DNS Sicherheit

TechTalk Reihe

bwInfoSec - Stefan Machmeier - 11.12.24

TechTalks

Ablauf

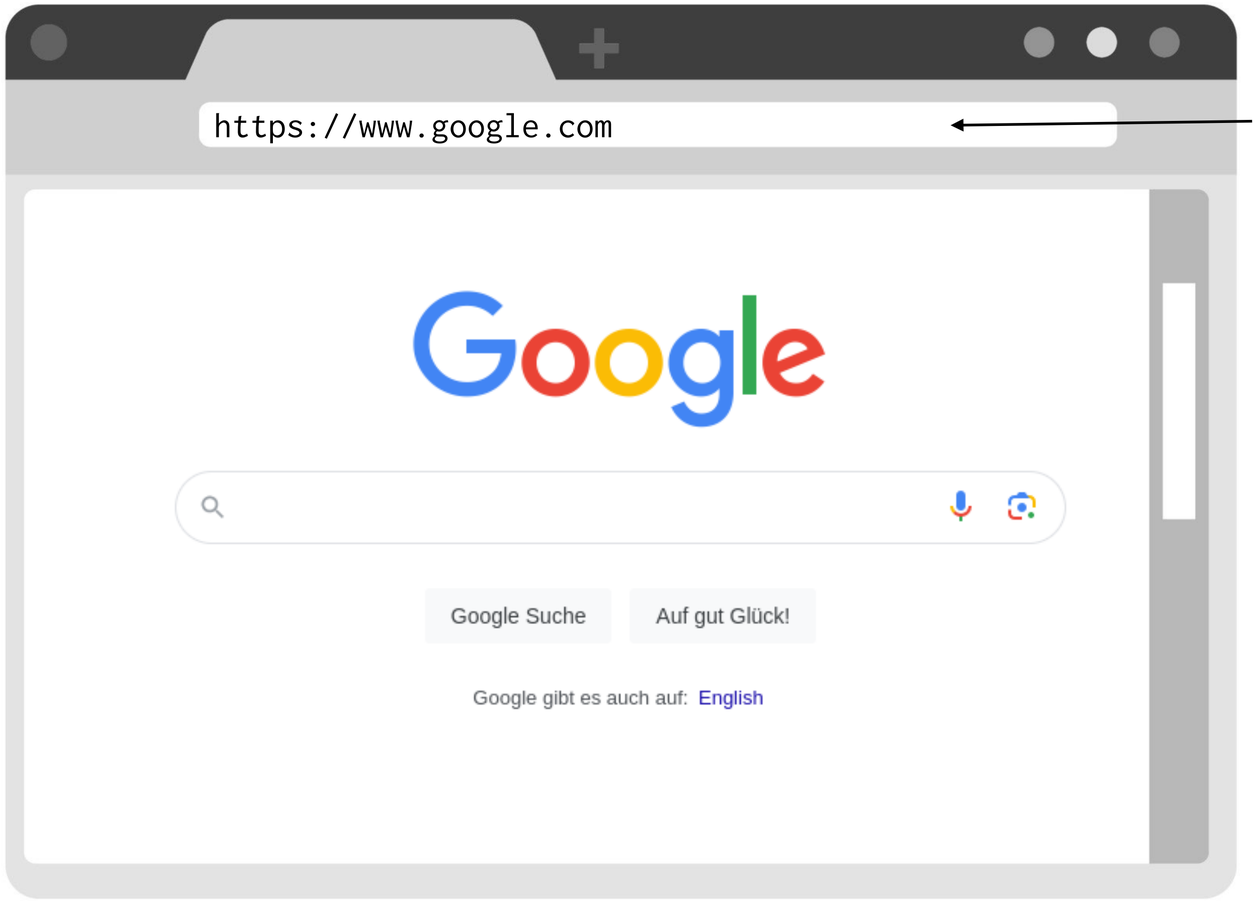
- 5 Min. - Domain Name System Protokoll
- 20 Min. - DNS Angriffe
- Fragerunde

Agenda
TechTalk

- Einführung DNS
- Vorstellung DNS Angriffe
  - DNS Tunnelling
  - DGAs
  - DNS Amplification Attack
- Zusammenfassung

DNS

Die Magie im Hintergrund …



Was passiert im Hintergrund?

- **Domain Name System**
  Resolution ist die Antwort!

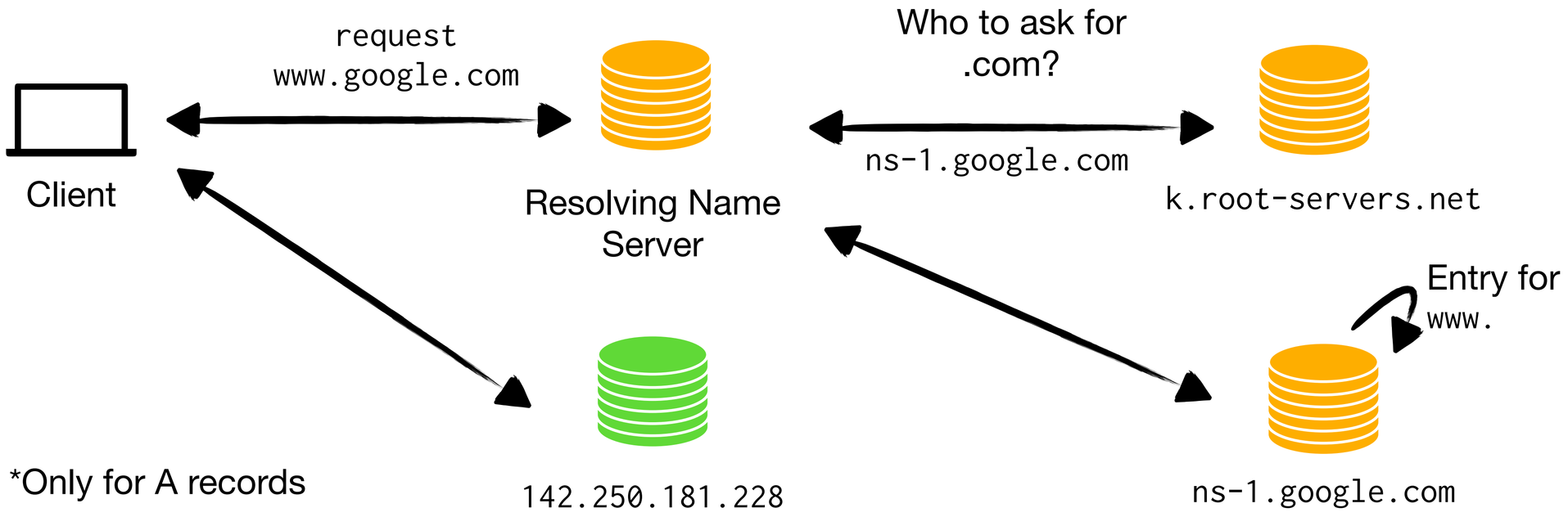
Domain Name System Protokoll

In a nutshell

- Spezifiziert durch RFC **1034** and **1035.**
- Hierarchisches verteiltes Datenbanksystem, das für die **Auflösung von Domänennamen in IP-Adressen** zuständig ist.

