ZAŠTITA KORISNIKA WEB PORTALA OD MALICIOZNIH NAPADA

Dalić, Toni

VISOKO UČILIŠTE ALGEBRA

DIPLOMSKI RAD

ZAŠTITA KORISNIKA WEB PORTALA OD MALICIOZNIH NAPADA

Toni Dalić

Zagreb, veljača 2019.

Predgovor

Prilikom uvezivanja rada, Umjesto ove stranice ne zaboravite umetnuti original potvrde o prihvaćanju teme diplomskog rada kojeg ste preuzeli u studentskoj referadi

Sažetak

Hrvatski:

Rad se bavi pregledom mogućih malicioznih prijetnji za korisnike Interneta u kontekstu sigurnosti podataka i imovine. Analizom najčitanijih web portala u Hrvatskoj prikazani su tehnološki i ljudski popusti koji mogu negativno utjecati na posjetitelje koji odgovornim ponašanjem i edukacijom trebaju prepoznati moguće prijetnje i odgovornim ponašanjem izbjeći mogućnost malicioznog napada. U radu su predstavljena tehnološka rješenja koja će pomoći korisnicima u zaštiti, kao i pregled najrelevantnijih web portala koji se bave problemima informacijske sigurnosti. Rad je također nastojao prikazati kako se uz pomoć najosnovnijeg marketinga pokušava doći do potencijalnih žrtava malcioznih napada.

Ključne riječi: web portal, socijalni inženjering, maliciozni program, informacijska sigurnost, računalni kriminal

Engleski:

The paper deals with an overview of possible malicious threats for Internet users in the context of security of data and property. By analyzing the most popular web portals in Croatia, there are technological and human discounts that can negatively affect visitors. Internet user's responsible behavior and education should identify possible threats and responsible behavior to avoid the possibility of a malicious attack. The paper presents technological solutions that will help protect users, as well as an overview of the most relevant web-portals dealing with information security issues. The paper also intents to show how the malicious programer get to their victims by using the most basic marketing campaings.

Keywords: web portal, social engineering, malicious program, information security, computer crime

Sadržaj

1. Uvod

Trend korištenja Interneta Kako u svijetu, tako i u Hrvatskoj, eksponencijalno raste. Primjerice, u Hrvatskoj je 2000. godine 7% populacije koristilo Internet, 2010. 57%, a u 2016. se procjenjuje da je 74% populacije koristilo Internet. Globalno se Internetom koristi 47% populacije. U Hrvatskoj je porast broja korisnika Interneta izraženiji u odnosu na nerazvijene zemlje koje nemaju dovoljno sredstava kako bi svojih građanima osigurali stabilan pristup, potporu u obliku edukacije te općenito razinu kupovne moći koja će građanima omogućiti samostalnu inicijativu u edukaciji i korištenju najnovijih tehnologija. Paralelno s brojem korisnika Interneta raste i broj Internet stranica te količina podataka koja se distribuira što institucijama, tvrtkama i organizacijama predstavlja problem u pogledu informacijske sigurnosti[1], odnosno ostavlja mogućnost zlonamjernim pojedincima ili organizacijama da iskoriste sigurnosne protokole i zaštite kako bi neželjeno utjecali na institucije, organizaciju ili pojedinca. Uvijek postoji mogućnost tehnološkog propusta koji može dovesti do malicioznog napada bilo malicioznim programom ili nekom od metoda socijalnog inženjeringa. Važno je da korisnici Interneta imaju sposobnost samostalnog uočavanja potencijalnih opasnosti te znanja o postojanju nadležnih službi koje kontinuirano rade na edukaciji građana. Rad na vidljivosti napora u području informacije sigurnosti može motivirati jedan dio građana da poduzmu preventivne mjere u zaštiti osobnih podataka i imovine, a drugima može pomoći u donošenju odluke i akciji i trenutku kada sumnjaju na mogućnost zlonamjernog napada. U radu će biti analizirani tehnološki i ljudski propusti najčitanijih web portala u Hrvatskoj te navedeni mogući negativni utjecaji na korisnika web portala. Također će biti analizirani dostupni online servisi i organizacije koje se bave zaštitom korisnika od svih vrsta malicioznih napada te preporuke o njihovom korištenju.

[1] Informacijska sigurnost je stanje povjerljivosti, cjelovitosti i raspoloživosti podatka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom potporom za poslove planiranja, provedbe, provjere i dorade mjera i standarda. (Ured vijeća za nacionalnu sigurnost, 2018)

2. Maliciozni računalni programi

Sve maliciozne programe možemo obuhvatiti pod zajednički naziv *malware*. Riječ *Malware* je skraćenica za „zlonamjerni software“ (engl. *Malicious software*), te se koristi kao *„…opći izraz za dio softvera ubačenog u informacijski sustav radi uzrokovanja štete tom sustavu ili drugim sustavima, ili radi obaranja tih sustava za njihovo korištenje u druge svrhe nego li u one koje namjerava vlasnik.“* (OECD, 2008.). Za sve vrste navedenih malicioznih programa je karakteristično da se preuzimaju i pokreću bez znanja korisnika, odnosno bez njegovog pristanka (CARNet, 2009.), a specifičnosti raspoznajemo prema njihovim funkcionalnostima i načinu ponašanja (Laktašić et al., 2012.):

- **multifunkcionalnost i modularnost**
  Multifunkcionalnost i modularnost odnosi se mogućnost zajedničkog djelovanja više malicioznih programa s ciljem postizanja napadačeva cilja. Primjerice, maliciozni program koji je već u sustavu može preuzeti dodatne maliciozne programe kako bi proširio svoje funkcionalnosti
- **dostupnost i primjerenost korisnicima** (engl. *User friendly,* hr. *lak za upotrebu*)
  Dostupnost se odnosi na slobodnu mogućnost preuzimanja ili kupnje, a *Primjerenost* označava mogućnost sofisticiranog napada van razina korisnikovih vještina.
- **upornost i učinkovitost**
  Upornost određuje težinu detekcije, a *Učinkovitost* mogućnost malicioznog programa da zaobiđe ugrađene sigurnosne mjere
- **mogućnost djelovanja na skup uređaja**
  Malware je dio širokog sustava cyber napada
- **profitabilnost**
  Korištenje zloćudnog programa s ciljem stjecanja financijske ili neke druge dobiti. Maliciozni programi ovakvog tipa predstavljaju računalni kriminal.

Maliciozne programe možemo kategorizirati:

- prema načinu širenja:
  - virusi
  - crvi
  - trojanski konji

- prema načinu djelovanja
  - špijunski programi (engl. *Spyware*)
  - oglašivački programi (engl. *Adware*)
  - kriminalni programi (engl. *Crimeware*)
  - programi koji se šire zastrašivanjem (engl. *Scareware*)
  - programe za tajno praćenje i bilježenje pritisnutih tipki na tipkovnici, odnosno računalu (engl. *Keylogger*)
  - programe za udaljenu kontrolu (engl. *Rootkit*)
  - software za otkupninu (engl. *Ransomware*)

Kada se maliciozni programi koriste s ciljem ostvarivanja financijske ili druge kriminalne koristi, tada za takva programe nazivamo *Krimeware* (engl. crimeware) Krimeware je potklasa *Malweara*, a pomaže u obavljanju kriminalnih radnji putem računala (Grubor i Franc, 2010.)

2.1. Virusi

Virus je vrsta računalnog programa koji pokretanjem i modifikacijom drugih programa i svojih kopija stvara neželjene učinke na računalu korisnika. Kada računalni program svojom modificiranom ili nemodificiranom kopijom ubacuje svoje naredbe u postupak izvršenja, takav legitiman program smatramo inficiranim[2]. Virusi su po svojoj strukturi kao i svi ostali programi, stoga računalo ne može raspoznati koji program se izvršava kontrolirano, a koji nekontrolirano (Dulčić, 2007.).

Nakon što se maliciozni software uspješno priključi na neki program, datoteku ili dokument, on neće početi sa svojim djelovanjem sve dok ponašanje korisnika ne uzrokuje pokretanje, odnosno izvršavanje koda štetnog programa. Osnovno obilježje programa za koji se maliciozni software veže je njegova tehnička mogućnost pokretanja i izvršavanja

[2] Latinski *inficere*, što znači "onečistiti", "zaraziti"

markonaredbi[3] . To znači da se virus neće aktivirati sve dok korisnik ne pokrene program koji je zaražen malicioznim programom, ne pokrenemo određeni dio programa ili otvori zaraženu datoteku ili dokument što znači da računalo može biti zaraženo virusom, a da to korisnik nikada ne sazna, odnosno da spletom okolnosti ne napravi radnje koje će posljedično aktivirati maliciozni program i napraviti štetnu radnju po njegovo računalo (uređaj), dokumente ili osobne podatke (Agencija za elektroničke medije, 2017.). Virusi se, osim napada na fizičke osobe mogu usmjeriti i prema institucijama, tvrtkama i bolnicama, a jedan od najopasnijih virusa pod nazivom „Stuxnet“ koji je inficirao računalo preko prijenosne USB memorije. Glavni zadatak Stuxneta bio je onemogućiti Iran u daljnjem razvoju nuklearne tehnologije na način da je slao tajne pratio standardne operativne procese nuklearne elektrane te modificirao podatke koji su se dalje slali u operativni sustav kako bi se činilo da nema nikakvih anomalija u procesima. Rezultat virusa možemo vidjeti iz izvješća međunarodnih inspektora za praćenje nuklearnog djelovanja u kojem stoji da su se neki dijelovi postrojenja u potpunosti uništili (Robić, 2018).

Najčešća zaštita od infekcije računala virusom je korištenje programa koji na temelju uzoraka prepoznaju datoteke koje su virusi ili potencijalno zaražene datoteke. Virusi koriste razne „tehnike“ kako bi izbjegli detekciju od strane takvih programa. Tako neki virusi imaju sposobnost da presretnu komunikaciju između antivirusnog alata i operacijskog sustava navodeći obmanjujući korisnika da je sve u redu ili da se prilikom detekcije repliciraju mijenjajući svoj kod i dužinu (Nacionalni CERT, 2018.).

2.2. Crvi

Računalni crvi su programi koji imaju sposobnost samo-umnožavanja s ciljem zagušenja prometa podataka na mreži ili punjenja tvrdog diska (engl. *Hard disk)*[4], neželjenim podacima do njegovog potpunog punjenja. Za cijelo vrijeme djelovanja, crv će se pretvarati da obavlja dio legitimnih poslova mreže. Crvi, za razliku od virusa nemaju mogućnost ubacivanja u neki legitiman program kako bi se širili, odnosno ne koriste domaćina. (Dulčić, 2007.) Cilj

[3] Makronaredba je niz naredbi i uputa koje grupirate kao pojedinačnu naredbu za automatsko izvršavanje zadataka (Microsoft, 2018)
[4] Medij za pohranu digitalnih informacija (Leksikografski zavod Miroslava Krleže, 2018.)

većine računalnih crva je, osim zagušiti promet ili tvrdi disk računala, koristiti tu istu mrežu koju zagušuje kako bi se razmnožio na što više računala u što kraćem vremenskom periodu. Računalni crvi će se mrežom razmnožavati na dva načina (Dulčić, 2007):

- interakcijom korisnika
- bez interakcije korisnika

Interakcija korisnika podrazumijeva akciju od strane pošiljatelja računalnog crva putem nekog od digitalnih komunikacijskih kanala. Digitalni kanali koji se najčešće koriste za slanje računalnog crva su elektronička pošta i čavrljanje[5]. U prošlosti je računalni crv putem elektroničke pošte stizao kao privitak, a najčešće uz primamljiv tekst koji će navesti potencijalnu žrtvu da klikne na poveznicu i bude preusmjerena na daljnje korake u preuzimanju malicioznog programa, a može i pokrenuti preuzimanje računalnog crva na računalo korisnika. Treće strane na koje korisnik bude preusmjeren mogu naći sigurnosne propuste na mreži i na taj način inficirati računalo. Isti princip navođenja žrtve primamljivim tekst pošiljatelji će koristiti i prilikom korištenja engl. Chatbotova (Nacionalni CERT, 2018.) Chatbotovi su programska rješenja koja omogućuju da umjetna inteligencija stupi u Interakciju s posjetiteljem, bez obzira radi li se o mrežnoj stranici ili aplikaciji. (Chatbot, 2017). Takvi Botovi imaju mogućnost prepoznati aktivnost korisnika, lokaciju te mnoge druge informacije koje analizom aktivnosti i pregledanih mrežnih stranica odabire poruku s kojom će pristupiti posjetitelju. Informacije o lokaciji najčešće se koriste za odabir jezika na kojem će se Chatbot aktivirati kako bi bili što uvjerljiviji u prijenosu poruke i navođenju korisnika da preuzme maliciozni program. Slična tehnologija krije se i iza programa za čavrljanje koji omogućuju interakciju umjetnom inteligencijom, kao i interakciju između dvije fizičke osobe.

