Etická analýza temného webu

Lukáš Rzavský

Bakalářská práce
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2018/2019

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Lukáš Rzavský**
Osobní číslo:	**A16085**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Softwarové inženýrství**
Forma studia:	**prezenční**
Téma práce:	**Etická analýza temného webu**
Téma anglicky:	**An Ethical Analysis of the Dark Web**

Zásady pro vypracování:

1. **Seznamte se s terminologií a historií vzniku temného webu.**
2. **Analyzujte a porovnejte možnosti připojení do temného webu.**
3. **Proveďte průzkum dostupných statistických informací do současnosti.**
4. **Připojte se a proveďte samotný etický průzkum temného webu.**
5. **Vhodně reprezentujte a vyhodnoťte sesbíraná data.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **NORRY, Andrew. The History of Silk Road: A Tale of Drugs, Extortion & Bitcoin [online]. November 20, 2018 [cit. 2018-11-23]. Dostupné z: https://blockonomi.com/history-of-silk-road/**
2. **GREENBERG, Andy. HACKER LEXICON: WHAT IS THE DARK WEB? [online]. 11.19.14 [cit. 2018-11-23]. Dostupné z: https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/**
3. **EGAN, Matt. What is the Dark Web & How to Access it [online]. 06 Apr 2018 [cit. 2018-11-23]. Dostupné z: https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/**
4. **FINKLEA, Kristin. Dark Web [online]. March 10, 2017 [cit. 2018-11-23]. Dostupné z: https://fas.org/sgp/crs/misc/R44101.pdf**
5. **Tor: Overview [online]. [cit. 2018-11-23]. Dostupné z: https://www.torproject.org/about/overview.html.en**

Vedoucí bakalářské práce: **Ing. Petr Žáček**
Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce: **3. prosince 2018**

Termín odevzdání bakalářské práce: **15. května 2019**

Ve Zlíně dne 7. prosince 2018

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

doc. Mgr. Milan Adámek, Ph.D.
děkan

prof. Mgr. Roman Jašek, Ph.D.
garant oboru

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně, dne: 13.05.2019

Lukáš Rzavský, v. r.
podpis diplomanta

ABSTRAKT

Bakalárska práca sa zaoberá problematikou nazývanou temný web, ktorá predstavuje jednu z častí Internetu. Táto časť prevažne zahŕňa nelegálne služby a produkty. Práca je založená na etickom prieskume temného webu a vychádza z pozorovania a pripojenia na temný web s cieľom zistenia aktuálneho stavu a porovnania s dostupnými štatistikami.

Klíčová slova: Internet, dark web, deep web, tor, etický prieskum, štatistiky temného webu

ABSTRACT

This thesis deals with the problematics of „Dark Web“, which is one of the parts of the known Internet. This part of the Internet contains mostly illegal services and products. This thesis is based on its ethical exploration and its basis comes from its observation and connection to it, in order to explore the current state and to compare it to existing statistics.

Keywords: Internet, dark web, deep web, ethical analysis, dark web statistics

Moje poďakovanie patrí vedúcemu bakalárskej práce Ing. Petrovi Žáčkovi za čas, ktorý mi venoval pri riešení otázok týkajúcich sa tejto bakalárskej práce, za cenné rady a pripomienky.

Prehlasujem, že odovzdaná verzia bakalárskej práce a verzia elektronická nahraná do IS/STAG sú totožné.

OBSAH

ÚVOD

Mnoho ľudí si neuvedomuje, že sieť, ktorú denne používajú na získavanie informácií alebo prehliadanie stránok nie je celý Internet, ktorý môžu prehliadať, ale zahŕňa len veľmi malú časť celého Internetu. Táto časť má názov Surface web. Nachádzajú sa tu aj ďalšie časti ako Deep web a Dark web (Temný web). Tieto časti nie sú prístupné pomocou bežných prehliadačov a užívateľ je nútený použiť špecializovaný softvér pre prístup k nim. Zatiaľ čo Deep web obsahuje databázy a služby, ktoré si vyžadujú autentifikáciu alebo rôzne iné platformy, Dark web je spájaný s nelegálnejšou činnosťou a kriminalitou.

Pojem temný web bol pre mňa veľkou neznámou. Vzhľadom na to, že na Internete sa nenachádza veľa článkov týkajúcich sa tejto problematiky, začal som podrobnejšie skúmať a sledovať, aké sú dostupné služby a akým spôsobom je možné získať o nich viac informácií. Cieľom tejto bakalárskej práce teda je priniesť ucelený pohľad do problematiky ako takej, od histórie vzniku temného webu, popis jednotlivých vrstiev Internetu a softvérov umožňujúcich prístup k temnému webu, doposiaľ dostupným štatistickým informáciám, až po samotný etický prieskum tejto časti Internetu.

Moja bakalárska práca sa skladá z dvoch častí. Teoretická časť je zložená z dvoch kapitol. V prvej kapitole som sa zameral na popis vrstiev Internetu, podrobnejší popis temného webu a históriu vzniku tohto webu. V druhej kapitole mojej bakalárskej práce som sa zameral na možnosti prístupu k temnému webu a ich porovnanie. Druhá časť je praktická a poukazuje na štatistiky dostupné do súčasnosti, ktoré som graficky a percentuálne spracoval v treťom bode bakalárskej práce. V ďalšom bode popisujem etický prieskum temného webu a poukazujem na nelegálne činnosti nachádzajúce sa v tejto časti webu. Rád by som však podotkol, že práca je zameraná len na prieskum a v žiadnom prípade nie na navádzanie k využívaniu webu na nelegálnu činnosť. V poslednom bode bakalárskej práce sa nachádza súhrn zistených informácií, od hrozieb až po obsah, ktorý je možné na temnom webe nájsť.

I. TEORETICKÁ ČASŤ

1 TERMINOLÓGIA A HISTÓRIA VZNIKU TEMNÉHO WEBU

Internet je plný informácií a každý z nás si môže vyhľadať a získať informácie podľa vlastného záujmu. Je zostavený z miliárd zariadení, ktoré sú navzájom prepojené a zdieľajú informácie po celom svete. [1] V súčasnosti je väčšina ľudí zvyknutá na Surface web, ktorý používajú takmer každý deň na získanie informácii alebo iné online služby a považujú ho spolu s Internetom za synonymá. No Internet je omnoho väčší, ako si mnoho ľudí predstavuje. [2] Surface web je len jednou z častí Internetu a predstavuje len 4% z celkového webu. Zvyšnú časť webu zahŕňa Deep web. Deep web obsahuje stránky, ktoré nie sú indexované vyhľadávačmi. To znamená, že nie sú dostupné pomocou tradičných vyhľadávačov. Ďalšou známou časťou webu je Dark web (Temný web), ktorý je súčasťou Deep webu. Dark web obsahuje skryté stránky, ktoré sú dostupné len pomocou špeciálnych softvérov. Kým obsah týchto stránok je dostupný, ich autori sú utajení. [3]

1.1 Vrstvy Internetu

Internet sa rozdeľuje na tri hlavné časti, ktorými sú Surface web, Deep web a Dark web. Každá z týchto troch častí predstavuje odlišný typ obsahu. [3]

1.1.1 Surface web

Surface web je časť Internetu, ktorá je viditeľná pre všetkých používateľov. Je tvorená statickými a pevnými stránkami. Tieto webstránky sú indexované vyhľadávacími nástrojmi ako je napríklad Google, Yahoo alebo Bing. [1] Akýkoľvek odkaz na Surface web bude odkazovať na bežné webové stránky, ktorých domény končia .com, .org, .net alebo s podobnými variantami a ktorých obsah nevyžaduje žiadnu špeciálnu konfiguráciu na prístup. [4] Užívateľ si môže jednoducho otvoriť webstránky a získavať informácie. Avšak zaujímavou informáciou je, že Surface web je minoritnou časťou z celkového Internetu, ktorý môžu užívatelia využiť. [1] Je taktiež domovom pre niektoré stránky Deep webu. Každá stránka, ktorá vyžaduje údaje k prístupu, je technicky súčasťou Deep webu, pretože vyhľadávač nemôže získať prístup k tomuto obsahu. Surface web je taktiež známy pod pojmami „Visible web, Indexed web alebo Clearnet“. [5]

1.1.2 Deep web

Deep web je často považovaný za synonymum s Dark webom, ale v skutočnosti sú to dva odlišné pojmy. Deep web je skrytý web, ktorý nie je viditeľný pre normálneho užívateľa. Pozostáva z webstránok, ktoré nie sú indexované tradičnými vyhľadávačmi ako Google, a preto nie sú dostupné pre tieto vyhľadávače. [1] Deep Web odkazuje na obsah skrytý za HTML formulármi. Aby sa užívateľ k takému obsahu dostal, musí mať špecializovaný prístup a vedieť o jeho existencii. Názov Deep Web vychádza zo skutočnosti, že takýto obsah bol vo vyhľadávačoch považovaný za nedosiahnuteľný. Deep Web je tiež považovaný za najväčší zdroj štruktúrovaných dát na webe. [6] Tento web zahŕňa okolo 96% celkového Internetu a zahŕňa dokonca aj stránky Dark webu. Obsahuje stránky, ktoré ponúkajú služby ako obchodné intranety, webmail platformy, databázy, online banking platformy a služby, ktoré si zvyčajne vyžadujú heslo alebo iné spôsoby autentifikácie. [7] Skoré odhady hovoria, že veľkosť Deep webu je okolo 4000 až 5000 násobne väčšia ako Surface web, avšak Deep web stále rastie, čo znemožňuje odhad veľkosti Deep webu. [3]

1.1.3 Dark web (Temný web)

Dark web je malá časť v rámci Deep webu, ktorá je spojená s kriminalitou a nelegálnymi online obchodmi. Pre prístup k týmto stránkam je užívateľ nútený použiť softvér zaručujúci anonymitu. [1] Tor a I2P sú systémy, ktoré zaručujú anonymitu a fungujú na princípe šifrovania prenosových dát vo vrstvách a presúva sa cez náhodne vybrané počítače po celom svete, z ktorých každý odstraňuje jednu vrstvu šifrovania pred tým, ako prenesie dáta na ďalší bod v sieti. Teoreticky to zaručuje anonymitu. [8] Ďalším softvérom, ktorý zaručuje anonymitu a umožňuje prístup k Dark webu, je Freenet. Mnoho užívateľov používa Dark web pre možnosť utajenia identity a vyhnutiu sa online monitoringu. Okrem utajenia identity sa Dark web používa aj na omnoho nelegálnejšie účely ako nákup a predaj nelegálnych drog, zbraní, exotických zvierat, ukradnutého tovaru a informácií (napríklad heslá a prístupy k účtom), falšovanie dokladov alebo detská pornografia. [2] Nachádzajú sa tu aj stránky s hazardnými hrami, zlodeji a mnoho iných nelegálnych služieb. [3] Vražda na objednávku je tiež jedna zo služieb Dark webu. Obeť môže byť odstránená za 1 až 3 týždne, ale zvyčajne nemôže byť mladšou ako 16 rokov alebo vysoko postavený politik. Existujú tu aj takzvané „Red rooms“, kde si užívatelia môžu platiť za mučenie obetí. [9] Nie však všetky služby Dark webu sú nelegálne. Tor je často používaný novinármi na kontaktovanie informátorov s cieľom zabezpečiť ich bezpečnosť od svojich vlád. Jednou z prvých veľkých stránok Dark

webu bola Torom skrytá služba WikiLeaks, vytvorená pre úniky citlivých firemných a vládnych dokumentov z anonymných zdrojov. Táto myšlienka sa odvtedy adaptovala nástroju zvanému SecureDrop, ktorý je integrovaný v službách Toru, aby akékoľvek novinárske organizácie mohli získavať anonymné príspevky. [8] V porovnaní so Surface webom je zložitejšie vyhľadávať stránky. Domény sú zámerne zavádzajúce a ťažko zapamätateľné (napr. Http://am4wuhz3zifexz5u.onion/). Ako používateľ musíte vedieť, čo hľadáte. [10]

Obrázok 1 – Rozdelenie Internetu [11]

1.1.3.1 Získavanie informácií o Dark webe

Je mnoho rozdielnych možností, ako získať informácie o Dark webe. Jedna z možností je obrátiť sa na Reddit, kde sa nachádza mnoho „subredditov“ vzťahujúcich sa na Dark Web, ako DarkNetMarkets, DeepWeb alebo Tor. Tieto fóra často poskytujú odkazy na stránky Dark webu. Reddit poskytuje verejnú platformu pre Dark web užívateľov, aby mohli diskutovať o rôznych aspektoch Toru. Nie je zašifrovaný, ani anonymný a ľudia, ktorí sa chcú zapojiť do diskusie si musia vytvoriť účet. [3]

1.1.3.2 Komunikácia na Dark webe

Ľudia, ktorí si však prajú bezpečnejšiu komunikáciu, môžu používať e-mail služby, web konverzácie alebo súkromné správy prístupné cez Tor:

- E-mail služby – typicky vyžadujú od užívateľov len prihlasovacie meno a heslo k registrácii. Tieto služby ponúkajú hlavne možnosť zasielania anonymných správ a zašifrovanú schránku.
- Anonymné real-timeové chat miestnosti ako The Hub a OnionChat. Kanály fór sú organizované podľa tém. Zatiaľ čo niektoré stránky pred zapojením sa do komunikácie nevyžadujú žiadne informácie od užívateľa, iné vyžadujú registráciu pomocou emailu.
- Súkromná komunikácia cez Tor Messenger je ďalším spôsobom pre užívateľov Tora, ktorí si prajú komunikovať cez pridanú vrstvu anonymity. Bitmessage je populárny komunikačný systém, ktorý ponúka zašifrovanú a silnú autentifikáciu. [3]

1.1.3.3 Navigácia na Dark webe

Obsah Deep a Dark webu nemôže byť vyhľadaný a následne indexovaný pomocou tradičných webových prehliadačov. Existujú však rôzne spôsoby pre navigáciu na Dark Webe. Užívatelia zvyčajne prehliadajú stránky Dark Webu prostredníctvom adresárov ako napríklad „The Hidden wiki“, ktorá organizuje stránky do kategórii, podobne ako Wikipédia. Okrem The Hidden Wiki môžu užívatelia použiť vyhľadávače ako napríklad Torch alebo DuckDuckGo. [3]

1.1.3.4 Platba na Dark webe

Bitcoin je nehmotná mena, ktorá je často používaná pri transakciách na Dark webe. Je to decentralizovaná digitálna mena, ktorá zaručuje anonymnú peer-to-peer transakciu. Užívatelia ich zvyčajne získavajú tým, že ich prijímajú ako platbu, vymieňajú si ich za tradičnú menu alebo ich „ťažia“. Ak sa pri platbe používa Bitcoin, transakcia sa zaznamenáva do peňaženky nazývanej „blockchain“. Informácie zaznamenávané v „blockchain“ predstavujú bitcoinové adresy odosielateľa a príjemcu. Adresa neidentifikuje jednoznačne žiadny bitcoin, adresy určujú len konkrétnu transakciu. Adresy užívateľov sú priradené a uložené v peňaženke. Peňaženka obsahuje súkromný kľúč, ktorý označuje tajné číslo, ktoré umožňuje jednotlivcovi minúť bitcoiny z jeho príslušnej peňaženky. Adresa transakcie a kryptografický podpis sú použité pre verifikáciu transakcie. [3]

Ethereum je taktiež kryptomena, ktorou je možné platiť na Dark webe. Je založená rovnako ako Bitcoin na decentralizovanej databáze – blockchain databáza. Avšak Ethereum sa líši svojím účelom a schopnosťou od Bitcoinu. Bitcoin blockchain je zameraná na sledovanie transakcií s virtuálnou menou bitcoin, Ethereum blockchain sa používa na spúšťanie zdrojového kódu akejkoľvek decentralizovanej aplikácie. [12]

Ďalšou kryptomenou používanou na Dark webe je mena zvaná Monero. Monero používa kryptografiu na ochranu odosielateľských a prijímacích adries. Taktiež pri transakciách sa používa kryptografia, čo zaručuje nemožnosť sledovania a dôveryhodnosť. Každá transakcia kryptomenou Monero štandardne zabraňuje odosielaniu a prijímaniu adries ako aj transakčným sumám. Toto vždy zapnutá služba zabezpečuje, že každá aktivita používateľa Morena zvyšuje súkromie všetkých ostatných používateľov. Na rozdiel od Bitcoinu, pri platbe Monerom si žiadny užívateľ nemôže pozrieť komu a koľko XMR (Monero) bolo odoslané. [13]

1.2 História Dark webu

História temného webu je skoro taká stará ako samotná história Internetu. Tá istá technológia, ktorá vytvorila Internet a web dostupnými, tiež umožnila byť temnému webu dostupným vďaka ich architektúre a dizajnu. Dokým ARPANET nemusel obsahovať temný web, netrvalo dlho a ľudia začali využívať túto technológiu na veci, ktoré chceli zachovať utajené. [14] Prvé zmienky temného webu začali už koncom 60. a začiatkom 70. rokov.

1.2.1 Prvá správa medzi počítačmi prepojenými pomocou ARPANETu

Študent Kalifornskej univerzity Charley Kline napísal 29.10.1969 prvú správu medzi počítačmi prepojenými pomocou ARPANETu (predok Internetu vytvorený Agentúrou Pentagonu pre pokročilé obranné výskumné projekty). Len prvé dve písmená z elektronického odoslania, „LOGIN“ sa dostali až k počítačom Standfordskej univerzity. [14] Netrvalo však dlho a ľudia si začali vytvárať „dark web stránky“ – alebo tajné stránky, ktoré používali ARPANET. [15]

1.2.2 Dátové raje

S narodením moderného webu, označovaným štandardizáciou balíka internetových protokolov z roku 1982, nastal aj veľký problém s ukladaním citlivých alebo nelegálnych údajov. [14] Aby sa užívatelia vyhli tomuto problému, pokúšali sa vytvoriť takzvané „dátové

raje“, kde by citlivé informácie mohli byť uložené ďaleko od zvedavých očí štátnych orgánov. Nestačilo izolovať informácie digitálne, mnoho užívateľov taktiež oddelili svoje dáta fyzicky.

