babiel

Fight for your website!

Beispiele zur Abwehr von Angriffen

Armin Pech

Babiel GmbH

```
ab -t 5 -c 11 -n 2016 https://openrheinruhr.de/
```

www.example.com is DOWN

- 18:40 Feierabend
- 18:50 Monitoring: Webseite DOWN
- 19:00 Frontend: 164.000 HTTPS-Conns
- 19:10 Connection Limit + IP-Blacklisting
- 19:15 Kontakte informiert

www.example.com is DOWN

- **19:20 Logfiles: Wordpress Pingback**

```
"GET / HTTP/1.0" 403 188 "-"
"WordPress/3.7.15; http://www.old-
 wordpress.com; verifying pingback
 from 123.45.67.98"
```

www.example.com is DOWN

- 19:40 Webseite wieder erreichbar
- Zeitraum: ~1 Stunde
- 16 Mio. TCP-Verbindungen (4.450/Sek.)
- 5,5 Mio. TLS-Verbindungen (1.530/Sek.)
- 32.000 HTTPS-Requests
- 6.700 Quell-IPs (Zombies)
- 3 Urspung-IPs (Badguys)

Motivation?


FFFFFFF
FFFFFFF
FFFFFFF
FFFFF
FFFFF
FFFFF
UUUU
UUUU
UUUU-


THE UNITED STATES OF AMERICA
ONE
ONE DOLLAR
THE UNITED STATES OF AMERICA
THE UNITED STATES OF AMERICA
FIVE
FIVE DOLLARS
FIVE


