UPOTREBA VPN SERVISA PROTIV HAKERSKE ŠPIJUNAŽE

Ph.D. candidate Alem Kozar, MA, email: alem.kozar@iu-travnik.com
Internacionalni Univerzitet Travnik u Travniku, Bosna i Hercegovina

SAŽETAK: Interesovanje za temu zaštita identiteta na Internetu stalno dobija na značaju, sa progresivnim rastom digitalne komunikacije i primjene Interneta kao informacione i komunikacione tehnologije u modernom dobu, sve većom cenzurom koju primjenjuju sigurnosne agencije vlada savremenih država, ISP kompanije (kroz zakonsku obavezu o zadržavanju podataka o aktivnostima korisnika), kompanije radi industrijske špijunaže i marketing kompanije radi utvrđivanja ciljnog tržišta. Ovdje spadaju i brojne druge organizacije i pojedinci koji motivisani različitim interesima tragaju za informacijama koje u suštini zadiru u privatnost pojedinaca ili kompanija. U radu se analizira zaštita identiteta na internetu korištenjem anonimnih mreža protiv hakerske špijunaže. Pod anonimnim mrežama podrazumjevaju se pristupi globalnoj mreži korištenjem VPN (Virtual Private network), web proxy i anonimnih mreža. Fokus analize je na topografiji i sigurnosti u zaštititi identiteta koju pruža Tor anonimna mreža.
Ključne riječi: VPN, web proxy, hakerska špijunaža, mreža, zaštta identiteta

USE OF VPN SERVICE AGAINST HACKER ESPIONAGE

Abstarct: Interest in the topic of identity protection on the Internet is constantly gaining in importance, with progressive growth of digital communication and application of the Internet as an information and communication technology in the modern age, the increasing censorship applied by the security agencies, governments of modern states, ISP companies (the legal obligation to retain data user activity), the company operates industrial espionage and marketing companies to determine the target market. There are a number of other organizations and individuals who are motivated diverse interests looking for information that essentially interfere with the privacy of individuals or companies. This paper analyzes the identity protection on the Internet using anonymous networks. By anonymous networks means access to a global network using VPN (Virtual Private Network), web proxy and an anonymous network against hacker espionage. The focus of analysis is on the topography and security to protect the identity provided by the Tor anonymous network.
Keywords: VPN, web proxy, hacker espionage, internet, identity protection

1. Uvod

Ukratko, VPN ili Virtuelna privatna mreža je definisana kao interkonekcija lokalne mreže koja koristi sigurne kriptirane načine međusobone komunikacije, obično putem interneta,. To znači da VPN produžava privatnu mrežu preko javne mreže odnosno preko internet.i to korisnicima omogućuje slanje i primanje osjetljivih podataka kao das u njihovi računari direktno povezani na isti privatni LAN, iako, fizički, oni nisu u istoj mreži.

Drugim rječima VPN je komunikacioni sistem koji koristi infrastrukturu Interneta za prilagodljiv i ekonomičan prijenos podataka između udaljenih ili virtualnih ureda, zatim zaposlenika koji se putem kućnih računara povezuju u privatnu računarsku mrežu. Osim Interneta, za ostvarivanje VPN veze moguće je koristiti različite tehnologije i komunikacione kanale kao što su dijeljene ATM mreže, privatne mreže ISP-a, i dr.

Dakle ovakava mreža kao što je VPN se može definisat još kao servis koji pruža sigurnu internet konekciju koristeći privatne mreže na pojedinim udaljenim lokacijama. Šta to znači "privatnim udaljenim lokacijama"?Kada neko koristi VPN, njegova računar se direktno povezuje prvo sa nekoliko različitih računara širom planete zavaravajući tako trag originalnog računara i njegovu lokaciju. Na ovaj način se postiže visoka bezbednost pri surfovanju, sa veoma malim šansama da korisnika neko špijunira.

Kad se koristi lokalna mreža za pristup raznim servisima na internet, izvor mrežnih zahtjeva je naša vlastita lokalna mreža LAN. Ako smo povezani sa VPN-om isav naš promet prolazi kroz njega, onda će vanjski svijet vidjeti dio VPN lokane mreže.

