IoT security and the DDoS Clearing House

João M. Ceron – INTERSECT
Research Engineer

INTERSCT.

SIDN LABS

IoT Security

- IoT devices are very verbose
  - Can perform high number packet

71 packets

TP Link Plug

587 packets

WeMoLink

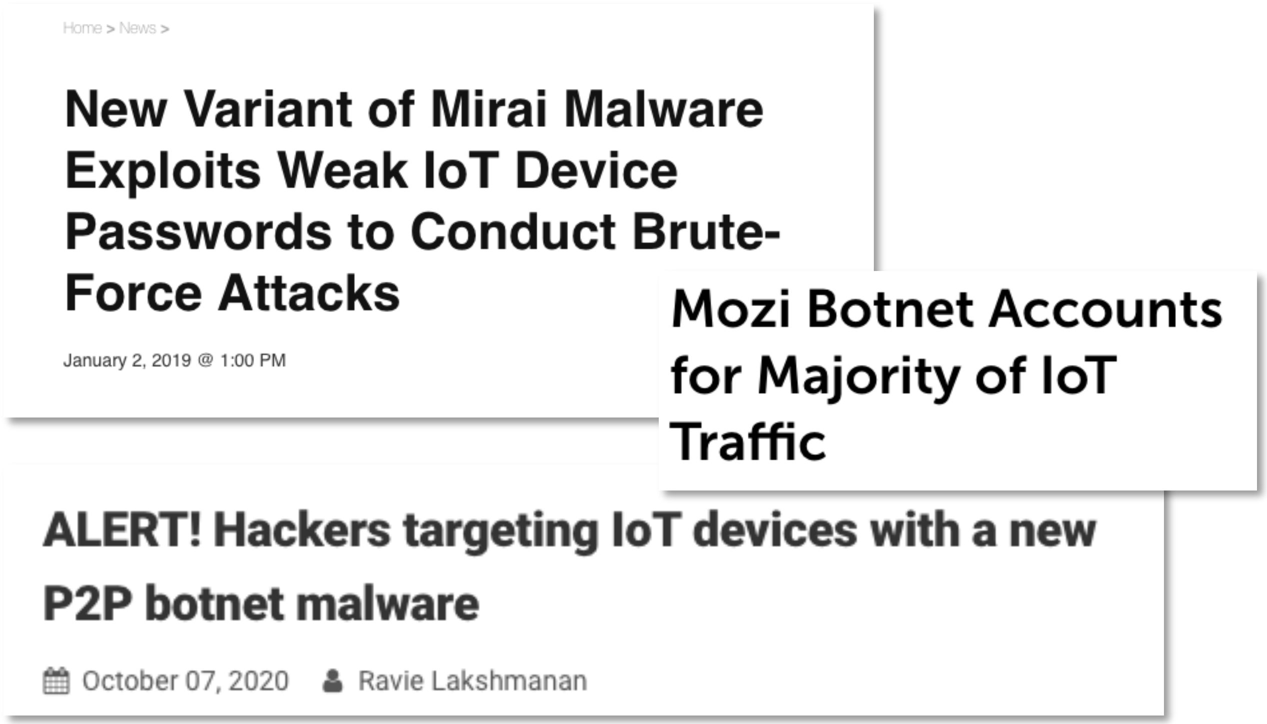
