Deskriptivna analiza mreže Darkweb u kontekstu pandemije COVID-19

Petrović, Kristijan

Sveučilište u Zagrebu
Fakultet prometnih znanosti

ZAVRŠNI RAD

Deskriptivna analiza mreže Darkweb u kontekstu pandemije COVID-19

Descriptive Analysis of Darkweb Network in the Context of COVID-19 Pandemic

Mentor: doc. dr. sc. Ivan Forenbacher

Student: Kristijan Petrović
JMBAG: 0246078703

Zagreb, lipanj 2022.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
ODBOR ZA ZAVRŠNI RAD

Zagreb, 4. svibnja 2022.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Arhitektura telekomunikacijske mreže**

ZAVRŠNI ZADATAK br. 6729

Pristupnik: **Kristijan Petrović (0246078703)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Deskriptivna analiza mreže Darkweb u kontekstu pandemije COVID-19**

Opis zadatka:

U radu je potrebno opisati koncept rada i način korištenja Darkweb (TOR) mreže. Analizirati arhitekturu Darkweb mreže te njezine prednosti i nedostatke. Opisati ponudu skrivenih servisa na Darkwebu u kontekstu pandemije COVID-19.

Mentor:

doc. dr. sc. Ivan Forenbacher

Predsjednik povjerenstva za završni ispit:

SAŽETAK

Anonimnost i sigurnost na Internetu omogućava se uporabom mračne mreže (engl. Darkweb) koja koristi luk usmjeravanje (engl. the onion routing – TOR) za sprječavanje analize prometa. Analiza prometa (engl. traffic analysis) je oblik mrežnog nadzora uz pomoć kojega se može ugroziti anonimnost i sigurnost korisnika. U radu će biti objašnjen rad TOR mreža i njihove skrivene usluge koje sve postoje, te koje će omogućiti unaprjeđivanje i razvoj zaštita protiv napada i zlonamjernih programa kao što su to analize prometa. Dodatno će biti prikazan način preuzimanja, instalacije, postavljanje postavki i pokretanje Darkweba. Zatim će biti prikazana arhitektura Darkweb (TOR) mreže i svaki dio u toj mreži biti će dodatno pojašnjen zajedno sa njihovim ulogama u mreži. Pandemijom koju je uzrokovao virus COVID-19 preoblikovan je način na koji se potražuje roba i usluge diljem svijeta. To dovodi do uporabe mračnih mrežnih tržnica koju su dostupne preko mračnih mreža koje su stekle veliku popularnost u tom razdoblju. Također biti će popraćena i kupnja proizvoda povezanih sa COVID-19.

KLJUČNE RIJEČI: Mračna mreža; luk usmjeravanje; analiza prometa; anonimnost; sigurnost; skrivene usluge; arhitektura; pandemija COVID-19; mračna mrežna tržnica

SUMMARY

Anonymity and security on the Interent is made possible by the use of the Darkweb, which uses the onion routing to prevent traffic analysis. Traffic analysis is a form of network monitoring that can threated user anonymity and security. The paper will explain the operation of TOR networks, their hidden services, all types of them that exist and which of them will enable the improvement and development of protection against attacks and malicious programs such as traffic analysis. Additionally, there will be shown how to download, install, set settings and run the Darkweb. Next, the architecture of the Darkweb network will be presented and each part in that network will be further explained along with their roles in the network. The pandemic caused by the COVID-19 virus has reshaped the way in which goods and services are demanded around the world. This leads to the use of Darkweb markets that are accessible through Darkweb which gained a lot of popularity during this period. Also the purchase of products related to COVID-19 will also be accompanied.

KEYWORDS: Darkweb; The onion routing; traffic analysis; anonymity; safety; hidden services; architecture; pandemic COVID-19; Darkweb market

Sadržaj

1. Uvod 1

2. Koncept rada Darkweb (TOR) mreže 3

2.1. Analiza prometa 5

2.2. Distribuirana anonimna mreža 9

2.3. Skrivene usluge 15

2.3.1. Usluge e-trgovine 16

2.3.2 Elektronička pošta 16

2.3.3. Pohranjivanje datoteke 17

2.3.4. Tražilice 17

2.3.5. Arhiva vijesti 17

2.4. Onion usmjeravanje 18

2.4.1. Podatkovne strukture za usmjeravanje 19

2.4.2. Odgovaranje na poruku 20

3. Korištenje Dark web (TOR) mreže 22

3.1. Preuzimanje Dark web (TOR) mreže na Windowsu i Mac operativnom sustavu 23

3.2. Instalacija Dark web (TOR) mreže na Windowsu i Mac operativnom sustavu 24

3.3. Povezivanje na Dark web (TOR) mreže na Windowsu i Mac operativnom sustavu 25

3.4. Pokretanje Dark web (TOR) mreže na Windowsu i Mac operativnom sustavu 26

4. Analiza arhitekture Dark web (TOR) mreže 29

5. Nedostatci i prednosti Dark web (TOR) mreže 31

6. Ponuda skrivenih servisa na Darkwebu u kontekstu pandemije COVID-19 34

7. Zaključak 41

Popis literature 42

Popis kratica 44

Popis slika 45

Popis tablica 46

Popis grafova 47

1. Uvod

Na samu spomen riječi Darkweb ljudima prvo pada na pamet neko okruženje na Internetu na kojem se odvijaju neke ilegalne radnje, te se mogu kupiti i prodavati oružja, droga, alkohol, lijekovi, itd. Međutim, Darkweb je potpuno legalna i sigurna mreža, te upravo zbog svog načina rada omogućuje korisnicima zaštitu, sigurnost privatnosti i anonimnost. Zbog odlične mogućnosti zaštite identiteta i anonimnosti vrlo često se zloupotrebljava kako se kriminalcima teško moglo uči u trag. Završni rad sastoji se od sljedećih poglavlja:

1. uvod
2. koncept rada Darkweb (TOR) mreže
3. korištenje Darkweb (TOR) mreže
4. analiza arhitekture Darkweb (TOR) mreže
5. nedostatci i prednosti Darkweb (TOR) mreže
6. ponuda skrivenih servisa na Darkwebu u kontekstu pandemije COVID-19
7. zaključak

Drugo poglavlje sastoji se od četiri potpoglavlja. U drugom poglavlju bit će objašnjen koncept rada Darkweb (TOR) mreže, na koji način funkcionira usmjeravanje internetskog prometa i kako omogućiti sprječavanje presretanja podataka u mreži. Također bit će objašnjeno kako se može nadziranja prometa u mreži pomoću analize prometa. Na kraju bit će objašnjene TOR skrivene usluge, kako i zašto ih se koristi, te koje su sve postojeće skrivene usluge unutar neke TOR mreže.

Treće poglavlje sastoji se od četiri potpoglavlja. U trećem poglavlju bit će navedeni svi operativni sustavi na kojim se može koristiti Darkweb (TOR) mrežu i koji model za povezivanje ona koristi. Zatim će u nastavku biti prikazani postupci preuzimanja, instalacije, povezivanja i pokretanja Darkweba. Također, biti će navedene sve razine zaštite koje se mogu birati prije uporabe Darkweba.

Četvrto poglavlje prikazuje arhitekturu neke Darkweb (TOR) mreže. Biti će navedeni svi dijelovi koji se nalaze u toj mreži, a na kraju će svaki dio te mreže biti detaljno objašnjen i pojašnjen.

Peto poglavlje uglavnom će se bazirati na prednostima i nedostatcima Darkweb (TOR) mreže. Kroz navedene primjere biti će obrazloženi pozitivni i negativni aspekti korištenja ove mreže.

Šesto poglavlje će ukratko opisati što i kako je započela pandemija uzrokovana virusom COVID-19, te kakav je ona imala utjecaj na globalnu ekonomiju i zbog kojih razloga su se ljudi odlučili za kupnju preko Darkweba. Zatim će u nastavku biti prikazano i objašnjeno kako je nastala Darkweb mreža, te koje su sve nove Darkweb mreže nastale. Uz pomoć priloženih tablica i grafova biti će objašnjene cijene i ponude proizvoda koji su povezani sa COVID-19 oglasima, te aktivnost na Darkweb tržnici.

Na kraju rada u sedmom poglavlju bit će donesen zaključak. U zaključku će biti navedeni svi bitni dijelovi ovog rada.

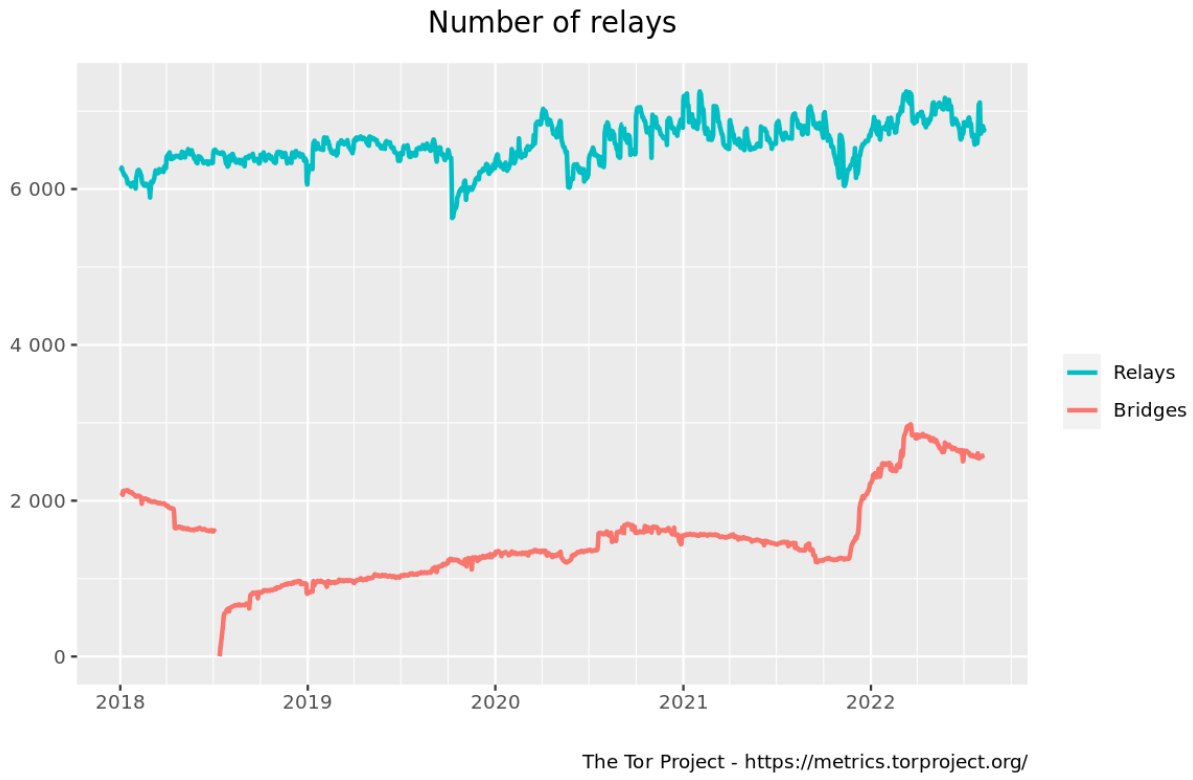
2. Koncept rada Darkweb (TOR) mreže

Dark web čini sadržaj koje je namjerno sakriven i dio je duboke mreže (engl. Deep web). Da bi mu se pristupilo potrebno je koristiti isključivo posebne programe i alate. Korisnicima klasičnih tražilica nije dostupan sadržaj Deep weba kao ni sadržaj Dark weba. Dark web se nalazi na privatnim mrežama koje su zasnivane na peer-to-peer povezanostima. Zbog strukture Dark weba pruža se privatnost identiteta i anonimnost korisnika [1].

TOR mreža je distribuirana anonimna računalna mreža koju tvore skupine volonterskih poslužitelja pomoću kojih promet putuje. Ujedno TOR mreža se oslanja na običan Internet, koristi IP protokol i korištenjem TOR-a garantirana se privatnost i sigurnost od praćenja aktivnosti na internetu. Uporabom alata za analizu prometa i nadzor mreže otkriva se IP adresa odredišta i IP adresa pošiljatelja, odnosno posjećene stranice. Moguće je korištenje dodatnih alata, IP adresa se dodatno može povezati i s fizičkom lokacijom korisnika interneta. TOR mreža omogućuje korisnicima povezivanje kroz niz virtualnih tunela što omogućuje dijeljenje informacija preko javnih mreža sigurnije i bez ugrožavanja privatnosti, za razliku od direktnog povezivanja na mrežu [2].

Usmjeravanje internetskog prometa funkcionira tako da cijeli promet do destinacije putuje najkraćim mogućim putem. Usmjerivač (engl. Router) će informacije koje su bitne za prijenos prometa iščitati iz zaglavlja podatkovnog paketa. Upravo iz tih informacija unutar usmjerivača može se vidjeti izvor podataka, odredište prometa i lokacija tog izvora. Pomoću analiza mrežnog prometa i alata za nadzor takav promet se lako otkriva, te njihova IP adresa odredišta i IP adresa pošiljatelja, odnosno stranice koje su bile posjećivane. Ujedno s druge strane, TOR koristi još i tzv. The Onion Routing gdje se preko mnogih čvorova unutar mreže prosljeđuje internetski promet [1].

Broj TOR mreža se sastoji od oko 5800 do 6500 poslužitelja koji se nazivaju „čvorovi“ (engl. relays) [3]. Na grafu 1. prikazan je broj čvorova tijekom posljednjih pet godina.



Graf 1. Prikaz broja čvorova

Izvor: [3]

Poslužitelji su zapravo računala korisnika odnosno tzv. “volonteri“, te njih može upotrijebiti i održavati bilo koja organizacija ili pojedinac u svijetu. Usmjeravanje luka upravo iz razloga sigurnosti koristi enkripciju na aplikacijskim sloju koja se ujedno slojevito primjenjuje unutar podatkovnih paketa koji se potom šalju kroz TOR mrežu. Takvi enkripcijski podaci prilikom slanja prolaze kroz više čvorova unutar mreže. Razlog zbog kojeg enkripcijski podaci prolaze kroz više čvorova u mreži, umjesto da direktno pristigne do njegovog odredišta je taj, u slučaju da dođe do presretanja na mreži isti neće biti u mogućnosti saznati informacije o početnoj IP adresi podatkovnog paketa koji je poslan, već će mu biti prikazana samo IP adresa onoga čvora na kojem se paket trenutno nalazi [4].

Vrste čvorova koje se koriste na TOR mreži su: srednji čvor (engl. middle relay), izlazni čvor (exit relay) i most čvor (engl. bridges relay). Srednjim čvorom sav TOR promet prolazi kroz najmanje tri TOR čvora prije nego što stigne do odredišta. Izlazni čvor je ujedno i posljednji čvor u TOR krugu, te on prosljeđuje TOR promet prema krajnjem odredištu. Most čvora nisu javno prikazani, a koriste se u prevenciji cenzure u zemljama koje blokiraju pristup IP adresama svih javno prikazanih TOR čvorova [5].

