“Mladi za napredek Maribora 2019”

36. Srečanje

TEMEN INTERNET

Računalništvo in informatika

Raziskovalna naloga

Avtor: AHAC – RAFAEL BELA, KLEMEN SKOK, ALEN FRIDAU

Mentor: BRANKO POTISK
Šola: SREDNJA ELEKTRO-RAČUNALNIŠKA ŠOLA MARIBOR
Število točk: 113
Mesto: 5
Priznanje: bronasto

Maribor, 2019

“Mladi za napredek Maribora 2019”

36. Srečanje

TEMEN INTERNET

Računalništvo in informatika

Raziskovalna naloga

Maribor, 2019

1 KAZALO

2 KAZALO SLIK

3 KAZALO GRAFOV

4 UVOD

4.1 Uvodne misli

Splet ali lažje prepoznan pod imenom WWW *(angl. world wide web)*, je hipertekstni sistem, ki deluje na medmrežju. Zasnovala sta ga Tim Berners-Lee in Robert Cailliau v Evropskem središču za jedrske raziskave CERN, kjer sta razvila sistem ENQUIRE*(angl. Enquire Within Upon Everything)*, čigar ime je povzeta po naslovu knjige, katere se Tim spominja iz otroštva. Način delovanja ENQUIRE-a je zelo podoben načinu delovanja spleta, ki ga poznamo danes, kljub temu, da je na videz drugačen. Tim Berners-Lee je dejal, da je bila njegova vodilna misel pri izdelovanju spleta misel za olajšan dostop do informacij, ki so bile na različnih strežnikih v raziskovalnem središču CERN. Brskalniki te dokumente prenesejo ter nam prikažejo tako imenovane »spletne strani«. Med spletnimi stranmi lahko zelo hitro prehajamo, za-to se je uveljavil izraz deskanje. URL*(angl. Uniform Resource Locator)* je »naslov«, ki nas napoti do neke spletne strani. Brskalnik naloži datoteko s tipom HTML*(angl. Hyper-Text Markup Language)*. Pomemben je tudi izraz HTTP*(angl. Hyper-Text Transfer Protocol)*, ki na omogoča dostop do ogromno vsebin, ki smo ji že omenili-spletne strani. Zraven omenjenega obstajajo še druge, ki se nahajajo v tako imenovanem temnem spletu. Temni splet ali nevidni splet *(angl. deep web, invisible web, hidden web)* je skriti del celotnega spleta, ki je večini nepoznan, kakor tudi neraziskan v večini, do katerega ne moremo dostopati z navadnimi brskalniki, kot so Google, Yahoo, Bing.[1]

Slika 1: World Wide Web

(https://blogthinkbig.com/wp-content/uploads/2014/08/internet-y-la-web-1-620x348.jpg)

4.2 Hipoteze in cilji

Hipoteze raziskovalne naloge so:

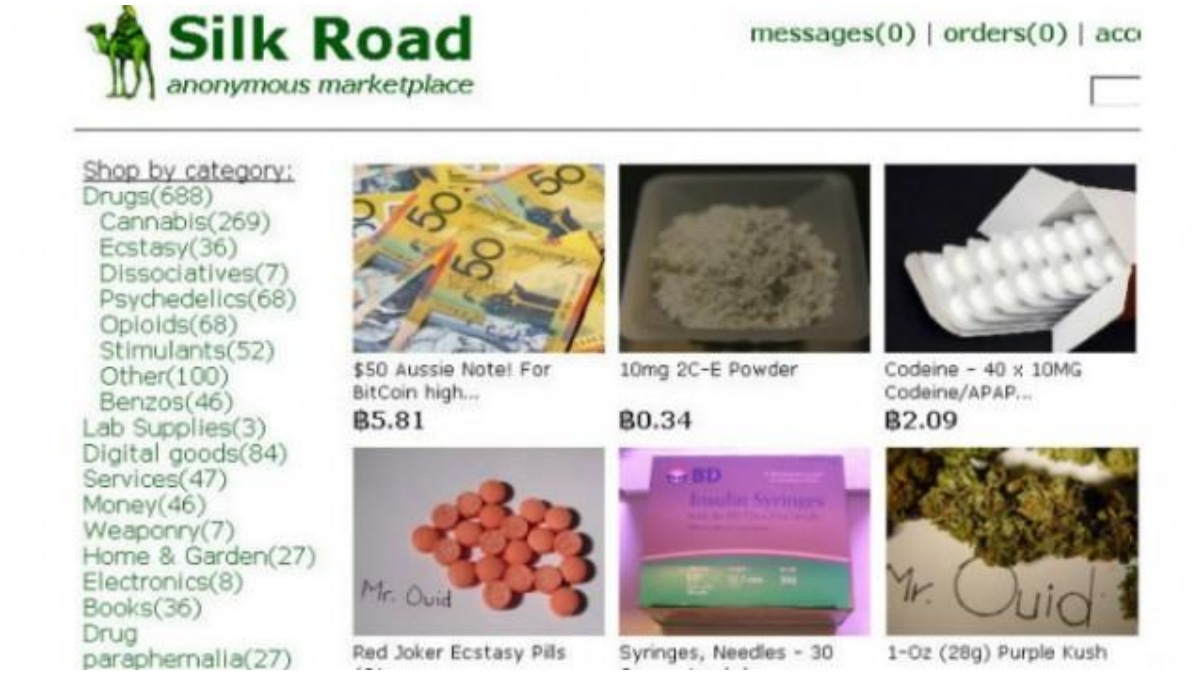
1. Predvidevamo, da smo ob vstopu v temen splet v nevarnosti.
2. Menimo, da temen splet uporabljajo kriminalci.
3. Temen splet bi naj bil središče za ilegalne dejavnosti.

Cilji raziskovalne naloge so ugotoviti:

1. Kako je možno dostopati do temnega spleta.
2. Je temni splet nevaren in kakšen je varen način dostopanja.
3. Za kaj se uporablja in kdo ga uporablja.
4. Kako je nastal in kdo ga nadzira.

5 METODOLOGIJA

Teorijo in podatke bomo črpali iz spletnih virov, jih med seboj primerjali in tako ovrgli ali potrdili naše hipoteze. Spletni viri so velikokrat lahko napačni, zato bomo potrdili pristnost podatkov, tako da najdemo več virov z enakimi podatki. Spletnih virov na temo temni splet ni veliko, verjetno zato ker je leta 2013 FBI ukinili eno največjih strani temnega spleta Silk Road in zaprli njenega ustanovitelja Rossa Ulbrichta, kar bi naj bil razlog za pomankanje virov. Še posebej pa je malo virov v slovenskem jeziku.



