Honeypots observations and their usefulness

CIRCL
Computer Incident
Response Center
Luxembourg

Gerard Wagener - *TLP:WHITE*

CIRCL

March 15, 2017

CIRCL
Computer Incident
Response Center
Luxembourg

- The Computer Incident Response Center Luxembourg (CIRCL) is a government-driven initiative designed to provide a systematic response facility to computer security threats and incidents
- CIRCL is the CERT for the private sector, communes and non-governmental entities in Luxembourg

Honeypots - introduction

Definition (Honeypots)

"A honeypot is security resource whose value lies in being probed, attacked, or compromised."[1]

Evolution

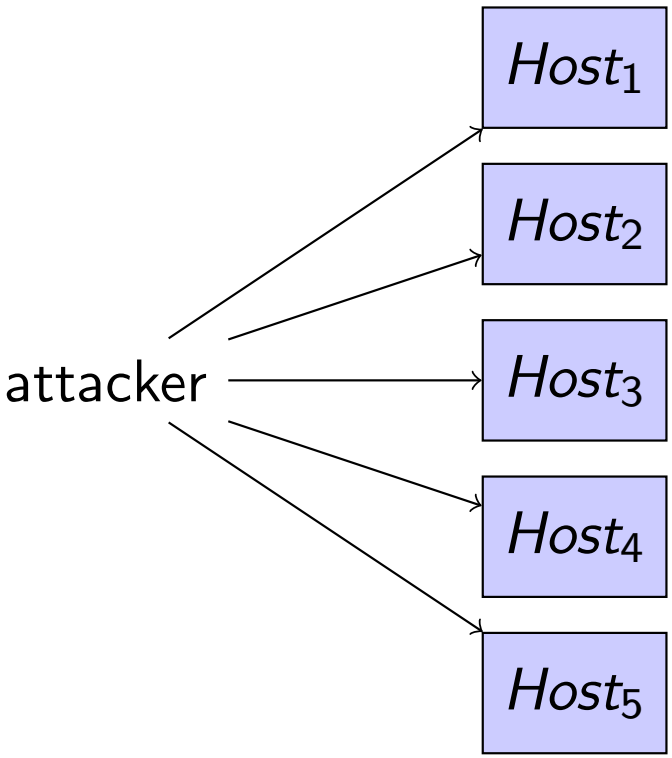
- Keeping attacker was experimented by Stoll in the late 80s[2]
- Honeypot concept pushed in the year 2002

[1] Lance Spitzner. Honeypots: Tracking Hackers. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2002, page 23.

[2] Clifford Stoll. Stalking the wily hacker. Commun. ACM, 31(5):484–497, 1988.

Honeypots - introduction

Opportunistic automated attacks

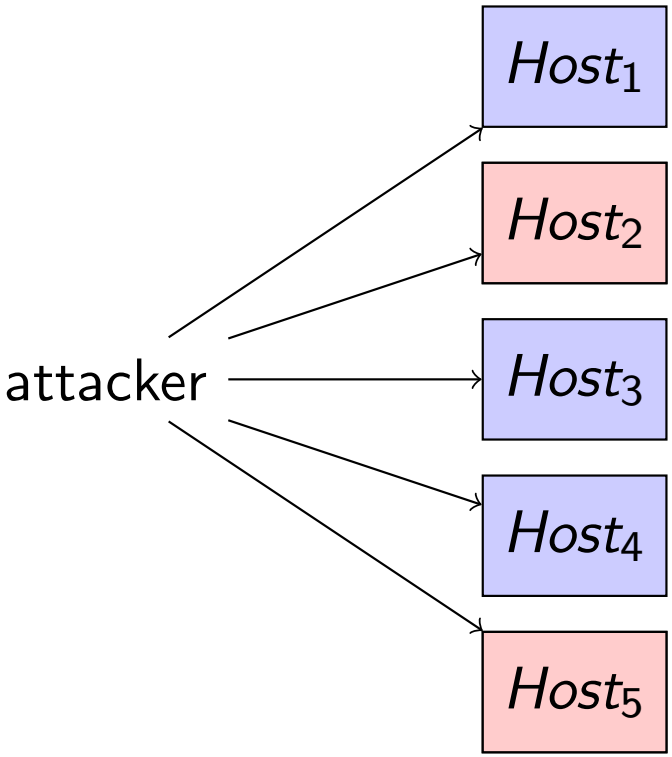


- Attacker scans arbitrary hosts
- 2^{32} possibilities for IPv4
- Abuse of vulnerable hosts

