RESTENA
Réseau Téléinformatique de l'Education Nationale et de la Recherche

CIRCL
Computer Incident Response Center Luxembourg

TNC'17 Networking Conference, Linz, Austria, 29 May- 2 June 2017

An extended analysis of an IoT malware from a blackhole network

A. Dulaunoy♦, G. Wagener♦, S. Mokkadem▪ and C. Wagner♣

♦ Computer Incident Response Center Luxembourg – CIRCL
▪ Université Catholique de Louvain
♣ Fondation RESTENA

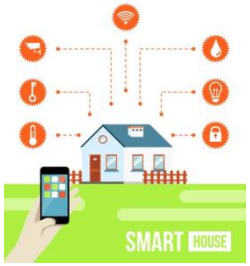
Introduction – Internet of Things (IoT)

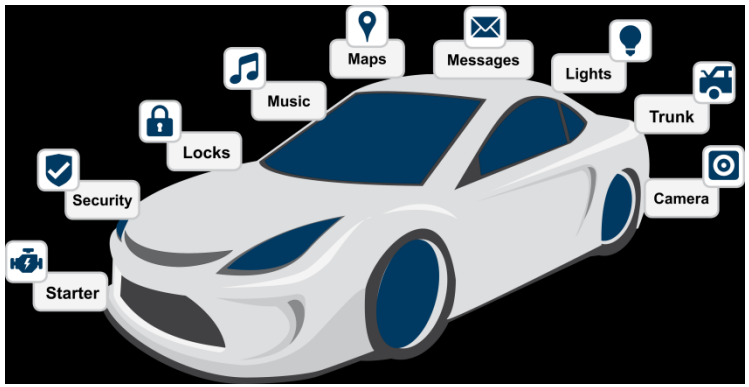
- Defined by the Oxford dictionnary as

"the interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data"

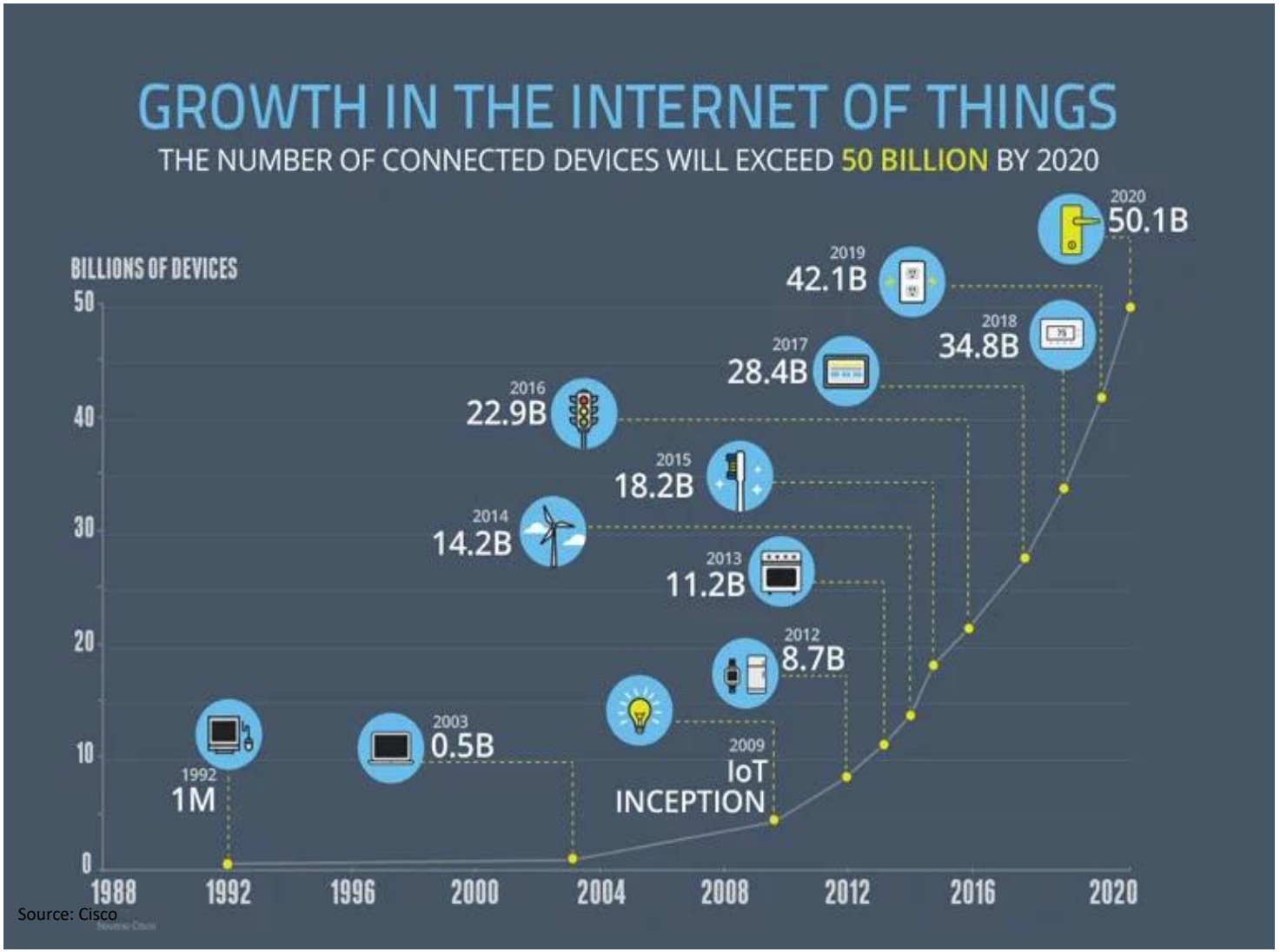
Introduction – Internet of Things (IoT)

