Dutch Continuity Board

Protecting The Netherlands against DDoS attacks.

About us
How we work
What does DDOS look like?
How do DDoS attacks work?
How does Anti-DDOS work?

1. Traffic is actively monitored.
2. During an attack, the traffic gets redirected to a mitigation center to get "scrubbed".
3. Legitimate traffic gets sent back to the customer site as the DDOS traffic gets removed.

- Legitimate traffic during normal conditions
- Denial of Service Traffic
- Monitoring Facility
- Internet
- Customer Site
- Mitigation Facility Centers
- Legitimate Traffic
- Denial of Service Traffic

Legitimate traffic normal conditions  DoS attack traffic  Legitimate traffic during attack
Observations

- Anonymous and hactivism on the rise

- Rise in multi-vector, volumetric attacks, longer duration

- **UDP Fragment, NTP, DNS amplification**, and **Chargen** still most popular

- Application level attacks on the rise

- Cloudflare and Spamhaus = 300 GB

- Latest American Observed DDOS = 1.7 TB
Dutch Continuity Board is similar to Abuse-IX. Dutch Continuity Board can share information and shut down traffic during incidents as well as regular process on malicious traffic, open resolvers, and other sources of attacks. This currently is supported by all Telco’s as well as NCSC; VNO NCW; NED ICT and is regarded favorably by EZ.
DCB Charter

- Structural cooperation among operators to mitigate severe DDoS attacks

- DCB resides under the Telecom ISAC and closely cooperates with other entities:
  - o-IRT-o
  - ICT response board
  - OPS-Trust DDoS working group

- Share information and best practices between operators

- BCP 38, 84, MANRS
Graduated levels of Readiness

DEFCON 5 FADE OUT

Customer base
Mobile
Home
Business

Access & Aggregation layer

Core Layer

Edge Layer

DDoS

Services

Internet Exchanges
Upstream providers
Private Networking Interconnects
Voice
TV
ISP services

Situation: Normal readiness..
Graduated levels of Readiness

DEFCON 4 DOUBLE TAKE

**Situation:** Anti-DDOS.nl traffic washing in effect.
Graduated levels of Readiness

DEFCON 3 ROUND HOUSE

Situation: Anti-DDOS.nl in effect with selective Black holing.
**Situation:** Malicious traffic is filtered on provider edge routers through Flowspec. Customer experience on average normal services. Possible some additional latency.
Situation: Malicious traffic is filtered on upstream(partner) providers edge routers. This solves congestion of links towards upstream/PNI providers. Customer traffic will recover.
Situation: Internet is down. Customers only can reach DCB partner infrastructure
Graduated levels of Readiness

**DEFCON 0 TELCO AUTONOMOUS**

**Situation:** Internet IS DOWN. Customers only can reach ISP services
Technical Approach

- Implementing required whitelists / blacklists at single operator.
- Implementing BGP Flow Specification by operators.
- Implementation of BCP38 by all operators would help significantly.
- Customers can acquire anti DDoS scrubbing service.
- Customer can effectively shut himself for DDoS by stopping export of certain routes to the internet.
Inter-operator cooperation

- It is the responsibility of the Telco provider to safeguard its customers from malicious network attacks.

- good due diligence in eliminating the source of the problems results in a good stable end-state.

- A single Telco provider cannot do this on their own, collaboration here between telcos is crucial for success. Each Telco is dependent on network due diligence of the up and downstream partner.

- Prevention and detection best practice is to eliminate problems at the source.
Inter-operator cooperation
Tooling

NetFlow to determine the source of the attack
Inter-operator cooperation
Tooling

DNS Traffic examination to block the use of malicious domains
Inter-operator cooperation
Routing Diversity as an Asset

Operator have different upstream providers which broadens their view on the source of the attack
Issues resolution through Inter-operator cooperation
Follow standards and truly work together in ops

- **Anti-Spoofing** = BCP 38 & 84
  - ingress filtering as a technique to ensure that incoming packets are actually from the networks from which they claim to originate

- **Routing Resilience Manifesto (MANRS)**
  - Provide a framework for ISPs to better understand and help address issues related to resilience and security of the Internet’s global routing system

- **Hierarchical Protocols** – DNS; NTP ; CAs

- **Upstreams embrace RPKI** – BGP : DNS SEC for DNS

- **NTP & use of Atomic Clocks**

- **Internet Abuse = Abuse –IX cooperation**

- **Mobile Abuse and resilience = GSMA WARP**

- **Fingerprint Booter & Stressors and share knowledge**
Board Members

- kpn
- T-Mobile
- Ziggo
- TELE2
- ZEELANDNET
- vodafone
- amsix
- SIDN
- UNIVERSITY OF TWENTE.