CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Malware na društvenim mrežama – primjer Koobface-a

NCERT-PUBDOC-2010-12-320

Nacionalni CERT

Sadržaj

1 Uvod

Društvene mreže korisnicima omogućuju komunikaciju i dijeljenje različitih multimedijskih sadržaja (fotografije, video zapisi…). Koristi od njih imaju i poslovne organizacije. Promidžbene poruke na društvenim mrežama donose veliku zaradu, a poslovne organizacije mogu izraditi vlastiti profil te se približiti svojim klijentima.

U zadnjih nekoliko godina društvene mreže bilježe gotovo eksponencijalan rast broja korisnika. Vodeća mreža, s 400 milijuna korisnika, je Facebook. I na drugim mrežama broj korisnika mjeri se u milijunima. Twitter ima 75 milijuna, a MySpace 125 milijuna korisnika.

Nažalost, s sve većim rastom društvenih mreža raste i broj kriminalaca koji u njima vide priliku za brzu zaradu. Zbog toga, danas je svaki korisnik društvenih mreža moguća žrtva zlonamjernih programa koji se šire putem mreže. Takvi zlonamjerni programi kradu sve osobne podatke do kojih mogu doći. Korisnik zbog toga može pretrpjeti krađu identiteta ili financijsku štetu.

Ovaj rad istražuje pojavu zlonamjernih programa na društvenim mrežama. Opisani su motivi autora zlonamjernih programa. Svim korisnicima društvenih mreža predložene su smjernice za zaštitu i sigurnu komunikaciju s drugim korisnicma. Prikazana je tehnička analiza Koobfacea – poznatnog primjerka zlonamjernog koda koji se širi društvenim mrežama.

2 Pojava zlonamjernih programa na društvenim mrežama

U osamdesetim i devedesetim godinama prošlog stoljeća osnovni motiv za razvoj i distribuciju zlonamjernih programa nije bio novac. Autori zlonamjernih programa svoje su primjerke razvijali kako bi pokazali veliko tehničko znanje, stekli slavu ili zadovoljili svoju znatiželju. U zadnjem desetljeću ovi motivi prešli su u drugi plan. Danas je većina primjeraka zlonamjernog koda razvijena kako bi omogućili zaradu svojim autorima.

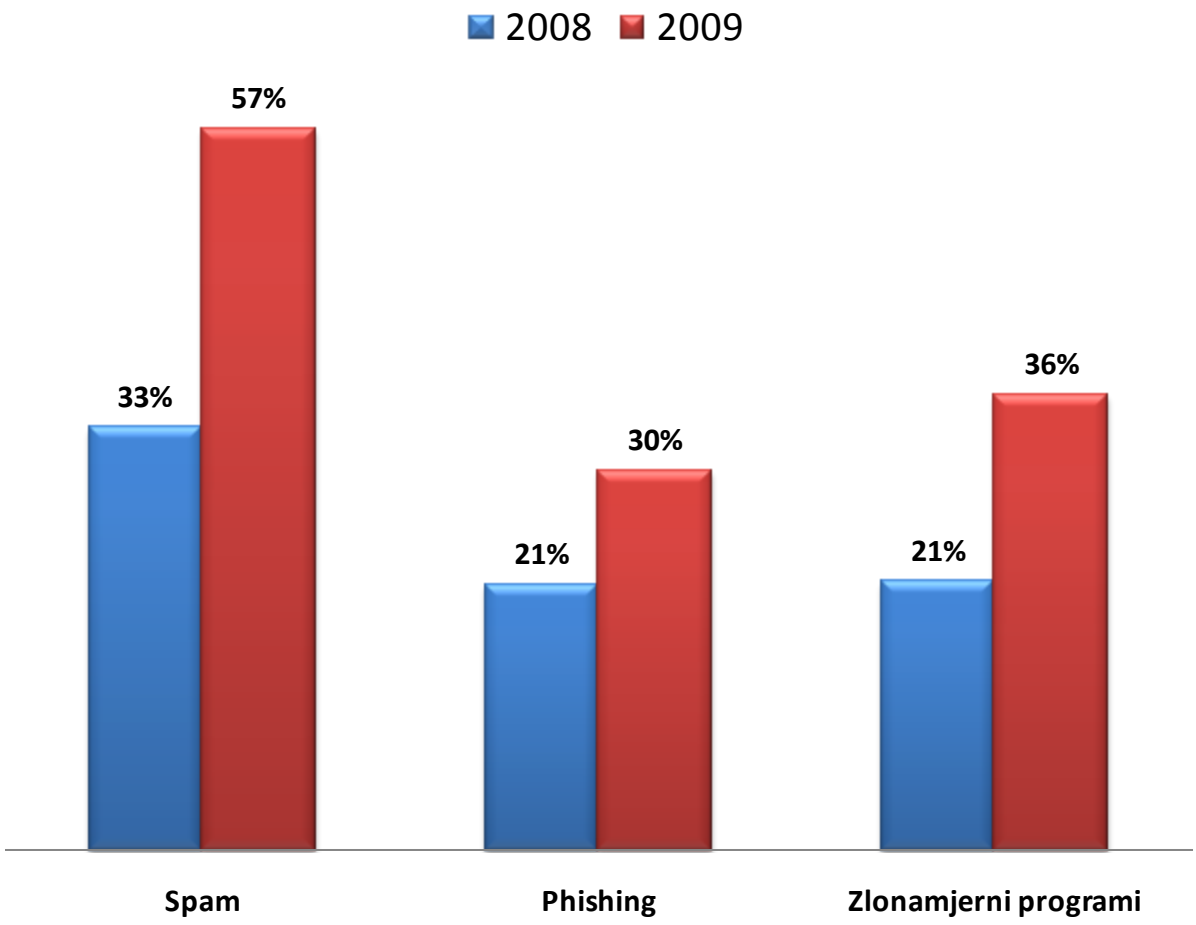
Kriminalci mogu zaraditi na krađi financijskih podataka drugih ljudi ili slanju neželjene elektroničke pošte. No, kako bi zarada bila velika, kriminalci moraju ukrasti podatke od velikog broja korisnika ili poslati veliki broj neželjenih poruka. Zbog toga su im društvene mreže postale zanimljivo područje za širenje zlonamjernih programa. Veliki broj korisnika na njima kriminalcima omogućuje krađu dovoljno financijskih podataka za ostvarivanje veće dobiti.

Računica je jednostavna. Ako neki primjerak zlonamjernog koda uspije zaraziti samo 1 promil korisnika na Facebooku[1], to znači da kriminalac koji njime upravlja ima pristup na 40 000 različitih korisničkih računa. Ukoliko samo sa 10% zaraženih računala kriminalac prikupi valjane financijske podatke i sa svakog ukrade 500 dolara ukupna dobit mu je dva milijuna dolara.

Ovaj veliki potencijal prepoznali su i kriminalci i već danas se na društvenim mrežama može pronaći mnogo različitih zlonamjernih programa. Nažalost, teško je pronaći točne statistike koje prikazuju trendove u prisutnosti zlonamjernih programa na društvenim mrežama. Zlonamjerni programi globalni su problem koji nadilazi granice pojedinih država. Kako ne postoji središnja organizacija koja prati i nadzire njihovo kretanje, ne postoje i jedinstvene i objektivne statistike. Situacija s društvenim mrežama je slična. One su zaokupljene velikim rastom, slabo ulažu u sigurnost svojih korisnika i ne prate pojavu zlonamjernih programa.

Jedini statistički podaci o zlonamjernom kodu na društvenim mrežama dostupni su u različitim izvještajima koje izrađuju antivirusne kompanije. Jedan takav izvještaj je Sophosov izvještaj o sigurnosnim prijetnjama za 2009. godinu. U izvještaju se navodi kako je čak 36% poslovnih organizacija primilo zlonamjerne programe putem društvenih mreža. Posebno je zabrinjavajući podatak kako je to rast za 69.8% u odnosu na 2008. godinu. Na sljedećem grafu prikazani su podaci o porastu *spama*, *phishinga* i zlonamjernih prorgama na društvenim mrežama.

