TEHNIČKO VELEUČILIŠTE U ZAGREBU

**SIGURNOST I ZAŠTITA INFORMACIJSKIH SUSTAVA**

**DARKNET - THENIČKI ASPEKTI**

**Ivan Filipović**

Zagreb, listopad 2020.

# Sažetak

Cilj ovog rada je upoznavanje sa tehnologijom na kojoj je baziran darknet tzv. „onion routing“ te utjecajem i razvojem te tehnologije kroz povijest. darknet je mreža kojoj se može pristupiti specifičnim software-om, konfiguracijom ona koristi nestandardizirane protokole i portove. Sama mreža je dio interneta koji je odvojen od vidljivog dijela slojevitim, „onion“, protokolima.

Početci darknet-a datiraju od samog početka interneta, gdje su se uz postojeći ARPAnet razvili skriveni serveri, ali tek 2002. objavom TOR-a darknet bio dostupan cijelom svijetu. Sredinom 1990 pojavila se potreba američkih obavještajnih agencija za sigurnom i tajnom komunikacijom te su počeli razvijati The Onion Routing, ideja je bila da se objavi i dopusti korištenje te tehnologije svijetu kako bi aktivnosti operativaca mogle biti prigušene sa aktivnostima drugih ljudi.

Seminarom ćemo opisati sam pristup darknet-u pomoću TOR-a, skraćenica od The Onion Routing te ćemo prikazati praktičnu primjenu tehnologije koja se koristi za ilegalne i legalne radnje.

# Ključne riječi

TOR – The Onion Routing

VPN – Virtual private network

Bitcoin

Hidden services

Darknet

Onion routing

Network Node – Mrežni čvor

Sadržaj

[Sažetak 2](#_Toc55171163)

[Ključne riječi 2](#_Toc55171164)

[1. Uvod 4](#_Toc55171165)

[2. Povijest Darknet-a 5](#_Toc55171166)

[3. TOR – The Onion Routing 8](#_Toc55171167)

[3.1 Imenici TOR mrežnih čvorova - Directory authorities 9](#_Toc55171168)

[3.2 Ulazni čvor – Entry node 9](#_Toc55171169)

[3.3 Središnji čvor 10](#_Toc55171170)

[3.4 Mostni čvor - Bridge Node 10](#_Toc55171171)

[3.5 Izlazni čvor – Exit node 11](#_Toc55171172)

[4. Skriveni servisi - Hidden services 11](#_Toc55171173)

[5. Skriveni servisi nove generacije 12](#_Toc55171174)

[6. Ranjivosti i poznati napadi na TOR mrežu 14](#_Toc55171175)

[6.1 SNIPER ATTACK 14](#_Toc55171176)

[6.2 Prisluškivanje izlaznog čvora 14](#_Toc55171177)

[6.3 Napadi na čvor sastanka 14](#_Toc55171178)

[7. Pristup Darknet-u 15](#_Toc55171179)

[8. Darknet u Hrvatskoj 17](#_Toc55171180)

[9. Zaključak 17](#_Toc55171181)

[10. Reference 18](#_Toc55171182)

# Uvod

Za razumijevanje ovog seminara Internet moramo podijeliti na površinski web, deepweb i darknet, *Slika 1*. Površinski web je najmanji dio interneta, ali i najviše korišteni dio interneta. Sastoji se od svih Internet stranica koje su indeksirane popularnim tražilicama kao što su Google, Yahoo ili Bing. Te se njima može pristupiti standardnim preglednicima bez posebnog software-a i konfiguracija.

Deepweb je najveći dio interneta te se on sastoji od stranica koje nisu indeksirane tražilicama. To su servisi koji se koriste u poslovne svrhe, razni servisi koje koriste vlade, vojske, akademske zajednice. To su servisi koji se koriste za mail usluge, online bankarstvo, web forume itd. Pristup deepwebu je moguć jedino direktnim URL-om ili IP adresom te je potrebna registracija i login takvim stranicama.

Slika na kojoj se prikazuje strijela

Opis je automatski generiran

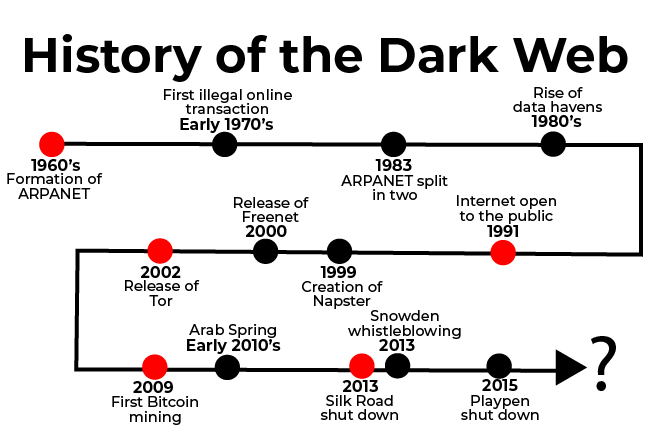
Slika 1. Struktura interneta

Darknet je dio deepweb-a koji je sakriven od svega navedenog te koristi specifični software, TOR, kao i posebnu konfiguraciju kako bi se spojili na server poslužitelja. TOR mreža je javno dostupan projekt koji korisnicima omogućuje anonimnost na internetu tj. darknet-u. Korištenje darknet-a ima svoje pozitivne i negativne strane te iako se kroz medije više spominju negativne strane darknet-a on ipak ima i pozitivnih strana u današnjem svijetu.

