Deep web i dark web – Potreba ili zloupotreba

Miloš Ilić, Petar Spalević
Elektrotehničko i računarsko inženjerstvo
Fakultet tehničkih nauka
Kosovska Mitrovica, Srbija
milos.ilic@pr.ac.rs, petar.spalevic@pr.ac.rs

Žaklina Spalević, Mladen Veinović, Khalid Salem Ali Aleja
Univerzitet Singidunum
Beograd, Srbija
zspalevic@singidunum.ac.rs, mveinovic@singidunum.ac.rs

Sažetak—**Brz tehnološki razvoj, razmena velike količine podataka kao i sve veća upotreba Interneta i društvenih mreža svakoga dana smanjuju mogućnosti zaštite privatnosti. Način rada savremenih pretraživača je takav da registruju i pamte svaku aktivnost internet korisnika. U cilju zaštite privatnosti razvio se deo Interneta pod nazivom deep web koji komercijalni pretraživači ne mogu da indeksiraju. Pored prednosti koje ovakav način rada donosi korisnicima, nemogućnost indeksiranja i praćenja aktivnosti korisnika u deep web-u otvorili su prostor za njegovo korišćenje u cilju bavljenja ilegalnim aktivnostima. Ovakav deo Interneta poznat po stranicama koje nude različit skup ilegalnih aktivnosti poznat je pod imenom dark web. U radu je dat kratak pregled evidentiranih ilegalnih aktivnosti nastalih upotrebom dark web-a. Ovakve aktivnosti su glavni pokazatelj zloupotrebe anonimnosti koju pruža ovaj deo interneta.**

Ključne reči-dark web; deep web; terorizam; ISIS; Tor;

I. UVOD

Razvoj informacionih tehnologija, pre svega Interneta, uneo je drastične promene u sve pore društvenog života, od kojih su neke izrazito pozitivne, a neke krajnje negativne i potpuno nepoželjne. Iz tog razloga internet korisnici moraju pronaći način da u najvećoj mogućoj meri iskoriste pogodnosti koje Internet pruža. Internet je neiscrpni izvor informacija, i kao takav je u svakodnevnoj upotrebi od strane pojedinaca i organizacija. U novije vreme državne uprave mnogih zemalja kreiraju različite servise za elektronsko upravljanje u cilju što efikasnije dostupnosti podataka i komunikacije sa svojim građanima. Statistika pokazuje da oko 1,6 milijardi ljudi širom planete svakog dana koristi Internet kako bi proverili svoj profil na Facebooku, Twiteru, nekom od mail account-a, pogledali video na YouTube-u, ili jednostavno vršili pretragu u cilju pronalaženja različitih informacija [1]. Pomenute aktivnosti korisnika spadaju u domen korišćenja takozvanog površinskog (*eng. surface*) dela weba. Pod pojmom površinskog weba spada sve ono što se može indeksirati korišćenjem javnih web pretraživača kao što su Google, Yahoo, Bing, itd [2]. Ovi pretraživači korišćenjem robota za indeksiranje obilaze sve dolazne i odlazne linkove sa trenutno posmatrane stranice i na taj način kreiraju mapu povezanosti stranice sa ostalim stranicama. Na ovakav način pretraživači imaju evidenciju o tome koje stranice je korisnik posećivao kao i koliko vremena je proveo na konkretnoj stranici.

Pored ovakvog vida praćenja veliki broj društvenih mreža posredno ili neposredno prati aktivnosti kako svojih korisnika, tako i internet korisnika uopšte. Ovde se izdvajaju različite situacije. Jedna od njih je kada korisnik poseti stranicu koja sadrži dodatak koji služi da se stranica lakše deli na društvenim mrežama, i koji se najčešće javlja u vidu Share ili Like dugmeta. Dodatak tada beleži koju je stranicu posećivao konkretni korisnik i informaciju o tome šalje na server društvene mreže, koji onda ukrštanjem podataka može da sazna gotovo sve o korisniku, naročito zbog toga što već ima veliki broj njegovih ličnih podataka. Ovakav vid praćenja aktivnosti internet korisnika krši jedan od osnovnih principa zaštite podataka o ličnosti – srazmernost obrade podataka u odnosu na svrhu za koju se podaci prikupljaju. Posebno je interesantno da do ukrštanja podataka dolazi bez obzira da li su korisnici ulogovani na društvenu mrežu ili ne. Takođe i slučajna ili kratkotrajna poseta određenoj društvenoj mreži može dovesti do toga da se instalira „treking“ kolačić, koji potom, posetom drugoj stranici na kojoj je bio prisutan dodatak za društvene mreže, može da otkrije podatke korisnika mreže kao što su IP adresa, Internet pretraživač koji koristi ovakav korisnik i stranica koja se posećuje [3].

