# DDoS Mitigation Service @Belnet
# &
# Case Study Ministry of Finance

Julien Dandoy, FODFin Technical Architect
Grégory Degueldre, Belnet Network Architect

Belnet
dedicated connectivity

.be

# Agenda

- DDoS : Definition and types
- DDoS Mitigation @ Belnet before
- DDoS Mitigation Service:  Architecture and characteristics
- Experience sharing from Ministry of Finance

# DoS : Definition

DoS – Denial of Service

A Denial of Service attack is an attempt to render a machine or network resource **unavailable to its intended users**, by temporarily or indefinitely **disrupting the services** of a host connected to the Internet.

What resources?

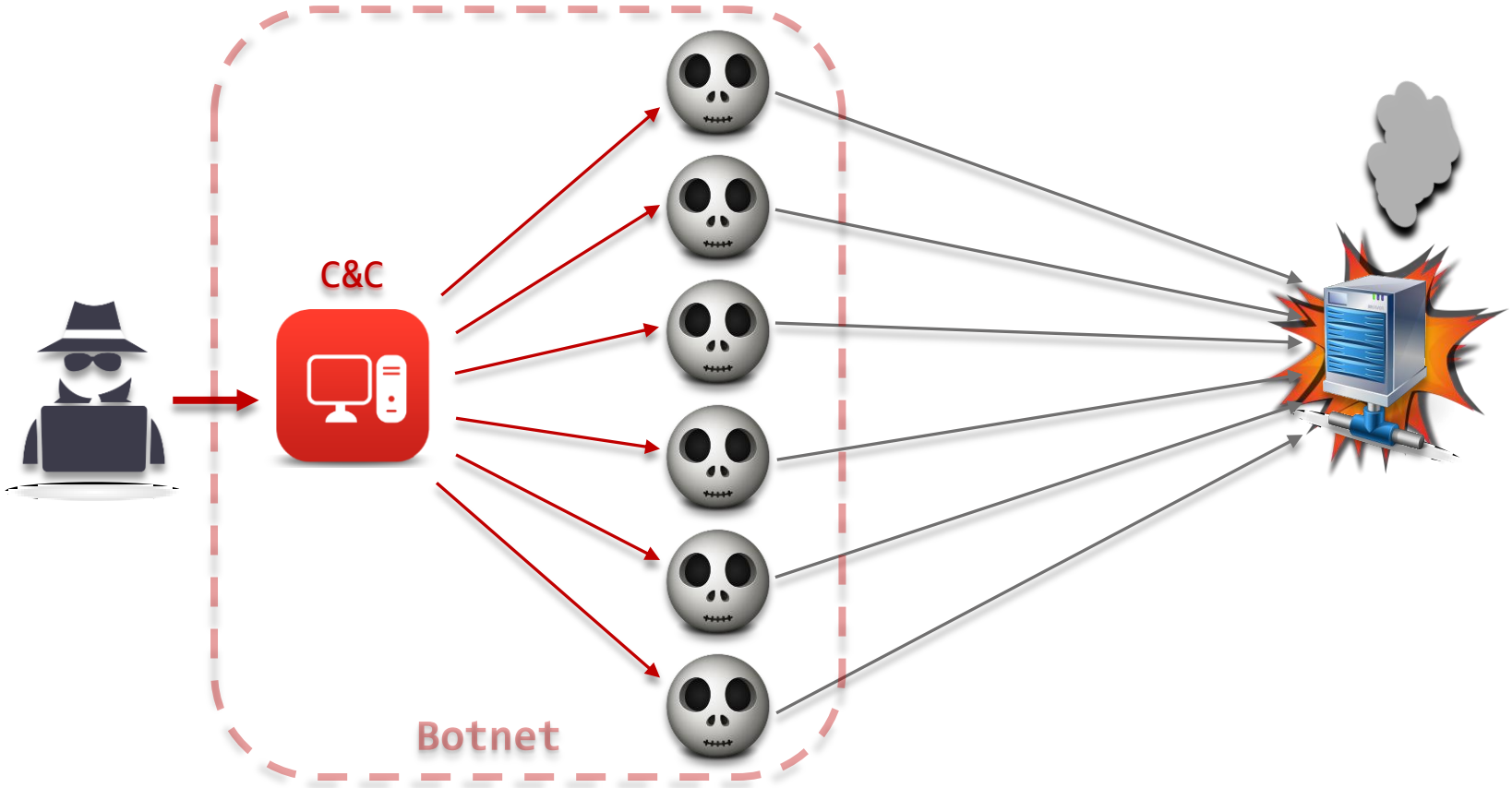
- Network server, client or router
- Network link or entire network
- …

