Vrstvy internetu, vyhledávání v nich a jejich bezpečnostní rizika

Štěpán Škorvánek

Bakalářská práce
2024

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav počítačových a komunikačních systémů

Akademický rok: 2023/2024

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Štěpán Škorvánek**
Osobní číslo:	**A21123**
Studijní program:	**B0688A140008 Informační technologie v administrativě**
Forma studia:	**Prezenční**
Téma práce:	**Vrstvy internetu, vyhledávání v nich a jejich bezpečnostní rizika**
Téma práce anglicky:	**Layers of the Internet, Searching in Them and Their Security Risks**

Zásady pro vypracování

1. Vytvořte rešerši na téma vyhledávání ve vrstvách internetu.
2. Analyzujte funkce a vlastnosti prohlížečů používaných v různých vrstvách internetu.
3. Popište bezpečnostní rizika vyhledávání v různých vrstvách internetu.
4. Proveďte analýzu způsobu vyhledávání a porovnejte výsledky, které jednotlivé vrstvy poskytují.
5. Vyhodnoťte výstupy analýzy a přínosy práce.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. DRBOLA, Vojtěch. Darknet: mýtus a realita kybernetického prostoru. Bakalářská práce. Česká republika: Masarykova univerzita, 2016.
2. JONES, Jack. Hacking & Tor: The Ultimate Beginners Guide To Hacking, Tor, & Accessing The Deep Web & Dark Web. Spojené státy americké: Createspace Independent Publishing Platform. ISBN 9781546342649.
3. JONES, Jack. Accessing the Deep Web & Dark Web with Tor: How to Set Up Tor, Stay Anonymous Online, Avoid NSA Spying & Access the Deep Web & Dark Web. Spojené státy americké: Createspace Independent Publishing Platform. ISBN 1545269920.
4. NETOLIČKA, Jan. Deep a Dark web – temná strana internetu. Online. IPure.cz. Dostupné z: https://ipure.cz/archiv/magazin/deep-a-dark-web-temna-strana-internetu/. [cit. 2023-11-10]
5. STROUKAL, Dominik. Dark Web: Sex, drogy a bitcoiny. Česká republika: Grada, 2020. ISBN 9788027129348.

Vedoucí bakalářské práce: **prof. Mgr. Roman Jašek, Ph.D., DBA**
Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce: **20. listopadu 2023**
Termín odevzdání bakalářské práce: **30. května 2024**

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

Ing. Miroslav Matýsek, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 1. prosince 2023

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne

……
Štěpán Škorvánek v.r.
podpis studenta

ABSTRAKT

Internet tvoří základ moderní komunikace a informačních technologií, avšak jeho struktura a způsoby vyhledávání v jednotlivých vrstvách přináší různá bezpečnostní rizika. Hlavním cílem této práce je analyzovat jednotlivé vrstvy internetu, prohlížeče, které se ve vrstvách využívají a jejich hlavní funkce. Dále způsoby vyhledávání a bezpečnostní rizika, které především temná strana internetu přináší. Práce využívá kombinaci teoretického a literárního přehledu o vrstvách, včetně analýzy vyhledávání v nich. Výsledky ukazují, že největší bezpečnostní rizika se nacházejí ve vrstvách darknetu, jelikož je zde obtížnější kontrola a regulace obsahu. Mezi hlavní hrozby patří podvody s kryptoměnami, hoaxy a phishingové útoky. Závěrem je důležité pro bezpečné pohybování na internetu je potřeba využívat technická opatření, která různé prohlížeče nabízejí, ať už se jedná o jakoukoli vrstvu internetu.

Klíčová slova: vrstvy intenetu, darknet, internet, prohlížeč, analýza vyhledávaní, rizika darknetu

ABSTRACT

The Internet forms the basis of modern communication and information technology, but its structure and the ways of searching in the different layers bring different security risks. The main objective of this paper is to analyze the different layers of the internet, the browsers used in the layers and their main functions. Furthermore, the search methods and the security risks that especially the dark side of the internet brings. The thesis uses a combination of theoretical and literature review of the layers, including an analysis of searches in them. The results show that the greatest security risks are found in the darknet layers, as it is more difficult to control and regulate content. The main threats include cryptocurrency fraud, hoaxes and phishing attacks. In conclusion, it is important to use the technical measures offered by different browsers to move safely on the internet, whatever the layer of the internet.

Keywords: internet layers, darknet, internet, browser, search analysis, darknet risks

Rád bych poděkoval prof. Mgr. Romanu Jaškovi, Ph.D., DBA za vedení práce a její realizaci. Poděkování také patří Fakultě aplikované informatiky Univerzity Tomáše Bati ve Zlíně za možnost studia.

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Internet se stal nepostradatelnou součástí moderního života, umožňující rychlou a efektivní komunikaci, přístup k informacím a poskytování širokého spektra služeb. Přestože většina uživatelů je obeznámena s povrchovým webem, který je snadno přístupný prostřednictvím běžných vyhledávačů jako Google, existují i další vrstvy internetu, které jsou méně známé, ale stejně důležité – hluboký web a darknet. Tyto vrstvy internetu mají odlišné charakteristiky, způsoby vyhledávání a představují různé bezpečnostní výzvy.

Cílem této bakalářské práce je podrobně analyzovat jednotlivé vrstvy internetu, způsoby vyhledávání informací v těchto vrstvách a prohlížečích a identifikovat související bezpečnostní rizika. Práce se zaměřuje na tři hlavní oblasti: struktura a charakteristiky vrstev internetu, funkce a vlastnosti prohlížečů používaných pro vyhledávání v těchto vrstvách a analýza bezpečnostních rizik spojených s vyhledáváním na povrchovém webu a darknetu.

Pro dosažení těchto cílů bude využita kombinace literární analýzy a případových studií. Literární analýza poskytne teoretický rámec a přehled dosavadního výzkumu, zatímco případové studie umožní praktickou analýzu rozdílů ve výsledcích vyhledávání a souvisejících bezpečnostních rizik.

Práce je rozdělena do 5 částí. První část se věnuje teoretickému rámci o vrstvách internetu a jeho vývoji. Druhá část popisuje funkce a vlastnosti prohlížečů, které jsou používané v různých vrstvách internetu. Třetí část se zaměřuje na bezpečnostní rizika vyhledávání a pohybu především na darknetu. Dále jsou popsány známé kriminální případy spojené s touto vrstvou internetu. Čtvrtá část je zaměřena na samotné způsoby vyhledávání a porovnávání výsledků, které jednotlivé vyhledávače poskytují a poslední část shrnuje závěry vyhledávání a vyhodnocuje analýzy a přínosy práce.

Tato práce přináší důležitý přehled o různých vrstvách internetu, jejich charakteristikách a bezpečnostních výzvách. Porovnáním vyhledávání na Googlu a darknetu a analýzou souvisejících rizik poskytuje užitečné poznatky pro uživatele internetu.

I. TEORETICKÁ ČÁST

1 INTERNET JAKO ZDROJ INFORMACÍ

Internet a jeho vývoj je pro lidstvo jedním z největších vynálezů 20. století. Jeho používání je pro nás v dnešní době běžnou součástí života a spoustu z nás, by si bez něj nedokázala už představit fungovat. Jeho rozšíření se za posledních 30 let zvětšilo zhruba z jedné desítky milionu na dnešních necelých 5,5 miliardy uživatelů, jak udává server statista.com. Z toho vyplývá, že internet v současné době využívá pravidelně zhruba 70% populace naší planety. Další kapitola nám přiblíží, jak se tato platforma vyvíjela a jak se jeho rozvoj dostal až k dnešní podobě. [2]

1.1 Začátky internetu

Historie internetu sahá do 60. let 20. století, kdy svět zužovala studená válka, do které byl zapojen Sovětský svaz a Spojené státy americké. Byla to právě USA, která přišla s nápadem, jak vytvořit decentralizovanou síť, kterou by mohli využít pro komunikaci mezi důležitými institucemi jako byla armáda, vláda a vědecká infrastruktura. Tato síť byla decentralizovaná z důvodu toho, aby byla schopná vydržet jaderné útoky, které touto dobou případně hrozily. Fungovat měla na základním principu, kdy se zprávy posílají po částech, tedy paketech a ty chodili na předem známou cílovou adresu. Stejně jako dnes, pokud by se ale s jednou stranou, ať už odesílatelem nebo příjemcem, něco stalo, např. pokud by nebyl připojen nebo by cesta nebyla správně určena, paket by nedošel do cíle.

V roce 1962 tedy vzniká projekt ARPA (Advanced Research Projects Agency), který vzniká pod hlavičkou ministerstva obrany USA. Následně v roce 1966 získal tehdejší ředitel oddělení úřadu pro Technologie zpracování informací (IPTO), Bob Taylor dotaci, díky které měli být schopni tuto síť zrealizovat. I přes tuto dotaci na výzkum jako první síť s paketovým přepínáním testují v National Research Laboratory ve Velké Británii, a to v roce 1968. O rok později ale nakonec přichází ARPA se svým projektem ARPANET, který byl důležitým pilířem pro vývoj internetu do dnešní podoby. Tehdy ještě experimentální počítačová síť, spustila svůj provoz v roce 1969 a fungovala do roku 1990, kdy byla kvůli nárůstu lokálních sítí pozastavena. K této síti se postupně začaly připojovat americké akademické ústavy a to UCLA (University of California Los Angeles), SCRI (Stanford Central Research Institute), UCSB (University of California Santa Barbara) a University of Utah. V roce 1973 se k této síti poprvé také připojily instituce, které nebyli americké, a to University College of London z Velké Británie a Royal Radar Establishment z Norska. V této době také vznikali nové možnosti, a to v podobě elektronické pošty, kterou využila v roce 1976 poprvé i tehdejší britská

královna Alžběta II. Už v roce 1983 bylo do sítě zapojeno přes 500 uzlů a oddělila se síť MILNET, která sloužila k vojenským účelům. Přelomovým rokem byl rok 1992, tedy pouhých 9 let od doby, co do sítě bylo zapojeno 500 uzlů, a to z toho důvodu, že byla překročena hranice 1 000 000 uzlů. Jak je známo, každá stanice zapojena do sítě musí mít přiděleno nějaké jméno, a proto byl v roce 1984 zaveden protokol DNS (Domain Name Service), který slouží pro překlad číselných IP adres na doménové jméno, které se pamatuje snadněji než dlouhé číslo. [1,3,4]

Obrázek č.1: Královna Alžběta II. posílá e-mail [58]

1.2 Vývoj internetu

V průběhu let, jak už bylo v předchozí kapitole zmíněno, se internet rozvíjel. Tyto fáze byly později pojmenovány a rozděleny do kategorií, podle jejich možností, které uživatel mohl využívat. Obecně jsou zatím známé 3 fáze, ale v průběhu let se tyto fáze určitě ještě rozšíří o další.

1.2.1 Web 1.0

První fází internetu, jak ho známe dnes, byl takzvaný Web 1.0. Toto období je fází hlavně v letech 1990 až 2000. Tento datum je však pouze orientační, protože nelze přesně definovat, kdy jeden web skončil a nahradil ho jiný, protože ke změnám docházelo postupně. Ovšem

tato raná fáze internetu se skládala ze statických webových stránek, které byly spojené hypertextovými odkazy, bez dalších vizuálních prvků, formulářů a dalších funkcí, na které jsme na běžných stránkách zvyklý. Tato fáze byla odborníky označována jako web „pouze pro čtení“, protože pro uživatele nenabízel žádné interaktivní prvky. Stránky byly hostovány na serverech, které byly provozovány poskytovatelem internetových služeb, nebo na bezplatném hostingu. Uživatelé tedy pouze získávali informace, nebo dostávali aktualizace již o předem známých problémech. V dnešní době také může být zarážející, že v době, kdy takzvaný Web 1.0 fungoval, bylo zakázáno mít na stránkách reklamy. [5,6,7]

1.2.2 Web 2.0

Druhou fází internetového vývoje byl Web 2.0. Jeho rozvoj probíhal přibližně v letech 2000 až 2010, stejně jako u předchozích nelze přesně určit dobu trvání. V této fázi se rozrostly webové stránky v oblasti dynamických webů, které by se dalo říct, že do jisté míry ovlivnily příchod chytrých telefonů a datového připojení telefonů k internetu. Tento web uživatelům umožňoval nejen vytvářet na jednu stránku, ale také sdílet nebo obsah přidávat jiné webové stránky. Hlavním milníkem je nástup také sociálních sítí. Nejznámější je určitě Facebook, ale také to byl například Twitter, který je dnes znám pod názvem X. Na těchto sdílených stránkách uživatelé přidávali různé informace nebo obrázky, které ostatní uživatelé mohli v reálném čase sledovat a reagovat na ně. Web 2.0 také dokázal posílit globalizaci a to tím, že nabídl větší propojitelnost, což pomohlo nejen běžným uživatelům, ale také komerčním společnostem, které tuto funkci využily pro svoje podnikání. Problémem Webu 2.0 bylo však to, že naše informace, které jsme někde při registraci použily, spadly do klína firmám, které weby provozovaly. Spoustu lidí si mohlo říct, že tyto informace jsou pro ně zanedbatelné a že nemají před světem co skrývat, ale kontext tohoto problému je mnohem větší. Na počátku této fáze také začínají první zmínky o dark webu, ke kterému se dostaneme později. [5,6,7]

1.2.3 Web 3.0 a budoucnost

Web 3.0 je fáze, kde by internet měl nabývat vyšší decentralizace, která umožňuje uživatelům větší kontrolu nad jejich daty a transakcemi. Tato fáze je podporována technologiemi jako blockchain a distribuované registry. Je zde také důraz na schopnosti systému porozumět kontextu potřeb uživatelů a poskytovat jim personalizovaný obsah a služby pomocí strojového učení. Web 3.0 také zahrnuje rozšířenou a virtuální realitu. Dále usnadňuje sdílení informací napříč platformy a přináší transformaci online prostoru, který přesouvá do

inteligentního a uživatelsky přizpůsobitelnému prostředí. Od roku 2023 se také objevila zpráva od Evropské komise, kde oznámili přijetí nové strategie pro Web 4.0 a virtuální světy. Má se jednat o plán, jak připravit Evropu na digitální budoucnost. Hlavní strategií je posílení pravomocí jednotlivců a zjednodušení přístupu k dovednostem, které podporují informovanost, kritické myšlení a schopnost analyzovat informace. Cílem je vytvořit komunitu talentovaných odborníků zaměřených na virtuální svět. [5,6,7]

2 VRSTVENÍ INTERNETU

Internet však není pouze to, co si pod ním lidé představují, jako například Google, Facebook nebo e-maily. Tyto služby, které jsou známé pro většinu lidí a mají s nimi pojem internet spojený, tvoří pouze 4 % celého množství internetu. Služby, které využívá miliardy lidí po celém světě jsou tedy jenom špička pomyslného ledovce. Je potřeba si tedy definovat 3 kategorie, na které se internet rozděluje.

2.1 Surface web

Jako první a jak už bylo zmíněno, jedná o špičku ledovce, je takzvaný Surface web. Jedná se o povrchovou část internetu, která je přístupná a viditelná pro všechny uživatele World Wide Webu. Dostupná je tato vrstva pomocí standartních prohlížečů jako jsou například Google Chrome, Microsoft Edge, Mozilla Firefox nebo Safari. Tyto prohlížeče procházejí indexují webové stránky, aby je pak mohli podle relevantnosti zobrazovat konkrétním uživatelům a poskytovaly jim nejlepší výsledky. Tato vrstva je ale přesným opakem jiné vrstvy a to Darknetu, který je popsán dále. [9,10,11]

2.2 Deep web

Deep web je první z částí internetu, která spadá do té neviditelné sféry a běžný uživatel se do ní nedostane. V této vrstvě se nachází data, která nejsou prohledávána a indexována vyhledávači. K deep webu se uživatel dostane tak, že použije autorizační nebo přihlašovací údaje nebo získat odkaz. Jedná se například o internetové peněženky nebo různé databáze, ať už akademické, vojenské nebo lékařské. Mohou to ale také být záznamy nebo informace o profilech na sociálních sítích. Tato vrstva tvoří pak zbylých přibližně 96 % internetu. [9,10,11]

2.3 Darknet

Poslední částí je Darknet, který je podstatě podmnožina Deep webu. Přístup k této části není jednoduchý, protože uživatel opět musí použít odkaz na konkrétní stránku, kterou by chtěl navštívit. Ten lze získat buď od jiného uživatele nebo existují různé seznamy stránek, které jsou dohledatelné přímo na internetu. Odkaz ale není jediný nástroj, který pro prohlížení této části uživatel potřebuje. Důležitou věcí je speciální prohlížeč. Těchto prohlížečů existuje mnoho a jsou to například DuckDuckGo, Whonix nebo I2P, který už není tolik používaný. Nejznámějším prohlížečem je však prohlížeč Tor, který si popíšeme v dalších kapitolách.

Spoustu běžných uživatelů si myslí, že už jenom přístup na Darknet jim způsobí problémy, ale opak je pravdou. Pokud uživatel chce Darknet používat pro jakékoliv účely, jeho účast je zcela anonymní, musí však dodržovat bezpečnostní pravidla. Anonymity však někteří jednotlivci využívají pro skrytí svých dat nebo k nezákonným aktivitám. Každý, kdo o Darknetu někdy slyšel si tedy představí jako první právě tyto nezákonné aktivity jako jsou například nelegální obchody se zbraněmi, drogami nebo orgány. Jsou zde k nalezení soukromé konverzace, soukromé záznamy od policie, armády nebo vlády, ale lze zde také narazit na běžná fóra a diskuze, které nic nelegálního nepředstavují. [9,10,11]

3 VÝVOJ DARKNETU

Doby, kdy se Darknet začal začal formovat, nelze určit. Jeho funkce, a to prohlížení stránek, které nebyly běžně dostupné se využívalo ale už v 90. letech minulého století a zde stránky sloužily k akademickým účelům. Darknet svou dnešní podobu dostal ale od počátku 21. století, kdy se začal šířit nejznámější prohlížet Tor.

