MASTERARBEIT

NUTZER- UND NUTZERINNENVERHALTEN IM DARKNET

Kommunikationskanäle und Risiken des unzensierten Netzwerkes

ausgeführt am

26. März 2021

Studiengang

Informationstechnologien und Wirtschaftsinformatik

Von: Eliska Krnavkova

Personenkennzeichen: 1910320038

Graz, am 26. März 2021 .....

Unterschrift

EHRENWÖRTLICHE ERKLÄRUNG

Ich erkläre ehrenwörtlich, dass ich die vorliegende Arbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen nicht benützt und die benutzten Quellen wörtlich zitiert sowie inhaltlich entnommene Stellen als solche kenntlich gemacht habe.

.....

Unterschrift

KURZFASSUNG

Das Darknet, von vielen auch als das „böse Internet“ bezeichnet, bringt aufgrund seiner mysteriösen Natur viele Fragen mit sich. Es handelt sich um einen Teil des Deep Webs mit der besonderen Eigenschaft, dass Links im Darknet von keiner Search Engine indiziert werden können. Dieses Netzwerk besitzt jedoch weitere interessante Eigenschaften. Der Grad an Anonymität, welcher Darknet-Nutzern ermöglicht wird, ist im Laufe der Zeit charakteristisch für das Darknet geworden und damit auch zu seinem größten Vorteil geworden. Die Chancen, welche mit dem hohen Anonymisierungsgrad verknüpft sind, bringen ein breites Spektrum an Handlungsmöglichkeiten mit sich.

Der Handel besitzt eine dominante Rolle im Darknet. Nicht nur diverse Drogen, sondern auch Fälschungen von persönlichen Dokumenten, schädliche Malware oder Hacking-Anleitungen sowie Schusswaffen können im Darknet problemlos erworben werden. Auch Rohdaten in unterschiedlichster Ausprägung spielen eine wichtige Rolle in diesem Netzwerk. So werden zahlreiche Whistleblowing-Seiten zum Vertrieb von Informationen verwendet oder auch weitere Kanäle, wie zum Beispiel Foren. Darknet-Nutzer können solche Daten konsumieren ohne Angst vor Zensur zu haben, da diese im Darknet keine Anwendung findet.

So wie das Darknet ursprünglich für die sichere Kommunikation des amerikanischen Militärs entwickelt wurde, wird es heutzutage - nicht mehr auf das Militär eingeschränkt - zum gleichen Zweck eingesetzt. Hierbei wird eine Vielfalt an attraktiven Kommunikationskanälen angeboten, welche die uneingeschränkte Konversation erst möglich machen. Solche Grenzenlosigkeit kann jedoch sehr schnell zu starken Änderungen in der Verhaltensweise beider Gesprächspartner führen. Versteckt hinter dem Gefühl unbeschränkter Anonymität können im Darknet die persönlichen Grenzen aufgebrochen werden und das Verhalten der Anwender dieses Netzwerks ändert sich. Nichtsdestotrotz bringen die Kontaktaufnahme und das Kennenlernen anderer Nutzer zahlreiche interessante Erfahrungen mit sich, der Aufenthalt im Darknet stellt ein attraktives, überwältigendes Erlebnis dar.

ABSTRACT

The darknet, also referred to by many as the "evil internet", raises many questions due to its mysterious nature. It is a part of the deep web with the special characteristic that links on the darknet cannot be indexed by any search engine. However, this network possesses further interesting qualities. The degree of anonymity provided to darknet users has become characteristic of the darknet over time and has thus also become its greatest advantage. The opportunities associated with the high degree of anonymity entail a broad spectrum of possibilities for action.

Trade plays a dominant role in the darknet. Not only various drugs but also forgeries of personal documents, harmful malware or hacking instructions as well as firearms can be easily acquired on the darknet. Furthermore, also raw data in various forms plays an important role in this network. For example, numerous whistleblowing sites are used to distribute information as are other channels such as forums. Darknet users can consume such data without fear of censorship as this does not apply in the darknet.

Just as the darknet was originally developed for the secure communication of the American military, it is used today - no longer restricted to the military - for the same purpose. A variety of attractive communication channels are offered which make unrestricted conversation possible in the first place. Such boundlessness, however, can very quickly lead to strong changes in the behavior of both conversation parties. Hidden behind the feeling of unrestricted anonymity, personal boundaries can be broken and the behavior of darknet users changes. Nevertheless, making contact and getting to know other participants leads to many interesting experiences; being on the darknet is an attractive, overwhelming experience.

INHALTSVERZEICHNIS

1 EINLEITUNG

„Darknet. Bereits der Name impliziert dunkle Machenschaften, Schattenwirtschaft, das „Böse“ im Netz. Über keinen Teil des Internets kursieren mehr Gerüchte und Mythen und kaum ein Teil bekommt derzeit mehr mediale Aufmerksamkeit“ (Rückert, 2018).

Die Attraktivität von Darknet und seine steigende mediale Berühmtheit machen dieses Netz zu einem interessanten Thema, welches eine breite Skala an attraktiven Forschungsbereichen für eine wissenschaftliche Arbeit bietet.

Diese Arbeit diskutiert dabei die Chancen und Risiken von Darknet mit dem Hauptfokus auf die Nutzungsmöglichkeiten dieses unzensierten Netzwerkes. Der besondere Fokus liegt auf einer genaueren Untersuchung des Charakters von Darknet verbunden mit einem tiefen Einblick in die breite Skala an Nutzungsmöglichkeiten, welche bei der Erleichterung des alltäglichen Lebens ihren Einsatz finden.

Durch eine umfangreiche Recherche sowie eine detaillierte Betrachtung der Eigenschaften des Darknets wird eine aufschlussreiche Differenzierung zwischen Surface Web, Deep Web und Darknet gewährleistet und deren Potenziale hervorgehoben.

1.1 Problemstellung und Motivation

Heutzutage werden zahlreiche Bereiche des alltäglichen Lebens digitalisiert und dadurch modernisiert. Nicht nur unsere, sondern auch die virtuelle Realität wird stets verändert beziehungsweise weiterentwickelt. Zahlreiche neue Möglichkeiten verleiten dazu, ausprobiert zu werden, um den eigenen Horizont zu erweitern. Wenige Nutzer stellen sich dabei die Frage nach der eigenen Sicherheit sowie nach der Sicherheit der Software. Denn die digitale Welt, das Netzwerk, wird immer noch als abstrakt wahrgenommen, die „unreale Realität“.

Doch wie soll denn das breite Web gesteuert und kontrolliert werden, um Gefahren und Sicherheitslücken vorzubeugen, wenn das World Wide Web so komplex aufgebaut und doch so allgegenwärtig ist? Die Schattenseite des Internets – das Darknet – bringt viele offene Fragen mit sich, welche mit Hilfe dieser Arbeit beantwortet werden sollen. Bereits der geheimnisvolle Charakter dieses Netzwerkes stärkt seine Attraktivität und das Interesse an der Bearbeitung der Thematik.

Die Ausarbeitung dieser Masterarbeit ermöglicht einen tiefen Einblick in den Bereich des unzensierten Netzwerkes. Aber nicht nur die Möglichkeit des Erwerbs neuer beziehungsweise

die Vertiefung bereits vorhandener Kenntnisse, sondern auch die starke Praxisbezogenheit sowie die aktuelle Relevanz dieser Thematik erwecken ein starkes Interesse. Der persönliche Fokus der Verfasserin liegt dabei auf der Analyse unterschiedlicher Nutzungsmöglichkeiten des Darknets, insbesondere deren Diversität und der daraus ableitbaren Relevanz für das alltägliche Leben. Die zusätzliche Möglichkeit, den eigenen Horizont in der Praxis durch die Fertigstellung dieser Arbeit erweitern zu können, unterstreicht die Attraktivität dieses Themas.

1.2 Zielsetzung

Im Theorieteil dieser Arbeit soll ein ausreichendes Grundverständnis für die diversen Teilbereiche des Webs geschaffen werden. Darauffolgend wird eine aussagekräftige Differenzierung zwischen Surface Web, Deep Web und Darknet geschaffen. Im Anschluss daran werden die Chancen und Risiken sowie die Einsatzmöglichkeiten des Darknets diskutiert und die damit in Verbindung stehenden Potenziale aufschlussreich miteinander verglichen. Das dient der Verdeutlichung und Veranschaulichung der Unterschiede zwischen den Einsatzbereichen des unzensierten Netzwerkes, sowie der Potenziale, welche andere Bereiche des World Wide Webs nicht bieten können.

Im praktischen Teil dieser Arbeit werden die im Darknet eingesetzten Kommunikationskanäle analysiert. Hierbei wird untersucht und dokumentiert, wie die Kommunikation abgewickelt wird, welche Medien eingesetzt und welche Maßnahmen vorgenommen werden. Ein besonderer Fokus liegt dabei auf der Vorgehensweise und auf der Wahrung der Anonymität der handelnden Parteien.

Eine umfangreiche Auswertung der Analyse der Kommunikation im Darknet soll dabei die relevanten Ergebnisse liefern, um die **Forschungsfrage**

„Welche Kommunikationskanäle werden für die Interaktion zwischen NutzerInnen vom Darknet am häufigsten eingesetzt?“

eindeutig beantworten zu können.

Große Aufmerksamkeit wird hierbei auch den Risiken solcher Aktionen gewidmet. Einerseits wird hier im Detail betrachtet, auf welchem Wege die eigene Identität geschützt werden kann und andererseits werden Möglichkeiten zum Schutz des eigenen Systems vor schädlicher Malware, Cyber-Attacken, Hackerangriffen und anderen Gefahren diskutiert.

Eine Analyse dieser Punkte soll dabei alle relevanten Daten liefern, um auch die **Subforschungsfrage** *„Welche Maßnahmen müssen ergriffen werden, um sowohl die Identität des Nutzers/der Nutzerin als auch seine/ihr System zu schützen?“* aussagekräftig beantworten zu können.

Als Hypothesen wurden die folgenden definiert:

Hypothese 1:

Nullhypothese: Das Darknet wird nur für illegale Geschäfte, wie z.B. Drogen-, Waffenverkauf oder Kinderpornographie verwendet. Für einen durchschnittlichen Internetnutzer hat dieses abgetrennte Netzwerk keinen Mehrwert.

Alternativhypothese: Das Darknet wird nicht nur für illegale Geschäfte verwendet. Aufgrund der sichergestellten Anonymität des Nutzers wird Darknet gehäuft auch in Ländern mit strikten Gesetzen und Einschränkungen der Privatsphäre eingesetzt, um diese zu umgehen.

Hypothese 2:

Nullhypothese: Für die Interaktion zwischen Nutzern des Darknets werden gesonderte Kommunikationskanäle verwendet. Bekannte soziale Netzwerke, wie zum Beispiel Facebook, stellen in diesem Fall für die Anonymität der Nutzer ein Risiko dar.

Alternativhypothese: Das Darknet und seine Nutzer verwenden für die Interaktion untereinander mehrere Kommunikationskanäle, unter anderem auch bekannte soziale Netzwerke wie Facebook, da bereits das Darknet an sich einen ausreichenden Grad an Anonymität den Nutzern gegenüber gewährleistet.

1.3 Vorgangsweise

Mit Hilfe umfangreicher Literatur- und Online-Recherchen wird zunächst versucht, sich einen klaren Überblick über das Darknet zu verschaffen. Darauffolgend werden die Vor- und Nachteile des Darknets analysiert und ein kritischer Vergleich zum Deep Web und Surface Web aufgestellt, um eine übersichtliche Abgrenzung zwischen diesen Begriffen zu schaffen.

Als Nächstes wird mit Hilfe passender Literatur auf die zahlreichen Nutzungsmöglichkeiten des Darknets fokussiert, um dieses verstehen und plausibel erklären zu können. Des Weiteren werden im Zuge dieser Arbeit Sicherheitslücken analysiert, welche mögliche Gefahren für den Nutzer und dessen System darstellen.

Der Praxisteil fokussiert sich zunächst auf den Aufbau der Arbeitsumgebung und auf das genaue Szenario der Handlungsaktion. Nach praktischer Untersuchung der Interaktionsformen und Gefahren im Darknet werden diese Ergebnisse detailliert analysiert. Den Abschluss dieser Arbeit bilden die Beantwortung der Forschungsfrage sowie ein Ausblick in die Zukunft des Darknets.

2 KOMPONENTEN DES WORLD WIDE WEB

Unsere Welt erlebte einen großen Erfolg, als im Jahre 1989 ein Physiker namens Tim Berners-Lee die Basis für das weltweit bekannte Internet erschaffen hat (Jacksi & Abass, 2019). Das Resultat dieses Ereignisses, das Internet, stellt einen immensen Meilenstein im Sinne der Digitalisierung dar und wird auch heutzutage von mehr als der Hälfte der Weltbevölkerung verwendet, davon größtenteils in Europa (vgl. Abbildung 1).

Diese Entwicklung der Gegebenheiten lässt sich leicht damit begründen, dass das Internet seinen Nutzern ein breites Spektrum an nützlichen und attraktiven Diensten bietet. Hierzu zählen zum Beispiel Messenger, E-Mail oder Konferenzdienste wie WhatsApp, Facebook oder Telegram. Der bekannteste Dienst des Internets ist jedoch das sogenannte World Wide Web, welches uns das Surfen im Internet und Besuchen von Webseiten möglich macht (Brandt, 2019).

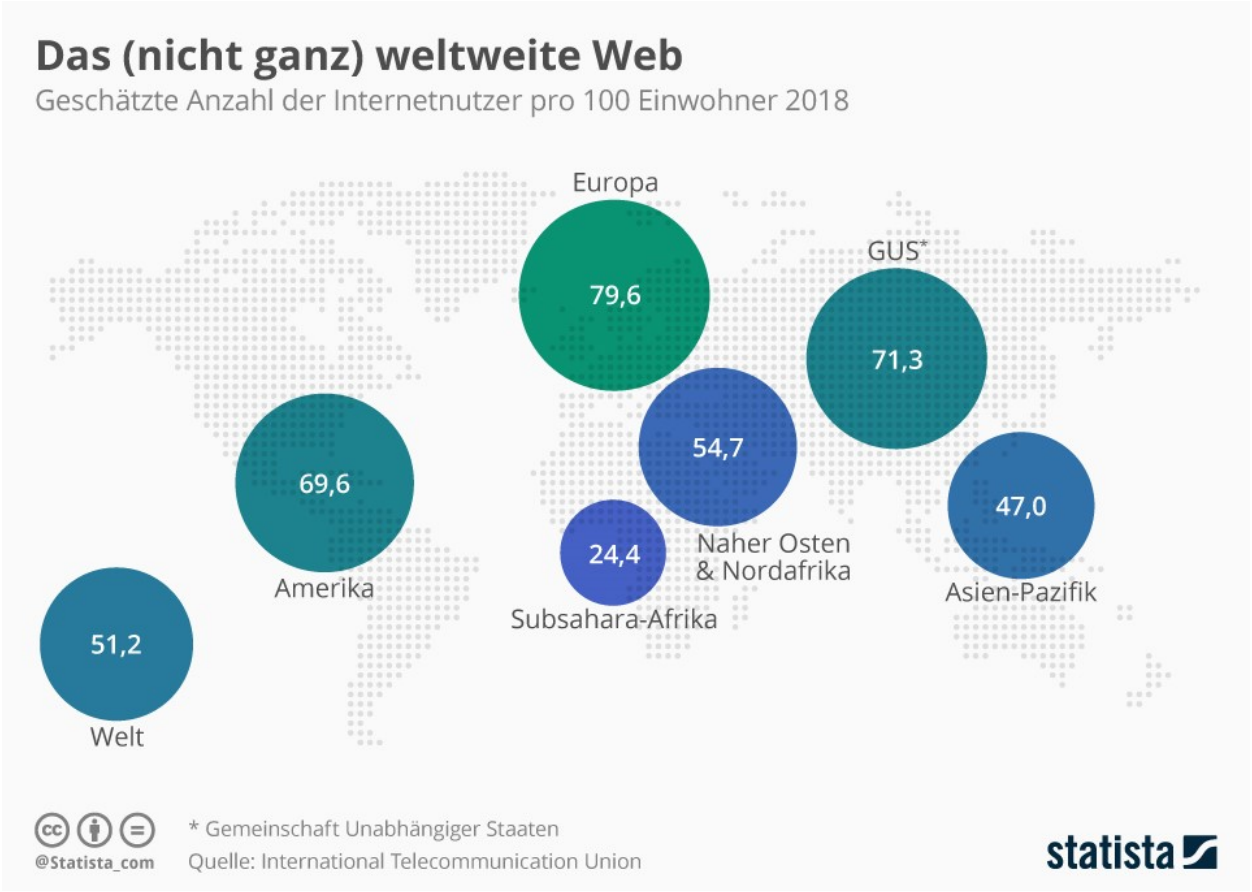


Abbildung 1: Geschätzte Anzahl der Internetnutzer pro 100 Einwohner (Brandt, 2019)

Die Erfindung des WWW *„förderte die weltweite Verbreitung durch den für Netzwerkanwendungen ermöglichten Zugriff auf die grafische Ebene und den multimedialen Reichtum von Offline-Computern, wodurch die Welt der Computer und des Internets konvergieren“ (Tardini & Cantoni, 2013).* Die Grundstruktur des World Wide Web wird durch die sinnhafte Verknüpfung aus Hypertexten und Computernetzwerken kreiert. Digitale Hypertexte sind in dieser Hinsicht ein Zusammenspiel von Knoten und Verlinkungen. Die Knoten besitzen eine bedeutende Rolle, indem sie Informationen – statischer oder dynamischer Natur – speichern.

Diese werden darauffolgend über Verlinkungen auf die erwünschte Destination transferiert. Verlinkungen dienen somit der Verbindung zwischen jeweiligen Knoten und machen damit den Informationsfluss im WWW überhaupt möglich. Dieses Zusammenspiel von Knoten und Verlinkungen, die Hypertexte, sind in der Praxis auf Webseiten zu finden, welche eine genaue Lokation im WWW darstellen (Tardini & Cantoni, 2013).

Um solche Internetseiten aufsuchen und aufrufen zu können, werden Browser verwendet, die Suchen im Web überhaupt erst ermöglichen. Das World Wide Web stellt eine gut durchdachte logische Struktur auf (Tardini & Cantoni, 2013).

Das World Wide Web als Ganzes ist so aufgeteilt, um seinen Nutzern eine komfortable Verwendung zu ermöglichen und um den Anforderungen seiner User zu entsprechen. Das WWW in das Surface Web und in das Deep Web unterteilt. Das Darknet wiederum ist Teil des Deep Web, wie in Abbildung 2 deutlich ersichtlich wird (Nelson, 2017).

Abbildung 2: Aufteilung vom World Wide Web (Nelson, 2017)

2.1 Das Surface Web

Das sogenannte „Surface Web“ zählt zu den Grundkomponenten des World Wide Web, seit der erste Browser im Jahre 1990 von Tim Berner-Lee zum Einsatz gebracht wurde. Dieser Abschnitt des Webs ist für jeden Nutzer leicht zugänglich und bildet heutzutage einen unverzichtbaren Teil des Alltags, sowohl für persönliche Angelegenheiten als auch für die Bewältigung beruflicher Aufgaben (Graham & Pitman, 2018).

Im Surface Web können mittels Suchmaschinen diverse Webseiten besucht werden, da diese indiziert werden. Einen Vorteil hierbei stellt die leichte Zugänglichkeit dar. Das Surface Web kann von jedem Nutzer problemlos erreicht und verwendet werden. Einen Nachteil verkörpert wiederum das breite Spektrum an Kontroll- und Monitoring-Maßnahmen. Diese Vorkehrungen werden ohne explizite Bekanntgabe an die User getroffen, was wiederum Streitigkeiten im Hinblick auf die Verletzung der Privatsphäre hervorrufen kann (Graham & Pitman, 2018).

Trotz der Tatsache, dass Surface Web von zahlreichen Nutzern täglich verwendet wird, stellt dieses mit weniger als fünf Prozent der WWW-Inhalte nur einen sehr geringen Teil des World Wide Web dar. Die restlichen 95 Prozent befinden sich im sogenannten „Deep Web“ (Ciancaglini, Balduzzi, McArdle, & Rösler, 2015).

2.2 Das Deep Web

Auch das Deep Web stellt eine grundlegende Komponente des World Wide Web dar. Der Hauptunterschied zwischen dem Surface Web und dem Deep Web besteht darin, dass Daten des Surface Web über Suchmaschinen aufspürbar sind, während Inhalte des Deep Web nicht frei zugänglich. Sites im Surface Web werden für Suchmaschinen indiziert, das Deep Web hingegen erscheint in keinem öffentlichen Index. Dieses Web umfasst also beispielsweise blockierte Seiten, welche ein erfolgreiches Überbrücken von sogenannten CAPTCHA voraussetzen, um Zugriff zu den erwünschten Inhalten zu bekommen. Zum Repertoire des Deep Web gehören auch dynamische sowie nicht verlinkte Seiten. Auch private Inhalte, welche eine Form des Logins als Berechtigungsnachweis benötigen und Netzwerke mit beschränktem Zugang bilden einen relevanten Teil vom Deep Web (Balduzzi & Ciancaglini, 2015).

Es gibt selbstverständlich Wege, um sich einen Zugang zum Deep Web zu verschaffen. Dabei werden unterschiedliche Methoden angewendet, um auf diesen Teil des Webs zuzugreifen. Solche verschlüsselten oder passwortgeschützten Bereiche können mit Hilfe dedizierter Browser sowie über eine Reihe komplexer Anmeldedetails erreicht werden. (Balduzzi & Ciancaglini, 2015).

Das Deep Web beinhaltet zahlreiche umfassende Datenbanken, welche akademische Informationen verwahren sowie all unsere medizinischen Aufzeichnungen, Finanzunterlagen, Rechtsdokumente und weitere relevanten Informationen, welche sicher aufbewahrt werden müssen (vgl. Abbildung 2). Mit der zunehmenden Sensibilität der Daten sowie der wachsenden Bedeutung von Informationen wurde ein sicherer Ort gesucht, wo diese Inhalte gespeichert werden können. Aus diesem Drang nach Schutz des eigenen Gedankenguts und der sensiblen Information ist die Notwendigkeit entstanden, einen Teil des Internets so zu sichern und zu

verschlüsseln, dass die aufbewahrten Inhalte nicht an unberechtigte Personen freigegeben werden (Quinney, 2016).

Nichtsdestotrotz wird das Deep Web trotz seines nachweislich nützlichen Charakters missverstanden und für einen Teil des WWWs gehalten, wo illegale Geschäfte abgewickelt werden. In der Realität sieht es jedoch so aus, dass viele legalen Teile des Deep Web in zahlreichen nützlichen Situationen des alltäglichen Lebens eingesetzt werden. Beispielsweise muss zur Behebung von Bargeld am Bankomaten die persönliche PIN-Nummer angegeben werden, um auf das eigene Bankkonto zugreifen zu können. Solche Informationen wie eine PIN-Nummer werden im Deep Web gespeichert. Es handelt sich beispielsweise um Daten, welche für die eigene Authentifizierung und Autorisierung benötigt und angegeben werden müssen, wenn der Zugang zu sensiblen Informationen erwünscht ist und gefragt wird (Quinney, 2016).

Es kann jedoch nicht abgestritten werden, dass im Deep Web auch illegale Aktivitäten stattfinden. Jener Teil des Deep Webs, der solche Interaktionen und Geschäfte ermöglicht, ist das sogenannte Darknet oder Dark Web (Ciancaglini, Balduzzi, McArdle, & Rösler, 2015).

2.3 Das Darknet

Das Darknet stellt für viele Internetnutzer ein Mysterium dar, eine Spielwiese für illegale Geschäfte. Oft werden hierbei jedoch auch die legalen und nützlichen Eigenschaften dieses Netzes vergessen: Netzwerke, welche im Internet betrieben werden und spezifische Anwendungsprotokolle sowie Autorisierungsschemata voraussetzen, um den Aufbau einer funktionalen Verbindung überhaupt zu ermöglichen. (Allahyari, Doran, Sadeghi, & Zabihimayvan, 2019).

Das Dark Web bildet zwar einen Teil des Deep Web, weist jedoch einen deutlichen Unterschied auf:

Sämtliche Inhalte des Darknets sind für standardisierte Web-Browser nicht zugänglich. Die Technologie zur Schaffung des Dark Web wurde ursprünglich Mitte der 1990er Jahre von US-Militärforschern geschaffen und finanziert, um Spionen und Geheimdiensten das anonyme Senden und Empfangen von Nachrichten zu ermöglichen (Kumar & Rosenbach, 2019).

Das Darknet umfasst Websites, die auf einer Art Infrastruktur betrieben werden, welche eine dedizierte Software erfordert, um Zugriff zu gewährleisten (beispielsweise „I2P“, „Riffle“ oder „Freenet“). Am häufigsten wird der sogenannte "The Onion Router" (auch als „TOR“ bekannt) eingesetzt. Der Name dieses bereits weit verbreiteten Tools hebt dabei die Form der Verschlüsselung der Anwendungsschicht innerhalb eines Kommunikationsprotokollstapels hervor und wird aufgrund seiner zahlreichen Schichten mit einer Zwiebel verglichen. Obwohl das TOR-Netzwerk primär als ein Kanal für kriminelle Aktivitäten und als Plattform für illegale Güter und Daten bekannt ist, war es ursprünglich als Fundament für freie Meinungsäußerung und Informationsverbreitung unter dem Deckmantel gegebener Anonymität konzipiert (Omar & Ibrahim, 2020).

Natürlich bietet die Natur des Darknets eine breite Skala an Diskussionsmaterial. Unter anderem stellt sich die Frage, ob der oft notwendige Schutz, den TOR seinen Nutzern durch die Gewährleistung der Anonymität bietet, die Risiken und Gefahren wert ist. Denn dieselben Funktionalitäten, welche die Privatsphäre von gewöhnlichen Nutzern schützen, machen TOR auf der anderen Seite zum wirksamen Mittel zur Durchführung illegaler Aktivitäten. Des Weiteren wird durch die Charakteristiken von TOR auch das Risiko einer Strafverfolgung immens minimiert. Zu dieser Thematik gibt es weiterhin sehr zwiegespaltene Meinungen. Es ist nicht möglich, diese Frage eindeutig zu beantworten, da sich empirische Untersuchungen nur auf die Analyse spezifischer Untermengen von TOR-basierten Untergruppen beschränken. Im Fokus liegt die Materie der gespeicherten Informationen, wie z.B. die Suche nach Drogenhändlern, hausgemachten Sprengstoffen oder Giften sowie terroristischen Aktivitäten und Kommunikationskanälen (Allahyari, Doran, Sadeghi, & Zabihimayvan, 2019).

2.4 Der Vergleich zwischen Surface Web, Deep Web und Darknet

Eine stark auffällige Differenz zwischen dem Surface Web und Darknet stellt der Aufbau der Darknet-URLs dar. Endet eine Webadresse mit der Top-Level-Domäne „.onion“, so handelt es sich um eine Seite aus dem Darknet. Außerdem sind die Hauptteile meist so kryptisch, dass weder der Name noch die Destination der Webseite leicht erkannt werden können (Iva, 2019).

Und es gibt weitere Unterschiede, welche beachtet werden sollten. Dem Deep Web sowie dem Darknet wird zunehmend Aufmerksamkeit gewidmet. Die meisten Internetnutzer verkehren jedoch trotzdem weiterhin öfter im Surface Web. Der Grund hierfür ist die Diversität hinsichtlich der Zugänglichkeit zwischen den drei betrachteten Webs. Während Surface Web frei über herkömmliche Browser zugänglich ist, wird für den Zugang zu Deep Web eine Form der Authentifizierung und Autorisierung benötigt. Diese wird in Form eines Passworts, einer Verschlüsselung oder beispielsweise eines Gateway-Zugangs dargestellt. Im Gegensatz dazu benötigt Darknet keine zusätzliche Authentifizierung oder Autorisierung. Zum Surfen in diesem Web werden lediglich dedizierte Netzwerke benötigt, wie zum Beispiel TOR, I2P oder Freenet, die solche Verbindungen erst ermöglichen (vgl. Tabelle Nr. 1).

Eine weitere Differenzierung liegt in der Indexierung durch Suchmaschinen. Inhalte des Surface Web sind von allen in diesem Web unterstützten Suchmaschinen indexiert. Im Gegensatz dazu weisen das Deep Web sowie das Darknet Inhalte auf, *„die von Suchmaschinen nicht erfasst werden, da sie nicht in deren Datenbestand aufgenommen wurden“* (Görmer, 2018).

Ein Aspekt, welcher wieder das Darknet von Surface und Deep Web unterscheidet, ist die Legalität der Inhalte. Während Surface Web sowie Deep Web nur sehr wenig illegalen Content aufweisen, ist das Darknet dafür bekannt, unter dem Schirm der Anonymität zahlreiches illegales Geschehen zu verstecken (vgl. Tabelle Nr. 1).

Mit einem Anteil des Surface Webs von weniger als 5 Prozent am gesamten bekannten World Wide Web-Inhalt ist diese Zahl bereits verschwindend gering, aber Schätzungen gehen davon aus, dass das Deep Web 500 bis 5000 Mal größer sein könnte. Perspektivisch gesehen gibt es etwa zwanzig Terabyte (TB) an Daten und etwa eine Milliarde Dokumente im Surface Web im

Vergleich zu 7.500 Terabyte (TB) an entdeckten Daten und fast 600 Milliarden entdeckten Dokumenten im Deep Web (vgl. Tabelle Nr. 1).

	Surface Web	Deep Web	Darknet
Zugänglichkeit	Leicht zugänglich	Zugänglich durch Passwort, Verschlüsselung oder über Gateway-Software	Zugänglich nur über dedizierte Browser
Index	Indexiert für Suchmaschinen	Nicht indexiert für Suchmaschinen	Nicht indexiert für Suchmaschinen
Legalität	Wenig illegale Aktivitäten	Wenig illegale Aktivitäten (Darknet ausgeschlossen)	Zahlreiche heterogene illegale Aktivitäten
Größe (relativ)	< 5% am bekannten WWW-Anteil	> 95% am bekannten WWW-Anteil und exponentiell wachsend	Unmessbar (aufgrund des Charakters)
Größe (absolut/geschätzt)	20 Terabyte an Daten und eine Milliarde Dokumente	7.500 Terabyte (TB) an entdeckten Daten und fast 600 Milliarden entdeckten Dokumenten	Unmessbar (aufgrund des Charakters)

Tabelle 1: Vergleich zwischen Surface Web, Deep Web Und Darknet (Quinney, 2016)

3 GRENZEN ZWISCHEN LEGALEN UND ILLEGALEN AKTIVITÄTEN IN DEEP WEB UND DARKNET

Nachdem das Deep Web einen so großen Anteil an bekannten WWW-Inhalten ausmacht, muss die Grenze zwischen legalen und illegalen Aktivitäten näher betrachtet und darauffolgend klar definiert werden. Dies dient auch als Vorbereitung für die praktische Untersuchung, welche im Kapitel 7 näher beschrieben wird. Mit der Durchführung einer ausführlichen Recherche soll sichergestellt werden, dass sich die Verfasserin im Laufe der praktischen Untersuchung stets innerhalb der Grenzen legaler Aktivitäten aufhält.

3.1 Legale Verwendung

Während das Deep Web inklusive Darknet wegen illegaler Aktivitäten bekannt wurde, gibt es auch für gesetzestreue Bürger unzählige legitime Einsätze dieses Bereichs. Einige basieren auf regulären Konzepten, wie das Teilen von Bild- und Videomaterial, die alle Vorteile der vom Deep Web angebotenen Sicherheit nutzen. Andere sind tiefer in der Natur des Deep Web verwurzelt, wie z.B. verschlüsselte Websites für Whistleblower oder e-Book-Sammlungen mit Hauptfokus auf aufrührerische Werke. Journalisten nutzen SecureDrop oder GlobalLeaks, um Dateien über das TOR-Netz zu teilen. Auch bekannte amerikanische Whistleblower wie Chelsea Manning oder Edward Snowden haben das TOR-Netzwerk verwendet, um auf eine sichere Weise die klassifizierten Akten der US-Regierung zu teilen, bevor sie online durchgedrungen sind (Sui, Caverlee, & Rudesill, 2015).

Laut Anwälten ist es erlaubt, eine funktionale Verbindung zum Deep Web aufzubauen und darin zu surfen. Was jedoch nach einer Verbindung mit diesem Teil des Internets von großer strafrechtlicher Relevanz ist, sind die Inhalte, mit welchen interagiert wird. Wird also eine Webseite besucht, welche keine illegalen Inhalte aufweist, so ist dies ein legales Verhalten. Auch die Nutzung von sozialen Netzwerken, welche nur zwischenmenschlicher Kommunikation an sich dienen, gehört zu legalen Aktivitäten. Sollten jedoch diese Kommunikationskanäle dazu verwendet werden, um eine illegale Tat zu begehen, beispielsweise für den Kauf von Waffen, Drogen oder gestohlenen Daten, so gilt dieser Akt als eine Straftat und macht den Betroffenen strafbar (Moore & Rid, 2016).

Eine beliebte Verwendung von Deep Web ist der Erwerb unzensierter Informationen. Dieses Web enthält tatsächlich den am stärksten expandierenden Vorrat an frischen Informationen im Internet und wird deswegen von zahlreichen Nutzern gerne besucht. Solche Websites sind in der Regel einfacher aufgebaut als die Seiten im Surface Web. Werden sie jedoch mit regulären Seiten des Surface Web verglichen, weisen die Inhalte des Deep Web einen markanten Detailgrad des Inhaltsmaterials auf. Und nachdem es sich in zahlreichen Fällen um geschützten Content handelt, ist die Qualität der Informationen vom Deep Web meist besser und wertvoller als die der Informationen vom Surface Web. Aufgrund dessen wird dieses Web von zahlreichen

Journalisten, Whistleblowern, politischen Akteuren und Menschenrechtsverfechtern in zahlreichen legalen Szenarien verwendet (Sui, Caverlee, & Rudesill, 2015).

Im Mai 2016 wurde eine umfangreiche Studie durchgeführt (Mirea, Wang, & Jung, 2018), um die Meinung über die „Kriminalität“ im Darknet zu untersuchen. Weniger als ein Drittel der Teilnehmer (5 von 17) bestätigte dabei, dass das Darknet ein gefährlicher Ort sei, es wurde jedoch bestritten, dass es von Natur aus kriminell sei. Auch wurde klar zum Ausdruck gebracht, dass das Darknet von der Natur aus neutral ist. Laut ihnen sind es die Nutzer, die die Kriminalität des Netzwerks überhaupt möglich machen. Des Weiteren herrschte unter diesen Probanden die Meinung, dass das Darknet als kriminell abgestempelt wurde, um Aktivitäten der Rechtsdurchsetzung und Regierungskontrolle zu rechtfertigen. Mehr als zwei Drittel der Teilnehmer (12 von 17) machten deutlich, dass jeder frei über die eigenen Handlungen entscheiden dürfen soll, ohne Angst vor Diskriminierung oder Strafverfolgung zu bekommen. So wurden beispielsweise folgende Aussagen getätigt:

> *„If you don’t explicitly search for child pornography you won’t find it. One has to differentiate. The Darknet can always be used and abused”*
> *(Mirea, Wang, & Jung, 2018).*

> *„The Darknet is not inherently criminal, just as the clear net is not inherently criminal either. I’m sure that both have illegal content such as child porn or what have you. Albeit, there are also legal uses for both. The government creating an image that the Darknet is criminal is simply them trying to take away the human rights to privacy without legally doing so”*
> *(Mirea, Wang, & Jung, 2018).*

> *„This actually made me laugh. What a nonsense! You really have to put in a lot of effort to hurt yourself or others through the Darknet. No such thing can happen accidently. The Darknet is not a threat to society, not more than the clear net anyway! I indeed think law enforcement exaggerated it all, just because they don’t like admitting that they will never have everything under control”*
> *(Mirea, Wang, & Jung, 2018).*

Diese drei Aussagen bringen zum Vorschein, dass das Darknet nicht nur für kriminelle Zwecke verwendet wird. In der Tat werden auch illegale Aktivitäten ausgeübt, jedoch wurde dieses Web ursprünglich ins Leben gerufen, um den Nutzern mehr Freiheit und zahlreiche uneingeschränkte Möglichkeiten zur legalen Verwendung zu bieten. So wurde und wird das Darknet zwar für Straftaten missbraucht, es gibt jedoch zahlreiche Nutzer, die es für den ursprünglichen, legalen Zweck verwenden (Sui, Caverlee, & Rudesill, 2015).

3.2 Illegale Verwendung

Das Wachstum von Deep Web und Darknet erlangte erst durch die Verhaftung von Ross William Ulbricht, im Oktober 2013, mehr Aufmerksamkeit. Ulbricht gab der "Silk Road" eine neue

Bedeutung. Öffentlich wurde er bekannt als Schöpfer und Betreiber eines gleichnamigen Marktplatzes im Darknet, auf dem Benutzer alle Arten von Schmuggelwaren finden konnten, insbesondere illegale Drogen (Konrad, 2013).

Silk Road war ein Online-Marktplatz, der sich hauptsächlich dem Verkauf illegaler Drogen widmete, darunter Cannabis sowie eine breite Palette von psychoaktiven Drogen wie Crystal Meth oder MDMA, verschreibungspflichtige Medikamente und ähnliches (vgl. Abbildung 3). Bereits die einfache Existenz eines „Online-Bitcoinmarktes“ für illegale Drogen verkörpert eine kriminelle Neuigkeit. Es bot zahlreichen Drogenhändlern einen virtuellen Ort, an dem sie für ihre Produkte Werbung machen und neue Kundschaft finden konnten, an die sie diese Produkte weltweit verkaufen können. Diese Verhandlungen passierten anonym und weitgehend außerhalb der Reichweite von Strafverfolgungsbehörden. Drogen wurden online von Verkäufern gekauft und mit der Post geliefert. Die Käufer waren durch ein sicheres Treuhandsystem geschützt. Sie bezahlten für ihre Drogen in Bitcoins (da hier die Identität nicht so leicht nachweisbar ist wie bei Kartenzahlungen), wodurch die Zahlung auf den Käufer nicht zurückzuführen war. Außerdem wurde die Kundschaft vor Betrügern geschützt, da die Zahlungen den Verkäufern erst dann freigegeben wurden, wenn die Käufer mit ihren Lieferungen zufriedengestellt wurden. Dieser Markt funktionierte erfolgreich, weil er im Deep Web gehostet war, wo die gesamte Kommunikation durch den Dienst „The Onion Router“ (TOR) anonym abgewickelt wurde. Die Website wurde im Februar 2011 vorgestellt und lief erfolgreich, bis sie am 2. Oktober 2013 vom FBI beschlagnahmt wurde. Bis dahin war Silk Road ein großer Erfolg mit einem enormen Zukunftspotenzial (Aldridge & Décary-Hétu, 2014).

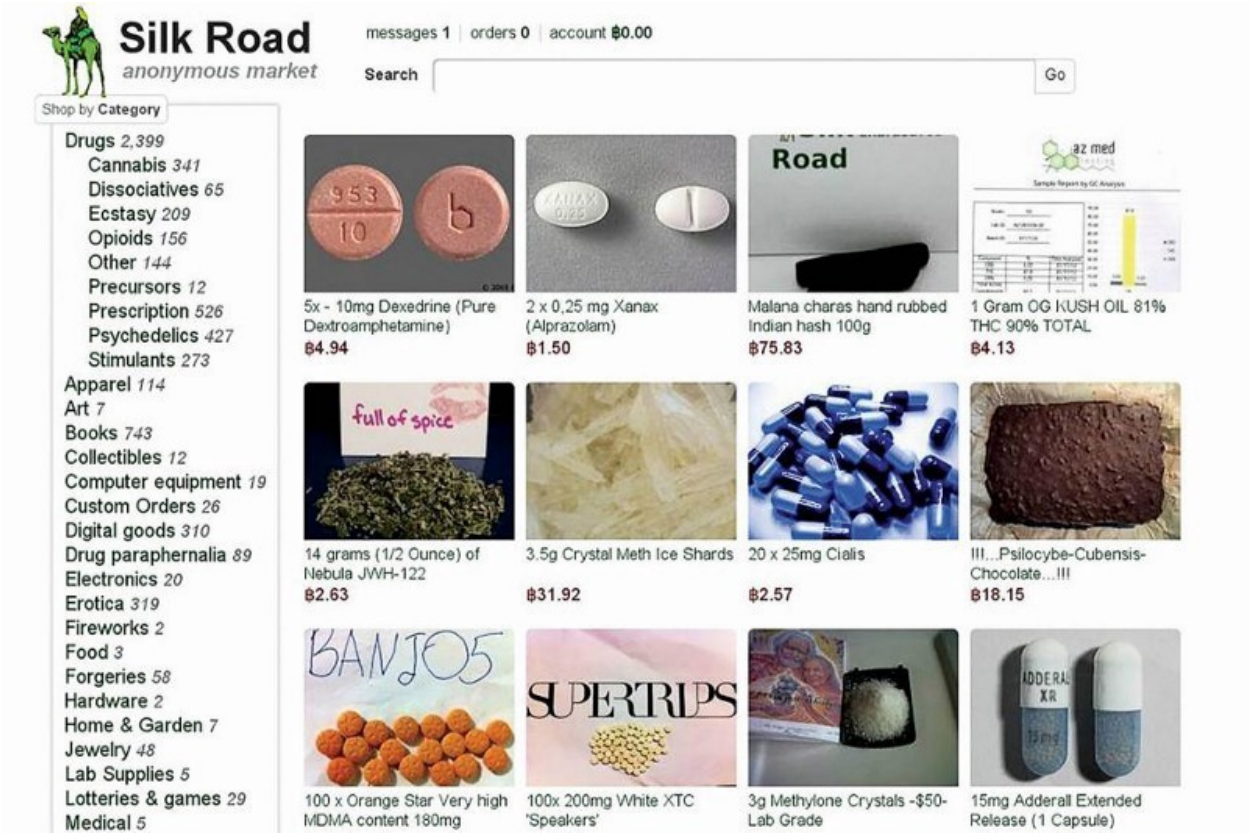


Abbildung 3: Screenshot von Silk Road (Nimfuehr, 2018)

Die Schließung von Silk Road und die Verhaftung von Ross William Ulbricht war jedoch nicht die erste oder letzte Tat, welche im Sinne der Minimierung illegaler Aktivitäten des Deep Web vorgenommen wurde.

Um die dichten Schichten der von TOR angebotenen Anonymität zu durchdringen, nutzte das FBI eine leistungsstarke Anwendung namens Metasploit in "Operation Torpedo", einer Aktion von 2012 gegen die Nutzer von drei kinderpornografischen Webseiten im Darknet. Des Weiteren beteiligte sich das FBI im Jahr 2014 an einem weltweiten Projekt mit dem Codenamen "Operation Onymous", wobei durch den Einsatz von Hacking und Malware, welche im Darknet häufig angewendet werden, illegale Aktivitäten entdeckt wurden. Der Einsatz dieser Hacking-Techniken zur Untersuchung von Deep Web sowie Darknet bringt zahlreiche rechtliche und ethische Herausforderungen mit sich. Leider ist die Unterscheidung zwischen legalen und illegalen Aktivitäten nicht gleich ersichtlich. Die Untersuchung riskiert, das Falsche zu tun, indem die Verfolgung legitimer Forschungsprojekte durchgeführt wird (Sui, Caverlee, & Rudesill, 2015).

Die österreichische Polizei startete im Jahre 2015 das Projekt „Joint investigation to combat drug trafficking via the virtual market Darknet within and also into the EU“, um kriminelles Handeln in Bezug auf Kauf und Verkauf von Drogen im Internet zu untersuchen und Maßnahmen zur Minimierung der Kriminalität zu definieren. Die Ergebnisse dieses Projekts mündeten in das seit 2017 existierende Projekt „Drug Policing – Schwerpunkt Westbalkan und Darknet“. Hier werden die gewonnenen *„Erkenntnisse und ausgebauten Netzwerke genützt, um die Kriminalitätsentwicklung beider Schwerpunkte zu bekämpfen“* (Bundeskriminalamt, 2017).

Behörden, Organisationen und Regierungen bemühen sich also darum, jene Nutzer des Darknets zu stoppen, deren Aktivitäten zum großen Problem für die Regierung und Öffentlichkeit werden: Hacker, Drogenhändler, Auftragskiller, Zuhälter, Menschenhändler, Kinderpornographen, Geldwäscher, Identitätsdiebe, politische Extremisten, Spione sowie Terroristen (Sui, Caverlee, & Rudesill, 2015).

Eine nähere Betrachtung von Tabelle 2 gibt eine klare Übersicht über häufig vorkommende illegale Inhalte und Taten der bereits genannten Strafakteure im Deep Web:

Illegales Produkt	Illegale Aktivität
Gefälschtes Geld	Dark Web agiert als Vertreiber von gefälschtem Geld, das mit einer Garantie die Standardprüfungen mit ultraviolettem Licht erfolgreich zu bestehen, verkauft wird. Dieses Geld in den Umlauf zu bringen ist strafbar (Dange, Malkan, & Jha, 2018)
Gefälschte Dokumente	Es werden gefälschte Pässe, Einwanderungspapiere, Führerscheine und andere Ausweisdokumente für jedes Land der Welt bereitgestellt. Sowohl das Vertreiben als auch das Erwerben dieser Dokumente ist strafbar (Ciancaglini, Balduzzi, McArdle, & Rösler, 2015).
Drogen	Verschiedene Arten von illegalen Drogen können im Dark Web erworben werden. Auch hier zählen der Kauf sowie Verkauf zu strafbaren Taten (Ciancaglini, Balduzzi, McArdle, & Rösler, 2015).
Gestohlene sensible Informationen	Als illegale Taten gelten der Kauf und Verkauf von gestohlenen Kreditkartendaten, Bankkontodaten und sogar persönliche Informationen wie Sozialversicherungsnummern (Bedi, Gupta, & Jindal, 2020)
Hackerangriffe	Hacker erwerben im Darknet gefährliche Malware. Außerdem können Hacker für einen Angriff gegen Individuen, Organisation und sogar Regierungen gekauft werden, wodurch eine Straftat begangen wird (Spalevic & Ilic, 2017).
Waffen und Munition	Der käufliche Erwerb von illegalen Waffen und Munition ist an sich schon strafbar. Verkäufer im Darknet garantieren, dass die verlangten Waren dem Käufer in einer speziellen Verpackung geliefert werden, die jede Art von Scan- und Sicherheitskontrollen durchlaufen (Dange, Malkan, & Jha, 2018).
Auftragsmörder	Im Darknet können auch Auftragskiller angeheuert werden. Dies ist, so wie außerhalb von Darknet auch, eine strafbare Tat. Die Kosten hängen von der Art des Mordes sowie vom sozialen Status des Opfers ab (Spalevic & Ilic, 2017).
Handel mit menschlichen Organen	Im Darknet können zahlreiche Produkte erworben werden, unter anderem auch menschliche Organe. Diese Art von Kaufaktionen ist illegal und kann zur Strafverfolgung führen (Spalevic & Ilic, 2017).
Terroristische Aktivitäten	Terroristen nutzen Darknet zur versteckten, sicheren Kommunikation und Propaganda sowie für das Anwerben und Trainieren von Rekruten (Sui, Caverlee, & Rudesill, 2015), (Weimann, 2018)
Kinderpornographie	Das Darknet wurde auch dafür bekannt, viele kinderpornografische Inhalte zu hosten. Aber nicht nur das Hosten dieser Seiten, sondern auch deren Besuch zählen zu illegalen Aktivitäten (Sui, Caverlee, & Rudesill, 2015).

Tabelle 2: Illegale Aktivitäten im Darknet (Bedi, Gupta, & Jindal, 2020)

Was sowohl aus der Mitverfolgung des „Silk Road“-Vorfalls als auch aus der Analyse der illegalen Inhalte und Aktivitäten ersichtlich wurde, ist der Fakt, dass vor allem Darknet-Märkte schon von der Natur aus ein perfektes Beispiel für illegales Handeln und das Umgehen von Vorschriften darstellen. Sie ziehen die Aufmerksamkeit illegaler Akteure auf sich, indem sie die Identitäten von Personen verbergen, welche an Transaktionen beteiligt sind und häufig Geschäfte über Bitcoin abwickeln. Eine massive Anzahl von Darknet-Transaktionen steht außerdem in Verbindung zur Schmuggelware. Selbst dort, wo ansonsten legitime Waren und Dienstleistungen angeboten werden, verkörpern Darknet Transaktionen eine Reihe von Verbrechen, Steuerhinterziehung bis hin zur Umgehung von Import- und Exportbeschränkungen (Sui, Caverlee, & Rudesill, 2015).

Trotz verstärkter Bemühungen der Strafverfolgungsbehörden um die Sabotage und Sperrung zahlreicher Bereiche der Darknet-Märkte hat sich die Darknet-Wirtschaft als widerstandsfähig erwiesen. Der Markt erholt sich nach einer Schließung oder einer Verhaftung immer wieder. Einen adäquaten Ersatz für Marktführer wie Silk Road zu finden kann einige Zeit in Anspruch nehmen. Ein temporärer Ersatz erscheint jedoch fast sofort, da konkurrierende Foren ständig um Marktanteile kämpfen. Dennoch verbessert sich die Strafverfolgung aus einer breiten Reihe von Gründen. Immer mehr Personen sind technologisch affin, verdächtige Akteure nehmen größere Ziele ins Visier und bekommen somit mehr Aufmerksamkeit. Außerdem schließen zunehmend mehr Verbrechen eine digitale Komponente mit ein, wodurch sie der Strafverfolgung das Ziel einfacher gestalten, Kriminalität im Cyberspace zu entdecken (Ablon, Libicki, & Golay, 2014).

4 NUTZUNGSMÖGLICHKEITEN DES DARKNETS

Es gibt eine breite Skala an Anwendungsmöglichkeiten, welche einen Vorteil aus der Anonymität, die das Darknet bietet, ziehen. Um jedoch den wahren Nutzen von Darknet passabel bewerten und darstellen zu können, müssen zuerst die Potenziale und Risiken dieses Netzwerks näher betrachtet werden. Die Chancen, welche dieses Web mit sich bringt, sollen ausgenutzt werden, zur Eindämmung und Vermeidung unnötiger Risiken müssen Vorsichtsmaßnahmen vorgenommen werden.

4.1 Potenziale und Risiken von Darknet

Die Beliebtheit und dazu eng stehende Berühmtheit vom Darknet steigen stets. Denn während für viele der Begriff vor einigen Jahren noch unbekannt war, hat heutzutage die Aufmerksamkeit, welche diesem Webzugang gewidmet wird, ein bemerkenswertes Maß angenommen. Um jedoch diese Entwicklungen besser verstehen zu können, müssen die Potenziale sowie Risiken, welche Darknet mit sich bringt, näher untersucht werden.

4.1.1 Potenziale von Darknet

Der wohl größte Vorteil, welchen Darknet bietet, ist die vollkommene Anonymität der Nutzer. Somit kann im Internet recherchiert werden, ohne dabei Bedenken zu haben, dass die eigene Privatsphäre verletzt wird. Dieser Schleier der Anonymität verleiht den Nutzern auch ein gewisses Maß an Mut, so dass beispielsweise auch introvertierte User das Selbstvertrauen finden, um mit anderen Personen auf sozialen Netzwerken online zu interagieren (Iva, 2019).

Außerdem handelt es sich um ein Medium, welches Meinungsäußerung, Organisation und Informationsfluss für diejenigen anbietet, die unter repressiven oder restriktiven Regierungen leben. Somit können mit Darknet, trotz anderweitigen Vorgaben der Regierung, diverse Kommunikationskanäle frei genutzt werden. Es gibt sogar ein dediziertes soziales Netzwerk, welches von TOR zur Verfügung gestellt wird. Der große Vorteil hierbei ist die Interaktion von Menschen, welche sich in der gleichen prekären Lage befinden und hier eine Möglichkeit der Organisation von Protesten oder zur einfachen Meinungsäußerung finden. So wird auch zum Beispiel in China, wo soziale Netzwerke so gut wie verboten sind, Darknet zur Verwendung von Facebook eingesetzt, um somit die Restriktionen der Regierung zu umgehen. Die Anonymität des Darknets bietet somit die Redefreiheit, um die eigene Meinung ohne Angst vor Bestrafung oder Verfolgung frei äußern zu können (Quinney, 2016). Das soziale Netzwerk „Facebook“ hat sogar eine eigene Darknet-Version veröffentlicht, um der Internetzensur in zahlreichen Ländern entgegenzuwirken. Damit soll sichergestellt werden, dass die Menschenrechte von Bewohnern solcher Gebiete unverletzt bleiben, hierbei im Detail die gesicherte Meinungsfreiheit (Iva, 2019).

Des Weiteren bringt das Darknet die Möglichkeit mit sich, ein breites Spektrum an politischen und wissenschaftlichen Ressourcen analysieren und durchforschen zu können. Der bedeutende

Vorteil hierbei besteht darin, dass diese Quellen ungefiltert und unzensiert sind. Somit kann jeder Nutzer an politischen Diskussionen, wissenschaftlichen Manuskripten und Forschungsergebnisse teilhaben und die eigentliche Information ohne jegliche Filterung nutzen.

Werden Transaktionen im Darknet abgewickelt, dann auch mit der entsprechenden Währung. Zahlungen gehören zum nächsten Vorteil des Dunklen Webs, da diese über Bitcoin anonym durchgeführt werden. Somit ist nicht nur die Anonymität der Person gewährleistet, sondern auch die Sicherheit, da keine sensiblen Kontodaten angegeben werden müssen, um den Einkauf/Verkauf erfolgreich abzuschließen (Iva, 2019).

Trotz zahlreicher Vorteile, die das Darknet bietet, gibt es einen sehr guten Grund, warum dieses Web mit Vorsicht zu genießen ist, und zwar die breite Skala an Nachteilen, welche bei der Nutzung vom Darknet in Kauf genommen werden müssen.

4.1.2 Risiken von Darknet

Die vom Darknet gewährleistete Anonymität bringt zwar zahlreiche Vorteile mit sich, zeigt jedoch auch eine Schattenseite. Der Deckmantel der Anonymität verleitet sehr schnell zu illegalen Aktivitäten. So ist auch gemessen worden, dass etwa 60% der Inhalte von diesem Web eine illegale Basis aufweisen (vgl. Abbildung 4). Werden Nutzer öfters mit illegalen Inhalten konfrontiert, neigen sie leichter dazu, in diese aktiv oder passiv verwickelt zu werden (Iva, 2019).

Abbildung 4: Nutzung von Darknet (Eckermann, 2017)

So ermöglicht das Darknet einen größtenteils problemlosen Zugang zu illegalen Seiten und teils sehr diffamierenden Inhalten. Neben pornografischen Seiten können auch Auftragsmörder sowie hausgemachte, instabile Gifte, wie Drogen oder Medikamente, gefunden werden. Die Anonymität der Nutzer macht es jedoch schwierig, die Besitzer und Verteiler solcher Inhalte zu finden und somit die Aktivitäten zu unterbinden. Es würde wiederum gegen die Natur des Darknets sprechen, sollten solche Akteure problemlos aufgespürt werden können (Iva, 2019).

Des Weiteren gibt es eine breite Skala an Vorsichtsmaßnahmen, die vorgenommen werden müssen, bevor das Darknet überhaupt betreten wird. Der Grund hierfür ist das fehlende Vertrauen bzw. die Regulierung, welche sonst beispielsweise beim Surface Web gegeben ist. Jeder Nutzer des Darknets muss sich einerseits vor IP-Leaks schützen, andererseits muss die verwendete Hardware gegen Angriffe von schädlicher Malware geschützt werden. Im Falle eines IP-Leaks lässt sich die aktuelle IP-Adresse des Nutzers bestimmen, obwohl dieser mit einem VPN

verbunden ist. Es wird allgemein empfohlen, eine Linux-basierte virtuelle Maschine (VM) zu verwenden, da Linux weniger anfällig ist als andere Betriebssysteme. Es wird empfohlen, diese VM mit einem VPN auszustatten, um die vollkommene Anonymität sicherzustellen (Iva, 2019).

Es sind jedoch nicht nur die Sicherheitslücken, welche Darknet zu einem wenig vertrauenswürdigen Kanal formen, sondern auch diverse Formen von Betrügen. Insbesondere E-Commerce-Betrüge finden ihre Opfer unter den Nutzern des „Dunklen Netzes“. Nachdem es einfach ist, die eigene Identität zu verschleiern, kommen Betrüger sehr leicht davon. Diesen auch noch vor der Kaufaktion zu enttarnen ist daher auch keine besonders leichte Aufgabe. Eine Rückerstattung des Kaufpreises ist im Darknet im Normalfall nicht möglich (Iva, 2019).

Ein weiteres gravierendes Problem stellen die kryptischen Links dar, welche im Darknet vorzufinden sind. Diese Links sind URLs, welche keinerlei Einsicht über den Inhalt der Webseite geben. Aus diesem Grund muss beim Recherchieren im Darknet besonders vorsichtig vorgegangen werden. Es ist sehr wahrscheinlich, dass ein User auf einer unerwünschten Site landet, da der angeklickte Link nicht eindeutig ist. Groß ist auch die Wahrscheinlichkeit, sich im Darknet strafbar zu machen, da sogar die Nutzung von manchen Webseiten als illegal angesehen wird (Iva, 2019).

Trotz der zahlreichen Risiken steigt jedoch die Häufigkeit des Einsatzes von Darknet exponentiell. Doch was genau sind die Nutzungsmöglichkeiten dieses Netzwerkes? Welche Einsatzbereiche machen das Darknet so attraktiv und so nützlich?

4.2 Inhalte und Handlungsmöglichkeiten im Darknet

Es gibt eine Vielzahl an Gründen, warum Internetnutzer in spezifischen Situationen anonym bleiben möchten und Webseiten besuchen oder gar einrichten, die nicht auf einen physischen Ort oder auf eine reale Person zurückgeführt werden können (vgl. Abbildung 5).

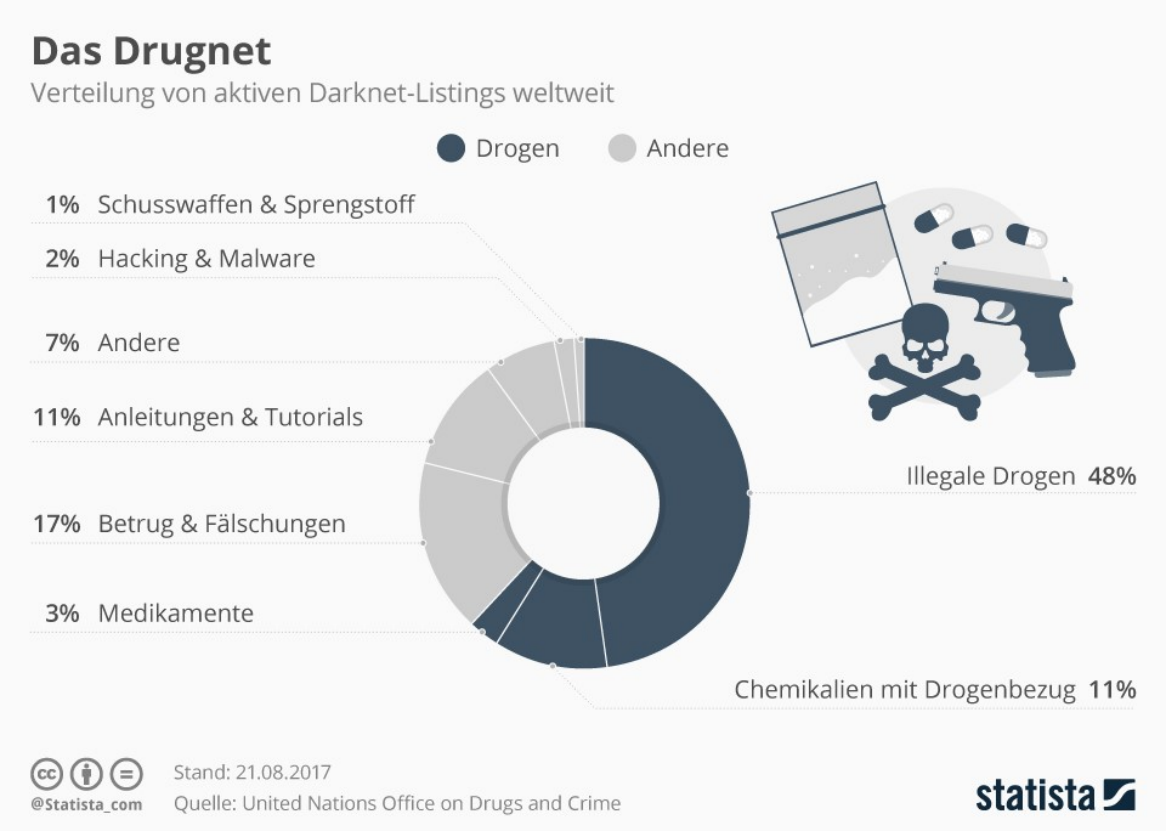


Abbildung 5: Verteilung aktiver Darknet-Listings weltweit (Brandt, 2018)

User, die Ihre Kommunikation vor staatlicher Überwachung abschirmen möchten, nutzen die Möglichkeiten der Tarnung durch das Darknet. Whistleblower können gefährliche, jedoch äußerst wichtige Informationen an Journalisten vertreiben, ohne eine auf sie zurückführende Spur zu hinterlassen. Der Bevölkerung in restriktiven Regimen wird ermöglicht, die Welt zu informieren, was in ihrem Land tatsächlich hinter den Kulissen passiert, ohne eine Strafverfolgung zu riskieren (Balduzzi & Ciancaglini, 2015).

Das Darknet und seine Dienste sind jedoch mit Vorsicht zu genießen. Es bietet den Nutzer zwar ein gewisses Maß an Anonymität, diese ist jedoch nicht stets gegeben, denn

> *„es gibt Seiten, die im TOR-Netzwerk feste .onion-Adressen haben, wie z.B. Facebook und die New York Times. Illegale Angebote wie Drogenmarktplätze ändern zwar ihre Adressen, sind aber darauf angewiesen gefunden zu werden“ (Avarikioti, Brunner, Kiayias, Wattenhofer, & Zindros, 2018).*

Außerdem kann die gegebene Anonymität leicht missbraucht werden, wie beispielsweise bei Usern, die ein Attentat gegen ein öffentlichkeitswirksames Ziel planen. Diese können dank Darknet deren Aktion gemeinsam organisieren, ohne zurückverfolgt werden zu können. Andere illegalen Dienstleistungen, wie zum Beispiel der Verkauf von Dokumenten oder gar Identitäten, werden unter dem Schirm des Darknets abgewickelt. Dasselbe gilt für Personen, die illegale Güter wie Drogen oder Medikamente anbieten (Balduzzi & Ciancaglini, 2015).

4.2.1 Drogenhandel

Die zunehmende Digitalisierung des alltäglichen Lebens, welche durch eine wachsende Verbreitung von Mobiltelefonen beschleunigt wurde, wandelte den Großteil des Drogenhandels von offenen in geschlossene Märkte um. So agierten gewisse Verkäufer nur noch mit Interessenten, welche sie persönlich kannten oder welche ihnen von vertrauenswürdigen Kontaktpersonen weitergeleitet wurden. Heutzutage bietet das Darknet solchen Verkäufern die Möglichkeit, einen offenen und freien, jedoch sicheren Markt zu leiten mit vielen für sie akkreditierten Interessenten (Aldridge & Décary-Hétu, 2016).

Der Drogenhandel findet im Darknet sowohl über größere Anbieter mit einem umfangreichen Angebot wie auch über Einzelhändler, welche sich auf bestimmte Produkte spezialisieren, statt. Ein wichtiger Vorteil dieser neuen Märkte liegt für die Verkäufer auch in der lokalen Unabhängigkeit der Geschäfte. Weder der Bewegungsradius des Verkäufers noch die exakt abgesteckten Geschäftsgebiete konkurrierender Verkäufer schränken den Handel der Darknet-Märkte ein. Außerdem werden weder der Händler noch der Käufer dem Risiko einer körperlichen Auseinandersetzung ausgesetzt, welches im Rahmen einer persönlichen Transaktion gegeben ist. (Soska & Christin, 2015).

Wie in Abbildung 6 dargestellt, bringen illegale Drogen für Darknet-Märkte den größten Gewinn. Es wurden Verkaufsproben von Silk Road 2, Evolution und Agora, berühmten Handlungsplattformen im Darknet, untersucht und mehr als die Hälfte des Gewinns (83%) stammt dabei von illegalen Drogen, 14% von legalen Drogen bzw. Medikamenten und die restlichen 2% von anderen Produkten, welche keinen Bezug zu Drogen haben.

