Centar Informacijske Sigurnosti

Besplatna zaštita desktop računala

kolovoz 2011.

CIS-DOC-2011-08-021

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

Prava korištenja

Sadržaj

1. Uvod

Svi korisnici računala žele nesmetano koristiti sve mogućnosti koje računala pružaju. Prijetnje sigurnom i nesmetanom korištenju računala su razni zlonamjerni programi. Riječ je o programima koji su dizajnirani za rušenje ili prekid operacija, skupljanje informacija koje vode prema gubitku privatnosti ili eksploataciji, dobivanje neovlaštenog pristupa resursima sustava i drugo zloćudno ponašanje. Zlonamjerni programi se mogu podijeliti na inficirajući, prikrivajući te profitni zlonamjerne programe. Više o zlonamjernim programima može se naći u nastavku dokumenta u poglavlju 3. Protiv zlonamjernih programa razvijaju se razni programi zaštite. Programi zaštite se mogu podijeliti na antivirusne, *anti-spyware*, vatrozid, *pop-up* blokere te filtre elektroničke pošte. Antivirusni programi koriste se za zaštitu od računalnih virusa i ostalih zlonamjernih prijetnji. Oni najčešće sadrže komponente pomoću kojih se, osim virusa, mogu detektirati te ukloniti i ostale vrste prijetnji, primjerice crvi, *rootkit* programi i trojanski konji. Više o zaštiti od zlonamjernih programa opisuju poglavlja 4 i 5. Opis najpoznatijih i najraširenijih besplatnih programa za zaštitu desktop računala dan je u poglavlju 5. Tamo su opisani najpoznatiji besplatni antivirusni alati Avast! Free Antivirus i Avira AntiVir Personal Edition. Također, dan je i kratak opis besplatnih *anti-spyware* alata Spybot - Search & Destroy i Windows Defender, zatim besplatnih vatrozida Comodo Internet Security i ZoneAlarm Free Firewall te besplatnih *pop-up* blokera i filtara elektroničke pošte.

Programi za zaštitu desktop računala mogu biti komercijalni i besplatni. Komercijalne je potrebno platiti, ali oni sadrže i neke povlastice koje besplatni alati nemaju, primjerice zaštitu u stvarnom vremenu i unaprijeđenu bazu podataka. Usporedba komercijalnih i besplatnih programa zaštite desktop računala dana je u poglavlju 6, dok se u poglavlju 7 može više pročitati o tome što se očekuje od besplatnih programa zaštite desktop računala u budućnosti.

2. Zašto štititi desktop računala?

Posjet nekim web stranicama može biti štetan za računalo, jer se većina zloćudnih programa i kodova skriva upravno na webu čekajući trenutak kada će se probiti u korisnički sustav. Bez obzira na to koliko je korisnik oprezan i izbjegava zaražene stranice, postoje trenuci kada će čak i u sustav iskusnih korisnika prodrijeti prijetnja. Osnovni način zaštite računala je korištenje nekog dobrog antivirusnog programa za zaštitu od zloćudnih programa.

Antivirusni i *antispyware* programi te usluge su napravljeni tako da pomognu održati računala sigurnima i oni mogu spriječiti potencijalne katastrofe koje se događaju kada u sustav uđu zlonamjerni programi. Računala s antivirusnim i *antispyware* programima nisu ranjiva na većinu zlonamjernih programa. Iz tog je razloga vrlo važno imati dobar program za zaštitu desktop računala. Razlozi za korištenje programa za zaštitu desktop računala navedeni su u nastavku i prikazani slikom (Slika 1):

Slika 1. Razlozi za zaštitu desktop računala
Izvor: LSS

- U prvom redu bitno je zaštiti računalo, iako to nije jedini razlog za posjedovanje dobrog programa.
- „*It will work while you play*“ („Radit će dok se korisnik igra“). Dobar sigurnosni program omogućuje korisniku da se koncentrira na stvari koje želi raditi. Dok korisnik radi na nekom izvješću ili igra računalne igrice, program radi u pozadini skenirajući računalo i tražeći zaražene datoteke u sustavu.
- Znak da korisnik posjeduje dobar program je taj da on provjerava svaki paket informacija koji je unesen u računalo. Ako nešto nije u redu, obavijestit će korisnika o tome i izolirati program. Izolacija programa se radi tako da se zaraženi program ili datoteka sprema u karantenu (posebno mjesto na računalo u koje se premještaju svi sumnjivi programi da bi se spriječilo njihovo pokretanje) dok se obavljaju daljnje provjere nad njim.
- Automatsko stvaranje sigurnosnih kopija (eng. *backup*) za računalo. Osim osiguravanja sustava od štetnih elemenata, dobar program će automatski spremiti sigurnosne kopije na izdvojenu lokaciju na koju se korisnik može kasnije referencirati ukoliko to poželi.
- Omogućavanje dobre sigurnosti podataka i sustava. Sigurnosni program štiti podatke od ciljanih ili nasumičnih napada zloćudnih napadača i zlonamjernih programa, ali također i od različitih unutarnjih i vanjskih prijetnji.
- Spremnost kada je to potrebno. Ako korisnik ima instaliran napredniji program za zaštitu, to mu omogućava rana upozorenja i signale kojima program osigurava da virusi i prijetnje budu detektirani i zaustavljeni prije nego što naprave ikakvu štetu.

- Posjedovanje unutarnje zaštite. Mnogi programi imaju sposobnost slijediti i pratiti unutarnju aktivnost korisnika, što pomaže u identificiranju pristupa i curenja informacija. Svaki korisnik ostavlja elektronički trag, a ova opcija omogućuje praćenje tog traga.

3. Prijetnje desktop računalima

3.1. Svrha malicioznih programa

Mnogi rani infektivni programi, uključujući i prvog internetskog crva (Morrisov crv) te veliki broj MS-DOS virusa, bili su pisani kao eksperimenti ili šale. Namjera im je bila da budu bezopasni ili dosadni, a ne da nanesu ozbiljnu štetu računalnim sustavima. U nekim slučajevima, počinitelj nije bio svjestan koliko bi štete njegova djela mogla napraviti. Mladi programeri koji su učili o virusima i njihovim tehnikama pisali su ih kao vježbu ili da vide koliko daleko su se mogli proširiti. Čak i dosta kasnije, 1999. godine, jako rašireni virusi kao što su Melissa i David bili su napisani kao obične šale. Prvi virus na mobilnim telefonima, Cabir, pojavio se 2004. godine.

Zloćudne namjere povezane s vandalizmom nalaze se u programima dizajniranima da prouzroče štetu ili gubitak podataka. Mnogi DOS virusi i Windows crvi, bili su dizajnirani da uništavaju datoteke na tvrdom disku ili sam datotečni sustav pišući pogrešne podatke na njega. Crvi koji se prenose mrežom, kao primjerice Code Red iz 2001. godine, spadaju u istu kategoriju. Napravljeni kako bi vandalizirali web stranice, crvi su zapravo *online* ekvivalent crtanju grafita s autorovim pseudonimom koji se pojavljuje svugdje gdje se crv nađe.

Od porasta i širenja širokopojasnog pristupa Internetu, zlonamjerni programi se počinu dizajnirati za profit, primjerice za prisiljeno oglašavanje. Tako od 2003. godine većina široko raširenih virusa i crva su dizajnirani kako bi preuzeli kontrolu nad računalima korisnika za iskorištavanje na crnom tržištu. Zaražena „*zombie*“ računala se koriste za slanje neželjenih poruka elektroničke pošte, zatim kako bi bila domaćin zabranjenim podacima kao što je dječja pornografija ili kako bi sudjelovala u distribuiranim napadima odbijanja usluge kao obliku ucjene.