Nejranější forma Darknetu, který známe dnes vznikla v březnu roku 2000, kdy irský student jménem Ian Clarke vytvořil a vydal peer-to-peer platformu s názvem Freenet. Ta sloužila pro anonymní komunikaci prostřednictvím decentralizované sítě uživatelů Freenetu. Jako první pak s pojmem Darknet přišli inženýři z Microsoftu v roce 2002, kdy toto označení použili v článku The Darknet and Future of Content Distribution a do mainstreamových médií se tento pojem dostal s jeho první definicí, která zněla: „*Darknet je kolekcí sítí a ostatních technologií, jež lidem umožnují nelegálně sdílet digitální soubory chráněné copyrightem prakticky beze strachu z odhalení*“. V tomto stejném roce, tedy 2002, přichází první raná verze prohlížeče Tor.

Postupem času, začali různí uživatelé této anonymity zneužívat a kolem roku 2010 se na Darknetu objevují první online trhy, které umožnovaly anonymní nákupy a prodeje nelegálních látek, zbraní anebo služeb. S rozvojem těchto nelegálních činností, které jsou často i medializované v mainstreamových médiích, si Darknet získal svou špatnou pověst. Jeho popularita stále vzrůstá a o tom svědčí i množství filmů nebo dokumentů, které na toto téma vznikají. Jedním z nejznámějších je dokument, který řeší kauzu ohledně online trhu s názvem Silk Road, který je popsán později v textu.

Darknet stále využívá spoustu uživatelů, kteří chtějí chránit své soukromí a svoji online indentitu. Jsou zde lidé, kteří žijí v totalitních režimech, novináři nebo aktivisté hledající bezpečné prostředí pro komunikaci a sdílení informací mezi sebou. Vyskytují se zde také legální projekty a komunity, které se snaží poskytnout prostor pro svobodu slova a sdílení informací a názorů mimo dostupný proud internetu. Důležitou věcí je ale si uvědomit, že pokud využíváte darknet k nelegálním aktivitám, může to nést vážné právní následky. Uživatelé zapojení do nelegálních činností, čelí rizikům jako je hlavně odhalení a následné trestní stíhání ze strany právních orgánů. [3,12,13]

4 EVIL MEDIA

Pojem Evil media se objevil s rychlým rozmachem nových médií, která vycházejí z digitálního kódování dat. Nástup těchto nových médií sahá již do počátku 19. století, kdy jejich velký vzestup nastal s nástupem prvních mechanických počítacích strojů a pokračoval dál s rozvojem digitálního kódování a internetu v následujících letech.

Digitální technologie jsou v současnosti klíčovou součástí našich životů. Evil média představují ty, která překračují hranici mezi teorií a praxí takovým způsobem, který není pro společnost akceptován. Příkladem zlého média může být internet. Když byl spuštěn v devadesátých letech 20. století, byl inovativní v profesní sféře a lidé ještě neznali jeho rozsah možností. Na počátku mohl internet být považován za více zlé médium než dnes, ale postupně přibyly technologie, které uživatele ochraňují před hackerskými útoky nebo chrání děti před obsahem, který jim není určen a první nelegální trhy na Darknetu byly zrušeny FBI.

Jelikož je Darknet součástí samotného internetu, spadá do konceptu Evil media stejně jako internet samotný. Problémem Darkentu je ale to, že bojovat prosti nelegální činnosti, která zde funguje je náročnější než na otevřeném internetu, a to kvůli funkcím, díky kterým je Darknet oblíbený – anonymita. Proto je Darknet společností odsuzován a označován spíše jako zlé médium, oproti internetu. V budoucnu se možná objeví technologie, které zamezí nelegální činnosti. Darknet je stále jendím z mála svobodných míst a pokud by se jeho svoboda omezila, měli bychom se zamyslet nad tím, jestli pro nás ještě někde nějaká svoboda vůbec existuje a jsme schopni si ji užívat. [9,14,57]

5 PRINCIPY PROHLÍŽEČŮ V SURFACE WEBU

Každá vrstva má své prohlížeče, díky kterým je možné vyhledávat a prohlížet jejich obsah. Tato kapitola je zaměřena na ty nejpoužívanější a principy jejich fungování.

5.1 Webový prohlížeč

Skoro každý uživatel internetu ví, co je to webový prohlížeč a jak ho používat, ale to, jak doopravdy funguje a co webový prohlížeč zpracovává na pozadí už není tak pro uživatele jasné. Nejjednodušeji se však popsat tak, že se jedná program, který umožňuje prohlížení internetové stránky. V podstatě spuštěním této aplikace se dostáváme do rozhraní, které nám zprostředkuje přístup k obsahu internetu. Taky by prohlížeč měl poskytovat dostatečnou ochranu soukromí a právě soukromí, bezpečnost a funkcionalita jsou klíčové vlastnosti, které ovlivňují používání prohlížečů.

5.1.1 Typy webových prohlížečů

Webové prohlížeče lze rozdělit na 2 typy, a to podle vykreslovacího jádra a podle textového nebo grafického zobrazování.

Vykreslovací jádro je software, který ze zdrojového kódu načte jeho vlastnosti a informace a z nich vykreslí podobu stránky uživateli. Mezi nejznámější vykreslovací jádra patří Web-Kit, který používá Google Chrome a Safari. Dalším je Gecko, který používá Mozilla Firefox, poté Trident, ten používá Internet Explorer a taky Presto, které vyvíjela společnost Opera.

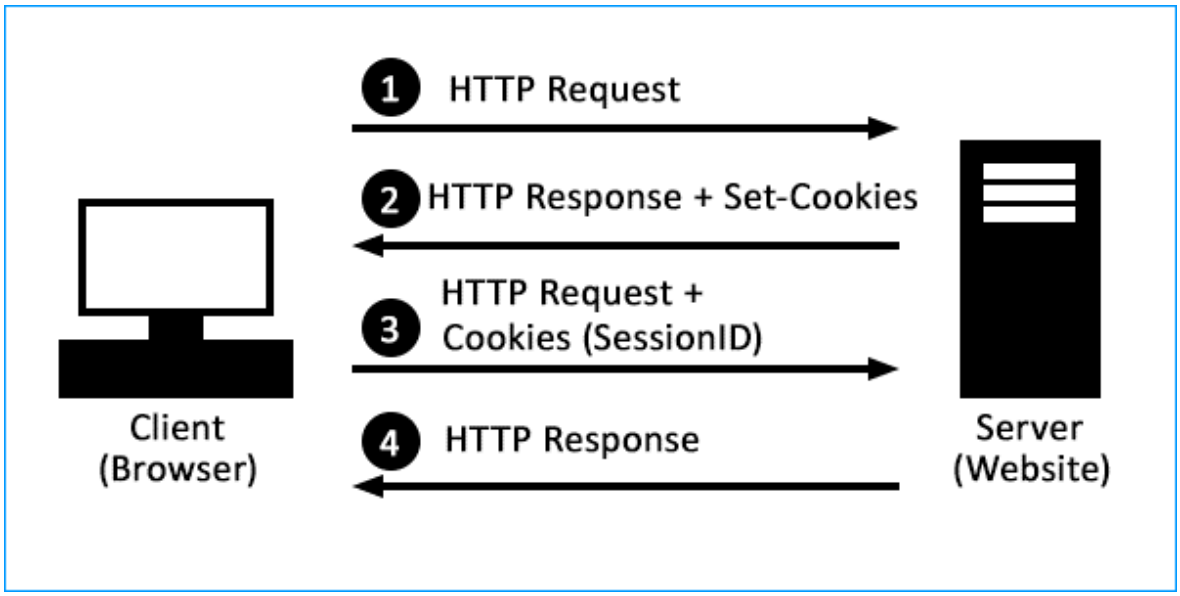
Dalším typem jsou grafické prohlížeče, mezi které se řadí víceméně všechny dostupné webové prohlížeče, jako už dříve zmíněný Chrome, Mozilla, Safari nebo Explorer. Textové prohlížeče už dnes nejsou tak známé a jak už název napovídá, prohlížeče zobrazují pouze text bez jakýchkoliv úprav. Takový prohlížeč je například Lynx, který se používá na znakových terminálech. Jeho poslední verze vyšla v roce 2018. Pro uživatele, kteří si chtějí zachovat typické prvky grafického prostředí v textovém rozhraní pak existuje například český prohlížeč Links, který má poslední verzi z roku 2023. [16,17,56]

5.2 Princip webového prohlížeče

Webový prohlížeč nás provádí online prostředím tak, že stahuje data z různých koutů webu a zobrazuje je na našem počítači nebo mobilním zařízení. Přenáší text, obrázky a videa skrze protokol Hypertext Transfer Protocol, tedy zkráceně HTTP. Když prohlížeč stáhne data,

použije své vykreslovací jádro, které bylo popsáno v předchozí kapitole a upraví stránku podle zdrojového kódu na to, co my vidíme. Každá stránka má potom svoji unikátní adresu – Uniform Resource Location, zkráceně URL adresu neboli webovou adresu. Ta potom prohlížeči určují, kde najde zdrojový kód stránky, který má převádět a kam ho má převádět.

Webové stránky si také ukládají data do souborů, kterým se říká cookies. Tyto soubory se ukládají do paměti za účelem jednoduššího použití stránky. Pokud se tedy na nějakou stránku například přihlásíme a data si necháme uložit, pomocí cookies na stránce můžeme zůstat přihlášeni i po opětovné návštěvě. Cookies mohou dále ukládat i podrobnější informace. Mohou sledovat stránky, které navštěvujete nebo obsah, který sledujete a následně na základě toho vám zobrazují další podobný obsah nebo reklamy. Cookies jsou mocný nástroj, a proto existují také takzvané cookies třetích stran, které jsou ze stránek, které uživatel nikdy nemusel navštívit a mohou uživatele tak sledovat a získávat citlivé informace, které by mohli být potencionálně zpeněžitelné. Naštěstí prohlížeče už nabízí funkci blokování těchto programů. [57]



Obrázek č.2: Princip HTTP Cookies [59]

5.3 Sledování uživatelů

V návaznosti na předchozí odstavec se dostáváme k problematice sledování uživatelů internetu. Internetové prohlížeče v sobě mají implementováno tolik funkcí a technologií, že v podstatě jakákoliv aktivita uživatele je do určité míry nějak zaznamenána neboli „trackována“. Ve většině případů jde právě o soubory cookies, které byly zmíněné v předchozí kapitole. Od 1. ledna 2022 platí zákon č. 374/2021 Sb., který by měl tuto problematiku

regulovat. Pokud se uživatel připojí k webové stránce, která má implementovanou funkci cookies, objeví se před ním buď vyskakovací okno, nebol lišta, která se uživatele ptá, zda chce cookies povolit a dá vám možnost si o této problematice i přečíst základní informace. Uživatel má tedy možnost povolit, odmítnout nebo si sám vybrat, které cookies odmítnout nebo povolit. Tyto data, která jsou následně zpracována jsou obrovská množství, ale pouze část z nich je využita pro cílené sledování aktivity uživatelů. Proč jsou ale uživatelé sledování? Důvodů může být hned několik a mohou se také lišit způsobem, jakým jsou data sbírána nebo o jaký druh dat se jedná.

Prvním důvodem může být webová analytika, jejímž cílem je analyzovat chování uživatelů připojených na webovém serveru. Jedná se především o to, aby bylo zjištěno chování uživatelů ve smyslu, kolik času stráví uživatel na serveru nebo z jakých adres se na web dostali. Dále také se zjišťuje, zda se uživatel na stránku vrací pravidelně nebo ji navštívil poprvé. Sbírání těchto dat je zásahem do soukromí, ačkoli si to uživatelé často neuvědomují.

Dalším důvodem, proč se tyto data shromažďují, může sloužit pro marketingové účely. To znamená, že pokud si někdo prohlíží různé webové stránky, tak se mu na nich zobrazují reklamy, které nabízejí podobný obsah nebo produkty, které si už dříve prohlížel na jiných stránkách. Tyto reklamy se zobrazují na základě historie prohlížení a cílí na to, aby se zobrazovaný obsah odpovídal zájmům uživatele. Při sledování historie prohlížení se sbírají data o nakupování, ale také o opět o chování., tedy jaké uživatel navštěvuje stránky a jak často, jedná se o zhruba stejný princip, jako u analytického využití. V roce 2016 vyšel článek od společnosti americké Adlucent, která se zaměřuje na internetový marketing, kde se firma dotázala tisíce uživatelů internetu, zda preferují náhodné reklamy nebo ty, které jsou jim generovány „na míru“. Tento průzkum pak jasně ukázal, že 71 % respondentů uvedlo, že preferuje takové reklamy, které jsou jim přizpůsobené a cílí na jejich osobní zájmy a nákupní zvyklosti. Dále se pak společnost požádala respondenty, aby seřadili výhody personalizované reklamy. Většina, 46 %, uvedla, že personalizované reklamy snižují výskyt pro ně irelevantních reklam, 25 % uvedl, že je to pro ně způsob, jak objevit nové produkty a 19 % uvedlo, že jim to usnadňuje a zrychluje nakupování online.

Dalším důvodem pro sběr dat, může být přizpůsobení obsahu. Tyto data se sbírají za účelem přizpůsobení stránky anebo zobrazování relevantního obsahu pro daného uživatele. Může se jednat o konkrétní rozvržení stránky nebo zobrazení podobného obsahu, který byl vyhledán dříve.

Posledním důvodem může být sledování kvůli nelegální činnosti. Může se jednat o krádež cizích přístupových údajů, sledování uživatele, aniž by s tím souhlasil nebo vydírání.

Dalším způsobem sledování uživatele může být sledování pomocí jeho IP adresy, které slouží k identifikování zařízení, které je připojeno k síti. IP adresa neslouží však pouze k identifikaci, ale také k lokalizaci. Svou roli také hraje to, jakého má uživatel poskytovatele internetu nebo jestli je jeho IP adresa veřejná nebo ne. Pokud má uživatel neveřejnou adresu, webová stránka nedokáže určit přesnou polohu zařízení, ale najdou pouze město nebo region, kde sídlí jejich internetový poskytovatel. U veřejné IP adresy se dá poloha určit přesněji, svou roli zde hraje i několik faktorů. Webová stránka se však nejprve musí dotázat, jestli ji uživatel svoji polohu povolí nebo zablokuje. Většinou se na polohu dotazují například mapy, nebo weby s předpovědí počasí, aby dokázali určit co nejbližší polohu pro správnost informací. V prohlížeči je možné si nastavit, zda uživatel chce mít povolenou polohu stále, ale také je zde možnost tuto funkci mít trvale zablokovanou. [1,18,19,23]

6 WEBOVÉ PROHLÍŽEČE

Doby, kdy na počítačích byl pouze jeden webový prohlížeč už jsou dávno minulostí. Nejznámějším prohlížečem je určitě z historického hlediska Internet Explorer od firmy Microsoft. Díky rozvoji technologií a firem, které si chtějí se svým prohlížeč vydobýt místo na trhu tak dnes už je k dispozici spoustu prohlížečů a každý uživatel si tak může vybrat, jaký mu vyhovuje ať už funkcemi nebo rozhraním nejvíce. Webová stránka statcounter.com udává každý měsíc statistiku nejpoužívanějších prohlížečů na světě. Z dlouhodobého hlediska ale jasně vyplývá, že mezi nejoblíbenější patří Google Chrome, který používá celosvětově 64,38 % a v České republice 55,66 % uživatelů. Jako další se umístil prohlížeč od firmy Apple Inc., Safari, který je na druhém místě s 18,86 % celosvětově a v České republice má zastoupení 15,46 %. Dále je Edge, 5,35 % celosvětově, 7,68 % v ČR, poté Firefox, 3,3 % celosvětově, ale v ČR je to 14,08 %. Jako poslední je prohlížeč Opera s 2,56 % celosvětově a v ČR 4,11 %. Každý z těchto prohlížečů dokáže samozřejmě zobrazit webové stránky a uživatelům nabízejí stejné funkce, které mohou různě pojmenované. [21,22,48]

6.1 Nejpoužívanější funkce v prohlížečích

6.1.1 Anonymní režim

Tento režim uživatel může využít, pokud se chce vyhnout sledování jeho prohlížení. V tomto režimu se nezaznamenává nic do historie prohlížení nebo stahování, neukládají se hesla nebo data zadaná do formulářů. Tento režim lze využít v případě, že uživatel používá cizí počítač, na kterém nechce s nikým sdílet svoje informace o prohlížení. Tuto funkce nabízejí všechny z jmenovaných prohlížečů. Tato funkce sice zastaví ukládání informací o prohlížení, ale nezastaví například škodlivé softwary, které jsou staženy v tomto režimu ani před poskytovatelem internetu, který se na historii může podívat. [24]

6.1.2 Změna vizuálu

Tato funkce slouží pouze ke změně vzhledu prohlížeče, ať už se jedná o tlačítka nebo vzhled domovské stránky. Tyto změny nemají žádný vliv na fungování prohlížeče, jedná se pouze pro případné zpříjemnění vizuálu pro uživatele.