Monitor unused IPs $\rightarrow$ Honeypots

Honeypots - introduction

Opportunistic automated attacks



- Attacker scans arbitrary hosts
- 2^{32} possibilities for IPv4
- Abuse of vulnerable hosts

Monitor unused IPs $\rightarrow$ Honeypots

Honeypots - introduction

Motivation to monitor unused IP addresses

- Do not monitor legitimate traffic
  - Reduce false positives
  - Avoid privacy issues
- Detect opportunistic attacks
- Detect misconfigured machines
- Detect victims: DDOS, compromised servers, ...

Honeypot observations capabilities

Interactions

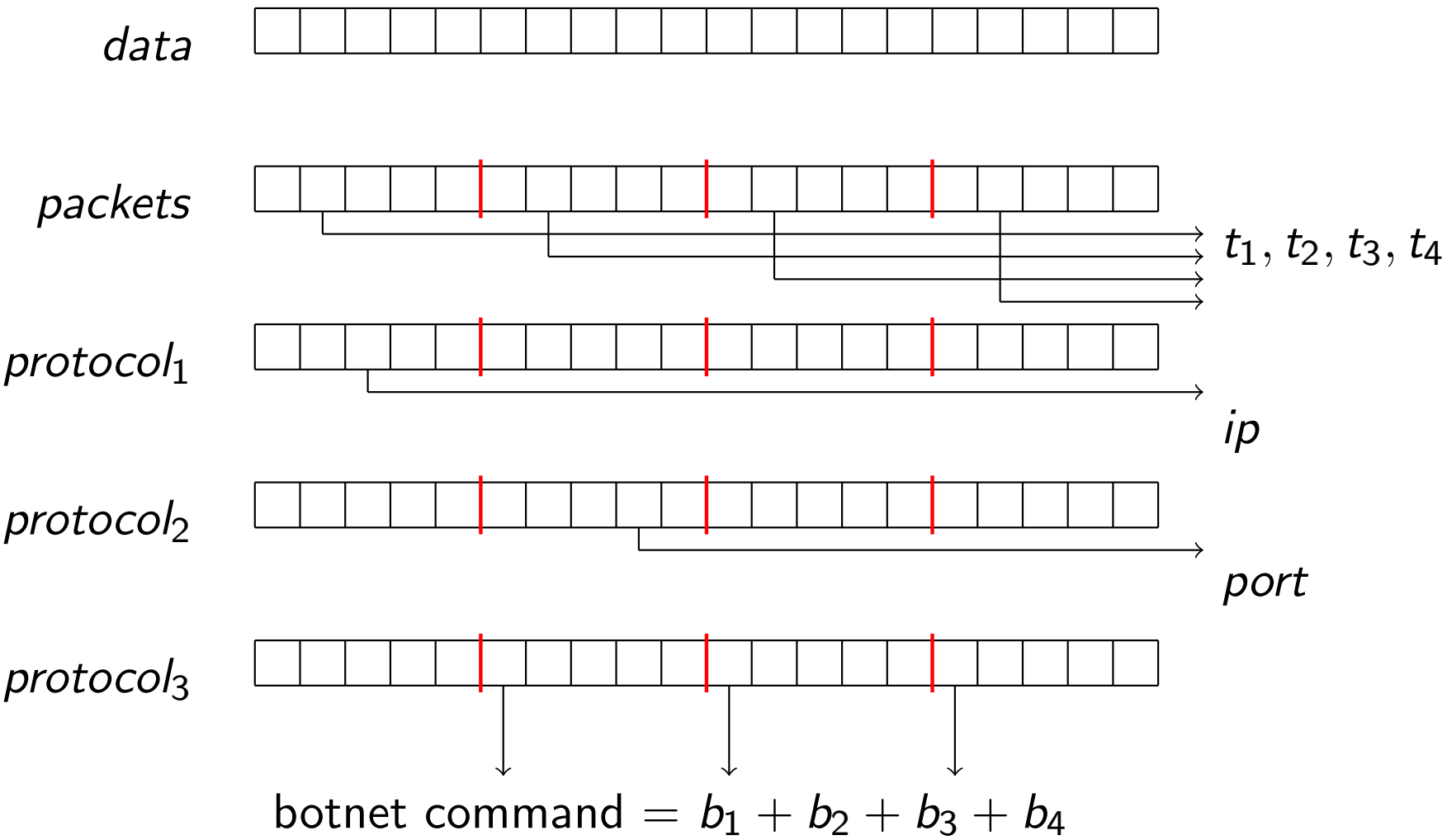
Information gain

- The more protocols you speak, the more information you get
- The more information you get, the more you get involved

Honeypot interaction levels

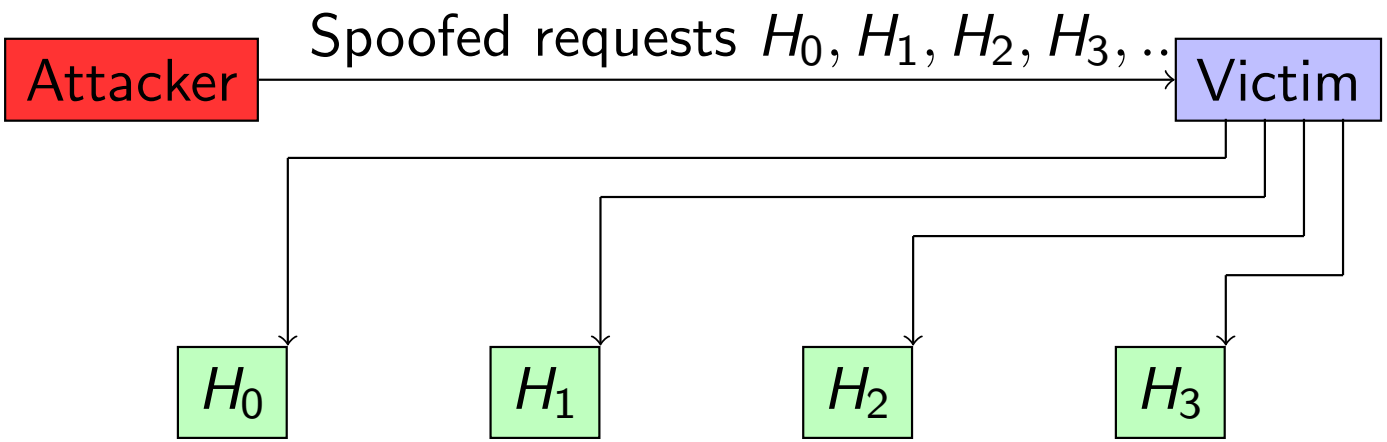
- Low interaction honeypots
- Mid interaction honeypots
- High interaction honeypots

