Cyber Attack in IoT on the rise
- Observing attacks in IoT using IoTPOT -

Koji Nakao
Distinguished Researcher - NICT
Guest Professor - Yokohama National University
Adviser - KDDI

2017/1/24

Cyber attacks in IoT on the rise

Thingbots: The Future of Botnets in the Internet of Things

February 20, 2016 | By Paul Sabanal

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

IoT Home Routers Botnet Leveraged in Large **DDoS Attack**

SucuriSecurity | sucuri.ne

Home Router Botnet Leveraged in
Large DDoS Attack

Is your refrigerator really 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 conce
boost in IoT services

by

News roundup: As Internet of Things conce
rise reality, one vendor is quick to
to combat the risks. Plus: 1% of use
e risk; Target pays up; Apple devic
ly secured in the enterprise.

RISK ASSESSMENT / SECURITY & HACKTIVISM

"Internet of Things" is the new Windows XP —malware's favorite target

Devices attacked our honeypot during Jan-June 2016

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/indivisuals

- 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.

https://en.wikipedia.org/wiki/Telnet

They are everywhere in Internet

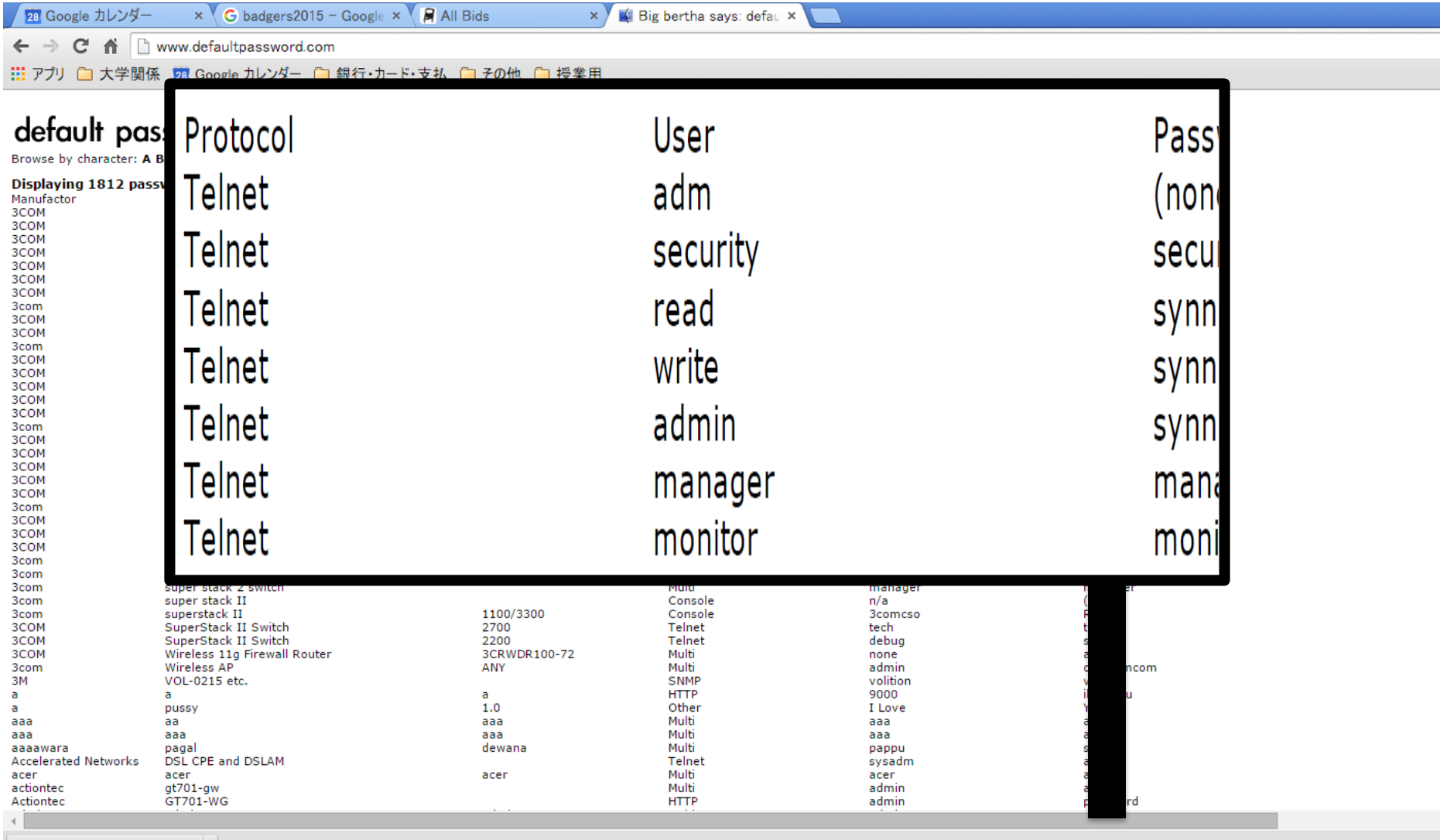
With default/weak id and password

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

[redacted]i.3.0.dm800s
[redacted]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”



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

Devices are inferred by telnet and web banners of these devices


HOW WE
MONITOR
ATTACKS

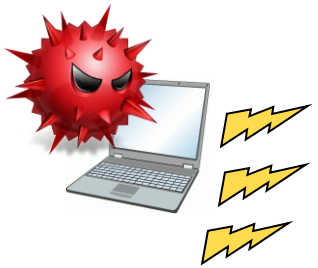
Two approaches to monitor attacks

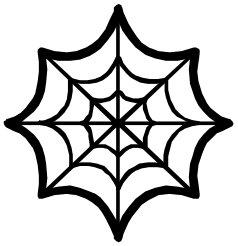
- **Passive monitoring**
  Prepare network to monitor attacks and wait
  - Darknet monitoring
  - Honeypot

- **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





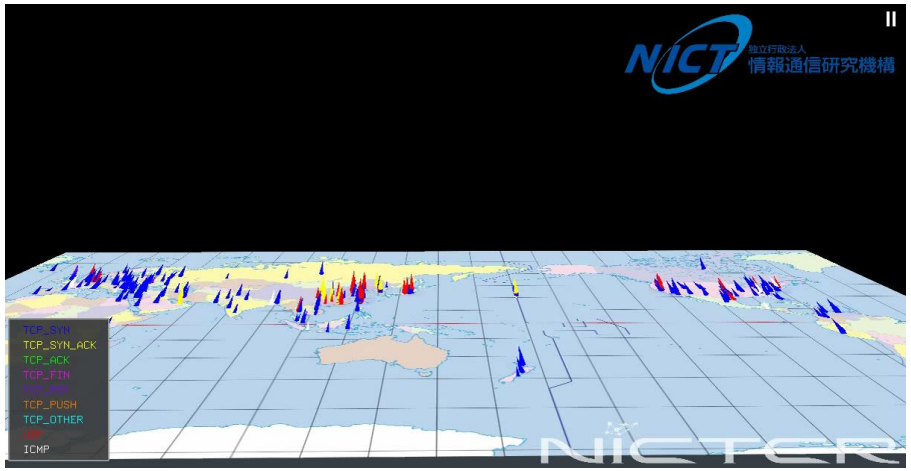
Many researchers/organization utilize darknet to monitor malicious activities like scanning, remote exploits, back scatters, etc

Scanning observation by nicter-Atlas

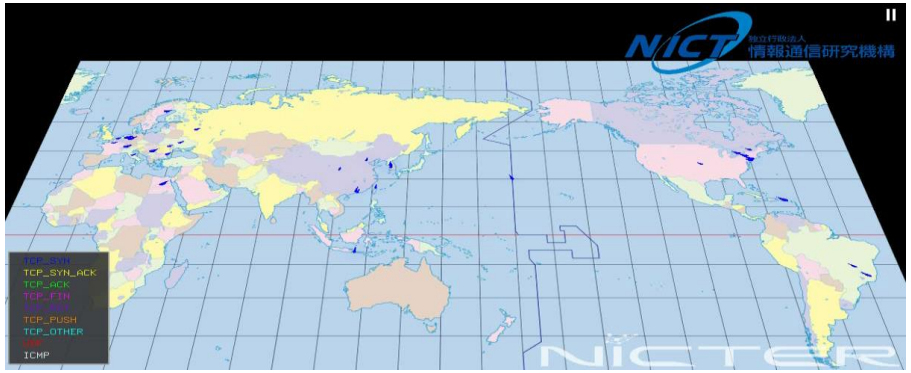
Recently, “scanning to Port 23 (telenet)” is getting larger!!

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

UDP
TCP SYN
TCP SYN/ACK
TCP Other
ICMP



Atlas All view



Atlas only port23

Increases of telnet attacks

packets

7
6
5
4
3
2
1

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%

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

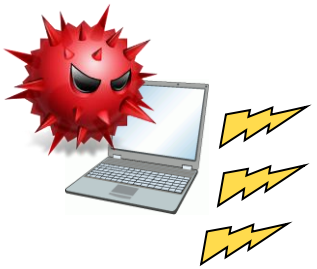
TCP 宛先ポート別パケット数 Top 10

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%

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

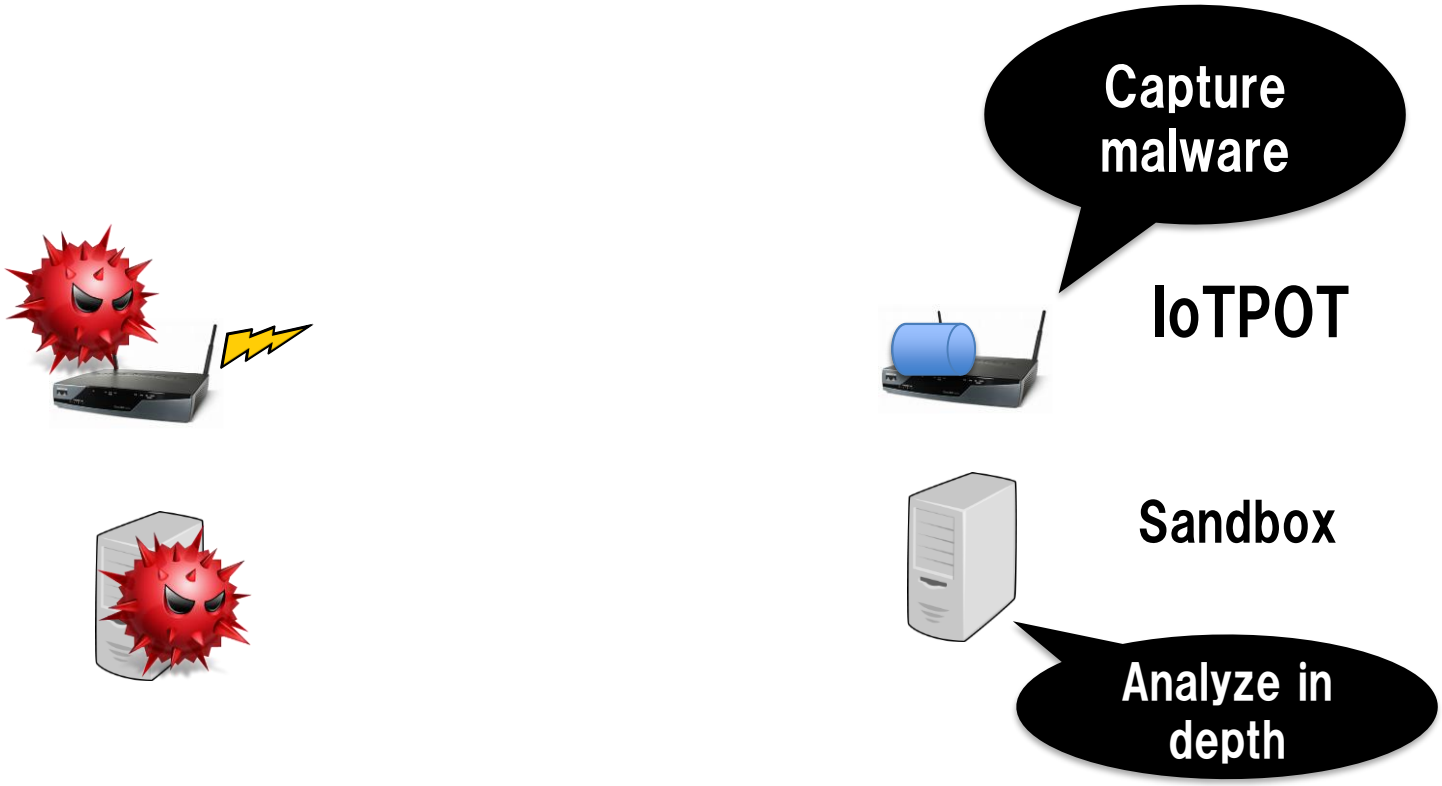
To monitor in depth

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



Our system: IoTPOT = IoT Honeypot

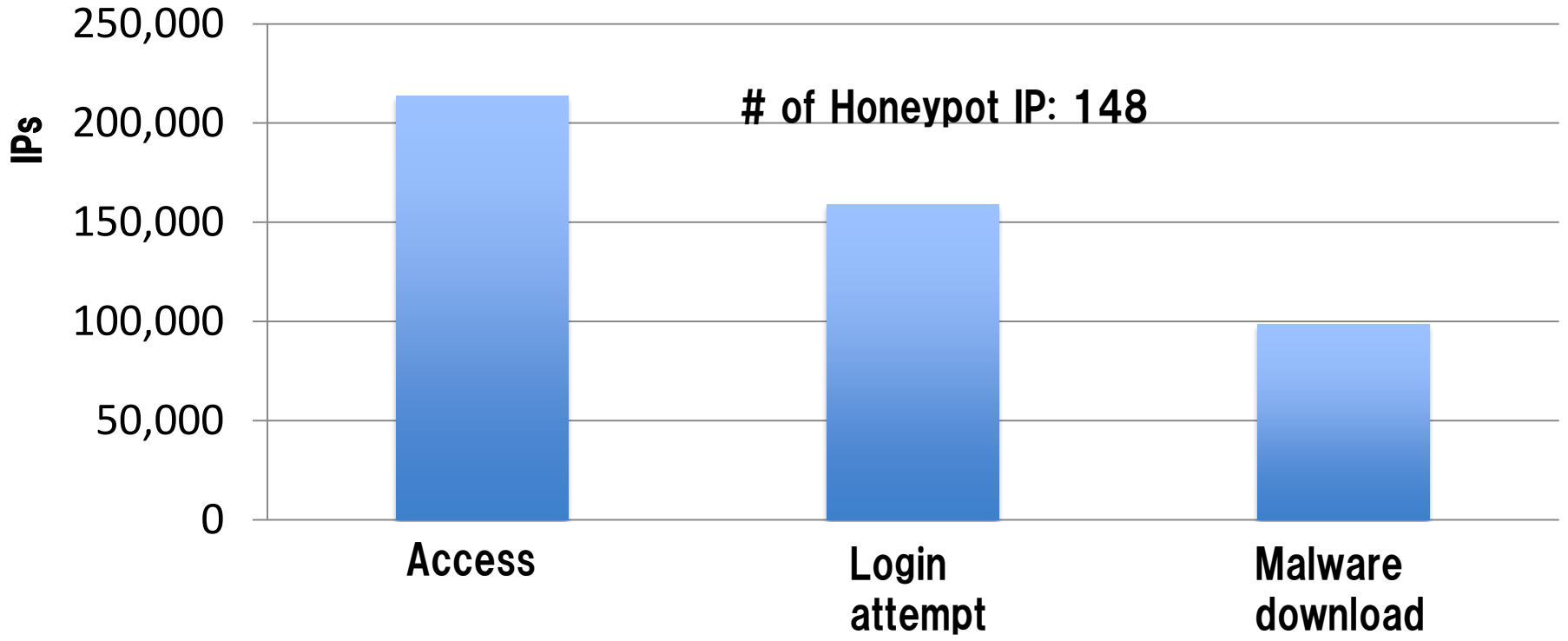
We use decoy system (honeypot) to emulate vulnerable IoT devices to monitor the attacks in depth



