Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

ILEGALNE AKTIVNOSTI U NEVIDLJIVOM WEB-u
ILLEGAL ACTIVITIES IN THE INVISIBLE WEB

Pregledni naučni rad

spec.krim. Marjanović Marjan[76]

Sažetak

Inspiracija za rad: Uloga hakera u vršenju ilegalnih aktivnosti pod okriljem nevidljivog dijela World Wide Web-a podstakla je autora na promišljanje o povezanosti ovih specifičnih delikvenata sa skrivenim oblastima savremene informatičke sfere.
Ciljevi rada: Autor svoja razmišljanja posvećuje ustanovljavanju veze, koju hakeri sasvim moguće imaju sa potencijalnim mogućnostima okruženja Deep Web-a.
Metodologija/dizajn: Analiza pojmova *haker* i *nevidljivi Web*, kroz njihovu fenomenološku uzajamnost, opredijelila je metodološki napore autora u svom istraživanju.
Ograničenja rada/istraživanja: Ograničenja u prikazivanju potpune slike temeljnih pojmova u ovom radu mogu predstavljati njihovi tekući vidovi ispoljavanja, koje autor zbog tehničke nemogućnosti sagledavanja cjelokupnog varijetata njihovih pojavnih oblika nije bio u mogućnosti da predstavi.
Rezultati: Veza hakera sa Deep Web-om, kako smatra autor, postoji u brojnim oblicima kriminalnih aktivnosti, od kojih će u radu biti akcentovani neki od hakerskih napada i terorizam.
Generalni zaključak: Nevidljivi deo Web-a, a posebno njegova tamna zona tzv. Darknet, čine naročitu pogodnost za djelovanje hakera *ante delictum*, kao i *post delictum*, čineći istovremeno optimalno informatičko okruženje za razmjenu podataka koji vode ka pripremanju ilegalne aktivnosti, baš kao i ka kapitalizovanju štete nastale hakerskim napadom.
Opravdanost istraživanja/rada: Ukazivanjem na postojanje veze hakera sa skrivenim dijelom World Wide Weba, autor nastoji da utiče na pojačavanje opreza i unapređivanje zaštite od hakerskih napada određivanjem preventivnog postupanja, koje svaki korisnik savremene globalne komunikacije može upotrijebiti na ličnom planu u razmjeni podataka putem Interneta.

Ključne riječi

haker, hakerski napad, Internet, terorizam, Deep Web, Dark Web

Summary

Reason for writing and research problem (s): The very role of hackers while dealing with illegal activities within surroundings of the invisible part of the World Wide Web motivated the author to analyze relations between this special kind of offenders and hidden areas of modern informatics sphere.

[76] Institut za procjenu rizika i kritičnu infrastrukturu, Podgorica, Crna Gora, marjan.marjanovic@iprki.me, marjan@securityguardmn.com

Aims of the paper (scientific and/or social): The author focused his attention to establishing of link that, very possible, connects hackers to the potential opportunities of the Deep Web zone.
Methodology/Design: Analyze of terms *hacker* and *invisible Web*, done through their phenomenological mutuality, prevailed the author's methodological efforts in this research.
Research/Paper limitation: Actual forms of exposing basic terms in the paper are probable limitation to have them presented completely, because of technical lack of the author's capability to make the full-scaled overview of their existing modalities.
Results/Findings: According to the author's opinion, the link between hacker and the Deep Web exists in the various types of criminal activities having hackers' attacks and terrorism as highlighted in the paper.
General Conclusion: Invisible part of Web and its dark zone so-called the Darknet, especially, make specific suitability for hacker's activity *ante delictum*, just as *post delictum*, having at the same time optimal informatics surroundings enabled for the data exchanging as ground of illegal activities preparation and likewise of getting profit out of damage committed by hacker's attack.
Research/Paper Validity: By pointing out on existing of connection between hacker and hidden part of the World Wide Web, the author tends to get caution heightened and to enhance protection considering hackers' attacks by defining preventive proceedings that can come in handy in exchanging personal data of every user of Internet global communication network.

Keywords
hacker, hacker's attack, Internet, terrorism, the Deep Web, the Dark Web

UVOD

Opseg Interneta daleko premašuje njegov vidljiv površinski dio, koji mnogi od nas dnevno posjećuju u svojim, gotovo, rutinskim pretragama. Drugi njegovi segmenti sadržani su u ukupnosti informatičko-komunikativnih mogućnosti nevidljivog dijela World Wide Web-a, koji ostaje skriven za standardne pretraživače, kao što je Googl. Ovaj virtuelni prostor za razmjenu informacija, nezamislivih granica, nazivamo Deep Web i on predstavlja izraz želja i neophodnosti različitih društvenih individualnih i grupnih, kako resornih tako i vanresornih, subjekata za diskretnom razmjenom podataka. Ovaj duboki i nevidljivi Web, ogromnih razmjera i neuporedivo prostraniji od svog vidljivog i svima dostupnog antipoda, pored legitimne namjene može imati i svoju tamnu stranu oličenu u njegovom skrivenom dijelu poznatom kao Dark Web ili Darknet. Ovaj tamni i nedostupni dio Web-a ima sve predispozicije za kreiranje informatičkog okruženja podesnog za skrivenu komunikaciju između kriminalnih grupa i pojedinačnih nosilaca kriminalnih aktivnosti. Pomoću naročitih softvera, kao što je The Onion Router (TOR), korisnici tamnog dijela Web-a uz zametanje tragova svog prisustva korišćenjem velikog broja računara drugih korisnika, krstare informatičkim vodama Deep Web-a tražeći mogućnosti za svoje ilegalno djelovanje (Finklea, 2017). Sajtovi za pretraživanje u nevidljivom Web-u olakšavaju surfovanje kroz Darknet, nudeći kategorizovane sadržaje koji se odnose na ilegalni promet opojnim drogama, krijumčarenje i nezakonito pribavljanje vatrenog oružja, organizovanje