Honeypot observations capabilities



Observing SYN floods attacks in backscatter traffic

Attack description

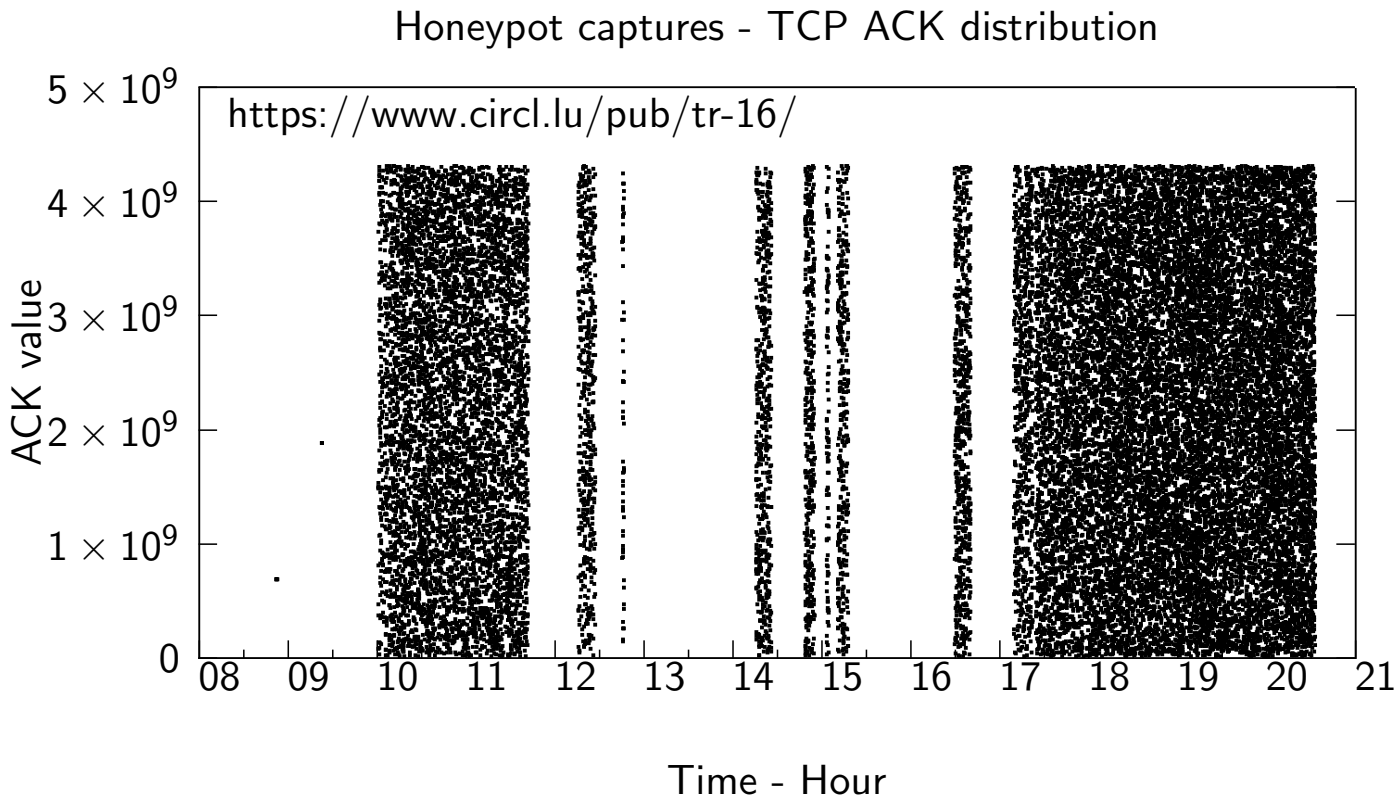


Connections
H_0
H_1
H_2
H_3

Fill up state connection state table of the victim

Observing SYN floods attacks in backscatter traffic