Yin Minn Pa Pa, Shogo Suzuki, Katsunari Yoshioka, Tsutomu Matsumoto, Takahiro Kasama, Christian Rossow, "IoTPOT: Analysing the Rise of IoT Compromises," USENIX WOOT 2015

Observation result (last year)

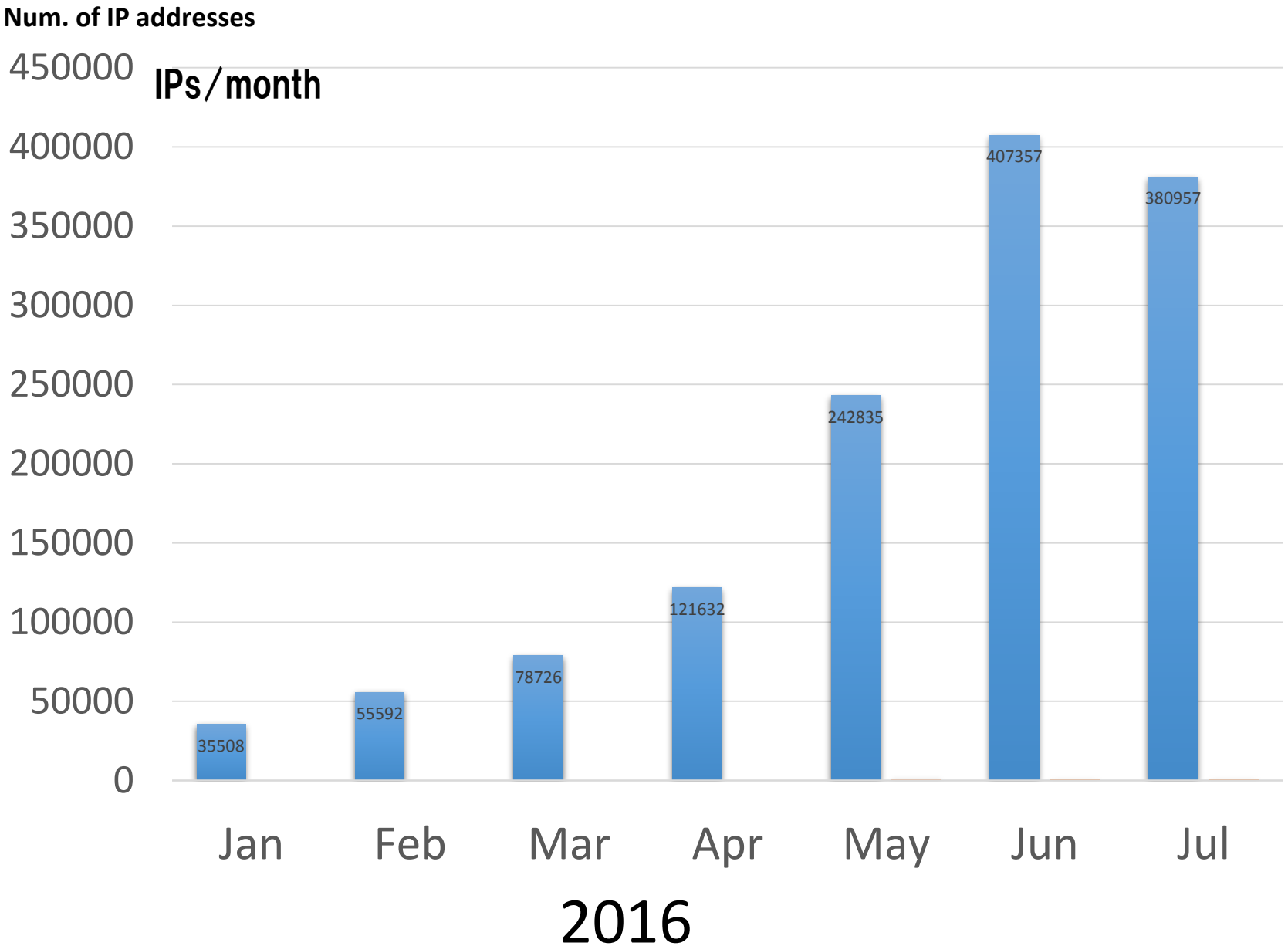
Period:2015/4/1～2015/7/31 (122days)



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

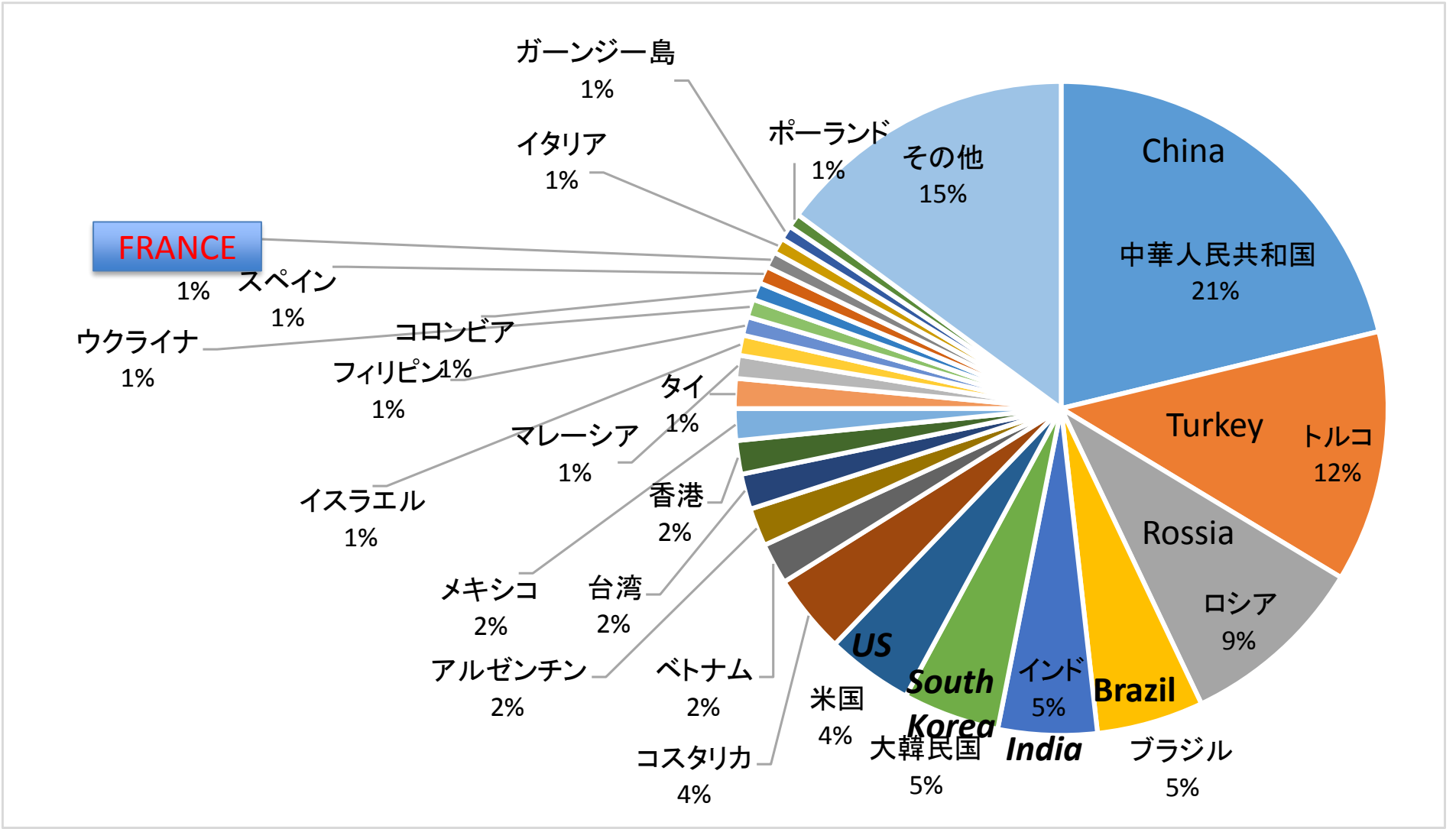
Binaries with 11 different CPU architectures
93% of the binaries were new in VT (as of 2015/9/24)

Increase of attacks



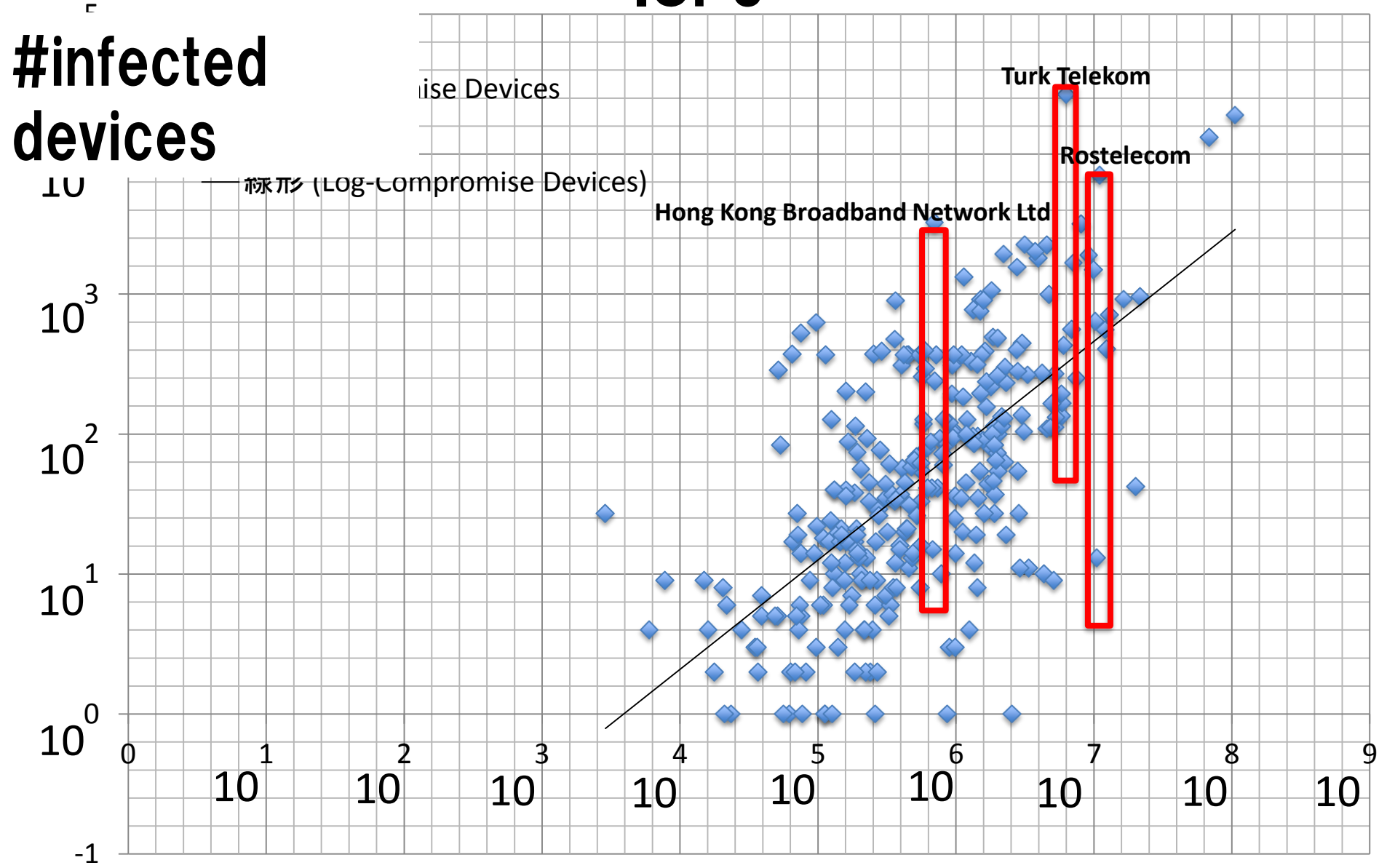
Source countries

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



ISPs

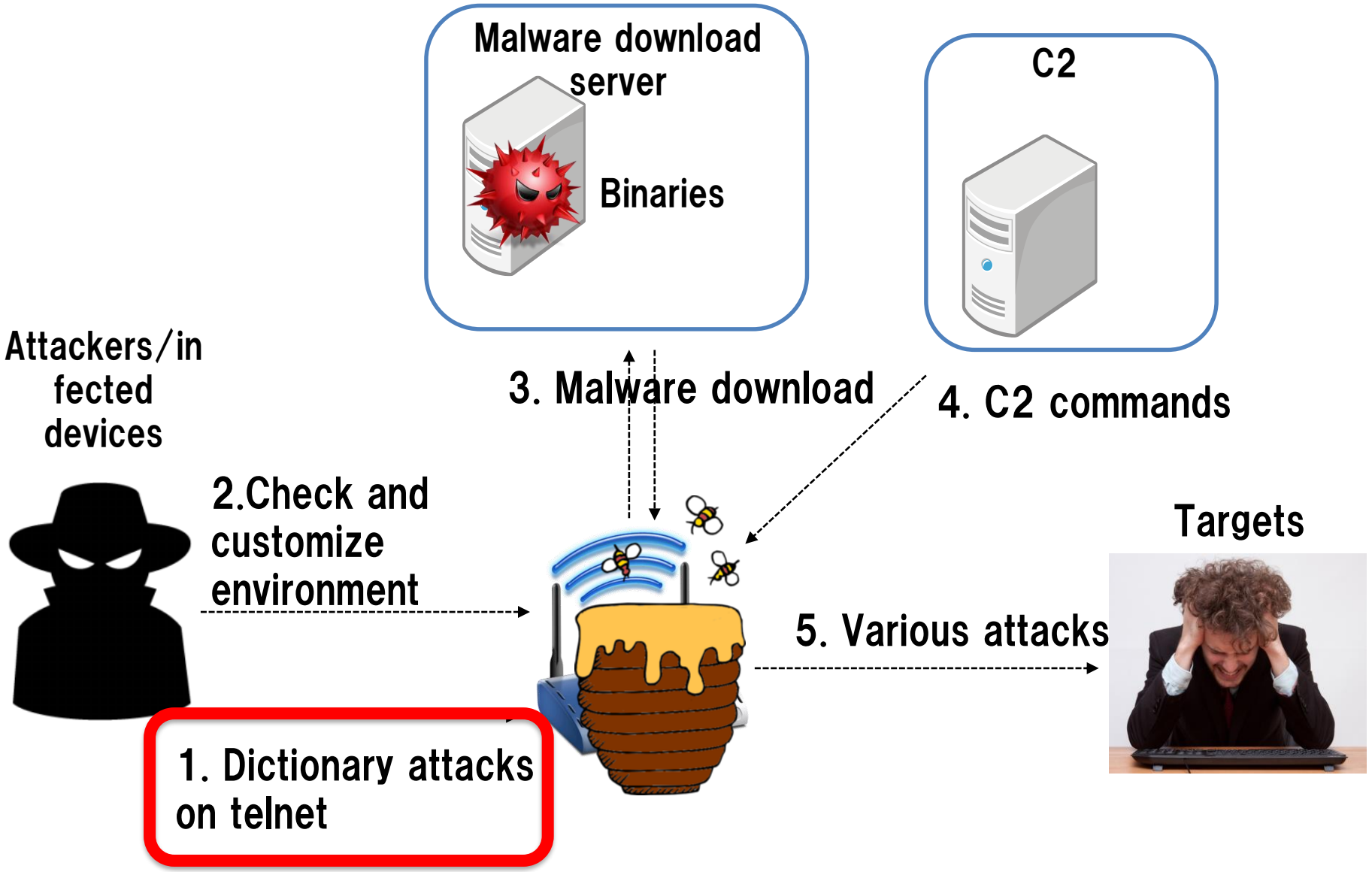
#infected devices



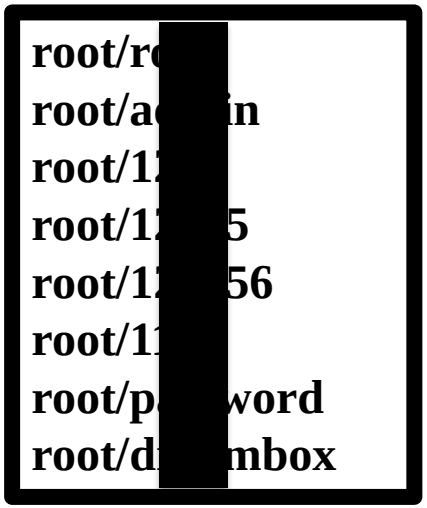
Thanks to Prof. Michel van Eeten of TU Delft for providing ISP data