Najveći napad računalnim crvom pokrenut je 12.05. 2017. Računalni crv zvao se engl. *Wanna cry* (hr. *Želim plakati)*. Rezultat napada bio je blokiranih oko 75.000 računala u preko stotinu zemalja svijeta. Računalni crv blokirao je i brojne institucije, bolnice, tvrtke… Kada bi crv inficirao računalo, prikazao je poruku te tražio uplatu 300 dolara u Bitcoinu.[6] Taj iznos vrijedio je samo prvih šest sati, nakon čega bi iznos počeo rasti. Virus je zaustavio Darien Huss koji je otkrio dio koda koji navodi računalnog crva da se spoji s mrežnom stranicom

[5] Engl. *Chat*; Komunikacija između dvaju ili više korisnika interneta razmjenom niza kratkih tekstovnih poruka koja se odvija se bez vremenske zadrške, tj. u realnom vremenu
[6] Oblik digitalnog novca

čiji se naziv sastoji od nasumičnih slova i brojeva. Naravno, računalni crv ne bi mogao pronaći tu stranicu jer ne postoji i nakon toga zaključao računalo. Darien Huss je zakupio domenu nakon čega se počelo na domenu prijavljivati tisuće računalnih. Do tada je, nažalost velik broj institucija, bolnica, tvrtki i privatnih osoba uplatio kako bi povratili kontrolu nad računalom i podacima (Večernji list, 2017.)

2.3. Trojanski konj

Trojanski konj (engl. *Trojan horse*) se izgleda kao i svaki drugi korisnički program i prilikom pokretanja započinje izvršavati svoju destruktivnu zadaću, npr. Brisanje svih podataka s tvrdog diska. On se ne može sam razmnožavati (za razliku od virusa ili crva), već njegovo razmnožavanje počinje akcijom korisnika (Nacionalni CERT, 2017.). Pod trojanskim konjima obično smatramo programe koji na izgled rade nešto korisno i poželjno, a zapravo izvršavaju aktivnosti koje korisnik nije očekivao ili ne želi (Dulčić, 2007.). Trojanski konj može izmijeniti operacijski sustav na zaraženom računalu, a posljedice mogu biti od prikaza reklamnog sadržaja, npr. Putem skočnih prozora[7] do preuzimanja potpune kontrole potpunu kontrolu nad zaraženim računalom čime napadač može (Nacionalni CERT, 2017.):

- koristiti zaraženo računalo kao dio „botnet“ mreže

Botnet je *„ …mreža računala, mobilnih uređaja ili Internet stvari (engl. Internet of things), često pod kontrolom jednog kontrolnog (P2P) poslužitelja, u koje su ubačeni automatizirani programi za ostvarivanje određenih zadataka* (PC ekspert, 2016). U ovom slučaju se ne radi o legitimnom botnetu za npr. Znanstvena istraživanja, već o malicioznom koji je namijenjen stjecanju financijske ili druge koristi protivno volji korisnika.

- ukrasti povjerljive informacije
- instalirati druge oblike zlonamjernog softvera
- slati, primati i modificirati datoteke zaraženog računala
- bilježiti pritisnute tipke
- pratiti (špijunirati) aktivnosti žrtve

[7] (engl *pop up) skočni prozor preglednika koji prikazuje reklame ili oglase*

- koristiti memoriju (prostor) tvrdog diska
- rušiti zaraženo računalo itd.

Nije nužno da napadač zarazi računalo kako bi preuzeo kontrolu već može skeniranjem otkriti računalo zaraženo trojanskim konjem te ga iskoristiti za preuzimanje kontrole. Trojanski konj se širi (Nacionalni CERT, 2017.)

- preuzimanjem zaraženog softvera
- kao dio softvera
- kao e-mail privitci
- putem zlonamjernih web stranica s dinamičkim sadržajem (npr. ActiveX)
- preko ranjivosti softvera

Antivirusni i drugi *anti-malware* programi (programi koji sprečavaju neželjene učinke zloćudnih programa), pružaju zaštitu od napada trojanskog konja, no ukoliko je napadač putem trojanskog konja ranije imao pristup računalu, tada je kompliciranije detektirati i ukloniti trojanskog konja obzirom da je prvo potrebno otkriti sve promjene koje je trojanski konj napravio na sustavu. Najčešće se tada pristupa formatiranju tvrdog diska, odnosno instalaciji novog operativnog sustava (Nacionalni CERT, 2018). Prvi korak zaštite od trojanskog konja je edukacija korisnika obzirom da je ljudski faktor presudan za pokretanje malicioznog programa, odnosno akcija od strane korisnika.

2.4. Špijunski softver

Špijunski softver (engl. Spyware) preuzima kontrolu nad računalom korisnika s ciljem prikupljanja informacija i podataka. Špijunski softver se razlikuje od i virusa ili crva je u tome što špijunski softver nema mogućnost repliciranja (CERT, 2018). Iako se ne mogu replicirati, mogu nanijeti korisniku mnogo veću štetu no što to mogu virusi ili crvi. Upravo zbog neozbiljnog shvaćanja razmjera štete koje spyware može prouzročiti, korisnici najčešće sami pristupaju preuzimanju nelegitimnih programa koji u sklopu instalacije nekog programa računalo zaraze spywareom. ISpyware ima mogućnost preusmjeravanja korisnika na proizvoljne stranice, preuzimanje oglasa (eng. Adware), mijenjanje mrežnih postavka računala, otežavanje mrežnog pristupa i sl. (Dulčić 2007.) Kada se Spyware program

pokrene na računalu može aktivno pratiti korisničke aktivnosti kao što je npr. Unos podataka u neku vrstu forme integrirane u sklopu legitimni ili nelegitimne Internet stranice. Najčešći slučaj zaraze događa se prilikom posjete stranica s ilegalnim pornografskim sadržajem koje sadrže zlonamjeran kod koji koristi sigurnosne propuste. Distributeri Spyware zloćudnog programa ga najčešće predstavljaju kao koristan i uslužan program koji se, nakon pokretanja instalacije od strane korisnika, instalira u sklopu legitimnog programa kojeg je korisnik preuzeo (CERT 2009). Iako određeni antivirusni programi nude zaštitu od spyware ugrađenu u sklopu antivirusne zaštite, u svijetu postoje i brojni proizvođači samostalnih anti-spyware programa (CERT, 2018). Treba imati na umu da postoje i lažni anti-spyware programi, odnosno programi koji se predstavljaju kao legitimni programi koji služe blokiranju i uklanjanju spyware, no u stvarnosti su oni sami spyware, a možemo ih podijeliti u dvije skupine (CERT 2009):

- legalni spyware programi (eng. *Domestic spyware*)

  Npr. Praćenje rada zaposlenika, nadzor djece i maloljetnika prilikom korištenja Interneta i sl.

- komercijalni spyware programi (eng. *Commercial spyware*) – ilegalni zlonamjerni programi.

Tvrtke ih koriste za prikupljanje informacija io navikama i interesima korisnika kako bi ih kasnije prodali trećim zainteresiranim stranama koji će koristiti podatke kako za prikaz raznih oglasnih i reklamnih sadržaja Spyware programe je također moguće razvrstati prema namjeni, i to u sljedeće kategorije:

• Internet URL zapisivači (eng. *Internet URL Loggers*),

  Bilježe web adrese koje korisnik posjećuje. Postavljaju se na tvrdi disk računala te neprekinuto rade tijekom povezanosti na Internet bez obzira koji Internet preglednik potencijalna žrtva koristi.

• snimači zaslona (eng. Screen Recorders)

  Omogućuju praćenje aktivnosti korisnika u obliku snimke zaslona.(eng. Screenshot). Ova vrsta programa je iznimno opasna jer može snimiti svaku korisnikovu radnju na računalu.

• snimači poruka e-pošte (eng. e-mail Recorders)

Nadgledaju i bilježe podatke vezane uz elektroničku poštu. Oni aktivnosti zapisuju u datoteke te ih šalju na unaprijed definirano odredište.

• zapisivači razgovora (eng. Chat Loggers)

Programi koji zapisuju svaku vrstu razgovora vođenu putem programa za razmjenu poruka (eng. Instant Messaging) poput Windows Live Messenger, Google Chat, AOL Messenger, itd.

• zapisivači tipki (eng. Keyloggers)

Izrazitu opasnost za korisnike jer bilježe svaku pritisnutu tipku na tipkovnici.

• snimači lozinki (eng. Password Recorders)

Snimači lozinki ciljano nadgledaju i bilježe samo pritisnute tipke pri upisu iste u polje za lozinku

• kolačići za praćenje (eng. *Tracking Cookies*)

Kolačići u računalnom svijetu označavaju podatke koje web preglednik pohranjuje. Preglednici preuzimaju određene podatke kako bi poboljšali korisničko iskustvo prilikom pregleda određene stranice te je upravo iz tih podataka moguće preuzeti podatke o vremenu, datumu, lokaciji posjeta i slično. Iako se smatra ilegalnom radnjom, ovu metodu najčešće koriste marketinške tvrtke ne bi li doznali navike korisnika te im plasirali reklamni sadržaj ovisno korisnikovim navikama i interesima. …"Ilegalna aktivnost praćenja korisničke aktivnosti se najčešće izvodi putem kolačića dobivenih od treće strane (eng. third party cookies). Naime, neke web stranice mogu sadržavati tekst, slikovne datoteke ili bilo koje druge medije koji nisu smješteni na istom poslužitelju kao i web stranica. Pri preuzimanju medija s nekog drugog poslužitelja, različitog od onog na kojem se nalazi tražena web stranica, web preglednik može također učitati kolačiće s tog poslužitelja. Upravo takvi kolačići su oni dobiveni od treće strane i marketinške tvrtke ih koriste za stvaranje profila korisnika kako bi bile u stanju ciljanim korisnicima prikazati određene elektroničke reklamne materijale".

• otimači web preglednika (eng. *Browser Hijackers*)

Ovi programi prilikom zaraze mijenjaju početnu stranicu i pretraživač korisnika ne bi li ga preusmjerili na stranice trećih strana s ciljem stjecanja financijske koristi od prikazivanja reklamnog sadržaja.

• otimači veze - dialer programi (eng. Modem Hijackers)

Ovi programi su učinkoviti isključivo pri povezivanju računala putem dial-up veze, tj. Izravnim spajanjem telefonske žice u računalo. Oni pokušavaju uspostaviti vezu Internetom putem brojeva sa skupim tarifama. Pojavom širokopojasnog Interneta onemogućeno je djelovanje ovih programa.

• otimači računala (eng. PC Hijackers).

Otimači računala preuzimaju nadzor nad računalom korisnika. Programi imaju sposobnost korištenja računala korisnika za slanje neželjene pošte na ciljane elektroničke adrese s ciljem izvršenja nezakonite radnje. Žrtve ne primjećuju da se putem njihovog računala izvršavaju radnje. Posljedice mogu biti od isključenja usluge od strane operatera, primjena zakonskih mjera ili krađa identiteta obzirom da takvi programi imaju mogućnost udaljene kontrole nad računalom žrtve. Napadač zarazom tuđeg računala dobiva sve administratorske ovlasti te pristup dokumentima žrtve što otvara mogućnost jednostavnijoj krađi identiteta (PC chip, 2016)

2.5. Usporedba zlonamjernih programa

U Tabeli 1. prikazane su glavne karakteristike prema vrsti malicioznog programa,. Sve navedene vrste malicioznih programa imaju sposobnost prouzročiti štetu za pojedinca, tvrtku ili instituciju na način da (CARNet, 2009):

- utječu na pouzdanost podataka (virus, crv, trojanski konj)
- otvaraju mogućnosti drugim malicioznim programima da zaraze računalo (crv i trojanski konj)
- unište podatke (virus i crv)
- ukradu podatke (spyware, crv i trojanski konj) ili nadgledati aktivnostima računalu (spyware i trojanski konj)

Računalni crv je potencijalno najopasnija prijetnja jer da utječe na pouzdanost podataka, otvara mogućnost druge vrste napada, ima mogućnost izvršavanja DDoS i MITM napada te može ukrasti ili uništiti naše podatke.

