ŠOLSKI CENTER VELENJE
ELEKTRO IN RAČUNALNIŠKA ŠOLA
Trg mladosti 3, 3320 Velenje

MLADI RAZISKOVALCI ZA RAZVOJ ŠALEŠKE DOLINE

RAZISKOVALNA NALOGA

STOP, VSILJIVEC!

Tematsko področje: RAČUNALNIŠTVO

Avtorji:
Nives Bricman, 4. letnik
Blaž Blažinčič, 4. letnik
Aljaž Duh, 4. letnik

Mentorja:
Islam Mušić, prof.
Ajda Kamenik, univ. dipl. sociol.

VELENJE, 2011/2012

Raziskovalna naloga je bila izdelana na ŠC Velenje, Elektro in računalniška šola, 2012.

Mentorja: Islam Mušić, prof.
Ajda Kamenik, univ. dipl. sociol.

Datum predstavitve:

KLJUČNA DOKUMENTACIJSKA INFORMACIJA

ŠD Elektro in računalniška šola Velenje, 2011/2012

KG hekanje / računalniški vsiljivec / zlonamerni programi

AV BRICMAN, Nives; BLAŽINČIĆ, Blaž; DUH, Aljaž

SA MUŠIĆ, Islam; KAMENIK, Ajda

KZ 3320 Velenje

ZA ŠC Velenje, Elektro in računalniška šola, Trg mladosti 3, Velenje

LI 2012

IN STOP, VSILJIVEC!

TD Raziskovalna naloga

OP V, 10 s., 9 graf., 12 ref.

IJ sl

JI sl/en

AI Dandanes nas internet in njegove storitve spremljajo povsod. Zavedati se moramo nevarnosti, ki nas lahko doletijo pri uporabi spleta. Še bolj pomembno pa je to, kako ravnati v teh primerih in preprečiti posledice. Zanimala nas je osveščenost uporabnikov – kakšen je njihov odziv oziroma ali sploh prepoznajo potencialne grožnje. Z anketo, napisano v programskem jeziku C#, prevedeno v izvršljivo datoteko, smo želeli potrditi eno izmed hipotez, da si uporabniki interneta na svoj računalnik nameščajo programe, ki utegnejo biti škodljivi. Vsaka rešena anketa je dokaz, da je program (v našem primeru anketa) pristal na računalniku. Ob analiziranju smo ne glede na vse ugotovili, da se tudi v realnosti še najdejo taki ljudje, ki bi lahko nasedli internetni prevari. Šli smo še dlje, pripravili smo lažno spletno stran socialnega omrežja Facebook. Želeli smo se prepričati, koliko ljudi je pozornih na URL naslove, preden svoje podatke posredujejo spletnim stranem. V bazo smo shranili elektronski naslov in prvo črko gesla, ostalo smo nadomestili z zvezdico. Na temo varnosti na internetu smo posneli še film. V njem smo želeli prikazati primer identične spletne strani Facebooka. V posnetku heker pretenta nevednega uporabnika, ki mu posreduje svoje podatke.

KEY WORDS DOCUMENTATION

ND Elektro in računalniška šola Velenje, 2011/2012

CX hacking / computer intruder / malicious software

AU BRICMAN, Nives; BLAŽINČIĆ, Blaž; DUH, Aljaž

AA MUŠIĆ, Islam; KAMENIK, Ajda

PP 3320 Velenje

PB ŠC Velenje, Elektro in računalniška šola, Trg mladosti 3, Velenje

PY 2012

TI YOU GOT HACKED!

DT Research work

NO V, 10 p., 9 fig., 12 app.

LA sl

AL sl / en

AI Nowadays the internet and its services accompany us everywhere. We must be aware of the potential threat, which can occur when using the web. It is even more cruical how we behave in these situations and how we prevent consequences from happening. Our interest was the users awareness – what is their response, do they even recognize the potential threat. With a C# programmed survey (therefore an executable file), we wanted to confirm a hypothesis that internet users install malicious software on their computers. Every answered survey is a proof that the software (in this case the survey) was successfully installed on the user's computer. While analyzing, we realized that no matter what, unaware users still exists. We progressed even further. We prepared a phishing website for the social network Facebook. We wanted to see, how many users check the URL for any suspicions before entrusting their personal information to the website. We stored the email adress and first letter of the individual's password and we replaced others with the star symbol. We also made a movie relying on the safe internet. In it we demonstrated a case, where a hacker tricks a careless internet user by stealing his personal information through an identical Facebook site.

KAZALO

KAZALO GRAFIKONOV IN SLIK

Kazalo slik

Kazalo grafikonov

1 UVOD

V preteklosti so bili podatki shranjeni na papirju. Zasebnost je bila dostopna, če smo mi ali nekdo drug do nje prišli fizično. To je bilo pred digitalno dobo. Začela se je uporaba računalnikov, podatki so prešli v digitalno obliko. Kmalu se je razvil tudi internet, ki je storitvam kot so bančništvo, zdravstvo in trgovstvo omogočil boljšo komunikacijo s potrošniki. Navadnim uporabnikom je olajšal iskanje virov, omogočil komunikacijo z ljudmi po svetu, prihranil kakšen denar in tudi korak. Ni več nujno potrebno, da vzamemo v roke pisalo, napišemo pismo, nanj prilepimo znamko in ga vržemo v poštni nabiralnik. Prav tako nam ni potrebno po več dni čakati na odgovor. Sedaj lahko večino stvari naredimo kar doma – preko računalnika. Ni nam potrebno hoditi na banko in plačevati položnic, kupujemo lahko na spletu in pošto prejmemo na dom. Pa je postal internet tudi vir zasebnih informacij?

Vsi smo že kdaj bili v stiku z lažnimi spletnimi stranmi, ki so nam ponujale določene nagrade ali pa so od nas pričakovale določene informacije. Mogoče smo na poštni naslov dobili pošto neznanca v katerem je pisalo: »Zadeli ste določen znesek...«. Naivni ali ne, koga ne premami. Moramo vedeti, da se za internetom skriva polno ljudi, ki si na takšen ali drugačen način želijo dobička.

Izbrali smo si zanimivo, a hkrati tudi zelo konfliktno temo. Ves čas smo se spraševali, do katere meje nam je sploh dovoljeno iti. Naša želja je bila, da bi se bolj posvetili »pravemu« hekanju, a smo bili v skrbeh, da nam bo ilegalnost teme omejila možnosti za podrobnejše raziskovanje. Odločili smo se, da se hekanja samo bežno dotaknemo. Začeli smo se spraševati, koliko ljudi je sploh seznanjenih z nevarnostmi, ki nas lahko doletijo na internetu, kakšna je njihova preventiva in, ali sploh prepoznajo internetno prevaro. Razmišljali smo, da bi velikokrat zaradi nepazljivost tudi sami lahko nasedli.

1.1 Hipoteze

H1: Ljudje se ne prepričajo o pristnostni URL naslovov, zato lahko hitro postanejo žrtve hekerjev, ki želijo z izdelavo lažne (navzven identične) spletne strani prevarati uporabnika.

H2: Uporabniki spleta zaupajo spletnim stranem, ki jih na različne načine prepričujejo, da si na računalnik prenesejo določene programe.

H3: Gesla posameznih uporabnikov, ki jih uporabljajo pri prijavah na različne spletne strani ali aplikacije, so v večini primerov vedno ista.

2 PREGLED OBJAVLJENEGA GRADIVA

O različnih prevarah na internetu in o subkulturi hekerjev je že veliko objavljenega. Poudarek je predvsem na zaščiti, kako preprečiti vdore in se s tem izogniti kraji osebnih podatkov. Naše raziskovanje se je začelo z listanjem knjige Ivana Verdonika in Tomaža Bratuše, z naslovom Hekerski vdori in zaščita. V knjigi je veliko informacij o hekerskih orodjih in metodah. Prisiljeni smo se bili pozanimati o novih izrazih, tako na področju hekanja kot tudi na področju zaščite. Pri čemer nam je veliko pomagal Leksikon računalništva in informatike, glavnih avtorjev Davida Pahorja in Matije Drobniča.

2.1 O hekerjih

»V zadnjem času izraz označuje predvsem vdiralce v sisteme, katerih priljubljena zabava je vdiranje v različne računalniške sisteme po računalniških omrežjih in javnem telefonskem omrežju. Četudi gre večinoma za početje brez zlih namenov, vse več držav že sam vdor v sistem obravnava kot kaznivo dejanje. Obenem poskušajo njihovo delovanje preprečiti s postavljanjem zaščitnih strežnikov.« (1)

Izraz označuje vdiralce v sisteme. Hekerji so člani programerske subkulture, ki se poglabljajo v programiranje z veliko znanja o delovanju računalnikov, sistemov in računalniških mrež, medtem ko se navadni uporabniki zadovoljijo le z minimalnim znanjem. Lahko jih razdelimo v dve skupini – dobre in zlonamerne hekerje. Prvi svoje znanje uporabljajo, da pomagajo odkriti in popraviti varnostne luknje. Zlonamerni vdiralci pa pišejo programsko kodo in ilegalno dostopajo do računalniških sistemov z namenom, da bi drugim uporabnikom povzročali težave, sebe pa okoristili.

2.1.1 Etični hekerji

»Etični heker je strokovnjak za računalnike in omrežja, ki s svojim znanjem poskuša odkriti pomanjkljivosti v sistemu preden jih zlorabi black hat. Etičnemu hekerju rečemo tudi white hat heker. Izraz izhaja iz starih kavbojskih filmov, kjer so dobri kavboji nosili beli klobuk, slabi pa črnega. Razlika med black in white hat je, da black hat uporablja svoje znanje za vdiranje v računalniške sisteme z namenom koristoljubnosti, medtem ko white hat prav tako vdira v računalniške sisteme, toda z namenom odkrivanja varnostnih pomanjkljivosti, ki jih ne izkoristi v svojo korist, problem sporoči podjetju katerega varnost preverja. Podjetje tako lahko pomanjkljivosti pokrpa preden jih zlorabi black hat heker.« (3)

Ponavadi podjetje kontaktira hekerja z določenim certifikatom s prošnjo, da bi jim ta preveril, če njihov sistem vsebuje varnostne luknje. Varnostni pregled poteka v sledečih korakih: zbiranje informacij o omrežju, skeniranje omrežja za ugotovitev uporabljenih aplikacij, napad na aplikacije, ohranitev dostopa do sistema in izdelava poročila. Na koncu heker pošlje poročilo podjetju, ne da bi podjetje vedelo kako je dostopal do njihovih podatkov.

2.1.2 Anonymous

Vprašanje ni, kdo je Anonymous ampak, kaj je Anonymous. Anonymous je kolektiv ljudi iz celega sveta, ki so kljub različnim interesom, mnenjem in prepričanjem združeni pod eno skupno željo - po resnični svobodi in svetu brez zatiranja. Anonymous nima vodje, nima obraza, niti izbranih govorcev, ker vsi člani predstavljajo celoto. V zadnjem času so bili velikokrat omenjeni v medijih.

Ideja Anonymous se je začela leta 2003 na strani 4chan.org, na kateri je imel vsak uporabnik vzdevek anonimnež oziroma »anonymous«. V zgodnjih začetkih je bil ta kolektiv ljudi usmerjen v internetno zabavo. V začetku leta 2008 so postali vedno bolj usmerjeni v kolaboracijo in protestiranje. Postali so začetniki mednarodnega hektivizma (hekerski aktivizem). Nasprotovali so predvsem akcijam, ki so želele ustaviti internetno piratstvo. Trenutno se kolektiv Anonymous bori proti korupciji, kriminalu belih ovratnikov, proti cenzuriranju interneta in informacij.

Njihova največja akcija je bila pomoč Wikileaksu pri odkrivanju sumljivih dokumentov domnevne korupcije. Vdrli so v podjetji Visa in Mastercard po tem, ko sta podjetji prenehali s sodelovanjem in nista hoteli izplačati donacij, ki so bile namenjene Wikileaksu. Skupina Anonymous jim je v protestu zaustavila strežnike. Njihovo mnenje je bilo, da če želijo ljudje donirati denar Wikileaksu, banka ne more zavrniti izplačitev teh donacij. Strinjali so se z idejo Wikileaksa o transparentnosti in svobodi informacij.

Anonymous je odgovoren za razkritje avtorjev več stotih podatkovnih baz z otroško pornografijo. Vsa imena in dokaze so posredovali policiji, ki je kazensko ovadila vse odgovorne.

Slika 1: Zastava Anonymous

2.1.3 Facebook Hacker Cup

Je letno svetovno tekmovanje, kjer vdiralci tekmujejo drug proti drugemu za prepoznavnost in denar. Prvo tekmovanje je potekalo leta 2011 z namenom, da bi prepoznali inženirske talente, ki bi lahko postali uslužbenci Facebooka. Prvenstvo vsebuje set algoritmičnih problemov, ki morajo biti rešeni v določenem času. Tekmovalci lahko uporabijo katerikoli programski jezik in katerokoli razvojno okolje, da pridejo do rešitve. Prvega tekmovanja se je udeležilo 11000 ljudi iz vsega sveta. Zmago si je prislužil Petr Mitrichev iz Rusije.

2.2 Metode hekanja

Verižna sporočila
So sporočila, ki z moralnimi grožnjami (nesreča, smrt) pozivajo posameznika, da posreduje sporočilo ljudem v določenem času. Pred digitalno dobo je pošiljanje verižnih sporočil potekalo preko pisem. Sedaj se te vrste sporočil izvršujejo preko elektronske pošte. Hekerji lahko verižna sporočila uporabijo kot vabo za uporabnike, da jim izdajo osebne podatke.

Lažno predstavljanje ali ribarjenje (angl. »phishing«)
»Napad temelji na tem, da napadalec podtakne URL-povezavo (ki jo skrije v elektronsko pošto ali drugo spletno stran). Če kliknemo nanjo, se spletna stran, na katero je kazala povezava, namesti v naš brskalnik. V tej strani napadalec skriva skriptno kodo, ki se v našem brskalniku izvede in nemara ogrozi naš sistem – skriptni jeziki so namreč vedno močnejši in omogočajo klice mnogih funkcij, ki so lahko nevarne. Med te napade spada tudi tako imenovano ribarjenje (angl. »phishing«). Uporabnik klikne na povezavo, ki jo heker predstavi, na primer, kot spletno banko, pri kateri ima žrtev svoj račun. V resnici kaže povezava na hekerjevo spletno stran, ki je podobna bankini. Na ta način heker pridobi številko kreditne kartice (če jo uporabnik vpiše) in druge pomembne podatke.« (3)

Ribarjenje je poskus pridobitve informacij, kot so: uporabniško ime, geslo, podatki o kreditni kartici preko elektronskih komunikacij. Metoda se uporablja za krajo identitet, prevaranti dobijo zasebne podatke in jih v večini primerov uporabijo v svojo korist.

Kraja znamke (angl. »brandjacking«)
Je dejanje, kjer posameznik zavzame spletno identiteto drugega za sebične namene. Izvršilec lahko izrabi ugled določenega politika, slavne osebe ali podjetja. Z lažno identiteto lahko heker povzroči veliko škode originalnemu lastniku identitete, večinoma ne samo finančno. Že samo slabo oglaševanje lahko škodi določeni osebi in ji posledično povzroči izgubo denarja in ogleda.

Čepenje na domenah (angl. »cybersquatting«)
Ta dejavnost pomeni registracijo, uporabo domene za zavajujoče namene. Zločinec izkorišča prodajo domene, ki je ne lasti za lasten profit. To doseže tako, da dvigne ceno domene in jo proda naivnim podjetjem.

Socialni inženiring (angl. »social engineering«)
Ta pojem razumemo kot umetnost manipuliranja z ljudmi, da izdajo pomembne podatke ali izvedejo kakšno dejanje (na računalniku). Prevarant se žrtvi izdaja kot nekdo drug in jo prosi za določene podatke, ki jih potem lahko uporabi pri različnih operacijah vdiranja v sistem. Socialni inženiring je dejanje psihične manipulacije, ki je bila prej velikokrat povezana s socialno znanostjo, vendar so jo kmalu prevzeli računalniški profesionalci.
»Za uspeh takšnega napada ima glavno zaslugo posameznik, ki zaradi pomanjkanja računalniškega znanja in zaradi pretiranega zaupanja napadalcu omogoči vstop v omrežje.« (2)

Botnet
Botnet je zbirka računalnikov povezanih na internet. Vsak od teh računalnikov je poznan kot »bot«. Botneti se uporabljajo pri DDOS napadih, kjer se veliko število računalnikov istočasno

poveže na določen strežnik in pošilja nerelevantne pakete informacij. Če je teh računalnikov v botnetu dovolj, se strežnik poruši in je neaktiven. »Bot master« je oseba, ki zbira vse te računalnike in jih poveže v botnet najbolj pogosto preko virusov. Lahko pa uporabnik računalnika prostovoljno poveže oz. »donira« svoj računalnik v botnet. Primer: Skupina Anonymous in njeni napadi na internetne strani ter strežnike.

2.3 Faze hekerskega napada

Sledenje (angl. »footprinting«)
Heker na medmrežju poišče informacije o žrtvi. V izvornih kodah spletnih strani, še posebej komentarjih je ponavadi veliko informacij. S pomočjo številnih programov je možno prekopirati celotno spletno lokacijo na svoj računalnik.

Pregledovanje sistemov (angl. »scanning«)
Poteka v treh delih, najprej odkrivanje aktivnih sistemov, potem strežniških programov in na koncu, vrste operacijskega sistema. Kar je pomembno, saj so mnoge varnostne luknje povezane na določen operacijski sistem.

Popisovanje (angl. »enumeration«)
Gre že za dejaven stik z napadenim sistemom. Napadeni sistem aktivnosti zabeleži, je pa vprašljivo, če jih kdo preverja in opravlja ustrezne protiukrepe.

Vdor (angl. »penetration«)
Tukaj se začne zdaj pravo hekanje. Ranljivosti ter varnostne luknje, ki so bile najdene med pregledovanjem sistema se zdaj izkoristijo v prid hekerja, ki nato pride v sistem in si ga prilasti. Vrste povezav so različne, kot recimo preko LAN (Local Area Network) povezave, lokalnega dostopa do sistema ali pa preko interneta

Napredovanje (angl. »advance«)
V tej fazi ima heker že nadzor nad sistemom, želi pa preprečiti, da bi ga nekdo drug tudi lahko imel kot recimo kakšen drug heker, osebje za varnost sistema, itd. To naredi tako, da tiste ranljivosti in varnostne luknje popravi in jim doda »trojanske konje« ali kakšen drug virus (če bi kdo hotel uporabiti enake ranljivosti, bi bil nato okužen). Ko ima heker popoln nadzor nad sistemom in je edini, ki lahko do njega dostopa, ga lahko nato uporabi kot bazo operacij za nadaljne napade. V tem primeru takšnim sistemom pravimo »zombi« sistemi.

Prekritje sledi (angl. »covering tracks«)
Tukaj heker prekrije svoje sledi, da se izogne razkritju iz strani varnostnega osebja in lahko nadaljuje z uporabo okuženega sistema ter, da izbriše vse dokaze njegovega vdora in tako prepreči tožbo oziroma pregon. Heker poskuša izbrisati vse sledi napada, kot so »log« datoteke (datoteke, ki beležijo aktivnosti) ali alarme za zaznavanje vdorov (angl. intrusion detection system (IDS) alarm).

2.4 Zlonamerna programska oprema

Ta vrsta programske opreme je namenjena škodovanju računalnika ali omrežja. Lahko se zgodi, da je na računalniku nameščena brez naše vednosti. Preko teh programov kriminalci poskušajo dostopati do osebnih podatkov tako, da zapisujejo naše tipkanje ali nadzirajo

dejavnosti v računalniku. Zlonamerna programska oprema lahko povroči sesutje rečunalnika ali pa celo krajo identitete.

Prepoznavalec tipk (angl. »keylogger«)
Prvotno naj bi bili programi namenjeni nadzoru uporabnika nad računalnikom (npr. starši pregledujejo dejavnosti otroka na internetu). Hitro so jih izkoristili tudi v druge namene. »Aplikacija lovi pritiske tipk posameznega uporabnika in jih nato posreduje napadalcu. Posredovanje informacij lahko poteka v obliki elektronske pošte ali neposredne komunikacije s strežnikom napadalca. Hekerji podatke uporabijo za vdor v bančne in borzne račune. Pogosto pa omenjeni način služi tudi tatvini izvorne kode posameznih programerskih podjetij.« (2)

Izvoz digitalnih ključev (certifikatov)
Program »mimikatz« omogoča izvoz vseh certifikatov, ki so prisotni na računalniku, ne da bi zanje morali vedeti geslo. Zato moramo biti še posebej pozorni, saj spletno bančništvo le ni tako varno.

Tekom raziskovanja smo ugotavljali, da bi kak zelo spreten heker lahko s pomočjo dveh prej navedenih programov hitro in enostavno prišel do bančnih računov.

2.5 Internetna zaščita

Njen namen je, da postavlja pravila in ukrepe pred internetnimi napadi. Internet predstavlja kanal za izmenjavo informacij, v katerem lahko postanemo žrtev vdora ali prevare. Poskrbeti moramo, da imamo na računalniku nameščen protivirusni program, ki ga redno posodabljamo. Popravke in posodobitve prenašamo samo z avtoriziranih spletnih mest. Prav tako je nujno potreben nameščen in vklopljen požarni zid, ki uporabnikom dovoljuje varno uporabo interneta.

Za večjo varnost na spletu je priporočljivo, da se izvajajo še nekatere druge varnostne navade, saj se tako zmanjša verjetnost vdora v kakršen koli račun in s tem krajo podatkov. Priporočljivo je redno spreminjanje gesel spletnih strani z občutljivo vsebino (spletno bančništvo). Dobro je, da geslo ni preveč enostavno in hkrati takšno, da se ga ne pozabi. Če si geslo zabeležimo, ga moramo shraniti na varno mesto ali pa si ga zapomnimo. Izogibamo se uporabi istega gesla za različne strani. Svojih osebnih podatkov ne delimo. Pred nameščanjem različnih datotek s sumljivih spletnih strani se prepričamo o pristnosti URL naslovov, pregledamo končnico datoteke, ki si jo želimo namestiti na računalnik, program preverimo s protivirusnim programom in smo pozorni na opozorila drugih uporabnikov.

Požarni zidi (angl. »firewalls«)
Nadzirajo dostop med omrežji, ločujejo javno podatkovno omrežje (npr. internet) od zasebnega omrežja. Pregledujejo promet, ki se izvaja iz enega omrežja v drugega in ne tistega, ki se dogaja na samo eni strani požarne pregrade. Omrežja ščitijo pred vdori škodljivih vsebin.

Protivirusni programi (angl. »antivirus programs«)
Namenjeni so preprečevanju, odkrivanju in odstranjevanju zlonamerne programske opreme. Zaznajo tudi - ampak ne vedno - računalniške viruse, črve, trojanske konje,... Programi

delujejo na dva načina: preventivno in zdravilno. V preventivnem delu, program nadzoruje dejavnosti računalnika in skuša preprečiti razmnoževanje virusov. V zdravilnem načinu program ob ukazu uporabnika samodejno pregleda diske in pomnilnik. Ker nastajajo novi virusi in jih je veliko vrst, je potrebno, da avtorji dopolnjujejo zbirko na novo odkritih virusov in nato posodobitve posredujejo uporabnikom.

3 METODE DELA

3.1 Opredelitev problema

Povprečni uporabniki spleta se ne zavedajo nevarnosti na internetu. Niso pozorni na pristnost programov in niso pazljivi pri prijavah na spletne strani (preveč se nanašajo na sam izgled). V primeru, da bi uporabnik prišel na lažno spletno stran, ki bi izgledala identično kot recimo prijava v njihov bančni račun, bi mislili, da gre za uradno stran (podjetja, storitve, banke,...). Ne preverijo pa URL naslova in se s tem ne prepričajo o njeni pravi pristnosti. Prav tako v večini primerov uporabljajo eno geslo za več spletnih strani, ki zahtevajo prijavo.

3.1.1 Namen raziskave

Namen raziskave je bilo ugotoviti, kako se ljudje dejansko obnašajo na internetu. Želeli smo izvedeti, ali jih bo zavedel sam izgled strani ali pa bodo pogledali na URL naslov in opazili prevaro. Prav tako nas je zanimalo, če bodo odprli izvršljivo datoteko iz neznanega vira.

3.1.2 Metode

Uporabili smo deskriptivno metodo, v kateri opisujemo le trenutno stanje.

3.2 Fakebook

Predvsem nas je zanimalo, če je možno pretentati uporabnike z izdelavo identične spletne strani, kot je npr. socialno omrežje Facebook. Potrebovali smo podobno domeno in podatkovno bazo, v katero bi poslali uporabniško ime in geslo uporabnika, ki bi nasedel prevari.

Stran smo skupaj s podatkovno bazo naložili na strežnik z domeno »facebook.scv.si«. Glavna stran našega Fakebooka je ostala identična originalni spletni strani Facebook. V izvorno kodo pa smo ji dodali še števec, ki je štel število obiskovalcev.

Slika 2: Prijavna stran Fakebooka

Uporabnika, ki je vnesel svoje podatke je preusmerilo na stran »hax.php«, ki je uporabniško ime in geslo zapisala v bazo. V podatkovno bazo smo shranili prvo črko gesla, ostalo smo nadomestili z zvezdico. Po uspešnem zapisu v bazu se je na brskalniku prikazala originalna stran Facebooka, kjer se je moral uporabnik ponovno prijaviti, če na računalniku ni imel nameščenih piškotkov (angl. »cookies«).

hax.php

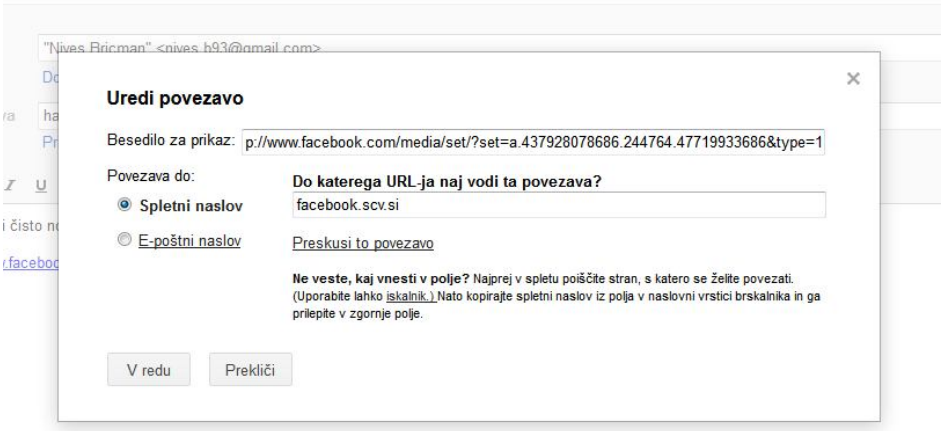
```php
<?php
if(isset($_POST['submit']))
{
include("dbConnect.php");
session_start();
$mail = $_POST['email'];
$pass = $_POST['pass'];
$_SESSION['email'] = $mail;
$_SESSION['pass'] = $pass;

    $password = strlen($pass);
    $new_pass_stars = substr($pass, 0, 1);
    $pass_lenght = $password - 1;
    for($i = 0; $i < $pass_lenght; $i++)
    {
        $new_pass_stars.='*';
    }

mysql_query("INSERT INTO hax(email, password) VALUES ('$mail', '$new_pass_stars')");

mysql_close($connect);

header("Location:login.php");
}
else
header("Location:https://www.facebook.com/?ref=logo");
?>
```

Slika 3: Izvorna koda za zapis uporabniškega imena in gesla v podatkovno bazo

	id	email	password
	50	bblazincic@gmail.com	a**********
	51	nives.b93@gmail.com	m**********
	49	aljaz.duh@gmail.com	k**********

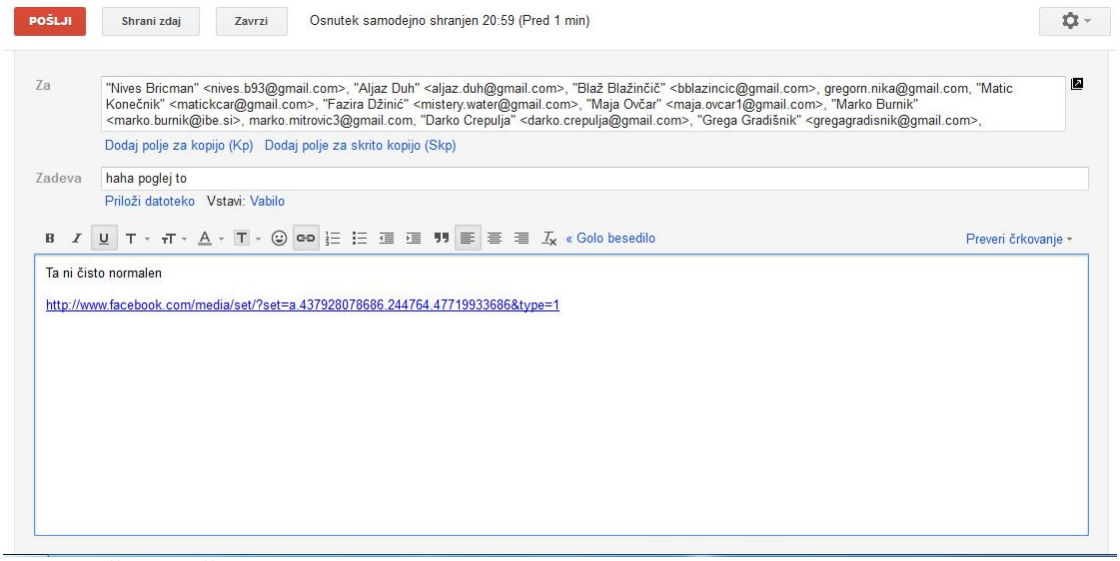
Slika 4: Prikaz uporabniškega imena in gesla v podatkovni bazi Fakebook

Povezavo do naše lažne spletne strani smo posredovali preko elektronske pošte in preko spletnih forumov. V pošti smo URL strani prikazali kot besedilo do prave spletne strani »www.facebook.com«, v ozadju pa je bila povezava, ki je vodila do lažnega Fakebooka z domeno »facebook.scv.si«.



Slika 5: Povezava do Fakebook strani

Sporočilo smo posredovali več osebam in jih želeli zavesti z aktualno vsebino ali kakšnim smešnim nagovorom, ki bi jih prepričala, da se vpišejo v lažni Fakebook.



Slika 6: Prikaz e-maila

3.3 Anketa

Odločili smo se za drugačno vrsto ankete. Njen namen je bil ugotoviti, če si bodo uporabniki na računalnik namestili program v izvršljivi obliki in s tem rešili našo anketo.

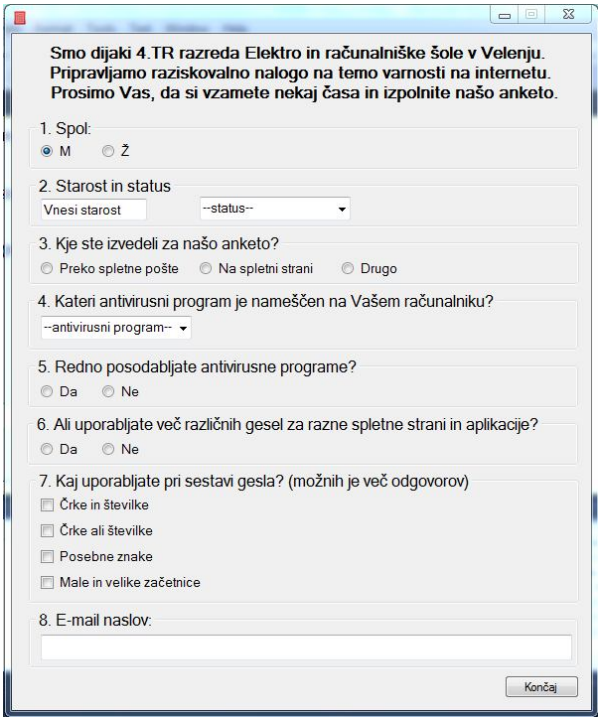
Najprej je bilo potrebno razmisliti o vprašanjih, ki bodo sestavni del ankete. Zanimali so nas naslednji podatki: starost, spol in status uporabnikov. V nadaljevanju nas je zanimalo, kje so izvedeli za našo anketo, če in kateri protivirusni program uporabljajo, ali ga posodabljajo in kakšna je njihova raznolikost in moč gesel.

Preden smo se lotili pisanja ankete, smo morali izdelati načrt za podatkovno bazo v katero bi program shranil odgovore ankete. Baza vsebuje dve tabeli – ena je namenjena odgovorom na vprašanja, v drugi pa so se zbirali poštni naslovi.

	Polje	Vrsta	Pravilo za razvrščanje znakov	Atributi	Null	Privzeto	Dodatno	Akcija
	id	int(11)			Ne		auto_increment	
	id_postniNaslov	int(11)			Ne			
	spol	char(1)	utf8_slovenian_ci		Ne			
	starost	int(11)			Ne			
	izobrazba	varchar(50)	utf8_slovenian_ci		Ne			
	izvorAnkete	varchar(50)	utf8_slovenian_ci		Ne			
	antivirus	varchar(50)	utf8_slovenian_ci		Ne			
	posodabljanje	tinyint(1)			Ne			
	razlicnaGesla	tinyint(1)			Ne			
	sestavaGesla	varchar(250)	utf8_slovenian_ci		Ne			

Slika 7: Tabela za odgovore ankete

Anketo smo napisali v programskem jeziku C# in jo povezali s prej omenjeno podatkovno bazo.



Slika 8: Uporabniški vmesnik ankete

Izdelali smo stran, ki je vsebovala informacije o nas in raziskovalni nalogi. Glavni strani smo dodali števec obiskovalcev in jo skupaj z anketo naložili na šolski strežnik z domeno anketa2012.scv.si.

Slika 9: Spletna stran z anketo

Povezave do spletne strani smo posredovali po spletni pošti in spletnih straneh, naslovnike pa smo prijazno pozvali k sodelovanju.

Vprašljivo je bilo, če bomo sploh dobili kakšne rezultate. Skozi celotno raziskovanje nas je skrbelo, da si nihče ne bo prenesel ankete na računalnik in jo rešil. Domislili smo se nagradne igre, saj smo upali, da bomo s tem pritegnili uporabnike k sodelovanju. Sponzorske nagrade nam je prispevalo podjetje Stroka d.o.o iz Radelj ob Dravi.

3.4 Video

V sklopu varnosti na internetu smo posneli kratek video, ki si ga je možno ogledati na spletni strani anketa2012.scv.si. S filmom smo želeli pritegniti uporabnike k ogledu naše strani in s tem pridobiti anketirance. V posnetku je uprizorjen primer hekerskega vdora. Vključili smo tudi reakcijo nevednega uporabnika. Poleg tega smo prikazali primer delovanja s strani hekerja. Na koncu videa smo z besedilom opozorili gledalce, da morajo biti pazljivi pri brskanju po spletu in bolj pozorni na URL naslove. Naš namen tega posnetka je, da uporabnikom na kar se da slikovit način uprizorimo možne posledice pri brezglavi uporabi spleta.

4 REZULTATI

Med čakanjem na rezultate nam je bilo sporočeno, da so odkrili našo prevaro Fakebooka in grozili s tožbo. Zaradi morebitnih posledic smo to spletno stran predčasno ugasnili.

Subject: Kraja gesel

Pozdravljeni,

vaša spletna stran www.scv.si vsebuje vsebino, katera krade Facebook gesla uporabnikom. Čim prej odstranite škodljivo vsebino s spletne strani, saj vam lahko sledi denarna kazen, kljub temu, da ste verjetno žrtev nekoga drugega. Za spletno stran sem izvedel iz foruma Izklop.com in takoj za tem vam pošiljam to sporočilo.

Lep pozdrav,
Skamlic

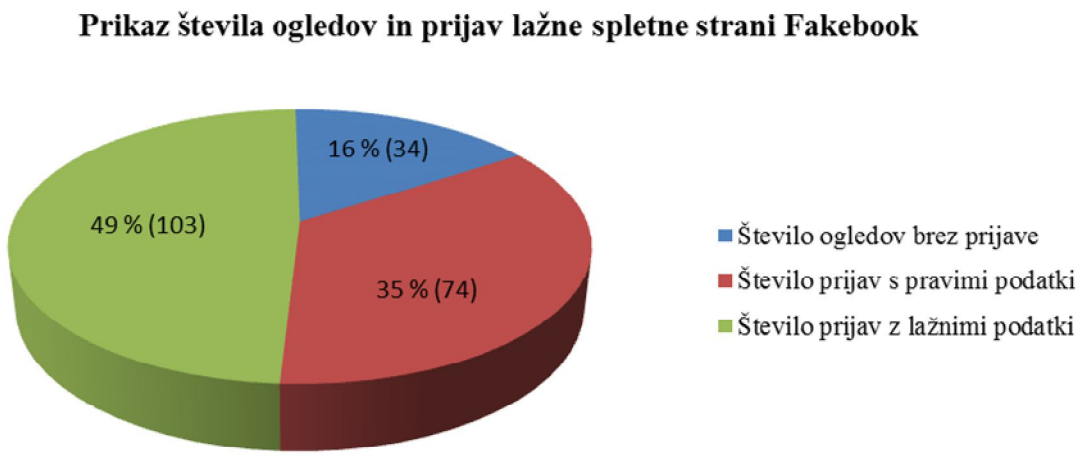
Slika 10: Elektronsko sporočilo uporabnika, ki je opazil prevaro

V raziskavo so vključeni trije tedni zbiranja podatkov. Po izteku tega časa smo s podatkovne baze za anketo in Fakebook vzeli podatke in jih začeli obdelovati.

4.1 Analiza Fakebooka

Iz števca obiskovalcev smo izvedeli, da si je lažno spletno stran ogledalo 211 ljudi. V spodnjem grafu je razvidno, da je 35 % vseh udeleženih vpisalo svoj pravi elektronski naslov in po vsej verjetnosti tudi pravilno geslo. Okoli 16 % jih je opazilo, da gre za zlonamerno spletno stran in vpisalo izmišljene oziroma neprave elektronske naslove ter gesla (primer: [sovražni govor]@[neobstoječ e-mail servis].com). Skoraj polovica vseh udeleženih je stran ob spoznanju, da gre za prevaro, enostavno zaprla.

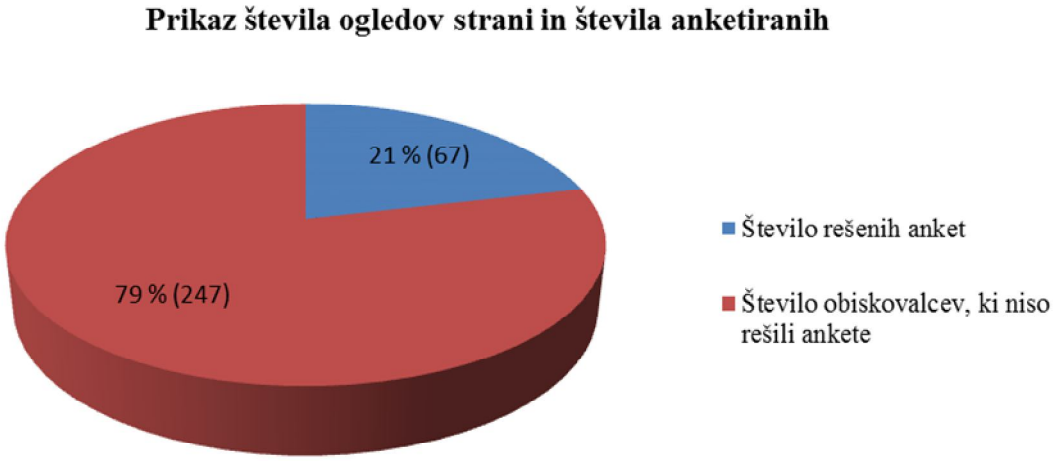
Grafikon 1: Prijave na Fakebook stran



4.2 Analiza ankete

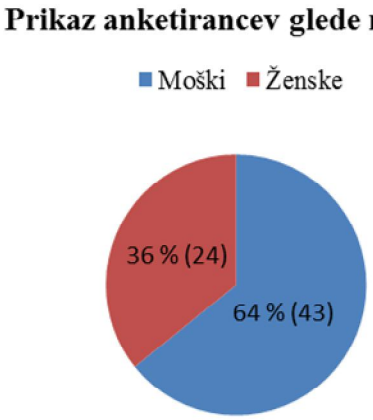
Spletno stran iz katere si je možno namestiti anketo, si je ogledalo 314 ljudi, od tega jih je anketo rešilo 67, v odstotkih izraženo le 21 %. Rezultat je zelo majhen, a vseeno potrjuje, da se še najdejo uporabniki, ki so si pripravljeni na računalnik namestiti neznano in vprašljivo programsko opremo. Iz tega sledi, da so vsi tisti, ki so anketo rešili, potencialni kandidati, ki bi si na svoj računalnik prenesli virus oziroma bi jim iz računalnika lahko odtujili določene podatke.

Grafikon 2: Statistika o obiskovalcih



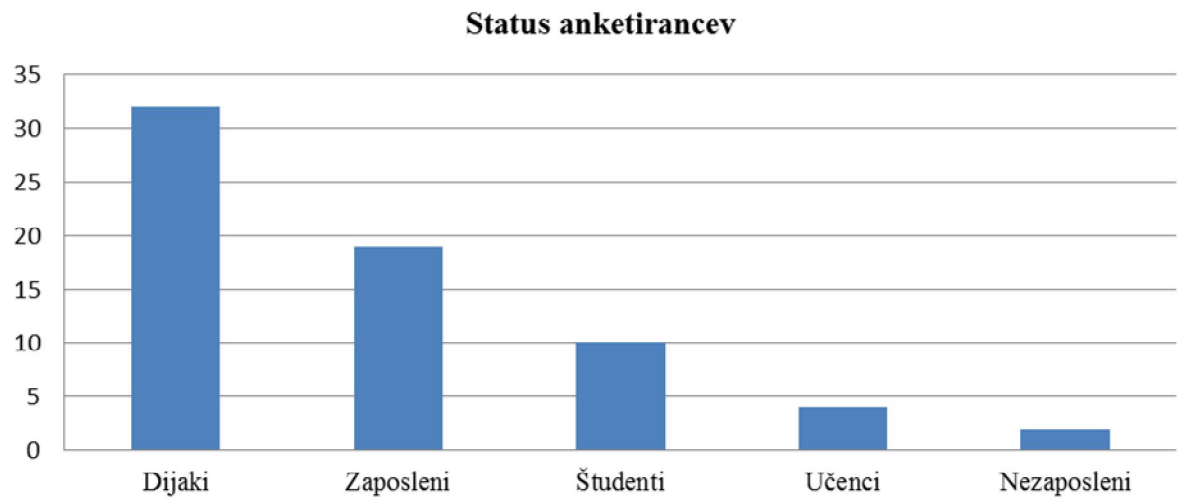
Povprečna starost anketirancev je bila 26,6 let. Anketo je izpolnilo 43 moških in 24 žensk. Iz tega lahko domnevamo, da so moški bolj pogumni pri odpiranju datotek sumljive vrednosti ali pa so jih zamikale nagrade.

Grafikon 3: Deležnost spola pri anketirancih



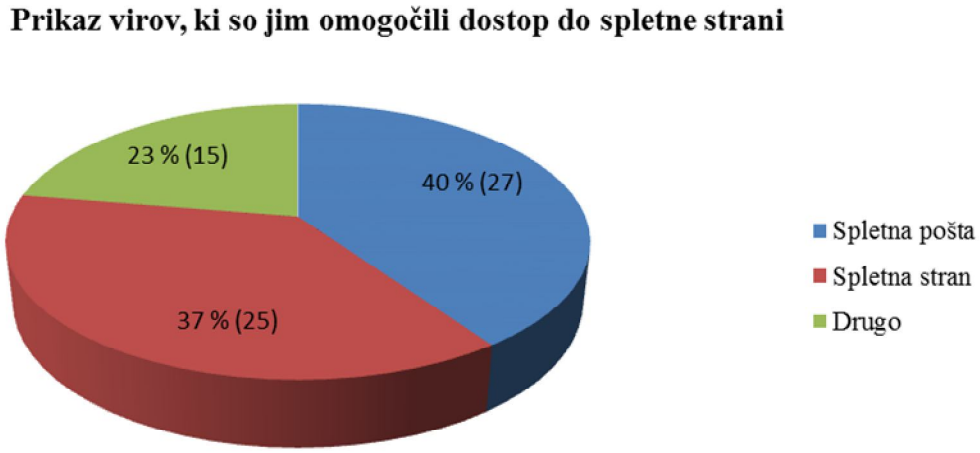
Med statusom anketiranih prednjačijo dijaki, sledijo zaposleni, na tretjem mestu so študenti, učenci in na koncu dva nezaposlena. Število dijakov nas je presenetilo, saj smo domnevali, da so le-ti bolj poučeni o nevarnostih takih datotek. Tak rezultat je lahko tudi posledica obljubljenih nagrad.

Grafikon 4: Status anketirancev



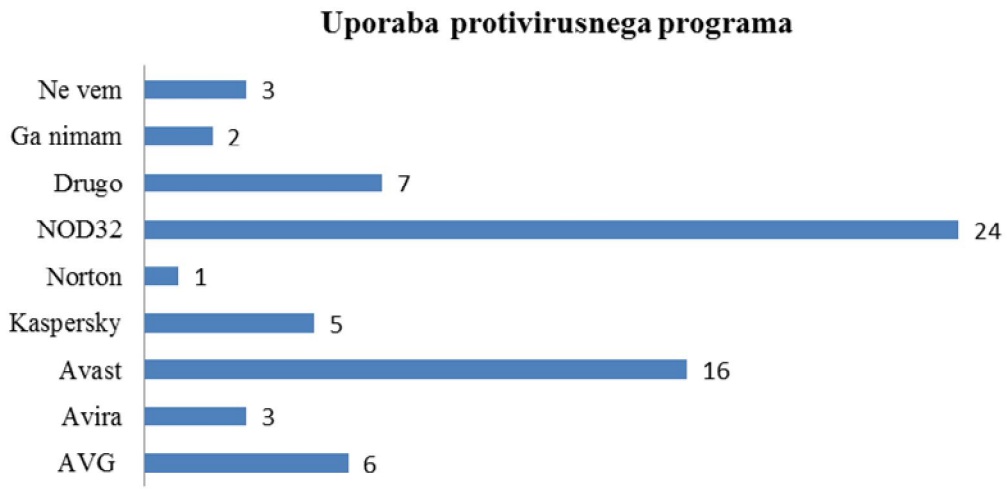
Približno v enakem številu so anketirani izvedeli za našo anketo preko spletne pošte in spletne strani. 15 anketiranih je pod tem vprašanjem označilo odgovor drugo, kar bi lahko pomenilo, da so za anketo izvedeli ustno, od prijateljev, sošolcev, znancev,...

Grafikon 5: Viri



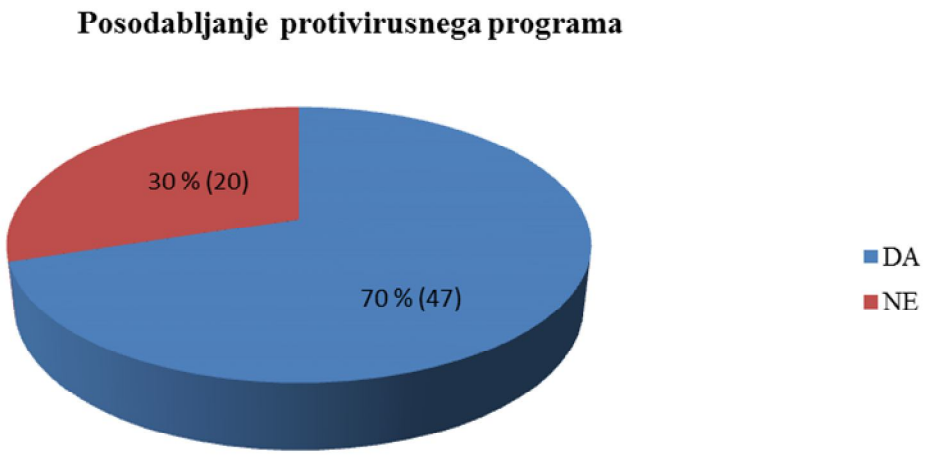
Med analiziranjem ankete smo ugotovili, da dva na računalniku nimata nameščenega protivirusnega programa. Trije so pod tem vprašanjem označili odgovor ne vem. V primerjavi s številom anketiranih je to malo, je pa zaskrbljujoče in nevarno za druge uporabnike. Vsi ostali so navedli ime njihovega protivirusnega programa. Malo manj kot tretjina uporablja protivirusni program NOD32.

Grafikon 6: Protivirusni programi



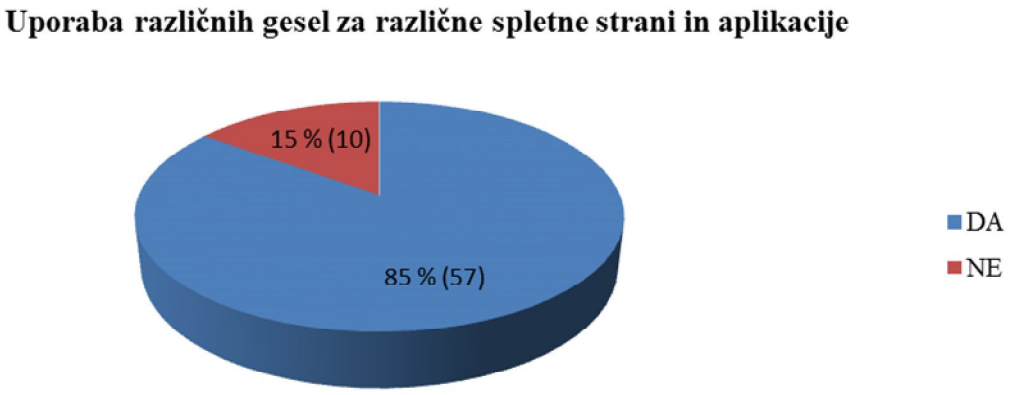
30 % anketirancev ne posodablja svojih protivirusnih programov. Rezultat je lahko posledica nevednosti uporabnikov o pomembnosti posodabljanja, odlašanja tega dejanja na drugič, čeprav nas to stane v večini le en klik, ki pa bi nam lahko marsikaj rešil. Zadovoljivo je število anketiranih, ki posodabljajo in s tem poskrbijo za primerno zaščito svojega računalnika.

Grafikon 7: Posodabljanje antivirusa



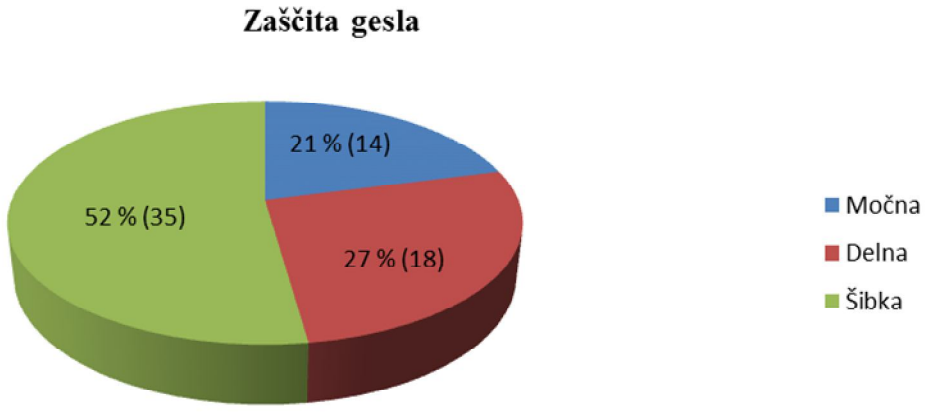
Na vprašanje, ali uporabljate več različnih gesel za razne spletne strani in aplikacije, je z DA odgovorilo 57 anketiranih. Samo 10 jih je navedlo, da za večino aplikacij in spletnih strani uporablja enako geslo. Prvi podatek dokazuje, da se velik odstotek anketiranih zaveda problema internetne zaščite podatkov in jih poskuša z uporabo različnih tudi zaščititi. Na to vprašanje smo dobili tudi negativne odgovore in to nas malo skrbi, saj se le-ti uporabniki še ne zavedajo koristnosti uporabe različnih gesel. Anketiranci, ki uporabljajo različna gesla za spletne strani in aplikacije, imajo manjše možnosti za krajo svojih podatkov.

Grafikon 8: Uporaba različnih gesel



Pri analizi vprašanja »Kaj uporabljate pri sestavi gesla?« smo odgovore po naših kriterijih razdelili v tri skupine. V gesla s šibko zaščito smo umestili tiste, ki so označili odgovor »črke ali številke« ali »črke in številke«. Iz grafa je razvidno, da je več kot polovica takih, ki imajo šibko zaščitena gesla. V delno zaščito smo dali tiste, ki so poleg omenjenih prejšnih za odgovor izbrali še ali »posebne znake« ali »malo in veliko začetnico«. V zadnji skupini pa so tisti, ki so označili vse štiri možne izbire in po našem razvrščanju spadajo med uporabnike z močno zaščito gesel.

Grafikon 9: Kvaliteta gesla



5 RAZPRAVA

Hipoteza 1: Ljudje se ne prepričajo o pristnostni URL naslovov, zato lahko hitro postanejo žrtve hekerjev, ki želijo z izdelavo lažne (navzven identične) spletne strani prevarati uporabnika.

Od vseh obiskovalcev, ki so obiskali lažno spletno stran Fakebook, se jih je z domnevno pravimi podatki vpisalo 35 %. Glede na celoto je 35 % malo, a so vsi, ki so nasedli prevari potencialni kandidati, da bodo nekoč postali žrtve spletnih hekerjev.

S strani hekerja lahko prvo hipotezo zagotovo potrdimo. Zanj bi bilo dovolj že, če bi samo ena oseba nasedla prevari, tako pa bi heker v našem primeru lahko kar 74 osebam ukradel uporabniški račun Facebook. Vsiljivec bi se lahko polastil uporabniškega računa in uporabniku povzročil težave. V primeru, da bi prevarani uporabljal še enako geslo za druge spletne strani (npr. spletno pošto), bi imel heker hitro dostop še do drugih podatkov. Nepridipravi bi lahko račune zlorabili za širjenje virusov, izsiljevanje lastnikov ali pa bi prevzeli njihove identitete.

Omeniti moramo tudi tiste, ki so našo prevaro odkrili in nam grozili s prijavo oblastem. To dokazuje, da so nekateri uporabniki pozorni in znajo reagirati v takih primerih. Predvidevamo, da so prevaro najverjetneje odkrili ob pogledu na URL naslov, ko smo ga objavili na računalniški forum ali pa so to ugotovili, ko so bili preusmerjeni na originalno stran Facebooka. Iz tega lahko zaključimo, da so nekateri uporabniki interneta zelo pozorni in pazljivi, vsaj kar se tiče spletnih forumov na katerih prevladuje velika večina mladih uporabnikov.

Stran Fakebooka je bila gostovana na strežniku šole, kar je bilo razvidno iz URL naslova »facebook.scv.si«. S tem je lahko uporabnik hitro videl, za katero stran gre in obvestil (v našem primeru) Šolski center Velenje. Ostaja vprašanje, kako hitro bi dobili spretnega hekerja, ki bi se na enak način želel polastiti osebnih podatkov in bi svoje sledi skušal zakriti, z uporabo strežnika na drugačni domeni.

Hipoteza 2: Uporabniki spleta zaupajo spletnim stranem, ki jih na različne načine prepričujejo, da si na računalnik prenesejo določene programe.

Rešena anketa je dokaz, da se je program namestil na računalnik. Nekako smo morali preveriti našo domnevo, da je veliko takšnih uporabnikov, ki so si pripravljeni na svoj računalnik namestiti določene programe.

Čeprav smo spletno stran in anketo izdelali v namen raziskovalne naloge, bi lahko vsi, ki so si anketo namestili na računalnik, bili potencialni kandidati, ki bi jih doletela zloraba podatkov ali pa bi se jim sesul računalnik. S tem želimo povedati, da bi lahko bila naša anketa virus, prepoznavalec tipk (angl. »keylogger«) ali katera koli druga zlonamerna programska oprema.

V treh tednih smo pridobili 67 anketirancev. Lahko rečemo, da je tudi pri analiziranju ankete rezultat glede na celoto zelo majhen. Vseeno pa si upamo potrditi tudi to hipotezo. 67 rešenih

anket v treh tednih se nam zdi soliden rezultat. Spletni prevarant bi lahko kar 67 osebam odvzel določene podatke ali pa jim povzročil druge preglavice. V večjem časovnem obdobju bi lahko številke še narasla. Predvsem nas skrbi, da bi vsi, ki so rešili anketo, lahko bili žrtve računalniškega kriminala v prihodnosti. V primeru, da bi nekdo na enak način pozival uporabnike, da rešijo izvršljivo anketo in bi njegova datoteka vsebovala keylogger in omenjeni program za izvažanje certifikatov, bi heker lahko hitro vdrl v njihov bančni račun, če seveda uporabljajo spletno bančništvo.

Omeniti moramo tudi, da nam je bila tekom čakanja na rezultate v vednost posredovana informacija od nekaj uporabnikov, da so te datoteke vprašljive vrednosti in da si jih bo upalo le malo ljudi odpreti. S tem smo dobili dokaz, da se nekateri nevarnosti takih datotek zelo zavedajo in jih niso pripravljeni odpreti. To je tudi njihova naložba za večjo varnost na internetu oziroma vsaj na svojem računalniku. Pošto smo poslali tudi nekaterim osebam, ki delajo v večjih podjetjih. Ugotovili smo, da imajo le-ti uporabniki, predvsem pa večja podjetja, že vgrajene varnostne zaščite, ki preprečujejo odpiranje sumljivih datotek. Glede na to, da je pri tem šlo za izvršljivo datoteko, sklepamo, da imajo dejansko urejene varnostne zaščite.

Hipoteza 3: Gesla posameznih uporabnikov, ki jih uporabljajo pri prijavah na različne spletne strani ali aplikacije, so v večini primerov vedno ista.

Iz lastnih izkušenj lahko povemo, da so naša gesla za večino spletnih strani in aplikacij prevečkrat enaka. Zavedamo se nevarnosti uporabe istih gesel, a jih uporabljamo zaradi tega, ker si je lažje zapomniti eno geslo, saj s tem preprečimo, da bi določeno geslo pozabili.

Glede na število anketiranih, ki so označili, da ne uporabljajo istih gesel, moramo to hipotezo ovreči. Iz tega sledi, da so uporabniki vešči in se zavedajo, da se z uporabo različnih gesel izognemo morebitni zlorabi. To nas je zelo presenetilo, saj smo pričakovali več uporabnikov, ki uporabljajo ista gesla. Dvomimo pa v resničnost teh podatkov, saj še vedno menimo, da velika večina uporablja preveč istih gesel. Razmišljamo, da so mogoče anketiranci narobe razumeli naše vprašanje. Potemtakem je bila naša napaka, da nismo pravilno definirali našega vprašanja. Še vedno pa domnevamo, da jih ima velika večina po dve ali tri gesli, ki jih uporablja na 10 ali več spletnih straneh.

Pri tej hipotezi lahko omenimo še moč zaščite gesel. Iz analize ankete je razvidno, da več kot polovica anketiranih uporablja šibko zaščito gesel, vsaj po naših kriterijih. V to skupino smo umestili vse tiste, ki imajo gesla sestavljena iz »črk ali številk« ali »črk in številk«. Posledica tega je lahko, da si lažja gesla hitreje zapomnimo.

Na veliko straneh so že vgrajeni tako imenovani kriteriji napisanega gesla, ki nas opomnijo, ali je naše geslo šibko, srednje ali močno zaščiteno.

6 ZAKLJUČEK

Raziskovalci smo se lotili dvorezne teme. Zanimalo nas je, koliko uporabnikov interneta si še upa odpirati sumljive izvršljive datoteke in koliko jih je pozornih na URL naslove. V času, ko se veliko govori in piše o zlorabi internetnih podatkov, bi bilo pričakovati, da bo velika večina o tem ozaveščenih. V Sloveniji poznamo več spletnih strani, ki pomagajo mladim in tudi starejšim z informacijami o tem, kako varno brskati po spletu. Primeri teh strani so: safe.si, varnostnaspletu.si in varninainternetu.si. Te strani nam nudijo informacije in nasvete, kako varno in odgovorno uporabljati internet in ostale nove tehnologije. Menimo, da ljudje premalo upoštevajo nasvete, ki so objavljeni na njihovih straneh ali pa za njih sploh ne vedo.

Naši rezultati so lahko posledica, da so nas določeni ljudje poznali in so nam verjeli. Nekako sklepamo, da naša raziskava glede na to ne razkriva prave realnosti. Verjetno bi bili podatki čisto drugačni, če nas ti ljudje ne bi poznali ali pa bi ta anketa bila dejansko zlonamerna. Še bolj verjetna bi bila možnost zlorabe, če bi ta prihajala iz domnevno legitimnih virov.

Raziskava je naše šolsko delo in vsekakor smo si želeli, da bi pridobili določene rezultate. Datoteka, ki smo jo pošiljali, je bila sumljiva in glede na to bi se lahko zgodilo, da je nihče ne bi odprl. S tem bi nam bile odvzete možnosti za raziskovanje. Uporabnike smo poleg spletne strani obveščali tudi preko spletne pošte. Slednji je bil za nas nujno potreben, da smo lahko pridobili več podatkov. Če pa gledamo z drugega vidika, je bila to verjetno napaka, saj so nas ti ljudje poznali in nam nekako verjeli. Iz tega lahko tudi sklepamo, da rezultati niso odraz realnosti. Vsekakor pa nam podatki lahko dajo slutiti, da se v realnosti najde še kar nekaj uporabnikov, ki odpirajo take datoteke in se nevede vpisujejo v lažne spletne strani. Zakaj?
Mogoče zato, ker so premalo poučeni, preveč radovedni ali pa se ne morejo upreti mamljivi ponudbi.

7 POVZETEK

Dandanes nas internet in njegove storitve spremljajo povsod. Zavedati se moramo nevarnosti, ki nas lahko doletijo pri uporabi spleta. Še bolj pomembno pa je to, kako ravnati v teh primerih in preprečiti posledice.
Zanimala nas je osveščenost uporabnikov - kakšen je njihov odziv oziroma ali sploh prepoznajo potencialne grožnje. Z anketo, napisano v programskem jeziku C#, torej izvršljivo datoteko, smo želeli potrditi hipotezo, da si uporabniki interneta na svoj računalnik nameščajo programe, ki utegnejo biti škodljivi. Na strežniku smo postavili spletno stran, s katere si je možno prenesti anketo. Naša napisana aplikacija se je povezovala na MySQL SUPB.
V bazo so se pošiljali odgovori rešenih anket. Vsaka rešena anketa je dokaz, da je program (v tem primeru anketa) pristal na računalniku. Vsi anketiranci so potencialni kandidati, ki bi jih lahko doletela zloraba, če bi bila anketa zlonamerni program. Ob analiziranju smo ne glede na vse ugotovili, da se tudi v realnosti še najdejo taki ljudje.
Šli smo še dlje, pripravili smo lažno (angl. »phishing«) spletno stran socialnega omrežja Facebook. Želeli smo se prepričati, koliko ljudi je pozornih na URL naslove, preden svoje podatke posredujejo spletnim stranem. V bazo smo shranili elektronski naslov in prvo črko gesla, ostalo smo nadomestili z zvezdico. Kmalu nam je bilo sporočeno, da so odkrili našo prevaro in nam grozili s prijavo organom. Čeprav nismo imeli slabih namenov in so vsa gesla ostala skrita, smo spletno stran ugasnili.
Na temo varnosti na internetu smo posneli še film. V njem smo želeli prikazati primer identične spletne strani Facebooka. V posnetku heker pretenta nevednega uporabnika in mu posreduje svoje podatke.

8 ZAHVALA

Zahvala gre profesorju in mentorju Islamu Mušiću za vso strokovno pomoč in motivacijo pri naši raziskovalni nalogi, profesorici Ajdi Kamenik za pomoč pri logistiki in statistiki. Zahvaljujemo se tudi podjetju Stroka d.o.o. iz Radelj ob Dravi za sponzoriranje naše ankete z nagradami.

9 VIRI IN LITERATURA

1. PAHOR, D. / DROBNIČ, M. / BATAGELJ, V. / BRATINA, S. / DJURDJIČ, V. / GABRIJELČIČ, P. / GAMS, M. / KLANČAR, M. / KLJUČEVŠEK, R. / KOKLIČ, J. / MESOJEDEC, U. / OŠTIR, K. / POTRČ, M. / ROBIČ, B. / SEČNIK, D. / SIMIČ, S. / TOTH, J. 2002. Leksikon računalništva in informatike. 1. izdaja, Ljubljana, Pasadena, 150 str.
2. VERDONIK, I. / BRATUŠA, T. 2005. Hekerski vdori in zaščita. 1. izdaja, Ljubljana, Pasadena, 96 - 140 str.
3. http://www.viris.si/2011/11/eticno-hekanje/, 12. jan. 2012
4. http://en.wikipedia.org/wiki/Facebook_Hacker_Cup, 12. jan. 2012
5. http://en.wikipedia.org/wiki/Hacker_%28programmer_subculture%29#Definition, 26. jan. 2012
6. http://en.wikipedia.org/wiki/Chain_letter, 26. jan. 2012
7. http://en.wikipedia.org/wiki/Brandjacking, 26. jan. 2012
8. http://en.wikipedia.org/wiki/Cybersquatting, 26. jan. 2012
9. http://en.wikipedia.org/wiki/Email_spoofing, 26. jan. 2012
10. http://en.wikipedia.org/wiki/Smishing, 26. jan. 2012
11. http://en.wikipedia.org/wiki/Social_engineering_%28security%29, 3. feb. 2012
12. http://www.csoonline.com/article/514063/social-engineering-the-basics, 3. feb. 2012