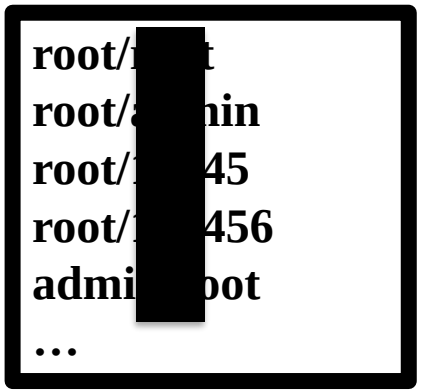
#users of ISP

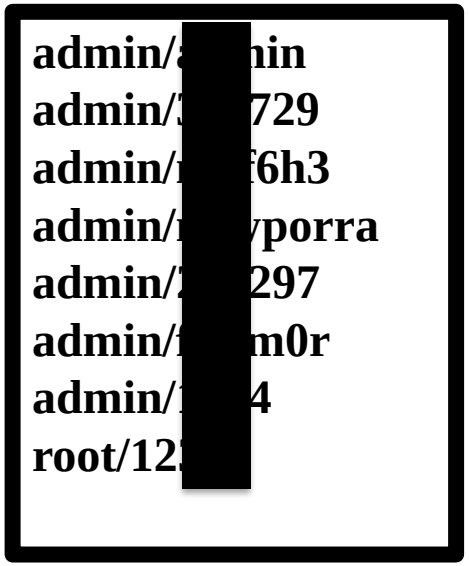
Telnet-based malware infection

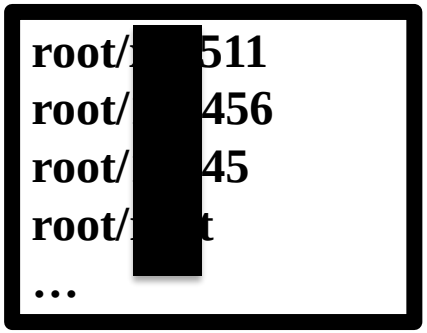


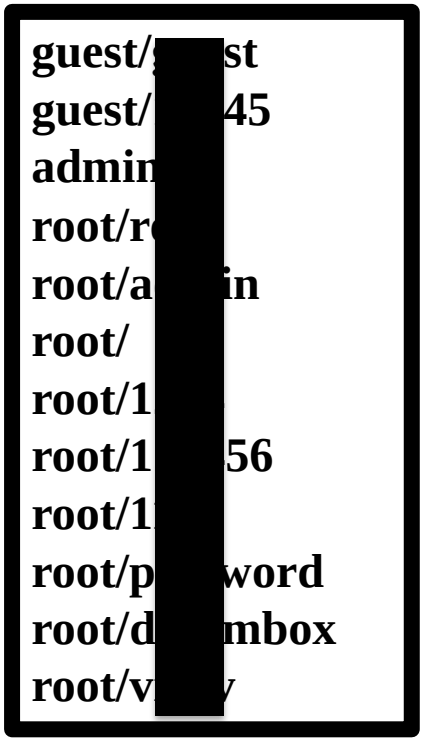
Dictionary used in 2015

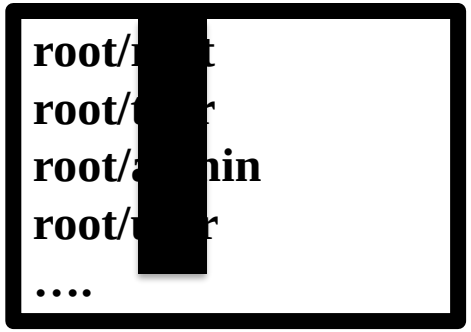




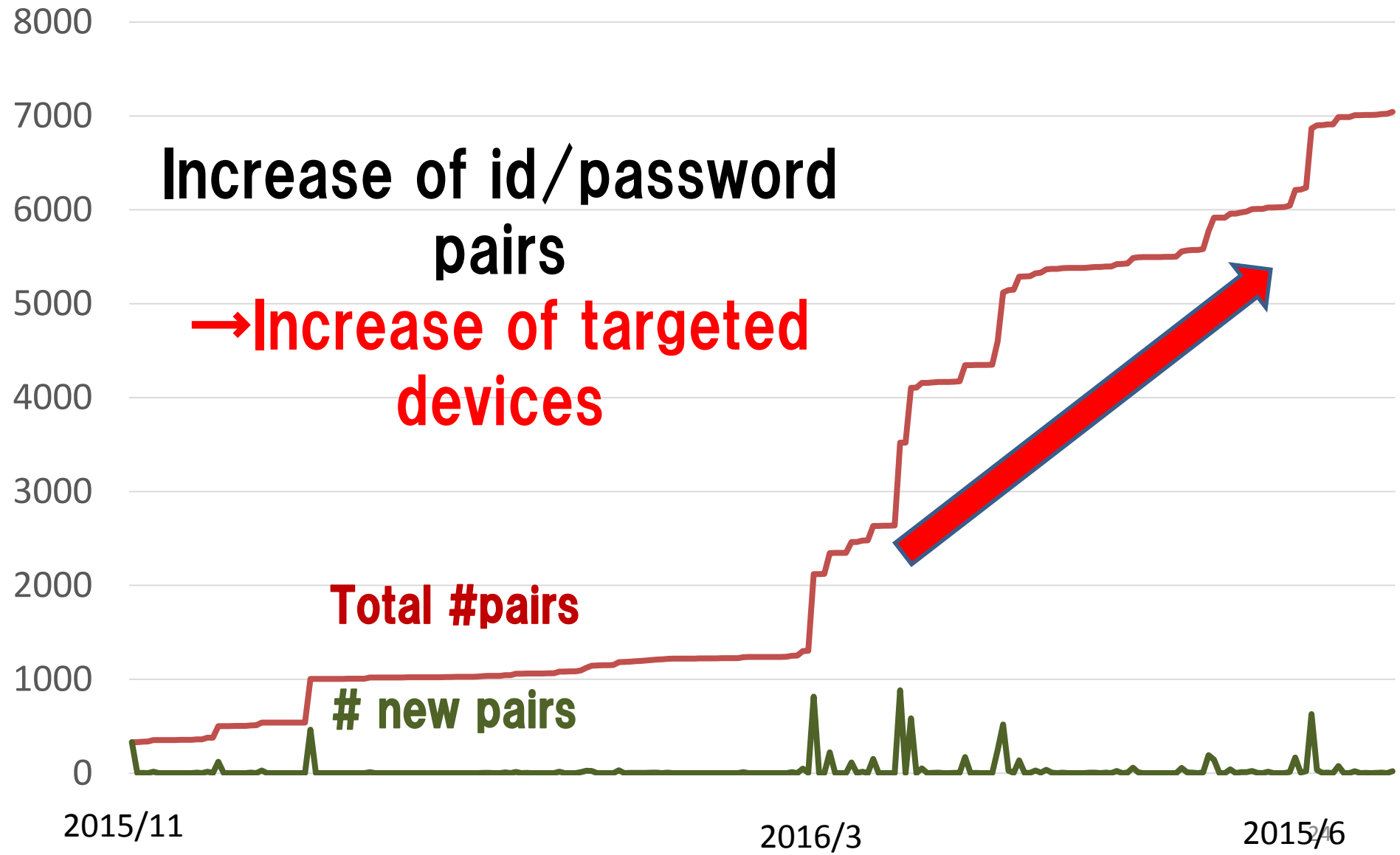




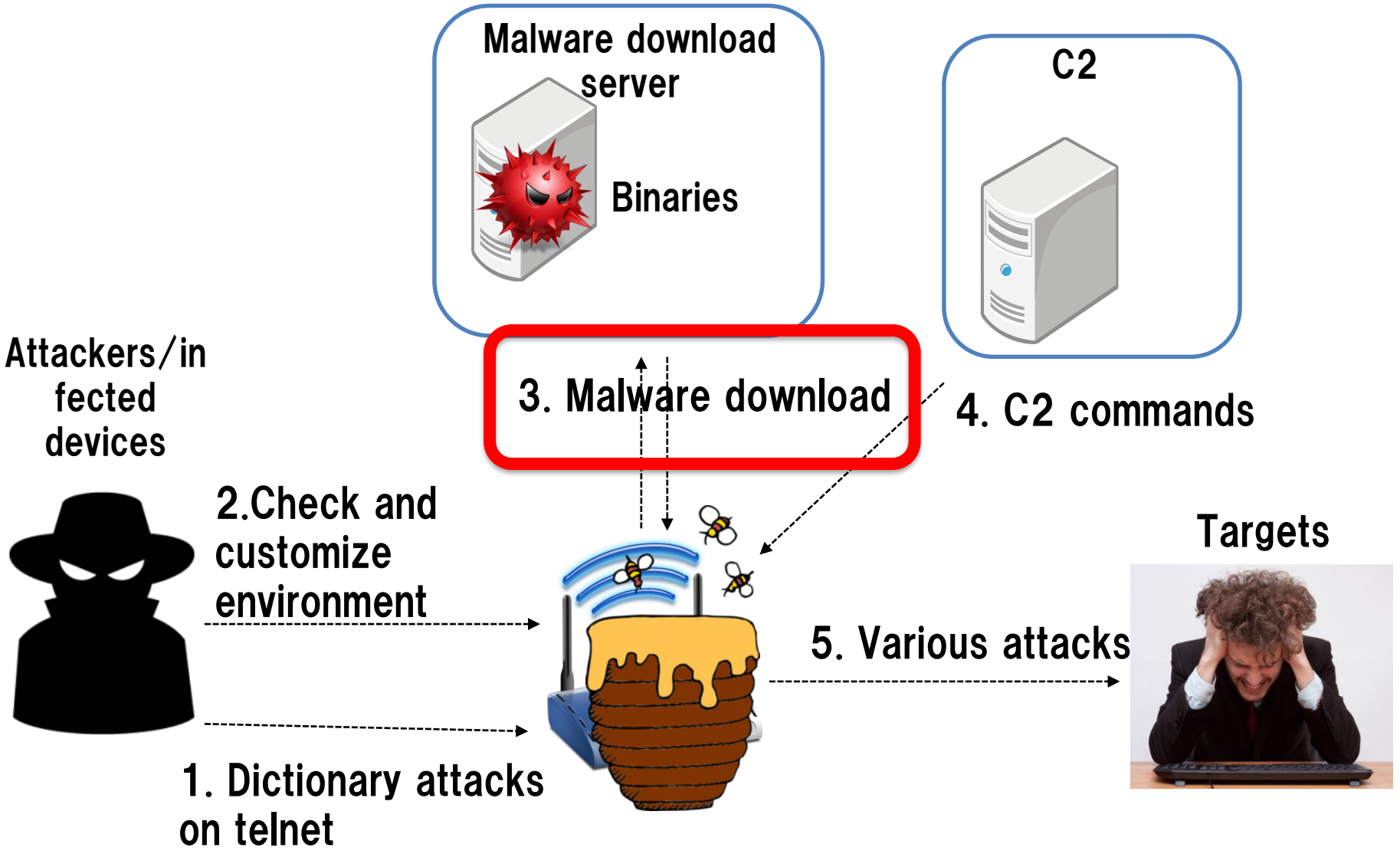




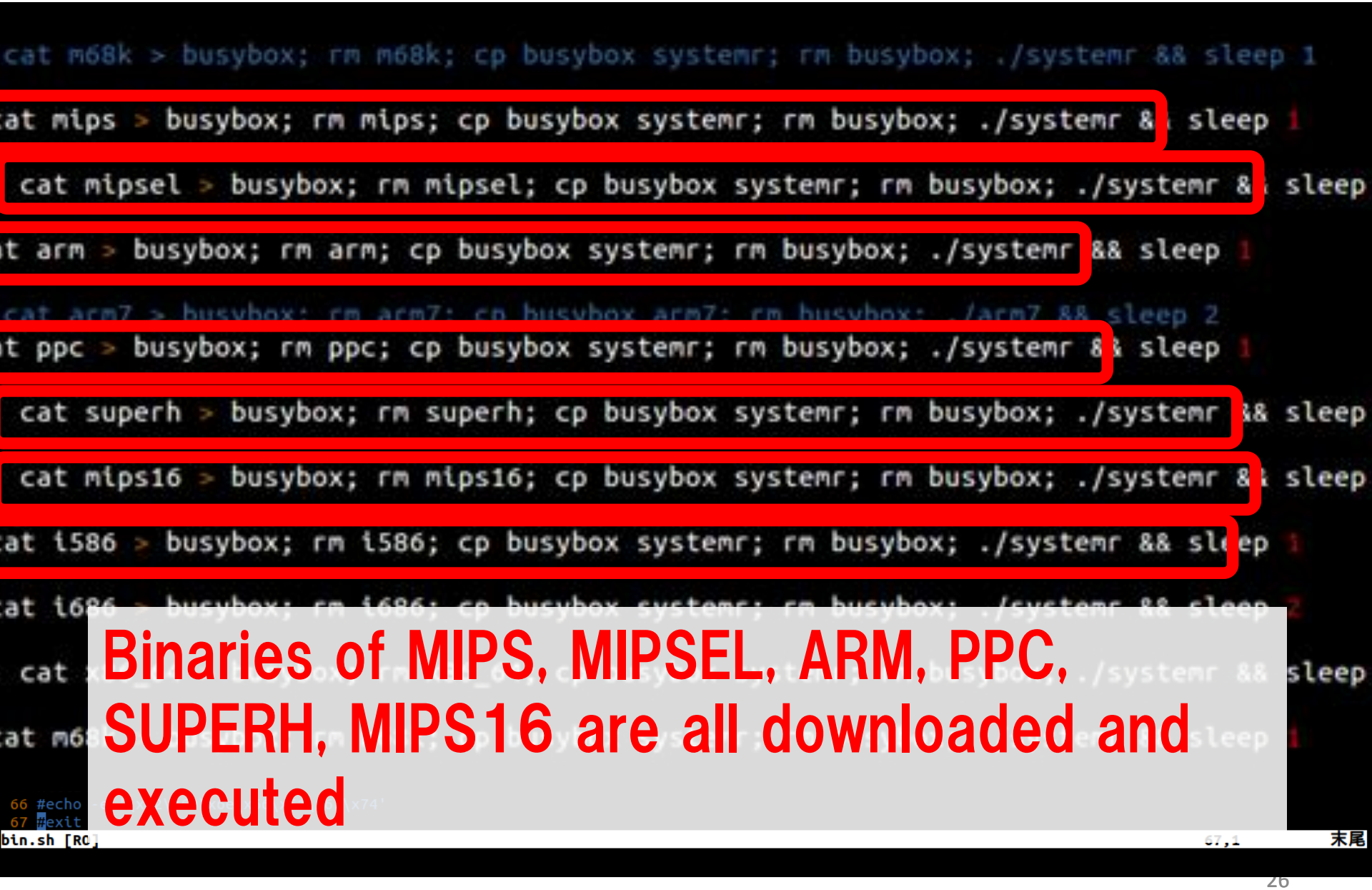
Increase of id/password pairs



Telnet-based malware infection



Eg. Malware binary downloads



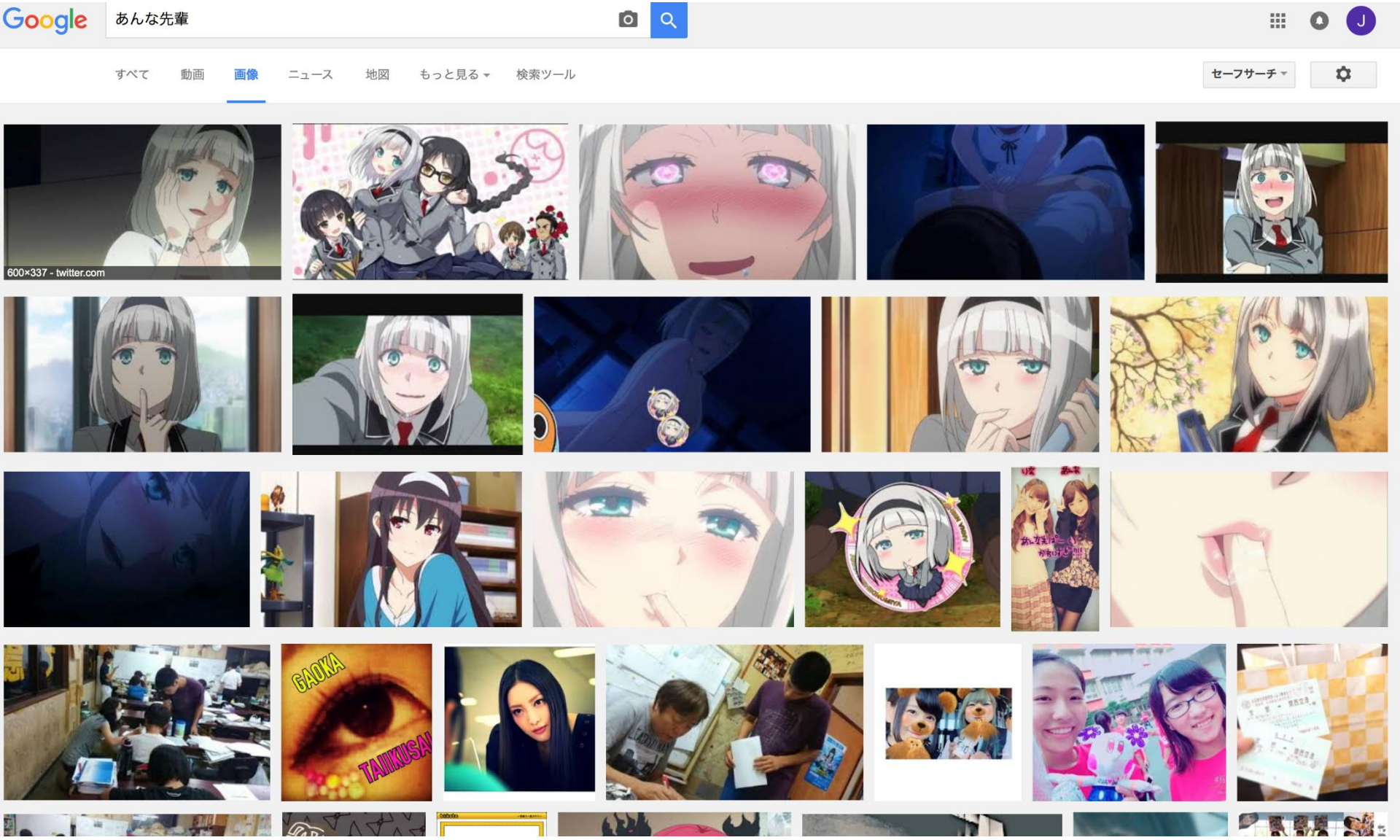
Latest IoT malware

<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