Izvor upita nije više Vaša mreža nego na koju je korisnik povezan preko VPN-a. To znači da web stranice I druge mreže sa kojima komuniciramo više neče vidjeti IP adresu korisnikovog računara kao izvora zahtjeva, nego IP adresu VPN-a kojeg korisnik koristi.

Slika I. Shematski prikaz funkcionisanja VPN-a

Ipak, tu je kvaka : ako koristimo VPN čiji je server smješten u našoj zemlji, koji također koristi isti ISP, onda je sasvim moguće da će internetski provajder moći vidjeti naš mrežni promet. Međutim neće bit u mogućnosti zaključiti da je direktno naš, budući da je porijeklo tog prometa VPN server a ne naš raćunar.

2. Povezivanje na VPN

Povezivanje sa VPN-on je moguće na nekoliko načina, ali opća ideja je da se treba potvrdit korisnikov identitet. Najjednostavniji način za uspostavljanje ove sigurne veze je prijavom direktno na server sa korisničkim imenom I passwordom.
Također postoji mogućnost instaliranja određenog softvera koji će nam omogućiti kreiranje sigurne veze. Taj program će vršiti kriptovanje I deskriptovanje podataka I to obično zahtjeva korisničko ime I password kako bi se potvrdio vlastiti identitet. U svakom slučaju postoji mogućnost upotrebe drugih oblika provjere autentičnosti , kao što su tokeni I ili smart kartice.

Prednost upotrebe tokena je činjenicada ga je vrlo teško hakirati I, s obzirom na to, gotovo je nemoguće ukrasti password. Također svaki token je jedinstven, što znači da će server odmah prepoznati svog korisnika.

2. 1. Prednosti upotrebe VPN-a

1. Promet između korisnika I VPN-a je kriptovan, tako da je nemoguće da neko vidi šta korisnik radi na internet.
2. Dokle god je korisnika povezan sa VPN-om, imat će pristup cijelom internet bez censure koja bi mogla da utiće na korisnika.
3. Može se pristupiti serverima i geografski ograničenim web stranicama, ako će korisnika koristit VPN server koji se nalazio u regiji u kojoj su dostupni ti server ili web stranice.
4. Serveri na koje se korisnik povezuje neće vidjet korisnikovu IP adresu, nego adresu VPN servera.
5. Mogučnost surfanja internetom, čitanje mailova ili slanje važnih informacija na javnim mrežama I to bez rizika da neko pokuša vršiti špijunažu.

2. 2. VPN poslužitelji

Slika II. NordVPN

NordVPN se kontinuirano brine o anonimnosti korisnika i poduzima sve kako nebi bilo nikakvih logova o korisnicima, njihovim IP adresama ili aktivnostima. Uz to, ne bilježe se nikakva vremena niti datumi.

Također ovaj poslužitelj ima fantastičnu zaštitu o kojoj se sam brine, odnosno imaju svoju infrastrukturu. Svaki korisnik koji "izlazi na internet" prođe preko dva njihova VPN server (barem 2 čvora, ako ne i više), te se koriste dva sloja 256 bitne enkripcijske zaštite. Također se može koristit kombinacija Tor+VPN. To znači da konekcija prolazi prvo kroz Nordove VPN servere, a zatim još I preko Tor mreže, što garantuje praktički 100% zaštitu.

Slika III. Private Internet Acces

privateinternetaccess™
for safe browsing, always use protection.™

Od dodatne zaštite imaju još i:

1. kill switch – ako pukne veza, neće se nikakakv promet preusmjeravati,
2. IPv6 leak protection,
3. DNS leak protection,
4. Shared IP System,

Imaju odlične custom aplikacije za Windowse, OS X (macOS), Linux, Android, iOS i uskoro dolazi Chrome extenzija! Od protokola korisnici mogu odabrati između ostalog, OpenVPN I IPSec. One imaju lokalni log radi debugiranja problema, ali se ti logovi redovno sami uništavaju.

Slika IV. ExpressVPN

ExpressVPN

ExpressVPN ne koristi logove prometa, niti logove koji bi ikako mogli povezati korisnika, aktivnost na internetu i vrijeme i datum korištenja usluge. Uz to, njihova cijela VPN servisa se zasniva na dijeljenim IP adresama pa se ne može niti jednoznačno utvrditi koji korisnik je koristio koju IP adresu.