2397 packets

HueSwitch

INITIALIZATION PROCESS

IoT Security

- Vulnerable devices can be abused



Home > News >

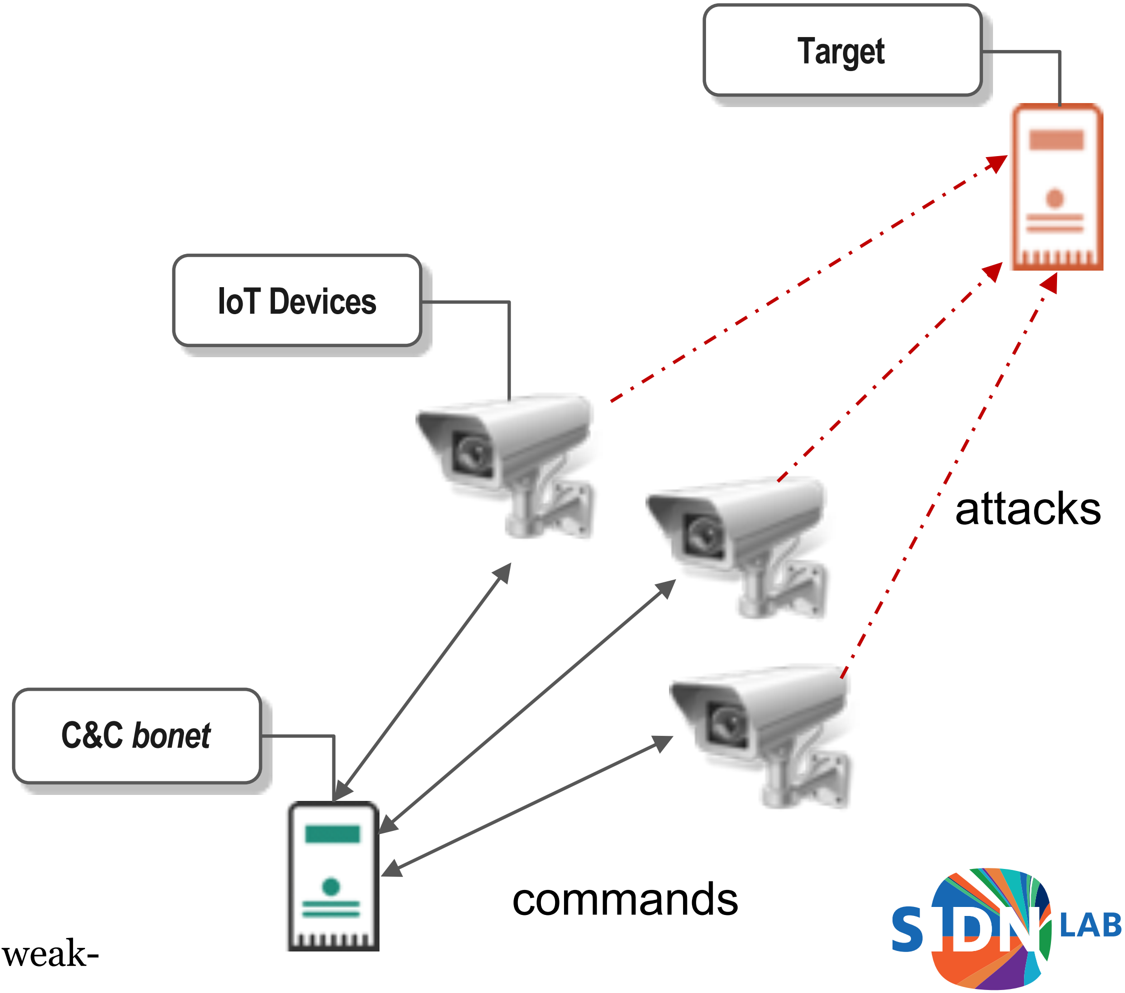
New Variant of Mirai Malware Exploits Weak IoT Device Passwords to Conduct Brute-Force Attacks

