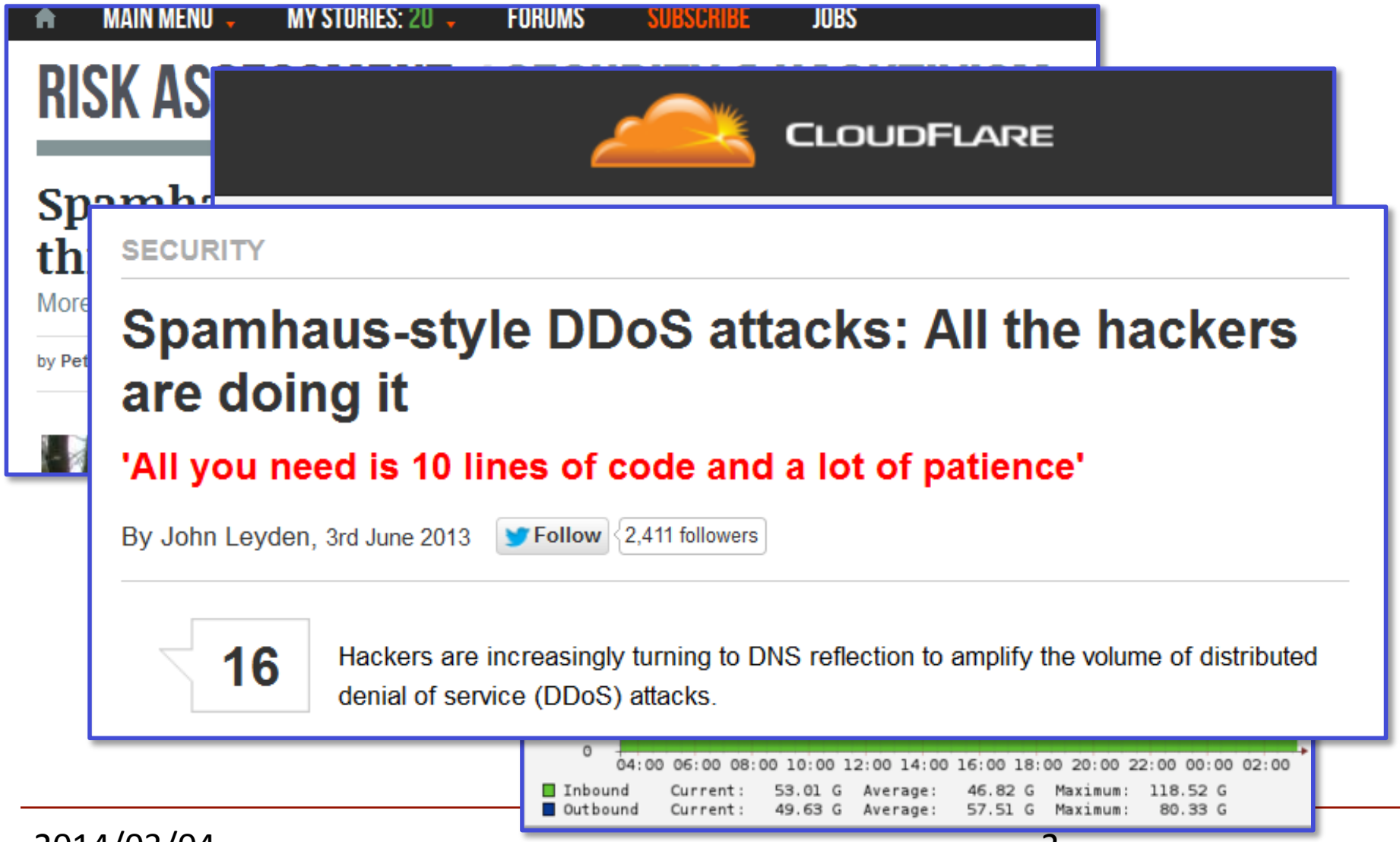
Open DNS Servers, NTP monlist BCP38

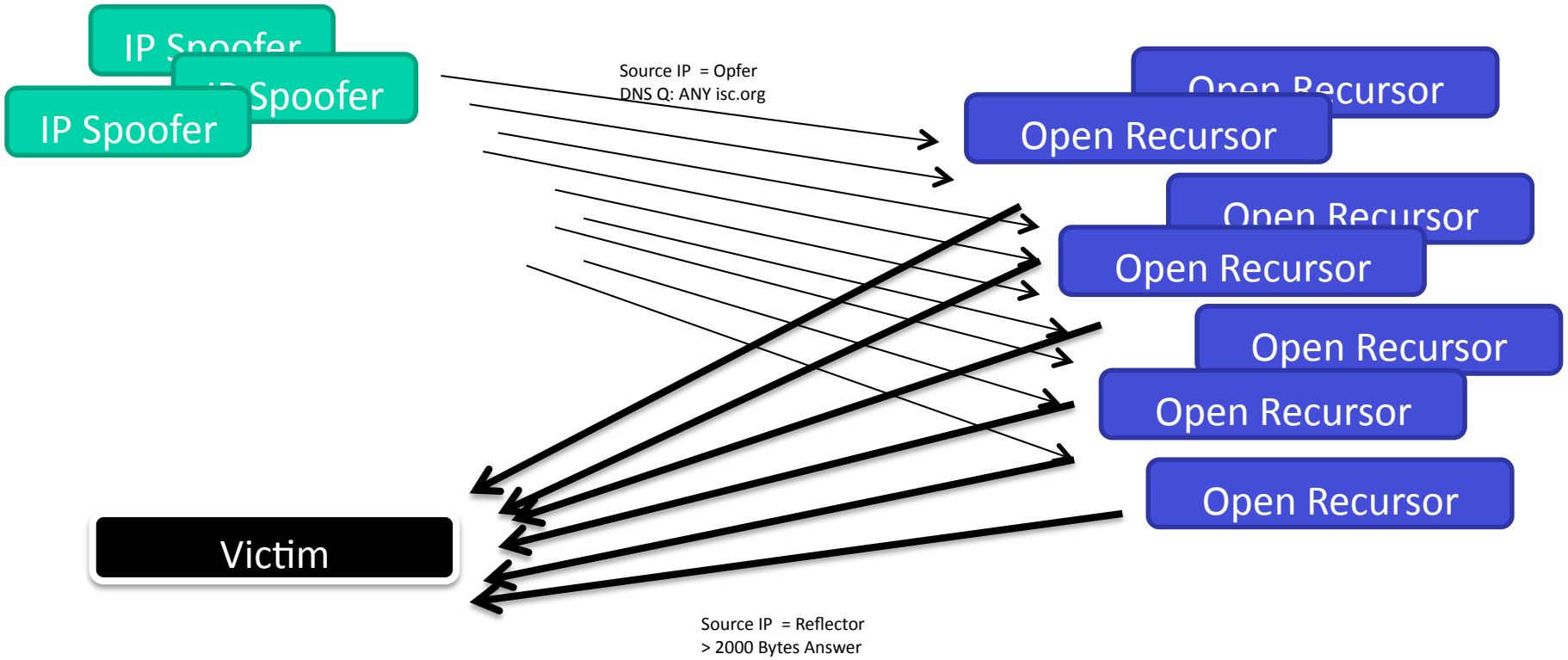
Otmar Lendl
<lendl@cert.at>

About a year ago …



A few weeks ago …

DNS Reflection Attack



Summary Reflected DDOS

- The victim only sees packets from the reflectors, not the attacker
- The reflectors only see the spoofed packets
- Amplification:
  - DNS: up to factor 100
  - NTP: with monlist, up to 1000
- Mitigation by filtering/rate-limiting might be possible

- See also
  - http://blog.cloudflare.com/understanding-and-mitigating-ntp-based-ddos-attacks
  - Other protocols as well: http://www.internetsociety.org/sites/default/files/01_5.pdf

What do we need to do?

- Prevent IP Address Spoofing
- Reduce number of reflectors/amplificators
- Trace-back capabilities
- Control Plane protection
- Cooperation during attacks

TODO 1: Anti-Spoofing

- Prohibit IP Address Spoofing
  - BCP38: Network Ingress Filtering
    - http://tools.ietf.org/html/bcp38
    - http://www.bcp38.info/
  - BCP84: Ingress Filtering for Multihomed Networks
    - https://tools.ietf.org/html/bcp84
  - The closer to the customer, the easier and better
  - **Datacenter**, DSL, Cable, leased lines, …
  - Small ISPs: filter towards the upstream
  - Automate!

TODO 2: Secure Servers

- Remove amplificators from our networks
  - Analogue to open SMTP relays or smurf amplifiers
- DNS
  - No open recursors
    - http://openresolverproject.org/
  - Rate-Limit on authoritative servers
    - http://www.redbarn.org/dns/ratelimits