trgovine falsifikovanim proizvodima, obezbeđivanje krivotvorenog novca ili ličnih dokumenata.[77] Načini komunikacije u Deep Web-u odnosno Darknet-u odvijaju se kao i na površinskom dijelu Web-a, razmjenom poruka posredstvom TOR-a, upotrebom zaštićenih elektronskih adresa, pa čak i brže kroz četovanje. Informatički alat, poput TOR-a, čija svrha je obezbjeđivanje anonimnosti sadržaja i aktivnosti u okolnostima nevidljivog Web-a, služi istraživačima i stručnjacima iz oblasti bezbjednosti da konstanto razvijaju i unapređuju načine i sredstva za otkrivanje skrivenih servisa i pojedinaca, koji vrše kriminalne aktivnosti u Darknet-u, kao tamnom i skrovitom dijelu Deep Web-a.

Okruženje dubokog Web-a pogoduje širokoj skali legalnih i nedozvoljenih aktivnosti, od očuvanja privatnosti korisnika do trgovine ukradene robe, uz upotrebu virtuelne valute Bitcoin (Finklea, 2017). Servisi kojima se eksploatiše Deep Web služe izbjegavanju zabrana, pristupu nedozvoljenim sadržajima,[78] ali i zaštiti tajnosti osjetljive komunikacije ili poslovnih planova. Ipak, veliki broj zlonamjernih učesnika, od nosilaca klasične kriminalne aktivnosti do članova terorističkih ćelija, pojedinačnih terorista, subjekata obavještajne djelatnosti odnosno aktera industrijske špijunaže, uzrokovao je da se u tamnom Webu odvijaju forumi za konverzaciju, razmjenu podataka, dogovore, koordiniranje kriminalnih aktivnosti i samo izvršenje krivičnih djela.

Međutim, baš kao što delinkventska populacija može koristiti anonimno okruženje Deep Web-a, tako ono služi i potrebama organa krivičnog gonjenja, ali i vojnih i obavještajnih subjekata u svrhu obavljanja nadzora i kontrole. Naravno, ovakve opcije omogućuju i hakerima da izvode svoje napade radi obaranja sajtova, prekida komunikacije, neovlašćenog upadanja u zaštićene sisteme, korišćenja tuđih ličnih podataka, krađe identiteta, pristupa poslovnim podacima, preusmjeravanja legalnih i ilegalnih novčanih tokova i preduzimanja drugih aktivnosti na ugrožavanju sistema za komunikaciju i skladištenje podataka u uslovima nevidljivog Web-a i njegovog skrivenog segmenta Darknet-a.

HAKERI I NEVIDLJIVI WEB

Internet je danas prepun prijetnji po bezbjednost korisnika. Hakeri i virusi vrebaju pod maskama raznovrsnih reklama i obavještenja čijim pregledom se aktiviraju hakerski upadi. Otvaranjem takvog sadržaja lozinka korisnika, istorija njegovih pretraga, elektronske poruke, ali i neke lične sklonosti i interesovanja, dolaze u ruke anonimnih delikvenata koji se nalaze bilo gdje u svijetu (Omand, 2016). Nakon toga dragocjeni podaci bivaju zlonamjerno prodati ili razmijenjeni u nevidljivom Web-u. Višestruko veći od površinskog Web-a koji je izraz uobičajene predstave redovnog korisnika Interneta, skriveni Web je informatičko okruženje koje okuplja sve one kojima je neophodna anonimnost. Pristupom preko TOR-a, koji se može besplatno preuzeti, omogućeno je kretanje kroz brojne serverske mreže koje su interkontinentalno rasprostranjene. U tamnom dijelu nevidljivog

[77] Kao što je npr. „Hidden Wiki".
[78] Ovde se misli na iskorišćavanje djece u pornografske svrhe.

Web-a, zvanom Darknet, zainteresovani korisnik pronaći će sadržaje kojima nije moguće neopaženo pristupiti u vidljivom Web-u, a koji se odnose na ilegalnu trgovinu oružjem, dječju pornografiju, ilegalnu ponudu opojnih droga, kompjuterske viruse, ukradene kreditne kartice, filmsku i muzičku pirateriju, uz mogućnost anonimnog plaćanja nabavke navedenog digitalnim novcem.

Prvi hakeri bili su srednjoškolci i studenti, koji su svoj informatički talenat usmjerili na zbijanje šala sa računarski povezanim sistemima.[79] Problem je uzrokovan činjenicom da se gotovo svaki sistem, od banke i bolnice do kritične infrastrukture, odjednom digitalizovao. Ovo je doprinijelo mogućnosti lake zarade i velikog profita za hakere (Pagliery, 2015). Njihova aktivnost postala je ilegalna, ali ih to nije sprečavalo da neovlašćeno preuzimaju, koriste i prodaju podatke. Što je više subjekata i informacija bilo povezano putem Interneta, rasle su mogućnosti i informatički volumen nevidljivog Web-a i njegovih hakerskih korisnika.

