Univerzita Hradec Králové

Fakulta informatiky a managementu

Katedra informačních technologií

Anonymita na Darkwebu

Bakalářská práce

Autor: Daniel Kučera
Studijní obor: Aplikovaná informatika, bakalářský

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

Hradec Králové Duben 2023

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 20.4.2023 Daniel Kučera

Poděkování:

Děkuji vedoucímu bakalářské práce doc. Ing. Vladimíru Soběslavovi, Ph.D. za metodické vedení práce a hodnotné tipy a rady během zpracovávání této práce. Dále bych rád poděkoval mým rodičům za jejich podporu po mnoha stránkách.

Anotace

Cílem této bakalářské práce je analyzovat problematiku anonymity na internetu, především v síti Darknet a způsoby, jak do dané sítě přistupovat. Důležité je si definovat pojmy jako je anonymita nebo soukromí nebo rozdíly mezi Deep webem a Dark webem. Tato práce je především zaměřena na Dark web, na to, jak se v něm pohybovat, na technologie, které lze použít a porovnávání jich či jejich kombinování, stejně tak jako na definici technologií, které naopak slouží ke sbírání dat uživatelů a jejich identifikaci. Rovněž tato práce pojednává o věcech, které lze v síti Darknet najít či jak je získat, o jeho účelu a historii. Výsledek této práce by měl čtenáři přinést důkladné znalosti o tom, jaké prostředky a postupy použít k tomu, aby mohl uživatel Darknet navštívit a jak se na něm pohybovat.

Annotation

Title: Darkweb anonymity

The goal of this bachelor's thesis is to analyze the problematics of the anonymity on the internet, especially on the Darknet network and options how to access it. It is important to define the terms like anonymity or privacy or the differences between the Deep web and Dark web. This thesis mainly focuses on the Dark web, the navigation on Dark web, the technologies that can be used and their comparisions and combinations, as well as the definition of technologies that on the other hand are used to collect user data and identify them. This thesis is also about things that can be found on the Darknet and how to get them, about purpose and history. The result of this thesis should give the reader thorough knowledge about what means and methods to use for accesing the Darknet and navigate on it.

Obsah

1 Úvod

Většina lidí při používání internetu nepřemýšlí o nějaké viditelnosti, identifikaci, dohledatelnosti či o tom, že je o nich sbíráno obrovské množství dat. Existuje však menší skupina lidí, pro jejíž aktivity je anonymita a soukromí na internetu nezbytné a sbírání dat o jejich činech by je mohlo ohrozit, a jelikož jde technologie neustále dopředu, je důležité pravidelně analyzovat anonymizující technologie, které momentálně existují. Spousta lidí si pod člověkem, který se za každou cenu snaží po sobě zahladit stopy, jako nějakého kriminálníka a dost možná mají ve spoustě případů pravdu. Na druhou stranu anonymity využívají i lidé ze zemí, kde je silná cenzura, a tito lidé tak pouze využívají internet stejným způsobem, jako my každý den. Rovněž může spousta lidí vidět anonymní prostory jako místo pro absolutní svobodu slova, což je v dnešní době silně probírané téma.

Z tohoto důvodu existuje Darknet – prostor, kde se člověk stává nedohledatelným, pokud k tomu použije správné technologie a postupy. Jedná se o kyberprostor plný různých fór či obchodů a stejně tak i dalšího jiného obsahu. Avšak, jak se dá čekat, nejedná se o žádné svaté místo, právě naopak, člověk si musí dávat pozor, kam chodí a na co kliká, aby se nedostal do problému a nepřišel například o všechny své peníze.

Součástí této práce je zanalyzovat technologie přístupu na Darknet, jako jsou internetové prohlížeče, a další anonymizující prostředky, jako jsou operační systémy či kryptoměny. Stejně tak je součástí této práce i analýza obsahu, k jakému se může uživatel jednoduše dostat a jak nepadnout do pasti podvodníkům.

2 Cíl práce

Anonymní kyberprostor není prostor, kde má běžný uživatel internetu důvod chodit, avšak důvodů, proč už tam někdo jde může být mnoho. Ať už se jedná o nákup nelegálního zboží, jako jsou drogy, zbraně či hackerské nástroje nebo objednávání nelegálních služeb, jako například hackerů či vrahů, rovněž se může jednat o lidi toužící po svobodě slova, protože jim to není na běžném internetu dovoleno. Z toho důvodu lze najít na Darknetu fóra, blogy a zpravodajské služby všeho druhu. Je tudíž patrné, že kromě různých kriminálníků se na Darkentu shází také lidé, kteří se chtějí pouze vyjádřit či poskytnout nějaké informace, které jinde zveřejnit nemohou.

Cílem této práce je analyzovat anonymizující technologie a přístupy na Darknet a porovnat je. Mezi takového technologie mohou patřit například internetové prohlížeče, operační systémy, kryptoměny či různé šifrovací nástroje zvyšující soukromí a anonymitu uživatele. Tato práce se rovněž věnuje tomu, jakým způsobem přistupovat k obsahu na Darknetu, jako jsou skryté služby a jaké kategorie skrytých služeb se na Darknetu nachází a jak moc často se může člověk setkat s podvodem a jak takový podvod poznat. Cíl této práce není jen o technologiích a nástrojích, ale má čtenáři i přiblížit, jak se má správně chovat a na co si má dávat pozor, aby zachoval svou anonymitu a nebyl podveden. Práce rovněž uvádí i postup, jak se na Darknetu pohybovat i jak na něm nakupovat.

Vypracování této práce spočívalo ve studii různých technologií a zásad anonymity a soukromí, stejně tak jako ve sběru dat na samotném Darknetu.

3 Metodika zpracování

Informace o různých technologií byly čerpány především z knih a studií zabývající se Darknetem a věcí kolem anonymity. Stávalo se, že i v pár let starých pracích se objevovaly technologie, které už dnes nefungují či se nepoužívají. Rovněž bylo také často čerpáno z oficiálních stránek či dokumentací daných technologií.

Co se týká sběru dat na Darknetu, ten probíhal dvěma způsoby – pomocí vyhledávače a pomocí internetových katalogů, tzv. wikiwebů, často označovaných jako „The Hidden wiki“. Tyto katalogy obsahovaly spoustu odkazů, a byly rozděleny do mnoha kategorií. Některé wikiweby také nabízely i ověření, zda je daná skrytá služba důvěryhodná či ne. Z důvodu velkého množství kategorií, které byly navíc na různých wikiwebech různé, byly tyto kategorie rozděleny do nadkategorií podle toho, jakého nadřazeného tématu se týkaly. Data z vyhledávače byly rovněž kategorizovány na základě klíčových slov, podle kterých byly skryté služby vyhledávány.

4 Rozdělení internetu

4.1 World Wide Web

World Wide Web (WWW) označuje systém pro prohlížení, ukládání a odkazování dokumentů, které se nachází v síti internet. Tyto dokumenty jsou popsány pomocí jazyka Hypertext Markup Language (HTML) a pro jejich přenos se využívá Hypertext Transfer Protokol (HTTP). Pro přístup na jednotlivé stránky se využívá internetového prohlížeče (Google Chrome, Mozilla Firefox apod.) a přistupuje se na ně pomocí URL odkazů, příkladem může být www.google.com či www.seznam.cz. Někteří lidé mohou zaměňovat pojmy World Wide Web a internet. Ve skutečnosti je WWW pouze aplikací, která na internetu běží.

World Wide Web lze rozdělit na tři úrovně – Surface web, Deep web a Dark web.

4.2 Surface web

Jedná se o část webu, který je jednoduše viditelný pro všechny uživatele a vše, co je potřeba udělat, aby se uživatel na tuto část webu dostal, je zadat URL adresu internetového prohlížeče. Příkladem Surface webu mohou být již výše zmíněné servery Google nebo Seznam.

Tuto část internetu také pomocí crawling strategií navštěvují web crawleři.
Crawling link hledá související informace skrz hypertextové odkazy z hlavní stránky dané domény [1]. Web crawler je internetový robot, který systematicky prohlíží celosvětový web a obvykle je používán vyhledávači (Google, Bing apod.) pro účely indexování webu [2]. Indexování webu znamená vytvoření indexů pro webové stránky, intranety apod., za účelem toho, aby se uživatel internetu dostal rychle a jednoduše na stránku, která obsahuje vyhledávaný pojem.

4.3 Deep web

Mnohem větší a zajímavější část webu tvoří Deep web. Deep web obsahuje část webu, která není indexována web crawlery. Tím pádem není tato část dohledatelná přes vyhledávače.

Deep web ukládá svůj obsah do databází, které poskytují výsledky dynamicky pouze v reakci na přímou žádost [3]. Pro přístup na Deep web je zapotřebí první zadat jisté údaje, jako může být například email, heslo, PIN či biometriky. Příkladem Deep webu může být například naše emailová schránka či náš Facebookový profil.

Podle webu Spiceworks je Deep web tvořen asi 7 500 terabyty dat, oproti tomu Surface web tvoří zhruba 19 terabytů dat. Tudíž množství dat na Deep webu je přibližně 400 až 500krát větší, než na Surface webu [4]. Pro představu je nejlepší použít ledovec – jen malá část celku je viditelná pro každého, zatímco mnohem větší část je "skrytá".

4.4 Dark web

Pojem Dark web (či Darknet) bývá velice často zaměňován s pojmem Deep web (či Deepnet). Ve skutečnosti se jedná o velice malý segment Deep webu, který je záměrně zakryt. K této části internetu se nedá připojit pomocí běžných nástrojů, ale je zapotřebí užití technologií k tomu určených. Dark web poskytuje uživatelům velkou dávku anonymity a bývá také často využíván k nelegálním činnostem.

Spiceworks uvádí, že se nedá přesně určit, jak velký Dark web je, ale podle některých expertů by obsah Dark webu mohl tvořit přibližně 5 % veškerého obsahu na internetu [4]. Garethu Owenovi [8] se podařilo dokázat, že vice než 40 % všech skrytých služeb na Dark webu není dostupných déle než 18 měsíců.

5 Anonymita na internetu

5.1 Anonymita

Pfitzmann A. [5] popisuje anonymitu stav, kdy subjekt není identifikovatelný v množině ostatních subjektů. Anonymita na internetu zahrnuje jak zachování soukromí uživatele na aplikační vrstvě (application level anonymity), tak skrývání síťových identifikátorů komunikujících partnerů v síťové vrstvě (network level anonymity) [6]. Síťový identifikátor (network ID nebo NetID) je fragment IP adresy, který klasifikuje síť pro konkrétního hostitele, tj. říká nám, ke které síti hostitel patří, obvykle se skládá z jednoho až čtyř oktetů v desítkovém vyjádření odděleném tečkami.

Mnoho lidí může při pohybu na internetu zaměňovat pojmy anonymita a soukromí, ve skutečnosti se jedná o dvě docela rozdílné věci. Henderson L. [7] vysvětluje tuto problematiku na příkladu, kdy při domácím používání Firefox uživatel zapne „privátní mód“. Tento mód zamezuje ukládání cookies či schopnost pamatovat si navštívené stránky a ukládat je do historie. Avšak nijak to neřeší problém s IP adresou. Vyhledávače stále vidí, co uživatel vyhledával a rovněž to vidí i jeho poskytovatel internetu. Oba dva subjekty vědí, na jakých stránkách uživatel byl a na jak dlouho. Jediný, kdo to nevidí, je uživatelova žena. Anonymní režim slouží jen proto, aby udržel v soukromí stránky, které uživatel navštíví v soukromí od jeho blízkého okolí. Anonymita na druhou stranu zdvihá soukromí na vyšší úroveň, neboť zakrývá IP adresu, a tím pádem i veškerou aktivitu na internetu za vrstvy a vrstvy digitálních bariér.

Existuje mnoho důvodů, proč někdo vyhledává anonymitu na internetu - spousta lidí si anonymní prostor na internetu spojí s nelegálními činnostmi jako je například nákup drog, zbraní, malware či nelegální pornografie, avšak někteří mohou chtít využít anonymního prostoru jako místo pro absolutní svobodu slova, pro překročení „*Velkého čínského firewallu*“, jež blokuje spoustu, pro západní svět základních webů, jako například Facebook, Gmail, Twitch či BBC nebo mohou být znepokojeni výpovědí Edwarda Snowdena, který vynesl na povrch pravdu o tom, jak americká NSA monitoruje uživatele internetu [28]. Edward Snowden je americký whistle-blower, bývalý zaměstnanec CIA a jako sub-kontraktor pracoval pro americkou NSA, který vynesl do médií informace o sledování telefonních komunikací bezpečnostními složkami USA a o tajném bezpečnostním programu PRISM [9].

PRISM je nástroj, pomocí kterého sbírá NSA data o uživatelích z velkých internetových serverů jako Facebook či Gmail. Vznikl jako reakce na teroristický útok na Světové obchodní centrum 11. září 2001 pod programem „Terrorist Surveillence Program“ prezidenta George Bushe. Jeho myšlenkou je, NSA že může požadovat osobní data uživatelů od technologických společností jako Microsoft, Apple či Yahoo [20].

5.2 Identifikační prostředky

Na internetu existuje spousta algoritmů, softwarů a nástrojů, které sbírají o uživatelích všemožné informace, podle kterých je pak možné dohledat, kdo daný počítač vlastně používá. K identifikaci uživatele slouží následující údaje či nástroje:

IP Adresa – jedná se o číslo, které identifikuje Internet protokol, což je protokol, pomocí kterého mohou mezi sebou počítače navzájem komunikovat. V dnešní době je nejrozšířenější IPv4, která se skládá ze 32bitů. Zapisovány jsou pomocí čtyř oktetů oddělených čárkou. Příkladem IPv4 může být adresa 192.168.0.1. Z důvodu nedostatku použitelných adres vznikl také IPv6, který je složen v 128bitů, jehož adresa je zapsána hexadecimálně. Příkladem IPv6 je 2001:0db8:85a3:0000:0000:8a2e:0370:7334. Pomocí IP adresy se dá zjistit, jakému patří poskytovateli internetu, přes kterého se dá zjistil konečný uživatel dané adresy.

Cookies – cookies jsou data, která jsou zapisována na pevný disk počítače. Vznikají při návštěvě webových stránek a uchovávají různé uživatelem nastavené preference. Můžou také sloužit například k autentifikaci či identifikaci uživatele. Avšak jsou také příčinou toho, že se uživateli začnou objevovat reklamy související s termíny, které dříve vyhledával například vyhledávačem Google. Cookies byly původně vytvořeny pro markentingové účely. Při načtení webové stránky na uživatele často vyskočí lišta oznamující využití cookies na stránce či úprava jejich nastavení, avšak nenabízí se možnost cookies odmítnout a pokud ano, tak stránka většinou uživatele přesměruje někam pryč.

Evercookies – (také známé jako supercookies) jedná se o JavaScriptovou API, která má za účel obnovit cookies, která uživatel smazal. Dokument „Tor stinks‘“, který v roce 2013

odtajnil Edward Snowden ukazuje, že NSA využívala evercookies pro sledování uživatelů, kteří používali Tor [10].

JavaScript – JavaScript (JS) je programovací jazyk, využívaný pro programování webových aplikací. JavaScript používá asi 98,2 % všech webových stránek [51]. JS je jednou z největších hrozeb pro anonymitu na internetu, protože dokáže zjistit IP adresu klienta používající danou webovou stránku či jiná data. Při anonymním prohlížení internetu musí být JS vždy zakázán, avšak to může často vést k tomu, že daná stránka nebude fungovat tak, jak má.

Metadata – V roce 2012 byl americký hacker Higinio Ochoa, známý také jako w0rmer, zadržen kvůli spojení s hackerskou organizací „CabinCr3w“, která tvořila součást Anonymous. Vypátrán byl na základě zveřejněné fotografie pořízené pomocí iPhone, která obsahovala EXIF data [11].

EXIF (Exchangeable image file format) je specifikace pro formát metadat, které jsou vloženy do souborů digitálními fotoaparáty. EXIF je podporován ve formátech jako JPEG nebo TIFF. Dokáží zaznamenat a uchovat data jako:

- Značka a model fotoaparátu
- Datum a čas pořízení snímku
- Nastavení fotoaparátu
- Místo pořízení snímku
- Informace o autorovi

Právě díky identifikace lokace, kterou EXIF provádí pomocí GPS, se podařilo vypátrat konkrétní dům, kde byla fotografie pořízena [11].

EXIF metadatům se dá vyhnout buďto za použití software, který je vymaže nebo přeformátováním fotografie do formátu, který EXIF nepodporuje jako PNG nebo GIF.

Snímání pohybu myši – v roce 2016 přišel Jose Carlos Norte s metodou, jak za pomocí pohybu a rychlosti myši a měření času identifikovat uživatele Tor, za předpokladu, že navštívil dané stránky jak pomocí Toru, tak pomocí běžného prohlížeče [12].

Geolokace – jedná se o metodu, jak identifikovat místo, kde se momentálně uživatel nachází. Tato metoda využívá kombinaci výše zmíněných nástrojů či informací, přičemž hlavními informacemi jsou například IP adresa či metadata.

5.3 Cypherpunk

První, kdo přišel s myšlenkou anonymity na internetu, a rovněž i anonymní kryptoměny, bylo aktivistické hnutí Cypherpunk, založené roku 1992 Johnem Gilmorem, Timem Mayem a Ericem Hughesem. V tomtéž roce byl také zveřejněn „A Cypherpunk's Manifesto". Počátky aktivit hnutí však datujeme od roku 1985 po zveřejnění textu „Security Without Identification: Transaction Systems to Make Big Brother Obsolete" od Davida Chauma, týkající se myšlenky vytvoření digitální a anonymní měny [13].

Jedním z nejdůležitějších software, které hnutí Cypherpunk využívalo, je PGP z od Phila Zimmermanna, který jej vytvořil, protože mu přišlo, že začínají digitální technologie narušovat soukromí uživatelů.

Mezi významné Cypherpunky patří také Jacob Appelbaum, který je jedním ze zakladatelů Tor Projectu a Julian Assange, který založil WikiLeaks, který se *„specializuje na analýzu a publikování velkých datových souborů, cenzurovaných nebo jinak omezených oficiálních materiálů zahrnujících válku, špionáž a korupci."* [14].

5.4 Zásady anonymního chování

Jako první je potřeba si uvědomit, že i sebe lepší anonymizující technologie dokáže poskytnout jistou úroveň anonymity pouze na technické úrovni. Nedokáže zabránit tomu, že se daný uživatel chová v anonymním prostoru lehkovážně a likviduje tak veškeré úsilí, které do své anonymity vložil.

Základní zásadou je nikdy nezmiňovat své skutečné údaje, ať už jde o jméno, datum narození, adresy (jak skutečné, tak virtuální), lokace, počasí, zaměstnání či plány na víkend. Při placení používat pouze dostatečně anonymní metody a kryptoměny. Nikdy nepoužívat platbu běžnou měnou. Dále je důležité se vyvarovat používání osobních emailů či přezdívek. Ideální je používání více emailů a přezdívek k různým účelům. Různá místa – různá jména – různé osobnosti – klidně i různá pohlaví. Uživatelská jména je vhodné volit obyčejná, například „Johnny" nebo „Peter", hlavní je, aby nemohly být nějak

spojeny s uživatelem. To samé platí pro emailové adresy. Vždy vypínat JavaScript. Nepoužívat pevný počítač doma, nýbrž nejlepší je sedět s notebookem na nějaké veřejné síti, pro menší možnost identifikace na základě IP adresy. Je však důležité najít takové místo, aby nebylo do notebooku vidět nějakou cizí osobou či kamerou.

Henderoson L. dále zmiňuje, že je vhodné nikdy nevypínat router. Vhodné je i nechat běžet anonymní programy jako I2P či Freenet dlouhodobě, protože pak je větší šance, že se v tom návalu dat a uživatelů člověk ztratí [7].

Důležité je dbát na pravopis a gramatiku – člověka může prozradit to, že dělá často stejné chyby na stejných místech v textu. Pokud si tohoto někdo všimne v případě „veřejné osobnosti“ a „anonymní osobnosti“, lze si pak lehce spojit, že se může jednat o tu samou osobu. To samé platí i o stylu psaní a vyjadřování - „veřejná osobnost“ a „anonymní osobnost“ by se nikdy neměla na internetu vyjadřovat stejně. Příkladem budiž případ UNABOM z minulého století z USA. Ted Kaczynski, přezdívaný Unabomber, je bývalý profesor matematiky, terorista a anarchista, autor manifestu „Industrial Society and Its Future“ známý také jako „Unabomber Manifesto“, který zasílal poštou bomby, důsledkem čehož 3 lidi zavraždil a 23 zranil. Prosazoval primitivní životní styl, který zahrnoval bydlení v chatě v lese bez zavedené elektřiny i vody. FBI neměla moc vodítek, které by vedly k jeho dopadení. Zásadní zlom přišel až ve chvíli, kdy si část jeho manifestu přečetl Kaczynského bratr David, který poznal způsob vyjadřování svého bratra, neboť si s ním dopisoval. Poté co David doložil dopisy svého bratra lingvistickým odborníkům, došli k závěru, že autor dopisů a manifesta je s největší pravděpodobností ten samý člověk. Momentálně si Ted Kaczynski odpykává doživotní trest ve vězení v Coloradu [17].

