Why you should take care of the network(s) around you

or

What (obvious) actions you can to make the Internet a bit less dangerous,

or

DDoS suckz

or

Make the Internet a better place

Agenda & Bio

- Agenda & Bio, (<- you are here)
- Who am I working for
- Why I submitted this talk / Back story,
- Resolution
- Lessons Learned
- How to be prepared
- What else ?
- Conclusion

Who am I : Will van Gulik, aka that guy who wants to peer.

What I do :

- Typing stuff on routers for ASNs, mostly for AS25091 & AS2613,
- Touching vinyl records with really loud electronic music,
- Writing science-fiction.

Shameless Marketing Slide

- **IP-Max SA** aka AS25091,
- Based in Geneva,
- Founded non-profit in 2005, company since 2012
- Provide Managed Network Platforms and Services
- European and Swiss network ring
- Present in 12 IXPs and 30 PoPs, 6 Countries (CH,FR,UK,DE,RU,ZA + IT/LU)
- MSK with low latency
- DE-CIX & France-IX Reseller, available in all our PoPs, Bundle possible (Trunk).

Why I submitted this talk & Back Story

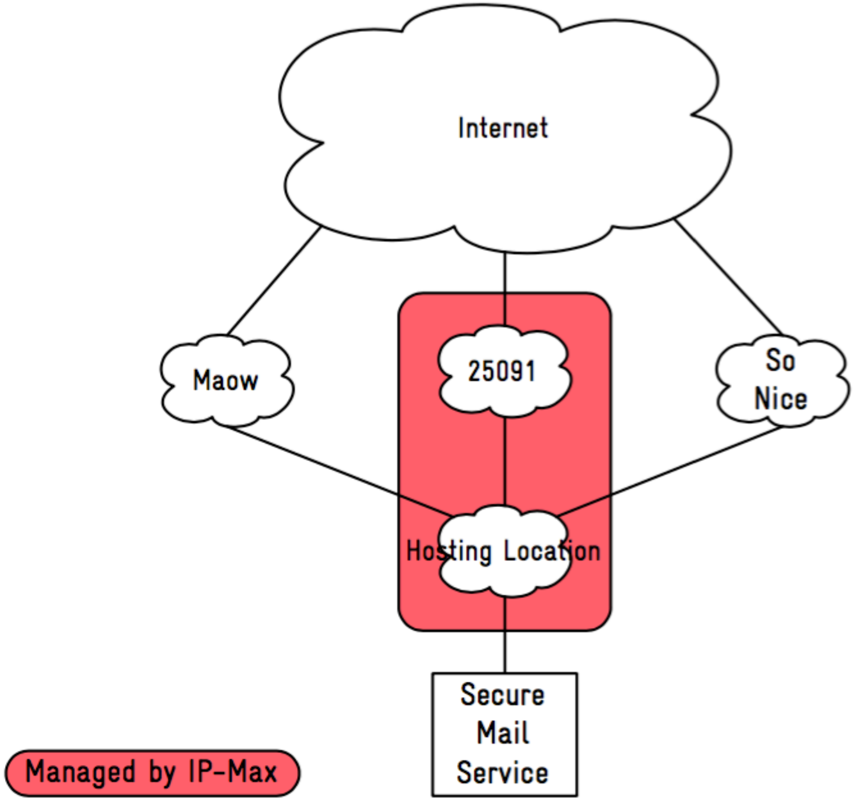
In November 2015, one of our customers got DDoSed.

The attacker has a well known action plan :

- Contact the owner asking for Bitcoins with a deadline,
- They do a demonstration attack,
- DDoS if no payment is done, or even if a payment is done.

