Security issues related to Vehicles and Secure OTA Software Updates

Masashi Eto
Research Manager,
Cybersecurity Human Resource Development Research Center,
NICT, Japan

National Institute of Information and Communications Technology

Outline

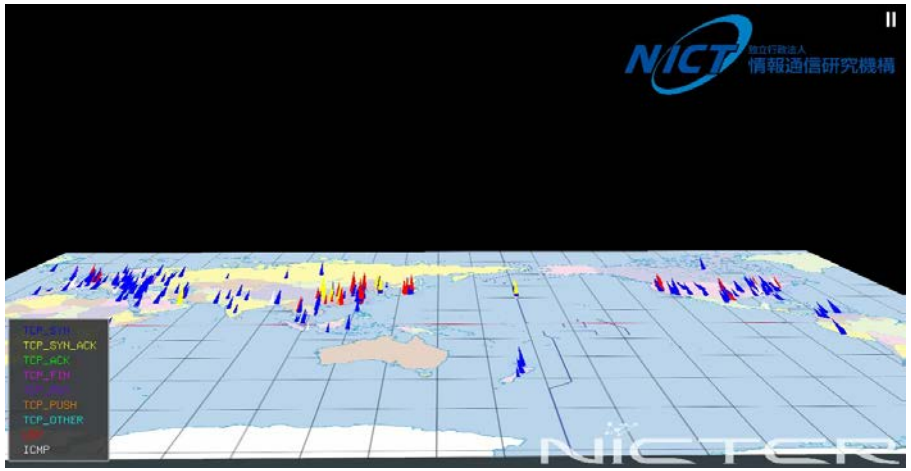
- ✓ Observing current IoT Attacks
  - Darknet basis attack observation
- ✓ Understanding Infected IoT devices
  - IoT Honeypot and Sandbox
- ✓ Secure OTA Updates for ITS/IoT software/firmware
  - As one of the countermeasures against threats in ITS/IoT environments -

Observing current IoT Attacks

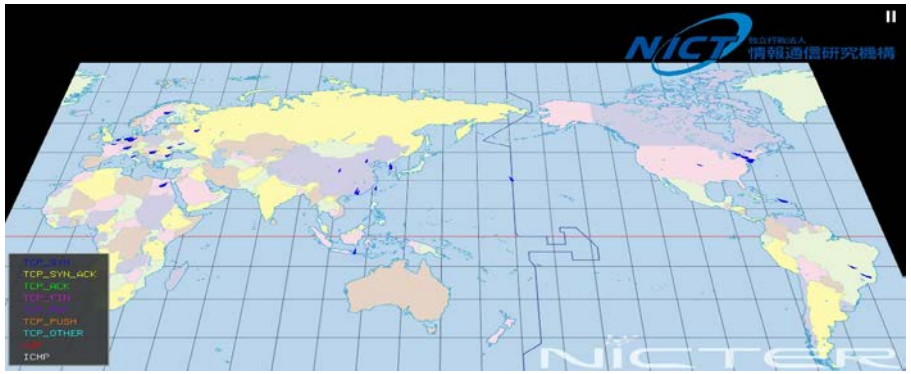
Scanning observation by darknet monitoring

- **Darknet:**
  - unused IP address range which is efficient for cyber-attack observation
- Capturing packets through darknet in real time basis.
- Color indicates the protocol types.

UDP
TCP SYN
TCP SYN/ACK
TCP Other
ICMP



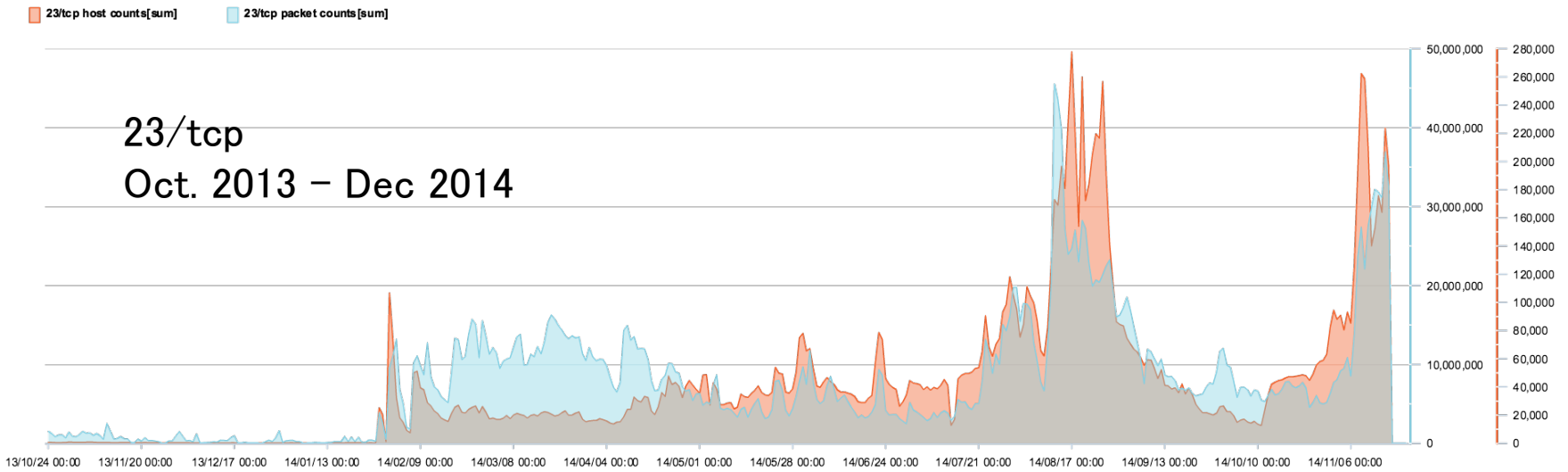
Atlas All view



Atlas only port23

National Institute of Information and Communications Technology

23/tcp Scan from Embedded Device



- **Infected Devices**
  - ✓Home Router
  - ✓Web Camera
  - ✓NAS: Network Attached Storage　　etc. etc...

National Institute of Information and Communications Technology

The attacking hosts are IoT devices

LED display control system

Solid Stage Recorder

Data Acquisition Server

150,000 attacking IPs

Wireless Router

TV Receiver

GSM Router

361 models

observed in 4 months

IP Phone

Parking Management System

VoIP Telephony System

Fire Alarm

Security Appliance

Internet Communication Module

Video Broadcaster

NICT National Institute of Information and Communications Technology

Why IoT devices?