Domain Name System Protokoll

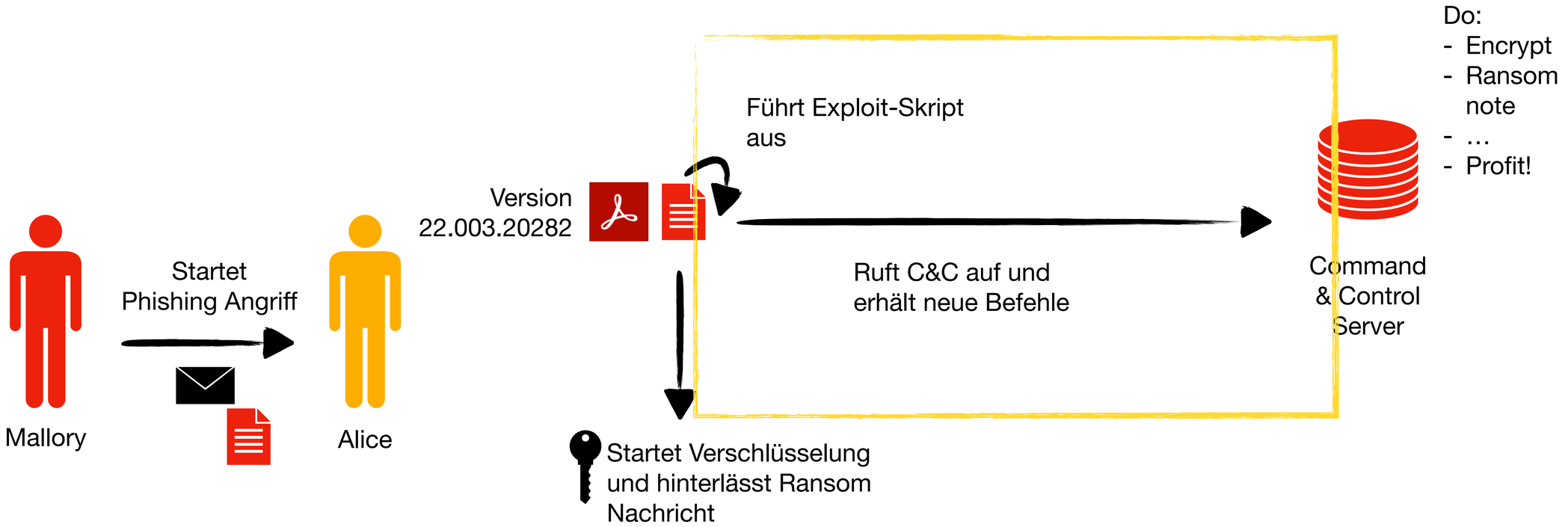
In a nutshell



DNS Tunnelling Angriffe

Warum ist das wichtig?