КИБЕРБЕРКУТ
МЫ НЕ ЗАБУДЕМ
МЫ НЕ ПРОСТИМ


WE ARE
ANONYMOUS

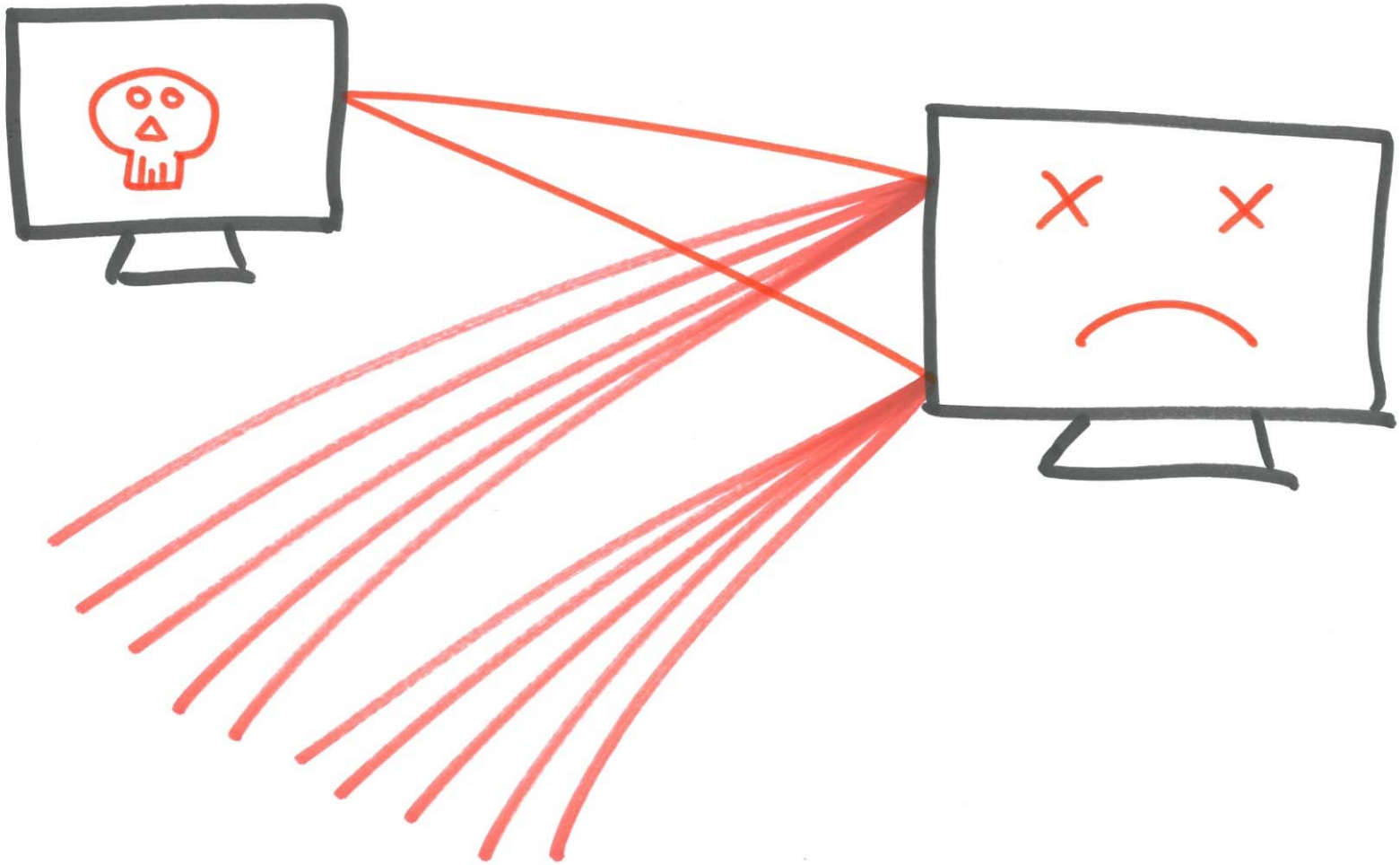
Vorzeichen

- Angriffe gegen Wettbewerber
- Politische Geschehnisse
- Sharing Plattformen
- Social Media
- Drohungen

