

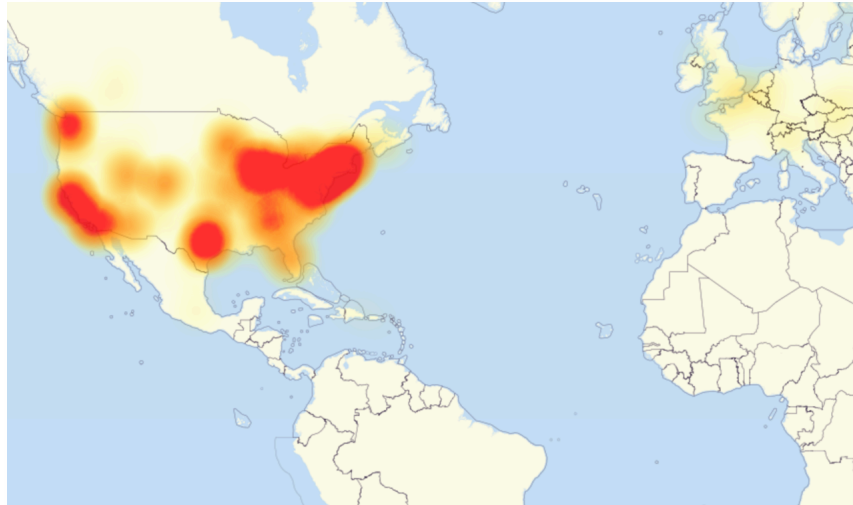
A light blue world map with white landmasses. A red circle highlights the Netherlands in Western Europe, with a red arrow pointing to it from the right.

# Increasing the resilience of the Netherlands' digital infrastructure together

**ISC2NL Cyber Resilience Event  
Amersfoort, the Netherlands  
May 28, 2019**

Cristian Hesselman (SIDN)

# DDoS examples



## 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

Home Nieuws Over DigiD Mochten Veiligheid Vraag en antwoord

DigiD

- DigiD aanvragen
- DigiD activeren
- Machtiging regelen
- Inloggen Mijn DigiD

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.

**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

Other targets: 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 spoil disaster for dozens of other countries.

By Zach Whitaker for Zero Day | November 3, 2016 - 10:48 (GMT-05:00) Topic: Security

RELATED STORIES

- Security: Why you still be used in China despite Huawei ban
- Security: Robobots, IBM aim to use cryptographic procedures for GDPR
- Security: Twitter closed a million accounts for terrorist content
- Security: 1.5 billion sensitive files exposed by misconfigured servers, storage and cloud services

NEWSLETTERS

ONE DAY

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 500Mbps 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 1a, began targeting a small, little-known African country, Liberia, sending

**MORE SECURITY NEWS**

- Parnera breach data leak reportedly exposed millions of customer records
- 1.5TB: 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 to security

