CONCORDIA

Cyber security cOmpeteNCe fOr Research anD InnovAtion

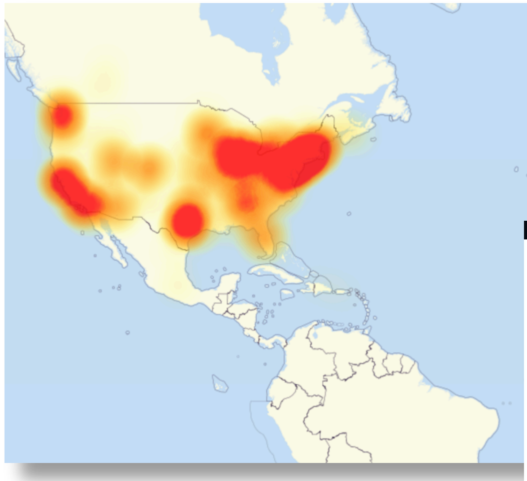
DDoS Clearing House for Europe
Cross-sector Pilot Demo

Cristian Hesselman
(SIDN Labs)

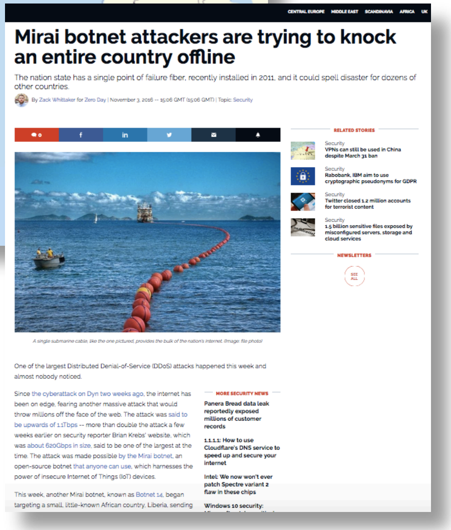
Ramin Yazdani
(UT)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 830927.

DDoS Examples



Mirai botnet: Dyn, OVH (hosting provider), Krebs On Security (website), Deutsche Telecom (ISP)



Mirai botnet attackers are trying to knock an entire country offline

The nation state has a single point of failure fiber, recently installed in 2011, and it could spell disaster for dozens of other countries.

By Zack Whittaker for Zero Day | November 3, 2016 -- 15:06 GMT (15:06 GMT) | Topic: Security

A single submarine cable, like the one pictured, provides the bulk of the nation's internet. (Image: file photo)

RELATED STORIES

Security
VPNs can still be used in China despite March 31 ban

Security
Rabobank, IBM aim to use cryptographic pseudonyms for GDPR

Security
Twitter closed 1.2 million accounts for terrorist content

Security
1.5 billion sensitive files exposed by misconfigured servers, storage and cloud services

NEWSLETTERS

One of the largest Distributed Denial-of-Service (DDoS) attacks happened this week and almost nobody noticed.

Since the cyberattack on Dyn two weeks ago, the internet has been on edge, fearing another massive attack that would throw millions off the face of the web. The attack was said to be upwards of 1.1Tbps -- more than double the attack a few weeks earlier on security reporter Brian Krebs' website, which was about 620Gbps in size, said to be one of the largest at the time. The attack was made possible by the Mirai botnet, an open-source botnet that anyone can use, which harnesses the power of insecure Internet of Things (IoT) devices.

This week, another Mirai botnet, known as Botnet 14, began targeting a small, little-known African country, Liberia, sending

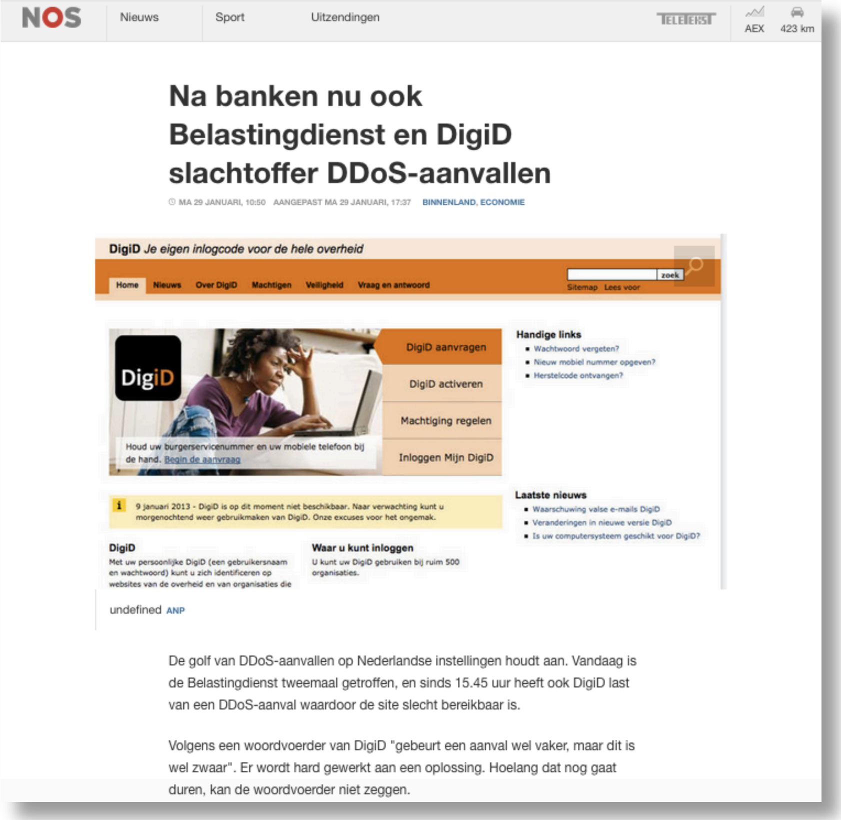
MORE SECURITY NEWS

Panera Bread data leak reportedly exposed millions of customer records

1.1.1.1: How to use Cloudflare's DNS service to speed up and secure your internet

