Cleaning up the mess

from monitoring to discovery and notification of infected/insecure IoT devices

Katsunari Yoshioka

Associate Professor

Yokohama National University

2019/4/24

5th France-Japan Cybersecurity Workshop

More and more devices are being connected providing valuable data for innovative services:

Internet of Things

IHS forecasts the industrial sector as being one-third of the total connected IoT devices by 2020. Source: IHS Markit

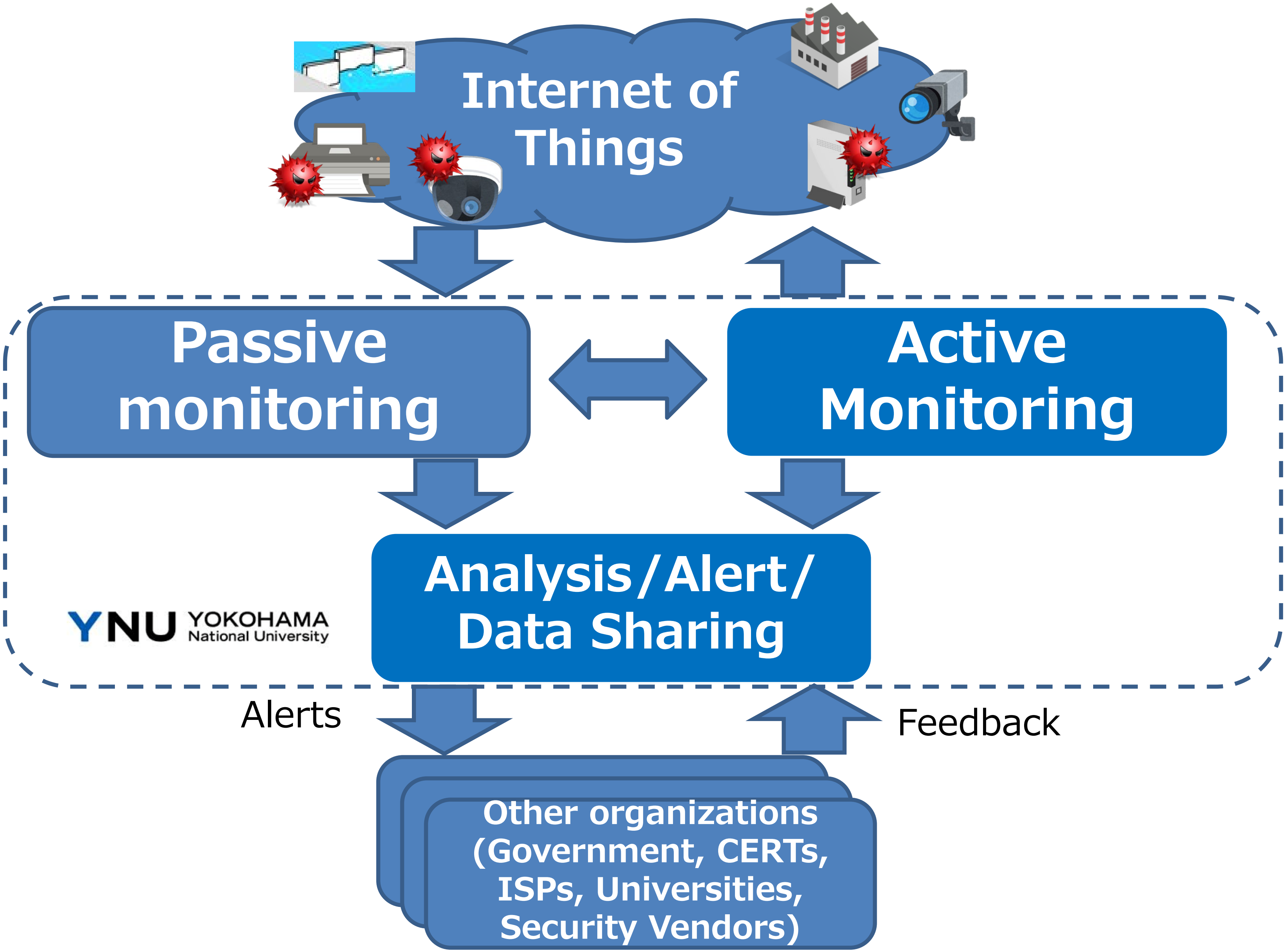
Botnet & DDoS

Internet-of-things is already full of “mess”

Exposed Facilities

Insecure Cameras

Monitoring, analysis, alert system at YNU



Internet of Things

Passive monitoring

Active Monitoring

Analysis/Alert/ Data Sharing

YNU YOKOHAMA National University

Alerts

Feedback

Other organizations (Government, CERTs, ISPs, Universities, Security Vendors)

YNU YOKOHAMA National University

NICT

UNIVERSITÄT DES SAARLANDES

TU Delft

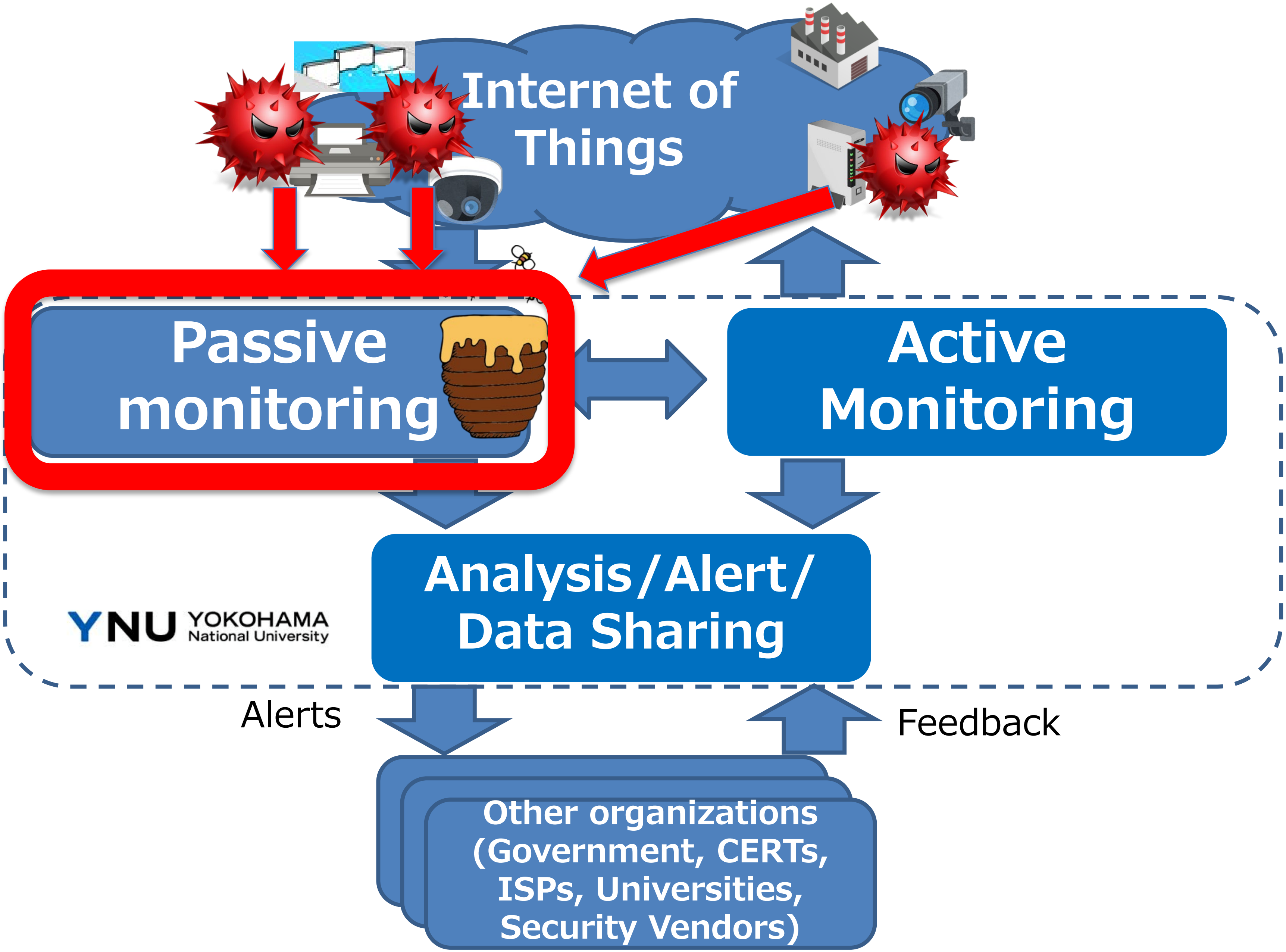
Delft University of Technology

CISPA

Center for IT-Security, Privacy and Accountability

EFFORT ONE:
OBSERVING AND CLEANING UP INFECTED DEVICES

Monitoring, analysis, alert system at YNU



Internet of Things

Passive monitoring

Active Monitoring

Analysis/Alert/ Data Sharing

YNU YOKOHAMA National University

Alerts

Feedback

Other organizations (Government, CERTs, ISPs, Universities, Security Vendors)

Devices attacked our honeypot

600,000+ devices

500+ types †

†inferred by telnet and web responses

Investigation from Jan-June 2016

Categories of Inferred compromised devices

- 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

- 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

Devices are inferred by telnet/web banners

ROUTE CAUSES OF THE MASS-COMPROMISE

Telnet

There infected devices run telnet

```
B[redacted]328 Broadband Router
```

```
ope[redacted].3.0.dm800se
```

```
Net[redacted]r login:
```

```
TL-[redacted]40N login:
```

```
[redacted]20-VoIP-AG login:
```

```
BC[redacted]328 xDSL Router
```

```
B[redacted]328 ADSL Router
```

```
Router [redacted] User Access Verification
```

```
[redacted]800se.login:
```

```
[redacted]dvs.login:
```

```
adv[redacted]s login:
```

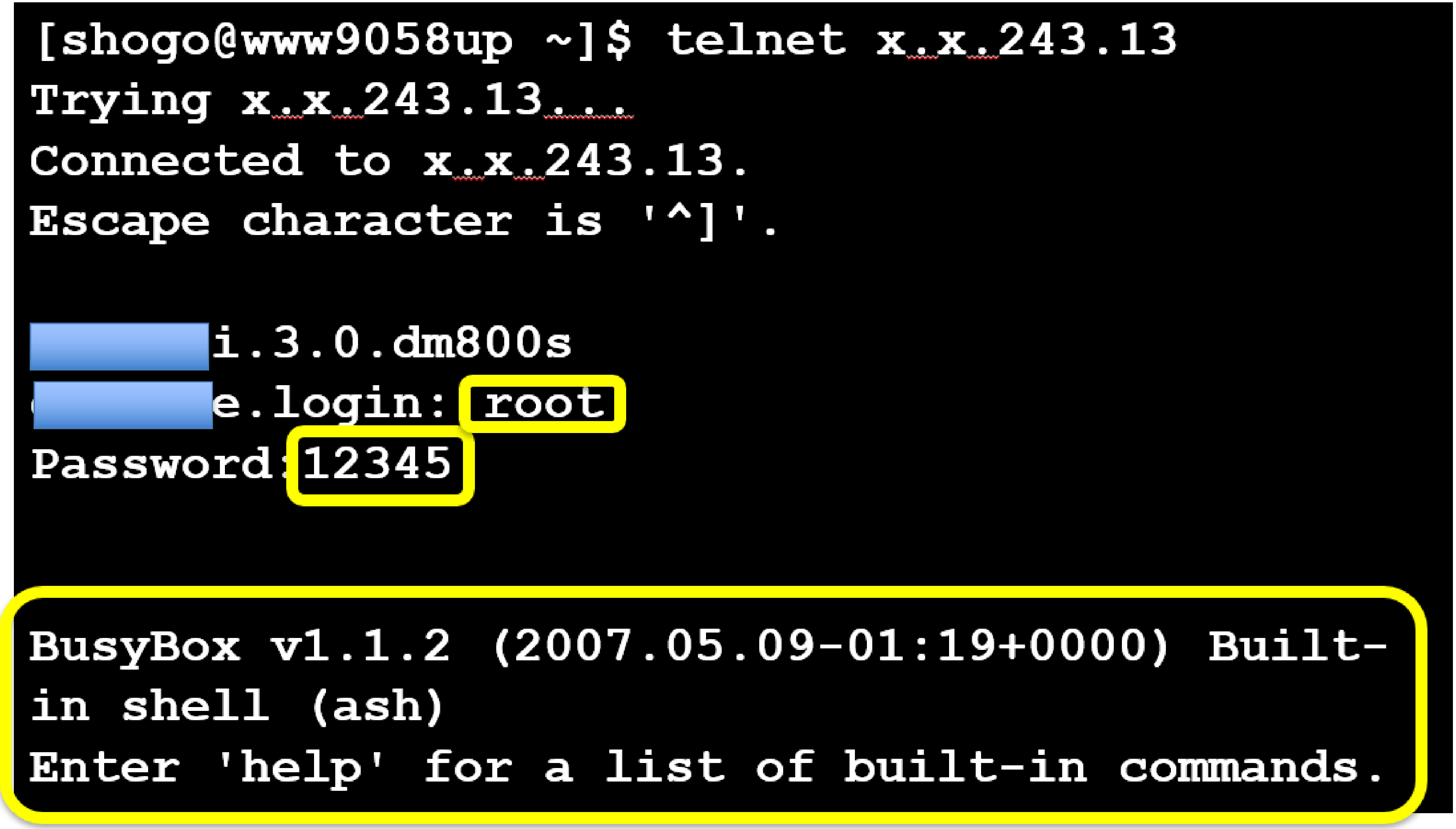
```
[redacted]vision login:
```

```
[redacted]x00 login:
```

```
Air[redacted]v2 login:
```

```
ope[redacted]4 et4x00
```

With default/weak id and password

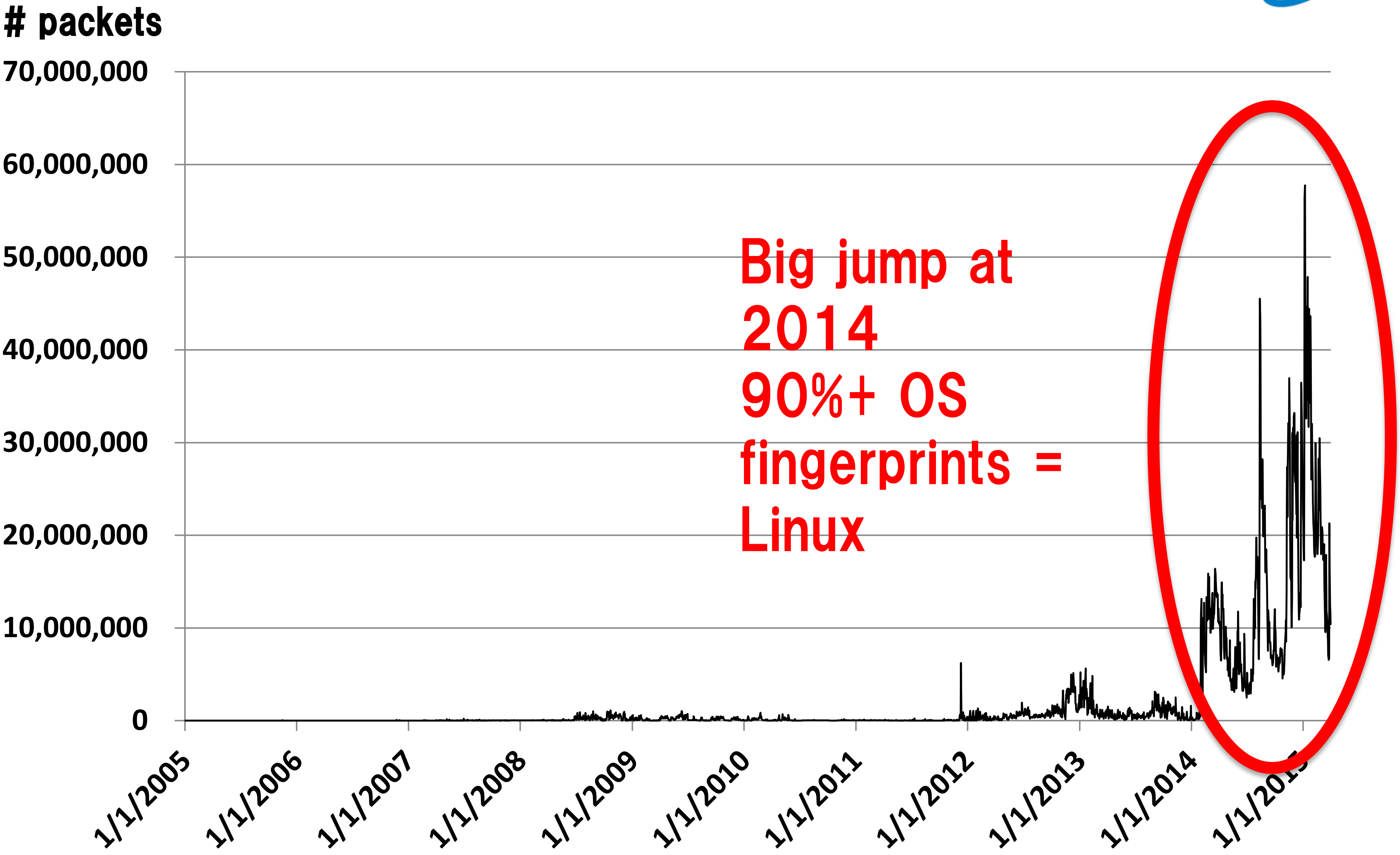


```
[shogo@www9058up ~]$ telnet x.x.243.13
Trying x.x.243.13...
Connected to x.x.243.13.
Escape character is '^]'.

[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.
```

