The D4 Project

Monitoring DDoS and malicious network activities at large scale

CIRCL
Computer Incident
Response Center
Luxembourg

Team CIRCL

TLP:WHITE

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

November 28, 2018

Background of the D4 project

- As a CSIRT, we handled multiple incidents involving (D)DoS such as ransom DDoS, active DDoS attacks or incident response during DDoS activities.
- Our response was often very reactive and we didn't have actional information to be **more proactive against (D)DoS**.
- Our honeypot infrastructure contained a lot of valuable traffic (such as **backscatter traffic**) related to DDoS and we didn't actively analysed such traffic.
- **The sharing of information in the field of DDoS was limited** compared to other threats (based on our experience with MISP).

DDoS blackmail

Blackmail send by email

‘‘Should we attack ...

There are proofs of our capabilities:

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

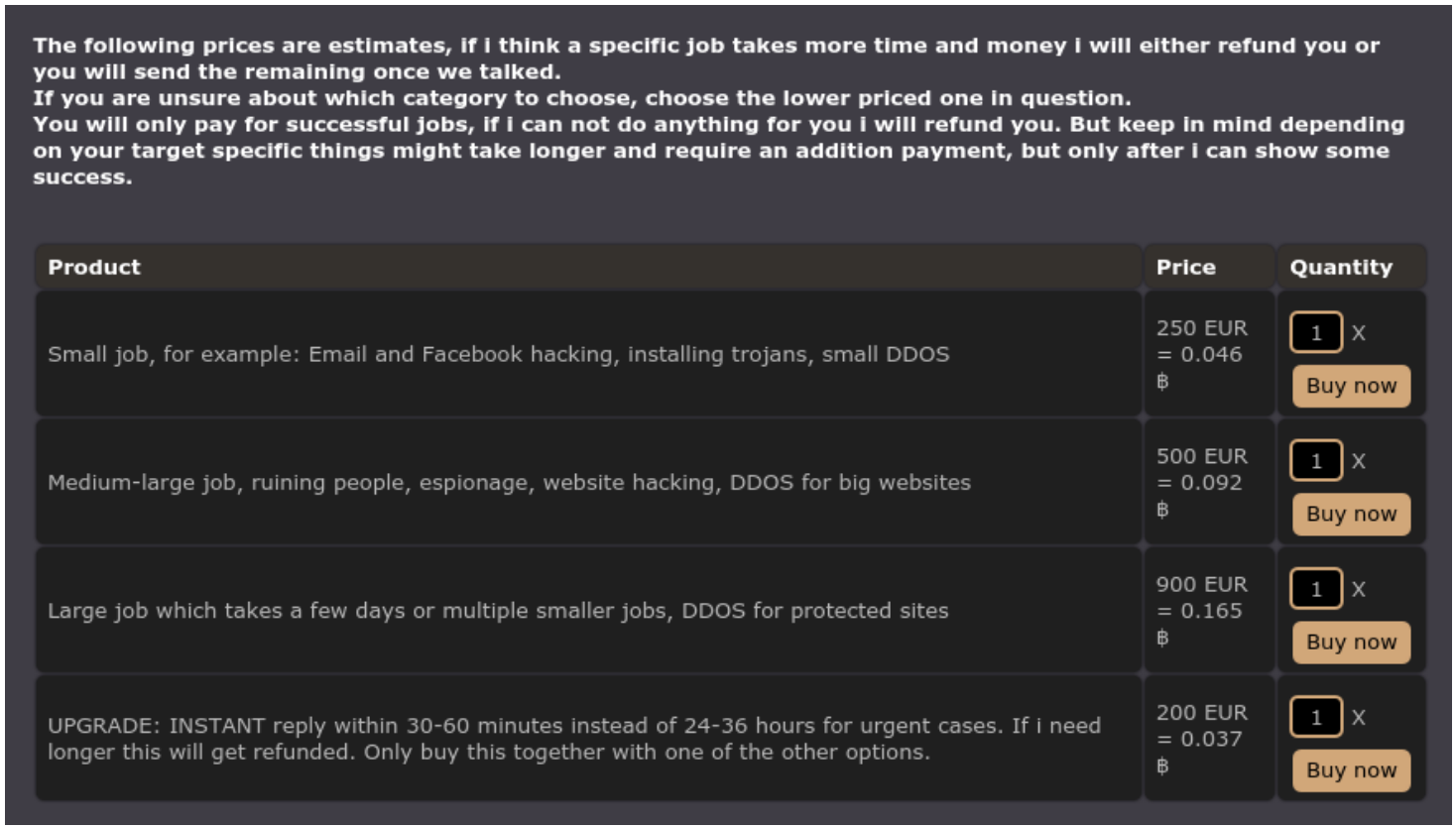
Now the real question is are are willing to pay a lifetime protection fee?

