SLAC 2016

- Workshop -

Fighting DDoS for Fun and Profit

Berlin, 17.06.2016

8ack GmbH

Agenda


400 GB/s
Amplification
BotNetz
DDoS
CyberCyber
Schutz
Misuse
Chaos
BGP
Angriff
Layer-7
Layer-3/4
Reflection
Layer-2
100Mio Devices
Assholes
Cyber-Cyber

Disclaimer


DON'T TRY WHAT YOU'RE
ABOUT TO SEE AT HOME
WE'RE WHAT YOU CALL
EXPERTS

Disclaimer

DDoS - was ist das?

DDoS - was ist das?

- TL;DR:
  Verbrauch aller Ressourcen -> Dienst/Netz nicht verfügbar

  DDoS-Angriffe sind die Molotov-Cocktails des Internet: manchmal machen sie einfach nur „PÜFF!“, manchmal sind verheerende Zerstörungen die Folge

DDoS - Auswirkungen

- bei Erfolg:
  - massiver Stress in der Administration
- nichts geht mehr, Ausfall von Infrastruktur
  - Kaskadeneffekte
  - Internetgateway
  - Mail / DNS / VOIP - Infrastruktur
  - einzelne Dienste, Kommunikationsschnittstellen

DDoS - Auswirkungen

- geerbte Probleme
  - z.B. zu geringe Netzsegmentierung
  - Risiken anderer Netzteilnehmer schlagen auf eigene Systeme durch
  - Ausfall von X führt zu Problemen bei Y,Z, z.B. DNS

DDoS - die globale Bedrohung

- DDoS-Angriffe
  - unterbinden internetbasierte Kommunikation und Geschäftstätigkeiten
  - sind für die Angreifer vergleichsweise billig
  - für Angreifer: moderate Skills notwendig, kaum eigene Infrastruktur
  - sind für die Angegriffene bei Erfolg immer ein Problem
- DDoS-As-A-Service: DDoS-Angriffe für 30 $/Monat mieten, ernstzunehmende Angriffe ab 50 €/h
- hohe Kosten für die Angegriffenen:
  für 50% der Angriffe > 10.000 $/h

DDoS - die globale Bedrohung

- Zahlen
  - 20 Mio NTP-Server
  - 40 Mio DNS-Server
  - 1 Mio CharGEn
  - 30-60 Mio SSDP
  - ——————————————————
  - 100 Mio potentielle Reflektoren (Volumenangriffe)

- Zahlen
  - 200.000 Server in Botnetzen
  - 1/3 der Webseiten WordPress X00.000 ?
  - 60% Apps und Dienste outdated
  - ——————————————————
  - mehrere 100.000 Bots

DDoS - die globale Bedrohung

DDoS-Attacke

Hackerangriff legt Schweden lahm

12.12.2014, 11:33 Uhr | t-online.de

ZUR STARTSEITE

Wer steckt hinter den DDoS-Attacken?

Wegen heftiger DDoS-Angriffe waren zahlreiche Schweizer Online-Shops unerreichbar. Wer war das? Fünf mehr und minder mögliche Szenarien.

Home | Video | Themen | Forum | English | DER SPIEGEL | SPIEGEL TV | Abo | Shop

SPIEGEL ONLINE NETZWELT

Politik | Wirtschaft | Panorama | Sport | Kultur | Netzwelt | Wissenschaft | Gesundheit | einestages | Karriere | Uni | Reise | Auto | Stil

ANZEIGE

KURZ NOTIERT: SECURITY

Aktuell: DDoS und Carbanak schlagen gegen Banken zu

An diesem Rosenmontag scheinen es besonders auf Banken abgesehen zu
inem Alert seines Emerceny Response Teams
rare auf entsprechende Pläne des Hacker-
Anonymous hin und auch zu Carbanak soll
us anderer Quelle) neue Informationen

k of England und die New York Stock Exchange
uem heutigen Montag an im Visier von DDoS-
ßt es aus Anonymus-Kreisen. Das
dest Radware. Mit Hilfe einer verteilen
er DDoS) soll die Netzwerkinfrastruktur
ngelegt werden. Auch andere Banken
(S-Systems (Bank for International Settlements) müssten, laut Radware, mit Angriffen

Wegen Jazenjuk-Besuch: Hacker legen Website der Bundeskanzlerin lahm

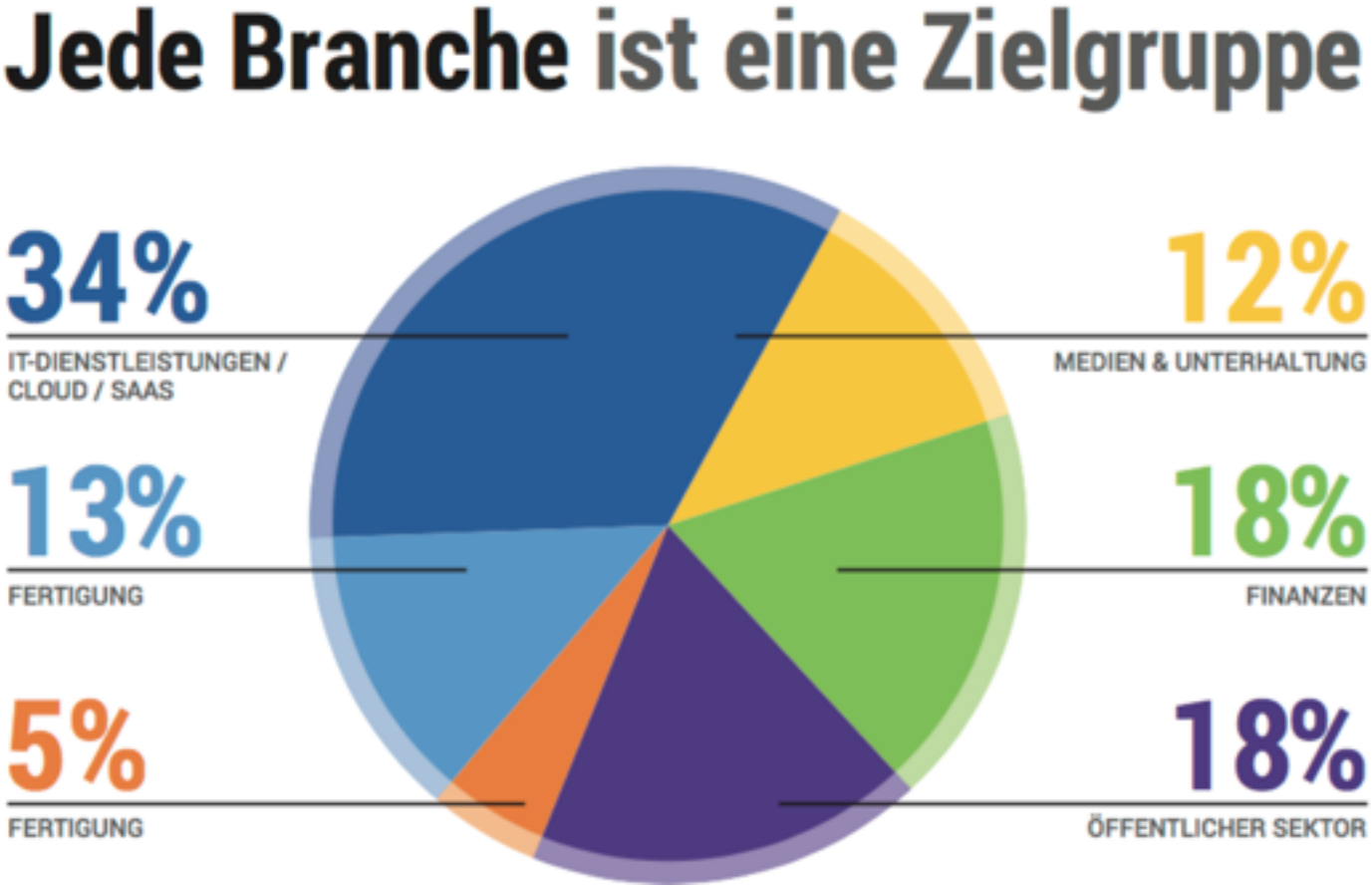
Spiegel Online zwischen Stromausfall und DDoS-Attacken

