DDoS Clearing House

João M. Ceron

SIDN Labs

(.nl)

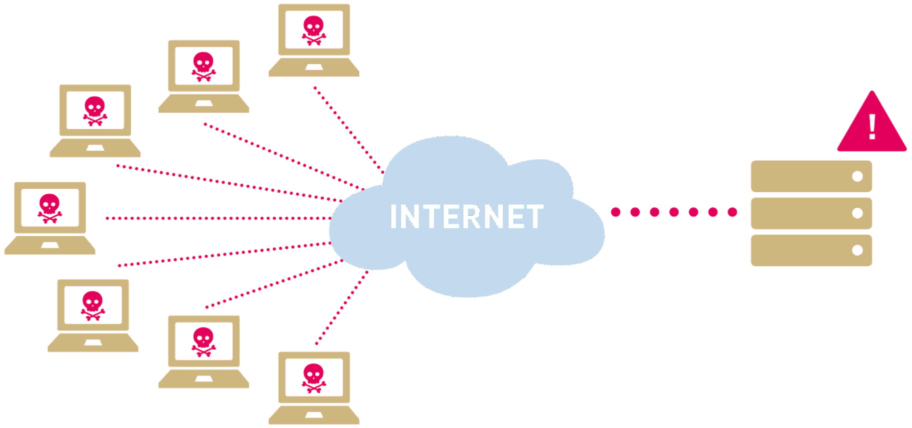
CENTR | 27 May 2020

Introduction

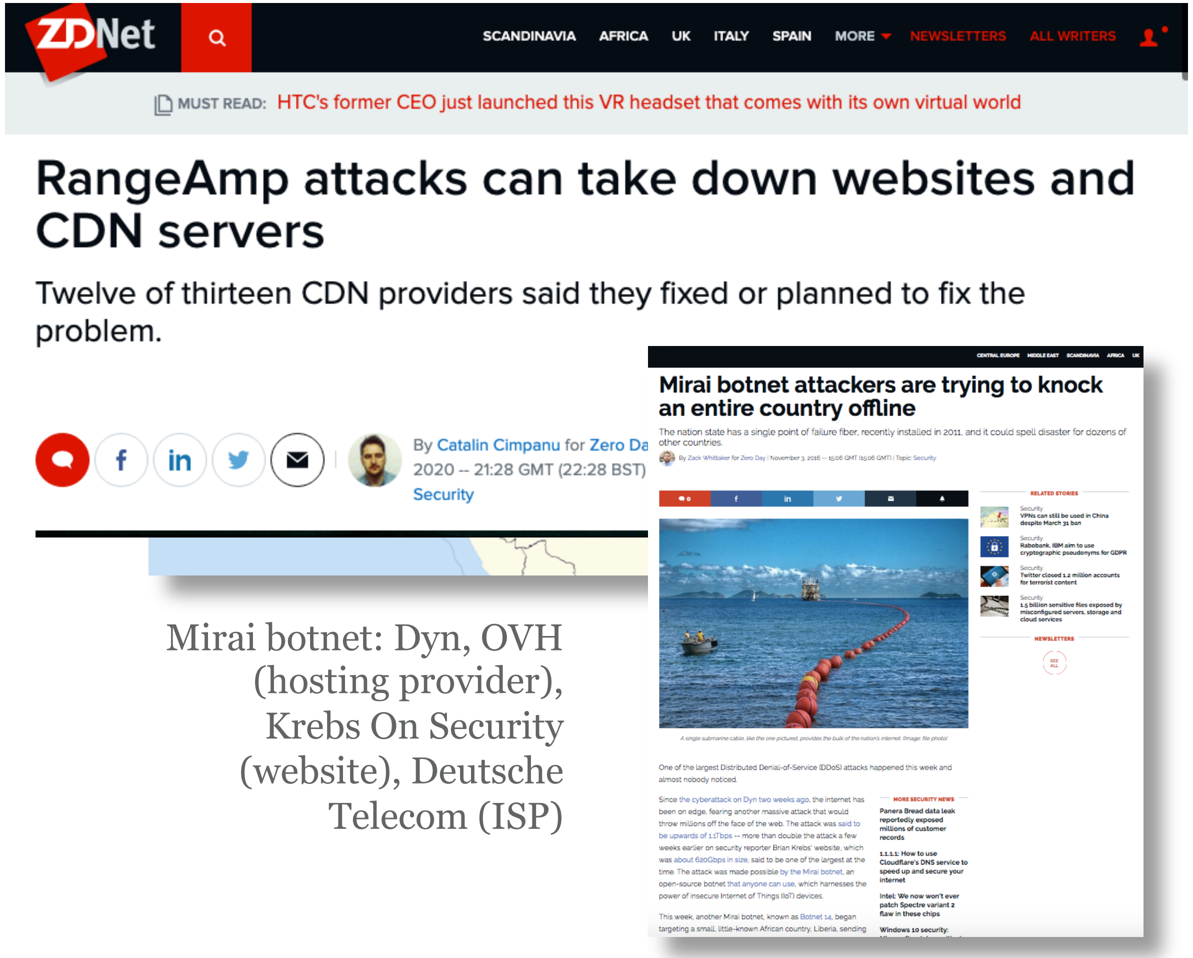
DDoS

- Distributed Denial of Services Attack
- Make service/machine unavailable
- Overwhelm the capacity of a site

Are DDoS attacks a problem nowadays?



DDoS Examples


ZDNet
SCANDINAVIA AFRICA UK ITALY SPAIN MORE NEWSLETTERS ALL WRITERS

MUST READ: HTC's former CEO just launched this VR headset that comes with its own virtual world

RangeAmp attacks can take down websites and CDN servers