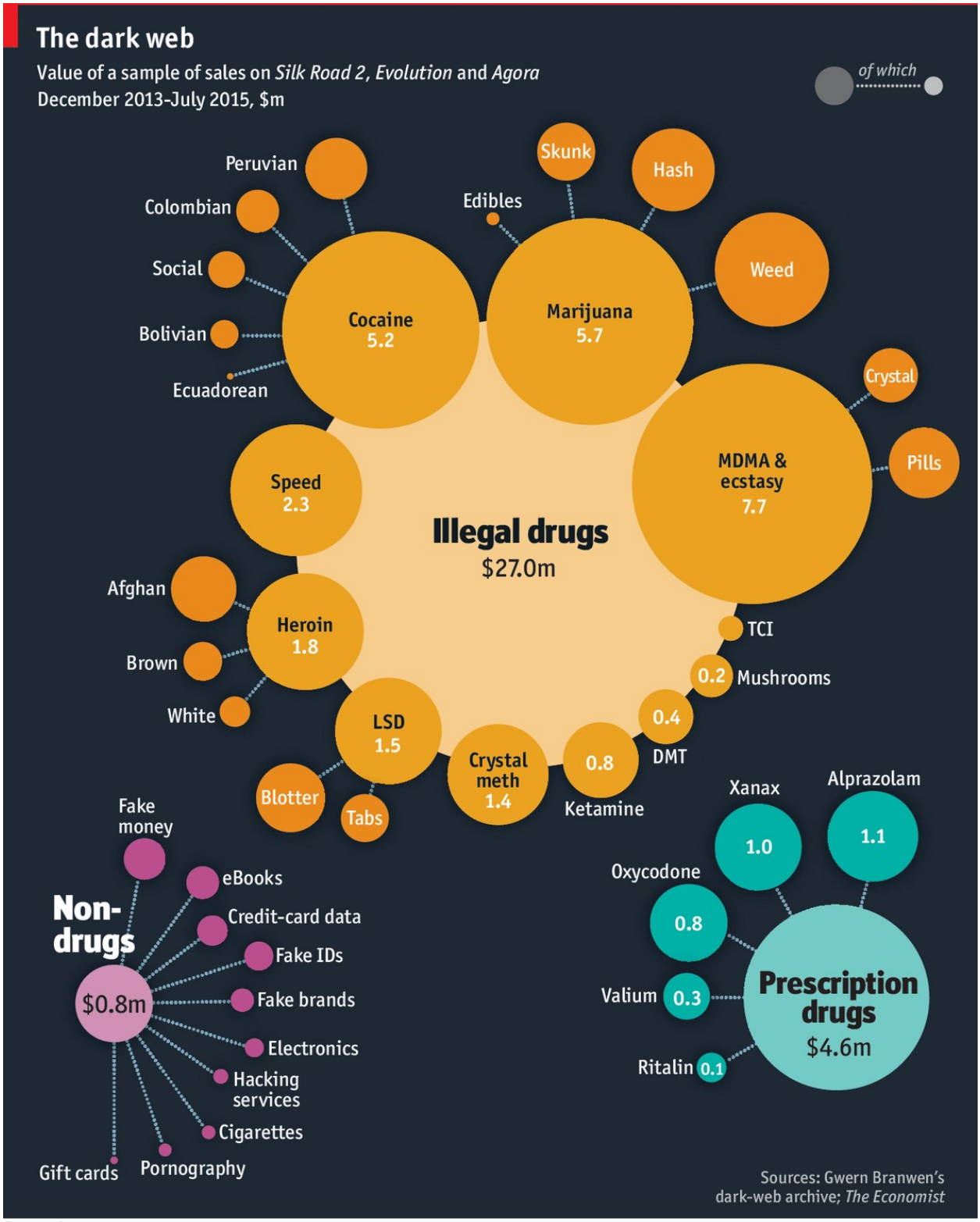


Abbildung 6: Drogenhandel im Darknet (Branwen, 2016)

Eine gemeinsam von der EMCDDA und Europol durchgeführte Darknet-Studie ergab, dass bis August 2017 mehr als 60% aller Leistungen auf fünf großen Darknet-Märkten weltweit mit dem illegalen Verkauf von Drogen, einschließlich drogenbezogener Chemikalien und Pharmazeutika,

in Verbindung standen (European Monitoring Centre for Drugs and Drug Addiction; Europol, 2017).

Allein der illegale Verkauf von Drogen machte fast die Hälfte aller solchen Angeboten aus. Interessenten, welche Drogen über das Darknet kaufen wollen, greifen typischerweise über den "Onion Router" (TOR) darauf zu, um sicherzustellen, dass ihre wahre Identität verborgen bleibt. Die Verwendung von für das Darknet spezialisierten Explorern ermöglicht die Navigation der Klientel auf erwünschte Marktplattformen, wo die erlangten Produkte typischerweise mit Kryptowährung wie Bitcoins erworben werden können (Horton-Eddison & Di Cristofaro, 2017).

Verdiente Bitcoins können wiederum für den Kauf anderer Waren und Dienstleistungen eingesetzt oder in verschiedene Landeswährungen umgetauscht werden. Die Zustellung der auf diesen Marktplätzen gekauften Drogen erfolgt in der Regel durch öffentliche oder private Postdienste, wobei Pakete oft an anonyme Postfächer, insbesondere an automatisierte "Packstationen", zur Selbstabholung geschickt werden (World Customs Organization, 2016).

Der Hauptvorteil für Anbieter und Kunden ist die Anonymität der Transaktion, da sie keinen physischen Kontakt erfordert. Der Handel im Darknet überwindet auch die Herausforderung, dass sich Anbieter und Kunden am selben Ort befinden müssen. Auch in solchen Fällen profitieren Kunden von den Rückmeldungen anderer Kunden über die Qualität der verkauften Produkte und über die Zuverlässigkeit des Anbieters. Darknet-Plattformen garantieren auch die Bezahlung der verkauften Waren, indem sie typischerweise Treuhandkontosysteme nutzen, die eine sofortige Zahlung für die bestellten Waren verlangen. Die endgültige Zahlung erfolgt erst dann, wenn die bestellten Waren tatsächlich beim Kunden eingetroffen sind und den Erwartungen entsprechen (Horton-Eddison & Di Cristofaro, 2017).

Ein analoger Erwerb wird dennoch häufig auch als einfacher in seiner Ausführung angesehen, da beispielsweise kein Erwerb von Kryptowährungen oder eine kompliziertere Geschäftsabwicklung notwendig sind. Je nach Art der angebotenen Drogen dürfte auch das jeweilige Konsumverhalten Auswirkungen auf die Attraktivität des Darknets als Erwerbsort haben, da aufgrund der Zustellung ein gewisser zeitlicher Rahmen zwischen dem Erwerb und dem Erhalt der Ware einzukalkulieren ist (Aldridge & Décary-Hétu, 2016).

Eine besonders relevante Bezugsquelle dürfte das Darknet daher besonders für solche Konsumenten darstellen, die über keine oder nur unzulängliche Kontakte zu analogen Händlern verfügen. Weiterhin ist davon auszugehen, dass besonders im Bereich des Drogenhandels das Darknet nicht nur von Endverbrauchern genutzt wird, sondern dass auch analoge Händler über diese Plattformen Waren zum Weiterverkauf erwerben. In solchen Fällen können jedoch nur Vermutungen getätigt werden, welche sich beispielsweise an der Höhe der getätigten Einkäufe orientieren. Eine wesentliche Rolle dürfte das Darknet für den internationalen Drogenhandel spielen. Welche Auswirkungen dieses Phänomen auf die Drogenmärkte im Allgemeinen hat, dürfte wesentlich von der jeweiligen Produktart abhängen. Während für Drogen, welche aus Ländern mit einem niedrigen technologischen Entwicklungsstand stammen (beispielsweise afghanisches Heroin) auch weiterhin klassische Versorgungswege die Regel darstellen dürften, kann das Darknet für andere Betäubungsmittel eine wichtige Verbindung zwischen Ländern, in

denen diese preiswert hergestellt oder legal erworben werden können, und den letztendlichen Endverbrauchern darstellen (Aldridge & Décary-Hétu, 2016).

Darknet-Märkte sind seit 2010 in Betrieb, obwohl sie erst seit der Einführung der Handelsplattform Silk Road im Februar 2011 tatsächlich an Bedeutung gewonnen haben. Sie bestehen aus Websites, die als Handelsplattformen genutzt werden, ähnlich wie legale Handelsplattformen im öffentlichen World Wide Web, dem Surface Web, die für den Erwerb legaler Waren und Dienstleistungen genutzt werden (European Monitoring Centre for Drugs and Drug Addiction; Europol, 2017).

Die Illegalität vieler Darknet-Transaktionen bedeutet jedoch, dass es signifikante Unterschiede zwischen Darknet und Surface Web-Handelsplattformen gibt. Zu diesen Unterschieden gehören vor allem die Verwendung spezieller Währungen wie Bitcoin, Treuhandkonten und das schnelle Auftauchen und Verschwinden von Handelsplattformen, die oft direkt mit illegalen Geschäftspraktiken verbunden sind. Basierend auf einer detaillierten Analyse von EMCDDA und Europol von 103 Darknet-Marktplätzen, die im Zeitraum 2011-2017 weltweit tätig waren, bleiben Darknet-Märkte im Durchschnitt acht Monate aktiv, wobei die langlebigsten im Durchschnitt knapp vier Jahre und die meisten nicht länger als ein Jahr in Betrieb sind (European Monitoring Centre for Drugs and Drug Addiction; Europol, 2017).

Die EBDD und Europol analysierten auch die Gründe für die Schließung von 89 weltweit operierenden Marktplätzen im Zeitraum von 2010 bis Ende Juli 2017. Sie fanden heraus, dass "Exit Scams", bei denen die Betreiber ihre Seiten plötzlich schließen und das gesamte Geld auf Treuhandkonten transferieren, der häufigste Grund für die Schließung war. Solche Schließungen, welche keinen öffentlich bekannten Grund haben, fanden laut der Studie in 35 % der Fälle statt, gefolgt von freiwilligen Ausstiegen (27 %), Schließungen aufgrund von Strafverfolgungsmaßnahmen (17 %) und Hacking durch Dritte (12 %) (European Monitoring Centre for Drugs and Drug Addiction; Europol, 2017).

Auch wenn die Strafverfolgungsbehörden nicht für den Großteil der Schließungen von Handelsplattformen verantwortlich waren, so konnten die Behörden im Juli 2017 doch einen ihrer größten Erfolge mit der Zerschlagung der damals größten Drogenhandelsplattform AlphaBay im Rahmen der „Operation Bayonet“ verbuchen. Dieses Projekt wurde gemeinsam von den Vereinigten Staaten, Kanada, Thailand, den Niederlanden, Europol und verschiedenen anderen europäischen Polizeibehörden durchgeführt. AlphaBay hat während seiner Existenz 200.000 Nutzer und 40.000 Verkäufer erreicht (Europol, 2017).

Beispiele haben jedoch gezeigt, dass sowohl Anbieter als auch Kunden nach der Schließung eines Darknet-Marktes einfach auf die nächstgrößere Handelsplattform migrieren und ihren Betrieb weiterführen (United Nations, 2016).

4.2.2 Betrug und Fälschungen

Die Kryptowährung Bitcoin wurde mit dem Hauptfokus auf Anonymität entwickelt. Daher wird sie auch häufig für den Kauf illegaler Waren und Dienstleistungen verwendet. Während jedoch alle Bitcoin-Transaktionen anonym sind, so sind sie doch in komplettem Umfang öffentlich. Die

Tatsache, dass jede Transaktion in der Bitcoin-Blockchain öffentlich zugänglich ist, bedeutet, dass sie durch Ermittler investigiert werden können. Das Geld zu verfolgen, während es sich im Systemumlauf befinden, ist somit zwar möglich, jedoch trotzdem schwierig umzusetzen. Infolgedessen ist eine Vielzahl an Diensten entstanden, die dem System weitere Anonymität verleihen, wodurch die elektronische Währung noch schwieriger zu verfolgen ist. Dies wird im Allgemeinen dadurch erreicht, dass Bitcoins durch ein spinnenartiges Netzwerk von Mikrotransaktionen transferiert werden bevor sie endgültig an den Empfänger gelangen. Der Geldbetrag verändert sich im Rahmen dieses Prozesses zwar nicht, die Transaktionen sind jedoch wesentlich komplizierter zu verfolgen (Ciancaglini, Balduzzi, McArdle, & Rösler, 2015).

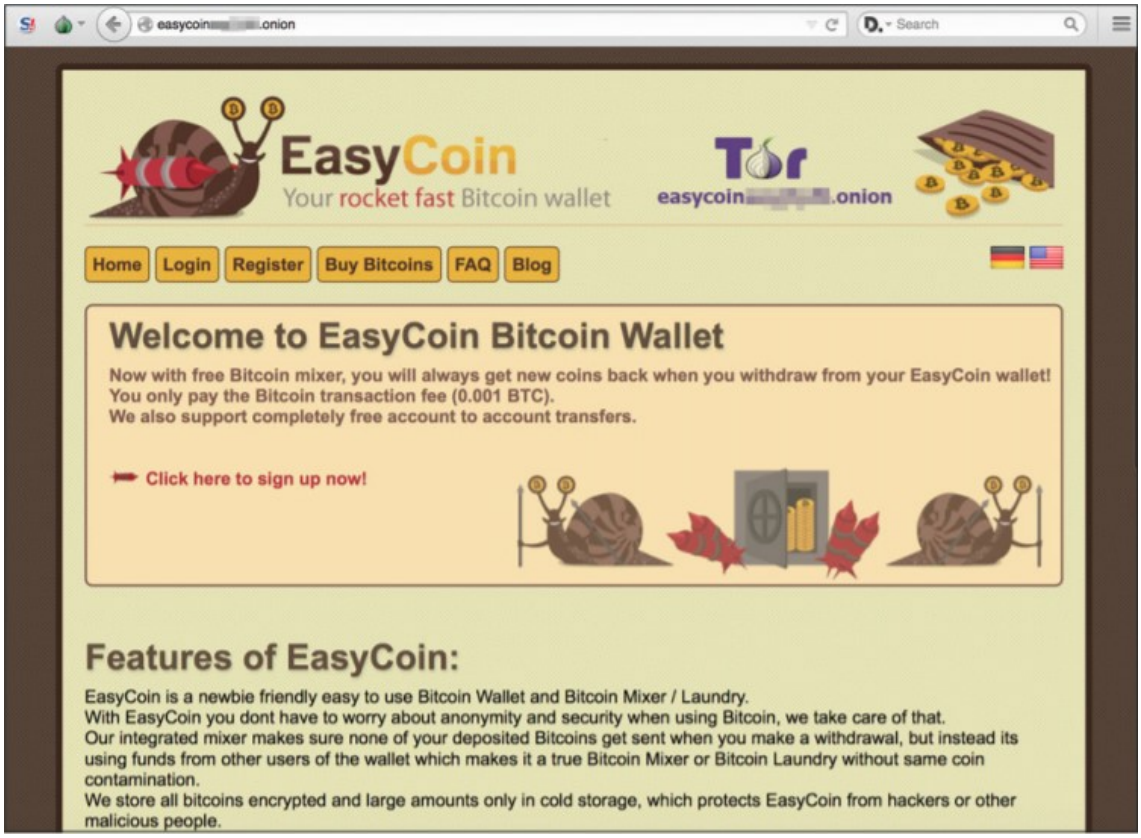


Abbildung 7: EasyCoin - Ein Beispiel für Bitcoin-Wäsche (Ciancaglini, Balduzzi, McArdle, & Rösler, 2015)

Bitcoin-Wäschedienste, wie beispielsweise in Abbildung 7 ersichtlich, helfen, die Anonymität des Geldtransfers im Bitcoin-System zu erhöhen. Letztendlich werden die meisten Bitcoin-Nutzer das Geld aus dem System abziehen wollen, um es in Bargeld oder in andere Arten von traditionellen Zahlungsmitteln umzuwandeln. Zu diesem Zweck existieren mehrere anonyme Dienste im Darknet. Diese ermöglichen es den Nutzern, Bitcoins gegen Geld, welches sogar direkt per Post verschickt wird, umzutauschen.

Seiten, wie zum Beispiel WeBuyBitcoins (vgl. Abbildung 8), tauschen echtes Bargeld gegen Bitcoins zu wettbewerbsfähigen Wechselkursen verglichen mit äquivalenten nicht-anonymen Diensten, die im Surface Web aktiv sind. Kriminelle Akteure, welche für potenziell größere Belohnungen ein höheres Risiko in Kauf nehmen würden, können eine Alternative nutzen - den Erwerb von Falschgeld mit Bitcoins (Ciancaglini, Balduzzi, McArdle, & Rösler, 2015).

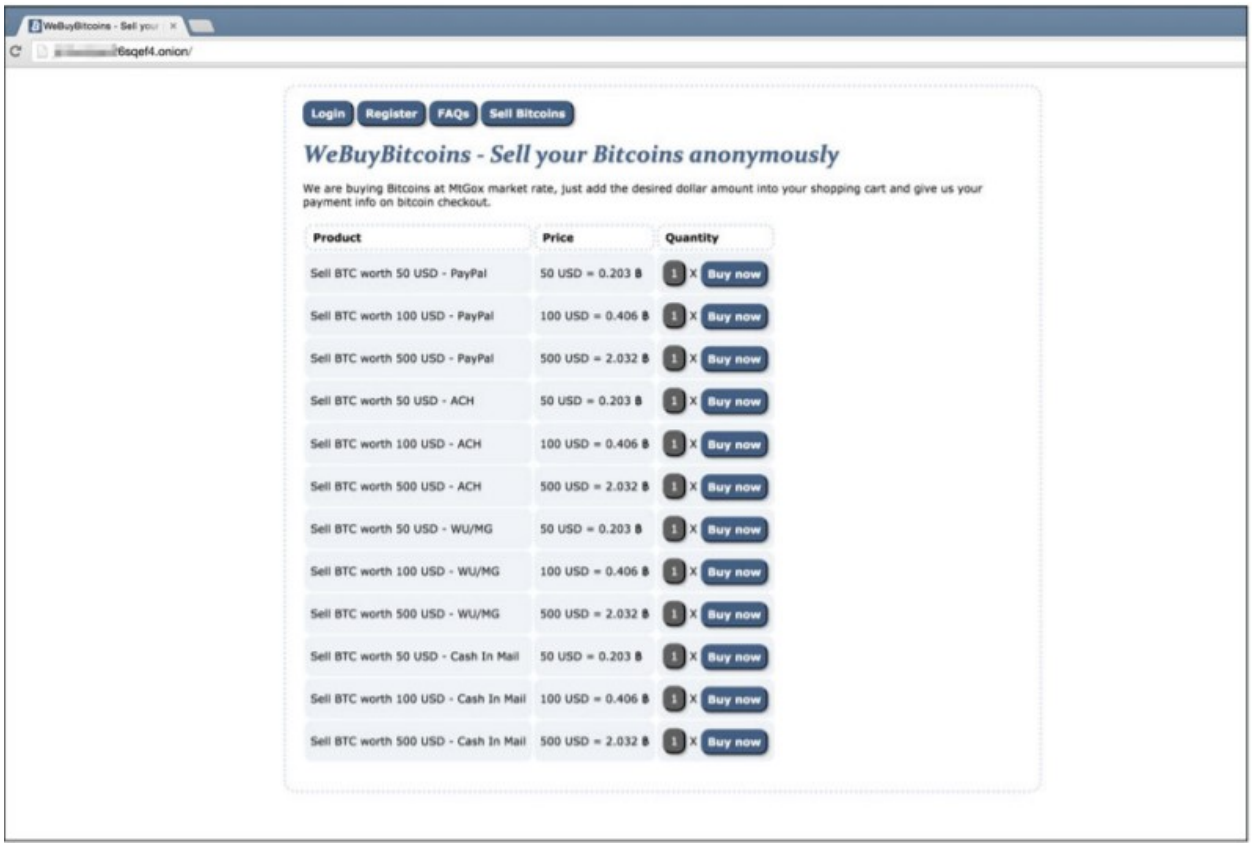


Abbildung 8: WeBuyBitcoins (Ciancaglini, Balduzzi, McArdle, & Rösler, 2015)

Beim Kauf und Verkauf von gestohlenen Konten im Darknet gehören Kreditkartennummern, Bankkontonummern und Anmeldedaten (wie in Abbildung 9) zu den am häufigsten verkauften Produkten. Wie im Surface Web sind die Preise auch im Darknet sehr unterschiedlich, für ausgereiftere Angebote werden in der Regel hohe Preise erzielt. Solche Konten werden in der Regel auf eine von zwei Arten verkauft. Hierbei handelt es sich entweder um hochwertige, verifizierte Konten mit einem genauen Kontostand oder aber um eine Massenware. Dieses Produkt umfasst eine bestimmte Anzahl nicht verifizierter Konten, die mit einer Garantie versehen sind, dass zumindest ein bestimmter Prozentsatz gültig ist. Die erste Kategorie gilt in der Regel als teurer, da sie mit einer größeren Wahrscheinlichkeit wirtschaftlichen Vorteil für einen Käufer bringt, während die zweite Kategorie deutlich günstiger ist. Ein Angebot, das im Deep Web besonders unkompliziert zu finden ist, sind reale, physische Kreditkarten (Ciancaglini, Balduzzi, McArdle, & Rösler, 2015).

Es gibt eine weitere Form der Klassifizierung von angebotenen, gestohlenen Dokumenten. Es wird unterschieden zwischen physischen Dokumenten und sogenannten „Scans“. Physische Dokumente sind gefälschte Pässe, die zum Verkauf angeboten werden. Die Verkäufer behaupten, dass die Dokumente von den Behörden als echt akzeptiert werden, da sie exakte Kopien und alle Sicherheitsmerkmale aufweisen. Scans sind nur eingescannte Kopien von echten Pässen, die für Identitätsbetrug verwendet werden. Das Risiko einer Enthüllung ist jedoch viel höher, da es sich in zahlreichen Fällen um kein akzeptables Dokument zur Identifizierung handelt (Baravalle, Lee, & Sanchez Lopez, 2016).

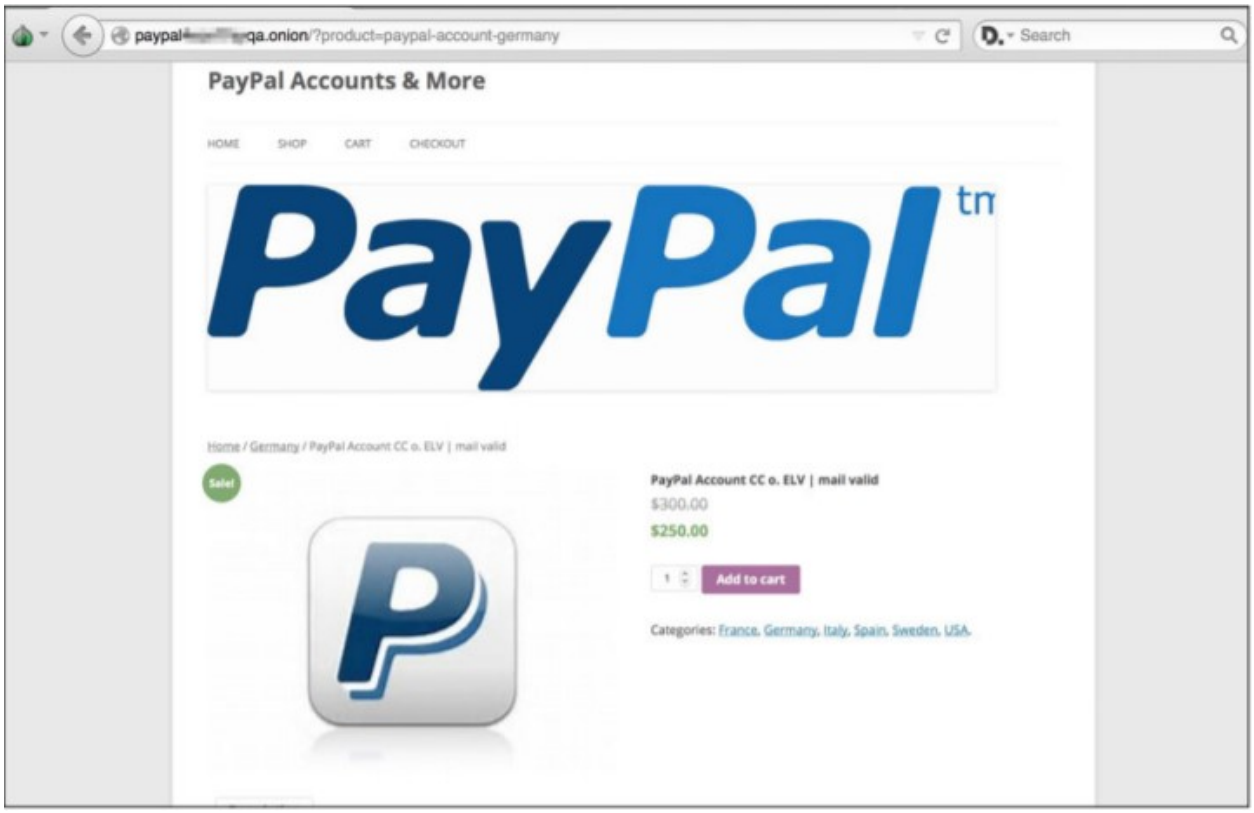
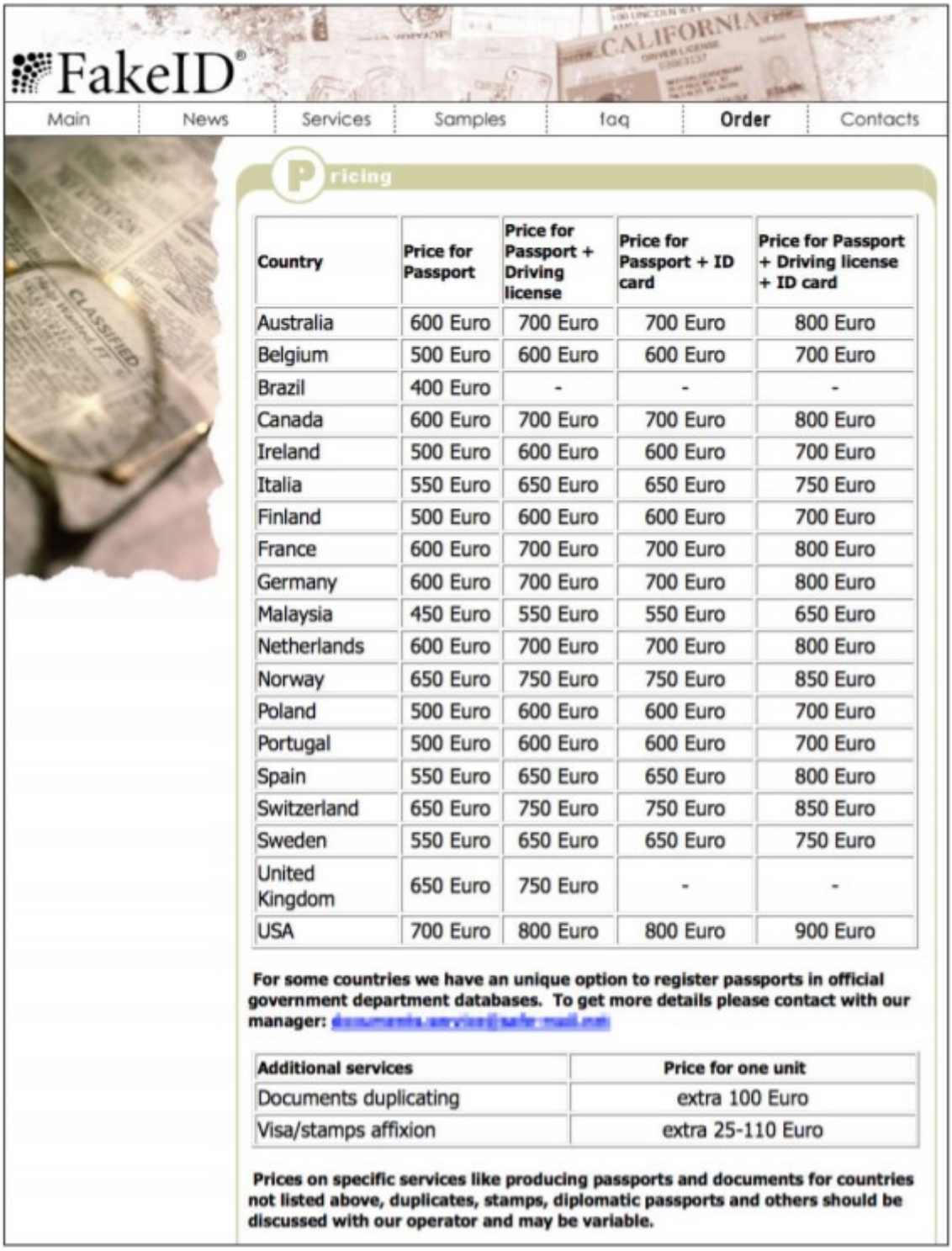


Abbildung 9: Kaufbarer PayPal Account (Ciancaglini, Balduzzi, McArdle, & Rösler, 2015)

Pässe und IDs sind einzigartige, sensible Dokumente. Sie dienen nicht nur als Ausweis für das Überschreiten von Grenzen (einschließlich solcher, die Käufer normalerweise nicht ohne Weiteres überqueren könnten), sondern quasi auch als Türöffner für ein breites Spektrum anderer lukrativer Tätigkeiten von der Eröffnung von Bankkonten über die Beantragung von Krediten bis hin zum Kauf von Immobilien und vieles mehr. Somit gelten sie im Darknet als besonders wertvoll und stark gefragt. Es gibt eine ganze Reihe von Seiten im Darknet, welche garantieren, Pässe und andere Formen von amtlichen Ausweisen zu verkaufen, und zwar zu Preisen, die von Land zu Land und von Verkäufer zu Verkäufer variieren (siehe Abbildung 10). Einen Nachteil bildet hierbei die Tatsache, dass die Überprüfung der Gültigkeit solcher Dokumente, ohne die Ware tatsächlich zu kaufen, praktisch unmöglich ist. Bei den entsprechenden Diensten kann es sich durchaus um einfachen Betrug handeln, der auf Interessenten abzielt, die eine Staatsbürgerschaft erhalten möchten, um in dem Land zu bleiben, in dem sie sich derzeit aufhalten (Ciancaglini, Balduzzi, McArdle, & Rösler, 2015).

Für potenzielle Kunde ist es jedoch nicht besonders leicht, gestohlene Dokumente zum Kauf zu finden, denn *„differently from the drugs market, the counterfeit documents market seems to be more concentrated – with less vendor operating in the niche”* (Baravalle, Lee, & Sanchez Lopez, 2016).



FakeID®

Main | News | Services | Samples | faq | **Order** | Contacts

Pricing

Country	Price for Passport	Price for Passport + Driving license	Price for Passport + ID card	Price for Passport + Driving license + ID card
Australia	600 Euro	700 Euro	700 Euro	800 Euro
Belgium	500 Euro	600 Euro	600 Euro	700 Euro
Brazil	400 Euro	-	-	-
Canada	600 Euro	700 Euro	700 Euro	800 Euro
Ireland	500 Euro	600 Euro	600 Euro	700 Euro
Italia	550 Euro	650 Euro	650 Euro	750 Euro
Finland	500 Euro	600 Euro	600 Euro	700 Euro
France	600 Euro	700 Euro	700 Euro	800 Euro
Germany	600 Euro	700 Euro	700 Euro	800 Euro
Malaysia	450 Euro	550 Euro	550 Euro	650 Euro
Netherlands	600 Euro	700 Euro	700 Euro	800 Euro
Norway	650 Euro	750 Euro	750 Euro	850 Euro
Poland	500 Euro	600 Euro	600 Euro	700 Euro
Portugal	500 Euro	600 Euro	600 Euro	700 Euro
Spain	550 Euro	650 Euro	650 Euro	800 Euro
Switzerland	650 Euro	750 Euro	750 Euro	850 Euro
Sweden	550 Euro	650 Euro	650 Euro	750 Euro
United Kingdom	650 Euro	750 Euro	-	-
USA	700 Euro	800 Euro	800 Euro	900 Euro

For some countries we have an unique option to register passports in official government department databases. To get more details please contact with our manager: [redacted]

Additional services	Price for one unit
Documents duplicating	extra 100 Euro
Visa/stamps affixion	extra 25-110 Euro

Prices on specific services like producing passports and documents for countries not listed above, duplicates, stamps, diplomatic passports and others should be discussed with our operator and may be variable.

Abbildung 10: Gefälschte Dokumente im Darknet (Ciancaglini, Balduzzi, McArdle, & Rösler, 2015)

Unter Hackern ist es typisch, dass sich Gruppen von Gleichgesinnten in lockeren oder engen Gruppen zusammenfinden. Aufgrund der Art der Aktivitäten, die sie durchführen, kommt es häufig zu Rivalitäten und Streitigkeiten zwischen konkurrierenden Gruppen. Wenn dies geschieht, ist es üblich, dass eine Gruppe versucht, die andere zu "doxen". Doxing beschreibt dabei das Ausforschen und Verbreiten der persönlichen Daten einer Person, was im Fall von Hackern einen Rivalen entlarvt und seine reale Identität mit seiner Online-Identität verknüpft. Die Mittel, um dies zu tun, variieren, aber sie kombinieren in zahlreichen Fällen den Zugriff auf öffentlich verfügbare

Daten auch über soziale Netzwerke und direktes Hacking (Ciancaglini, Balduzzi, McArdle, & Rösler, 2015).

Abbildung 11: Cloudnine - Dienst für geleakte Informationen (Ciancaglini, Balduzzi, McArdle, & Rösler, 2015)

Diese Bloßstellung privater Informationen ist jedoch keineswegs nur auf rivalisierende Hacker beschränkt. Es ist üblich, dass Hacker Unternehmen, Prominente und andere Personen des öffentlichen Lebens ins Visier nehmen. Die Bloßstellung eines Unternehmens kann sich natürlich nicht nur auf Hacker beschränken, sie kann auch von Insidern verursacht werden, wie im Fall von Wikileaks. Es ist sehr schwer zu bestimmen, ob diese Details den Tatsachen entsprechen. In zahlreichen Fällen enthalten die durchgesickerten Details sensible Informationen über Geburtsdaten, Sozialversicherungsnummern, persönliche E-Mail-Adressen, Telefonnummern oder private Adressen. Zum Beispiel ermöglicht die in Abbildung 11 dargestellte Seite namens „Cloudnine“ die Auflistung von Informationen über öffentliche Personen, welche FBI-Agenten, politische Persönlichkeiten sowie Berühmtheiten betreffen können (Ciancaglini, Balduzzi, McArdle, & Rösler, 2015).

4.2.3 Hacking und Malware

In vielerlei Hinsicht sind das Darknet und Malware perfekt füreinander geeignet insbesondere in Bezug auf das Hosten einer Command-and-Control (C&C)-Infrastruktur. Es liegt in der Natur von versteckten Diensten als auch Websites wie TOR oder I2P, den Standort von Servern mithilfe starker Kryptografie zu verbergen. Dies macht es im Wesentlichen unmöglich, mit traditionellen Mitteln wie der Untersuchung der IP-Adresse eines Servers die Überprüfung von Registrierungsdetails durchzuführen. Darüber hinaus ist die Nutzung dieser Websites und Dienste nicht besonders schwierig. Es ist daher nicht überraschend, dass eine Reihe von Cyberkriminellen TOR für C&C verwenden (Yaneza, 2014).

Die größte Herausforderung stellen die sogenannten „Hacker-Märkte“ dar. Diese Plattformen werden eingesetzt, um Malware und Hacker-Dienste käuflich zu erwerben. Sehr gefragt sind hier die sogenannten „Botnets“. Botnets wurden bereits am Anfang des 21. Jahrhunderts in vielen Fällen als grundliegendes Equipment für illegale Tätigkeiten eingesetzt. In der Zeitperiode 2003-2004 wurden sie überwiegend für das Spamming eingesetzt (vgl. Abbildung 12). Als Spamming werden unerwünschter Nachrichten bezeichnet, welche in den meisten Fällen über elektronische Kommunikationskanäle versendet werden. Im Jahre 2007 begannen sie mit dem Einsatz von P2P-Verbindungen, wodurch das Herunterfahren solcher Botnets immens erschwert wurde. Im Jahre 2010 kam es jedoch zu einem Umbruch. Botnets haben an Effektivität beim Spammen der Opfer verloren, da zunehmend Gegenmaßnahmen entwickelt wurden. Somit sind Botnets diesen Gegebenheiten angepasst und für DDoS-Attacken umdisponiert worden (Ablon, Libicki, & Golay, 2014).

> *„Botnets have grown substantially, and that growth has greatly enabled DDoS attacks. For example, a November 2005 DDoS attack against godaddy.com lasted only one hour; just over three years later godaddy.com sustained a DDoS attack that rendered its sites unavailable for 24 hours. This second attack could not have persisted for so long without the availability of significantly larger botnets (Namestnikov, 2009).”*

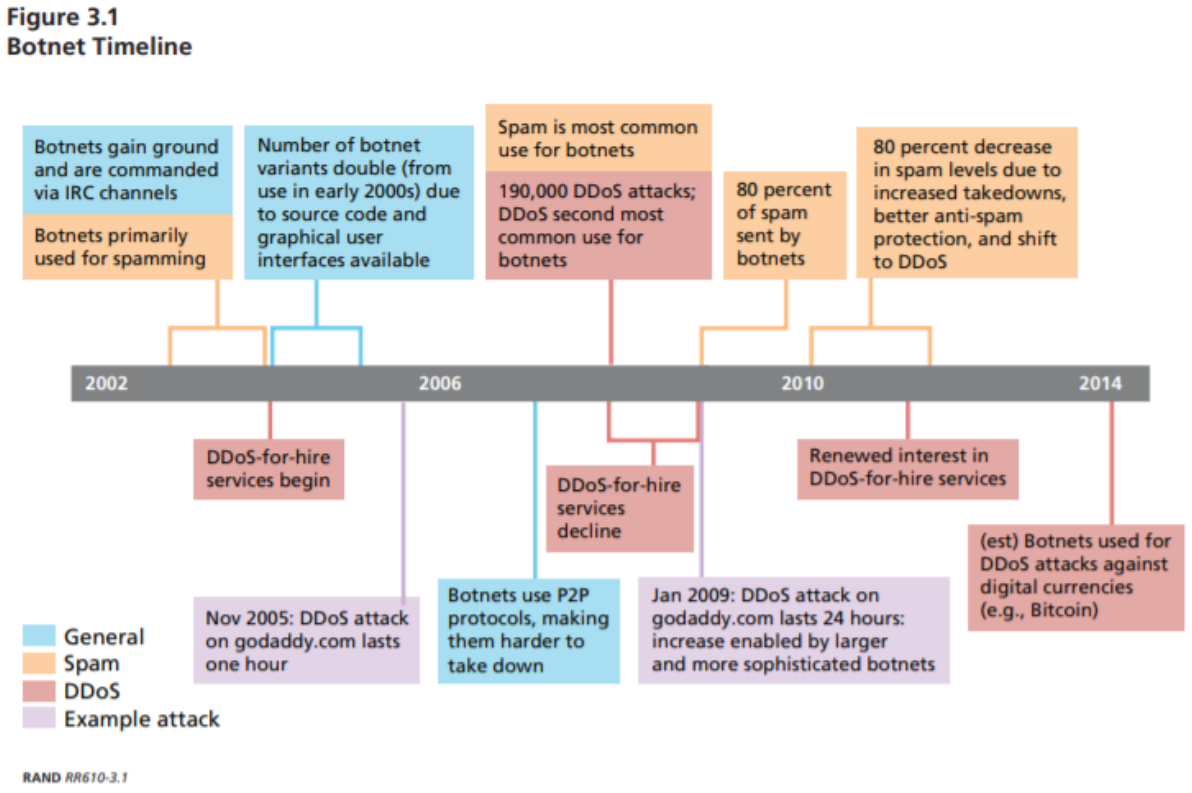


Abbildung 12: Lebenszyklus von Botnets (Ablon, Libicki, & Golay, 2014)

Größere Botnets haben zusätzlich auch das Knacken von Passwörtern optimiert, indem dieser Prozess schneller und einfacher gemacht wurde. So können Cyberkriminelle in wenigen Stunden Aufgaben erledigen, welche sonst Jahre in Anspruch genommen hätten. In den letzten Jahren haben Kriminelle begonnen, Botnet-Hosts als Proxys zu verwenden während sie mit gefälschten

Kreditkartendaten Einkäufe tätigen. Durch den Kauf mit einer IP-Adresse aus dem gleichen Gebiet, aus dem die gestohlene Kreditkarte stammt, entgehen die Käufer der Überprüfung, welche anhand vom Transaktionsprofil der Kreditkartenunternehmen durchgeführt wird. Das Mining digitaler Währungen ist zu einer weiteren beliebten Aufgabe der Botnets geworden. Der Zero-Access-Botnet, derzeit einer der größten bekannten Botnets, beschäftigt sich ausschließlich mit Bitcoin-Mining und Klickbetrügen (Ablon, Libicki, & Golay, 2014).

Auch Trojaner- und Virensoftware werden zusammen mit detaillierten Implementierungsanweisungen in zahlreichen Fällen über Darknet-Plattformen angeboten. Ein "Trojaner" ist eine Form von Malware, die den Betrieb von Computersystemen beeinträchtigt und wichtige Daten stiehlt. Außerdem kann ein Trojaner das System anfällig für die Einrichtung von Hintertüren und Fernzugriff machen. Ein "Virus" ist eine Form von Malware, die eine Benutzeraktivierung voraussetzt, um Zugriff auf Computersysteme zu erhalten. Einmal installiert, können Viren Prozesse manipulieren und die Systemfunktionalität beeinträchtigen. Trojaner sind, wie ihr historischer Namensvetter, begehrt, weil sie darauf ausgelegt sind, einen Computer oder Netzwerke zu umgehen und eine Hintertür für Angreifer zu schaffen oder eine Nutzlast wie einen Virus zu liefern. Diese sind von Angreifern erwünscht, da sie schwer zu erkennen und aufgrund ihrer Allgegenwärtigkeit schwer zuzuordnen sind. Aus diesem Grund lassen sich Angreifer nicht davon abhalten, diese Angriffsformen zu nutzen (Broadhurst, et al., 2018).

Zu der bekanntesten Malware, welche im Darknet zu finden ist, gehört auch VAWTRAK. Diese Malware sind Banking-Trojaner, die sich über Phishing-E-Mails verbreiten. Jedes Exemplar agiert mit einer Gruppe von C&C-Servern, deren IP-Adressen durch den Download einer dechiffrierten Symboldatei (favicon.ico), wie in Abbildung 12 dargestellt, von einigen fest kodierten TOR-Seiten abgerufen werden. Dies bietet den Vorteil, dass zwar der Standort eines kriminellen Servers anonymisiert wird, nicht aber die Benutzer, die darauf zugreifen, was jedoch kein Problem darstellt, da alle "Benutzer" Systeme sind, die von der Malware infiziert wurden (Ciancaglini, Balduzzi, McArdle, & Rösler, 2015).

Abbildung 13: Favicon der VAWTRAK Malware (Ciancaglini, Balduzzi, McArdle, & Rösler, 2015)

Eine weitere große Malware-Familie, die das Darknet nutzt, ist CryptoLocker. CryptoLocker bezieht sich auf eine Ransomware-Variante, die persönliche Dateien der Opfer dechiffriert, bevor sie auf eine Seite umgeleitet werden, auf der sie bezahlen können, um wieder Zugriff auf ihre Dateien zu erhalten. CryptoLocker ist auch intelligent genug, um die Zahlungsseite automatisch an die lokale Sprache und die Zahlungsmittel des Opfers anzupassen. TorrentLocker - eine CryptoLocker-Variante - nutzt TOR, um Zahlungsseiten zu hosten, und setzt zusätzlich Bitcoin als Zahlungsmittel ein. Das zeigt, warum das Darknet für Cyberkriminelle attraktiv ist, die bereit sind, ihre Infrastrukturen robuster gegen mögliche Schließungen zu machen. (Hoffer, 2018).

Hacking-Tools beziehen sich auf Formen von Software, die speziell für die Durchführung bösartiger Aktivitäten entwickelt wurden. Zu dieser Kategorie gehören eine Reihe von Tools, die von Strafverfolgungsbehörden häufig für kriminelle Aktivitäten identifiziert werden. Diese Kategorie umfasst eine Reihe von verschiedenen Formen von Malware. Solche Tools können verwendet werden, um Fernzugriff oder Penetrationstests zu ermöglichen und werden häufig in "Paketen" angeboten. Ein Beispiel dafür wäre der sogenannte „Zeus“. Zeus ist eine Art Trojaner-Malware, die eine Hintertür in betroffenen Windows-Computern einrichtet und in der Lage ist, Passwörter über Keylogger zu sammeln. Keylogger sind verdeckte Malware, die sich der Entdeckung entziehen können und in der Lage sind, die Tastaturaktivitäten auf kompromittierten Systemen aufzuzeichnen. Gestohlene Kennwörter und Daten können dann für eine tiefere Systeminfiltration verwendet werden. Durch das Stehlen von Passwörtern und Daten können Angreifer effektiv die Schutzmaßnahmen, wie Firewalls oder Virenscanner, umgehen, indem sie sich als legitime Benutzer ausgeben (Broadhurst, et al., 2018).

4.2.4 Waffenhandel

Der illegale Handel mit Waffen ist ein globales Problem, das die Rechtsstaatlichkeit, die Arbeit der Polizei und die Sicherheit der Zivilbevölkerung bedroht. Die Bedrohung wird in Konfliktgebieten, in denen das Monopol eines Staates über die Gewaltmittel angefochten wird, im noch größeren Ausmaß verstärkt. Der Handel mit illegalen Schusswaffen, Munition und Sprengstoffen ist eine zentrale kriminelle Aktivität, die organisierte Kriminalität ermöglicht, Gewalt und Terrorismus schürt und zu zivilen Unruhen beiträgt. Viele im Darknet erworbene Schusswaffen und andere Waffen wurden zur Begehung von Terrorakten und gezielter Gewalt verwendet (Paoli, Aldridge, Ryan, & Warnes, 2017).

Im Darknet sind tödliche Waffen jederzeit und von überall für jeden zugänglich. Jeder kann jede beliebige Waffe auf den Dark-Web-Seiten wie „Liberator“, „Armory“ oder „Black Market Reloaded“ kaufen. Um sie im Darknet zu bekommen, wird keine Hintergrundüberprüfung benötigt und es muss keine Wartezeit in Kauf genommen werden. Da in den meisten Ländern der Verkauf von Waffen entweder verboten oder reguliert ist, nutzen die Verkäufer von Schusswaffen im Darknet diese Situation aus. Das Darknet macht den weltweiten Waffenhandel möglich. Obwohl der Wert und das Volumen der im Dark Web gehandelten Schusswaffen im Vergleich zu anderen

Produkten wie Drogen verschwindend gering ist, sind die Auswirkungen auf das Sicherheitsszenario immens, wie zahlreiche Terroranschläge in Europa zeigen (Murali, 2019).

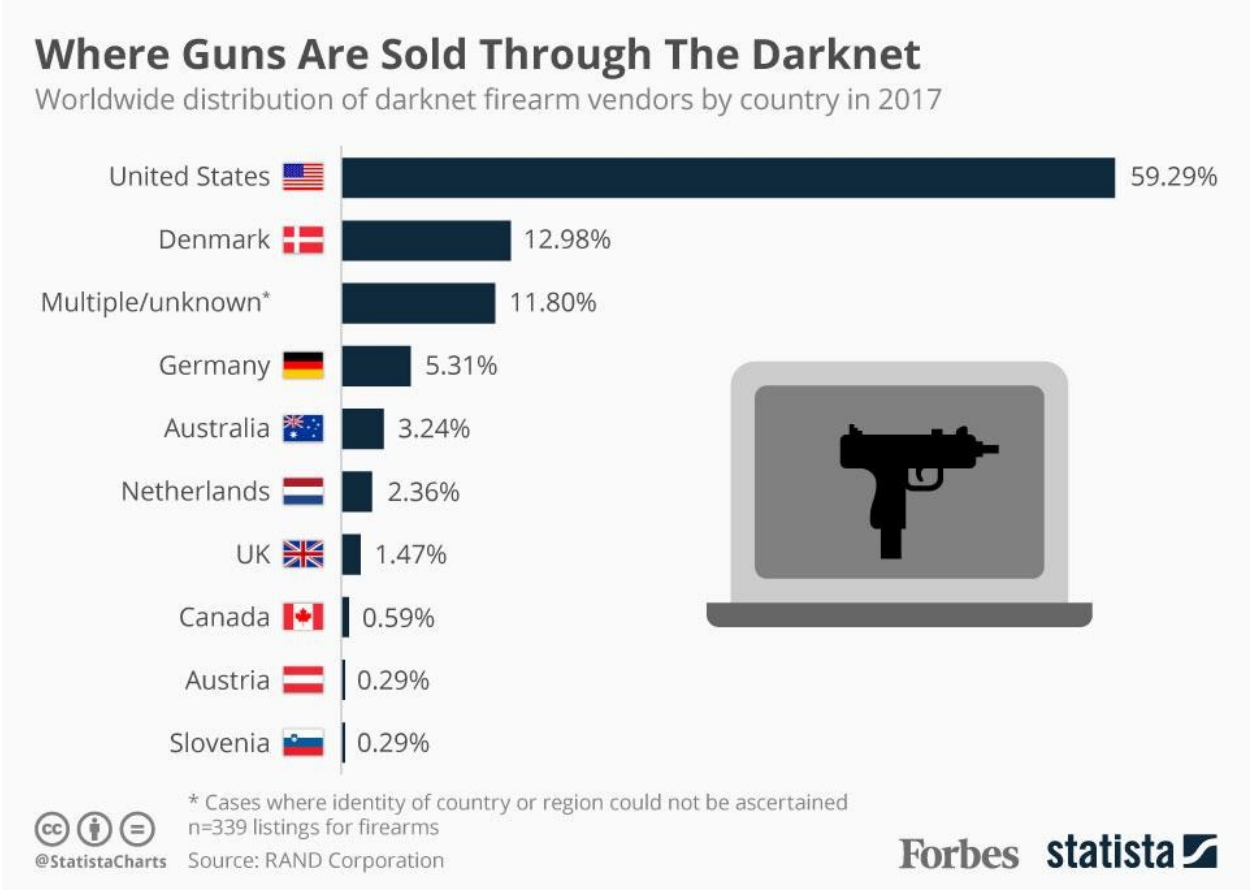


Abbildung 14: Waffenhandel in Darknet (McCarthy, 2018)

Eine Studie der RAND Corporation analysierte die Größe des Waffenhandels auf globalen Krypto-Märkten und fand heraus, dass das Darknet tatsächlich die Verfügbarkeit von Schusswaffen zu ähnlichen Preisen wie im illegalen Straßenhandel ermöglicht. Die Vereinigten Staaten sind das häufigste Herkunftsland für Waffenverkäufe im Darknet mit fast 60 Prozent der analysierten Angebote (vgl. Abbildung 14) (McCarthy, 2018).

Trotzdem stellt Europa den größten Markt für Schusswaffen im Darknet dar, mit einem etwa fünfmal höheren Umsatz als in den Vereinigten Staaten. Auf Länderebene hatte Dänemark den zweithöchsten Anteil an Schusswaffenverkäufern im Darknet (13%), gefolgt von Deutschland (5%) (McCarthy, 2018).

Darknet klassifiziert Waffen, wie z.B. Pistolen, Sprengstoff, Munition, Langwaffen und andere. Unter Munition findet man aufgelistete Geschosse in allen Größen und Formen. Die RAND Corporation Europe, eine Non-Profit-Organisation, die mit der Universität Manchester zusammenarbeitet, fand 52 einzelne Anbieter, die Waffen oder analoge Produkte wie Munition, Sprengstoff oder Komponenten wie Schalldämpfer in 811 Listings und 18 Märkten verkaufen (Murali, 2019).

Der Berlusconi-Markt bietet eine große Auswahl an Waffen für Käufer an. Sie verschicken die meisten von ihnen weltweit, während sie einige lokal verkaufen. Die Darknet-Märkte verlangen

von den Käufern, sich zu registrieren, um vollen Zugriff auf die bei den Anbietern verfügbaren Artikel zu erhalten. Ein Anbieter wie Veronique hat Munition auf Lager, deren Preise zwischen 20 € und 80 € pro Stück liegen. In der Kategorie Langwaffen verkauft Goblin-King die in Russland hergestellte Saiga MK für rund 3.000 €, was aktuell 0,436207 Bitcoins entspricht. Der Verkäufer bietet den Service mit vollem Treuhandschutz an, bei dem die Kunden erst dann zahlen müssen, wenn sie mit der Qualität der Waffe zufrieden sind. Unter der Kategorie Sprengstoff werden sowohl Granaten als auch Chemikalien und Sprengstoff angeboten (Murali, 2019).

Der Handel mit Schusswaffen durch Umleitung von legalen auf illegale Märkte stellt eine Bedrohung für die öffentliche Sicherheit dar. In Australien, wo der legale Schusswaffenbesitz streng geregelt ist, werden illegale Schusswaffen von Gruppen des organisierten Verbrechens sowie von Kriminellen erworben. Illegale Schusswaffen sind ein Mittel zur Einschüchterung und zur Begehung von Gewalttaten. Sie ermöglichen die Beteiligung an der organisierten Kriminalität und anderen schweren Straftaten (Broadhurst, Foye, Jiang, & Ball, 2020).

Der Versand von im Darknet erworbenen Waffen ist bei weitem der schwierigste Vorgang im gesamten Prozess einer Kaufaktion. Der Postdienst, welcher früher das gängigste Verfahren für den Versand einer Waffe war, wird heute von den meisten Strafverfolgungsbehörden überwacht. Die Waffen werden daher in abgeschirmten Verpackungen versandt, indem sie in legalen Waren wie Elektronik, Büchern und Kleidung versteckt werden, um einer Entdeckung durch die Behörden zu entgehen. Diese illegalen Waffen werden auch zerlegt und in verschiedenen Paketen zu verschiedenen Zeiten verschickt. Kürzlich wurden einige Gegenstände von den Behörden in alten Stereoanlagen und Druckern entdeckt (Murali, 2019).

Die Waffenhändler arrangieren auch "Dead Drops", bei denen die zusammengebauten Waffen in einem Park, einer Gasse oder in einem unfruchtbaren Boden an einem abgelegenen Ort vergraben werden. Nachdem die Käufer bezahlt haben, erhalten sie die GPS-Koordinaten und eine Beschreibung der Gegenstände, die sie unter der Erde finden werden. Forscher fanden in einer Studie heraus, dass Schusswaffen-Verkäufe einen monatlichen Umsatz von 80.000 US-Dollar generiert haben. Nachdem der Käufer die Waffe in Empfang genommen und auf ihre Qualität geprüft hat, können die Kunden die Zahlung abschließen, indem sie auf unterschiedlichen Plattformen im Darknet ein Treuhandkonto einrichten (Murali, 2019).

Ein Beispiel für den grenzüberschreitenden Charakter des Darknet-Waffenhandels ist eine gemeinsame Operation im Jahr 2018, an der das US Bureau of Tobacco, Alcohol, Firearms and Explosives, der US Postal Inspection Service, der Australian Customs and Border Protection Service und die australische Bundespolizei beteiligt waren und bei der in Australien illegale Schusswaffen sichergestellt wurden, die mit Bitcoin im Darknet gekauft wurden. Vier Männer mit Wohnsitz im US-Bundesstaat Georgia bekannten sich schuldig, Schusswaffen auf dem Postweg versteckt in elektronischen Geräten von den USA nach Australien geschmuggelt zu haben. Die illegalen Feuerwaffen wurden durch ein in den USA ansässiges Syndikat (alias "CherryFlavour") beschaffen, welches ein internationales Feuerwaffenhandelsunternehmen betrieb, das über 70 Feuerwaffen zu überhöhten Preisen in andere Länder verschickte. Die beliebte Glock-Pistole, die normalerweise für 500 US-Dollar verkauft wird, war über "CherryFlavour" für 3.400 US-Dollar erhältlich. In einem anderen Fall im Jahr 2018 verhaftete die Polizei von New South Wales einen

28-jährigen Mann, da er versucht hatte, drei Schusswaffen und Munition aus dem Darknet zu kaufen, indem er monetäre Einheiten von seinem Kryptowährungskonto überwies (Broadhurst, Foye, Jiang, & Ball, 2020), (Paoli, Aldridge, Ryan, & Warnes, 2017).

Oft führen Terroristen und Kriminelle illegale Geschäfte im Schutz des anonymen Darknets durch. Dies erfolgt von der Sicherheit ihres Zuhauses aus und ohne vorherige Verbindungen zu Lieferanten. Die Daten zeigen, dass die meisten Waffen, die im Dark Web erhältlich sind (60 %), aus den USA stammen. Europa ist der größte Markt für Waffen aus dem Dark Web. Insgesamt werden im Dark Web mehr neue und leistungsfähige Schusswaffen zu den gleichen oder niedrigeren Kosten angeboten als auf der Straße oder am Schwarzmarkt (Murali, 2019).

Es gibt jedoch keine zuverlässigen Beweise für einen direkten Zusammenhang zwischen dem Online-Waffenmarkt im Dark Web und dem Terrorismus. Die aus den offiziellen Unterlagen der Staatsanwaltschaft Stuttgart vorliegenden Informationen weisen darauf hin, dass die bei den Pariser Anschlägen im November 2015 verwendeten Waffen im Darknet bei einem deutschen Anbieter mit dem Nutzernamen "DW Guns" gekauft wurden. In einem anderen Fall wurde entdeckt, dass Ali David Sonboly, ein jugendlicher Angreifer iranischer Herkunft, der sich offenbar von Anders Breiviks rechtsextremen Terroranschlägen in Oslo, im Jahr 2011 inspirieren ließ, seine Waffen im Darknet gekauft hatte und mit diesen am 22. Juli 2016 in München neun Menschen erschoss (Paoli, Aldridge, Ryan, & Warnes, 2017).

Im September 2017 enthüllten die Behörden in Großbritannien, dass Umair Khan aus Birmingham, als veraltet eingestufte Munition aus dem Darknet gekauft und zu funktionierenden illegalen Waffen umgebaut hatte, die er an kriminelle Banden verkaufte. Die Ermittlungen ergaben außerdem, dass Khan im Zeitrahmen von August 2014 bis Februar 2017 geschätzte 50.000 Pfund für den Kauf von über 50 Revolvern und über 1.600 Schuss Munition ausgegeben hatte. Später stellte man fest, dass zwei 16-jährige Jungen seine Waffen erhalten hatten. Es stellte sich außerdem heraus, dass Khan ein Waffenhändler für Gruppen des organisierten Verbrechens war, ohne zu wissen, wo und wie von ihm verkaufte Waffen angewendet wurden (Murali, 2019).

Die Tatsache, dass nicht nur Kriminelle und Terroristen anonyme Käufe tätigen können, sondern auch gefährdete und besessene Einzelpersonen Waffen beschaffen können, stellt eine immens große Gefahr dar. Jeder kann sich mit dem Darknet verbinden und hat innerhalb von Minuten Zugang zu einer Vielzahl von Anbietern, die Waffen verkaufen, welche in den meisten Fällen illegal vertrieben werden. Das Darknet erleichtert den illegalen Waffenhandel auf globaler Ebene, indem es die geografischen Barrieren zwischen Verkäufern und Käufern abbaut und das persönliche Risiko verringert, wobei es ihre Identitäten durch die Anonymität des Darknets verschleiert. Die Regierungen haben das Potenzial von Kryptowährungen für den Missbrauch von Terrorismus im Darknet nur langsam erkannt. Bitcoin ist zur prominenten Währung des Darknets geworden, um illegale Waren wie Waffen online zu kaufen. Die Kreuzung von Dark Web und Bitcoin, die von der organisierten Kriminalität genutzt wird, stellt vielleicht die größte Bedrohung dar. Ähnlich wie organisierte Kriminelle könnten terroristische Organisationen Bitcoin nutzen, um eine Reihe von Waffen, einschließlich Schusswaffen oder Material zum Bombenbau, im Darknet käuflich zu erwerben (Murali, 2019).

4.2.5 Weitere Inhalte

Einer der besorgniserregendsten Dienste im Darknet sind Auftragskiller oder Auftragsmörder. Es gibt mehrere solche Dienste im Darknet. Selbst die Seiten, welche auf Darknet solche Dienstleistungen anbieten, warnen, dass es sich um ein sehr geheimes Geschäft handelt. Auf einer Seite wird zum Beispiel deutlich darauf hingewiesen, dass sie keine Beweise für frühere Arbeiten, Erfolge oder sogar Feedback von früheren Kunden anbieten können, da alle Verträge privat sind. Stattdessen müssen die Interessenten mit Hilfe eines seriösen Treuhandservice beweisen, dass sie genug Bitcoins für die angebotene Dienstleistung haben. Erst wenn ein Auftragskiller den Auftrag ausgeführt und den Nachweis erbracht hat, werden die Gelder freigegeben (Ciancaglini, Balduzzi, McArdle, & Rösler, 2015).

Die Preise variieren je nach der bevorzugten Art des Todes oder der Verletzung und dem Status des Zieles. Ross Ulbricht, der als Betreiber des berüchtigten Silk-Road-Forums für illegale Drogen bekannt geworden ist, hat tatsächlich versucht, fünf der Partner, mit denen er sich zerstritten hatte, ermorden zu lassen (Greenberg, 2015).

Eine andere Variante solcher Dienste ist die sogenannte "Crowdsourced Assassination". Eine Website ermöglicht es Benutzern, potenzielle Ziele vorzuschlagen. Andere können dann Geld in Form von Bitcoins auf die vorgeschlagenen Opfer einzahlen. Attentäter können darauffolgend anonym vorhersagen, wann und wie die Ziele sterben werden. Wenn die Person tatsächlich stirbt, werden alle Vorhersagen aufgedeckt und die Attentäter, die eine genaue Übereinstimmung vorgeschlagen haben, können das Geld einfordern (Ciancaglini, Balduzzi, McArdle, & Rösler, 2015).

Unter anderem haben sich aber auch Blogs einen festen Platz unter frequent eingesetzten Inhalten des Darknets erarbeitet. Hierbei sind alle Seiten gemeint, die eine vordefinierte Gruppe an Autoren besitzen, die wiederholend Inhalte verfassen. Diese Blog-Inhalte setzen keine Interaktion zwischen den Nutzern voraus, wodurch sie sich von einem Forum unterscheiden. Hierzu gehören auch Nachrichten und Marketingseiten, die nicht einer bestimmten Gruppe oder einem bestimmten Zweck zugeordnet werden können. Als Beispiel dafür kann etwa der Aktivismus, wie es auch beim Menschenrechtsaktivismus der Fall ist, genannt werden. Ein anderes Beispiel wäre das sogenannte „Whistleblowing“, das insbesondere durch Wikileaks an Bekanntheit gewonnen hat, *„aber auch sogenannte SecureDrops einbezieht, durch die Personen anonym Journalist*innen Daten zuspielen können“* (Najjar & Schwaß, 2019).

5 SCHUTZ VOR GEFAHREN DES DARKNETS

Im Darknet gibt es ein breites Spektrum an Risiken, welchen jeder Nutzer ausgesetzt wird. In den meisten Fällen werden insbesondere Darknet-Nutzer als solche angegriffen, sowie deren Software und Daten, welche im Darknet leicht attackiert oder gar gestohlen werden können. Um somit beim Nutzen des Darknets die höchstmögliche Sicherheit zu erlangen, müssen entsprechende Maßnahmen und Vorkehrungen getroffen werden.

Im Laufe der Zeit sind Cyber-Attacken zu einer der größten Herausforderungen der heutigen Gesellschaft geworden. Es gibt verschiedene Arten von Cyberangriffen, wie z. B. DDoS-Angriffe, Malware-Infektionen, Drive-by-Download-Angriffe, Sondierungen zum Auffinden von Sicherheitslücken, Spam-Mails, um auf bösartige Websites anzulocken, Phishing, und gezielte E-Mail-Angriffe, die darauf abzielen, Geld sowie wichtige Informationen zu stehlen und öffentliche Dienste zu stören oder gar zu stoppen. Um Benutzer vor solchen Cyberangriffen zu schützen, ist es wichtig, bösartige Aktivitäten im gesamten Internet zu erfassen (Nishikaze, et al., 2015), (Broadhurst, et al., 2018), (Patterson, 2019), (Bischoff, 2020).