21. November 2015 By Lars 'Ghandy' Sobiraj — 25 Comments

Twittern

45 20

DDoS - die globale Bedrohung



Motive

- kriminelle Geschäftsmodelle:
  - Erpressung -> hauptsächlich gegen ECommerce
  - Unterbinden von Konkurrenz, betrügerische Geschäfte
- politische Akteure:
  - Informationsunterdrückung (DDoS gegen Parteien und Institutionen)
- staatliche gesponsert
  - Störung kritischer Infrastruktur (KRITIS -> Windparks, Kraftwerke, Bahn)
  - Informationsunterdrückung (Great Firewall-DDoS, Angriffe gg ukr. RZ)

DDoS - Akteure

- Booter-Services (Stresstester)
  - Volumen: 5 GB/s (meist < 1 GB/s)
  - Applikation: meist nur Web
  - funktioniert gegen Home-DSL (Gamer)
  - funktioniert gegen schwache Server
  - ab 30 $/Monat
  - nicht sehr zuverlässig
  - keine Gefahr für alles, was nicht Wald & Wiesen-Infra ist

DDoS - Akteure

- Erpressergangs
  - Volumen: bis 100 GB/s
  - Applikation: alle
  - manchmal auch Botnetze / 20.000 Bots (meist Server)
  - 1 BTC - 15 BTC
  - teilweise Trittbrettfahrer
  - Doomsday für ungeschützte Systeme
  - Schweiz, DE, Hoster, ECommerce, Banken, ISP

DDoS - Akteure

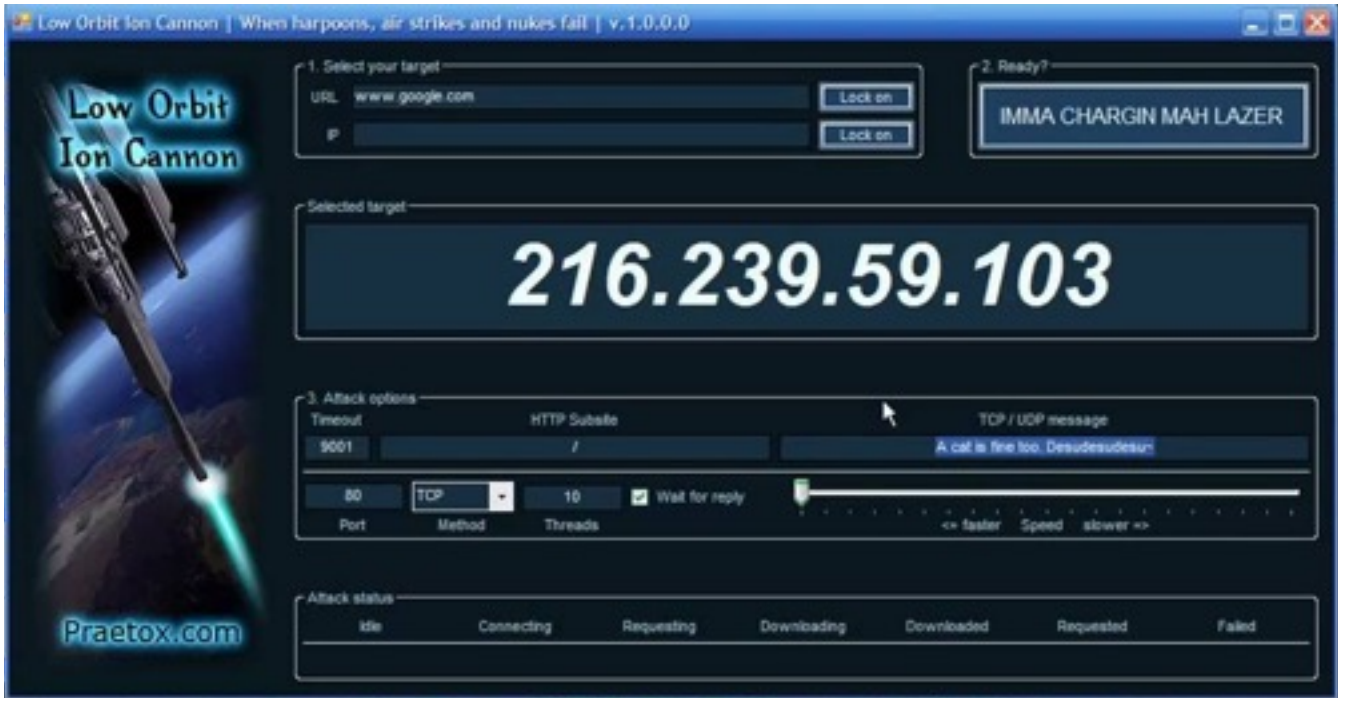
- DDoS-4-Rent
  - Botmaster
  - Einzelakteure/kleine Gruppen
  - ab 50 € / h je 1 GB/s (2 Mio pps)
    wird günstiger, ab 5 €/h ?
  - Botnetze (1000+)
  - Amplification/Reflektion
  - kann ungeschützten Systemen gefährlich werden