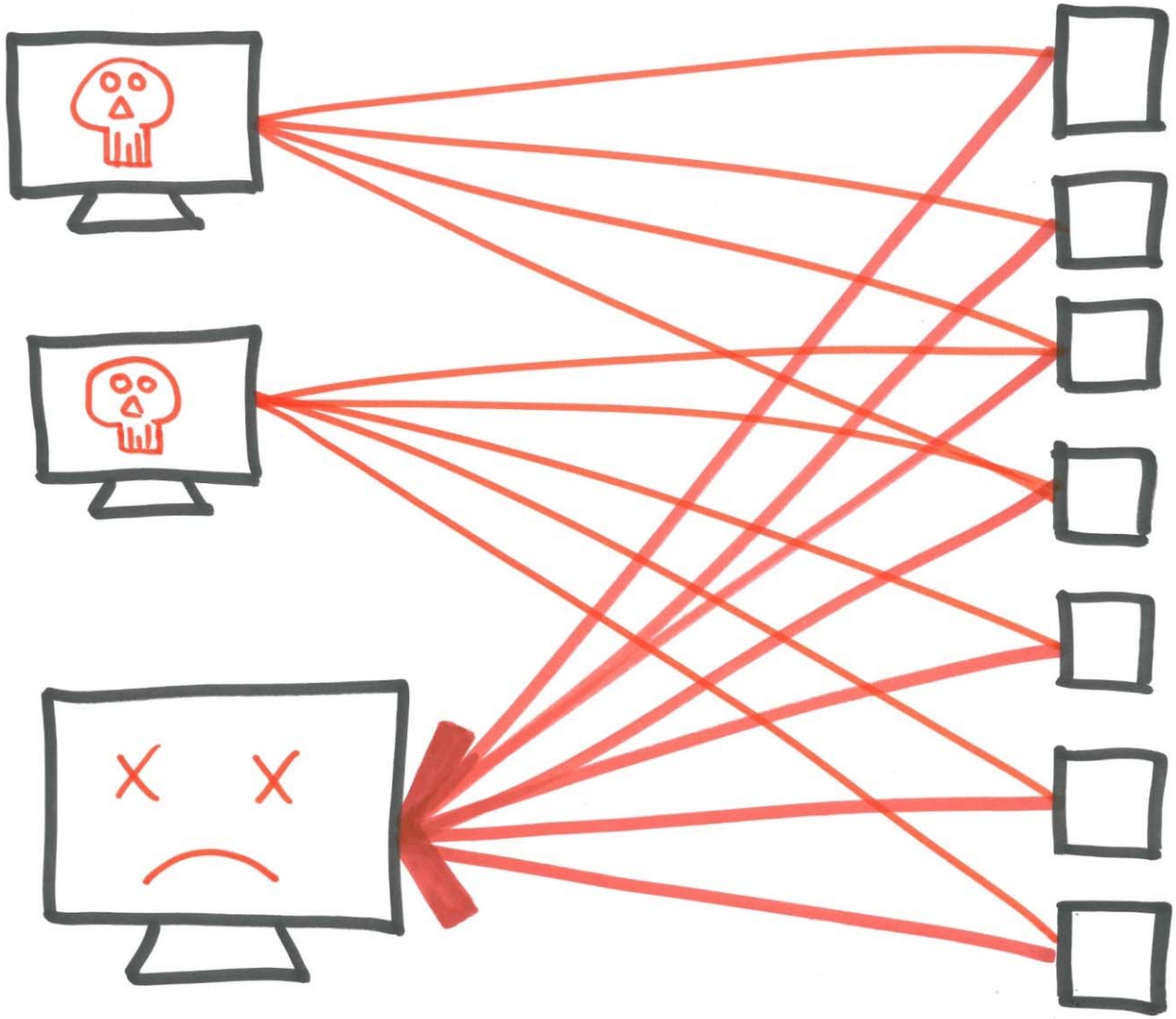
Gesehen Angriffe seit 2013

- Amplification: NTP, DNS (Public Services)
- SYN-Flood, IP-Fragments, TCP Window Size
- Web LOIC (Anonymous, Tango Down)
- HTTP Pingback
- HTTP Reflection / Download
- HTTP Low and Slow (Slowloris)
- Layer 7: Spezifische Lastgenerierung

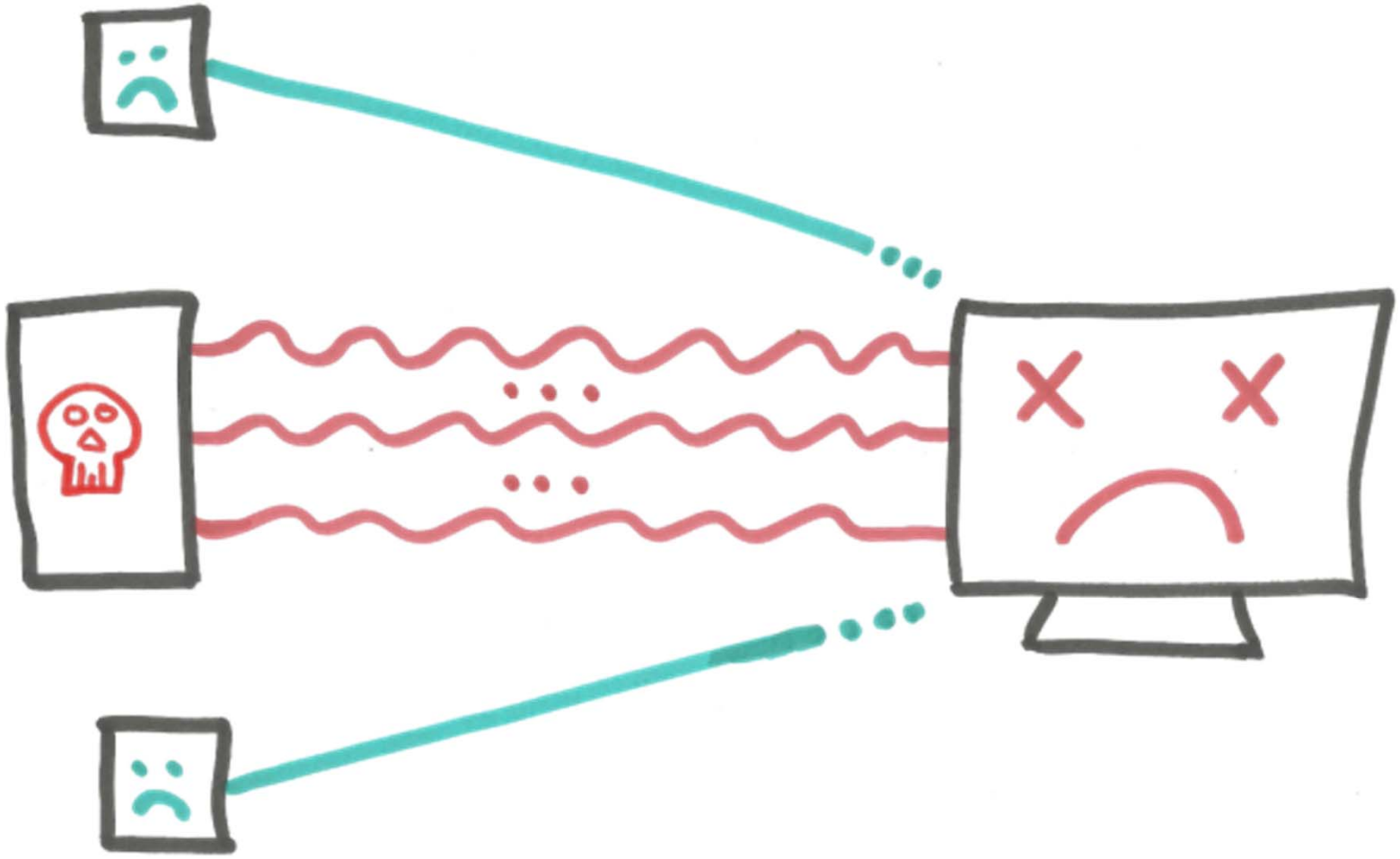
Flooding (TCP SYN)