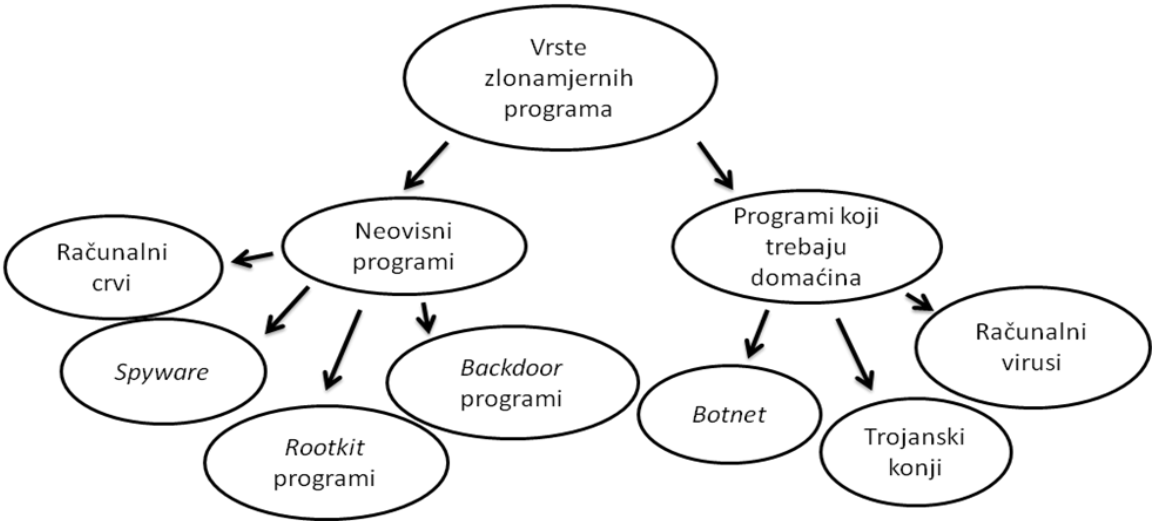
Još jedna striktno profitna kategorija zlonamjernih programa se pojavljuje u obliku *spywarea*, programa dizajniranih za nadziranje korisnikovog pretraživanja weba, prikazivanje neželjenih elektroničkih oglasa ili preusmjeravanje dohotka oglašavanja ka tvorcu *spywarea. Spyware* programi se ne šire poput virusa, već su instalirani iskorištavanjem sigurnosnih rupa ili dolaze u paketu s programima koje korisnik instalira, kao što su primjerice *peer-to-peer* aplikacije.

3.2. Zloćudni programi

Zlonamjerni ili zloćudni programi (eng. *Malware*), čije je ime nastalo kao skraćenica od eng. *malicious software*, sastoje se od programa (kodova, skripta, aktivnog sadržaja i drugih oblika programa) dizajniranih za rušenje ili prekid operacija, skupljanje informacija koje vode prema gubitku privatnosti ili eksploataciji, dobivanje neovlaštenog pristupa resursima sustava te ostalo zloćudno ponašanje. Izraz je općeniti termin kojeg koriste računalni stručnjaci, a obuhvaća razne oblike neprijateljskih i napadačkih programa ili programskog koda (Slika 2).

Glavna značajka po kojoj se program smatra zloćudnim je namjena koju stvaratelj takvog programa želi postići. Pojam uključuje računalne viruse, crve, trojanske konje, *spyware*, nečisti *adware*, *scareware, crimeware*, većinu *rootkita*, te ostale zloćudne i neželjene programe. U pravnom rječniku, zlonamjerni programi su poznati i pod nazivom „zaraživači računala“ (eng. *Computer contaminant*), a taj se naziv koristi u pravnim zakonima nekoliko sjevernoameričkih država, uključujući i Kaliforniju te Zapadnu Virginiju.

Preliminarni rezultati organizacije Symantec objavljeni 2008. godine sugerirali su da broj proizvedenih zloćudnih programa i ostalih neželjenih programa vjerojatno čak i premašuje broj legitimnih programa. Prema organizaciji F-Secure, 2007. godine je proizvedeno toliko zlonamjernih programa kao u prijašnjih 20 godina ukupno. Najčešći put kojeg tvorci zlonamjernih programa koriste kako bi došli do korisnika je Internet, a to se primarno odnosi na elektroničku poštu i WWW (eng. *World Wide Web*).



Slika 2. Vrste malicioznih programa
Izvor: LSS

Nadmoćnost zloćudnih programa kao pokretača organiziranog internetskog kriminala, skupa s činjenicom o općenitoj nemogućnosti tradicionalne *anti-malware* zaštite da se odupre kontinuiranoj proizvodnji jedinstvenih i novih zlonamjernih programa, rezultirala je potpuno novim načinom razmišljanja o vođenju poslova na Internetu. Došlo je do saznanja da će neki broj internetskih korisnika uvijek biti zaražen iz nekog razloga te da se mora nastaviti poslovati i sa zaraženim korisnicima. Rezultat toga je značajan naglasak na tzv. *back-office* sustave, dizajniranim da uoče neovlaštene aktivnosti povezane s naprednim zloćudnih programima na korisničkim računalima.

Bitno je naglasiti da zlonamjerni program nije isto što i neispravan program, tj. program koji ima legitimnu svrhu, ali sadrži štetne pogreške. Ponekad je zlonamjerni program prerušen kao obični program i može se pojaviti na legitimnim stranicama. Iz tog razloga, neki sigurnosni programi, kao primjerice McAfee, zlonamjerne programe nazivaju potencijalno neželjenim programima (eng. *Potentially Unwanted Programs*, PUP). Iako je računalni virus zlonamjerni program koji se sam može reproducirati, taj termin se često pogrešno upotrebljava kako bi se označila cijela kategorija zlonamjernih programa.

3.2.1. Inficirajući zlonamjerni programi

Najpoznatiji tipovi inficirajućih zlonamjernih programa, virusi i crvi, najpoznatiji su po svom specifičnom načinu širenja. Termin računalni virus se koristi za program koji je inficirao neki izvršni program i pri pokretanju uzrokuje širenje virusa na druge izvršitelje. Virusi također mogu sadržavati i korisni sadržaj koji izvodi neke druge akcije, često zloćudne. S druge strane, crv je program koji se aktivno prenosi mrežom kako bi zarazio druga računala. On također može sadržavati i korisni sadržaj. Ove definicije vode prema zaključku kako virus zahtijeva korisničku intervenciju za širenje, dok se crv širi automatski. Koristeći ovaj zaključak, infekcije koje se šire elektroničkom poštom ili Microsoft Word dokumentima, a koje se oslanjaju na primatelja koji otvara datoteku ili poštu i pritom zarazi sustav, su klasificirane kao virusi, a ne kao crvi.

- **Virusi**

Prije nego što je pristup Internetu postao raširen, virusi su se širili na osobnim računalima inficirajući pokretačke sektore disketa. Umetanjem svoje kopije u instrukcije strojnog koda, virusi su pokretani kad god je bio pokretan program ili sam sustav. Rani računalni virusi su bili pisani za sustave Apple II i Macintosh, ali su postali raširenij s dominacijom sustava IBM PC i MS-DOS. Virusi koji inficiraju izvršne datoteke su ovisni o izmjenjivanju programa među korisnicima ili pokretačkim disketama pa se šire brzo u računalnim krugovima. Porastom korištenja platformi Microsoft Windows u 1990-im godinama i prilagodljivim makronaredbama njenih programa, postalo je moguće pisati inficirajući kod u makro jeziku Microsoft Worda i sličnim programima. Ovi makro virusi inficirali su dokumente , a ne

programe (izvršne datoteke), ali su se oslanjali na činjenicu da su makronaredbe u Word dokumentima zapravo oblik izvršnog koda.

- **Crvi**

Prvi crvi, inficirajući programi prenošeni mrežom, nisu potekli s osobnih računala, već sa sustava Unix. Prvi poznati crv pojavio se 1988. godine, a inficirao je sustave SunOS i VAX BSD. Za razliku od virusa, ovaj crv se nije umetao u druge programe, već je iskorištavao sigurnosne rupe (ranjivosti) u mrežnim poslužiteljima i pokretao se kao odvojeni proces. Na isti način se ponašaju i današnji crvi. Danas se crvi uglavnom pišu za operacijske sustave Windows, iako ih je nekoliko, kao crvi Mare-D ili Lion,napisano i za sustave Linux te Unix. Današnji crvi u principu rade na isti način kao i Internetski crv iz 1988. godine. Oni skeniraju mrežu i utječu na ranjiva računala kako bi se replicirali. Pošto ne trebaju ljudsku intervenciju, crvi se šire nevjerojatnom brzinom. Primjerice, crv SQL Slammer je inficirao tisuće računala u samo nekoliko minuta.