Pojam haker prati podrazumijevajuće loša konotacija, ali nemaju svi hakeri loše namjere u svojim postupanjima. Zapravo, neki autori smatraju da postoji hakerska etika čiji parametri prate nivo bunta protiv tehnološke dominacije u jednom društvu (Martin i Newhall, 2016). Haker može biti svako ko posjeduje znanje i vještine da putem informatičkog programa izbjegava bezbjednosne mjere koje štite lični računar, tehnički uređaj ili računarsku mrežu. Hakerski upad u računarski sistem ili sam računar je ilegalan čin, izuzev ako nije učinjen uz pristanak vlasnika. Šta je to što potiče hakera da prodre u nečiji računar i otuđi ili uništi lične podatke ili čak preusmjeri tuđa finansijska sredstva? „Thycotic“, softverska kompanija koja je specijalizovana za zaštitu pristupnih lozinki, sprovela je istraživanje u kome je postavljeno pitanje američkoj hakerskoj grupi „Black Hat“ zašto čine ovakve zlonamjerne akte.[80] Tom prilikom je 51% hakera izjavilo da ih neovlašćeni upadi u tuđe zaštićene sisteme uzbuđuje i zabavlja, njih 19% u svojim odgovorima bilo je opredijeljeno za finansijsku dobit kao smisao hakerisanja, etičkim razlozima rukovodilo se 29% ispitanika, a preostalih 1% imalo je želju da budu ozloglašeni (Williams, 2015).

Hakere možemo klasifikovati u tri grupe. Kompanija za tehnološku bezbjednost „Norton Security“, svaku od grupa simbolično je predstavila šeširom određene boje. Tako se razlikuju „bijeli“, „sivi“ i „crni šeširi“, kao tri esencijalno različite grupe hakera. Ovi nazivi potiču od crnih šešira koje su u filmovima o Divljem Zapadu nosili tzv. „loši momci“, dok su šešire bijele boje nosili oni koji su poštovali zakon. Termin „sivi šešir“ odnosio bi se na sve one hakere koji se ne mogu svrstati kategorično na navedene opozitne strane. Inače, hakeri su označeni na pomenuti način prema razlozima koji ih pokreću u njihovim postupanjima, kao i u odnosu na to da li su njihovi akti nezakoniti (Kovacs, 2015). „Bijeli šeširi“ koriste svoje znanje u oblasti informatičke tehnologije isključivo u dobre svrhe. Često ih nazivaju „etičkim hakerima“ jer ih kompanije plaćaju radi rešavanja problema i ojačavanja mjera bezbjednosti u svrhu zaštite programa, koje koriste u svom radu (Kovacs, 2015).

[79] Tako je jedan od prvih računarskih virusa načinio diplomac američkog Univerziteta Cornell.
[80] Bilo je ispitano 127 osoba.

Primjer ove vrste hakerisanja je program sa nazivom „HP Tipping Point“, koji je pokrenut 2005. godine radi detektovanja manjkavosti u sistemu zaštite Interneta. Neki autori navode da je ovakav „lovački“ program podešen da prima preporuke za prevenciju upada u sistem (Zetter, 2013). U tom smislu, nedostaci u zaštiti sistema pogodni su za korigovanje, na koje „bijeli hakeri“ ukazuju programerima konkretne kompanije. „Sivi šeširi“ su posvećeni traženju propusta u zaštiti sistema i njegova ranjivost služi im za zabavu. Kada jednom otkriju „rupu u brani“ ova vrsta hakera će učiniti dvije stvari: obavijestiće kompaniju ili pojedinca o postojećoj slabosti što će naplatiti manjim novčanim iznosom radi otklanjanja nedostatka ili će o ovakvom problemu obavijestiti javnost putem Interneta (Kovacs, 2015). Na prikazani način francuske komanije „Vupen“ i „Zerodium“, koje su specijalizovane za otkrivanje propusta u on-line bezbjednosti (Zetter, 2016), uspješno su detektovale dvije slabosti u Crome's Pwn2Own zaštitnom programu i pomogle rešavanje ovog problema (Zetter, 2012). „Crni šeširi“ su najopasnija vrsta hakera. Ovi hakeri su, također, vrlo vješti u upadima u računarske mreže jer umiju da naprave zlonamjerne programe (malware) putem kojih ostvaruju pristup u mrežne informatičke sisteme (Kovacs, 2015). Postoji veliki broj hakerskih grupa „crnih šešira“ u svijetu, koji neprestano izvode nedozvoljena hakerska postupanja. Jedna od najpoznatijih su „Anonymous“ koji operišu kroz pojedinačne akcije kojima se drugi pridružuju, te tako udruženi postižu uspjeh (Norton, 2012).

Veliki je broj preduzetih istraživanja psihološke pozadine hakerske motivisanosti za potčinjavanjem sistema. Prema riječima jednog od rukovodilaca u kompaniji „Thycotic“,[81] otkrivanje razloga zašto je neko zainteresovan za krađu podataka ili hakovanje sistema je vrhunski prioritet u obezbjeđivanju zaštite pristupa tajnim dokumentima. Zaštita informacija je uvek od najveće važnosti, obzirom da terorističke grupe ulažu stalne napore kako bi izvršile upade u mrežne sisteme i uništile ili neovlašćeno preuzele povjerljive informacije.