- 24/7 online
- No AV
- Weak/Default login passwords
- with global IP address and open to Internet

Understanding Infected IoT devices

We would like to know..

Malware

- What kind of malware?
- How many different kinds?

Targets

- What IoT devices are targeted?

Monetization

- What the attackers do after compromising these devices?

We have developed the first honeypot for IoT

Challenges

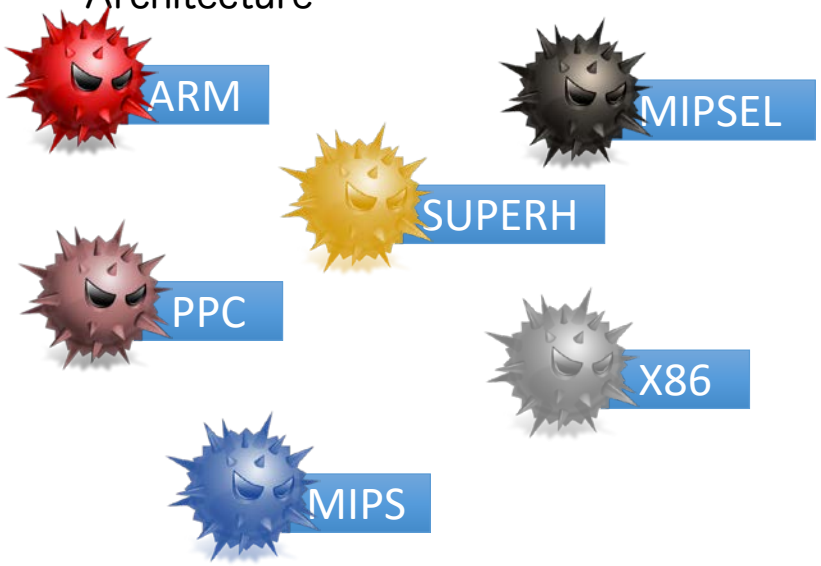
Honeypot

IoT devices listening on Telnet

- Emulating diverse IoT devices
- Handling to capture malware of different CPU architectures

Sandbox: IoTBOX

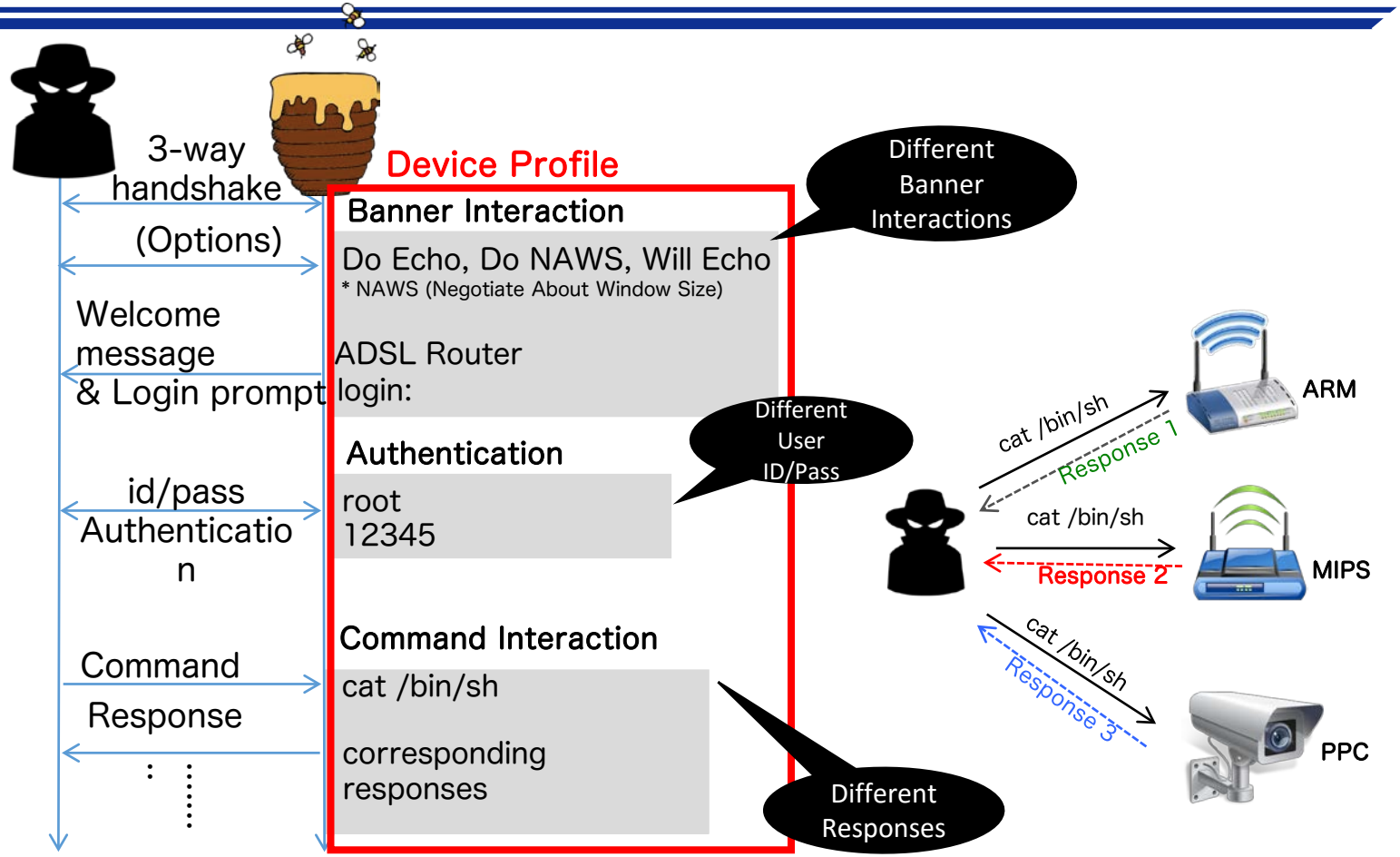
IoT malware of different CPU Architecture