January 2, 2019 @ 1:00 PM

Mozi Botnet Accounts for Majority of IoT Traffic

ALERT! Hackers targeting IoT devices with a new P2P botnet malware

October 07, 2020 Ravie Lakshmanan



https://thehackernews.com/2020/10/p2p-iot-botnet.html

https://threatpost.com/mozi-botnet-majority-iot-traffic/159337/

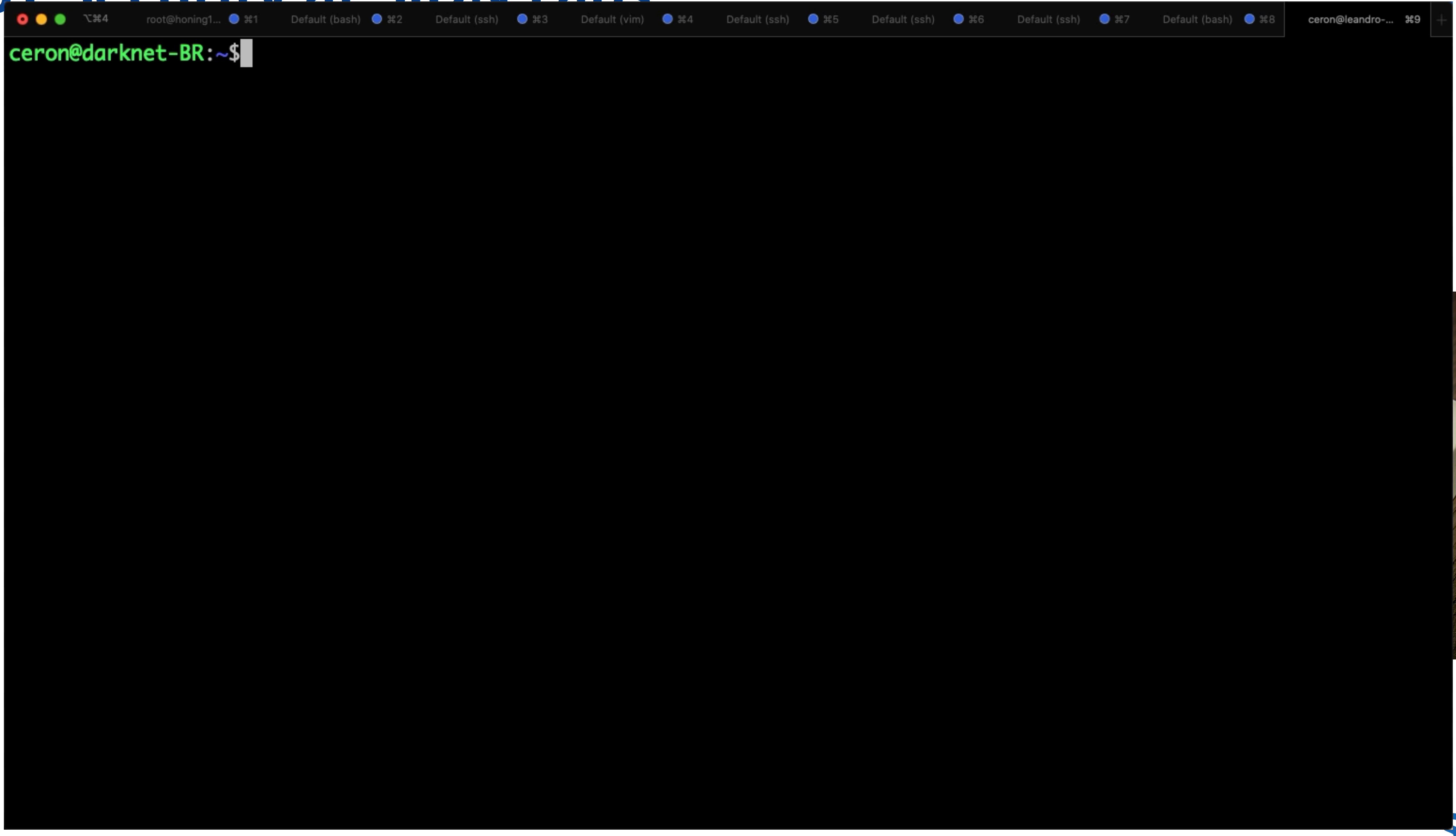
https://securityintelligence.com/news/new-variant-of-mirai-malware-exploits-weak-iot-device-passwords-to-conduct-brute-force-attacks/

IoT Security at SIDN Labs

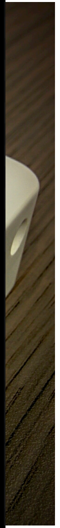
- The SPIN project
  - Open-source platform to measure, visualise, and control IoT device network traffic
    - https://github.com/sidn/spin/
  - OpenWRT-based