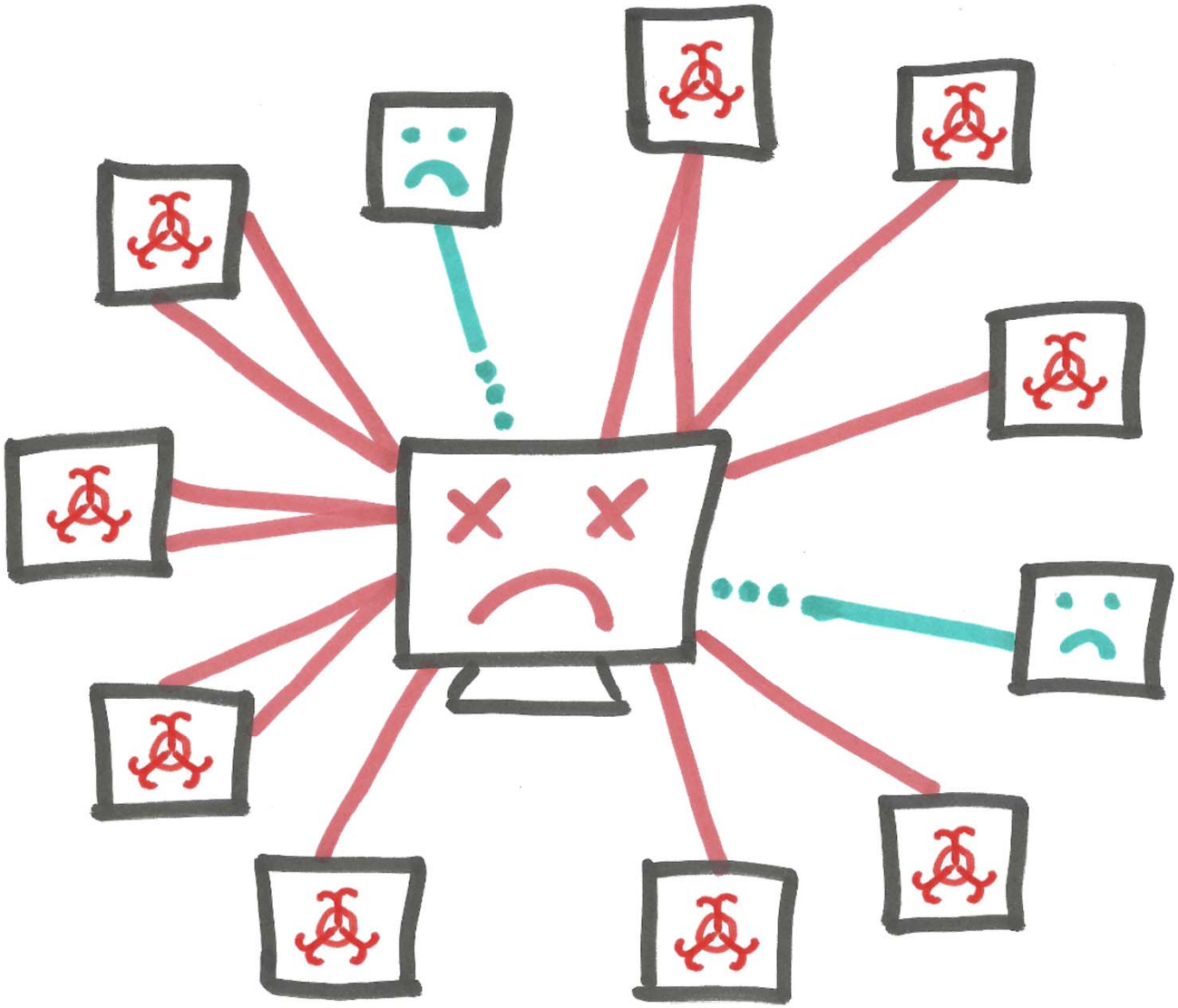
Amplification (UDP)