6.1.3 Synchronizace nastavení

Pokud uživatel nějaký prohlížeč navštěvuje často a na například na více zařízeních, je umožněno si vytvořit účet, na kterém si uloží svoje nastavení, hesla, vzhled nebo oblíbené stránky.

Pokud poté přijde na jiný počítač nebo na přenosné zařízení a přihlásí se na svůj účet, veškerá nastavení, které jsou zde nastavena se synchronizují a všechny nastavené prvky vypadají stejně jako na primárním domácím zařízení.

6.1.4 Správce hesel

S přihlášeným účtem v prohlížeči má uživatel možnost ukládat své heslo do správce. Přihlašování na různé weby je pak jednodušší, protože mu prohlížeč sám nabídne předvyplnění jeho údajů na dané stránce. To stejné platí také o vyplnění osobních údajů při nákupech online nebo různých formulářů. Nemusí to být pouze základní údaje jako jméno a příjmení, ale také adresa, e-mail nebo telefonní číslo.

6.1.5 Režim pro vývojáře

V režimu pro vývojáře si uživatel může prohlížet zdrojový kód stránky, ve kterém se nacházejí detailní informace o stránce, jeho formátování a také zde může přepisovat různé prvky na stránce, které se pak ale samozřejmě neuloží.

6.1.6 RSS čtečky

Tyto čtečky, které jsou v prohlížečích zabudované slouží k přístupu k aktuálním informacím nebo novinkách z různých webů. Pokud daná stránka nabízí funkci odběru, stačí se přihlásit a poté dané informace zprostředkovávají uživateli. [25]

6.1.7 Antiphishing

Tato funkce je důležitá pro soukromí a bezpečnost uživatele. V odkazech, které uživatel otevře vyhledává hrozby a malwary. Může se jednat jmenovitě o falešné stránky bank nebo jiné online služby. Pokud se objeví podvodná stránka, antiphishing ji ihned zablokuje. Funkce také zaznamenává statistiky, kolik webů zkontrolovalo a kolik jich zablokovalo. [26]

6.1.8 Doplňky, plug-iny

Doplňky přidávají funkce, které v základní výbavě prohlížeče nepodporují. Jedná se tedy o rozšíření funkcí daného prohlížeče. Mezi nejoblíbenější plug-iny, které byly používány v roce 2023 v prohlížeči Google Chrome patří například funkce Speechify, která slouží k předčítání textů. Dalším je Sider a ten přidá do Chromu lištu, pro umělou inteligenci. A samozřejmě asi nejznámějším plug-inem je funkce AdBlock, která blokuje reklamy na webových stránkách. Tato funkce byla používána především uživateli stránky YouTube. Kvůli

blokaci reklam, ale společnost přichází o peníze, a tak své uživatele nutí k tomu, aby místo blokátorů raději zaplatili za jejich premium verzi, kde se reklamy nevyskytují.

6.2 Nejpoužívanější webové prohlížeče

Předchozí kapitola nabídla seznam nejpoužívanějších webových prohlížečů jak celosvětově, tak i v České republice. Tato kapitola se na konkrétní prohlížeče zaměřuje od těch nejpoužívanějších po méně využívané.

6.2.1 Google Chrome

Google Chrome je multiplatformní prohlížeč od společnosti Google, který na trh přišel v roce 2008, nejprve pouze pro operační systém Windows. Později se však také dostal na systémy Linux, MacOS, ale také mobilní systémy Android a iOS. Hned po vydání se díky své jednoduchosti a funkcím stal nejpopulárnějším prohlížečem na trhu. Tento prohlížeč je postaven na otevřeném a svobodném zdrojovém kódu od Googlu, který nese název Chromium. Google Chrome nejprve používal vykreslovací jádro WebKit, které bylo považováno za nejlepší vykreslovací jádro pro prohlížeče, později však, konkrétně v roce 2013 přišel Google Chrome s novinkou. Tou novinkou bylo vykreslovací jádro Blink, který v podstatě z WebKit vychází a postupem času se od něj snažil odlišovat. Hlavním cílem změny jádra mělo být zvýšení výkonu, kompatibility a stability na všech zařízeních, které podporují Google Chrome. Právě použitím nového jádra tak Google cílil na hlavní aspekty toho, proč by si uživatelé měli vybrat jejich prohlížeč. Chrome je jedním z nejrychlejších prohlížečů na trhu. Dále je jednoduchý, umožňuje synchronizaci, různá rozšíření a také je znám svou bezpečnostní architekturou, kde je možné využití sandboxu, který byl z počátku pro uživatele lehce kontroverzní. Tato funkce se zavedla v druhé polovině roku 2023 a měla by sloužit jako testovací náhražka cookies třetích stran. Google se tak chystá na vypnutí sledovacích cookies, které by údajně mělo přijít v druhé polovině roku 2024. Princip sandboxu je takový, že pokud prohlížeč narazí na nějakou pochybnou nebo podezřelou stránku, přesune ji do sandboxu, kde ji před uživatelem uzavře, aby ho stránka nezahlcovala obsahem, který pro něj není relevantní nebo ho ochránila ho před spamem.

Google Chrome má také vlastní správce úloh, pomocí kterého lze zjistit, jaké je využití komponent v počítači v závislosti na otevřené jednotlivé karty a pluginy v prohlížeči. Díky správci úloh také Chrome nevypne celý prohlížeč v případě, že nějaká stránka havaruje nebo se zablokuje.

Obrovskou výhodou je samozřejmě propojení účtů a služeb od Googlu. Díky jednomu účtu je možné synchronizovat záložky, historii, hesla a další data, která mohou být uložena na jiných zařízeních. Dále také má Chrome svůj vlastní obchod, ve kterém je spousta různých rozšíření, které mohou prohlížení zpříjemnit nebo prohlížeči dodat funkce, které v základě nemá.

Google Chrome má také automatické aktualizace, takže uživatel ani nezaregistruje, že nějaká změna proběhla. Od spuštění v roce 2008 vyšlo už téměř 30 verzí tohoto prohlížeče, a to pouze na desktopová zařízení. Pro mobilní operační systémy, které se na Androidu a iOS objevili v roce 2012 vyšlo již přes 15 verzí.

Chrome se také často schází s kritikou, a to hlavně kvůli nárokům, které jsou zejména poznat na zabírání operační paměti. Toto využití se děje z toho důvodu, že Chrome načítá stránky dopředu. Dalším problémem pro uživatele je ten, že se Chrome do počítače dostane s jiným programem a uživatelé tak o jeho instalaci nevědí. Když Google Chrome přišel s verzí Chrome 69, tak si uživatelé stěžovali na vynucené přihlašování. Pokud se uživatel přihlásil k jedné službě, přihlášení proběhlo ke všem ostatním službám a také i do samotného prohlížeče, proto tuto funkci Chrome plánuje ve verzi 70 smazat, aby se uživatelé necítili ohroženi na soukromí. Ve verzi Chrome 70 by také měla být možnost mazání cookies, protože v předchozích verzích tomu tak nebylo. Zkrátka i když je Google Chrome celosvětově nejpoužívanějším prohlížečem, jeho funkce nejsou stále za téměř 20letou existenci vyšperkované do dokonalosti a má stále co zlepšovat. [27,28,29]

6.2.2 Safari

Safari je prohlížeč, který vyvíjí společnost Apple Inc. Primárně je vyvíjen pro jejich zařízení a jejich operační systém iOS a macOS. Poprvé na trh tento prohlížeč přišel v roce 2003 a to nejprve k samostatnému stažení a později se stal součástí operačního systému Mac OS X 10.3. Od té doby je vydáván jako výchozí prohlížeč ke každé nové verzi operačního systému. V roce 2007 byl tento prohlížeč vydán také k operačnímu systému Windows, jelikož měl Apple dohodu s konkurenčním Microsoftem. Před tím, než se Safari stalo výchozím prohlížečem, na zařízeních byl původně Internet Explorer. S příchodem prvního iPhonu v roce 2007 se tedy Safari rozšířilo i na Windows. Tato spolupráce však dlouho nefungovala a Safari se už v roce 2010 odsunulo pouze na produkty od Applu. Problémem byla hlavně funkčnost prohlížeče. Apple si vytvářel prohlížeč pro svá zařízení a aby na nich fungoval dobře,

proto od roku 2012, kdy Safari na Windows ztroskotalo, už žádnou verzi pro Windows nevyvíjí.

Safari používá stejné renderovací jádro, jako dříve používal Google Chrome a to WebKit. Safari přineslo funkce, které jsou dnes už běžné téměř ve všech prohlížečích a spousta prohlížečů jeho funkce právě okopírovalo. Jedná se například o blokovaní reklam nebo režim čtení. Tento prohlížeč také jako první blokoval cookies třetích stran. Obrovskou výhodou tohoto prohlížeče je kompatibilita mezi jednotlivými zařízeními od Applu. Pokud uživatel vlastní 2 zařízení od Applu a na jednom z nich si rozečte například nějaký článek, na druhém zařízení si ho může dočíst. Tento prohlížeč umožňuje synchronizaci dat mezi zařízeními, pokud si v uživatel v Safari zkopíruje odkaz, má ho zkopírovaný i v druhém zařízení. Jeho omezení přichází však v rozšíření, které se dají do Safari nainstalovat. Oproti jiným prohlížečům, je jejich množství omezeno. Výhodou je však zabezpečení a ochrana uživatelů, protože prohlížeč blokuje cookies třetích stran a chrání před malwarem a phishingem. [30,31,50]

6.2.3 Microsoft Edge

Microsoft Edge je webový prohlížeč, který vyvíjí společnost Microsoft a poprvé byl na trh uveden v roce 2015, jakožto výchozí prohlížeč tehdy nového operačního systému Windows 10. Jedná se o nástupce dlouho používaného prohlížeče Internet Explorer, který byl výchozím pro uživatele na předchozích verzích systému Windows. Microsoft Edge byl původně postaven na vykreslovacím jádře EdgeHTML, ale bylo tomu však pouze v letech 2015 až 2019.

V roce 2019 prošel celý Edge změnou, a hlavně přechodem na vykreslovací jádro Chromium, což je stejné jádro, který je používané v nejpopulárnějším prohlížeči Google Chrome. Přestavba jádra přinesla několik výhod jako například lepší kompatibilita se standarty webu, více rozšíření do prohlížeče a také zlepšení výkonu. Touto přestavbou se Edge dostal blíže ke konkurenčním prohlížečům a získal si větší pozornost na trhu. Přestože Edge už s jeho předchůdcem Internetem Explorerem nemá nic moc společného, uživatelé stále raději volí jiné možnosti pro prohlížení internetu z toho důvodu, že Edge k jeho předchůdci stále přirovnávají. Edge nabízí široký výběr doplňků a funkcí, které uživateli pomohou lépe personalizaci. Obsahuje také integrované bezpečnostní prvky, které mohou zamezit sledování, filtrovat nebezpečné stránky a chránit proti phishingu. Výhodou je také to, že Edge je

integrován s operačním systémem Windows, takže nabízí synchronizaci s Microsoft účtem, a tedy celkovou synchronizaci s nastavením a přenosem dat mezi zařízeními.

Aktuálně existují tři veze tohoto prohlížeče a ty se liší v aktualizacích. První verzí je Dev Channel, která je aktualizovaná jednou týdně. Druhou je Canary Channel, která je aktualizována jednou denně a poslední je Beta Channel a ta aktualizuje pouze jednou za půl roku. Záleží už jenom na náročnosti uživatele, jakou verzi si vybere, jelikož těmito aktualizacemi si vybírá, zda chce novinky prohlížeče dostávat co nejdříve, nebo si vystačí s klasickou verzí a nepotřebuje prohledávat nastavení a zjišťovat, které nové funkce přibyly. [32,51]

6.2.4 Mozilla Firefox

Mozilla Firefox je dalším velice oblíbeným prohlížečem, jehož vývoj má na starost nezisková organizace Mozilla Corporation. Historie tohoto prohlížeče sahá do roku 2002, kdy vývoj započal jako projekt, který byl zaměřený na vytvoření moderního a otevřeného prohlížeče, který by mohl konkurovat tehdejší jedničce na trhu Internet Exploreru od společnosti Microsoft.

První verze se objevila o 2 roky později, tedy v roce 2004 a to jako nástupce balíčku Mozilla Suite. Mozilla Suite byl internetový balíček, který obsahoval webový prohlížeč, e-mailového klienta a editor HTML kódu. Vývoj tohoto balíčku skončil v roce 2006 a od té doby se společnost zaměřila pouze na samotný prohlížeč. Později však zachovali i e-mailového klienta, který nese název Mozilla Thunderbird. První verze z roku 2004 si velmi rychle získala uživatelskou základnu díky své rychlosti a bezpečnosti. Jedním z faktorů, který také Firefoxu přispěl k jeho úspěchu je jeho open-source povaha. To znamená, že k jeho vývoji mohli přispívat vývojáři a komunity po celém světě, díky čemu docházelo k rychlé inovaci a zdokonalování. V roce 2010 s příchodem nové verze 3.6, přišlo také nové renderovací jádro Gecko, které slouží kromě renderování stránek také k vykreslování grafického rozhraní. Aktuálně toto multiplatformní jádro spravuje a vyvíjí právě Mozilla Corporation.

Další zajímavostí je také to, že příchod verze 3.0 zaznamenal takový úspěch, že první den po zveřejnění na trh bylo staženo přes 8 milionů kopií toho prohlížeče a díky takovému počtu je Firefox zapsán do Guinnessovy knihy rekordů za největší počet stažených kopií. Ještě větší úspěch je však to, že počet stažených kopií verze 4 byl poté ještě větší. Jeho úspěch byl také podpořen z důvodu kritiky, která se v době vývoje dostávala Internet Exploreru, který nedodržoval webové standardy a měl bezpečností problémy, kvůli kterým byl náchylný na spyware a malware.

Firefox se v roce 2017 rozhodl, že přejde na nový design, který je znám pod názvem „Firefox Quantum“. Tato aktualizace přinesla modernější rozhraní, zdokonalení výkonu a samozřejmě si opět tímto krokem posílil pozici na trhu. Jeho funkce jsou pak obdobné jako u ostatních prohlížečů. Jedná se například o ochranu soukromí, vysoký výkon, personalizace nebo synchronizace. Zajímavou funkcí však může být Firefox Monitor. Tato funkce umožňuje uživatelům zkontrolovat, jestli u jejich účtů nedošlo k úniku dat, jelikož spolupracuje s databází Have I Been Pwned, na které se tyto informace dají ověřit. Další funkcí je Firefox Send, kdy se jedná o službu pro sdílení souborů, které mohou mít velikost až 2,5 GB. Soubory je možné posílat šifrovaně a lze nastavit jejich expiraci, což zajišťuje větší bezpečnost a soukromí dat. Posledními funkcemi, které stojí za zmínku mohou být čtečka článků, která umožňuje uložení článku nebo videa, které je možné shlédnout později nebo i offline, nebo Mozilla VPN. Ta slouží k šifrovanému připojení k internetu a skrývání IP adresy. [15,33,34]

6.2.5 Opera

Opera je posledním z oblíbených prohlížečů, který vyvíjí norská firma Opera Software. Historicky se dostáváme až do roku 1995, kdy programátor Jon Stephenson von Tetzchner a Geir Ivarsøy společně začali spolupracovat na vývoji tohoto prohlížeče. Opera nejprve používala vykreslovací jádro Presto, u kterého vydržela až do roku 2013, kdy Opera přešla na jádro WebKit, ze kterého nyní vychází jádro Chromium, o kterém už byla dříve řeč. Vývoj Opery zažil několik klíčových mezníků ve své historii, a to nejprve v roce 1996 již s verzí 2.0. Ta umožňovala podporu kaskádových stylů, dále vylepšené vyhledávání a možnost otáčení obrázků. Verze 3.0, která vyšla jenom o rok později přinesla podporu JavaScriptu a stylu CSS, což přineslo lepší kompatibilitu s moderními webovými stránkami. Již v roce 1999 s verzí 5.0 Opera dokázala podporovat většinu moderních webových standardů. V roce 2009 byla poprvé představena také Opera Turbo, která umožňuje komprimovat data a zvyšovat rychlost načítání stránek, a to zejména při pomalejším nebo omezeném internetovém připojení. Dále v roce 2019, během herní konference byla oznámena Opera GX, která se zaměřuje na hráče videoher. Tento prohlížeč oproti standartnímu umožňuje omezit využití sítě, paměti a procesoru. Přidal také synchronizaci s aplikacemi jako je Discord nebo Twitch.