    - Destrination 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.



The Attacker may be very OTAKU (Comic fanatic).

Further information on “Mirai”

DDoS Attacks

- Krebs on Security（16/9/20）
  -Akamai Service

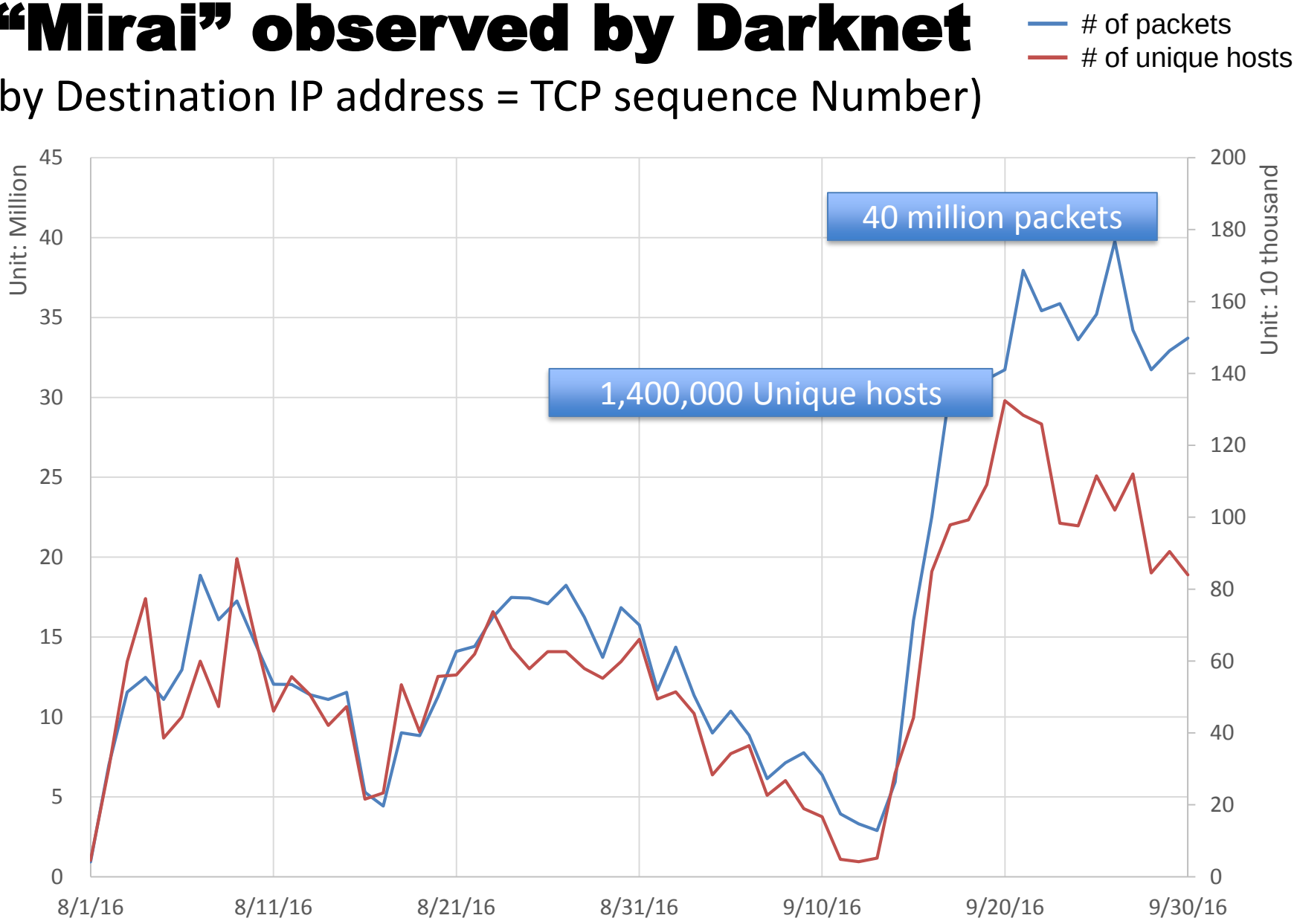
- DNS of DYN (16/10/21)
  -Netflix
  -Twitter
  -Amazon

- Types of Infected:
  -Printer
  -Camera
  -Router
  -DVR and etc.

- Architecture used:
  -ARM
  -ARM7
  -MIPS
  -PowerPC
  -SH4
  -SPARC
  -X86

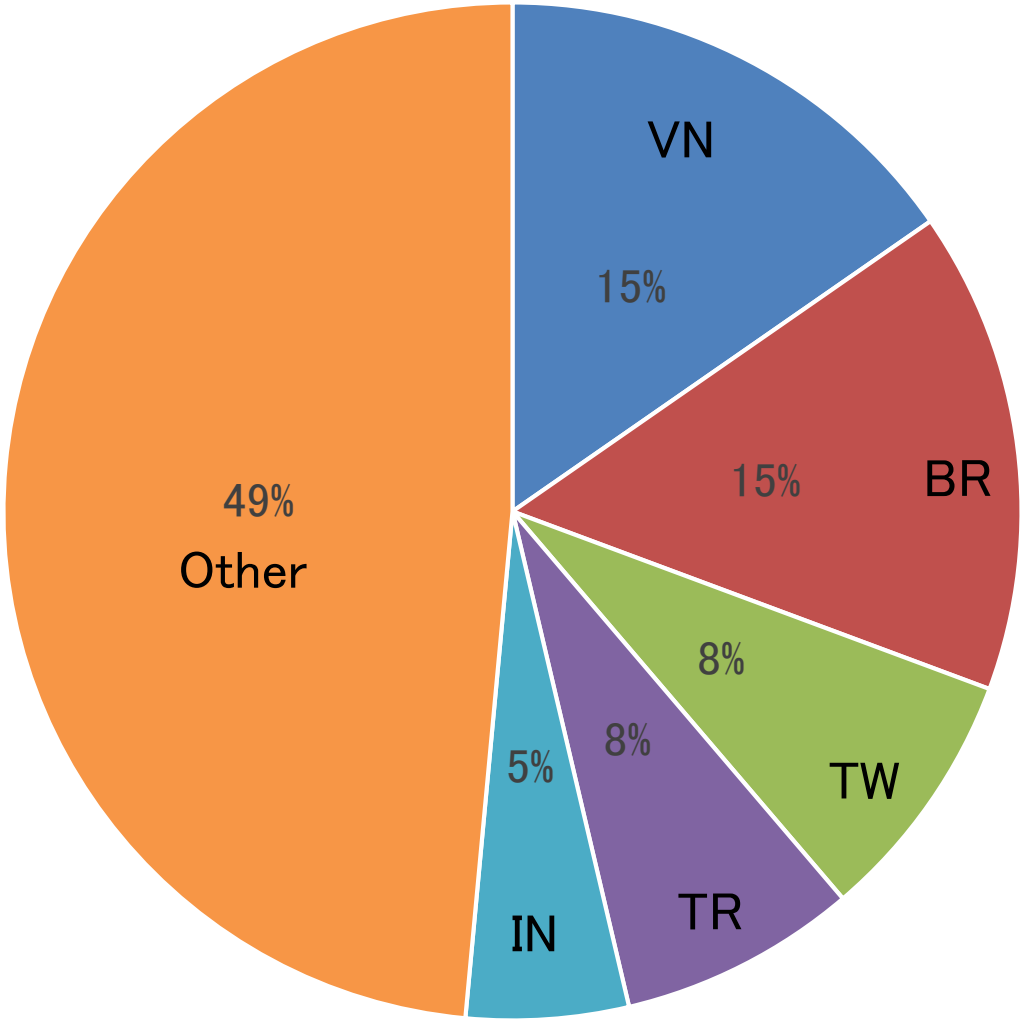
“Mirai” observed by Darknet

(by Destination IP address = TCP sequence Number)

