Blackhole Networks

a source of intelligence to support investigations

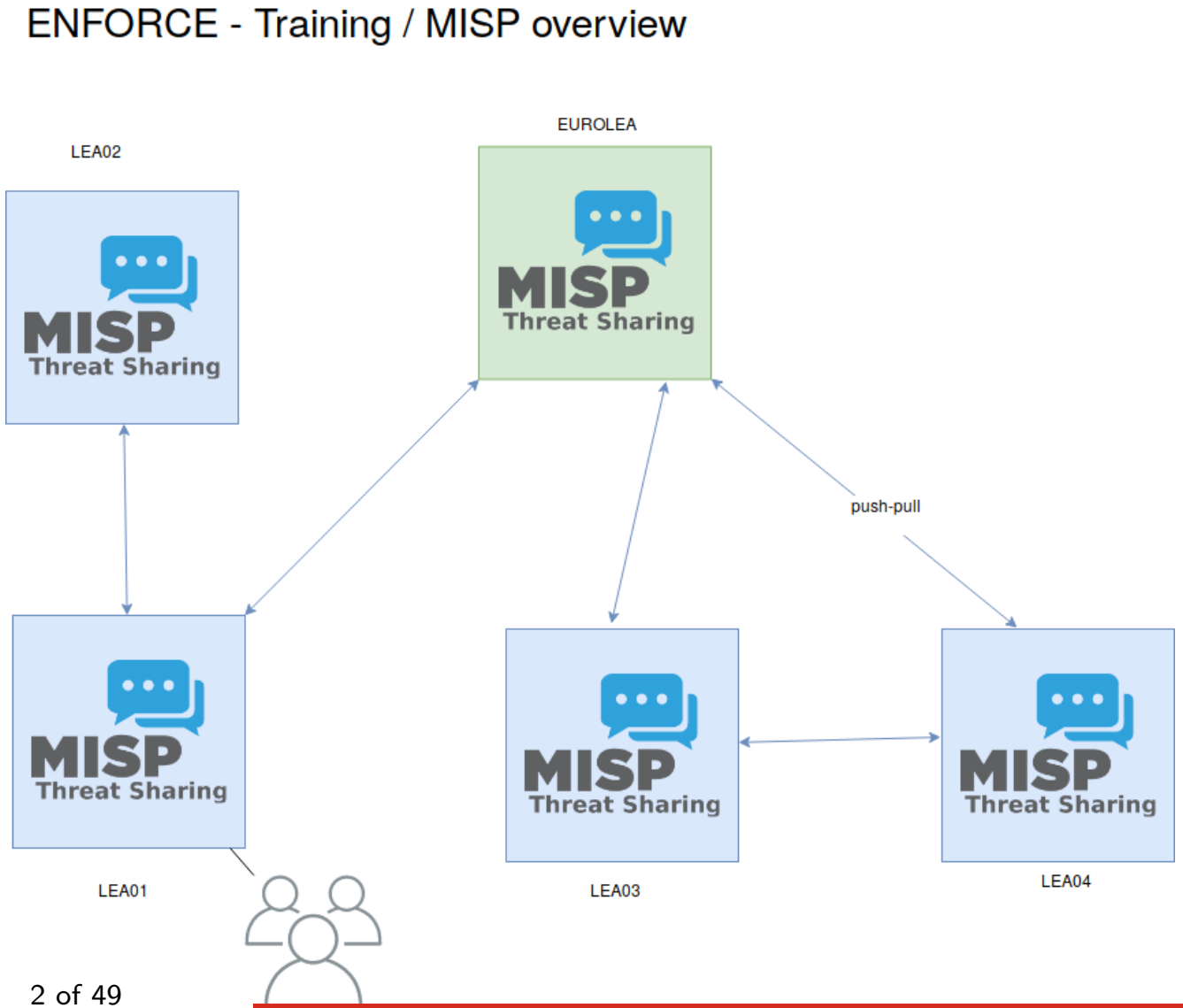
CIRCL
Computer Incident
Response Center
Luxembourg

Alexandre Dulaunoy CIRCL -
TLP:WHITE

Team CIRCL

November 27, 2019

Enforce information sharing overview



Workshop details

- 48 pcaps (2 days) are distributed (TLP:GREEN) from two blackhole networks (193.168.81.0/27 - 185.194.92.0/22)
- During the workshop, **each team can analyse the network capture without restriction** (any tools can be used) and **interesting discoveries can be shared** during the session (e.g. via MISP)
- Content of the network captures are unknown to CIRCL, the goal is to have an interactive session to share findings and techniques

Motivation and background

- IP darkspace or black hole is
  - **Routable non-used address space** of an ISP (Internet Service Provider),
  - incoming traffic is unidirectional
  - and **unsolicited**.
- Is there any traffic in those darkspaces?
- If yes, what and why does it arrive there?
  - And **on purpose** or **by mischance**?
- What's the security impact?
- What are the security recommendations? How can we use the information to improve traffic analysis?
- Terminology: Honeypot versus darkspace

