A Guide About DDoS Attacks
Understanding and anticipating DDoS

Guillaume Valadon
guillaume.valadon@ssi.gouv.fr

RIPE 70 - May, 11 2015

ANSSI

Created on July 7th 2009, the ANSSI is the national cyberdefence agency

Main missions:

- Prevention
- Defence of information systems

One of its priorities is the Internet resilience.

http://www.ssi.gouv.fr/en/

A guide about DDoS attacks ?

Why ?

Goal

Give an overview of the existing DDoS protection solutions:

- Describe each solution
- Give its scope, and its possible limitations

Target

Mainly for **customers of network operators**

Who ?

Written in cooperation with French network operators

Companies and network operators involved

- Acorus Networks
- Bouygues Telecom
- Cyber Test Systems
- France-IX
- Free / Online
- Jaguar-Network
- Orange France
- SFR
- Zayo France

Where ?

Only in French so far

Links

- Official guide, `http://www.ssi.gouv.fr/guide-ddos`
- Light PDF, `https://transfer.sh/11Sij4/guide-ddos.light.pdf`
- Google Translate, `https://goo.gl/UL8M1d`

What is inside ?

1. **DDoS attacks**
   - What is a DDoS attack ? Who can be targeted ?
2. **How to defend against DDoS attacks ?**
   - Filtering (at the edge of the network, in the cloud)
   - Dedicated protection services
3. **How to react in case of attack ?**
   - Attack detection and reaction
   - Incident notification
4. **How to avoid participating in a DDoS attack ?**
   - Reduce the attack surface, traffic filtering

How to defend against DDoS attacks ?

Describe each solution, give its scope and limitations

Edge filtering

- Limitations of firewalls / load balancers
- Benefits of dedicated DDoS filtering equipments, and their limitations as observed by network operators

Filtering capabilities of network operators

Dedicated protection services

- Describe existing traffic redirection methods (DNS based, rerouting via BGP)

How to react to an attack ?

During the attack

- Identify the target and the nature of the attack (volumetric or application level attack, protocols used ...)
- Find the sources of the attack (is it possible to list the sources of the attack ? Is it coming from a single provider / transit operator ?)

After the attack

Who to contact in order to **declare the incident** and to **file a complaint** ?

How to avoid participating in a DDoS attack ?

Recalls the best practices !

Disable unused services

Harden the configuration of exposed services (examples : NTP, SNMP)

Keep frameworks and CMS up to date. Follow development best practices

Filter outbound traffic to prevent IP address spoofing

Conclusion

Shall it be translated to English ?

How did it work ?

- Good feedbacks from French NOG
- Some parts were discussed then fixed

Please send comments to:

`guide.ddos_at_ssi.gouv.fr`

Questions?

English version at `https://goo.gl/UL8M1d`