- Handle to run malware of different CPU architectures

National Institute of Information and Communications Technology

Emulating different devices

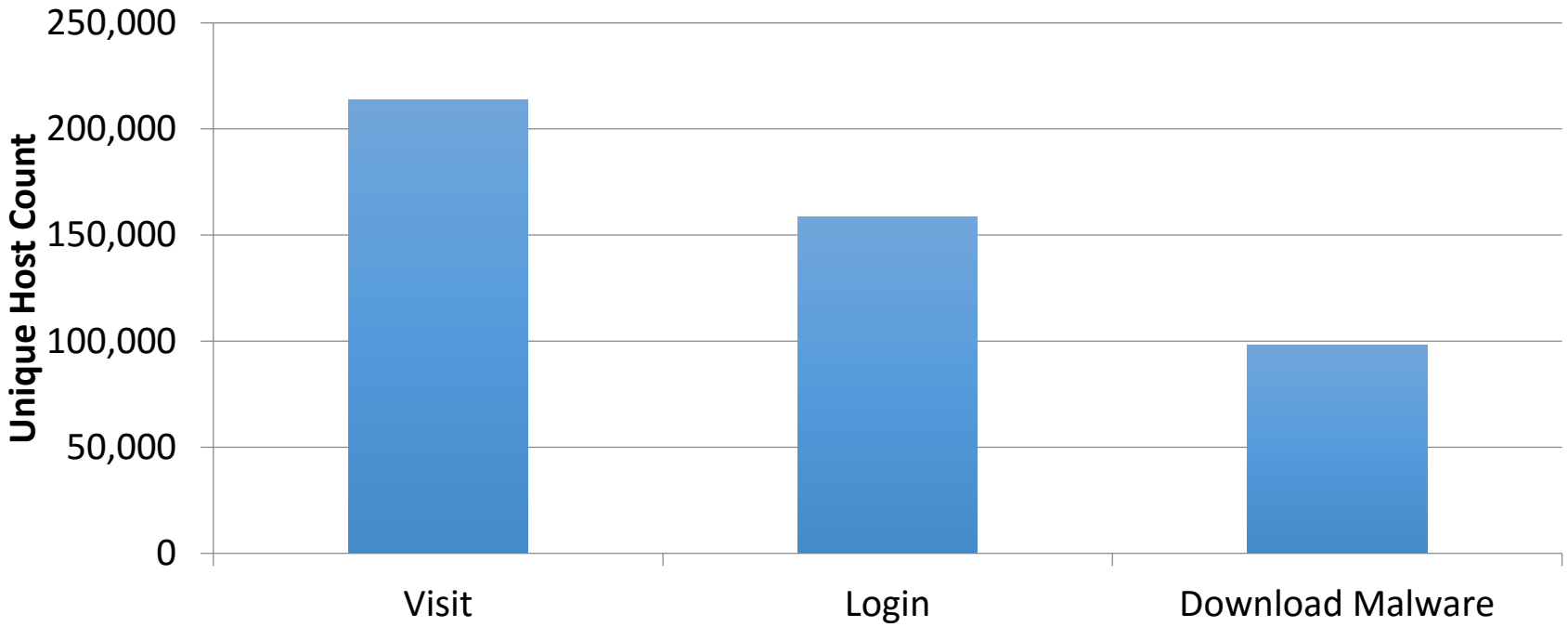


- **Different Banner Interactions**
  - Scanning Internet on port 23 to get different banners
- **Different User ID/Pass**
  - Obtain weak/default ID/Pass by web search
- **Different Interactions/Responses**
  - Learn from actual devices
  - System with general configuration for embedded devices (e.g. OpenWRT…)

National Institute of Information and Communications Technology

IoTPOT results

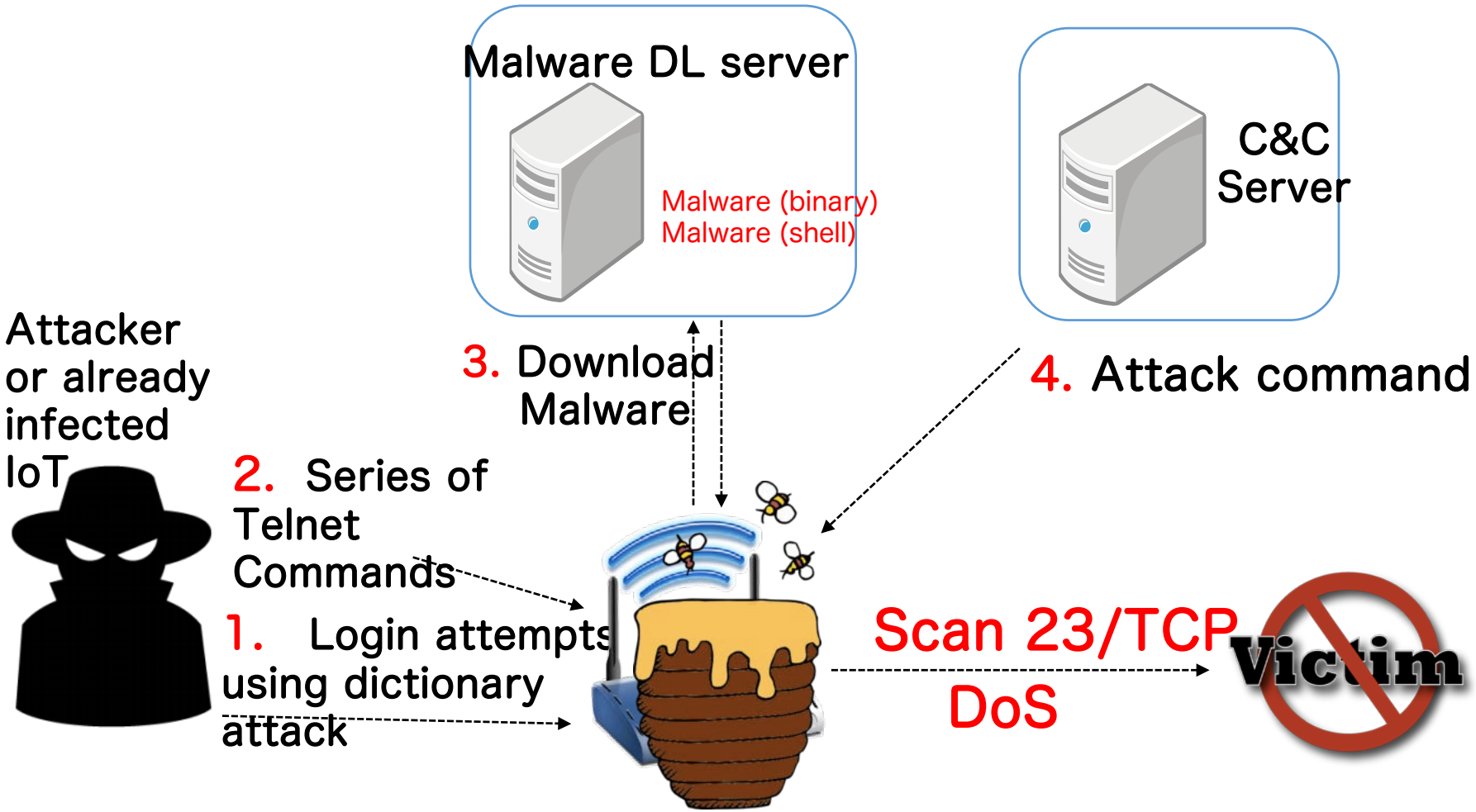
- During 122 days of operations [April 01 to July 31 - 2015]