- D DoS – **Distributed** Denial of Service
  - The attack originates not from one or a few machines, but is distributed across **a vast amount of attacking machines** all over the internet



Belnet dedicated connectivity

# DDoS : So how does it work?






Belnet
dedicated connectivity

# DDoS types

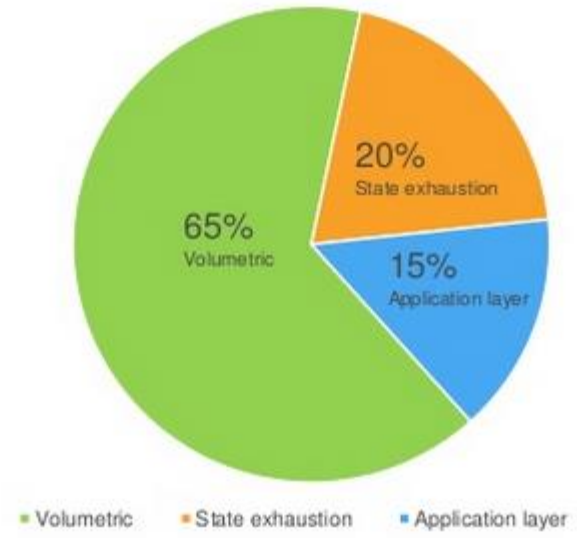
| Layer | Function |
|---|---|
| Application (7) | Services that are used with end user applications |
| Presentation (6) | Formats the data so that it can be viewed by the user<br><br>Encrypt and decrypt |
| Session (5) | Establishes/ends connections between two hosts |
| Transport (4) | Responsible for the transport protocol and error handling |
| Network (3) | Reads the IP address form the packet. |
| Data Link (2) | Reads the MAC address from the data packet |
| Physical (1) | Send data on to the physical wire. |

