Denial of Service durch Paketfluten:

Warum 100 Gigabit/sec der neue Normalzustand sind

Otmar Lendl
<lendl@cert.at>

Vorstellung …

- Mag. Otmar Lendl
  - Computerwissenschaften und Mathematik an der Universität Salzburg
  - Betreibe seit 1991 Server im Internet
  - 5 Jahre ISP-Erfahrung (EUnet, KPNQwest)
  - nic.at R&D (primär ENUM, zwei RFCs geschrieben)
  - Seit 2007: Teamleitung Österreichisches nationales CERT

Nationales CERT?

- Computer Emergency Response Team

- Interessante Rolle:
  - Keine Weisungsrechte
  - Keine Meldepflichten an uns
  - Zuständig für das ganze Land
  - Fokuspunk für Netzwerksicherheit:
    - Informationsaustausch
    - Kooperation
    - Koordination

Tagesgeschäft

- Was gibt es neues?
  - Warnungen
  - Medienarbeit
  - Tageszusammenfassungen
- Was muss gefixt werden?
  - Einholen von Informationen
  - Weitergabe an Verantwortliche
- IT-Security Community Hub
  - Human Networking
  - Koordination bei Vorfällen

Denial of Service Basics

- Angriff auf die Verfügbarkeit
- Auf welchen Layer?
  - Web-Application
    - Etwa viele Suchanfragen
  - Webserver
    - Slowloris & co
  - TCP
    - SYN floods
  - Layer 3
    - UDP / DNS-Reflection
  - Lower Layers
    - IPv6 ND, …

- Aber auch:
  - Network Infrastructure
  - DNS
  - Bereitschaftspersonal
  - Helpdesk
  - Presse
  - Management