Prema Nacionalnom Certu (2008), izraz DoS (eng. Denial of Service) označava …*napad uskraćivanja usluga. Takav napad karakterizira namjerno generiranje velike količine mrežnog prometa da bi se zasitili mrežni resursi i poslužitelji. Zbog prevelikog opterećenja oni više nisu u stanju pružati namijenjene usluge. Posljedica toga je nemogućnost legitimnih korisnika da koriste mrežne usluge poput: e-mail, weba i sl.* Izraz DDoS (eng. Distributed Denial of Service) označava *...oblik napada uskraćivanjem usluga u kojem su izvori mrežnog prometa (napada) distribuirani na više mjesta diljem Interneta. Ta računala iz kojih se obavlja napad nisu u vlasništvu napadača, već neka žrtva koja u pravilu i nije svjesna da se njeno računalo koristi za napade protiv drugih računala i sustava. Najčešće se radi o računalima koja sadrže neku ranjivost što omogućuje napadaču razbijanje sustava zaštite te širenje zlonamjernog koda. Nakon toga računalo je u vlasti napadača koji jednom naredbom pokreće DDoS napad s mnogih provaljenih računala na ciljano računalo. Postoje razni alati koji omogućavaju automatizirano izvođenje napada, ali i alati koji služe u svrhu zaštite od takvih napada.*

	Spyware	**Virusi**	**Crvi**	**Trojanski konji**
Rezidentnost u radnoj mermoriji	Ne	Da / Ne	Da	Ne
Mogućnost replikacije	Ne	Da	Da	Ne
Zapisivanje na tvrdi disk	Da	Da	Ne	Da
Razina rizika	Visoka	Srednje visoka	Visoka	Visoka
Primjetnost pristunosti na računalu	Da	Da	Ne	Ne
Izvori zaraze	Internet	Internet, prijenosni mediji	Internet	Internet
Učinak na normalan rad računala	Da	Da	Da / Ne	Da / Ne
Utjecaj na pouzdanost podataka na računalu	Ne	Da	Da	Da
Otvaranje mogućnosti za drugu vrstu napada	Ne	Ne	Da	Da
Mogući napadi	-	-	DDos, MITM	DDoS, MITM
Opasnost od uništavanja podataka	Ne	Da	Da	Ne
Opasnost od krađe podataka	Da	Ne	Da	Da
Nadgledanje aktivnosti na računalu	Da	Ne	Ne	Da

Tablica 2.1 Usporedba malicioznih programa

3. Socijalni inženjering

Socijalni inženjering nije izravan tip proboja informacijske sigurnosti, već je metoda indirektnog pristupa gdje napadač kao vjerodostojna i povjerljiva strana navodi korisnike da predaju vjerodostojnice, odnosno provjerljive informacije, lozinke ili osobne podatke (CERT 2010)

- Prijevarom
- Upadom u mrežu
- Industrijskom špijunažom
- Krađom identiteta
- Narušavanjem sustava ili mreže

Socijalni inženjering napadi mogu biti usmjerene na osobe (zasnivaju se na međuljudskim vezama i prijevarama uz uporabu zastrašivanja) ili preko računala / tehnologija gdje se napadi odvijaju iskorištavanjem ranjivosti u sustavu (npr. Pop-up prozori koji zahtijevaju unos osobnih podataka) (CERT, 2010) U kategoriju *Crimwera* spadaju i programi koji se koriste u napadima socijalnog inženjeringa (Grubort i Franc, 2010). Prema nacionalnom CERT-u, Socijalni inženjering je *g niz tehnika pomoću kojih pojedinac, iskorištavanjem ljudskih pogrešaka i slabosti, utječe na drugog pojedinca kako bi ga naveo da učini nešto što nije u njegovom interesu. Socijalni se inženjering najčešće koristi u svrhu otkrivanja njihovih povjerljivih informacija ili dobivanja pristupa nekim drugim resursima do kojih napadač inače ne bi mogao doći.* Takve tehnike pomažu probijanju informacijske sigurnosti, a najčešće se koriste ljudske ranjivosti, slabosti ili pogreške kroz ljudske osobine kao što su povjerenje, želja za pomoći ili nemarnost ne bi li prijevarom stekli ne pripadajuću financijsku ili drugu korist.

Socijalni inžinjeri koriste socijalne tehnike za izvršenje svojih napada, a to može više-manje biti bilo tko. Nije nužno da osoba bude tehnički potkovana i poznaje hakerske tehnike kako bi probila sigurnosni sustav. Socijalni inženjer može biti i nezadovoljan zaposlenik koji neovlašteno preuzme podatke. Upravo nepostojanje profila socijalnog inžinjera predstavlja izazov instiucijama, organizacijama i pojedincima u prepoznavanju potencijalnih opasnosti. Kao prilog tvrdnji Nacionalni CERT (2018) prenosi citat Mitnicka i Simona iz knjige *The art of deception: Controlling the human element of security*

„Neka tvrtka je možda kupila najbolje sigurnosne tehnologije koje novac može kupiti, obučila svoje ljude toliko dobro da zaključavaju sve svoje tajne prije vraćanja kući noću i unajmila zaštitare od najboljih sigurnosnih tvrtki. Ta tvrtka je i dalje u potpunosti ranjiva."

CIS je 2012. objavio informaciju da je 70% napada na sustav interne naravi. Tehnike su raznolike, od krađe zapisanih lozinki do izvođenja složenijih scenarija te nisu nužne vezane uz Internet, već se mogu koristiti i u telefonskim pozivima, fizičkom poštom, pa čak i susret napadača s potencijalnom žrtvom. U Svim slučajevima ase napadač predstavlja kao povjerljiva strana.

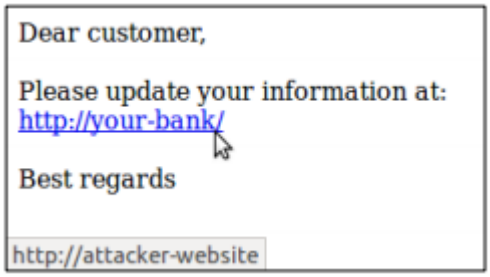
Ciklus socijalnog inženjeringa može biti jednostavniji (npr. krađa osobnih podataka radi daljnje prodaje na crnom tržištu), ili kompleksniji koji uključuje više tehnika, napadača, ali i žrtava. Tehnike socijalnog inženjeringa su tehnike obmane koje omogućuju razvijanje lažnog scenarija (priče) i odnosa sa žrtvom. Kako se socijalni inženjering razvijao paralelno s granama informacijske sigurnosti, tehnike socijalnog inženjeringa su često usko povezane s tehnikama napada na računalne sustave, fizičku sigurnost i slično. Za razliku od ostalih tehnika, tehnike socijalnog inženjeringa nije moguće nabrojati obzirom da je njegova suština prijevara ljudi (CERT, 2017.), a nove se tehnike stvaraju i postojeće prilagođavaju društvenim i socijalnim promjenama u društvu te psihološkom profilu žrtve (ovisno o kvaliteti podataka i informacija koje je napadač stekao). Lažni identitet je prvi bitan korak jer je da bi scenarij uspio i žrtva bila prevarena, neophodno je postići povjerljiv odnos sa žrtvom, a to je moguće samo ukoliko žrtva napadača percipira kao povjerljivu stranu. Lažno predstavljanje mijenja se ovisno o metodi komunikacije s potencijalnom žrtvom (elektronička pošta, email, telefon, licem u lice, SMS, telefaks, pošta…), a niti jedna metoda komunikacije ne može garantirati vjerodostojnost. U svim načinima komunikacije moguće je lažirati identitet (promjena pošiljatelja kod elektroničke pošte ili pošte, telefonski broj, osobna iskaznica, vizitka), pa čak i kod komunikacije licem u lice gdje se napadač može lažno predstaviti. Najčešći primjer obmane u komunikaciji licem u lice je prilikom kupnje ili prodaje putem Internet oglasnika (lažna imena kod prodaje ukradene robe). Socijalni inžinjeri u pravilu izbjegavaju komunikaciju licem u lice te preferiraju elektroničku komunikaciju koju svi svakodnevno koristimo (CERT, 2'017), a s druge strane digitalni način komunikacije omogućuje lakši pristup većem broju ljudi, odnosno mogućnost više pojedinačnih napada, testiranja lažnih profila i scenarija i slično. Osim lažnog identiteta, napadi koriste druge razne tehnike kako bi lažna priča bila što uvjerljivij, a informacije korištene prilikom napada mogu biti tražene od strane žrtve ili referencirane od strane

napadača. Jedna od najkorištenijih vrsta napada je *Phishing* (varijanta engleske riječi za pecanje, *engl. Fishing).* To je vrsta socijalnog inženjeringa koja se odnosi na prijevare kojima se služe zlonamjerni korisnici šaljući lažne poruke putem postojećih internet servisa.. Kriminalci od korisnika pokušavaju prikupiti povjerljive podatke (korisnička imena, lozinke, podaci s kreditnih kartica i sl.) putem raznih načina manipulacije kako bi ostvarili kriminalne radnje, najčešće ostvarivanje financijske koristi. U pravilu se velika većina phishing napada odvija putem elektroničke pošte obmanjivanjem mete da preuzme i pokrene zlonamjerni program), no razvoj kompleksnosti napada i razvojem tehnologija napadači sve češće koriste i druge tehnologije kao što su programi i aplikacije za trenutnu komunikaciiu (Whatsapp, Viber, Snapchat, Skype…) te SMS (engl. *Short messaging servise*) u mobilnoj telefoniji. U CERTu upozoravaju na posebnu vrstu phisinga tzv. spearphishing (od eng. spearfishing – lov riba kopljem). Obične phishing poruke šalju se na velik broj email adresa i nisu personalizirane, odnosno prilagođene meti. Zbog mnoštva profila ljudi koji se kriju iza tisuća email adresa, takve su poruke jednostavne i mnogima sumnjive već na prvi pogled. Napadači ih šalju u dani da će iz pogleda sigurnosti i korištenja Interneta, slabije obrazovani korisnici pratiti upute dati podataka ili preuzeti i pokrenuti maliciozni program.. S druge strane Spearphishing (kombinacija engl riječi Spear – koplje i Fishing – pecanje), je napad koji cilja točno određenu osobu ili organizaciju. *Takva se* poruka se najčešće ne ističe značajno od brojnih drugih poruka koje je meta primila, dok su napadi prilagođeni meti na način da je napadač naizgled osoba s kojom meta često komunicira, adresa naizgled poznata sa sadržajem koji odgovara kontekstu i sadrži detalje specifične za korisnika imaju mnogo veću šansu za uspjeh. Valja imati na umu da takvi napadi zahtijevaju mnogo pripreme zbog čega je *Spearphising* moguće samo jedan ciklus kompleksnijeg napada. Nacionalni CERT (2018) navodi *... da je spearphishing jedna od najvećih prijetnja sigurnosti organizacija danas! (CERT, 2018).*

Kako se tehnike socijalnog inženjeringa i napada na računalne sustave mijenjaju promjenom i razvojem ljudskih navika, socijalnih normi, navika i informacijske sigurnosti, tako se i phishing tehnike konstantno mijenjaju i razvijaju, odnosno personaliziraju i prilagođavaju potencijalnoj meti. Iz navedenog nije moguće precizno definirati niti nabrojati sve tehnike phishinga, no prepoznajemo određene tehnike koje čine bazu phishing napada. Phishing napad može sadržavati jednu ili više naprednih tehnika (CERT, 2018), a ključna je uvjerljivost poruke jer bez uvjerljive poruke nema uspješnog napada stoga se napadači predstavljaju kao postojeće ili nepostojeće osobe, institucije ili organizacije. Predstavljanje

kao povjerljiva strana nije pitanje tehničkog znanja već vremena, odnosno resursa koje će napadač uložiti. Kombinacijom tehnika socijalnog inženjeringa, elektroničke pošte te raznih internetskih tehnologija daju nebrojene mogućnosti napadaču da malicioznim programom zaraze računalo žrtve. Tako napadač može npr. Registrirati domenu sličnu domeni tvrtke i kontaktirati metu elektroničkom poštom. (ako se napadač lažno predstavlja kao tvrtka). Paypal, može poslati poruku s adresa kao što su paypal@gmail.com, support@paypal.napadačevadomena.com i slično), napraviti lažnu web stranicu npr., Paypal tvrtke ili napraviti kopiju web stranice na drugoj domeni, profil tvrtke na društvenim mrežama i slično. Uvjerljivosti priče ide u prilog i detaljna priprema lažne priče (engl. *Pretex*), spominjanje relevantnih imena (engl. *Name dropping*), organizacije, korištenje primjerenog žargona, obraćanje nagrade ili prijetnju kaznu zbog npr. Lažnog problema s računalom) i slično. Ukoliko napadač kontaktira metu i jasno otkrije svoj identitet, onda nije više riječ o phishingu već socijalnom inžinjerignu (kod npr. ucjena) Napadači će ili pokušati uvjeriti mete da posjete neku odredišnu web stranicu ili će napraviti lažnu kopiju stranice (obično je domena lažne stranice slična nazivu kopirane stranice).

Na primjeru (Slika 1) vidljivo je da se iz perspektive mete u tekstu nalazi naizgled poveznica web stranice banke, dok se u statusnoj traci prikazuje stvarno odredište



Slika 3.1 Sakrivanje odredišta

Drugi način je korištenje servisa za skraćivanje URL-a koji su dostupni na Internetu i besplatni, npr. Bit.ly, tinyurl.com i sl. Ovdje valja izdvojiti potencijalno najopasniju prijetnju, tzv. Ranjivost otvorenog preusmjeravanja. Ovdje napadač koristi ranjivost web stranica koji omogućava prikrivanje URL-a na način da pošalje meti poveznicu, npr: http://example.com/?redirect=<napadačev URL> koja u konačnici preusmjerava metu na napadačev URL. Ovu prijetnju je tim više teže za otkriti jer dio URL-a http://example.com/ na prvu daje korisniku za zaključiti da se radi o vjerodostojnom odredištu Napadač kod napada malicioznim programima meti predstavlja maliciozni program kao povjerljivu i istinitu datoteku , program ili aplikaciju (npr. račun, ugovor, slika, program za pregledavanje

fotografija, poruka i sl.), koji se obično nalazi u privitku elektroničke poruke. Napadač se može poslužiti brojnim informacijama i podacima koje korisnici Intertneta javno objavljuju. Jedan od slučajeva potencijalne opasnosti web portala je korištene aplikacije koja omogućuje registraciju i prijavu korisnika putem Facebook profila. Portali koriste ovu metodu jer je Facebook u Hrvatskoj najkorištenija društvena mreža s preko 2.000.000 aktivnih korisnika (Arbona, 2018)

Što više informacija napadač posjeduje o potencijalnoj žrtvi, to će lakše prilagoditi scenarij i povećati izglede uspješnosti napada. Mnogi korisnici Facebooka su tehnički nedovoljno obučeni ili nedovoljno educirani o potencijalnim opasnostima. Stoga ne čudi što velik broj korisnika javno objavljuje podatke koji bi mogli biti korišteni za izvođenje napada (npr. Datum rođenja, imena djece ili email adresa). Napadač tako može na email adresu poslati elektroničku poruku prilagođenu interesima koje je žrtva javno objavila. Životni ciklus phishing napada putem Faceooka odvija se kao i napada putem elektroničke pošte – napadač korisniku pošalje poveznicu koja rezultira zarazom računala žrtve malicioznim programom te se nastavlja širiti. (CARNet 2013). Da bi socijalni inženjering bio uspješan nije potrebno da žrtva uopće sudjeluje u procesu direktno na način da poduzima određene akcije i korake prema uputama napadača. Svi upisani podaci u bilo koju formu za registraciju ili prijavu ostaju zapisani na nekom serveru. Takvi podaci dostupni su napadačima bez obzira sudjeluje li potencijalna žrtva. Masovni podaci kasnije se mogu prodavati na crnom tržištu, ali i koristiti za ciljane napade.

