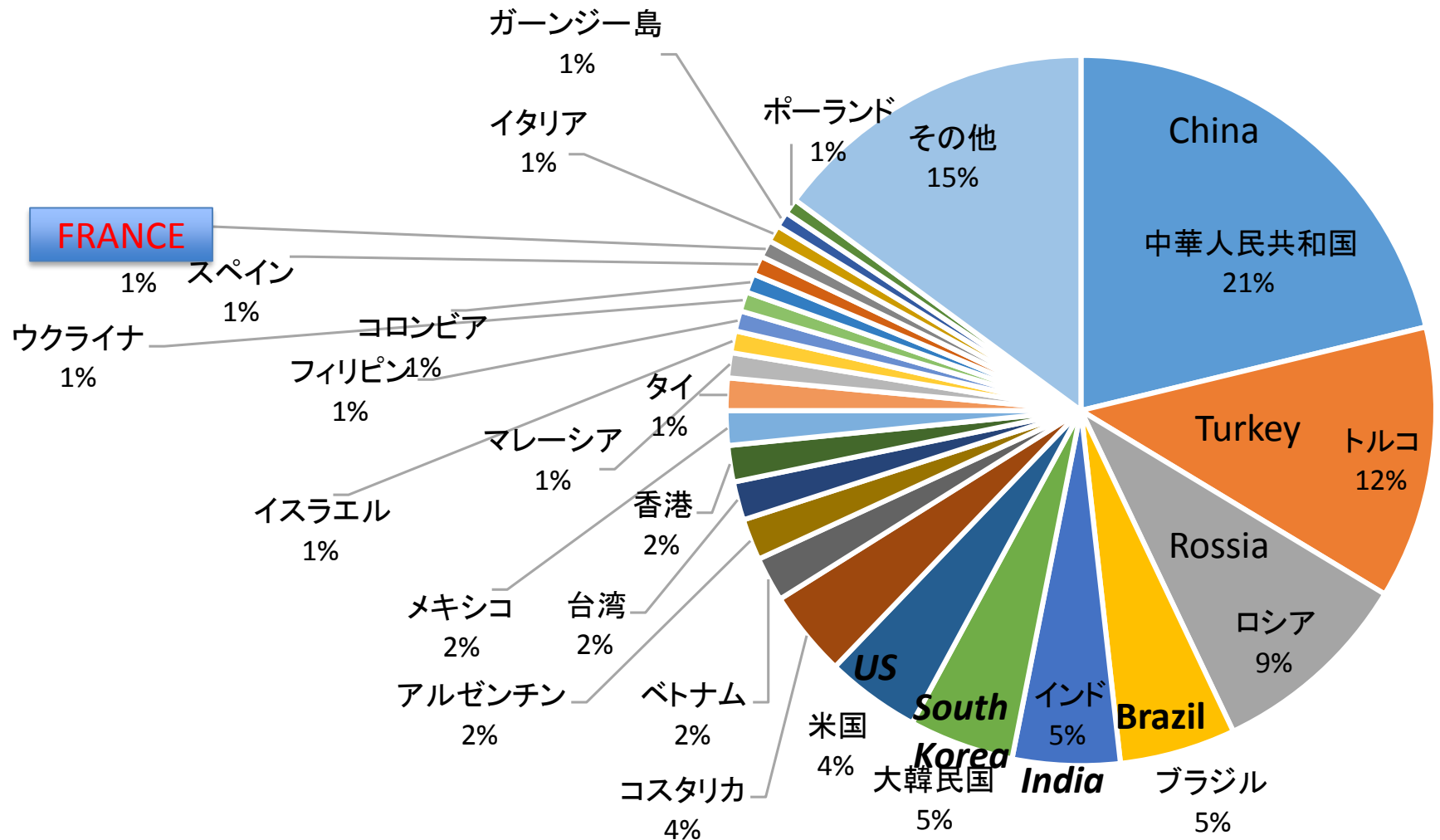
Increase of attacks

Num. of IP addresses



Source countries

Period: 2015/05/01 - 2016/02/21



ISPs

#infected devices

10

形状 (Log-Compromise Devices)

10^3

10^2

10^1

10^0

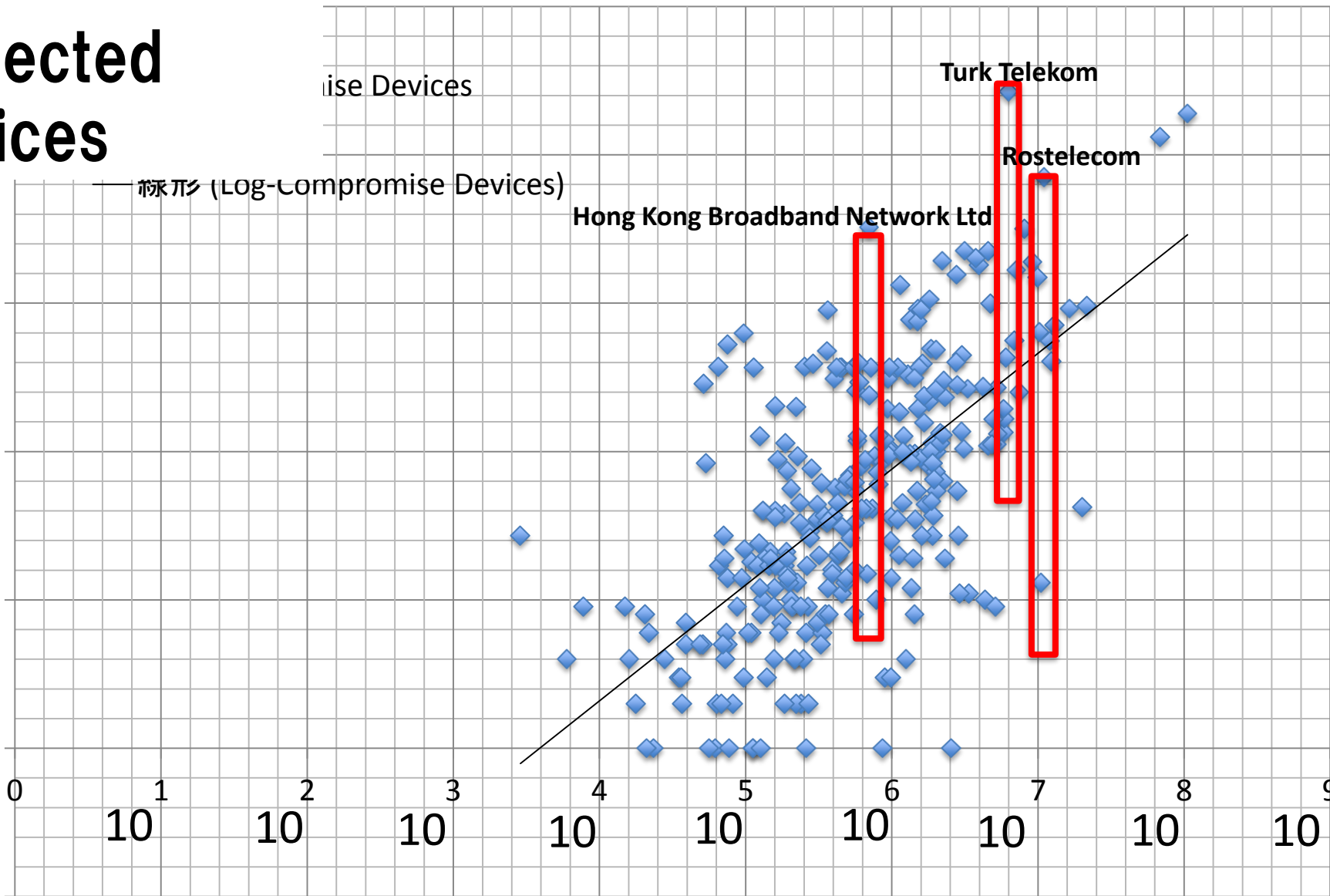
-1

ise Devices

Turk Telekom

Rostelecom

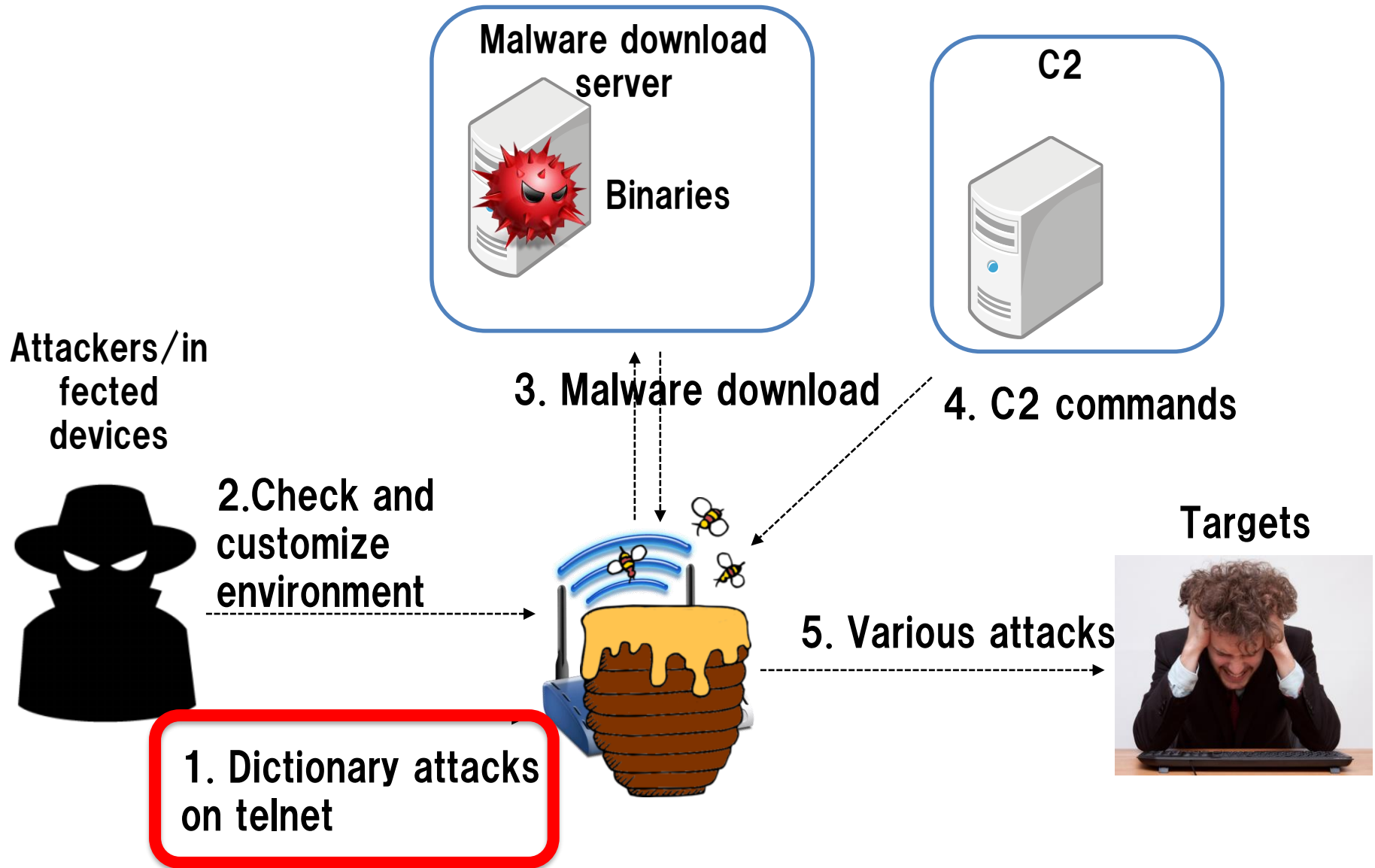
Hong Kong Broadband Network Ltd



Thanks to Prof. Michel van Eeten of TU Delft for providing ISP data

#users of ISP

Telnet-based malware infection



Dictionary used in 2015

```
root/ro[REDACTED]  
root/admin  
root/1[REDACTED]  
root/1[REDACTED]5  
root/1[REDACTED]56  
root/1[REDACTED]  
root/password  
root/d[REDACTED]mbox
```

```
root/[REDACTED]t  
root/s[REDACTED]in  
root/[REDACTED]45  
root/[REDACTED]456  
admin[REDACTED]oot  
...
```