**Application-layer DDoS attack**

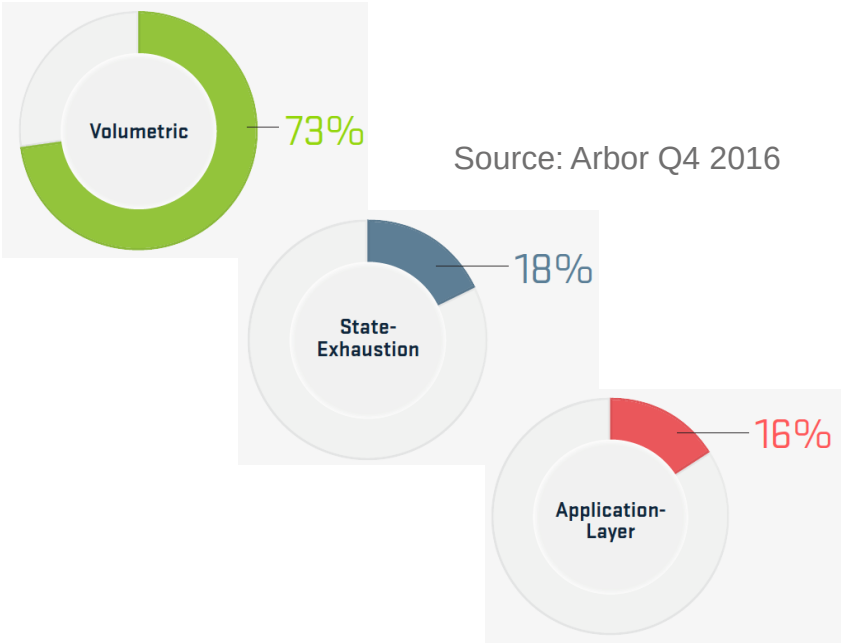
**State-exhaustion DDoS attack**

**Volumetric DDoS attack**

# DDoS Attack trends




Source: AWS shield protect web application of Amazon




Source: Arbor Q4 2016

# Background 2016

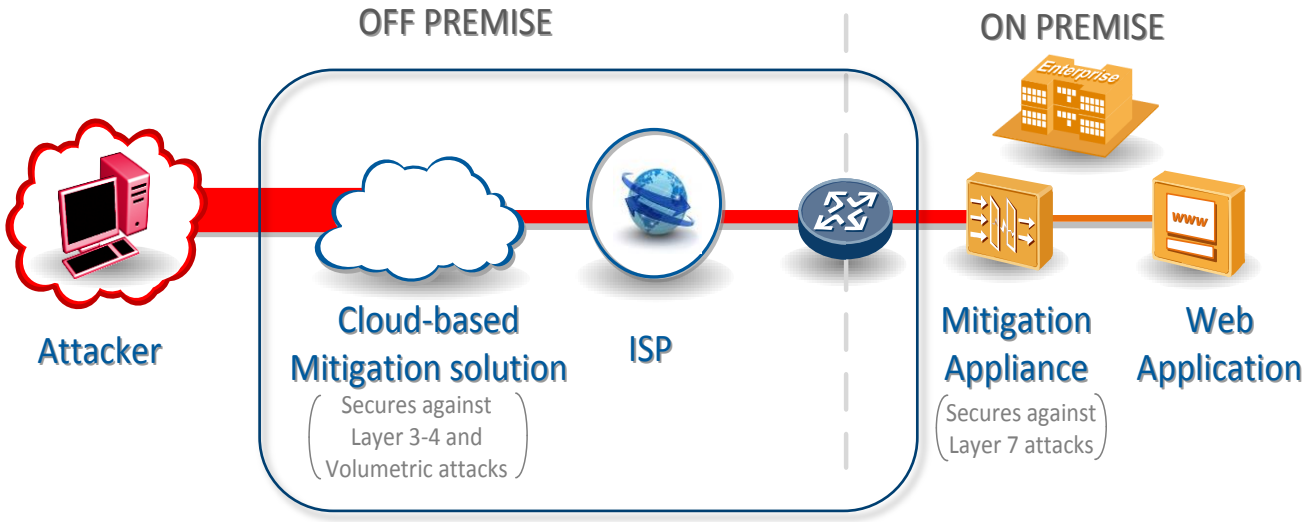
- A lot of DDoS attacks against:
  - Federal institutions
  - Education institutions

- Manual mitigation:
  - Customer complaint
  - Analyze of the traffic
  - Identify of the attack pattern
  - Apply some filters

- Negative aspects
  - Slow to implement
  - Analyze required each time attack vector changed
  - Only a reactive process