4. Statistika incidenata

Gotovo sva kaznena djela u sebi „posjeduju“ neki digitalni uređaj. FBI navodi kako u 85% svih kriminalističkih istraživanja pojavljuje digitalni dokaz, a u čak 65% slučajeva su ti dokazi ključni (Čosić, 2013). Prema istraživanju provedenom od strane Symanteca (2017), u 2016. godini zabilježeno je 1.209.000 napada, od čega je 15 napada zabilježenih koji su doveli do otkrivanja ili krađe više od 10.000.000 korisnika. Ukupno je otkriveno ili ukradeno 1,1 milijarda identiteta ukupno, odnosno 927.000 prosječno prema napadu. U zadnjih 8 godina je ukradeno ili otkriveno više od sedam milijardi identiteta. Globalno se % neželjene pošte (*Spama*) smanjuje, od 60% u 2014 na 53% u 2016. Zanimljiv je trend smanjenja kritičnih napada na web stranice. Prema istom istraživanju kod 76% svih skeniranih stranica zabilježene tu ranjivosti, no kritične ranjivosti u 2014. čine 20%, u 2015. 15% i u 2016 9% od svih pronađenih ranjivosti. Pozitivan trend prati i smanjenje broja zabilježenih napada na web servise dnevno, s 340.000 dnevno u 2015. na 229.000 u 2016. Ono što predstavlja izazov naporima institucija i antivirusnih programa jest razvoj novih malicioznih programa. Institut AV-test svakodnevno registrira preko 350.000 novih malicioznih programa. Eksponencijalan rast potvrđuje i rast broja zabilježenih malicioznih programa s 29 milijuna u 2009. na 719 milijuna u 2017. (AV-TEST, 2018).

Na razini Europske unije kibernetički kriminal doseže do 20% ukupnog broja kaznenih dijela i može se očekivati da će s vremenom postati dominantni oblik kriminalnih radnji. Po broju pretrpljenih napada u 2017. godini prednjači industrija s 24,8%, državne institucije s 11,9% te privatne osobe s 9,3% (Tportal, 2017).

IBM je objavio istraživanje u kojem se navodi da je broj phishing napada i spamova u 2017. godini porastao četiri puta u odnosu na 2016.. Stručnjaci iz IBM—a procjenjuju da će se trend rasta nastaviti i u 2018. godini (Telegram, 2017.).

U svijetu postoje brojne nacionalne i nezavisne institucije koje se bave bilježenjem kriminalnih radnji, a u Hrvatskoj je mjerodavan Nacionalni CERT. U svom godišnjem izvještaju za 2017. godinu (2018) navode kako su zabilježili i obradili 732 prijave u nadležnosti od čega su vodeći tipovi kompromitirano web sjedište (eng. Web defacement) s izmjenjenom početnom stranicom, phishing URL i phishing (tablica 2). Iako broj zabilježenih phishing napada na godišnjoj razini pada u Hrvatskoj je bilježimo porast trenda. U CERTU smatraju da je rezultat rasta broja phishing incidenata u Hrvatskoj nekoliko

phishing kampanja koje su ciljane korisnike u Hrvatskoj. Uspješnost kampanja je potpomogla dobra prilagodba na Hrvatski jezik , a u većini napada se napadač predstavljao kao osoba nadređena žrtvi.

Prema izvješću MUP-a u godišnjem pregledu za 2016. godinu navode ukupno prijavljenih kaznenih djela protiv računalnih sustava, programa i podataka 1.553 od kojih je 1396 razriješeno s jednom uhićenom osobom.

Tip incidenta	**Broj**	**Trend**
Web defacemenet	370	Rast
Phishing URL	127	Pad
Phishing	59	Rast
Malware URL	42	Pad
Spam	29	Rast
Nedozvoljena mrežna aktivnost	28	Rast
Spam URL	26	Rast
Bot	20	Rast
Ostale vrste napada i zlouporabe	12	Rast
DoS	10	Pad
Malware domain	4	Rast
Ostala kompromitirana računala	3	Pad
C&C	2	-
UKUPNO	**732**	**Rast**

Tablica 4.1 Prijave prema tipu incidenta

5. Analiza potencijalnih opasnosti web portala u Hrvatskoj – empirijsko istraživanje

Predmet ovog istraživanja su propusti na web portalima u Republici Hrvatskoj koji mogu dovesti do napada malicioznim programima

5.1. Metodologija istraživanja

Empirijsko istraživanje propusta na web stranicama u Republici Hrvatskoj provedeno je u razdoblju od u razdoblju od 01.08.2018. do 10.08.2018. putem Internetskog preglednika Google Chrome. U istraživanju je primijenjena metoda analize sadržaja kao subjektivna interpretacija mogućih propusta od strane sustava, administratora ili autora. U pregledu će biti i navedeni propusti koje ne možemo definirati kao maliciozni program (tehnike socijalnog inženjeringa), no zbog sve veće kompleksnosti u izvođenju prijevara biti će spomenute jer uvijek postoji mogućnost da se radi o samo jednoj fazi u ciklusu napada.

Prema Leksikografskom zavodu Miroslava Krleže, web ili mrežni portal je *mrežno mjesto koje raznovrsnim sadržajima, najsvježijim informacijama, naprednim mogućnostima i mnogobrojnim poveznicama nudi širokomu krugu korisnika ishodišno mjesto na webu. Može biti općeg usmjerenja (vijesti, tematske rubrike, gradski vodiči) te posebnog usmjerenja (znanstveni, obrazovni, enciklopedijski i drugi portali). Najčešće ga uređuje stalno uredništvo, pa nalikuje elektroničkomu časopisu, a vode ga medijske kuće, davatelji internetskih usluga i sl. Obično se financira iznajmljivanjem oglasnoga prostora (reklamna zastavica – engl. banner, iskočni prozor – engl. pop-up window) ili drugim oblikom mrežnog oglašavanja.* U Hrvatskoj je zabilježen 1121 web portal (Svi portali, 2018).

Reuters u svom istraživanju (2018) navodi listu najčitanijih web portala (Tablica u Hrvatskoj prema kriteriju broj otvaranja od strane jedinstvenih korisnika unutar razdoblja od 7 dana)

Redni broj	Naziv	Postotak
1.	Index.hr	57 %
2.	24sata.hr	55 %
3.	Jutarnji.hr	45 %
4.	Net.hr	42 %
5.	TPortal.hr	40 %
6.	Dnevnik.hr	38 %
7.	Vecernji.hr	35 %
8.	HRT.hr	23 %

Tablica 5.1 Najčitaniji web portali u Hrvatskoj

Pregled stranica uključuje i analizu stranica putem besplatnog online alata Virus Total. Ovaj online skener Google preporuča na svom portalu https://safebrowsing.google.com/ koji sadrže najvažnije smjernice i preporuke za zaštitu korisnika. Također valja spomenuti da je Google i preuzeo vlasništvo nad alatom (Techcrunch, 2012).

Svi navedeni portali označeni su kao sigurni od strane Virus Totala te niti u jednom članku nije uočena potencijalno maliciozna poveznica u tekstu autora.

5.2. Potencijalne opasnosti

5.1.1. Obavijest o kolačićima i dostupne informacije o prikupljanju podataka

Kada se radi o pouzdanim mrežnim mjestima kao što su navedeni portali, korisnici mogu biti sigurni da kolačići neće biti korišteni u svrhu malicioznih napada već optimizaciji korisničkog iskustva. Kolačići su male tekstualne datoteke koje se pohranjuju na računalo ili mobitel prilikom posjete određenom web mjestu. Putem njih web mjesto pamti naše radnje koje se odnose na postavke prikaza i načinu korištenja, različite statističke podatke o lokaciji s koje posjetitelj dolazi, razne statističke podatke o broju otvaranja i korištenju mrežnog mjesta, odluku o prihvaćanju kolačića i slično. Oni mogu prikupljati i osobne podatke, no tek nakon što ih korisnik da na raspolaganjem putem neke forme. OD vrsta kolačića razlikujemo (Adriamedia, 2018).

1. Privremene kolačiće (sesije) uklanjaju se s računala po zatvaranju preglednika, a služe pohrani privremenih podataka (npr. Stavke u košarici kod Internet trgovina ili unesene podatke u formu prilikom registracije)
2. Stalne kolačiće (spremljene) koji ostaju na računalu i nakon zatvaranja preglednika. To mogu biti npr. podaci za prijavu koji olakšavaju i ubrzavaju prijavu korisnika na razne servise. Mogu biti spremljeni neodređeno dugo vremena.
3. Kolačići prve strane koji dolaze s web mjesta koje se pregledava. Mogu biti privremeni i stalni.
4. Kolačići trećih strana koji dolaze sa trećih web lokacija, a čiji kod poziva mjesto koje korisnik gleda. Najčešće se koriste u marketinške svrhe kako bi korisniku plasirali relevantan oglas temeljem navika korištenja, odnosno podataka zabilježenih na prethodnim stranicama.

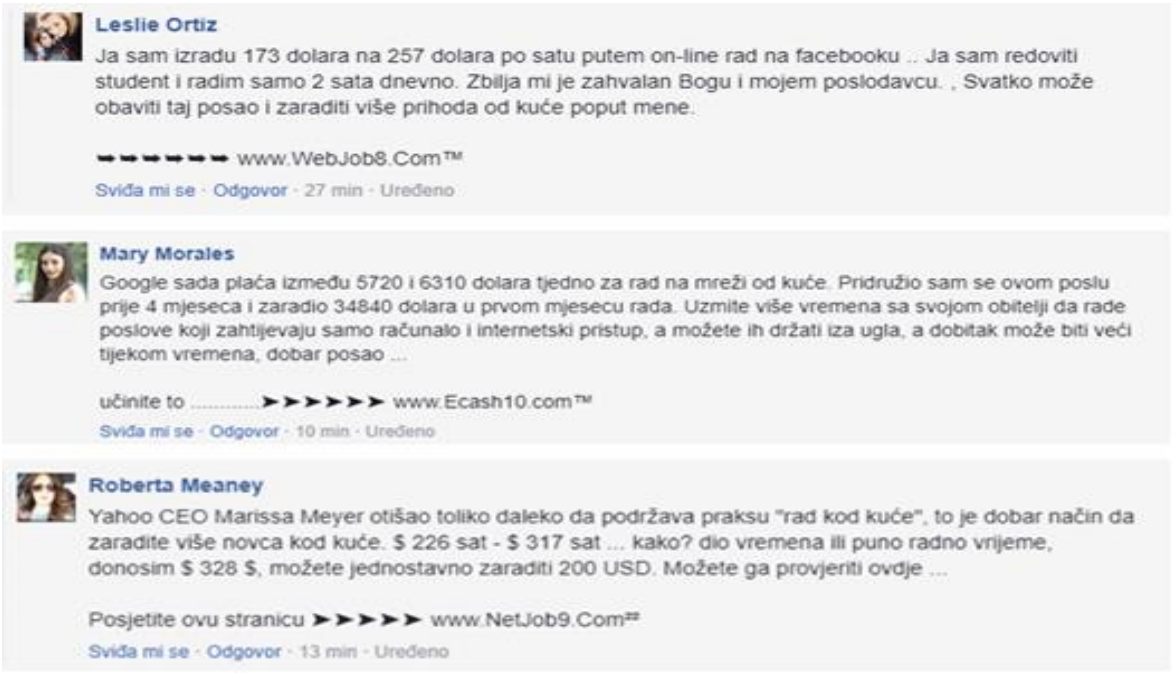
Ono što je važno je jasna i razumljiva obavijest korisniku o vrsti podataka koji se prikupljaju te informacije i dijeljenju navedenih podataka trećim stranama kako bi korisnik samostalno mogao donijeti odluku o nastavku korištenja portala. Svi navedeni portali prilikom posjeta prikazuju jasnu obavijest o korištenju kolačića, no određeni portali u uvjetima korištenja nemaju jasno naznačeno o kojim se kolačićima i servisima trećih strana radi. Iako obavijest o kolačićima nije direktno vezana uz maliciozne programe, krađa podataka registriranih korisnika web portala direktno od portala ili trećih strana može dovesti do napada malicioznim programom u slučaju kompleksnijeg ciklusa socijalnog inženjeringa. Jutarnji.hr i Net.hr su jedini promatrani portali koji imaju jasno naznačen proces postupanja s podacima i uključenost trećih strana.

Problem koji može nastati iz prihvaćanja određenih kolačića je učestalo uznemiravanje u marketinške svrhe od strane portala 24sata.hr, odnosno njihovih klijenata i partnera jer, kako navode:*... vaše osobne podatke učinimo dostupnima i drugim društvima unutar Styria Media Grupe i klijentima, a sve s ciljem ispunjenja svrhe za koju su navedeni osobni podaci prikupljeni.* Primjer može biti periodični pozivi za pretplatu na 24sata, Jutarnji.hr ili neki drugi portal iz grupacije, kao i druge usluge.