Mnohé z týchto dátových rajov existovali na ostrovoch v Karibiku, konkrétne v Anguille a v mnohých smeroch fungovali rovnako ako daňové raje. Vzhľadom k tomu, že raje spadli mimo hlavnú krajinu, platili rôzne pravidlá a ľudia sa mohli vyhýbať určitým zákonom. [15]

1.2.3 Nelegálne zdieľanie dát

Vzhľadom na to, že v deväťdesiatych rokoch minulého storočia sa Internet stal maintreamom, klesajúce náklady na ukladanie dát spolu s pokrokom v kompresii súborov spôsobili výbuch aktivity dark webu, keďže používatelia začínajú zdieľať materiály chránené autorskými právami. V deväťdesiatych rokoch internetový peer-to-peer prenos údajov vytvára decentralizované dátové uzly, z ktorých niektoré ako tzv. „topsites“ (odkiaľ pochádza väčšina nelegálnych hudobných a filmových súborov), sú chránené heslom a známe iba členom. [14] Nebolo prípustné ukradnúť hudbu a dať ju iným ľuďom zadarmo, takže mnohé z týchto služieb sa neindexovali na dark webe. Dnes takmer všetky tieto služby existujú na dark webe, aby sa vyhli súdnym sporom a zachovali si anonymitu. [15]

1.2.4 Freenet

Začiatkom roku 2000, vývojár Ian Clarke uvoľnil Freenet ako súčasť svojej vysokoškolskej diplomovej práce. Revolučný softvér, ktorý ponúka anonymný prechod do najtmavších stránok webu, kde je možné získať všetko, od detskej pornografie po inštrukcie na vytvorenie výbušnín. [14] Freenet tiež indexuje niekoľko webových stránok nachádzajúcich sa na dark webe, ktoré by inak nebolo možné nájsť. Umožňuje používateľom prístup k všetkým druhom nezákonného a citlivého obsahu a zároveň poskytuje ochranu identity. [15]

1.2.5 HavenCo

Ryan Lackey a Sean Hastings začali v júni v roku 2000 biznis na Sealande, bizarnom, nominálne nezávislom štáte, umiestnenom na námornej pevnosti z 2. svetovej vojny pri britskom pobreží. Začiatkom, zvaným HavenCo, plánovali hosťovanie súkromných dát (okrem spamu, detskej pornografie, prania špinavých peňazí) na vysokoúrovňových serveroch chladených dusíkom a ukrytých v pevnostiach. [14] Hoci zakázal určité typy obsahu, HavenCo umožňoval veľa slobody. Avšak nikdy nebol finančne úspešný. Obzvlášť po tom, ako ho Sealand znárodnil. [15]

1.2.6 Tor

Výskumníci z U.S. Naval Research Laboratory vydali 20.9.2002 skorú verziu Tor ("The Onion Router"), ktorá zakrýva miesto a IP adresu užívateľov, ktorí používajú tento softvér. Pôvodne navrhnutý k ochrane identity amerických činiteľov a disidentov v represívnych krajinách, ako je Čína. [14] Tor veľmi rýchlo priťahoval ľudí, ktorí ho chceli použiť na nezákonné účely. To sa stalo jedným z najlepších spôsobov, ako nakupovať alebo prezerať všetky druhy nezákonného obsahu, hoci ho americká vláda vytvorila. [15]

1.2.7 Distribúcia obsahu, chráneného autorskými právami

Magazín Wired odhadoval, že „média dark webu distribuujú viac ako pól milióna filmov každý deň“. Poháňaný rozkvitajúcou šírkou pásma, „podzemná sieť“ exploduje do veľkého porušovania osobných práv, od hollywoodských trhákov až po Microsoft Office. Štúdie firmy IDC odhadujú, že softvérové pirátstvo v roku 2005 stálo tento biznis na celom svete 34 miliárd dolárov. [14] Samotné USA stratilo 6,9 miliardy dolárov len kvôli krádeži softvéru. [15]

1.2.8 Bitcoin

Prvá zmienka o Bitcoine bola už v roku 2008, kedy Satoshi Nakamoto vydal dokument, ktorý podrobne opisuje myšlienku Bitcoinu. Avšak až 3. januára 2009 sa prvý Bitcoin dostal na trh. [15] Satoshi Nakamoto „vyťažil“ prvý Bitcoin, formu nevystopovateľnej kryptomeny. Na rozdiel od predchádzajúcich mien, ktoré zlyhali, pretože užívatelia si mohli kopírovať ich peniaze, Bitcoin využíva inovatívne verejnú účtovnícku knihu, ktorá zabraňuje dvojitému míňaniu. Kryptomena sa stáva okamžitým hitom dark webu, jeho anonymita je dokonalým nástrojom na pranie peňazí a kriminálnej aktivity. [14]

1.2.9 Rozdiel medzi Dark webom a Deep webom

Začiatkom roka 2010 publikácie začali vysvetľovať rozdiel medzi dark webom a deep webom. Zatiaľ čo deep web zahŕňa ľubovoľnú časť Internetu, ktorá nie je prístupná bežným prehliadačom alebo vyhľadávacím nástrojom ako je Google, dark web sa skladá z konkrétnych stránok, ktoré sa chcú vyhnúť detekcii.

Používatelia dark webu chcú zostať anonymní. Majú tendenciu byť ľuďmi, ktorí chcú získať prístup k nelegálnym alebo citlivým informáciám. Na dark webe kupujú drogy, pripravujú teroristické útoky alebo distribuujú nezákonný sexuálny materiál bez obáv z následkov. Iní,

ktorí ho používajú, zahŕňajú politických disidentov a novinárov v represívnych režimoch. [15]

Kyber ochranná firma Procysive odhaduje, že dark web je domovom pre „viac ako 50 000 extrémistických web stránok a viac ako 300 teroristických fór“. [14]

1.2.10 Silk Road

Blog vydaný Gawkerom uvádza 1.6.2011 výstavu na Silk Road, tajnom obchode, ktorý „nakupuje a predáva nelegálne drogy tak ľahko ako nákup elektroniky“. Je to ako Amazon.com pre metamfetamín a LSD, s výnimkou toho, že sú dostupné len pre užívateľov Toru. [14] Expozé skončilo zvýšením návštevnosti stránky a významne zvýšilo hodnotu Bitcoinu. Avšak aj štátne orgány začali venovať Silk Road veľkú pozornosť. [15]

1.2.11 Zatknutie Erica Eoina Marquesa

Írsky úrad napadol 1.8.2013 dublinský byt Erica Eoin Marquesa, popisovaného FBI ako „najväčší sprostredkovateľ detského porna na planéte“. Jeho zatknutie sa zhoduje so záhadným vypnutím obrovských častí dark webu, údajne ako súčasť operácie FBI, ktorá využila zraniteľnosti vo webovom prehliadači Mozzila k identifikácii užívateľov Toru. Užívateľské identity sú údajne späť smerované na sever v Severnej Virgínii. [14] Zatknutie bolo tiež významné, pretože kvôli tomu štátne orgány našli spôsob, ako preniknúť do anonymity Toru. [15]

1.2.12 Utajená komunikácia

Len pár dní po zatknutí Erica Eoina Murquesa v roku 2013 [15] americká vláda zachytáva tajnú komunikáciu medzi šéfom Al-Kaidy Ayman al-Zawahiri a Nasir al-Wuhayshi, vedúcim Al-Kaidy na Arabskom polostrove Jemen. Tajná online komunikácia viedla k „zabarikádovaniu“ veľvyslanectiev v 21 krajinách v moslimskom svete. [14]

1.2.13 Zatknutie Rossa Williama Ulbricha

FBI zastavila Silk Road a zatkla 1.10.2013 Rossa Williama Ulbricha, známeho svojím online menom „Dread Pirate Roberts“, za údajné plánované riadenie Silk Road. Podľa obžaloby podanej na americkom federálnom súde táto stránka dosiahla viac ako 1,2 miliardy dolárov z predaja medzi rokmi 2011 až 2013. [14] Zastavenie však viedlo k vzostupu podobných webových stránok súvisiacich s drogami. V priebehu jedného mesiaca vznikla spoločnosť

Silk Road 2.0, ktorá nahradila bývalú webovú stránku, aj keď bola v roku 2014 taktiež zatvorená. [15]

1.2.14 Predstavenie Silk Road 2.0

Stránka Technews uvádza, že online obchody ako Black Market Reloaded a Deepbay, ktoré otvorene reklamujú narkotiká, zaznamenávajú prudký nárast sledovanosti. „Nepochybne sa všetci preskupíme na inom mieste“, napísal jeden z moderátorov Silk Roadu po tom, čo bol online trh zrušený. „Teším sa, keď vás znovu uvidím. Stále sa venujem obchodovaniu bez zásahu vlády do vašich osobných záležitostí“. Tesne mesiac po zrušení pôvodného Silk Road, bol nový anonymný dark web trh zvaný Silk Road 2.0 opäť online. [14]

1.2.15 Štúdie Dark webu

V roku 2016 štúdie s názvom "Cryptopolitik and the Darknet" od výskumníkov na King's College v Londýne zistili, že webové stránky na dark webe sú najčastejšie používané na kriminálnu činnosť. Zistili 5205 webových stránok TOR a boli schopní klasifikovať obsah pre 2723 ľudí. Z toho vyplýva, že 1547 (57%) ponúklo nelegálne informácie a služby. Patrí sem napr. pranie špinavých peňazí, predaj zbraní, falšovaná mena, odcudzenie kreditných kariet, predaj liekov a nelegálnych drog, hackovanie, násilie, nájom vrahov a materiál pre dospelých vrátane násilia na deťoch a zvieratách. Aj v roku 2016 úrad OSN pre drogy a kriminalitu vydal svoju Svetovú správu o drogách, ktorá zistila, že počet užívateľov drog, ktorí nezákonne nakupovali drogy na dark webe narastal. [15]

1.2.16 Pokračovanie v tempe nárastu Dark webu

Keďže ľudia naďalej používajú dark web, potreba a hodnota kryptomien naďalej narastá. Bitcoin a iné kryptomeny ako sú Monero a Litecoin, poskytujú menej zistiteľné zdroje platieb, čo umožňuje kupujúcim a predávajúcim ľahšie utajiť nelegálnu aktivitu. Dark web a kryptomena vzájomne profitujú. Pokiaľ existuje dark web, pravdepodobne budú existovať aj kryptomeny. [15]

2 ANALÝZA A POROVNANIE MOŽNOSTÍ PRIPOJENIA DO TEMNÉHO WEBU

Tradične, keď užívateľ navštívi akúkoľvek stránku nachádzajúcu sa na Surface webe, je sledovaný prostredníctvom IP adresy. Pre prístup k temnému webu je užívateľ donútený zachovať si svoje súkromie a použiť špecializovaný softvér, zaručujúci anonymitu na maskovanie svojej identity a ochranu proti nebezpečenstvám na temnom webe. [16]

2.1 Tor

Tor je najpoužívanejší open source softvér pre anonymné prehliadanie Internetu. Bol vyvinutý v polovici deväťdesiatych rokov výskumníkmi z U.S. Naval Research Laboratory ako „The Onion Routing Program“. Pôvodne bol vyvinutý hlavne preto, aby chránil vládnu komunikáciu. [17]

Sieť Tor je platformou umožňujúcou anonymnú komunikáciu. Základnou myšlienkou, ktorú ponúka Tor, je smerovanie prevádzky cez prekrývajúcu sa sieť smerovačov, ktoré fungujú na celom svete a sú riadené dobrovoľníkmi. Toto smerovanie zahŕňa viac ako sedem tisíc vrstiev, ktoré sa primárne zameriavajú na skrytie identity používateľa, polohy a používania. Sieť Tor sa skladá z troch rôznych typov uzlov: adresárových serverov, výstupných bodov a interných vrstiev. Skupina pripojených smerovačov vytvára obvod šifrovaných spojení cez vrstvy v sieti Tor. Žiadny zdroj na tejto dráhe vrstiev nepozná úplnú cestu okruhu alebo totožnosť a umiestnenie ostatných účastníkov v okruhu. V ideálnom prípade je takýto obvod udržiavaný nažive približne 10 minút, potom sa novým požiadavkám poskytne nový okruh. Tým sa používateľ stáva menej zraniteľným voči každému, kto pozoruje sieť alebo vykonáva analýzu návštevnosti. [18]

Tor taktiež umožňuje dosiahnuť obsah, ktorý nie je prístupný z bežných prehliadačov. Umožňuje používateľom publikovať webové stránky a iné služby bez toho, aby bolo možné odhaliť umiestnenie stránky. Jednotlivci používajú Tor pre sociálne citlivú komunikáciu: diskusné miestnosti a internetové fóra pre ľudí, ktorí boli znásilnení a zneužívaní alebo ľudí, ktorí trpia na rôzne choroby. Novinári používajú tento softvér pre bezpečnejšiu komunikáciu s informátormi. Taktiež sa používa aj ako náhrada tradičných VPN, ktoré odhaľujú počet a čas komunikácie. Tor pomáha znižovať riziká jednoduchých a sofistikovaných analýz návštevnosti prostredníctvom distribúcie vašich transakcií na viacerých miestach na

Internete, takže žiadny bod vám nemôže prepojiť váš cieľ. Tor funguje iba pre toky TCP a môže byť použitý ľubovoľnou aplikáciou s podporou SOCKS. [19]

2.2 I2P (The Invisible Internet Project)

Hlavným zameraním I2P bolo vytvoriť sieť v rámci Internetu. Komunikačný mechanizmus I2P silne spolieha na smerovanie založené na paketoch. Tento projekt bol navrhnutý od začiatku na pripojenie sa k Temnému webu. [20]

I2P je anonymná sieť, ktorá odhaľuje jednoduchú vrstvu, ktorú aplikácie môžu použiť k anonymnému a bezpečnému posielaniu správ medzi sebou. Celá komunikácia je ukončená šifrovaním (4 vrstvy šifrovania sa používajú pri odosielaní správy) a dokonca aj koncové destinácie sú kryptografické identifikátory (dvojica verejných kľúčov).

K anonymizácii odosielaní správ má každá klientska aplikácia vlastný I2P „router“, ktorý buduje niekoľko prichádzajúcich a odchádzajúcich „tunelov“ – postupnosť účastníkov, ktorí odovzdávajú správy jedným smerom (ku a od klienta). Na druhej strane, ak klient chce odoslať správu inému klientovi, klient odošle túto správu z jedného zo svojich odchádzajúcich tunelov, ktoré sa zameriavajú na vstupné tunely niekoho z ostatných klientov a nakoniec dosiahnu cieľ. Každý účastník siete si vyberá dĺžku týchto tunelov a tým robí kompromis medzi anonymitou, latenciou a výkonnosťou podľa vlastných potrieb. Výsledkom je, že počet uzlov je potrebné minimum k splneniu podmienok komunikácie bez ohrozenia odosielateľa a príjemcu. V rámci siete I2P aplikácie nie sú obmedzené v tom, ako môžu komunikovať - tie, ktoré zvyčajne používajú UDP, môžu využívať funkčnosť základnej I2P a tie, ktoré zvyčajne používajú TCP, môžu využívať TCP ako streamingovú knižnicu. Existuje generická TCP/I2P tunelová aplikácia, ktorá umožňuje účastníkom preposielať TCP prúdy (streamy) do I2P siete ako aj prijímať streamy mimo siete a preposielať ich špecifickým TCP/IP adresám. I2P nie je vlastne outproxy sieť - klient, ktorému posielate správu, je kryptografický identifikátor, nie nejaká IP adresa, takže správa musí byť adresovaná niekomu, kto používa I2P. Je však možné, že tento klient je „outproxy“, čo vám umožňuje anonymne využívať ich internetové pripojenie. Aby sme to dokázali, eepproxy bude akceptovať bežné URL adresy bez I2P a presmerovať ich na konkrétne miesto určenia, ktoré používa proxy server HTTP, umožňujúce jednoduché anonymné prehliadanie normálneho webu. Jednoduché outproxy ako tie, ktoré nie sú z dlhodobého hľadiska realizovateľné z viacerých dôvodov (vrátane nákladov na prevádzku jedného,

rovnako ako anonymity a bezpečnostných problémov, ktoré zavádzajú), ale za určitých okolností by táto technika mohla byť vhodná. [21]

2.3 Freenet

Freenet je plne distribuovaná, peer to peer anonymná sieť, ktorá povoľuje užívateľom prehliadať web anonymne, zdieľať a publikovať obsah rovnako ako webové stránky zvané „freesites“. Môže byť definovaný ako internet v rámci Internetu, pretože užívatelia nie sú obmedzení zdieľaním dát, ale môžu používať Freenet pre akýkoľvek účel. Na základe zvýšenia robustnosti siete a eliminácii jednotlivých porúch sa využíva plne decentralizovaná architektúra. Snahou Freenetu bolo vytvoriť komunikačnú sieť odolnú voči cenzúre. [18]

Freenet taktiež nasleduje mechanizmy, ktoré používajú I2P a Tor pričom komunikácia medzi uzlami je šifrovaná a smeruje cez ďalšie uzly v sieti, čo sťažuje sledovanie zúčastnených zdrojov a obsahu.