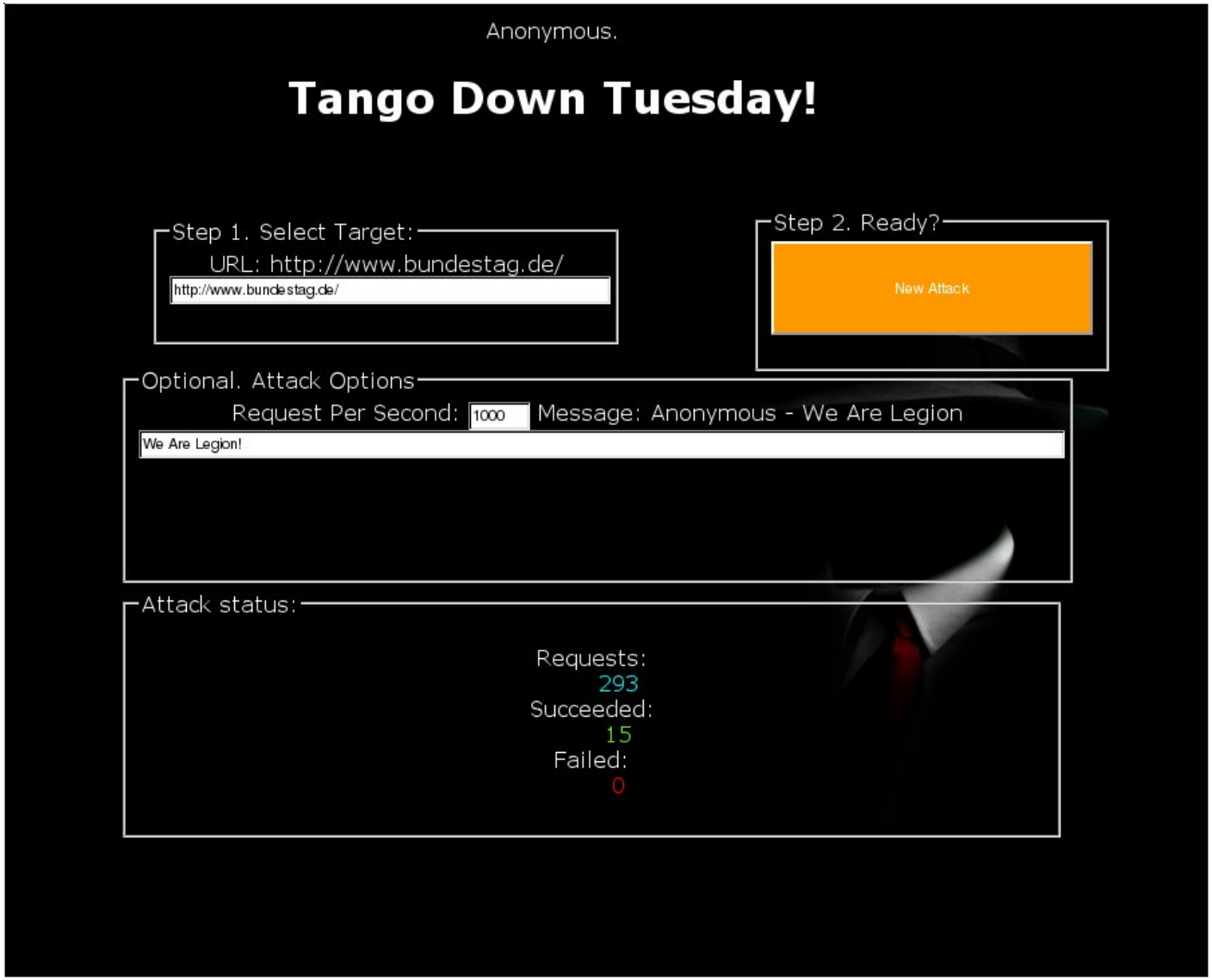
Low and Slow



Botnet / Web LOIC



Web LOIC


Anonymous.
Tango Down Tuesday!
Step 1. Select Target:
URL: http://www.bundestag.de/
http://www.bundestag.de/
Step 2. Ready?
New Attack
Optional. Attack Options
Request Per Second: 1000
Message: Anonymous - We Are Legion
We Are Legion!
Attack status:
Requests:
293
Succeeded:
15
Failed:
0

Web LOIC

```
GET /?id=1300380622178&msg=We%20Are%20Legion! HTTP/1.1
Host: www.bundestag.de
User-Agent: Mozilla/5.0 (X11; Linux x86_64) Firefox/8.0
Accept: image/png,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Connection: keep-alive
Referer: http://pastebin.com/RrsXbQ.html
```

Offline – und jetzt?