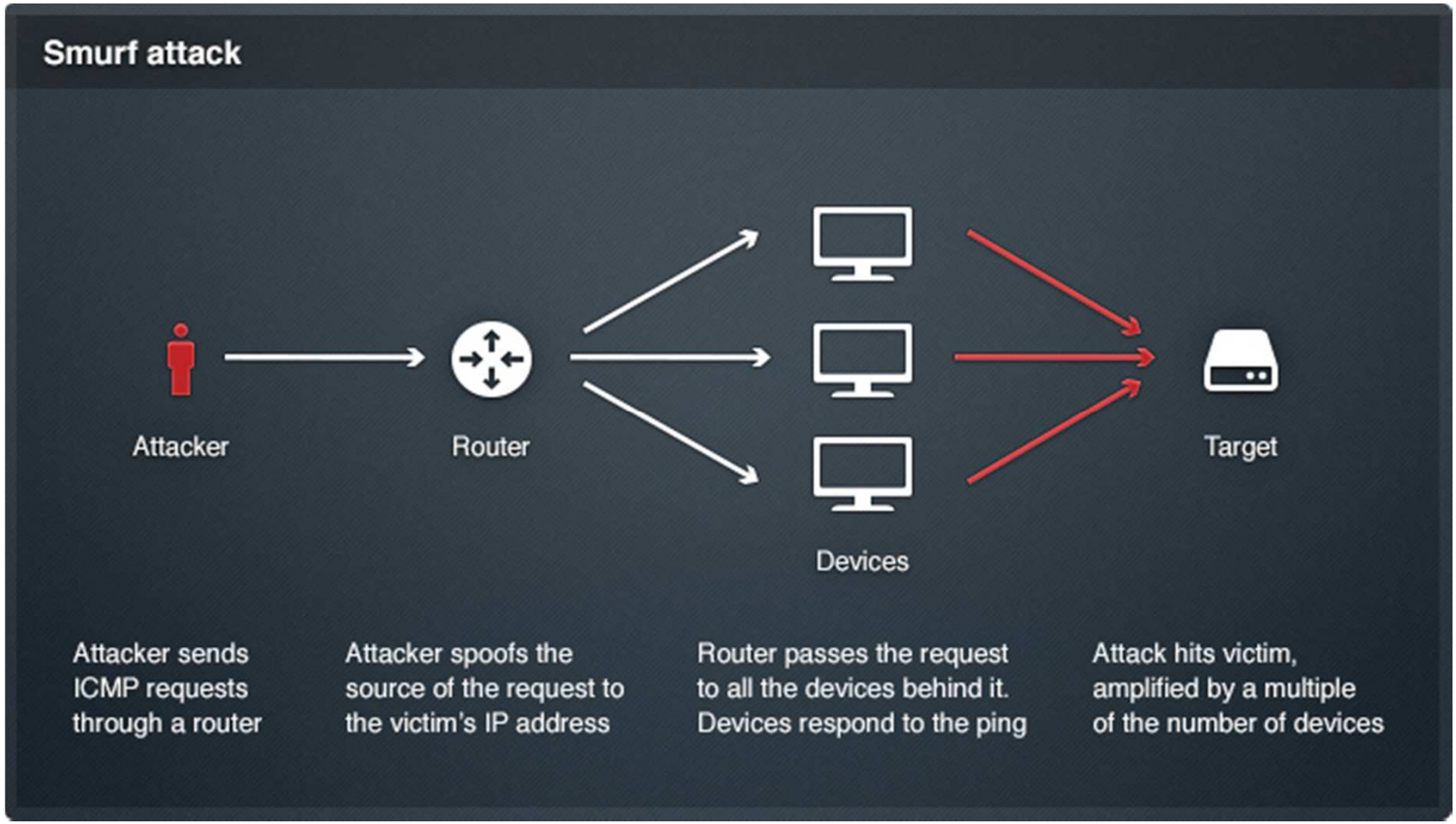
DOS vs DDOS

- Direkter, einfacher DOS Angriff ist sehr selten
  - Attribution
- Distributed Denial of Service
  - Angreifer bedient sich verteilter Ressourcen im Netz
  - Botnets
  - Reflection Attacks

Beispiel: Brobot

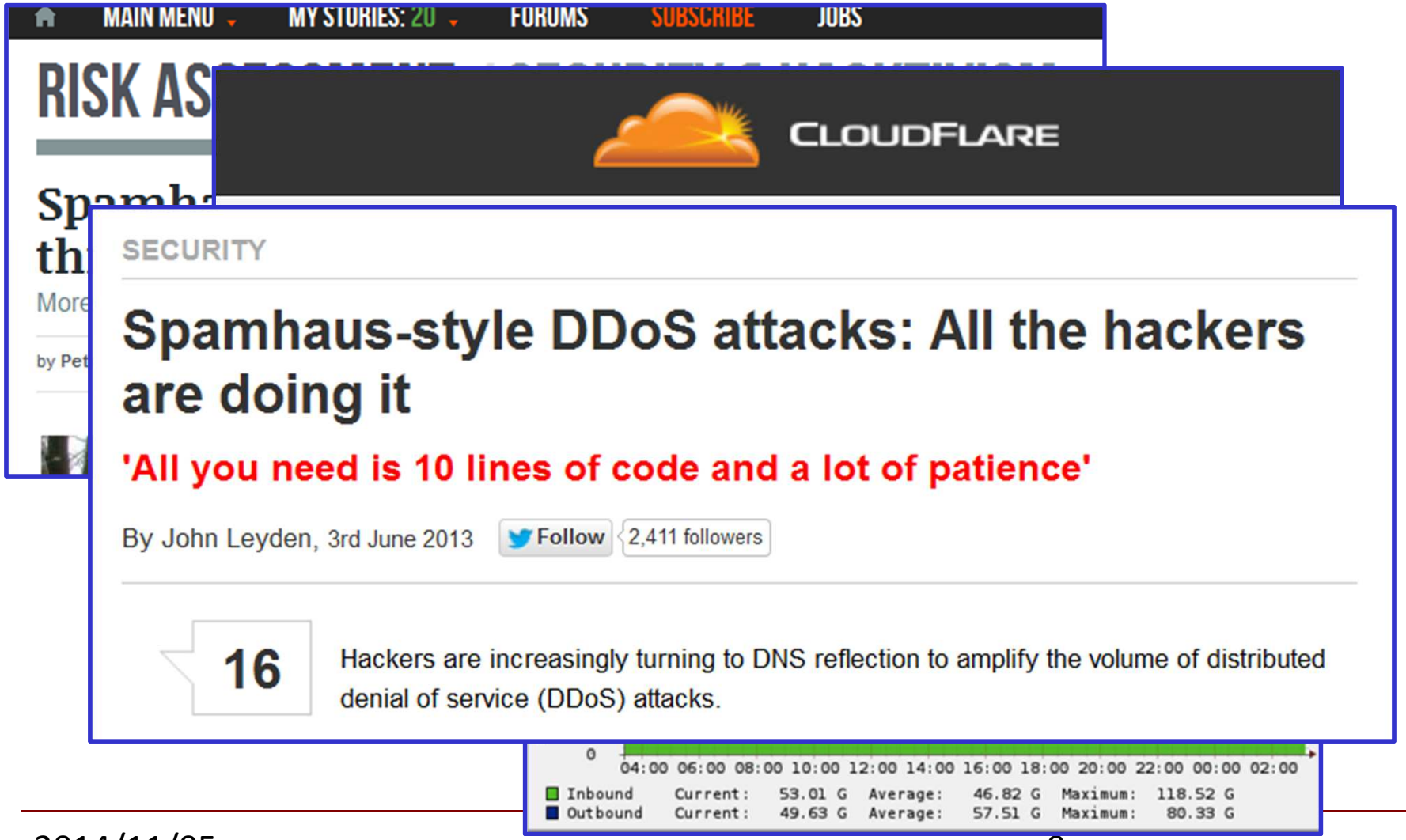
- Gehackte Webseiten
  - eval(base64_decode($_REQUEST['c_id']))
  - Eigentlicher Angriffs-Code kommt dynamisch
  - Mehrstufiges System
  - Serveranbindung, nicht ADSL
- Ziel
  - US Banken Herbst 2012 bis Mitte 2013
  - Mitigation immer noch ongoing