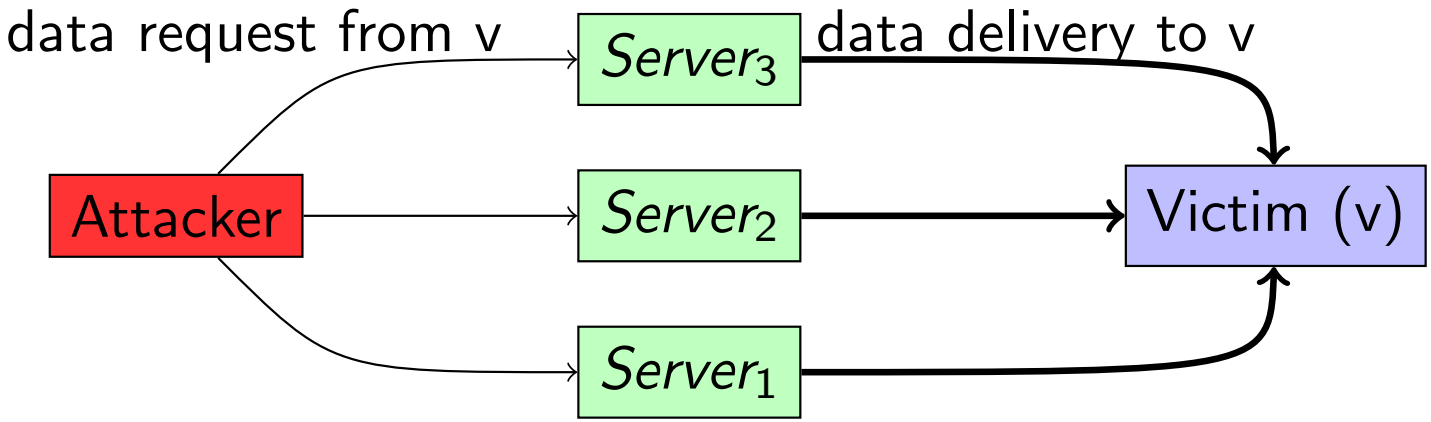
Plotting TCP acknowledgement numbers



Observing amplification attacks

Definition

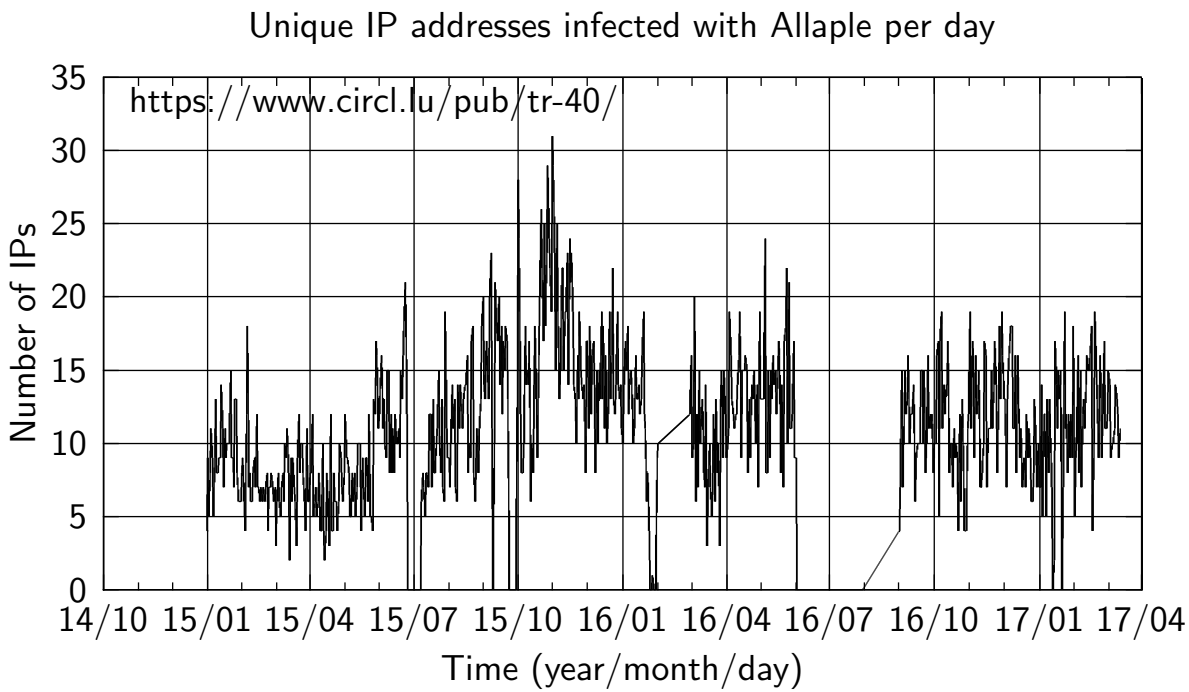
- y request of x bytes triggers responses of (x+Δ) bytes $\times$ selected vulnerable server (y)
- Abuse of vulnerable servers