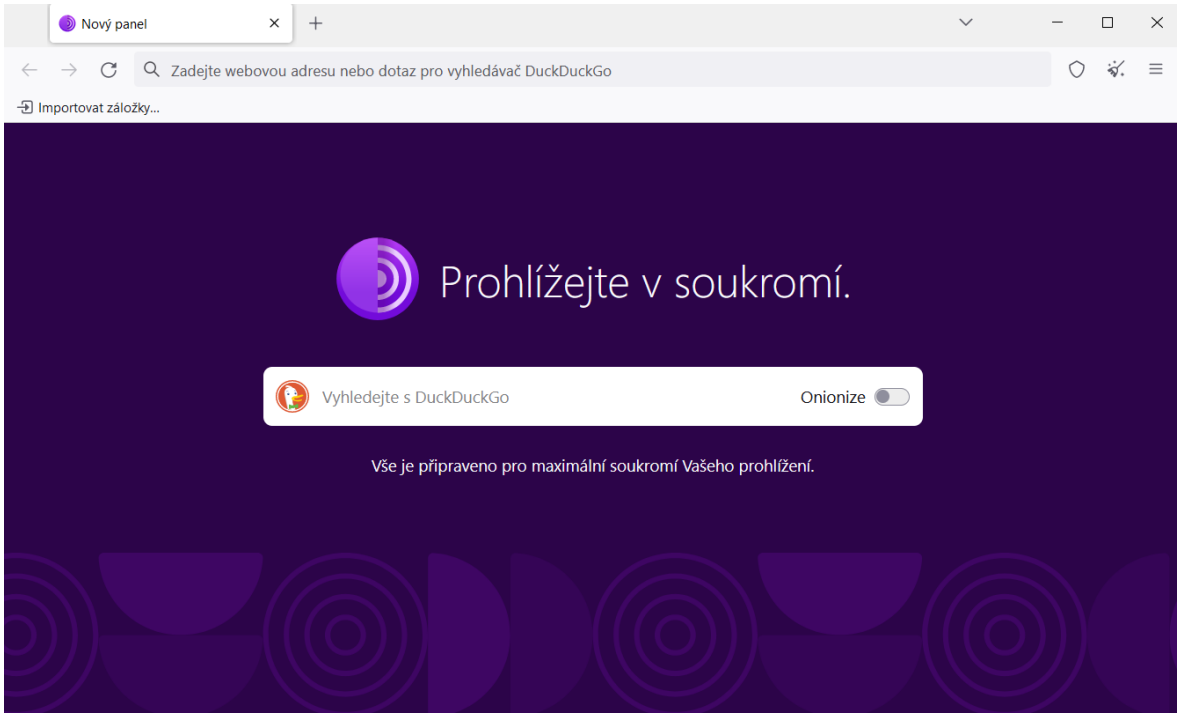
Mezi klíčové funkce tohoto prohlížeče můžeme zařadit vestavěný blokátor reklam, díky blokaci zrychluje načítání stránek. Nabízí navigaci pomocí gest a klávesových zkratek, díky kterému je snadná orientace na webech i bez myši. Dále je to funkce Stash. Ta uživateli ukládá a organizuje obsah jenž si uživatel chce prozkoumat později. Opera má také

vestavěnou VPN, její využití je stejné jako u předchozího prohlížeče Mozilla Firefox. Dále podporuje sociální sítě a zjednodušuje přístup k nim, díky umístění na boční panel. Má také svou mobilní verzi, která je vyvíjena od roku 2005 a je dostupná na všechny jak operační systémy pro počítač, tak pro všechny mobilní operační systémy, a navíc i pro zařízení Nintendo DS, Nintendo WII, automobily, televizory terminály a další. [52,53]

6.2.6 Tor

Předchozí kapitoly se zaměřovali na běžně používané prohlížeče, které pracují na takzvané „Surface web“ vrstvě internetu. Prohlížeč Tor bývá hlavně skloňován s pojmem Darknet, čili s tím, že je díky Toru se na tuto stranu internetu dostat. Tato část není dostupná z prohlížečů jako Google Chrome nebo Mozilla Firefox, ale právě přes anonymní sítě, jako je právě Tor, který slouží k zabezpečení identity uživatele, soukromého prohlížení a komunikaci online.

Tor je zkratka pro anglický termín The Onion Routing, což je anonymní komunikace, která probíhá přes počítačovou síť. Tento projekt vznikl díky americkému námořnictvu, konkrétně díky její výzkumné laboratoři, kde cílem tohoto projektu bylo vytvoření a zabezpečení armádní online komunikace. Celkově na tomto projektu pracovalo 5 vědců – Paul Syverson, Michael Reed, David Goldschlag, Roger Dingledine a Nick Mathewson, kteří s dalšími spoluzakladateli později vytvořili neziskovou organizaci The Tor Project, díky které mohl vývoj pokračovat.



Obrázek č.3: Úvodní stránka prohlížeče Tor, verze 13.0.14

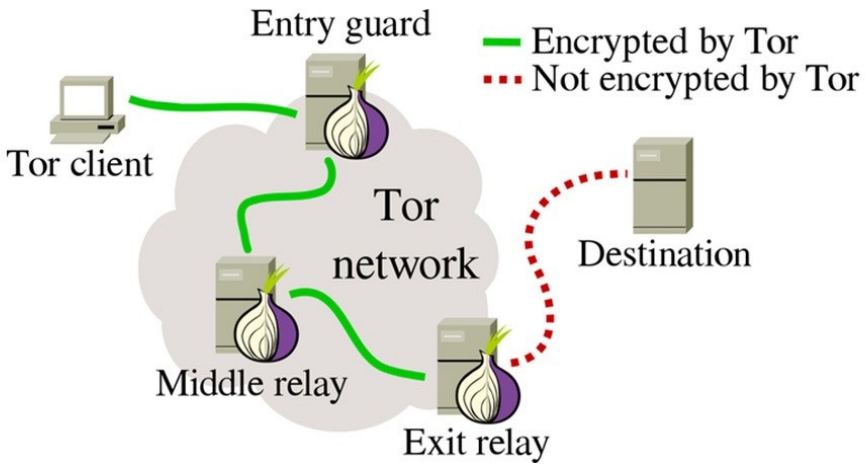
Princip Onion Routingu je takový, že pokud uživatel chce této služby využívat, nejprve spustí Tor, který mu automaticky vytvoří takzvanou „onion route“. Jedná se o cestu, která je složena z řady proxy serverů, které jsou po celém světě. Tato cesta vede skrze síť dobrovolníků a je složena z několika relací neboli „relay“. Každá relace zná pouze svého předchůdce a další relay, kterému má data poslat dále. Data, která uživatel posílá jsou potom opakovaně šifrována ve více vrstvách. Každý relay použije svůj unikátní klíč k zašifrování a tím vytváří další vrstvu. Každá vrstva šifrování obsahuje instrukce pro následující relay, díky kterým dokáže data dešifrovat a předat dále. Když data dorazí na poslední relay, odstraní se poslední vrstva šifrování a data se doručí na cílovou adresu a jsou připravena k použití. Po doručení dat k cílové adrese, server odpovídá na požadavek a posílá odezvu stejnou cestou, kterou data původně přišla, jenom do opačného směru. Opět jsou data šifrována v každém relayi a jsou tedy chráněna i na cestě zpět. Tímto způsobem se zajišťuje, že data putují do cíle a zpět v soukromí.

Komunikace v síti probíhá přes 3 hlavní body. Prvním je takzvaný „Entry guard“. Přes tuto bránu vstupují do sítě všechny uživatelovi požadavky a jeho účelem je snížit riziko útoků na uživatele. Jelikož každý uživatel má svůj Entry Guard přiřazen na určité období, tak díky

němu uživatel komunikuje pouze s jedním konkrétním relayem, což útočníkům snižuje šanci na sledování.

Další část architektury je Middle Relay, který funguje jako prostředník pro posílání mezi jednotlivými relayi. Jeho funkce je rozložení rizika pro případné útoky nebo sledování na více relayů a tak zvýšit odolnost a bezpečnost sítě. Uživateli je Middle Realy přiřazen specificky podobně jako Entry Guard.

Posledním bodem je Exit Relay. Ten slouží k poskytování připojení uživatelů ke stránkám. Každý Exit Relay má vlastní IP adresu, která je viditelná pro webové servery, a to jim umožňuje zobrazovat obsah a odpovídat na požadavky uživatelů Torů. Exit relaye jsou kritickým bodem v síti, protože jsou jediným místem, kde uživatel opustí anonymní prostředí. Provozovatelé těchto relayí musí být obeznámeni s bezpečnostními a právními záležitostmi, které se provozů týkají.



Obrázek č.4: Onion routing [60]

Tor využívají různé skupiny lidí z různých důvodů. Do hlavních kategorií se řadí například lidé, kteří žijí v zemích, kde mají omezený přístup k internetu. Tito lidé používají Tor k obejití blokovaných webů a služeb, které by pro ně nebyly normálně dostupné.

Další mohou být novináři a aktivisté pro zajištění soukromí u citlivých informacích například o lidských právech, korupci nebo politické situaci.

Jelikož tato síť byla vyvinuta původně pro státní orgány, tak ji využívá například policie nebo armáda a soudy za účelem shromažďování důkazů a sledování podezřelých aktivit.

Poslední velkou skupinou mohou být IT specialisté, kteří zde mohou zkoušet nová nastavení systému, firewallů a podobně. Této skupině Tor může sloužit jako takový sandbox, kde mohou bezpečně testovat nové technologie. Mohou také v případě výpadku DNS serverů využít tuto síť k opětovnému navázání spojení. [9,54]

6.2.7 I2P

Prohlížeč I2P se označuje za alternativu nejznámějšího Toru. Zkratka I2P znamená Invisible Internet Project, a proto by se dalo říct, že to není úplně běžný prohlížeč, ale spíše anonymní síť, která byla vytvořena pro zvýšení soukromí a bezpečnosti na internetu.

Anonymní prostředí poskytuje uživatelům svobodnou činnost. Tato síť je šifrovaná a je typu peer-to-peer, provozovatel tak není schopen sledovat činnost, zdroj zpráv nebo jejich cíl. Přenosové kanály I2P jsou odolné proti rozpoznání a blokování cenzury. Síť má i svůj DNS systém, tedy protokol pro překládání adres, díky kterému je možné vlastní hostování a zrcadlení obsahu na internetu. Mezi vestavěné funkce patří například e-mailový klient, šablona pro tvorbu webových stránek nebo klient BitTorrent. Lze však přidat i další rozšíření do konzole.

Pro komunikaci na síti, I2P používá přenosových tunelů, které slouží k utajení provozu a komunikace, která je přes ně přenášena. Každé spojení je šifrováno od jednoho směrovače k dalšímu a také od jednoho klienta k dalšímu klientovi. Komunikace tedy probíhá přes směrovače a jednosměrné tunely, mezi nimiž probíhá komunikace pomocí protokolů. Klienti se připojují k různým směrovačům a dočasně používají tunely pro odesílání komunikace.

Provoz je tvořen dobrovolníky, stejně jako u Toru, ale i přes to je stále Tor nebo VPN lepší volbou pro anonymní použití internetu. [4,9,55]

7 RIZIKA DARKNETU

Předchozí kapitola se zaměřovala na funkce, na které uživatel může narazit při používání převážně Surface webu. Teď je třeba se zaměřit na funkce a rizika, které sebou může nést prozkoumávání darknetu a jeho stránek, ať už legálních nebo nelegálních, kterých se zde nachází desítky tisíc. Pokud se návštěvník chová, tak jak má, v podstatě mu žádné nebezpečí nehrozí, ale na některých stránkách může nechtěné kliknutí na špatné místo vyvolat nemilou reakci.

7.1 Kryptoměny

Jelikož veškeré transakce, které na darknetu probíhají, jsou realizovány pomocí kryptoměn. V důsledku toho jsou podvody s nimi v podstatě nejběžnějším typem podvodů, které na darknetu probíhají. Pokud se na tržištích pohybuje běžný uživatel, který nemá zkušenosti, pro podvodníky je velice jednoduché z nich dostat peníze. Jedná se o poměrně stejné podvody, jako jsou phishingové útoky v rámci Surface webu, kdy se podvodníci snaží získat peníze z kreditních karet. O co se tedy jedná a proč jsou kryptoměny tak zásadní v temné části internetu.

Kryptoměny jsou digitální nebo virtuální druhy měn, které fungují na decentralizovaných platformách a díky tomu jsou ochráněny před sledováním vládními, a i jinými institucemi. Tyto nehmotné měny fungují na principu peer-to-peer, kdy jsou uživatelé přímo spojeni. Je obecně známé, že kryptoměny se dají těžit na počítačových zařízeních a díky tomu, že uživatelé těží na počítači a pomocí určeného softwaru, tak podporují jiné transakce, které probíhají. Tím, že pomáhají zpracovat transakce, si uživatelé vysloužíí malou odměnu, která je tvořena z kryptoměny, která se tak začíná cirkulovat v oběhu.

Jedním z důležitých ukazatelů vývoje trhu s kryptoměnami je určitě jejich kurz. Ten se řídí podle kurzů normálních měn, které jsou používány v běžném životě, jako je například koruna nebo euro. Tyto kurzy jsou určovány poptávkou a nabídkou na trhu. Kurzy virtuálních měn jsou především známé svou volatilitou, což znamená že jejich hodnota rychle stoupá, ale také naopak rychle klesá. To způsobují různé regulace nebo výkonnost trhu. Dále jsou kurzy ovlivněny na základě různých burz, kdy každá burza nabízí odlišný kurz. Investoři, kteří do těchto měn investují proto provádí důkladný výzkum a mohou využívat různých rad od odborníků, než do měn své peníze investují. Kryptoměny také nepodléhají inflaci a neúčtují si poplatky za transakce nebo je také nemožné jakoukoliv transakci v kryptoměnách

zrušit. Mezi nejoblíbenější a nejobchodovanější kryptoměny v roce 2024 patří stále nejznámější Bitcoin, Ethereum nebo Cardano. [9,35]

7.1.1 Bitcoin

Bitcoin na kryptoměnových burzách je stále nejrozšířenější měnou, a to také v návaznosti na jeho využití v prostředí Darknetu. Byl vytvořen v roce 2009 a jeho stvořitelem je člověk, který si říká Satoshi Nakamoto. Není jisté, zda jde o pravé jméno člověka, skupiny nebo o pseudonym. Toto jméno pochází z japonštiny, ale jenom díky tomu není možné určit, o kterého člověka se jedná. Spekulace však říkají, že se jedná právě o skupinu lidí a Satoshi Nakamoto je pseudonym celé skupiny. Pomocí příspěvků a komentářů, kde se osoba pod tímto jménem vyjadřovala britskou angličtinou to naznačuje tomu, že minimálně jedna osoba z tohoto uskupení by měla pocházet ze zemí Commonwealthu, tedy ze sdružení Spojeného království Velké Británie a Severního Irska a jeho bývalých dominií a kolonií. Později přišel švýcarský expert Stefan Thomas také s teorií, že na základě doby přispívání na fóra osoba nepřispívá mezi pátou a jedenáctou hodinou Greenwichského středního času, což by znamenalo, že pokud Satoshi žije normálním životem a má běžné návyky, měl by se nacházet v časovém pásmu, které odpovídá východu severní a střední Ameriky.

Obrázek č.5: Socha zakladatele Bitcoinu – Satoshi Nakamoto, v Budapešti [61]

Vývojem Bitcoinu také započala éra kryptoměn, protože z jeho kódu, který je open source vyhází většina kryptoměn. Když se Bitcoin na trhu objevil, lidé využili toho, že jeho těžkou se daly vydělat velké peníze. Následně ale při čím dál větším nárůstu na popularitě, se zvyšoval i počet transakcí a držitelů Bitcoinu, což vede k tomu, že jeho těžba je náročnější. Bitcoin má uživatel uložen ve své virtuální peněžence a uživatel si může vybrat, který typ peněženky si vybere. V roce 2023 mezi nejoblíbenější patřily Trust Wallet, Exodus Wallet nebo Coinomi Wallet a to hlavně díky své podpoře velkého počtu různých kryptoměn. Konkrétně však Bitcoinové peněženky jsou oblíbené například Trezor, Ledger Nano nebo MetaMask.

Získat Bitcoin lze několika způsoby a tím nejjednodušším a nejdostupnějším je určitě přes směnárny, které provozují firmy nebo podnikatelé a Bitcoin, jak prodávají, tak na nakupují. Kurz u těchto firem je velmi podobný tomu oficiálnímu a aktuálnímu. Co může pořizovatele odradit nebo zaskočit je, že nákup u těchto směnáren se eviduje, takže se udělá zápis o celém obchodu se všemi podstatnými údaji.

Další možnost získaní Bitcoinu mohou být Bitcoinové bankomaty, u kterých je možné Bitcoin koupit nebo prodat, a to za použití hotovosti. Dále také nabízejí možnost vytvoření vlastní peněženky, které vygeneruje klíč a díky tomuto klíči jsou nákupy a prodeje dále anonymní. V České republice se tyto bankomaty stále rozšiřují a k začátku roku 2024 jich je po republice kolem 70.

Třetím způsobem může být těžení Bitcoinu, kdy poměr vytěžené kryptoměny za dobu těžení a spotřebování energie, může být nevýhodné. Poslední možností je nákup přes peer-to-peer obchody, kde lze najít osoby, které kryptoměny prodávají a přímo s nimi obchodovat. Uživatelé si vymění údaje o peněženkách a zašlou peníze. V těchto obchodech osoby získávají hodnocení od lidí, se kterými obchodovali, a tak díky recenzím je možné si vybrat ověřenou osobu a vyhnout se podvodům. [9,36,37]

7.1.2 Kriminalita a kryptoměny

Tyto dva pojmy – kriminalita a kryptoměny, jsou termíny, které v tématu darknetu jdou ruku v ruce. Kryptoměny jsou jistý pomocník ke konání nelegální činnosti na darknetu. Jak bylo už dříve zmíněno, kryptoměny jsou hlavní platební měnou v této sféře a jejich využití nemusí být vždy pouze ve formátu nákup, prodeje nebo převodu, ale mohou být také využity k vydírání. Jak tomu bývá, pokud se nějaká firma nebo instituce dostane do křížku s hackerskou skupinou, ta od napadeného subjektu pak žádá určité výkupné, aby svou činností nezpůsobili

ještě větší škody. Jelikož výkupné ve formě běžné měny, tedy v našem případě například koruny, eura nebo dolaru, by bylo jednodušeji dohledatelné a pro hackery nebezpečnější, protože se zvyšuje riziko odhalení, žádají výkupné v kryptoměnách, jehož transakce jsou anonymní. Pokud se jedná o převod mezi peněženkami, údaje o transakcích jsou v peněženkách uchovány a pro odhalení by musela být určitá peněženka přímo dohledána.