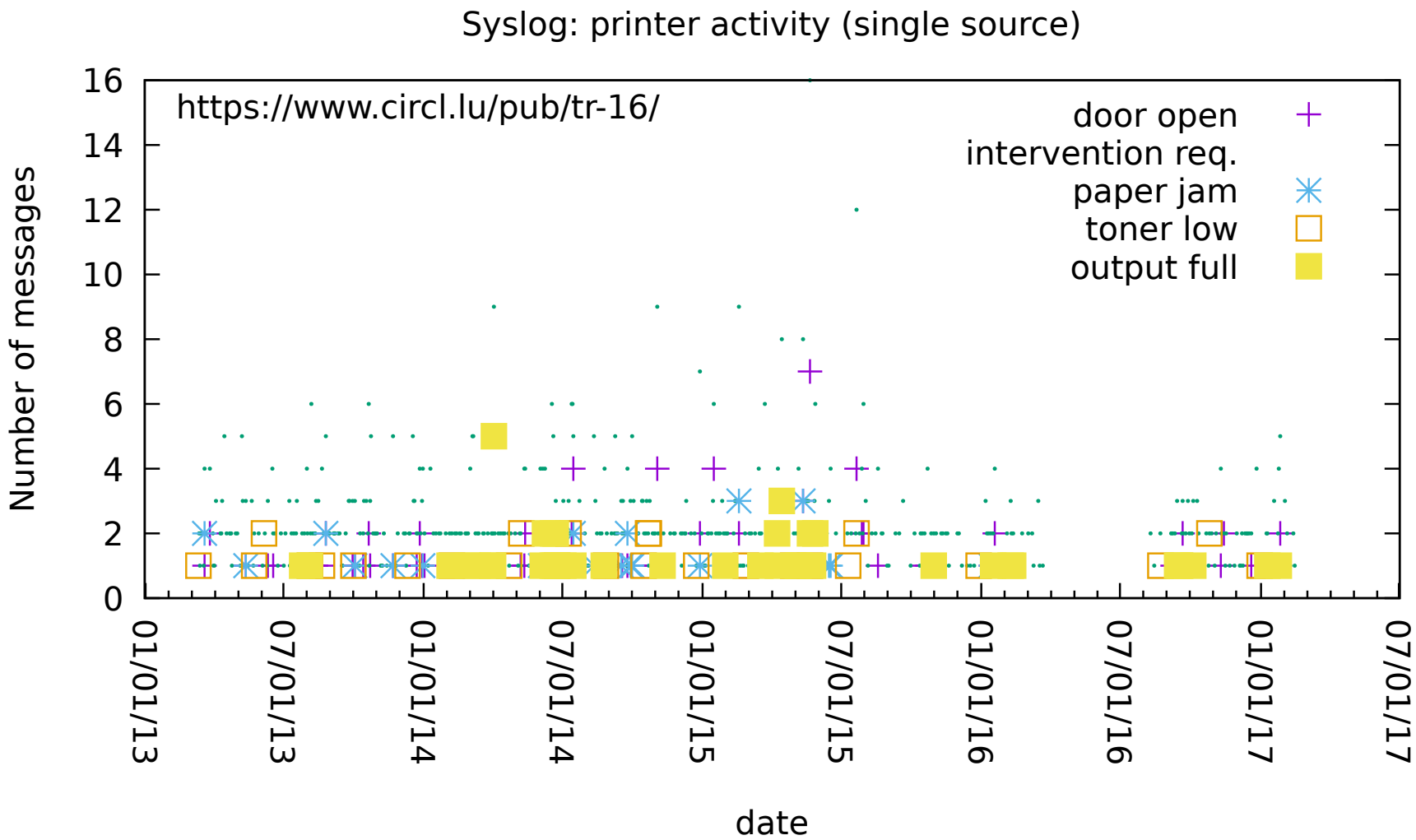
4 years in the life of a printer

from a series of packets hitting our darkspace

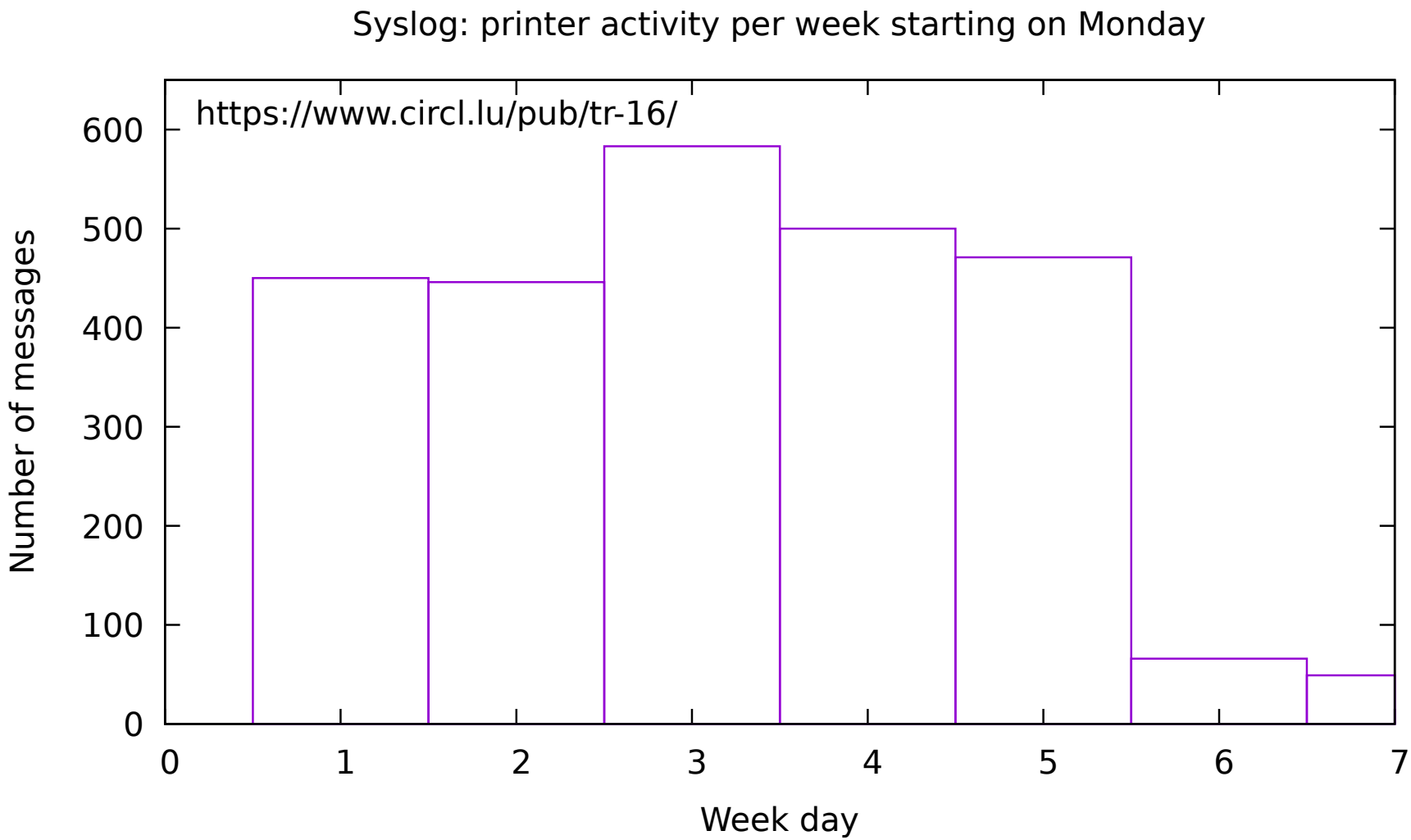
Printer sending syslog to the IP darkspace

```
2014-03-12 18:00:42
   SYSLOG lpr.error printer: offline
     or intervention needed
2014-03-23 21:51:24.985290
   SYSLOG lpr.error printer: paper out
   ...
2014-08-06 19:14:57.248337
   SYSLOG lpr.error printer: paper jam
```