3.2.2. Prikrivajući zlonamjerni programi

- **Trojanski konj**

Kako bi zloćudni program postigao svoje ciljeve, mora raditi bez zatvaranja ili brisanja od strane korisnika ili administratora računalnog sustava na kojem je pokrenut. Prikrivenost može u prvom redu pomoći zlonamjernom programu kako bi uopće bio instaliran. Kada je zloćudni program prerušen kao nešto bezazleno ili poželjno, korisnici se nađu u kušnji da ga instaliraju bez znanja o tome što on zapravo radi. Ovo je tehnika koju koristi trojanski konj ili trojanac. Općenito, trojanski konj je bilo koji program koji privuče korisnika na njegovo pokretanje, prikrivajući štetan i zloćudan sadržaj. Taj sadržaj može djelovati odmah, što vodi mnogim nepoželjnim učincima kao što su brisanje korisnikovih podataka ili daljnja instalacija zloćudnih ili nepoželjnih programa. Trojanski konji poznati kao *dropperi* koriste se kako bi započeli proboj crva, tj.- ubacivanje crva u lokalnu mrežu korisnika. Jedan od najpoznatijih načina distribuiranja *spywarea* je također trojanski konj, spojen s dijelom korisnog programa kojeg korisnik preuzme s Interneta. Kada korisnik instalira program, *spyware* se instalira zajedno s njim. Autori *spywarea* koji pokušavaju djelovati na legalan način koriste ugovor o licenci u kojem se nalazi zapis o ponašanju *spywarea*, kojeg korisnici rijetko čitaju ili razumiju.

- ***Rootkit***

Jednom kada je maliciozni program instaliran na sustav, nužno je da ostane prikriven, kako bi izbjegao detekciju i uklanjanje. Isto vrijedi i kada ljudski napadač izravno upadne u računalo. Aplikacije poznate kao *rootkit* programi dopuštaju to prikrivanje modificirajući operacijski sustav domaćina i sakrivajući na taj način zlonamjerni program od korisnika. *Rootkit* može spriječiti vidljivost zloćudnog procesa u listi procesa sustava ili pak spriječiti čitanje njegovih podataka. Originalno, *rootkit* je bio skup alata koje napadač instalira na sustavu Unix, dozvoljavajući korisniku dobivanje administratorskog, odnosno korijenskog (eng. *Root*) pristupa. Danas se ovaj termin koristi mnogo općenitije kao naziv za tehnike prikrivanja u zloćudnim programima. Neki zloćudni programi sadrže module za obranu od uklanjanja, ne kako bi se sakrili, već kako bi suzbili pokušaje odstranjivanja iz sustava. Rani primjer takvog ponašanja je uočen u Jargon File paru programa koji su napadali sustav Xerox CP-V . Svaki „program duh“ je detektirao činjenicu kako je drugi proces ugašen te je započinjao novu kopiju nedavno ugašenog programa u nekoliko milisekundi. Jedini način za gašenje oba duha je bilo istovremeno gašenje (vrlo teško izvedivo) ili namjerno rušenje sustava. Slične tehnike koriste neki moderni zlonamjerni programi, koji započinju određeni broj procesa za nadziranje i ponovno započinju jedan drugoga po potrebi. U slučaju kada korisnik pokrene operacijski sustav Microsoft Windows zaražen takvim programom, ako ga želi ručno zaustaviti, može koristiti karticu *„processes”* Task Managera kako bi našao glavni proces (onaj koji uvijek iznova pokreće tzv. „uskrsnule procese“) i pokrenuti funkciju '*end process tree*', koja neće uništiti samo glavni proces, već i procese nastale od njega. Neki zlonamjerni programi koriste i druge tehnike, kao što je imenovanje zaražene datoteke slično legitimnoj ili provjerenoj datoteci (npr. expl0rer.exe).

- ***Backdoor***

Backdoor je metoda zaobilaženja normalne procedure autentikacije. Jednom kada je sustav kompromitiran (jednom od gore navedenih metoda, ili nekim drugim načinom), jedan ili više *backdoor* programa mogu biti instalirani kako bi omogućili lakši pristup u budućnosti. *Backdoor* također može biti instaliran prije zlonamjernog programa kako bi napadaču omogućio ulaz. Postojala je ideja da proizvođači računala unaprijed instaliraju *backdoor* na svoje sustave kako bi korisnicima omogućili tehničku podršku, ali to nikad nije pouzdano realizirano. Napadači tipično koriste *backdoor* programe kako bi osigurali daljinski pristup računalu, dok pokušavaju ostati prikriveni. Za instalaciju *backdoor* programa, napadači mogu koristiti trojanske konje, crve ili neke druge metode.

3.2.3. Profitni zlonamjerni programi

Tijekom 1980-ih i 1990-ih godina, uzimalo se zdravo za gotovo kako su zlonamjerni programi nastali kao oblik vandalizma ili šale. Nešto kasnije, najveći dio takvih programa napisan je iz profitnih razloga (financijski ili neki drugi). Zapravo, ovo se može shvatiti kao izbor autora zlonamjernih programa da unovče kontrolu nad zaraženim sustavima, tj. da pretvore tu kontrolu u izvor prihoda.

- ***Spyware***

Spyware programi se komercijalno proizvode u svrhu prikupljanja informacija o korisnicima računala, pokazujući im *pop-up* oglase ili mijenjajući ponašanje web preglednika u financijsku korist autora *spywarea*. Primjerice, neki *spyware* programi preusmjeravaju pretraživače na plaćene stranice s oglasima. Ostali, često u medijima nazivani "*stealware*", prepišu marketinške kodove tako da preusmjeravaju prihod tvorcu *spywarea* umjesto prvotnom primatelju. *Spyware* programi su ponekad instalirani kao trojanski konji neke vrste, a razlikuju se po tome jer ih njihovi tvorci prezentiraju otvoreno kao poslove, primjerice prodajući prostor za oglašavanje na *pop-up* reklamama stvorenim zlonamjernim programom. Većina takvih programa predstavi korisnicima ugovor (licencu) koji sadržajem štiti autora od optužbe za računalnu kontaminaciju. Ipak, *spyware* EULA (eng. *End User License Agreement*) još uvijek nije podržan na sudu.

- ***Spam***

Još jedan način koji je financijski motivirao tvorce zlonamjernih programa da profitiraju od svojih djela je direktna upotreba zaraženih računala za rad za svoje tvorce. Zaražena računala se tako koriste za slanje neželjenih poruka elektroničke pošte (eng. *spam*). Računalo u tom stanju je poznato pod nazivom *zombie* računalo. Prednost upotrebe zaraženih računala je ta da ona omogućavaju anonimnost, te štite spamere od suđenja. Spameri također koriste zaražena računala kako bi teretili anti-spam organizacije s raširenim napadima odbijanja usluge.

- ***Botnet***

Kako bi koordinirali aktivnost mnogo zaraženih računala, napadači koriste koordinirajuće sustave poznate pod nazivom *botnet*. U *botnetu*, zlonamjerni program ili *malbot* se prijavljuje na IRC (eng. *Internet Relay Chat*) ili neki drugi sustav za razmjenu poruka, tako da napadač može davati instrukcije svim zaraženim sustavima istovremeno. Botnet se može koristiti i kako bi doveo unaprijeđeni program do zaraženog sustava, čuvajući njegovu otpornost na antivirusni program ili druge sigurnosne mjere.

- ***Key logger***

Tvorac zlonamjernog programa može profitirati krađom osjetljivih informacija žrtve. Neki programi instaliraju *key logger* program, koji presreće korisnikove pritiske tipki dok unosi lozinke, brojeve kreditnih kartica ili druge korisne informacije koje se mogu zloupotrijebiti. To se izravno prenosi tvorcu zlonamjernih programa, omogućavajući razne vrste prijevara. Slično tome, takav program može kopirati i CD (eng. *Compact Disc*) ključ ili lozinku za *online* igre, omogućavajući svom tvorcu krađu računa ili virtualnih predmeta.

- ***Dialer***

Još jedan način krađe novca od vlasnika zaraženog računala je preuzimanje kontrole nad *dial-up* modemom i pozivanje skupih brojeva. *Dialer* poziva telefonsku liniju primarne brzine

prijenosa (s posebnim tarifama naplate) kao primjerice američki „broj 900“, ostavljajući liniju otvorenu i naplaćujući poziv korisniku.