Tento anonymní způsob transakcí je překážkou pro policii a další orgány, kteří se snaží získat podrobnosti o osobách, které na temném webu provádějí nelegální činnost. Pokud je Bitcoin použit k nějaké transakci, tak je tato skutečnost zaznamenána do block chainu, kde se zapíší obě strany, mezi kterými transakce proběhla. Tyto informace mohou poskytnout klíčová vodítka k vyhledání a odhalení pachatelů, kteří nelegální činnost provádí. Technologie, které tyto činnosti mohou rozluštit se stále zlepšují, ale i hackeři a kriminálníci používají stále vylepšené a složité překážky pro orgány, které se jejich totožnost snaží odhalit.

Pokud se policie snaží dostihnout pachatele pomocí adresování jeho transakcí, postup je velmi náročný. Jednou z možností je to, že zajistí bitcoinové adresy a poté pomocí určených programů, které umí prozkoumat prohlížeč Tor, vyhledají adresy, které mají, co dočinění s prodejem nelegálních služeb nebo látek. Tento postup lze využít u Bitcoinu nebo Ethereum. Poté, co dostanou výstup s vylistovanými adresami, snaží se najít spojitost v block chanu, kde by tyto transakce měli být zaevidovány. Dále vyšetřování pokračuje na běžné, surface, vrstvě internetu, kde jsou vyhledávány adresy, které policie získala pomocí dalších programů a jsou nějak spojené s výsledky z block chainu. Při vyhledávání tras, kudy kryptoměny procházely je důležitý hlavně start a cíl. Při sledování tras přichází na řadu hledání chyb, kterých se osoby mohly dopustit a díky tomu policie může zjistit jejich totožnost.

Pokud běžný neznalý uživatel prochází darknet, je důležité si uvědomit, jaká rizika ho tam čekají, konkrétně v souvislosti s kryptoměnami. Je zde mnoho falešných směnáren a burz, které se tváří jako pravé, legitimní platformy, a přitom slouží pouze k získání financí uživatele. V návaznosti na to je možné zde narazit přímo na podvodné prodejce kryptoměn, kdy prodejci mohou nabízet měny, které vůbec neexistují, nebo nemají žádnou cenu. [37,38,40]

7.2 Exitové strategie

Pokud uživatel prohlíží různé obchody a tržiště na darknetu, je velice pravděpodobné, že se s tímto problémem setká. Nedojde mu to však hned, ale pouze pokud se rozhodne něco si objednat. Exitová strategie spočívá v tom, že daný prodejce, který vlastní e-shop, přijímá od

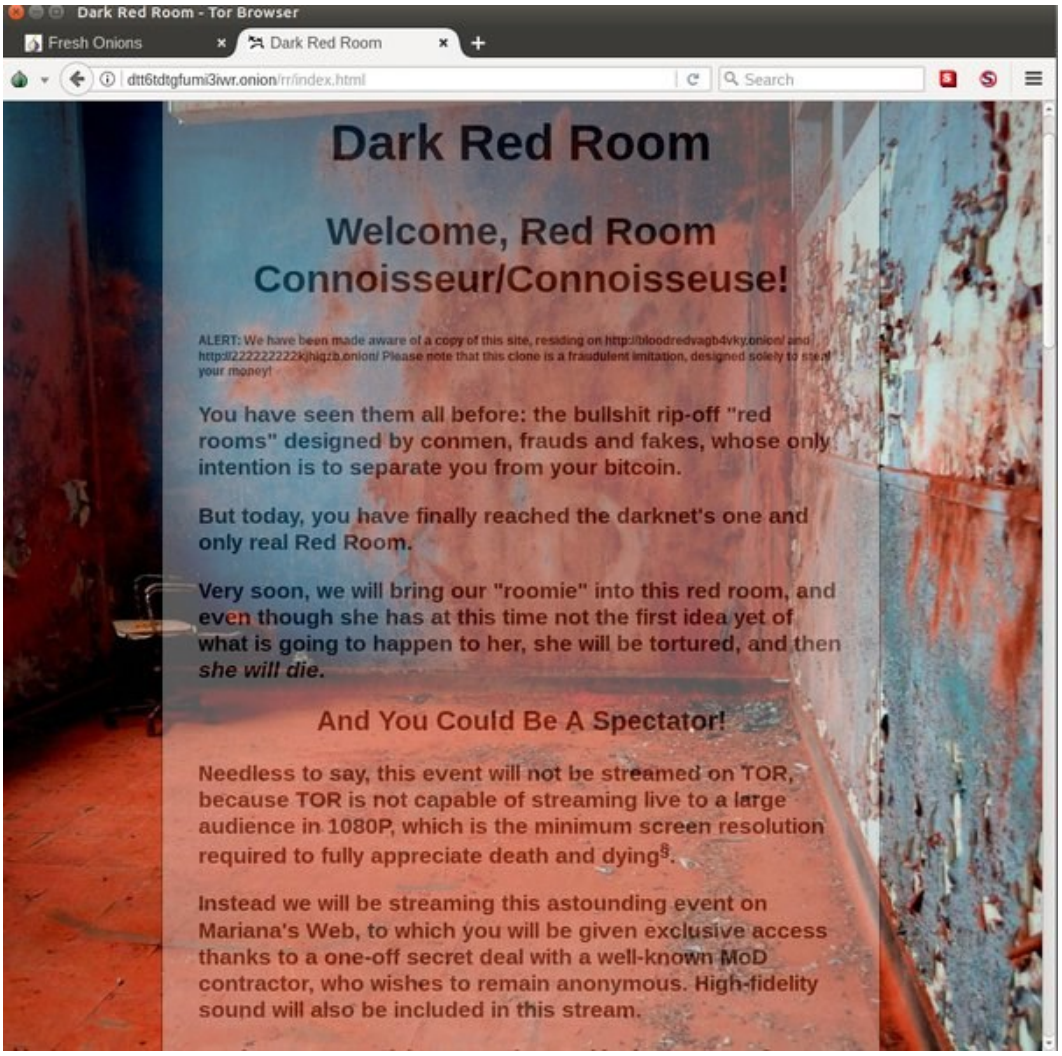
zákazníků objednávky, u kterých vyžaduje zaplacení předem. Pokud však zákazník zboží zaplatí, v tomto případě mu objednané zboží nikdy nedorazí. Jedná se tedy o velmi jednoduchý podvod, kdy podvodník získá kryptoměnu zákazníka. Avšak provozovatel e-shopu může být dopaden, toho si je velmi dobře vědom, proto využívá exitovou strategii, která může zahrnovat několik prvků.

Ve většině případů, pokud prodejce ví, že udělal chybu a může se na něj přijít, může aplikovat například zničení dat, které by mu při odhalení byly akorát na škodu. V podstatě všichni obchodníci, ale vědí, co dělají, a proto používají falešné identity, šifrované zprávy, VPN anebo změny IP adres, aby k jejich odhalení nedošlo.[40]

7.3 Hoax

Hoaxy jsou informace a zprávy, které jsou šířeny za účelem rozšíření dezinformace a také vyvolání paniky. Nebo mohou být cíleny na osoby z důvodu manipulace. Hoaxy se mohou týkat všemožných témat, ale pro podvodníky, kteří tyto zprávy šíří, slouží k tomu, aby vyvolaly strach v důvěřivých osobách, kteří na ně narazí anebo k získání osobních údajů či finančních prostředků.

Asi nejznámějším hoaxem, který se na darknetu šíří jsou takzvané „red rooms“. Jedná se o živé přenosy nebo videa, na kterých se nachází obtěžování, mučení, vraždy a jiné nechutné záběry, které mohou lidé sledovat a za případný poplatek také vymyslet nebo vybrat, co se má s obětí dít dále. Jak už bylo ale řečeno, jedná se většinou o hoax nebo o přehnané spekulace. Povědomí o „red rooms“ se šíří hlavně v souvislosti s extrémní brutalitou, šílenstvím a zvráceností. I přes tyto domněnky nebyly nikdy nalezeny důkazy, že by tyto služby existovali a opravdu se vysílaly v přímém přenose. [40,41]



Obrázek č.6: Falešná red room webová stránka [62]

7.4 Terorismus

Jelikož darknet není tolik monitorován, jako je tomu u běžné otevřené vrstvy internetu, objevují se zde videa a zprávy, které mohou souviset s terorismem. Může se jednat o záběry, které znázorňují popravy, přestřelky anebo jiné brutální činy, které zástupci teroristických skupin mohou natočit.

Nemusí se jednat pouze o videa a zprávy, ale člověk je schopen se dostat až uzavřených skupin, které mohou temné části internetu využívat k anonymní komunikaci mezi sebou a také plánování různých brutálních aktivit. Bohužel díky anonymitě tato forma komunikace umožňuje organizovat útoky a šířit svoji ideologii bez odhalení jejich identity. Teroristické skupiny zde šířením své propagandy využívají komunikaci pro rekrutování nových osob a zapojování jich do teroristických činností.

Tyto skupiny také ve velkém využívají nelegálních nákupů zbraní a dalších materiálů, například výbušnin nebo materiálů, ze kterých se výbušnina dá vyrobit. K získání prostředků na tyto činy jim pomáhá praní špinavých peněz, nelegální obchodování nebo podvody s kryptoměnami, které byly popsány v dřívější kapitole. Ve skupinách se objevují i hackeři a experti. Ti pomáhají skupinám s kybernetickými útoky, vývojem různých škodlivých softwarů nebo nelegálním obchodováním. [39,40]

7.5 Phishing

Nejvíce podvodů vzniká za použití starého dobrého phishingu. Jedná o typ podvodu, kdy se útočník snaží získat citlivá data uživatele ať už během elektronické komunikace nebo pomocí škodlivého softwaru.

Hlavní technikou pro získání těchto dat, jsou falešné URL adresy, kdy útočník zamění znění této adresy, ale pouze takovým způsobem, kterého si běžný uživatel nemusí na první pohled všimnout. Díky prokliknuti na falešnou stránku se uživatel může dostat například na tržiště, které je vytvořené pouze za účelem získání osobních informací uživatele, jako jsou přihlašovací údaje. Stránky jsou navrženy tak, aby běžný uživatel nepoznal rozdíl od skutečných stránek. V případě darknetu tyto podvody mohou být jednodušší, protože spousta neškolených uživatelů stránky na této části internetu ani nezná a neví, jaké mohou mít podoby. Na těchto stránkách, ale i na těch, které nejsou přetvořeny na falešné, se mohou objevovat škodlivé soubory, ty mohou být schované jenom za odkazy, které nevypadají nijak podezřele. Pokud uživatel na tento odkaz klikne a začne stahovat malware, po jeho stažení začne program prohledávat jeho zařízení za účelem nalezení citlivých informací. Pokud program nalezne například sken občanského průkazu, je možné, že podvodník ji později bude nabízet na nelegálních tržištích k zakoupení nebo jenom k prohlédnutí, což je samo o sobě velkým problémem.

Anonymita, jenž darknet poskytuje, je komplikací pro boj proti phishingovým útokům a je těžké podvodníky vysledovat a dostihnout. Z tohoto důvodu by uživatelé, kteří se na darknetu pohybují, by měli dbát na opatrnost a pečlivě zkoumat autentičnost stránek a odkazů, co se objeví před nimi. Díky phishingu a jeho taktikám si podvodníci mohou přijít na finanční odměny a nemusí nikdy být dopadeni, proto se tyto podvody neustále vyvíjí a rozšiřují, a to nejen ve světě temného webu. [40]

8 KRIMINALITA NA DARKNETU

V předchozích kapitolách byly popsány rizika, se kterými se člověk při použití temné strany internetu může setkat. Spousta těchto podvodů a nelegálních činností byla ale odhalena policií a pachatelé byli dopadeni a dále byly mediálně rozšířeny. V této kapitole budou popsány jedny z nejznámějších případů, které s nelegálními činnostmi na darknetu jsou spojené a jaký čekal jejich pachatele osud.

8.1 Tržiště Silk Road

Pravděpodobně nejznámější, nejrozšířenější a nejkontroverznější online tržiště v historii, které se na darknetu kdy objevilo. Historie této stránky sahá do roku 2011, kdy byla poprvé spuštěna. Toto tržiště založil tehdy 27letý Ross Ulbricht, který měl přezdívku Dread Pirate Roberts, neboli Strašlivý pirát Roberts. Tento pseudonym je jméno z knihy Princezna nevěsta od spisovatele Williama Goldmana a jméno se předávalo jako titul z jednoho hrdiny na druhého. Silk Road bylo v roce 2013 uzavřeno FBI a Ross Ulbricht si odpykává doživotní trest ve vězení.

Díky kombinaci technologie anonymizace dat, obchodních platforem a systému určité zpětné vazby byl Silk Road jasná volba pro obchodníky s drogami. Tržiště bylo přístupné pouze přes prohlížeč Tor, která zajišťovala anonymitu uživatelských dat a aktivit. Jelikož Tor zakrývá adresy a nikdo nebyl schopný jejich činnost vystopovat, Silk Road, Tor a kryptoměny byly v té době nejlepším nástrojem pro nelegální obchodování. Jedním z důvodů, proč se Silk Road stal oblíbeným, byla možnost zpětné vazby od zákazníků, tato funkce byla implementována přímo na stránce a zákazníci psali hojně po recenze po obdržení jejich produktu. Bohužel však tyto recenze a zpětné vazby vedly k tomu, že podvodní prodejci byli odhaleni a ti, kteří zboží opravdu posílali si upevňovali svoji pozici na trhu. Na tržišti se prodávalo spousta nelegálních věcí, ale nejoblíbenějším byly drogy Jmenovitě od slabších, jako je marihuana až po tvrdé jako heroin a další. Uživatelé často nebyli omezeni ani množstvím a mohli si objednat drogy v různých platformách a různých množstvích.

Obrázek č.7: Úvodní stránka tržiště Silk Road [63]

Dostupné zboží a služby byly poskytovány více než 100 000 zákazníkům a během 2 a půl roku existence tohoto tržiště generovala prodeje v hodnotě 183 milionů dolarů a provize ve výši 13 milionů dolarů. Tyto částky se odvíjí od hodnoty Bitcoinu, kterým se na platformě platilo, kterou tato kryptoměna měla v době transakcí.

Konec Silk Road přišel v roce 2013 a to poté, co FBI ve spolupráci DEA (Úřad pro potírání drog), IRS (Hlavní finanční úřad Spojených států) a celníků vypátrala původ této stránky. Tyto útvary přiznaly, že i když jim v řešení tohoto případu značně překážela anonymita, kterou Tor a anonymizace, dokázali tyto faktory potlačit a uzavřít největší trh s drogami na světě. Po uzavření stránky FBI zabavila přes 144 000 Bitcoinů, které tehdy měly hodnotu okolo 34 milionů dolarů a také dostala za mříže několik uživatelů stránky, včetně hlavního zakladatele Rosse Ulbrichta. Ten si během existence tohoto tržiště přišel na přibližně 80 milionů dolarů. Ross Ulbricht byl v roce 2015 poslán do vězení odsouzen na doživotí za praní špinavých peněz, hackerství a obchodování s falešnými dokumenty a drogami. Jeho trest mu neumožňuje možnost podmínečného propuštění.

Jeho zatčení doprovázelo několik kontroverzí. Vícero osobností se veřejně přihlásili k jeho podpoře, jelikož se jim doživotní trest zdál moc přísný na to, že Ulbricht měl před Silk Road bezproblémový život a nespáchal nikdy žádný násilný čin. Později také vznikla internetová stránka, která nese název Free Ross Ulbricht a ta žádá o prezidentskou milost

prostřednictvím peticí, jenž se rozhodlo podepsat necelých 600 000 osob. Stránka popisuje jeho život, nespravedlivost jeho odsouzení vůči ostatním zúčastněným na případu Silk Road a také zobrazuje počet dní, které Ulbricht už ve vězení strávil. [42,43,44,45]

Obrázek č.8: Plakát podporující Ulbrichta [64]

8.2 Daisy's Destruciton

Tento případ se točí kolem stránky s názvem No Limits Fun a jejího provozovatele Petera Scullyho, který je považován za nejhoršího a nejodpornějšího pedofila na světě.

Peter Scully se narodil v roce 1963 v Austrálii a zpočátku žil úplně normální život. Nic nenaznačovalo tomu, že by měl být takovou zrůdou, jaká se z něho později vyklubala. Scully podle lidí, kolem kterých se dříve pohyboval velmi inteligentní a charismatický člověk. V rodné Austrálii zpočátku žil běžný život se svou manželkou a dvěma dcerami. V roce 2011 se však něco v jeho životě změnilo a jakožto podnikatel s nemovitostmi provedl podvod, který investory stál více než 2,5 milionu dolarů. Aby nemohl být z tohoto podvodu obviněn, utekl do Manily na Filipíny a vše, co měl doma, včetně manželky a dcer nechal za sebou v Austrálii. Australská komise po jeho uprchnutí na Filipíny přišla na to, že Scully byl zapleten do 117 podvodů souvisejících s podvody s nemovitostmi.

