Security considerations for a vehicular multimedia architecture - from use of IoT perspective -

Koji Nakao

ITU-T SG 17 – WP 2 (Cyber Space Security) Chairman

NICT - Distinguished Researcher,

Yokohama National University – Guest Professor,

CABINET SECRETARIAT – National center of Incident and readiness for Cybersecurity (NISC) – Security Advisor

Latest Threats based on Malwares

Malware Chronology (1960-2010)

Year	Malware
1960	
1961	Creeper (1st worm)
1962	# The term "virus" first appeared in a SF novel "When HARLIE Was O
1963	
1964	
1965	# The term "worm" first appeared in a SF novel"The Shockwave Rider"
1966	
1966	
1968	
1969	
1980	Xerox PARC Worm
1981	
1982	Elk Cloner(1st virus)
1983	
1984	# Cohen defined virus in his paper "Computer Viruses - Theory and Exp
1985	
1986	Brain (1st IBMPC virus), PC-Write (1st Trojan horse), Virdem
1986	Cascade, Jerusalem, Lehigh, Christmas Tree, MacMag
1988	Byte Bandit, Stoned, Scores, Morris Worm
1989	AIDS(1stransomware), Yankee Doodle, WANK

Discovery

Year	Malware
1990	1260 (1st polymorphic virus), Form, Whale
1991	Tequila, Michelangelo, Anti-Telefonica, Eliza
1992	Peach (1st anti-antivirus programs), Win.Vir_1_4 (1st Windows virus)
1993	PMBS
1994	Good Times (1st hoax)
1995	Concept (1st macro virus)
1996	Laroux, Staog (1st Linux m.w.)
1996	ShareFun, Homer, Esperanto
1998	Accessiv, StrangeBrew (1st Java m.w.), Chernobyl
1999	Happy99, Tristate, Melissa, ExploreZip, BubbleBoy, Babylonia
2000	Loveletter, Resume, MTX,Hybris
2001	Anna Kournikova,BadTrans, CodeRed I, Sircam,CodeRed II, Nimda, K
2002	LFM-926 (1st Flash m.w.), Chick, Fbound,Shakira, Bugbear
2003	Sobig, SQLSlammer, Deloder, Sdbot, Mimail, Antinny, MSBlaster, Wel Agobot, Swen, Sober
2004	Bagle, MyDoom, Doomjuice, Netsky,WildJP, Witty,Sasser, Wallon, Bob Cabir(1stSymbianm.w.), Amus, Upchan , Revcuss, Lunii, Minuka, Vund
2005	Bropia, Locknut,BankAsh,Banbra, Anicmoo, Commwarrior, Pgpcoder, Gargafx, Peerload, Cardblock,PSPBrick (1st PSP m.w), DSBrick (1st Nin m.w.), Dasher
2006	Kaiten, Leap (1st Mac OS X m.w.),Redbrowser, Cxover,Exponny, Mdropper,Flexispy, Spaceflash,Stration, Mocbot, Fujacks, Allaple
2006	Storm Worm,Pirlames, Zlob, Srizbi (1st full-kernel m.w.), Silly, Pidief
2008	Mebroot,Infomeiti, Conficker
2009	Virux, Yxes,Gumbler, Induc, Ikee (1stiPhonem.w.)
2010	Zimuse, Trojan-SMS.AndroidOS.FakePlayer (1st Androidm.w.), Stuxnet

Experimentation

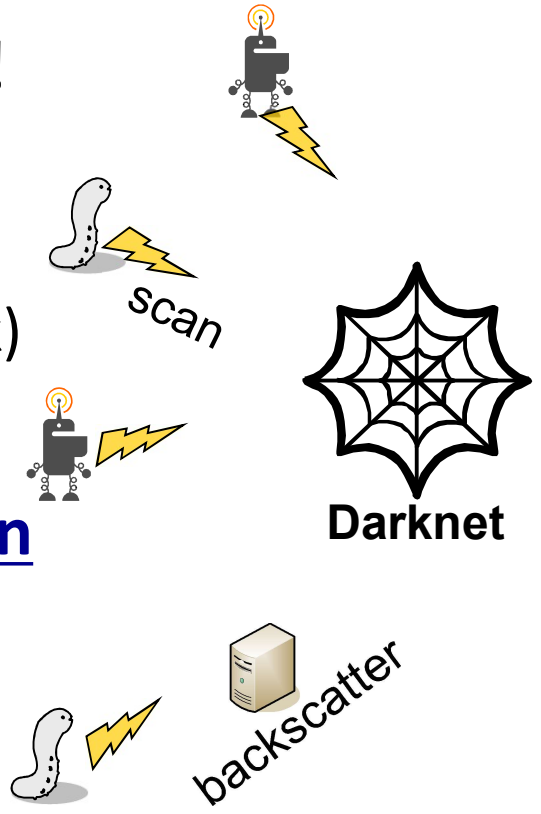
Criminal Exploitation

Types of Malwares (purpose basis)

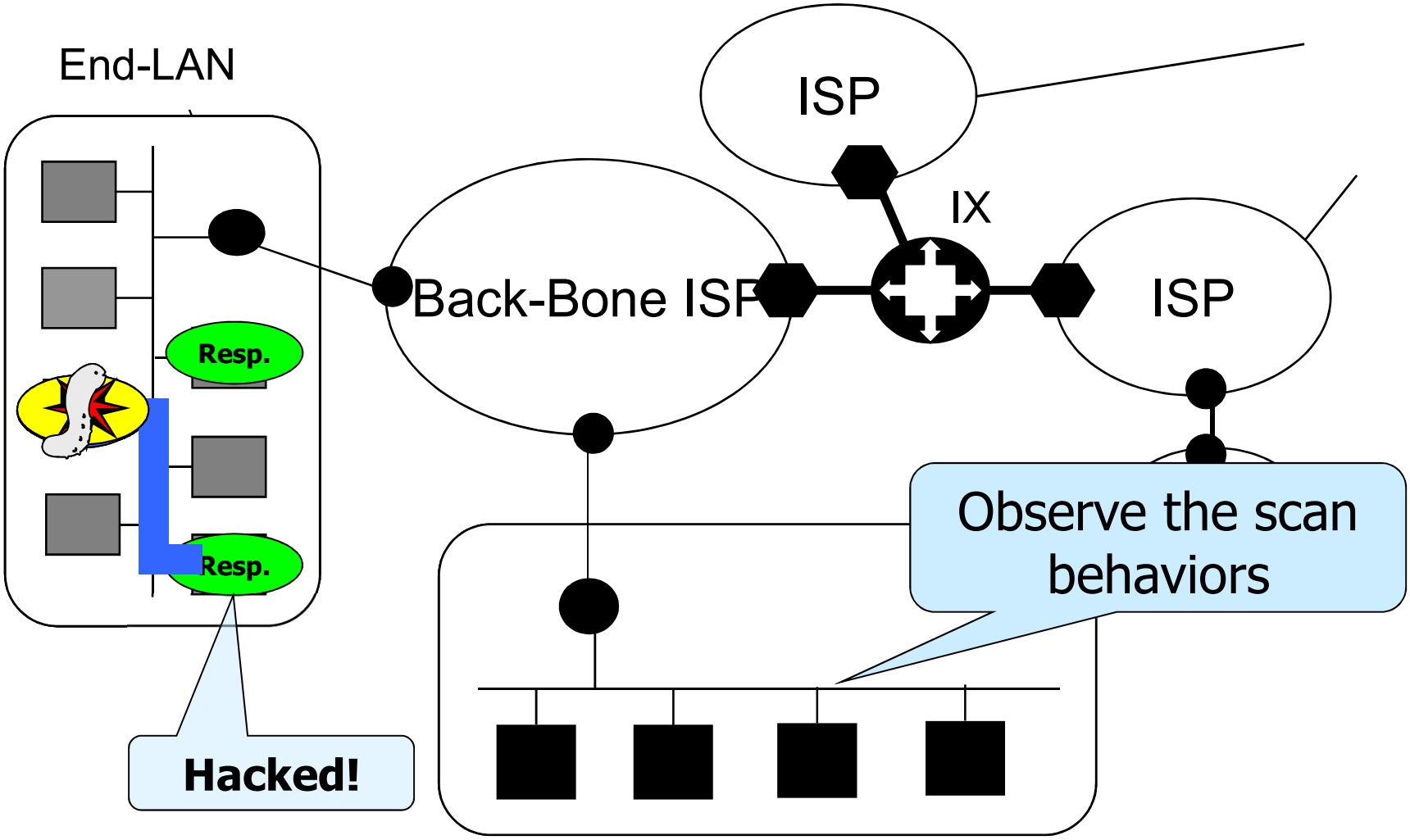
- Spyware
  - ✓ **Spyware** is a type of
    small pieces of infor
    spyware is typically
    also categorized in s
- Adware (Advertising-Su
  - ✓ **Adware** is any softw
    advertisements to a
    Adware, by itself, is
    spyware such as key
- Ransomware
  - ✓ **Ransomware** is com
    contains, hostage ag
- Scareware
  - ✓ **Scareware** comprise
    limited or no benefi
    practices. The sellin
    perception of a thre

What is Darknet?

- **Darknet**: Unused IP addresses space
- **In theory**: any packets should **NOT** arrive at the darknet because they are not connected to any hosts.
- **In fact**: quite a few packets **DO** arrive!
- Packets arriving at the darknet are…
  - **Scans by malwares**
  - Backscatter (reflection of DDoS attack)
  - Miss configurations etc.
- Darknet traffic reflects **global trend in malicious activities** on the Internet.



Malware infection behavior and Darknet monitoring



Atlas: Geographical Traffic Visualization

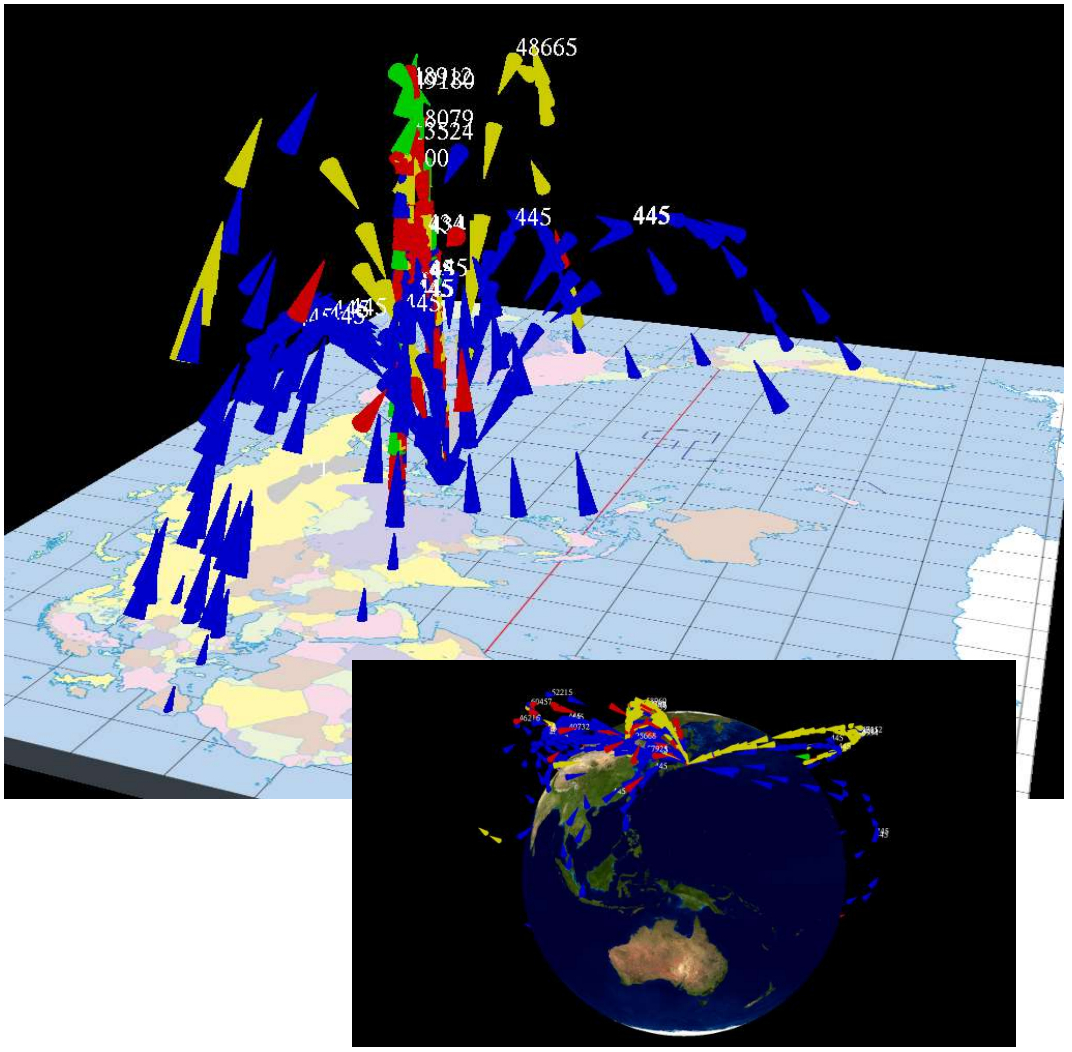
• Shows geographical positions of a packet's src and dst from the IP addresses **in real-time**

•**Each packet** is represented by **a rocket** traversing from source to destination

• The **color** of the rocket indicates the type of packet

• The **altitude** of the rocket is in proportion to its dst port number

- **UDP**
- **TCP SYN**
- **TCP SYN/ACK**
- **TCP Other**
- **ICMP**

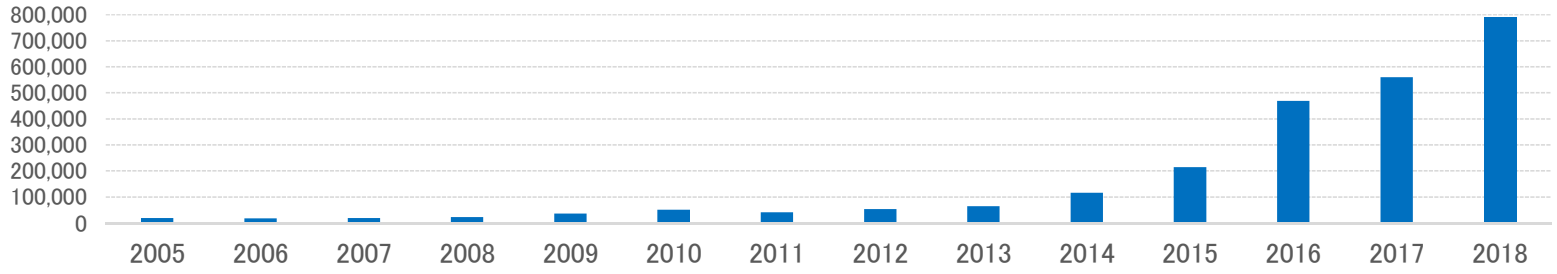


Yearly Stats of Darknet Traffic（2005-2018）

Year	Number of Packets (yearly)	Num. of Observed IPs	Captured number of Packets in 1 IP address
2005	約 3.1億	16000	19,066
2006	約 8.1億	100000	16,231
2006	約19.9億	100000	19,118
2015	約545.1億	280000	213,523
2016	約1,281億	300000	469,104
2016	約1,504億	300000	559,125
2018	**約212,100,000,000**	**300000**	**689,866**