3.2.4. Zlonamjerni programi za krađu podataka

Zlonamjerni programi za krađu podataka je web prijetnja kojom se kradu žrtvini osobni podaci i podaci o vlasništvu s namjerom unovčavanja ukradenih podataka izravnom upotrebom ili ilegalnom distribucijom. Prijetnje sadržaju koje spadaju pod ovu skupinu programa su: *keylogger, screen scraper, spyware, adware, backdoor* i *bot*. Ovaj termin se ne odnosi na aktivnosti kao što su *spam, phishing*, DNS (eng. *Domain Name System*) trovanje itd. Ipak, kada ove prijetnje rezultiraju preuzimanjem datoteka ili izravnom instalacijom, kao što se to događa kod većine napada, datoteke koje služe kao agenti za zamjenske informacije spadaju u kategoriju zlonamjernih programa za krađu podataka. Svojstva ovakvih programa su da ne ostavljaju tragove događaja, skrivaju se u web prometu, ometaju kriptiranje diska, itd. Primjeri zlonamjernih programa za krađu podataka su:

- **Bancos** – krade informacije i čeka korisnike da pristupe web stranicama banki, zatim ometa tu stranicu kako bi ukrao povjerljive informacije.
- **Gator** – *spyware* koji prikriven motri navike korisnika u pretraživanju weba, šalje podatke na analizu i zatim korisniku šalje ciljane *pop-up* oglase.
- **LegMir** – *spyware* koji krade osobne informacije kao što su korisnička imena i lozinke povezane s *online* igrama.
- **Ohost** – trojanski konj koji modificira „*Hosts*“ datoteku preusmjeravajući se na drugi DNS poslužitelj pri posjećivanju stranica banki, a zatim otvara autentikacijsku stranicu kako bi ukrao podatke za prijavu.

3.3. Grayware

Grayware (ili *Greynet*) je termin korišten za klasifikaciju programa koji se ponašaju na nepoželjan način, ali nisu toliko štetni niti nose ozbiljne prijetnje kao zlonamjerni programi. Naziv *grayware* obuhvaća *spyware, adware, dialer*, šaljive programe, alate za daljinski pristup i druge neželjene datoteke ili programe osim onih koji su dizajnirani kako bi naštetili radu računala na mreži. Termin *grayware* je u upotrebi od rujna 2004. godine.

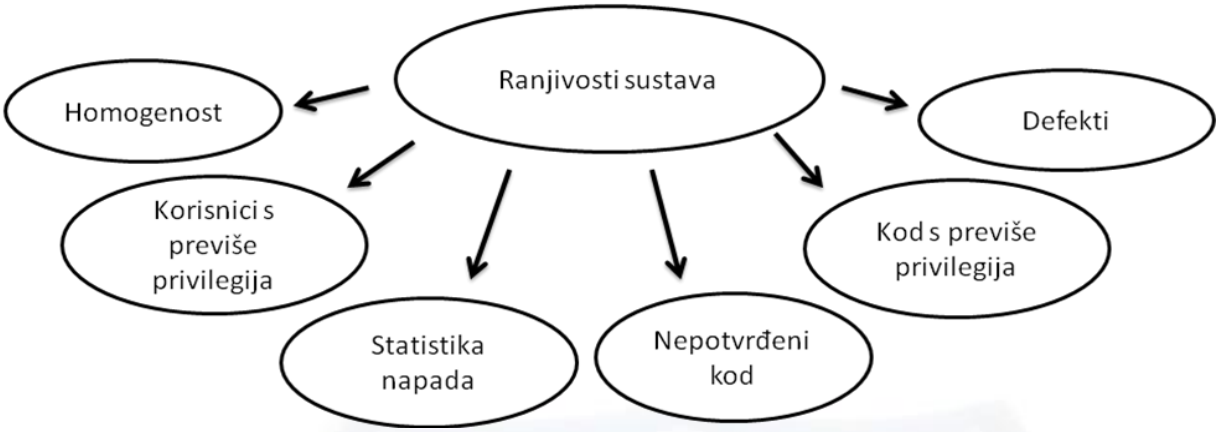
Grayware se odnosi na programe ili datoteke koje nisu klasificirani kao virusi, trojanski konji i slično, ali ipak negativno utječu na rad računala i unose značajne sigurnosne rizike organizaciji. Često *grayware* izvodi mnoštvo neželjenih akcija, kao što su dosađivanje korisnicima s *pop-up* prozorima, praćenje korisničkih navika i nepotrebno izlaganje računala ranjivostima.

Spyware je program koji instalira komponente na računalo u svrhu snimanja korisničkih navika u pretraživanju weba (primarno u marketinške svrhe). *Spyware* šalje te informacije svom autoru ili drugim zainteresiranim stranama dok je računalo na mreži. *Spyware* se često preuzme s programima identificiranim kao „besplatna preuzimanja“ te ne obavijesti korisnika o svom postojanju, niti pita dopuštenje za instalaciju svojih komponenti. Informacije koje *spyware* skuplja mogu uključivati pritisak na tipke na tipkovnici, a one mogu sačinjavati privatne informacije kao što su korisnička imena, lozinke i brojeve kreditnih kartica.

Adware je program koji prikazuje reklamne oglase u internetskim preglednicima kao što su Internet Explorer ili Mozilla Firefox. Iako se ne kategorizira kao zlonamjerni programi, većina korisnika smatra *adware* invazivnim. *Adware* programi često stvaraju neželjene učinke na sustavu, kao što su dosadni *pop-up* oglasi i općenita degradacija bilo u mrežnoj povezanosti ili u radu sustava. *Adware* programi se tipično instaliraju kao odvojeni programi grupirani s određenim besplatnim programom. Mnogi korisnici nesvjesno pristaju na instalaciju *adwarea* prihvaćajući EULAugovor prilikom instalacije besplatnih programa. *Adware* se često instalira u kombinaciji sa *spyware* programima. Oba programa potpomažu međusobne funkcionalnosti. *Spyware* programi promatraju ponašanje korisnika na Internetu, dok *adware* programi prikazuju oglase koji odgovaraju informacijama dobivenih s profila korisnika.

4. Zaštita desktop računala

Općenito, pod pojmom napadnutog sustava podrazumijeva se samostalno računalo i operacijski sustav, mreža ili program. Različiti faktori koji čine sustav ranjivijim dani su u nastavku i prikazani slikom (Slika 3).



Slika 3. Ranjivosti od strane malware programa
Izvor: LSS

- **Homogenost** – primjerice kada sva računala na mreži koriste isti operacijski sustav pa se preko iskorištavanja jednog računala mogu iskoristiti i sva ostala.
- **Statistika napada** – jednostavno iz razloga što je velika većina zlonamjernih programa pisana kako bi napala sustave Windows, većina takvih sustava ranjiva je na napade (bez obzira na sigurnosnu snage ili slabosti samog sustava Windowsa).
- **Defekti** –zlonamjerni program utječe negativno na dizajn operacijskog sustava.
- **Nepotvrđeni kod** – kod s diskete, CD-ROM-a ili USB (eng. *Universal Serial Bus*) uređaja može se izvršiti bez pristanka korisnika.
- **Korisnici s previše privilegija** – neki sustavi dopuštaju svim korisnicima mijenjanje njihove unutarnje strukture.
- **Kod s previše privilegija** – neki sustavi dopuštaju kodu pokrenutom od strane korisnika da dosegne sva prava tog korisnika.

Čest uzrok ranjivosti mreža je homogenost ili programska monokultura. Primjerice, sustavi Microsoft Windows ili Apple Mac imaju veliki udio na tržištu pa koncentracija na jednog od njih može omogućiti napadaču rušenje velikog broja sustava. Umjesto toga, uvođenje nehomogenosti (raznolikosti), upravo zbog otpornosti, može povećati kratkoročne troškove održavanja sustava. Ipak, posjedovanje nekoliko različitih čvorova bi onemogućilo rušenje cijele mreže i omogućilo tim čvorovima da pomognu pri oporavku onih zaraženih. Tako odvojena, funkcionalna redundancija izbjegla bi cijenu cjelokupnog rušenja sustava i time bi se riješio problem štete svim računalima u nekoj mreži.

Većina sustava sadrži greške ili rupe u programskim funkcijama, koje zlonamjerni program može iskoristiti. Tipični primjer je slabost prekoračenja veličine međuspremnika, pri kojoj sučelje dizajnirano za spremanje podataka u malu količinu memorije dopušta pozivatelju nabavku više podataka nego što stane. Ti dodatni podaci se zapišu preko izvedbene strukture samog sučelja. Na taj način, zlonamjerni program može prouzročiti da sustav izvršava zaraženi kod, nadomještanjem legitimnog koda s vlastitim instrukcijama (ili vrijednostima podataka) kopiranima u pravu memoriju, izvan područja međuspremnika.

U početku, računala su pokretana s disketa pa su ne tako davno diskete bile uobičajeni uređaji za podizanje sustava. To je značilo da iskvarena disketa može srušiti računalo prilikom podizanja, a isto se odnosi i na CD-e, iako to danas više nije toliko uobičajeno.

