How to benefit from DDOS ecosystem

The D4 project

CIRCL
Computer Incident
Response Center
Luxembourg

Gérard Wagener
TLP:GREEN

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

November 13, 2018

Co-financed by the European Union
Connecting Europe Facility

How to use our tools and databases in case of DDOS

Part 1 - DDOS threat evaluation

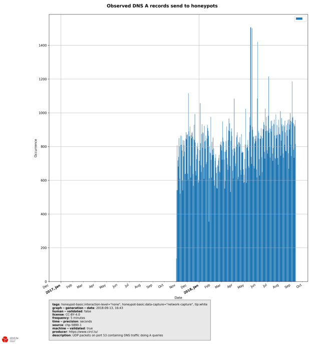
The accidental denial of service

Denial of services not triggered by an attacker

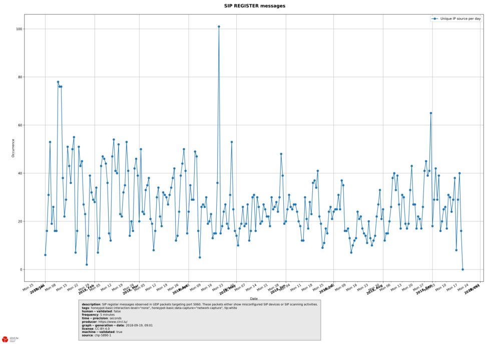
- Configuration errors in DNS, PABX, proxies, ...
- Asymmetric routing
- IP conflicts
- Never experienced software / hardware side effects
  - Experienced often after equipment replacement
  - Full state table management of firewalls
  - Load balancing edge cases
  - Interception proxies
  - Untested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

The accidental denial of service

Configuration errors are quickly done



tags: honeypot-basic:interaction-level="none", honeypot-basic:data-capture="network-capture", tlp:white
graph − generation − date: 2018-09-13, 16:43
human − validated: false
license: CC-BY-4.0
frequency: 5 minutes
time − precision: seconds
source: chp-5890-1
machine − validated: true
producer: https://www.circl.lu/
description: UDP packets on port 53 containing DNS traffic doing A queries



description: SIP register messages observed in UDP packets targeting port 5060. These packets either show misconfigured SIP devices or SIP scanning activities.
tags: honeypot-basic:interaction-level="none", honeypot-basic:data-capture="network-capture", tlp:white
human − validated: false
frequency: 5 minutes
time − precision: seconds
producer: https://www.circl.lu/
graph − generation − date: 2018-09-19, 09:01
license: CC-BY-4.0
machine − validated: true
source: chp-5890-1

`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

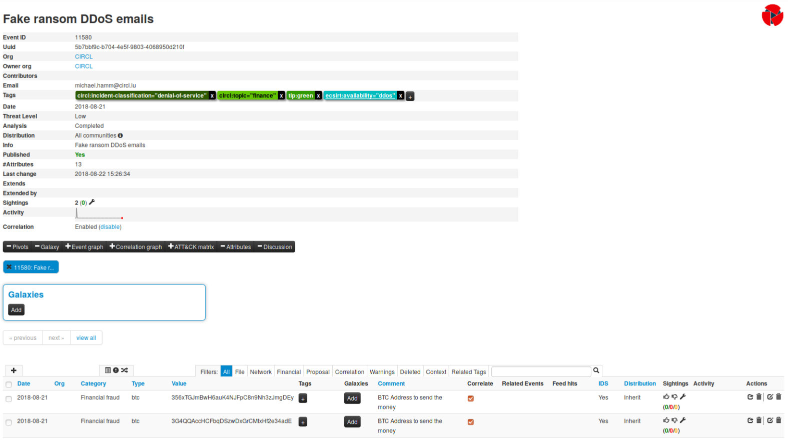
Search information on the attacker

- 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



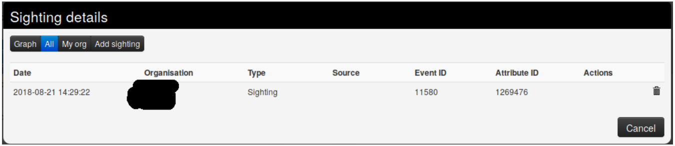
Fake ransom DDoS emails

Event ID	11580
Uuid	5b7bbf9c-b704-4e5f-9803-4068950d210f
Org	CIRCL
Owner org	CIRCL
Contributors	
Email	michael.hamm@circl.lu
Tags	circl:incident-classification="denial-of-service" x circl:topic="finance" x tlp:green x ecsirt:availability="ddos" x +
Date	2018-08-21
Threat Level	Low
Analysis	Completed
Distribution	All communities
Info	Fake ransom DDoS emails
Published	Yes
#Attributes	13
Last change	2018-08-22 15:26:34
Extends	
Extended by	
Sightings	2 (0)
Activity	
Correlation	Enabled (disable)