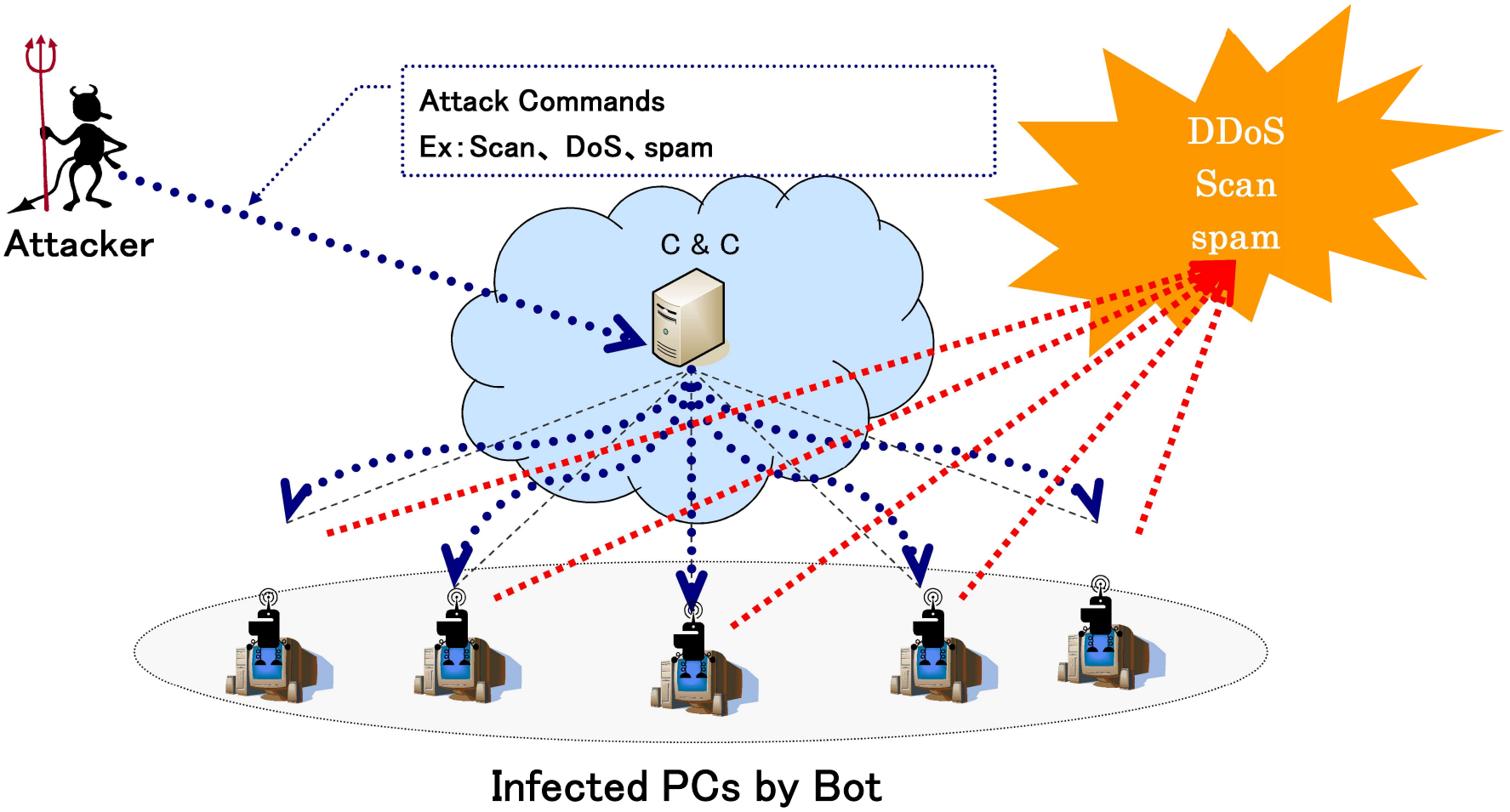
In our NICTER (darknet), number of captured packets per a single darknet IP address is

689,866 in 2018!!!



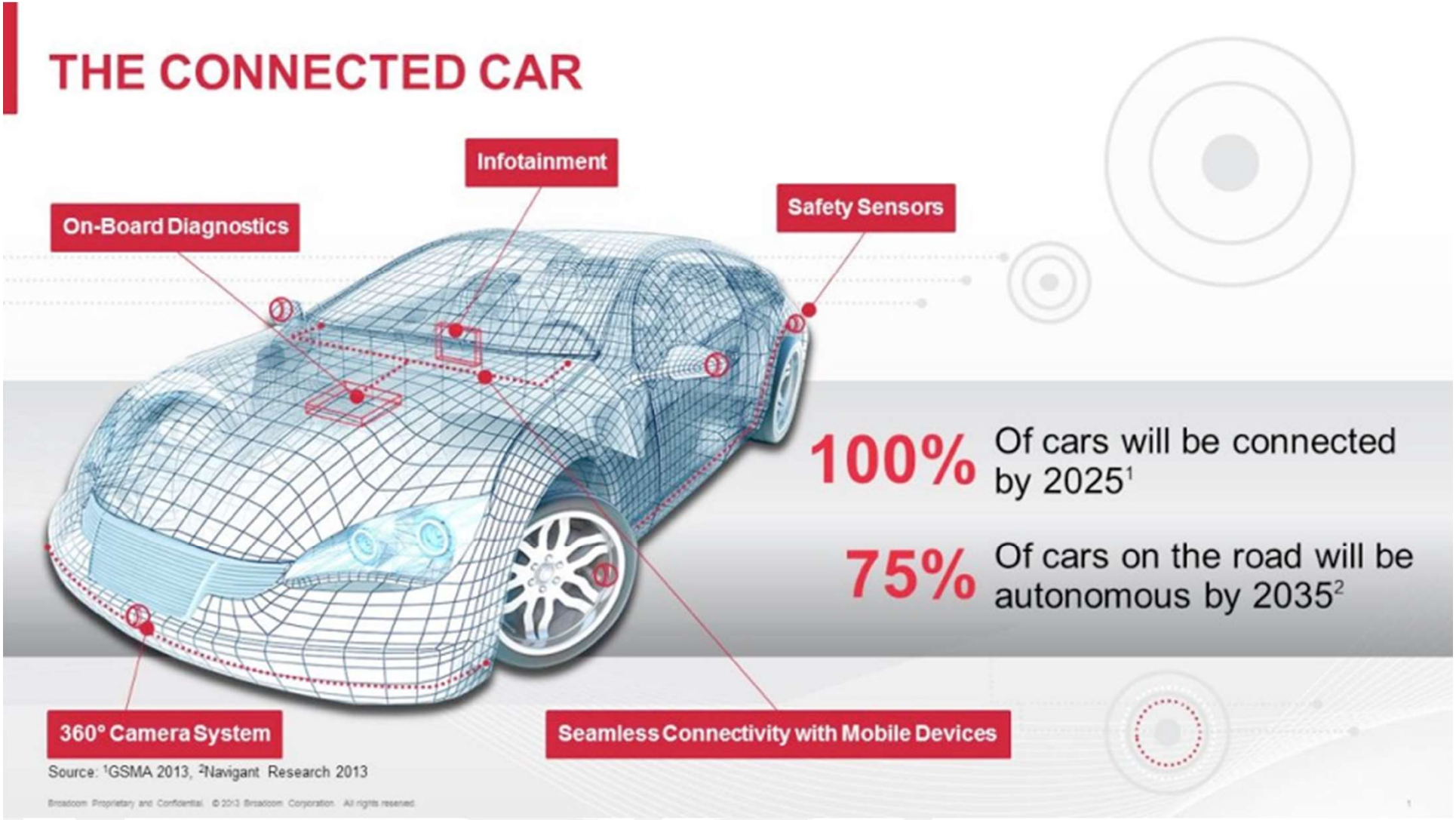
Captured number of Packets in 1 IP Address

Botnet (Basic tool of Attacks)



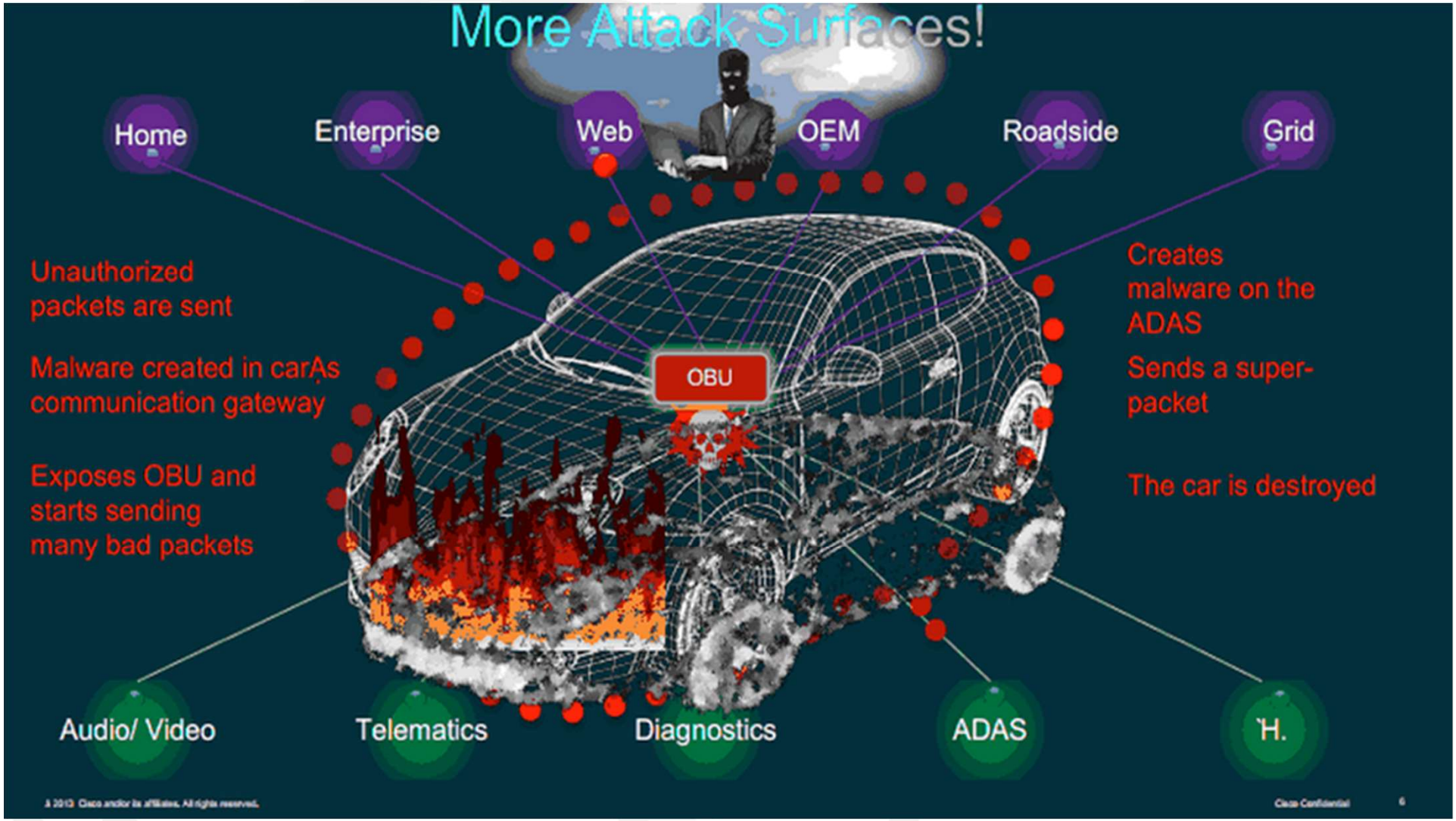
Issues related to “Vehicle Multimedia” in SG 17 (Security)

Focus on “Connected Car”



http://johndayautomotivelectronics.com/top-five-technologies-enabling-the-connected-car/

Increasing Attack Surfaces



http://gigaom.com/2013/08/06/ciscos-remedy-for-connected-car-security-treat-the-car-like-an-enterprise/

X.1361: Security threats in connected vehicles

Determined at the last SG16:
Based on the result of UNECE WP29 TFCS
(Recommendation Cybersecurity)

Scope :

Recommendation X.1361 describes security threats to connected vehicles (vehicle eco-system), for reference and use in other Recommendations developed by ITU-T . It identifies security threats to the connected vehicle (eco-system).

Content

National Institute of Information and Communications Technology

6.2 Threats to vehicles regarding their communication channels

There are communication channels in vehicles including external communications such as connect to back-end servers and/or other vehicles and in-vehicle communications such as CAN, LIN (Local Interconnect Network), MOST (Media Oriented Systems Transport), and FlexRay. Communication channels may be used as attack interfaces for spoofing, eavesdropping, manipulating messages, and so on.

a. Spoofing messages or data received by the vehicle
b. Communication channels used to conduct unauthorized manipulation, deletion or other amendments to vehicle-held code/data
c. Untrusted/unreliable messages through communication channels or session hijacking/replay attacks by means of vulnerable communication channels
d. Information disclosure
e. Denial of service attacks via communication channels to disrupt vehicle functions
f. Privileged access by an unprivileged user
g. Viruses embedded in communication media
h. Messages with malicious content

6.5 Threats to vehicles regarding their external connectivity and connections

For a variety of convenient services, vehicles can be equipped with components to communicate with back-end servers and can communicate to everything enabled by road users over a wireless connection. The more vehicles connect to external entities for enhancing connectivity, the more threats and vulnerabilities show up because attack surfaces are expanded which are led by additional interfaces.

a. Manipulation of the connectivity of vehicle functions

b. Hosted third-party software

An infotainment system of the modern vehicles that can be connected to the in-vehicle network may allow installation of 3rd party applications. The 3rd party applications can be corrupted or have poor software security and be used as methods to attack vehicle systems.

c. Devices connected to external interfaces

- external interfaces such as USB port: they can be used to attack through code injection
- infected media with the virus: the virus can attack the in-vehicle system via the infected media
- diagnostic access: diagnostic functions accessed by Bluetooth dongles in OBD port are used to view the status of vehicles and manipulate vehicle parameters which are included in the vehicle software.