Slika 2: Silk Road

(https://www.extremetech.com/wp-content/uploads/2013/10/silk-road-header-640x353.jpg)

6 DISKUSIJA

6.1 Nastanek

Izraz za temen splet je prvotno (okoli leta 1970) označeval omrežja, ki so bila izolirana od ARPANET-a *(angl. Advanced Research Projects Agency Network)*, ki se je kasneje razvil v internet, ki ga poznamo danes. Temni internet je lahko dostopal ARPANET-u, vendar preko naslovov, ki se niso pojavili v seznamu omrežij ter niso »odgovarjale« pozvedbam. Ime se nanaša na izraz »black box«, ki pod prenesenim pomenom pomeni napravo, katere vsebina nam ni znana.[5]

Slika 3: Arpanet

(https://www.colocationamerica.com/images/arpanet.png)

Tehnično gledano noben ne nadzira temnega interneta, saj ni samo ena oseba, ki bi ga imela za svojega. Nadzirajo in spreminjajo ga lahko vsi, saj je možno ustvarit spletno stran na temnem spletu, s tem da jo nadziraš sam. Torej, ni osebe, ki bi sama upravljala in nadzirala temen splet.

6.2 Varnost

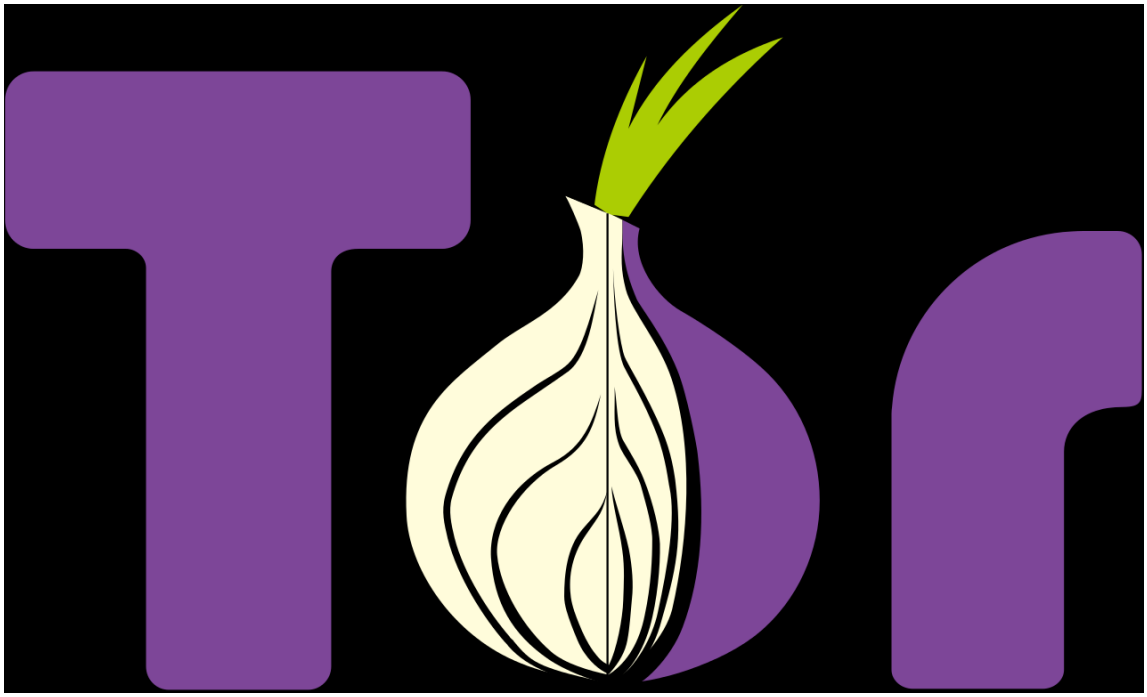
Če hočemo uporabljati temen internet varno je zelo pomembno, da smo na njem anonimni.
To lahko storimo s pomočjo tehnologije in s pravilno rabo temnega spleta.

6.2.1 Tor

Najbolj znan način dostopa do temnega spleta je preko brskalnika The Onion Router, krajše Tor (*angl. Tor Browser*). Spletne strani na temnem internetu imajo v URL-ju namesto .com ali .org .onion in to pomeni, da so dostopne samo uporabnikom brskalnika Tor.

Tor je brezplačen in odprtokodni grafični spletni brskalnik, ki nam omogoča anonimno brskanje po temnem spletu. Tor je ustvarila Vojna mornarica Združenih držav Amerike (*angl.*

United States Navy) leta 1995, kasneje pa ga je razvijala Agencija za napredne obrambne analize ZDA (*angl. Defense Advanced Research Projects Agency (DARPA)*).



Slika 4: Tor logotip

(https://commons.wikimedia.org/wiki/File:Tor-logo-2011-flat.svg)

Tor se večinoma uporablja, če nekdo želi postat anonimen iz takih ali drugačnih razlogov.

Novinarji ga uporabljajo, da varno sprejemajo sporočila in datoteke od ljudi, ki so pod nadzorom represivnih režimov. Kitajski novinarji in državljana pa ga uporabljajo, da pišejo o trenutnih dogodkih in kontroverznih temah. Preko Tora tudi širijo in spodbujajo politične in socialne reforme.

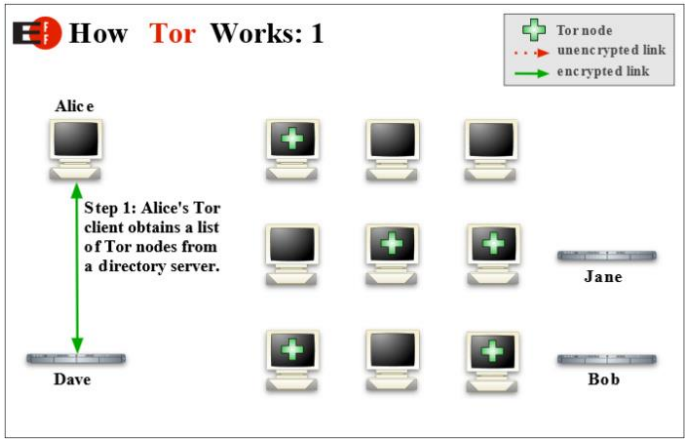
Uporabljajo ga tudi različni aktivisti, da varno širijo svoje ideje v krajih kjer je komunikacija strogo nadzorovana. Prijavitelji nepravilnosti širijo informacije o pokvarjenih ljudeh, podjetjih in korporacijah.

Tor uporabljajo tudi velika podjetja, saj z njim preverjajo svojo konkurenco, brez da bi jih ta zaznala.

