Increasing Trust in the Internet

Triple I: a GFCE Capacity-building project

RIPE NCC Regional Meeting Almaty, 25 September 2018

Maarten Botterman

“What to do to improve justified trust in using the Internet and email in the region”

Purpose of the Day

Internet Infrastructure Initiative

- Aim: to help build a robust, transparent and resilient internet infrastructure.
- Rationale: A robust, open and resilient internet infrastructure is key to counter infringements and threats to the cyber domain, and increases justified trust, as it:
  - diminishes the chances and impact of cyber-attacks (like DDoS) and cybercrime (hacking malware, phishing, botnets) and SPAM.
  - enables the public to maintain confidence and trust;
  - is a precondition for the use of the internet as a means to boosting innovative and economic activities.
- Offering: this Initiative seeks to deepen and broaden the know-how in locally applying, testing and monitoring compliance with widely agreed open internet standards.
  - Key elements include national internet infrastructure protection, internet exchange points, registries, open source software, email security and routing security.

Setting up Capacity building events

- Targeted at regions that are catching up
- Bringing together regional stakeholders
- Awareness raising on Open Internet Standards
- Inspiration through Good Practice Examples
- Impact through joint commitment for action

Supported by global and regional stakeholders

- GFCE members
  - Governments
  - International Organisations
  - Businesses
- Regional Internet Registries
  - All regions
- Internet Society
  - Global office
  - Local chapters
- NL Ministry of Economic Affairs

Internet Society

lacnic

AFRINIC

APNIC

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

GFCE

AfricaCERT
United in promoting cyber security in Africa

Ministerie van Economische Zaken

PANEL AGENDA

Intro GFCE Triple-I

Maarten Botterman

Intro: Better Use of Today's Open Internet Standards

Hisham Ibrahim (RIPE NCC)

Inspiration from Good Practice: joint mitigation of DDOS

Aiko Pras (Professor, Twente University - via video)

Panel discussion: Increasing Trust in the use of Internet and e-mail

Kristina Hakobyan (CEO, Global AM); Yuriy Kargapolov, (Chair, ISOC IoT SIG); Talant Sultanov (Chair, Internet Society-Kyrgyz Chapter), Bakhrom Nasirjanov (Megafon Tajikistan)

From State-of-Practice to State-of-the-Art, together

Joint priority setting and action planning

- Almaty, Kazachstan, hosted by RIPE NCC, supported by RIPE/ISOC/Kazachstan Telecom, 25 September 2018
- Delhi, India, hosted by Indian Summerschool for Internet Governance, supported by ISOC/APNIC/Indian Govt, 12 October 2018
- Daejeon, Korea, hosted by APRICOT2019,supported by APNIC/ISOC/dotASIA, 23 February 2019

Next events under preparation

WWW.THEGFCE.COM

Help make the Internet more reliable in your region

1

Contribute with good practice examples to events

2

Support an event in your region as co-organizer or participant

3

Improve the reliability of Internet by taking action

Triple I is a GFCE project

www.thegfce.com

For more information contact:
maarten@gnksconsult.com

About Maarten Botterman

- More than 25 years experience with work “in the public interest”: where connected technologies touch society - internationally
- Independent analyst, strategic advisor, moderator and chairman, see for more: www.gnksconsult.com
- Currently chairing: IGF Dynamic Coalition on Internet of Things (www.iot-dynamic-coalition.org/); PICASSO Policy Expert Group (www.Picasso-project.eu), and Supervisory Board of NLnet Foundation (www.nlnet.nl.)
- ICANN Board Member (www.icann.org)
- Full CV: https://www.linkedin.com/in/botterman
- Email: maarten@gnksconsult.com

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

Cristian Hesselman[1], Jeroen van der Ham[2], Roland van Rijswijk[3], Jair Santanna[2], Aiko Pras[2]

