Quo Vadis DDoS
TRENDS UND PERSPEKTIVE

QUELLENANGABEN

Allianz für Cybersicherheit - Arbor - BITKOM - Bundesministerium des Innern - Heise - Link11 - NSFOCUS - Prolexic

Schockzahlen DDoS-Angriffe

28
PRO STUNDE

10
PRO TAG

2200
PRO JAHR

400
GBPS

300+ %
NTP-AMPLIFICATION ATTACK

220+ %
BANDBREITE

Schockzahlen DDoS-Angriffe

LINK11

3/5
DER UNTERNEHMEN

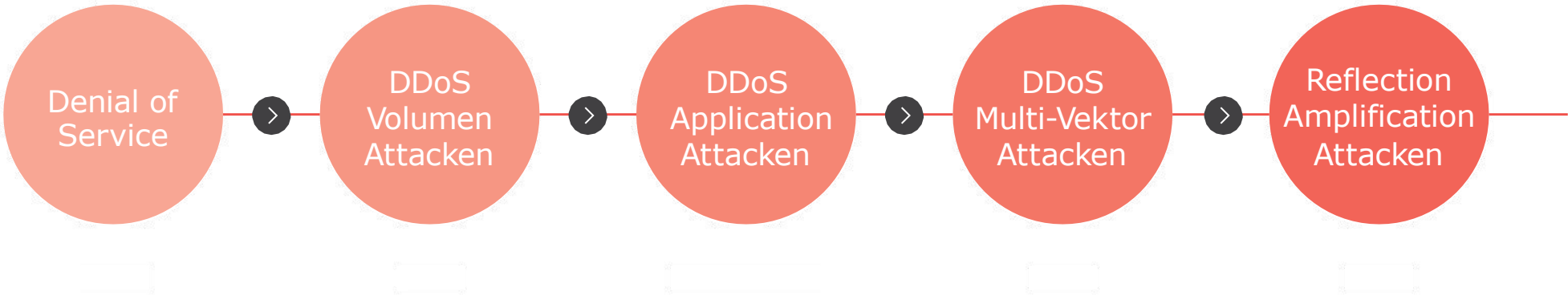
2/3
DER RECHENZENTREN

30
MINUTEN

1666
STUNDEN

319
EINZELANGRIFFE

Evolution von DDoS-Attacken



Evolution von DDoS-Attacken

WHAT IS NEXT ?