- What and where is IoT? … Almost everywhere?





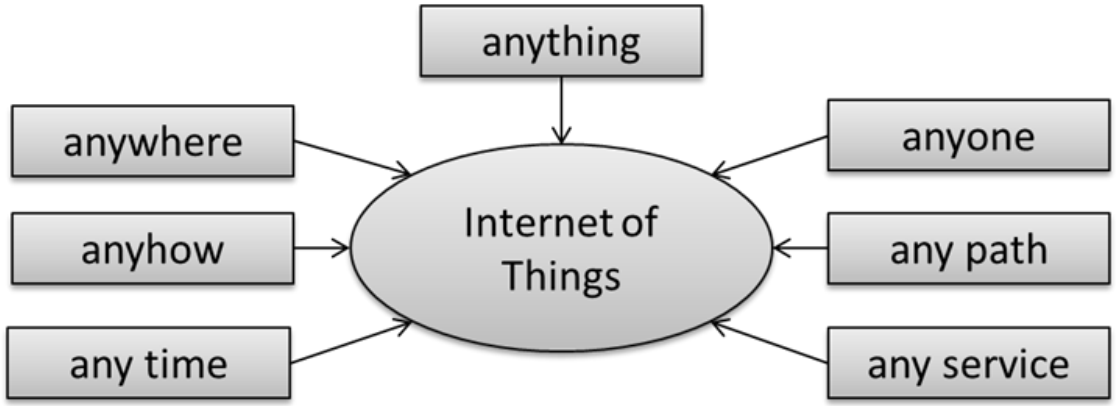
Introduction – Internet of Things (IoT)



Source: Cisco

Introduction – Internet of Things (IoT)

- IoT device design
  - Easy to use for user → most convincing argument
    - Connect and use
    - No tedious configuration needed
  - Fast
    - Only for the purpose of the device
      (and maybe some data collection?)
  - cheap
  - "any"paradigm



Introduction – Internet of Things (IoT)

- Plethora of security issues
  - Weak to no security features at all
  - Vulnerabilities range from
    - Default passwords
      - "admin" "administrator" "1234" "admin1234" "none"
    - Weak C implementations
    - Devices cannot be patched or only hardly updated (if supported)
  - High exposure to unsophisticated attacks

Blackhole traffic

- Blackhole traffic
  - Routable non-used address space of an ISP
  - Arriving traffic is unidirectional and unsolicited
  - A particularity of the used blackhole
    - Close to private network address space (RFC 1918)
  - Traffic contains
    - Noise and scans for vulnerable systems, ex. SSH brute-force
    - Backscatter traffic, ex. spoofed DoS
    - Self-replicating code using network as vector, ex. Conficker
    - Badly configured devices, ex. printers, server, routers, IoT devices

```
SYSLOG lpr.error printer: offline
  or intervention needed
SYSLOG lpr.error printer: paper out
...
SYSLOG lpr.error printer: paper jam
```

Blackhole traffic

- The observations from the blackhole
  - Long term analysis
    - Started in 2014
      - presented paper about misconfigured devices @TNC2014
    - 2 IPv4 subnets
      - Close to RFC 1918
  - IoT malware and classical malware
    - Focus on Mirai analysis
  - Other botnet traffic
    - Recent observations after Mirai