5.1 Schutz des Nutzers

Die Überwachung von Identitätsdiebstahl ist entscheidend, wenn verhindern werden soll, dass private Informationen missbraucht werden. Alle Arten von persönlichen Daten können online gewinnbringend verbreitet werden. Passwörter, Bankkontonummern, physische Adressen und Sozialversicherungsnummern zirkulieren im Darknet. Böswillige Akteure können diese nutzen, um die Identität des Opfers zu stehlen, finanziellen Diebstahl zu begehen und in andere Online-Konten einzudringen. Lecks in persönlichen Daten können auch zu einer Rufschädigung und den damit verbundenen Folgen führen. Aber wie können solche Aktionen verhindert werden?

5.1.1 Schutz der Anonymität

Der Zugriff auf das Darknet ist eine triviale Aufgabe, die von jedem durchgeführt werden kann, der einen dedizierten Browser wie TOR oder I2P herunterladen und installieren kann. Nur die Installation des Browsers kann jedoch nicht die Anonymität im Darknet garantieren. Weitere Schritte sind erforderlich, um die Anonymität eines Anwenders während der Nutzung des Darknets zu erhöhen. Es gibt eine Vielzahl an unterschiedlichen Methoden, die eingesetzt werden können, um das Risiko der Entdeckung zu verringern (Broadhurst, et al., 2018).

Eine der Techniken, welche die Anonymität des Users erhöhen, ist die Wahl des richtigen Browsers.

TOR (siehe Abbildung 15) ist der beliebteste Browser für den Zugang zum Darknet und ermöglicht den Zugriff auf Domains mit dem Suffix ".onion". Er ist einfach zu installieren und besitzt zahlreiche Features, welche auch bei modernen Browsern wie Google Chrome, Firefox oder auch Internet Explorer zu finden sind. TOR wird mit einer Vielzahl an fest eingebauten Sicherheits- und

Verschlüsselungsfunktionen vorinstalliert, die IP-Adressen verschleiern und somit den Nutzern einen höheren Grad an Anonymität anbieten. Diese Sicherheitsfunktionen verschlüsseln die IP-Adresse des Benutzers beim Surfen im Darknet, was eine individuelle Identifizierung erschwert, aber nicht unmöglich macht (Patterson, 2019).

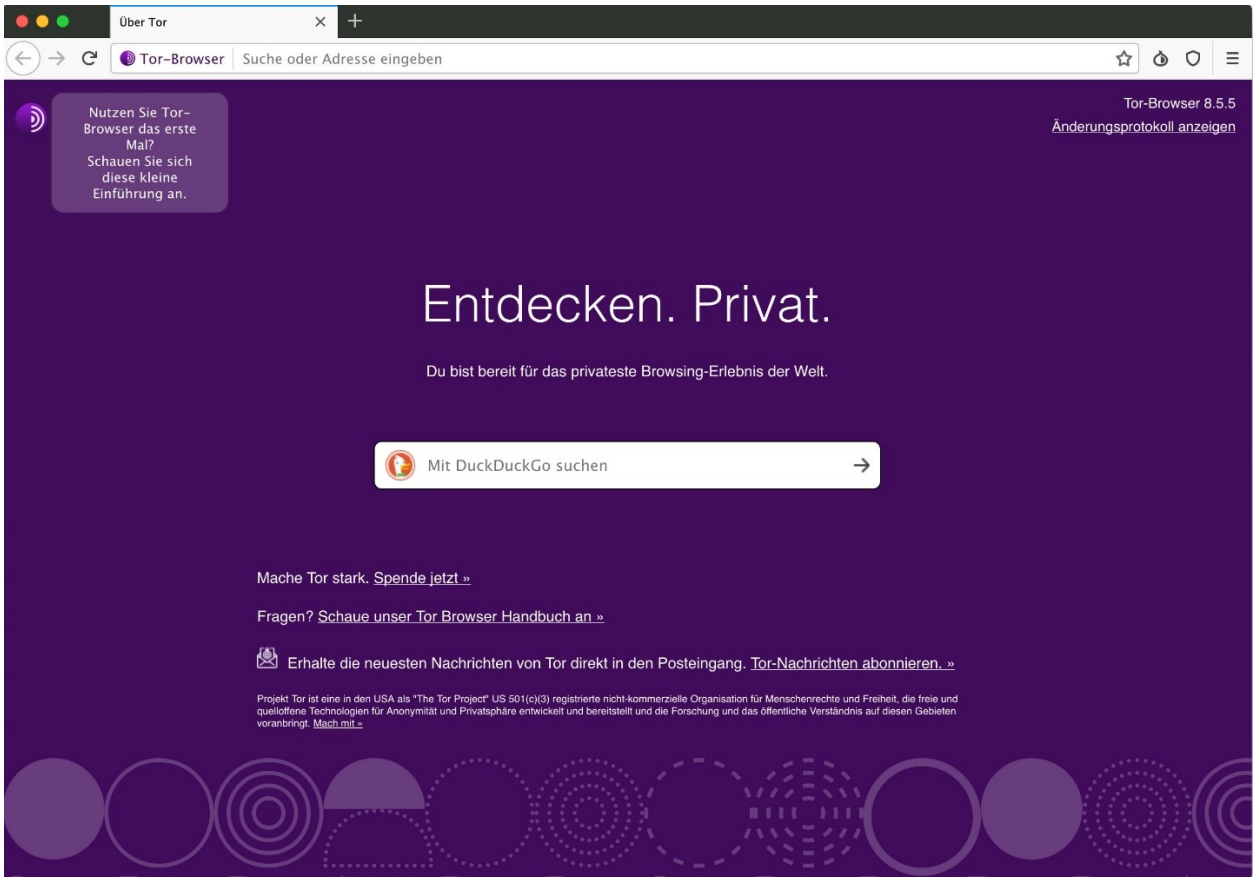


Abbildung 15: TOR-Browser Startseite (Rentrop, 2019)

I2P ist der zweitpopulärste Darknet-Browser und ermöglicht Nutzern den Zugriff auf seine eigene Reihe von versteckten Seiten, auch bekannt als "eepsites". Er ist ähnlich wie TOR, da er den Nutzern die Möglichkeit bietet, die IP zu verschleiern und den Zugriff auf versteckte Websites im Darknet ermöglicht. Die primäre Eigenschaft von I2P ist jedoch, als ein "Netzwerk innerhalb des Internets" zu fungieren, das den Datenverkehr auf sich selbst beschränkt und dadurch der Definition eines Darknets entspricht. I2P verfügt über einen zuverlässigeren Dienst, da es paketbasiertes Routing anstelle eines leitungsbasierten (wie etwa bei TOR) verwendet. Das bedeutet, dass es in der Lage ist, Netzwerküberlastungen und Serviceunterbrechungen zu umgehen, ähnlich wie die Oberflächennetze des IP-Routings (Broadhurst, et al., 2018).

Freenet ist der drittbeliebteste Darknet-Browser. Er ähnelt der Funktionalität von I2P mehr als der von TOR, bietet aber zahlreiche einzigartige Funktionen. Wie I2P ist auch Freenet ein in sich geschlossenes Netzwerk innerhalb des Darknets, das nicht auf das Surface Web zugreifen kann. Außerdem kann der Freenet-Browser nur die Inhalte aufrufen, die in seinen verteilten Peer-to-Peer-Datenspeicher hochgeladen wurden. Im Gegensatz zu TOR und I2P benötigt Freenet keinen Server, um Inhalte zu hosten und funktioniert wie die Surface Web Cloud. Das bedeutet, dass etwas, das auf Freenet hochgeladen wurde, online bleibt, auch wenn der Hochladende das

Programm nicht mehr nutzt. Schließlich bietet der Browser den Benutzern zwei Möglichkeiten sich zu verbinden. Die Open-Net-Funktion erlaubt es den Benutzern sich automatisch mit Peers und Seiten im Freenet-Netzwerk zu verbinden. Die "Darknet"-Funktion erlaubt es den Benutzern zu wählen, mit wem sie sich verbinden und die Freunde des Benutzers festlegen. Dadurch entsteht eine geschlossene Gruppe, auf die nur autorisierte Benutzer zugreifen können (Broadhurst, et al., 2018).

Nachdem die Auswahl getroffen wurde, welcher Browser für die Arbeit im Darknet eingesetzt werden soll, wird empfohlen, auch ein VPN einzusetzen, um die eigene Identität zu schützen. Virtual Private Networks (VPNs) werden regelmäßig von TOR-Benutzern verwendet, um eine weitere Ebene des Identitätsschutzes hinzuzufügen. VPNs ermöglichen es den Nutzern, den gesamten Netzwerkverkehr zu verschlüsseln und ihn durch einen bestimmten Server zu leiten und schaffen so effektiv einen gefälschten geografischen Zugangspunkt zum Internet. Es gibt zwei Methoden, ein VPN zu benutzen, während man in TOR surft: VPN vor dem Zugriff auf TOR, und VPN nach dem Zugriff auf TOR. Beide Methoden verbergen den Standort und die Identität des Benutzers auf eine eigene Art und Weise, haben jedoch auch ihre Vor- sowie Nachteile (Bischoff, 2020).

Wenn ein Benutzer sein VPN einschaltet, bevor er TOR startet, benutzt er TOR über VPN. TOR über VPN ist die häufigste und gängigste Methode, um mit identitätsverschleiernder Technologie auf das Darknet zuzugreifen. Die IP des Benutzers nimmt nur den verschlüsselten VPN-Netzwerkverkehr wahr. Das bedeutet, dass sie keine Kenntnis über die Nutzung von TOR durch den Benutzer in ihrem Netzwerk hat. Viele TOR-Benutzer abonnieren verschlüsselte VPNs, die den Datenverkehr nicht protokollieren und bezahlen dafür mit Kryptowährung, um ihre Anonymität zu gewährleisten. TOR über VPN schützt die Nutzer jedoch nicht vor bösartigen Exit-Knoten, die den Internetverkehr des Benutzers entschlüsseln, persönliche Daten stehlen oder bösartigen Code einschleusen können (Bischoff, 2020).

Wenn Benutzer auf TOR zugreifen und dann ein VPN benutzen, benutzen sie VPN über TOR. Diese Methode ist weniger populär als TOR über VPN und erlaubt keinen Zugriff auf Webseiten mit versteckten Diensten, wie zum Beispiel solche mit der Endung .onion. Diese eingeschränkte Zugänglichkeit ist darauf zurückzuführen, dass das VPN der zugreifende Akteur anstelle von TOR ist. Das bedeutet, dass der gesamte TOR-Verkehr durch das VPN geleitet wird. Obwohl VPN über TOR eine eingeschränkte Erreichbarkeit hat, hat es auch seine Vorteile. Es erlaubt einem Benutzer, gegenüber seinem VPN anonym zu bleiben (solange eine geheime Zahlungsmethode verwendet wird über Zahlungsmittel wie Kryptowährungen) und ermöglicht den Zugang zu Webseiten, die TOR sonst blockiert hätten. Wenn Benutzer einen Exit-Node passieren, bleiben ihre Informationen sicher und verschlüsselt, da sie durch das VPN maskiert werden (Bischoff, 2020).

Eine weitere Technik zur Verschleierung der Identität ist der Einsatz einer „Virtual Box“, welche mit einer virtuellen Maschine gleichzusetzen ist.

Das Amnesic Incognito Live System (TAILS) basiert auf Debian (ein freies Betriebssystem, das für Anonymität bei der Nutzung von TOR konzipiert wurde) und bildet eine 'Virtual Box' oder virtuelle Maschine mit einer zusätzlichen Verschlüsselung. TAILS wurde durch Edward Snowden

berühmt, als er Geheimnisse der US National Security Agency (NSA) an die Medien weitergab, bevor er aus den USA flüchtete. Die Verwendung von TAILS hat sich als eine große Hürde für die Strafverfolgung erwiesen, da es die Identifizierung von Cyberkriminellen und Terroristen erheblich erschwert. TAILS wird mit einem modifizierten TOR-Browser sowie einer Reihe von Identitätsverschleierungs- und Schutzfunktionen ausgeliefert, einschließlich einer zusätzlichen Verschlüsselung. Es ist so konzipiert, dass es von einem USB- oder DVD-Laufwerk (auf einem beliebigen Betriebssystem) gestartet werden kann, um keine Informationen auf das lokale Laufwerk des verwendeten Geräts zu schreiben und somit keinen digitalen Fußabdruck zu hinterlassen (Broadhurst, et al., 2018).

Whonix ist auf maximale Sicherheit und Geheimhaltung ausgelegt und basiert, wie TAILS, auf einem Debian-Betriebssystem. Im Gegensatz zu TAILS ist es jedoch so konzipiert, dass es auf einem Computer über eine virtuelle Maschine installiert und ausgeführt werden kann, die auf kommerziellen Standard-Betriebssystemen wie Windows, Ubuntu, MacOS und Qubes basiert. Das Programm erstellt auf dem Computer des Benutzers zwei untergeordnete Betriebssysteme, genannt "Gateway" und "Workstation", um einen umfassenden Schutz sowohl vor Malware als auch vor Identitätsmissbrauch des Benutzers über IP-Adresslecks zu gewährleisten (Broadhurst, et al., 2018).

Der Schlüssel zur erhöhten Anonymität liegt in der einzigartigen Funktionsweise von Whonix. Whonix als Ganzes besteht aus zwei Teilsystemen. Das Surfen im Internet, das Betrachten von Dokumenten oder jede andere Art von anonymer Arbeit werden ausschließlich über die "Workstation"-Komponente durchgeführt, die eher einem Standard-Betriebssystem ähnelt. Der einzige Zweck der "Gateway"-Komponente ist es, als Vermittler zwischen dem Internet und der Workstation zu fungieren. Der gesamte Verkehr von der Workstation wird durch das Gateway geleitet, das dann über TOR auf das Internet zugreift. Im Wesentlichen bedeutet dies, dass die Workstation immer noch geschützt ist, auch wenn das Gateway kompromittiert wurde. Die Herausforderung für die Strafverfolgung liegt in dem oben beschriebenen Modell. Es gibt keinen klaren Weg, um die Whonix-Workstation sinnvoll zu identifizieren, da sie so gut durch die Verwendung von TOR, einem Gateway und optional einem VPN geschützt ist. Allerdings stellt die Tatsache, dass Whonix oft innerhalb eines Host-Betriebssystems ausgeführt wird, eine wesentliche Schwachstelle dar. Wenn das Host-Betriebssystem, insbesondere MacOS oder Windows, kompromittiert werden kann, kann die Verwendung von Whonix leicht durch den Einsatz von datenklauender Malware, wie zum Beispiel einem Keylogger, überwacht werden. Daher werden die meisten Darknet-Benutzer, die Anonymität über alles andere stellen, ein Host-Betriebssystem wie Ubuntu oder, im Fall von Whonix, Qubes verwenden (Broadhurst, et al., 2018).

5.1.2 Schutz vor Betrug

Dark-Web-Anbieter haben das Geschäft mit dem Betrug gründlich systematisiert und bieten alles von Bankkonten über vollständige Identitäten bis hin zu Kreditkarten oder Musik-Streaming Berechtigungsnachweisen an (Gollnick & Wilson, 2016).

Nachdem Nutzer in vielen Fällen das Darknet betreten, um Waren zu erwerben, wird eine große Bedeutung auch der Sicherung der Märkte zugeschrieben. Um das Risiko eines Betrugs zu minimieren oder gar zu vernichten, werden zahlreiche Techniken angewendet.

Marktplätze haben sich seit den Anfängen von Silk Road und Agora weiterentwickelt. Sie sind nicht länger eine einseitige Website mit minimaler Sicherheit. Marktplätze verwenden eine Reihe von Verteidigungsmaßnahmen, darunter Alternative Links, CAPTCHAs sowie DDoS-Schutz (Broadhurst, et al., 2018).

Durch die Bereitstellung alternativer Zugangsmöglichkeiten können Darknet-Märkte die Betriebszeit aufrechterhalten und den Betrieb fortsetzen, indem sie die Last der Benutzeraktivität verteilen. Durch das Hosten alternativer Links können Darknet-Märkte auch die störende Wirkung von DDoS-Attacken einschränken. Alternative Links ändern sich oft im Laufe der Zeit in dem Versuch, anhaltende DDoS-Angriffe abzuschwächen. Diese Änderungen an der .onion-Adresse von Marktplätzen werden oft von Marktadministratoren gemeldet, da eine Änderung der URL ein Zeichen für einen Phishing-Versuch der Strafverfolgungsbehörden, eine Störung durch kriminelle Konkurrenten oder andere dritten Parteien sein kann (Broadhurst, et al., 2018).

Die meisten virtuellen Marktseiten verfügen zusätzlich über einen CAPTCHA-Schutz (siehe Abbildung 16), um den Effekt von Bot- und anderen automatisierten Browser-Aktivitäten zu minimieren. Durch erfolgreiches Lösen der CAPTCHA-Herausforderung ist ein Benutzer in der Lage auf den Marktplatz zu gelangen und ihn zu erkunden. Oft setzen Marktseiten ein erstes CAPTCHA ein, um die Anmeldeseite zu sichern und ein zweites CAPTCHA zum Schutz des Anmeldevorgangs. CAPTCHAs werden oft zusammen mit DDoS-Schutz implementiert, um den Schutz zu erhöhen (Broadhurst, et al., 2018).

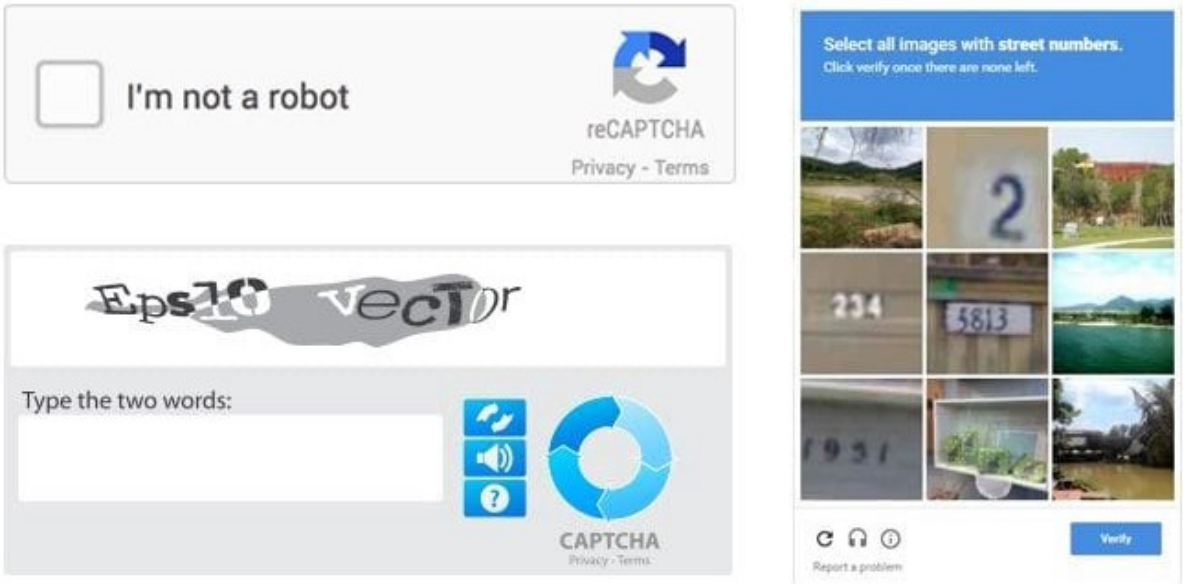


Abbildung 16: Formen von CAPTCHA (Hahn, 2020)

Darknet-Märkte haben ihre eigenen Formen des DDoS-Schutzes. Diese reichen von der Verwendung von proprietären Diensten wie "CloudFlare" bis hin zu benutzerdefinierten "Auto-Lock-Outs" als Reaktion auf verdächtige Aktivitäten. Durch das Markieren von verdächtigem

Browser-Verhalten hat der Systemadministrator die Möglichkeit, Benutzer auszusperren oder CAPTCHA-Herausforderungen zu erzwingen, um das Ausmaß potenzieller Konsequenzen des verdächtigen Verhaltens zu begrenzen. Darknet-Märkte variieren in ihren Fähigkeiten zum DDoS-Schutz. Groß angelegte DDoS-Angriffe gegen Darknet-Märkte kommen häufig vor, allerdings selten in dem Ausmaß wie im Fall von Github. Laut einer Untersuchung von Verisign/Merril Research (2018) ist ein Drittel aller Ausfallzeiten auf DDoS-Attacken zurückzuführen. Kürzlich überstand Github, eine Open-Source-Entwicklerplattform, den größten aufgezeichneten DDoS-Angriff mit einem Datenverkehr von 1,35 Terabit pro Sekunde. Ein digitales System bewertete das Ausmaß des DDoS und innerhalb von 10 Minuten wurde Unterstützung durch einen Mitigation-Service bereitgestellt. Das Schadensausmaß war minimal, wobei es während der Dauer des DDoS zu zeitweiligen Ausfällen kam. Glücklicherweise hatte Github seine Traffic-Kapazität für das Ereignis vorher modelliert (Broadhurst, et al., 2018).

5.1.3 Sichere Kommunikation

Sicheres Messaging ist ein wichtiger Bestandteil von Darknet-Transaktionen. Kommunikation über E-Mails kann nur schwer gesichert werden. Aufzeichnungen existieren überall und die E-Mail-Anbieter geben zu, dass sie gerichtlichen Anordnungen nachkommen. Es kann davon ausgegangen werden, dass alles, was in einer E-Mail steht, nur einen Schritt davon entfernt ist, öffentlich zu sein. Um Transaktionen im Darknet durchzuführen, muss daher die gesamte Kommunikation mit einer Form der Verschlüsselung gesichert werden. (Wernicke, 2016).

Sollten Nutzer jedoch trotzdem E-Mail als Kommunikationskanal im Darknet einsetzen wollen, so gibt es einige Möglichkeiten, welche angewendet werden können, um eine akzeptable Form der Kommunikationssicherheit zu gewährleisten.

Hushmail ist das führende Java-basierte E-Mail-Verschlüsselungsprogramm, das im Browser implementiert ist. Auch Safe-mail bietet wie Hushmail eine browserbasierte Oberfläche. Obwohl keine dieser Lösungen ideal ist, können sie nützlich sein, um zuvor verschlüsselte Dateien über eine einfache Schnittstelle zu versenden. Es wird empfohlen bei der Verwendung der Interfaces diskret zu sein. Wenn versendete E-Mails illegale Aktivitäten beinhalten und unverschlüsselt sind, werden Beweise einschließlich der Identität preisgegeben. Wenn sich Nutzer mit diesen E-Mail-Alternativen verbinden und mit TOR surfen, können Sie zwar nicht identifiziert werden, aber der Inhalt der E-Mail kann trotzdem gelesen werden (Wernicke, 2016).

Mozillas Thunderbird wäre eine weitere Möglichkeit, um die Kommunikation im Darknet sicher abzuwickeln. Es ist ein Offline-Reader, welcher speziell für E-Mails konzipiert wurde. Enigmail ist ein Add-on zu Thunderbird, das für die automatische Ver- und Entschlüsselung von Nachrichten geschaffen wurde. Ein großes Problem bei dieser Lösung ist jedoch, dass die ein- und ausgehenden E-Mail-Adressen sichtbar bleiben und problemlos ausgelesen werden können (Wernicke, 2016).

Die beste Lösung ist die Verwendung des I2P-Browsers, der sein eigenes anonymes E-Mail-Programm I2P-Bote integriert hat, welches einen sicheren E-Mail-Versand garantiert. Generell sollte der Fokus auf einer guten Balance zwischen Anonymität und Sicherheit liegen. Thunderbird

sollte verwendet werden, wenn Sicherheit in den Mittelpunkt gestellt wird und browserbasierte Applikationen, wenn der Schwerpunkt auf der Erhöhung der Anonymität liegt (Wernicke, 2016).

Eine weitere Möglichkeit zur Erhöhung der Kommunikationssicherheit ist die Nutzung von PGP. PGP ist ein Verschlüsselungsprotokoll, das eine spezielle Form der Authentifizierung (vgl. Abbildung 17) anwendet, um eine sichere Datenkommunikation zu gewährleisten. Zu diesem Zweck erzeugt PGP einen öffentliche und einen privaten Schlüssel. Ein öffentlicher PGP-Schlüssel wird verwendet, um jede Kommunikation von dem Besitzer des öffentlichen Schlüssels zu chiffrieren. Der private PGP-Schlüssel wird darauffolgend verwendet, um jede Nachricht, die an den Besitzer des öffentlichen Schlüssels gesendet wird, zu entschlüsseln. Dieser Austausch verhindert, dass eine empfangene oder abgefangene Nachricht von einer anderen Person als dem Besitzer des privaten PGP-Schlüssels entschlüsselt werden kann. Innerhalb der Darknet-Märkte erlaubt dies den Anbietern ihren öffentlichen PGP-Schlüssel bekannt zu machen, um die Korrespondenz zu ermöglichen (Broadhurst, et al., 2018).

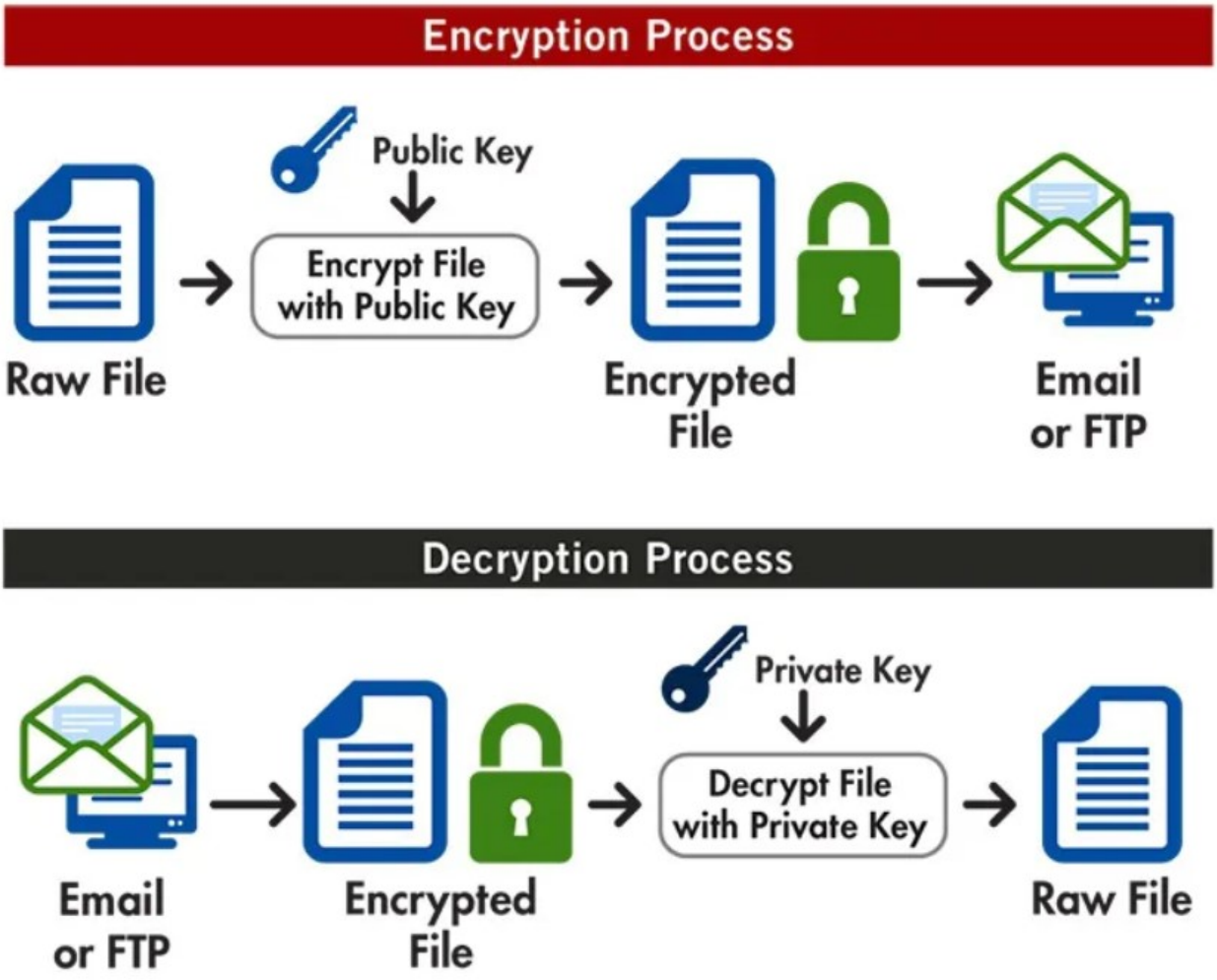


Abbildung 17: Verschlüsselung bei PGP (Mills, 2020)

Auch Instant-Messenger sind aufgrund der erhöhten Sicherheit eine wertvolle Kommunikationsform. Bei bestimmten IM-Anbietern und Protokollen werden keine historischen Daten gespeichert. Pidgin zum Beispiel ist ein universeller Open-Source-IM-Client und kann auf eine Reihe von Chaträumen gleichzeitig zugreifen. Pidgin erreicht sieben von sieben Punkten auf

der Secure Messaging Scorecard der Electronic Frontier Foundation, wenn es zusammen mit dem OTR-Protokoll implementiert wird. Dies ist ein kryptografisches Protokoll, das eine Ende-zu-Ende-Verschlüsselung bietet. Wenn es mit einem Open-Source-IM-Client verwendet wird, ist es sehr schwierig, die mit dem OTR-Protokoll verschlüsselte Konversation abzufangen. Beim Erstellen einer IM-Identität wird außerdem empfohlen, einen verdeckten und gesicherten Browser wie TOR zu verwenden. Dies verhindert, dass die Identität des Benutzers enthüllt wird und hilft sich vor dem Abhören zu schützen (Wernicke, 2016).

5.2 Schutz der Software

Antimalware- und Antiviren-Schutz ist ebenso wichtig, um zu verhindern, dass böswillige Akteure legitime Darknet-Besucher ausnutzen. Das Darknet ist überfüllt mit gestohlenen Daten von Benutzern, welche mit einer Malware infiziert wurden. Angreifer können Tools wie Keylogger verwenden, um Daten zu sammeln und das System auf jedem Teil des Webs zu infiltrieren. Der Schutz vor Attacken gefährlicher Malwarestellt somit einen wichtigen Faktor bei der Nutzung von Darknet dar.

Angesichts der zunehmenden Bedrohung durch Cyberangriffe benötigen Darknet-Nutzer neue Tools, Techniken und Ansätze, um ihre Software zu schützen. Leider sind die kriminellen Innovationen oft schneller als die Verteidigungsbemühungen. Im April 2019 registrierte das AV-Test Institute, eine auf IT-Sicherheit spezialisierte Forschungseinrichtung, mehr als 350.000 neue Malware-Samples pro Tag. Laut dem 2019 Internet Security Threat Report von Symantec haben Cyberangriffe, die auf Schwachstellen in der Lieferkette abzielen, im Jahr 2018 um 78% zugenommen (Huang, Siegel, Pearlson, & Madnick, 2019).

Auch breit angelegte Angriffe werden immer häufiger. Im Oktober 2016 legte ein DDoS-Angriff, Unternehmen wie Netflix, PayPal, Reddit, Twitter, Spotify und Amazon lahm. Im Jahr 2017 betrafen die Ransomware-Angriffe “WannaCry“ und “NotPetya“ das Gesundheitswesen, das Bildungswesen und andere Sektoren auf der ganzen Welt. Aus einem Bericht des britischen Gesundheitsministeriums geht hervor, dass die Beseitigung von Konsequenzen des “WannaCry“-Angriffes insgesamt 92 Millionen Pfund gekostet hat. Im selben Jahr, als die Cyberverteidigungs-Community herausfand, wie man Ransomware bekämpfen kann, tauchte Cryptojacking, die Entführung fremder Rechner zum Mining von Kryptowährung, als Bedrohung auf. Die von Symantec entdeckten Cryptojacking-Angriffe stiegen im Jahr 2017 um 8.500%. Im Jahr 2018 fiel der Wert von Kryptowährungen um 90%, dennoch blockierte Symantec viermal so viele Cryptojacking-Angriffe wie im Vorjahr (Huang, Siegel, Pearlson, & Madnick, 2019).

> *„Eine weitverbreitete Art von Schadprogrammen ist die sogenannte Ransomware. Diese verschlüsselt die Daten des infizierten IT-Systems sowie häufig auch weitere Daten, die etwa über Netzfreigaben erreichbar sind. In der Regel verwenden die Angreifer dabei Verschlüsselungsmethoden, die ohne Kenntnis des Schlüssels nicht umkehrbar sind, und erpressen damit ihre Opfer um hohe Geldsummen. Besteht kein wirksamer Schutz gegen Schadprogramme und sind keine ergänzenden Vorkehrungen wie Datensicherungen getroffen, kann die Verfügbarkeit von*

Informationen erheblich eingeschränkt, Daten verloren gehen, sowie massive finanzielle und Image-Schäden eintreten“
(Bundesamt für Sicherheit in der Elektrotechnik, 2021).

Nachdem die Gefahr, welche durch Malware, Hackerangriffe und weitere Formen von Attacken verursacht wird, groß und allgegenwärtig ist, wird jedem Besucher des Darknets empfohlen, seine Software und Daten gegen Schadsoftware mit zusätzlichen Mitteln zu schützen. Bereits durch das regelmäßige Ausführen von Sicherheitsupdates sowie durch die Aktivierung der Firewall wird die Sicherheit der Software immens erhöht. Ein aktueller Virenscanner sollte zusätzlich installiert und reguläre Checks ausgeführt werden (Frickel, 2016).

Virenscanner sind von dem Betriebssystem der Ziel-Hardware abhängig. Für diese Arbeit sind die Betriebssysteme Windows und Linux von Bedeutung, deswegen werden in den nächsten Schritten die Virenscanner für diese zwei Betriebssysteme diskutiert.

Im Januar 2021 wurde ein Virenscanner-Test für Programme, welche unter Windows laufen können, durchgeführt (siehe Abbildung 18). Die Virenscanner wurden nach dem schulischen Benotungssystem bewertet. Die ausschlaggebenden Charakteristiken waren der Preis, die Gesamtbewertung, die Schutzwertung, die Performance sowie das Handhaben von Fehlalarmen (Geiger, 2021).

DIE BESTEN VIRENSCANNER IM TEST

	Testsieger	Preistipp / 2. Platz	Preistipp / 3. Platz	Bester Schutz / 4. Platz
Produktname	Kaspersky Antivirus Pro	Avast Free Antivirus	AVG Free Antivirus	F-Secure SAFE
				
Preis	ca. 26 Euro	kostenlos	kostenlos	ca. 23 Euro
Gesamtwertung	sehr gut (1,2)	sehr gut (1,5)	sehr gut (1.5)	gut (1,6)
Schutzwertung	sehr gut (1,4)	sehr gut (1,3)	sehr gut (1,3)	sehr gut (1,0)
Performance	sehr gut (1,0)	sehr gut (1,4)	sehr gut (1,4)	sehr gut (1,1)
Fehlalarme	sehr gut (1,1)	gut (2,3)	gut (2,3)	ausreichend (3,7)

Abbildung 18: Virenscanner-Test 2021 (Geiger, 2021)

Am besten hat sich der Kaspersky Antivirus Pro platziert. Dennoch konnte Kaspersky nicht alle Virenangriffe im Test unter realen Bedingungen unbeschadet überstehen. Bis auf drei konnten alle der 1509 Angriffe erfolgreich entdeckt und blockiert werden. Eine übermäßige Systembelastung muss bei diesem Virenscanner nicht befürchten werden, vor allem schwächere PCs werden im Vergleich zu anderen Programmen kaum ausgebremst, was einen immensen Vorteil gegenüber anderen Anbietern darstellt. Insgesamt kam es zu nur zwei Fehlalarmen, was bei einem Testumfang von insgesamt 10.102 Testfällen gut vertretbar ist (Geiger, 2021).

Bei Avast Free Antivirus handelt es sich um den zweitbesten Virenscanner, der zudem ohne weitere Kosten eingesetzt werden kann. In Bezug auf die Systembelastung wird diese Lösung jedoch besonders im Hinblick auf ältere oder weniger leistungsstarke Geräte nicht empfohlen. Auf leistungsstarken Rechnern sollte die Arbeitsgeschwindigkeit jedoch nicht merklich gebremst werden. Ein weitaus schlechteres Ergebnis erzielte der Virenscanner bei Fehlalarmen. Im Test erfasste er 18 fälschliche Hinweise auf Bedrohungen, die keine Bedrohung signalisierten (Geiger, 2021).

AVG Free Antivirus hat sich in dem Virenscanner-Test auf dem dritten Platz positioniert. Nachdem dies eine weit verbreitete und oft eingesetzte Lösung ist, reicht es auch, das Programm aktuell zu halten, um den bestmöglichen Schutz zu erzielen. Auch bei der Bewertung von Fehlalarmen und der Performance hat der AVG Free Antivirus ein gutes Ergebnis erreicht. Doch zum großen Teil (50 %) liegt das an der Schutz-Wertung. Im Test wurden letztendlich vier Infektionen übersehen. Im Datei-Scan-Test präsentiert AVG Free Antivirus eine höchstmögliche Schutzrate (Geiger, 2021).

Der F-Secure SAFE ist, laut der Bewertung von Herrn Geiger aus dem Jahr 2021, ein Sicherheitstipp, denn dieser Virenscanner ließ im Testszenario keine Bedrohungen passieren. Der vierte Platz in der Statistik ist leider den schlechten Ergebnissen bei den häufigen Fehlalarmen zuzuschreiben. Insgesamt wurden leider ganze 53 Fehlalarme ausgelöst. In den Sachen Performance gibt F-Secure dennoch ein ausgezeichnetes Bild ab, kein anderer Virenschutz hat so wenig Einfluss auf die Leistung eines neueren Gesamtsystems. Beim Test entwischt diesem Virenscanner nur ein einziger Angriff. Das ist eine Spitzenleistung in Sachen Schutz, bei einer so hohen Anzahl an Fehlalarmen ist dies für User aber störend bis beunruhigend. (Geiger, 2021).

Unter Linux wird kein zusätzlicher Virenscanner benötigt, da das Betriebssystems schon ein sehr umfangreiches Sicherheitskonzept mit sich bringt und nur wenig Schadsoftware im Umlauf ist, welche explizit für Linux konzipiert wäre. Nichtsdestotrotz wird auch trotz dieses Faktes eine Vielzahl an Virenscannern für Linux angeboten, die sich beispielsweise auf Dateiservern als nützlich erweisen, die auch bei anderen Betriebssystemen wie Windows ihren Einsatz finden (Geiger, 2015).

Ähnlich wie bei Windows fallen beim Erwerb der besten Virenschutzlösungen auch unter Linux hohe Kosten an. Bei den Desktop-Lösungen stellt sich ESET NOD32 Antivirus for Linux mit 99,8% Erkennung bei der Windows-Malware und 99,7% Erkennung bei den Linux-Viren als sehr wirksam heraus. Beim speziellen File-Server-Schutz führt wiederum das Schutzprogramm von Kaspersky. Kaspersky Anti-Virus for Linux File Server erkennt insgesamt 99,8% der Windows-Malware und 98,8% der Linux-Schadprogramme. Symantec Endpoint Protection Manager brilliert bei Windows-Malware, wo er 100% an Viren erkennt, schafft aber bei Linux-Viren nur 97,2%. Kaspersky Endpoint Security dagegen erkennt alle Linux-Schadprogramme, erreicht aber eine Erkennungsrate von nur 96,3% bei Windows (Geiger, 2015).

6 TOR-NETZWERK

Die meisten Darknet-Inhalte finden sich im TOR-Netzwerk, auf welches über den TOR-Browser zugegriffen werden kann. TOR ist ein Netzwerk aus verschlüsselten, virtuellen Tunneln, welche es Anwendern erlaubt, das Internet anonym zu nutzen, indem deren Identität sowie Netzwerkverkehr verschleiert werden. Mit dem Einsatz von hidden-service Protokoll ermöglicht es TOR seinen Nutzern auch anonym Websites zu hosten, die nur für diejenigen zugänglich sind, die sich im TOR-Netzwerk befinden (Kumar & Rosenbach, 2019).

Das TOR-Netzwerk ist die Abkürzung für „The Onion Router“ (der Zwiebel-Router), da es viele Verschlüsselungsebenen bzw. Schichten gibt, die den Informationsaustausch schützen. TOR lebt am Rande des Internets und dient als zugrundliegende Technologie für das Darknet (Kumar & Rosenbach, 2019).

Der Onion Router ist ein virtuelles Computernetzwerk, welches die Analyse des Netzwerkverkehrs verhindert und es den Benutzern daher ermöglicht, Informationen im Internet mit fast vollkommener Anonymität zu veröffentlichen und durchzusuchen. Es erlaubt den Benutzern Zensur und Netzwerkfilter zu umgehen sowie den Zugang zu versteckten Darknet-Ressourcen. Es ist also ein Werkzeug, das je nach den Absichten des Benutzers für legale Zwecke oder für illegale Aktionen und in Extremfällen für brutale Verbrechen genutzt werden kann. Unabhängig von der Häufigkeit sowie vom Ausmaß solcher illegalen Aktionen ist die Wahrscheinlichkeit, den tatsächlichen Täter zu identifizieren, sehr gering, was für die Wirksamkeit der Sicherheitsmaßnahmen spricht (Nastuła, 2020).

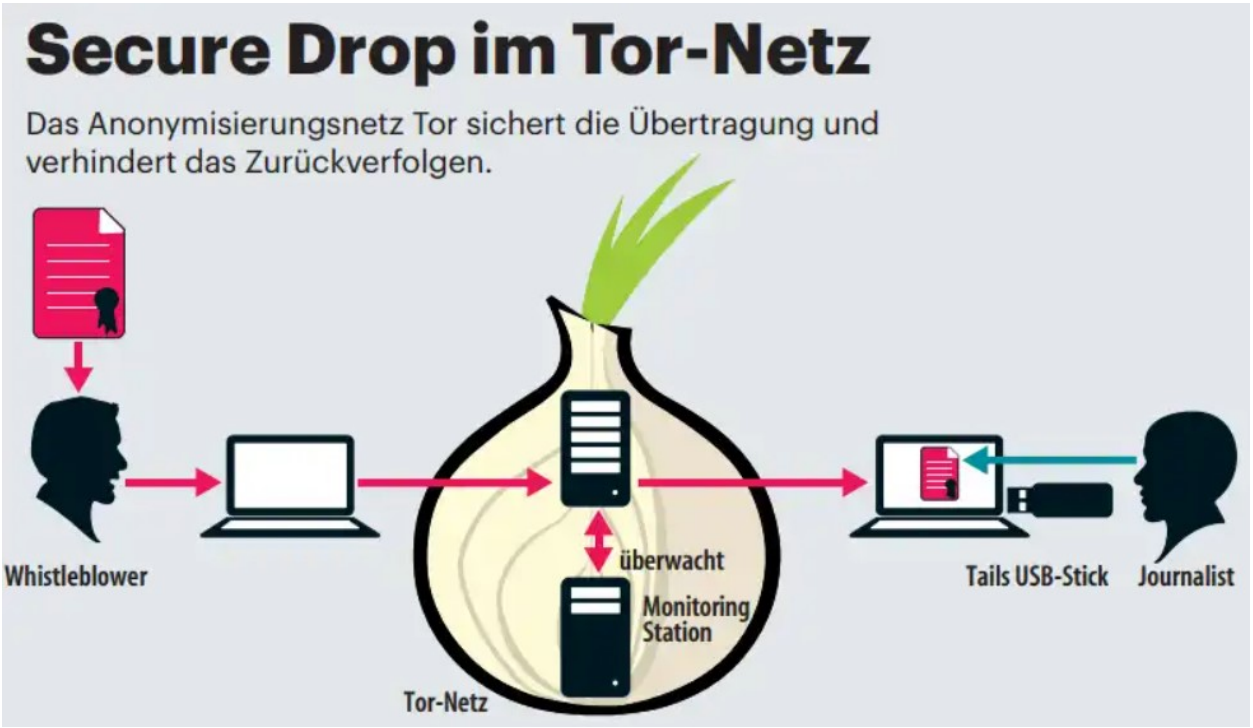


Abbildung 19: Sichere Datenübertragung im TOR-Netzwerk (Schmidt, 2016)

Somit wird nicht nur die Kommunikation zwischen Parteien geschützt, sondern auch eine sichere Datenübertragung, wie sie in Abbildung 19 zu sehen ist, sichergestellt (Schmidt, 2016).

6.1 Geschichte

"The Onion Routing Program" war ein Projekt, das ursprünglich Mitte der 1990er Jahre von zwei Mitarbeitern des United States Naval Research Laboratory entwickelt wurde: dem Mathematiker Paul Syverson und den Informatikern Michael G. Reed und David Goldschlag (Goldschlag, Reed, & Syverson, 1996). Das Programm wurde entwickelt, um die damit abgewickelte Kommunikation vor der Regierung zu schützen. In den Jahren 2004-2005 wurde das Projekt von der Non-Profit-Organisation "Electronic Frontier Foundation" weitergeführt. Diese Organisation hat es sich zur Aufgabe gemacht, die bürgerlichen Freiheiten in der digitalen Welt zu verteidigen und sich für Menschenrechte zu engagieren (Nastuła, 2020).

Das Hauptziel des Projekts war die Trennung von Identifikationsinformationen des Routings und der Entwurf eines anonymen Kommunikationsnetzwerks für die militärische Kommunikation. Nach öffentlicher Bekanntgabe wurde dieses Netzwerk stets untersucht sowie umfangreiche Forschungen durchgeführt, was zu verschiedenen Überarbeitungen des Projekts führte (Syverson, 2011).

Seit 2006 wird die Entwicklung der Software und die Popularisierung des Projekts von einer gemeinnützigen Forschungs- und Bildungsorganisation namens "The TOR Project" betreut. Die Organisation hat ihren Hauptsitz in den USA. Sie sammelt Gelder nicht nur von internationalen privaten Spendern, sondern auch von öffentlichen Quellen (einschließlich der Regierungen von beispielsweise USA, Schweden oder Deutschland), internationalen Organisationen (z.B. The Human Rights Watch), Universitäten, Forschungszentren und Unternehmen (einschließlich Google und Mozilla) (Nastuła, 2020).

Die Haltung bestimmter Regierungen gegenüber dem TOR-Netzwerk kann in einigen Fällen extrem sein. Einige Länder, darunter die Vereinigten Staaten, unterstützen die Entwicklung des TOR-Netzwerks. Tatsächlich deuten Informationen aus dem Jahr 2014 darauf hin, dass die US-Regierung offiziell Schritte unternommen hat, um zur Stärkung des Netzwerks beizutragen, indem sie auf seine potenziellen Fehler und Schlupflöcher hingewiesen hat. Im Gegensatz dazu verurteilen andere Regierungen wie die von Saudi-Arabien, den Vereinigten Arabischen Emiraten und dem Irak offen den Betrieb des TOR-Netzwerks und blockieren seine Seiten und den Zugang zu den Zugangsknoten. Interessanterweise hat das russische Innenministerium im Jahr 2014 in einem Wettbewerb 110.000 Dollar angeboten, um einen Weg zu finden, die Identitäten der Nutzer des TOR-Netzwerks zu knacken. Der Wettbewerb war nur für russische Bürger gedacht. Dieses große Interesse der Behörden am TOR-Netzwerk war auf zwei Tatsachen zurückzuführen. Erstens hat das Unterhaus des russischen Parlaments ein Gesetz verabschiedet, das Internetfirmen verpflichtet, persönliche Daten russischer Bürger im Land zu speichern. Zum anderen begannen regierungsfeindliche Akteure das TOR-Netzwerk für ihre interne Kommunikation zu nutzen. Länder, in denen das Internet stark zensiert wurde, wie Venezuela

oder China, haben TOR und ähnliche Technologien, einschließlich virtueller privater Netzwerke verboten (Nastuła, 2020).

6.2 Allgemeine Funktionsweise

Das Wesen des TOR-Netzwerkbetriebs basiert auf dem Prinzip der mehrfachen Datenverschlüsselung und ihrer Übertragung durch mehrere Netzwerkknoten, die Router oder Zwiebelknoten genannt werden (siehe Abbildung 20). Der Zugang zum Netzwerk beginnt mit dem Herunterladen und Installieren des TOR-Browsers, der optisch einer modifizierten Version von Mozilla Firefox ähnelt und auch in mehreren Sprachen für Windows, Linux, und Mac verfügbar ist. Verschlüsselte Informationspakete durchlaufen aufeinanderfolgende Onion-Router, die jeweils eine Schicht der Verschlüsselung entfernen, um die Adresse des nächsten Verkehrsknotens zu erreichen und das Datenpaket weiterzuleiten. Die Software, welche die Internetverbindung herstellt, kann das TOR-Netzwerk über die SOCKS-Schnittstelle nutzen. Der letzte Knoten, der als Ausgangsknoten bezeichnet wird, ist das "schwächste Glied" des TOR-Netzwerks, da die zwischen dem Ausgangsknoten und dem Zielserver übertragenen Informationen nicht verschlüsselt sind. Das TOR-Netzwerk wird von einigen Benutzern des Netzwerkes selbst entwickelt, die die Knoten-Server erstellen. Die Herausgeber des TOR-Netzwerks betonen, dass dieses Tool nicht alle Probleme im Zusammenhang mit der Anonymität im Internet löst und empfehlen einen zusätzlichen technologischen Schutz, der parallel zum TOR-Browser verwendet werden sollte (Nastuła, 2020).

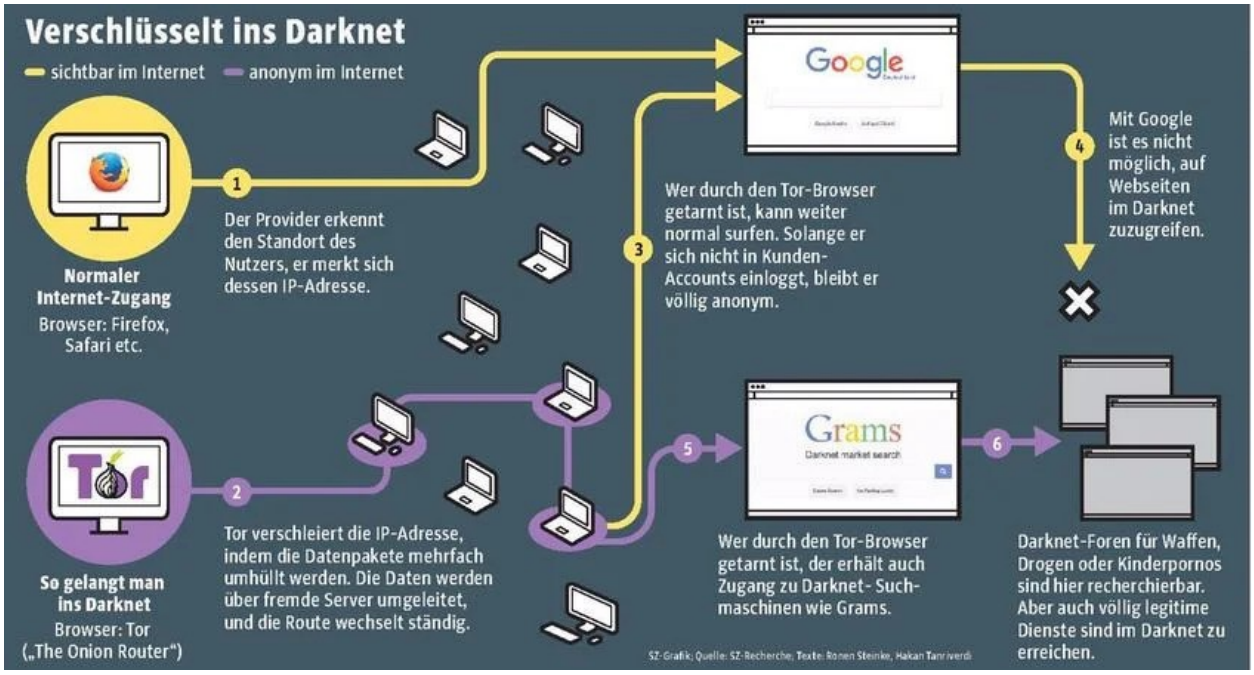


Abbildung 20: Funktionsweise TOR (Tanriverdi, 2017)

6.2.1 Surfen im TOR-Netzwerk

Jeder Internetnutzer, der auf beliebige Inhalte aus dem Darknet zugreifen will, wird keine expliziten Schlüsselwörter in einem Standard-Browser eingeben, sondern muss anonym mit dem TOR-Browser zugreifen, der seine Identität verschleiert, darunter z. B. die IP-Adresse oder den physischen Standort. Aus diesen Gründen ist es schwierig für Strafverfolgungsbehörden oder digitale Forensiker den Ursprung des Datenverkehrs, den Standort oder die Eigentümer eines Computers sowie weitere Informationen zur Identifizierung der realen Person im Darknet zu ermitteln (Rathod, 2017).

> *"TOR is the most popular browser used to access the darknet and allows users to access domains with the '.onion' suffix" (Broadhurst, et al., 2018).*

Aufgrund ihres Designs und der mehrfachen Verschlüsselung sind TOR-Seiten puristisch ansprechend, aber der Browser selbst arbeitet viel langsamer als herkömmlich bekannte Browser im World Wide Web (wie beispielsweise Chrome oder Firefox). Die URL von Seiten im TOR-Netzwerk, das von seinen Nutzern oft als "Onionland" bezeichnet wird, besteht aus einer Folge von 16 zufälligen Buchstaben und Zahlen, die mit der Onion-Domain endet. Die Onion-Domain befindet sich hinter einer zusätzlichen Firewall und ist vor der Network Address Translation (NAT) versteckt, einem Dienst, der die Adresse einer Seite in eine besser lesbare Adresse umwandelt. Eine solche Lösung bewirkt, dass nur Benutzer, die die Adressen bestimmter Seiten kennen, Zugriff auf die Inhalte haben. Auch Suchmaschinen für versteckte Seiten wie The Hidden Wiki, notEvil, TORCH oder DuckDuckGO bieten Hilfe bei der Orientierung im Darknet an (Nastuła, 2020).

TOR besteht aus einem globalen Overlay-Netzwerk von Schichten, das bei der Erreichung von Privatsphäre und Anonymität für den Internetverkehr der Benutzer hilft. Für jede Kommunikation erstellt das TOR-Netzwerk einen virtuellen Kreislauf aus mindestens drei aufeinanderfolgenden, zufällig ausgewählten Schichten. Die Informationen über die Schichten werden von dem TOR-Client am Quellrechner von einem Verzeichnisserver heruntergeladen. Verschlüsselungsschlüssel werden mit den ausgewählten Servern unter der Verwendung eines Schlüsselaustauschprotokolls ausgewechselt (Jadoon, Iqbal, Amjad, Afzal, & Bangash, 2019).

Auf dem Quellknoten werden die Datenpakete mehrfach verschlüsselt, einmal für jeden Schichtenknoten mit dem Verschlüsselungsschlüssel des jeweiligen Knoten, bevor die Pakete an ihr Ziel weitergeleitet werden. Daher wird die äußerste Schicht der Verschlüsselung vom Eingangsknoten entschlüsselt, während die innerste Schicht der Verschlüsselung für den Ausgangsknoten zum Entschlüsseln bestimmt ist. Jeder Schichtenknoten entschlüsselt das empfangene Paket mit seinem eigenen Entschlüsselungsschlüssel, um die Adresse des nächsten Hops für das empfangene Paket zu ermitteln. Auf diese Weise hat jeder TOR-Knoten das Wissen über die Schichtenknoten, die nur einen Schritt von ihm entfernt sind (Jadoon, Iqbal, Amjad, Afzal, & Bangash, 2019).

Am Ausgangsknoten wird die innerste Schicht der Verschlüsselung entschlüsselt und das unverschlüsselte Datenpaket wird in dieser Form an sein endgültiges Ziel weitergeleitet. So bleibt

die Privatsphäre der Daten des Benutzers bis zum letzten Hop erhalten. Im Falle von https über das Tor-Netzwerk, werden die Daten zwischen dem letzten Hop und dem Ziel ebenfalls verschlüsselt. Außerdem ändert der TOR-Browser alle zehn Minuten seinen Pfad, um die Anonymität der Benutzer zu gewährleisten (Jadoon, Iqbal, Amjad, Afzal, & Bangash, 2019).

Die Anonymität wird im Tor-Netzwerk außerdem verstärkt, indem die Schichtenknoten des Overlays keine Kenntnis über die Vorgänger- und Nachfolger-Knoten im gesamten virtuellen Kreislauf haben. Um die Anonymität weiter zu erhöhen, wird jeder neue virtuelle Kreislauf mit einem neu ausgewählten Satz von Schichtenknoten aufgebaut (Jadoon, Iqbal, Amjad, Afzal, & Bangash, 2019).

Die Hauptzahlungsmethode im TOR-Netzwerk sind Kryptowährungen und unter ihnen die am häufigsten verwendete - Bitcoin. Kryptowährungen haben immens an Popularität gewonnen. Der Grund dafür ist deren dezentraler, sicherer und anonymer Charakter, der durch die Peer-to-Peer-Architektur unterstützt wird und die Übertragung von Geldmitteln und anderen digitalen Vermögenswerten zwischen zwei verschiedenen Personen ohne einen zentralen Emittenten ermöglicht. Bitcoin-Zahlungen sind seit dem im Jahr 2011 von Ross Ulbricht gegründeten Silk-Road-Forum im TOR-Netzwerk populär geworden, auf dem Drogen, Kinderpornografie, Sprengstoff, Massenvernichtungswaffen, gestohlene Zahlungskarten und Auftragsmorde angeboten wurden. Die Plattform wurde als "Drogen-Amazon" bezeichnet. Es wird geschätzt, dass der Umsatz auf Silk Road über neun Millionen Bitcoins betrug, was etwa einer Milliarde Dollar entspricht. Im Jahr 2013 führte ein Routinefehler der Administratoren des Forums zu dessen Beschlagnahmung und Schließung durch das FBI, was diese Art von Aktivitäten im TOR-Netzwerk jedoch nicht stoppte. An seiner Stelle wurden andere internationale Schwarzmärkte geschaffen. Es wird angenommen, dass Bitcoin vom Gründer der Silk Road Ross Ulbricht geschaffen wurde. Laut dem Bericht über Krypto-Kriminalität, der im Januar 2019 von "Chainalysis", einem Unternehmen, das sich mit Blockchain-Analysen beschäftigt, veröffentlicht wurde. Im Jahr 2018 lag das Gesamtvolumen des Handels auf dem Schwarzmarkt auf dem Niveau von 600 Mio. USD und am Ende des Jahres lag es bei über 2 Mio. USD pro Tag (Nastuła, 2020).

6.2.2 Ausbreitung und Größe vom TOR-Netzwerk

Das TOR-Netzwerk soll in erster Linie ein Ort für den freien Austausch von Ideen und Meinungen sein, sowie ein Raum, der frei von Manipulation ist und einen sicheren und anonymen Zugang zur Wahrheit gewährleistet. Diese Slogans sind Teil der Aktivitäten von internationalen Menschenrechtsorganisationen, darunter Human Rights Watch, Global Voices und Reporter ohne Grenzen. Diese Organisationen empfehlen die Nutzung des TOR-Netzwerks. Auch Privatpersonen entscheiden sich für die Nutzung des TOR-Netzwerks, da sie Angst um ihre Privatsphäre, Identitätsdiebstahl, Fehlinformationen und die Einschränkung der Privatsphäre seitens staatlicher Stellen und internationaler Konzerne haben (Nastuła, 2020).

Beamte der Polizei und anderer Strafverfolgungsbehörden, des Militärs oder spezieller Dienste, wie ursprünglich von den Schöpfern des TOR-Netzwerks beabsichtigt, nutzen es zur Sicherung und Übermittlung von Informationen, die sie durch operative Tätigkeiten erhalten haben. IT-

Sicherheitsanalytiker und -Manager nutzen das TOR-Netzwerk auch, um die Vertraulichkeit der Netzwerkkorrespondenz zu gewährleisten oder die Wirksamkeit implementierter Firewall-Systeme zu testen (Nastuła, 2020).

Der Preis für kostenlose Dienste im Surface Web ist die Kontrolle durch Konzerne, die aus offensichtlichen finanziellen Gründen und oft auch aufgrund politischer Ziele Profile erstellen und Informationen bestimmter Benutzer aussuchen. Unbegrenzte Auswahl und freier Zugang zum gesamten Wissensspektrum ist bereits eine Illusion. Deshalb ist das TOR-Netzwerk ein wichtiges Werkzeug für Journalisten, Kriegsberichterstatter oder auch Mitarbeiter von Sicherheitsdiensten, für die es sowohl aus ideologischen als auch aus Sicherheitsgründen wichtig ist, an verlässliche, transparente und zuverlässige Informationen zu gelangen. In vielen totalitären Ländern, in denen Regierungen den Zugang der Bürger zur unbegrenzter Kommunikation einschränken, ermöglicht das TOR-Netzwerk, diese Blockaden zu umgehen und mit der demokratischen Welt, freien und unabhängigen Medien und unzensierter Literatur in Kontakt zu treten (Nastuła, 2020).

In Ägypten nutzten während des Arabischen Frühlings tausende von Bürgern den TOR-Browser, um trotz der strengen Internetbeschränkungen des Regimes von Hosini Mubarak Informationen auszutauschen. Ebenso nutzten die Rebellen im konfliktgeplagten Syrien, die über das Internet digitale Beweise für die Verbrechen des Regimes offenlegen wollten, das TOR-Netzwerk als Werkzeug für die freie Kommunikation (Nastuła, 2020).

Im Jahr 2010 zeichnete die Free Software Foundation das TOR-Netzwerk in der Kategorie "Public Benefit Design" für seinen Beitrag zu Whistleblower-Aktivitäten, Menschenrechtskampagnen und den Aktivitäten von Dissidentenbewegungen aus. Die Stiftung begründete den "Award for Projects of Social Benefit" wie folgt: *"TOR hat es etwa 36 Millionen Menschen auf der ganzen Welt ermöglicht, Zugangs- und Meinungsfreiheit im Internet zu erfahren, während sie gleichzeitig die Kontrolle über ihre Privatsphäre und Anonymität behalten. Das Netzwerk hat sich als Dreh- und Angelpunkt für die Dissidentenbewegungen im Iran und in jüngster Zeit in Ägypten erwiesen“* (Sullivan, 2011).

Revolutionäre nutzen das TOR-Netzwerk auch zur Selbstorganisation, ohne Angst vor Eingriffen durch die Behörden, gegen die sie in Opposition stehen. Es ist auch ein Werkzeug für Aktivisten, Whistleblower und Menschen, die für Freiheit und Bürgerrechte kämpfen. Ein Beispiel dafür war die Aktion des Mauretaniers Nasser Weddady, der über das TOR-Netzwerk den Kampf gegen die in Mauretanien praktizierte Sklaverei begann (Nastuła, 2020).

Laut dem letzten Bericht von TOR metrics (TOR Project, kein Datum) gibt es mehr als 2,5 Millionen aktive TOR-Benutzer mit über 6000 Knoten, die ihren Datenverkehr übertragen und 25,5 Gbit/s Bandbreite für das TOR-Netzwerk. Der TOR-Browser ist der einfachste Weg, sich mit dem TOR-Netzwerk zu verbinden, um den Datenverkehr der Nutzer weiterzuleiten. TOR-Browser ist eine modifizierte Version von Mozilla Firefox mit einigen zusätzlichen Funktionen zur Erhöhung der Anonymität und Privatsphäre. Einige dieser Funktionen sind der TOR-Launcher, TOR-Button und HTTPS-Everywhere. Standardmäßig ist Browsing für den privaten Modus konfiguriert, mit der Option, die Browseraktivitäten und die damit verbundenen Artefakte wie Cookies und andere Daten nach dem Schließen des Browsers zu löschen (Jadoon, Iqbal, Amjad, Afzal, & Bangash, 2019).

Seit 2018 ist es viel einfacher, das TOR-Netzwerk auch auf Smartphones zu nutzen. Eine Reaktion auf die Marktnachfrage war der Testdienst in Form von Onion3G-SIM-Karten der englischen Firma Brass Horn Communications, der automatisch alle mobilen Daten über das TOR-Netzwerk verwaltet und keine zusätzliche Konfiguration erfordert. Die Karte ist Prepaid und kann also jederzeit mit Kreditkarte oder Kryptowährung aufgeladen werden (Nastuła, 2020).