Unutar TOR mreže pohranjeni su svi čvorovi u poslužiteljskom direktoriju (engl. server directory) iz kojeg slučajnim odabirnom uzimaju određeni čvorovi pomoću kojih će on putovati. Unutar TOR mreže nijedan čvor nema prikaz cijele putanje paketa već može vidjeti od kojeg čvora je zaprimio paket, te gdje je taj isti paket dalje potrebno usmjeriti. Radi zaštite TOR stavlja sloj enkripcije na IP adresu i sadržaj paketa čvora [1].

Pomoću provjere sigurnosnih ključeva slojevi enkripcije se postepeno uklanjaju kod svakog prijelaza paketa preko čvora. Korištenjem ovog načina usmjeravanja paketa odredištu će biti vidljiva samo IP adresa posljednjeg čvora u putanji paketa, odnosno čvora. Neki pružatelji usluge interneta iste odluče blokirati upravo iz razloga što su sve IP adrese čvorova TOR mreže javno dostupne. Upravo u takvim slučajevima može se koristiti tzv. mostovi, a razlog njihove uporabe je taj da za razliku od ostalih vrsta čvorova oni nisu navedeni u TOR-ovom poslužiteljskom direktoriju [1].

2.1. Analiza prometa

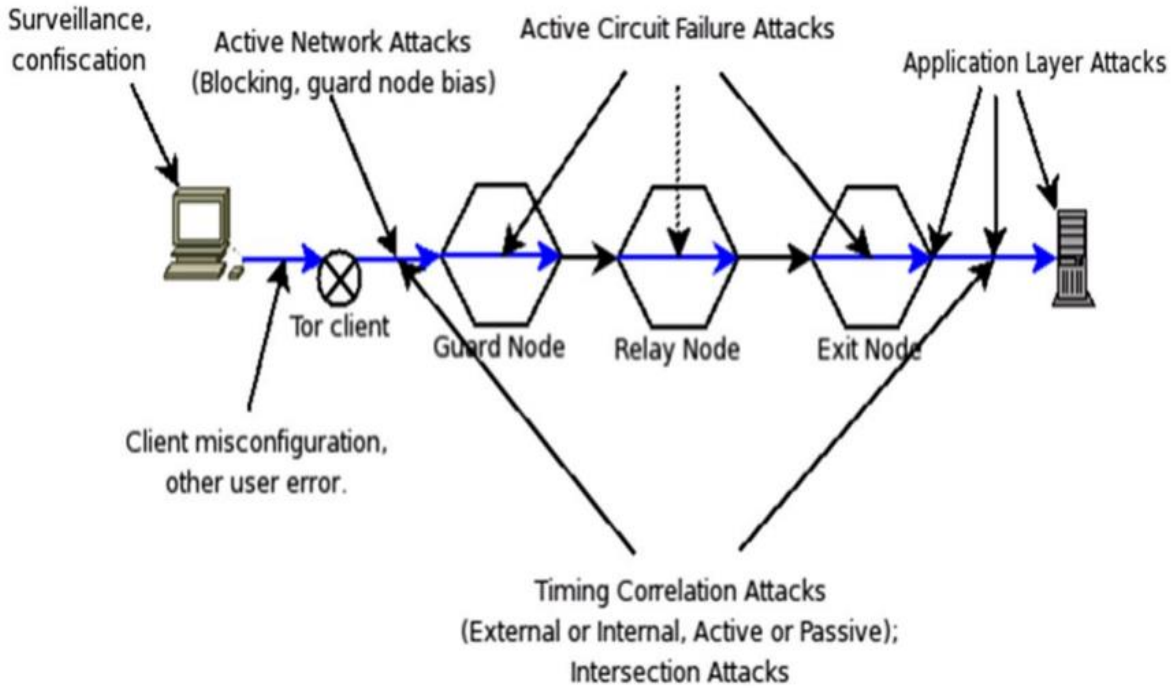
Oblik nadzora Internet aktivnosti koji omogućuje utvrđivanje odredišta i izvorišta komunikacije naziva se tzv. analiza prometa (engl. traffic analysis) od koje TOR mreža koristi štit. Takve informacije zlonamjernom korisniku mogu otkriti podatke o interesima i navikama nekog pojedinca. Trgovačke web stranice korištenjem prikupljenih informacija i podataka uz pomoć analize prometa, prilagođavaju ili mijenjaju cijene usluga i proizvoda na osnovi institucije ili zemlje iz koje neki korisnik pristupa stranici [6].

Analizom prometa također može biti ugrožena fizička sigurnost korisnika npr. ukoliko korisnik pristupa zabranjenim web stranicama iz zemalja koje imaju na vlasti diktatorski režim. Podatkovni paketi na Internetu formirani su od korisničkih zaglavlja i podataka koje se upotrebljava za njihovo usmjeravanje. Korisnički dio paketa označava podatke koji se šalju, a neki od tih primjera su: web stranice, elektronička pisma, multimedijalne datoteke itd. Moguće je saznati puno o korisnikovim aktivnostima, te o podacima koje prima i šalje uz pomoć analize prometa bez obzira što su podaci kriptirani i zaštićeni [6].

Analiza je usmjerena na zaglavlje paketa koje može otkriti njihovo odredište i izvorište, vrijeme slanja, veličinu i brojne druge podatke razlog je zbog kojeg je to moguće. Analiza zaglavlja paketa je osnovni problem za privatnost korisnika upravo iz tog razloga što primatelj može saznati gore navedene podatke o pošiljatelju, ali ujedno isto je moguće i ovlaštenim poslodavcima u komunikaciji, kao što je to npr. Internet usluga, ali povremeno i neovlaštenim napadačima [6].

Jedan od jednostavnijih oblika analize prometa je upravo presretanje paketa dok putuje od izvorišta do odredišta, te pregledavanje njihovih zaglavlja. Ujedno napredna analiza prometa koristi složene statičke metode za praćenje komunikacijskih uzoraka koje omogućuju prisluškivanje nekoliko područja Interneta, te brojne pojedince i organizacije [6].

Postoje i tvrdnje da je NSA i FBI kompromitirala TOR mreže i dodala brojne vlastite čvorove u mrežu. Veliki broj njihovih čvorova navodno je namijenjen da budu izlazni i ulazni čvorovi u TOR mreži. Ta dva čvora su kritični čvorovi u kojima se promet može izravno promatrati prije ili nakon enkripcije. Smatra se da NSA i FBI koriste upravo ovaj pristup analize prometa, a razlog je taj što nakon pristupanja ulaznim i izlaznim čvorovima na TOR mreži mogu precizno identificirati osobu koja se spaja na određenu web stranicu [4]. Na slici 1. prikazan je napad na TOR mrežu.



Slika 1. napad na TOR mrežu

Izvor: [7]

Budući da mreža čvorova podržava tzv. “volontere“ da doniraju svoje uređaje i koriste ih kao izlazne i ulazne čvorove, možemo zaključit da su glasine kako takve metode koriste agencije za provođenje zakona istinite, te oni već imaju svoje uređaje koji obavljaju ove ključne zadatke [4].

Dobar primjer je da se zamisli neka prostorije unutar koje više ljudi govori u hodu, tada uočavamo se da je teško identificirati bilo koja dva govornika. Postoje mnogi načini kako saznati identitet govornika, ujedno i izolirati bilo koji par govornika. Prva metoda koja se može upotrijebiti je vrlo jednostavna, a to je korištenjem njihovih imena. Ukoliko netko od strana koje govore spomene ime osobe s kojom razgovara na početku svojih poruka, moguće je identificirati parove koji međusobno razgovaraju. Ukoliko se jedna osoba zove npr. osoba 1 i razgovara sa drugom osobom pod imenom npr. osoba 2, osoba 1 će tijekom njihovog razgovora spomenuti ime osobe 2, te će osoba 2 spomenuti nakon toga ime osobe 1 kada bude odgovarala [4].

Međutim, pretpostavimo da ljudi u sobi ne spominju imena niti daju bilo kakve identifikacijske informacije o svojim sugovornicima. Ukoliko osobe ne daju nikakve identifikacijske informacije o njima, postaje znatno teže identificirati dvije osobe koje razgovaraju unutar prostorije. U ovom slučaju se koristi druga metoda pomoču koje ih se identificira. Prvo se mora promatrati način komunikacije između njih, tada se uočava kada oni počinju i prekidaju svoju komunikaciju. Ako osoba 1 razgovara sa osobom 2, očekujemo da će osoba 2 početi odgovarati kada osoba 1 prestane govoriti. Znači, kada osoba 2 govori osoba 1 će biti tiho, a kada osoba 1 govori osoba 2 će biti tiho. Ukoliko oni i govore nerazumnim jezikom postojat će način na koji će se moći reći da osoba 1 razgovara sa osobom 2 [4].

Ovi primjeri suptilno objašnjavaju rad i na koji način radi analiza prometa. Kada njuškalo (engl. snooper) primijeti da dvije osobe komuniciraju, u TOR-ovom slučaju to su korisnik i poslužitelj internet stranice, moguće je saznati ili utvrditi njihovu komunikaciju pomoću analize prometa. Najvažniji čvorovi unutar TOR mreže koje je potrebno nadgledati su ulazni i izlazni čvorovi. Bayesova vjerojatnost je metoda koja se koristi za prikupljanje dokaza da bi se potvrdila komunikacija tj. razgovor između dviju osoba. Ta metoda se upotrebljava kao standard za prikupljanje dokaza [4].

Istražitelji u većini slučajeva moraju suziti dokaze koje imaju kako bi se pronašli počinitelji zločina. To isto vrijedi i za TOR mrežu unutar koje ima jako puno korisnika i ako je samo jedan kriv za zločin ostale treba polako eliminirati iz kruga fokusa tijekom istrage. Nakon nekoliko ponavljanja elimininiranja onih koji imaju malu vjerojatnost da su odgovorni za zločin, ostat će nekolicina koja ima vrlo veliku vjerojatnost da su počinitelji zločina. TOR mreža radi dobar posao koji omogućuje svojim korisnicima anonimnost, te stoga istrage na dark web-u nisu toliko jednostavne kao one na površinskim mrežama. Na površinskoj mreži istražiteljima je vrlo lako pronaći pomoću IP adrese uređaja i lokaciju istog. Istražitelji mogu jednostavno presresti promet između počinitelja i poslužitelja, te jednostavno iščitati zaglavlja paketa kako bi dobili informacije o odredištu i izvorištu [4].

Sve u svemu, velika slabost TOR-a je analiza prometa kao što je to vidljivo iz tekstova gore. Upotrebljavaju je agencije za provođenje zakona na TOR mreži, ali i kriminalci. Jedini faktor koji ometa uspjeh TOR-a su cijena i troškovi koji se ulažu u rad TOR mreža. Skupo je posjedovati poslužitelje koji ispunjavaju uvjete da budu ulazni i izlazni čvorovi. Država može priuštiti kupnju skupih poslužitelja namijenjenih za tu svrhu, ali ujedno i kriminalne organizacije isto tako mogu uložiti ogromne iznose stečene nezakonitim putem kako bi kupili slične poslužitelje i računala. Međutim za neke je to preskupo upravo iz razloga što treba imati kontrolu nad velikim brojem ulaznih i izlaznih čvorova kako bi se spriječilo uplitanje, povezivanje, prisluškivanje i iščitavanje tajnih informacija i podataka [4].

2.2. Distribuirana anonimna mreža

Transakcije unutar TOR mreže distribuiraju se preko većeg broja posrednika od kojih nijedan ne poznaje odredište niti izvorište što onemogućava rad analize prometa. TOR mreža prenosi internetski paket podataka kroz niz čvorova koji putuju od izvora paketa pa sve do odredišta. Svaki čvor unutar TOR mreže je neovisan i ne mogu znati cijeli put podataka paketa. Što znači da nitko ne može ukazati na vezu (engl. link) između izvora i odredišta. U isto vrijeme kako bi se osigurala sigurnost i privatnost TOR korisnika (engl. users) nasumično se odabiru čvorovi iz TOR mrežnog sustava kako bi utvrdio put od izvora do odredišta. TOR korisnici nakon nekog vremena mijenjaju odabrane čvorove, a razlog mijenjanja očituje se u činjenici da postavljanjem novih čvorova postavljamo novi put i tako sprječavamo praćenje puta [8].

TOR čvor je distribuirani mrežni čvor koji ima ulogu usmjeravanja u TOR mreži. U anonimnoj komunikaciji unutar Tor mreže postoje tri vrste čvorova, a to su [9]:

- Middle relays – sav TOR promet prolazi kroz najmanje tri TOR čvora prije nego što dođe na odredište. Middle čvorovi su prva dva relaja koji zaprimaju promet, te ga prosljeđuju dalje.
- Bridges relay – nisu javno izlistani, a koriste se u sprječavanju cenzura u zemljama koje blokiraju pristup IP adresama svih javno izlistanih TOR čvorova.
- Exit relay – prosljeđuje TOR promet prema krajnjem odredištu.

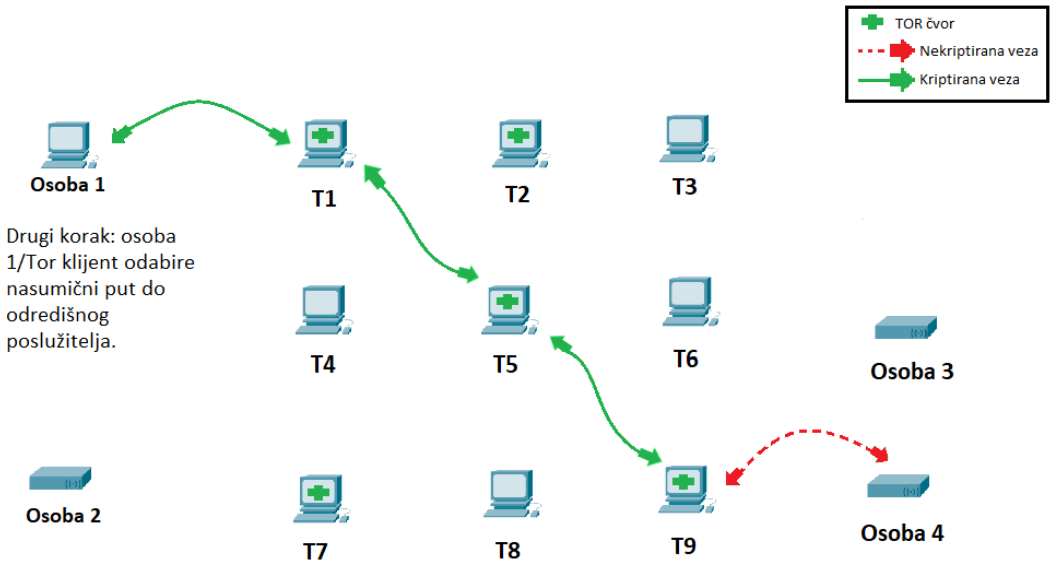
Čvor poslužitelja može jedino posjećivati odredišne web stranice, te je također sposoban prenijeti druge podatke paketa kroz TOR čvor. Poslužitelj može pokrenuti TOR usmjerivač, te čim to učini može postati posrednički čvor za sve druge TOR rutere unutar mreže. Druga vrsta TOR mreže je klijentski čvor (engl. client node). On može samo započeti TOR usmjerivač, ali ne može prenijeti čvorove. Zatim imamo i TOR čvor koji je poznat kao imenički poslužitelj (engl. Directory server) koji pohranjuje informacije o čvorovima poslužitelja koji su dostupni u TOR mreži [8].