TOR je baziran na „onion routing-u“, ukratko komunikacija na darknet-u je zapakirana u više slojeva enkripcije te se ona dešifrira na više mrežnih čvorova koji se zovu „onion router-i“ nakon što je dešifriran zadnji sloj poruka je dostavljena na željenu lokaciju. Pošiljatelj ostaje anoniman jer svaki posljednj čvor zna samo sadržaj poruke. Samo ime „onion routing“ je dodijeljeno jer se takva slojevita slikovito podsjeća na strukturu luka. Iako je anonimnost glavna prednost darknet-a, razvile su se metode i tehnike kojim se može otkriti korisnike i poslužitelje.

# Povijest Darknet-a

ARPAnet, Advance Research Projects Agency network, je preteča današnjeg interneta, razvijen 1960-tih nastao je na ideji decentralizirane mreže za dijeljenje informacija i komunikaciji bez upotrebe telefona u jeku hladnog rata kao odgovor na opasnost da u slučaju rata neprijatelj ne može onesposobiti komunikaciju. Usporedno na ARPAnet-u razvijale su se i tajne stranice koje nisu bile na listi dostupnih lokacija te je tu začeta ideja o tajnosti i skrivenosti određenih lokacija na mreži.



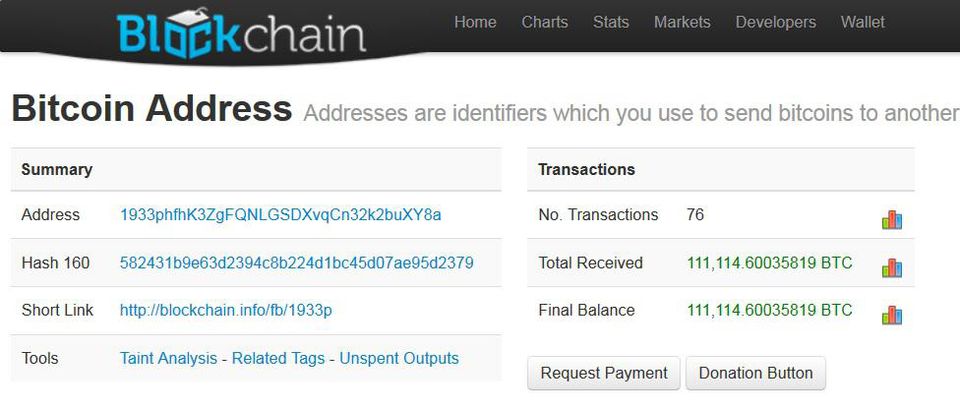
Slika 2. Povijest darknet-a

Iako je američka vlada tijekom godina ARPAnet sve više privatizirala, i dalje je omogućavala istraživačima, koji su prije svega radili na sveučilištima u cijeloj zemlji, slobodu pokušavanja radikalnih eksperimenata. To se može vidjeti u omogućavanju prve ilegalne mrežne transakcije korištenjem ARPAnet-a početkom 1970-ih. Studenti Stanforda koristili su račune na ARPAnet-u u Laboratoriju za umjetnu inteligenciju kako bi izvršili komercijalnu transakciju marihuane sa svojim kolegama s MIT-a (Kastner, 2020).

1990-tih Internet je pušten u javnost te se čovječanstvo tek upoznavalo sa njegovim mogućnostima, već tada se Internet počeo koristiti u ilegalne svrhe, ilegalno dijeljenje glazbe preko interneta i kršenje autorskih prava izvođača. Također 1990-tih Paul Syverson, Michael G. Reed, and David Goldschlag počinju razvijati „Onion routing“ u Mornaričkom razvojnom laboratoriju za sigurnije komuniciranje obavještajnih agencija te je patenti od strane američke mornarice 1998 (Wikipedia, 2017).

2002. TOR je predstavljen javnosti i tu godinu možemo smatrati početkom samog Darkneta. TOR je besplatan i dostupan svima te u svojim početcima je bio jako kompleksan te su ga upotrebljavali ljudi sa dobrim tehničkim znanjem, nakana izumitelja je bila da se oni koji žive pod opresivnim režimima mogu nositi sa cenzurom informacija koje sam taj režim može spriječiti da izađu u javnost. Tek 2008. se razvio TOR Internet preglednik koji je omogućio dostupnost darknet-a svima. No 2009. godina je bila prekretnica u smislu da su od tada kriminalne aktivnosti na darknet-u mogle biti monetizirane, izumljena je i puštena u javnost prva kripto valuta Bitcoin koja je njenim korisnicima omogućila neovisnost o centralnim bankarskim sustavima te samim time stvorila anonimnost prilikom novčanih transakcija.