- A lot of requests from customers about what could be done

# Service Architecture

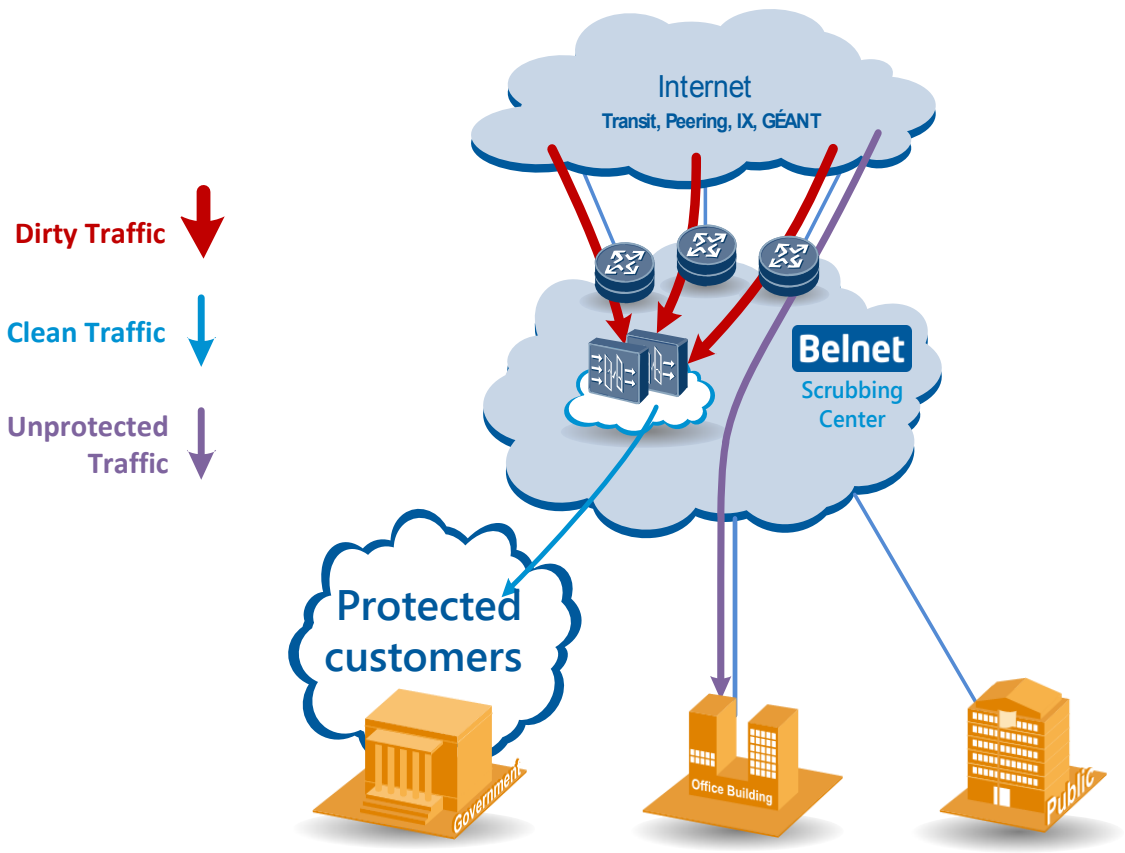



- Belnet replied to the customer requests and started a project to implement DDoS Mitigation Service



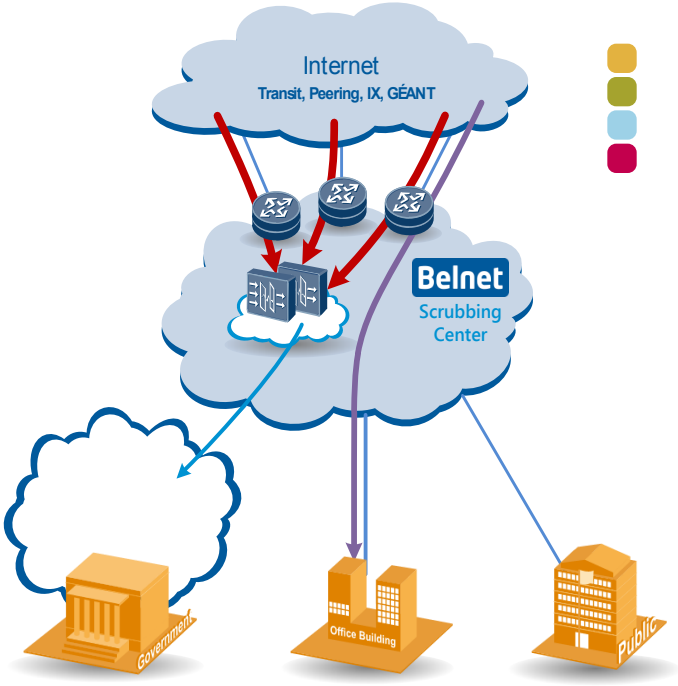
Belnet
dedicated connectivity

# Belnet Architecture



# Service Description

- Always On
- Automatic Detection
- Automatic Mitigation
- Protection against:
  - Volumetric attacks (reflection/amplification)
  - L3, L4 attacks, IPv4 and IPv6
  - Flooding (SYN, ACK, PSH, RST, ICMP, UDP)
  - Fragments
  - Protocol Anomalies






Belnet
dedicated connectivity

# Belnet DDoS Mitigation
# Standard DoS Profile

| DoS Vector |
| --- |
| ICMP flood |
| IP fragment flood |
| TCP PSH flood |
| TCP RST flood |
| TCP SYN ACK flood |
| TCP SYN flood |
| UDP flood |


## With Belnet

- Traffic does NOT leave Belnet network
- No re-routing latency
- Can protect 1 IP or whole subnet
- No extra bandwidth cost for clean traffic
- Future Proof
  - *cf. BGP Origin Validation*

**One partner for everything**


## Without Belnet

- Customer traffic re-routed outside to third party
- Clean traffic re-enters network via GRE tunnel
- Minimum size /24
  *Cannot protect individual 1 IPs*
- Additional bandwidth cost for GRE
- Not future proof
  - *BGP hijacking*

2 Parties, 2 services, 2 contracts

# Project and proof of concept

- April 2016: Project DDoS Mitigation Service started
- May 2016: Hardware installed in our DataCenters
- Summer 2016: First tests
- Sep/Oct 2016: 3 customers protected by the solution
- Oct 2016 – Apr 2017: Fine tuning
- June 15th 2017: Launch date