Slika 2. Izgradnja liste TOR čvorova

Izvor: [8]

Na slici 2. prikazana je izgradnja liste TOR čvorova. Liste TOR čvorova nastaju tako da osoba 1, koja je TOR klijent, želi posjetiti odredište tj. osobu 4 koja je u stvari web stranica. Između osobe 1 i osobe 4 postoji mnogo TOR poslužitelja odnosno čvorova poput osobe 2 i osobe 3. Kako bi osoba 1 bila u mogućnosti komunicirati sa web stranicom osobe 4, osoba 1 treba prikupiti sve potrebne informacije o TOR-ovim čvorovima poslužitelja. U ovom slučaju osoba 2 je imenički poslužitelj i on ispunjava ovaj zahtjev. Onog trenutka kada osoba 1 pronađe potrebne podatke o TOR-ovom poslužitelju započinje uspostavljanje krugova koji će voditi do odredišta [8].

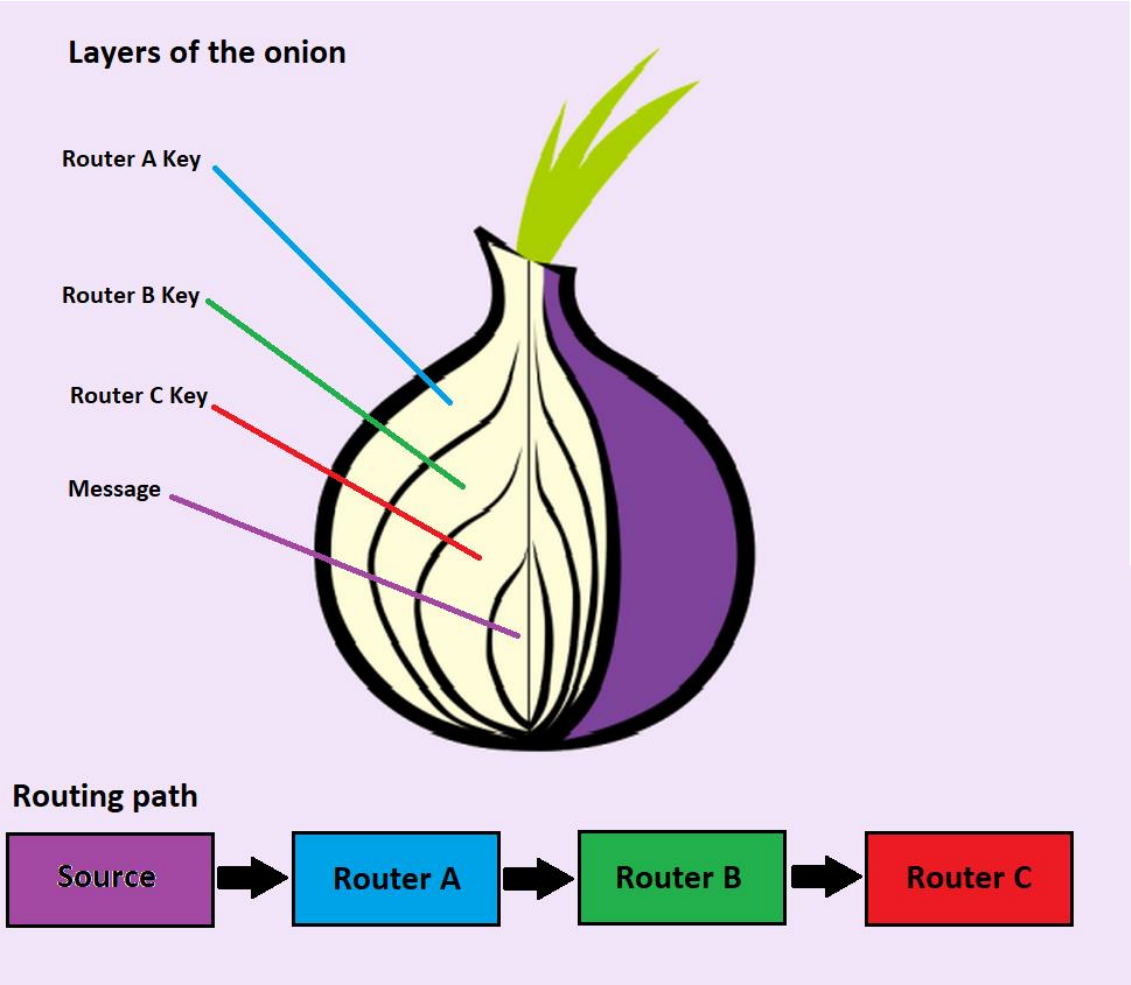
Sada kada TOR klijent ima sve potrebne informacije o TOR čvorovima vrijeme je za izgradnju sklopova. TOR klijent uspostavlja TOR krug s 3 druga TOR čvora. Krug kroz koji će se kretati podaci je postavljen, te će imati i privatni ključ. Krug je napravljen kao jedan skok u jednom trenutku. Svaki TOR čvor zna samo informacije od prethodnog čvora. Sve ostale informacije i podaci se ne dostavljaju na sljedeće čvorove. Nakon što se krug završi postavljen je čvor klijenta i započinju se slati paketi podataka. TOR klijent može uspješno prenijeti tražene podatke apsolutno sigurno i bez otkrivanja osjetljivih informacija poput IP adresa ili podataka korisnika [8]. Na slici 3. prikazan je prijenos podataka kriptiranih veza između nasumično odabranih poslužitelja.



Slika 3. Prijenos podataka kriptiranih veza između nasumično odabranim poslužiteljima

Izvor: [8]

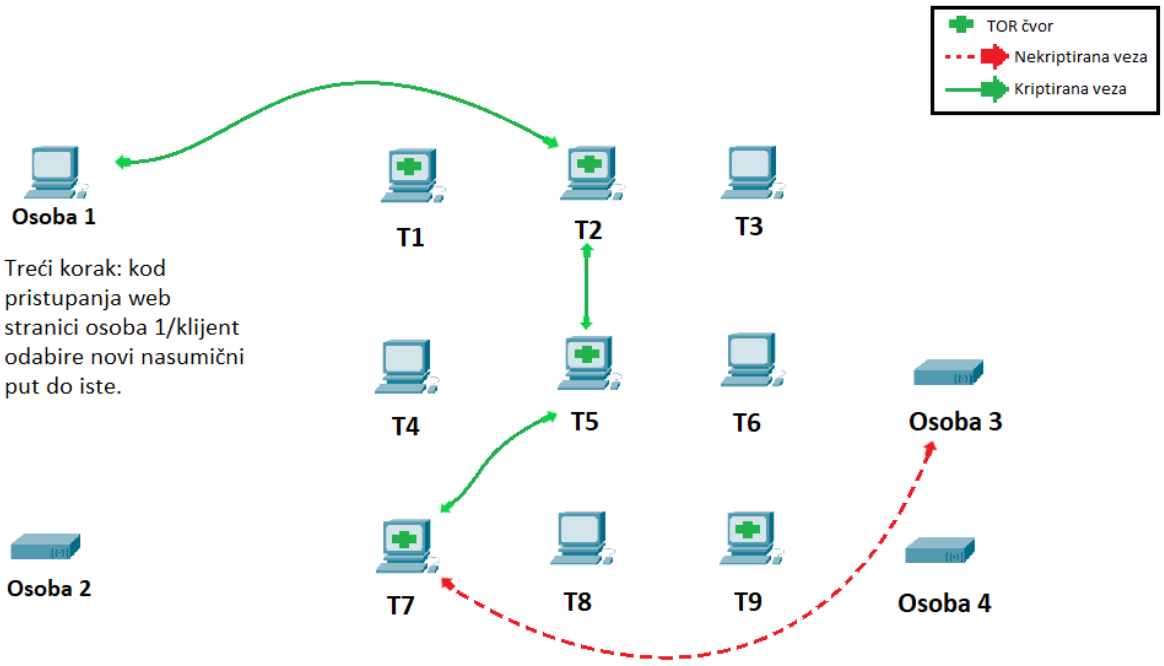
Paketi podataka koje prenosi TOR klijent su kao troslojni luk rutera (engl. onion router). Jedan skok kroz krug može omotati samo jedan sloj svojim privatnim ključem. Svaki skok kroz TOR čvor poznaje samo svoj prethodni i nasljedni čvor [8]. Na slici 4. prikazana je struktura paketa podataka TOR mreže uz pomoć slojeva luka.



Slika 4. Struktura paketa podataka u slojevima luka

Izvor: [8]

U krugu TOR-a konačno se kreira posrednički čvor ili poslužiteljski čvor koji je definiran kao izlazni čvor. Upravo kao što je ranije opisano kroz cijeli put pakirani podaci su osigurani kroz prijenosni sloj sigurnosnih protokola [8].



Slika 5. Odabir nove nasumične putanje

Izvor: [8]

Kao što je prikazano na slici gore, kada osoba 1 šalje po prvi put podatkovne pakete koristi krugove kosi se sastoje od 3 čvora. U slučaju da osoba 1 sada želi posjetiti drugu web stranicu, TOR će za nju postaviti novi krug koko bi zaštitio anonimnost osobe 1 [8]. Na priloženoj slici 5. prikazan je princip rada Onion komunikacije i način na koji osoba 1 pristupa osobi 3, to jest nekoj novoj web stranici. Princip rada prikazan je koracima, a koraci su [9]:

1. TOR klijent/osoba 1 šalje zahtjev prema TOR web stranici.
2. Osoba 1 šalje zahtjev TOR direktoriju za TOR čvorove koji će činiti rutu do osobe 3 ili TOR web stranice.
3. TOR direktorij zatim odgovara s podacima o najmanje tri TOR čvora koji će činiti rutu kao što je prikazano na slici, a ta ruta će sadržavati: osoba 1 - T2 - T5 - T7 – TOR web stranica. Dodatno se šalje Circuit ID što predstavlja identifikator komunikacijske sesije. T2 i T5 su middle čvorovi, a T7 je exit čvor.

4. Klijent i tri TOR čvora zatim uspostavljaju simetric key kriptografiju koja će se koristiti za kriptiranje sadržaja kojeg želimo poslati prije slanja na linkove. Svaki TOR čvor ima svoj ključ samo klijentsko računalo ima sve ključeve.
5. Klijent zatim kriptira sadržaj paketa za svaki link na ruti osoba 1 - T2 - T5 - T7 - web stranica u različitim slojevima, krenuvši odostraga: T7 - web stranica, T5 - T7, T2 - T5, osoba 1 - T1.
6. Osoba 1 šalje tako kriptirani paket prethodno definiranom rutom.
7. Svaki čvor prilikom dobivanja paketa može vidjeti samo one informacije koje ga se tiču upravo iz razloga što nema ključeve za ostale čvorove.
8. Nakon što paket stigne na čvor T7, paket se dekriptira i takav se šalje do web stranice. Ovo je jedini link na ruti gdje paket nije kriptiran jer se web stranica ne nalazi u TOR mreži.
9. Web stranica šalje odgovor kako web stranica ne zna izvorni čvor, te vrača paket prema čvoru T7.
10. Zatim čvor T7 provjerava svoje zapise utvrđuje da se radi o CID 7, te zna koji je bio prethodni čvor u toj ruti (čvor T5). Prije nego što šalje paket kriptira svojim ključem.
11. Postupak se ponavlja na svakom čvoru T5 i T2 dok odgovor ne stigne do TOR klijenta/osoba 1.
12. Klijent po primitku paketa, enkripciju skida „sloj po sloj“ koristeći sva tri enkripcijska ključa [9].

TOR se može definirati kao učinkoviti alat za enkripciju podataka tijekom prijenosa podataka, te postiže anonimnost i sigurnost od neobičnih prijenosnih ruta. Anonimni komunikacijski sustavi dizajnirani su da zaštite korisnika od zlonamjernih mreža i web stranica koje pokušavaju prikupiti skrivene podatke i informacije [8].

2.3. Skrivene usluge

TOR skrivene usluge (engl. TOR hidden services) ili usluge luka (engl. onion services) su stranice i mrežna mjesta koja nisu dostupna za korištenje putem standardnih mrežnih pretraživača već im se može pristupiti isključivo putem TOR mreže. TOR sustav nudi različite usluge koje omogućavaju zaštitu privatnosti, odnosno skrivanje identiteta korisnika. Spomenute usluge obuhvaćati održavanje poslužitelja sustava trenutnih poruka ili objavljivanje web stranica. Ostali korisnici mogu pristupiti takvim skrivenim uslugama korištenjem TOR-a pristupnih točaka bez poznavanja identiteta pružatelja usluge. Upravo na ovaj način može se postaviti web stranica na kojoj korisnici mogu bez straha od cenzure i zabrana objavljivati vlastite sadržaje, a da pri tome nije moguće otkriti tko je osoba koja je postavila takvu stranicu niti tko su korisnici koji na njoj objavljuju sadržaje [6].

Postoje četiri cilja za dizajnirane TOR skrivenih usluga, a to su [10]:

- Kontrola pristupa (engl. access – control) – izdavač mora filtrirati dolazne zahtjeve tako da napadači ne mogu preplaviti usluge stvaranjem većeg broja veza za povezivanje.
- Pouzdanost (engl. robustness) – izdavač mora imati mogućnost sakrivanja identiteta duže vrijeme i usluge ne bi trebale biti vezane samo s jedinim onion usmjerivačem. Ujedno izdavač bi trebao biti u mogućnosti preseliti usluge na različiti onion usmjerivač.
- Otpornost (engl. resistance) – napadači ne bi smjeli uokviriti sastanak usmjerivača tako što će nuditi ilegalne usluge koje će natjerati promatrača da povjeruje da je usmjerivač stvorio tu uslugu.
- Transparentnost aplikacije (engl. application transparency) – prisiljavanje korisnika da pristupi usluzi korištenjem TOR mreže, ali isto tako ne bismo trebali prisiljavati izdavače da naprave bilo kakve promjene u primjenama.

2.3.1. Usluge e-trgovine

Svaki posao unutar TOR mreže koji za svoj pothvati ima zarađivanje novca, bez obzira jeli legalan ili nezakonit, je usluga e-trgovine (engl. e-commerce services). Na dark web-u ima veliki niz e-trgovina unutar kojih se prodaje droga, oružje, ukradene kreditne kartice, lažne valute, lažne osobne iskaznice, hakirani PayPal računi, lažne vozačke dozvole, zloćudni softveri, kupovanje pratitelja za sve društvene mreže, pa sve do hrane, odjeće, obuće, kućnih potrepština itd. Međutim, većina crnih tržišta (engl. black market) koji su uspostavljeni na TOR-u i bave se nezakonitom prodajom su praćene i ukinute od strane agencija koji se bave provođenjem zakona na dark web-u kao što su to npr. FBI, NSA, CIA [4].

2.3.2 Elektronička pošta

TOR mreža također daje mogućnost primanja i slanja elektroničke pošte (engl. email) na mreži, a pritom osigurava anonimnost primatelja i pošiljatelja. Upravo zbog anonimnosti koja se pruža korisnicima koji imaju osjetljive informacije i žele spriječiti njihovo presretanje ili prosljeđivanje drugima [4].