Každý užívateľ je žiadaný prispievať do siete tým, že poskytuje objem prenosových dát a časť ich hard disku pre úložisko dát. Táto časť slúži pre ukladanie súborov, akokoľvek užívateľ nemôže nájsť obsah týchto súborov, pretože sú zašifrované. Žiadny užívateľ nevie, čo má uložené v úložisku dát. Freenet je schopný ukladať len populárny obsah. Súbory sa automaticky uchovávajú alebo sú odstránené v závislosti od toho, aké sú populárne. To zapríčiňuje, že najmenej populárny obsah je automaticky zmazaný, čím sa vytvorí priestor pre nový alebo populárny obsah. [18]

Freenet možno použiť len na prístup k obsahu, ktorý je nahratý do Freenet siete. Freenet sa používa na publikovanie „freesites“, komunikáciu prostredníctvom fór, distribúciu obsahu a tiež na sťahovanie. Komunikácia na Freenete je presmerovaná cez alternatívne uzly, čo znižuje šancu, že užívatelia budú odhalení. Freenet tiež dovoľuje užívateľom pristupovať k súborom dokonca aj vtedy, keď je užívateľ, ktorý nahral súbor offline. [22]

Ak chce užívateľ pridať nový súbor, pošle správu o vložení do siete, ktorá obsahuje súbor, ktorému je pridelený GUID, ktorý je nezávislý na umiestnení, čo vedie k uloženiu súboru na jednu zo sád uzlov. Súbor môže byť replikovaný alebo migrovaný na iné uzly v sieti.

Ďalšou výhodou je, že žiadny uzol nie je zodpovedný za obrovské súbory dát. Uzly, ktoré dostávajú stále nové dáta, vymazávajú neobnovené dáta vtedy, ak alokovaná pamäť na disku je plná. Aby užívateľ mohol načítať súbory, odošle správu s požiadavkou obsahujúcu GUID. Po dosiahnutí uzlov, ktoré obsahujú súbor, uzol prenesie informácie späť k pôvodcovi

požiadavky. Šifrovanie dát a odosielanie žiadostí znemožňuje zistenie, kto vložil obsah do siete, kto ho vyžadoval a kde bol obsah uložený. [23]

2.4 Porovnanie možností pripojenia k temnému webu

Tor a I2P sú veľmi podobné. Oba softvéry poskytujú anonymné proxy siete na rozdiel od Freenetu. [24] Freenet je viac distribuované dátové úložisko s ustanoveniami aplikácii, ktoré umožňujú ešte väčšiu a anonymnú komunikáciu. Všetky z nich poskytujú používateľom anonymitu, no poskytujú odlišné funkcie a majú vlastnú úroveň anonymity.

Tor poskytuje prehliadač s názvom „Tor Browser“, ktorý funguje prostredníctvom siete šifrovaných tunelov medzi smerovačmi siete, ktoré sú náhodne vybrané a vytvárajú okruh, v ktorom každý smerovač obsahuje len informácie o predchádzajúcich a následných pripojeniach a existuje len 10 minút. Po tomto čase sa poskytne nový okruh. Tor ponúka taktiež funkcie, ktoré zlepšujú nastavenia ochrany osobných údajov a zabezpečenia. [18] Využíva prístup založený na adresári - poskytuje centralizovaný bod na riadenie celkového „pohľadu“ siete, ako aj zhromažďovania a reportovania štatistík, na rozdiel od distribuovanej databázy I2P a užívateľskému výberu. [24]

I2P neposkytuje žiadny prehliadač, ale musí byť manuálne nainštalovaný pomocou RP inštalácie. I2P šifruje svoje dáta v 4 vrstvách a dokonca uzly sú kryptografické identifikátory, takže nikto z príjemcov správy neodhalí ich IP adresy. [21] Zatiaľ čo základným zámerom spoločnosti Tor je umožniť svojim používateľom prístup na Internet anonymne, l2P sa zameriava na vytváranie vlastných interakcií. Preto sieť I2P nie je dostupná z bežného počítača. Po nainštalovaní softvéru RP sa počítač môže pripojiť k sieti a pôsobiť ako smerovač a začať smerovať prevádzku. Vytvára tak dynamickú a decentralizovanú sieť, čo sťažuje zistiť, čo sa prenáša na každom smerovači.

Freenet na rozdiel od týchto sietí neposkytuje proxy sieť, ale vysoko decentralizovanú peer-to-peer platformu. Komunikácia uzlami Freenet je šifrovaná a je smerovaná cez iné uzly, aby bolo veľmi ťažké určiť, kto a aké informácie požaduje. Dokým Tor a I2p používajú smerovače pre komunikáciu, Freenet pracuje na princípe ukladania šifrovaných častí dát na pevný disk každého užívateľa bez toho, aby vedeli celý obsah. [25] Je plne decentralizovaná kvôli zníženiu zraniteľnosti voči útokom. Používateľ sa môže rozhodnúť, s ktorými používateľmi sa chce spojiť. Obsahuje režim „Darknet“, v ktorom sa užívateľ môže

rozhodnúť pripojiť sa len k jeho priateľom a režim „Opennet“, kde užívateľ pozná niekoľko centrálnych uzlov, vďaka ktorým sa dokáže pripojiť na ďalšie uzly. [26]

Rýchlosť

Čo sa týka objemu prenosových dát, Tor je z týchto troch softvérov najmenej efektívny. Ak ide o latenciu, I2P je o niečo lepší. Freenet stráca v oboch týchto aspektoch, pretože každý užívateľ musí prispievať k objemu prenosových dát, ktoré používa, aby sa mohol pohybovať v celej sieti. Požiadavka je smerovaná cez veľa uzlov v sieti a výsledkom je, že spotreba objemu prenosových dát je relatívne väčšia v porovnaní s ostatnými systémami. [18]

Darknet stránky

V prípade statického obsahu, je Freenet v popredí, pretože má schopnosť udržať obsah aj vtedy, keď je užívateľ offline alebo prestane používať platformu. I2P zase obsahuje obrovskú ponuku skrytých služieb a mnoho eepsites. [18]

Obsah

Obsah všetkých troch platforiem sa líši v ich hlavných cieľoch. Tor bol navrhnutý, aby zjednodušil prístup k bežnému Internetu a zároveň bol anonymný, obsah Toru je obsahom celého Internetu. Tor taktiež poskytuje niektoré skryté služby. I2P sa zameriava na vytváranie siete v rámci Internetu a má omnoho viac skrytých služieb ako Tor a má viac obsahu so zdieľaním súborov. Freenet obsahuje oveľa viac statického obsahu a môže uchovávať dáta aj po tom, čo sa poskytovateľ odhlási alebo prestane používať platformu. Freenet môže obsahovať akýkoľvek obsah, pokiaľ zostane populárny. [18]

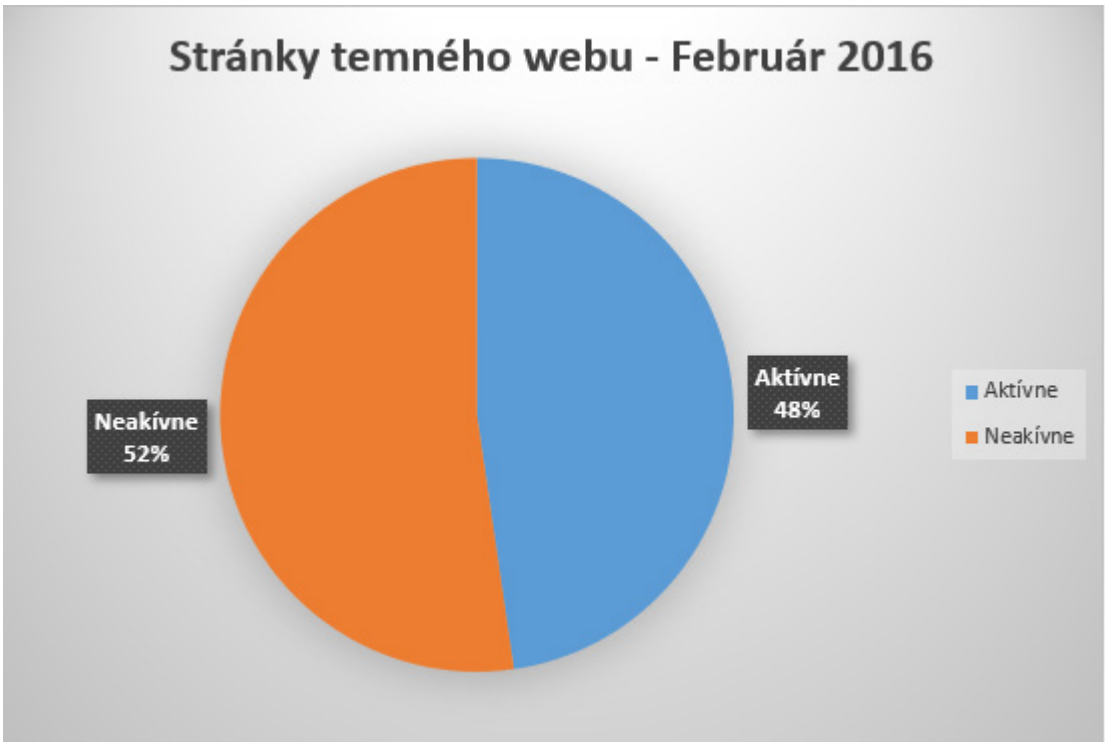
II. PRAKTICKÁ ČASŤ

3 PRIESKUM DOSTUPNÝCH ŠTATISTICKÝCH INFORMÁCIÍ DO SÚČASNOSTI

Pretože mnohí ľudia nie sú oboznámení s tmavým webom a jeho obsahom, rád by som v tejto časti poukázal na môj prieskum dostupných štatistických informácii. Podotýkam, že štatistiky nemusia byť presné, keďže zdrojov so štatistikami temného webu je málo, a preto nebolo možné dané informácie overiť. V tomto bode rozoberám rozsah aktívnych a nelegálnych stránok. Ďalej sa zaoberám službami, ktoré môžete v tejto časti webu nájsť, akou menou sa najčastejšie dané služby platia a následne aj samotnou využiteľnosťou týchto služieb.

3.1 Aktivita stránok temného webu

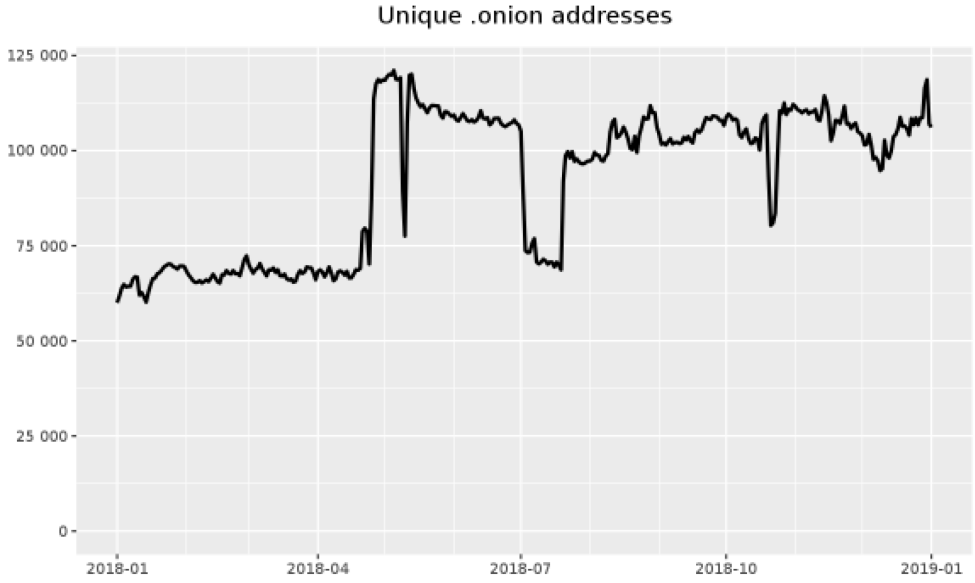
Podľa štatistík z februára 2016 vidieť, že až 52% stránok temného webu tvoria neaktívne adresy. Tieto adresy mohli byť zablokované alebo zrušené federálnymi agentúrami alebo neobsahujú žiadny obsah. Zvyšnú časť zahŕňajú stránky, ktoré sú aktívne, čo znamená, že sú dostupné pre užívateľov temného webu.



Obrázok 2 – Aktivita stránok temného webu [27]

3.2 Onion adresy

Tor Metriky zbierajú anonymizované údaje o užívateľoch, službách a prevádzke softvéru Tor. Najväčší počet adries v rozmedzí roku 2018 a 2019 bol zaznamenaný v máji roku 2018, kedy počet stránok vzrástol na zhruba 122000. Tento počet sa však nerovná reálnemu počtu stránok temného webu, keďže niektoré stránky majú niekoľko rôznych adries s doménou „.onion“. Mnohé z týchto stránok taktiež nemusia mať žiadny obsah. Od roku 2018 sa počet adries Toru navýšil z hodnoty 58000 na hodnotu 108000. Počet týchto adries sa však neustále mení, či už pribúdaním alebo ich uzatváraním.

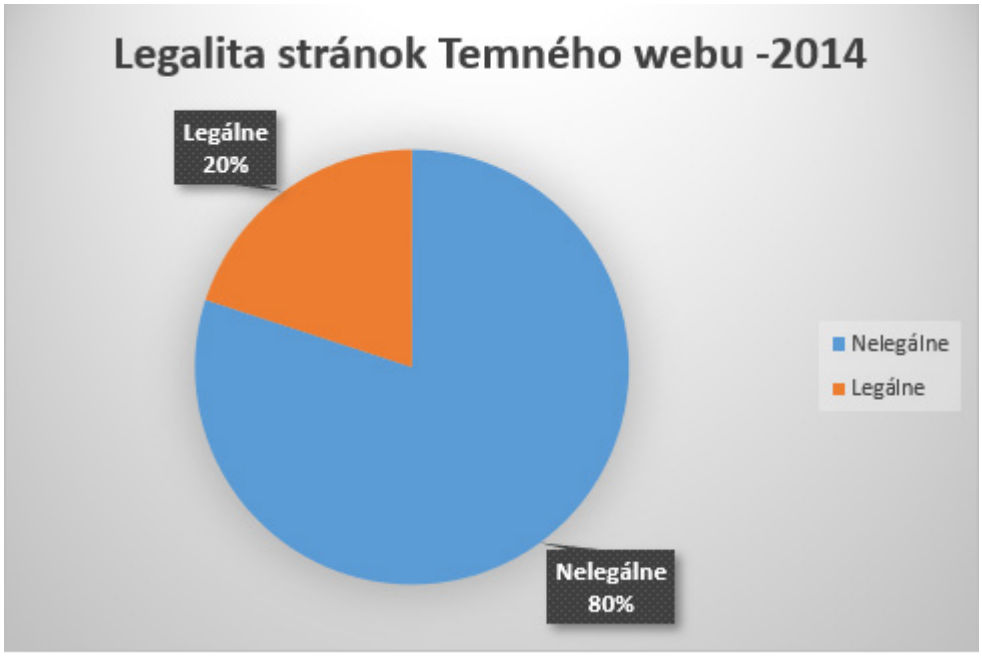


Obrázok 3 – Onion adresy [28]

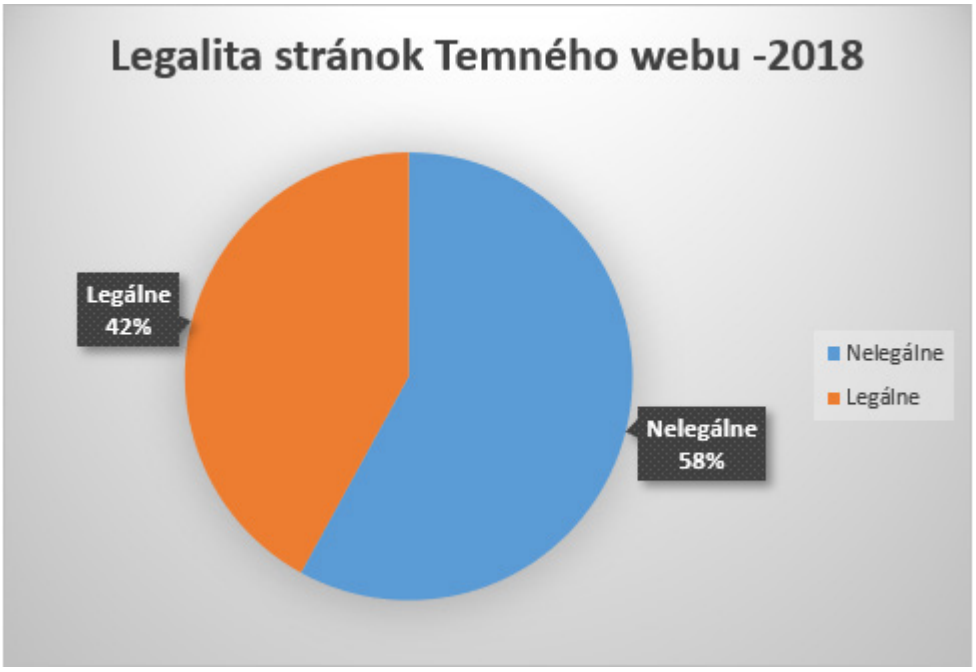
3.3 Legalita stránok

Štúdie, vykonané doktorom Garethom Owenom ukázali, že v roku 2014 až 80% návštevnosti temného webu cez prehliadač Tor bolo zneužité na nelegálne činnosti ako prezeranie detskej pornografie, online trhoviská s drogami a inými službami. Len zvyšných 20% malo legálnejšie využitie. Avšak štúdie z roku 2018 poukazujú, že okolo 58% návštevnosti temného webu práve cez tento softvér bolo využité na nelegálne služby a len 42% pre legálne činnosti tohto webu.

Tieto štúdie poukazujú, že od roku 2014 po rok 2018 došlo k poklesu zneužívania temného webu na nelegálne činnosti až o 22%.