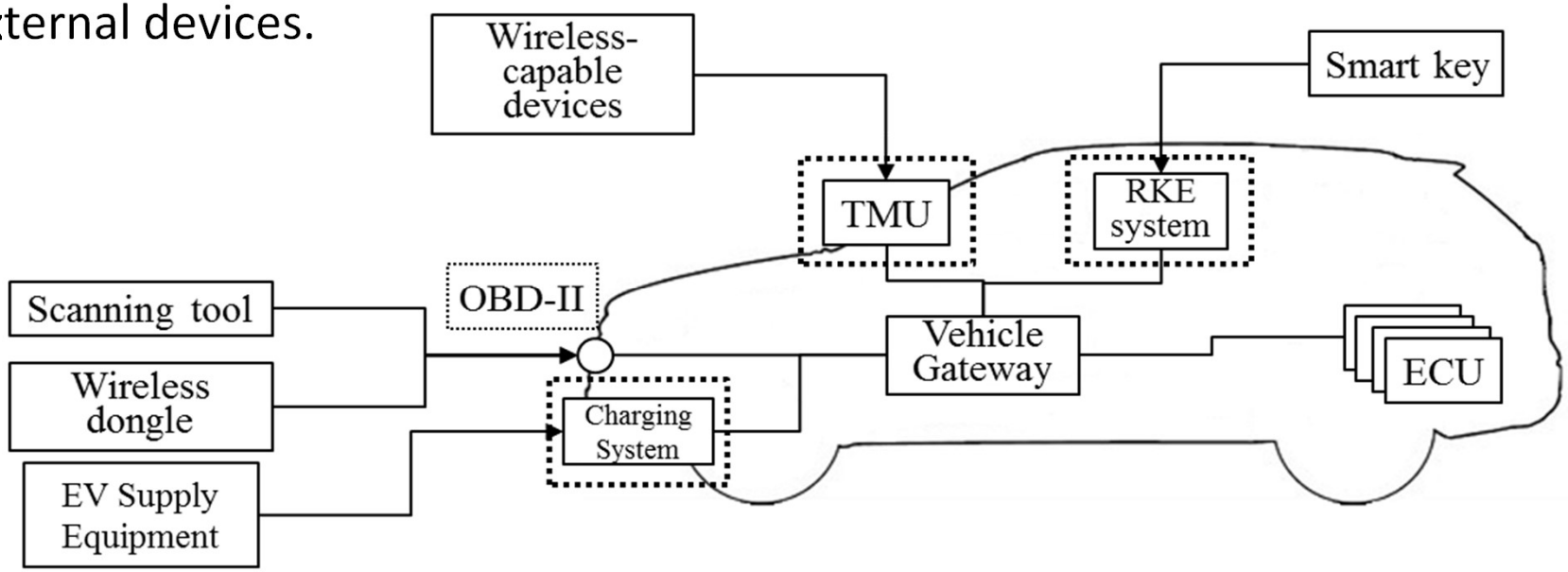
Draft Rec. X.itssec-3

Title: Security requirements for vehicle accessible external devices

Summary

- The purpose of this draft new Recommendation is to standardize security requirements for vehicle accessible external devices in telecommunication network environments.
- This draft new Recommendation provides security threats in vulnerable points like OBD-II port or wireless connectivity and security requirements for vehicle accessible external devices to secure access to the vehicle internal systems and safe usage of their information.

The following figure illustrates a set of assumed interfaces for accessing external devices.

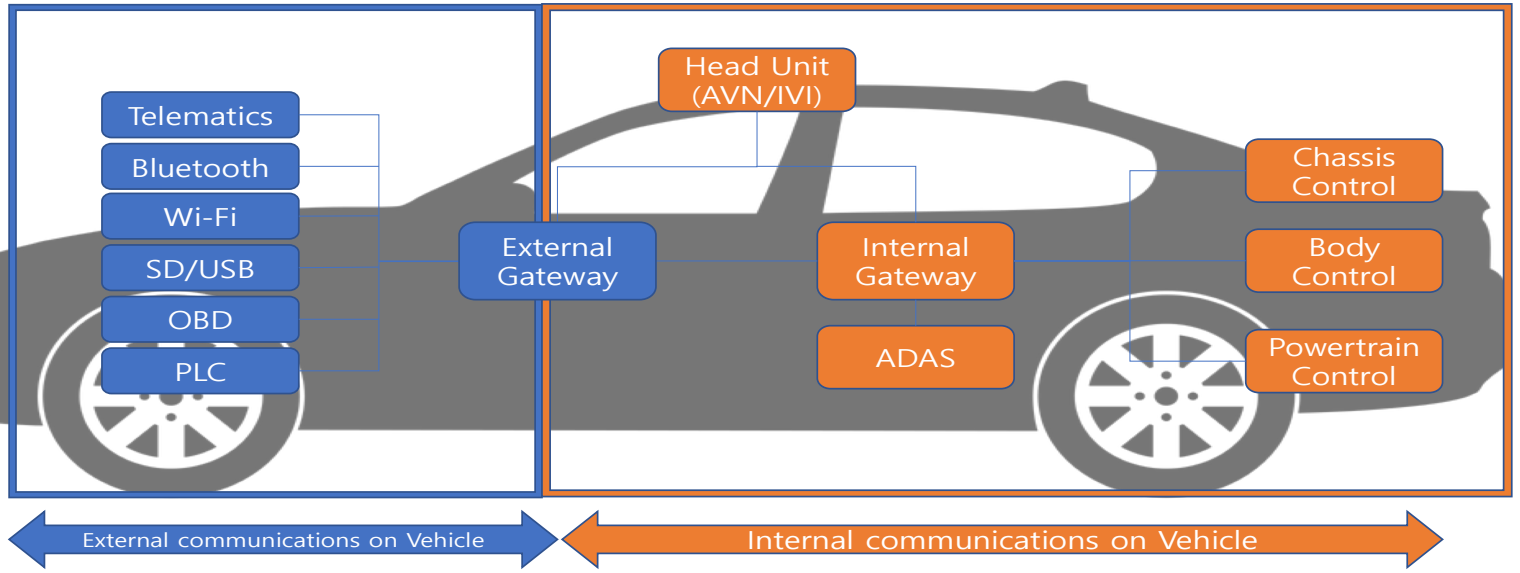


Draft Rec. X.itssec-4

Title: Methodologies for intrusion detection system on in-vehicle systems (under development)

Scope: This new Recommendation aims to provide the Methodologies for intrusion detection system on in-vehicle systems. This Recommendation will include detection models and pattern rules to recognize for the impact and likelihood of threats on vehicle systems throughout the monitoring on internal communications in the vehicle. This Recommendation will contain classifying and understanding threats on the internal communication network as CAN in vehicles which is working with specialized protocols.

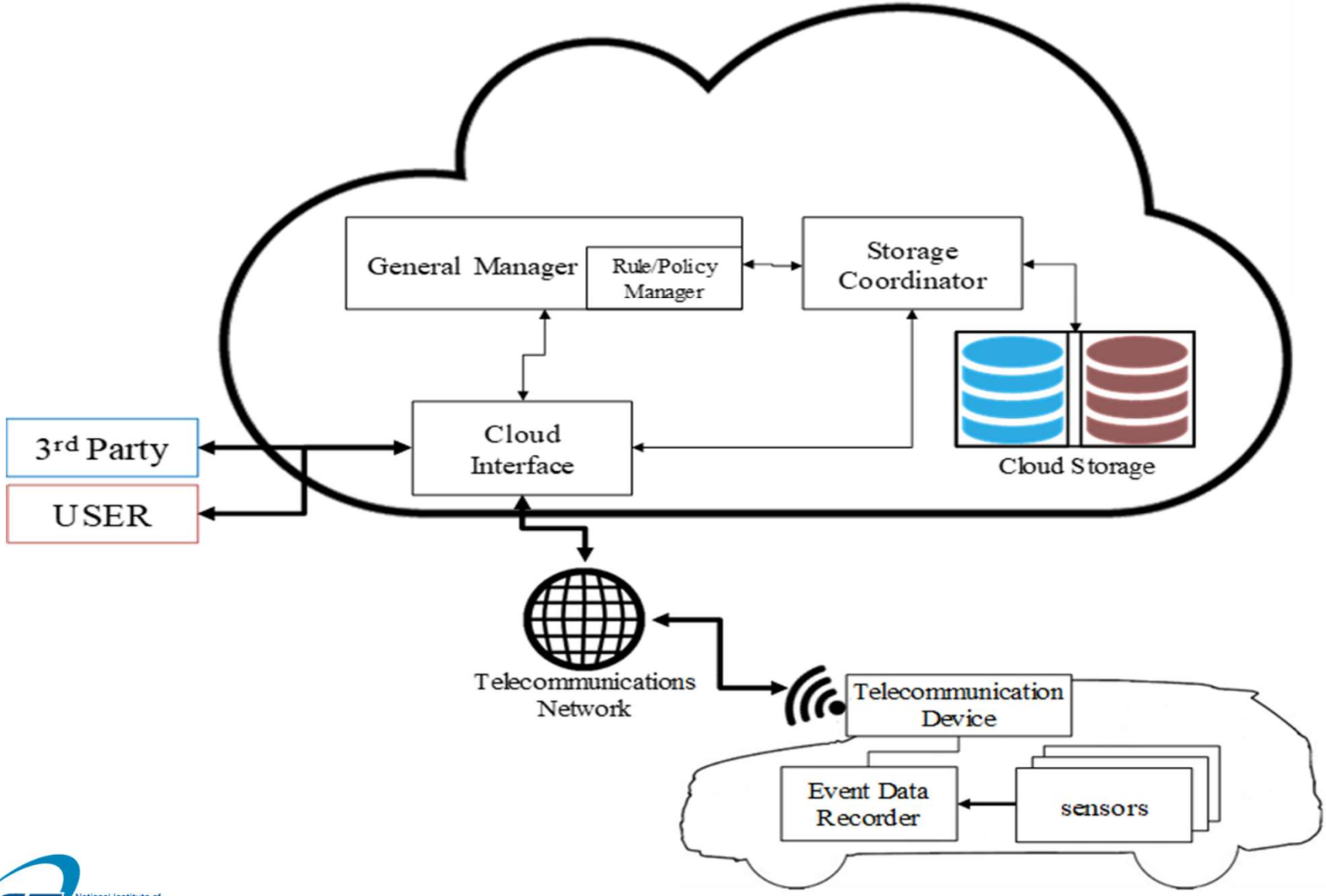
This Recommendation mainly focuses on the internal communications on the In-vehicle network as CAN which cannot be supported by general IDS, to ensure detecting threats which are impacting ECUs communications by using various efficient light-weight detection models such as Signature based model, Entropy based model, Self-Similarity based model, Hazard Survival based model, etc.



According to the current trend of connectivity among the vehicles, the event data recorders on automotive will be implemented to increase its overall safety. However, it has various vulnerabilities in the process of collecting, transferring, storing, managing and using the event data according to its distinctive characteristic of the automotive environment. Therefore, it is necessary to study these vulnerable points, security requirements and use cases for cloud-based event data recorders in automotive environments.

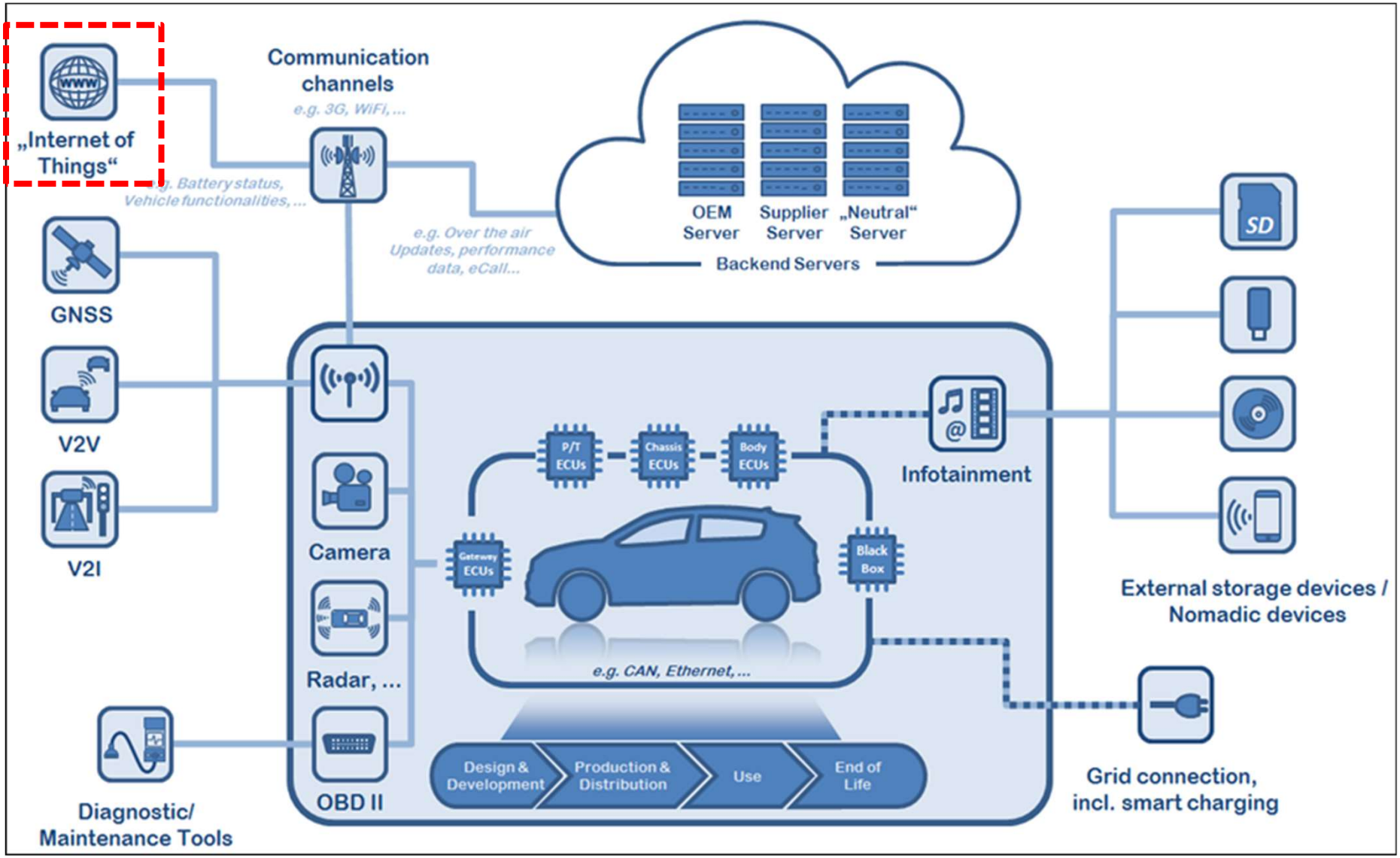
The purpose of this draft Recommendation is to standardize security guideline for cloud-based event data recorders in an automotive environment. This draft Recommendation provides threats, vulnerability, security requirements and use cases for cloud-based event data recorder in an automotive environment.