Elektronička pošta u TOR mrežama ima i neke od najbitnijih uloga, a to je omogućavanje zviždačima, vladinim špijunima i građanima koji se nalaze unutar zemlje koja ima stroga diktatorska prava da sigurno i anonimno prenose informacije i podatke agencijama za provođenje zakona kao što su to FBI, NSA i CIA. Međutim, zbog anonimnosti i sigurnosti koje pruža slanje elektroničke pošte unutar TOR-a dolazi do zloupotrebljavanja [4].

Te na taj način kriminalci i teroristi mogu komunicirati na načine na koje im se ne može lako ući u trag i otkriti razgovore koje su vodili o mogućim napadima, prodaji ilegalnih stvari i razmjeni obavještajnih podataka [4].

2.3.3. Pohranjivanje datoteke

TOR mreža ujedno nudi i usluge pohranjivanja datoteka (engl. file storage) korisnicima, tj. mjesto gdje korisnici mogu čuvati svoje osjetljive digitalne datoteke sigurno bez brige o njihovoj sigurnosti i privatnosti. Razlog zbog kojeg je TOR mreža bolja za pohranu je taj da kod pohrane u oblaku (engl. cloud storage) upravo radi direktne povezanosti dolazi do rizika za sigurnost i anonimnost budući da hakeri, dobavljači oblaka i agencije za provođenje zakona mogu vrlo lagano pokušati otvoriti datoteke. Najčešće korišteni sustav za pohranu datoteka na TOR-u zove se Free Haven. Izgrađen je od strane studenata MIT-a kako bi osigurao da podaci koji će se spremati u ovu aplikaciju budu sigurni, pouzdani, anonimni i stalno dostupni korisnicima [4].

2.3.4. Tražilice

Baš kao što standardni Internet ima Google, Yahoo Search, Bing i druge, tako i TOR mreža ima svoje tražilice (engl. search engines). Neke od tražilica na TOR mreži su: DuckDuckGo, Ahmia, BTDigg i Searx. Razlozi zbog kojih se preferiraju tražilice sa dark web-a su ti što osiguravaju korisnicima zaštitu od dijeljenja informacija o svojoj lokaciji, Internet aktivnosti i povijesti pretraživanja što korisnicima daje osjećaj sigurnosti. Internet tražilica kao što je to Google optužene su za prikupljanje podatka, informacija i praćenje pretraživanja korisnika koje bi se poslije koristile za postavljanje preporučenih reklama na temelju onoga što neki korisnik pretražuje [4].

2.3.5. Arhiva vijesti

Postoje dijelovi TOR mreže koji sadrži arhivu vijesti (engl. news archives) i drugih dokumenata. Može im se pristupiti ukoliko se želi čitati starije i novije vijesti bez napuštanja TOR mreže. Neke tvrtke poput New York Times-a koje se bave objavom sadržaja i novosti iz svijeta, također objavljuju redovno svoj sadržaj na TOR mrežama. Druge stranice za arhiviranje vijesti uključuju DeepDotWeb i BuggedPlanet [4].

2.4. Onion usmjeravanje

Funkcionalnost TOR mreže se temelji na već opisanom tzv. the onion routing, a riječ je o tehnici anonimne komunikacije unutar neke računalne mreže koju su razvili Paul Syverson, Michael Reed i David Goldschlag. Onion usmjeravanje temelji se na miješanim mrežama (engl. mix networks) koje je napravio David Chaum, ali također uključuje brojne nadogradnje i izmjene ove tehnike od kojih je uvođenje koncepta onion usmjerivača najznačajnije. Jednu od stvari koju provode usmjerivači je enkripcija podataka koja se koristi za usmjeravanje u nekoliko enkripcijskih slojeva [6].

Svrha onion usmjeravanje je očuvanje privatnosti primatelja i pošiljatelja poruke, te ujedno i zaštita sadržaja samo poruke prilikom putovanja kroz mrežu. Kako bi se omogućila zaštita i anonimnost korisnika koristi se Chaumovih miješana kaskada. Funkcionira tako da poruka kroz mrežu putuje preko niz posrednih poslužitelja (engl. proxy server) koji se u ovom slučaju nazivaju onion poslužitelji, te oni zapravo spomenutu poruku onda preusmjeravaju na nepredvidljiv način. Kako bi se onemogućilo neovlašteno pregledavanje sadržaja te poruke, tzv. prisluškivanje (engl. eavesdropping) poruka se prije samog prijenosa među poslužitelje kriptira [6].

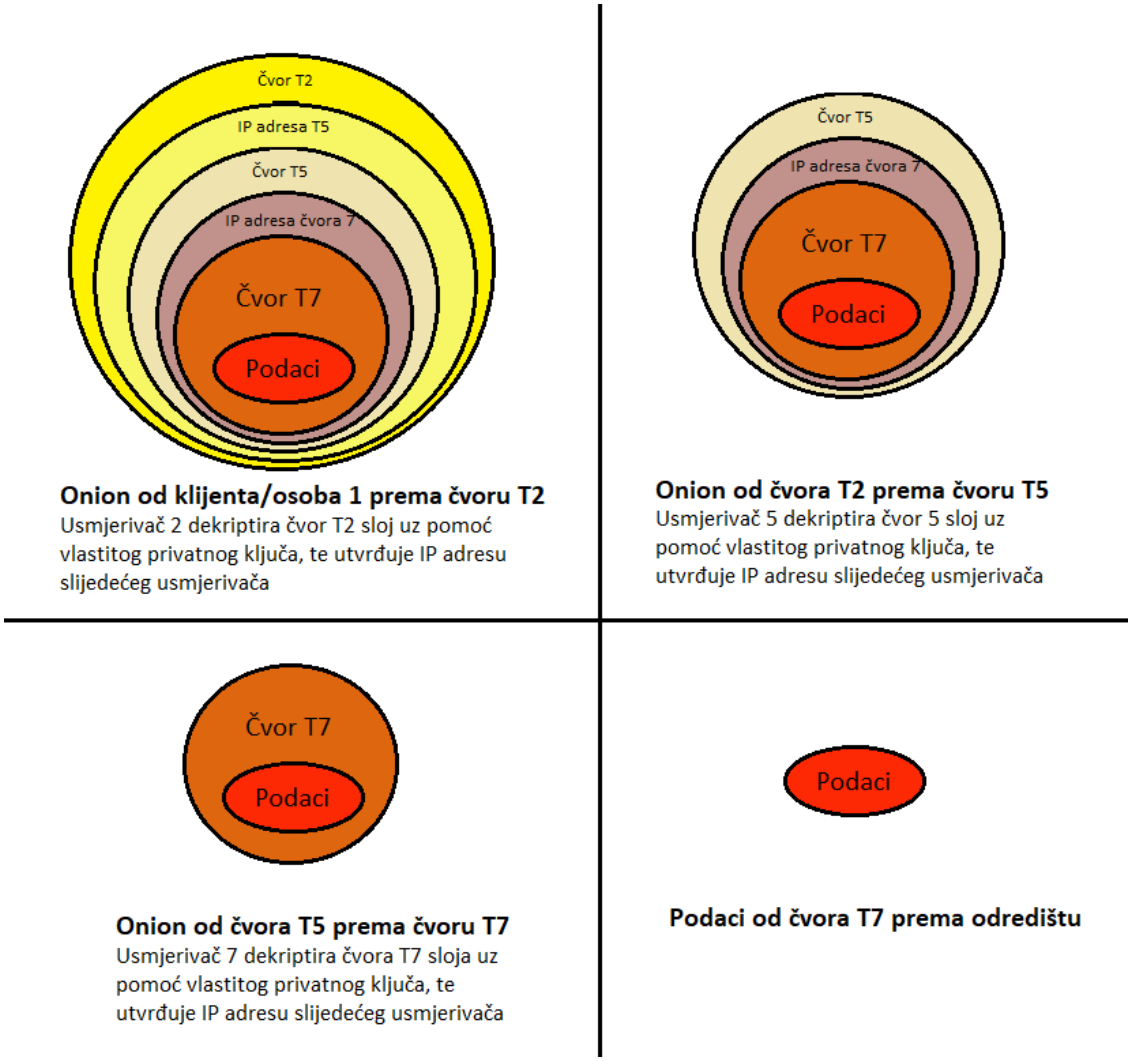
Najosnovnija i najbitnija prednost koju donosi općenito miješana kaskada i onion usmjeravanje je činjenica da bi se uspostavila anonimna komunikacija nije nužan ispravan rad apsolutno svih poslužitelja preko kojih je ostvarena veza. Ukoliko napadač i uspije postići pristup jednom ili više onion poslužitelju korisnikova anonimnost na mreži nije ugrožena. Razlog zbog kojeg je poruka i dalje sigurna je taj što se u mreži onion usmjeravanja poruka višestruko kriptira. Način na koji bi se mogao saznati put kojim se poruka kretala bio bi da se stekne kontrola nad svim poslužiteljima [6].

2.4.1. Podatkovne strukture za usmjeravanje

Podatkovne strukture (engl. routing onions) se koriste u onion routing mreži, te se uz pomoć podatkovne strukture uspostavlja veza za slanje poruke. Kako bi formiranje ovakve strukture bilo moguće početni usmjerivač nasumično odabire određeni broj onion usmjerivača i potom šalje svakom poruku koja će sadržavati simetrični ključ za dekriptiranje poruka i upute za slanje poruke sljedećem usmjerivaču [6].

Sve poruke uključujući i izvornu poruku kriptirane su privatnim ključem odgovarajućeg usmjerivača. Podatkovna struktura je građena na način da dolazak do unutrašnjeg sloja gdje se nalaze poruke, informacije ili podatci zahtjeva prvo dekripciju vanjskih slojeva kao luk „sloj po spoj“ .Tek nakon toga može se pristupiti unutrašnjosti [6].

Korištenu podatkovnu strukturu najbolje opisuje analogija s lukom (engl. onion - luk). Svaki usmjerivač nakon što zaprimi poruku „guli“ jedan „sloj po sloj“ kao „luk“ korištenjem vlastitog privatnog enkripcijskog ključa, te tako može doći do podataka koji su mu potrebni za usmjeravanje ostataka podatkovne strukture. Ostatak koji se proslijedi sastavljen je od uputa za usmjeravanje i poruke koja je namijenjena svim sljedećim usmjerivačima. Posljednji usmjerivač na toj vezi zatim uklanja posljednji enkripcijski sloj, te odredištu dostavlja izvornu poruku [6]. Na slici 6. prikazana je podatkovna struktura za usmjeravanje.



Slika 6. Podatkovna struktura za usmjeravanje, onion

Izvor: [6]

Upravo radi ovakve strukture usmjeravanja potpuni sadržaj podatkovne strukture moguće je otkriti jedino ako ona pravilnim redoslijedom prođe kroz sve čvorove već utvrđene veze [6].

2.4.2. Odgovaranje na poruku

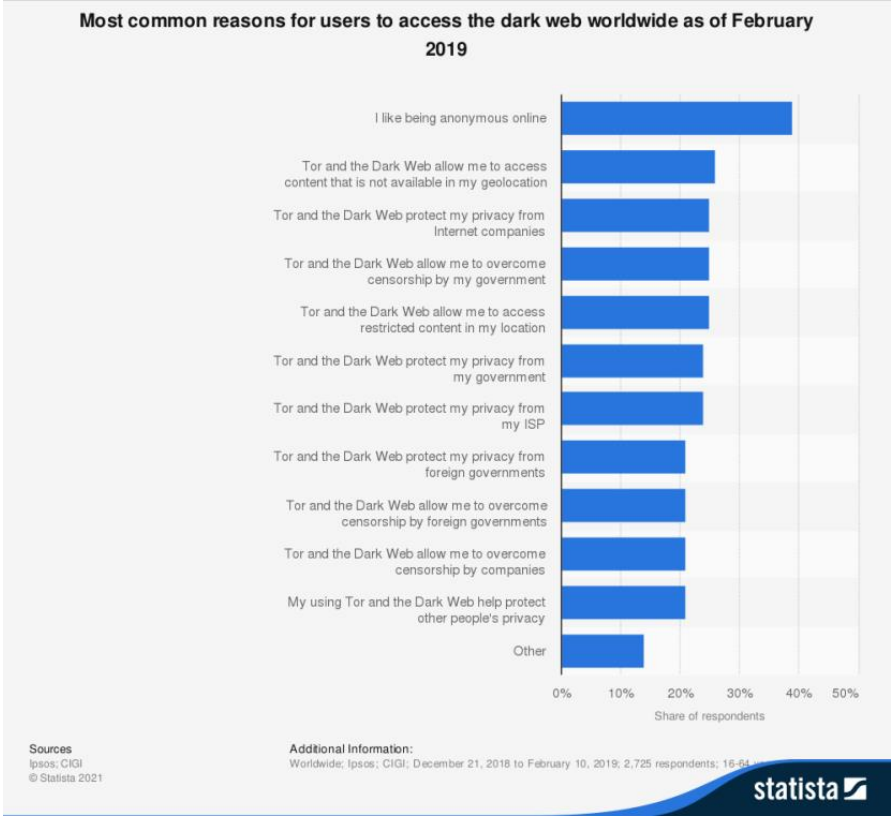
Onion usmjeravanje omogućuje slanje poruke primaocu, ali i mogućnost da korisnik koji je primio poruku šalje odgovor pošiljatelju bez da se otkrije identitet od oba korisnika. To je moguće upravo zbog korištenja podatkovne strukture za odgovaranje na poruke (engl. reply onion) [6].

Osnovna razlika između podatkovne strukture za odgovaranje na poruke i podatkovne strukture za usmjeravanje je u tome što onion za odgovaranje sadrži opis puta koji će biti korišten za natrag prema pošiljatelju. Kako bi započela dvosmjerna komunikacija između pošiljatelja i primatelja, pošiljatelj stvara onion i onion za odgovaranje [6].

Primatelj dobiva skupa s poslanom porukom i onion za odgovaranje, a kojega je moguće iskoristiti za slanje odgovora na poruku od pošiljatelja. Identitet pošiljatelja za odgovaranje su zaštićeni maksimalno višeslojnom enkripcijom što znači da bi se probila zaštita i otkrila poruka potrebno je imati privatne ključeve ili izvesti uspješan napad na sve usmjerivače koji se nalaze na povratnoj vezi [6].

3. Korištenje Dark web (TOR) mreže

Korištenje Dark web (TOR) mreže moguće je koristiti na Windows, Linux, Mac OS X, Unix i BSD operacijskim sustavima. Preuzimanje, instalacija i pokretanje Dark weba na većini operativnih sustava je jednaka. TOR koristi P2P (engl. peer-to-peer) povezivanje, a to je zapravo decentralizirani komunikacijski model u kojem svaka stranka može započeti komunikaciju s drugom strankom, te svaka stranka ima iste sposobnosti. P2P model pošiljateljima i primateljima u procesu daje mogućnost da se u isto vrijeme ponašaju kao klijent i server, a takav model se razlikuje od modela server/klijent u kojem klijent zahtjeva pristup serveru. TOR ne samo da se koristi za komunikaciju već se koristi za kupovinu i prodaju preko Interneta zbog pojačane sigurnosti [11]. Na grafu 2. prikazani su najčešći razlozi korisnika za pristupanje na Dark web mrežu diljem svijeta u 2019 godini.

