

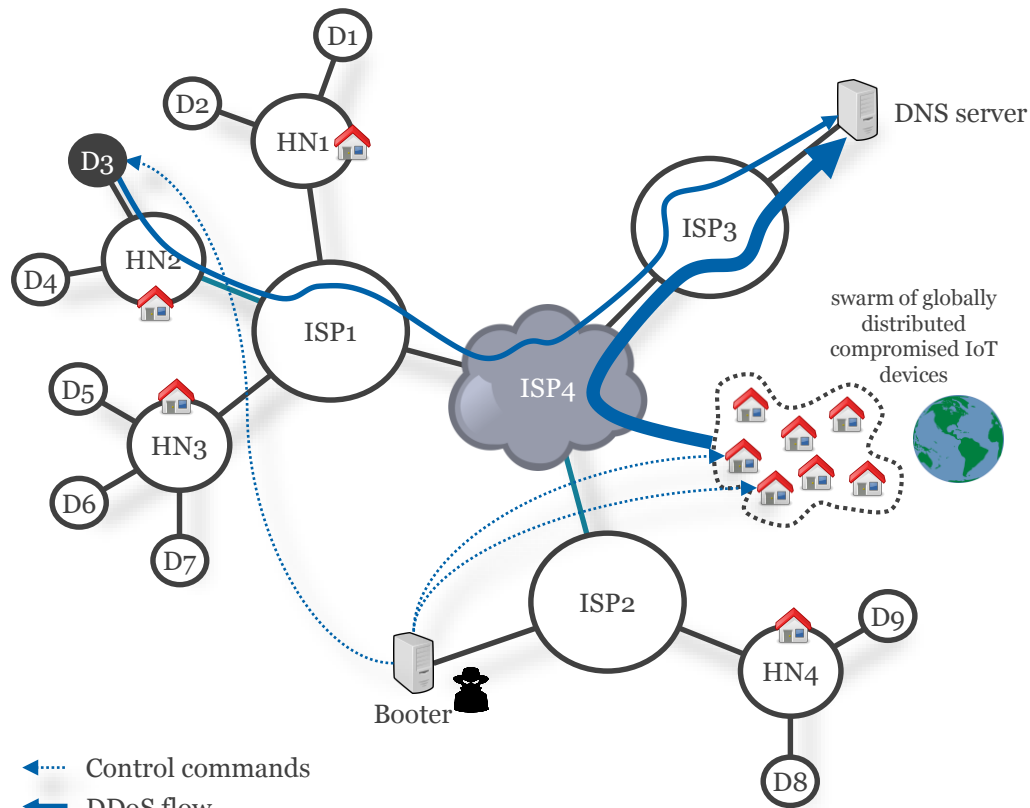
A proactive and collaborative DDoS mitigation strategy for the Dutch critical infrastructure

Cristian Hesselman¹, Jeroen van der Ham², Roland van Rijswijk³, Jair Santanna², Aiko Pras²

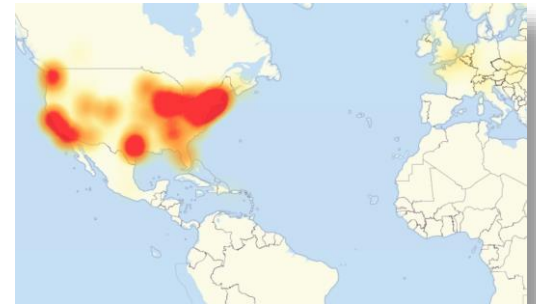
1) SIDN Labs, 2) University of Twente, 3) SURFnet

ccNSO Members Day #2 | ICANN62, Panama City | Jun 27, 2018

DDoS attacks (on the DNS)



- ⋯ Control commands
- DDoS flow
- HN = Home Network
- D = IoT device



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 -- 10:05 GMT (10:05 GMT) | Topic: Security

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 600Gbps 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
- 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

Other targets: OVH (hosting provider), Krebs On Security (website), Deutsche Telecom (ISP)

DDoS trends

- Volume at 1+ Tbps, likely going up (Dyn @ 1.2 Tbps, GitHub @ 1.3 Tbps)
- Many widely distributed DDoS sources (Mirai: 600K, bots all over the world)
- IoT bots mutating and spreading quickly (Mirai: 75-minute doubling time)
- Easier to launch through booters/stressers (Mirai)
- Combination of direct and reflection attacks (Mirai)
- DNS increasingly a high-profile target (DNS root 2015, Dyn 2016)

The Netherlands

- DDoS attacks on Dutch critical infrastructure operators (Jan 2018)
- Estimated 40 Gbps attacks resulted in service outages at several operators
- Reactive and individual DDoS mitigation strategy
 - (Commercial) DDoS protection services per critical service provider
 - Person-to-person incident response communications during attacks