Nasuprot površinskom delu weba koji je indeksiran, dubinski deo (*eng. deep*) obuhvata deo web stranica na Internetu koje nisu indeksirane. Ovo zapravo znači da su stranice koje pripadaju deep web-u samostalne i da nema linkova koji bi ih povezivali međusobno. Upravo zbog ovakvih karakteristika javni pretraživači ne mogu da pristupaju stranicama koje pripadaju deep web-u. Pristup se obavlja samo pomoću korišćenja specifičnog softvera, konfiguracije, ili uz ovlašćenje vlasnika stranice, često koristeći nestandarde komunikacione protokole. Ovakva organizacija deep web-a nudi visok stepen privatnosti svojim korisnicima pa je iz tog razloga veoma često u upotrebi od strane ljudi koji ne žele da njihova aktivnost na Internetu bude praćena. Broj stranica, a samim tim i količina podataka koji se mogu naći na deep web-u znatno su veći nego što je to slučaj sa površinskim delom web-a. Ne postoje tačni podaci o tome koliko puta je veći deep web od površinskog dela weba. Niko pouzdano ne zna kolika je veličina deep weba, zato što retko ko ima pristup gotovo svemu što se tu može naći. Dakle, to je jedan univerzum sajtova na kojima se mogu pronaći informacije, ponude, slike, zvučni i video zapisi o stvarima sa kojima se veliki broj korisnika površinskog weba nikada nije susreo [4]. Prema nekim istraživanjima odnos proporcija ove dve internet sfere jeste da površinski deo zauzima oko 4%, dok deep web zauzima oko 96% globalne mreže. Anonimnost koja se pruža korisnicima deep web-a iskorišćena je kao vid zaštite za širenje različitih ilegalnih aktivnosti, što je dovelo do izdvajanja

jednog njegovog dela. Ovaj deo deep web-a i interneta uopšte naziva se dark web. Kao i što samo ime sugeriše aktivnosti korisnika u ovom delu interneta nisu nimalo svetle. Neke od aktivnosti korisnika ovog dela interneta su: trgovina informacijama, oružjem, falsifikovanim dokumentima i novcem, pa sve do trgovine ljudskim organima. Pored same trgovine ilegalnom robom ovaj deo interneta često je korišćen od strane terorista i terorističkih organizacija za mobilizaciju novih članova prikupljanje i deljenje informacija.

Cilj ovog rada je pregled tehnologija na kojima se bazira rad deep i dark weba, sličnosti i razlika između ova dva dela interneta. Takođe rad daje pregled dokumentovanih ilegalnih aktivnosti koje se mogu naći pretragom dark web-a.

II. DEEP WEB I DARK WEB - SLIČNOSTI I RAZLIKE

Veliki broj ljudi vođen informacijama dobijenim iz različitih medija, kao i određenog broja internet članaka, foruma i blogova izjednačava termine deep i dark web. Jedina sličnost između ova dva dela interneta je anonimnost korisnika i nemogućnost indeksiranja od strane javnih web pretraživača. Za pristup i jednom i drugom delu Interneta potreban je poseban softver koji omogućava anonimnost podataka i IP adrese korisnika. Ovaj softver poznat je pod imenom Tor (eng. *The Onion Router*). Osnovna namena ovog softvera je da posluži kao gateway ka ovom delu Interneta. Kako bi sakrio adresu internet korisnika Tor vrši preusmeravanje signala preko gotovo 6000 servera [5]. Kako bi se stvorila privatna i zaštićena veza unutar Tor mreže, klijentska aplikacija inkrementalno izgrađuje vezu između izvorišta i odredišta paketa podataka, a koja se sastoji od kriptovanih veza između nasumično odabranih serverskih stanica. Ova veza nastaje u koracima, tako da pojedinačni server zna samo od kojeg servera je dobio pakete i kojem serveru ih treba proslediti. To se postiže korišćenjem posebnog ključa za enkripciju u svakom koraku. Jednom kada je veza uspostavljena njome je moguće prenošenje različitih vrsta podataka korišćenjem različitih programskih paketa [6].