[1] Podsjetimo, Facebook trenutno (srpanj, 2010.) ima oko 400 milijuna korisnika

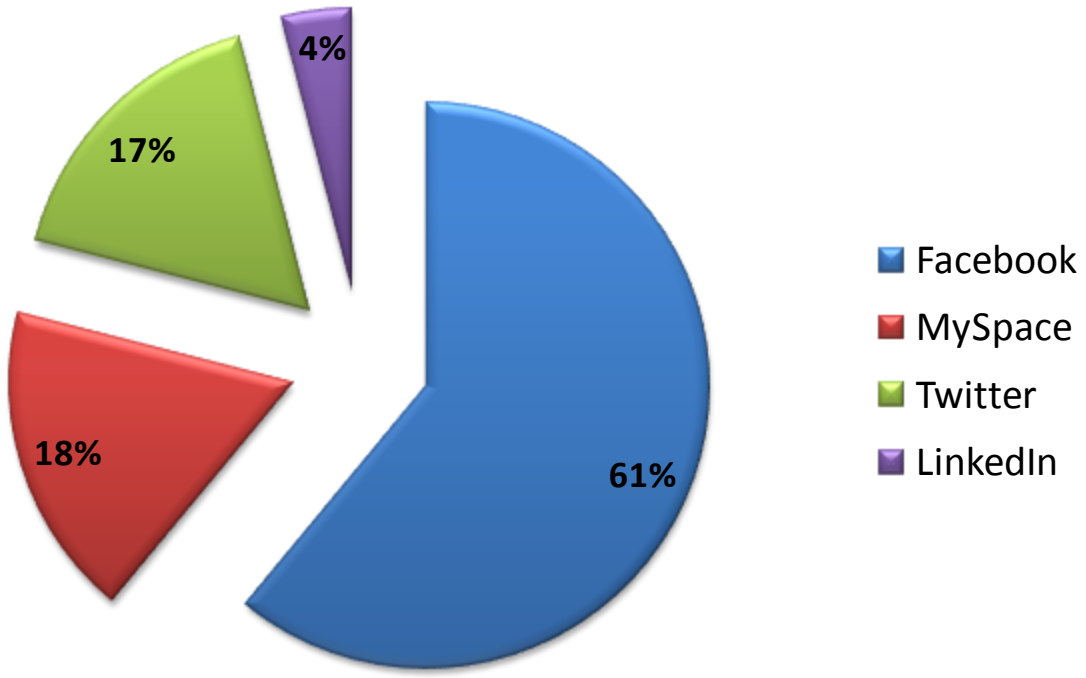


Slika 2.1 - Prikaz porasta prijetnji na društvenim mrežama

Graf prikazuje postotak poslovnih organizacija koje su se suočile s *spamom, phishingom* ili zlonamjernim programima na društvenim mrežama. Ovo su najčešće vrste prijetnji na društvenim mrežama. Na njih ne treba gledati kao na tri potpuno odvojene i nepovezane kategorije. Naime, *spam* i *phishing* uvjetovani su pojavom većeg broja zlonamjernih programa. Kao što će kasnije na primjeru biti pokazano, kriminalci, između ostalog, zlonamjerne programe koriste za slanje *spam* poruka i distribuciju *phishing* web stranica. Prema tome, pojavom sve većeg broja zlonamjernih programa raste i broj *spam* poruka i *phishing* napada.

Iz grafa 2.1 važno je prepoznati kako je došlo do porasta broja prijetnji. Sa sve većim rastom društvenih mreža ovakav trend moguće je očekivati i u budućnosti.

Raspored prijetnji po različitim društvenim mrežama je očekivan. Najviše prijetnji dolazi s Facebook-a budući da je to daleko najveća društvena mreža. Detaljniji udio društvenih mreža u prijetnjama prikazan je na sljedećem grafu.



Slika 2.2 - Udio broja prijetnji po društvenim mrežama

Više od pola prijetnji dolazi s Facebooka. S druge strane, LinkedIn slovi kao najsigurnija društvena mreža. No, iako na njoj nema mnogo zlonamjernih programa, LinkedIn mogućim napadačima može poslužiti kao izvor informacija o organizacijskoj strukturi pojedinih kompanija.

U [1] navodi se kako 72% poslovnih organizacija strahuje da bi postupci njihovih zaposlenika na društvenim mrežama mogli ugroziti korporativnu sigurnost. Kako je to porast od 66% u odnosu na prošlu godinu nameće se zaključak da organizacije postaju svjesne rizika koji dolazi s društvenim mrežama.

Ipak, bez obzira na zabrinutost, 49% organizacija svojim zaposlenicima omogućuju slobodan pristup svim društvenim mrežama. U istom izvještaju, navodi se kako je to porast od 13% u odnosu na prošlu godinu.

Iz ovog kratkog statističkog pregleda moguće je izvesti nekoliko zaključaka:

1. Društvene mreže iznimno su popularne i imaju jako veliki broj korisnika.
2. Kriminalci su prepoznali moguću korist od popularnosti društvenih mreža i na njima šire zlonamjerne programe.
3. U budućnosti je moguće očekivati stalni rast prijetnji na društvenim mrežama. Zbog toga je potrebno uložiti napor u edukaciju korisnika društvenih mreža i time smanjiti širenje zlonamjernih programa i štete koje od njih nastaju.

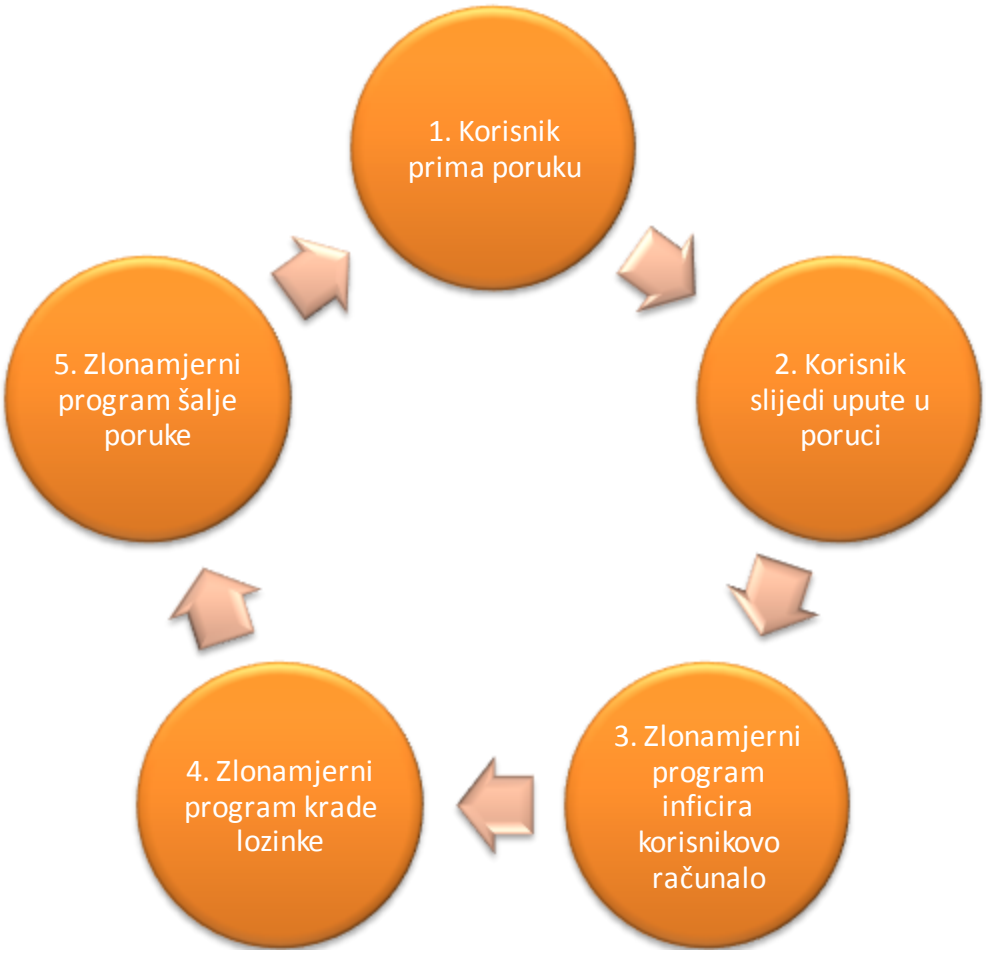
3 Širenje zlonamjernih programa na društvenim mrežama

Kada je riječ o načinu na koji se zlonamjerni programi šire putem društvenih mreža gotovo uvijek se radi o socijalnom inženjeringu. Rijetko koji primjerak zlonamjernih programa na društvenim mrežama koristi neki automatiziran način širenja za kojega nije potrebna interakcija korisnika. Zapravo, u praksi nije zabilježen niti jedan takav slučaj.