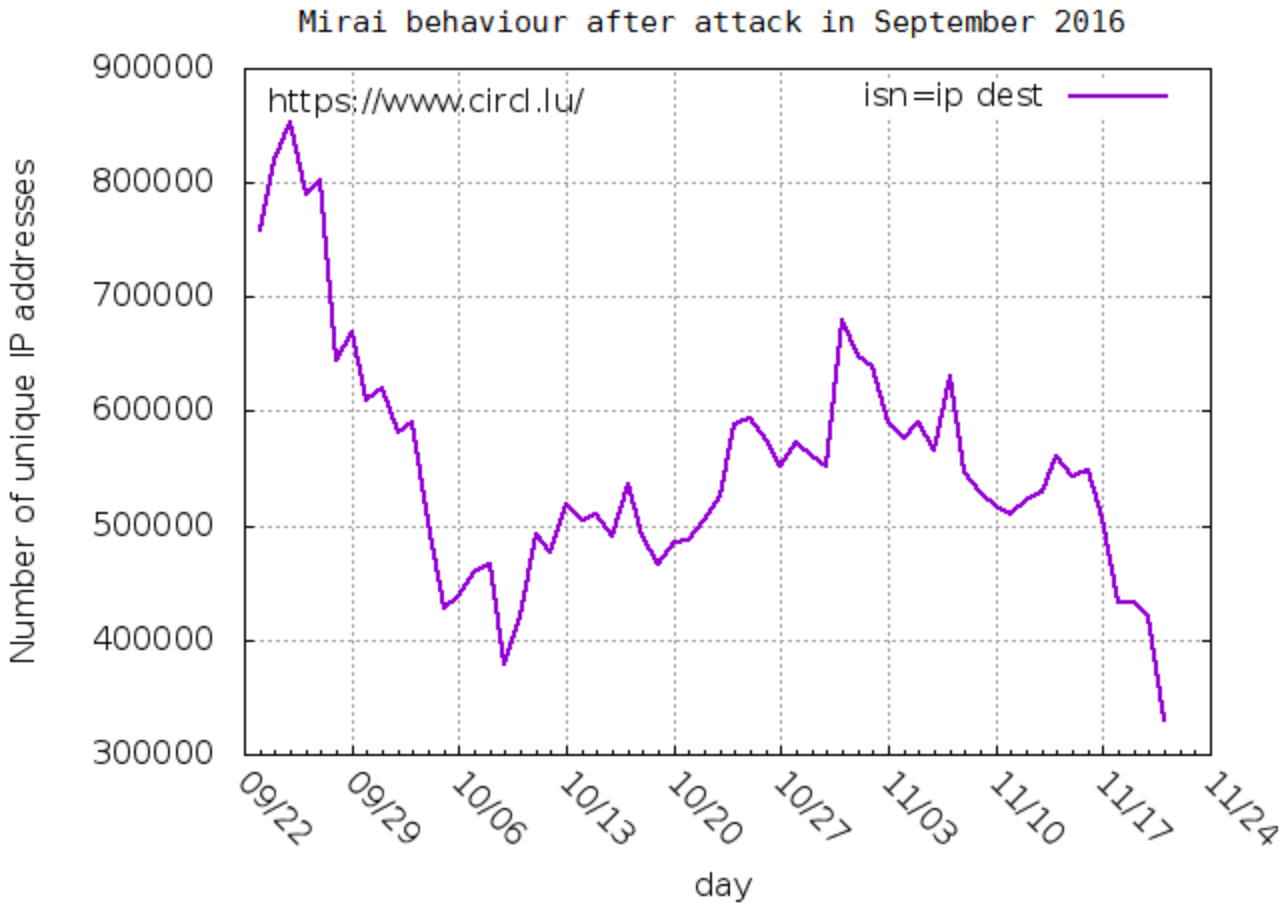
Iot Malware analysis - Mirai

- Fingerprinting Mirai
  - First appeared in August 2016
  - Strongest attack in IoT history in September 2016
    - Strong DDOS attack against a significant DNS-provider
    - Side effects on other large sites such as OVH, GitHub, Amazon,…
    - Estimated overall throughput of attack reached 1.2 Terabits/s
    - Involved more than 100 000 compromised devices
      - DVR players and digital cameras
  - Few weeks earlier
    - Less strong attack on the security blog "Krebs on Security"
    - Only reached estimated throughput of 665 Gigabits/s