Tek nakon razvoja bitcoina na darknet-u su se počela razvijati ilegalna tržišta sa ilegalnim ali i legalnim proizvodima i uslugama. 2011. imamo prvu Stranicu na darknet-u koja je bila ilegalno tržište tzv. SilkRoad. 2013. FBI je ugasio stranicu Silk Road te Pošto je FBI ugasio server, njihova vlada postala je novi vlasnik svih BitCoin računa koje su zaplijenili s njima. Među svim računima nađen je račun od osnivača Silk Road-a koji je sadržavao 111,000 BitCoina, koji su u to vrijeme vrijedili 17,000,000 $. (Hill, 2013).

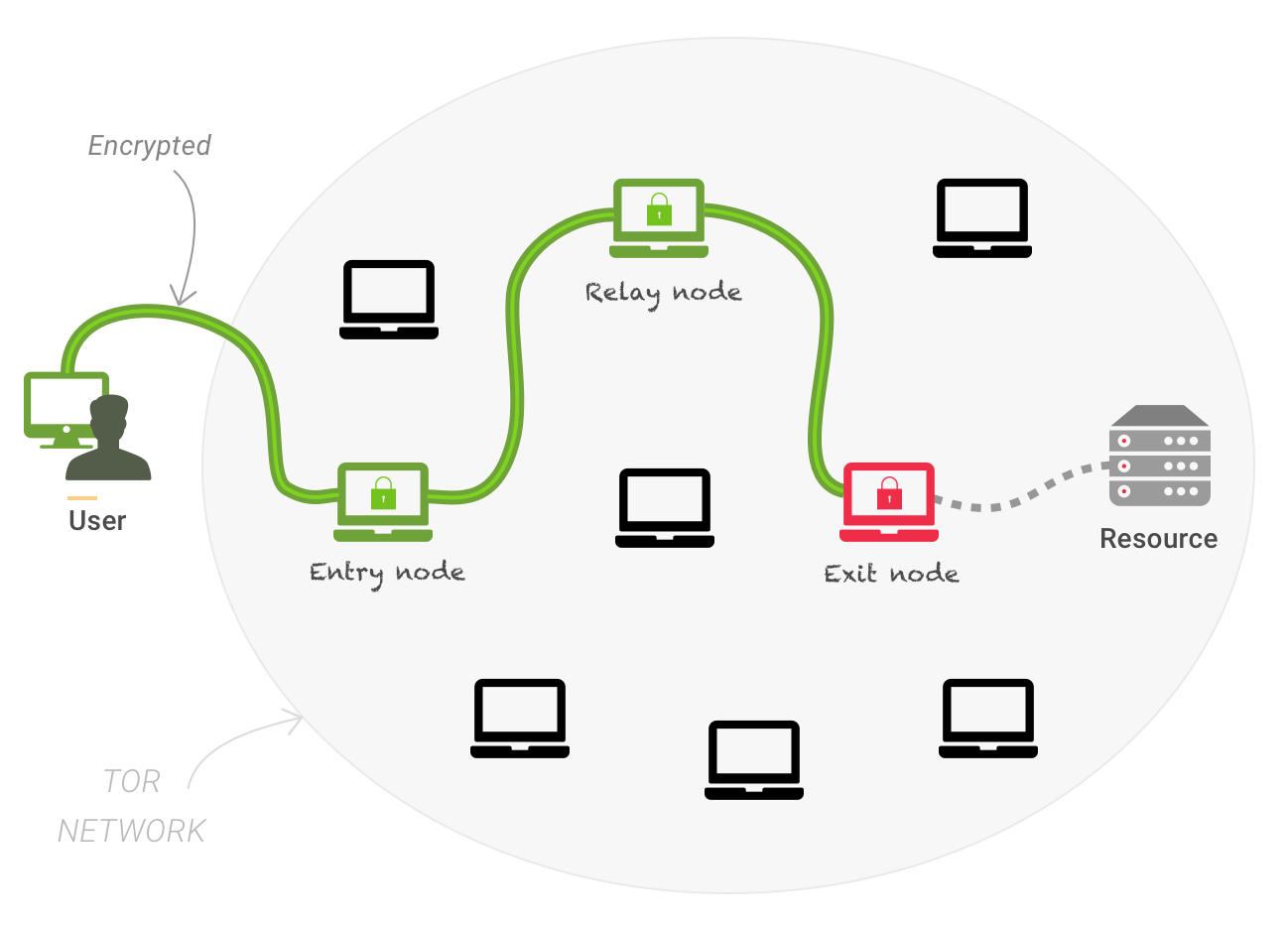


Slika 3. BitCoin novčanik Silk Road osnivača

2015. FBI je ugasio darknet stranicu sa dječjom pornografijom koja je brojala preko 150000 korisnika te je uhićeno više od 1000 ljudi diljem svijeta.