Twelve of thirteen CDN providers said they fixed or planned to fix the problem.

By Catalin Cimpanu for Zero Da
2020 -- 21:28 GMT (22:28 BST)
Security

CENTRAL EUROPE MIDDLE EAST SCANDINAVIA AFRICA UK

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)

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

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

MORE SECURITY NEWS

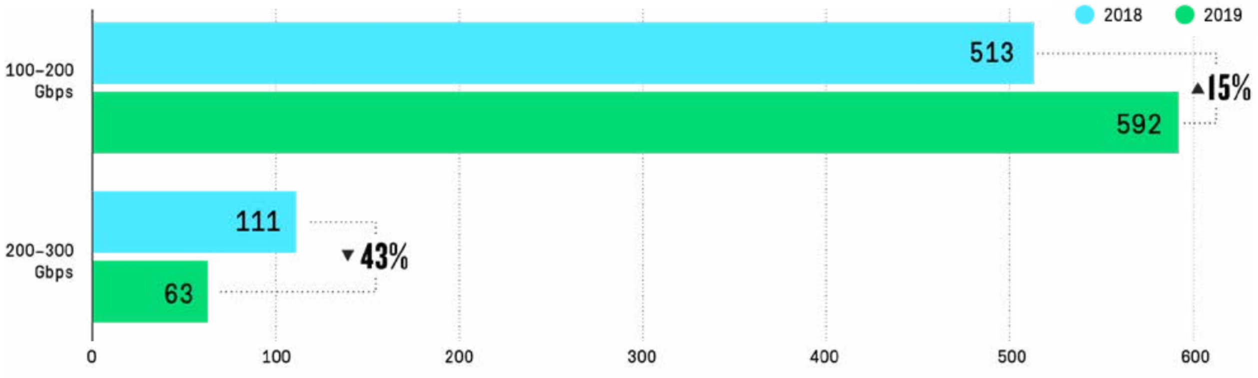
Panera Bread data leak reportedly exposed millions of customer records

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:

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



NETSCOUT report 2019

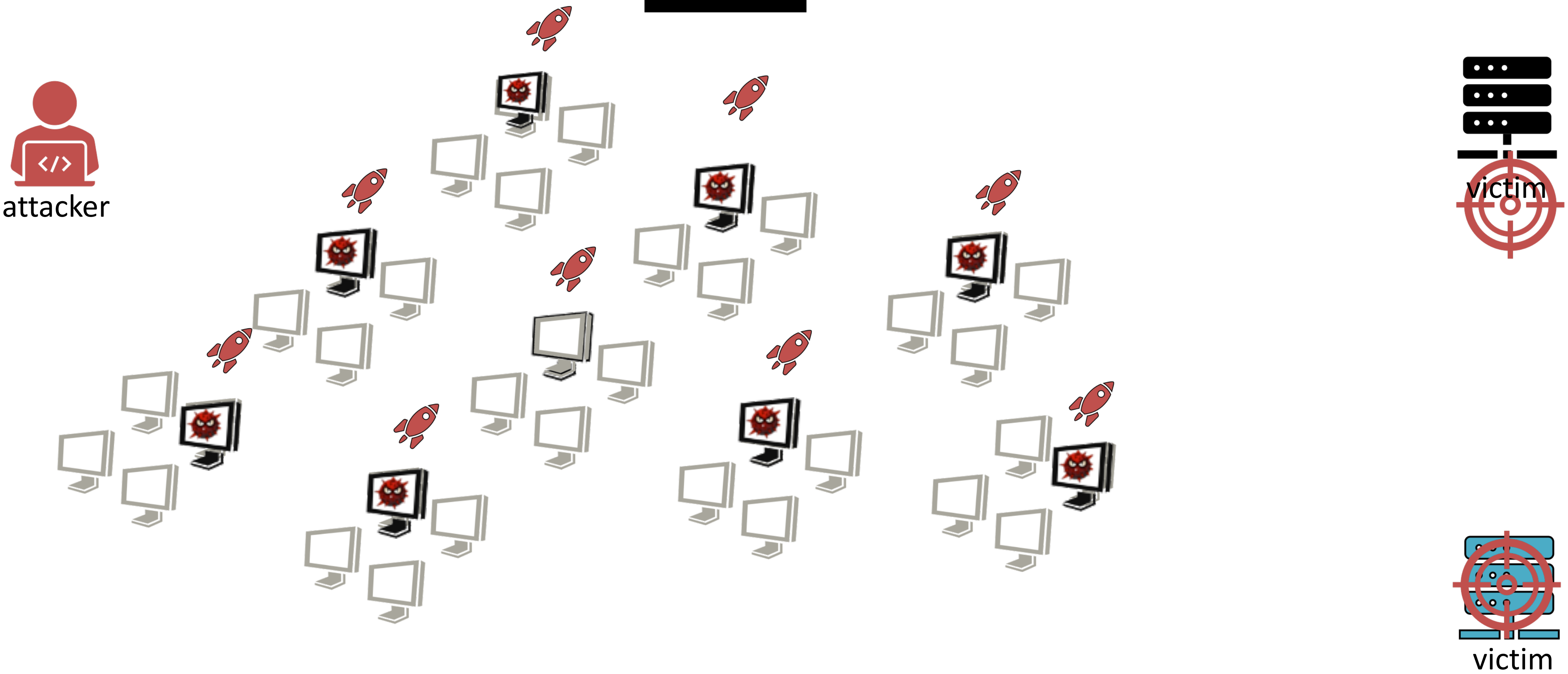
DDoS attacks: bigger, smarter and more frequent