Vielfältige Volumen-Attacken

FLODDING ATTACKEN

Überlastung der Bandbreite und Netzwerkressourcen,
z.B. per TCP/UDP ICMP Floods

PROTOCOL EXPLOITATION ATTACKEN

Ressourcen-Zugriff über Features und Bugs,
z.B. per ACK, TCP

DISTRIBUTED REFLECTION DoS

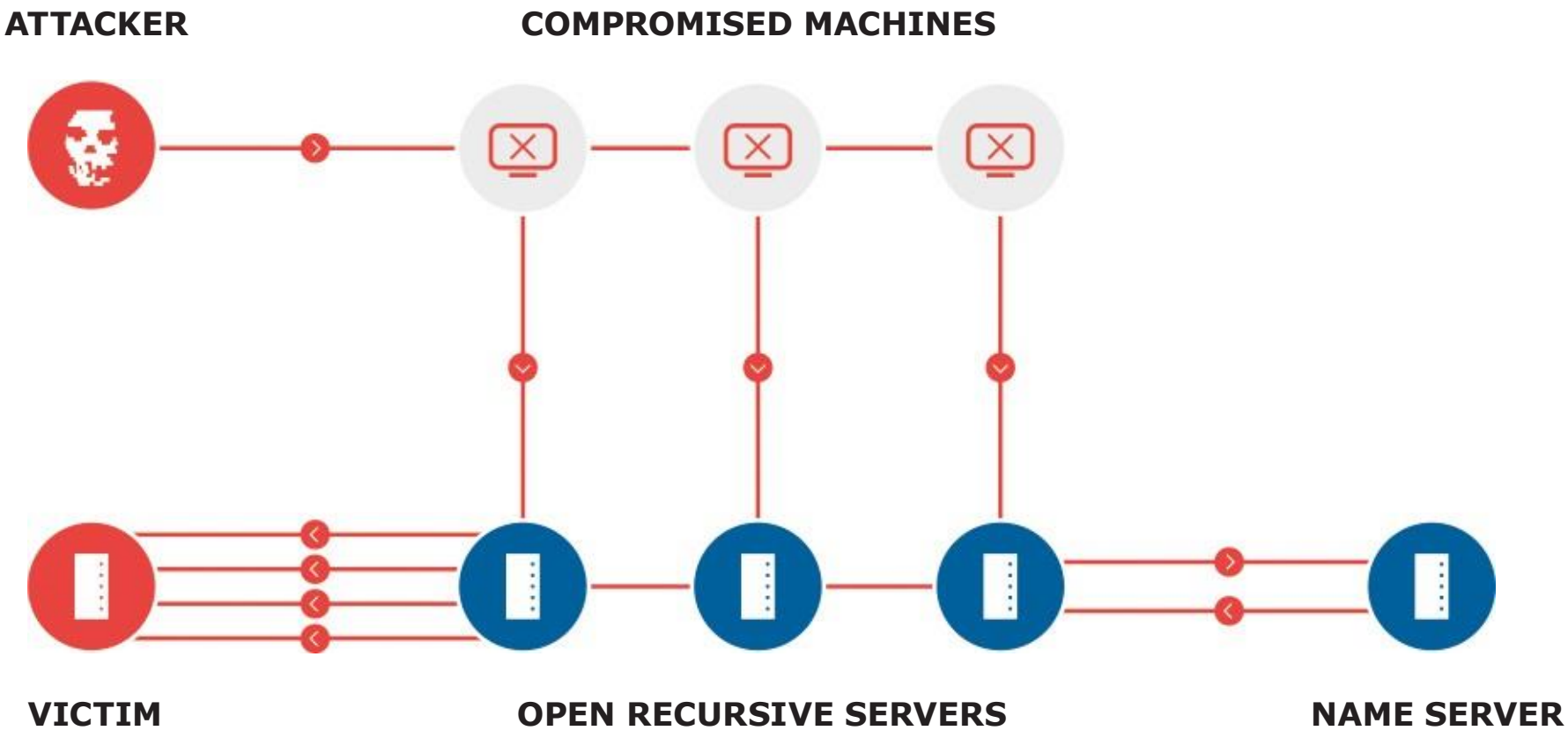
Distributed Reflection DoS

- Reflektoren als weiteres System zwischen Botnet und Ziel-Server **NEU**
- Die Botnet-Rechner schicken ihre gespooften Anfragen nicht direkt an Ziel-Server, sondern an regulär arbeitende Internetdienste
- Diese Reflektoren senden ihre Antworten an Opfer-Adresse
- Reflektoren führen „unbewusst" die eigentliche Attacke aus
- DRDoS ist effektiver als DDoS. Durch die Reflektoren ist
  DIE ANGRIFFSVERTEILUNG BESSER
  DIE VERKEHRSBELASTUNG HÖHER
  DAS ZIEL (ÜBERLAST) SCHNELLER ERREICHT
- Beispiele: NTP Reflection, DNS Reflection, CHARGEN

Volumen-Attacken per DNS Reflection

- Nutzen Sicherheitslücken in DNS-Servern aus
- Gespoofte Anfragen an Name Server über Protokol UDP
- keine Absender-Verifizierung
- Antworten gehen von Name Servern an die IP-Adresse des Opfers
- Vervielfältigung des DDoS-Traffics durch zusätzliche Netzwerkgeräte, häufig offene Resolver
- Antworten des DNS-Servers deutlich größer als die Anfrage
- Mit Einführung der Standard Domain Name Security Extensions (DNSSEC) stieg die Antwortgröße von 512 Bytes auf 4.000+ Bytes