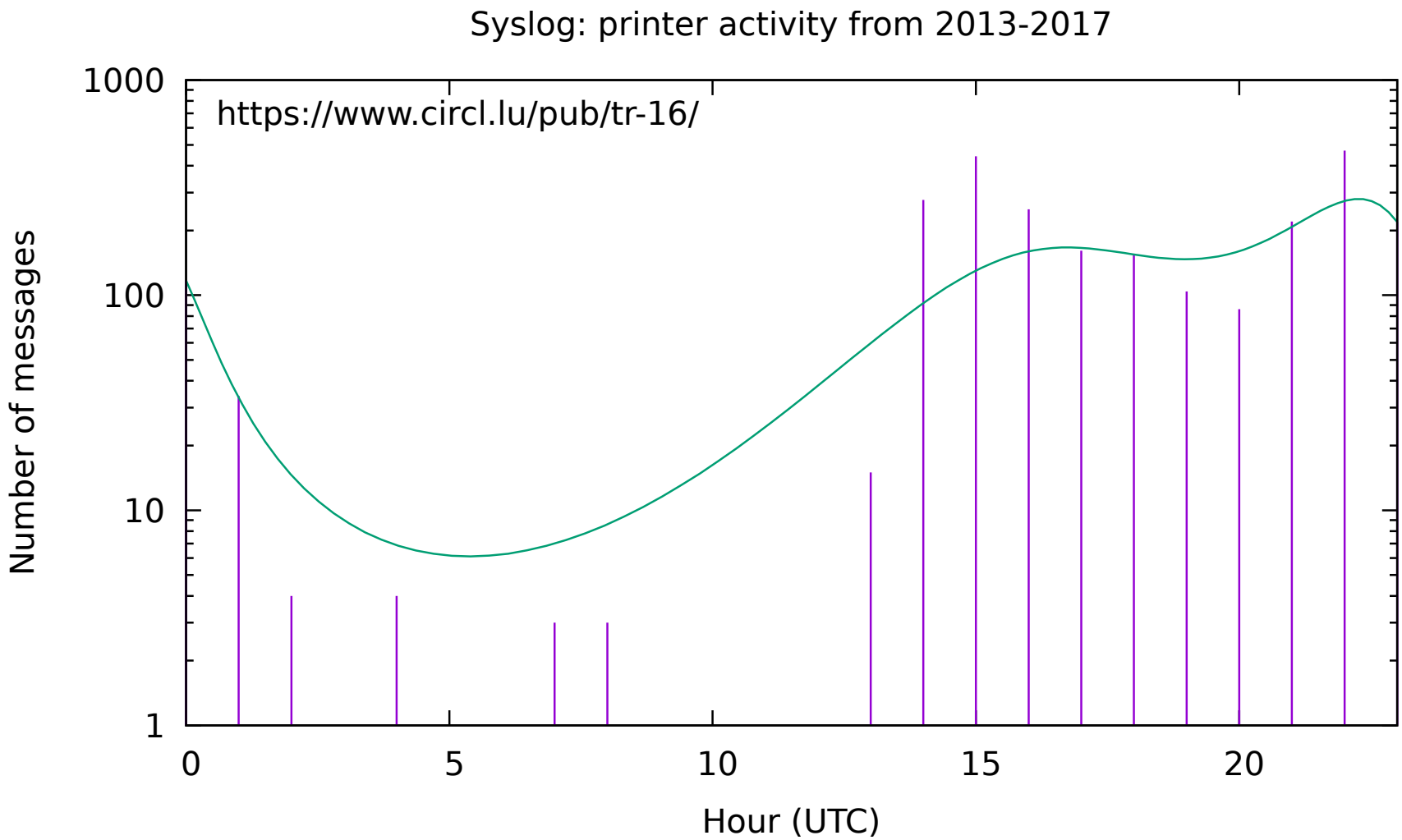
4 years in the life of a printer



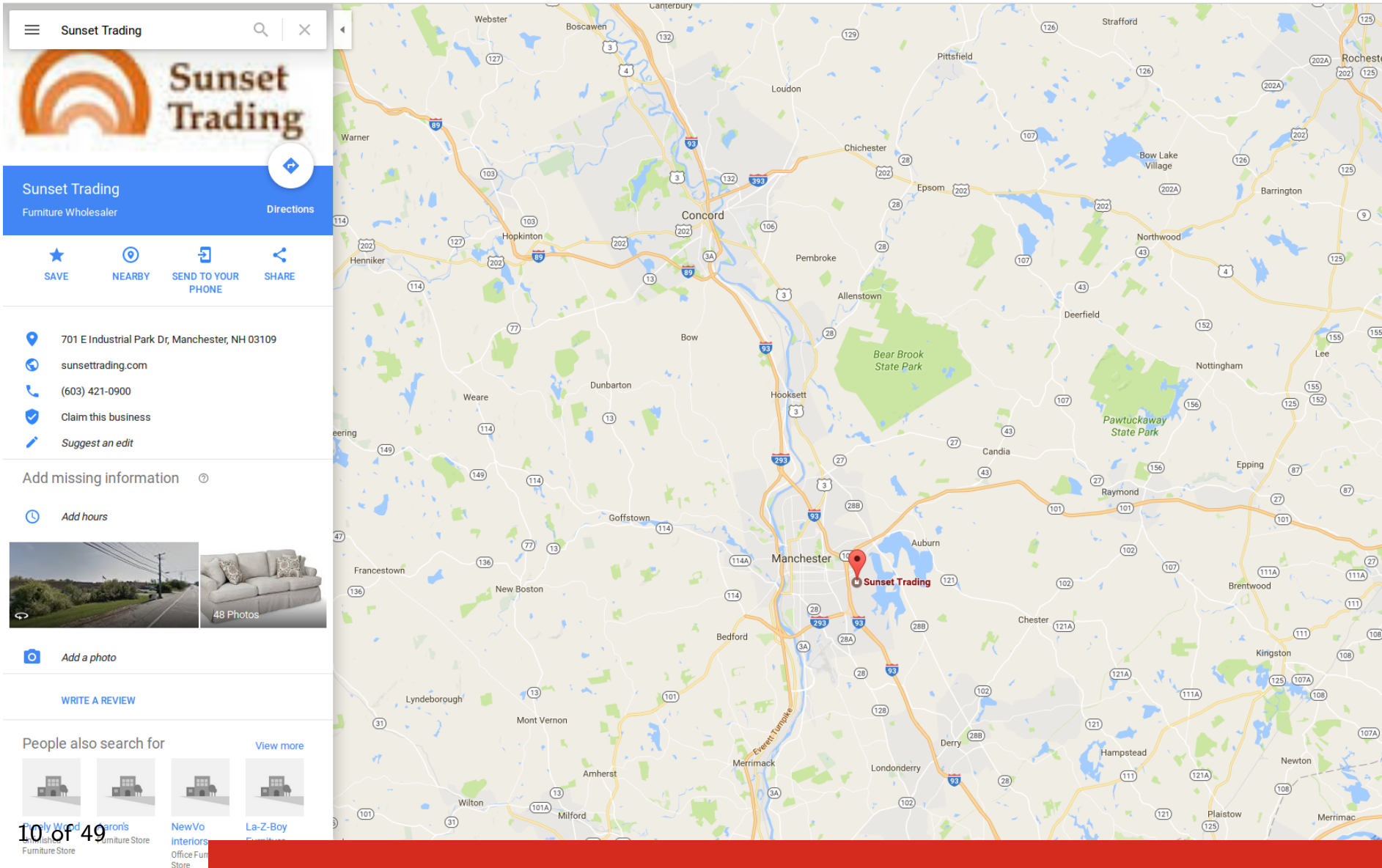
Business days based on the printer activity



Printer activity and business hours



Where is the printer?



Origin of traffic in the black hole

- Attackers (and researchers) scan networks to find vulnerable systems (e.g. SSH brute-force)
- Backscatter traffic (e.g. from spoofed DoS)
- Self-replicating code using network as a vector (e.g. conficker, residual worms)
- Badly configured devices especially embedded devices (e.g. printers, server, routers)
  - $\rightarrow$ **Our IP darkspace is especially suited for spelling errors from the RFC1918 (private networks) address space**

Why is there traffic

Typing/Spelling errors with RFC1918 networks

- While typing an IP address, different error categories might emerge:

Hit wrong key	19**2**.x.z.y →	19**3**.x.y.z
	172.x.y.z	1**5**2.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

Research activities related to spelling errors

Spelling errors apply to text but also network configuration

- 34% omissions of 1 character
  - Example: Network $\rightarrow$ Netork
- 23% of all errors happen on 3rd position of a word
  - Example: Text $\rightarrow$ Test)
- 94% spellings errors are single errors in word
  - And do not reappear