Intel: We now won't ever patch Spectre variant 2 flaw in these chips

Windows 10 security:



Na banken nu ook Belastingdienst en DigiD slachtoffer DDoS-aanvallen

MA 29 JANUARI, 10:50 AANGEPAST MA 29 JANUARI, 17:37 BINNENLAND, ECONOMIE

DigiD *Je eigen inlogcode voor de hele overheid*

Houd uw burgerservicenummer en uw mobiele telefoon bij de hand. Begin de aanvraag

Handige links
- Wachtwoord vergeten?
- Nieuw mobiel nummer opgeven?
- Herstelcode ontvangen?

9 januari 2013 - DigiD is op dit moment niet beschikbaar. Naar verwachting kunt u morgenochtend weer gebruikmaken van DigiD. Onze excuses voor het ongemak.

Laatste nieuws
- Waarschuwing valse e-mails DigiD
- Veranderingen in nieuwe versie DigiD
- Is uw computersysteem geschikt voor DigiD?

DigiD
Met uw persoonlijke DigiD (een gebruikersnaam en wachtwoord) kunt u zich identificeren op websites van de overheid en van organisaties die

Waar u kunt inloggen
U kunt uw DigiD gebruiken bij ruim 500 organisaties.

undefined ANP

De golf van DDoS-aanvallen op Nederlandse instellingen houdt aan. Vandaag is de Belastingdienst tweemaal getroffen, en sinds 15.45 uur heeft ook DigiD last van een DDoS-aanval waardoor de site slecht bereikbaar is.

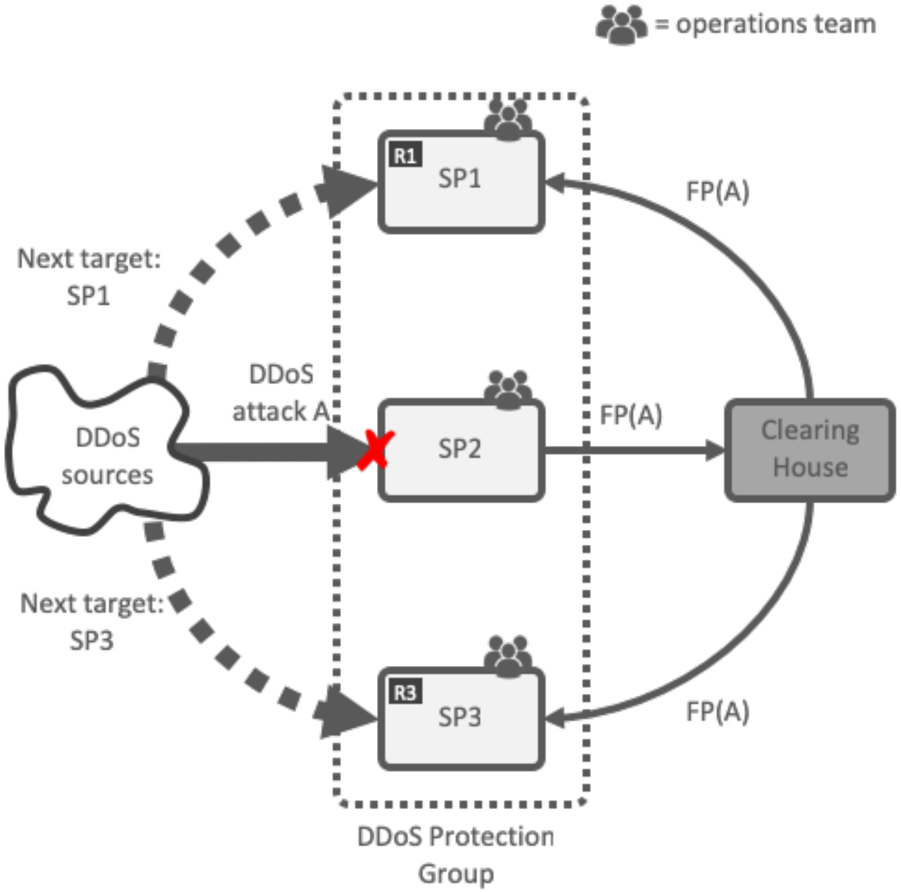
Volgens een woordvoerder van DigiD "gebeurt een aanval wel vaker, maar dit is wel zwaar". Er wordt hard gewerkt aan een oplossing. Hoelang dat nog gaat duren, kan de woordvoerder niet zeggen.