Dakle, možemo zaključiti da nevidljivi Web ima dvostruku ulogu u odnosu na hakersku aktivnost. Najprije, pruža mogućnosti za njihovo djelovanje uz postojanje svojih tamnih zona oličenih u Darknetu, kao garanciji anonimnosti i skrivenosti prisutnih korisnika. Zatim, obezbjeđuje utočište i zametanje tragova brojnim nosiocima kriminalnih aktivnosti u cyber okruženju, između kojih i hakerima. S druge strane, hakeri koriste neslućene razmjere Deep Web-a, pogotovo njegovog tamnog dijela Darkneta, kako bi svoje napade izvodili kako na ciljeve površinskog Weba, tako i na određene mete iz kriminalnog miljea dubokog Weba. Tako se, naprimjer, preusmjeravanje finansijskih sredstava može vršiti i sa skrivenih računa članova organizovanih kriminalnih grupa, ali se mogu blokirati i cyber aktivnosti terorističkih ćelija, te ometati njihova diskretna komunikacija i vođenje poslova, kojima se finansiraju.

[81] Riječ je o ekspertu po imenu Jonathan Cogley.

ZNAČAJ TAMNOG WEB-a

Dark Web je informatički prostor u kome se odvija najviše on-line kriminalnih aktivnosti i nalazi se daleko van efektivnog domašaja organa krivičnog gonjenja. Anonimnost je pravilo za postupanje i kretanje u okruženju tamnog Web-a, a identitet i pozicija korisnika skriveni su i od najupornijih nastojanja policije i obaveštajnih agencija (Omand, 2016).

Darknet funkcioniše prema različitim kriterijumima u odnosu na ostale djelove Interneta. Uobičajeno je da korisnik upotrebljava pretraživač kao što je Google, koji omogućuje pristup traženoj adresi na Web-u. Željena destinacija biće dostignuta jer je sadržaj na vidljivom površinskom Web-u indeksirana, zbog čega je pretraživački programi mogu automatizovano eksploatisati i održavati neprestano sakupljajući i klasifikujući podatke. Ovo olakšava globalni Domain Name sistem, koji pojednostavjuje registrovanje Web adrese u jedinstveni 32-bitni, a u današnje vrijeme i 128-bitni digitalni numerički zapis, u smislu Internet protokola odnosno IP adrese, kako bi usmjerio server da uputi korisnički zahtjev na odgovarajući sajt. Ipak, ovaj površinski Web je samo mali dio Interneta, čak 500 puta manji od njegove ukupnosti. Preostali dio, tzv. duboki Web, nije dostupan redovnom korisničkom protokolu jer mu nije ni namijenjen.

Moglo bi se napraviti poređenje nevidljivog segmenta Interneta sa dijelom grada u kome se nalaze poslovne kompanije, istraživačke laboratorije i vladine agencije, kojima prosječan građanin nije ovlašćen da pristupi. Očigledno je da to može da učini samo određena osoba uz posebnu propusnicu (Omand, 2016). Prateći dalje naš zamišljeni grad, Darknet bi predstavljao kvart „crvenih fenjera“ sa veoma malim brojem zgrada, koje bi inače bilo teško pronaći, jer skriveni operateri ne žele da eksponiraju aktivnosti koje se odvijaju u „zgradama“. U nekom trenutku, ovde se mogu pronaći noćni klubovi, kockarnice, narkomanska svratišta ili bordeli, ali i mjesta okupljanja siromašnih mladih slikara i pisaca, radikalnih političara i disidenata (Omand, 2016). Zbog navedenog, može se zaključiti da je tamni Web ukupnost sajtova koji mogu biti dostupni i vidljivi smo onim korisnicima koji baš njih i traže, naravno pod određenim uslovima zaštite bezbjednosti operatera sajtova i njihovih posjetilaca. Jaka enkripcija i protokoli koji garantuju anonimnost obezbjeđuju skrivenost IP adresa servera pokretača sajtova Darkneta, tako da se ne može utvrditi ko ih posjećuje čak i kada bi ovi sajtovi bili locirani i stavljeni pod prismotru.

Početnim istraživanjima ustanovljeno je da Deep Web, time i Darknet, predstavlja najveći izvor svježih informacija na Internetu. Sajtovi koji ih sadrže, po prirodi, su malog obima ali kompleksne dubine, u poređenju sa regularnim sajtovima površinskog Web-a. Paradoksalno, ali istinito, zaštićenost sadržaja sajtova tamnog Web-a doprinosi njihovom većem kvalitetu i vrijednosti od onih u vidljivoj zoni Interneta. Više od polovine sadržaja nevidljivog Web-a smješteno je u naročite direktorijume, kao što je www.thehiddenwiki.net, što ih čini dostupnijim i preciznijim odredištima pretrage (Sui, Caverlee i Rudesill, 2015).