Obrázok 4 – Legalita temného webu rok 2014 [29]

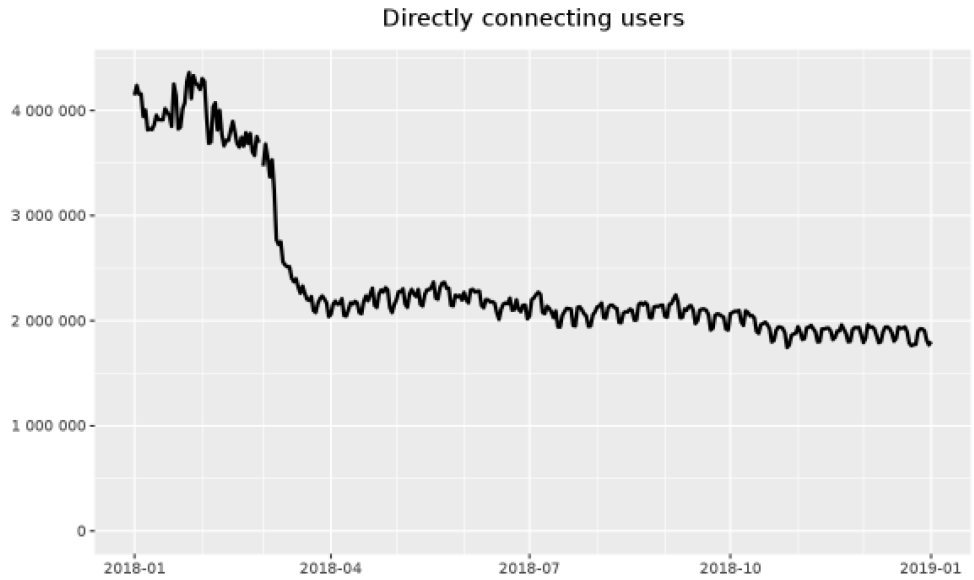


Obrázok 5 – Legalita stránok temného webu rok 2018 [29]

3.4 Užívatelia Temného webu

V metrikách Toru taktiež zaznamenávajú denné používanie Toru. Začiatkom roku 2018 mal Tor okolo 5 000 000 užívateľov, avšak v apríli roku 2018 bol zaznamenaný rapídny pokles užívateľov, kedy toto číslo kleslo o takmer 3 000 000 a hodnota sa ustálila na 2 000 000 užívateľov až do roku 2019. Tieto čísla sú založené na predpoklade, že priemerný užívateľ

vykoná okolo 10 adresárových požiadaviek denne. Skutočný počet užívateľov preto môže byť rozličný od tohto čísla. Tieto hodnoty však nepopisujú presný počet užívateľov temného webu. Tor metriky odhadovali, že v roku 2015 okolo 3,4% užívateľov použili Tor na prístup k temnému webu, čo by v súčasnosti predstavovalo okolo 68000 užívateľov využívajúcich Tor na služby temného webu.

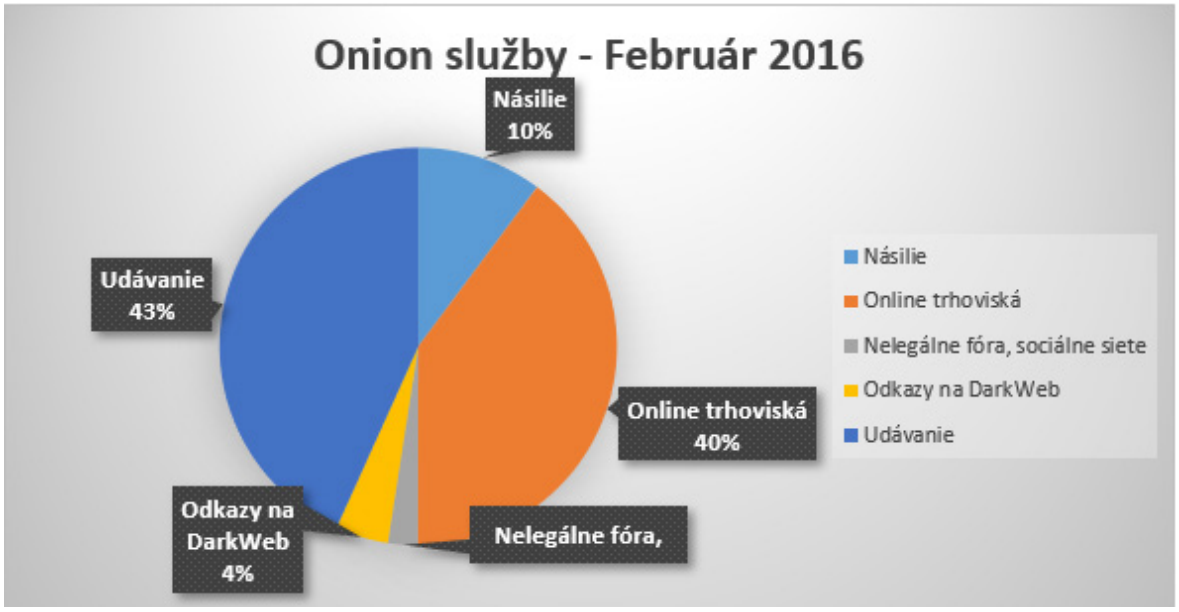


Obrázok 6 – Užívatelia Toru [30]

3.5 Onion Služby

Temný web je známy hlavne tým, že zahŕňa nelegálny obsah ako je predaj drog, zbraní, pornografia a iné nelegálne služby.

Štatistiky z februára 2016 poukazujú, že dominantné služby nachádzajúce sa na temnom webe sú služby udávania. Tieto služby zahŕňali vyše 43% zo všetkých služieb dostupných na temnom webe. Ďalšími službami, ktoré sa vyskytovali najčastejšie na temnom webe, sú služby týkajúce sa online trhovísk. Tieto trhoviská zahŕňali okolo 40%. Násilie pokrývalo okolo 10% zo všetkých služieb a zvyšné percentá služieb patrili službám ako sú adresáre odkazov alebo nelegálne fóra a sociálne siete.



Obrázok 7 – Onion služby [27]

3.6 Najvyužívanejšie služby temného webu

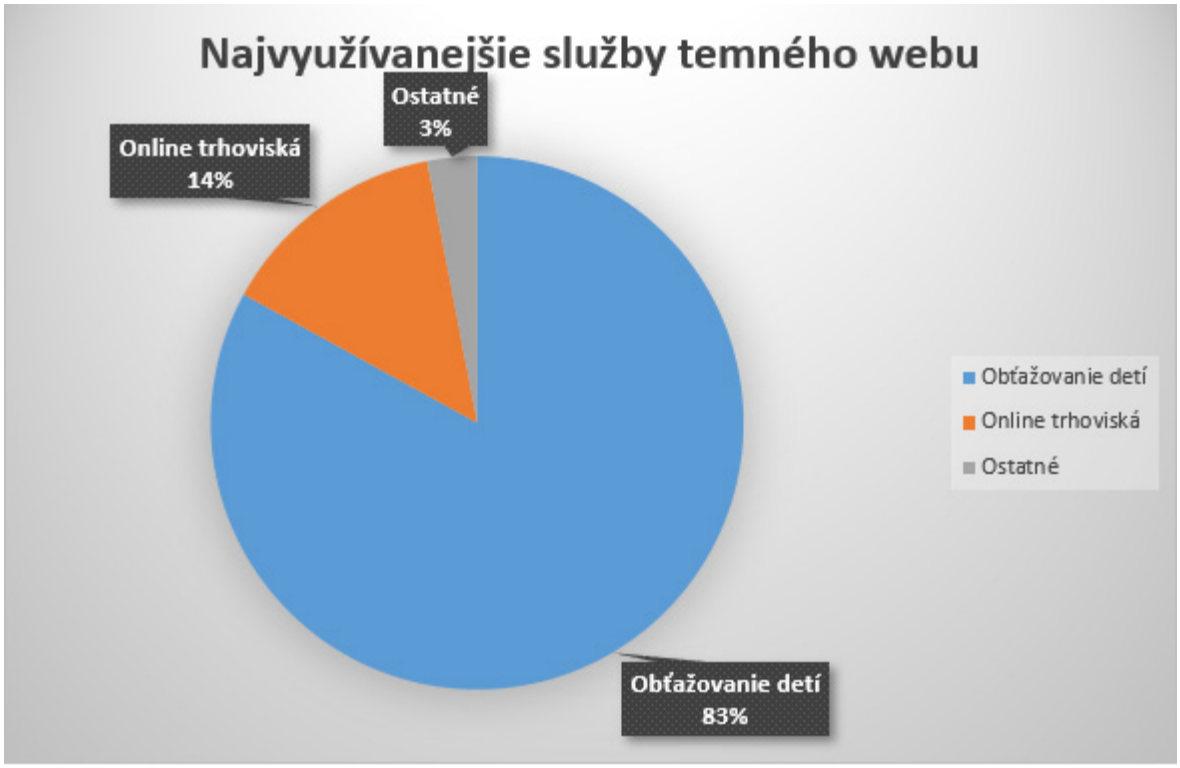
Štúdie vykonané výskumníkmi z Univerzity Portsmouth vo Veľkej Británii z decembra 2014 sa zaoberali najvyužívanejšími službami na temnom webe. Pre získanie daných informácií zapojili 40 počítačov, aby pôsobili ako prístupné body v sieti Tor. Šokujúcim výsledkom štatistík najvyužívanejších služieb temného webu je, že len 2% zo všetkých služieb nachádzajúcich sa na temnom webe, pokrývalo až okolo 83% návštevnosti temného webu pomocou softvéru Tor. Tieto služby obsahujú detskú pornografiu a iný obsah, týkajúci sa obťažovania detí. Mnohé z týchto stránok dokonca obsahovali aj slovo „pedo“ v názve domény.

Ďalších 24% zahŕňajú online trhoviská ako napríklad Silk Road alebo Wall Street Market, ktoré ponúkajú tovar ako drogy, zbrane, falošné peniaze, falšovanie osobných údajov a rôzny nelegálny tovar.

Tieto štúdie taktiež poukazujú, že 97% z celkovej návštevnosti temného webu pomocou Toru sa používa na nelegálnu činnosť.

Len zvyšné 3% návštevnosti zahŕňajú nie tak „temné“ služby.

Tieto štúdie boli dostupné z viacerých zdrojov [31, 32, 33], no ako si môžete všimnúť, súčet hodnôt týchto štúdií dosahuje hodnotu 110%, čo znamená, že tieto výsledky nie sú úplne presné.



Obrázok 8 – Najvyužívanejšie služby temného webu [31]

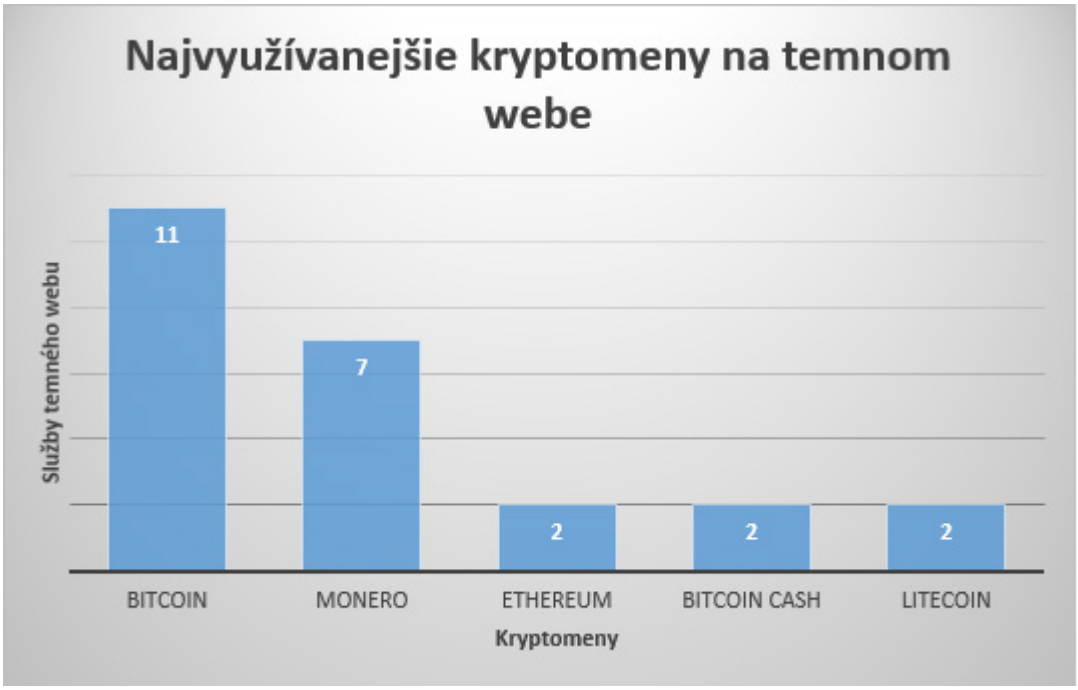
3.7 Kryptomeny využívané na temnom webe

Platba pomocou kryptomien sa stala populárna tým, že zaručuje bezpečnosť kupujúcim a aj predávajúcim. Umožňuje prevádzať anonymné online transakcie, bez ktorých by boli užívatelia ľahko vystopovateľní. Tieto štatistiky boli vytvárané z 12 náhodne vybraných stránok nachádzajúcich sa na temnom webe.

Najčastejšie podporovanou kryptomenou na temnom webe je decentralizovaná kryptomena s názvom Bitcoin. Táto mena je využívaná až na 11 stránkach z 12 a stala sa populárna práve tým, že je navrhnutá, aby nikto nemohol ovplyvňovať, falšovať túto menu, zabavovať účty a ani nijako ovládať peňažné toky, čo umožňuje zachovanie anonymity.

Ďalšou, avšak už menej podporovanou kryptomenou, je Monero. Táto mena je využívaná v 7 z 12 vybraných služieb a stala sa známou vďaka tomu, že ponúka väčšiu anonymitu ako Bitcoin.

Zvyšné kryptomeny ako Ethereum, Bitcoin Cash a LiteCoin boli menej používané pri vybraných službách nachádzajúcich sa na temnom webe.



Obrázok 9 – Najvyužívanejšie kryptomeny na temnom webe [34]

3.8 Súhrn štatistík

Mojím pôvodným predpokladom bolo, že majoritné využívanie temného webu je za účelom predaja a nákupu narkotík a iného ilegálneho tovaru, avšak konečný výsledok štatistík vyvrátil môj predpoklad a ukázalo sa, že najpoužívanejšou službou je bohužiaľ obťažovanie detí.

4 ETICKÝ PRIESKUM TEMNÉHO WEBU

Samotný prístup k temnému webu je jednoduchý, je však potrebné dbať na ochranu svojich osobných informácií a identity, teda zaručiť svoju anonymitu a bezpečnosť proti hackerom a rôznym iným nástrahám na temnom webe. Pri prezeraní stránok s nelegálnou činnosťou je veľmi dôležité zostať anonymným. Ak pristupujete k temnému webu pomocou Tor prehliadača a VPN softvéru, nikto vás nemôže sledovať a nikto nevie vašu polohu. Dôvodom je, že oba programy vytvárajú spoločne dve vrstvy ochrany vašej identity. Tor skrýva celú vašu komunikáciu na temnom webe pomocou Tor smerovania a VPN maskuje vašu IP adresu náhradou adresy pochádzajúcej z inej krajiny, čo dokonale pokrýva vašu bezpečnosť pred útokmi hackerov.

Pre zaručenie väčšej úrovne bezpečnosti som použil VPN s názvom „Hotspot Shield“, ktorý je dostupný z webovej stránky „https://www.hotspotshield.com“. Po stiahnutí tohto programu nasleduje jednoduchá inštalácia, po ktorej je možné program použiť. Pomocou VPN budú všetky vaše aktivity skryté od poskytovateľov internetových služieb a vládnych agentúr, pretože všetky aktivity budú šifrované. Nikto nebude vedieť, že používate Tor a už vôbec nie vašu aktivitu na temnom webe.

Nasledujúcim krokom, pre pripojenie k temnému webu, je použitie jedného zo softvérov, ktorý zaručuje anonymitu a umožňuje prístup k temnému webu. Ako bolo spomenuté v prvom bode tejto práce, temný web nie je prístupný z obyčajných prehliadačov ako je Google Chrome, Mozilla Firefox a podobné tradičné prehliadače, pretože stránky temného webu nie sú indexované týmito prehliadačmi. Existuje niekoľko rôznych softvérov, ktoré umožňujú prístup k temnému webu. Najznámejšie z nich sú Tor, I2P a Freenet. Pre pripojenie k tejto časti webu som zvolil najpoužívanejší softvér s názvom Tor. Jeho získanie je taktiež jednoduché, avšak je dôležité použiť oficiálne stránky Tor. Je voľne prístupný z webovej stránky „https://www.torproject.org/“. Po stiahnutí aplikácie nasleduje jednoduchá inštalácia, po ktorej ste schopní prehliadať stránky temnej časti webu. Pomocou Toru získate prístup k webovým stránkam s doménou „.onion“. Táto aplikácia si vždy po spustení skontroluje aktualizácie a aktualizuje najnovšiu verziu, aby bola čo najbezpečnejšia.

Rád by som však upozornil, že využívanie služieb ponúkaných na stránkach zahrnutých v tejto časti bakalárskej práce sú nelegálne a nijako nepodporujem, neodporúčam a ani nenavádzam ľudí, aby tieto stránky navštevovali. Tento bod slúži ako vzdelávací sprievodca, ktorý poukazuje na služby zahrnuté na temnom webe.

4.1 The Hidden Wiki

The Hidden Wiki slúži ako adresár odkazov na online stránky s doménou „.onion“. Je výborným rozbehovým bodom na prehliadanie temného webu pre nováčikov. Užívatelia sa môžu jednoducho presmerovať pomocou odkazov na rôzne stránky temného webu.