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

Aiko Pras

Prof. Internet Security

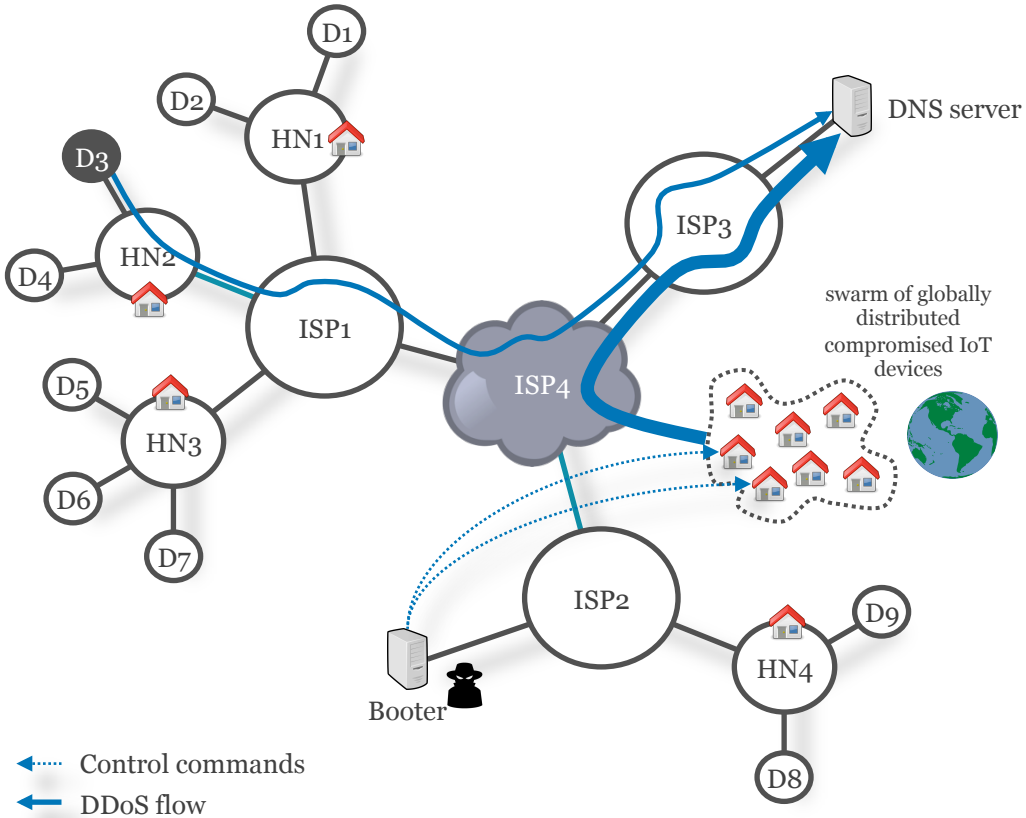
University of Twente

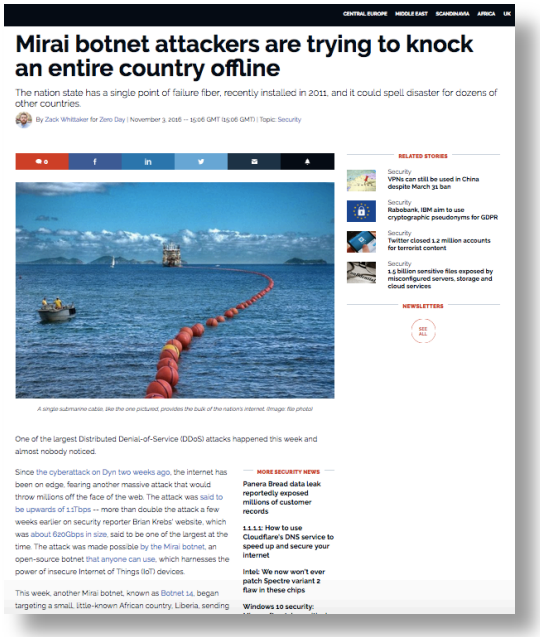
The Netherlands

https://people.utwente.nl/a.pras

SURF NET UNIVERSITY OF TWENTE. SDN LABS

DDoS attacks (on the DNS)





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

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

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

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:

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

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

SURFNET UNIVERSITY OF TWENTE. SDN LABS

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

NOS Nieuws Sport Uitzendingen TELETEKST AEX 423 km

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 Machtigen Veiligheid Vraag en antwoord zoek Sitemap Lees voor

DigiD

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

DigiD aanvragen
DigiD activeren
Machtiging regelen
Inloggen Mijn DigiD

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.