Wer kennt noch smurf?



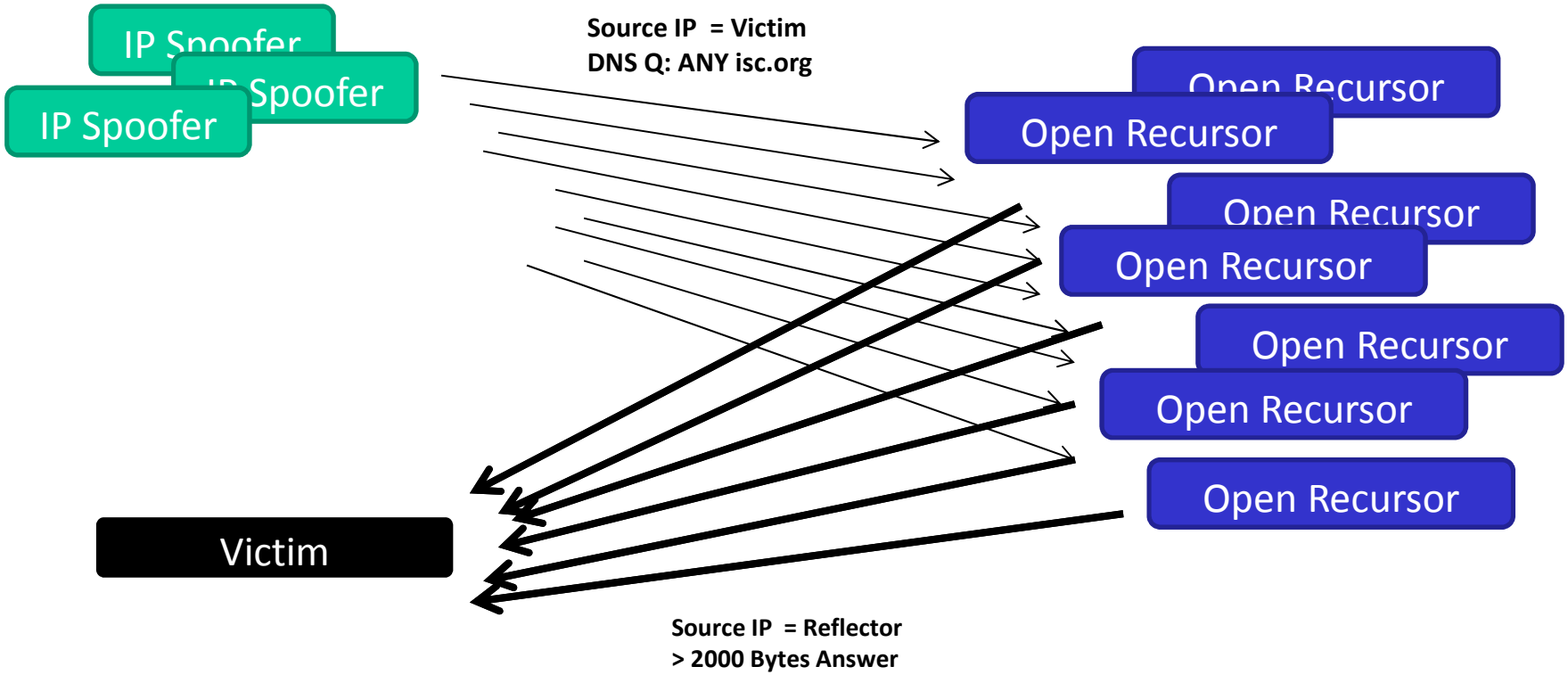
Bildquelle: https://www.cloudflare.com/ddos

