Da li ste bezbedni na Internetu?

Seminarski rad u okviru kursa
Metodologija stručnog i naučnog rada
Matematički fakultet

Nevena Ajvaz, Natalija Jovanović, Marija Milićević, Tijana Nikčević
nevena.ajvaz@hotmail.com, natalija.jovanovic996@gmail.com,
marija.milicevic.10.23@gmail.com, tijana.nikcevic1@gmail.com

April 2019.

Sažetak

Internet je jedno od najmoćnijih oružja današnjice koji nudi mnoge pogodnosti ako se koristi u prave svrhe. Bezbednost na Internetu je veoma veliki problem i u vezi sa tim upoznaćemo se sa najčešćim vrstama sajber napada, kriminala i pojmom glasanja putem Interneta. Videćemo zašto je naša bezbednost ugrožena i kroz primere poznatih napada opisati načine na koje se ona narušava.

Sadržaj

1 Uvod

U ovom radu ćemo se na početku upoznati sa pojmom sajber kriminala [4], kao i problemom rasprostranjenosti sajber napada. Dalje će biti prikazane 3 najčešće vrste napada - fišing, SQL injekcija [16] i DoS. U četvrtom poglavlju, koje se odnosi na primere napada, biće prikazani problemi najvećih svetskih kompanija [2] i država [11] i kako su se one suočavale sa tim. Sajber kriminal brzo napreduje, što prouzrokuje razvoj i nastanak novih vrsta napada. Nakon ovoga, pozabavićemo se temom glasanja putem Interneta.

2 Pojam sajber kriminala

Visokotehnološki ili sajber kriminal (eng. *cyber crime*) predstavlja moderni vid kriminala, tačnije, putem računara. Sajber kriminalci su osobe ili grupe ljudi koji koriste tehnologiju kako bi izveli zlonamerne aktivnosti putem mreže sa ciljem da ukradu osetljive podatke neke firme, lične informacije ili da profitiraju [5]. Takođe, treba napraviti razliku između sajber kriminalca i hakera. Sajber kriminalci sa lošim namerama vrše upad u računare, dok hakeri traže inovativne načine da koriste sistem, bili ti načini loši ili dobri.

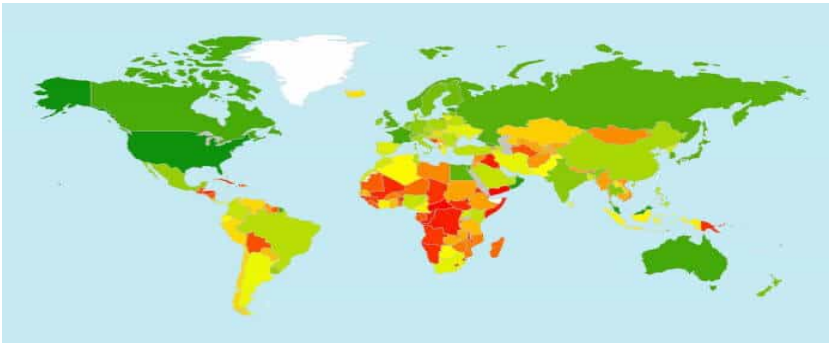
Zakoni koji se odnose na ovu vrstu kriminala se dopunjuju i razvijaju u zemljama širom sveta. Nerazvijene zemlje su najizloženije sajber napadima. U takvim zemljama je zakon o ovoj oblasti slabo definisan, a u nekim ni ne postoji. U tabeli 1 mogu se videti podaci koji su vezani za Srbiju mereni po globalnom indeksu sajber bezbednosti [1] (eng. *GCI - Global Cybersecurity Index*). U tabeli su prikazane neke od najvažnijih stavki koje se odnose na Srbiju [13].

MERENJA	POSTIGNUĆE		
	nisko	srednje	visoko
Zakon o sajber kriminalu			x
Zakon o bezbednosti na Internetu	x		
Preduzimanje mera protiv sajber kriminala	x		
Zaštita dece na Internetu			x
Strategija	x		
Zaposleni u istraživanju	x		
Kampanje za osvešćivanje javnog mnjenja	x		
Programi edukacije	x		
Javno-privatno partnerstvo		x	

Tabela 1: Prikaz stanja o sajber kriminalu u Srbiji po podacima iz 2017. godine

Iz priloženog se vidi da je Srbija zemlja sa niskom stopom posvećenosti suzbijanju sajber kriminala. Na slici 1 može se videti ova stopa za ostale zemlje sveta.

[1] Pouzdan izvor koji meri posvećenost država bezbednosti na Internetu.



Slika 1: Stopa GC indeksa u svetu. Tamnozelenom bojom obeležene su zemlje sa visokom posvećenošću, dok su crvenom obeležene sa niskom

3 Sajber napadi i vrste

Sajber napad predstavlja napad od računara do računara koji povređuje poverljivost, integritet i informacije koje se nalaze na napadnutom računaru [11]. U mnogim zemljama, Internet odvija ključnu ulogu u svakodnevnom životu ljudi. Olakšava virtuelnu komunikaciju među ljudima, podstiče razvoj novih poslovnih modela i kompanija, menja način na koji ljudi kupuju. U 2018. godini, transfer novca koji uključuje prodaju i kupovinu putem Interneta, iznosila je oko $2.8 biliona. Prema statističkim studijama [15], smatra se da će u 2021. ta vrednost iznositi oko $4.88 biliona. Iz ovih razloga, nije neobično da je sa porastom popularnosti Interneta porasla i stopa kriminala na njemu. U ovom poglavlju će biti obrađene tri vrste napada putem Interneta.