Discovering the attacking infrastructure

Historical example: Allaple worm from 2006 - 2017

Attackers constantly scan for vulnerable hosts

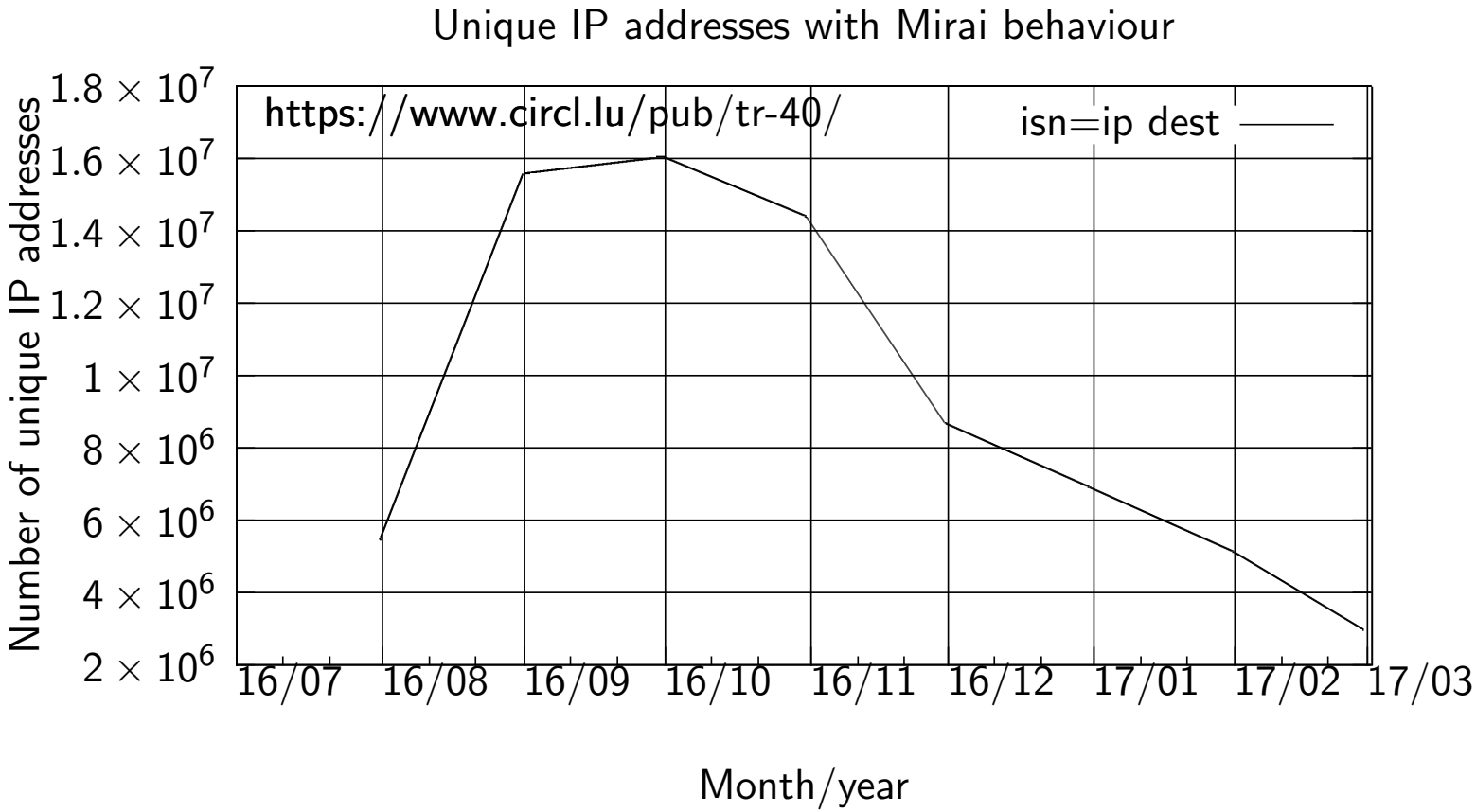


Probes for more than 10 years

Discovering the attacking infrastructure

Popular example: Mirai

Variant ISN=destination IP



Observing misconfigured systems

Human and Internet addressing is a good mix for errors