5.1.2. Maliciozne poveznice u komentarima

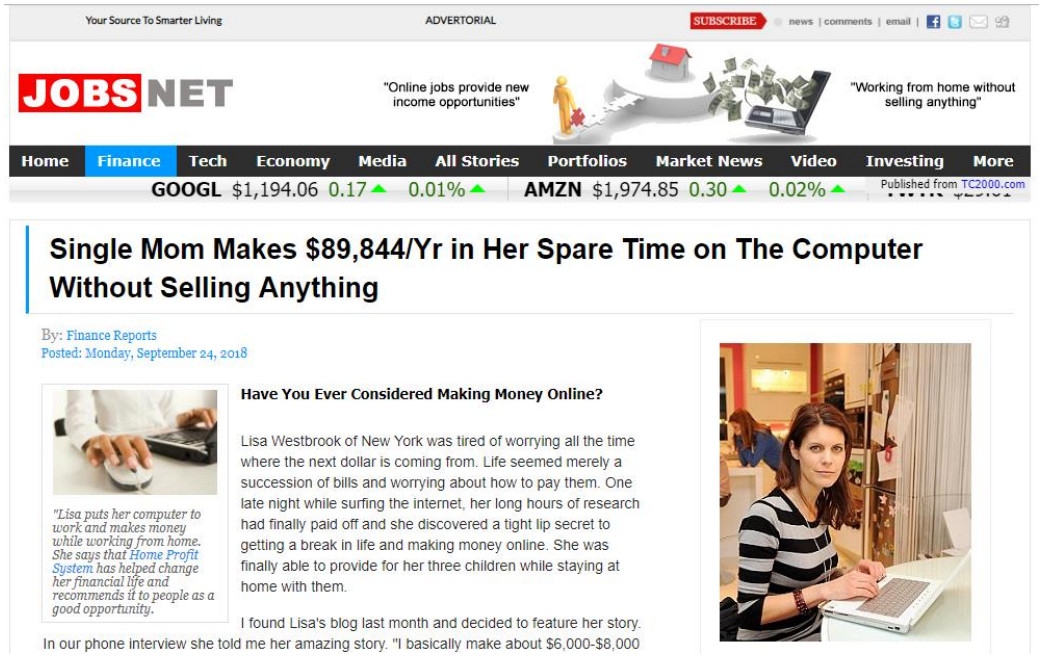
Od promatranih portala, mogućnost komentiranja imaju portali Jutarnji Online, Net.hr, Index.hr, 24sata.hr dok Tportal, Dnevnik.hr, Večernji online te hrt.hr nemaju tu mogućnost. Maliciozne poveznice uočene su na portalima Index.hr, 24sata.hr i Net.hr u promatranom razdoblju.

Pouzdani portali neće sadržavati poveznice na sumnjiva odredišna mjesta obzirom da sami autori prilikom unosa poveznice provjeravaju izvor podataka, a i većina informacija se preuzima iz pouzdanih izvora. Problem mogu stvarati fizičke osobe ili umjetna inteligencija koja ima mogućnost masovnog plasiranja malicioznih reklama na različitim platformama Iako postoje različite tehničke zaštite koje vlasnika domene štite od tzv. Spam Botova – kompjuterskih programa namijenjenih registraciji na stranici i ostavljaju generičkih poruka putem komentara koji pozivaju korisnika da posjeti zaraženu web lokaciju (Slika 5.1) nije moguće spriječiti spamove u komentarima ukoliko napadač napravi lažni facebook profil ili registraciju putem email računa te ručno zalijepi tekst u komentar. Spam koji je objavljen u komentarima ručno, ne automatski i generički, moguće je kontrolirati kontinuiranim pregledima objavljenih komentara i ručnim brisanjem. Takvi komentari bivaju vidljivi sve do trenutka dok ga administrator ručno ne obriše, te kao takav može oštetiti veći broj korisnika. Neke poveznice trećih strana imaju za cilj zaraziti računalo dok druge predstavljaju jednu od faza u ciklusu socijalnog inženjeringa zbog čega nisu registrirane kao nesigurne od strane niti jedne umjetne inteligencije. Ovaj problem je izražen ukoliko se radi o prodaji „čudotvornih“ lijekova po sniženim cijenama.



Slika 5.1 Primjeri malicioznih komentara

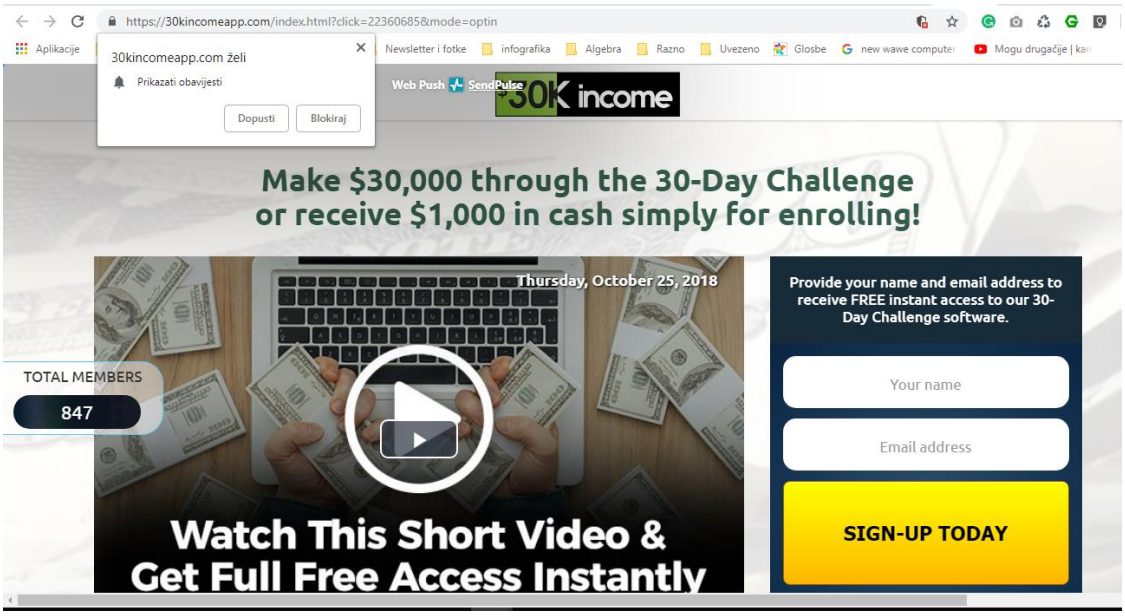
Kada korisnik unese adresu jednu od navedenih Internet adresa u preglednik preusmjeren je na domenu http://jobs.net-careers.info/?bo0763 (Slika 5.2).



Slika 5.2 Phishing domena

Virus total ocijenio je ovu stranicu nesigurnom zbog mogućnosti Phishinga.

Odabiru bilo koje stavke glavnog izbornika stranice (Slika 5.2), korisnik je preusmjeren na web stranicu https://30kincomeapp.com/index.html?click=22360685&mode=optin (Slika 4.), koja poziva na akciju korisnika obećavajući sigurnu zaradu uz davanje informacija kao što su email adresa i broj telefona (Slika 5.3).



Slika 5.3 Forma za unos podataka

Virus Total ovu stranicu nije označio kao nesigurnu.

Naknadnom kontrolom zabilježene su maliciozne poveznice u komentarima koje su zaobišle tehničku i ljudsku provjeru te nisu uklonjene više tjedana

Iako su maliciozni komentari u većini zabilježenih slučajeva obrisani u kratkom roku (do 15 minuta), postoje iznimke gdje je maliciozni komentar ostao neobrisan (Slika 5.1), odnosno javna, dulje od 10 tjedana, tj. do završetka pisanja ovog rada.

Slika 5.4 Komentar koji nije uklonjen

Odabirom bilo koje poveznice u komentaru potencijalna žrtva preusmjerena je na mrežnu stranicu https://pokermania1.com/id/poker. Radi se o stranici koja se izvorno prikazuje na Indonezijskom s mogućnošću odabira Engleskog jezika, a poziva posjetitelje da sudjeluju na turniru u Pokeru koji ima bogat nagradni fond (Slika 5.4.) Iako stranica prilikom registracije traži osjetljive podatke o računima i banki korisnika (Slika 5.5.) sve ponuđene banke su nepoznate Europskom tržištu pa je malo vjerojatno da će osoba koja je stigla preko poveznice u komentaru neobjavljene na hrvatskom portalu namijenjenom hrvatskom govornom području pratiti upute, tim više što je potrebno odabrati jednu od Indonezijskih banaka prilikom registraciju.. Zabrinjavajuće je što nigdje ne postoji niti jedan podatak o fizičkoj i pravnoj osobi koja kroz mrežnu stranicu pruža uslugu, a poveznica na stranicu Uvjeta korištenja nalazi se samo prilikom registracije te nije ispravna, odnosno korisnika preusmjerava natrag na početnu stranicu. Ovo potvrđuje nemogućnost pro-aktivne borbe protiv različitih vrsta malicioznih napada.

Slika 5.5 Moguća maliciozna stranica koja zahtjeva popunjavanje osobnih podataka

5.2.3. Maliciozne poveznice u oglasima

Maliciozne poveznice u oglasima pronađene su na portalima index.hr i tportal.hr

Potencijalne opasnosti pronađene na web portalima nisu direktno vezane uz preusmjeravanje korisnika na potencijalno opasne mrežne stranice, već su promatrane kao moguć početak kompleksnijeg ciklusa socijalnog inženjeringa koji može u određenom trenutku dovesti do inficiranja računala korisnika malicioznim programom. Tijekom istraživanja su identificirana dva glavna problema

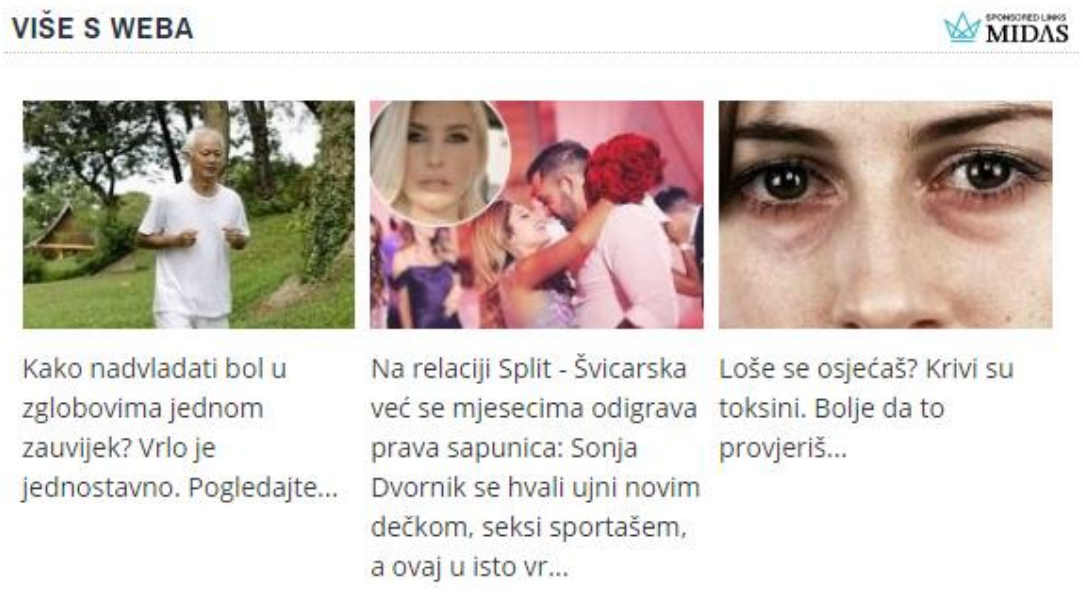
Net.hr, Jutarnji.hr i Tportal.hr u sklopu članaka sadrže listu poveznica na sadržaj trećih strana (Slika 5.). Uredništvo portala nema mogućnost odabira konkretnog sadržaja koji će se prikazivati, već … *se razmjena vrši putem RSS feeda, a sustav pomoću algoritma samostalno definira koji će se sadržaj najbolje čitati na partnerskom portalu i samostalno optimizira proces razmjene prometa.* (Midas, 2018). To znači da će se uz portale koji obrađuju teme vezane uz digitalne tehnologije prikazivati sadržaj drugih portala vezan uz digitalne

tehnologije. Problem nastaje kada se mrežu prikazanim sadržajem pojave stranice koje se lažno oglašavaju, bilo u pogledu prodaje lažnih proizvoda ili prikupljanju podataka za razne lažne nagradne igre.. Oglašavani proizvodni najčešće su vezani uz mršavljenje i druge zdravstvene probleme. Ovako prikupljeni podaci mogu se koristiti za daljnji napad malicioznim programom. Takve stranice u pravilu ne sadrže maliciozne programe, no nemaju protokol kriptiran SSL-om i ne pružaju vjerodostojne informacije o načinu korištenja prikupljenih podataka.