Razlika između deep i dark web-a je velika počevši od veličine jednog i drugog dela Interneta pa sve do sadržaja koji oni nude. Deep web obuhvata uglavnom web sajtove koji nisu zlonamerni, kao što su primera radi email nalozi, servisi za čije je korišćenje potrebno platiti kao što je Netflix, kao i sajtovi kojima se pristupa kroz logovanje putem online forme. Jednostavno na deep webu se nalaze strane koje nisu indeksirane, odnosno označene tako da se ne mogu pronaći uz pomoć običnih alata za pretraživanje. Ovakve web strane spadaju pod domenom deep weba, jer im je nemoguće pristupiti bez posebne dozvole, a takođe ih pretraživači neće vratiti kao rezultat pretrage. Praktično ukoliko bi pretraživač mogao da vrati ovakve web strane kao rezultate pretrage to bi značilo da neko može da pristupi gmail nalogu određene osobe prostom pretragom prema imenu osobe [7].

Pored upotrebe od strane običnih korisnika deep web često koriste i programeri različitih kompanija, koje eventualno žele da testiraju kreirane web sajtove pre nego što ih učine dostupnim za indeksiranje i pristup sa strane površinskog interneta. Kao osobe koje stalno imaju potrebu za pronalaženjem informacija do kojih se ne može doći pretragom površinskog interneta deep web koriste i novinari. Takođe, deep web pruža mnogo veću anonimnost, pa iz tog razloga ljudi u totalitarističkim zemljama kao što je Severna Koreja koriste deep web kako bi zaobišli sigurnosne sisteme i ograničenja u dostupnosti informacija koje im je Vlada postavila u pogledu korišćenja Interneta [1]. Korišćenjem deep web-a državljani ovih zemalja ostvaruju međusobnu komunikaciju, informišu se o dešavanjima širom sveta, i u isto vreme informišu ostatak sveta o dešavanjima u svojoj zemlji.

Dark web se može posmatrati kao mali deo deep weba koji je zbog anonimnosti koju nudi svojim korisnicima postao popularan kod zlonamernih korisnika. Pristup ovom delu Interneta kao što je već navedeno je gotovo identičan pristupu deep web-u. Iz domena korisnika dark web-a poznato je da ovom delu Interneta pristupaju samo korisnici koji tačno znaju šta traže i kako najefikasnije da pronađu stranice koje su im potrebne. Upotreba dark web-a povezuje se sa raznim ilegalnim aktivnostima kao što su hakovanje, dečija pornografija, razni oblici ilegalne trgovine uključujući trgovinu drogom i oružjem, prostitucija i tako dalje.

III. ILEGALNE AKTIVNOSTI KORISNIKA DARK WEB-A

Veliki broj istraživanja u kojima se posmatraju aktivnosti korisnika dark web-a, kao i sve ono što se može pronaći pristupom njegovim stranicama nesumljivo polazi od stranice pod nazivom *Put Svile (eng. Silk Road)*. Ovo je bila čuvena stranica na kojoj su korisnici jednostavnim klikom mogli da poruče bilo koju vrstu opijata koja im je potrebna, uključujući i različite vrste kako dozvoljenih tako i zabranjenih lekova. Osnivač i vlasnik bio je Ross Ulbrich 29. godišnji programer, koji se predstavljao pod pseudonimom pirat Roberts (*eng. Dread Pirate Roberts*). Od 2011. godine do 2013. godine on je stvorio imperiju vrednu 1,2 milijarde dolara. [8]. Zanimljiva i pomalo zastrašujuća činjenica jesta da je ovaj sajt funkcionisao kao bilo koji drugi portal za online kupovinu. Sva poručena roba bi stizala posredstvom kurirskih službi na kućnu ili dogovorenu adresu.

O upornosti ljudi koji se bave ovakvim vidom kriminala svedoči i podatak da je samo mesec dana nakon hapšenja Ulbricha i gašenja portala, portal postao ponovo aktivan na dark web-u, ovoga puta u verziji 2.0. Sajt je veoma brzo doživeo ekspanziju. Prema podacima FBI-a imao je prosečno oko 150.000 aktivnih posetilaca i zarađivao je mesečno oko 8 miliona dolara od prodaje robe i usluga. Nakon godinu dana rada sajt je ugašen, dok je administrator Blake Benthall uhapšen [9]. Od trenutka gašenja sajt nije bio aktivan svega sat vremena, nakon čega je opet pokrenut i nastavio je sa radom, ovoga puta u verziji 3.0. Ova činjenica pokazuje jačinu dark web-a i postojanost portala koji se na njemu nalaze [10].