Automatizirano širenje obično se odvija iskorištavanjem neke poznate ili nepoznate ranjivosti u softveru kojega koristi moguća žrtva. Napadač razvija zlonamjerni program tako da on iskoristi ranjivost kako bi pokrenuo izvršnu datoteku na žrtvinom računalu. Ukoliko napadač koristi ranjivost u popularnom softveru on može zaraziti veliki broj računala potpuno neprimjetno. Problem za napadača je što mora pronaći ranjivost koja se može iskoristiti i što postoji mogućnost da ranjivost relativno brzo bude uklonjena ažuriranjem softvera.

S druge strane, širenje putem socijalnog inženjeringa temelji se na varanju korisnika. Napadač će pokušati nagovoriti korisnika da na svojem računalu pokrene izvršnu datoteku zlonamjernog programa. Iako će veliki broj korisnika prepoznati prijevaru, napadaču to ne smeta. Budući da na društvenim mrežama postoji mnogo korisnika, napadaču je dovoljno da prevari mali postotak njih i time osigura rasprostranjenost svojeg zlonamjernog programa.

Zlonamjerni programi se na društvenim mrežama šire u nekoliko koraka. Budući da se koraci stalno ponavljaju govorimo o ciklusu širenja zlonamjernih programa. Koraci su prikazani na sljedećem dijagramu.



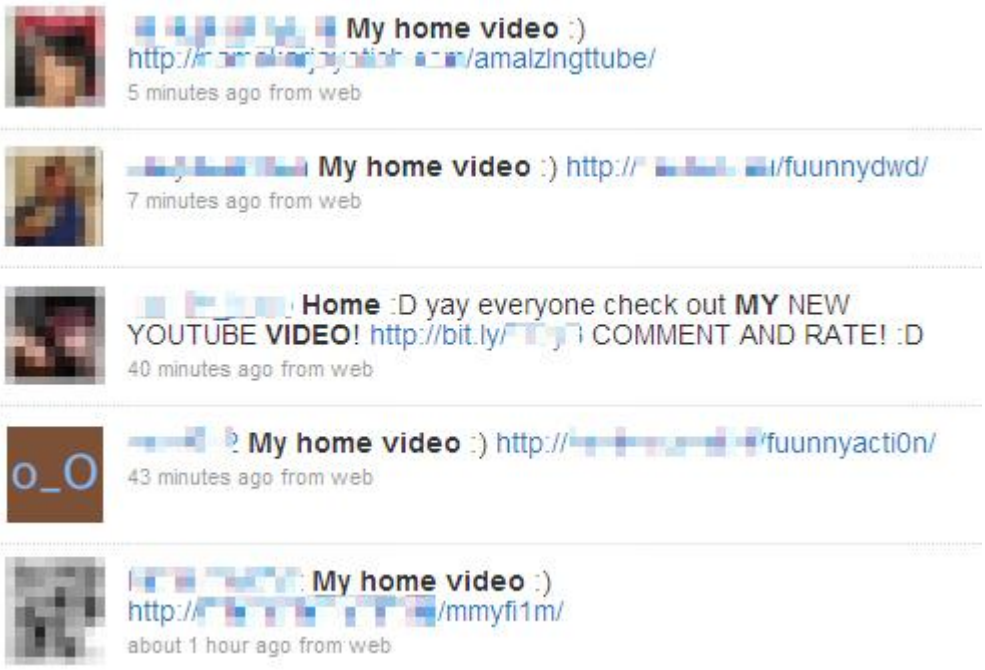
Slika 3.1 - Koraci širenja zlonamjernih programa na društvenim mrežama

Cijeli ciklus započinje kada korisnik na društvenoj mreži primi neku poruku. Ovdje nije riječ isključivo o porukama koje korisnik dobiva u svoj privatni pretinac. Poruke korisnik može dobiti na svoj zid (eng. *wall*) ili može pogledati poruku na zidu svojeg prijatelja.

Poruka redovito sadrži poveznicu na neku nepoznatu web stranicu. Uz poveznicu u poruci se nalazi i kratak tekst koji „pojašnjava“ o kakvoj poveznici je riječ. Tekst zapravo kod korisnika pobuđuje znatiželju da posjeti web stranicu na koju je dana poveznica. Neki primjeri teksta koji se često mogu naći u takvim porukama su:

- „Moj kućni video :)“ (eng. *My home video :)*)
- „Vidio sam te u ovom videu, pogledaj!“ (eng. *I saw your silly face in that movie*)
- „Jako smješno :D“ (eng. *Funny*)

Sljedeća slika prikazuje takvu poruku. Poruka na slici poslana je na društvenoj mreži Twitter.



Slika 3.2 - Zlonamjerna poruka poslana na Twitter

Izvor [1]

Web stranica koja se navodi u poruci imitira neki od popularnih servisa za dijeljenje video zapisa (najčešće youtube). Kada korisnik želi pogledati video, web stranica će ispisati poruku da je potrebno preuzeti i instalirati odgovarajući program za reprodukciju. Ovdje nije riječ o stvarnom programu za reprodukciju video zapisa već o zlonamjernom programu. Kada ga korisnik pokrene, njegovo računalo će biti zaraženo.

Zlonamjerni program koji je zarazio računalo korisnika će na razne načine pokušati ukrasti njegove lozinke za pristup svim društvenim mrežama koje on koristi. Ukoliko u tome uspije, program će na svim društvenim mrežama u ime žrtve slati poruke drugim žrtvama na već opisani način. Time je ciklus gotov. Nakon svakog punog ciklusa, zlonamjerni program zarazio je još jedno računalo.

Poruke koje zlonamjerni program šalje korisnicima dolaze od njihovih prijatelja i poznanika. Zbog toga veća je vjerojatnost da će neki korisnik slijediti poveznicu unutar primljene poruke.

Nažalost, zbog ovakvog načina širenja, više nije moguće u potpunosti vjerovati prijateljima na društvenim mrežama.

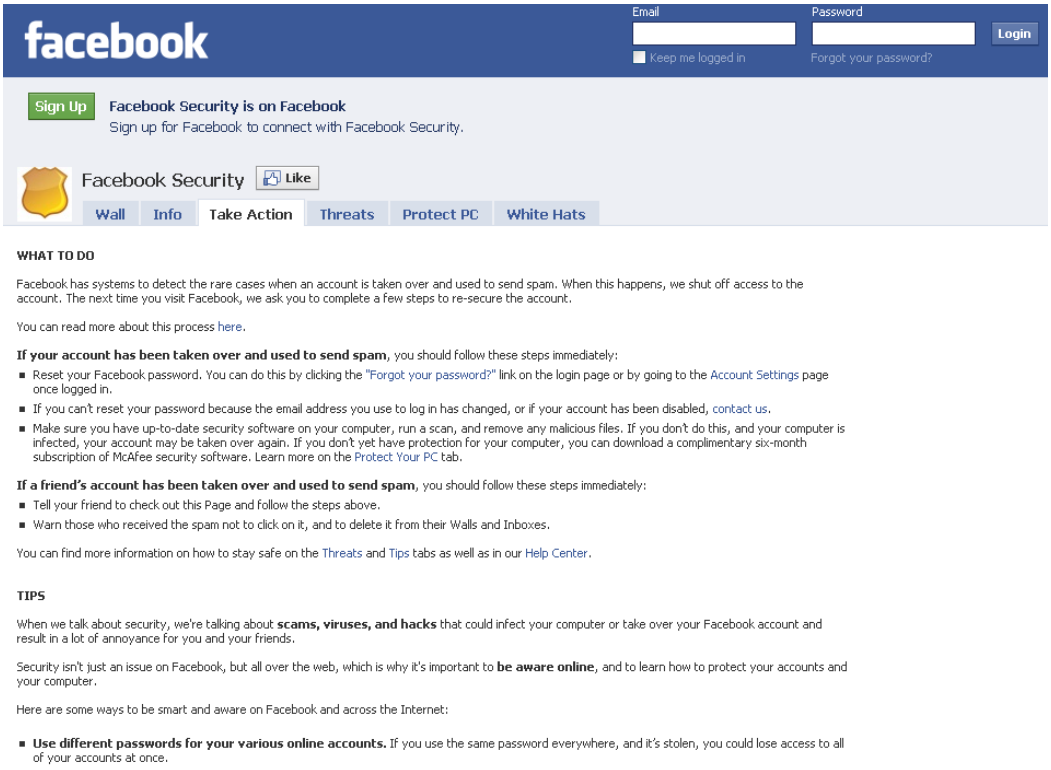
4 Zaštita na društvenim mrežama

Na početku svojeg razvoja društvene mreže bile su zaokupljene što većim rastom. U takvim uvjetima malo pažnje se posvećivalo privatnosti i zaštiti korisnika. Danas se osjećaju posljedice takvog postupanja u vidu pojave zlonamjernih programa i općeg osjećaja nesigurnosti na društvenim mrežama.