- Collect malicious IoT Traffic
  - honeypot

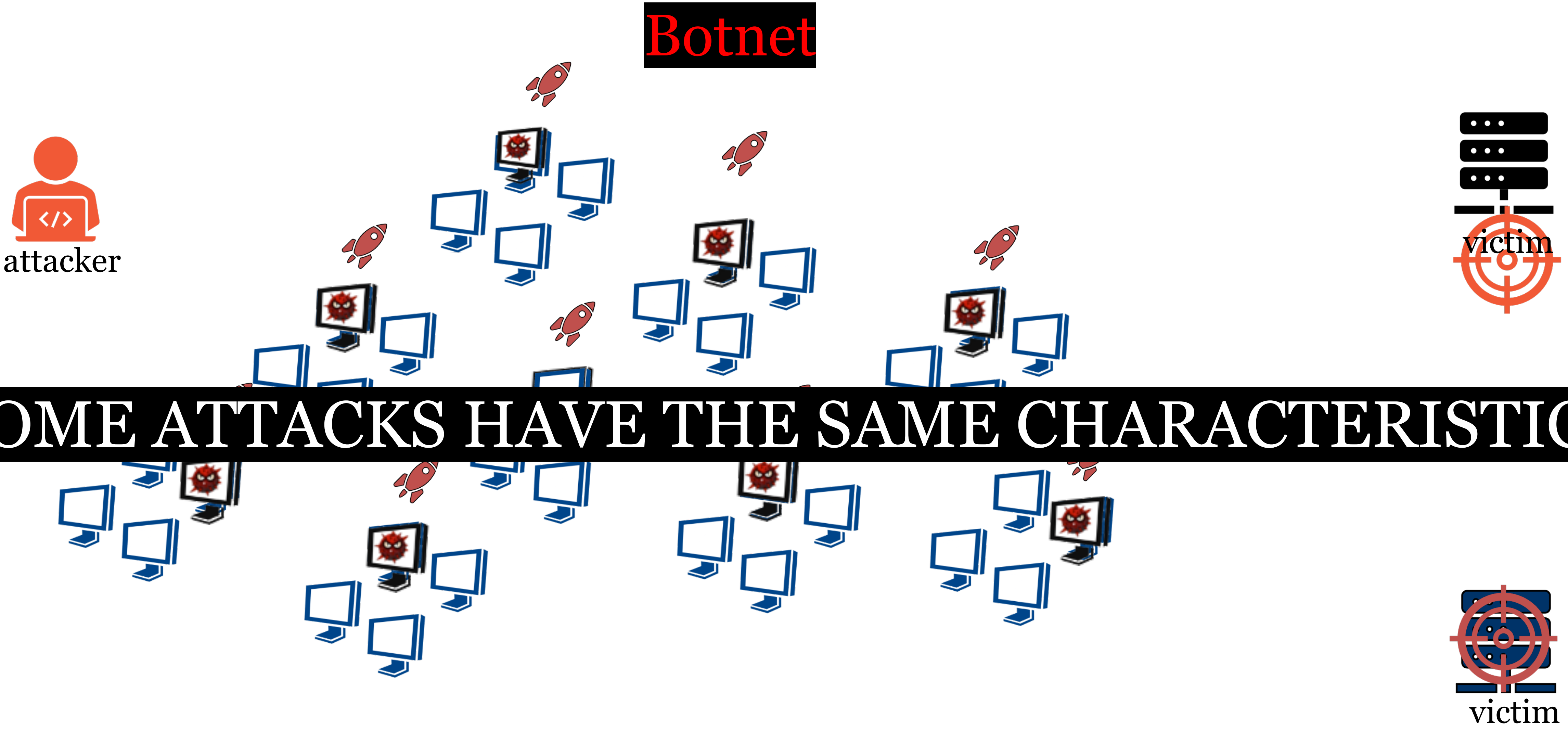
IoT Security at SIDN Labs



```
ceron@darknet-BR:~$
```



