FIRST AID by

CERT.hr

PRIRUČNIK I CD ZA
RAČUNALNU SIGURNOST
KORISNIKA INTERNETA

CARNet

SADRŽAJ

UVOD

Kada se spomene računalna sigurnost, malo je ljudi koji će u mislima stvoriti jasnu sliku pojma o kojem je riječ. Većina nas čula je za viruse, hackere* i otuđenja potpomognuta računalom, no rijetko tko razumije o čemu se tu zapravo radi. Ovoj situaciji ne pomaže konfuzija u medijima koji nas zasipaju novim riječima čija se značenja nerijetko preklapaju pa čak i mijenjaju ovisno o izvoru vijesti.

Problem računalne sigurnosti počiva na osnovnoj razlici između čovjeka i računala - inteligenciji. Naime, inteligencija je nešto što čovjek ima, a računalo ne, ma što vam govorili. Dakle čovjek ima sposobnost snalaženja u novonastalim situacijama, dok računalo poduzima unaprijed predviđene radnje. Zbog ove razlike čovjek će gotovo uvijek moći prevariti računalo i trebat će drugi čovjek da bi tu prijevaru prepoznao. Često je krajnji korisnik taj koji će morati procijeniti što računalu dopustiti.

Računala danas, osim za zabavu i učenje, koristimo i za komunikaciju i ozbiljan rad, zbog čega njihova pouzdanost više nije zanemariva. Sigurnost računala ne čini samo zaštita vaše privatnosti, već podrazumijeva da vam je na raspolaganju kada ga trebate i da je pod vašom kontrolom kako ne biste došli u opasnost da odgovarate za tuđe prekršaje.
Statistike pokazuju da između 60 i 70% prometa elektroničke pošte otpada na neželjene poruke. U poslovnim je mrežama 5 - 20% sveg prometa maliciozno, odnosno štetno za sigurnost i raspoloživost resursa organizacije. Ovi podaci posljedica su velikog porasta upotrebe računala u poslovne svrhe paralelno sa sporim stvaranjem svijesti o problemima računalne sigurnosti. Prvi korak prema sigurnom korištenju računala i Interneta je instalacija sigurnosnih alata koji računalo štite od poznatih prijetnji i brinu se da korisnik odlučuje koje se radnje na njemu smiju odvijati. Upoznavanjem s ovim alatima i njihovom svrhom naučit ćete ponešto i o prijetnjama te razumijevanjem učiniti vaš rad na računalu sigurnijim. Na CD-u priloženom uz brošuru pronaći ćete izbor alata koje uz pomoć interaktivne aplikacije možete instalirati na svoje računalo.
U prilozima na kraju ove brošure pronaći ćete pojmovnik koji vam može pomoći pri razumijevanju poglavlja koja čitate.

*Hackeri i crackeri: riječ hacker u svakodnevnom govoru rabi se na pogrešan način. Hacker je žargonski naziv za osobu s visokim stupnjem poznavanja neke tehnologije koja je sposobna iz nje izvući maksimum. Hacking u kontekstu računalne tehnologije znači vješto pisanje ili prilagođavanje programa. Riječ cracker, s druge strane, označava osobu koja svoje znanje koristi kako bi "slomila" program, odnosno probila se kroz neki sustav zaštite.

Tko upravlja mojim računalom?

Sigurnim računalom upravlja njegov korisnik. Prvi znak da vaše računalo nije sigurno je da ne možete objasniti što neka aplikacija na vašem računalu radi i odakle je uopće došla ili da su vaši računalni resursi (uključujući pristup Internetu) neobjašnjivo vrlo aktivni dok vi ništa ne radite.

Korisnikovo računalo prilikom priključenja na Internet, bilo stalnom vezom ili telefonskim pristupom, postaje doslovno dijelom Interneta. Dodjeljuje mu se IP adresa (vidi Pojmovnik i Podjela nadležnosti na Internetu) po kojoj je u tom trenutku dostupno sa svih drugih računala na Internetu, kao što su sva druga računala dostupna njemu. Među tim računalima se, osim poslužitelja e-maila, web-stranica i drugih servisa koje koristimo, nalazi i mnogo onih koja su zaražena nekim oblikom virusa ili crva ili su na drugi način prijetnja našoj sigurnosti. Svim tim računalima smo izloženi kada postanemo dijelom Interneta.

Često se na računalo bez korisnikovog znanja instalira neželjena aplikacija (vidi: Spyware/Adware) krijući se pod primamljivim nazivom ili koristeći nesavršenosti web-preglednika. Takva aplikacija trudit će se da nam ne oda svoju prisutnost i potajno prikupljati naše e-mail adrese, lozinke, kupovne navike i slične podatke, vrlo vrijedne zlonamjernim stranama. Na sličan će način mnogi virusi, crvi i trojanski konji*, o kojima će kasnije biti više riječi, nastojati što duže prikriti svoju prisutnost kako bi se što više proširili. Posljedica ovih aktivnosti je nepouzdan rad računala, rizik zloupotrebe vaše kreditne kartice (ukoliko ste podatke o njoj unosili u računalo) i uskraćivanje usluge vašeg Internet Service Providera, odnosno onemogućavanje pristupa Internetu.

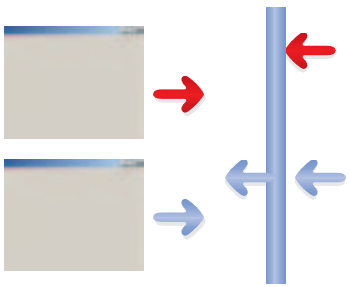
Od većine ovakvih prijetnji možemo se preventivno braniti sigurnosnim alatima, a neki od tih alata pomoći će i u smanjenju štete nastale kada je naše računalo već kompromitirano. U sljedećim poglavljima upoznat ćemo vas s vrstama i radom nekih takvih alata:

Osobni vatrozid - zaštita pristupa vašem računalu s Interneta
Antivirusni softver - kontrola koda koji se izvršava na računalu i prepoznavanje zlonamjernih aplikacija
Čistači neželjenih aplikacija - uklanjanje prepoznatih aplikacija instaliranih bez našeg odobrenja

*Virusi, crvi, trojanski konji: zlonamjeran kôd koji se samostalno izvršava na vašem računalu i širi na druga računala putem Interneta (vidi: Nametnici).

Osobni vatrozid

Osobni vatrozid (izvorno personal firewall) aplikacija je koja nadzire komunikaciju između računala i mreže. Njegova je uloga ograničiti tu komunikaciju na onu predviđenu normalnom upotrebom računala, čime se postiže zaštita od neovlaštenog pristupa. U praksi nas osobni vatrozid štiti od pokušaja preuzimanja kontrole nad našim računalom zlonamjernim pristupom njegovim servisima. Najčešći oblik takvog pristupa jesu mrežni crvi koji se na taj način šire.



Nakon instalacije na vaše računalo, osobni vatrozid nadzire aktivnosti drugih aplikacija (npr. web-preglednika) i uređaja putem kojih pristupate mreži (npr. modem ili mrežna kartica). Kako bi što više pojednostavnili podešavanje, proizvođači osobnih vatrozida većinom su se odlučili komunikaciju kroz mrežne uređaje podijeliti na računala kojima vjerujemo i s kojima dijelimo svoje resurse (lokalna mreža) i ona prema kojima smo nepovjerljivi (ostatak Interneta). S aplikacijama je sličan slučaj: web-pregledniku i e-mail klijentu dopustit ćemo da slobodno komuniciraju s ostalim računalima na Internetu, dok aplikaciji čije nam porijeklo nije poznato obično to nećemo dopustiti. Takva je aplikacija možda crv koji se nastoji proširiti ili neka aplikacija instalirana bez našeg znanja koja želi nekome poslati naše lozinke i druge povjerljive podatke.

Osobni vatrozidovi obično su koncipirani na način da korisnika pitaju želi li dopustiti neku komunikaciju koja se sprema započeti. U početku će takvih pitanja biti mnogo dok naš osobni vatrozid ne "nauči" koji promet je dozvoljen, a koji nije. Kada odgovarate na ova pitanja, razmislite znate li što je uzrokovalo pokušaj komunikacije. Ako ne znate, pokušajte saznati. Ništa se loše neće dogoditi blokirate li pristup aplikaciji kojoj taj pristup treba - aplikacija neće uspjeti pristupiti resursu koji je tražila, a vi ćete sljedeći put znati ispravno odgovoriti na isto pitanje.

Razina sigurnosti koja se postiže aktivnošću osobnog vatrozida više je nego dovoljan razlog da mu poklonite vaše strpljenje u prvim danima, dok ga ne podesite na ispravan način. Mnogi napadi na vaše računalo (ili čak s vašeg računala) bit će zaustavljeni u korijenu.

Antivirusni softver

Uloga antivirusnog softvera na računalu je spriječiti aktiviranje poznatih zlonamjernih aplikacija, poznatijih pod nazivima virusi, crvi i trojanski konji. Ovi nametnici ometaju ili čak onemogućuju normalan rad na vašem računalu, a mnogi od njih se usput nastoje i proširiti na druga računala, zbog čega možete imati problema s vašim pružateljem internetskih usluga i drugim korisnicima.

Kao što je već spomenuto, antivirusni softver prepoznaje zlonamjerne aplikacije koje su mu poznate, što čini uspoređivanjem njihovog koda s bazom takozvanih antivirusnih definicija. Neki antivirusni alati nude i metodu pod nazivom heuristika koja nastoji prepoznati nametnike po njihovom ponašanju, međutim budući da autor zlonamjerne aplikacije može isprobati svoj kod antivirusnim programom prije puštanja na mrežu, ova je metoda vrlo niske efikasnosti. Zbog toga je vrlo važno redovito ažurirati definicije vašeg antivirusnog softvera posjećivanjem stranice proizvođača ili korištenjem automatskog ažuriranja dostupnog u većini antivirusnih alata (automatic update).

Kada antivirusni softver prepozna zlonamjernu aplikaciju koja se želi aktivirati, obično postavi pitanje korisniku što želi poduzeti. Tipični ponuđeni odgovori su "obrisati", "očistiti", "karantenizirati" i "ignorirati". Opcija "očistiti" nastoji iz datoteke ukloniti zlonamjeran kod koji je u nju umetnut. Ova metoda vrlo rijetko uspije jer se danas rijetko koji nametnik nastanjuje unutar druge datoteke. Obično je cijela datoteka zlonamjerna, zbog čega je opcija "obrisati" najlogičniji izbor. Ako niste sigurni da je datoteka o kojoj se radi zlonamjerna, odnosno strahujete da biste mogli obrisati nešto što će vam kasnije trebati, koristite opciju "karantenizirati". Ova opcija posprema datoteku na sigurno mjesto odakle se neće moći samostalno aktivirati, a vi ćete kasnije po potrebi moći doći do nje.

Čistači neželjenih aplikacija

Za neželjene aplikacije vjerojatno ste čuli pod nazivom spyware, adware i dialeri, o kojima možete više saznati u narednim poglavljima. Njihovi uklanjatelji poznati su pod nazivom anti-spyware i djeluju na sličnoj osnovi kao i antivirusni softver - prepoznaju unaprijed ugrađene definicije poznatih neželjenih aplikacija. Doduše, dok je većina antivirusnog softvera stalno aktivna, uklanjatelji neželjenih aplikacija uglavnom se pokreću na zahtjev korisnika.

Osim što štite vašu privatnost, ovi se alati brinu i o zaštiti vaše e-mail adrese od neželjenih poruka (obično su e-mail adrese na računalu prvo što spyware "ukrade"). Neki od njih, npr. SpyBot Search & Destroy, imaju mogućnost trajne zaštite vašeg web-preglednika uklanjanjem nekih njegovih ranjivosti i blokiranjem neovlaštenog pristupa vašoj početnoj stranici te podešavanjima pretraživanja Interneta.

Budući da kao i antivirusni softver zahtijeva stalno ažurne definicije kako bi mogao prepoznati nove oblike neželjenih aplikacija, potrebno je nove definicije često i redovito preuzimati s Interneta putem web-stranice proizvođača ili ugrađene mogućnosti automatskog ažuriranja.

Sigurnosne zakrpe

Dosad smo već mnogo puta spomenuli ranjivosti operativnog sustava i aplikacija koje su uzrok mnogim sigurnosnim problemima. Ranjivosti su uzrok nesavršenosti aplikacija, što se najviše odnosi na način kako aplikacije interpretiraju korisničke zahtjeve. Lukav i zlonamjeran korisnik može formirati zahtjev kakav aplikacija ili neki servis operativnog sustava ne očekuju i na taj način uzrokovati da se odvije neki dotad nepredviđen slijed događaja. U praksi je servis prevaren i dodjeljuje korisniku pristup resursima na koje on ne bi smio imati prava.