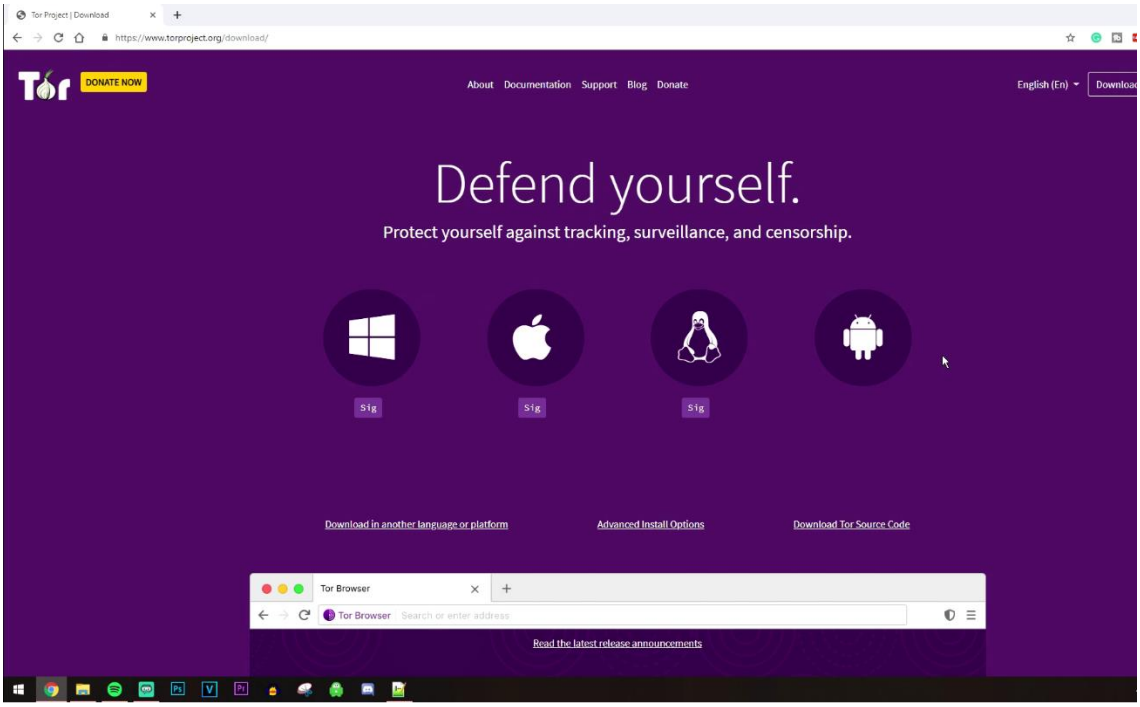


Graf 2. Najčešći razlozi korisnika za pristupanje na Dark web

Izvor: [12]

3.1. Preuzimanje Dark web (TOR) mreže na Windowsu i Mac operativnom sustavu

Prije samog početka rada u Dark webu potrebno je na računalo skinuti TOR preglednik (engl. TOR browser) koji će nam omogućiti anonimnost i sigurnost na Dark webu. Na slici 7. prikazano je na kojoj se web stranici se skida TOR preglednik.

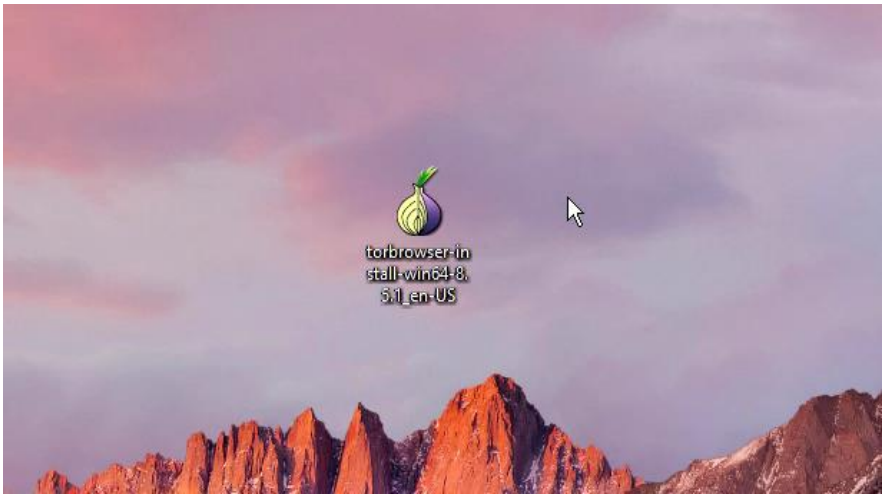


Slika 7. Web stranica za skidanje TOR preglednika

Nakon što korisnik uđe na stranicu, da bi skinuo TOR preglednik potrebno je odabrati za koji operativni sustav korisnik želi skinuti taj TOR preglednik u ovom primjeru korisnik odabire Microsoft Windows. Nakon toga program za instalaciju se preuzima.

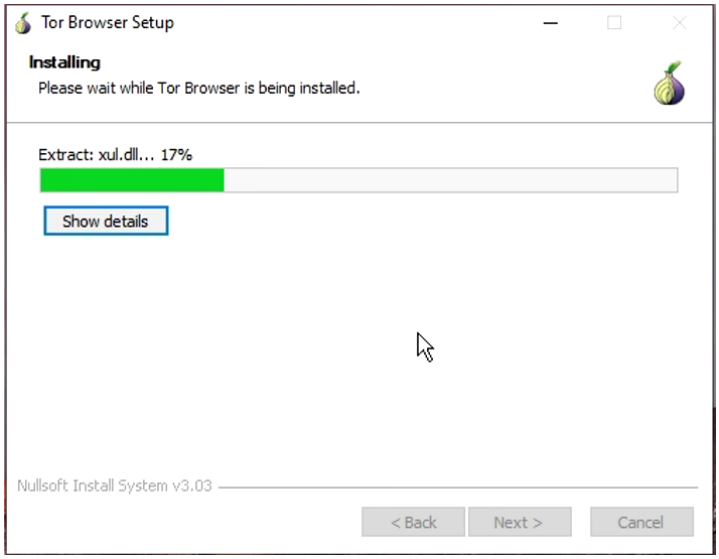
3.2. Instalacija Dark web (TOR) mreže na Windowsu i Mac operativnom sustavu

Korisnik klikne na ikonu kako bi započeo instalaciju programa TOR preglednika. Na slici 8. prikazan je skinuti program za instalaciju TOR preglednika.



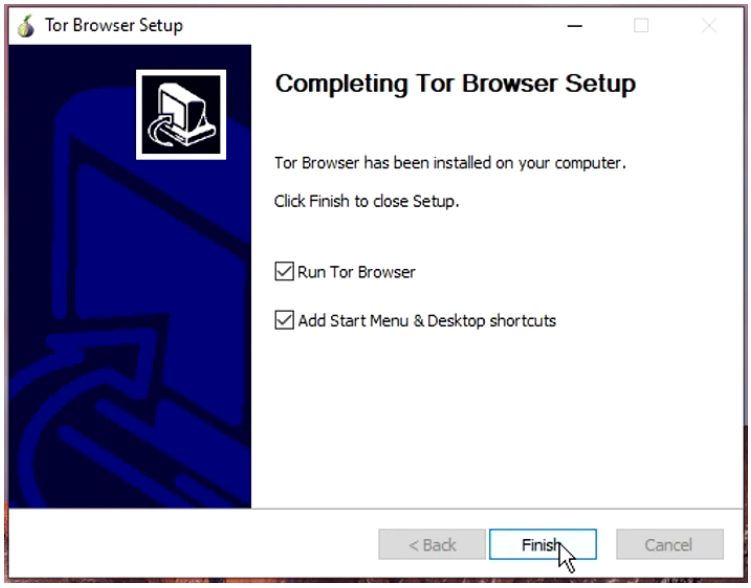
Slika 8. Program za instalaciju TOR preglednika

Zatim korisnik mora pokrenuti program za instalaciju kako bi instalirao TOR preglednik na svoje računalo. Na slici 9. prikazana je instalacija TOR preglednika.



Slika 9. Instalacija TOR preglednika

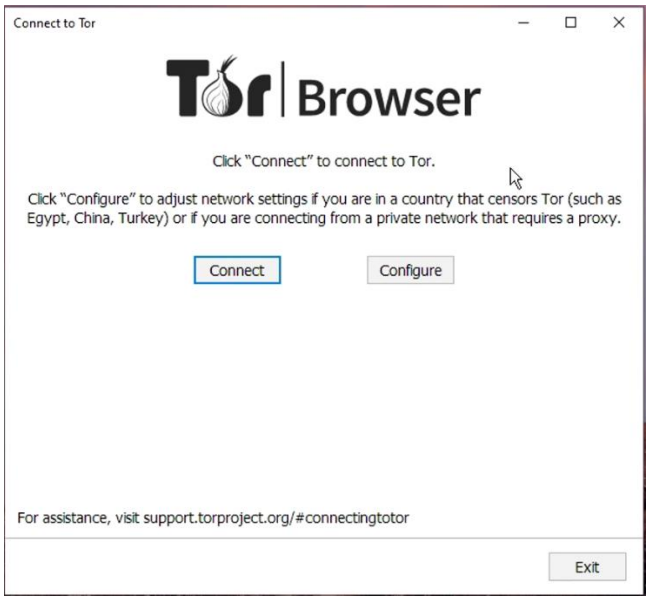
Nakon što instalacija završi korisnik klikne završi (engl. finish) kako bi se pokrenuo TOR preglednik. Na slici 10. prikazan je završetak instalacije.



Slika 10. Završetak instalacije

3.3. Povezivanje na Dark web (TOR) mreže na Windowsu i Mac operativnom sustavu

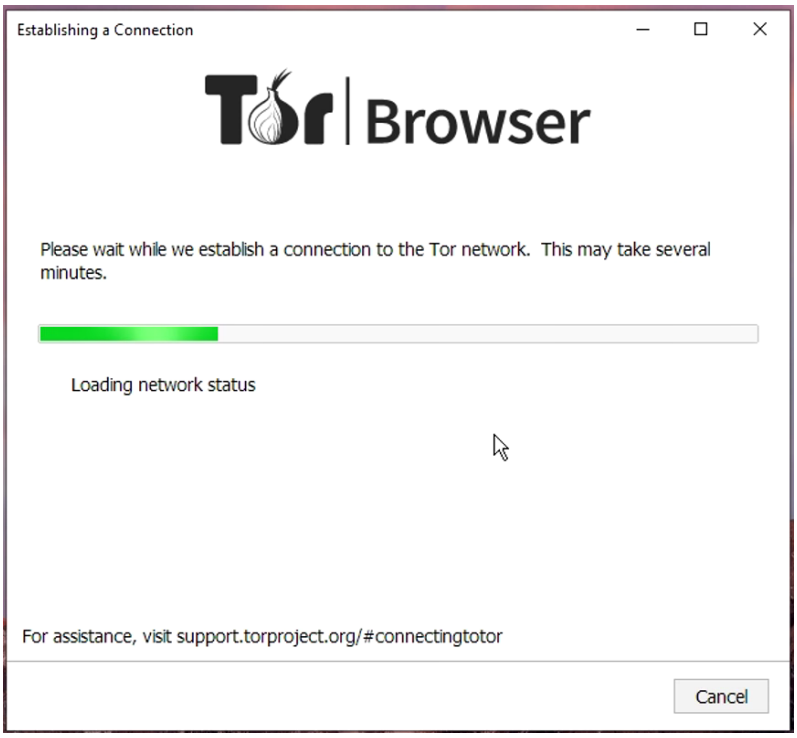
Za povezivanje na TOR mrežu, te kako bi se korisnik povezao sa TOR preglednikom potrebno je kliknuti na spoji (engl. connect). Na slici 11. prikazano je spajanje na TOR mrežu.



Slika 11. Spajanje na TOR mrežu

Zatim se obavlja spajanje na TOR mrežu. U ovom koraku nisu potrebne nikakve konfiguracije (engl. configurations) upravo iz razloga što TOR sam konfigurira sve, te

korisniku pruža najbolju zaštitu i anonimnost. Na slici 12. prikazano je povezivanje i konfiguracija TOR preglednika.



Slika 12. Povezivanje i konfiguracija TOR preglednika

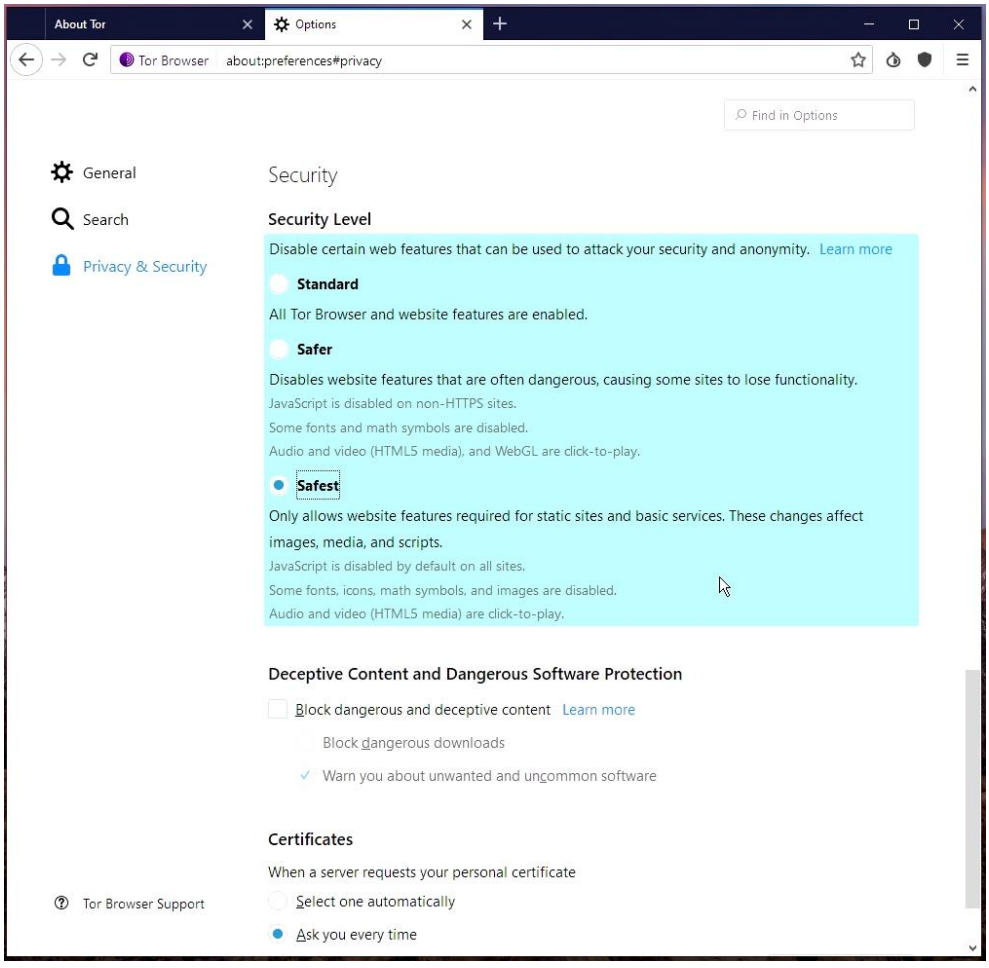
3.4. Pokretanje Dark web (TOR) mreže na Windowsu i Mac operativnom sustavu

Nakon konfiguracije povezani smo na TOR mrežu, te se pali TOR preglednik pomoću kojega korisnik može pretraživati Dark web. Međutim, prije početka pretraživanja na TOR pregledniku korisnik mora u postavkama (engl. settings) odrediti koju razinu sigurnosti želi koristiti.