January 2018

https://en.wikipedia.org/wiki/2016_Dyn_cyberattack
https://www.zdnet.com/article/mirai-botnet-attack-briefly-knocked-an-entire-country-offline/

DDoS Clearing House Concept

- Continuous and automatic sharing of “DDoS fingerprints” buys providers time (proactive)
- Extends DDoS protection services that critical service providers use and does not replace them
- Generic: for example, per Member State, per sector, per business unit



T3.2 Objectives

- Pilot a DDoS Clearing House with European industry for Europe to proactively and collaboratively protect European critical infrastructure against DDoS attacks

- Key outputs: pilots in NL >> IT, DDoS clearing house cookbook

- Build on existing components

Key challenge: increase to TRL 5-7 and grow deployment

P-NL P-IT … ⇨ EU

Starting Point: Pilot in the Netherlands

amsix

kpn

POLITIE

SURF
CONCORDIA partner

DNB

SIDN
CONCORDIA partner

National Cyber Security Centre
Ministry of Justice and Security

Betaalvereniging
Nederland

UNIVERSITY
OF TWENTE.
CONCORDIA partner

NLix
The Interconnect Exchange

Belastingdienst

Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

DINL
Stichting
Digitale Infrastructuur
Nederland

NBIP
nationale
beheersorganisatie
internet
providers

vodafone Ziggo

Plus NoMoreDDoS and Dutch Continuity Board

Y1 Accomplishments

- Experimental setup (ddosdb.nl) pilot NL
- Draft data sharing agreement for pilot phase 1
- Draft organizational structure
- Draft overall architecture
- System requirements (funded by NBIP, SURF, NCSC-NL)
- Extensive dissemination (e.g., One Conference, Open Door Event)

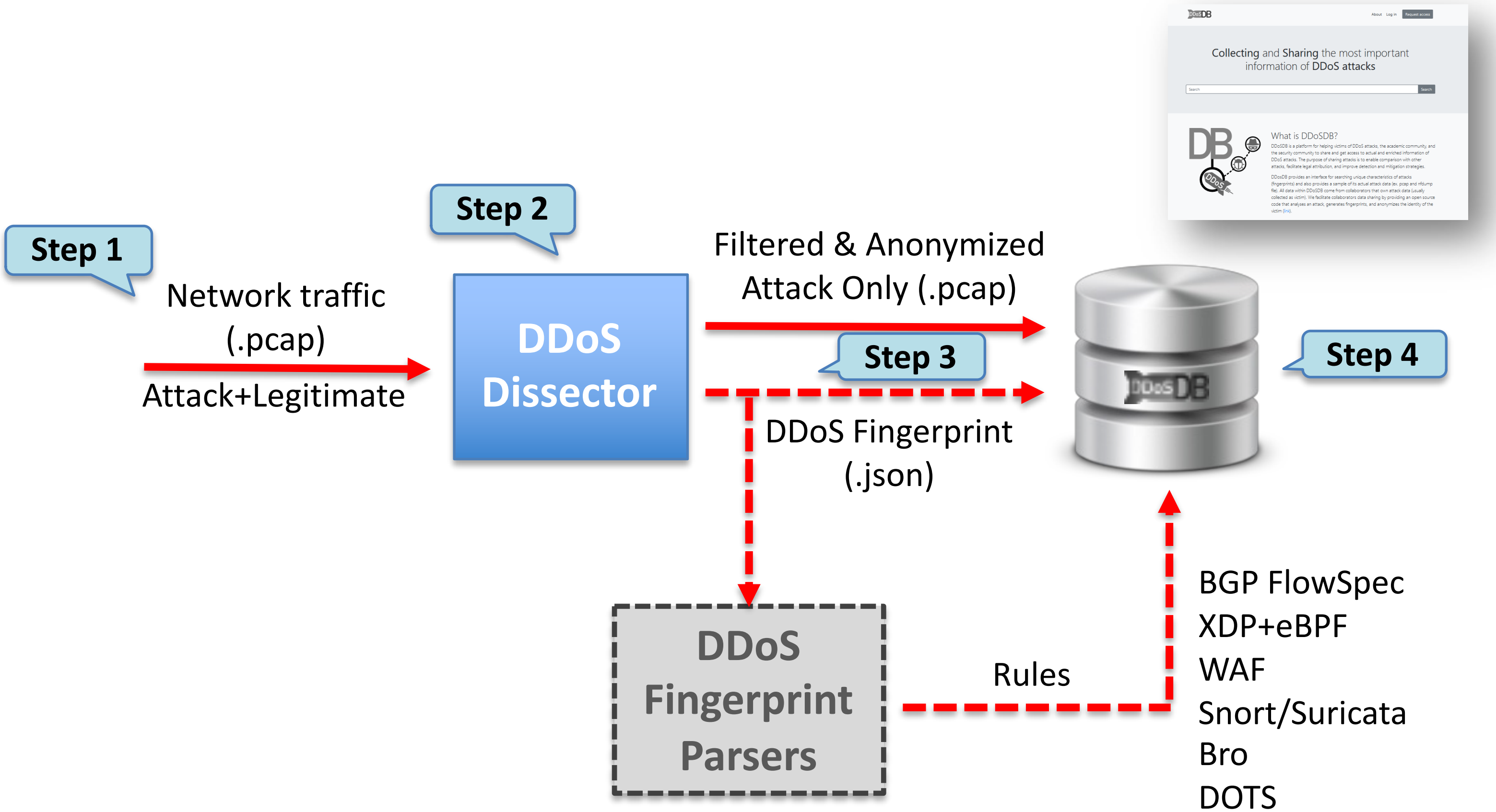
Y1 Lessons Learned

- **Key lesson learned: much more than a technical challenge**
- Need for a DDoS clearing house widely acknowledged
- Clearing house needs to be anchored in an “anti-DDoS coalition”
- Value of clearing house community goes beyond sharing fingerprints
- An anti-DDoS coalition needs a legal working group
- Start small, then grow (personal trust is crucial in early stages)
- Keep initial data sharing agreement crisp, simple, and scalable
- Early collaboration with legal experts and ops teams is a must
- CONCORDIA partners play a challenging bridging role

Y2 Plans

- NL pilot: blog on lessons learned, sign data sharing agreement, start sharing in non-production environment, improve software
- Set up an instance of the clearing house at specifically for T3.2 (ddosdb.eu), run experiments, translate the data sharing agreement from Dutch to English
- Further reinforce collaboration within Task 3.2 as well as with other related tasks in CONCORDIA (Tasks 1.1., 1.2, 3.1, 3.3, and 3.5)

Demo: Clearing House Prototype



DDoSDB

About Log in Request access

Collecting and Sharing the most important information of DDoS attacks

Search Search

What is DDoSDB?