Sigurnosne zakrpe su obično mali instalacijski paketi koje proizvođač operativnog sustava ili neke aplikacije objavljuje kao reakciju na otkriveni propust. U tom se paketu nalazi ispravljena verzija dijela aplikacije u kojem se nalazi greška i kôd potreban da se staro rješenje zamijeni novim. Korisnicima Microsoftovog operativnog sustava Windows najvažnije su zakrpe za sam operativni sustav određene verzije i za web-preglednik Internet Explorer. Također su važne sigurnosne zakrpe za alate kao što su osobni vatrozid i antivirusni softver.

Do sigurnosnih zakrpa možete doći posjetivši stranicu proizvođača aplikacije koju želite zaštititi. Korisnici operativnog sustava Windows mogu koristiti servis Windows Update (http://windowsupdate.microsoft.com) ili na stranicama TechNeta pojedinačno pristupiti zakrpama koje ih zanimaju.

Dodatni savjeti

Računalna sigurnost samo je još jedan od mnogih oblika zaštite vas i vaše imovine, zbog čega, kao i drugi oblici sigurnosti, nikada ne može biti potpuna i na kraju najviše ovisi o ljudskom faktoru, odnosno - vama. Korisnik svjestan važnosti sigurnosti i informiran o opasnostima koje ga vrebaju često će svojom predostrožnošću spriječiti mnogo incidenata koje niti jedan sigurnosni alat ne bi zaustavio.

Vaše najjače oružje u borbi protiv zlonamjernog koda i korisnika Interneta je vaš razum. Kako u životu inače izbjegavate opasne situacije i nastupate s oprezom prema stranama čije su vam namjere nepoznate, tako i u elektroničkoj komunikaciji trebate primijeniti slična pravila. Običnu poštu može vam poslati bilo tko i potpisati se bilo kojim imenom. Tako vam bilo tko može poslati i elektroničku poštu, predstaviti se kao banka ili neko poduzeće i tražiti od vas povjerljive informacije. Primite takvu poruku s dozom sumnje - ne vjerujte joj bez razmišljanja. Jeste li je zatražili? Ima li ona uopće smisla? Možete li telefonom provjeriti njezinu vjerodostojnost? Vaše računalo služi vama na korist i prema tome treba činiti ono što vi od njega tražite. Ne preskačite upite aplikacija koje vas upozoravaju kakve posljedice ima radnja koju upravo poduzimate. Možda kada pročitate poruku ustanovite da to zapravo niste željeli niti zatražili.

U većini slučajeva postoji više korisničkih aplikacija koje zadovoljavaju određenu primjenu - više različitih web-preglednika, više e-mail klijenata i slično. Različite aplikacije ne rješavaju iste logičke probleme na jednak način premda se korisniku može činiti da se uglavnom ponašaju jednako. Zbog tog različitog pristupa, zlonamjeran kôd pisan s ciljem napada na najraširenija aplikaciju na nekoj drugoj neće funkcionirati. Prema tome, upotrebom alternativnih aplikacija u svakodnevnom radu značajno smanjujete izloženost takvim napadima. Alternativne aplikacije neće biti bez propusta, no njihovi propusti će u manjem broju biti poznati i korišteni pri izradi novih virusa, crva, spywarea i sličnih nametnika. Na CD-u priloženom uz brošuru pronaći ćete alternativni web-preglednik - Mozilla Firefox.

Mnogi korisnici odustanu od korištenja alternativnih aplikacija zbog njihove nemogućnosti da prikažu neke stranice ili e-mail poruke. Uzrok ovim problemima je taj što kao i zlonamjerni korisnici, autori web-stranica i e-mail poruka, koriste najraširenije aplikacije. Nekada te aplikacije greškom formiraju kôd nečitljiv u drugim preglednicima ili koriste dodatne mogućnosti kojih u drugim aplikacijama nema. Dobar pristup ovom problemu je korištenje alternativnih aplikacija uz zadržavanje najraširenijih za takve iznimne slučajeve.

Lozinke koje koristite za pristup Internetu, elektroničkoj pošti ili web-stranicama koje omogućavaju online trgovinu ne smiju biti predvidljive. Zamislite da na raspolaganju imate mjesece za isprobavanje različitih kombinacija znakova kako biste pogodili tuđu lozinku. Računalo može isprobati vrlo velik broj različitih kombinacija znakova u vrlo kratkom vremenu. Pritom će se služiti rječnicima raznih jezika, pokušati sve kombinacije mogućih datuma rođenja, jednostavne lozinke kao što su vaše korisničko ime uz moguć dodatak jedne ili dvije znamenke i slično. Kako biste izbjegli mogućnost da računalni programi dizajnirani za pogađanje lozinki pogode vašu, ona ne smije sadržavati predvidljive podatke. Dobra metoda postavljanja lozinke je skraćenica od 6 - 8 znakova (izaberite neku rečenicu koja će samo vama imati smisla) uz ubacivanje 2 - 4 interpunkcijska znaka ili broja.

Na Windowsima korisnici često rade i pristupaju Internetu pod administratorskim ovlastima. Ako ne razumijete pojam administratorskih ovlasti, najvjerojatnije je i kod vas takav slučaj. Naime Windows 2000 i XP su višekorisnički operativni sustavi, što znači da se svojim računalom možete služiti pod više od jednim identitetom uz koji je vezan različit stupanj pristupa računalnim resursima. Zlonamjeran kôd često zahtijeva visok stupanj pristupa vašem računalu kako bi izvršio štetne promjene, što znači da kreiranjem dodatnog korisničkog računa sa smanjenim ovlastima znatno smanjujete mogućnost da netko preuzme kontrolu nad vašim računalom. Najjednostavnija mjera opreza je koristiti korisnički račun sa smanjenim ovlastima svaki put kada se spajate na Internet. Ukoliko koristite stalnu vezu, pod tim biste računom trebali raditi u svim slučajevima osim kada sami želite poduzeti neku radnju za koju vam je potreban administrativni pristup računalu.

Kada unosite podatke u web-formular na nekoj stranici, ti se podaci prenose Internetom u svom izvornom obliku, nezaštićeni. Za takve podatke postoji rizik da ih netko može presresti i pročitati, a da vi to nikada ne saznate. Povjerljivost informacija koje putuju između vašeg računala i web-poslužitelja osigurava enkripcija, odnosno šifriranje podataka u protoku. Stranice koje na taj način prihvaćaju vaše podatke prepoznat ćete po tome što ispred web-adrese sadrže https umjesto http. Vaš web-preglednik također će u statusnoj liniji simbolom lokota naznačiti da se nalazite na sigurnoj stranici.

NAMETNICI

Virusi i crvi

Zlonamjeran kod koji nazivamo virusima i crvima prepoznajemo po mogućnosti samoumnažanja. Kada se izvrše na računalu, među prvim koracima nastoje pronaći sljedeću žrtvu i njoj poslati vlastitu kopiju. Virusi se od crva razlikuju po tome što "inficiraju" neku datoteku, odnosno svoj kod dodaju na neki već postojeći, čekajući da se ta datoteka upotrijebi kako bi se ponovno aktivirali. Povećanjem mogućnosti računala ovaj je korak postao nepotreban i viruse su zamijenili crvi koji svoj kod u cijelosti pohranjuju u stalnu memoriju, na što skrovitije mjesto.

Crvima je obično namjena preuzeti kontrolu nad računalom i omogućiti udaljenu kontrolu čak i nakon primjene sigurnosnih zakrpa. Ovo postižu otvaranjem takozvanih "stražnjih vrata" (backdoor) kroz koja autor može izdavati naredbe vašem računalu bez vašeg znanja. Čak i kada crv sam po sebi nema zlonamjernog koda, što je ponekad bio slučaj, količina mrežnog prometa koji stvara šireći se može usporiti ili čak onemogućiti normalan rad na Internetu ili lokalnoj mreži. Neki crvi posegnut će i za vašim lozinkama i osobnim podacima te ih staviti na raspolaganje autoru.

Većina današnjih crva dolazi na naša računala putem e-maila ili mrežnih servisa. Potonji su opasniji jer u pravilu ne zahtijevaju interakciju s korisnikom, već samostalno preuzimaju kontrolu nad računalom i nastavljaju širenje. Od njih se efikasno možemo braniti vatrozidom, no čak i uz vatrozid preporučuje se primjena sigurnosnih zakrpa. Ova dvostruka zaštita garantira zadovoljavajuće visok stupanj sigurnosti.

Crve koji se šire kroz mrežne servise primijetit ćete kao pokušaje spajanja na vaše računalo koje vatrozid blokira. U ovom slučaju potpuno su bezopasni jer pokušaj iskorištavanja nekog sigurnosnog propusta na vašem računalu nije mogao biti izveden. U slučaju širenja e-mailom vidjet ćete poruku s privitkom sumnjivog nastavka. Tekst poruke uglavnom će nastojati raznim psihološkim trikovima nagovoriti korisnika da otvori privitak. U pravilu, privici za koje niste potpuno sigurni da dolaze iz povjerljivog izvora i da ih očekujete zaslužuju sumnju. Ukoliko su još uz to i izvršni (prilikom pregleda postaju aktivni, odnosno upravljaju vašim računalom), sumnja postaje nužnost. Izvršni privici mogu se pojaviti u obliku mnoštva nastavaka, a navest ćemo samo neke učestalije:

bat	exe	pif	scr	cmd	vbs	js

Budući da se osim ovih nastavaka pojavljuju još mnogi drugi, dobar način procjene radi li se o opasnom privitku je razmisliti od koga nam dolazi taj privitak, jesmo li ga zatražili i znamo li čemu služe datoteke s primljenim nastavkom. Ukoliko nam je nastavak nepoznat, trebamo postupiti oprezno i provjeriti da li nam je poruka poslana od nekoga kome vjerujemo.

Što ako je vaše računalo već pod kontrolom nekog virusa ili crva? U ovom bi slučaju vaš antivirusni alat trebao biti od pomoći. Pokrenite ga i odaberite opciju Full System Scan ili Scan files and folders, pri čemu odaberite sve diskovne kratice. Ovaj postupak obično će potrajati i na kraju vam ponuditi mogućnost da očistite kompromitirane datoteke. Na žalost, antivirusni alati zbog rapidnog razvoja crva ponekad nisu potpuno uspješni u uklanjanju, u kojem slučaju preporučujemo da potražite pomoć stručnjaka.

Trojanski konji

Naziv trojanski konj nastao je po poznatoj priči o osvajanju Troje zloupotrebom povjerenja. Drveni konj predstavljen je kao poklon stanovnicima grada, a u njemu su se nalazili ratnici koji su, čim je pala noć, grad napali iznutra. Na sličan se način virtualni trojanski konj može predstaviti kao igra ili zanimljiv sadržaj koji vam netko šalje u e-mail poruci. Kada se pokrene, na vaše računalo se instalira aplikacija za udaljenu kontrolu.

Osim u e-mail porukama, trojanski konji mogu se pojaviti u obliku datoteka na webu ili mrežama za razmjenu datoteka (peer to peer). Mogućnosti su neograničene jer je metoda širenja - vaše povjerenje.

Zbog ovog individualnog pristupa, trojanski konji često nisu globalno raširenі i mnogi oblici nikada ne stignu do proizvođača antivirusnih alata. Budući da je vaš antivirusni alat jedina specijalizirana aplikacija zadužena za prepoznavanje ovakvog koda, lako je moguće da je jedini izlaz potražiti stručnu pomoć. Jedan od simptoma koje pokazuje računalo na kojem se nalazi trojanski konj je pokušaj podizanja poslužitelja na vašem računalu koji očekuje naređenja autora. Uz instaliran i aktivan vatrozid, ovaj pokušaj bit će evidentiran i moći ćete ga zaustaviti.

Dialeri

Naziv ovog oblika zlonamjernog koda dolazi od engleske riječi *dial*, što u danom kontekstu znači birati broj (na telefonu). *Dialeri* nam često dolaze jednakim putevima kao i trojanski konji. Njihova je zadaća u trenutku aktiviranja prekinuti postojeću vezu s Internetom i uz pomoć modema birati broj u nekoj dalekoj zemlji kako bi ostvarili dobit autoru kroz astronomske cijene poziva. Ako se na ispisu vašeg telefonskog računa pojave čudni međunarodni brojevi, vrlo vjerojatno imate *dialer* na računalu.

Uklanjanjem *dialera* obično se bave alati za uklanjanje neželjenih aplikacija o kojima je bilo riječi u prethodnim poglavljima. Svakako također provjerite postoje li neočekivani unosi u postavkama *Dial-Up Networking* ili *Network Connections*.

Spyware i adware

Ciljani marketing u današnjem je svijetu izuzetno popularan, a zbog svoje velike efikasnosti neki oglašivači posežu i za ilegalnim metodama prikupljanja podataka o potencijalnim kupcima. Podaci koji vam se možda čine nebitnima, kao što su stranice koje ste posjetili ili sadržaj anketa koje ste ispunili, oglašivačima govore o vašim potrošačkim navikama. Često će se iz tih podataka moći saznati i pristupne šifre za *online* kupovinu ili druge oblike financijskog poslovanja. Aplikacije koje se bave neovlaštenim prikupljanjem ovakvih podataka zovemo *spyware*.

