Darknet

Einige NZZ - Schlagzeilen

Schweiz: Verträge der Schweizer Luftwaffe nach Hackerangriff im Darknet veröffentlicht
(nzz, 5.1.2024)

Ein 53-jähriger Zürcher befindet sich in einem erbitterten Streit mit seiner Ex-Partnerin. Dann bestellt er im Darknet einen Auftragsmörde
(NZZ, 27.1.2024)

Die Massage-Connection: Wie zwei Zürcher die Schweiz im Darknet mit Kokain versorgt haben (NZZ, 31.1.2024)

Kinderpornografie flutet das Internet. «Wir machen so viel, und doch wird es schlimmer», sagt ein Zürcher Ermittler (NZZ, 18.3.2024)

Einige SRF - Schlagzeilen

Kinderpornografie flutet das Internet. «Wir machen so viel, und doch wird es schlimmer», sagt ein Zürcher Ermittler
(SRF, 24.8.2023)

Daten des Fedpol im Darknet veröffentlicht
(SRF, 3.6.2023)

Auszug aus Hooligan-Datenbank im Darknet gefunden
(SRF, 12.7.2023)

CH-Media Daten im Darknet: Wie brisant sind die Daten?
(SRF, 4.5.2023)

Alle diese Schlagzeilen haben dann zu Fragen geführt:

Was steckt hinter dem Darknet?

Darknet - eine helle Seite des Internets?

ChatGPT

Inhalt

I. Was ist das Darknet

Versuch einer Definition

Darknet

Digitaler Ort, der sich mit

technologischen Mitteln abschirmt und

Anonymität bei der Nutzung

herstellt.

Teilbereiche des Internets

Clear Web:

- Öffentlich zugängliche Website
- Über Suchmaschinen wie Google auffindbar
- Bsp.: Nachrichtenartikel, E-Commerce, Social-mediaplattformen

Deep Web:

- Nicht-indexierte Webseiten
- Passwortschutz / spez. Zugriffsberechtigungen
- Bsp.: Private E-Mail-Konto, Online-Banking, medizinische Aufzeichnungen, Online-Speicher

Ca. 90 - 95 % des Internets

Darknet:

- Spezielle Zugangssoftware (Torbrowser)
- Datenverkehr stark verschlüsselt / anonymisiert
- Teil vom Deep Web (ca. 5 %)
- Bsp.: Legale und illegale Webseiten / Communities

I. Was ist das Darknet

Einige Zahlen

Nutzer: 2 000 000 bis 5 000 000 / Tag

Umsatz:
- 2022: 1.5 Milliarden $ (Hydra geschlossen)
- 2021: 3.1 Milliarden $

Produkte / Preise

Geklonte Visa/Mastercard mit PIN	$25
Online Banking login	$120
gehacktes Facebook-Konto	$ 65
EU-Pass	$4000
Android Malware	$900
DDoS-Attacke	$15 - $1000

II. Wie funktioniert Darknet

Technologische Mittel

Netzwerk-Architektur
Verteiltes Netzwerk mit freiwilligen Knotenpunkten / Bridges
-> TOR-Netzwerk