Juni 2013


MAIN MENU
MY STORIES: 20
FORUMS
SUBSCRIBE
JOBS
CLOUDFLARE
SECURITY
Spamhaus-style DDoS attacks: All the hackers are doing it
'All you need is 10 lines of code and a lot of patience'
By John Leyden, 3rd June 2013
Follow
2,411 followers
16
Hackers are increasingly turning to DNS reflection to amplify the volume of distributed denial of service (DDoS) attacks.
0
04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 00:00 02:00
Inbound Current: 53.01 G Average: 46.82 G Maximum: 118.52 G
Outbound Current: 49.63 G Average: 57.51 G Maximum: 80.33 G

Februar 2014

DNS Reflection



Reflected DDOS

- Das Opfer sieht nur Pakete vom Reflektor, nicht vom Angreifer
- Der Reflektor sieht nur normale (aber gespoofte) Anfragen
- Verstärkungsfaktor:
  - DNS: bis zu ~ 100
  - NTP: mit monlist bis zu 1000

- Siehe auch
  - http://blog.cloudflare.com/understanding-and-mitigating-ntp-based-ddos-attacks

ntp reflection

- Aktuell ein ernstes Problem
- ntp hat zwei Teile:
  - Time Sync
  - Control Protocol
    - Hier ist das Problem
    - monlist: Liste aller clients
    - version: Ausführliche Statusinformationen
- Tactical Mitigation?

Mitigation: Leg 1

- IP-Spoofer -> Amplification
- Rate-Limit auf transit/peering links, das Pakete mit folgenden Eigenschaften einschränkt:
  - Protokoll: UDP
  - Destination Port: 123
  - Packet Size (IP Layer): Ungleich 76 Byte

```
11:50:50.034744 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto UDP (17), length 76)
    10.10.1.130.56924 > 131.130.250.250.123: NTPv4, length 48
```

- Kurz: Limitiere alle NTP Anfragen, die nicht ganz normale time-sync Operationen sind.
- Das ist insbesondere relevant, wenn man die ntp-server im eigenen Netz nicht schnell in den Griff bekommen kann.