DDoS - Beispiele

- Habbo Hotel (2006)

DDoS - Beispiele

- LOIC: VISA, PayPal, MasterCard (2010)



DDoS - Beispiele

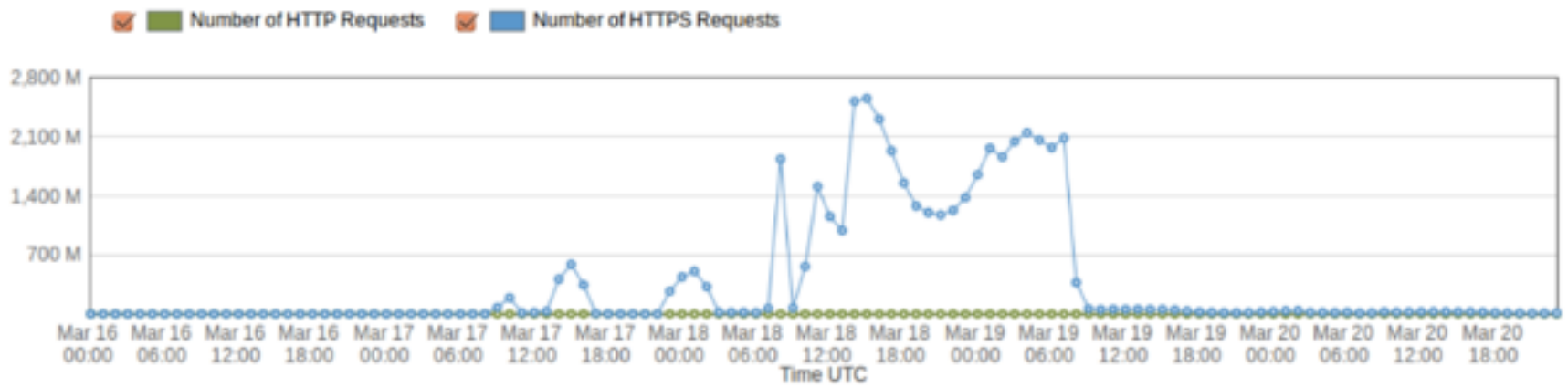
- Ausfall TeliaSonera - Schweden Offline (2014)
  - Angriff gegen eine Gamin-Site
  - TeliaSonera überlastet
  - 60% der schw. Haushalte offline
  - VOIP komplett ausgefallen

DDoS - Beispiele

- Login-Bereiche Steam/EA Sports (2014,2015)

DDoS - Beispiele

- GreatCannon -> GitHub (2015)
  - 10 Mio Rechner über Javascript-Include
  - 1-50 Requests/Minute/Rechner



HTTP Requests:	**Total:** 0.2275 M	**Average:** 0.0019 M	**Minimum:** 0.0005 M	**Maximum:** 0.0423 M
HTTPS Requests:	**Total:** 43,874.9973 M	**Average:** 365.625 M	**Minimum:** 0.1442 M	**Maximum:** 2,558.823 M
All Requests:	**Total:** 43,875.2248 M	**Average:** 182.8134 M	**Minimum:** 0.0005 M	**Maximum:** 2,558.823 M

DDoS - Beispiele

- französische Streiks

DDoS - Negativbeispiel

- aus dem wahren Leben: ISP, mittelgroß
  - Business-DSL ohne DDoS-Schutz
  - nur ein Netz (/21, 1000 Kunden)
  - alle DNS-Server in diesem Netz
  - alle MX in diesem Netz
  - freies, stadtweites WLAN, auch über das Netz
  - Aussage (OT): DDoS? hatten wir noch nie …

DDoS - Negativbeispiel

- Problem:
  - jeder Kunde erbt die Bedrohung aller anderen Kunden
  - Angriffsziele gut zu verschleiern
  - kleine Ursache, große Wirkung
    (Slow Volume High Package -> Switch OFF)
  - Angriffe gegen Infrastruktur gefährden alle Kunden
  - freies WLAN (*.internet, nicht nur HTTP(S))

DDoS - Beispiel

- aus dem wahren Leben: Wohnungsgenossenschaft
  - auf dem platten Land: 16 MBit Business-DSL, feste IP, Fritzbox
  - VOIP, Verwaltungstool-as-a-Service, Email intern
  - 5 Tage Angriff, kein Email, kein Telefon, keine Anfragen, keine Möglichkeit der Kontaktaufnahme, keine Services
  - 1. Tag: Fehlersuche mit dem Provider Teil 1
  - 2. Tag: Fehlersuche mit dem Provider Teil 2
  - 3. Tag: Notfallbetrieb über UMTS
  - Chaos, riesen Backlog im Support, nach 2 Wochen wieder Normalbetrieb
  - Kosten für den Angreifer: 50 € / Tag

DDoS - Angriffsarten

- Volumenangriffe (V)
  - gegen den Uplink
  - gegen die Switch/NIC-Kapazitäten
- gegen Applikationen (A)
  - CPU, RAM, HD
  - Connections
  - Verarbeitungsressourcen

- Security-Devices (Sekundär)
  - IDS/IPS
  - Firewalls
  - bei Überlastung:
    Bypass, Schutz deaktiviert
  - SmokeScreening:
    Viiiiiieeeeeel Noooiiiise,