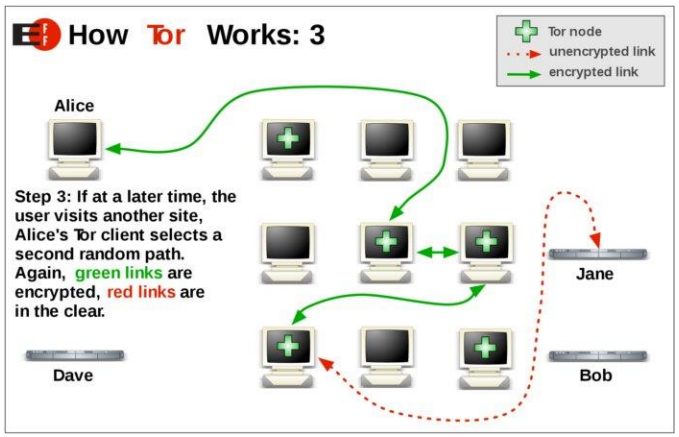
Vojska uporablja Tor, da bi zavarovala vojaške interese, operacije in vojake. Vojska z Torom tudi zbira in posreduje podatke.

Zaradi dobre anonimnosti Tor uporabljajo tudi kriminalci, pedofili, hekerji, preprodajalci z mamili, belim blagom in morilci.

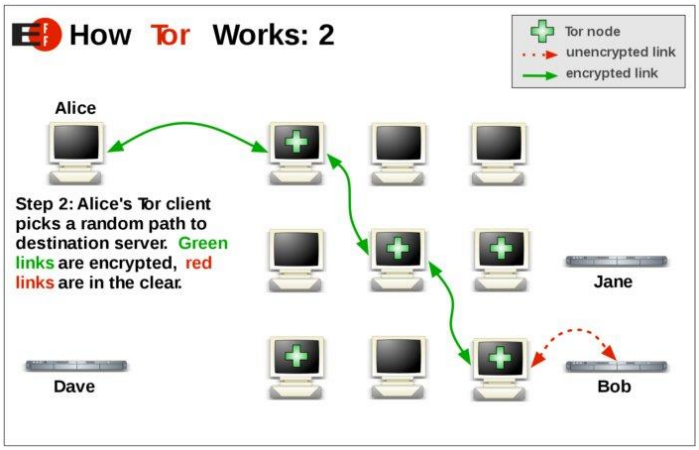
Tor usmeri vse tvojo internetni promet skozi Tor omrežje in ga s tem naredi anonimnega. Tor je sestavljen iz treh delov, kot so sestavljene plasti čebule, zato je tudi logotip Tor-a čebula. Najprej Tor usmeri tvoj internetni promet do javnega vstopnega vozlišča (*angl. entry node*), nato ga preusmeri do naključno izbranega sredinskega releja *(angl. middle relay*), na koncu pa izvrže tvoj internetni promet skozi tretje in zadnjo izhodno vozlišče (*angl. exit node*). Če živiš na področju kjer ni dovoljena uporaba Tora, ga lahko ponastaviš, da uporablja mostove *(angl. Bridge*). Naslovi bridge IP niso javno in zato jih ne moreš postaviti na črno listo.



Slika 5: 1. korak anonimnosti v Tor-u (https://www.csoonline.com/article/3287653/privacy/what-is-the-tor-browser-how-it-works-and-how-it-can-help-you-protect-your-identity-online.html)



Slika 6: 2. korak anonimnosti v Tor-u (https://www.csoonline.com/article/3287653/privacy/what-is-the-tor-browser-how-it-works-and-how-it-can-help-you-protect-your-identity-online.html)



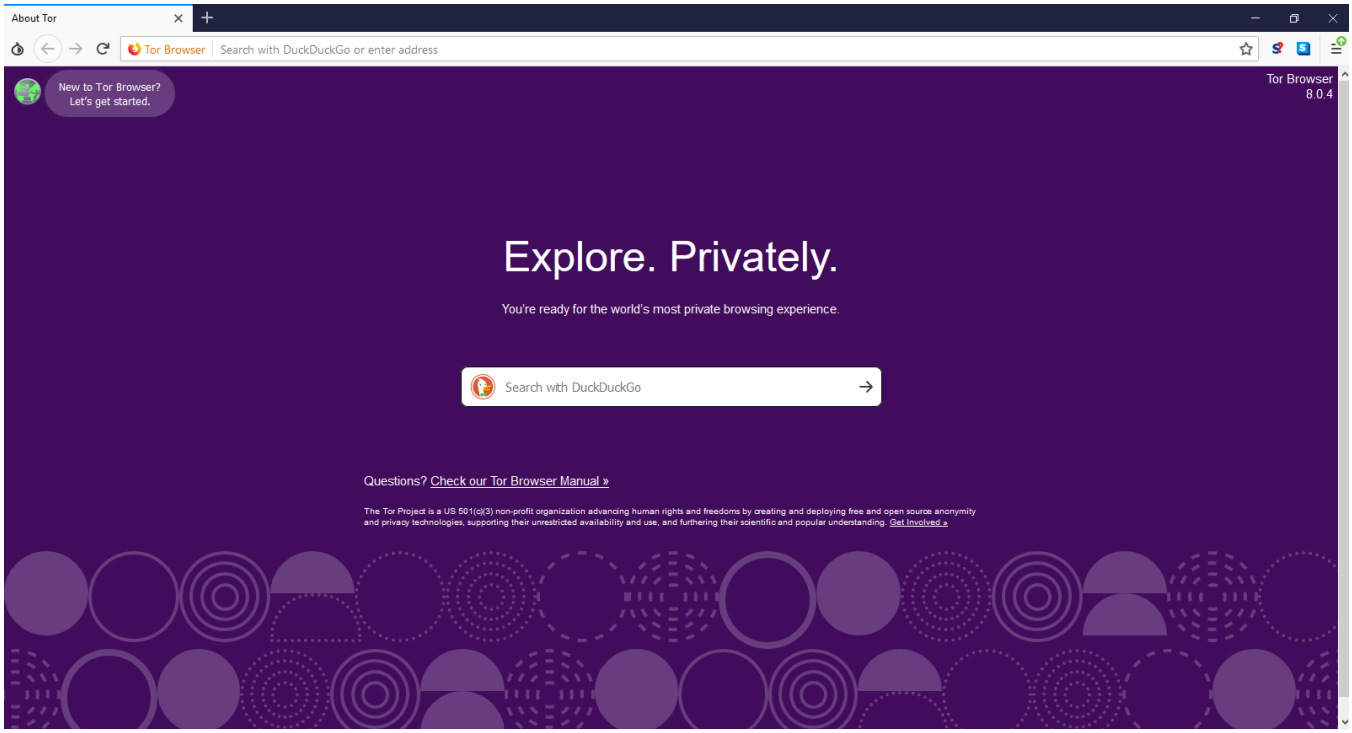
Slika 7: 3. korak anonimnosti v Tor-u (https://www.csoonline.com/article/3287653/privacy/what-is-the-tor-browser-how-it-works-and-how-it-can-help-you-protect-your-identity-online.html)

Tor je trenutno najbolj anonimen način brskanja po spletu, ampak ni popoln. Trenutno smo priča ″vojni″ med raziskovalci, ki hočejo povečati anonimnost Tora, in vlado, ki poskuša ugotoviti kako Tor naredi svoje uporabnike anonimne.