Adware je komplement *spywareu* i koristi se prikupljenim podacima kako bi vam u što većem broju i što nametljivije prikazivao reklame vezane uz vaše navike. Obično se pojavljuje u obliku bezbrojnih iskačućih prozora (*pop-up windows*) koji se pojavljuju niotkuda dok koristite web-preglednik ili vam jednostavno prikazuje stranice koje reklamira umjesto onih koje ste tražili. Pritom značajno opterećuje vaše računalo i pristup Internetu, što rad može učiniti neugodnim ili čak nemogućim. Operativni sustav na koji se sustavno instalira *adware* kroz duži period obično završi u nepopravljivom stanju koje zahtijeva ponovnu instalaciju.

Najveći izvor *spywarea* i *adwarea* su stranice vezane uz pornografsku i kockarsku industriju, makar to danas nije pravilo. Koristeći se propustima u vašem web-pregledniku i mameći korisnika da zaobiđe sigurnosne dijaloge, instalira se na vaše računalo bez vašeg eksplicitnog pristanka. Zbog toga se preporuča korištenje alternativnog web-preglednika, a neke od čistača neželjenih aplikacija možete isprobati s CD-a priloženog uz ovu brošuru.

Spyware i *adware* uklanja se korištenjem uklanjatelja neželjenih aplikacija. Budući da komercijalni motivi čine ovaj oblik zlonamjernog koda vrlo otpornim, često je potrebno koristiti više od jednog uklanjatelja neželjenih aplikacija kako bi se računalo potpuno očistilo.

NEŽELJENI SADRŽAJ

Spam

Bezbrojne poruke koje neki korisnici primaju, a koje reklamiraju proizvode za koje nikada niste izrazili interes, *e-mail* obavijesti o temama na koje se niste pretplatili, lažne privatne poruke koje vode na stranice pornografskog sadržaja samo su neki od oblika *spama*. Ukratko, svaka poruka distribuirana masovno koju niste zatražili klasificira se kao *spam*.

Današnji zabrinjavajući podatak da je tri četvrtine svih *e-mail* poruka na Internetu *spam* uzrok je ekonomije velikih brojki. Naime, poslati nekoliko milijuna poruka putem *e-maila* postaje sve lakše i jeftinije, dok će se među tih nekoliko milijuna primatelja gotovo sigurno naći neki koji će proizvod naručiti ili slijediti link koji nekome osigurava naplatu reklame. Budući da širenjem *spama* troškovi održavanja *e-mail* poslužitelja vrtoglavo rastu, a korisnost *e-maila* zbog količine smeća naglo opada, pružatelji internetskih usluga diljem svijeta vrlo oštro sankcioniraju dokazane distributere. Zbog ovog fenomena industrija *spama* sve manje zazire od ilegalnih metoda distribucije.

Velik broj crva u optjecaju od 2003. godine služi pretvaranju računala običnih korisnika u mašineriju za masovno raspačavanje spama. Spajajući se sa zaraženog računala na zaraženo računalo, autori ovih poruka skrivaju svoj identitet i koriste vaše računalne resurse za svoje potrebe. Tako se događa da korisnici na svoje iznenađenje dobiju upozorenje od svog pružatelja internetskih usluga da šalje masovne poruke koje nikada nisu vidjeli, što rezultira blokiranjem pristupa dok se računalo ne očisti.

Još jedan poznat oblik masovno distribuiranih poruka su prijevare (*hoax*).

Svaka poruka koja korisnika lažnim informacijama nagovara da oda povjerljive podatke ili bez opravdanog razloga poduzme neku radnju je prijevara. Najčešće se radi o krađi pristupnih podataka vašem bankovnom računu, no uobičajena su i lančana pisma koja upozoravaju korisnike o nepostojećim prijetnjama ili ih nagovaraju da poduzmu neku destruktivnu radnju na svom računalu.

Najpoznatiji oblici prijevara traže od primatelja da preko svog bankovnog računa prebaci pozamašnu svotu novca. Nesretni korisnici primamljeni bogatim provizijama često ostanu bez novca, dajući nepoznatoj strani podatke o pristupu svojem računu ili nesvjesno sudjeluju u ilegalnoj novčanoj transakciji. Među benignijim oblicima naći ćemo lance sreće (ili nesreće) i obavijesti o lažnim virusima.

Prosječna prijevara prepoznatljiva je po izrazito dramatičnom tonu i tekstu koji senzacionalistički govori o nekoj nevjerojatnoj pojavi. Obično se oslanja na izjavu unutar teksta u kojoj autor upotrebljava izraze kao "znam da zvuči nevjerojatno" ili "začudit ćete se što vam pišem" kako bi priskrbio vaše bezuvjetno povjerenje. Primite ovakve poruke "sa zrnom soli". Ako imate realan razlog vjerovati da je poruka autentična, pokušajte provjeriti identitet pošiljatelja komunicirajući s njim. Svako odbijanje da vam se odaju detalji o identitetu ili insistiranje na korištenju kontaktnih informacija odvojenih od adrese pošiljatelja upućuje na prijevaru.

NADLEŽNE SLUŽBE

Podjela nadležnosti na Internetu

Službe s kojima će korisnik u potrazi za zaštitom svojeg računala kontaktirati zovu se *abuse*-službe i CERT-ovi. U nastavku slijedi objašnjenje što su ove službe i kako odrediti koja od njih može pomoći.

Manji pružatelji internetskih usluga obično imaju nad sobom svog pružatelja internetskih usluga preko kojeg pristupaju mreži. Tako postoji hijerarhija nadležnosti nad virtualnim prostorom koja završava na upravnim tijelima koja taj prostor dodjeljuju. U Sjedinjenim Američkim Državama tu ulogu obavlja ARIN, u Europi RIPE, u Japanu JPNIC i tako dalje. Korisnici Interneta odgovorni su svojem pružatelju internetskih usluga, koji je odgovoran svojem pa tako sve do upravnog tijela za taj dio internetskog prostora. Kada imamo problem s učestalim prekršajima pravila korištenja koje čini neki korisnik Interneta, logičan postupak je prijaviti slučaj sa svim prikupljenim podacima pružatelju internetskih usluga na kojeg je prekršitelj priključen. Kako saznati taj podatak, bit će opisano u sljedećem poglavlju. Služba koja zaprima ovakve pritužbe zove se *abuse*-služba (engl. *abuse* - zloupotreba). Kada smo sigurni da je naš zahtjev opravdan, a nadležna služba ništa ne poduzima, obraćamo se *abuse*-službi više instance po ovdje opisanoj hijerarhiji.

U slučajevima kada se želimo informirati o sigurnosti ili prijaviti hitan sigurnosni problem, obraćamo se CERT-u organizacije koje smo korisnik ili nacionalnom CERT-u ako je takav najbliža instanca. CERT je kratica za *Computer Emergency Response Team* i označava odjel koji se bavi općenitim rješavanjem sigurnosnih problema izvan obima rada *abuse*-službi. Hrvatski CERT izdaje ovu brošuru.

Kao što je bilo riječi u poglavlju "Tko upravlja mojim računalom?", svako računalo priključenjem na Internet dobiva svoju IP adresu koja ga jedinstveno označava među svim ostalim računalima. Taj podatak je ujedno i identifikacijski i govori onima s kojima komuniciramo odakle naše računalo dolazi. S udaljene lokacije običan korisnik ne može saznati točno o kojem se računalu radi samo po njegovoj adresi, međutim pružatelju internetskih usluga taj je podatak dostupan. Zato prilikom prijavljivanja problema vezanih uz promet s nekog računala na Internetu, radilo se o crvu, pokušaju napada, sumnjivoj *e-mail* poruci ili nečem drugom, IP adresa u kombinaciji s vremenom događaja čini najvažniji par informacija za svaki incident. Također je izuzetno bitno uz vrijeme istaknuti vremensku zonu jer su računalno-sigurnosni incidenti često globalni.

Vrijeme je presudno i zbog određivanja identiteta korisnika čijem je računalu tada dodijeljena IP adresa - u nekom drugom trenutku ista adresa može biti dodijeljena nekom drugom. Tipičan primjer promjenjivih IP adresa pojavljuje se u okruženju pristupa putem telefonske linije i modema, takozvanom *dial-upu*.

Kada imamo IP adresu nekog računala koje želimo prijaviti, koristimo se servisom WHOIS kako bismo otkrili nadležnog pružatelja internetskih usluga i kontakt-adresu njegove *abuse*-službe. WHOIS klijenti većinom su besplatni i dostupni za besplatan *download* s Interneta, a mnogi se mogu koristiti i putem web-sučelja bez potrebe za instalacijom na vaše računalo. CERT preporuča korištenje WHOIS servisa dostupnog na web-adresi http://www.cyberabuse.org/whois.

Više o servisu WHOIS možete pročitati u prilogu posvećenom toj temi na str. 23.

Kako i što prijaviti

Kao što vjerojatno nećete prijaviti baš svakog pješaka koji prelazi cestu dok je upaljeno crveno svjetlo na semaforu ili svako nepropisno parkirano vozilo, kod prijave sigurnosnih incidenata također je važno razdvojiti bitno od nebitnog. Incident koji se po vašem mišljenju prečesto ponavlja, događa samo vama ili imate razloga vjerovati da je vezan uz istog korisnika obično vrijedi prijaviti. Reagirajte kada prikupite dovoljno podataka iz vašeg vatrozida ili drugih izvora. Nastojte razumjeti što prijavljujete ili se informirati.

Prijave koje ne sadrže sve podatke potrebne za obradu opterećuju i usporavaju rad *abuse*-službi, što rezultira manjom efikasnošću i u krajnjem obliku niži stupanj sigurnosti svih korisnika. Zato uvijek provjerite da vaša prijava sadrži IP adresu, vrijeme i podatke iz kojih se nedvojbeno može zaključiti o kakvom se tipu prekršaja ili opasne aktivnosti radi. Iz istog razloga je važno incident uvijek prijaviti nadležnoj *abuse*-službi prekršitelja, a ne svom pružatelju internetskih usluga kako se ne bi gubilo vrijeme na preusmjeravanje.

Koristite i redovito ažurirajte sigurnosne alate, kao što su ovi predloženi u brošuri. Alati smanjuju mogućnosti napada na vaše računalo, čime vas svrstavaju u uži krug dobro zaštićenih korisnika. Ne postoji savršeno zaštićeno računalo, no uz malo truda vaše će biti manje privlačno potencijalnom napadaču. Na CD-u uz brošuru također se nalazi i **alternativni web-preglednik** Mozilla Firefox. Kako je Microsoftov Internet Explorer najrašireniji web-preglednik, većina zlonamjernog koda pisana je upravo s namjerom iskorištavanja njegovih propusta. Korištenjem Mozilla Firefoxa ili nekog drugog alternativnog web-preglednika uvelike smanjujete mogućnost zloupotrebe vašeg računala.

Redovito ažuriranje odnosi se i na vaš operativni sustav (najčešće Windows) i aplikacije koje često koristite, a pogotovo aplikacije koje imaju pristup Internetu. Povremeno za operativni sustav i takve aplikacije izlaze zakrpe, odnosno kôd koji popravlja uočene sigurnosne propuste i onemogućava njihovo iskorištavanje. **Redovito posjećujte Windows Update i stranice proizvođača važnijih aplikacija.**

Čuvajte svoje osobne informacije, čak i one koje ne smatrate privatnima. Vaša fizička ili elektronička adresa, podaci o dobi, spolu, potrošačkim navikama i mnoge druge na prvi pogled malo vrijedne informacije na crnom tržištu imaju svoju cijenu. Neke od tih informacija mogu se kombinirati i iskoristiti na vašu štetu, kao na primjer vaša kućna adresa, broj kreditne kartice i datum njenog isteka. Zato svoje podatke u web-formulare upisujte samo kada je to nužno i na stranicama čija je sigurnost i povjerljivost provjerena. Sigurnost protoka podataka između vas i stranice na koju ih upisujete označava simbol lokota u statusnoj liniji vašeg web-preglednika i https umjesto http protokola u adresnoj liniji. Redovito brišite history vašeg web-preglednika, odnosno zapis adresa koje ste posjetili, a pogotovo nakon trgovine putem Interneta.

Lozinke koje koristite za pristup raznim servisima, Internetu i svojem računalu odraz su vašeg identiteta. Ako su prejednostavne, netko ih može pogoditi (sjetite se: računala pogađaju mnogo brže od ljudi). Krađa identiteta danas je popularna kriminalna aktivnost i moguće su razne zloupotrebe, od kojih vas neke mogu i materijalno oštetiti. Nastojte koristiti različite lozinke za pristup različitim servisima (pogotovo po povjerljivosti unesenih podataka) i vodite računa da vaša lozinka sadrži 6 - 8 znakova i da koristite velika i mala slova, brojeve i znakove interpunkcije.