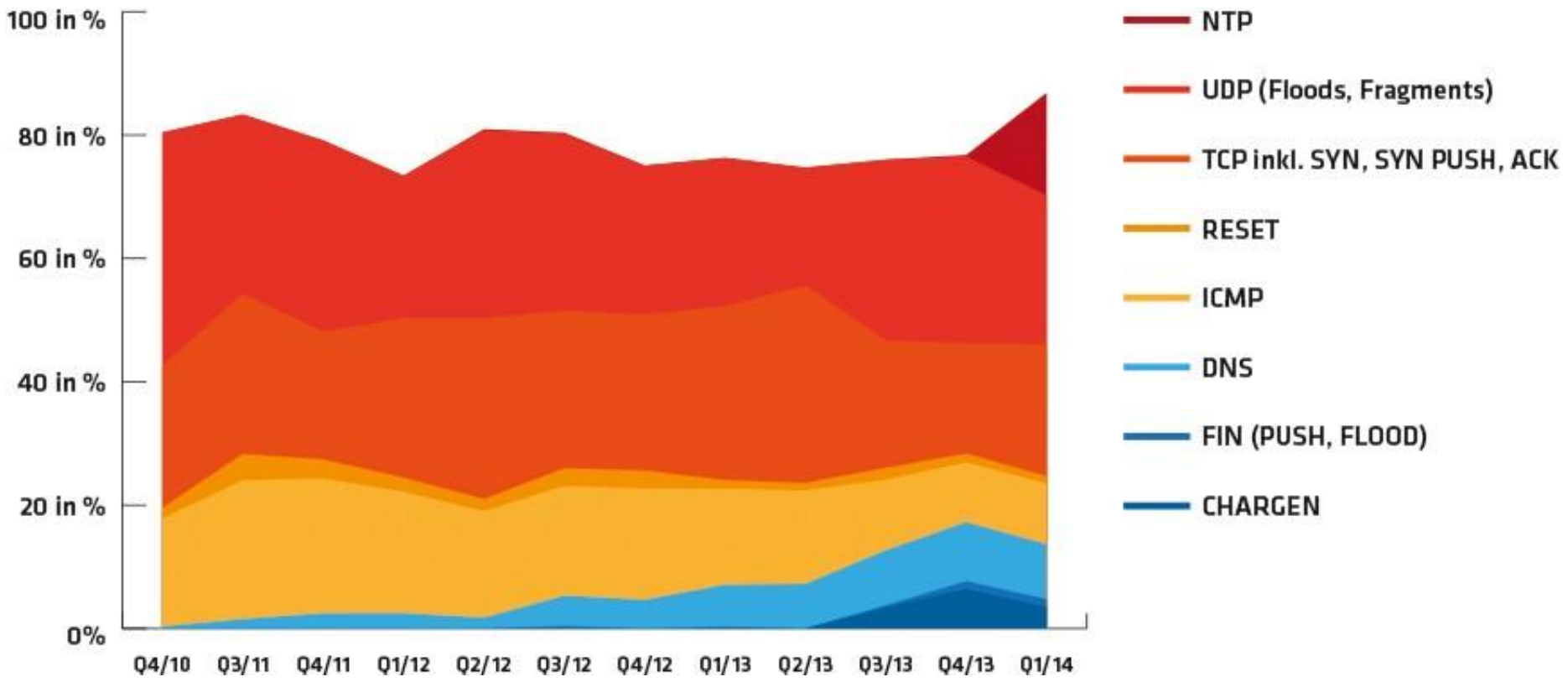
Volumen-Attacken per DNS Reflection



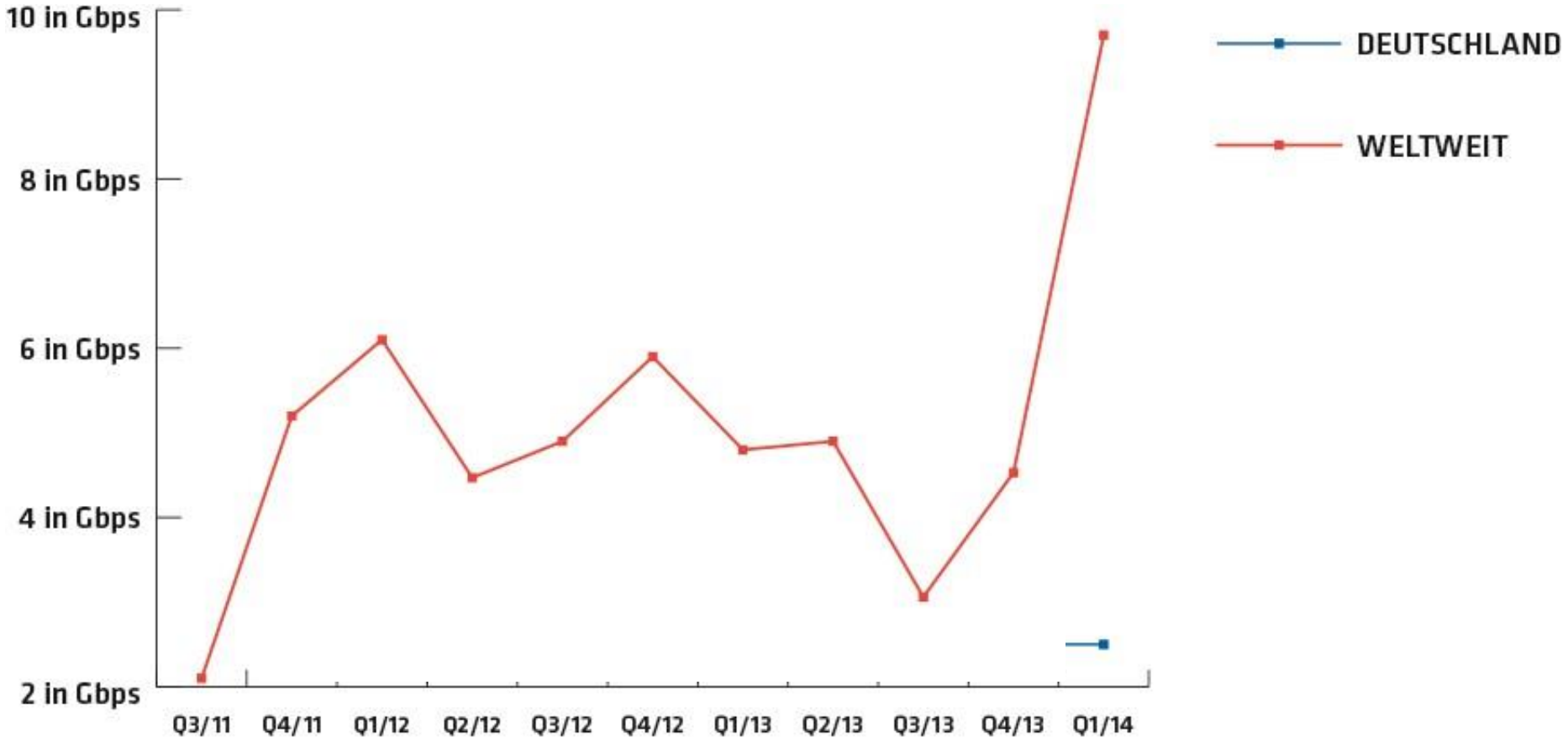
Volumen-Attacken per DNS Reflection

- Einbindung von Network Time Protocol (NTP) Servern, die Zeitangaben liefern
- Gefälschte Datenpakete fragen Zeit beim NTP-Server an
- Antworten des NTP-Servers an IP-Adresse des Opfers
- Antwort-Pakete größer als gefälschte Anfrage
- Reflection durch NTP-Server auf ganzer Welt
- 2.000+ aktive Zeit-Server weltweit