□	Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
□	2018-08-21		Financial fraud	btc	356xTGJmBwH6auK4NJFpC8n9Nh3zJmgDEy	+	Add	BTC Address to send the money	☑			Yes	Inherit	(0/0/0)		
□	2018-08-21		Financial fraud	btc	3G4QQAccHCFbqDSzwDxGrCMtxHf2e34adE	+	Add	BTC Address to send the money	☑			Yes	Inherit	(0/0/0)		

Is the event known?

MISP sightings



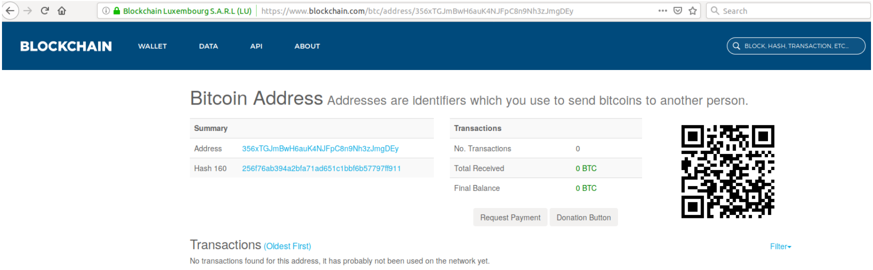
Sighting details

Date	Organisation	Type	Source	Event ID	Attribute ID	Actions
2018-08-21 14:29:22	[redacted]	Sighting		11580	1269476	🗑

Did other organizations saw some attributes?

Is the event known?

Did others paid



Blockchain Luxembourg S.A.R.L (LU)
https://www.blockchain.com/btc/address/356xTGJmBwH6auK4NJFpC8n9Nh3zJmgDEy
Search
BLOCKCHAIN
WALLET
DATA
API
ABOUT
BLOCK, HASH, TRANSACTION, ETC...

Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	356xTGJmBwH6auK4NJFpC8n9Nh3zJmgDEy
Hash 160	256f76ab394a2bfa71ad651c1bbf6b57797ff911

Transactions	
No. Transactions	0
Total Received	0 BTC
Final Balance	0 BTC

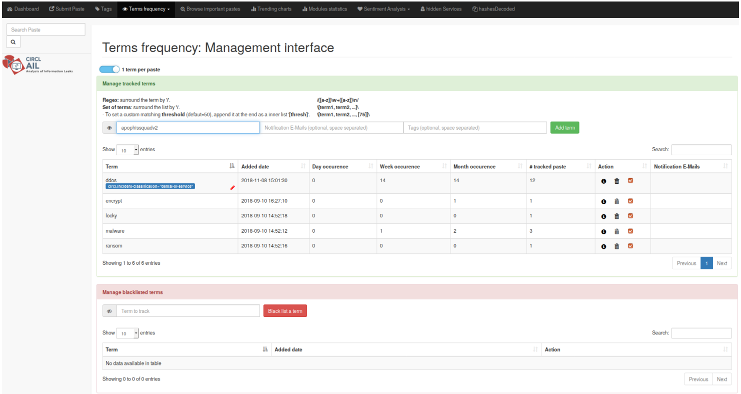
Request Payment
Donation Button

Transactions (Oldest First)

No transactions found for this address, it has probably not been used on the network yet.