Sajt The Armory, je jedan u nizu specijalizovanih sajtova za trgovinu vatrenim, tupim i oštrim oružjem kojim se mogu naneti povrede opasne po život. Prodaja oružja i municije obavlja se na sličan način širom drugih sajtova, od kojih neki garantuju isporuku širom planete, i to pod parolom "Dostavljamo globalno, jer svi imaju pravo da se zaštite" [11]. Na raspolaganju je bukvalno sve, od pištolja do eksploziva C4. Isporuka se vrši u posebnim pakovanjima, tako da mogu da prođu rendgensku kontrolu. Takođe veoma često se oružje

pakuje u igračke, ali i u različite druge instrumente i električne uređaje [12].

Postoje primeri koji pokazuju da je dark web savršeno mesto za Cyber kriminal. Ovo je jedinstveno mesto gde u isto vreme korisnici mogu postati vlasnici različitih vrsta malvera, ali takođe i žrtve istih. Za distibuciju malvera koriste se svi poznati metodi phishing-a i pharming-a. Jedna velika grupa malvera koji se mogu naći na dark web-u su CryptoLocker malveri. Ovi malveri nakon pristupa fajlovima žrtve vrše kriptovanje istih. Nakon kriptovanja fajlova, žrtva biva redirektovana na stranicu na kojoj se od nje traži da izvrši plaćanje ukoliko želi da povrati kontrolu nad svojim podacima. Veoma često su zahtevi za plaćanjem kao i informacije potrebne da bi se izvršila transakcija ispisani na maternjem jeziku žrtve. Uloga Tor-a u ovakvim transakcijama jeste da hostuje sajtove za plaćanje u cilju izvršenja plaćanja pomoću bitcoin-a koji su veoma česta valuta plaćanja usluga na dark web-u [13].

Cyber kriminalci na dark web-u često nude hakerske uluge u najam. Primera radi kineska grupa Hidden Lynx tvrdi da ima do sto profesionalnih cyber lopova, među kojima ima i onih koji su upali u računarske sisteme Google-a, Adobe-a i Lockheed Martina. U zavisnosti od složenosti posla i rizika koji on nosi, tarife su u opsegu od nekoliko desetina do nekoliko hiljada dolara. Nude se različite usluge od ispravljanja ocena u školama, preko krađi pristupnih šifri za različite naloge, do prisvajanja osetljivih podataka privrednih društava ili organizacija.

Klijenti koji iz bilo kojih razloga imaju potrebu da angažuju plaćene ubice, mogu zadovoljiti svoje potrebe stupanjem u kontakt preko dark web-a. Jedan od primera opisan u [11] prikazuje osobu, navodno verifikovanog plaćenika "sa osmogodišnjim iskustvom" koji nudi usluge isključivo za plaćenje unapred u Bitcoin-ima. U kontaktu sa ovakvim osobama dozvoljeno je samo razmenjivanje informacija o žrtvi. Zahteva se da cela komunikacija, kao i svaki kontakt email-om moraju biti kriptovani. U slučaju da bilo koji deo komunikacije nije kriptovan, biće obrisan. Portali koji nude ovakve tipove uluga veoma često navode da su njihovi članovi bivši vojnici i plaćenici Legije stranaca. Ovakvi portali posvećuju veliku pažnju zaštiti komunikacije i tajnosti klijenata. Od informacija o meti prema kojoj će delovati, ovi online plaćenici zahtevaju ime, kućnu i adresu na kojoj im se nalazi radno mesto, što više fotografija i podataka o tome s kim žrtva živi, registarski broj, opis i sliku vozila koje koristi.