4.1.1 The Hidden Wiki URL adresa

- http://zqktlwi4fecvo6ri.onion

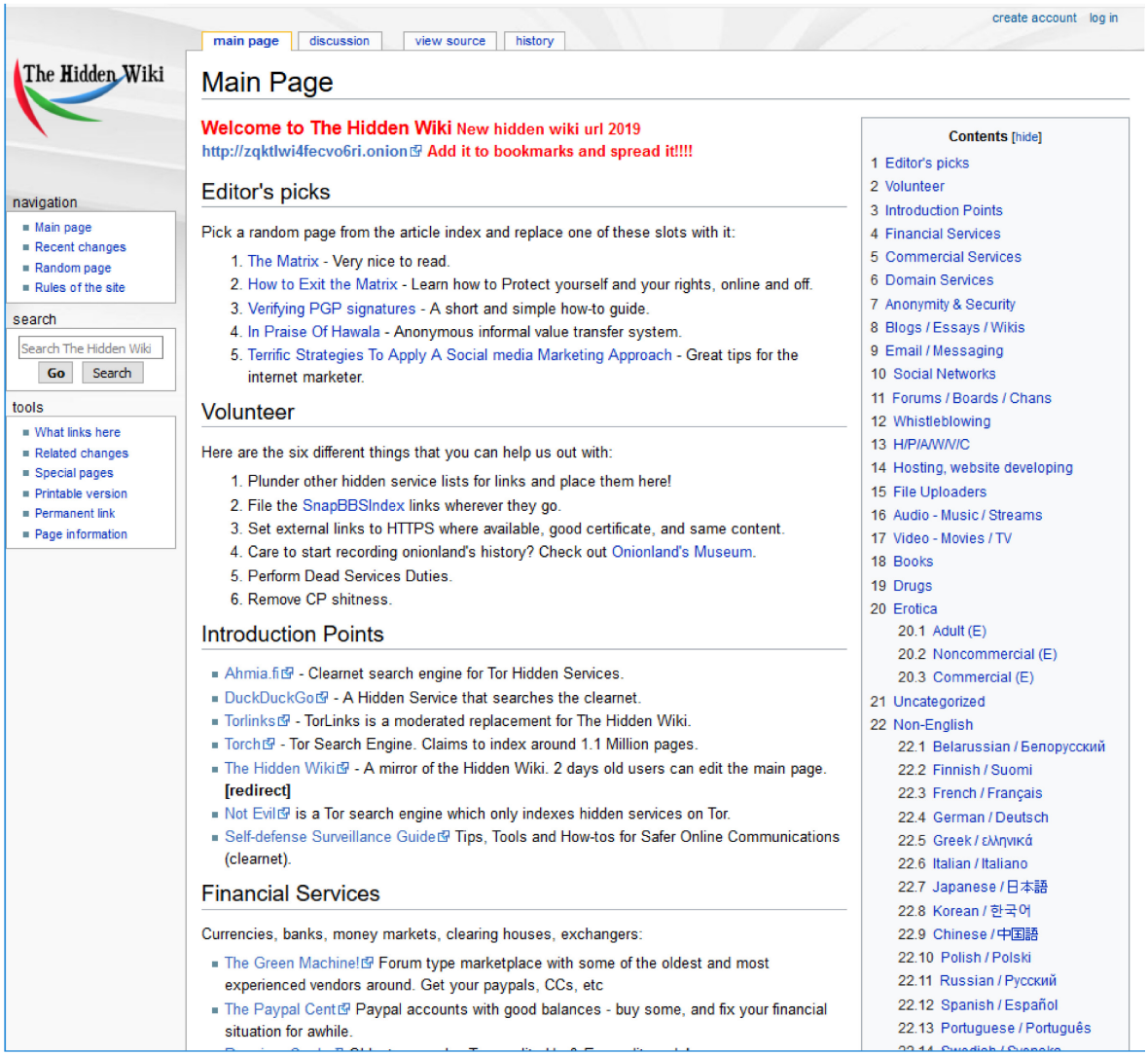
4.1.2 Užívateľské rozhranie

The Hidden Wiki pozostáva z jednoduchého rozhrania, pomocou ktorého môže užívateľ ľahko dosiahnuť to, čo hľadá.

Vo vrchnej časti sa nachádza navigačný panel, ktorý ponúka užívateľom presmerovanie na časti stránky, ako je úvodná strana, história zmien alebo diskusie ohľadom The Hidden Wiki.

Pod navigačným panelom sa nachádza najdôležitejšia časť stránky, ktorá obsahuje názvy kategórií s krátkym popisom a odkazom na príslušné stránky.

Na pravej strane je zahrnutý zoznam kategórií, ktorý slúži na navigáciu ku kategóriám obsahujúcich odkazy.



Obrázok 10 – The Hidden Wiki

4.2 Torch

Torch je jeden z najznámejších a najobľúbenejších vyhľadávačov na deep webe. Funguje na princípe Google. Stačí jednoducho zadať dotaz a Torch vám zobrazí výsledky vyhľadávania. Pomocou tohto prehliadača môže užívateľ jednoducho vyhľadávať služby na temnom webe. Avšak veľkou nevýhodou tohto prehliadača je, že mnoho nájdených výsledkov vyhľadávania vás presmeruje na už neaktívne stránky.

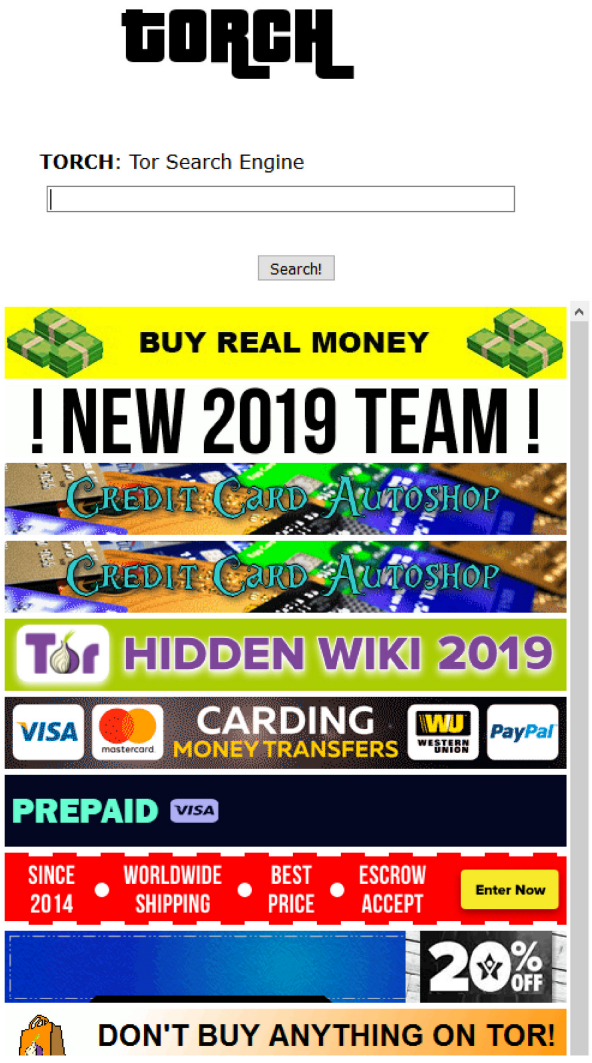
4.2.1 Torch URL adresa

- http://www.xmh57jrzrnw6insl.onion

4.2.2 Užívateľské rozhranie

Torch obsahuje veľmi jednoduché užívateľské rozhranie, je podobné Google. Nachádza sa tu vyhľadávacie pole, ktoré slúži na zadanie kľúčového slova hľadaného výrazu a tlačidlo pre vyhľadanie. Po zadaní dotazu sa zobrazia výsledky hľadania, pomocou ktorých sa jednoducho presmerujete na danú adresu.

Pod tlačidlom vyhľadávania sa nachádza mnoho reklamných odkazov.



Obrázok 11 – Torch

4.3 Wall Street Market

Wall Street Market patrí medzi jeden z najznámejších a najnovších trhov s nelegálnym tovarom na temnom webe. Tento trh obsahuje vyše 27000 položiek, ktoré sú dostupné pre užívateľov. Medzi položkami sa nachádza tovar ako drogy, falzifikáty, šperky, zlato, rôzne služby, softvér a malware, bezpečnosť a hosting, podvody, digitálne tovary, návody a

tutoriály a podobne. V dobe riešenia bakalárskej práce bol Wall Street Market aktívny, no 2.5.2019 bolo toto online trhovisko zrušené medzinárodnou políciou.

4.3.1 Wall Street Market URL adresa

- http://wallstyizjhkrvmj.onion

4.3.2 Registrácia

Pred samotnou registráciou je užívateľ donútený vyplniť captcha kód (Turingov test), ktorý slúži na odlíšenie skutočných užívateľov od počítačov. Po vyplnení tohto kódu nasleduje jednoduchá registrácia, kde je žiadané od užívateľa vyplniť len užívateľské meno, heslo a opäť potvrdenie captchou, že sa jedná o reálneho užívateľa. Po zadaní týchto údajov, získate novo vytvorený účet, pod ktorým sa môžete prihlásiť. Tento účet je však možné použiť len pre nákup. Ak si však chcete vytvoriť účet slúžiaci aj na predaj tovaru, musíte doplniť do svojho účtu aj PGP kľúč.

4.3.3 Užívateľské rozhranie

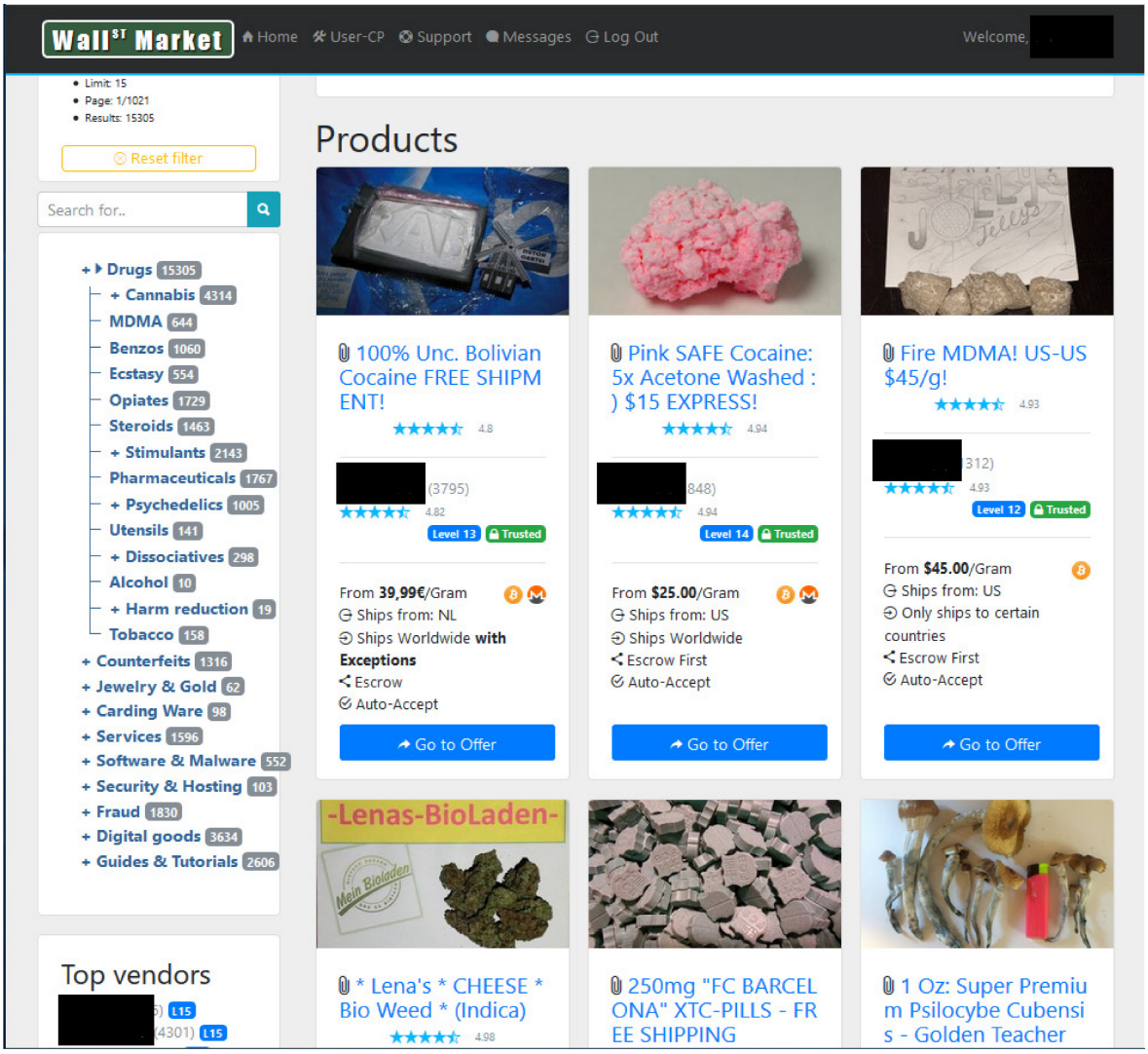
Je vybavený jednoduchým rozhraním so všetkými sekciami a funkciami, ktoré sa dajú ľahko nájsť.

Ak užívateľ potrebuje vykonať zmeny v nastaveniach svojho účtu, stačí kliknúť na názov účtu v pravom hornom rohu stránky alebo kliknúť na odkaz „User-CP“ v hornej časti stránky.

V hornej časti sa nachádza obvyklá ponuka odkazov, ktoré odkazujú na ovládací panel používateľa (User-CP), často kladené otázky, fórum, podporu a odporúčania. Na ľavej strane je krátky zoznam kategórií a v hornej časti je užitočný vyhľadávací panel, kde môžete priamo zúžiť vyhľadávanie na konkrétne produkty v konkrétnych kategóriách bez toho, aby ste museli zadávať kľúčové slová.

Pod kategóriami sa nachádza sekcia s názvom „Top Vendors“, ktorá sa na väčšine populárnych trhovísk na temnom webe nenachádza. Táto sekcia je užitočná hlavne pre nováčikkov na tomto trhu, pretože obsahuje dôveryhodných dodávateľov. To však neznamená, že novší predajcovia sú ignorovaní. Hneď pod touto sekciou sa nachádza ďalšia časť s názvom „Rising Vendors“, ktorá obsahuje novších dodávateľov, ktorí predávajú častejšie a vo vyšších množstvách.

Zvyšok obrazovky zahŕňa stredový panel, kde sa nachádzajú samotné produkty, ktoré vyhľadávate.



Obrázok 12 – Wall Street Market

4.3.4 Produkty

Toto trhovisko obsahuje skoro všetky možné druhy nelegálneho tovaru okrem detskej pornografie a zbraní.

Obsahuje desať hlavných kategórií, ktorými sú:

- Drugs – „Drogy“ – 15304 položiek
- Counterfeits – „Falzifikáty“ – 1316 položiek
- Jewelery & Gold – „Šperky a zlato“ – 62 položiek
- Carding Ware – „Kradnutý tovar“ – 98 položiek

- Services – „Služby“ – 1596 položiek
- Software & Malware – „Softvér a malvér“ – 552 položiek
- Security & Hosting – „Bezpečnosť a hosting„– 103 položiek
- Fraud – „Podvody“ – 1830 položiek
- Digital Goods – „Digitálny tovar“ – 3634 položiek
- Guides & Tutorials – „Príručky a tutoriály“ – 2606 položiek

Dominantnou kategóriou je kategória obsahujúca rôzne druhy drog. Táto kategória obsahuje vyše 15000 produktov, ktoré zahŕňajú viac ako polovicu celkového počtu produktov tohto trhu. Je rozdelená na podkategórie ako marihuana, MDMA, extáza, steroidy a ďalšie rôzne druhy.

Druhou najobľúbenejšou kategóriou je digitálny tovar, ktorý zahŕňa okolo 3600 položiek. Táto kategória je rozdelená na softvér, e-knihy, hry a podobné podkategórie.

Návody a príručky sú tiež jednou z kategórii, ktoré obsahujú dominantnejší počet položiek. V tejto kategórii si môžete objednať návody, ako variť alebo pestovať svoje vlastné drogy, ako sa hacknúť do účtov a rôzne iné návody.

Ďalej sa tu nachádzajú sekcie so šperkami, hostingom, bezpečnosťou ako napríklad VPN, falzifikáty, kradnutý tovar a tak ďalej.

4.3.5 Platba

Typ platby hrá hlavnú rolu o súkromí a anonymite, ako aj vplyvoch celkovej ceny a času potrebného na nákup tovaru, pretože každá mena má svoj vlastný poplatok za transakcie a časové požiadavky. Wall Street Market podporuje dve najčastejšie využívané kryptomeny, ktorými sú Bitcoin alebo Monero.

4.4 Silk Road 3.1

SilkRoad je pravdepodobne najpopulárnejšia stránka na temnom webe. Užívatelia si môžu objednať rôzne druhy drog, e-knihy, údaje k bankovým účtom, kreditné karty a podobný tovar.

4.4.1 Silk Road 3.1 URL adresa

- http://silkroad7rn2puhj.onion

4.4.2 Prístup

Prístup k SilkRoadu je veľmi jednoduchý. Po zadaní captchy, ste okamžite presmerovaní na úvodnú stranu, odkiaľ si môžu užívatelia priamo objednávať tovar. Na rozdiel od Wall Street Marketu nie je nutná žiadna registrácia pred nákupom. Registrácia je plne voliteľná užívateľom a objednávať tak môžete s registráciou a aj bez nej.

4.4.3 Užívateľské rozhranie

Rozhranie SilkRoad 3.1 je úplne odlišné a jedinečné ako väčšina iných tradičných trhovísk.

V hornej časti stránky sa nachádza navigačný panel, ktorý pomáha užívateľom dostať sa na rôzne časti trhu ako je úvodná stránka, registrácia, prihlásenie, fóra a podobné dôležité časti stránky.