Vaš web-preglednik dolazi s ugrađenim sigurnosnim provjerama za mnoge rizične aktivnosti i u slučajevima gdje postoji mogućnost preuzimanja kontrole nad vašim računalom na to će vas upozoriti. Zlonamjerna strana koja od vas želi ukrasti podatke pokušat će vas nagovoriti da upozorenja vašeg preglednika preskočite sadržajem stranice ili poruke koju pregledavate. Uvijek pažljivo pročitajte upozorenja i razmislite vjerujete li dovoljno autoru sadržaja da biste mu prepustili potpunu kontrolu nad vašim računalom.

Izvor e-mail poruke podatak je kojeg je lako moguće krivotvoriti. Kada vam netko šalje obično pismo, na koverti se može predstaviti kao bilo tko. Slično vrijedi i za polje "From" e-mail poruke. Imajte to na umu kada čitate poruku koja od vas traži da poduzmete neku radnju koja vam se ne čini sigurnom (na primjer da na nekom web-formularu ažurirate svoje podatke za pristup bankovnom računu). Datoteke koje primite kao privitak u e-mail porukama vrlo su opasne i potrebno je biti siguran u njihov izvor i sadržaj.

Neželjene e-mail poruke (spam) često sadrže poveznicu (link) na kojoj se navodno možete odjaviti s liste primatelja takvih poruka. Ovo je u gotovo svim slučajevima laž, a ponekad se radi i o stranicama na kojima možete zaraditi neki zlonamjeran kod. Ne slijedite poveznice za odjavu u spam-porukama!

Poruke prijevare (hoax) navode vas da učinite štetnu promjenu na svom računalu, unesete svoje povjerljive podatke na neku stranicu ili uplaćujete novac u ime nekih sumnjivih poslova. Ne vjerujte e-mail porukama za koje ne možete provjeriti identitet pošiljatelja.

Kada želite prijaviti korisnika koji ugrožava vašu ili tuđu sigurnost svojim postupcima, važno je da vodite računa kome treba poslati prijavu. Većinom ljudi intuitivno pretpostave da se trebaju obratiti abuse-službi svog pružatelja internetskih usluga (ISP), no to je pogrešno. Incident uvijek prijavljujete abuse-službi nadležnoj za izvor napada.

Vaše računalo prilikom priključenja na Internet dobiva svoju IP adresu, a na sličan način dobit će je i računalo korisnika kojeg želite prijaviti. Osnovni preduvjet prijavljivanju sigurnosnog incidenta je mogućnost da saznate IP adresu izvora napada. Za svaki tip incidenta do nje dolazite na drugačiji način. Nekada je to log* vašeg osobnog vatrozida, nekada zaglavlje vaše e-mail poruke, a postoje i drugi načini. Kod svake pojedine aplikacije način dolaženja do podatka o izvoru napada je specifičan pa je potrebno konzultirati priloženu dokumentaciju.

Imate li podatak o IP adresi s koje smatrate da je učinjen neki prekršaj, sljedeći korak je saznati tko je nadležan za raspon kojem ta IP adresa pripada. Pritom se koristite servisom WHOIS, dostupnom u obliku klijentskih aplikacija za download ili izravnu upotrebu putem web-stranice. U odgovoru potražite e-mail abuse-službe ili sličan opis kraj kojeg će se pojaviti e-mail adresa na koju trebate poslati prijavu.

Ponekad se događa da problem prijavite abuse-službi nekog manjeg poduzeća ili ustanove koja nema resursa ili volje riješiti vaš problem. U tom vam slučaju preostaje samo obratiti se višoj instanci, odnosno uputiti servisu WHOIS upit za takozvani parent-objekt. Budući da se pretraživanje parent-objekata razlikuje kod različitih WHOIS klijenata, preporučujemo da konzultirate priloženu dokumentaciju ili proučite web-stranicu na kojoj se WHOIS koji koristite nalazi. Kada ste pronašli višu nadležnu službu, slijedite isti postupak, uz napomenu da vaša prethodna prijava nije zadovoljavajuće riješena.

*log: zapis aktivnosti alata ili aplikacije, obično u obliku tekstualne datoteke.

Pojmovnik

osobni vatrozid
(engl. personal firewall) aplikacija koja kontrolira uspostavljanje veza između vašeg i udaljenih računala, dopuštajući isključivo sigurnu komunikaciju

antivirusni softver
aplikacija koja kontrolira aktivnost izvršnog koda na vašem računalu i nastoji prepoznati viruse, crve ili trojanske konje te ih blokirati

čistači neželjenih aplikacija
(engl. anti-spyware, anti-adware) na zahtjev pronalazi i uklanja aplikacije instalirane na računalo bez korisnikova pristanka

sigurnosne zakrpe
(engl. security patches) javno dostupni paketi proizvođača neke aplikacije koji uklanjaju pronađene ranjivosti i propuste

virus
zlonamjeran (engl. malicious) kôd koji se širi dodavanjem svog koda drugim aplikacijama

crv
(engl. worm) zlonamjeran kod koji se širi kopiranjem svog cjelokupnog sadržaja kroz neki medij komunikacije, npr. e-mail ili servis vašeg operativnog sustava

trojanski konj
zlonamjeran kôd koji se predstavlja kao bezazlena aplikacija i zahtijeva neku radnju korisnika kako bi se instalirao

stražnji ulaz
(engl. backdoor) postupak otvaranja slobodnog pristupa vašem računalu nakon aktiviranja zlonamjernog koda

spyware
aplikacija koja neovlašteno prikuplja vaše osobne podatke i šalje ih autoru

adware
aplikacija koja bez vašeg pristanka prikazuje oglase umjesto ili u sklopu sadržaja koji želite pregledavati

dialer
aplikacija koja prekida vezu s vašim pružateljem internetskih usluga i ostvaruje skupu telefonsku vezu s dalekim zemljama

spam
neželjene, obično reklamne poruke koje se distribuiraju nesrazmjerno velikom broju korisnika

prijevare
(engl. hoax) poruke koje se širenjem lažnih informacija nastoje proširiti i nagovoriti korisnika da poduzme neku štetnu ili čak ilegalnu radnju

abuse-služba
služba unutar tijela nadležnog za upravljanje dijelom internetskog prostora koja obrađuje prijave kršenja pravila korištenja njihovih usluga

CERT
(krat. Computer Emergency Response Team) služba koja se općenito brine o sigurnosti nekog dijela Interneta i u suradnji s drugim srodnim službama o sigurnosti Interneta u cjelini

IP adresa
jedinstvena krajnja adresa na Internetu - jedno računalo može primati komunikaciju na više IP adresa (veliki poslužitelji), no jedna IP adresa može pripadati samo jednom računalu u jednom trenutku

WHOIS
servis putem kojeg određujemo administrativne kontakte tijela nadležnog za neki raspon IP adresa

zaglavlje e-mail poruke
(engl. e-mail header) dio e-mail poruke koji se ne prikazuje prilikom uobičajenog pregleda, a sadrži podatke o postupku dostavljanja te poruke kroz više poslužitelja

PRIMJERI

Primjer crva

U ovom prilogu pronaći ćete primjere nametnika i sumnjivih poruka o kojima je bilo riječi u brošuri. Primjeri vam mogu poslužiti kako biste prepoznali opasan sadržaj po nekim njegovim ključnim karakteristikama i saznali na koji se način u praksi provode prijevare spominjane u brošuri.

Crv Netsky.D

```
Return-Path: <sender@example.com>
Received: from server1.example.com (server1.example.com [*.*.*.*])
          by server2.example.com (0.0.0/8.12.10) with ESMTP id
          i2B9v2102442315
          for <recipient@example.com>; Thu, 11 Mar 2004 10:57:54 +0100 (CET)
Received:from example.com ([1.1.1.1])
          by server1.example.com (0.0.0/8.12.10) with ESMTP id
          i2B9uq0U012227
          for <recipient@example.com>; Thu, 11 Mar 2004 10:56:53 +0100
Message-Id: <200403110956.i2B9uq0U012227@server1.example.com>
From: sender@example.com
To: recipient@example.com
Subject: Re: Your picture
Date: Thu, 11 Mar 2004 10:57:55 +0100
MIME-Version: 1.0
Content-Type: multipart/mixed;
              boundary="----=_NextPart_000_0007_00001D8D.00004942"
X-Priority: 3
X-MSMail-Priority: Normal
X-Trace: server1.example.com 1078999021 12396 *.*.*.*
         (Thu, 11 Mar 2004 10:57:01 +0100)
X-UIDL: `4:"!IR*"!X9;!!P)L!!

This is a multi-part message in MIME format.

------=_NextPart_000_0007_00001D8D.00004942
Content-Type: text/plain;
              charset="Windows-1252"
Content-Transfer-Encoding: 7bit

Your document is attached.
```

```
------=_NextPart_000_0007_00001D8D.00004942
Content-Type: application/octet-stream;
                    name="your_picture.pif"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
                          filename="your_picture.pif"
```

Ovdje priložen tekst predstavlja zaglavlja e-mail poruke, odnosno dio poruke koji nije vidljiv dok je čitate u vašem pregledniku elektroničke pošte. Do zaglavlja poruke u različitim klijentima dolazi se na različit način, o čemu se možete informirati u dokumentaciji priloženoj uz klijent koji koristite.

U ovom primjeru podebljanim slovima označeni su podaci koji su nam od interesa. Važna i slabo poznata činjenica vezana uz elektroničku poštu jest nepouzdanost adrese pošiljatelja, pa čak i primatelja. Sigurno ste dosad primili barem jednu e-mail poruku u čijem je polju To stajala adresa koja nema veze s vama. Kao i kod obične pošte, adresa pošiljatelja i primatelja (osim adrese primatelja na omotnici) može biti lažan podatak.

Prilikom dostave elektroničke pošte svaki poslužitelj koji zaprimi poruku na njezin vrh dodaje jedno zaglavlje Received. U tom zaglavlju zapisuje od koga je primio poruku, kada ju je primio i neke podatke o sebi. U gornjem primjeru poruku je prvi primio server1.example.com, kojem je poslana od strane računala na IP adresi 1.1.1.1. Budući da je ovo prvi korak, on nam otkriva pošiljatelja. Doduše, sam pošiljatelj mogao je postaviti to zaglavlje Received, nastojeći prevariti korisnika koji ga čita. Zato je važno da zaglavlja interpretira stručno osoblje.

Za ovu poruku zaključili smo da sadrži crv po nekim tipičnim sumnjivim obilježjima. Prvenstveno po činjenici da sadrži privitak (engl. attachment) s nastavkom pif. Ovaj nastavak arhaizam je iz vremena podizanja DOS aplikacija pod Windowsima i danas se ne koristi gotovo ni za što dobronamjerno. Gledajući poruku u cjelini, njezin naslov, tijelo i ime privitka služe isključivo sugeriranju korisniku da privitak otvori, što je dosta sumnjivo. Zaključujemo da je s ovakvom porukom u najmanju ruku potrebno postupati oprezno.

Poruka prijevare "Microsoft/AOL merger"

Subject: AOL and Microsoft Merger....

I am forwarding this because the person who sent it to me is a good friend and does not send me junk. Microsoft and AOL are now the largest Internet company and in an effort make sure that Internet explorer remains the most widely used program, Microsoft and AOL are running an e-mail beta test. When you forward this e-mail to friends, Microsoft can and will track it (if you are a Microsoft Windows user) for a two week time period. For every person that you forward this e-mail to, Microsoft will pay you $245.00, for every person that you sent it to that forwards it on, Microsoft will pay you $243.00 and for every third person that receives it, you will be paid $241.00. Within two weeks, Microsoft will contact you for your address and then send you a check. I thought this was a scam myself, but two weeks after receiving this e-mail and forwarding it on, Microsoft contacted me for my e-mail and within days, I received a check for $24800.00. Name of an individual listed here FCG Inc. Wayne PA 610 225 xxxx xxxxxx@fcg.com

U ovoj poruci autor nas pokušava uvjeriti da će nam neka treća strana (Microsoft) platiti što prosljeđujemo njegovu poruku. Ovakav pristup tipičan je primjer takozvanog socijalnog inženjeringa, odnosno manipuliranja ljudskim faktorom u svrhu širenja autorove poruke. Po čemu možemo zaključiti da je ova poruka prijevara? Za početak, informacija nam stiže iz druge ruke (dakle ne izravno od Microsofta), i to od nama nepoznate osobe. Vjerovati takvoj informaciji jednako je rizično kao i vjerovati bilo kome koga sretnete na ulici. Nadalje, velika i ugledna poduzeća u pravilu vam se ne obraćaju van lista na koje ste pretplaćeni.