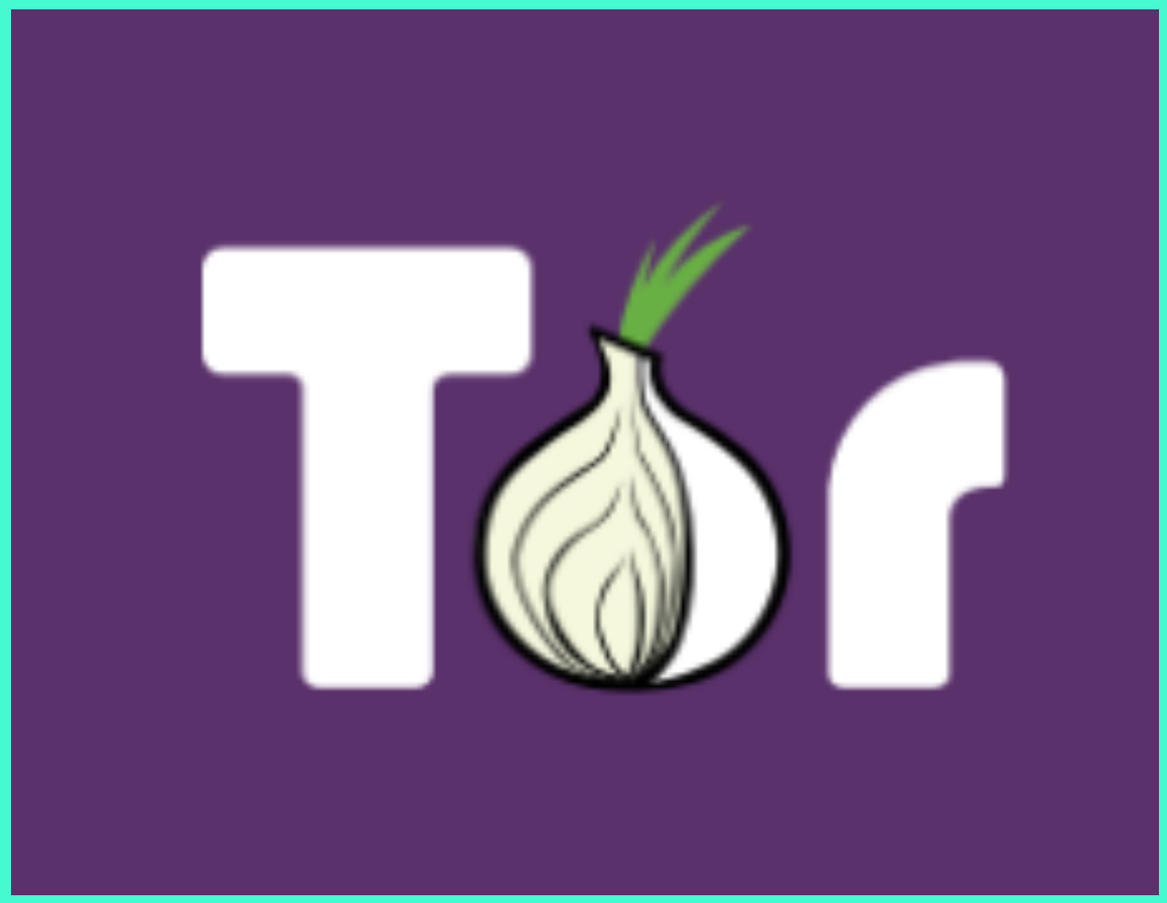
Zugang
Spezielle Browser (TOR)
Spezielle Suchmaschinen (DuckGoGo)

Anonymität
Verschleierte IP-Adressen
mehrfache Verschlüsselung
Kryptowährungen

Inhalt

II. Wie funktioniert Darknet

Technologische Mittel



The
Onion
Routing

II. Wie funktioniert Darknet

Das TOR-Netzwerk

Relays (Knoten, Nodes)
zwischen 6000 bis 7000 aktiv
öffentlich bekannt
Rückgrat des Tor-Netzwerkes
anonymisieren den Datenverkehr

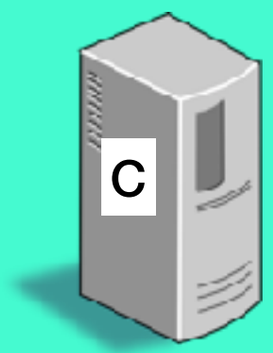
Betreiber

- Freiwillige Einzelpersonen
  (*Einsatz für Datenschutz und Anonymität im Internet)*
- Organisationen und Unternehmen
  (Förderung der Meinungsfreiheit, Menschenrechte, sichere Kommunikationswege)
- Forschungs- und Bildungseinrichtungen
  (Tor-Netzwerk für Forschungs- und Bildungszwecke
- Tor-Project
  (aktuelles Verzeichnis der Relais, Routing sicherstellen)