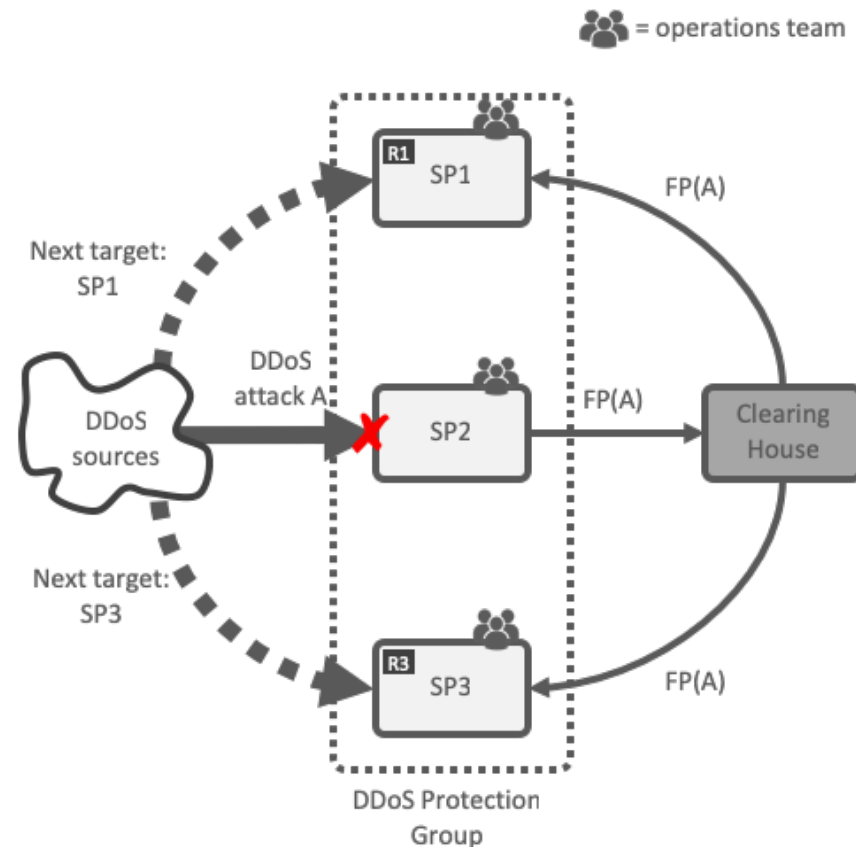
## A few DDoS trends

- Volume at 1+ Tbps, likely going up (Dyn 1.2 Tbps, GitHub 1.3 Tbps)
  - Many widely distributed sources (Mirai 600K, Hajime 400K)
  - High propagate rates (e.g., Mirai from 42K to 71K bots in 1 hour)
  - Complex traffic (e.g., bot churn, volumetric/TCP state exhaustion)
  - Easier to launch through booters/stressers (Mirai)
  - Reflection attacks possible (e.g., Mirai and Reaper botnets)
- ➔ Our society increasingly depends on network services!

- Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z., Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, “Understanding the Mirai Botnet”, 26th USENIX Security Symposium, 2017
- S. Herwig, K. Harvey, G. Hughey, R. Roberts, and D. Levin, “Measurement and Analysis of Hajime, a Peer-to-peer IoT Botnet”, Network and Distributed Systems Security (NDSS) Symposium 2019, San Diego, CA, USA, February 2019

## New: DDoS information sharing in NL

- 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
- Improves attribution, allowing for better prosecution and increased deterrent effects
- Open to all critical providers in the Netherlands (Internet, financial, energy, water, etc.)



# DDoS fingerprints = summary of DDoS traffic

- Domain names used, source IP addresses, protocol, packet length, no victim IP addresses
- Optional extensions: PCAPs, device-specific packet filter rules that ops teams used, suspected type of DDoS attack (e.g., Mirai or Hajime-powered), contact details of ops team
- Created from network measurements (e.g., PCAP, Netflow, IPFIX, sFlow, Logfile)

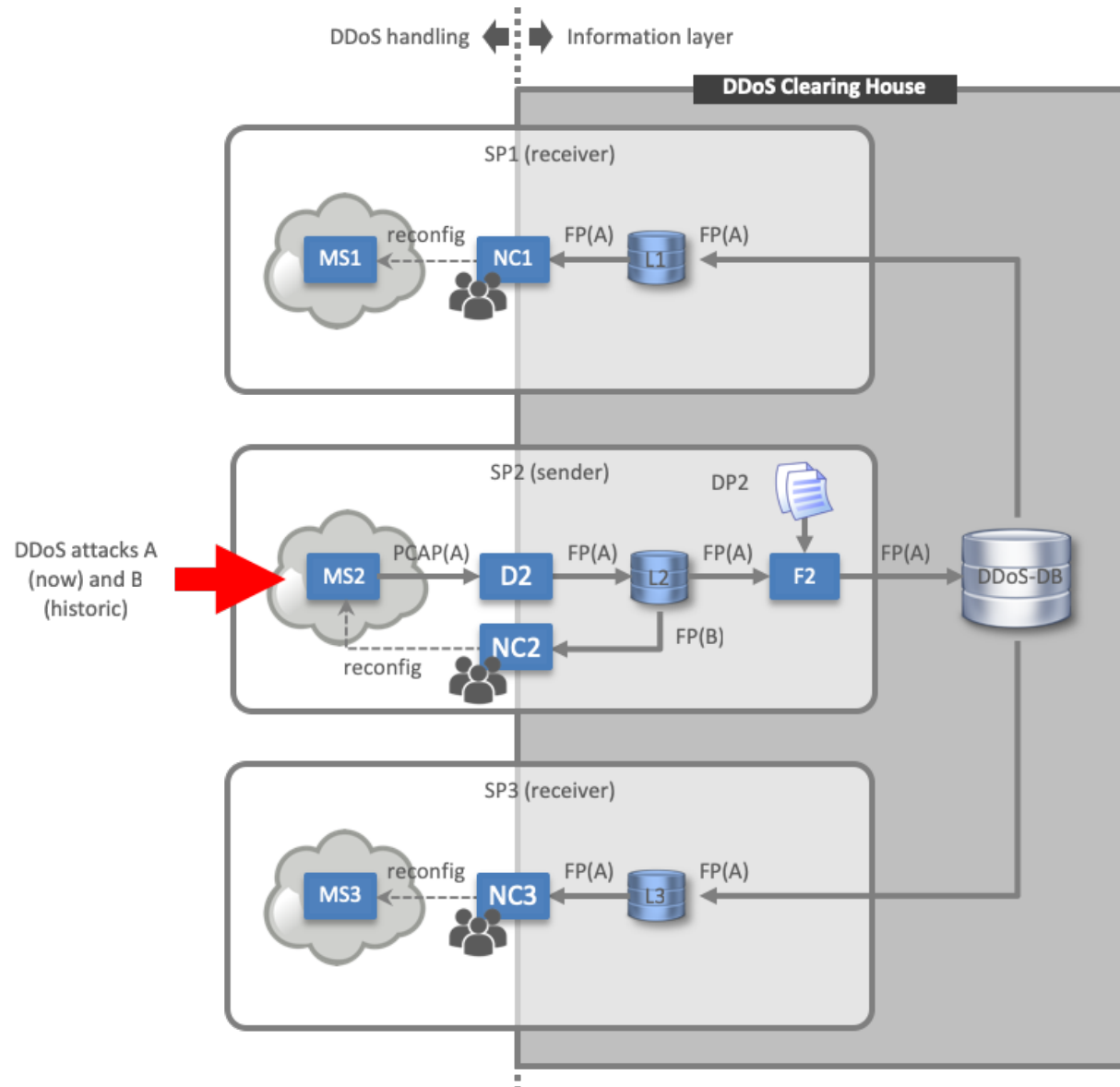
```
{
  file_type: "pcap"
  protocol: "DNS"
  additional: {
    dns_query: "6666.forfun.net"
    dns_type: 1.0
  }
  src_ips: [
    {
      ip: "10.1.1.1"
      ...
    }
  ]
  total_src_ips: 48
  src_ports: [
    9158
    18547
    23807
    22764
    31949
    55211
    7931
    57670
    25282
    10232
    ...
  ]
  total_src_ports: 1439
  dst_ports: [
    53
  ]
  total_dst_ports: 1
  key: "b49ce8969cef5f5ce15f4d29d3329d6"
  start_time: "2019-02-21 19:51:59"
  duration_sec: 4.447622060775757
  avg_pps: 15014.989827699528
  avg_bps: 1126124.2370774646
  multivector_key: "b49ce8969cef5f5ce15f4d29d3329d6"
  src_ips_size: 48
  blame: {
    name: "HelloWorld"
    description: "This is a test blame on a test fingerprint from a test user for testing purposes."
  }
}
```

```
{
  file_type: "pcap"
  protocol: "DNS"
  additional: {
    dns_query: "arctic.gov"
    dns_type: "255"
  }
  src_ips: [
    {
      ip: "46.175.17.69"
      ...
    }
  ]
  total_src_ips: 91412
  src_ports: [
    53
  ]
  total_src_ports: 1
  dst_ports: [
    26294
    7929
    54453
    16031
    60150
    45091
    26079
    60552
    26309
    45611
    ...
  ]
  total_dst_ports: 30284
  key: "b83fd600020362a3d8950315f60a91a3"
  start_time: "2019-03-07 18:58:41"
  duration_sec: 126.19218683242798
  avg_pps: 27128.43866115077
  avg_bps: 23728633.999950055
  multivector_key: "b83fd600020362a3d8950315f60a91a3"
  src_ips_size: 91412
}
```