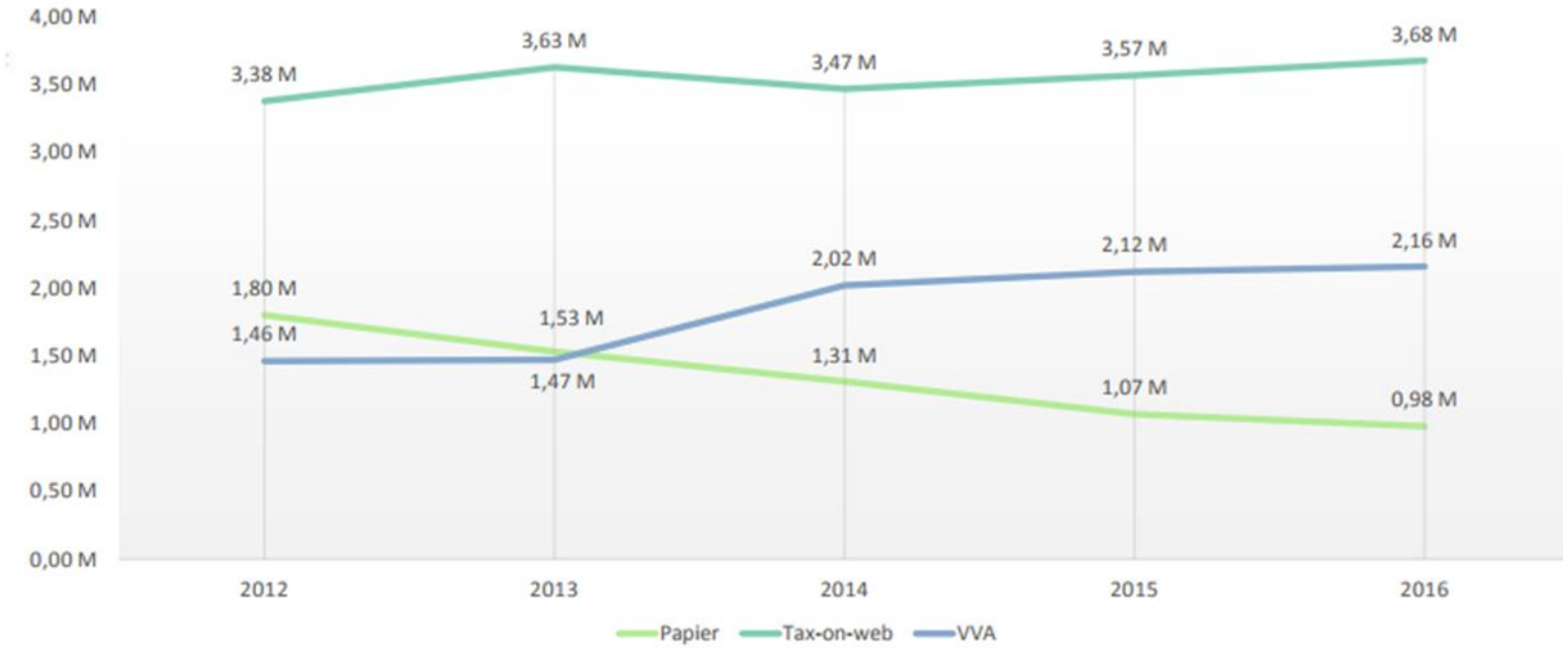

# Federal Public Service FINANCE



Belnet
dedicated connectivity




Belnet
dedicated connectivity




Tax-on-web 2017 compte actuellement

3 0 3 4 0 9 3 déclarations

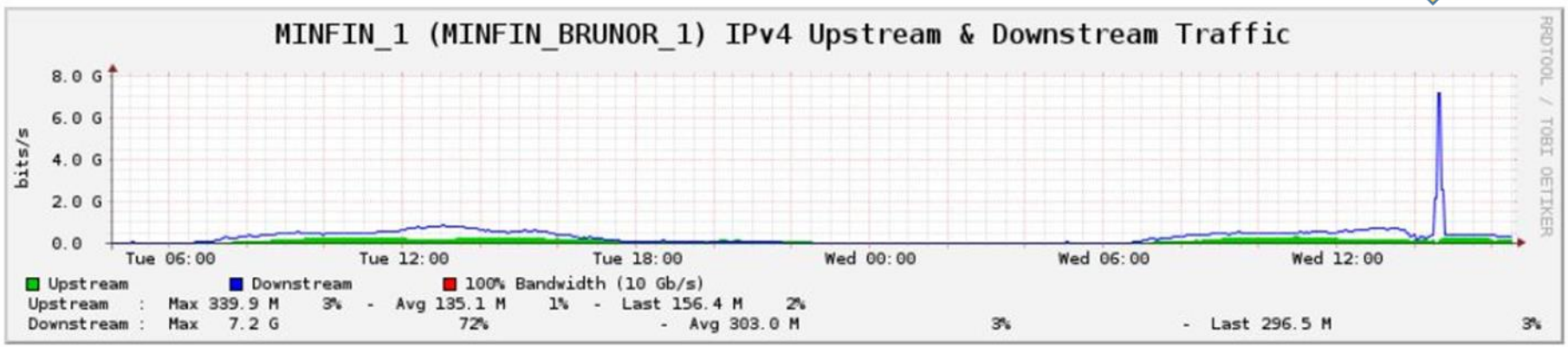


Belnet
dedicated connectivity

# DDOS attack on Tax-on-Web

- 8 june 2016
- Attack on a public IP of the outer firewall
  - 10 Gbps internet link saturated