DDoSDB is a platform for helping victims of DDoS attacks, the academic community, and the security community to share and get access to actual and enriched information of DDoS attacks. The purpose of sharing attacks is to enable comparison with other attacks, facilitate legal attribution, and improve detection and mitigation strategies.

DDosDB provides an interface for searching unique characteristics of attacks (fingerprints) and also provides a sample of its actual attack data (ex. pcap and nfdump file). All data within DDoSDB come from collaborators that own attack data (usually collected as victim). We facilitate collaborators data sharing by providing an open source code that analyses an attack, generates fingerprints, and anonymizes the identity of the victim (link).

Contact

Research Institute CODE
Carl-Wery-Straße 22
81739 Munich
Germany

contact@concordia-h2020.eu

Follow us

www.concordia-h2020.eu

www.twitter.com/concordiah2020

www.facebook.com/concordia.eu

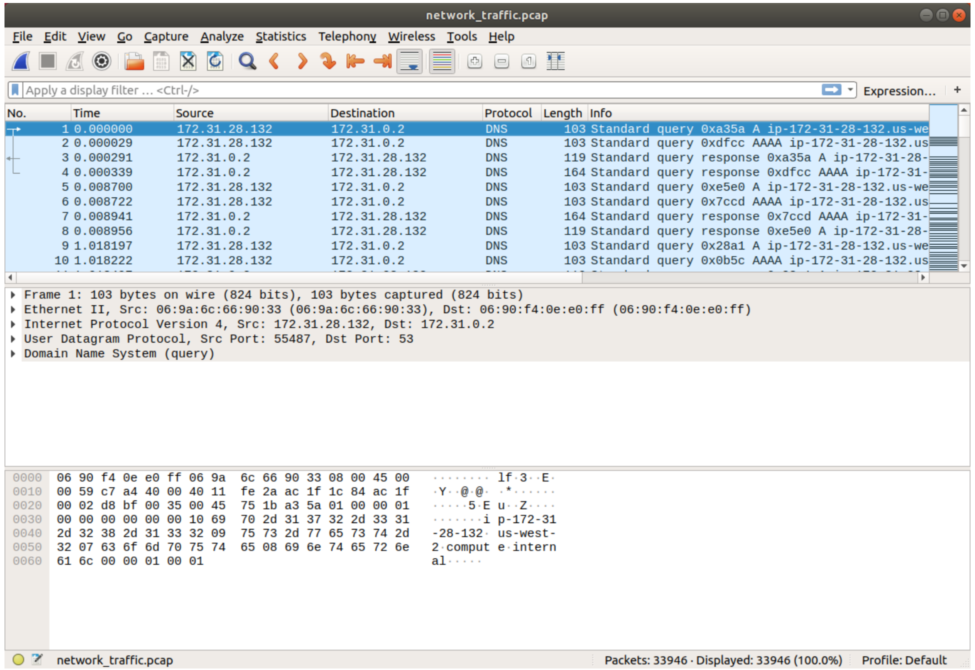
™

www.linkedin.com/in/concordia-h2020

Backup Slides

Input: Network Traffic

- Captured traffic (.pcap) includes attack traffic as well as legitimate traffic containing private info about the target network


network_traffic.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+

```
No.      Time       Source          Destination     Protocol Length Info
       1 0.000000   172.31.28.132   172.31.0.2      DNS         103 Standard query 0xa35a A ip-172-31-28-132.us-we
       2 0.000029   172.31.28.132   172.31.0.2      DNS         103 Standard query 0xdfcc AAAA ip-172-31-28-132.us
       3 0.000291   172.31.0.2      172.31.28.132   DNS         119 Standard query response 0xa35a A ip-172-31-28-
       4 0.000339   172.31.0.2      172.31.28.132   DNS         164 Standard query response 0xdfcc AAAA ip-172-31-
       5 0.008700   172.31.28.132   172.31.0.2      DNS         103 Standard query 0xe5e0 A ip-172-31-28-132.us-we
       6 0.008722   172.31.28.132   172.31.0.2      DNS         103 Standard query 0x7ccd AAAA ip-172-31-28-132.us
       7 0.008941   172.31.0.2      172.31.28.132   DNS         164 Standard query response 0x7ccd AAAA ip-172-31-
       8 0.008956   172.31.0.2      172.31.28.132   DNS         119 Standard query response 0xe5e0 A ip-172-31-28-
       9 1.018197   172.31.28.132   172.31.0.2      DNS         103 Standard query 0x28a1 A ip-172-31-28-132.us-we
      10 1.018222   172.31.28.132   172.31.0.2      DNS         103 Standard query 0x0b5c AAAA ip-172-31-28-132.us
```

