Univerzita Hradec Králové

Fakulta informatiky a managementu

Katedra informačních technologií

Analýza sítě Darknet se zaměřením na Darkweb

Diplomová práce

Autor: Bc. Jindřich Dědek
Studijní obor: N1802 Aplikovaná informatika, navazující magisterský

Vedoucí práce: Ing. Vladimír Soběslav, Ph.D.

Hradec Králové duben 2019

Prohlášení:

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a s použitím uvedených zdrojů a literatury.

V Hradci Králové dne 29.4.2019 Jindřich Dědek

Poděkování:

Děkuji vedoucímu diplomové práce Ing. Vladimíru Soběslavovi, Ph.D., za metodické vedení práce, odbornou pomoc a rady při zpracování této práce. Děkuji taktéž mamince a tatínkovi, jejichž neutuchající verva po vzdělání a životních úspěších obou jejich synů mi dodávala motivaci po celou dobu studia, jež mimo jiné, nezanedbatelnou částí přispěla i k dokončení této práce, potažmo dosažení vysněného vzdělání. Taktéž děkuji všem blízkým za podporu, trpělivost a vytváření ideálních podmínek po celou dobu studia.

Anotace

Tato diplomová práce s názvem “Analýza sítě Darknet se zaměřením na Darkweb” se zaměřuje zejména na širokou IT analýzu Darkwebu v síti Tor, především pak jejího obsahu a problematiky s ním spojené. Darkweb je velice úzce spjat s internetovou anonymitou, přesněji řečeno, je na ní založen a anonymita na internetu je taktéž velmi žhavé téma poslední doby. Cílem této práce je analyzovat používané technologie a nabízené služby na Darkwebu a jeho skrytých službách, specifikovat anonymitu na internetu, definovat identifikační technologie a způsoby on-line anonymizace. Hlavní část práce se pak věnuje Darkwebu jako takovému, jeho definici a vymezení rozdílů mezi Darkwebem a Deepwebem. Následuje vymezení technologií Darkwebu, účelu, historie a obsahu. Část práce pojednává i o jiných softwarových anonymizačních sítích a systémech, zejména pak klade důraz na projekt The Onion Routing. V závěru se práce věnuje analýze IT služeb a produktů dostupných na Darkwebu anonymizační sítě Tor. Hlavním záměrem práce je pak kvantitativně porovnat zastoupení IT služeb a produktů na Darkwebu této anonymizační sítě. Následně ověřit dostupnost těchto skrytých služeb a kvantitativně analyzovat jejich typové zastoupení. Tyto cíle jsou podpořeny cíli dílčími, mezi které práce uvažuje kvantitativní ověření poměru lokalizací skrytých služeb na Darkwebu, analýzu nabídky IT služeb a produktů na Darkweb marketech či nabídky IT služeb na Darkwebu sítě Tor. Tyto záměry jsou docíleny na základě manuálně vytvořeného data setu se stovkami záznamů jednotlivých skrytých služeb, jež nabízí produkty či služby spojené s tématikou informačních technologií na Darkwebu sítě Tor. Práce následně jako celek přináší čtenáři ucelený a detailní pohled na široké spektrum problematiky týkající se Darkwebu.

Summary

Analysis of the Darknet network with focus to the Tor Darkweb

This master thesis titled “Analysis of the Darknet network with focus to the Darkweb” deals mainly with the IT analysis of the Darkweb in the Tor network. It’s mainly focused to its content and problematics widely connected with the Darkweb. Darkweb is very closely connected with the internet anonymity, more precisely, it’s based on the internet anonymity. The main goal of this master thesis is to analyse used technologies and offered services on Darkweb and its Onion hidden services, to specify internet anonymity, to define identification data and the possible ways of internet anonymization. The main part of this thesis is dedicated to Darkweb, it’s definition and differences between Deepweb and Darkweb. The definition of Darkweb technologies follows also with the purpose, history and content definition. Part of this thesis deals about other software anonymization networks and systems, but mainly it emphasizes on the Onion Routing project. Next part of this publication aims to content analysis of the products and services available on the Darkweb on the Tor anonymization network. The main intention of this work to quantitatively compare the quantity representation of the IT products and services on the Darkweb. Then to verify the availability of these hidden services and to analyze their type representation. These goals are supported by partial goals such as quantitative analysis of language mutations of Onion hidden services on Darkweb, analysis of the IT services and products on Darkweb markets or offer of the IT services on the Darkweb of Tor network. These intensions are achieved based on manually created dataset with hundreds of records of the Tor hidden services which offers IT products or offers related to IT on the Tor Darkweb. The publication brings comprehensive and detailed view of the Tor Darkweb to its reader.

Obsah

1 Úvod

V posledních několika desetiletích se technologie rozvíjí enormním tempem a jinak tomu není ani u IT a všech jeho odvětví. Nicméně stejně tak rychle jako světlé stránky technologií se rozvíjí i ty temnější. Temnější a takové, kde anonymita na internetu je zásadní, neboť kde dochází i k aktivitám takovým, jejichž charakter by většina západní jurisdikce označovala jako protiprávní. Temnější je mnohdy označována i skrytá součást internetu zvaná Darkweb. Tématem této diplomové práce je právě analýza tohoto prostoru, specifikace jeho principů, obsahu a definice oblastí s ním spojených a to zejména se zaměřením na Darkweb v anonymizační síti Tor.

S tímto tématem je úzce spjata i anonymita na internetu. Internetová anonymita je fenoménem dnešní doby. Jak je vidno z běžného používání internetu, čím dál častěji jsme v kyberprostoru nuceni využívat naši pravou identitu, či nějakým způsobem prokazovat některé ze svých osobních údajů. Ať už jde o sociální sítě či internetové obchody, ale i různé online nástroje či prezentační stránky. Je-li řeč o Darkwebu, zde je anonymita absolutní „Alfa omega" celé podstaty věci. Neboť i pro pouhý přístup je uživatel, ve svém vlastním zájmu, nucen učinit několik opatření pro zajištění vlastní anonymity. V práci je anonymita na internetu definována ve spojitosti právě s přístupem do kyberprostoru Darkweb.

Pro přístup na Darkweb a anonymizaci uživatele pak slouží různé postupy a nástroje, které je vhodno i kombinovat. Mezi základní anonymizační software umožňující přístup k Darkwebu patří software Tor (The Onion Routing). Jedná se o internetový prohlížeč, původně navržen a implementován k ochraně vládní komunikace, nyní jednička na trhu anonymizačních softwarů pro prohlížení sítě s více než dvěma miliony aktivních uživatelů. [1] Samozřejmě ne vždy je software využíván k ilegálním aktivitám, často je taktéž využíván například k ochraně soukromí či k zajištění svobody slova. Součástí obsahu práce je právě popis principů práce tohoto anonymizačního softwaru.

Při rešerši tématu bylo zjištěno, že neexistuje, zejména v českém jazyce, velké množství relevantních prací a zdrojů věnujících se tomuto odvětví. Částečně i proto

bylo zvoleno toto téma s cílem analyzovat a vytvořit jasný a ucelený pohled na problematiku moderního Darkwebu a jeho IT služeb a produktů. Práce v žádném případě nenabádá k porušování kybernetických ani jiných zákonů, taktéž neobhajuje nezákonné praktiky v tomto dokumentu zmíněné. Veškeré informace obsažené v této práci jsou určeny primárně ke studijním a výzkumným účelům.

2 Cíl práce

Anonymizační sítě jsou obecně považovány za místo, kam běžný uživatel internetu nechce zavítat, neboť se zde údajně vyskytuje nepřehledné množství ilegálních aktivit, kriminálních služeb, omamných a psychotropních látek a dalších ilegálních či nemorálních služeb a produktů. To je z části pravda. Skutečně je možné takový obsah na tzv. Darkwebu nalézt. Darkweb má ovšem i takové uživatele, jež touží po svobodě slova, anonymitě na internetu a mají tendenci hájit zájmy soukromí uživatele v síti. I takové požadavky mimo jiné anonymizační sítě nabízí. Povaha témat vyskytujících se na skrytých službách těchto sítí je široká. K dispozici jsou služby politických témat, témata týkající se anonymity a soukromí či témata, která lze považovat za plně legální, ale i například služby nájemných vrahů či markety nabízející omamné a psychotropní látky.

Cílem této práce je tuto skutečnost analyzovat a zaměřit se zejména na služby a produkty s povahou IT. Za takové lze považovat veškeré služby nabízející například různé druhy kybernetických útoků, veškeré Darkweb markety, jež nabízí software či jiné digitální produkty, ale případně i fóra věnující se těmto tématům, ať již legálním či nikoliv. Cílem práce je taktéž nabídku těchto služeb zmapovat, analyzovat stav trhu a jeho nabídky, zjistit funkčnost či mutaci vybraných skrytých služeb a definovat popularitu jednotlivých IT služeb na Darkwebu. Práce je zaměřena zejména na Darkweb anonymizační sítě Tor.

Tento cíl je založen na komplexním manuálním sběru dat, a to zejména odkazů na dané webové servery služeb onion, jejich klasifikaci, kategorizaci a na následném statistickém zpracování. Výstupem bude tedy graficky znázorněná analýza poměrů témat jednotlivých IT služeb nabízených na Darkwebu, poměr již neaktivních služeb či jejich jazykové dělení. Vytvořený datový soubor bude součástí práce.

3 Metodika zpracování

Adresy skrytých služeb onion jsou odvozeny od privátního klíče daného webové serveru a zpravidla vypadají jako nesmyslný shluk mnoha písmen a číslic. Díky své složitosti jsou tedy velice obtížně zapamatovatelné. Standardním přístupem k těmto službám tedy bývají tzv. „vstupní body“, za tyto body se považují různé služby a pro každého uživatele mohou být rozdílné. Tyto služby slouží jako jakýsi seznam odkazů na onion služby v anonymizační síti. Adresy těchto vstupních bodů jsou často lehce dostupné a jsou mnohdy k nalezení i na standardním, všem známém internetu.

Na takovýchto seznamech je společně s odkazem na danou službu mnohdy stručně popsán i obsah takových služeb. Služby jsou zpravidla segmentovány dle typu obsahu. Nicméně mnoho z těchto služeb již není funkčních. Gareth Owen ve své publikaci „The Tor Dark Net“ z roku 2015 dokázal, že více než 40 % skrytých služeb na Darkwebu není dostupných déle jak 18 měsíců. [2]

Základním prvkem výzkumu této práce je sběr dat. Smyslem práce není jít do hloubky a sbírat všechny odkazy na skryté služby, ale využít pouze nejznámějších vstupních bodů a nasbírat zejména relevantní data, která na první pohled mohou působit dojmem, že se na nich nachází alespoň nějaké služby či produkty týkající se IT. Tato skutečnost je odvozena zejména z kategorizace odkazu na daném vstupním bodě či z popisu nebo názvu služby. Pro potřeby této práce jsou data získávána ze vstupních bodů Darkwebu.

Z těchto zdrojů jsou sbírány odkazy na skryté služby, ale i jejich název, popis dle daného zdroje, kategorizace dle zdroje a zdroj, odkud daný odkaz pochází. V případě duplicit je ponechán zdroj, na kterém se podařilo službu dohledat dříve. Z důvodu kladení důrazu na relevanci obsahu skrytých služeb k IT jsou jednotlivé záznamy přebírány manuálně, bez využití skriptů či automatizovaných nástrojů.

Po vytvoření dostatečně obsáhlého data setu jsou služby podstoupeny k další analýze. Každý nashromážděný obsah je za pomoci VPN a prohlížeče Tor Browser otevřen. Je zaznamenán datum návštěvy dané služby a její stav, zdali je server dostupný, či nikoliv. Následně je kategorizován obsah těchto služeb, zdali se jedná o službu, market, blog či něco jiného. Kategorizován je následně typ obsahu, zdali se

jedná o software, drogy, hackerské služby, market s různými druhy zboží, elektroniku, aj. Ericsson Marin a spol. ve svém článku „Product Offerings in Malicious Hacker Markets“, kde se zaměřují zejména na analýzu IT obsahu Darkwebu marketů, zmiňují, že nejvíce zastoupenou produktovou kategorií jsou kategorie, týkající se finančnictví. Za takové považujeme odcizené kreditní karty či PayPal účty, falzifikáty bankovek, osobní údaje z kreditních či debetních karet, aj. Tato práce se zaměřuje na širší oblast Darkwebu na síti Tor, nikoliv pouze markety, ale obdobně pouze na produkty IT povahy. [3]

Současně je zaznamenáván i jazyk dané skryté služby a skutečnost, zdali nabízí nějakou službu týkající se IT, či nikoliv. Zajímavým předpokladem je fakt, na který upozorňuje Alex Biryukov a spol. v publikaci „Content and popularity analysis of Tor hidden services“, kde uvádí, že až 84 % obsahu Darkwebu na síti Tor je lokalizováno do anglického jazyka. [4]

V případě nedostupnosti služby se vychází z dostupných informací od daného zdroje. V případě nutnosti registrace na některém z Darkweb marketů i pro nahlédnutí na obsah byly použity vytvořené testovací přihlašovací údaje.

V závěru práce jsou pak data zpracována a sumarizována pro dosažení specifikovaných cílů práce. Jejich podoba je vyjádřena graficky pomocí grafů a tabulek, čímž je zaručeno plné porozumění významu práce.

Nutno zdůraznit, že sbírány byly pouze skryté služby Tor s příponou .onion, neboť na některých ze vstupních bodů lze nalézt i odkazy do standardní sítě internet. Taktéž ze seznamu byly odstraněny duplicity. Metodika sběru dat a jejich následného zpracování je detailněji popsána v kapitole 6.

4 Anonymita na internetu

Stejně tak jako v osobním životě každého člověka má soukromí a anonymita významnou funkci a důležitost i v prostředí internetu. Zvláště v současnosti, v období neuvěřitelně rychle se zdokonalujících technologií je toto téma jedním z hlavních a nejvíce diskutovaných témat světových korporací na trhu informačních technologií. Bylo dokázáno, že mnoho internetových stránek, portálů a služeb, které uživatel navštěvuje, sbírá o uživatelích drobné a útržkovité informace. Tyto informace uživatel poskytuje vědomě či nevědomě a dle toho také mohou mít přímo či nepřímo vypovídající povahu. Poskytne-li tedy uživatel na navštěvovaných stránkách své citlivé údaje, s největší pravděpodobností to dělá vědomě, nicméně, že stránky sbírají o uživateli i data typu IP adresa, čas strávený na stránce, použitý prohlížeč či zařízení, ze kterého uživatel na web přistupuje, a mnoho dalších údajů, již většina uživatelů netuší. Existuje tedy velké množství dat, které lze považovat za nevědomě poskytované údaje. Tyto drobné informace často nemusí mít příliš velkou vypovídající hodnotu, pokud je jich ale o konkrétním uživateli velké množství a v dlouhém časovém intervalu, jejich vypovídající hodnota rapidně roste a je možné se dozvědět mnoho zásadních informací o internetových aktivitách uživatele či o něm samotném. Na území České republiky je stále sběr a nakládání s osobními informacemi zákonně omezen. Nicméně i přesto je to silný zásah do osobního soukromí, a proto možnosti, jak se na internetu anonymizovat, se stále více a více zdokonalují a stávají se oblíbenými a hojněji využívanými nástroji všední práce na počítači.

4.1 Definice anonymity na internetu

Termín anonymita pochází z řeckého slova „anonymia“ a ve volném překladu znamená „bezejmenný“. V běžném použití v dnešní době se termín „anonymita“ používá k popisu situací, kde jméno či identita dané osoby není známa. Některé zdroje uvádí, že definovat anonymitu jako osobu beze jména je nepřesné. Taktéž uvádí, že za anonymní osobu může být považována i osoba, která je neidentifikovatelná, nedosažitelná či nevystopovatelná. [5]

Je-li řeč o anonymitě v kontextu internetu, je důležité zmínit období let 1994-1996, jež se obecně považuje za mezník masového rozšíření internetového připojení do běžných domácností. S tímto vývojem logicky přichází i vývoj softwaru, aplikací a služeb, které poskytují mnohem širší možnosti využití internetového připojení. Tento rozmach přináší i počátek sledování a identifikace uživatelů v síti. Kromě profilu s osobními údaji či údaji, které uživatel dobrovolně na internetových stránkách poskytuje, lze mezi identifikační údaje také zařadit způsoby sledování a identifikace uživatelů v síti internet blíže popsanými v kapitole 4.2.

Anonymitou v prostředí internetu pak rozumíme takové opatření a nastavení softwarových či hardwarových prostředků, jež zajistí nezjistitelnost či falsifikaci těchto údajů, což silně napomůže k vysoké pravděpodobnosti nemožnosti identifikace reálného uživatele či zařízení v síti.

4.2 Identifikační technologie

Identifikačními technologiemi se rozumí takové softwarové prostředky a algoritmy, které díky svým implementacím dokáží do určité míry zaznamenávat některé aktivity a sbírat údaje o uživateli. Takových údajů se pak i za relativně krátký časový úsek může nasbírat obrovské množství a o uživateli mohou mít značně vypovídající hodnotu, což eliminuje anonymitu uživatele. Pro anonymitu uživatele na internetu, je nutno obstarat taková opatření, jež sběr informací a funkcionalitu těchto technologií znemožní. Marek Plevný ve své práci „*Darknet sítě jako způsoby ochrany soukromí uživatele internetu*“ uvádí následující identifikační technologie jako nejrozšířenější: [6]

IP adresa – Základní identifikační údaj každého zařízení připojeného do sítě. Slouží k odlišení síťových rozhraní v síti. Ve verzi IPv4 se jedná o 32bitové číslo. Kvůli nedostatku IPv4 adres byl zaveden protokol IPv6, který reprezentuje 128bitová adresa zapsaná hexadecimálně. Z této adresy lze zjistit například přibližnou pozici zařízení a jméno internetového poskytovatele.

HTTP cookies – Soubory cookies označují malé množství dat, jsou generovány WWW serverem, následně odesílány do prohlížeče, který je poté ukládá do zařízení uživatele. Tyto soubory mohou obsahovat různé informace, nastavení a preference uživatele. Jako například autentizaci či identifikaci uživatele, či uživatelské preference nastavení webové stránky.

Evercookies – Na rozdíl od cookies výše zmíněných jsou uživateli často považovány za nežádoucí. Hlavním rozdílem je pak fakt, že se tyto cookies po jejich smazání opět obnoví, jak již název napovídá. Evercookies jsou využívány zejména pro uložení dat využívaných pro sledování internetové aktivity uživatele, toto ukládání a využívání dat funguje v nezávislosti na použitém webovém prohlížeči. Tato data jsou žádoucí například pro webové analytiky zabývající se analýzou využívání webových serverů.

Browser fingerprinting – Tímto termínem se označuje metoda sběru informací za účelem identifikace uživatele. Na rozdíl od cookies lze za pomoci této metody identifikovat uživatele či zařízení i v případě uživatelem zakázaných cookies

v nastavení prohlížeče. Fingerprinting ukládá informace zejména o použitém prohlížeči, operačním systému, využívaném rozšíření v prohlížeči atp.

Geolokace – Tato metoda zpravidla využívá mix výše uvedených metod. Na základě dat z IP adresy, nastavení jazyka v zařízení, časové zóny či poskytovatele internetu dokáže spolehlivě zjistit přibližnou lokaci uživatele. Nicméně metod na určení lokace jak statických, tak i přenosných zařízení existuje celá řada. Při nevyužívání anonymizačních opatření je tedy zjistitelnost lokace vskutku banální. Například v roce 2014 společnost IBM představila algoritmus, jenž dokáže zjistit polohu uživatele na základě chování a jeho příspěvků na sociálních sítích. [7]

Traffic analysis – Jedna z nejkomplexnějších identifikačních technik. Jedná se o analýzu tekoucích dat mezi serverem a uživatelem. Její podstata spočívá v kombinaci částí jednotlivých již zmíněných technik. I přesto, že je síťový provoz často šifrovaný, ani například protokol HTTPS[1] chráněný pomocí SSL/TLS není proti analýze síťového provozu zcela odolný. [9]

Data jsou obvykle obsažena v tzv. paketu společně s daty, která odesíláme, či přijímáme. Data jsou zpravidla využívána k identifikaci odkud a kam data proudí a zdali skutečně patří nám. Přesto, že data mohou být považována za identifikační, ne vždy jsou zneužívána k nežádoucím aktivitám ze strany poskytovatelů internetových služeb.