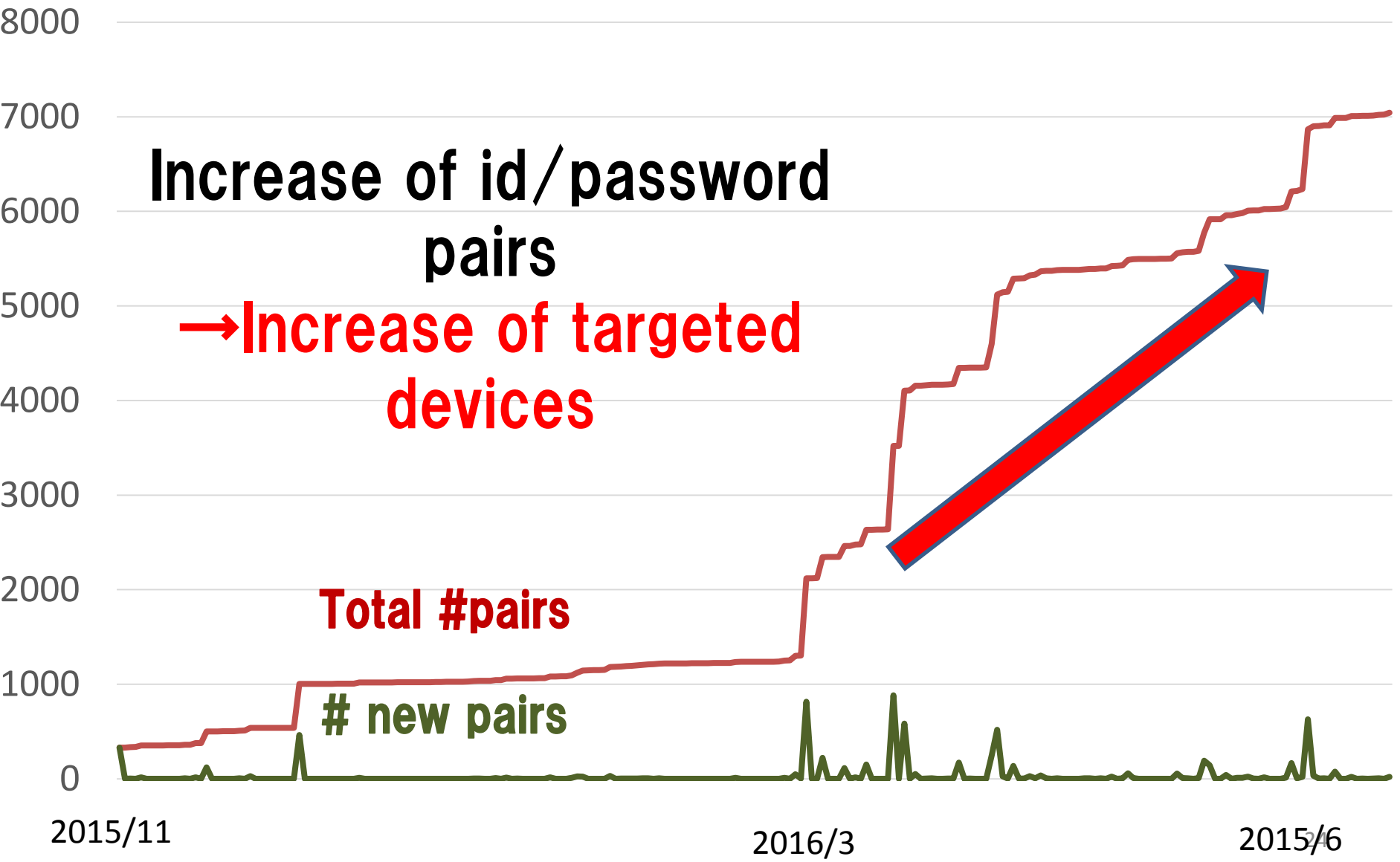
```
admin/[REDACTED]in  
admin/[REDACTED]729  
admin/[REDACTED]6h3  
admin/[REDACTED]yporra  
admin/[REDACTED]297  
admin/[REDACTED]m0r  
admin/[REDACTED]4  
root/12[REDACTED]
```

```
root/[REDACTED]511  
root/[REDACTED]456  
root/[REDACTED]45  
root/[REDACTED]t  
...
```

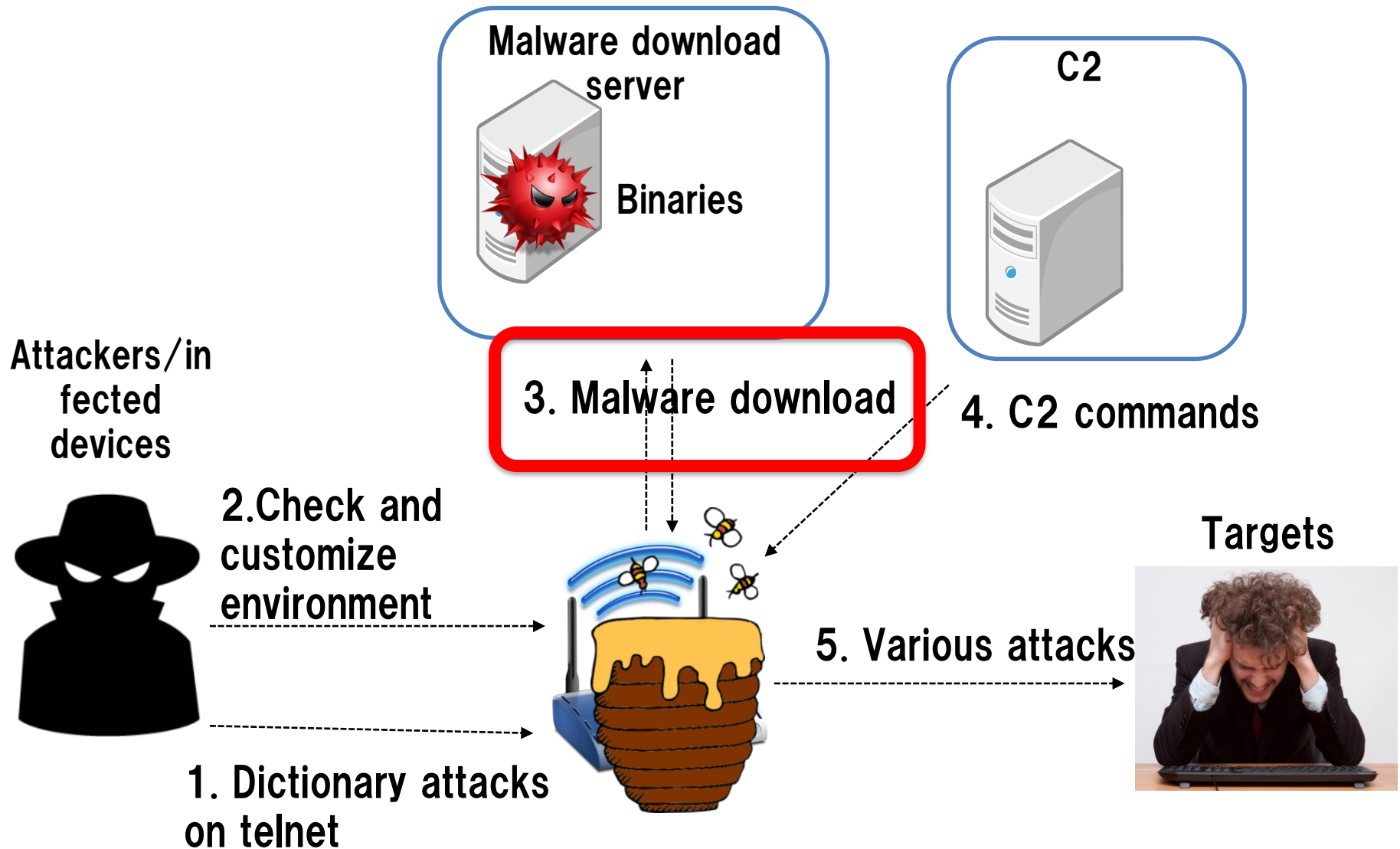
```
guest/[REDACTED]st  
guest/[REDACTED]45  
admin[REDACTED]  
root/ro[REDACTED]  
root/admin  
root/[REDACTED]  
root/1[REDACTED]  
root/1[REDACTED]56  
root/1[REDACTED]  
root/password  
root/d[REDACTED]mbox  
root/v[REDACTED]y
```

```
root/[REDACTED]t  
root/[REDACTED]r  
root/admin  
root/[REDACTED]r  
....
```

Increase of id/password pairs



Telnet-based malware infection



Eg. Malware binary downloads

```
cat m68k > busybox; rm m68k; cp busybox systemr; rm busybox; ./systemr && sleep 1
cat mips > busybox; rm mips; cp busybox systemr; rm busybox; ./systemr && sleep 1
cat mipsel > busybox; rm mipsel; cp busybox systemr; rm busybox; ./systemr && sleep 1
cat arm > busybox; rm arm; cp busybox systemr; rm busybox; ./systemr && sleep 1
cat arm7 > busybox; rm arm7; cp busybox arm7; rm busybox; ./arm7 && sleep 2
cat ppc > busybox; rm ppc; cp busybox systemr; rm busybox; ./systemr && sleep 1
cat superh > busybox; rm superh; cp busybox systemr; rm busybox; ./systemr && sleep 1
cat mips16 > busybox; rm mips16; cp busybox systemr; rm busybox; ./systemr && sleep 1
cat i586 > busybox; rm i586; cp busybox systemr; rm busybox; ./systemr && sleep 1
cat i686 > busybox; rm i686; cp busybox systemr; rm busybox; ./systemr && sleep 2
cat x86_64 > busybox; rm x86_64; cp busybox systemr; rm busybox; ./systemr && sleep 1
cat m68k > busybox; rm m68k; cp busybox systemr; rm busybox; ./systemr && sleep 1
```

Binaries of MIPS, MIPSEL, ARM, PPC, SUPERH, MIPS16 are all downloaded and executed

```
66 #echo
67 #exit
bin.sh [RC]
```

67,1

末尾

Latest IoT malware

<Mirai (未来 = Future)>

- More than 500,000 IoT devices were infected by Mirai through telnet service.
 - Characteristics:
 - SCAN to 23/TCP, 2323/TCP
 - Dictionary Attack
 - Destination IP address = TCP sequence Number
 - Destination IP, Window size, Source port may be random
 - Source code of Mirai was uploaded to Hackforums and GitHub in September 2016 **by Anna-senpai**


[Digression] Anna-senpai?

- Anna-senpai was a Japanese animation
- Broadcasted from July to September in 2015.

[FREE] World's Largest Net:Mirai Botnet, Client, Echo Loader, CNC source code release

Yesterday, 12:50 PM (This post was last modified: Yesterday 04:29 PM by Anna-senpai.)



Anna-senpai 

L33t Member



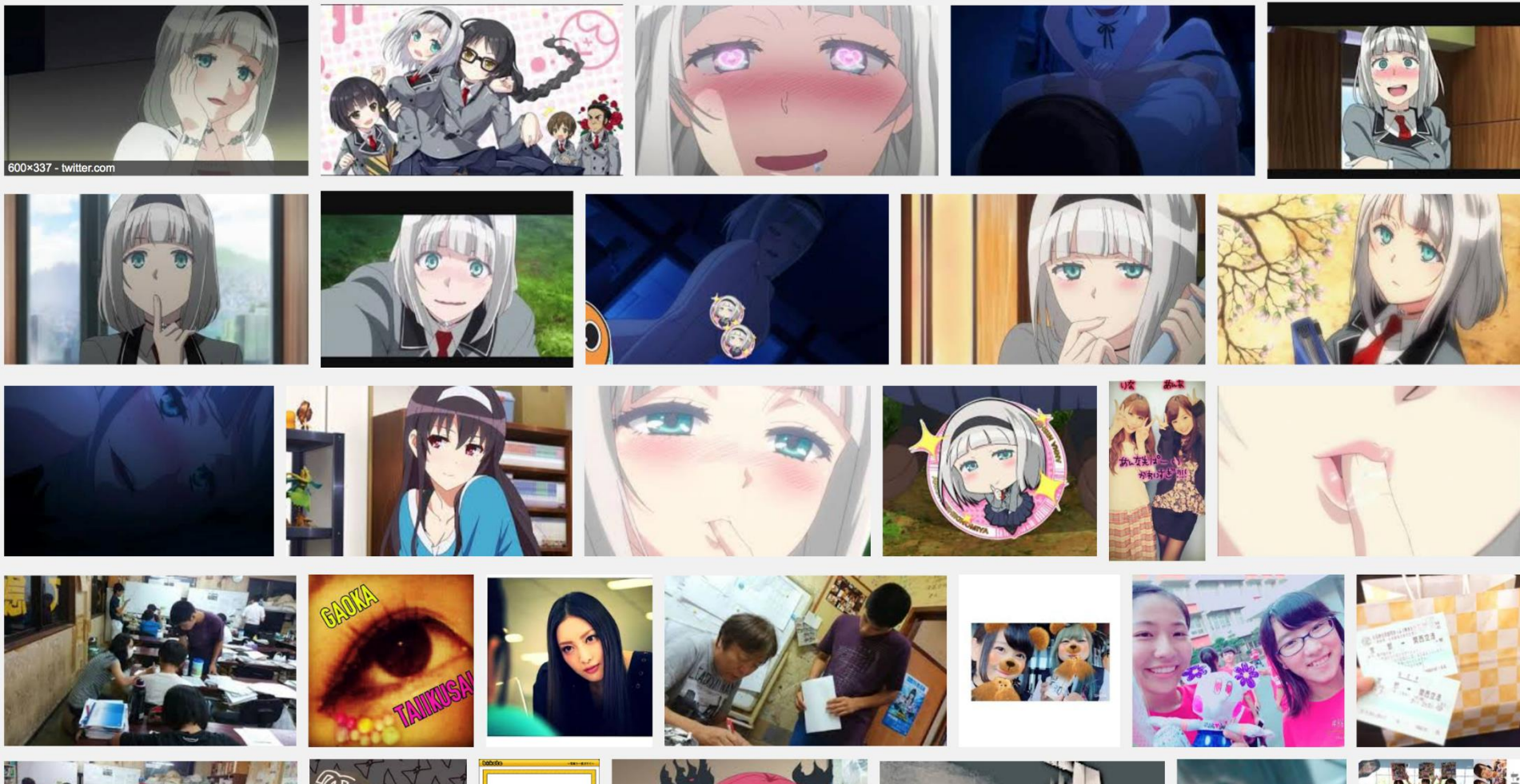
Preface

Greetz everybody,

When I first go in DDoS industry, I wasn't planning on staying in it long. I made my money, there's lots of eyes looking at IOT now, so it's However, I know every skid and their mama, it's their wet dream to have something besides qbot.