Increases of telnet attacks

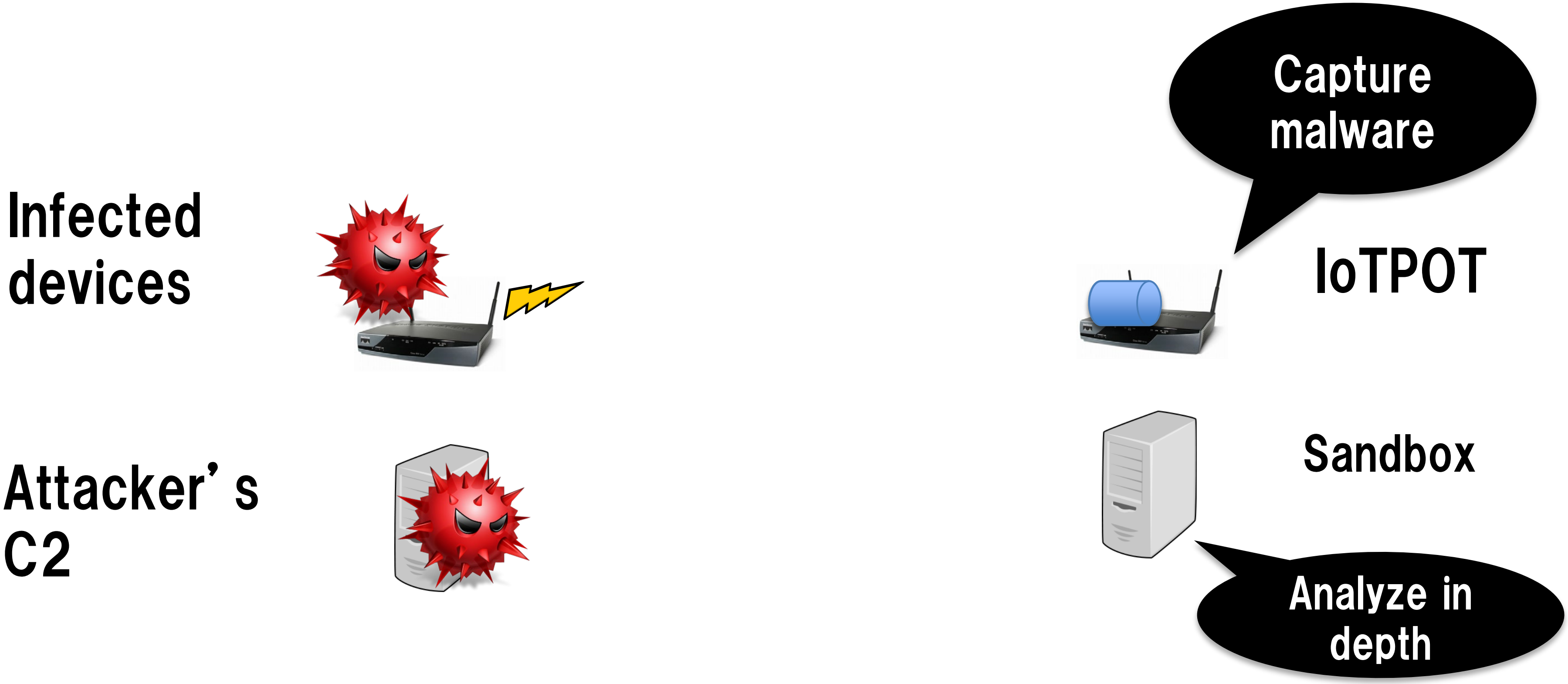


Big jump at 2014
90%+ OS fingerprints = Linux

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

Our system: IoTPOT = IoT Honeypot

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



Infected devices

Attacker’ s C2

Capture malware

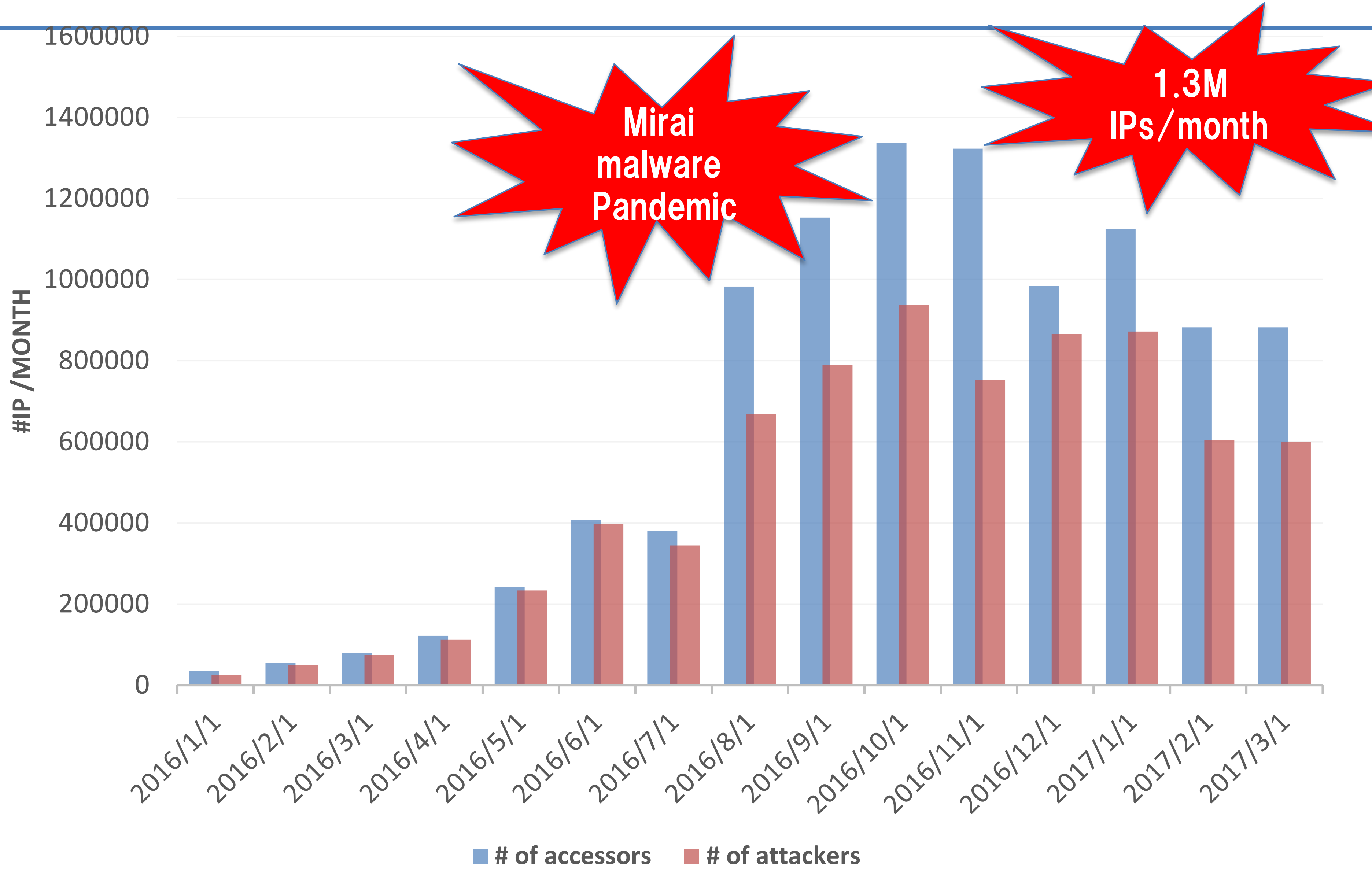
IoTPOT

Sandbox

Analyze 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

# accessors/attackers IPs

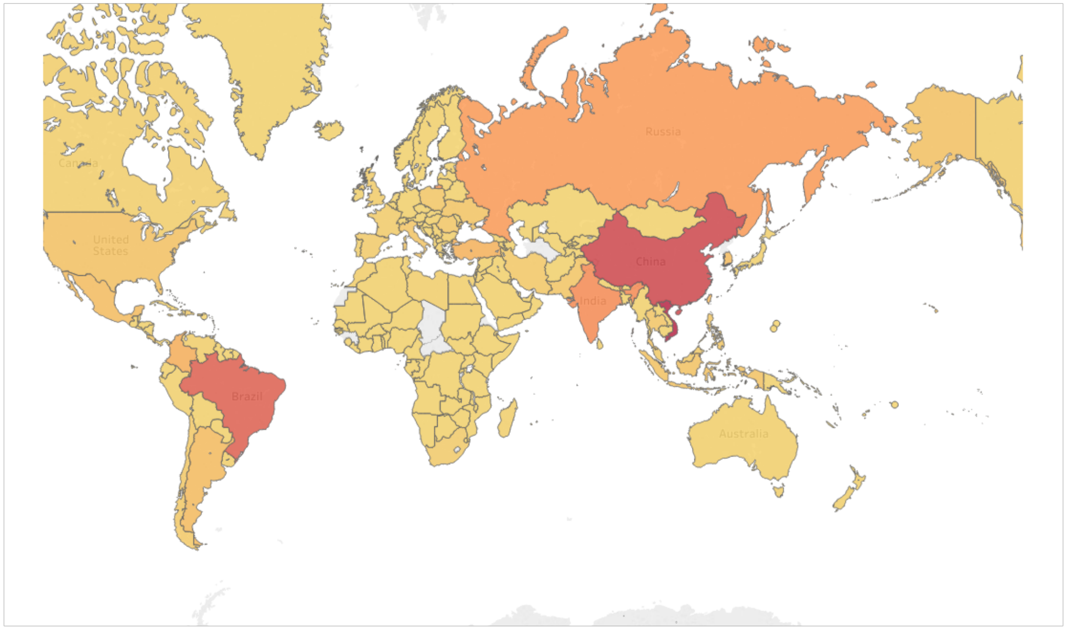


Mirai malware Pandemic

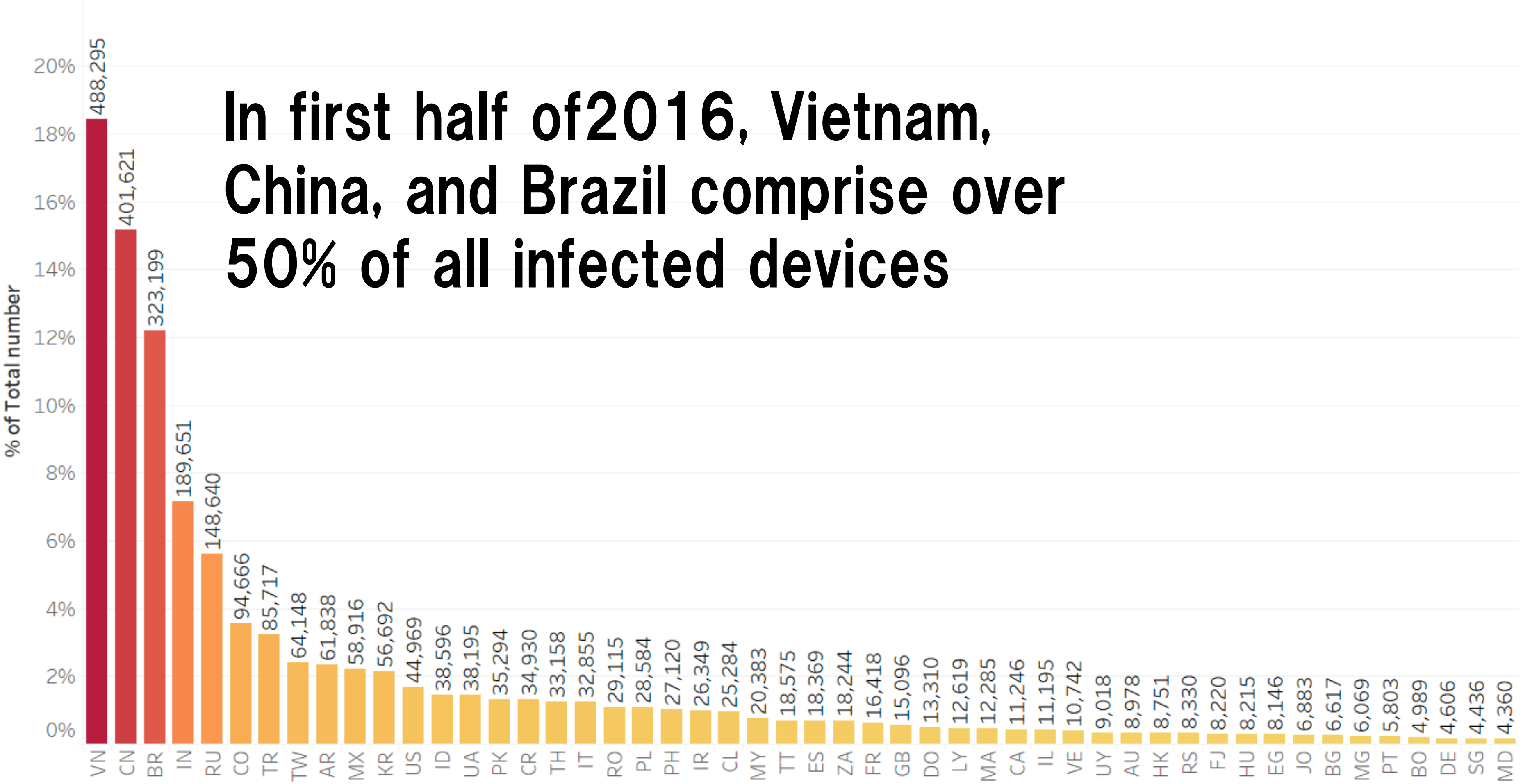
1.3M IPs/month

Worldwide pandemic

- Attacks from Over 200 countries/regions
- Especially Asian and South American countries have many infected devices

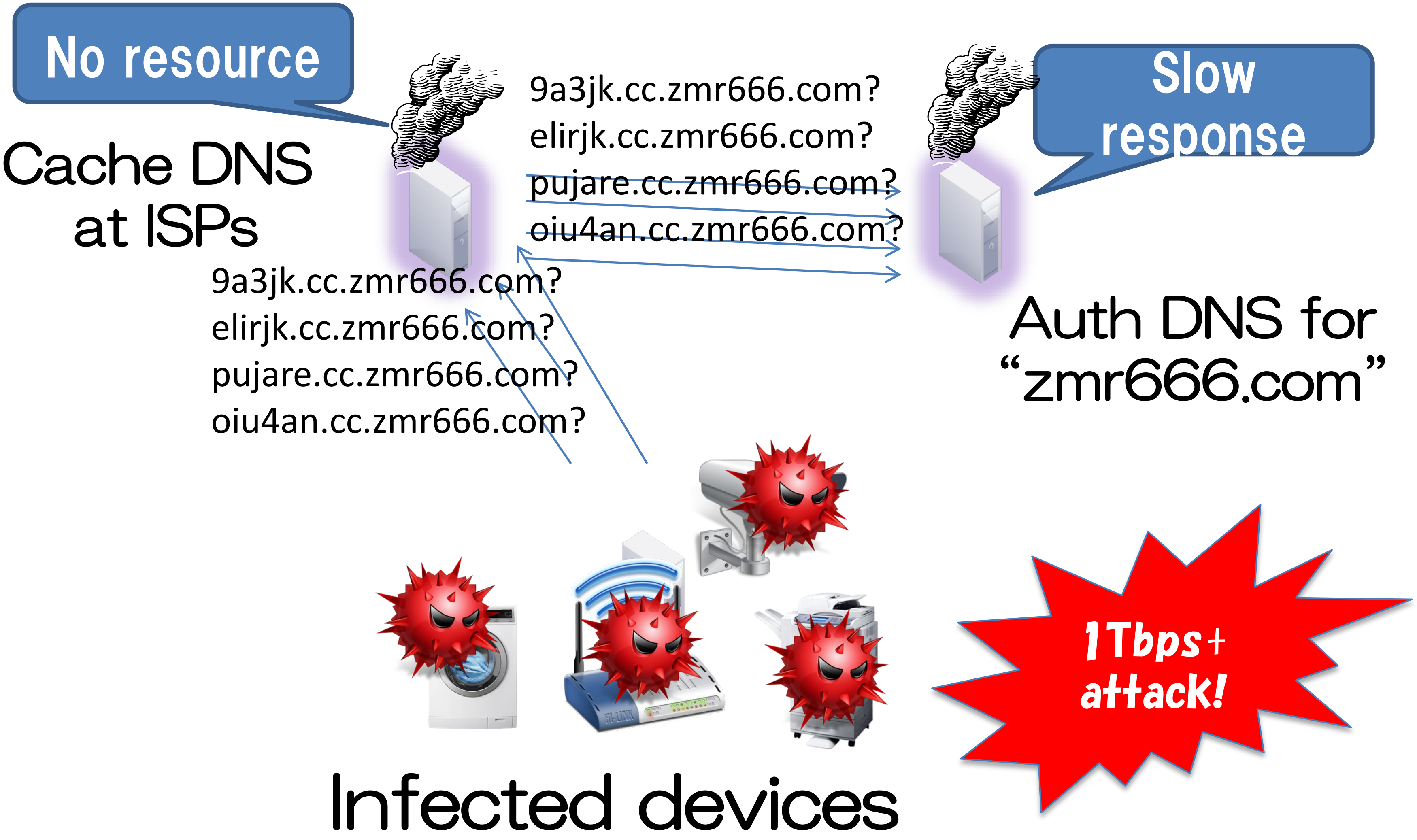


Top countries with infected devices



In first half of2016, Vietnam, China, and Brazil comprise over 50% of all infected devices

Denial of Service (DoS)



No resource

Cache DNS
at ISPs

9a3jk.cc.zmr666.com?
elirjk.cc.zmr666.com?
pujare.cc.zmr666.com?
oiu4an.cc.zmr666.com?

Slow response

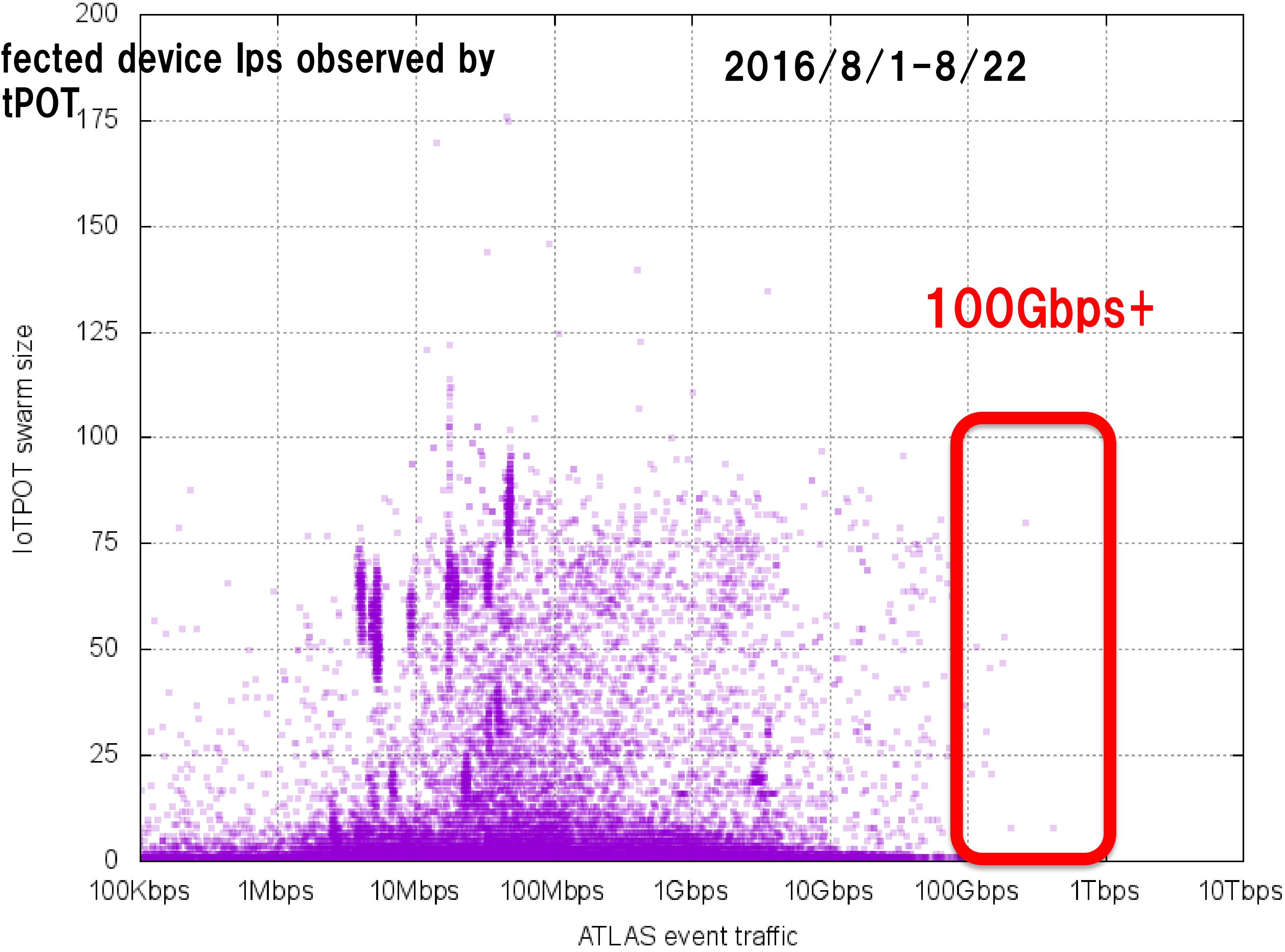
Auth DNS for
“zmr666.com”

9a3jk.cc.zmr666.com?
elirjk.cc.zmr666.com?
pujare.cc.zmr666.com?
oiu4an.cc.zmr666.com?

1Tbps+
attack!