3.1 Fišing (eng. *phishing*)

Fišing je vrsta društvenog inženjeringa (eng. *social engineering*)[2] gde se napadač pomoću elektronske pošte ili zlonamernih veb sajtova lažno predstavlja kao pouzdana organizacija ili kompanija kako bi prikupio lične podatke od pojedinca ili kompanije [3]. Engleski termin *phishing* je prvi put korišćen 1996. a nazvan je po pecanju jer mejlovi služe kao mamac kojim se ljudi navode da daju svoje podatke. „Ph“ umesto „f“ u zapisu reči je aluzija na termin *phreaks* koji označava ljude koji su eksploatisali telekomunikacije, a neki ih smatraju i prvim hakerima [8]. Napadi fišinga se često sastoje od slanja korisnicima mejlova koji izgledaju kao da su iz bankarske ili finansijske institucije ili veb servisa preko kojeg pojedinac ima račun. Cilj fišinga je da prevari primaoca da da svoje podatke za prijavljivanje ili druge osetljive informacije. Na primer, napadač može da pošalje milione mejlova sa botnet-a[3]. Poruke obaveštavaju primaoce da je njihov nalog za elektronsku trgovinu bio kompromitovan i upućuju ih na veb lokaciju gde bi rešili problem. Korisnici koji kliknu na link dođu do veb stranice koja je napravljena tako da podseća na originalni sajt za elektronsku trgovinu. Kada se nađu na sajtu, od njih se traži korisničko

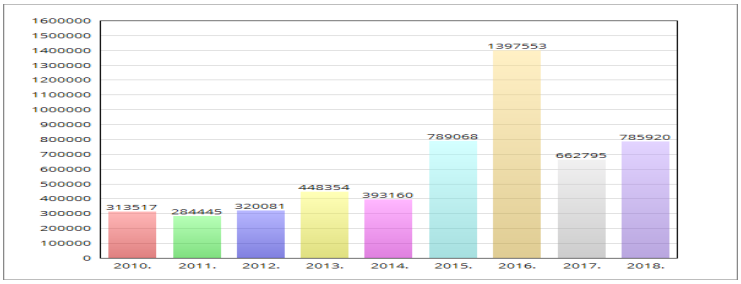
[2]Obmana kojom se manipuliše ljudima da daju poverljive informacije.

[3]Mreža privatnih računara, zaraženih zlonamernim softverom, koji se kontrolišu kao grupa bez znanja vlasnika, npr. za slanje spama.

ime, lozinka i druge privatne informacije. Te informacije mogu da se iskoriste za krađu identiteta.

Ciljano orijentisan fišing (eng. *spear phishing*) je varijanta fišinga u kojoj napadač bira adrese elektonske pošte tako da cilja jednog ili određenu grupu primalaca. Na primer, napadač može ciljati starije osobe kao osobe koje se smatraju lakovernijima ili članove grupa koji imaju pristup vrednim informacijama. Ciljano orijentisan fišing može biti veoma delotvoran jer omogućava napadaču da uobliči napad tako da žrtva zbog hitnosti ili poverenja određenim osobama bude manje oprezna. Za ovo je potrebno da napadač prikupi lične podatke o žrtvi, kao što su imena prijatelja, poslodavac, rodni grad, lokacije koje posećuje, šta je nedavno kupila na mreži itd. Na primer, napadač može da pošalje mejl ka nekoliko ljudi koji izgleda kao da je od njihovog direktora, kojim ih poziva na sastanak putem Gmail-a, a link u poruci navodi primaoce da se prijave na Gmail da prisustvuju sastanku.

Fišing se pojavio negde oko 1995, ali je postao čest tek nakon 10 godina. Prvi napadi bili su vezani za AOL (eng. *America Online*), u to vreme najpopularniji internet provajder[12]. 2000ih godina su napadi prešli na platne sisteme poput E-Gold, eBay i PayPal. Zanimljivo je povećanje napada na kinesku elektronsku trgovinu, što ukazuje na povećanje važnosti kineske ekonomije [11]. Na slici 2 prikazana je količina sajtova za fišing koje je otkrila APWG (eng. *Anti-Phishing Working Group*) tokom godina [1].



Slika 2: Količina otkrivenih sajtova za fišing

3.2 SQL injekcija

SQL[4] injekcija je umetanje dela ili celog SQL upita obično preko polja za unos na veb stranici. Ukoliko ovako nešto uspe može se pristupiti osetljivim podacima iz baze, mogu se modifikovati podaci, izvršiti administrativne operacije nad bazom itd.

Primer 3.2.1

```
txtUserId = getRequestString("UserId");
txtSQL = "SELECT * FROM Users WHERE UserId = " +
    txtUserId;
```

U primeru 3.2.1 kreira se SELECT upit dodavanjem sadržaja promenljive txtUserId na select string. Sadržaj promenljive je sadržaj polja za unos

[4]Standardni jezik za skladištenje, manipulaciju i dohvatanje podataka u bazama podataka.

korisničkog id-a.

Jedan od načina upotrebe SQL injekcije zasniva se na činjenici da je `1=1` uvek istinito. Pod pretpostavkom da je korisnik u polje za unos uneo `105 OR 1=1`, SQL upit iz primera 3.2.1 bi izgledao ovako:

```
SELECT * FROM Users WHERE UserId = 105 OR 1=1;
```

Ovakav upit vratiće sve redove tabele „Users“. Šta ako tabela „Users“ sadrži imena i šifre? Može se pristupiti svim imenima i šiframa iz baze jednostavno dodavajući `105 OR 1=1` u polje za unos korisničkog imena.

`""=""` je uvek istinito. Ovo je još jedan način upotrebe SQL injekcije.

Primer 3.2.2

```
uName = getRequestString("username");
uPass = getRequestString("userpassword");

sql = 'SELECT * FROM Users WHERE Name ="' + uName + '"
    AND Pass ="' + uPass + '"'
```

Ukoliko naš kod izgleda kao u primeru 3.2.2 može se pristupiti korisničkim imenima i šiframa u bazi unoseći `" OR ""="` u polje za šifru i u polje za korisničko ime. Kod na serveru će kreirati ispravan SQL upit:

```
SELECT * FROM Users WHERE Name ="" OR ""="" AND Pass =""
    OR ""="";
```

Ovakav upit vratiće sve redove iz tabele „Users“.