Iako su društvene mreže i danas prvenstveno usmjerene k rastu, nemoguće je poreći da su postale svjesnije svoje uloge u očuvanju sigurnosti vlastitih korisnika. Neki istraživači na području sigurnosti složiti će se kako ipak one ne ulažu dovoljno napora u rješavanje tog zadatka, ali neki pomaci su vidljivi. Društvene mreže pokušavaju povećati sigurnost korisnika na tri načina:

1. Edukacijom
2. Filtriranjem sadržaja
3. Suspenzija korisničkih računa

Edukacija korisnika odnosi se na objašnjenja vezana uz pojavu sigurnosnih prijetnji i savjete kako se zaštititi. Facebook i Myspace svojim korisnicima aktivno pokušavaju pružiti takvu edukaciju. Obje društvene mreže su dodale posebne dijelove o sigurnosti u sustav pomoći. Uz to, na njima je moguće pronaći i virtualne korisnike koji su dodani kako bi pravim korisnicima pomogli u sigurnom korištenju mreže. Sljedeća slika prikazuje savjete koji se mogu pronaći na Facebook-u.



Slika 4.1 - Sigurnosni savjeti na Facebooku

Facebook ima poseban centar za sigurnost na adresi www.facebook.com/security. Ondje je također moguće pronaći razne informacije o problemu zlonamjernih programa, spam porukama, *phishing* napadima i sl. Myspace ima posebnog virtualnog korisnika koji stvarnim korisnicima pomaže u pitanjima sigurnosti ili ih obavještava ukoliko netko s njihova računa pošalje *spam* poruke.

Druga mjera kojom društvene mreže pokušavaju povećati sigurnost svojih korisnika je **filtriranje sadržaja**. Facebook, Twitter i Myspace koriste filtriranje URL adresa koje korisnici izmjenjuju u porukama. Provjerava se svaka poruka koju neki korisnik pošalje, ukoliko ona sadrži poveznicu na poznatu zlonamjernu stranicu slanje poruke neće uspjeti, a korisnik će dobiti obavijest o tome.

Naravno, ovakvo filtriranje nije savršeno. Nove zlonamjerne stranice pojavljuju se svakodnevno i teško je održavati ažuriranu bazu svih poznatih zlonamjernih stranica.

Zadnji korak koje društvene mreže primjenjuju kako bi zaštitile svoje korisnike je **suspenzija zaraženih korisničkih profila.** Ukoliko neki korisnički račun šalje mnogo iznimno mnogo *spam poruka*, Twitter, Facebook i MySpace će ga blokirati kako bi spriječili moguće širenje zlonamjernih programa.

No, nije dovoljno osloniti se na sigurnosne mehanizme društvenih mreža. Svaki korisnik morao bi biti svjestan opasnosti na koje može naići prilikom korištenja društvenih mreža. Za poboljšanje vlastite sigurnosti dovoljno je slijediti nekoliko jednostavnih smjernica:

- Informirati se o novim prijetnjama i ne ignorirati sigurnosna upozorenja koje objavljuje društvena mreža.
- Ne slijediti sumnjive poveznice unutar poruka na društvenim mrežama.
- Koristiti redovito ažuriran antivirusni softver.

5 Koobface

Koobface, anagram riječi Facebook, naziv je za računalni crv koji se pojavio u prosincu 2008. godine. Četiri mjeseca kasnije pojavila se nova, znatno opasnija verzija tog crva. Koobface je prvi računalni crvi koji se uspješno i dugo širi po društvenim mrežama. On je pokazao da društvene mreže mogu biti opasne i pokrenuo je trend razvoja zlonamjernih programa koji se šire putem njih.

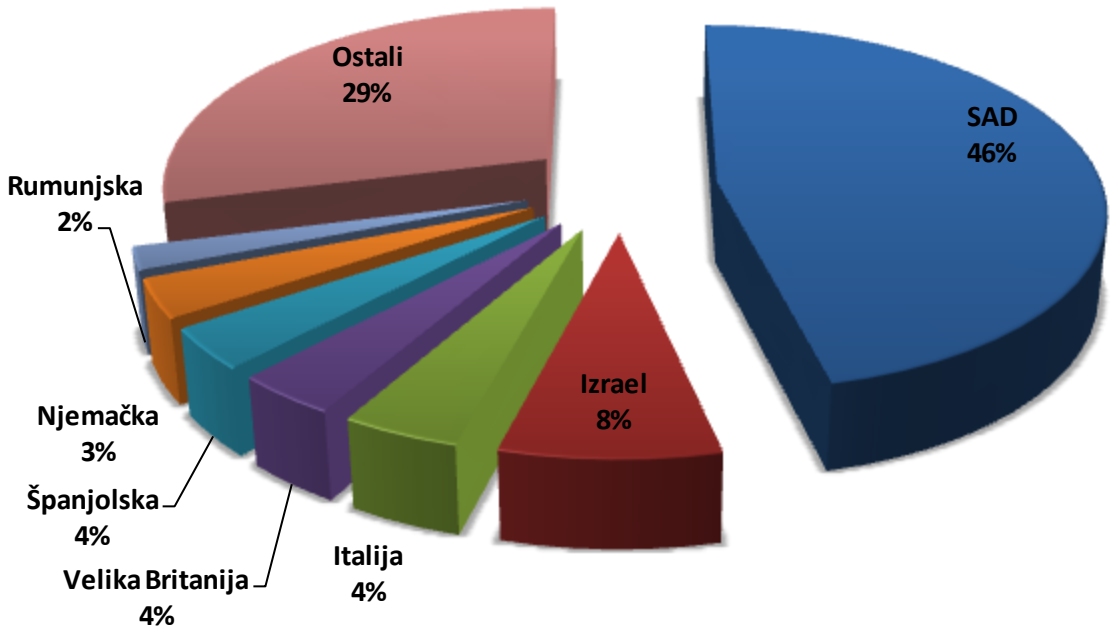
Osim toga, Koobface je poseban po svojoj komponetiziranoj arhitekturi. Dok većina zlonamjernih programa svoju funkcionalnost implementira unutar jedne izvršne datoteke, Koobface koristi mnoštvo različitih komponenata. Svaka komponenta ima određenu zadaću, a sve zajedno tvore jedan Koobface *botnet*. Sljedeća tablica prikazuje sve komponente Koobfacea.

Tabela 5.1 - Komponente Koobfacea

Komponenta	Opis
Komponenta za širenje.	Osigurava širenje putem različitih društvenih mreža.
Web poslužitelj	Pretvara zaraženo računalo u web poslužitelja s kojeg se poslužuju zlonamjerne stranice.
Komponenta za reklame	Prikazuje reklame žrtvi i preuzima lažne antivirusne alate s interneta.
Komponenta za razbijanje CAPTCHA-e	Žrtvi prikazuje CAPTCHA-u koju treba riješiti. Sva rješenja šalje kontrolnom poslužitelju.
Komponenta za preusmjeravanje pretraga.	Za svaku pretragu koju žrtva obavi putem popularnih tražilica ova komponenta vraća lažne rezultate.
Lažni DNS poslužitelj	Komponenta vraća lažne IP adrese za svaki DNS upit koji napravi zaraženo računalo.
Komponenta za krađu podataka	Komponenta krade privatne podatke žrtve i šalje ih napadaču.
Komponenta za krađu licenci	Komponenta krade licence za softver s zaraženog računala.