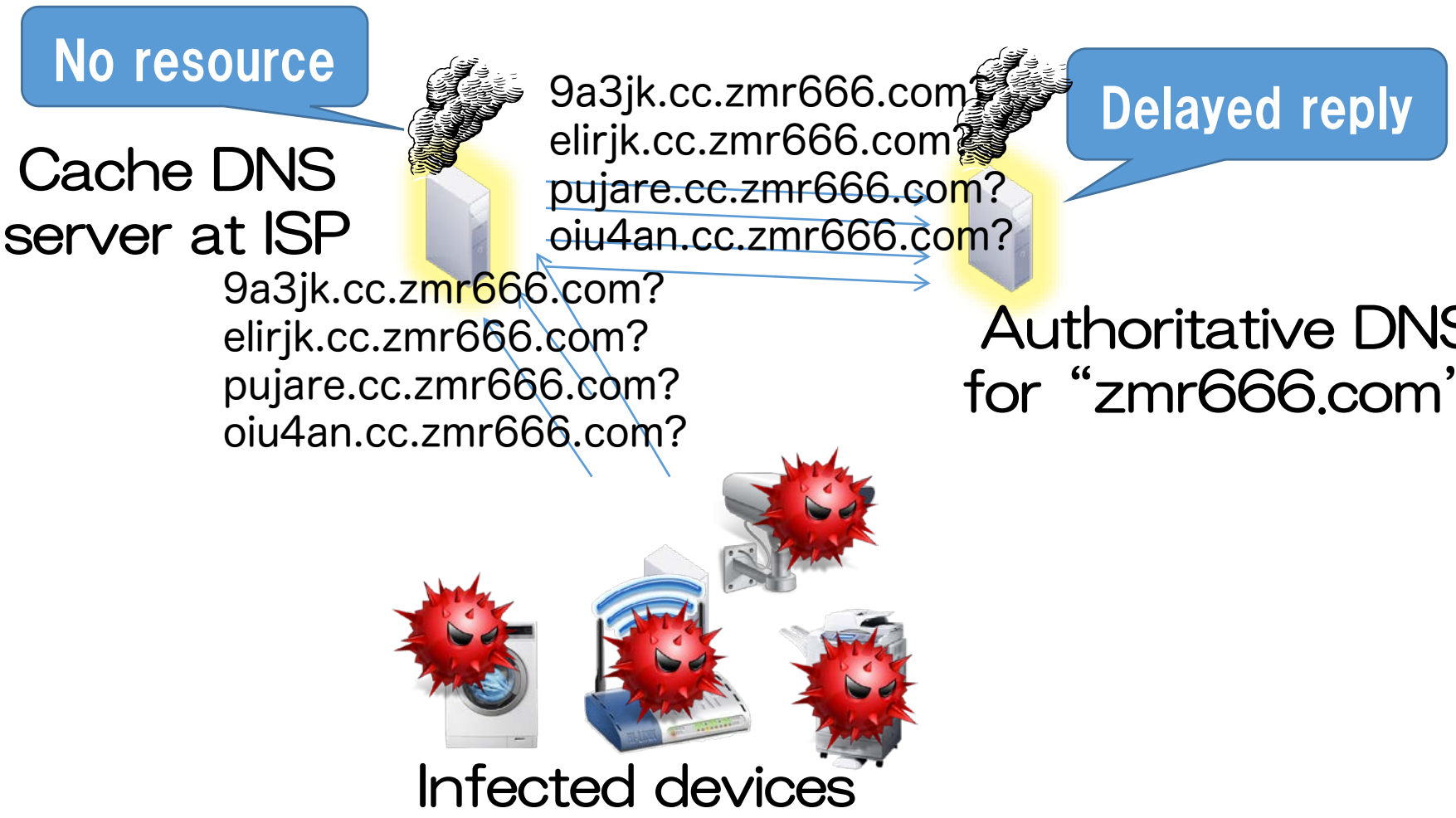
- 90,394 Malware Download Attempts
- Malware of 11 different CPU architectures
- 93% of downloaded binaries are new to Virus Total (2015/09)