  - IPS module of the firewall crashed
  - Firewall CPU at 100%

**Graphics* of your connection(s)**
**Financieren/Finances - PoP Access FEDMAN**



# DDOS attack on Tax-on-Web

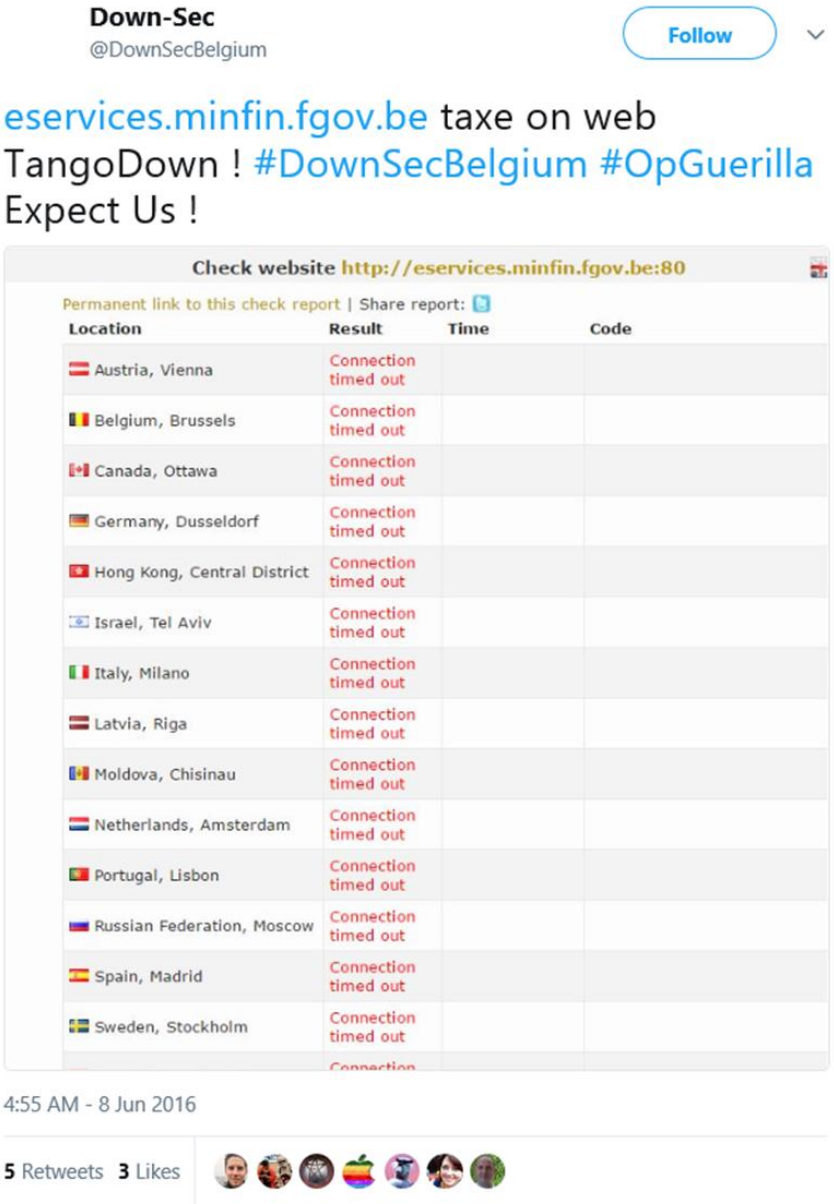
- Duration +- 20m between 14h20 and 14h40
- Impact:
  - standstill of all incoming from the internet, including Tax-on-Web
  - standstill of outgoing traffic to internet, s.a. O365.