Razine zaštite su:

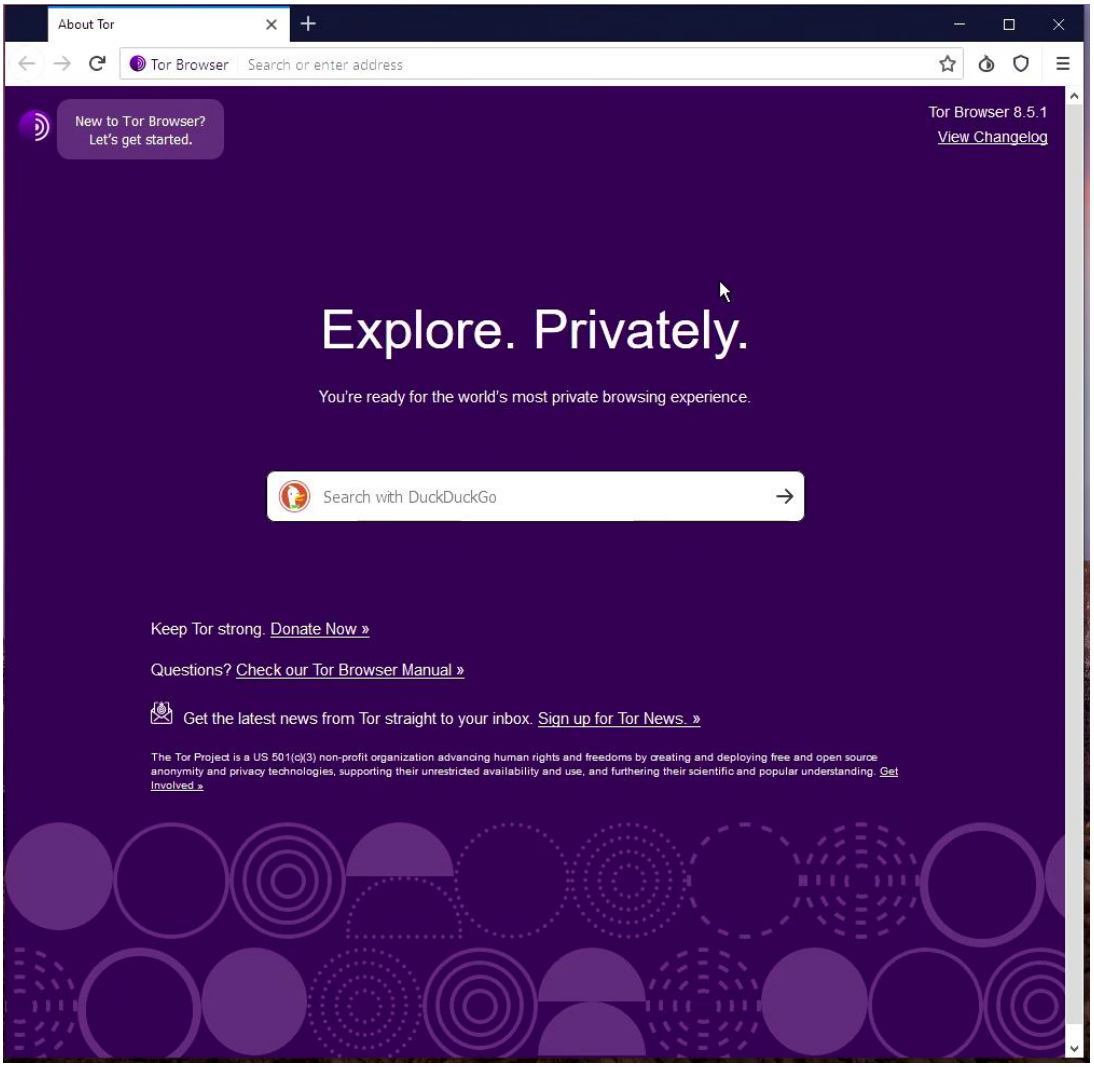
- Standardna zaštita (engl. standard security) – omogućava sve karakteristike TOR preglednika i web stranice.
- Sigurnija zaštita (engl. safter security) – onemogućuje karakteristike web stranice koje su često opasne, zbog čega neke stranice gube funkcionalnost.
- Najsigurnija zaštita (engl. safest security) – dopušta samo karakteristike web stranice koje su potrebne za statičke web stranice i osnovne usluge. Ove promjene utječu na slike, medije i skripte.

Na slici 13. prikazane su postavke za odredit razinu sigurnosti.



Slika 13. Odabir razine sigurnosti

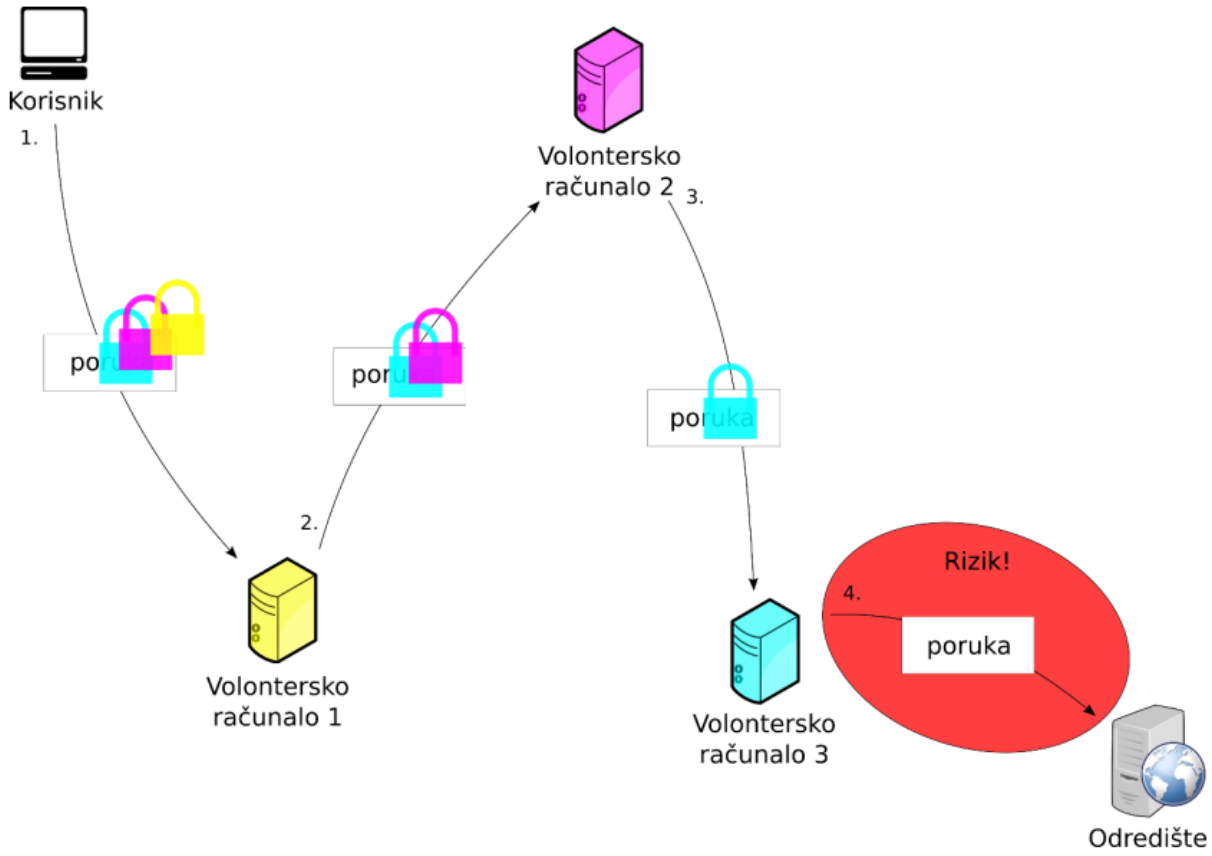
Kada je korisnik odabrao razinu zaštite koju želi koristiti spreman je za pretraživanje na TOR pregledniku, a pomoću kojega može sigurno i anonimno pretraživati na Dark webu. Na slici 14. prikazan je TOR preglednik.



Slika 14. TOR preglednik

4. Analiza arhitekture Dark web (TOR) mreže

Glavni dio u arhitekturi TOR mreže su TOR čvorovi (engl. TOR nodes ili relays). Razlog zbog kojeg su TOR čvorovi najbitniji je taj što bilo koje računalo na kojem raditi TOR softver kao prenositelj poruke (engl. relay), a ne kao korisnik mreže. Međutim, nisu svi TOR čvorovi isti te imaju različite uloge neki su npr. mosni čvorovi (engl. bridge relays) ili zaštitnici ulaza (engl. entry guards). Arhitektura TOR mreže ne bi mogla funkcionirati bez imenika TOR čvora (engl. directory authorities). Svi dijelovi arhitekture Dark web-a (TOR) mreže biti će objašnjene u nastavku [13]. Na slici 15. prikazana je arhitektura Dark web (TOR) mreže.



Slika 15. Arhitektura Dark web (TOR) mreže

Izvor: [13]

Zaštitnici ulaza (engl. entry guards ili entry nodes) je koncept koji je uveden kako bi se smanjio mogućnost da napadači preuzmu kontrolu nad prvim čvorom nekog korisnika. Prilikom spajanja na TOR mrežu TOR softver će odabrati za ulazni čvor onaj koji je označen zastavicom zaštitnika (engl.guard flag). TOR čvorovima kojima su dodijeljene te zastavice duže vrijeme su dio TOR mreže te prenose velike količine prometa [13].

Imenici TOR čvorova (engl. directory authorities) unutar sebe imaju ugrađene IP adrese i kriptografske ključeve kako bi se korisnik mogao spojiti na TOR mrežu sigurno. Kako bi TOR softver saznao koji čvorovi postoje na korisničkom računu provjerava slijedeće: preuzima popis TOR čvorova, provjerava koliko imenika TOR čvorova zaista dostupno i ako je popis ispravno potpisala većina odnosno više od pola imenika TOR čvora [13].

Mosni TOR čvorovi (engl. bridge TOR relays) uvedeni su kako bi se zaobišlo blokiranje TOR mreže. Mosni TOR čvorovi su jako slični običnim čvorovima jedina razlika je u tome što se njihove IP adrese ne nalaze u javnim imenicima TOR čvorova, te nigdje ne postoje neki drugi potpuni ili javni popisi mosnih čvorova. Upravo iz tog razloga oni koji postavljaju cenzuru ili zabranu prikaza nemaju jednostavan način na koji bi blokirali pristup svim mosnim čvorovima. Onim korisnicima kojima pristup uobičajenim TOR čvorovima blokira cenzura mogu se na TOR mrežu spojiti upravo preko mosnih čvorova [13].

Priključni prijevoznici (engl. pluggable transports) su mehanizmi koji maskira promet između mosnog čvora TOR mreže i korisnika. Razlog maskiranja prometa između njih je taj da se sakrije činjenica da se zapravo radi o prometu TOR mreže [13].

TOR sakriveni servisi (engl. TOR hidden services) često se koriste na novinarskim blogovima i web stranicama koje žele izbjeći cenzuru i progon u diktatorskim režimima zbog informacija koje objavljuju. Umjesto prave domene na Internetu (npr. fpz.hr) skriveni servisi imaju posebnu (.onion) domenu, te je skrivene servise moguće upotrijebiti isključivo kroz TOR mrežu. Prednost sakrivenih servisa je taj što servis ne zna identitet korisnika, ali ni korisnik ne znam identitet skrivenog servisa [13].

5. Nedostatci i prednosti Dark web (TOR) mreže

Na samo spomen riječi Dark web vrlo često prvo što ljudima padne na pamet je neko okruženje u kojem se odvijaju neke kriminalne ili ilegalne radnje. Međutim, Dark web je potpuno legalna i sigurna mreža, ali zbog svog načina rada i pružanja anonimnosti uz pomoć TOR mreže vrlo često se zloupotrebljava i koristi za ilegalne radnje.

Neke prednosti Dark web (TOR) mreže su: omogućavanje anonimnosti web stranice i poslužitelja, štiti privatnost korisnika skrivanjem njihove IP adrese, pružanje sigurnosti prolaskom podataka kroz različite čvorove, aktivnosti korisnika na Internetu nije moguće pratiti, itd. Neki od nedostataka Dark web (TOR) mreže su: teško može zaštiti korisnika od analize prometa, zaštita na izlaznom čvoru je vrlo nisaka, otkrivanje DNS zahtjeva, zlouporaba, itd. [7]. Radi toga Dark web ima svoje prednosti i nedostatke koji će biti navedeni i objašnjeni u nastavku teksta.

Dark web (TOR) mreža ima puno prednosti koje nudi svojim korisnicima, a neke od njih su [14]:

- Zaštita od slabih i jakih napada – dizajneri koji su napravili anonimnu Dark web (TOR) mrežu priznaju da ona ne sprječava protivnike na globalnoj razini koji imaju pristup mreži, resurse i sposobnost da nadziru promet svih mrežama na kojima su njihovi korisnici spojeni. Međutim, TOR obećava svojim korisnicima zaštitu od slabih i jakih napada od strane pojedinaca ili drugih koji imaju sposobnosti za napad na one korisnike koji nisu tehnološki osviješteni i koji nemaju zaštitu na uređajima. Ujedno omogućuje sprječavanje analize prometa, osiguravanja povjerljivosti podataka koji se prenose putem Interneta za sve korisnike, nebitno bili oni primatelji ili pošiljatelji.

- Niti jedan TOR čvor nije svjestan kompletnog plana komunikacije – nakon što se formiraju svi TOR čvorovi koji sudjeluju u tom krugu svaki čvor zna samo prethodnika od kojeg je zaprimio podatke, te sljedeći čvor na koji treba dalje prenijeti te podatke. To se ne odnosi na zadnji čvor koji može identificirati sadržaj ćelija, ali ne i identitet pošiljatelja. Makar jedan čvor bio ugrožen ili djeluje zlonamjerno tako da pokušava uz pomoć analize prometa prikupiti informacije i podatke pošiljatelja, te podatke nažalost neće moći prikupiti upravo iz razloga što svaki čvor zna samo one podatke koji se odnose na njega.
- TOR gradi anonimne puteve za klijente na temelju popisa čvorova mosta – kada korisnik zahtjeva formiranje kruga tada se preuzima šifrirani popis svih dostupnih mostova s jednog od pet čvorova, te ih se zatim dešifrira na razini korisnika kako bi se uspostavio skok unutar TOR kruga. Jednom kada se prvi skok uspostavi s mostom onda se TOR čvorovi dodaju postepeno kako bi se povećala sigurnost uspostavljanja kruga za razliku od pojedinačnog kontaktiranja kruga.