Zbog svega navedenog, Darknet je izuzetno nekontrolisan dio Interneta. U okruženju tamnog Web-a anonimnost je primarna karika u protokolarnom lancu ostvarivanja pristupa, kako bi se operateri i ostali korisnici osigurali da ničije pretraživanje Darkneta ne bude praćeno od strane policije ili nekog drugog bezbjednosnog subjekta (Omand, 2016).

HAKERSKI NAPADI I TERORIZAM

Terorizam je akt upotrebe sile i prijetnje radi zastrašivanja i prisile. Godinama smo svedoci terorističke prijetnje na svjetskom planu, koja se neprestano razvija. U poslednje vrijeme, sa tehnološkim napretkom, ova prijetnja postala je još prisutnija i destruktivnija.

Internet je postao neodvojivi dio svakodnevnog života u gotovo svakom kutku naše planete, što je pogodovalo prijetnji sajber terorizma da dostigne viši nivo nego ikada. Terorističke grupe poput ISIS-a i Al-Qaeda, sada, imaju mogućnost prikrivanja u debelim sjenkama digitalnog svijeta Darkneta i koriste enkriptovane poruke za širenje ekstremizma. Tamni Web nudi ovim radikalnim grupama nevidljivi prostor za regrutovanje i radikalizaciju, širenje propagande, uvećavanje finansijskih sredstava i koordiniranje akcija i napada (Weimann, 2016).

Na hiljade foruma i soba za četovanje, kako na površinskom tako i u tamnom Web-u, dostupno je potencijalnim sledbenicima radikalne i ekstremističke ideologije da stupe u kontakt i komuniciraju sa terorističkim ćelijama, te razmjenjuju sa njima podatke uz potpuno skrivanje svog identiteta. Još 2001. godine, Al Qaeda je svoj prvi forum plasirala na Internetu, koji jeste bio uklonjen, ali je pregršt drugih sajtova nasilih i ekstremnih islamista nastavilo da postoji čak i u vidljivom Web-u uz kontakte visoke frenkventnosti (Cox, 2015). Ova mjesta za on-line susrete nije moguće detektovati, niti im pristupiti sa globalnog korisničkog nivoa, zbog čega se mogu posmatrati kao virtuelna zona islamskih ekstremista. Kako bi što više širile svoje poruke i regrutovale nove sledbenike, terorističke grupe promovišu upotrebu ovakvih enkriptovanih i anonimnih sajtova. Naprimjer, ISIS-ov medijski predstavnik sa nazivom Al-Hayat Media Center postavio je link i smjernice za pristup novom sajtu u Dark Web-u (Weimann, 2016).

Inače, terorističke organizacije koriste tamni Web kao informatički prostor u kome skrivaju svoje finansije, uvećavaju zaradu, vrše novčane transfere, ilegalno nabavljaju eksplozivna sredstva i oružje, pri čemu koriste virtuelni novac (Weimann, 2016). Obzirom da se može transferisati bez mogućnosti praćenja tokova transfera, Bitcoin je kao izmišljena valuta postao neka vrsta terorističke monete. Terorističke grupe ostvaruju prihode, iz kojih finansiraju napade, putem donacija od simpatizera ili prodajom ukradene robe. Dark Web podstiče rast i razvoj terorizma i to od malih grupa, koje djeluju na određenoj geografskoj lokaciji, do globalne prijetnje. Sa svakodnevnim tehnološkim progresom, prijetnja terorizma se sve više širi i uvećava bez obzira na napore vlada u svijetu da održe korak u ovoj borbi sa nevidljivim protivnikom.

Povezanost hakera sa terorizmom dolazi od mogućnosti da u tamnom Web-u hakeri prodaju kodove za pristup određenim osjetljivim sistemima,[82] nudeći ih onome ko najviše ponudi na kriminalnom tržištu. Kupci mogu biti terorističke grupe, pojedini ekstremisti, diktatorski režimi, državne obaveštajne službe, organizovane kriminalne grupe, kao i sajber ratnici[83] (LeFrancois i sar., 2018). Primjer za ovakvu vezu hakerskih napada i terorizma upravo je prodavanje koda „Zero-day".

Kod „Zero-day" odnosi se na ranjive softvere odnosno one sa nedostacima, koji su zbog toga pogodni za eksploatisanje ili napadanje uz upotrebu zloćudnih kodova radi plasiranja virusa, trojanaca odnosno drugih malware-a. Naziv „Zero-day" potiče od broja dana u kojem vremenskom periodu je otkrivena slabost softvera od strane njegovog tvorca ili prodavca. Obzirom da su osjetljive tačke u ovakvim slučajevima nepoznate autorima i prodavcima softvera, oni su veoma opasni po računarske sisteme jer sistemi zaštite od malware-a prilikom ažuriranja nisu u mogućnosti da ustanove propust i da detektuju prostor za hakerski napad kroz taj propust. Ovo je razlog zašto je „Zero-day" kod dragocjen za hakere dajući im prilike za izvođenje napada, ali istovremeno i rijedak da se pribavi (Zetter, 2014).

Hakeri su uvijek korak ispred u traženju opcija za napade na Web-u. Tako su u prilici da pronađu ovu vrstu koda, koja ukazuje na postojanje rupa u zaštitnoj strukturi softvera. Kada hakeri otkriju propust u softveru, sačine kod za probijanje zaštite, posle čega odlučuju šta će da učine sa tim podacima i kodom. Dok neki od njih o ovome obavještavaju prodavce softvera, drugi pronađeno prodaju bilo kome, od organizovanih kriminalnih grupa do zloglasnih pojedinaca koji vode diktatorske režime (Goodman, 2016).