Kao i u slučaju virusa i crva, prijevare mogu stizati s lažnom adresom pošiljatelja. Neke prijevare predstavit će se kao da dolaze od banke ili velikog proizvođača i morat ćete sami zaključiti koliko takvoj poruci možete vjerovati. U svakom slučaju, poruke koje vas nagovaraju da ih prosljeđujete gotovo sigurno su prijevare jer se takav način oglašavanja smatra neetičnim i ugledni proizvođači ga zaobilaze. Ako imate ikakvog razloga sumnjati u informacije iznesene u nekoj e-mail poruci, najbolji način da provjerite je da se obratite zastupništvu ili izravno osobi koja vas je kontaktirala.

Među najopasnijim oblicima prijevara su one koje vas nagovaraju da prebacite veliku količinu novca s nekog računa. Obično dolaze u obliku tužne priče o nečijoj životnoj tragediji zbog koje je novac ostao blokiran na računu neke daleke zemlje. Reagiranjem na ovakvu poruku možete se zaplesti u lanac na prvi pogled malih troškova koji će od vas biti zahtijevani ili, još gore, biti namamljeni da posjetite kriminalce u nekoj državi s upitnom policijskom zaštitom.

Prijevare slične prethodnima su lažni dobici na lutriji, kada, da biste se domogli fiktivnog dobitka, prolazite kroz isti ciklus kao ovaj opisan maloprije.

Primjer spama

Neki oblici spama prepoznatljivi su odmah samim time što su nečitljivi. Naime, slati spam je jeftino pa mnogi pošiljatelji koje zanima samo lokalno tržište primjerice Kine ili Rusije svejedno šalju svoje poruke na sve adrese kojih se mogu domoći. Tako dobivamo čudne nečitljive poruke na raznim jezicima.

Drugi česti oblik su poruke koje se bave ilegalnom prodajom softvera. Već u naslovu poruke susrest ćete se s nazivima raznih verzija Windowsa ili poznatih grafičkih alata.

Mnoge poruke pisane su kao da vam se obraća poznata osoba i preporučuje vam neku web-stranicu. Ako vam je sumnjivo što vam netko za koga nikada niste čuli piše vrlo opširnu preporuku neke stranice, imate razloga za sumnjičavost.

Posljednja velika skupina spama koju ćemo spomenuti neželjene su poruke običnog prodajnog karaktera, odnosno oglašavaju neki proizvod kojeg vam žele prodati i navode vas da posjetite njihovu stranicu ili ispunite web-narudžbu. Budući da je spam usko povezan s crvima i ilegalnim metodama prikupljanja osobnih podataka, lako se može dogoditi da, umjesto na plaćanje narudžbe, vaš novac ode u nepovrat, a vaše računalo bude zaraženo trojanskim konjem ili nekim oblikom spywarea. Naša je preporuka da se kod internetske trgovine držite provjerenih ponuđača.

Subject: Try Viagra for Free

Always wanted to try the drug the world has been talking about?

Well now is your chance to try it for FREE!!!

Get FREE Viagra here: www.123getnow.com/free/?bonsay

Remove yourself here: www.4drugs123.com/rm.html

U ovom primjeru oglašava se web-stranica ponuđača Viagre koji među ostalim ima neku besplatnu promotivnu ponudu. Ključni dio je zadnji red u kojem se spominje web-adresa na kojoj se možete odjaviti s liste primatelja (na koju se gotovo sigurno nikada niste prijavili). Nikako ne slijedite ove poveznice (link) - one u najvećem broju slučajeva služe autoru da verificira vašu e-mail adresu kako bi ona postigla što veću cijenu na crnom tržištu. Postoje čak i primjeri u kojima poveznica vodi do stranice sa zlonamjernim kodom.

Upute za instalaciju i korištenje alata koji se nalaze na CD-u u prilogu ovoj brošuri.

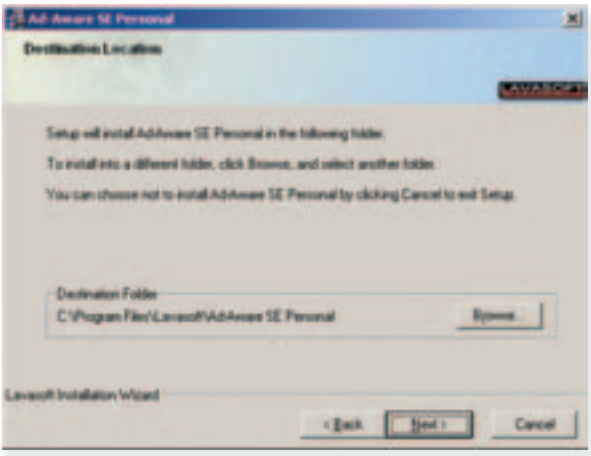
Ad-Aware SE Personal

Instalacija

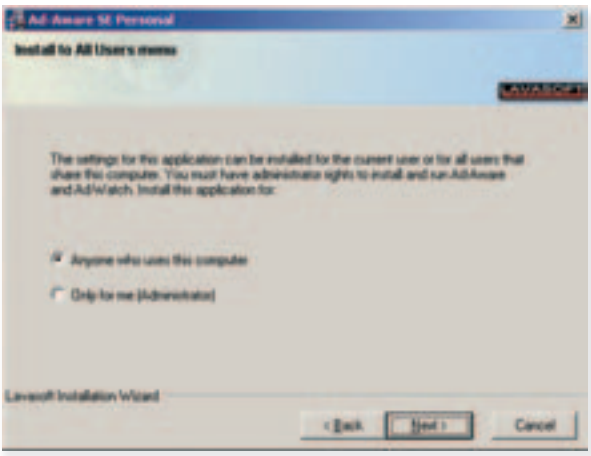
1. Nakon pokretanja instalacije Ad-Awarea SE Personal pojavljuje se sljedeći prozor. Kliknite *Next* kako biste započeli proces instalacije.

2. Pročitajte tekst licence i upoznajte se s pravilima korištenja aplikacije. Kliknite na kućicu pored *I accept the license agreement*, a zatim na *Next*.

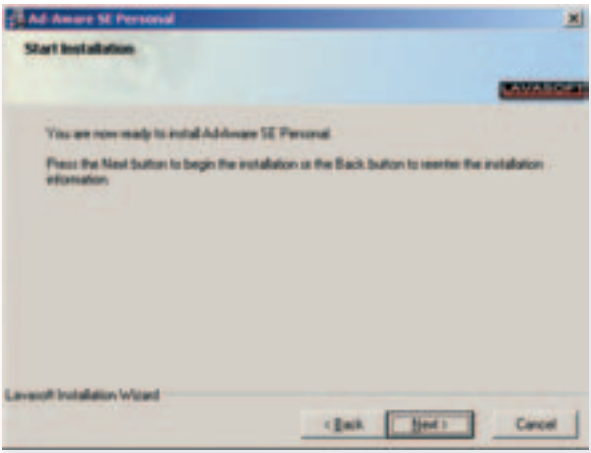
3. Kliknite *Next*. Upućeniji korisnici mogu pritiskom na tipku *Browse* po želji promijeniti lokaciju na disku na koju će se aplikacija instalirati.



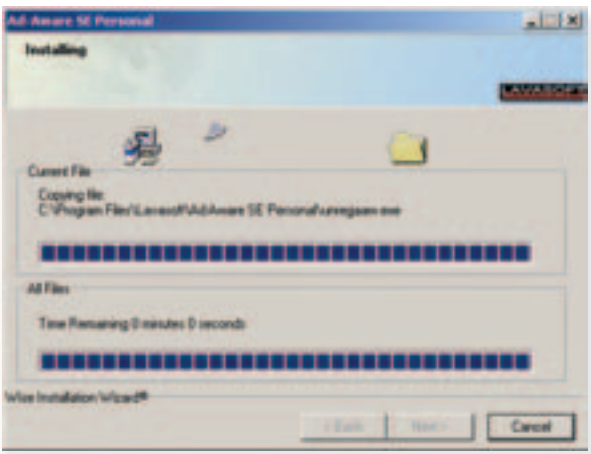
4. Kliknite *Next*.



5. Kliknite *Next*.



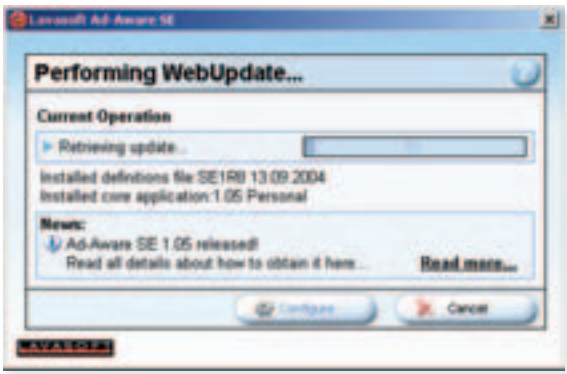
6. Instalacija započinje.



7. Kliknite na kućicu *Open the help file now* kako biste uklonili kvačicu.

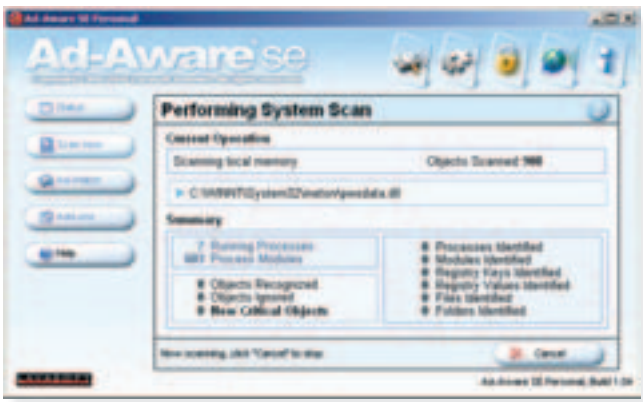
8. Aktivirajte svoju vezu na Internet kako bi Ad-Aware mogao pristupiti novim definicijama. Kliknite *Finish*.

9. Pojavljuje se prozor u kojem možete pratiti postupak ažuriranja.



Korištenje

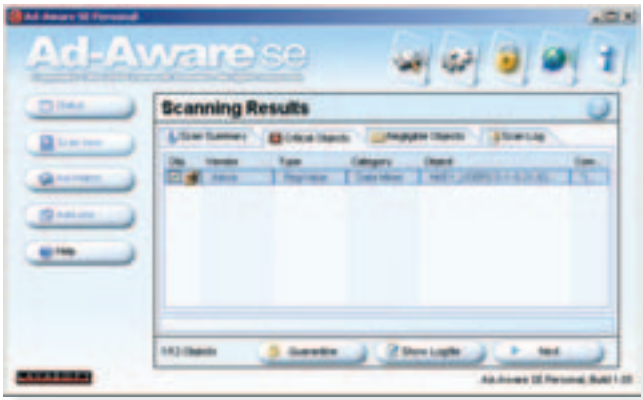
1. Po završetku ažuriranja, Ad-Aware započinje pretraživanje vašeg računala u potrazi za nepoželjnim aplikacijama. Pričekajte da ovaj proces završi.



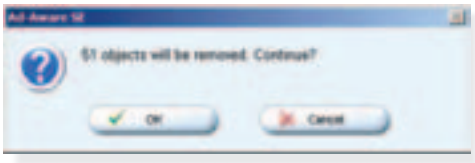
2. Po završetku pretraživanja, Ad-Aware prikazuje pronađene nepoželjne aplikacije.

3. Kliknite desnom tipkom miša na jednu od pronađenih aplikacija i odaberite *Select All Objects*.

4. Uz svaku od pronađenih aplikacija sada se nalazi kvačica. Kliknite *Next*.

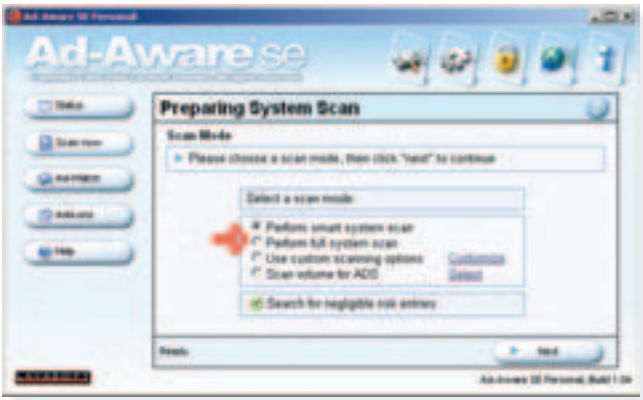


5. Potvrdite čišćenje nepoželjnih aplikacija klikom na *OK*.



1. Ažuriranje definicija poželjno je obavljati prije svakog pokretanja traženja nepoželjnih aplikacija. Ovaj postupak identičan je ažuriranju definicija prilikom instalacije, a do njega se dolazi klikom na opciju *Check for updates now* u donjem desnom kutu kontrolnog prozora Ad-Awarea.