Mitigation: Leg 2

- Reflector -> Opfer
- Rate-Limit auf folgendes:
  - Protokoll: UDP
  - Source Port: 123
  - Packet Size (IP Layer): = 468 Bytes

```
12:05:33.392196 IP (tos 0x3,CE, ttl 56, id 59859, offset 0, flags [none], proto UDP (17),
length 468) 178.188.XXX.XX.123 > 10.10.1.130.34085: NTPv2, length
```

- Das sind NTP Antworten, die auf mehrere Pakete aufgeteilt werden. (NTP benutzt nicht IP-Layer Fragmentation, sondern macht das auf Application Layer, und erzeugt so konstante Paketlängen (bis auf das letzte Fragment), siehe RFC 1305, Appendix B)

Status ntp in Österreich

- Das Thema wurde Anfang 2014 heiß
- CERT.at bekam und verwendete Daten von http://openntpproject.org/
  - Viel positives Feedback
  - Erste Zahlen schauten gut aus
  - In die Maschinerie eingebaut und nicht mehr genau nachgesehen

Kalte Dusche

Geographic Distribution. We also investigated the geographical distribution of the amplifiers. For this, we used the MaxMind GeoIP database [23] to assign a country to the IP address of an amplifier. We then compared how the numbers of amplifiers evolve in single countries.

US and Europe compared to the rest of the world. But it also shows that the current network of CERTs is not perfectly connected to share our information equally in all countries. For example, also European countries like France (35.1%) and Austria (47.1%) lag behind the average decrease. However, on an absolute scale, the situ-

- https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/kuhrer

Andere UDP Protokolle?

Aus: http://christian-rossow.de/articles/Amplification_DDoS.php

	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

Wie viele gibt es?

CERT.at

Protocol	Amplifiers	Tech.	t_{1k}	t_{100k}
SNMP v2	4,832,000	Scan	1.5s	148.9s
NTP	1,451,000	Scan	2.0s	195.1s
DNS_{NS}	255,819	Crawl	35.3s	3530.0s
DNS_{OR}	7,782,000	Scan	0.9s	92.5s
NetBios	2,108,000	Scan	3.4s	341.5s
SSDP	3,704,000	Scan	1.9s	193.5s
CharGen	89,000	Scan	80.6s	n/a
QOTD	32,000	Scan	228.2s	n/a
BitTorrent	5,066,635	Crawl	0.9s	63.6s
Kad	232,012	Crawl	0.9s	108.0s
Quake 3	1,059	Master	0.6s	n/a
Steam	167,886	Master	1.3s	137.1s
ZAv2	27,939	Crawl	1.5s	n/a
Sality	12,714	Crawl	4.7s	n/a
Gameover	2,023	Crawl	168.5s	n/a