Amplification attacks

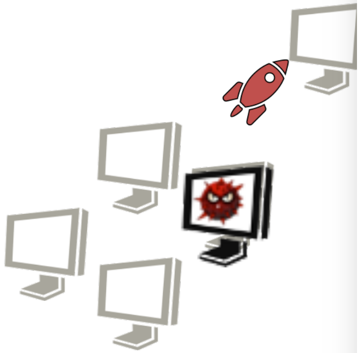
IoT

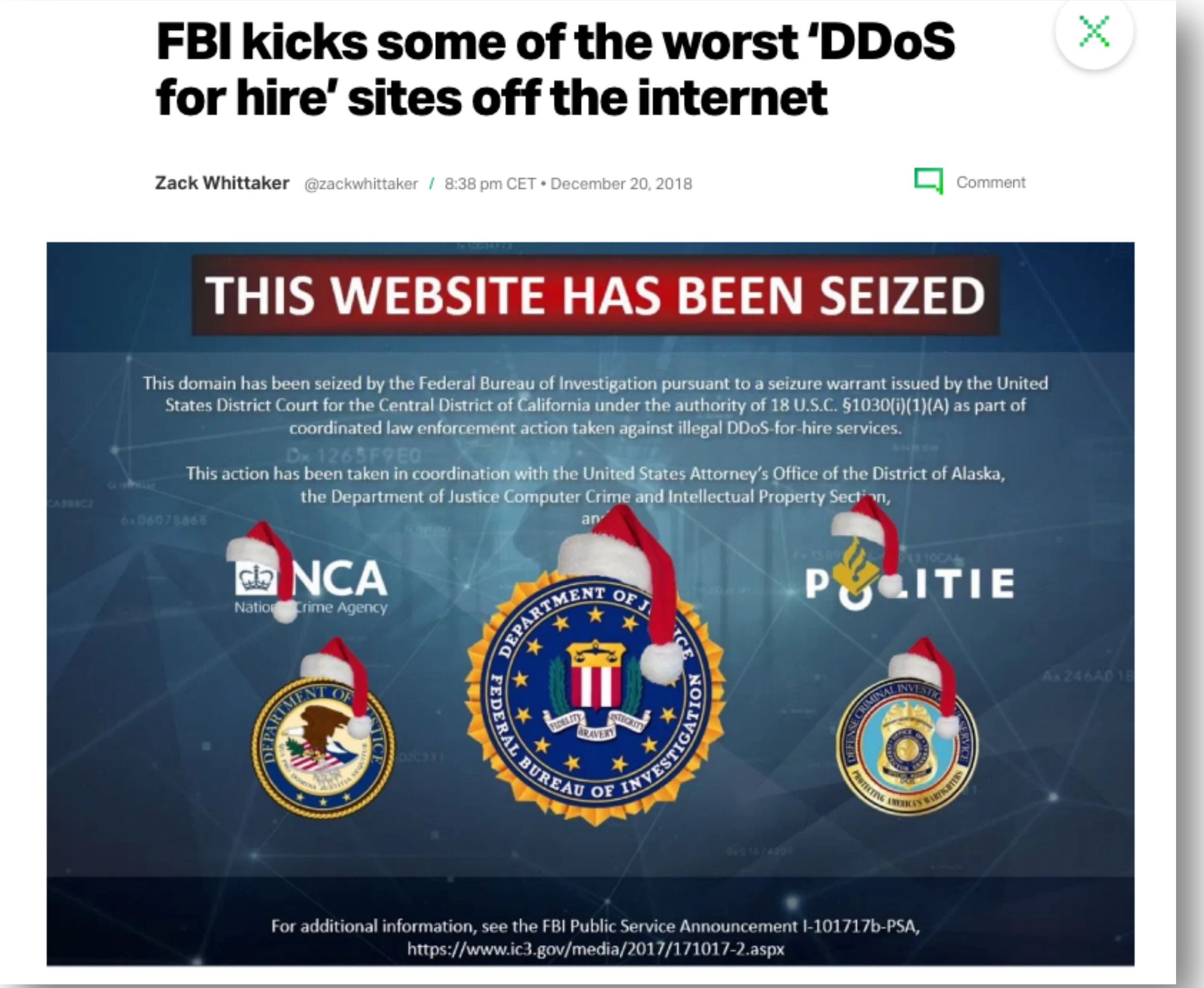
https://www. https://www.zdnet.com/article/mirai-botnet-attack-briefly-knocked-an-entire-country-offline/
zdnet.com/article/rangeamp-attacks-can-take-down-websites-and-cdn-servers/

Botnet



SOME ATTACKS HAVE THE SAME CHARACTERISTICS attacker





FBI kicks some of the worst 'DDoS for hire' sites off the internet

Zack Whittaker @zackwhittaker / 8:38 pm CET • December 20, 2018

Comment

THIS WEBSITE HAS BEEN SEIZED

This domain has been seized by the Federal Bureau of Investigation pursuant to a seizure warrant issued by the United States District Court for the Central District of California under the authority of 18 U.S.C. §1030(i)(1)(A) as part of coordinated law enforcement action taken against illegal DDoS-for-hire services.