Dark web (TOR) mreža ima i neke nedostatke koji mogu naštetiti njihovim korisnicima, a neke od njih su [6]:

- Otkrivanje DNS zahtjeva – kao i mnogi drugi sustavi koji štite anonimnost Internet korisnika zahtjevi DNS-a upućuju se tako da ne moraju koristiti TOR posrednog poslužitelja. Uporabom TOR programskih paketa torify naredbe ili Pivoxy poslužitelja dozvoljava se ispravljanje ovog nedostatka. Ujedno aplikacije koje koristi SOCKS5 poslužitelja omogućuju da se zahtjevi koji se temelje na imenu mogu usmjeravati DNS zahtjeve preko TOR mreže prilikom čega će se pretraživanje zapisa (engl. lookup) provoditi na samom izlazu čvora, te će tako DNS zahtjevi ostvariti istu razinu anonimnosti kao i sav ostali promet na TOR mreži.

- Zlouporaba TOR mreže – anonimnost unutar TOR mreže omogućuje slanje elektroničkih poruka koje nisu poželjne, tzv. spam pošte. Upravo radi toga je izvorno podešen da se TOR poslužiteljima zabrani izlaz paketa iz mreže koji bi trebali ići prema portu 25 iz razloga jer ga koristi SMTP (engl. Simple Mail Transfer Protocol) protokol. Još jedan način zlouporabe je taj da se pokušava prenijeti velike količine podataka preko TOR mreže, a razlog zbog kojeg je to loše je taj da poslužitelje održavaju „volonteri“ koji ustupaju vlastite resurse za korištenje potpuno besplatno.
- Analiza prometa – omogućuje napadaču koji ima djelomičan pristup TOR mreži otkrivanje čvorova preko kojih se ostvaruje anonimna veza. Upravo radi mogućnosti otkrivanja čvorova dolazi do problema u kojem TOR mreža postaje ranjiva i značajno se gubi anonimnost korisnika.

6. Ponuda skrivenih servisa na Darkwebu u kontekstu pandemije COVID-19

COVID-19 privlači globalnu pozornost nakon što Kina stavlja grad Wuhan u iznenadnu karantenu na dan 23. siječnja 2020. godine. Svjetska zdravstvena organizacija proglasila je pandemiju na dan 11. studenog 2020. godine, a od početka pandemije do ovog trenutka pisanja teksta u cijelom svijetu od CODVID-19 virusom zaraženo je bilo 590 miliona ljudi, te umrlo 6.44 miliona [15].

Kako bi se obuzdala pandemija uvedene su razne mjere kao npr. socijalno distanciranje, testiranje, karantena, ograničeno putovanje i praćenje kontakata koje je bilo ključno za suzbijanje ove pandemije. Upravo radi ovih mjera došlo je do pada globalnog gospodarstva i promijenilo potražnu za uslugama i robom u cijelom svijetu, te se procjenjuje da je gubitak svjetskog BDP-a bio od 2.5% do 3% od početka krize [15].

Radi ograničenja i zabrane kretanja dolazi do velike potražnje za hranom, higijenskih potrepština u ovom slučaju najviša je bila potražnja za wc papirom, alkoholom (kojemu je radi ove krize cijena porasla skoro za duplo), lijekovima, raznim tabletama, maskama, itd. Zbog nestašice i rasta cijena osnovnih proizvoda za život, i dezinformacija na Internetu veliki broj ljudi pokušava ispuniti svoje potrebe korištenjem nedopuštenim i rizičnih Internet stranica, te online kanala [15].

Ova pandemija preoblikovala je način na koji se potražuje usluge i roba diljem svijeta. Upravo kombinacija hitne situacije u javnom zdravstvu, panika potaknuta dezinformacijama i ekonomska nevolja gurnula je kupce i prodavače prema mračnoj strani ekonomije. Drugim riječima ta mračna strana ekonomije naziva se mračna web tržnica (engl. Dark web marketplace) koje je dostupna putem besplatnih softvera, te je stekla veliku popularnost [15].

Tijekom ovog poglavlja biti će prikazana analiza Dark web tržnice, te koji su proizvodi povezani sa COVID-19 najčešće traženi. Pratimo vremensku evoluciju kategorija proizvoda uključujući osobnu zaštitnu opremu, medicinske prijevare i lijekovi. Analizom navedenih podataka otkriveno je kako se online mračno tržište razvijalo tijekom pandemije i koliko je zapravo važno kontinuirano praćenje Dark web tržišta, pogotovo sada kada su dostupna razna cjepiva i lijekovi protiv virusa COVID-19 [15].

Moderne Dark web tražilice rade online izvan svjetske mreže (engl. World Wide Weba), tj. u šifriranom dijelu Interneta čiji sadržaj često nije indeksiran na standardnim web tražilicama. Jedna od prvih takvih tržnica je bio Silk Road marketplace pokrenut 2011. godine koji je započeo novi način trgovanja oružjem, drogom, alkoholom i drugim ilegalnim proizvodima na Internetu. Razlog zbog kojeg je bio uspješan je taj što je nudio razne skrivene usluge (engl. hidden service), a neke od tih skrivenih usluga su [15]:

- Osigurana zaštita od dijeljenja informacija o korisnicima kao što su: njihova trenutna lokacija, Internet aktivnosti i povijest pretraživanja.Ova značajka korisnicima daje osjećaj sigurnosti i anonimnosti.
- Potencijalni kupci pristupali su na Dark web tržnicu preko TOR preglednika što je otežavalo njihovo slijeđenje pomoću analize prometa.
- Kupnja se obavljala pomoću kripto valute Bitcoin, a ne preko kreditnih ili debitnih kartica kupca. Ova značajka korisnicima omogućuje dodatni stupanj privatnosti, kako kupcima tako i prodavačima, jer se prilikom plaćanja Bitcoin-om ne može saznati identitet osobe koja njime raspolaže.

Nakon što je FBI srušio i zatvorio Silk Road došlo je do pojavljivanja novih Dark web tržnica koje su korisnicima nudile znatno povećanje skrivenih usluga koje korisnicima omogućuje znatno veću sigurnost i razinu privatnosti za razliku od njihovog prethodnik. Oni su također nudili kupnju i prodaju oružja, droge, lijekova, hrane, kreditnih kartica, lažnih osobnih iskaznica, itd. [15].

Skrivene usluge koje su nadovezane su [15]:

- Nevidljivi Internetski projekt (engl. invisible Internet project) – potpuno šifrirana privatna mreža koja štiti aktivnosti i lokacije na TOR pregledniku.
- Escrow provjera usluge (engl. escrow check out services) – omogućuje zaštitu kupca od prevare na taj način da kupac mora platiti dogovoreni iznos do određenog vremena, a prodavač mora osigurati proizvod koji prodaje.

U tablici 1. prikazan je popis svih Dark web tržnica, zajedno s njihovom specijalizacijom i kratkim opisom.

Dark Web Markets	Specijalizacija	Opis
Atshop	Digitalna roba	Atshop platforma za kupnju na e-trgovini
Black Market Guns	Oružje	Tržnica oružja, izlaz je za prevare prema onion.live
CanadaHQ	Mješovito	Tržnica kriptovalutama s više dobavljača
Cannabay	Droga	Tržnica droge na ruskom jeziku s fokusom na kanabis
Cannazon	Droga(Kanabis)	Tržnica droge samo za proizvode od kanabisa
Connect	Mješovito	Društvena mreža na kojoj se nalazi tržnica za prodaju nedopuštene robe
Cypher	Mješovito	Cypher je tržnica s više dobavljača za prodaju droge i digitalne robe
DarkBay/DBay	Mješovito	Dark Web Market je tržnica sa više dobavljača koje prodaju digitanu robu, drogu i usluge
Dark Market	Mješovito	Dark Web Market je tržnica sa više dobavljača koje prodaju digitanu robu, drogu i usluge
Darkseid	Oružje	Dark Web Market za oružje
ElHerbolario	Droga	Online prodavaonica jednog dobavljača, koja prodaje 3 proizvoda, prvenstveno naklonjena kanabisu
Empire	Mješovito	Alphabay stil Dark Web Market sa BTC, LTC, XMR, MultiSig i PGP 2FA
Exchange	Mješovito	Tržnica na kineskom jeziku
Genesis	Digitalna roba	Tržnica koja prodaje digitalne identitete za mogućnost preuzimanja računa
Hydra	Droga	Dark Web Market na ruskom jeziku upotrebljava se za prodaju droge
MagBO	Digitalna roba	Trgovina karticama i računima
MEGA Darknet	Mješovito	Dark Web Market na ruskom jeziku
Monopoly	Droga	Više dobavljača koji su fokusirani primarno na prodaju droge
Mouse in Box	Digitalna roba	Tržište koje prodaje pakete podataka o prijavama koje su dobivene iz Web preglednika uz pomoć softvera koji krade podatke
Plati.Market	Digitalna roba	Dark Web Market za prodaju digitalne robe
Rocketr	Digitalna roba	Tržnica za prodaju ilegalnih digitalnih roba
Selly	Digitalna roba	Tržnica za prodaju ilegalnih digitalnih roba
Shoppy.gg	Digitalna roba	Tržnica za prodaju ilegalnih digitalnih roba
Skimmer Device	Skimmer uređaji	Tržnica koje prodaje skimmer uređaje
Tor Market	Droga	Dark Web Market za prodaju droge koji je fokusiran na opskrbu droge na Novom Zelandu
Torrez	Mješovito	Torrez je tržnica od vise dobavljača koji koriste plaćanje bez novčenika
Venus Anonymous	Mješovito	Dark Web Market sa više dobavljača koji prodaju drogu i robu
White House	Mješovito	Dark Web Market sa više dobavljača koji se bave prodajom kriptovaluta
Wilhaben	Mješovito	Dark Web Market na njemačkom jeziku koji se bavi prodajom nedopuštene robe
Yellow Brick	Mješovito	Dark Web Market sa više dobavljača koji se bave prodajom kriptovaluta

Tablica 1. Popis svih Dark web tržnica, te njihove specijalizacije i kratki opis

Izvor: [15]

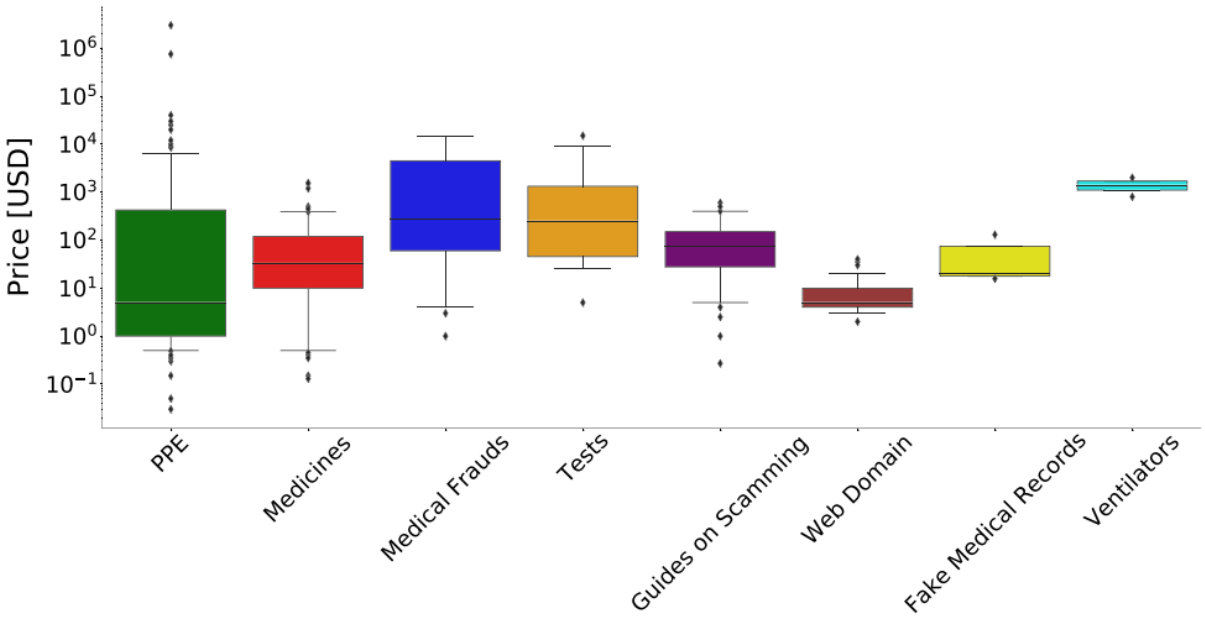
Svaka Dark web tržnica bila je indeksirana najmanje 90 različitih dana. Tijekom indeksiranja Dark web tržnica pregledane su prodaje proizvoda povezanih sa COVID-19 oglasima i sukladno sa time napravljene su kategorije. Jedan dio odabranih oglasa bili su stvarni oglasi specifični za COVID-19, a drugi dio oglasa je bio samo paravan koji je omogućio je trgovcima ilegalnih proizvoda da npr. pod lijekove prodaju kokain. Razlog toga je popuštanje mjera koje su bile uvedene radi suzbijanja pandemije, te je to dovelo do slabije provjere [15]. U tablici 2. prikazane su kategorije proizvoda koje su povezane sa COVID-19 oglasima i njihovo objašnjenje.

Kategorije	Primjeri
Osobna zaštitna oprema	Rukavice, maske, mediciski ogrtači, n95
Lijekovi	Azithromycin, chloroquine, azithromycin, favipiravir, remdesivir tablete
Vodiči o prijevarama	Kako nezakonito dobiti pomoćne pakete za COVID-19
Web domene	covid-testing.in, coronavintheworld.com
Medicinske prijevare	Protuotrovi, cijepiva, navodno ljekovite rekreacijske mješavine droga
Testovi	Dijagnoza i test
Lažni medicinski kartoni	Medicinska dokumentacija i Liječničke potvrde
Respiratori	Medicinski respiratori
Spominjanje COVID-19	Računalo, droge, prevare (prikazane u tablici 1.)

Tablica 2. Kategorije proizvoda povezane sa COVID-19 oglasima i njihovo objašnjenje

Izvor: [15]

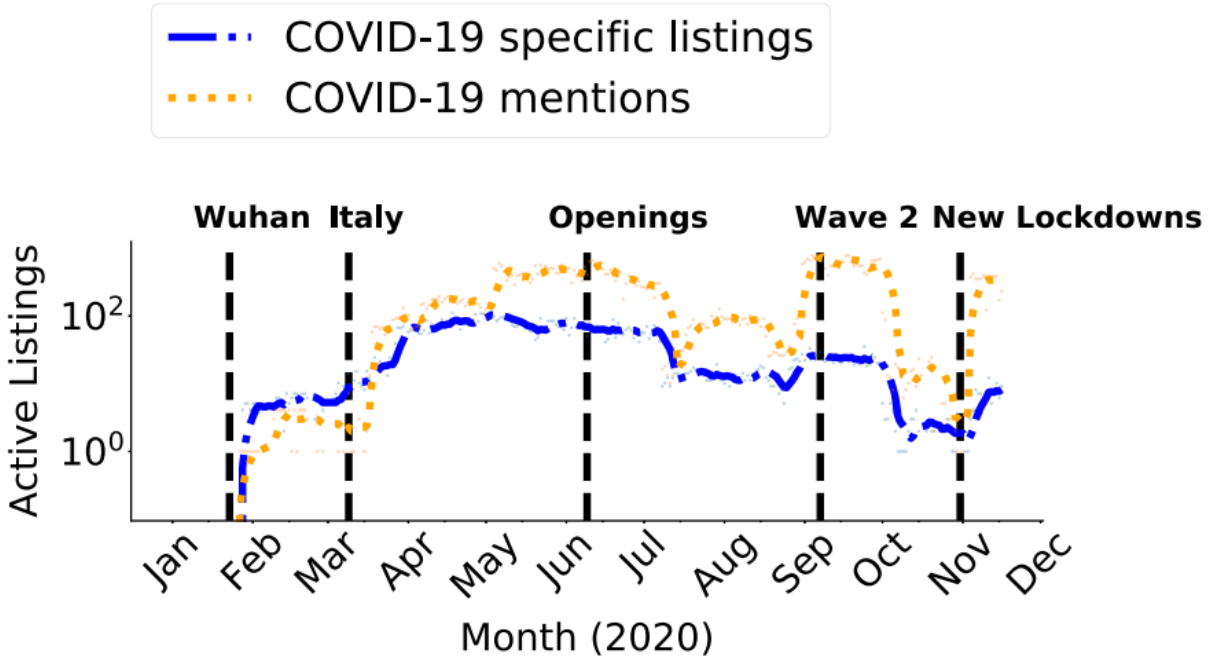
Okvirni prikaz cijena oglasa za svaku od gore navedenih kategorija povezanih sa COVID-19 proizvodima prikazana je na grafu 2. Svaki kvadrat unutar grafa prikazuje najnižu i najvišu cijenu nekog proizvoda, a vodoravna crta na sredini grafa prikazuje prosječnu cijenu neke kategorije. Točkice predstavljaju izuzetke koji dignu ili spuste cijenu iznad ili ispod vrijednosti proizvoda [15]. Na grafu 3. prikazana je okvirna cijena za sve kategorije proizvoda koji su povezani sa COVID-19 oglasima.