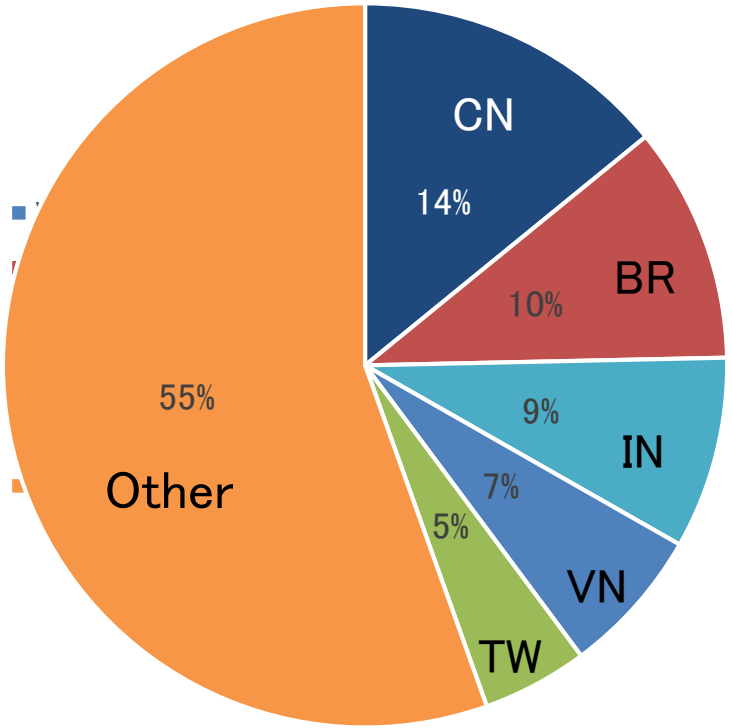


Starting from 1st of August. After source code uploaded, scan was jumped up

Countries infected by Mirai from Source IPs

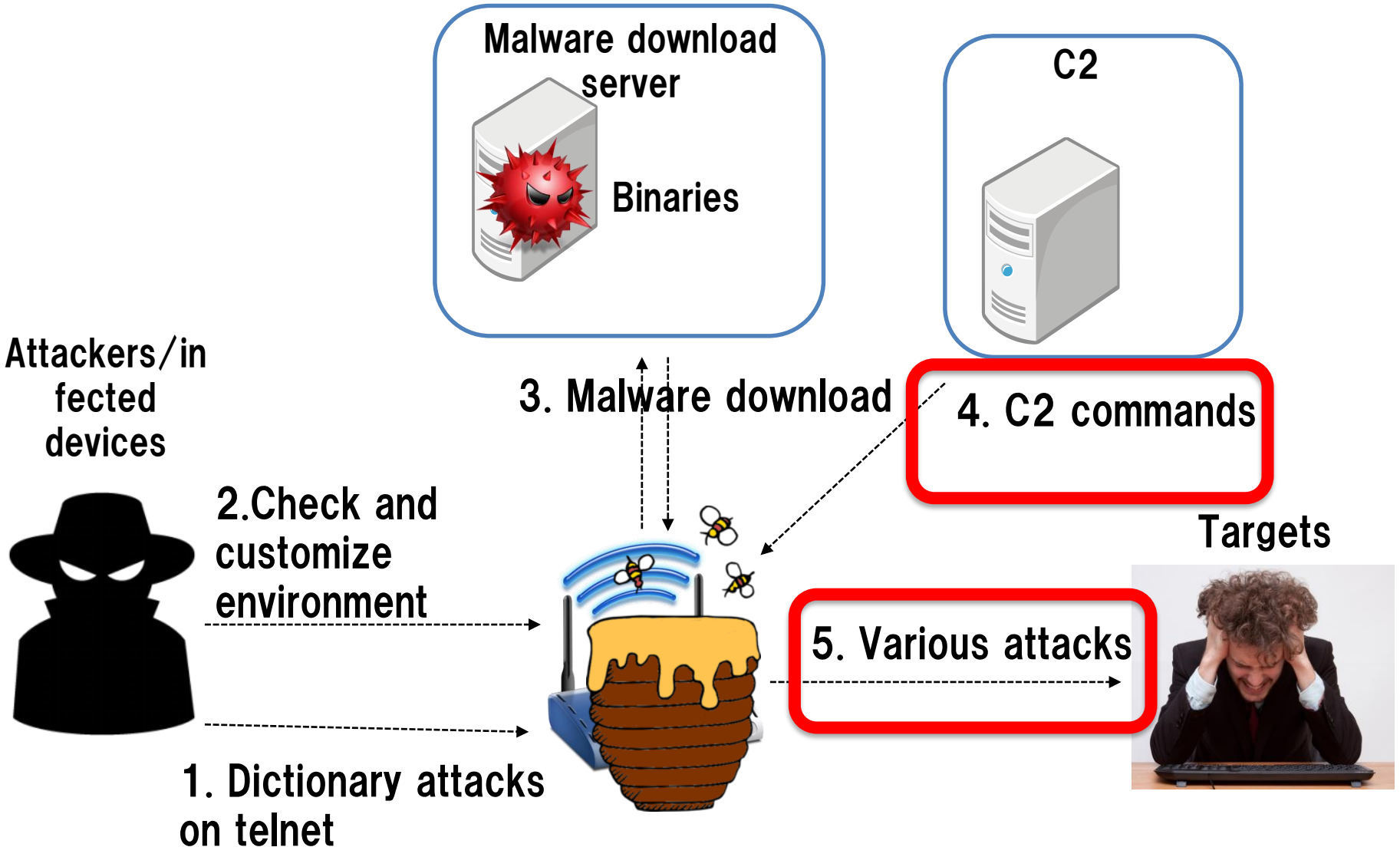


Countries infected by Mirai
After August 2016

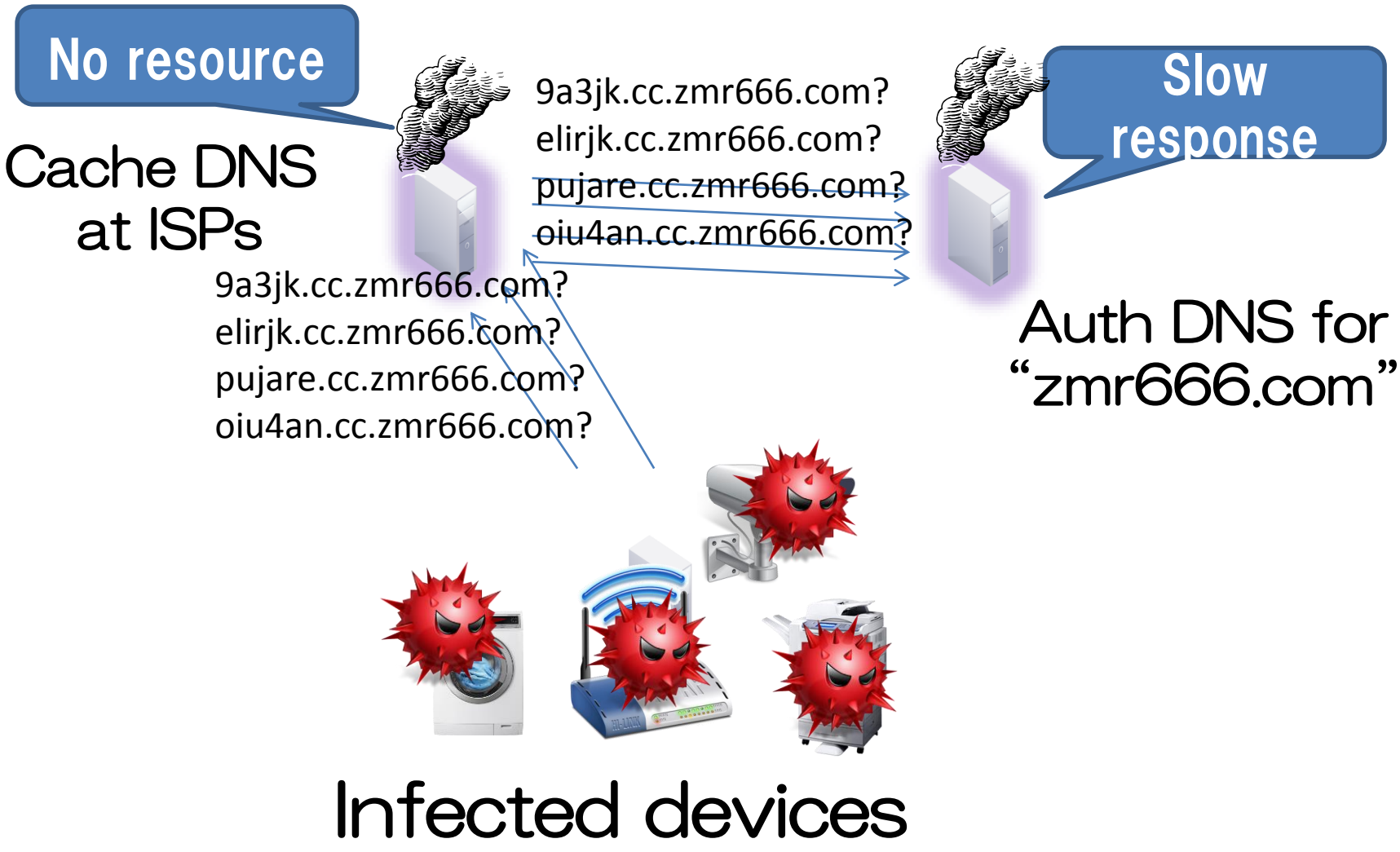


Courtiers infected by IoT malwares
Before August 2016

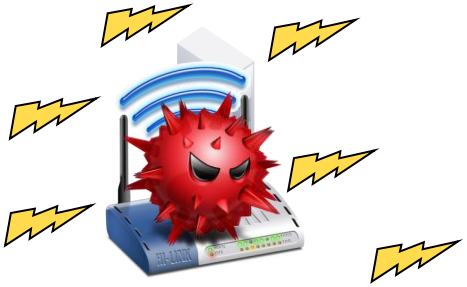
Telnet-based malware infection



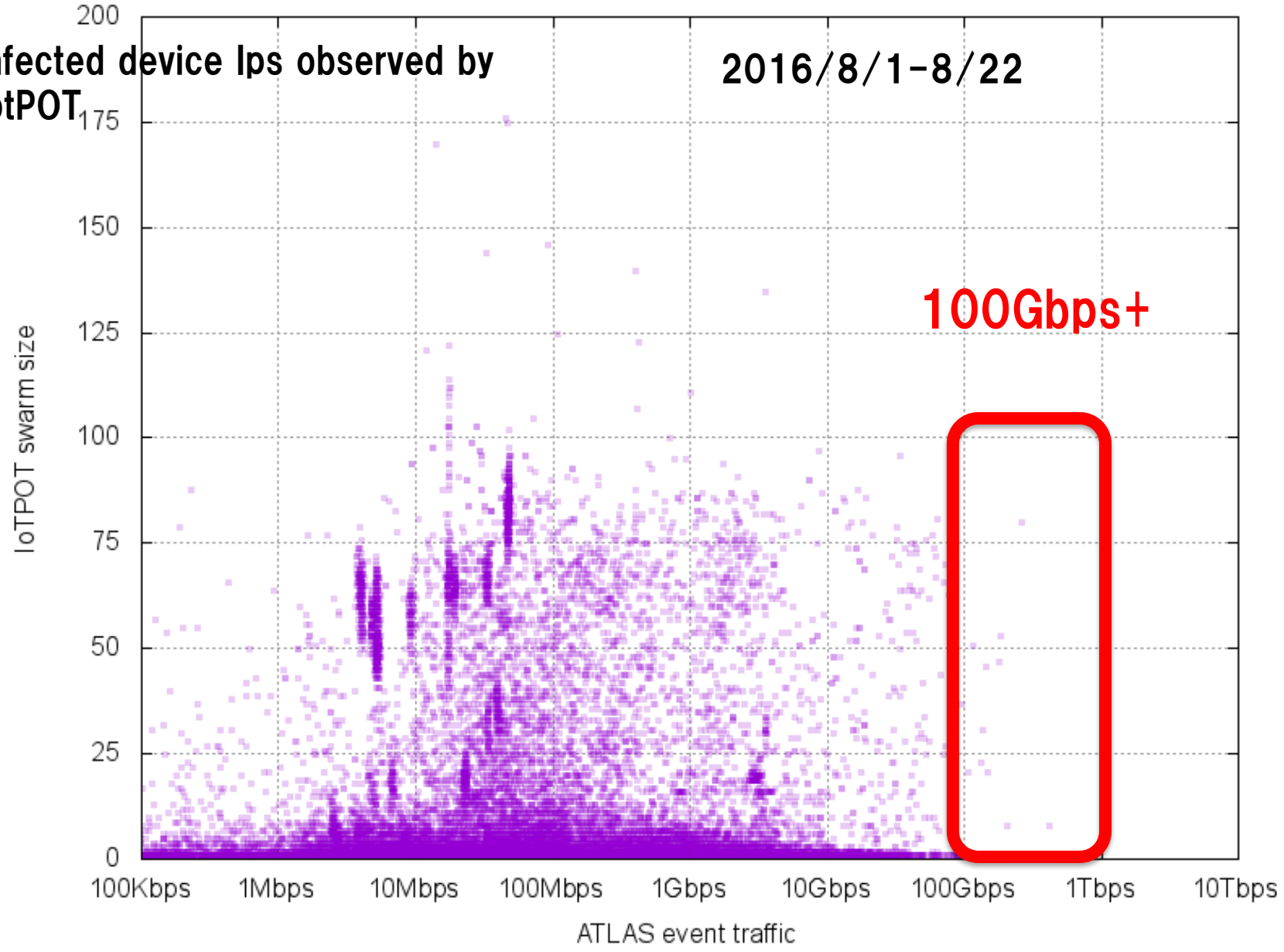
Dinial of Service (DoS)



Propagation



Infected devices



Size of attacks Arbor networks observed

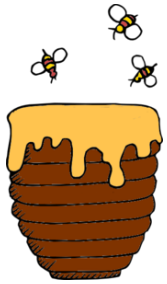
The matching result is provided by Arbor Networks ASERT Japan

Two approaches to monitor attacks

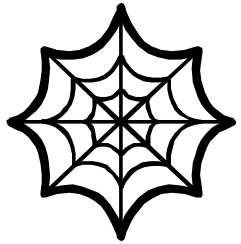
- **Passive monitoring**
  Prepare network to monitor attacks and wait
  - Darknet monitoring
  - Honeypot

- **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



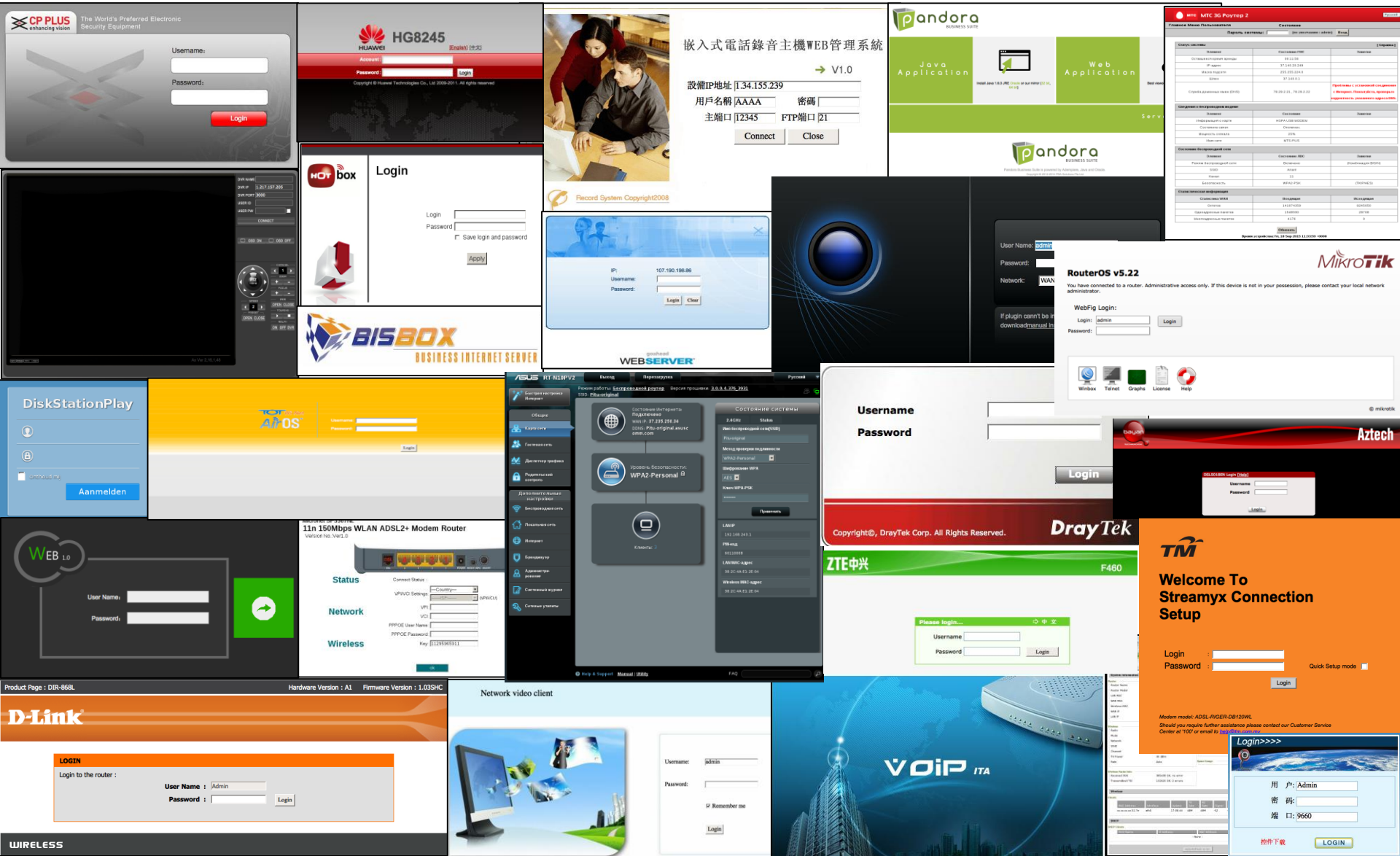
Honeypot



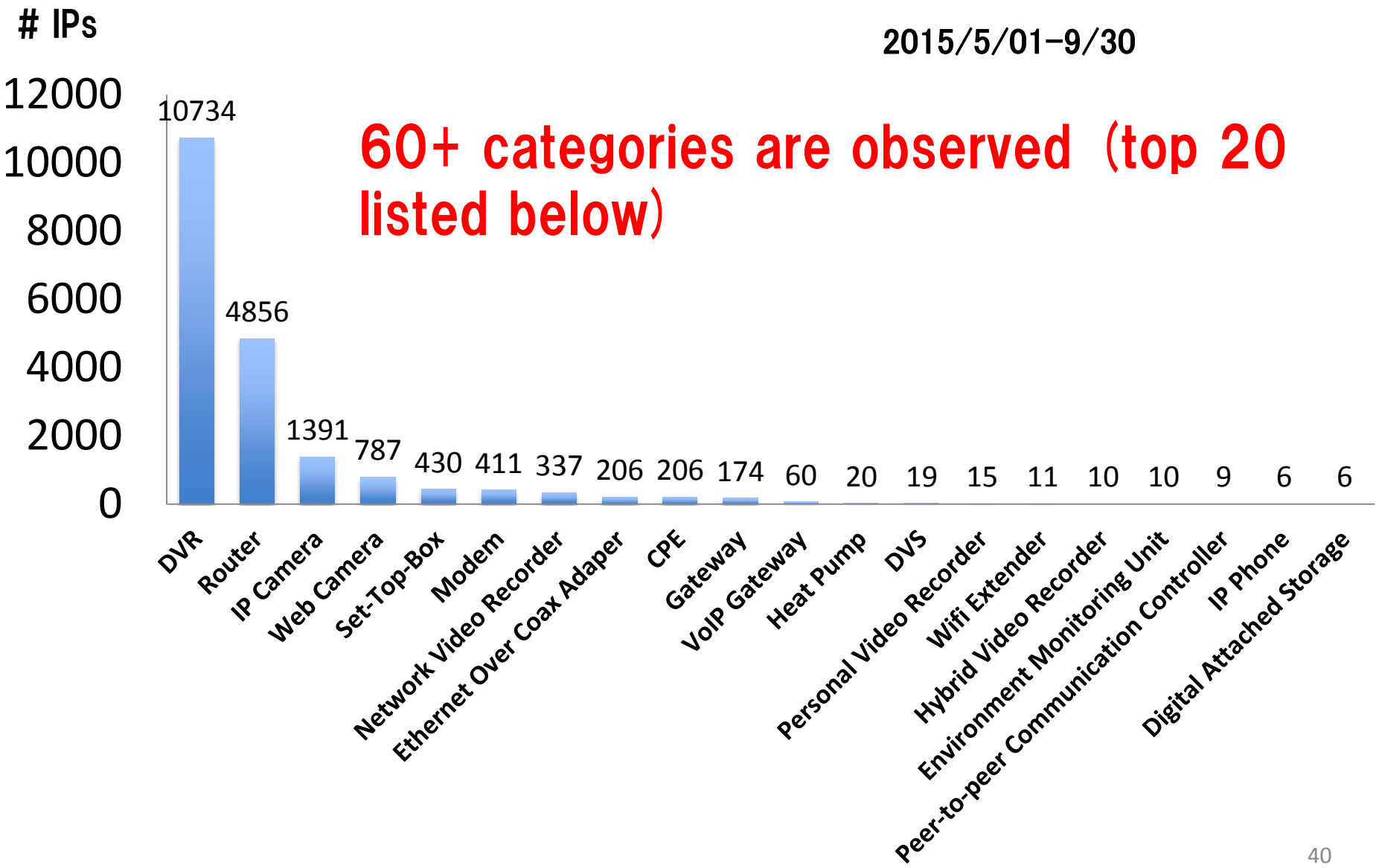
Darknet

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

Examples of web interfaces of infected devices



Device categories



Categories of Inferred Infected devices (2016.9)