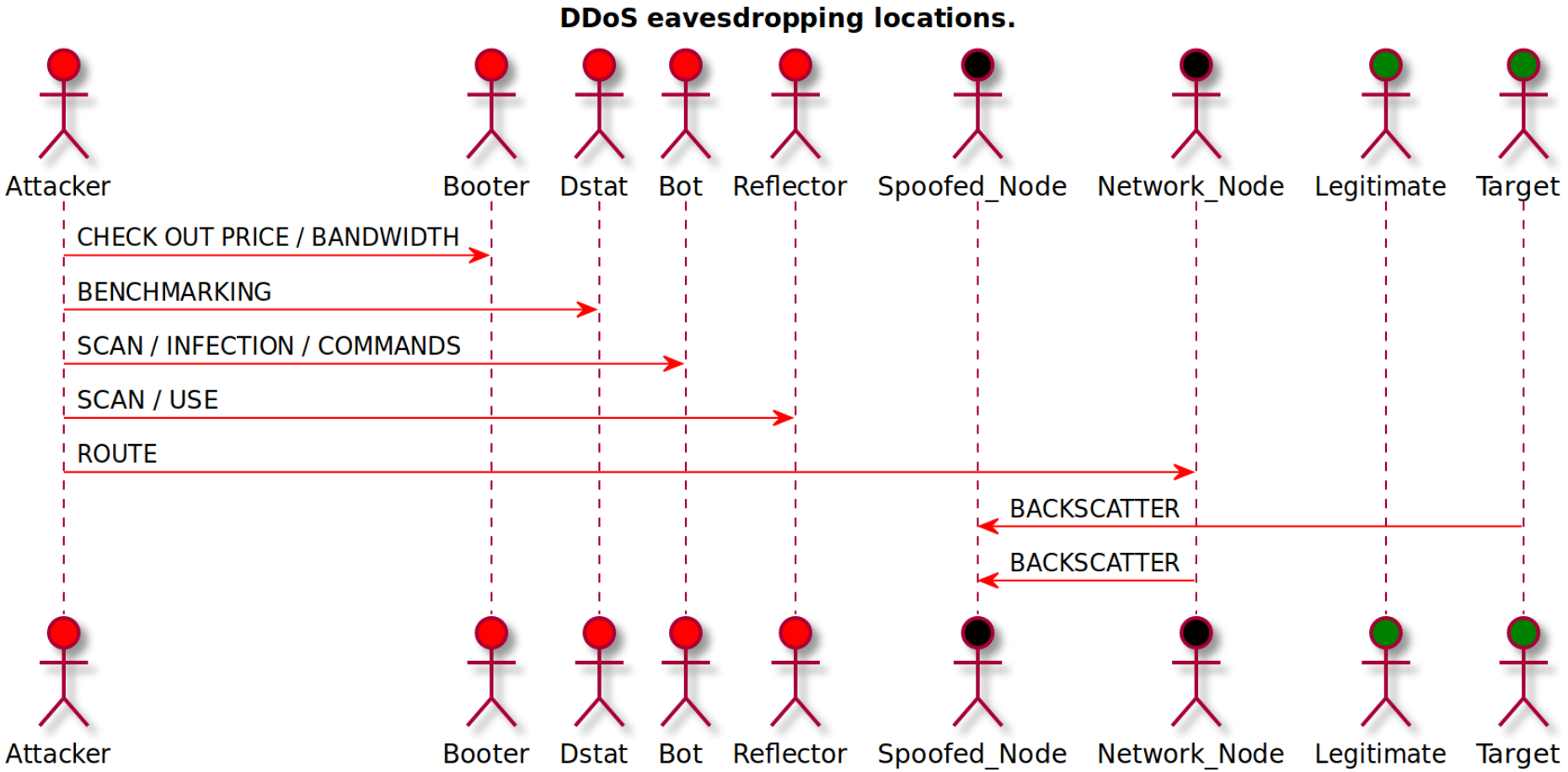
References

- Pollock J. J. and Zamora A., Collection and characterization of spelling errors in scientific and scholarly text. J. Amer. Soc. Inf. Sci. 34, 1, 51 58, 1983.
- Kukich K., Techniques for automatically correcting words in text. ACM Comput. Surv. 24, 4, 377-439, 1992.

backscatter traffic

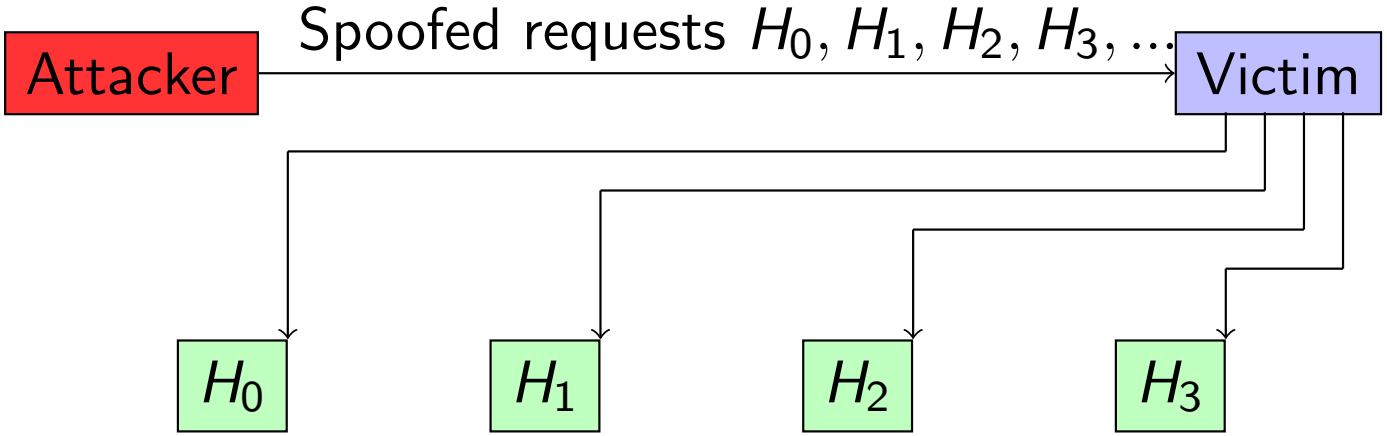
why DDoS victims are not always silent

DDoS overview



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

How does backscatter look like?

```
2017-09-16 10:02:22.807286 IP x.45.177.71.80 > x.x
    .105.167.39468: Flags [.], ack 1562196897, win
    16384, length 0
2017-09-16 10:02:27.514922 IP x.45.177.71.80 > x.x
    .121.213.62562: Flags [.], ack 14588990, win 16384,
    length 0
2017-09-16 10:02:28.024516 IP x.45.177.71.80 > x.x
    .100.72.30395: Flags [.], ack 24579479, win 16384,
    length 0
2017-09-16 10:02:30.356876 IP x.45.177.71.80 > x.x
    .65.254.17754: Flags [.], ack 318490736, win 16384,
    length 0
```

What are the typical characteristics?

Is it DDoS backscatter traffic?

Problem

- Distinguish between compromised infrastructure and backscatter
- Look at TCP flags $\rightarrow$ filter out single SYN flags
- Focus on ACK, SYN/ACK, RST...
- Do not limit to SYN/ACK or ACK $\rightarrow$ ECE (ECN Echo)/CWR[1]

```
tshark -n -r capture-20170916110006.cap.gz -T fields -e
    frame.time_epoch -e ip.src -e tcp.flags
1505552542.807286000 x.45.177.71 0x00000010
1505552547.514922000 x.45.177.71 0x00000010
```

[1] https://tools.ietf.org/html/rfc3168

What can be derived from backscatter traffic?

- **External point of view** on ongoing denial of service attacks
- Confirm if there is a DDoS attack
- Recover time line of attacked targets
- Review targeted services (DNS, webserver, ...)
- Infrastructure changes (e.g. change of routing)
- Assess the state of an infrastructure under denial of service attack
  - Detect failure/addition of intermediate network equipments, firewalls, proxy servers etc
  - Detect DDoS mitigation devices
- Tools, Techniques and Tactics[2] used by the attackers

[2] https://www.misp-project.org/taxonomies.html#_ddos_2

Getting DDoS attack information or validation

Example nationalcrimeagency.gov.uk

UK's National Crime Agency hit by DDoS attack, following LizardStresser arrests

Last week, users of Lizard Squad's DDoS-on-demand service were feeling the heat after arrests were made by UK police. This week, it's the UK's National Crime Agency which has found itself the victim of a denial-of-service attack.