6.3 Nachteile und Risiken des TOR-Netzwerks

Die Bereitstellung von umfassender und fehlerfreier Anonymität steht im Zentrum der akademischen Forschung und technischen Diskussion. Aus technischer Sicht mag das Design der TOR-Architektur so aussehen, als ob es dieses Ziel erreichen kann, aber es gibt viele Probleme, die das System anfällig für Fehler und Malfunktionen macht. Die Ursachen können sehr unterschiedlich sein. In manchen Fällen handelt es sich um einen Nutzungsfehler, in anderen entstehen Probleme durch das Onion-Routing oder es handelt sich um indirekte Probleme, die die Erfolgsrate des Systems beeinflussen (Çalışkan, Minárik, & Osula, 2015).

TOR ist ein sehr umfangreiches und effektiv entwickeltes Projekt. Die Ergebnisse mancher Studien zeigen aber leider, dass es einige Möglichkeiten gibt, die wahren Identitäten von TOR-Benutzern aufzudecken. Einige dieser Techniken sind leicht durchzuführen, besonders die, die aus Benutzerfehlern entstehen. Andere benötigen fortgeschrittene technische Fähigkeiten und viel Zeit. Einige dieser Angriffe können IP-Adressen aufdecken, während andere zeigen, was TOR-Benutzer zu einem bestimmten Zeitpunkt tun und erfordern Ableitungen sowie Schätzungen, um die Person zu finden. Diese Bedrohungen können standardmäßige Benutzerfehler sowie TOR-bezogene Probleme sein (Çalışkan, Minárik, & Osula, 2015).

6.3.1 Schwachstellen in der Umsetzung

Es ist sehr üblich, dass Nutzer beim Surfen im Internet beliebige Dokumente sowie Grafiken zur näheren Betrachtung öffnen oder Browser-Erweiterungen aktiv einsetzen. Im TOR-Browser können solche Aktionen jedoch die Funktionsweise des Systems stören und im schlimmstmöglichen Fall sogar die reale IP-Adresse des Nutzers offenbaren. Die Ursache für diese Malfunktion liegt im Handlungsmechanismus von TOR (Çalışkan, Minárik, & Osula, 2015).

TOR wurde so konzipiert, dass eine Kommunikation nur zwischen den jeweiligen Schichten ermöglicht wird, bevor der Ausgangsknoten erreicht wird. Beim Ausführen von Dateien, welche in Dokumenten eingebettet sind oder einen Teil der Grafik darstellen wird diese Kommunikationskette zwischen den TOR-Schichten unterbrochen und eine fehlerhafte Funktionsweise ausgelöst. Dieses Fehlverhalten kann von böswilligen Akteuren ausgenutzt werden, um die tatsächlichen IP-Adressen legitimer Nutzer zu erfahren. Im Spezialfall ist die Verwendung von Torrent über TOR nicht besonders ratsam, da die bereits beschriebene Problematik auch in solchen Fällen eintreffen kann. Anwendungen, welche über Torrent Dateien zur Verfügung stellen bzw. das Teilen dieser Dateien ermöglichen, können die Einstellungen des

TOR-Browsers ignorieren und direkte Verbindungen zu anderen Nutzern herstellen (Çalışkan, Minárik, & Osula, 2015).

Des Weiteren wird behauptet, dass die Anonymität beim Surfen im TOR-Netzwerk durch die Tatsache, dass Ver- sowie Kaufaktionen mit anonymer Bezahlung über Kryptowährungen abgewickelt werden, stark steigt. Im Oktober 2014 haben Forscher der Universität Luxemburg jedoch gezeigt, dass es der Einsatz von Kryptowährungen Man-in-the-Middle-Angriffen ermöglicht, die volle Kontrolle über Informationsflüsse zwischen Nutzern zu bekommen (Biryukov & Pustogarov, 2014).

Besonders aufmerksam sollte der Nutzer sein, wenn er http- anstelle von https-Seiten besucht. Die Ausgangsknoten von TOR überprüfen zwar alle Internet-Pakete, welche sie passieren, wenn im TOR jedoch http-Seiten aufgesucht werden, wird das System anfällig für jegliche Formen von unerwünschten Überprüfungen durch Dritte (Çalışkan, Minárik, & Osula, 2015).

Einige Risiken der Nutzung von TOR sind jedoch nicht nur Malfunktionen zuzuschreiben, sondern auch dem menschlichen Versagen. Wenn ein Benutzer dazu verleitet werden kann, eine ungewöhnliche Aktion auszuführen, besteht stets das Risiko, dass dadurch seine Identität enthüllt wird. Im schlimmsten Fall können dadurch auch die Identitäten der Akteure preisgegeben werden, welche mit solch einem Nutzer interagieren (Çalışkan, Minárik, & Osula, 2015).

Die TOR-Gruppe entwickelt stets zusätzliche Sicherheitsmechanismen, sowie Funktionen und Werkzeuge, um die Nutzung von TOR zu optimieren. Trotz dieser Bemühungen gibt es Studien, welche Probleme mit der TOR Umgebung aufzeigen, wobei private Daten über die Nutzer veröffentlicht werden können (Ball, Schneier, & Greenwald, 2013).

Ein atypisches Verhalten sollte bereits eine Andeutung für eine potenzielle Attacke darstellen. Wenn TOR-Nutzer über Telekommunikationsanbieter auf dedizierte Server umgeleitet werden, kann dies bereits ein erstes Anzeichen für einen Man-in-the-Middle Angriff sein. Dies kann geschehen, indem der Verkehr zwischen einem TOR-Benutzer und dem legitimen Server abgefangen wird, obwohl diese Aktion nur für die US National Security Agency (NSA) möglich sein sollte (Schneier, 2013).

Des Weiteren wurde im Rahmen einer akademischen Forschung bewiesen, dass ein Akteur, der die Kontrolle über eines oder mehrere Kommunikationsknoten übernimmt, im Laufe von drei Monaten regelmäßiger TOR-Nutzung mit einer Wahrscheinlichkeit von über 50% die Identität anderer Nutzer enthüllen kann. Nach sechs Monaten liegt die Wahrscheinlichkeit bei bereits 80%. Dies stellt ein typisches Beispiel für sogenannte Korrelationsangriffe auf die verschlüsselten Daten in der TOR-Umgebung dar (Johnson, Wacek, Jansen, Sherr, & Syverson, 2013).

Im Jahr 2002 wurde eine weitere berühmte Angriffstechnik bekannt, welche sich große Peer-to-Peer-Netzwerke ins Visier nimmt, der sogenannte Sybil-Angriff. Demnach soll es möglich sein, die Systeme von Peer-to-Peer-Netzwerken, auch im Falle des TOR-Netzwerks, durch das Fälschen von Identitäten zu täuschen. Im Laufe der Zeit wurden jedoch Präventivmaßnahmen entworfen, um Anonymisierungsnetzwerke vor solchen Angriffen zu schützen (Chandhana & Mary, 2012), (Çalışkan, Minárik, & Osula, 2015).

Verschlüsselte Verbindungen zwischen zufällig ausgewählten Schichten sowie die stetige Aktualisierung von Schaltungen solcher Schichten im Abstand von zehn bis 15 Minuten sind nur einige der Sicherheitsvorkehrungen, die TOR seinen Nutzern zur Verfügung stellt und somit die sichere Nutzung gewährleistet. Versteckte TOR-Brücken werden verwendet, um das TOR-Netzwerk zu erreichen und stellen somit einen wichtigen Bestandteil des Anonymisierungsmodells von TOR dar. Nichtsdestotrotz müssen aber auch indirekte Probleme in Kauf genommen werden, welche die Privatsphäre der Benutzer von TOR beeinträchtigen, beispielsweise die Sicherheitslücken im TOR-Browser (Çalışkan, Minárik, & Osula, 2015).

Der TOR-Browser wirkt mit dem Angebot einer datenschutzfreundlichen Online-Kommunikation auf eine Vielzahl von Internet-Anwendern sehr attraktiv. Dieser Browser bietet zwar viele Chancen für seine Nutzer, weist aber auch zahlreiche Schwachstellen auf. Im Wesentlichen basiert der TOR-Browser auf Firefox mit spezifischen Konfigurationen, welche jedoch Freiraum für diverse kritische Schwachstelle schaffen. Hierbei handelt es sich um kein direktes Problem der TOR-Architektur. Die Schwachstelle bringt nichtsdestotrotz jeden TOR-Nutzer in Gefahr. Ein erfolgreicher Angriff könnte die Ausführung von beliebigem Code auf dem Computer des Opfers ermöglichen. Nicht nur die Privatsphäre des Angegriffenen, sondern auch seine Hardware können durch diese Art von Angriffen kompromittiert werden (Çalışkan, Minárik, & Osula, 2015).

Eine weitere Gefahr in der Online-Welt stellt der Heartbleed-Bug dar, der sich eine schwerwiegende Sicherheitslücke in der populären kryptografischen Softwarebibliothek OpenSSL zum Nutzen macht. Diese Schwachstelle führte zur Enthüllung von geheimen Informationen wie den Benutzernamen, Passwörtern und anderen kritischen Daten von Diensten, die OpenSSL im Einsatz haben. Auch zahlreiche https-Seiten wurden zu Opfern dieser Gefahr, unter anderem auch im TOR-Netz. Einige der TOR-Anwendungen und TOR-Clients waren anfällig für diese Schwachstelle, da sie die verwundbare Version von OpenSSL nutzten. Es war nicht möglich, die Situation zu lösen, indem man nur die Client-Anwendungen patcht, die eine verwundbare OpenSSL im Einsatz haben. Der Fehler beeinträchtigte auch die Kapazität der TOR-Schichten um bis zu 12%, da die Schichten, welche die Hauptkomponenten der TOR-Architektur darstellen, ebenfalls verwundbar waren. Der Schaden, den Heartbleed anrichtete, betraf TOR und seine Nutzer und ist ein gutes Beispiel dafür, wie indirekte Probleme zu ernsthaften Datenschutzproblemen für TOR-Nutzer führen können (Hern, 2014), (Çalışkan, Minárik, & Osula, 2015).

6.3.2 Missbrauch und Straftaten

Abhängig von der Intention können die Vorteile des Darknets sowohl für legale Absichten verwendet werden als auch leider für illegale Zwecke missbraucht werden. Die Anonymität trägt zur freien Meinungsäußerung bei und hilft, objektive Einschätzungen und eine verbesserte rechtliche und sogar soziale Beratung zu erreichen. Auf der anderen Seite kann die Anonymität des TOR-Netzwerks aber auch dazu führen, dass einige Straftaten leichter zu begehen sind und einen Anreiz zur Ausweitung dieser schändlichen Aktivitäten bieten, die ohne das Netzwerk nicht stattfinden würden. Darüber hinaus könnte die uneingeschränkte Anonymität zur Einschüchterung und Belästigung führen und die Meinungsfreiheit untergraben, wenn die

Belästigung andere daran hindert, sich an den öffentlichen Debatten zu beteiligen und ihre Meinung zu äußern (Nastuła, 2020).

Jamie Bartlett beschreibt das Darknet als eine seltsame Mischung aus Kriminalität und Idealismus, in dem Dissidenten-Seiten neben Drogen- und Terroristenseiten stehen und als globales Phänomen behandelt werden sollten (Bartlett, 2014). Im Darknet herrschen Freiheit und Anonymität, die es den Nutzern erlauben unzensierte Inhalte und illegale Waren oder Dienstleistungen auszutauschen. Die Anonymität bedroht die Sicherheit und erhöht die Neigung zu unangemessenem Verhalten, insbesondere wenn der Benutzer von der Abwesenheit rechtlicher Sanktionen überzeugt ist (Nastuła, 2020).

Im TOR-Netzwerk finden sich Websites, die sich auf den Handel mit illegalen Gütern wie Waffen, Drogen, gestohlenen Waren und illegalen Dienstleistungen spezialisiert haben, Kinderpornografie-Foren, Torrent-Dienste, oppositionelle und politische Hetzseiten. Der bekannteste Dienst, der die versteckten Plattformen des TOR-Netzwerks in die internationalen Wirtschaftsmärkte einführte, war die bereits erwähnte Silk Road. Der bekannteste Drogenmarkt funktionierte auf einer ähnlichen Basis wie eBay oder Amazon und ermöglichte eine anonyme Kontaktaufnahme zwischen Verkäufern und Kaufinteressenten für verbotene Substanzen aller Art. Mehrere Faktoren trugen zu dem beispiellosen Erfolg des Dienstes bei. Zunächst einmal eine sehr hohe Qualität der Drogen, die zu erschwinglichen Preisen verkauft wurden, und ein freundliches, einfaches System zur Nutzung der Website. Der entscheidende Faktor könnte aber auch die Einstellung des Schöpfers und Administrators der Seite Ross Ulbricht sein, dessen technologische, organisatorische und ideologische Lösungen ein Beispiel für die nachfolgenden Webseiten wurden, die im TOR-Netzwerk entstanden (Nastuła, 2020).

Ulbricht moderierte die Silk Road sehr genau und reagierte sofort auf alle Täuschungsversuche und Transaktionen, die den Kunden schaden könnten (Sommers & Bernstein, 2020). Nachdem die Website geschlossen wurde, entstanden an ihrer Stelle neue, darunter die populärsten Alpha Bay und Hansa, deren Betrieb 2017 ebenfalls von den Strafverfolgungsbehörden eingestellt wurde. Die wachsenden Marktbedürfnisse führen jedoch dazu, dass anstelle von geschlossenen Websites neue geschaffen werden, die sowohl Technologien als auch Anbieter und Kunden früherer Plattformen übernehmen. Die Handelsaktivitäten im TOR-Netzwerk verlagerten sich nach 2017 auf die russischsprachige Website "Hydra" und die ebenso beliebten "Dream Market" und "Wall Street Market" (Nastuła, 2020).

Im TOR-Netzwerk sind Dienste, die sich mit Hacking-Diensten beschäftigen, wie HeLLForum, Hacker Place oder Rent-A-Hacker sehr aktiv. Ein Großteil der Kommunikation der Hacking-Communities ist für die Öffentlichkeit geschlossen, und der Zugang zu den einzelnen Foren ist an eine Einladung geknüpft. Die Webseiten bieten Exploits, Trojaner, Ransomware-Generatoren oder Cybercrime-as-a-Service an. Es gibt auch zahlreiche bezahlte Angebote zur Durchführung von DDoS-Attacken. Auf Darknet-Märkten werden auch Dienste zum Diebstahl von persönlichen Daten angeboten, insbesondere von Dokumenten, die Träger von persönlichen Daten sind und als zweite Form der Authentifizierung verwendet werden können, wie z. B. Reisepässe, Sozialversicherungsnummern und sogar Stromrechnungen. Es gibt ein wachsendes Interesse und eine steigende Nachfrage nach Trainings-Tutorials, die Anleitungen für Hacker und

Kriminelle enthalten, sowie nach Anleitungen für die Organisation von Spam- und Phishing-Kampagnen. Das TOR-Netzwerk ist auch ein Ort, an dem man dem Online-Glücksspiel nachgehen kann, das in einigen Ländern, wie zum Beispiel Polen, illegal ist (Nastuła, 2020).

Pornografische Websites, insbesondere solche, die gewalttätige Kinderpornografie enthalten, werden sowohl von Gegnern als auch von Befürwortern des TOR-Netzwerks als dessen dunkelster und moralisch inakzeptabler Ort angesehen. Es gibt Diskussionen darüber, in welchem Alter es am besten ist, ein Kind zu vergewaltigen, aus welchem Land und wie man es bekommt, Beschreibungen, wie man die Körper von Toten schändet, Links zu Filmen, die bestialische Vergewaltigungen an Frauen, Kindern und Tieren enthalten. Eine der brutalsten und beliebtesten Websites war "Hurt2theCore", die in zahlreiche Foren und Kategorien unterteilt war, darunter: "Grausamkeit", "Sextouristik und Prostitution", "Hurtcore - wie man ihn zum Schreien bringt". Foren mit Bild- und Videomaterial waren in Untergruppen unterteilt: Männer, Frauen, Neugeborene, Säuglinge, Kleinkinder, Teenager und Erwachsene. Bei pornografischen und pädophilen Webseiten oder solchen, die Anleitungen und Hinweise zur sexuellen Abweichung geben, werden die Inhalte hingegen kostenlos zur Verfügung gestellt. Dies erschwert den Strafverfolgungsbehörden die Ermittlung einzelner Nutzer dieser Portale. Ein Beamter, der in einen solchen Dienst eindringen möchte, müsste daher eine Straftat begehen (Nastuła, 2020).

Neue Technologien erzeugen neue Bedrohungen, deren Folgen oft die Welt der Politik erreichen. Dies kann durch die kriminelle Welt geschehen und kann die Stabilität des Gleichgewichts der politischen Kräfte in der Welt beeinträchtigen oder gar das Gleichgewicht der politischen Macht global destabilisieren. Zu Beginn des Jahres 2018 hat die Welle der Deepfakes zugenommen, die als neue ernsthafte Bedrohung für viele Bereiche der Sicherheit angesehen werden kann. Bei Deepfakes handelt es sich um unterschiedlich manipuliertes audiovisuelles Material. Die auf künstlicher Intelligenz basierende Technologie, die von einem anonymen Benutzer mit dem Pseudonym "deepfakes" geschaffen wurde, ermöglicht es, das Gesicht aus einem Video durch ein beliebiges anderes zu ersetzen, d. h. den Inhalt von audiovisuellen Werken zu erstellen oder zu verändern (Roose, 2018).

Anfänglich wurden Deepfakes vor allem in der Pornoindustrie eingesetzt, wurden aber schnell auch für alle Arten von politischen Aktivitäten attraktiv. Die offensichtlichen Gefahren für die Authentizität der übertragenen Inhalte, ethische Aspekte und die Angst vor Missbrauch des Rufes einer Person in einem noch nie erlebten Ausmaß haben dazu geführt, dass Deepfakes von Webseiten und Portalen, auf denen sie bisher veröffentlicht wurden, im Surface Web verboten wurden. Nach den Verboten sind Deepfakes in das TOR-Netzwerk umgezogen und ihre Schöpfer arbeiten an der Verfeinerung der aufgezwungenen Bilder durch immer bessere technische Lösungen. Bedrohungen durch dieses Verbrechen treten sowohl im Strafrecht als auch im Zivil- und Wirtschaftsrecht auf. Die Opfer werden durch die Veränderung ihrer Gesichter zu Hauptdarstellern von pornografischen Filmen und können Gegenstand betrügerischer Erpressung von Geld und vertraulichen Informationen sein. Deepfakes sind auch eine potenzielle Waffe, die eingesetzt werden kann, um die Glaubwürdigkeit einer Person, die eine moralische Autorität darstellt, zu untergraben. Im Falle der Veröffentlichung von anstößigen Inhalten werden Persönlichkeitsrechte und der Ruf des Unternehmens verletzt, was dessen weitere wirtschaftliche Entwicklung bestimmen kann. Darüber hinaus scheinen Deepfakes ein ideales Werkzeug zu sein,

um falsche Beweise zur Verwendung in Gerichtsverfahren zu erstellen. Schließlich stellen sie eine ernsthafte Bedrohung für die nationale Sicherheit, die Demokratie und die Privatsphäre dar (Roose, 2018).

Nachdem zahlreiche Nutzer TOR wählen, um ins Darknet zu gelangen, denn *“TOR is the most popular browser used to access the darknet and allows users to access domains with the ‘.onion’ suffix” (Broadhurst, et al., 2018).,* wurde diese Komponente näher untersucht, um sich auf die praktische Untersuchung entsprechend vorzubereiten. Es sind zwar zahlreiche Gründe bekannt, welche von der Nutzung vom TOR-Browser und dem Besuch von .onion-Seiten abraten, die ausführliche Recherche hat jedoch effektiv zur Risikominimierung beigetragen, sodass die Autorin für einen Ausflug ins Darknet mit TOR bereit ist. Die zahlreichen Vorteile werden ausgenutzt und die bekannten Gefahren gemieden.

7 PRAKTISCHE UNTERSUCHUNG

Alle Erkenntnisse aus vorherigen Kapiteln werden nun eingesetzt, um eine reale Nutzung des Darknets vorzubereiten und darauffolgend durchzuführen. Einer passenden Vorbereitung wird eine große Bedeutung zugeschrieben, da diese eine Vielzahl an Risiken minimieren oder gar vorbeugen kann.

7.1 Motiv und Szenario

Die Forschungsfrage dieser Arbeit lautet:

„Welche Kommunikationskanäle werden für die Interaktion zwischen NutzerInnen vom Darknet am häufigsten eingesetzt?“

Um auf diese Frage eine aufschlussreiche und korrekte Antwort liefern zu können, muss das Testszenario sorgfältig überlegt und vorbereitet werden.

Das Testszenario wird in fünf Schritten durchgeführt:

1. Allgemeine Analyse des Darknets

In dieser Phase wird das Darknet kennengelernt und es werden erste Besuche über den Tor-Browser getätigt. In diesem Schritt soll die Verfasserin erste Erfahrungen sammeln, um die Orientierung im Darknet zu erleichtern. Des Weiteren wird eine Auswertung von Onion-Links aufgestellt, um die populärsten Kommunikationskanäle zur Interaktion im Darknet zu identifizieren und diese im nächsten Schritt näher zu analysieren.

2. Analyse der Kommunikation auf Darknet-Märkten

Darknet-Märkte (wie Silk Road) haben viele Internetnutzer überhaupt erst auf das Darknet aufmerksam gemacht. Nachdem diese Plattformen einen großen Teil des Darknets abdecken, wird auch hier die Kommunikationsweise untersucht. Hierfür wird ein passender Markt gesucht sowie ein passender Verkäufer. Obwohl der Kauf nicht abgeschlossen wird, wird die Verfasserin versuchen, sich trotzdem nur auf legale Waren fokussieren. Das Ziel dieses Schrittes ist zu untersuchen, über welche Wege die Kommunikation zwischen einem Käufer und Verkäufer passiert, sowie welche Kommunikationsanomalien vorkommen (beispielsweise eine einfache, strikte Wortwahl, um durch Zufall keine persönlichen Informationen preiszugeben).

3. Analyse der Kommunikation über Foren

Foren werden im Darknet häufig für allgemeinen Meinungsaustausch eingesetzt. In diesem Schritt wird sich die Verfasserin aktiv in eine Forum-Diskussion einbinden. Es wird auch die Art der Kommunikation der Beteiligten untersucht, um festzustellen, wie groß die Differenzierung zum Surface Web aufgrund der erhöhten Anonymität ist.

4. Analyse der Kommunikation über Chatrooms

Auch Chatrooms werden von vielen Besuchern des Darknets zur Kommunikation und Datenaustausch verwendet. Insbesondere in Ländern, welche von strengen politischen Einschränkungen und Maßnahmen betroffen sind, wird diese Lösung häufig eingesetzt. Das Ziel dieser Analyse ist nicht nur die Untersuchung der Kommunikation, sondern auch die Ermittlung der Vorteile, welche Chatrooms im Darknet mit sich bringen.

5. Ausarbeitung und Zusammenfassung der Ergebnisse

Im letzten Schritt wird untersucht, ob eine einheitliche Kommunikationsweise, welche auf allen drei untersuchten Plattformen vorkommt, nachgewiesen werden kann. Neben den einheitlichen Merkmalen wird der Fokus jedoch auch auf die Anomalien gelegt. Hierbei sind Ausreißer sowie untypisches Verhalten von besonderem Interesse. Die Forschungsfrage wird aussagekräftig beantwortet.

7.2 Vorbereitungen

Um die Risiken, welche mit der Nutzung von Darknet verbunden sind, möglichst minimal zu halten und um qualitativ hochwertige Ergebnisse im Rahmen der praktischen Untersuchung zu bekommen, wurden zwei Formen der Vorbereitung durchgeführt – eine theoretische und eine technische.

7.2.1 Theoretische Vorbereitung - Interview

Im Rahmen der theoretischen Vorbereitung wurde ein Interview durchgeführt. Der Befragte, der aus verständlichen Gründen anonym bleiben möchte, ist ein Bekannter der Verfasserin, welcher bereits mehrmals das Darknet besucht hat und somit seine breitgefächerte Erfahrung teilen kann (Anonym, 2021).

Das Interview umfasst insgesamt 16 Fragen. Diese wurden von der Verfasserin gestellt und basieren auf dem Wissen, welches durch die ausführliche Recherche in vorherigen Kapiteln dieser Arbeit aufgebaut werden konnte.

Die erste Frage lautet:

1. *Warum haben Sie da Darknet aufgesucht? Was hat Sie auf das Darknet aufmerksam gemacht*?

Der erste Besuch des Befragten im Darknet fand im Jahr 2012 statt. Damals hat er sich über einen auf Windows installierten Tor-Browser verbunden. Der Grund für diesen ersten Besuch war die Möglichkeit, mit diesem „illegalen“ Ausflug vor Schulfreunden angeben zu können. Nachdem der Interviewte das erste Mal von Darknet gehört hat, lauteten die ersten Gedanken wie folgt: „So schwer wird das doch wohl nicht werden, ins Darknet zu kommen“.

Die zweite Frage befasst sich mit der Häufigkeit der Darknet-Besuche:

2. *Wie oft waren Sie bereits im Darknet unterwegs?*

Für den Befragten war diese Frage nicht einfach zu beantworten, denn eine explizite Zahl wäre nicht sehr repräsentativ für die Zeit, die er im Darknet verbracht hat. In Stunden gerechnet hat er seinen Angaben zufolge etwa um die 100 bis 150 Stunden im Darknet verbracht. Die meiste Zeit wurde ins reine Suchen investiert: „Zu wissen, dass eine gewisse Seite existiert bedeutet ja nicht, sie auch finden zu können."

Nachdem das Thema Sicherheit eine äußerst bedeutende Rolle in Bezug auf Darknet spielt, beschäftigt sich die nächste Frage mit Sicherheitsmaßnahmen, welche eingesetzt wurden:

3. *Wie haben Sie sich verbunden? Welche Sicherheitsmaßnahmen haben Sie vorgenommen?*

Bei den ersten zwei Besuchen im Darknet wurde mit einer über Google gefundenen Anleitung der Tor-Browser auf einem Windows 7 Rechner installiert. Die einzige Sicherheitsmaßnahme war „der Entschluss, keine persönlichen Informationen preiszugeben". Die Idee über Windows ins Tor-Netzwerk einzusteigen hat jedoch den Nachteil mit sich gebracht, dass der Computer nach jedem Besuch im Darknet komplett neu aufgesetzt werden musste. „Die Menge an Viren, Trojanern und in erster Linie Adware war unbeschreiblich. Und leider auch nicht mehr mit Bereinigungs-Tools entfernbar".

Heutzutage nutzt der Befragte ein Linux-basiertes Betriebssystem namens Tails (Tails, kein Datum), um die Sicherheit während der Nutzung zu erhöhen. „Das hat den wunderbaren Vorteil, dass es einerseits als Live-System von einem USB-Stick aus verwendbar ist und dass es anderseits keine Spuren auf der Festplatte des Rechners hinterlässt, da das gesamte OS rein auf dem Arbeitsspeicher läuft. Der Arbeitsspeicher wiederum hat den Vorteil, dass er kein persistenter Speicher ist und sich komplett leert, sobald der Strom abgedreht wird." Beim Surfen im Darknet werden die Sicherheitsmaßnahmen abhängig von der Intention des Besuchs gewählt. Wenn der Hauptfokus auf einer sicheren Kommunikation liegt, so wird nach einem Kommunikationsweg gesucht, welcher es erlaubt, die Verschlüsselung der Nachrichten selbst zu kontrollieren. Sollen möglichst wenige Anhaltspunkte in Form von Metadaten an Gesprächspartner übermittelt werden, dann wird ein einfaches Vokabular angewendet (beispielsweise einfaches, sauberes Englisch ohne komplexe Satzstellungen). Bei jedem Ausflug ins Darknet überlegt sich der Befragte ganz genau, welche Risiken dabei auftreten und wie diese minimiert werden können.

Zunächst wurde untersucht, welche Inhalte besonders interessant waren:

4. *Was hat Sie beim Surfen im Darknet am meisten interessiert oder sogar fasziniert?*

„Das Internet selbst ist einer der größten Meilensteine unserer modernen Weltgeschichte." Auch wenn dem Befragten bewusst ist, wie umfangreich das World Wide Web ist und dass nicht alle Inhalte zugänglich sind, war die Erkenntnis, dass das von den meisten Menschen verwendete Internet, also das Surface Web, nur einen unglaublich kleinen Teil des gesamten Internets darstellt, eine unbeschreibliche Erfahrung. Die Möglichkeit, aus dem von unseren Regierungen und ISPs vorgegebenen „sicheren" Internet auszubrechen und sich in riskantes und gefährliches Terrain zu begeben, war ein Gefühl, dass sich nur mit dem wunderbaren Begriff Freiheit beschreiben lässt."

Des Weiteren wurde auch untersucht, welche Inhalte besonders schockierend waren:

5. *Was hat Sie beim Surfen im Darknet am meisten schockiert bzw. überrascht?*

Dem Befragten war bereits vor seinem ersten Besuch im Darknet bewusst, was die Einsatzgebiete sind und somit auch welche Inhalte zu erwarten sind. Trotzdem war es sehr überraschend, wie direkt die Werbungen für Produkte im Darknet konzipiert sind. „Auf einer Seitenbeschreibung ohne blumige Worte umschrieben zu lesen „Der größte Drogen und Waffenmarkt der EU – jetzt mit Paketverfolgung“ war eine surreale Erfahrung.“ Die falsche Erwartungshaltung des Interviewten war, dass für solche Themen auch im Darknet etwas verschleiert geworben wird.

„Der größte Schockmoment für mich war jedoch das Ergebnis meiner persönlichen Unvorsichtigkeit. Ich habe an dem Tag nichts Spezielles im Darknet gesucht, mein Ziel war es eher, spannende Artikel von Whistleblowern zu entdecken. Dabei bin ich auf eine Seite gestoßen, die einen sehr zweideutigen Namen und nichts mit meiner Idee einer Suche zu tun hatte.“ Den Aussagen des Interviewten zufolge gelangt man – wenig überraschend - im Darknet sehr schnell auf unerwünschten Seiten mit beunruhigenden Inhalten.

Nachdem das Hauptaugenmerk der praktischen Untersuchung auf die Interaktion mit anderen Nutzern gelegt wird, wurde auch im Rahmen des Interviews untersucht, ob eine Kommunikation stattgefunden hat:

6. *Haben Sie Kontakt zu anderen Darknet-Nutzern aufgenommen und wenn ja, in welcher Form?*

Der Befragte hat insgesamt zweimal Kontakt zu anderen Nutzern aufgenommen. In beiden Fällen wurde hierfür eine verschlüsselter Schweizer E-Mail-Service namens „Protonmail“ (ProtonMail, kein Datum) eingesetzt. Dieser E-Mail-Service wurde aufgrund des Vorteils gewählt, dass es eine Verschlüsselung mittels OpenPGP (ProtonMail, kein Datum) aufweist, problemlos zu nutzen ist und eine moderne Weboberfläche sowie eine zufriedenstellende Dokumentation beinhaltet.

Im ersten Fall wurde die Kommunikation zum Informationserwerb genutzt. „Eine Seite hat Kreditkarteninformationen zum Verkauf angeboten und ich habe ganz ungeniert nachgefragt, woher sie diese Informationen eigentlich bekommen und wie ihr Geschäftskonzept aussieht. Entgegen meiner Erwartungen habe ich sogar eine recht aufschlussreiche Antwort erhalten.“ Der Preis für diese Kontaktaufnahme war eine Vielzahl an Spam, welche darauffolgend erhalten wurde. Im zweiten Fall wurde der Kontakt aufgrund eines Problems bei der Registrierung auf einer Seite aufgenommen. Der Befragte hat, um das Problem zu lösen, direkt den Support kontaktiert. „Interessant dabei war allerhöchstens, dass der Support dort um ein Vielfaches kompetenter war, als ich es im Surface Web jemals erlebt habe.“

Nachdem Darknet-Märkte einen großen Teil des Netzwerks abdecken, beschäftigt sich die nächste Frage mit einem potenziellen Kauf bzw. Verkauf einer Ware:

7. *Haben Sie im Darknet eine Ware verkauft oder gekauft?*

„Ich habe zwei Mal etwas gekauft. Beide Male habe ich mit Bitcoin bezahlt. Die eine Ware ist angekommen, das war ein Kaktus, der bei uns wegen seiner Inhaltsstoffe nicht käuflich zu

erwerben ist. Die andere ist nicht angekommen, da ich zu diesem Zeitpunkt noch nicht gewusst habe, wie eine sichere Transaktion dort abzuwickeln ist. Kurz gesagt hat sich jemand über mein Geld gefreut und hatte keinerlei Anreiz, mir dafür etwas zukommen zu lassen."

Des Weiteren wurde diskutiert, ob der Befragte immer noch das Darknet besucht:

8. *Besuchen Sie das Darknet weiterhin und falls nicht, warum?*

Aufgrund des bereits beschriebenen Schockmoments, bei dem der Befragte ungewollt auf einer Seite mit unerwünschten, äußerst beunruhigenden Inhalten gelandet ist, besucht er das Darknet nicht mehr. Diskussionen über das Darknet führt er in alltäglichen Konversationen jedoch weiterhin.

Nachdem das Darknet einige Unterschiede im Vergleich zum Surface Web aufweist, war für dieses Interview auch besonders interessant, ob diese Diversität im Rahmen der praktischen Nutzung auffällt:

9. *Sind Ihnen große Unterschiede zum Surfen im Surface Web aufgefallen und wenn ja, welche?*

„Ja, es gibt große Unterschiede. Der erste, der einem sofort auffällt, ist das Thema der Ladezeiten. Sie kennen vermutlich Momente, in denen Sie nur unglaublich langsames Internet zur Verfügung haben. In denen eine Seite eine gefühlte Ewigkeit braucht, bis sie vollständig geladen wird. So ähnlich ist das auch im Darknet. Einerseits ist der Aspekt der Sicherheit über das Tor-Netzwerk ein entscheidender Faktor dafür, andererseits aber auch die fehlende Regulierung und Optimierung des Darknets."

Ein weiterer Unterschied, welcher angeführt wurde, ist die Verfügbarkeit von Seiten. „Seiten mit illegalen Inhalten werden oft von Behörden attackiert oder entfernt. Andere werden von versierten Gruppen mit unlauteren Absichten übernommen oder attackiert. Es gibt eine Vielzahl von Gründen, warum ein Link, der gestern noch tadellos funktioniert hat, heute nicht mehr erreichbar ist. Oder zwar noch erreichbar ist, aber auf einmal eine gänzlich andere Seite aufruft. Oder im schlimmsten Fall eine Seite aufruft, die exakt so aussieht wie die gewünschte Seite, allerdings nur eine Kopie ist, die einzig und allein dem Zweck dient, Ihnen Ihre Zugangsdaten zu stehlen. Wer im Darknet unterwegs ist, muss sich also in Geduld üben und lernen, Seiten zu erreichen, Fakes zu erkennen und diese auch zu überprüfen."

Im nächsten Schritt wurde überprüft, ob Darknet aus Sicht des Befragten empfehlenswert ist:

10. *Würden Sie das Darknet anderen Internetnutzern empfehlen?*

Wenn die betrachteten Internetnutzer in einem Land leben, welches einer Diktatur unterliegt, dann würde der Befragte das Darknet empfehlen, um der staatlichen Zensur und Regulierungen zu entkommen. Bei einer solcher Lösung muss jedoch auch mit Risiken gerechnet werden. „In China beispielsweise gibt es Berichte über mehrjährige Haftstrafen aufgrund der Verwendung eines VPN-Dienstes. Hier ist also beim Informationsaustausch im Darknet Vorsicht geboten."

Bei den restlichen Nutzern sollte zuerst überlegt werden, welche Intention hinter der Nutzung von Darknet liegt. Sollte der Erwerb illegaler Waren im Fokus liegen, so ist das Darknet die einzige Alternative zum Schwarzmarkt. Falls der Internetnutzer jedoch keinen Gefahren

gegenübergestellt werden möchte, welche im schlimmsten Fall äußerst unangenehme Konsequenzen mit sich tragen können, so sollte er das Darknet nicht nutzen. „Es ist spannend den Ausflug ins Darknet zu wagen, aber wirklichen Nutzen haben Sie als Normalverbraucher dadurch nicht."

Nachdem der Befragte bereits viel Erfahrung beim Surfen im Darknet gesammelt hat, wurde untersucht, welche Tipps er einem Einsteiger geben würde:

11. *Welche Tipps würden Sie einem Einsteiger in das Thema „Darknet" geben? Worauf soll unbedingt geachtet werden?*

„Überlege dir zuerst, warum du das Darknet nutzen willst.", so der Befragte. Falls es sich um keinen berechtigten Grund handelt, so sollte kein Ausflug ins Darknet gewagt werden. Sollte ein Besuch jedoch weiterhin interessant und gewollt sein, so sollte sich der Nutzer zuerst mit allen Aspekten des Darknets vertraut machen, indem vorab eine ausführliche Recherche dieses Netzwerks durchgeführt wird. „Welche Arten von Personen nutzen das Darknet und wofür? Wie kann ich meine Kommunikation verschlüsseln? Wie stelle ich sicher, nicht betrogen zu werden? Und die wichtigste aller Fragen: Was habe ich zu verlieren, wenn mich jemand gezielt attackiert?" Wenn somit der Grund des Darknet-Besuchs sowie die damit verknüpften Risiken dem Nutzer bewusst sind, dann kann nur durch die empirische Forschung an Erfahrung gewonnen werden.

Die sich ausbreitenden Digitalisierung von zahlreichen Bereichen des alltäglichen Lebens wird uns weiterhin begleiten. Interessant wäre jedoch zu wissen, ob hierbei auch das Darknet weiterhin eine Rolle spielen wird:

12. *Finden Sie, dass das Darknet ein Zukunftspotenzial besitzt?*

„Das ist eine schwierige Frage. Ich hoffe, dass das Darknet auch in Zukunft keine größere Rolle im Alltag der meisten Menschen in Europa spielen wird. Der einzige Grund, der mir spontan einfallen würde, warum es dazu kommen könnte, wäre eine Entwicklung in Richtung eines totalitären Überwachungsstaates. Den Zwang, sich im Darknet bewegen zu müssen, nur um die eigene Meinung ohne Konsequenzen mit Mitmenschen teilen zu können, wünsche ich mir bei uns jedenfalls nicht."

Des Weiteren wurde untersucht, in welchen Bereichen das Darknet eingesetzt werden sollte:

13. *Wofür sollte Ihrer Meinung nach das Darknet am besten eingesetzt werden?*

„Wenn ich diese Frage nicht aus einer technischen Perspektive heraus beantworte, sondern eher aus Sicht bekannter Verwendungszwecke, dann würde ich behaupten, dass die Möglichkeit zum politischen Protest die einzig positive und gleichzeitig auch die wichtigste Einsatzmöglichkeit darstellt." Hierbei meint der Befragte, dass vor allem Bewohner von Ländern, in denen die Meinungsfreiheit unterdrückt wird, indem politische Gegner aktiv bekämpft werden, das Darknet nutzen können, um solch eine Diktatur zu umgehen oder gar gegen sie zu demonstrieren.

Nachdem die Nutzung des Darknets sowohl von legaler als auch von illegaler Natur sein kann, wurde als Nächstes diskutiert, ob je Zweifel aufgekommen sind, ob hierbei eine Grenze durch den Befragten überschritten worden ist:

14. *Haben Sie je daran gezweifelt, ob Ihr Aufenthalt im Darknet von legaler Natur ist?*

Der Befragte hat bei jeder Verwendung des Darknets gewusst, ob die durch ihn ausgeführte Aktionen von legaler oder illegaler Natur waren. Es ist an sich legal im Darknet zu surfen, was jedem Nutzer bewusst ist, der sich ein entsprechendes Vorwissen geschaffen hat, bevor er den Ausflug ins Darknet gewagt hat.

Das Darknet ist ein großes und wenig erforschtes Gebiet. Dadurch kann die Orientierung in diesem Netzwerk eine komplizierte Angelegenheit werden. Aus diesem Grund wurde als Nächstes erfragt, ob dies auch beim Befragten eine gewisse Herausforderung dargestellt hat:

15. *Wie haben Sie sich im Darknet orientiert? Woher wussten Sie wo Sie was finden?*

Auch der Befragt ist der Meinung, dass die Orientierung im Darknet keine einfache Aufgabe ist. „Dazu muss einem anfangs erst einmal bewusstwerden, dass das bekannte, sichere Surface Web gerade einmal vier Prozent der im Internet verfügbaren Informationen abdeckt."

Aufgrund dessen erfordert das Surfen im Darknet viel Geduld. Es gibt zwar zahlreiche Browser, die diese Aufgaben erleichtern, es ist jedoch trotzdem aufwendiger und komplizierter als das Suchen von Inhalten im Surface Web.

„Etwas einfacher gestaltet sich das Surfen dann, wenn man den Namen der gewünschten Seite bereits kennt. In diesem Fall gibt es die Möglichkeit, alternative und überprüfbare Links für das gewünschte Ziel zu finden. Links, die entweder ein zeitliches Ablaufdatum haben oder aus anderen Gründen nicht mehr funktionieren, lassen sich durch solche Seiten angenehm durch aktuellere ersetzen."

Die letzte Frage ist eher allgemeinen Natur und befasst sich damit, welche Seiten bereits besucht wurden:

16. *Welche Seiten haben Sie im Darknet besucht?*

Nachdem die Namen von Webseiten im Darknet stets wechseln und die URLs aus einem 16-stelligen Code bestehen, ist es schwierig, sich an diese zu erinnern. Nur populäre und oft besuchte Seiten besitzen Namen, welche im Darknet allgemein bekannt sind. Der Befragte hat einen Darknet-Markt besucht, den sogenannten „Genesis Market" sowie das „Protonmail" für verschlüsselte Konversationen eingesetzt.

7.2.2 Technische Vorbereitung – Aufbau des Arbeitsumfelds

Im Rahmen der technischen Vorbereitung wird ein virtuelles Environment aufgebaut, um sowohl die Identität als auch die Software der Verfasserin zu schützen. Die Wahl fällt dabei auf die Nutzung einer virtuellen Maschine, um sicherzustellen, dass kein Desaster-Szenario vorkommt bzw. dass die Konsequenzen eines solchen zumindest minimal gehalten werden.

Für die Virtualisierung wird die „Oracle Virtual Box" (Oracle, kein Datum) eingesetzt, da diese bereits im Rahmen des Studiums verwendet wurde und das bereits erworbene Know-how genutzt werden kann. Auf der virtuellen Maschine wird TAILS als Live-System verwendet. Der Vorteil dieser Lösung besteht darin, dass nur der Arbeitsspeicher genutzt wird, wodurch alle potenziell gefährlichen Daten nach dem Ausschalten der virtuellen Maschine verloren gehen (Broadhurst,

et al., 2018). Wie in Abbildung 21 zu sehen ist, wird zuerst mit Standard-Einstellungen gearbeitet, welche bereits das geforderte Maß an Sicherheit gewährleisten.

Abbildung 21: Einrichtung TAILS

TOR agiert adäquat zu einem Virtual Private Network, somit wäre die Nutzung eines zusätzlichen VPN Clients überflüssig oder gar störend (Shanika, 2020). Für das Surfen im Darknet wird der Tor Browser eingesetzt. Die Suchmaschine „DuckDuckGo“ (DuckDuckGo, 2021) erleichtert hierbei die Orientierung in dem unzensierten Netzwerk.

7.3 Durchführung der Untersuchung

Die praktische Untersuchung wird im Zeitrahmen von etwa einem Monat durchgeführt. Die Themen wurden dabei wie folgt aufgeteilt:

7.3.1 Allgemeine Analyse des Darknets

Im ersten Schritt der Untersuchung wird der erste Ausflug ins Darknet getätigt. Die Verfasserin soll sich mit der aufgebauten Umgebung vertraut machen, sowie eine bessere Orientierung im Darknet gewinnen. Der Umgang mit dem Tor-Browser soll erlernt werden.

Kennenlernen der Infrastruktur

Nachdem die virtuelle Maschine gestartet wird, muss bei jeder Nutzung TAILS als Betriebssystem ausgewählt werden, da dieses als Live-System verwendet wird und nie am persistenten Speicher installiert wird. Bereits hier macht sich die erste Hürde bei der Nutzung von TAILS erkenntlich – die Ladezeiten sind sehr lang und sollte nicht genug RAM zur Verfügung stehen, so stürzt das System ab.

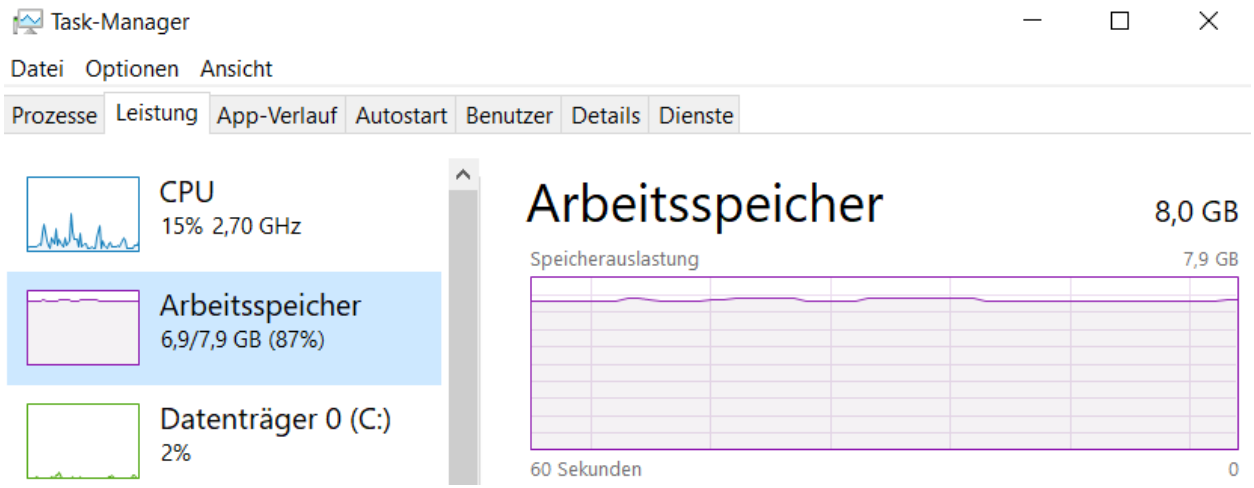


Abbildung 22: Auslastung Arbeitsspeicher

Wie in Abbildung 22 zu sehen ist, wird der Arbeitsspeicher nur durch reines Starten von TAILS bereits zu 87% ausgelastet. Langsame Ladezeiten sowie stockender Datenverkehr sind auch auf dem Host-System (auf welchem die VM läuft) zu erkennen. Paralleles Streamen von Musikvideos ist kaum möglich, die Performance leidet.

Nachdem TAILS ein Linux-basiertes System ist, ist die Orientierung für jeden Nutzer, welcher bereits Linux verwendet hat, keine große Herausforderung. Die Suche nach einem Browser, um ins Internet zu gelangen, ist einfach. Wie in Abbildung 23 zu sehen ist, muss der Tor-Browser nicht explizit nachinstalliert werden, da dieser mit dem TAILS-System ausgeliefert wird. Daneben gibt es auch den sogenannten „Unsafe Browser“. Die Nutzung dieses Browsers muss bei jeder Installation von TAILS, d.h. bei jedem Start der virtuellen Maschine, explizit erlaubt werden. Da diese Tatsache sehr beunruhigend oder gar riskant scheint, wurde dieser Browser von der Verfasserin nicht getestet. Mit TAILS werden auch weitere interessante Applikationen mitgeliefert:

„Electrum Bitcoin Wallet“ dient der Verwaltung von Bitcoins, da dies die herkömmliche Zahlungsart im Darknet ist. „Onion Circuit“ protokolliert wiederum die Knoten, welche bei der Verwendung vom Tor Browser passiert wurden. Die aufgebauten Kanäle werden angezeigt, heruntergebrochen in drei Bereiche – den Eintrittsknoten, Mittelknoten und Ausgangsknoten. „OnionShare“ wird eingesetzt, um Daten, Dokumente, Grafiken und weitere Dateien mit anderen Nutzern sicher zu teilen. Beim „Pidgin Internet Messenger“ handelt es sich um einen Instant Messenger, der das asynchrone Versenden von Nachrichten ermöglicht. „Thunderbird“, wie bereits von Mozilla Firefox bekannt, ist ein E-Mail-Dienst und wird zum sicheren Versenden von E-Mails eingesetzt.

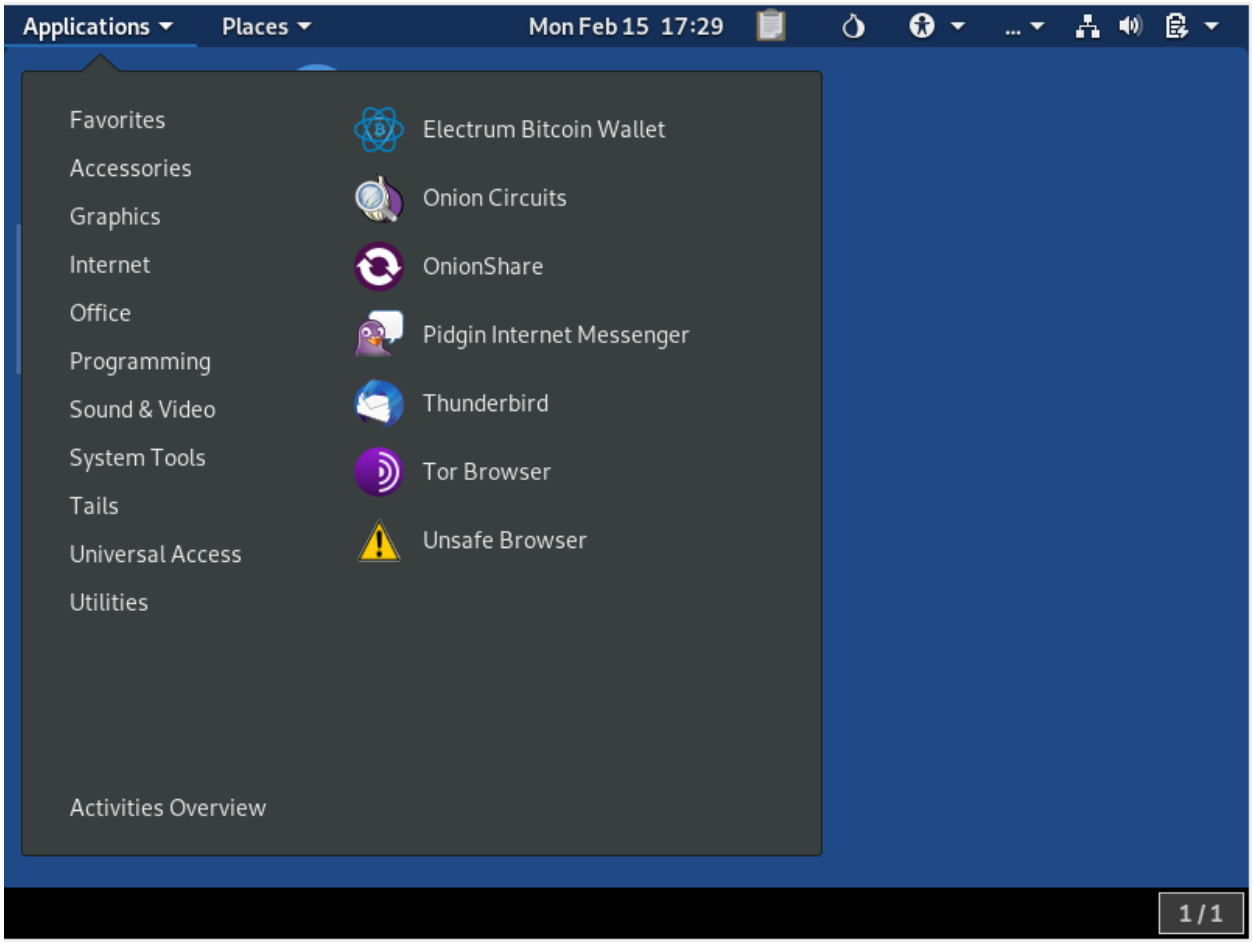


Abbildung 23: Internetzugang TAILS

Wie bereits zu diesem Zeitpunkt ersichtlich ist das TAILS-System so aufgebaut, um keine Informationen von der Identität des Nutzers preiszugeben. Diese Applikationen, welche bereits installiert mitgeliefert werden, bieten dem Anwender maximale Anonymität und Sicherheit der eigenen Daten an.

Wird der TOR-Browser gestartet, so landet der Nutzer, wie in Abbildung 24 ersichtlich, auf der Startseite von TAILS.

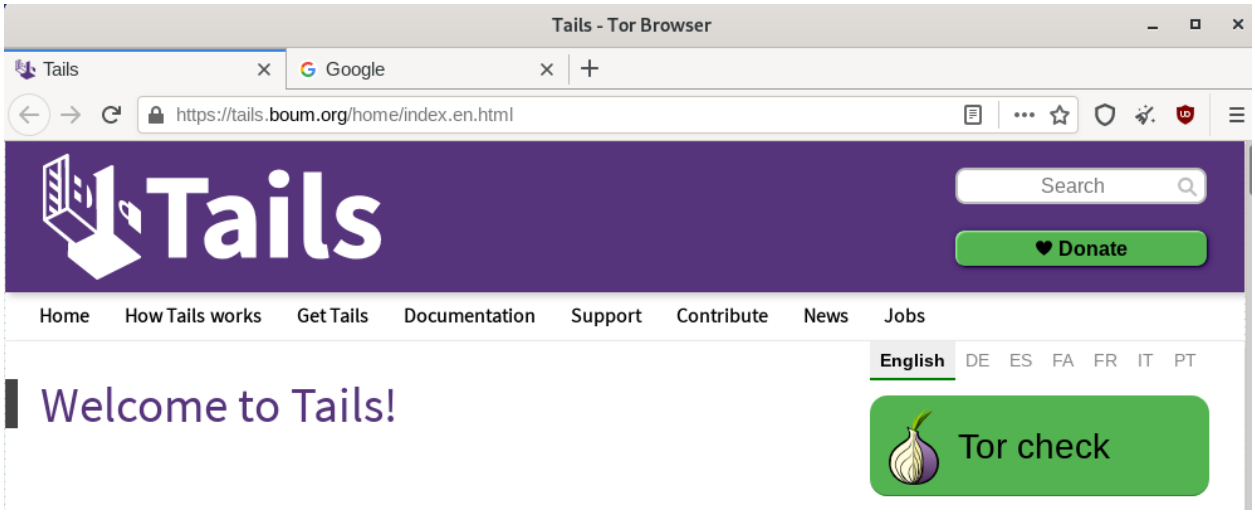


Abbildung 24: Startseite TAILS

Anhand von der Domäne „.org“ ist jedoch ersichtlich, dass wir uns noch nicht im Darknet befinden. Diese Feststellung ist ernüchternd, es wurde eine direkte Verbindung mit dem Darknet erwartet. Nachdem jedoch der TOR-Browser auch für das Surfen im Surface Web eingesetzt werden kann und wird, ist solch eine Startseite begründbar.

Zuerst wird die Seite „Google“ aufgerufen. Es sind, wie in Abbildung 25 ersichtlich, keine großen Abweichungen zum Google im Surface Web erkennbar bis auf die Spracheinstellung.

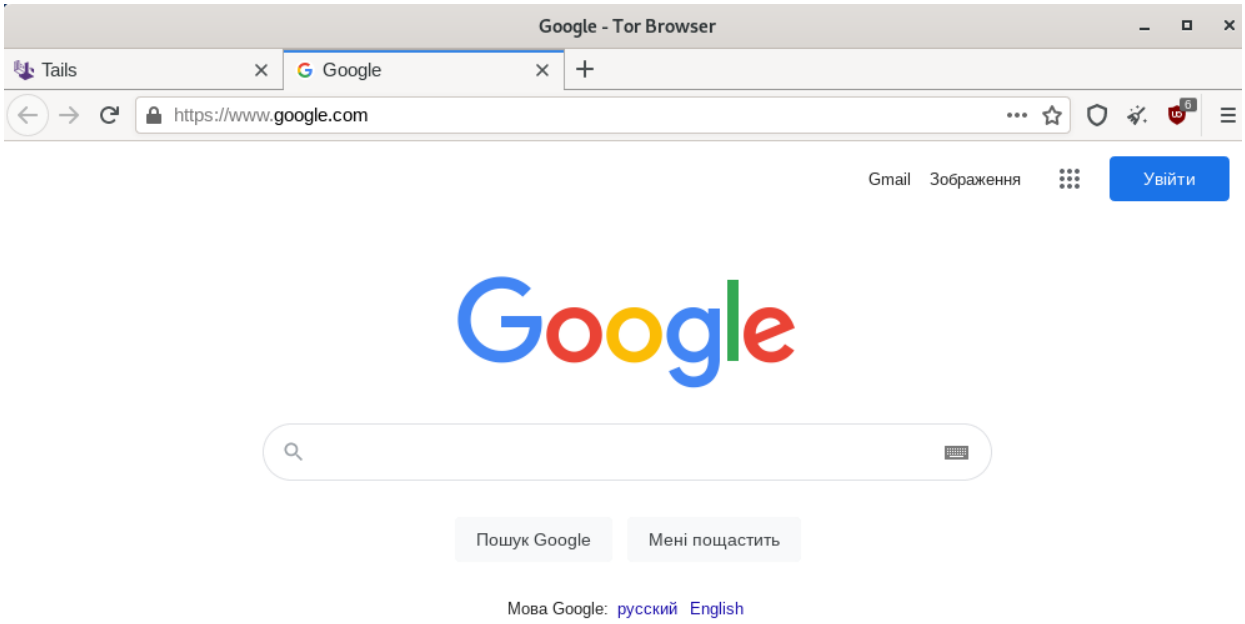


Abbildung 25: Google in TOR

Die Schriftzüge deuten auf eine slawische Sprache hin. Nachdem Google die Sprache der Geolocation automatisch anpasst, stellt sich nun die Frage, wo sich die IP der VM befindet. Der TOR-Browser agiert wie ein VPN und verschleiert die tatsächliche IP des Nutzers. Somit wurde auch in diesem Fall die tatsächliche IP durch einen Platzhalter ersetzt. Eine weitere Recherche ergibt, wie in Abbildung 26 dargestellt wird, dass unsere IP-Adresse in Polen positioniert wurde und die Sprache, welche für Google verwendet wird, somit polnisch ist.

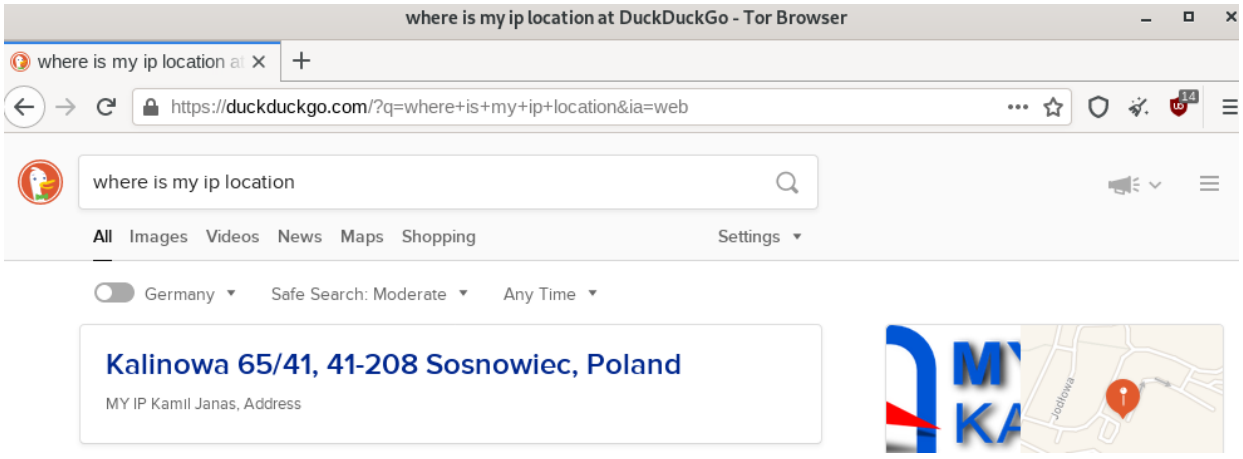


Abbildung 26: IP-Verschleierung durch TOR

Im Rahmen der weiteren Recherche wird eine sehr hilfreiche Funktionalität des TOR-Browsers entdeckt. Die Option „New Identity“, welche in der Menü-Bar zu findet ist, ermöglicht das zurücksetzen der Identität des Nutzers (siehe Abbildung 27). Bei der Aktivierung dieser Funktionalität werden alle Tabs geschlossen, der Nutzer bekommt eine neue IP-Adresse und landet wieder auf der Startseite. Zur Überprüfung, ob dieser Vorgang erfolgreich durchgeführt wurde, werden die IP-Adresse sowie die Geolocation abgefragt. Die IP-Adresse wurde tatsächlich geändert und ist nun eine andere, lokalisiert in New Jersey in den Vereinigten Staaten.

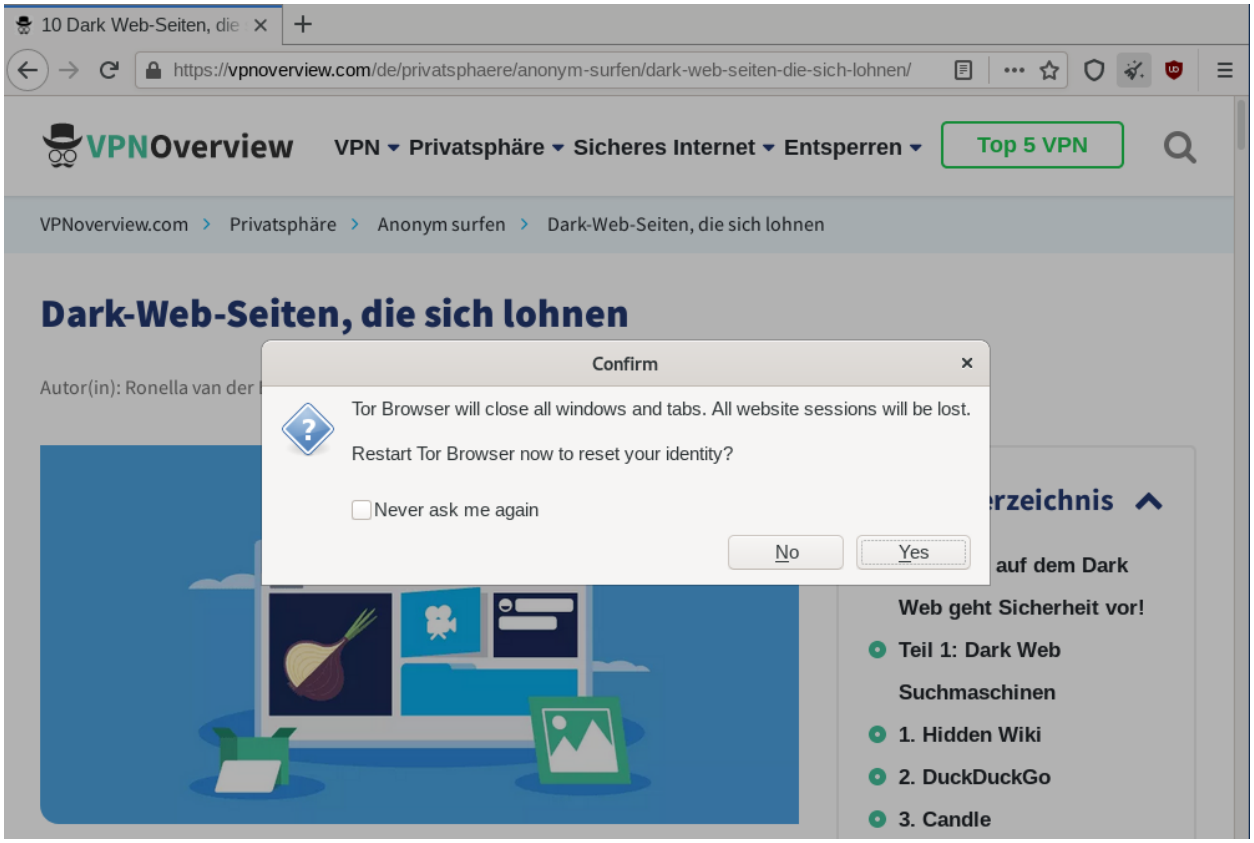


Abbildung 27: "New Identity" Funktionalität

Was im weiteren Zuge der Arbeit verstärkt bemerkt wird, sind die sehr langen Ladezeiten. Wird in der Search Engine ein Suchbegriff eingegeben, so nimmt eine Suchanfrage in manchen Fällen ganze zwölf Minuten in Kauf, bevor die Ergebnisse angezeigt werden.

Bevor jedoch mit dem Surfen im Darknet tatsächlich begonnen werden kann, muss der TOR-Browser richtig eingestellt werden.