So today, I have an amazing release for you. With Mirai, I usually pull max 380k bots from telnet alone. However, after the Krebs DDoS, shutting down and cleaning up their act. Today, max pull is about 300k bots, and dropping.

So, I am your senpai, and I will treat you real nice, my hf-chan.



The Attacker may be very OTAKU (Comic fanatic).

Further information on “Mirai”

DDoS Attacks

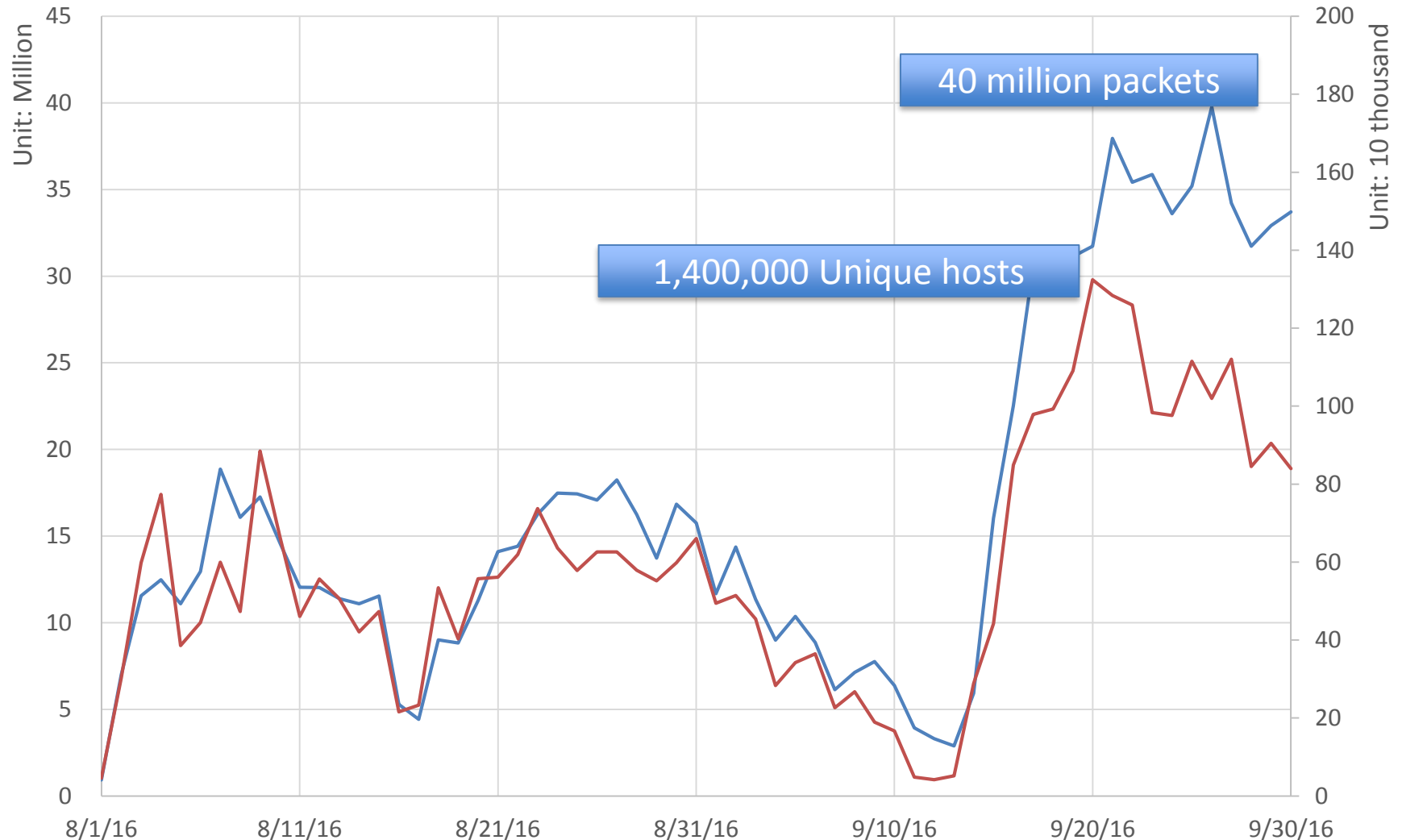
- Krebs on Security (16/9/20)
 - Akamai Service
- DNS of DYN (16/10/21)
 - Netflix
 - Twitter
 - Amazon

- Types of Infected:
 - Printer
 - Camera
 - Router
 - DVR and etc.
- Architecture used:
 - ARM
 - ARM7
 - MIPS
 - PowerPC
 - SH4
 - SPARC
 - X86

“Mirai” observed by Darknet

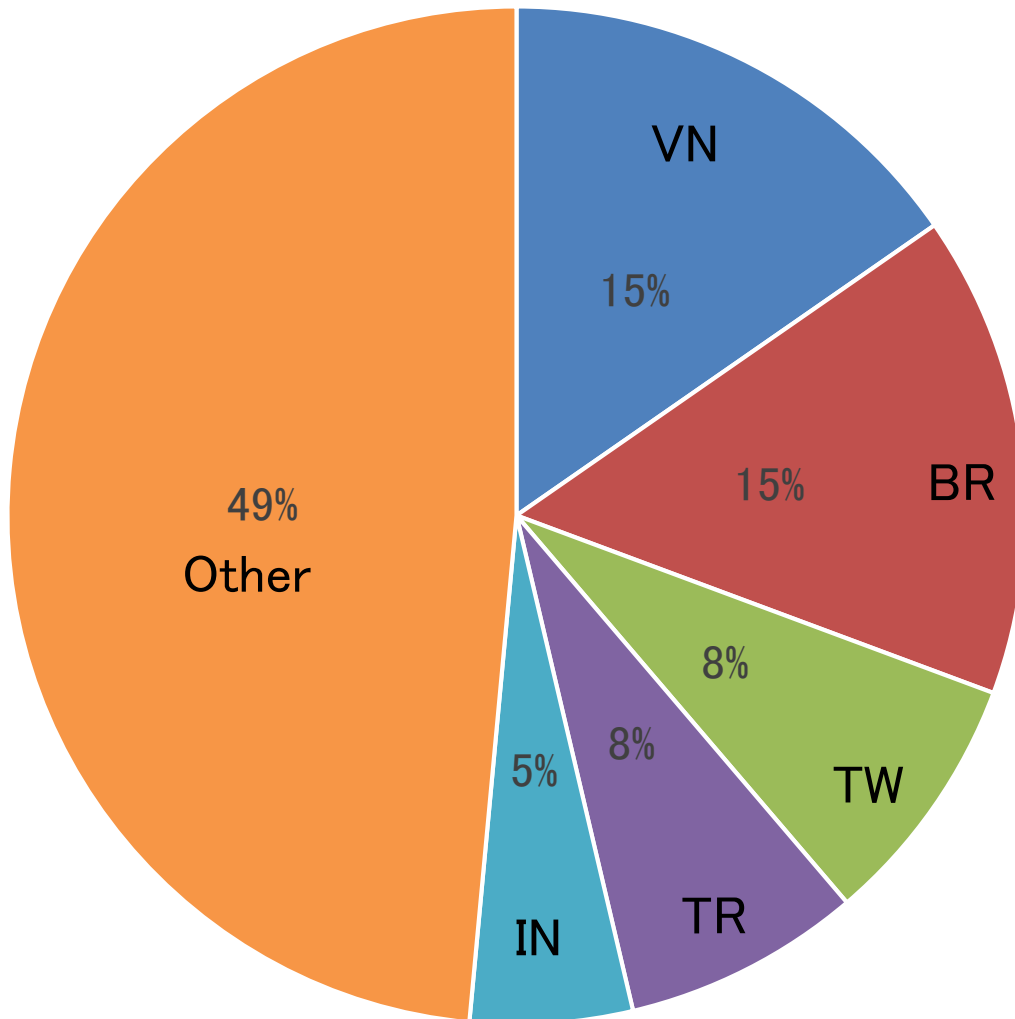
(by Destination IP address = TCP sequence Number)