Graham Cluley 1 Sep 2015 - 02:01PM

Getting additional information

Example nationalcrimeagency.gov.uk

- Gather potential IP addresses (via DNS or Passive DNS)
- Check all records type (A, AAAA, MX, CNAME)

```
nslookup nationalcrimeagency.gov.uk

Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   nationalcrimeagency.gov.uk
Address: 194.61.183.46
```

Getting additional information on DDoS attacks

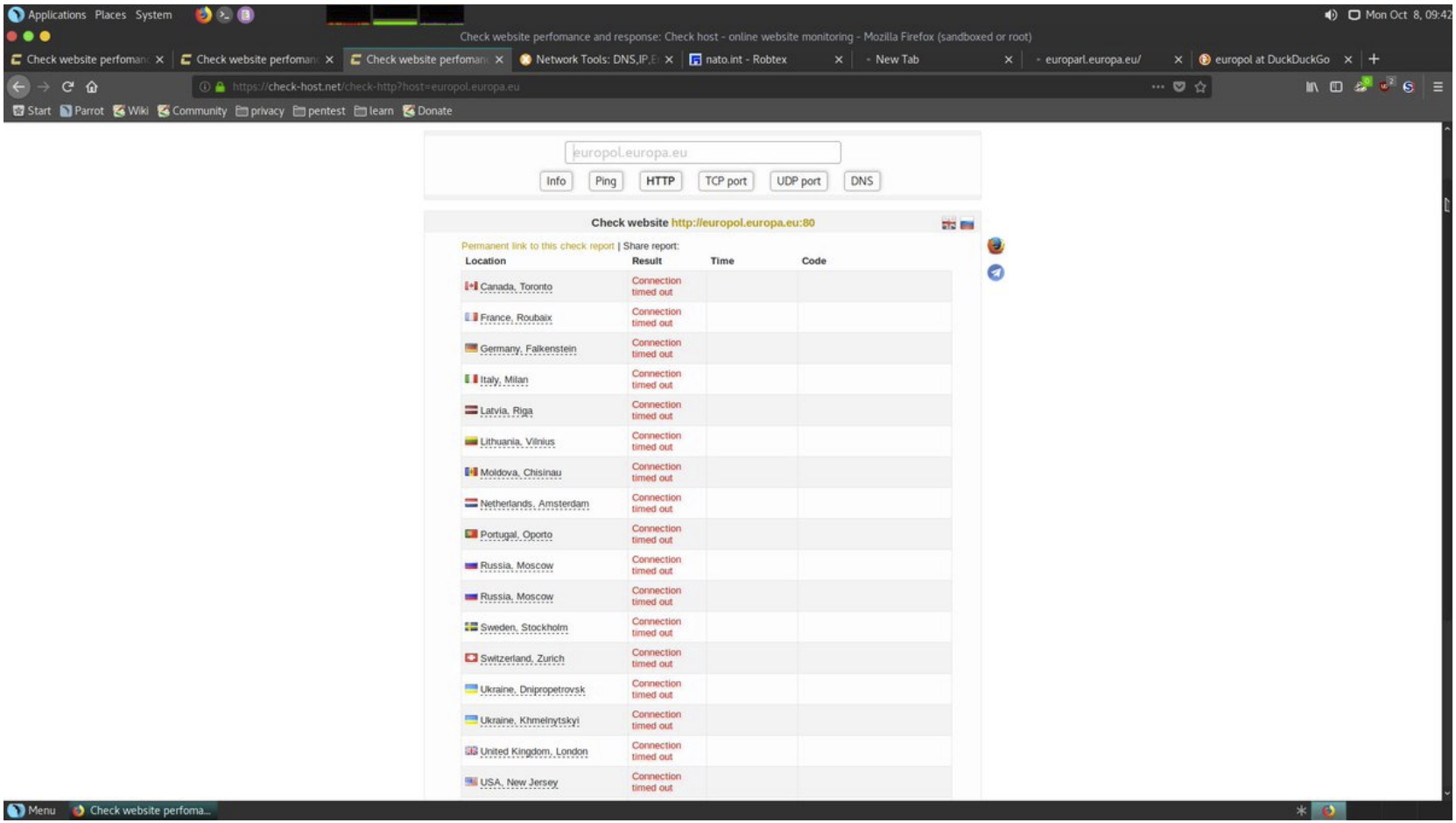
Example nationalcrimeagency.gov.uk

```
find files/2015/08/28/ -type f | parallel -j 7 '
    tcpdump -n -r {1} "host 194.61.183.46"'

17:10:06.857475 IP 194.61.183.46.80 > x.x.109.194.17293
   Flags [S.], seq 1635851834, ack 1801912321, win 0, length 0
17:10:14.869661 IP 194.61.183.46.80 > x.x.109.73.58142:
   Flags [S.EW], seq 1066513712, ack 4190371841, win 0, length 0
17:10:14.881036 IP 194.61.183.46.80 > x.x.111.106.49231:
   Flags [S.EW], seq 1531124927, ack 252116993, win 0, length 0
17:10:15.186684 IP 194.61.183.46.80 > x.x.102.45.62535:
   Flags [S.EW], seq 486934691, ack 536346625, win 0, length 0
17:10:18.946674 IP 194.61.183.46.80 > x.x.67.46.62399:
   Flags [S.EW], seq 234597292, ack 4069785601, win 0, length 0
```

Dealing with DDoS claims

Screenshots from the attacker are valuable information



Dealing with DDoS claims

Screenshots from the potential attacker are valuable information

- If some operational security is done
  - Hide displayed hints (i.e. user name, IP address, country)
- Local time
- Used operating system
- Used browser
- Used browser plugins
- Bookmarks
- Open other tabs
- Configured search engines
- Some cases images contains meta data such as exif
- **Validating the claims** against DDoS backscatter

DDoS backscatter limitation or drawbacks

- Visibility limited by the spoofed networks from the DDoS attackers
- The size of the network telescope
- The state of the network infrastructure from the victims (e.g. how long the infrastructure is active)
- If the conditions are there, **only a subset of the returned packets will be received**

How to write a Gartner market survey?

What are the most common antivirus software?