Belnet
dedicated connectivity

# Claim by Down-Sec Belgium

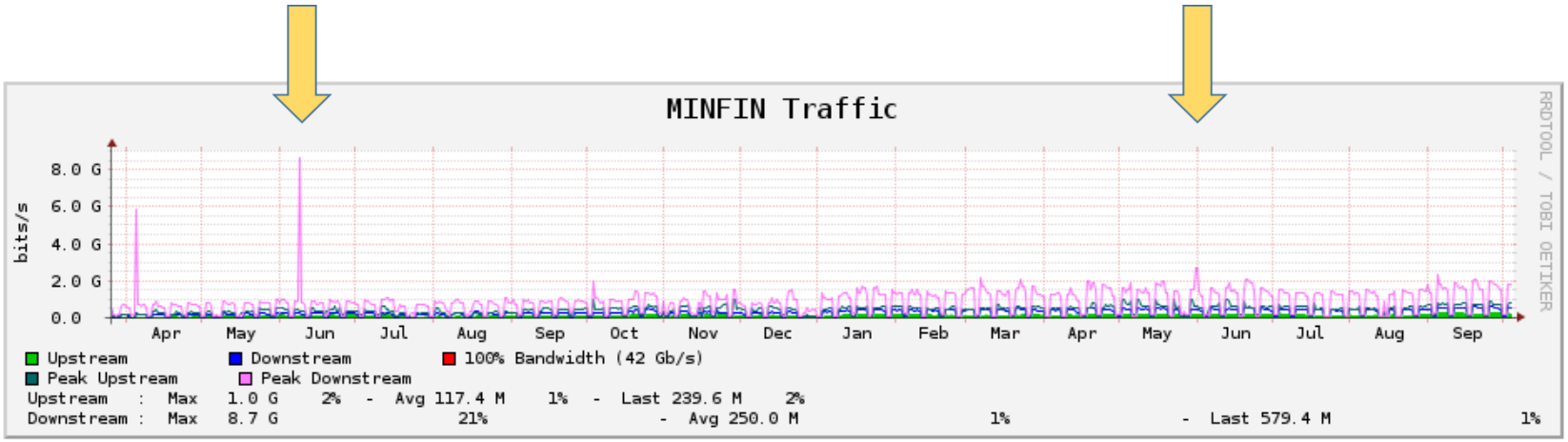
- The attack was claimed on Twitter
- The attack was part of a larger anti-government campaign by Down-Sec Belgium
- Other government sites such as senate.be and premier.be had been attacked in the weeks before

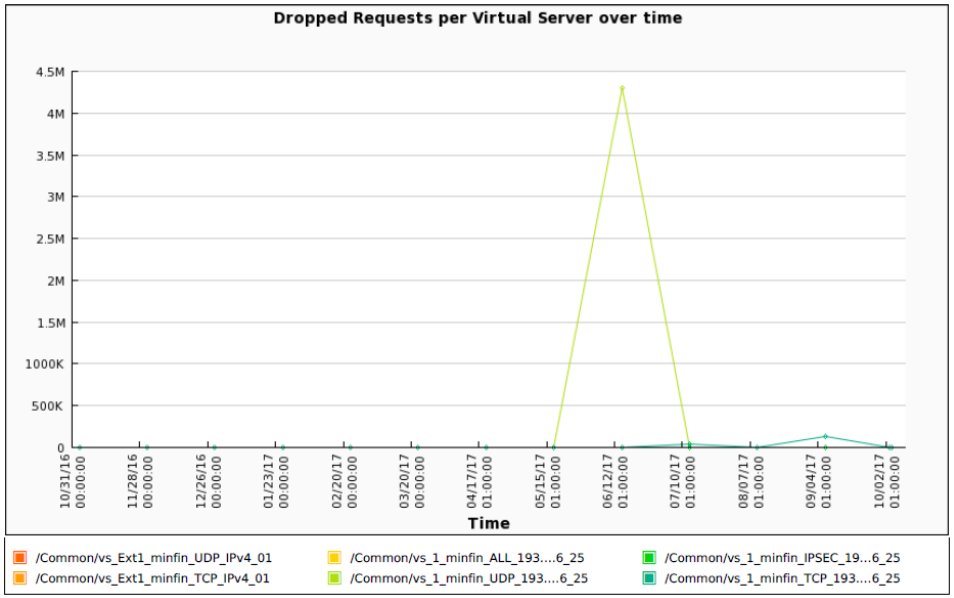


# Countermeasures

- Limitation of traffic originated from foreign countries to a certain maximal bandwidth
- Discussions with Belnet were started to use their anti-DDOS protection services