Jak sám prohlásil velkým zvratem v jeho životě bylo, když ho zneužil při dospívání kněz. Jeho řádění započalo až na Filipínách, kde údajně založil spolek pro zneužívání dětí a jejich záznamy nabízel na darknetu za poplatky. Neoperoval sám, ve spolku působilo několik dalších predátorů a násilníků. Oběti Scully sháněl od chudých rodin, kterým nalhával, že jejich dětem se dostane šance na vzdělání nebo pracovní příležitosti. V těchto praktikách mu pomáhali jeho dvě přítelkyně, které si na Filipínách našel, Carme Ann Alvarez a Leizyl Margallo. Nejznámějším a nejbrutálnějším případem se stalo video s Daisy's Destruciton. Toto video prodával na svých stránkách klientům za 10 000 dolarů. Ve videu bylo znázorněno znásilnění a mučení tří mladých dívek, jedné z dívek bylo jedenáct let, druhé dvanáct let a poslední pouhých 18 měsíců. Právě nejmladší z obětí se jmenovala Daisy a podle ní bylo toto video pojmenováno.

Video si rychle získalo pozornost a jedním z osob, kterým se nahrávka dostala do ruky byl Matthew Graham, jeden z největších distributorů dětské pornografie, který byl na darknetu známý přezdívkou Lux. Ten však video po nějaké době zveřejnil, a to vedlo k tomu, že se dostalo až do rukou policie. Nizozemský tým pro vykořisťování dětí ihned započal vyšetřování s cílem najít oběti a také bylo zahájeno mezinárodní pátrání po osobách, které za tyto činy byli zodpovědné. Jediné vodítko, které se policii pomohlo, bylo zjištění, že video pochází z Filipín. Velký zlom přišel na přelomu let 2014 a 2015, kdy se policejní stanici v Malaybalay objevily dvě dívky, které na zveřejněné nahrávce figurovaly a všechny činy nahlásily, což vedlo k identifikaci Scullyho. Ten byl dopaden 20. února 2015 mezinárodní policií. Podle zdrojů byl Scully obviněn ze 75 případů znásilnění dětí a byli objeveni i jeho komplicové, kteří byli z Německa, Brazílie a Filipín. Mezitím co byl Scully ve vězení a čekalo se na jeho rozsudek, říjnu roku 2015 vypukl požár v důkazní místnosti, a to vedlo k poškození a zničení všech klíčových důkazů. Lidé věřili, že násilníci podplatili místní policii, aby tuto místnost podpálil, protože korupce na Filipínách byla častá. I přes zničení důkazů byl Scully v roce 2018 obviněn a odsouzen na doživotí i spolu s jeho komplici. Místní úřady dokonce přemýšleli o znovuzavedení trestu smrti. V roce 2022 byl Scully souzen podruhé a soud mu přidal dalších 129 let ve vězení. Peter Scully je důkazem, že existují lidé mnohem horších rozměrů, než si dokáže někdo představit. [46,47]

8.3 Nájemná vražda

Tato kapitola popisuje případ amerického doktora Jamese Wana, který si v roce 2022 objednal na darkwebu vraždu svoji tehdejší přítelkyně. Přesné informace o tom, proč se Wan chtěl své přítelkyně zbavit nejsou jisté.

Vše začalo 18. dubna 2022, kdy se James Wan pomocí svého telefonu připojil k darknetu a vyhledal dostupné služby nájemného vraha. Když vyplňoval objednávku, tak zde vypsal základní údaje jako je jméno, adresa, facebookový účet a popis a registrační značku auta, které jeho přítelkyně používala. Wan také mohl napsat nějaký speciální požadavek, což také provedl a do zprávy uvedl „*Můžete vzít peněženku, telefon a auto. Střelte a běžte. Nebo si vezměte auto*“. Po odeslání objednávky Wan převedl zálohu, která činila 50 % z celkové částky, kterou vrah požadoval a to přibližně 8 000 dolarů, které zaslal v Bitcoinu.

Wan po dvou dnech kontaktoval správce stránky, že se jeho transakce neukazuje na jeho výpisu, a tak se zajímal, zda je vše v pořádku. Den na to mu správce stránky odepsal s tím, že chce, aby mu Wan poslal adresu Bitcoinové peněženky, na kterou platbu zaslal, což také Wan udělal. Vše probíhalo naprosto stejně, jako při běžných problémech s transakcemi v normálním životě, správce se Wanovi snažil celou dobu radit a pomáhat. Poté, co správce obdržel adresu a snímek obrazovky, kde byla provedená transakce, odpověděl, že tato adresa není ani v jejich systému a že Wan udělal chybu. Musel tedy poslat dalších 8 000 dolarů na novou adresu a zde už dostal potvrzení, že transakce proběhla. Poslední zpráva, která mezi vrahem a Wanem proběhla byla „*Nehoda nebo normální střelba?*“, odpověď zněla „*Nehoda je lepší*“.

O týden později provedl další transakci v hodnotě 8 000 dolarů, která bylo potřebná k dokončení kontraktu. Snažil se ještě zjistit informace jako jak dlouho to bude trvat, nebo jaký je pokrok, ale odpovědi se mu nedostalo. Později na účet doplnil ještě dalších 1 200 olarů z důvodu poklesu kurzu Bitcoinu. Celkově tak náklady tvořily více než 25 000 dolarů.

Nic z toho, co si Wan domluvil však nedopadlo. FBI velmi brzy obdržela od anonymního zdroje tip, že se vražda chystá. Tento tip měla být organizace lidí, kteří velmi pravidelně kontrolují příspěvky na fórech, kde objednávka proběhla, aby právě bylo zamezeno těmto činům. FBI tak okamžitě zasáhla, přítelkyni umístila do bezpečí a zatkla Jamese Wana. Ten se ke všemu ihned přiznal a všechny záznamy z jeho telefonu jeho přiznání potvrdily. Vraždu musel okamžitě zrušit a o všechny peníze přišel. Po obvinění z pokusu o najmutí vraha byl Wan odsouzen na více než 7 let ve vězení. Tato událost ukazuje, že i přes

anonymitu na temného webu FBI a ostatní organizace stále aktivně bojují proti násilným a nelegálním zločinům a snaží se chránit občany. [48]

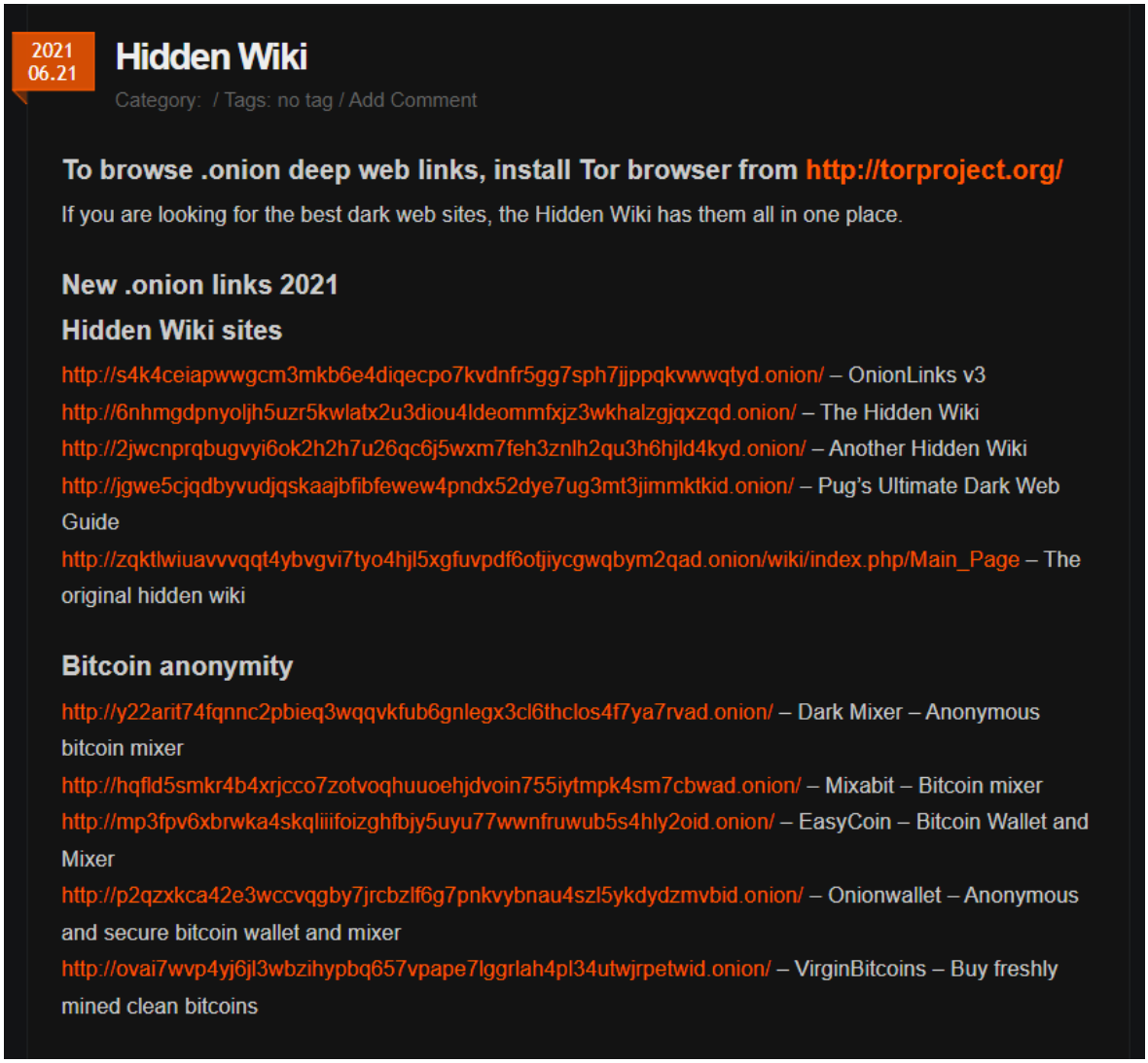
9 ROZCESTNÍKY

Rozcestníky darknetu by se daly popsat jako webové stránky, které poskytují seznamy odkazů, díky nimž se lze dostat na temnou stranu internetu. Protože z běžných prohlížečů se na darknet dostat nedá a odkazy na tyto stránky nebylo dříve možné běžně najít, vznikly seznamy a ty obsahují přímo onion odkazy, které lze vložit do Toru. Tyto rozcestníky mohou být rozděleny do kategorií, například tržiště, fóra, politika nebo erotika. Seznamy jsou pro uživatele darknetu užitečným nástrojem, jelikož bez přímých odkazů je velice obtížné konkrétní stránku najít. Spousta rozcestníků se snaží obsah odkazů filtrovat, aby se uživatel nedostal do problémů na nelegálních stránkách, ale toto riziko stále existuje a pokud si uživatel nedá pozor, může být zatažen do podvodu nebo nějakého útoku. Existuje sousta volně dostupných rozcestníků a mezi nejznámější patří TheHiddenWiki nebo Fresh Onions.

The Hidden Wiki je jedna z nejstarších a nejznámějších stránek tohoto typu. Obsahuje širokou škálu odkazů, které jsou řazeny do různých kategorií jako tržiště, politika, fóra a další. The Hidden Wiki je provozována dobrovolníky, kteří nemají mezi sebou jednoho určitého správce, a tak mohou být odkazy často nefunkční z důvodu nepravidelné aktualizace. Vše závisí na aktivitě daných dobrovolníků. I přes to se však na stránce objevuje spousta odkazů, které mohou začátečníkům, kteří jdou navštívit darknet poprvé, velmi pomoci a být užitečná.

Fresh Onion funguje na stejném principu, jako The Hidden Wiki. Jeho výhodou je však pravidelnější aktualizace a širší škála odkazů v různých kategoriích. Další možnost je také internetové fórum Reddit, kde uživatelé darknetu a Toru mají svoje kanály, do kterých se mohou další uživatelé přidávat a sdílet mezi sebou zajímavé odkazy, na které narazili při zkoumání darknetu.

Odkazy, která uživatele přesměrují na darknet nevypadají jako běžné odkazy používané na Googlu. Jelikož tyto odkazy často obsahují název stránky a dále několik dalších pro uživatele náhodných znaků, tak je těžké si odkaz zapamatovat. Proto jsou tyto rozcestníky vytvářeny a spravovány, aby nebyla ohrožena anonymita návštěvníka, pokud by si odkazy ukládal do svého zařízení. [9,49]



Obrázek č.9: Rozcestník TheHiddenWiki

II. PRAKTICKÁ ČÁST

10 VYHLEDÁVÁNÍ NA DARKNETU

Praktická část se zabývá vyhledáváním na darknetu a následnému porovnání se surface webem. Jak se moc se vyhledávání liší, jak hluboko se lze díky rozcestníkům dostat. Dále obsahuje krátký dotazník ohledně bezpečnosti a používání internetu.

10.1 Používání prohlížeče Tor

Pro vyhledávání a prohlížení darknetu byl zvolen nejoblíbenější prohlížeč Tor, konkrétně verze 13.0.0. Ten se po instalaci a spuštění zeptá na připojení k síti, to probíhá přes připojení na proxy servery, které provozují tisíce dobrovolníků po celém světě. Uživatel dostane volbu, zda si připojení chce nastavit sám nebo při každém spuštění připojit k síti automaticky. Po připojení se načte samotná vyhledávácí stránka, v případě verze 13.0.0. se načte vyhledáváč DuckDuckGo, který je od verze 6.0.6 primárním vyhledávačem prohlížeče Tor. Je tomu tak z toho důvodu, že DuckDuckGo nezaznamenává, neshromažďuje ani sdílí osobní údaje nebo historii vyhledávání, a proto ho Tor používá jako nejlepší volbu pro anonymní vyhledávání. Další důležitá funkce je povolení vyhledávání onion stránek. Pokud uživatel tuto funkci nepovolí, nebude moct vyhledávat žádný jiný obsah než stránky, které jsou běžné dostupné na surface webu. Uživatel však normální stránky jako Google nebo Facebook může jednoduše vyhledat a používat.

Každý vyhledaný výraz anebo načtená stránka uživateli ukazuje, kudy vede řetězec sítí, přes které je ke stránce připojený. Zobrazují se zde 3 uzly mezi prohlížečem a danou stránkou. První uzel je takzvaný „Guard“ (česky „Strážce“) a ten kontaktuje prohlížeč, když se chce připojit do Tor sítě. Tento uzel je nezbytný pro zachování bezpečnosti a anonymity uživatelů. Slouží k minimalizaci rizika útoků, které mohou být například útoky k odhalení skutečné IP adresy zařízení, takzvané „korelační útoky“. Každý z těchto 3 uzlů může, ale nemusí být pokaždé v jiném státě. Uživatel má také možnost si tento řetězec znovu vygenerovat, což může vést i opakovanému načtení stránky. Při tomto generování však Guard zůstává většinou stejný, na což samotný prohlížeč upozorňuje, protože Guardy jsou pečlivě vybírány a udržovány v rámci této sítě.

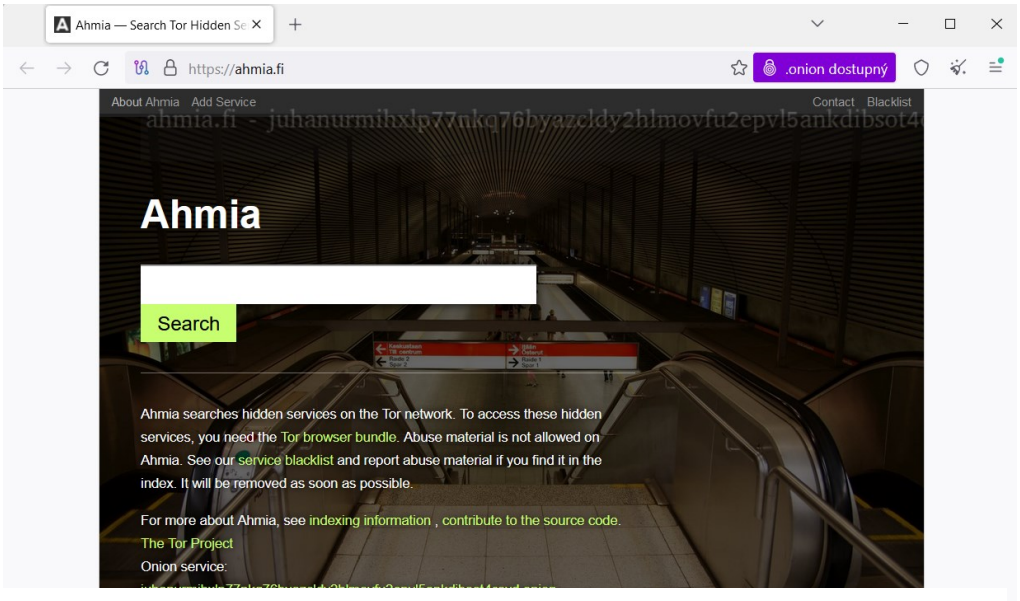
Dále také tyto uzly ovlivňují geolokační přesměrování. Například stránka Googlu může na základě IP adresy, kterou má přiřazenou od výstupního uzlu Tor sítě, přesměrovat uživatele do verze pro jinou zemi. Pokud je výstupní uzel například v Německu, pravděpodobně se

Google načte v němčině a bude předpokládat, že má vyhledávat stejné výsledky jako by vyhledával přímo pro Německo.