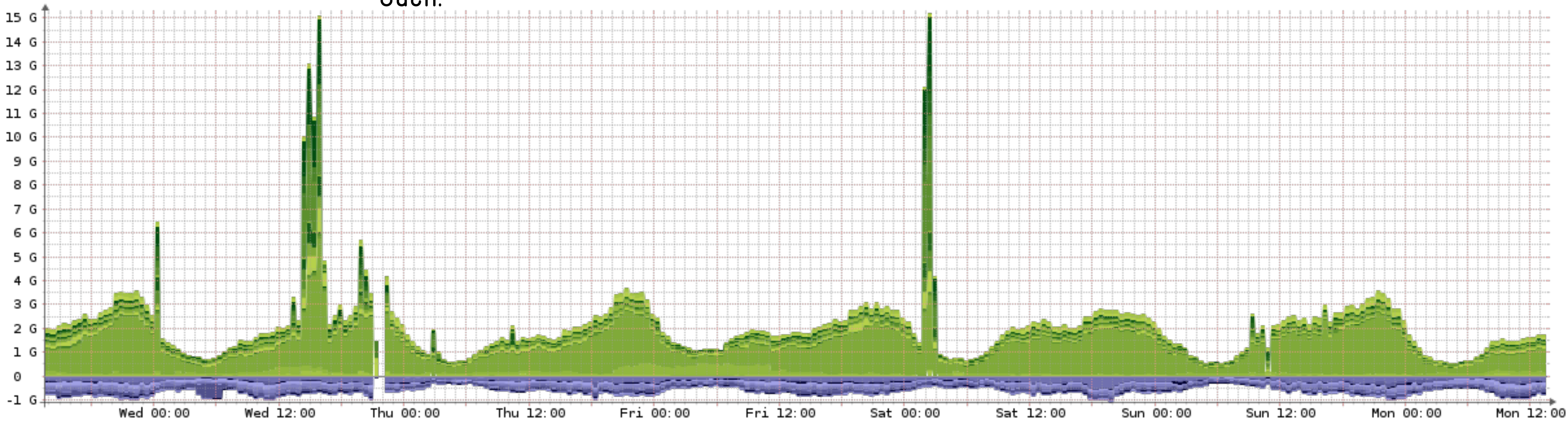
Back Story #2

Network situation :



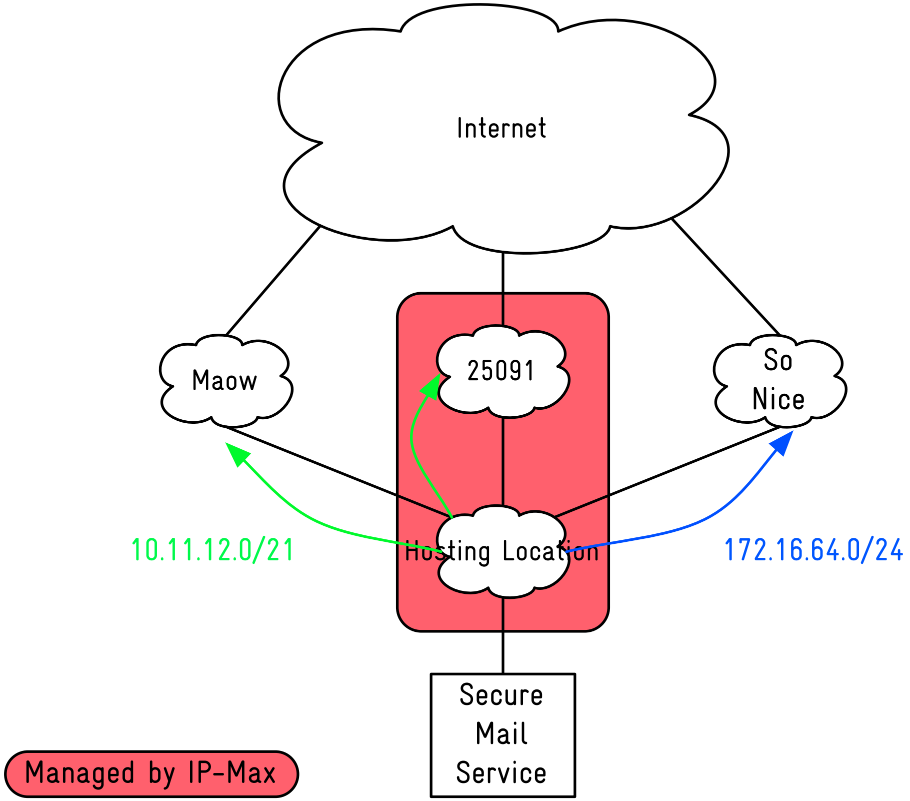
Back Story #3

- November 2015 :
  - Ouch.