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

Monitoring future publications in AIL



Terms frequency: Management interface

1 term per paste

Manage tracked terms

Regex: surround the term by '/'. /([a-z])\w+([a-z])\n/
Set of terms: surround the list by '\'. \[term1, term2, ...]\
- To set a custom matching **threshold** (defaut=50), append it at the end as a inner list '**[thresh]**'. \[term1, term2, ..., [75]]\

apophissquadv2

Notification E-Mails (optional, space separated)
Tags (optional, space separated)
Add term

Show 10 entries

Search:

Term	Added date	Day occurence	Week occurence	Month occurence	# tracked paste	Action	Notification E-Mails
ddos circl:incident-classification="denial-of-service"	2018-11-08 15:01:30	0	14	14	12		
encrypt	2018-09-10 16:27:10	0	0	1	1		
locky	2018-09-10 14:52:18	0	0	0	1		
malware	2018-09-10 14:52:12	0	1	2	3		
ransom	2018-09-10 14:52:16	0	0	0	1		

Showing 1 to 6 of 6 entries

Manage blacklisted terms

Show 10 entries

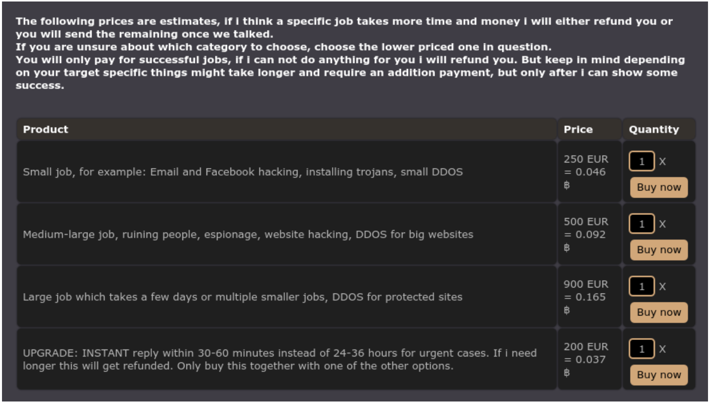
Search:

Term	Added date	Action
No data available in table		

Showing 0 to 0 of 0 entries

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

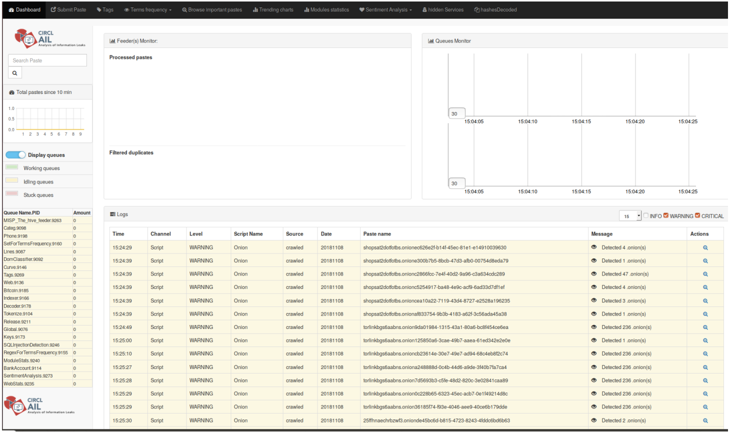
How serious do you take such services?

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 → differences
- Check threat sharing platforms to check .onion addresses

Crawl hidden services with AIL



Queue Name.PID	Amount
MISP_The_hive_feeder.9263	0
Categ.9098	0
Phone.9198	0
SetForTermsFrequency.9160	0
Lines.9087	0
DomClassifier.9092	0
Curve.9146	0
Tags.9269	0
Web.9136	0
Bitcoin.9185	0
Indexer.9166	0
Decoder.9178	0
Tokenize.9104	0
Release.9211	0
Global.9076	0
Keys.9173	0
SQLInjectionDetection.9246	0
RegexForTermsFrequency.9155	0
ModuleStats.9240	0
BankAccount.9114	0
SentimentAnalysis.9273	0
WebStats.9235	0