Mnoge baze podržavaju grupu SQL upita razdvojenih ; simbolom. Ukoliko bi korisnik u polje za korisnički id uneo `105; DROP TABLE Suppliers`, SQL upit iz primera 3.2.1 izgledao bi ovako:

```
SELECT * FROM Users WHERE UserId = 105; DROP TABLE
    Suppliers;
```

3.3 DoS napadi

DoS (eng. *Denial-of-Service*) napad je radnja koja sprečava legitimitne korisnike da koriste usluge računara, tj. napadač utiče da mašina ili mrežni resurs budu nedostupni korisnicima tako što privremeno ili neograničeno ometa usluge hosta[5] povezanog na Internet. DoS napad može da uključi neovlašćeni pristup jednom ili više računarskih sistema, ali cilj napada nije krađa informacija, nego remećenje sposobnosti servera da odgovori na korisničke zahteve tako što zatrpava metu mrežnim saobraćajem ili šalje informacije koje aktiviraju razne nezgode. Ometanje normalnog rada računarskih usluga može da napravi veliku štetu. Firma koja se bavi nekom vrstom prodaje putem Interneta može da izgubi posao, vojsci može da se prekine komunikacija, Vladi ili nekoj neprofitnoj organizaciji može da se desi da ne može da prenese svoju poruku javnosti.

DoS napad je primer „asimetričnog“ napada, tj. napada u kome jedna osoba može dosta da naškodi velikoj organizaciji. Pošto se terorističke organizacije specijalizuju za asimetrične napade, neki strahuju da će DoS napadi postati važan deo terorističkog oružja.

[5]Računar koji čuva veb sajt ili druge podatke kojima se može pristupiti preko Interneta ili neke druge mreže (izvor - Oxford Dictionaries).

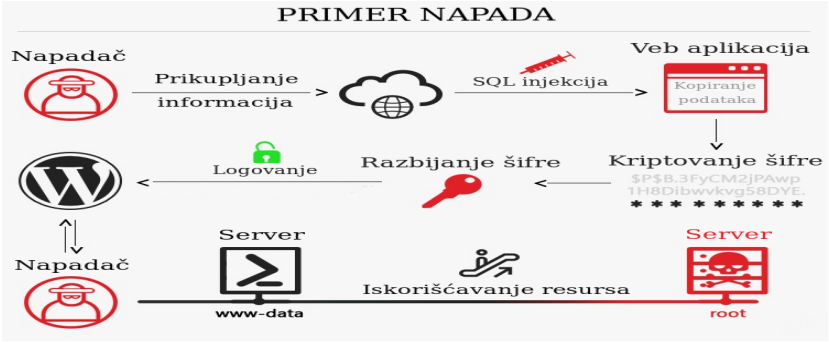
3.3.1 DDoS napadi

Dodatni tip DoS napada je DDoS (eng. *Distributed Denial-of-Service*) napad. Glavna razlika je u tome što meta nije napadnuta sa jedne lokacije, već sa više njih odjednom [6]. Do DDoS napada se dolazi kada višestruki sistemi vode sinhronizovani DoS napad na jednu metu. Podela hostova koji određuju DDoS daje napadaču više prednosti:

- Napadač može iskoristiti veći kapacitet resursa mašine kako bi izvršio ozbiljan razoran napad
- Lokacije napada se teško određuju zbog slučajne podele napadačkih sistema
- Teže je ugasiti više mašina nego jednu
- Pravu napadačku grupu (eng. *attacking party*) je veoma teško identifikovati, jer se oni prikrivaju iza mnogih (uglavnom kompromitovanih) sistema

Mnoge sigurnosne tehnologije su razvile mehanizme za odbranu od mnogih vrsta DoS napada, ali, zbog jedinstvenih karakteristika, DDoS se još uvek smatra ozbiljnom pretnjom.

Na kraju, kao ilustrativan primer, na slici 3 se može videti kako proces jednog sajber napada može da izgleda.



Slika 3: Sajber napad

4 Primeri napada

U ovom poglavlju biće prikazani neki primeri napada na države i velike svetske gigante u poslednjih petnaest godina. Ovakvi napadi mogu biti izvršeni od strane pojedinca ili grupe ljudi i podjednako su bitni kao opomena za učenje na greškama.

4.1 Primeri samostalnih napada

DŽENSON DŽEJMS ANČETA Dženson Džejms Ančeta, radnik u jednom Internet kafeu, je 2004. i 2005. napravio mrežu od oko

400000 botova, uključujući i računare kojima je upravljalo Ministarstvo odbrane SAD-a. Softveri za reklame (eng. *adware companies*), spameri i ostali su platili Ančeti da koriste te računare. Nakon što ga je FBI uhapsio, Ančeta se izjasnio krivim za razne optužbe, uključujući prekršavanje zakona o zlostavljanju računara. U maju 2005, federalni sudija je osudio Ančetu na 57 meseci zatvora i tražio od njega da plati $15000 američkoj Vladi zbog napada na Ministarstvo odbrane. Zbog njegovih ilegalinih aktivnosti, Vlada je Ančeti oduzela njegov 1993 BMW, više od $60000 u kešu, kao i njegovu računarsku opremu.

PHARMAMASTER Izraelska kompanija Blue Security je napravila sistem za zastrašivanje spamova kako bi pomogla ljudima koji ne žele da primaju spamove. Blue Security je prodavala svoj sistem preduzećima, dok su individualci mogli besplatno da štite svoje računare. Oko pola miliona ljudi se prijavilo za ovu besplatnu uslugu. Korisnici su na svojim računarima učitali bot po nazivu Blue Frog koji je integrisan sa Yahoo! Mail-om, Gmail-om, Hotmail-om i proverava da li su dolazeći mejlovi spamovi. Kada naiđe na spam poruku, bot kontaktira Blue Security server kako bi otkrio izvor tog mejla i zatim spameru šalje opt-out[6] poruku.

Spameri koji neselektivno šalju mejlove na milione adresa su počeli da primaju stotine hiljada opt-out poruka, koje su ometale njihove operacije. Šest najboljih svetskih spamera se dogovorilo da koristi softver za filtriranje koji je razvio Blue Security kako bi odstranili Blue Frog korisnike sa svojih mejl lista.

Jedan spamer, čiji je nadimak bio PharmaMaster, nije se povukao. On je pretio Blue Frog korisnicima porukama kao što je na primer sledeća: „Nažalost, zbog taktika koje koristi Blue Security, primaćete ovu poruku ili druge besmislene spamove 20-40 puta više nego inače“. On je održao svoje obećanje, pa je 1. maja 2006. počeo da šalje Blue Frog korisnicima 10 do 20 puta više spamova nego inače.