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

How serious do you take such mails?

DDoS services (found by AIL)

Example of a Tor hidden service



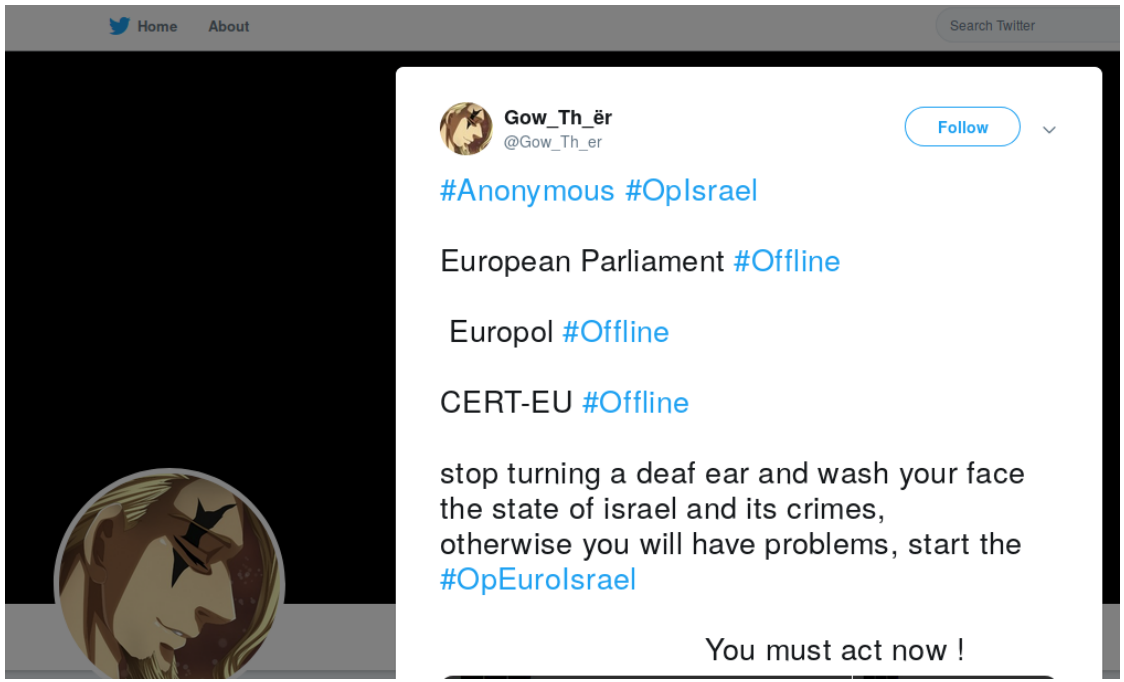
The following prices are estimates, if i think a specific job takes more time and money i will either refund you or you will send the remaining once we talked.
If you are unsure about which category to choose, choose the lower priced one in question.
You will only pay for successful jobs, if i can not 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?