- Surveillance camer
  - 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/indivisuals

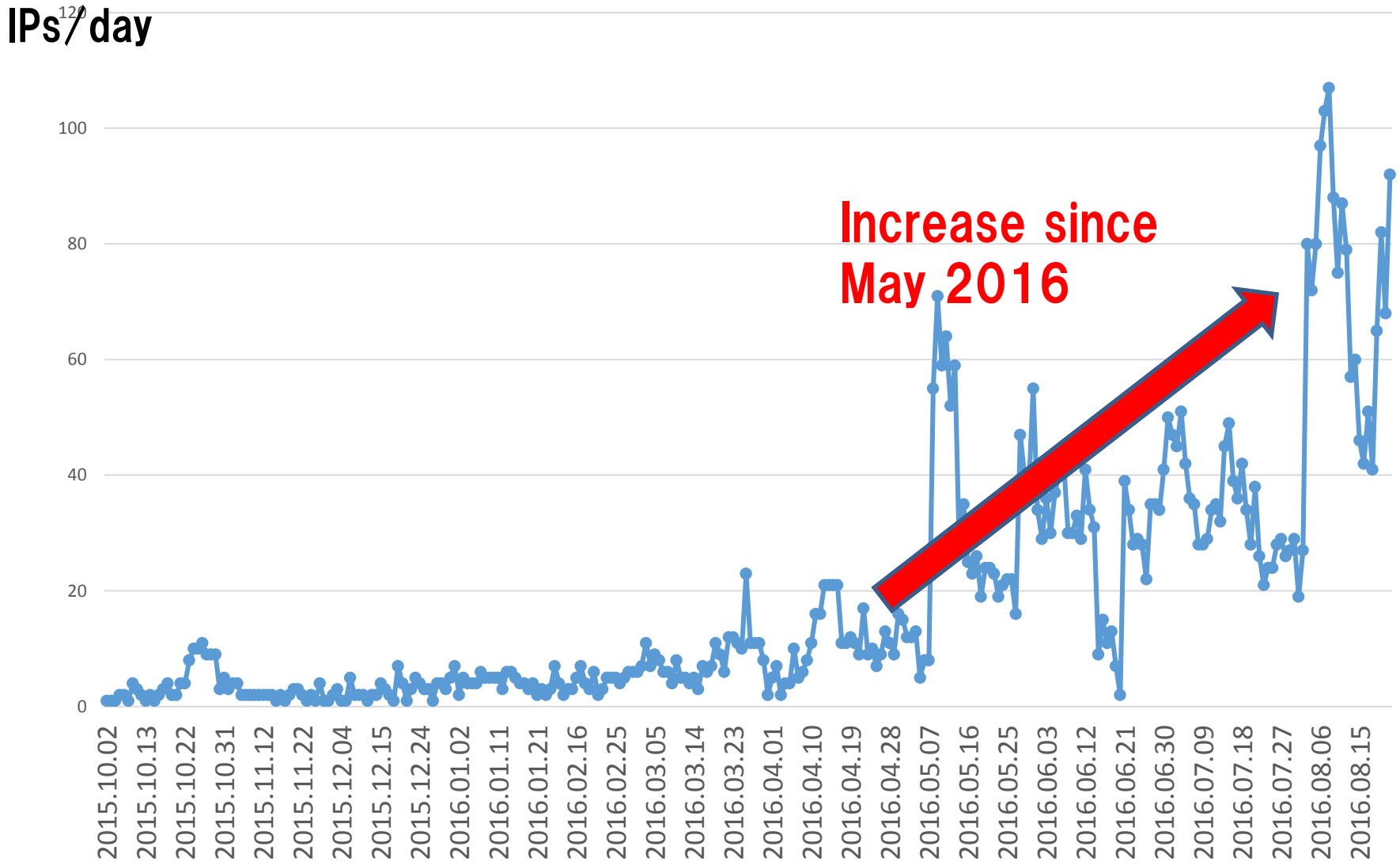
- Web cam, Video rec
- Home automation GW
- Solar Energy Control System
- Energy demand monitoring system


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

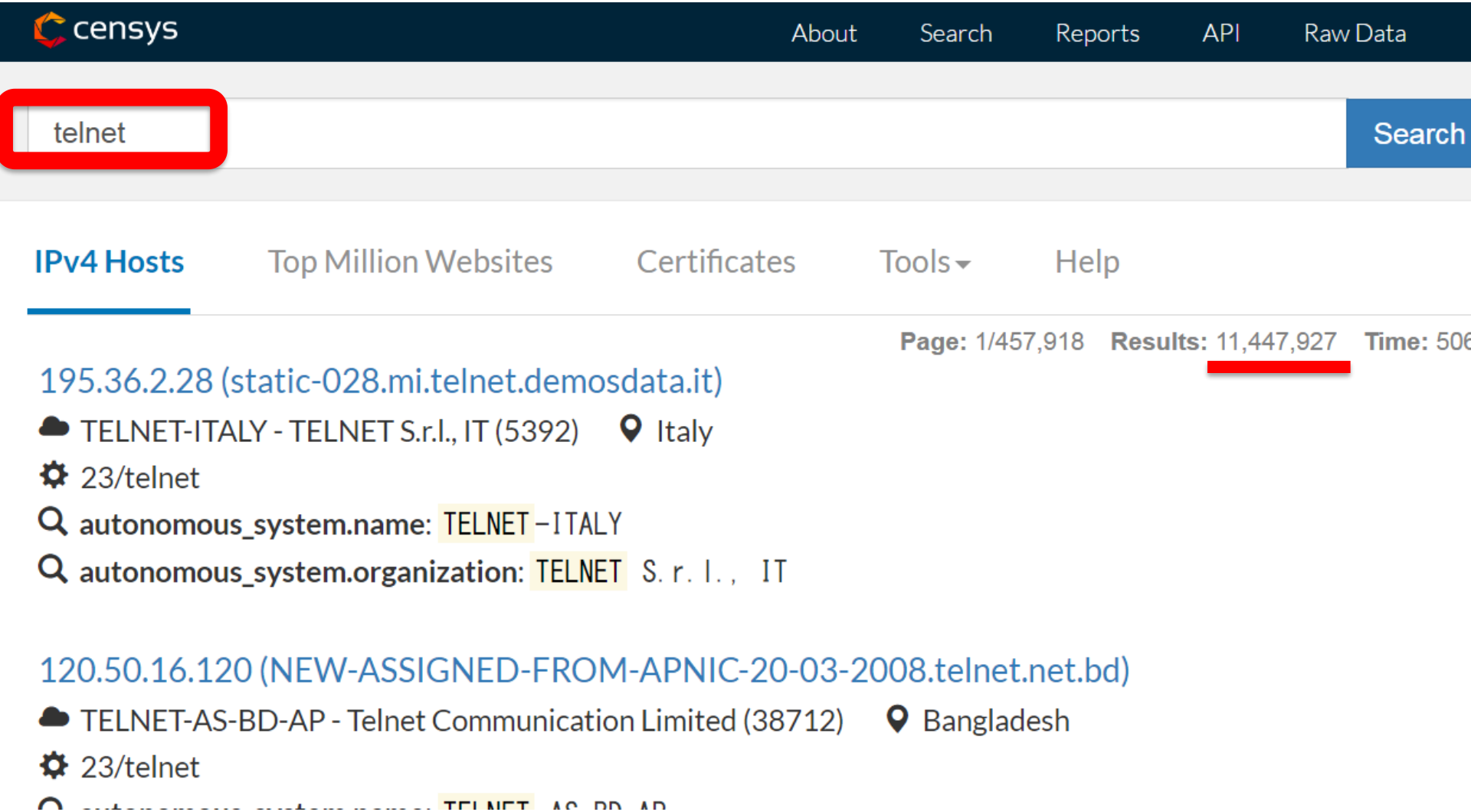


- Etc
  - Heat pump
  - Fire alert system
  - Medical device (MRI)
  - Fingerprint scanner

Infected devices in Japan (Daily count)



Potential victims?



Other vulnerabilities?

Other vulnerabilities

- IoTPOT implements following vulnerabilities exploited in the wild
  - DVR configuration leak

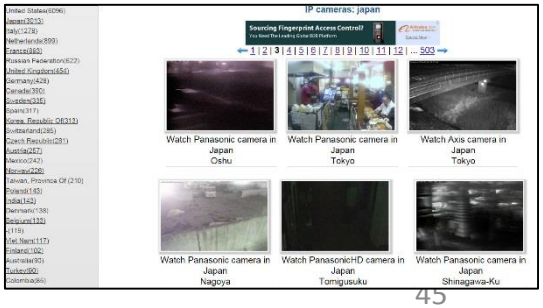
    Config files of Several DVR manufacturers can be accessed from WAN [7]

  - 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/

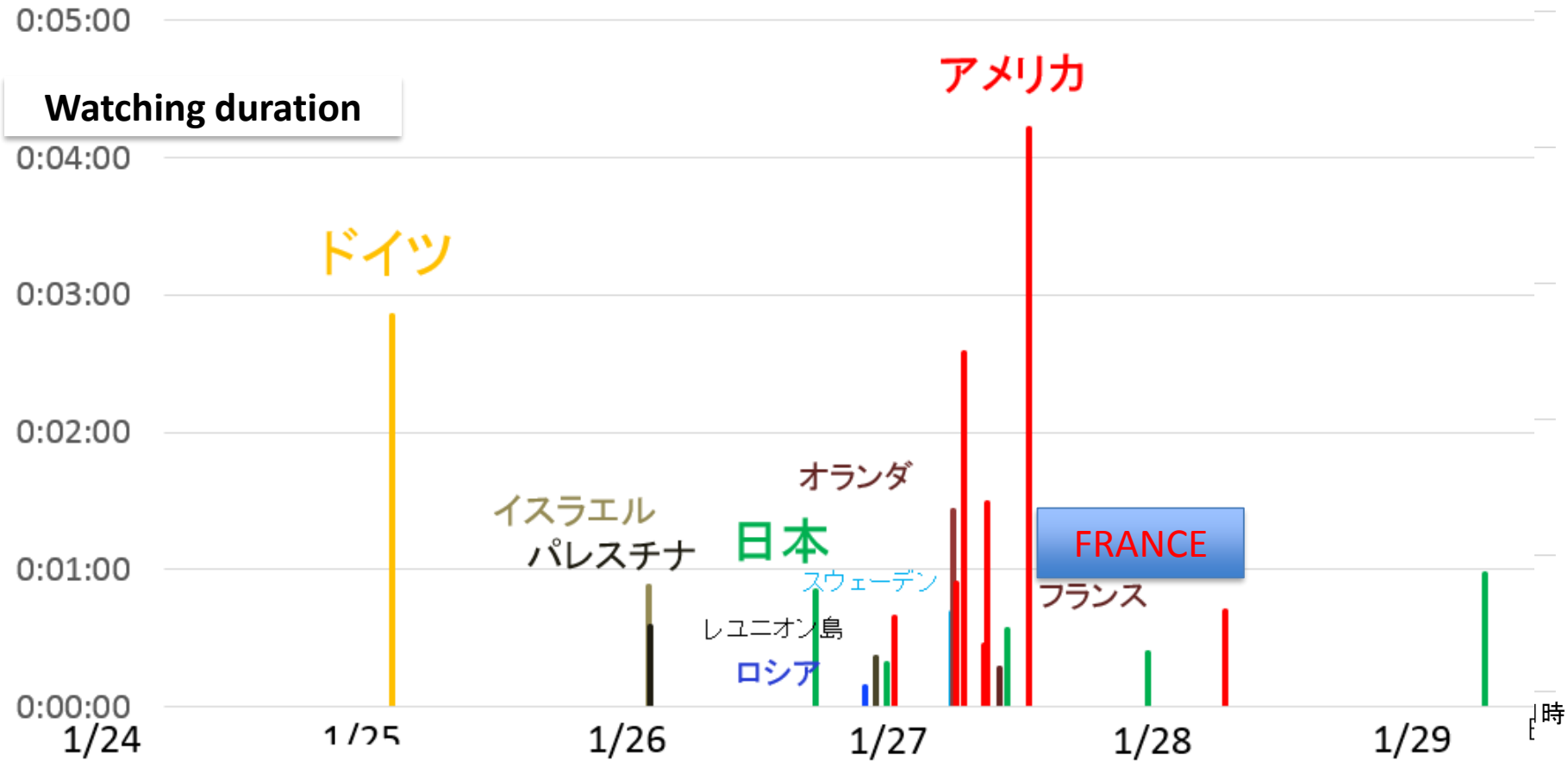
Insecam


PanasonicHD
Linksys
Sony
TPLink
Foscam
Netcam
New online cameras
Sitemap by cities
Add surveillance camera
FAQ
Contacts
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)
Japan was
No 3
(2016/9/15)
IP cameras: united states
10 | ... 1099
Watch Sony camera in
United States
Aurora
Watch Sony camera in
United States
Groton
City
Kitchen
Sport
Cofeehouse
Service
Entertainment
Interesting
Village
Server
Religion
Mall
Square
Barbershop
Airline
Animal
Warehouse
Bar
River
Beach
Construction
Guess