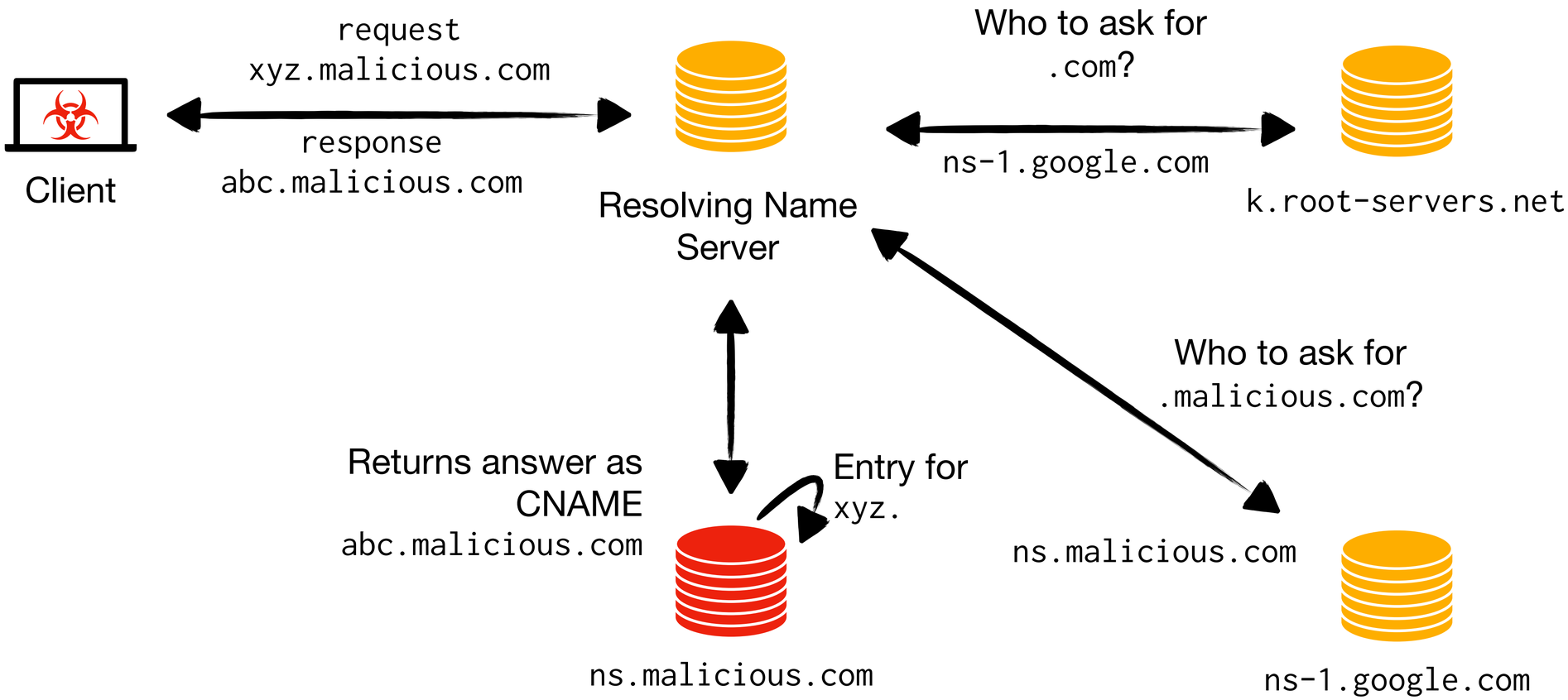
Kurze Übersicht zu Ransomware Angriffe



See: CVE-2023-21608

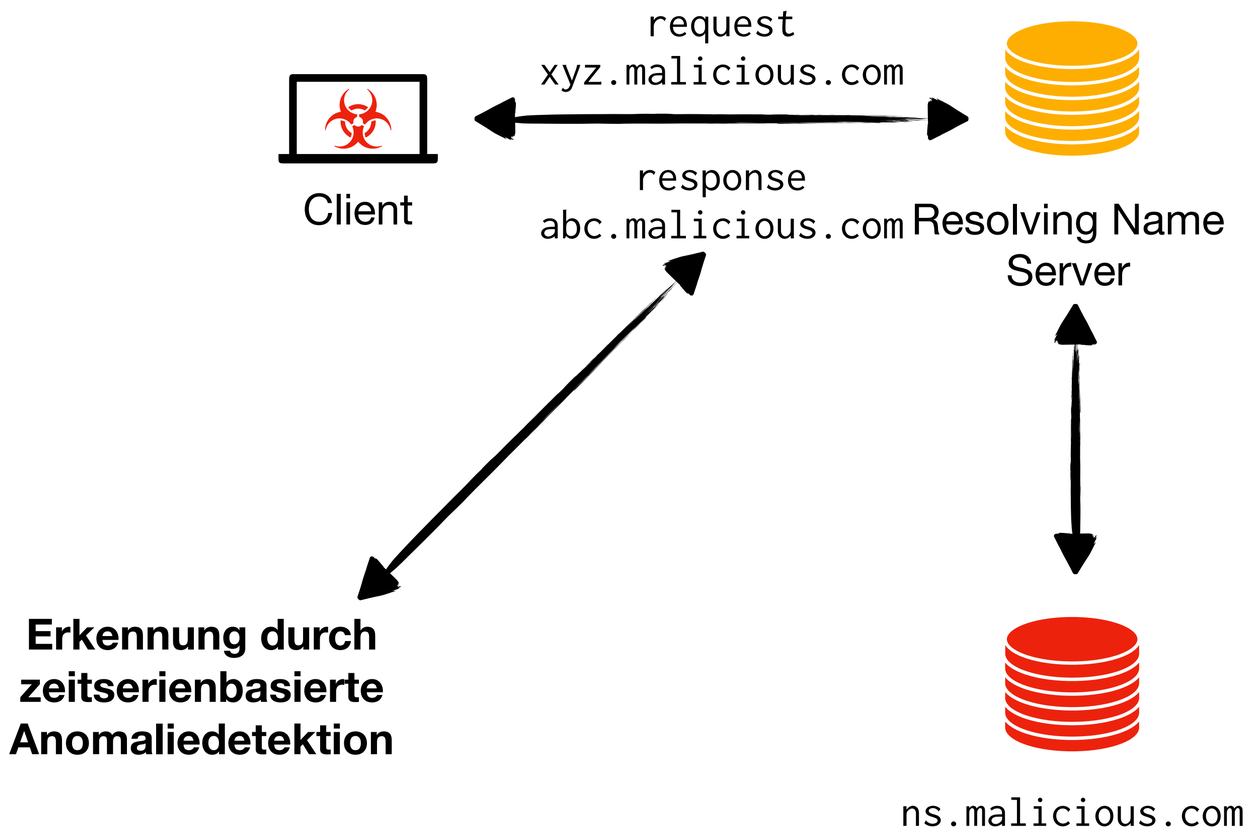
DNS Tunnelling

Angriff



Daten-Exfiltration

- Bestehende Verbindungen ermöglichen Angreifern die Exfiltration von Daten.
- **Sehr selten**, aber relevant für neue Exfiltrationstechniken.



Verfügbare Tools

- Große Auswahl an Werkzeugen verfügbar.
- Wir untersuchen hier:
  - `iodine`
  - `dnspot`
  - `dnscat2`
  - `dns2tcp`

Verfügbare Tools

- Unterstützt verschiedene **Encodings**, **Resource Records** (RR), und **Extensions**.

Method	Name	Encoding	RR	Extension
IP over DNS	`dnscat2` `iodine`	Hexadecimal Base32, Base64, Base128	A, AAAA, CNAME, TXT, MX A, CNAME, NULL, SRV, TXT, MX	✗ DNS (EDNS(0))
TCP over DNS	`dns2tcp`	Base64	TXT, KEY	✗
Custom over DNS	`dnspot`	Base32	CNAME	✗