Narednog dana je počeo da napada sam Blue Security. Lansirao je DDoS napad sa desetina hiljada botova ciljajući Blue Security servere. Ogromna količina dolaznih poruka je onemogućila Blue Frog uslugu. Kasnije su se DDoS napadi fokusirali na druge kompanije koje pružaju Internet usluge Blue Security-u. Na kraju su napadi ciljali preduzeća koja su plaćala usluge Blue Seciruty-u. Kada je Blue Security shvatio da ne može da zaštiti svoje klijente od DDoS napada i mejlova sa virusima, nevoljno je prekinuo svoju uslugu.

ALBERT GONZALEZ Albert Gonzalez je 2010. osuđen na 20 godina zatvora nakon što se izjasnio krivim za korišćenje SQL injekcija kako bi ukrao više od 130 miliona brojeva kreditnih i debitnih kartica. Neki od tih brojeva su prodati onlajn, što je dovelo do neovlašćenih kupovina i povlačenja banaka. Ciljevi napada su bili Heartland Payment Systems, 7-Eleven, Hannaford Brothers Supermarkets, TJX, DSW, Barnes & Noble, OfficeMax, i Dave & Buster lanci restorana. Većina brojeva je ukradena od firme Heartland Payment Systems, procenjujući gubitak na $130 miliona.

[6]Instrukcija od strane primaoca mejla da se spreči dalje slanje robe, informacija ili poruka od strane pojedinca ili kompanije.

4.2 Primeri napada na države

GRUZIJA (2008) Gruzija je jedna od bivših Sovjetskih republika koja je stekla nezavisnost 1991. godine. Južna Osetija, oblast na teritoriji Gruzije koja je pripadala Rusiji do 1991, nakon kratkog rata iste godine, postaje i međunarodno priznata kao autonomna pokrajina Gruzije. Nakon provokacije separatista u Južnoj Osetiji, Gruzija šalje vojsku na ovu teritoriju 7. avgusta 2008. godine. Ruske snage su 8. avgusta ušle u Južnu Osetiju i ove dve strane su se borile četiri dana. Ovaj sukob je ostao zapamćen i iz razloga što je gruzijska Vlada i pre nego što je ruska vojska došla na teritoriju Južne Osetije imala problem sa velikim DDoS napadom. Njihova Vlada nije bila u mogućnosti da komunicira sa ostatkom sveta. Mnogi veb sajtovi su bili srušeni na nekoliko sati. Gruzijska vlast je bila primorana da lokacije nekih svojih veb servera prebaci na SAD. Postojale su sumnje je da je napad izvršila grupa kriminalaca pod nazivom „Russian Business Network“, smeštenih u Sankt Peterburgu u Rusiji, ali je ostalo nerazlučeno da li je ova grupa imala neke veze sa ruskom vojskom.

Na isti dan godinu dana kasnije, kompanija Twitter je bio onesposobljena u celom svetu na nekoliko sati zbog masovnih DDoS napada. Maks Keli, šef za bezbednost u kompaniji Facobook, rekao je da je svrha napada bila da se spreči objavljivanje teksta gruzijskog političkog blogera, pozivajući se na činjenicu da su istovremeno pali i ostali sajtovi koje je ovaj bloger koristio. Ti sajtovi su bili Facebook, LiveJournal i Google.

SAD I JUŽNA KOREJA (2009) DDoS napad na američku i južnokorejsku Vladu je izvršen tokom vikenda uoči 4. jula, američkog Dana nezavisnosti. Tom prilikom zabeležen je pad više od trećine veb sajtova u ovim državama. U Americi je napadnuta Bela kuća, američki trezor, Tajna služba, njujorška berza i kompanija NASDAQ. U Južnoj Koreji, DDoS napad je izvršen na Plavu kuću (predsednička palata), Ministarstvo odbrane i Narodnu skupštinu.

Ova vrsta napada se smatra relativno malom jer je izvršen uz pomoć botnet-a koristeći između 50 i 65 hiljada računara, što se smatra malom cifrom u poređenju na velike napade gde se koristi oko milion računara. Ipak, ova vrsta napada je ostala zapamćena i po tome što su južnokorejski sajtovi ostali nedostupni čak do 9. jula. Pretpostavljalo se da je napad izvršen kao vid osvete jer su Ujedinjene Nacije uvele određene sankcije Severnoj Koreji u tom periodu. I do danas se još uvek ne zna ko je tačno izveo ovaj napad jer su napadači koristili računare koji su bili u posedstvu drugih ljudi.

4.3 Primeri napada na kompanije

Yahoo! Yahoo! je jedan od najvećih giganta na Internetu. Ova kompanija je 2016. godine objavila informaciju da je bila žrtva jednog od najvećih napada u istoriji; 2013. je grupa hakera kompromitovala 3 milijarde naloga korisnika. Pored imena, datuma rođenja, mejl adresa i šifara, zaštitna pitanja i odgvori su takođe otkriveni. Pored ovog napada, 2014. je zabeležen još jedan napad na ovu kompaniju. Tada su obelodanjena imena, mejl adrese, datumi rođenja i brojevi telefona 500 miliona korisnika. Ovoga puta su šifre ostale zaštićene.

eBay Ova kompanija se bavi prodajom proizvoda putem Interneta. Bila

je napadnuta u maju 2014. kada su otkrivena imena, adrese, datumi rođenja i enkriptovane šifre[7] od 145 miliona korisnika. Kriminalci su „upali“ u bazu tako što su koristili kreditacije troje zaposlenih i imali su pristup unutrašnjosti 229 dana. U tom periodu su imali vremena da pristupe bazi podataka korisnika. Informacije koje se tiču finansija kao što su brojevi kreditnih kartica su ostale zaštićene jer se ta vrsta podataka čuva u odvojenoj bazi.

Uber Uber je američka kompanija koja se predstavlja kao mreža koja pruža usluge transporta. Ona je 2016. bila napadnuta od strane samo dva hakera koji su uspeli da dođu do imena, mejl adresa i brojeva telefona 57 miliona korisnika Uber aplikacije. Takođe, otkriveni brojevi vozačkih dozvola 600 hiljada vozača na ovoj platformi.
Hakeri su pristupili i Uberovom nalogu na GitHub platformi[8] gde su pronašli korisničko ime i lozinku kreditacije ka AWS[9] nalogu. Uber je ovaj napad objavio godinu dana kasnije. Ova kompanija je platila $100 hiljada hakerima da unište podatke.