Gotovo svaka od ovih komponenti implementirana je u nekoliko različitih izvršnih datoteka ili dinamičkih biblioteka. Ovako veliki broj komponenti Koobfaceu daje iznimnu fleksibilnost. Ukoliko njegov autor želi promijeniti funkcionalnost crva, može poboljšati samo jednu komponentu, pri tome ne mijenjajući ostale. Takva poboljšanja zahtijevaju manje vremena i resursa. Zbog toga su stručnjaci u [2 str. 4] zaključili kako je „Koobface *botnet* stalno u fazi razvoja i promjena koje proširuju njegovu funkcionalnost. Cijeli Koobface više je od sume svojih dijelova i pokretna je meta za antivirusne stručnjake.“

Broj računala zaraženih Koobfaceom procjenjuje se na 60 000. No, broj treba uzeti s rezervom. Zbog fleksibilne prirode Koobfacea teško je dati točnu procjenu. Sljedeći graf prikazuje udio pojedinih zemalja u broju zaraženih računala.

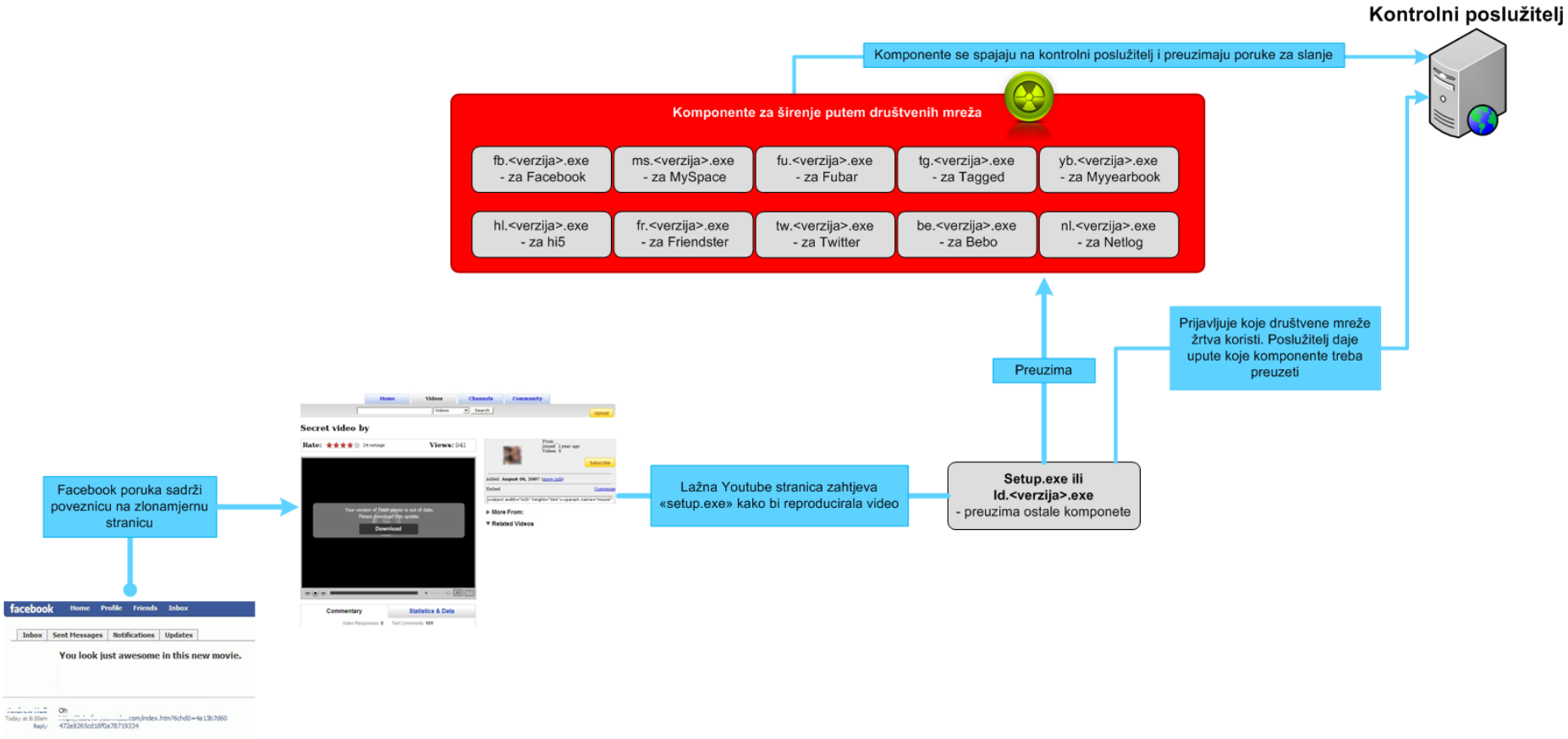


Slika 5.1 - Udio pojedinih zemalja u broju zaraženih računala

Očekivano, u SAD-u se nalazi daleko najveći broj zaraženih računala. Ostale zemlje dijele tek neznatne postotke. Razlog tomu je što najviše korisnika društvenih mreža s područja engleskog jezika dolazi iz SAD-a.

5.1 Komponenta za širenje na društvenim mrežama

Koobface se na društvenim mrežama širi kroz interakciju korisnika. On šalje veliki broj poruka korisnicima u kojima ih upućuje na gledanje video zapisa na stranici koja imitira YouTube. Ukoliko korisnik želi pogledati video zapis on prvo mora preuzeti datoteku `setup.exe` i pokrenuti ju. Navedena datoteka će korisnikovo računalo zaraziti Koobfaceom. Proces inficiranja i širenja putem društvenih mreža prikazan je na sljedećoj slici.



Slika 5.2 - Prikaz širenja Koobface-a

Izvor [4 str. 2]

`Setup.exe` ne sadrži funkcionalnost Koobfacea. Njegova osnovna zadaća je preuzimanje i instalacija drugih komponenti na računalo žrtve. `Setup.exe` svoju zadaću ispunjava u tri koraka:

1. Sastavlja listu svih društvenih mreža koje korisnik posjećuje
2. Listu šalje kontrolnom poslužitelju
3. Od kontrolnog poslužitelja prima upute koje komponente treba preuzeti i instalirati na računalo žrtve.

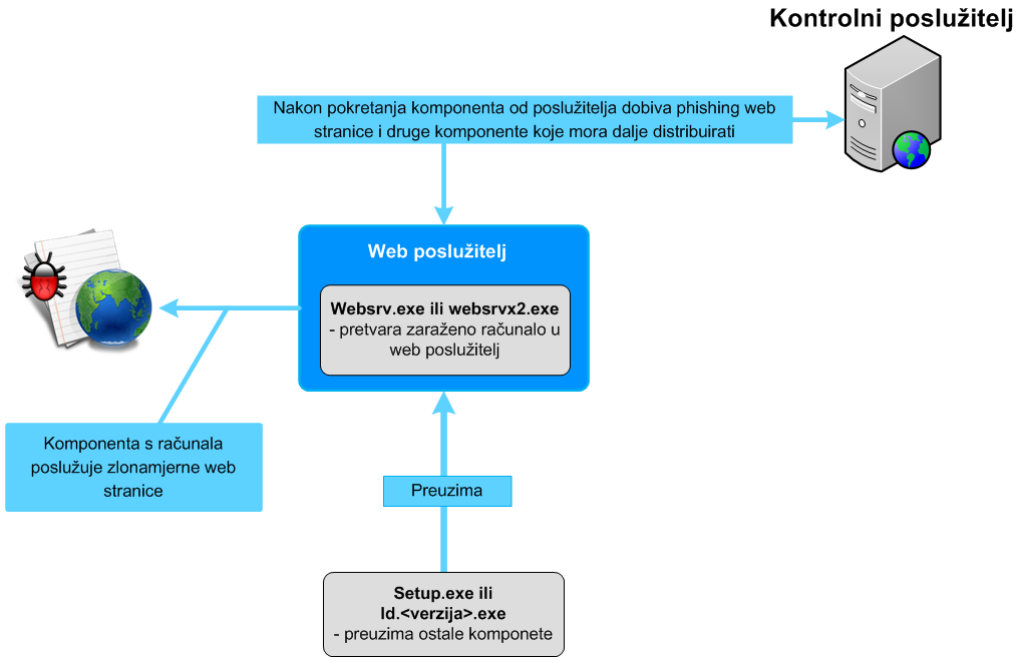
Kako bi ustanovio koje društvene mreže korisnik posjećuje, `setup.exe` će pretražiti sve web *cookie* koje se nalaze na tvrdom disku zaraženog računala. Ukoliko otkrije neki *cookie* koji odgovara društvenoj mreži, program zaključuje da žrtva koristi tu društvenu mrežu.