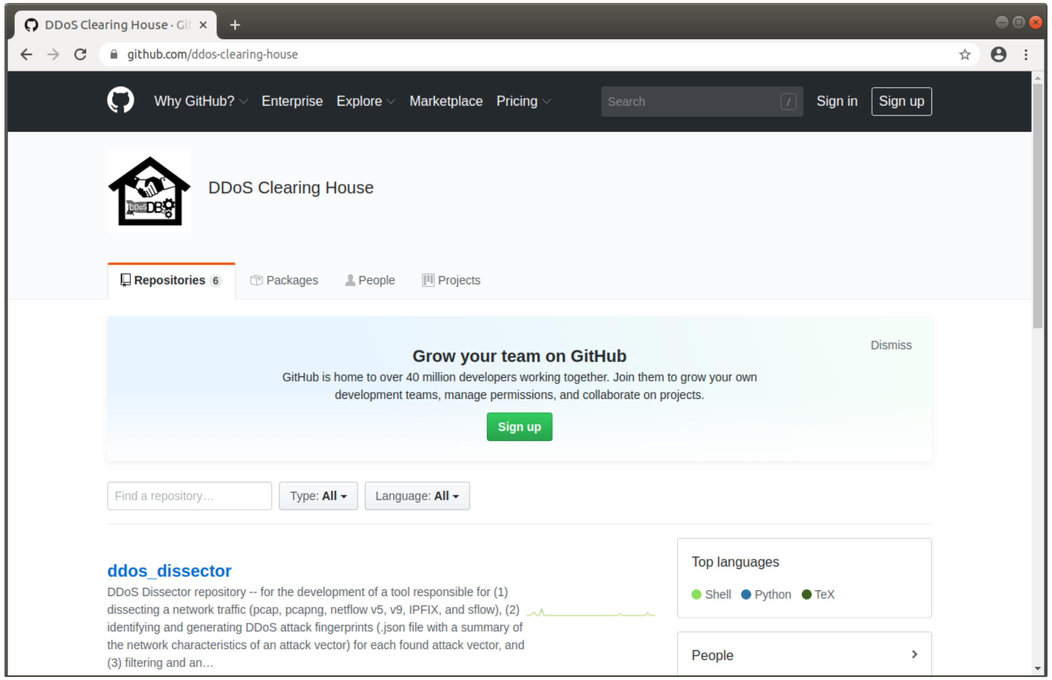
```
▸ Frame 1: 103 bytes on wire (824 bits), 103 bytes captured (824 bits)
▸ Ethernet II, Src: 06:9a:6c:66:90:33 (06:9a:6c:66:90:33), Dst: 06:90:f4:0e:e0:ff (06:90:f4:0e:e0:ff)
▸ Internet Protocol Version 4, Src: 172.31.28.132, Dst: 172.31.0.2
▸ User Datagram Protocol, Src Port: 55487, Dst Port: 53
▸ Domain Name System (query)
```

```
0000  06 90 f4 0e e0 ff 06 9a  6c 66 90 33 08 00 45 00   ········ lf·3··E·
0010  00 59 c7 a4 40 00 40 11  fe 2a ac 1f 1c 84 ac 1f   ·Y··@·@· ·*······
0020  00 02 d8 bf 00 35 00 45  75 1b a3 5a 01 00 00 01   ·····5·E u··Z····
0030  00 00 00 00 00 00 10 69  70 2d 31 37 32 2d 33 31   ·······i p-172-31
0040  2d 32 38 2d 31 33 32 09  75 73 2d 77 65 73 74 2d   -28-132· us-west-
0050  32 07 63 6f 6d 70 75 74  65 08 69 6e 74 65 72 6e   2·comput e·intern
0060  61 6c 00 00 01 00 01                               al·····
```

network_traffic.pcap | Packets: 33946 · Displayed: 33946 (100.0%) | Profile: Default

DDoS Dissector

- *ddos_disector* library filters, anonymizes and summarizes the input traffic and provides a fingerprint (.json) and anonymized attack only trace (.pcap) as outputs



Grow your team on GitHub

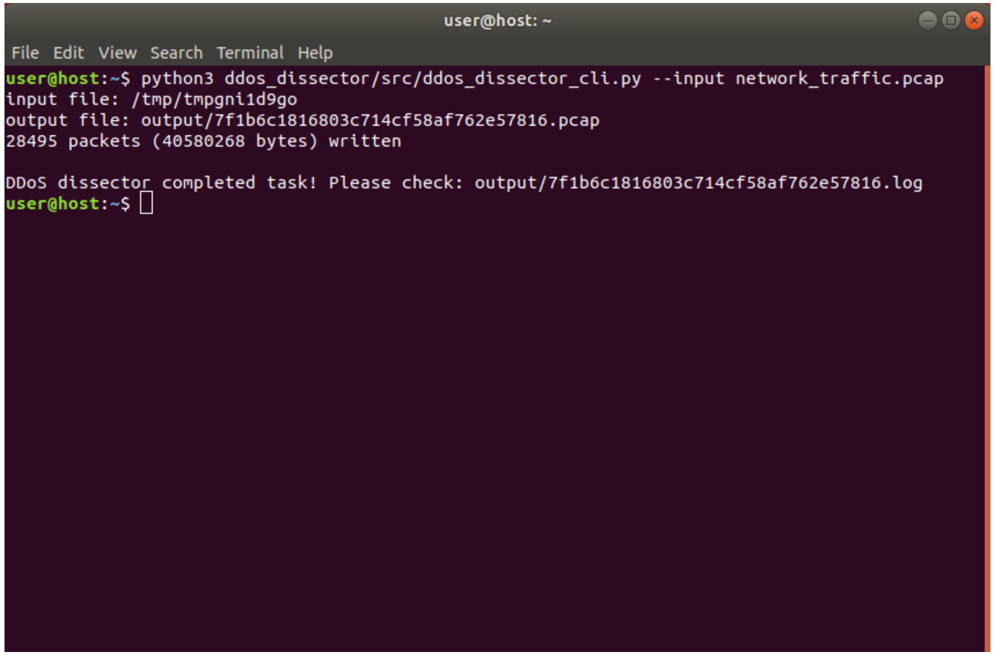
GitHub is home to over 40 million developers working together. Join them to grow your own development teams, manage permissions, and collaborate on projects.