Při možnosti výběru mezi proprietárním nebo otevřeným softwarem je z hlediska anonymity lepší volit otevřený. Kromě toho, že otevřený software bude s největší pravděpodobností zdarma, zatímco proprietární ne, máme díky otevřenosti technickou dostupnost kódu, a tudíž máme možnost si sami ověřit, že se v daném software neskrývá žádný spyware či nějaké „zadní vrátka“ organizace jako například NSA.

5.5 Anonymizující technologie

5.5.1 PGP

PGP[1], celým názvem „Pretty Good Privacy“ je software, který poprvé zveřejnil Phil Zimmermann v jedné ze skupin Usenetu[2] a během pár týdnu jej stáhly tisíce lidí po celém světě. *„Před PGP nebylo možné, aby spolu dva lidé komunikovali na dlouhou vzdálenost bez risku toho, že by je někdo zachytil.“* řekl Zimmermann. Do dnešního dne se jedná o jednu z nejvíce používaných forem šifrování emailové komunikace [15].

V dnešní době funguje PGP jako otevřený software pod názvem OpenPGP, slouží k šifrování emailových komunikaci založených na principu konec-konec (end-to-end). Je dostupný na všechny běžné platformy jako Windows, Mac OS, GNU/Linux, Android či iOS.

5.5.2 VeraCrypt

VeraCrypt[3] je software, který slouží pro šifrování oddílu na disku. Důvodem, proč jej uvádím jako anonymizující technologie je, že sice nezajišťuje anonymitu na internetu, ale uchovává v soukromí data na disku uživatele v případě, že by bylo zařízení vystaveno útoku hrubou silou (brute-force attack). Jedná se o útok, kdy se útočník snaží rozluštit šifru bez znalostí klíče k dešifrování. V praxi se jedná o testování různých kombinací hesel a heslových frází. Vznikl jako fork (alternativní větev) programu Truecrypt a řeší spoustu jeho nedostatků. Jedná se o otevřený software dostupný pro běžné operační systémy jako Windows, Mac OS či Linux.

Základní vlastnosti

Henderson L. [7] popisuje základní vlastnosti VeraCryptu následovně:

- Vytváří virtuální zašifrovaný disk uvnitř souboru a připojuje jen jako skutečný disk.
- Šifruje celý oddíl nebo úložiště jako USB flash disk nebo pevný disk.
- Šifruje diskový oddíl nebo pevný disk, kde je Windows naistalován (pre-boot authentication).

---

[1] PGP je k dostání na adrese https://www.openpgp.org/software/.
[2] Usenet je systém internetových diskuzních skupin.
[3] VeraCrypt je dostupný ke stažení na webu https://www.veracrypt.fr/en/Downloads.html.

- Šifrování je automatické, v reálném čase (on the fly) a transparentní.
- Paralelizace a pipelining umožňují, že data jsou čtena a zapisována stejně rychle, jako kdyby disk nebyl zašifrován.
- Šifrování může být na moderních procesorech hardwarově akcelerováno.

Alternativa

Alternativou k VeraCryptu/Truecryptu je například Drivecrypt. Drivecrypt je proprietární placený software umožňující téměř to samé, co VeraCrypt resp. Truecrypt. Vzhledem k tomu, že Drivecrypt neumožňuje široké veřejnosti nahlédnout do jeho kódu, je z hlediska soukromí a anonymity lepší používat VeraCrypt.

5.5.3 VPN

Celým názvem Virtual Private Network (Virtuální privátní síť), je prostředek, který umožňuje klientům zamaskovat jejich IP adresu za jinou IP adresu, klidně z jiného konce světa. Mnoho lidí využívá VPN například pro sledování seriálů na Netflixu, které jsou v jejich zemi zakázané, neboť daný internetový server si bude myslet, že se klient opravdu připojuje ze země, ze které daná IP adresa pochází. Většina společností provozujících VPN nabízí své služby za peníze, avšak existují i neplacené alternativy, ty však většinou vydělávají na uživatelích pomocí reklam.

Podle webu Bussines 2 Community [16] patří mezi TOP 3 VPN poskytovatele v česku:

1. NordVPN
2. UltraVPN
3. CyberGhost VPN

NordVPN

NordVPN[4] [64] nabízí měsíční, roční či dvouroční plán.

Tabulka 1. Nabídka služeb NordVPN.

Název	Complete	Plus	Standard
Cena měsíčního plánu	14,49€/měsíc	12,99€/měsíc	11,99€/měsíc
Cena ročního plánu	7,49€/měsíc	5,99€/měsíc	4,99€/měsíc
Cena dvouročního plánu	5,99€/měsíc	4,49€/měsíc	3,49€/měsíc
30denní záruka vrácení peněz	✓	✓	✓
Zabezpečená, vysokorychlostní VPN	✓	✓	✓
Ochrana proti malware	✓	✓	✓
Blokování reklam a trasování	✓	✓	✓
Mezi platformní manažer hesel	✓	✓	×
Data breach skener	✓	✓	×
1 TB šifrovaného cloudového úložiště	✓	×	×

Zdroj: https://nordvpn.com/

[4] NordVPN je k dostání na adrese https://nordvpn.com/.

Pro předplacení NordVPN je potřeba zadat email. Platit je možno buďto pomocí Kreditní nebo debetní karty, Google Pay nebo Bitcoinem.

UltraVPN

UltraVPN[5] [65] rovněž nabízí měsíční, roční nebo dvouroční plán.

Tabulka 2. Předplatné služeb UltraVPN.

Měsíční	Roční	Dvouroční
7,09€/měsíc	2,82€/měsíc	1,88€/měsíc

Zdroj: https://ultravpn.com/

Všechny tyto varianty nabízí:

- Garanci vrácení peněz do 30 dnů.
- Ochranu všech zařízení
- Nejlepší šifrování v oboru
- Přístup k více než 1000 secure serverům
- Neomezený bandwidth
- Technickou podporu 24/7

Pro předplacení je nutno zadat emailovou adresu. Možnost platby je buďto pomocí kreditní či debetní karty, přičemž kromě údajů je potřeba také zadat zemi a poštovní směrovací číslo. Další možností platby je PayPal.

Cyber Ghost VPN

Cyber Ghost VPN[6] [66] nabízí měsíční, šestiměsíční nebo dvouleté předplatné.

Tabulka 3. Předplatné služeb Cyber Ghost VPN.

Měsíční	Seštiměsíční	Dvouroční
11,99€/měsíc	6,99€/měsíc	2,11€/měsíc

Zdroj: https://www.cyberghostvpn.com/

[5] UltraVPN je k dostání na adrese https://ultravpn.com/.
[6] Cyber Ghost VPN je k dostání na adrese https://www.cyberghostvpn.com/.

Všechny tarify nabízí:

- 45denní záruku vrácení peněz
- 100% zásady neuchovávání žádných záznamů
- Ochranu až pro 7 zařízení
- Samostatné aplikace pro Apple, Android, Windows, Linux atd.
- Zákaznická podpora 24/7
- 9700+ VPN serverů z 91 zemí
- ID Guard zdarma

Cyber Ghost VPN požaduje emailovou adresu. Možnosti platby jsou buďto platební kartou, PayPal, Google Pay či Bitcoin.

Závěr

Z této analýzy dojdeme k závěru, že byť VPN poskytují určitou úroveň soukromí, nelze se zde bavit o anonymitě. Za předpokladu, že klient zaplatí za službu například platební kartou, pak veškerá anonymita padá a je o klientovi dohledatelná téměř každá identifikační informace. Bitcoin je sice mnohými považován za anonymní platidlo, ale to není úplně pravda. Problematiku Bitcoinu řeší tato práce později. To samé platí už jen z principu, že při používání VPN musí klient poskytnou společnosti svou IP adresu, jejíž problematika je popsána výše.

Je tedy možné být anonymní pomocí VPN? Ne. Avšak existuje způsob, jak maximalizovat své soukromí a být téměř anonymní. Jedním takovým řešením je použití MullvadVPN.

Mullvad VPN

Mullvad VPN[7] [67] nabízí anonymní účet – není zapotřebí zadání žádných osobních údajů, ani přihlašování se na nějaký účet. Pro zvýšení anonymity, je možné navštívit této společnosti přes .onion odkaz. Tato služba funguje na principu toho, že při zakládání účtu stránka klientovi vygeneruje číselný kód, pomocí kterého se bude moct připojit, až za něj zaplatí. Existuje mnoho způsobu, jak si předplatit tuto službu, avšak při použití .onion

[7] Mullvad VPN je k dostání na adrese https://mullvad.net/en/ nebo o54hon2e2vj6c7m3aqqu6uyece65by3vgoxxhlqlsvkmacw6a7m7kiad.onion.

odkazu je povolená možnost platby pouze Cash, Monero, Bitcoin, Bitcoin Cash a Voucher - tudíž metody, které jsou mnohem anonymnější, než placení běžnou kartou. Při platbě přes Monero nabízí Mullvad VPN následující předplatné:

Tabulka 4. Předplatné služeb Mullvad VPN.

1 měsíc	2 měsíce	3 měsíce	6 měsíců	1 rok
4,5€	9€	13,5€	27€	54€

Zdroj: https://mullvad.net/en/

Mullvad VPN na základě používaného OS nabízí:

Tabulka 5. Nabídka služeb Mullvad VPN.

OS	Windows	macOS	Linux	Android	iOS
Externě auditované	✓	✓	✓	✓	✓
Otevřený software	✓	✓	✓	✓	✓
Split tunneling[8]	✓	×	✓	✓	×
Vlastní DNS[9] server	✓	✓	✓	✓	×
Multihopping	✓	✓	✓	×	×
Přesměrovávání portů	✓	✓	✓	✓	✓
Shadowshocks proxy	✓	✓	✓	×	×
Nahlašování problémů v aplikaci	✓	✓	✓	✓	✓
Blokování reklam a trasování	✓	✓	✓	✓	✓
Automatická rotace WireGuard[10] klíče	✓	✓	✓	✓	✓

Zdroj: https://mullvad.net/en/

Jediný problém, který se zde může vyskytnout je, že i přes vše, co Mullvad VPN nabízí, stejně musí nakonec klient poskytnout IP adresu. Avšak, není zapotřebí použít vlastní IP adresu, nýbrž lze využít veřejného připojení, například v kavárně. Tudíž při případném

[8] Split tunneling umožňuje některým aplikacím či zařízením přistupovat na internet přes VPN, zatímco ostatní aplikace či zařízení mohou přistupovat bez VPN.
[9] DNS – Jmenný systém (Domain name system) slouží k převodu IP adres a doménových jmen.
[10] WireGuard je protokol, který implementuje šifrované VPN.

trasování IP adresy by byla zjištěna pouze adresa kavárny, nikoliv klienta. Poskytnutí skutečné IP adresy se dá vyvarovat za zakoupení služby skrze Tor – v tom případě je společnosti poskytnuta pouze adresa koncového uzlu.

5.5.4 Proxy

Proxy server slouží jako prostředník komunikace mezi uživatelem a koncovým serverem a často se používá jako jeden z nástrojů na zvýšení soukromí uživatelů. Proxy vytváří dojem, že je konkrétním klientským počítačem, který komunikuje s se serverem. Ve skutečnosti klienti posílají své požadavky na proxy server, který je pak přeposílá na server. Tudíž to, co server od proxy získá, jsou požadavky různých klientů. Proxy server odděluje intranet od internetu. Proxy může mít formu jak software, tak hardware či jako online služba [18].

Existuje mnoho druhů proxy, většinou se dělí podle účelu nebo typu. V rámci této práce je k proxy přistupováno jako k anonymizujícímu nástroji.

5.5.5 Overlay síť

Overlay síť (overlay network) je počítačová síť, virtuální či logická, která je postavena na vrstvě jiné počítačové sítě. Příkladem overlay sítě jsou například propojené uzly (nodes), které jsou umístěny na vrchol už existující sítě. Internet sám o sobě byl postaven jako overlay síť na vrcholu již existující telefonní sítě. Overlay síť je velice důležitý koncept v otázce nástrojů zajišťujících anonymitu na internetu. Na principu overlay sítí fungují například peer-to-peer sítě nebo služba BitTorrent [19].

Výhody a nevýhody

Gula J. [19] popisuje výhody a nevýhody overlay sítí následovně:

Výhody:

- **Postupně rozvíjející se:** S overlay sítí nejsou nutné žádné změny v aktuální internetové infrastruktuře a přidáním uzlů do překryvné vrstvy lze cestu dat v substrátové síti řídit s velkou přesností.
- **Adaptabilní:** I když má překryvná síť omezenou sadu tras, může tyto trasy optimalizovat tak, aby vyhovovaly potřebám aplikace, například nalezením tras, které mají menší latenci než dnešní IP infrastruktura na úkor šířky pásma.
- **Robustní:** Přidáním více a více uzlů se překryvná síť může stát robustnější než její substrátová síť. To by mohlo být použito k vytvoření dvou nezávislých cest mezi dvěma uzly, což mu umožní rychle přesměrovat a opravit chyby.
- **Přizpůsobitelné:** Overlay uzly mohou být reprezentovány víceúčelovými počítači, které jsou vybaveny jakýmkoli potřebným vybavením. Ukázkovým příkladem je široké využití místa na disku.

Nevýhody:

- **Údržba:** Údržba musí být možná na dálku, jinak je zbytečná, jelikož správce overlay sítě je fyzicky daleko od spravovaných strojů. Fyzická údržba musí být minimalizována.
- **Připojení:** Velký počet hostitelů se nachází za překladem síťových adres (NAT) a za proxy. Značná část internetu leží za firewally.
- **Neefektivita:** Ve srovnání se službami založenými na směrovačích nemohou overlay sítě dosáhnout stejné účinnosti, ale když overlay síť roste, může se efektivitě těchto služeb přiblížit.
- **Ztráta informací:** K odvození topologie substrátové sítě je zapotřebí značného úsilí, protože overlay sítě jsou postaveny na síťové infrastruktuře IP, jejíž konektivita je omezena pouze firewally, NAT a proxy.

5.5.6 I2P

Invisible Internet Project[11] je otevřená klientská aplikace napsaná v jazyce Java, která umožňuje anonymní surfování po internetu. Dostupná je na různé platformy jako Windows, Linux, macOS či Android.

Historie

Projekt poprvé začal v roce 2002. Vizí pro I2P síť je „poskytovat plnou anonymitu, soukromí a zabezpečení na nejvyšší možné úrovni. Decentralizovaný a peer-to-peer internet znamená, že se již nemusíte starat o to, aby váš ISP[12] kontroloval váš provoz. To umožní (lidem) provádět bezešvé aktivity a změnit způsob, jakým se díváme na zabezpečení, a dokonce i internet, využívající kryptografii veřejného klíče, steganografii IP[13] a ověřování zpráv. Internet, který měl takový být, již brzy bude."
I2P síť je plně zašifrovaná peer-to-peer overlay síť [21].

Architektura

Pro anonymní připojení používá aplikace vlastní router, který vytváří tunely. Tunel představuje jednotlivé klienty, kteří posílají svá data jedním směrem. Klient pošle data do odchozího tunelu a na druhé straně jsou data z příchozího tunelu přijata. Klient sám má možnost si vybrat, jak dlouhý bude tunel, který použije. Od velikosti tunelu se pak odvíjí úroveň výkonosti, latence a anonymity, které klient nabyde [23].

Využívá takzvaného *„Garlic routingu"* (GR) (česnekového směrování), což je termín odvozen od *„Onion routingu"* (OR) (cibulového směrování), kterého využívá Tor, z nějž také vychází. Podle oficiálního webu [21] si lze pod pojmem GR ve spojení s I2P se dají nejčastěji představit tři věci:

- Vrstvené šifrování – OR vytváří cesty a tunely pomocí různých peerů a posílaná data jsou pak následně šifrována. Obecně se v případě GR jedná téměř o totéž, co v případě OR. Samozřejmě se implementace I2P poněkud liší od implementace Tor.

[11] I2P je dostupný ke stažení zdarma na adrese https://geti2p.net/en/download .
[12] ISP – Internet Service Provider – poskytovatel internetu.
[13] Steganografie IP je technika skrytí informace uvnitř paketu, aniž by došlo ke změně jeho struktury.

- Sdružování více zpráv k sobě – zpráva se dá popsat jakožto stroužek, které když sdružíme, nám vytvoří celý česnek. Na podobném principu zde funguje GR, který dokáže sdružit několik zpráv k sobě. Každá zpráva nese instrukce o tom, kam má být doručena a ke zpracování této informace dojde až při koncovém bodu. Tímto postupem se výrazně liší od OR, který využívá Tor.
- ElGamal/AES šifrování – jedná se o kombinaci symetrických a asymetrických šifrovacích algoritmů, které I2P využívá pro poskytnutí datové integrace Garlic zpráv.

Obsah

I2P poskytuje připojení k anonymním stránkám jménem *eepsites*, ke kterým je možné se připojit pouze za použití I2P aplikace, obdobně, jako v případě onion stránek a Toru. Eepsites adresy lze poznat podle koncovky .i2p. Takovou adresu má například stránka ransack.i2p, což je jeden z nejpoužívanějších vyhledávačů při používání I2P.

I2P vs Tor

Henderson L. popisuje výhody I2P oproti Toru následovně [7]:

- Skryté služby se jsou mnohem rychlejší než v případě Toru.
- Nenachází se zde tolik DOS (Denial of service) útoků, jako případě Toru.
- Je kompatibilní s peer-to-peer sdílením souborů (Tor není).
- Tor tunely fungují déle než tunely I2P. To zajišťuje méně útoků hackerů.
- Každý peer přesměrovává data pro ostatní.
- Nabízí TCP/UDP.
- Je napsán v Javě.

Naopak výhody Toru oproti I2P jsou následující:

- Tor má mnohem více uživatelů, než I2P; mnohem větší podpora od akademických zdrojů, pravidelné vylepšování stability a odolnosti proti útokům.
- Projekt je financován ze spousty zemi napříč celým světem.
- Velký počet výstupních uzlů.
- Přeložen do spousty jazyků.
- Optimalizován pro výstupní provoz.
- Více optimalizovaná paměť než v případě I2P.

- Napsán v jazyce C.

5.5.7 Freenet

„Neustále se obávám o své dítě, i když je ještě příliš mladá na to, aby se vůbec přihlašovala na internet. Zde je to, čeho se obávám. Obávám se, že za 10 nebo 15 let za mnou přijde a řekne ‚Tati, kde jsi byl, když zrušili svobodu tisku na internetu? '"
Těmito slovy Mikea Godwina z *Electronic Frontier Foundation*, což je mezinárodní nezisková skupina bojující za digitální práva, začíná podle oficiálního webu popis toho, co vlastně Freenet[14] je [22].

Jedná se o otevřený a decentralizovaný peer-to-peer software umožňující lidem brouzdat internet s notnou dávkou anonymity. Freenet je dostupný na všechny základní platformy jako Windows, Linux, macOS či Android. Základní myšlenkou projektu, jak vyplývá z výše uvedeného citátu, je boj proti cenzuře a boj za svobodu slova na internetu.

Obsah

Klient má možnost navštěvovat stránky, tzv. „freesites", které jsou dostupné pouze za při použití aplikace Freenetu. Freenet také nabízí dva zabezpečovací protokoly – *Opennet* a *Darknet*. Opennet umožňuje klientovi připojit se k jakémukoliv jinému uživateli. Další, tzv. „Darknet" mód, umožňuje připojení a komunikaci pouze s „přáteli" klienta, s lidmi, které daný klient sám do tohoto protokolu přidá, a tudíž je velice obtížné detekovat jakýkoliv provoz. Příkladem odkazu je freesite může být třeba http://localhost:8888/USK@0npnMrqZNKRCRoGojZV93UNHCMN-6UU3rRSAmP6jNLE,~BG-edFtdCC1cSH4O3BWdeIYa8Sw5DfyrSV-TKdO5ec,AQACAAE/fms/147/ , který odkazuje na stránku Freenet Message System, která nabízí jeden ze způsobů, jak komunikovat v prostředí Freenetu.

