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)

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


Control commands

DDoS flow

HN = Home Network
D = IoT device
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 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