Concept: Concept of Cloud-Based EDR



IoT used in “Vehicle”

Reference Model discussed in WP29



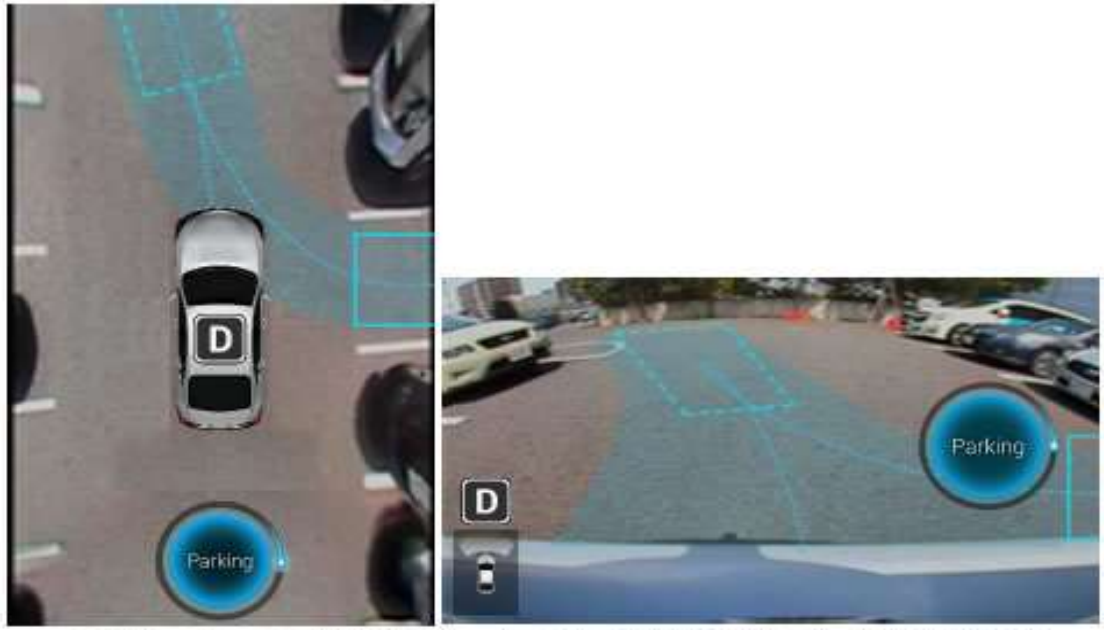
“Smiling Road” provides guidance for safe driving

“Smiling Road” provided by Sompo Japan Nipponkoa is a service that manages the safe driving of drivers by means of a drive recorder equipped with communication functions. A service that sends feedback such as safe driving diagnosis to the driver or company based on data such as mileage, speed, and number of sudden braking.

http://www.sjnk.jp/hinsurance/smilingroad/pc/

Remote Parking system (under development)

“Remote parking” is a system that enables “remote parking”. The car can be parked easily with a smartphone in the unattended state, according to the parking style such as tandem / parallel. Automatic parking is also possible, and safety confirmation at that time can also be done on the screen. It also has a function to automatically stop the vehicle because it can detect pedestrians and obstacles. Currently in the development stage.
http://www.ntt.com/business/services/iot/iot/iot.html



アプリケーションの駐車プレビュー画面(左:縦(俯瞰視点)、右:横(運転席視点)

出庫時の車両位置選択画面

IoT Threat

IoT Applied Domains in Japan

Tracking

Monitoring
Analysis

Optimization

New
Services

1. Automobile
2. Objects
3. Human
4. Livestock
5. Agri-Field
6. Factory
6. Home/Building
8. Shops
9. Public Facility
10. Energy Plant
11. Transport Condition
12. Truck Operation
13. Human Health
14. Livestock
15. Physical Security
16. Disaster
16. Nature Environment
18. Energy Consumption
19. Factory Production
20. Supply-Chain
21. Delivery Route
22. Sharing service
23. Wearable Device
24. Smart Product
25. Connected Car
26. Smart/Telematics Insurance
26. Smart retails
28. IoT Payment Device

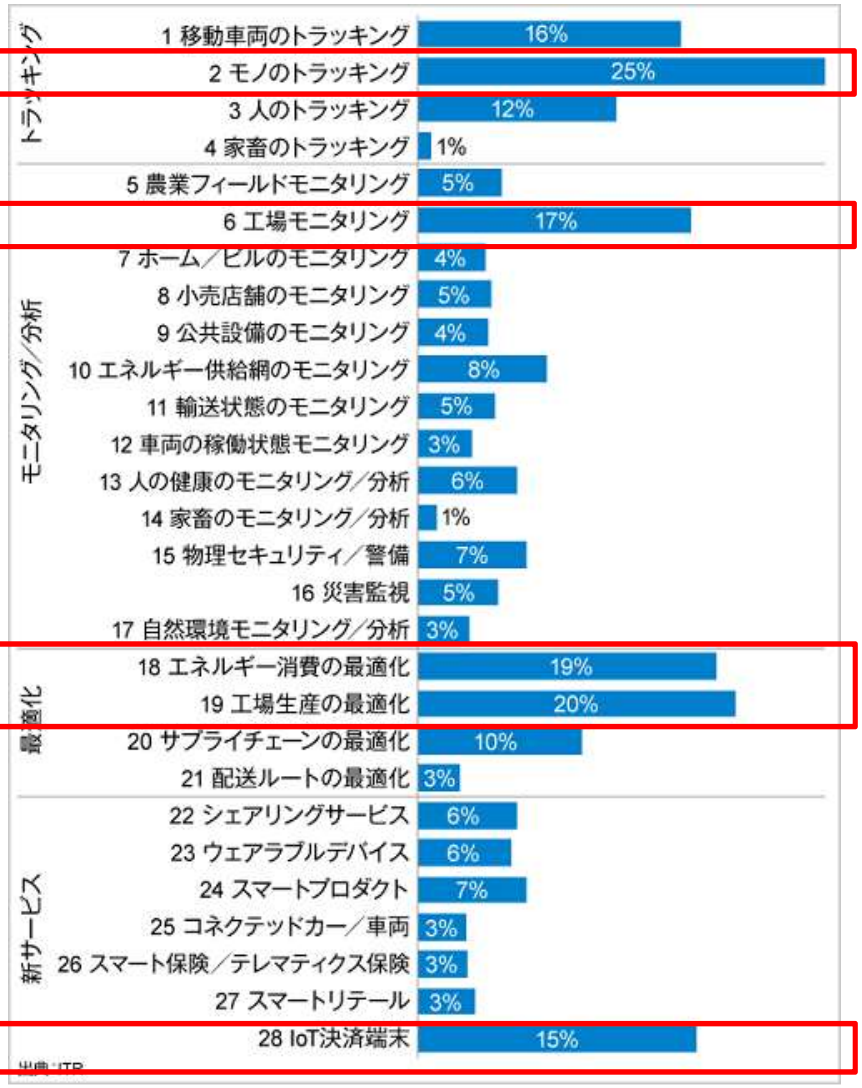


図. IoT導入企業における分野ごとの実施率(全業界平均)

ITR/2016
https://www.itr.co.jp/company/press/161012PR.html

CEATEC 2018 cnet japan記事より

https://japan.cnet.com/article/35126302/

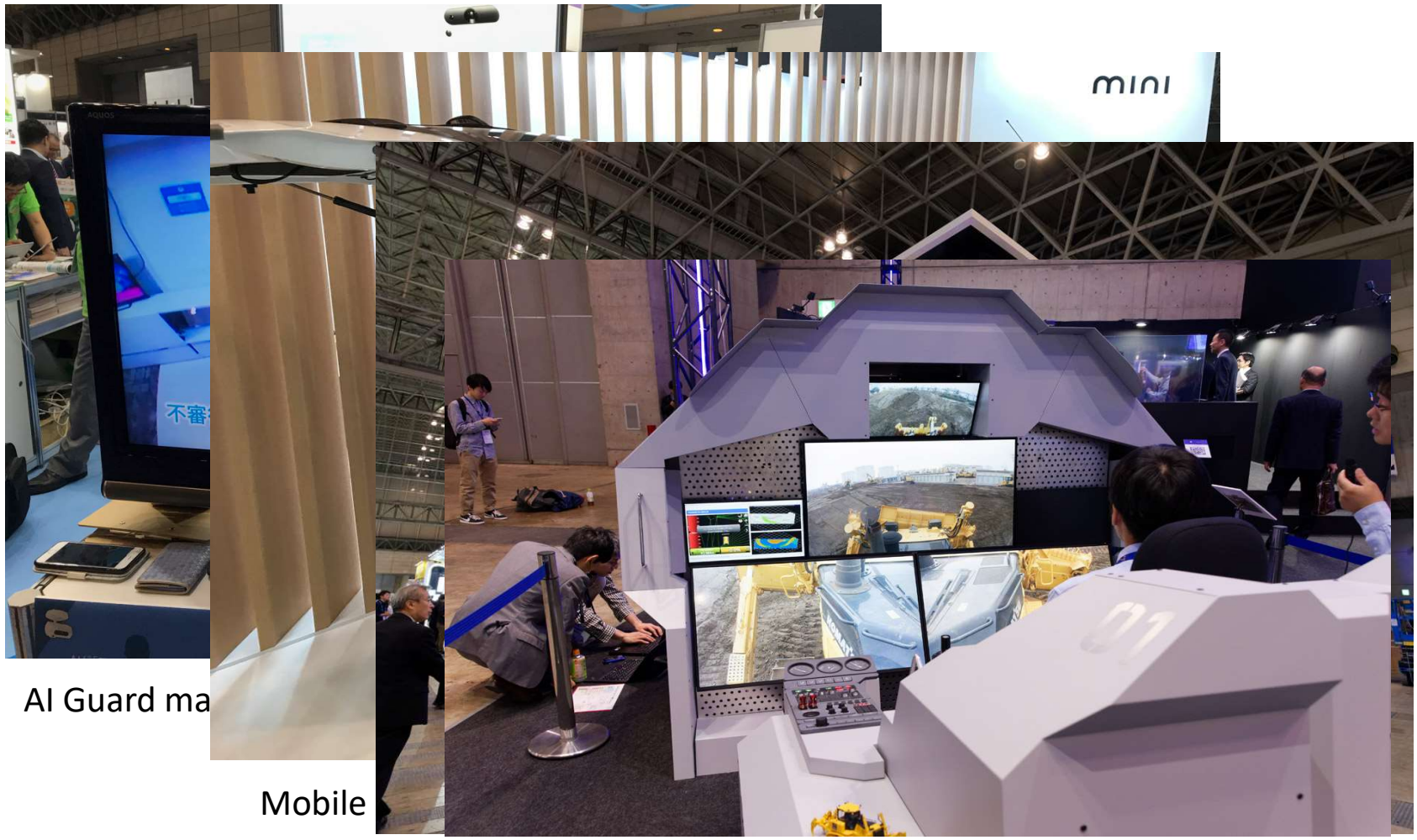
Walk-thro
at convenience store

Robo-

Bathroom Monitor (Vital-Heart rate, Water Temp, Time in Bath)

CEATEC 2018 Internet Watchより

https://internet.watch.impress.co.jp/docs/event/1148031.html



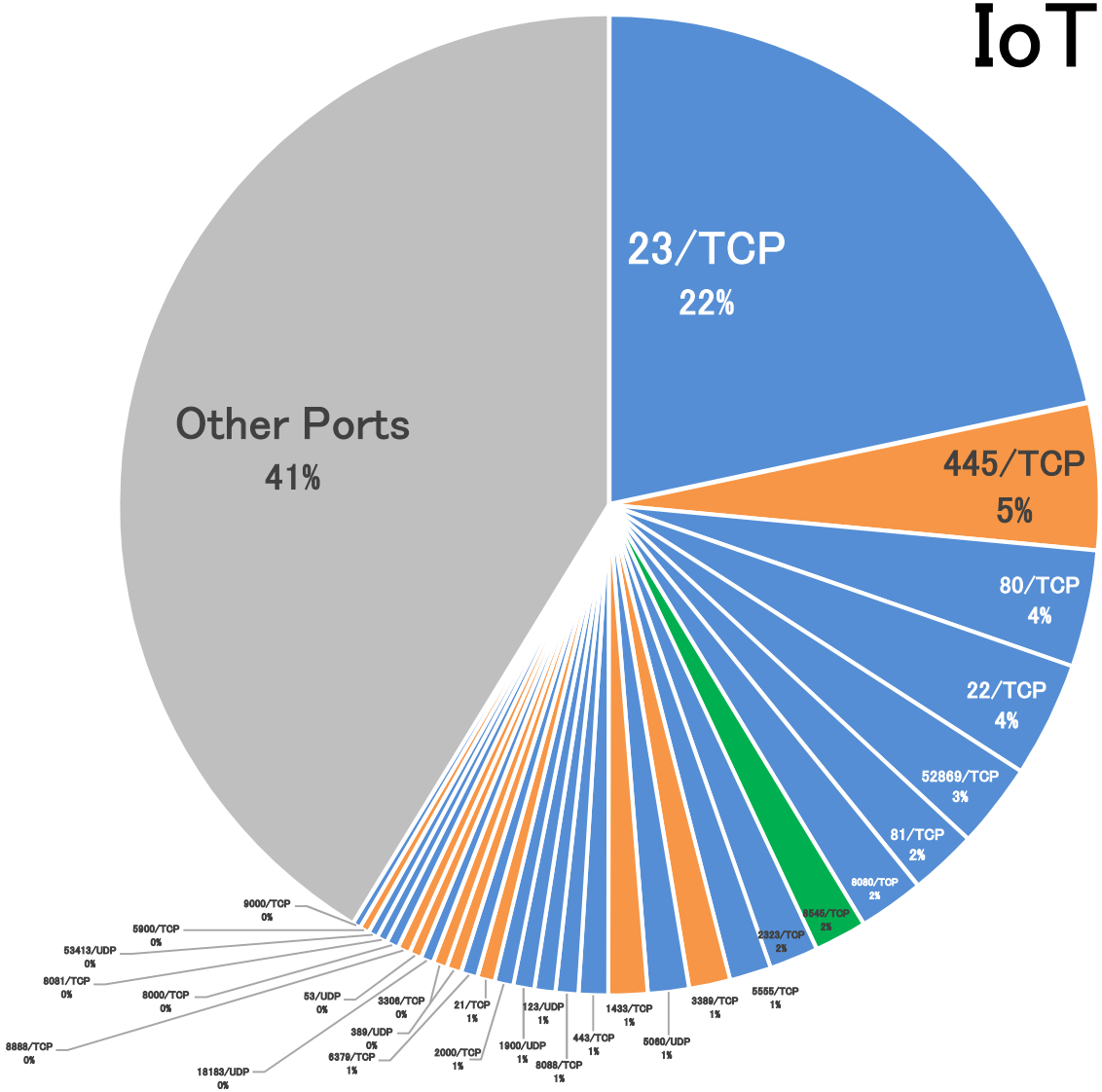
AI Guard ma

Mobile

Remote Construction

Distribution of Port Numbers (2018)

IoT = 46.6%



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 ion devices

Home Router Botnet Leveraged in
Large DDoS Attack

Is
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
o combat the risks. Plus: 1% of use
e risk; Target pays up; Apple devic
y secured in the enterprise.