[1] HTTPS (Hyper Text Transfer Protocol Secure) je komunikační protokol využívající HTTP společně s TSL či SSL. Využíván zejména při komunikaci prohlížeče s webovým serverem. Dnes běžně využíváno i pro elektronickou poštu, online bankovnictví atp. Využívá asymetrickou kryptografii k identifikaci webových serverů, což je dosaženo pomocí podepsaných certifikátů vydaných certifikačními autoritami. [8]

4.3 Identifikační údaje

Existuje mnoho různých identifikačních údajů, které provozovatel internetových služeb může sbírat a uchovávat. K většině z nich jim zpravidla uživatel dává souhlas registrací či používáním takovýchto služeb. Nicméně přesto existuje velké množství údajů, které samy o sobě nemají konkrétní vypovídající hodnotu, ale pokud jsou spojeny s jinými údaji, jejich vypovídající hodnota může rapidně stoupat. Zákony české republiky definují osobní údaje následovně:

„Osobním údajem je jakákoliv informace týkající se určené nebo určitelné fyzické osoby, k níž se osobní údaje vztahují. Tato se považuje za určenou nebo určitelnou, jestliže lze fyzickou osobu přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro její fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.“ [10]

Úřad pro ochranu osobních údajů ČR poté tyto údaje rozděluje do několika skupin. Adresní a identifikační, citlivé, popisné či údaje o jiné osobě.

Mezi další méně osobní údaje lze zařadit právě ty, které jsou často, ať vědomě či nevědomě uživateli, sbírány internetovými službami, nástroji, sociálními sítěmi, internetovými obchody aj. Mezi takové lze zařadit například.: Stav vztahu, zaměstnání, výše příjmu, rasa, etnická příslušnost, kontakty, konverzace, kalendář, historie vyhledávání, informace o webovém prohlížeči, navštívené internetové stránky, shlédnutá videa, dokumenty, historie nákupů, knihy, hudba, videohry, používaná zařízení či data pro rozeznávání obličeje.

4.4 Cypherpunk

Nedílnou součástí historie spojenou s anonymitou na internetu je tzv. hnutí „Cypherpunk“. Cypherpunk bylo uskupení vznikající v San Francisku kolem roku 1981, tedy nedlouho před vznikem Word Wide Webu. Všechny jeho členy spojovalo jediné, a to nadšení do šifrování a ochrany soukromí. Zlomový byl pro Cypherpunk rok 1992, neboť začal vycházet tzv. „Cypherpunk mailing list“, jenž sloužil k diskuzím o kryptografii a vlivu kryptografie na společnost. Během několika dní tento list získal více než 700 tisíc fanoušků. Jedním z přispěvatelů se stal i Julian Assange, nyní známý jako zakladatel serveru WikiLeaks. Členové hnutí Cypherpunk se zabývali taktéž tvorbou šifrovacích nástrojů, díky čemuž později vydali první kryptoměnu DigiCash, což byl první pokus o nezávislou, digitální, decentralizovanou měnu. Tento pokus se ovšem neshledal s úspěchem. [11]

Jedním z nejdůležitějších softwarových programů pro Cypherpunk byl software PGP od Paula Zimmermana, který Cypherpunk rozšířil mezi další uživatele, a to zejména kvůli jeho jednoduchosti. Tento software, založený na principu asymetrické kryptografie, umožňoval šifrování a podepisování a byl využíván zejména pro šifrování emailové komunikace. [12]

Hnutí Cypherpunk dalo myšlenku, jež se rychle celosvětově rozšířila. Na myšlence od Cypherpunk nyní staví mnoho softwarových vývojářů, jež staví myšlenku anonymity na internetu a anonymní komunikace. Jako příklad z nich lze uvést právě The Tor Project, kterému jsou věnovány další kapitoly v této práci.

4.5 Způsoby anonymizace

Již od éry Cypherpunk a příchodu WWW se softwaroví inženýři zabývají vývojem různých anonymizačních nástrojů a sítí. Tyto softwarové nástroje dokáží uživateli internetu poskytnout určitou anonymitu. Jedním z nejpoužívanějších způsobů anonymizace je právě využití anonymizačních sítí. Výhodou anonymizační sítě je zejména schopnost poskytnout anonymitu jak uživateli, tak cílovému serveru se službou, ke které se uživatel připojuje, i jejímu provozovateli. Obecně řečeno, jedná se o spojení uživatelů v síti, používajících určitý anonymizační software. Tato síť je poté poskytnuta jako komunikační síť pro všechny uživatele v síti. Mezi nejzvučnější zástupce těchto sítí patří zejména Tor, Freenet či I2P. Tyto sítě jsou určeny k obdobnému účelu, ovšem každá z nich funguje na mírně odlišném principu. Detaily těchto služeb jsou popsány v následujících kapitolách. [6]

Kromě anonymizačních sítí existují i nástroje či služby, které poskytují jednostrannou anonymitu zejména koncových uživatelů v síti. Nástrojů, jak ochránit své soukromí, je několik. Některé z těchto nástrojů jsou obecně popsány v dalších kapitolách. Pro dosažení vyšší anonymity je možné některé z těchto služeb a nástrojů kombinovat.

4.5.1 Freenet

Freenet je anonymizační síť založená v březnu roku 2000 vývojářem Ianem Clarkem, hlavním cílem Freenetu bylo umožnit uživatelům sítě jistotu svobody slova. Funguje jako adaptivní síť na P2P[2] architektuře a je poskytována zdarma jako open-source. Obdobně jako ostatní anonymizační sítě poskytuje vysokou míru anonymity jejím uživatelům. Pro prohlížení sítě Freenet je možné využít jakýkoliv z běžně dostupných internetových prohlížečů. [14]

[2] Peer-to-peer (klient-klient) je typ počítačové sítě, kde jsou komunikující strany spojeny napřímo. Oproti síti klient-server, kde klienti vždy komunikují se serverem, přes který komunikují i s ostatními klienty. Architektura P2P nevyužívá serverové služby. Primární výhodou P2P je fakt, že s počtem uživatelů v síti roste i přenosová rychlost, oproti klient-server, kde uživatelé kapacitu serveru dělí. Oproti P2P tedy s počtem uživatelů přenosová rychlost klesá. [13]

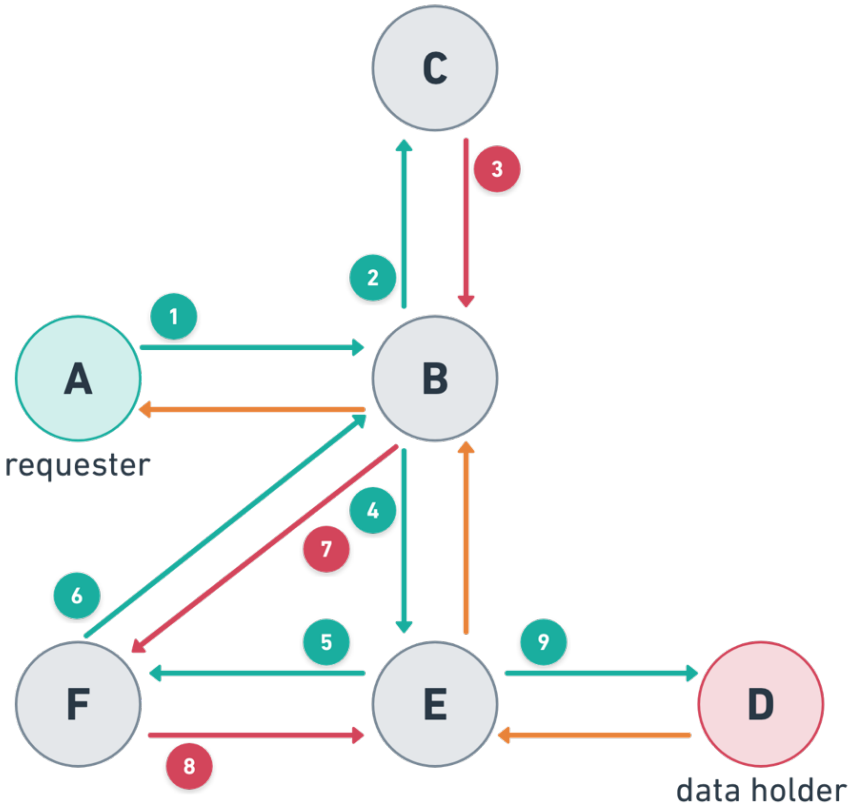
Freenet funguje na principu decentralizovaného anonymního úložiště dat, kde oproti anonymizační síti Tor není třeba mít vlastní server. Síť tedy není závislá na žádném centrálním serveru, neboť každý z počítačů připojených do sítě Freenet sdílí část svého diskového úložiště. Veškerá data nahrávaná do sítě Freenet jsou před nahráním šifrována a rozdělena na části. Tyto jednotlivé části jsou poté nahrány na různé uzly sítě, tedy na disková úložiště jednotlivých uživatelů. Na základě toho poté daný uzel není schopen zjistit, co se u něj v úložišti nachází a není tedy možné ani taková data jakýmkoliv způsobem cenzurovat. V okamžik nahrávání souboru se taktéž data několikrát zreplikují, jejich existenci tedy neohrozí případná nedostupnost či vypnutí některého z uzlů v síti. [15]

Anonymizační síť Freenet neposkytuje kompletní síťovou indexaci domén v síti, neexistuje tedy ani žádný vyhledávač. Společně se sdílením datového úložiště každý uzel obsahuje taktéž dynamickou směrovací tabulku, která obsahuje adresy a šifrovací klíče ostatních známých uzlů v síti. Síť staví na své uživatelské základně. Čím více uživatelů v síti, tím větší datové úložiště a zároveň vyšší úroveň bezpečnosti, neboť jak není možné zjistit původce dat v síti, tak není možné pro daný uzel odhalit, jaká data se nachází na jeho datovém úložišti. [15]

Model funkcionality sítě je tvořen na principu předávání klíčů tak, že žádosti jsou předávány od jednoho uzlu na další přes řetězec požadavků proxy, ve kterém vždy daný uzel rozhodne, kam požadavek zaslat následně. Navržené směrovací algoritmy jsou implementovány tak, aby se daný uzel rozhodoval vždy pouze na základě lokálních, nikoliv globálních, informací o síti. Kvůli zachování anonymity každý uzel zná pouze své přímé sousedy. Každý síťový požadavek obsahuje také tzv. „hops-to-live“ limit. Jedná se o maximální počet přechodů na následující uzel, aby nedocházelo k nekonečným smyčkám a byla eliminována teoretická možnost, že paket nikdy nedorazí do svého cíle. Tento limit se snižuje po každém průchodu uzlem, v případě dosažení nulové hodnoty se paket zahodí. Každému požadavku je taktéž přidělen pseudounikátní identifikační klíč. Tento identifikátor umožňuje uzlu odmítnout požadavek v případě, že ho již v minulosti zpracoval. V takovém případě se požadavek vrací k předchozímu uzlu, který ho následně odešle na jiný uzel. Tímto

opatřením lze předejít nekonečným smyčkám. Cesta konkrétního požadavku končí v cíli či vypršením jeho hops-to-live limitu. [15]

Schéma typického požadavku zobrazuje následující diagram. Kde uzel A je uživatel odesílající požadavek na data v uzlu D. Požadavek je jednotlivými uzly přeposílán dál. Uzel C nemá dalšího přímo připojeného souseda, proto požadavek odesílá zpět. Následně požadavek putuje přes uzly E a F. Poté ho uzel B opět zasílá zpět, neboť tento uzel již požadavek navštívil. Uzel D je pak cílový uzel daného požadavku. Odpověď je následně směrována zpět na uzel A. [16]



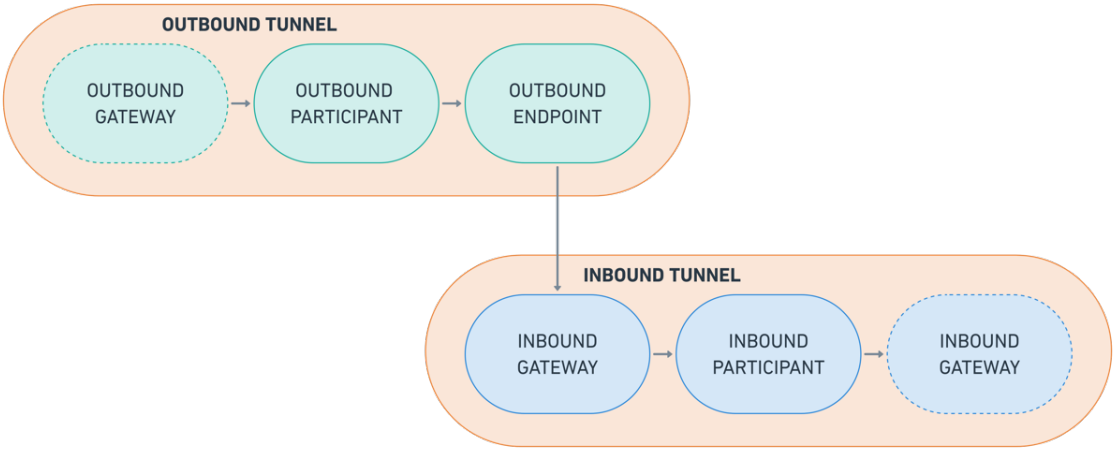
Obrázek 1: Diagram požadavku v síti Freenet [16]

4.5.2 I2P

I2P neboli Invisible Internet Project je P2P překryvná anonymizační počítačová síť, jež anonymizuje interakci uživatelů v síti. Projekt byl poprvé představen v roce 2003, jedná se o podobnou anonymizační síť jako je síť Tor, nabízí množství funkcí jako prohlížení webu, chatování, elektronickou poštu či sdílení souborů. Software pro využití této sítě je open-source. [17]

Přesto, že mnoho vývojářů I2P přešla z vývojářských komunit předchůdců této sítě IIP či Freenet, mají tyto sítě podstatné rozdíly v jejich designu, konceptu a implementaci. Zatímco IIP byla založena na anonymně centralizovaném serveru IRC, I2P je P2P komunikační vrstva navržená pro využití standardních internetových služeb jako je sdílení souborů, chatování, prohlížení webu či provozování těchto služeb. Sama o sobě síť tedy neposkytuje žádné služby, jedná se o nadstavbu TCP/IP určenou pro anonymizaci komunikace. [17]

Pro využití sítě I2P je nutné mít nainstalovanou klientskou aplikaci I2P, která je vývojáři poskytována jako open-source. Každé klientské zařízení s touto aplikací je poté využito jako routovací uzel sítě. Každý uzel má poté několik příchozích a odchozích tunelů. Na rozdíl od sítě Tor je komunikace v síti I2P proto jednosměrná. Odesílá-li klient zprávu adresátovi, odesílá ji přes odchozí tunel s cílem dosáhnout příchozího tunelu adresáta. Každý uživatel v této síti si může zvolit délku těchto tunelů, čímž vybírá kompromis mezi mírou anonymity, latencí a propustností sítě. Tím je docílena vysoká složitost sledování příchozích a odchozích zpráv mezi dvěma subjekty sítě, protože každá ze zpráv jde do cíle po jiné cestě. [18]



Obrázek 2: Diagram I2P tunelové komunikace [18]

I2P využívá tzv. „Garlic routing“, což je nadstavba Onion Routingu využívaného v síti Tor. U Garlic Routingu každá šifrovaná vrstva zprávy může obsahovat více šifrovaných zpráv. Obdobně jako v síti Tor, v I2P neexistuje statický záznam, tedy

routovací tabulka, routerů v síti. Celá síť I2P je postavena nad protokolem UDP, jenž je rozšířen o protokol SSU[3] (Secure Semi-Reliable UDP). Tento protokol v síti slouží zejména pro šifrování a ověřování integrity. [17]

Oficiální stránky projektu I2P porovnávají řešení I2P sítě oproti síti Tor a opačně. Oproti Tor uvádějí mnoho výhod, některé z nich jsou následující: [18]

- Rychlejší skryté služby.
- Dostatečně malá síť na to, aby nebyla zablokována.
- Podpora TCP i UDP.
- Integrovaný mechanismus automatické aktualizace sítě.
- Tunely v I2P mají krátkou životnost, což stěžuje potenciálním útočníkům tunel napadnout.

4.5.3 The Tor Project

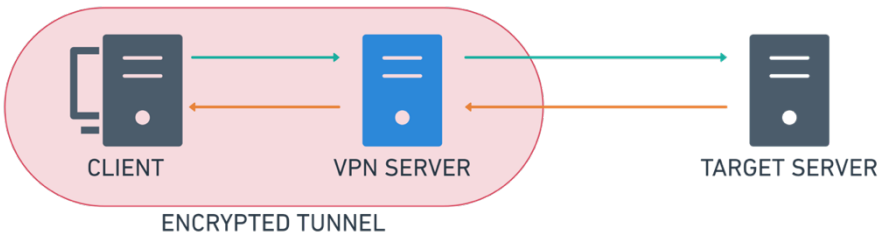
The Tor Project je nezisková organizace spravující jednu z nejrozšířenějších anonymizačních sítí TOR. Jedná se o anonymizační síť založenou na bázi Onion Routingu. Tor je optimalizován pro imunitu proti tzv. „traffic analysis“ útoku a podporuje svobodu a soukromí uživatelů v síti. Síť využívá model klient-server, čímž se liší například od obdobné sítě Freenet. Datový tok od klienta k serveru prochází sítí Tor, čímž je možné zakrýt IP adresu odesílatele i příjemce. Pro připojení k této síti je nutné využít open-source software Tor Browser, díky kterému lze anonymně využívat různé síťové služby jako elektronickou poštu, instant messaging, využívat webová fóra, prohlížet internetové stránky či provádět důvěrné anonymní obchodování. Tor je jedním ze stěžejních témat této práce a je detailněji popsán v dalších kapitolách.

[3] Secure Semi-Reliable UDP je protokol, který funguje na transportní vrstvě a poskytuje zašifrované spojení mezi dvěma I2P routery. SSU je rozšíření UDP protokolu. Obdobně s tímto protokolem I2P využívá NTCP a NTCP2. Nazývá se „semi-reliable“, protože opakovaně přenáší nepotvrzené zprávy do určitého množství opakování. Poté jsou nedoručené zprávy zahozeny. [18]

4.5.4 VPN

VPN (Virtual Private Network) je jedním ze základních prostředků pro ochranu soukromí a zvýšení bezpečnosti na internetu. VPN je hojně využívána společně s anonymizačními sítěmi. Obecně řečeno, VPN je propojení počítačů do zabezpečené soukromé sítě. Mezi klientem a cílovým serverem se vytvoří šifrovaný tunel, skrz který probíhá veškerá datová komunikace. VPN se hojně využívá například i pro potřeby, kdy je nutné se zabezpečeně připojit do místní sítě svého zaměstnání, školy atp. VPN se hodí pro různé využití, jako je například i obejití geolokace, ochrana soukromí, mixování provozu či obejití blokace portů a protokolů. VPN je tedy širší označení, tato práce poodhaluje principy funkcionality VPN pro poskytnutí zabezpečeného připojení s prostředníkem, přes kterého je šifrován veškerý síťový provoz uživatele.

Pro použití VPN je nutné na uživatelském zařízení využít VPN klienta. Pomocí tohoto klienta jsou data již na klientském zařízení zašifrována a následně přes vytvořený tunel přeposlána na vybraný VPN server. Tento server přijatá data rozšifruje a následně přepošle k cílovému serveru. Opačně tomu je při zpětné komunikaci server-klient. Server VPN je tedy jakýsi prostředník mezi komunikací. Díky takovému modelu klient ani cílový server vzájemně neznají svoji IP adresu. Oba znají pouze IP adresu serveru VPN. Cílový server tedy ani neví, odkud je k němu přistupováno.



Obrázek 3: Model komunikace přes VPN [vlastní zpracování][4]

[4] Schéma znázorňuje zjednodušený model komunikace přes VPN server. Komunikace klient – VPN server prochází skrz šifrovaný tunel. Následně VPN server s cílovou službou již komunikuje standardní cestou.