This action has been taken in coordination with the United States Attorney's Office of the District of Alaska, the Department of Justice Computer Crime and Intellectual Property Sect n, an

For additional information, see the FBI Public Service Announcement I-101717b-PSA, https://www.ic3.gov/media/2017/171017-2.aspx

victim

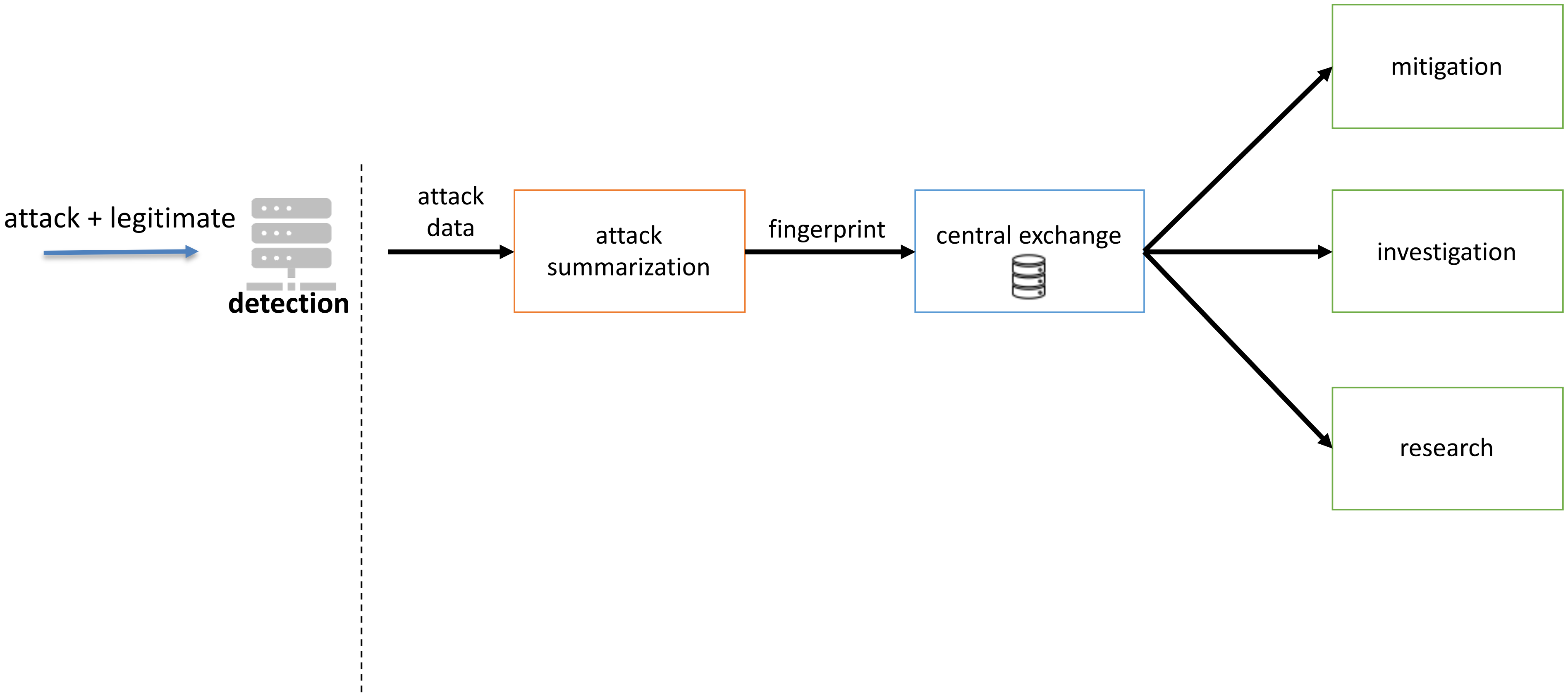
victim

DDoS Clearing House Concept

Platform for sharing DDoS Characteristics (fingerprints)