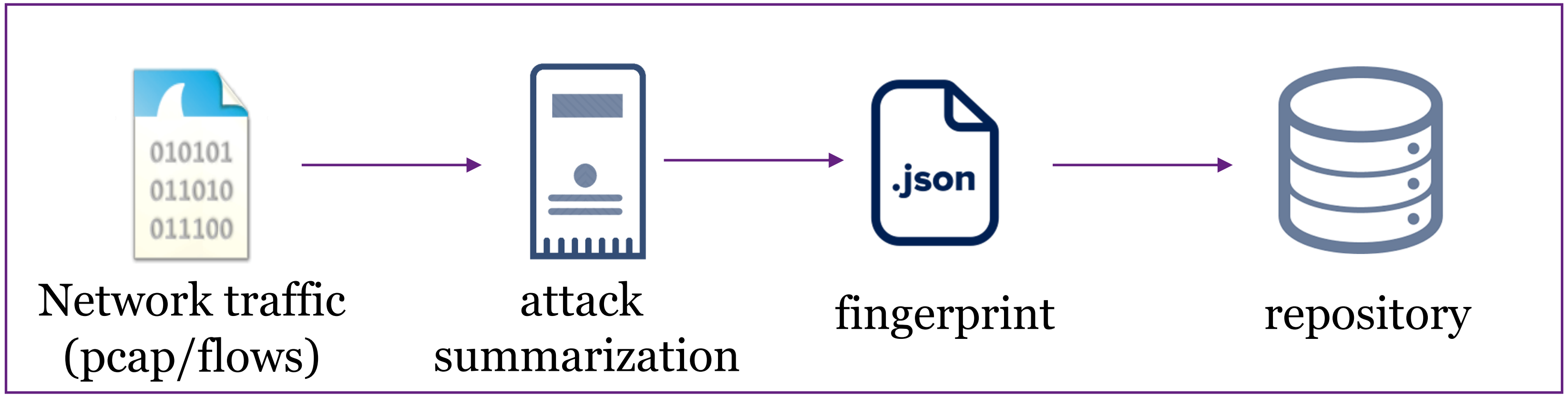
SOME ATTACKS HAVE THE SAME CHARACTERISTICS



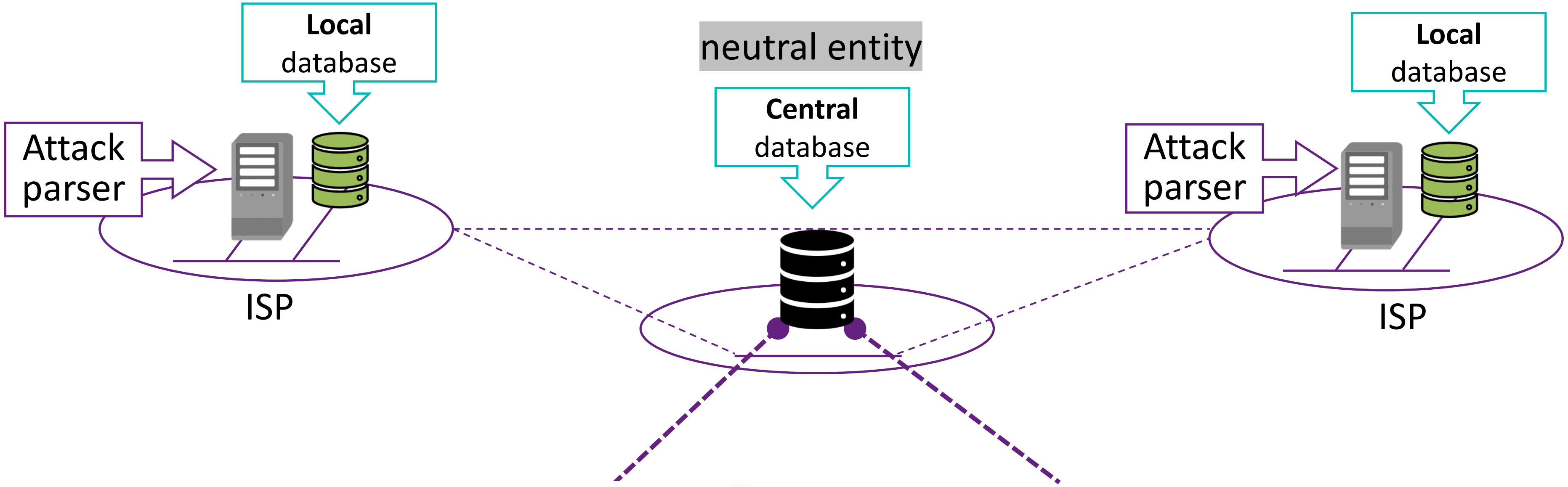
DDoS Clearing House Concept

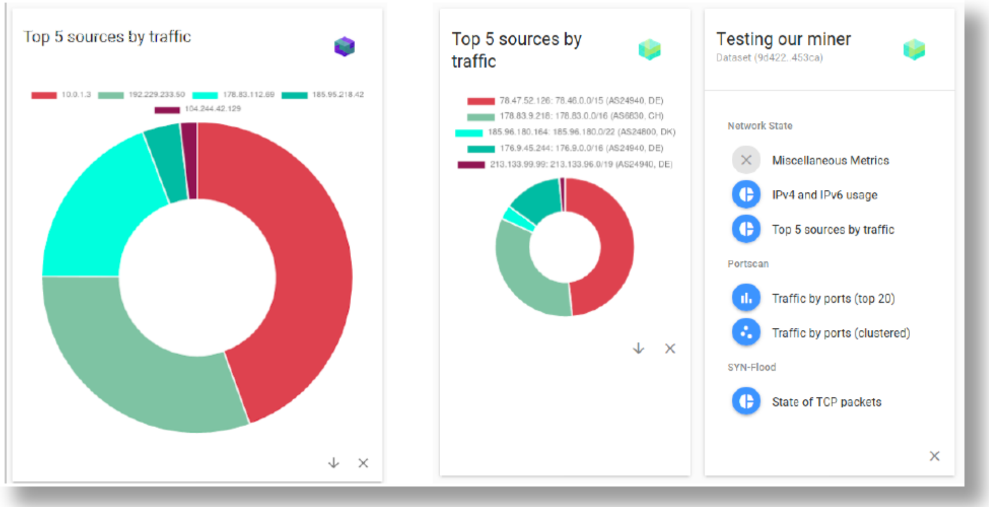