NICT National Institute of Information and Communications Technology

General flow of telnet based attacks

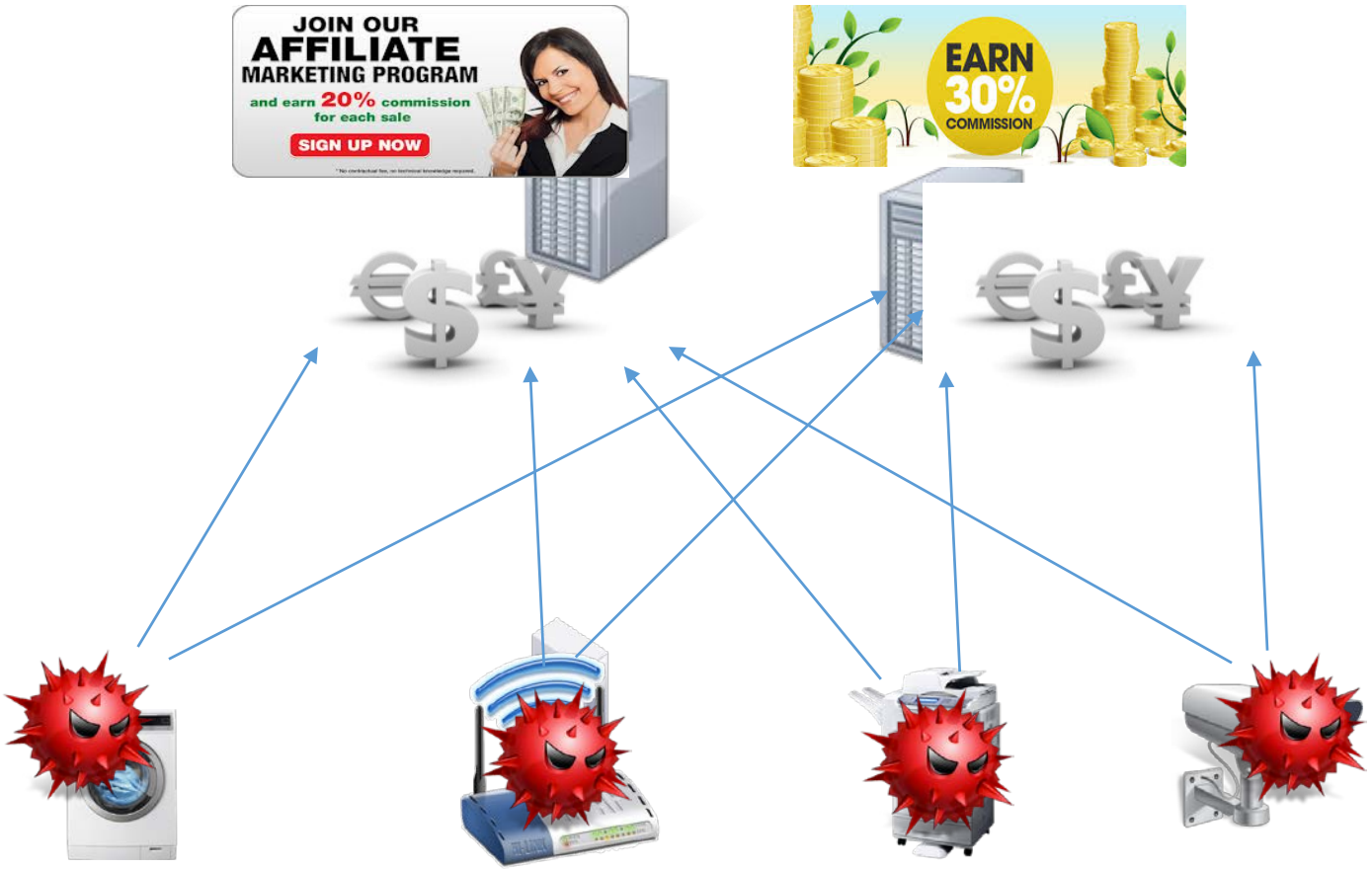


Attack Example1: DNS Water Torture attacks



Attack Example-2: Click fraud

Infected devices imitates user clicks