by using the DNS queries hitting your darkspace

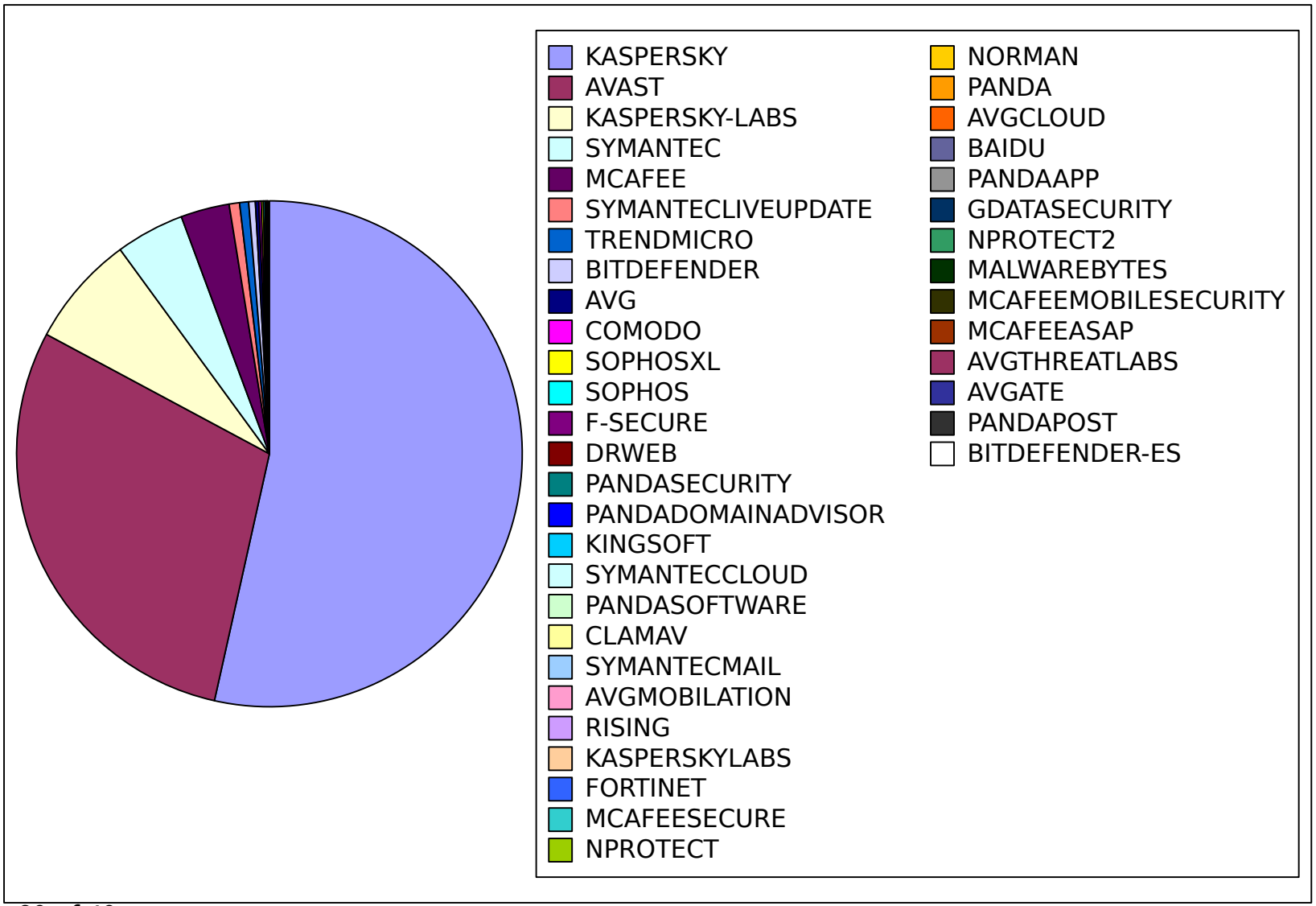
Sample subset of DNS queries towards antivirus vendors domains

```
1 0.0.0.16a8.20ae.2f4a.400.7d.igkhab8lsrnzhj726ngu8gbsev.
      avqs.mcafee.com A INET 127.161.0.128
2 0.0.0.16a8.20ae.2f4a.400.7d.sdszgsg5a6j516p9nui9jfz5mj.
      avqs.mcafee.com A INET 127.161.0.128
3 40.ucp-ntfy.kaspersky-labs.com
4 46.ucp-ntfy.kaspersky-labs.com
5 6.ucp-ntfy.kaspersky-labs.com
6 dnl-06.geo.kaspersky.com.<COMPANYNAME>.local
7 shasta-mr-clean.symantec.com
8 shasta-mrs.symantec.com
9 shasta-nco-stats.symantec.com
```

Scripting your statistics for antivirus installations

- Extract **a list of words** from VirusTotal (antivirus products supported)
- Match the DNS queries with extracted words (e.g. be careful with fake antivirus)
- **Filter per source IP address** (or aggregated subnets) to limit the result per organisation
- Plot the number of hits per aggregated words using in a single antivirus product name

A/V Statistics from Misconfigured Resolvers



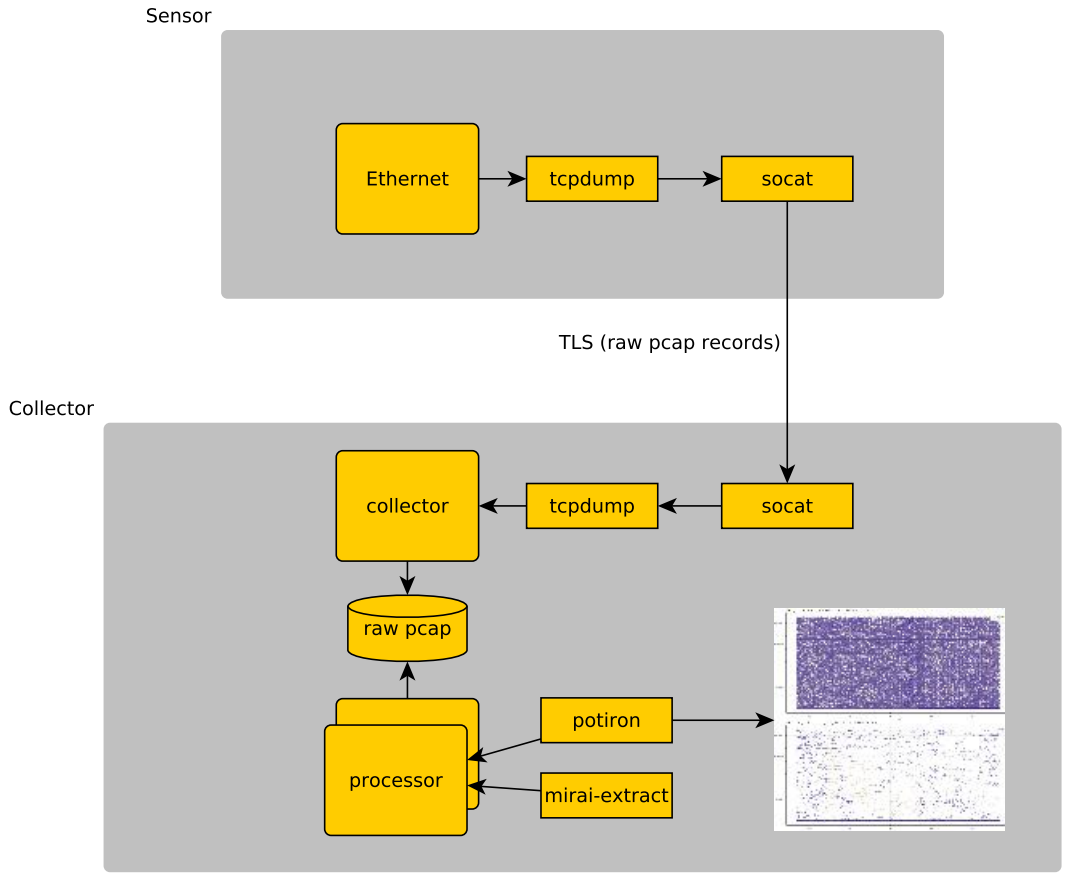
How do we collect all this crap?