# After one year of collaboration





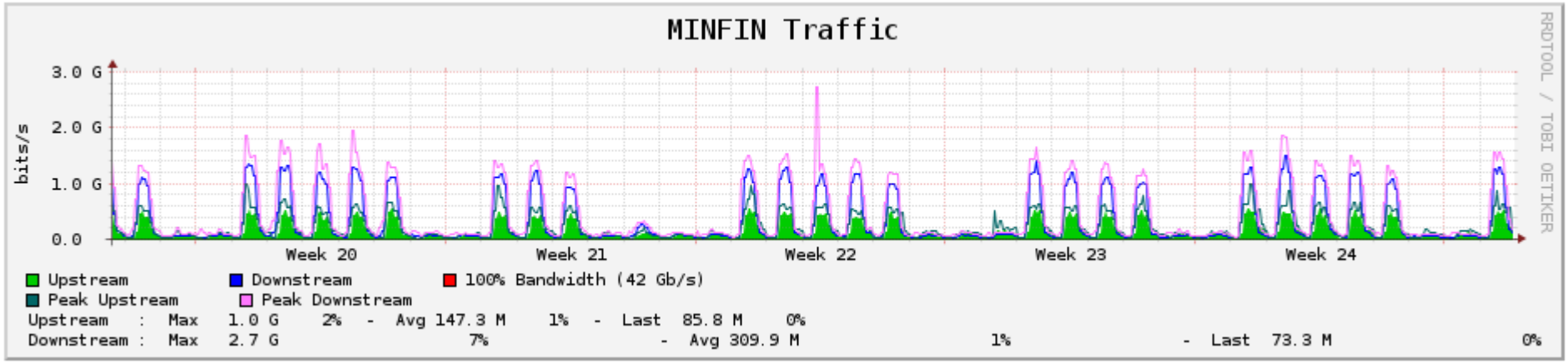

Belnet
dedicated connectivity

# Thank you
## for your attention

Belnet
dedicated connectivity

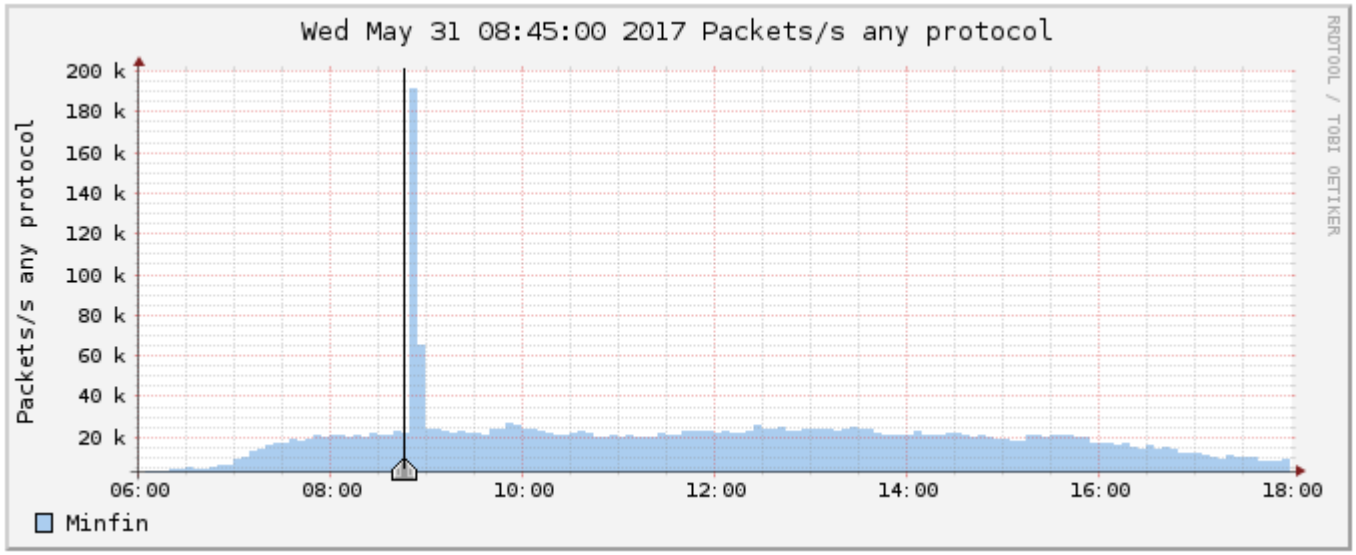

Belnet
dedicated connectivity
.be

# Monitor




- Monitoring of the capacity is done after the mitigation

# Netflow




- Netflow collects data before the mitigation

- Characterisics
  - UDP port 443



Belnet
dedicated connectivity