Live Demo

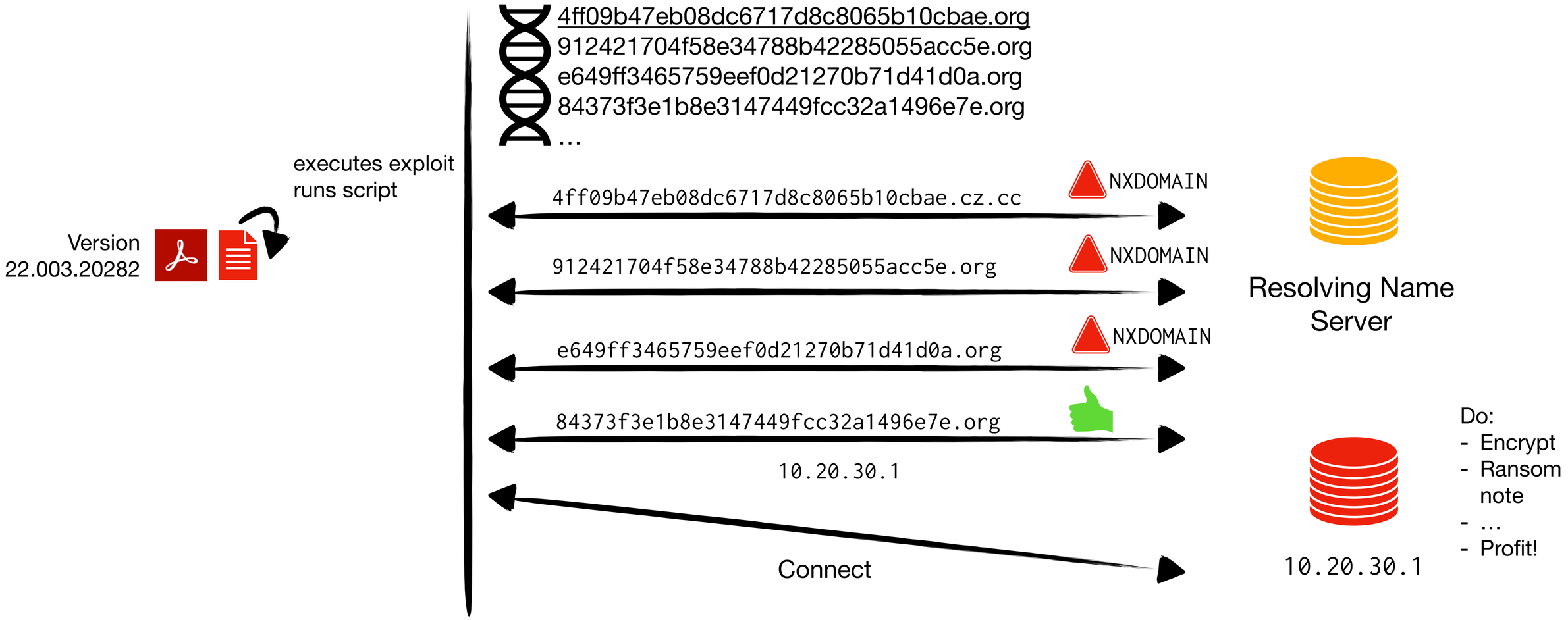
Detektion

- Relative einfach aufgrund der hohen DNS Anfragen (volumenbasiert).
- Als Beispiel:
  - k-Nearest-Neighbor (kNN) Klassifikation liefert bereits gute Ergebnisse.

Domain Generation Algorithmen

Domain Generation Algorithmen

Kurze Einführung



DGA?

Welche Domain stammt von einem DGA

qaskebf.com

oder

arnavutkoyemlakdanismanligi.com

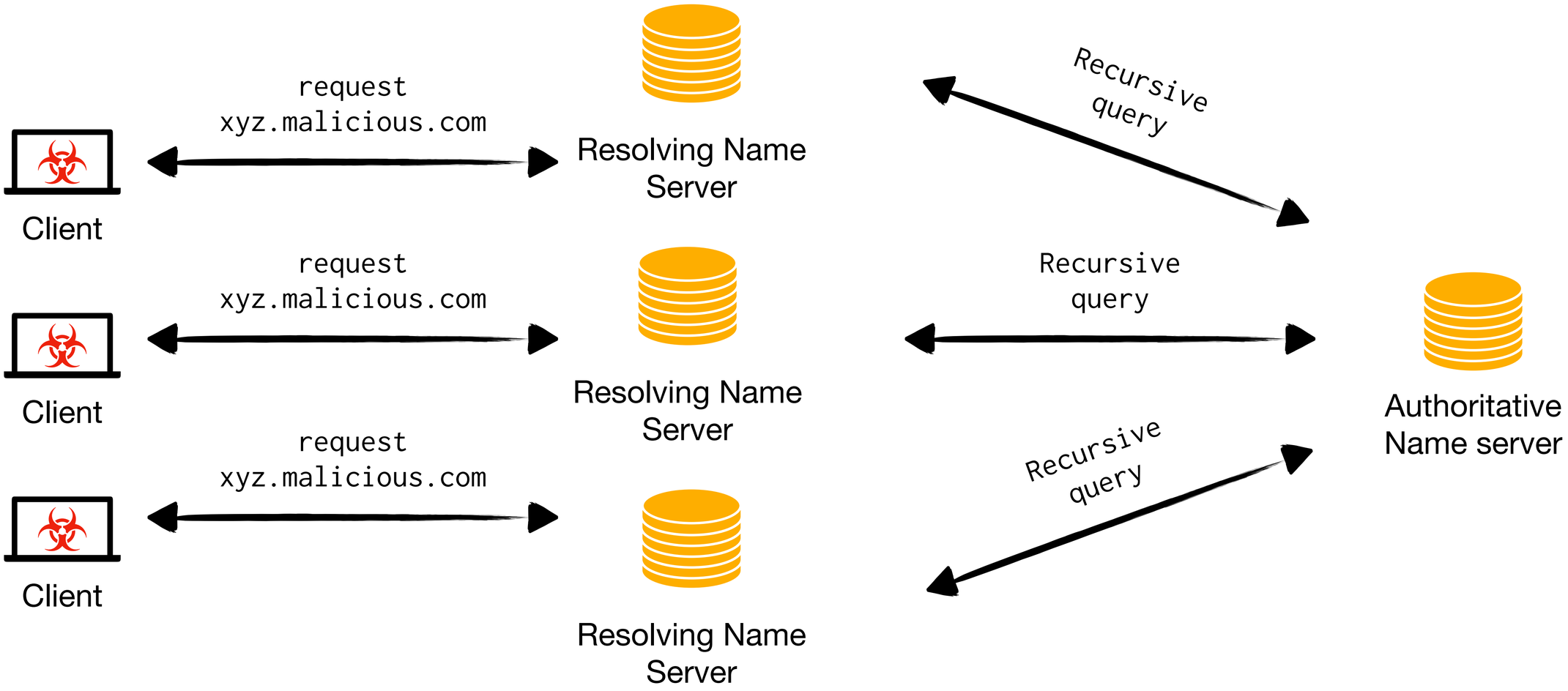
DGA für DDoS Angriffe

Water Torture Attack

- Abfragen können sich **wiederholen**, **kontinuierlich** erfolgen und **langsam** an **Intensität** zunehmen.
- **Ziel**: Ressourcen des DNS-Servers **zu überlasten** und seine Funktionsfähigkeit **zu stören**.
- Meist verbreitete DNS Water Torture DDoS Angriffe:
  - Pseudorandom Subdomain (**PRSD**) Angriff
  - NXDOMAIN (**NX**) Angriff
  - Pointer (**PTR**) Angriff