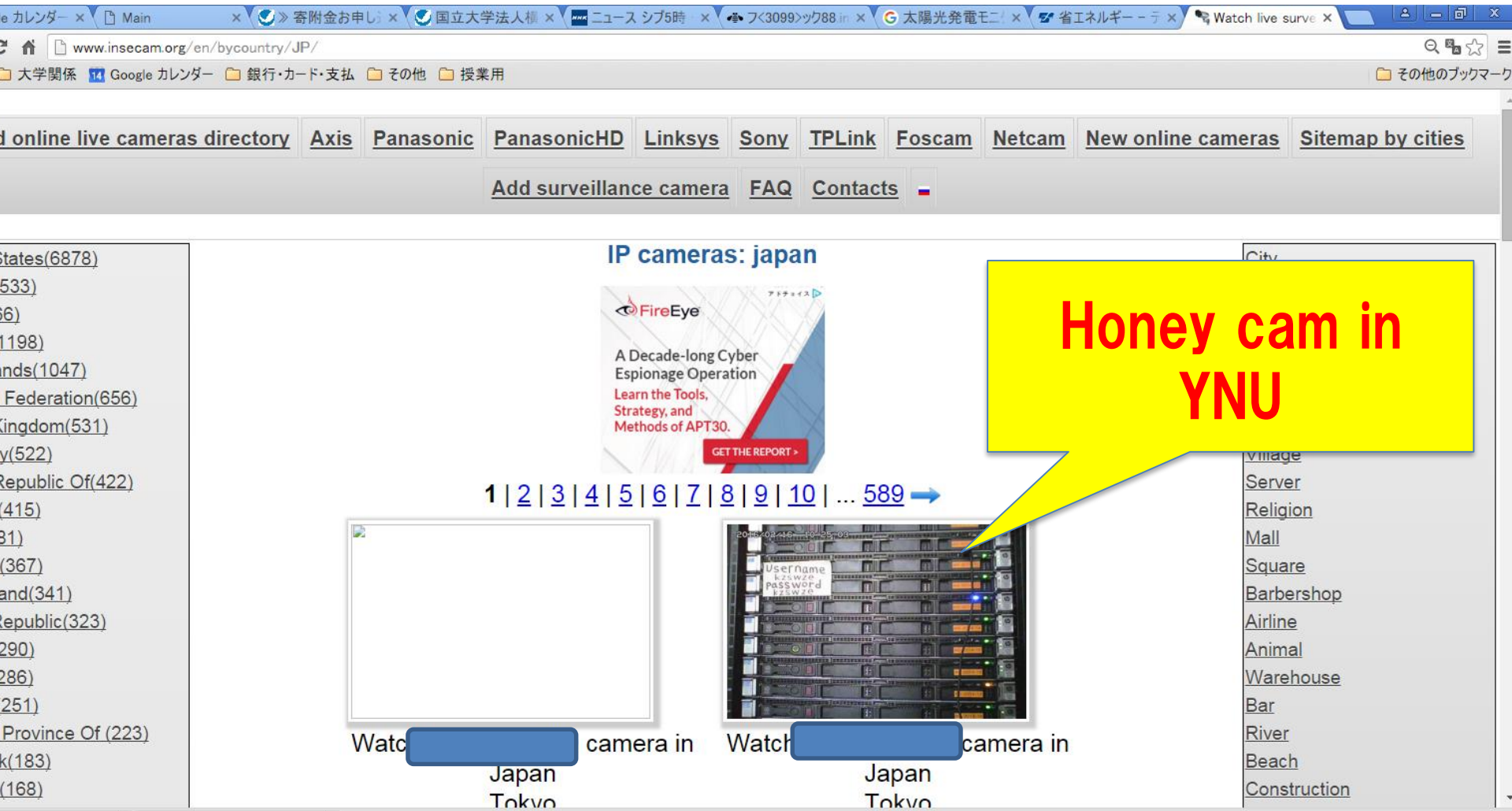
Honey IP cam at YNU

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

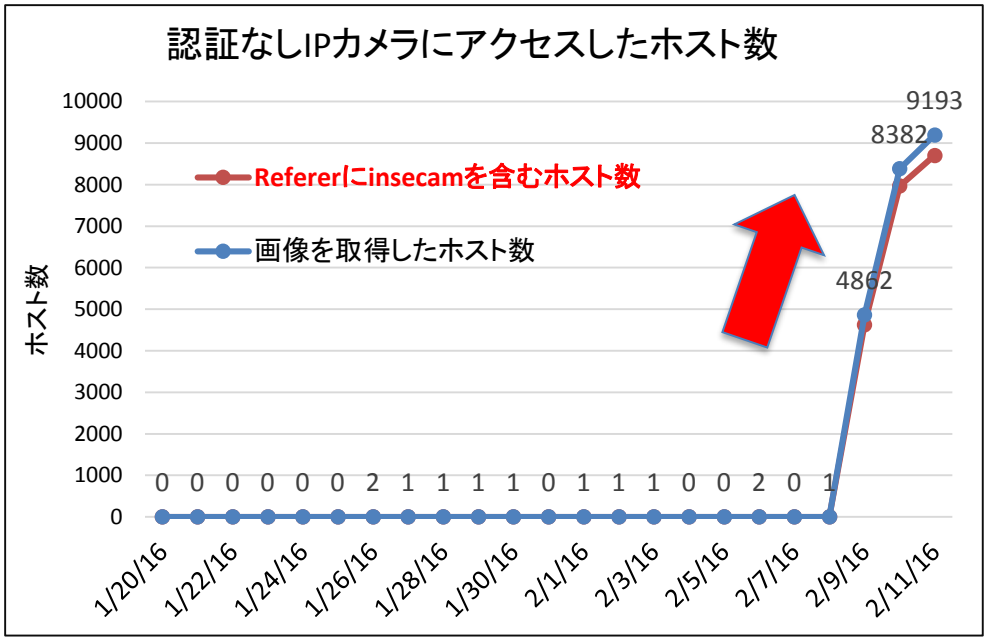


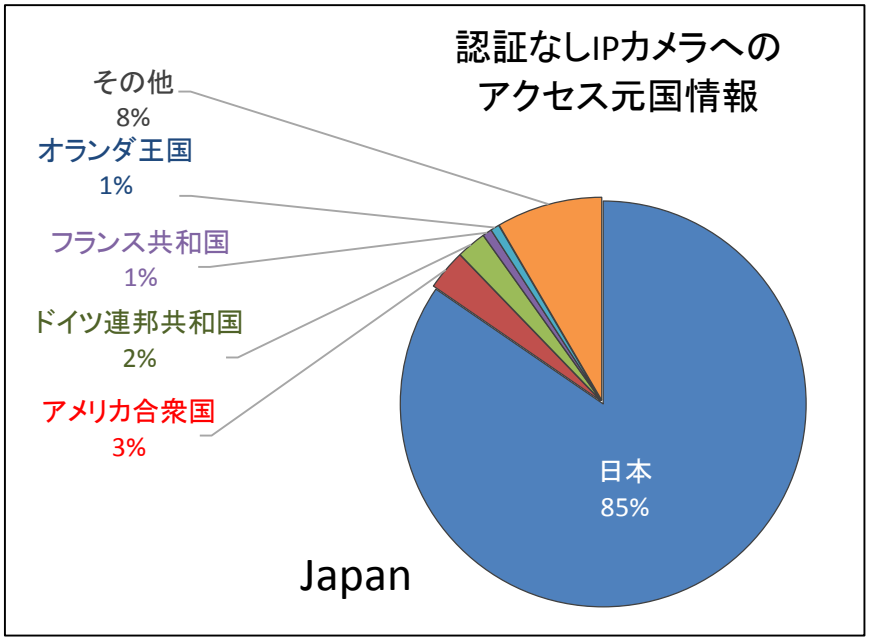
Honey cam was on Insecam!



Insecam attracts 1000+ times accesses

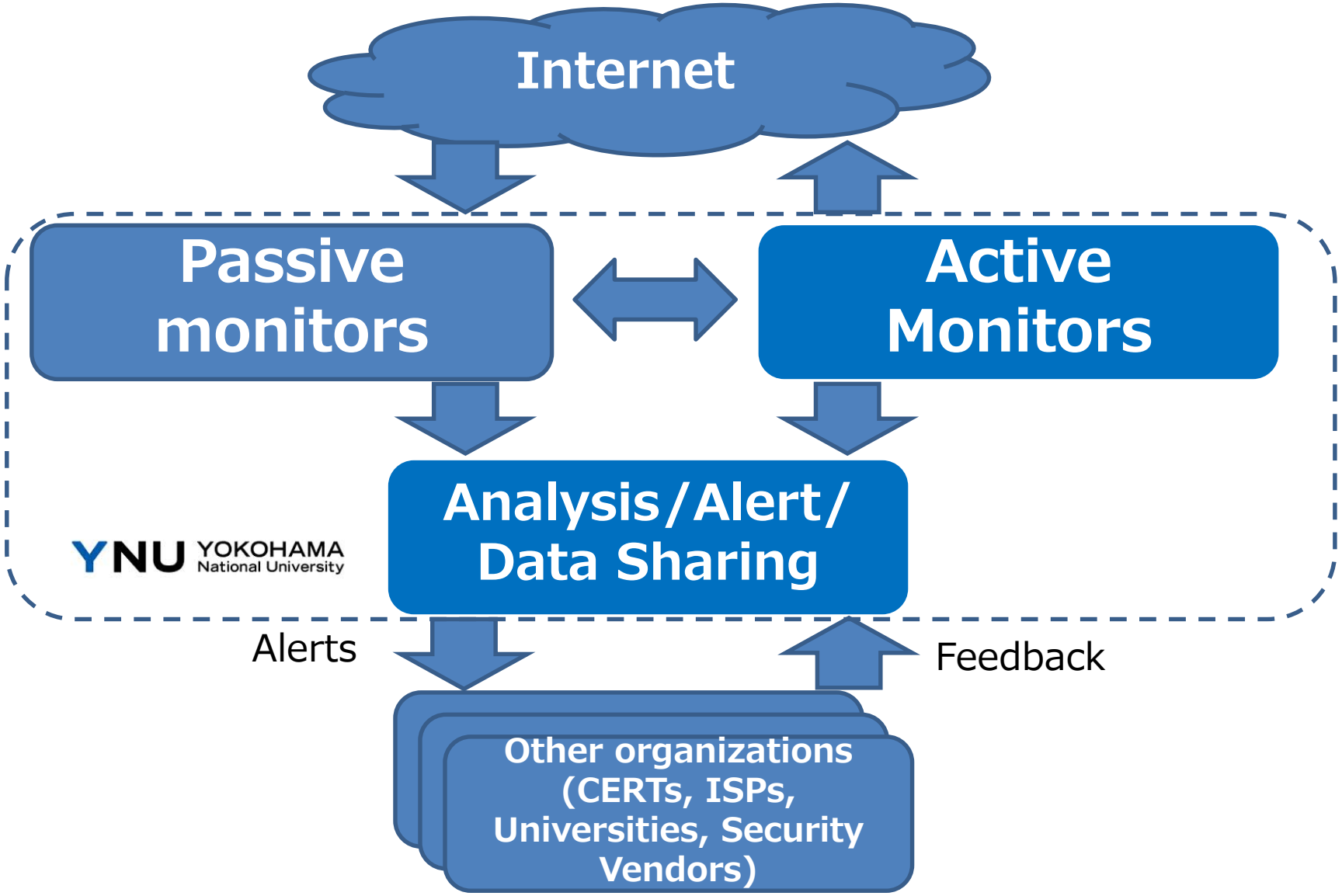
- **After our honey cam is on Insecam, accessing hosts are 1000+ times more!**
- **80% from Japan**



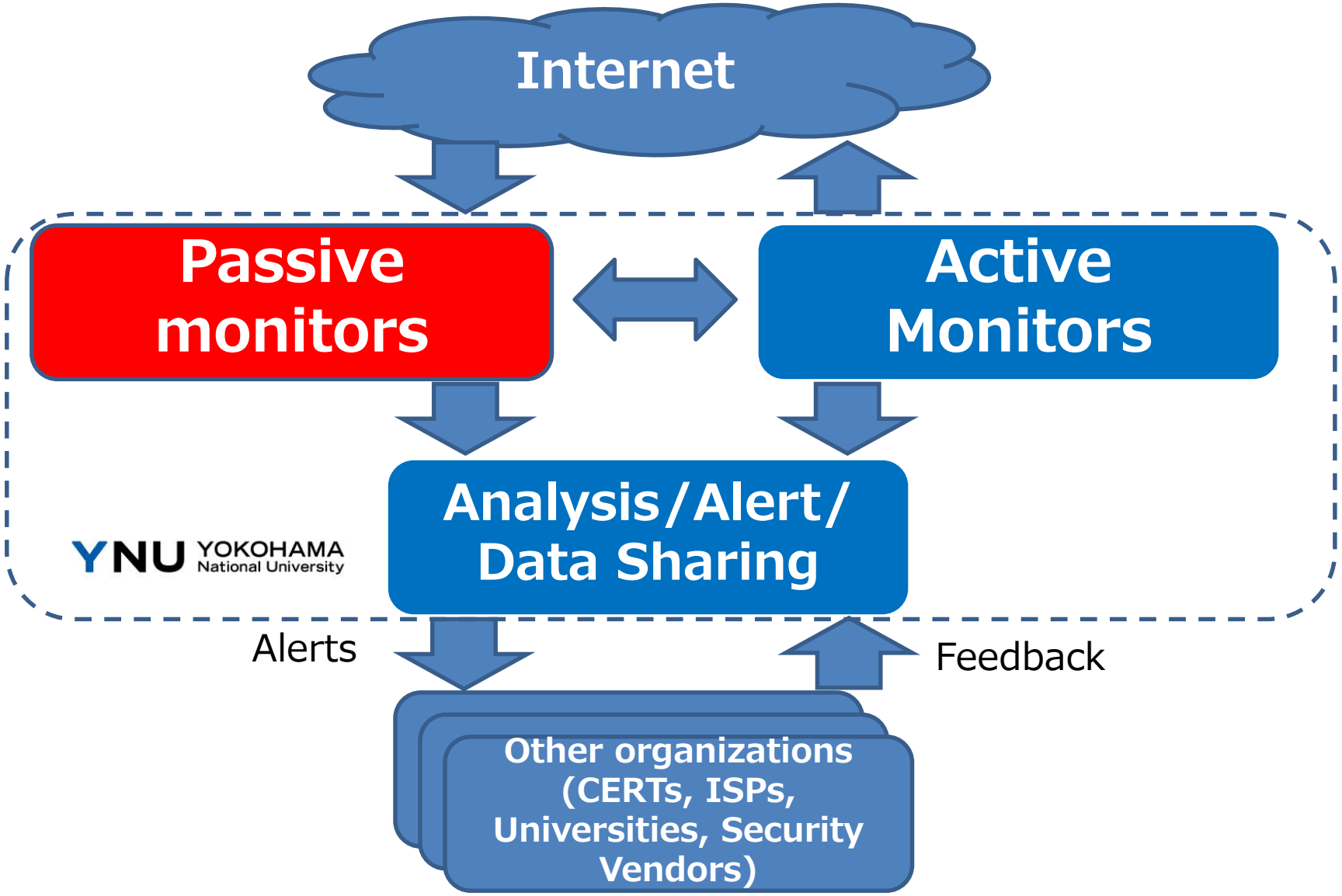


People do not scan for cameras but simply look at those sites (insecam, shodan, etc)

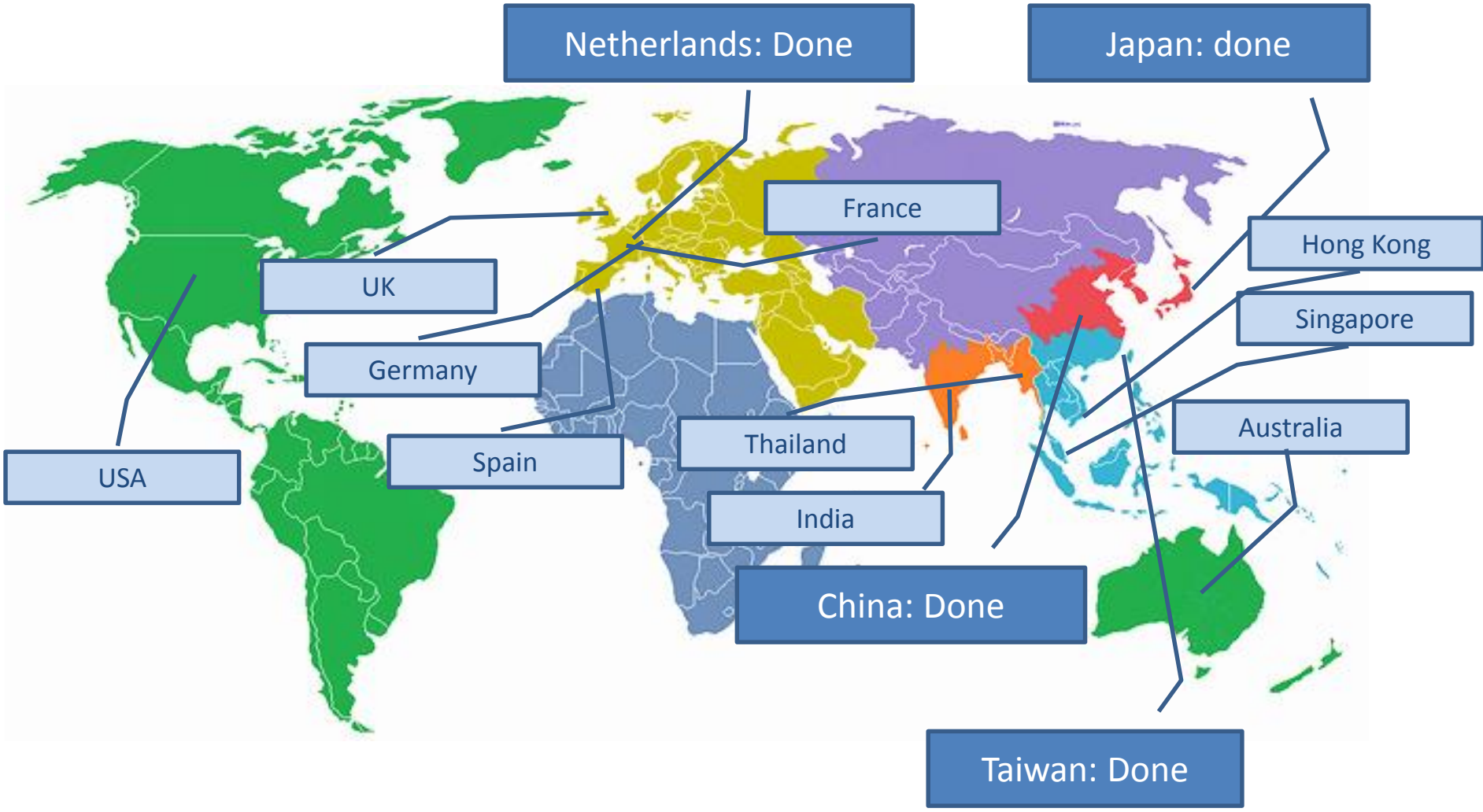
Monitoring, analysis, alert system at YNU