TOR ermöglicht die Wahl eines sogenannten „Security Level“. Hierbei wird unter „Standard“, „Safer“ und „Safest“ unterschieden. Standard erlaubt die Nutzung aller Features, welche von TOR sowie aufgesuchten Webseiten angeboten werden. Der Modus „Safer“ blockiert wiederum Features, welche gefährlich sein könnten und die einwandfreie Funktionalität des Browsers beeinträchtigen würden. Zu solchen Features gehören beispielsweise JavaScript-Komponenten auf http-Seiten, spezifische Schriftarten sowie mathematische Symbole. Audio- sowie Video-Dateien dürfen in diesem Security Level nur manuell gestartet werden. Der „Safest“ - Modus ermöglicht nur das Nutzen solcher Features, welche für die Verwendung statischer Seiten sowie

Basisservices unbedingt notwendig sind. Diese Einschränkungen beziehen sich auf den Einsatz von Bildern, Medien und Skripten.

Selbstverständlich ist es mit Hilfe der Einstellungen von TOR auch möglich, alle Cookies zu löschen. Cookies sollen zwar keine persönlichen Informationen sammeln und stellen somit auch keine direkte Gefahr dar, trotzdem wird der Nutzer direkt darüber informiert, dass alle Cookies nach dem Schließen jeder TOR-Sitzung automatisch gelöscht werden.

Des Weiteren können pro Eingabe- sowie Ausgabegerät Berechtigungen vergeben werden. Default-mäßig werden Pop-Up Fenster blockiert sowie Warnmeldungen gesendet, wenn eine Webseite versucht, Add-Ons im Hintergrund zu installieren. Die Add-Ons, welche von TOR-Browser automatisch ausgeliefert werden, sind „HTTPS Everywhere“, „NoScript“ und „uBlock Origin“ (siehe Abbildung 28).

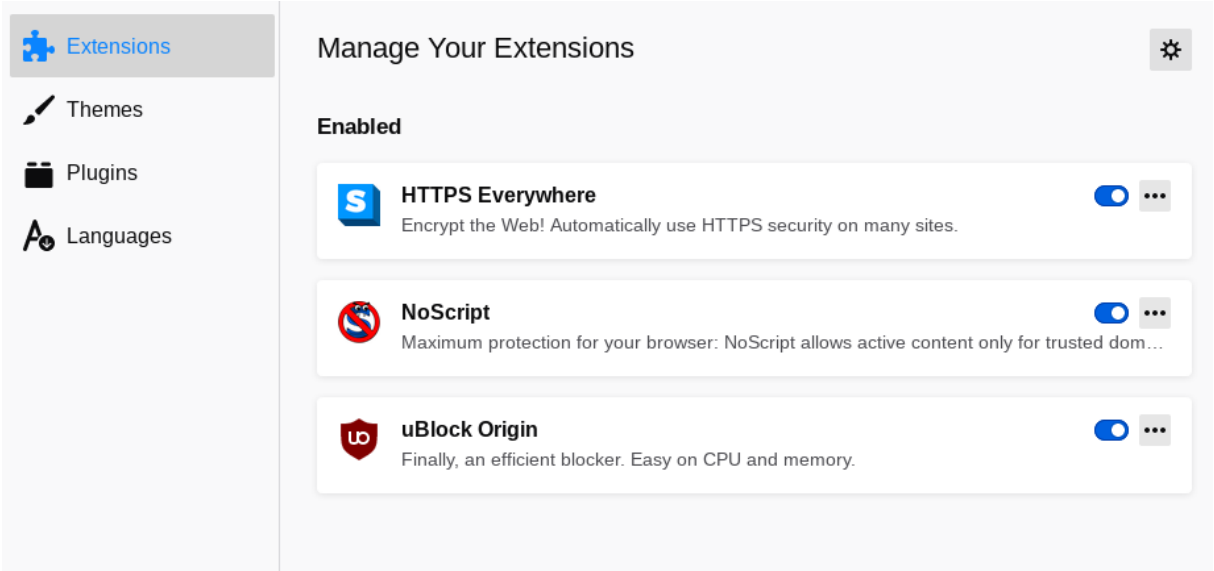


Abbildung 28: TOR Add-Ons

Sobald die Einstellung des TOR-Browser erfolgreich abgeschlossen und die Eingaben überprüft wurden, kann auf der TAILS-Startseite ein letzter Check durchgeführt werden. Dieser berichtet, ob TOR-Browser richtig konfiguriert wurde oder nicht. Laut Abbildung 29 ist alles bereit für das Surfen im Darknet.

Abbildung 29: Abschluss Konfiguration TOR

Untersuchung von Darknet

Eine nähere Untersuchung von Darknet-Seiten stellt eine herausfordernde Aufgabe dar. Das Onion-Netzwerk ist so aufgebaut, dass die URLs im Rahmen eines sich wiederholenden Prozesses immer geändert oder gar gelöscht werden, wenn sie zum Opfer einer Strafverfolgung werden.

Im nächsten Schritt sollen die bekannten Onion-Seiten gefiltert werden, indem nur diejenigen aussortiert werden, die als ein Kommunikationskanal agieren. Um diesen Schritt tätigen zu können, wird nach sogenannten „Wikis“ gesucht. Diese bieten eine kategorisierte Sammlung von Onion-URLs und ermöglichen somit eine optimierte Orientierung im Darknet. Das Ziel ist es, mindestens drei Wikis zu finden. Die Links, welche auf solchen Seiten gefunden werden, werden mittels eines Excel-Sheets ausgewertet. Die Ergebnisse, somit die Kommunikationsformen, welche die größte Anzahl an Links und somit die meisten Anbieter aufweisen, werden in den nächsten Kapiteln näher untersucht.

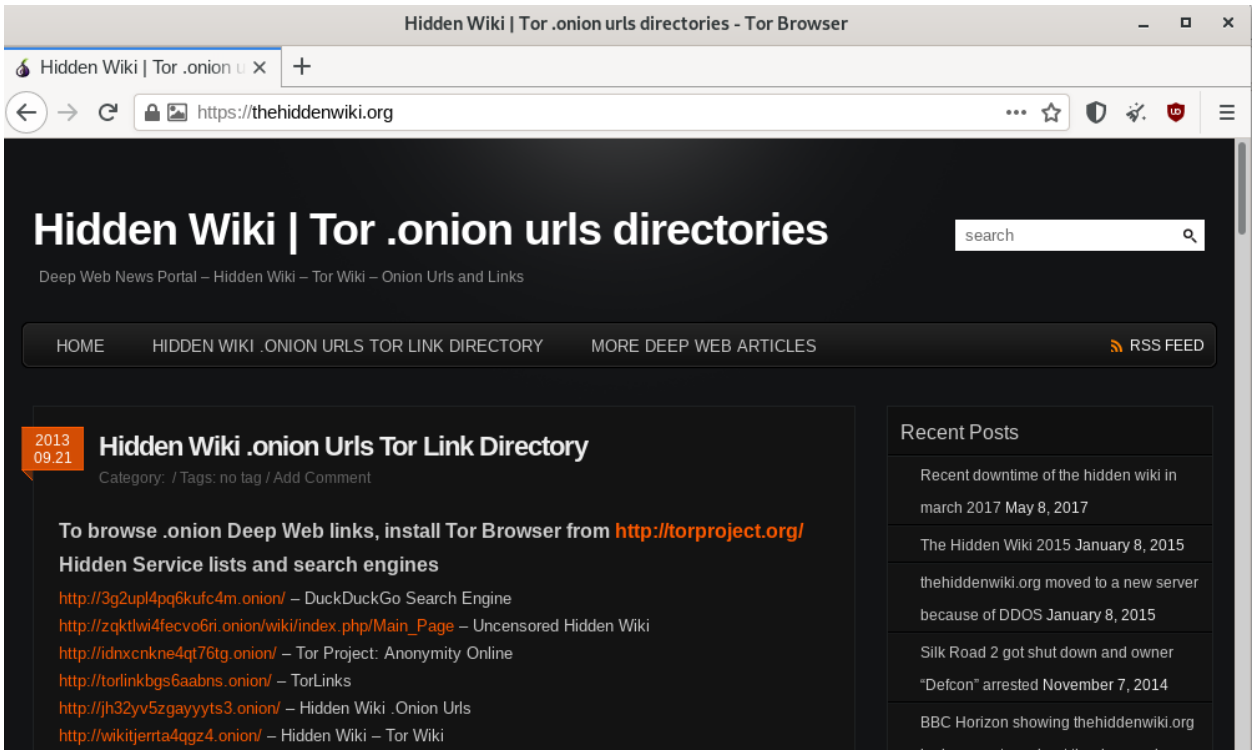


Abbildung 30: HiddenWiki im Surface Web

Wird im Surface Web nach „beliebte Darknet Seiten“ gesucht, so gelingt der Nutzer auf die Seite von “VPNOverview“ (van der Burgt, Dark-Web-Seiten, die sich lohnen, 2020). Diese schlägt als erste Destination die HiddenWiki vor. HiddenWiki agiert als ein Lexikon und listet diverse, kategorisierte Onion-Links auf, um den Nutzern die Orientierung im Darknet zu erleichtern. Es gibt auch eine Kopie dieser Seite im Surface Web (TheHiddenWikki, 2021). Um zu verhindern, dass diese Suchen auf die wahre Identität zurückverfolgt werden können, wird die Suche direkt in der virtuellen Maschine getätigt. Obwohl diese Seite das letzte Mal im Jahr 2013 gewartet wurde (siehe Abbildung 30) und zahlreiche Links bereits tot bzw. veraltet sind, funktionieren die von Wikis weiterhin. So leitet der zweite Link der Kategorie „Hidden Service lists and search engines“ auf die Onion-Version von HiddenWiki (HiddenWikki - Onion, 2021).

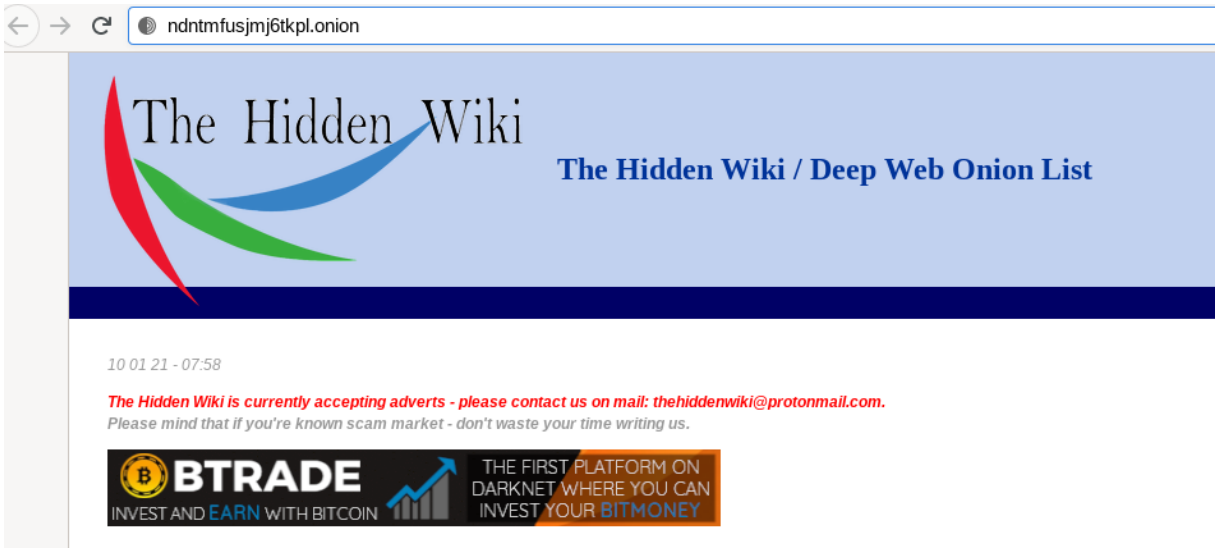


Abbildung 31: HiddenWiki im Darknet

HiddenWiki im Darknet (siehe Abbildung 31) ist eine umfangreiche Sammlung von Onion-Links. Diese sind in genau 18 Kategorien aufgeteilt. Es werden Seiten von Märkten, Blogs, Messaging-Plattformen sowie Bibliotheken und viel mehr angezeigt. Viele Links weisen auch eine bestimmte Kennzeichnung auf. Grünes „Verified“ steht für bestätigte Seiten, welche problemlos besucht werden können. Links mit einem gelben „Caution“ sollten nur mit Vorsicht genossen werden, hierbei kann es sich um eine gefährliche Seite handelt. Ein rotes „Scam“ steht hierbei für eine betrügerische Seite und mittels dieser Kennzeichnung werden die Nutzer gewarnt, dass sie diese Seiten nicht besuchen sollten. Es wird außerdem markiert, welche Links bereits tot und welche noch aktiv sind. HiddenWiki ist ein hervorragendes Instrument, um effektiv die Orientierung im Darknet zu gewinnen.

Abbildung 32: TorLinks im Darknet

Ein weiteres Wiki, welches im Darknet zur Optimierung der Orientierung dient, ist das sogenannte „TorLinks“ (TorLinks, 2021) (siehe Abbildung 32). Der Index dieser Seite ist zwar nicht so umfangreich wie bei HiddenWikki, jedoch trotzdem sehr informativ. Auch hier sind Onion-Links in diverse Kategorien aufgeteilt. Zusätzlich dazu wird angegeben, ob es sich um eine kommerzielle

oder um eine nicht-kommerzielle Rubrik handelt. An sich ist die Seite sehr einfach gestaltet, was der Übersichtlichkeit dient und die Orientierung auf dem Wiki erleichtert.

Zusätzlich wurden noch zwei weitere Seiten untersucht, welche im Darknet als Wikis agieren. „OnionDir“ (OnionDir, 2021) ist eine sehr vereinfachte Liste mit reiner Aufreihung von Onion-URLs, ohne jegliche Kommentare. „TrustWiki“ (TrustWiki, 2021) gehört wiederum zu der Sorte von Wikis, die im Aussehen auffälliger sind als die Alternativen. Dies liegt darin, dass diese Seite zahlreiche Werbungen aufweist. Hierbei handelt es sich um bewegliche Bilder mit grellen Farben, welche gleich die Aufmerksamkeit des Besuchers auf sich ziehen. Aus diesem Grund ist die Orientierung auf diesem Wiki komplizierter als bei den anderen Lexika, da der Nutzer stets abgelenkt wird.

Würde man heute im Surface Web die Popularität eines Links bewerten müssen, so würde man auf die Backlink-Statistik zugreifen (die sogenannte „Link Popularity“) (SEO-united, kein Datum), (searchmetrics, kein Datum). Nachdem die Natur des Darknets dieses leider nicht erlaubt, wird eine Alternative genutzt. Das Prinzip der Link Popularity wird trotzdem angewendet. Es werden aus vier Wikis Onion-Links gesammelt und in Kategorien aufgeteilt. Kategorien, welche sich auf bidirektionale Kommunikation fokussieren oder diese anbieten, werden im nächsten Schritt näher angesehen. Je mehr Links einer Kategorie entsprechen, umso beliebter ist diese Kategorie (so das Prinzip von Link Popularity). Darauffolgend wird diese Auswertung nach Duplikaten durchsucht. Abschließend werden die populärsten Vertreter der einzelnen Rubriken näher diskutiert und praktisch untersucht.

Auswertung von Onion-Links

Im nächsten Schritt werden die Links, welche auf HiddenWikki, TorLinks, OnionDir und TrustWiki zu finden sind, gesammelt. Insgesamt werden 798 Onion-Links kategorisiert und ausgewertet. 357 davon kommen von HiddenWiki, 190 von TorLinks, 179 von OnionDir und 72 von TrustWiki.

Diese Links werden im nächsten Schritt in entsprechende Kategorien aufgeteilt (siehe Abbildung 33). Hierbei liegt der Fokus auf der Kommunikationsform. Unidirektionale Kommunikation ermöglicht die Kommunikation nur in eine Richtung, wie beispielsweise bei Blogs, wo Inhalte mit anderen Nutzern zwar geteilt werden, diese jedoch nicht direkt reagieren können. Bidirektionale Kommunikation erlaubt die Kommunikation in beide Richtungen. Sender und Empfänger einer Nachricht können direkt in Kontakt treten.

Zur unidirektionalen Kommunikation gehören Kategorien wie Erotik, Hacking, Hosting, Blogs oder Politik. Diese Rubrik umfasst auch alle Whistleblowing-Seiten. Zu dieser Gruppe gehören auch die sogenannten „Support-Leistungen“. Hier werden alle Links gesammelt, welche den Darknet-Nutzer die Orientierung im Darknet sowie die Verwendung der hier angebotenen Komponenten erleichtern. Es handelt sich um Links, welche die Suche im Darknet vereinfachen oder Informationen zum System und VPN-Anbietern sowie zur Optimierung der Anonymität liefern.

Unter der Kategorie „Others“ verbergen sich Links, welche keiner spezifischen Kategorie zugeordnet werden können. Hierzu gehören zum Beispiel sogenannte „Scam-Lists“, welche die Links auflisten, die nur zur Ausnutzung der Darknet-User auf betrügerischer Art eingesetzt

werden. Diese Kategorien werden im Zuge dieser Arbeit jedoch nicht weiter untersucht, da der Fokus dieser Arbeit auf der bidirektionalen Kommunikation liegt.

Unter bidirektionaler Kommunikation verbergen sich Kategorien wie Foren, Chatrooms, soziale Netzwerke, E-Mail, File Sharing und Marktplätze. Diese wiederum werden hinuntergebrochen auf Finanzen (Links, welche sich mit Geldwäsche beschäftigen), kommerzielle Marktplätze, welche Güter zu Verkauf anbieten, und auf Drogen-Märkte. Bei Chatrooms werden auch IRC- und XMMP-Links mitberücksichtigt. Hierbei handelt es sich um Protokolle, welche zentrale Chaträume erstellen und somit die Kommunikation in Echtzeit zwischen mehreren Nutzern ermöglichen (SEO-Analyse, kein Datum), (ComputerWeekly, TechTarget, 2016).

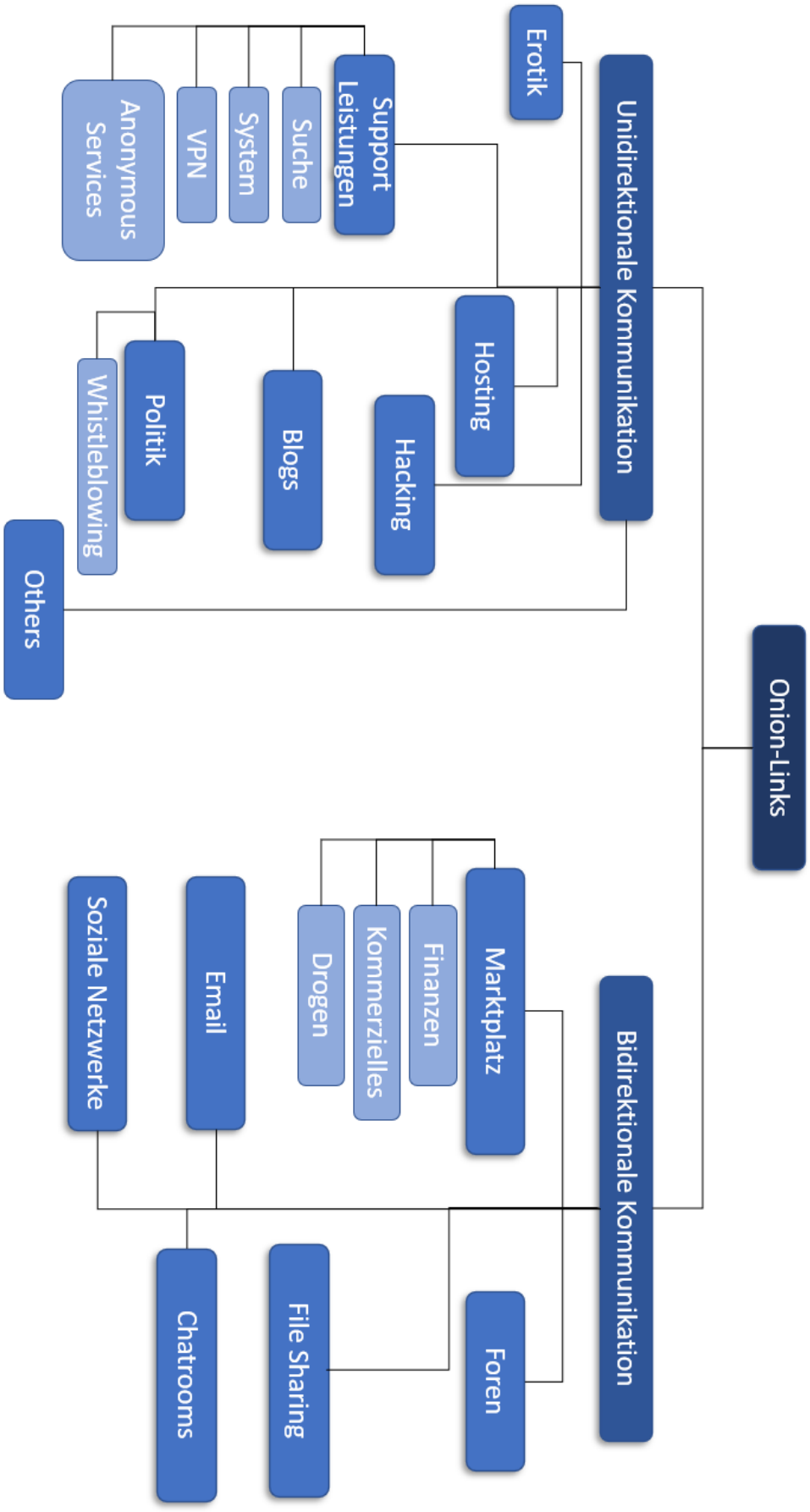


Abbildung 33: Kategorisierung von Onion-Links

Nachdem alle Onion-Links in Kategorien aufgeteilt wurden, liegt nun der Fokus auf dem Bereich der bidirektionalen Kommunikation. Pro Kategorie werden alle Links aufgelistet, Duplikate aussortiert und entfernt, um das Ergebnis nicht zu verfälschen, und die Gesamtanzahl ermittelt (siehe Abbildung 34 und 35).

Email	Soziale Netzwerke	Chatrooms
http://secmailm453q7piv.onion/	http://nmrha3y4l3d6hqz4.onion/	http://xqz3u5drneuzhaeo.onion/users/chatroom/
http://eludemaillhqfkh5.onion/	http://connectkjsazkwud.onion/	http://xqz3u5drneuzhaeo.onion/users/efgchat/
http://bitmailendavkbec.onion/	http://galaxy3m2mn5iqtn.onion/	http://notestjxctkwbk6z.onion/
http://protonirockerxow.onion/	http://injz4qvzyun6zq3a.onion/	http://u6lyst27lmelm6oy.onion/index.php
http://grrmailb3fxpjbwm.onion/	http://blkbook7i4cpw4s6.onion/	http://chat7zlxojqcf3nv.onion/
http://ctemplar42u6fulx.onion/	http://u4uoz3aphqbdc754.onion/	http://ak5tvnvmhlmfqwjx.onion/theleak/chat.php
http://4v6veu7nsxklglnu.onion/SimplePM.php	http://ofrmtr2fphxkqgz3.onion/	http://bah37war75xzkpla.onion/
http://a5ec6f6zcxtudtch.onion/	http://ay5kwknh6znfmcbb.onion/torbook/	https://privnote.com/
http://c4wcxidkfhvmzhw6.onion/	http://ajqaivfxtqy3fdlr.onion/torbook/	https://crypto.cat/
http://jhiwjjlqpyawmpjx.onion/	http://lotjbov3gzzf23hc.onion/	https://bitmessage.org/wiki/Main_Page
http://k54ids7luh523dbi.onion/	http://npdaaf3s3f2xrmlo.onion/	http://bm6hsivrmdnxmw2f.onion/
http://sc3njt2i2j4fvqa3.onion/	http://hbjw7wjeoltskhol.onion	http://fncuwbiisyh6ak3i.onion/
http://365u4txyqfy72nul.onion/	http://r5c2ch4h5rogigqi.onion/	http://tetatl6umgbmtv27.onion/
http://sms4tor3vcr2geip.onion/	https://www.facebookcorewwwi.onion/	http://qj3m7wxqk4pfqwob.onion/
http://torbox3uiot6wchz.onion/	http://galaxy3bhpzxecbywoa2j4tg43muepnhfalars4cce3fcx46qlc6t3id.onion/	http://chatboxdb7vifffz.onion/
http://wi7qkxyrdpu5cmvr.onion/	http://notbumpz34bgbz4yfdigxvd6vzwtxc3zpt5imukgl6bvip2nikdmdaad.onion/	http://evilchatxp24s7vb.onion/
http://hxuzjtocnzvv5g2rtg2bhwkcbupmk7rclb6lly3fo4tvqkk5oyrv3nid.onion/	http://nzh3fv6jc6jskki3.onion/	http://danschatjr7qbwip.onion/
https://protonirockerxow.onion/		http://ozi62yyo6o4upexr.onion/chat/chat.php
http://mail2tor2zyjdctd.onion/		http://v6tlwjbbtdqs7wsq.onion/
http://secmail63sex4dfw6h2nsrbmfz2z6alwxe4e3adtkpd4pcvkhht4jdad.onion/		http://aqmeyxn5fycgigz7.onion/
https://www.guerrillamail.com/		irc://itapxk4hwi3k5ktj.onion:6697
http://eludemailxhnqzfmxehy3bk5guyhlxbunfyhkcksv4gvx6d3wcf6smad.onion/		ircs://w4a6ssearu46yphm.onion:6697/

Abbildung 34: Auswertungstabelle Onion-Links

Aufteilung Onion-Links pro Kategorie	
Marktplätze	108
Foren	58
Chatrooms	55
Email	25
Soziale Netzwerke	17
File Sharing	14

Abbildung 35: Gesamtanzahl Onion-Links pro Kategorie

Aus diesen Werten wurde darauffolgend zur Veranschaulichung der Resultate ein Kreisdiagram gebildet (siehe Abbildung 36).

Insgesamt wurden 347 Links ermittelt. Nach der Entfernung von Duplikaten sind 277 Links für die Auswertung übriggeblieben. Die höchste Anzahl entspricht den Darknet-Märkten mit insgesamt 108 Links. Den größten Anteil bilden die kommerziellen Marktplätze, also Plattformen, welche jede Art von Gütern (außer Drogen) zum käuflichen Erwerb anbieten. Auf dem zweiten Platz haben sich Foren platziert, gefolgt von Chatrooms. Diese drei Kategorien werden im folgenden Schritt näher betrachten und auf Duplikate überprüft.

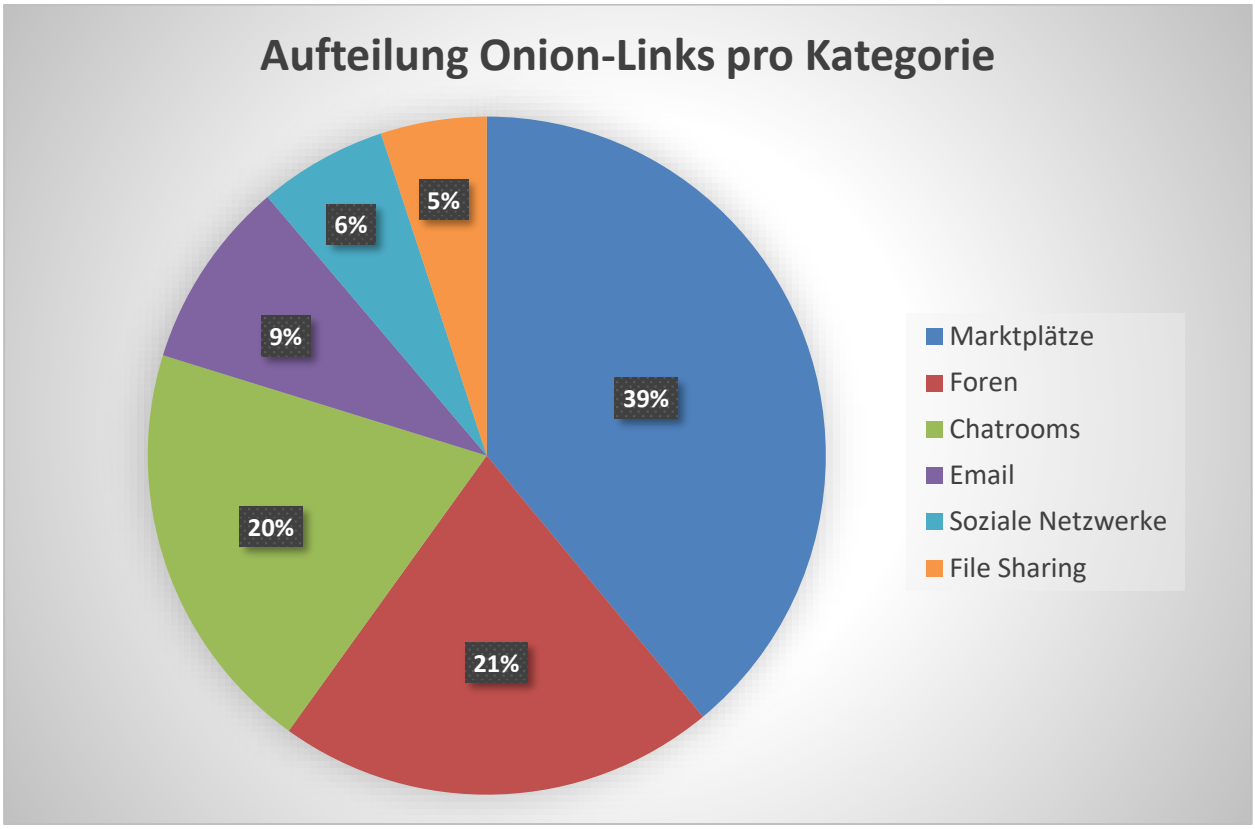


Abbildung 36: Auswertungen von Onion-Links

In Bezug auf Darknet-Märkte, welche kommerzielle Güter anbieten, wurde am öftesten die Seite „USfakeIDs - High quality USA Fake Drivers Licenses“ entdeckt. Der Link von dieser Plattform (USfakeIDs - High quality USA Fake Drivers Licences, 2021) ist genau viermal in der Auswertungsliste vorgekommen. Nachdem Ergebnisse aus insgesamt vier Wikis ausgewertet werden, ist das Vierfache eines Links das Maximum, welches erzielt werden kann. Dieses Ergebnis sagt aus, dass der Link auf allen vier Wikis vorkommt.

Von allen aufgelisteten Foren wurde am häufigsten die Seite „Talk.Masked | Talks and Notes. 2nd generation“ gefunden. Der Onion-Link dieses Forums (Talk.Masked | Talks and Notes. 2nd generation, 2021) wurde in der Liste dreimal protokolliert.

Bezüglich der Chatrooms wurde insbesondere die Seite „Chat with strangers“ auffällig. Diese wurde in der Sammlung der Links mit der URL (Chat with strangers, 2021) zweimal dokumentiert.

Die Kommunikationsform auf den Plattformen „USfakeIDs“, „Talk.Masked“ und „Chat with strangers“ werden in den nächsten Kapiteln näher betrachtet und entsprechend dokumentiert, damit einerseits die Kommunikationsformen anderer Nutzer untersucht sowie die Kontaktaufnahme selbst praktisch getestet werden kann.

7.3.2 Analyse der Kommunikation auf Darknet-Märkten

Darknet-Märkte erfreuen sich einer großen Popularität unter den Darknet-Nutzern. Laut einer Studie werden auf umfangreichen Marktplätzen zwischen 300.000 und 600.000 Dollar pro Tag umgesetzt (Mey, 2016). Vor allem bei solchen Umsätzen ist es besonders wichtig, dass die

Kommunikation zwischen Ankäufer und Verkäufer problemlos abgewickelt wird. Sollte die Ware nicht eintreffen oder beschädigt sein, muss der Käufer eine Möglichkeit haben, um den Vendor schnell und problemlos zu kontaktieren.

„USfakeIDs - High quality USA Fake Drivers Licenses“ gehört zu den großen Verkaufsplattformen von Darknet. Allgemein bietet die Seite gefälschte amerikanische Führerscheine als Form von Identitätsnachweis an. Es kann aus über 15 amerikanischen Bundesstaaten ausgewählt werden. Alle Exemplare können um den gleichen Preis erworben werden, und zwar für 200 amerikanische Dollar (0,0041 Bitcoin).

An sich ist die Seite sehr einfach aufgebaut. Die Produktübersicht stellt eine kleine Auflistung der Ware dar. Unter dem Feld FAQs verbirgt sich ein kurzer Eintrag, welcher beschreibt, welche Informationen vom Käufer für die Fertigstellung eines gefälschten Ausweises benötigt werden. Dazu wird auf eine Handvoll Links verwiesen, welche zum Mining von Bitcoins genutzt werden können.

Wie auch auf gewöhnlichen Marktplätzen im Surface Web (beispielsweise Amazon) muss sich ein Darknet-Nutzer zuerst registrieren, um einen Kauf tätigen zu können. Die Registrierung besteht nur aus vier Feldern: einem Benutzernamen, Passwort, der Bestätigung des Passworts und einer CAPTCHA-Abfrage. Nach der Registrierung wird in roter Schrift darauf hingewiesen, dass das Passwort sicher aufbewahrt werden muss, da es aus Sicherheitsgründen nicht automatisch wiederhergestellt werden kann, sollte es verloren gehen oder vergessen werden. Nach einem erfolgreichen Login werden bereits mehrere Optionen angeboten. Unter anderem eine genaue Übersicht über die Menge an Bitcoins, welche vom eingeloggten User bereits hochgeladen wurden und zur Verfügung stehen. Zusätzlich wird ein neuer Tab namens „Messages“ ersichtlich. Dieser verbirgt jedoch eine unerfreuliche Nachricht (siehe Abbildung 37).

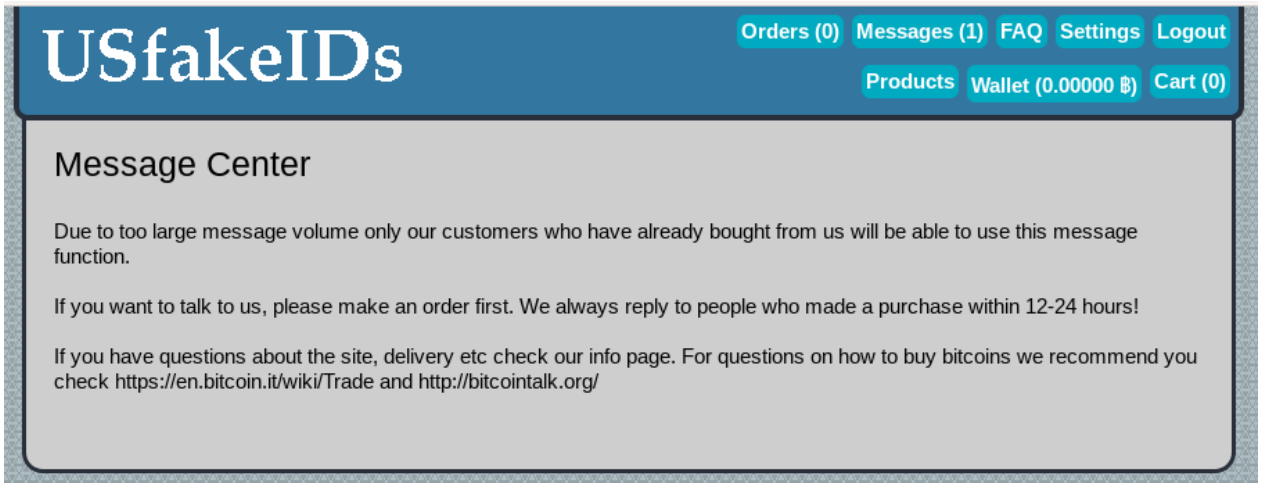


Abbildung 37: Messages USfakeIDs

Eine Grundvoraussetzung dafür, dass sich ein Käufer mit dem Händler in Kontakt setzen kann, ist eine bereits abgeschlossene Bestellung. Ohne diese Erstbestellung ist es also nicht möglich den Verkäufer zu kontaktieren. Ein Darknet-Nutzer wird somit dazu gezwungen, zumindest eine Bestellung „blind“ abzuschließen, ohne beim Verkäufer nach dem Ursprung, der Qualität oder Risiken verbunden mit der angebotenen Ware zu fragen.

Hier wird die Möglichkeit der Kommunikation also einerseits als eine Marketingstrategie eingesetzt, welche den potenziellen Kunden zum Kauf zwingt, andererseits wird sie gefiltert und dadurch vermieden, dass Nachrichten zum Händler gelangen, die mit keiner bereits abgeschlossenen Bestellung verbunden sind. Es wird behauptet, dass die Antwortzeit, sobald eine Bestellung abgeschlossen wurde, bei potenziellen Fragen oder anderen Anliegen zwischen 12 und 24 Stunden liegt.

In weiterer Folge wurden aus der Kategorie „kommerzielle Marktplätze“ noch zwei andere Seiten untersucht, darunter „UK Passports“ (UK Passports, 2021) und „USA Citizenship“ (USA Citizenship, 2021), welche in der Auswertungsliste jeweils dreimal vorkommen.

Beide Seiten ähneln optisch sehr stark der Seite „USfakeIDs“. Auch hier muss zuerst die Registrierung abgeschlossen werden, bevor weitere Aktionen ausgeführt werden. Wie zu erwarten war, muss auch bei „UK Passports“ und „USA Citizenship“ zuerst eine erste Bestellung abgeschlossen werden, bevor der Händler kontaktiert werden darf. Auch hier bewegt sich die Antwortzeit im Zeitrahmen 12 – 24 Stunden.

Um zu untersuchen, ob diese vermarktete Form der Kommunikation auch bei anderen Marktplätzen genutzt wird, wurden zusätzlich noch zwei Exemplare aus den Kategorien „Marktplatz – Drogen“ und „Markplatz – Finanzen rausgesucht. Die Drogenmärkte vertritt in diesem Fall die Seite „EuCanna“ (EuCanna, 2021), (mit genau drei Ergebnissen in der Auswertungstabelle), welche verschiedene Arten von Cannabis anbietet. Nach der Registrierung wurde auch von dieser Seite vorausgesetzt, dass eine Bestellung abgeschlossen wird, bevor Kontakt aufgenommen werden darf.

In Bezug auf Marktplatz - Finanzen, also Märkte, welche sich mit Geldwäsche beschäftigen und gefälschtes Geld anbieten, wurde die Seite „HQER – High Quality Euro Replicas / Counterfeits“ gewählt (auch diese Seite ist in der Auswertungsliste von Onion-Links insgesamt dreimal vorgekommen) (HQER - High Quality Euro Replicas /Counterfeits, 2021).

Nach einer erfolgreichen Registrierung wurde das gleiche Ergebnis wie bei den vorigen vier Beispielen erwartet. Wider Erwartungen wurde hier jedoch nicht vorausgesetzt, dass eine Bestellung zuerst abgeschlossen sein muss, bevor der Händler kontaktiert werden kann. Es wird ein kleines Fenster angeboten, welches genutzt werden kann, um eine Nachricht an den Betreiber der Seite zu senden. Außerdem wird der Nutzer gleich mit dem Benutzernamen angesprochen und aktiv dazu aufgefordert, mit dem Händler in Kontakt zu treten. Wie in Abbildung 38 zu sehen ist, wurden zwei Fragen in einfachem Englisch formuliert. Es wird danach gefragt, worauf insbesondere aufgepasst werden soll, wenn mit den gefälschten Banknoten gezahlt wird bzw. wie hoch das Risiko ist, enttarnt zu werden. Das Absenden der Nachricht hat ganze zwei Minuten gedauert. Danach wurde die Seite neu geladen und die Frage im Message-Board angezeigt.

Interessant ist nun zu beobachten, ob eine Antwort innerhalb von 12 bis 24 Stunden eintrifft, oder ob durch die Möglichkeit der freien Kommunikation die Antwortzeiten verlängert werden.

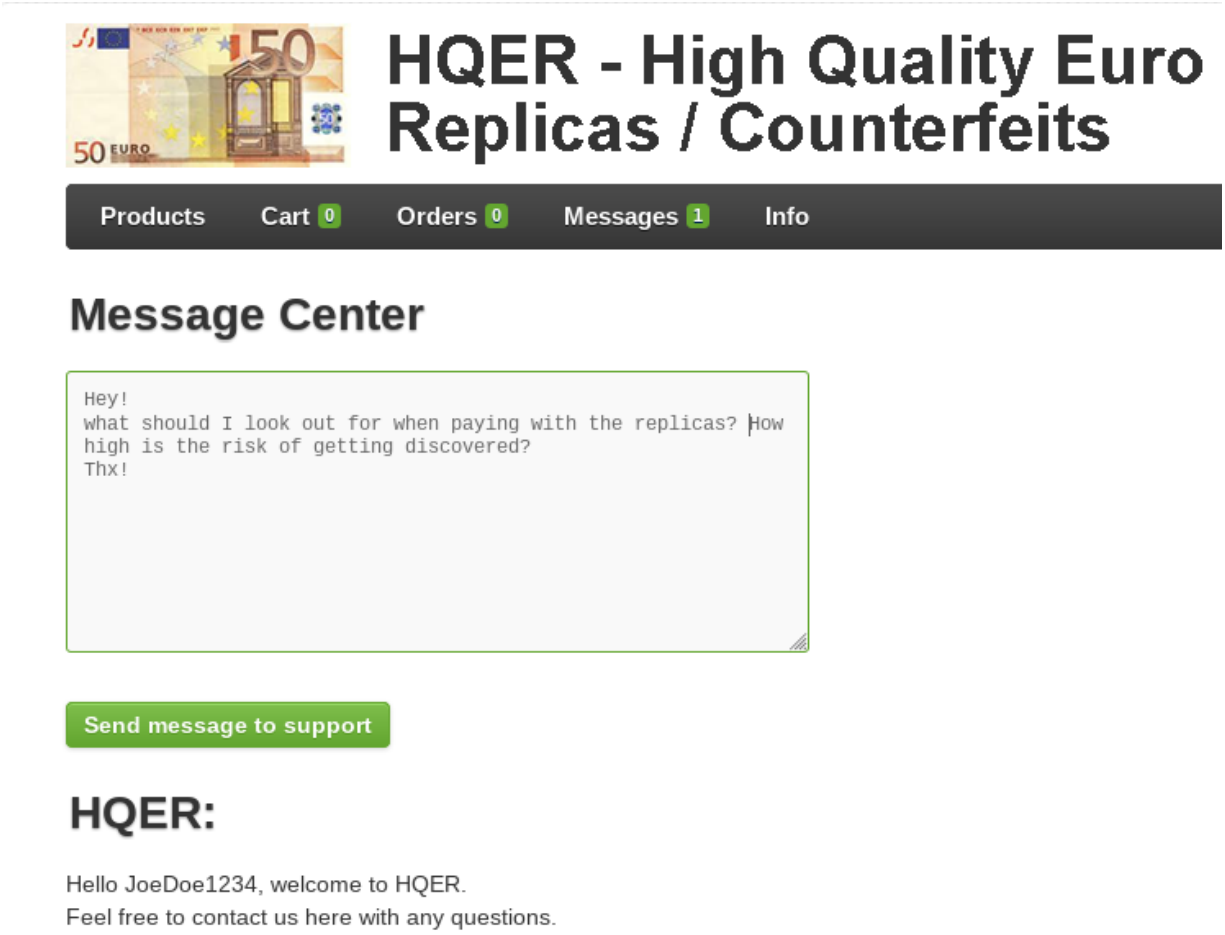


Abbildung 38: Messages HQER-Markt

24 Stunden nach der Erstellung der Nachricht wird die Webseite nochmal aufgerufen, um zu überprüfen, ob bereits eine Antwort erhalten wurde. Dies wird 48 sowie 72 Stunden nach dem Nachrichtversand wiederholt. Die Frage bleibt jedoch unbeantwortet. Auch eine Woche später wird leider keine Reaktion ersichtlich.

Aus Sicherheitsgründen wird vom Händler angeboten, den ganzen Message-Board zu löschen und somit alle Fragen und Antworten zwischen dem Käufer und Verkäufer zu entfernen.

7.3.3 Analyse der Kommunikation über Foren

Die zweitgrößte Rubrik in unserer Auswertung der Link-Kategorien wird mit 21% den Foren zugeschrieben. Laut der allgemeinen Definition wird ein Forum als eine Internetseite bezeichnet, *„auf der Meinungen, Gedanken und oft auch Dateien ausgetauscht und diskutiert werden“* (Ascherman, 2015). Nachdem die vom Darknet ermöglichte Anonymität einen der größten Vorteile des besagten Netzwerkes darstellt, ist es nachvollziehbar, dass ausgerechnet jene Plattformen, die diesen freien Meinungsaustausch ermöglichen – und somit Foren - unter den Nutzern an Beliebtheit gewinnen.

Um diese Plattformen auch praktisch näher zu untersuchen, wurde das Darknet-Forum „Talk.Masked | Talks and Notes. 2nd generation“ ausgewählt. Nach der Eingabe des Onion-Links

(Talk.Masked | Talks and Notes. 2nd generation, 2021) bricht die Suche jedoch mit der Meldung ab, dass die Seite leider nicht erreichbar ist. Es wäre möglich, dass das Forum aufgrund von Fremdeinwirkungen entweder heruntergefahren oder auf einen alternativen Link umgesiedelt werden musste. Solch ein Vorfall liegt leider in der Natur des Darknets. Nachdem es sich um ein Netzwerk mit keinen spezifischen Restriktionen handelt, werden gehostete Seiten öfter angegriffen als im Surface Web, worunter die Lebensdauer von Links leidet.

Als Ersatz wurde das Forum „DNMAvengers“ (mit zwei Treffern in der Auswertungstabelle) ausgewählt. Hinter dem Link (DNMAvengers, 2021) verbirgt sich eine deutlich komplexer aufgebaute Seite als es bei Darknet-Märkten der Fall ist.

Bevor dem Nutzer die Registrierung am Forum erlaubt wird, muss einer Nutzungsklausel zugestimmt werden. Diese weist darauf hin, dass unpassende, feindliche, verstörende Inhalte von Administratoren gelöscht werden. Bei inakzeptablem Verhalten werden Nutzer ohne Vorwarnung gebannt. Außerdem sichern die Administratoren deren Glaubwürdigkeit und Ruf, indem sie darauf aufmerksam machen, dass sie für die Inhalte von Postings und direkten Nachrichten anderer Nutzer nicht verantwortlich sind. Es wird ausdrücklich darauf hingewiesen, dass Cookies nach dem Login am Gerät des Nutzers gespeichert werden.

Nachdem bei der Registrierung am Forum vorausgesetzt wird, dass eine valide E-Mail-Adresse für eine potenzielle Kommunikation mit den Administratoren der Webseite angegeben wird, muss zuerst ein temporäres E-Mail-Konto angelegt werden. Hierzu nutzen wir den E-Mail-Dienst namens „ProtonMail“ (ProtonMail, 2021), da dieser im Rahmen des im früheren Kapitel beschriebenen Interviews stark gelobt wurde.

ProtonMail hat eine sehr angenehme Nutzeroberfläche und die Bedienung ist sehr einfach. Der Nachteil dieses E-Mail-Dienstes sind jedoch die Ladezeiten. Bei Nachrichten, welche Bilder, Icons oder Label beinhalten, werden diese exportiert und als Anhang der E-Mail angezeigt, um die minutenlangen Ladezeiten zu umgehen.

Nach einer Eingabe der neuen E-Mail-Adresse wird die Registrierung am Forum erfolgreich abgeschlossen und der Nutzer wird auf die Startseite von DNMAvengers geleitet. Hier befinden sich mehre Diskussionsräume, welche thematisch voneinander abgegrenzt werden. Neben allgemeinen Einträgen, welche die Nutzung vom Forum für neue Anwender erklären, finden wir auch Diskussionen zu den Themen „General Discussion“, „Regional Discussion“, „Announcement & News“, „Quality Control“ und „Vendor Products & Markets“.

Insbesondere die Händler bilden eine interessante Gruppe in diesem Forum. Es werden dedizierte Diskussionsräume angeboten, welche für Händler als eine Marketing-Plattform agieren. Sie nutzen Foren also als eine kostenlose Werbestelle. Größtenteils werden zahlreiche Drogen und ähnliche Substanzen angeboten. Außerdem werden Links geteilt, welche zu Darknet-Märkten leiten, die als vertrauenswürdig bezeichnet werden.

Einen vertrauenswürdigen Händler erkennt man auch an der Bezeichnung „Verified Market Vendor“. Dies bedeutet, dass der Händler beim Administrator des Forums um eine offizielle Verifizierung angefragt hat. Nach einer genauen Überprüfung bekommt ein legitimer Händler die entsprechende, verifizierte Bezeichnung und wird der Gruppe von legitimen Verkäufern

hinzugefügt. Es gibt jedoch auch weitere Gruppen, welchen die Nutzer des Forums hinzugefügt werden können. Der Administrator hat die Bezeichnung „Administrator“. Des Weiteren gibt es noch die Gruppen „Captain“, „Super Moderator“, „Mod & Verified Tester“ und „OG Avenger“. Der Grund für diese Bezeichnungen, sowie die Gruppen, weldieche sich dahinter verbergen, bleiben jedoch unbekannt. Alle Gruppentypen besitzen auch eine entsprechende Anzahl an Sternen. Der Administrator besitzt das Maximum, welches insgesamt acht Sternen entspricht und die Rangposition innerhalb des Forums symbolisiert.

Nicht nur die Händler müssen sich vom Administrator verifizieren lassen. Auch alle anderen Nutzer müssen nach der Registrierung überprüft werden. Zu diesem Zeitpunkt befinden sie sich im Status „Registered (not verified)“. Erst nach einer erfolgreichen Verifizierung durch den Administrator erhält ein Nutzer die Bezeichnung „Verified User“ und dazu eine Bewertung von zwei Sternen. Ohne diese Statusänderung wird es dem Nutzer weder ermöglicht, in einem der thematischen Diskussionsräumen zu posten noch direkte Nachrichten zu versenden.

Die Nutzung und Aufbau vom Forum ähneln stark einem Messenger. Es wird sogar der Aktivitätsstatus der User angezeigt. Ein grüner Kreis steht für „Online“, ein gelber für „Away“ und ein Grauer für „Offline“. Die Profilseite weist sogar Informationen über private Nachrichten, Gruppenmitgliedschaften und sogenannte „Buddy/Ignore List“ auf.

Um sich verifizieren zu lassen, wird bereits das erste Posting auf der Startseite gemacht. Bevor dieses verfasst wird, wird eine Analyse der Kommunikationsart der anderen Nutzer durchgeführt, um sich der Gesellschaft anzupassen und nicht aufgrund einer unpassenden Wortwahl aus der Menge rauszustechen. Die Kommunikation wird in sehr einfachem Englisch geführt. Die Nutzer verwenden kurze, leicht aufgebaute Sätze. Der Groß- und Kleinschreibung wird nicht besonders viel Aufmerksamkeit geschenkt. Die Atmosphäre ist sehr freundlich. Ein Nutzer äußert sich über das Forum, es fühle sich an wie sein Zuhause (siehe Abbildung 39).

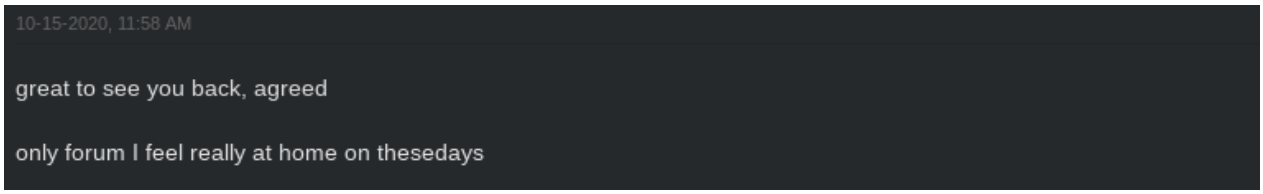


Abbildung 39: Nutzereinstellung zum Forum

Der erste Post der Verfasserin besteht somit aus nur zwei einfachen Sätzen, welche nicht besonders viele Informationen über die Nutzerin enthüllen:

> *„I am a new member looking for trustworthy vendors and interesting discussions. Also extremely interested in the darknet and curious about what is going on in the onion land”*

Nach 24 Stunden wird überprüft, ob sich der Status unseres Nutzers bereits geändert hat und wir somit vom Administrator als legitimer Nutzer anerkannt und der Gruppe von verifizierten Nutzern hinzugefügt wurden. Der erste Blick auf die Profilinformationen zeigt einen Erfolg (siehe Abbildung 40).

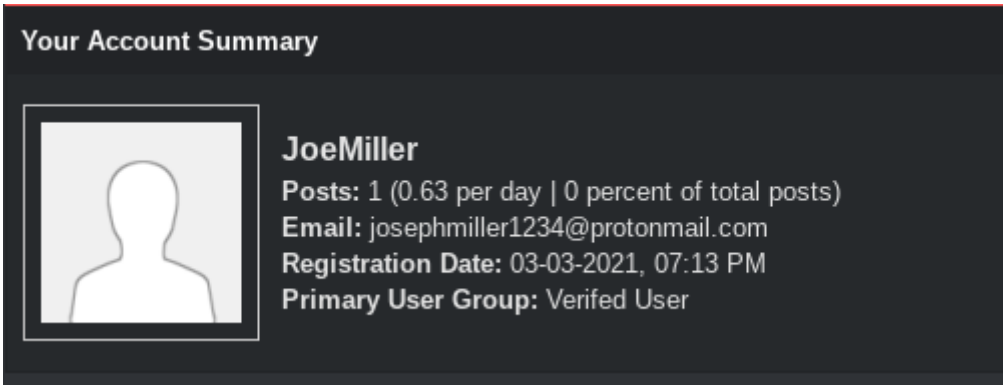


Abbildung 40: Profilansicht DNMAvengers

Nachdem wir nun an allen Diskussionen teilnehmen dürfen, werfen wir einen Blick auf das Board und einige Einträge. Das Konzept hinter den diversen Nutzergruppierungen und Bezeichnungen bleibt weiterhin unbekannt. Somit wird der „Captain“, also der Betreiber der Seite, welcher uns verifiziert hat, über eine direkte Nachricht kontaktiert.

Pro Eintrag im Forum werden die Anzahl von Antworten und Views mitprotokolliert und angezeigt. Wird der Papierkorb (also die bereits gelöschten Einträge) nicht mitberücksichtigt, so bekommt mit fast 3000 Nachrichten der Diskussionsraum „Introduction section for newly registered members“ die meisten Rückmeldungen. Hier haben wir bereits unseren Eintrag verfasst, um uns vorzustellen und verifizieren zu lassen.

Die meisten Views weist mit etwa 9500 Ansichten wiederum die Sektion „Markets“ auf. In diesem Bereich, wie der Name schon verrät, werden Diskussionen zum Thema Darknet-Märkte geführt.

Wir verfassen einen Post, um nach Tipps zu vertrauenswürdigen Plattformen zu fragen. Nachdem das Thema „Drogen“ im Forum allgegenwärtig ist, fokussiert sich unsere Frage auf Drogenhändler, welche nach Europa liefern.

Des Weiteren posten wir auch in die Rubrik „Kryptowährungen“. Hier fragen wir nach Erfahrungen und Meinungen anderer Nutzer zu einer Verbindung zwischen Twitter-Einträgen von Elon Musk und der Aktie von Bitcoin und Dogecoin. Gefragt wird, ob Posts von Musk auf Twitter eine Auswirkung auf den Aktienmarkt haben könnten.

Allgemein bietet dieses Forum eine Vielzahl an Kommunikationsmöglichkeiten. Es können neue Diskussionsthemen eingetragen, auf bestehende reagiert sowie direkte Nachrichten verschickt werden. Die Anzahl der Diskussionsräume ist groß und die Bedienung der Seite sehr einfach.

Nachdem die Kommunikation über Foren so breit gefächert ist und viele Möglichkeiten anbietet, wird noch ein weiteres besucht, um mehr Eindrücke zu dieser Kommunikationsform zu bekommen.

Wird im Surface-Web nach Darknet-Seiten gesucht, leitet die Suche zu einigen passenden Empfehlungen. So entdecken wir eine nützliche Liste von Ronella van der Burgt, welche uns auf die Seite „HiddenAnswers“ verweist. *„Sie könnten also Themen entdecken, von denen Sie lieber nichts wissen wollten“* (van der Burgt, Dark-Web-Seiten, die sich lohnen, 2020).

Es handelt sich hierbei um ein Forum, da HiddenAnswers die für Foren charakteristischen Merkmale aufweist. Die Kommunikation erfolgt asynchron und Einträge werden gespeichert. Außerdem gibt es eine Gruppe von Administratoren, welche sich um die Geschehnisse auf der Webseite kümmert. Themen werden in Kategorien aufgeteilt (SEO-Analyse, kein Datum).

Was wir untersuchen wollen, ist die Ehrlichkeit und die Offenheit der Nutzer. Wie diskret läuft die Kommunikation ab, wenn alle Teilnehmer anonym sind?

Nachdem die Seite von HiddenAnswers aufgerufen wird (HiddenAnswers, 2021), wirkt die Offenheit der Nutzer sehr ernüchternd. Neben allgemeinen Erkundungen zum Darknet und seinen Diensten werden auch Fragen gestellt wie „What do you think happen for abused child porn kids when they grow up?“ oder „What song would you kill yourself to?“. Neben solchen unangenehmen Fragen gibt es jedoch auch zahlreiche andere, die sehr persönlich sind und sich auf die uneingeschränkte Offenheit der Nutzer verlässt (siehe Abbildung 41).

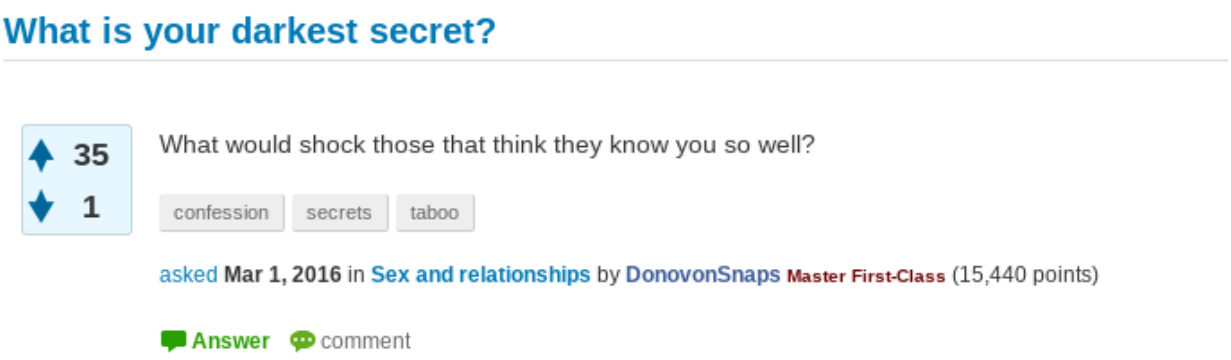


Abbildung 41: „What is your darkest secret?” - HiddenAnswers

Die Antworten auf diese Frage sind sehr unterschiedlich. Einige Nutzer belächeln sie nur, andere wollen deren wahre Geheimnisse nicht preisgeben und die restlichen Anwender antworten zwar ehrlich, jedoch mit so unpassenden, beunruhigenden bis verwerflichen Geschichten. Diese erzählen von Prostitution, Missbrauch, Pädophilie, Depressionen, Mord. Die Schreibweise und Wortwahl sind sehr breitgefächert, emotionsvoll bis beängstigend. Selbstverständlich besteht keine Garantie, dass diese Geschichten der Wahrheit entsprechen. Es stellt sich jedoch die Frage, warum die Erzähler lügen sollten, wenn deren Identität nicht enthüllt werden kann.

Eine weitere Frage auf HiddenAnswers, erkundet sich danach, ob die Gefragten online sowie offline die gleiche Person sind, ohne jegliche Abweichungen im Verhalten.

Hierbei werden viele unterschiedliche Antworten geliefert. Einige Forum-Nutzer behaupten, sie seien online sowie offline eine und dieselbe Person und das Verhalten würde sich kaum unterscheiden. Andere geben zu, dass sie online ehrlicher und offener agieren und offline eher unsicher, schüchtern und introvertiert sind (siehe Abbildung 42). Nur sehr wenige sind offline offener und direkter als bei der Interaktion im WWW.

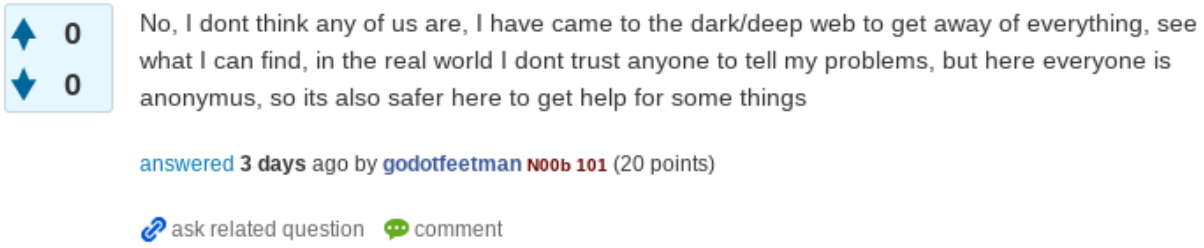


Abbildung 42: Unterschiede zwischen der Interaktion online und offline – HiddenAnswers

HiddenAnswers stellt ein perfektes Beispiel dar, wie offen und ehrlich die Kommunikation im Darknet ablaufen kann, eine Sicherheit für die Korrektheit der Antworten gibt es aber selbstverständlich nicht. Natürlich gibt es auch Nutzer, die trotz der gegebenen Anonymität nicht jeden Gedanken oder jede Meinung teilen möchten. Die Scheugrenze ist jedoch im Darknet auf jeden Fall deutlich niedriger als es im Surface Web der Fall ist.

7.3.4 Analyse der Kommunikation über Chatrooms

Auf dem dritten Platz bei der Auswertung von Kommunikationsplattformen im Darknet bzgl. Popularität haben sich dicht hinter Foren die sogenannten „Chatrooms“ platziert. Chatrooms werden zur Kontaktaufnahme und zum Meinungsaustausch zwischen zwei oder mehreren Nutzern angewendet. Diese Kommunikation passiert in Echtzeit, synchron und die gesendeten Nachrichten werden nicht über längere Zeit gespeichert (TechTarget , 2005).

Zur Untersuchung der Nutzung von Chatrooms im Darknet wurde die Webseite „Chat with strangers“ ausgewählt. Nach dem Aufruf der Seite (Chat with strangers, 2021) wurde eine einfach gestaltete Seite geladen. Den Nutzern werden zwei Optionen angeboten: „Random chat“ oder „Chat with friend“. Laut der „About“-Seite, welche auch auf der Startseite verlinkt ist, bieten diese zwei Möglichkeiten entweder eine Konversation mit anderen, fremden Nutzern oder mit Bekannten. Im zweiten Fall wird ein Link generiert, welcher mit dem Gesprächspartner geteilt werden kann. Außerdem wird die Anzahl von Nutzern angezeigt, welche im Moment online sind. Bisher wurden immer mehr als 100 Nutzer angezeigt, die höheren Zahlen werden zu späteren Abendstunden erreicht.

Bei Auswahl der Option „Random Chat“. wird man gleich zu Beginn zur Begrüßung aufgefordert. Nun wird man vor die erste Hürde gestellt. Es stellt sich die Frage: „Wie fange ich eine Konversation an, wenn ich alles, unzensiert und anonym fragen kann?“.

Insgesamt werden zehn Konversationen geführt. Die kürzesten dauern nur Sekunden. Beim Kommunizieren über Chatrooms ist offensichtlich der Faktor der Kommunikation in Echtzeit besonders ausschlaggebend. Bei einer Konversation braucht die Verfasserin eine Minute, um eine passende Antwort zu formulieren, was jedoch dem Gesprächspartner zu lange dauert und somit wird von seiner Seite der Chat abgebrochen. Eine schnelle Reaktion ist zwar bedeutsam, in dem aktuellen Szenario jedoch schwierig. Nachdem TAILS über den Arbeitsspeicher läuft, dauert es länger bis neue Inhalte geladen werden. Dies stellt die größte Herausforderung bei der Kommunikation über Chatrooms dar.