U zavisnosti od dogovora, tim ubica navodi da pripreme za posao, putovanje, lociranje i praćenje mete zahtevaju oko dva meseca, pri čemu troškovi kupovine avionske karte, oružja i smeštaja, po njihovim tvrdnjama, nisu uračunati u cenu samog ubistva. Jedan od portala pod nazivom *C'thulu* nudi odabir načina ubistva od regularnog, preko mučenja i silovanja, do bombaškog napada. Cene usluga su u rasponu od 3.000 dolara do 180.000 dolara u zavisnosti od odabrane kategorije i društvenog položaja žrtve. Cena se naravno razlikuje od toga da li je osoba koju treba ubiti pojedinac nepoznat široj javnosti ili se radi o javnoj ličnosti, političaru, pripadniku organa reda, itd.

Na dark web-u se veoma često obavlja trgovina falsifikovanim novcem, menicama, čekovima, kao i drugim hartijama od vrednosti. Stranice koje nude trgovinu falsifikovanim novcem navode različite vrste garancija u vidu opisa postupka kreiranja koji pokazuje da je kako tvrde prodavci falsifikovani novac kreiran na identičan način kao i pravi novac. Dostupne su praktično sve valute koje se isplati falsifikovati. Kvalitet falsifikovanih novčanica kao i količina koja se prilikom jedne transakcije može nabaviti variraju od slučaja do slučaja. U ovakvim transakcijama, najčešći pariteti su da se za 600 pravih američkih dolara mogu se dobiti 2.500 falsifikovanih, a za 500 pravih eura 2.000 falsifikovanih. Sve transakcije se obavljaju uz obećanje da kupljene novčanice mogu proći standardne provere, uključujući i onu ultraljubičastim svetlom [14]. U velikom broju slučajeva se naravno plaćanje za falsifikovani novac odvija u Bitcoin-ma.

Postoji i nekoliko sajtova na dark web-u koji tvrde da se bave prodajom pasoša i ličnih dokumenata. Cena ovakvih usluga zavisi od zemlje za koju se dokumenta izrađuju, kao i od samog prodavca. Validnost ovakvih dokumenata je teško proveriti, posebno kada se radi o državljanstvima. Ovakvi servisi mogu i biti kreirani u domenu prevare za emigrante koji žele da na bilo koji način dođu do državljanstva zemlje u kojoj se nalaze. Cena recimo pasoša, vozačke dozvole i lične karte za Australiju iznosi 800 eura na portalu pod nazivom Fake ID. Na istom portalu najskuplja dokumenta su za USA, a najjeftinija za Maleziju [13].

Ukradene informacije o bankarskim nalozima, brojevima kreditnih kartica, online aukcijama, takođe se mogu kupiti. Atlantik karding je lokacija na dark web-u na kojoj se mogu kupiti informacije o tuđim kreditnim karticama, adresama i sličnim privatnim informacijama. Cene se kreću između 5 i 80 dolara. Kvalitet informacija zavisi od cene. Sa druge strane, prodaja naloga se vrši na jedan od dva načina. Prvi način podrazumeva kupovinu pojedinačnog naloga, za koji su date detaljne informacije o količini sredstava na njemu. Drugi način podrazumeva kupovinu veće količine naloga od kojih je određeni broj verovatno validan. Prvi način je daleko isplativiji, jer kupac uvidom u količinu sredstava na računu ima veće garancije da će uložena sredstva povratiti i dodatno zaraditi. Pored toga, postoji i ponuda kupovine fizičkih platnih i kreditnih kartica različitih banaka [13].

Postoji veći broj primera gde su kao predmet sticanja zarade korišćena deca. Tokom 2011. godine Europol je u koordinaciji sa trinaest agencija različitih zemalja uhapsio 184 osobe osumnjičene za zlostavljanje dece i širenje dečije porrnografije u vidu slika [15]. Slična akcija sprovedena je u Velikoj Britaniji. U ovoj akciji uhapšeno je 650 ljudi, koji su optuženi za različine vidove zlostavljanja dece, od posedovanja slika, pa čak i do konkretnih slučajeva podvođenja [16]. Na teritoriji Severne Irske u 2015. godini uhapšeno je 37 osoba pod optužbom da su se na Tor-u bavile distribucijom dečije pornografije i pedofilijom [17].