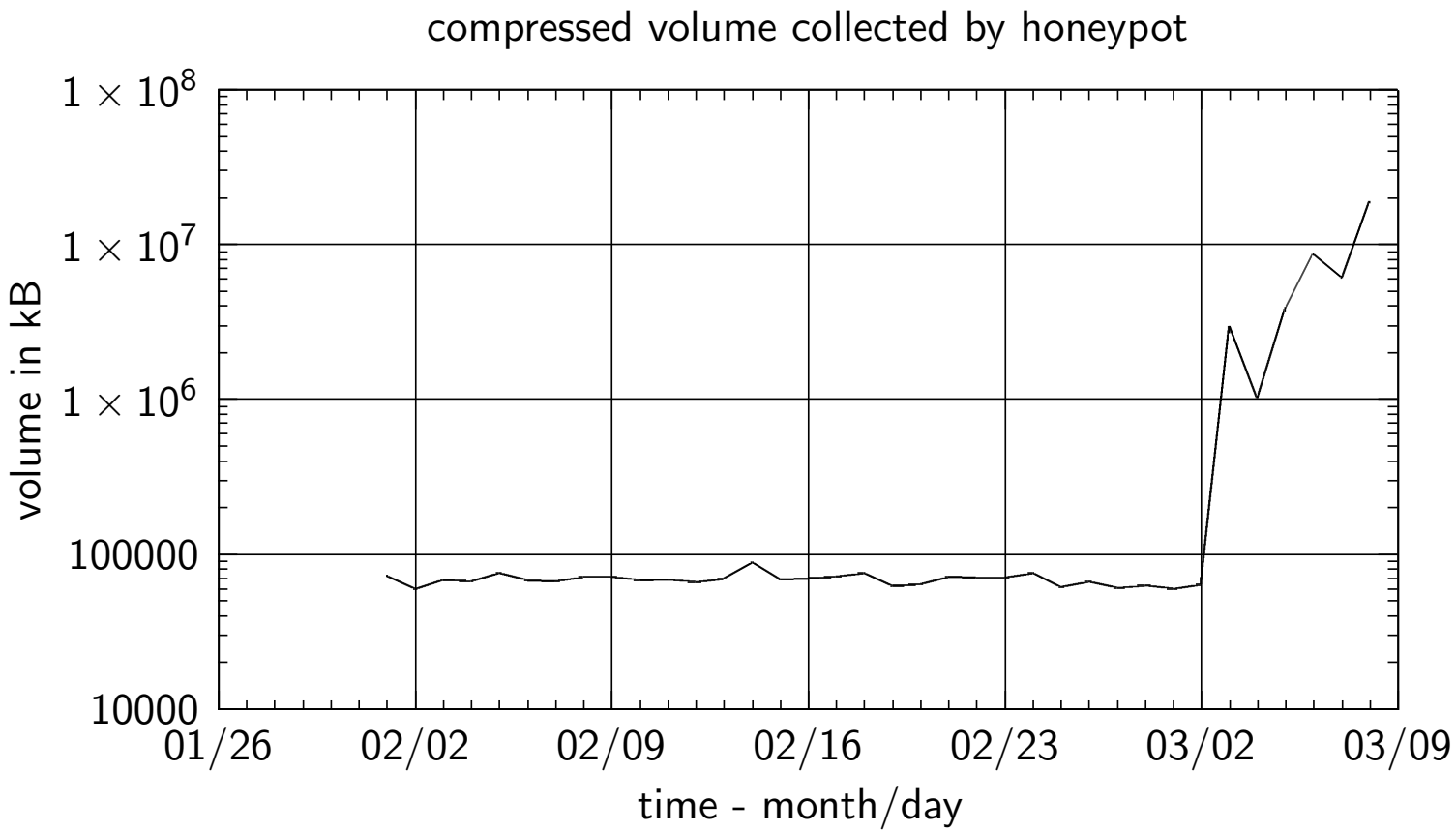
- Just look at "internal"[3] addresses that should not go on Internet
- Further reading: `https://www.circl.lu/assets/files/circl-blackhole-honeynetworkshop2014.pdf`

Hit wrong key	19**2**.x.z.y →	19**3**.x.y.z
Omission of number	1**9**2.x.y.z →	12.x.y.z
Doubling of keys	10.a.b.c →	10**0**.a.b.c
	172.x.y.z	1**5**2.x.y.z