Při vyhledávání si uživatel také jistě všimne, že načítání stránek a prohlížeče není tak rychlé, jako například v Google Chrome. To je způsobeno několika důvody. Prvním důvodem je právě cesta přes několik uzlů sítě. Cesta může být složitější a další než přímé spojení mezi prohlížečem a serverem, jak to bývá u běžných prohlížečů. Dále je každý uzel zodpovědný za šifrování a dešifrování dat. Tor také může být přetížen kvůli počtu uživatelů a aktivit v síti. Některé stránky mohou být blokované pro přístup přes Tor síť, což buď může připojení zpomalit nebo úplně připojení znemožnit. Dalšími důvody také může být nízká dostupnost výstupních uzlů nebo dynamická změna cesty v síti.

10.2 Vyhledávání napříč prohlížeči

Prohledávání temné části internetu se může zdát zprvu jako zábavná činnost, při které je možné narazit a spousty zajímavých věcí, ale opak je často pravdou. Většina stránek je opravdu nudná a nenabízí nic moc zajímavého. Při prohledávání je větší šance narazit na opuštěné stránky, které nikdo nespravuje a nic nenabízí než na zajímavé informace. Pokud uživatel neví, kde hledat, nebo jaké nástroje použít, vyhledávání může zabrat opravdu dlouhou dobu. Proto je pro vyhledávání dobré použití rozcestníků, které byly popsány v teoretické části. Nejznámějším rozcestníkem pro onion odkazy je pravděpodobně TheHiddenWiki, ale jelikož není tak často aktualizována, odkazy bývají často nefunkční. Existuje však také webová stránka s názvem Ahmia.



Obrázek č.10: Rozcestník Ahmia

Tato stránka slouží jako přímý rozcestník mezi klasickým vyhledáváním pomocí klíčových slov a onion odkazů. V tomto případě pak lze jasně vidět, jak se vyhledávání liší, protože při zadání běžné fráze, kterou uživatelé internetu používají denně, web Ahmia vypíše odkazy na stránky, které jsou spojeny s nelegální činností. Stránka funguje na takovém principu, že do vyhledávácí lišty je zadán hledaný výraz, například „facebook“. Ahmia tento výraz přijme a zpět pošle několik odkazů, které jsou převedeny do onion formátu. Jediné, co tento vyhledávač blokuje, je pornografie a urážlivý materiál.

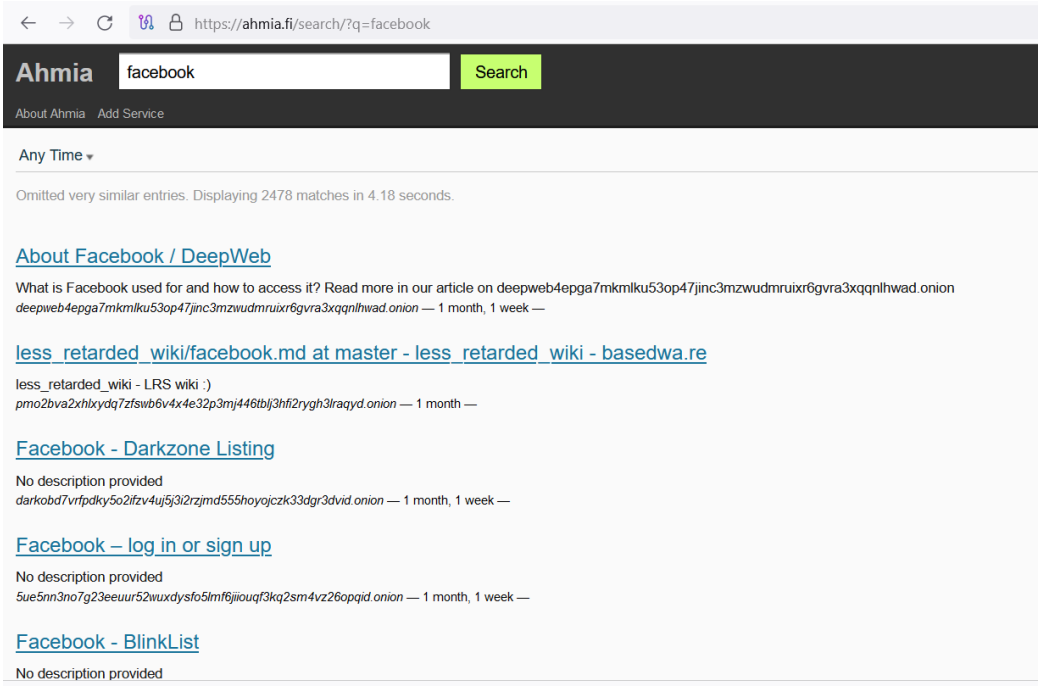
I přesto, že tento rozcestník nabídne velké množství odkazů za pár sekund, načítání samotných stránek trvá i několik minut a často se ani nenačtou nebo nabízejí odkaz na jinou stránku nebo na jiný rozcestník. Například funkční odkaz, který přesměrovává na skutečný facebook, byl až čtvrtý možný z nabízených a není vyloučeno, že odkaz není falešný a slouží k získání přihlašovacích údajů, protože při zadávání údajů nebyly znaky hesla skryty za tečky nebo symboly, jak je běžné.

Dalším rozdílem je také přibližný počet vyhledaných výsledků napříč různými vyhledávači. Při posuzování vyhledávání daného výrazu mezi třemi vyhledávači, tedy Google, Ahmia a DuckDuckGo se počet výsledků značně liší. Hledaným výrazem bylo slovo „facebook“. Výsledek vypadal takto.

Tabulka č.1: Porování výsledků vyhledávání „facebook“

Vyhledávač	**Doba trvání**	**Přibližný počet výsledků**
Google	0,28 s	25,270 mld
Ahmia	4,18 s (Google Chrome) 3,94 s (Tor)	2 478 (Chrome) 2 478 (Tor)

DuckDuckGo v tabulce není zahrnuto z důvodu, že tento prohlížeč nezobrazuje ani dobu trvání vyhledávání a ani počet výsledků. Je tomu tak z toho důvodu, že využívá způsob vyhledávání, který je velmi přesný, to znamená, že každý symbol vyhledávání je brán v potaz. Ostatní prohlížeče mohou hledané výrazy trochu pozměnit a také v případě Google, jsou hledané výrazy filtrovány.



Obrázek č.11: Vyhledávání na Ahmia

Po vyhledávání běžných výrazů, které jsou víceméně všude stejné je také ale zajímavé vyzkoušet vyhledávání věcí, které si běžný uživatel nevyhledává každý den a které uživatele na rozcestníku zavedou na temnější místa. Například výraz „weapons“, tedy zbraně. Výraz „weapons“ zadaný do vyhledávače Google vyhledá očekávané výsledky. Mezi výsledky se nejprve objeví odkaz na stránku Wikipedie, co to zbraně vlastně vůbec jsou. Další odkazy směřují podobným směrem. Jedná se o různé seznamy, kde jsou zbraně rozděleny podle použitelnosti a dalších faktorů. Ve všech případech se jedná pouze o dokumenty nebo články. Pokud je však vyhledáno „weapons shop“, objeví se stránky, které nabízí buď airsoftové zbraně plynové. Některé obchody nabízí i zbraně, na které je potřeba zbrojní průkaz, ale ty prodávají pouze na osobní odběr po předložení průkazu. Ve vyhledávači Ahmia je tomu však opět jinak. Nabídka desítek online obchodů, kde je možné sehnat nelegálně zbraň jakéhokoli typu, ale také různá fóra, na kterých uživatelé diskutují výrobu ať už zbraní nebo nábojů. DuckDuckGo poté vyhledá podobné výsledky jako Google, ale ty nejsou tolik filtrované. Následný počet výsledků se liší takto.

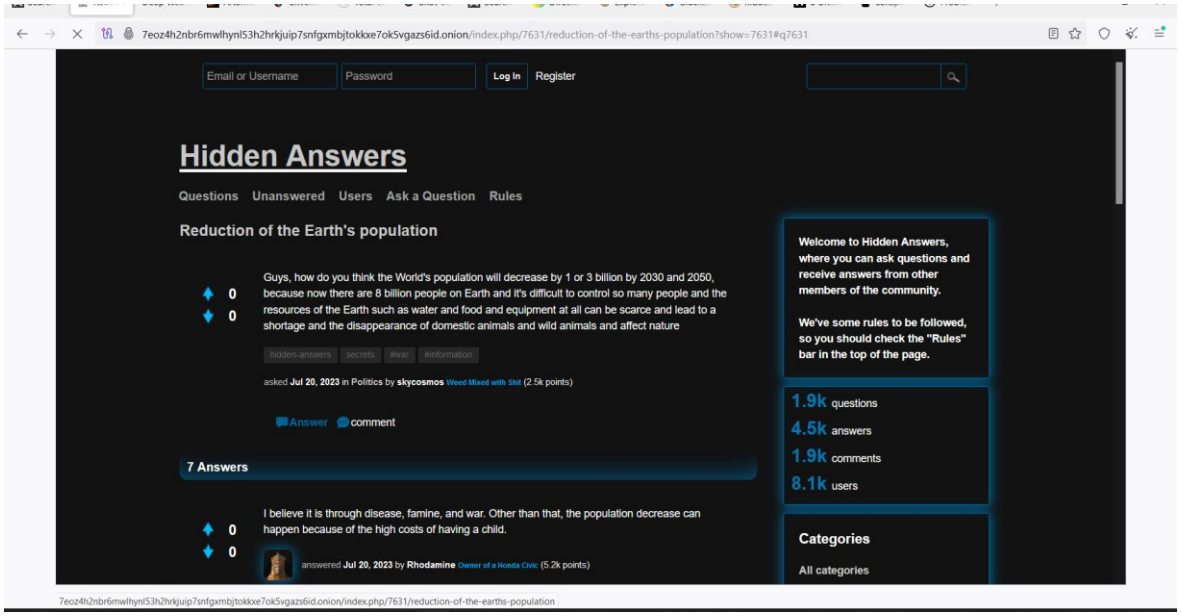
Tabulka č.2: Porovnání vyhledávání výsledků „weapons“

Vyhledávač	**Doba trvání**	**Přibližný počet výsledků**
Google	0,36 s	1,830 mld
Ahmia	2,24 s (Google Chrome) 1,67 s (Tor)	2 478 (Chrome) 768 (Tor)

Dalším hledaným výrazem bylo spojení „conspiracy theories“, tedy konspirační teorie. Témata nejrůznějších konspiračních teorií hýbou společností a spousta z nich má své příznivce, kteří jim věří a shromažďují důkazy a podklady, které následně sdílejí na internetu. Vyhledávač Google vyhodil odkazy na stránky, které popisují, co to konspirační teorie jsou a jaké konkrétní existují nebo které jsou oblíbené. Rozcestník Ahmia však vyhledal stovky odkazů na různá fóra, kde uživatelé píší své poznatky nebo předkládají důkazy o daných konspiračních teoriích. Dále se na rozcestníku nachází velké množství stránek, které konkrétní konspirace popisují a přikládají desítky odkazů na údajné důkazy. Jelikož samotný rozcestník Ahmia neposkytl takové množství odkazů jako předtím, byl použit i rozcestník Torch. Odkazy z těchto rozcestníků také vedly na stránku „Hidden Answers“, což je velké anonymní diskuzní fórum využívané k pokládání otázek, na které se nedají dohledat často odpovědi nebo si zde uživatelé objasňují různé konspirační teorie.

Tabulka č.3: Porovnání vyhledávání výsledků „conspiracy theories“

Vyhledávač	**Doba trvání**	**Přibližný počet výsledků**
Google	0,28 s	86,4 mil
Ahmia	2,70 s (Google Chrome) 1,75 s (Tor)	1 150 (Chrome) 697 (Tor)
Torch	-	211 (Tor)



Obrázek č.12: Fórum Hidden Answers

Zajímavým výrazem pro vyhledávání byl také „hacking“. Google nabízí obrovské množství odkazů, kdy většina z nich popisuje, co je to hacking, kdo je hacker, jaká je jeho práce a jak se hackování bránit. Dále je možné najít i informace o různých kurzech, které je možné absolvovat a prohloubit tak své znalosti v této problematice. Některá fóra nebo stránky se tváří jako, že jsou schopny někoho naučit hackovat, ale realita je jiná a žádné konkrétní postupy, díky kterým se laik dokáže naučit nabourat do cizího zařízení k dohledání nejsou. Rozcestník Ahmia pak především nabízí odkazy na online obchody, kde je možné si hackera objednat na jakoukoli práci. Další možností je zakoupení ukradených nebo hacknutých účtů na různé platformy a sociální sítě, jako je Instagram, WhatsApp nebo Steam. Lze zde objevit i odkazy na různé softwary, jež by s hackováním mohli někomu pomoct, ale s velkou pravděpodobností jediný, kdo bude obětí hackování bude uživatel, který si daný software stáhne. Jsou zde také návody na hackování nejrůznějších platforem nebo dokonce i mobilních operačních systému. Tento výraz nabízí opravdu rozmanití výběr odkazů a možností.

Tabulka č.4: Porovnání vyhledávání výsledků „hacking“

Vyhledávač	Doba trvání	Přibližný počet výsledků
Google	0,28 s	550 mil
Ahmia	3,33 s (Google Chrome) 3,33 s (Tor)	1 970 (Chrome) 1970 (Tor)
Torch	-	39 283 (Tor)

Posledním výrazem je slovo „drugs“. Tento výraz je vyhledáván z toho důvodu, že je to pravděpodobně první věc, kterou si spousta lidí představí, když se řekne slovo darknet. Lidem se vybaví nelegální obchody, na kterých se dají drogy a různé prášky pro přípravu daných drog sehnat. A jejich mínění je správné. Ahmia a Torch vyhledávají obrovské množství online obchodů s drogami. V těchto obchodech je na výběr ze spousty dostupných i nedostupných drog, a hlavně v neomezeném množství. Je možné objednat například 2 gramy nějaké odrůdy marihuany, ale také gramů klidně 50. Obchody jsou to, co mezi odkazy dominuje, ale je při důkladnějším prohledávání se dá narazit i na fóra, kde je popsáno, jak si například vytvořit doma amfetamin. Výroba je zde popsána krok po kroku, s přesným množstvím jednotlivých látek, včetně chemických vzorců a odborných popisů. Na dalších fórech lze dohledat prodejce ale i kupce, kteří drogy prodávají na ulicích. Na určitém fóru se stačí překliknout do konkrétní země a dále se bez problému domluvit s dealery na setkání a koupi látek. V rámci drog je darknet opravdu rozmanité místo a nabízí nespočet možností, na rozdíl od Googlu, který je opět vyfiltrován a zbaven všech potencionálně nebezpečných stránek. Znovu se na Googlu nachází pouze informativní články a dokumenty, seznamy, historie a především následky, jaké užívání může mít.

Tabulka č.5: Porovnání vyhledávání výsledků „drugs“

Vyhledávač	Doba trvání	Přibližný počet výsledků
Google	0,30 s	8,920 mld
Ahmia	3,30 s (Google Chrome) 3,30 s (Tor)	1 710 (Chrome) 1 710 (Tor)
Torch	-	34 511 (Tor)

10.2.1 Shrnutí

V rámci této studie byly porovnávány výsledky vyhledávání různých výrazů na Googlu a na darknetu. Zatímco výsledky na Googlu byly převážně legální a informačního charakteru, výsledky na darknetu často obsahovaly odkazy na nelegální činnosti, jako jsou obchod s nelegálním zbožím nebo službami. Výsledky vyhledávání na Googlu poskytovaly široké spektrum informací z legálních zdrojů, jako jsou zpravodajské články, odborné studie a e-shopy. Naopak vyhledávání na darknetu často vedlo na stránky a fóra nabízející nelegální produkty a služby, které byly skryty před běžnými vyhledávači. Tento kontrast ukazuje na významné rozdíly ve funkci a účelu těchto dvou částí internetu.

Tato zjištění mají významné důsledky pro uživatele internetu. Zatímco běžní uživatelé mohou na Googlu snadno nalézt legální a bezpečné informace, vyhledávání na darknetu představuje vysoké riziko, včetně možnosti setkat se s nelegálními aktivitami a potenciálně škodlivým obsahem. Navíc anonymita a šifrování na darknetu komplikují sledování a stíhání těchto aktivit, což představuje další bezpečnostní výzvy.

Pro zlepšení bezpečnosti uživatelů by mělo být zvýšeno povědomí o rizicích spojených a měly by být posíleny technologie a postupy pro detekci a prevenci nelegálních aktivit na darknetu. Spolupráce mezi národními a mezinárodními orgány je klíčová pro účinné řešení těchto problémů.

Závěrem lze říci, že rozdíly mezi výsledky vyhledávání na Googlu a darknetu odhalují klíčové aspekty fungování a bezpečnostních rizik internetu. Zatímco Google slouží jako užitečný nástroj pro legální informace, darknet představuje prostor s vysokými riziky, vyžadující zvýšenou pozornost a regulační opatření. Další výzkum by měl být zaměřen na vývoj účinných technologií a postupů pro identifikaci a prevenci nelegálních aktivit na darknetu.

ZÁVĚR

Tato bakalářská práce se zaměřila na analýzu vrstev internetu, způsoby vyhledávání v nich a jejich související bezpečnostní rizika. Hlavní cíle práce byly analyzovat strukturu a charakteristiky jednotlivých vrstev internetu, popsat způsoby vyhledávání informací v prohlížečích, včetně jejich hlavních funkcí a identifikovat bezpečnostní rizika.

Práce ukázala, že internet se skládá ze tří hlavních vrstev: povrchového webu, hlubokého webu a darknetu. Povrchový web je snadno přístupný prostřednictvím běžných vyhledávačů jako Google a obsahuje převážně legální a veřejně dostupné informace. Hluboký web zahrnuje data a stránky, které nejsou indexovány běžnými vyhledávači, jako jsou databáze a interní firemní stránky. Dark web je pak specifická část hlubokého webu, která vyžaduje speciální prohlížeče, jako je Tor, a je známý svou anonymitou a často nelegálním obsahem.