5 Sajber kriminal

Glavni trend koji pokreće evoluciju računarskih napada i eksploatacija uključuje motiv rasta profita zasnovanog na zlonamernom kodu - malveru (eng. *malware, malicious code*). Neki napadači prodaju prilagođeni malver za kontrolu mašina žrtava kupcu koji je najviše ponudio. Mogu iznajmiti gomile zaraženih sistema, koji su korisni za isporuku nepoželjne pošte (spamova), fišing shema, DoS napada ili za krađu identiteta. Špijunske kompanije i preterano agresivni oglašivači kupuju takvu vrstu koda kako bi se infiltrirali i kontrolisali žrtvine mašine. Jedna zaražena mašina na kojoj iskaču reklame i prilagođavaju se rezultati pretrage može da košta svega $1 mesečno. *Keylogger*[10] na zaraženoj mašini može da pomogne napadaču da skupi brojeve kreditnih kartica i ukrade $1000 ili više od žrtve pre nego što se otkrije prevara. Ako kontroliše 10000 mašina, napadač može solidno da zaradi od sajber kriminala.

Kada kriminalci budu otkrili pouzdan način za zaradu novca na ovoj grani kriminala, broj incidenata ovog tipa će se neizbežno povećati. Napadači su osmislili različite poslovne modele koji su niskog rizika, tako da je mala verovatnoća da će napadač biti uhvaćen ukoliko pažljivo skriva svoje tragove. Tako mogu da se zarade stotine hiljada ili čak milioni dolara.

Faktor koji podstiče rast sajber napada je bot (skraćenica od reči *robot*) softver. Ovaj softver dozvoljava napadaču da kontroliše neki sistem širom Interneta. Jedan napadač ili grupa napadača može da postavi ogromne botnet-ove širom sveta. Mašine koje kontrolišu botovi omogućavaju napadačima da postavljaju virtualne superračunare koji mogu da predstavljaju rivale nacionalnoj računarskoj snazi. Mogu da koriste te resurse da bi stvorili ogromnu poplavu, razbiju (eng. *crack*) kripto ključeve

[7] Ovakvi podaci su nečitljivi osobama koji ne poseduju ključ kako bi ih dekodirali i saznali njihovo značenje.

[8] Hosting servis baziran na vebu koji se koristi za kontrolu verzija. https://github.com/

[9] Amazon Web Services (AWS) je ogranak kompanije Amazon koja na zahtev pojedinca, kompanije ili Vlade pruža računarske resurse.

[10] Softver ili hardver koji ima sposobnost da beleži sve što je otkucano na tastaturi i taj sadržaj čuva u kriptovanom fajlu.

ili lozinke, ili da bi istražili osetljive finansijske podatke koji se koriste za krađu identiteta.

Botovi i ostali alati koji se koriste za napade su postali veoma modularni, svaki modul se sastoji iz softverskih komponenti koje omogućavaju napadačima da brzo menjaju funkcionalnost kako bi pokrenuli nove vrste napada. Obični botovi danas sadrže 50 do 100 različitih funkcionalnih modula; napadač može da ugasi ili odstrani module koji nisu potrebni za dati napad, dok lako integriše nove funkcije koda.

Ubrzavajući evoluciju, napadači se sve više oslanjaju na bot kod koji se sam preobražava, dinamički stvarajući funkcionalno ekvivalentnu verziju sa različitim skupovima osnovnog koda. Takav polimorfni kod pomaže napadačima da izbegnu alate za detekciju koje antivirusi i *antispyware* softveri[11] danas koriste. Ovaj dinamički samopodešavajući kod je teže filtrirati, s obzirom da konstantno menja svoj osnovi softver. Ova „pokretna meta“ koda otežava analizu od strane branilaca. Polimorfni kod podstiče ciljeve napadača jer napadači imaju dužu kontrolu nad botnetom izbegavajući filtriranje i detekcije, tako da mogu da zarade što više novca od zaraženih sistema.

6 Glasanje putem Interneta

Postoje mnogi načini na koje napadači mogu da naruše bezbednost umreženih računara. Međutim, praktičnost i niska cena obavljanja poslova putem Interneta donose značajne prednosti, pa nije iznenađujuće da se onlajn rešenje često predlaže kada postoji problem sa tradicionalnim načinom. U ovom delu biće prikazani predlozi za sprovođenje izbora putem Interneta.

6.1 Motivacija za glasanje putem Interneta

Predsednički izbori 2000. godine su bili jedni od najneizvesnijih u istoriji SAD. Presudni su bili izborni glasovi države Florida. Bez njih ni demokrata Al Gor (eng. *Al Gore*), ni republikanac Džordž Buš (eng. *George V. Bush*) nisu imali većinu glasova. Buš je pobedio sa razlikom od 537 glasova u odnosu na Al Gora. Bušova prednost bila je neverovatno mala: manje od 2 glasa na svakih 10.000 glasova.

Većina okruga u Floridi koristila je mašinu za glasanje u kojoj birači biraju kandidata tako što olovkom probuše rupu u kartici pored odgovarajućeg imena (Slika 4). Prvi problem sa ovim načinom glasanja je da olovka ponekad ne probuši glatko rupu i takve glasove mašina za automatsko prebrojavanje obično ne uračuna. Zbog toga je bilo potrebno ručno prebrojavanje koje se fokusiralo na identifikaciji takvih glasačkih listića. Druga nepravilnost bila je da su neki birači u okrugu Palm Beach bili zbunjeni glasačkim listićima i želeći da glasaju za kandidata Al Gor koji je bio drugi na listi s leve strane, probušili drugu rupu koja zapravo odgovara kandidatu Patu Bakananu. Ova konfuzija je možda koštala Al Gora glasova koji su mu bili potrebni za pobedu na Floridi.

Problemi sa izborima na Floridi doveli su do raznih akcija za poboljšanje pouzdanosti glasačkih sistema u SAD [11]. Mnoge države su zamenile papirne sisteme elektronskim glasačkim aparatima za direktno očitavanje, a neke su predložile da se koristi glasanje putem Interneta.