Postoje podaci da su pripadnici grupe Islamska država Irak i Levant upravo korištenjem dark weba osigurali naoružanje za napade u Parizu i Briselu. Organizacije kao što su ISIL i Al-Kaida koriste dark web za aktivnosti koje nisu direktni napadi putem interneta, ali su u funkciji osnovnih ciljeva i posredna su

sredstva terora i terorizma. Jedan od vidova korišćenja interneta u terorističke svrhe odnosi se na vrbovanje i regrutovanje novih snaga, uglavnom mlađe populacije, širenjem propagandnih materijala kao što su video snimci u kojima opisuju ciljeve za koje se bore, načine borbe i značaj njihovog rata. Određen broj ljudi se pronalazi u tome i želi da im se priključi. Pored regrutovanja novih članova dark web servisi u funkciji terorizma veoma često se koriste za ostvarivanje sigurne komunikacije. Ovakva komunikacija je nalik društvenim mrežama i forumima, sa razlikom da je praćenje ovakvog vida komunikacije gotovo nemoguće. Takođe teroristi koriste dark web za ostvarivanje finansiranja svojih organizacija, pranje novca, kupovinu oružja municije i eksploziva. Sve pomenute aktivnosti kao i u ranijim primerima zloupotreba interneta obavljaju se u bitcoin-ima ili drugim vidovima kriptovanih valuti [18].

Web portali na dark web-u se štite na najrazličitije načine. Jedan od osnovnih načina jeste provera posetilaca koji prema ponašanju odudaraju od standarnog šablona. Ukoliko administratori prema ponašanju i rečniku prepoznaju posetioca kao nametljivog uljeza pokrenuće osnovnu proveru. Prismotra se može prepoznati ukoliko posetilac u jednom trenutku, dok kuca, vidi samo red u kome treba da se unese tekst, bez prethodnog teksta. Sledeći korak jeste da se na računar posetioca ubaci takozvani key logger program koji snima sve što posetilac kuca na tastaturi. Na ovakav način ostvaruje se maksimalna kontrola nad svim što posetilac radi sve dok se ne proveri o kome se radi i koje su mu namere.

IV. ZAKLJUČAK

Poput izdvajanja u načinu organizovanja životnih aktivnosti, priklanjanju kriminalnim grupama ili vođenju mirnog načina života, izvojili su se i internet korisnici. Upravo iz tog razloga ideja anonimnosti na kojoj je bazirano kreiranje stranica dostupnih na deep web-u zloupotrebljena je sa najgorim namerama. Dark web i sve ono što se može naći na stranicama koje mu pripadaju svrstava ga u broj jedan cyber pretnju. Obim ilegalnih aktivnosti i njihova raznovrsnost, kao i zastrašujući broj korisnika ovog dela Interneta pokazuju da su trgovina narkoticima, oružjem, švercovanom robom, delovanje terorističkih grupa, njihova organizacija, snabdevanje oružjem i municijom, regrutovanje novih članova kao i zadovoljavanje različitih potreba dobili jednu potpuno novu dimenziju gde je veoma teško utvrditi ko je sa suprotne strane servera. Borba protiv aktivnosti prisutnih na dark web-u zahteva angažovanje stručnih ljudi iz oblasti borbe protiv cyber kriminala. Međutim i pored svih napora ovakva borba nije nimalo laka o čemu svedoči i pomenuti primer *Silk Road* portala koje je odolevao svakom mogućem gašenju duži niz godina.

Sama veličina deep web-a i potraga za anonimnošću nesumnjivo dovode do pitanja šta je to što je dovelo do toga da toliki obim podataka bude podvedem pod deep web, i da li je privatnost korisnika površinskog dela web-a toliko ugrožena? Odgovor na ovo pitanje i kreiranje veze između smanjenja privatnosti korisnika i kreiranja deep web-a je jedno od mogućih proširenja ovog istraživanja kojim će se autori baviti u nastavku svog rada.

ZAHVALNICA

Ovaj rad je podržan od strane Ministarstva prosvete, nauke i tehnološkog razvoja, Vlade Republike Srbije u okviru projekta TR 35023 i TR 35026.

LITERATURA

[1] M. Mitrović, Mračne tajne globalne mreže, Nova energija, Preuzeto: 21.12.2016., sa : http://www.novaenergija.net/mracne-tajne-globalne-mreze/

[2] Bright Planet, Clearing up confusion – deep web vs. dark web, Retrieved: 21.12.2016., from: https://brightplanet.com/2014/03/clearing-confusion-deep-web-vs-dark-web/

[3] M. Stojković, Fejsbuk i praćenje korisnika putem dodataka za društvene mreže, PravoIKT Serbian ICT Law resource, Preuzeto: 25.12.2016. sa: http://pravoikt.org/fejsbuk-i-pracenje-korisnika-putem-dodataka-za-drustvene-mreze/

[4] Steve, Surface web, deep web, dark web -- What's the difference?, CambiaResearch, Retrieved: 25.12.2016., from: https://www.cambiaresearch.com/articles/85/surface-web-deep-web-dark-web----whats-the-difference

[5] Z. Čekerevac, Z.Dvorak, and P. Čekerevac, "Da li je „tamni internet" dubok i taman? ", FBIM Transactions, str. 1-12, 2016.