Slika V. Anonymizer

ANONYMIZER®

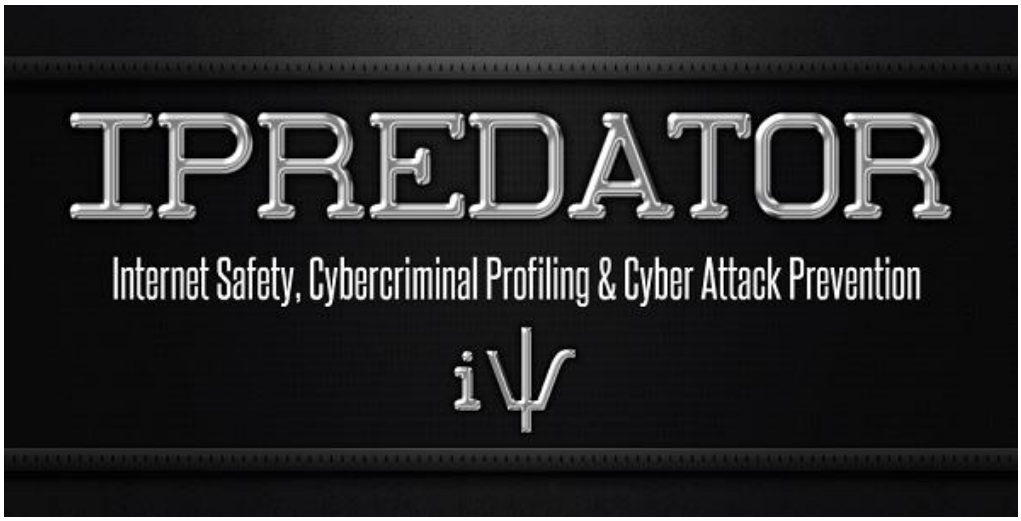
Anonymizer je jedna od rijetkih VPN servisa koji još uvijek nema u ponudi plaćanje putem Bitcoina, ali je to u planu za ovu godinu. S druge strane može se platit sa bilo kojom

kreditnom karticom. Ne čuvaju se nikakvi posebni podaci osim ako je korisnik platio VPN uslugu.

Slika VI. TorGuard

TorGuard ima svoje custom aplikacije za Windows, Mac, Linux i Android koje koriste OpenVPN. Imaju i aplikaciju za iOS, ali ona koristi IPSec jer je Aple ograničen u tom pogledu i ne dozvoljava korištenje OpenVPN-a. Sve spomenute aplikacije ne spremaju nikakve logove na lokalni uređaj.

Slika VII. IPredator



IPredator ne sadrži nikakve logove o korisnicima niti je ikako moguće povezati pravu IP adresu korisnika i vrijeme korištenja servisa. Jedino što se privremeno koristi je spremanje IP adrese u bazu podataka, sve do uspostave veze. U tom trenu se taj podataka briš iz njihove baze podataka.

Posluju u Švedskoj i tamo se nalaze svi njihovi serveri.

Špijunaža preko interneta sve opasnija

Računarska špijunaža usmjerena na državnu infrastukturu bit će glavna opasnost na Internetu sljedeće godine, ocjenila je u svojoj studiji kompanija za proizvodnju antivirusnog softvera McAfee. Prema toj studiji, računarski kriminal će također ugrožavati on-line bankarstvo, a pojedine vlade i grupe koristit će Internet za kibernetičku špijunažu i za izvršenje "kibernetičkih napada".

Prema toj studiji, računarskikriminal će također ugrožavati on-line bankarstvo, a pojedine vlade i grupe koristit će Internet za kibernetičku špijunažu i za izvršenje "kibernetičkih napada".
Ciljevi napada bit će osjetljivi sistemi državne mrežne infrastrukture, kao što su elektro-mreže, sistemi upravljanja aviosaobraćajem, financijsko tržište i upravljačke računarske mreže.

Korištenje Interneta za web špijunažu je prisutno u približno 120 zemalja.

Iz početnih pojedinačnih pokušaja napadi su se razvili u dobro organizovane i bogato finansirane aktivnosti čiji je cilj politička, vojna, ekonomska i tehnološka špijunaža.

Novi štetni programi su sve otporniji i stalno se usavršavaju i sadrže visoko uređene funkcije, na primjer u oblasti šifrovanja.