RISK ASSESSMENT / SECURITY & HACKTIVISM

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

Categories of Inferred Infected devices(2016.9)

- Surveillance camera
  - IP camera
  - DVR
- Network devices
  - Router, Gateway
  - Modem, bridges
  - WI[illegible] routers
  - N[illegible] ob[illegible] or[illegible]ge
  - Security appliances
- Telephone
  - VoIP Gateways
  - IP Phone
  - GS[illegible] Routers
  - A[illegible] h[illegible] adapter
- 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
- [illegible] automa[illegible]n [illegible]W
- [illegible]la Energy [illegible]nt[illegible]l Syst[illegible]
  - Energy demand monitoring system
- Broadcasting
  - Media broadcasting
  - Digital voice recorder
  - Video co[illegible]ec
  - Set-top-box
- Etc
  - Heat pump
  - Fire alert system
  - Medical device(MRI)
  - Fingerprint scanner






600,000+IPs

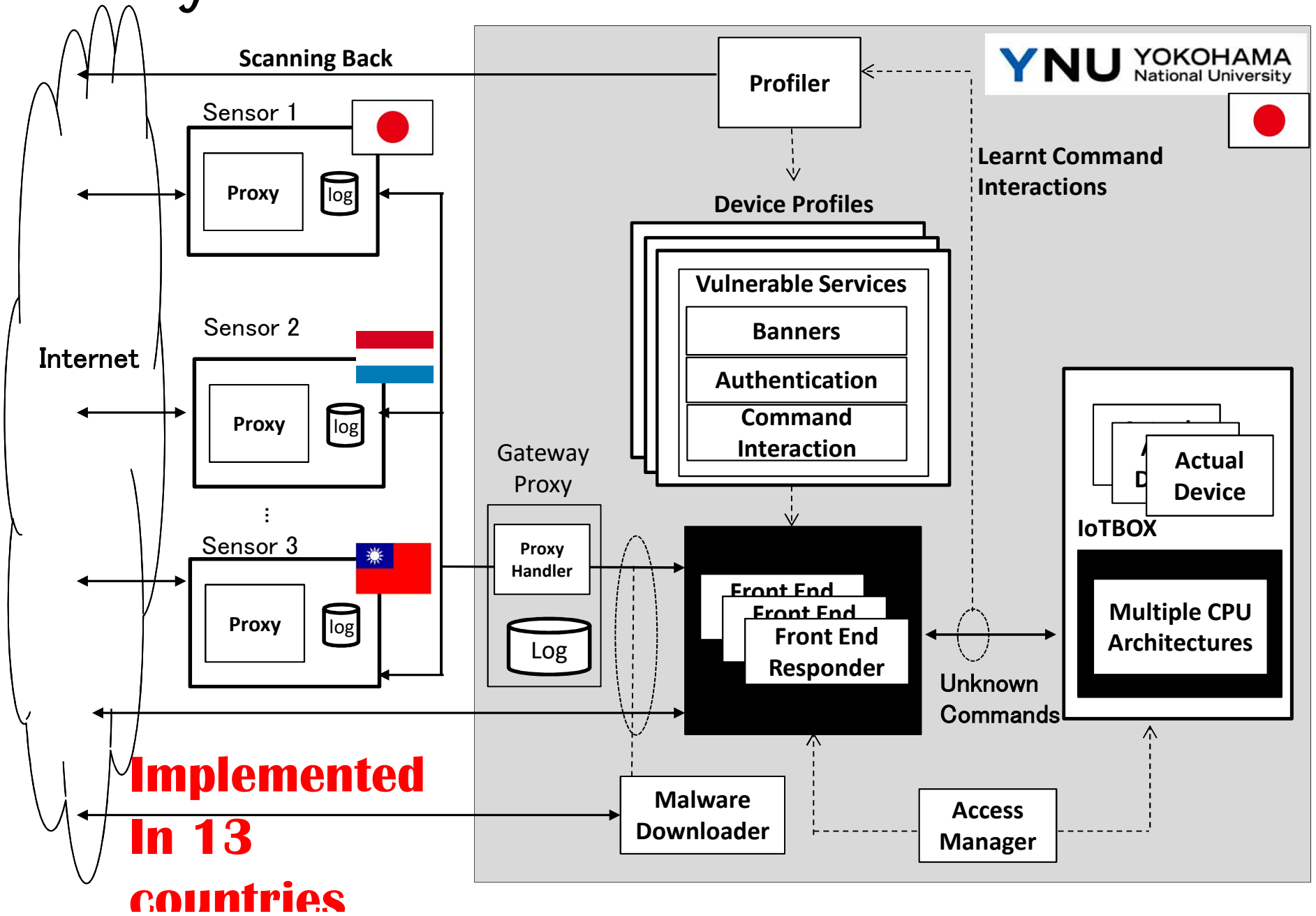
500+ device types †

†inferred by telnet and web responses

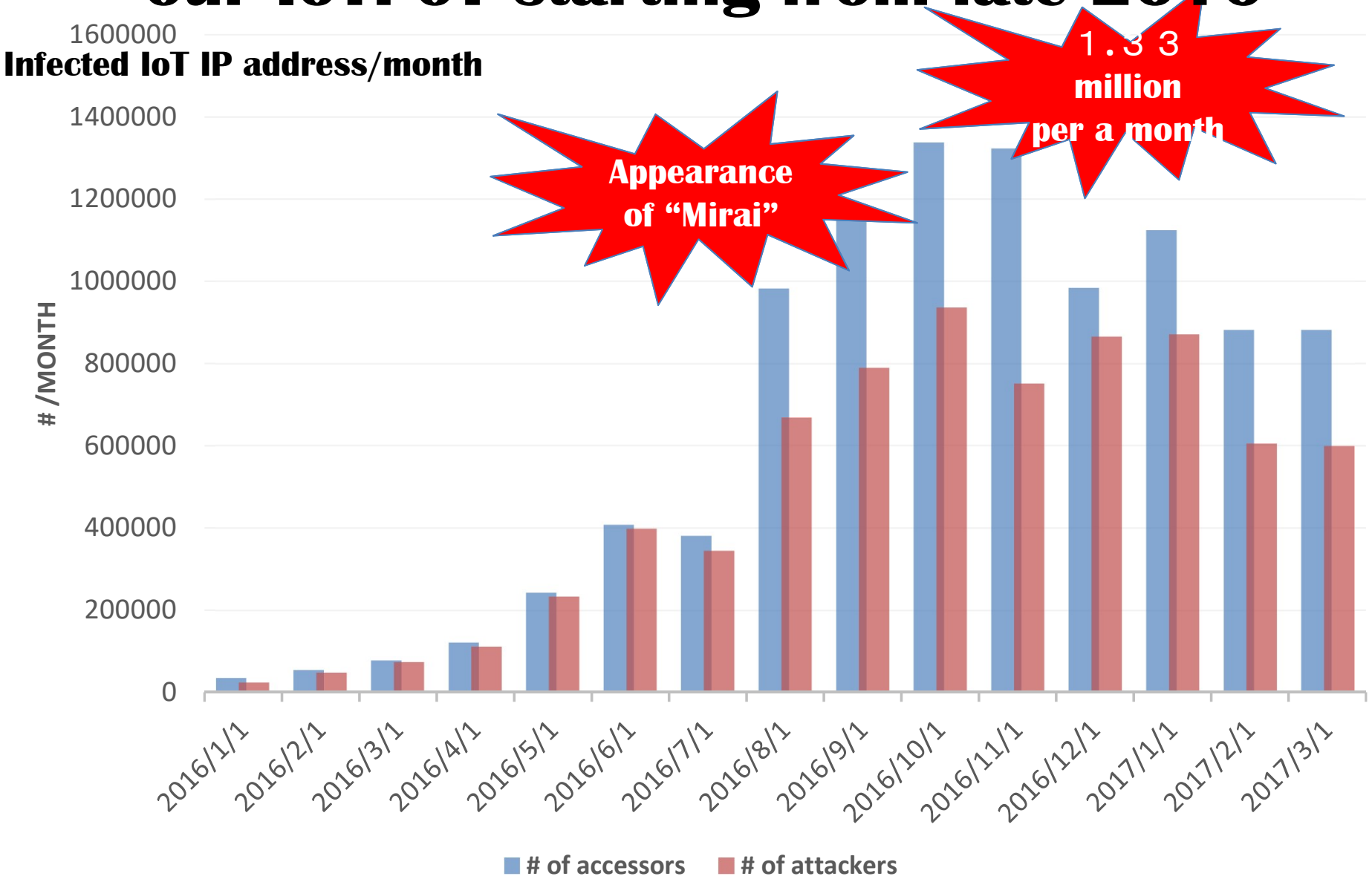
Why IoT devices?

- 24/6 online
- No AV
- Weak/Default login passwords
- with global IP address and open to Internet

System Architecture of IoTPoT

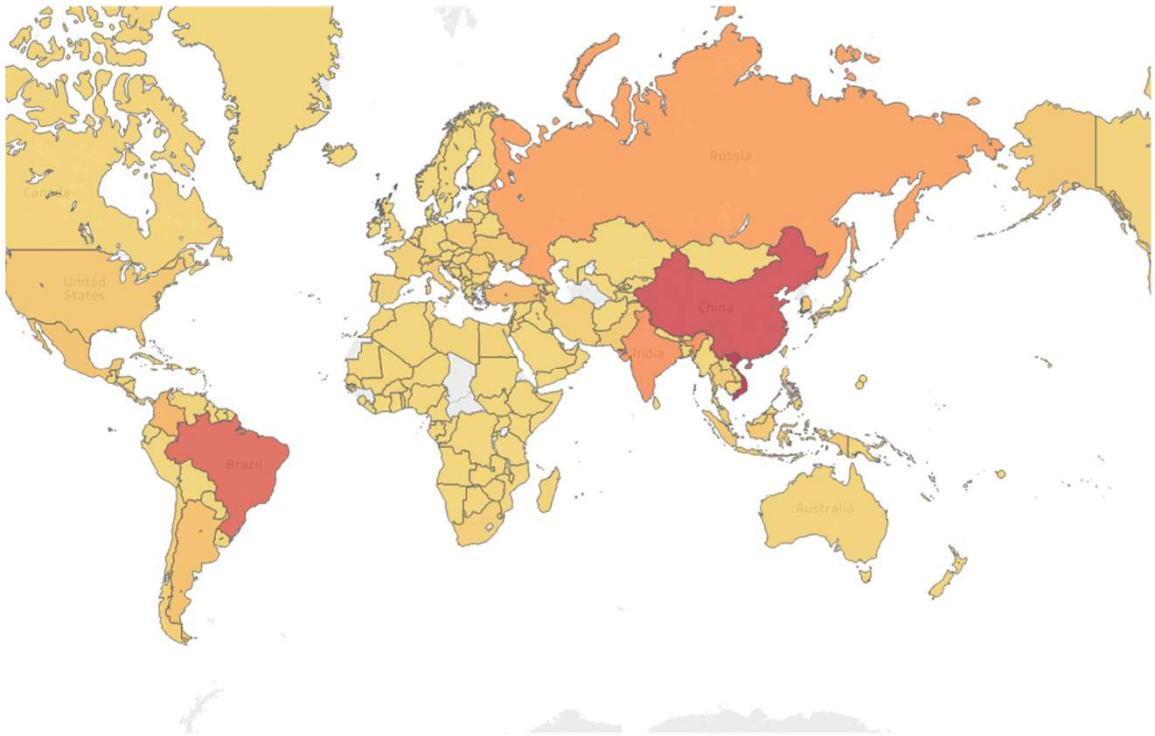


Rapid Increase of Access/Attack to our IoTPoT starting from late 2016



Worldwide spread infection

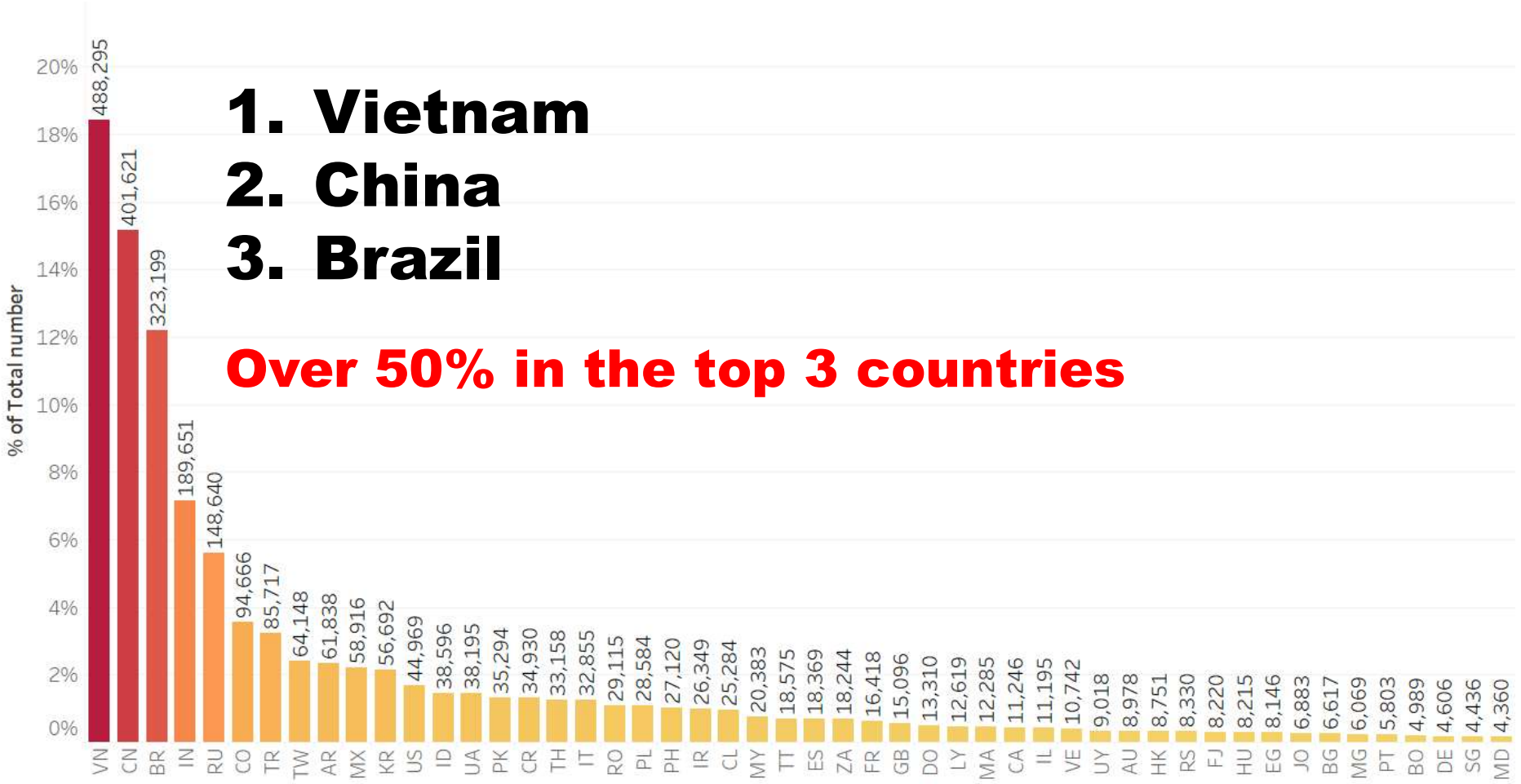
- **Observed from 218 countries and/or regions**
- **Especially from Asian Countries**