- Ruhe bewahren – es ist nur eine Webseite!
- Notfallplan vorhanden?
- Aufgaben verteilen; Teamwork
- Kommunikation: Kontakte informieren
- Dokumentation: Zeit, Status, Reaktion

Offline – und jetzt?

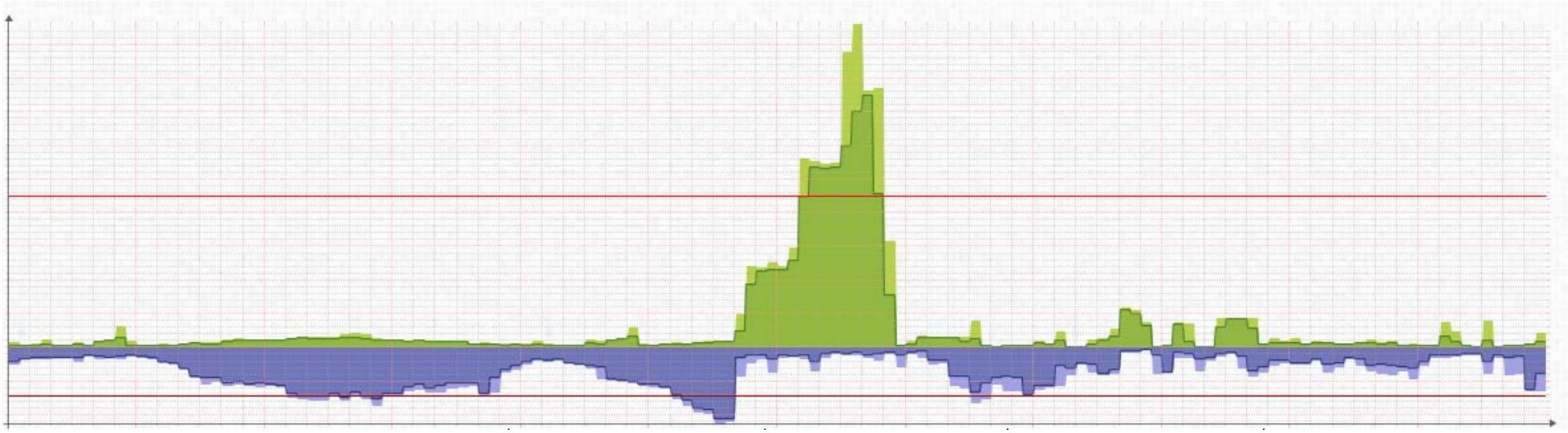
- Traffic Capture; Logfiles aufbewahren
- Muster erkennen (Layer, Requests)
- Gegenmaßnahmen einleiten
- Angriffe melden:
  - whois: ASN Kontakt
  - CERT: Meldestelle@bsi.bund.de
  - ISPs