Najboljši način kako odkriti uporabnike Tora je z vdiranjem. FBI (*angl. Federal Bureau of Investigation*) je to metodo uporabila že večkrat, da so našli številne kriminalce. Pri tem jim je zelo pripomogel člen 41, ki FBI-ju omogoča, da vdre v veliko število računalnikov, pod enim nalogom. To je lahko zelo zaskrbljujoče, ker lahko v te pasti padejo tudi nedolžni uporabniki Tor-a. Kljub temu se splača uporabljati Tor saj zelo dobro zavaruje tvojo identiteto.

Tor je namenjen vsem vrstam internetnega prometa ampak je optimiziran za surfanje po spletu.

Največja slabost Tor-a je to, da se mora sporočilo na zadnjem vozlišču dešifrirati preden pride na končni cilj. Nekdo, ki upravlja končno vozlišče lahko to sporočilo vidi. Leta 2007 je Švedski raziskovalec Dan Egerstad uspel prestreči državna E-sporočila. Taka sporočila je težko prestreči, ker Tor naključno zbira izhodna vozlišča.



Slika 8: Brskalnik Tor

(lasten vir)

6.2.2 VPN

VPN omogoča uporabniku, da šifrira ves internetni promet, ki potuje v in iz njegove naprave ter ga preusmeri prek strežnika na lokacijo, ki jo izbere. VPN v kombinaciji z Tor dodatno prispeva k varnosti in anonimnosti uporabnika. Združevanje Tor-a in VPN-a izboljša varnost na temnem spletu. VPN in Tor lahko uporabljamo na dva različna načina; Tor nad VPN-om in VPN nad Tor-om.

Če se najprej povežemo na VPN in potem zaženemo Tor, uporabljamo Tor nad VPN-om. Najprej bo interneti promet šel skozi VPN serverje in nato se bo odbil na Tor-ovo omrežje. Ponudnik internetnih storitev (*angl. Internet service provider (ISP)*) lahko vidi samo šifriran VPN promet in ne bo vedel, da uporabljaš Tor. Če uporabljaš Tor nad VPN-om moraš zaupati svojemu VPN ponudniku, saj lahko vidi, da uporabljate Tor in lahko hrani dnevnike prometa (*angl. Traffic logs*) in dnevnike sej (*angl. session logs*). Dnevniki prometa vsebujejo vsebino internetnega prometa, kot so iskalne poizvedbe in obiskana spletna mesta, medtem ko dnevniki seje vsebujejo podatke, kot je IP naslov, ob času ko se vključi VPN, in koliko podatkov je bilo prenesenih. Dnevniki prometa so bolj zaskrbljujoči kot dnevniki sej, vendar niti eni niti drugi niso zaželeni, zato je pomembno, da se uporablja VPN, ki tega ne beleži. Tor nad VPN-om te ne zavaruje pred zlonamernimi izhodnimi vozlišči.

VPN nad Tor-om je manj popularen in Tor ga odsvetuje. Zelo malo VPN ponudnikov ponuja to storitev in ne dosegajo visokih hitrosti internetnega prometa. Pri tem načinu internetni promet poteka najprej skozi omrežje Tor, nato pa skozi omrežje VPN. To pomeni, da VPN ponudnik ne vidi tvojega pravega IP naslova in VPN te zaščiti pred zlonamernimi izhodnimi vozlišči. Velika slabost tega je, da ponudnik internetnih storitev lahko vidi, da se uporablja Tor, kar je v nekaterih krajih lahko zelo zaskrbljujoče. Tudi v tem primeru je zelo pomembno, da se uporablja VPN, ki ne zapisuje dnevnikov. VPN nad Tor-om je zelo občutljiv na časovne napade (*angl. timing attack*). Časovni napad je izkoristek v varnosti omrežja in napadalcu omogoči, da odkrije ranljivost v sistemu, tako da preuči odzivani čas različnih vnosov.

Slika 9: Delovanje VPN-a
(https://9to5mac.com/guides/vpn/)

6.2.3 I2P

I2P je anonimna mreža kot Tor, ampak se od Tor-a razlikuje v tem, da I2P-ja ne moremo uporabiti, da bi dostopali javni internet, ampak samo skrita in specifična omrežja. Z I2P-jem ni mogoče uporabiti spletnih mest .onion, ker je to popolnoma ločeno omrežje od Tor. Namesto tega I2P uporablja lastno znamko skritih lokacij, imenovanih »eepsites«.

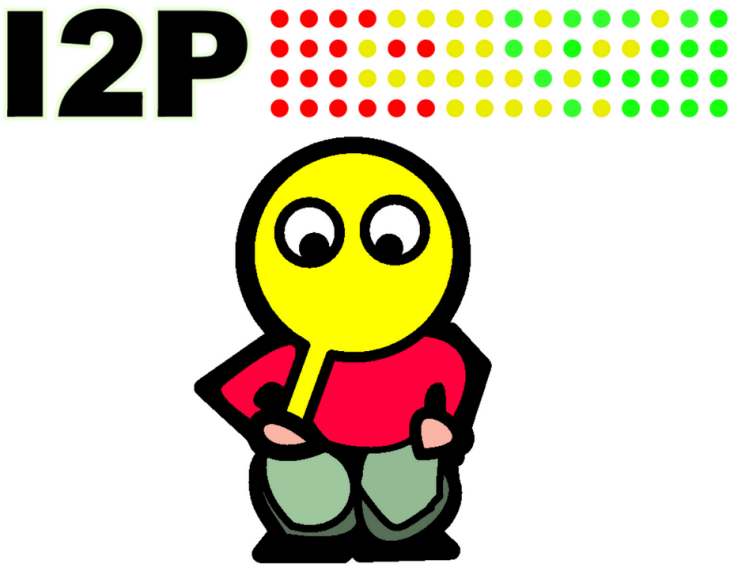
I2P je peer-to-peer omrežje (P2P). To pomeni, da se uporabniki povezujejo in si delijo vire, pasovno širino in shrambo. Vsaka naprava v omrežju deluje kot usmerjevalnik. I2P vzpostavi vhodne in izhodne tunele z ostalimi usmerjevalniki. Zaradi tega potujejo sporočila skozi več

izhodnih predorov, preden pridejo do končne destinacije. Sprejeti podatki so tudi potovali skozi več predorov. Zaradi tega sistema so sporočila šifrirana.