Vielfältige Volumen-Attacken



Durchschnittliche Angriffsbandbreite



Applikations-Attacken – gut getarnt

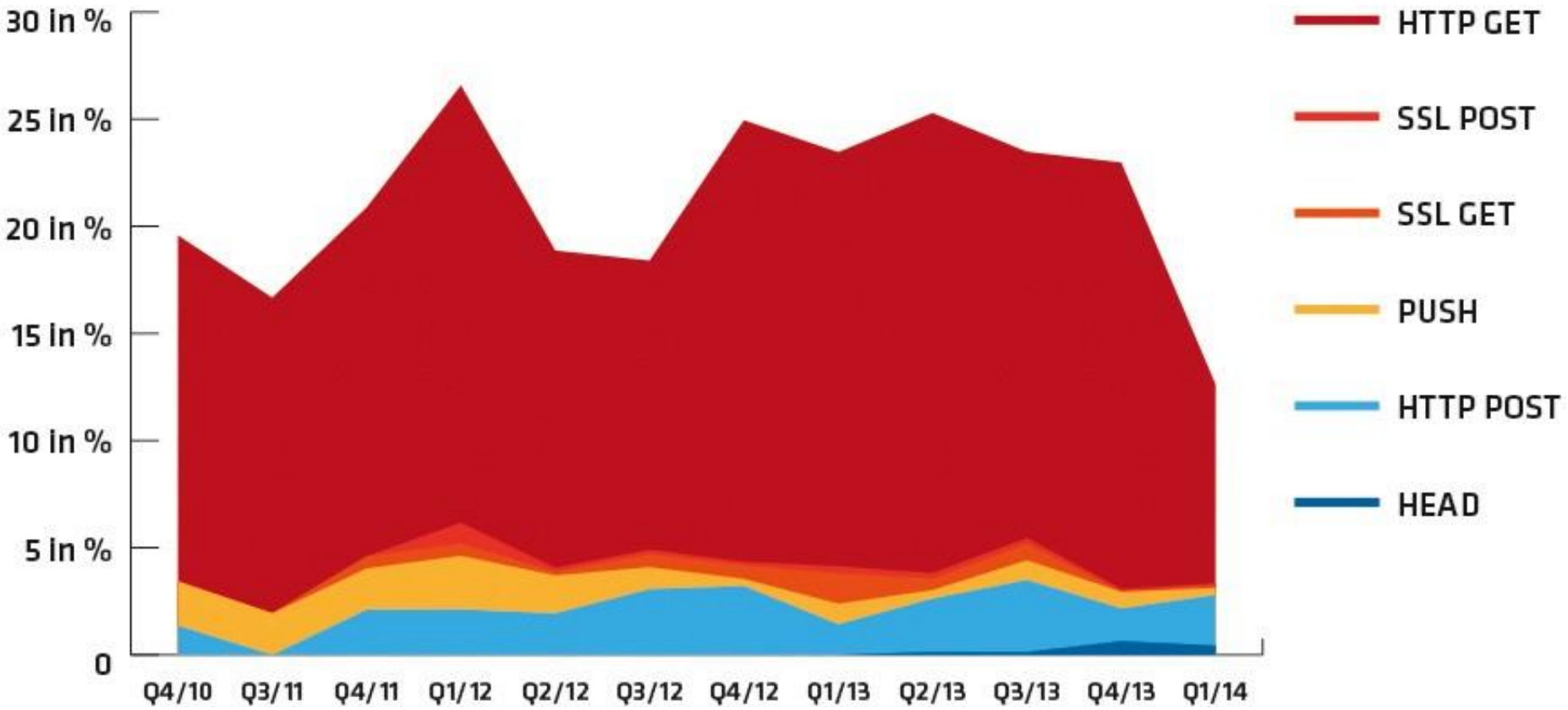
Applikations-Attacken – gut getarnt

- “appliactionflood“ und „low and slow“

- application flood
  ÜBERFLUTUNG DES WEBSERVERS MIT GROßVOLUMIGEN HTTP-ANFRAGEN WIE SUCH-ABFRAGEN, HTTP-ANFRAGEN PASSIEREN FIREWALLS, IPS UND APPLICATION CONTROL WIE LEGITIME ANFRAGEN

- low and slow
  NUTZEN SCHWACHSTELLEN IN LAYER 7 AUS, ANFRAGEN SELBST SIND KLEIN, VERBINDUNGEN WERDEN DAFÜR ABER LANGE OFFEN GEHALTEN, z.B. PER HTTP GET