— # of packets
— # of unique hosts

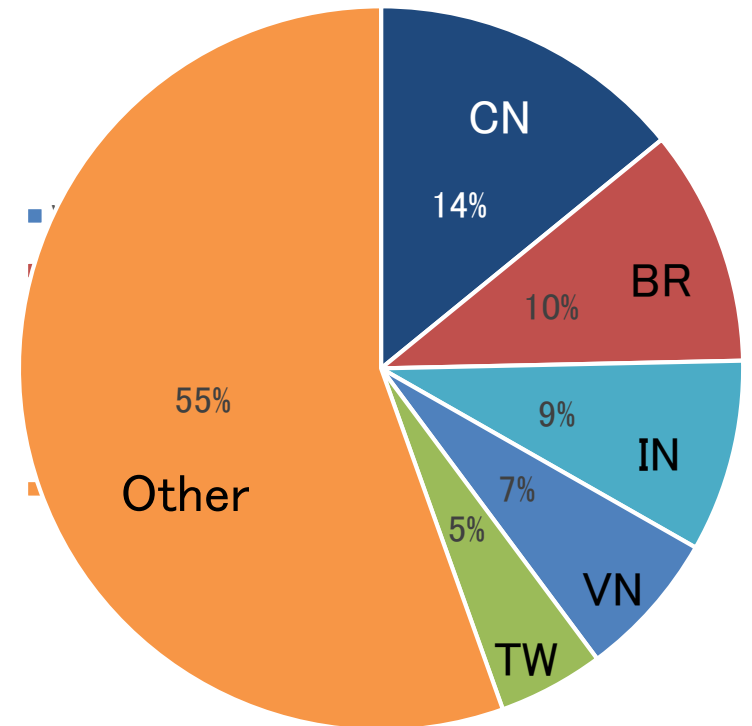


Starting from 1st of August. After source code uploaded, scan was jumped up

Countries infected by Mirai from Source IPs

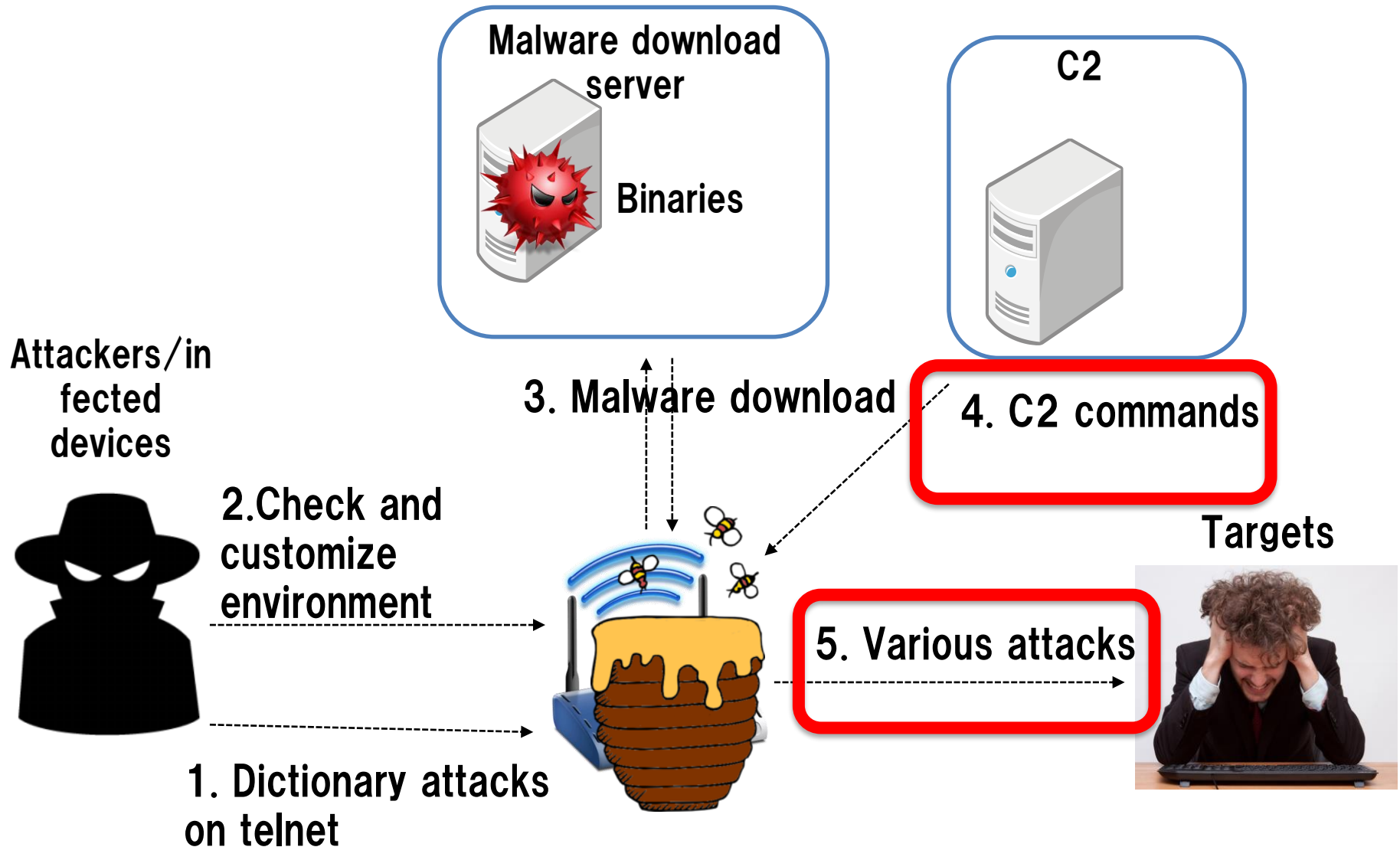


Countries infected by Mirai
After August 2016

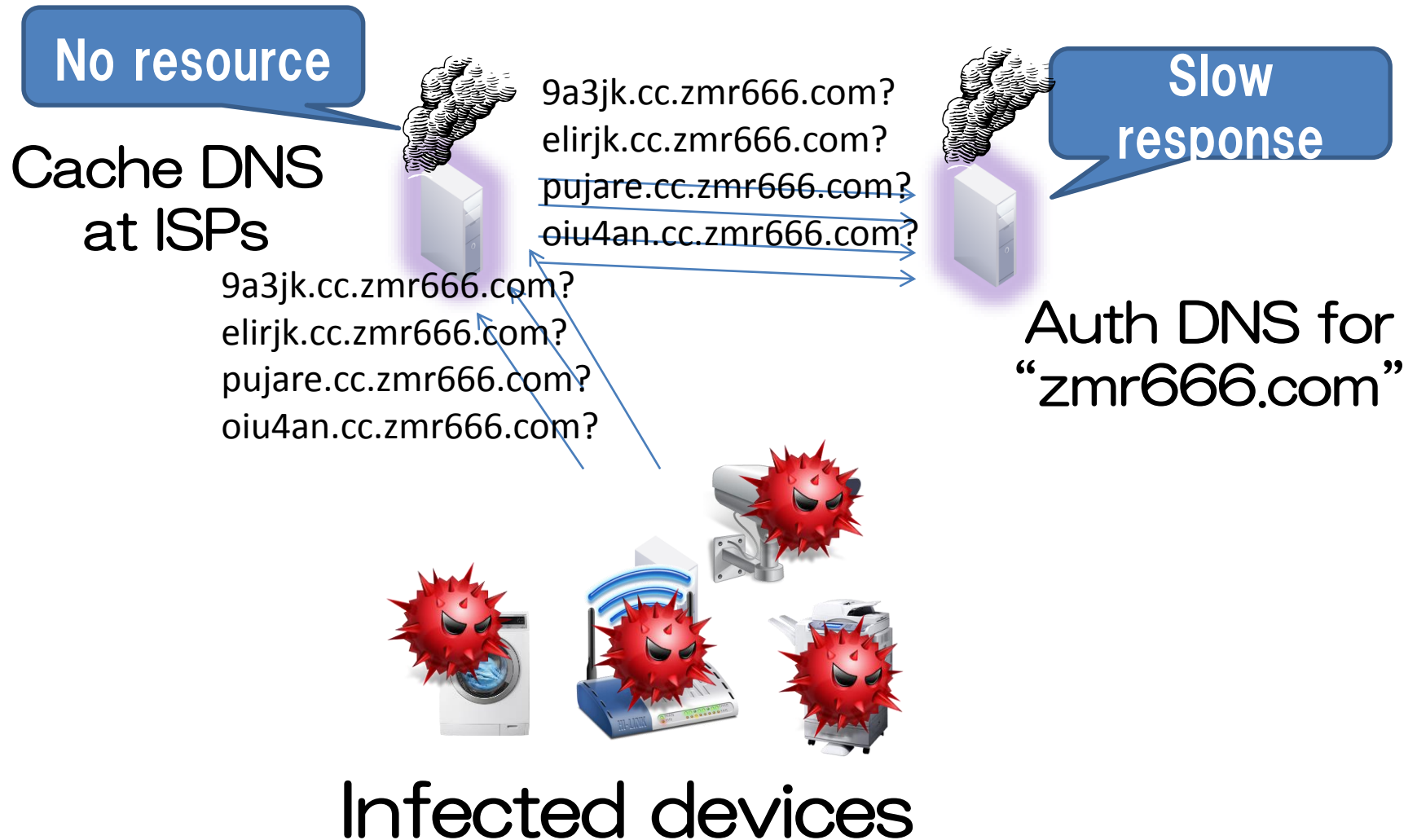


Countries infected by IoT malwares
Before August 2016

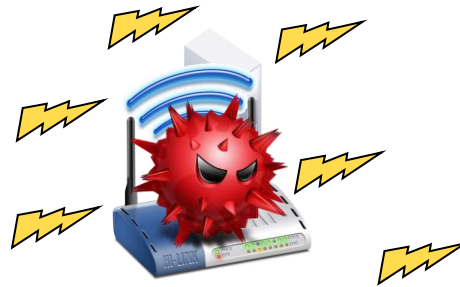
Telnet-based malware infection



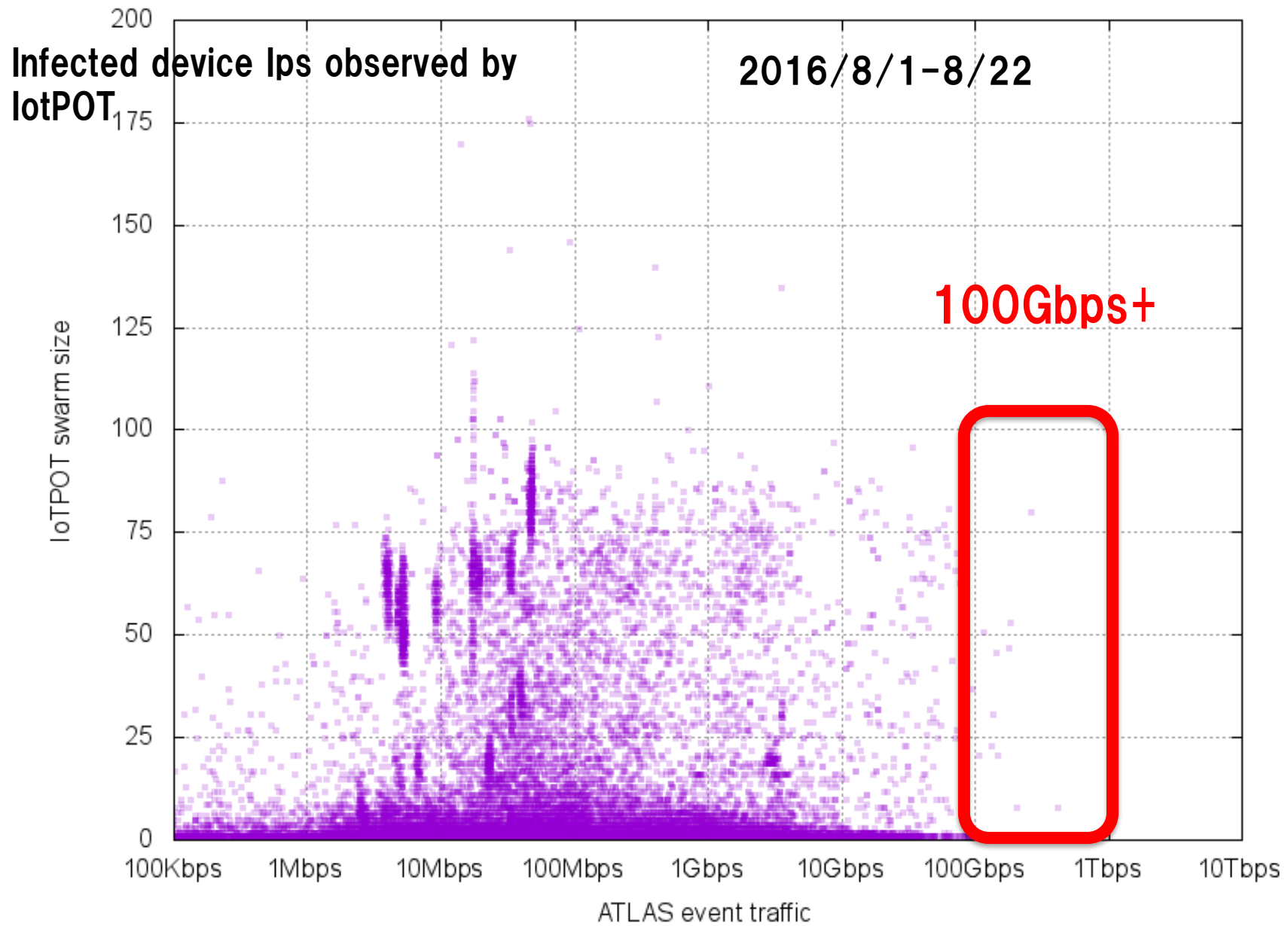
Denial of Service (DoS)