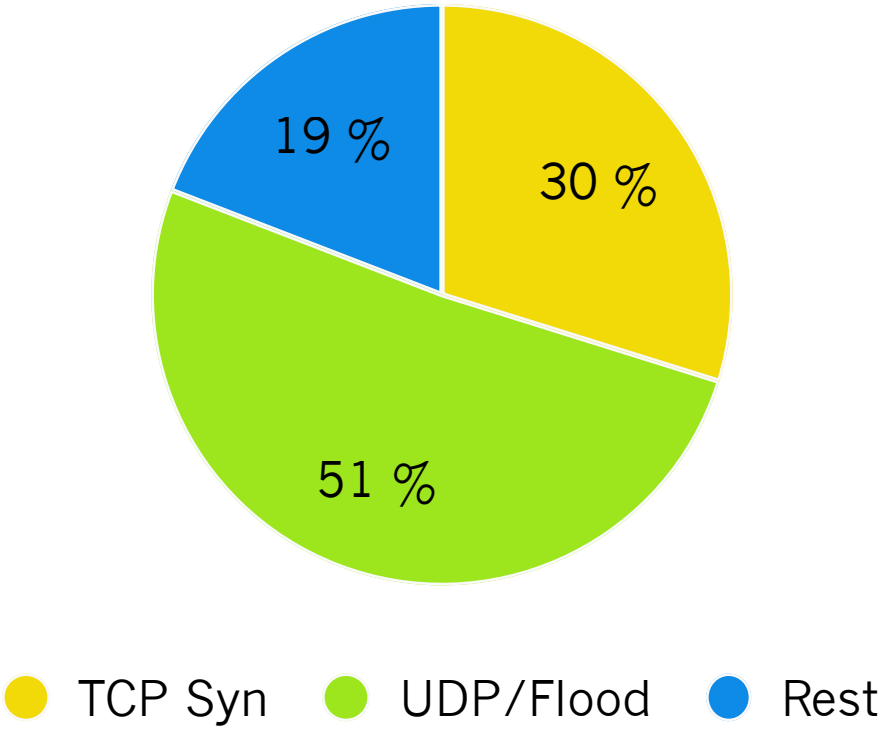
kaum Signal

DDoS - Volumenangriffe

- Volumenangriffe gegen den Uplink (Demo)
  - Netzwerk-Kapazität
  - Switch/NIC-Verarbeitungskapazität
  - Botnetz (TCP/UDP-Floods)
  - Reflektion/Amplification (NTP, DNS, SSDP)
  - Problem: 100 Mio Devices und Server mißbrauchbar