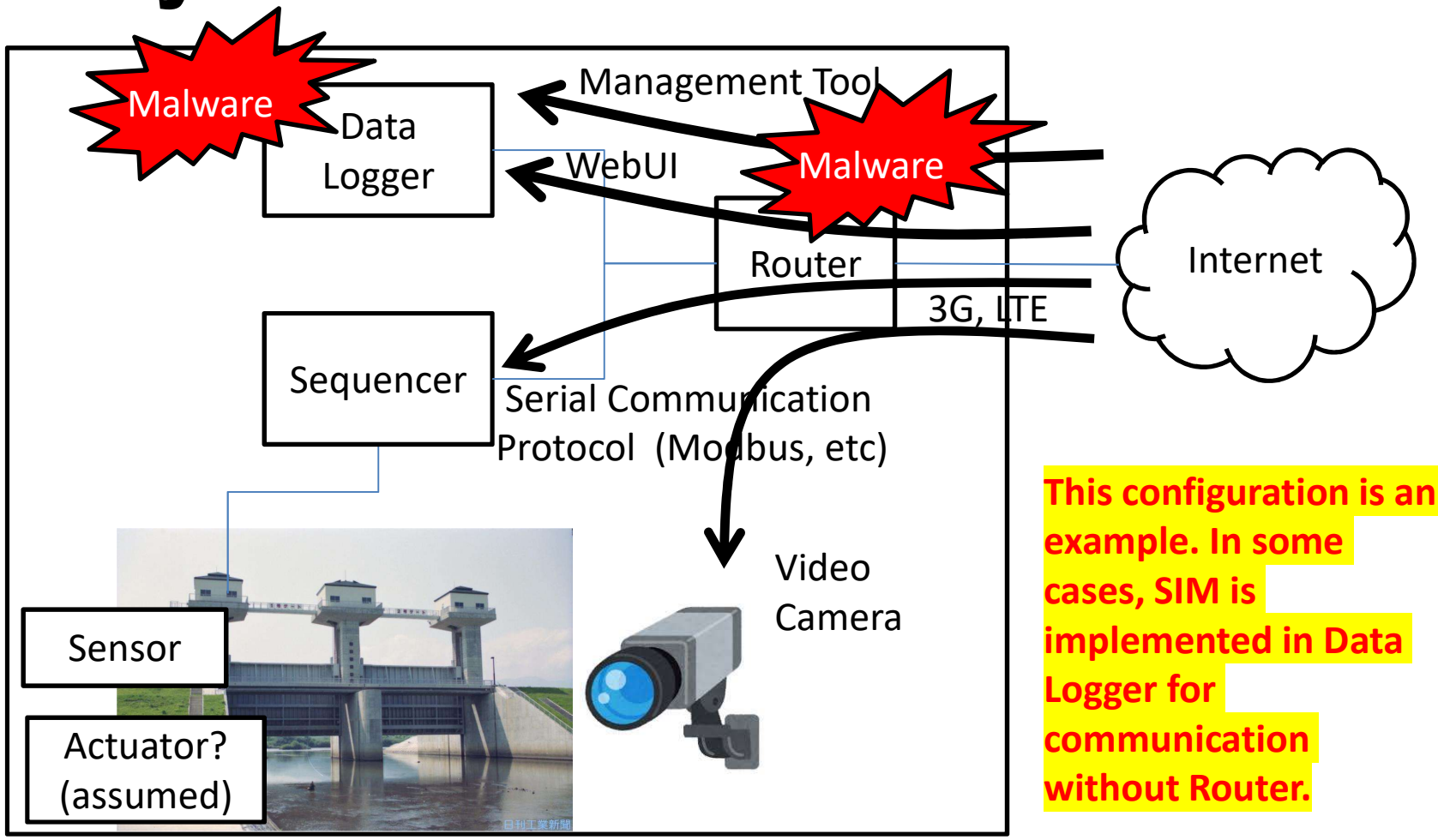
Number of Infected IoT devices by country (IP addresses)

1. Vietnam
2. China
3. Brazil

Over 50% in the top 3 countries



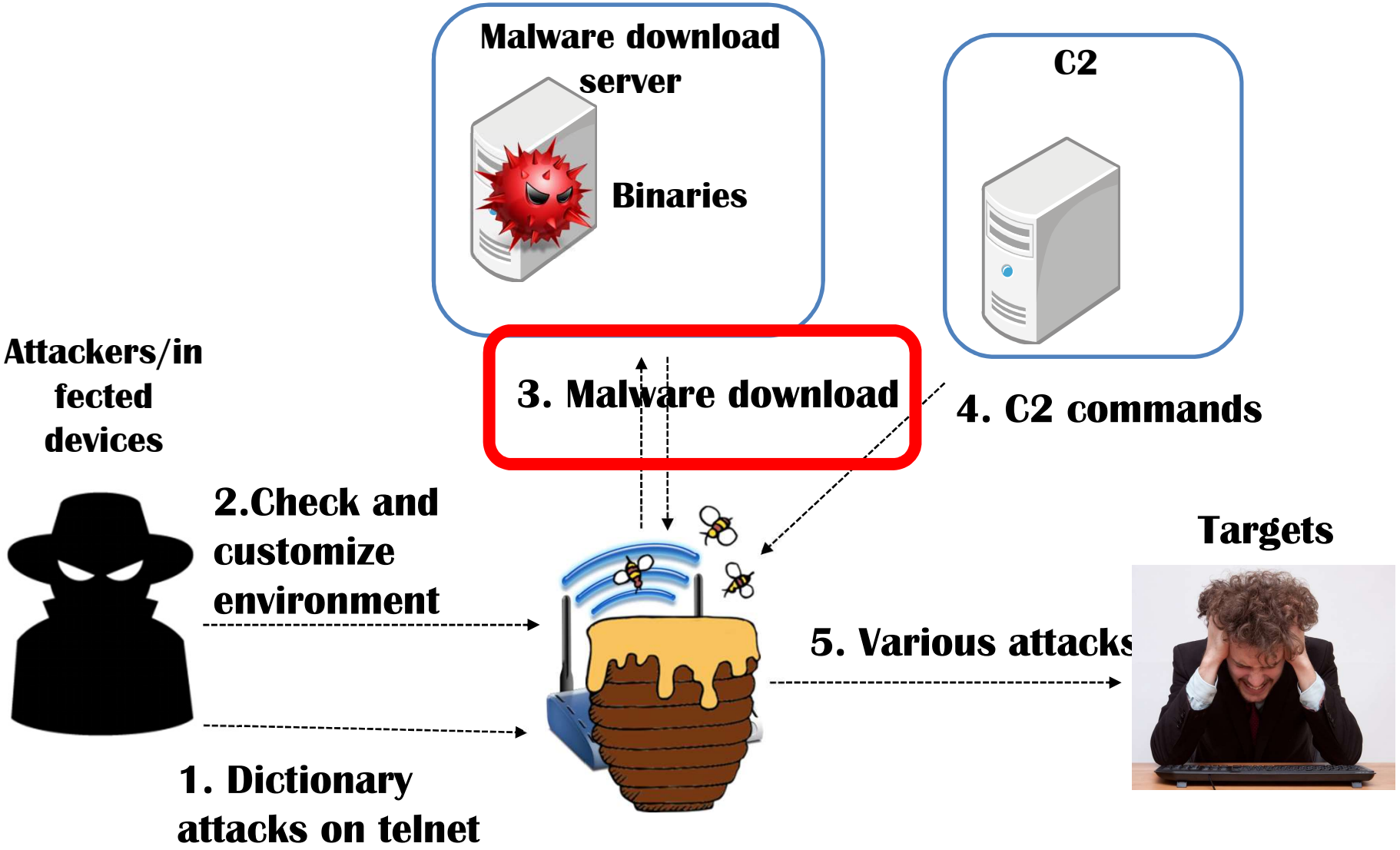
Typical Network/System Configuration of Important IoT Devices and Supposed Security Problems



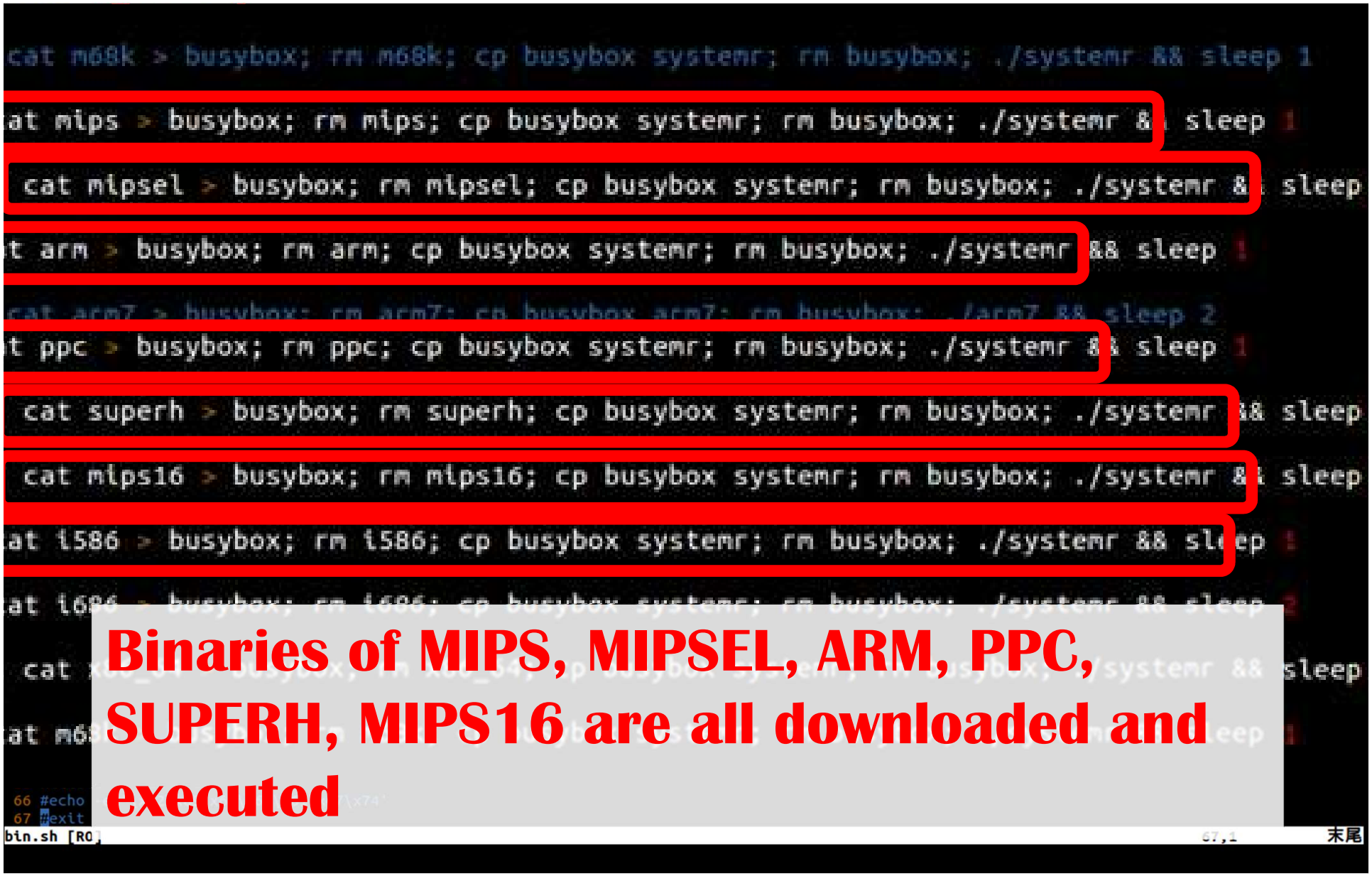
This configuration is an example. In some cases, SIM is implemented in Data Logger for communication without Router.

* The above configuration is inferred from network observation from global scans and being confirmed by the hearing survey.

Telnet-based malware infection



e.g. Malware binary downloads



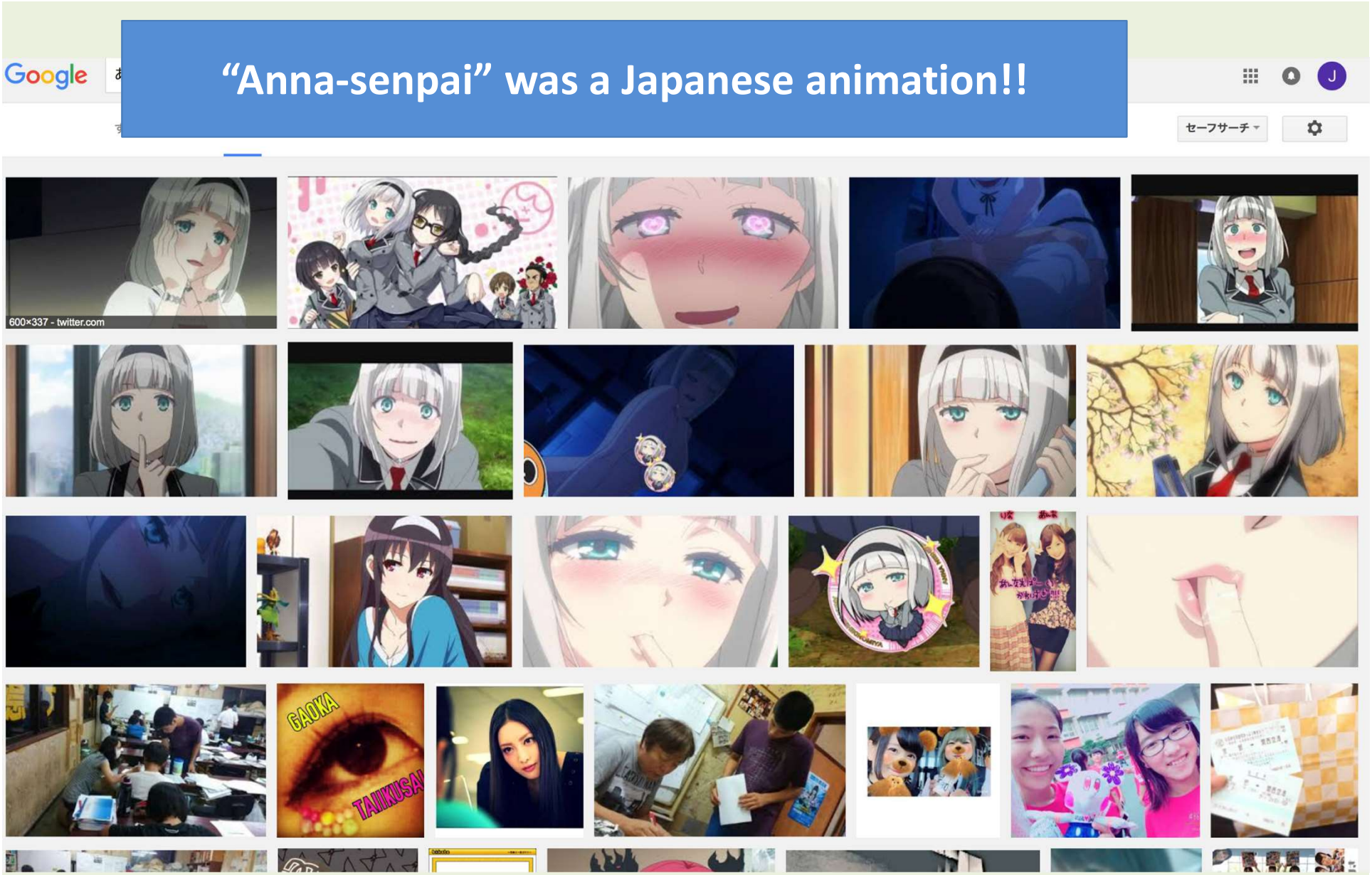
Binaries of MIPS, MIPSEL, ARM, PPC, SUPERH, MIPS16 are all downloaded and executed

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**

“Anna-senpai” was a Japanese animation!!