Infected devices

Infected device Ips observed by IotPOT



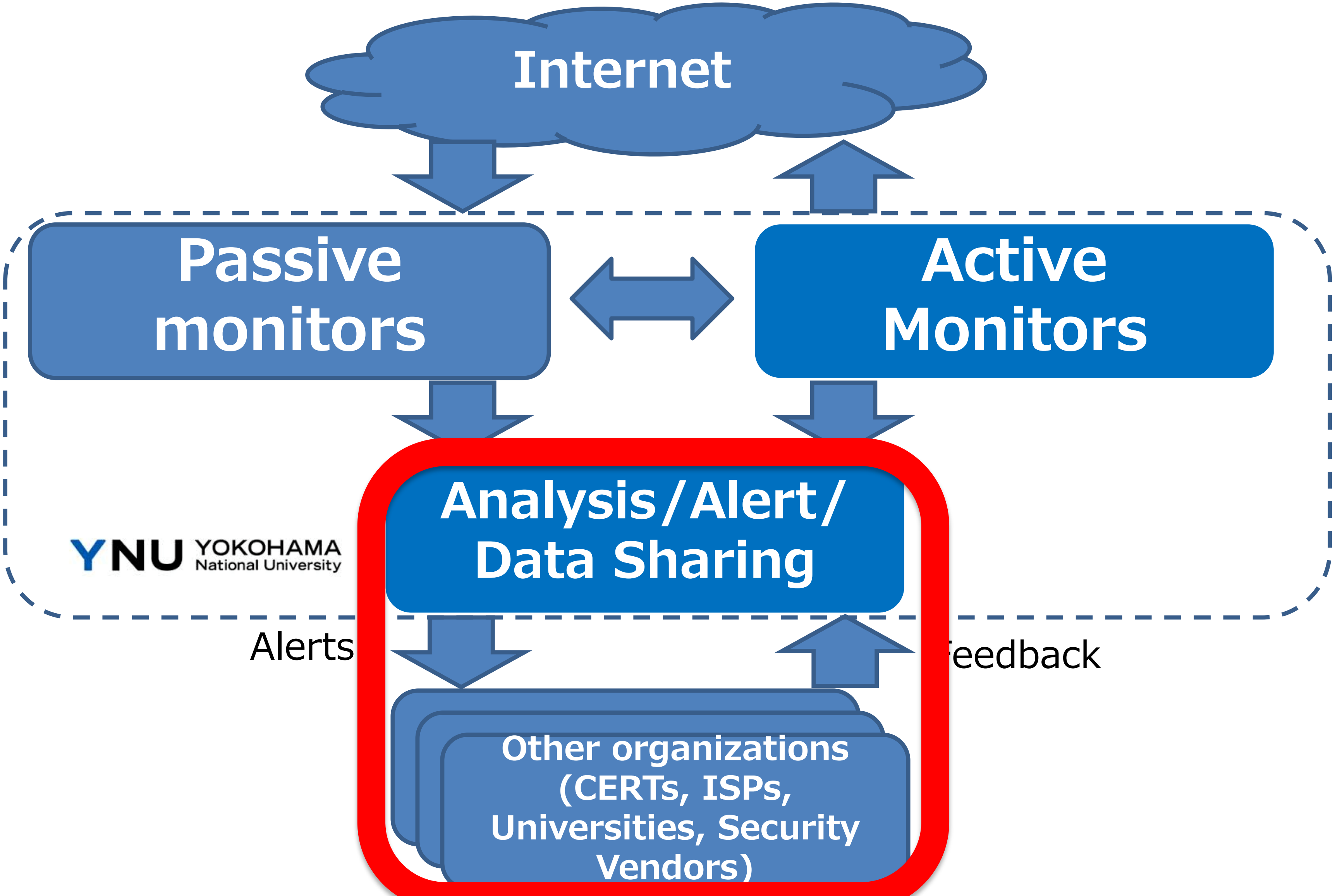
2016/8/1-8/22

100Gbps+

Size of attacks Arbor networks observed

The matching result is provided by Arbor Networks ASERT Japan

Monitoring, analysis, alert system at YNU



Internet

Passive monitors

Active Monitors

Analysis/Alert/ Data Sharing

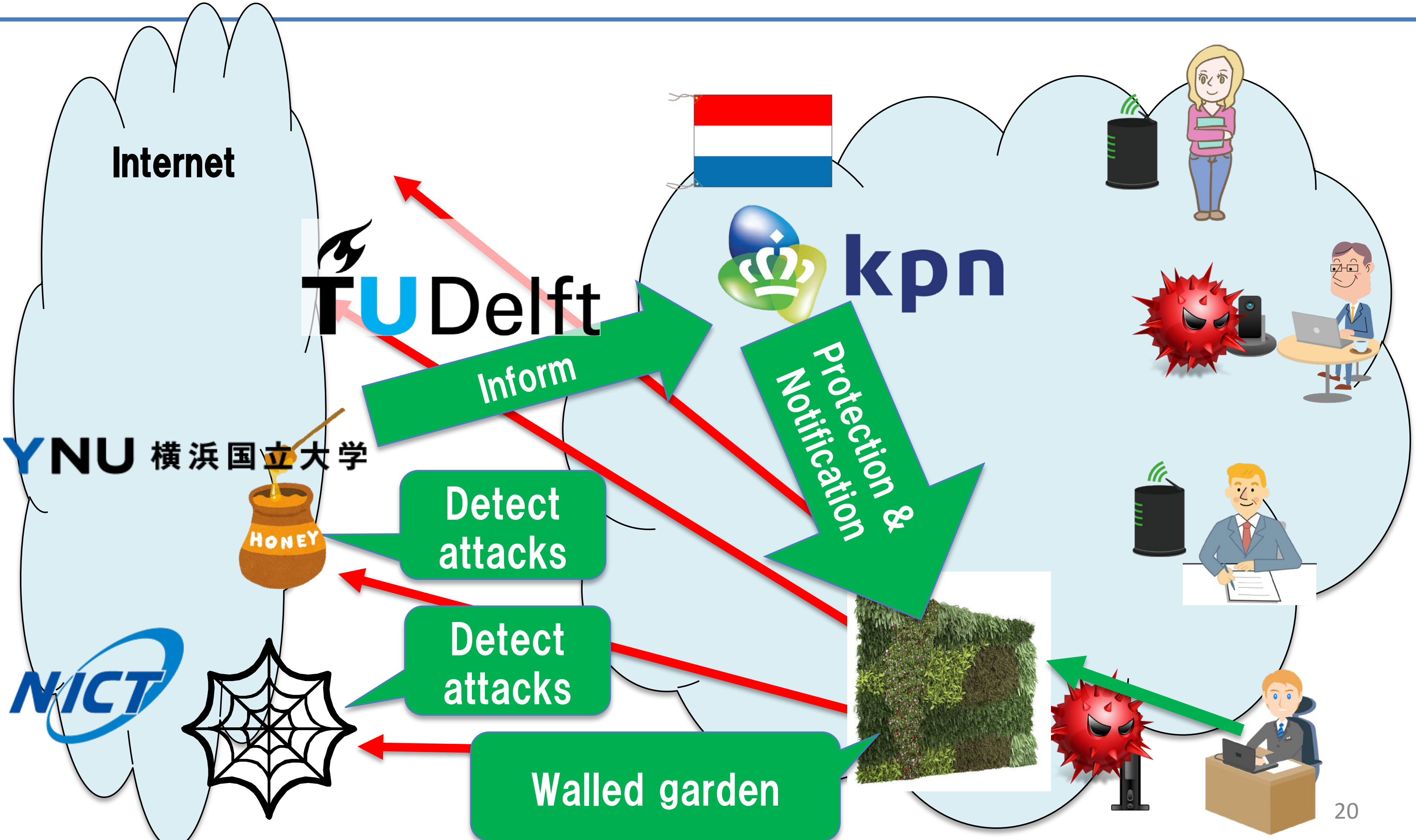
YNU YOKOHAMA National University

Alerts

Feedback

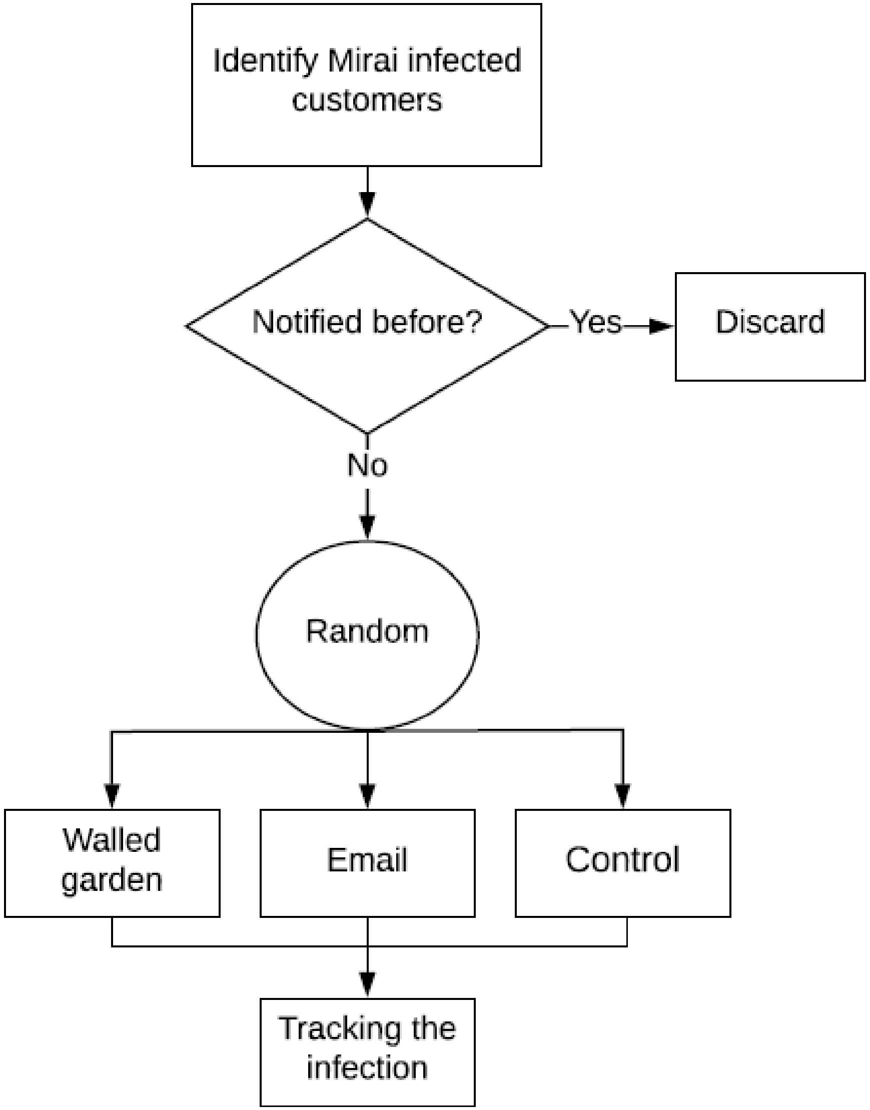
Other organizations (CERTs, ISPs, Universities, Security Vendors)

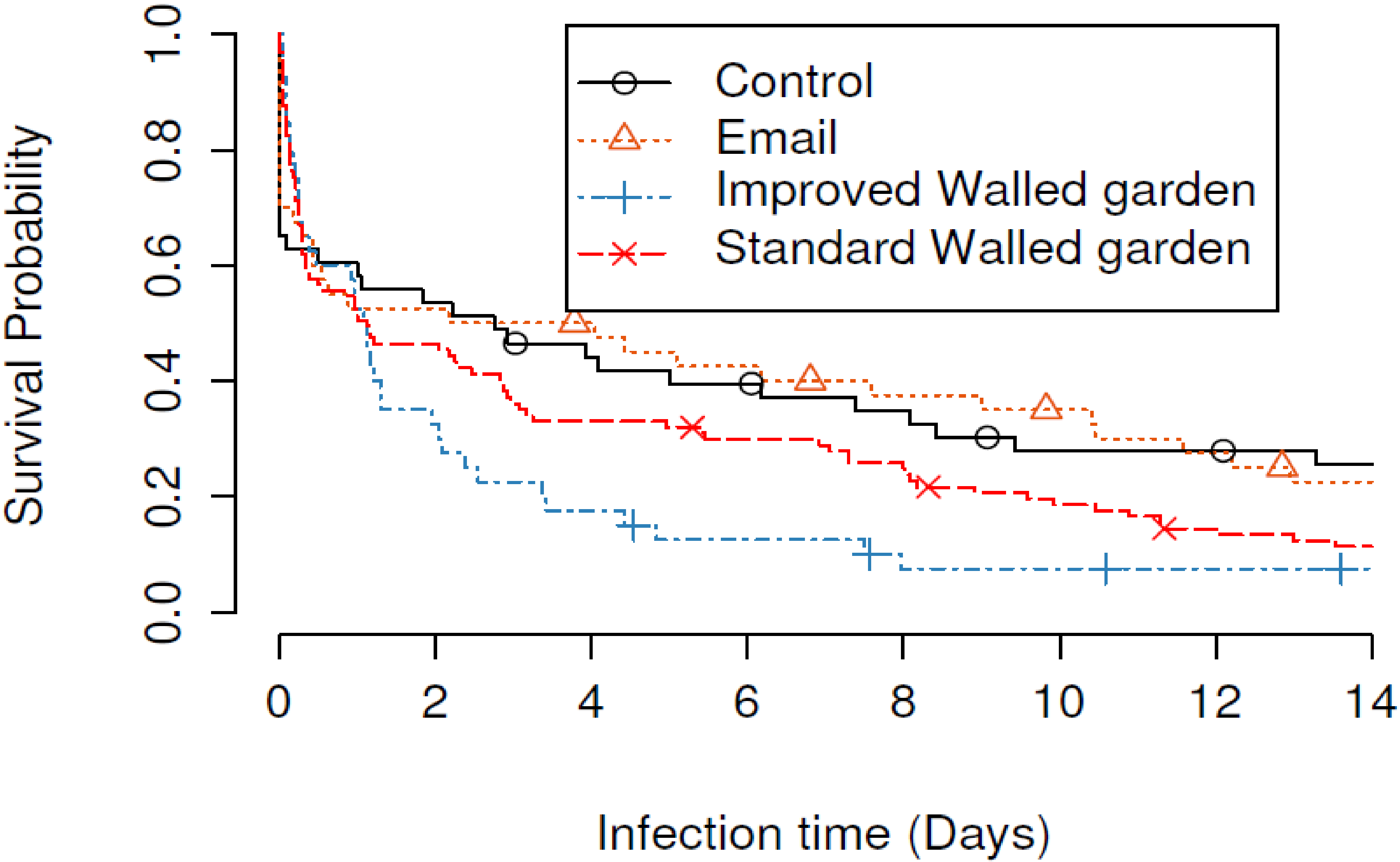
Cleaning the infected “things”



O. Cetin, C. Gañán, L. Altena, D. Inoue, T. Kasama, K. Tamiya, Y. Tie, K. Yoshioka, M. van Eeten, "Cleaning Up the Internet of Evil Things: Real-World Evidence on ISP and Consumer Efforts to Remove Mirai," The Network and Distributed System Security Symposium (NDSS 2019), 2019 (Distinguished Paper Award).

Notification Experiment





We are now preparing our new notification experiment with Japanese ISP, who can not afford Walled Garden approach. Our plan is to use SMS and/or letters.

Data sharing

- We have provided our dataset to

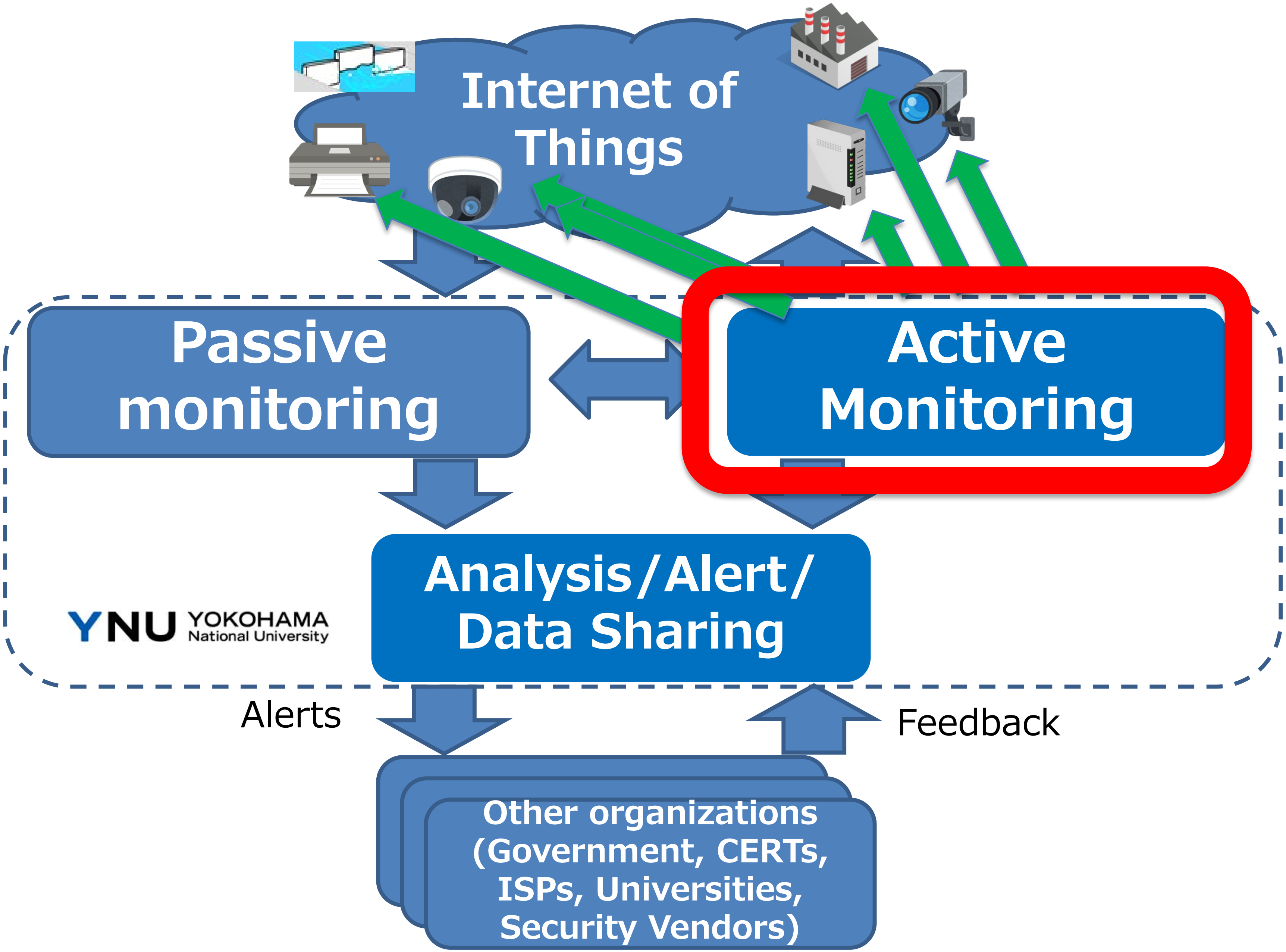
70+ organizations (including academia, industry, government/certs, and individual researchers) of

25+ countries/regions.

- Dataset:
  - Malware binaries
  - Honeypot traffic (pcap)

EFFORT TWO:
DISCOVERING INSECURE DEVICES

Monitoring, analysis, alert system at YNU



Internet of Things

Passive monitoring

Active Monitoring

Analysis/Alert/ Data Sharing

YNU YOKOHAMA National University

Alerts

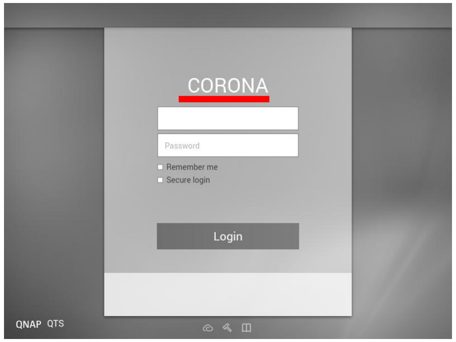
Feedback

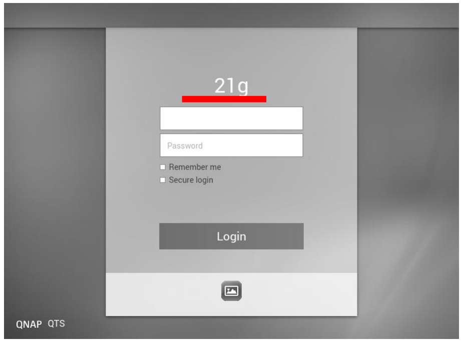
Other organizations (Government, CERTs, ISPs, Universities, Security Vendors)

Network scans on webUI and discovery of exposed IoT devices

Overview

❖ WebUIs of same/similar IoT devices are very similar





- We cluster WebUI images obtained by network scanning

WebUI of the same/similar devices should form large clusters

Experiment

- 14,744 image data from a certain Japanese AS

  －Percentage of IoT WebUIs

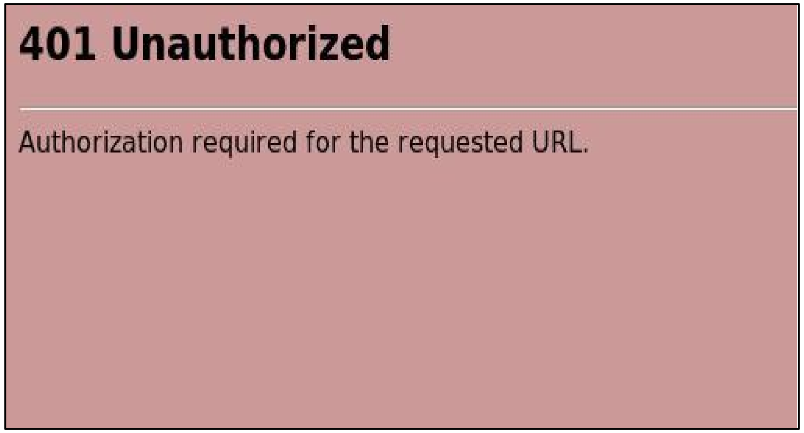
  ※by manual inspection with random sampling

  →35%

- **We call a cluster “IoT cluster” if it contains 50% or more IoT devices of the same/similar categories**

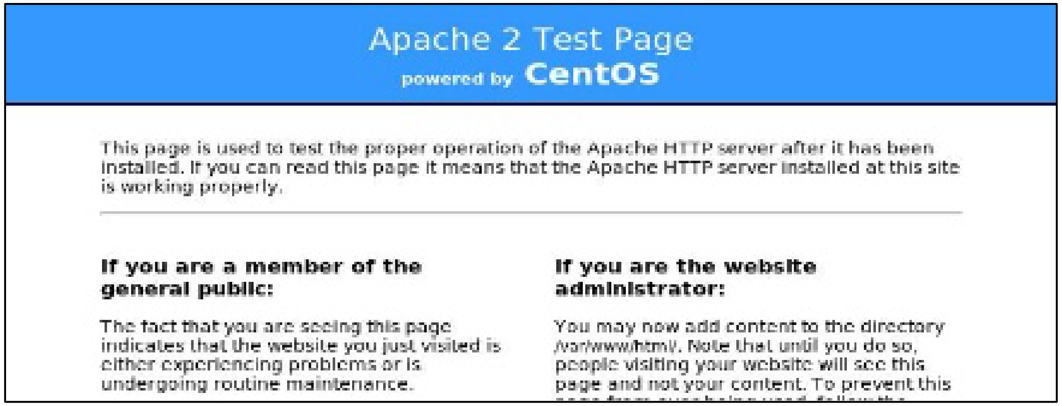
Filtering noises

- Filtering for the following 3 kinds of clusters
  - Error message pages
  - Blank pages
  - Server test/default pages



401 Unauthorized

Authorization required for the requested URL.



Apache 2 Test Page

powered by CentOS

This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page it means that the Apache HTTP server installed at this site is working properly.

If you are a member of the general public:

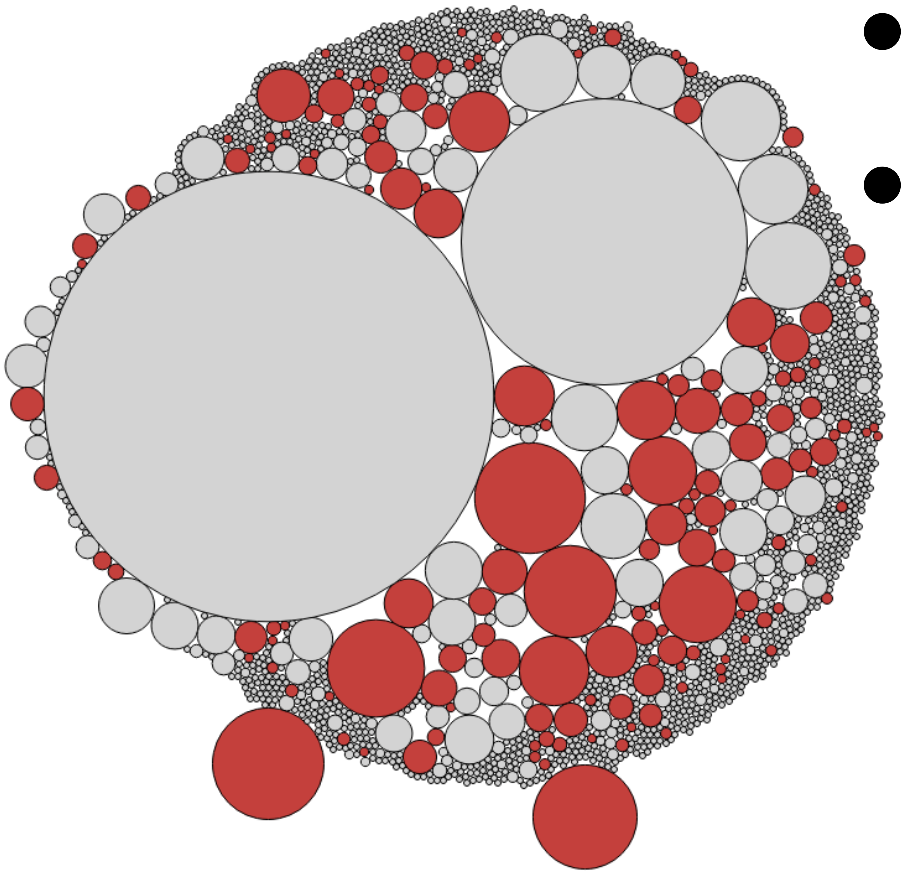
The fact that you are seeing this page indicates that the website you just visited is either experiencing problems or is undergoing routine maintenance.