to advertising web sites

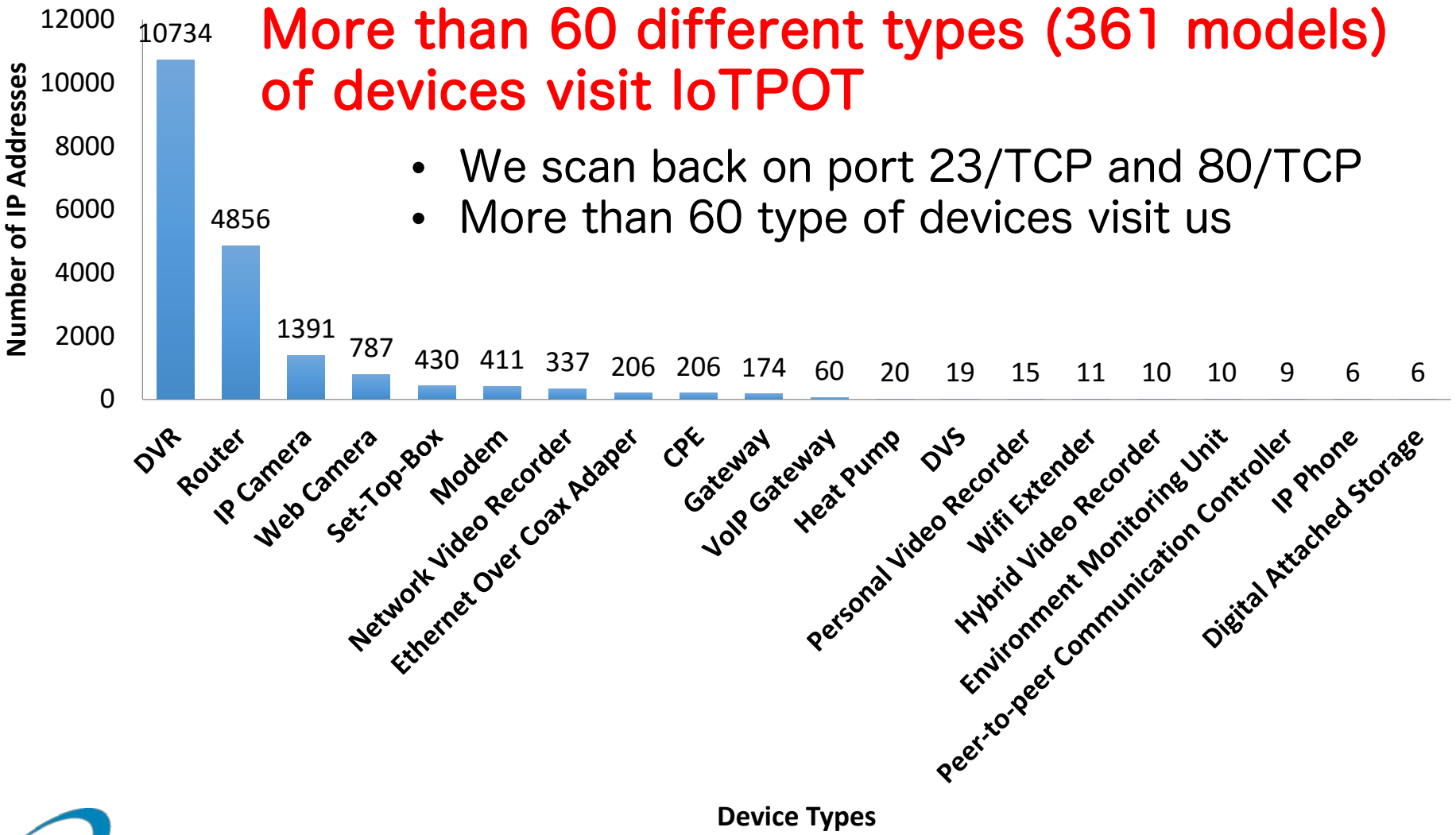


Infected Devices

Attack Example-3: Stealing credential from PPV

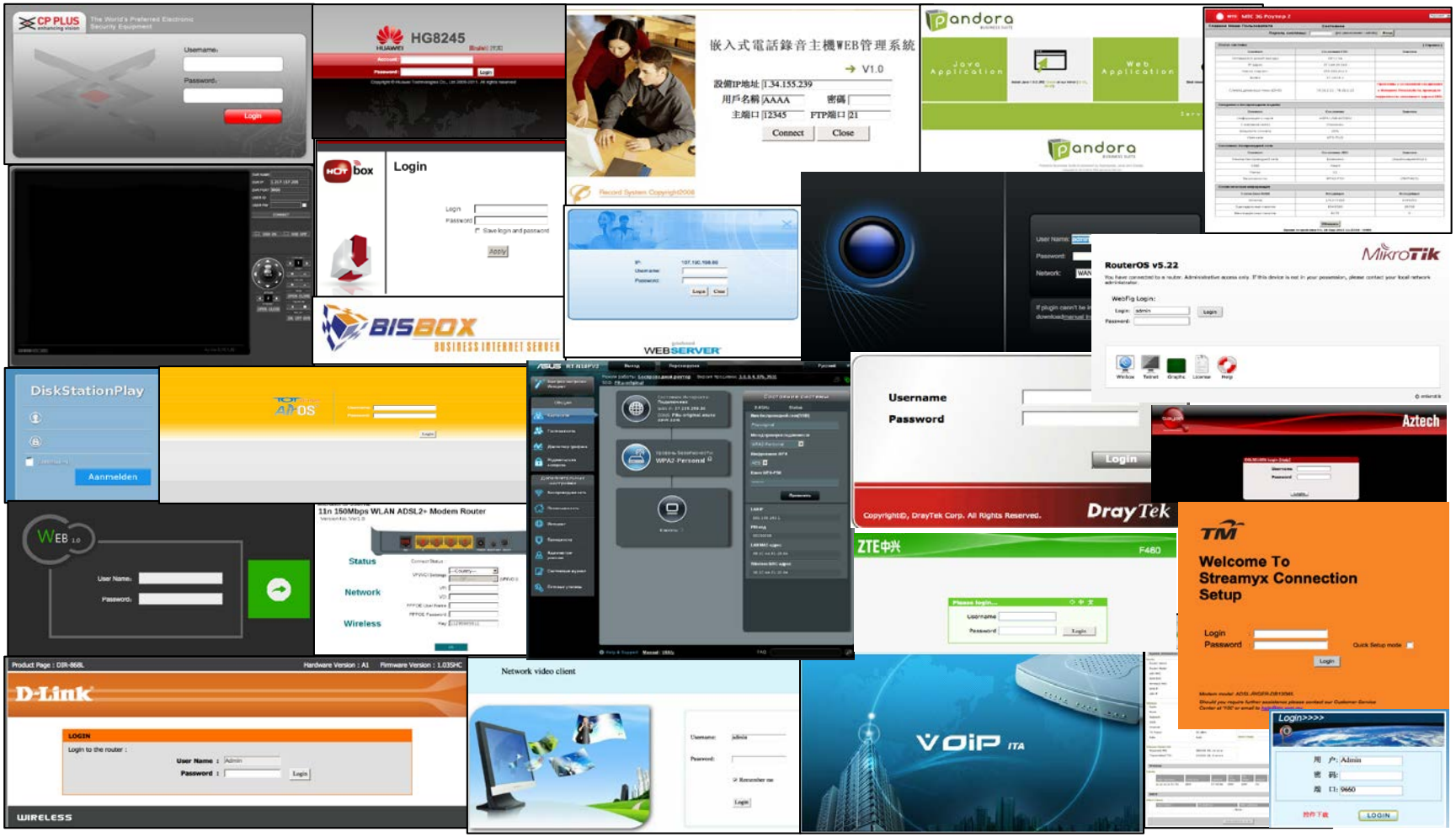
Particular set top boxes are being targeted (such as dreambox)