Vhodným doplněním komunikace přes VPN je použití HTTPS protokolu pro zabezpečenou komunikaci. HTTPS je kombinací HTTP a SSL (ev. TSL). Největší výhodou tohoto připojení je ověřování identity cílového webového serveru a šifrování přenášených dat. V případě využití VPN pouze v kombinaci s protokolem HTTP, data jsou šifrována pouze v tunelu mezi klientem a serverem VPN. Od serveru VPN do cílového serveru jsou tedy přenášena bez šifrování. V případě využití HTTPS jsou data šifrována i na cestě od VPN serveru směrem do cílové destinace.

Nevýhodami využití VPN může být například nižší rychlost, vyšší latence či blokace IP adres serverů VPN na cílových serverech. Standardně se mírně sníží rychlost komunikace se serverem, tato rychlost zejména závisí na poskytované rychlosti datových center, jež VPN využívá. Protože při použití VPN každý paket musí projít více uzlů, než dojde do cílové destinace, celková latence se tím zvyšuje až o několik desítek milisekund a to zejména v závislosti na vzdálenosti mezi jednotlivými uzly komunikace. V neposlední řadě je nutné mezi nevýhody zařadit blokace IP adres VPN serverů ze strany cílových služeb. Vzhledem k tomu, že jsou VPN servery často zneužívány k ilegálním či nevhodným aktivitám, cílové servery mnohdy blokují i celé rozsahy IP adres poskytovatelů VPN.

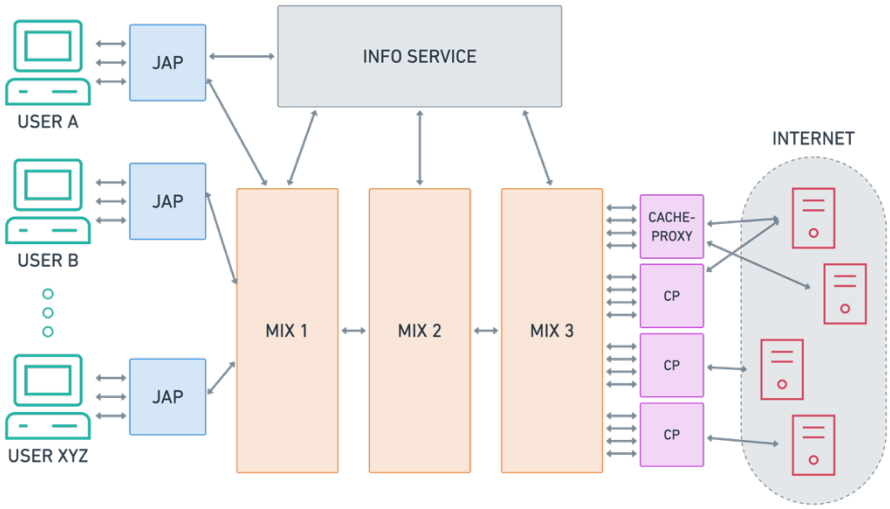
VPN je úzce spojena s tématem Darkwebu, služby Tor a Onion Routingu či s dalšími anonymizačními sítěmi. Obdobně, jako uvádí Paul Syverson ve své publikaci „A Peel of Onion“, je vhodné tyto nástroje kombinovat. Taková kombinace maximalizuje anonymitu i soukromí přístupu k datům Darkwebu a téměř znemožní potenciální identifikaci uživatele. [19]

4.5.5 JAP/JonDo

Java Anon Proxy, také znám pod označením JonDo, je multiplatformní open-source nástroj napsaný v programovacím jazyce Java, určen pro prohlížení webu anonymně. Základ tvoří funkce lokálního proxy serveru. Ten následně zajišťuje spojení s anonymizační sítí. JAP funguje na principu tzv. kaskád, kde kaskáda je samostatná síť poskytovaná nezávislou organizací. Rychlost přenosové komunikace závisí na technologickém vybavení poskytovatele kaskády a na jejím vytížení. Oproti anonymizační síti Tor si uživatel může sám zvolit, jakou kaskádu využije. Zpravidla

tak volí na základě důvěry k danému poskytovateli či referenčnímu systému. Tor je tedy jedna komplexní anonymizační síť, kde každý připojený uživatel může představovat samostatný server. JAP naopak staví na zmíněných kaskádách, na serverech poskytovatele kaskády je veškerá komunikace promíchána, čímž se anonymizuje odesílání paketů. Následně nelze přesně určit, který paket směřuje ke kterému cíli. Bezpečnost se tedy s vytížením sítě zvyšuje na úkor její rychlosti. [20]

Oficiální dokumentace technologie JAP vysvětluje funkcionalitu na následujícím schématu: [20]



Obrázek 4: Diagram funkce technologie JAP [20]

JAP – Klientský software nainstalovaný na zařízení uživatele.

MIX – Anonymizační server, který mixuje datové toky různých uživatelů.

INFO SERVICE – Nezávislá služba, jež poskytuje meta-informace o dostupných mixech (kaskáda), počtu uživatelů a aktuální zátěži mixu.

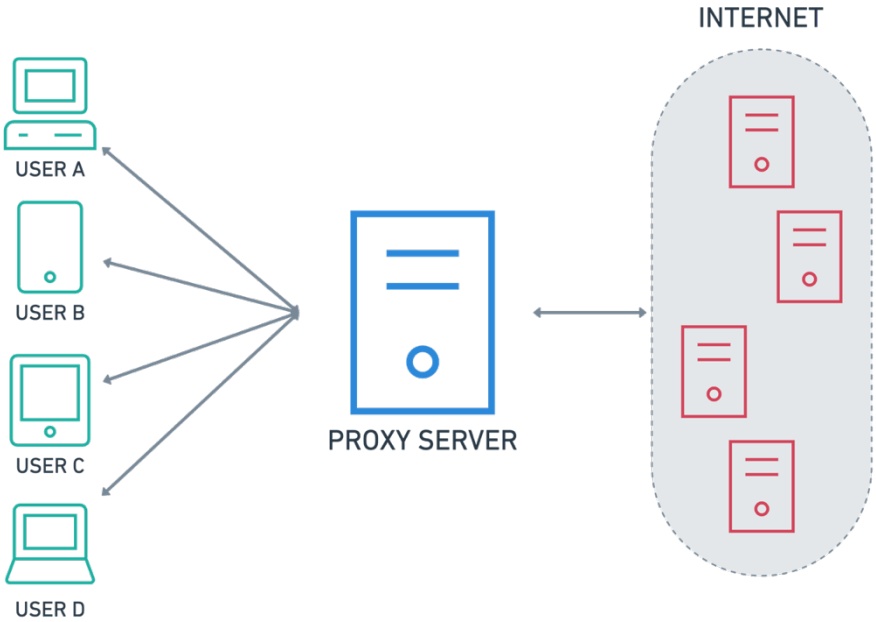
Po spuštění JAP klienta služba ověří aktuálnost aplikace u Info Service, pokud není aktuální, uživatel musí nainstalovat verzi aktuálnější. Pokud není nainstalována nejaktuálnější verze softwaru JAP, služba nemůže být použita. Následně se daný JAP registruje s prvním MIX serverem zvolené kaskády. Síťové spojení zůstává až do odhlášení aktivní. Každý paket od uživatele je odeslán přes JAP, tedy ne přímo do sítě internet. JAP software data zašifruje a odešle na první MIX server, který

následně data zamixuje a odešle na další MIX server v dané kaskádě. Analogicky se paket dostane ke třetímu MIX serveru, který data rozšifruje a pomocí Cache Proxy následně odešle k cíli do sítě internet. Každý MIX server provádí s každým paketem kryptografické operace, takže veškerá data jsou čitelná pouze, pokud prošla správným MIXem ve správném pořadí. Tímto je zajištěno, že potenciální odposlech komunikace přijímá pouze šifrovaná data a není již tedy možné určit odesílatele. [20]

4.5.6 Proxy server

Jedná se o jeden ze základních bezpečnostních a anonymizačních nástrojů. Proxy server funguje jako prostředník v komunikaci mezi uživatelem a cílovým serverem. Proxy server se tváří sám jako klientský počítač komunikující s cílovou službou. Zastupuje hned několik koncových uživatelů a přijatou odpověď od cílové služby opět přeposílá zpět na klienta. Proxy server může mít formu softwaru v uživatelském počítači, případně formu hardwaru, ale obdobně i online služby. Mnoho online služeb poskytující proxy fungují přímo v prohlížeči, kde na stránkách poskytovatele stačí zadat adresu, na kterou se chcete připojit. Poskytovatel následně umožní uživateli anonymně přistupovat k dané adrese bez nutnosti instalace dalšího softwaru či změny síťového nastavení. [21]

Existuje mnoho různých typů proxy serverů, jež se dělí dle jejich typu či účelu použití. Vzhledem ke kontextu této práce je zde pouze zmíněna funkce proxy serveru zejména jako anonymizačního nástroje. Funkce proxy serveru je mnohdy využívána společně s anonymizačními sítěmi, případně jinými doplňujícími službami pro zajištění vyšší míry anonymity. Následující diagram popisuje základní funkcionalitu proxy serveru, kde cílová služba v internetu nezná IP adresu uživatele.



Obrázek 5: Diagram funkce proxy serveru [22]

4.5.7 Proxy chaining

Proxy chaining je nadstavba využití proxy serveru. Jedná se o využití dvou a více proxy serverů na jeden požadavek. Spojení mezi uživatelem a cílovou destinací tedy neprobíhá pouze přes jediného prostředníka, proxy server, ale hned přes několik. V případě využití proxy chainingu pak cílový webserver zná IP adresu pouze posledního využitého proxy serveru. Proxy chaining jako takový neomezuje počet využitých proxy serverů, nicméně s růstem počtu využitých proxy serverů roste i latence a rychlost připojení, ovšem pravděpodobnost vystopování uživatele značně klesá. Každý následující proxy server tedy zná pouze IP adresu jeho předchůdce. V případě, že nějaký proxy server v řetězovém spojení nebude k dispozici, spojení s cílovou službou nemůže být navázáno. Je tedy nutné tento proxy server vyměnit či ho úplně z řetězu odebrat. Pro využití proxy chainingu existují uživatelské softwarové nástroje. Mezi nejznámější patří Proxifier, kde je nutné pouze nakonfigurovat jednotlivé proxy servery k využití. Proxy chaining je taktéž považován za jednu z primitivních, ovšem efektivních metod, jak získat poměrně vysokou anonymitu na internetu jednoduchým způsobem. [23]

4.5.8 TAILS

The Amnestic Incognito Live System, zkráceně TAILS, je live operační systém spustitelný z paměťového média. Tento operační systém je založen na linuxové distribuci Debian s uživatelským prostředím GNOME 2 a zaměřuje se především na soukromí a anonymitu uživatele a zařízení, na kterém je spuštěn. Operační systém byl poprvé zveřejněn v roce 2009. OS TAILS slouží jako ucelený balík anonymizačních a bezpečnostních nástrojů a služeb. Vzhledem k tomu, že je OS bootován „live" na hostitelském zařízení, nezanechává žádné digitální stopy ohledně jeho spuštění či využívání. Pro veškerou síťovou komunikaci využívá síť Tor a používá moderní kryptografické metody pro šifrování souborů, elektronické pošty či IM. TAILS přináší mnoho předinstalovaných uživatelských aplikací jako je například webový prohlížeč, klient elektronické pošty či balík pro kancelářskou práci. [24]

Každý předinstalovaný software v OS TAILS je nakonfigurován pro připojení k internetu zásadně přes síť TOR, v případě, že se aplikace pokusí připojit k internetu napřímo, TAILS tento pokus automaticky zablokuje. Oficiální stránky projektu TAILS vyzdvihují možnost spuštění OS na jakémkoliv počítači, vzhledem k tomu, že je OS vydáván pouze jako „live", využívá tedy pouze RAM a médium, na kterém je OS uložen a ze kterého je spuštěn. Nevyužívá pevné disky počítače, na kterém je spouštěn. TAILS využívá několik kryptografických nástrojů k ochraně dat, například využívá LUKS[5] pro šifrování paměťového média, na kterém je OS uložen. Automaticky používá HTTPS protokol pro šifrování síťové komunikace, OpenPGP[6] pro šifrování a podepisování emailů a dokumentů. Pro šifrování IM využívá

[5] Linux Unifed Key Setup je utilita pro šifrování pevného disku a jiných paměťových médií využívána zejména distribucemi Linux. [25]

[6] OpenPGP je protokol pro šifrování emailové komunikace využívající kryptografii s veřejným klíčem. Protokol definuje standardy formátů pro šifrované zprávy, podpisy, privátní klíče a certifikáty pro výměnu veřejných klíčů. [12]

kryptografický nástroj OTR[7]. Při ukončení OS TAILS využívá technologii Nautilus Wipe, jež kompletně vymaže použité soubory a odstraní veškeré stopy vedoucí k užívání TAILS z hostitelského počítače. [24]

4.5.9 Whonix

Whonix, dříve znám pod označení TorBOX, je operační systém, obdobně jako TAILS, založen na distribuci operačního systému Linux Debian a taktéž se zaměřuje na anonymitu a bezpečnost uživatele. Byl založen v roce 2012 a stejně jako TAILS je stále aktualizován. Ke komunikaci v síti využívá technologii Tor. Největším rozdílem mezi TAILS a Whonix je nemožnost spustit Whonix jako „live" operační systém z paměťového média. Tento operační systém je instalován na hostitelský operační systém jako virtuální OS. Přichází s množstvím předinstalovaných a předkonfigurovaných aplikací. [26]

Operační systém Whonix je založen na principu dvou virtuálních izolovaných částí, a to na část pracovní, zvanou „Workstation", a část síťovou, zvanou „Gateway". Pracovní část je kompletně izolovaná část, která může využívat síťového připojení vytvořeného pouze síťovou bránou. Síťová část je taktéž izolována od zbytku systému a pro veškerou síťovou komunikaci využívá síť Tor. Díky těmto izolacím nemůže například malware[8] běžící v pracovní části způsobit prozrazení IP adresy. Nicméně pro využití Whonix musí uživatel instalovat obě dvě části jako virtuální systém na svém hostitelském operačním systému. [26]

Díky izolovaným částem lze anonymně využívat prakticky všechny aplikace v uživatelském prostředí Whonix. Vzhledem k tomu, že operační systém běží ve virtualizovaném prostředí, aplikace běžící v něm ani neznají reálnou IP adresu zařízení. Obdobně tyto aplikace neznají ani hardware fyzického zařízení, na kterém

[7] Off-the-record messaging je kryptografický protokol pro šifrování IM zpráv. Používá kombinaci symetrické šifry, Diffie-Hellman výměnu klíčů a hashovací funkci SHA-1.

[8] Malware je označení pro jakýkoliv druh počítačového škodlivého softwaru. Tedy softwaru, který je určen k poškození systému, odcizení dat, vniknutí do souborového systému či jiného protiprávního či nemravného jednání. Jedná se nejčastěji o počítačové viry, trojské koně, sledovací software či reklamní software atp.

jsou spuštěny, a nemají přístup k jakýmkoliv prostředkům či aplikacím nainstalovaným v hostitelském operačním systému. Whonix poskytuje taktéž tzv. pokročilou konfiguraci. Tato konfigurace poskytuje dva fyzicky oddělené počítače pro každou část operačního systému Whonix. Síťová část běží na fyzickém hardwaru jednoho z hostitelských počítačů jako instalovaný operační systém. Pracovní část poté běží na druhém počítači, ovšem jako virtualizovaný operační systém. Toto řešení poskytuje ještě znatelně vyšší míru bezpečnosti a anonymity, neboť zamezuje útočníkům dostat se do pracovní částí operačního systému v případě přímého útoku na software, pomocí něhož je pracovní část operačního systému Whonix virtualizována. [26]

4.6 Kvantitativní měření anonymity

Anonymita není absolutní pojem. Anonymita v síti je vždy pouze potenciálně teoretického či pravděpodobného charakteru, neboť i přes množství opatření, zabezpečení a anonymizace, se obecně s technologií anonymizace vyvíjí i možnost potenciálního prolomení anonymity, tudíž odkrytí identity uživatele či zařízení v síti. Na otázku ohledně anonymity v síti tedy není možné jednoznačně odpovědět ano či ne. Existují ovšem metriky, které dokáží sílu anonymity charakterizovat kvantitativním či kvalitativním způsobem. Tyto metriky berou v potaz mnoho různých aspektů působících na sílu anonymity v síti. Kvantitativní a kvalitativní způsoby vyjádření síly anonymity pak dokáží uživatelům naznačit, nikoliv zaručit, míru pravděpodobnosti anonymity v síti. Jako jednu ze základních metrik kvantitativní charakteristiky anonymity lze označit tzv. velikost anonymitní množiny. S tím přímo souvisí i charakteristika anonymity zvaná kvalitativní, tato charakteristika vystihuje odolnost vůči různým druhům kybernetických útoků pro odhalení anonymity. Existuje množství více či méně významných metrik ovlivňující ať již kvantitativní tak i kvalitativní charakteristiku anonymity, nicméně je nutné zdůraznit, že tyto metriky a měření anonymity obecně jsou pouze v rovině teoretické informatiky.

5 Analýza Darkwebu

5.1 Vymezení terminologie

Pro plné pochopení práce v celém svém rozsahu je nutné definovat některé základní pojmy, které se v této části práce odráží a s její problematikou souvisí. Jedná se především o pojmy, které jsou často v neodborných zdrojích mylně zaměňovány či chybně interpretovány. Za nejdůležitější část je považována specifikace pojmů Darkweb a Deepweb (často uváděny i jako Darknet a Deepnet). Právě tyto dva pojmy jsou často mylně zaměňovány, či jejich zásadní významový rozdíl nebývá dostatečně specifikován.

World Wide Web (WWW) – Jedná se o označení pro systém, prohlížení, sdílení a ukládání informací v síti internet, kde informačními datovými zdroji jsou webové stránky identifikovány pomocí URL. Tyto zdroje poté odkazují na další pomocí hypertextových odkazů a jsou přístupné pomocí tzv. prohlížečů. Webové stránky můžou být pak formátovány v tzv. HTML jazyce a jsou uchovávány v počítačích pomocí webového serveru, který odpovídá požadavkům ze zařízení uživatele.

Surface web – Dnešní World Wide Web spojuje obrovské množství internetových stránek. Moderní internetové vyhledávače pak indexují miliardy z nich. Část internetu, resp. jeho obsahu, která je indexovaná a volně přístupná, je nazývána právě jako Surface web. [27]

Deepweb (Deepnet) – Mnoho neodborných zdrojů často chybně zaměňuje význam slov Deepweb a Darkweb, nebo je uvádí jako shodné. Významy obou těchto termínů jsou ovšem zásadně rozdílné. Deepweb lze částečně charakterizovat jako inverzní část sítě internet oproti Surface webu. Většina obsahu World Wide Webu není přímo dostupná a není tedy indexovaná v internetových vyhledávačích. Nejčastěji se jedná o portály, které jsou přístupné pod přihlašovacími údaji, pod určitou IP adresou atp. Tato část WWW se nazývá Deepweb. Deepweb je několikanásobně rozsáhlejší nežli Surface web, některé zdroje uvádí, že Deepweb zabírá 96 % velikosti celého World Wide Webu, 4 % poté tedy indexovaný Surface web. Deepweb jsou tedy i soubory, textové stránky, databáze či další vyhledávači neindexované informace a data. [27]

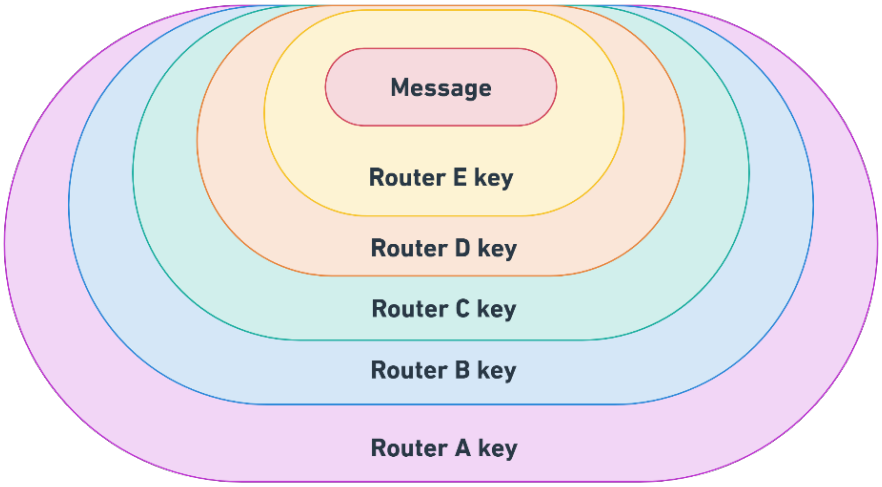
Darkweb (Darknet) – Darkweb je podčást Deepwebu. Největší část Darkwebu zastává anonymní síť Tor, přístupná pomocí specializovaného internetového prohlížeče. Anonymní síť Tor obsahuje přístupné neindexované služby Onion. Funkce těchto služeb je detailněji popsána v následujících kapitolách. Jako Darkweb jsou tedy označovány zejména služby Onion.