~~Detection~~

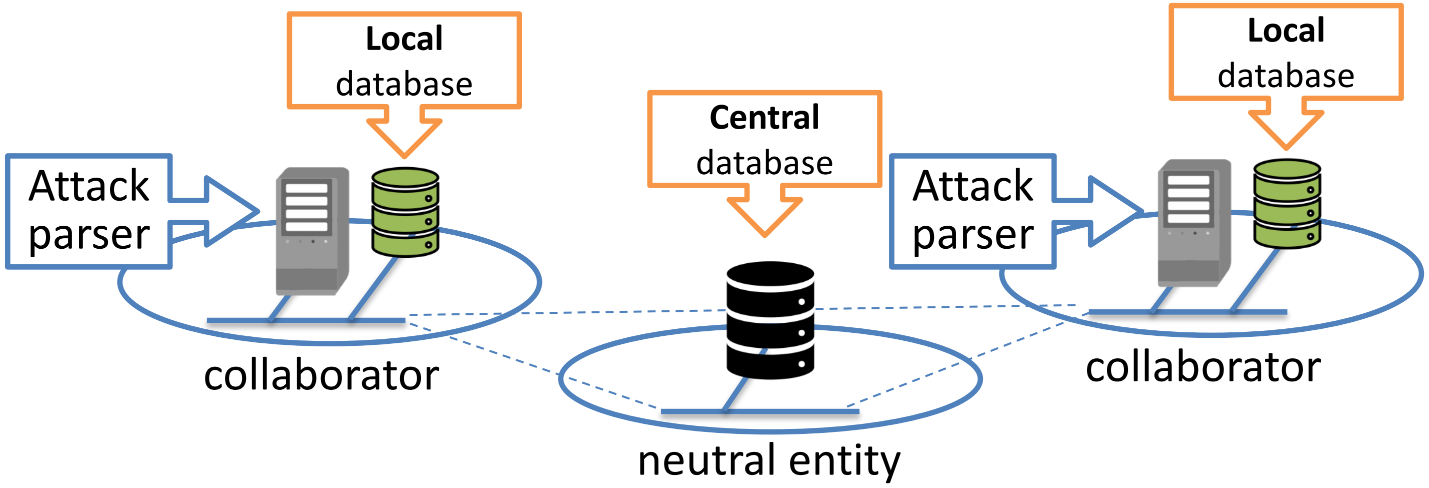
~~Mitigation~~



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



Project Objectives

- DDoS Clearing House with European industry

- Pilot
  - Netherlands
  - Italy

- Cookbook
  - Legal
  - Technical

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
http://www.nomoreddos.org/

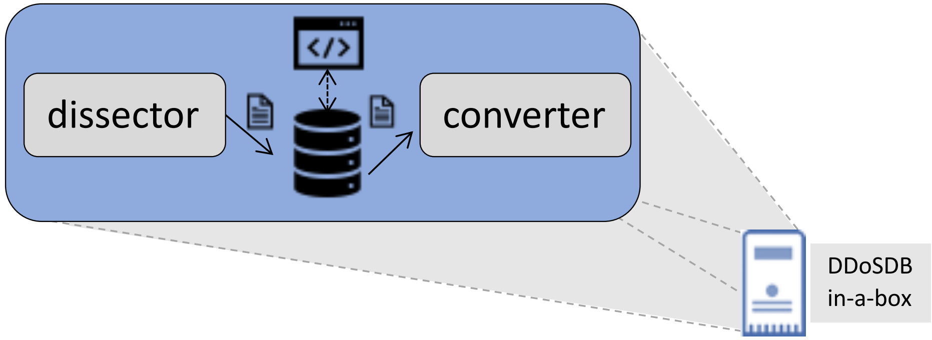
2019 Accomplishments

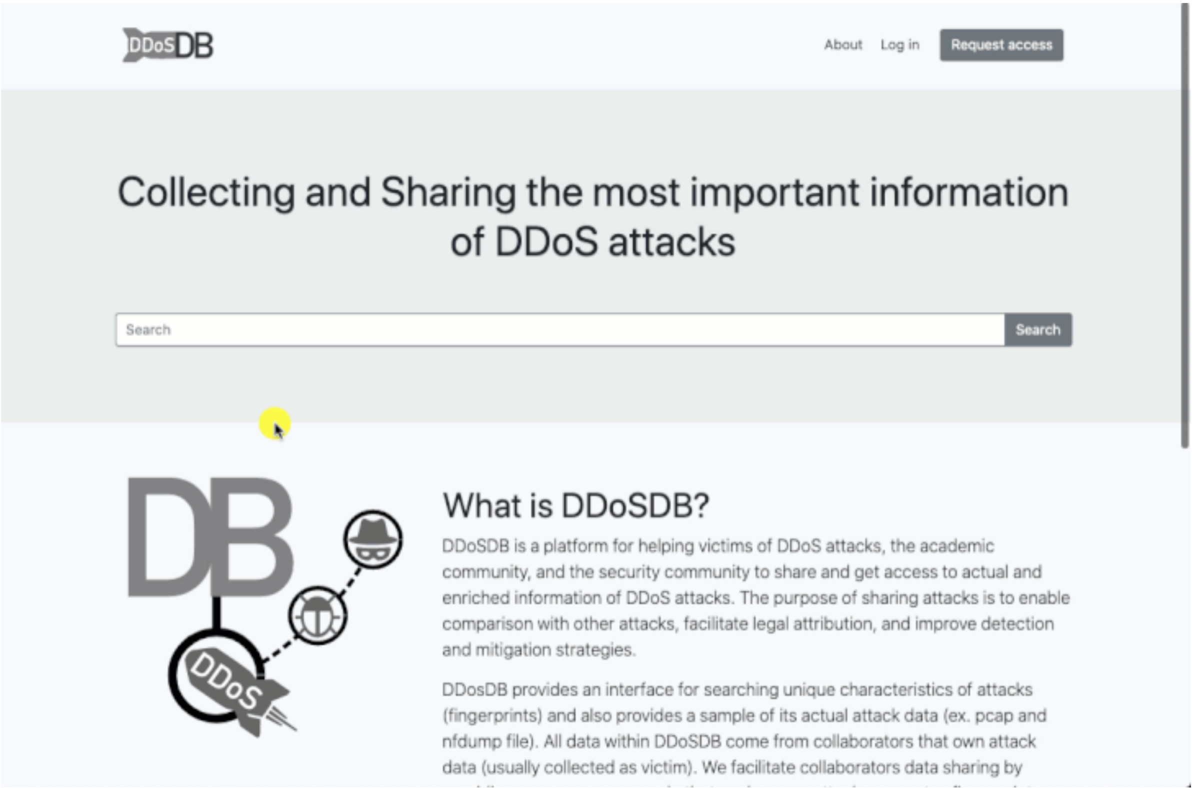
- Experimental setup (ddosdb.nl) pilot NL
- Draft data sharing agreement for pilot phase 1
- Draft overall architecture
- Extensive dissemination (e.g., One Conference, Open Door Event)

- **Key lesson learned: the legal part is much more time-consuming than the technical part**

2020 Plans

- NL pilot:
  - Translate the data sharing agreement from Dutch to English
  - Process DDoS attacks in regular basis
  - Share in non-production environment
  - Improve the software





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

Joins Us!

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

CONCORDIA

Cyber security cOmpeteNCe fOr Research anD InnovAtion

joao.ceron@sidn.nl

SIDN, SURFnet, and the University of Twente 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

Thank you.

SIDN LABS