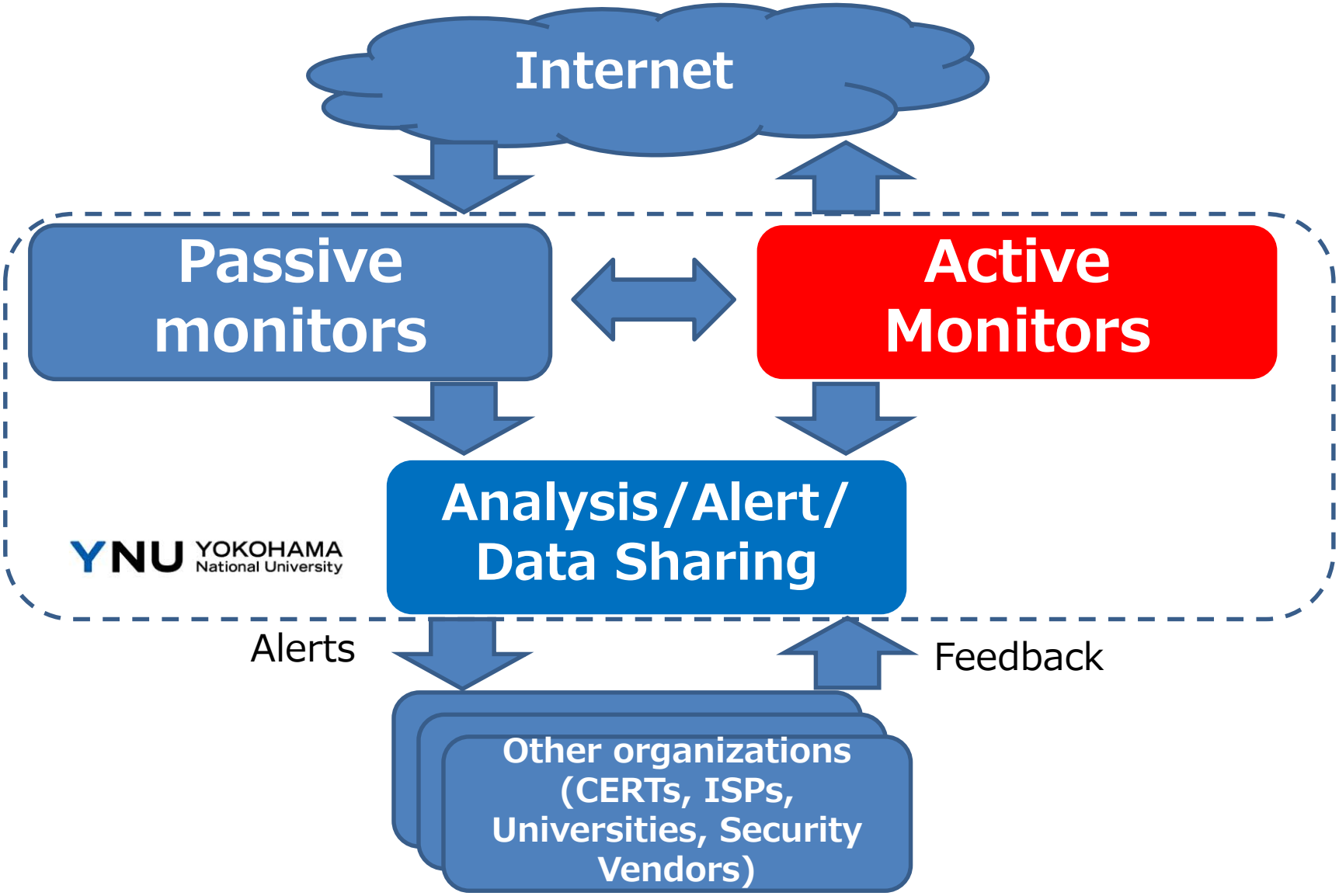
Monitoring, analysis, alert system at YNU



More sensors!



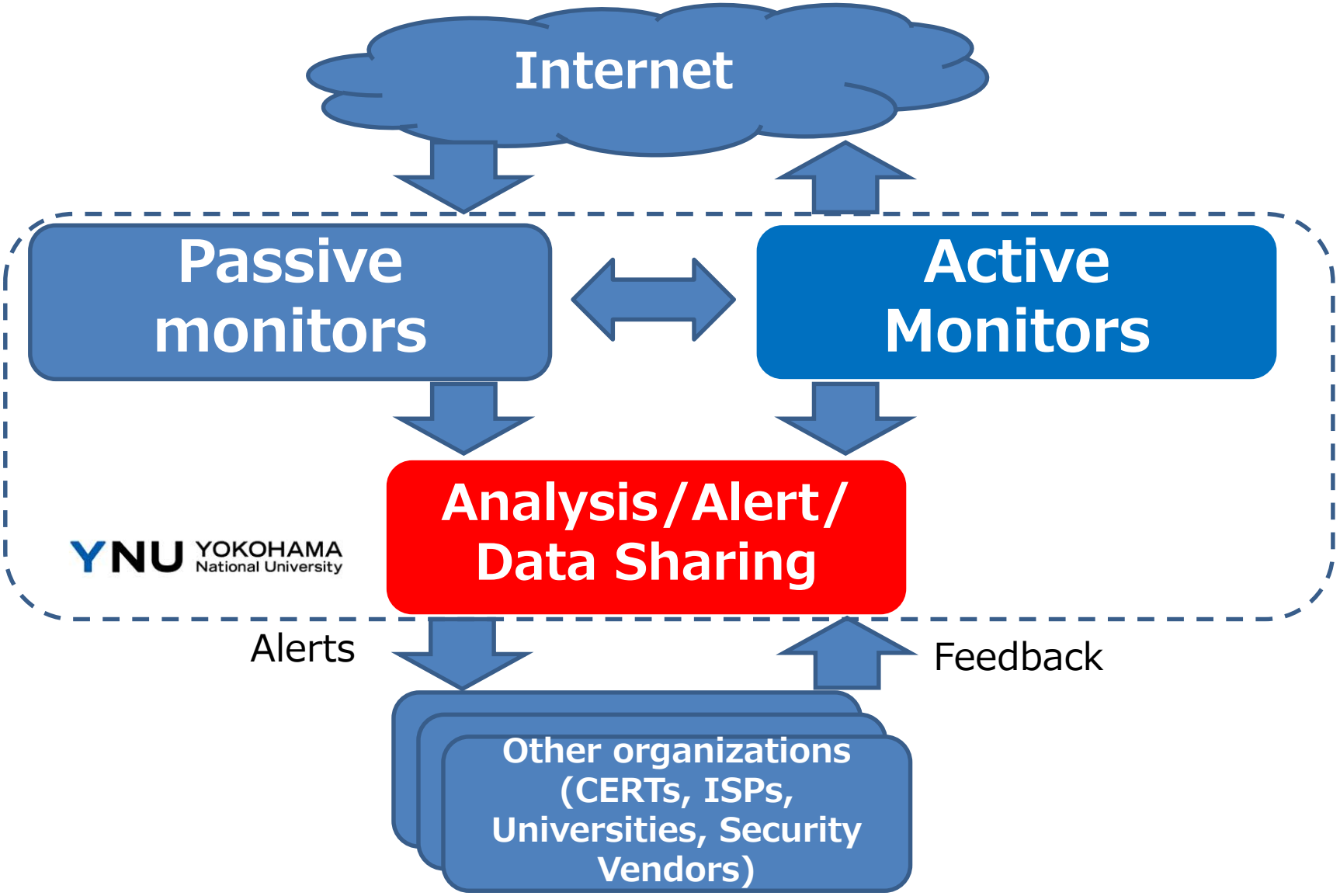
Monitoring, analysis, alert system at YNU



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

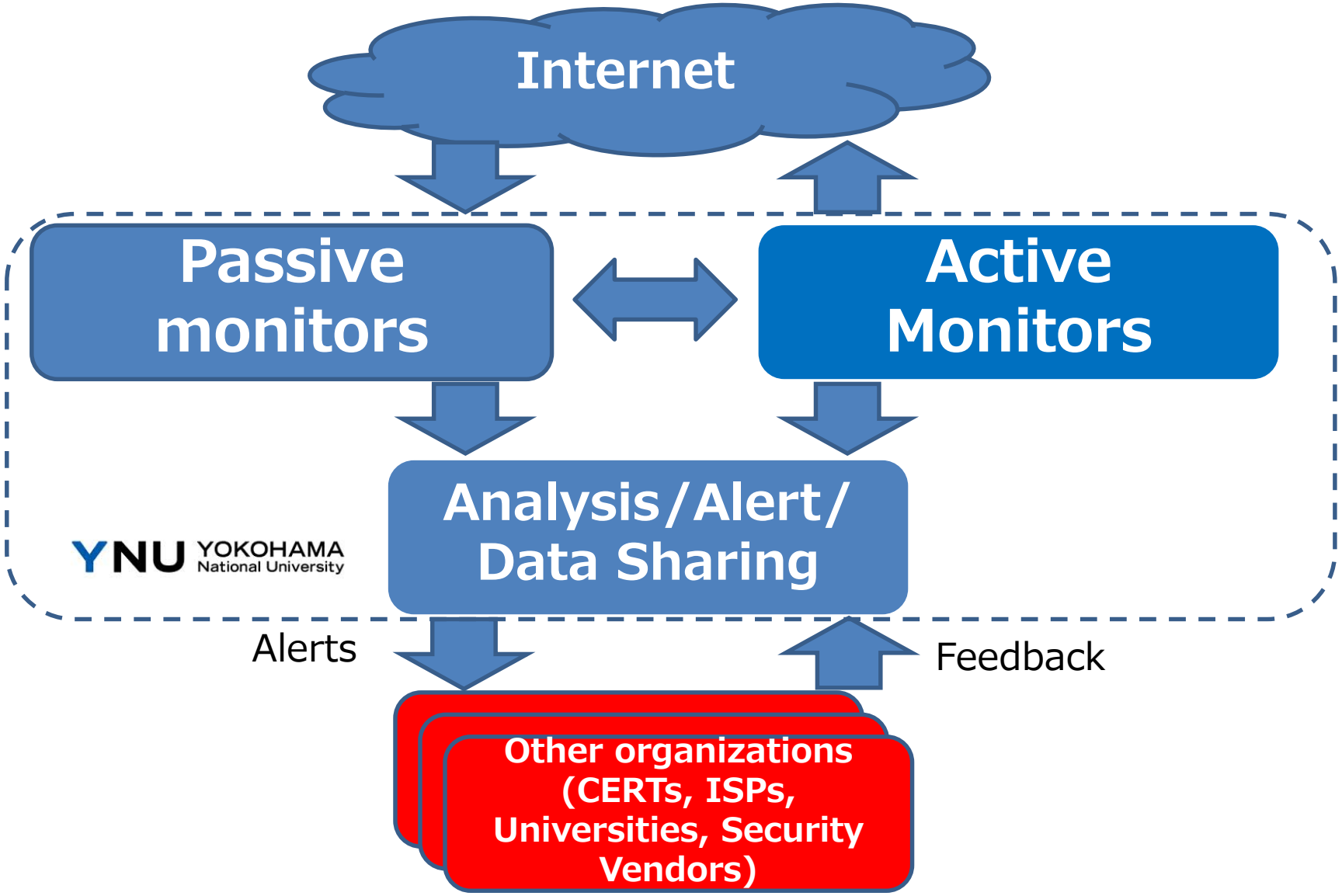
Monitoring, analysis, alert system at YNU



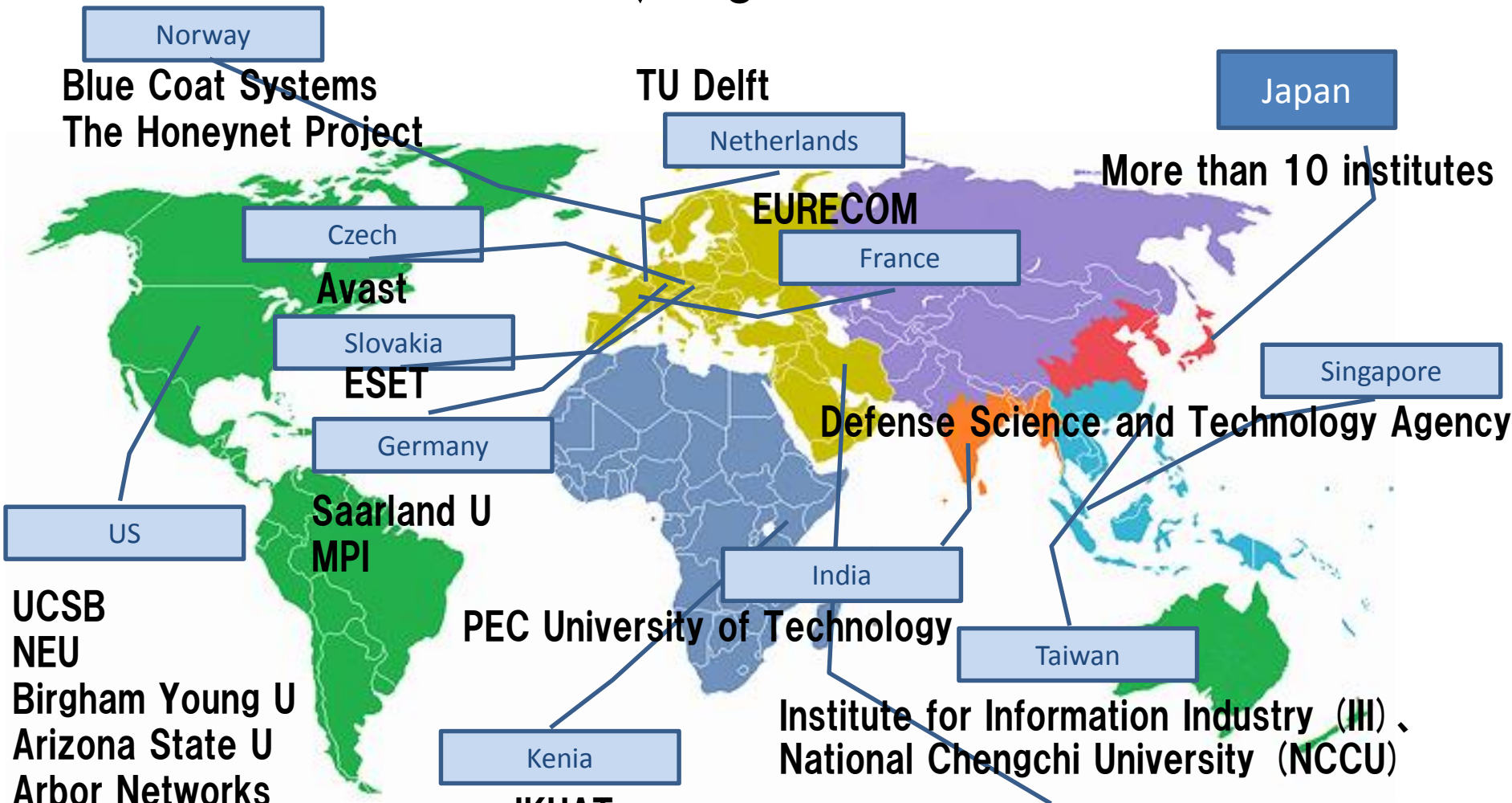
Analysis/Alert/Data sharing

- 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