Za razliko od Tor-ovega čebulnega usmerjanja (*angl. onion routing*), I2P uporablja česnovo usmerjanje (*angl. garlic routing*). Razlika je v tem, da čebulno usmerjanje vsebuje eno sporočilo med tem ko česnovo usmerjanje vsebuje niz sporočil, ki se odcepijo ko dosežejo svojo končno destinacijo. Zaradi tega je sledenje in vdiranje v sporočila težje.

Zaradi tunelov v I2P omrežju je zelo težko izvesti časovne napade. Ker lahko uporabnik sam prilagodi dolžino in trajanje, ki ga sporočilo porabi v tunelih je zelo težko odkriti časovne vzorce.

I2P omrežje ni namenjeno povprečnemu uporabniku, saj najbolje deluje z operacijskim sistemom Linux in njegova instalacija je zelo zapletena, kar lahko odvrže veliko uporabnikov. I2P ni zasnovan, da bi lahko anonimno brskal po straneh kot je Google.



Slika 10: I2P logotip (https://steemit.com/steemstem/@j1337/i2p-the-invisible-internet-project-overview-of-private-networks-nodes-and-more)

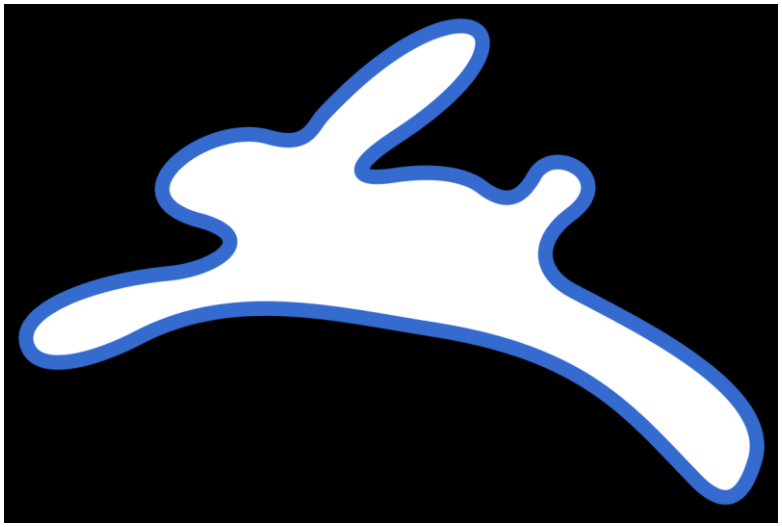
6.2.4 Freenet

Tako kot I2P Freenet-a ne moreš uporabljati za dostop spletnih mest v javnem spletu. Uporablja se lahko samo za dostop do vsebine, naložene v Freenet, ki je razdeljen med vrstnike (P2P). za razliko od Tor-a in I2P-ja ne potrebuje strežnika za gostovanje vsebine, temveč vsebino prenese in tam ostane za nedoločen čas.

Freenet omogoča uporabnikom, da se povežejo z enim od dveh načinov: darknet in opennet.

Darknet omogoča, da določiš svoje prijatelje v omrežju in se z njimi povežeš in deliš vsebino. To omogoča skupinam ljudi, da ustvarijo zaprte anonimne mreže, sestavljene izključno iz ljudi, ki jih poznajo in jim zaupajo. Zaradi tega je Freenet zelo popularen na Kitajskem in v državah, kje rimajo zelo stroge režime.

Lahko pa se uporabnik poveže z načinom opennet, ki samodejno dodeli vrstnike v omrežju. V opennet-si povezan z več šifriranimi vozlišči.



Slika 11: Freenet logotip

(https://en.wikipedia.org/wiki/Freenet)

6.3 Kako ostati varen na temnem spletu?

Večina komercialnih operacijskih sistemov (OS) kot sta Windows in MAC zapisujejo podatke na disk in to lahko pusti dokaze o dejavnosti na temnem spletu. Za najboljšo varnost je potrebna namestitev OS-a TAILS (The Amnesic Incognito Live System). TAILS je posebna distribucija Linuxa, ki se v celoti izvaja v pomnilniku in ne pusti nobenih datotek ali piškotkov na trdem disku razen, če se mu to naroči.

Slika 12: TAILS logotip

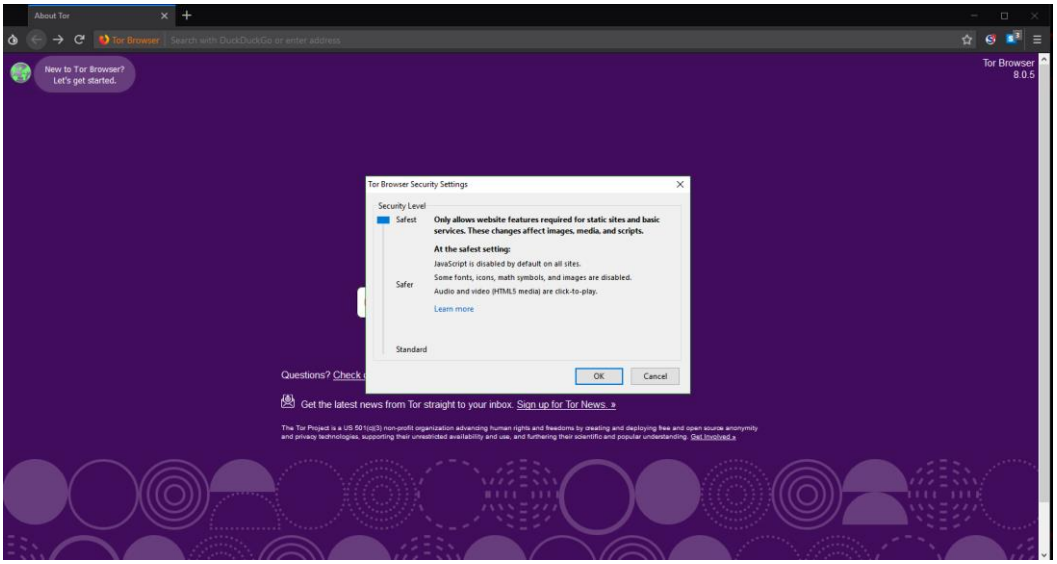
(https://denovatoanovato.net/tails-privacidad-y-el-anonimato-libero-su-version-3-9/)

Pomembno je tudi, da se nikoli ne nameščajo programi, ki so na voljo preko povezav. Torej, če neka spletna stran pravi, da se mora posodobiti določena programska oprema in vam do te programske opreme ponuja povezavo, se ta programska oprema ne sme naložiti saj lahko vsebuje škodljivo kodo. Zato moramo v brskalnik vtipkati spletno mesto pravega prodajalca.