Vielfältige Applikations-Attacken



Multi-Vektor-Attacken

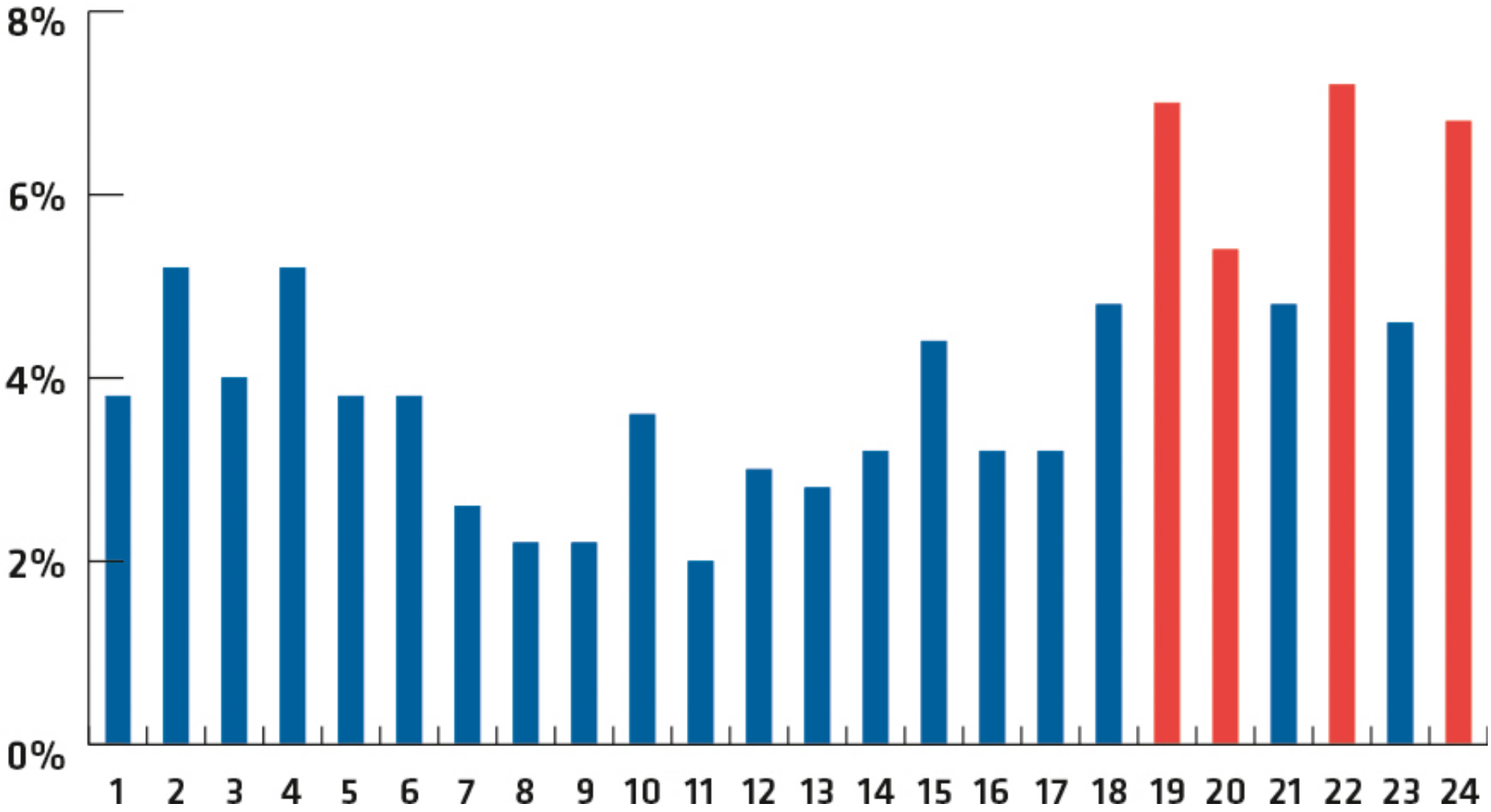
- Kombination von Volumen- und Applikations-Attacken
  ICMP+TCP+UDP+DNS
  ICMP+TCP
  TCP HYBRID
  ICMP+TCP+UDP