SHARING DDoS CHARACTERISTICS

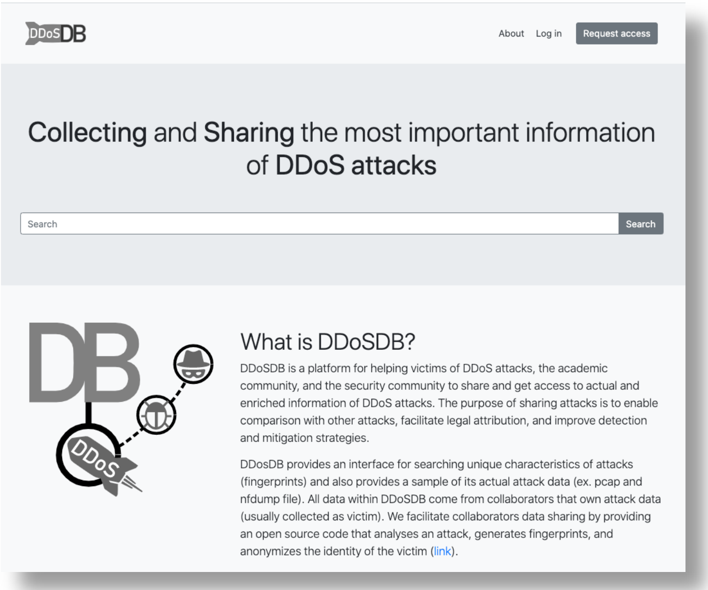
- Continuous and automatic sharing of "DDoS fingerprints" buys ISPs time (proactive)
- Extend DDoS protection services
  - Not a detection tool