[3] RFC1918

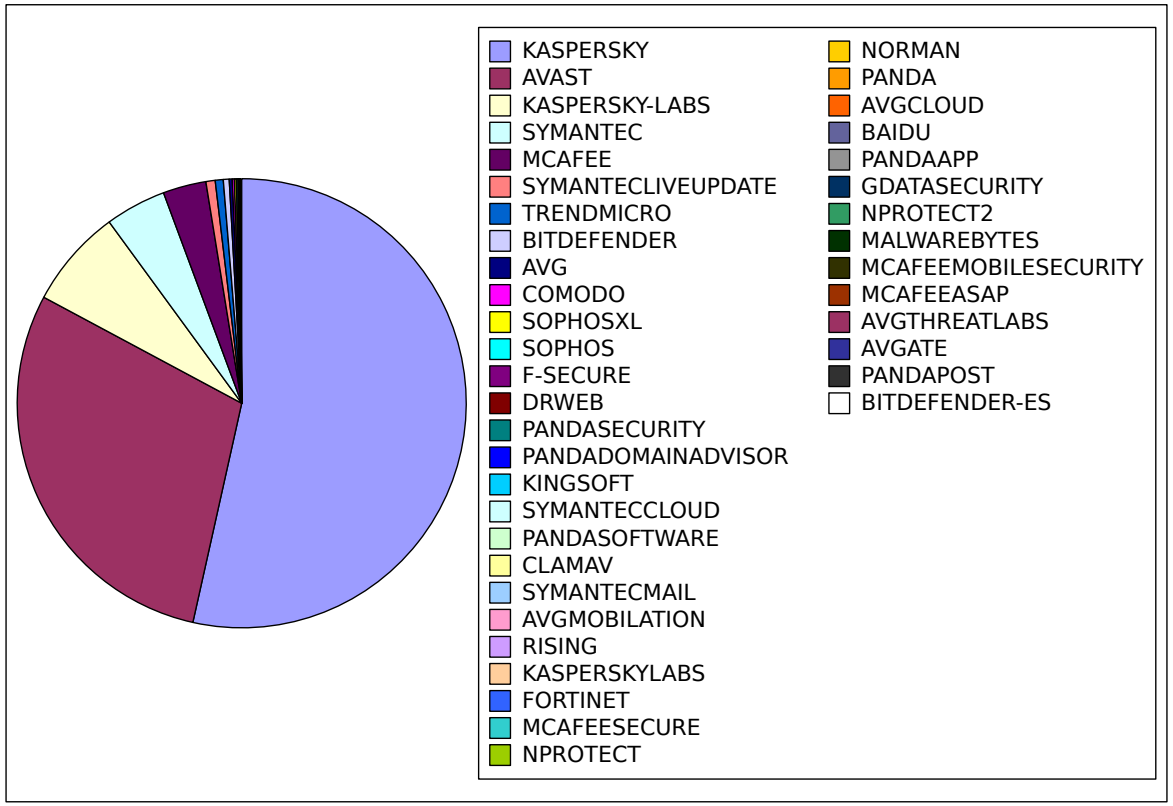
Observing misconfigured systems

Generic metrics



Observing misconfigured systems

Badly configured DNS resolvers



Antivirus software trying to fetch their updates from honeypots

Improving threat intelligence data

MISP sightings

Definition

- Threat intelligence data lookup in honeypot data
- Feedback to threat intelligence platform via sighting[4]
- Link threat intelligence data with honeypot observations
  - Identify opportunistic attacks
  - Identify misconfigured systems
  - Refresh time-to-live of attributes seen in honeypots
  - Determine the freshness of information

[4] http://www.misp.software/2017/02/16/Sighting-The-Next-Level.html

Conclusions

- Usefulness of honeypots
  - Detect opportunistic attacks
  - Detect trends: Netis backdoor,Heartbleed, Mirai,...
  - Detect misconfigured machines
  - Discover victims: DDOS, compromised servers, ...
  - Measuring attacker's capabilities
- Ongoing best effort research activities at CIRCL
- Getting involved[5]

[5] https://circl.lu/pub/tr-16/