If you are the website administrator:

You may now add content to the directory /var/www/html/. Note that until you do so, people visiting your website will see this page and not your content. To prevent this

Initial clustering results

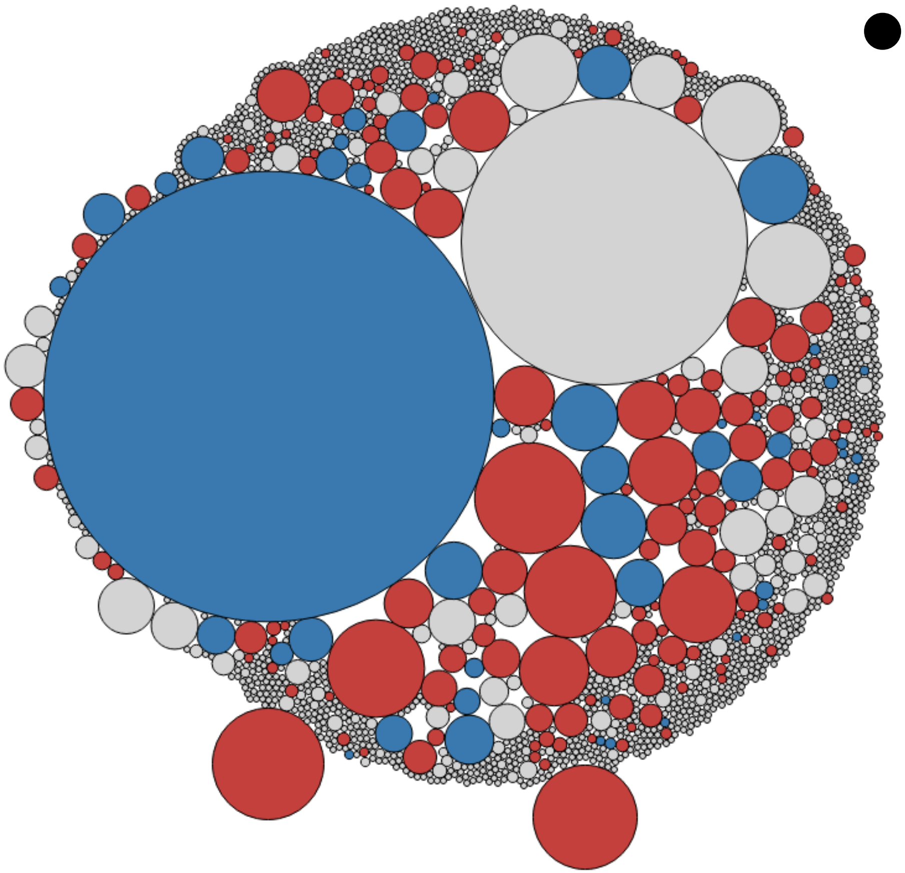
- Showing all the clusters include singletons
- A circle represents a cluster



🔴 IoT cluster

⚪ NOT IoT cluster

Clustering result



- Many “error message page” exist, and form large clusters

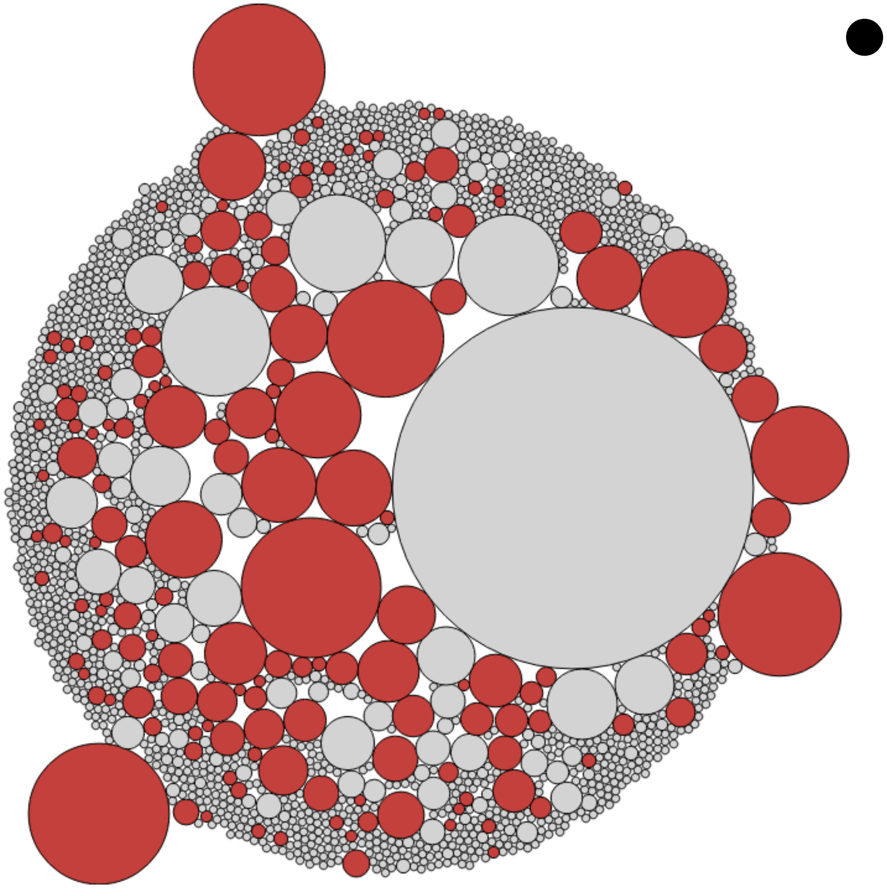
→Exclude 🔵

🔴 IoT cluster

⚪ NOT IoT cluster

🔵 Error message page cluster

Clustering result

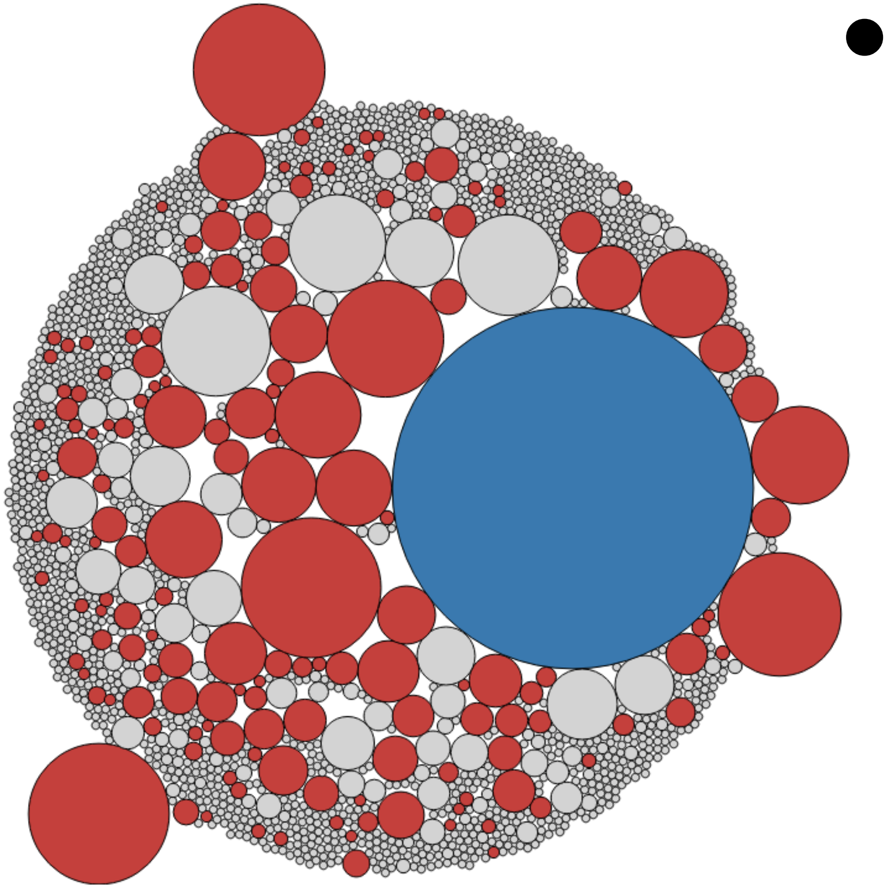


- Result of excluding “Error message pages”

🔴 IoT cluster

⚪ NOT IoT cluster

Clustering result



- Many “blank page ” exist, and form a large cluster

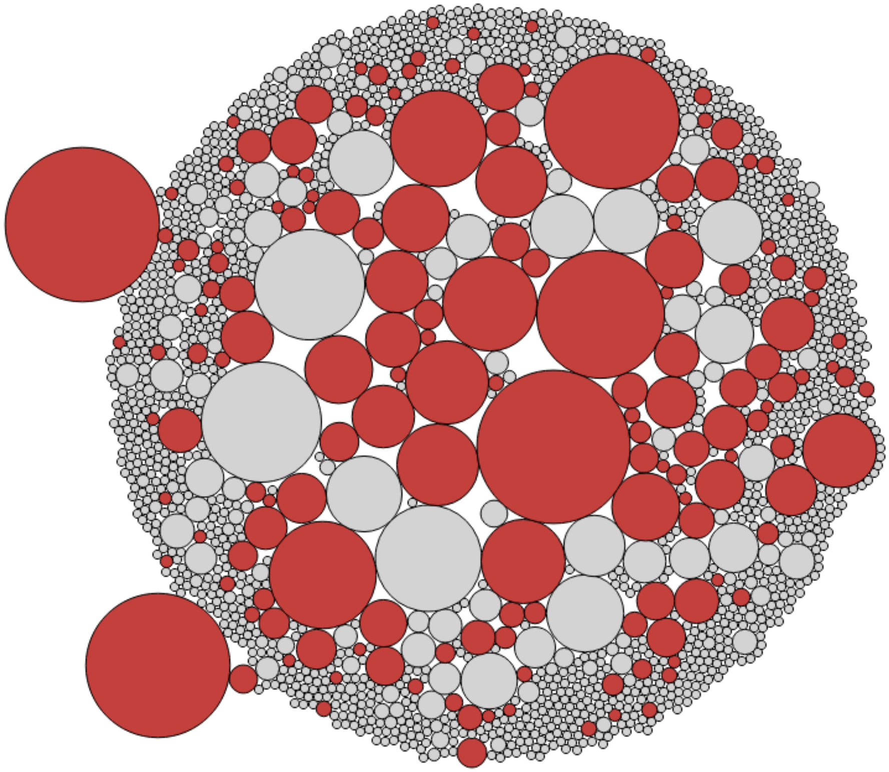
→Exclude 🔵

🔴 IoT cluster

⚪ NOT IoT cluster

🔵 Blank page cluster

Clustering result

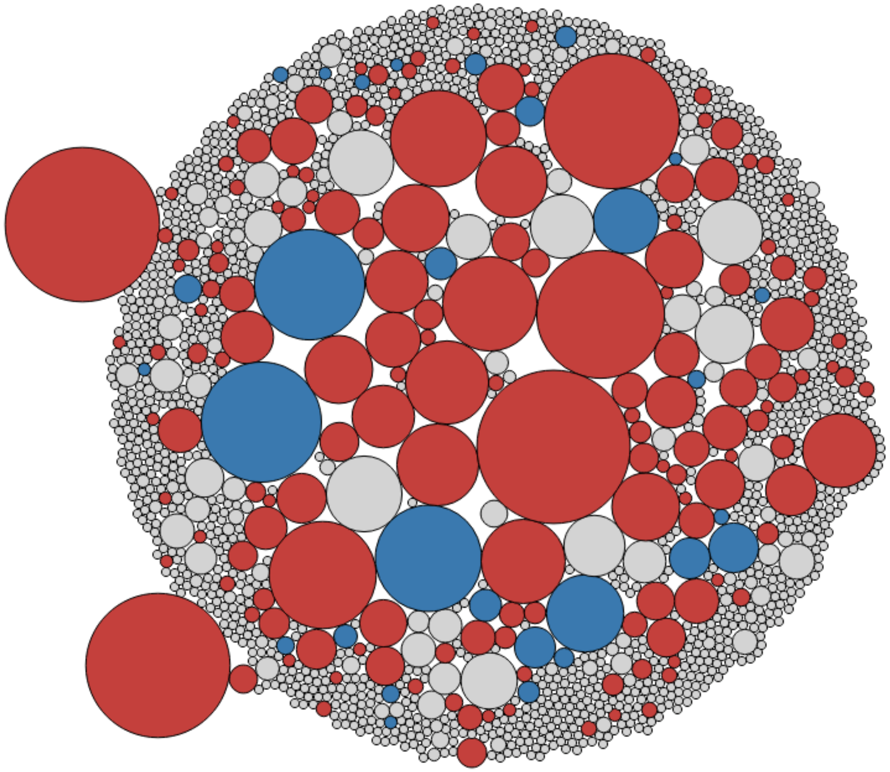


- Result after excluding “blank pages”

🔴 IoT cluster

⚪ NOT IoT cluster

Clustering result

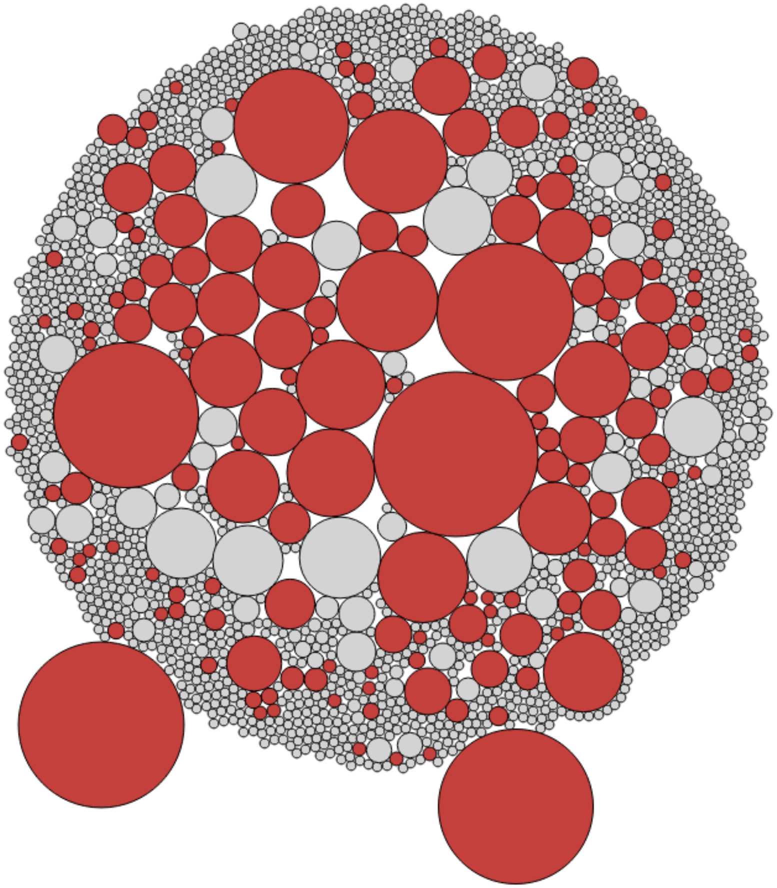


- Many “server test/default page ” exist, and form large clusters

→Exclude 🔵

🔴 IoT cluster
⚪ NOT IoT cluster
🔵 Server test/default page cluster

Filtering particular clusters

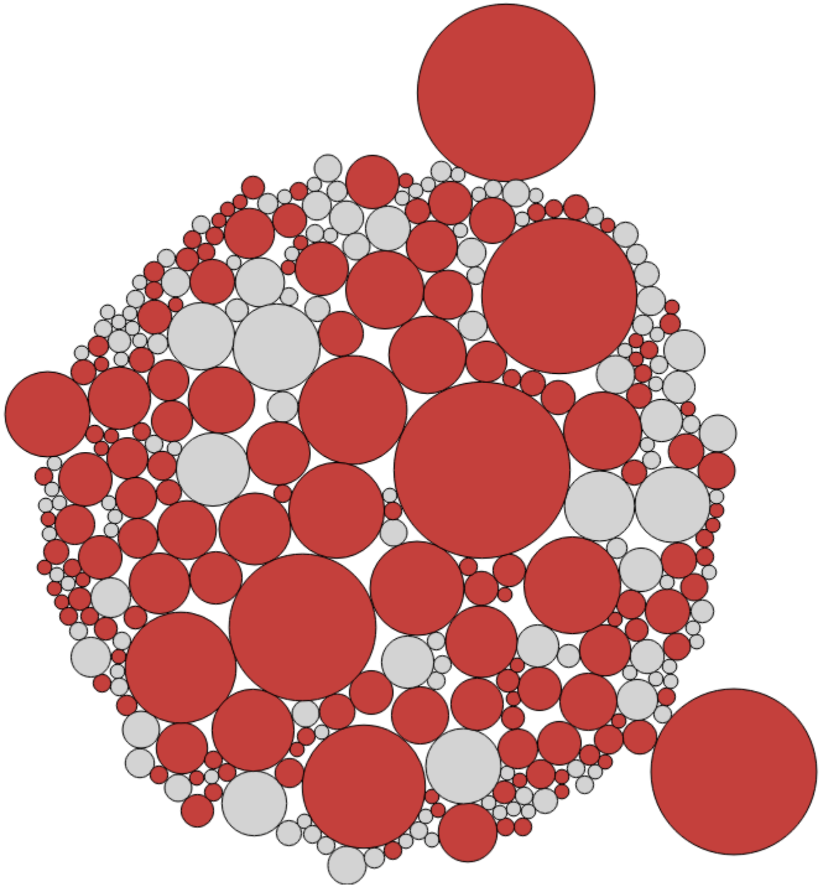


- Result after excluding “server test/default page cluster”
- Because 88% of singletons are common web page ※, we also exclude them

（※confirmed by random sampling）

🔴 IoT cluster
⚪ NOT IoT cluster

Clustering result



By excluding the following clusters, it was found that the WebUI images of the IoT devices forms larger clusters than common Web pages

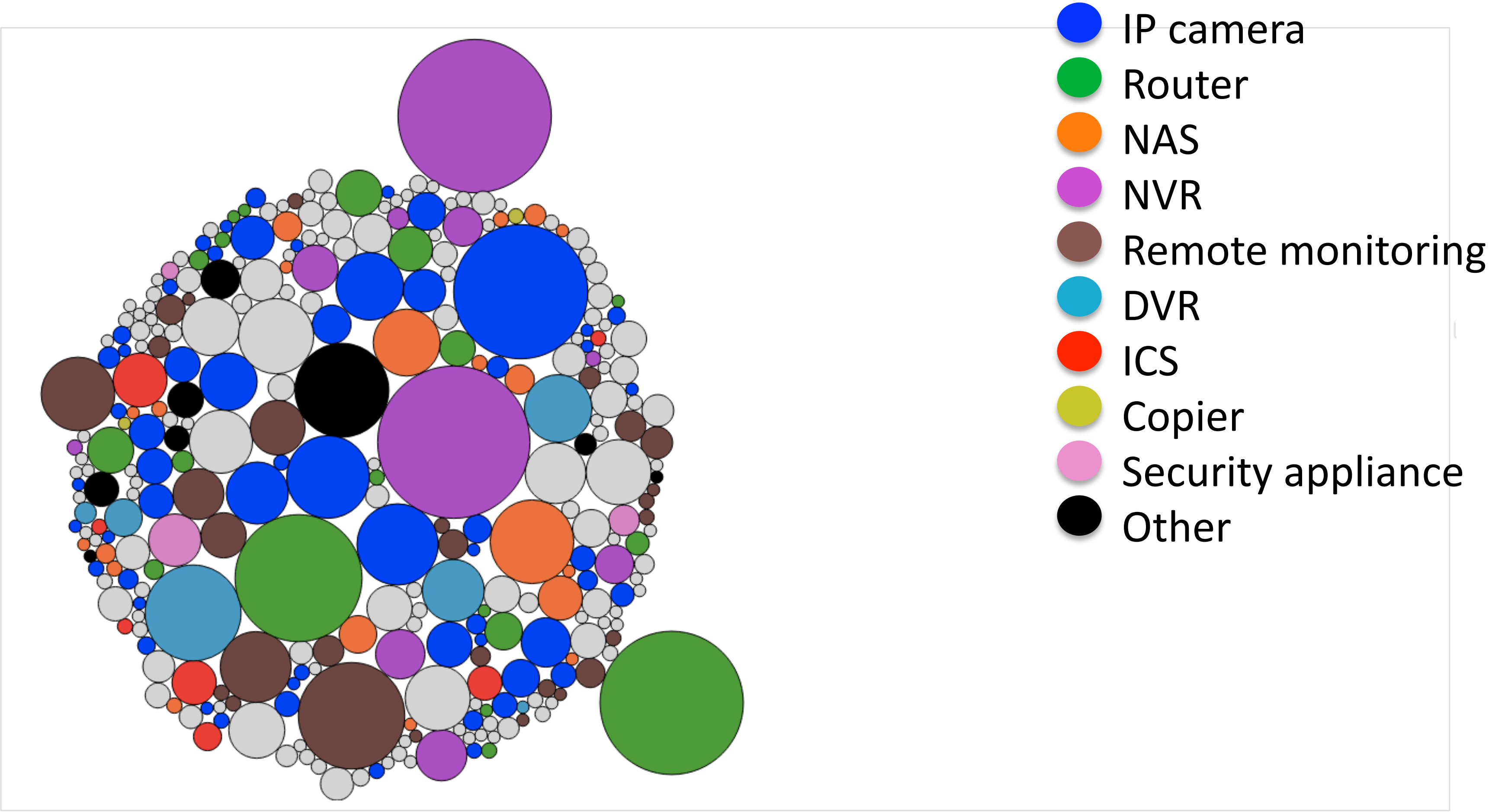
- Error message page cluster
- Blank page cluster
- Server test/default page cluster
- Singletons