Iot Malware analysis - Mirai

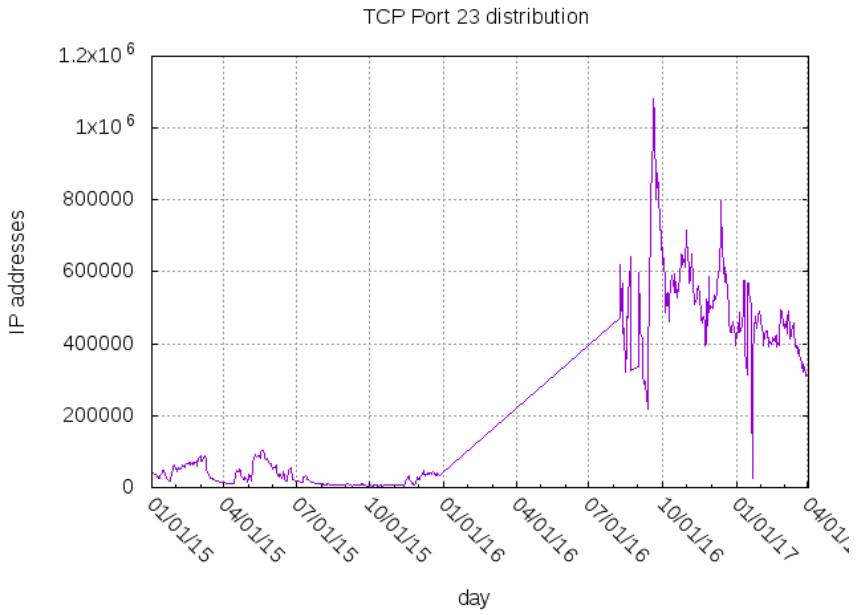
- Difference of Mirai to other attacks
  - Executed by compromised easy-to-hack IoT devices
  - On a very large scale
- Mirai was not only a "one time headliner"
- Source code shortly leaked after attack
  - Reach out for devices exposing telnet services on port 23 and 2323 (both TCP)
  - Bruteforce telnet servers with 63 default passwords
- Mirai fingerprint
  - Set the ISN (Initial sequence number) number to port number