Velikim tržištem za pronalaženje propusta u softverima upravljaju obavještajne službe jer su ovakvi kodovi izuzetno vrijedni, ne samo „crnim hakerima" već i državnim obavještajnim subjektima, kao i onim sajber ratnicima koji su resorno angažovani[84] (Greenberg, 2015). Primjera radi, u Sjedinjenim Američkim Državama, National Security Agency (NSA) je zbog velikog broja „Zero-day" propusta u programima bila prinuđena da ih detektuje i popravi do nivoa na kome ova ranjivost više nije ugrožavala američku nacionalnu bezbjednost (Greenberg, 2015). Naravno, postojeća prijetnja od terorističkih napada samo je pojačala ovu budnost vladinog sektora na međunarodnom planu.

[82] Kao što su to sistemi javnog transporta, koji podrazumijevaju drumski, železnički, vodni i vazdušni saobraćaj.
[83] Grupni naziv za individualne korisnike Interneta, koji svojim napadima nanose štetu ostalim korisnicima uz široku lepezu motivacije za ovakvo zlonamjerno postupanje na World Wide Web-u.
[84] Poput onih koje angažuju američke National Security Agency (NSA) i Cyber Command.

MOGUĆNOST ZAŠTITE OD SAJBER NAPADA

Hakerski napadi postaju sve češći i uobičajeniji jer ih olakšava činjenica da je sve više uređaja uvezano u informatičkom prostoru, koji neki autori nazivaju „Internetom stvari" (Thielman i Hunt, 2016). Malware-i mogu ugroziti svaki od umreženih uređaja, od aparata za kafu do frižidera, a da mjere zaštite zataje zbog nedovoljne brzine u odgovoru na prijetnju (Thielman i Hunt, 2016).

Poznavanje specifične opasnosti hakerskih napada i upućenost u brojne modalitete njihovih prijetnji, nisu dovoljni za formiranje konačnog odgovora na pitanje: „Kako da riješimo problem hakerisanja?" Prije nego što se posvetimo razmišljanju o zaštiti od hakerske prijetnje na pojedinačnom planu, važno je razmotriti na koji način će kompanije najprije na Web-u napraviti sigurne sajtove za svoje korisnike. Dugi niz godina, kompanije su zanemarivale značaj formulisanja poslovne strategije u kojoj je integrisano praktikovanje sajber bezbjednosti. Normativni poredak pati od nejasnoća, promjenjivih kriterijuma, te nestandardizovanih rešenja. Ukratko, proaktivan pristup poslovnih subjekata i dalje je nesistematičan i ad hoc determinisan, bez imperativa prilagođavanja okolnostima u nevidljivom Web-u u svrhu zaštite svojih korisnika od sajber napada, što u izvjesnoj mjeri pokazuje nemar kompanija prema održavanju stepena povjerenja konzumenata njihovih produkata (Lipka, 2015). Ipak, postoje i primjeri kako su neki segmenti u organizaciji društvenog života ozbiljno shvatili opasnost sajber prijetnji. Tako je, na Floridi, uspostavljen sistem upozoravanja na hakerske upade (LeFrancois i sar., 2018). U osnovi ovog sistema je kriterijum da se u lične podatke pored jedinstvenog broja socijalnog osiguranja i broja kreditne kartice, ubrajaju i elektronska adresa, kao i zaštitna pitanja i odgovori. Također, na Floridi se od kompanija zahtijeva da obavijeste tužioca ukoliko je više od pet stotina individualnih korisnika pogođeno sajber prijetnjom (LeFrancois i sar., 2018).

U svakom slučaju, koncept sajber bezbjednosti morao bi da predstavlja više od obavještavanja pojedinca da je bio izložen napadu hakera, u kojem su mu otuđeni podaci. Bez toga, primjer sa Floride ostaje na reaktivnom nivou jer se odnosi na amortizovanje posljedica problema, do koga je već došlo. Odgovarajući pristup u zaštiti od hakerisanja podrazumijeva proaktivnost i prilagodljivost koncepta, koji prati tehnološki razvoj, izmjenu normative i trendove poslovne prakse i koji bi, prije svega, bio preventivno usmjeren na samu realizaciju hakerskog napada.

Kompanije mogu primijeniti nekoliko strategija u svojim poslovnim planovima radi zaštite podataka svojih korisnika. Najprije, mogu da upotrebe postupak dvostruke potvrde prilikom pristupanja računima. Naprimjer, studentski portal američkog Univerziteta James Madison zahtijeva od korisnika unošenje podataka o korisničkom imenu i lozinki, poslije čega je neophodno odgovoriti na prethodno određeno zaštitno pitanje ili upotrebiti jednokratnu lozinku koja je dostavljena na korisnikovu elektronsku adresu (LeFrancois i sar., 2018). Pored ovog načina zaštite, kompanije mogu enkriptovati podatke koji se šalju putem javnih mreža ili se pohranjuju na mobilne uređaje, da bi potom od korisnika bilo

zahtijevano da izmijeni inicijalnu lozinku posle izdavanja računa (LeFrancois i sar., 2018). Naravno, ovi protokoli zaštite se uče i vježbaju, zbog čega je neophodno vršiti obuku zaposlenih bar na godišnjem nivou kako bi sigurnosne mjere bile uvijek odgovarajuće i ažurirane. Važno je da kompanije imaju zaštitne procedure koje ispunjavaju uslove obezbjeđivanja privatnosti i sigurnosti na svojim sajtovima. Između ostalog, to je garant održavanja povjerenja u takvu kompaniju, njen uspon na tržištu i zaštitu pojedinačnih korisnika od opasnosti sajber prijetnji.