🔴 IoT cluster

⚪ NOT IoT cluster

シー

Device category

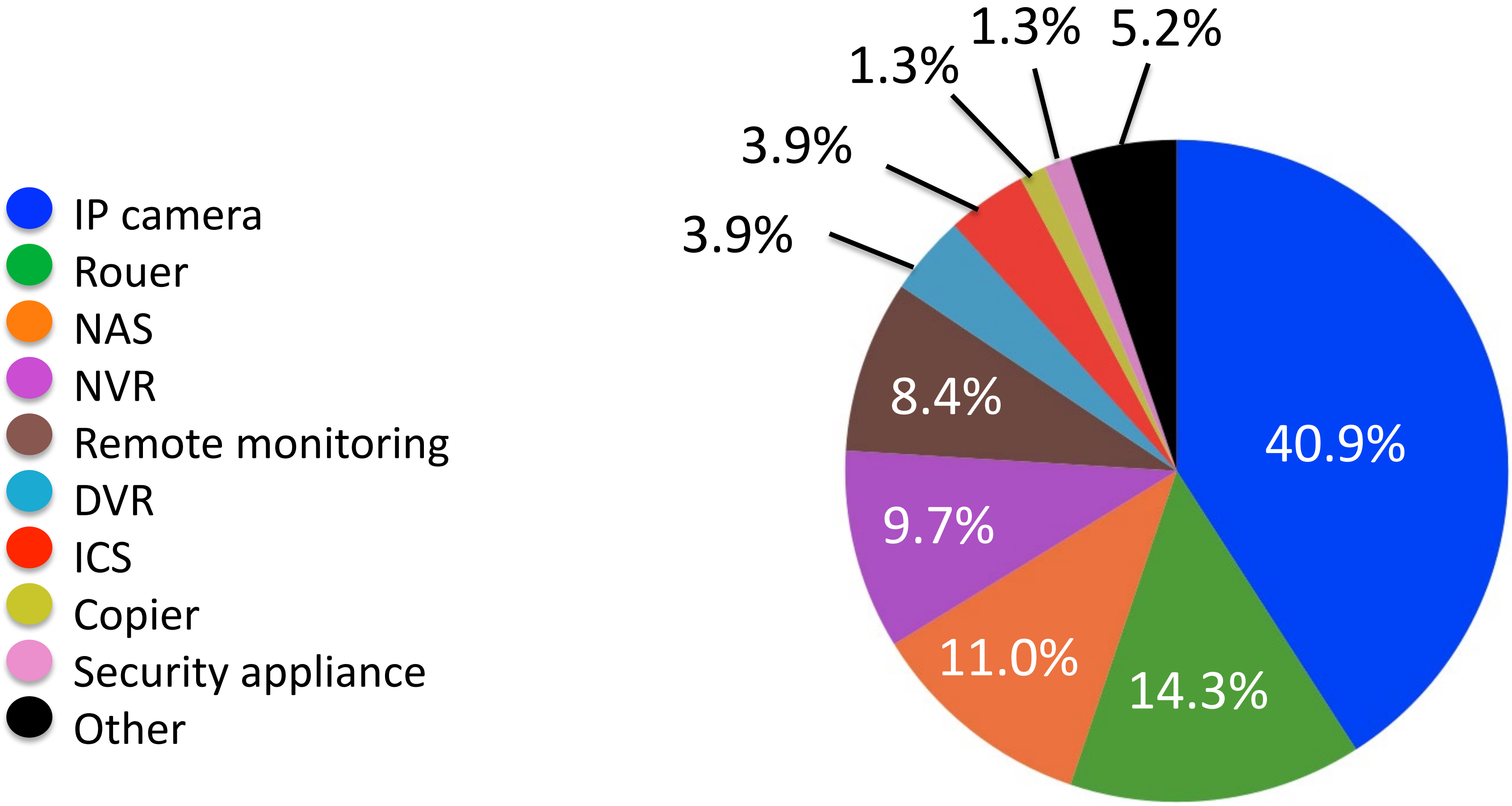


- ● IP camera
- ● Router
- ● NAS
- ● NVR
- ● Remote monitoring
- ● DVR
- ● ICS
- ● Copier
- ● Security appliance
- ● Other

シー

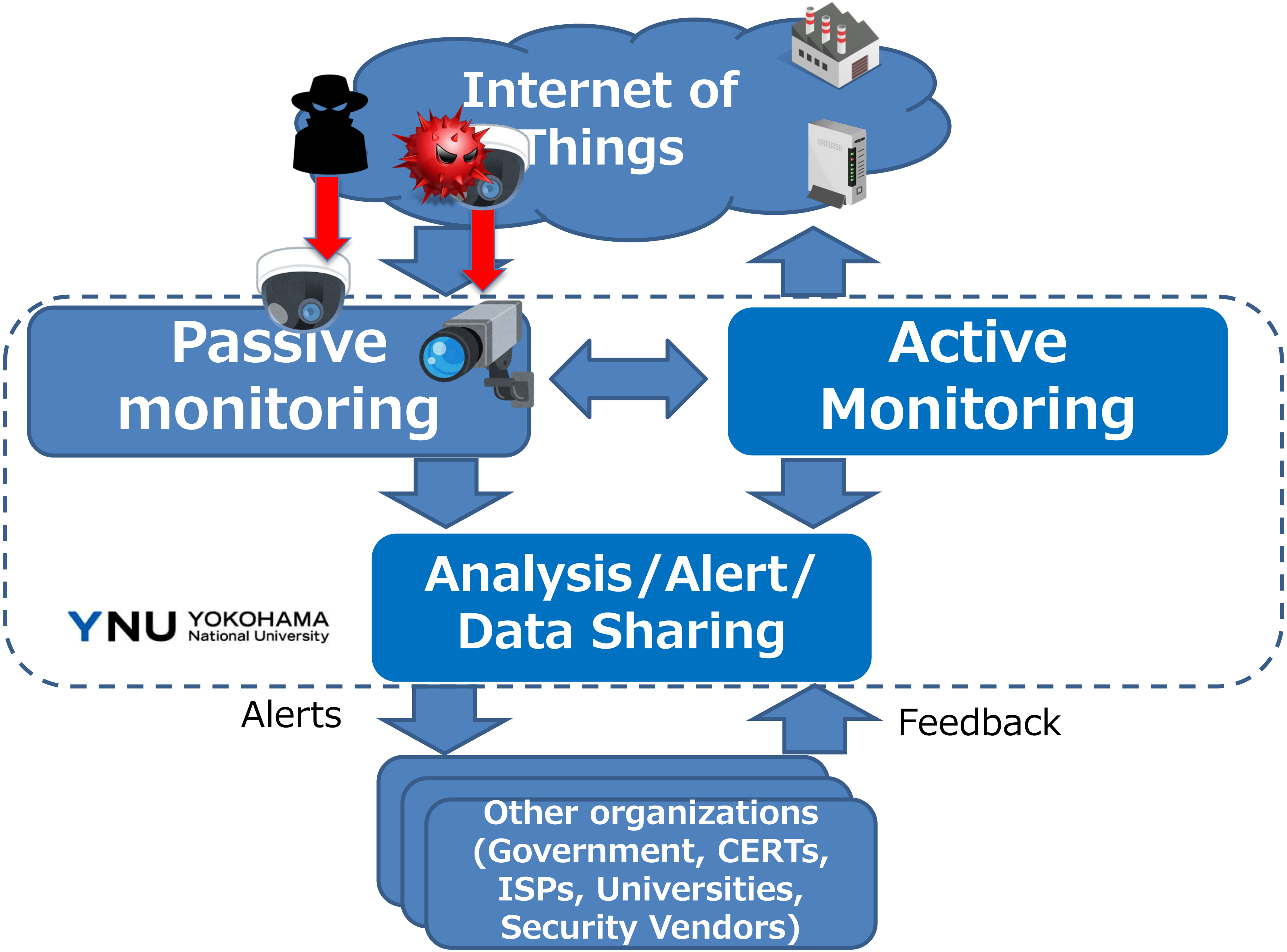
Discovered IoT devices

- We found 154 models of IoT devices in single AS



EFFORT THREE: UNDERSTANDING THE RISK OF INSECURE/EXPOSED CAMERAS

Monitoring, analysis, alert system at YNU


Internet of Things
Passive monitoring
Active Monitoring
Analysis/Alert/ Data Sharing
YNU YOKOHAMA National University
Alerts
Feedback
Other organizations (Government, CERTs, ISPs, Universities, Security Vendors)

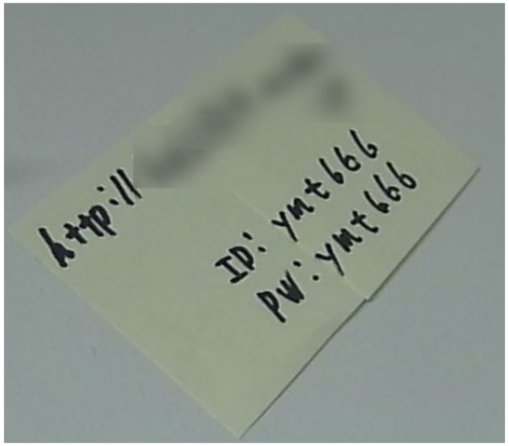
Experiment of decoy IP camera

Peeping observation experiment with two kinds of decoy IP Cameras

Decoy IP Camera exposing bait URL (“URL honey camera”)

exposing bait URL and ID/password

Investigate whether human beings are viewing images



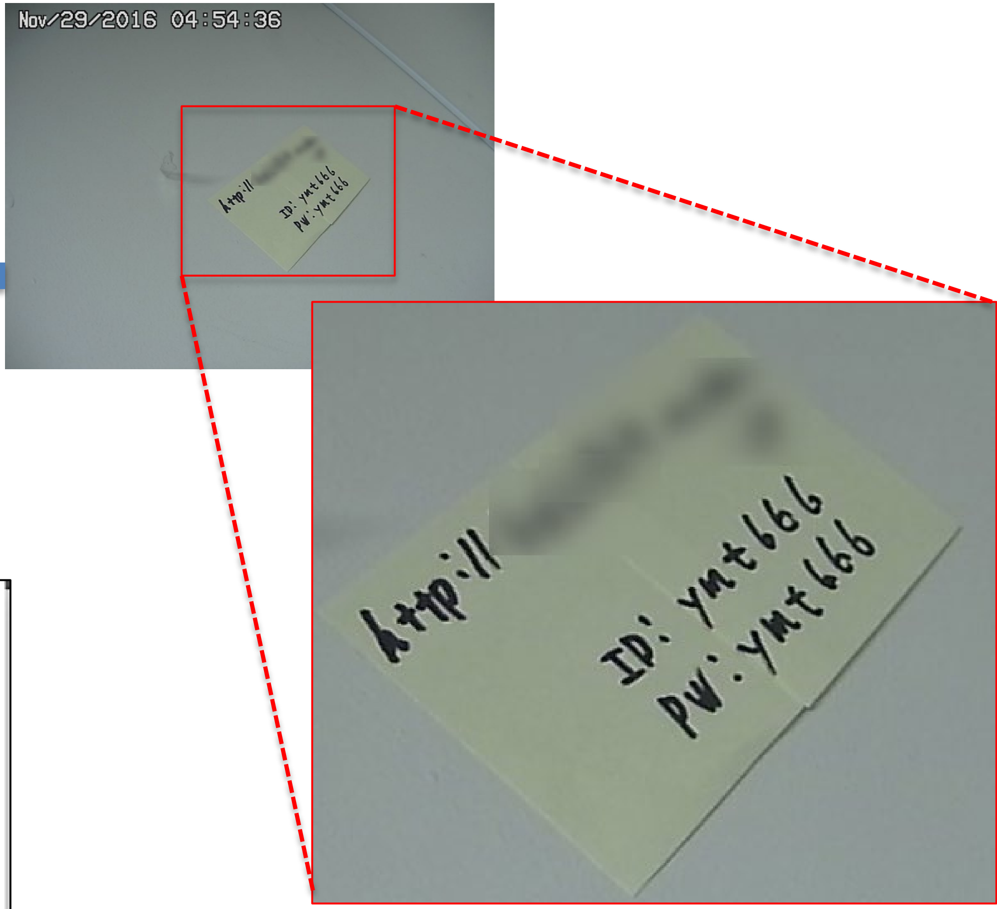
Decoy IP Camera monitoring living room (“living room honey camera”)

monitoring a room for observation simulating a living room at home

More “interesting” camera view for observing long-term peeping

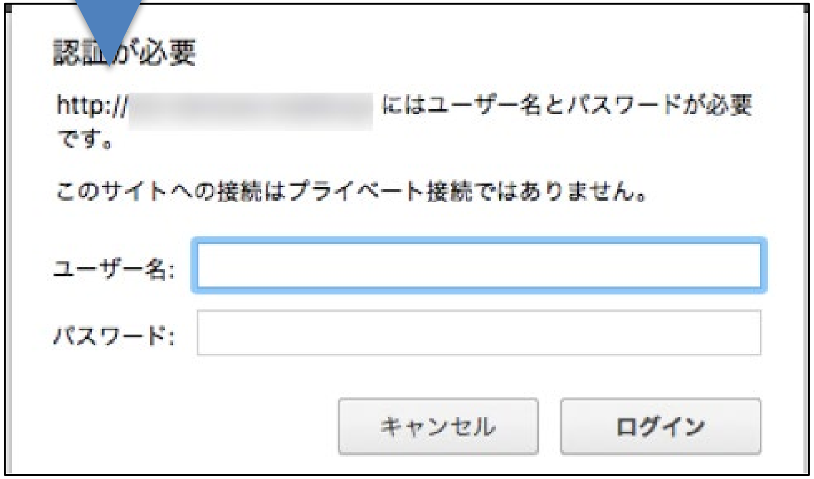
URL honey camera

1. Peeping



2. Access URL

3. Enter ID / Password



認証が必要

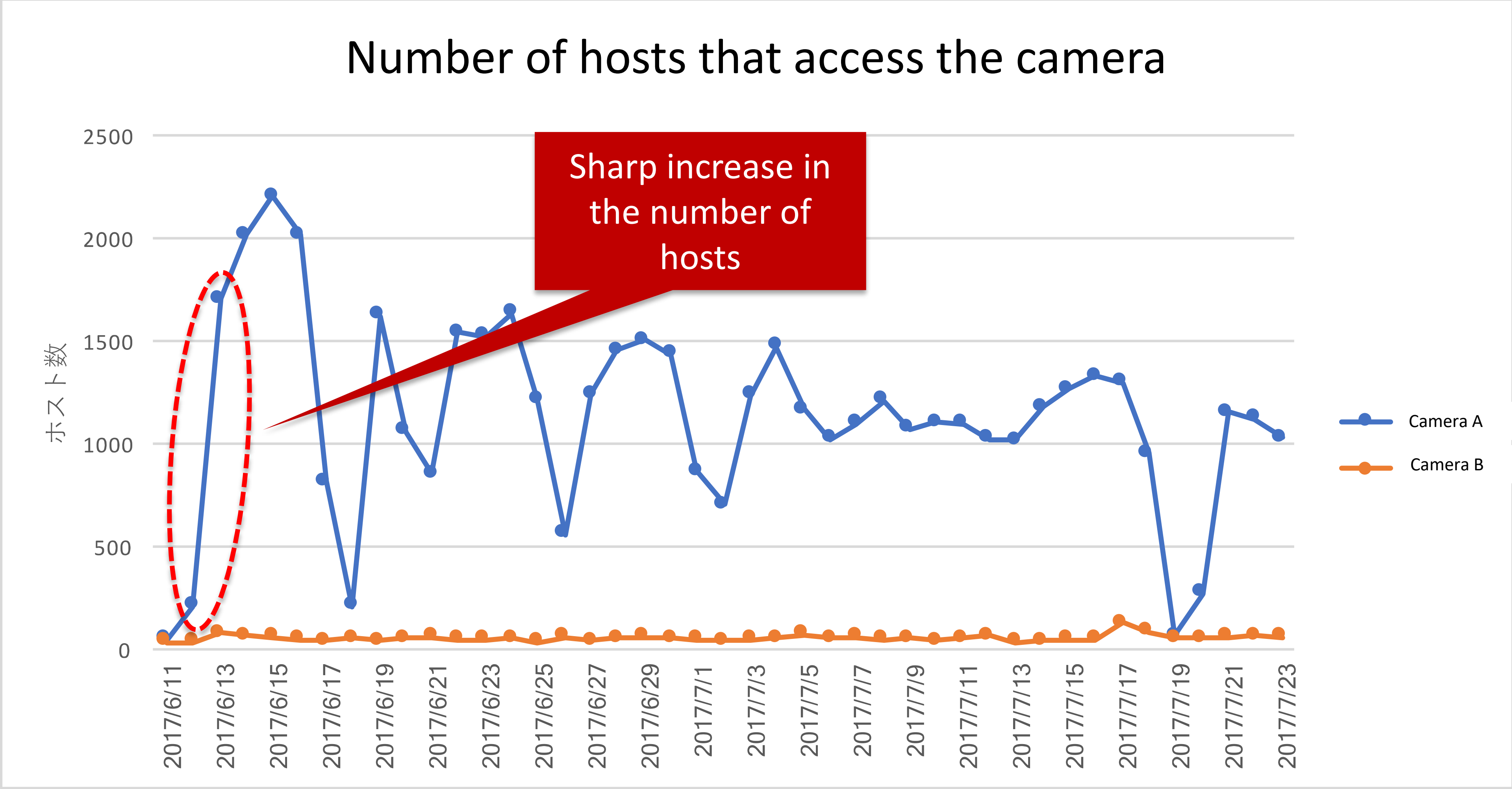
http://[redacted] にはユーザー名とパスワードが必要です。

このサイトへの接続はプライベート接続ではありません。

ユーザー名:

パスワード:

Observation result with URL honey camera



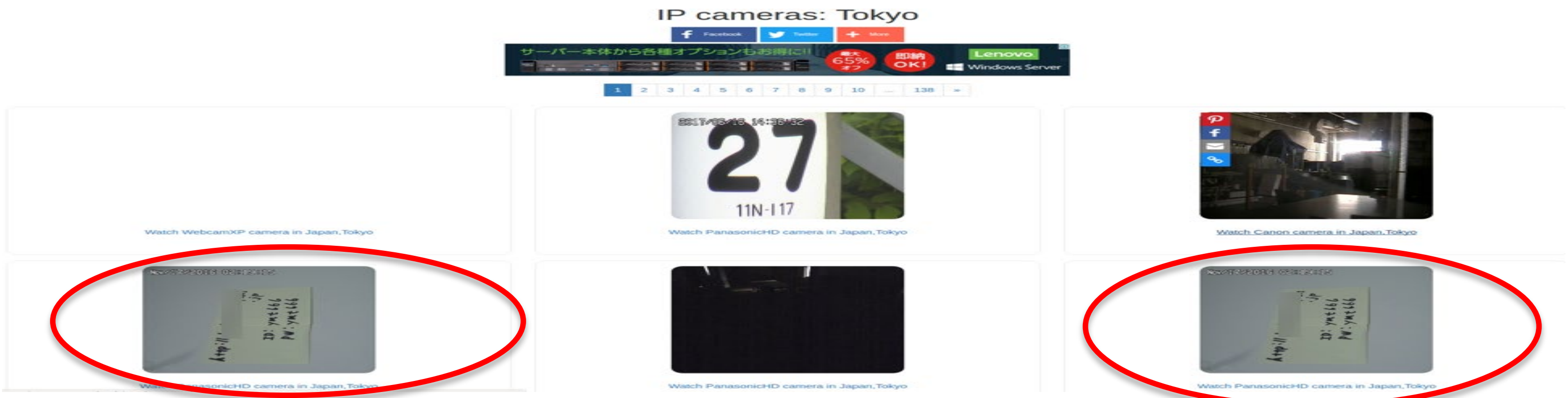
Sharp increase in the number of hosts

Insecam registration

- Massive requests via insecam were observed

```
GET /xxxxxxx/xxxxx?resolution=640&amp;quality=1&amp;
Language=0&amp;COUNTER HTTP/1.1
Referer: http://www.insecam.org/en/bycountry/JP/?page=4
```

- Honey cam was registered to insecam


IP cameras: Tokyo
Facebook
Twitter
More
1 2 3 4 5 6 7 8 9 10 … 138 »
Watch WebcamXP camera in Japan,Tokyo
Watch PanasonicHD camera in Japan,Tokyo
Watch Canon camera in Japan,Tokyo
Watch PanasonicHD camera in Japan,Tokyo
Watch PanasonicHD camera in Japan,Tokyo
Watch PanasonicHD camera in Japan,Tokyo

Peeps jumped to more than 20,000 times per day by the registration to Insecam

Access to the bait URL

Host that sent the request	Acess host using domain of URL	Login challenge host	Host that entered ID/password displayed on camera A
583	422	235	217

- Observed access to the bait URL from 422 IP addresses

Humans are watching images of cameras

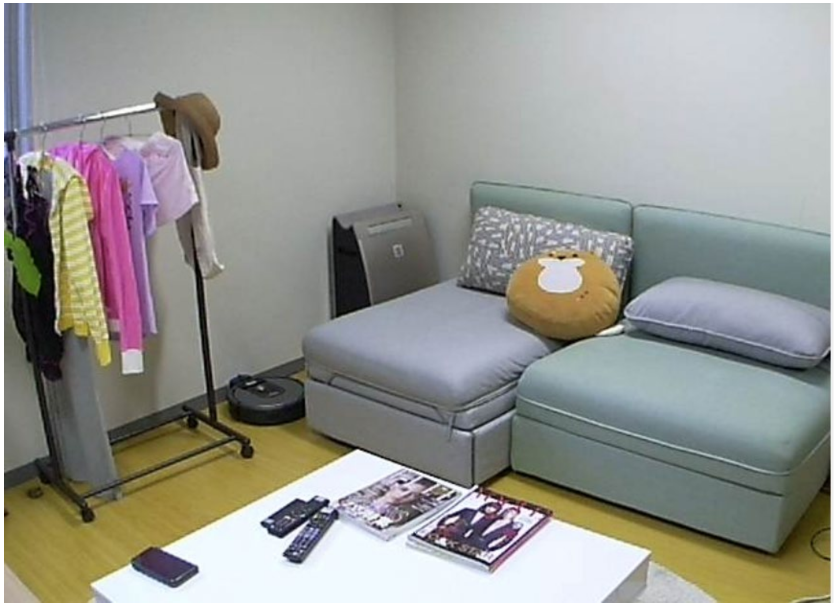
- 217 IP address entered ID / password displayed on camera A

Some peepers go “beyond peeping” (login challenge)

Decoy IP Camera monitoring living room

Decoy IP Camera with bait URL is static and not interesting.

We prepare a room that is more “interesting” and observe long-term peeping.