DDoS Clearing House Concept







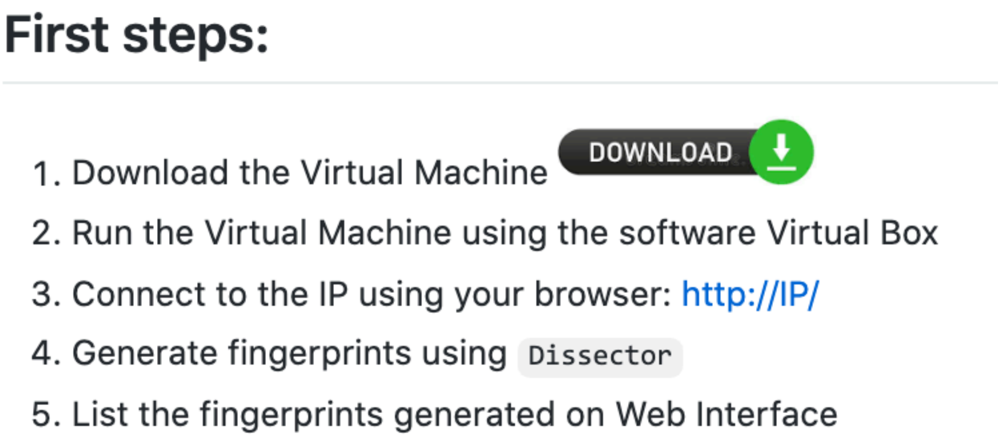
Collecting and Sharing the most important information of DDoS attacks

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).

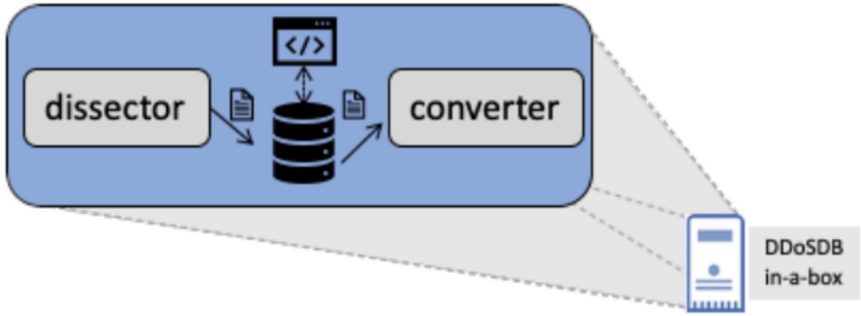
How can I test the software?