Das TOR-Netzwerk

II. Wie funktioniert Darknet

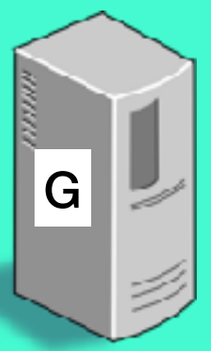
83.76.177.172 computeria-horgen.ch

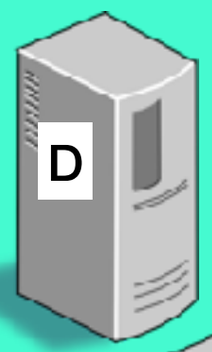


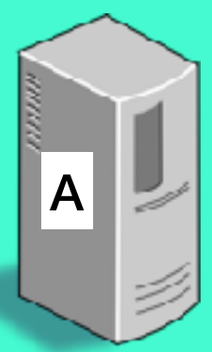
213.329.221.71

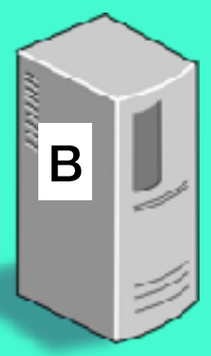
> 7000 Knoten -> 2 bis 4 Mio User/Tag

> 2500 Bridges -> 120000 User/Tag









213.329.221.71

II. Wie funktioniert Darknet

Das TOR-Netzwerk

Bridges
Keine genauen Zahlen, mehrere Tausend
Nicht im öffentlichen Verzeichnis von Tor
Dienen der Umgehung der Zensur
-> absichtlich versteckt, dynamisch

Betreiber

- Freiwillige Einzelpersonen
  (*Einsatz für Datenschutz und Anonymität im Internet)*
- Organisationen und Unternehmen
  (Förderung der Meinungsfreiheit, Menschenrechte, sichere Kommunikationswege)
- Forschungs- und Bildungseinrichtungen
  (Tor-Netzwerk für Forschungs- und Bildungszwecke
- Tor-Project
  (aktuelles Verzeichnis der Relais, Routing sicherstellen)

II. Wie funktioniert Darknet

Normaler Verbindungsaufbau

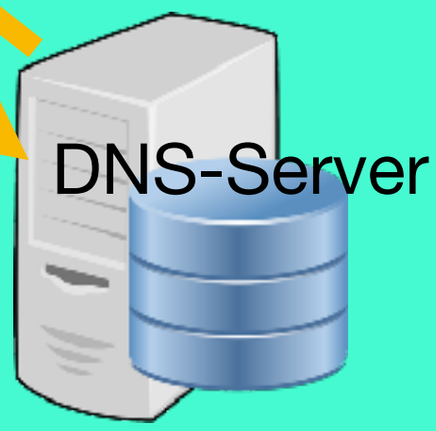
83.76.177.172

213.329.221.71

83.76.177.172

213.329.221.71

computeria-horgen.ch



Ich kenne dich 83.76.177.172!