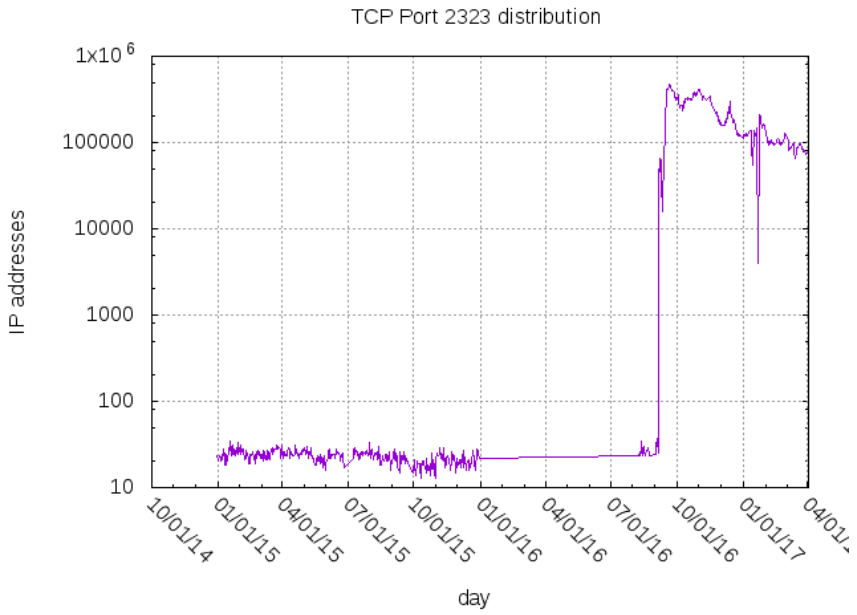
Iot Malware analysis – Mirai behaviour



Iot Malware analysis - Mirai

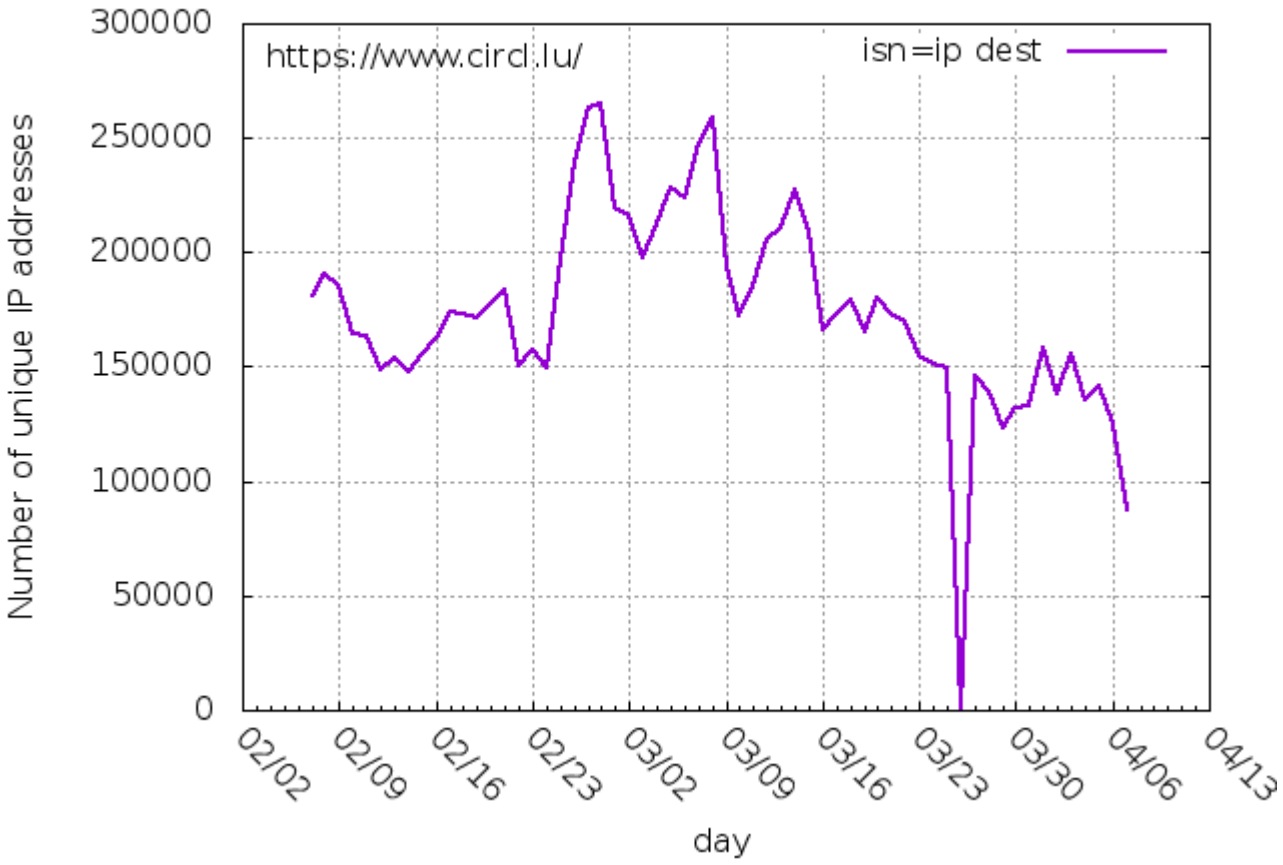
- Distribution of port 23 and 2323 over last 28 months