Architektura

Freenet, na rozdíl od Toru, nepotřebuje vlastní server, nýbrž využívá diskového úložiště uživatelů pro ukládání dat, takže není závislý na žádném centrálním serveru. Před nahráním dat do sítě Freenet jsou data zašifrována a rozdělena. Tyto části dat jsou pak ukládány do úložišť uživatelů, jinými slovy, do různých uzlů sítě. Tím pádem není pro uzel

[14] Freenet je dostupný zdarma ke stažení na adrese https://freenetproject.org/pages/download.html .

možné tyto informace uložené v úložišti identifikovat a kontrolovat. Aby nedošlo k nedostupnosti dat při nedostupnosti jednotlivých uzlů, jsou data během nahrávání několikrát zkopírována [23].

Použití

Instalační průvodce Freenetu nabízí mimo jiné i češtinu. Po instalaci a spuštění aplikace je možné přistoupit do sítě Freenet klidně i prostřednictvím Tor prohlížeče, jen je potřeba jej správně nakonfigurovat. Samotné procházení sítě je však velice pomalé. Na Freenetu lze navštívit jen to, co je dostupné jen na něm. Na rozdíl od Toru v něm není možné prohledávat Surface web.

5.5.8 Tor

Tor[15] je otevřený software od neziskové organizace The Tor Project umožňující anonymní komunikaci po internetu. Myšlenkou Toru je vytvořit nástroj umožňující uživatelům soukromý přístup na necenzurovaný web [24]. Název Tor pochází z pojmu The Onion Rounting, na jehož principu je fungování Toru založeno. Jedná se o nejznámější a nejpoužívanější nástroj svého druhu. Podle webu TrueList využívá Tor přibližně 2 miliony lidí denně, přičemž největší podíl z toho tvoři uživatelé z Ruska [25].

Jak již bylo zmíněno, Tor funguje na principu technologie OR, to znamená, že posílaná data jsou šifrována a provoz dále vede skrze koncové uzly (exit nodes), které mají několik vrstev kryptografie. Od této představy vrstev také pochází název Onion Rounting, jakožto podobnost s cibulí, která je taky tvořena vrstvami. Tím dochází také k zamaskování IP adresy. Toho se dá ověřit jednoduchým testem: v běžném prohlížeči, při návštěvě webu https://www.mojeip.cz/ se zobrazí IP adresa uživatele. Při použití Toru se zobrazí IP adresa koncového uzlu.

Historie

OR je známý již od devadesátých let. Původně byl vyvíjen Paulem Syversenem, Michaelem G. Reedem a Davidem Goldschlagem, kteří byli pověřeni námořnictvem USA, aby vyvinuli program, který by realizoval ochranu komunikace rozvědčíků Spojených Států. Později byl program vyvíjen agenturou DARPA, což je agentura amerického ministerstva obrany,

[15] Tor je k dispozici zdarma na adrese: https://www.torproject.org/download/. Je dostupný pro platformy Windows, macOS, Linux a Android.

která zajišťuje vývoj vojenských technologií. Později byl projekt vydán pod volnou licencí společností Electronic Frontier Foundation, stále za velké podpory Amerického námořnictva [26]. Z toho vyplývá, že i přes to, že je Tor jeden z nejlepších anonymizujících nástrojů, jeho nevýhodou je fakt, že samotný princip jeho fungování je založen na technologii vyvíjenou americkými službami. Tudíž je pravděpodobné, že americké tajné služby budou s fungováním a problematikou Toru dobře obeznámeni, což jim dává možnost vyvíjet technologie na prolamování anonymity.

Elementy

Gula J. popisuje ve své práci [19] základní elementy Toru následovně:

- **Onion směrovače**: Představují základní stavební kameny sítě Tor. Virtuální obvody, které přenášejí data, se skládají z těchto onion směrovačů. Tyto směrovače vytvářejí overlay topologii sítě Tor. Pracují na portu 9001 přes TCP a ve výchozím režimu čekají na příchozí požadavky na připojení. Tyto směrovače jsou rozděleny do tří skupin – vstupní hlídky, střední přenosy/uzly a výstupní přenosy/uzly. Onion směrovače mají specifický identifikační klíč, který určuje jeho umístění, typ uzlu a další informace o konkrétním uzlu.
- **Onion proxy**: Řízení datových transakcí mezi uživatelskými aplikacemi a sítí Tor. Vytvářejí virtuální okruhy a získávají aktuální informace o topologii a stavu sítě. Tyto informace jsou získávány z adresářových serverů.
- **Adresářové servery**: Tyto servery standardně používají port 9030. Ukládají informace o globálním pohledu na topologii a stavu jednotlivých uzlů v síti Tor. Správci adresářových serverů mají seznam známých onion routerů. Každý router má certifikát, který je podepsán identifikačním klíčem routeru.
- **Skryté služby**: Tyto služby jsou dostupné prostřednictvím serverů, které poskytují služby anonymity. To je možné díky integrovanému mechanismu v Toru. Mechanismus skrývá skutečnou identitu serverů a činí je anonymními. Jsou přístupné pomocí upraveného názvu domény, která je interní pro síť Tor.
- **Mosty**: Představují speciální vstupní směrovač, který se používá v boji proti cenzuře. Informace o tomto směrovači nejsou veřejně dostupné na adresářovém serveru. Proto není možné je skupinově blokovat.
- **Uživatelé**: Lze je rozdělit do dvou skupin podle typu připojení, které používají pro připojení k Toru. Přímé uživatele, kteří se připojují prostřednictvím veřejně

přístupných onion směrovačů a cenzurované uživatele, kteří se připojují pomocí mostu. Obě skupiny využívají skryté služby, které Tor nabízí.

Skryté služby

Tor, na rozdíl od Freenetu, umožňuje procházení Surface webu a je možné se jednoduše dostat na stránky typu YouTube nebo Reddit. Pro prohlížení Surface webu používá v základu vyhledávač DuckDuckGo. Především ale Tor poskytuje přístup ke skrytým službám. Ke skrytým službám lze přistupovat pomocí tzv. onion odkazů. Název vychází z faktu, že tyto odkazy používají doménu .onion. URL těchto stránek je většino tvořena různými, nic neříkajícími kombinacemi čísel a písmen. Tyto řetězce znaků jsou odvozeny z vygenerovaných veřejných klíčů. Příkladem onion adresy může být odkaz na výše zmiňovaný Mullvad VPN: o54hon2e2vj6c7m3aqqu6uyece65by3vgoxxhlqlsvkmacw6a7m7kiad.onion. Avšak jsou i případy, kdy jsou odkazy tvořeny smysl dávajícími slovy, například Facebook má adresu facebookwkhpilnemxj7asaniu7vnjjbiltxjqhye3mhbshg7kx5tfyd.onion (dříve také facebookcorewwwi.onion) [52]. Jelikož není možné si takovéto řetězce pamatovat, existují portály, které nabízejí výpis těch hodně používaných. Nejznámější je The Hidden Wiki. Jedná se o skupinu wikiwebů, které poskytují onion odkazy na různé skryté služby. Většinou jsou dané odkazy rozděleny do kategorií jako například Bitcoin, drogy, pornografie apod. Původní The Hidden Wiki fungovala jako skrytá služba. Dnes existuje takovýchto stránek několik a jsou volně přístupné na Surface webu.

Provoz koncového uzlu

Provoz koncového uzlu může být sice šlechetná věc, jelikož klient takto přispívá k funkci sítě Tor. Byť samotný provoz nelegální není může se rychle stát nelegálním stát. Příkladem budiž případ Rakušana Williama Webera z roku 2012, který byl zatčen za provozování koncového uzlu, přes který byla distribuována dětská pornografie. Weber operoval 7 koncových uzlů, přes které proudily terabyty dat denně. Sám Weber tvrdil, že neměl tušení, jaká data přes jeho uzly uživatele posílají a stál si za tím, že provozuje dané uzly pouze za účelem, aby poskytl uživatelům možnost necenzurovaného přístupu na internet bez strachu ze stíhání státem [27].

Co Tor nedokáže

Henderson L. [7] uvádí následující:

- **Tor nedokáže ochránit klienta před přílohami:** toto není limitováno pouze na spustitelné soubory, ale i na Flash videa, RealPlayer či Quicktime, pokud je uživatel stále používá, neboť tyto aplikace mohou být nakonfigurovány tak, aby odesílaly skutečnou IP adresu klienta protivníkovi. Vždycky je důležité volit otevřený software, pokud je to možné.
- **Tor nedokáže dobře provozovat Torrent:** spousta lidí to používá, přesto to je velký problém. Tor rovněž nemůže provozovat P2P aplikace jako eMule nebo Limewire. Jednoduše to vysává spoustu bandwidth a způsobuje to velice pomalý provoz ostatním uživatelům Toru. Navíc některé koncové uzly jsou už v základu nastaveny tak, aby blokovaly takovýto provoz. K tomu ještě bylo dokázáno, že je možné odhalit IP adresu klienta, který používá Torrent přes Tor. Pro Torrent je mnohem lepší volbou používat VPN.
- **Tor nedokáže zakrýt indentitu:** tuto část tato práce rozebírá v zásadách anonymního chování. Tor je pouhý nástroj umožňující určitou úroveň anonymity. Za předpokladu, že klient porušuje zásady anonymity, jako například, že používá svůj skutečný email všude, kde může, je jakýkoliv anonymizující nástroj zbytečný.

5.5.9 Tails

„Pokud se podíváte na to, jakým způsobem byli whistlebloweři chyceni po roce 2013, je jasné, že ta absolutně nejdůležitější věc, co udělat, abyste si zajistili anonymitu, je snížit počet míst ve vaší provozní činnosti, kde můžete dělat chyby. Tor a Tails přesně to dělají.“
—**Edward Snowden**, NSA whistleblower

„Tails rozšiřuje ochrany Toru na celý operační systém a dělají to s neochvějným závazkem k jejich společenské smlouvě. Tails je oblíbený společník Toru.“
—**Roger Dingledine**, spoluzakladatel projektu Tor

Celým názvem The Amnestic Incognito Live System[16], je otevřený a na zabezpečení zaměřený operační systém Unixového typu založený na Linuxové distribuci Debian. Pro

[16] Tails je dostupný zdarma na adrese: https://tails.boum.org/install/index.en.html.

prohlížení internetu využívá prohlížeč Tor. Dále také obsahuje aplikace pro práci s dokumenty či zabezpečenou komunikaci [29]. Mimo jiné obsahuje i aplikace, které nelze s anonymitou nijak spojovat, jako například GIMP nebo Audacity. Tails dbá na anonymitu tak moc, že i samotní autoři jsou neznámí [7].

Funkce

Tails funguje odděleně od operačního systému a pevného disku. Tudíž odpadá riziko chycení počítačového viru. Tails udržuje vše v čistém stavu – když klient vypne Tails, veškerá jeho činnost zmizí. Podle oficiálního webu [29] patří mezi nabídku nástrojů pro udržování soukromí uživatele následující:

- Prohlížeč Tor a *uBlock*, pro blokování reklam.
- *Thunderbird*, pro zašifrování emailů.
- *KeePassXC*, pro vytvoření a uložení silných hesel.
- *LibreOffice*, balíček pro kancelářské práce.
- *OnionShare*, pro sdílení souborů přes Tor.
- *Metadata Cleaner*, pro odstranění metadat se souborů.

Instalace

Jelikož se jedná o tzv. Live System, není možné Tails uložit na hard disk. Jediný způsob, jak uchovávat Tails je pomocí médií jako flash disk, DVD nebo SD. Z těchto médií lze poté Tails nabootovat. Nevýhodou DVD však je, že s každou aktualizací se musí dané DVD vypálit znovu, což samozřejmě u flash disku nehrozí.

Tails nabízí čtyři možnosti instalace na základě toho, z jakého operačního systému ho chce uživatel stáhnout – Windows, macOS, Linux nebo Ubuntu/Debian terminál. Postup instalace je na každé této platformě podobný, ale maličko jiný – je důležité postupovat podle postupu popsaného na oficiální stránce. Nabízí verzi ke stažení jak na flash disk, DVD tak i na Virtuální stroj. Velikost instalačního souboru je přibližně 1.3 GB a mimo klasický způsob nabízí stránka i stažení přes BitTorrent. Během instalace je potřeba provést verifikaci, ideálně pomocí OpenPGP. K instalaci je také si zapotřebí pořídit dodatečnou aplikaci. V případě Linuxu se jedná o GNOME, v případě Windows a macOS to je aplikace balenaEtcher [29].

Limity Tails

Henderson L. [7] popisuje limity Tails následovně:
Tails ani Tor nedokáží zašifrovat dokumenty automaticky. Pro tyto případy je potřeba použít GnuPG nebo LUKS. Avšak některé dokumenty jako Word nebo Atlantis mohou požadovat registrační informace v rámci daného dokumentu. Při registrování věcí používaných v Tails je vhodné používat falešných údajů. Dále je vhodné zmínit, že Tails neskrývá fakt, že jej uživatel používá před jeho ISP (pokud nepoužívá Tor mosty). ISP ovšem nedokáže vidět, k čemu přesně uživatel Tails nebo Tor používá. Poslední nevýhodou je fakt, který platí o každém anonymizujícím nástroji – Tails nedokáže zabránit lidskému selhání. Vhodné je nepoužívat Tails najednou pro dva projekt, ale pro každý projekt zvlášť. Izolování obou identit prospívá posílení anonymity jedince.

5.5.10 Qubes OS

„Pokud to se svým soukromím myslíte vážně, Qubes OS je ten nejlepší operační systém, co je dnes v dostání. Používám ho já, zdarma.“
—**Edward Snowden**, NSA whistleblower

„Když používám Qubes cítím se jako Bůh. Software si myslí, že to má pod kontrolou, že si může dělat co chce? Nemůže. Já to mám pod kontrolou.“
—**Micah Lee**, ředitel informačního zabezpečení zpravodajského serveru The Intercept, poradce pro DDoSecrets

Qubes OS[17] je otevřený, na zabezpečení orientovaný operační systém [30].

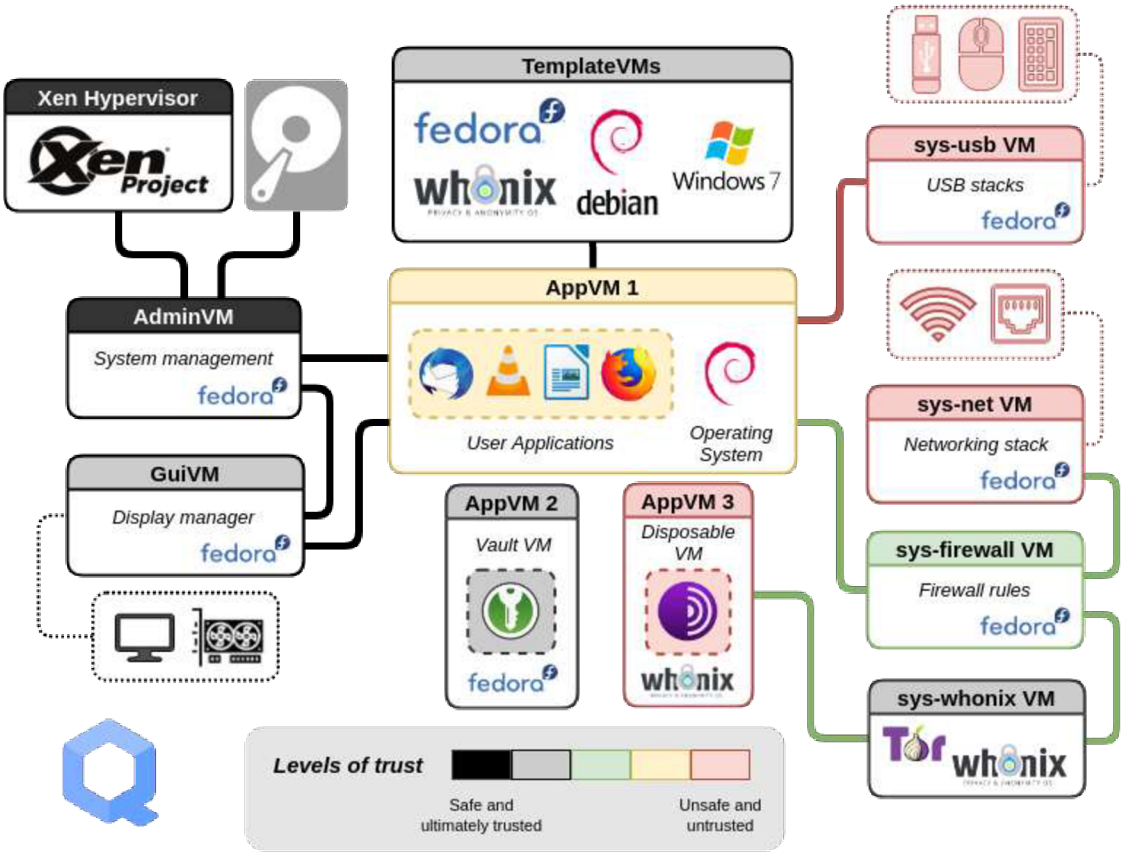
Architektura

Qubes OS využívá virtualizaci založenou na Xenu, která umožňuje vytváření a správu izolovaných oddílů nazývaných qubes.
Tyto qubes jsou implementovány jako virtuální stroje a jejich specifikacemi jsou:

- **Účel:** předdefinovaná sada jedné nebo více izolovaných aplikací, pro osobní nebo profesionální projekty, umožňují správu síťového zásobníku, firewallu či plnění dalších, uživatelem definovaných účelů.

[17] Qubes OS je dostupný zdarma na adrese: https://www.qubes-os.org/downloads/.

- **Povaha:** virtuální stroje jsou založeny na populárních operačních systémech jako Fedora, Debian či Windows.
- **Úroveň důvěry:** od úplné po neexistující. Všechna okna jsou zobrazena v jednotném pracovním prostředí s nefalšovatelnými barevnými okraji oken, takže různé úrovně zabezpečení jsou snadno rozpoznatelné [30].



Obr. 1. Úrovně důvěry Qubes OS.
Zdroj: https://www.qubes-os.org/intro/

Mezi základní funkce Qubes OS patří:

- **Silná izolace:** izoluje různé části softwaru jako by byly nainstalovány na různých fyzických strojích s využitím pokročilých virtualizačních technik.
- **Systém šablon:** používá aplikace qubes ke sdílení kořenového systému souborů, aniž by uživatel musel obětovat zabezpečení pomocí inovativního systému šablon.
- **Více operačních systémů:** používá více operačních systémů současně, včetně Fedory, Debianu a Windows.
- **Jednorázový:** vytváří za běhu věci na jedno použití, které se po vypnutí samy zničí.
- **Integrace Whonixu:** spouští Tor bezpečně v celém systému pomocí Whonix s Qubes.

- **Izolace zařízení:** bezpečná manipulace se zařízením pomocí izolace síťových karet a USB řadičů.
- **Split GPG**: využívá Split GPG, pro udržení soukromých klíčů v bezpečí.
- **U2F proxy:** Qubes U2F proxy pro použití dvoufaktorových autentizačních zařízení bez vystavení webového prohlížeče plnému USB zásobníku [30].

Architektura Qubes umožňuje vytvářet oddělené virtuální stroje (domény – qubes), ve kterých pak běží aplikace, což samo o sobě nepřidává tolik na anonymitě, avšak jedná se o skvělý nástroj pro ochranu proti malware, jelikož je pro daný malware velice náročné dostat se pryč z dané domény [32].

Použití

Jak lze vidět na obrázku 1., Qubes OS používá různé úrovně důvěry, pro procházení nedůvěryhodných webových stránek by měl uživatel použít qube s nejnižší důvěrou, pro práci s důvěryhodnými aplikacemi klidně qube s důvěrou nejvyšší. Smyslem těchto úrovní důvěry je, že každý qube má možnost ovlivnit další aplikace v dané qube.

Dalším použitím Qubes OS je fakt, že v něm lze používat Whonix, přičemž se Whonix skládá ze dvou částí – Workstation a Gateway. Tyto části lze spustit v oddělených qubes, což je ještě více odděluje od sebe a nebudou schopny ovlivňovat další aplikace v jiných qubes.

5.5.11 Whonix

Whonix[18] je otevřený desktopový operační systém zaměřený na pokročilé zabezpečení a soukromí. Whonix je založen na Linuxové distribuci Kicksecure, která je založena na Debianu, anonymní síti Tor a na principu zabezpečení pomocí izolace. Jedná se o anonymní operační systém, který běží jako aplikace a přesměrovává veškerou internetovou komunikaci přes Tor. Whonix je instalován na hostitelský počítač jako virtuální operační systém [31].