Problem:
Fehlende Anonymität

Das TOR-Netzwerk

II. Wie funktioniert Darknet

83.76.177.172 computeria-horgen.ch

213.329.221.71

TOR

C

F

G

A

D

B

E

Netzwerk-
Verzeichnis

213.329.221.71

DNS-Server

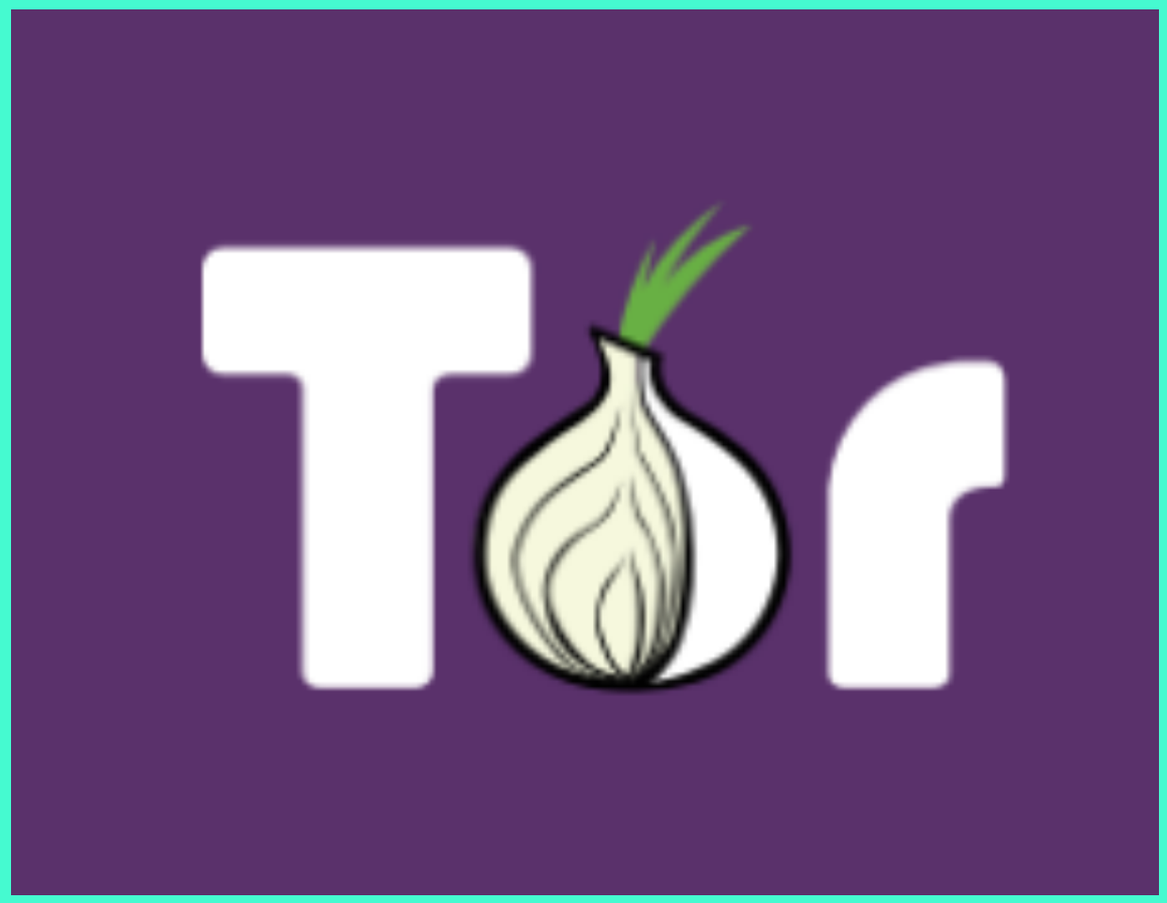
Entry-Node = A

Middle Relay = F

Exit Node = G