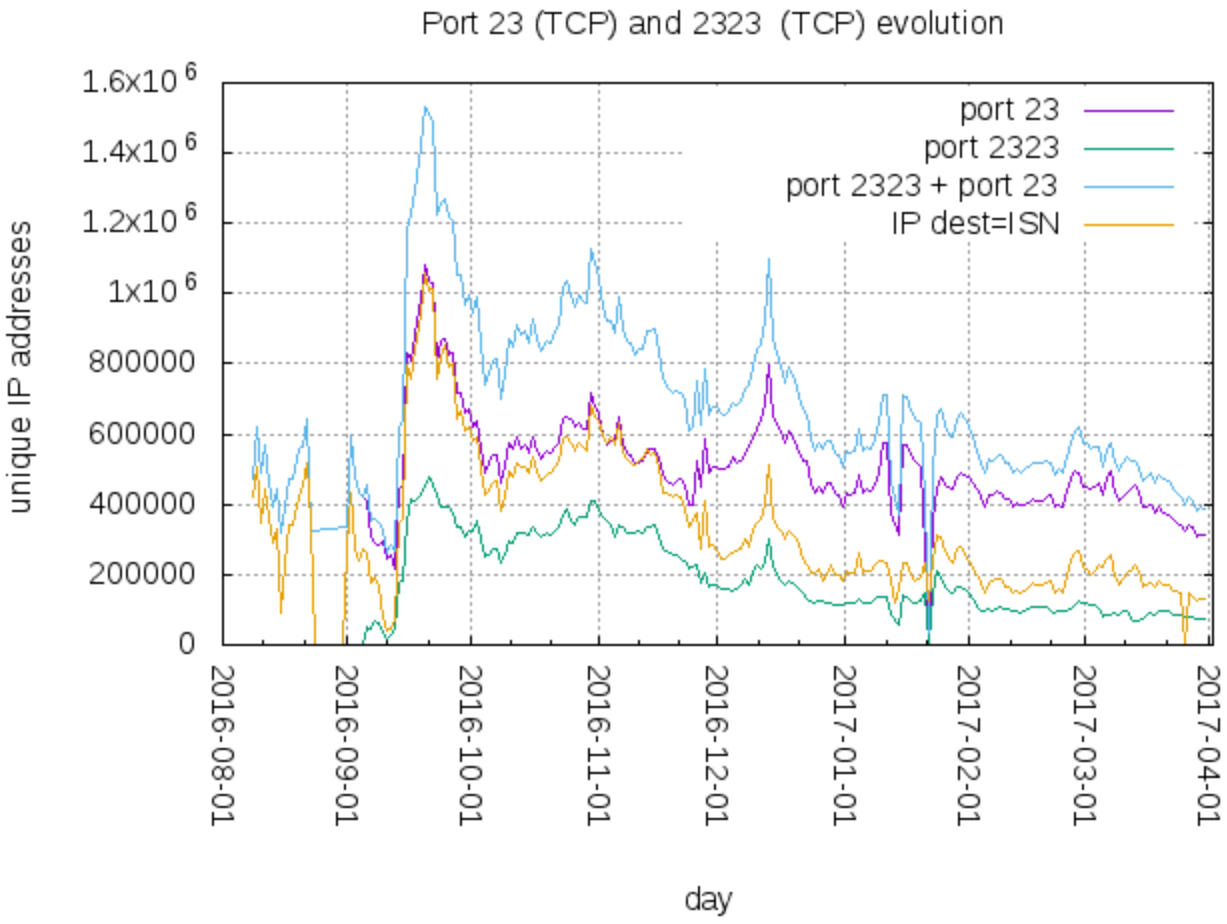


Iot Malware analysis - Mirai

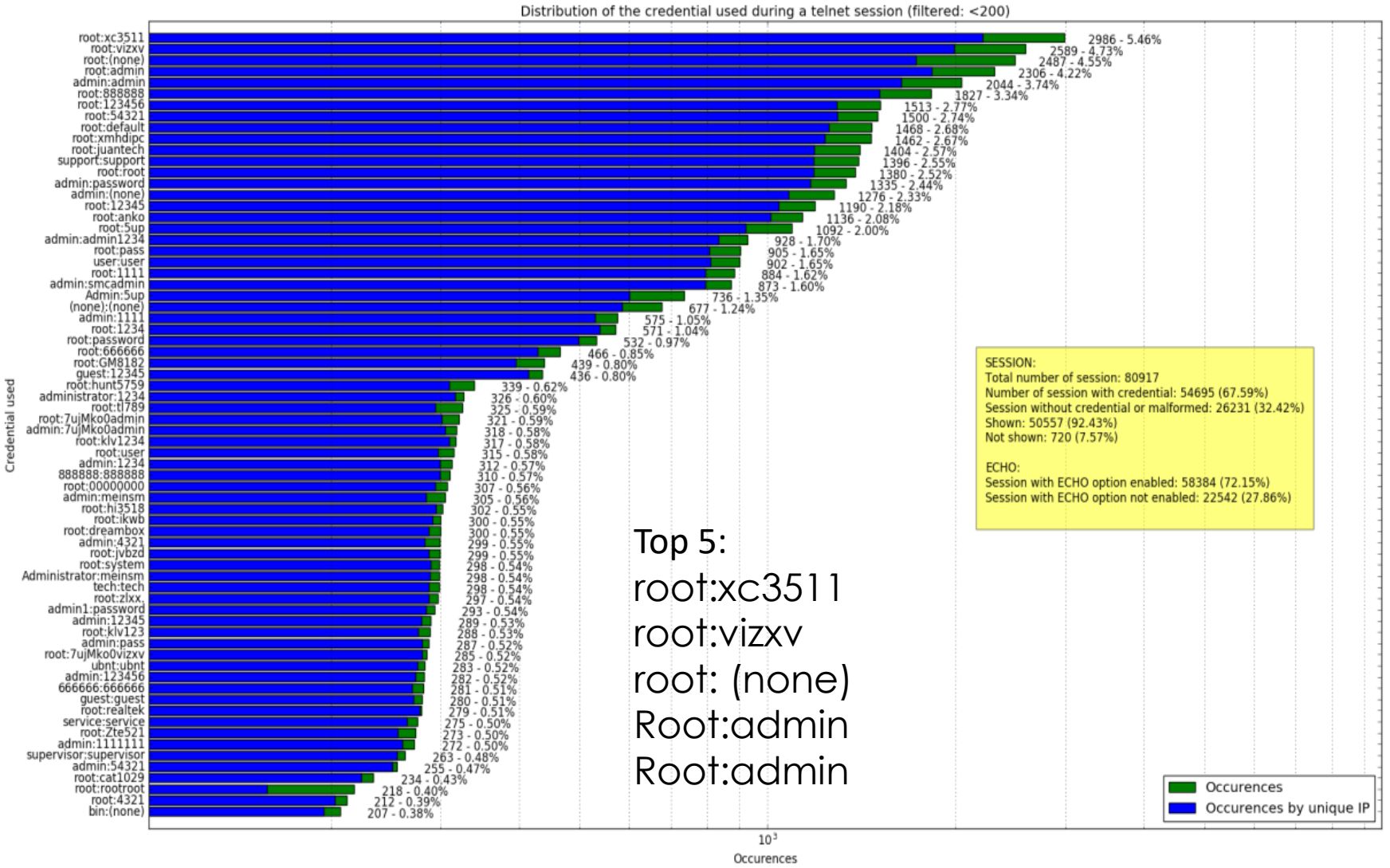
Mirai behaviour from February to April 2017