- NTP
  - Restrict access
  - Disable control commands
    - http://openntpproject.org/
- chargen
  - No, it is not 1992 any more
- …

TODO 3: Traceback!

- We need to know who is generating spoofed packets
  - Otherwise we will not get the required pressure
- Assuming an amplificator in **your** network: can you trace back the forged packets?
- Tools & Processes & Skills
  - Netflow -> Interface
  - How to trace back over shared IXP LANs?

TODO 4: Protect yourself

- The Spamhaus DDOS last year:
  - Initially against webservers
  - Then against the unicast addresses of Cloudflare sites
  - Then against the interface address of the supporting routers
  - Then against the IXP address of the ISP
- Thus:
  - Protect your control plane
  - Ideally: filter traffic towards routers as early as possible
  - Do we need to announce the IXP prefix?

TODO 5: Cooperation!

- Smaller (i.e. not Tier1) networks cannot mitigate every attack
- Mitigation needs cooperation
  - Establish rapport with your upstreams
  - What can they do manually?
  - Automatic features (remote triggered blackholing?)
  - Get to know your peers / CERTs / LE
- Plan ahead:
  - See Barry Greene‘s „The Service Provider Tool Kit” http://www.nanog.org/meetings/abstract?meet=54

Outlook

- We‘re seeing significant DDOS activity
- Booter services offer that for minimal money
- Extortion racket in Asia

- **We need to fix this.**

- If not, we‘re opening ourselves up for regulatory intervention.

Questions?

Otmar Lendl <lendl@cert.at>

+43 1 5056416 711