[11] Vrsta programa napravljena za sprečavanje i otkrivanje neželjenih instalacija špijunskih softvera i uklanjanje tih programa ukoliko su instalirani.

Slika 4: Glasački listić - predsednički izbori na Floridi, SAD 2000.g.

Međutim, glasanje putem Interneta u SAD je i danas omogućeno samo za vojna lica u inostranstvu i to samo u nekim državama [10]. Estonija je bila prva zemlja koja je omogućila svim svojim građanima da glasaju putem Interneta na lokalnim i nacionalnim izborima, 2005. godine. Norveška je omogućila glasanje putem Interneta 2011. i 2013. godine, ali se nakon toga vratila na stari način glasanja. Postoji 14 zemalja koje u današnje vreme koriste Internet kao opciju za glasanja, makar u nekim svojim delovima i tu spadaju i Kanada, Francuska i Švajcarska.

6.2 Etička procena

U ovom poglavlju biće diskutovano o glasanju putem Interneta na osnovu prikazanih rizika i benefita.

BENEFITI GLASANJA PUTEM INTERNETA

- Glasanje putem Interneta daje ljudima priliku da glasaju iz svojh domova, ukoliko nisu u mogućnosti da dođu do biračkog mesta.
- Glasovi koji se šalju putem Interneta mogu se prebrojati mnogo brže od glasova na papiru.
- Elektronski glasovi ne bi imali nikakvu dvosmislenost.
- Izbori koji su sprovedeni na Internetu koštali bi manje nego tradicionalni izbori.
- Glasanje putem Interneta eliminisalo bi rizik da neko manipuliše glasačkom kutijom u kojoj se nalaze glasački listići.
- Dok na većini izbora ljudi glasaju za jednog kandidata, drugi izbori omogućavaju da osoba glasa za više kandidata. Na primer, školski odbor može imati tri slobodna radna mesta, a od glasača se moze tražiti da glasaju za tri kandidata. Bilo bi lako isprogramirati obrazac za glasanje kako bi se sprečilo da ljudi glasaju za više ljudi nego što bi trebalo.
- Ponekad, dugi i komplikovani glasački papiri rezultiraju tome da glasač slucajno zaboravi da zaokruži kandidata za određenu poziciju. Veb forma bi mogla da se dizajnira da bude na više strana i da svaka strana ima kandidata za jednu poziciju.

RIZICI GLASANJA PUTEM INTERNETA

- Glasanje putem Interneta daje prednost onima koji su u finansijski boljoj situaciji tj. ljudima koji imaju računare i Internet.
- Isti sistem vrši autentifikaciju glasača i beleži glasački listić. Ovo otežava čuvanje privatnosti glasača.

- Glasanje putem Interneta povećava mogućnost za kupovinu i prodaju glasova. Pretpostavimo da se osoba X složi da glasa za kandidata Y u zamenu za isplatu od osobe Z. Ako osoba X glasa sa njegovog računara, može da dozvoli osobi Z da gleda kako je glasao za Y, dokazujući na taj način da je ispunio svoje obećanje. Ovo je mnogo manje verovatno na zvaničnom biračkom mestu koje nadgledaju izborni zvaničnici.
- Veb lokacija koja održava izbore očigledna je meta DDoS napada. Za razliku od korporativnih veb stranica, koje privlače pažnju tinejdžera hakera, veb stranica za nacionalne izbore mogla bi privući pažnju stranih vlada ili terorista koji pokušavaju poremetiti izborni proces.
- *Backdoor* Trojanac[12] (eng. *backdoor Trojan*)[13] koji vreba na računaru glasača bi mogao da omogući da glasač bude posmatran ili čak da omogući da neko drugi glasa umesto pravog glasača.
- Napadač može da prevari korisnika da misli da je povezan sa serverom za glasanje kada je u stvari povezan sa lažnim serverom za glasanje koji je kontrolisan od strane napadača. Na primer, napadač može da pošalje mejl u kojem se glasači pozivaju da kliknu na link da bi došli do mesta glasanja. Učinivši to, oni bi bili povezani sa lažnim glasačkim mestom. Napadač može tražiti potrebne informacije birača, a zatim koristiti te informacije da se poveže sa pravim biračkim mestom i glasa za kandidata za koga želi.

„Siguran sistem za glasanje putem Interneta je teorijski moguć, ali to bi bila prva sigurna umrežena aplikacija ikada stvorena u istoriji računarstva.“, napisao je Bruce Schneier[14].

U aprilu 2001. Vivendi Universal, pariski medijski konglomerat, održao je glasanje putem Interneta za svoje akcionare. Hakeri su napravili da se glasovi nekih velikih akcionara računaju kao uzdržani. Ako ovakvi privatni izbori mogu privući pažnju hakera, pretpostavlja se da bi neki veći izbori bili atraktivnija meta.

Svaki izborni sistem koji se oslanja na bezbednost ličnih računara kojim upravljaju obični građani biće osetljiv na prevare. Iz tog razloga, postoji jak argument zašto vlada ne bi dozvolila da se na taj način sprovede glasanje.

7 Zaključak

Iz svega priloženog, korišćenje Interenta bi trebalo da bude odgovorno. Videli smo da ni ozbiljne organizacije nisu uspele da se odbrane od zlonamernih napada. Stoga, svako od nas treba biti svestan ozbiljnosti napada kojim može biti izložen i oprezan prilikom ostavljanja ličnih i poverljivih informacija.

Literatura

[1] APWG.org. APWG News. https://www.apwg.org//apwg-news-center/.

[12] Štetni program maskiran u program koji je koristan, dok u pozadini izvršava zlonamerne akcije bez znanja korisnika.

[13] Trojanac koji napadaču daje pristup računaru žrtve.

[2] CSO. The 18 biggest data breaches of the 21st century. https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

[3] US-CERT (eng. *The United States Computer Emergency Readiness Team*). What Is Phishing? https://www.us-cert.gov/report-phishing.

[4] Larry K. Wentz Franklin D. Kramer, Stuart H. Starr. *Cyberpower and National Security, poglavlje Advancement of Computer and Network Attack and Exploitation Methodologies, strane 163-164.* Potomac Books, Inc., 22841 Quicksilver Drive Dulles, Virginia, 2009.