5.2 Onion routing

Onion routing jako technika anonymizace síťové komunikace byl navržen v 90. letech minulého století, a to zejména pro utajení interní komunikace v U.S. Naval Research Laboratory armády spojených států amerických, nicméně zanedlouho poté tuto techniku začala využívat i veřejnost. Onion routing (OR) neboli v překladu „Cibulové směrování“ je technika pro soukromou komunikaci dvou síťových aktérů skrz veřejnou síť. Poskytuje anonymní spojení těchto aktérů, jež je silně odolné vůči analýze síťového provozu či explicitnímu odposlechu síťové komunikace. Spojení pomocí onion routingu je anonymní oboustranně, a to téměř v reálném čase. Může být použit kdekoliv, kde lze využít socketovou komunikaci. Tzv. „onion“ je datová struktura, kterou směrovače považují za cílovou adresu daného paketu. Nicméně každá „onion“ struktura se liší u každého navštíveného síťového směrovače. To platí i pro každý jiný síťový prvek, přes který tento paket cestuje. [28] Detaily principů fungování onion routingu jsou konkrétněji popsány v kapitole 5.2.1.

5.2.1 Principy fungování Onion Routingu

Jak bylo uvedeno v předcházejícím odstavci, Onion routing je technika pro anonymizaci síťové komunikace přes internetovou síť. V síti Tor jsou jednotlivé pakety zpráv zapouzdřeny v jednotlivých vrstvách šifrování v aplikační vrstvě komunikačního protokolu. Analogicky k vrstvám cibule, odkud daný termín pochází. Šifrované údaje jsou přenášeny přes sérii několika náhodně vybraných síťových uzlů po celém světě, nazývaných jako „Onion routers“, kde každý uzel tzv. „odloupne“ jednu vrstvu, čímž odhalí další cílové místo dat, kam následně zbývající šifrovaná data předá. Jakmile se dešifruje poslední vrstva, data dorazí do cílového místa určení. Odesílatel i příjemce zůstávají anonymní, neboť každý uzel, přes který paket putuje, zná pouze předchozí a nadcházející uzel. Konečný router poté dešifruje poslední, vnitřní vrstvu šifrování, a odešle data do cíle, bez znalosti zdrojové IP adresy. [28]



Obrázek 6: Diagram vrstev zprávy v Onion routingu[9] [vlastní zpracování]

Autoři technologie Onion Routing M. G. Reed, P. F. Syverson a D. M. Goldschlag v jedné ze svých prvních publikací z roku 1998 věnující se této problematice uvádějí:

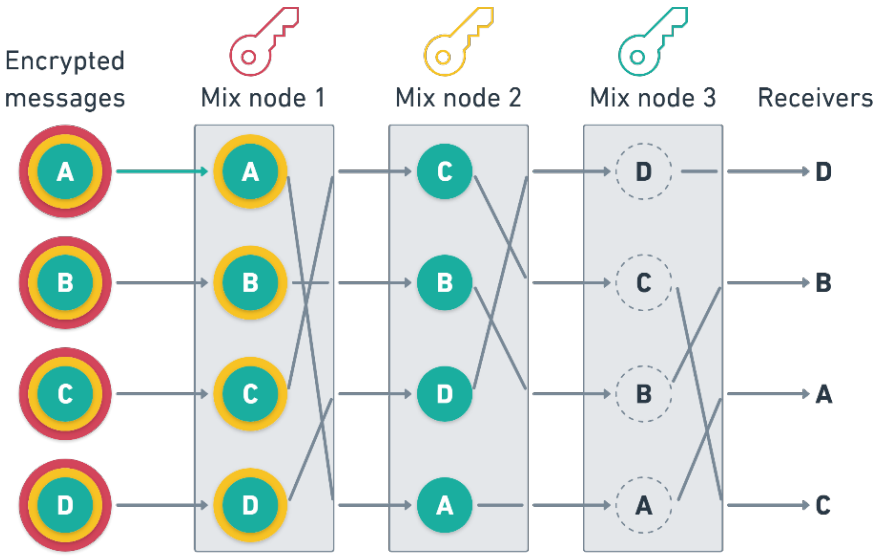
„Communications are intended to be private in the sense that both the public network itself and any eavesdropper on the network cannot determine the contents of messages flowing from Alice and Bob, and she cannot tell that Alice and Bob are communicating with each other.“ [28]

Dle výše uvedených autorů Onion Routingu, taktéž OR klade důraz na anonymitu odesílatele a příjemce zprávy. Přesto, že jsou obě strany schopné vzájemně komunikovat, svoji identitu nejsou navzájem schopni určit. Onion Routing operuje mezi dynamicky vytvořenými spojeními v síti Onion routerů (síťových směrovačů). Funkcionalitou rozšířené směrovače poté autoři nazývají „Mix“. Počítačová síť Mix je detailněji popsána v následujícím odstavci.

[9] Uzel A odstraní šifrovací vrstvu, aby věděl, kam má nadále zprávu zaslat. Daný uzel neví, zdali předchozí je odesilatel či pouze jiný uzel, přes který komunikace přechází. Obdobně to netuší ani o nadcházejícím uzlu. Router B odstraní další vrstvu, nadcházející uzly obdobně. Jakmile se odstraní poslední vrstva, zpráva se dostane do své cílové destinace.

Mix je zařízení typu store-and-forward, které přijímá řadu zpráv s pevnou délkou, provádí kryptografické transformace a poté předává zprávu dalšímu uzlu v dané komunikaci. Tento uzel není předvídatelný z pořadí vstupů. Každá zpráva mezi shodným příjemcem a odesílatelem může tedy jít jinou cestou. Onion Routing zasílá tuto zprávu přes velké množství Mixů, z tohoto důvodu je identifikace příjemce i odesílatele velice složitá. Síť těchto routerů, Mixů, je distribuovaná, odolná proti chybám a pod kontrolou více distribučních domén. Není tedy možné, aby jediný router omezil komunikaci, ohrozil funkcionalitu sítě či soukromí uživatele. Zatímco Onion routery komunikují téměř v reálném čase, Mixy jsou schopni danou zprávu uchovat až po dobu neurčitou a vyčkat, až obdrží odpovídající množství zpráv, které poté, pro větší anonymizaci, mohou zamíchat dohromady. Toto omezení komunikace v reálném čase je značným rozdílem mezi Mixy a klasickými Onion routery. [28]

Mix sítě jsou routovací protokoly založené na řetězci proxy serverů, kde je komunikace velice složitě vystopovatelná. Každý uzel v této síti vyčká, než obdrží určitý počet zpráv, ty poté v náhodném pořadí odešle do následující destinace, tedy do následujícího uzlu. Každá zpráva je pro každý uzel šifrována pomocí veřejného klíče, zpráva je tedy „zaobalena“ do vrstev. Každý proxy server ze zprávy poté odebere jednu vrstvu šifrování, aby zjistil, kam dále zprávu zaslat. Tento koncept byl poprvé popsán Davidem Chaumem v roce 1981. Právě na tomto konceptu je Onion Routing postaven. [29]



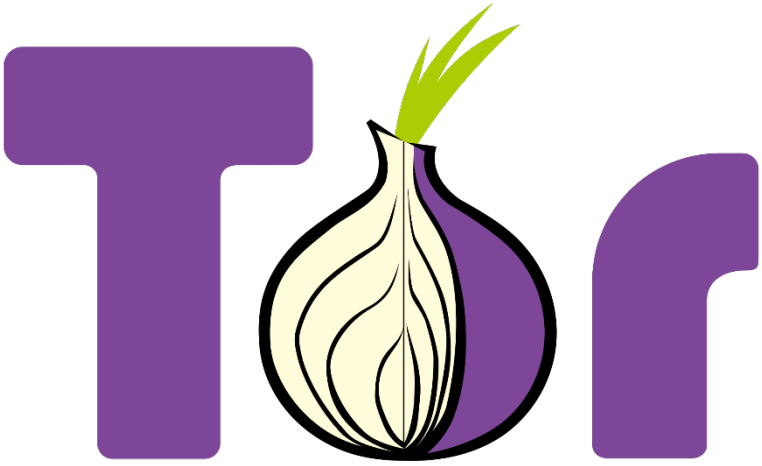
Obrázek 7: Popisný diagram Mix sítě[10] [30]

5.2.2 Tor Browser

Tor Browser je software pro anonymizaci internetové komunikace od organizace The Tor Project, Inc.[11] Častěji znám pod svým nepříliš přesným akronymem Tor, který může mást ve spojitosti s technikou Onion Routing, přesto, že tyto pojmy spolu velice úzce souvisí. Jedná se o jeden z vůbec nejrozšířenějších prohlížečů subdomén .onion. Yasha Levine ve svém článku z roku 2014 uvádí, že většina vývoje softwaru Tor Browser byla financována federální vládou Spojených států amerických. [31]

[10] Zprávy jsou šifrovány sekvencí veřejných klíčů. Každý uzel odstraní jednu vrstvu pomocí vlastního veřejného klíče. Uzel zamíchá zprávy a v náhodném pořadí odesílá na následující uzel. Poslední uzel přepošle zprávy cílovému adresátovi. [30]

[11] Nezisková organizace založena roku 2006 Rogerem Dingledinem a Nickem Mathewsonem ve Spojených státech amerických. Tato organizace stojí za vývojem prohlížeče Tor Browser, na který je taktéž primárně zaměřena. [1]



Obrázek 8: Logo prohlížeče Tor Browser [1]

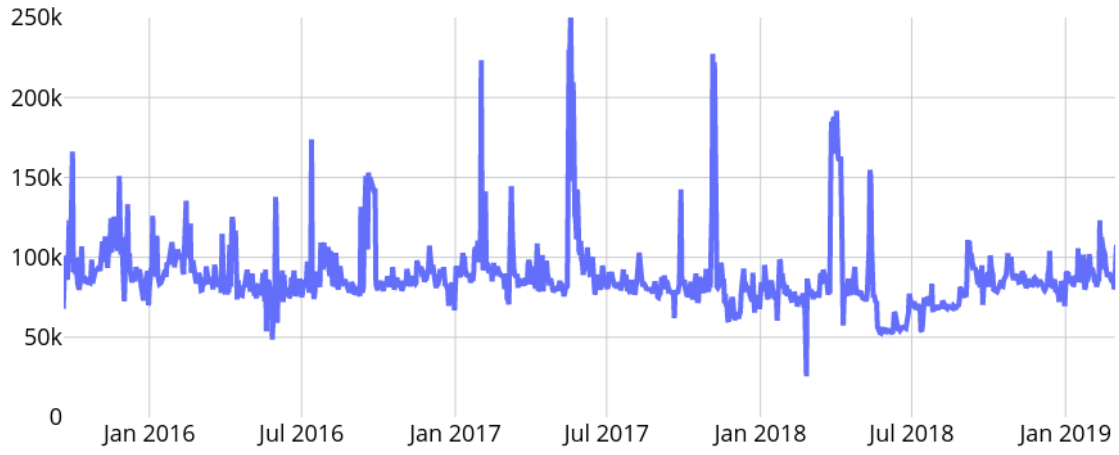
Jedná se o software, internetový prohlížeč, který zajišťuje anonymní pohyb uživatele na internetu. K internetové komunikaci Tor Browser využívá model klient-server, kde uživatel využívá klientskou část a jeho komunikace prochází přes serverovou část složenou z více než šesti tisíc routerů. [32] Tato komunikace skrývá identitu uživatele jako IP adresu a další údaje, na základě kterých by bylo možné uživatele či zařízení v síti identifikovat. Prohlížeč je tedy vhodný k ochraně osobních údajů či soukromí uživatelů, dle tvůrců jeho přidaná hodnota tkví ve svobodném přístupu k informacím. Přesto, že Tor je využíván jako anonymizační software, nedokáže internetové službě skrýt skutečnost, že uživatel k ní přistupuje právě přes prohlížeč Tor. Některé internetové služby omezují funkcionality uživatelům využívajícím prohlížeč Tor Browser. Vzhledem k tomu, že se jedná o open-source software[12], lze ho využívat zdarma.

Tor Browser je bezpochyby jedním z nejrozšířenějších nástrojů založených na Onion Routing principu. Mimo jiné Tor Browser umožňuje i anonymní webhosting. Tor Browser je vhodný i pro komunikaci v reálném čase díky jeho nízké latenci. Původní teoretický koncept, navržený R. Dingledinem a N. Mathewsonem uvažoval

[12] Open-source software je počítačový program s otevřeným zdrojovým kódem, u něhož je obvykle, na základě licence softwaru, uživateli umožněno software upravovat či distribuovat.

každého uživatele v síti Tor jako samostatný komunikační uzel, přes který bylo možné zprávy zasílat. Tor Browser tento koncept vylepšuje a umožňuje uživateli využívat síť Tor bez toho, aniž by jeho zařízení muselo být součástí sítě využito jako komunikační uzel.

Tor Browser je univerzální, volně dostupný internetový prohlížeč, přinášející velmi vysokou míru anonymity uživatele. Tor Browser je schopen zobrazit a pracovat se standardními internetovými službami, ale i se skrytými službami anonymní sítě Tor .onion.



Graf 1: Počet stažení Tor Browser [33]

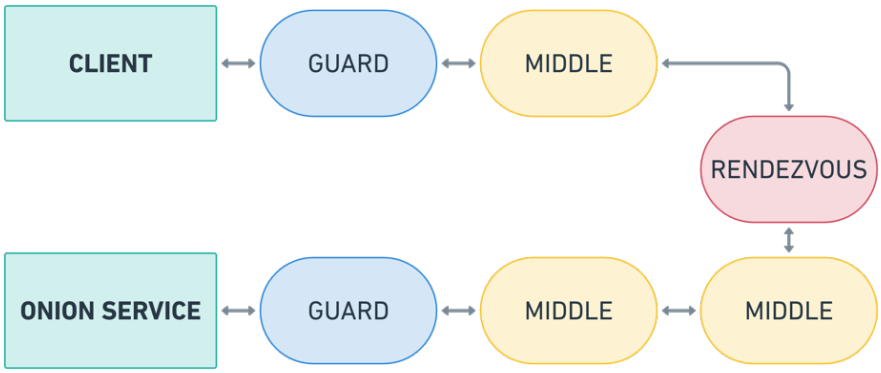
5.2.3 Onion služby

Onion služby, až do roku 2015 nazývány jako „Skryté Onion Služby“, jsou privátní, anonymizované služby v síti Tor s generovaným názvem a pseudo doménou .onion. Přejmenování přišlo s jejich rozšířením a to zejména, aby odrážely fakt, že služby nabízí i „něco více“ nežli pouze skrývání služeb, a to zejména koncové šifrování a anonymizaci. Tyto služby jsou mnohdy taktéž označovány právě jako „Dark web“. V roce 2018 se Onion služby těšily největší slávě, v květnu 2018 jich bylo aktivních přes 120 000. Nyní jich je aktivních zhruba 90 000. [34]

Graf 2: Počet Onion služeb v síti Tor [33]

Označení .onion je generická pseudo doména nejvyššího řádu. Tato pseudo doména se využívá k označení skrytých služeb v síti Tor. Název onion odkazuje na techniku Onion Routing pro anonymní přístup na internet pomocí softwaru Tor. Pro přístup na skrytou službu s příponou .onion se využívá proxy server, klient zašle požadavek na proxy server, který ho přes anonymní síť Tor následně přepošle k uživateli. Tyto adresy bývají obvykle automaticky generovány Tor klientem, skládají se z čísel a písmen tvořících šestnáctiznakový řetězec. Ovšem v roce 2018 společnost The Tor Project spustila novou generace Onion služeb, jejichž doménu tvoří padesáti šesti znakový šifrovaný řetězec obsahující veřejný klíč, kontrolní součet a číslo verze. Nová verze Onion služeb používá nový typ šifrování, mimo jiné zvyšuje zabezpečí a anonymitu těchto služeb, ale ještě více stěžuje čtení a zapamatování již takto složité onion adresy. [34]

Tyto služby jsou založeny na TCP protokolu a jsou přístupné pouze v sítí Tor, tedy skrz prohlížeče, jako je právě Tor Browser. Anonymita těchto služeb je vzájemná, neboť klient nezná server a naopak. Klient k Onion službám přistupuje přes doménu .onion, která je využitelná pouze v síti Tor. Cestu mezi klientem a serverem s Onion službou standardně spojuje cesta, při defaultním nastavení klienta, šesti Tor uzly. Tato cesta je znázorněna v následujícím diagramu:



Obrázek 9: Diagram Tor spojení mezi klientem a Onion službou[13] [34]

5.2.4 Historie TOR

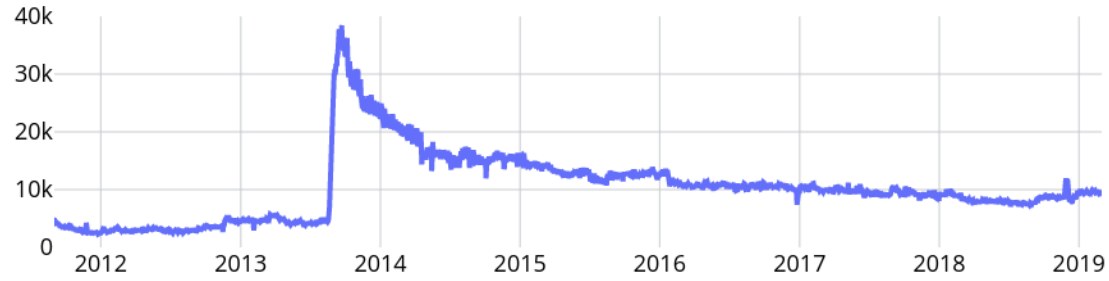
Historie Onion Routingu sahá až do druhé poloviny 90. let minulého století, kde základní koncept a principy cibulového směrování byly představeny v roce 1997 americkou armádou. Následně, roku 2002, byla uvedena první alfa verze softwaru pro cibulové směrování. První veřejná verze pak o dva roky později, ve stejný rok americká armáda vydává software Tor pod otevřenou licencí. V roce 2006 hlavní vývojáři Tor, zakládají neziskovou organizaci The Tor Project, která se zabývá zejména vývojem softwaru Tor. Od tohoto okamžiku popularita Tor enormně stoupá i mezi veřejností a lidmi požadujícími být v síti anonymizováni. V roce 2012 má Tor, zejména software Tor Browser 800 000 uživatelů, dva roky na to dosahuje své největší slávy a software využívá téměř šest miliónů lidí po celém světě. Nyní si software udržuje více než dva miliony aktivních uživatelů. Další ze zlomových roků pro projekt Tor je rok 2018, kde přímo společnost The Tor Project přináší aplikaci Orbot, oficiální Tor prohlížeč pro platformu Android. Nicméně již v roce 2015 společnost Guardian Project představila aplikaci Orfox, které poskytovala prohlížení Tor, skrytých služeb onion, taktéž na platformě Android. Nicméně se nejednalo o

[13] Pomocí tří uzlů klient vytvoří spojení až k tzv. „rendezvous“ uzlu, jenž je považován za místo spojení. Onion služba poté vytvoří spojení ke stejnému uzlu přes uzly dva. Po výsledném spojení ani jeden z aktérů nezná IP adresu toho druhého. [34]

oficiální aplikaci, ovšem společnost The Tor Project tuto aplikaci doporučovala jako vhodné řešení pro uživatele mobilních zařízení platformy Android. [1]

Graf 3: Počet uživatelů v síti Tor [33]

Graf 4 zobrazuje počet uživatelů v síti Tor pocházejících z České republiky. Nutno podotknout, že oproti ostatním státům světa, zejména pak Spojeným státům americkým, jsou uživatelé z České republiky skutečně zanedbatelnou částí uživatelů sítě Tor. Zatímco v České republice se drží denní návštěvnost sítě Tor pod 15 000 přístupů denně, v USA je to kolem 400 000 přístupů každý den. Nejvyšší nárůst denních uživatelů v roce 2014 byl způsobem zejména rapidní změnou smluvních podmínek společnosti Google, jenž začal mnohem více sledovat chování uživatelů internetu. Důsledkem tohoto opatření následně začali uživatelé vyhledávat možnosti anonymizace na síti, proto se jich mnoho přesunulo právě do sítě Tor. Nicméně od té doby má počet denních přístupů spíše klesající tendenci. [33] [35]



Graf 4: Počet uživatelů z ČR v síti Tor [33]

5.2.5 Obsah onion služeb

Darkweb na základě svého obsahu bývá často označován za místo sloužící převážně k online ilegálním aktivitám. Částečně tomu i tak je, vzhledem ke své schopnosti anonymizace je mnohdy k ilegálním účelům využíván. Skutečnost, že Darkweb je opravdu ze své větší části využíván zejména k ilegálním účelům, dokazuje i Gareth Owen z University of Portsmouth ve své publikaci The Tor Dark Net z roku 2015, kde více než šest měsíců analyzoval typ a popularitu onion služeb v síti Darkweb. Dle jeho studie jsou markety na síti Darkweb druhým nejpopulárnějším obsahem. Z jeho dat je zřejmé, že drtivá většina zboží na Darkweb marketech jsou ilegální drogy. [2]

Nicméně obsah sítě Darkweb je rozmanitý. Nejedná se pouze o markety, ale obsahem na Darkwebu může být i fórum, chatovací místnost, souborový server či jakákoliv jiná online služba tak, jak je známa ze sítě internet. Na Darkwebu existují samostatné služby, na kterých lze dohledat odkazy na určité skryté onion služby. Gareth Owen ve své publikaci procházel síť Darkweb a analyzoval typ obsahu. Procházel jednotlivé onion služby, ukládal do databáze část textových informací, na základě kterých následně vyprodukoval list s kategoriemi, které nejvíce pokrývaly obsah dané služby. Owen pouze určoval kategorie obsahu, neurčoval, zdali je daná služba legální, zdali nabízí legální služby či nikoliv. Nicméně přesto v závěru usuzuje, že většina služeb na síti Darkweb je spíše ilegálního charakteru. Owen a jeho tým klasifikoval obsah Darkwebu do následujících kategorií: [2]

Abuse – Sexuální násilí.