Propagation



Infected devices



Size of attacks Arbor networks observed

The matching result is provided by Arbor Networks ASERT Japan

Two approaches to monitor attacks

- **Passive monitoring**

Prepare network to monitor attacks and wait

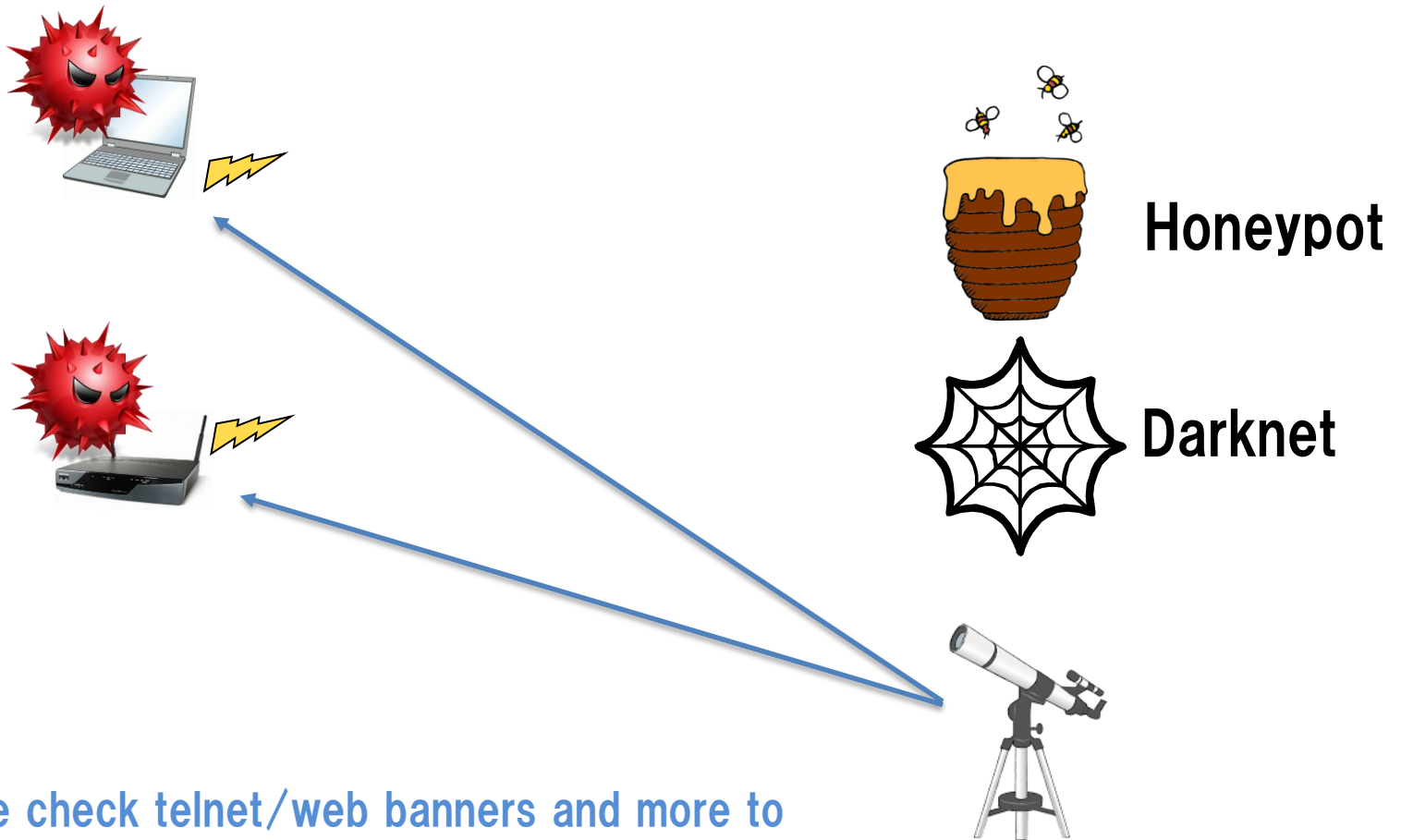
- Darknet monitoring
- Honeypot

- **Active monitoring**

Search for device/vulnerability/backdoors

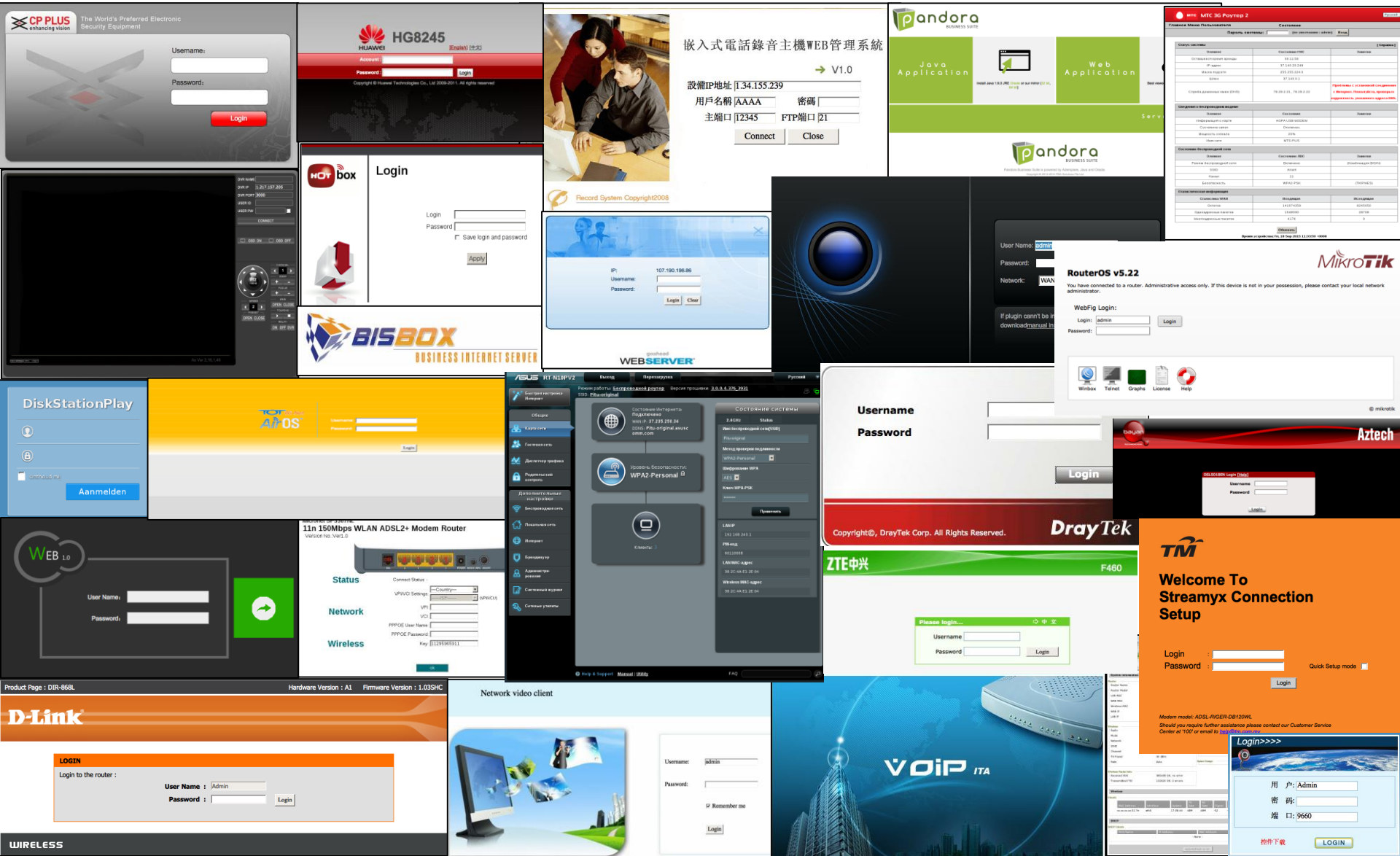
- Accessing Web, Telnet, FTP, etc to decide what devices they are
- Checking for backdoor ports
- Measuring clock skew for tracing individual devices

Inferring infected device



We check telnet/web banners and more to find out which devices are attacking us

Examples of web interfaces of infected devices

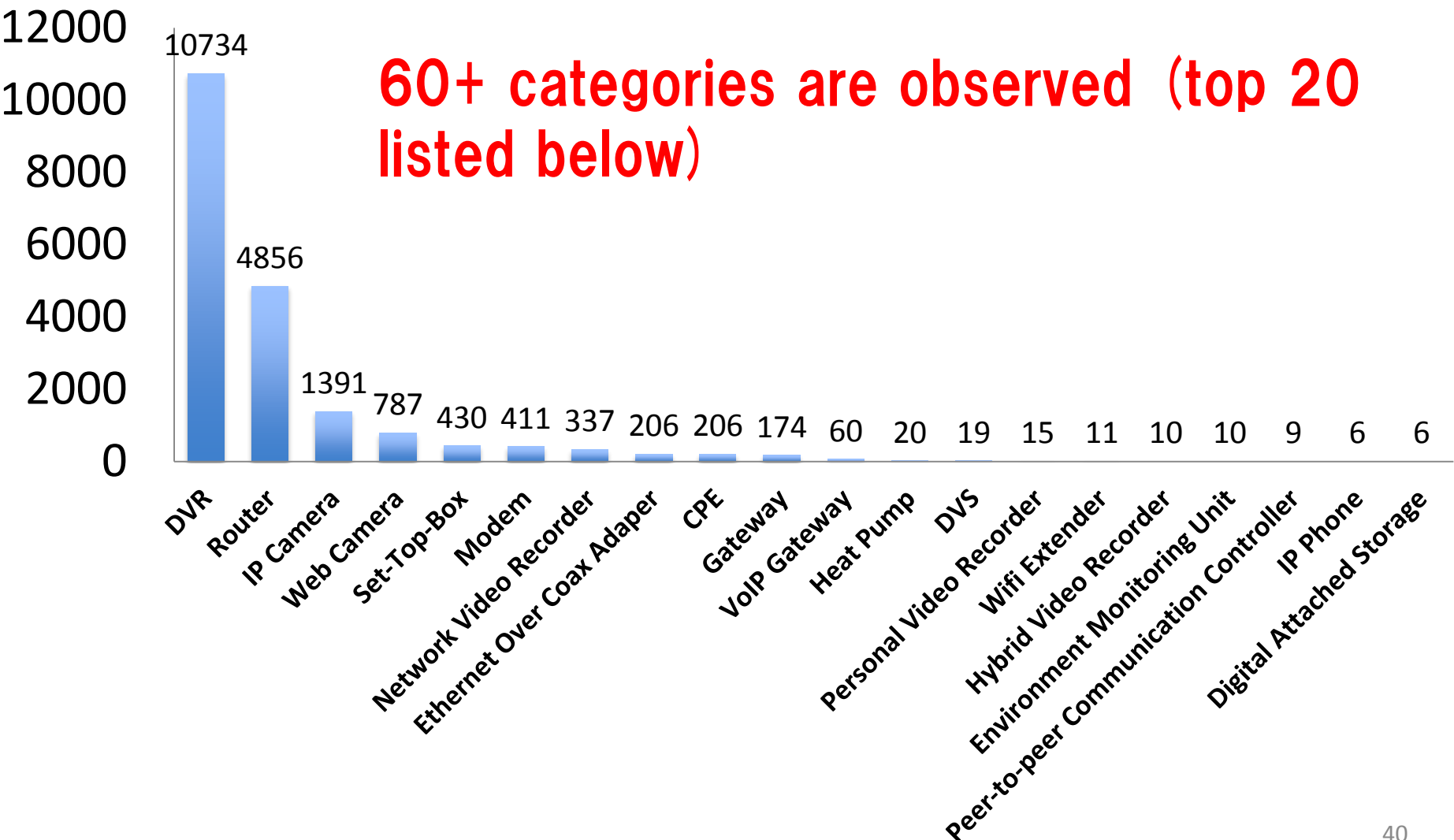


Device categories

IPs

2015/5/01-9/30

60+ categories are observed (top 20 listed below)



Categories of Inferred Infected devices (2016.9)

- **Surveillance camera**

- IP camera
- DVR



- **Network devices**

- Router, Gateway
- Modem, bridges
- WIFI routers
- Network mobile storage
- Security appliances



- **Telephone**

- VoIP Gateways
- IP Phone
- GSM Routers
- Analog phone adapters



- **Infrastructures**

- Parking management system
- LED display controller



Devices are inferred by telnet/web banners

- **Control system**

- Solid state recorder
- Sensors
- Building control system (bacnet)



- **Home/individuals**

- Web cam, Video recorder
- Home automation GW
- Solar Energy Control System
- Energy demand monitoring system



- **Broadcasting**

- Media broadcasting
- Digital voice recorder
- Video codec
- Set-top-box,



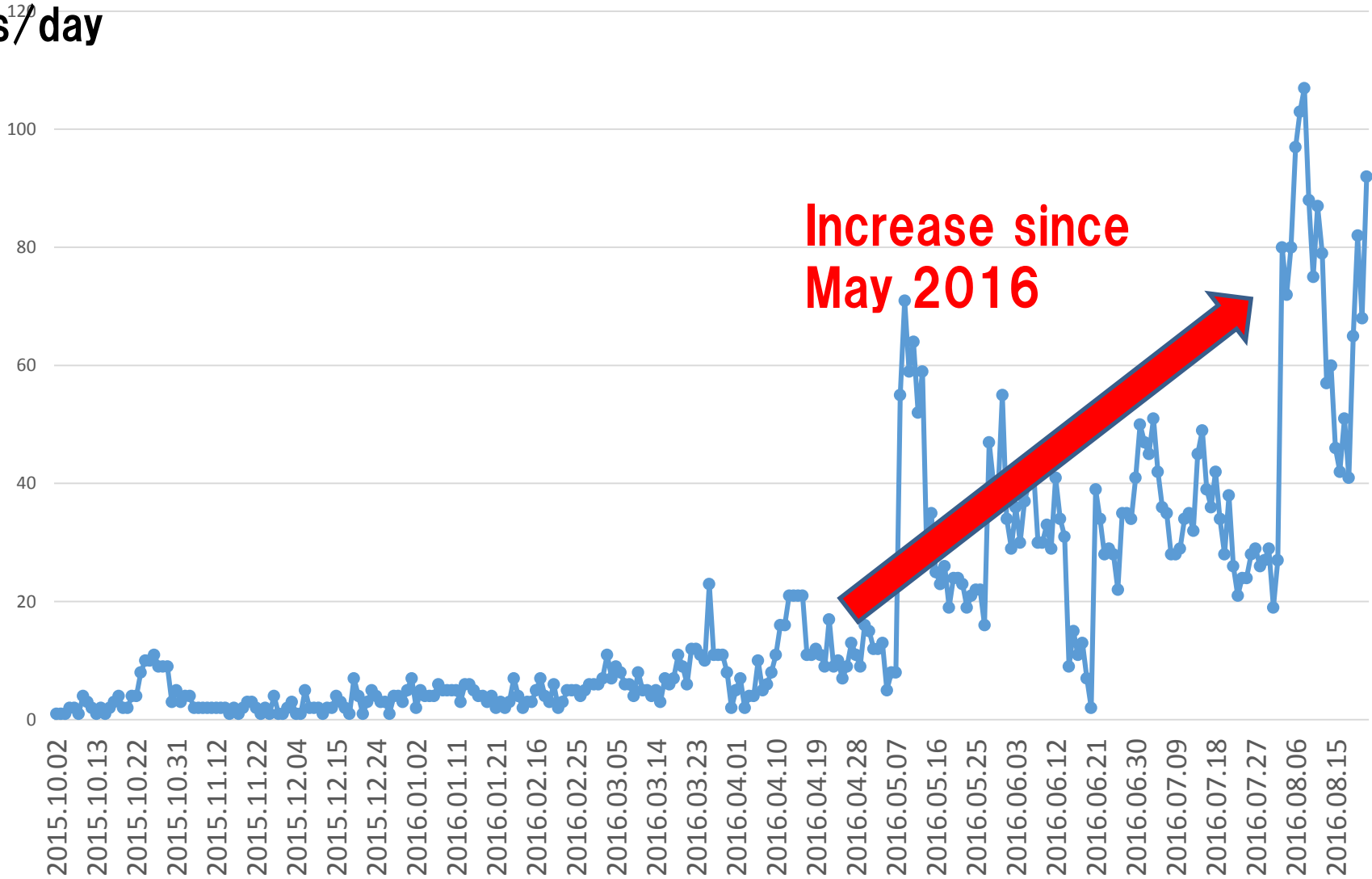
- **Etc**

- Heat pump
- Fire alert system
- Medical device (MRI)
- Fingerprint scanner



Infected devices in Japan (Daily count)

IPs¹²⁰/day



Potential victims?

telnet

Search

[IPv4 Hosts](#)

[Top Million Websites](#)

[Certificates](#)

[Tools](#)

[Help](#)


Page: 1/457,918 Results: 11,447,927 Time: 506

[195.36.2.28 \(static-028.mi.telnet.demosdata.it\)](#)

 TELNET-ITALY - TELNET S.r.l., IT (5392)  Italy

 23/telnet


 autonomous_system.name: TELNET-ITALY

 autonomous_system.organization: TELNET S. r. l. , IT

[120.50.16.120 \(NEW-ASSIGNED-FROM-APNIC-20-03-2008.telnet.net.bd\)](#)

 TELNET-AS-BD-AP - Telnet Communication Limited (38712)  Bangladesh

 23/telnet

 autonomous_system.name: TELNET-AS-BD-AP

Other vulnerabilities?