Back Story #4

- " Why didn't you stop announcing the prefix ? "
  - It's not really efficient to keep the customer reachable, is it?



Back Story #5

Ransom :

- Don't pay !
- If you do, you are paying the next attacks,
- We still got attacked afterward
- Were there multiple attackers ?

Fast forward to today :

- They are supposed to be jailed
- We didn't hear about many real similar attacks after us
- But things got worse for some other people nowadays.

Backstory #6 & Resolution

“ Everyone got his peering war. “

Resolution :

- Re-use one of our backup transit, with a different path to the DC
- DDoS protection offer
- IP-Max send a router to the DC
- Over a week-end (yes, it’s actually doable)
- Get debriefing dinner with the target on Sunday evening

Lessons Learned

- Don't pay ransom
- There is many evil people on the internet
- Attacks are not all the same :
  - UDP DNS / NTP
  - Various amplification method
  - TCP BGP Flood
  - Link saturation
  - DoS & DDoS
- Be prepared,
- Why ?
  - Because IoT and other botnets, DDoS as a service, etc. (Octave, Akamai, und so weiter)
  - We can improve the situation, check that talk from the last Ripe Meeting : https://ripe73.ripe.net/archives/video/1457/

Be Prepared

- Have a backup plan and good partners
- Be ready to modify your BGP setup, (announce a more specific /24)
- Have spare devices ready to announce a prefix over GRE
- Ask for blackholing communities of your uplinks and IXPs, and be ready to act (Fastnetmon, ExaBGP)
- Get a real OOBM
- Have your contact info up to date, (RIR Database, PeeringDB)
- Monitor your network from inside and outside and collect data/ evidences (Observium, ELK, NetFlow, #othertoolsIdontknowof, Nlnog Ring SQA, Ripe Atlas, stat.ripe.net)
- Automate your processes (ansible, puppet, napalm, abuse.io)

What Else ?

Make internet a better place :

- Be informed, read BCOPs
- Implement MANRS
  - https://www.routingmanifesto.org/
- Implement uRPF / BCP38/84
  - http://www.bcp38.info/index.php/Main_Page
  - https://tools.ietf.org/html/bcp84
  - http://spoofer.caida.org/
- Filter your peers & customers (easy in the Ripe region !)
  - Use BGPq3 (https://github.com/snar/bgpq3)
  - Offer RTBH to your BGP customers (Configuration examples : http://www.senki.org/wp-content/uploads/2015/03/008-Remote-Triggered-Black-Hole-RTBH-2012-02-04.pdf , http://packetlife.net/blog/2010/aug/23/source-based-rtbh/ https://www.m00nie.com/2014/01/bgp-rtbh-setup-using-exabgp/ , http://www.swinog.ch/meetings/swinog25/p/04_ddos-black-holing-with-exabgp-in-a-provider-network-swinog-25.pdf)
- Know your vulnerable devices, use Shadowserver, Qrator, etc
  - https://www.shadowserver.org/
  - https://radar.qrator.net/
  - http://openresolverproject.org/
  - http://openntpproject.org/
  - https://www.shodan.io/
  - https://ddosmon.net/statistic
  - http://data.netlab.360.com/mirai-scanner

What Else ? #2

Make internet (even more) a better place :

- NLNog
  - Ring & RingSQA https://ring.nlnog.net/
- Support and request Large BGP Communities to your vendor (http://largebgpcommunities.net/)
- Register on UTRS, (RS with 173 sessions of 142 network for RTBH)
  - https://www.team-cymru.org/UTRS/index.html
- Fredy's idea and beyond :
  - Community driven RS for Swiss routes and RTBH only, in CIXP and SwissIX ? Anyone is interested ? in a (community driven) RS for RTBH only and Swiss only prefixes on Swissix and Cixp ?

Conclusion

Are you doing your part ?

You too can make the internet a better place !

Thanks !
Questions ?

http://www.ip-max.net
http://www.as2613.net
will (at) ip-max (dot) net
will (at) as2613 (dot) net