Anonymity – Obsah cílený na vzdělávání využití anonymizačních nástrojů.

Bitcoin – Služby poskytující směnu kryptoměn. Praní špinavých peněz.

Blog – Osobní či tematický blog.

Books – Elektronické knihy. Obsah pod autorským právem nabízen zdarma.

Chat – Chatovací místnosti.

Counterfeit – Služby nabízející padělané dokumenty, cestovní pasy či peníze.

Directory – Stránky poskytující odkazy na jiné onion služby.

Drugs – Nákup či prodej narkotik.

Forum – Diskuzní fóra.

Fraud – Obsah zaměřující se na získání peněžního obnosu podvodem.

Gambling – Obsah podporující hazardní hry.

Guns – Stránky zaměřené na prodej zbraní.

Hacking – Stránky poskytující instruktáž hackerství či nabízející hackerské služby.

Hosting – Darkweb webhosting.

Mail – Darkweb emailové služby a klienti.

Market – Darkweb markety prodávající jiné zboží než drogy.

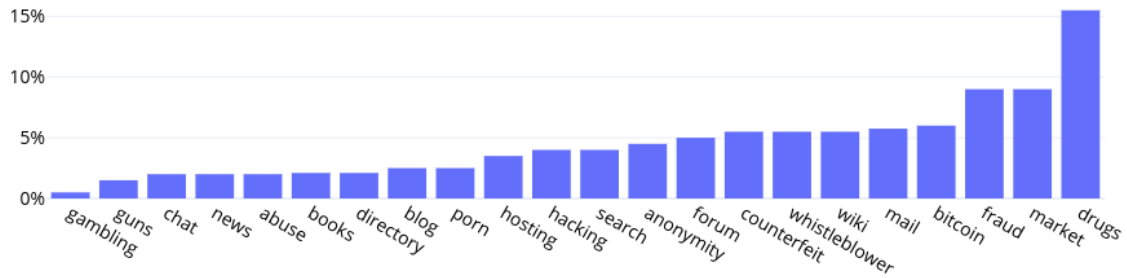
News – Novinky, aktuální události a události týkající se Darkwebu.

Porn – Pornografie, jež by z větší části byla legální dle obvyklé západní jurisdikce.

Search – Služby podporující částečné vyhledávání na Darkwebu.

Whistleblower – Stránky typicky využívané novináři.

Wiki – Obdoba encyklopedie, uživatelsky editovatelný obsah.



Graf 5: Množstevní zastoupení typů obsahu služeb na Darkwebu [2]

Graf 5 znázorňuje procentuální množstevní zastoupení obsahu Darkwebu dle specifikovaných témat. Obsah Darkwebu je různorodý, přesto největší část zmíněných témat dle Owena zaujímají služby s drogovou tematikou. [2]

5.2.6 Slabé stránky onion routingu

Stejně tak jako každý jiný software má i onion routing své slabé stránky. Tyto slabé stránky pramení ze všech zaujatých stran v Tor, ať už jde o slabé stránky ve vývoji softwaru, či o slabé stránky při využívání softwaru. Všechny potenciálně mohou narušit hlavní účel Tor, tedy deanonymizovat uživatele. Taktéž vzhledem k výše zmíněné vyskytující se kriminalitě na Darkwebu, existují instituce, zejména vládní agentury, které mohou mít zájem o deanonymizaci uživatele v síti a jeho co nejpřesnější identifikaci. Proto se ve světě vyskytují studie, pracující na softwarech a kybernetických útocích, které mají za cíl anonymitu v síti Tor narušit či úplně odstranit.

Jedním z typických útoků cílících na znedostupnění uzlu sítě Tor může být tzv. Sniper Attack. Jedná se o DoS[14] útok na jakýkoliv uzel v síti. Tento útok dokáže zahltit operační paměť daného zařízení. Rob Jansen a kolektiv ve své publikaci uvádějí, že při reálném útoku je za pomocí tohoto typu útoku možné docílit výpadku dvaceti nejpoužívanějších uzlů v síti Tor za 29 minut. Tento útok dokáže nejen vyřadit z provozu uzly sítě Tor, ale dokáže i deanonymizovat skrytou službu v síti. Pomocí selektivního DoS útoku je útočník schopen donutit skrytou službu, aby pro komunikaci použila uzel, jenž je pod jeho kontrolou, čímž lze docílit zjištění identity dané skryté služby. [37]

Dalším příkladem útoků v síti Tor může být útok Routing Attacks on Privacy in Tor (RAPTOR). Útok se vyznačuje skutečností, kde útočník sleduje komunikaci na obou stranách sítě. Útočník odchytává jednotlivé pakety, které následně analyzuje. Komparativní analýzou jednotlivých paketů, porovnávání jejich velikostí a časů, dokáže útočník uživatele sítě Tor identifikovat. Útok je zpravidla realizován pomocí

[14] Denial of Service je typ kybernetického útoku, jehož cílem je znedostupnit cílovou službu ostatním uživatelům. Zpravidla je toho docíleno zasíláním množství opakovaných požadavků na danou službu v jeden okamžik, čím nastane pád služby. Rozšířením je pak DDoS, jež spočívá v zapojení několika zařízení k odesílání opakovaných požadavků na službu v jeden okamžik, čímž je DDoS efektivnější. [36]

k tomu určených robotů, kteří síť sledují a analyzují jednotlivé pakety. Mnohdy jsou účastníky v síti Tor zpravidla jako výstupní uzly. [38]

Mezi slabé stránky Tor sítě, specificky pak Tor prohlížeče od společnosti The Tor Project, lze i zařadit síťovou rychlost. Je nutné zdůraznit, že rychlost prohlížení sítě Tor klesá zejména s počtem sériově využitých uzlů, přes které daná informace probíhá. V porovnání pak s klasickými komerčními prohlížeči je rychlost Tor Browser až několikrát pomalejší. Při každé komunikaci zde probíhá šifrování dané zprávy, jež je odesílána právě přes komunikační uzly.

Síť Tor obecně staví na uživatelské základně. Při komunikaci zpráva od příjemce přechází přes několik náhodně vybraných, nezávislých uzlů, než dorazí ke svému příjemci. Čím je více uživatelů v síti, tím je tedy větší pravděpodobnost anonymity daného uživatele v síti. Každý uzel zná vždy pouze své dva sousední uzly, respektive uzly, které daná zpráva navštívila v předešlém kroku, a který uzel zpráva navštíví v kroku následujícím, neboli, kam má daný uzel zprávu přeposlat. Pokud by se teoreticky znal dostatečný počet poskytovatelů jednotlivých uzlů, předaly si informaci o putování zprávy, bylo by možné cestu zprávy vystopovat, tedy vystopovat i příjemce a odesílatele. [1]

Samozřejmě, obdobně jako ve známé síti internet, se lze setkat s mnoha slabými stránkami, které nejsou specifickou záležitostí pro síť Tor. Existuje další množství kybernetických útoků, které lze praktikovat nezávisle na druhu sítě. Za takové lze považovat například Sibyl Attack, DNS Leak, Traffic Analysis atp. V neposlední řadě je také důležité zmínit uživatele v síti. Často se slabým článkem stává právě uživatel sám, neboť může svým neopatrným chováním v síti sám svoji identitu vyzradit a to například zveřejněním svých citlivých údajů. Neposlední součást slabých stránek této sítě lze považovat i nedostatky na straně konfigurace uzlu. Přesto, že konfigurace uzlu pro připojení do sítě Tor je relativně triviální záležitostí a návodů na instalaci připojení lze na internetu nalézt nespočet, konfigurace skryté služby již vyžaduje určité technické znalosti. Při nedostatečné konfiguraci skrytých služeb v síti Tor se uživatel může vystavit riziku snadnější deanonymizaci ze strany útočníka.

6 Kvantitativní analýza nabídky IT služeb a produktů na Darkwebu

6.1 Oblast zkoumání

V předchozí části práce byly popsány principy činnosti jednotlivých anonymizačních sítí jednotlivě provozujících pseudosítě internetu, často označované jako Darkweb. Tato část práce se věnuje analýze obsahu zejména anonymizační sítě Tor. Jednotlivé sítě jsou postaveny na odlišných principech a technologiích. Lze je tedy vzájemně brát jako analogické, nicméně samostatně fungující celky. Přesto, že mají mnoho vlastností i technologických zázemí obdobné, v mnoha aspektech se liší. Porovnávání jednotlivých anonymizačních sítí ovšem není předmětem této práce.

Tato práce se věnuje analýze obsahu zejména anonymizační sítě Tor a jejích skrytých služeb. Srovnáme-li způsob uchovávání obsahu jednotlivých anonymizačních sítí, můžeme nalézt jisté rozdíly. Například Tor, obdobně jako I2P, oproti ostatním sítím uchovávání obsahu neřeší. Alfa omega těchto sítí je anonymizace komunikace a přenosu dat. V síti Tor jsou tedy data vždy uložena jen na jediném místě. Na jediném serveru. Což oproti Freenetu může ústit v nevýhodu. Pokud je tedy daný server odpojen či z nějakého jiného důvodu nedostupný, ani data na serveru nejsou v síti dostupná. Tato skutečnost má následně za důsledek nedostupnost mnoha skrytých služeb, jejichž odkazy jsou na Darkwebu k nalezení. Služby, které jsou přístupné nyní, nemusí být již dostupné zítra, jak tomu i bylo při sběru dat k této práci.

Práce se zaměřuje zejména na kvantitativní analýzu IT služeb a produktů dostupných na Darkwebu v síti Tor. V zájmu této práce není služby analyzovat kvalitativně, testovat a definovat, zdali se jedná o služby skutečné, či o podvodné. Není pochyb, že i takové služby se na Darkwebu nachází. Dle Owena podvodných služeb na Darkwebu může být poměrně velká část, neboť dle jeho studie, více než 40 % pozorovaných skrytých služeb nebylo dostupných déle jak 18 měsíců. [2]

6.1.1 Skryté služby Tor

Skryté služby, neboli služby onion v síti Tor, o nichž detailně hovoří kapitola 5.2.3. společně tvoří obsah Darkwebu. Skrytá služba je vlastně schopnost uživatele hostovat službu v síti Darkweb anonymně. Skryté služby jsou hojně využívány nejen pro hostování nelegálních služeb či marketů, ale i pro hostování fór či politických blogů, ve státech, kde svoboda slova není samozřejmostí a přispěvatelé chtějí zůstat anonymní, bez strachu z postihu. Se schopností anonymizace si velkou slávu skryté služby taktéž získaly díky možnosti provozovat služby, které jsou ilegálně orientovány. Obsah, který by byl dle většiny západních jurisdikcí označen za nelegální, se vyskytuje na skrytých službách skutečně velice hojně. [2]

Skrytých služeb existuje mnoho. Zejména, je-li jejich dělení uvažováno dle anonymizační sítě. Protože anonymizační síť Tor je obecně aktuálně považována za nejrozšířenější, veškerá data analyzované v této práci pocházejí z anonymizační sítě Tor.

6.1.2 Obsah sítě Tor

Anonymizační služba Tor spojuje skryté služby různého typu obsahu. Můžou se zde nacházet běžné webové stránky, ale i komplexnější webové služby. Rozsah sítě Tor je skutečně různorodý. Na Darkwebu se nacházejí i některé služby, které standardně známe ze sítě internet. Darkweb není pouze místo plné nelegálních obchodů či aktivit, mezi služby standardně dostupné přes síť internet i přes síť Tor lze zařadit například službu Facebook.

Dle serveru Tor Metrics se k dubnu 2019 na Darkwebu sítě Tor nachází až 95 000 unikátních adres onion. Mezi tyto adresy se řadí ale i již nefunkční služby, či zrcadlující odkazy na shodnou službu. Největší počet skrytých služeb v síti tor byl zpozorován v prvním čtvrtletí roku 2017 a obdobně i v prvním čtvrtletí roku 2018, kdy se počet unikátních onion odkazů v síti Tor vyšplhal až na 120 000. [33]

Dle studie popsané v kapitole 5.2.2 z roku 2015, kde G. Owen and N. Savage analyzovali témata obsažené na skrytých službách Darkwebu se největšímu zastoupení těší služby a jejich obsah, jenž je spojený s drogami a jinými ilegálními látkami, toto zastoupení, dle Owena, tvoří až 15 % celého obsahu Darkwebu na síti

Tor. Následuje kategorie, kterou Owen nazval „market“ s 9% podílem. Mezi další témata, jež jsou relevantní k této práci lze zařadit například „mail“ s 5% zastoupením, či hacking se 4% zastoupením a v neposlední řadě „hosting“ s 3% zastoupením.

Cath Everett, jež působí jako nezávislá novinářka, ve své publikaci „Should the dark net be taken out?“ z roku 2015 uvádí, s odkazem na členy organizace The Tor Project, že díky schopnosti sítě Tor anonymizovat komunikaci, nikdo přesně neví, kolik služeb, nikoliv odkazů, se v síti nachází. Nicméně přesto odhadují, že něco mezi 1000–1200 a zhruba tři miliony uživatelů. Everett taktéž uvádí, že dle Tima Watsona (Cyber Security Center at Warwick), až 80 % uživatelů Darkwebu, může navštěvovat Darkweb za účelem přístupu či sdílení ilegálních materiálů týkajících se násilí na dětech. [39]

V polovině roku 2016 autoři E. Marin, A. Diab a P. Shakarian vydali publikaci „Product Offerings in Malicious Hacker Markets“, kde během šesti měsíční periody manuálně analyzovali obsah sedmnácti vybraných Darknet marketů, jež nabízejí hackerské a jiné IT služby či produkty. Autoři specifikovali 17 marketů s celkovým počtem 16 122 produktů. Z tohoto počtu produktů autoři definovali 22 kategorií, ke kterým následně kvantitativně produkty přiřazovali. Z jejich výzkumu vyplývá, že největší kvantitativní zastoupení z jejich hlediska má kategorie „carding“ s 1263 produkty. Jedná se o kategorii, do které spadají například falešné kreditní karty, kradené karty, či odcizená čísla kreditních karet atp. Ostatně všechny první tři kategorie, které mají největší kvantitativní zastoupení dle autorů se týkají peněžních služeb či produktů, ať již odcizených PayPal účtů či hotovostních kreditních karet. [3]

6.2 Způsob připojení k Darkwebu na síti Tor

Při připojení a procházení Darkwebu byl kladen důraz zejména na anonymitu a bezpečnost. Nebyly navštěvovány stránky, které neobsahovaly žádný popis a nebylo tudíž možné ani předpokládat, co se na takových skrytých službách nachází. Všechny navštívené skryté služby měly předpoklad výskytu IT služeb či produktů na základě jejich popisu u zdroje, ze kterého k nim bylo přistupováno, či dle názvu, domény nebo dostupného obrázku.

Oproti klasické síti internet, se k Darkwebu na síti Tor není možné připojit prostřednictvím standardních internetových prohlížečů, jako jsou například: Internet Edge, Mozilla Firefox, Google Chrome atp. Pro připojení k této síti je nutné využít speciální software.

Pro zvýšení bezpečnosti a anonymity v síti Tor byla využita komerční VPN služba TunnelBear. Tento software nabízí jednoduché rozhraní pro tunelové připojení do mnoha států světa. Software byl použit ve verzi 3.8.6. Vzhledem k tomu, že tato služba je zdarma pouze pro přenos max. 500 MB, byl využit jejich prémiový plán, jenž je účtován měsíčně a vychází na 9.99 amerických dolarů za měsíc. [40] Na trhu s VPN službami existuje mnoho různých analogických produktů. Služba TunnelBear byla vybrána na základě dvou faktorů. Jednak proto, že ji server techradar.com zařadil mezi deset nejlepších poskytovatelů služeb VPN a taktéž, protože nabízí již zmíněnou zkušební dobu, která je limitována maximálním datovým přenosem. [41]

Pro připojení k síti Tor a následnému sběru dat byl využit nejrozšířenější software Tor Browser verze 8.0.8. Software je detailněji popsán v kapitole 5.2.2. Jedná se o otevřený software, který je poskytován k použití zdarma. Software byl použit na platformě MacOS. [1]

6.3 Sběr dat

6.3.1 Získávání dat

Veškerá data byla získávána ručně, bez využití jakýchkoliv automatizovaných skriptů či nástrojů. Odkazy na skryté služby byly sbírány z tzv. „vstupních bodů“, jedná se o stránky, na kterých se zpravidla nacházejí jednotlivé odkazy ke skrytým službám na Darkwebu v síti Tor. Vstupní body, jež uvádí Tabulka 1, jsou považovány za nejrozšířenější, neboť jsou k nalezení i na některých standardních internetových stránkách, jež se věnují Darkwebu. Detailní informace ohledně těchto statistik jsou k dispozici v přiloženém data setu. Všechny odkazy, které byly pro tuto práci sbírány, byly ještě před samotným navštívením podloženy alespoň jedním z několik faktorů, na základě kterého se dalo předpokládat, že se na daném odkazu skryté služby nalézá obsah relevantní k této práci:

Kategorizace – Některé z uvedených zdrojů jednotlivé odkazy kategorizují. Mezi relevantní kategorie pro sběr odkazů z uvedených zdrojů patří například: Hacking, Software, Technology, Operating system, Market, Hacking forum aj.

Popis – K odkazům obsahujícím jakoukoliv formu popisu bylo přistupováno individuálně. Domníval-li se autor po jeho přečtení, že se na dané skryté službě může nacházet jakýkoliv relevantní obsah pro tuto práci, jenž by se dal analogicky přiřadit k některé z výše uvažovaných kategorií, byl tento odkaz taktéž zaznamenán. V případě opaku nikoliv.

Doménové jméno – Jak bylo již zmíněno, doménová jména skrytých služeb jsou zpravidla tvořena hashem z privátního klíče daného serveru. Obvykle tedy vypadají jako shluk náhodných čísel a písmen. Výjimku částečně tvoří některé služby, jež mají název či klíčové slovo na počátku doménového jména před hashem. Příkladem může být skrytá služba TechShop s doménovým jménem techshop255zo43b.onion.