Potrebne se je tudi izogniti izvajanju Javascript-a. Zato je potrebno, da se naloži vtičnik (*angl. Plugin*) NoScript. NoScript omogoča, da se Javascript začasno izvaja na samo zaupanja vrednih spletnih mestih.

Pomembno je tudi, da brskalnik ni nikoli v maksimiranem načinu, saj lahko spletne strani ugotovijo resolucijo ekrana. Nikoli se ne smejo deliti osebni podatki in vsi nakupi morajo biti plačani z Bitcoin-om, da bi zagotovil svojo anonimnost.

Nikoli se ne sme iskati nezakonitih spletnih mest. veliko od teh spletnih mest so prevari ali pa vabe namenjene kriminalcem.



Slika 13: Varnostne opcije v Tor-u

(lasten vir)

6.4 Uporabnost temnega spleta

Dostop do temnega spleta je mogoč vsakemu posamezniku, ki je nekoliko bolj vešč v uporabi računalnika, kar je obenem slabost, kakor tudi nekaj dobrega. To pomeni, da so na temnem spletu posamezniki, ki uporabljajo temen splet za »dobre namene« in tudi za »slabe namene«. Možnost za izvajanje ilegalnih dejavnosti na temnem spletu omogoča anonimnost, ki jo ponuja Tor. Temni splet je tako dom mnogim pedofilom, prodajalcem prepovedanih drog, prodajalcem orožja, kakor tudi prevarantov, terorističnim organizacijam, ki na temnem spletu organizirajo spletne igralnice, prodajalnice orožja, drog, Bitcoin-ov, denarnih vrednosti v računalniških igrah,… Bitcoin je kriptovaluta, ki s pomočjo kriptografije uporabnikom omogoča zasebnost in zaščito transakcij, zato je za ta posel ravno pravšnji. Nastanek Bitcoin-a sega v leto 2008, ko ga je razvil oziroma so ga razvili posamezniki ali posameznik z vzdevkom Satoshi Nakamoto. Identiteta posameznikov oziroma posameznika ostaja skrivnost. Bitcoin je torej elektronski sistem denarja, ki ne potrebuje posrednika. Transakcije in nastanek Bitcoin-a poteka po odprtokodnem kriptograskem protokolu. Najmanjša enote je Satoshi. Poleg Bitcoin-a je še na stotine drugih kriptovalut, po imenu altcoins, ki so alternative Bitcoin-u, s tem, da se razlikujejo v načinu delovanja, in sicer v:

1. hitrosti transakcij,
2. velikosti blokov,
3. metodah distribucij,
4. algoritmih preverjanja,
5. namenu uporabe.

Bitcoin je tako najbolj znan izmed mnogih kriptovalut, kjer se pojavi še ime litecoin, ki pa ima malo drugačen namen – postati pravo plačilno sredstvo.

6.4.1 Dohodek pri kriptovalutah

Uporaba kriptovalut v Sloveniji ni prepovedana. Dohodek dobljen iz kriptovalut namreč ni obdavčen, vendar je obdavčen dohodek kriptovalut pri rudarjenju.

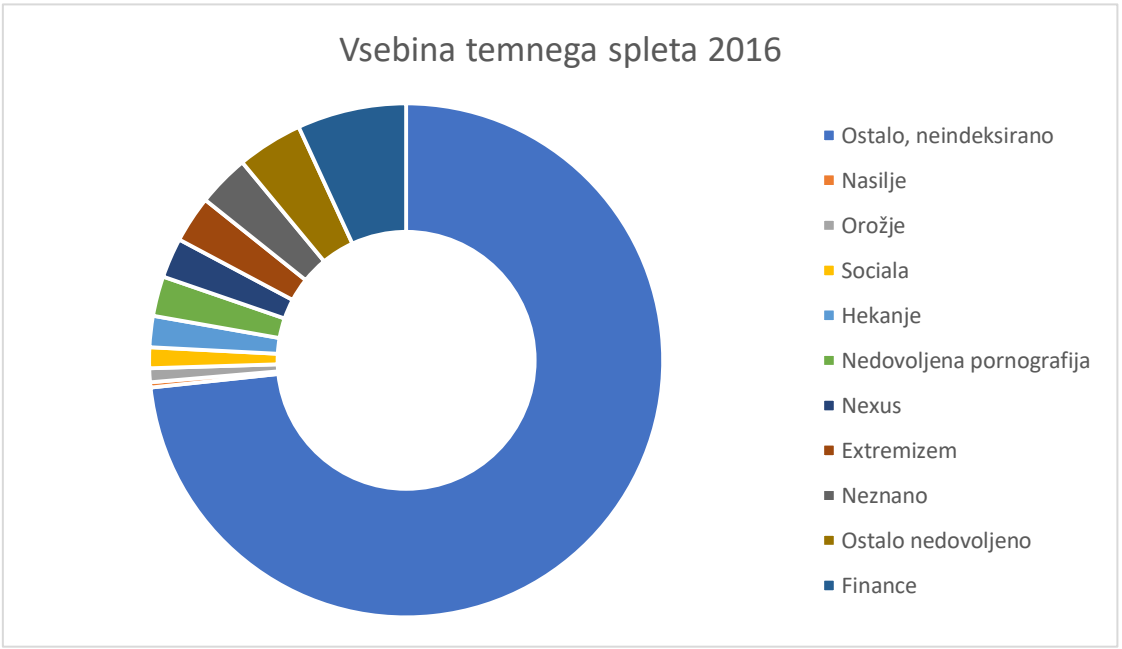
6.4.1.1 Rudarjenje

Plačevanje z Bitcoin-om poteka neprestano, zato je pomembno da se transakcije beležijo, vendar z anonimnostjo. Bitcoin mreža ta problem rešuje ta problem tako, da vse transakcije opravljene v določenem časovnem obdobju zbere v seznam – blok. Rudarji torej potrjujejo te posle in jih zapisujejo v glavno knjigo. Glavna knjiga *(angl. blockchain)* mora biti močno zaščitena, saj vsebuje zelo pomembne podatke. Ko je ustvarjen nov blok, torej takrat, ko se zgodijo nove transakcije, so podatki, ki so vzeti iz bloka zakodirani z matematičnim postopkom, ki rudarjem vrne veliko krajše, na videz naključno, zaporedje črk in številk. Ta postopek je relativno enostaven, vendar je nemogoče proces obratno izvršiti, kar nam daje zelo dobro varnost. Ob vsakem uspešno ustvarjenem verigi blokov, so posamezniki, ki so pri tem sodelovali nagrajeni s plačilom 25 Bitcoin-ov, vendar zaradi velikega števila udeleženih je to plačilo razdeljeno med vse tako, da več operacij kot je nekdo opravil, večji delež plačilo bo imel izplačano.