DDoS - Volumenangriffe

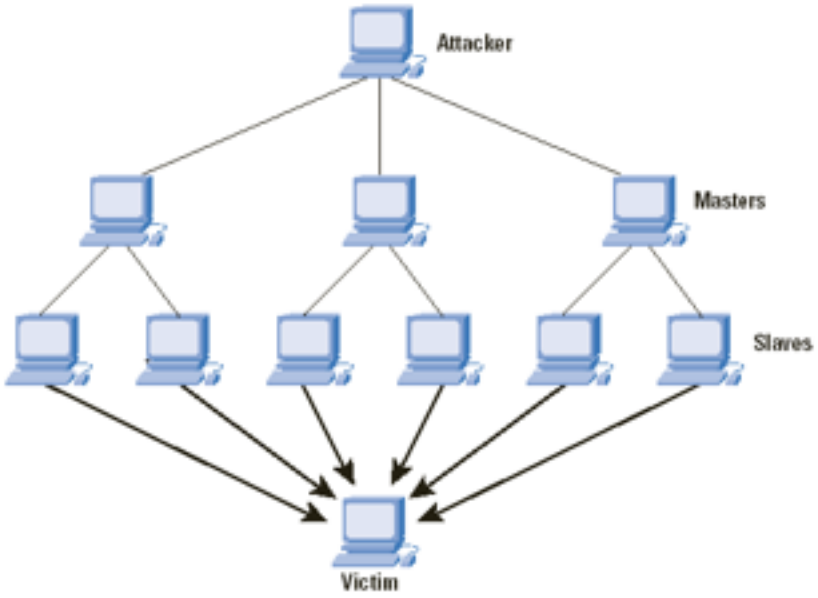
- Amplification-Faktoren

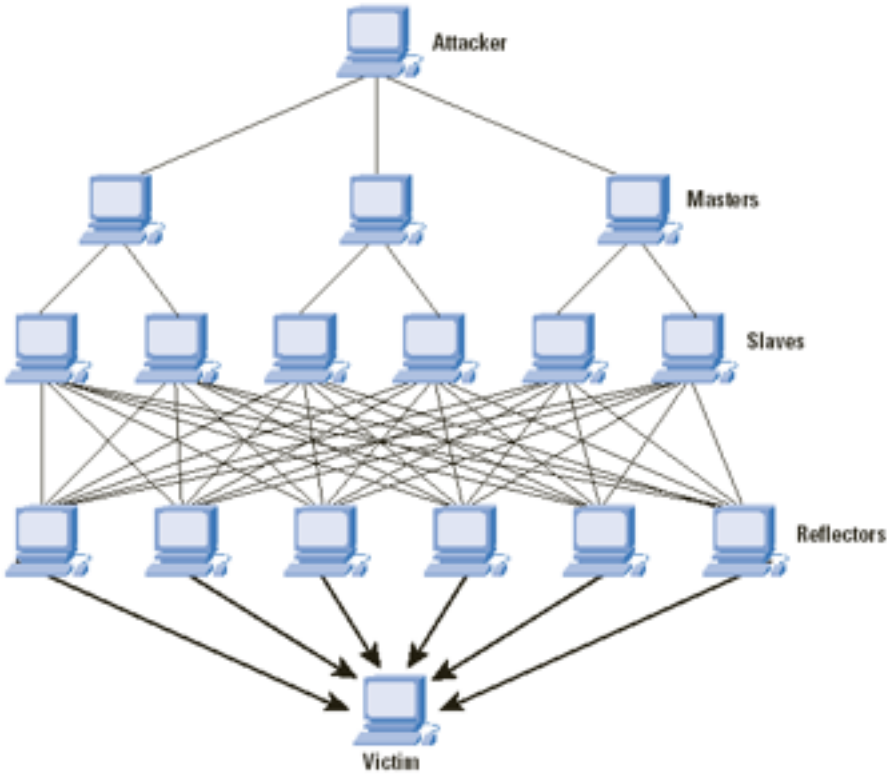


DNS	30-50
NTP	400-500
CharGen	300-400
SSDP	30

DDoS - Volumenangriffe

- Botnet vs Amplification/Reflection



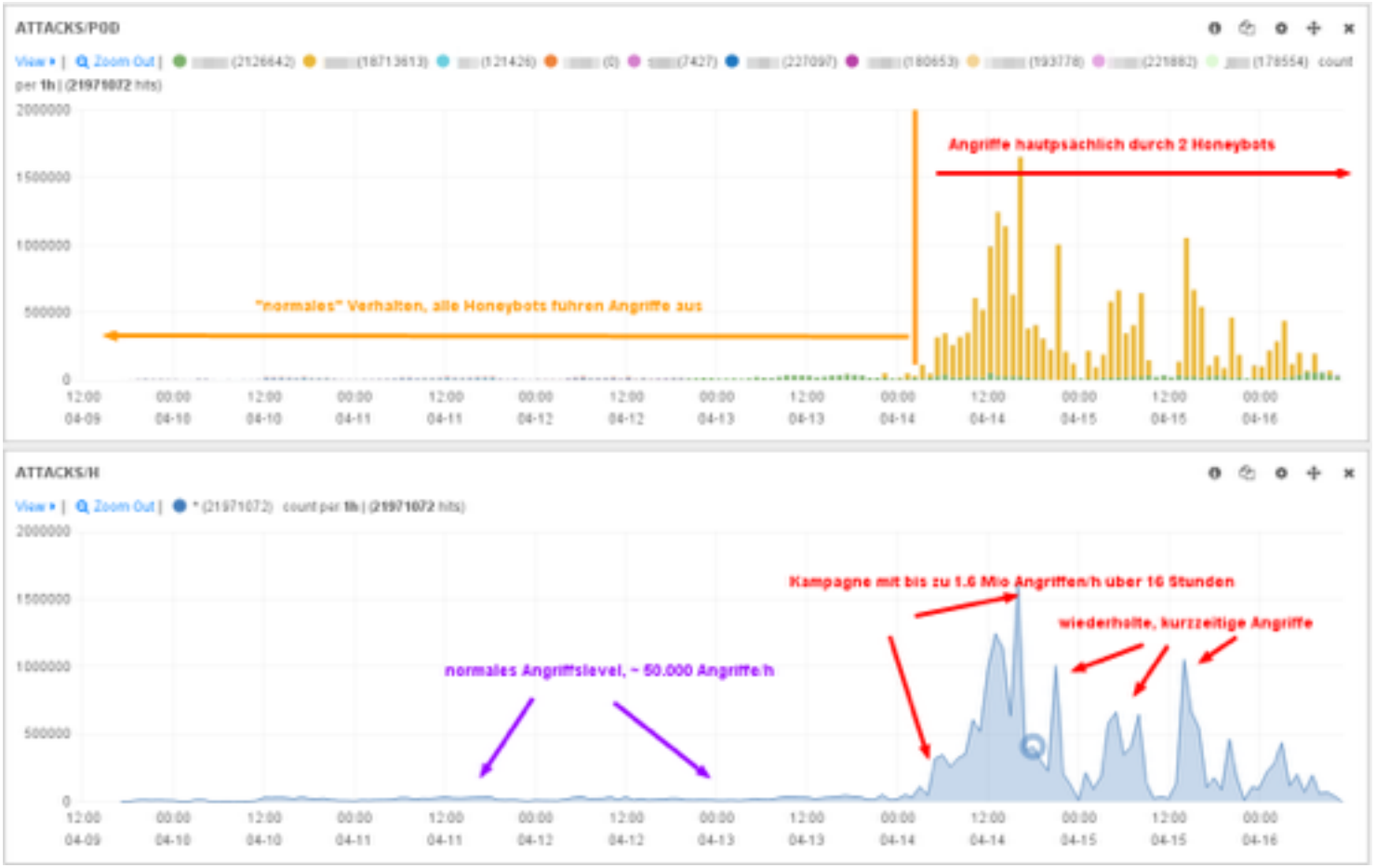


DDoS - Volumenangriffe

- 100 GB/s Angriff auf RZ in UK
- insg 15 Wellen, 9 Tage

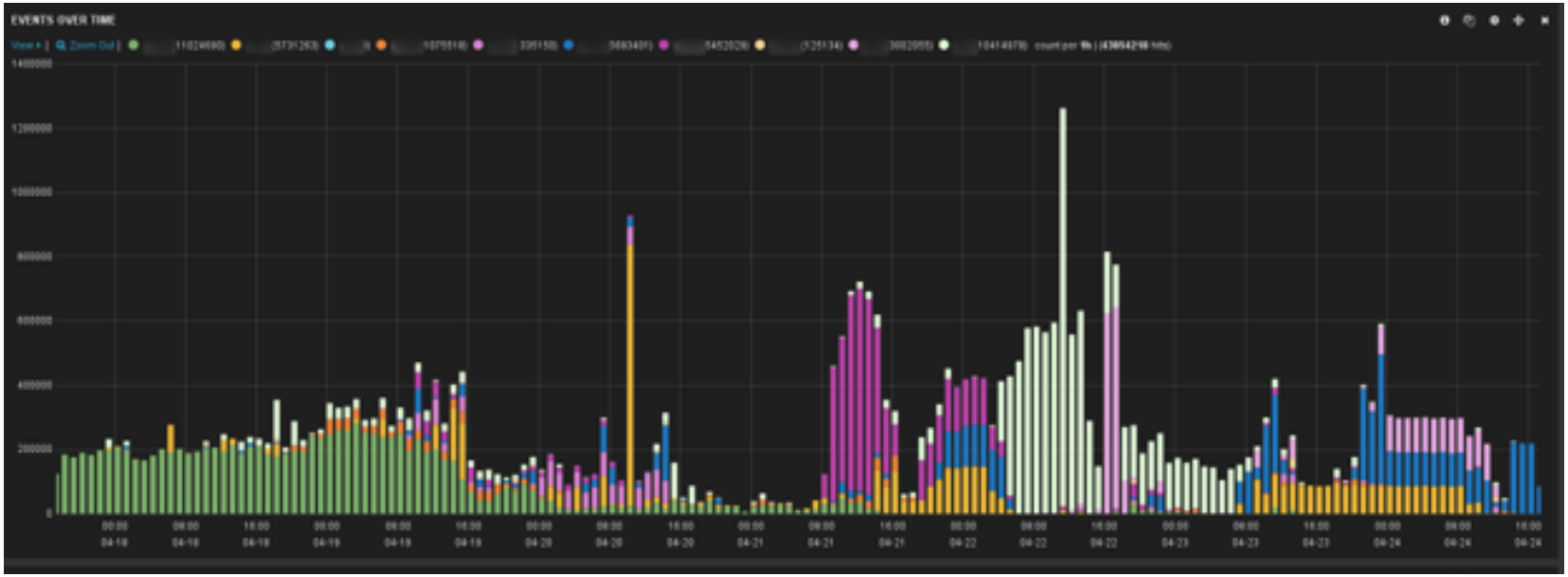
DDoS - Volumenangriffe

- Angriff auf chin. ISP



DDoS - Volumenangriffe

- 7-Tage-Kampagne



DDoS - Schutz

- it’s the Knowlegde, Stupid!
  - potentielle Bedrohung analysieren
  - Bewusstsein schaffen
  - Netz/System-Setup entsprechend konzipieren
  - Schutzmechanismen implementieren
  - Notfallübungen, analog zu Backup/Restore