Die längste Konversation dauert 21 Minuten. Im Rahmen dieses Gesprächs wird sogar der reale Instagram-Profil geteilt. Im Laufe des Gesprächs fragt das Gegenüber außerdem nach dem Namen. Selbstverständlich lügen beide. Wir haben uns jedoch für einen weiblichen Namen entschieden, um zu sehen, ob vor Frauen private Informationen leichter preisgegeben werden. Das Ergebnis ist, dass unser Gegenüber den Kontakt zu uns nicht verlieren will (siehe Abbildung 43). Die Wahrscheinlichkeit, dass sich zwei Gesprächspartner nach einem abgebrochenen Chat auf derselben Plattform nochmal treffen, ist sehr gering, da die Kommunikation auf einem Zufallsprinzip aufgebaut wird. Überraschend ist in diesem Fall, dass nach einer ICQ-Nummer gefragt wird, wobei sich dieser Kommunikationskanal seit Jahren keiner großen Popularität mehr erfreuen kann.

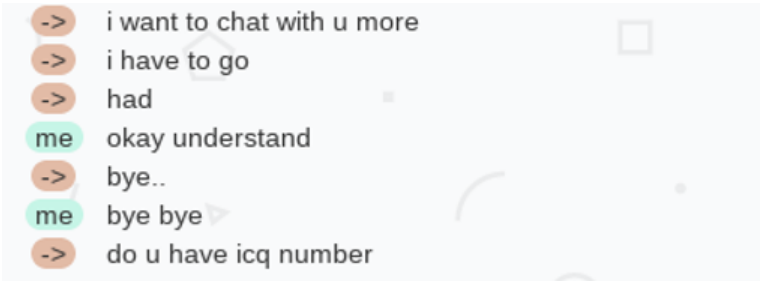


Abbildung 43: Chat über "Chat with strangers"

Um auszutesten, wo die Grenze der offenen Konversation ist, wird auch nach der Herkunft des Gesprächspartners gefragt. Ein anderer Nutzer, welcher bereits im Jahr 2019 das Darknet besucht hat, hat die Frage nicht beantwortet, sondern den Hinweis gegeben „i cant say – you know“. Ein anderer Nutzer, welcher erst seit ein paar Wochen im Darknet unterwegs ist, hat zumindest die Information über den Kontinent, auf dem er sich befindet, preisgegeben.

Die Direktheit, mit welcher man in manchen Gesprächen konfrontiert wird, ist jedoch manchmal sehr beunruhigend bis beängstigend. So fragt ein minderjähriges Mädchen nach jemandem, der es im Darknet zu einem Pornostar machen würden. Andere Anwender fragen direkt „like little boys?“ oder „wanna see my son?”. Ein Nutzer hat in einem Moment zugegeben sich für Hacking zu interessieren und darauffolgend gefragt, ob wir ein „crazy pic“ herunterladen möchten. Dies könnte ein Hacking-Versuch sein, deswegen wird das Gespräch gleich beendet.

Allgemein ist deutlich geworden, dass Chats vor allem zum Wissensaustausch genutzt werden. Entweder die Nutzer sind das erste Mal im Darknet und wollen sich allgemeine Tipps von erfahrenen Mitgliedern holen. Oder sie suchen nach Plattformen, die bestimmte Güter und Dienstleistungen anbieten. Nachdem im Darknet viele betrügerischen Seiten zirkulieren, ist es verständlich, dass zuerst bei Anderen nachgefragt wird, bevor ein misslungener Kauf getätigt wird. Die Kommunikation ist zwar sehr offen und direkt, es gibt jedoch trotzdem Grenzen, es werden nicht alle Informationen mit dem Gesprächspartner geteilt.

7.4 Zusammenfassung der Ergebnisse und Ausblick in dir Zukunft

Nachdem das Darknet viele Vorteile mit sich bringt, ist es nachvollziehbar, dass sich dieses Netzwerk einer hohen Anzahl an Nutzern erfreut. Das Netzwerk stellt für viele das böse, unerforschte Internet dar und genau diese Charakteristik macht das Darknet so attraktiv, denn Neugierde liegt in der Natur des Menschen.

Die Anonymität und die damit verbundene Freiheit können in keinem anderen Teil des WWW in dem Ausmaß gefunden werden, wie es beim Darknet der Fall ist.

Oscar Wilde durchschaute die wahre Natur des Menschen bereits Ende des 19. Jahrhunderts, denn er schrieb:

„Man is least himself when he talks in his own person. Give him a mask, and he will tell you the truth" (Wilde, 1981).

Nachdem das Darknet freie Meinungsäußerungen und offene Diskussionen über Ideen oder private Gedanken ermöglicht, stellt sich somit die Frage, ob Oscar Wilde Recht hat und ob die Kommunikations- sowie Verhaltensweise der Menschen sich ändert, wenn sie hinter einer Maske versteckt sind bzw. in diesem Fall hinter dem vom Darknet ermöglichten Grad an Anonymität.

Auf Basis dieser Gedanken ist die Forschungsfrage der Masterarbeit entstanden:

„Welche Kommunikationskanäle werden für die Interaktion zwischen NutzerInnen vom Darknet am häufigsten eingesetzt?"

Die Frage wurde mit Hilfe einer umfangreichen Auswertung von Onion-Links, welche von vier Wikis im Darknet gesammelt wurden, beantwortet.

Der Ansatz dafür basiert auf der Logik von „Link-Popularity" und liefert drei eindeutige Ergebnisse:

- Darknet-Märkte,
- Foren und
- Chatrooms

stellen die am häufigsten eingesetzten Kommunikationskanäle im Darknet dar.

Nachdem Darknet-Märkte stark vertreten sind, wurde eine regere Kommunikation erwartet. Überraschenderweise wird die Möglichkeit einer Kontaktaufnahme als Marketing-Komponente eingesetzt, denn in vielen Fällen muss zuerst eine Bestellung getätigt werden, bevor der Verkäufer kontaktiert werden kann. Die Kommunikation war sehr enttäuschend, auch Tage nach dem Versenden einer Nachricht wurde keine Rückmeldung erhalten.

Während erste Erkenntnisse und Erfahrungen mit Darknet-Märkten eher ernüchternd waren, so war die Kommunikation über Foren im Darknet jedoch überwältigend.

Foren legen viel Wert auf die Sicherheit der Nutzer. Nur glaubwürdige Anwender dürfen an der Kommunikation aktiv teilhaben. Händler dürfen nicht spammen, sondern bekommen dedizierte Kanäle für deren Postings. Die Anonymität, welche bei Diskussionen über Foren gegeben ist,

wird genutzt, um die dunkelsten Gedanken loszuwerden, Meinungen zu äußern und Ideen zu teilen ohne Angst vor Verachtung oder anderen Konsequenzen zu haben.

Die Nutzer sind perfekt geschützt und sprechen somit direkt aus der Seele heraus. Der Wahrheitsgehalt ihrer Antworten kann aufgrund der Anonymität aber natürlich nicht überprüft werden und so stellt sich immer auch die Frage nach der Glaubwürdigkeit einer Aussage, da Lügen anonym hervorragend verbreitet werden können.

Von allen drei Kommunikationskanälen bringen uns die Chatrooms der Natur des Darknets am nächsten. Die Anwender bekommen das echte Gefühl, ein Teil der Darknet-Community zu sein. Das Gespräch dauert zwar nur ein paar Minuten, besitzt jedoch ein dediziertes Ziel. Die Offenheit, Direktheit und Ehrlichkeit der Kommunikation per Chatrooms kann in manchen Fällen jedoch beunruhigend bis beängstigend sein.

In Bezug auf die Beantwortung der Hypothesen kann festgestellt werden, dass das Darknet nicht nur für illegale Geschäfte verwendet wird und somit Alternativhypothese eins als zutreffend angesehen werden kann. Weiters verwenden das Darknet und seine Nutzer für die Interaktion untereinander mehrere, oben angeführte Kommunikationskanäle, womit auch Alternativhypothese zwei zutrifft.

Es gibt viele Vorteile, die das Darknet mit sich bringt, viele Chancen und Opportunitäten, welche im Surface Web nicht realisierbar wären. Jedenfalls ist die Annahme, das Darknet würde nur für illegale Tätigkeiten genutzt werden, falsch, zahlreiche Personengruppen die Anonymität des Darknets benötigen, um beispielsweise der Unterdrückung eines diktatorischen Staates entgegenzuwirken.

Der Kommunikationsablauf im Darknet ist stark von der Verschleierung der Identität beeinflusst. Die Personen kommunizieren viel direkter und offener als im Surface Web. Die Freiheit der Äußerung, welche im Darknet erlaubt wird, kann, wie es bei vielen Bereichen des Darknets der Fall ist, auch für nicht legitime Absichten genutzt werden.

Drogen, Waffen oder Sexualdelikte gehören zu einigen der Themen, welche im Darknet gehäuft behandelt werden. Allgemein kann gesagt werden, dass die anonyme Kommunikation im Darknet ein deutlicher Vorteil des Netzwerks ist, solange sie für legale, sinnvolle Themen eingesetzt wird.

Außerdem kann der Grundgedanke hinter Darknet, so die volle Freiheit beim Abwickeln eines Gesprächs, nicht zur Gänze ausgenutzt werden, da trotzdem im Hinterkopf behalten werden muss, dass die Polizei und Staatsbehörden hinter jedem Nutzer versteckt sein könnten.

Das Darknet hat sicherlich ein starkes Zukunftspotenzial. Solange es einen Nutzen für dieses Netzwerk geben wird, wird es auch weiterhin bestehen. Der Mensch ist ein neugieriges Wesen, das viel Wert auf die eigenen Freiheiten legt.

Die Natur des Darknets macht es schwer bis unmöglich, dieses Netz zu zensurieren oder Seiten vom Netz zu nehmen. Um jedoch zu verhindern, dass eine potenziell höhere Nutzerzahlen des Darknets in Zukunft katastrophale Konsequenzen mit sich bringen, müssen Regierungen und

Strafverfolgungsbehörden Interventionsstrategien einführen und einen angemessenen regulatorischen Rahmen schaffen. Das Darknet erzeugt keine illegalen Waren, sondern fungiert als Vermittler für den Handel mit diesen in der analogen Welt. Um ein solideres Verständnis für die Rolle des Darknets bei der Ermöglichung des Handels zu generieren, müssen kontinuierlichere Überwachungssysteme implementiert werden.

Das Darknet wird für viele ein Mysterium bleiben. Es wäre dennoch empfehlenswert die Bevölkerung entsprechend aufzuklären, da das Darknet ein faszinierendes Netzwerk mit einer hohen Attraktivität darstellt.

Am gefährlichsten ist die Nutzung von Darknet für unerfahrene Nutzer, welche sich vor dem Ausflug ins Darknet nicht entsprechend informiert und vorbereitet haben. Genau solche unvorbereiteten Ausflüge ins Darknet machen betrügerisches Handeln überhaupt erst möglich. Wäre man jedoch besser informiert, so würde man einsehen, wie viele Potenziale das Darknet mit sich bringt, wie viele Vorteile sich hinter diesem Netzwerk verbergen und wie bereichernd die Erfahrung eines direkten Kontakts mit dem Darknet für jeden Einzelnen sein kann.

ANHANG A - 1. Anhang

Am 04. Februar 2021 fand in Graz ein Interview zwischen einem Darknet-Nutzer, welcher aufgrund der Thematik anonym bleiben möchte, und der Autorin statt mit dem Ziel, die Meinung der befragten Person zu Darknet zu analysieren sowie ihre bereits gesammelten Erfahrungen zu diskutieren.

Transkript:

Interview am 04. Februar 2021

Teilnehmer:

A = Anonymer Befragter (Gast)

K = Eliska Krnavkova (Interviewer)

K: Warum haben Sie da Darknet aufgesucht? Was hat Sie auf das Darknet aufmerksam gemacht?

A: Mein erster Besuch im Darknet war im Jahr 2012, damals noch über einen auf Windows installierten Tor-Browser. Der Grund für diesen ersten Besuch war denkbar einfach. Ich habe zum ersten Mal vom Darknet gehört und mir gedacht „So schwer wird das wohl nicht werden, ins Darknet zu kommen“. Da ich in dieser Zeit noch in einem Alter war, in dem man seine Schulfreunde gerne beeindruckt hat, wird wohl auch die Möglichkeit, mit diesem „illegalen“ Ausflug angeben zu können, eine wesentliche Rolle gespielt haben.

K: Wie oft waren Sie bereits im Darknet unterwegs?

A: Die Frage ist gar nicht so einfach zu beantworten. Wenn ich ihnen jetzt eine Zahl nennen würde, wäre das nicht sehr repräsentativ für die Zeit, die ich im Darknet verbracht habe. In Stunden gerechnet habe ich geschätzt etwa um die 100 bis 150 Stunden dort verbracht. Die meisten davon mit reinem Suchen. Zu wissen, dass eine gewisse Seite existiert bedeutet ja nicht, sie auch finden zu können.

K: Wie haben Sie sich verbunden? Welche Sicherheitsmaßnahmen haben Sie vorgenommen?

A: Bei meinen ersten zwei Ausflügen ins Darknet habe ich mit einer über Google gefundenen Anleitung den Tor-Browser auf meinem Windows 7 Rechner installiert. Würde ich Ihre Frage meinem damaligen, jungen Selbst stellen, wäre meine Antwort vermutlich „Ich pass schon auf“ gewesen. Kurz gesagt, meine damalige einzige Sicherheitsvorkehrung war der Entschluss, keine persönlichen Informationen preiszugeben. Die Idee über Windows ins Tor-Entz einzusteigen hatte auch den tollen Vorteil, dass mein PC nach jedem Besuch im Darknet komplett neu

aufgesetzt werden musste. Die Menge an Viren, Trojanern und in erster Linie Adware war unbeschreiblich. Und leider auch nicht mehr mit Bereinigungs-Tools entfernbar.

Wenn ich mich heute ins Darknet wage, dann mit angemessenen Sicherheitsvorkehrungen. Ich bin kein Experte auf dem Gebiet der Cyber-Security und gebe auch nicht vor, einer zu sein. Aber ein gewisses Maß an Recherche und bisherigen Erfahrungen hat mich auf einen Wissenstand gebracht, mit dem ich mich beim Surfen im Darknet nichtmehr fürchten muss. Welche Maßnahmen ich nun genau treffe? Ich lasse mir einen großen Teil der Sicherheit von einem dafür geschaffenen Linux-basierten Betriebssystem abnehmen: Tails. Das hat den wunderbaren Vorteil, dass es einerseits als Live-System von einem USB-Stick aus verwendbar ist und anderseits keine Spuren auf der Festplatte des Rechners hinterlässt, da das gesamte OS rein auf dem Arbeitsspeicher läuft. Der Arbeitsspeicher hat wiederrum den Vorteil, dass er kein persistenter Speicher ist und sich komplett leert, sobald der Strom abgedreht wird. Beim Surfen im Darknet selbst hängen meine Maßnahmen immer vom Grund ab, wieso ich gerade da bin. Will ich mit Personen kommunizieren? Dann suche ich mir einen sicheren Kommunikationsweg, bei dem ich die Verschlüsselung meiner Nachrichten selbst kontrollieren kann. Ist es wichtig, möglichst wenige Anhaltspunkte in Form von Metadaten an meinen Kommunikationspartner zu senden? Dann verwende ich einfache Worte. Am besten einfaches, sauberes Englisch ohne komplexe Satzstellungen. Am Ende läuft es für mich darauf hinaus, dass ich mir vor jeder Aktion im Darknet genau überlege, welche Risiken dabei auftreten können und wie ich diese minimiere.

K: Was hat Sie beim Surfen im Darknet am meisten interessiert oder sogar fasziniert?

A: Das Internet selbst ist einer der größten Meilensteine unserer modernen Weltgeschichte. Ich war früher immer der Meinung, dass ich niemals alle Seiten die man googeln kann in meinem Leben besuchen werde oder könnte. Und obwohl das vermutlich immer noch zutrifft, war die Erkenntnis, dass das von den meisten Menschen verwendete Internet, also das Surface Web, nur einen unglaublich kleinen Teil des gesamten Internets darstellt, eine unbeschreiblich befreiende Erfahrung. Die Möglichkeit, aus dem von unseren Regierungen und ISPs vorgegebenen „sicheren“ Internet auszubrechen und sich in riskantes und gefährliches Terrain zu begeben, war ein Gefühl, dass sich nur mit dem wunderbaren Begriff Freiheit beschreiben lässt.

K: Was hat Sie beim Surfen im Darknet am meisten schockiert bzw. überrascht?

A: Mit dieser Frage begeben wir uns in ein Themengebiet, in das sich die meisten Menschen vermutlich nur ungern begeben. Noch vor meinem ersten Besuch im Darknet war mir bewusst, wofür es verwendet wird und was mich dort erwartet. Trotzdem hat mich dabei als erstes überrascht, wie unverhohlen Werbung für gewisse Themen gemacht wird. Auf einer Seitenbeschreibung ohne blumige Worte umschrieben zu lesen „Der größte Drogen und Waffenmarkt der EU – jetzt mit Paketverfolgung“ war eine surreale Erfahrung. Aus irgendeinem Grund habe ich damals erwartet, dass solche Dinge auch im Darknet etwas verschleiert umschrieben werden. Erwartet hätte ich mir etwas wie „Kaufen Sie unsere bunten Smarties“.

Wobei dabei natürlich jeder weiß, dass keine wirklichen Smarties gemeint sind. Aber nein. „Wir haben die besten Drogen!“ hat mich dann doch überrascht. Es war so … direkt.

Der größte Schockmoment für mich war jedoch das Ergebnis von Unvorsichtigkeit meinerseits. Ich habe an dem Tag nichts Spezielles im Darknet gesucht, mein Ziel war es eher, spannende Artikel von Whistleblowern zu entdecken. Dabei bin ich auf eine Seite gestoßen, die einen sehr zweideutigen Namen hatte. Ich kann mich nicht mehr genau daran erinnern, aber es war etwas in der Richtung wie „Minor leaks“. Übersetzt habe ich das als „kleinere Enthüllungen“ gelesen. Ich werde jetzt nicht im Detail darauf eingehen. Sie können sich vermutlich denken, was dort zu sehen war.

K: Haben Sie Kontakt zu anderen Darknet-Nutzern aufgenommen und wenn ja, in welcher Form?

A: Ja, Kontakt zu anderen Nutzern habe ich zweimal aufgenommen. Beide Male habe ich dafür einen verschlüsselten Schweizer Email-Service Namens Protonmail verwendet. Dieser E-Mail Service hat den unglaublich angenehmen Vorteil, dass ein Tool zur Verschlüsselung mittels OpenPGP bereits mitverbaut ist. Einfach zu nutzen, moderne Weboberfläche und gute Dokumentation.

Warum ich Kontakt aufgenommen habe? Das erste Mal um Informationen zu erhalten. Eine Seite hat Kredikarteninformationen zum Verkauf angeboten und ich habe ganz ungeniert nachgefragt, woher sie diese Informationen eigentlich bekommen und wie ihr Geschäftskonzept aussieht. Entgegen meiner Erwartungen habe ich sogar eine recht aufschlussreiche Antwort erhalten. Dafür ab diesem Zeitpunkt auch eine Menge Spam. Die zweite Kontaktaufnahme war im Gegensatz recht langweilig. Ich hatte ein Problem bei der Registrierung auf einer recht bekannten Seite und deswegen den Support kontaktiert. Interessant dabei war allerhöchstens, dass der Support dort um ein Vielfaches kompetenter war, als ich es im Surface Web jemals erlebt habe.

K: Haben Sie im Darknet eine Ware verkauft oder gekauft?

A: Ich habe zwei Mal etwas gekauft. Beide Male habe ich mit Bitcoin bezahlt. Die eine Ware ist angekommen, das war ein Kaktus, der bei uns wegen seiner Inhaltsstoffe nicht käuflich zu erwerben ist. Die andere ist nicht angekommen, da ich zu diesem Zeitpunkt noch nicht gewusst habe, wie eine sichere Transaktion dort abzuwickeln ist. Kurz gesagt jemand hat sich über mein Geld gefreut und hatte keinerlei Anreiz, mir dafür etwas zukommen zu lassen. Man lernt ja bekanntlich aus seinen Fehlern.

K: Besuchen Sie das Darknet weiterhin und falls nicht, warum?

A: Derzeit besuche ich das Darknet so gut wie gar nicht. Wenn das Thema in Gesprächen mit Freunden aufkommt, kommt hin und wieder Tails zum Einsatz um zu zeigen, welche unglaublichen und dubiosen Seiten man im Darknet findet. Das Stöbern habe ich mittlerweile aufgegeben. Den Grund dafür ist der vorhin beschriebene Schockmoment.

K: Sind Ihnen große Unterschiede zum Surfen im Surface Web aufgefallen und wenn ja, welche?

A: Diese Frage stellen sich vermutlich die wenigsten, die kein technisches Vorwissen haben. Ja es gibt große Unterschiede. Der erste der einem sofort auffällt, ist das Thema der Ladezeiten. Sie kennen vermutlich Momente, in denen Sie nur unglaublich langsames Internet zur Verfügung haben. In denen eine Seite eine gefühlte Ewigkeit braucht, bis sie vollständig geladen wird. So ähnlich ist das auch im Darknet. Einerseits ist der Aspekt der Sicherheit über das Tor-Netzwerk ein entscheidender Faktor dafür, andererseits auch die Fehlende Regulierung und Optimierung des Darknets.

Ein weiterer Punkt der mir dazu einfällt ist die Verfügbarkeit oder Erreichbarkeit von Seiten. Seiten mit illegalen Inhalten werden oft von Behörden attackiert oder entfernt. Andere werden von versierten Gruppen mit unlauteren Absichten übernommen oder attackiert. Es gibt eine Vielzahl von Gründen, warum ein Link, der gestern noch tadellos funktioniert hat, heute nicht mehr erreichbar ist. Oder zwar noch erreichbar ist, aber auf einmal eine gänzlich andere Seite aufruft. Oder im schlimmsten Fall eine Seite aufruft, die exakt aussieht wie die gewünschte Seite, allerdings nur eine Kopie ist, um ihre Zugangsdaten zu stehlen. Wer im Darknet unterwegs ist, muss sich also in Geduld üben und lernen, Seiten zu erreichen, Fakes zu erkennen und diese auch zu überprüfen.

K: Würden Sie das Darknet anderen Internetnutzern empfehlen?

A: Die Antwort auf diese Frage muss ich an eine Bedingung knüpfen. Leben diese „anderen Internetnutzer“ in einem Land, dessen Regierungsform einer Diktatur gleichkommt? Dann würde ich das Darknet empfehlen, da es die einzige Möglichkeit ist, der örtlichen Zensur zu entkommen. Leider ist dieser Weg auch mit enormem Risiko verbunden. In China beispielsweise gibt es Berichte über mehrjährige Haftstrafen aufgrund der Verwendung eines VPN-Dienstes. Hier ist also beim Informationsaustausch im Darknet Vorsicht geboten.

Für alle anderen gilt: Es kommt darauf an. Haben Sie vor, mit illegalen Machenschaften Geld zu verdienen oder Gegenstände zu erwerben, die Sie aus gutem Grund nicht legal erwerben dürfen? Dann bleibt Ihnen neben dem Schwarzmarkt nur noch das Darknet als Option. Für alle, die jedoch ein Leben ohne Angst führen wollen, kann ich das Darknet nicht empfehlen. Es ist spannend den Ausflug ins Darknet zu wagen, aber wirklichen Nutzen haben Sie als Normalverbraucher dadurch nicht.

K: Welche Tipps würden Sie einem Einsteiger in das Thema „Darknet“ geben? Worauf soll unbedingt geachtet werden?

A: Überlege dir zuerst, warum du das Darknet nutzen willst. Falls es kein wirklich guter Grund ist, wäre das der richtige Zeitpunkt, sich nicht weiter mit dem Thema zu beschäftigen. Du willst dich trotzdem weiter damit beschäftigen? Dann solltest du dich zuerst mit allen Aspekten des Darknets vertraut machen. Welche Arten von Personen nutzen das Darknet und wofür? Wie kann ich meine

Kommunikation verschlüsseln? Wie stelle ich sicher, nicht betrogen zu werden? Und die wichtigste aller Fragen: Was habe ich zu verlieren, wenn mich jemand gezielt attackiert? Wenn du dir also sicher bist, worauf du dich einlässt und dir das Risiko bewusst ist, bleibt nur noch die Erfahrung, die du beim Surfen im Darknet selbst erhältst. Simples learning by doing.

K: Finden Sie, dass das Darknet ein Zukunftspotenzial besitzt?

A: Das ist eine schwierige Frage. Ich hoffe, dass das Darknet auch in Zukunft keine größere Rolle im Alltag der meisten Menschen in Europa spielen wird. Der einzige Grund, der mir spontan einfallen würde, warum es dazu kommen könnte wäre eine Entwicklung in Richtung eines totalitären Überwachungsstaates. Den Zwang, sich im Darknet bewegen zu müssen, nur um die eigene Meinung ohne Konsequenzen mit Mitmenschen teilen zu können, wünsche ich mir bei uns jedenfalls nicht.

K: Wofür sollte Ihrer Meinung nach Darknet am besten eingesetzt werden?

A: Wenn ich diese Frage nicht aus einer technischen Perspektive heraus beantworte, sondern eher aus der, der typischen und bekannten Verwendungszwecke – dann würde ich behaupten, dass die Möglichkeit zum politischen Protest die einzig positive und gleichzeitig auch wichtigste Einsatzmöglichkeit darstellt. In Ländern, in denen politische Gegner unterdrückt, inhaftiert, gefoltert und ermordet werden, bietet das Darknet oft einen der letzten Möglichkeiten, diesen politischen Systemen Widerstand zu leisten.

K: Haben Sie je daran gezweifelt, ob Ihr Aufenthalt im Darknet von legaler Natur ist?

A: Im Gegenteil. Ich war mir jederzeit bewusst, welche meiner Aktionen legaler und welche davon illegaler Natur waren. Die Vorstellung, dass das Surfen im Darknet selbst illegal ist legt man ziemlich schnell ab, wenn man sich ein wenig damit beschäftigt hat. Das ist an sich nicht verboten. Nur nicht sonderlich ratsam für Personen, die sich davor nicht ausreichend informiert haben. So in etwa wie das in Österreich beliebte Skitouren-gehen. Man ist sich darüber bewusst, dass man präparierte Pisten verlässt und sich in Gefahr begibt. Dieses Bewusstsein schafft allerdings auch instinktiv ein gewisses Maß an gesteigerter Wahrnehmung.

K: Wie haben Sie sich im Darknet orientiert? Woher wussten Sie wo Sie was finden?

A: Die Orientierung im Darknet ist anfangs wirklich eine der unangenehmsten Tätigkeiten. Dazu muss einem anfangs erst einmal bewusstwerden, dass das bekannte, sichere Surface Web gerade einmal vier Prozent der im Internet verfügbaren Informationen abdeckt. Der Rest davon befindet sich im Darknet oder Dark Web.

Das finden von gesuchten Informationen ist deshalb ein Prozess, der eine Mengen an Geduld erfordert. Natürlich gibt es Linksammlungen und Suchmaschinen, die die Suche erleichtern, aber ganz so einfach wie etwas zu googeln ist es dann letztlich doch nicht.

Etwas einfacher gestaltet sich das Surfen dann, wenn man den Namen der gewünschten Seite bereits kennt. In diesem Fall gibt es die Möglichkeit, alternative und überprüfbare Links für das gewünschte Ziel zu finden. Links die entweder ein zeitliches Ablaufdatum haben oder aus anderen Gründen nicht mehr funktionieren, lassen sich durch solche Seiten angenehm durch aktuellere ersetzen.

K: Welche Seiten haben Sie im Darknet besucht?

A: Natürlich kann ich mich nicht an alle besuchten Seiten erinnern. Was auch daran liegt, dass viele der Seiten die ich besucht habe keinen eindeutigen Namen besitzen. Nur die populärsten Seiten haben Namen, die im Darknet bekannt sind. Der einzige Darknet-Marktplatz den ich besucht habe war der Genesis Market. Neben Protonmail, das auch über das Surface Web erreichbar ist, kann ich mich leider an keine sonstigen, eindeutigen Seiten mehr erinnern.

ANHANG B - 2. Anhang

Protokoll – praktische Untersuchung von Darknet-Seiten

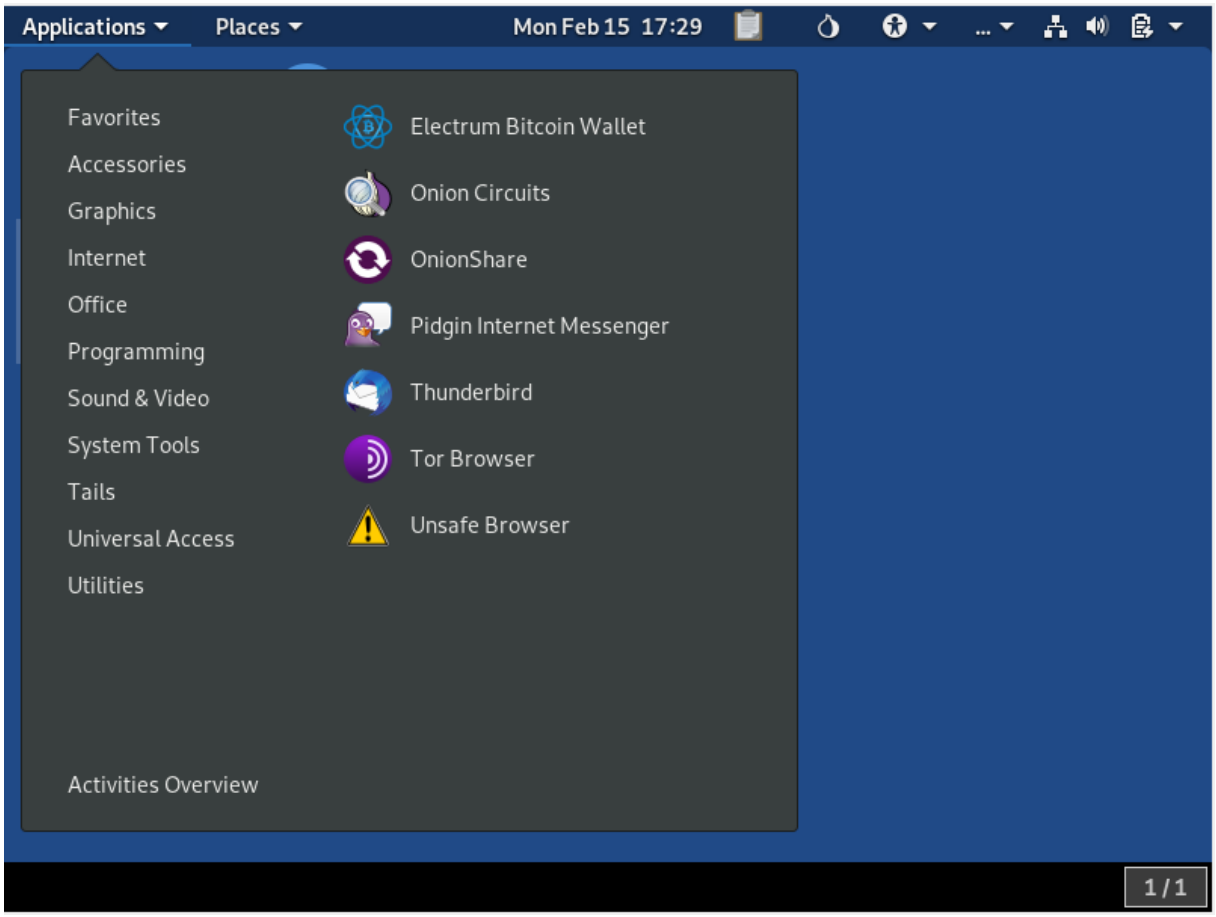
Allgemeine Analyse:

VM wurde gestartet.

Tails wurde geladen und das System hochgefahren.

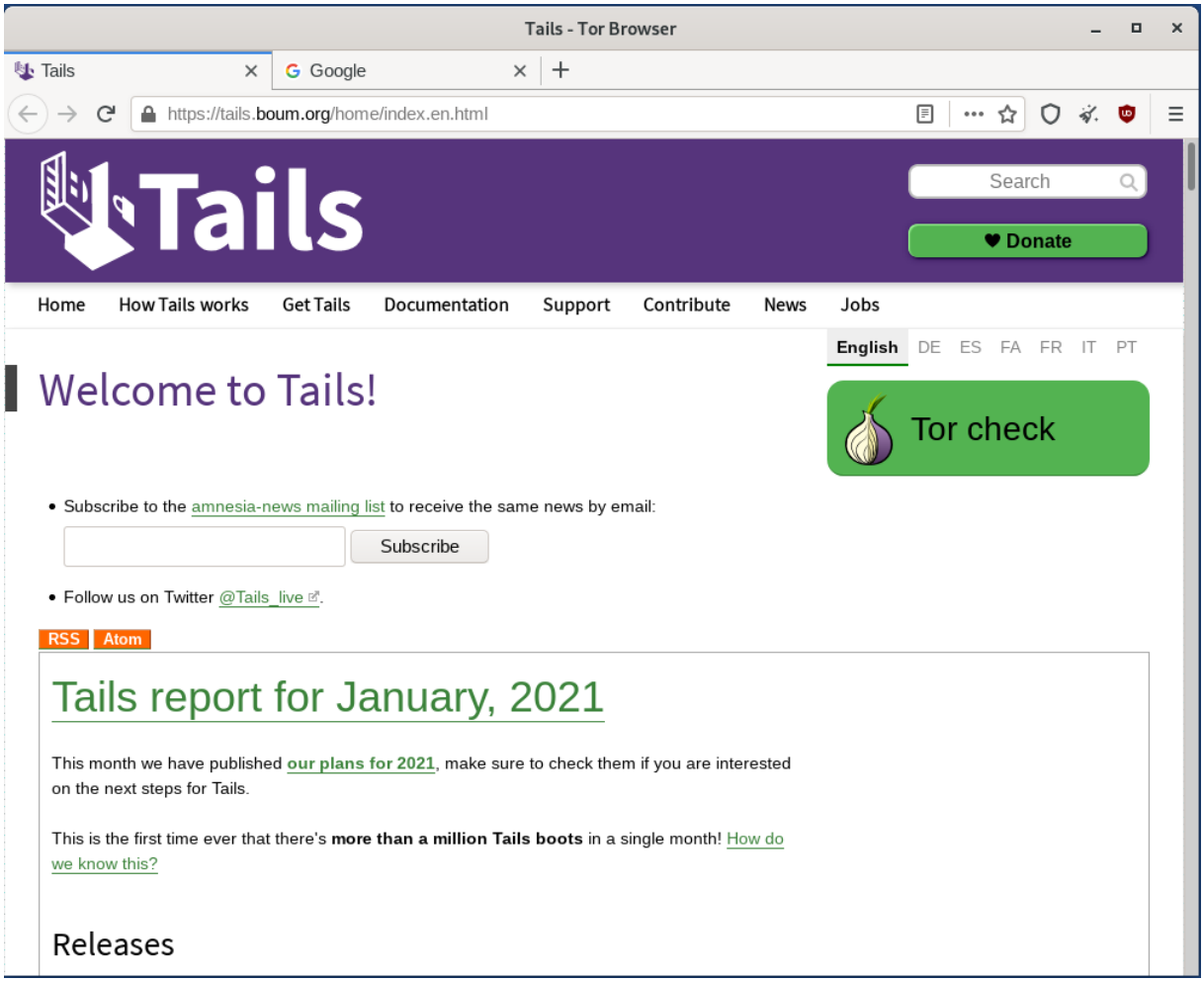
Suche im Menü nach einem bereits vorinstallierten Browser

Auswahl zwischen „Tor Browser“ und „Unsafe Browser“



Unsafe Browser klingt stark beunruhigend also wählen wir lieber den Tor Browser.

Erste Bemerkung: Computer, auf welchem Hardware läuft, ist viel langsamer. Performance leidet darunter, dass Tails direkt auf den Arbeitsspeicher zugreift und über diesen läuft.

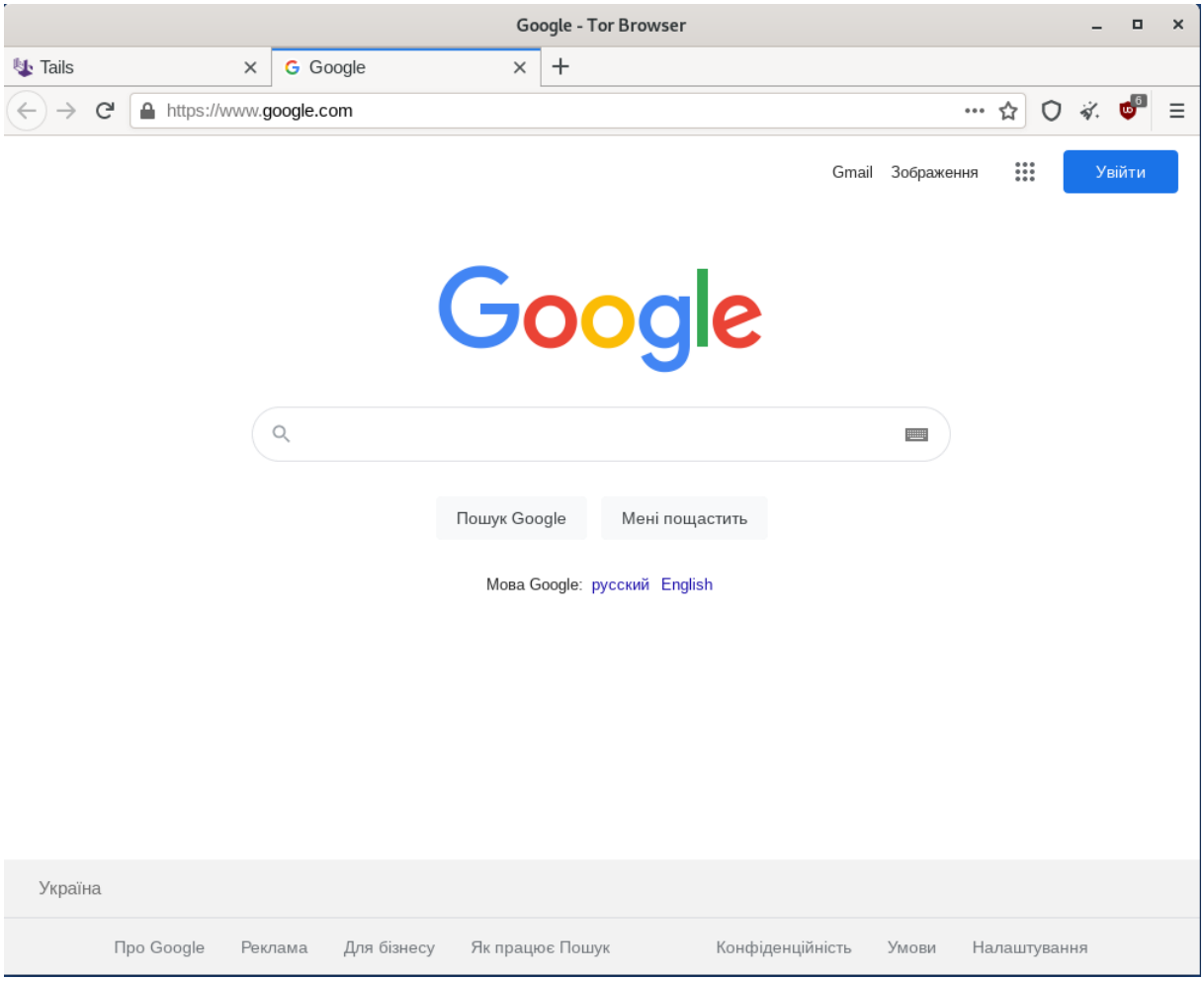


Startseite: Homepage Tails

Aufrufen von Google.com

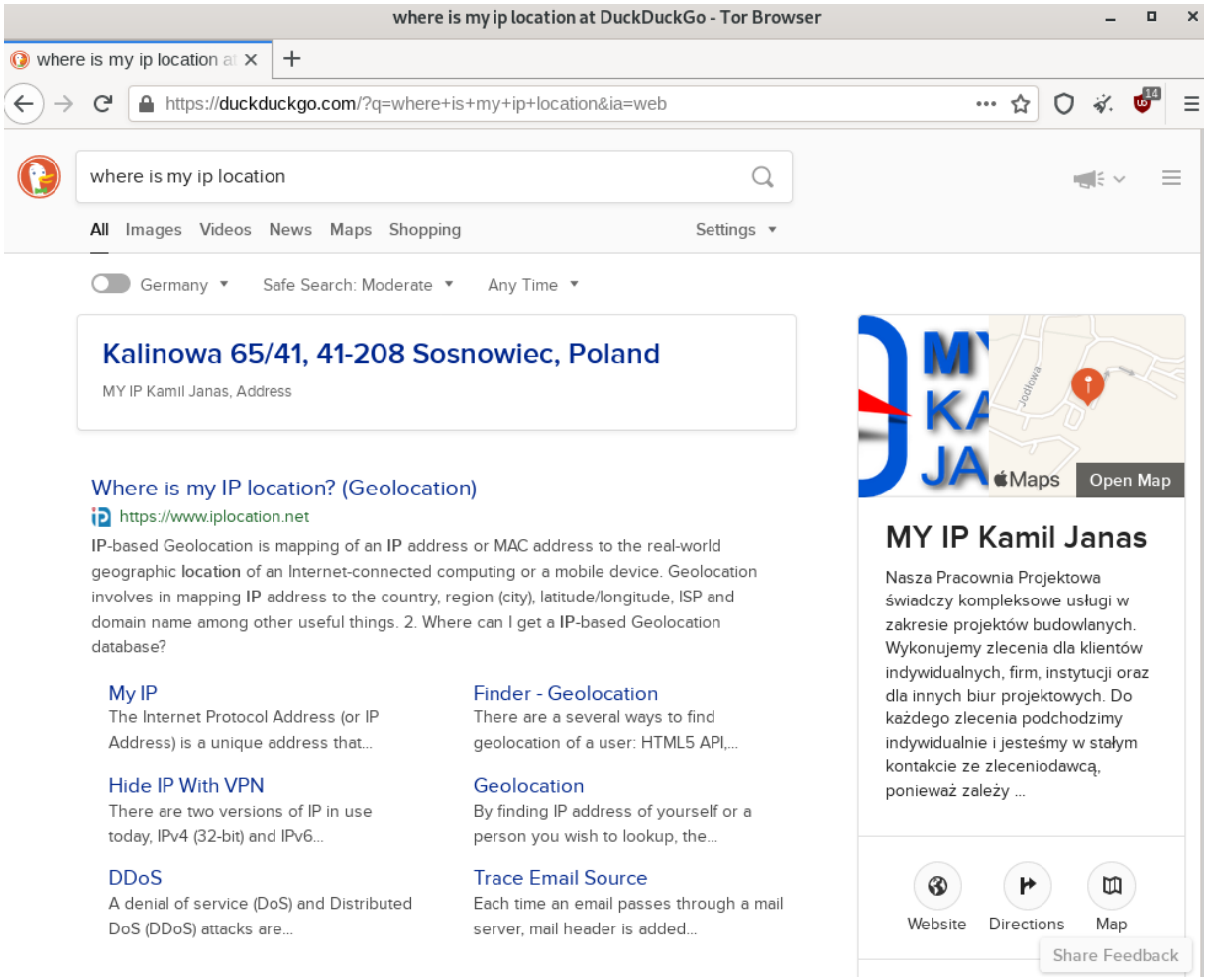
Erwartung: nicht möglich, nicht erwünscht, nicht aufrufbar

Realität: normal aufrufbar, googeln ist möglich

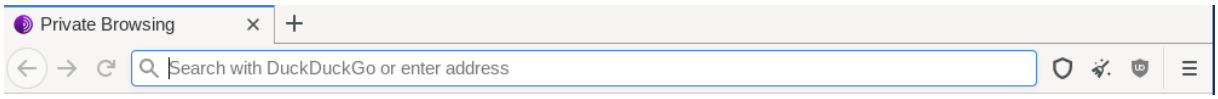


Bemerkung: Computer erhitzt sehr schnell, Lüfter ist stark aktiv

Bei Eingabe und Bestätigung der Suchanfrage wird automatisch über Default Search Engine „Duckduckgo“ gesucht:

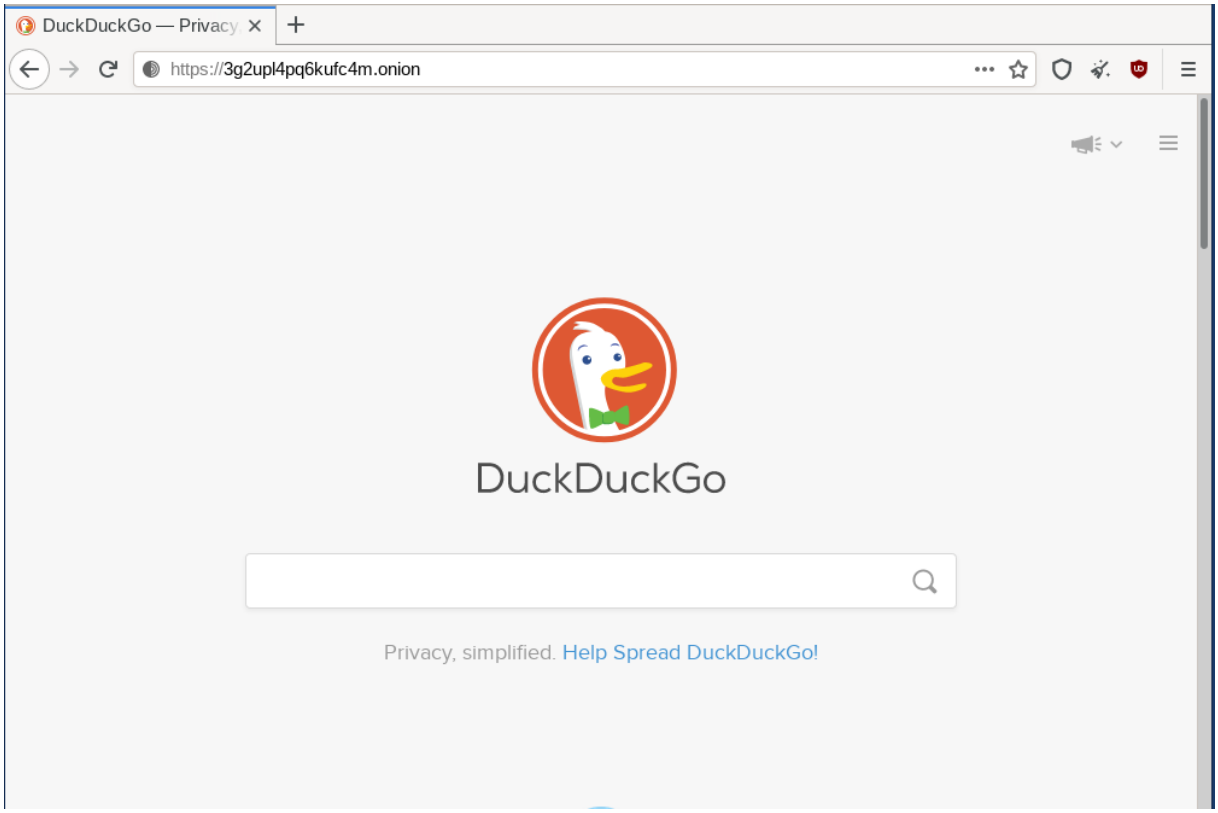


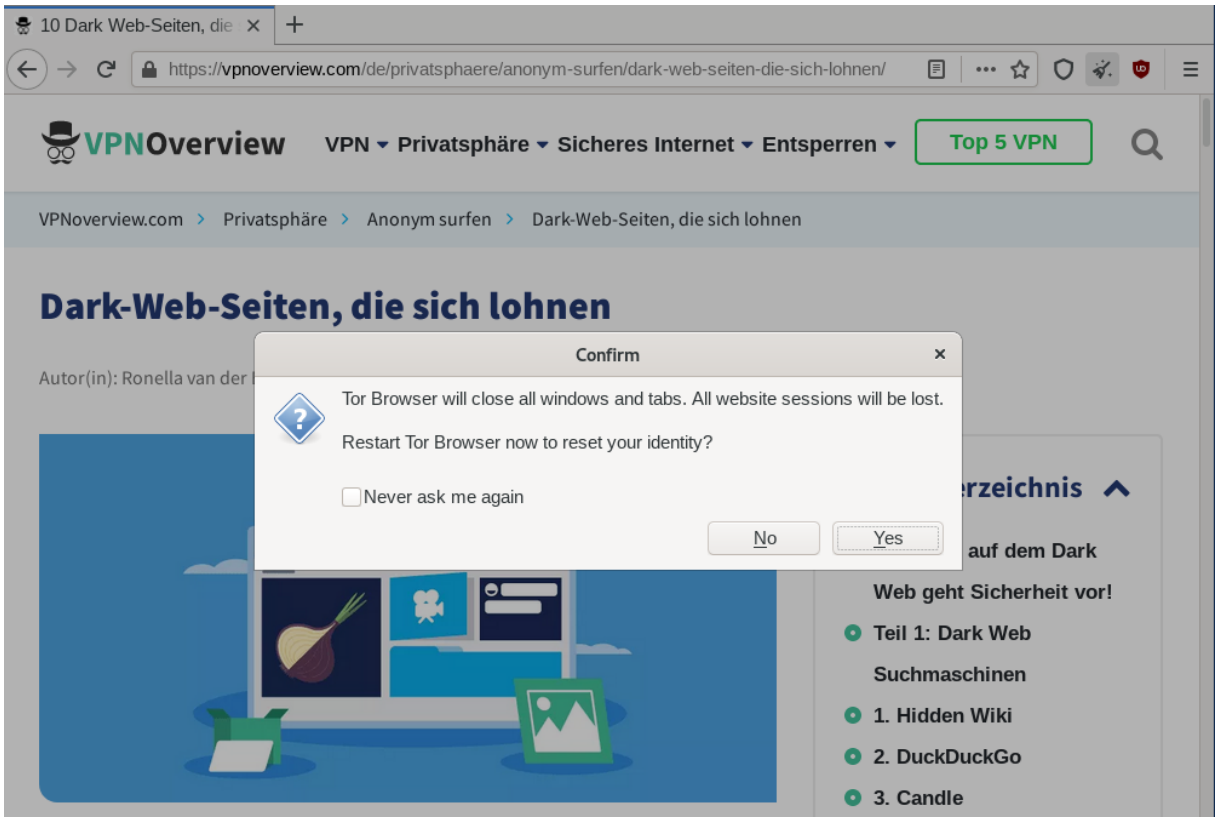
Verschleierung der IP-Adresse funktioniert einwandfrei.

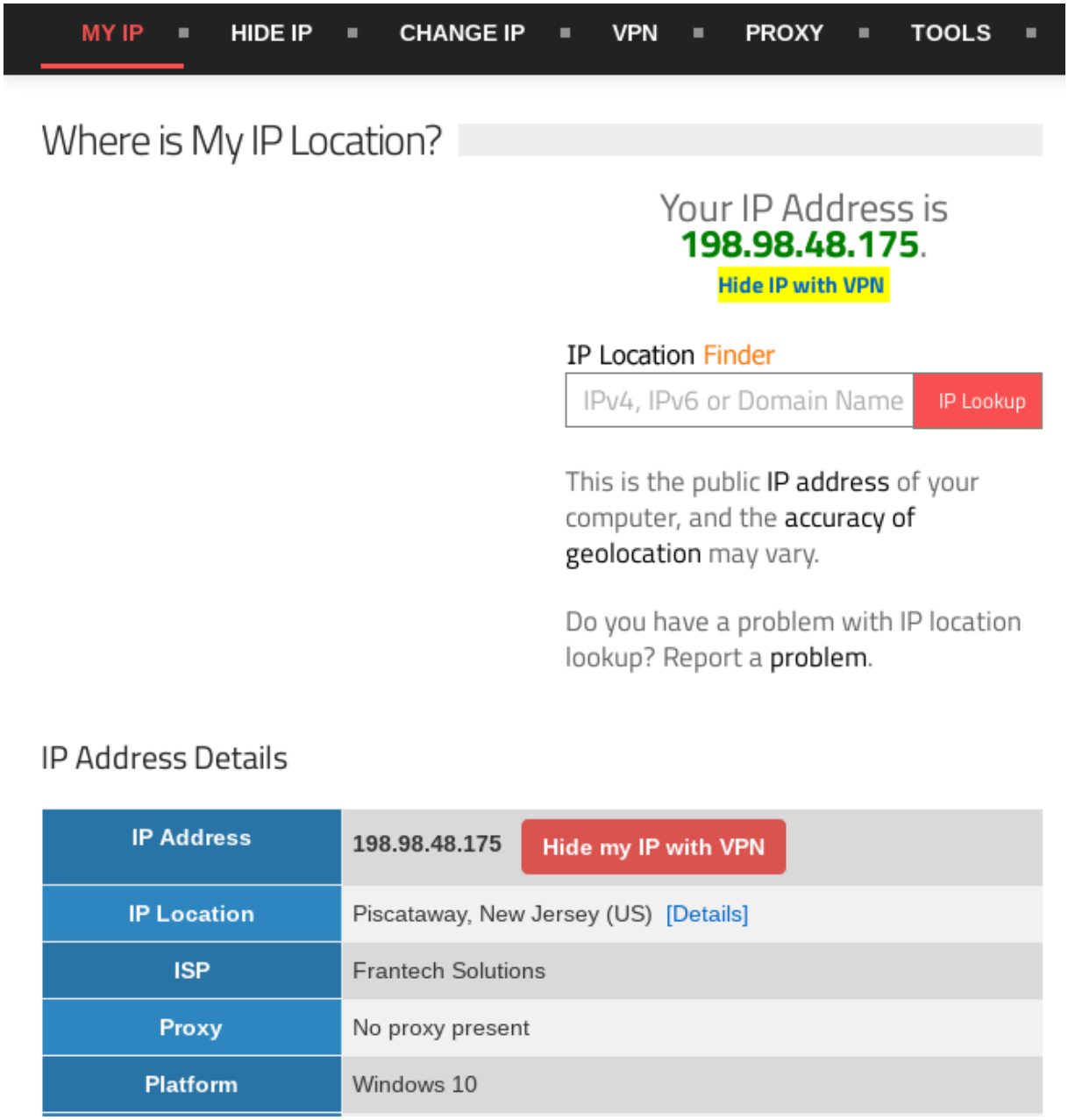


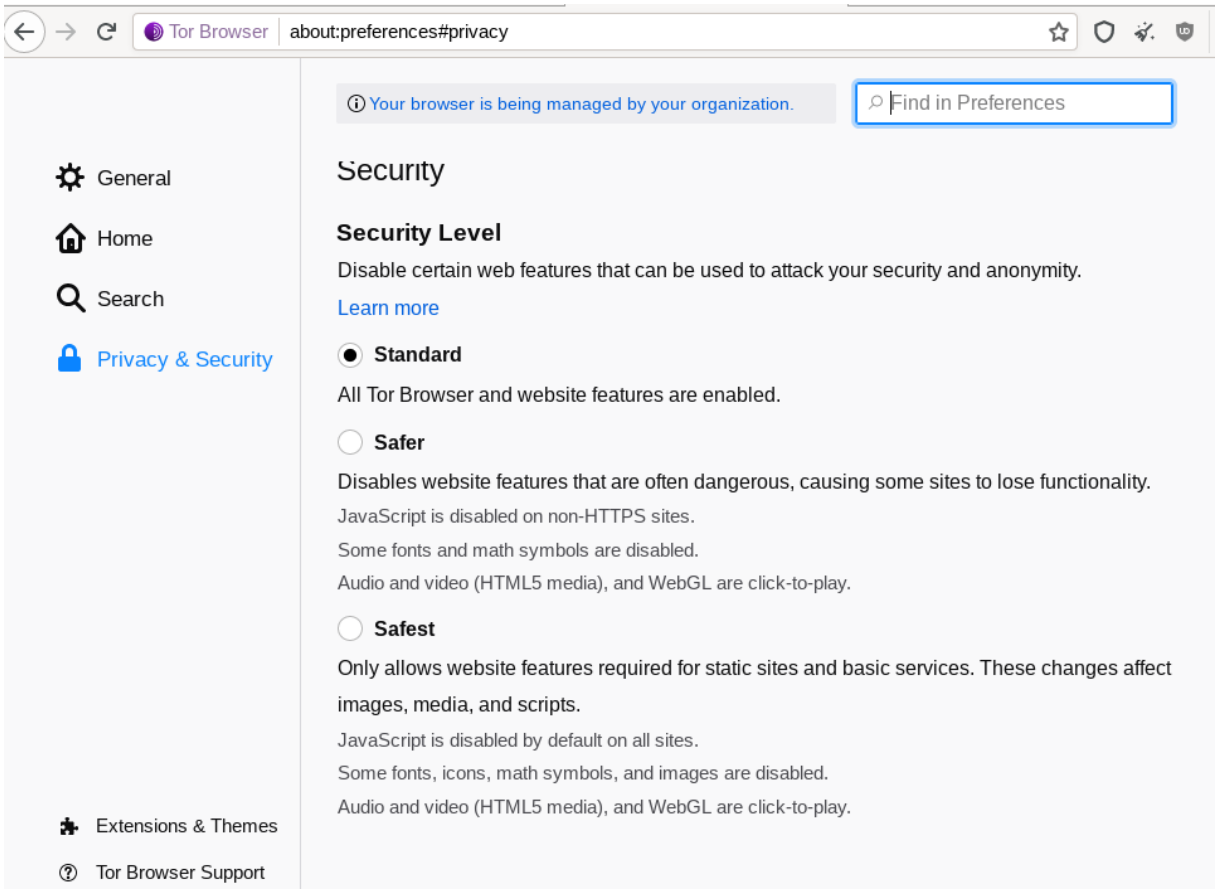
Sehr lange Ladezeiten, einfach Suchanfrage benötigt um die 12 Minuten

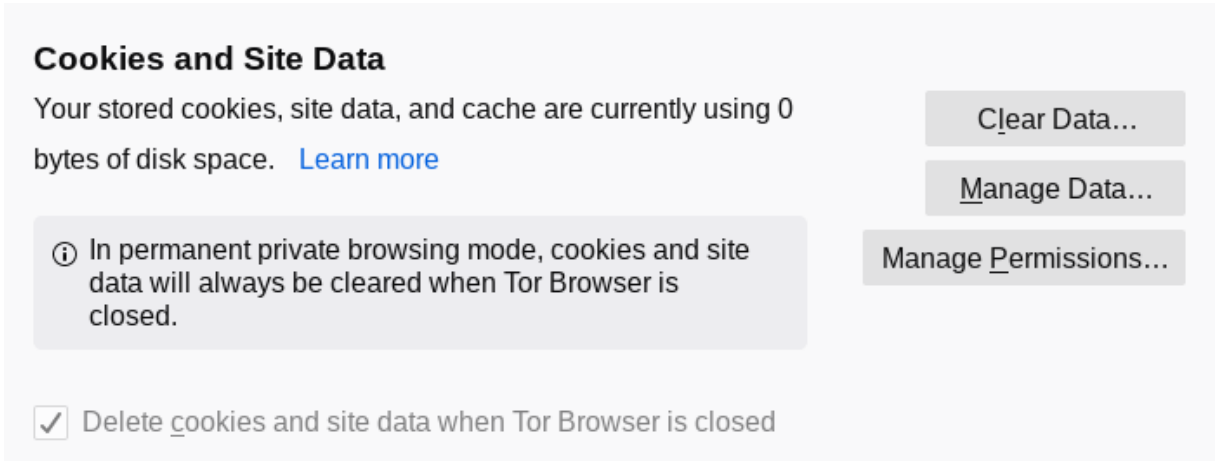
DuckDuckGo im Darknet und erster Onion-Besuch:

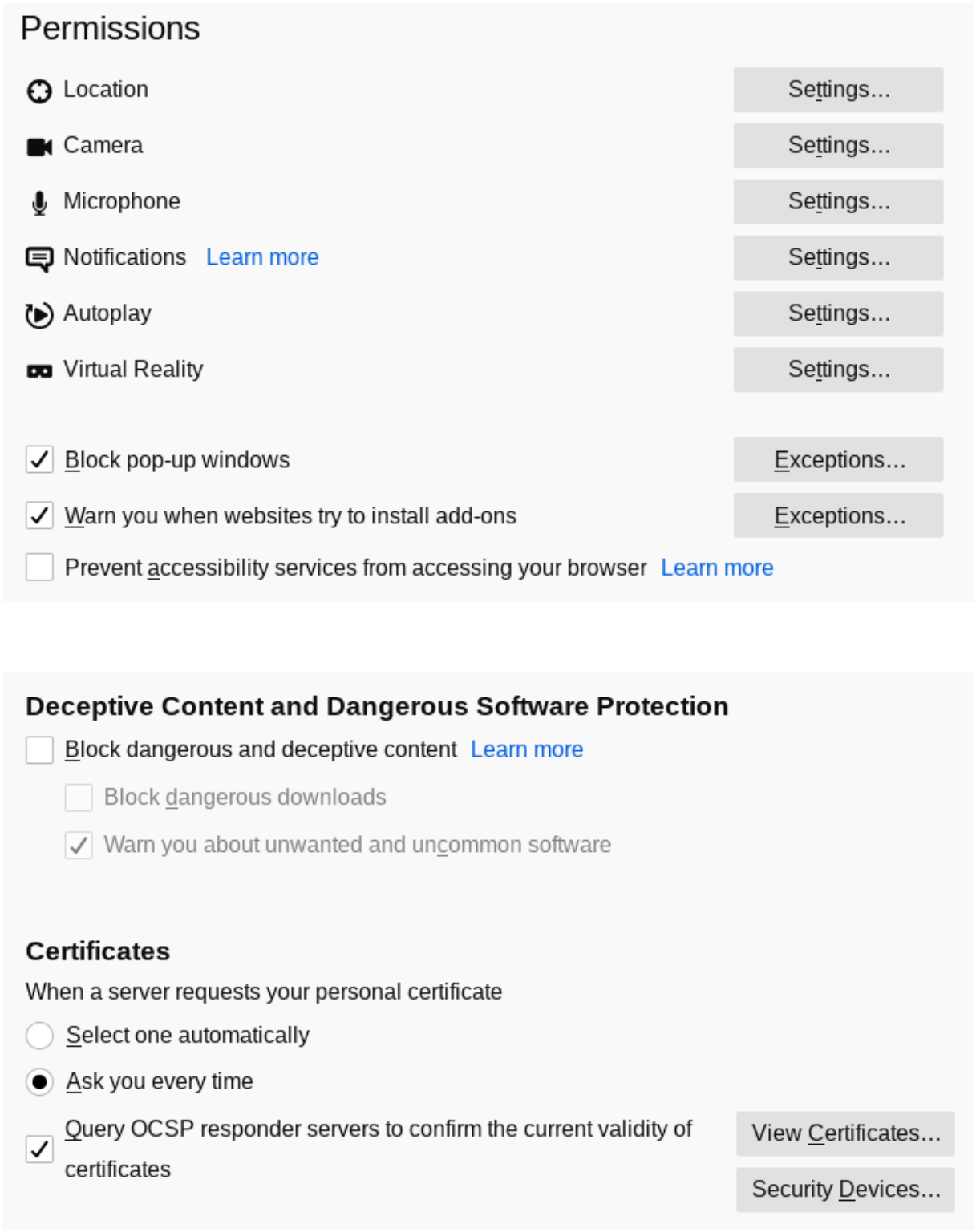

DuckDuckGo — Privacy
https://3g2upl4pq6kufc4m.onion
DuckDuckGo
Privacy, simplified. Help Spread DuckDuckGo!