Kako je na slici prikazano, Koobface se može širiti putem mnogo različitih društvenih mreža. To jedan od razloga zašto je Koobface uspio zaraziti tako veliki broj računala. O fleksibilnosti crva svjedoči činjenica da na računalo žrtve instalira samo one komponente koje su potrebne.

Iako za svaku društvenu mrežu postoji zasebna izvršna datoteka, sve one imaju istu funkcionalnost. Šalju *spam* poruke drugim korisnicima. Kontrolni poslužitelj određuje sadržaj koji poruke moraju imati.

5.2 Web poslužitelj komponenta

Koobface ima komponentu koja zaraženo računalo pretvara u web poslužitelj. Nakon instalacije, komponenta obavještava kontrolni poslužitelj kako je započela s radom. Osim toga, komponenta kontrolni poslužitelj izvještava o tome koliko dugo radi.



Slika 5.3 - Koobfaceov web poslužitelj

Kontrolni poslužitelj će komponentu koristiti za posluživanje zlonamjernih web stranica. Riječ je o lažnim YouTube web stranicama koje nagovaraju korisnika na pokretanje zlonamjerne

`setup.exe` datoteke. Osim zlonamjernih web stranica zaraženo računalo posluživat će i ostale komponente Koobface crva.

Izvršna datoteka web poslužitelja nosi naziv `websrv.exe` ili `websrvx2.exe`. Prisutnost tih datoteka na računalu može biti indikator zaraženosti Koobfaceom.

5.3 Komponenta za reklame i razbijanje CAPTCHA-e

Putem zasebne komponente za reklamu, Koobface žrtvi prikazuje različite reklame za sumnjive proizvode. Popis reklama koje treba prikazati komponenta dobiva od kontrolnog poslužitelja. Ova komponenta žrtvama pokušava instalirati i lažni antivirusni softver.

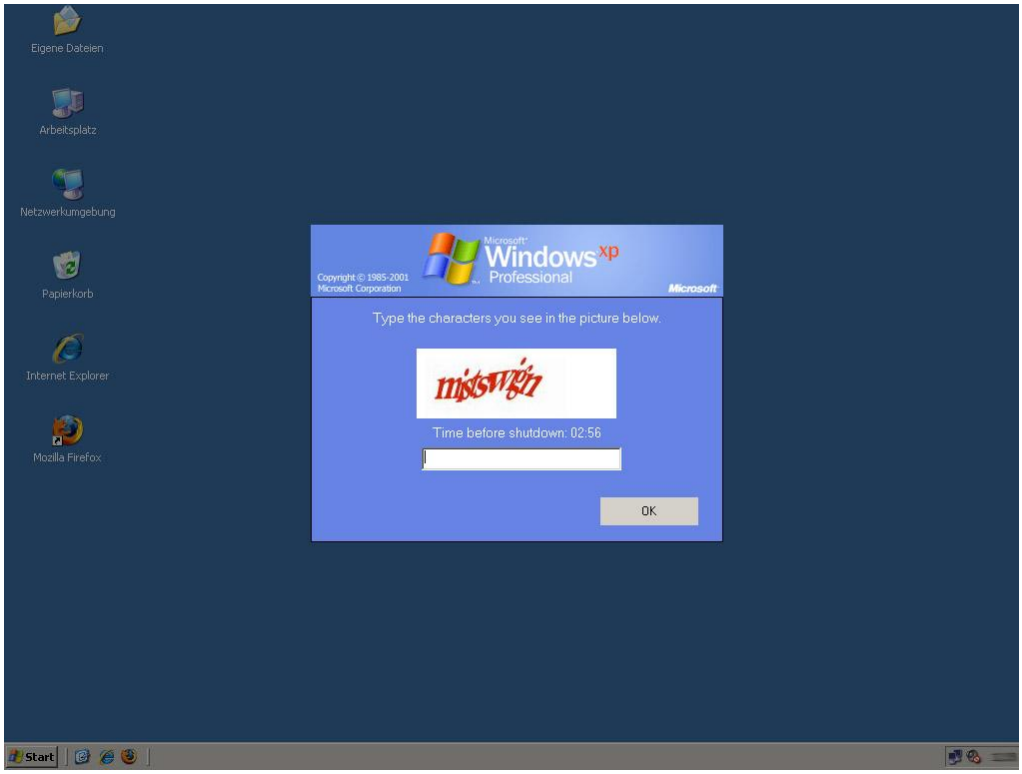
Prodavanje lažnog antivirusnog softver jedan je od izvora financiranja kriminalaca koji šire Koobface. Komponenta žrtvama prikazuje prijeteće poruke koje ju informiraju o tome kako joj je računalo zaraženo različitim virusima i trojanskim konjima. Žrtvi se savjetuje da kupi antivirusni softver kako bi uklonio zarazu i zaštitio vlastito računalo. Riječ je o lažnom antivirusnom alatu koji je zapravo prikriveni zlonamjeran program.

Još jedna u nizu mnogih mogućnosti Koobfacea je razbijanje CAPTCHA-e. CAPTCHA je tip provjere kojom se pokušava osigurati da jedna strana u komunikacijskom kanalu nije računalo, već čovjek. Kod ove provjere jedna strana obično šalje male slike na kojoj je prikazan iskrivljen tekst drugoj strani. Prva strana potom od druge traži da joj pošalje tekst sa slike. Pretpostavka je da čovjek neće imati poteškoća u prepoznavanju teksta, a računalo to neće moći napraviti budući da ne postoji dovoljno dobar algoritam koji bi mogao prepoznati takav, iskrivljeni, tekst.

Društvene mreže koriste CAPTCHA provjere kod slanja većeg broja poruka. Ukoliko korisnik šalje poruke na društvenim mrežama, morati će proći CAPTCHA provjeru kako bi društvena mreža bila sigurna da nije riječ o automatskom slanju poruka koje provodi neki računalni program. Time se pokušava ograničiti širenje *spam* poruka.

Umjesto naprednih algoritama za rješavanje CAPTCHA provjera, Koobface taj posao prepušta svojim žrtvama. Za tu svrhu on ima posebno dizajniranu komponentu koja korisnicima prikazuje CAPTCHA slike koje moraju riješiti.

Komponenta slike preuzima od kontrolnog poslužitelja. Nakon što preuzme sliku, komponenta žrtvi prikazuje poruku kako će joj računalo biti ugašeno ukoliko ne riješi CAPTCHA provjeru. Poruka je prikazana na sljedećoj slici.