DGA für DDoS Angriffe

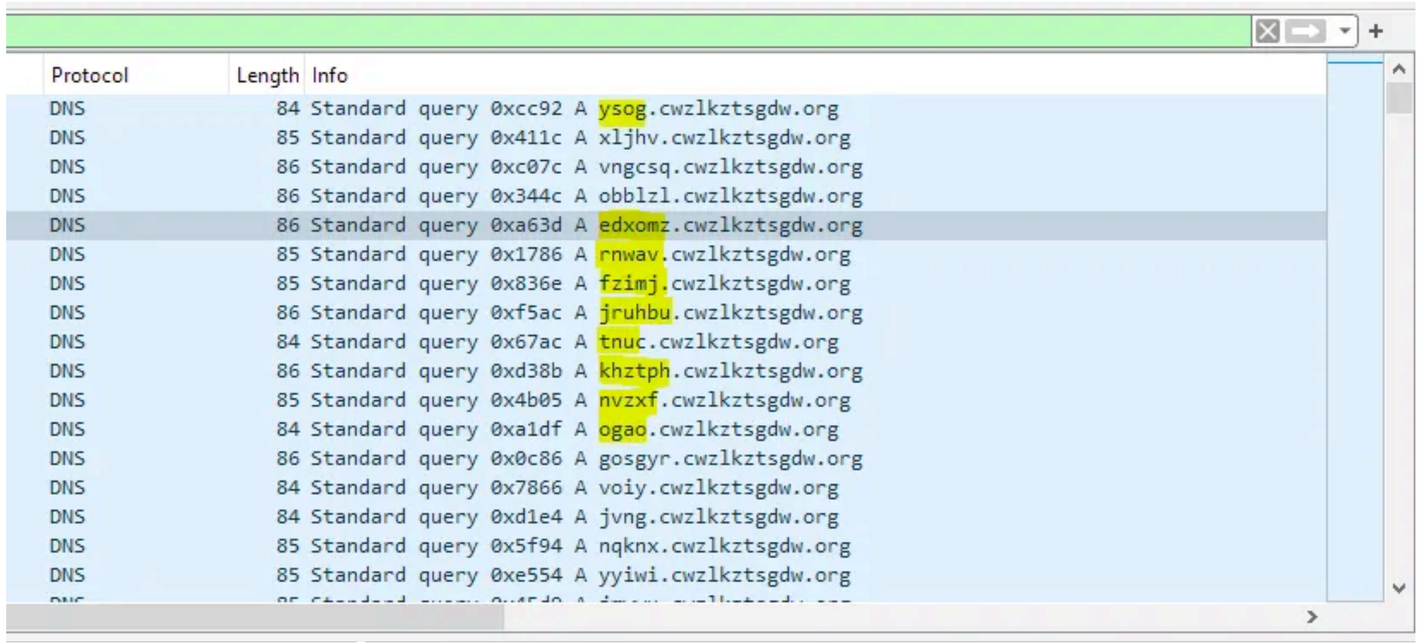
PRSD and NX DDoS Angriff



DGA für DDoS Angriffe

PRSD Angriff

- Angriff mit DGA generierten Domains.

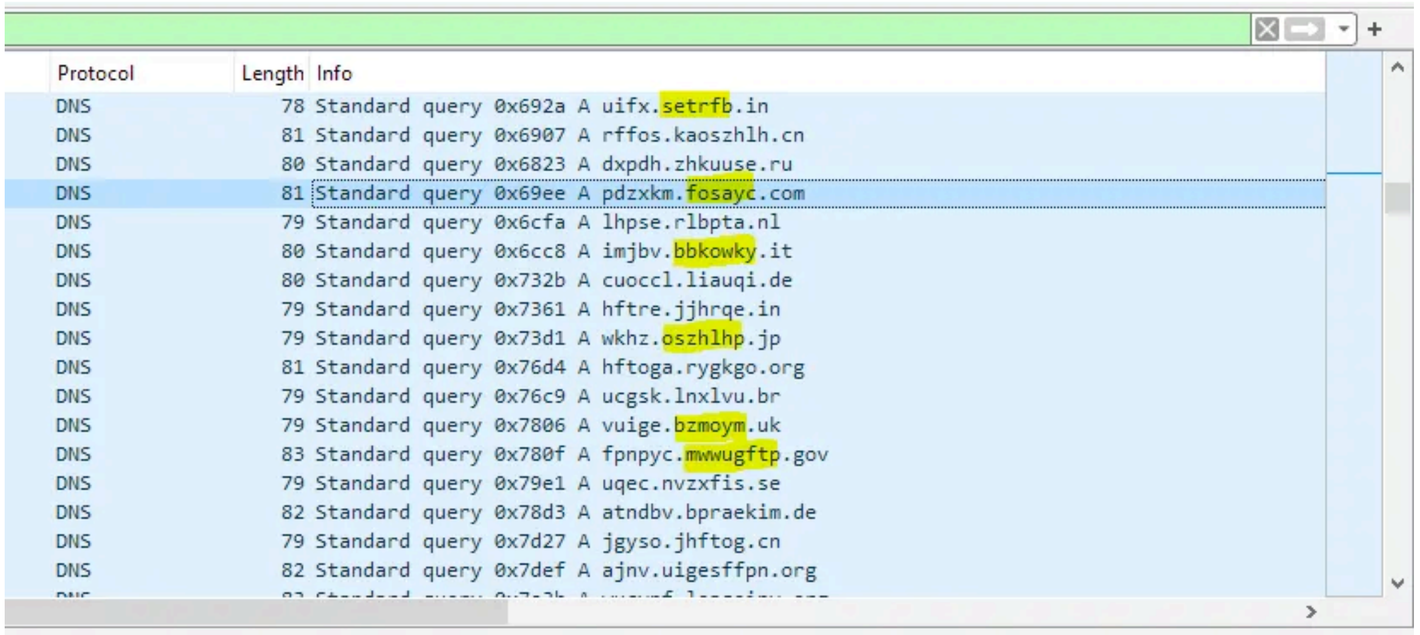


Protocol	Length	Info
DNS	84	Standard query 0xcc92 A ysog.cwzlkztsgdw.org
DNS	85	Standard query 0x411c A xljhv.cwzlkztsgdw.org
DNS	86	Standard query 0xc07c A vngcsq.cwzlkztsgdw.org
DNS	86	Standard query 0x344c A obblzl.cwzlkztsgdw.org
DNS	86	Standard query 0xa63d A edxomz.cwzlkztsgdw.org
DNS	85	Standard query 0x1786 A rnwav.cwzlkztsgdw.org
DNS	85	Standard query 0x836e A fzimj.cwzlkztsgdw.org
DNS	86	Standard query 0xf5ac A jruhbu.cwzlkztsgdw.org
DNS	84	Standard query 0x67ac A tnuc.cwzlkztsgdw.org
DNS	86	Standard query 0xd38b A khztph.cwzlkztsgdw.org
DNS	85	Standard query 0x4b05 A nvzxf.cwzlkztsgdw.org
DNS	84	Standard query 0xa1df A ogao.cwzlkztsgdw.org
DNS	86	Standard query 0x0c86 A gosgyr.cwzlkztsgdw.org
DNS	84	Standard query 0x7866 A voiy.cwzlkztsgdw.org
DNS	84	Standard query 0xd1e4 A jvng.cwzlkztsgdw.org
DNS	85	Standard query 0x5f94 A nqknx.cwzlkztsgdw.org
DNS	85	Standard query 0xe554 A yyiwi.cwzlkztsgdw.org

DGA für DDoS Angriffe

NX Angriff

- Anfragen von nicht-existenten Domains.