DDoS - Schutz

- Basics im Setup
  - DNS: mind 2 Lokationen, besser: 3 versch. Provider
  - Kernservices identifizieren, eigenes Netz/DMZ
  - Fallbacks, wo möglich
  - Logs und Netflows
  - VPN-IP != Haupt-IP des Gateways
  - vorbereitet sein
  - Last Exit: Blackholing (BGP)

DDoS - Schutz - vorbereitet sein

- eigene Bedrohungslage analysieren
  - Paperwork
  - ist ext. Schutz möglich? (z.B. PCI DSS)
  - What if … für die wichtigsten Dienste
- Setup
  - Netze segmentieren
  - Angriffspunkte absichern (DNS, Mail)
  - Redundanzen, wo notwendig

DDoS - Schutz - vorbereitet sein

- Stresstests - Live oder Simulation
  - Watt de Buer nich kennt …
  - Wir sind sicher, wir haben DDoS-Schutz!
  - Schwachpunkte finden, Workflows optimieren
  - Handgriffe trainieren
  - Notfallpläne (ausdrucken)
  - Kontaktwege über Handy

DDoS - Schutz - vorbereitet sein

DDoS - Schutz - technisch

- eine Frage der techn. Limits:
  die Leitung muss immer dicker sein als das Angriffsvolumen + Traffic
  Lösung: nur Scrubbing-Center (Cloud)
- PerfTuning NIC -> bis 50% mehr Leistung (bedingt)
  Lösung: nur Scrubbing-Center (Cloud)
- Ideallösung PAL: Netzprovider hat eine DDoS-Lösung, die den Angriff zuverlässig herausfiltert

DDoS - Schutz - technisch

- Appliances
  - 40-150 GB/s
  - Tuning und Settings müssen! getestet werden
  - keine ClickAndRun - Lösung
  - Uplink ist das Limit
  - Inbound, Standby, Out-of-Band/Detection-Only
  - Workflows und Tests sind wichtig

DDoS - Schutz - technisch

- Cloud/Hybrid-Lösung
  - Goldstandard: 300GB/s
  - Platinstandard: 1000 GB/s
  - inbound oder on-demand (BGP-Rerouting)
  - muss trainiert werden
  - Daten gehen im Zweifelsfall über ein externes RZ

DDoS - Spaß am Gerät

- Wir basteln uns ein Reflektion/Amplification Botnetz
  - Poor Mans Botnet
  - keine große Infrastruktur, kein C&C
  - keine „Hacking-Skills“
  - moderate Programmierskills
  - moderate Kenntnisse von TCP/IP-Netzen
  - jeder halbwegs erfahrene Linux/Netzwerk-Admin

DDoS - Spaß am Gerät

- Wir basteln uns ein Reflektion/Amplification Botnetz
  - scans.io -> alle pot. Reflektion-Targets, ca 400 GB Daten
  - Scanner, Receiver, und Sender, kein C&C
  - Reflektion-Scans: 2 Tage, 1000 Reflektoren
  - 20 Server a 5 Euro/Monat als Sender
  - pro Sender: 50 Reflektoren a 0.1 Mbit/s
  - Faktor: 100 -> 0.1 Mbit in == 10 Mbit out * 1000 == 10 GB/s
  - nach 3 Tagen einsatzbereit
  - Kosten: knapp 100 Euro/Monat + Arbeitszeit