Slika 5.6 Primjer reklama na web portalu

Slika 5.7 "Medicinski“ portal na koje vodi reklama

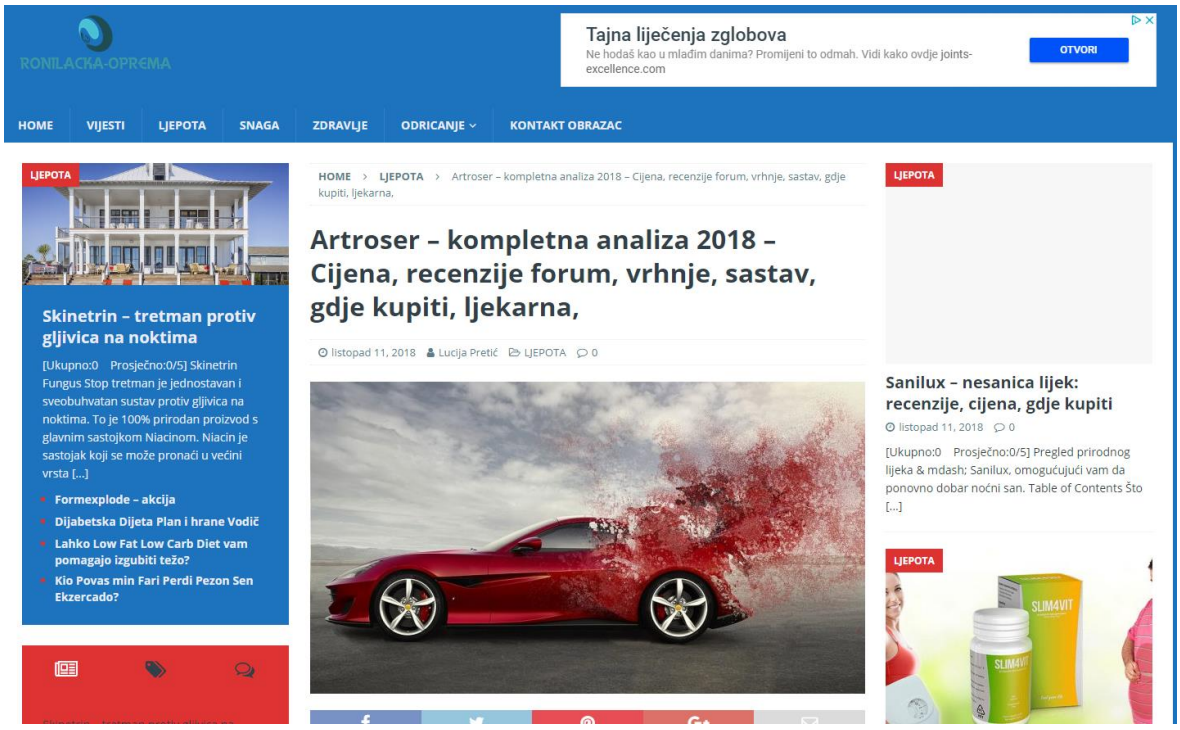
Kad korisnik odabere prvu reklame za tablete za skidanje masnoće (Slika 5.6.), biva preusmjeren na web stranicu (Slika 5.7.) koja se predstavlja kao medicinski portal. Stranica je označena kao sigurna iako traži dopuštenje da obavještava korisnika putem notifikacija što predstavlja potencijalnu opasnost. Obzirom da je prošlo više tjedana od kada je ova poveznica zabilježena do trenutka pregleda, odnosno pokušaja naručivanja proizvoda, odredišna stranica nije zabilježena obzirom da je sustav poveznica na stranicama promijenjen. Takva naknadna provjera poveznice otkrila je da sustav na svim mrežnim adresama koje se više ne koriste za prodaju nekog proizvoda napravljena redirekcija kako bi korisnici koji su kliknuli na poveznicu bili usmjereni na aktivan proizvod koji se prodaju. Ne postoji logična poveznica u sustavu već je preusmjeravanje napravljeno masovno što potvrđuje situacija kada kliknemo da kada korisnik klikne poveznicu da naruči tablete za mršavljenje, bude preusmjeren na odredišnu stranicu tableta za zglobove. Radi se o istoj odredišnoj stranici kojoj je moguće pristupiti putem maliciozne poveznice objavljene na tportalu. Stranica nudi već poznate pozive za ostavljanjem podataka i učlanjenjem u VIP klub i to na način obmane. Kada korisnik klikne poveznicu koja ga navodi da pristupi VIP Klubu, dobiva poruku da je prihvatio da ga stranica redovito obavještava o novim promocijama putem preglednika. Pretpostavka je da će maliciozni program nastojati prikazivati što više malicioznih reklama kroz različite digitalne kanale koje zahtjevaju korištenje preglednika.



Slika 5.8 Primjer reklama na web portalu

Slika 5.9 Portal na koji vodi reklama

Prilikom pokušaja pronalaska više informacija o proizvodu na tražilici Google upisom „Artroses tablete", „Artroser zglobovi" ili „artroser prevara" dobivamo isprepletenu mrežu koje su loše prevedene na Hrvatski te sve više-manje dijele isti dizajn, imaju izmišljene autore i svjedočanstva. Dizajn stranica prati nekoliko modela unutar kojih se mijenjaju boje i logotipovi.



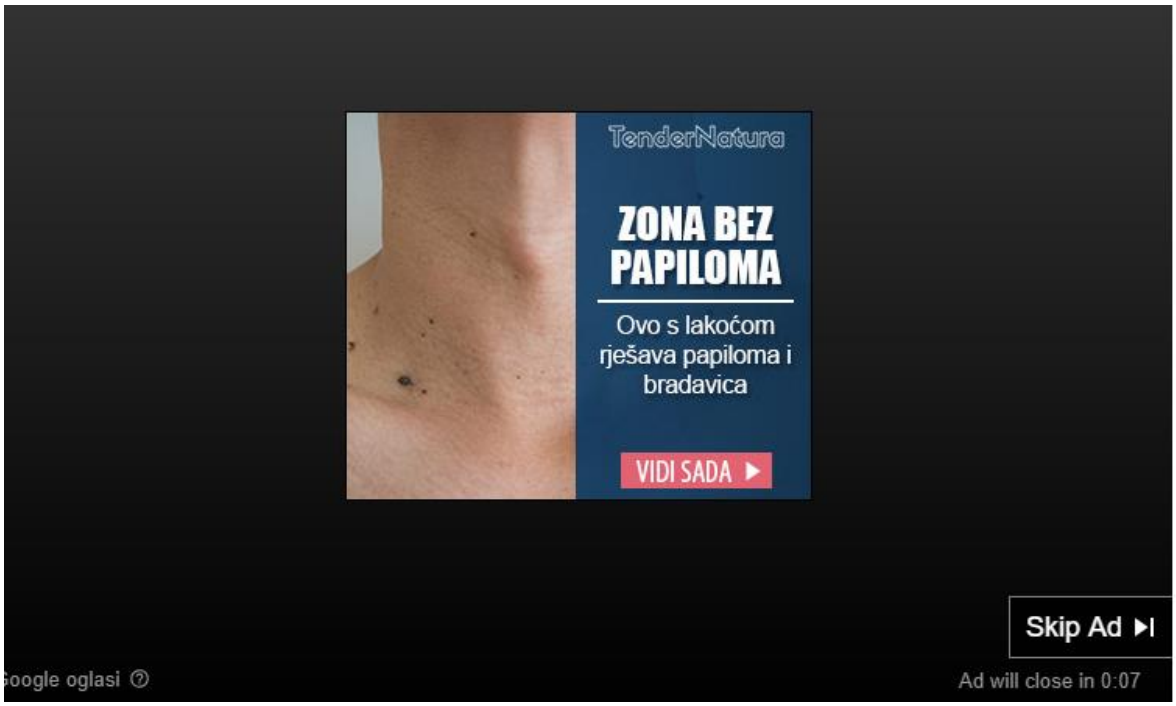
Slika 5.10 Portal sa lažnim informacijama o proizvodu

Detaljnijim pregledom stranica vidljivo je da napadači objavljuju i drugi sadržaj koji se reklamira kao edukativan, a stvarna intencija mu je ponovo navesti korisnika da kupi ovaj proizvod ili sličan. Obrazac ponašanja procesa kupovine je jednak na svim stranicama. Moguće je da koriste ovaj sadržaj iz više razloga

- Da objavljivanjem novog sadržaja prikriju stvarnu aktivnost kod Google pregleda
- Više stranica znači i manju šansu da sve stranice budu detektirane korištenjem ključnih riječi - moguće je utjecati da informacije koje bi otkrile prijevaru budu istisnute na npr. 10 ili 20. stranicu Googlea
- Jednu stranicu moguće je koristiti za više prevara – odredišni tekst o zglobovima mamit će korisnika da kupi tablete za zglobove, a onaj o mršavljenju navest će korisnika da kupi tablete za mršavljenje. Svi tekstovi se unutar jedne mrežne stranice predstavljaju kao edukativan sadržaj.

Stranice nisu u potpunosti dovršene s obzirom da samo preusmjeravaju korisnika na početnu stranicu, neke rezultiraju padom stranice, a neke nisu dovršene, odnosno napisane su na nekim drugim jezicima.

Poveznice na treće strane mogu se javiti i u tekstualnim oglasima (Slika 5.10.) ili video oglasima (Slika 5.11.) u sklopu video priloga.



Slika 5.11 Primjer reklama u video prilozima

Jedan od najvećih napada na najveću oglašivačku mrežu AdSense (Googleov proizvod), dogodio se 2015. godine. Radi se o ranije opisanim reklamama *...koje su nasumično preusmjeravali korisnike na sajtove na kojima su se korisnicima nudili proizvodi za njegu kože, poboljšanje pamćenja i mršavljenje. Sajtovi su imitirali postojeće ugledne blogove i magazine, kao što je Forbes, Good Housekeeping i drugi, ali i nepostojeće a navodno ugledne web sajtove. Da bi sve bilo uverljivije, na sajtovima se nalazio veliki broj lažnih komentara korisnika kojima su navodno pomogli ovi proizvodi (Informacija, 2015.)*

Google navodi da sadržaj reklama provjerava i umjetna inteligencija, ali i ljudi prije nego li se javno objavi. Obzirom da Google Adsense koristi preko više od 2.500.000 stranica (SimilatrTech, 2018.), uvijek postoje iznimke. Googleovi sigurnosni napori u brojkama u 2017 (Search Engine land, 2018):

Ukinuto:

- 79 milijuna oglasa koji su slali korisnike na maliciozne treće strane
- Uklonjeno 400.000 malicioznih stranica
- 66 milijuna spam oglasa
- 48 milijuna oglasa koji su rezultirali preuzimanjem malicioznih programa.

Googleov direktor Scott Spencer zaključio je da se radi o preko 100 malicioznih oglasa svake sekunde, stoga je razumljivo da dio odgovornosti moraju preuzeti i stranice koje objavljuju oglase (Search Engine Land, 2018). Kako Google ne može kontrolirati niti biti odgovoran za preusmjeravanje na maliciozne lokacije trećih strana, tako niti portali ne mogu 100% garantirati iskustvo bez malicioznih pokušaja. Valja napomenuti da nije uvijek potrebna radnja korisnika da bi računalo bilo napadnuto malicioznim programom. Napad se može dogoditi odmah po pokretanju i prikazivanju reklame (IT klinika, 2017)..

5.2.4. Javno objavljivanje informacija / podataka

Portali Jutarnji Online, Net.hr, Index.hr, 24sata.hr imaju sustav komentiranja gdje nije potrebna registracija, već se korisnik može prijaviti putem Facebook profila. Korisnici koji javno iznose stavove te imaju osobne informacije javno vidljive na Facebooku mogu postati žrtva napada malicioznim programom. Napadač može,. Npr. kod osobe koja voli sport u privatnoj poruci putem Facebooka poslati primamljiv naslov prilagođen stavovima koje je javno iznio u komentaru na određenu temu uz poveznicu na vanjski izvor koji će inficirati

računalo korisnika malicioznim programom. Ovaj problem je odgovornost korisnika obzirom da je sustav komentiranja putem Facebooka masovno korišten na web portalima.

5.2.5. Krađa osobnih podataka

Krađa osobnih podataka potencijalna je opasnost neovisno o mrežnoj stranici koju posjećujemo. Iako odgovornim ponašanjem možemo postići određeni nivo sigurnosti, ništa ne možemo učiniti kada je u pitanju krađa podatak sa servera. Ovaj problem ne bi bio toliko izražen da su u pitanju samo posjetitelji koji koriste mogućnost komentiranja. Problem ovdje stvaraju povezani servisi razvijeni od strane web portala, a najbolji primjeri za to su oglasnik Index oglasi razvijen od strane portala Index.hr te email servis Freemail razvijen od strane portala Net.hr.

Index oglasi predstavljaju visoki rizik obzirom da je potrebno unijeti OIB što može predstavljati veliki problem. Do krađe može doći i prilikom unosa ukoliko je računalo zaraženo ScreenRecorderom, Keyloggerom ili klasičnom krađom podataka. Na hrvatskom cyber prostoru teško je pronaći bilo kakve informacije o krađi podataka. Možemo izdvojiti tek jedan slučaj gdje je došlo do krađe podataka korisnika servisa Freemail. Problem je uočen slučajno kada su djelatnici portala Blog.hr vidjeli neobično visok broj hakiranih blogova. Detaljniji pregled pokazao je da su svi zahtjevi pristigli od korisnika koji su imali otvoren mail na servisu Freemail.

5.2.6. Sigurnosni protokol

Protokoli su strogo propisana pravila komunikacije kojem se služe računala kako bi se sporazumjela. Najprikladniji protokol za komunikaciju prilikom posjeta mrežnoj stranici je HTTP (engl. HyperText Transfer Protocol) protokol koji propisuje pravila prijenosa mrežne stranice od poslužitelja do korisnika. Kombinacijom HTTP i SSL certifikata (eng. Secure Socket Layer) napravljen je HTTPS protokol koji putem kriptirane veze (SSL certifikat djeluje kao zaštitni sloj) kako bi se spriječili mogući upadi od trećih strana u komunikaciju. Google Chrome korisnike obavještava o sigurnosti određene web lokacije putem sigurnosnih simbola uz upisani web adresu.