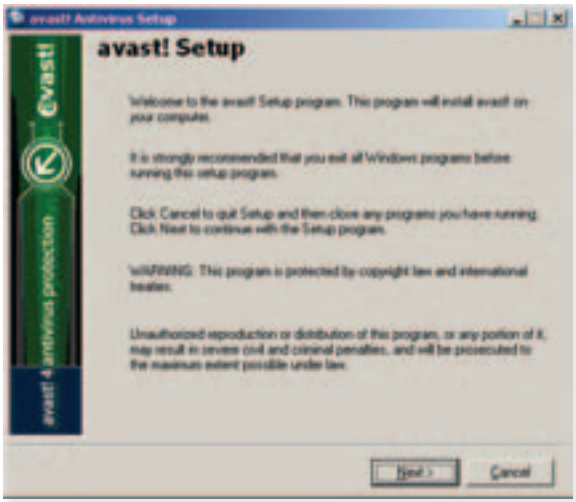
2. Nakon uspješnog ažuriranja, pretraživanje započinjete klikom na *Scan now* u lijevom stupcu prozora. Odaberite kućicu pored *Perform full system scan* i kliknite *Next*. Instalacija i inicijalno čišćenje vašeg sustava je završeno.



Avast!

Instalacija

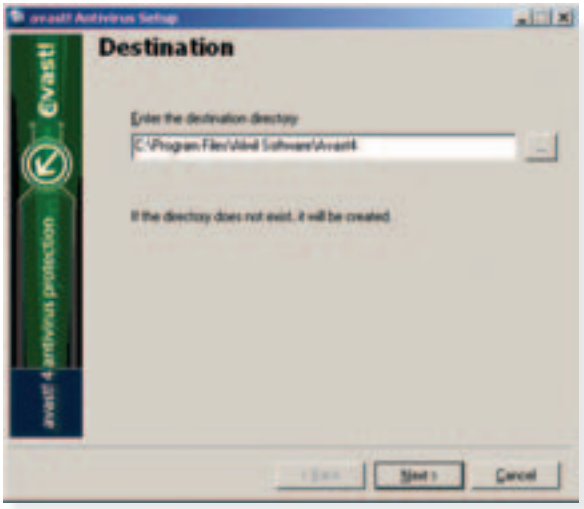
1. Nakon pokretanja instalacije alata avast! pojavljuje se sljedeći prozor. Kliknite *Next*.



2. Pojavit će se prozor s minimalnim zahtjevima za instalaciju. Kliknite *Next*.

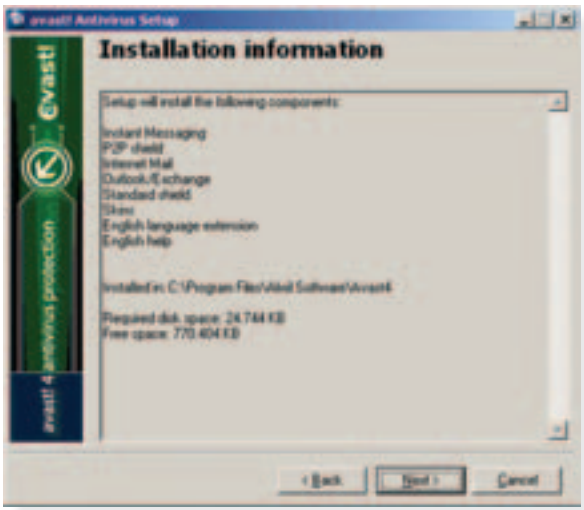
3. Pročitajte tekst licence i upoznajte se s pravilima korištenja aplikacije. Kliknite na opciju *I agree*, a zatim na *Next*.

4. Kliknite *Next*. Upućeniji korisnici mogu pritiskom na tipku [...] po želji promijeniti lokaciju na disku na koju će se aplikacija instalirati.

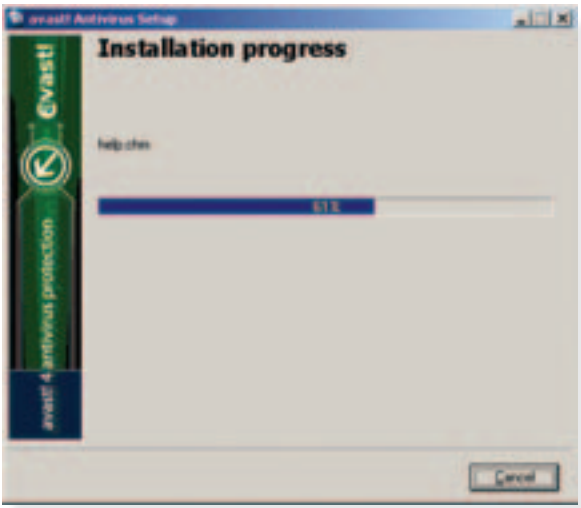


5. Na odabiru komponenti kliknite *Next*. Pojavljuje se popis odabranih komponenti. Za ispravan rad u većini okruženja nije potrebno mijenjati standardne postavke.

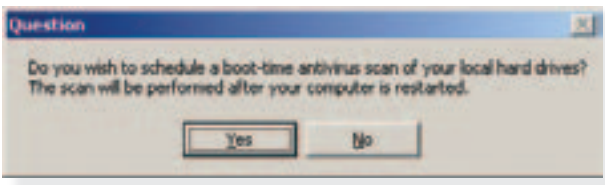
6. Kliknite *Next*.



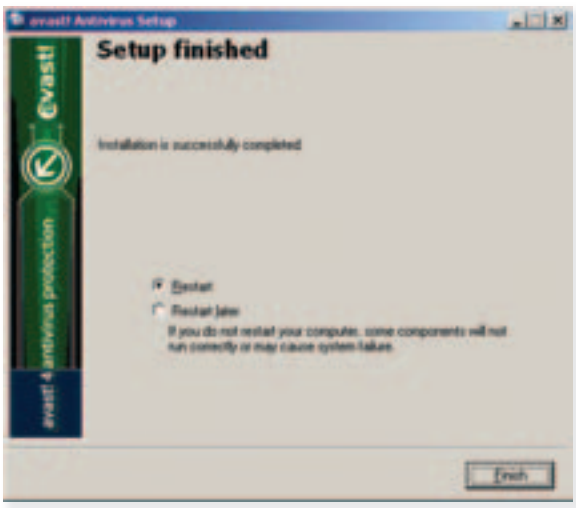
7. Instalacija započinje.



8. Pojavit će se upit želite li da avast! pregledava računalo pri pokretanju. Kliknite *Yes*.

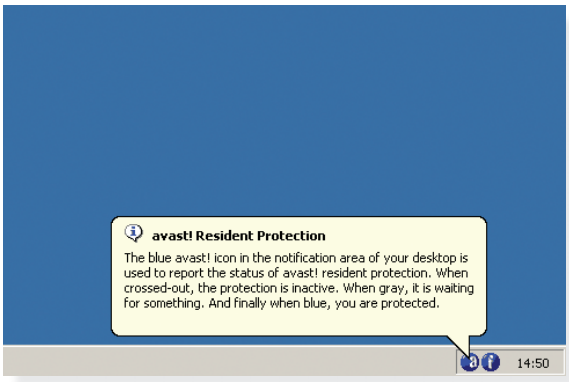


9. Nakon što kliknete *Finish*, instalacijski program će restartati računalo.

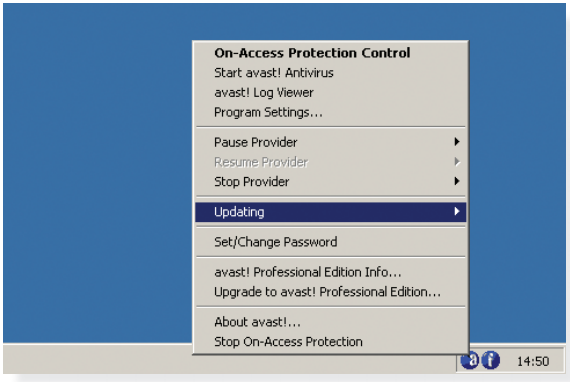


10. Nakon ponovnog pokretanja avast! će vas pozdraviti sljedećim prozorom. Kliknite *Ok*.

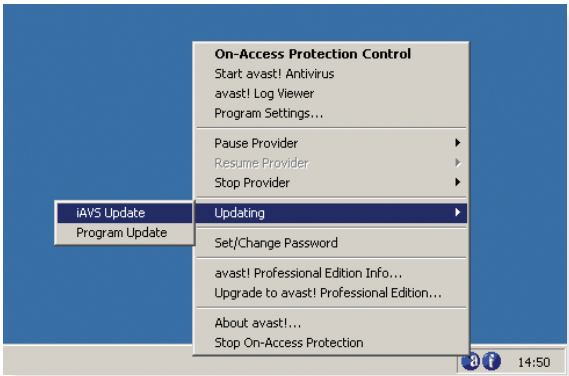
11. U donjem desnom kutu vašeg zaslona pojavit će se dvije plave statusne ikone. To znači da je avast! uspješno instaliran.



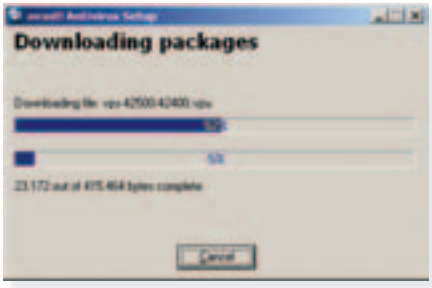
1. Ažuriranje: Kako bi antivirusni program avast! uspješno detektirao nove viruse, crve i trojanske konje, potrebno je redovito koristiti opciju ažuriranja antivirusnih definicija. Toj opciji pristupa se iz kontekstnog izbornika avast!-ove ikone u statusnoj traci.
   Aktivirajte svoju vezu na Internet kako bi avast! mogao pristupiti novim definicijama. Desnom tipkom miša kliknite na plavi kružić s malim bijelim slovom "a" u statusnoj traci. U izborniku zadržite pokazivač miša na stavci *Updating*.



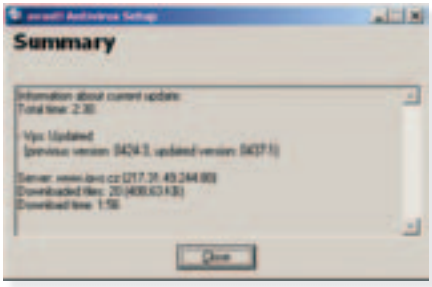
2. Odaberite *iAVS Update*.



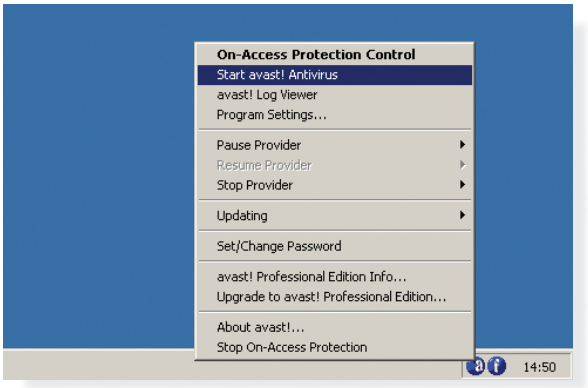
3. Pojavit će se prozor u kojem možete pratiti proces ažuriranja antivirusnih definicija.



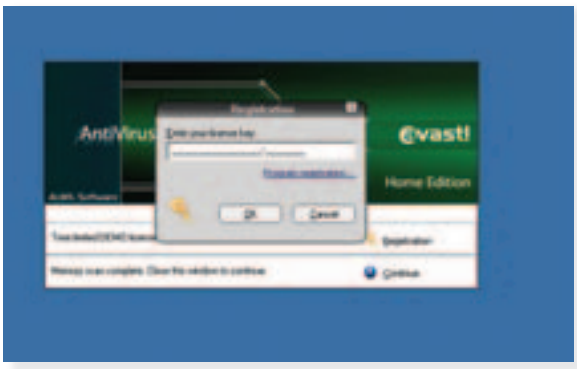
4. Pričekajte da ažuriranje završi. Pojavit će se sljedeći prozor. Kliknite *Close*. Avast je spreman za korištenje.



5. Još jednom kliknite desnom tipkom miša na plavu avast! ikonu. Odaberite opciju *Start avast! Antivirus*.



6. Pri prvom pokretanju programa avast! potrebno je upisati broj licence za aktivaciju besplatne inačice alata. Licencu dobivate e-mailom nakon registracije na web stranicama proizvođača. Kliknite *OK* nakon što ste upisali tražene podatke.

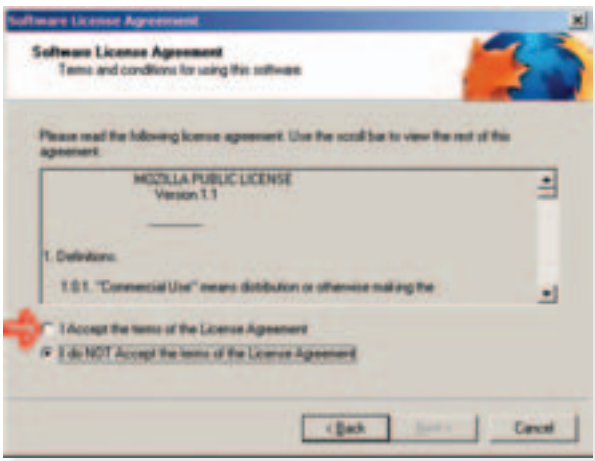


7. Program vas pozdravlja kratkim uputama o korištenju. Kliknite na kućicu *Don't show this window next time* i zatvorite prozor klikom na X u gornjem desnom kutu prozora.