Crv nuwar je bio prvi primjer te vrste opasnog koda i stručnjaci smatraju da će se naredne godine pojaviti niz sličnih.
Također će se u većoj mjeri javiti napadi usmjereni na telefoniranje putem Interneta i zloupotreba sajtova za druženje tipa MySpace ili Facebook.

Česti napadi usmjereni na banke mogu, prema mišljenju stručnjaka, ozbiljno da ugroze povjerenje javnosti u on-lajn bankarstvo i da budu kočnica elektronske trgovine.

Ne možete biti totalno anonimni na internetu ?
Po tim nekim zakonitostima, podatak o tome šta se radi na internetu može provajderima da zatraži samo policija preko suda države u kojoj se korisnik ili korisnici nalaze ali opet to je zakonitost za koju obični smrtnici znaju, postoje i zakonitosti koje korisnici ne znaju a koje se uveliko dešavaju.

Čovjek koji je bio dio takvog aparata koji je pratio sve šta se dešava u online vodama, nije više mogao da trpi to kršenje prava na privatnost te je izašao u javnost sa istinom i dokazima, šta je sve radila američka agencija NSA pod izgovorom odbrane od terorizma.

Ukratko, NSA, pratila je šefa u nekoj kompaniji, predsjednika vlade, električara iz distribucije, generalnog sekretara UN-a, kancelarku Njemačke, studenta iz Sarajeva, koje sajtove obilaze, koje podatke ostavljaju, imali uvid u njihove mailove, pratili šta rade po društvenim mrežama i slično, a sve pod izgovorom odbrane od zlih momaka iz Al Kaide.

Sve i da su korisnici skriveni iza 100 proksija, VPN-ova, fajervolova, TOR-ova opet će vlasnik tamo nekog sajta znati da ste bili na toj i toj stranici, gledali to i to, mozda će uspjeti i

da korisniku instaliraju trojanca kojim će aktivirati korisnikov laptop web kameru ili mikrofon pa opet imati uvid u to kako taj neki korisnik izgleda, koja mu je boja glasa, šta priča ili šta se priča u sobi gdje je laptop, ako ga neko nazove imenom i prezimenom znat će i te informacije.

Čak i sami profesionalni hakeri mogu biti uhakovani a da to ne znaju istom tehnikom. Recimo, ruski haker je bio uhakovan uključivanjem njegove kamere mimo njegovog znanja pri tome su mu računar zarazili virusom koji je on lično napisao.

U ovom djelu bit će objašnjeno kako se možesmanjiti izlaganje korisnikove privatnosti na minimalnu razinu i gdje vrebaju opasnosti uz praktičan primjer i to opet ne znači da se treba zaključati u bunker, da se postaveoko njega nagazne mine, da se ugasi sve šta ima struje u sebi pa tek tad budete sigurni.

Ukratko, sve šta se objavi na društvenim mrežama, komentariše po drugim sajtovima ili facebooku, ili komentariše po bilo kojem sajtu sa pravim imenom i prezimenom, mail koji se pošalje tom i tom, formu ili anketu koja se popuni od strane korisnika tu i tu, nalog koji je korisnik napravio na tom i tom forumu, može biti vidljiv na internetu, sa sve fizičkom lokacijom nekog korisnika ako taj isti korisnik nije iza TOR-a, proxi-ja ili VPN-a. Svaka korisnikova neoprezna objava na društvenim mrežama, komentar na sajtu i slično može biti direktan udar na privatnost korisnika.

Špijunaža svjetskih funkcionera

Američka nacionalna sigurnosna agencija (NSA) prisluškivala je više od 60 miliona telefonskih razgovora u Španiji između decembra 2012. i januara 2013., naveo je Španski dnevni list El Mundo, a američki veleposlanik u Madridu je pozvan u ministarstvo vanjskih poslova.

Prema dokumentima koje je pribavio bivši analitičar NSA-e Edward Snowden a koje je prenio El Mundo, ta agencija je špijunirala 60,5 miliona telefonskih razgovora u Španiji između 10. decembra 2012. i 8 januara 2013. List navodi da NSA "nije snimila sadržaj poziva, već serijski broj telefona, mjesto na kojem se nalaze, broj telefona i upotrijebljene SIM kartice kao i trajanje poziva".