Graf 3. Okvirne cijene svih kategorija proizvoda koji su povezani sa COVID-19 oglasima. Izvor: [15]

Distribucija cijena za ove kategorije prikazuje kako mnogi oglasi imaju niske cijene od oko nekoliko dolara ili manje samo nekoliko proizvoda je premašilo cijenu od tisuću ili više dolara npr. respiratori su oko 1400 dolara, medicinske prijevare su oko 275 dolara, medicinske zapisi su oko 130 dolara, testovi su oko 250 dolara, vodiči o prijevarama su oko 75 dolara, lijekovi su oko 33 dolara, te web domene i osobna zaštitna oprema su najjeftiniji proizvodi s srednjom cijenom od oko 5 dolara. Ukupna vrijednost kategorija proizvoda iznosi oko 563.202 dolara, a isključeni iz ukupne cijene su proizvodi koji imaju cijenu veću od 40.000 dolara. U slučaju da prodavači objavljuju oglase po visokim cijenama to obično znači da prodavač želi zaustaviti prodaju s očekivanjem da će proizvod ponovno prodati u budućnosti. Upravo iz tog razloga se ovi proizvodi uklanjaju sa popisa, ali iz bog toga što bi nenormalno visoka cijena uveliko precijenila prodajnu cijenu stvarno aktivnih cijena [15].

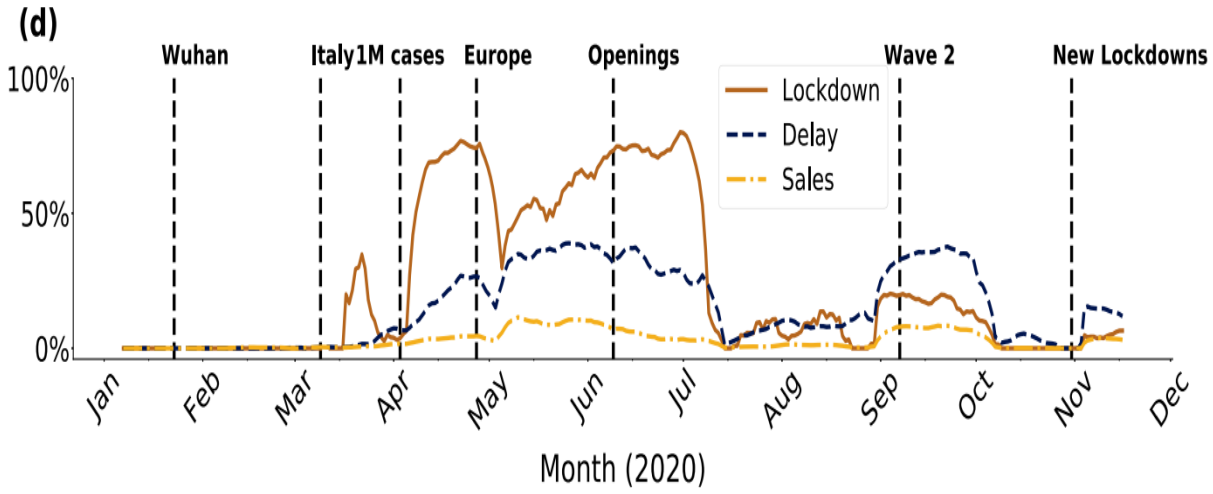
Broj aktivnih jedinstvenih oglasa evoluirao je tijekom vremena. Prvi poseban popis proizvoda povezani sa virusom COVID-19 počeo je nakon zatvaranja Wuhana 28. siječnja 2020. godine. Nakon uvođenja karantene mnoge zemlje su u ožujku bile odgovorne za porast broja tih oglasa, a do svibnja se broj povećao. U lipnju nakon što su mjere karantene u zemljama na sjevernoj polutci počele popuštati moguće je primijetiti kako pada broj nekih oglasa povezanih sa virusom COVID-19 koji se dalje nastavljao sve do studenog. Zatim se primjećuje dva iznenadna porasta COVID-19 u kombinaciji sa drugim valom zaraze u Europi u rujnu i nove mjere karantene u studenom [15]. Na grafu 4. prikazana je longitudinalna analiza aktivnosti Dark web tržnice.



Graf 4. Longitudinalna analiza aktivnosti Dark web tržnice

Izvor: [15]

Analizom je ustanovljeno da svi unosi u Dark web tržnicu su većinom povezani sa COVID-19, ali i neki od unosa koji se pretražuju su: izolacija, kašnjenje, karantena, problem sa dostavom, popust, rasprodaja, ili posebna ponuda [15]. Na grafu 5. prikazani su postotci upisivanja ključnih riječi izolacija, kašnjenje i rasprodaja unutar Dark web tržnice.



Graf 5. Postotak upisivanja ključnih riječi izolacija, kašnjenje i rasprodaja unutar Dark web tržnice

Izvor: [15]

7. Zaključak

U današnje vrijeme napretka tehnologije gotovo pa je nemoguće ostati anoniman na Internetu i naravno to sa sobom donosi određene opasnosti. Upravo radi potrebe za zaštitom podataka od napada i pokušaja narušavanja anonimnosti na Internetu razvijene su nove mreže. Jedna od tih mreža je Darkweb kojemu je najlakše i najsigurnije pristupiti preko TOR preglednika. Razlog zbog kojeg je TOR mreža popularna među korisnicima je taj što omogućuje skrivanje IP adrese korisnika, anonimnost web stranice i poslužitelja, pružanje sigurnosti tako što podaci prolaze kroz različite čvorove i aktivnosti korisnika nije moguće pratiti.

Međutim, ništa nije savršeno pa tako i TOR mreža. Mogućnosti napada i dalje postoje i to „najčešće“ uporabom analize prometa koji će napadačima omogućiti probijanje zaštite, preuzimanje identiteta, podataka i lokaciju korisnika. Bez obzira što je TOR mreža potpuno legalna i sigurna. Zbog svog načina rada ona se često zloupotrebljava za prodaju ilegalnih stvari. Upravo radi sprječavanja zločina postoje agencije za provođenje zakona koje takve prodaje otkrivaju i uklanjaju radi veće sigurnosti na mreži.

Početkom pandemije COVID-19 došlo je do potpunog zatvaranja i uvođenja karantene za sve. Upravo iz tog razloga dolazi do pada globalnog gospodarstva i proizvodnje. Radi pada proizvodnje dolazi do povećanja cijene osnovnih potrepština, ali i nestašica hrane, higijenskih potrepština, pića, lijekova, itd. To je bio razlog zbog kojega se veći broj ljudi odlučuje na kupnju na rizičnim i ilegalnim Internet tržnicama kao što su to Dark web tržnice.

Tijekom razdoblja pandemije dolazi do porasta prijevara kupaca koji kupuju na Darkweb tržnicama, ali i povećanja prodaje ilegalnih stvari npr. pod maske ili tablete protiv virusa COVID-19 podavala se je droga. Međutim, nisu se samo ilegalne stvari bile prodavane preko tih tržnica već je bilo i pravih stvari te njihov tijek i prodaja su bili prikazani u ovom radu. Da bi se omogućilo što sigurnije i anonimnije pristupanje i kupnja na tim tržnicama bez da se otkrije identitet kupca i prodavača napravljen je niz skrivenih usluga.

Popis literature

[1] Radočaj E. *Duboka mreža i mračni Internet.* Završni rad. Sveučilište u Zagrebu, Filozofski fakultet; 2020. Preuzeto s: https://urn.nsk.hr/urn:nbn:hr:131:048569 [Pristupljeno: 5. kolovoza 2022.]

[2] TOR. *Tor: Overview*. Preuzeto s: https://2019.www.torproject.org/about/overview.html.en [Pristupljeno: 5. kolovoza 2022.]

[3] Tor Metrics. *Servers.* Preuzeto s: https://metrics.torproject.org/networksize.html [Pristupljeno: 5. kolovoza 2022.]

[4] Ozkaya E, Islam R. *Inside the Dark Web.* Boca Raton: CRC Press. Preuzeto s: https://dokumen.pub/inside-the-dark-web-978-0-367-23622-9.html [Pristupljeno: 5. kolovoza 2022.]

[5] Tor. *Types of Relays On The Tor Network.* Preuzeto s: Tor Project | Types of relays on the Tor network [Pristupljeno: 5. kolovoza 2022.]

[6] Nacionalno središte za sigurnost računalnih mreža i sustava. *Tor – mreža za anonimnost*. Preuzeto s: https://www.cert.hr/wp-content/uploads/2019/04/CCERT-PUBDOC-2007-07-197.pdf [Pristupljeno: 5. kolovoza 2022.]

[7] Shubhdeep K, Sukhchandan R. *Dark Web: A Web of Crimes.* Preuzeto s: https://www.researchgate.net/publication/338878596_Dark_Web_A_Web_of_Crimes [Pristupljeno: 5. kolovoza 2022.]

[8] Bahalul H, Amdadul B, Sharaban N. *Anonymity Network Tor and Performance Analysis of ARANEA; an IOT Based Privacy-Preserving Router.* Preuzeto s: https://www.researchgate.net/publication/333617007_Anonymity_Network_Tor_and_Performance_Analysis_of_ARANEA_an_IOT_Based_Privacy-Preserving_Router [Pristupljeno: 5. kolovoza 2022.]

[9] Komutacijski procesi i sustavi. *Komutacija u mreži za anonimnost.* Preuzeto s: https://moodle.srce.hr/2021-2022/pluginfile.php/6325054/mod_resource/content/2/13.%20Komutacija%20u%20mreži%20za%20anonimnost.pdf [Pristupljeno: 6. kolovoza 2022.]

[10] Dingledine R, Mathewson N, Syverson P. *Tor: The Second-Generation Onion Router.* San Diego: The USENIX Association; 2004. Preuzeto s: https://www.usenix.org/legacy/publications/library/proceedings/sec04/tech/full_papers/dingledine/dingledine.pdf [Pristupljeno: 6. kolovoza 2022.]

[11] Bago N. *Deep web.* Završni rad. Sveučilište Sjever; 2016 Preuzeto s: https://urn.nsk.hr/urn:nbn:hr:122:862701 [Pristupljeno: 7. kolovoza 2022.]

[12] Statista. *Most common reasons for users to access the dark web woeldwide as of February 2019.* Preuzeto s: https://www.statista.com/statistics/1015244/global-dark-web-usage-reasons/ [Pristupljeno: 12. kolovoza 2022.]

[13] Hrvatska akademska i istraživačka mreža. *Tor mreža – tehnička pozadina i napredno korištenje.* Preuzeto s: https://www.cert.hr/wp-content/uploads/2018/02/tor_tehnicka_pozadina_i_napredno_koristenje.pdf [Pristupljeno: 15. kolovoza 2022.]

[14] Ramzi A. *The TOR dana communication system: A survey.* Preuzeto s: https://www.researchgate.net/publication/265645745_The_TOR_data_communication_system_A_survey [Pristupljeno: 15. kolovoza 2022.]

[15] Bracci A, Nadini M, Aliapoulios M, McCoy D, Gray I, Teytelboym A, Gallo A, Baronchelli A. *Dark Web Marketplaces and COVID-19: before the vaccine.* Preuzeto s: https://epjdatascience.springeropen.com/articles/10.1140/epjds/s13688-021-00259-w [Pristupljeno: 16. kolovoza 2022.]

Popis kratica

TOR	(The Onion Routing) luk usmjeravanje
BDP	(Gross Domestic product) bruto domaći proizvod
FBI	(Federal Bureau of Investigation) savezni ured za istrage
NSA	(Nacional Security Agency) agencija za nacionalnu sigurnost
CIA	(Central Intelligence Agency) središnja obavještajna agencija

Popis slika

Slika 1. napad na TOR mrežu 7
Slika 2. Izgradnja liste TOR čvorova 10
Slika 3. Prijenos podataka kriptiranih veza između nasumično odabranim poslužiteljima 11
Slika 4. Struktura paketa podataka u slojevima luka 12
Slika 5. Odabir nove nasumične putanje 13
Slika 6. Podatkovna struktura za usmjeravanje, onion 20
Slika 7. Web stranica za skidanje TOR preglednika 23
Slika 8. Program za instalaciju TOR preglednika 24
Slika 9. Instalacija TOR preglednika 24
Slika 10. Završetak instalacije 25
Slika 11. Spajanje na TOR mrežu 25
Slika 12. Povezivanje i konfiguracija TOR preglednika 26
Slika 13. Odabir razine sigurnosti 27
Slika 14. TOR preglednik 28
Slika 15. Arhitektura Dark web (TOR) mreže 29

Popis tablica

Tablica 1. Popis svih Dark web tržnica, te njihove specijalizacije i kratki opis..... 36
Tablica 2. Kategorije proizvoda povezane sa COVID-19 oglasima i njihovo objašnjenje...
..... 37

Popis grafova

Graf 1. Prikaz broja čvorova 4
Graf 2. Najčešći razlozi korisnika za pristupanje na Dark web 22
Graf 3. Okvirne cijene svih kategorija proizvoda koji su povezani sa COVID-19 oglasima. 38
Graf 4. Longitudinalna analiza aktivnosti Dark web tržnice 39
Graf 5. Postotak upisivanja ključnih riječi izolacija, kašnjenje i rasprodaja unutar Dark 40

Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOSTI

Izjavljujem i svojim potpisom potvrđujem da je završni rad
(*vrsta rada*)
isključivo rezultat mojega vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju upotrijebljene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedopušten način, odnosno da je prepisan iz necitiranog rada te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog/diplomskog rada pod naslovom Deskriptivna analiza mreže Darkweb u kontekstu pandemije COVID-19 , u Nacionalni repozitorij završnih i diplomskih radova ZIR.

Student/ica:

U Zagrebu, 30.9.2022

Petrović

(ime i prezime, *potpis*)