The Attacker may be very OTAKU (Comic fanatic).

Further information on “Mirai”

DDoS Attacks

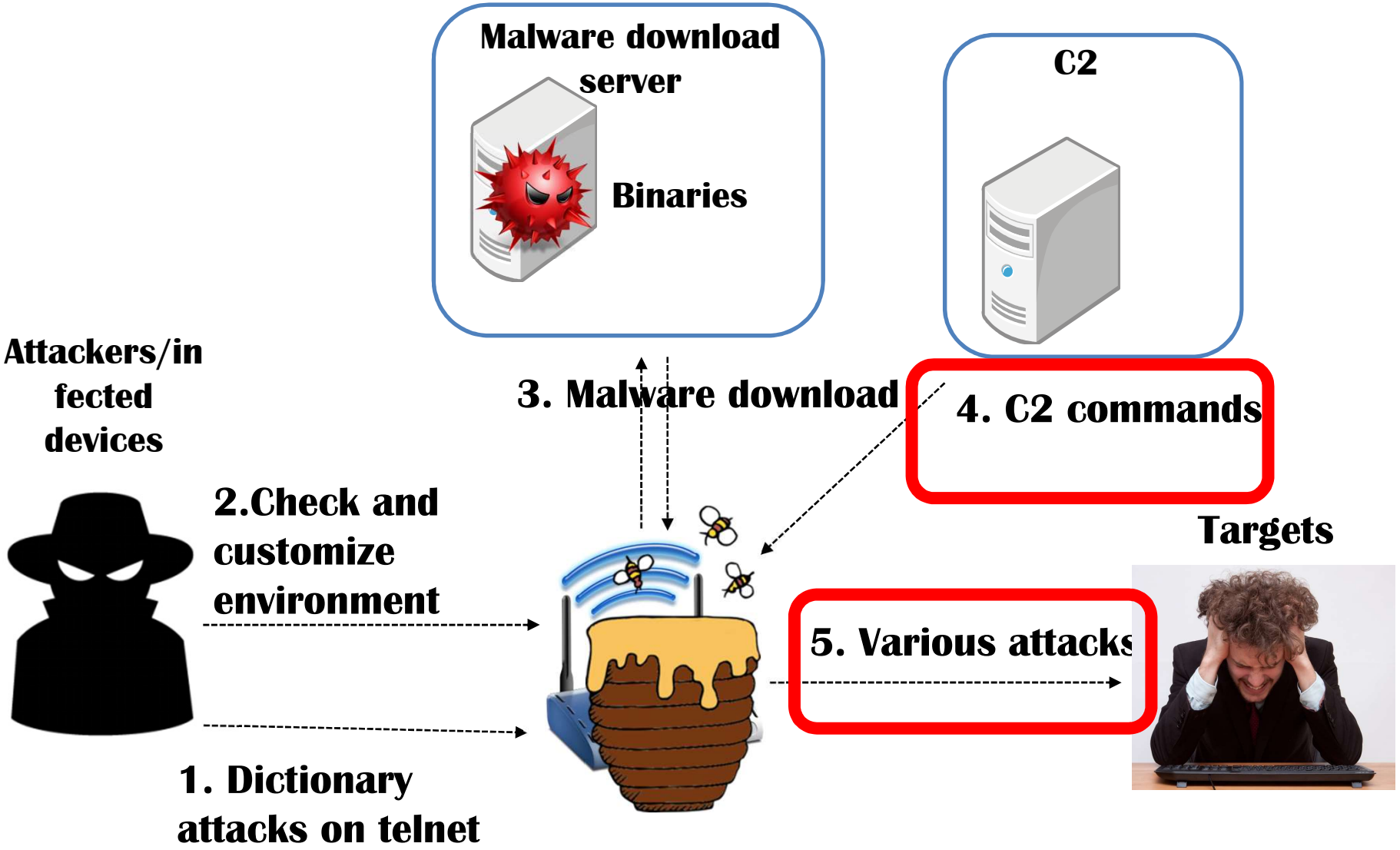
- Krebs on Security（16/9/20）
  - -Akamai Service

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

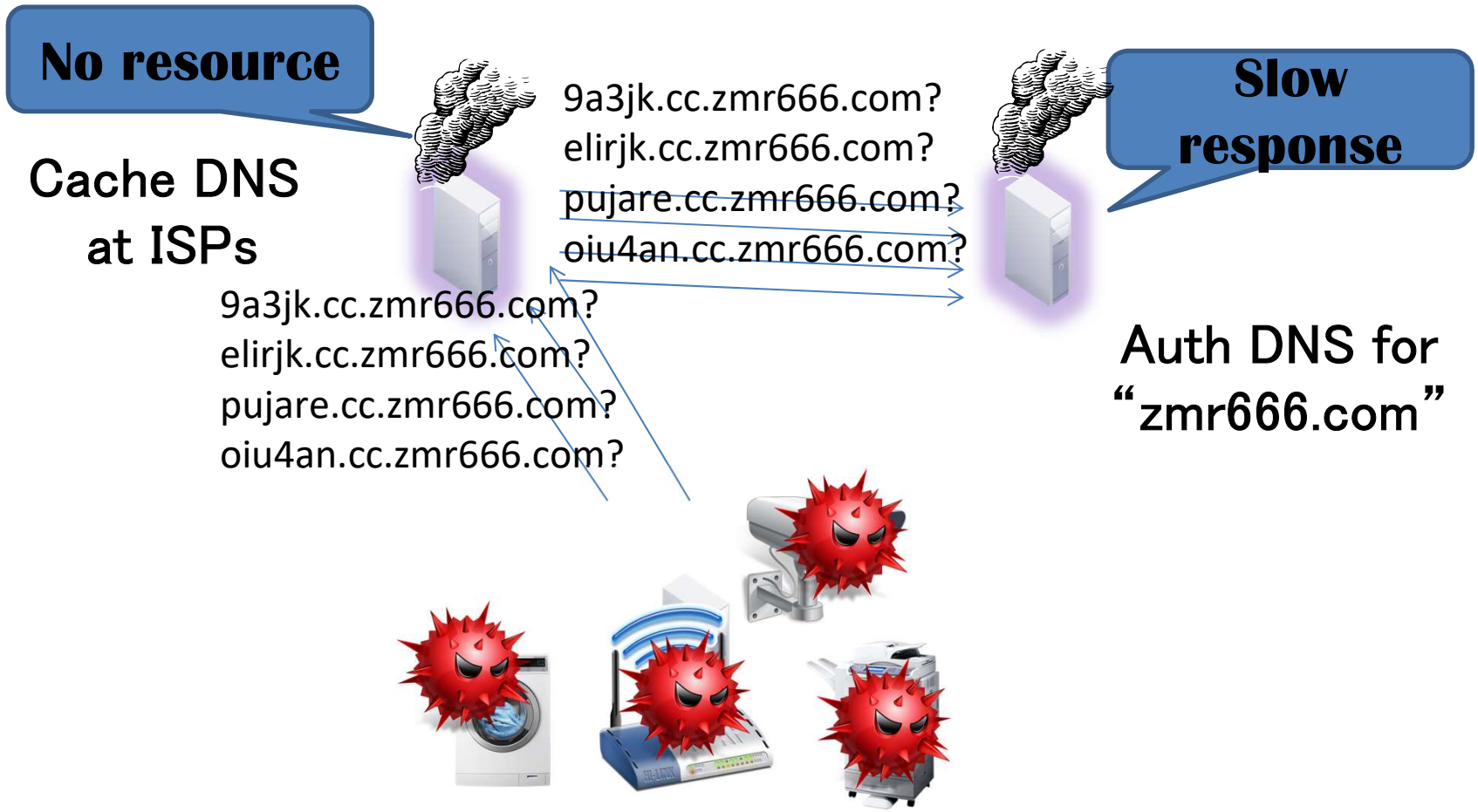
- Types of Infected:
  - -Printer
  - -Camera
  - -Router
  - -DVR and etc.

- Architecture used:
  - -ARM
  - -ARM6
  - -MIPS
  - -PowerPC
  - -SH4
  - -SPARC
  - -X86

Telnet-based malware infection



Dinial of Service (DoS)

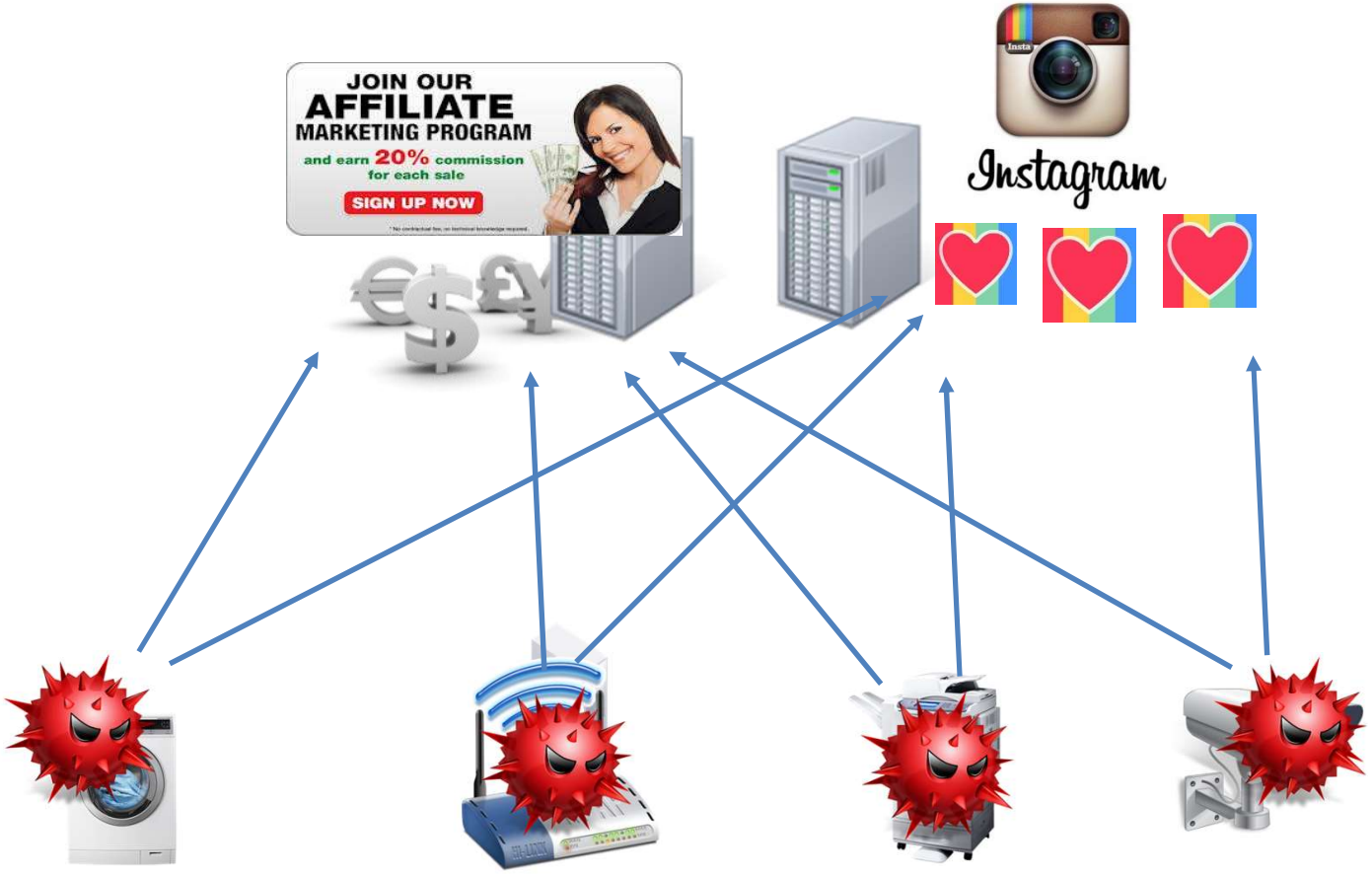


Propagation

Infected devices

Click fraud

Infected devices imitates user clicks to advertising web sites.