II. Wie funktioniert Darknet

Technologische Mittel



The
Onion
Routing

II. Wie funktioniert Darknet

Technologische Mittel

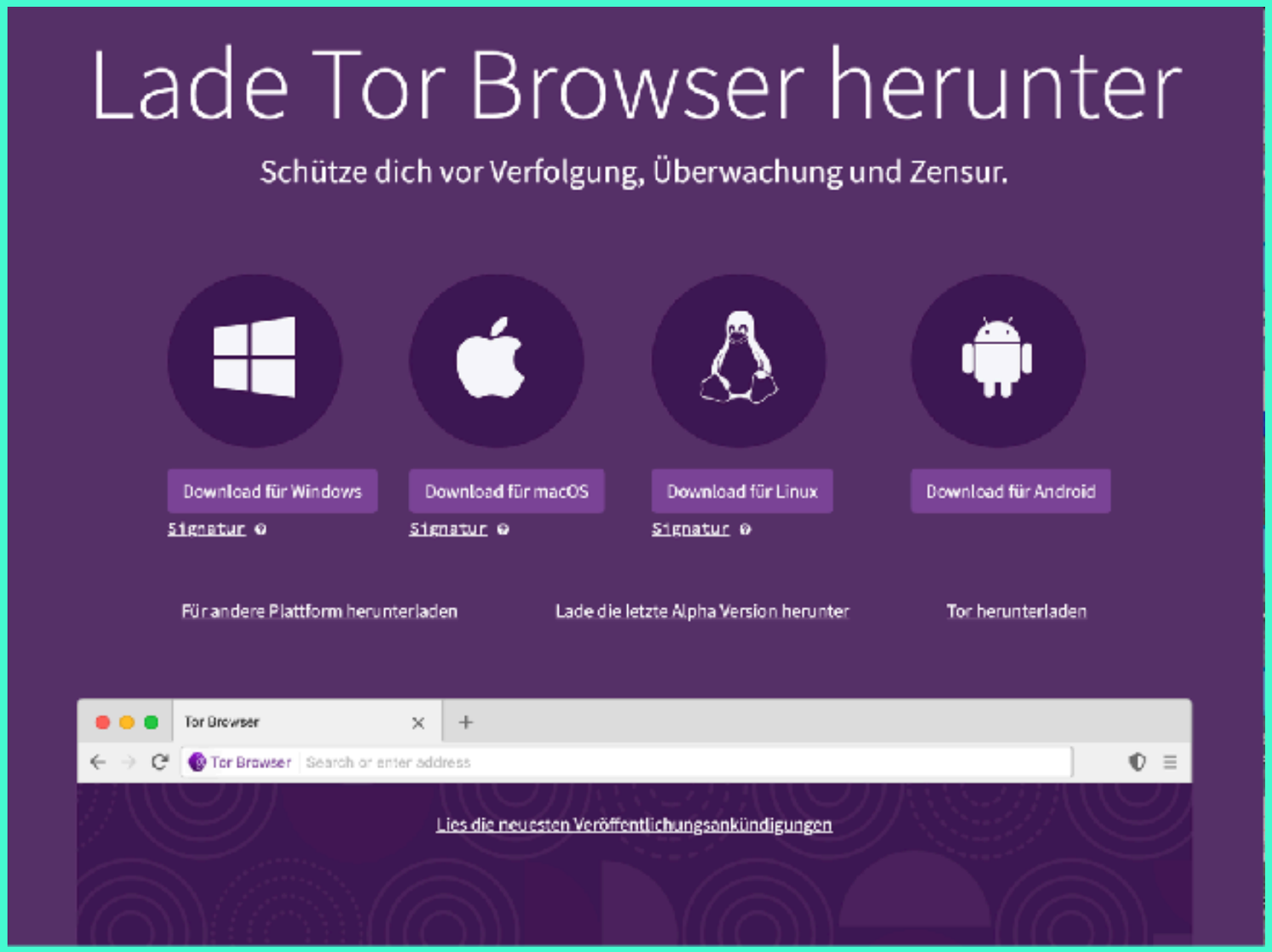
TOR - Browser

DuckDuckGo

- Basiert auf Firefox
- auf möglichst grosse Sicherheit torkonfiguriert
- DuckDuckgo als Standard-„Suchmaschine“