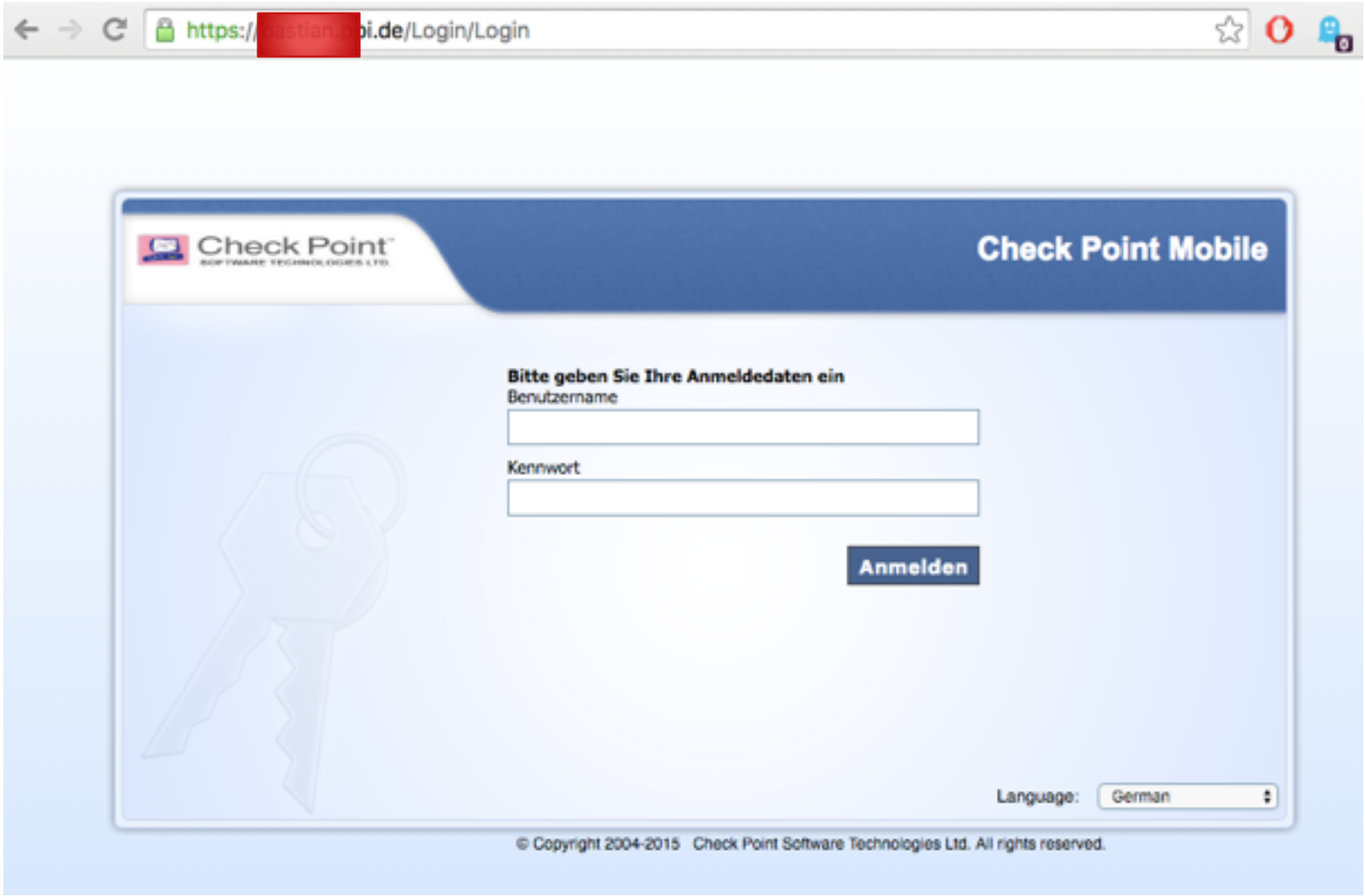
DDoS - Spaß am Gerät

- die fiesen Nummern
  - Tsunami-Floods
  - Low Volume High PkgCount
  - FastFlux - Attacks
  - Stop-And-Go
  - Angriffe gegen DNS, MX
  - verteilte Infrastruktur -> verteilte Angriffsziele

DDoS - Volumenangriffe - Schutz

- aber aber … Firewalls mit eingebautem Anti-DDoS-Filter!
  - 😀 TCP-Syn-Floods
  - 😀 UDP-Floods
  - 😱 Uplink-Saturation
  - 😱 NIC-Saturation
  - 😱 Log/Service Saturation

DDoS - Volumenangriffe - Schutz



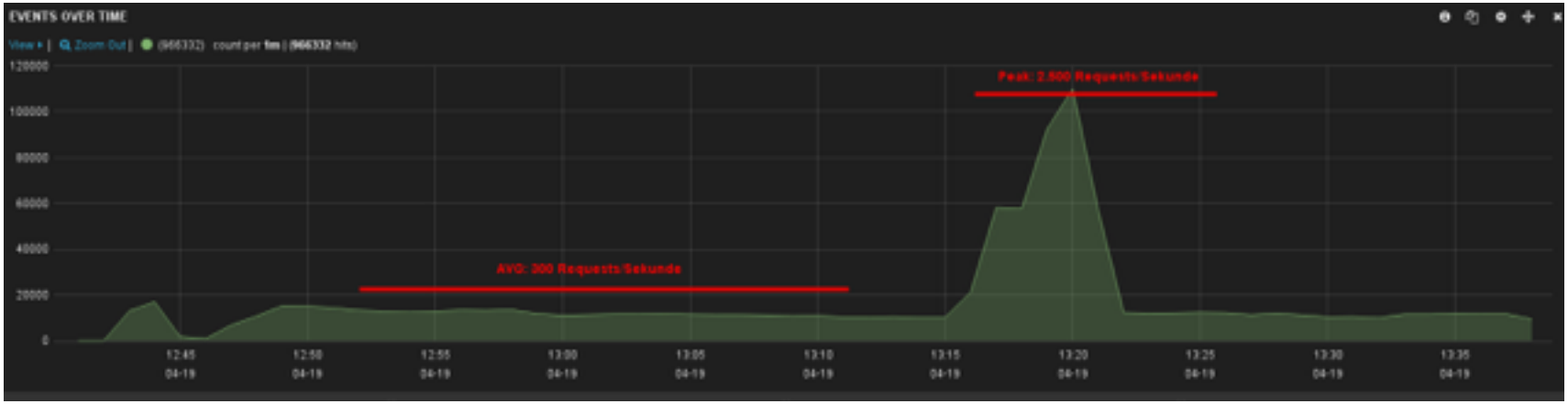
DDoS - Angriffe - Application/Layer7

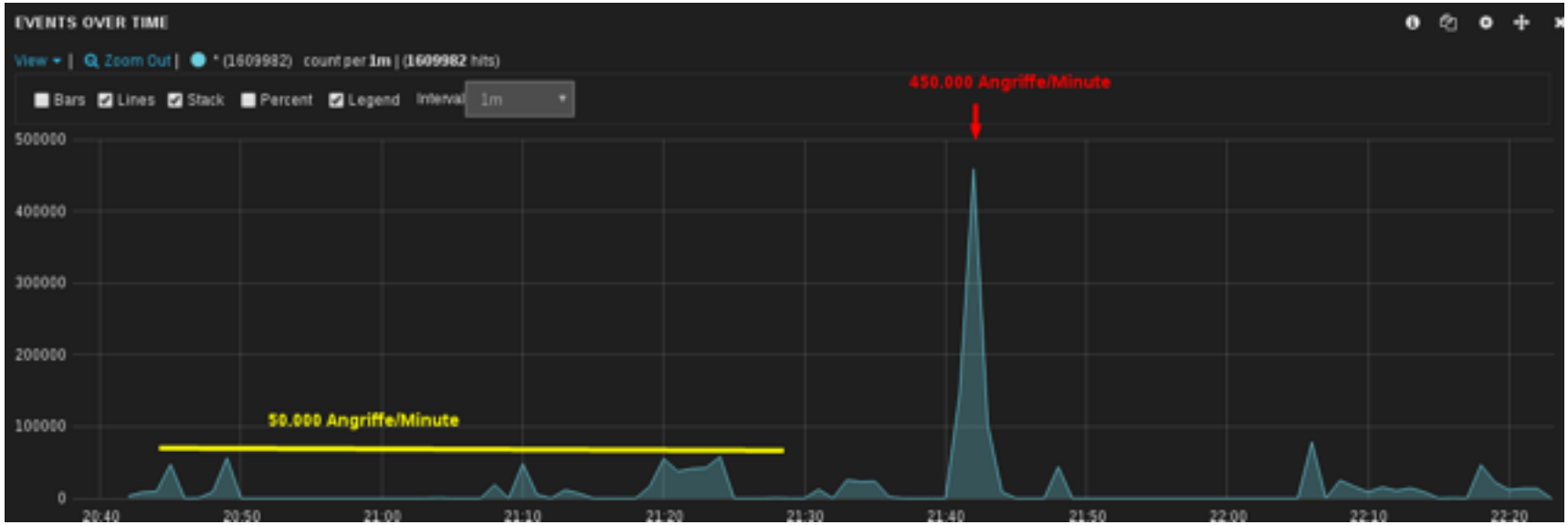
- Angriffe gegen Applikationen (A)
  - CPU, RAM, HD
  - Connections
  - Verarbeitungsressourcen
  - Logs