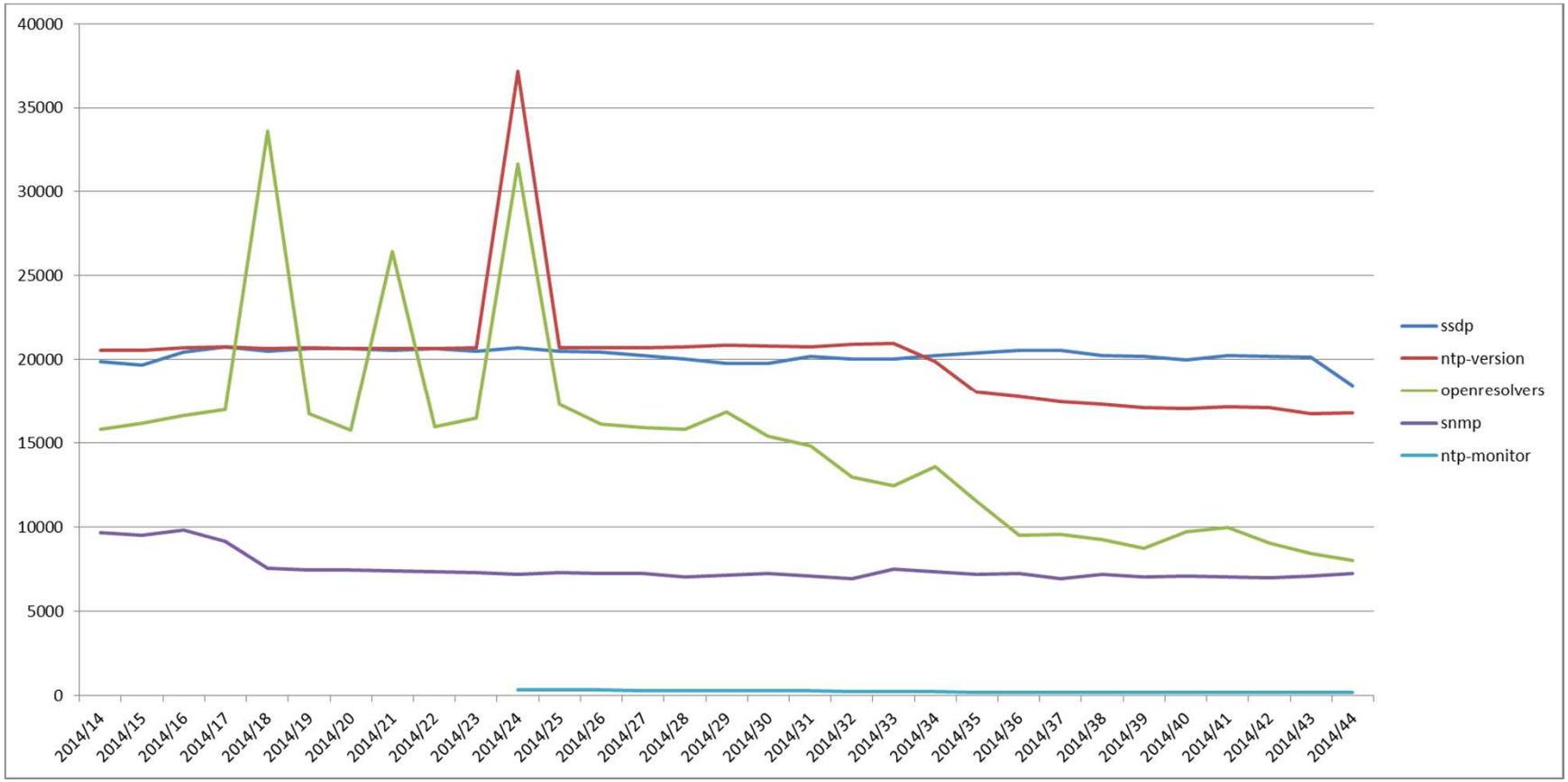
- **The scannings will continue until the Internet improves**
  - The news and our networks have been full of articles and packets related to the different UDP amplification attacks that have been ongoing. We and several other researchers have been looking at this problem for a while and while there are not any easy solutions we can at least make network owners more aware of the issues that we can see on their networks from the outside. This has led to some interesting results, most of which are not pleasant.
  - There are also a large number of services that should not be exposed because they are usually trivial to exploit or abuse. Some of these might expose data or even allow remote access to systems that should not be open to the public.

- http://blog.shadowserver.org/2014/03/28/the-scannings-will-continue-until-the-internet-improves/

Andere Protokolle?

Protokoll	IP-Adressen in AT (gerundet)
DNS Open Resolver	9.000
NTP Version	17.500
NTP Monlist	168
SNMP	6.900
SSDP	20.200
chargen	178
QOTD	63
IPMI	2.400

Entwicklung?



Nur UDP?

- TCP sollte durch den three-way-handshake abgesichert sein
- Diverse Bugs in Implementationen
  - ☹
  - Siehe https://www.usenix.org/conference/woot14/workshop-program/presentation/kuhrer

TCP Amplifiers (1)

Table 1: Number of potential amplifiers with an amplification factor > 20 based on scans of 20 million hosts

	20 million random hosts			Estimation (IPv4)
Protocol	# Responsive	# Amplifiers	Amplifier Ratio	# Amplifiers
FTP	705,371	13,701	1 : 51	2,945,715
HTTP	715,354	1,746	1 : 409	375,390
IMAP	683,567	9	1 : 75,951	1,935
IPP	702,590	19	1 : 36,978	4,085
IRC	648,688	7	1 : 92,669	1,505
MySQL	672,336	8	1 : 84,042	1,720
NetBIOS	517,482	44	1 : 11,760	9,460
NNTP	667,598	8	1 : 83,449	1,720
POP3	689,716	7	1 : 98,530	1,505
SIP	711,210	87	1 : 8,174	18,705
SMTP	674,815	12	1 : 56,234	2,580
SSH	657,916	384	1 : 1,713	82,560
Telnet	575,067	9,315	1 : 61	2,002,725