Erkennung

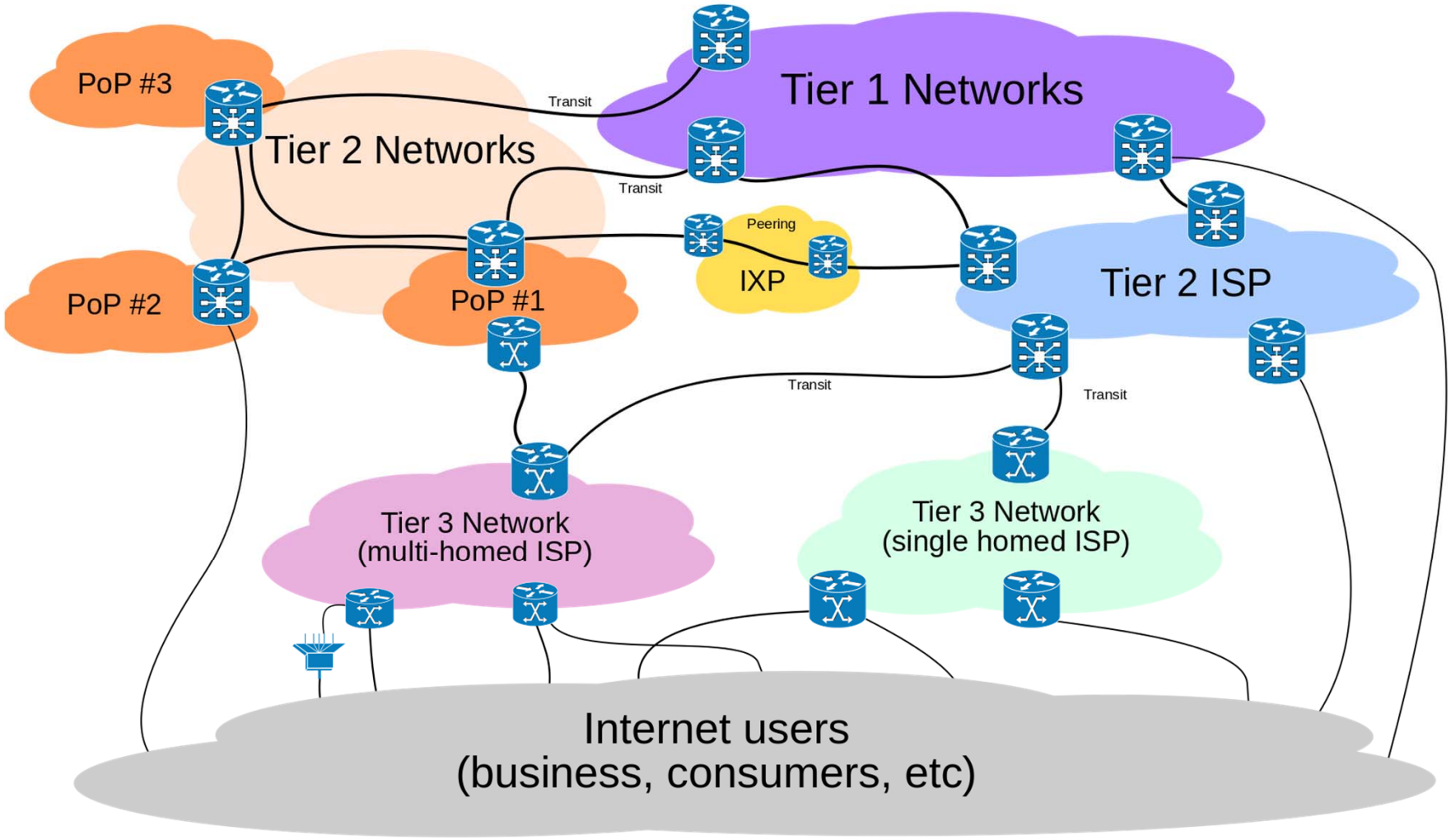
- **Detection**
  - Anomalien
  - Pakete pro Sekunde
  - Bandbreite
- **Tools**
  - Icinga
  - NetFlow, Sflow

Erkennung

- Monitoring & Bewertung



Reaktion: Wo ansetzen?



Gegenmaßnahmen - DO

- Personal schulen; Übungen
- Stateless Protokolle blocken (NTP, DNS)
- Protokoll/Port Whitelist (TCP/HTTP)
- Möglichst früh filtern!
- Mit Carrier arbeiten (Transit ACL)
- Appliances (Achtung: SPOF/Bottleneck)

Gegenmaßnahmen - DO

- Horizontal + vertikal skalieren
- Frontend: Mehr Connections
- Backend: Schnelle Auslieferung
- Caching: Backends schützen
- Anwendungen optimieren
- TLS mit ECC statt RSA (>10x schneller)

Gegenmaßnahmen - DO

- Limitierung Bandbreite / Requests je IP
- Services separieren (IPs)
- Mehr Bandbreite, VIEL MEHR!
- Gesamten Netzpfad beachten
- TCP Kernel Tuning (Reuse, Queue)
- Externe DDoS Mitigation Services

Gegenmaßnahmen - DO

- Whitelisting HTTP Methoden
- Pattern blocken: User-Agent, Referer
- Redirects; Cookies
- Javascript
- Captcha
- geoip