Fingerprint - Attack trace

Compare

# Clearing house overall architecture (DRAFT)



## DDoS clearing house NL partners

- Embraced by a coalition of 25 players from industry (ISPs, xSPs, IXPs, banks, not-for-profit DPS) and gov't (ministries and agencies)
- Including various existing collaborative anti-DDoS initiatives, such as the Dutch Continuity Board (DCB), NoMoreDDoS, NBIP-NaWas
- Working groups:
  - Clearing house
  - Cross-industry information sharing
  - Outreach
  - Ground rules and incident response
  - Exercises
- Facilitated by Dutch National Cyber Security Centre (NCSC-NL)

# Status

- Technical track
  - Operational version of DDoS-DB based on open source prototype developed by the University of Twente
  - Closed user group: KPN, THTC, NBIP, NCSC-NL, SIDN, UT, NL-ix, VodafoneZiggo, Dutch Payment Association
- Legal track: data sharing agreement
  - Draft developed by legal experts of SIDN and KPN
  - Covers topics like governance, liability, and audits
  - Focus on simplicity, scalability (NL/EU), and various devops phases



# Next steps

- Pilot in the Netherlands (short-term)
  - Approach: start small and iteratively scale up to more partners
  - First share pre-generated fingerprints, then on-the-fly generated prints
- DDoS clearing house for Europe
  - Part of CONCORDIA project ([www.concordia-h2020.eu](http://www.concordia-h2020.eu))
  - Development of a clearing house “cookbook”
  - Second pilot in Italy
- Envisioned long-term growth paths
  - Netherlands → Europe → global
  - Extend to “non-critical” service providers





## Q&A

Cristian Hesselman  
Director SIDN Labs  
+31 6 25 07 87 33  
cristian.hesselman@sidn.nl  
@hesselma

The development of the Dutch national DDoS clearing house is a joint effort of NBIP-NaWas, KPN, THTC, NCSC-NL, Dutch Payment Association, VodafoneZiggo, NL-ix, SIDN, SURFnet, and the University of Twente (WG clearing house). 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.