II. Wie funktioniert Darknet

Technologische Mittel



https://www.torproject.org/de/download/

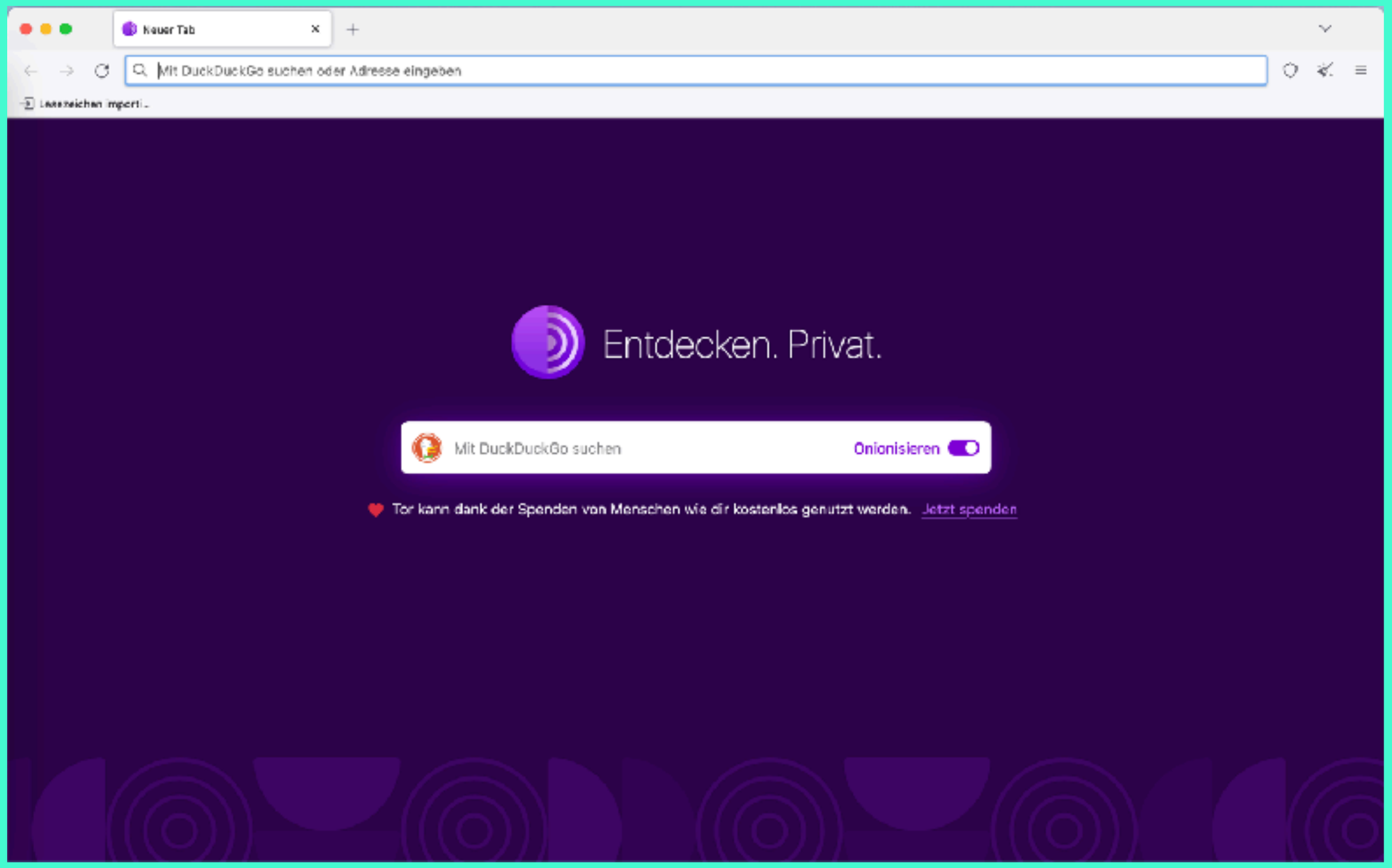
Technologische Mittel

… und iOS?

AppleStore:
- ONION Browser
- ORBOT VPN-Zugang

Entwickler eng mit Tor-Project verbunden
Apple Vorgaben (iOS-Browser-Webkit) reduzieren Privatsphäre

Technologische Mittel



Tor-Browser: Startbild

Inhalt

III. Historischer Kontext

Ursprünge und frühe Entwicklung

1995-1997: Entwicklung des „Zwiebel-Routing“ durch US Naval Research Laboratory (NRL).
Ziel: gegen Lauschangriffe und Traffic-Analyse resistente Kommunikationsmethode für das **Militär**.

1997: Erste wissenschaftliche Arbeiten zum „Zwiebel-Routing“ veröffentlicht (Paul Syverson, Michael G. Reed, David Goldschlag).

Entwicklung und frühe Implementierung

2002: Erstes Tor-Netzwerk implementiert (Leitung Paul Syverson, Roger Dingledine, Nick Mathewson).
Projekt Name: „T**he Onion Routing**“ -> **Tor**

2004: Tor wird **Open Source**, externe Entwickler beteiligen sich.

2006: **Tor-Project** als **gemeinnützige Organisation** gegründet.
Ziel: Entwicklung und Verbreitung von Tor zu fördern.
Unterstützung u.a. durch Electronic Frontier Foundation (EFF)

III. Historischer Kontext

Verbreitung und Akzeptanz

2008: **Tor Browser Bundle** veröffentlicht -> Vereinfacht den Zugang zum Netzwerk für den Endbenutzer (vorkonfigurierter Tor Browser).