Whonix funguje na principu dvou oddělených virtuálních částí - „Workstation“ a „Gateway“. Workstation je pracovní desktop, slouží pro veškerou práci, jakou chce uživatel v daném OS vykonávat. Gateway slouží pro komunikaci. Veškerá komunikace,

[18] Whonix je dostupný ke stažení zdarma na adrese: https://www.whonix.org/wiki/Download.

která ve Workstation probíhá, proudí skrz Tor, OS neumožní použití běžných prohlížečů, pokud však není Gateway spuštěn zároveň s Workstation, žádná komunikace skrz Tor neprojde. Tyto části jsou od sebe naprosto izolovány.

Henderson L. [7] vypichuje následující významné vlastnosti Whonixu, které jej činí více bezpečným:

- Anonymní publikování/Anti-cenzura.
- Anonymní email s Thunderbirdem nebo TorBirdy.
- Přidává proxy za Tor (klient -> Tor -> proxy).
- Ochrana proti úniku IP/DNS protokolu.
- Skrývá fakt, že klient používá Tor.
- Skrývá fakt, že klient používá Whonix.
- Mixmaster přes Tor.
- Zabezpečený a distribuovaný mechanismus synchronizace času.
- Zabezpečení pomocí izolace.
- Možnost posílání emailů anonymně bez registrace.
- Podpora VPN.
- Anonymní použití Adobe Flash
- Anonymní použití Javy/JavaScriptu

5.5.12 Tails vs Qubes OS vs Whonix

Všechny tři tyto distribuce jsou skvělými anonymizujícími nástroji. Operační systémy zaměřené především na zabezpečení/soukromí uživatele. Můžeme je rozdělit do dvou kategorií – Live CD a virtuální OS. Do kategorie Live CD spadá Tails, do druhé spadá Qubes OS a Whonix.

Následující tabulka ukazuje, proti kterým dohledatelným otiskům prstů[19] dané OS brání:

Tabulka 6. Porování OS z hlediska obrany proti otiskům prstů.

OS	Dočasné internetové soubory a cache soubory	Únik IP adresy	Úniky DNS a WebRTC[20]	Korelace provozu	Náhodné úniky provozu Clearnetu[21]	Analýza stylometrie[22]
Tails	✓	✓	✓		✓	
Qubes		✓	✓		✓	
Whonix		✓	✓	✓		

Zdroj: https://www.comparitech.com/blog/vpn-privacy/anonymity-focused-linux-distributions/

Všechny tyto tři OS mají své výhody a nevýhody, porovnání z webu Comparitech [32] je popisuje následovně:

Tails:

- **Výhody:**
  - Live CD jsou obecně velice jednoduché na použití. Stačí je jednou vypálit a pak použít kdekoliv, což je výhodné, pokud uživatel používá více nedůvěryhodných počítačů.
  - Tor ve výchozí konfiguraci OS poskytuje okamžitou anonymitu.
- **Nevýhody:**
  - Tails sám od sebe nešifruje dokumenty vytvořené během jeho používání, ale má funkci vytrvalého šifrovaného svazku, kterou lze k tomu použít.
  - Všechna Live CD neřeší problém jednolitosti; operační systém nemá žádnou segregaci, tudíž rizikové aktivity v jedné aplikaci mohou ovlivnit další aplikace.

[19] Otisk prstu (fingerprint) je pojem v kyberbezpečnosti, který značí skupinu informací, které se dají použít k identifikaci.
[20] WebRTC je rozhraní pro podporu telefonních hovorů, video chatu a p2p sdílení souborů.
[21] Clearnet je termín označující opak Darknetu. Popisuje veškerou část internetu, která nespadá pod Darknet.
[22] Stylometrie se často používá k přiřazování autorství, času a původu k anonymním nebo sporným dokumentům.

Qubes OS:

- **Výhody:**
    - Oddělení aplikací použitím sandboxových virtuálních strojů zajišťuje, že napadená aplikace nebo škodlivý JavaScript neovlivní další aplikace nebo hostitelský operační systém.
    - Použití Whonixu uvnitř Qubes OS zajišťuje ještě větší úroveň oddělení od internetu pomocí nuceného přesměrování veškerého internetového provozu přes Whonix Tor Gateway.
- **Nevýhody:**
    - Qubes se obtížně testuje, protože ve virtuálním počítači někdy nefunguje dobře či vůbec.

Whonix:

- **Výhody:**
    - Použití VirtualBoxu zajišťuje, že Whonix může používat nejširší okruh lidí. VirtualBox je dostupný pro každý přední operační systém a je zdarma.
    - Základní instalace je velmi jednoduchá a není zapotřebí žádných odborných znalostí k tomu, aby jej uživatel rozjel.
- **Nevýhody:**
    - I přes to, že je Workstation oddělená od hostitelského počítače, k žádné další separaci už nedochází. Provádění jak riskantních, tak bezpečných operací ve Workstation je stejně nebezpečné jako dělat je na hostitelském počítači.
    - Jelikož je anonymita poskytnuta pouze ve virtuálním stroji Workstation, může se stát, že jej klient zapomene použít a místo toho použije hostitelský stroj.

5.5.13 Kryptoměny

Kryptoměny jsou typem digitální měny či internetových peněz, které nemají fyzickou podobu. Často jsou decentralizované a otevřené. Používají zašifrované transakce, které jsou často transparetní a sledovatelné ve veřejné databázi, tzv. blockchainu. Transakce často fungují na principu peer-to-peer. Kryptoměny jsou velice bezpečným platidlem, avšak i tak se výjimečně stane, že dojde ke krádeži. Kryptoměny nejsou kontrolovány žádným státem či institucí. Většina kryptoměn má omezené množství, jež je možno vytěžit. Nejznámější kryptoměnou je Bitcoin (BTC) a lidé, kteří mluví o kryptoměnách, mají často na mysli právě Bitcoin. Bitcoin se stal tak silným jménem, že se kryptoměny většinou rozdělují do dvou kategorií – Bitcoin a altcoin, kde altcoin představuje jakoukoliv jinou kryptoměnu než Bitcoin. Kryptoměn existuje velká spousta, přičemž obecně nejsilnější jsou už dlouhé roky Bitcoin a Ethereum (ETH) [53]. Existují však i kryptoměny, které jsou kromě transakcí také silně zaměřeny na soukromí a anonymitu uživatele, jako například Monero (XMR), Dash (DASH) či Zcash (ZEC). Vedle „seriosních“ kryptoměn existují i kryptoměny, které byly vytvořeny za účelem recese, tzv. memecoin, mezi takové patří například Dogecoin (DOGE), který je považován za úplně první memecoin na světě, či třeba PUTinCoin (PUT) [54], [55], [56], [57], [58]. Kryptoměny jsou předním platidlem používaným na Dark webu.

Historie

Počátky kryptoměn se dají datovat až do 80. let minulého století, kdy začal americký kryptograf a počítačový odborník David Chaum experimentovat s elektronickou měnu a roku 1983 prezentoval svůj návrh elektronického anonymního systému eCash, který fungoval na konceptu slepých podpisů, které zakrývají obsah zprávy a pomoci veřejného a soukromého klíče dojde k ověření identity uživatele. Některé kryptoměny tento koncept využívají dodnes [13].

V roce 1998 vývojář Wei Dain vytvořil distribuovaný elektronický platební systém B-money, ve kterém původně navrhl použití dvou protokolů, kde jeden vyžadovat nesynchronní a neměnný kanál. B-money však nikdy nesklidil velký úspěch. Další kryptoměnou je Bit Gold, kterou vytvořil Nick Szabo, jenž je považován za pionýra, jenž vytvořil koncept, který vedl ke vzniku Bitcoinu. Tento koncept využívá spoustu blockchainových technik, jako třeba peer-to-peer síť, těžbu či kryptografii a asi nejvíce revolucionářská byla jeho vize decentralizace, jelikož se chtěl pomocí Bit Goldu odpoutat

od závislosti na centralizovaných distribucích a autoritách. I přes to, že byl Bit Gold ve výsledku velice neúspěšný, nepochybně byl velice důležitý pro budoucnost kryptoměn [33].

Další důležitou zmínkou je Hashcash, který je považován za jednu z nejúspěšnějších kryptoměn z éry před Bitcoinem. Byl vytvořen k mnoha účelům, mimo jiné také k prevenci nevyžádané pošty a proti DDoS[23] útokům. Odesílatel emailu přiložil před odesláním zprávy k hlavičce razítko, jehož výpočet zabral nezanedbatelné množství času a tím eliminoval spamy [13].

Všechny tyto tři výše zmíněné kryptoměny měly obrovský vliv na vnik, dnes historicky neúspěšnější kryptoměny, Bitcoinu.

Bitcoin

Bitcoin je kryptoměna vytvořena jedincem či skupinou pod pseudonymem Satoshi Nakamoto roku 2008. Jedná se o protokol umožňující peer-to-peer transakce, bez zásahu třetích stran, využívající technologie blockchainu. Bitcoiny se vytváří jako výsledek procesu nazývaného těžení. Bitcoin se dělí na jedno zvané satoshi, jeden satoshi je 100 000 000 BTC. Na světě existuje 2,099,999,997,690,000 jednotek satoshi, tzn. že maximální počet všech Bitcoinů, které kdy budou existovat, je přibližně 21 milionů. Čím více Bitcoinů bylo vytěženo, tím déle trvá vytěžit další. Předpokládá se, že poslední Bitcoin bude vytěžen kolem roku 2140 [34]. Podle webu Investopedia [35] bylo ke dni 29. 1. 2023 vytěženo již 19,276,325 Bitcoinů.

Monero

Monero je otevřená a decentralizovaná kryptoměna, založená roku 2014, zaměřená především na soukromí uživatele, využívající protokol CryptoNote, který se zaměřuje na vyřešení některých nedostatků Bitcoinu, mj. i otázku dohledatelnosti transakcí. Rovněž jako Bitcoin, i Monero se získává procesem těžení, avšak na rozdíl od Bitcoinu, Monero nemá žádný maximální počet bloků, kterých lze dosáhnout, avšak mají dynamickou velikost [36].

---

[23] DDoS - Distributed Denial of Service je druh kybernetického útoku, kdy útočník provádí opakovaný pokus o připojení za pomocí velkého množství počítačů, což způsobuje pád serveru.

Dash

Dash, dříve také známy jako Digital Cash, Darkcoin či XCoin, je otevřená a peer-to-peer kryptoměna zaměřená na soukromí a anonymitu uživatele, založená na kryptoměně Bitcoin [37]. Dash využívá tzv. „masternodes“, jedná se o servery, které jsou navrženy tak, aby poskytovaly pokročilé služby a správu blockchainu. Masternodes hostují plné kopie blockchainu a poskytují síti druhou vrstvu, která usnadňuje pokročilé funkce, jako InstantSend nebo CoinJoin [38].

Zcash

„Momentálně považuji Zcash za nejvíce zajímavý, protože jeho vlastnosti zajišťující soukromí jsou vážně unikátní.“

—**Edward Snowden**, NSA whistleblower

Zcash je decentralizovaná, peer-to-peer kryptoměna založená na Bitcoinu s několika klíčovými vylepšeními, jako například chránění adres. Zcash byl vytvořen týmem světově uznávaných vědců z MIT. Zcash se snaží svým klientům poskytnout rychlou, bezpečnou a spolehlivou metodu obchodování na internetu. Podobně jako Bitcoin i Zcash používá veřejný blockchain [40].

Kryptoměnová peněženka

Své kryptoměny si musí člověk někde uchovávat. K tomuto účelu byly vytvořený kryptoměnové peněženky. Krypto peněženky slouží k uchovávání privátních klíčů neboli hesel, které slouží k přístupu k dané kryptoměně. Mohou mít mnoho podob, jak hardwarové, jako například Cryptosteel, což je kovová kapsule, určená na ukládání důležitých dat, která dokáže vydržet i v extrémních podmínkách, jako jsou i různé přírodní katastrofy, tak i nabízí zašifrování heslem, tak mohou být peněženky i softwarové, například v podobě různých mobilních aplikací, či je dokonce možné mít peněženku uloženou na papíře [59], [60].

Mnoho kryptoměn nabízí své vlastní peněženky, například Monero nabízí vlastní Monero GUI Wallet a Monero CLI Wallet, které nabízí peněženku ve formě jak grafického rozhraní, tak příkazového řádku. Zcash nabízí například YWallet či Zecwallet [61], [62].

Zajímavým projektem byl Dark Wallet, což byl brzký pokus o navýšení anonymity Bitcoinových transakcí. Byť nebyl nikdy dokončen, inspiroval další projekty, jež se snaží zvýšit anonymitu používání Bitcoinu. Mezi takové patří například Samourai Wallet či Electrum Wallet [45].

Anonymita kryptoměn

Různé kryptoměny nabízí různé úrovně soukromí a anonymity za pomoci různých technologií. V první řade je dobré zmínit, že pro zvýšení zabezpečení a anonymity, je vhodné kombinovat více krypto peněženek, jak hardwarových, tak softwarových. V případě centralizovaných kryptoměn se nedá o otázce anonymity moc bavit, jelikož si při jejich používání musí uživatelé založil účet za použití svých skutečných údajů a souhlasit s jejich zpracováním. Největším problémem decentralizovaných kryptoměn je transparentnost. Tato část pojednává o srovnání anonymizujících technologií jednotlivých kryptoměn.

- **Bitcoin:** Byť spousta lidí považuje Bitcoin za anonymní platidlo, pravdou je, že Bitcoin sám o sobě moc anonymní není, i když je možné různými kroky jeho anonymitu navýšit. Hlavním problémem u Bitcoinu je fakt, že i když je decentralizovaný, tak veškeré transakce jsou zcela transparentní. Na problém transparentnosti Bitcoinu poukazuje i Edward Snowden, který se vyjádřil, že Bitcoin je asi nejtransparentnější, ze všech kryptoměn a je lepší dívat se po alternativách. Každá peněženka v bitcoinové síti má veřejnou adresu, kterou lze považovat za „pseudonymní" identitu. Čím dále si mohou uživatelé Bitcoinů ponechat své pseudonymní identity od svých skutečných identit, tím anonymnější budou jejich identity. To se však často snáze řekne, než udělá – IP adresy lze vysledovat, lze identifikovat vzorce transakcí a další faktory mohou orgánům činným v trestním řízení nebo dokonce jen zvědavým členům veřejnosti umožnit zjistit, komu konkrétní adresa peněženky patří [39]. Volejník R. [26] se tomuto problému věnuje, i s jejich nevýhodami, a vyčleňuje následující možnosti:
    - **Bitcoinové bankomaty:** Existují po světě rozmístěné bankomaty, které umožňují lidem fyzicky vkládat peníze, výměnou za Bitcoin či naopak. Nevýhodou těchto bankomatů však je, že jsou často velice dobře monitorovány, ostatně jako běžné bankomaty.
    - **Šejkr:** Jedná se o mixovací službu, kde uživatel pošle své Bitcoiny na server, kde se nahrnou na hromadu společně s Bitcoiny dalších uživatelů a poté jsou vlastníkovi v menších částkách vráceny. Je však důležité, aby vrácena částka

dorazila na nově vzniklou peněženku, jinak je celý proces zbytečný. Nevýhodou šejkru však je, že klient posílá své Bitcoiny cizí, anonymní osobě s tím, že doufá, že se mu pak vrátí zpět na jiný účet. Existují případy lidí, kteří byli tímto způsobem okradeni. Šejkr si navíc za své služby účtuje poplatky – jedno až tři procenta z dané částky.

- **CoinJoin:** Jedná se o metodu, kdy uživatel složí částku do velké transakce, kterou sdílí s jinými uživateli, kde dojde k množstevní shodě s jinými uživateli. Funkci lze popsat například takto: uživatel A posílá peníze B a C posílá peníze D. Pokud jsou obě částky stejné, CoinJoin tyto vstupy zamění. Výstupem transakce bude tedy to, že A zaplatí D a C pošle své Bitcoiny B. Čím více uživatelů používá tyto servery, tím více se vstupy a výstupy transakce mixují. Velké množství uživatelů tak zlepšuje soukromí a vytváří transakci složitější na vystopování. Nevýhodou CoinJoin však je, že byl za účelem analýzy vytvořen software CoinJoin Sudoku, jež dokázal sjednotit 69 % vstupů s 53 % výstupy u jedné transakce. Pro zvýšení účinnosti je lepší metodu CoinJoin několikrát opakovat, ale i tak se pravděpodobně uživatel nedostane na 100% anonymnost.
- **Tor:** Problém, se kterým se lze setkat při používání Toru, je tzv. Man-in-the-middle Attack neboli „muž uprostřed“. Pokud je tento útok úspěšný, dokáže útočník nejen identifikovat uživatele, ale zároveň ho i připravit o finance.

- **Monero:** Na rozdíl od kryptoměn jako Bitcoin či Zcash, Monero není transparentní. Každý uživatel je při používání Monera již od začátku anonymní. Odesílatel, příjemce i částka jsou skryty, a to za pomocí technologií jako Stealth Addresses, Ring Signatures a RingCT [36]. Monero dále využívá technologii CryptoNote, jež zajišťuje anonymní transakce pomocí I2P funkci, která skrývá IP adresy a také díky čtyřem bezpečnostním klíčům. Krom základního veřejného a soukromého spend klíče má Monero ještě veřejný a soukromý view klíč, skrývající identitu příjemce. Ring Signature slouží ke skrytí identity odesílatele, jelikož transakci nepodepisuje pouze pravý odesílatel, ale další již v blockchainu použité podpisy pro zmatení. RingCT slouží pro skrytí výše transakce. Další výhodou Monera je zaměnitelnost. To znamená, že není možné zjistit, k čemu byla daná transakce použita [13].

- **Dash:** Dash využívá algoritmus X11. Řetězový hashovací algoritmus X11 využívá posloupnosti jedenácti hashovacích algoritmů[24] pro princip Proof-of-Work[25]. To proto, aby distribuce zpracování byla spravedlivá a mince byly distribuovány v podstatě stejným způsobem, jako Bitcoiny. Algoritmus X11 používá více řad 11 různých hashů (blake, bmw, groestl, jh, keccak, skein, luffa, cubehash, shavit, simd, echo), což z něj dělá jeden z nejbezpečnějších a nejpropracovanějších kryptografických hashů používaných moderními kryptoměnami. Mezi výhody algoritmu W11 patří, že zvýšená složitost a sofistikovanost zřetězeného algoritmu poskytuje vyšší úroveň zabezpečení a menší nejistotu pro digitální měnu ve srovnání s algoritmy PoW s jedním hashem, která nejsou chráněna proti bezpečnostním rizikům, jako je Selhání jednoho bodu (SPOF – Single Point Of Failure) [38]. Dále Dash využívá technologie Instant Send, které slouží pro rychlé potvrzení, a Private Send. Private Send je mixovací služba založena po vzoru CoinJoinu, jež mixuje Bitcoiny a funguje na velice podobném principu. Jedná se o obdobu určenou pro Dash, jelikož je tato služba provozována pomocí masternodes, ve které uživatelé Dashe mixují své mince s jinými uživateli. Na rozdíl od Monera, Dash používá veřejný transparentní blockchain. Pokud někdo zná danou Dash adresu, dokáže vidět všechny transakce, které jsou dovnitř a ven. Monero na rozdíl od Dashe poskytuje uživateli soukromí a anonymitu, aniž by musel cokoliv dělat, v případě Dashe musí uživatel sám využívat mixovací služby závislé na masternodes, které zajišťují decentralizovanost, určitou úroveň soukromí a docela spolehlivé mixování [41].
- **Zcash:** Zcash nabízí dva typy adres: soukromé (z-adresy) a transparentní (t-adresy). Transakce mezi soukromými adresami jsou soukromé a neodhalují žádnou adresu ani částku. Transakce transparentní jsou zcela viditelné jako například v případě Bitcoinu. Zcash podporuje MultiSigna transakce, o kterých bude tato práce pojednávat později [40]. Dále Zcash využívá technologii Halo 2, která využívá kryptografický „zero-knowledge“ protokol. Zero-knowledge umožňuje jedné straně dokázat straně druhé, že dané prohlášení je pravdivé, aniž by byly odhaleny jakékoliv další informace. Například, pokud bychom měli náhodný hash náhodného čísla, mohli bychom dokázat druhé straně, že existuje číslo s takovou hash hodnotou, aniž

[24] Hash je funkce umožňující převod vstupních dat do malého čísla.
[25] Proof-of-Work (PoW) je technika kryptoměn, pomocí které se ověřuje hodnota nové transakce přidané do blockchainu.

bychom jí odhalili. Můžeme dokázat, že dané číslo existuje a i to, že známe jeho hodnotu, aniž bychom jí vyzradili [42]. Halo 2 také zahrnuje tzv. Pasta křivky. Pasta křivky jsou kryptografický konstrukt, který se skládá ze dvou eliptických křivek, pojmenovaných po dvou planetách – Pallas a Vesta. Pasta křivky spolu tvoří cyklus: pořadí každé křivky je přesně základním polem té druhé. Tato vlastnost je kritická pro efektivitu rekurzivních důkazních systémů. Jsou navrženy tak, aby byly vysoce 2-adické, což znamená, že v každém poli existuje velká multiplikativní podskupina s mocninou dvou. Mezi výhody Pasta křivek patří, že jsou postaveny na konstrukci 255bitového primárního pole, což zajišťuje 126bitovou ochranu proti Pollard rho útokům[26] a umožňuje, aby komprimovaná reprezentace bodů byla 32 bajtů. Obě pole nemají multiplikativní podskupiny 5. řádu, 7. řádu atd., takže umocňování těmito malými prvočísly je permutace, což je zásadní požadavek pro algebraické hashovací funkce, jako je Rescue a Poseidon [44].