Time	Channel	Level	Script Name	Source	Date	Paste name	Message	Actions
15:24:29	Script	WARNING	Onion	crawled	20181108	shopsat2dotfotbs.onionec626e2f-b14f-45ec-81e1-e14910039630	Detected 4 .onion(s)	
15:24:39	Script	WARNING	Onion	crawled	20181108	shopsat2dotfotbs.onione300b7b5-8bcb-47d3-afb0-00754d8eda79	Detected 1 .onion(s)	
15:24:39	Script	WARNING	Onion	crawled	20181108	shopsat2dotfotbs.onionc2866fcc-7e4f-40d2-9a96-c3a634cdc289	Detected 47 .onion(s)	
15:24:39	Script	WARNING	Onion	crawled	20181108	shopsat2dotfotbs.onionc5254917-ba48-4e9c-acf9-6ad33d7df1ef	Detected 4 .onion(s)	
15:24:39	Script	WARNING	Onion	crawled	20181108	shopsat2dotfotbs.onioncea10a22-7119-43d4-8727-e2528a196235	Detected 3 .onion(s)	
15:24:39	Script	WARNING	Onion	crawled	20181108	shopsat2dotfotbs.onionaf833754-9b3b-4183-a62f-3c56ada45a38	Detected 1 .onion(s)	
15:24:49	Script	WARNING	Onion	crawled	20181108	torlinkbgs6aabns.onion9da01984-1315-43a1-80a6-bc8f454ce6ea	Detected 236 .onion(s)	
15:25:00	Script	WARNING	Onion	crawled	20181108	torlinkbgs6aabns.onion125850a6-3cae-49b7-aaea-61ed342e2e0e	Detected 1 .onion(s)	
15:25:10	Script	WARNING	Onion	crawled	20181108	torlinkbgs6aabns.onioncb23614e-30e7-49e7-ad94-68c4eb8f2c74	Detected 236 .onion(s)	
15:25:27	Script	WARNING	Onion	crawled	20181108	torlinkbgs6aabns.oniona248888d-0c4b-44d6-a9de-3f40b7fa7ca4	Detected 236 .onion(s)	
15:25:28	Script	WARNING	Onion	crawled	20181108	torlinkbgs6aabns.onion7d5693b3-c5fe-48d2-820c-3e02841caa89	Detected 236 .onion(s)	
15:25:29	Script	WARNING	Onion	crawled	20181108	torlinkbgs6aabns.onion0c228b65-6323-45ec-acb7-0e1f49214d8c	Detected 236 .onion(s)	
15:25:29	Script	WARNING	Onion	crawled	20181108	torlinkbgs6aabns.onion36185f74-f93e-4046-aee9-40ce6b179dde	Detected 236 .onion(s)	
15:25:30	Script	WARNING	Onion	crawled	20181108	25ffhnaechrbzwf3.oniondel45bc6d-b815-4723-8243-4fddc6bd6b63	Detected 2 .onion(s)	

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)

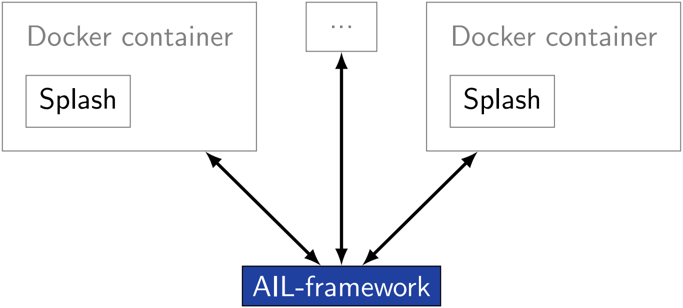
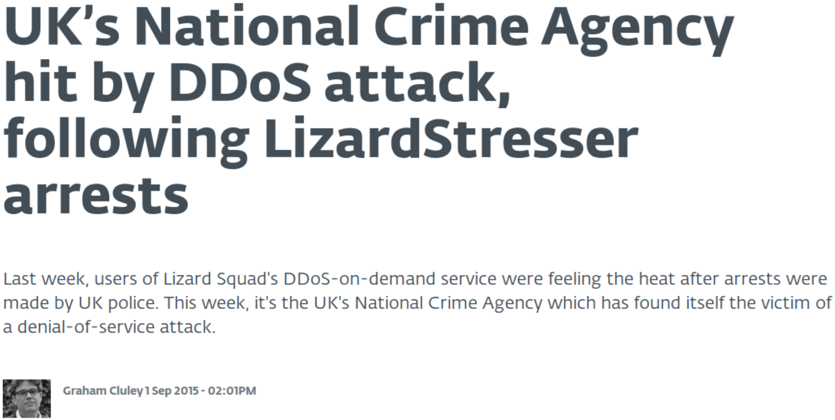