[5] Trend Micro. Cybercriminals, 2019. https://www.trendmicro.com/vinfo/us/security/definition/cybercriminals.

[6] Palo Alto Networks. What is a Denial-of-Service attack? https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos.

[7] Phishing.org. 10 Ways To Avoid Phishing Scams. http://www.phishing.org/10-ways-to-avoid-phishing-scams.

[8] Phishing.org. History of Phishing. https://www.phishing.org/history-of-phishing.

[9] PhoenixNAP. 7 Tactics To Prevent DDoS Attacks And Keep Your Website Safe. https://phoenixnap.com/blog/prevent-ddos-attacks.

[10] David Pogue. Get Out the iVote. *Scientific American*, 2016. https://www.scientificamerican.com/article/when-will-we-be-able-to-vote-online/.

[11] Michael J. Quinn. *Ethics for the information age.* Pearson Education, One Lake Street, Upper Saddle River, New Jersey 07458, 2015.

[12] Koceilah Rekouche. Early Phishing. https://arxiv.org/abs/1106.4692.

[13] Brahima Sanou. Global Cybersecurity Index 2017. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.

[14] Bruce Schneier. Technology Was Only Part of the Florida Problem. *Computerworld*, 2000.

[15] Statista. Retail e-commerce worldwide. https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/.

[16] W3Schools. SQL Injection. https://www.w3schools.com/sql/sql_injection.asp.

A Dodatak

Sada kad su objašnjeni glavni problemi na Internetu koji se tiču bezbednosti i kako do njih dolazi, postavlja se pitanje da li se oni mogu sprečiti i da li je bilo kakav vid zaštite moguć? U ovoj glavi biće prikazano na koje načine se možemo zaštititi od najčešćih vrsta sajber napada koje su opisane u poglavlju 3.

A.1 Zaštita od fišinga

Fišing prevare su prisutne od samog početka Interneta i one neće nestati u skorije vreme. Srećom, postoje načini kako da ne postanete žrtva istih. Neke osnovne smernice za zaštitu od fišinga [7] su:

1. **Budite informisani o tehnikama fišinga.** Sve vreme se razvijaju novi načini za fišing prevare. Ukoliko niste upućeni u nove tehnike fišinga, možete vrlo lako pasti na njih. Što pre saznate za njih, rizik da se tako nešto desi biće mnogo manji.
2. **Razmislite pre nego što kliknete.** U redu je kliknuti na linkove na pouzdanim sajtovima. Ali ako kliknete na linkove koji se pojavljuju u nasumičnim mejlovima, to i nije tako pametan potez. Pređite preko linkova za koje niste sigurni da su pouzdani pre nego što kliknete na njih i prikazaće vam se prava adresa linka.
3. **Proverite sigurnost sajta.** Prirodno je biti oprezan kada je reč o ostavljanju poverljivih finansijskih informacija na mreži. Međutim, sve dok ste na bezbednom sajtu ne bi trebalo da naiđete na probleme. Pre nego što pošaljete bilo koju poverljivu informaciju, uverite se da adresa sajta počinje sa „https“[14] i da pored adrese postoji ikonica zaključanog katanca.
4. **Instalirajte anti-fišing *tulbar* (eng. *toolbar*)** [15]**.** Na ovaj način pokreću se brze provere lokacija koje posećujete i upoređuju se sa listama poznatih fišing lokacija. Ako naiđete na zlonamernu stranicu, bićete upozoreni.
5. **Redovno proveravajte svoje naloge na Internetu.** Naviknite se da često menjate lozinke i proveravate mesečne izveštaje kako biste se uverili da nije došlo do transakcija bez vašeg znanja.
6. **Ažurirajte vaš pregledač.** Popularni pregledači izbacuju poboljšanja bezbednosti sve vreme.
7. **Koristite zaštitne zidove (eng. *firewall*)**[16]**.** Kvalitetni zaštitni zidovi se ponašaju kao baferi između vas, vašeg kompjutera i osobe koja želi da upadne u vaš računar. Trebalo bi koristiti dve vrste i to: lični zaštitni zid(eng. *personal firewall*) i mrežni zaštitni zid (eng. *network firewall*). Prva opcija je vrsta softvera, a druga vrsta hardvera. Kada se zajedno koriste drastično smanjuju šansu da do fišinga dođe.
8. **Budite oprezni sa iskačućim prozorima.** Često se maskiraju u legitimne komponente veb sajta a u stvari budu pokušaji fišinga. Mnogi popularni veb pregledači vam omogućavaju da ih blokirate.
9. **Nikada nemojte davati lične informacije.** Kao opšte pravilo, nikada ne bi trebalo da dajete lične i finansijski poverljive informacije putem Interneta. Kada ste u nedoumici, posetite zvanični sajt kompanije, potražite njihov broj telefona i nazovite ih. Nikada nemojte unositi poverljive informacije preko linkova koji se nalaze u mejlovima.

[14] Bezbedna verzija protokola HTTP (eng. *Hyper Text Transfer Protocol*). „S“ dolazi od *secure* što nam govori da je komunikacija između pretraživača i veb sajta enkriptovana.

[15] Traka sa ikonicama koje su prečice do nekih softverskih alata.

[16] Hardver ili softver koji u sklopu računarske mreže sprečava neželjeni prenos podataka preko mreže.

10. **Koristite antivirusni program.** Antivirus skenira svaki fajl koji dolazi preko Interneta na vaš računar i pomaže u sprečavanju oštećenja vašeg sistema.

A.2 Zaštita od SQL injekcije

U poglavlju 3.2 videli smo na koje sve načine možemo biti izloženi SQL injekciji. Zaštita od ovakvih napada je moguća korišćenjem SQL parametara. To su vredosti koje su dodate SQL upitu u vreme izvršavanja na kontrolisan način.

Primer A.2.1

```
txtUserId = getRequestString("UserId");
txtSQL = "SELECT * FROM Users WHERE UserId = @0";
db.Execute(txtSQL,txtUserId);
```

Primer A.2.1 je deo koda u ASP.NET-u u kome se koriste parametri. Parametri su predstavljeni znakom @. SQL mehanizam proverava parametre kako bi se uverio da su ispravni i da se tretiraju bukvalno a ne kao deo SQL-a koji se izvršava [16].