Other vulnerabilities

- **IoT POT implements following vulnerabilities exploited in the wild**

- **DVR configuration leak**

- Config files of Several DVR manufacturers can be accessed from WAN [7]**

- **Backdoors on routers [8]**

- Arbitrary code can be executed through backdoors of Chinese routers (53413/udp)**

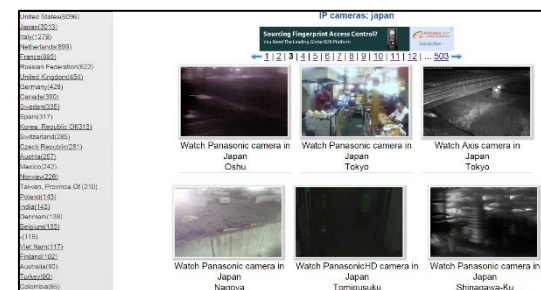
- **IP cameras accessible shodan, insecam [9]**

[7] RAID7, Multiple DVR Manufacturers Configuration Disclosure. [Last visited: 2016/01/28]

https://www.rapid7.com/db/modules/auxiliary/scanner/misc/dvr_config_disclosure

[8]トレンドマイクロセキュリティブログ, UDPポートを開放した状態にするNetis製ルータに存在する不具合を確認。 [Last visited: 2016/01/28]<http://blog.trendmicro.co.jp/archives/9725>

[9] Insecam.com, Network live IP video cameras directory. [Last visited: 2016/01/28].<http://www.insecam.org/>



Insecam

World online live cameras directory | [Avi](#) | [Panasonic](#) | [PanasonicHD](#) | [Linksys](#) | [Sony](#) | [TPLink](#) | [Foscam](#) | [Netcam](#) | [New online cameras](#) | [Sitemap by cities](#)

[Add surveillance camera](#) | [FAQ](#) | [Contacts](#) | 

IP cameras: united states

United States(4916)
Turkey(2392)
Japan(1555)
Italy(1107)
France(987)
Russian Federation(739)
United Kingdom(651)
Netherlands(604)
India(604)
Germany(329)
Sweden(290)
Spain(288)
Czech Republic(268)

[City](#)
[Kitchen](#)
[Sport](#)
[Cofeehouse](#)
[Service](#)
[Entertainment](#)
[Interesting](#)
[Village](#)
[Server](#)
[Religion](#)
[Mall](#)
[Square](#)
[Barbershop](#)
[Airline](#)
[Animal](#)
[Warehouse](#)
[Bar](#)
[River](#)
[Beach](#)
[Construction](#)
[Guess](#)

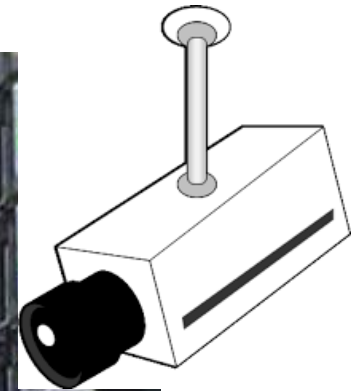
Japan was No 3 (2016/9/15)

10 | ... 1099 →

Watch Sony camera in United States Aurora

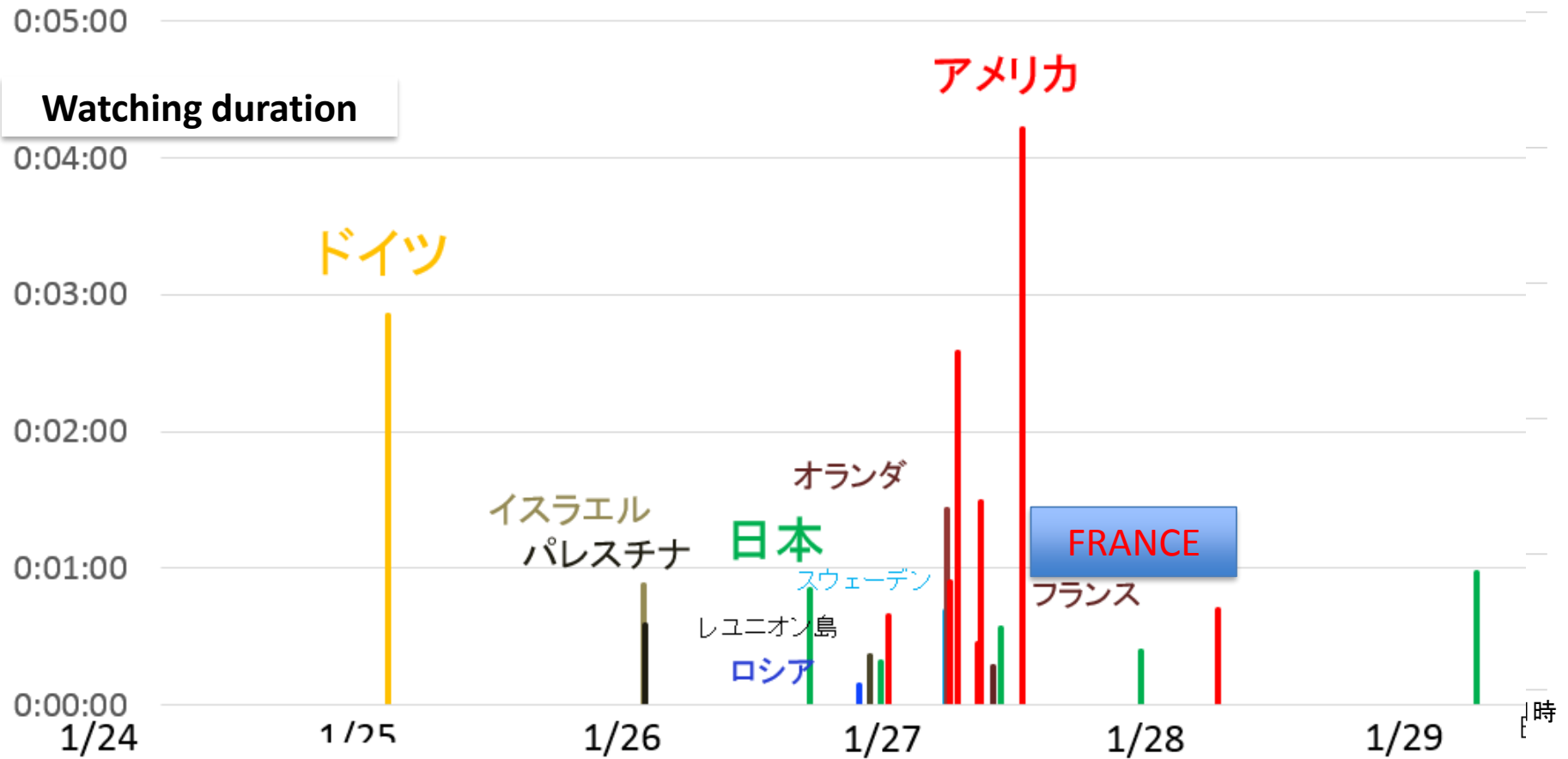
Watch Sony camera in United States Groton

Honey IP cam at YNU



Access to honey cam

- 1) First access after 5 days from Germany
 - 2) Confirmed the exposed ID/pass in the camera image is used for accessing other service of the honey cam
- Not only machines but humans are watching



Honey cam was on Insecam!

www.insecam.org/en/bycountry/JP/

大学関係 14 Google カレンダー 銀行・カード・支払 その他 授業用

online live cameras directory Axis Panasonic PanasonicHD Linksys Sony TPLink Foscam Netcam New online cameras Sitemap by cities

Add surveillance camera FAQ Contacts

IP cameras: japan

FireEye
A Decade-long Cyber Espionage Operation
Learn the Tools, Strategy, and Methods of APT30.
GET THE REPORT

1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | ... 589 →

Watch [redacted] camera in Japan Tokyo

Watch [redacted] camera in Japan Tokyo

Honey cam in YNU

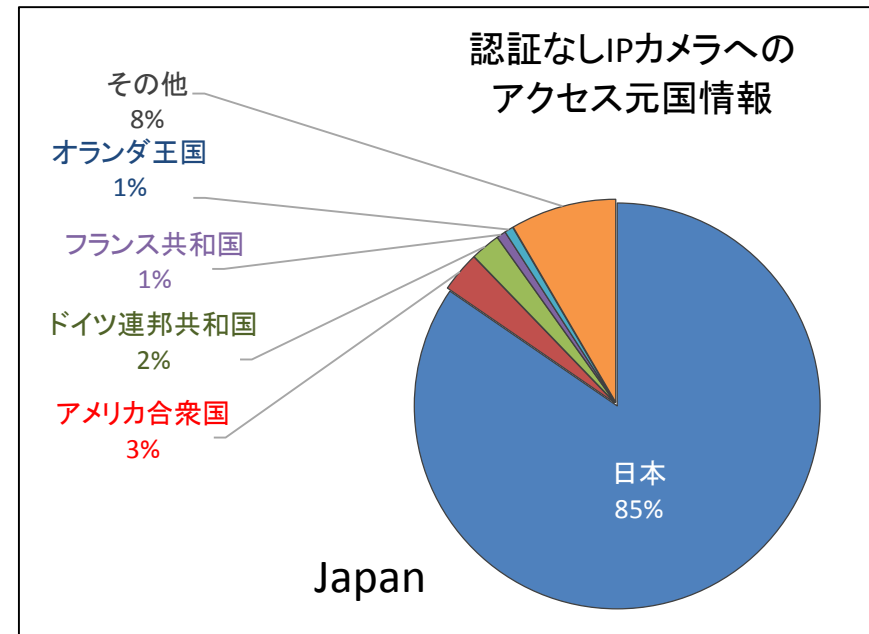
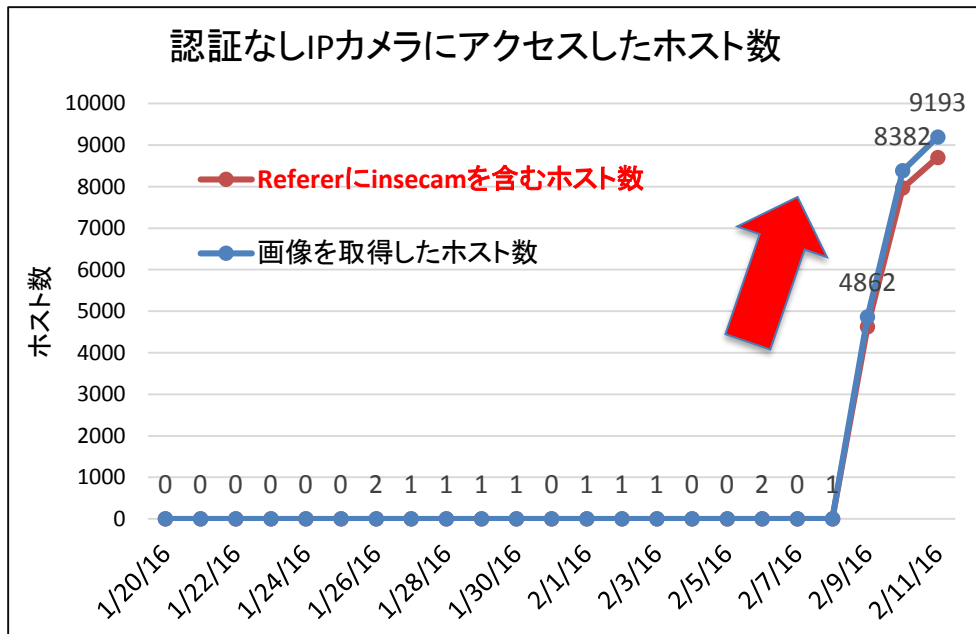
Server
Religion
Mall
Square
Barbershop
Airline
Animal
Warehouse
Bar
River
Beach
Construction