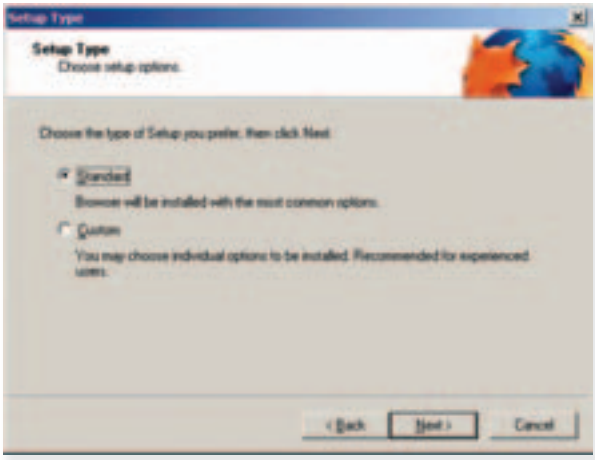
8. avast! je aktivan i spreman za rad.

1. Nakon pokretanja instalacije Mozilla Firefoxa pojavljuje se sljedeći prozor. Kliknite *Next*.

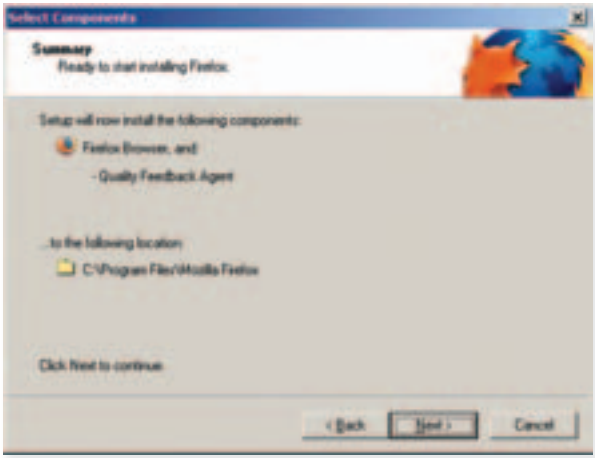
2. Pročitajte tekst licence i upoznajte se s pravilima korištenja aplikacije. Kliknite na kućicu pored *I Accept the terms of the License Agreement*, a zatim na *Next*.



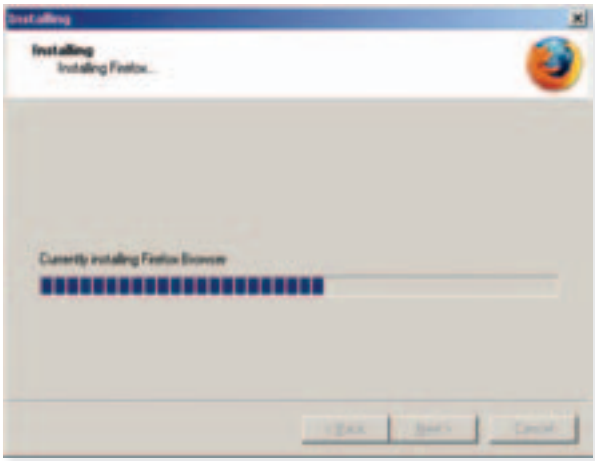
3. Kliknite *Next*.



4. Kliknite *Next*.

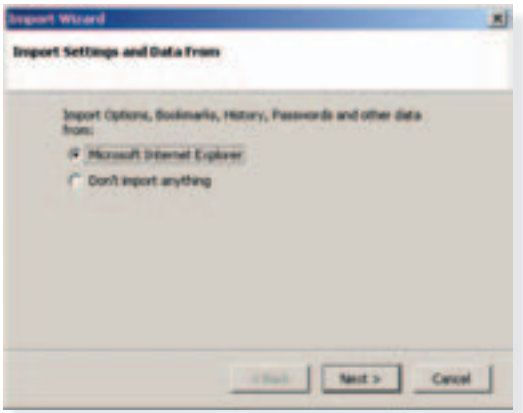


5. Instalacija započinje.

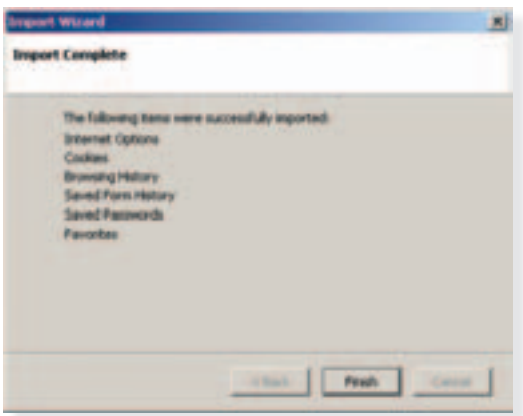


6. Kliknite Finish. Po želji isključite prvu kućicu ako ne želite da Firefox Start bude vaša početna stranica. Mozilla Firefox je spreman za korištenje.

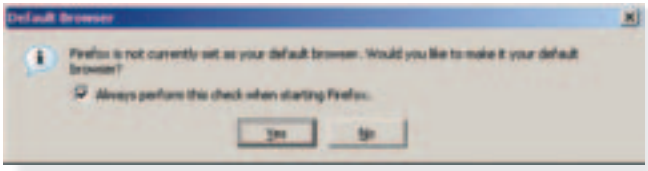
7. Nakon pokretanja Firefox provjerava želite li preuzeti postavke i favorite iz Internet Explorera. Kliknite *Next*.



8. Firefox vas izvještava što je sve preuzeto. Kliknite *Finish*.



9. Želite li da vam Firefox bude defaultni web preglednik, kliknite *Yes*.

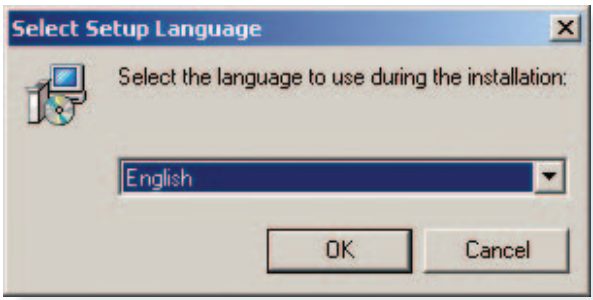


10. Firefox je spreman za rad.

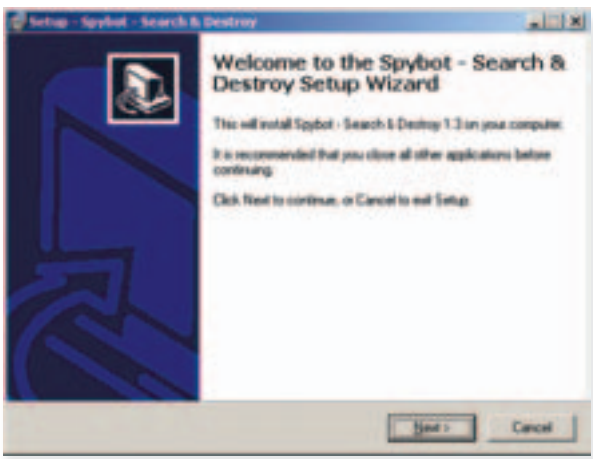
Spybot - Search & Destroy

Instalacija

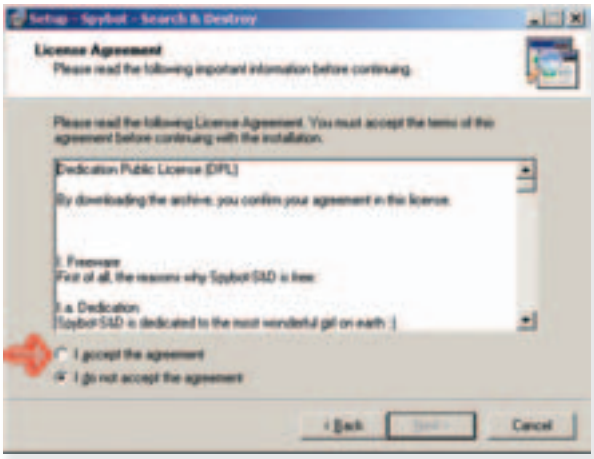
1. Nakon pokretanja instalacije Spybot - Search & Destroya pojavljuje se prozor za odabir jezika. Kliknite *Ok*.



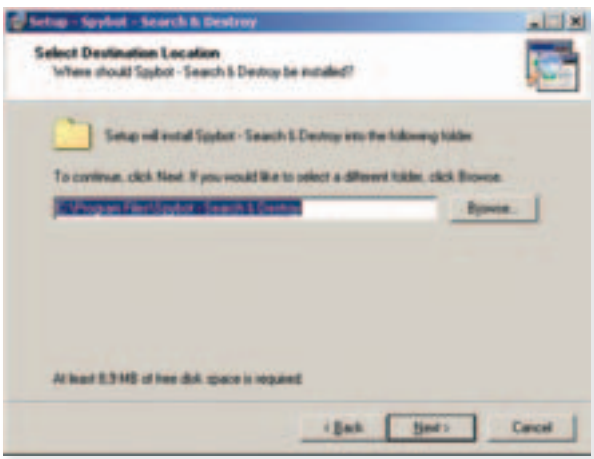
2. Kliknite *Next*.



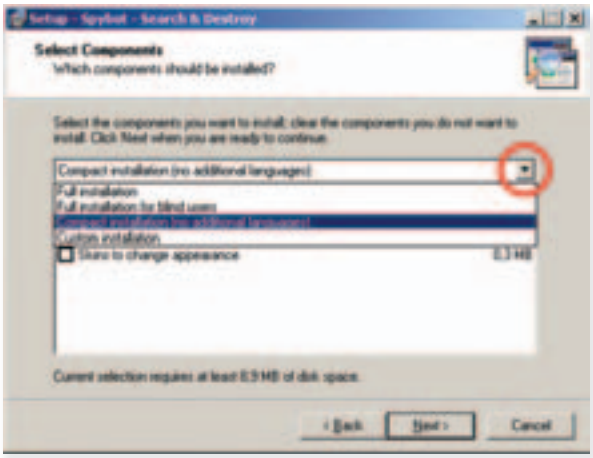
3. Pročitajte tekst licence i upoznajte se s pravilima korištenja aplikacije. Kliknite na opciju *I accept the agreement*, a zatim na *Next*.



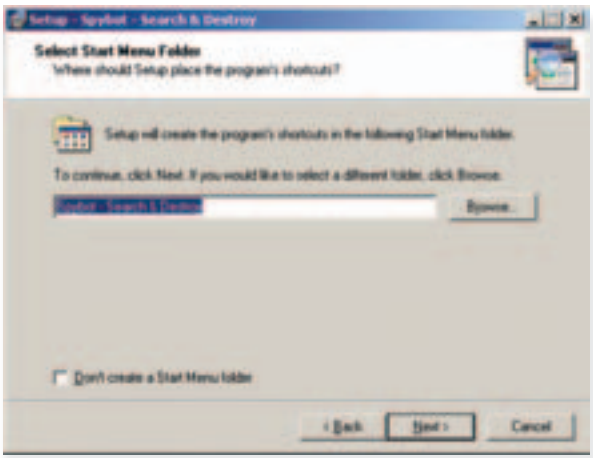
4. Kliknite *Next*. Upućeniji korisnici mogu pritiskom na tipku *Browse* po želji promijeniti lokaciju na disku na koju će se aplikacija instalirati.



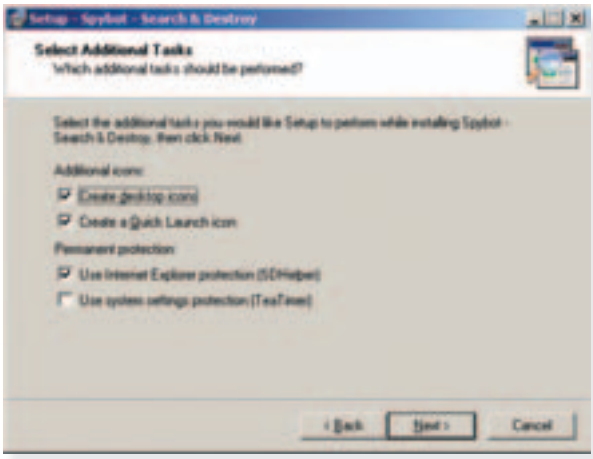
5. Kliknite na strelicu pored padajućeg izbornika i odaberite *Compact installation (no additional languages)*.