A.3 Zaštita od DDoS napada

Evolucija DDoS napada ne pokazuje nikakve znakove usporavanja. Njihova snaga i učestalost stalno rastu, uključujući kombinovani ili hibridni pristup. Nemoguće ih je prepoznati bez ranog otkrivanja opasnosti i sistema za profilisanje saobraćaja[17]. U stvari, moguće je da se napad prepozna samo kada sajt usporava ili se ruši. Ovo posebno važi sa sofisticirane napade koji koriste kombinovani pristup i ciljaju više nivoa istovremeno. Ovi napadi ciljaju podatke, aplikacije i infrastrukturu istovremeno kako bi povećali šanse za uspeh. Kako bi se odbranili od ovih napada, potrebni su planovi „za bitku“, kao i pouzdane prevencije od DDoS-a i rešenja za ublažavanje napada. Takođe, potrebna je integrisana bezbednosna strategija koja štiti sve nivoe infrastrukture. Šta sve treba uraditi kako bismo se zaštitili od DDoS napada [9]:

1. **Razviti plan odgovora na DDoS napad.** Veće kompanije, za razliku od manjih, zahtevaju kompleksniju infrastrukturu i potrebno je više timova koji rade na planiranju sprečavanja DDoS napada. Kada se desi DDoS napad, nema vremena da se razmišlja o najboljim koracima, već je potrebno da se oni unapred definišu kako bi se omogućile brže reakcije i izbegli bilo kakvi uticaji napada. Izrada plana odgovora na incidente je ključni prvi korak ka sveobuhvatnoj strategiji odbrane. U zavisnosti od infrastrukture, plan za odgovor na DDoS napad može da bude poprilično iscrpljujuć. Prvi korak obično definiše ishod napada. Treba se postarati da centar za podatke bude uvek spreman na napad, a tim je svestan svojih odgovornosti. Na taj način se može minimizovati uticaj napada i mogu se sačuvati meseci oporavka. Ključni elementi ostaju isti za bilo kakvu vrstu kompanije i oni uključuju:

[17] Sistem koji prikuplja i evaluira podatke veza na osnovu grafa koji se sastoji iz veza zasnovanih na mrežnom saobraćaju i kasnije može da detektuje neki abnormalan saobraćaj upoređivajući ga sa napravljenim profilom.

- **Kontrolnu listu sistema** - listu stvari koje treba implementirati kako bi se osigurale napredne identifikacije pretnji, procena i alati za filtriranje.
- **Formiranje tima za odgovor na napad** - odgovornosti se definišu za svakog člana tima kako bi se osigurale reakcije na napad kad se on bude desio.
- **Definisanje obaveštenja i procedura eskalacije** - treba se pobrinuti da svaki član tima zna tačno kome treba da se obrati kada do napada dođe.
- **Uključivanje liste unutrašnjih i spoljašnjih kontakata** - odnosno osoba koje treba da budu informisane o napadu. Treba razviti strategije za komunikaciju sa klijentima, provajderom *cloud* usluga i bilo kakvim prodavcima bezbednosti.

2. **Osigurati svoju mrežnu infrastrukturu.** Ublažavanje ugrožavanja bezbednosti mreža se može postići jedino strategijama zaštite na više nivoa. Ovo uključuje napredne sisteme za sprečavanje upadanja u sistem i upravljanje pretnjama, koji kombinuju zaštitne zidove, VPN (eng. *Virtual Private Network*), anti-spam, filtriranje sadržaja, balansiranje opterećenja i druge slojeve tehnika odbrane od DDoS-a. Zajedno oni omogućavaju konstantnu i konzistentnu zaštitu mreže kako bi sprečili DDoS napade. Većina standardne mrežne opreme dolazi sa ograničenim opcijama za ublažavanje DDoS napada, tako da je poželjno da se uključe neke dodatne usluge. Takođe je poželjno da su svi sistemi ažurirani. Kod neažuriranih sistema je moguća česta pojava propusta koji se tiču bezbednosti i DDoS napadači pronalaze te propuste.
3. **Vežbati osnove bezbednosti mreže.** Najosnovnija protivmera za sprečavanje DDoS napada je omogućavanje što je manje moguće grešaka sa strane korisnika. Angažovanje u jakim bezbednosnim praksama može onemogućiti kompromitovanje poslovnih mreža. Vežbanje bezbednosti uključuje kompleksne šifre koje se redovno menjaju, anti-fišing metode i bezbedne zaštitne zidove. Samo ove mere neće zaustaviti DDoS napad, ali mogu da posluže kao bitna sigurnosna osnova.
4. **Održavati jaku arhitekturu mreže.** Fokusiranje na bezbednost arhitekture mreže je od vitalnog značaja za bezbednost. Firme bi trebalo da naprave suvišne mrežne resurse; ako je jedan server napadnut, ostali mogu da upravljaju dodatnim mrežnim saobraćajem. Ako je moguće, server treba locirati na različitim geografskim mestima. Tako rasipani resursi predstavljaju težu metu za napadača.
5. **Iskoristiti *cloud*.** Korišćenje *cloud* usluga pruža dosta pogodnosti. *Cloud* ima veći protok i više resursa nego bilo koja privatna mreža. Kako se broj DDoS napada povećava, oslanjanje isključivo na lokalni hardver će verovatno propasti. Aplikacije zasnovane na *cloud*-u mogu da priguše štetan ili zlonameran saobraćaj pre nego što stigne do željene lokacije. Uslugama na *cloud*-u upravljaju softver inženjeri čiji je posao da prate dešavanja na vebu koja se tiču najnovijih DDoS taktika. Različite kompanije imaju različita okruženja za podatke i aplikacije. Hibridna okruženja mogu biti

pogodna za postizanje prave ravnoteže između sigurnosti i fleksibilnosti, posebno za proizvođače koji nude rešenja „po meri“.

6. **Razumevanje znakova upozorenja.** Neki simptomi DDoS napada uključuju gašenje mreže, povezivanje na neku privatnu mrežu kompanije ili naizmenično gašenje veb stranica. Nijedna mreža nije savršena, ali ukoliko se čini da je nedostatak performansi produžen ili ozbiljniji nego obično, na mrežu se verovatno izvršava DDoS napad i kompanija treba preduzeti mere.