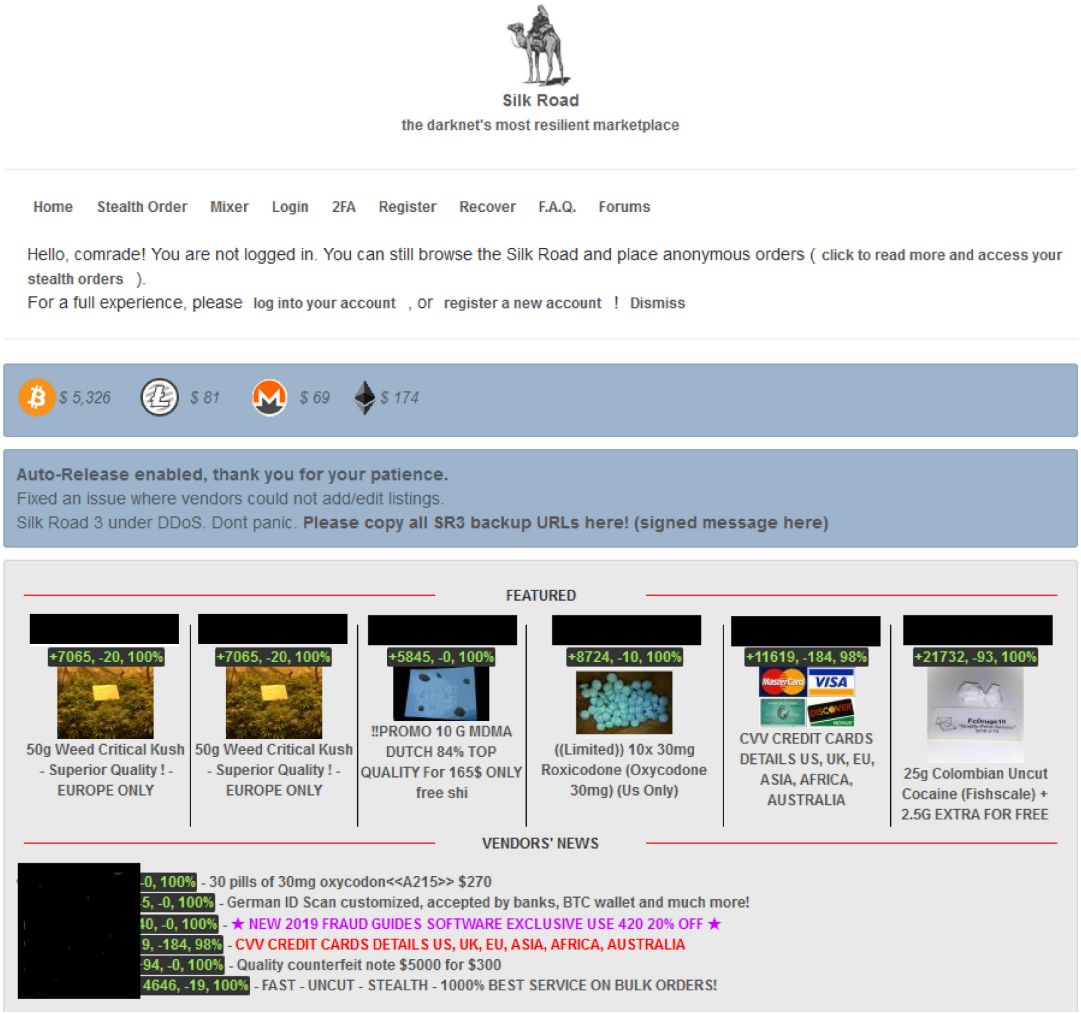
Pod hlavným navigačným panelom sa nachádza informatívna lišta, ktorá zobrazuje aktuálne ceny kryptomien využívaných na tomto trhovisku.

Ďalej sa tu nachádza časť pozostávajúca z vybraných predajcov s krátkymi popismi ich produktov spolu s počtom predajov a ich negatívnymi alebo pozitívnymi recenziami.

Dôležitou časťou trhoviska je vyhľadávací panel, v ktorom si užívateľ môže zvoliť filtráciu tovaru pomocou kľúčových slov, odkiaľ bude tovar dodávaný, služby Escrow a možnosti zoradenia.

Na pravej strane sa nachádza krátky zoznam kategórií, ktoré pomáhajú užívateľovi zúžiť hľadanie produktov.

Každý z produktov uvádza zoznam najdôležitejších informácii o produkte, vrátane podpory Escrow , ceny, akceptovaných mien a základných informácii o predávajúcom.



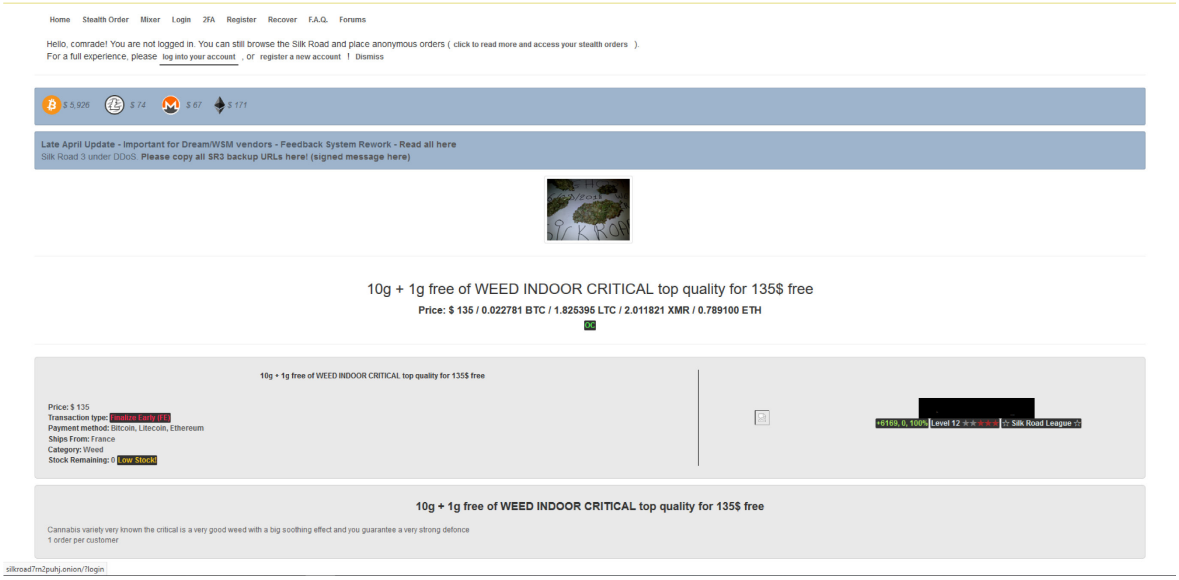
Obrázok 13 – Silk Road 3.1

4.4.4 Produkty

Presný počet produktov na SilkRoad 3.1 je nejasný, pretože nie je jasne uvedený počet a manuálne spočítanie je nereálne vzhľadom k tomu, že každá kategória obsahuje od 20 do 50 strán s produktami.

Primárnymi produktami tohto trhoviska sú drogy ako napríklad marihuana, stimulanty, opioidy a rôzne iné druhy drog. Každá táto kategória taktiež obsahuje svoje vlastné podkategórie, čo umožňuje jednoduchšie vyhľadávanie presných produktov.

Nachádza sa tu aj tovar pod kategóriami „Digital“ a „Physical“. Digitálne produkty zahŕňajú CC, VCC, rôzne účty atď. Fyzické produkty zase zahŕňajú falzifikáty a kradnutý tovar.



Obrázok 14 – Popis produktu na Silk Road 3.1

4.4.5 Platba

SilkRoad 3.1 podporuje jednu z najznámejších kryptomien s názvom Bitcoin. Táto mena má však menšie nevýhody, ako je vyšší transakčný poplatok a mierne dlhšie transakčné časy. Kvôli tomu je možné platiť aj menami ako sú Monero, Litecoin alebo Ethereum. Voľba meny však závisí od dodávateľa.

4.5 Red Room

Red Room je skrytá online služba, kde sa môže užívateľ zúčastniť interaktívneho mučenia alebo vraždy. Vo všeobecnosti obsahuje explicitné obťažovanie a mučenie vysielané online zločincom, ktorý tieto činy uskutočňuje. Užívateľ si zaplatí za sledovanie alebo si môže vyžiadať mučenie osôb so zaviazanými očami. Zločinec však vykoná len tú žiadosť, ktorá je zaplatená. Podľa množstva peňazí, ktoré prevedú zločincovi, začne mučenie podľa inštrukcií.

4.5.1 Red Room URL adresa

- http://redroomfing27toi.onion/

Obrázok 15 – Úvodná strana Red Room

4.5.2 Obsah

Red Room môže byť považovaný za video portál, takže môžete očakávať, že všetky druhy videí, ktoré sa tu nachádzajú súvisia s určitým druhom spôsobovania bolesti iným osobám. Na hlavnej stránke sa zobrazujú rôzne balíčky, z ktorých si vyberiete služby, ktoré žiadate z danej stránky.

Detská pornografia

Väčšina normálne zmýšľajúcich ľudí si ani len nechce predstaviť niečo podobné tomuto druhu ubližovania. No ako ste si mohli všimnúť zo štatistík uvedených v treťom bode bakalárskej práce, až 83% návštevnosti temného webu, smeruje práve na služby ponúkajúce detskú pornografiu alebo všeobecne ubližovanie deťom. Práve na týchto stránkach si ľudia môžu platiť za sledovanie zneužívania detí.

Táto kategória môže obsahovať:

- Mučenie – Fyzicky ubližovať a „užívať“ si sadistické pôžitky z ich bolesti
- Znásilnenie – Sexuálne zneužitie dieťaťa bez ohľadu na jeho pohlavie
- Nečinnosť – Je to špeciálny druh pornografie, kde sa s dieťaťom nič nerobí, obeť je len zviazaná na posteli alebo o stoličku bez oblečenia a všetky kamery smerujú práve na obeť

Vražda

Divák môže zaplatiť za vraždu náhodnej obete alebo divákom užívateľom určenej osoby. Vrah prakticky vykonáva rozkazy od zákazníka. Môžete si vybrať z viacerých kategórií ako je pomalá smrť, podrezanie alebo iné metódy vraždy.

Znásilnenie

Znásilnenie či už mužov alebo žien je tiež jednou zo „zábav“ pre návštevníkov týchto stránok. Opäť platí, že znásilnenie má aj rôzne kategórie, čokoľvek čo si dokážete predstaviť, ako spôsobiť sexuálnu bolesť osobe je vraj možné a dostupné na stránke Red Room.

Všeobecné mučenie

V tejto kategórií existujú videá všeobecného mučenia. Ide napríklad o odtrhnutie nechtov, krájanie jazyka, vyberanie očí, v podstate všetko, čo si dokážete predstaviť pod pojmom „mimoriadne bolestivé“.

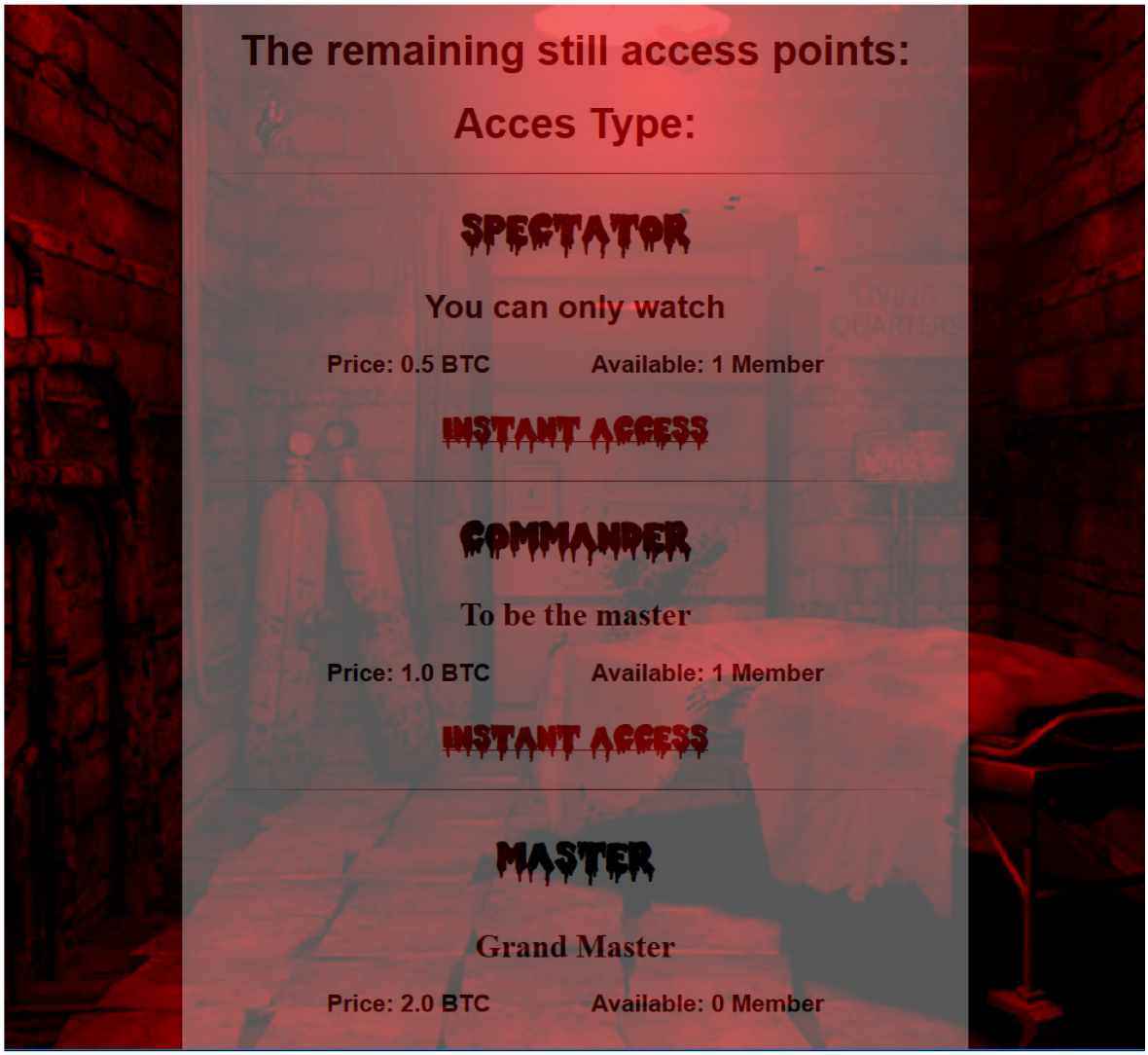
Komunikácia

Niektoré Red Roomy ponúkajú možnosť „chatu“. V prípade, že sa nezaujímate o videá, môžete sa tam pripojiť k „podobne zmýšľajúcim“ ľuďom bez toho, aby ste odhalili svoju identitu. Slúži ako sociálna sieť pre ľudí, ktorí patria do rôznych „sadistických“ kategórií.

Existujú rôzne balíky, ktoré oddeľujú „divákov“ od „chatujúcich“ a tak sa cenové balíky líšia aj pre rôzne použitia.

Platba

Red Rooms akceptujú ako spôsob platby len Bitcoin.



Obrázok 16 – Red Room

4.6 Dream Market

Dream Market je jeden z najväčších trhovísk na temnom webe. Bol založený v roku 2013. Je známy hlavne svojou bezpečnosťou a spoľahlivosťou. Obsahuje zoznamy produktov a služieb, ktoré sú nezákonné alebo zakázané na ostatných internetových trhoviskách. Patria sem napríklad drogy, príslušenstvo pre drogy, zakázané digitálne produkty, služby hackovania, falšovania, falzifikáty a iné nelegálne produkty. Tento trh bol 30.4.2019 zrušený. Pôvodná adresa Dream Marketu stále obsahuje kategórie s počtom položiek, avšak nie je možné si položky zobraziť. Namiesto položiek je zanechaný odkaz, ktorý poukazuje, že celé trhovisko sa presúva na partnerskú spoločnosť s onion adresou „weroidjak-zxqds2l.onion“. Táto stránka by mala byť veľmi podobná Dream Marketu.

4.6.1 Dream Market URL adresa

- http://4buzlb3uhrjby2sb.onion

4.6.2 Registrácia

Registrácia je pomerne jednoduchá. Do formulára na registráciu nového účtu je nutné vyplniť užívateľské meno, heslo, PIN a CAPTCHA kód na potvrdenie reálneho užívateľa. Po vyplnení formulára a kliknutí na tlačidlo registrácie budete automaticky prihlásení do svojho účtu a presmerovaní na úvodnú stranu Dream Marketu.

4.6.3 Užívateľské rozhranie

Tak ako väčšina trhovísk na temnom webe, aj Dream Market obsahuje jednoduché užívateľské rozhranie, čo uľahčuje užívateľovi vyhľadať produkty.

Vo vrchnej časti sa nachádza navigačný panel, ktorý umožňuje presmerovanie na časti stránky, ako je úvodná strana, správy, údaje o účte a vyhľadávanie služieb pomocou kľúčových slov.

Na ľavej strane sa nachádza krátky zoznam kategórií, ktoré pomáhajú užívateľovi zúžiť hľadanie produktov.

Hlavnou časťou trhoviska je vyhľadávací panel, pomocou ktorého si užívateľ jednoducho filtruje služby. Tento filter vám umožňuje triediť výsledky na základe miesta doručenia, miesta odoslania, služby Escrow, kryptomeny, kategórie a cenového rozpätia. Máte tiež možnosť zobraziť výsledky podľa ceny (najnižšej až najvyššej alebo najvyššej až najnižšej) a obmedziť výsledky iba na tie záznamy, ktoré ste si vyfiltrovali.

Pod vyhľadávacím panelom sa nachádza sekcia s vyfiltrovanými dostupnými službami. Samotné položky obsahujú dôležité informácie, ako je výstižný popis produktu, cenu, názov dodávateľa a podporu služby Escrow.