---

by listening to the void

Collection and Analysis Framework

Collection and Analysis Framework



Collection and Analysis Framework

or to keep the collection as simple as possible

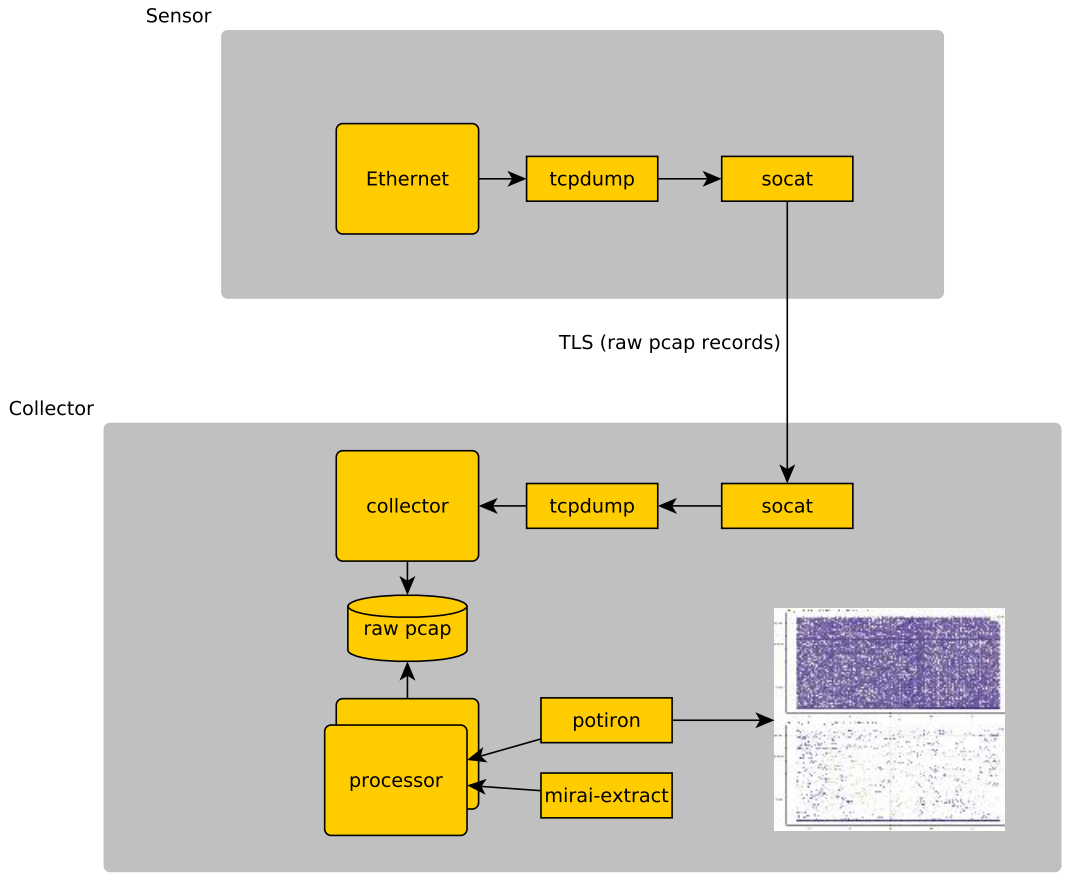
- Minimal sensor collecting IP-Darkspace networks (**close to RFC1918 address space**)
- Raw pcap are captured with the full payload
- Netbeacon[3] developed to ensure consistent packet capture
- Potiron[4] to normalize, index, enrich and visualize packet capture

[3] `https://github.com/adulau/netbeacon/`

[4] `https://github.com/CIRCL/potiron`

Blackhole & honeypot operation

Collection and analysis framework



Blackhole operation

Definition (Principle)

- KISS (Keep it simple stupid)
- Linux & OpenBSD operating systems

Sensor

```
tcpdump -l -s 65535 -n -i vr0 -w - '( not port $PORT
    and not host $HOST )' | socat - OPENSSL-CONNECT:
    $COLLECTOR:$PORT,cert=/etc/openssl/client.pem,cafile
    =/etc/openssl/ca.crt,verify=1
```

Dataset collected and statistics on one single blackhole

- From 2012-03-12 until Today (still active)
- More than 700 gigabytes of compressed raw pcap collected
- Constant stream of packets from two /22 network blocks
  - no day/night profile.
- Some peaks at 800kbit/s (e.g. often TCP RST from backscatter traffic but also from typographic errors)

General observations

- A large part of traffic is coming from badly configured devices (**RFC1918 spelling errors**)
  - Printers, embedded devices, routers or even server.
  - Trying to do name resolution on non-existing DNS servers, NTP or sending syslog messages.
- Even if the black hole is passive, payload of stateless UDP packets or even TCP (due to asymmetric routing on misspelled network) datagrams are present
- Internal network scanning and reconnaissance tool (e.g. internal network enumerationi)
- The recursive effect of statistics (e.g. nmap-services)

Observation per AS

Traffic seen in the darknet

N	Frequency	ASN
1	4596319	4134
2	1382960	4837
3	367515	3462
4	312984	4766
5	211468	4812
6	166110	9394
7	156303	9121
8	153585	4808
9	135811	9318
10	116105	4788

- Occurrences of activities related to the proportion of hosts in a country
- The Great Firewall of China is **not filtering leaked packets**
- Corporate AS number versus ISP/Telco AS number

How to build your "next" network reconnaissance tools?

---

by listening to the void

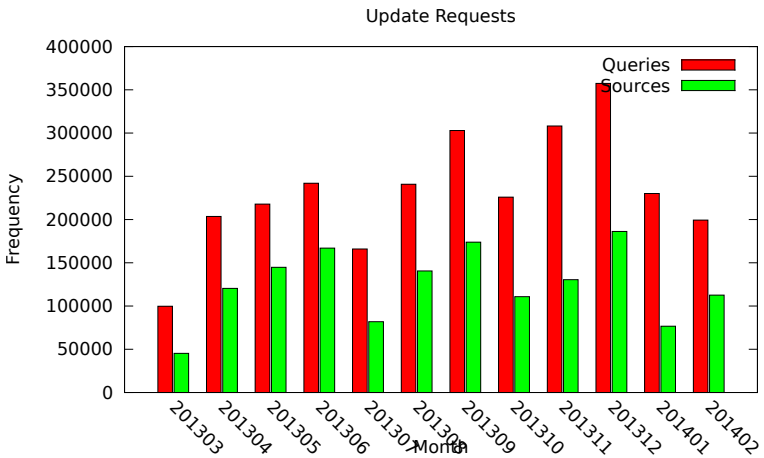
Network reconnaissance (and potential misuse): DNS

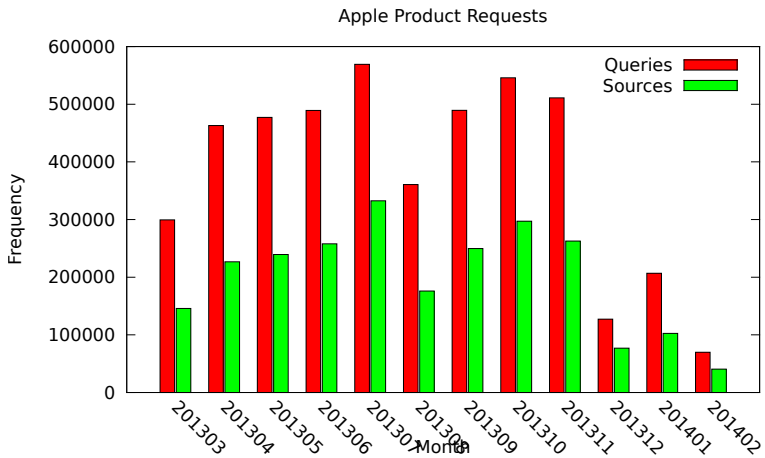
```
1 3684 _msdcs.<companyname>.local
2 1232666 time.euro.apple.com
3 104 time.euro.apple.com.<mylocaldomain>
4 122 ocsp.tcs.terena.org
5 50000+ ocsp.<variousCA>
```

- DNS queries to an incorrect nameserver could lead to major misuse
- **A single typographic error in a list of 3 nameservers is usually unnoticed**

Software Updates/Queries from Misconfigured Resolvers

- Discovering software usage (and vulnerabilities) can be easily done with passive reconnaissance
- Are the software update process ensuring the integrity of the updates?





Network Reconnaissance - A source for your smart DNS Brute-Forcer

ASTTF.NET	HELP.163.COM	
ASUEGYI.INFO	HP_CLIENT1	
ASUS1025C	MACBOOKAIR-CAD7	
DEFAULT	MACBOOK-B5BA66	
DELICIOUS.COM	MACBOOKPRO-5357	
DELL	MAIL.AFT20.COM	And many more ...
DELL1400	S3.QHIMG.COM	
DELL335873	SERVERWEB	
DELL7777	SERVEUR	
DELL-PC	SERVICE.QQ.COM	
DELLPOP3	SMTP.163.COM	

Building your DNS brute-forcer

- Smart DNS Brute-Forcer[5][6] uses techniques from natural language modeling with Markov Chain Models
- The processor relies on passive DNS data to generate the statistics and extract the features.
- The DNS queries seen in the **IP darkspace can be considered as a passive DNS stream** with a focus on internal network.
- Providing a unique way to create **internal DNS brute-forcers from external observations**.