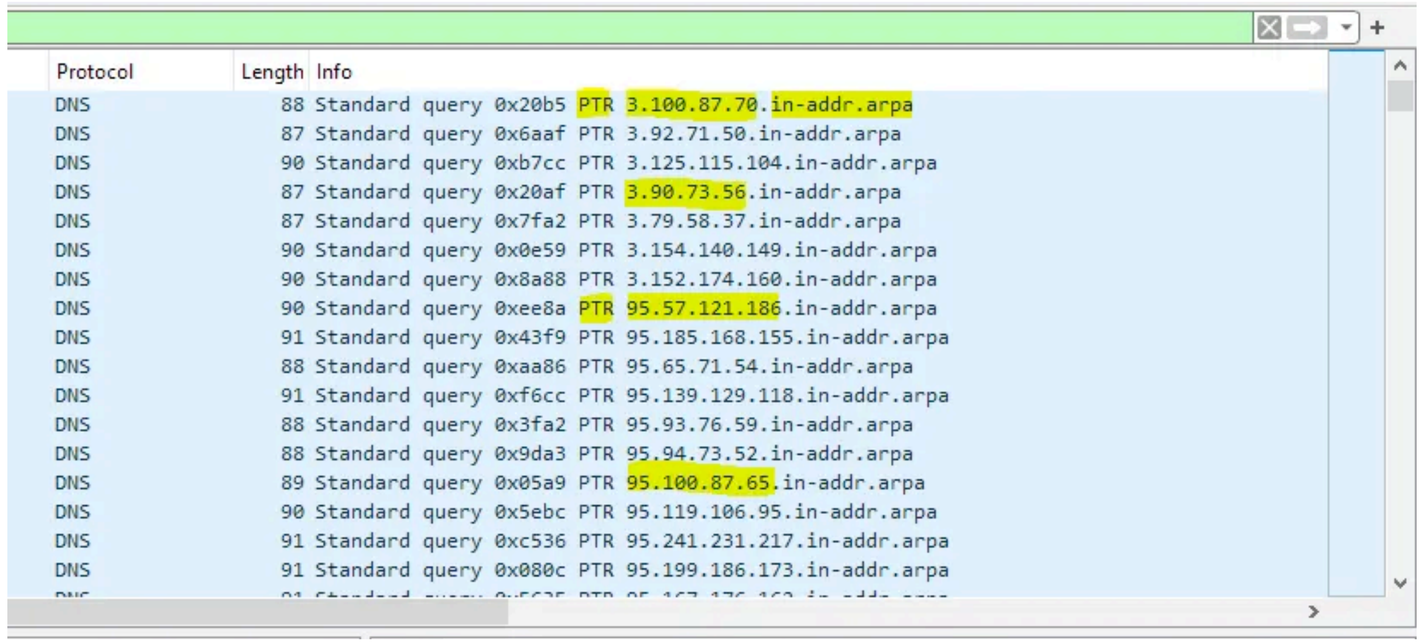


Protocol	Length	Info
DNS	78	Standard query 0x692a A uifx.setrfb.in
DNS	81	Standard query 0x6907 A rffos.kaoszhlh.cn
DNS	80	Standard query 0x6823 A dxpdh.zhkuuse.ru
DNS	81	Standard query 0x69ee A pdzxkm.fosayc.com
DNS	79	Standard query 0x6cfa A lhpse.rlbpta.nl
DNS	80	Standard query 0x6cc8 A imjbv.bbkowky.it
DNS	80	Standard query 0x732b A cuoccl.liauqi.de
DNS	79	Standard query 0x7361 A hftre.jjhrqe.in
DNS	79	Standard query 0x73d1 A wkhz.oszhlhp.jp
DNS	81	Standard query 0x76d4 A hftoga.rygkgo.org
DNS	79	Standard query 0x76c9 A ucgsk.lnxlvu.br
DNS	79	Standard query 0x7806 A vuige.bzmoym.uk
DNS	83	Standard query 0x780f A fpnpyc.mwwugftp.gov
DNS	79	Standard query 0x79e1 A uqec.nvzxfis.se
DNS	82	Standard query 0x78d3 A atndbv.bpraekim.de
DNS	79	Standard query 0x7d27 A jgyso.jhftog.cn
DNS	82	Standard query 0x7def A ajnv.uigesffpn.org

DGA für DDoS Angriffe

PTR Angriff

- **Ziel**: Überlastung durch gezielte reverse DNS lookups.



Protocol	Length	Info
DNS	88	Standard query 0x20b5 PTR 3.100.87.70.in-addr.arpa
DNS	87	Standard query 0x6aaf PTR 3.92.71.50.in-addr.arpa
DNS	90	Standard query 0xb7cc PTR 3.125.115.104.in-addr.arpa
DNS	87	Standard query 0x20af PTR 3.90.73.56.in-addr.arpa
DNS	87	Standard query 0x7fa2 PTR 3.79.58.37.in-addr.arpa
DNS	90	Standard query 0x0e59 PTR 3.154.140.149.in-addr.arpa
DNS	90	Standard query 0x8a88 PTR 3.152.174.160.in-addr.arpa
DNS	90	Standard query 0xee8a PTR 95.57.121.186.in-addr.arpa
DNS	91	Standard query 0x43f9 PTR 95.185.168.155.in-addr.arpa
DNS	88	Standard query 0xaa86 PTR 95.65.71.54.in-addr.arpa
DNS	91	Standard query 0xf6cc PTR 95.139.129.118.in-addr.arpa
DNS	88	Standard query 0x3fa2 PTR 95.93.76.59.in-addr.arpa
DNS	88	Standard query 0x9da3 PTR 95.94.73.52.in-addr.arpa
DNS	89	Standard query 0x05a9 PTR 95.100.87.65.in-addr.arpa
DNS	90	Standard query 0x5ebc PTR 95.119.106.95.in-addr.arpa
DNS	91	Standard query 0xc536 PTR 95.241.231.217.in-addr.arpa
DNS	91	Standard query 0x080c PTR 95.199.186.173.in-addr.arpa

Live Demo

Detektion von DGAs

- Mittels Entropie Werten der Domain-Anfragen feststellbar.
- **Allerdings**: DGAs sind nicht nur bösartig.
- **DGArchive**: Öffentliche Datenbank für bekannte DGAs.