4.6.4 Produkty

Dream Market obsahuje 5 hlavných kategórií, ktorými sú:

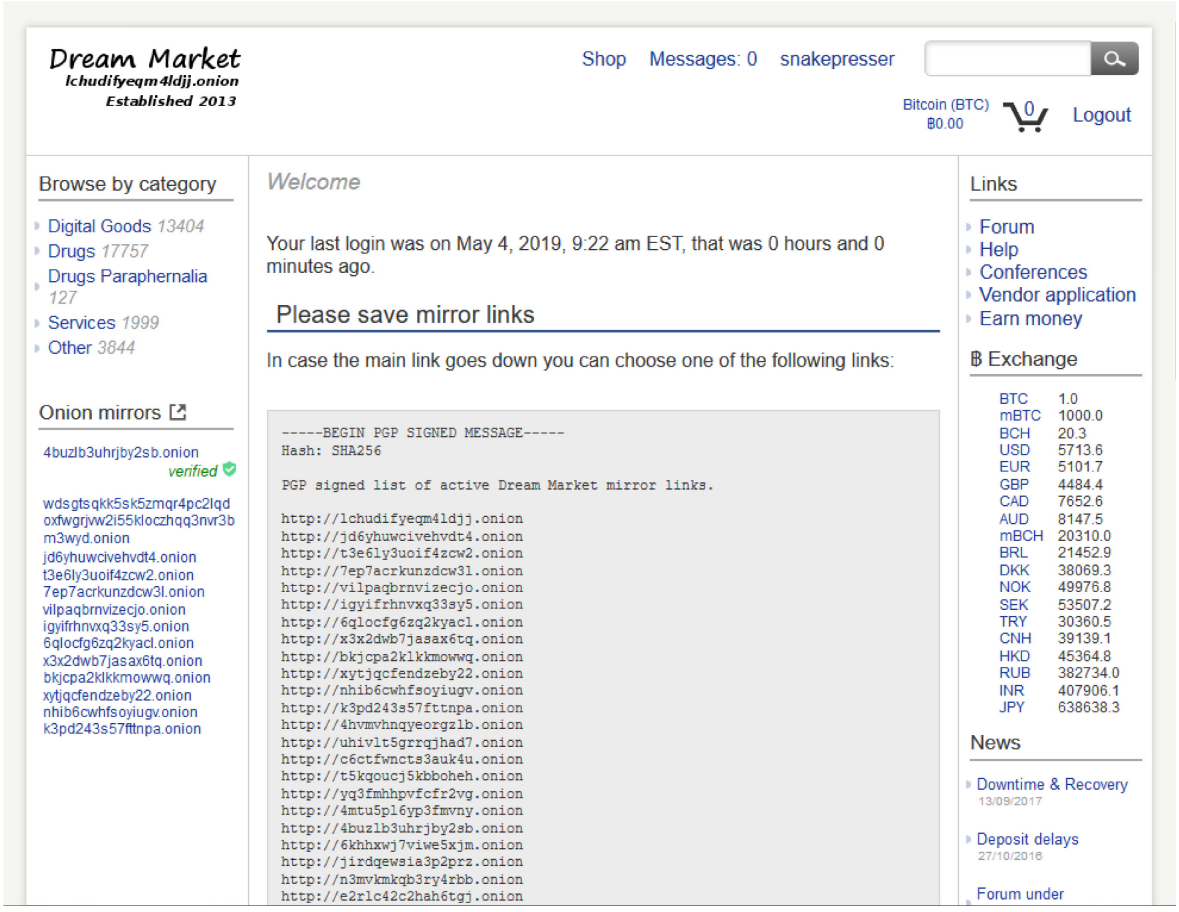
- Dogital goods – „Digitálny tovar“ – 13404 položiek
- Drugs – „Drogy“ – 17757 položiek
- Drugs Paraphemalia – „Drogové príslušenstvo“ – 127 položiek
- Services – „Služby“ – 1999 položiek

- Other – „Ostatné“ – 3844 položiek

V kategórií digitálneho tovaru môžete nájsť recepty na prípravu drog, e-knihy, erotický obsah, softvéry a rôzne iné položky. Kategória Drogy neobsahuje rozsiahly zoznam podkategórií, ale najobľúbenejšie položky sú zahrnuté ako barbituráty, benzíny, marihuana, disociácie, extáza, opioidy, lieky na predpis, psychedeliká, RC, steroidy, stimulanty ako aj produkty na chudnutie. Kategória drogového príslušenstva neobsahuje podkategórie, ale obsahuje takmer všetky požadované položky. Na druhej strane, kategória služby predstavuje nasledujúce podkategórie: hackovanie, pasy, falošné peniaze. Nakoniec kategória ostatné obsahuje falzifikáty, elektroniku, šperky, laboratórne potreby, obranné produkty a informácie.

4.6.5 Platba

Dream Market podporuje ako možnosť platby kryptomeny Bitcoin a Bitcoin Cash.



Obrázok 17 – Dream Market

4.7 Tochka

Tochka je online trhovisko ruského pôvodu, ktoré vzniklo v januári 2015. Umožňuje rýchly predaj položiek na tmavom webe bez toho, aby sa predávajúci a kupujúci museli stretnúť alebo komunikovať. Trh Tochka môžete nájsť aj pod názvom T.chka, kde bodka sa vyslovuje ako „o“.

4.7.1 Tochka URL adresa

- http://tochka3evlj3sxdv.onion

4.7.2 Registrácia

Registrácia účtu je rýchly a jednoduchý proces. Registračný formulár vás požiada, aby ste vyplnili užívateľské meno a heslo a uviedli, či chcete účet kupujúceho alebo dodávateľa. Po zadaní CAPTCHA kódu môžete pokračovať kliknutím na tlačidlo Register a vytvoriť svoj účet. Po dokončení registrácie budete automaticky prihlásení do svojho účtu.

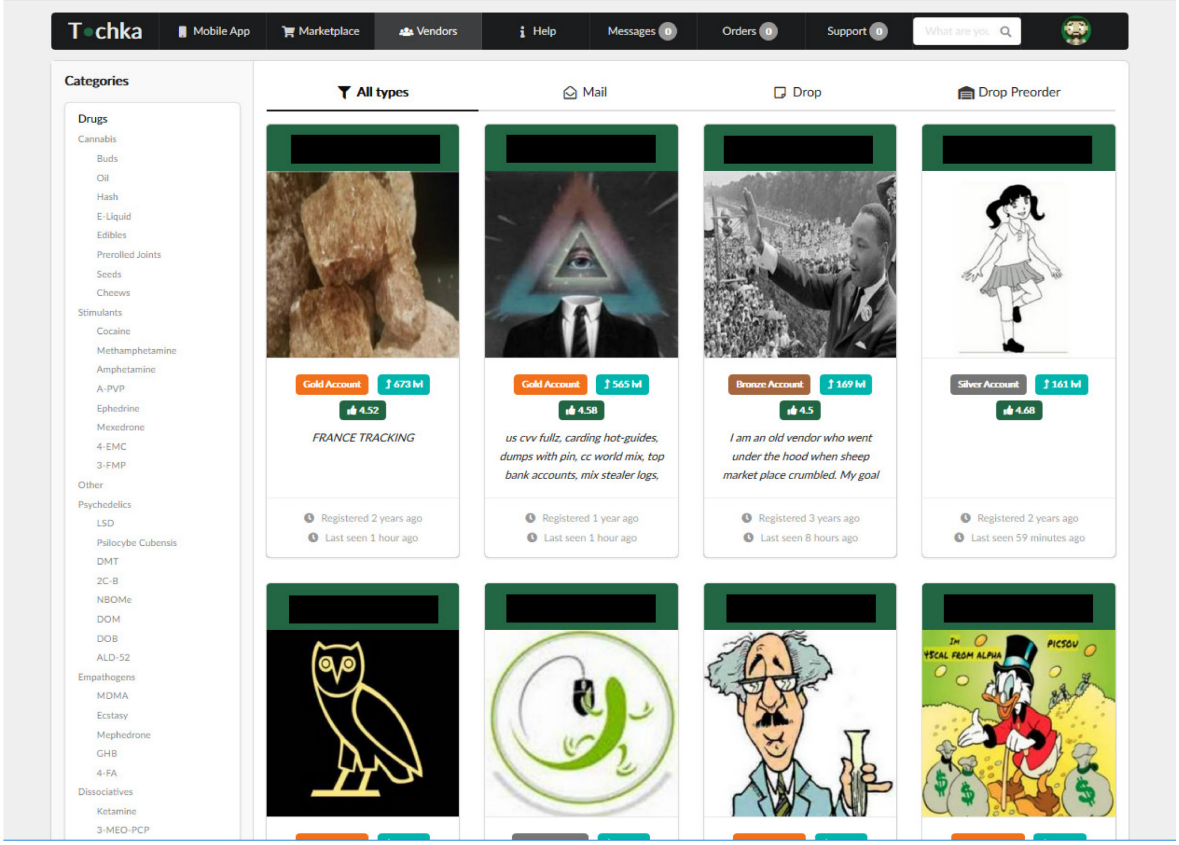
4.7.3 Užívateľské rozhranie

Tochka oproti ostatným trhoviskám obsahuje pomerne moderné užívateľské rozhranie.

Vo vrchnej časti sa nachádza navigačný panel, ktorý umožňuje stiahnutie aplikácie Tochka alebo presmerovanie na časti stránky ako je úvodná strana zobrazujúca produkty, zoznam dodávateľov s dôležitými informáciami ako je užívateľské meno a hodnotenie. Ďalej tu môžete nájsť položku s názvom „Help“, kde môžete získať dôležité informácie ako napríklad: ako nakupovať, ako predávať, informácie o leveloch dodávateľov a tak ďalej. Môžete si taktiež pozrieť doručené správy, informácie o objednávke alebo o svojom účte.

Na ľavej strane sa nachádza navigácia s kategóriami produktov, čo umožňuje jednoduché vyhľadanie produktov. Môžete si zvoliť odkiaľ chcete, aby bol tovar dodávaný alebo podľa akého kritéria by mal byť zoradený.

Dôležitou časťou rozhrania je stredný panel, v ktorom sa nachádzajú vyfiltrované produkty. Každá položka obsahuje hlavné informácie o produkte, ako je popis produktu, názov dodávateľa, hodnotenie dodávateľa a cenu.



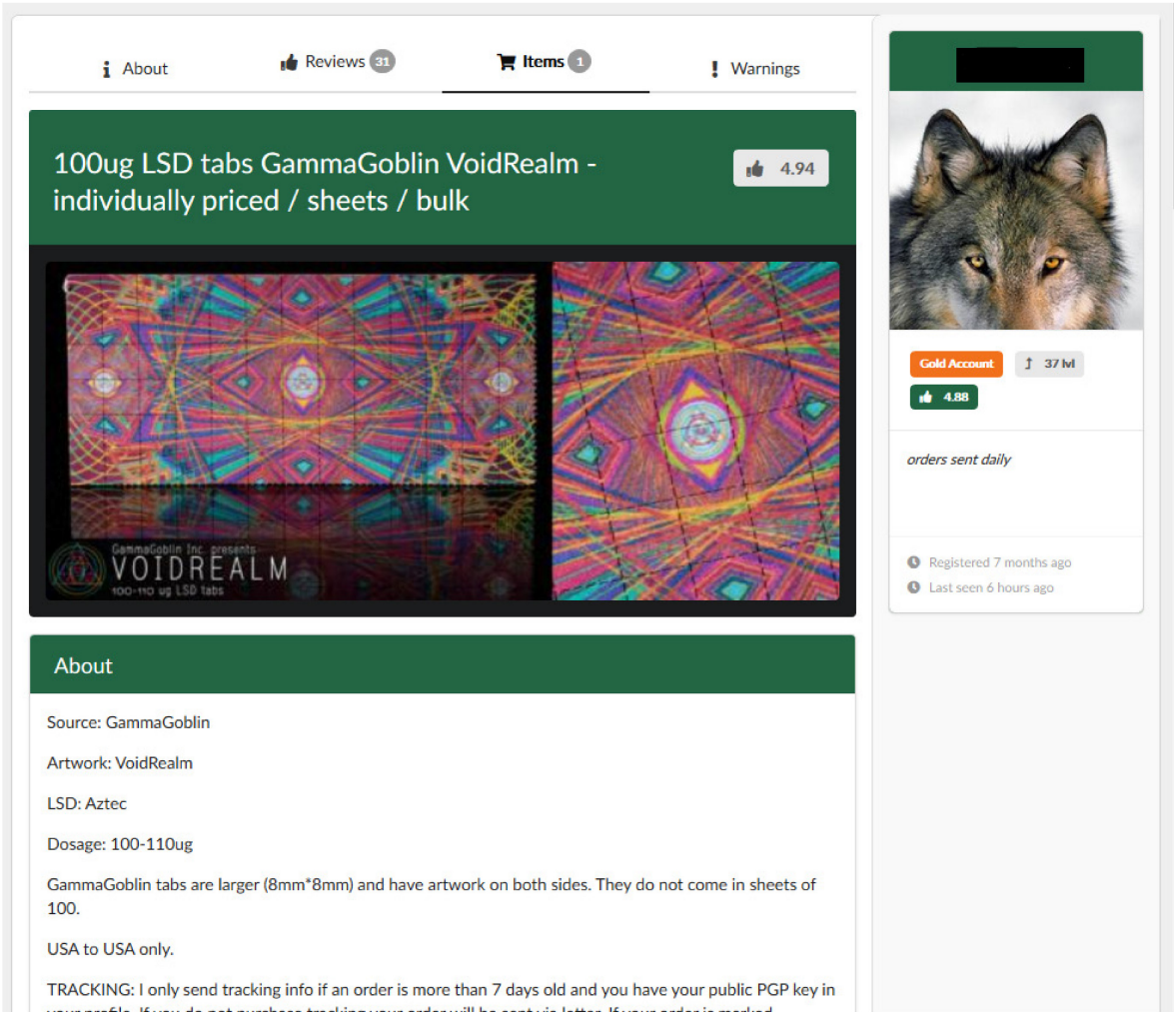
Obrázok 18 – Tochka

4.7.4 Produkty

Produkty sú rozdelené do troch hlavných kategórií:

- Drugs – „Drogy“ – 3196 položiek
- Prescription – „Lieky na predpis“ – 1324 položiek
- Steroids – „Steroidy“ – 173 položiek

Primárnou kategóriou sú Drogy. Táto kategória obsahuje rozsiahly počet podkategórií ako marihuana, stimulanty (kokaín, metamfetamín),), psychedeliká (LSD,DMT), empatogény (MDMA, extáza), disociatíva (ketamín), opiáty, tabak alebo poppery. V kategórií lieky na predpis môžete nájsť položky ako Xanax, opoidy alebo viagru a produkty podobného typu. V poslednej kategórií sa nachádzajú rôzne druhy steroidov ako napríklad testosteron, trenbolon, clenbuterol a rôzne iné dopingové produkty.



Obrázok 19 – Popis produktu na Tochke

4.8 Hacker's Bay

HackerBay je skupina pozostávajúca z vysoko kvalifikovaných hackerov v rôznych oblastiach, schopných obísť niekoľko kybernetických pravidiel a protokolov, aby sa dosiahol očakávaný výsledok akejkoľvek pridelenej úlohy. Táto skupina hackerov ponúkajú služby ako hacknutie sa na webovú stránku, hacknutie počítača, zmenenie hesla, DDoS útok na servery, hacknutie e-mailu a rôzne iné služby týkajúce sa hackovania.

4.8.1 Hacker's Bay URL adresa

- http://huomyxhpzx6mw74e6jfxtj5kmxov6wdmc62ylk6oc7feht5gntuawaqd.onion

4.8.2 Užívateľské rozhranie

HackerBay obsahuje veľmi jednoduché rozhranie. Jedná sa o jednoduchú stránku s navigačným panelom umiestneným vo vrchnej časti stránky, pomocou ktorej sa môžete presmerovať na úvodnú stranu alebo na kontaktné údaje hackerov.

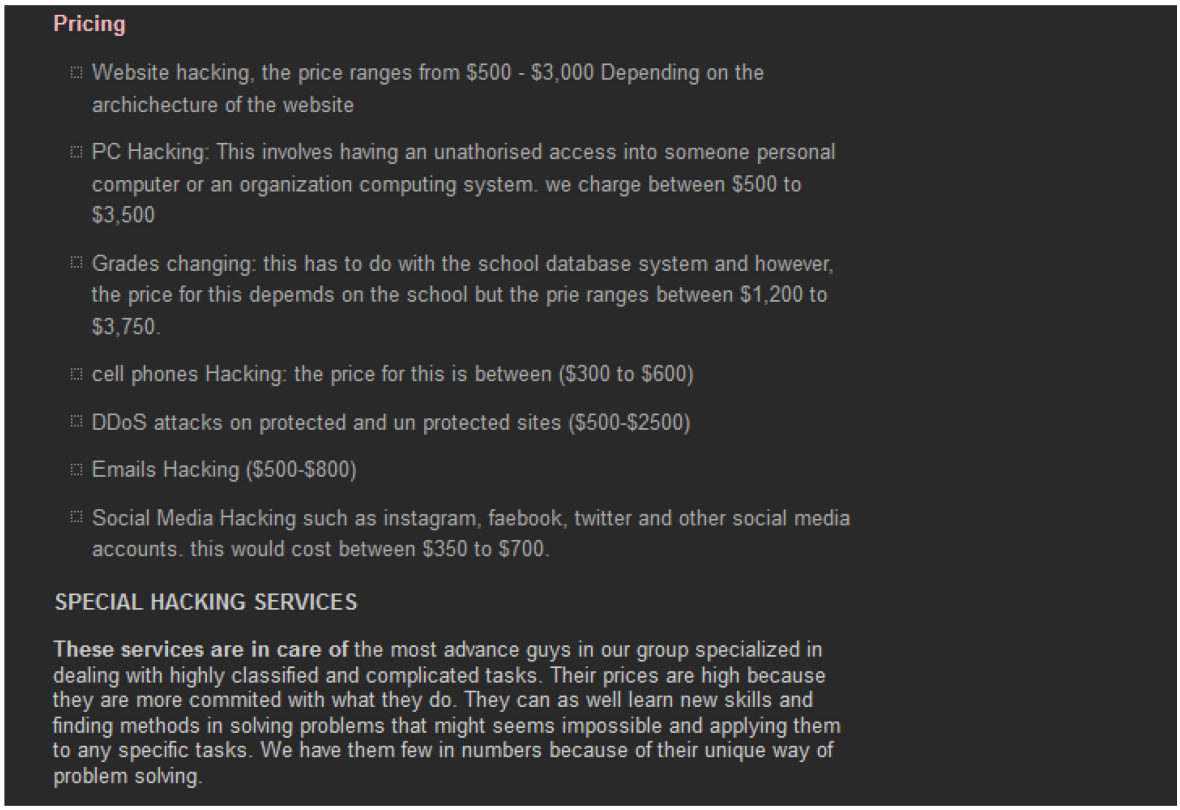
Úvodná strana obsahuje popis skupiny ponúkajúcej dané služby a ich technické zručnosti. Najdôležitejšou časťou stránky je odsek popisujúci služby, ktoré ponúka a ich cenník.