DDoS - Angriffe L7

- HTTP Reflection Attacken
  - WordPress xmlrpc.php
  - Drupal
  - Joomla
- CDN Reflection Attacks
  - Akamai (2015)
  - Cloudflare (2016)
- BruteForce-Attacks
  - MySQL
  - RDP
  - SSH
- SSL Exhaustion (CPU)
  - Renegotiation

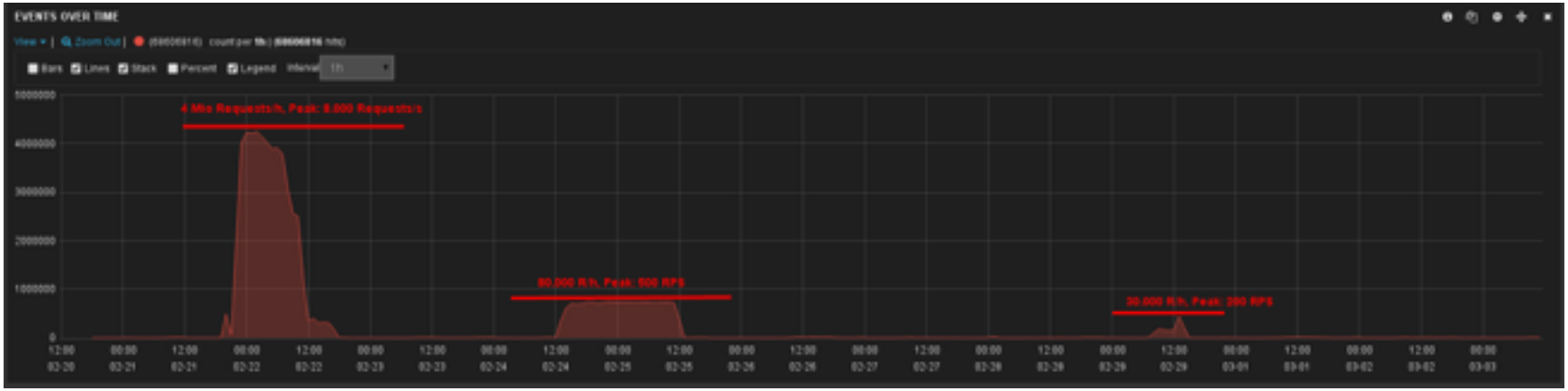
DDoS-Angriffe - HTTP/Reflection

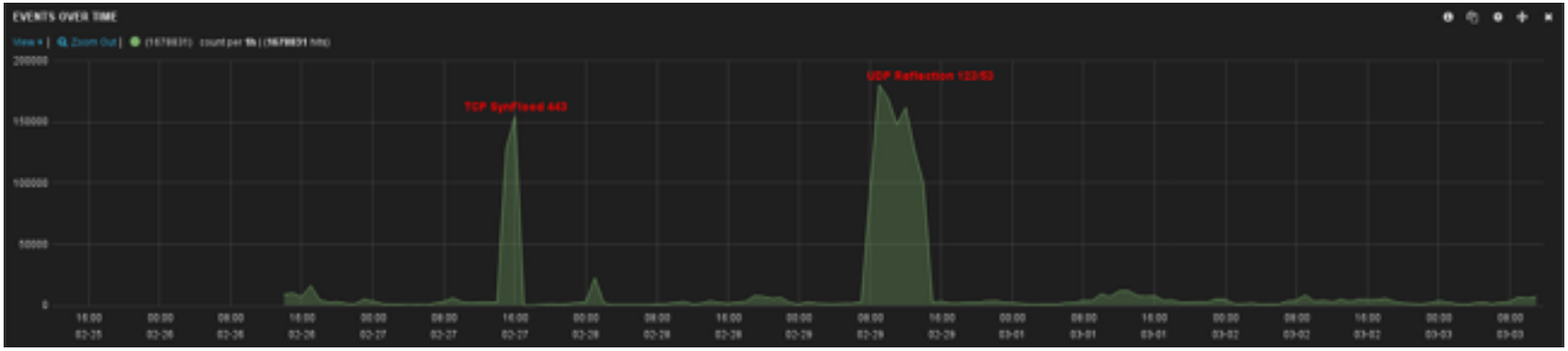




DDoS-Angriffe

- L7 - SSL Renegotiation, Floods





DDoS-Angriffe - CDN-Reflection

- Cloudflare CDN-Attack

DDoS-Angriffe - Google

- Google Docs

DDoS - Angriffe L7

- Auswirkungen:
  - Service Down
  - Backend Down

- Schutz:
  - Logik in der Anwendung
  - Rate-Limiting

DDoS - Angriffe L7

- Schutz/HTTP:
  - Caching, Optimierung
  - ~~Challenges~~ sind gescriptet lösbar
  - WAF/HTTP-Anti-DDoS (verhaltensbasiert)

DDoS - Layer 7

- die fiesen Nummern
  - Upstream-Saturation (Server)
  - FastFlux / Low Volume High Count
  - Angriffe auf einzelne neuralgische Punkte
  - Stop-And-Go

DDoS - Angriffe - Was Tun im Falle eines Falles?

DDoS - Erstmaßnahmen

- Vorbeugen ist besser als auf die Schuhe k*tzen
- notwendiges Personal alarmieren, aber: viele Köche …
- wenn möglich, Profis zu Rate ziehen
- gedruckte Netzwerk/Systemdoku/Topologie Notfallpläne bereithalten
- Art und Weise des Angriffs analysieren und bewerten
- ISP/Provider informieren und Hilfe einholen
- absolut kritische Dienste und Verbindungen identifizieren und priorisieren, alles andere Sperren
- Fallbacks und Mitigations eruieren

DDoS - Erstmaßnahmen

- Auswirkungen auf Business an Verantwortliche melden
- DNS TTL runtersetzen
- Logs, Netzwerk-Analyse:
  - kann die Attacke in der Systematik bewertet werden?
  - Signaturen?
  - Lohnt ein DogFight?
  - Kann der Angriff gebremst werden?
  - können Teile der Infrastruktur deaktiviert werden?
  - !! immer nur EINE Maßnahme zur Zeit

DDoS - Erstmaßnahmen

- Blackholing
- Umrouten von Netzen / BGP
- Strafverfolgungsbehörden
- ständig abwägen:
  - was ist absolut notwendig?
  - was habe ich noch zur Verfügung?

DDoS - Nachbetrachtung nach einem Angriff

- Lessons learnt
- gab es eine Erpressung?
- Systeme optimieren
- Workflows optimieren
- notwendige Mitigations eruieren
- GOTO 10

Fragen?

ddos@8ack.de

https://8ack.de