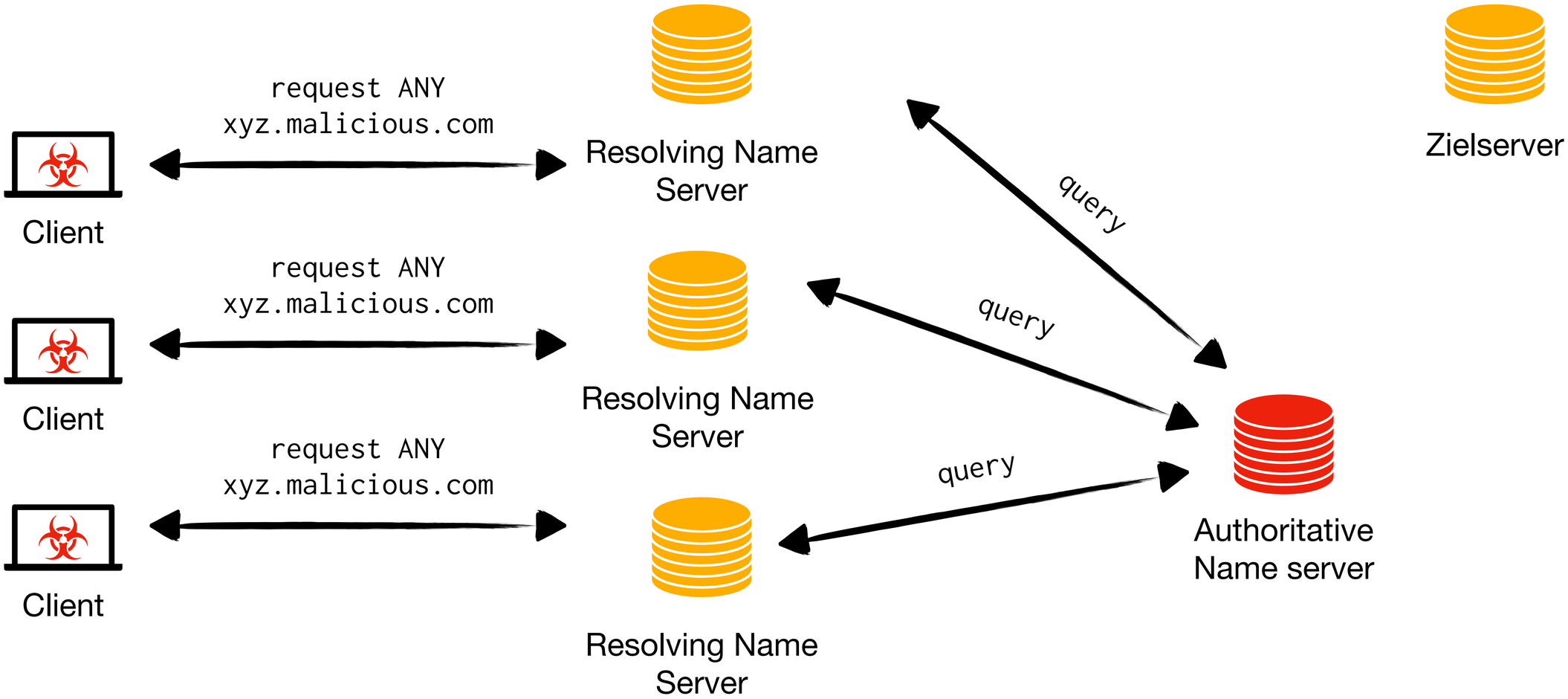
DNS Amplification Angriff

DNS Amplification Angriff

- Kleine Anfragen (ungefähr 60 Bytes) können eine mehr als **4000 Byte Antwort** provozieren.
- **IP-Spoofing** erforderlich.
- Durch Extended DNS wesentlich effektiver.
- **Ziel**: Überlastung des Zielservers durch große Antwortpakete.