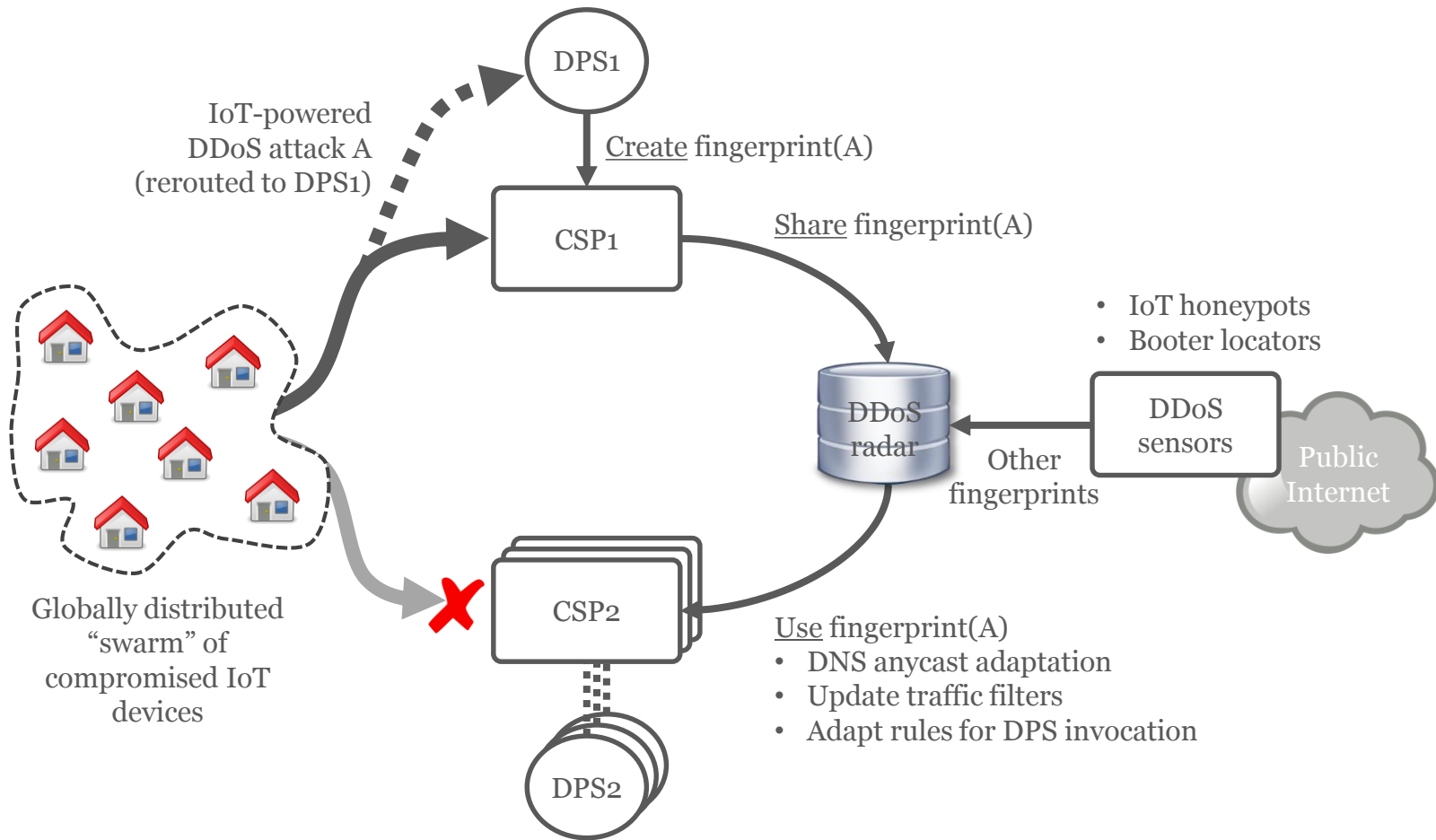


A screenshot of a news article from NOS (Dutch public broadcaster) titled "Na banken nu ook Belastingdienst en DigiD slachtoffer DDoS-aanvallen". The article is dated MA 29 JANUARI, 10:00 and is categorized under BINNENLAND, ECONOMIE. The article text reads: "De golf van DDoS-aanvallen op Nederlandse 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." The screenshot also shows a navigation bar with "Home", "Nieuws", "Over DigiD", "Machtigen", "Veiligheid", and "Vraag en antwoord". There are also sections for "Handige links" and "Laatste nieuws".

A proactive and collaborative strategy

- Improve information position of Dutch critical service providers by continually and automatically sharing fingerprints of actual and potential DDoS sources
- Widens view of critical service providers, enabling them to proactively prepare for attacks that have not hit them yet
- Information provisioning layer that extends existing DDoS protection services that Dutch critical service providers use and does not replace them
- Improve attribution of perpetrators and booter operators, allowing for better prosecution and increased deterrent effects
- Onboard all critical providers in NL (Internet, financial, energy, water, etc.)

DDoS radar (IoT example)



CSP = Critical Service Provider (e.g., a bank, ISP, or a registry)
DPS = DDoS Protection Service (e.g., Nawas or commercial such as Arbor)

Fingerprint

- Summary of DDoS traffic
 - Domain names used
 - Source IP addresses
 - Protocol
 - Packet length
- Created from traffic capture files like PCAPs
- Victim IP addresses not part of fingerprint
- Challenge: creation at high speed (10s of Gbps)

Status and next steps

- DDoS radar embraced by broad coalition of 25 players from industry (ISPs, xSPs, IXPs, banks, not-for-profit DPS) and gov't (ministries and agencies)
- Dutch Continuity Board (DCB) acts as springboard, supported by Dutch National Cyber Security Center (NCSC-NL)
- Develop DDoS radar based on existing components, such as
 - DDoS-DB of the University of Twente (ddosdb.org)
 - NaWas' DDoS pattern recognition system (ddos-patterns.net)
- Working groups: (1) clearing house, (2) cross-industry information sharing, (3) outreach, (4) ground rules and incident response, and (5) exercises

Longer-term

- Pilot part of an EU cybersecurity research project (under review) + development of a blueprint “business plan” to sustainably run (national) DDoS radars
- Envisioned growth path: (1) Netherlands → Europe → global and (2) extend to “non-critical” service providers

Q&A

Cristian Hesselman

Head of SIDN Labs

+31 6 25 07 87 33

cristian.hesselman@sidn.nl

@hesselma

Blog: https://www.sidnlabs.nl/a/news/a-proactive-and-collaborative-ddos-mitigation-strategy-for-the-dutch-critical-infrastructure?language_id=2



UNIVERSITY
OF TWENTE.