DDoS activities

DDoS claims



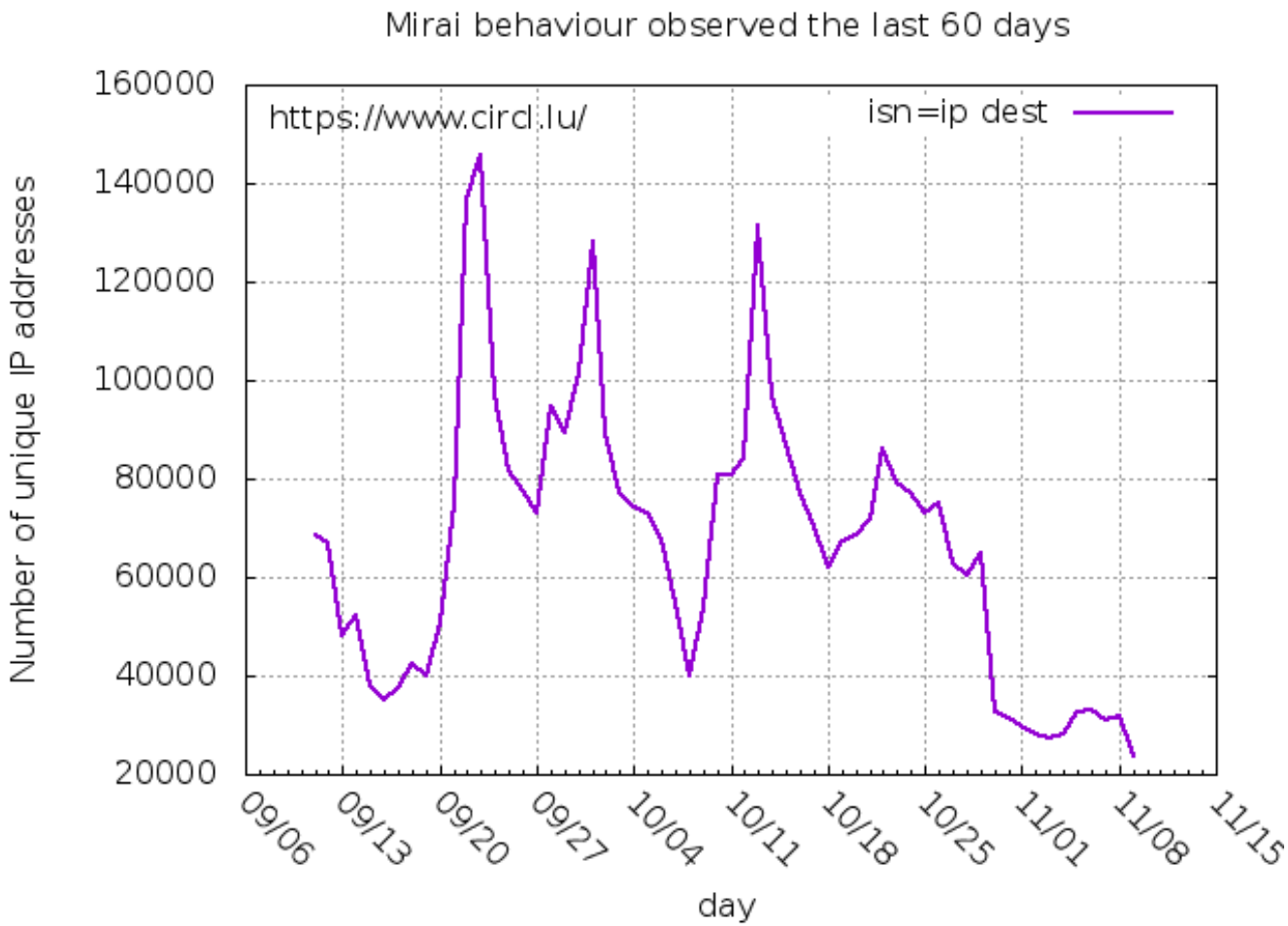
How serious do you take such claims?