2010er Jahre: Zunehmende Bekanntheit
Nutzung durch Aktivisten, Journalisten und Nutzern in Ländern mit strenger Internetzensur
Empfehlung durch **Edward Snowden** -> Wahrung Privatsphäre

Technologische und gesellschaftliche Entwicklungen

2013: Snowdens Enthüllungen NSA Massenüberwachung
-> gesteigertes Interesse an Datenschutz-Tools

2014: Einführung des „**Hidden Service Protocol**“ -> Onion Services
Hosten von anonymen Webseiten unter .onion-Domains
zusätzliche Anonymitätsschichten

Inhalt

IV. Legale Aktivitäten im Darknet

Grundsatz

Ich darf mich im Darknet bewegen; dies ist nicht illegal.
Das Netzwerk per se ist nicht unzulässig.
Straffällig wird man beim Konsumieren oder Herunterladen illegaler Inhalte, beim Erwerb von rechtswidrigen Waren und Dienstleistungen.

Schutz der Privatsphäre und Anonymität

- Journalisten und Whistleblower
  Anonym und sicher mit Quellen kommunizieren (*SecureDrop*)
- Aktivisten und Dissidenten
  Umgehung der Zensur / Überwachung in repressiven Ländern

Sicheres Browsen

- Normaler Benutzer: Online-Aktivitäten vor Tracking und Überwachung schützen

IV. Legale Aktivitäten im Darknet

Forschung und Bildung

- Akademische Forschung:
  Studien über Cyberkriminaltät, Sicherheit, andere relevante Themen.
- Lehrmaterialien
  Verteilung von Lehrmaterialien, Zugriff auf Bildungsressourcen (Regionen mit eingeschränktem Zugang zum Internet

Marktplätze und Dienstleistungen

- Spezialisierte Dienstleistungen (für IT-Sicherheitsexperten)
- Austausch von Wissen und Dienstleistungen
  (aus Datenschutzgründen nicht im normalen Internet)

IV. Legale Aktivitäten im Darknet

Freie Meinungsäusserung

Verschiedene Diskussionsforen ermöglichen freie Kommunikation ohne Zensur oder Verfolgung.

Zugang zu blockierten Informationen

- Umgehung von Zensur:
  Zugang zu blockierten Websites und Informationen

Inhalt

V. Illegale Aktivitäten

Marktplätze für illegale Waren

- Drogen
- Gefälschte Ausweise
- Waffen
- Gestohlene Daten
- Hacker-Software

Cyberkriminalität

- Hacking
- Phishing-Angriffe
- Ransomware
- Gestohlene persönliche Informationen
- Hacker-Software

Kinderpornografie und Menschenhandel

V. Illegale Aktivitäten

Herausforderung für Strafverfolgungsbehörde

- Anonymität:
  erschwert Identifizierung und Verfolgung der Straftäter
- Kryptowährungen:
  Finanzielle Transaktionen nur schwer zurückverfolgen
  (98 % der Transaktionen in Bitcoin oder Monero)

Bekämpfung der illegalen Aktivitäten

- Internationale Zusammenarbeit entscheidend
- Bemühungen, Anonymität zu verringern

V. Illegale Aktivitäten

Erfolge der Ermittlungsbehörden

- Zerschlagung Plattform „Welcome to Video“ (2018)
  - eine der grössten Kinderpornografie-Websites
  - 337 Personen in 38 Ländern verhaftet
  - 23 Kinder gerettet

- Zerschlagung der Darknet-Märkten Alphabay und SilkRoad
  - Drogen, Waffen, Hacking-Dienstleistungen

- DarkMarket wird 2021 zerschlagen (Deutschland)
  - Marktplatz mit 550’000 Usern

- „ChipMixer“ März 2024 zerschlagen (Kanton Zürich)
  - online Geldwäsche

Inhalt

VI. Bekannte Darknet Marktplätze

Silk Road
- 2011 gegründet (Ross Ulbricht)
- Tor-Netzwerk, Bitcoin
- Hauptsächlich Drogen; gefälschte Ausweise, Waffen
- 2013 vom FBI geschlossen, Ross Ulbricht lebenslange Haft (2017)
- mehrere Nachfolger

AlphaBay
- 2014 als Nachfolger von Silk Road gegründet (Alexandre Cazes)
- Tor-Netzwerk, Kryptowährungen
- Drogen, gestohlene Daten, gefälschte Dokumente, Hacking-Dienste, Waffen
- grösste, bekannteste Darknet-Plattform
- 2017 geschlossen, internationale „Operation Bajonet“
- Viele Nachfolge-Organisationen -> geschlossen durch Behörden