Darknet je imao i pozitivne trenutke u svojoj povijesti, bio je jedan od alata koje su aktivist u arapskom proljeću koristili za razmjenu informacija, slučaj Edwarda Snowdena je također jedan od pozitivnih primjera upotrebe darknet-a odnosno TOR-a kao i wikileaks koji je teško dostupan preko standardnih pretraživača.

# TOR – The Onion Routing

Kao što je već spomenuto TOR je skraćenica naziva „The onion routing “ koji omogućuje anonimnost na internetu. Promet TOR- mreže je je kriptiran sa tri sloja koja prolaze nasumično kroz mrežu te se dešifrira na tri mrežna čvora. Zadnji sloj dešifrira treći sloj te se poruka dostavlja serveru. Ovakva metoda enkripcije prikriva tragove korisnika, ali ne i samu poruku.

Slika 4. Tor mrežna shema

Tor mrežu čine mrežni čvorovi tzv. TOR čvorovi koji su bilo koje računalo koje koristi TOR software kao relej a ne kao korisnik mreže. Ti čvorovi su održavani od strane volontera i trenutno ih je sa današnjim datumom 6759 (Tor metrics, 2020). Svi TOR čvorovi nisu isti i imaju različite uloge u cijeloj mreži npr. Imamo ulazni čvor, središnji čvor, mostni čvor i izlazni čvor. Cijela mreža ne bi mogla raditi da nema imenika TOR čvorova.

## Imenici TOR mrežnih čvorova - Directory authorities

Da bi se spojili na TOR mrežu, naš software na računalu mora prvo saznati koji čvorovi postoje. Radi toga su u TOR preglednik ugrađeni kriptografski ključevi kao i IP adrese imenika čvorova, te je postupak spajanja sljedeći:

1. Software preuzima popis TOR čvorova od bilo kojeg imenika. Taj je potpis u pravilu digitalno potpisan od strane svih imenika TOR čvorova
2. Pomoću ugrađenih kriptografskih računa provjerava se koliko je imenika potpisalo ispravno popis
3. Ako je ispravno potpisan potpis više od pola imenika isti se smatra ispravnim te se koristi za spajanje na TOR mrežu

Ukoliko napadač želi kompromitirati imenik on ih mora uspješno kompromitirati više od pola imenika TOR čvorova.

Postoji devet imenika TOR čvorova koje održavaju osobe koje su dugo aktivne te im vjeruje TOR zajednica. Dogovor i digitalni potpis na imenik TOR čvorova se vrši svakih sat vremena putem glasanja osoba koje održavaju imenik TOR čvorova

## Ulazni čvor – Entry node

## 

Ulazni čvor je mjesto ulaza u TOR mrežu i svaki korisnik Mreže se spaja prvo na njega, ulazni čvor vidi IP adresu korisnika. Tu i na izlaznom čvoru su glavne mane TOR mreže, gubitak anonimnosti. Kako bi otkrili korisnikovu aktivnost na darknet-u moramo nadzirati ulazni i izlazni čvor. Npr. imamo kontrolu nad ulaznim i izlaznim čvorom te možemo vidjeti kako korisnik ulazi u TOR mrežu, ali ne možemo vidjeti što šalje zbog enkripcije poruke. Na izlaznom čvoru vidimo da posjećena ilegalna stranica ima posjetitelje, ali i dalje ne znamo da li je jedan od njih promatrani korisnik a i ako znam i dalje ne vidimo njegove aktivnosti na posjećenoj stranici. Analizom prometa poslanih informacija kao i analizom primljenih informacija može se otkriti da li je i što je korisnik radio na promatranoj web stranici.

Kako bi se zaštitila anonimnost i spriječila kontrola nad ulaznim čvorom uveden je metoda ulaznog čuvara gdje će TOR software koristiti samo one ulazne čvorove koji su označeni sa tzv. „guard flags“, to je oznaka koja se dodjeljuje čvorovima koje duže vrijeme sudjeluju u mreži i samim time se onemogućuje vladinoj agenciji ili napadaču postavljane velikog broja ulaznih čvorova kako bi pratili ulaze na TOR mrežu i oni se mijenjaju svakih 2 do 3 mjeseca.

## Središnji čvor

Središnji čvorvi pokrivaju veći dio TOR mreže u bilo kojoj komunikaciji na mreži. Sastoje se od releja kroz koje se prenose kriptirani podaci i niti jedan čvor ne zna više od prethodnog i sljedećeg čvora. Svi dostupni središnji čvorovi prikazuju se ulaznim i izlaznim čvorovima tako da se bilo koji može povezati s njima radi prijenosa. Čak i ako je poznato da bilo koji središnji čvor prenosi zlonamjerni promet, oni se ne smatraju odgovornima jer nisu ni izvor ni odredište prometa. Središnjem čvoru nikada neće biti dopušteno da djeluje kao izlazni čvor.