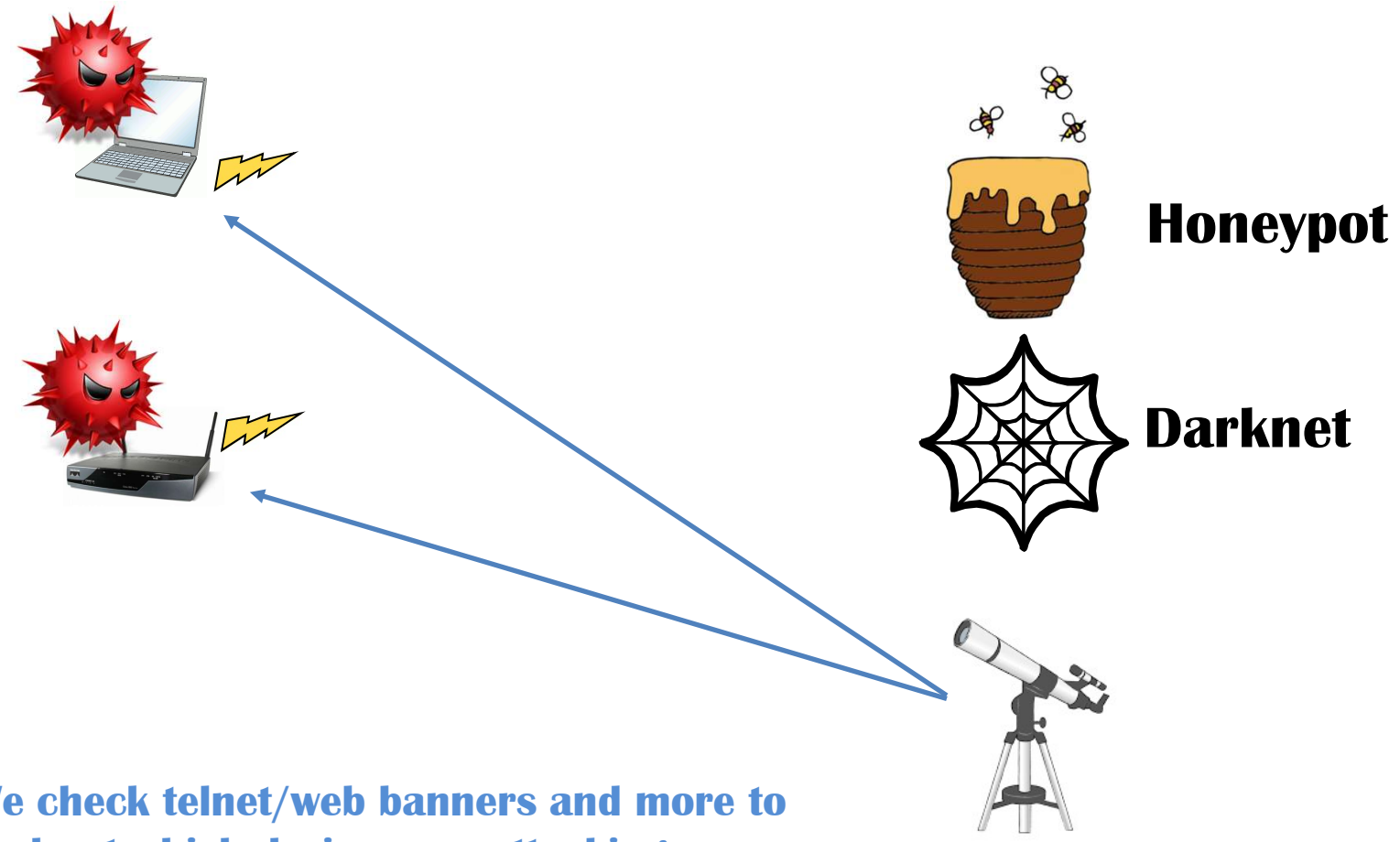


Infected devices

Stealing credential from PPV (Pay Per TV)

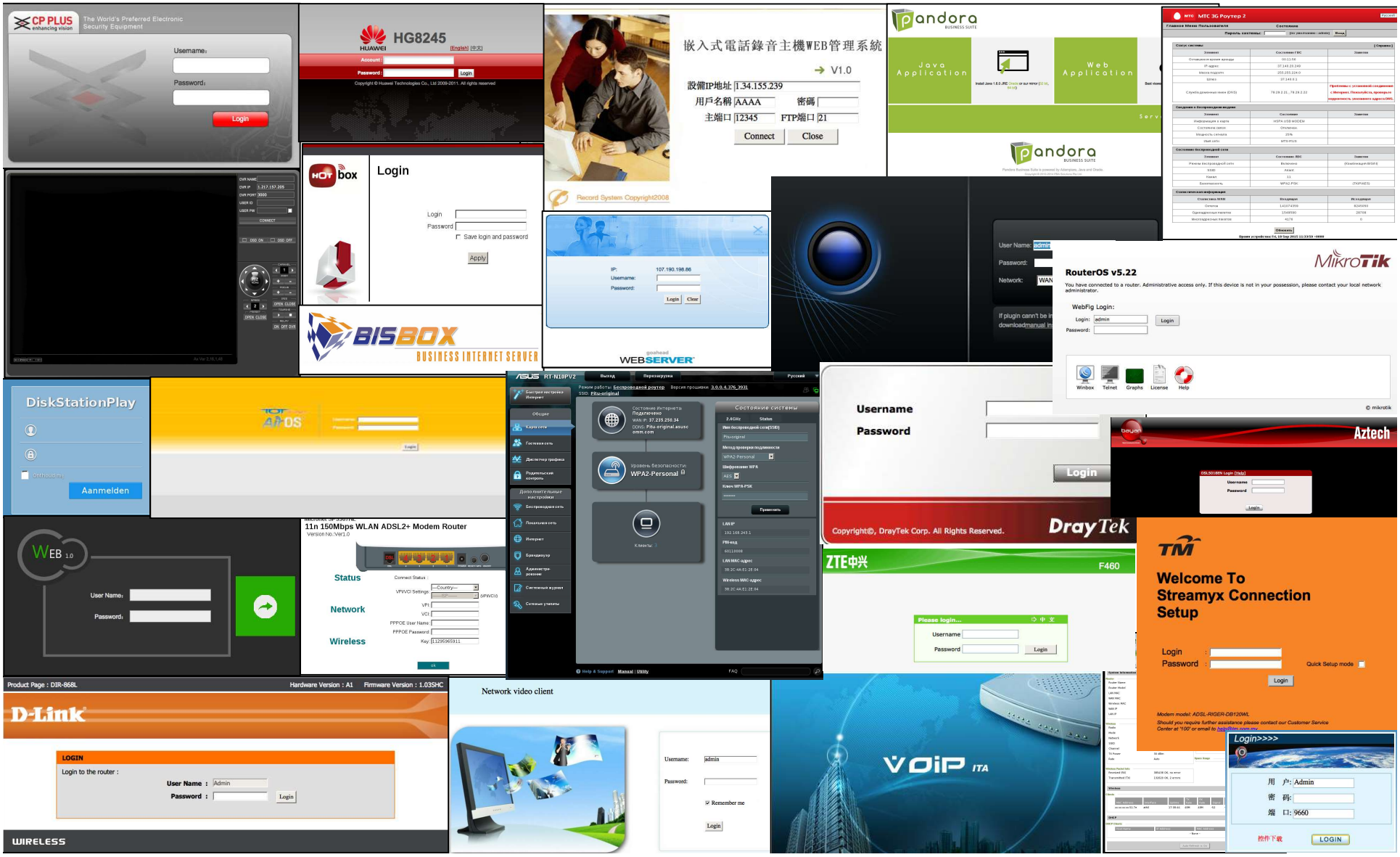
Particular set top boxes are being targeted (such as dreambox).

Inferring infected device

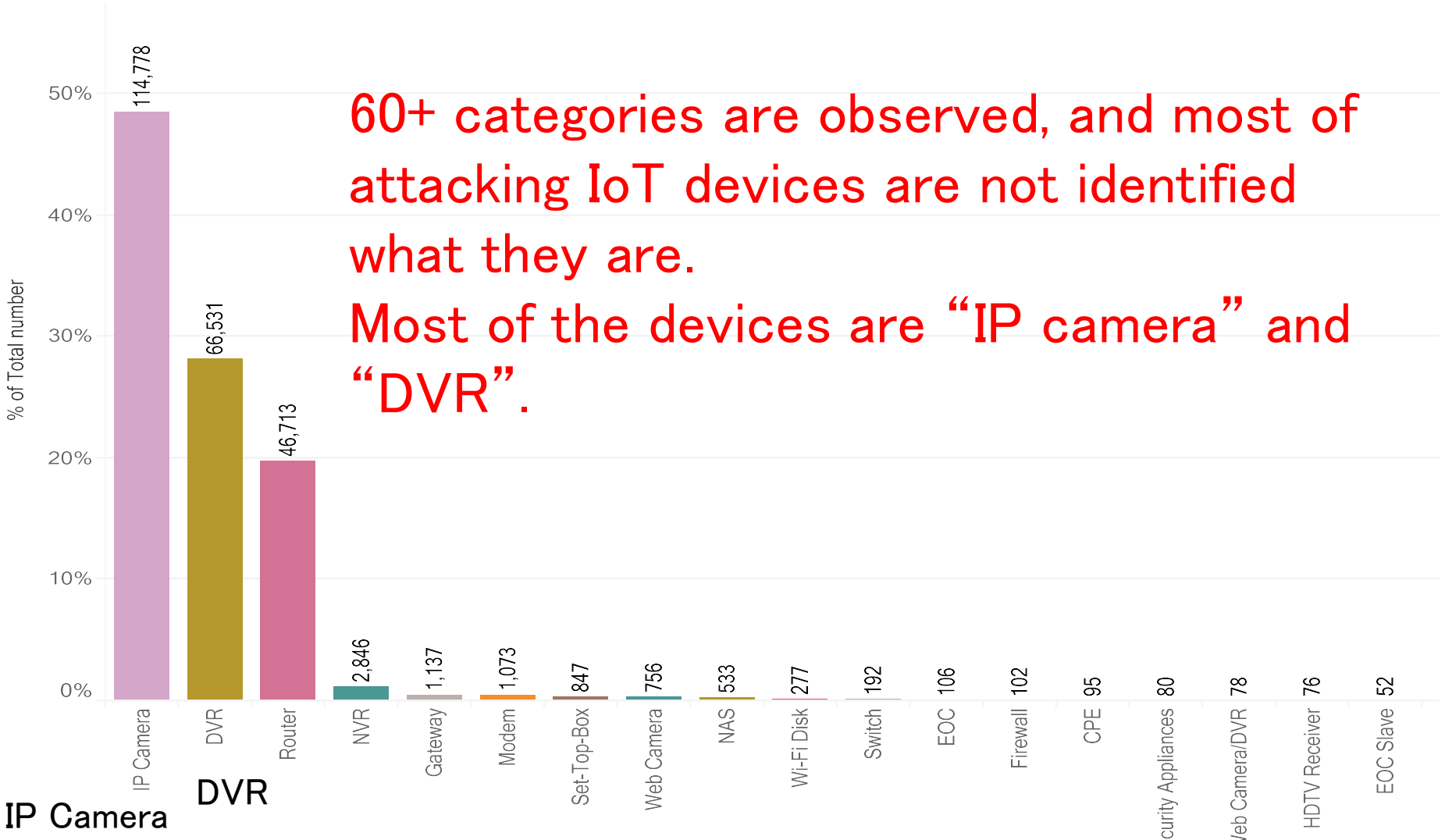


We check telnet/web banners and more to find out which devices are attacking us

Examples of web interfaces of infected devices



Device categories



60+ categories are observed, and most of attacking IoT devices are not identified what they are.

Most of the devices are “IP camera” and “DVR”.

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





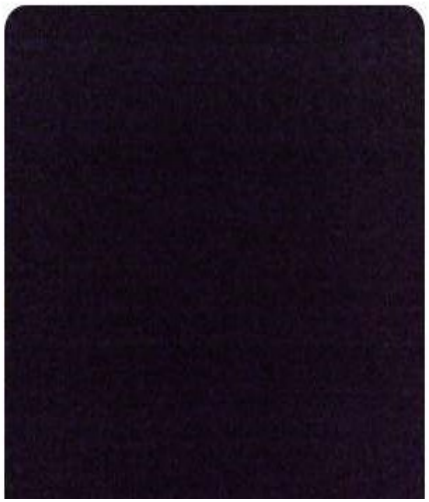

Peep Camera Site: Insecam

https://www.insecam.org/

United States(5590)
Japan(2085)
Italy(1087)
France(996)
Germany(622)
Korea, Republic Of(621)
Turkey(599)
United Kingdom(523)
Netherlands(494)
Czech Republic(427)
Taiwan, Province Of (393)
Russian Federation(378)
Austria(348)
Spain(267)
Israel(265)
Switzerland(258)
Canada(250)
Sweden(238)
Australia(231)
-(201)
Norway(195)
Poland(180)
India(175)
Romania(146)

Japan is No 2 (2018/10/2)

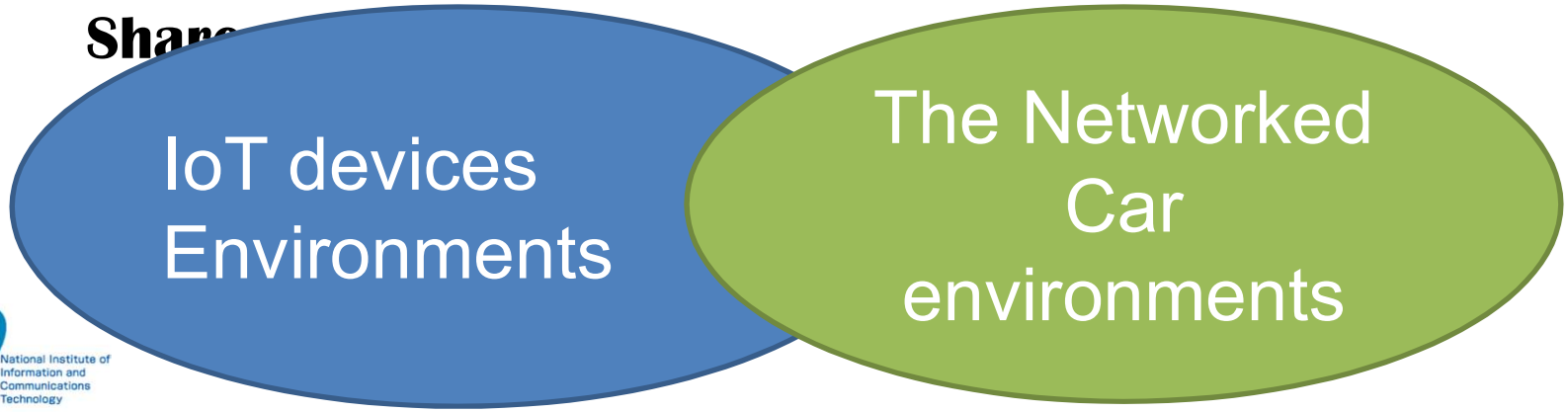
6 7 8 9 10 ... 348 »



Conclusion

<Important Security Issues>

1. Monitoring and Analyzing Vehicle threats and vulnerabilities
2. Detection of Malwares injection
3. Secure Software/Firmware updates
4. Ensuring Data Confidentiality and Privacy
   – Use of “Lightweight Cryptography”
5. Remote Maintenance and Remote Kill Switch
6. Provision of Authentication and Access Control
7. Improvement of Incident handling and Information Shar



The way for move forward with FG-VM

A) Prepare and specify “Security Requirements” to SG 17. SG 17 will produce a set of related Recommendations;

Or

B) Discuss and study “Security related deliverable” in FG-VM as an additional activity.

Note: this is not authorized by SG 17 at this point in time…

Thank you for listening