Experiment Overview

	Country	ID/password	IP address	Camera operation function	Observation period	Observed days
A	Japan	No authentication	10	✓	2017/10/06～ 2017/11/25	51d
C	Japan	No authentication	10	✓	2017/10/06～ 2017/11/25	51d
D	Japan	No authentication	10	✓	2017/10/06～ 2017/11/25	51d
E	Japan	No authentication	10	×	2017/10/06～ 2017/11/25	51d
F	China	admin/****** (Default)	1	✓	2017/09/21～ 2017/11/25	66d

※Living honey camera A and URL honey camera A are the same type

Access to living room honey camera

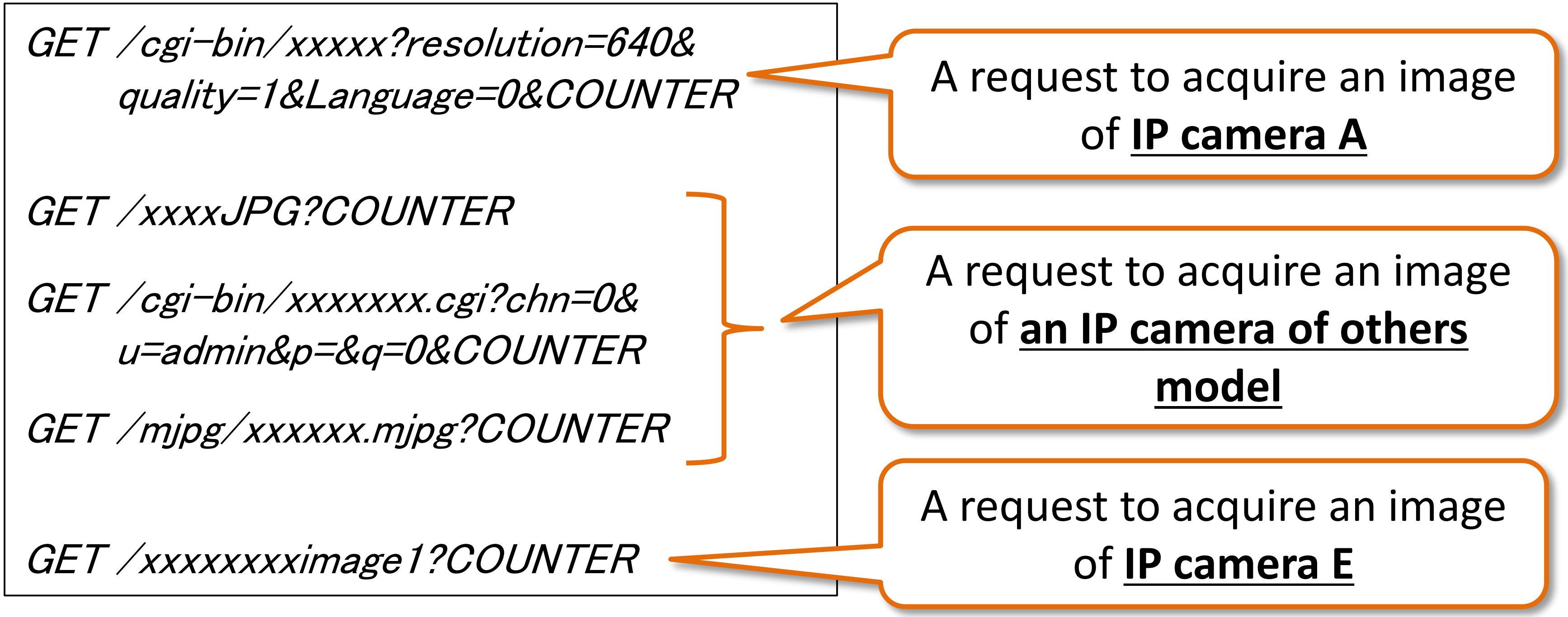
	Host that sent the request	Login host	Peeping host	Host that operated the camera
A	1755		33	8
C	1998		66	18
D	1806		13	1
E	1749		4	
F	876	51	32	6

- Peeping in for a long time(Camera A)
- Peeping with vulnerability exploitation(Camera F)
- Changing the port for camera viewing (Camera F)

- None of the cameras were registered to Insecam, but multiple and continuous peeps were observed

Camera controlled by an attacker

Automated image acquisition for multiple cameras



```
GET /cgi-bin/xxxxx?resolution=640&
        quality=1&Language=0&COUNTER

GET /xxxxJPG?COUNTER

GET /cgi-bin/xxxxxxx.cgi?chn=0&
        u=admin&p=&q=0&COUNTER

GET /mjpg/xxxxxx.mjpg?COUNTER


GET /xxxxxxxximage1?COUNTER
```

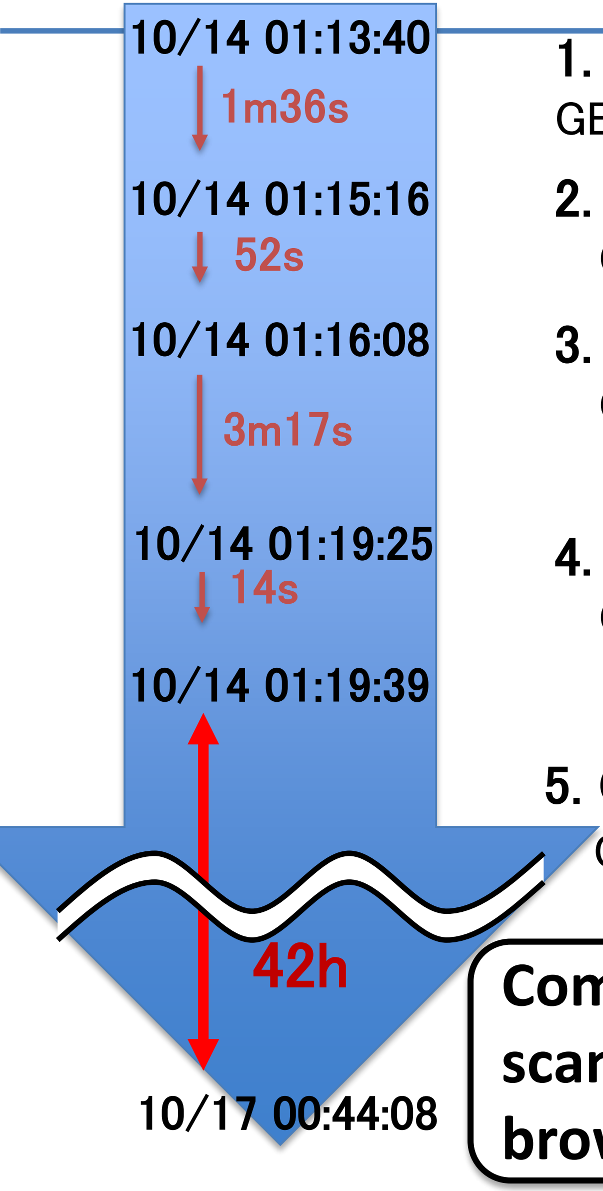
A request to acquire an image of **IP camera A**

A request to acquire an image of **an IP camera of others model**

A request to acquire an image of **IP camera E**

We observed automated requests **collecting images from multiple IP cameras**

Continuous and “efficient” peeping



10/14 01:13:40

1m36s

10/14 01:15:16

52s

10/14 01:16:08

3m17s

10/14 01:19:25

14s

10/14 01:19:39

42h

10/17 00:44:08

1. Automated search for cameras Tools

GET /xxxxxx.cgi?user=yyyy&pwd=yyyyy

2. Automated search for cameras Tools

GET /cgi-bin/xxxxxx

3. Manual peep using browser (access by human)

GET /cgi-bin/xxxx?resolution=1280x960&quality=1 &page=yyy&Language=z

4. Image acquisition of camera A using tool Tools

GET /xxxxxxxxJPEG , GET /cgi-bin/xxxxxx

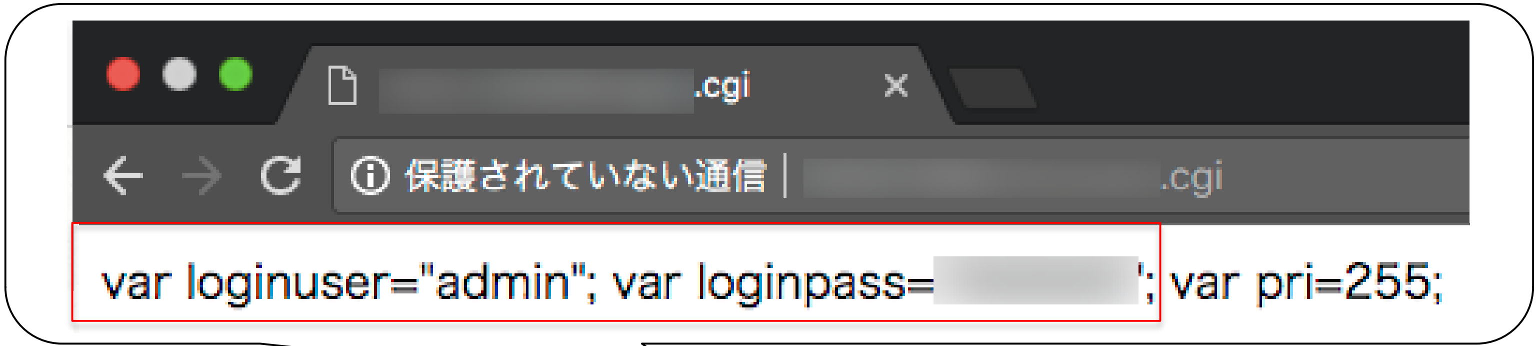
5. Continuous and automated acquisition of images Tools

GET /cgi-bin/xxxxxx?fake=yyyy

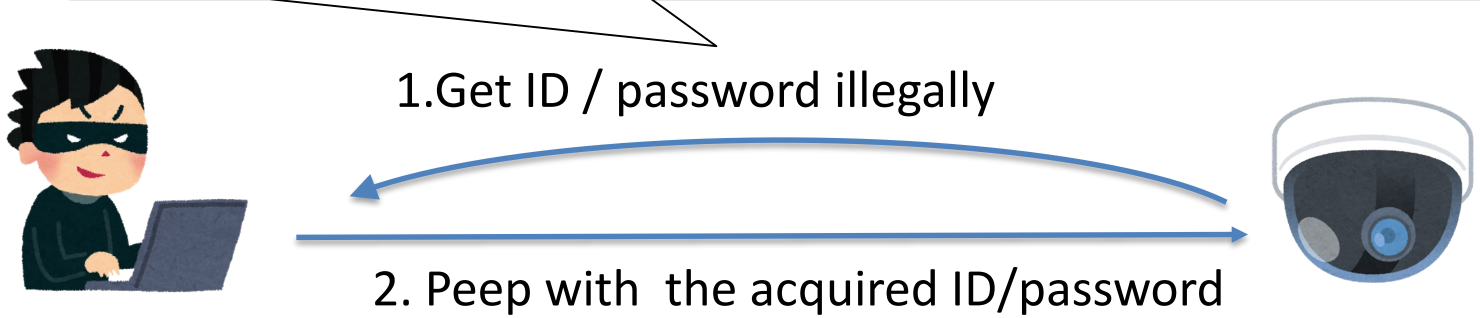
Combination of automated accesses by camera scanner and auto image capture and manual browsers access (by human) are observed

Peeping with vulnerability exploitation(Camera F)

- Camera F vulnerability
  - ID / password can be acquired without authentication by specific request
- Observed access flow(4 IP address)



```
var loginuser="admin"; var loginpass=[redacted]"; var pri=255;
```



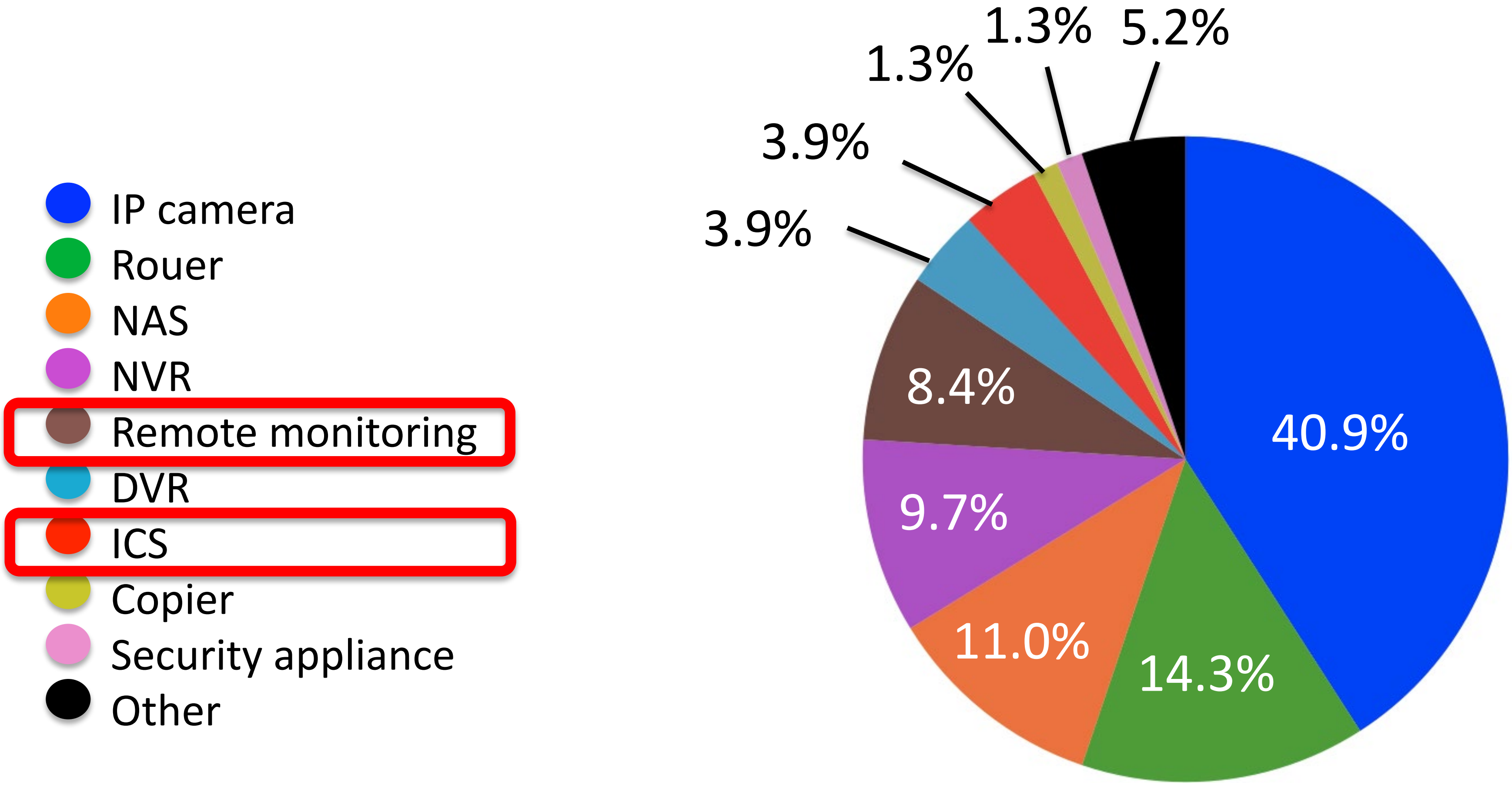
1.Get ID / password illegally

2. Peep with the acquired ID/password

EFFORT FOUR: UNDERSTANDING THE RISK OF INSECURE/EXPOSED FACILITIES

Discovered IoT devices

- We found 154 models of IoT devices in single AS



Case:

Waterworks Monitoring System

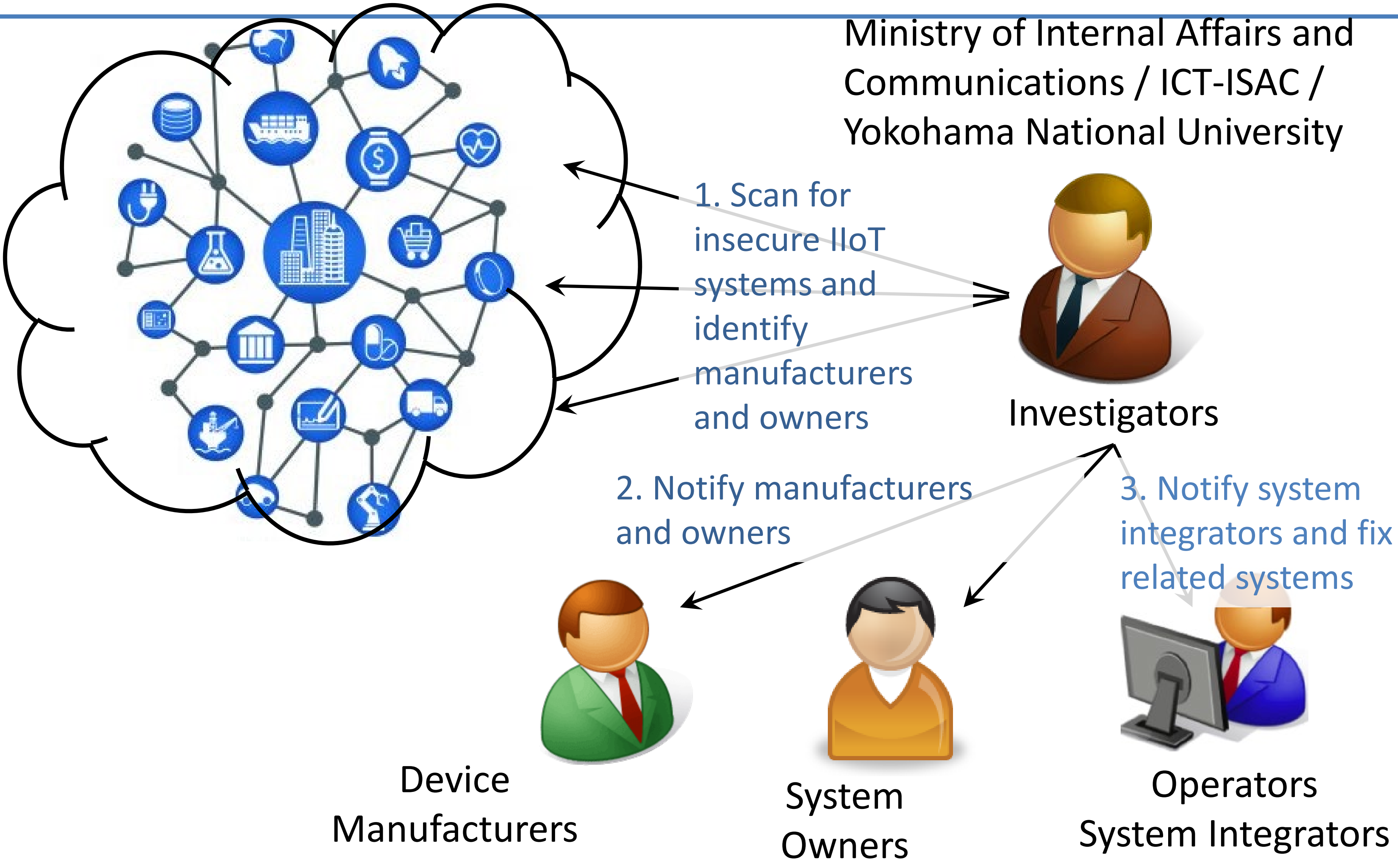
Example Case:

River Gate

Case:

Power Substation

Investigation by the government (2017)



Ministry of Internal Affairs and Communications / ICT-ISAC / Yokohama National University

1. Scan for insecure IIoT systems and identify manufacturers and owners

Investigators

2. Notify manufacturers and owners

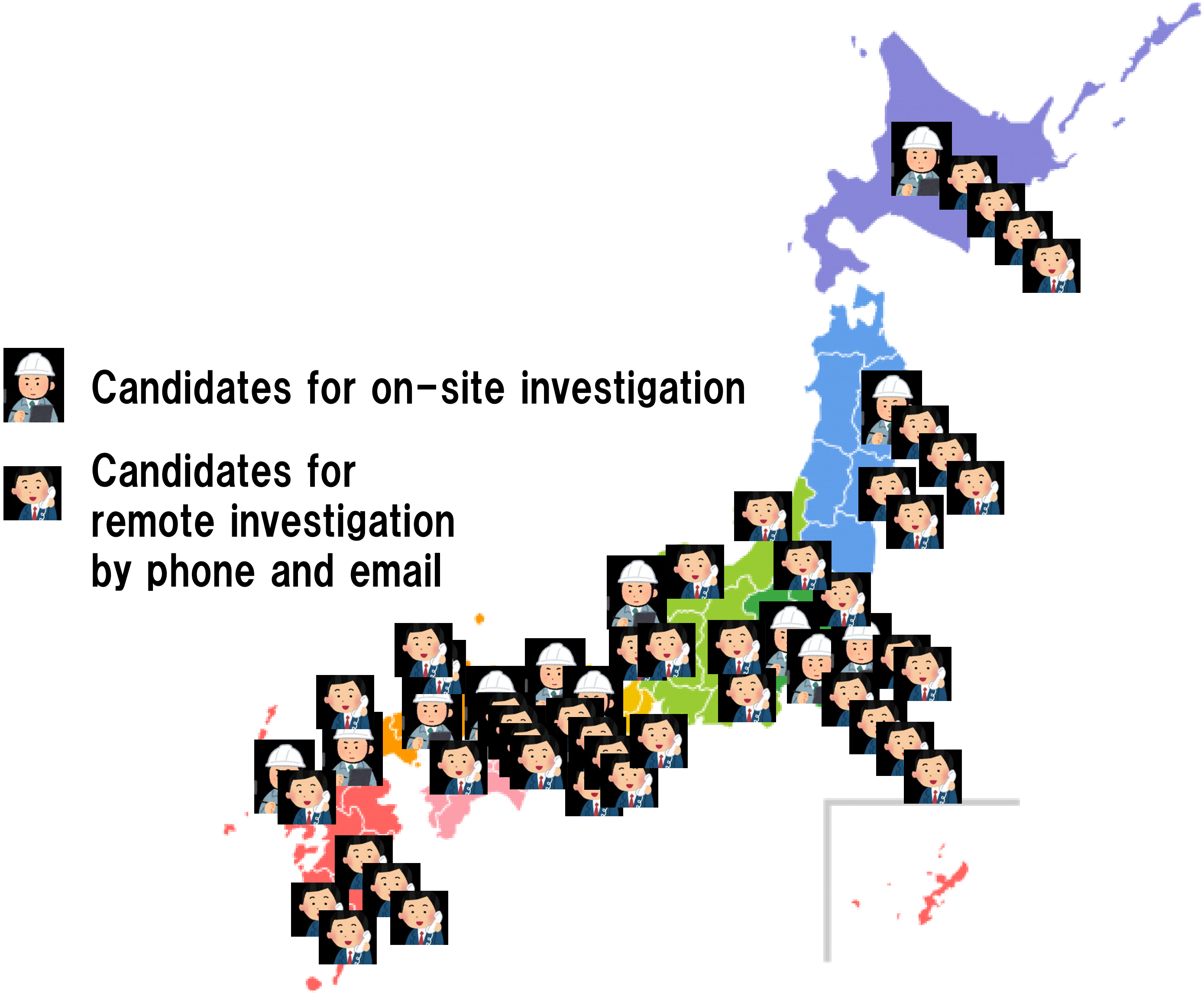
3. Notify system integrators and fix related systems