WallStreet Market
- 2016 gegründet
- Tor-Netzwerk, Kryptowährungen
- Drogen, gefälschte Dokumente, gestohlene Daten, Malware, Hacking-Dienste
- 2019 Betreiber mit Nutzerguthaben verschwunden durch Behörden (D, NL, USA) geschlossen

Inhalt

Sicherheitsrisiken

Malware und Viren

- **Verbreitung von Schadsoftware**
  - bösartige Daten herunterladen / infizierte Links anklicken
- **Ransomware**
  - Ransomware Angriffe über Darknet orchestriert

Datendiebstahl

- **Phishing / Scanning**
  - zahlreiche Betrugsseiten
- **Datenlecks**
  - Kreditkartendaten / persönliche Identitätsdaten zum Verkauf

Illegale Aktivitäten

- **Drogenhandel, Waffenhandel, illegale Marktplätze, Pornographie**
  - unwissentlich in kriminelle Machenschaften verwickelt

Sicherheitsrisiken

Malware und Viren

- **Verbreitung von Schadsoftware**
  - bösartige Daten herunterladen / infizierte Links anklicken
- **Ransomware**
  - Ransomware Angriffe über Darknet orchestriert

Datendiebstahl

- **Phishing / Scanning**
  - zahlreiche Betrugsseiten
- **Datenlecks**
  - Kreditkartendaten / persönliche Identitätsdaten zum Verkauf

Illegale Aktivitäten

- **Drogenhandel, Waffenhandel, illegale Marktplätze, Pornographie**
  - unwissentlich in kriminelle Machenschaften verwickelt

VII. Sicherheitsrisiken und Schutzmassnahmen

Schutzmassnahmen

Aktualisierung von Software
- Regelmässige Updates von Tor und andere SW essentiell

Verwendung von VPN
- kann zusätzliche Sicherheit bieten

Vorsicht
- links und Dateien nur von vertrauenswürdigen Quellen

Anonymität wahren
- nie persönliche Daten preisgeben
- sichere Kommunikationsmethoden nutzen

Inhalt

VIII. Zukünftige Entwicklungen

Technologische Entwicklungen

- Weiterentwicklung der Anonymisierungstechnologien
  - Verbessert Privatsphäre
  - Erschwert Kampf gegen illegale Aktivitäten
- Blockchain und Smart Contacts
  - Neue Möglichkeiten für sichere und anonyme Transaktionen

Ethik und Regulierung

- Balance zwischen Privatsphäre und Sicherheit
- Verstärkte internationale Zusammenarbeit

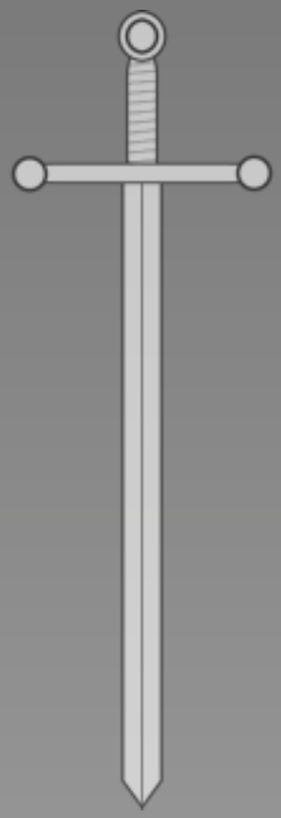
Verantwortung der Plattformen

- Bekämpfung illegaler Inhalte
  Eigenleistung der Plattformen zum Schutz vor Missbrauch
- Transparente Governance
  Protokolle, Regeln/Richtlinien, Moderationssysteme

Bildung und Aufklärung

Darknet

IX. Fazit



Vorteile in Bezug auf

- Anonymität
- Privatsphäre

Nachteilig in Bezug auf

Illegale Aktivitäten

Wichtig

Risiken erkennen
Schutzmassnahmen ergreifen

X. Fragen

Quellen

Tor Projekt: www.torproject.org

Tor Statistik: https://metrics.torproject.org/userstats-relay-table.html

Avast: https://www.avast.com/de-de/c-dark-web-facts

Literatur: Darknet, Stefan Mey, Verlag C.H. Beck, 2021

Diverse „Gespräche“ mit ChatGPT