[26] Pollard rho útok je druh útoku, který používá algoritmus na principu náhodné procházky, aby našel kolize ve funkcích.

6 Analýza Darknetu

6.1 Historie

Samotný začátek Darknetu sahá až po počátky samotného internetu, kdy byl v roce 1969 americkým ministerstvem obrany zpuštěn ARPANET, což byla síť, která umožňovala komunikovat počítačům mezi sebou. ARPANET používaly především americké univerzity, až se z něj stal časem základní kámen toho, čemu dnes říkáme internet. Věří se, že skrze ARPANET proběhl úplně první internetový obchod v historii, kdy se v roce 1971 nebo 1972 studenti ze Standfordovy univerzity domluvili se studenty z Massachusettského technologického institutu na prodeji marihuany. V roce 1989 sir Tim Berners-Lee, pracovník CERNu, vytvořil World Wide Web a o rok později k němu používané standardy, jako HTML, URI / URL a HTTP. V roce 1991 byl pak internet přístupný mezi širokou veřejnost [46].

Úplně první formou moderního Darknetu bylo, když v roce 2000 student Ian Clarke vyvinul a vydal Freenet. Samotné zpopularizování Darknetu však přineslo až spuštění Toru v roce 2002. Tor byl vytvořen pro americké zpravodajské služby, aby mohly komunikovat přes internet bez možnosti identifikace. Tor byl vydán v roce 2004 jako otevřený software a poté financován pomocí neziskové organizace jménem Tor Project [47].

6.1.1 Silk Road

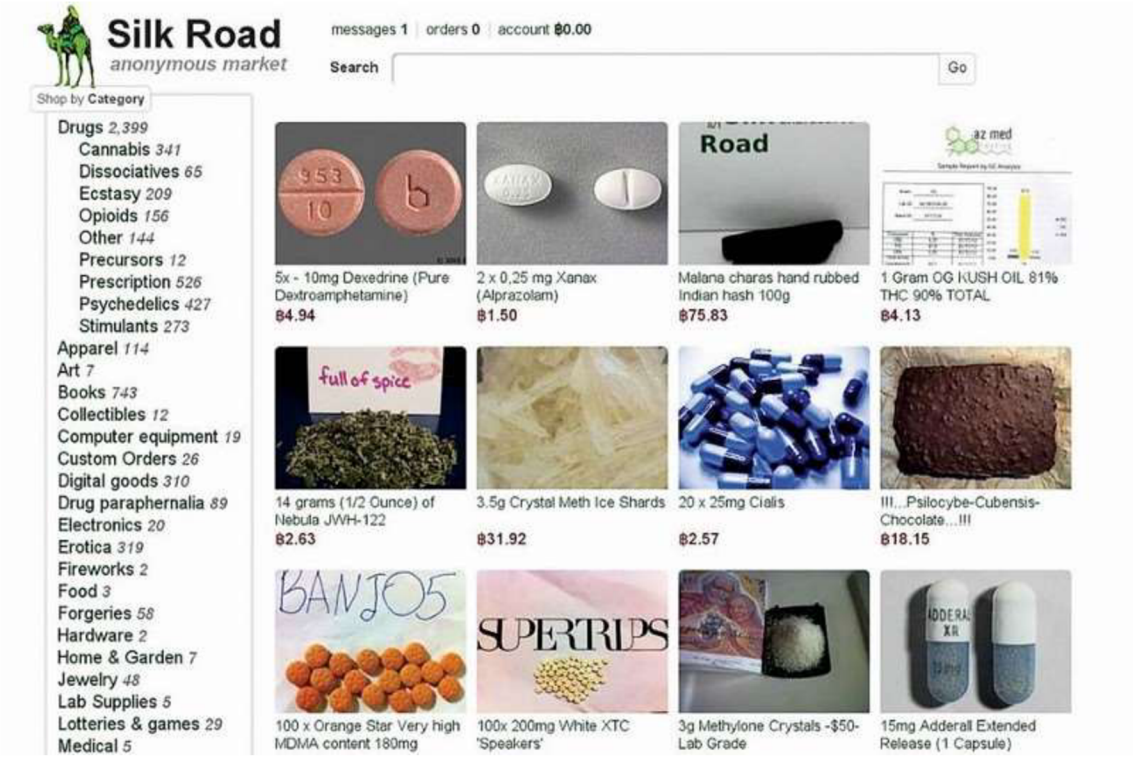
Silk Road je historicky první darknetové tržiště spuštěné Rossem Ulbrichtem v roce 2011. Myšlenka založení Silk Road napadla Ulbrichta už v roce 2009, jelikož začal chápat daně a vládu jako formu donucování. Jeho hlavní myšlenkou bylo: *„vytvořit webové stránky, kde si mohou lidé koupit cokoliv anonymně, bez zanechání stop, které by k nim mohly vést.“*. Později se rozhodl pro pěstování psychedelických hub, které chtěl na svém webu prodávat. Ulbricht využíval služby Freedom Hosting, která za poplatek umožňovala hostování .onion webů. Servery Freedom Hostingu byly však opakovaně napadány hnutím Anonymous kvůli poskytování dětské pornografie [48].

Silk Road byl prvně spuštěn v roce 2011 na adrese tydgccykixpbu6uz.onion, dále Ulbricht vytváří stránky silkroad420.wordpress.com a silkroadmarket.org, kde se snaží svůj

obchod zpropagovat a poskytuje návod, jak se na něj dostat. Propagandu svého obchodu také provozoval na jiných stránkách, zaměřených například na psychedelika [48].

Pět měsíců po spuštění se na serveru gawker.com objevuje článek „The Underground Website Where You Can Buy Any Drug Imaginable“, který popisuje zážitky softwarového developera Marka, který si na Silk Road koupil LSD. V tomto období dojde k velkému nárustu prodejců na Silk Road, kteří mimo produktů, jako je marihuana, stimulanty, opiáty apod., nabízí i služby a digitální zboží. Po vydání tohoto článku se sice návštěvnost stránky rapidně zvýšila, na druhou stranu se v tomto období dostalo Silk Road do hledáčku agentů DEA[27]. V roce 2012 byl však policejními složkami provoz Silk Road ukončen a v roce 2015 byl Ross Ulbricht odsouzen k odnětí svobody na doživotí, bez možnosti předčasného propuštění [48].

Byť samotná existence Silk Road trvala pouhý rok, byla předchůdcem mnoha obdobných tržišť, které po jejím zániku vznikly.



Obr. 2. Silk Road.
Zdroj: https://ipure.cz/archiv/magazin/deep-a-dark-web-temna-strana-internetu/

[27] DEA – Drug Enforcement Administration je americký policejní orgán, zabývající se bojem proti pašování a distribuci drog.

6.2 Obchodování na Darknetu

Na Darknetu se vyskytuje obrovské množství černých trhů nabízející všemožné produkty, avšak spousta z nich rovněž fungují pouze jako podvodné stránky. Podvodné obchody většinou nemají dlouhou životnost kvůli špatné reputaci či kvůli naštvaní špatných lidí, kteří pak daný obchod bombardují DDoS útoky. Existují však způsoby, jak může klient snížit šanci toho, že při nákupu na černém trhu bude okraden.

Mezi první indicie patří recenze. Velké a důvěryhodné obchody budou mít na svých stránkách spoustu kladných a důvěryhodných recenzí. Je však důležité umět rozeznat skutečné recenze od falešných.

6.2.3 Escrow

Dalším a vysoce používaným způsobem je využití escrow transakcí. Escrow transakce se používají při internetových nákupech v případě, že se prodejce a kupec neznají a není mezi nimi velká důvěra, a to především, když se jedná o nákup drahých věcí. Funkce escrow spočívá v tom, že mezi prodejcem a kupcem vzniká dohoda, že, za poplatek, bude platba procházet přes třetí osobu. Kupec tak při nákupu zašle peníze třetí osobě, která je drží, dokud prodejce nesplní všechny náležitosti obchodu. Poté, co kupec potvrdí, že zboží obdržel, pošle osoba držící peníze prodejci [49].

Použití escrow na Darknetu zavedl Silk Road. Na Silk Road si kupec vytvořil peněženku specifickou pro daný web a přesunul do ní své Bitcoiny ze své osobní peněženky. Poté, co byla objednávka zadána, převedl kupec své Bitcoiny ze Silk Road peněženky do peněženky kontrolované administrátorem Silk Road. Prodejce byl informován, že peníze kupce byly složeny do úschovy. Když pak kupce obdržel daný produkt, informoval o tom web a peníze byly poslány do Silk Road peněženky prodejce. Při návštěvě Silk Road vyskočila na uživatele zpráva pro nově příchozí:
„Vždy používejte systém escrow! Toto nelze více zdůraznit. 99 procent podvodů pochází od lidí, kteří si zakládají falešné účty prodejců a žádají kupující, aby jim zaplatili přímo nebo uvolnili platbu před doručením objednávky.“, tomuto se také říká podvod předběžné platby (Finalize Early – FE) [15].

6.2.4 MultiSigna

V roce 2014, administrátor stránky Silk Road 2.0, Defcon, navrhl novou, bezpečnější platební metodu za pomocí peněženky, ke které potřebujete více privátních klíčů, tzv. Multi-signature escrow (MultiSigna). Tato metoda funguje na principu toho, že se po přijetí nákupu prodejcem vytvoří nová krypto peněženka. Prodejce musí schválit objednávku, kupec musí schválit obdržení. a nakonec schvaluje samotná stránka. Peníze jsou však obdrženy až v případě, kdy aspoň 2 ze 3 použijí svůj podpis za pomocí PGP klíčů. Žádná strana tak nemůže zmizet s penězi. Pokud by došlo k nějakým problémům, dostává kupec peníze zpět [15].

6.2.1 Doručení zboží

Jamie Bartlett [15], který se rozhodl vyzkoušet nákup drog z Darknetu osobně, popisuje svou zkušenost takto: *„Je tu ještě jedna poslední překážka, kterou je třeba překonat: dostat se ke svým drogám. U všech chytrých platebních a mixovacích systémů musím uvést skutečnou adresu, abych mohl obdržet svůj produkt. Někteří lidé používají to, čemu se říká „drop address" – opuštěný dům s fungující poštovní schránkou. Většina lidí, včetně mě, prostě dodá svou domovskou adresu a důvěřuje v sílu „maskování". Prodejci jsou často řazeni podle toho, jak rychle a snadno jsou jejich balíčky doručeny – nebo jak důmyslně produkt maskují. Přestože se o maskovacích metodách mého prodejce v jeho recenzích nemluvilo – ze strachu, že by upozornil úřady, což jsem se dozvěděl na jednom fóru – byl velmi chválen. A taky docela oprávněně. Jednoho rána, pět dní poté, co jsem zadal svou objednávku, mi domů dorazil bílý balíček. Je velký asi jako pohlednice, ale trochu objemný – vycpaný bublinkovou fólií. Jméno a adresa, které jsem na stránku zadal pomocí svého klíče PGP, byly vytištěny na malé nálepce. Vypadalo, vonělo a vzbuzovalo to pocit přesně jako každý jiný balík, který jsem ten týden dostal. Uvnitř byl výrobek pečlivě zapečetěný, měl správnou hmotnost a podle mého známého odborníka se jevil jako mimořádně kvalitní. Poslední věc, kterou jsem musel před uzavřením účtu udělat, bylo zanechat krátkou a jednoduchou recenzi: ‚Drogy dorazily tak, jak je popsáno. 4/5.'".*

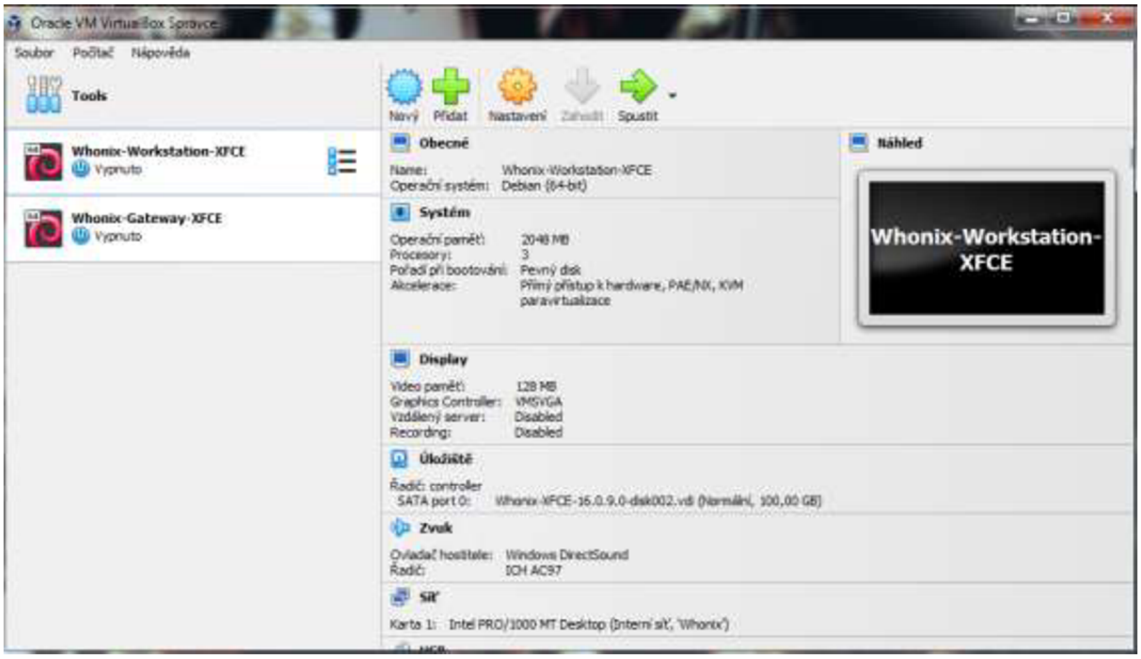
6.2.2 Hackování

Dalším velice oblíbeným zbožím na Darknetu hackovací pomůcky. Můžeme najít spoustu obchodů, které vedle různých malwarů[28] nabízí také například nástroje pro exploit[29], které jsou často používány například pro útoky nultého dne[30] (Zero day) či spoustu služeb typu „jako služba“[31] (as-a-Service), jako například DDoS-as-a-Service, Hacking-as-a-Service či Spam-as-a-Service. Malware je často nabízen s unikátními technikami na obcházení detekce, jako je různé zabalování, šifrování či svazování. Někteří prodejci dokonce nabízí i záruku toho, kolik uživatelů bude moct daný malware infikovat, než jej většina antivirů odhalí. Ceny těchto služeb v případě exploit nástrojů se většinou pohybují mezi 15 – 10 000 americkými dolary. Jednou z nejdůležitějších kritérií u ceny je délka licence. Například v roce 2011 stál Blackhole v1.2.1 700 dolarů za 3 měsíce nebo 1 500 dolarů za rok, zatímco Robopak stál 150 dolarů na týden a 500 dolarů za měsíc. Zero day exploity bývají dražší, a to většinou mezi 500 a 300 000 dolary a často závisí na kritériích jako je stáří nebo sofistikovanost. Příkladem rozsahu cen zero day exploitů z roku 2012 je 60 000 – 120 000 dolarů za Windows, 100 000 – 250 000 za iOS, 30 000 – 60 000 za Android a 5 000 – 30 000 za Adobe Reader [50].

[28] Malware je označení pro škodlivý software, příkladem může být například počítačový virus, červ, či trojský kůň.
[29] Exploit je označení většinou pro program, který využívá chyby v systému pro svůj prospěch.
[30] Zero day je druh útoku, který využívá nějaké chyby v systému, která ještě není moc známá a tudíž není pro ní moc obranných prostředků.
[31] As-a-service je byznysový model, ve kterém se prodavač snaží poskytnout zákazníkovi něco jako službu.

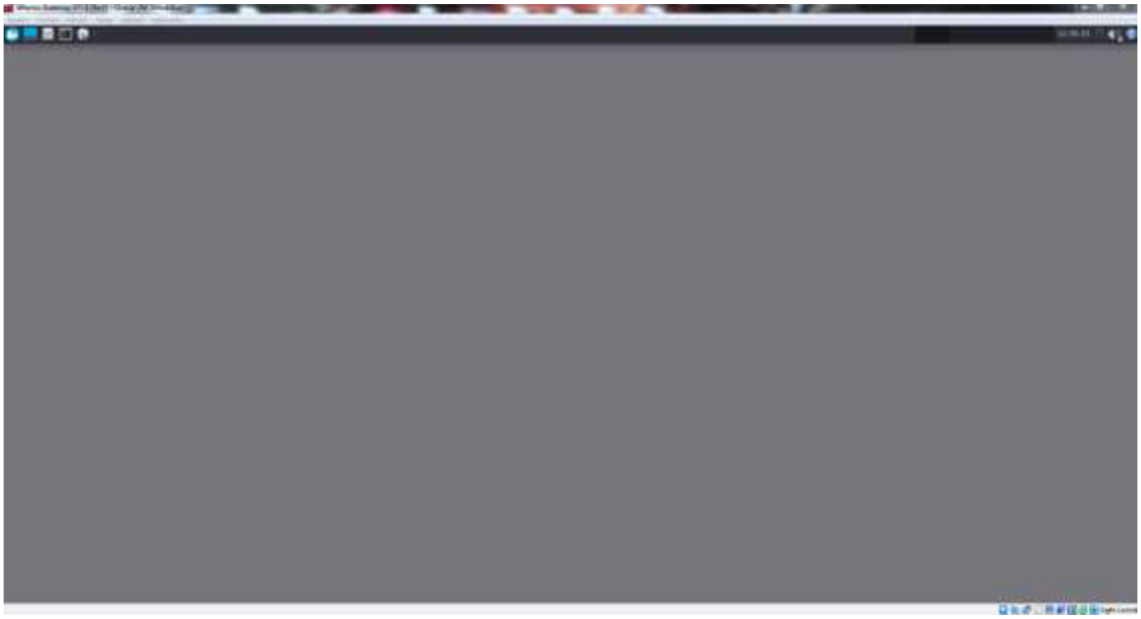
6.3 Pohyb na Darknetu

Pro demonstraci pohybu na Darknetu byl použit operační systém Whonix, který lze spustit jako virtuální OS, například za pomocí aplikace Oracle VirtualBox.



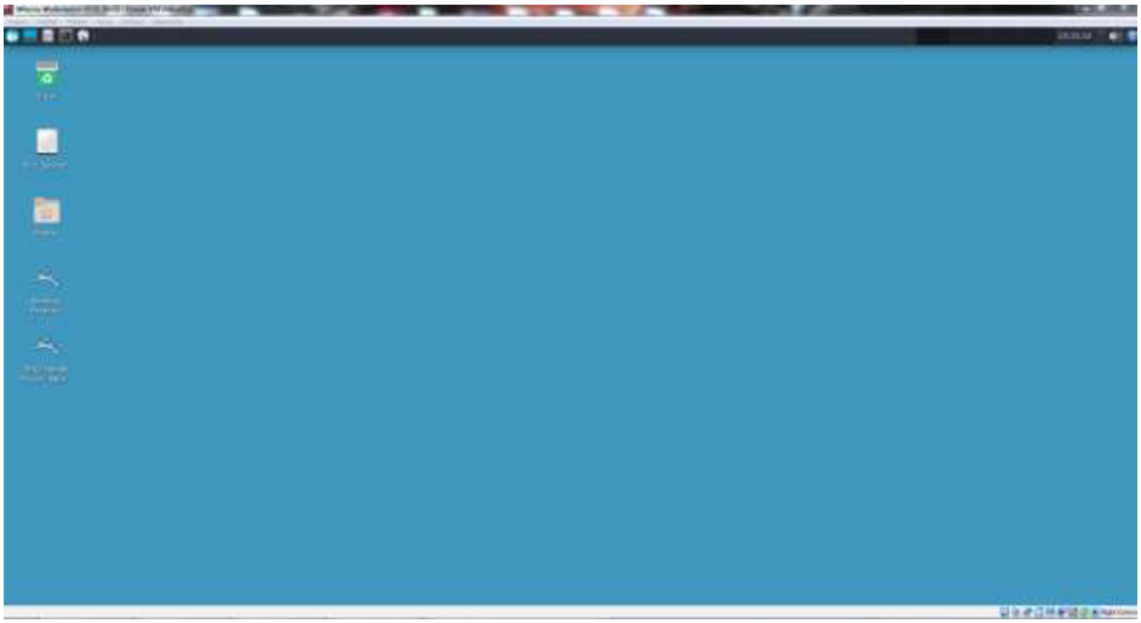
Obr. 3. Oracle VirtualBox.
Zdroj: vlastní zpracování.