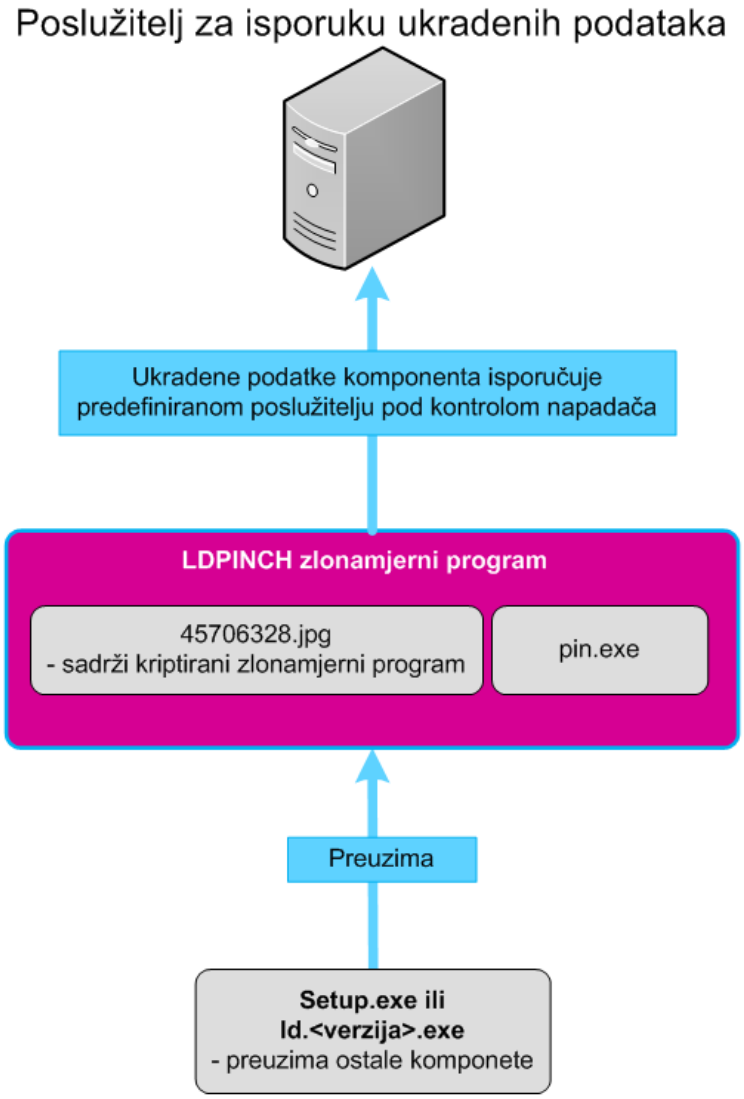
Slika 5.4 - Poruka korisniku za rješavanje CAPTCHA-e

Koobface neće ugasiti računalo ni nakon isteka vremena, već će pričekati žrtvu da riješi CAPTCHA sliku. Također, Koobface ne provjerava da li je korisnik upisao ispravno rješenje budući da ni on sam ne zna koje je rješenje ispravno.

Kada korisnik upiše rješenje Koobface će rezultat poslati kontrolnom poslužitelju. Na ovaj način Koobface može vrlo brzo riješiti gotovo bilo koji CAPTCHA test bez uporabe naprednih algoritama za prepoznavanje slova. Što više računala zarazi, to će više CAPTCHA testova riješiti, a to mu omogućuje da zarazi još više računala.

5.4 Komponente za krađu podataka, preusmjeravanje web pretraga i DNS upita

Koobface krade privatne podatke s zaraženog računala. U prvom redu to se odnosi na korisnička imena i lozinke za različite servise. Za krađu podataka koristi primjerak iz TROJ_LDPINCH grupe zlonamjernih programa. Riječ je o dobro poznatoj skupini zlonamjernih programa, koji su prvi puta otkriveni 2003. godine. Bez obzira na to, Koobface ih uspješno koristi kako bi krao podatke s zaraženog računala.



Slika 5.5 - Koobface krade žrtvine povjerljive podatke

Primjerci iz te grupe zlonamjernih programa dizajnirani su za krađu korisničkih imena i lozinki iz popularnog softvera. Neki od softvera od kojih se podaci kradu su:

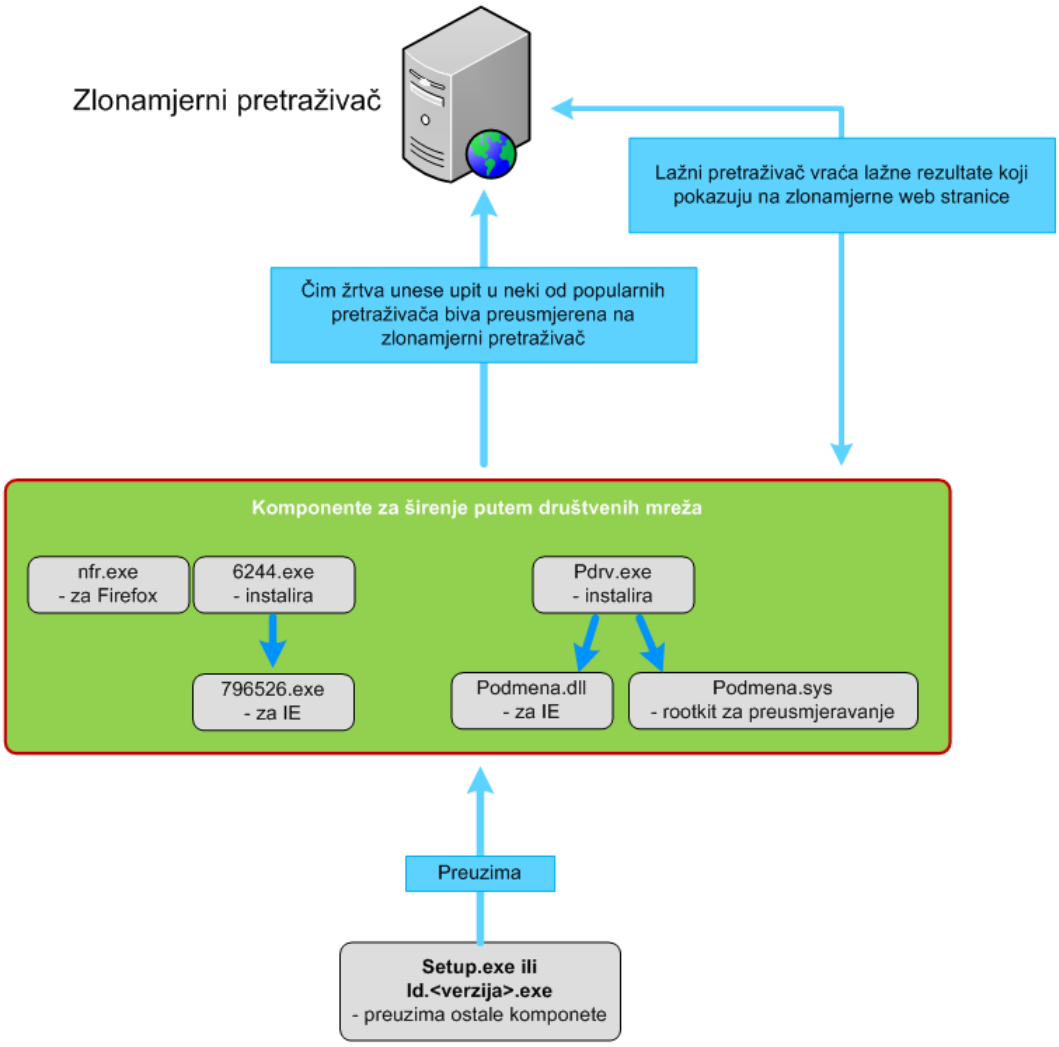
- FileZilla
- Mozilla Thunderbird
- Internet Explorer
- ICQ

- Trillian
- cuteFTP
- …

Svi podaci koje ova komponenta prikupi isporučuju se na predodređeni poslužitelj kojeg kontrolira napadač. Taj predodređeni poslužitelj ne mora biti isti kao Koobfaceov glavni kontrolni poslužitelj. Ova komponenta ukradene podatke može slati na bilo koju lokaciju.

Zanimljivo je da izvršna datoteka u kojoj je implementirana komponenta dolazi unutar .jpg datoteke. To je još jedan od načina kojim Koobface pokušava izbjeći detekciju.

Koobface također preusmjerava sve web pretrage koje obavlja žrtva. Komponenta za preusmjeravanje pretraga prepoznaje web pretrage upućene na Google, Yahoo, MSN, Ask ili Live. Svaki zahtjev koji žrtva uputi na neki od tih pretraživača biti će preusmjeren na zlonamjerni pretraživač koji je pod kontrolom napadača.