Slika 14: Kriptovalute
(https://www.studentarija.net/wp-content/uploads/2018/01/kriptovaluta.jpg)

6.5 Stanje temnega spleta

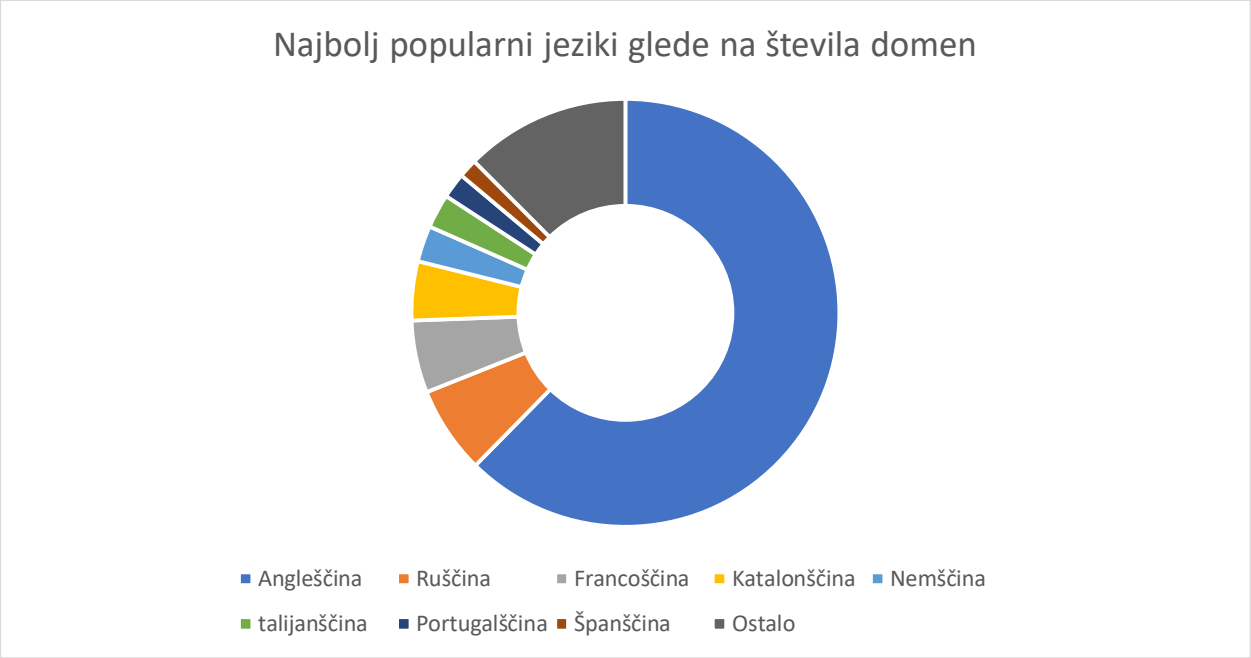
V študiji so ugotovili da na temnem spletu prevladuje nelegalna pornografija, črni trg, skupine hekerjev in botnet (je škodljiva koda, ki se poveže s strežnikom napadalca) operacije.



Graf 1: Vsebina temenega spleta
(https://siol.net/digisvet/novice/temni-splet-kaj-se-skriva-v-globinah-dezele-kriminala-in-prikritih-storitev-445007)

Za transakcije na temnem spletu se uporabljajo kriptovalute, zaradi zasebnosti oziroma anonimnosti in zaščitene transakcije, najbolj uporabljena kriptovaluta pa je Bitcoin. Na

temnem spletu različne strani uporabljajo različne jezike, najbolj priljubljen jezik je angleščina,”Od 3454 uspešno preiskanih domen jih je bilo 2154 v angleškem jeziku, kar predstavlja 62% vseh strani. Sledijo ruski jezik (228 strani) in francoski (189 strani).”(Luka Demšar, Temni splet in kriminal,2016).



Graf 2: Popularnih jezikov domen
(Luka Demšar, Temni splet in kriminal,2016).

7 RAZPRAVA

Cilji raziskovalne naloge so ugotoviti:

1. Kako je možno dostopati do temnega spleta.
2. Je temni splet nevaren in kakšen je varen način dostopanja.
3. Za kaj se uporablja in kdo ga uporablja.
4. Kako je nastal in kdo ga nadzira.

1. Iz zbranih podatkov smo dobili zanesljive informacija, kako dostopati do temnega spleta in sklepamo, da je to možno preko brskalnika Tor z uporabo spletnih strani z povezavo .onion. Temnih spletnih strani sami nismo obiskovali, ker nam nevarnosti le teh niso popolnoma jasne in zaradi tega temeljijo naši zaključki zgolj po najdenih spletnih virih.
2. Glede naše aktivnosti in zbrane podatke se ga je priporočljivo izogibati, zaradi ilegalnih aktivnosti na njem, ter večje možnosti da nam nekdo želi škodovati. Z uporabo VPN-a se lahko bolje zaščitimo pred vdori, vendar ni povsem zanesljiv.
3. Temni splet predvsem uporabljajo kriminalci, novinarji, vojska, podjetja za industrijsko vohunjenje in ljudje kjer je dostop do interneta strogo omejen. Uporablja se predvsem za anonimno širjenje podatkov, prodajo drog, otroške pornografije, ponarejen osebne izkaznice, prodajo osebnih podatkov ipd.
4. Nastanek ni ravno določen izraz temen internet oziroma ang. dark web se je pojavil leta 1970 in je označeval ves internet ki ni bil dostopen ARPNETA, ki se je razvil v internet, kot ga poznamo danes. Ne moremo reči, da temen splet kdor koli nadzira, ker lahko vsak ustvari svojo stran in jo nadzira.

Hipoteze raziskovalne naloge so:

1. Predvidevamo, da smo ob vstopu v temen splet v nevarnosti.
2. Menimo, da temen splet uporabljajo kriminalci.
3. Temen splet bi naj bil središče za ilegalne dejavnosti.