## Mostni čvor - Bridge Node

Mostni čvorovi nisu navedeni u imeniku TOR čvorova. Većina ulaznih i izlaznih čvorova javno je dostupna na Internetu i stoga ih se može blokirati ako se želi ograničiti korištenje TOR-a. Mnogi davatelji internetskih usluga, korporativne organizacije, pa čak i vlade imaju postavljene filtre koji zabranjuju upotrebu TOR-a. Npr. kineska vlada blokirala je sve javno dostupne čvorove na njihovom great firewall of China. Da bi se izbjegao takav scenarij, postoje Mostni čvorovi. Korisnik mora drugačije konfigurirati postave kako vi se spojio na TOR mrežu preko mostnog čvora

## Izlazni čvor – Exit node

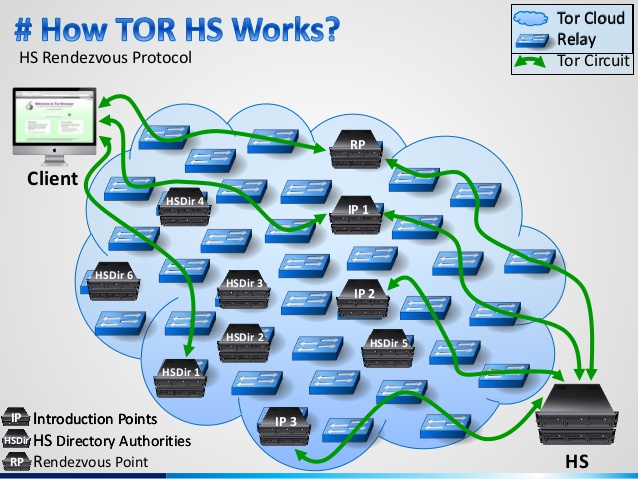
Izlazni čvor je zadnji korak u spajanju sa odredištem. To su čvorovi koji podatke šalju na odredište i često se smatraju krivcem jer se izlazni čvor doživljava kao podrijetlo prometa. Stoga će IP izlaznog čvora biti izravno vidljiv odredištu i često će primati više pritužbi, pravnih obavijesti, obavijesti o uklanjanju itd.

# Skriveni servisi - Hidden services

Normalno korištenje TOR mreže omogućava korisnicima anonimnost u normalnoj upotrebi interneta kao što je pregledavanje web stranica ili komunikacija sa drugim ljudima. No također se uz to javila i potreba za anonimnošću web poslužitelja. Kao primjer imamo web stranice i blogovi za objavu cenzuriranih podataka kao oružje u borbi protiv cenzure u opresivnim režimima. TOR omogućava takvu uslugu pomoću svojih skrivenih servisa tzv. „hidden services“ ili onion services. Kako je TOR mreža pod stalnim napadom raznih vladinih agencija daljnjim razvojem se pojavile skriveni servisi nove generacije.

Adresa skrivenog servisa, tzv. .onion domena, su kriptografski i automatski generirane pomoću TOR softwarea. Izgledaju ovako http://idnxcnkne4qt76tg.onion/, to je web mjesto torproject.org koje je posluženo preko skrivenih servisa.

Ne postoji registar .onion adresa. TOR mreža koristi .onion adresu za usmjeravanje zahtjeva na skriveni servis i vraćanje podataka sa skrivenog servisa anonimnom korisniku. Dizajn TOR mreže osigurava da korisnik ne može znati gdje se poslužitelj nalazi i poslužitelj ne može saznati IP adresu korisnika, osim namjernim zlonamjernim sredstvima poput skrivenog koda za praćenje ugrađenog u web stranice koje isporučuje poslužitelju. Uz to, dizajn mreže Tor, kojom upravljaju tisuće dobrovoljaca, osigurava da je nemoguće cenzurirati ili blokirati određene .onion adrese. (Phobos, 2013)

Za razliku od korištenja TOR sa normalnim servisima kod komunikacije sa skrivenim servisima se promet putuje kroz šest TOR čvorova od kojih tri bira korisnik dok je ostala tri bira skriveni servis i međusobno nemaju informacije o identitetu jednog i drugog.

Slika 5. Shema Komunikacije sa skrivenim servisima

# Skriveni servisi nove generacije

Danas darknet stranice ne čuvaju tajnost svoga postojanja i na internetu možemo pronaći njihove .onion adrese kako bi što više ljudi ih moglo pronaći npr. svatko tko želi pristupiti WikiLeaks-u može naći njihovu stranicu, wlupld3ptjvsgwqw.onion, i pristupiti njoj preko TOR preglednika isto tako prije samog gašenja Silk Road-a desetci tisuća ljudi je znalo za njihovu .onion adresu.