10 Dark Web-Seiten, die
https://vpnoverview.com/de/privatsphaere/anonym-surfen/dark-web-seiten-die-sich-lohnen/
VPNOverview
VPN
Privatsphäre
Sicheres Internet
Entsperren
Top 5 VPN
VPNoverview.com
Privatsphäre
Anonym surfen
Dark-Web-Seiten, die sich lohnen
Dark-Web-Seiten, die sich lohnen
Autor(in): Ronella van der
Confirm
Tor Browser will close all windows and tabs. All website sessions will be lost.
Restart Tor Browser now to reset your identity?
Never ask me again
No
Yes
erzeichnis
auf dem Dark
Web geht Sicherheit vor!
Teil 1: Dark Web
Suchmaschinen
1. Hidden Wiki
2. DuckDuckGo
3. Candle

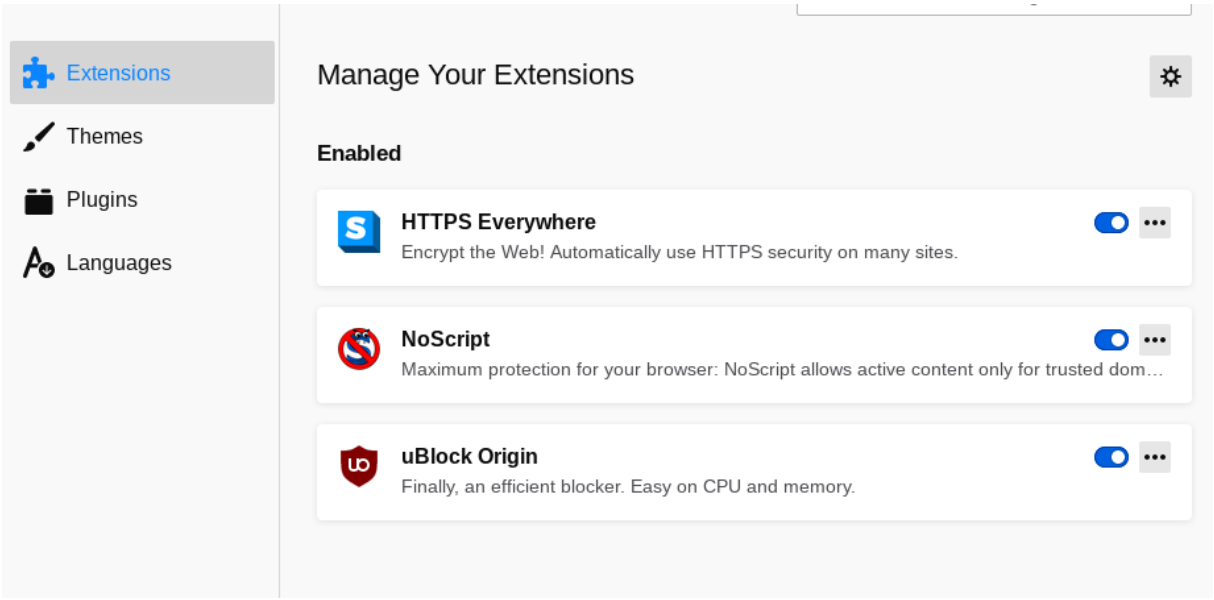

MY IP
HIDE IP
CHANGE IP
VPN
PROXY
TOOLS
Where is My IP Location?
Your IP Address is
198.98.48.175.
Hide IP with VPN
IP Location Finder
IPv4, IPv6 or Domain Name
IP Lookup
This is the public IP address of your computer, and the accuracy of geolocation may vary.
Do you have a problem with IP location lookup? Report a problem.
IP Address Details
IP Address
198.98.48.175
Hide my IP with VPN
IP Location
Piscataway, New Jersey (US) [Details]
ISP
Frantech Solutions
Proxy
No proxy present
Platform
Windows 10


Tor Browser
about:preferences#privacy
Your browser is being managed by your organization.
Find in Preferences
General
Home
Search
Privacy & Security
Extensions & Themes
Tor Browser Support
Security
Security Level
Disable certain web features that can be used to attack your security and anonymity.
Learn more
Standard
All Tor Browser and website features are enabled.
Safer
Disables website features that are often dangerous, causing some sites to lose functionality.
JavaScript is disabled on non-HTTPS sites.
Some fonts and math symbols are disabled.
Audio and video (HTML5 media), and WebGL are click-to-play.
Safest
Only allows website features required for static sites and basic services. These changes affect images, media, and scripts.
JavaScript is disabled by default on all sites.
Some fonts, icons, math symbols, and images are disabled.
Audio and video (HTML5 media), and WebGL are click-to-play.

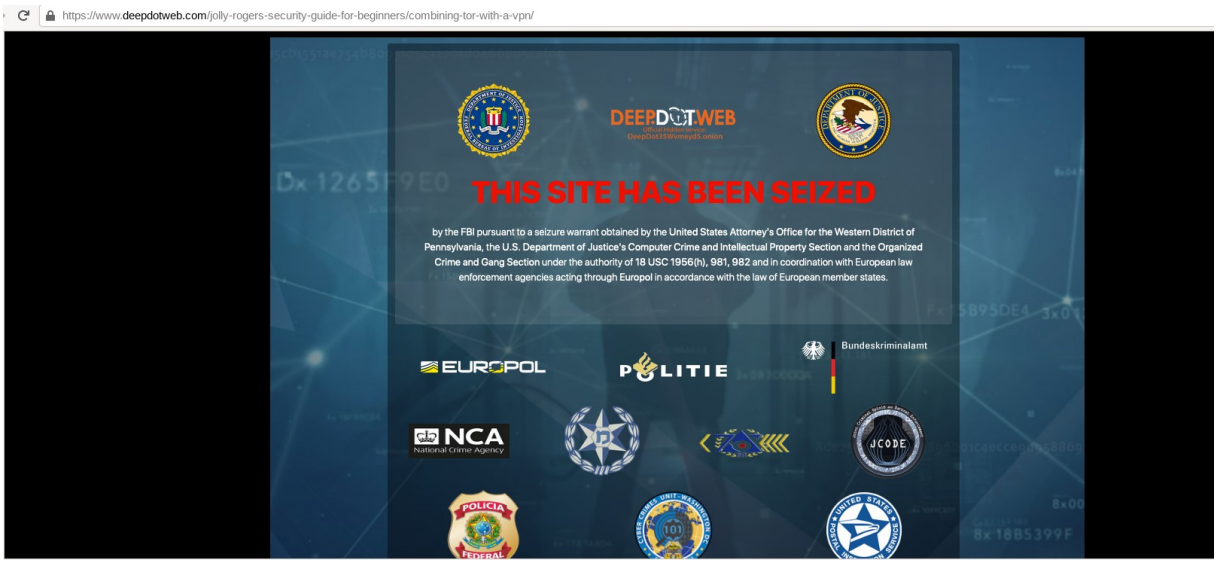

Cookies and Site Data
Your stored cookies, site data, and cache are currently using 0 bytes of disk space. Learn more
Clear Data…
Manage Data…
Manage Permissions…
In permanent private browsing mode, cookies and site data will always be cleared when Tor Browser is closed.
Delete cookies and site data when Tor Browser is closed

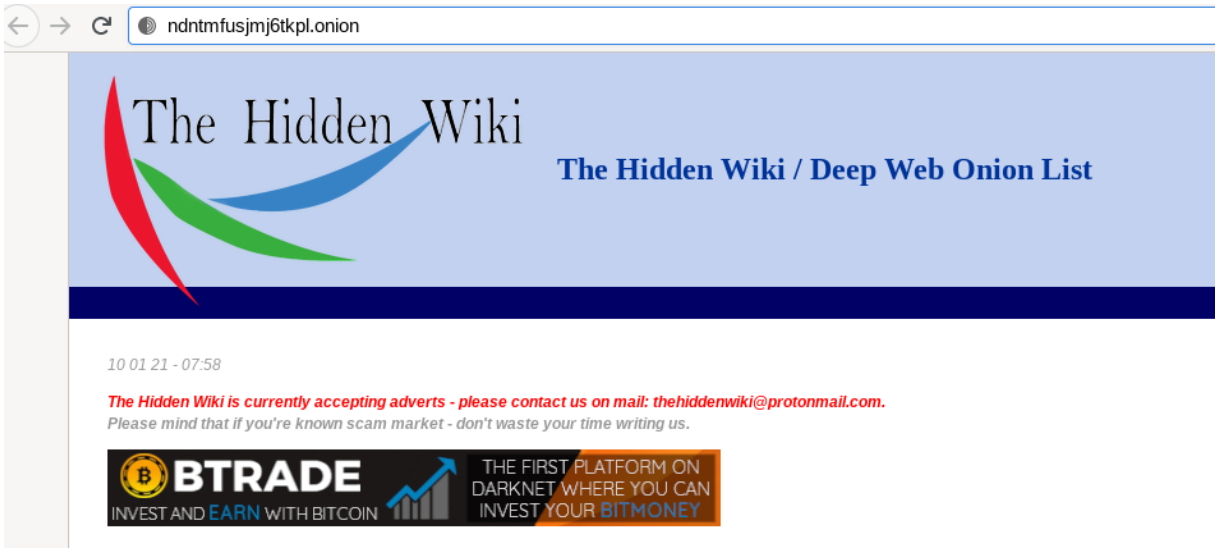

Permissions
Location
Settings...
Camera
Settings...
Microphone
Settings...
Notifications
Learn more
Settings...
Autoplay
Settings...
Virtual Reality
Settings...
Block pop-up windows
Exceptions...
Warn you when websites try to install add-ons
Exceptions...
Prevent accessibility services from accessing your browser
Learn more
Deceptive Content and Dangerous Software Protection
Block dangerous and deceptive content
Learn more
Block dangerous downloads
Warn you about unwanted and uncommon software
Certificates
When a server requests your personal certificate
Select one automatically
Ask you every time
Query OCSP responder servers to confirm the current validity of certificates
View Certificates...
Security Devices...

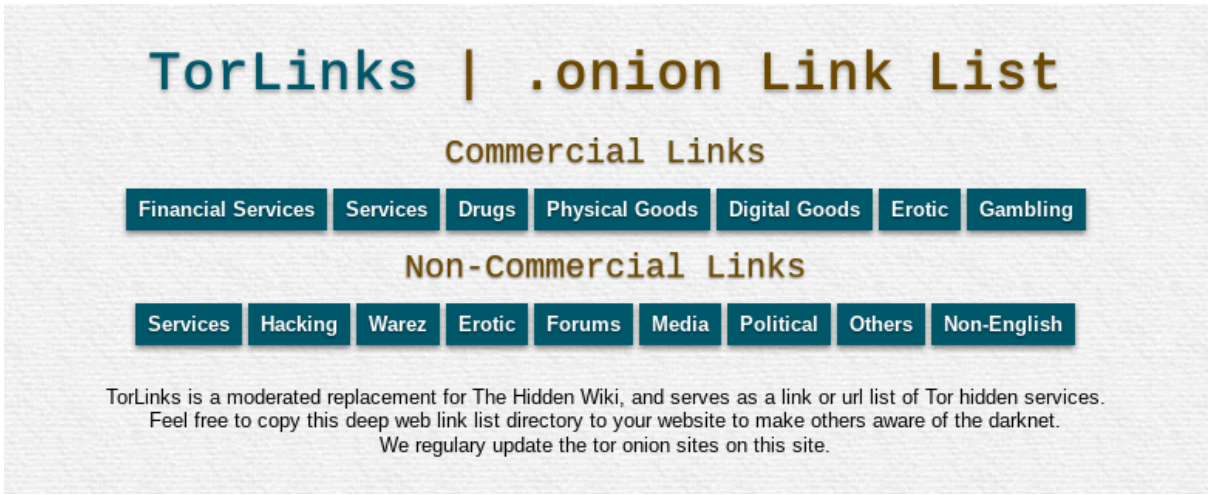
Add-Ons:

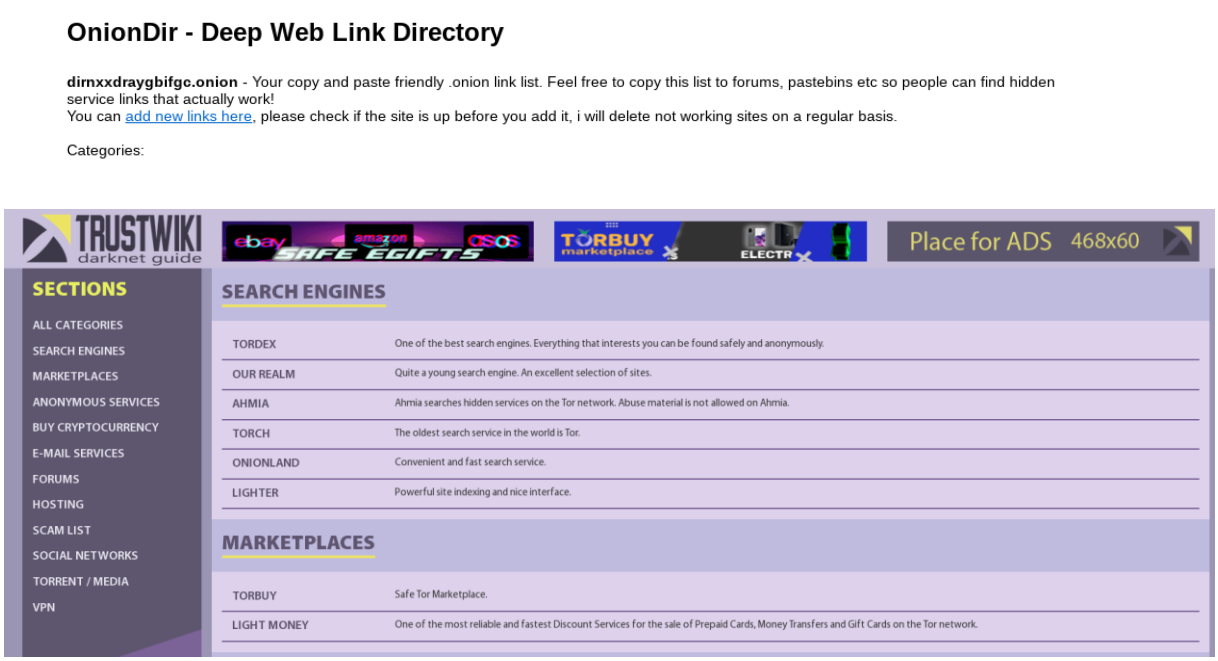

Extensions
Themes
Plugins
Languages
Manage Your Extensions
Enabled
HTTPS Everywhere
Encrypt the Web! Automatically use HTTPS security on many sites.
NoScript
Maximum protection for your browser: NoScript allows active content only for trusted dom…
uBlock Origin
Finally, an efficient blocker. Easy on CPU and memory.


Congratulations. This browser is configured to use Tor.
Your IP address appears to be: 213.164.204.94


https://www.deepdotweb.com/jolly-rogers-security-guide-for-beginners/combining-tor-with-a-vpn/
DEEPDOTWEB
THIS SITE HAS BEEN SEIZED
by the FBI pursuant to a seizure warrant obtained by the United States Attorney's Office for the Western District of Pennsylvania, the U.S. Department of Justice's Computer Crime and Intellectual Property Section and the Organized Crime and Gang Section under the authority of 18 USC 1956(h), 981, 982 and in coordination with European law enforcement agencies acting through Europol in accordance with the law of European member states.
EUROPOL
POLITIE
Bundeskriminalamt
NCA
National Crime Agency
JCODE

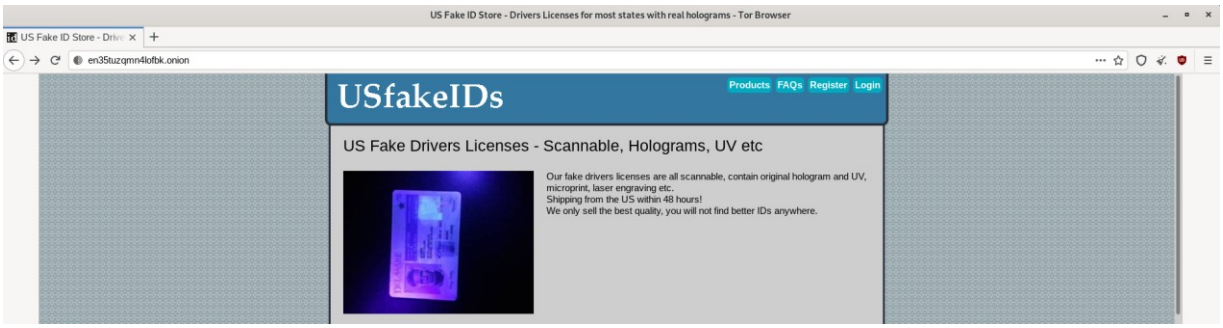






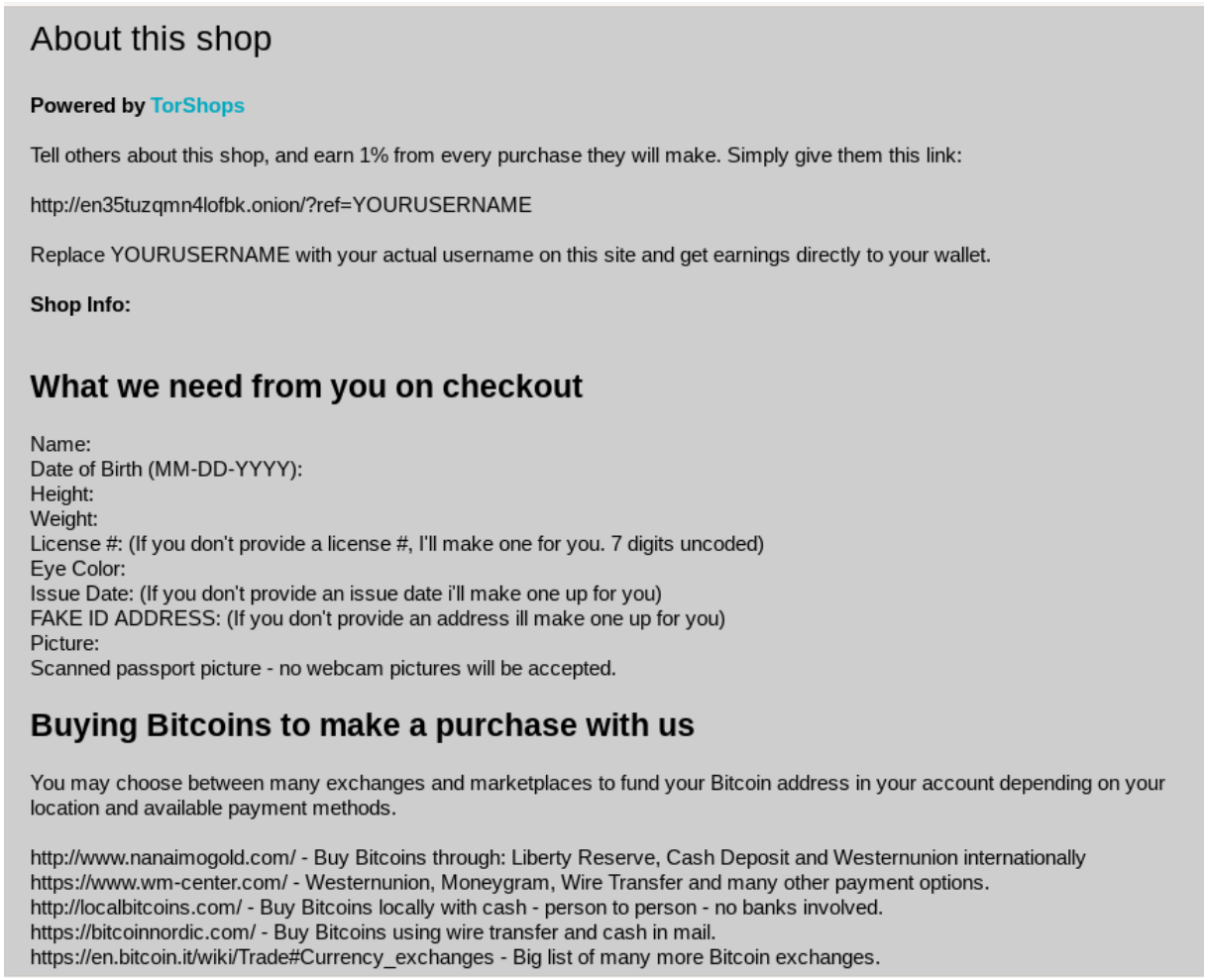
Mit der Zeit verschlechtert sich die Performance immer weiter. Programme auf der Host-Maschine sind gelabelt mit „Keine Rückmeldung“.

Sehr einfach aufgebaute Webseite:



Ware beschränkt auf US-IDs in amerikanischen Staaten:

Product	Price	Quantity
Delaware	200 USD = 0.00410 ฿	1 X Buy now
Illinois	200 USD = 0.00410 ฿	1 X Buy now
South Carolina	200 USD = 0.00410 ฿	1 X Buy now
New Jersey	200 USD = 0.00410 ฿	1 X Buy now
Colorado	200 USD = 0.00410 ฿	1 X Buy now
Pennsylvania	200 USD = 0.00410 ฿	1 X Buy now
Montana	200 USD = 0.00410 ฿	1 X Buy now
Indiana	200 USD = 0.00410 ฿	1 X Buy now
Wisconsin	200 USD = 0.00410 ฿	1 X Buy now
Alaska	200 USD = 0.00410 ฿	1 X Buy now
Tennessee	200 USD = 0.00410 ฿	1 X Buy now
Arizona	200 USD = 0.00410 ฿	1 X Buy now
New York	200 USD = 0.00410 ฿	1 X Buy now



About this shop

Powered by TorShops

Tell others about this shop, and earn 1% from every purchase they will make. Simply give them this link:

http://en35tuzqmn4lofbk.onion/?ref=YOURUSERNAME

Replace YOURUSERNAME with your actual username on this site and get earnings directly to your wallet.

Shop Info:

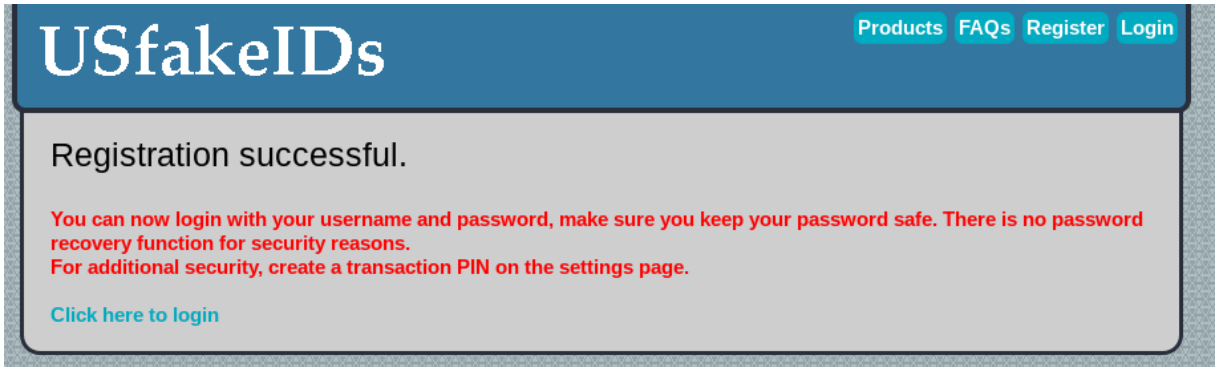
What we need from you on checkout

Name:
Date of Birth (MM-DD-YYYY):
Height:
Weight:
License #: (If you don't provide a license #, I'll make one for you. 7 digits uncoded)
Eye Color:
Issue Date: (If you don't provide an issue date i'll make one up for you)
FAKE ID ADDRESS: (If you don't provide an address ill make one up for you)
Picture:
Scanned passport picture - no webcam pictures will be accepted.

Buying Bitcoins to make a purchase with us

You may choose between many exchanges and marketplaces to fund your Bitcoin address in your account depending on your location and available payment methods.

http://www.nanaimogold.com/ - Buy Bitcoins through: Liberty Reserve, Cash Deposit and Westernunion internationally
https://www.wm-center.com/ - Westernunion, Moneygram, Wire Transfer and many other payment options.
http://localbitcoins.com/ - Buy Bitcoins locally with cash - person to person - no banks involved.
https://bitcoinnordic.com/ - Buy Bitcoins using wire transfer and cash in mail.
https://en.bitcoin.it/wiki/Trade#Currency_exchanges - Big list of many more Bitcoin exchanges.



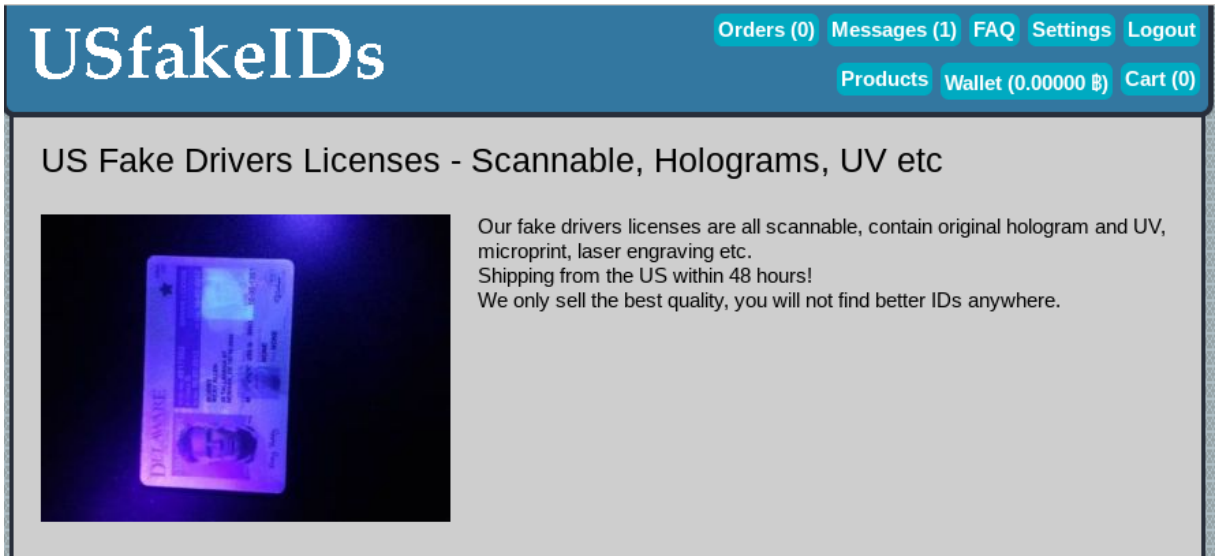
USfakeIDs

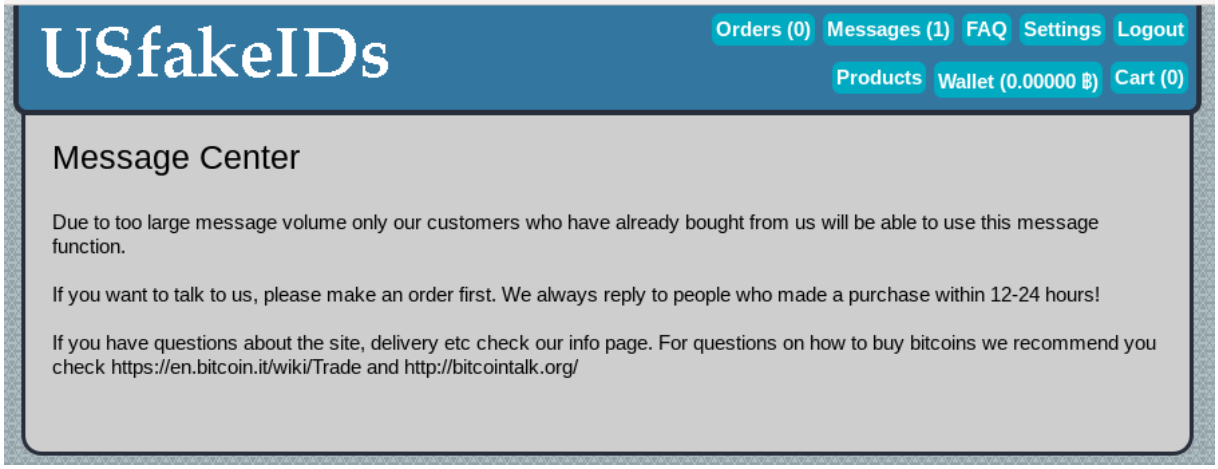
Products FAQs Register Login

Registration successful.

You can now login with your username and password, make sure you keep your password safe. There is no password recovery function for security reasons.
For additional security, create a transaction PIN on the settings page.

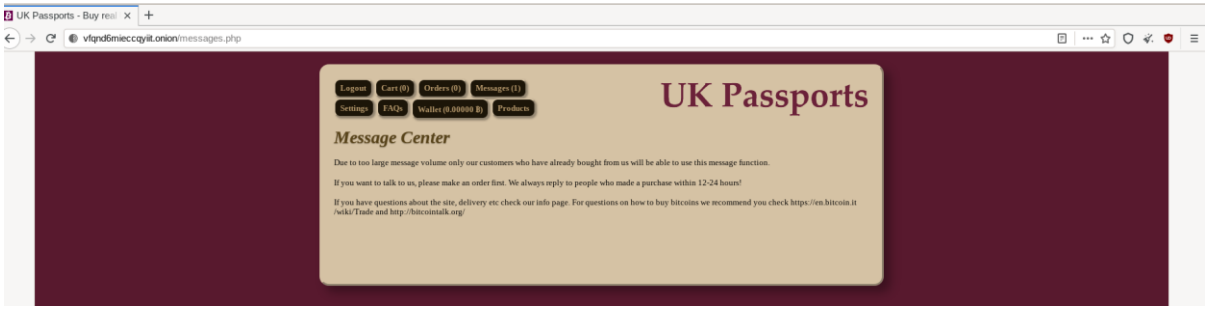
Click here to login



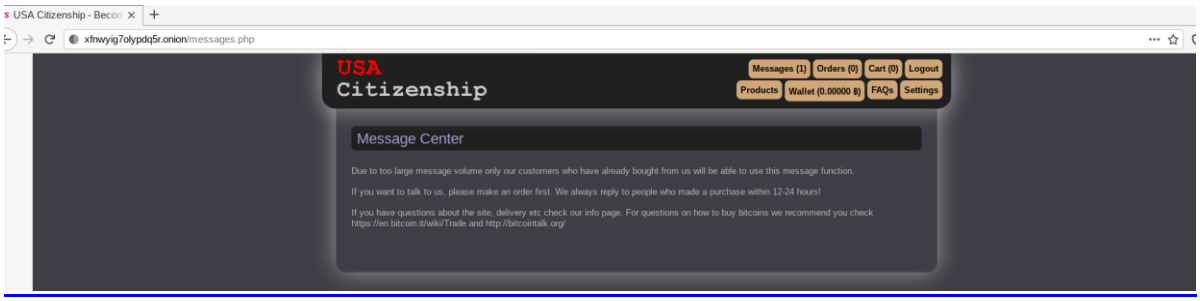


Registrierung als Grundvoraussetzung bei jedem Shop.

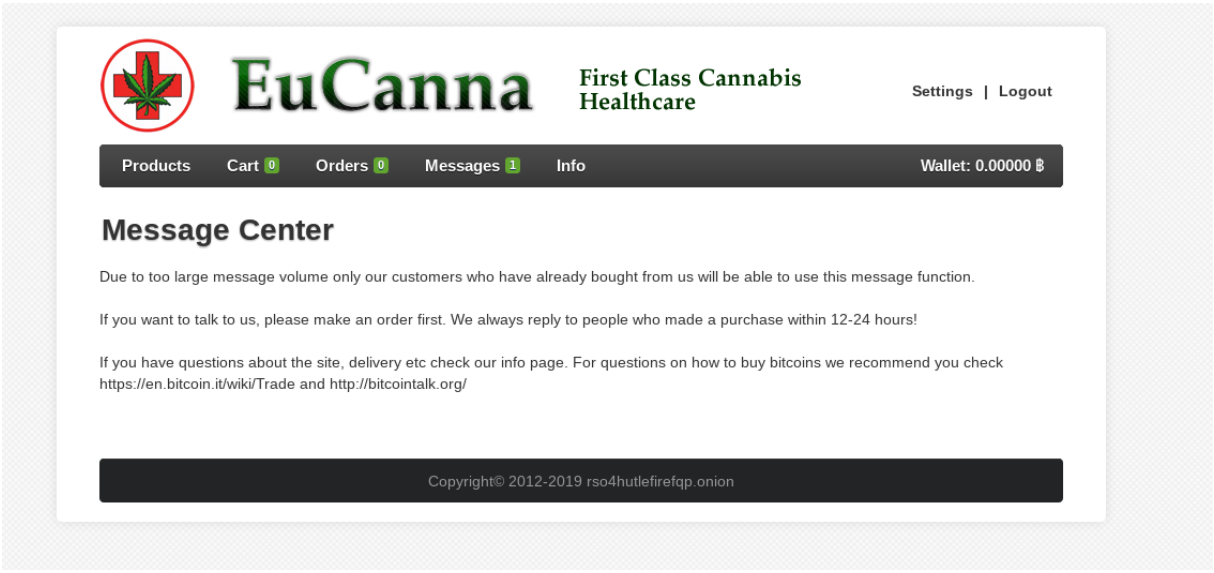
http://vfqnd6mieccqyiit.onion/ (3 Hits)



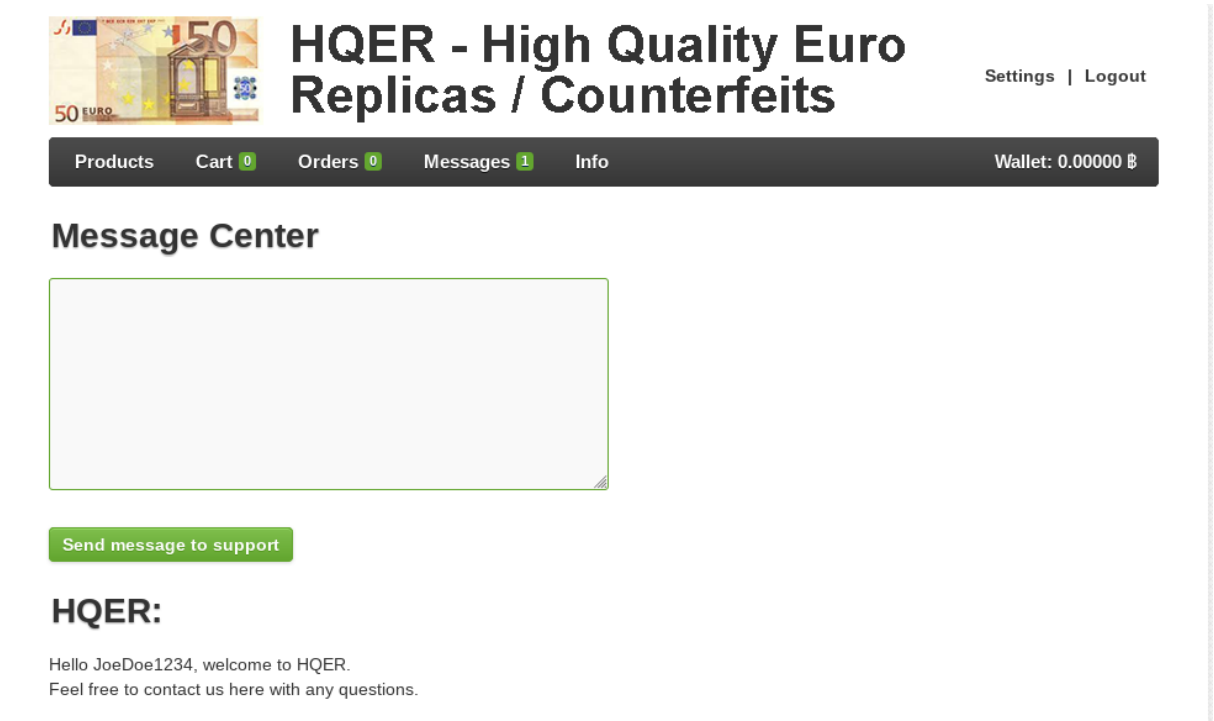
http://xfnwyig7olypdq5r.onion/ (3 Hits)



http://rso4hutlefirefqp.onion/messages.php (3 Hits)



http://y3fpieiezy2sin4a.onion/messages.php (3 Hits)



HQER - High Quality Euro Replicas / Counterfeits

Settings | Logout

Products | Cart 0 | Orders 0 | Messages 1 | Info | Wallet: 0.00000 ฿

Message Center

Hey!
what should I look out for when paying with the replicas? How high is the risk of getting discovered?
Thx!

Send message to support

HQER:

Hello JoeDoe1234, welcome to HQER.
Feel free to contact us here with any questions.

Message Center

Send message to support

JoeDoe1234:

Hey!
what should I look out for when paying with the replicas? How high is the risk of getting discovered?
Thx!

HQER:

Hello JoeDoe1234, welcome to HQER.
Feel free to contact us here with any questions.

Delete all messages

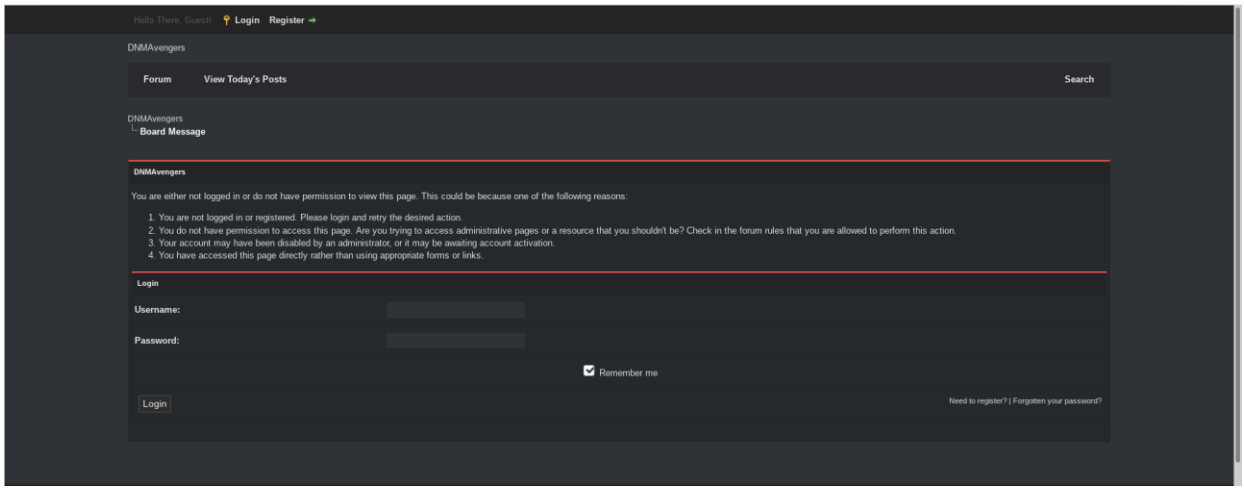
Check to confirm deletion

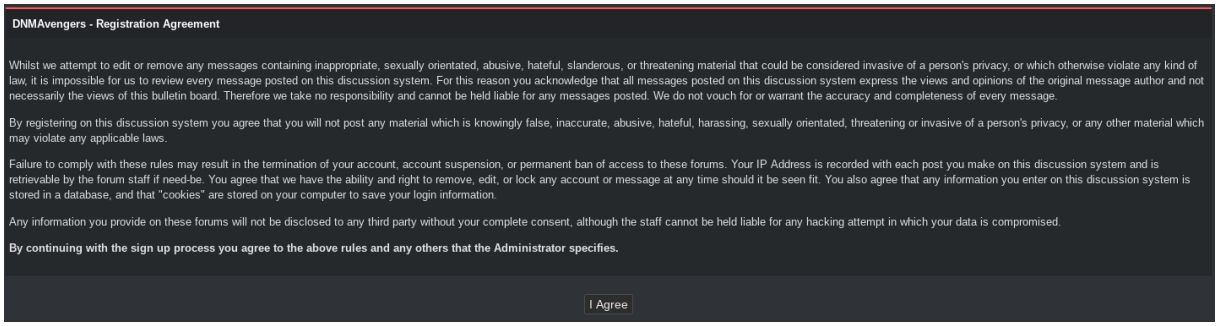
HQER

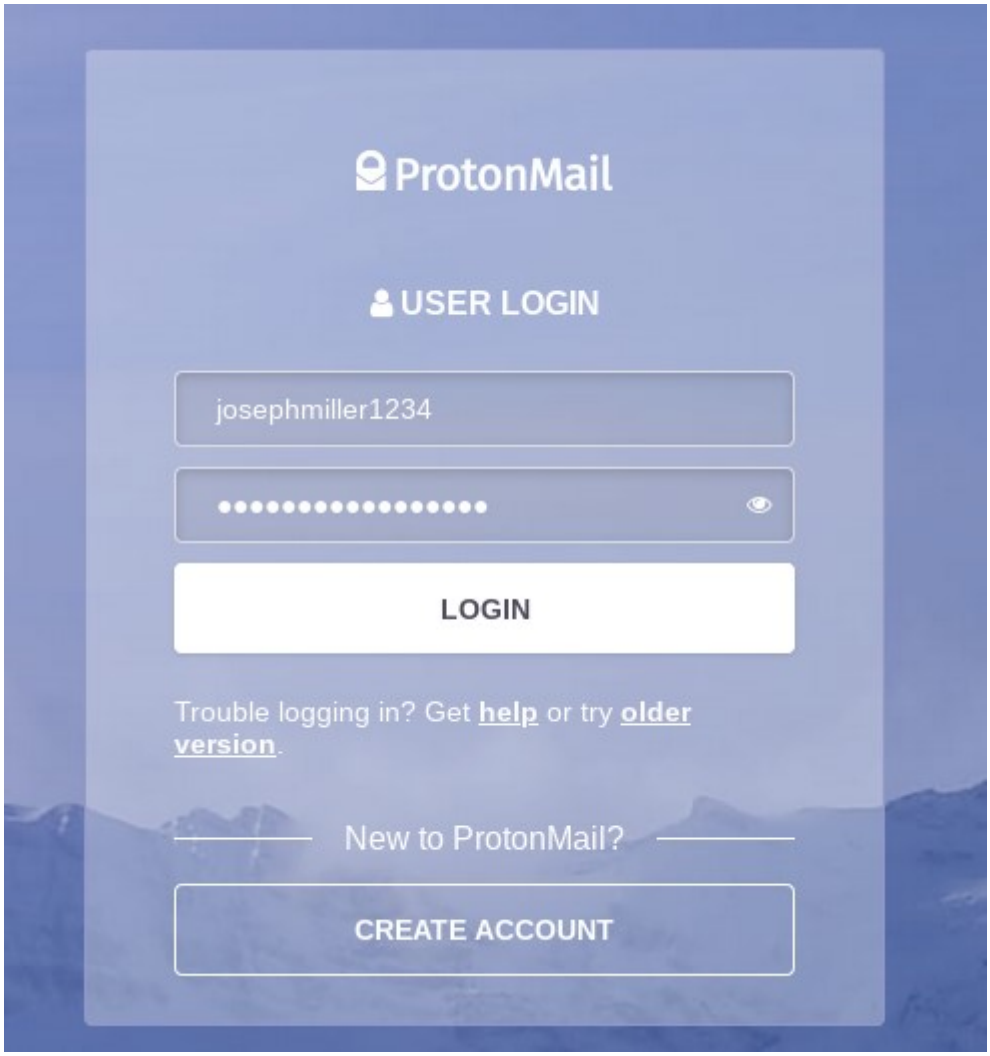
FORUM:

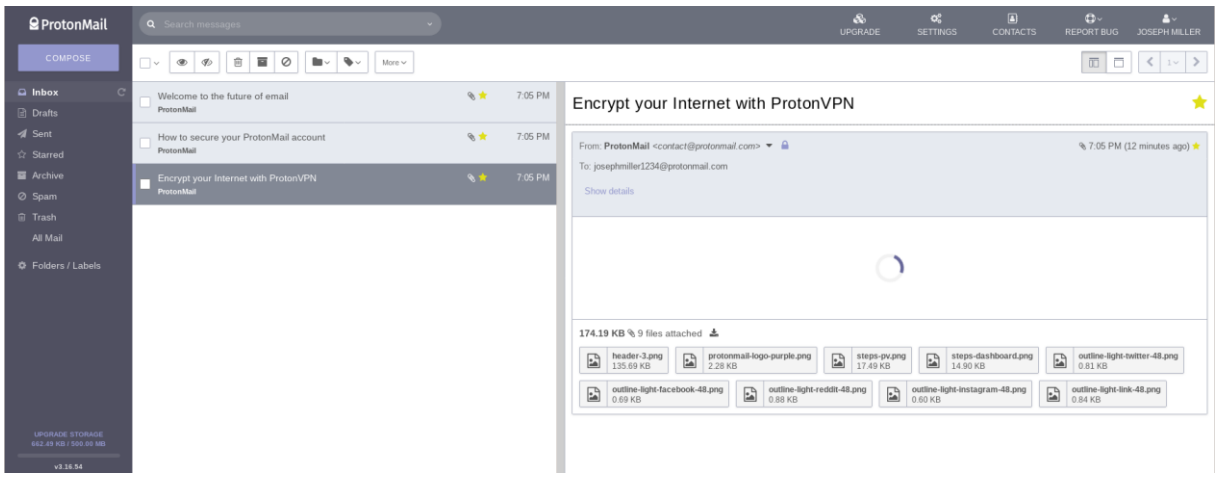
http://avengersdutyk3xf.onion/

http://avengerssbkfrkhlbpxmonvdvsyi3xesvzar2oxincbqx5rqoehpkwqd.onion/ (2 hints)

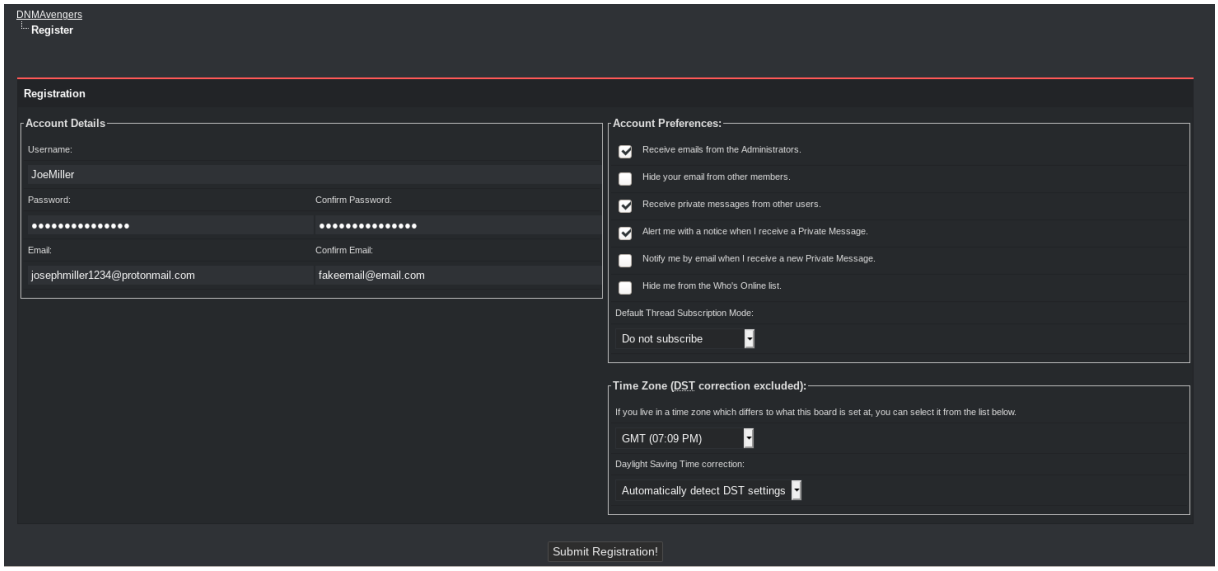


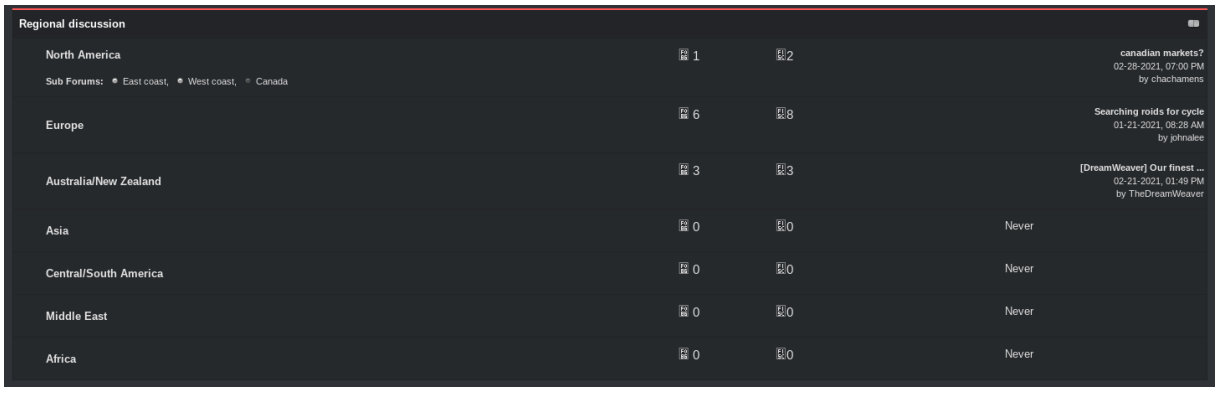



ProtonMail
USER LOGIN
josephmiller1234
LOGIN
Trouble logging in? Get help or try older version.
New to ProtonMail?
CREATE ACCOUNT

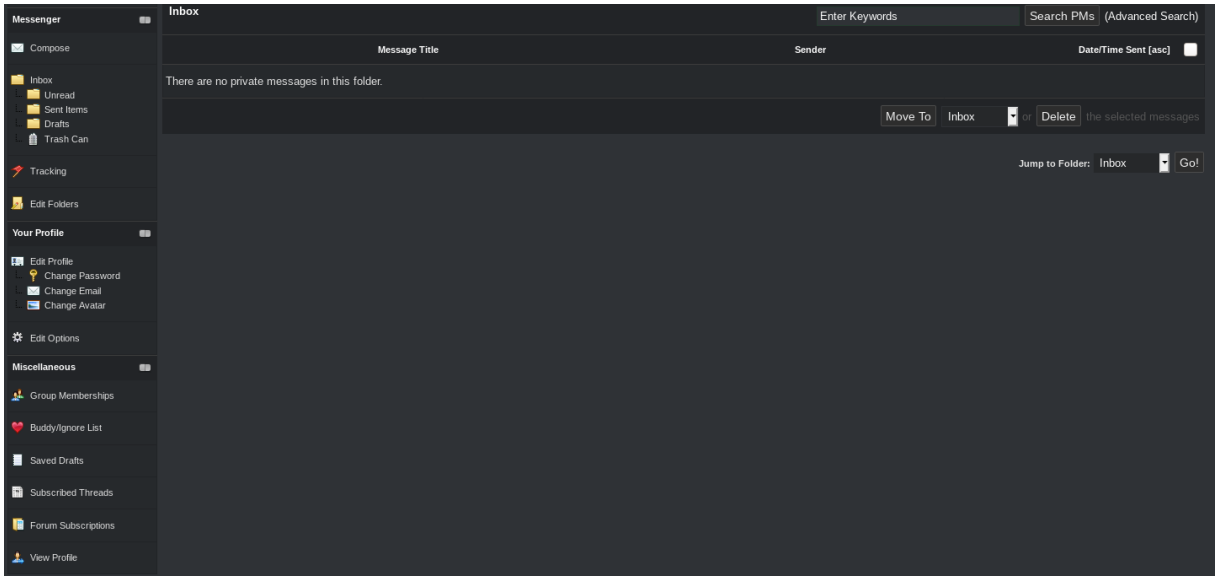

ProtonMail
Search messages
UPGRADE
SETTINGS
CONTACTS
REPORT BUG
JOSEPH MILLER
COMPOSE
Inbox
Drafts
Sent
Starred
Archive
Spam
Trash
All Mail
Folders / Labels
Welcome to the future of email
How to secure your ProtonMail account
Encrypt your Internet with ProtonVPN
Encrypt your Internet with ProtonVPN
From: ProtonMail
To: josephmiller1234@protonmail.com
Show details
174.19 KB 9 files attached

Forum-Boards:

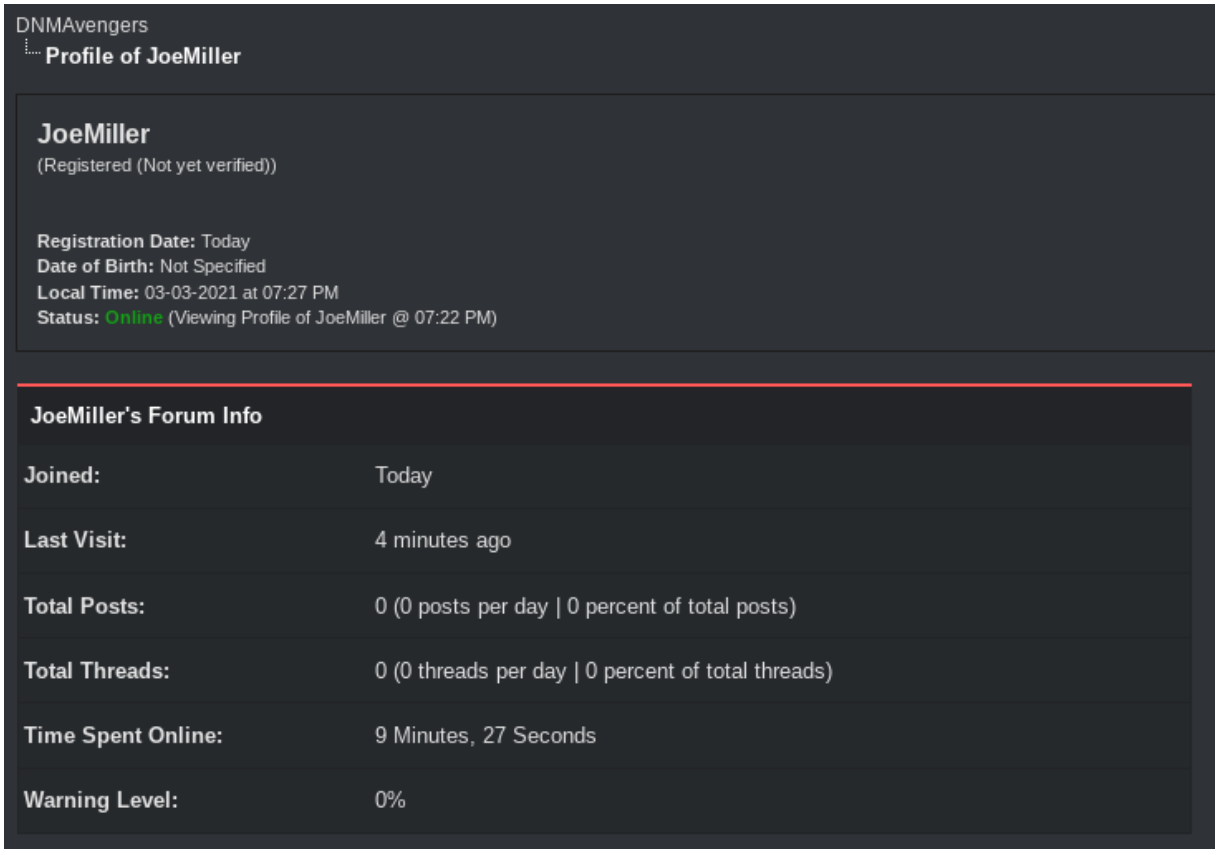


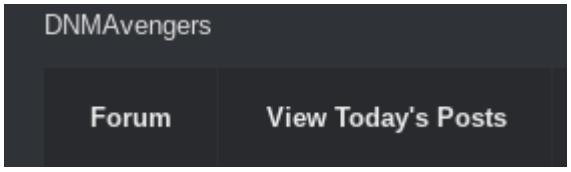


Forum – Private Messages:

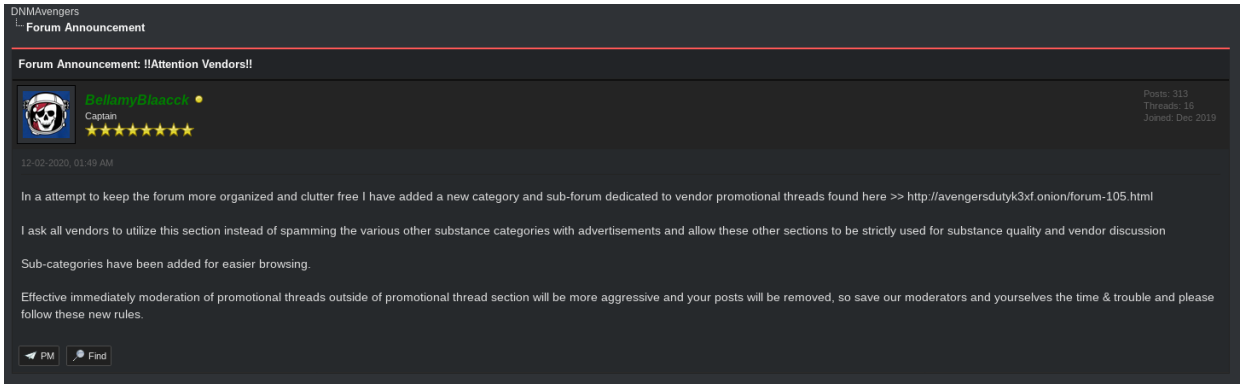


Forum Profile:





Zu viel Werbung in den Foren:



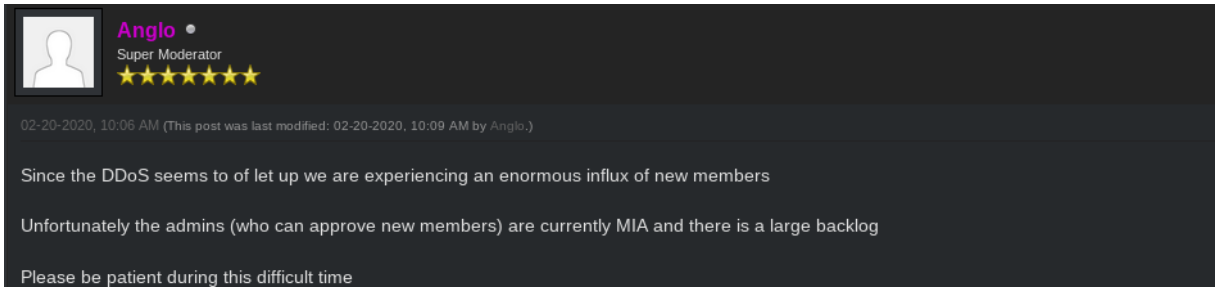
Foren werden von Verkäufern als Werbestelle verwendet.