Jak je popsáno v 5.5.11., Whonix se dělí na dvě části – Workstation a Gateway. Workstation slouží pro veškerou práci uživatele, zatímco Gateway slouží pouze pro připojení na internet. Bez běžícího Gateway není možné používat prohlížeč. Pro prohlížení Darknetu je tedy nezbytné, aby oba dva virtuální OS běžely zároveň.



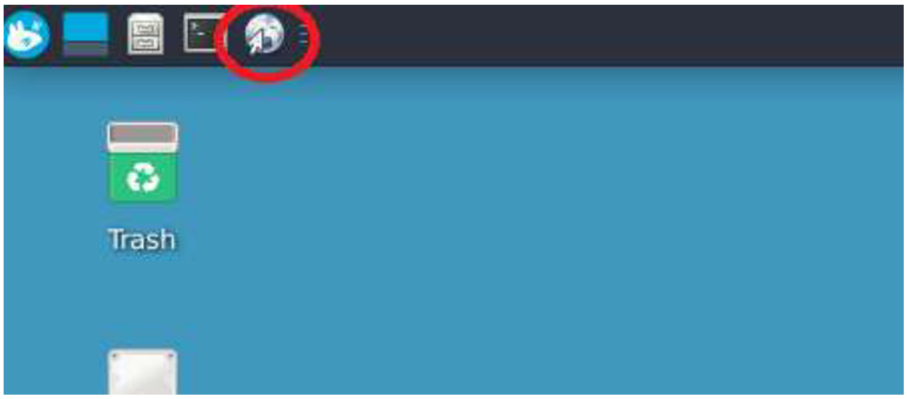
Obr. 4. Whonix Gateway.
Zdroj: vlastní zpracování.

Jak je patrné z obrázku, na ploše Gatewaye se nic nenachází. Gateway není určen pro práci, avšak lze v jeho terminálu provádět různé operace.



Obr. 5. Whonix Workstation.
Zdroj: vlastní zpracování.

Plocha Workstation už vypadá lépe a obsahuje také zástupce aplikací. Pro přístup na internet je potřeba kliknout na ikonu prohlížeče v hlavním panelu nahoře. Ikona prohlížeče je na níže přiloženém obrázku zvýrazněna červeným kroužkem.

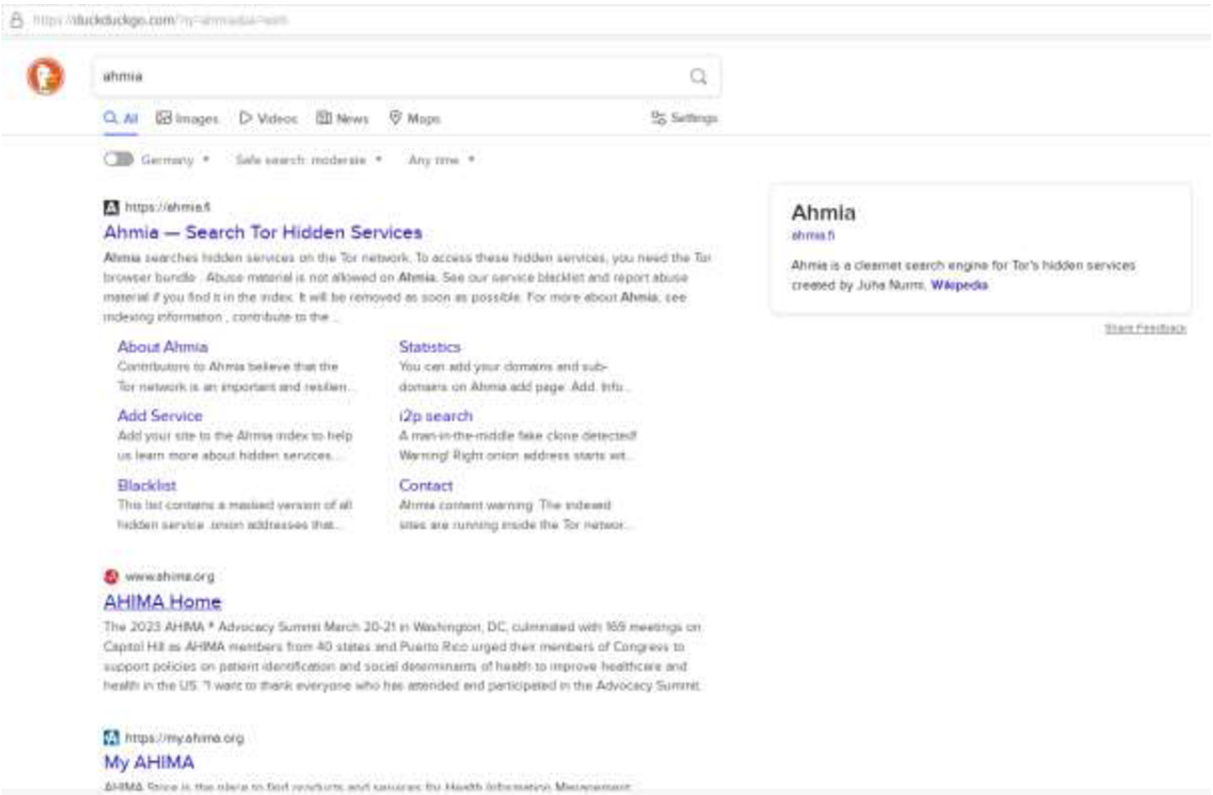


Obr. 6. Prohlížeč.
Zdroj: vlastní zpracování.

Už při prvotním spuštění Whonixu není zapotřebí provádět nějaké konfigurace či instalace. Všechno, včetně instalace Toru probíhá už při instalaci samotného OS, přičemž se instalace dá více specifikovat pomocí průvodce instalací. Hned při spuštění Whonixu lze tedy přistoupit na internet. Při kliknutí na ikonu prohlížeče se spustí prohlížeč Tor – Whonix nepovolí uživateli žádnou nezabezpečenou formu přístupu na internet.

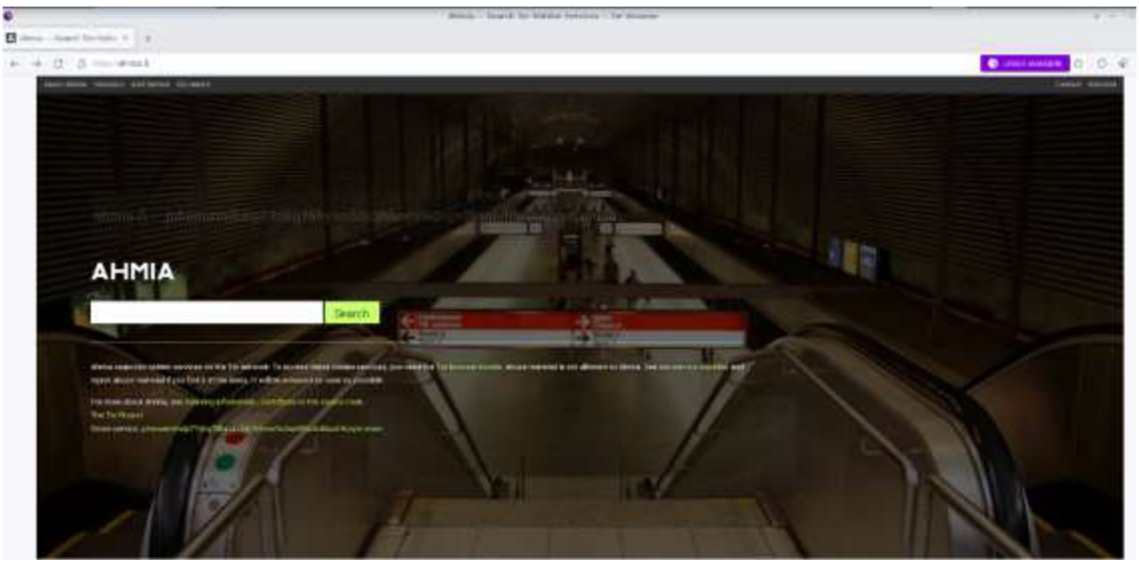
Obr. 7 Uvítací stránka Whonixu v prohlížeči Tor.
Zdroj: vlastní zpracování.

Při spuštění Toru lze vidět podobný scénář, jako při spuštění jiného regulérního internetového prohlížeče, jako je Firefox či Chrome. Po načtení prohlížeče uživatele jako první přivítá uvítací stránka Whonixu. Do horního vyhledávače lze zadávat odkazy na stránky či klíčová slova. Při zadání klíčového slova nám vyhledávač DuckDuckGo (DDG) ukáže stránku výsledků. DDG však neindexuje skryté služby, proto je zapotřebí se první dostat na stránku vyhledávače, který toto dokáže. Dobrým příkladem takového vyhledávače je Ahmia, na který se dá dostat i na Clearnetu.



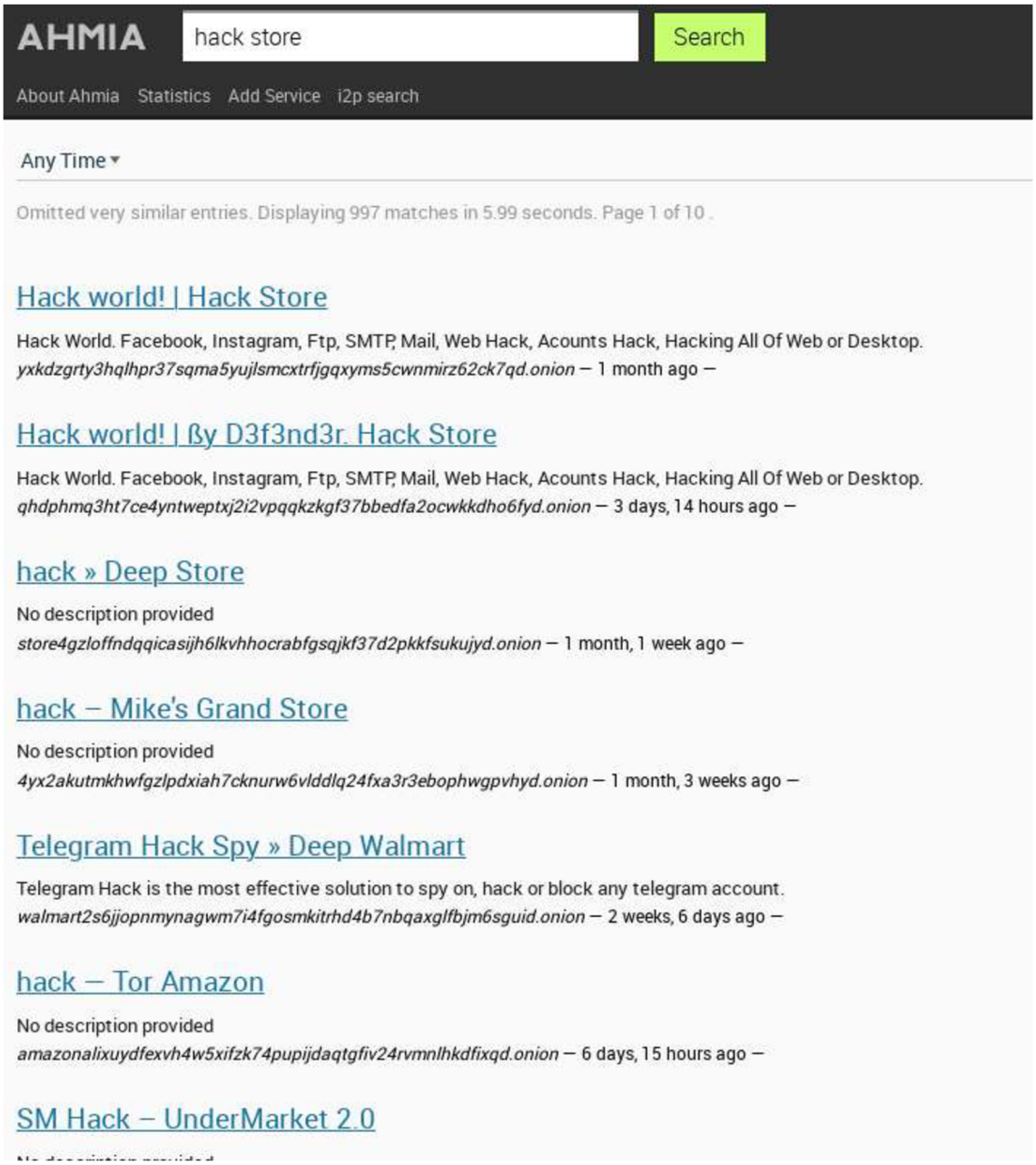
Obr. 8. Stránka výsledů vyhledávače DDG v prohlížeči Tor.
Zdroj: vlastní zpracování.

Lze tedy přistoupit na stránku vyhledávače Ahmia pomocí vyhledávače DDG nebo zadáním URL adresy do vyhledávače Toru.



Obr. 9. Vyhledávač Ahmia v prohlížeči Tor.
Zdroj: vlastní zpracování.

Na hlavní stránce vyhledávače se nachází především pole pro vyhledávání klíčových slov, ale také další věci, jako je onion adresa stránky či odkazy na stránky „O Ahmii“ či „Kontakty“. Do pole pro vyhledávání můžeme psát slova, na základě kterých bude vyhledávač, v tomto případě, již nabízet odkazy na skryté služby.

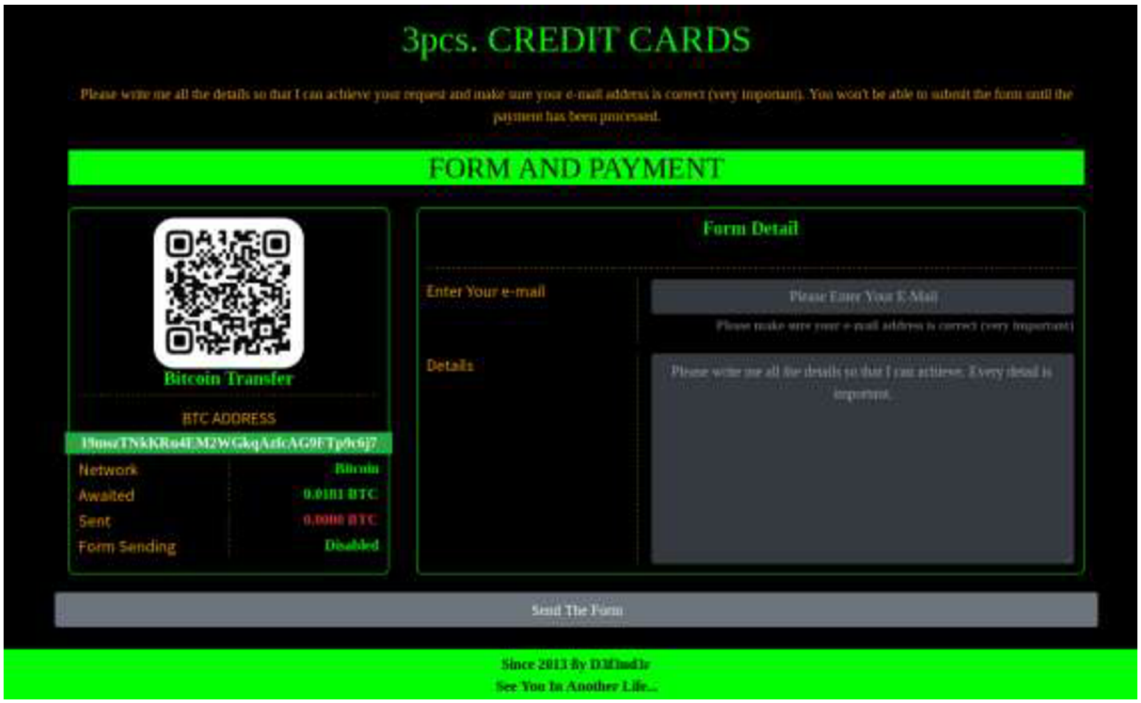


Obr. 10. Stránka výsledků vyhledávače Ahmia.
Zdroj: vlastní zpracování.

V tomto případě jsem se rozhodl vyhledat klíčové slovo „hack store“, přičemž mi stránka nabídla 997 výsledků. Vstoupil jsem tedy na první z nich.

Obr. 11. Web Hack world!.
Zdroj: vlastní zpracování.

Po kliknutí jsem se dostal na stránku nabízející hackerské služby. Na stránce se lze dočíst něco o pozadí hackera, jaké služby nabízí a za kolik.

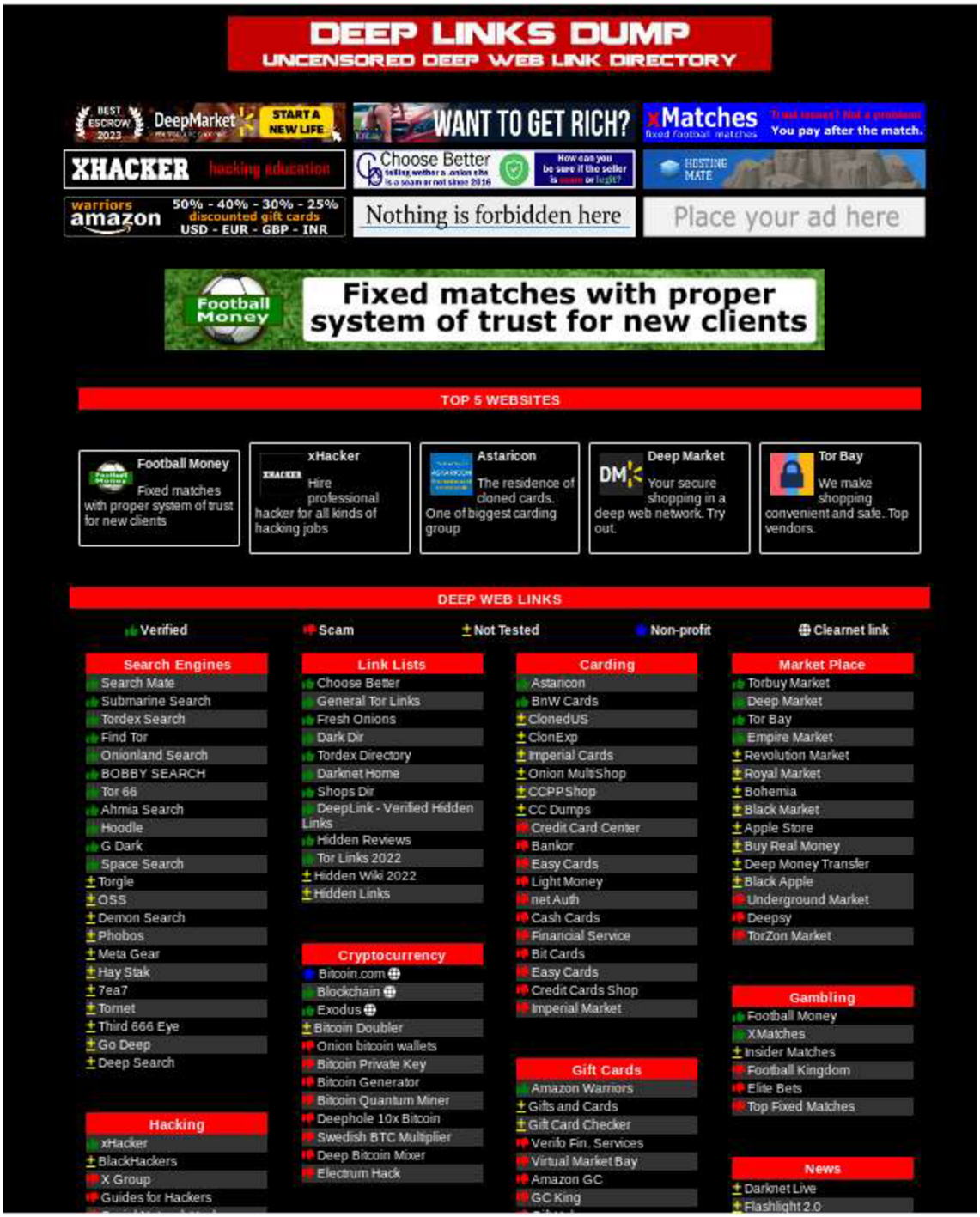


Obr. 12. Objednávka na webu Hack world!.
Zdroj: vlastní zpracování.

