GovCERT AUSTRIA

CERT.at

DDOS, Blackmail, Bitcoins

Robert Waldner

<waldner@cert.at>

CERT.at?

- Nothing to do with certificates/certifications
- National Computer Emergency Response Team
- Constituency: Austria
- Operated by nic.at, the .at TLD registry

Who?

- Network techie with EUnet/KPNQwest from 1998 to 2001
  - I can probably still *spell* B..G..P.. correctly
- Security consultant till 2008
- CERT.at from then on

The problem

- DDoS, especially with reflection
- Small request packet with spoofed source address
- Large answer packet(s) to spoofed source address (victim)

Scope

- We have confirmed reports of up to 80 GBit/s attacks in Austria
  - No hard numbers for PPS
- Some folks report up to a couple hundred Gbit/s
  - Be wary, especially with reports from companies that want to sell you their DDoS prevention gear/service

Where does that come from?

- There‘s a couple „DDoS-as-a-service“ providers
  - Some act via botnets
  - Some via rented servers
    - Anyone remembering the bullet-proof hosters of ages past?
- Operating from the same „underground“ forums as malware/exploit kit authors
- You can „buy“ a couple GBit/s outbound for as little as $25/15 minutes

Cheap, fast, reliable – pick any two

- Cheap?
  - It‘s so cheap your average script kiddie can afford it
- Fast?
  - These „couple GBit/s“ then quickly become a couple ***dozen*** GBit/s after reflection
- Reliable?
  - Who cares

Script Kiddies, really?

- Yes, here‘s their MO:
  - Do a „test“ run for 15-60 minutes
    - (they invested all of maybe 50-100 USD for that)
  - Send an extortion mail to victim, demanding couple BTC (1k EUR upwards), threaten longer/ larger DDoS if victim doesn‘t pay

Do they follow through?

- Do they follow through?
  - Some do, most don‘t
- Who are the victims?
  - Last year it was mostly small(-ish) ISPs
    - DD4BC, Armada Collective
  - Current batch targets financial sector
    - ISPs and their other customers are collateral damage

But it‘s not *just* kiddies

- Last month the incumbent telco in Austria was hit
- Attackers were smart
  - Hit the DNS resolvers
  - Customers see „the whole intertubeweb is b0rken“
  - Attackers modified target/mode when the defenders stopped one vector

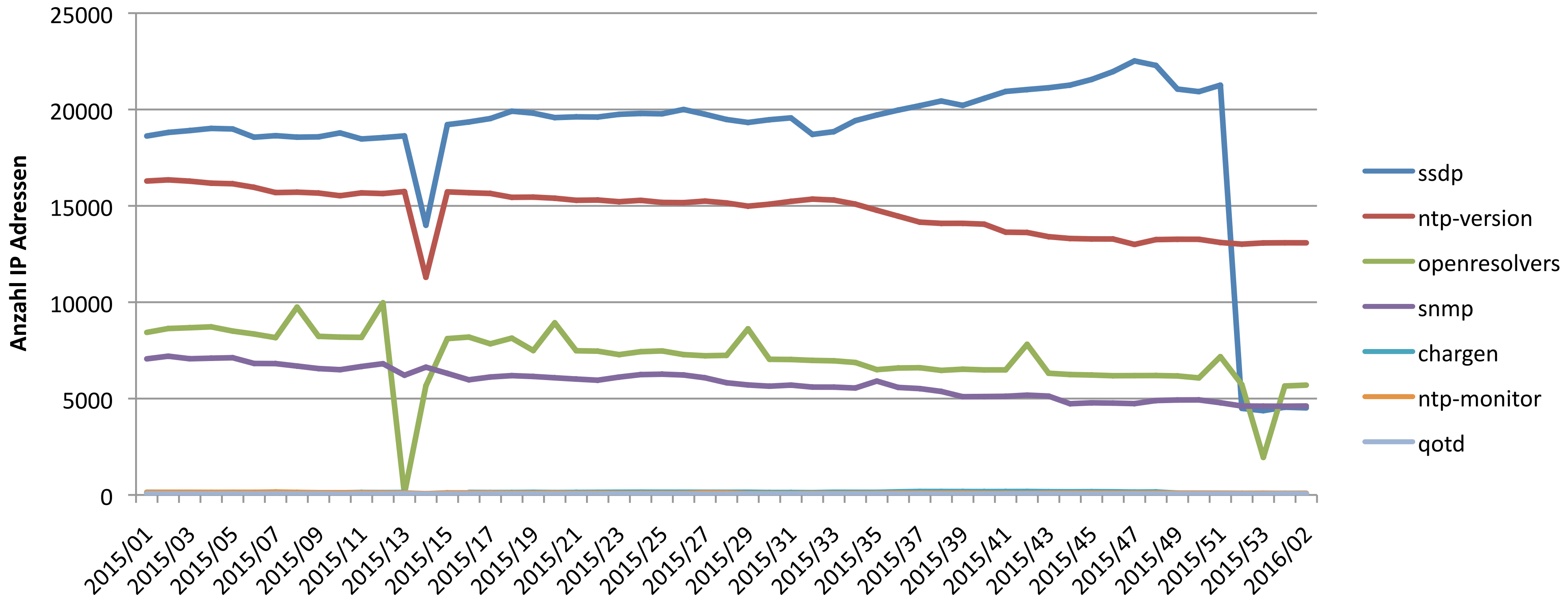
Maybe I‘ll just pay

- Probability says that they’ll be back with a larger demand next month
- Probability also says that once someone pays, another attacker will come along
  - Those kiddies brag to each other …

But what‘s a couple reflectors between friends

CERT.at

GovCERT AUSTRIA



What can I do?