ddos_dissector

DDoS Dissector repository -- for the development of a tool responsible for (1) dissecting a network traffic (pcap, pcapng, netflow v5, v9, IPFIX, and sflow), (2) identifying and generating DDoS attack fingerprints (.json file with a summary of the network characteristics of an attack vector) for each found attack vector, and (3) filtering and an…

DDoS Dissector

- *ddos_disector* library filters, anonymizes and summarizes the input traffic and provides a fingerprint (.json) and anonymized attack only trace (.pcap) as outputs

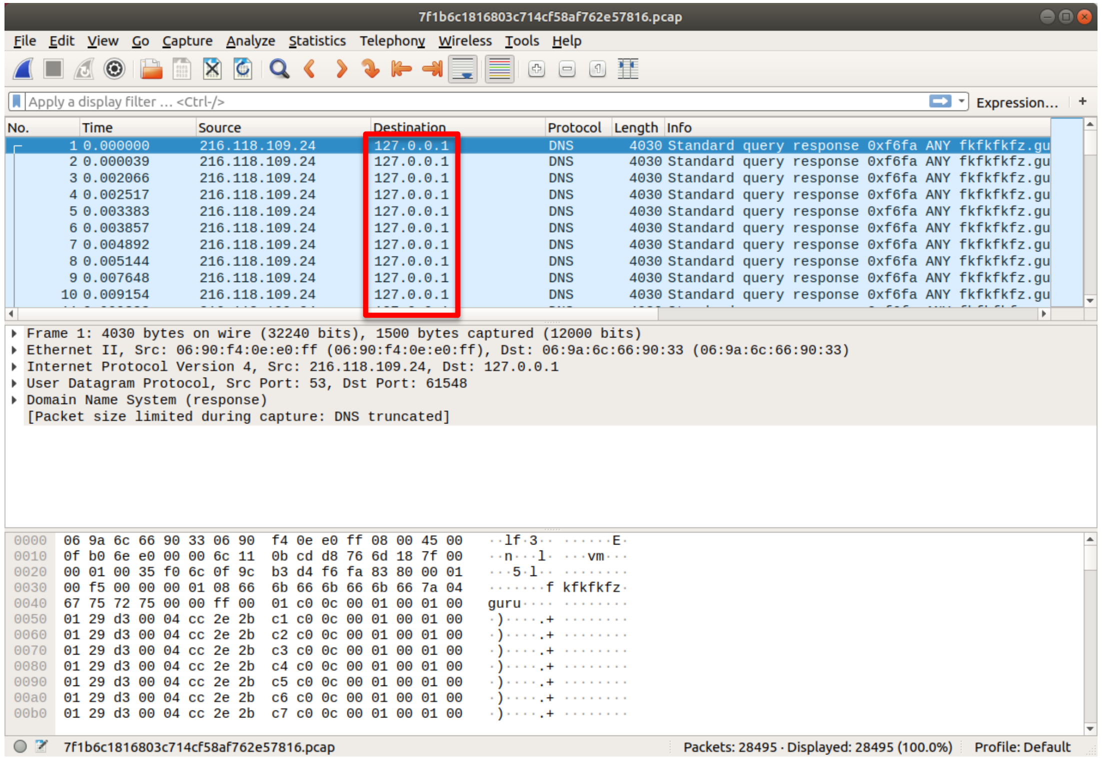


```
user@host:~$ python3 ddos_dissector/src/ddos_dissector_cli.py --input network_traffic.pcap
input file: /tmp/tmpgni1d9go
output file: output/7f1b6c1816803c714cf58af762e57816.pcap
28495 packets (40580268 bytes) written

DDoS dissector completed task! Please check: output/7f1b6c1816803c714cf58af762e57816.log
user@host:~$ 
```

Output: Attack Trace

- Anonymized and filtered attack only trace (.pcap)


7f1b6c1816803c714cf58af762e57816.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+

```
No.  Time      Source          Destination  Protocol Length Info
   1 0.000000  216.118.109.24  127.0.0.1    DNS     4030 Standard query response 0xf6fa ANY fkfkfkfz.gu
   2 0.000039  216.118.109.24  127.0.0.1    DNS     4030 Standard query response 0xf6fa ANY fkfkfkfz.gu
   3 0.002066  216.118.109.24  127.0.0.1    DNS     4030 Standard query response 0xf6fa ANY fkfkfkfz.gu
   4 0.002517  216.118.109.24  127.0.0.1    DNS     4030 Standard query response 0xf6fa ANY fkfkfkfz.gu
   5 0.003383  216.118.109.24  127.0.0.1    DNS     4030 Standard query response 0xf6fa ANY fkfkfkfz.gu
   6 0.003857  216.118.109.24  127.0.0.1    DNS     4030 Standard query response 0xf6fa ANY fkfkfkfz.gu
   7 0.004892  216.118.109.24  127.0.0.1    DNS     4030 Standard query response 0xf6fa ANY fkfkfkfz.gu
   8 0.005144  216.118.109.24  127.0.0.1    DNS     4030 Standard query response 0xf6fa ANY fkfkfkfz.gu
   9 0.007648  216.118.109.24  127.0.0.1    DNS     4030 Standard query response 0xf6fa ANY fkfkfkfz.gu
  10 0.009154  216.118.109.24  127.0.0.1    DNS     4030 Standard query response 0xf6fa ANY fkfkfkfz.gu
```

