



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

**Regional Triple-I Meeting
October 12, 2018
New Delhi, India**

Cristian Hesselman

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, all over the world)
 - Bots spreading quickly (Mirai: 75-minute doubling time)
 - Easier to launch through booters/stressers (Mirai)
 - Combination of direct and reflection attacks (Mirai)
- ➔ At the same time, increased dependency on network services

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, focuses on person-to-person comms during attacks (reactive)
- Trigger to change: estimated 40 Gbps DDoS attacks in January 2018, resulting in various service outages

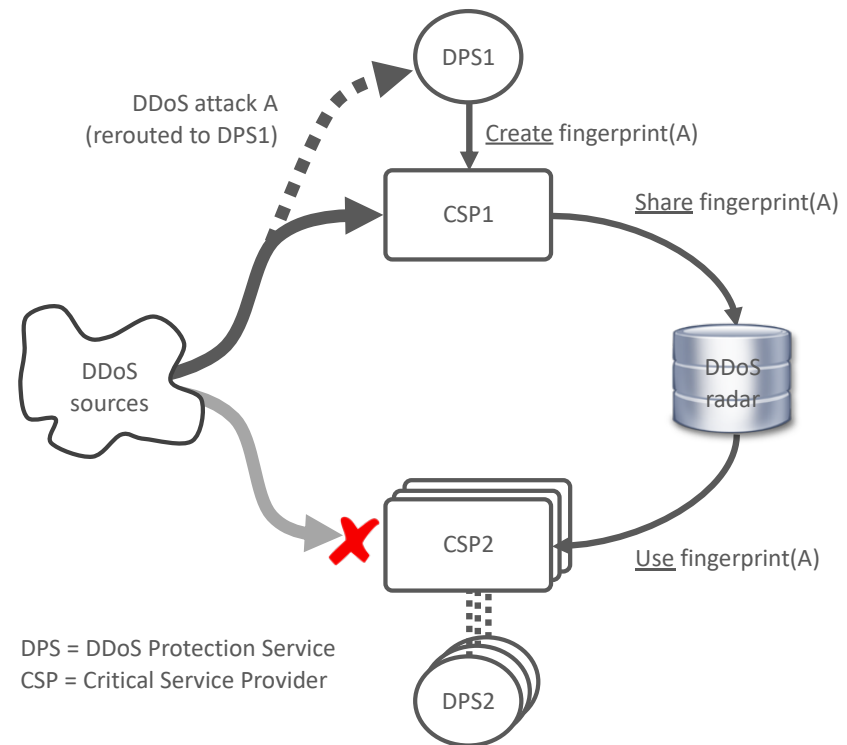


The screenshot shows the NOS website with a news article titled "Na banken nu ook Belastingdienst en DigiD slachtoffer DDoS-aanvallen". The article is dated 9 January 2018 and reports that DigiD is currently unavailable due to a DDoS attack. The website interface includes a navigation bar with "NOS", "Nieuws", "Sport", and "Uitzendingen". The article content includes a sub-header "DigiD: Je eigen inlogcode voor de hele overheid" and a list of "Handige links" such as "Wachtwoord vergeten?", "Nieuw mobiel nummer opgeven?", and "Herstelde ontvanger?". A "Laatste nieuws" section lists updates about DigiD's availability and system changes. The article text states that the wave of DDoS attacks on Dutch institutions continues, with the tax authority being hit twice and DigiD being unavailable for 15.45 hours. A quote from a DigiD spokesperson is also included.



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
- Created from traffic capture files like PCAPs
- Victim IP addresses not part of fingerprint
- Challenge: creation at high speed (10s of Gbps)

Status

- System part of 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 Center (NCSC-NL)

Next Steps

- Agree on and flesh out charter/manifesto
- Develop clearing house, using existing components
 - DDoS-DB of the University of Twente (ddosdb.org)
 - NaWas' DDoS pattern recognition system (ddos-patterns.net)
- Pilot system with several partners
 - Including development of a “cookbook” to run system elsewhere
 - Operational, legal, financial, and governance aspects
 - Part of the work taking place in an EU cybersecurity research project
- Envisioned growth paths
 - Netherlands → Europe → global
 - 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](#)