Device Manufacturers

System Owners

Operators System Integrators

Discovered candidates for investigations



Candidates for on-site investigation

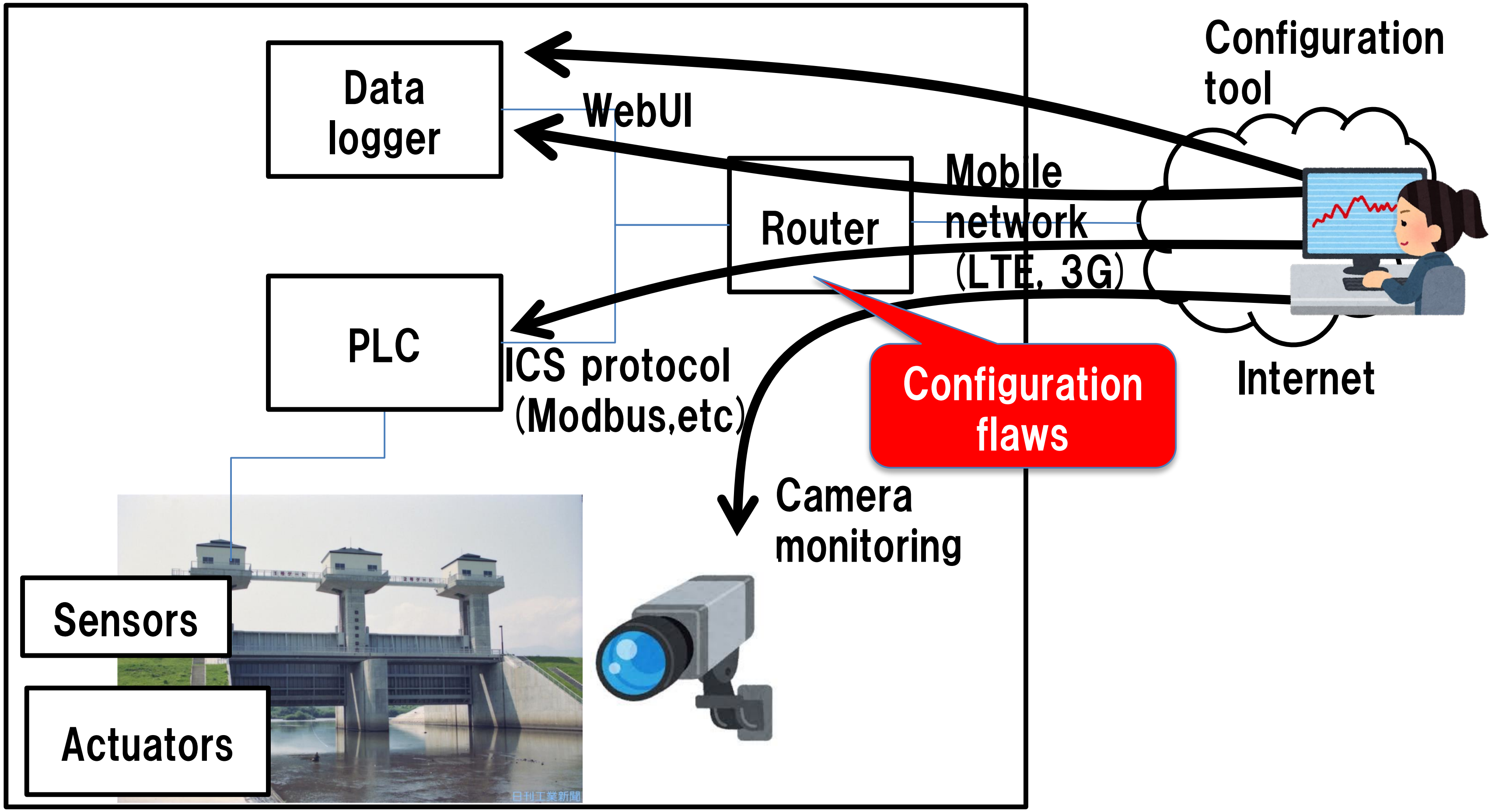
Candidates for remote investigation by phone and email

Summary of investigation results (published by MIC)

- Discovered vulnerable devices: 150
- Device users can be inferred:77
- Notified and fixed:36

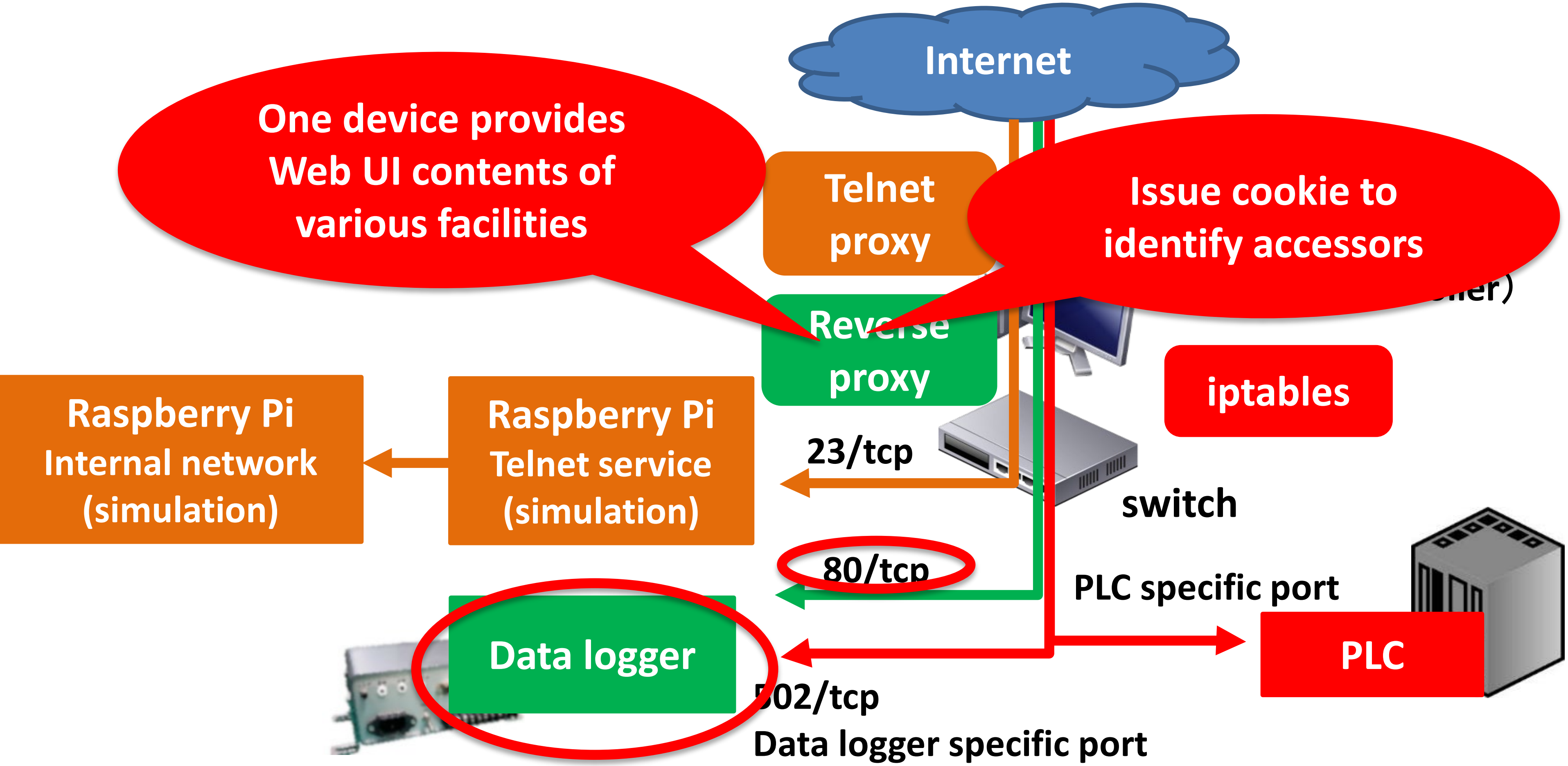
- Example of the discovered facilities/system
  - Power monitoring
  - Water level monitoring
  - Safety control system for disaster
  - Gus monitoring and alert system

Typical connection of discovered facilities



Honeypot of remote monitoring system

- We build the honeypot using real PLC and data logger


Internet
One device provides Web UI contents of various facilities
Telnet proxy
Issue cookie to identify accessors
ller)
Reverse proxy
iptables
Raspberry Pi Internal network (simulation)
Raspberry Pi Telnet service (simulation)
23/tcp
switch
80/tcp
PLC specific port
Data logger
PLC
502/tcp
Data logger specific port

Observation experiment

- Period：Sep 8th 2018 ~ Dec 6th 2018（89 days）
- Observation in 30 IP addresses

Refer to 14 critical infrastructure fields[6]
Identified by *N*ational center of *I*ncident readiness and *S*trategy for *C*ybersecurity (NISC)

28 IP addresses

Critical infrastructures
（14×2 = 28）

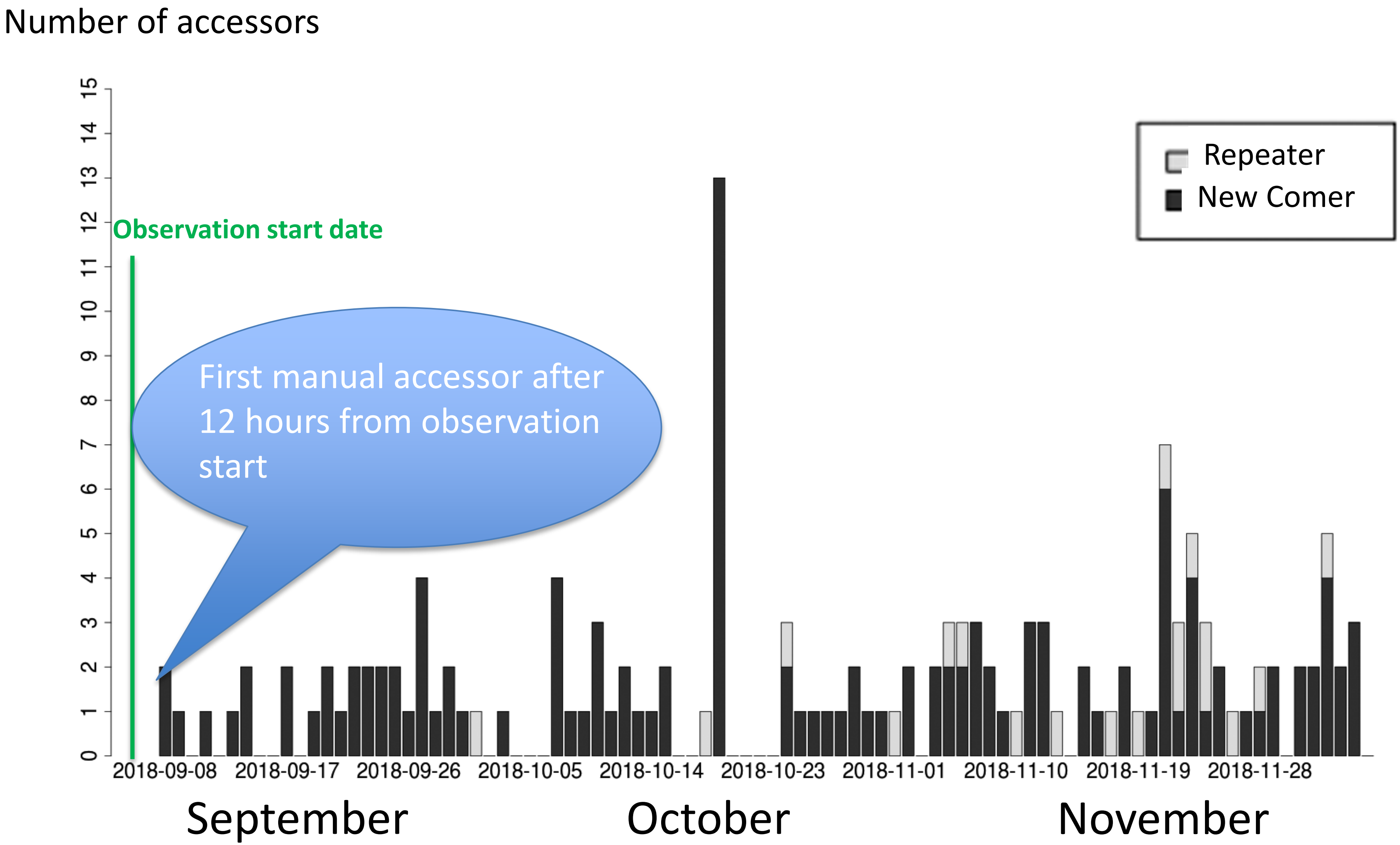
2 IP addresses

Non-critical infrastructure
（School、Commercial facility）

- Access to honeypot without authentication

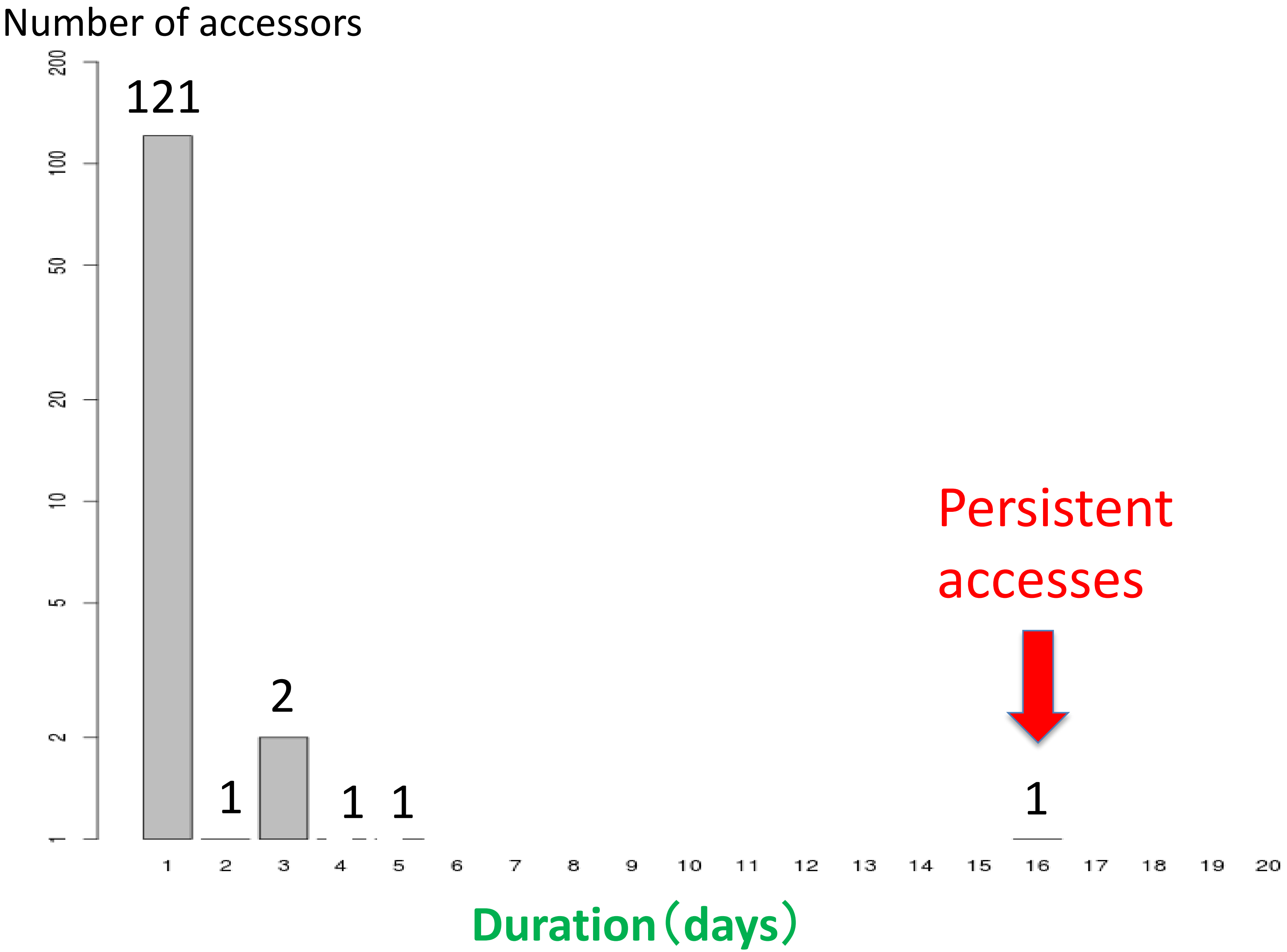
[6] National center of Incident readiness and Strategy for Cybersecurity(NISC), “4th Action Plan for Information Security Countermeasure of Critical Infrastructure, ” https://www.nisc.go.jp/active/infra/outline.html (last visited 2019/01/16)

Access to honeypot (manual)