Veleposlanik SAD-a James Costos je bio pozvan dati objašnjenja navodnih prisluškivanja Španskih zvaničnika koja su otkrivena javnosti, a uslijedila su nakon drugih otkrića o američkim špijuniranjima 35 svjetskih čelnika.

Nakon otkrića da Amerikanci špijuniraju cijeli svijet pa čak možda i Angelu Merkel, Njemačka i Brazil počeli su raditi na rezoluciji UN-a o zaštiti ličnih sloboda. Traže da se u prava pojedinca uvrsti i odredba o zaštiti privatnosti na internetu. I jedna i druga država ljutito su reagovale nakon što su se pojavile informacije da se špijuniraju Angela Merkel i brazilska predsjednica Dilma Rousseff.

S druge strane američko prisluškivanje mobitela njemačke kancelarke izazvalo je napetost u transatlantskim odnosima. Predsjednik Obama morao je dati objašnjenje. Ali, američki stručnjaci su bili postavili pitanje: Čemu toliko uzbuđenje? "Malo prisluškujemo, pa šta? Tako bi se ukratko mogle sažeti reakcije u Sjedinjenim Američkim Državama nakon što je

objavljeno da je američka Agencija za nacionalnu sigurnost NSA vjerovatno prisluškivala i mobilni telefon Angele Merkel. Slučaj je dospio na naslovne stranice tek rijetkih američkih novina. CNN je prenio izjavu savezne kancelarke da se 'prijatelji ne prisluškuju' i to je to". Peta Heokstra, koji je do 2007. vodio Odbor za tajne službe američkoga Kongresa, također misli da se u Europi previše prašine diglo bez potrebe. "Mislim da se u svijetu tajnih službi podrazumijeva da smo dobri prijatelji – Francuzi, Njemci, Izraelci, Amerikanci ali dođu vremena kada se međusobno špijuniramo i to svako može razumjeti“, rekao je Hoekstra za Deutsche Welle dodajući da europski saveznici špijuniraju u SAD-u.

3. Zaključak

Problem zaštite identiteta je višeslojan; vezan je za informatičku kulturu; navike pojedinca; materijalni status. Izazov počinje od operativnog sistema (licencirani ili piratska verzija), preko servera koji koristimo u različite svrhe i internet lokacija koju posjećujemo.Virtuelne privatne mreže, web proxy servisi i Tor mreža svakako smanjuju stepen rizika izloženosti pojedinca od gubitka digitanog identiteta. Tor projekat postoji dvanaest godina. Treća generacija aplikacije nudi najbolju zaštitu. Prednost Tor mreža u poređenju sa drugim softverski anonimnim mrežama ogleda se u luk rutiranju saobraćaja, koji mijenja čvorišta metodom slu- čajnog izbora, prilikom svakog url-ovanja nove lokacije na Internetu. Dodatnu sigurnost predstavlja kodiranje i dekodiranje sadržaja na svakom čvorištu. Najbolji rezultati postižu se kad je kompletan saobraćaj pod SSL i TLS protokolom, uključujući i pristup odredišnom serveru na javnoj mreži. Povećanje broja releja, koji čine okosnicu privatne mreže, predstavlja dodatnu sigurnost za korisnike. Releji su u najvećem broju u vlasništvu volontera, koji mogu isti računar koristiti i za druge namjene i tu leži sjenka na izuzetno dizajniranoj privatnoj mreži. Rizik od napada virusom kojim se uspostavlja kontrola nad računarom je vrlo velika.

4. Literatura

[1] Keith D. Watson, e Tor Network, “A Global Inquiry into the Legal Status of Anonymity Networks”, 11 Wash. U. Glob. Stud. L. Rev. 715, 2012.
[2] P. Staletić, N. Staletić, “Piraterija digitalnog sadržaja na Internetu”, XII međunarodni naučno-stručni simpozijum, Jahorina, 2013.
[3] The hacker News, “Tor anonymizing network compromised by French researchers”, http://thehackernews. com/2011/10/tor-anonymizing-network-compromisedby.html, 3. februar 2014
[4] http://mondo.rs/a83538/Mob-IT/Vesti/Spijunaza-preko-Interneta-sve-opasnija.html
[5] https://bs.wikipedia.org/wiki/ATM
[6] http://pcchip.hr/internet/sto-je-vpn-za-sto-se-koristi/
[7] http://www.pametnitelefoni.rs
[8] http://www.4dportal.com/hr