No postojala je ranjivost u samom dizajnu mreže koja je omogućila vladinim agencijama, napadačima i ostalima koji su ju iskorištavali da saznaju za postojanje skrivenog servisa. TOR mreža se sastoji od računala volontera koja služe kao čvorovi te omogućuje skakanje prometa diljem svijeta i svatko može postaviti svoje računalo kao čvor sa jedom od spomenutih uloga.

Da bi taj sustav usmjeravanja funkcionirao, svi sakriveni servisi moraju objaviti svoje postojanje tim direktorijima. Istraživanje objavljeno na hakerskoj konferenciji Defcon 2014. godine pokazalo je da je više od 100 od 3,000 direktorija tajno pretražilo svaku stranicu čiju je adresu saznalo, kako bi skenirali darkweb za prethodno neotkrivene web stranice.

Sljedeća generacija sakrivenih servisa koristit će pametnu metodu za zaštitu tajnosti tih adresa. Umjesto da svoju .onion adresu objavi direktorijima sakrivenih servisa, oni će umjesto toga izvući jedinstveni kriptografski ključ iz te adrese i dati taj ključ Tor-ovim direktorijima sakrivenih servisa. Svaki Tor korisnik koji traži određenu sakriveni servis može obaviti istu derivaciju kako bi provjerio ključ i usmjerio se na ispravnu adresu u mreži. No direktorij sakrivenih servisa ne može izvući .onion adresu iz ključa, čime se sprječava otkrivanje bilo kakve tajne darknet adrese. Rezultat ovakvih metoda bit će nevidljive web stranice. Mala skupina suradnika mogla bi, primjerice, prebaciti datoteke na računalo poznato samo njima. Nitko drugi nikad neće moći naći skriveni servis, a još manje mu pristupiti. Možete stvoriti skriveni servis na svom računalu, omogućiti način da se neprimjetno povežete s njim s bilo kojeg mjesta na svijetu, zadržavajući njegovo postojanje tajnim. TOR već nudi metodu da se sakrivenih servisa učine nepristupačnim za sve osim određene Tor preglednike, ali uključuje i nezgodne promjene konfiguracijskih datoteka preglednika. Novi sustav čini taj stupanj tajnosti daleko pristupačnijim prosječnom korisniku.

Sljedeća generacija sakrivenih servisa također će se prebaciti s korištenja 1024-bitnih RSA šifriranih ključeva na kraće, ali teže probojne, ključeve s eliptičkom krivuljom ED-25519. A promjene direktorija sakrivenih servisa znači da će se i URL-ovi sakrivenih servisa promijeniti sa 16 znakova na 50. No, Mathewson tvrdi da ta promjena ne utječe na pristupačnost dark web adresa jer su već sad preduge za zapamtiti. (Greenberg, 2017)

# Ranjivosti i poznati napadi na TOR mrežu

## SNIPER ATTACK

Zagušivanje izlaznih čvorova. DDoS napad koji zagušuje redove izlaznog čvora sve dok čvor ne ostane bez memorije, te radi toga ne može poslužiti pravog klijenta. Na ovaj način povećava se šansa da će se koristiti izlazni čvorovi kojima upravlja napadač. Preusmjeravanje Tor prometa. (Rob, Florian, Aaron, & Bjorn, 2015)

## Prisluškivanje izlaznog čvora

TOR ne šifrira promet između izlaznog čvora i servera, bilo koji izlazni čvor može snimiti sav promet koji prolazi preko njega koji ne koristi SSL ili TLS enkripciju.

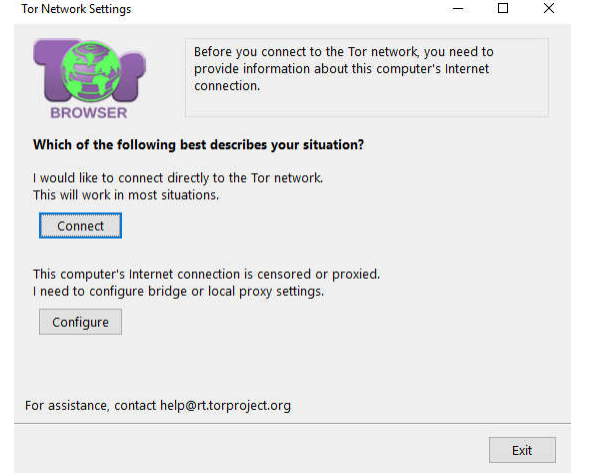
## Napadi na čvor sastanka

Ako nekoliko napadača može poremetiti skriveni servis onemogućavanjem njezinih čvorova za sastanke. Napadač koji kontrolira korisnikovu čvor za sastanke može zagušiti korisnika zahtjevima za sastanak ili spriječiti da važeći zahtjevi za sastanak dođu do njega.

Većina rušenja i napada na skrivenih servisa je od strane vladinih agencija i grupe etičkih hakera, prvenstveno jer služe kao mjesto za ilegalno tržište ili sponzoriraju dječju pornografiju i terorizam. No na temelju grešaka kriminalaca dolazi i do njihovog pada npr. Silk Road je ugašen jer je jedan od administratora servera to obavljao u Internet kafiću te se spajao direktno na server i to ne preko TOR preglednika.