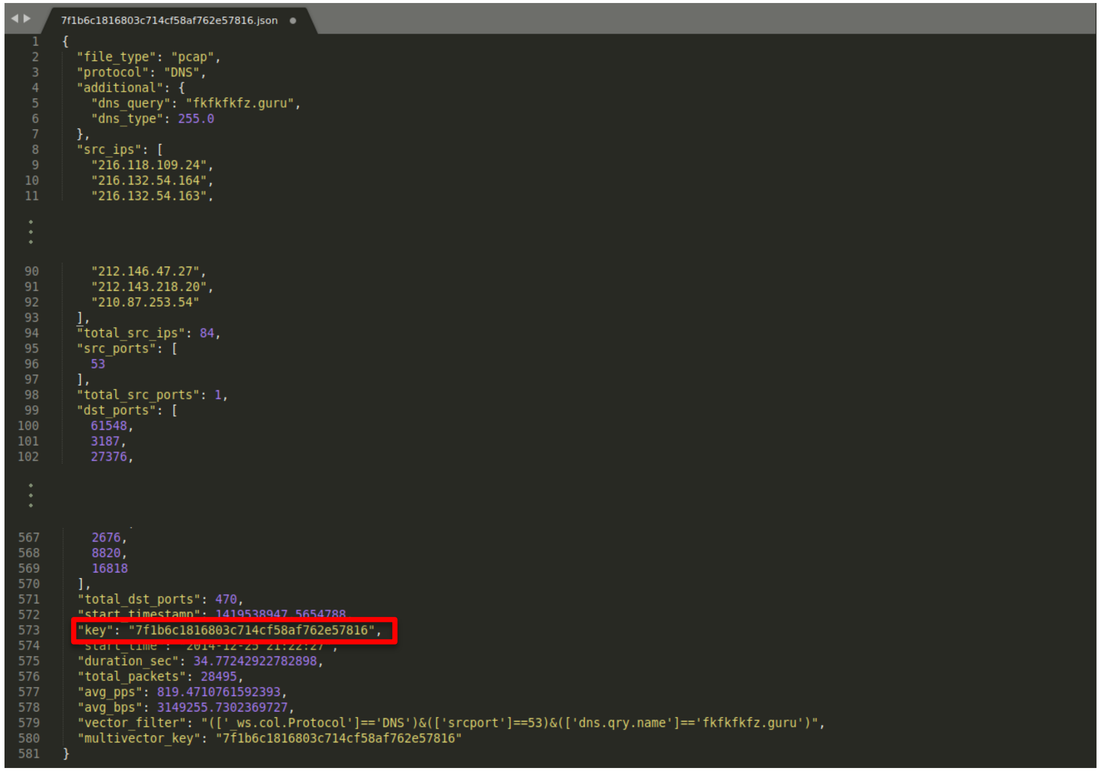
```
Frame 1: 4030 bytes on wire (32240 bits), 1500 bytes captured (12000 bits)
Ethernet II, Src: 06:90:f4:0e:e0:ff (06:90:f4:0e:e0:ff), Dst: 06:9a:6c:66:90:33 (06:9a:6c:66:90:33)
Internet Protocol Version 4, Src: 216.118.109.24, Dst: 127.0.0.1
User Datagram Protocol, Src Port: 53, Dst Port: 61548
Domain Name System (response)
[Packet size limited during capture: DNS truncated]
```

```
0000  06 9a 6c 66 90 33 06 90  f4 0e e0 ff 08 00 45 00   ··lf·3·· ······E·
0010  0f b0 6e e0 00 00 6c 11  0b cd d8 76 6d 18 7f 00   ··n···l· ···vm···
0020  00 01 00 35 f0 6c 0f 9c  b3 d4 f6 fa 83 80 00 01   ···5·l·· ········
0030  00 f5 00 00 00 01 08 66  6b 66 6b 66 6b 66 7a 04   ·······f kfkfkfz·
0040  67 75 72 75 00 00 ff 00  01 c0 0c 00 01 00 01 00   guru···· ········
0050  01 29 d3 00 04 cc 2e 2b  c1 c0 0c 00 01 00 01 00   ·)····.+ ········
0060  01 29 d3 00 04 cc 2e 2b  c2 c0 0c 00 01 00 01 00   ·)····.+ ········
0070  01 29 d3 00 04 cc 2e 2b  c3 c0 0c 00 01 00 01 00   ·)····.+ ········
0080  01 29 d3 00 04 cc 2e 2b  c4 c0 0c 00 01 00 01 00   ·)····.+ ········
0090  01 29 d3 00 04 cc 2e 2b  c5 c0 0c 00 01 00 01 00   ·)····.+ ········
00a0  01 29 d3 00 04 cc 2e 2b  c6 c0 0c 00 01 00 01 00   ·)····.+ ········
00b0  01 29 d3 00 04 cc 2e 2b  c7 c0 0c 00 01 00 01 00   ·)····.+ ········
```

7f1b6c1816803c714cf58af762e57816.pcap   Packets: 28495 · Displayed: 28495 (100.0%)   Profile: Default