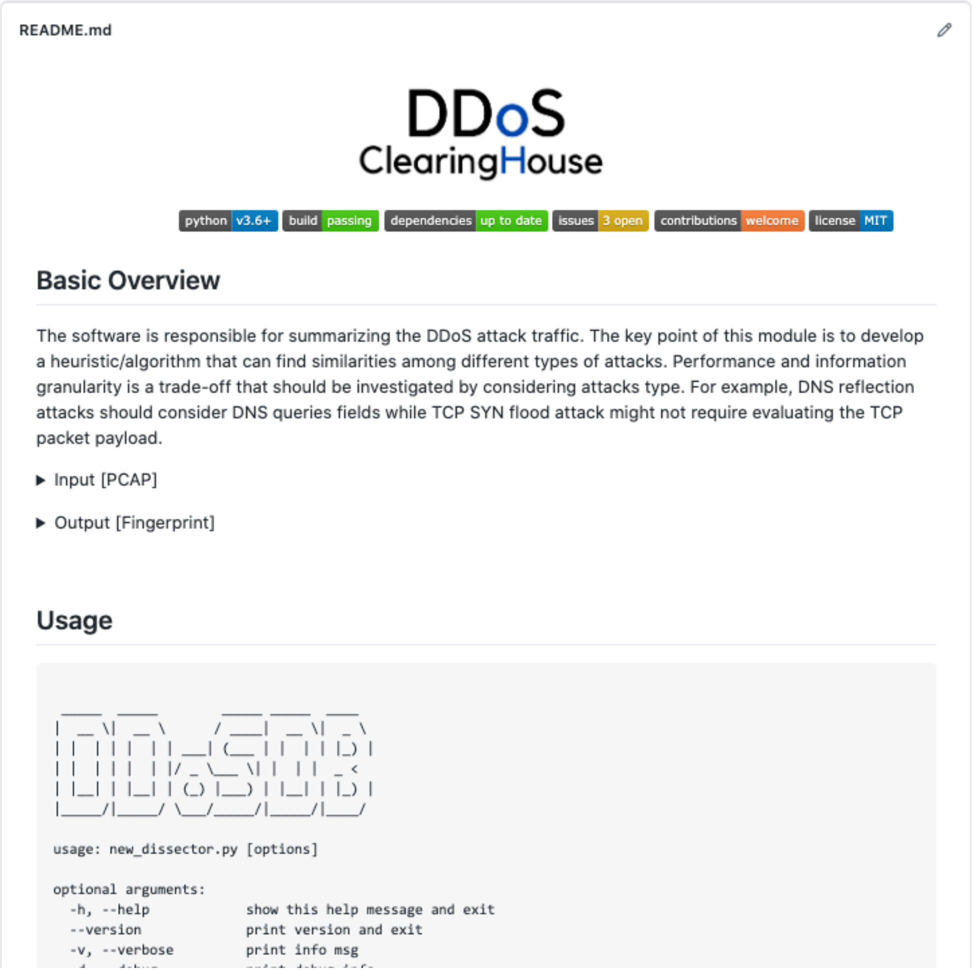


First steps:

1. Download the Virtual Machine DOWNLOAD
2. Run the Virtual Machine using the software Virtual Box
3. Connect to the IP using your browser: http://IP/
4. Generate fingerprints using `Dissector`
5. List the fingerprints generated on Web Interface

https://github.com/ddos-clearing-house/dddosdb-in-a-box





Basic Overview

The software is responsible for summarizing the DDoS attack traffic. The key point of this module is to develop a heuristic/algorithm that can find similarities among different types of attacks. Performance and information granularity is a trade-off that should be investigated by considering attacks type. For example, DNS reflection attacks should consider DNS queries fields while TCP SYN flood attack might not require evaluating the TCP packet payload.

▶ Input [PCAP]

▶ Output [Fingerprint]

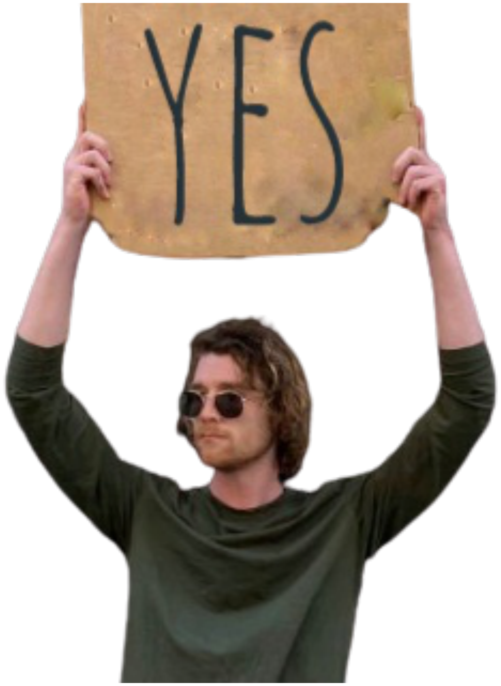
Usage

```
 _____  _____        _____ _____  ____
|  __ \|  __ \      / ____|  __ \|  _ \
| |  | | |  | | ___| (___ | |  | | |_) |
| |  | | |  | |/ _ \\___ \| |  | |  _ <
| |__| | |__| | (_) |___) | |__| | |_) |
|_____/|_____/ \___/_____/|_____/|____/

usage: new_dissector.py [options]

optional arguments:
  -h, --help            show this help message and exit
  --version             print version and exit
  -v, --verbose         print info msg
  -d, --debug           print debug info
```

FAQ

- Can I use the software without sharing my pcaps?
- Can I share anonymized pcaps?
- Can I help you to code the software?

- https://github.com/ddos-clearing-house



Summary

- IoT security is fundamental to protect/increase Internet stability
- Vulnerable IoT devices can be used to perform powerful DDoS attacks
- Mitigation solutions should take into account IoT devices

INTERSCT.

CONCORDIA

Cyber security cOmpeteNCe fOr Research anD InnovAtion

No More DDoS

Anti-DDoS-Coalitie

SIDN and SURF were partly funded by the European Union's Horizon 2020 Research and Innovation program under Grant Agreement No 830927. Project website: https://www.concordia-h2020.eu/

SIDN LABS

INTERSCT.

Thank you!

joao.ceron@sidn.nl

14 oktober 2020

SIDN LABS