Vyhledávání v různých vrstvách internetu přináší různé výsledky a rizika. Zatímco vyhledávání na Googlu vede k legálním a informačním stránkám, vyhledávání na dark webu často odhaluje nelegální činnosti, včetně obchodování s drogami, zbraněmi a kradenými daty. Tento kontrast zdůrazňuje potřebu opatrnosti a informovanosti uživatelů o bezpečnostních rizicích spojených s používáním různých částí internetu.

Bezpečnostní rizika se liší podle vrstvy internetu. Povrchový web je relativně bezpečný, ale i zde mohou uživatelé narazit na phishingové stránky a malware. Hluboký web obsahuje citlivá data, která jsou cenným cílem pro kybernetické útoky. Dark web představuje největší bezpečnostní výzvy kvůli anonymitě a nelegálním aktivitám, které se zde odehrávají.

Závěrem lze říci, že tato práce přinesla důležitý přehled o strukturálních a bezpečnostních aspektech různých vrstev internetu a jejich prohlížečů. Vyhledávání a používání internetu by mělo být vždy prováděno s ohledem na potenciální rizika a s využitím nejlepších dostupných bezpečnostních opatření.

SEZNAM POUŽITÉ LITERATURY

[1] NGO ANH, Tuan. *Problémy vyhledávání informací v prostředí Internetu*. Bakalářská práce. Praha: Vysoká škola ekonomická v Praze, 2015.

[2] STATISTA. *Statista*. Online. Dostupné z: https://www.statista.com/. [cit. 2024-05-14].

[3] HOUSER, Pavel. Sciencemag.cz: Historie Internetu v datech. Online. *Sciencemag.cz*. 2017. Dostupné z: https://sciencemag.cz. [cit. 2024-05-14].

[4] CZ.NIC. Jak na internet: Doména, IP adresa, DNS. Online. *Jaknainternet.cz*. Dostupné z: https://www.jaknainternet.cz/page/1261/domena,-ip-adresa,-dns/. [cit. 2024-05-14].

[5] Spot the Difference: Rozdíl mezi Web 1.0, Web 2.0 a Web 3.0. Online. *Spotthedefference.com*. Dostupné z: https://cs.spot-the-difference.info/difference-between-web-1. [cit. 2024-05-14].

[6] ROUSE, Margaret. What is Web 1.0. Online. *Technopedia.com*. 2021. Dostupné z: https://www.techopedia.com/definition/27960/web-10. [cit. 2024-05-14].

[7] MTVSV. Srovnání: Web 2.0 vs. Web 3.0. Online. *Nftspace.cz*. 2023. Dostupné z: https://www.nftspace.cz/vzdelavani/srovnani-web-2-0-vs-web-3-0/. [cit. 2024-05-14].

[8] MISHEVA, Galina. Komise představila novou strategii EU pro web 4.0 a virtuální prostředí. Online. *Digikoalice.cz*. 2023. Dostupné z: https://digikoalice.cz/komise-predstavila-novou-strategii-eu-tykajici-se-internetu-4-0-a-virtualniho-sveta/. [cit. 2024-05-14].

[9] DRBOLA, Vojtěch. *Darknet: mýtus a realita kybernetického prostoru*. Bakalářská práce. Brno: Masarykova univerzita, 2017.

[10] Incognito Forensic Foundation: The Layers of the Web – Surface Web, Deep Web and Dark Web. Online. *Ifflab.org*. 2019. Dostupné z: https://ifflab.org/the-layers-of-the-web-surface-web-deep-web-and-dark-web/. [cit. 2024-05-14].

[11] RÝC, Tomáš. *Analýza Darknetu se zaměřením na forenzní zkoumání*. Bakalářská práce. České Budějovice: Jihočeská univerzita v Českých Budějovicích, 2019.

[12] ACON, Brian. IdentityIQ: THE ORIGINS AND HISTORY OF THE DARK WEB. Online. *Identityiq.com*. 2024. Dostupné z: https://www.identityiq.com/articles/the-origins-and-history-of-the-dark-web/. [cit. 2024-05-14].

[13] MCCORMICK, Ty. Foreign Policy: The Darknet: A Short History. Online. *Foreignpolicy.com*. 2018. Dostupné z: https://foreignpolicy.com/2013/12/09/the-darknet-a-short-history/. [cit. 2024-05-14].

[14] FULLER, Matthew a GOFFEY, Andrew. *Evil Media*. Velká Británie: The MIT Press, 2012. ISBN 978-0262017855.

[15] Mozilla: Získejte prohlížeč, který chrání, co je důležité. Online. *Mozilla.org*. Dostupné z: https://www.mozilla.org/cs/firefox/new/. [cit. 2024-05-14].

[16] *Lynx*. Online. In: Wikipedia: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, 2023. Dostupné z: https://cs.wikipedia.org/wiki/Lynx. [cit. 2024-05-14].

[17] *Links*. Online. In: Wikipedia: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, 2024. Dostupné z: https://cs.wikipedia.org/wiki/Links. [cit. 2024-05-14].

[18] PAUZER, Holly. Adlucent: 71% OF CONSUMERS PREFER PERSONALIZED ADS. Online. *Adlucent.com*. 2016. Dostupné z: https://www.adlucent.com/resources/blog/71-of-consumers-prefer-personalized-ads/. [cit. 2024-05-14].

[19] ČESKÁ REPUBLIKA. Zákon č. 374/2021 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, a některé další zákony. In: *Sbírka zákonů č. 374/2021*. Dostupné z: https://www.zakonyprolidi.cz/cs/2021-374/zneni-20220701/.[cit. 2024-05-14].

[20] DVOŘÁK, Jakub. Chraňte si soukromí a nenechte se vystopovat webovými stránkami. Online. *IDnes.cz*. 2021. Dostupné z: https://www.idnes.cz/technet/internet/ip-adresa-geolokalizace-wifi-anonymni-rezim-supercookies-evercookies-gps-vpn.A210113_082413_sw_internet_dvr. [cit. 2024-05-14].

[21] Most popular web browsers in 2024. Online. *OBERLO.com*. 2024. Dostupné z: https://www.oberlo.com/statistics/browser-market-share. [cit. 2024-05-14].

[22] Browser Market Share Worldwide. Online. *Statcounter.com*. 2024. Dostupné z: https://gs.statcounter.com/. [cit. 2024-05-14].

[23] PLEVNÝ, Marek. *Darknet sítě jako způsob ochrany soukromí uživatelů internetu*. Diplomová práce. Vysoká škola ekonomická v Praze, 2017.

[24] Akademie CZ.NIC. Jak na internet: Funkce webového prohlížeče. Online. *RVP.cz*. 2015. Dostupné z: https://clanky.rvp.cz/clanek/c/Z/19655/jak-na-internet-funkce-weboveho-prohlizece.html. [cit. 2024-05-14].

[25] ŠPULÁK, Ondřej. RSS čtečky přináší vše důležité na jednom místě. Tipy na ty nejlepší. Online. *Computerworld.cz*. 2022. Dostupné z: https://www.computerworld.cz/clanky/rss-ctecky-prinasi-vse-dulezite-na-jednom-miste/. [cit. 2024-05-14].

[26] O funkci Anti-Phishing. Online. *Kaspersky.com*. 2020. Dostupné z: https://support.kaspersky.com/KSCloud/iOS2.0_TR31/cs-CZ/197525.htm. [cit. 2024-05-14].

[27] FIKAR, Jan. Chrome zapíná kontroverzní Privacy Sandbox. Online. *Root.cz*. 2023. Dostupné z: https://www.root.cz/zpravicky/chrome-zapina-kontroverzni-privacy-sandbox/. [cit. 2024-05-14].

[28] *Google Chrome*. Online. In: Wikipedia: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, 2023. Dostupné z: https://cs.wikipedia.org/wiki/Google_Chrome. [cit. 2024-05-14].

[29] Seznamte se s funkcemi, díky nimž se Chrome odlišuje od ostatních prohlížečů. Online. *Google.com*. Dostupné z: https://www.google.com/intl/cs/chrome/browser-features/. [cit. 2024-05-14].

[30] HOLUB, Vratislav. Proč skončil prohlížeč na Windows? Apple by jej mohl po letech vrátit zpět. Online. *Jablíčkář.cz*. 2022. Dostupné z: https://jablickar.cz/proc-skoncil-prohlizec-na-windows-apple-by-jej-mohl-po-letech-vratit-zpet/. [cit. 2024-05-14].

[31] JANÍČEK, Jaroslav. Safari Recenze. Online. *5nej.cz*. 2022. Dostupné z: https://www.5nej.cz/safari-recenze/. [cit. 2024-05-14].

[32] *Microsoft Edge*. Online. In: Wikipedia: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, 2024. Dostupné z: https://cs.wikipedia.org/wiki/Microsoft_Edge. [cit. 2024-05-14].

[33] *Mozilla Firefox*. Online. In: Wikipedia: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, 2024. Dostupné z: https://cs.wikipedia.org/wiki/Mozilla_Firefox. [cit. 2024-05-14].

[34] SOUCET. Firefox Monitor – často kladené dotazy. Online. *Support.mozilla.org*. Dostupné z: https://support.mozilla.org/cs/kb/firefox-monitor-casto-kladene-dotazy. [cit. 2024-05-14].

[35] MAKOVSKÝ, Jiří. Inflace kryptoměny – jak funguje, co ji způsobuje a na co dávat pozor. Online. *Trade.cz*. 2023. Dostupné z: https://www.tradecz.cz/inflace-kryptomeny-jak-funguje-co-ji-zpusobuje-a-na-co-davat-pozor/. [cit. 2024-05-14].

[36] HEDVIGY, Ľubomír. TOP softwarové peněženky pro kryptoměny (2023) – Kterou vybrat? Online. *Kryptonovinky.cz*. 2023. Dostupné z: https://www.kryptonovinky.cz/top-softwarove-penezenky-kryptomeny/. [cit. 2024-05-14].

[37] TĚTEK, Josef. Bitcoin (VŠE, CO CHCETE VĚDĚT). Online. *Alza.cz*. 2024. Dostupné z: https://www.alza.cz/bitcoin. [cit. 2024-05-14].

[38] EHRA00. Kryptoměny v kontextu dark webu. Online. *Informacnigramotnost.cz*. 2023. Dostupné z: https://www.informacnigramotnost.cz/kryptomeny-v-kontextu-dark-webu/. [cit. 2024-05-14].

[39] KILIÁN, Karel. Velký policejní zátah na dark webu: 179 zatčených, zabavené zbraně a půl tuny návykových látek. Online. *Zive.cz*. 2020. Dostupné z: https://www.zive.cz/clanky/velky-policejni-zatah-na-dark-webu-179-zatcenych-zabavene-zbrane-a-pul-tuny-navykovych-latek/sc-3-a-206109/default.aspx. [cit. 2024-05-14].

[40] MACHÁČ, Roman. Láká vás Dark Web? Zde je 5 důvodů, proč se temnému zákoutí obloukem vyhnout. Online. *Mobilizujeme.cz*. 2023. Dostupné z: https://mobilizujeme.cz/clanky/laka-vas-dark-web-zde-je-5-duvodu-proc-se-temnemu-zakouti-obloukem-vyhnout. [cit. 2024-05-14].

[41] DESHMUKH, Akansha. Dark web ‘Red Rooms’ remain an urban legend despite the existence of ‘Daisy’s Destruction’. Online. *Timesofindia.com*. 2023. Dostupné z: https://timesofindia.indiatimes.com/blogs/darksides/dark-web-red-rooms-remain-an-urban-legend-despite-the-existence-of-daisys-destruction/. [cit. 2024-05-14].

[42] ROSNER, Yotam; LONDON, Sean a MENDELBOIM, Aviad. Backdoor Plots: The Darknet as a Field for Terrorism. Online. *Inss.org.il*. 2013. Dostupné z: https://www.inss.org.il/publication/backdoor-plots-the-darknet-as-a-field-for-terrorism/. [cit. 2024-05-14].

[43] THE INVESTOPEDIA TEAM. What Was the Silk Road Online? History and Closure by FBI. Online. *Investopedia.com*. 2023. Dostupné z: https://www.investopedia.com/terms/s/silk-road.asp. [cit. 2024-05-14].

[44] ALBUS, Jeff. DOJ moves 30K BTC connected to Silk Road seizure. Online. *Blockworks.com*. 2024. Dostupné z: https://blockworks.co/news/doj-moves-silk-road-bitcoin. [cit. 2024-05-14].

[45] ULBRICHT, Lyn. The Official website for Ross Ulbricht. Online. *Freeross.org*. 2013. Dostupné z: https://freeross.org/. [cit. 2024-05-14].

[46] STUDNIČKA, Jan. Zrůdný Peter Scully: Pod maskou podvodníčka se skrýval tvůrce nejbrutálnějších oplzlých filmů... s dětmi. Online. *G.cz*. 2023. Dostupné z: https://g.cz/zrudny-peter-scully-pod-maskou-podvodnicka-se-skryval-tvurce-nejbrutalnejsich-oplzlych-filmu-s-detmi/. [cit. 2024-05-14].

[47] *Peter Scully*. Online. In: Wikipedia: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, 2024. Dostupné z: https://en.wikipedia.org/wiki/Peter_Scully. [cit. 2024-05-14].

[48] Doctor sentenced in dark web murder-for-hire plot. Online. *Justice.gov*. 2024. Dostupné z: https://www.justice.gov/usao-ndga/pr/doctor-sentenced-dark-web-murder-hire-plot. [cit. 2024-05-14].

[49] Online. TheHiddenWiki. 2007. Dostupné z: https://thehiddenwiki.org/. [cit. 2024-05-14].

[50] *Safari (web browser)*. Online. In: Wikipedia: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, 2024. Dostupné z: https://en.wikipedia.org/wiki/Safari_(web_browser). [cit. 2024-05-14].

[51] YASAR, Kinza. Microsoft Edge. Online. *Techtarget.com*. 2023. Dostupné z: https://www.techtarget.com/whatis/definition/Microsoft-Edge. [cit. 2024-05-14].

[52] *Opera (webový prohlížeč)*. Online. In: Wikipedia: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, 2024. Dostupné

z: https://cs.wikipedia.org/wiki/Opera_(webov%C3%BD_prohl%C3%AD%C5%BEe%C4%8D). [cit. 2024-05-14].

[53] Funkce. Online. *Help.opera.com*. Dostupné z: https://help.opera.com/cs/latest/features/. [cit. 2024-05-14].

[54] Co je Tor? Online. *Alza.cz*. Dostupné z: https://www.alza.cz/co-je-tor. [cit. 2024-05-14].

[55] PEKÁR, Marian. The Invisible Internet Project (I2P): alternativa sítě Tor. Online. *Root.cz*. 2016. Dostupné z: https://www.root.cz/clanky/the-invisible-internet-project-i2p-alternativa-site-tor/. [cit. 2024-05-14].

[56] BOŘIL, Daniel. *Webové prohlížeče*. Bakalářská práce. Praha: Vysoká škola ekonomická v Praze, 2012.

[57] GALUŠKOVÁ, Petra. *Evil media a umění nových médií*. Bakalářská práce. Brno: Masarykova univerzita, 2016.

[58] Obrázek: *Královna Alžběta II. posílá e-mail*. Online. In: Wired.com. 2012. Dostupné z: https://media.wired.com/photos/59326d9bedfced5820d1051f/master/w_2560%2Cc_limit/queen-opening-arpanet-link-1976.jpg. [cit. 2024-05-14].

[59] Obrázek: *Princip HTTP Cookies*. Online. In: Study-ccna.com. 2024. Dostupné z: https://study-ccna.com/wp-content/images/http_process_explained.jpg. [cit. 2024-05-14].

[60] Obrázek: *Onion routing*. Online. In: Fossbytes.com. 2021. Dostupné z: https://fossbytes.com/wp-content/uploads/2015/09/tor-working.png. [cit. 2024-05-14].

[61] Obrázek: *Socha zakladatele Bitcoinu – Satoshi Nakamoto, v Budapešti*. Online. In: Nypost.com. 2021. Dostupné z: https://nypost.com/wp-content/uploads/sites/2/2021/09/satoshi-nakamoto-87.jpg?resize=1024,682&quality=75&strip=all. [cit. 2024-05-14].

[62] Obrázek*: Falešná red room webová stránka*. Online. In: Quora.com. 2019. Dostupné z: https://qph.cf2.quoracdn.net/main-qimg-1d1c5b02ab1fdfd37fb3c6a2f05fecd9-pjlq. [cit. 2024-05-14].

[63] Obrázek: *Úvodní stránka tržiště Silk Road*. Online. In: Theguardian.com. 2013. Dostupné z: https://i.guim.co.uk/img/static/sys-images/Guardian/Pix/pictures/2013/3/22/1363967178098/Silk-Road-009.jpg?width=700&dpr=2&s=none. [cit. 2024-05-14].

[64] Obrázek: *Plakát podporující Ulbrichta*. Online. In: News.bitcoin.com. 2016. Dostupné z: https://static.news.bitcoin.com/wp-content/uploads/2016/01/free_ross-229x300.jpg. [cit. 2024-05-14].

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

Příloha č. 1 DVD s prací v elektronické podobě

PŘÍLOHA P I: DVD S PRACÍ V ELEKTRONICKÉ PODOBĚ