[5] `https://www.foo.be/papers/sdbf.pdf`

[6] `https://github.com/jfrancois/SDBF`

Network Reconnaissance: NetBios Machine Types (1 week)

23	Browser Server
4	Client?
1	Client? M <ACTIVE>
21	Domain Controller
1	Domain Controller M <ACTIVE>
11	Master Browser
1	NameType=0x00 Workstation
1	NameType=0x20 Server
105	Server
26	Unknown
1	Unknown <GROUP> B <ACTIVE>
5	Unknown <GROUP> M <ACTIVE>
1322	Workstation
1	Workstation M <ACTIVE>

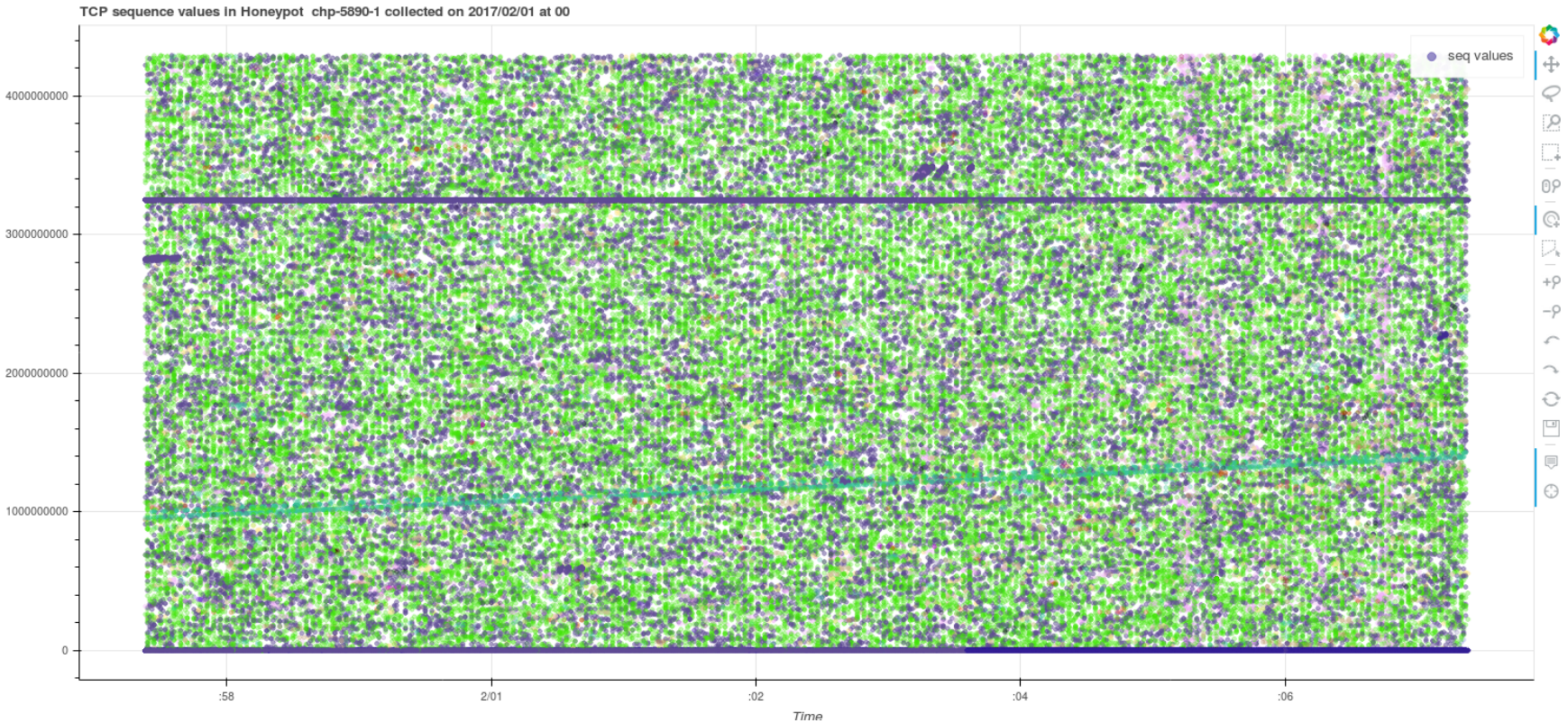
How to configure your router (without security)

Enable command logging and send the logs to a random syslog server

```
Aug 13 10:11:51 M6000-G5 command-log:[10:11:51 08-13-2012
  VtyNo: vty1  UserName: XXX IP: XXX ReturnCode: 1
  CMDLine: show subscriber interface gei-0/2/1/12.60
Aug 13 10:46:05 M6000-G5 command-log:[10:46:05 08-13-2012
  VtyNo: vty2  UserName: XXX IP: XXX  ReturnCode: 1
  CMDLine: conf t ]
Aug 13 10:46:10 M6000-G5 command-log:[10:46:10 08-13-2012
  VtyNo: vty2  UserName: XXX IP: XXX  ReturnCode: 1  CMD
Line: aaa-authentication-template 1100 ]
...
```

We will let you guess the sensitive part afterwards...

Finding origin of traffic by TCP sequence analysis



```
211                 iph->id = rand_next();
212                 iph->saddr = LOCAL_ADDR;
213                 iph->daddr = get_random_ip();
214                 iph->check = 0;
215                 iph->check = checksum_generic((uint16_t *)iph, sizeof (struct iphdr));
216
217                 if (i % 10 == 0)
218                 {
219                     tcph->dest = htons(2323);
220                 }
221                 else
222                 {
223                     tcph->dest = htons(23);
224                 }
225                 tcph->seq = iph->daddr;
226                 tcph->check = 0;
227                 tcph->check = checksum_tcpudp(iph, tcph, htons(sizeof (struct tcphdr)), sizeof (struct tcphdr));
228
229                 paddr.sin_family = AF_INET;
230                 paddr.sin_addr.s_addr = iph->daddr;
231                 paddr.sin_port = tcph->dest;
232
233                 sendto(rsck, scanner_rawpkt, sizeof (scanner_rawpkt), MSG_NOSIGNAL, (struct sockaddr *)&paddr, sizeof
234             }
```

Recommendations for operating an IP darkspace

- **Capture raw packets at the closest point**, don't filter, don't try to be clever, just store it as it.
- **Test your network collection mechanisms** and storage. Send test network beacons. Check the integrity, order and completness of packets received.
- You never know in advance which features is required to distinguish a specific pattern.
- Did I mention to store **RAW PACKETS**?

Security conclusions

- Security recommendations
  - **Default routing/NAT to Internet in operational network is evil**
  - Use fully qualified domain names (resolver search list is evil too)
  - Double check syslog exports via UDP (e.g. information leakage is easy)
  - Verify any default configuration with SNMP (e.g. enable by default on some embedded devices)
- Offensive usage? What does it happen if a malicious "ISP" responds to misspelled RFC1918 addresses? (e.g. DNS/NTP requests, software update or proxy request)
- Some research projects on this topic? Contact us `mailto:info@circl.lu`

IP darkspace and LE conclusions

- **IP darkspace can be a complementary source of intelligence**
- Many network telescope are operated by researchers and have different way to collect network packets and provide access
- CIRCL recently started the D4 project[7], to provide an unified way to collect network packets from distributed IP darkspaces and provide unified access to contributors
- Some IP darkspace are more interesting than others depending of the case investigated (e.g. DDoS tooling always spoofing specific network spaces, networks addresses similar to RFC1918)

[7] https://www.d4-project.org/