- Anteil bereits bei 4,5 Prozent aller DDoS-Angriffe

- Tendenz steigend

Startzeit von DDoS-Attacken – weltweit

Perfekter Zeitpunkt, wenn Geschäftszeiten sowohl in Europa als auch in USA sind



Quellen des DDoS-Traffics nach Ländern

USA

FIRST

China

SECOND

Thailand

THIRD

Türkei

Deutschland

Brasilien

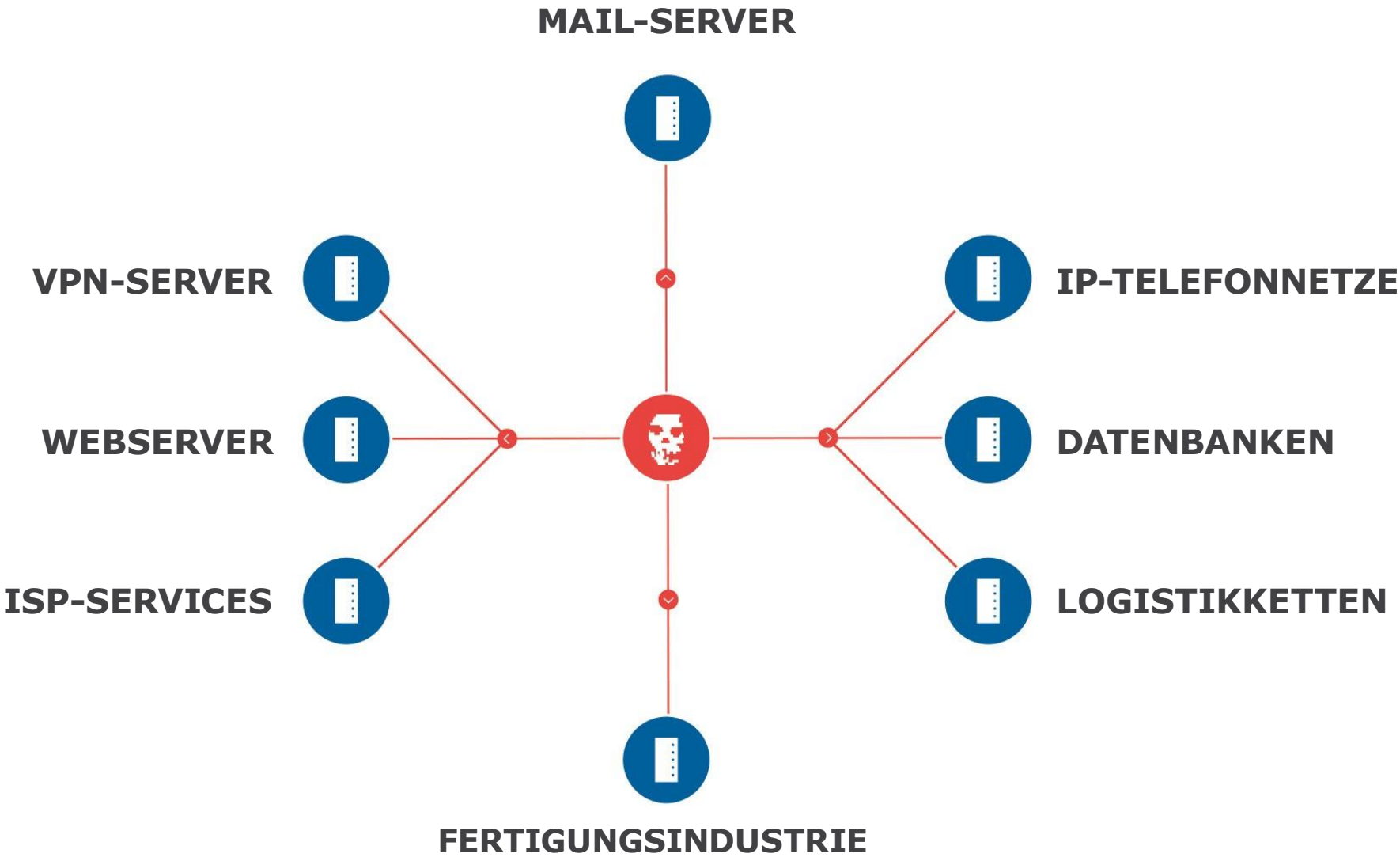
Italien

Indonesien

Südkorea

Saudi-Arabien

Im Visier


MAIL-SERVER
VPN-SERVER
WEBSERVER
ISP-SERVICES
IP-TELEFONNETZE
DATENBANKEN
LOGISTIKKETTEN
FERTIGUNGSINDUSTRIE

Trends

- Volumen-Attacken nehmen mit steigender Anbindung der Rechner zu
- Angriffe auf Applikations-Ebene tarnen sich immer besser wie normale User und Browser
- Neue DDoS-Vektoren wie DRDoS breiten sich aus