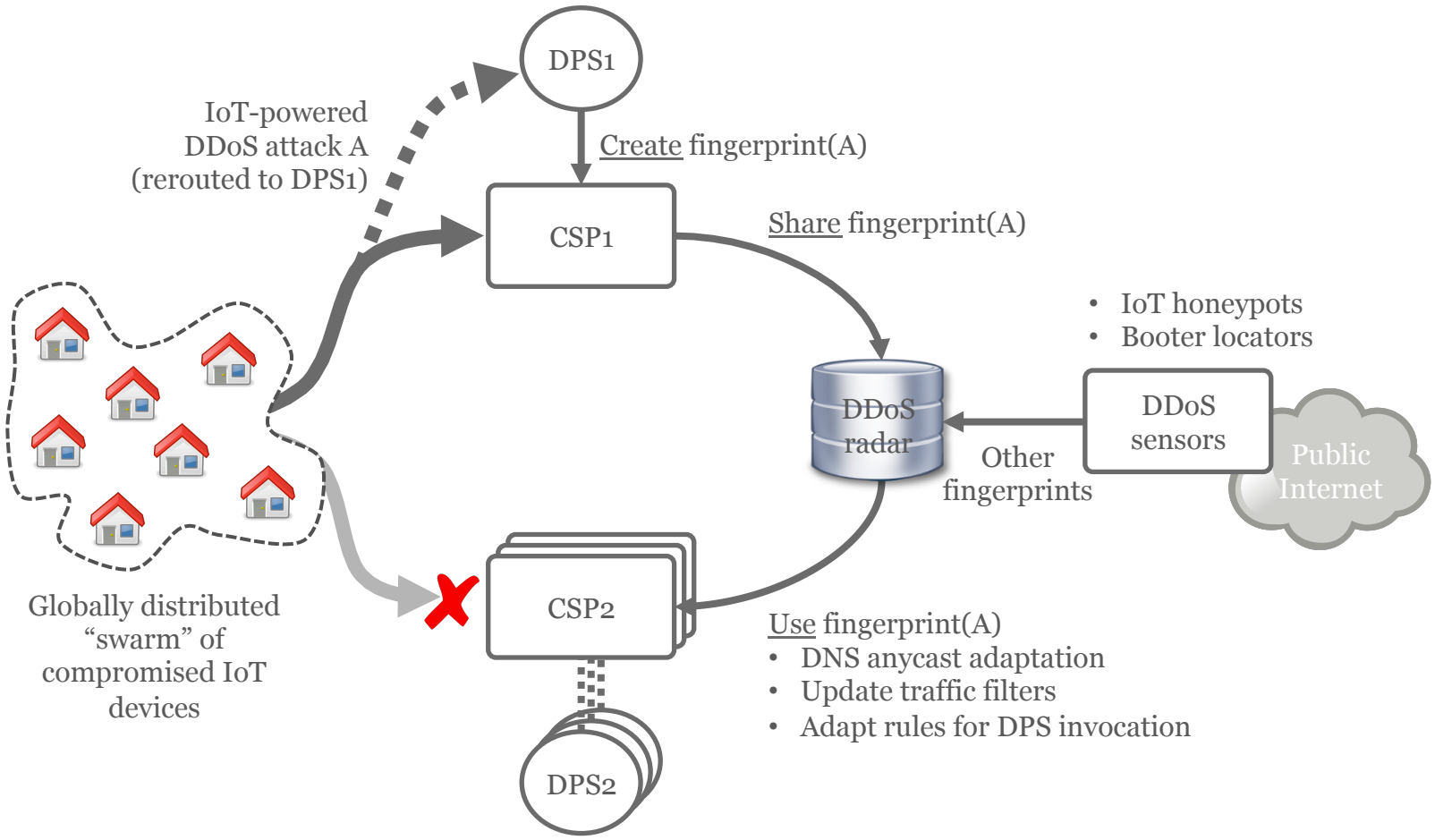
Volgens een woordvoerder van DigiD "gebeurt een aanval wel vaker, maar dit is wel zwaar". Er wordt hard gewerkt aan een oplossing. Hoelang dat nog gaat duren, kan de woordvoerder niet zeggen.

SURF NET UNIVERSITY OF TWENTE. SIDN LABS

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)

SURF NET UNIVERSITY OF TWENTE. SDN LABS

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 (CONCORDIA) + 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