Název skryté služby – S největší pravděpodobností se jedná o nejvyskytovanější atribut u doménové adresy skryté služby na všech zdrojích, ale zároveň o ten nejméně relevantní. Mnohdy není možné určit typ obsahu pouze z názvu. Tento atribut měl při sběru odkazů tedy nejnižší míru relevance a byl využit pouze

v případě, že jiný atribut se u daného odkazu nevyskytoval. V případě využití se dbalo na relevanci názvu služby k tématu této publikace.

V zájmu experimentu této práce nebylo žádoucí navštěvovat skryté služby Darkwebu, jež obsahují jakoukoliv formu nevhodného či nerelevantního obsahu k této práci. Při následné analýze bylo zjištěno, že ne vždy byl tento předpoklad naplněn a daná služba relevantním obsahem disponovala. Mezi relevantní obsah okruhově patří zejména jakékoliv hackerské či kybernetické služby, ať již legální či nikoliv. Darknet markety nabízející digitální produkty či služby jako jsou například odcizené databáze, odcizené účty k internetovým službám či sociálním sítím, hackerské nástroje nebo pirátský software.

Na základě výše uvedené metodiky sběru odkazů skrytých služeb na Darkwebu, se podařilo získat 323 relevantních odkazů. Společně s těmito odkazy byly tabulkově zaznamenávány i faktory, které k zaznamenání onion adresy vedly. Jedná se o výše uvedenou kategorizaci, popis, doménové jméno či název skryté služby. Zaznamenaná adresa zpravidla obsahovala alespoň jeden tento faktor. Primárním účelem tohoto prvotního filtrování skrytých služeb byl zájem autora vyhnout se možnému navštívení potenciálních skrytých služeb s násilnou a podobně nevhodnou tematikou, jež není relevantní k této studii.

Celkem bylo nalezeno dvanáct vstupních bodů, ze kterých byly odkazy čerpány. V přiloženém data setu jsou odkazy na tyto zdroje k dispozici. Po prozkoumání těchto zdrojů bylo nalezeno 323 odkazů, na kterých se, dle prvotní filtrace, mohly nacházet produkty či služby vztahující se k tématu práce. Vstupní body a počet skrytých služeb z nich převzatých zobrazuje Tabulka 1. V této tabulce je taktéž zahrnuta statistika dostupnosti sebraných skrytých služeb z daného zdroje. Následně byla analyzována každá služba zvlášť. Její dostupnost byla ověřena přístupem na daný odkaz. Z celkového počtu sebraných služeb jich bylo v době přístupu k nim dostupných 53,9 %. Jednotlivé zdroje byly taktéž kategorizovány dle jejich typu následovně:

Informační stránka – Jedná se o rozsáhlé servery, které se věnují problematice Darkwebu. Lze na nich najít mnoho různých informací, relevantních i k jiným anonymizačním sítím, nežli je síť Tor. Tyto servery zpravidla mají i své standardní

internetové stránky umístěné na dobře známé síti internet. Jsou zpravidla legální a neporušují běžné zákony. Mezi takové servery patří například deepweblinks.com.

Vyhledávač – Vyhledávače skrytých služeb onion. Za pomocí vyhledávačů byly doplněny některé odkazy na skryté služby. Slabou stránkou těchto vyhledávačů je fakt, že každý z nich indexuje odlišné skryté služby a to ne zdaleka všechny. Mnoho z nalezených služeb se ve výsledcích mnohokrát opakovalo i při využití jednoho vyhledávače. I při prozkoumání několika stran výsledků jich většina nebyla relevantních.

Seznam odkazů – Typický vstupní bod Darkwebu a zároveň nejspolehlivější zdroj získávání odkazů skrytých služeb. Na zdrojích tohoto typu lze nalézt až několik desítek odkazů. Odkazy jsou zde zpravidla kategorizovány a doplněny o název či popis. Některé z těchto zdrojů jsou pravidelně aktualizovány a nefunkční odkazy jsou odstraněny. Mnohdy případně daný záznam disponuje příznakem, který signalizuje stav neboli dostupnost služby skrývající se pod daným odkazem.

Název	Celkem služeb		Z toho dostupných		Typ zdroje
	Počet	%	Počet	%	
Deep-webLinks	176	54,5 %	73	41,5 %	Information site
DeepWebLink	6	1,9 %	1	16,7 %	
Flashlight	32	9,9 %	9	28,1 %	
Tor66	15	4,6 %	14	93,3 %	Search engine
Ahmia	10	3,1 %	10	100,0 %	
Tordex	21	6,5 %	18	85,7 %	
OnionList	35	10,8 %	24	68,6 %	Links list
Tor Scam List	1	0,3 %	1	100,0 %	
The Hidden Wiki	3	0,9 %	1	33,3 %	
Onion Linkliste	11	3,4 %	11	100,0 %	
DimensionX	3	0,9 %	2	66,7 %	
Russian road	10	3,1 %	10	100,0 %	Links directory
Celkem	**323**	**100,0 %**	**174**	**53,9 %**	

Tabulka 1: Zdroje, převzaté služby a jejich dostupnost [vlastní zpracování]

6.3.2 Kategorizace dat

Po finálním zkompletování seznamu skrytých služeb, relevantních pro výzkumnou činnost této práce, byl každý odkaz jednotlivě navštíven a byla extrahována další data z dané skryté služby. Tato kategorie jednoznačně definuje jednotlivé sloupce

v přiloženém data setu. V případě, že některé hodnoty jsou prázdné, či jsou označena jako „unknown“, nebyla možné tato data dohledat. Mezi možné důvody této skutečnosti může patřit například nedostupnost služby či lokalizace služby do jazyka, jehož znalostí autor nedisponuje atp.

ID – Jednoznačný identifikátor daného záznamu skryté služby. Slouží zejména pro interní účely, ev. pro efektivnější odkaz na konkrétní záznam v data setu.

Date of access – Datum navštívení a analýzy dané skryté služby. V případě opakovaného navštívení byla data včetně data opakovaného přístupu k dané skryté službě aktualizována.

Source link – Onion či standardní doménová adresa zdroje, ze kterého odkaz na danou skrytou službu pochází.

Source name – Název zdroje, ze kterého daný odkaz pochází. Seznam zdrojů reflektuje Tabulka 1.

Source subtitle / type – Podnadpis či typ dané služby pro lepší porozumění typu zdroje.

Content type – Obecný typ dané služby. Jedná se o kategorizaci autorem a to na základě typu služby. Jednomu záznamu v data setu náleží právě jedna kategorie. Kategorizováno bylo dle následujícího konečného seznamu:

- **market** – Darkweb obchod. Obvykle nabízí více druhů či kusů zboží všeho druhu. Analogie ke standardnímu e-shopu. Produkty jsou zde vystaveny obvykle formou jednotlivých položek.
- **service** – Služby všeho druhu, jak digitální, tak fyzické. Jedná se o hackerské, kybernetické či programovací služby, ale i služby poskytující digitální služby jako Git, souborový hosting, emailové či chatovací služby. Do této kategorie spadají i skryté služby nabízející služby nájemných vrahů, padělání peněz či nabízející jiné služby, ať již kriminálního charakteru či nikoliv.
- **blog** – Obvykle osobní blog uživatele či skupiny. Stránka pouze ke čtení. Není možné zde přispívat. Zpravidla vždy zaměřen na konkrétní druh obsahu.

- **other** – Skryté služby, jež nebylo vhodné kategorizovat dle výše uvedených kategorií. Jedná se například o skrytou službu se seznamem kriminálních případů, server s poptávkami po citlivých údajích osob atp.

Content specific type – Jedná se o detailnější kategorizaci autora. Byl stanoven následující seznam konečných kategorií a každému záznamu v data setu byla přiřazena právě jedna kategorie.

- **hacking** – Služby hackerského a kybernetického charakteru. Skryté služby nabízející hackerské služby, odcizení internetových účtů, DDoS útoky, odcizení citlivých údajů, počítačová kriminalita aj.
- **software** – Software, služby či digitální produkty i hackerského charakteru. Pirátské kopie či licenční klíče. Aplikace sloužící k prolomení hesel. Operační systémy, prohlížeče, VPN služby, Git, hostingové služby aj.
- **crimes** – Služby kriminálního a nelegálního charakteru, nespadající pod počítačovou kriminalitu či prodej drog. Jedná se o služby nájemných vrahů, útočníků či teroristů.
- **drugs** – Jedná se zpravidla o fyzické zboží typu omamných a psychotropních látek obvykle dostupných na Darkweb marketech. Jedná se o ilegální zboží.
- **electronics** – Elektronika a hardware. Notebooky, telefony, sluchátka, chytré hodinky atp. Produkty společností jako Apple, Samsung aj.
- **financial** – Finanční služby a produkty. Padělané peníze, odcizené PayPal účty, dárkové karty, šeky, kreditní karty, klonované kreditní a debetní karty či citlivé údaje z nich.
- **guns** – Zbraně a produkty týkající se zbraní. Specializované Darknet markety na zboží tohoto typu.
- **multiple product types** – Podkategorie Darknet marketu. Jedná se o markety, které nejsou zaměřeny na určitý druh zboží, ale nabízejí jich nespočet. Standardně nejznámější místa na Darkwebu.

- **forum** – Standardní fórum, ať již se zaměřením na určité téma či nikoliv. Pro přidávání příspěvků, mnohdy i pro jejich čtení, je nutná registrace. Fórum může částečně působit i jako market. Je možné se na těchto typech skrytých služeb setkat s nabídkou či poptávkou různých služeb a produktů.
- **personal site** – Osobní stránka skupiny či jednotlivce. Nemusí být zaměřena na konkrétní téma. Mnohdy pouze funkční skrytá služba bez větší vypovídající hodnoty.
- **other** – Ostatní služby všeho druhu, jež nebylo možné či vhodné kategorizovat dle specifikovaných kategorií.
- **unknown** – Skryté služby, jejichž kategorizaci se nepodařilo specifikovat. Zpravidla nebyly dostupné, či jejich zdrojový popis nebo doménové jméno nebyly dostatečně vypovídající pro spolehlivé určení jejich obsahu.

Language – Lokalizace, jakou daná skrytá služba disponuje. V případě, že disponuje vícero jazyky vč. anglického, je anglický jazyk uveden jako výchozí. Hodnota „unknown“ reprezentuje neúspěšný pokus o zjištění lokalizace, zejména z důvodu nedostupnosti dané skryté služby.

State – Hodnota nabývá dvou stavů: „alive“ a „dead“, signalizuje dostupnost dané skryté služby v den přístupu na ni.

Site title – Název skryté služby.

Address – Onion doménová adresa skryté služby.

Description (source) – Popis dané skryté služby převzatý ze zdrojového serveru, odkud odkaz na danou skrytou službu pochází.

Offers IT services / products – Hodnota nabývá dvou stavů. „Y“ a „N“, signalizuje, zdali se na dané skryté službě nachází IT služby či produkty. Za IT služby či produkty považujeme následující:

- Software či digitální nástroje všeho druhu. Jeho digitální kopie, licenční klíče, pirátské kopie či návody k jeho použití.
- Hackerské, kybernetické či programovací služby. Osobní stránky nabízející či propagující tyto činnosti.

- Digitální produkty a dokumenty jako databáze, účty k internetovým službám, kradené dokumenty aj.
- Technologie a služby provozující svoji činnost na Darkwebu jako například souborový hosting, Git, emailové či chatovací služby.
- Fóra a blogy věnující se tématům výše zmíněným.
- Darkweb markety obsahující služby či produkty výše zmíněné.

Category – Informativní kategorizace skryté služby ze zdroje odkazu.

Subtitle – V případě, že dané skrytá služba disponuje podtitulkem s jistou informační hodnotou, je ze skryté služby převzat a umístěn do tohoto sloupce.

Notes – Poznámky autora. Mnohdy vztahující se k obsahu dané služby.

Registration necessary – Hodnota nabývá dvou stavů. „Y“ a „N“. Některé služby, zejména Darkweb markety, vyžadují registraci uživatele i pro nahlédnutí do jejich obsahu. V takovém případě byl do služby registrován testovací uživatel a tato skutečnost je v tomto sloupci označena stavem „Y“.

Number of offered services – Jedná se čistě o informativní statistiku, vypovídá o počtu nabízených IT služeb na dané konkrétní skryté službě. Tato statistika vychází čistě z kategorizace v dané službě. Různé služby mohou mít kategorizaci rozdílnou.

6.4 Analýza dat

V této kapitole je představena analýza vytvořeného data setu. Analýza se zaměřuje na kvantitativní zastoupení jednotlivých faktorů zaznamenaných v přiloženém data setu. Analýza popularity obsahu skrytých služeb je v tomto případě klíčová. Vzhledem k tomu, že sběr dat byl již od počátku zaměřen zejména na skryté služby týkající se produktů a služeb IT, předpokládá se, že budou mít největší procentuální konečné zastoupení právě témata taková, jež tématiku IT odráží. Díky tomuto přístupu se předpokládá, že analýza bude taktéž disponovat vypovídající hodnotou, ohledně jednoduchosti získání relevantního odkazu a zároveň důvěryhodnosti zdroje. Během sběru dat se podařilo shromáždit 323 zdánlivě relevantních odkazů na skryté služby v síti Tor, jež byly následně detailně analyzovány.

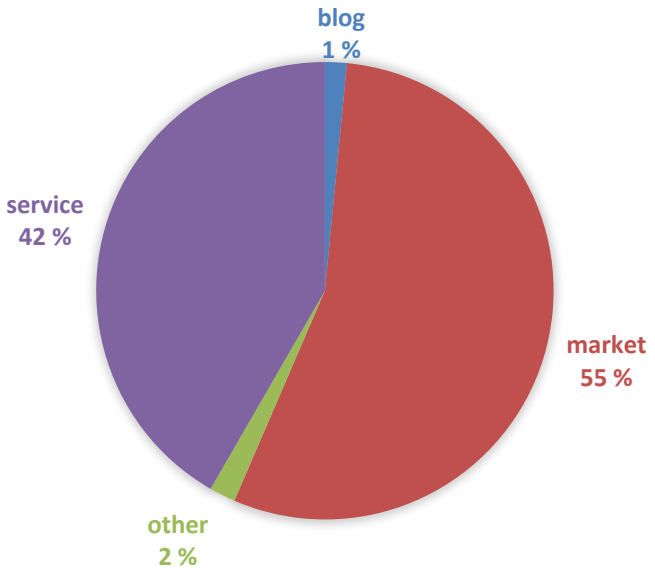
6.4.1 Zastoupení témat obsahu skrytých služeb

Data zastoupení témat zobrazují kvantitativní zastoupení jednotlivých kategorizací v data setu, jež jsou popsána v kapitole 6.3.2. Owen ve své studii, jež disponuje detailnější kategorizací a cílí na širokou škálu skrytých služeb na Darkwebu, uvádí, že skryté služby typu market můžou dosahovat až deseti procent velikosti celého obsahu Darkwebu na síti Tor. Přesto taktéž uvádí tématiku drog, jako nejrozšířenější na celém Darkwebu sítě Tor. Tato tematika dle Owena může dosahovat až šestnácti procent celého rozsahu Darkwebu. [2]

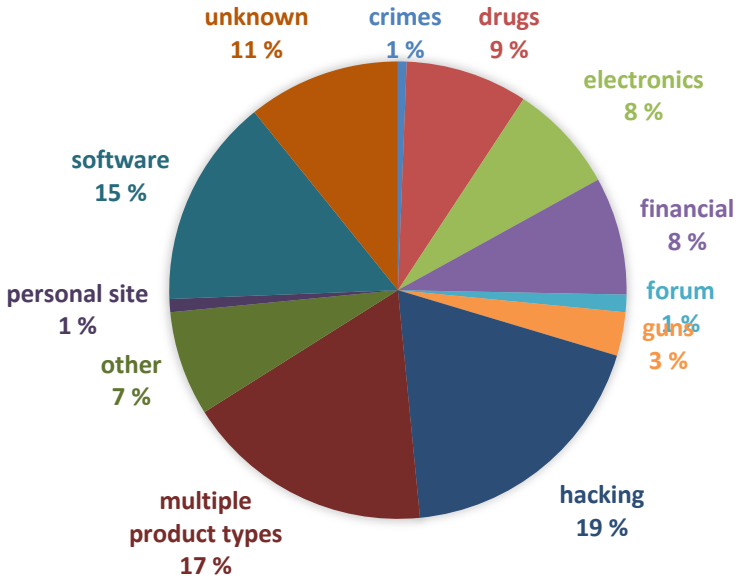
Typ služby	Počet			%	
	dostupné	mrtvé	celkem		z toho dost.
blog	**3**	**2**	**5**	**1,5 %**	**60,0 %**
hacking	1	1	2	0,6 %	50,0 %
other	2		2	0,6 %	100,0 %
software		1	1	0,3 %	
market	**104**	**73**	**177**	**54,8 %**	58,8 %
crimes	1	1	2	0,6 %	50,0 %
drugs	26	2	28	8,7 %	92,9 %
electronics	14	11	25	7,7 %	56,0 %
financial	23	4	27	8,4 %	85,2 %
guns	9	1	10	3,1 %	90,0 %
hacking	4		4	1,2 %	100,0 %
multiple product types	19	37	56	17,3 %	33,9 %
other	3		3	0,9 %	100,0 %
unknown	5	17	22	6,8 %	22,7 %
other	**1**	**5**	**6**	**1,9 %**	**16,7 %**
other	1		1	0,3 %	100,0 %
unknown		5	5	1,5 %	
service	**66**	**69**	**135**	**41,8 %**	**48,9 %**
forum	2	2	4	1,2 %	50,0 %
hacking	27	28	55	17,0 %	49,1 %
other	11	7	18	5,6 %	61,1 %
personal site	2	1	3	0,9 %	66,7 %
software	24	23	47	14,6 %	51,1 %
unknown		8	8	2,5 %	
Celkem	**174**	**149**	**323**		

Tabulka 2: Zastoupení kategorizací skrytých služeb [vlastní zpracování]

Tabulka 2 znázorňuje kvantitativní zastoupení jednotlivých kategorizací skrytých služeb. Následně se zaměřuje na procentuální zastoupení funkčních skrytých služeb v dané kategorizaci a v konkrétní okamžik přístupu k nim. Zajímavou statistikou zůstává fakt, že po Darkweb marketech jsou druhou nejvíce zastoupenou kategorií služby, týkající se hackerské tematiky, jež zaujímají celých 17 % celého vzorku. Následuje zastoupení s kategorizací software se 14% zastoupením. Tyto statistiky, jak již bylo zmíněno, byly předpokladem sběru dat, jež byl zaměřen právě na problematiku IT produktů a služeb na Darkwebu sítě Tor. Oproti tomu primární kategorie market zabírá celých 54,8 % vzorku. Překvapující může být, že více než polovina těchto skrytých služeb byla v okamžiku přístupu funkční. Procentuální zastoupení základní kategorizace skrytých služeb pak graficky znázorňuje Graf 6. Oproti tomu kategorizaci detailnější a její procentuální zastoupení znázorňuje Graf 7.



Graf 6: Primární kategorizace skrytých služeb [vlastní zpracování]

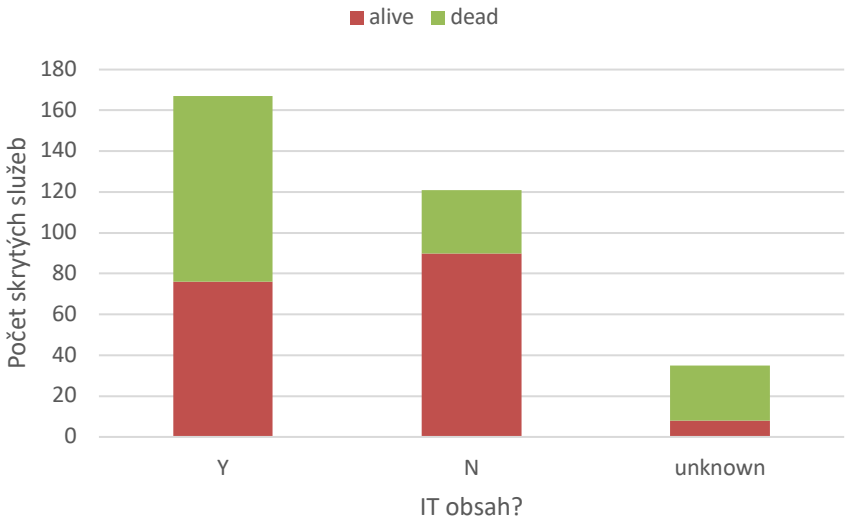


Graf 7: Detailní kategorizace skrytých služeb [vlastní zpracování]

6.4.2 IT obsah skrytých služeb a jejich dostupnost

Kompletní data byla sbírána na základě přístupu jednotlivě, ke každé skryté službě v data setu. Obdobně tomu bylo i při zaznamenávání dostupnosti dané služby. Služba byla označena za nedostupnou v případě, že se k ní i při opakování pokusu o připojení připojit nepodařilo. Opakování proběhlo neprodleně po neúspěšném pokusu o připojení. Služba byla označena za dostupnou v případě úspěšného pokusu o připojení a načtení jejího obsahu. Služba byla označena za dostupnou i v případě, pokud byl její obsah prázdný, nicméně cílový server, na kterém je služba umístěna, byl dostupný.