Gegenmaßnahmen - Maybe

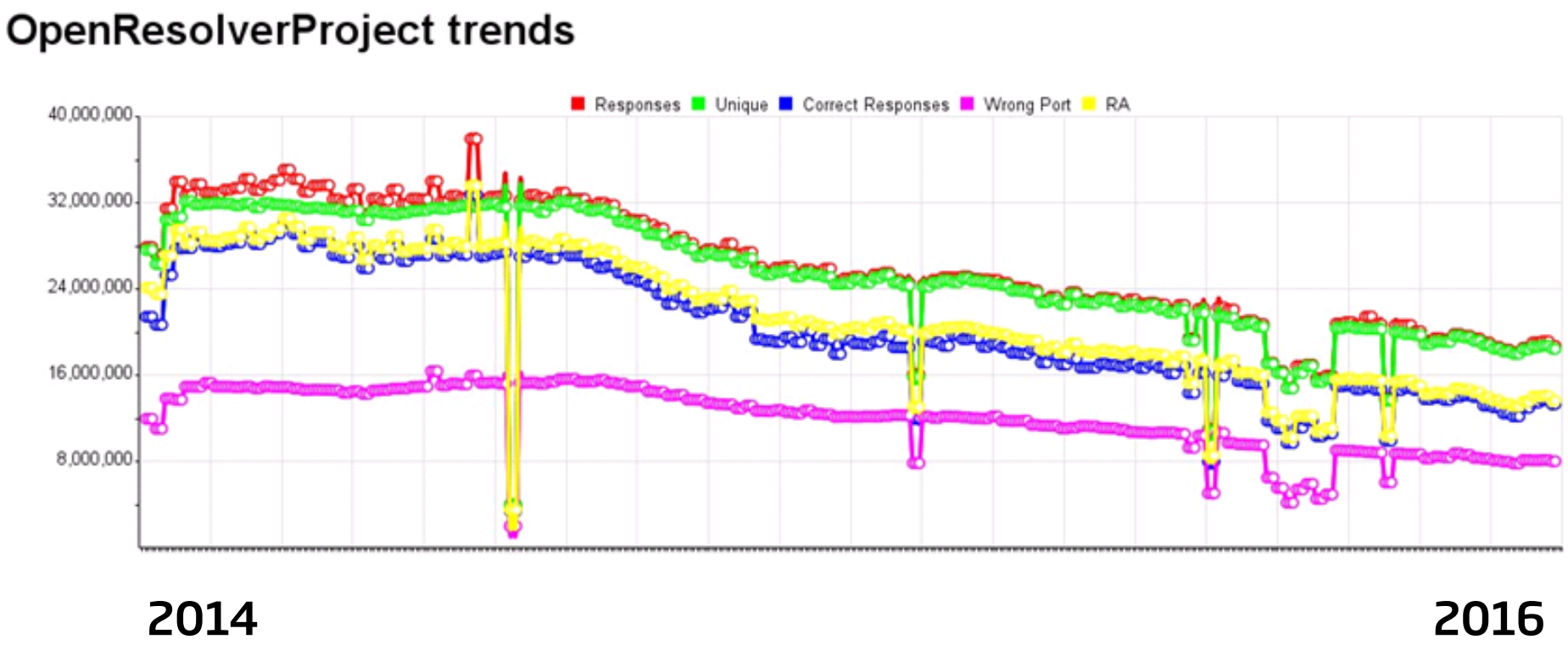
- Viele Endpunkte (DNS Fast Flux)
- CDN / Proxy Provider (Origin geheim halten)
- Blackholing (Null Routing)
- Anycast

Gegenmaßnahmen - DON'T

- Detaillierte Analyse zu Beginn
- Einzelne IPs bei SYN blocken
- Layer-Gegenmaßnahmen mischen
- Coding auf Backends

Weitere Gegenmaßnahmen

- Eigene Services richtig konfigurieren



Aussicht

- Bandbreite der Angriffe nimmt zu
- Mehr Angriffsquellen (Botnets, IoT)
- Gebuchte Attacken
- Layer 7 gefährlich
- Angriffe werden zur Regel

Vielen Dank für euer Interesse!

- https://talk.babiel.com/orr16/ddos (Folien)

Kollegen gesucht:

- https://babiel.com/jobs

kununu (IT-Branche)
Platz 11
Score 4,44

Verbunden bleiben:

- talk@babiel.com
- twitter.com/Babiel
- facebook.com/babiel.gmbh