[6] C. Grannan, What's the Difference Between the Deep Web and the Dark Web?, Encyclopedia Britannica, Retrieved: 27.12.2016. from: https://www.britannica.com/demystified/whats-the-difference-between-the-deep-web-and-the-dark-web

[7] CARNet, "Tor - mreža za anonimnost", CarNet-Hrvatska akademija i istraživačka mreža. str. 1-15, 2007.

[8] K. Zetter, "How the Feds Took Down the Silk Road Drug Wonderland" Wired, Retrieved 10.01.2017., from: www.wired. com/2013/11/silk-road/.

[9] J. Cook, "FBI Arrests Former SpaceX Employee, Alleging He Ran The 'Deep Web' Drug Marketplace Silk Road 2.0", Business Insider, November 2014., Retrieved 09.01.2017., from: www.businessinsider.com/fbi-silk-road-seizedarrests-2014-11.

[10] K. Knibbs, "Silk Road 3 Is Already Up, But It's Not the Future of Darknet Drugs." Gizmodo, November 2014. Retrieved 10.01.2017. from: http://gizmodo.com/silk-road-3-is-already-up-butits-not-the-future-of-da-1655512490

[11] M. Luković, "Deep internet - Droga, ubistva, pornografija - šta se sve krije u crnoj web rupi?", Before After, Maj 2014, Preuzeto 12.01.2017., sa: http://www.beforeafter.rs/tehnologija/deep-internet/

[12] N1, "Darknet - mračna strana surfovanja internetom", N1 SCI-TECH portal Zagreb, April 2015, Preuzeto 12.01.2017., sa: http://rs.n1info.com/a50647/Sci-Tech/Sve-o-Deep-Web-ili-Darknetu.html

[13] V. Ciancaglini, M. Balduzzi, R. McArdle, and M. Rosler, "Below the Surface: Exploring the Deep Web", Trend Micro, pp. 1-48.

[14] Vijesti online, "Tamni internet: Tu su hakeri, prodavci ljudskih organa, oružja", Vijesti online, April, 2015, Preuzeto 30.10.2016., sa: http://www.vijesti.me/techno/tamni-internet-tu-su-hakeri-prodavci-ljudskih-organa-oruzja-828308

[15] Europol, "Operation Rescue", Europol, 2014., Retrieved 19.09.2016., from: www.europol.europa. eu/content/operation-rescue.

[16] BBC, "Child abuse image investigation leads to 660 arrests", BBC News, July 2014., Retrieved 19.9.2016. from: www.bbc.com/news/uk-28326128.

[17] BBC, "50 arrests in NI online abuse images probe in past year, say police." BBC News, 2015, Retrieved 20.10.2016., www.bbc.com/news/uk-northern-ireland-31896685.

[18] G. Weimann, "Terrorist Migration to the Dark Web, " Perspectives on terrorism, vol. 10, no. 3, 2016.

ABSTRACT

Privacy and protection are one of the main lifestyle issues people tend to preserve and protect. Rapid technological development, exchange of large amounts of data as well as the increasing use of the Internet and social networks can significantly reduce privacy protection. Modern browsers register and save every user activity. In order to prevent indexing ond activity tracking, and therefore increase privacy protection, a new part of the Internet, popularly called deep web, has been developed. However, along with all the advantages this mode brings, inabily of indexing and user activity tracking in deep web part of the Internet have created a platform for illegal activities. One part of the Internet that offers wide variety of illegal activity is popularly reffered as dark web. It is known for pages that are related to different illegal activities. The paper gives a brief overview of registered illegal activities generated using dark web. These activities are the main indicator of anonymity abuse afforded by this part of the Internet.

DEEP AND DARK WEB - NECESSITY OR MISUSE

Milos Ilic, Petar Spalevic, Zaklina Spalevic, Mladen Veinovic