Po kliknutí na tlačítko „Buy“ u první služby jsem byl přesměrován na stránku vyžadující platbu za pomocí Bitcoinu a k tomu zadání emailu a detailů. Bez zaplacení předem není možné tento formulář odeslat.

Nevýhodou tohoto způsobu procházení Darknetu je, že jednak zdaleka všechny skryté služby nejsou indexovány a jednak není jasné, jak moc důvěryhodné daná skrytá služba je. Například tato stránka nabízí hackerské služby, avšak se na ní nenachází žádné recenze uživatelů a prodávající považuje okamžitou platbu předem bez využití escrow, což hodně zavání podvodem a uživatel Darknetu by nikdy neměl takto neobezřetně nakupovat.

Dalším způsobem, jak se přistoupit na různé skryté služby, je za pomocí wikiwebů. Wikiwebů je spousta, jak na Clearnetu, tak Darknetu a není tak těžké nějaký najít. Já pro demonstraci použil wikiweb Deep Links Dump.



Obr. 13. Deep Links Dump.
Zdroj: vlastní zpracování.

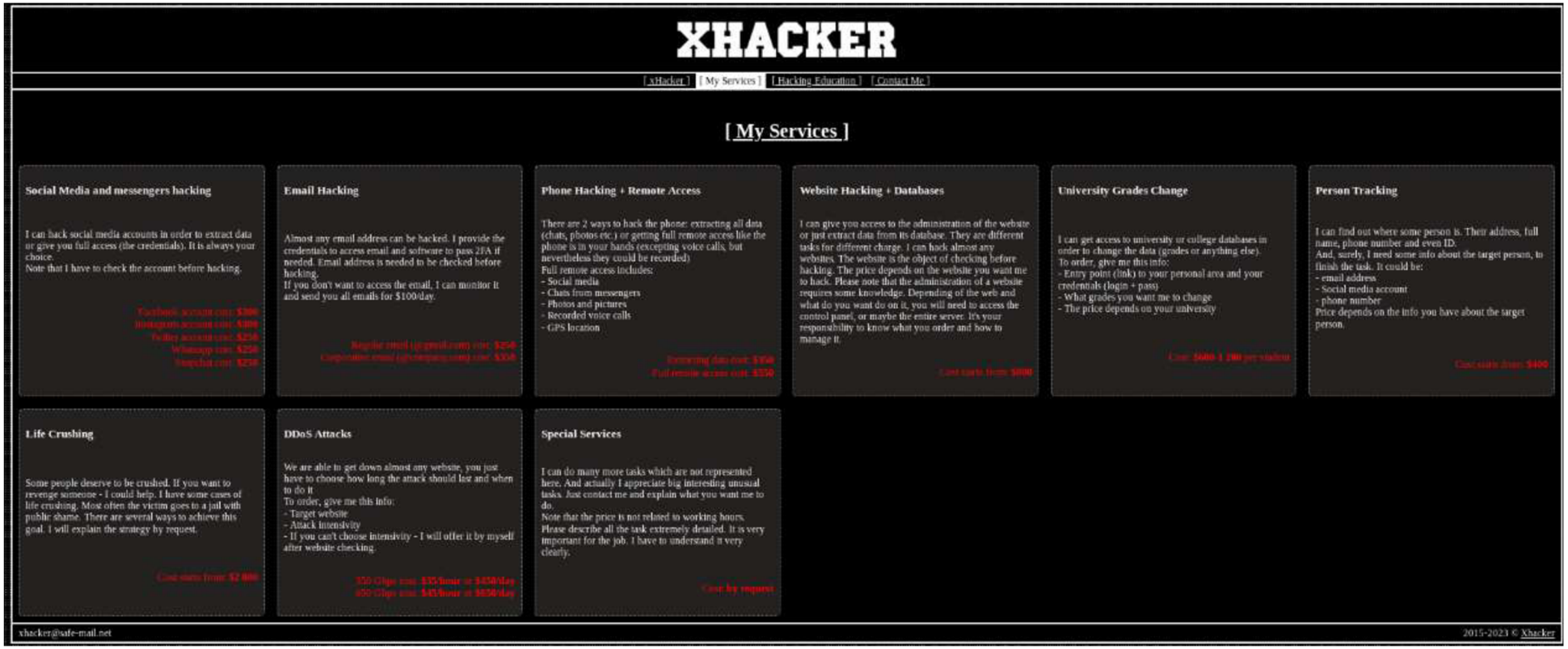
Jak je zřejmé, wikiweb obsahuje spoustu odkazů na různé skryté služby rozdělené do příslušných kategorií. V tomto případě poskytuje wikiweb i dodatečné informace k daným odkazům, především však míru ověření.

- Verified – ověřená důvěryhodná stránka.
- Scam – podvodná stránka.
- Not tested – stránka, která nebyla dostatečně ověřena.

- Non profit – nezisková organizace.
- Clearnet – odkaz vedoucí na Clearnet.

Rozhodl jsem se tedy navštívit skrytou službu „xHacker“, která je v kategorii „Hacking“ a patří mezi ověřené stránky.

Obr. 14. Úvodní stránka webu xHacker.
Zdroj: vlastní zpracování.
Na úvodní stránce prodejce popisuje své pozadí, zkušenosti, služby, ceny, způsob platby a escrow.



Obr. 15. Stránka služeb webu xHacker.
Zdroj: vlastní zpracování.
Na stránce „My Services“ lze vidět nabízené služby, jejich popis a jejich ceny.

Obr. 16. Stránka kontaktu webu xHacker.
Zdroj: vlastní zpracování.

Na stránce „Contact Me“ zveřejňuje prodejce svůj email a svůj veřejný PGP klíč, kde rovněž radí, že je pro zvýšenou úroveň anonymity lepší PGP použít.

Při porovnání webu xHacker s webem předchozím, je vidět, že xHacker dbá více na anonymitu kupujícího i na férovost obchodu s tím, že přistupuje na uzavření obchodu

pomocí escrow služby, kterou si kupující sám zvolí. Je tedy patrné, že web xHacker je mnohem důvěryhodnější než první zmíněný web. Na Darknetu si však člověk nikdy nemůže být na 100 % jistý, proto je důležité vše dělat rozvážně a na vlastní nebezpečí.

6.4 Obsah Darknetu

Sběr dat za účelem analýzy obsahu byl prováděn dvěma způsoby:

- Získávání dat z vyhledávače za pomoci klíčových slov
- Získávání dat z wikiwebů s odkazy na skryté služby

Získávání dat z vyhledávače

K této metodě získávání dat bylo použito darknetového vyhledávače Submarine (no6m4wzdexe3auiupv2zwif7rm6qwxcyhslkcnzisxgeiw6pvjsgafad.onion), do kterého bylo zadáno šest klíčových slov vázaných ke šesti kategoriím. Jako relevantní kategorie byly zvoleny Drogy, Pornografie, Hackování, Kryptoměny, Zbraně a Komunikace.

Tabulka 7. Kategorie výsledků a jejich klíčová slova.

Drogy	Pornografie	Hackování	Kryptoměny	Zbraně	Komunikace
Drugs	Porn	Hack	Bitcoin	Ammo	Discussion
Cocaine	Sex	Hacker	Bitcoin Wallet	Firearm	Forum
Heroin	Porn Video	Exploit	Crypto	Glock	Chat
Meth	Adult Video	Malware	Bitcoin Mixer	Explosives	Chat room
Lsd	Erotic	Trojan	Mining	Gun	News
Weed	Hentai	DDoS	Xmr	Guns	Media

Zdroj: vlastní zpracování.

Sběr byl vykonán za pomocí metody web scrapingu, konkrétně pomocí pavouka aplikace Scrapy, kterého bylo zapotřebí upravit pro vyhledávání v prohlížeči Tor. Za tímto účelem byl poupraven soubor settings.py přidáním níže uvedeného kódu.

```
DOWNLOADER_MIDDLEWARES = {
   'scrapy.downloadermiddlewares.httpproxy.HttpProxyMiddleware': 110,
   'scrapy.downloadermiddlewares.useragent.UserAgentMiddleware': None,
   'scrapy_fake_useragent.middleware.RandomUserAgentMiddleware': 400,
    'tor_ip_rotator.middlewares.TorProxyMiddleware': 100
}

TOR_IP_ROTATOR_ENABLED = True
TOR_IP_ROTATOR_NEW_IP_TIMEOUT = 600

TOR_PROXY_PORT = 9050
```

Kód 1. Úprava settings.py pro Tor

Na výše uvedeném kódu lze vidět, že proxy port byl nastaven na 9050, protože tomuto portu Tor ve výchozím nastavení naslouchá. Dále je vhodné zmínit Tor IP Rotator, který zajišťuje změnu IP adresy po určité době za účelem navýšení anonymity uživatele pavouka. HttpProxyMiddleware slouží k použití HTTP proxy. UserAgentMiddleware nastavuje hlavičku „User-Agent“ pro daný dotaz. Čísla u daných middlewarů[32] značí prioritu, s jakou budou spuštěny. Nižší hodnota znamená vyšší prioritu, tudíž middleware s nižší prioritou budou spuštěny první. Middlleware s prioritou None bude vždy spuštěn až nakonec.

[32] Middleware je v tomto kontextu komponenta, která stojí mezi Scrapy a pavoukem a stará se o zpracovávání dotazů a odpovědí.

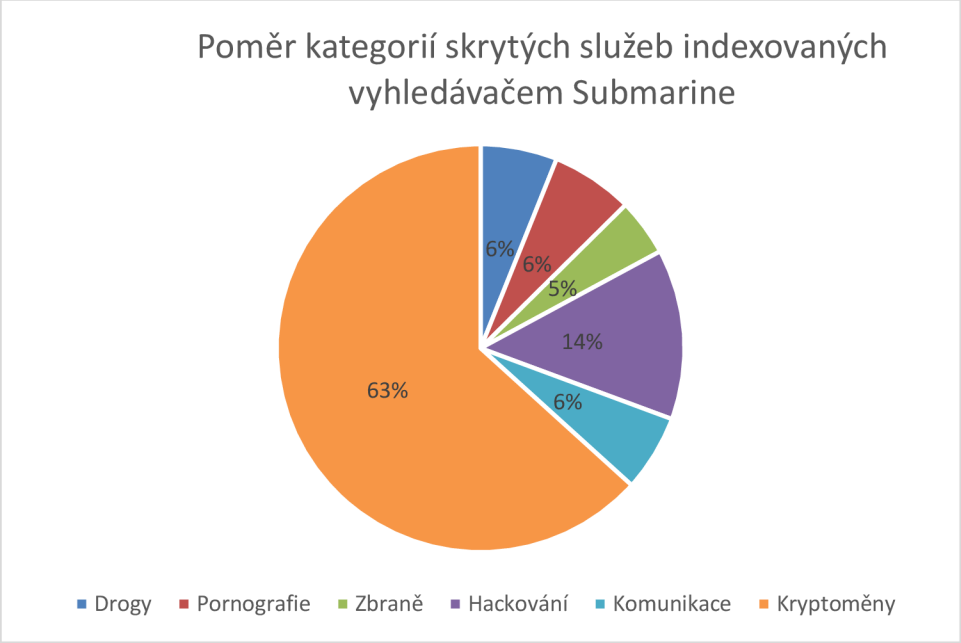
Pro samostatné sbírání dat byl pak využit následující kód napsaný v jazyce Python.

```
import scrapy


class SubmarineSpider(scrapy.Spider):
    name = "submarine-spider"
    allowed_domains =
["http://no6m4wzdexe3auiupv2zwif7rm6qwxcyhslkcnzisxgeiw6pvjsgafad.onion/"]


    def __init__(self, keyword=None, num=None, **kwargs):
        super().__init__(**kwargs)
        self.keyword = keyword
        self.num = num
        self.start_urls =
["http://no6m4wzdexe3auiupv2zwif7rm6qwxcyhslkcnzisxgeiw6pvjsgafad.onion/sear
ch.php?term={}&page={}".format(self.keyword, self.num)]


    def parse(self, response):
        for result in response.xpath('//div[@class="container"]//ul[@class="list"]/li'):
            url = result.xpath('a[@class="text-custom"]/text()').get()
            title = result.xpath('h4[@class="link-header"]/a/text()').get()
            description = result.xpath('p/text()').get()
            yield {
                'url': url,
                'title': title,
                'description': description,
            }
```

Kód 2. Scrapy pavouk

Tento kód byl zpočátku vygenerován za pomocí umělé inteligence ChatGPT a pak řádně ručně poupraven do funkční podoby. Při spuštění je zapotřebí zadat klíčové slovo (keyword), které má být prohlížečem vyhledáváno a číslo stránky výsledků (num), která má být procházena. Pavouk pak projde tuto stránku a z výsledků posbírá volně dostupná data, jako jsou odkazy (url), názvy skrytých služeb (title) či jejich popisy (description) a tyto data pak následně uloží do souboru. Pro účely této práce byly výsledky ukládány do souboru CSV.

Celkem bylo z těchto klíčových slov nasbíráno 2 777 odkazů, z nichž 1612 (58 %) bylo unikátních v jednotlivých kategoriích. Jednotlivé kategorie byly poměrově zastoupeny následovně:



Graf 1. Poměr kategorií skrytých služeb indexovaných vyhledávačem Submarine. Zdroj: vlastní zpracování.

Z grafu je zřejmé, že majoritní zastoupení zde mají skryté služby, které byly indexovány pod kategorií Kryptoměny. S výrazným rozdílem následují stránky týkající se hackování a zbylé kategorie jsou rozloženy téměř rovnoměrně. Důležité je však myslet na to, že toto rozdělení neukazuje míru obsahu na celém Darknetu, ale pouze míru obsahu v daných kategoriích, ke kterým se může uživatel dostat za použití vyhledávače Submarine. Jiné vyhledávače mohou indexovat jiné stránky jinými způsoby a tím pádem může dojít k naprosto odlišnému poměru kategorií. Dále je důležité upozornit, že dané výsledky ukazují opravdu jen skryté služby, které byly nějakým způsobem naindexovány a je velice pravděpodobné, že se na Darknetu nachází více stránek, které nejsou indexovány žádným způsobem a lze se k nim dostat pouze prostřednictvím odkazu. Rovněž je důležité zmínit, že veškeré stránky v této analýze jsou onion stránky, tudíž dostupné přes Tor. Nejsou zde uvedeny další darknetové služby jako eepsites nebo freesites. Dalším omezením této analýzy je jazyk. Byť je obsah na Darknetu tvořen z většiny angličtinou, existují však i skryté služby v jiných jazycích jako ruština, francouzština či čínština. K analýze této strany Darknetu by bylo vhodné použít klíčová slova v daných jazycích.

Získávání dat z wikiwebů

K získání dat z wikiwebů bylo použito sedm skrytých služeb fungujících jako internetové katalogy. Na těchto katalozích byly spočítány odkazy rozdělené do kategorií a pro přehlednost ještě roztříděny do šestnácti nadkategorií následovně:

Tabulka 8. Kategorie, do který byly rozděleny kategorie z wikiwebů.

Odkazy	Peníze	Kryptoměny	Obchody	Komunikace
Search engines	Carding	Crypto	Marketplace	Email
Link lists	Gift Cards	Bitcoin	Markets	Blogs
Catalogs	PayPal			Forums
Wikis	Transfers			Communication
	Escrow			Social
	Money			
	Financial services			

Zdroj: vlastní zpracování.

Tabulka 9. Kategorie, do který byly rozděleny kategorie z wikiwebů.

Elektronika	Hazard	Hackování	Hosting	Dokumenty
Electronics	Gambling	Hacking	Hosting	Documents
				Counterfeits

Zdroj: vlastní zpracování.

Tabulka 10. Kategorie, do který byly rozděleny kategorie z wikiwebů.

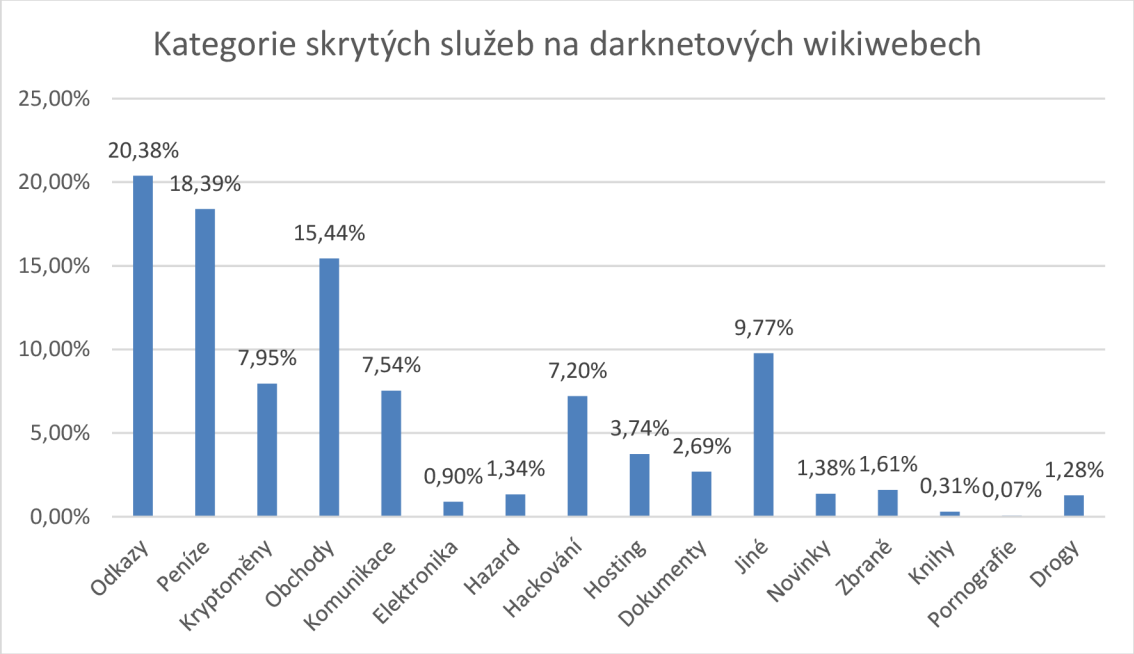
Drogy	Pornografie	Novinky	Zbraně	Knihy	Jiné
Drugs	Porn	News	Weapons	E-books	Other

Zdroj: vlastní zpracování.

Data byla sbírána z následujících wikiwebů:

- Fresh Onions
- Darknet Home
- Tor Links
- DeepLink Onion Directory
- TOR LINKS
- Deep Links Dump
- Tasty Onions

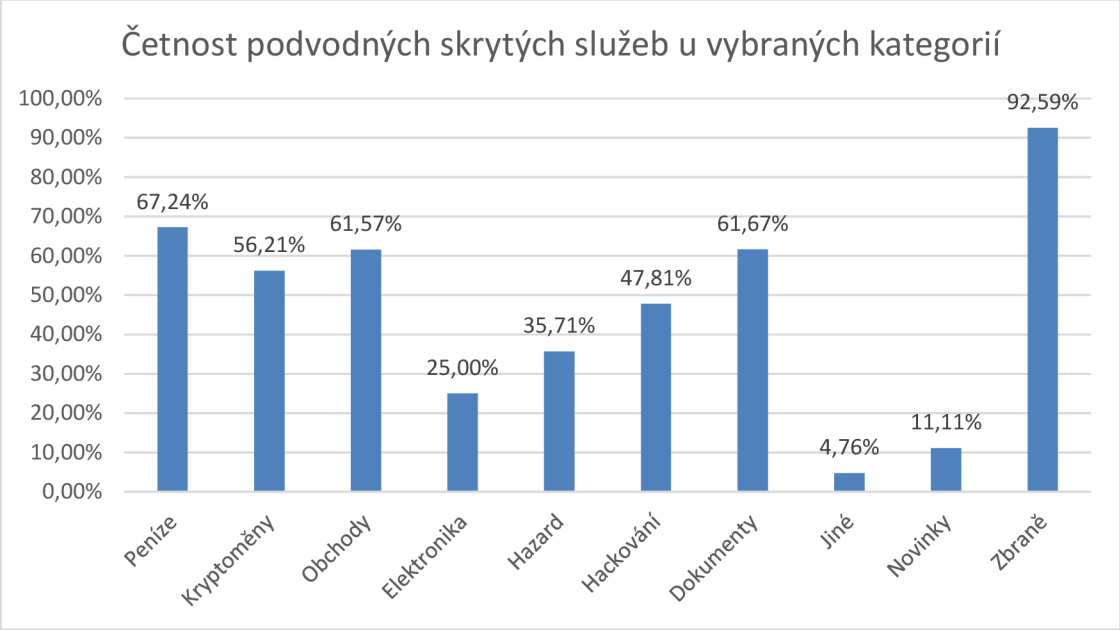
Z těchto sedmi wikiwebů bylo celkem posbíráno 3 259 odkazů, které byly kategorizovány do šestnácti výše uvedených kategorií. Celkový poměr kategorií na všech sedmi wikiwebech vypadá následovně:



Graf 2. Kategorie skrytých služeb na darknetových wikiwebech.
Zdroj: vlastní zpracování.