1. Sigurno
2. Nema informacije ili nije sigurno
3. Nije sigurno ili opasno.

Svi mrežni portali koji su predmet istraživanja označeni su kao sigurni od strane preglednika Chrome, odnosno veza s portalom je osigurana SSL certifikatom.

5.3. Zaključak istraživanja

Edukacija korisnika je ključ obzirom da je korištenje portala i korištenje interneta, odnosno valja primjenjivati univerzalna pravila bez obzira u kojoj se digitalnoj okolini korisnici nalazili kako bi se mogućnost zaraze računala svela na najnižu moguću razinu. Sigurnost portala, odnosno mogući sigurnosni propusti kao teme nisu zastupljene među tim istim portalima, odnosno postoji tek nekoliko zabilježenih slučaja. Dovoljni i razumni napori su uloženi od strane IT odjela i administratora kako bi se maliciozne poveznice svele na najmanju moguću razinu, a sve ostalo je pitanje edukacije korisnika. Iako se prosječnom korisniku može neka poveznica činiti kao smiješan pokušaj prijevare, onim lakovjernijim to može predstavljati ozbiljan problem no, kao što sam spomenuo, taj dio je več odgovornost korisnika. Glavni propust i odgovornost portala je korištenje nepouzdanih sustava za prikazivanje oglasa trećih strana (oglašivačke mreže). Google možda nije u mogućnosti pratiti sve oglase zbog velike količine objavljenih oglasa po minuti, no hrvatski portali trebali bi detaljnije analizirati oglase koji se pojavljuju uz članak. Na svim portalima kod kojih je uočen problem prikazivanja malicioznih oglasa, najčešće u obliku lažnih proizvoda. Midas i slične oglašivačke mreže korisniku plasiraju maksimalan broj validnih oglasa koji su najčešće poveznice na druge portale, a preostali dio (najčešće 1-3) oglasa plasira koji su maliciozni. Razlog može biti nedovoljno napredna zaštita koja bi prevenirala prikaz ovakvih oglasa. Drugi razlog može biti i visok udio prihoda od prikazivanja takvih oglasa u ukupnoj strukturi prihoda. Ovaj razlog može se i pripisati portalima koji zbog loše popunjenosti oglašivačkih kapaciteta na slabije čitanim i rangiranim rubrikama poseže za ovakvim rješenjima kao neki oblik pasivnog prihoda. Ovakvi oglasi neće se prikazati na naslovnici, već isključivo na unutarnjim predlošcima. Bilo da je razlog nedovoljno razvijena zaštita ili financijska korist i dalje je odgovornost na korisniku koji treba razumijeti okolinu u kojoj se nalazi.

6. Tehnička zaštita korisnika

Kada govorimo o tehničkoj zaštiti, govorimo o mogućnosti sustava da automatski prepozna poželjan od neželjenog sadržaja, što uključuje odbacivanje i propuštane, a dijeli se prema smještaju filtera u mreži. Filter može biti u obliku programa na računalu ili na posrednom (engl. Proxy) računalu koje može štititi više računala. Na ovaj oblik Internetske usluge korisnici se mogu i pretplatiti. Metode tehničke zaštite mogu se zasnivati na temelju baze provjerenih podataka (statički pristup), ili analize svakog novog sadržaja (dinamički pristup). Iako dinamičke metode nisu sasvim točne te često puta mogu siguran sadržaj ocijeniti kao nesiguran. Obje metode koriste se podjednako, a Nacionalni CERT preporuča sljedeće metode tehničke zaštite korisnika (CERT 2009)

6.1. Vatrozid

Vatrozid je osnovna zaštita računala koja provjerava dolaze li podaci iz dopuštene mreže te prate odlazi promet po sličnim pravilima kao i za dolazni promet. Vatrozid nije u mogućnosti prepoznati kod, spam, scam poruke ili nepoželjan sadržaj jer nije oblikovan da provjerava podatke, već samo pošiljatelja i priključnicu s koje šalje podatke te ocjenjuje njegovu pouzdanost. (CERT, 2009). Napadači mogu zaobići Vatrozid maskiranjem, odnosno sakrivanjem IP adrese na način da koriste virtualne privatne mreže, tzv. VPN (engl. Virtual private network). Radi se interkonekciji lokalne mreže koristeći kriptirane načine komunikacije na način da serveri na koje se korisnik povezuje vide i bilježe IP adresu servera putem kojeg se korisnik spaja, a ne IP adresu korisnika. VPN na taj način stvara privatan „tunel“ u obliku zatvorene veze koju ne može dekriptirati neka druga strana (PC Chip, 2016.)

6.2. Antivirusni alati

Antivirusni alati su programi koji analiziraju datoteke s izvršnim programskim kodom prilikom otvaranja, slanja ili primanja datoteka što podrazumijeva i periodičnu provjeru svih datoteka sustava. Oni ne raspoznaju opasna web odredišta, već samo prisutnost zlonamjernog koda u datoteci u obliku virusa, ali i drugih štetnih programa. Razlikujemo besplatne i verzije koje se naplaćuju, a stručnjaci iz CERT-a navode kako su u većini slučajeva i besplatne inačice dovoljne za adekvatnu zaštitu.(CERT, 2018.)- Anti botnet ne nudi direktno preuzimanje programa već upućuje korisnike na mrežne stranice proizvođača gdje je moguće preuzeti besplatne inačice programa. a izdvajaju programe *Avast, AVG, Avira, Malwarebytes i Panda kao besplatne inačice koje je moguće preuzeti na* Cert i Carnet putem portala Anti-botnet su u suradnji i s tehnološkim partnerima i proizvođačima antivirusnih alata *Avira, Gdata* i *Surfright* razvio je alat za detekciju i uklanjanje antivirusnih programa EU cleaner. On ne zamjenjuje antivirusni alat već služi za dodatno skeniranje sustava.

6.3. Filtri neželjene pošte

Velik broj internetski servisa za elektroničku poštu kao što su Gmail, Hotmail, Yahoo i drugi imaju ugrađene filtere koji analiziraju dolaznu poštu i smještaju je u zaseban pretinac. Ovakvi automatski filteri neće obrisati dolaznu poštu koju identificiraju kao *Spam* iz razloga što i legitimna poruka može biti označena kao spam. Automatski filteri provjerit će nalazi li se IP adresa pošiljatelja na tzv. Crnoj listi (engl. Blacklist), radi li se o tzv. *Zombi računalu* (računalo nad kojim je prethodnim napadima stečen neovlašten pristup pa se koristi za i daljnje izvršenje napada) ili koristiti statističke metode koje na temelju poznatih uzoraka poruka uči prepoznavati dotad neviđene poruke(CERT, 2018). Kombinacija navedenih filtera će podići razinu zaštite korisnika, no najvažnije je odgovorno ponašanje korisnika. Ukoliko neka poruka i zaobiđe filtere, na korisniku je da prema nazivu, domeni , naslovu i tijelu elektroničke poruke procijeni radi li se o neželjenoj pošti. Stručnjaci iz CERTa svakako preporučaju držanjem osobne email adrese tajnom te otvaranje posebne mail adrese koja će se koristiti u situacijama gdje je potrebno dati podatke o email adresi nepouzdanom partneru obzirom da postoje maliciozni alati koji posjećuju mrežne stranice i prikupljaju dostupne email adrese.(npr. Forumi). Primarni elektronički račun treba koristiti samo za

bitnu i provjerenu komunikaciju, kao što je npr. Komunikacija s bankom, kod prijave za posao, komunikaciju s prijateljima i slično. Također se ne preporuča odgovaranje na takve poruke jer time se otkriva pošiljateljima da se radi o aktivnoj mail adresi čime se potiče daljnja zloupotreba, kao ni otvaranje raznih poveznica koje se nalaze u tijelu poruke . Otvaranje poveznica također odaje informacije o aktivnosti email adrese, a može se raditi i o phishing ili drugoj vrsti napada.

6.4. Zaštita preglednika

Globalno najpopularniji preglednici su Chromeom (59.61 posto tržišnog udjela); Internet Explorerom (14.18 posto tržišnog udjela) i Firefoxom (12.85 posto tržišta). Osim što imaju ugrađene sustave koji štite korisnika od različitih malicioznih napada, ovi preglednici nude i širok raspon nadogradnji i dodataka u pogledu poboljšanja sigurnosti korisnika. Antibotnet na svom portalu objavljuje preporuke o korištenju dodataka i proširenja za internetske preglednike s ciljem zaštite korisnika. Preporuke se odnose na Internetske pretraživanje Google Chrome, Mozilla Firefox i Internet Explorer, a treba imati na umu da nisu svi dodaci dostupni za sve preglednike, odnosno da se dodaci i proširenja razlikuju od preglednika do preglednika – kod nekih preglednika dati će više mogućnosti tehničke prilagodbe proširenja ili dodatka, a na nekima manje.

- Blokiranje reklama

  Iako mnogo korisnika koristi ovakve tipove programa kako bi izbjegla reklamne sadržaje koji mogu biti obavezni prije pregleda željenog sadržaja (npr. Obavezan pregled reklame prije nastavka na željeni video ili članaka), alati ovakvog tipa štite korisnika i od neželjenih virusa koje može preuzeti na internetu. Stručnjaci iz CERT-a preporučaju korištenje programa Adblock Plus, Adguard i uBlock Origin. Ovi dodaci imaju mogućnost podešavanja na način da da blokiraju samo oglase i skočne prozore koji sadrže maliciozne programe,, a propusti će prikazivanje nenametljivih oglasa (moguće je podesiti i blokiranje svih oglasa). odnosno blokiranjem Dodatke nije moguće direktno preuzeti na stranicama Anti botnet portala već korisnika preusmjeravaju na provjerene mrežne stranice za preuzimanje dodataka ovisno o pregledniku kojeg korisnik koristi.

- Privatnost

  Dodaci za zaštitu privatnosti štite korisnika na način da sprečavaju odredišna web mrežna mjesta da prikupljaju previše podataka o korisniku, blokiraju aktivaciju koda za praćenje, krađu lozinki i slično. Razni dodaci nude i različite mogućnosti ovisno o pregledniku, a preporučeni za korištenje su Disconnect, Ghostery, HTTPS Everywhere, Privacy Badger, Self-destructing Cookies, Tab Cookies i WebRTC Leak Prevent

7. Edukacija korisnika

Ključ zaštite korisnika je edukacija. Niti jedan pojedinac ne može pratiti promjene u tehnologiji, zakonodavnom okviru, trendovima, a niti se može osloniti na neko tehničko rješenje obzirom da proboj tehničke sigurnosti sustava ne mora biti dio ciklusa socijalnog inženjeringa. U ovom radu neće biti opisane konkretne upute pojedinih operativnih radnji u pogledu tehničke sigurnosti korisnika obzirom na velik broj različitih operativnih sustava, internetskih preglednika i sl. te njihovih verzija. U nastavku rada će se u pogledu edukacije prosječnog korisnika interneta biti navedene preporuke od strane najrelevantnijih mrežnih stranica, a koje možemo podijeliti u

- Preporuke tehničke zaštite korisnika
- Preporuke edukacije korisnika o korištenju

Mrežne stranice koje se mogu smatrati relevantnima, istinitima i ažurnima djeluju na nacionalnoj razini i najčešće su osnovane os strane Vladinih agencija, Instituta ili udruga te se financiraju iz javnih prihoda, a od kojih valja izdvojiti:

- **Cert.hr** – Nacionalni CERT. *CERT (eng. Computer Emergency Response Team) ili CSIRT (engl. Computer Security Incident Response Team) je organizacijski entitet koji reagira na računalno-sigurnosne incidente, te preventivnim djelovanjem radi na poboljšanju računalne sigurnosti informacijskih sustava. Nacionalni CERT osnovan je u skladu sa Zakonom o informacijskoj sigurnosti RH i prema tom zakonu CERT je nacionalno tijelo za prevenciju i zaštitu od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj. Jedna od glavnih zadaća je usklađivanje postupanja u slučaju sigurnosnih računalnih incidenata na javnim informacijskim sustavima nastalih u Republici Hrvatskoj, ili u drugim zemljama i organizacijama, kad su povezani s Republikom Hrvatskom. Prema Pravilniku o radu Nacionalnog CERT-a, on se bavi incidentom, ako se jedna od strana u incidentu nalazi u RH (odnosno, ako je u .hr domeni ili u hrvatskom IP adresnom prostoru) (CERT, 2018)* . Kao nacionalni entitet, njegova misija je zaštita pravnih i fizičkih osoba u Hrvatskoj proaktivnim mjerama (prije incidenta) i reaktivnim mjerama kroz upozorenja i preporuke. Nacionalni CERT na svojim mrežnim stranicama redovito objavljuje preporuke u

pogledu sigurnosti i obavještava javnost o aktivnostima i događanjima. (CERT, 2018)