TCP Amplifiers (2)

Table 2: Number of potential amplifiers per protocol based on scans in the entire IPv4 address space

		# Amplifiers with amplification factor					
Protocol	# Responsive	> 20	> 50	> 100	> 500	> 1,000	> 2,500
FTP	152,026,322	2,913,353	3,500	1,868	1,032	937	847
HTTP	149,521,309	427,370	15,426	6,687	1,596	649	347
NetBIOS	82,706,193	12,244	2,449	1,463	873	811	783
SIP	154,030,015	22,830	5,158	3,913	3,289	3,123	2,889
SSH	141,858,473	87,715	4,611	2,141	1,275	1,176	1,082
Telnet	126,133,112	2,120,175	16,469	7,147	2,008	1,393	994

Was tun bei TCP?

- Wir haben dazu noch keine Datenquelle.
- Siehe Paper, es dürften primär embedded devices / Appliances sein
- Im DDOS-Fall:
  - RST senden kann etwas helfen.

Aktuelle Empfehlungen

TODO 1: Anti-Spoofing

- IP Address Spoofing unterbinden
  - 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
  - Um so näher am Kunden, um so einfacher und besser
  - **Datacenter**, DSL, Kabel, Standheitungen, …
  - Kleine ISPs: Filter am Upstream
  - Automatisieren!

TODO 2: Server Absichern

- Reflektoren/Verstärker aus dem Netz nehmen.
  - Vergleichbar mit den offenen SMTP Relays vor 20 Jahren
- DNS
  - Keine offenen rekursiven Nameserver
    - http://openresolverproject.org/ (Datenqualität ist nicht perfekt)
  - Rate-Limit auf authoritativen Servern
    - http://www.redbarn.org/dns/ratelimits
- NTP
  - Zugang (insb. Control Protocol) einschränken
    - http://openntpproject.org/
- SSDP
  - CPE Konfiguration testen und fixen
- …

TODO 3: Traceback!

- Wir müssen wissen, aus welchen Netzen die gefälschten Pakete kommen
  - Sonst wird dort nie aufgeräumt
- Angenommen der Verstärker ist in **Ihrem** Netz: Können sie die gefälschten Pakete rückverfolgen?
- Werkzeuge & Prozesse & Fähigkeiten
  - Netflow -> Interface
  - Und bei Internet Exchange Points?

TODO 4: Das eigene Netz schützen.

- Der Spamhaus DDOS ging:
  - Initial gegen den Webserver
  - Dann gegen die Cloud-basierte DDOS Protection
  - Dann gegen die unicast addressen der Cloudflare sites
  - Dann gegen deren Routen
  - Dann gegen deren Adresse am London Internet Exchange
- Daher:
  - Absicherung der eigenen control plane
  - Optimal: Paket an eigene Infrastruktur erst gar nicht ins Netz lassen

TODO 5: Kooperation!

- Kleinere (d.h. nicht Tier1) Netzwerken können nicht jeden Angriff abwehren
- Mitigation braucht Kooperation
  - Beziehung zum Upstream ISP aufbauen
  - Was kann dieser manuell machen?
  - Automatiken? (z.B. remote triggered blackholing)
  - Vernetzung mit Peers / CERTs / LE
- Vorausplanen:
  - Siehe auch Barry Greenes „The Service Provider Tool Kit" http://www.nanog.org/meetings/abstract?meet=54

Ausblick

- DDOS Angriffe sind keine Seltenheit
- Man kann sie für sehr wenig Geld kaufen („Booter“ oder „Stresser“ Services)
- Motive?
  - Erpressung
  - Payback
  - Oft auch ohne bekanntem Grund
- Viele Firmen sind darauf überhaupt nicht vorbereitet

- **So wichtig wie das Internet inzwischen ist, müssen wir das in den Griff bekommen.**

Fragen?

Otmar Lendl <lendl@cert.at>

+43 1 5056416 711