Ve shodný okamžik byl zaznamenáván i datum přístupu k dané skryté službě. V případě opakovaného přístupu ke skryté službě v pozdější datum byla data upravena a aktualizována dle momentálního stavu. Owen ve zmíněné publikaci uvádí, že během jeho studie v rozmezí 18 měsíců pouze zhruba 5 % skrytých služeb přetrvalo funkčních. Více než polovina vznikla v této periodě a zbytek zanikl. Nicméně faktor persistence není součástí pozorování skrytých služeb v této práci. [2]



Graf 8: IT obsah ve skrytých službách Darkwebu [vlastní zpracování]

Na základě kritérií specifikovaných v kapitole 6.3.2 byl ke každému záznamu v data setu evidován i stav, nabývající hodnot ano / ne / není známo, jenž vypovídá o

obsahu konkrétní skryté služby, zdali se na něm nachází produkty či služby, které uvedená kapitola definuje jako IT. Výše zobrazený graf, Graf 8, znázorňuje zastoupení této statistiky. Vzhledem k metodice sběru dat bylo předpokládáno vysoké zastoupení skrytých služeb v data setu, které skutečně IT obsahem disponují. Tento předpoklad nebyl naplněn. Z celkového vzorku v data setu IT obsahem disponovalo pouze 51,7 % skrytých služeb, dalších 10,8 % nebylo možné z různých důvodů jednoznačně určit. Ze vzorku skrytých služeb, jež IT službami či produkty skutečně disponovaly, jich pak bylo dostupných méně než polovina. Oproti tomu služby, jež tímto obsahem nedisponují, dosahují až 75 % dostupnosti.

6.4.3 Lokalizace skrytých služeb

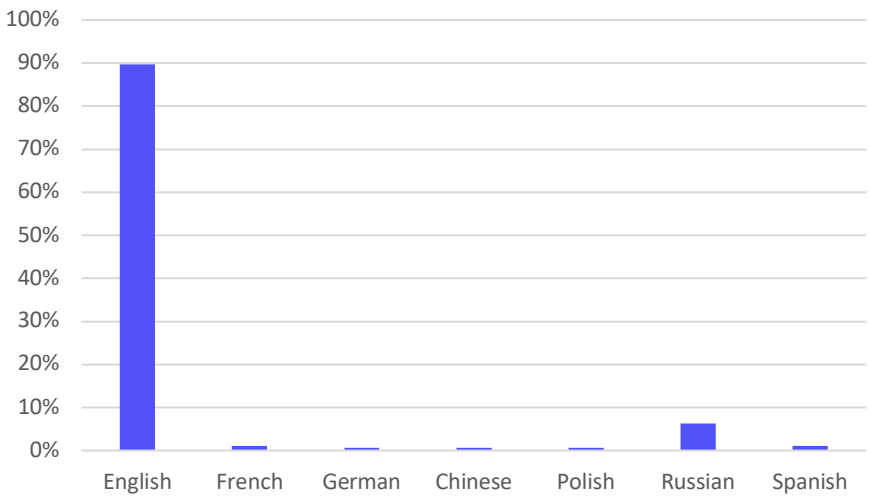
Nedílnou součástí skrytých služeb na Darkwebu sítě Tor je jejich obsahová lokalizace. Přesto, že před přístupem na danou skrytou službu okolnosti mnohdy nasvědčovaly skutečnosti, že obsah služby je lokalizován do anglického jazyka, několikrát tomu tak při analýze nebylo. Z důvodu relevantnosti tohoto experimentu, byla lokalizace zjišťována pouze u funkčních, tedy přístupných, skrytých služeb, u kterých bylo možné lokalizaci spolehlivě určit. Anglický jazyk byl výchozím jazykem, tedy v případě, že skrytá služba byla lokalizována do více jazyků a anglický byl součástí, do data setu byl uveden právě jazyk anglický. V případě, že součástí nebyl, byl zaznamenán jazyk výchozí.

Stát	Průměrná denní návštěvnost	
	počet	%
United States	388035	19,5 %
Russia	284932	14,3 %
Germany	166773	8,4 %
Indonesia	122878	6,2 %
France	99638	5,0 %
United Kingdom	71160	3,6 %
Ukraine	70459	3,5 %
India	62143	3,1 %
Netherlands	51202	2,6 %
Canada	38162	1,9 %

Tabulka 3: Státy s nejvíce uživateli sítě Tor [33]

Portál Tor Metrics, oficiální informační portál projektu The Onion Routing, uvádí průměrnou denní uživatelskou návštěvnost v síti Tor dle států. Tuto návštěvnost k 1. 4. 2019 pro prvních deset států s nejvyšším denním průměrným počtem přístupů zobrazuje Tabulka 3. Nejvíce průměrných denních přístupů náleží uživatelům ze Spojených států amerických, jež dosahují 19,5 % návštěvnosti sítě Tor. Následují uživatelé z Ruska s 14,3 %. Na třetí pozici je Německo, jež zastává 8,4 % všech přístupů k síti Tor. [33]

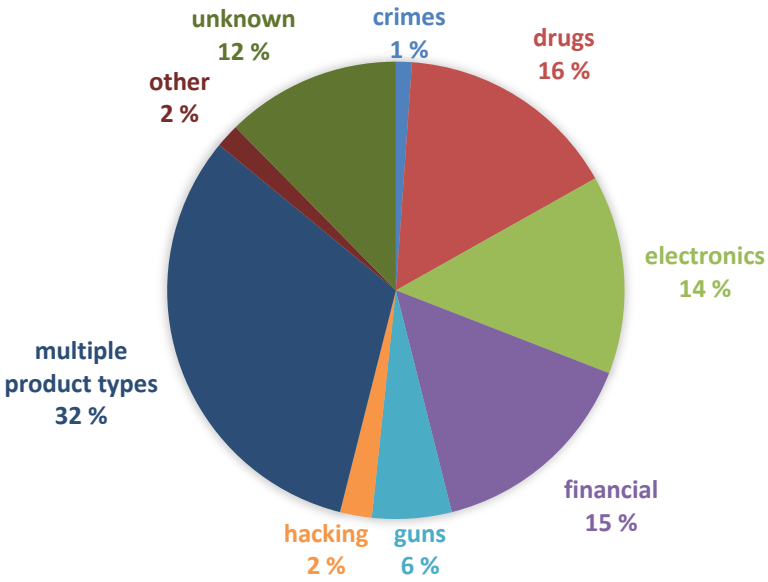
Na základě těchto statistik lze předpokládat, že největší zastoupení testovaných skrytých služeb bude lokalizováno v anglickém jazyce i v testovaném data setu. Obdobně druhým nejvíce zastoupeným jazykem skrytých služeb by měl být jazyk ruský. Mutace byla zjišťována pouze u přístupných skrytých služeb. K dispozici bylo 174 přístupných záznamů. Z analýzy vyplývá, že 156 analyzovaných skrytých služeb, tedy necelých 90 %, bylo skutečně lokalizováno v anglickém jazyce. Následovala lokalizace v jazyce ruském, jenž měl ovšem znatelně nižší zastoupení a to konkrétně 11 skrytých služeb, což je necelých 6,5 % z celého testovaného vzorku. Následovaly další mutace, které tvoří ovšem již relativně zanedbatelné procento testovacího vzorku, neboť se objevovaly nahodile, a bylo jich skutečně minimum. Graf 9 dokazuje splněný předpoklad a zobrazuje konečný seznam vyskytnutých lokalizací skrytých služeb v analyzovaném vzorku a jejich procentuální zastoupení.



Graf 9: Jazyková lokalizace skrytých služeb [vlastní zpracování]

6.4.4 Darkweb markety

Darkweb markety a obchody jim podobné jsou specifickou a velice rozšířenou platformou skrytých služeb v síti Tor. Z celého datového vzorku této práce, jak znázorňuje Graf 6, tvořily Darkweb markety celých 54,8 % celku. Z těchto vzorků bylo v okamžik přístupu dostupných necelých 60 % všech marketů v data setu. Darkweb markety v data setu byly segmentovány dle jejich obsahového zaměření tak, jak je specifikováno v kapitole 6.3.2. Tuto segmentaci znázorňuje Graf 10. Graf bere v potaz všechny Darkweb markety z data setu, aniž by bral v potaz jejich dostupnost. Markety, jež byly v okamžik přístupu nedostupné, byly kategorizovány na základě informací od zdroje, ze kterého odkaz na danou skrytou službu pochází.



Graf 10: Zastoupení zaměření Darkweb marketů [vlastní zpracování]

Marin Ericsson a spol. z Arizona State University, se ve své publikaci z roku 2016 věnují kvantitativní analýze IT služeb a produktů nabízených na marketech sítě Tor. Autoři analyzovali 17 vybraných Darkweb marketů, nabízejících tyto služby a produkty, jež celkově obsahovaly 16122 produktů. Nejpočetněji zastoupenou kategorií, dle Marina, jsou kategorie analogické k „financial“ v této práci, jež v jeho studii obsazují první tři pozice, z celkových 34 dle nejpočetnějšího zastoupení. [3]

Celkové zastoupení jednotlivých zaměření Darkweb marketů zobrazuje Tabulka 4. Tabulka vyjadřuje kvantitativní poměr jednotlivých zaměření marketů, vzhledem

k jejich dostupnosti. Obdobně znázorňuje stav, zdali daná kategorizace marketů nabízí IT služby či produkty, či zdali je pro zobrazení obsahu nutná registrace na marketech v dané kategorizaci. Tyto statistiky tabulka znázorňuje právě v poměru k dostupným marketům v data setu. V případě, že daný market nebyl dostupný, stav nabídky IT služeb či produktů byl uveden na základě informací, jež poskytoval zdroj daného odkazu na skrytou službu marketu. V případě dostupnosti se pak vyhodnocení tohoto parametru řídilo specifikací, jež je uvedena v kapitole 6.3.2. Pokud market nebyl dostupný, či byl lokalizován do jazyka, jehož znalostí autor nedisponuje, stav „nutné registrace“ pro zobrazení obsahu byl označen jako „unknown“. V opačném případě pak byl tento stav označen dle nutnosti registrace i pro zobrazení obsahu daného marketu.

Obsah marketu	Celkem	Dostupné					
		Celkem		Nabízí IT služ. / prod.		Nutná registrace	
		počet	%	počet	%	počet	%
crimes	2	1	50,0 %				
drugs	28	26	92,9 %	1	3,8 %	6	23,1 %
electronics	25	14	56,0 %				
financial	27	23	85,2 %			2	8,7 %
guns	10	9	90,0 %			2	22,2 %
hacking	4	4	100,0 %	4	100,0 %		
multiple product t.	57	20	35,1 %	12	60,0 %	8	40,0 %
other	3	3	100,0 %				
unknown	22	5	22,7 %			1	20,0 %
Celkem	**178**	**105**	**59,0 %**	**17**	**16,2 %**	**19**	**18,1 %**

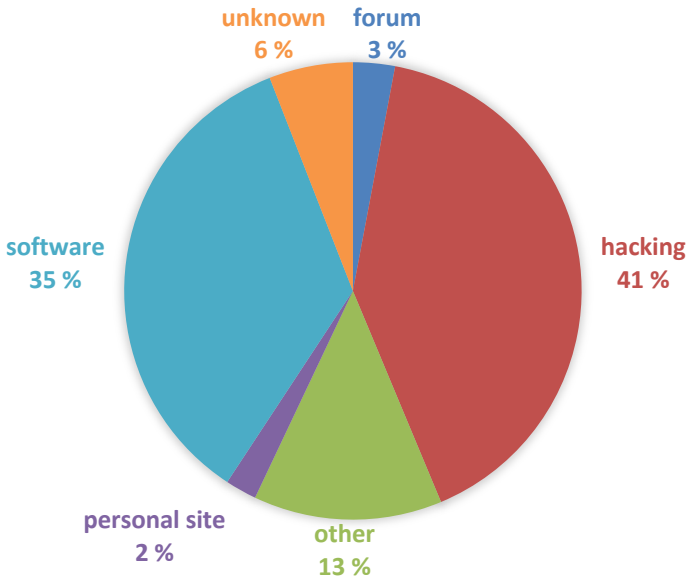
Tabulka 4: Data Darkweb marketů v síti Tor [vlastní zpracování]

Z tabulky vyplývá několik zásadních faktů. Nejvíce Darkweb marketů na síti Tor se nezaměřuje na specifický obsah. Nýbrž nabízí různé druhy zboží, jež dále interně kategorizuje. Takové markety by se vzdáleně daly přirovnat k dnešním standardním e-shopům, jaké známe ze sítě internet. V případě, že Darkweb market disponuje obsahovým zaměřením, v nejvíce případech se jedná o produkty typu omamných a psychotropních, zpravidla ilegálních, látek. Shodné zaměření marketů disponuje i vysokou mírou dostupnosti, jež v testovaném data setu dosáhla 92,9 %. Oproti tomu markety, jež se zaměřují pouze na hackerské služby či produkty, nemají na Darkwebu vysoké zastoupení, nicméně všechny s tímto zaměřením byly v okamžik

přístupu dostupné. Ze všech analyzovaných Darkweb marketů jich bylo dostupných 59 %.

6.4.5 Nabízené služby na Darkwebu

Darkweb na síti Tor nabízí taktéž významné množství služeb, ať již IT povahy či nikoliv. Darkweb disponuje službami legálními, ale i takovými, jež by se daly považovat za nelegální. Služby na Darkwebu, jež jsou definovány v kapitole 6.3.2, zastupují až 42 % všech vzorků v data setu, tuto skutečnost znázorňuje Graf 6. Mnoho služeb je nabízeno i formou produktů na marketech, nicméně takové služby jsou v této práci zpracovány jako součást marketů. Nejvíce významným faktorem v tomto typu obsahu skrytých služeb je zastoupení kategorií označených jako „software“ či „hacking“. Společně takový obsah Darkwebu zaujímá až 76 % ze všech dostupných služeb.



Graf 11: Zastoupení kategorií služeb na Darkwebu [vlastní zpracování]

Z celkového vzorku 135 služeb nabízených na Darkwebu sítě Tor jich bylo v okamžik přístupu dostupných téměř 50 %. Tento fakt již potvrzuje obdobnou statistiku ostatního obsahu Darkwebu uvedenou v předchozích kapitolách, kde se dostupnost skrytých služeb taktéž zpravidla pohybuje okolo poloviny všech testovaných záznamů. Tabulka 5 znázorňuje zastoupení jednotlivých kategorií služeb na Darkwebu a jejich dostupnost. Veškeré služby poskytující, propagující či

distribuující různý druh softwaru zaujímají 35 % všech služeb. Mezi tuto kategorii patří například jak služby typu SaaS, tak i statické informační skryté služby, jež software pouze propagují. Mnoho z navštívených služeb byly legitimní servery propagující různé šifrovací nástroje, šifrovací emailové služby aj. Mnoho z takových služeb na síti Tor jsou analogické k takovým, které jsou dobře známy ze sítě internet.

Kategorizace služby	Celkem		Dostupné	
	počet	%	počet	%
forum	4	2,96 %	2	50,0 %
hacking	55	40,74 %	27	49,1 %
other	18	13,33 %	11	61,1 %
personal site	3	2,22 %	2	66,7 %
software	47	34,81 %	24	51,1 %
unknown	8	5,93 %		
Celkem	**135**	**100,00 %**	**66**	**48,9 %**

Tabulka 5: Zastoupení služeb na Darkwebu [vlastní zpracování]

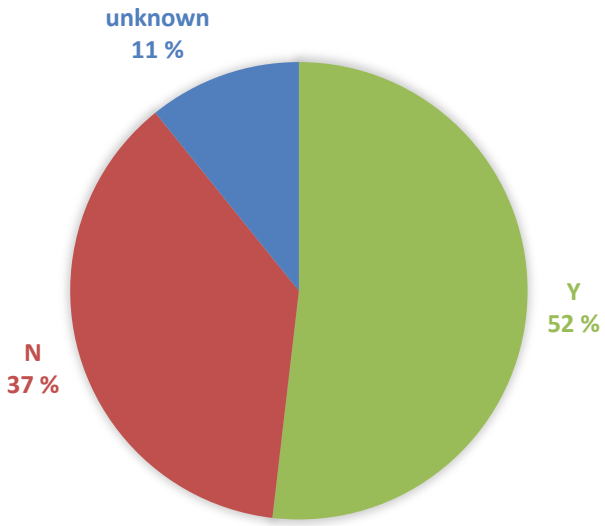
6.5 Shrnutí výsledků

Informační stránky o Darkwebu jako vhodné vstupní body

Tabulka 1 zobrazuje typy zdrojů, ze kterých byly přejímány jednotlivé záznamy v testovaném data setu. Z analýzy vyplývá, že jako nejvhodnější vstupní body pro navštívení Darkwebu se jeví informační stránky věnující se Darkwebu. Příkladem může být server dostupný ze sítě internet za pomocí standardních internetových prohlížečů www.deepweblinks.com, z něhož bylo přejato 176 odkazů na skryté služby sítě Tor, jež se jevily jako relevantní pro tuto práci. Naopak bylo zjištěno, že vyhledávače skrytých služeb v síti Tor nedosahují vysoké relevance výsledků, neboť z těchto zdrojů byla přejata minoritní část data setu. Nicméně přesto důležitým faktem zůstává, že v případě nalezení relevantního výsledku za pomoci vyhledávačů, dosahovaly tyto výsledky vysoké míry dostupnosti. Například z vyhledávače skrytých služeb Tordex bylo přejato 21 relevantních odkazů na skryté služby. Z těchto přejatých odkazů bylo dostupných 18, tedy 85,7 %.

Nespolehlivá kategorizace skrytých služeb od zdrojů odkazů

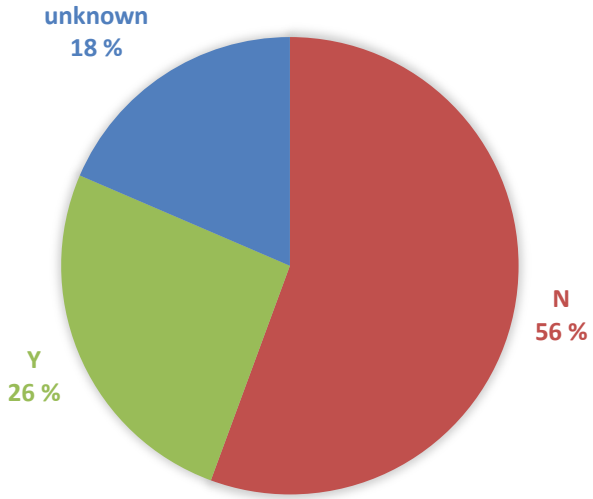
Veškerá data do data setu byla vybírána na základě metodiky specifikované v kapitole 6.3.1. Předpokladem tedy bylo vysoké procento relevance obsahu skrytých služeb zaměřeného či alespoň týkajícího se IT. Tento předpoklad nebyl naplněn. Jak doplňuje Graf 12, skupina skrytých služeb, u nichž byl jejich obsah definován jako IT relevantní, tedy nabízející, propagující či jiným způsobem obsahující IT služby a produkty, zaujímá pouze 52 % celého vzorku. U 11 % všech vzorků nebylo možné tuto skutečnost z různých důvodů definovat. Standardně z důvodu nedostupnosti dané skryté služby v okamžik přístupu, či z důvodu lokalizace stránky do jazyka, jehož znalostí autor nedisponuje.