Looking back on devices visiting IoTPOT



National Institute of Information and Communications Technology

Web interfaces of devices attacking us

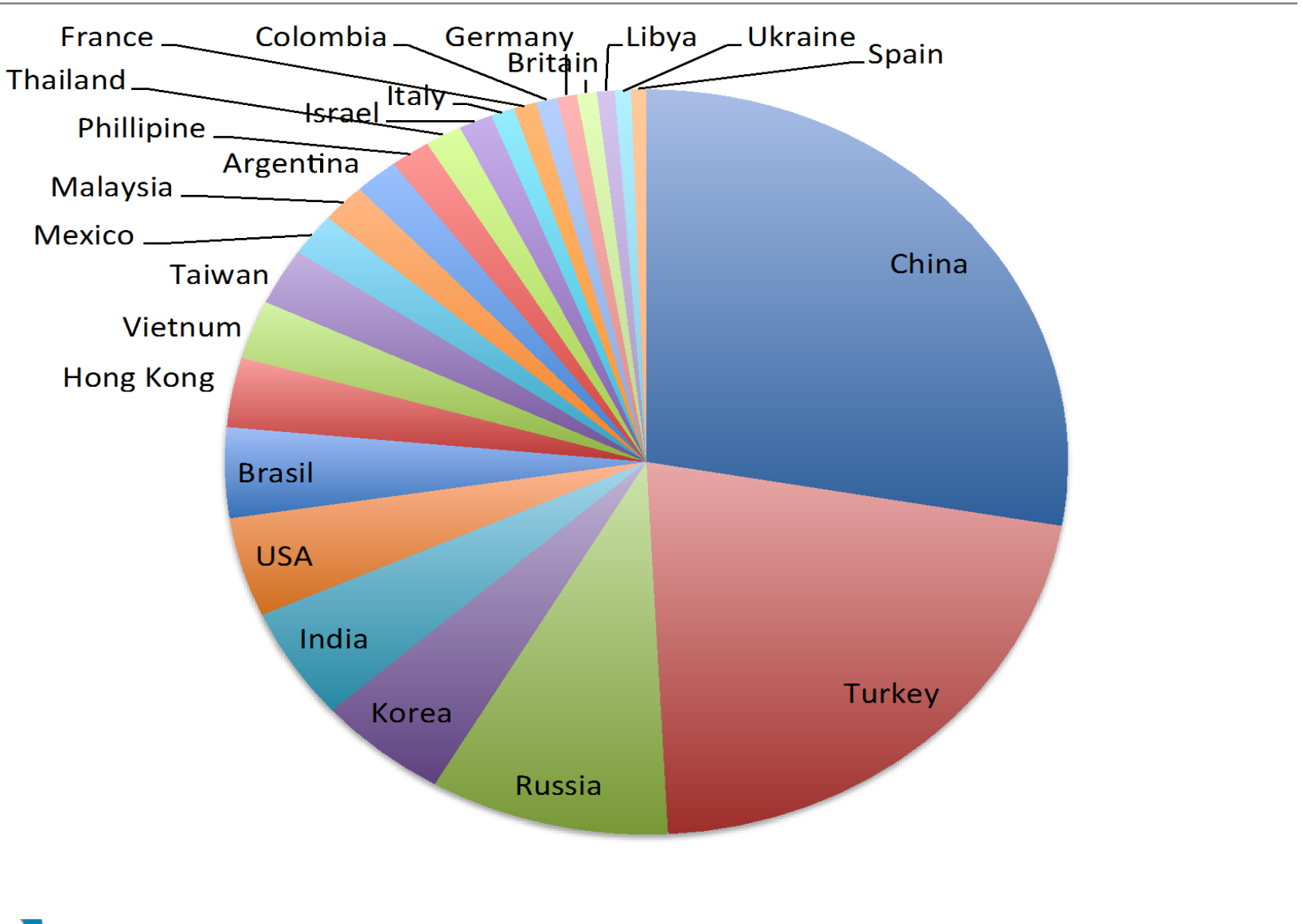


National Institute of Information and Communications Technology

Categorizing IoT device types infected by Malwares

Category	Device	Category	Device
Surveillance Group	IP Camera	Industrial Control System	Solid State Recorder
	DVR		Internet Communication Module
Networking Related Devices	Router		Data Acquisition Server
	Gateway		BACnet I/O Module
	Modem	Personal	Web Camera
	Bridge		Personal Video Recorder
	Security Appliance		Home Automation Gateway
Telephone System	VoIP Gateway	Broadcasting Facility	Digital Video Broadcaster
	IP Phone		Digital Video Scaler
	GSM Router		Video Encoder/Decoder
	Analog Phone Adapter		Settop Box
Infrastructure	Parking Management System	Other	Heat Pump
	LED display control system		Fire Alarm System
			Disk Recording System
			Optical Imaging Facility
			Fingerprint Scanner

AS with more than 1,000 infected IoT Devices



Key findings through our challenges

– Malware

- At least 6 DDoS malware families target IoT devices via Telnet
- Malware samples of 11 different CPU architectures are captured
- 93 % of samples are new to Virus Total
- One family has quickly evolved to target more devices with as many as 9 different CPU architectures

– Targets

- More than 60 types (361 models) of IoT devices are infected

– Monetization

- 11 types of DDoS attacks
- Scans (TCP/23,80,8080,5916 and UDP/ 123,3143)
- Fake web hosting
- Click fraud attacks
- Stealing credential of PPV and so on

Secure OTA Updates for ITS/IoT software/firmware

- One of the countermeasures against threats in ITS/IoT environments -

National Institute of Information and Communications Technology

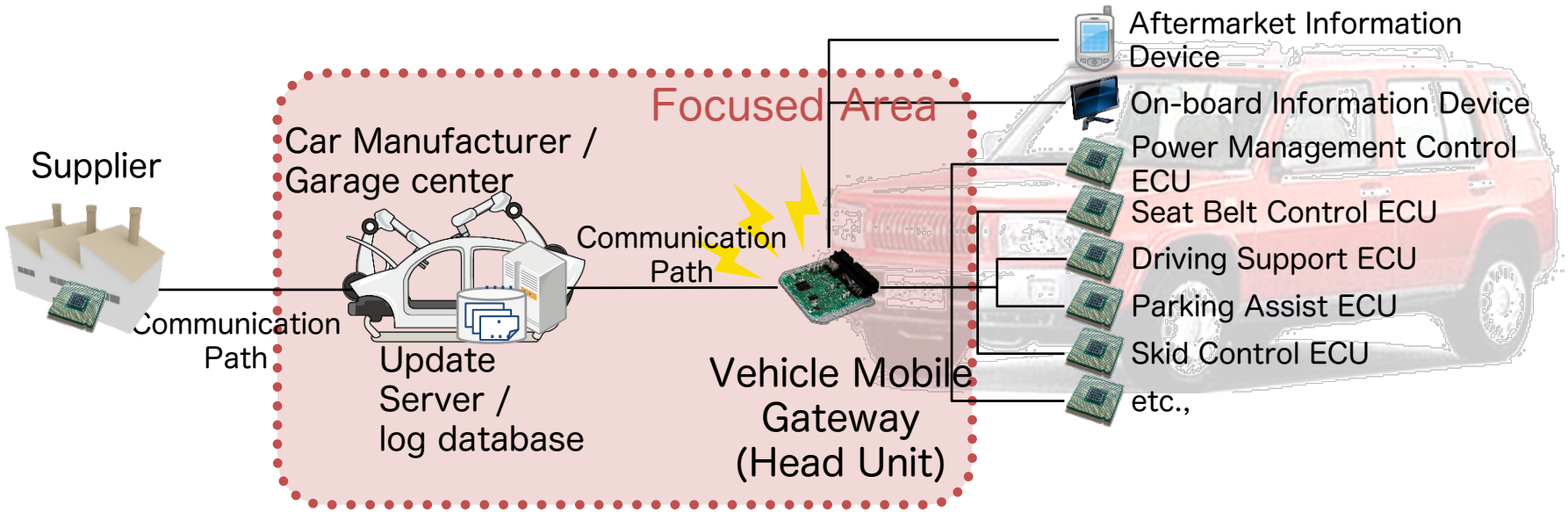
Development of an ITU-T Recommendation

- **ITU-T: International Telecommunication Union, Telecom sector**
  - SG17: Responsible for security standards
- **Title of Recommendation**
  - "Secure software update capability for ITS communications devices" (X.itssec-1)
- **Purpose**
  - to provide common methods to update the software by a secure procedure including security controls and protocol definition
  - The adoption of the Recommendation is not mandatory for automotive industries, but the Recommendation would be a guideline of the baseline security for networked vehicle.
- **Editors**
  - Masashi Eto (NICT)
  - Koji Nakao (KDDI/NICT)