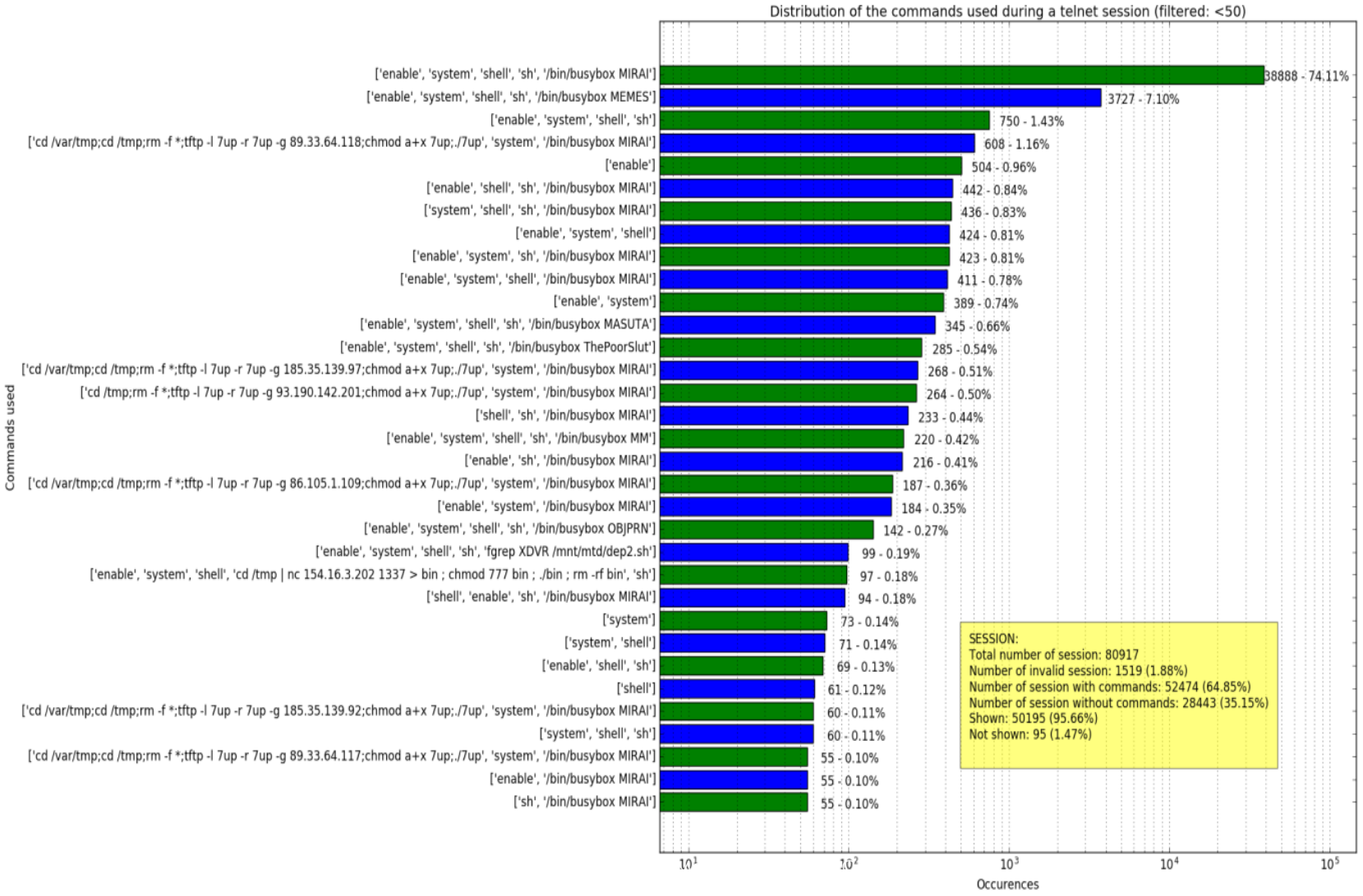
Evolution of Mirai



Telnet sessions - credentials



Telnet sessions - commands



Other malware observations

Frequency	Port numbers
17 040 164	53413
252 652	9999
11 087	534
7 188	54544
2 666	32764
1 810	5900
1 046	22
782	43413
200	29172
69	3074
25	23
22	53418

- Same blackhole dataset
- Other interesting port numbers
  - Port 53413
  - Port 9999
- Searches showed
  - Vulnerabilities detected for

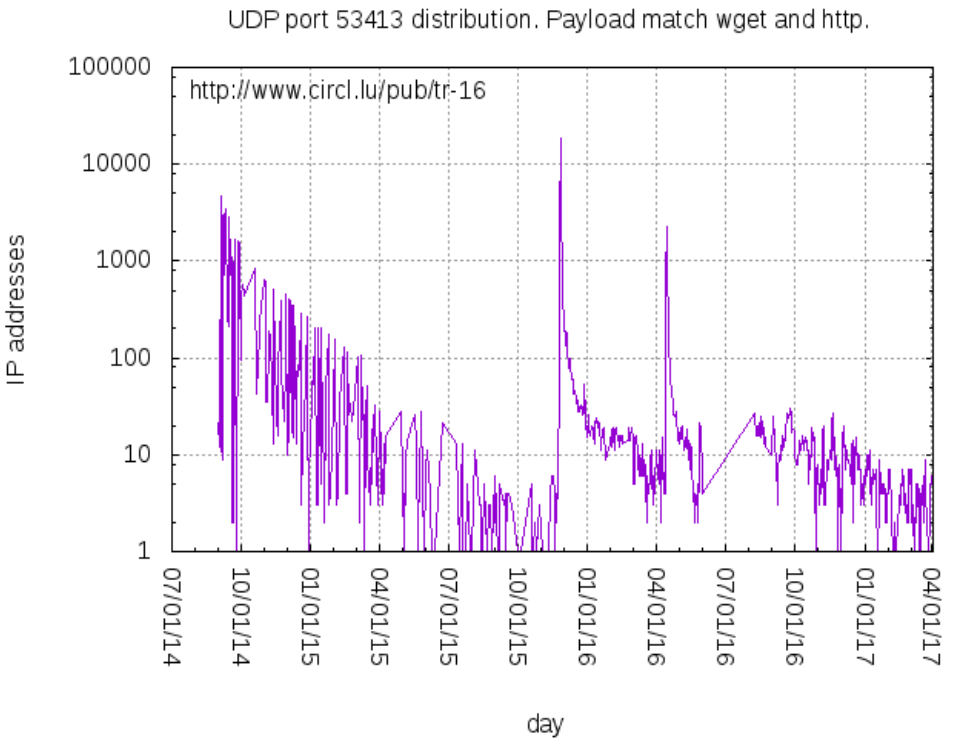
Netis router

- payload keywords “wget”/”http” used in exploit code

Asus router

- backdoor provides root priviledges

Other malware observations



- First peak close to vulnerability disclosure in 2014
- Second peak in 2015
  - Unique IP-addresses > factor 86
- Third peak in 2016
- Assumption
  - Still attractive for hackers even years after disclosure

Recent Mirai evolutions

- Mirai activities have not ceased yet!
  - Still a lot of Mirai activities observable in blackhole
- New variants have appeared
  - In February 2017 new variant
    - Windows machines compromised by trojans
    - Has built-in bitcoin mining module

    →Not only DDoS but increase attackers revenue
  - In April 2017
    - Brickerbot

    → Not only compromises also destoys device by permanent DoS

Conclusion

- Presented observations on Mirai
  - Future work long term observations on IoT malware
- IoT devices are installed and forgotten
  - Easy to use
    - Fast and cheap
  - Do not ask for maintenance
    - No or weak security only
- To reduce impact
  - Awareness next to users
  - Security by design
  - Vulnerabilities reported/shared within cybersecurity community (f.ex: MISP)

QUESTIONS?

THANK YOU!

Hack.lu is an open convention/conference where people can discuss about computer security, privacy, information technology and its cultural/technical implication on society.
13th edition (17-19 October 2017) in Luxembourg