Gotovo svakodnevno provodi se 1200 DDoS napada. Jedan napad na IP adrese sa vidljivog weba bez upotrebe TOR-a limitirao bi mogućnost prolaženja prometa kroz čvorove i učinio bi TOR mrežu beskorisnom. Čak se i TOR prigušio na budućnost svojih servisa. Nakon što je Vlada SAD-a oduzela i ugasila preko 400 web stranica u samo jednoj operaciji (Onymus), pojavio se članak na službenoj stranici TOR-a koji je sadržavao sljedeće: „Na neki način, iznenađujuće je da su sakriveni servisi preživjeli ovoliko dugo. Pažnja koju su dobivali je minimalna uspoređujući sa njihovom socijalnom vrijednosti i uspoređujući sa količinom odlučnosti svojih protivnika.“ (Inside the Dark Web, 2015)

# Pristup Darknet-u

Za Pristup darknet-u potrebno je instalirati TOR pretraživač. Prilikom prvog pokretanja potrebno se spojiti na TOR mrežu

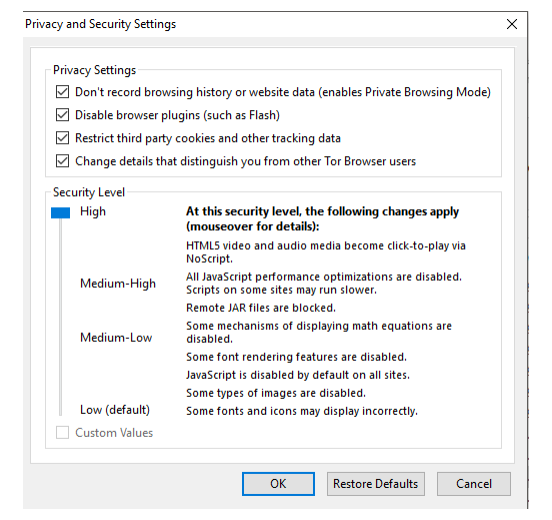
Slika 6. Spajanje na TOR mrežu

TOR nam omogućava anonimnost prilikom surfanja internetom te ukoliko želimo biti još sigurniji u našu anonimnost može se koristiti i VPN.

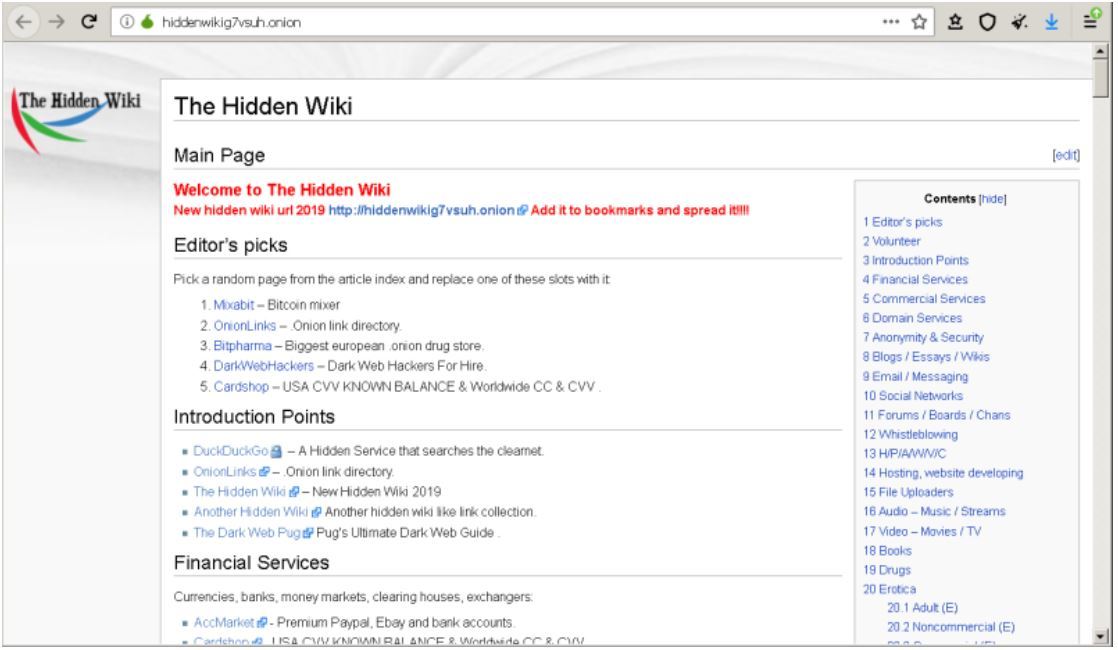
Za dodatnu anonimnost postoje razni operacijski sustavi koji koriste TOR mrežu.