- **Don‘t be part of the problem**
  - Do proper egress filtering: BCP38 etc.
  - Act on abuse reports, don‘t just /dev/null them
- ‘net hygiene is important
  - And it starts with you
  - Yes, that means getting your customers to fix their reflection-prone services
- Don‘t be afraid to talk to your local CERT and LE if you get hit (or even just threatened)

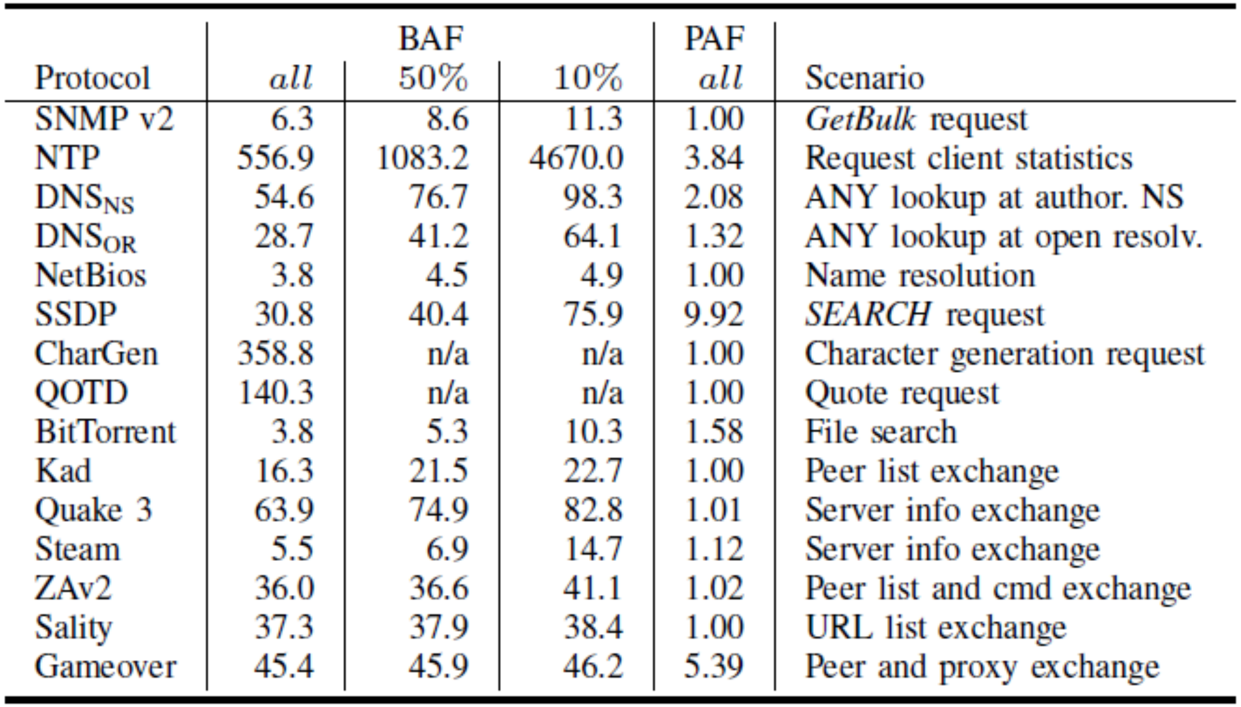
Reflectors

- Each of those boxes has at least half an MBit/s of upstream (residential gear)
- With, say, reflection via DNS (ANY query for DNSSEC signed zone) an attacker gets amplification of up to 50x
  - 60 bytes request, 3kB answer
  - and that answer will be fragmented to make filtering so much more fun
- Go figure

It‘s not just DNS and bots

- Amplification of up to 50x
  - What can a single server (be it virtual or HW) with GBit/s uplink do?
  - Exactly

Fun (&profit?)



	BAF			PAF	
Protocol	*all*	50%	10%	*all*	Scenario
SNMP v2	6.3	8.6	11.3	1.00	*GetBulk* request
NTP	556.9	1083.2	4670.0	3.84	Request client statistics
DNS_{NS}	54.6	76.7	98.3	2.08	ANY lookup at author. NS
DNS_{OR}	28.7	41.2	64.1	1.32	ANY lookup at open resolv.
NetBios	3.8	4.5	4.9	1.00	Name resolution
SSDP	30.8	40.4	75.9	9.92	*SEARCH* request
CharGen	358.8	n/a	n/a	1.00	Character generation request
QOTD	140.3	n/a	n/a	1.00	Quote request
BitTorrent	3.8	5.3	10.3	1.58	File search
Kad	16.3	21.5	22.7	1.00	Peer list exchange
Quake 3	63.9	74.9	82.8	1.01	Server info exchange
Steam	5.5	6.9	14.7	1.12	Server info exchange
ZAv2	36.0	36.6	41.1	1.02	Peer list and cmd exchange
Sality	37.3	37.9	38.4	1.00	URL list exchange
Gameover	45.4	45.9	46.2	5.39	Peer and proxy exchange

Read up

- Excellent paper by Christian Rossow
  - The preceding list is also from him
  - http://www.christian-rossow.de/articles/Amplification_DDoS.php

Lather, rinse, repeat

- Do egress filtering
  - yes, this means BCP38 etc.
- Act on abuse reports
- Work with customers to fix their open resolvers, NTP servers, SSDP, Chargen/QOTD …

Lather, rinse, repeat: round #2

- Talk to your local CERT/CSIRT/NCSC/..
- Talk to LE
  - An OPSEC error might lead to an arrest like with DD4BC (https://www.europol.europa.eu/content/international-action-against-dd4bc-cybercriminal-group)

Questions?

Robert Waldner <waldner@cert.at>
+43 1 5056416 78