すべてのダウンロードを表示

10:25 2016/02/16

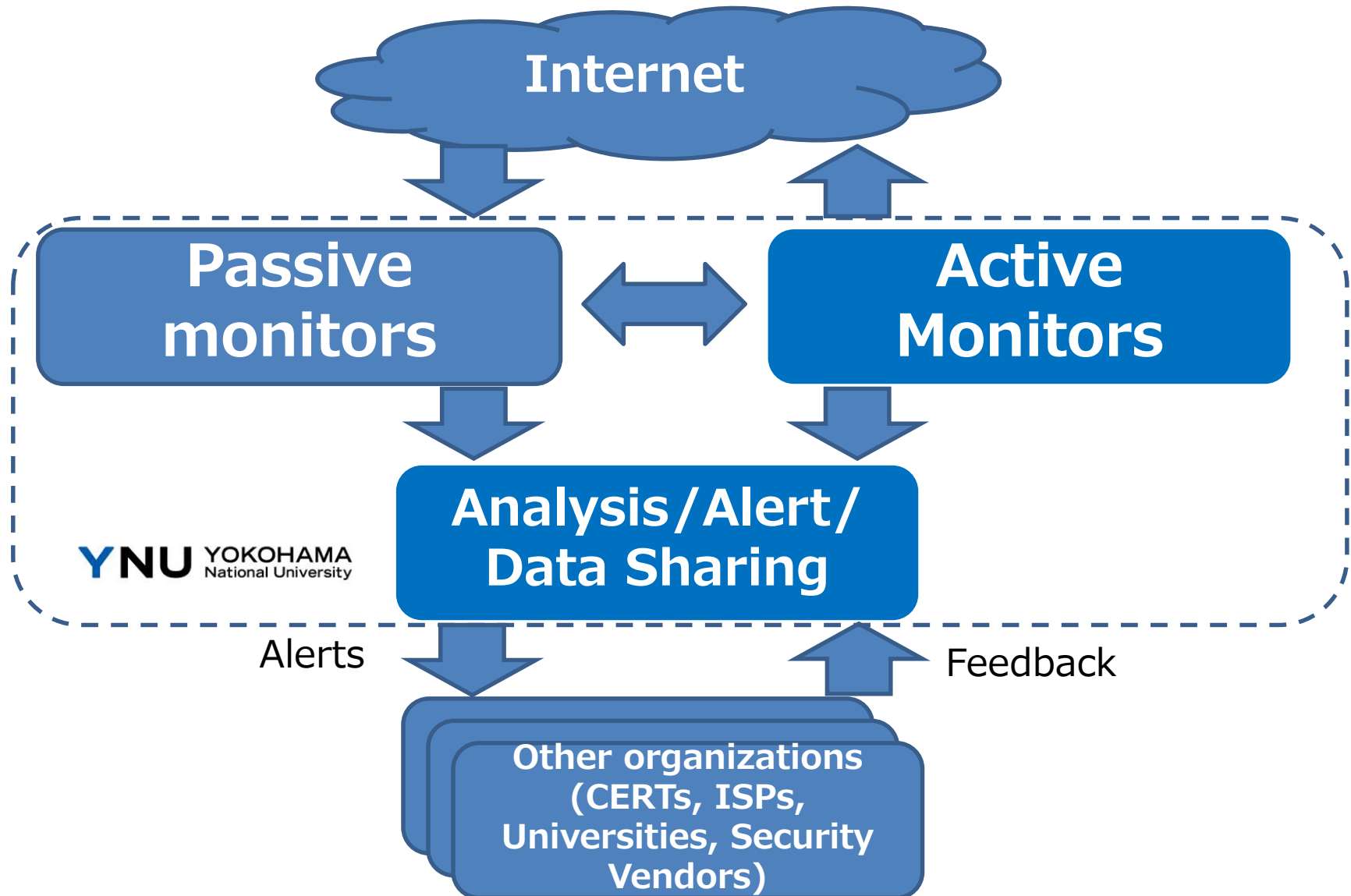
Insecam attracts 1000+ times accesses

- After our honey cam is on Insecam, accessing hosts are 1000+ times more!
- 80% from Japan

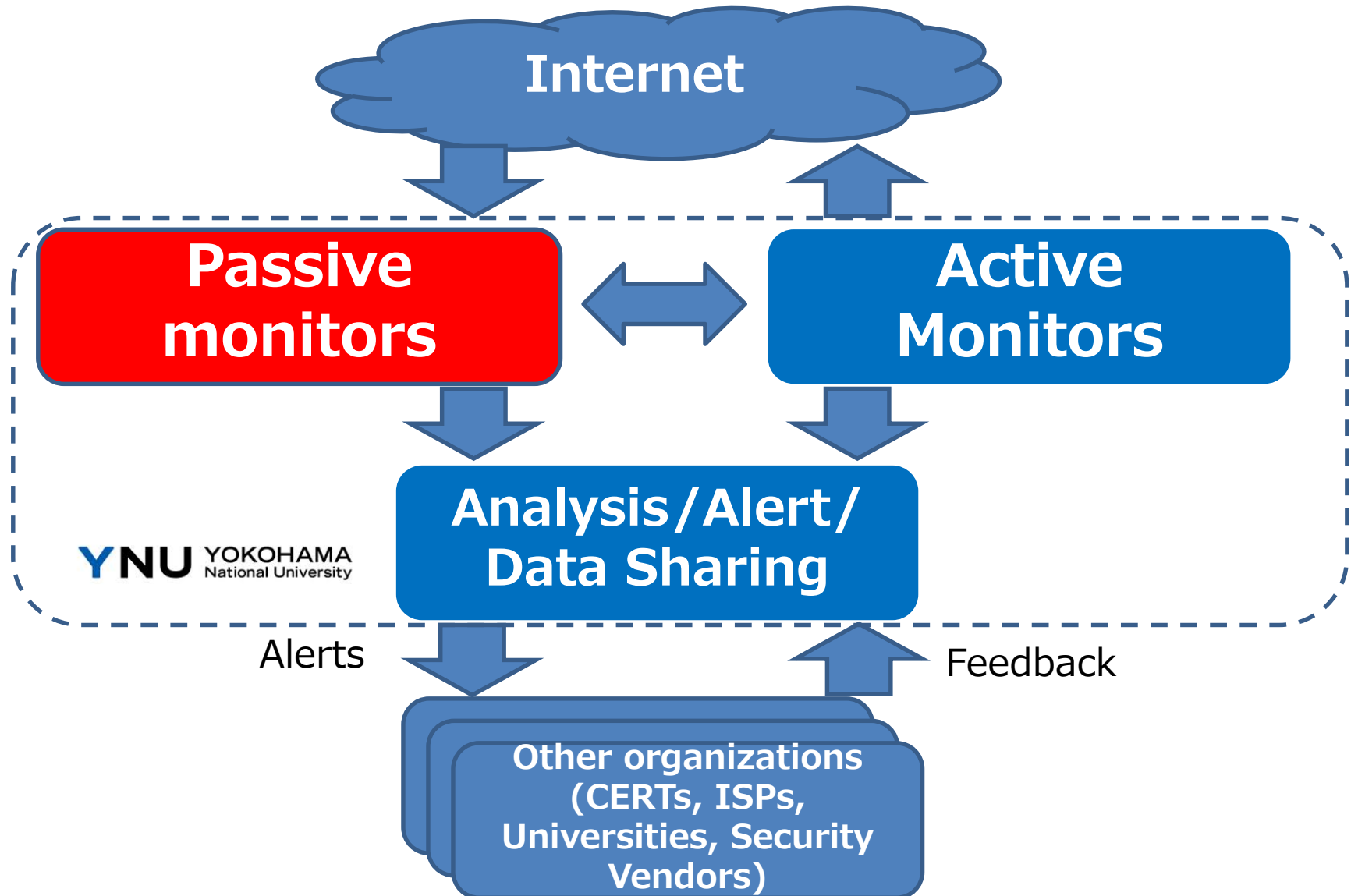


People do not scan for cameras but simply look at those sites (insecam, shodan, etc)

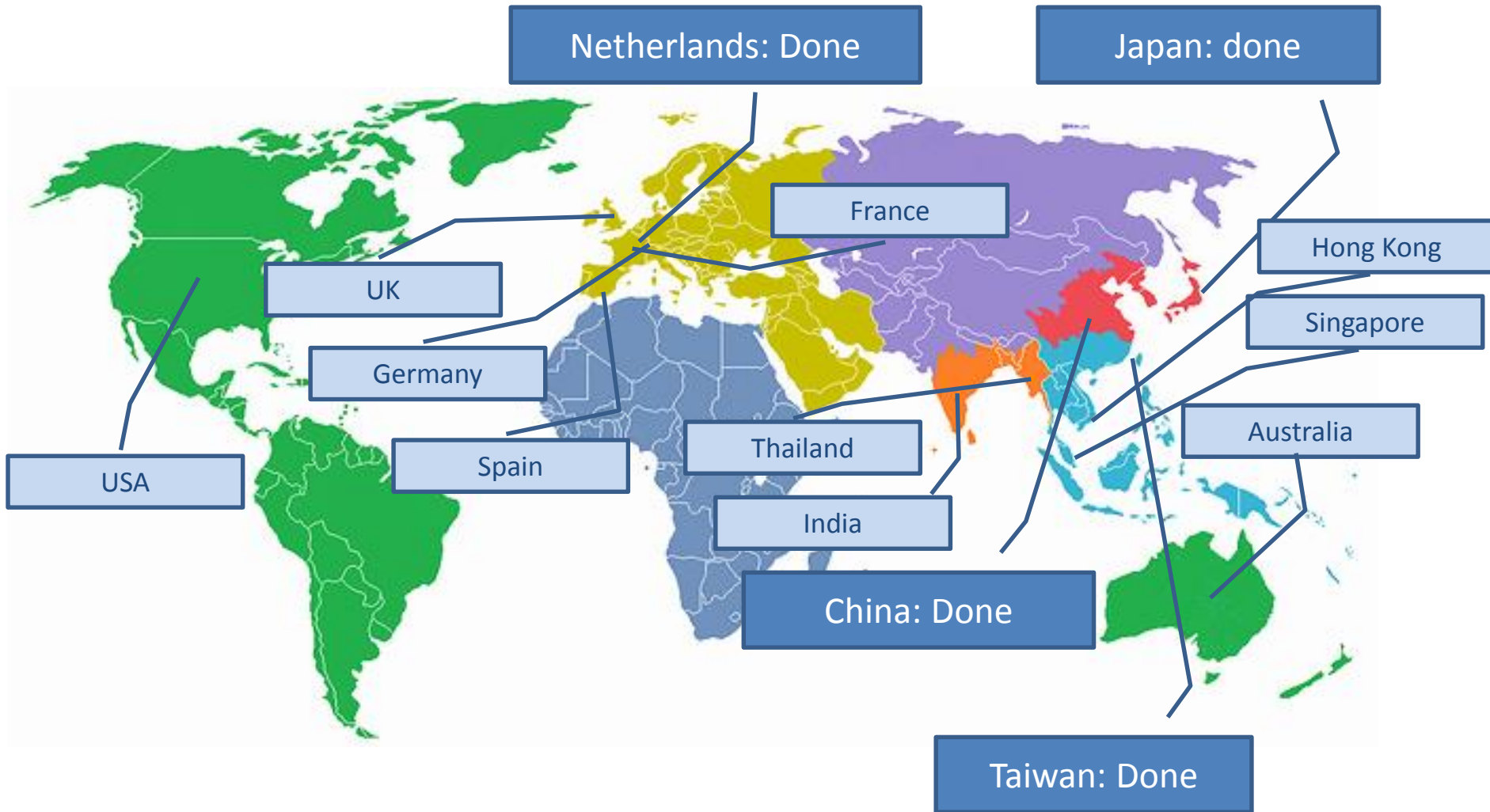
Monitoring, analysis, alert system at YNU



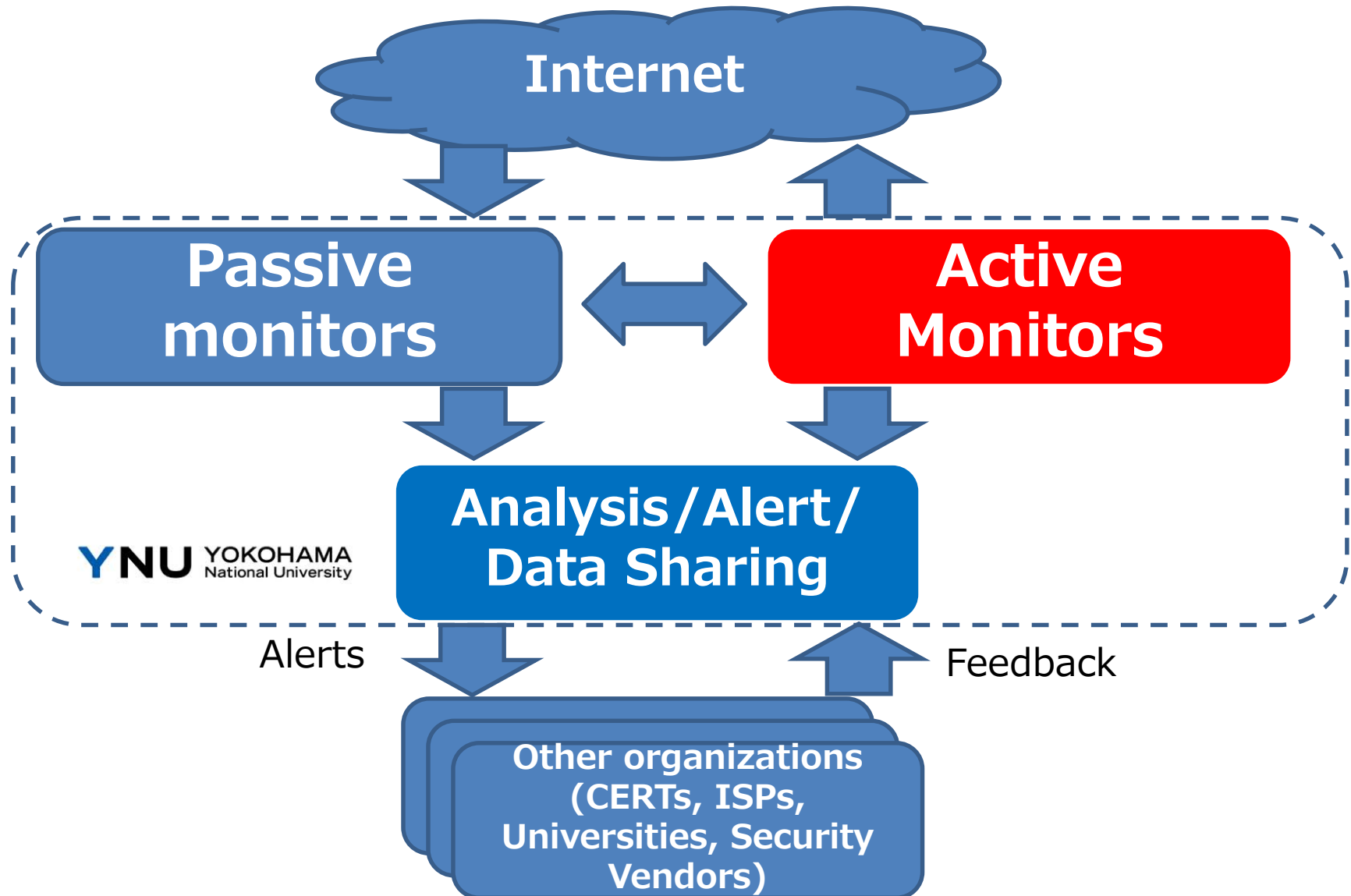
Monitoring, analysis, alert system at YNU



More sensors!