Output: DDoS Fingerprint

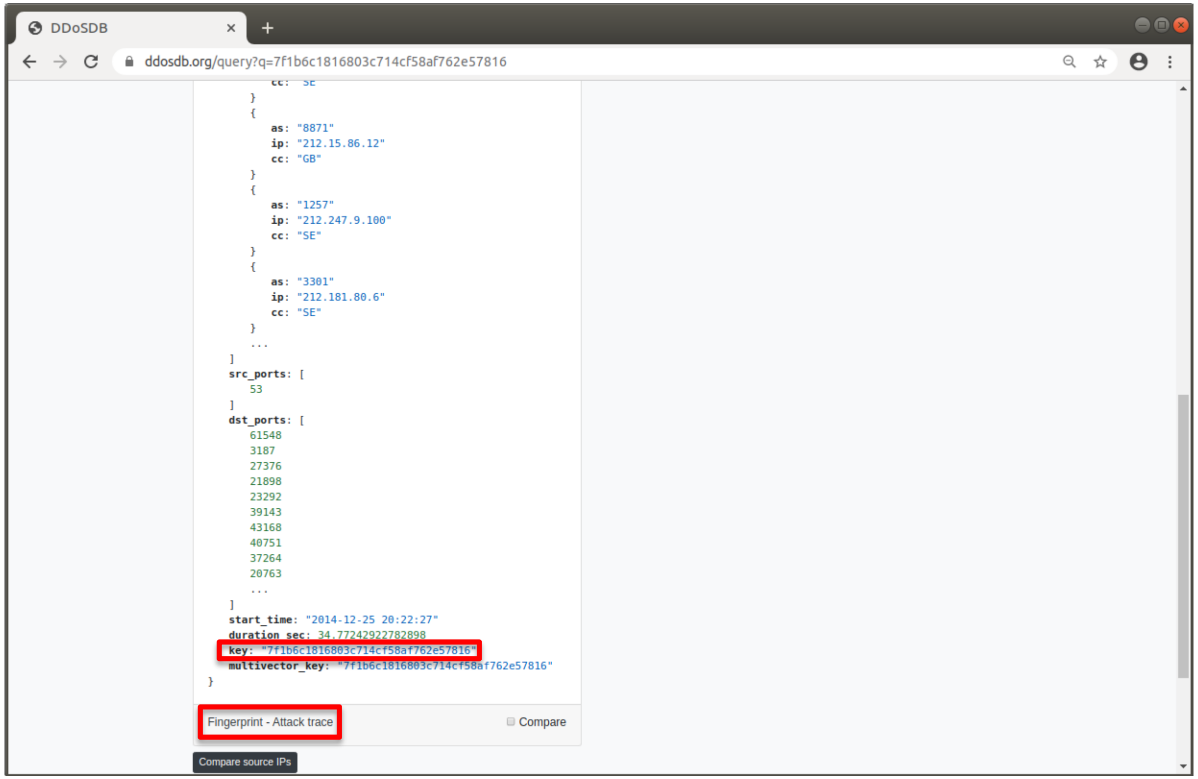
- Attack fingerprint (.json)



```
{
  "file_type": "pcap",
  "protocol": "DNS",
  "additional": {
    "dns_query": "fkfkfkfz.guru",
    "dns_type": 255.0
  },
  "src_ips": [
    "216.118.109.24",
    "216.132.54.164",
    "216.132.54.163",
⋮
    "212.146.47.27",
    "212.143.218.20",
    "210.87.253.54"
  ],
  "total_src_ips": 84,
  "src_ports": [
    53
  ],
  "total_src_ports": 1,
  "dst_ports": [
    61548,
    3187,
    27376,
⋮
    2676,
    8820,
    16818
  ],
  "total_dst_ports": 470,
  "start_timestamp": 1419538947.5654788
  "key": "7f1b6c1816803c714cf58af762e57816",
  "start_time": "2014-12-25 21:22:27",
  "duration_sec": 34.77242922782898,
  "total_packets": 28495,
  "avg_pps": 819.4710761592393,
  "avg_bps": 3149255.7302369727,
  "vector_filter": "(['_ws.col.Protocol']=='DNS')&(['srcport']==53)&(['dns.qry.name']=='fkfkfkfz.guru')",
  "multivector_key": "7f1b6c1816803c714cf58af762e57816"
}
```

DDoSDB

- Outputs are stored in DDOSDB database for data sharing and proactive mitigation of attacks



DDoSDB
ddosdb.org/query?q=7f1b6c1816803c714cf58af762e57816

```
            cc: "SE"
        }
        {
            as: "8871"
            ip: "212.15.86.12"
            cc: "GB"
        }
        {
            as: "1257"
            ip: "212.247.9.100"
            cc: "SE"
        }
        {
            as: "3301"
            ip: "212.181.80.6"
            cc: "SE"
        }
        ...
    ]
    src_ports: [
        53
    ]
    dst_ports: [
        61548
        3187
        27376
        21898
        23292
        39143
        43168
        40751
        37264
        20763
        ...
    ]
    start_time: "2014-12-25 20:22:27"
    duration_sec: 34.77242922782898
    key: "7f1b6c1816803c714cf58af762e57816"
    multivector_key: "7f1b6c1816803c714cf58af762e57816"
}
```

Fingerprint - Attack trace
□ Compare
Compare source IPs

Future Work

- Developing DDoS fingerprint parsers to convert fingerprints to rules and share these rules with stakeholders

- These rules can be applied to different mitigation boxes in the network with different levels of specificity to mitigate DDoS attacks