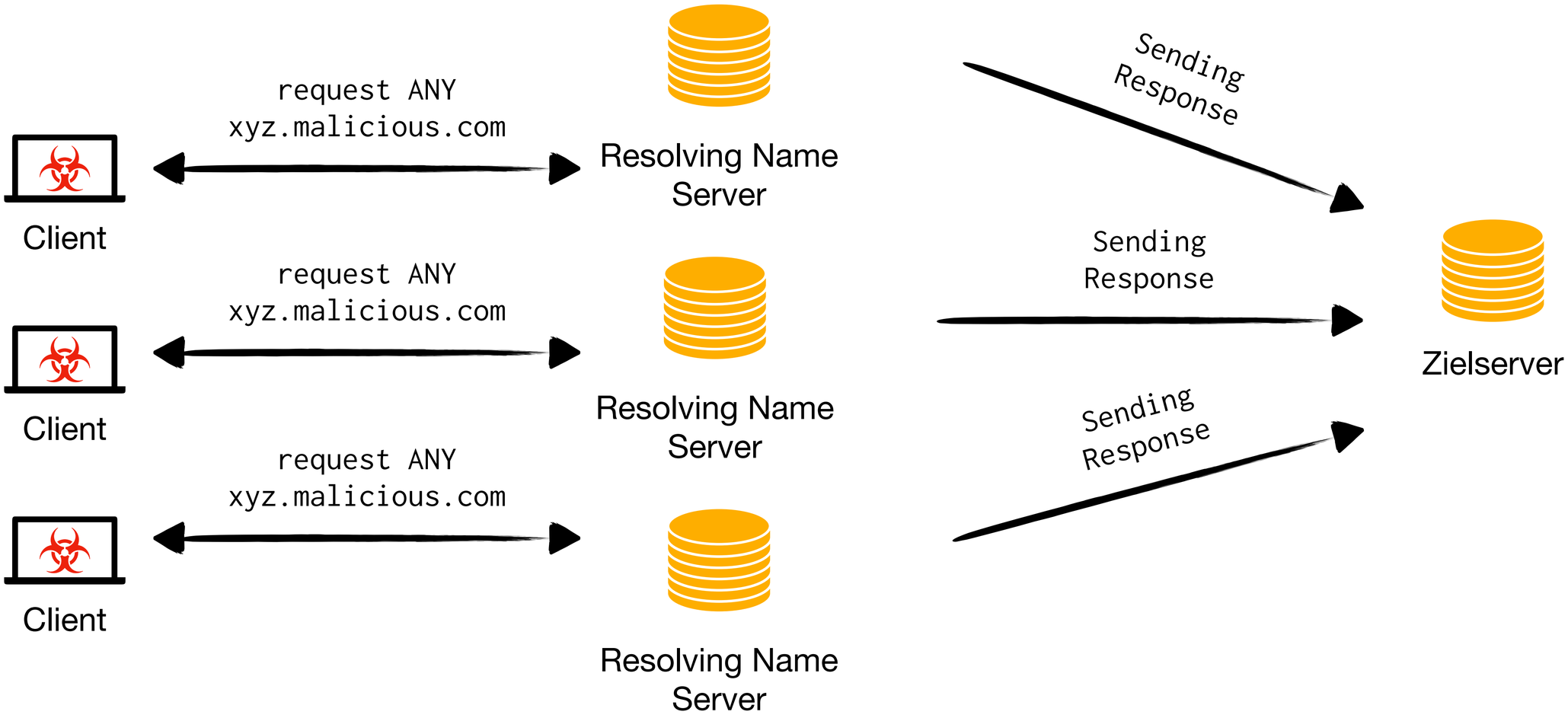
DNS Amplification Angriff

Kurze Einführung



DNS Amplification Angriff

Kurze Einführung



Live Demo

https://github.com/lilmond/Ultimate-DNSAmp

Mitigation von DNS Amplification

- Verschiedene Möglichkeiten, als Beispiel:
  - DNS Server Konfiguration:
    Verarbeitung von vertrauenswürdigen IP-Adressen
  - Rate Limiting:
    Maximale Anfrage einer IP-Adresse über bestimmten Zeitinterval
  - IP Spoofing :
    Umsetzung von Egress-Filtering
  - Firewalling:
    Detektion von volumenbasierten Anfragen

IDS Lösung

heiDGAF

- **Aktuell**: Entwicklung eine verteilten IDS Lösung als Open-Source Projekt.
- Unterstützt die Detektion von DGAs
- Mehr unter https://heidgaf.readthedocs.io

Lösungen

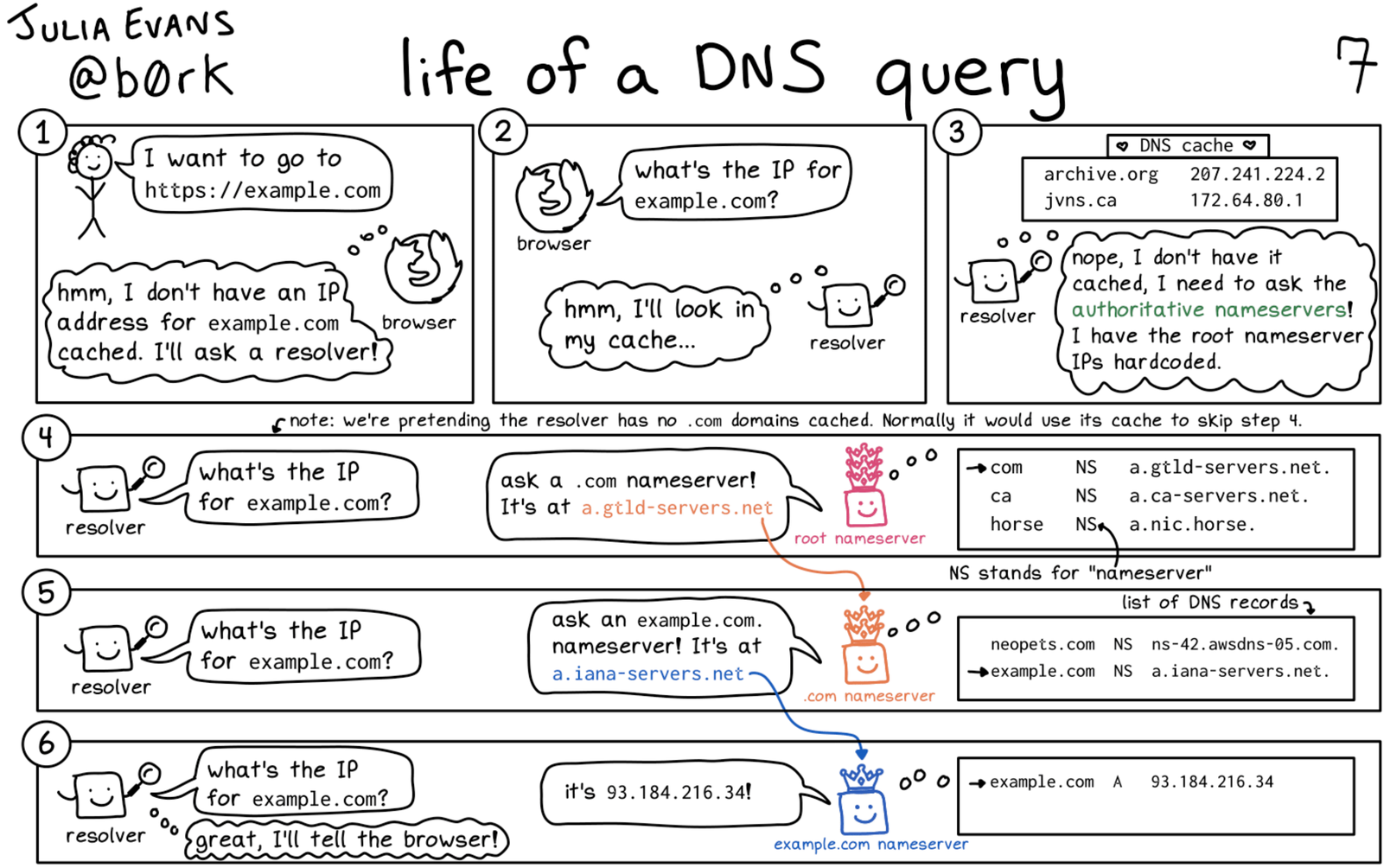
DNS aber sicher?

- DNS over HTTPS:
  - Aus Sicht des Angreifers einfacher Exfiltration oder Kommunikation mit C&C zu betreiben.
  - **Allerdings:** Fingerprinting ist möglich.
- DNSSEC:
  - Reduziert **nicht zwingend** die Angriffsoberfläche.
  - Hilft bei Amplification Angriffen.

Zusammenfassung

- **DNS** ist eines der meistgenutzten Protokolle.
- Angriffe sind möglich und auch in der Praxis relevant.
- Mitigation je nach Angriff umsetzbar.

Zusammenfassung



https://wizardzines.com/comics/life-of-a-dns-query/