- **Antibot.hr** - besplatan servis osnovan od strane CERT-a korisnicima nudi mogućnost preuzimanja antivirusnih programa, dodataka za preglednike, programe za sigurnosnu provjeru, druge razne alate za zaštitu tableta i pametnih telefona, te Općenite sigurnosne preporuke i instrukcije za različite teme vezane za Internet.
  - **Azop.hr** – Agencija za zaštitu osobnih podataka redovito objavljuje edukativne materijale i mišljenja vezanih na temu obrade osobnih podataka i usklađenosti a zakonodavstvom. (Azop, 2018)
  - **Medijskapismenost.hr** – osnovan od strane Agencije za elektroničke medije redovito objavljuje članke i publikacije koje se bave sigurnosti djece i roditelja prilikom korištenja Interneta. Posebno se nastoji potaknuti vrednovanje i kritičko promišljanje kod djece i mladih prilikom korištenja Interneta, a fokus stavlja na edukaciju i zaštitu djece od neželjenog i štetnog sadržaja s ciljem edukacije i informiranja djece, roditelja, odgojitelja i nastavnika o važnosti medijske pismenosti. Portal redovno objavljuje članke i publikacije te je na godišnjoj bazi organizator dana medijske pismenosti. *Agencija za elektroničke medije i Ured UNICEF-a za Hrvatsku, pod pokroviteljstvom Ministarstva kulture i Ministarstva znanosti i obrazovanja, u suradnji s brojnim partnerima i medijskim kućama pokrenuli su Dane medijske pismenosti. Od 19. do 21. travnja 2018., ali i tijekom cijele druge polovice travnja pa i početkom svibnja odvijale su se brojne aktivnosti i događanja s ciljem informiranja i educiranja djece, roditelja, nastavnika i odgojitelja o toj važnoj temi i vještini.* (Agencija za elektroničke medije, 2018.).
- **Csi.hr** – Centar za sigurniji Internet – Centar za nestalu i zlostavljanu djecu. Članovi Centra su stručnjaci s područja informatike, računalnog programiranja, kriminalistike, računalne forenzike, prava, pedagogije i psihologije. Centar organizira brojne preventivne projekte, izdaje brošure te je organizator Dana sigurnijeg Interneta. *Svake veljače udruženje Insafe/INHOPE uz potporu Europske Komisije organizira Dan Sigurnijeg Interneta kojemu je cilj promicanje sigurnije i odgovornije upotrebe online tehnologije i mobilnih uređaja, posebice među djecom i mladima. Svake godine na drugi dan drugog tjedna drugog mjeseca tisuće ljudi diljem svijeta se udruže kako bi sudjelovali u događajima i aktivnostima kojima žele podići svijest o sigurnosnim problemima na internetu.*

Dan sigurnijeg interneta se organizira u sklopu projekta „Safer Internet Centre Croatia: Making internet a good and safe place" (2015-HR-IA-0013) kojega sufinancira Europska unija iz programa Department C – Connecting Europe Facility (CEF). Centar ima i uspostavljen broj za prijavu nezakonitog e-sadržaja te besplatan broj za pomoć i podršku u slučaju nasilja, savjete za zaštitu na Internetu, preporuke kako sigurnije koristiti Internet te što napraviti i kako se nositi s neprimjerenim kontaktom na Internetu.(CSI, 2018)

8. Zaključak

Napredak u razvoju tehnika socijalnog inženjeringa, kao i dolazak sve obrazovanijih i maštovitijih napadača uključile su razne institucije i organizacije u rješavanje problema aktivne i pravovremene zaštite. Upravo domišljatost i maštovitost napadača onemogućuje pravovremenu zaštitu jer je potrebno vrijeme da institucije i organizacije reagiraju prilikom pojave nove vrste napada. Radi brzine reakcije, odnosno bržeg prijenosa podataka o novim malicioznim programima i tehnikama, nacionalni centri ostvaruju međunarodnu suradnju s drugim centrima, kao i proizvođačima sigurnosnih, antivirusnih sustava. Kako bi se minimizirao utjecaj napada koji stignu do žrtve prije npr. zakrpa u antivirusnom programu ili obavijesti policije, Nacionalni centri u suradnji s udrugama i drugim organizacijama aktivno sudjeluju u informiranju građana. Edukacija korisnika Interneta je ključna kako bi se cjelokupni sustav zaštite održao jer bez edukacije i informiranja nema saznanja o dostupnim programskim načinima zaštite i ažuriranja što korisnika stavlja u ranjiv položaj spram napada malicioznim programima. Za drugu vrstu napada, onu koja nije ograničena tehnološkim rješenjima već koristi ljudski faktor, je mnogo teže pripremiti korisnika. Nove metode psihološke manipulacije mogu biti personalizirane i usmjerene na točno određenom pojedinca stoga je potrebno edukaciju usmjeriti osnovnim pravilima odgovornog ponašanja na Internetu kako se korisnici ne bi sami doveli u situaciju da postaju žrtve (javno objavljivanje osobnih podataka, davanje pristupnih podataka nepoznatim osobama, uplate novca na nepoznate račune, izbjegavanje reklama koje djeluju sumnjivo i sl.) Sva navedena pravila, odnosno problematika sigurnosti podataka i imovine u digitalnom svijetu, ne mogu se u većoj ili manjoj mjeri pripisati korištenju web portala naspram drugih tehnologija (društvene mreže i tražilice), ili web stranica. Neke od specifičnosti portala koje povećavaju mogućnost programskog ili ljudskog proboja zaštita su velika količina sadržaja koja se svakodnevno generira, velik broj interno razvijenih aplikacija (za igranje, telefonski imenik, osobni horoskop), velik broj poveznica prema trećim stranama, angažman korisnika putem komentara, korištenje trećih strana za prikazivanje oglasa, analizu posjetitelja i slično. U Hrvatskoj se najčitaniji web portali drže aktualnih sigurnosnih normi i ulažu napore kako bi sveli mogućnost napada na najmanju moguću razinu.

Popis tablica, grafikona i slika

Slike

Tablice

Litertura

[1] Agencija za zaštitu osobnih podataka, Što je krađa identiteta?, http://azop.hr/aktualno/detaljnije/krada-identiteta-i-kako-se-zastititi

[2] Antibot, Kako se zaštititi?, http://www.antibot.hr/introduction/aspekti-sigurnosti.html

[3] Arbona, Tko su hrvatski Facebook korisnici, 2018, https://www.arbona.hr/blog/internet-ili-internetski-marketing/infografika-tko-su-hrvatski-facebook-korisnici-2016-vs-2018/695 (15.07.2018.)

[4] AV TEST, Malware, https://www.av-test.org/en/statistics/malware/

[5] Avira, https://www.avira.com/en/about-avira?100_million_avira_users.html=

[6] CARNet, Filtriranje web sadržaja, 2009.,

[7] CARNet, Napredne tehnike socijalnog inženjeringa, , 2010.,

[8] CARNet, Opasnostni Facebooka,

[9] CARNet, Phishing, 2018., https://www.cert.hr/wp-content/uploads/2018/05/phishing.pdf

[10] CARNet, Ransomware - plati svoje podatke, 2017.,

[11] CARNet, Sigurnije na Internetu

[12] CARNet, Spyware programi, 2009 https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2009-10-280.pdf

[13] CARNet, Uvod u socijalni inženjeringe, 2017.,

[14] Carnet, Zaštita privatnosti na Internetu, 2015

[15] Centar za sigurniji Internet, Dan sigurnijeg Interneta 07.02.2017., 2017., http://www.dansigurnijeginterneta.org/dan-sigurnijeg-interneta-07-02-2017/

[16] CERT, O trojanskim konjima, https://www.cert.hr/trojanski_konji/

[17] CERT, Godišnji izvještaj Nacionalnog CERT-a za 2017. godinu, 2018., https://www.cert.hr/wp-content/uploads/2018/03/CERT.hr_godisnji_izvjestaj_2017.pdf

[18] CERT, O Adware/Spyware softveru, https://www.cert.hr/adware/

[19] CERT, O crvima, https://www.cert.hr/crvi/

[20] CERT, O nacionalnom CERT-u, https://www.cert.hr/onama/

[21] CERT, O socijalnom inženjeringu, https://www.cert.hr/socijalni_inzenjering/

[22] CERT, O virusima, https://www.cert.hr/virusi/

[23] CSI, Helpline, http://csi.hr/helpline/hr/simple

[24] CSI, Hotline, http://csi.hr/hotline/

[25] CSI, Opis dana sigurnijeg Interneta, 2018., http://csi.hr/p/dsi2018opis

[26] Čosić Jasmin i Bača, Miroslav, Prevencija računalnog kriminaliteta, 2013.

[27] Dulčić, K., Oblici štete od računalnih virusa i odgovornosti za štetu, Pravni fakultet Rijeka, 2007.

[28] Filozofski fakultet Osijek, Safer Internet Centre Croatia: Making internet a good and safe place (CEF-TC-2014-1 005, 2016)

[29] Grubor, G. i Franc, I., Novi koncept malicioznih programa, 2010.

[30] Index, GODIŠNJE ISTRAŽIVANJE REUTERSA Index.hr je internet medij broj 1 u Hrvatskoj, 2017.https://www.index.hr/vijesti/clanak/reuters-potvrdio-index-je-broj-jedan-u-hrvatskoj/978590.aspx

[31] Ivezić, Bernard, Dok u Europi online kriminal čini 20 posto ukupnih kaznenih djela, u Hrvatskoj on prema statistici iznosi svega 0,5 posto, Poslovni Dnevnik, 2018., http://www.poslovni.hr/tehnologija/dok-u-europi-online-kriminal-cini-20-posto-ukupnih-kaznenih-djela-u-hrvatskoj-on-prema-statistici-iznosi-svega-05-posto-337382

[32] Karakaš, Bernard, Najveći hakerski napad u povijesti, na meti bile bolnice, državne institucije, tvrtke, Večernji list, 2017 https://www.vecernji.hr/vijesti/najveci-hakerski-napad-u-povijesti-1169605

[33] Ledinek, Sanja, Što je Botnet i DDoS napad - osnove koje bi trebali znati , PC Expert, 2016., http://www.pcekspert.com/clanak/sto-je-botnet-i-ddos-napad-osnove-koje-bi-trebali-znati/

[34] Leksikografski Zavod Miroslav Krleža, WWW, http://www.enciklopedija.hr/natuknica.aspx?ID=66413

[35] Luzar, Ivan, Izgleda da ljudi kod nas dosta nasjedaju na lažne poruke na internetu, Telegram, 2018, https://www.telegram.hr/biznis-tech/izgleda-da-ljudi-kod-nas-dosta-nasjedaju-na-lazne-poruke-na-internetu-novo-istrazivanje-kaze-da-21-unese-svoje-podatke/

[36] Medijska pismenost, http://www.medijskapismenost.hr/dani-medijske-pismenosti/

[37] Medijska pismenost, http://www.medijskapismenost.hr/o-nama/

[38] Medijska pismenost, Vaše računalo možda je zaraženo virusima, a da to ni ne znate, 2007., http://www.medijskapismenost.hr/vase-racunalo-mozda-je-zarazeno-virusima-a-da-to-ni-ne-znate/ (15.07.2018.)

[39] Microsoft, Stvaranje i pokretanje Markonaredbe, https://support.office.com/hr-hr/article/stvaranje-i-pokretanje-makronaredbe-c6b99036-905c-49a6-818a-dfb98b7c3c9c (14.07.2018.)

[40] Ministarstvo unutarnjih poslova, Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata u 2015. godini, 2016. https://mup.hr/public/documents/Statistika/Pregled%20sigurnosnih%20pokazatelja%20u%202015.%20godini.pdf

[41] OECD, Malicious Software (Malware): A Security Threat to the Internet Economy, 2008., preuzeto pri http://www.oecd.org/internet/ieconomy/40724457.pdf (16.07.2018.)

[42] PC CHIP, Najbolji alati za blokiranje oglasa (ad blockers) na internetu, 2018., https://pcchip.hr/internet/korisne-aplikacije/najbolji-alati-za-blokiranje-oglasa-ad-blockers-na-internetu/

[43] PC CHIP, Rootkit - špijun u vašem računalu, 2016. https://pcchip.hr/softver/sigurnost/rootkit-spijun-vasem-racunalu/

[44] PC CHIP, Što je VPN? Za što se koristi?, 2016., https://pcchip.hr/internet/sto-je-vpn-za-sto-se-koristi/

[45] Reuters, Reuters Institute Digital News Report 2018, 2018., http://media.digitalnewsreport.org/wp-content/uploads/2018/06/digital-news-report-2018.pdf?x89475

[46] Rukavina, Damir, Chrome, Firefox ili Explorer? Evo koji je preglednik najsigurniji, Tportal, 2017., https://www.tportal.hr/tehno/clanak/chrome-firefox-ili-explorer-evo-koji-je-preglednik-najsigurniji-foto-20171108

[47] Symantec, Internet security Threat Report, 2017., https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

[48] Tech Crunch, Google Acquires Online Virus, Malware and URL Scanner VirusTotal, 2012., https://techcrunch.com/2012/09/07/google-acquires-online-virus-malware-and-url-scanner-virustotal/

[49] The World Bank, Individuals using the Internet, https://data.worldbank.org/indicator/IT.NET.USER.ZS

[50] Ured vijeća za nacionalnu sigurnost, Što je informacijska sigurnost, https://www.uvns.hr/hr/sto-je-to-informacijska-sigurnost

[51] https://www.informacija.rs/Vesti/Google-zaustavio-napad-malicioznim-reklamama.html

[52] https://searchengineland.com/google-says-removed-3-2b-ads-violation-advertising-policies-2017-294068

[53] https://www.it-klinika.rs/blog/milioni-racunara-zarazeni-kroz-maliciozne-oglase

[54] https://dnevnik.hr/vijesti/hrvatska/blogeri-razotkrili-hakeri-mjesecima-citali-mailove-korisnika-net-hr-a.html

[55] https://www.cis.hr/dokumenti/zatitabazapodataka.html

[56] https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2008-09-240.pdf

[57] http://chatbot.com.hr/sto-je-chatbot/