Tails (skraćeno od eng. the amnesic incognito live system) je operacijski sustav namijenjen čuvanju privatnosti i anonimnosti. Za razliku od konvencionalnih operacijskih sustava, Tails se obično instalira na USB stick ili na DVD te se preko njih pokreće. Zbog toga je Tails moguće koristiti s gotovo bilo kojeg računala (ne samo na vlastitim računalima, već primjerice i u knjižnici) te on tijekom rada na računalu neće ostaviti nikakve tragove. Za anonimnu i privatnu komunikaciju Tails se oslanja na Tor mrežu.

Također je preporučljivo da se onesposobe sve JavaScript skripte koje bi mogli dobiti od skrivenog servisa jer se upravo radi te skrivenosti na njima mogu nalaziti zlonamjerne skripte i malware-i.



Slika 7. Postavke sigurnostina TOR pregledniku

Kao prvi skriveni servis koji sam naša je HiddenWiki koji meni kao početniku služi kao početna točka za daljnje istraživanje darknet-a. oko 60% .onion adresa koje se nalaze na HiddenWiki je legalnog sadržaja dok su ostale ilegalne .onion adrese služile za prodaju droge, oružja i eksplicitnih seksualnih sadržaja.

Slika 8. HiddenWiki

# Darknet u Hrvatskoj

Najpopularnija upotreba darkneta u Hrvatskoj je za kupovinu droge preko skrivenih servisa. Tako naprimjer imamo slučaj iz Splita gdje je 22-godišnjak uhićen sa 116 grama amfetamina koje je kupio preko darknet-a. Policija je znala za njegovu transakciju te su ga uhvatili na izlasku iz pošte.

# Zaključak

Sloboda izražavanja mora biti dopuštena – za to putem interneta potrebna vam je anonimnost da biste iskoristili to pravo. Anonimne mrežne komunikacije nude toliko prednosti da umanjuju nedostatke.

TOR projekt se sastoji od ljudi koji istražuju, projektiraju, grade i analiziraju anonimne komunikacijske sustave. Fokus je na praktičnim sustavima za internetske veze s malim kašnjenjem koje se odupiru analizi prometa, prisluškivanju i drugim napadima od strane napadača izvan mreže tako i napadačima unutar mreže. „Onion routing“ sprječava da se zna tko s kime komunicira - mreža zna samo da se komunikacija odvija. Uz to, sadržaj komunikacije skriven je od prisluškivača do točke na kojoj promet napušta TOR mrežu. Izvorni dizajn onion routing-a zasnovan je na višeslojnim enkripcijama javnog ključa. Čvor bi znao samo svoje izravne susjede, a izvor i odredište ostaju anonimni.

Postoji nekoliko ranjivosti sa izvornom idejom, npr. ranjivost izlaznih čvorova, kontrola zagušenja itd.

TOR se bavi svim tim ranjivostima i radi u stvarnom vremenu na svjetskoj mreži. Postupak instalacije i postavljanja za Tor također je vrlo jednostavan. Pristup blokiranim web lokacijama bez ostavljanja bilo kakvih tragova ili posluživanje skrivenih servisa putem Interneta, a da vas nikad ne prepoznaju kao vlasnika servisa su glavne prednosti TOR-a.

Iako se puno kriminalnih i ružnih stvari događa na darknet-u ipak ima puno više svojih pozitivnih strana te nam omogućuje potpunu slobodu u današnje svijetu interneta bez privatnosti.

# Reference

Greenberg, A. (20. Siječanj 2017). *https://www.wired.com*. Dohvaćeno iz https://www.wired.com: https://www.wired.com/2017/01/get-even-easier-hide-dark-web/

Hill, K. (17. Listopad 2013). *Forbes*. Dohvaćeno iz https://www.forbes.com: https://www.forbes.com/sites/kashmirhill/2013/10/17/does-this-17-million-bitcoin-wallet-belong-to-alleged-silk-road-mastermind-ross-ulbricht/?sh=32508c4621fa#230bba815385

Inside the Dark Web. (Veljača 2015). *PC MAGAZINE DIGITAL EDITION*.

Kastner, E. (7. Veljača 2020). *HISTORY OF THE DARK WEB [TIMELINE]*. Dohvaćeno iz https://www.soscanhelp.com: https://www.soscanhelp.com/blog/history-of-the-dark-web#theearlydays

Phobos. (4. Kolovoz 2013). *blog.torproject.org*. Dohvaćeno iz https://blog.torproject.org: https://blog.torproject.org/hidden-services-current-events-and-freedom-hosting

Rob, J., Florian, T., Aaron, J., & Bjorn, S. (2015). The Sniper Attack: Anonymously Deanonymizing. Washington, USA.

*Tor metrics*. (1. Studeni 2020). Dohvaćeno iz https://metrics.torproject.org/: https://metrics.torproject.org/bubbles.html

Wikipedia. (1. Ožujak 2017). *Wikipedia*. Dohvaćeno iz https://en.wikipedia.org: https://en.wikipedia.org/wiki/Onion\_routing