1. Iz zbranih podatkov naša prva hipoteza deloma drži, ker ni nujno da smo takoj ob vstopu tarča napada. Pred napadi oziroma vdori je se možno bolje zaščititi z VPN-om, ampak nam ne nudi popolne zaščite. Na temnem spletu samo lahko v nevarnosti tudi, zato ker ga uporablja veliko kriminalcev in nikoli ne vemo s kom imamo opravka in kakšni so njihovi nameni.
2. Po vseh zbranih podatkih smo ugotovili, da temen splet res uporabljajo kriminalci, vendar niso edini uporabniki. Poleg kriminalcev, ki uporabljajo temen splet za prodajo in kupovanje drog ter ponarejenih osebnih izkaznic ipd., uporabljajo temen splet še novinarji za zbiranje in objavljane anonimnih podatkov, ljudje ki imajo zelo omejen dostop do internetne vsebine in uporabljajo temen splet da pridejo do informacij, podjetja da dobijo informacije svoje konkurence. Iz tega lahko potrdimo našo hipotezo. [3]
3. Čeprav se temen splet uporablja za mnoge ilegalne dejavnosti ni središče ilegalnih dejavnosti, ampak so ilegalne dejavnosti središče temnega spleta. Tako ovržemo našo hipotezo, da je temni splet središče ilegalnih dejavnosti.

8 ZAKLJUČEK

Do temnega spleta je možno dostopati z brskalnikom Tor. Temen splet je nevaren ampak se je možno zaščititi, uporablja se za ilegalne dejavnosti, prodajo ilegalnih in ponarejenih izdelkov. Izraz temen internet *(angl. Dark web)* izvira iz leta 1970 in označuje internet ki ni povezan s površinskim spletom, noben ga ne nadzira, saj ni v lasti ene osebe ali organizacije.
Ugotovili smo, da naša hipoteza da smo ob vstopu v temen splet v nevarnosti, deloma drži kajti če ne uporabimo VPN-a (Virtual Prviate Network) smo lahka trača hekerjem ki lahko takoj pridobijo naš IP naslov in s tem našo lokacijo, ter nam z lahkoto vdrejo v naš računalnik. Torej ob vstopu v temen splet smo lahko v nevarnosti, vendar ne takoj ob vstopu, saj ni nujno da smo tarča hekerjem, ki bi želeli izvedeti naš IP naslov, če pa uporabimo VPN(Virtual private network) smo bolje zaščiteni pred hekerji. Za hipotezo, da temen internet uporabljajo kriminalci smo ugotovili da drži vendar ga ne uporabljajo izključno kriminalci uporabljajo ga še podjetja za vohunjenje, ljudje ki imajo strogo omejen dostop do površinskega internet. Naša zadnja hipoteza je deloma pravilna, čeprav se temen splet uporablja predvsem za ilegalne dejavnosti kot so: prodaja drog, prodaja ponarejenih osebnih izkaznic, prodaja ponarejenih vozniških izpitov ipd., ni središče ilegalnih dejavnosti, kvečjemu so ilegalne dejavnosti središče temnega spleta.

9 VIRI

WorldWideWeb : Proposal for a HyperText Project, avtor neznan Dostopna na URL naslovu: https://www.w3.org/Proposal (15.12.2018) [1]

Hacker Lexicon: What is the Dark Web, avtor neznan Dostopna na URL naslovu: https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/ (16.12.2018) [2]

Darknet – Temni del interneta, Jan Konečnik, Tednik Dostopna na URL naslovu: https://www.rtvslo.si/znanost-in-tehnologija/darknet-temni-del-interneta/404795 (16.12.2018) [3]

Kaj vse se skriva pod površino spleta, Marjan Kodelja Dostopna na URL naslovu: https://sl.wikipedia.org/wiki/Globoki_splet (18.12.2018) [4]

Avtor neznan, Om Darknet, avtor neznan Dostopna na URL naslovu: https://web.archive.org/web/20150325025545/http://darknet.se/about-darknet/ (19.12.2018) [5]

ŽLOGAR, Marjan, 2017, Temni splet – kaj se skriva v globinah dežele kriminala in prikritih. Dostopno na URL naslovu: https://siol.net/digisvet/novice/temni-splet-kaj-se-skriva-v-globinah-dezele-kriminala-in-prikritih-storitev-445007 (20.12.1018) [6]

Avtor neznan, Silk Road: Theory & Practice (2011). Dostopno na URL naslovu: http://www.gwern.net/Silk-Road (21.12.2018) [7]

Rudarjenje, avtor neznan Dostopno na URL naslovu: https://kriptovalute.si/bitcoin-mining/ (27.12.2018) [8]

Top ways to earn money from cryptocurrencies, Sudhir Khatwani Dostopno na URL naslovu: https://coinsutra.com/earn-money-from-cryptocurrencies/ (5.1.2018) [9]

DEMŠAR, Luka, 2016, Temni splet in kriminal : diplomsko delo univerzitetnega študija [na spletu]. Univerza v Mariboru, Fakulteta za varnostne vede. Dostopno na URL naslovu: https://dk.um.si/IzpisGradiva.php?lang=slv&id=62169 (5.1.2018) [10]

KLOSOWSKI (2014), Thorin, What Is Tor and Should I Use It?. Dostopno na URL naslovu: https://lifehacker.com/what-is-tor-and-should-i-use-it-1527891029 (5.1.2019) [11]

Avtor neznan, Inception, Dostopno na URL naslovu: https://www.torproject.org/about/torusers.html.en (5.1.2019) [12]

Porup , J.M., 2018, What is the Tor Browser? How it works and how it can help you protect your identity onlineb. Dostopno na URL naslovu: https://www.csoonline.com/article/3287653/privacy/what-is-the-tor-browser-how-it-works-and-how-it-can-help-you-protect-your-identity-online.html (6.1.2019) [13]

BISCHOFF, Paul, 2018, Step by step guide to safely accessing the dark net and deep web. Dostopno na URL naslovu: https://www.comparitech.com/blog/vpn-privacy/how-to-access-the-deep-web-and-darknet/ (9.1.2019) [14]

NORRIS, John, The Privacy Pros and Cons of the I2P Network, Dostopno na URL naslovu: https://www.vpnmentor.com/blog/pros-cons-i2p-network/ (12.1.2019) [15]

MCDOWELL , Guy, 2013, The Web Hidden On The Web – FreeNet. Dostopno na URL naslovu: https://www.makeuseof.com/tag/freenet-the-private-internet/ (12.1.2019) [16]

BARTOLETTI, Anthony, 2018, Any advice on how to stay safe on the deep/dark web?. Dostopno na URL naslovu: https://www.quora.com/Any-advice-on-how-to-stay-safe-on-the-deep-dark-web (12.1.2019) [17]