Graf 12: Skryté služby nabízející IT služby či produkty [vlastní zpracování]

Markety jako majoritní část Darkwebu

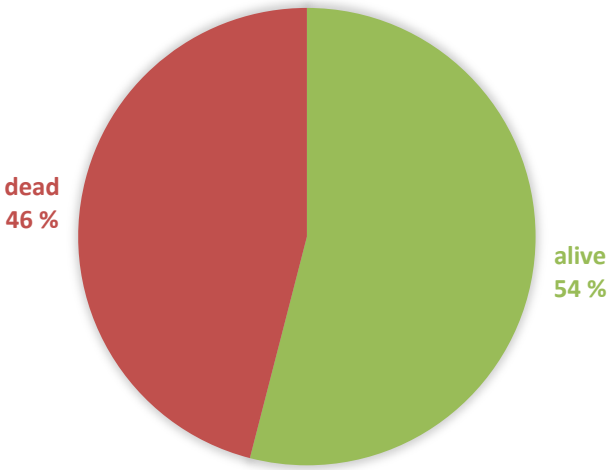
Obsah Darkwebu na síti Tor je obvykle definován velice široce. V případě primární kategorizace definované v kapitole 6.3.2 ale nadpoloviční část celého vzorku zaujímají Darkweb markety. Na skryté služby typu market je možné na Darkwebu tedy narazit běžně. Zpravidla lze i narazit na mnoho odlišných odkazů, jež zdrcadlují na shodný market. V průběhu analýzy a sběru data bylo takových odkazů identifikováno hned několik. Ovšem zrcadlující odkazy nejsou součástí této práce a z data setu byly odstraněny. Poměr Darkweb marketů oproti ostatním primárním kategorizacím znázorňuje Graf 6. Poměr marketů na síti Tor zaujímá 55 % celého sebraného vzorku. Ovšem vzhledem k povaze této práce je důležité zmínit fakt, že pouze 26 % všech marketů v data setu má ve své nabídce služby či produkty definované jako IT v kapitole 6.3.2. Tento fakt znázorňuje Graf 13.



Graf 13: Darkweb markety nabízející IT služby či produkty [vlastní zpracování]

Vysoká míra nedostupnosti skrytých služeb

Na zdrojích všech druhů, ze kterých byla data do data setu čerpána, lze nalézt vysoké procentu odkazů odkazujících na již nedostupné služby. Součástí této analýzy není hledání důvodu, proč tomu tak je, nicméně dle testovaných kritérií se nedostupnost služeb zpravidla pohybuje okolo 50 %. Tuto skutečnost znázorňuje Graf 14. Ze všech testovaných odkazů na skryté služby v data setu jich bylo dostupných pouze 54 %.



Graf 14: Celková dostupnost skrytých služeb v data setu [vlastní zpracování]

Anglický jazyk

Lokalizace skrytých služeb byla dalším z pozorovaných faktorů daného záznamu v data setu. Jazyk, do kterého byla skrytá služba lokalizována, byl zaznamenáván pouze u skrytých služeb, jež byly v okamžik přístupu dostupné, a bylo tedy možné jejich lokalizaci spolehlivě stanovit. O této analýze pojednává kapitola 6.4.3, jež dokazuje, že drtivá většina testovaných skrytých služeb jsou, dle předpokladu, lokalizovány do jazyka anglického. Z celého testovaného vzorku zastoupení služeb lokalizovaných do anglického jazyka zaujímá až 90 %. Následuje jazyk ruský, jež byl lokalizací necelých 7 % celého testovaného vzorku.

Specifikum drogové tématiky na Darkwebu

Přesto, že tato práce nebyla zaměřena na tematiku omamných či psychotropních látek a témat s tím spojených, analýza dokazuje, že se jedná o jedno z nejvíce zastoupených témat obsahu Darkwebu na síti Tor. I vzhledem k metodice sběru dat bylo předpokládáno, že skryté služby specificky se zaměřující na toto téma budou z data setu eliminovány. Nicméně tato problematika je úzce spjata s nespolehlivostí informací získaných, společně s odkazem na danou službu, z uvedených zdrojů těchto dat. Graf 7 dokazuje, že ze všech testovaných záznamů v data setu bylo 9 % specificky zaměřeno právě na drogovou tematiku. Obdobně Graf 10 znázorňuje, že 16 % všech testovaných Darkweb marketů se specificky zaměřuje pouze na produkty, jež lze definovat jako drogy, přesněji omamné či psychotropní látky. Jak uvádí Tabulka 4, u Darkweb marketů s tímto zaměřením dosahovala jejich dostupnost 92,9 % celého vzorku, což lze považovat za dostupnost vysokou, neboť se jedná o hodnotu vysoce nadprůměrnou.

Hackerské služby a software na Darkwebu

Tuto kategorii skutečně nabízených služeb a produktů bylo možné analyzovat ve dvou rovinách. Jednou z nich byly produkty této povahy nabízené na Darkweb marketech a druhou pak služby, jež nabízí služby či produkty této tematiky.

Jedná-li se o Darkweb markety, největší zastoupení mají takové, jež se nezaměřují na konkrétní druh obsahu a nabízejí široký sortiment produktů a služeb. Mezi takovým bývá i tematika spojená se softwarem, digitálními produkty či kybernetickými službami. V tomto případě se jedná až o 32 % data setu. Ze všech Darknet marketů IT služby či produkty nabízí až 26 % testovaného celku, jak znázorňuje Graf 13. V případě specifického zaměření Darknet marketu na hackerské služby se již jedná o minoritní zastoupení, které dosahuje 2 % všech marketů v data setu, což jsou čtyři záznamy data setu. Všechny čtyři tyto skryté služby byly v okamžik testování dostupné.

Záznamy data setu, jež byly typově kategorizovány jako služby, jsou na IT obsah znatelně bohatší. Skryté služby, které nabízí hackerské služby, zaujímají v celém data setu 41 % a služby, které propagují či nabízejí software, zaujímají až 35 %. Tuto skutečnost dokazuje Graf 11. Dostupnost těchto služeb pouze potvrzuje průměrné hodnoty z předchozích poznatků. V případě softwaru se jedná o 51,1 % dostupnosti a v případě hackerských služeb pak 49,1 %. Tyto statistiky podkládá Tabulka 5.

7 Závěry a doporučení

I přes specifické zaměření analýzy Darkwebu na síti Tor výzkum dokazuje, že obsah Darkwebu je velice rozmanitý a variabilní. Při hledání konkrétního obsahu se není vhodné spoléhat na poskytované skryté služby a informace vstupních bodů Darkwebu. Výzkum nebyl zaměřen na identifikaci výskytu ilegálních aktivit na Darkwebu, nicméně i oproti tomuto faktu lze konstatovat skutečnost, že většina navštívených skrytých služeb během analýzy disponovala alespoň částí nabídky služeb či produktů, u nichž lze jejich legálnost přinejmenším zpochybnit, ne-li vyloučit. Za součást rozmanitosti a variability obsahu skrytých služeb v síti Tor lze také považovat dostupnost skrytých služeb. Bylo prokázáno, že jejich dostupnost lze považovat spíše za neuspokojivou, neboť přesto, že vstupní body sítě poskytují množství odkazů a informací ke službám na Darkwebu, mnoho z nich není dostupných. Nedostupnost jednotlivých skrytých služeb na Darkwebu se pohybuje až okolo poloviny všech analyzovaných vzorků. Vstupní body Darkwebu se jeví jako nepříliš často aktualizované.

Při analýze zaměření obsahu jednotlivých skrytých služeb bylo zjištěno, že v případě určitého zaměření dané skryté služby, se ve většině případů jedná o market, jež zaujímá až 55 % testovaného vzorku. Nicméně nutno podotknout, že služby informatického a kybernetického typu lze nalézt pouze na minoritní části těchto marketů. Naopak v případě služeb na Darkwebu z analýzy vyplývá, že služby, jež nabízejí hackerské, programátorské či kybernetické služby, zaujímají až 41 % všech služeb na Darkwebu. Za hackerskými službami následují služby propagující, poskytující či jinak distribuující různé druhy softwaru. Tato tematika zaujímá až 35 % služeb z kategorizace skrytých služeb definovaných jako služby v této práci.

Výzkum dokazuje, že i přes nestabilitu skrytých služeb na Darkwebu, lze nalézt určité množství nabídky IT produktů či služeb. Lze využít hackerských či programátorských služeb, ale obdobně je možné narazit i na značné množství nabídky softwaru, ať již pirátského či legálního, databází a jiných digitálních produktů. Přesto, že pro přístup na Darkweb sítě Tor jsou požadovány určité technické znalosti a zkušenosti a jeho procházení není tak rychlé, jak může být

uživatel z užívání běžného internetu zvyklý, je to vcelku dostupný nástroj, jak se k takovým službám, ať již legálním či nikoliv dostat.

Tato práce neslouží jako návod a nenabádá k užívání nelegálních služeb na Darkwebu. Nenabádá k jakémukoliv protiprávnímu jednání spojeného s touto tematikou. Výzkum byl zaměřen čistě na kvantitativní analýzu IT nabídky na Darkwebu. Kvalitativní analýza nebyla záměrem práce, ani v možnostech autora. Nicméně kvalitativní analýza nabízených IT služeb a produktů na Darkwebu se jeví jako vhodné rozšíření tohoto experimentu. Funkcionalitu a dostupnost nabízených služeb či produktů bez zakoupení není možné ověřit. Obecně tematika Darkwebu je zajímavá a vhodná oblast pro další zkoumání a testování, jež by potenciálně mohlo být realizováno v nějakém z nadcházejících projektů na Fakultě informatiky a managementu Univerzity Hradec Králové.

8 Seznam použitých zkratek

OR	Onion Routing (routovací technologie)
TOR	The Onion Routing (software)
IP	IP adresa
I2P	Invisible Internet Project (anonymizační síť)
P2P	Peer-to-peer (typ počítačové sítě)
VPN	Virtual Private Network
HTTP	Hyper Text Transfer Protocol
HTTPS	HTTP Secure
WWW	World Wide Web
SSL	Secure Sockets Layer (protokol)
TLS	Transport Layer Security (kryptografický protokol)
TCP	Transmission Control Protocol
URL	Uniform Resource Locator
PGP	Pretty Good Privacy
IIP	Invisible IP
TCP/IP	Transmission Controll Protocol / Internet Protocol
UDP	User Datagram Protocol
IRC	Internet Relay Chat
SSU	Secure Semi-Reliable UDP
OS	Operační Systém
IM	Instant Messaging
LUKS	Linux Unified Key Setup
PGP	Pretty Good Privacy
DoS	Denial of Service
DDoS	Distributed Denial of Service
HTML	Hyper Text Markup Language
SaaS	Software as a Service

9 Seznam použitých zdrojů

[1] The Tor Project Inc, „The Tor Project". [Online]. Dostupné z: https://www.torproject.org/.

[2] G. Owen a N. Savage, „The Tor Dark Net", zář. 2015.

[3] E. Marin, A. Diab, a P. Shakarian, „Product offerings in malicious hacker markets", in *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, 2016, s. 187–189.

[4] A. Biryukov, I. Pustogarov, F. Thill, a R. Weinmann, „Content and Popularity Analysis of Tor Hidden Services", in *2014 IEEE 34th International Conference on Distributed Computing Systems Workshops (ICDCSW)*, 2014, s. 188–193.

[5] K. A. Wallace, „Anonymity", *Ethics and Information Technology*, roč. 1, č. 1, s. 21–31, bře. 1999.

[6] M. Plevný, „Darknet sítě jako způsob ochrany soukromí uživatelů internetu - VŠKP - VŠE". [Online]. Dostupné z: https://vskp.vse.cz/68651_darknet_site_jako_zpusob_ochrany_soukromi_uzivatelu_internetu.

[7] J. Mahmud, J. Nichols, a C. Drews, „Where Is This Tweet From? Inferring Home Locations of Twitter Users", s. 4.

[8] Z. Durumeric, J. Kasten, M. Bailey, a J. A. Halderman, „Analysis of the HTTPS Certificate Ecosystem", in *Proceedings of the 2013 Conference on Internet Measurement Conference*, New York, NY, USA, 2013, s. 291–304.

[9] P. Schamberger, „Anonymita v prostředí internetu". [Online]. Dostupné z: https://is.cuni.cz/webapps/zzp/detail/137279/.

[10] ČR, „101/2000 Sb. Zákon o ochraně osobních údajů", *Zákony pro lidi*. [Online]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-101.

[11] S. Falkon, „Cypherpunks and the rise of cryptocurrencies", *The Startup*, 25-lis-2017.

[12] „OpenPGP", *OpenPGP*, 15-úno-2019. [Online]. Dostupné z:

https://www.openpgp.org/about/history/.

[13] R. Schollmeier, „A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications", in *Proceedings First International Conference on Peer-to-Peer Computing*, 2001, s. 101–102.

[14] „Freenet - official website". [Online]. Dostupné z: https://freenetproject.org/author/freenet-project-inc.html.

[15] I. Clarke, O. Sandberg, B. Wiley, a T. W. Hong, „Freenet: A Distributed Anonymous Information Storage and Retrieval System", in *Designing Privacy Enhancing Technologies: International Workshop on Design Issues in Anonymity and Unobservability Berkeley, CA, USA, July 25–26, 2000 Proceedings*, H. Federrath, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, s. 46–66.

[16] „Freenet", *Wikipedia*. 17-bře-2019.

[17] M. Ehlert, *I2P Usability vs. Tor Usability A Bandwidth and Latency Comparison*. .

[18] „Invisible Internet Project - Official website". [Online]. Dostupné z: https://geti2p.net/en/about/intro.

[19] P. Syverson, „A Peel of Onion", in *Proceedings of the 27th Annual Computer Security Applications Conference*, New York, NY, USA, 2011, s. 123–137.

[20] „JAP - Official website", *JAP - Anonymity and Privacy*. [Online]. Dostupné z: https://anon.inf.tu-dresden.de/index_en.html.

[21] „Proxy.org - The Proxy Authority". [Online]. Dostupné z: https://proxy.org/.

[22] „What is a Proxy Server? Benefits, Types, Implementations and Security", *Hide IP Proxy*, 18-dub-2018. .

[23] „Proxy Chaining", *Infosec Resources*, 24-srp-2015. [Online]. Dostupné z: https://resources.infosecinstitute.com/proxy-chaining/.

[24] „Tails - Official website", *Tails - about*. [Online]. Dostupné z: https://tails.boum.org/about/index.en.html.

[25] „Cryptsetup and LUKS", *GitLab*. [Online]. Dostupné z: https://gitlab.com/cryptsetup/cryptsetup.

[26] „Whonix". [Online]. Dostupné z: https://www.whonix.org/.

[27] B. He, M. Patel, Z. Zhang, a K. Chen-Chuan Chang, „Accessing the deep Web: A survey", *ResearchGate*. [Online]. Dostupné z: https://www.researchgate.net/publication/220425814_Accessing_the_deep_Web_A_survey.

[28] M. G. Reed, P. F. Syverson, a D. M. Goldschlag, „Anonymous connections and onion routing", *IEEE Journal on Selected Areas in Communications*, roč. 16, č. 4, s. 482–494, kvě. 1998.

[29] C. Bettini, S. Jajodia, P. Samarati, a S. X. Wang, *Privacy in Location-Based Applications: Research Issues and Emerging Trends*. Springer Science & Business Media, 2009.

[30] „Mix network", *Wikipedia*. 16-led-2019.

[31] Y. Levine, „Almost Everyone Involved in Developing Tor was (or is) Funded by the US Government", *Pando.com*, 16-čvc-2014. [Online]. Dostupné z: https://pando.com/2014/07/16/tor-spooks/.

[32] „TorStatus - Tor Network Status". [Online]. Dostupné z: http://torstatus.blutmagie.de/.

[33] „Tor Metrics". [Online]. Dostupné z: https://metrics.torproject.org/.

[34] P. Winter, A. Edmundson, L. M. Roberts, A. Dutkowska-Żuk, M. Chetty, a N. Feamster, „How Do Tor Users Interact With Onion Services?", prezentováno v 27th {USENIX} Security Symposium ({USENIX} Security 18), 2018, s. 411–428.

[35] „Odvrácená strana internetu: český Darknet v číslech", *Česko v datech*. [Online]. Dostupné z: https://www.ceskovdatech.cz/clanek/28-odvracena-strana-internetu-cesky-darknet-v-cislech/.

[36] „WWW Security FAQ: Securing Against Denial of Service Attacks". [Online]. Dostupné z: https://www.w3.org/Security/Faq/wwwsf6.html.

[37] R. Jansen, F. Tschorsch, A. Johnson, a B. Scheuermann, „The Sniper Attack: Anonymously Deanonymizing and Disabling the Tor Network", OFFICE OF NAVAL RESEARCH ARLINGTON VA, úno. 2014.

[38] Y. Sun *et al.*, „{RAPTOR}: Routing Attacks on Privacy in Tor", prezentováno v 24th {USENIX} Security Symposium ({USENIX} Security 15), 2015, s. 271–286.

[39] C. Everett, „Should the dark net be taken out?", *Network Security*, roč. 2015, č. 3, s. 10–13, bře. 2015.

[40] „TunnelBear: Secure VPN Service", *TunnelBear: Secure VPN Service*. [Online]. Dostupné z: https://www.tunnelbear.com/.

[41] A. M. a day ago VPN, „The best VPN service 2019", *TechRadar*. [Online]. Dostupné z: https://www.techradar.com/vpn/best-vpn.

10 Seznam obrázků

11 Seznam tabulek

12 Seznam grafů

Univerzita Hradec Králové
Fakulta informatiky a managementu
Akademický rok: 2017/2018

Studijní program: Aplikovaná informatika
Forma: Prezenční
Obor/komb.: Aplikovaná informatika (ai2-p)

Podklad pro zadání DIPLOMOVÉ práce studenta

PŘEDKLÁDÁ:	ADRESA	OSOBNÍ ČÍSLO
Bc. Dědek Jindřich	Hornická 594, Rtyně v Podkrkonoší	I1600282

TÉMA ČESKY:

Analýza P2P sítě Darknet se zaměřením na Darkweb

TÉMA ANGLICKY:

Analysis of Darknet P2P network

VEDOUCÍ PRÁCE:

Ing. Vladimír Soběslav, Ph.D. - KIT

ZÁSADY PRO VYPRACOVÁNÍ:

Diplomová práce by se měla zabývat specifikací a analýzou P2P sítí typu Darknet z IT pohledu. Užší zaměření by měla mít na WWW obsah Darkwebu. V první části by měly být specifikovány všechny základní a použité pojmy, rozdíly mezi Deepwebem, Darkwebem a Darknetem. Měla by zde být charakterizována funkcionalita anonymních sítí a kryptoměn. V neposlední řadě by v práci měla být již konkrétnější specifikace Darkwebu a jeho obsahu jak z obecného či právního hlediska, tak z pohledu IT a zde nabízených služeb. Další částí by měla být analýza, porovnání a charakteristika nabízených kybernetických útoků na Darkwebu.

SEZNAM DOPORUČENÉ LITERATURY:

1) FEIGENBAUM, Joan. Digital rights management: ACM CCS-9 workshop DRM 2002, Washington, DC, USA, November 18, 2002 : revised papers. New York: Springer-Verlag, c2003. ISBN 978-3-540-40410-1.
2) 2006 40th Annual Conference on Imformation [sic.] Sciences and Systems: Princeton, N.J., March 22-24, 2006. Piscataway, N.J.: Institute of Electrical and Electronics Engineers, c2006. ISBN 1-4244-0349-9.
3) MARTIN, James. Drugs on the dark net: How cryptomarkets are transforming the global trade in illicit drugs. Springer, 2014.
4) Qin, Jialun, et al. "The dark web portal project: collecting and analyzing the presence of terrorist groups on the web." Proceedings of the 2005 IEEE international conference on Intelligence and Security Informatics. Springer-Verlag, 2005.
5) Chen, Hsinchun. "Dark web forum portal." Dark Web. Springer New York, 2012. 257-270. 6) Gehl, Robert W. "Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network." new media & society 18.7 (2016): 1219-1235.

Podpis studenta: ..... Datum: 08/08/16

Podpis vedoucího práce: ..... Datum: 10.10.2016