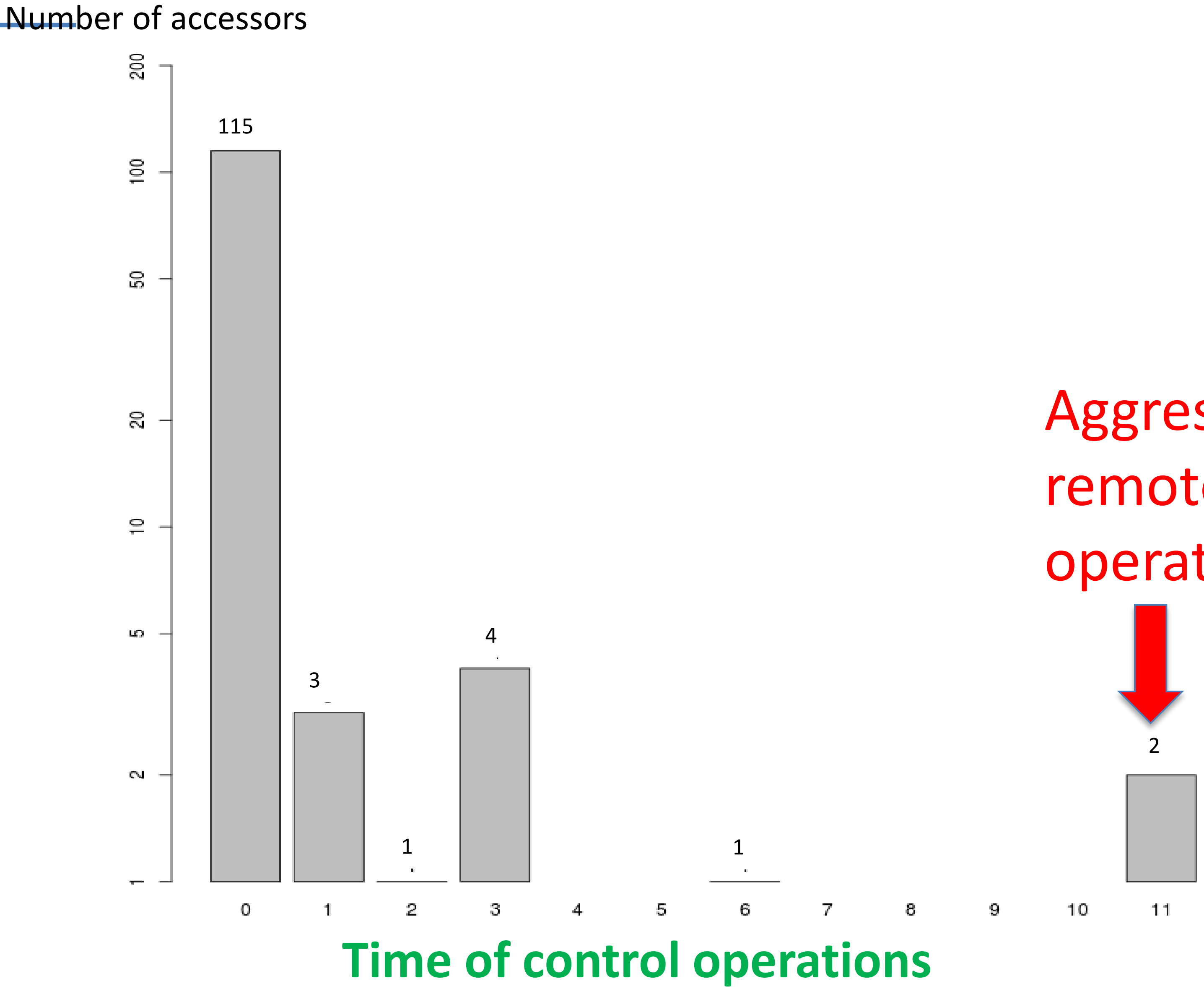


First manual accessor after 12 hours from observation start

Duration of each manual access

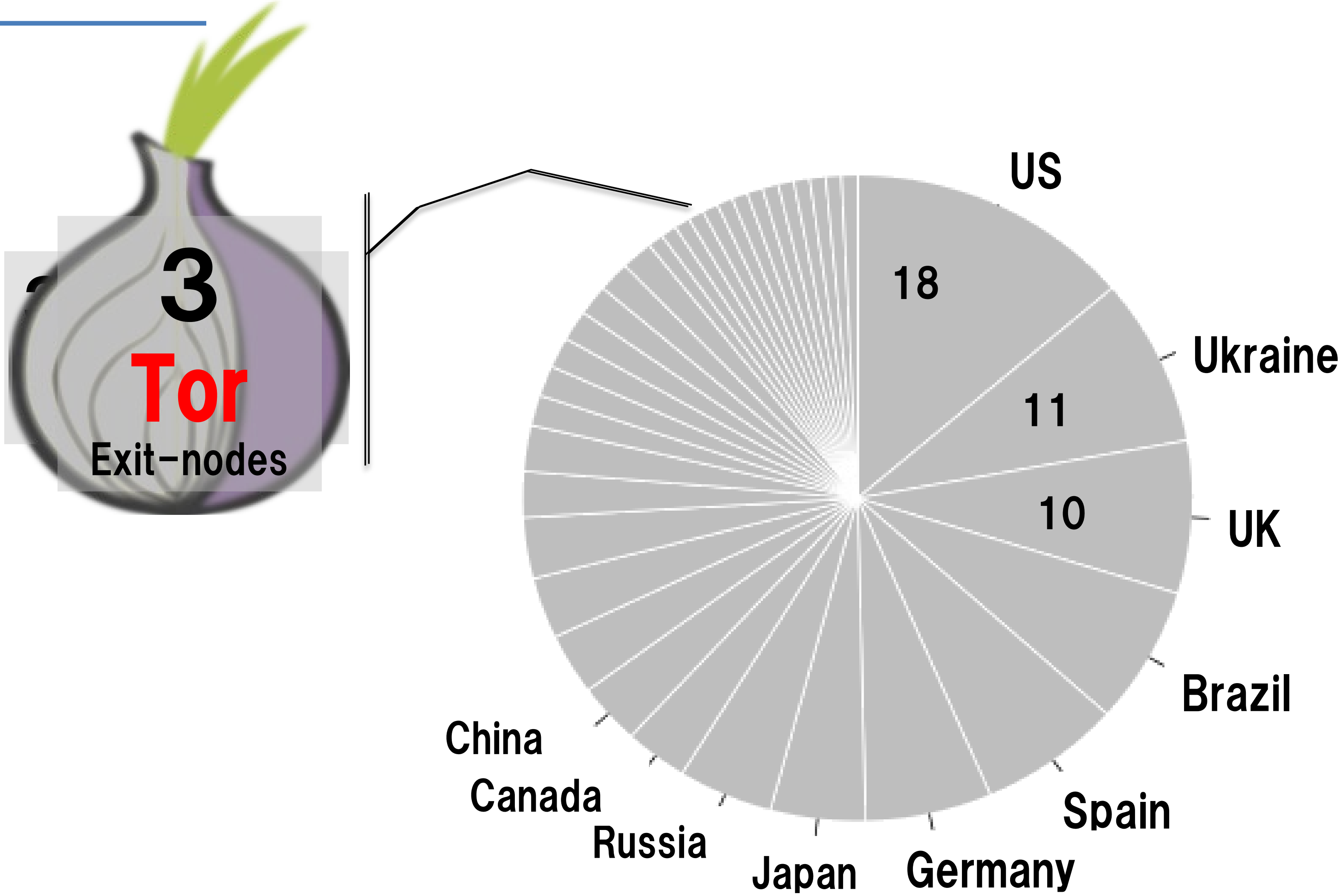


Critical control operations

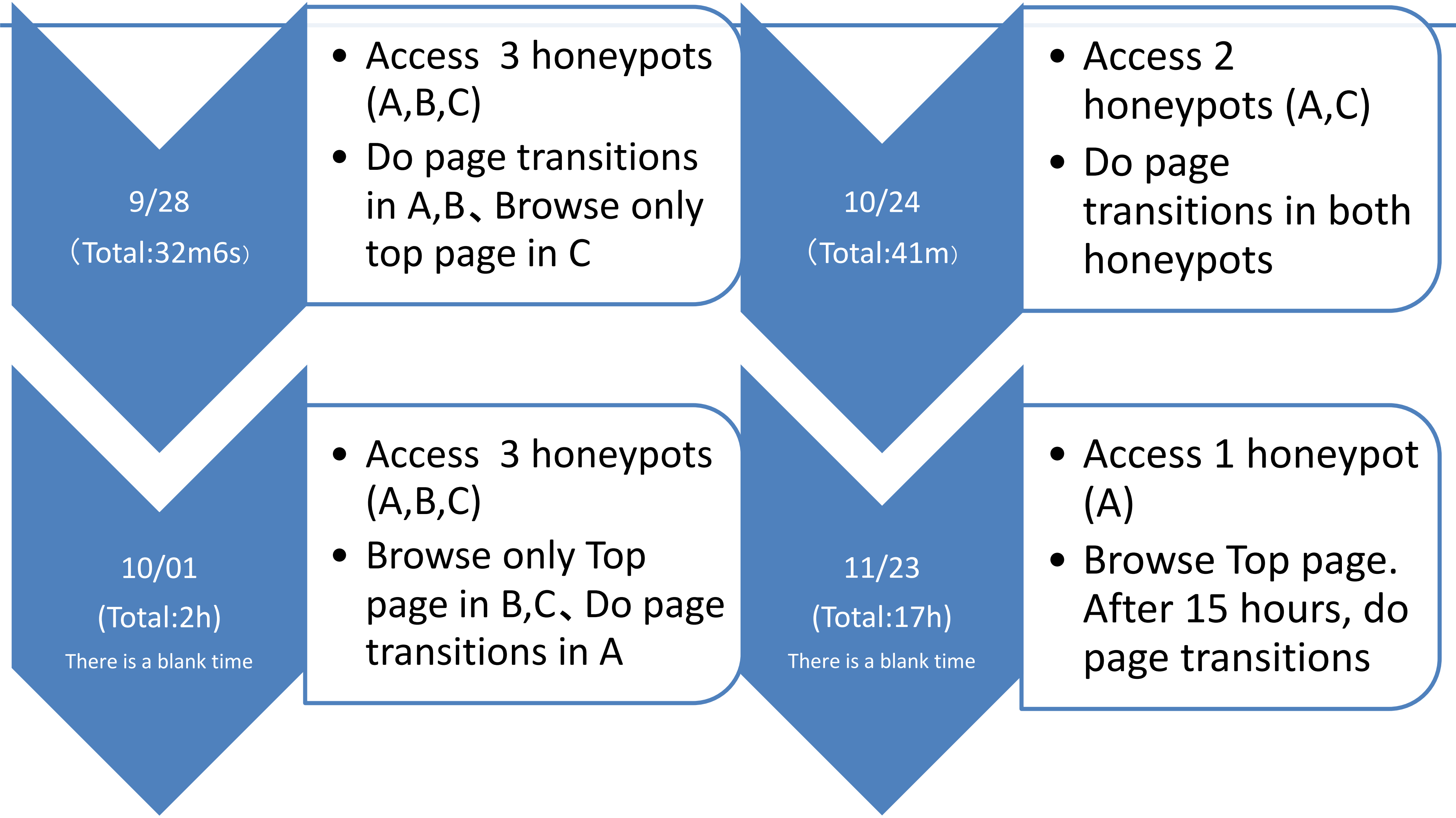


Aggressive remote operation

Source of manual accesses



“Careful” visitor



9/28

（Total:32m6s）

- Access 3 honeypots (A,B,C)
- Do page transitions in A,B、Browse only top page in C

10/01

(Total:2h)

There is a blank time

- Access 3 honeypots (A,B,C)
- Browse only Top page in B,C、Do page transitions in A

10/24

（Total:41m）

- Access 2 honeypots (A,C)
- Do page transitions in both honeypots

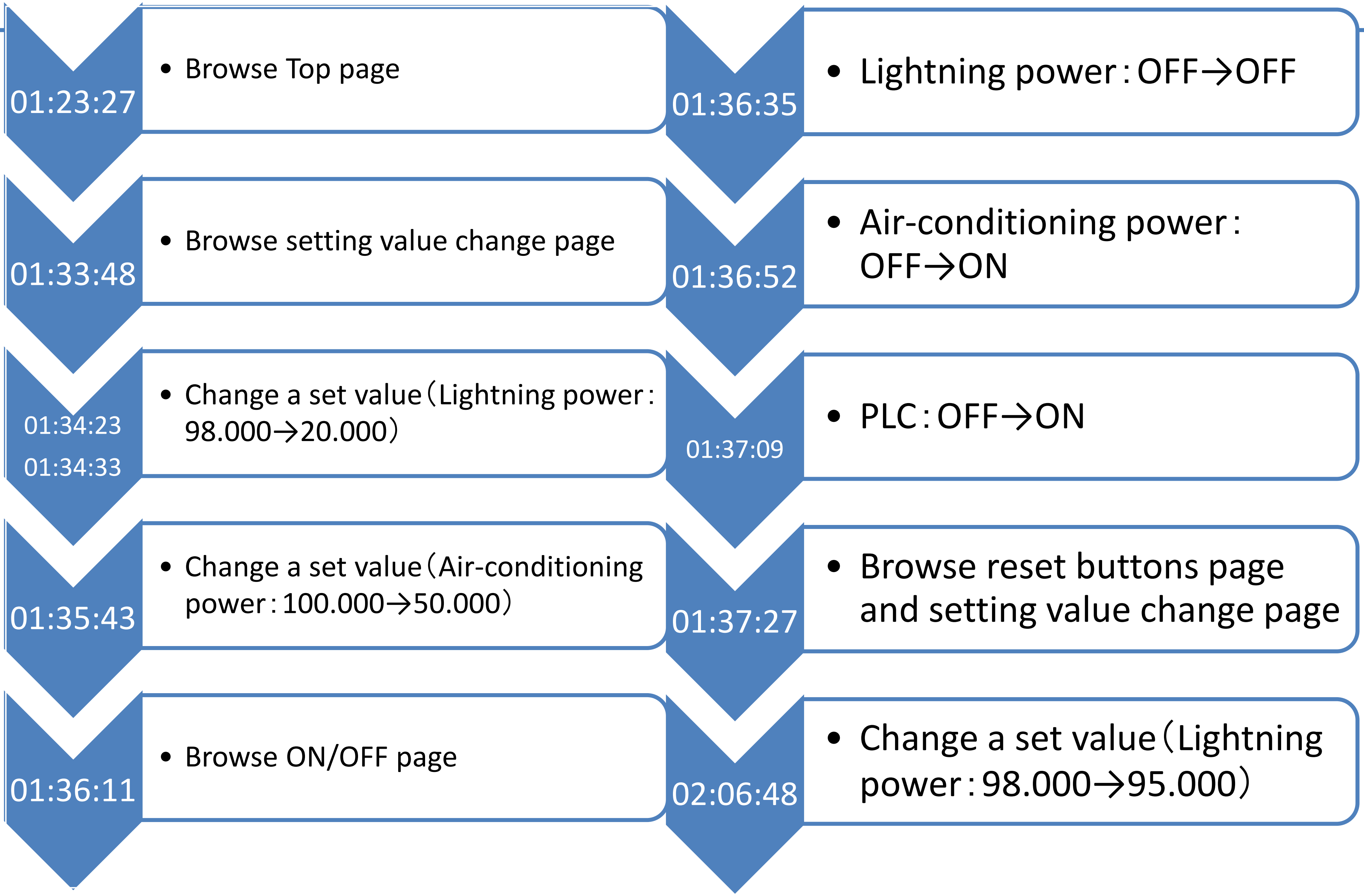
11/23

(Total:17h)

There is a blank time

- Access 1 honeypot (A)
- Browse Top page. After 15 hours, do page transitions

“Aggressive” visitor



01:23:27
- Browse Top page

01:33:48
- Browse setting value change page

01:34:23
01:34:33
- Change a set value（Lightning power：98.000→20.000）

01:35:43
- Change a set value（Air-conditioning power：100.000→50.000）

01:36:11
- Browse ON/OFF page

01:36:35
- Lightning power：OFF→OFF

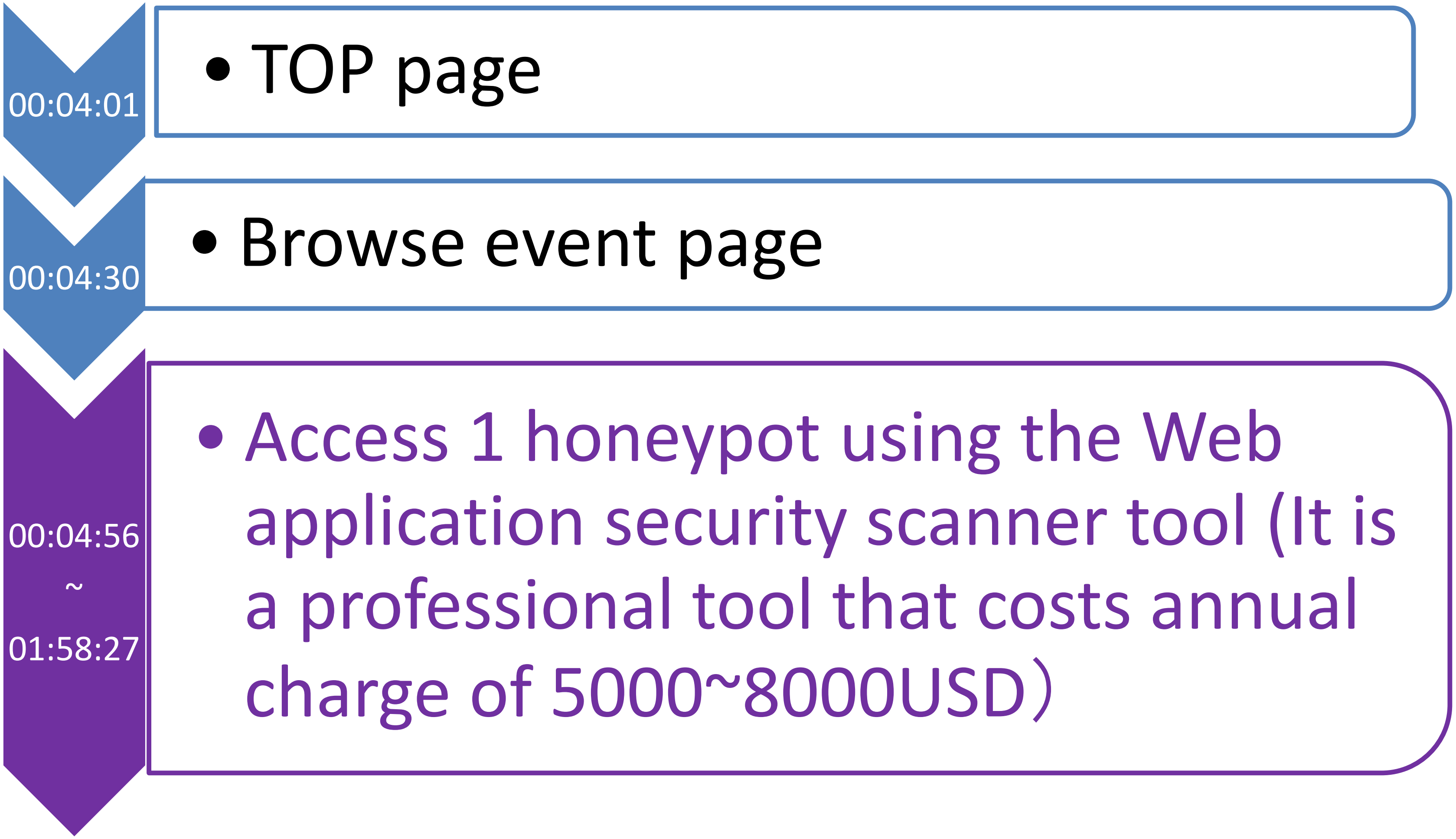
01:36:52
- Air-conditioning power：OFF→ON

01:37:09
- PLC：OFF→ON

01:37:27
- Browse reset buttons page and setting value change page

02:06:48
- Change a set value（Lightning power：98.000→95.000）

“Rich” visitor



00:04:01

- TOP page

00:04:30

- Browse event page

00:04:56 ~ 01:58:27

- Access 1 honeypot using the Web application security scanner tool (It is a professional tool that costs annual charge of 5000~8000USD）

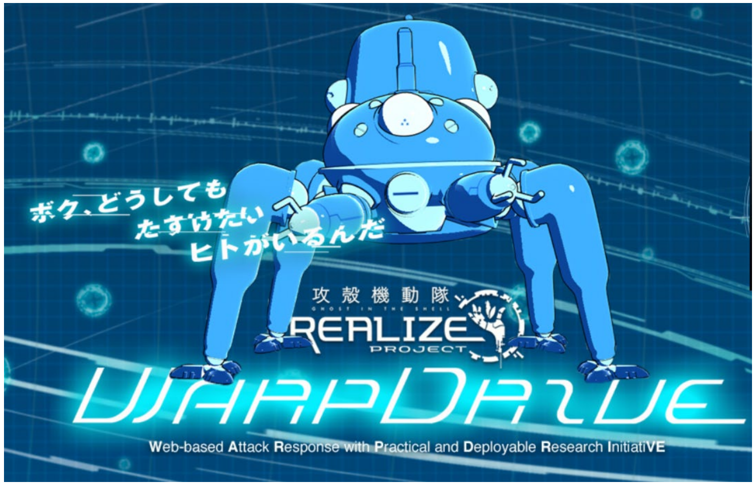
We informed about these observation to MIC

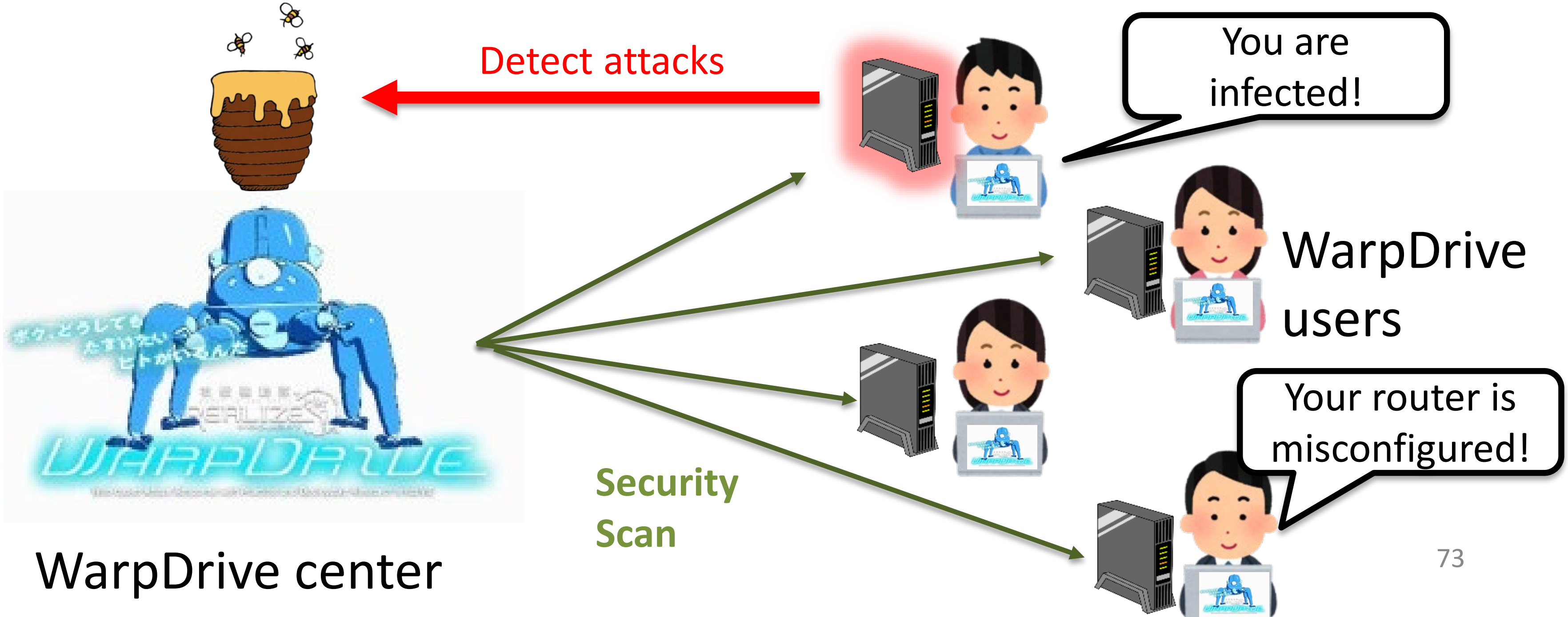
Summary

- People are not yet aware of the risk of connecting “things” to the world and thus creating the big “mess”.
- Combination of active and passive monitoring helps understanding the situation.
- Notification is the key activity for making the situation better. (Japanese government (MIC, NICT) just initiated huge nation-wide investigation and notification project for insecure IoT devices.)
- Reaching “last one mile” to the end users is the key for effective notification.

In order to reach the last one mile…

In NICT-sponsored security project WarpDrive, we have distributed dedicated security agents (Tachikoma security agent) to 7000+ end-users for assisting their security.


ボク、どうしても
たすけたい
ヒトがいるんだ
攻殻機動隊
REALIZE
PROJECT
WARPDRIVE
Web-based Attack Response with Practical and Deployable Research InitiatiVE



Thank you!

Katsunari Yoshioka, Ph.D
Yokohama National University
yoshioka@ynu.ac.jp

For more, please visit:

IoTPOT – Analysing the Rise of IoT Compromises, Yokohama National University
http://ipsr.ynu.ac.jp/iot/

References:

O. Cetin, C. Ganan, L. Altena, D. Inoue, T. Kasama, K. Tamiya, Y. Tie, K. Yoshioka, M. van Eeten, "Cleaning Up the Internet of Evil Things: Real-World Evidence on ISP and Consumer Efforts to Remove Mirai," The Network and Distributed System Security Symposium (NDSS 2019), 2019.

Yin Minn Pa Pa, Suzuki Shogo, Katsunari Yoshioka, Tsutomu Matsumoto, Takahiro Kasama, Christian Rossow "IoTPOT: A Novel Honeypot for Revealing Current IoT Threats," Journal of Information Processing, Vol. 57, No. 4, 2016.

Yin Minn Pa Pa, Shogo Suzuki, Katsunari Yoshioka, and Tsutomu Matsumoto, Takahiro Kasama, Christian Rossow, "IoTPOT: Analysing the Rise of IoT Compromises," 9th USENIX Workshop on Offensive Technologies (USENIX WOOT 2015), 2015.