D4 project

- Raised from CIRCL research program (HoneyBot project)
- **Development of the DDoS detection and monitoring 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 to evaluate the risks of DDoS
- Provision and advisory support services
  - Extension of CIRCL services especially to AIL and DMA
  - **Training courses based on D4 project results** (e.g. DDoS monitoring/mitigation strategies, network monitoring and analysis)

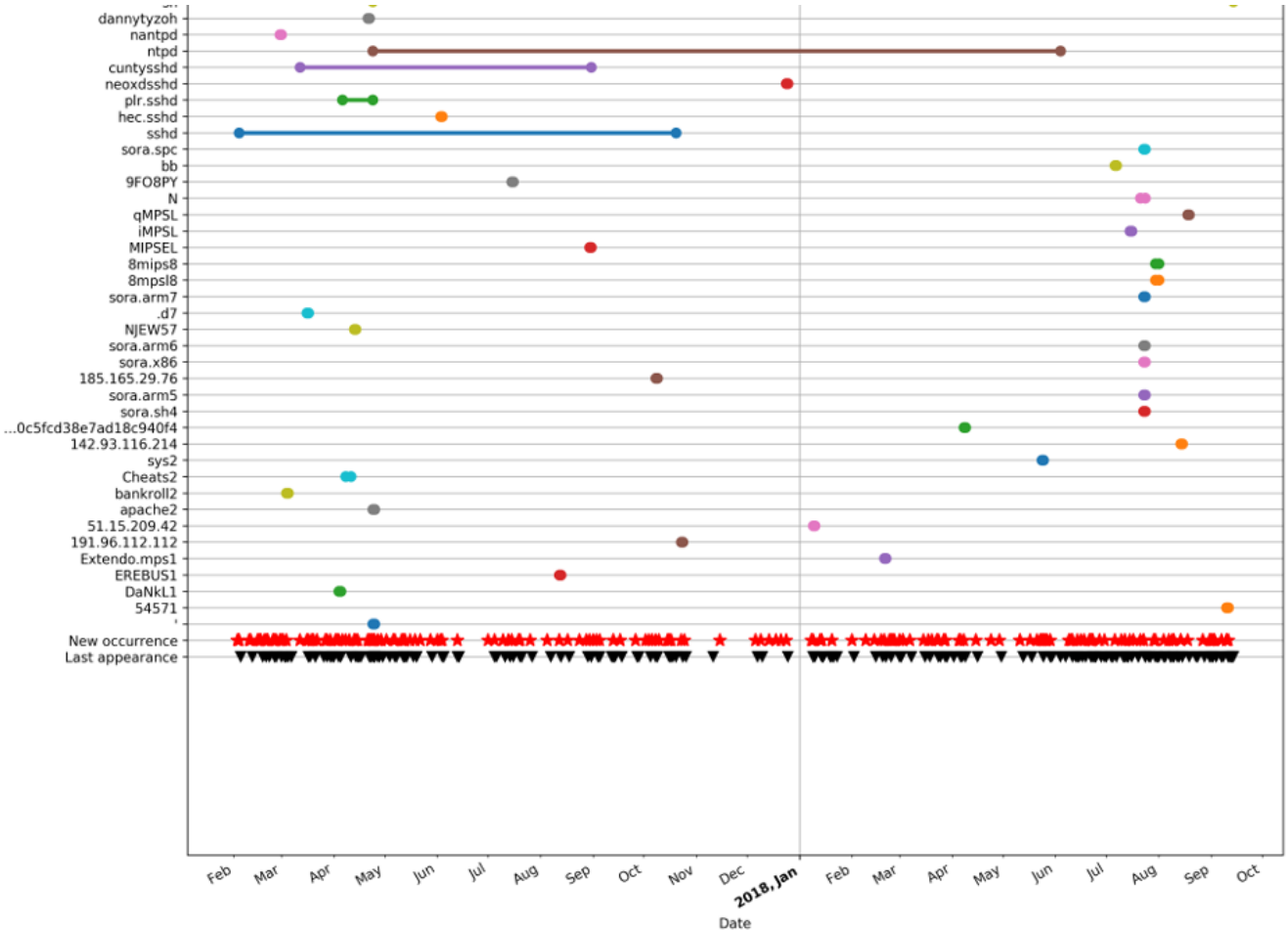
Examples of passive DDoS capacity measurements

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 source project[1]
- Join the project info@circl.lu by **joining the core work-group, contributing monitoring capabilities, contribute to the software or hosting a sensor**
- Co-financed by CEF action No: 2017-LU-IA-0099

[1] `https://www.github.com/D4-project`