U nekim sustavima, korisnici koji nisu administratori imaju previše privilegija, u smislu da imaju mogućnost modificirati unutarnju strukturu sustava. U nekim okruženjima, korisnici imaju previše privilegija jer im je dodijeljen status administratora ili neki drugi sličan status koji im ne pripada. Ovo

je primarno konfiguracijska odluka, ali na sustavima Microsoft Windows uobičajena konfiguracija je ta da se korisniku dodjeljuje previše privilegija. Ovakva situacija vlada zbog odluke tvrtke Microsoft kako bi povećali kompatibilnost sa starim sustavima povrh sigurnosne konfiguracije u novijim sustavima te zato što su tipične aplikacije razvijane bez razmišljanja o manje privilegiranim korisnicima. Kako se povećavalo iskorištavanje privilegija, prioritet se pomiče uoči izdavanja operacijskog sustava Microsoft Windows Vista. Kao rezultat toga, mnoge postojeće aplikacije koje zahtijevaju prevelike privilegije mogu imati probleme u kompatibilnosti s sustavom Vista. Ipak, značajka User Account Control u operacijskom sustavu Vista pokušava popraviti aplikacije koje nisu dizajnirane za niže privilegirane korisnike, ponašajući se kao most u rješavanju problema privilegiranog pristupa prisutnog u naslijeđenim aplikacijama.

Zlonamjerni program, koji se pokreće kao previše privilegirani kod, može iskoristiti te privilegije kako bi srušio sustav. Gotovo svi poznati operacijski sustavi te mnoge skriptne aplikacije dopuštaju kodu previše privilegija, uglavnom tako da kada korisnik izvrši taj kod, sustav prepusti kodu sva prava tog korisnika. Na taj način korisnik postaje ranjiv u obliku dodataka elektroničke pošte, koji mogu, ali i ne moraju biti prerušeni. U posljednje vrijeme se sve češće upozorava korisnike da otvaraju samo one dodatke kojima vjeruju te da budu obazrivi prema kodu primljenom od nepoznatih izvora. Također je uobičajeno da su operacijski sustavi dizajnirani tako da njihovi pokretački programi zahtijevaju povećane privilegije, dok ih opskrbljuje sve veći broj proizvođača sklopovlja.

Kod s prevelikim privilegijama datira iz vremena kada je većina programa bila dostavljana skupa s računalom ili pisana kod kuće, a popravljanje tog koda bi jednim potezom učinilo većinu antivirusnih programa suvišnim. Sustav bi morao zadržati privilegirane profile te znati koje primijeniti za svakog pojedinog korisnika i program. U slučaju novo instaliranog programa, administrator bi morao ponovno postaviti zadane profile za novi dio koda. Eliminacija ranjivosti pokretačkih programa je teža nego kod proizvoljnih izvršnih programa. Dvije tehnike koje mogu pomoći, korištene u sustavu VMS (eng. *Virtual Memory System*), su označavanje memorije samo onih registara uređaja koji su u pitanju i sučelje sustava koje povezuje upravljački program s prekidima iz uređaja. Ostali pristupi su:

- različiti oblici virtualizacije, koji dopuštaju kodu neograničen pristup samo virtualnim resursima,
- različiti oblici sigurnosnih mehanizama, kao što su Sandbox ili Jail te
- sigurnosne funkcije Jave u komponenti *java.security*.

Ovakvi pristupi, ako nisu potpuno integrirani s operacijskim sustavom, udvostručit će uloženi trud te neće biti globalno primjenjivani, što će štetno utjecati na sigurnost.

5. Besplatni programski alati za zaštitu desktop računala

Kako su napadi zlonamjernim programima postajali sve češći počeli su se razvijati i specifični programi za borbu protiv njih. *Anti-malware* programi se mogu boriti protiv zlonamjernih programa na dva načina:

- Mogu priuštiti zaštitu protiv instalacije programa zaraženog zloćudnim programom na računalo. Ovaj tip zaštite od zloćudnih programa radi na isti način kao i antivirusna zaštita, tako da *anti-malware* program skenira sve nadolazeće podatke s mreže tražeći program zaražen zlonamjernim programom i blokira sve uočene prijetnje.
- *Anti-malware* programi se mogu koristiti isključivo za detekciju i otklanjanje programa zaraženog zloćudnim programom koji je već instaliran na računalu. Ovaj tip zaštite od zlonamjernih programa je mnogo poznatiji i lakši za korištenje. Ovakav *anti-malware* program skenira sadržaj registara, datoteka i programa u operacijskom sustavu te osigurava listu pronađenih prijetnji, dopuštajući korisniku izbor podataka koje želi izbrisati ili zadržati te mogućnost usporedbe te liste s listom poznatih zloćudnih komponenti, uklanjajući pritom odgovarajuće datoteke.

Zaštita od zlonamjernih programa radi na isti način kao i antivirusna zaštita. Program skenira podatke na disku za vrijeme preuzimanja i blokira aktivnost komponenata poznatih kao zloćudni program. U nekim slučajevima, može prekinuti i pokušaje instalacije pokretačkih podataka ili modifikacije postavki preglednika. Upravo iz razloga što su mnoge komponente zlonamjernih programa instalirane kao rezultat iskorištavanja slabosti Internet preglednika ili pogrešaka korisnika, korištenje sigurnosnog programa (od kojih su neki *anti-malware*, iako neki i nisu) kako bi se razdvojilo preglednike može biti efektno u ograničavanju počinjene štete. Opis besplatnih *anti-malware* programa podijeljenih po skupinama dan je u nastavku dokumenta.

5.1. Besplatni antivirusni programi

Računalni virus je prijetnja od koje se najviše strahuje u računalnom svijetu. Jednom kada uđe u računalo, virus se širi vrlo brzo dok ne zarazi većinu datoteka. Zaražene datoteke se postepeno kompromitiraju, budući da im virus mijenja programsko okruženje, što ih čini beskorisnima. Kao rezultat toga, datoteke se ne mogu otvoriti ili ne funkcioniraju korektno te je moguće čak izgubiti pristup postavkama računala, ukoliko je računalo zaraženo naprednijim virusom. Zloćudni korisnici pomoću ovih programa kradu informacije. Kako bi se spriječila ova prijetnja, na računalu mora biti instaliran antivirusni program. Besplatni programi mogu se preuzeti s Interneta, iako su najmoćniji oni komercijalni. Najpoznatije marke na tržištu, kao što su BitDefender i Kaspersky, jamče uklanjanje i zabranu ulaza većini, ako ne čak i svim vrstama virusa. Također, važno je redovno ažuriranje antivirusnog programa kako računalo ne bi postalo podložno napadima novih vrsta virusa. U novije vrijeme većina antivirusnih programa sadrži komponente pomoću kojih se mogu detektirati te ukloniti i ostale vrste zloćudnih programa iz skupina prikrivajućih i inficirajućih programa, primjerice crva, *rootkita* i trojanskih konja.

5.1.1. Avast! Free Antivirus

Avast! Free Antivirus spada u kategoriju odličnih besplatnih antivirusnih alata. Kvalitetom detekcije virusa može konkurirati kvalitetnim komercijalnim antivirusnim programima. Avast također posjeduje veliki broj opcija koje uključuju *realtime* mogućnosti skeniranja weba, elektroničke pošte, IM (eng. *Instant Messaging*), P2P (eng. *Peer-to-peer*), itd. Troši vrlo malo resursa u sustavu te je sa svojim mogućnostima vrlo dobra alternativa ostalim komercijalnim alatima. Sučelje programa Avast! Free Antivirus prikazuje Slika 4.

Slika 4. Sučelje programa Avast! Free Antivirus
Izvor: pcmag.com

5.1.2. Avira AntiVir Personal Edition

Avira AntiVir Personal Edition (Slika 5) je jedan od najboljih besplatnih alata ukoliko se korisnik želi zaštititi od virusa, *spywarea,* crva, *rootkita* itd. AntiVir je vrlo malen i troši malo resursa, dok je s druge strane detekcija zlonamjernih programa na visokoj razini.

AntiVir u svojoj besplatnoj inačici ima neke nedostatke. Besplatna inačica Avire dolazi s reklamama koje se pojavljuju kod svakog novog ažuriranja programa ili baze virusa, no te reklame je moguće ugasiti. Još jedan nedostatak je taj što Avira u besplatnoj inačici ima vremenski ograničenu licencu. Može se nakon isteka zatražiti i stvoriti nova, ali ona zahtjeva određene dodatne korake i zamara korisnika koji to mora s vremena na vrijeme napraviti nanovo. Besplatna inačica ne uključuje skeniranje poruka elektroničke pošte. Ovo i nije toliko loše ukoliko korisnik koristi neki od web servisa za čitanje poruka, primjerice Gmail, ali s druge strane to znači da Avira neće obavijestiti korisnika kada primi virus u lokalnom klijentu elektroničke pošte. No, svakako će obavijestiti ukoliko se isti pokuša otvoriti.