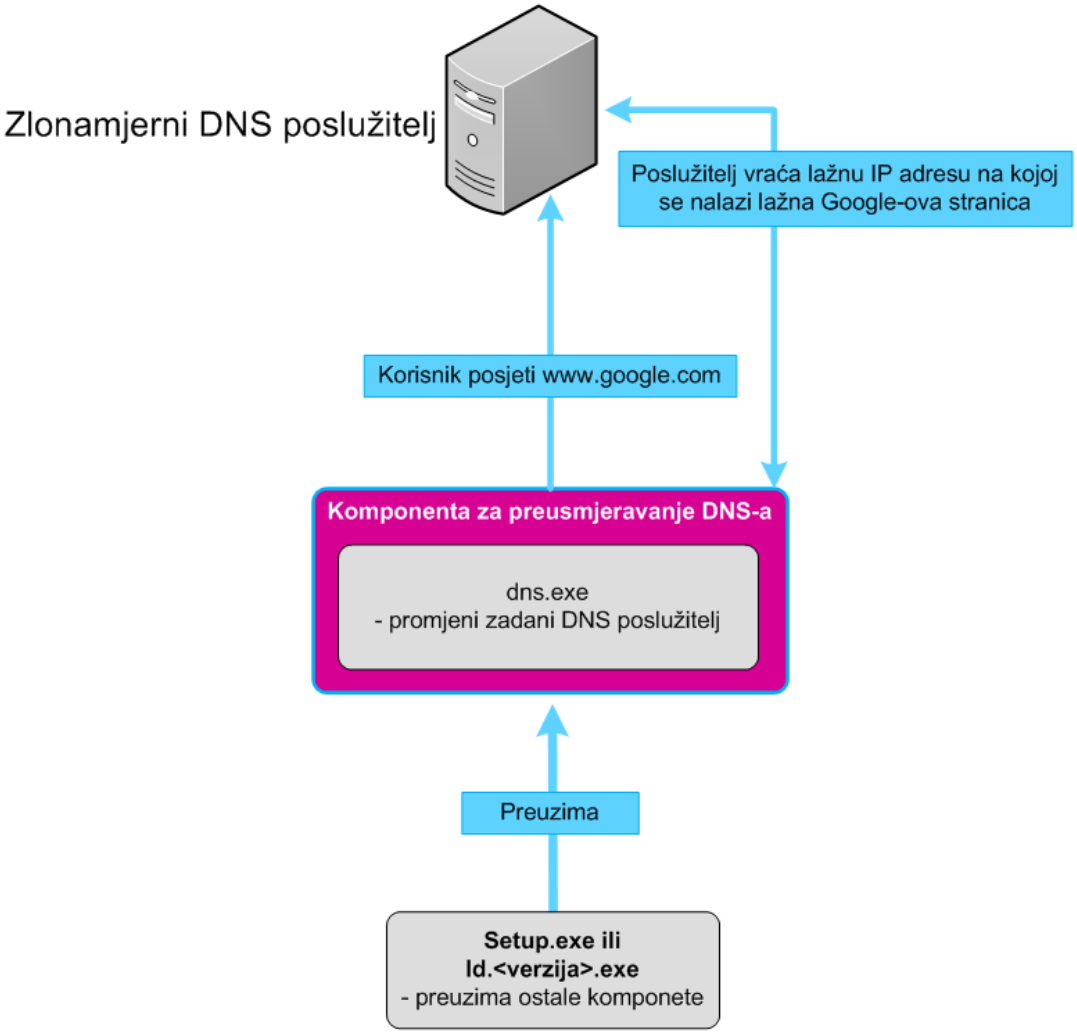


Slika 5.6 - Koobface preusmjerava sve pretrage koje žrtva obavlja

Pretraživač će korisniku kao rezultat pretrage prikazati zlonamjerne web stranice koje sadrže brojne reklame i pokušavaju s žrtvinog računala ukrasti privatne podatke.

Koobface trenutno podržava preusmjeravanje web pretraga unutar Firefoxa i Internet Explorera. Za svaki preglednik postoji posebna verzija izvršne datoteke koja implementira funkcionalnost preusmjeravanja. Kod Internet Explorera riječ je o datoteci `podmena.dll`[2], a kod Firefoxa o datoteci `nfr.exe`. Ove dvije datoteke se oslanjaju na upravljački program `podmena.sys` koji unutar jezgre Windows operacijskog sustava preusmjerava mrežni promet na zlonamjerni pretraživač.

Osim preusmjeravanja web pretraga, Koobface na žrtvinom računalu preusmjerava sve DNS upite. Za to preusmjeravanje opet postoji zasebna komponenta koja na zaraženom računalu mijenja IP adresu glavnog DNS poslužitelja.



Slika 5.7 - Koobface i lažni DNS poslužitelj

Komponenta će računalo podesiti tako da za sve DNS upite koristi zlonamjerni DNS poslužitelj koji je pod kontrolom napadača. Na taj način napadač dobiva kontrolu nad web mjestima koje korisnik posjećuje. On može podesiti DNS poslužitelj da vraća lažne IP adrese za bilo koju domenu koju korisnik posjećuje. Time napadač može provesti opasne `phishing` napade ili žrtvi blokirati pristup bilo kojem web mjestu. Napadači to često koriste kako bi blokirali pristup do antivirusnih alata ili stranica koje se bave informacijskom sigurnošću.

[2] Podmena je riječ u ruskom jeziku koja se može prevesti kao „preusmjeravanje“

6 Zaključak

Zbog velikog broja korisnika i naglog rasta zlonamjerni programi su se proširili po društvenim mrežama. Statistike jasno pokazuju kako su korisnici u opasnosti i da je nužan oprez prilikom korištenja svih mogućnosti društvenih mreža.

Kriminalci će učinit sve kako bi proširili svoje zlonamjerne programe na što više računala i time sebi osigurali zaradu. Svjedok tome je i Koobface, izrazito fleksibilan i kompleksan primjerak zlonamjernog programa. Sa svojom komponetiziranom arhitekturom i brojnim modulima Koobface uspješno odolijeva naporima antivirusne industrije da ga neutralizira.

U obrani od takvih zlonamjernih programa nužna je suradnja svih strana – korisnika, društvenih mreža i antivirusnih kompanija. Prva crta obrane mora biti edukacija i podizanje razine svijesti o izvorima prijetnji i načinu širenja zlonamjernih programa. Važno je odrediti jasne smjernice za sigurno postupanje te poticati korisnike, ali i društvene mreže da ih provode.

7 Literatura

[1]. **Sophos.** *Sophos Security Threat Report: 2010.* s.l. : Sophos, 2010.

[2]. **TrendMicro.** Koobface message. *Koobface message.* [Mrežno] TrendMicro. [Citirano: 30. 6 2010.] http://www.trendmicro.com/vinfo/images/blog/twitter-spam-2.jpg.

[3]. **Baltazar, Jonell, Costoya, Joey i Flores, Ryan.** *The Heart of KOOBFACE C&C and Social Network Propagation.* s.l. : Trend Micro Research Paper, 2009.

[4]. —. *The Real Face of KOOBFACE: The Largest Web 2.0 Botnet Explained.* s.l. : Trend Micro Threat Research, 2009.

[5]. **M86 Security.** *M86 Security Labs Report.* s.l. : M86 Security, 2010.

[6]. **LeClaire, Jenifer.** Social Networking Sites in the Crosshairs? *Technology News.* [Mrežno] TechNewsWorld, 1. 3 2007. [Citirano: 30. 5 2010.] http://www.technewsworld.com/story/54932.html?wlc=1277800091.

[7]. **Sophos.** Malware and spam rise 70% on social networks. *Sophos.* [Mrežno] Sophos, 1. 2 2010. [Citirano: 30. 6 2010.] http://www.sophos.com/pressoffice/news/articles/2010/02/security-report-2010.html.

[8]. **Gallagher, Sean.** Social Networks a Magnet for Malware. *Internetnews.com.* [Mrežno] Internetnews, 17. 2 2009. [Citirano: 30. 6 2010.] http://www.internetnews.com/bus-news/article.php/3803051/Social-Networks-a-Magnet-for-Malware.htm.

[9]. **Cluley, Grahm.** More Mikeyy worm madness on Twitter. *Graham Cluley's blog.* [Mrežno] 13. 4 2009. [Citirano: 30. 6 2010.] http://www.sophos.com/blogs/gc/g/2009/04/13/mikeyy-worm-madness-twitter/.

[10]. **Arrington, Michael.** MySpace Is In Real Trouble If These Page View Declines Don't Reverse. *TechCrunch.* [Mrežno] TechCrunch, 18. 5 2009. [Citirano: 30. 6 2010.] http://techcrunch.com/2009/05/18/myspace-is-in-real-trouble-if-these-page-view-declines-dont-reverse/.