Z grafu je zřejmé, že největší zastoupení na wikiwebech mají skryté služby týkající se odkazů na jiné skryté služby, peněz či obchodování, dále také komunikace a největší vyloženě ilegální kategorií je hackování, zatímco další ilegální kategorie, jako drogy či zbraně, tvoří jen velice malou část celku.

Tři ze sedmi výše zmíněných wikiwebů rovněž nabízely k poskytovaným odkazům také ověření, zdali je daná stránka podvod. Četnost podvodnosti daných kategorií, na základě těchto tří stránek, vypadá takto:



Graf 3. Četnost podvodných skrytých služeb u vybraných kategorií.
Zdroj: vlastní zpracování.

Jak je patrné, téměř veškeré skryté služby zaměřené na zbraně byly podvodné. U poloviny všech kategorií byla podvodnost větší, než 50 %. Z toho vyplývá, že u procházení Darknetu je velice důležité dbát na důvěryhodnost a úroveň ověření skrytých služeb. Na těchto třech wikwebech bylo v průměru 41,78 % odkazů odkazujících na podvodné skryté služby.

Závěr

Při porovnání výsledků z wikiwebů a vyhledávače si lze všimnout, že největší zastoupení mají skryté služby týkající se peněz. Z ilegálních kategorií v obou případech vládne hackování, zatímco zbraně a drogy spadají do nejnižších příček. Největší výjimku tvoří především pornografie, která je na wikiwebech téměř nedohledatelná, avšak pomocí vyhledávače se lze k nějakým výraznějším výsledkům dopracovat.

7 Závěry a doporučení

Co se týká technologií, tato práce dokazuje, že existuje několik způsobů, jak navštívit Darknet a jak navýšit svou anonymitu, především za pomocí nástrojů, jako jsou OS, prohlížeče či kryptoměny. Každá tato technologie a každý tento nástroj má své výhody a nevýhody a záleží čistě na uživateli, co je pro něj nejvýhodnější použít. Přemýšlet by měl člověk především o tom, proč chce vlastně Darknet navštívit, jak moc potřebuje po sobě zakrýt stopy a také jestli má k tomu dostatečně výkonný stroj. Jak bylo zmíněno v kapitole 5.5.10., Qubes OS lze možno zkombinovat s Whonixem, ale vezmeme-li fakt, že Qubes OS poběží na virtuálním stroji a Whonix poběží na virtuálním stroji v Qubes OS, dochází již ke dvojité virtualizaci, což kdejaký slabší počítač nemusí vydržet. Co se týká VPN, rozebíraných v kapitole 5.5.3., nejsou zdaleka tak anonymizující, jak se může podle reklam na internetu zdát. Ve skutečnosti může posloužit VPN jako extra vrstva proti případným útočníkům a jako skrytí aktivit před poskytovatelem internetu. Avšak, stále to znamená poskytnout svou IP adresu třetí straně, která ve výsledku vidí váš provoz. Uvedenou výjimku zde tvoří Mullvad VPN, který dbá na anonymitu svých uživatelů a pokud je tato VPN služba zakoupena skrze Tor, dozví se poskytovatel služby pouze adresu daného koncového uzlu, nikoliv reálnou adresu uživatele, což je podle mě nejlepší způsob, jakým používat VPN společně s Torem. Nevýhodou použití VPN na Darknetu však může být pomalejší připojení, když už samotné připojení v síti Darknet není tak rychlé, jako připojení na Clearnetu. Extra vrstva ochrany se navíc dá získat i když uživatel použije Tor most. Pro komunikaci pomocí emailu by měl člověk ideálně vždy používat nástroj PGP. Důležité je opět zmínit, že i když všechny tyto nástroje jsou velice užitečné, vždycky je velice důležité to, jak se člověk chová, protože to dokáže vždy jakoukoliv úroveň anonymity naprosto zničit.

Co se obsahové části týče, je důležité, aby si člověk dával pozor, kam chodí a ověřoval si skryté služby, ať už za pomocí recenzí, či tím, jak daný web přistupuje k férovosti a soukromí klienta, v případě obchodů či služeb například použitím escrow. Bylo dokázáno, že narazit na podvodnou skrytou službu není těžká věc – přece jen dává smysl, že v prostoru, kde je člověk alespoň zdánlivě nedostižitelný, se bude vyskytovat spousta lidí, co budou chtít této nedostižitelnosti využít pro svůj prospěch na úkor jiných.

Na závěr bych ještě rád zmínil, že veškeré informace v této práci mají pouze analyzační a vědecký účel a nemají žádným způsobem napomáhat a vybízet lidi k dělaní ilegálních

aktivit, nikoho takového neobhajuji a veškeré takovéto jednání odsuzuji. Tato práce slouží pouze k zvýšení povědomí o anonymitě a soukromí uživatelů na internetu a o tom, jak se může člověk bránit.

8 Seznam použité literatury

Seznam použité literatury

[1] SULTANA, J., JILANI, Abdulkhadar. Exploring and Analysing Surface, Deep, Dark Web and Attacks. International Journal of Scientific & Technology Research 10, no. 4., 2021 [cit. 2022-12-04]. ISBN: 978-3-030-69173-8.

[2] Web Browsers Introduction. [cit. 2022-12-04] Dostupné z: https://web.archive.org/web/20211206205907/https://webbrowsersintroduction.com/.

[3] BERGMAN, Michael K. The Deep Web: Surfacing Hidden Value. White paper. BrightPlanet LLC, 2021. [cit. 2022-12-05].

[4] Spiceworks IT Security Hub. Dark Web vs. Deep Web. [cit. 2022-12-05]. Dostupné z: https://www.spiceworks.com/it-security/security-general/articles/dark-web-vs-deep-web/amp/.

[5] PFITZMANN, Andreas, MARIT Hansen. Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology. 2006. [cit. 2022-12-04].

[6] ANDERSSON, Christer, PANCHENKO Andriy. Practical Anonymous Communication on the Mobile Internet Using Tor. Ve sborníku z 28 výroční konference o aplikacích počítačové bezpečnosti, upraveno H. Federrathem a D. Gollmannem, 331-340. IEEE, 2013. [cit. 2022-12-04] ISBN: 978-1-4244-0974-7

[7] HENDERSON, Lance. The Darknet Super Pack: How to Be Anonymous Online with Tor, Bitcoin, Tails & Freedom. CreateSpace Independent Publishing Platform, 2017. ISBN: 1976483220.

[8] OWEN Gareth, SAVAGE Nick. „The Tor Dark Net“. 2015.

[9] "Edward Snowden." Encyclopædia Britannica. [cit. 2023-02-10]. Dostupné z: https://www.britannica.com/biography/Edward-Snowden.

[10] ‚Tor stinks‘ NSA presentation - full document revealed. The Guardian, 2013. [cit. 2023-02-10]. Dostupné z: https://www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document.

[11] Hacking cases: Body of evidence. The Age, 2012. [cit. 2023-02-10]. Dostupné z: https://www.theage.com.au/technology/hacking-cases-body-of-evidence-20120411-1wsbh.html.

[12] NORTE, Carlos J. Advanced Tor Browser Fingerprinting. Jose Carlos Norte Personal Blog, 2016. [cit. 2023-02-11] Dostupné z: http://jcarlosnorte.com/security/2016/03/06/advanced-tor-browser-fingerprinting.html.

[13] DRBOLA, Vojtěch. Hnutí Šifropunk: problematika kryptoměn a anonymity v kyberprostoru [online]. Brno, 2019. Dostupné z: https://theses.cz/id/cras7s/.

Diplomová práce. Masarykova univerzita, Filozofická fakulta. Vedoucí práce PhDr. Martin Flašar, Ph.D.

[14] What is WikiLeaks? WikiLeaks. [2023-02-12] Dostupné z: https://wikileaks.org/What-is-WikiLeaks.html.

[15] BARTLETT, Jamie. The Dark Net: Inside the Digital Underworld. New York: Melville House Publishing, 2015. ISBN: 978-1-61219-490-5

[16] Nejlepší VPN v České republice – Recenze top 9 poskytovatelů pro rok 2023. Business 2 Community. [cit. 2023-02-13] Dostupné z: https://www.business2community.com/cz/vpn/nejlepsi-vpn.

[17] Unabomber. FBI. [cit. 2023-02-16]. Dostupné z: https://www.fbi.gov/history/famous-cases/unabomber.

[18] Proxy. [cit. 2023-02-14]. Dostupné z: https://proxy.org/.

[19] GULA, Ján. Sběr metadat uživatelů a zařízení z Darkwebu [online]. Brno, 2019. Dostupné z: https://theses.cz/id/dam68o/. Bakalářská práce. Vysoké učení technické v Brně.

[20] The NSA spying scandal: a cheat sheet. The Verge, 2013. [cit. 2023-02-16]. Dostupné z: https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet.

[21] About I2P. I2P. [cit. 2023-02-14]. Dostupné z: https://geti2p.net/en/about/intro.

[22] About Freenet. Freenet Project. [cit. 2023-02-15]. Dostupné z: https://freenetproject.org/pages/about.html.

[23] SCHRŮTA, Jakub. Analýza vybraných specifik práce stránek Darkweb v síti Darknet [online]. Praha, 2022. Dostupné z: https://theses.cz/id/96ra5x/. Diplomová práce. Vysoká škola finanční a správní, a.s. Vedoucí práce Mgr. Ing. Dominik Stroukal, Ph.D.

[24] History of Tor. The Tor Project. [cit. 2023-02-15]. Dostupné z: https://www.torproject.org/about/history/.

[25] Tor Stats – 2023. TrueList, 2023. [cit. 2023-02-15]. Dostupné z: https://truelist.co/blog/tor-stats/ .

[26] VOLEJNÍK, Robert. Darknet – fikce či realita anonymity skrytých služeb Tor a systému bitcoin [online]. Brno, 2016. Dostupné z: https://theses.cz/id/6uz1xn/. Bakalářská práce. Masarykova univerzita, Filozofická fakulta. Vedoucí práce Mgr. Viktor Pantůček, Ph.D.

[27] Austrian police raid privacy network over child porn. BBC News, 2012. [cit. 2023-02-15]. Dostupné z: https://www.bbc.com/news/technology-20554788.

[28] GILMOUR, Dave. Which websites and online services are banned in China? TechRadar, 2021. [cit. 2023-02-10]. Dostupné z:

https://www.techradar.com/vpn/which-websites-and-online-services-are-banned-in-china.

[29] Tails. Tails. [cit. 2023-02-27]. Dostupné z: https://tails.boum.org/index.en.html.

[30] "ntroduction | Qubes OS. Qubes OS Project. [cit. 2023-02-28]. Dostupné z: https://www.qubes-os.org/intro.

[31] About - Whonix. Whonix. [cit. 2023-02-29]. Dostupné z: https://www.whonix.org/wiki/About.

[32] BENNETT, Paul. Anonymity-focused Linux distributions. Comparitech, 2021. [cit. 2023-02-29]. Dostupné z: https://www.comparitech.com/blog/vpn-privacy/anonymity-focused-linux-distributions/.

[33] KRAMER, Shoshanna. Were There Cryptocurrencies Before Bitcoin? Investopedia, 2021. [cit. 2023-03-02]. Dostupné z: https://www.investopedia.com/tech/were-there-cryptocurrencies-bitcoin/.

[34] Bitcoin - Bitcoin Wiki. Bitcoin Wiki. [cit. 2023-03-02]. Dostupné z: https://en.bitcoin.it/wiki/Bitcoin.

[35] LEE, Timothy. What Happens to Bitcoin After All 21 Million Are Mined? Investopedia, 2021. [cit. 2023-03-02]. Dostupné z: https://www.investopedia.com/tech/what-happens-bitcoin-after-21-million-mined/.

[36] About Monero - Monero. Monero Project. [cit. 2023-03-03]. Dostupné z: https://web.getmonero.org/resources/about/.

[37] CHEN, James. What Is Dash Cryptocurrency? Investopedia, 2021. [cit. 2023-03-03]. Dostupné z: https://www.investopedia.com/tech/what-dash-cryptocurrency/.

[38] Masternodes - Dash. Dash. [cit. 2023-03-03]. Dostupné z: https://www.dash.org/masternodes/.

[39] HOD, David. Edward Snowden's Big Problem: Bitcoin Privacy, Not Scalability. Finance Magnates, 2019. [cit. 2023-03-03]. Dostupné z: https://www.financemagnates.com/cryptocurrency/news/edward-snowdens-big-problem-bitcoin-privacy-not-scalability/.

[40] The Basics - Zcash. Electric Coin Company. [cit. 2023-03-04]. Dostupné z: https://z.cash/the-basics/.

[41] Privacy: Dash vs Monero. Edge, 2018. [cit. 2023-03-04]. Dostupné z: https://edge.app/blog/tips-and-tutorials/privacy-dash-vs-monero/.

[42] Zk-SNARKs - Zcash. Electric Coin Company. [cit. 2023-03-04]. Dostupné z: https://z.cash/technology/zksnarks/.

[43] Technical Explainer: Halo on Zcash. Electric Coin Company, 2020. [cit. 2023-03-05]. Dostupné z: https://electriccoin.co/blog/technical-explainer-halo-on-zcash/.

[44] The Pasta Curves for Halo 2 and Beyond. Electric Coin Company, 2021. [cit. 2023-03-05]. Dostupné z: https://electriccoin.co/blog/the-pasta-curves-for-halo-2-and-beyond/.

[45] Dark Wallet. Investopedia. [cit. 2023-03-06]. Dostupné z: https://www.investopedia.com/terms/d/dark-wallet.asp.

[46] Expert Explanation: History of the Dark Web. FraudWatch International, 2019. [cit. 2023-03-16]. Dostupné z: https://fraudwatch.com/expert-explanation-history-of-the-dark-web/.

[47] Dark web. Encyclopedia Britannica, 2021. [cit. 2023-03-16]. Dostupné z: https://www.britannica.com/topic/dark-web.

[48] VELÍSEK, Jiří. Historie darknet marketů a principy jejich fungování [online]. Brno, 2017. Dostupné z: https://theses.cz/id/gst7bl/. Bakalářská práce. Masarykova univerzita, Filozofická fakulta. Vedoucí práce Mgr. Marek Timko, Ph.D.

[49] What is Escrow? Escrow.com. [cit. 2023-03-17]. Dostupné z: https://www.escrow.com/what-is-escrow.

[50] BURGESS, Jonas. Malware and Exploits on the Dark Web. Belfast. Queen's University Belfast, 2017. [cit. 2023-03-22]. Dostupné z: https://pureadmin.qub.ac.uk/ws/portalfiles/portal/199051581/Malware_and_Exploits_on_the_Dark_Web.pdf.

[51] Usage statistics of JavaScript as client-side programming language on websites. W3Techs. [cit. 2023-02-10]. Dostupné z: https://w3techs.com/technologies/details/cp-javascript.

[52] Facebook onion service, Wikipedia. [cit. 2023-02-15]. Dostupné z: https://en.wikipedia.org/wiki/Facebook_onion_service.

[53] Kurzy kryptoměn. Kriptomat. [cit. 2023-03-01]. Dostupné z: https://kriptomat.io/cs/kurzy-kryptomen/.

[54] Monero (XMR). [cit. 2023-03-01]. CoinMarketCap. Dostupné z: https://coinmarketcap.com/cs/currencies/monero/.

[55] Dash (DASH). [cit. 2023-03-01]. CoinMarketCap. Dostupné z: https://coinmarketcap.com/currencies/dash.

[56] Zcash (ZEC). [cit. 2023-03-01]. CoinMarketCap. Dostupné z: https://coinmarketcap.com/currencies/zcash.

[57] Dogecoin (DOGE). [cit. 2023-03-01]. CoinMarketCap. Dostupné z: https://coinmarketcap.com/currencies/dogecoin/.

[58] PutinCoin (PUT). [cit. 2023-03-01]. CoinMarketCap. Dostupné z: https://coinmarketcap.com/currencies/putincoin/.

[59] Cryptosteel. [cit. 2023-03-06]. Dostupné z: https://cryptosteel.com/.

[60] What Is a Paper Wallet? Gemini Cryptopedia. Gemini. 2022. [cit. 2023-03-06]. Dostupné z: https://www.gemini.com/cryptopedia/paper-wallet-crypto-cold-storage.

[61] Downloads. Getmonero. [cit. 2023-03-06]. Dostupné z: https://www.getmonero.org/downloads/.

[62] Wallets. Zcash. [cit. 2023-03-06]. Dostupné z: https://z.cash/wallets/.

[63] NordVPN. [cit. 2023-02-13]. Dostupné z: https://nordvpn.com/.

[64] UltraVPN. [cit. 2023-02-13]. Dostupné z: https://ultravpn.com/.

[65] Cyber Ghost VPN. [cit. 2023-02-13]. Dostupné z: https://www.cyberghostvpn.com/.

[66] Mullvad VPN. [cit. 2023-02-13]. Dostupné z: https://mullvad.net/en/.

UNIVERZITA HRADEC KRÁLOVÉ
Fakulta informatiky a managementu
Akademický rok: 2021/2022

Studijní program: Aplikovaná informatika
Forma studia: Prezenční
Obor/kombinace: Aplikovaná informatika (ai3-p)

Podklad pro zadání BAKALÁŘSKÉ práce studenta

Jméno a příjmení:	**Daniel Kučera**
Osobní číslo:	**I2000380**
Adresa:	Budovatelská 810, Studénka – Butovice, 74213 Studénka 3, Česká republika
Téma práce:	Anonymita na Darkwebu
Téma práce anglicky:	Darkweb anonymity
Jazyk práce:	Čeština
Vedoucí práce:	doc. Ing. Vladimír Soběslav, Ph.D. Katedra informačních technologií

Zásady pro vypracování:

Anotace: Cílem této bakalářské práce je analyzovat problematiku anonymity na internetu, především v síti Darknet, s důrazem na nalezení způsobů, jak do dané sítě přistupovat. Bakalářské práce dále vymezuje pojmy, jako je anonymita nebo soukromí a definuje rozdíly mezi Deep webem a Dark webem. Tato práce je zaměřena především na Dark web, dále pak na to, jak se v něm pohybovat, na technologie, které lze použít a porovnávání jich či jejich kombinování, stejně tak jako na definici technologií, které naopak slouží ke sbírání dat uživatelů a jejich identifikaci. Rovněž tato práce pojednává o věcech, které lze v síti Darknet najít či jak je získat, o jeho účelu a historii. Výsledek této práce by měl čtenáři přinést důkladné znalosti o tom, jaké prostředky a postupy použít k tomu, aby mohl uživatel Darknet navštívit a jak se na něm pohybovat.

Obsah:

1. Úvod
2. Cíl práce
3. Metodika zpracování
4. Rozdělení internetu
5. Anonymita na internetu
6. Analýza Darknetu
7. Závěr

Seznam doporučené literatury:

1. Bartlett, J. The Dark Net: Inside the Digital Underworld, 2016. ISBN 9781612195216.
2. Henderson, L. The Darknet Super-pack: How to Be Anonymous Online With Tor, Bitcoin, Tails & More. 2017. ISBN 1976483220.
3. DĚDEK, Jindřich. Analýza P2P sítě Darknet se zaměřením na Darkweb. Hradec Králové, 2019. Diplomová práce. Univerzita Hradec Králové, Fakulta informatiky a managementu.
4. GULA, Ján. Sběr metadat uživatelů a zařízení z Darkwebu. Brno, 2019. Bakalářská práce. Vysoké učení technické v Brně.
5. VOLEJNÍK, Robert. Darknet – fikce či realita anonymity skrytých služeb Tor a systému bitcoin. Brno, 2016. Bakalářská práce. Masarykova univerzita, Filozofická fakulta.
6. SCHRŮTA, Jakub. Analýza vybraných specifik práce stránek Darkweb v síti Darknet. Praha, 2022. Diplomová práce. Vysoká škola finanční a správní, a.s.
7. DRBOLA, Vojtěch. Hnutí Šifropunk: problematika kryptoměn a anonymity v kyberprostoru. Brno, 2019. Masarykova univerzita, Filozofická fakulta.

Podpis studenta: Datum:

Podpis vedoucího práce: Datum: