CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Spyware programi

CCERT-PUBDOC-2009-10-280

+CERT.hr u suradnji s LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom CARNet CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. UVOD 4

2. DEFINICIJA, POVIJEST I RAZVOJ SPYWARE PROGRAMA 5

2.1. POVIJEST I RAZVOJ 5
2.2. STATISTIKE 6

3. USPOREDBA S DRUGIM VRSTAMA ZLONAMJERNIH PROGRAMA 7

3.1. VIRUSI 7
3.2. CRVI 8
3.3. TROJANSKI KONJI 8
3.4. USPOREDBA ZLONAMJERNIH PROGRAMA 9

4. VRSTE SPYWARE PROGRAMA 10

4.1. INTERNET URL ZAPISIVAČI 11
4.2. SNIMAČI ZASLONA 11
4.3. SNIMAČI PORUKA E-POŠTE 11
4.4. CHAT LOGGERI 12
4.5. KEYLOGGERI 12
4.6. SNIMAČI LOZINKI 12
4.7. KOLAČIĆI ZA PRAĆENJE 12
4.8. OTIMAČI WEB PREGLEDNIKA 13
4.9. OTIMAČI VEZE 13
4.10. OTIMAČI RAČUNALA 14

5. NAČINI ZARAZE SPYWARE PROGRAMIMA 15

6. NEGATIVNI EFEKTI ZARAZE 18

6.1. ELEKTRONIČKI REKLAMNI MATERIJALI 18
6.2. KRAĐA IDENTITETA I PRIJEVARA 19
6.3. ŠPIJUNAŽA 19
6.4. PRIMJERI 19

7. NAČINI ZAŠTITE 20

7.1. LAVASOFT AD-AWARE 20
7.2. SPYBOT - SEARCH AND DESTROY 21
7.3. PREPORUKE 22

8. ZAKLJUČAK 23

9. REFERENCE 24

1. Uvod

Spyware programi su zlonamjerni programi koji ciljano prikupljaju podatke o korisniku, te ih šalju na unaprijed definirano odredište bez znanja ili pristanka korisnika. Ovakvi su programi velika prijetnja privatnosti korisnika, podacima na njegovom računalu, a mogu uzrokovati i materijalnu štetu. U 10 godina prisutnosti *spyware* programa uočen je trend velikog rasta ove „industrije“. Naime, naziv industrija možda najbolje opisuje namjenu *spyware* programa. Tvrtke (rjeđe pojedinci) izrađuju *spyware* programe kako bi prikupile čim veći broj podataka o korisnicima i njihovim navikama. Takve informacije imaju vrlo veliku vrijednost u marketinškoj industriji koja iskorištava dobivene podatke u svrhu oglašavanja raznih proizvoda, usluga, itd.

Potencijal *spyware* programa je neograničen, što je shvatljivo kada se spomene činjenica da je nekakav oblik *spyware* programa, prema istraživanju tvrtke Aladdin, prisutan na 55% računala. Postotak je nevjerojatan, uzevši u obzir da se smatra da su mnogo veća prijetnja virusi, crvi ili pak trojanski konji. Postotak računala zaraženih drugim vrstama zlonamjernih programa nije niti približno velik kao navedeni postotak računala zaraženih *spyware* programima.

Kao i od svakog zlonamjernog programa, tako i od *spyware* programa se moguće zaštititi. Programi za zaštitu od *spyware*-a nude niz funkcionalnosti koje će korisnikovo računalo u većini slučajeva obraniti od napada ili očistiti od zaraze.

Trenutno dostupne metode zaštite često nisu dovoljne, upravo zbog nedovoljnog znanja korisnika po pitanju *spyware* programa. Stoga se, prije instalacije bilo kakvog programa za zaštitu od *spyware* programa, savjetuje primjerena edukacija o vrstama, mogućim načinima zaraze, posljedicama zaraze i na kraju mogućim zaštitama od *spyware* programa. Kako bi se na ispravan način educiralo korisnike u ovom dokumentu su obrađene prethodno nabrojane cjeline. Također, uz opis dva besplatna *antispyware* programa, navedeni su i savjeti za korisnike kako bi svoja računala sačuvali od zaraze *spyware* programima.

2. Definicija, povijest i razvoj spyware programa

Termin *spyware* je u početku obilježavao sklopovlje (*eng. hardware*) namijenjeno za nadzor, praćenje ili drugu aktivnost koja uključuje špijunažu pojedinca ili skupine. Navedeni termin je poprimio svoje današnje značenje tek 1999. godine kada je spomenut u kontekstu zlonamjernih programa korištenih u svrhu krađe osobnih informacija, narušavanja privatnosti pojedinaca, te otuđivanja povjerljivih i osjetljivih podataka (npr. intelektualnog vlasništva).

Postoji više definicija *spyware* programa, ali dvije koje vrlo dobro opisuju stvarnu namjenu i djelovanje ovih programa su definicije tvrtki McAfee Inc. i Trend Micro Inc., koje proizvode alate za zaštitu od zlonamjernih programa. Prema navodima ovih tvrtki *Spyware* programi su:

- zlonamjerni programi koji nadgledaju i prikupljaju korisničke podatke u različite svrhe.
- zlonamjerni programi koji šalju korisničke podatke trećoj osobi bez znanja ili pristanka korisnika.

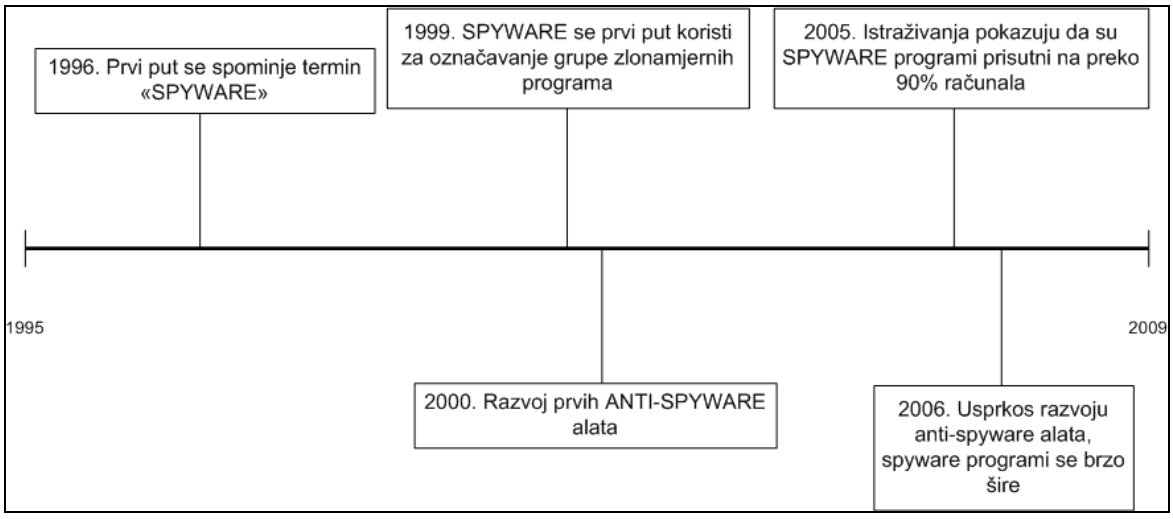
Iako su ove dvije navedene definicije poprilično točne u samom opisu svojstava i funkcija *spyware* programa, svaka definicija za sebe ne daje potpuni opis zlonamjernog djelovanja *spyware* programa. *Spyware* programe bi se preciznije moglo definirati kao zlonamjerne programe koji se bez znanja ili pristanka korisnika postavljaju na računalo, a svoju zlonamjernu djelatnost izvode nadgledanjem i prikupljanjem osobnih informacija ili povjerljivih i osjetljivih podataka, te slanjem istih trećoj osobi (napadaču)bez znanja ili pristanka korisnika .

2.1. Povijest i razvoj

Usprkos mišljenju većine korisnika da *spyware* programi ne mogu uzrokovati toliku štetu kao npr. virusi, crvi i trojanski konji, oni su velika prijetnja njihovim računalima i podacima. Upravo zbog gotovo neozbiljnog shvaćanja ove vrste zlonamjernih programa korisnici nesvjesno sami pokreću preuzimanje *spyware* programa na računalo, te time riskiraju gubitak i otkrivanje podataka, krađu identiteta, materijalnu štetu, itd. Većina *spyware* programa je konstruirana tako da nadgledaju svaku korisničku akciju na računalu, te o tome izvještava napadača. *Spyware* programi predstavljaju veliku prijetnju obzirom na opseg poslova koji većina korisnika obavlja putem Internet servisa. Upravo zbog toga je potrebno obratiti posebnu pažnju kod pregledavanja sadržaja na Internetu.

Prema zajedničkom istraživanju tvrtke *AOL* i udruge *National Cyber-Security Alliance* iz 2005. godine, kada je zaraza *spyware* programima naglo porasla, otkriveno je da:

- je čak 61% ispitanika izjavilo kako je njihovo računalo bilo zaraženo nekom vrstom *spyware* programa,
- 92% ispitanika čija su računala bila zaražena nisu bili svjesni prisutnosti *spyware* programa i
- 91% ispitanika nije dalo pristanak za instalaciju *spyware* programa.



Slika 1. Kronološki prikaz događaja vezanih uz *spyware* programe

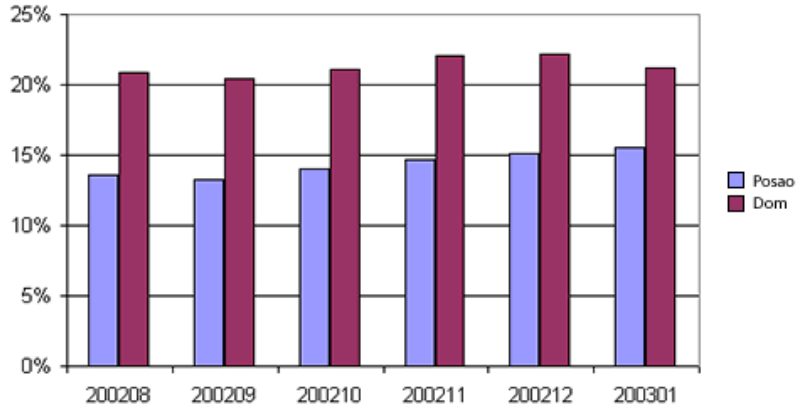
Smatra se da su od 2006. godine *spyware* programi postali veća prijetnja računalima od drugih vrsta zlonamjernih programa. Zaraza računala *spyware* programima je uvelike porasla uslijed propusta u korištenim programima, te naivnosti i neznanja korisnika.

Broj *spyware* programa tijekom posljednjih 5 godina bilježi značajan rast. Uzrok takvog rasta je iskorištavanje marketinških prilika korištenjem *spyware* programa radi stjecanja materijalne ili druge koristi. U samom početku *spyware* programi su korišteni u marketinške svrhe, a poznatiji su i pod nazivom *adware* programi. Međutim, tvrtke sve više i više shvaćaju potencijal koji *spyware* programi imaju u svijetu u kojem se velik broj ljudi služi Internetom, pa stoga potiču razvijenje novih vrsta zlonamjernih *spyware* programa.

Većina korisnika pod terminom *spyware* podrazumijeva zlonamjerne programe za neželjeno oglašavanje, krađu podataka i mnoge druge aktivnosti. Međutim, *Spyware* programe često koriste i administratori mrežnih sustava pri npr. nadgledanju aktivnosti korisnika u sustavu kako bi se sustav zaštitilo od zlonamjernog djelovanja korisnika.

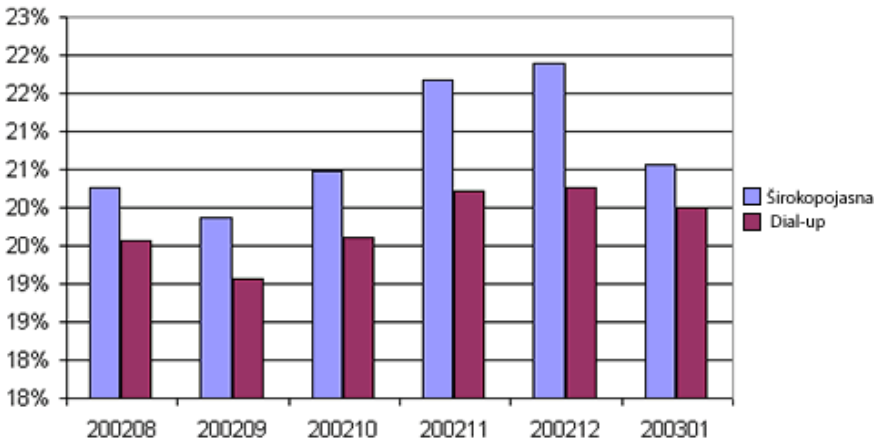
2.2. Statistike

Istraživanja u svrhu izrade statističkih izvješća vezanih uz *spyware* programe iz 2002. godine ukazuju na trend porasta broja *spyware* programa. U nastavku se nalaze grafički prikazi statističkih podataka razvrstani prema kategorijama korisnika (osobne potrebe – „Dom“ i poslovno okruženje – „Posao“).



Slika 2. Prikaz postotka zaraženih računala prema okruženju (08.2002. - 01.2003.)

Kao što je vidljivo iz gornjeg prikaza, u poslovnom se okruženju pridaje veći oprez pri pregledavanju sadržaja Interneta, ali također i da postoji neka vrsta nadzora u odnosu na računala koja korisnici koriste u svome domu. Razlika između postotka zaraženih računala u poslovnom okruženju i broja vlastitih zaraženih računala je u prosjeku između 5-7%.



Slika 3. Prikaz postotka zaraženih računala prema vrsti veze (08.2002. - 01.2003.)

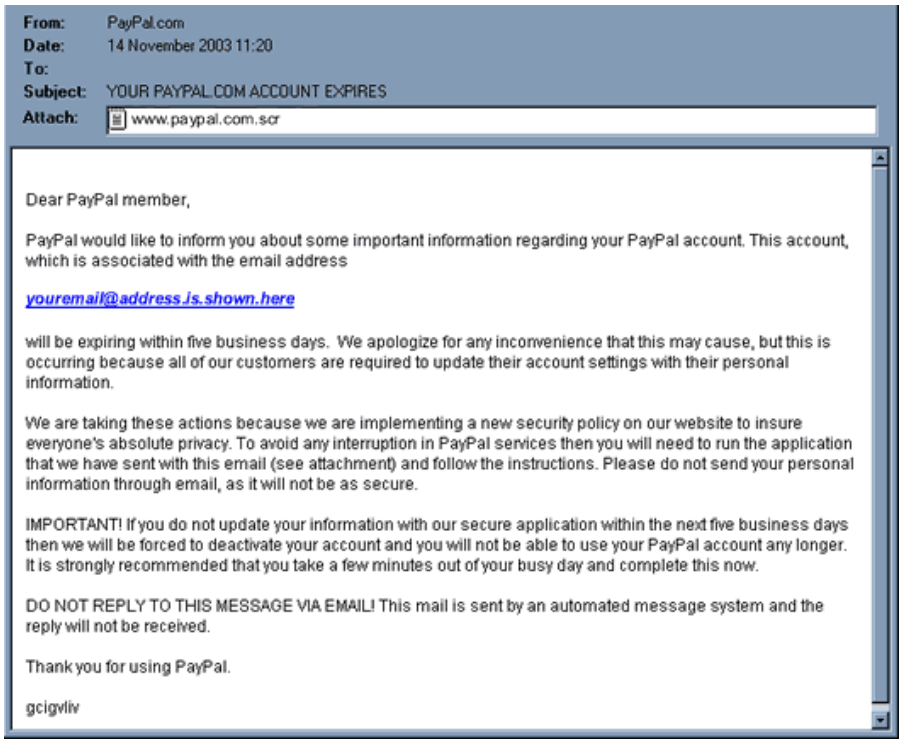
Prikazani dijagram na Slici 3. upućuje na činjenicu da se pojavom širokopojasnog Interneta uvelike povećao i broj računala zaraženih *spyware* programima. Međutim, postotak zaraženih korisnika koji su koristili *dial-up* Internet vezu također je visok. U današnje vrijeme, širokopojasni Internet je postao svakodnevica, stoga je moguće zaključiti da su postoci prikazani u gornjem dijagramu veći za otprilike 3-4 puta.

3. Usporedba s drugim vrstama zlonamjernih programa

Svaki od zlonamjernih programa se razlikuje prema načinu zaraze računala, načinu širenja, opsegu potencijalne štete, itd. Naime, ne mogu svi zlonamjerni programi uzrokovati jednaku štetu, tj. opasnije je (u većini slučajeva) ne opaziti napad na korisnikovu privatnost izveden *spyware* programima nego uočiti zarazu računala virusom koji je onesposobio operacijski sustav računala u izvođenju osnovnih funkcija. Nedostatak stručnosti i znanja često dovodi do krivog razumijevanja opsega potencijalnih šteta koje neki zlonamjerni program može prouzročiti na korisničkom računalu. Korisnici nisu svjesni da je opseg potencijalne štete zarazom *spyware* programima često mnogo veći nego kod zaraze ostalim vrstama zlonamjernih programa (virusima, crvima ili trojanskim konjima). Da bi se razjasnile osnovne razlike i dao uvid u načine zaraze i širenja, te štetu koju pojedine vrste zlonamjernih programa mogu uzrokovati, u nastavku su uspoređene glavne skupine zlonamjernih programa sa *spyware*-om.

3.1. Virusi

Virusi su zlonamjerni programi koji zaraze računalo korisnika bez njegovog znanja ili pristanka s ciljem uzrokovanja štete(brisanje i uništavanje podataka, programa i operacijskih sustava) na korisnikovom računalu. Međutim, rijetki su virusi kojima je cilj nanijeti štetu korisniku u smislu krađe identiteta ili osobnih informacija. Smatra se da napadači nemaju namjeru ugroziti pojedinca i kao takvog ga izložiti opasnostima materijalne ili bilo kakve druge štete, već jednostavno zaraziti čim veći broj računala virusom.


From: PayPal.com
Date: 14 November 2003 11:20
To:
Subject: YOUR PAYPAL.COM ACCOUNT EXPIRES
Attach: www.paypal.com.scr

Dear PayPal member,

PayPal would like to inform you about some important information regarding your PayPal account. This account, which is associated with the email address

youremail@address.is.shown.here

will be expiring within five business days. We apologize for any inconvenience that this may cause, but this is occurring because all of our customers are required to update their account settings with their personal information.

We are taking these actions because we are implementing a new security policy on our website to insure everyone's absolute privacy. To avoid any interruption in PayPal services then you will need to run the application that we have sent with this email (see attachment) and follow the instructions. Please do not send your personal information through email, as it will not be as secure.

IMPORTANT! If you do not update your information with our secure application within the next five business days then we will be forced to deactivate your account and you will not be able to use your PayPal account any longer. It is strongly recommended that you take a few minutes out of your busy day and complete this now.

DO NOT REPLY TO THIS MESSAGE VIA EMAIL! This mail is sent by an automated message system and the reply will not be received.

Thank you for using PayPal.

gcigvliv

Slika 4. Prikaz neželjene poruke e-pošte sa brzom poveznicom

Virusi se najčešće šire putem drugih često korištenih programa ili datoteka na druge dijelove korisnikovog računala bez njegovog znanja ili pristanka. Jedan od čestih načina zaraze računala virusom je putem neželjenih poruka e-pošte (*eng. spam e-mail*). Neželjena poruka e-pošte sadrži

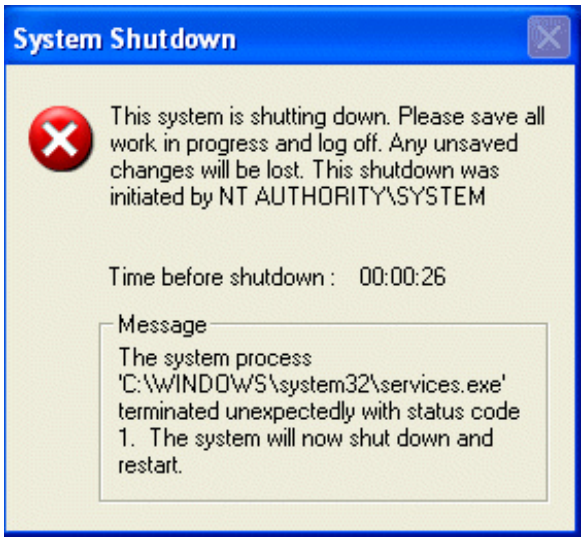
poveznicu (*eng. hyperlink*) koja korisnika vodi na krivotvorenu web stranicu na kojoj se automatski pokreće preuzimanje datoteke bez znanja i pristanka korisnika, ili se automatski pokreće preuzimanje krivotvorenog zlonamjernog programa koji sadrži virusni kod.

Također, moguće je da se zlonamjerni virus nalazi u privitku ovakvih poruka e-pošte, u obliku datoteke ili slike, zavaravajući korisnika da preuzme virus i tako zarazi računalo. Virus nakon preuzimanja zarazi računalo korisnika koristeći napadaču poznate propuste u programima koje korisnik upotrebljava (najčešće web preglednici ili klijenti za e-poštu). Ponovnim pokretanjem tih programa virus se širi na sve dostupne programe i/ili datoteke. Virusi uzrokuju uočljivo neobično i nesvakidašnje ponašanje računala, te štetu na datotekama koje su zarazili svojim kodom.

3.2. Crvi

Crvi (*eng. worm*) su zlonamjerni programi koji se upisuju u radnu memoriju računala i u njoj ostaju aktivni (*eng. memory resident*). Crvi se šire iskorištavanjem propusta u TCP/IP (*eng. Transmission Control Protocol/Internet Protocol)* stogu operacijskih sustava ili programa postavljenih na operacijskom sustavu. Ova vrsta zlonamjernih programa se učitava u radnu memoriju računala sa udaljene lokacije, te se na taj način širi na velik broj računala bez da se zapisuje na tvrdi disk računala. Za razliku od virusa, crvima nisu potrebni programi posrednici kako bi se proširili na što veći broj programa, datoteka, a naposljetku i računala.

Crvi se šire postavljanjem svojih jednakih kopija na druga računala, pa stoga mogu u kratkom vremenu zaraziti velik broj računala. Opseg moguće štete se kreće od uzrokovanja štete na operacijskom sustavu, gašenja računala ili usporavanja rada sa mrežnim resursima.



Slika 5. Prikaz okvira dijaloga pri zarazi crvom koji gasi računalo

3.3. Trojanski konji

Trojanski konji su zlonamjerni programi koji na računalu korisnika ostvaruju mogućnost krađe podataka ili čak preuzimanja nadzora nad računalom. Trojanski se konji najčešće sastoje od dva dijela:

- *poslužitelja* - dio koji se postavlja na računalo korisnika. Pokretanjem poslužitelja napadač je u mogućnosti izvesti napad.
- *klijenta* - program kojim napadač stječe mogućnosti otuđivanja podataka na računalu žrtve.

Napadač mora poznavati IP adresu žrtve kako bi mogao pristupiti računalu. Većina trojanskih konja nakon zaraze zapisuje IP adresu žrtve, te je prosljeđuje napadaču. Najčešći način zaraze računala trojanskim konjima je preuzimanje neke krivotvorene datoteke ili programa s Interneta, pri čemu se trojanski konj predstavlja korisniku kao koristan program. Trojanski konji imaju različite namjene, od uništavanje podataka pa sve do pokretanja drugih vrsta zlonamjernih napada.

3.4. Usporedba zlonamjernih programa

U nastavku dokumenta prikazana je tablica usporedbe navedenih vrsta zlonamjernih programa u odnosu na *spyware* programe kako bi se stekao dojam o opasnostima koje prijete korisnicima, te mogućem opsegu štete koju prikazani zlonamjerni programi mogu uzrokovati na računalu.

Tablica 1. Usporedba zlonamjernih programa

	Spyware	Virusi	Crvi	Trojanski konji
Rezidentnost u radnoj memoriji	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 prisutnosti na računalu	Da	Da	Ne	Ne
Izvori zaraze	Internet	Internet, prijenosni računalni mediji (CD, DVD, USB)	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

4. Vrste spyware programa

Na Internetu je prisutan velik broj različitih vrsta *spyware* programa, međutim općenito ih je moguće svrstati u dvije skupine:

- legalni *spyware* programi (*eng. Domestic Spyware*) i
- komercijalni *spyware* programi (*eng. Commercial Spyware*) – ilegalni zlonamjerni programi.

Legalni *spyware* programi su programi koje su na računala postavili vlasnici tvrtke kako bi administratori mreže bili u mogućnosti nadgledati aktivnosti zaposlenika. Ovakvi se programi najčešće plaćaju, te služe za zaštitu intelektualnog vlasništva, podataka, te mrežnog sustava od mogućih prijetnji.

Također, osim u poslovne svrhe, legalne *spyware* programe je moguće upotrijebiti za nadzor djece i maloljetnika prisutnih na Internetu. Ukoliko roditelji sumnjaju da djeca posjećuju zabranjene ili stranice neprimjerene maloljetnicima, u mogućnosti su na računalo postaviti legalne *spyware* programe koji će praćenjem aktivnosti i bilješkama prikazati rezultate određenih aktivnosti na računalu. Roditelji su u mogućnosti pregledavati bilješke o pregledavanim web stranicama, bilješke o dopisivanju putem programa za razmjenu poruka, poruka e-pošte, itd.

Nesvakidašnji slučajevi, međutim također legalni, su primjeri kada nadležne vlasti imaju mogućnost postavljanja *spyware* programa na računala u svrhu praćenja napadača, kriminalaca i ostalih pojedinaca za koje se sumnja da svojim ponašanjem i postupcima krše određene zakonske okvire.

Komercijalni *spyware* programi su programi koje tvrtke koriste za prikupljanje informacija o korisnikovim navikama pri pregledavanju Internet sadržaja. Takve tvrtke prikupljene podatke prodaju trećim zainteresiranim stranama koje potom korisnike „zatrpavaju“ elektroničkim oglasnim materijalima (oglasima za koje se procjenjuje da su od neke vrste interesa korisniku).

Slika 6. Prikaz zaslona računala zaraženog komercijalnim *spyware* programima

Ovakvi programi su ilegalni, ali vrlo lak način prikupljanja informacija o ciljanim korisnicima. Najveću korist od uporabe ovih programa stekla je marketinška industrija zbog čega su *spyware* programi sveprisutni i potrebno je obratiti pažnju pri pregledavanju Interneta, pogotovo pri posjećivanju nepoznatih web stranica, preuzimanju programa nepoznatih autora, itd.

Spyware programe je također moguće razvrstati prema namjeni, i to u sljedeće kategorije:

- Internet URL zapisivači (*eng. Internet URL Loggers*),
- snimači zaslona (*eng. Screen Recorders*),
- snimači poruka e-pošte (*eng. e-mail Recorders*),
- zapisivači razgovora (*eng. Chat Loggers*),
- zapisivači tipki (*eng. Keyloggers*),
- snimači lozinki (*eng. Password Recorders*),
- kolačići za praćenje (*eng. Tracking Cookies*),
- otimači web preglednika (*eng. Browser Hijackers*),
- otimači veze - dialer programi (*eng. Modem Hijackers*) i
- otimači računala (*eng. PC Hijackers*).

U nastavku poglavlja je ukratko opisana svaka od navedenih vrsta *spyware* programa.

4.1. Internet URL zapisivači

Internet URL (*eng. Uniform Resource Locator*) zapisivači su programi koji nadgledaju i bilježe adrese web stranica koje je korisnik posjetio. Ovi programi rade neovisno o vrsti korištenog web preglednika (Microsoft Internet Explorer, Mozilla Firefox, Opera, Google Chrome, itd.). Postavljaju se na tvrdi disk računala, te neprekinuto rade tijekom povezanosti na Internet.

Internet URL zapisivači spadaju i u legalne i komercijalne *spyware* programe, jer ih je moguće koristiti u svrhu nadgledanja posjećenih web stranica (nadređene osobe ili roditelji), ali i u svrhu prikupljanja informacija o korisniku kako bi se saznali njegovi interesi.

4.2. Snimači zaslona

Snimači zaslona su programi koji napadaču omogućuju nadgledanje svih korisnikovih radnji na računalu u obliku snimki zaslona (*eng. Screenshot*) malene veličine ili video zapisa. Nakon zaraze, ovakvi se programi postavljaju na tvrdi disk računala. Većina ovakvih programa ima tzv. okidač, tj. algoritam kojim se uključuju. Okidači su najčešće radnje korisnika na računalu poput pokretanja web preglednika ili drugih programa.

Ova je vrsta *spyware* programa posebno opasna upravo zato jer može snimiti svaku korisnikovu radnju na računalu, od upisivanja povjerljivih informacija (korisničkih imena, lozinki, brojeva kreditnih kartica, itd.) do datoteka koje sadrže podatke. Nakon snimanja zaslona, program na zadanu lokaciju šalje rezultate aktivnosti nadgledanja korisnika, bez znanja ili pristanka korisnika. Ovakve je programe također moguće koristiti legalno, međutim češći su primjeri ilegalne upotrebe.

4.3. Snimači poruka e-pošte

Snimači poruka e-pošte, kao što i samo ime kaže, imaju svrhu nadgledanja i snimanja podataka vezanih uz e-poštu. Ovakvi programi bilježe sve podatke vezane uz poslane i primljene poruke e-pošte (naslov poruke, naslove privitaka, sadržaj poruke, pošiljatelja i primatelja, itd). Otkrivene aktivnosti zapisuju u datoteke, te šalju na zadano odredište. Ovakvi programi se često sastoje od dva dijela, *spyware* programa za nadgledanje, te odredišnog sučelja na kojem se prikazuju rezultati nadzora u obliku tekstualne datoteke.

Programe za snimanje poruka e-pošte je moguće na vlastitu odgovornost preuzeti putem Interneta, međutim nisu besplatni i preuzimanje istih se ne preporuča jer mogu sadržavati druge *spyware* zlonamjerne programe. Kao i u prethodnim primjerima, zabilježeni su slučajevi korištenja ove vrste *spyware* programa u legalne svrhe, ali češći su slučajevi ilegalne upotrebe.

4.4. Chat loggeri

Chat loggeri su programi koji zapisuju svaku vrstu razgovora vođenu putem programa za razmjenu poruka (*eng. Instant Messaging*) poput Windows Live Messenger, Google Chat, AOL Messenger, itd. Ovi programi bilježe sve podatke vezane uz razgovore (datum i vrijeme dolazne poruke, odlazne poruke, pošiljatelje i primatelja itd.).

Iako se ovakvi programi smatraju vrlo korisnim alatom za nadzor djece i maloljetnika na Internetu, mogu se pokazati izrazito opasnim za privatnost korisnika ukoliko su postavljeni na računalo korisnika s namjerom narušavanja privatnosti.

4.5. Keyloggeri

Ovi programi predstavljaju izrazitu opasnost za korisnike jer bilježe svaku pritisnutu tipku na tipkovnici. Napadač je u mogućnosti ovom vrstom zlonamjernog programa nanijeti veliku štetu korisniku čije je računalo zaraženo. Svaka pritisnuta tipka se zapisuje u tekstualnu datoteku, te potom šalje na unaprijed određeno odredište.

Keylogger programe je vrlo teško neprimjetno postaviti na računalo zaštićeno antivirusnim alatom, stoga se najčešće nalaze u kombinaciji sa virusom ili trojanskim konjem koji imaju mnogo veću mogućnost proboja na korisnikovo računalo. Kao zaštita od *keylogger* programa preporuča se uporaba antivirusnih i *antispyware* alata, ali također i programa koji imaju funkciju „maskiranja“ pritisnutih tipki, tj. *keyscrambler* programa.

4.6. Snimači lozinki

Snimači lozinki ciljano nadgledaju i bilježe samo pritisnute tipke pri upisu iste u polje za lozinku. Primjerice, ako se korisnik želi prijaviti na određeni web servis kako bi izveo željene radnje. Za napadača pribavljanje korisničkog imena korisnika predstavlja jednostavniji postupak od pribavljanja lozinke, stoga u takvim slučajevima snimači lozinki napadačima olakšavaju zlonamjernu djelatnost.

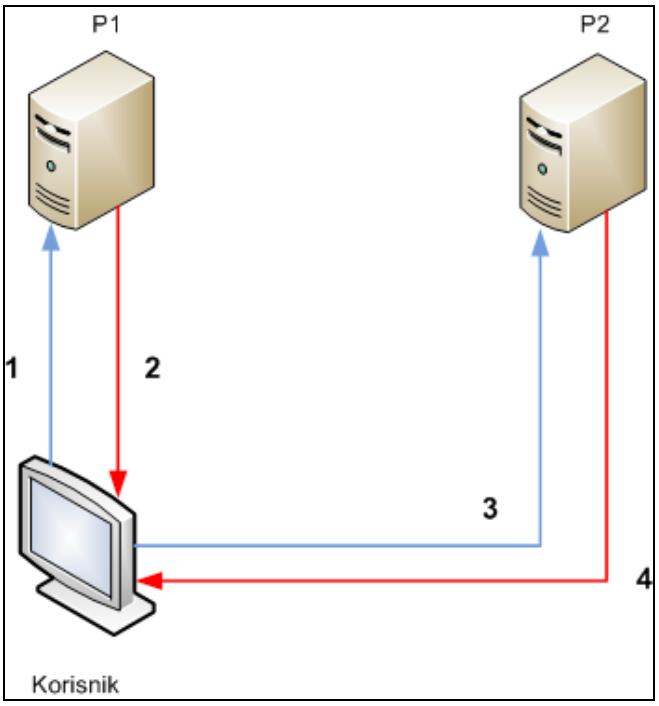
Snimači lozinki predstavljaju veliku opasnost za web servise i korisnike koji ne koriste dvofaktorsku ili više faktorsku autentikaciju. Više o autentikaciji moguće je doznati u dokumentu „Tehnike generiranja jednokratnih lozinki“ (CCERT-PUBDOC-2009-04-262) objavljenom na službenim stranicama CERT-a.

4.7. Kolačići za praćenje

Općenito, termin kolačić u računalnom svijetu označava podatke na računalu koji je pohranio web preglednik. Kolačići mogu sadržavati korisničke postavke, identifikacijske podatke za poslužitelja, te druge podatke koje web stranice mogu koristiti.

Kolačići za praćenje se koriste za nadgledanje i stvaranje bilješki o korisnikovim navikama vezanim uz pregledavanje Interneta. Poslužitelj svake web stranice koju korisnik posjeti u trenutnom radnom okviru dijaloga web preglednika stvara bilješke u obliku kolačića. Pregledavanjem bilješke preglednika (*eng. Log file*) moguće je doznati koje je web stranice korisnik posjetio u koje vrijeme. Web stranice koriste praćenje kolačićima kako bi doznale broj posjetitelja, vrijeme i datum posjeta, itd. Međutim, praćenje povijesti pregledanih web stranica koriste i marketinške tvrtke kako bi doznale navike korisnika što se smatra ilegalnom radnjom. Na ovaj način ugrožava se privatnost korisnika.

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.



Slika 7. Prikaz zaraze kolačićima za praćenje

Zaraza se odvija kako slijedi:

1. Korisnik šalje poslužitelju 1 (P1) zahtjev za učitavanje tražene web adrese.
2. Poslužitelj 1 korisniku informaciju da se neke datoteke sa web stranice nalaze na poslužitelju 2 (P2), te ga preusmjerava na njega.
3. Web preglednik korisnika šalje poslužitelju 2 zahtjev za preuzimanje datoteka.
4. Poslužitelj 2 korisniku šalje tražene datoteke, ali i kolačiće za praćenje.

4.8. Otimači web preglednika

Otimači web preglednika su vrsta *spyware* programa koja pri zarazi korisnikovog računala zamjenjuje početnu web stranicu, stranicu pogreške i Internet tražilicu preglednika sa vlastitom. Ovakvi se programi najčešće koriste kako bi se promet preusmjerio na željenu web stranicu zbog povećanja zarade na elektroničkim reklamnim materijalima koji su prikazani na odredišnoj web stranici.

Postoje primjeri ovakvih programa koji također prikupljaju podatke o korisniku. Većina ovakvih programa neće dopustiti korisniku da promijeni početnu web stranicu u željenu, međutim uz zaštitu antivirusnim i *antispyware* programima korisnik će biti u mogućnosti otkloniti ovu vrstu zlonamjernog programa. Neki *antispyware* programi pri zarazi otimačem web preglednika obavještavaju korisnika da je početnu web stranicu promijenio neki program, te zahtijevaju pokretanje pretraživanja računala u svrhu pronalaska *spyware* programa.

4.9. Otimači veze

Ova vrsta *spyware* programa učinkovita je jedino pri povezivanju računala na Internet putem *dial-up* veze, tj. izravnim spajanjem telefonske žice u računalo. *Dialer* je zlonamjerni program koji se spaja na Internet putem analogne telefonske ili ISDN (*eng. Integrated Services Digital Network*) veze.

Dialer programi pokušavaju uspostaviti vezu na Internet putem brojeva sa skupim tarifama ili brojeva iz drugih zemalja, što korisniku nanosi vrlo veliku materijalnu štetu. Ovakvi se programi najčešće postavljaju na računalo korisnika zbog otvaranja neželjenih poruka e-pošte ili preuzimanja programa putem Interneta. Zabilježeni slučajevi diljem svijeta svjedoče o velikim materijalnim štetama za korisnike. U Hrvatskoj su 2007. godine također zabilježeni slučajevi djelovanja *dialer* programa pri čemu su iznosi računa telefonskih usluga iznosili i do 18.000 kn. Pojavom širokopojasnog Interneta onemogućeno je djelovanje ovih programa.

4.10. Otimači računala

Uporabom širokopojasnog Interneta i visokih brzina pri pregledavanju pojavila se nova vrsta *spyware* programa - otimači računala. Naime, napadač pomoću ovakvog programa može preuzeti nadzor nad računalom i koristeći se brzom vezom povezivanja na Internet slati nebrojeno mnogo neželjenih poruka e-pošte na ciljane adrese e-pošte.

Napadači najčešće ciljaju korisnike koji imaju izuzetno pogodne uvjete za ovakve radnje, tj. visoku brzinu širokopojasnog Interneta (2 Mb/s naviše). Žrtve ovakvih napada najčešće ne primjećuju da je putem njihovog računala izvedena nezakonita radnja. Ukoliko ponuđač Internet usluga otkrije ovakvu radnju kod nekog korisnika moguće je isključenje usluge, pa čak i primjena zakonskih mjera.

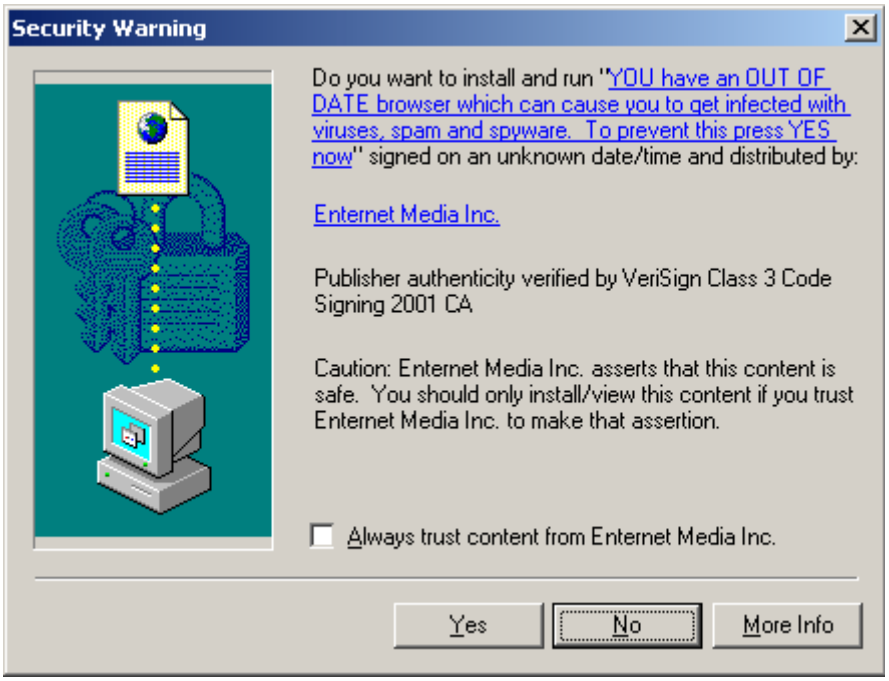
5. Načini zaraze spyware programima

Spyware programi se razlikuju od virusa, crva i trojanskih konja po tome što najčešće ne mogu raditi svoje kopije na zaraženom računalu, tj. napraviti što više jednakih kopija radi otežavanja otkrivanja antivirusnim ili *antispyware* alatom. Najčešći način zaraze *spyware* programima je putem Interneta. Kao što je ranije napomenuto, *spyware* programi se na računalo korisnika postavljaju zavaravanjem korisnika ili iskorištavanjem sigurnosnih propusta u korištenim operacijskim sustavima ili programima.

Gotovo svi *spyware* programi se postavljaju na računalo bez znanja ili pristanka korisnika, stoga se pokazuje važnim korisnike osvijestiti o mogućim načinima zaraze . Velik broj korisnika je svjestan da su *spyware* programi štetni za podatke na računalu, njihovu privatnost i normalan rad računala, pa primjenjuju oprez pri pregledavanju sadržaja Interneta. Međutim, napadači se služe raznim prijevarama kako bi postavili svoje *spyware* programe na računala korisnika.

Jedan od čestih načina zaraze je iskorištavanje sigurnosnih propusta u web preglednicima. Tako se primjerice velik broj korisnika web preglednika Internet Explorer susreo sa iznenadnim upitom za postavljanje zlonamjerne *ActiveX* kontrole na računalo. *ActiveX* kontrole služe za određivanje komponenata (npr. funkcija nekog web servisa) koje obavljaju određene funkcije ili više funkcija u Microsoft Windows operacijskom sustavu. Microsoft Internet Explorer je najčešće korišteni preglednik, ali istovremeno i web preglednik sa dugom povijesti sigurnosnih propusta koje zlonamjerni programi mogu iskoristiti.

Kada korisnik posjeti zlonamjernu stranicu pojavi se upit za postavljanje zlonamjerne *ActiveX* kontrole.



Slika 8. Prikaz *ActiveX* kontrole koja na računalo postavlja *spyware* program

Na slici je moguće uočiti da se korisnika pita želi li na svoje računalo postaviti ponuđenu *ActiveX* kontrolu. Ukoliko korisnik odluči postaviti ponuđenu kontrolu na računalo, isto biva zaraženo *spyware* programom. Naravno, koristeći se prijevarom, napadač u objašnjenju zahtjeva za postavljanje navodi razne razloge koji bi mogli zabrinuti korisnika, te ga privući da *spyware* program postavi na vlastito računalo. Najčešći navodi u ovakvim primjerima su obavijesti o zaraženosti računala zbog neprimjerene zaštite računala. U ovakvim je slučajevima preporučeno, kao mjera opreza, napustiti posjećenu web stranicu.

Također, jedan od načina zaraze *spyware* programima je postavljanje na računalo „besplatnih" programa koji osim svojih funkcionalnosti sadrže i *spyware* program. Poznat slučaj ovakvog načina zaraze je u slučaju P2P (*eng. Peer-To-Peer*) programa za preuzimanje sadržaja sa Interneta „*Kazaa*" (alat koji se koristi za preuzimanje multimedijskih i drugih datoteka i podataka izravno od drugog korisnika). Naime, već pri instalaciji, tj. pri pregledu ugovora s krajnjim

korisnikom (*eng. End User License Agreement*) potrebno je dati pristanak za postavljanje željenog programa na računalo, ali zajedno s istim i drugih programa (*spyware*) čije funkcionalnosti nisu objašnjene niti prikazane. Međutim, tvrtku *Sharman Networks* se također optužuje za postavljanje drugih *spyware* programa na računala korisnika bez znanja ili pristanka.

Slika 9. Prikaz okvira dijaloga pri instalaciji P2P programa *Kazaa*

Neki od *spyware* programa koje je na računalo postavljao program *Kazaa* su:

- razni Internet URL zapisivači koji su unaprijed određenim tvrtkama slali podatke o navikama korisnika pri pregledavanju sadržaja Interneta i
- razni otimači web preglednika koji su korisnike preusmjeravali na unaprijed određene web servise radi materijalne koristi.

Zbog otkrića da program *Kazaa* na računala korisnika također postavlja i *spyware* programe zaustavljena je distribucija ovog programa, te su izdana upozorenja korisnicima.

Napadač postavljanjem zlonamjernog koda u web stranicu može iskoristiti sigurnosne propuste u web pregledniku i automatski pokrenuti preuzimanje *spyware* programa na računalo korisnika. Ukoliko korisnik posjeti takvu web stranicu koja sadrži zlonamjerni kod, te ukoliko sigurnosni propust u web pregledniku nije ispravljen, nemoguće je utjecati na proces preuzimanja *spyware* programa na računalo korisnika. U ovakvim slučajevima korisnici nisu svjesni da su preuzeli zlonamjerni program pa stoga ne mogu uočiti niti zarazu sve dok ne pokrenu neki *antispyware* program.

Napadači mogu *spyware* programe korisnicima predstaviti kao korisne programe (npr. dodatke web preglednicima, alate za zaštitu od *spyware* programa, itd.), te na prijevaru zaraziti korisnikovo računalo. Razlika između *spyware* programa i trojanskih konja je da se kod trojanskih konja korisniku nudi koristan program koji sadrži i zlonamjerni kod. Takvi su programi sve češći i češći na Internetu. Autori ovakvih programa su nepoznati ili navedene tvrtke zapravo ne postoje, stoga je vrlo važno informirati se prije odabira alata za zaštitu.

Slika 10. Prikaz *spyware* programa predstavljenog kao *antispyware* program

6. Negativni efekti zaraze

Na računalu zaraženom *spyware* programom najčešće je moguće pronaći više izvora zaraze, tj. više *spyware* programa. Jedan od najčešćih simptoma koje korisnici nakon zaraze *spyware* programima zamjećuju su čudno ponašanje i vrlo usporen rad računala u odnosu na normalno stanje.

Neki od efekata zaraze računala *spyware* programima mogu biti:

- visoka aktivnost procesora računala, iako korisnik ništa ne radi,
- porast zauzetog prostora na tvrdom disku,
- pojava elektroničkih reklamnih materijala,
- „smrzavanje“ programa,
- nemogućnost ispravnog pokretanja računala,
- „smrzavanje“ računala,
- nemogućnost ostvarivanja veze na Internet i
- nemogućnost ostvarivanja veze na lokalnu mrežu (*eng. Local Area Network*).

U nekim slučajevima, zaraza *spyware* programima nema niti jedan od gore navedenih simptoma, te predstavlja posebnu opasnost. Ukoliko korisnik nema primjerenu zaštitu nije u mogućnosti otkriti ovakve *spyware* programe, što može uzrokovati velike nevolje po pitanju privatnosti korisnika. Nadalje, moguće je da *spyware* programi onesposobe vatrozide (*eng. firewall*) i antivirusne alate, te na taj način omoguće zarazu još većim brojem zlonamjernih programa. Također, poznato je da *spyware* programi mogu utjecati na sigurnosne postavke web preglednika smanjenjem razine ili potpunim uklanjanjem sigurnosnih elemenata web preglednika.

6.1. Elektronički reklamni materijali

Velik broj *spyware* programa nakon zaraze računala prikazuje neželjene elektroničke reklamne materijale. Ti se reklamni materijali prikazuju pokretanjem određenog programa, najčešće web preglednika, u nekom unaprijed zadanom vremenskom periodu. Neki *spyware* programi prikazuju reklamne materijale s obzirom na sadržaj web stranice koju je korisnik posjetio.

Slika 11. Prikaz zaslona računala zaraženog *spyware* programima za prikaz reklamnih materijala

U ovakvim se reklamnim materijalima često mogu naći oglasi neprimjerenog sadržaja, stoga ovakva vrsta marketinških aktivnosti podliježe i dodatnim kaznenim mjerama.

6.2. Krađa identiteta i prijevara

Krađa identiteta u svrhu ostvarivanja materijalne koristi ili prijevare drugih pojedinaca smatra se teškim prekršajem, te se u nekim državama kažnjava izuzetno strogim mjerama (SAD). Najvažnija funkcija *spyware* programa je nadzor i otkrivanje povjerljivih podataka te osobnih informacija što predstavlja veliku prijetnju za korisnike.

Krađom identiteta napadač je u mogućnosti nanijeti materijalnu štetu ili štetu ugledu korisnika lažno se predstavljajući drugim pojedincima ili servisima koje korisnik uobičajeno upotrebljava.

6.3. Špijunaža

Termin špijunaže se u ovom kontekstu ponajprije odnosi na nadziranje navika korisnika i intelektualnog vlasništva pojedinca ili tvrtke, što može rezultirati ozbiljnim gubicima. Svaki pojedinac ima zakonsko pravo na vlastitu privatnost koja se narušava *spyware* programima. Otkrivanje osobnih informacija bez korisničkog znanja ili pristanka predstavlja opasnost za korisnika isto kao i za njegovu okolinu, te predstavlja ilegalnu aktivnost.

Spyware programi prikupljaju informacije o korisnicima, te na temelju tih (ilegalno prikupljenih) informacija ostvaruju financijsku dobit.

Također je korisno navesti nadzor zaposlenika pomoću *spyware* programa na radnom mjestu. Ukoliko je nekim službenim dokumentom tvrtke (npr. sigurnosnom politikom) unaprijed određen takav postupak, radnje vezane uz nadzor se smatraju zakonitim.

6.4. Primjeri

Među najpoznatijim primjerima postavljanja *spyware* programa na računala korisnika je slučaj vezan uz tvrtku *Sony*. Naime, tvrtka *Sony* je na glazbene CD medije proizvedene 2005. godine postavljala, uz glazbeni sadržaj, dva dodatna programa kojima je ugrozila korisnike koji su pokušali CD medije preslušavati na računalu. Odmah po ubacivanju CD medija u računalo, bez znanja i pristanka korisnika pokrenula se instalacija tih programa. Programi su opasni jer su na računalo korisnika postavljali *spyware* program, otvarajući mogućnost zaraze drugim zlonamjernim programima. Protiv navedene tvrtke pokrenuti su brojni sudski postupci vezani uz ovaj slučaj, te isplaćene naknade korisnicima koji su ugroženi ovim proizvodom (otprilike 20.000 USD po korisniku.

Američka federalna trgovačka komisija (*eng. US Federal Trade Commission*) je u nekoliko navrata sudskim postupcima pokušala prisiliti tvrtke proizvođače *spyware* programa da zaustave zarazu računala. Zabilježen je slučaj u kojem je tvrtka *Seismic Entertainment Productions* zbog zaraze računala *spyware* i drugim zlonamjernim programima te uzrokovanja štete na računalima bila prisiljena isplatiti iznos od otprilike 3.5 milijuna američkih dolara (17 milijuna kuna). Slična je optužnica podignuta i protiv tvrtke *CyberSpy Software LLC*, a postupak je još u tijeku. Više o navedenim slučajevima moguće je saznati na adresama:

http://www.ftc.gov/opa/2006/11/seismicodysseus.shtm
http://www.ftc.gov/opa/2008/11/cyberspy.shtm
http://docs.law.gwu.edu/facweb/claw/FTCcrackSpyw.pdf

Za europski primjer je korisno navesti slučaj u Nizozemskoj gdje je „Nezavisna agencija za nadzor pošte i telekomunikacija“ (*eng. Independent Authority of Posts and Telecommunications*) s milijun eura kaznila vlasnike i direktore tvrtki čiji nazivi nisu objavljeni jer su s namjerom nadgledanja korisničkih aktivnosti, a suprotno zakonskim okvirima, na 22 milijuna računala postavile *spyware* program pod nazivom „DollarRevenue”.

7. Načini zaštite

Iako *spyware* programi predstavljaju veliku opasnost za računala koja zbog neprimjerene zaštite ili ljudske pogreške imaju visoku stopu zaraze, moguće je obraniti se od ovih zlonamjernih programa. Najbolja pomoć za obranu protiv *spyware* programa je svakako primjerena edukacija korisnika. Velik pomak u edukaciji korisnika o *spyware* programima napravila je udruga *Anti-Spyware Coalition*. Detaljnim opisima i definicijama te korisnim savjetima vezanim uz *spyware* programe prikazali su običnom korisniku opasnosti koje zaraza računala *spyware* programima nosi. Detaljnije informacije o navedenoj udruzi nalaze se na web adresi:

http://www.antispywarecoalition.org

Sama edukacija korisnika o ovoj temi nije dovoljna jer se *spyware* programi postavljaju na računalo bez ikakvih upozorenja, stoga se preporuča korištenje provjerenih *antispyware* alata. Trenutno većina proizvođača antivirusnih rješenja ima u ponudi i *antispyware* programe, ali učinkovitost tih proizvoda ne mora biti na jednakoj razini kao i antivirusnih programa. Naime, velik broj uglednih proizvođača antivirusnih programa je kupio male tvrtke proizvođače *antispyware* programa, te proizvode tih malih tvrtki prodaju pod vlastitim imenom. Prije odabira kvalitetnog i pouzdanog *antispyware* programa potrebno je pregledati stručne komentare proizvoda koji će dati precizniji uvid u svojstva proizvoda. Na tržištu postoje programi koje je potrebno plaćati, ali i oni koji su besplatni za korištenje. Korisno je napomenuti da je i proizvođač operacijskih sustava Microsoft napravio korak ka zaštiti korisnika od *spyware* programa. Naziv Microsoftovog programa je *Windows Defender* i besplatan je za preuzimanje korisnicima operacijskih sustava Windows.

Antispyware programi mogu raditi na dva načina:

1. *Stalna zaštita (eng. Real Time Protection)* - *antispyware* program je stalno aktivan u radnoj memoriji računala te neprestano nadzire aktivnosti na računalu. Ukoliko se neki *spyware* program pokuša postaviti na računalo, *antispyware* program automatski blokira postavljanje i na taj način osigurava zaštitu računala, podataka i korisnika.
2. *Na zahtjev (eng. On Demand)* - *antispyware* program pregledava računalo kako bi otkrio je li računalo zaraženo nekim *spyware* programom. Pregled može pokrenuti korisnik, a moguće je namjestiti i željeni raspored pregleda računala koji se pokreće automatski.

U nastavku su ukratko navedena svojstva dva popularna *antispyware* programa koji su besplatni za korištenje, *Lavasoft Ad-Aware* i *Spybot - Search and Destroy*.

7.1. Lavasoft Ad-Aware

Lavasoft Ad-Aware je, kao što je ranije napomenuto, besplatan za korištenje ali moguće je i kupiti inačicu koja, ovisno o željenom paketu, ima proširene mogućnosti (antivirusna zaštita, zaštita mrežnog sustava, besplatna tehnička podrška, itd.). Ovaj program ima mogućnost stalne zaštite, ali i pokretanja pregleda na zahtjev. Program se redovito ažurira *antispyware* definicijama koje tvrtka Lavasoft redovito postavlja. *Lavasoft Ad-Aware* glasi kao jedan od pet najkvalitetnijih *antispyware* programa prema stručnim e-časopisima (u konkurenciji s programima *Spy Sweeper*, *Spyware Doctor*, *STOPzilla* i *Anti Malware*). Stoga se preporuča korisnicima koji nisu spremni izdvojiti novčana sredstva za nabavu ovakvog programa. Korisničko sučelje je jednostavno za korištenje i vrlo razumljivo.

Navedeni program moguće je besplatno preuzeti sa službenih web stranica tvrtke Lavasoft:

http://www.lavasoft.com/products/ad_aware_free.php?t=techspecs

Slika 12. Prikaz korisničkog sučelja *antispyware* programa *Lavasoft Ad-Aware*

Kao što je vidljivo iz gornjeg prikaza, na početnom prikazu je moguće saznati vrijeme i datum posljednjeg pregleda računala, status stalne zaštite, te jesu li *antispyware* definicije ažurirane.

7.2. Spybot - Search and Destroy

Program Spybot - Search and Destroy može otkriti i izbrisati *spyware* programe, a uz to može popraviti i izbrisati ActiveX kontrole, kolačiće, te ostale dijelove programa koji mogu ugroziti računalo ili korisnika. Program je u potpunosti besplatan za kućnu upotrebu, ali se upotreba u poslovne svrhe plaća.

Slika 13. Prikaz korisničkog sučelja *Spybot - Search and Destroy antispyware* programa

Program se redovito ažurira *antispyware* definicijama, međutim nema mogućnost stalne zaštite, već jedino uklanjanja *spyware* programa. Iako ovaj program uspijeva izbrisati većinu poznatih *spyware* programa, problem je što nepoznate *spyware* programe ne uspijeva ukloniti. Program je dostupan na nekoliko jezika među kojima je i hrvatski. Korisničko sučelje jednostavno je za korištenje i pogodno za upotrebu. Program je moguće preuzeti sa službenih web stranica:

http://www.safer-networking.org/hr/spybotsd/index.html

7.3. Preporuke

Najbolja zaštita od *spyware* programa je na prvom mjestu osviještenost korisnika o potencijalnim opasnostima i štetama koje *spyware* programi mogu uzrokovati. Stručnjaci preporučaju poduzimanje sljedećih koraka kako bi se korisnik zaštitio od *spyware* programa:

- redovito ažuriranje sigurnosnih zakrpa za programe isto kao i onih za operacijske sustave,
- optimalno postavke sigurnosti i privatnosti u web pregledniku - više je moguće saznati u dokumentu „Metode za poboljšanje sigurnosti web preglednika“ (CCERT-PUBDOC-2009-09-276) objavljenom na službenim stranicama CERT-a,
- preuzimanje programa s Interneta samo s službenih stranica,
- obvezno čitanje sigurnosnih upozorenja, ugovora i ostalih dokumenata vezanih uz postavljanje programa na računalo,
- oprez pri pregledavanju sadržaja Interneta i pri pojavi sumnjivih i/ili neobičnih okvira dijaloga,
- primjena opreza pri preuzimanju besplatnih programa i
- korištenje dostupnih alata za otkrivanje i brisanje *spyware* programa s računala.

8. Zaključak

Spyware programi otkriveni su tek 1999. godine, te su se u 10 godina proširili na procjenjuje se više od 55% računala diljem svijeta. Teško je prosuditi točan smjer evolucije *spyware* programa, ali sasvim je izvjesna činjenica da neće jednostavno nestati. *Spyware* programi se šire poput parazita, velikom brzinom zaraze velik broj računala. Gledajući prema dosadašnjoj stopi razvoja, *spyware* programi će postati veća i opasnija prijetnja od bilo kojeg drugog zlonamjernog programa jer na drugim vrstama zlonamjernih programa nema toliko prilike za ostvariti materijalnu ili bilo kakvu drugu dobit. Broj računala zaraženih *spyware* programima daleko je veći nego broj računala zaraženih virusima i drugim zlonamjernim programima, što upućuje na veliku opasnost.

U ranijim godinama, *spyware* programi su bili relativno jednostavni, međutim bilo ih je teško za otkriti jer javnost nije obraćala mnogo pažnje na njih. Korisnici nisu bili u mogućnosti pronaći ovakve programe na računalu niti ih ukloniti. Danas je razina svijesti o *spyware* programima veća jer su korisnici shvatili o kakvim se zapravo opasnostima radi. Za očekivati je da će u budućnosti biti mnogo teže pronaći *spyware* programe prisutne na računalu korisnika jer *spyware* programi još uvijek imaju mogućnost korištenja tehnika prikrivanja koje mogu preuzeti od virusa, crva ili drugih vrsta zlonamjernih programa. Zaraze će postajati sve složenije, počevši od jedne datoteke nasumičnog imena zapisane na tvrdom disku, pa do velike količine zapisa u registru operacijskog sustava ili konfiguracijskim datotekama. Pitanje je vremena kada će *spyware* programi preuzeti sva svojstva virusa i drugih zlonamjernih programa kako bi prikrili svoju prisutnost na nekom računalu i progresivno se širili.

Na korisnicima je da odluče o razini znanja koju žele usvojiti o *spyware* programima. Edukacija, kao prva mjera opreza kada su u pitanju *spyware* programi (a i računalne sigurnosti općenito), je značajan korak ka zaštiti podataka i samog računala. Također, korištenje *antispyware* alata uvelike pomaže pri zaštiti, otkrivanju i brisanju *spyware* programa sa računala. Uz postojanje besplatnih *antispyware* alata korisnicima je uvelike olakšano korištenje računala na Internetu. Pregledavanjem sumnjivih web stranica ili instalacijom besplatnih programa čiji su autori nepoznati, korisnici riskiraju vlastitu sigurnost. Uvijek je korisno napomenuti da se velik dio zaštite od zlonamjernih programa pripisuje primjeni opreza pri pregledavanju sadržaja Interneta.

Bitka sa *spyware* programima će se svakako nastaviti jer pripadaju industriji koja na njima (ilegalno) stječe veliku materijalnu korist. Mogući način zaustavljanja epidemije *spyware* programa je uvođenje strogih zakonskih okvira koji će novčanim i drugim mjerama kažnjavati tvrtke koje na ovaj ilegalan način krše privatnost korisnika. Nezakonito zadiranje u korisnikovu privatnost mora biti kažnjeno odgovarajućim mjerama. Nevjerojatna je činjenica da tvrtke za koje je javno obznanjeno da se bave ovom djelatnosti pomoću *spyware* programa imaju zakonske temelje za opstanak na tržištu. Kao što je navedeno u dokumentu, postoje slučajevi kažnjavanja tvrtki koje su s namjerom prikupljanja podataka o korisnicima, međutim teško je prosuditi zadovoljavaju li novčani iznosi izrečenih kazni štetu nanesenu korisnicima.

9. Reference

[1] Spyware programi, http://en.wikipedia.org/wiki/Spyware, listopad 2009.

[2] Statistike o utjecaju spyware programa, http://www.lavasoft.com/support/spywareeducationcenter/spyware_statistics.php, listopad 2009.

[3] Statistike o spyware programima, http://www.aladdin.com/csrt/spyware-statistics.aspx, 2009.

[4] Usporedba: virusi, crvi, trojanski konji i spyware programi, http://www.networkingreviews.com/2008/03/22/comparison-virus-warm-adware-spyware-trojan/, ožujak 2009.

[5] Vrste spyware programa, http://anti-spyware-review.toptenreviews.com/types-of-spyware.html, 2009.

[6] Kolačići za praćenje, http://en.wikipedia.org/wiki/HTTP_cookie#Tracking, listopad 2009.

[7] Otimači web preglednika, http://en.wikipedia.org/wiki/Browser_hijacker, listopad 2009.

[8] Kazaa P2P program, http://en.wikipedia.org/wiki/Kazaa#Bundled_malware, 2009.

[9] Antispyware dokumenti, http://www.antispywarecoalition.org/documents/index.htm, 2009.

[10] Lavasoft Ad-Aware, http://www.lavasoft.com/products/ad_aware.php, 2009.

[11] Spybot - Search and Destroy, http://www.safer-networking.org/hr/download/index.html, 2009.