Teško je predvidjeti nove moduse rizika koje sa sobom donosi brz tehnološki napredak, ali to ne znači da koncepti sajber bezbjednost ne budu integrisani u sisteme zbog čega kreatori zaštite moraju da komuniciraju sa poslovnim jedinicama i pravnim savjetnicima, kako bi ovi sistemi zaštite bili efikasni i ostvarivi. Kada se u kompanijama uspostavi zaštitni sistem za prepoznavanje prijetnje od hakerskih napada, neophodno je upozoriti pojedinačne korisnike o koracima koje moraju preduzeti kako bi se osigurali u on-line okruženju (Miller, 2016).

Funkcionisanje protokola sajber bezbjednosti je krupan zalogaj za kompanije i pojedince. Upotreba Interneta u obrazovanju i organizovanju svakodnevnog života je veliki zahtjev (Freedman, 2016). Elektronsko bankarsko poslovanje, kao i on-line kupovina, postali su neophodnost našeg doba. Trgovinska mreža gotovo u potpunosti se nalazi u okruženju World Wide Web-a. Sajber napadi ne završavaju se odredišnom destinacijom on-line transakcije. Neovlašćeni pristup podacima i hakovanje u on-line saobraćaju nanosi štetu globalnoj ekonomiji u svijetu u iznosu koji premašuje 400 milijardi američkih dolara godišnje (Johnson, 2016). Lični podaci, kao što su ime, prezime, adresa prebivališta, elektronska adresa, telefonski broj, dostupni su na Internetu. Distribucija ličnih podataka je uslovljena stepenom kulturnog razvoja jednog društva i običajnog miljea u kome se odrasta. Naša civilizacija uveliko počiva na imperativu on-line prisutnosti na World Wide Web-u, kako na privatnom, tako i na profesionalnom planu, a time i izloženosti napada iz dubokog i tamnog Web-a. Sve dok svjetska Internet mreža bude izgledala zabavno i bezopasno, postojaće i tamna strana globalnog Web-a, zbog čega je nužna zaštita sigurnosti svakog korisnika, bio on pojedinac ili kompanija, jedan od prioriteta vremena.

ZAKLJUČAK

Deep Web i Darknet sve više postaju predmet interesovanja istraživača, organa krivičnog gonjenja i donosilaca političkih odluka. Međutim, jasan uvid u prirodu i kvantitet ovih slojeva Interneta nije moguć. Anonimnost je vrlo često podržana pretraživačkim servisima kao što je TOR i skriva korisnike Interneta koji teže destinacijama u najdubljim zonama Web-a, što takođe doprinosi zamagljivanju prave slike stanja u nevidljivom Web-u, baš kao i nestalnost sajtova koji se u njemu hostuju. Individualni korisnici, poslovni subjekti i vlade mogu imati i koristi od razmjene podataka u Deep Web-u. U njegovom tamnom prostoru odvijaju se legalne, baš kao i nezakonite, aktivnosti i to od obezbjeđivanja diskretnog komuniciranja po osjetljivim temama sa najvišom oznakom povjerljivosti do

krijumčarenja zabranjenih proizvoda poput opojnih droga, oružja, ličnih podataka i kodova putem kojih se prolazi kroz zaštitu softvera.

Uprkos zahtjevima za povećanjem zaštite privatnosti i podizanjem nivoa bezbjednosti u on-line okruženju, možemo se pitati i da li će korespondencija između individualnih korisnika izmijeniti svoj tok prevashodno u smislu upotrebe servisa koji obezbjeđuju anonimnost, kao što je TOR (Ciancaglini i sar., 2015). Još uvijek se ne očekuje preovlađujući podsticaj za upotrebom pretraživača u okruženju anonimnih platformi za razmjenu podataka, ali je vrlo vjerovatno da će tehnološki razvoj doprinijeti da se još više poveća stepen zatamnjivanja Darkneta (Ciancaglini i sar., 2015). Naravno, ovo će uzrokovati da se organi krivičnog gonjenja i donosioci političkih odluka preispitaju u kom pravcu će se boriti sa negativnom stranom tehnološkog napretka i njegovim efektima u uslovima nevidljivog Web-a, kako bi efikasno suzbijali zloupotrebu sajber prostora uključujući i okruženje tamnog Web-a.

Dark Web je, po svojoj prirodi, anoniman i u njemu nije moguće praviti razliku između korisnika koji teže privatnosti svog boravka na Internetu i nosilaca kriminalnih aktivnosti. Pred agencijama za primjenu zakona je težak zadatak da otkriju delinkvente, a da pri tom ne naruše pravo na privatnost onih koji ne postupaju kriminalno. Sasvim je moguće da najbolji način za rješavanje ovakvog problema otkrivanje ilegalnih sajtova, a ne zlonamjernih korisnika (Chertoff, 2017). Pod plaštom svojih zakonskih ovlašćenja, državni hakeri mogu demaskirati posjetioce nezakonitih sajtova postavljanjem naročitih softvera u pokretačke programe njihovih računara. S druge strane, ukoliko državni organa zatvori neki sajt, umjesto njega pojaviće se nekoliko novih sa nezakonitim sadržajima. Vjerujemo da bi krivično gonjenje korisnika ilegalnog sajta obeshrabrilo druge korisnike, koji bi zbog opreza da ne budu otkriveni izbjegavali da rizikuju sa traženjem takvih destinacija u nevidljivom Web-u. Vjerujemo da bi ovo na svoj način doprinijelo umanjenju nedozvoljenih radnji u informatičkom prostoru Deep Web-a, a time i njegovog tamnog dijela Darkneta.

LITERATURA

- Chertoff, M. (2017). A public policy perspective of the Dark Web. *Journal of Cyber Policy*, Vol. 2, No. 1, 26-38.
- Ciancaglini, V., et al. (2015). Below the Surface: Exploring the Deep Web. *Trend Micro*, June 2015, 1-48.
- Finklea, K. (2017). Dark Web. *Congressional Research Service*, March 10, 1-16.
- Freedman, E. (2016) As holidays approach, keeping information safe from hackers becomes even more important. *The Breeze*. Dostupno na: https://www.breezejmu.org/news/as-holidays-approach-keeping-information-safe-from-hackers-becomes-even/article_eb892b64-b774-11e6-934d-cfbde922b479.html, preuzeto 21.06.2019.
- Goodman, M. (2016). *Future crimes: Inside the digital underground and the battle for our connected world*. New York: Anchor Books.
- Greenberg, A. (2015). New dark-web market is selling zero-day exploits to hackers. *Security*. Dostupno na: https://www.wired.com/2015/04/therealdeal-zero-day-exploits/, preuzeto 19.06.2019.
- Johnson, K. (2016). Managing cyber risks. *Georgia Law Review*, Vol. 50:547 2016, 547-592.
- LeFrancois, D., Reilly, C., Munn, R., Strasel, A., Garcia, J., & Chiles, L. (2018). Hackers and the dark net: A look into hacking and the deep web. *James Madison Undergraduate Research Journal,* 2017-2018, Vol. 5, Issue 1, 33-43.
- Lipka, M. (2015). Percentage of companies that report systems hacked. *Money Watch*. Dostupno na: https://www.cbsnews.com/news/percentage-of-companies-that-report-systems-hacked/, preuzeto 29.05.2019.
- Miller, K. (2016). What we talk about when we talk about "Reasonable Cybersecurity": A proactive and adaptive approach. *The Florida Bar Journal*, September/October 2016, 23-31.
- Kovacs, E. (2015). What is the difference between black, white and grey hackers? *Emerging Threats*. Dostupno na: https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html, preuzeto 19.05.2019.
- Martin, B., & Newhall, J. (2016). Technology and the guilty mind: when do technology providers become criminal accomplices? *Journal of Criminal Law & Criminology*, Vol. 105, No. 1, 95-148.
- Norton, Q. (2012). How Anonymous picks targets, launches attacks, and takes powerful organizations down. *Wired*. Dostupno na: https://www.wired.com/2012/07/ff-anonymous/, preuzeto 21.06.2019.
- Omand, D. (2016). The Dark Net: Policing the Internet's underworld. *World Policy Journal*. Winter 2015/2016, 74-82.
- Pagliery, J. (2015). The evolution of hacking. *CNN Business*. Dostupno na: https://edition.cnn.com/2015/03/11/tech/computer-hacking-history/, preuzeto 15.05.2019.

- Sui, D., Caverlee, J. & Rudesill, D. (2015). The Deep Web and the Dark Net: A look inside the Internet's massive black box. *Science and Technology Innovation Program*, STIP 03, August 2015, 1-17.
- Thielman, S., Hunt, E. (2016). Cyber Attack: Hackers 'Weaponised' Everyday Devices With Malware. *The Guardian*. Dostupno na: https://www.theguardian.com/technology/2016/oct/22/cyber-attack-hackers-weaponised-everyday-devices-with-malware-to-mount-assault, preuzeto 24.05.2019.
- Weimann, G. (2016). Going dark: Terrorism on the Dark Web, *Studies in Conflict & Terrorism*, Vol. 39, No. 3, 195-206.
- Williams, W. (2014). What motivates modern hackers? *Betanews*. Dostupno na: https://betanews.com/2014/08/14/what-motivates-modern-hackers/, preuzeto 01.06.2019.
- Zetter, K. (2012). Chrome owned by exploits in hacker contests, but Google's $1M purse still safe. *Wired*. Dostupno na: https://www.wired.com/2012/03/pwnium-and-pwn2own/, preuzeto 07.06.2019.
- Zetter, K. (2013). IE11 Preview bug bounty. *Wired*. Dostupno na: https://www.wired.com/2013/06/microsoft-bug-bounty-program/, preuzeto 05.06.2019.
- Zetter, K. (2016). Hacker Lexicon: What are white hat, gray hat, and black hat hackers? *Wired*. Dostupno na: https://www.wired.com/2016/04/hacker-lexicon-white-hat-gray-hat-black-hat-hackers/, preuzeto 09.06.2019.