Collaboratively increasing the resilience of critical services in the Netherlands through a national DDoS clearing house

Internet Infrastructure Security Day at APRICOT2019
February 23, 2019
Daejeon, South Korea

Cristian Hesselman (SIDN)

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)

➔ At the same time, our societies increasingly depend 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

Netherlands critical infrastructure

- Services whose “failure or disruption … would result in severe social disruption and poses a threat to national security” (NL gov’t)
- Providers protect their services through (3rd party) DDoS mitigation systems (e.g., scrubbing)
- Limited DDoS information sharing, focus on person-to-person comms during attacks (reactive)
- Trigger to change: estimated 40 Gbps DDoS attacks in January 2018, resulting in various service outages

NOS Nieuws Sport Uitzendingen TELEBLIK 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.

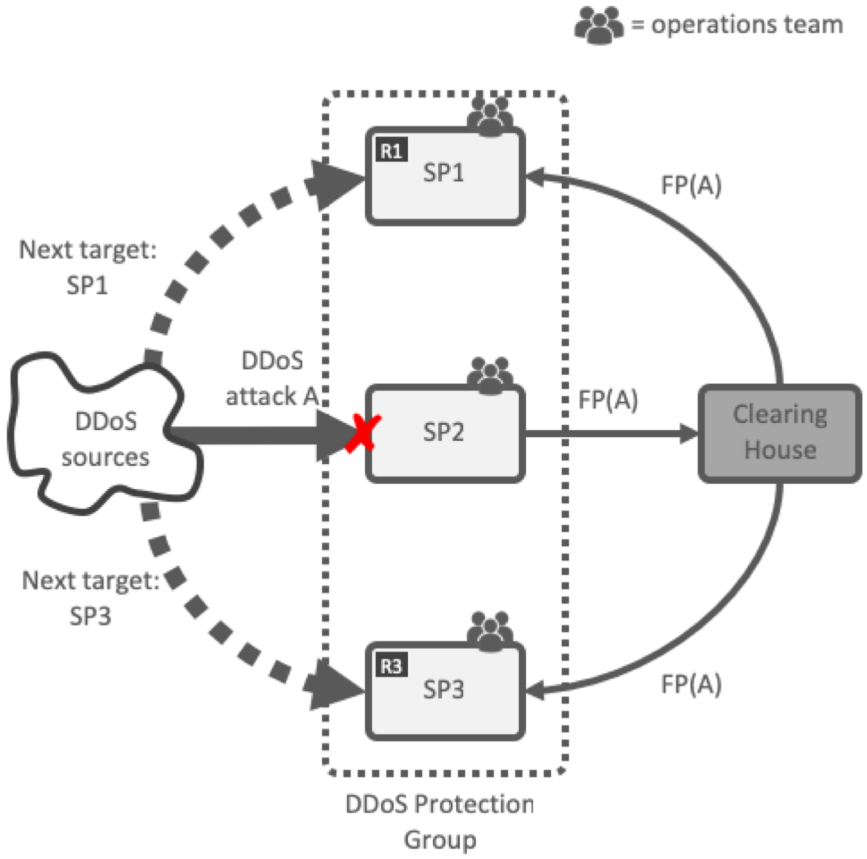
undefined ANP

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.

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!
- Created from network measurements
  - Examples: PCAP files, Netflow, IPFIX, sFlow, and Logfile
- Fingerprint extension records (optional)
  - 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
- Challenge: creation at high speed (10s of Gbps)

Status

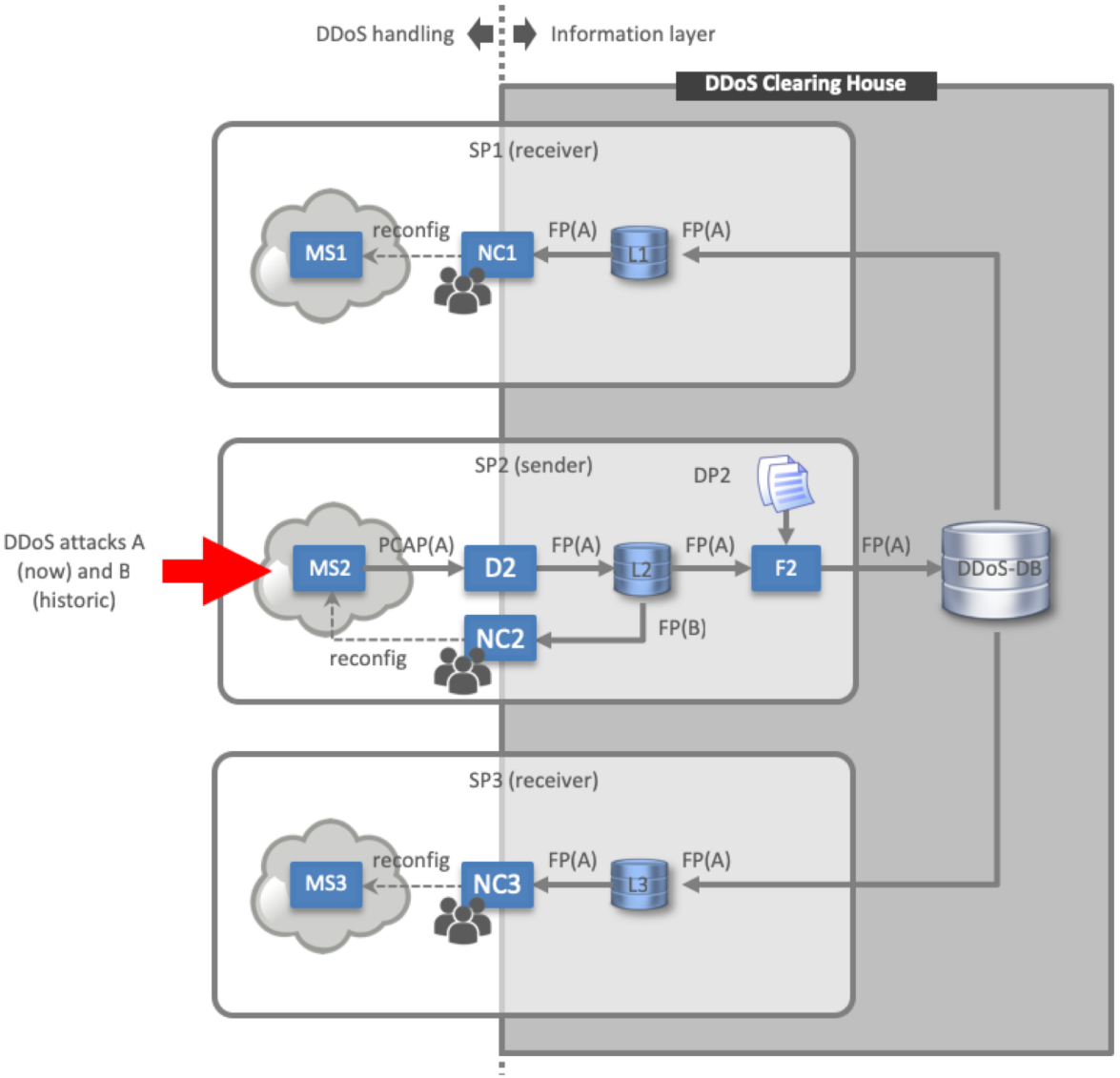
- Embraced by a coalition of 25 players from industry (ISPs, xSPs, IXPs, banks, not-for-profit DPS) and gov't (ministries and agencies)

- Including various existing collaborative anti-DDoS initiatives, such as the Dutch Continuity Board (DCB), NoMoreDDoS, and 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)

Clearing house overall architecture (DRAFT)



Clearing house pilot

- Netherlands
  - Approach: start small and iteratively scale up to more partners
  - Infra operators: NBIP, KPN, VodafoneZiggo, NL-ix, SIDN
  - Government: THTC, NCSC-NL
  - Financial: Dutch Payment Association
  - Research: University of Twente
- European Union
  - Part of CONCORDIA project (www.concordia-h2020.eu)
  - Development of a “cookbook” to run system in multiple member states
  - Use cases are pilot in the Netherlands and a second one in Italy
- Develop clearing house
  - Extend and improve existing components
  - DDoS-DB of the University of Twente (ddosdb.org)
  - NBIP’s DDoS pattern recognition system (ddos-patterns.net)

Next steps

- Initial version of NL pilot
  - Setting up joint development and experimentation environment
  - First share pre-generated fingerprints, then on-the-fly generated prints
- Agree on and flesh out charter/manifesto
  - WG Ground rules and incident response
- Envisioned growth paths
  - Netherlands → Europe → global (e.g., through CONCORDIA)
  - 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, KPN, THTC, NCSC-NL, Dutch Payment Association, VodafoneZiggo, NL-ix, SIDN, and the University of Twente (WG clearing house). SIDN and the University of Twente were partly funded by the European Union's Horizon 2020 Research and Innovation program under Grant Agreement No 830927.