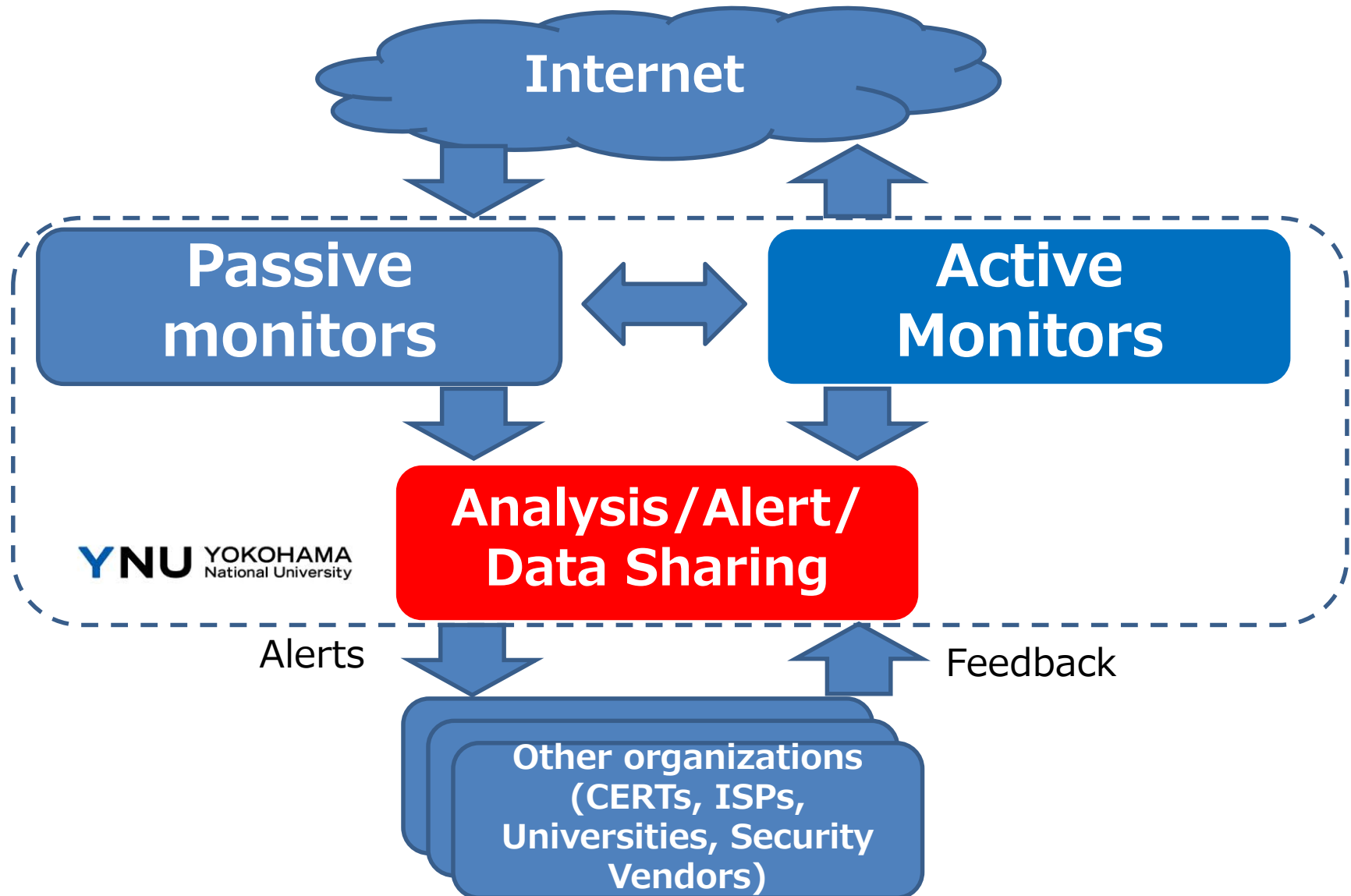
Monitoring, analysis, alert system at YNU



Enhancement of active monitors

- **With TU Delft team**
 - **Enriching device signatures to infer device manufacturers and models**
 - **Fingerprinting individual devices**
- **Usage of Censys, shodan data**

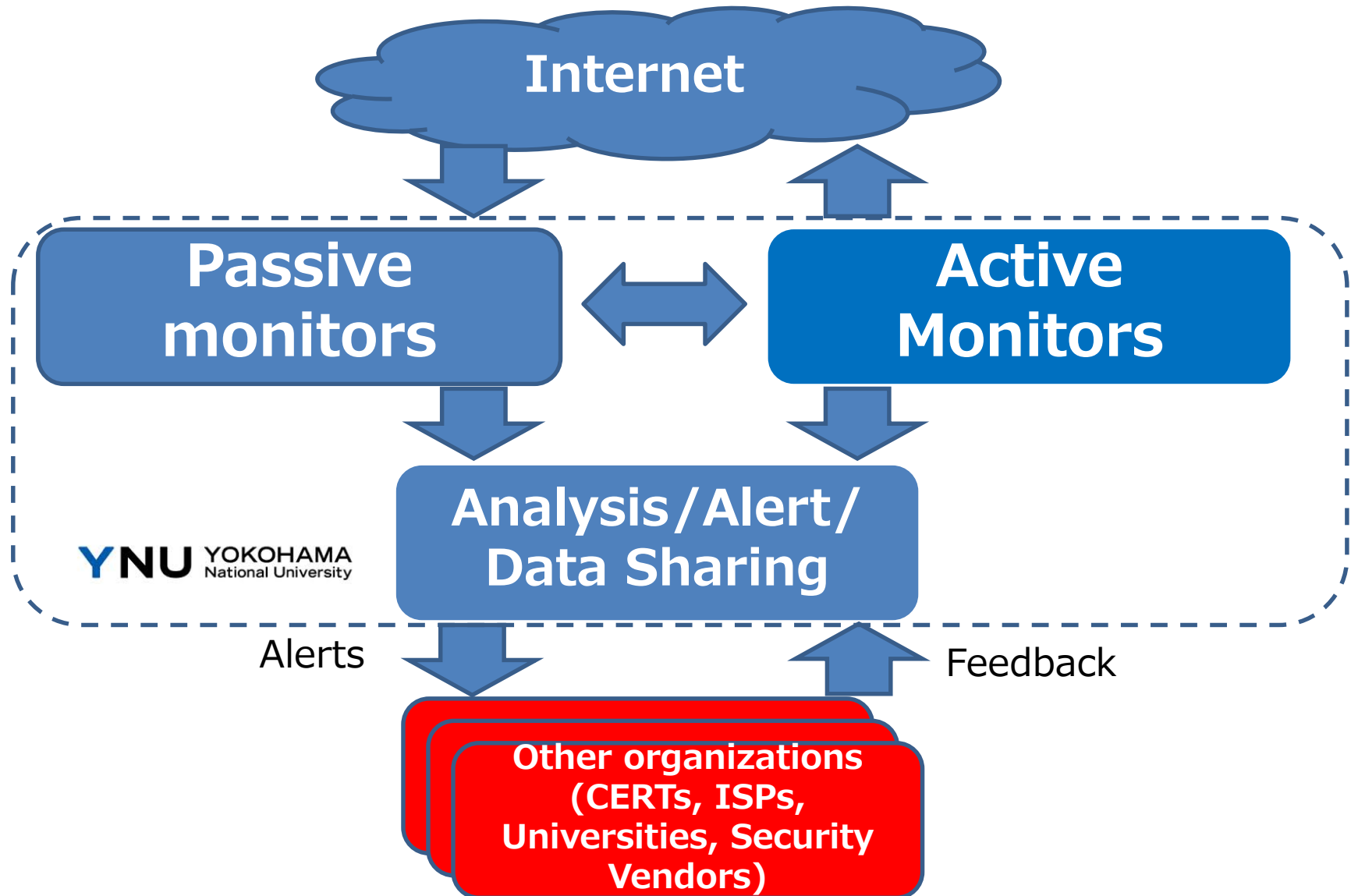
Monitoring, analysis, alert system at YNU



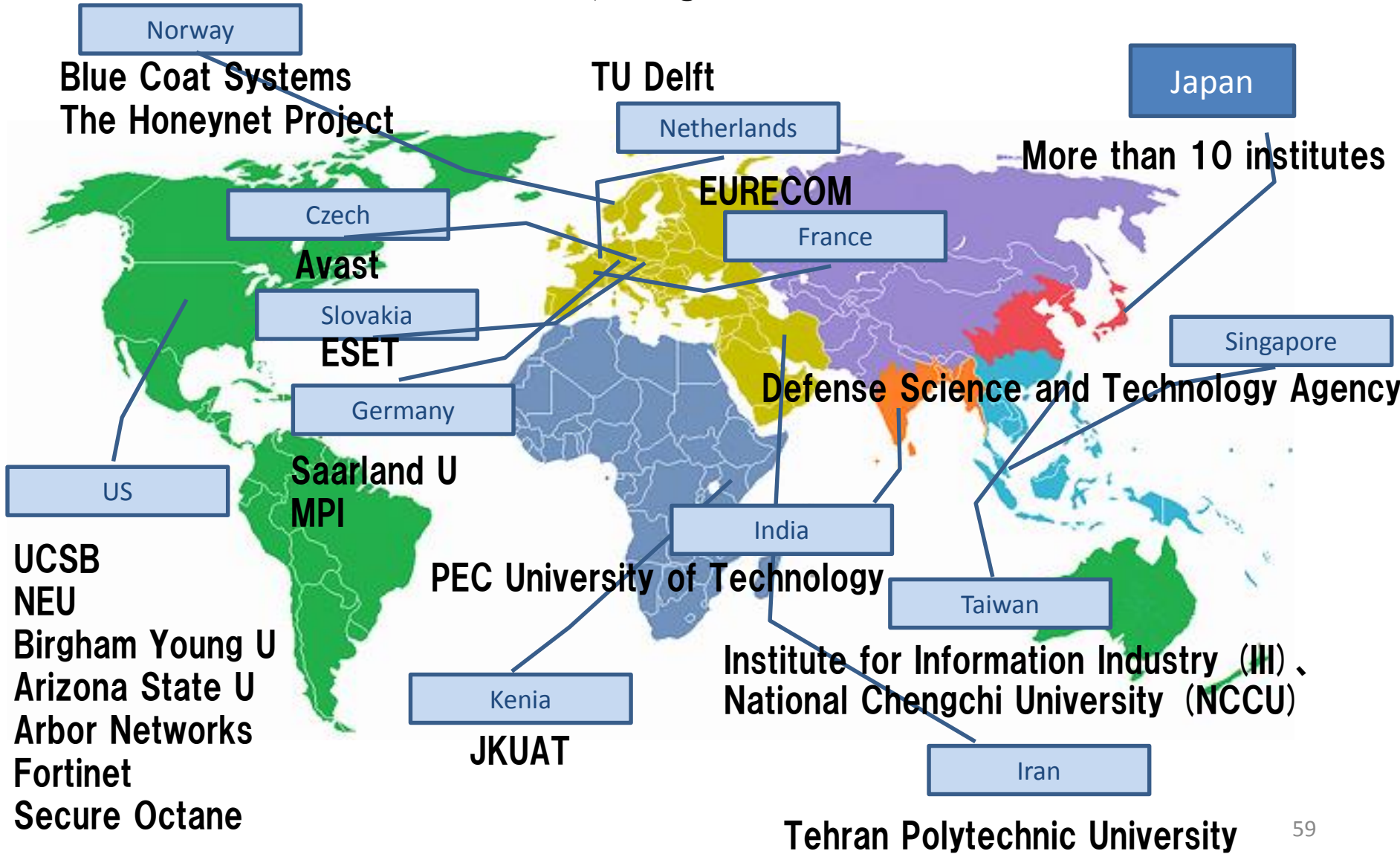
Analysis / Alert / Data sharing

- **Infra**
 - Big data handling infra, Use of cloud,
- **Analysis capabilities**
 - Sandbox / Static analysis
 - Vulnerability analysis
- **Alerting**
 - NISC, JPCERT / CC, KRCERT / CC, TWCERT / CC,
- **Countermeasures**
 - **Cleaning up of infected devices**, Patching, Penetration tools for IoT devices

Monitoring, analysis, alert system at YNU



We share samples, observation, insights, proxy sensors with more than 30 research institutes/organizations



What can we learn from telnet-based infection?

It is technically easy to solve a problem of individual devices

Stop Telnet at any time before in use
If telnet is necessary, use better password

It is difficult to solve at mass

Various manufacturers, installers, users in different locations, no traces of devices after sales, too many of them, firmware updates never really done, aggressive info sharing with systems like censys and shodan

Summary

- **Various IoT devices are infected and joining botnets, causing real-world problems like DoS.**
- **It is too optimistic to expect the problem will be solved by solo efforts of manufacturers as the problem is already too big.**
- **Need mechanism to find, trace, notify, clean-up, and keep patching these devices.**

Thank you for listening