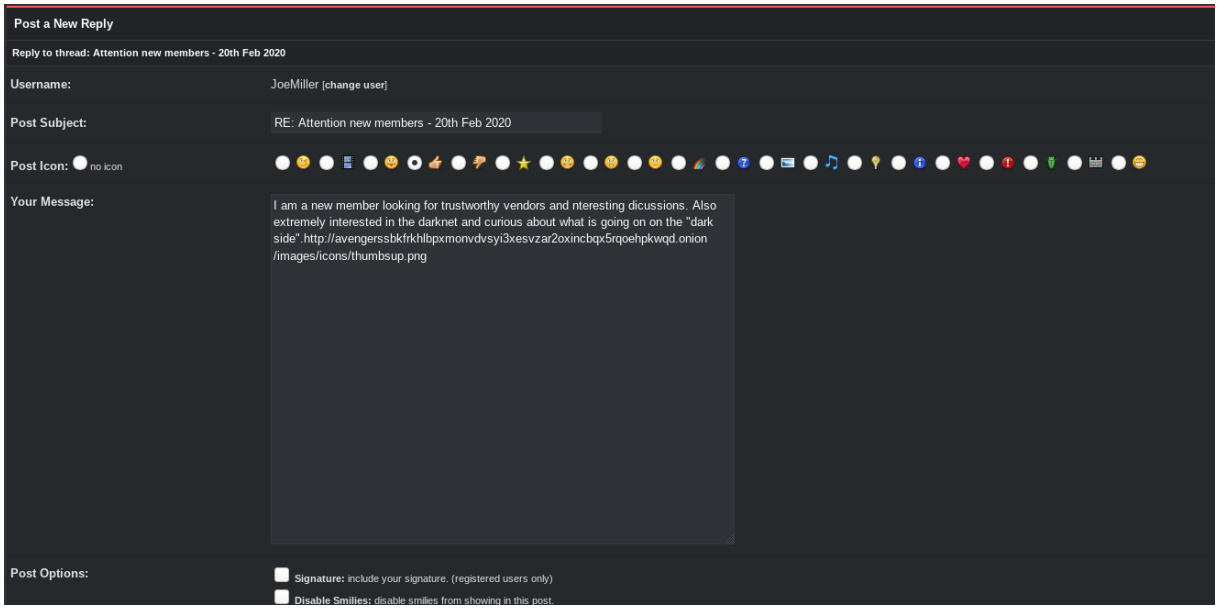
Ähnelt einem Messenger, da sogar der Status vom User angezeigt wird (Online, Away, Offline)

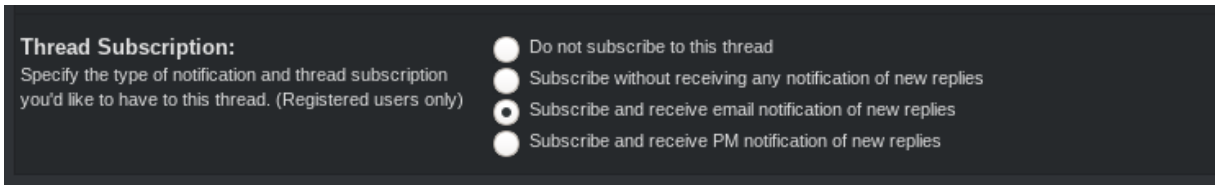
Rollenzuweisungen (Administrator = Captain (8) aber auch Super Moderator (7), normaler Nutzer = Verified User (2), Verkäufer = Verified Market Vendor (6))

Sternenbewertungen

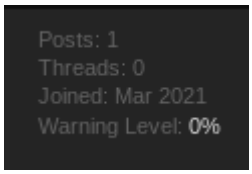
Nach der Registrierung muss ein User vom Admin verifiziert werden, um den Status „Verified User“ zu erhalten:



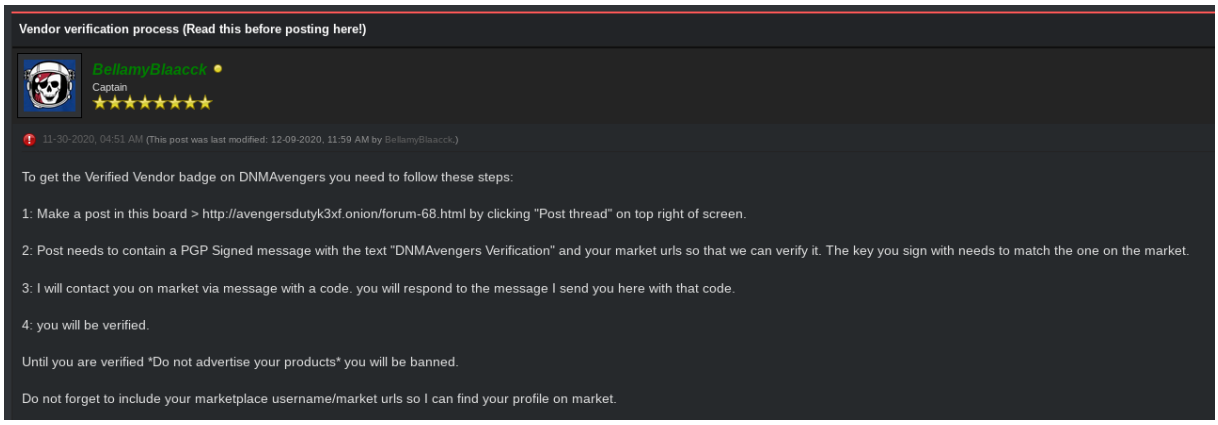


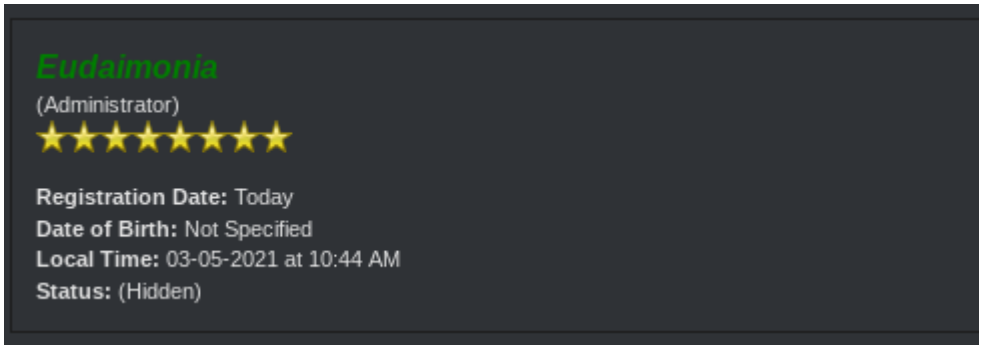


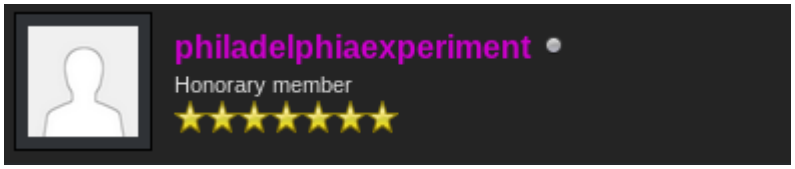
Bei eigenem User Account wird ein sogenannter Warning Level in % angezeigt und gibt an, wie „nah“ man eine Bannung ist:

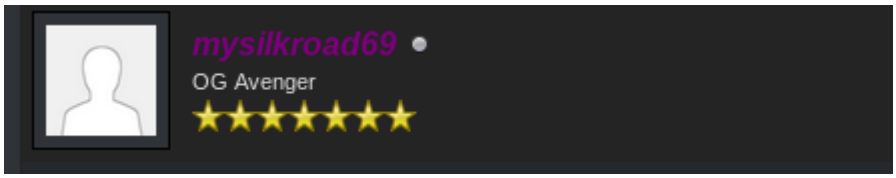


Verifizierung von Verkäufern:

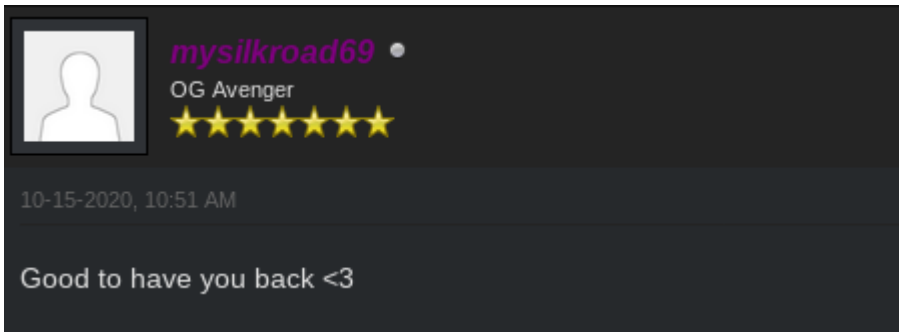


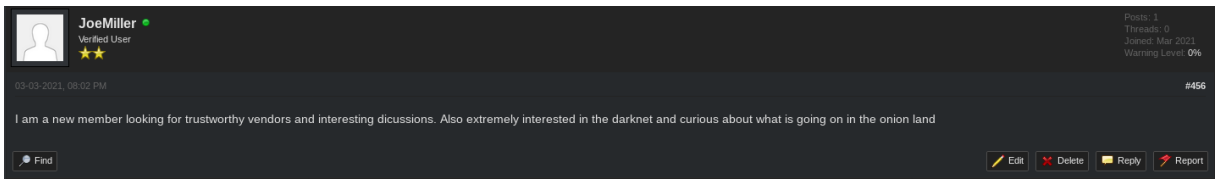


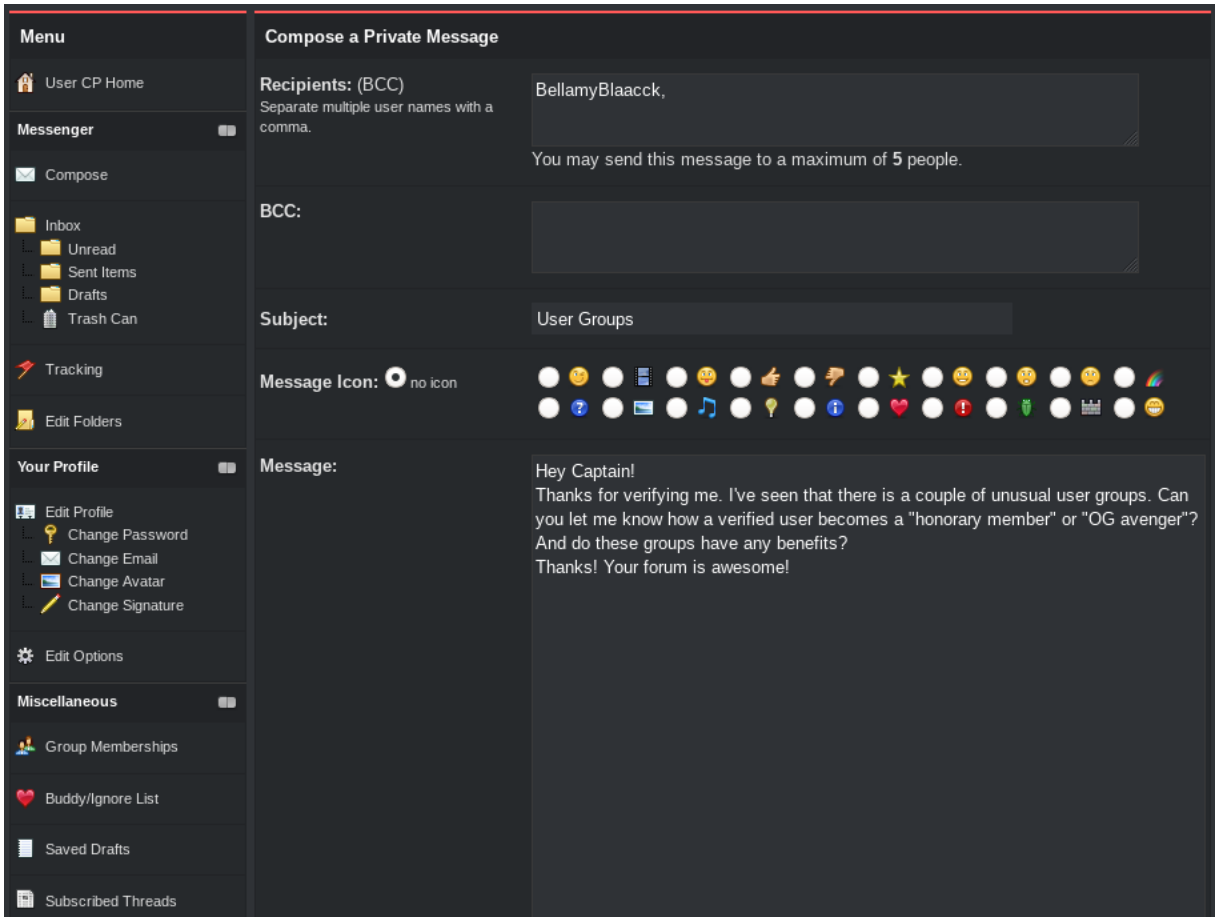


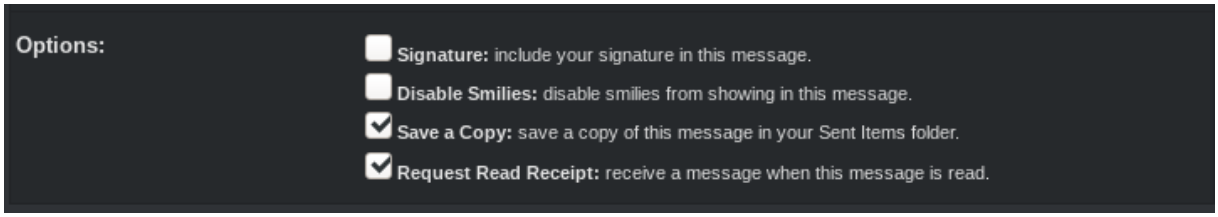


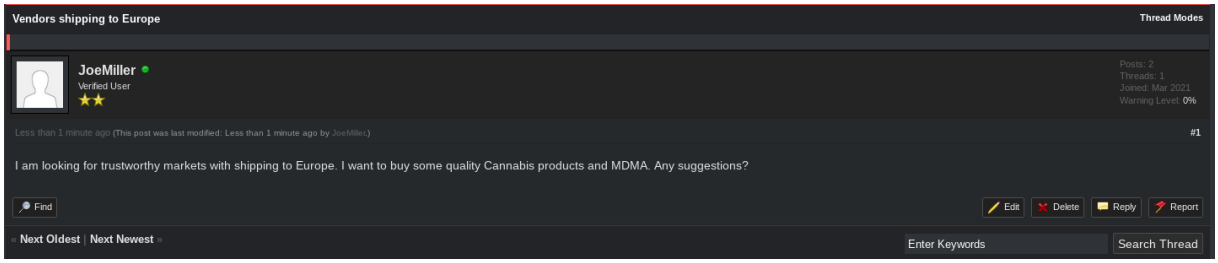
Kommunikation und Einstellung zum Forum:



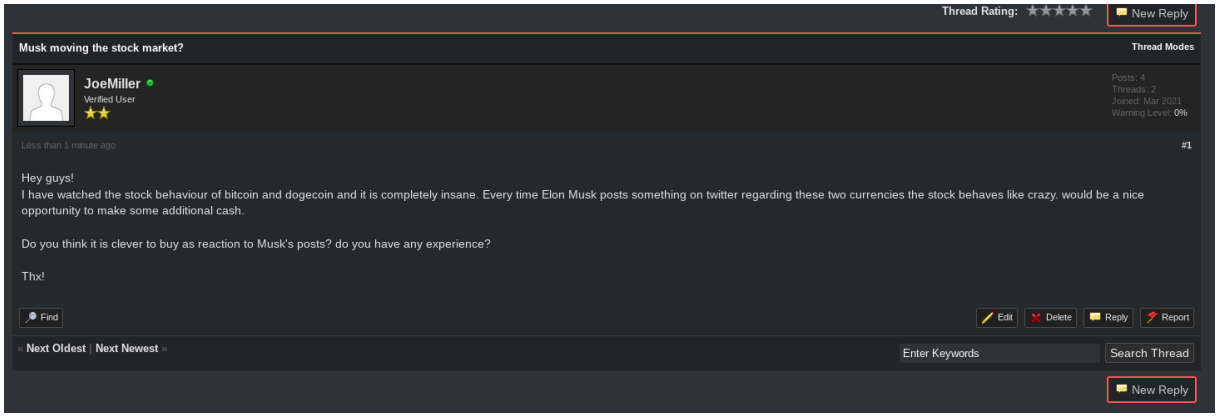


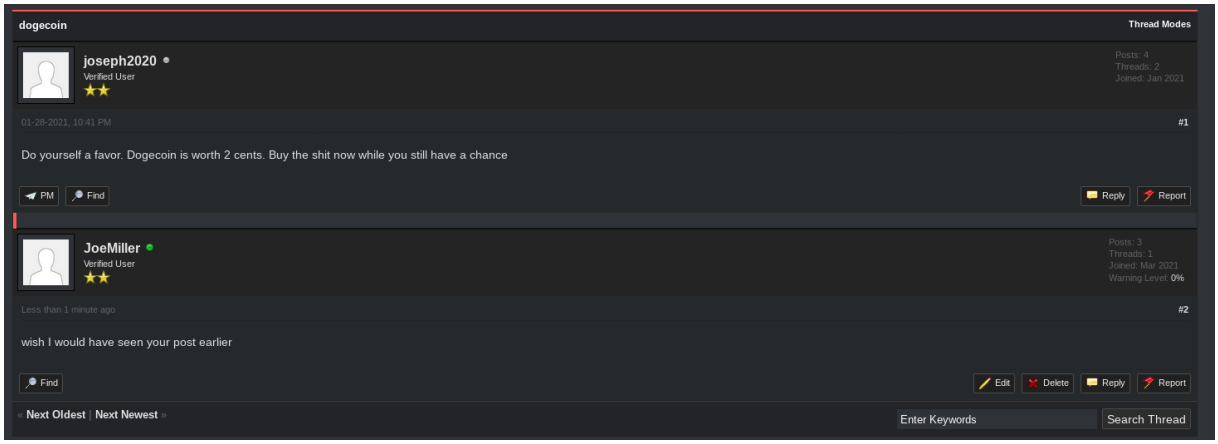




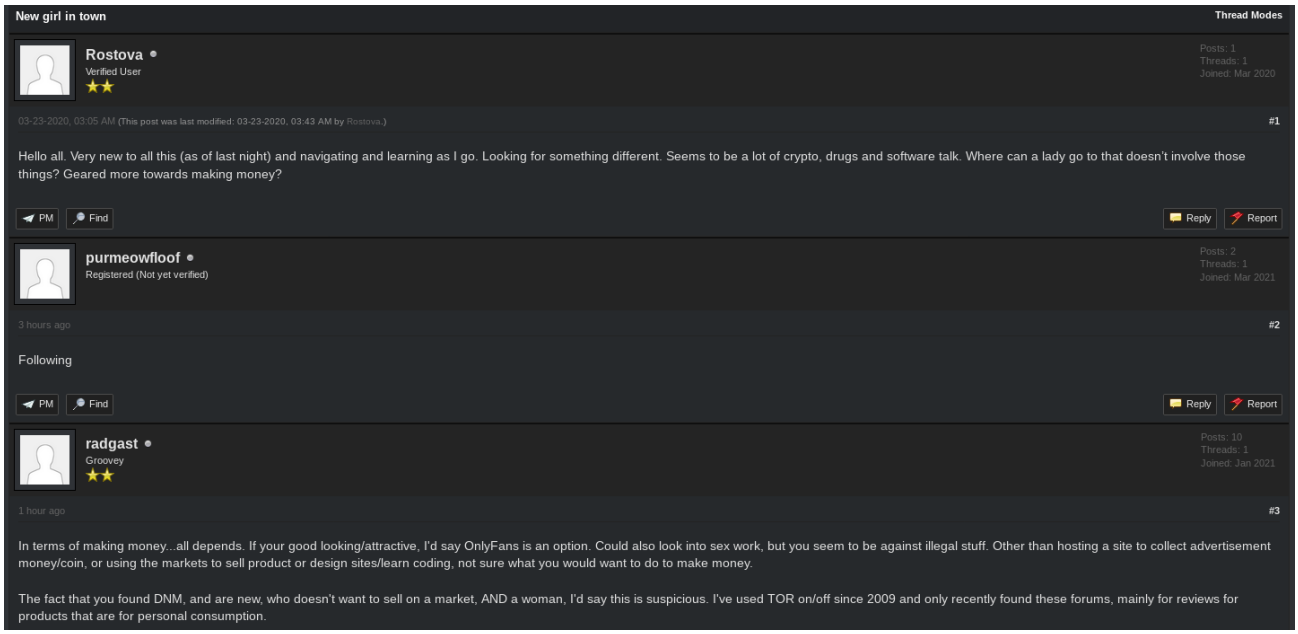


Innerhalb von 1 Minute bereits 3 Views





05.03.2021:
Bisher keine Antwort auf meine Nachrichten. Möglicher Grund: Name JoeMiller zeigt daraufhin, dass ich ein Mann „bin“

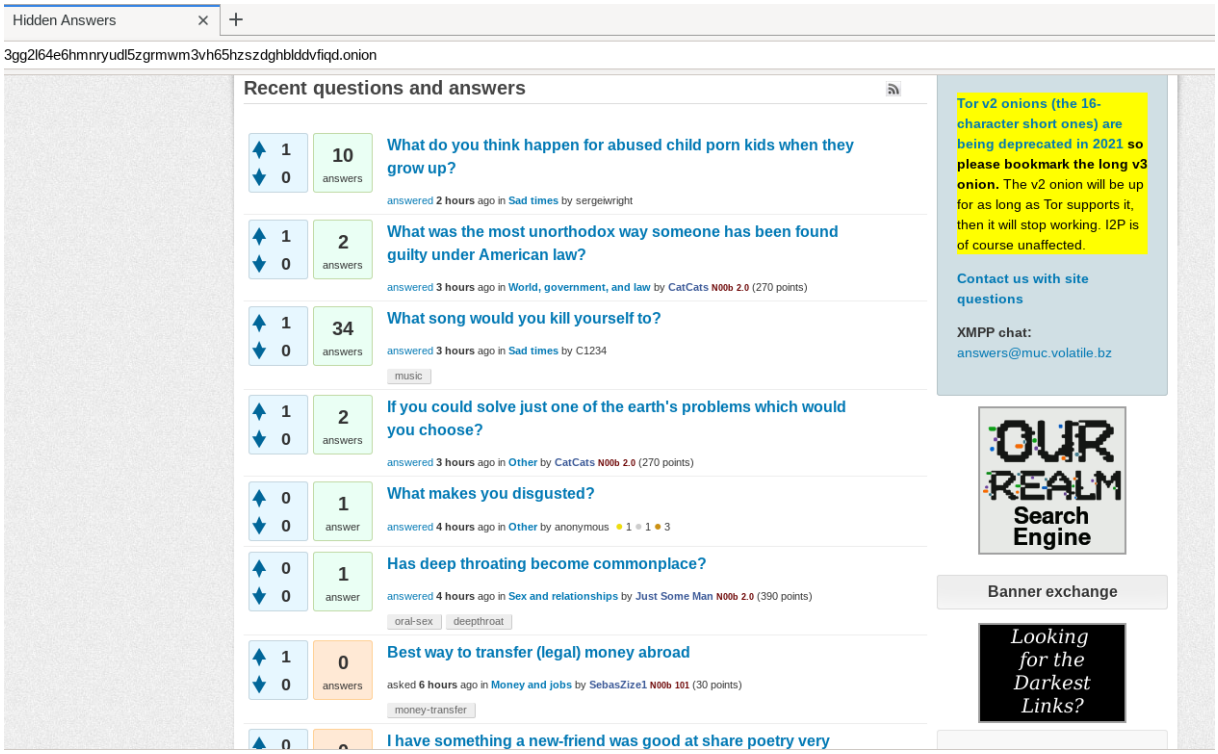


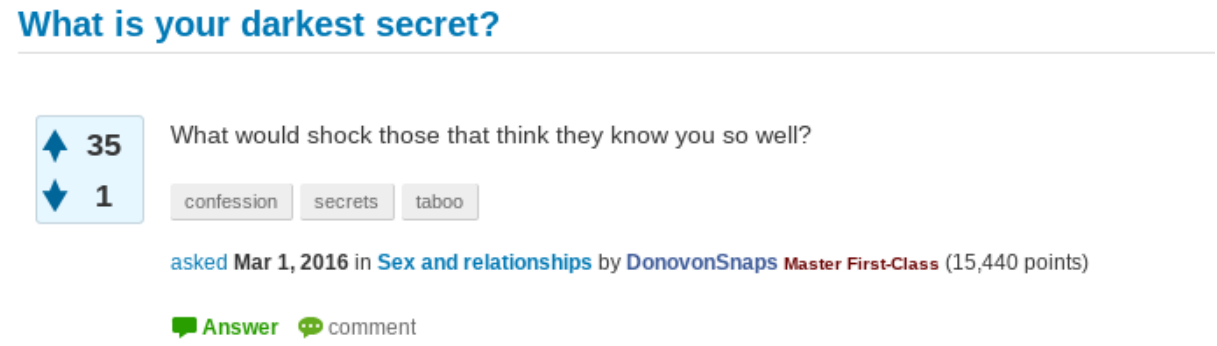
http://answerszuvs3gg2l64e6hmnryudl5zgrmwm3vh65hzszdghbldvfiqd.onion/

Internet forum

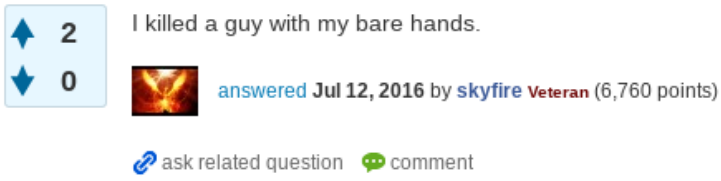
Template:Pp-semi-indef

An **Internet forum**, or **message board**, is an online discussion site where people can hold conversations in the form of posted messages.<ref name="vBfaqFORUM">Template:Cite web</ref> They differ from chat rooms in that messages are often longer than one line of text, and are at least temporarily archived. Also, depending on the access level of a user or the forum set-up, a posted message might need to be approved by a moderator before it becomes visible.





Antworten:



i can't breathe
just let me catch my breath
truth is i'm alone. so very alone. i'm a kissless virgin who never even loved anyone. i'm in the ripe age of passion and yet i feel like i'm not worth it. my slight narcissism is coupled to terrible self-esteem.
i just want to curl up in someone's neck and fall asleep for the most tender sleep.
i want to love someone. i'm so damned, i can't
anyone can relate?

 commented Sep 29, 2016 by feliavlov Champ reply

2
0

I often have fantasies of killing or torturing people. Especially on a large scale, mass shooting type thing. I don't think I would or could ever do it. But sometimes it feels like it's the only way to relieve any of the pain and anger I have from my clinical depression. It's just so not like me, you know? A year ago I could never imagine myself thinking things like this. I've never told anybody I know.

Seriously not trying to be an edgelord. I wish I could just get over this. :p

answered **Jul 18, 2016** by anonymous

ask related question comment

Are you the same person online than you are offline?

0
0

 asked **6 days** ago in Other by xardas Vanguard (39,380 points)

Answer comment

Are you the same person on the dark web than on the surface web?

commented 5 days ago by Eli Knight reply

No , in darkWeb i'm observant i'm not interrupting with people except for this site. In the Web , i have a youtube channel with 1,5k sub were i make music and a soundcloud, i'm in a lot of forum , I love helping people . And in real life i'm very shy

commented 4 days ago by QPX19 N00b 101 reply

Antworten:

0
0

No, I dont think any of us are, I have came to the dark/deep web to get away of everything, see what I can find, in the real world I dont trust anyone to tell my problems, but here everyone is anonymus, so its also safer here to get help for some things

answered **3 days** ago by godotfeetman N00b 101 (20 points)

ask related question comment

0
0

I'm more outgoing and articulate online because I can take time to type out things. In real life I am shy around strangers and can't talk much, or what I say comes out awkward.

answered **6 days** ago by anonymous

ask related question comment

0
0

Pretty close. I'm more willing to discuss certain ideas or topics offline but generally speaking I'm pretty consistent offline.It depends on what we're talking about;

answered **6 days** ago by **madeinchaos** Champ (51,495 points)

ask related question comment

0
0

Well, I'm technically the same person yes, but I like the anon nature of the onion internet- can freely express ideas....great for the introverted. :)

answered **4 days** ago by **PiSquared** N00b 2.0 (330 points)

ask related question comment

0
0

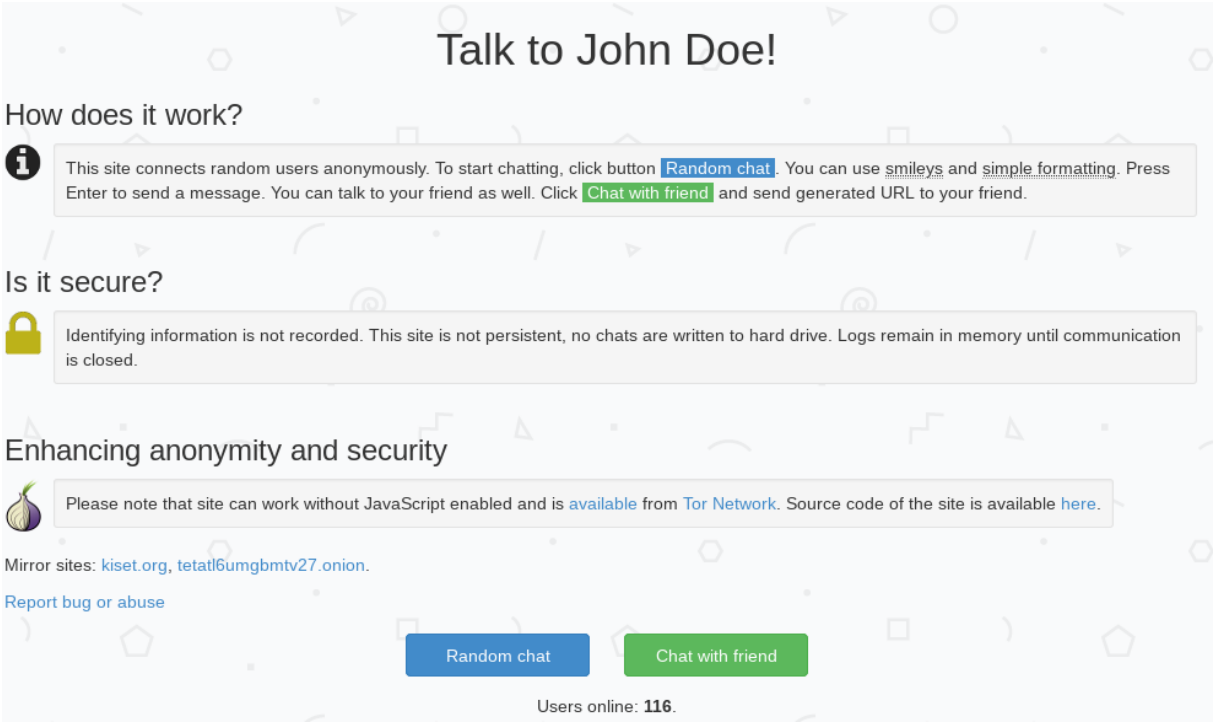
Yes

answered **6 days** ago by **Trying** N00b 3.0 (690 points)

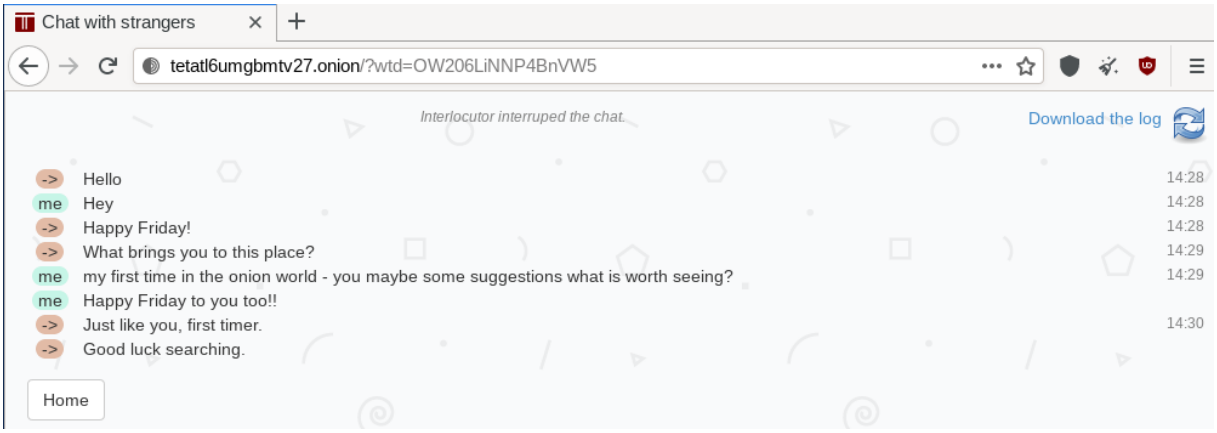
ask related question comment

Chat with strangers:

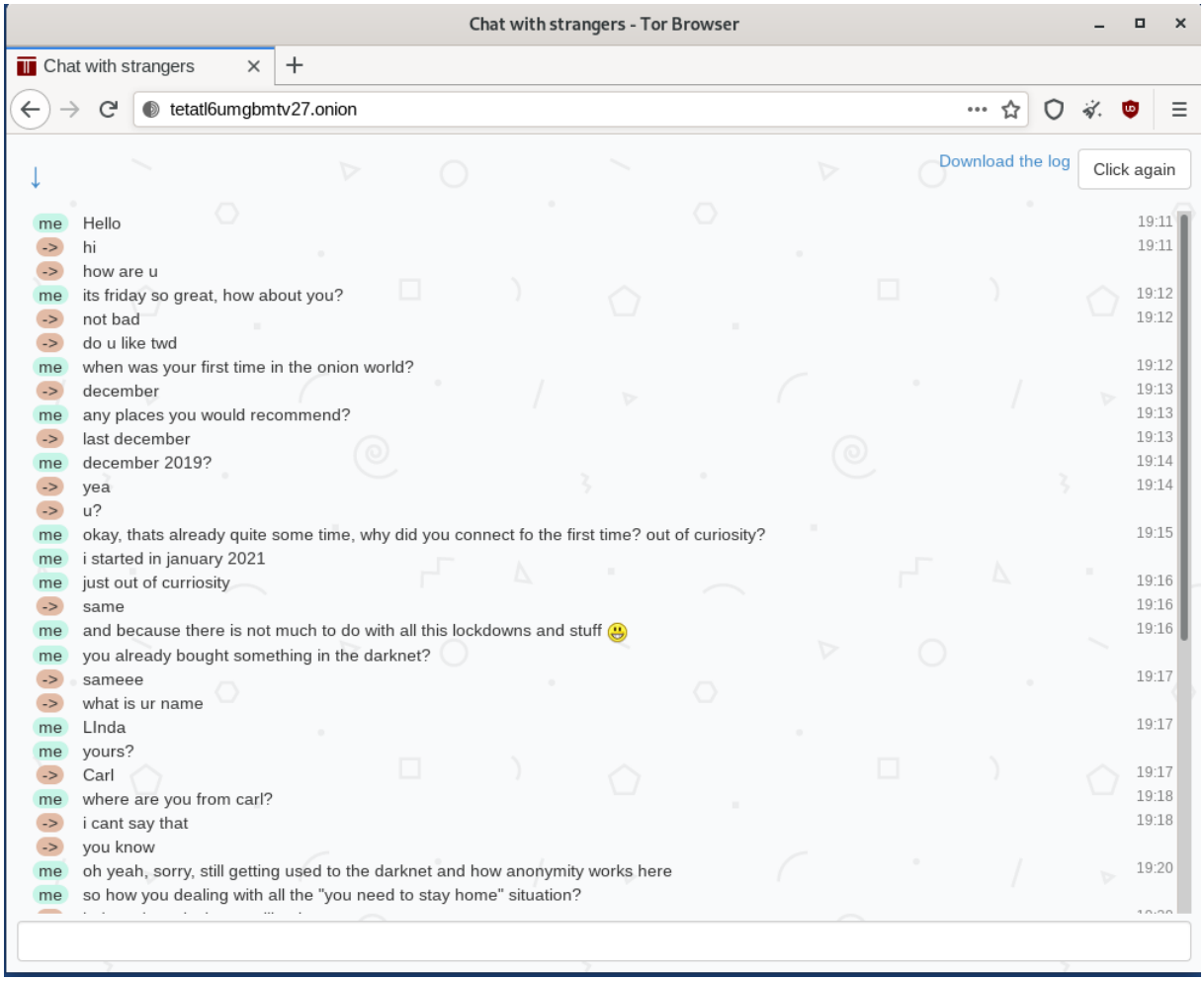
http://tetatl6umgbmtv27.onion/

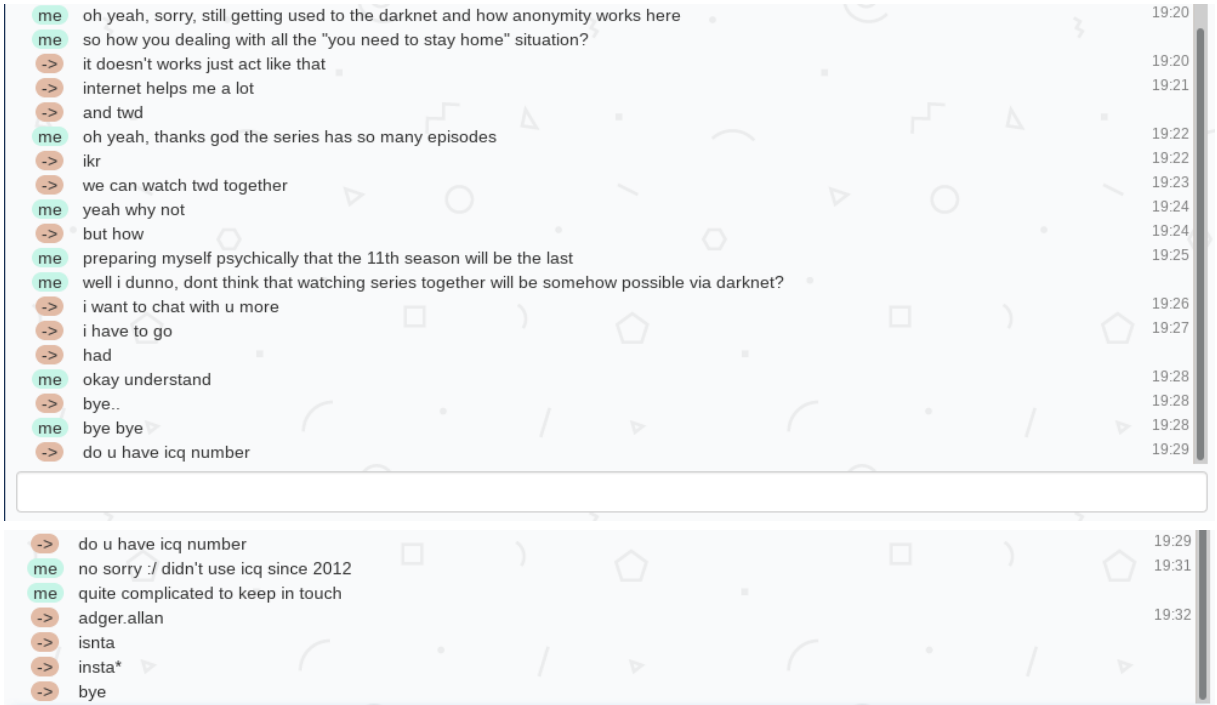


Chat Nr.1:



Chat nr.2:



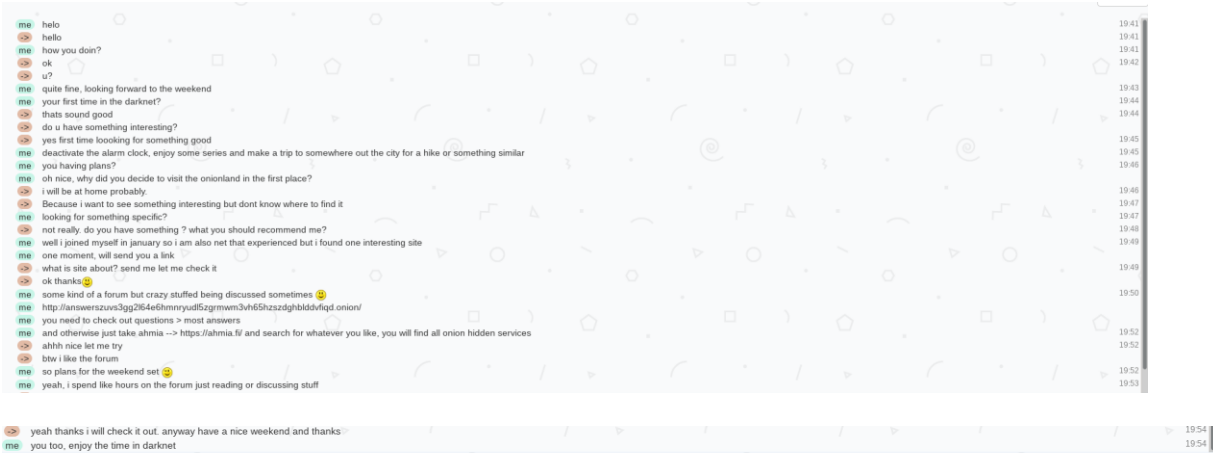


Sehr stressig, da synchrone Kommunikation, mit langen Ladezeiten jedoch schwierig

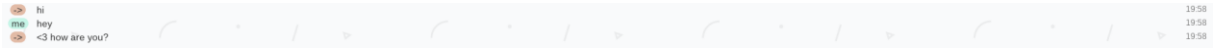
Instagram-Profil geteilt, weil ich einen **weiblichen** Namen verraten habe?

Es ist schwierig, ein Gespräch anzufangen, wenn jegliche Fragen gestellt werden können.

Chat Nr. 3:

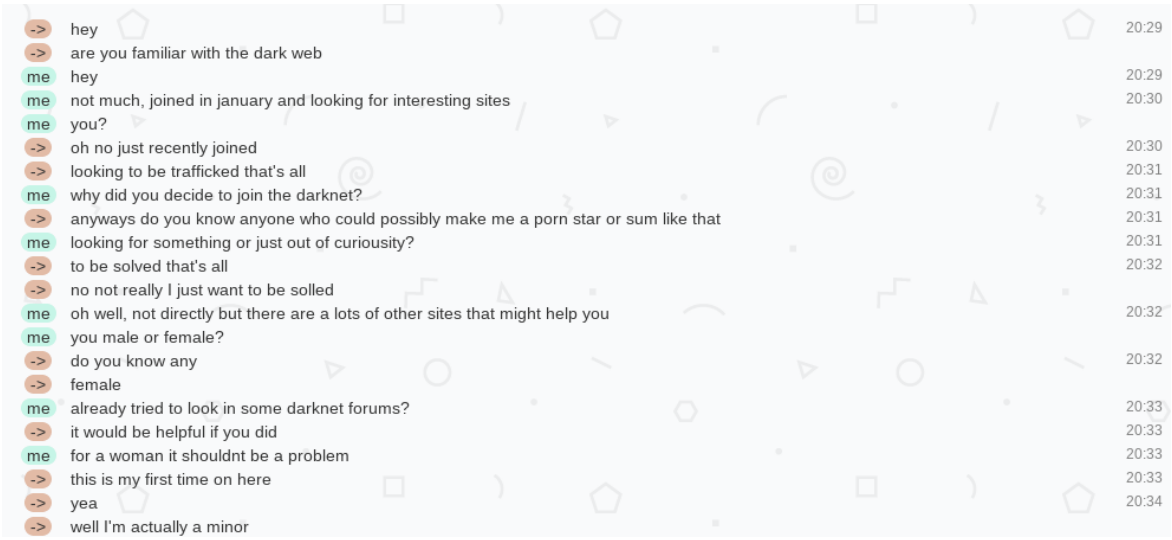


Chat Nr. 4:



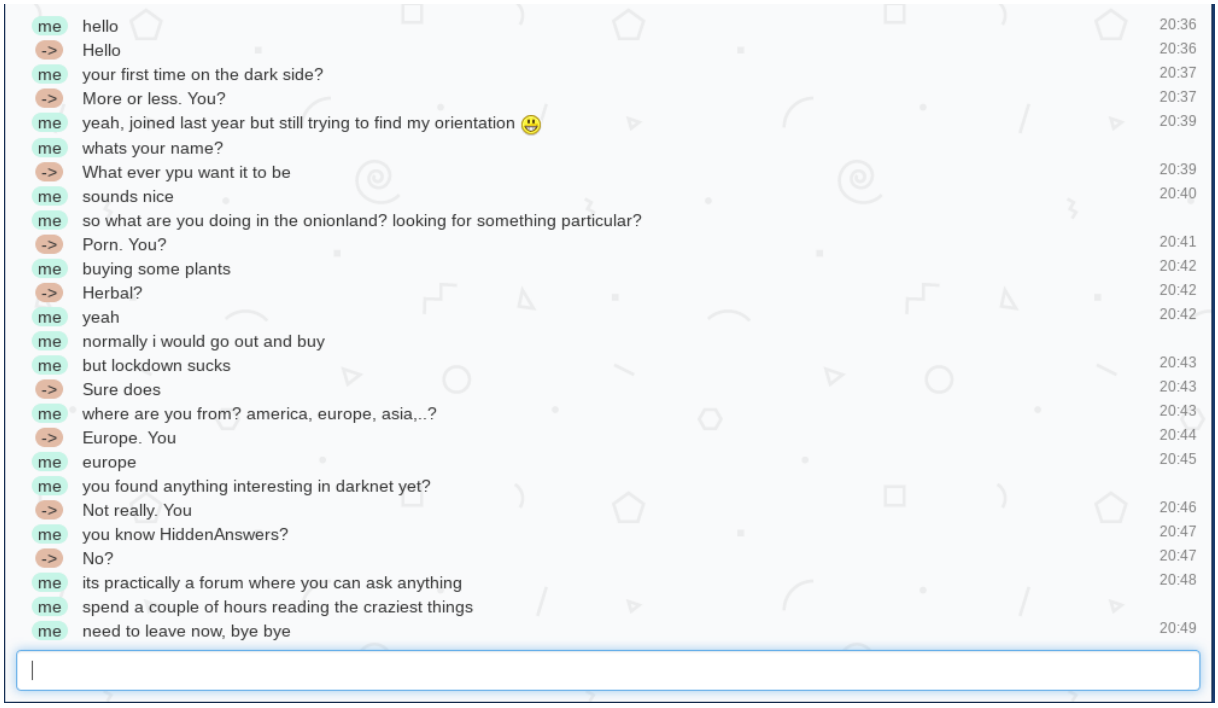
Eine Minute nicht geantwortet und schon wurde der Chat vom Gesprächspartner geschlossen.

Chat Nr.5:

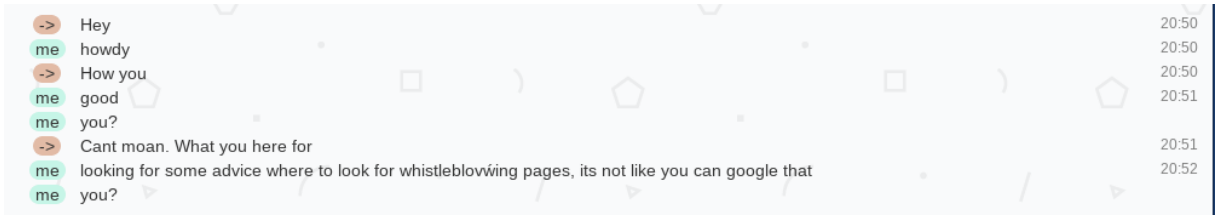


Die Direktheit, mit welcher man konfrontiert wird, ist manchmal einschüchternd bis verstörend

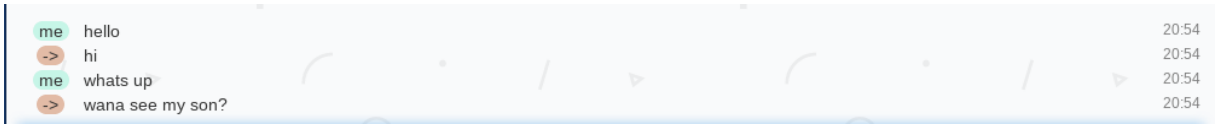
Chat Nr.6:



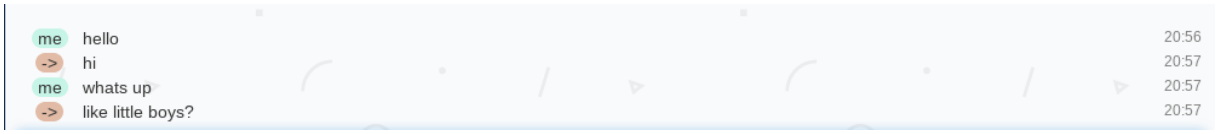
Chat Nr. 7:



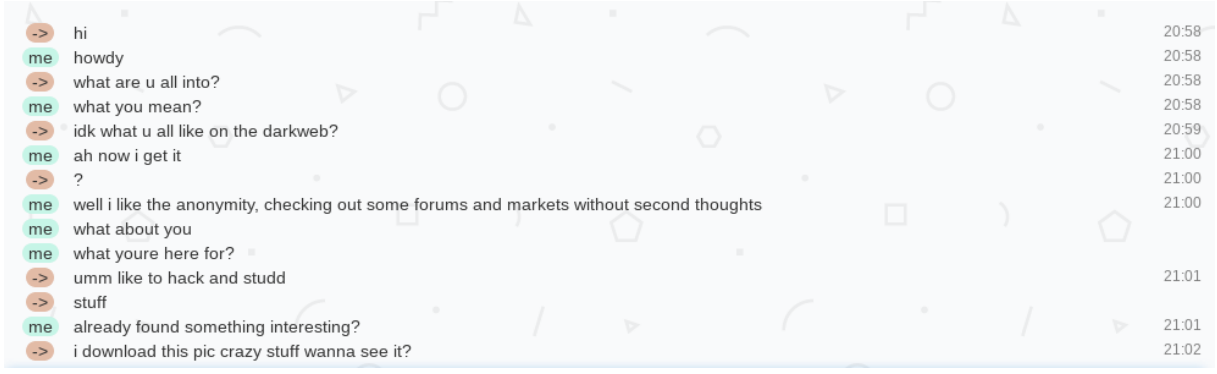
Chat Nr. 8:



Chat Nr. 9:



Chat Nr. 10:



ABKÜRZUNGSVERZEICHNIS

DDoS ..... *Distributed Denial-of-Service*
EBDD ..... *Europäische Beobachtungsstelle für Drogen und Drogensucht*
EMCDDA ..... *European Monitoring Centre for Drugs and Drug Addiction*
FBI ..... *Federal Bureau of Investigation*
I2P ..... *Invisible Internet Project*
IM ..... *Instant Messenger*
OTR ..... *Off-The-Record*
P2P ..... *Peer-To-Peer*
PGP ..... *Pretty Good Privacy*
URL ..... *Uniform Ressource Locator*
VM ..... *Virtuelle Maschine*
VPN ..... *Virtual Private Network*
WWW ..... *World Wide Web*
z.B. ..... *zum Beispiel*

ABBILDUNGSVERZEICHNIS

TABELLENVERZEICHNIS

LITERATURVERZEICHNIS

Ablon, L., Libicki, M., & Golay, A. (2014). *Markets for Cybercrime Tools and Stolen Data.* Von Jstor: https://www.jstor.org/stable/10.7249/j.ctt6wq7z6 abgerufen

Aldridge, J., & Décary-Hétu, D. (13. Mai 2014). *Not an 'Ebay for Drugs': The Cryptomarket 'Silk Road' as a Paradigm Shifting Criminal Innovation.* Von SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2436643 abgerufen

Aldridge, J., & Décary-Hétu, D. (September 2016). Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets. *International Journal of Drug Policy*, S. 7-15.

Allahyari, M., Doran, D., Sadeghi, R., & Zabihimayvan, M. (2019). A Broad Evaluation of the Tor English Content Ecosystem. *10th ACM Conference*, (S. 1).

Anonym. (4. Februar 2021). Sammlung von Erfahrungen aus dem Darknet. (E. Krnavkova, Interviewer)

Ascherman, T. (7. Juni 2015). *Was ist ein Forum? Einfach erklärt*. Von CHIP: https://praxistipps.chip.de/was-ist-ein-forum-einfach-erklaert_41375 abgerufen

Avarikioti, G., Brunner, R., Kiayias, A., Wattenhofer, R., & Zindros, D. (2018). *Structure and Content of the Visible Darknet*. Von https://arxiv.org/pdf/1811.01348.pdf abgerufen

Balduzzi, M., & Ciancaglini, V. (2015). Cybercrime in the Deep Web. *Black Hat EU*, (S. 1). Amsterdam.

Ball, J., Schneier, B., & Greenwald, G. (4. Oktober 2013). NSA and GCHQ target Tor network that protects anonymity of web users. *The Guardian*, S. https://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption.

Baravalle, A., Lee, S. W., & Sanchez Lopez, M. (2016). Mining the Dark Web: Drugs and Fake Ids. (S. 1-7). London: University of East London.

Bartlett, J. (2014). *The Dark Net: Inside the Digital Underworld.* Brooklyn, London: Melville House.

Bedi, P., Gupta, N., & Jindal, V. (2020). Dark Web: A Boon or a Bane. In *Encyclopedia of Criminal Activities and the Deep Web.* IGI Global.

Biryukov, A., & Pustogarov, I. (2014). *Bitcoin over Tor isn't a good idea.* University of Luxemburg.

Bischoff, P. (7. Dezember 2020). *Step by step guide to safely accessing the dark web*. Von comparitech: https://www.comparitech.com/blog/vpn-privacy/access-dark-web-safely-vpn/ abgerufen

Brandt, M. (28. Juni 2018). *Das Drugnet*. Von Statista: https://de.statista.com/infografik/14470/verteilung-von-aktiven-darknet-listings-weltweit/ abgerufen

Brandt, M. (12. März 2019). *Das (nicht ganz) weltweite Web*. Von Statista: https://de.statista.com/infografik/5583/geschaetzte-anzahl-der-internetnutzer-weltweit/ abgerufen

Branwen, G. (14. Juli 2016). *The data of the dark web*. Von The Economist: https://www.economist.com/graphic-detail/2016/07/14/the-data-of-the-dark-web abgerufen

Broadhurst, R., Foye, J., Jiang, C., & Ball, M. (2020). *Illicit firearms and weapons on darknet markets.* Australian National University's Cybercrime Observatory; School of Regulation and Global Governance.

Broadhurst, R., Lord, D. R., Maxim, D., Woodford-Smith, H., Johnston, C. R., Caroll, S., . . . Sabol, B. (2018). *Malware Trends on 'Darknet' Crypto-markets: Research Review.* Australian National University Cybercrime Observatory and the Korean Institute of Criminology.

Bundesamt für Sicherheit in der Elektrotechnik. (01. Februar 2021). *OPS.1.1.4 Schutz vor Schadprogrammen*. Von IT-Grundschutz: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/04_OPS_Betrieb/OPS_1_1_4_Schutz_vor_Schadprogrammen_Edition_2021.pdf?__blob=publicationFile&v=2 abgerufen

Bundeskriminalamt. (2017). *Lagebericht - Suchtmittelkriminalität 2017.* Österreich: Bundeskriminalamt.

Çalışkan, E., Minárik, T., & Osula, A.-M. (2015). *Technical and Legal Overview of the Tor Anonymity Network.* Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

Chandhana, S. D., & Mary, A. (10. Februar 2012). Defending Against Sybil Attacks in Anonymizing Networks. *Journal of Computer Applications*, S. 389-395.

Chat with strangers. (22. Februar 2021). Von http://tetatl6umgbmtv27.onion/ abgerufen

Ciancaglini, V., Balduzzi, M., McArdle, M., & Rösler, M. (2015). *Below the Surface: Exploring the deep Web.* Trend Micro.

ComputerWeekly, TechTarget. (Juli 2016). *XMPP (Extensible Messaging and Presence Protocol)*. Von ComputerWeekly: https://www.computerweekly.com/de/definition/XMPP-Extensible-Messaging-and-Presence-Protocol abgerufen

Dange, V., Malkan, K., & Jha, M. (2018). *Monograph on Darknet.* Pune: Dhole Patil College of Engineering.

DNMAvengers. (24. Februar 2021). Von http://avengerssbkfrkhlbpxmonvdvsyi3xesvzar2oxincbqx5rqoehpkwqd.onion/ abgerufen

DuckDuckGo. (16. Februar 2021). Von https://duckduckgo.com/?va=b&t=hc abgerufen

Eckermann, I. (2017). *Was ist eigentlich das Darknet?* Von G DATA: https://www.gdata.de/ratgeber/was-ist-eigentlich-das-darknet abgerufen

EuCanna. (24. Febuar 2021). Von http://rso4hutlefirefqp.onion/ abgerufen

European Monitoring Centre for Drugs and Drug Addiction; Europol. (2017). *Drugs and the darknet - Perspectives for enforcement, research and policy.* Luxemburg: Publications Office of the European Union.

Europol. (20. Juli 2017). *MASSIVE BLOW TO CRIMINAL DARK WEB ACTIVITIES AFTER GLOBALLY COORDINATED OPERATION*. Von Europol: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation abgerufen

Frickel, C. (25. Februar 2016). *Wie schützt man sich generell vor Schad-Software?* Von Focus Online: https://www.focus.de/digital/computer/tid-23846/online-durchsuchung-so-schuetzen-sie-sich-vor-dem-bundestrojaner_aid_673567.html abgerufen

Geiger, J. (15. Oktober 2015). *Linux Virenscanner Test: Nur ein kostenloser bietet Schutz*. Von CHIP: https://www.chip.de/artikel/Linux-Virenscanner-Test-Nur-ein-kostenloser-bietet-Schutz_139987731.html abgerufen

Geiger, J. (21. Januar 2021). *Virenscanner-Test 2021: Die besten Security-Suiten für Windows*. Von CHIP: https://www.chip.de/artikel/Virenscanner-Test-Windows-Das-sind-die-besten-Security-Suiten_179237183.html abgerufen

Goldschlag, D., Reed, M., & Syverson, P. (1996). Hiding Routing information. In D. Goldschlag, M. Reed, & P. Syverson, *Lecture Notes in Computer Science* (S. 137-150). Berlin, Heidelberg: Springer.

Gollnick, C., & Wilson, E. (2016). *Separating Fact from Fiction: The Truth about the Dark Web.* Terbium Labs.

Görmer, J. (2018). Anonymität im Darknet - Nutzer und Usability im Vergleich der drei Hauptvertreter. *Hochschulschrift*. Anhalt: Hochschule Anhalt.

Graham, R., & Pitman, B. (2018). Freedom in the wilderness: A study of a Darknet space. *The International Journal of Research into New Media Technologies*, S. 2-18.

Greenberg, A. (2. Februar 2015). *Read the Transcript of Silk Road's Boss Ordering 5 Assassinations*. Von Wired: https://www.wired.com/2015/02/read-transcript-silk-roads-boss-ordering-5-assassinations/ abgerufen

Hahn, J. (15. Januar 2020). *Solving Noisy Text CAPTCHAs*. Von Medium: https://medium.com/analytics-vidhya/solving-noisy-text-captchas-126734c3c717 abgerufen

Hern, A. (17. April 2014). Tor may be forced to cut back capacity after Heartbleed bug. *The Guardian*, S. https://www.theguardian.com/technology/2014/apr/17/tor-heartbleed-bug-vulnerable-servers.

HiddenAnswers. (27. Februar 2021). Von http://answerszuvs3gg2l64e6hmnryudl5zgrmwm3vh65hzszdghbldvfiqd.onion/ abgerufen

HiddenWikki - Onion. (18. Februar 2021). Von http://ndntmfusjmj6tkpl.onion/ abgerufen

Hoffer, M. (2018). *Einführung ins Darknet.* Norderstedt: Books on Demand.

Horton-Eddison, M., & Di Cristofaro, M. (2017). *Hard Interventions and Innovation in Crypto-Drug Markets: The escrow example.* Swansea: Global Drug Policy Observatory, Swansea University.

HQER - High Quality Euro Replicas /Counterfeits. (24. Februar 2021). Von http://y3fpieiezy2sin4a.onion/ abgerufen

Huang, K., Siegel, M., Pearlson, K., & Madnick, S. (Juni 2019). Casting the Dark Web in a New Light. *MIT Sloan Management Review*, S. 1-9.

Iva, S. (2. August 2019). *Was ist das Darknet? Die wichtigsten Fragen und Antworten*. Von Focus Online: https://www.focus.de/digital/experten/versteckter-teil-des-internets-was-ist-das-darknet-die-wichtigsten-fragen-und-antworten_id_10992451.html abgerufen

Jacksi, K., & Abass, S. (September 2019). Development History Of The World Wide Web. *International Journal of Scientific & Technology Research 8(9)*, S. 75-79.

Jadoon, A. K., Iqbal, W., Amjad, M., Afzal, H., & Bangash, Y. A. (26. März 2019). Forensic Analysis of Tor Browser: A Case Study for Privacy and Anonymity on the Web. *Forensic Science International 299*, S. 59-73.

Johnson, A., Wacek, C., Jansen, R., Sherr, M., & Syverson, P. (2013). Users Get Routed: Traffic Correlation on Tor by Realistic Adversaries. *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security.* Berlin: ACM.

Konrad, A. (2013). Feds Say They've Arrested 'Dread Pirate Roberts,' Shut Down His Black Market 'The Silk Road'. *Forbes*.

Kumar, A., & Rosenbach, E. (September 2019). The Truth about the Dark Web. *Finance & Development*, S. 22-25.

McCarthy, N. (23. März 2018). *Where Guns are Sold Through The Darknet*. Von Statista: https://www.statista.com/chart/13327/where-guns-are-sold-through-the-darknet/ abgerufen

Mey, S. (2. August 2016). *Die Kartografen des Darknets*. Von Spektrum.de: https://www.spektrum.de/news/wie-illegal-ist-das-darknet/1418700 abgerufen

Mills, M. (13. Juni 2020). *What is PGP: Definition, Characteristics and Utilities* . Von ITIGIC: https://itigic.com/what-is-pgp-definition-characteristics-and-utilities/ abgerufen

Mirea, M., Wang, V., & Jung, J. (2018). The not so dark side of the darknet: a qualitative study. *Security Journal*, 102-118.

Moore, D., & Rid, T. (1. Februar 2016). Cryptopolitik and the Darknet. *Survival - Global Politics and Strategy*, S. 7-38.

Murali, J. (2019). A Bustling Darknet Weapons Market. *DECCAN Chronicle*, 5.

Najjar, M., & Schwaß, H. (2019). *Das Darknet - Im Licht der Öffentlichkeit.* Halle-Wittenberg: Martin-Luther-Universität Halle-Wittenberg.

Namestnikov, Y. (2009). *The economics of Botnets.* Von Secure List by Kaspersky: https://securelist.com/the-economics-of-botnets/36257/ abgerufen

Nastuła, A. (April 2020). Dilemmas related to the functioning and growth of Darknet and the Onion Router network. *Journal of Scientific Papers Social development & Security*, S. 3-10.

Nelson, L. (1. August 2017). *The deep web, the dark web, and simple things*. Von Medium: https://medium.com/@smartrac/the-deep-web-the-dark-web-and-simple-things-2e601ec980ac abgerufen

Nimfuehr, M. (18. August 2018). *Silk Road: A Cautionary Tale about Online Anonymity*. Von Medium: https://medium.com/@marcell74/the-silk-road-a-real-thriller-and-the-truth-about-the-anonymity-of-bitcoin-198b519ca397 abgerufen

Nishikaze, H., Ozawa, S., Kitazono, J., Ban, T., Nakazato, J., & Shimamura, J. (2015). Large-Scale Monitoring for Cyber Attacks by Using Cluster Information on Darknet Traffic Features. *Procedia Computer Science*, S. 175-182.

Omar, Z. M., & Ibrahim, J. (2020). An Overview of Darknet, Rise and Challenges and Its Assumptions. *International Journal of Computer Science and Information Technology*, 110-116.

OnionDir. (18. Februar 2021). Von http://dirnxxdraygbifgc.onion/ abgerufen

Oracle. (kein Datum). *About VirtualBox*. Von VirtualBox: https://www.virtualbox.org/wiki/VirtualBox abgerufen

Paoli, G., Aldridge, J., Ryan, N., & Warnes, R. (2017). *Behind the curtain: The illicit trade of firearms, explosives and ammunition on the dark web.* RAND Corporation.

Patterson, D. (11. März 2019). *How to safely access and navigate the Dark Web*. Von TechRepublic: https://www.techrepublic.com/article/how-to-safely-access-and-navigate-the-dark-web/ abgerufen

ProtonMail. (25. Februar 2021). Von https://protonirockerxow.onion/ abgerufen

ProtonMail. (kein Datum). *How to use PGP?* Von ProtonMail Support: https://protonmail.com/support/knowledge-base/how-to-use-pgp/ abgerufen

ProtonMail. (kein Datum). *ProtonMail*. Von https://protonmail.com/de/ abgerufen

Quinney, A. (27. Juni 2016). *surface web vs deep web vs dark web*. Von Service Care Solutions: https://www.servicecare.org.uk/news/surface-web-vs-deep-web-vs-dark-web-61792715468 abgerufen

Rathod, D. (Juli-August 2017). Darknet Forensics. *International Journal of Emerging Trends & Technology in Computer Science*, S. 77-79.

Rentrop, C. (24. November 2019). *Anonym und sicher surfen: Alles über den Tor-Browser*. Von Netzwelt: https://www.netzwelt.de/news/173549-anonym-sicher-surfen-alles-ueber-tor-browser.html abgerufen

Roose, K. (5. März 2018). Here Come the Fake Videos, Too. *The New York Times*, S. Section A, Seite 1.

Rückert, C. (Mai/Juni 2018). Das Darknet: Blick in eine Schattenwelt. *Politische Studien 479 im Fokus "Die digitale Revolution"*, S. 10.

Schmidt, J. (4. August 2016). *Tor und die versteckten Dienste*. Von heise Security: https://www.heise.de/security/artikel/Tor-und-die-versteckten-Dienste-3280904.html abgerufen

Schneier, B. (4. Oktober 2013). Attacking Tor: how the NSA targets users' online anonymity. *The Guardian*, S. https://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity.

searchmetrics. (kein Datum). *Link Popularity*. Von searchmetrics: https://www.searchmetrics.com/glossary/link-popularity/#:~:text=Link%20popularity%20refers%20to%20the,website%20of%20a%20car%20dealer abgerufen

SEO-Analyse. (kein Datum). *Forum Begriffserklärung und Definition*. Von SEO-Analyse: https://www.seo-analyse.com/seo-lexikon/f/forum/ abgerufen

SEO-Analyse. (kein Datum). *IRC Begriffserklärung und Definition*. Von SEO-Analyse: https://www.seo-analyse.com/seo-lexikon/i/irc/ abgerufen

SEO-united. (kein Datum). *Was ist Link Popularity*. Von SEO-united: https://www.seo-united.de/glossar/link-popularity/ abgerufen

Shanika, W. (12. Juli 2020). *VPN with Tails — The Basics You Need to Know*. Von Privacy Affairs: https://www.privacyaffairs.com/vpn-with-tails/ abgerufen

Sommers, C., & Bernstein, E. (10. November 2020). *Inside the FBI takedown of the mastermind behind website offering drugs, guns and murders for hire*. Von CBS News: https://www.cbsnews.com/news/ross-ulbricht-dread-pirate-roberts-silk-road-fbi/ abgerufen

Soska, K., & Christin, N. (2015). Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem. *24th USENIX Security Symposium* (S. 33-48). Washington,D.C.: Carnegie Mellon University.

Spalevic, Z., & Ilic, M. (Januar-März 2017). THE USE OF DARK WEB FOR THE PURPOSE OF ILLEGAL ACTIVITY SPREADING. *Ekonomika*, S. 73-82.

Sui, D., Caverlee, J., & Rudesill, D. (2015). *The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box.* Washington DC: Wilson Center - Science and Technology Innovation Program.

Sullivan, J. (22. März 2011). *2010 Free Software Awards announced*. Von FSF - Free Software Foundation: https://www.fsf.org/news/2010-free-software-awards-announced abgerufen

Syverson, P. (2011). A peel of onion. *ACSAC '11: Proceedings of the 27th Annual Computer Security Applications Conference* (S. 123-137). Washington DC: ACM.

Tails. (kein Datum). *Tails*. Von Tails: https://tails.boum.org/index.de.html abgerufen

Talk.Masked | Talks and Notes. 2nd generation. (22. Februar 2021). Von http://ci3hn2uzjw2wby3z.onion/ abgerufen

Tanriverdi, H. (2017). Drei Gründe, warum Ermittler erfolgreich Drogenplätze aus dem Darknet werfen. *Süddeutsche Zeitung*, https://www.sueddeutsche.de/digital/kriminalitaet-drei-gruende-warum-ermittler-erfolgreich-drogenplaetze-aus-dem-darknet-werfen-1.3646725-2.

Tardini, S., & Cantoni, L. (2013). World Wide Web. In *Encyclopedia of Media and Communication* (S. 715). Toronto-Buffalo-London: University of Toronto Press.

TechTarget . (September 2005). *chat room*. Von WhatIs: https://whatis.techtarget.com/definition/chat-room#:~:text=A%20chat%20room%20is%20a,to%20communicate%20in%20real%20time.&text=Users%20can%20enter%20chat%20rooms,a%20practice%20known%20as%20lurking. abgerufen

TheHiddenWikki. (18. Februar 2021). Von https://thehiddenwiki.org/ abgerufen

TOR Project. (kein Datum). *Tor Metrics*. Von TOR Project: https://metrics.torproject.org/ abgerufen

TorLinks. (18. Februar 2021). Von http://torlinkbgs6aabns.onion/ abgerufen

TrustWiki. (18. Februar 2021). Von http://wiki6dtqpuvwtc5hopuj33eeavwa6sik7sy57cor35chkx5nrbmmolqd.onion/?section=all abgerufen

UK Passports. (24. Februar 2021). Von http://vfqnd6mieccqyiit.onion/ abgerufen

United Nations. (2016). *World Drug Report 2016.* New York: United Nations publication.

USA Citizenship. (24. Februar 2021). Von http://xfnwyig7olypdq5r.onion/ abgerufen

USfakeIDs - High quality USA Fake Drivers Licences. (22. Februar 2021). Von http://en35tuzqmn4lofbk.onion/ abgerufen

van der Burgt, R. (18. Dezember 2020). *Dark-Web-Seiten, die sich lohnen*. Von VPNOverview: https://vpnoverview.com/de/privatsphaere/anonym-surfen/dark-web-seiten-die-sich-lohnen/ abgerufen

Weimann, G. (2018). *GOING DARKER? THE CHALLENGE OF DARK NET TERRORISM.* Washington DC: Woodrow Wilson Center.

Wernicke, C. (2016). *Darknet, Bitcoin, Fraud.* CreateSpace Independent Publishing Platform.

Wilde, O. (1981). *Der Kritiker als Künstler: Diverse Aspekte zu Oscar Wildes "The Critic as Artist".* Corpus of Electronic Texts Edition.

World Customs Organization. (2016). *Illicit Trade Report 2015.* Brüssel: World Customs Organization.

Yaneza, J. (4. Februar 2014). *Defending Against Tor-Using Malware, Part 2*. Von trendmicro: https://blog.trendmicro.com/trendlabs-security-intelligence/defending-against-TOR-using-malware-part-2/ abgerufen