Obrázok 20 – Hacker's Bay

4.8.3 Služby

- Hacknutie webovej stránky – od 500$ do 3000$, záleží od architektúry stránky
- Hacknutie počítača – od 500$ do 3500$, zahŕňa neautorizovaný prístup do niekoho osobného počítača
- Zmenenie stupňa titulu - od 1200$ do 3750$
- Hacknutie mobilného telefónu - od 300$ do 600$
- DDoS útok na chránené a nechránené stránky - od 500$ do 2500$
- Hacknutie e-mailu - od 500$ do 800$

- Hacknutie sociálnych sietí - od 350$ do 700$, zahŕňa Facebook, Instagram, Twitter a iné účty



Obrázok 21 – Služby ponúkané na Hacker's Bay

5 SÚHRN

Táto práca slúži pre zber informácií za účelom prevencie, a preto by som chcel poukázať na to, že prítomnosť nelegálnej aktivity spochybňuje „charakter“ niektorých užívateľov temného webu. Z toho dôvodu je dôležité dbať na ochranu osobných informácií a identity. To je možné dosiahnuť pomocou používania VPN a špecializovaného softvéru ako napríklad Tor. Do problémov na temnom webe sa dá dostať už len jednoduchým prezeraním. Nachádzajú sa tu ľudia a veci, ktorým by ste sa mali snažiť vyhnúť:

- Vírusy – niektoré webové stránky môžu infikovať vaše zariadenie vírusmi a existuje veľa rôznych vírusov, na ktoré si treba dať pozor. Je dôležité sa vyhýbať sťahovaniu zo stránok, ktorým nedôverujete.
- Hackeri – môžete tu nájsť mnoho fór hackerov a stránok, na ktorých si môžete objednať ich služby, práve preto sa tu vyskytuje možnosť hacknutia aj vášho zariadenia
- Zneužitie webkamery – webové stránky nachádzajúce sa na temnom webe sa môžu pokúsiť dostať sa do vášho zariadenia pomocou nástroja zvaného „RAT“. To môže viesť k zneužitiu vašej webkamery a umožní im vidieť, čo sa deje za vaším zariadením, čiže odhaliť aj vašu identitu. Preto je vhodné si pred prezeraním temného webu prekryť webkameru.

Temný web pracuje s vysokým stupňom anonymity. Je hostiteľom tak ako pre neškodné aktivity a obsah, tak aj pre nelegálny obsah. Pre príklad, temný web môže obsahovať stránky, ktoré môžu byť niečo na spôsob knižného klubu, ktoré dodávajú eKnihám profesionálnejšiu podobu. Avšak temný web je viac známy temným obsahom – čo znamená ilegálny a niekedy znepokojujúci obsah. Môžete tu naraziť napríklad na:

- Ukradnuté informácie a tovar – od prístupových údajov až po čísla bankových účtov
- Nelegálne látky – drogy, lieky na predpis, toxické chemikálie, steroidy
- Nebezpečné a znepokojujúce služby – vrahovia na objednávku, detská pornografia, falšovaný tovar, zbrane, hackeri

Je teda veľmi dôležité zvážiť niekoľko bezpečnostných otázok:

- Trestný prvok – nachádzajú sa tu stránky prevádzkované zločincami. Okrem predaja nelegálneho tovaru, či služieb sa môžu snažiť získať vaše osobné údaje alebo súbory z vášho zariadenia

- Porušenie zákona – objednávanie tovaru a služieb, ktoré sú vo väčšine prípadoch nelegálne. Ako sú napríklad drogy, zbrane atď.
- Podozrivé odkazy – kliknutie na odkaz alebo prevzatie súboru môže infikovať vaše zariadenie škodlivými vírusmi
- Orgány činné v trestnom konaní - úradníci činní v trestnom konaní pôsobia na temnom webe, aby chytili osoby zapojené do trestnej činnosti

Veľmi nečakaným a nemilým prekvapením je, že až 83% návštevnosti temného webu je so zameraním na služby obťažovania detí. Z toho dôvodu poukazujem na služby, ktoré sa týkajú tejto problematiky a podľa môjho názoru by bolo vhodné zamerať sa na zrušenie práve stránok s obsahom podobným, ako na stránkach Red Room, poprípade snažiť sa vyhľadať návštevníkov a ľudí vykonávajúcich tieto služby, pretože každá jedna činnosť, ktorú tieto služby ponúkajú, je podľa môjho názoru priam neľudská a zrušenie tejto činnosti je nutné pre zabránenie ubližovania deťom a ostatným osobám.

5.1 Výhody a nevýhody temného webu

Aj keď je temný web spájaný prevažne s nelegálnou činnosťou, obsahuje aj niekoľko výhod ako napríklad:

- Anonymita pre ľudí, ktorí chcú súkromne prezerať Internet
- Je to miesto, kde majú ľudia prístup k webovým stránkam, ktoré môžu byť obmedzené ich poskytovateľom internetových služieb z dôvodu ich umiestnenia
- Poskytuje prístup ľuďom v krajinách, ktoré majú prísne zákony o cenzúre

Samozrejme však nemôže existovať dobré bez zlého, najmä ak ide o temný web.

Nevýhody:

- Je ťažké regulovať temný web, takže užívatelia sú nútení komunikovať s ľuďmi na vlastné riziko
- Obsah trhovísk na temnom webe tvorí zväčša nelegálny tovar
- Je jednoduché obísť autority na temnom webe

ZÁVER

Cieľom mojej práce bola etická analýza časti Internetu nazývaná temný web. Jedná sa o časť Internetu, ktorá nie je štandardnými vyhľadávačmi indexovaná a tým pádom je pre väčšinu užívateľov veľká neznáma. Typickou črtou pre túto časť Internetu je taktiež jej neprístupnosť. Je totiž nutné využitie špeciálneho softvéru pre prehliadanie stránok, ktoré sú jeho súčasťou. Prehliadanie samotné nie je napriek všeobecnej mienke ilegálnou činnosťou, avšak využívanie služieb je trestné. Hlavnou úlohou bolo teda demistifikovať túto, z veľkej časti neprebádanú, časť Internetu, poskytnúť v rámci hraníc etiky všeobecný prehľad o jej službách, typoch stránok, na ktoré môže užívateľ naraziť počas prehliadania a v neposlednom rade upozorniť na možné riziká a podvody, ktorým by sa mali užívatelia vyvarovať. V žiadnom prípade teda táto práca neslúži k propagácii a nabádaniu na ilegálnu činnosť, čo by som obzvlášť rád zdôraznil.

Rád by som podotkol, že v čase riešenia bakalárskej práce, odkaz [26] fungoval, no momentálne je nedostupný/zrušený.

Pre správne pochopenie podstaty temného webu bolo nutné sa pozrieť do jeho počiatkov a myšlienky, vďaka ktorej vznikol. Pre tento účel som popísal jednotlivé vrstvy Internetu a špeciálne sa zameral na detailný popis temného webu a jeho histórie.

V počiatkoch svojej analýzy temného webu som sa zameral na bezpečnostnú stránku. Zozbieral som informácie o rôznych typoch softvérov, vďaka ktorým som získal prístup na stránky temného webu. Najznámejšími nástrojmi pre prehliadanie sú Tor, I2P a Freenet. Vykonal som porovnanie týchto nástrojov a pre praktickú časť som zvolil nástroj Tor, najmä kvôli jeho rozsiahlej komunite. Všeobecne sa odporúča, v rámci bezpečnosti proti útokom hackerov, maskovať svoju identitu pomocou VPN služby. Pre účely tejto práce som využil službu Hotspot Shield.

Keďže stránky temného webu nie sú štandardne indexované, nie je možné ich vyhľadávať pomocou tradičných vyhľadávačov ako Google, Yahoo atď. Existujú však alternatívy špecifické pre temný web ako je Torch. Nie je to však spoľahlivý nástroj, pretože väčšina stránok, ktoré som sa snažil navštíviť pomocou tohto vyhľadávača, bolo už zrušených alebo blokovaných. Najlepšou cestou teda je poznať konkrétne adresy stránok pre typ služby, ktorú užívateľ hľadá. V rámci tohto prehliadania som bol schopný zozbierať dáta o približnom počte rôznych služieb, medzi ktoré patria najmä online trhoviská SilkRoad 3.1, Wall Street Market a Dream Market poskytujúce rôzny nelegálny tovar ako sú drogy, falzifikáty a

kradnutý tovar. Bohužiaľ neoddeliteľnou súčasťou temného webu a jeho služieb sú aj takzvané „Red Room“, ktoré za poplatok umožňujú sledovanie živého videa zobrazujúce rôzne typy ubližovania osobám pre „potešenie“ diváka. Určité zdroje tvrdia, že značná časť týchto videí nie je pravá. Treťou, často využívanou službou, spomenutou v mojej práci, je Hacker’s Bay, ktorá poskytuje služby ako hacknutie webových stránok alebo zariadení užívateľov.

V mojej práci som teda popísal históriu, rôzne spôsoby pripojenia sa na túto sieť, predložil doposiaľ dostupné štatistické výsledky a zhrnul ich do prehľadného celku, ktorý informuje čitateľa o nástrahách a bezpečnosti temného webu a vykonal prieskum temného webu, z ktorého informácie som spolu s dostupnými informáciami zhrnul. Práca bola vypracovaná bez porušenia zákona.

ZOZNAM POUŽITEJ LITERATÚRY

[1] What is Surface Web, Deep Web and Dark Web? [online]. Apr 9, 2018 [cit. 2019-05-07]. Dostupné z: https://medium.com/@hackersleague/what-is-surface-web-deep-web-and-dark-web-cdbaf71b30d5

[2] The Dark Web: A Seemingly Endless Market for Drug Trafficking [online]. Apr 9, 2018 [cit. 2019-05-07]. Dostupné z: https://jolt.richmond.edu/2017/10/18/the-dark-web-a-seemingly-endless-market-for-drug-trafficking/#_ftnref1

[3] Dark Web [online]. Oct 18, 2017 [cit. 2019-05-07]. Dostupné z: https://fas.org/sgp/crs/misc/R44101.pdf

[4] The Surface Web [online]. [cit. 2019-05-07]. Dostupné z: https://davidenewmedia.wordpress.com/workingterms/the-surface-web/

[5] What is the Difference Between the Surface Web, the Deep Web, and the Dark Web? [online]. March 10, 2017 [cit. 2019-05-07]. Dostupné z: https://resources.infosecinstitute.com/what-is-the-difference-between-the-surface-web-the-deep-web-and-the-dark-web/#gref

[6] The Deep Web [online]. [cit. 2019-05-07]. Dostupné z: https://davidenewmedia.wordpress.com/workingterms/deep-web/

[7] What's the Dark Web & How to Access It in 3 Easy Steps-2019 [online]. [cit. 2019-05-07]. Dostupné z: https://www.vpnmentor.com/blog/whats-the-dark-web-how-to-access-it-in-3-easy-steps/

[8] GREENBERG, Andy. HACKER LEXICON: WHAT IS THE DARK WEB? [online]. 11.19.14 [cit. 2019-05-07]. Dostupné z: https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/

[9] What is the difference between the dark web and the deep web? [online]. [cit. 2019-05-07]. Dostupné z: https://www.quora.com/What-is-the-difference-between-the-dark-web-and-the-deep-web

[10] Browsing the Dark Web [online]. [cit. 2019-05-07]. Dostupné z: https://davidenewmedia.wordpress.com/accessing-the-dark-web/browsing-the-dark-web/

[11] The "Deep Web" is Not All Dark [online]. [cit. 2019-05-07]. Dostupné z: https://www.deepwebtech.com/deepweb-not-darkweb/

[12] Ethereum (VŠETKO, ČO CHCETE VEDIEŤ) [online]. 28. mája 2018 [cit. 2019-05-07]. Dostupné z: https://www.alza.sk/ethereum?layoutAutoChange=1

[13] What is Monero (XMR)? [online]. [cit. 2019-05-07]. Dostupné z: https://ww.getmonero.org/get-started/what-is-monero/

[14] Dark Web History: Where Did It Come From? [online]. December 23, 2018 [cit. 2019-05-07]. Dostupné z: https://www.technadu.com/dark-web-history/52017/

[15] BREEDING, Jordan. The Origin And History Of The Dark Web [online]. December 23, 2018 [cit. 2019-05-07]. Dostupné z: https://www.ranker.com/list/history-of-the-dark-web/jordan-breeding

[16] THE DARK WEB & DEEP WEB: HOW TO ACCESS THE HIDDEN INTERNET TODAY [online]. February 27, 2019 [cit. 2019-05-07]. Dostupné z: https://digital.com/blog/deep-dark-web/

[17] ALBAUGH, Dave. What is Tor? How to use it safely and legally (plus 5 Tor alternatives) [online]. June 11, 2018 [cit. 2019-05-07]. Dostupné z: https://www.comparitech.com/blog/vpn-privacy/ultimate-guide-to-tor/

[18] Comparison of Anonymous Communication Networks-Tor, I2P, Freenet [online]. 07 | July -2017 [cit. 2019-05-07]. Dostupné z: https://www.irjet.net/archives/V4/i7/IRJET-V4I7518.pdf

[19] Tor: Overview [online]. [cit. 2019-05-07]. Dostupné z: https://2019.www.torproject.org/about/overview.html.en?fbclid=IwAR1LoaK4cPKN4XJS0TT_OnNQcbR_5jjJKKohQUV9u8aTkdxQY0YZGAWQChI

[20] HOLDEN, Ed. An Introduction to Tor vs I2P [online]. [cit. 2019-05-07]. Dostupné z: https://www.ivpn.net/privacy-guides/an-introduction-to-tor-vs-i2p

[21] The Invisible Internet Project (I2P) [online]. [cit. 2019-05-07]. Dostupné z: https://geti2p.net/en/about/intro

[22] Freenet [online]. [cit. 2019-05-07]. Dostupné z: https://www.techopedia.com/definition/7314/freenet

[23] Freenet – Another Secure Anonymity Browser [online]. 14 January 2018 [cit. 2019-05-07]. Dostupné z: https://darkwebnews.com/anonymity/freenet-secure-anonymity-browser/

[24] Tor / Onion Routing [online]. [cit. 2019-05-07]. Dostupné z: https://www.i2p.net/en/comparison/tor

[25] GODWIN, Mike. What is Freenet? [online]. [cit. 2019-05-07]. Dostupné z: https://freenetproject.org/pages/about.html

[26] Freenet [online]. [cit. 2019-05-07]. Dostupné z: https://emu.freenetproject.org/pipermail/chat/2009-February/001872.html

[27] Cryptopolitik and the Darknet [online]. 01 Feb 2016 [cit. 2019-05-07]. Dostupné z: https://www.tandfonline.com/doi/pdf/10.1080/00396338.2016.1142085?needAccess=true

[28] Onion Services [online]. [cit. 2019-05-07]. Dostupné z: https://metrics.torproject.org/hidserv-dir-onions-seen.html

[29] Dark Web Traffic Is Most Likely Illicit [online]. [cit. 2019-05-07]. Dostupné z: https://blog.ipswitch.com/monitor-dark-web-traffic-with-whatsup-gold-2018

[30] Users [online]. [cit. 2019-05-07]. Dostupné z: https://metrics.torproject.org/userstats-relay-country.html?start=2018-01-01&end=2019-01-01&country=all&events=off

[31] Study claims more than 80% of 'dark net' traffic is to child abuse sites [online]. [cit. 2019-05-07]. Dostupné z: https://www.theguardian.com/technology/2014/dec/31/dark-web-traffic-child-abuse-sites

[32] Dark Net Traffic Study Provides Disturbing Results [online]. 26 February 2018 [cit. 2019-05-07]. Dostupné z: https://darkwebnews.com/news/dark-net-traffic-study-provides-disturbing-results/

[33] GREENBEG, Andy. OVER 80 PERCENT OF DARK-WEB VISITS RELATE TO PEDOPHILIA, STUDY FINDS [online]. 12.30.14 [cit. 2019-05-07]. Dostupné z: https://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/

[34] The State of Opioid Sales on the Dark Web [online]. June 2018 [cit. 2019-05-07]. Dostupné z: https://safemedsonline.org/wp-content/uploads/2018/06/Opioid-Sales-on-the-Dark-Web-LegitScript-June-2018-Report.pdf

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

ARPANET	Advanced Research Projects Agency Network
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
GUID	Globally Unique Identifier (Unikátny identifikátor)
HTTP	Hypertext Transfer Protocol
I2P	Invisible Internet Project
IP	Internet Protocol (Logický číselný identifikátor daného uzla (najčastejšie počítača) v sieti)
TCP	Transmission Control Protocol
UDP	User Diagram Protocol
URL	Uniform Resource Locator
VPN	Virtual Private Network

ZOZNAM OBRÁZKOV