Increasing trust in the digital infrastructure through a national DDoS clearing house

Internet Infrastructure Initiative Day
Africa Internet Summit (AIS2019)
Sun Jun 16, 2019
Kampala, Uganda

Cristian Hesselman (SIDN)
DDoS examples

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


January 2018
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!

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)
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)
  – Development of a clearing house “cookbook”
  – Second pilot in Italy

• Envisioned long-term growth paths
  – Netherlands → Europe → global
  – Extend to “non-critical” service providers
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.