Slika 5. Sučelje programa Avira AntiVir Personal Edition
Izvor: emule.com

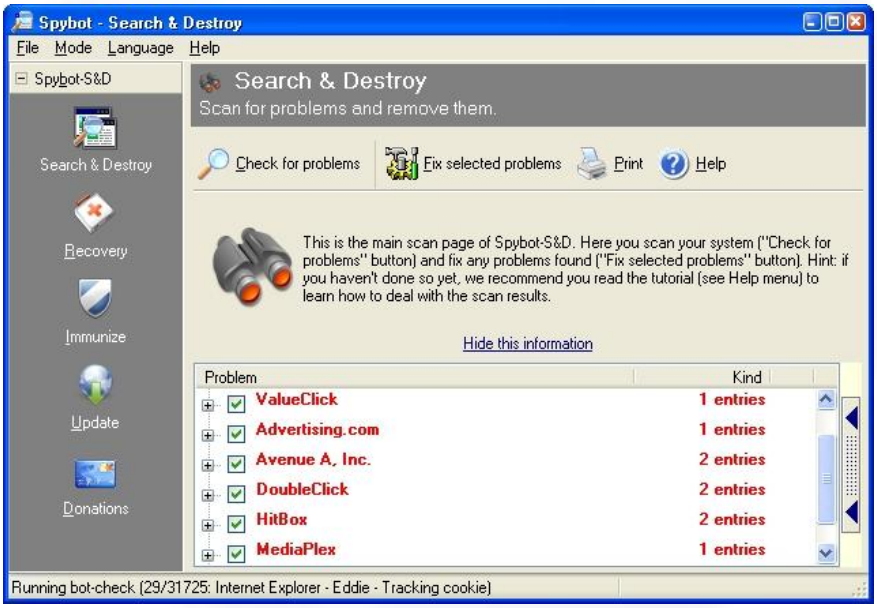
5.2. Besplatni anti-spyware programi

Iako su računalni virusi jedna od najopasnijih prijetnji na Internetu, *spyware* je zasigurno ona najbrojnija. Većina *spyware* programa koji dođu na računalo mogu dovesti do pada sustava, što znači da su opasni gotovo kao virusi. Postoje i vrste spywarea koje služe kao ulazna vrata za viruse i ostale *spyware* programe. U početku su se za borbu protiv virusa i *spywarea* koristili neovisni programi, no u današnje vrijeme većina razvojnih programera integrira upotrebu oba programa u svoje proizvode, kako bi korisnicima osigurali potpuniju sigurnost.

5.2.1. Spybot - Search & Destroy

Spybot - Search & Destroy (Slika 6) je vrlo dobar program za detekciju i uklanjanje *spywarea*. Kao što je ranije rečeno, *spyware* tiho prati korisničko ponašanje u svrhu stvaranja marketinškog profila korisnika. Taj profil se kasnije bez znanja korisnika prodaje tvrtkama za oglašavanje i slično. Spybot - S & D je besplatan alat, što ga uz ostale prednosti čini odličnim izborom za uklanjanje *spywarea*. Popis prijetnji koje Spybot - S & D može ukloniti može se vidjeti u navigacijskoj traci na lijevoj strani ukoliko se odabere *Support -> Threads*. Za uvod u Spybot - S & D, može se pročitati vodič na adresi:

http://www.safer-networking.org/en/tutorial/index.html



Slika 6. Sučelje programa Spybot – S & D
Izvor: safer-networking.org

5.2.2. Windows Defender

Windows Defender, otprije poznat kao Microsoft Anti Spyware, je Microsoftov proizvod za sprječavanje, uklanjanje i izoliranje *spywarea* u operacijskim sustavima Microsoft Windows. Uključen je u početku u sustave Windows Vista i Windows 7, a dostupan je i za besplatno preuzimanje za operacijske sustave Windows XP i Windows Server 2003. Windows Defender omogućuje skeniranje *spywarea,* poput ostalih besplatnih proizvoda za skeniranje *spywarea* dostupnih na Internetu te uključuje velik broj sigurnosnih agenata koji nadziru nekoliko uobičajenih lokacija koje koristi operaciiski sustav Windows kako bi se uočile promjene koje mogu biti prouzročene *spywareom*. Također, omogućava i jednostavno uklanjanje instaliranih komponenti ActiveX. U njega je integrirana i podrška za Microsoft SpyNet mrežu koja omogućuje korisnicima da prijave Microsoftu one programe koje

smatraju *spywareom* te kojim aplikacijama i pokretačkim programima dopuštaju da budu instalirani na njihovim sustavima.

5.3. Besplatni vatrozid programi

Već samo spajanje na Internet je dovoljno da privuče u računalo zloćudne programe. Nekada čak i prije nego korisnik skenira računalo s maloprije spomenutim sigurnosnim programima, zlonamjerni program je već zarazio dio datoteka. Postoje čak i programi dizajnirani da onemoguće djelovanje antivirusnih i antispyware programa čim uđu u računalo. Vatrozid je prva linija obrane računala. Radi se o mrežnom uređaju ili programu smještenom između lokalne i javne mreže, dizajniranim za zaštitu povjerljivih podataka od neautoriziranih korisnika. Programiran je tako da djeluje blokirajući zloćudnim programima pristup računalu prema skupu pravila koje definira sigurnosna politika. Prema tome, ispravan rad vatrozida zahtjeva precizno određivanje niza pravila o dopuštenom i zabranjenom prometu. Osnova rada sastoji se u ispitivanju IP paketa između klijenta i poslužitelja. Vatrozid može biti implemntiran programski ili sklopovski. Programski vatrozid štiti jedno računalo, osim kada je baš to računalo predodređeno za zaštitu cijele mreže. Radi se o programu instaliranom na računalu koji obavlja filtriranje paketa. Sklopovski vatrozid je stvarni uređaj, a prednost je maksimizacija brzine provjere paketa i olakšana konfiguracija.

Postoji više tipova vatrozida prema tome gdje se odvija, presreće i prati komunikacija:

- **Vatrozid mrežnog sloja** – također zvan filter paketa, implementiran je za rad na niskoj razini TCP/IP (eng. *Transmission Control Protocol/Internet Protocol*) modela. Omogućuje propuštanje samo onih paketa koji zadovoljavaju određeni skup pravila koje je definirao administrator. Moderni vatrozidi filtriraju promet na temeljnu brojnih atributa poput IP adrese, izvorne i odredišne adrese, protokolima i sl.
- **Vatrozid aplikacijskog sloja** – implementiran na aplikacijskom sloju TCP/IP modela te može presresti sve pakete koji putuju do ili iz aplikacije. U principu, ovaj tip vatrozida može spriječiti sav neželjen promet koji dolazi na zaštićeno računalo te time spriječiti širenje računalnih crva ili trojanskih konja. Funkcioniraju određivanjem da li neki proces treba prihvatiti određenu vezu, a rad je sličan kao i kod filtera paketa, s razlikom da se obavlja primjena pravila filtriranja na procese umjesto na priključke.
- **Posrednički vatrozid** – uređaj koji propušta određene ulazne pakete, a ostale blokira.

5.3.1. Comodo Internet Security

Comodo Internet Security je dugo smatran jednim od najboljih dostupnih vatrozidnih alata. Comodo je danas kompanija koja nudi potpunu Internetsku sigurnost omogućujući mnoga rješenja za koja je potrebno platiti, ali ipak omogućuju i opsežan besplatan skup alata za Internetsku sigurnost (uključujući i vatrozid).. Comodo uključuje antivirusni program i vatrozid, a na korisnicima je da odluče žele li zadržati antivirusnu zaštitu aktivnom ili koristiti samo vatrozid. Comodo sadrži mnoge napredne mogućnosti koje pomažu zaštiti računalo korisnika ako zlonamjerni program postane aktivan u njegovom sustavu. To uključuje mogućnost zaključavanja određenih datoteka i registarskih ključeva. Comodo je također često hvaljen jer zauzima malo resursa, što je dobro za svaki besplatni proizvod pa je prema tome najbolji vatrozid za računala koja su starija i teško pokreću vatrozidne programe.

Slika 7. Sučelje programa Comodo Internet Security
Izvor: techmixer.com

5.3.2. ZoneAlarm Free Firewall

ZoneAlarm Free Firewall je bio jedan od prvih vatrozida dostupnih na računalima s operacijskim sustavima Windows. Za sobom ima dugu povijest odlične zaštite protiv brojnih tipova prijetnji. Iako su osnovne funkcije ZoneAlarma ostale iste, značajno je izmijenjen tokom godina. Besplatna inačica ZoneAlarma sadrži mnoge napredne mogućnosti, kao što su automatska Wi-Fi sigurnost, *anti-phishing* zaštita te detekcija ponašanja prijetnji. Mnoge od ovih dodatnih mogućnosti nisu uobičajene za sam vatrozid, ali je za korisnike uvijek dobro imati dodatnu zaštitu. ZoneAlarm omogućuje najbolju sveukupnu vatrozidnu zaštitu i dobar je izbor za napredne korisnike.

5.4. Besplatni filtri elektroničke pošte

Filtriranje poruke elektroničke pošte označava njihovu obradu prema posebnim kriterijima. Najčešće se to odnosi na automatsku obradu ulaznih poruka, ali može uključivati i provjeru odlaznih poruka elektroničke pošte. Filtere mogu instalirati korisnici kao posebni program ili kao dio programa za rukovanje porukama elektroničke pošte. Korisnima je omogućeno definiranje pravila za automatsko filtriranje poruka. Većina programa također uključuje i funkcije za automatsko filtriranje poruke neželjene elektroničke pošte. Davatelji usluga pristupa Internetu često ugrađuju ovakve filtre u svoje agente za prosljeđivanje poruke korisnicima, čime osiguravaju uklanjanje prijetnji (poput poveznica na web stranice sa zlonamjernim sadržajem) prije nego poruka dospije do korisnika.

Zaštita od poruke neželjene elektroničke pošte obavlja se preko raznih anti-spam tehnika uključenih u proizvode, usluge ili programe. Mogu se podijeliti u četiri osnovne kategorije: tehnike koje zahtijevaju djelovanje korisnika, tehnike koje se mogu administratori mogu automatizirati, tehnike koje mogu automatizirati pošiljatelji poruka te tehnike koje su ugradili sigurnosni istražitelji. Detekcija neželjenih poruke elektroničke pošte temelji se na sadržaju poruke, a odvija se provjerom ključnih riječi. Osim toga, postoji i provjera koja se ne zasniva na sadržaju nego na statističkom značenju.

5.4.1. POPFile

POPFile je besplatni, filtar elektroničke pošte, otvorenog koda, originalno napisan u jeziku Perl, a napisao ga je John Graham-Cumming i održava ga tim volontera. Koristi Bayesov klasifikator za filtriranje pošte te mu to omogućuje da „nauči“ klasificirati vodeći se korisnikovim željama. Tipično se koristi za filtriranje poruka neželjene elektroničke pošt, ali može se upotrebljavati i za sortiranje pošte u kategorije koje korisnik odredi, primjerice poslovne poruke, privatne poruke i sl. Program radi u nekoliko različitih načina rada, a u najpopularnijem načinu postavlja se kao posrednički poslužitelj između poslužitelja elektroničke pošte i poslužitelja POP3 (eng. *Post Office Protocol*). Kada se pošta preuzme preko protokola POP3, filtar ga identificira i klasificira te radi modifikacije određene od strane korisnika, proširujući mu ime imenom odgovarajuće kategorije kojoj poruka pripada. U drugom načinu rada, POPFile može raditi kao poslužitelj IMAP (eng. *Internet Message Access Protocol*) koji nadzire korisnikov IMAP poslužitelj tražeći nadolazeću poštu i poruke koje je sam korisnik premjestio.

5.4.2. Spamihilator

Spamihilator je besplatni program koji filtrira neželjene poruke elektoničke pošte prije nego što one stignu do poslužitelja elektroničke pošte. Spamihilator se uključuje kao lokalni posrednički poslužitelj između poslužitelja elektroničke pošte i poslužitelja POP3, djelujući slično kao antivirusni program. Program ispituje pristigle poruke svojim filtrima prema smislenim kriterijima filtriranja. Filtri Spamihilatora mogu se po volji korisnika uključivati i isključivati te mogu biti individualno konfigurirani. Tvorci Spamihilatora postavili su na svoju web stranicu jednu vrstu programa *Plugin-Software-Development* korisnicima na raspolaganje, kako bi zainteresirani programeri mogli proizvesti vlastite filtre. Sučelje program prikazano je na Slika 8.

Slika 8. Sučelje programa Spamihilator
Izvor: spamihilator.softonic.de

5.5. Besplatni programi za blokiranje pop-up oglasa

Prilikom posjeta nekim web stranicama, često se dogodi da novi prozori iskoče na korisničkom ekranu. Ako se previše prozora pojavi, oni mogu uzrokovati pad sustava ili preusmjeriti korisnika na stranice sa zloćudnim programima. Programi za blokiranje *pop-up* prozora programirani su tako da sprečavaju iskakanje takvih prozora. Mogu se nalaziti u paketu s drugim sigurnosnim

programima ili alatnim trakama web preglednika. Neki vatrozidi sadrže ugrađene programe za blokiranje, što povećava razinu zaštite koju nude.

5.5.1. Adblock Plus

Adblock Plus (ABP) je proširenje koje filtrira sadržaj za web preglednike Mozilla Firefox (uključujući i Firefox za mobilne telefone) i Google Chrome. ABP dopušta korisnicima da spriječe prikazivanje i preuzimanje nekih elemenata web stranica, kao što su primjerice različiti oglasi. Kao i Mozillin ugrađeni dodatak za blokiranje slika, Adblock blokira HTTP (eng. *Hypertext Transfer Protocol*) zahtjeve prema njihovoj izvornoj adresi te blokira *i-frame* elemente, skripte i Flash animacije. Također, koristi automatsko generirane stilove pokrivanja kako bi sakrio elemente kao što su tekstualni oglasi na stranici, tako da ih ne blokira pri njihovom učitavanju već ih sakriva, a to je poznato pod nazivom „sakrivanje elemenata“.

5.5.2. Hitware Popup Killer

Hitware Popup Killer je besplatni program koji blokira *pop-up* oglase. Pokreće se u sustavskoj traci, te neprimjetno uklanja neželjene oglase čak i prije nego se pojave. Osim toga, sprječava neke neželjene posljedice, kao primjerice zaključavanje web preglednika. Korisnik može izabrati želi li biti informiran o tome kada je *pop-up* prozor zatvoren. Osim toga, Hitware Popup Killer pomaže korisnicima da se riješe dosadnih *pop-up* oglasa zasnovanih na protokolu IP, koji zagušuju Messenger servis koji bi trebao slati tekstualne poruke preko mreže koristeći IP adresu računala.

6. Usporedba s komercijalnim alatima

Programi za zaštitu desktop računala razvijeni su kako bi zaštitili računala od štetnih sadržaja. Kako su se programi razvijali, razvijale su se i mnoge nove i poboljšane opcije. Uz sve te izbore koje programi nude, nametnulo se pitanje razlikuje li se plaćeni računalni sigurnosni program od onog besplatnog, no za to još uvijek ne postoje konkretni dokazi.

S jedne strane, plaćeni program je bolji, jer pruža poboljšano iskustvo, dodatne mogućnosti i tehničku podršku. S druge strane, ako korisnik zna kako rukovati sigurnošću svog računala, moguće je uživati povlastice plaćenog programa i u besplatnoj inačici. Te povlastice uključuju:

- **Različite mogućnosti skeniranja** – omogućuju brzo tipično skeniranje ili potpuno skeniranje u nekim mapama/pogonskim jedinicama ili specificiranim mapama u računalu.
- **Unaprijeđena *spyware* bazu podataka** – omogućuje najnovije preventivne mjere kako bi se osigurala sigurnost računala.
- **"*Real time*" zaštita (zaštita u stvarnom vremenu)** – štiti računalo prilikom korištenja Interneta od novih prijetnji koje se svakodnevno pojavljuju.

U svijetu tehnologije teško je navesti tržišnu marku čiji je sigurnosni program najbolji jer svako računalo i svaki korisnik ima različite zahtjeve. Ipak, ovisno o zahtjevima korisnika besplatni sigurnosni program može biti jednako dobar, ili čak i bolji, od onog plaćenog.

Danas korisnici računala mogu birati među raznim besplatnim i komercijalnim antivirusnim programima kako bi odabrali onaj koji najbolje odgovara njihovim potrebama. No, iako nisu svi besplatni programi takvi, neki od njih ne mogu detektirati i uništiti pojedine viruse i ostale prijetnje. Također, među njima postoje programi koji su zastarjeli i preslabi da bi zaštitili podatke u računalu. Kako besplatni programi imaju specificiran probni period (npr. 30 dana, godinu dana i sl.), nakon tog perioda program će prestati unaprjeđivati svoje antivirusne mogućnosti (skeniranje prijetnji, automatsko skeniranje i sl.), pa će računalo postati podložno zlonamjernim prijetnjama. S druge strane, ako se sigurnosni program kupi, razvojni programer će biti odgovoran za sva pitanja povezana s programom (tehnička podrška).

7. Budućnost besplatnih alata za zaštitu desktop računala

Većina korisnika upotrebljava besplatne *anti-malware* programe jer traže načine za uštedu novca. Ipak, budućnost besplatnih *anti-malware* programa još uvijek je prilično neizvjesna. Naime, postoje neki očiti nedostaci na koje se korisnici žale pri njihovoj upotrebi, a oni su navedeni u nastavku.

- **Niska razina zaštite** – obično besplatne inačice antivirusnih programa omogućavaju samo skenirane zlonamjernih programa, a ponekad uključuju i dodatke za web preglednike koji obavljaju blokiranje zlonamjernih poveznica. Napredne značajke, poput vatrozida, uobičajeno su ograničene na plaćene inačice.
- **Nedostatak tehničke podrške** – većina tvrtki pruža neki oblik podrške korisnicima, ali samo za plaćene inačice programa. Besplatne inačice često sadrže samo baze s često postavljenim pitanjima.
- **Sadržavanje reklamnih materijala** – većina besplatnih antivirusnih programa sadrži neki oblik reklamnih materijala za ostale proizvode firme.
- **Osvježavanje baze potpisa virusa** – iako većina firmi održava baze plaćenih i besplatnih inačica istima, mogu postojati male razlike. Primjer je firma Avast koja je besplatnu inačicu namijenila prosječnim korisnicima, a plaćenu naprednim.

Sve u svemu, besplatni *anti-malware* programi podliježu nekim očitim problemima koji ne pogađaju korisnike plaćenih anti-malware programa jer su za funkcionalnost istih odgovorni brojni razvojni inženjeri. Ipak, besplatni *anti-malware* programi će zasigurno opstati dokle god budu postojali korisnici koji su u nemogućnosti priuštiti si neku od plaćenih inačica.

8. Zaključak

Zaštita računala je u današnje vrijeme, zbog velikog broja prijetnji, nužna za svakog korisnika. Komercijalni programi pružaju odličnu zaštitu protiv svih vrsta prijetnji, a jamstvo za tu zaštitu daju tvrtke koje su napravile program. Također, dobra stvar kod komercijalnih programa je postojanje službe za pomoć korisnicima. Nedostatak komercijalnih programa je, naravno, da se oni moraju plaćati. Besplatni programi za zaštitu desktop računala prosječnom korisniku mogu pružiti solidnu zaštitu od spomenutih prijetnji. Mnogi od tih programa već danas mogu konkurirati i komercijalnim programima. Problemi nastaju nakon nekog dužeg vremena zbog nemogućnosti redovite obnove baze prijetnji i manje efektnog skeniranja računala. Korisnici mogu koristiti besplatne programe zaštite, ali tada moraju više pažnje pridavati sigurnosti svog računala. Korisnici bi program nakon određenog vremena trebali nadograditi, raspitati se o mogućnostima novih prijetnji te kako njihov program reagira na njih itd. Još jedna mogućnost, koja se često spominje, je korištenje više besplatnih alata za zaštitu. Time je korisničko računalo sigurno od prijetnji, ali se gubi poprilična količina resursa u sustavu.

Svako računalo spojeno na mrežu trebalo bi sadržavati neki oblik zaštite, a korisnicima se savjetuje odabir onog oblika koji najbolje odgovara njihovim potrebama i zahtjevima. Bez obzira da li se odlučili za komercijalnu ili besplatnu inačicu programa, važno je voditi računa o sigurnosti sustava te pravovremeno i periodički obnavljati programe za zaštitu i provoditi skeniranje računala.

9. Leksikon pojmova

Rootkit (Oblik zlođudnog programa)

Rootkiti su zlonamjerni programi koji su napravljeni da bi preuzeli kontrolu nad operacijskim sustavom tako da nadomjeste procese i podatke u sustavu bez dopuštenja korisnika.

http://os2.zemris.fer.hr/ns/2008_Mackovic/rootkit.htm

Virus (Računalni virus)

Virusi su programi koji se mogu kopirati i zaraziti računalo bez znanja ili dopuštenja korisnika. Računalo se može zaraziti na razne načine preko Internet-a, CD-a, USB-a... Virusi dolaze većinom sa drugim programima, kao što su npr. Trojanski konji kako bi maskirali svoj rad i kako bi ih bilo još teže za otkriti. Namjene virusa su različite, mogu služiti samo kako bi radili štetu no neki su manje štetni i samo usporavaju računalo i smetaju korisniku u radu. Virusi se spremaju u memoriju računala i pokreću se s operacijskim sustavom i inficiraju programe koji se pokreću.

http://www.ust.hk/itsc/antivirus/general/whatis.html

Spyware (Maliciozni program koji se koristi za špijunažu)

Špijunski program (engl. *Spyware*) je program koji se tajno instalira na računalu kako bi presretao ili potpuno preuzeo kontrolu nad računalom bez dozvole korisnika. Iako bi se iz naziva moglo zaključiti da samo špijunira rad korisnika, većina spywarea radi puno više od toga. Mogu služiti kako bi sakupljali informacije o korisniku, mijenjali početnu stranicu u Internet pregledniku, instalirali dodatne programe na računalo i drugo.

http://os2.zemris.fer.hr/ns/2008_Mackovic/Spyware.htm

Phishing (Napad na računalni sustav)

Phishing je način prikupljanja nekih osjetljivih informacija, kao što su korisnička imena, lozinke i detalji kreditnih kartica, maskiranjem u pouzdan entitet elektroničkih komunikacija.

http://www.webopedia.com/TERM/P/phishing.html

Crv (Računalni crv)

Računalni crv je samo-replicirajući zlođudni program koji koristi mrežu računala kako bi poslao vlastite kopije na druge čvorove mreže bez pomoći korisnika. Ovakvo širenje računalnom mrežom je obično posljedica ranjivosti računala.

http://virusall.com/computer%20worms/worms.php

Trojanski konj (Zlođudni program koji se pretvara kao legitimna aplikacija)

Trojanski konj je oblik zlođudnog programa koji se pretvara kao legitimna aplikacija. U početku se pretvara kao da obavlja korisnu funkcionalnost za korisnika, no u pozadini izvodi štetne radnje (na primjer, krađa informacija). Za razliku od crva, ovaj oblik zlođudnih programa se ne širi samostalno.

http://www.webopedia.com/TERM/T/Trojan_horse.html

WWW (World Wide Web)

WWW (eng. *World Wide Web*) je jedna od najkorištenijih usluga Interneta koja omogućava dohvaćanje dokumenata. Dokumenti mogu sadržavati tekst, slike i multimedijalne sadržaje, a međusobno su povezani poveznicama (eng. *Hiperlink*).

http://www.webopedia.com/TERM/W/World_Wide_Web.html

10. Reference

[1] desktopsecurity.org: Desktop Security, http://www.desktopsecurity.org/, srpanj 2011.

[2] desktopsecuritysoftwareguide.com: Free vs. Paid Computer Security Software, http://desktopsecuritysoftwareguide.com/free-vs-paid-computer-security-software/, siječanj 2009.

[3] Larry Seltzer: Can You Afford To Use Free Antivirus?, http://securitywatch.pcmag.com/malware/284496-can-you-afford-to-use-free-antivirus, lipanj 2009.

[4] spamfaq.net: Should I Use Free Antivirus For My Business?, http://www.spamfaq.net/should-i-use-free-antivirus-for-my-business/, srpanj 2011.

[5] Desktop Security Software Guide: 7 Reasons Why You Need the Best Desktop Security Software, http://desktopsecuritysoftwareguide.com/7-reasons-why-you-need-the-best-desktop-security-software/, srpanj 2010.

[6] Desktop Security Software Guide: Programs to Keep Your Computer Safe, http://desktopsecuritysoftwareguide.com/programs-to-keep-your-computer-safe/, srpanj 2010.

[7] squidoo.com: 20 Free Windows Desktop Security Tools, http://www.squidoo.com/desktopsecurity, siječanj 2011.