National Institute of Information and Communications Technology

Secure OTA Updates for ITS/IoT software/firmware

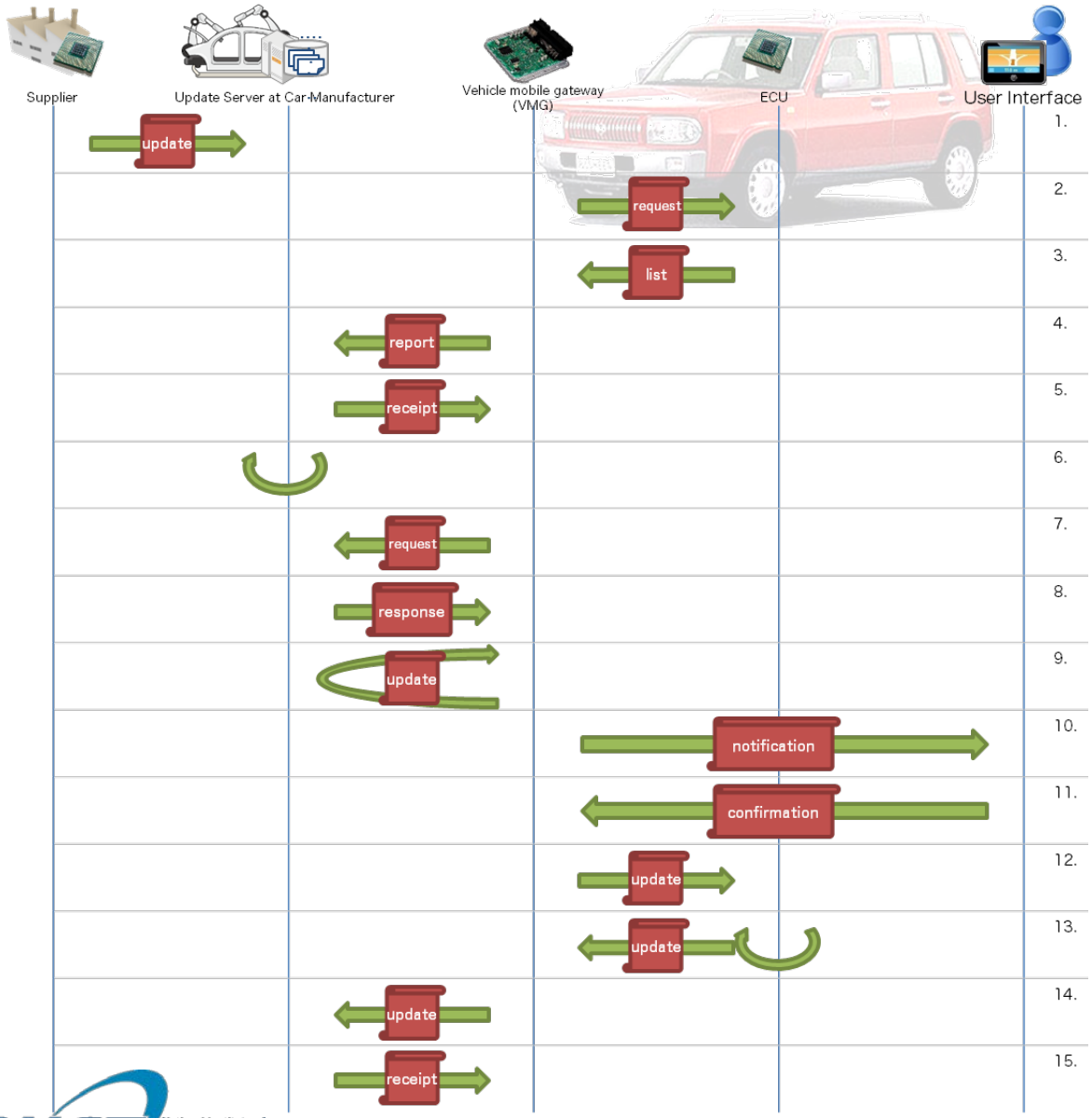
- General model of networked vehicle



This procedure is under development for ITU-T Recommendation (will be fixed in September, 2016)

National Institute of Information and Communications Technology

An example of ITS software remote update procedure



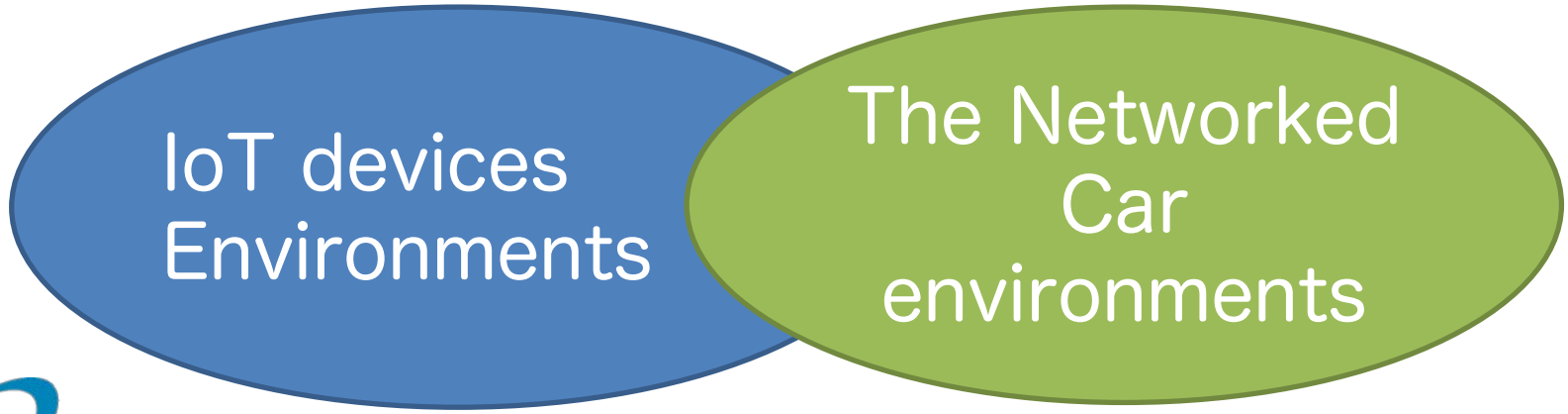
1. update
2. request — Request of diagnose of software status
3. list — Result of diagnose with software status
4. report — Report of results of ECUs in a vehicle
5. receipt — Receipt for submit of diagnose report
6.
7. request — Request of update module
8. response — Update module is provided
9. update
10. notification — Notification to User (driver) for Updates
11. confirmation — Confirmation for the update
12. update — Request for updates to ECUs
13. update — Results for updates in ECUs
14. update — Report of application of the update
15. receipt — Conformation from the Update server

National Institute of Information and Communications Technology

Conclusion

<Security Key Controls for ITS/IoT environments>

1. Threat observation/analysis and Vulnerability detection
2. Malware/intrusion detection
3. Remote curing method for vulnerable IoT devices
4. Remote OTA Software Update (ITU-T)
5. Data Confidentiality
   – Light-weight crypto
6. Appropriate Authentication and Access control
7. Incident handling and Information (threat) sharing



Thank you for your attention!