Figure: Architecture of AIL and its hidden services crawler

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

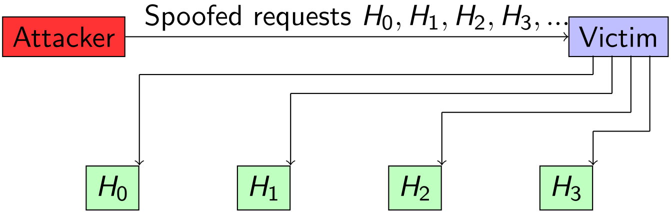
Example nationalcrimeagency.gov.uk

```
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

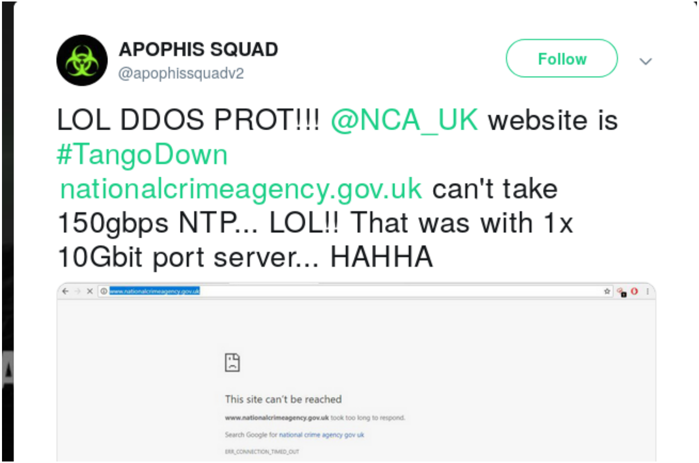


Connections
H_0
H_1
H_2
H_3

Fill up state connection state table of the victim

Dealing with DDOS claims

Other DDOS on nationalcrimeagency.gov.uk



APOPHIS SQUAD
@apophissquadv2

LOL DDOS PROT!!! @NCA_UK website is #TangoDown nationalcrimeagency.gov.uk can't take 150gbps NTP... LOL!! That was with 1x 10Gbit port server... HAHHA

www.nationalcrimeagency.gov.uk

This site can't be reached

www.nationalcrimeagency.gov.uk took too long to respond.

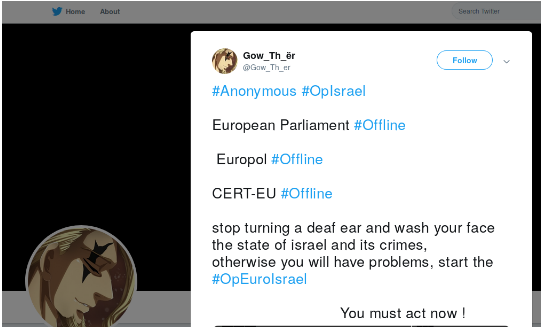
Search Google for national crime agency gov uk

ERR_CONNECTION_TIMED_OUT

How is the claim "proved"?

Dealing with DDOS claims

DDOS targeting European Parliament, Europol and cert.eu



Gow_Th_ër
@Gow_Th_er

#Anonymous #OpIsrael

European Parliament #Offline

Europol #Offline

CERT-EU #Offline

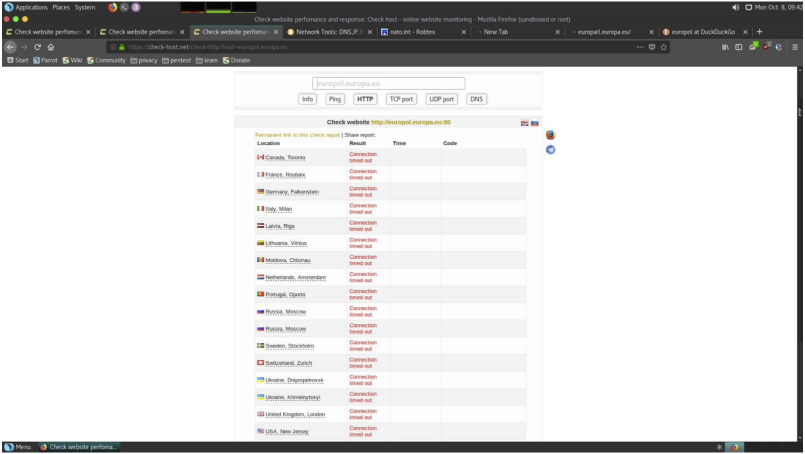
stop turning a deaf ear and wash your face the state of israel and its crimes, otherwise you will have problems, start the #OpEuroIsrael

You must act now !

How is the claim "proved"?

Dealing with DDOS claims

Screenshots from the attacker are valuable information



Applications Places System
Mon Oct 8, 09:42
Check website perfomance and response: Check host - online website monitoring - Mozilla Firefox (sandboxed or root)
Check website perfoman
Check website perfoman
Check website perfoman
Network Tools: DNS,IP,E
nato.int - Robtex
New Tab
europarl.europa.eu/
europol at DuckDuckGo
https://check-host.net/check-http?host=europol.europa.eu
Start Parrot Wiki Community privacy pentest learn Donate
europol.europa.eu
Info
Ping
HTTP
TCP port
UDP port
DNS
Menu
Check website perfoma...

Check website http://europol.europa.eu:80

Permanent link to this check report | Share report:

Location	Result	Time	Code
Canada, Toronto	Connection timed out		
France, Roubaix	Connection timed out		
Germany, Falkenstein	Connection timed out		
Italy, Milan	Connection timed out		
Latvia, Riga	Connection timed out		
Lithuania, Vilnius	Connection timed out		
Moldova, Chisinau	Connection timed out		
Netherlands, Amsterdam	Connection timed out		
Portugal, Oporto	Connection timed out		
Russia, Moscow	Connection timed out		
Russia, Moscow	Connection timed out		
Sweden, Stockholm	Connection timed out		
Switzerland, Zurich	Connection timed out		
Ukraine, Dnipropetrovsk	Connection timed out		
Ukraine, Khmelnytskyi	Connection timed out		
United Kingdom, London	Connection timed out		
USA, New Jersey	Connection timed out		

Dealing with DDOS claims

Screenshots from the attacker are valuable information

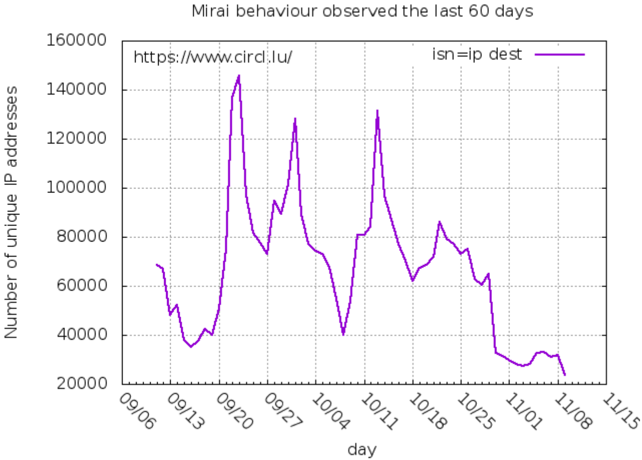
- If some operational security is done
  - Hide displayed hints (i.e. user name, IP address, country)
- Local time
- Used operating system
- Used browser
- Used browser plugins
- Bookmarks
- Open other tabs
- Configured search engines
- Some cases images contains meta data such as exif.
- ...

D4 project

- Raised from CIRCL research program
- Development of the DDoS detection platform
  - Deployment of distributed DOS detection devices on voluntary basis
- 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

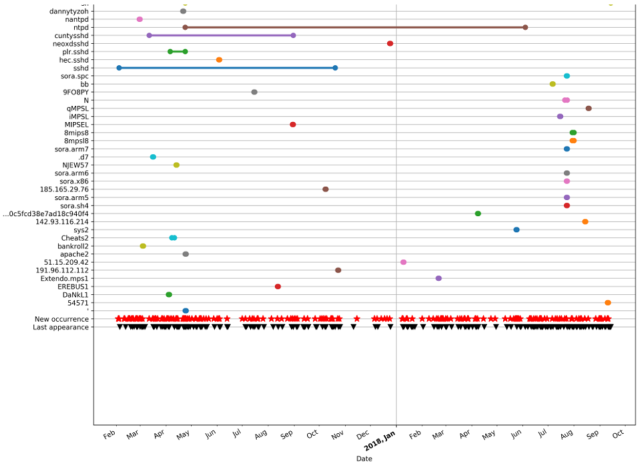
Examples of passive DDOS capacity measurements

Mirai



Examples of passive DDOS capacity measurements

Partial Netis or similar exploits



Conclusions

- D4 is a collaborative project to gather information about DDOS
- D4 is an open project
- Join the project info@circl.lu
- Co-financed by CEF action No: 2017-LU-IA-0099

Part 2 - DDOS analysis D4 project objectives

Current DDOS mitigation limitations

Detection and reporting time

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

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

D4 objectives