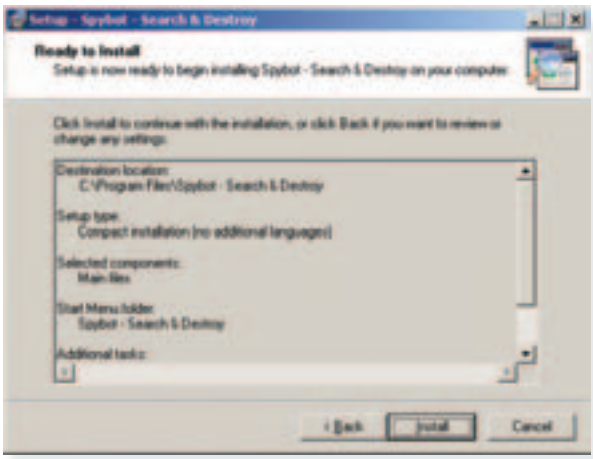
6. Kliknite *Next*.



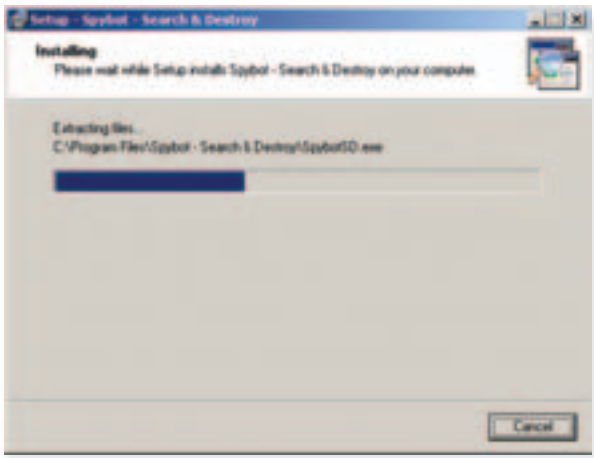
7. Kliknite *Next*.



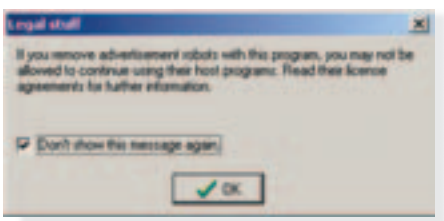
8. Kliknite *Install*.



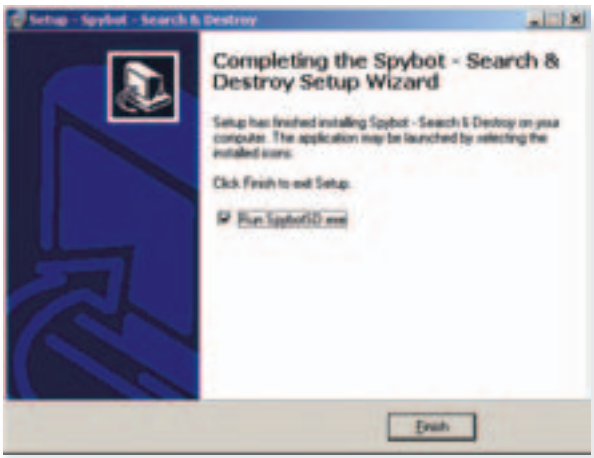
9. Instalacija započinje.



10. Pojavljuje se kratko upozorenje koje vas se tiče jedino ukoliko koristite sponzorirani softver, što kod većina korisnika nije slučaj.
Označite kućicu *Don't show this message again* i kliknite *OK*.



11. Kliknite *Finish*. Pojavit će se Spybot-S&D Wizard.

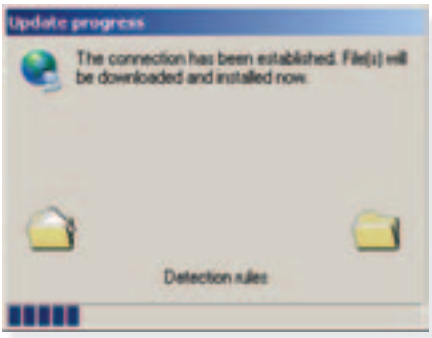


12. Kliknite *Create registry backup* kako biste napravili sigurnosnu kopiju podataka u slučaju da dođe do većih problema s čišćenjem nepoželjnih aplikacija. Po završetku ovog procesa kliknite *Next*.

13. Aktivirajte svoju vezu na Internet kako bi Spybot - Search & Destroy mogao pristupiti novim definicijama. Kliknite *Search for updates*. Kada proces završi, tipka *Download all available updates* više neće biti zasivljena i moći ćete na nju kliknuti.

14. Kliknite na tipku *Download all available updates*.

15. Pojavit će se sljedeći prozor u kojem možete pratiti postupak ažuriranja. Pričekajte da završi. SpyBot je ažuriran i spreman za korištenje.



1. Korištenje: Nakon instalacije na vašoj radnoj površini (Desktop) trebala bi se nalaziti ikona Spybot - Search & Destroy aplikacije. Dvokliknite ikonu kako biste pokrenuli aplikaciju. Pričekajte nekoliko trenutaka.

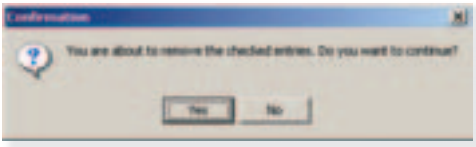
2. Kliknite tipku *Check for problems*.

3. Pričekajte dok proces pregledavanja vašeg računala ne završi.

4. Na prikazu će se pojaviti popis pronađenih problema.

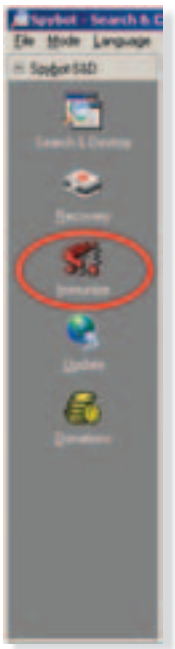
5. Kliknite *Fix selected problems*.

6. Potvrdite da želite očistiti označene probleme klikom na tipku *Yes*.

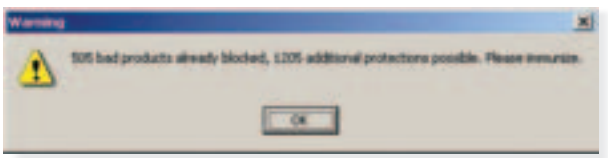


7. Kliknite *OK* na izvještaj o izvršenim radnjama.

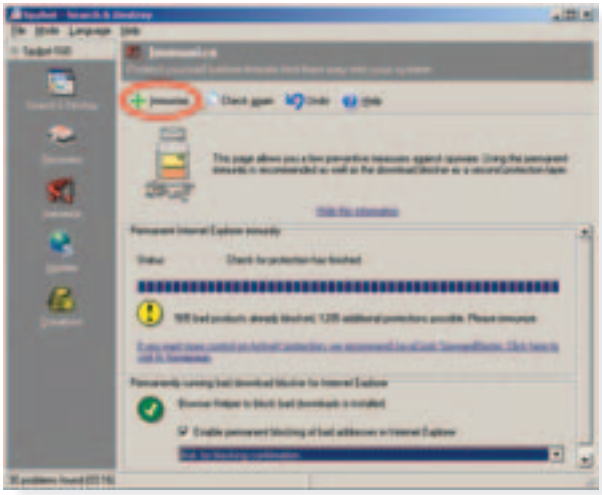
8. Spybot - Search & Destroy ima mogućnost trajne zaštite Internet Explorera protiv nekih oblika zloupotreba njegovih slabosti. Ta mogućnost zove se *Immunize*. Kliknite na ikonu *Immunize* u lijevom stupcu glavnog prozora. Spybot - Search & Destroy obavijestit će vas o mogućim načinima zaštite vašeg web-preglednika.



9. Kliknite *Ok*.



10. Kliknite *Immunize*.



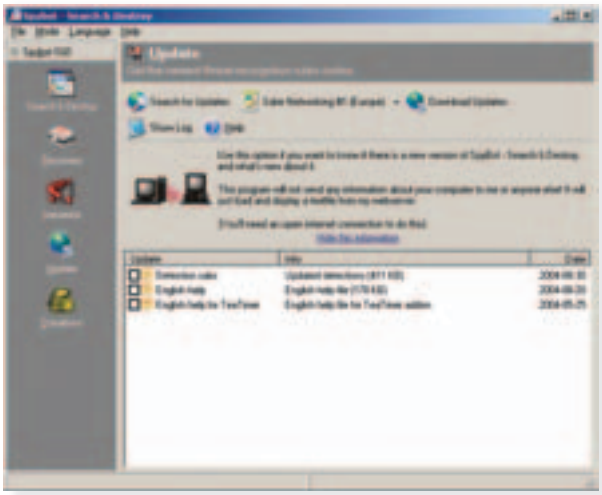
11. Sljedeći put kada pokrenete opciju Immunize prije sljedećeg ažuriranja, trebala bi se pojaviti sljedeća poruka.

Ažuriranje

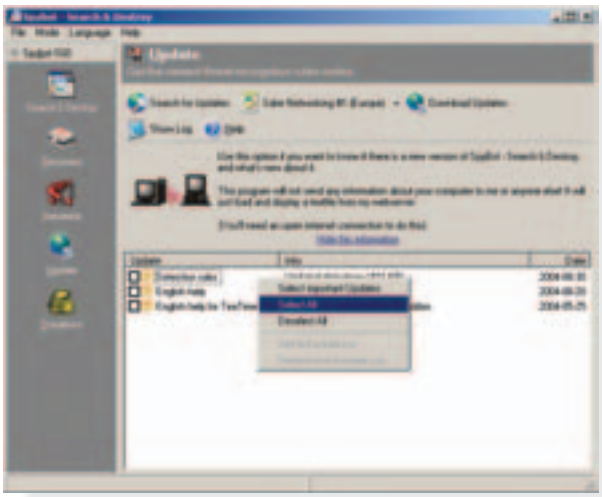
1. Ažuriranje: Ažuriranje je preporučljivo obavljati prije svakog pokretanja procesa traženja i čišćenja neželjenih aplikacija. Aktivirajte svoju vezu na Internet kako bi Spybot - Search & Destroy pristupio novim definicijama. Kliknite *Search for Updates*.

2. Pojavit će se sljedeći prozor u kojem možete pratiti postupak prikupljanja informacija. Pričekajte da završi.

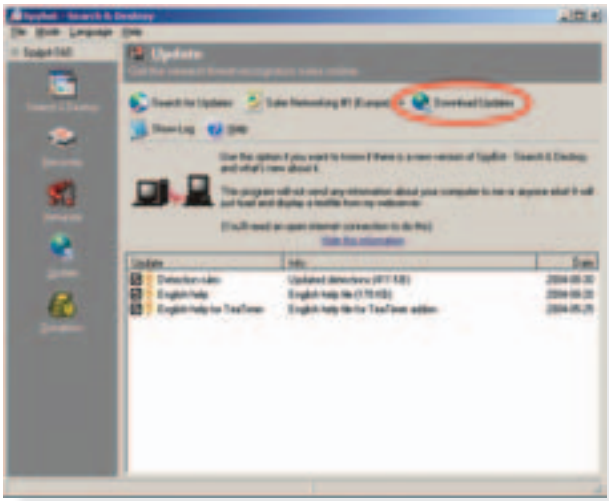
3. Na prikazu će se pojaviti popis mogućih stavki za preuzimanje definicija s nekog od Spybot - Search & Destroyjevih poslužitelja.
   Ako se pojavi obavijest *No new updates available*, najnovije definicije već su instalirane i ažuriranje nije potrebno.



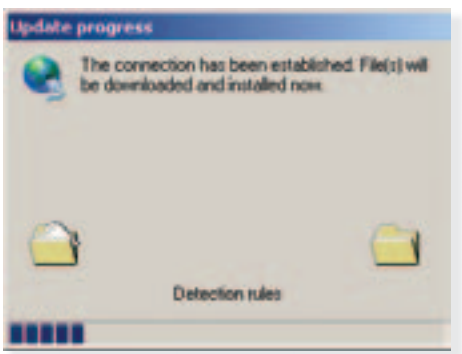
4. Desnom tipkom miša kliknite na područje unutar popisa. Odaberite stavku *Select all* iz izbornika.



5. Kliknite *Download updates*.



6. Pojavit će se sljedeći prozor u kojem možete pratiti postupak ažuriranja. Pričekajte da završi. Instalacija i inicijalno čišćenje vašeg računala je završeno.

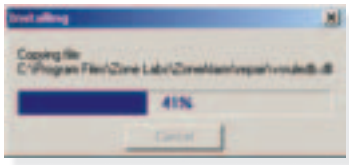


1. Nakon pokretanja instalacije ZoneAlarma pojavljuje se sljedeći prozor. Kliknite *Next*. Upućeniji korisnici mogu pritiskom na tipku *Browse* po želji promijeniti lokaciju na disku na koju će se aplikacija instalirati.

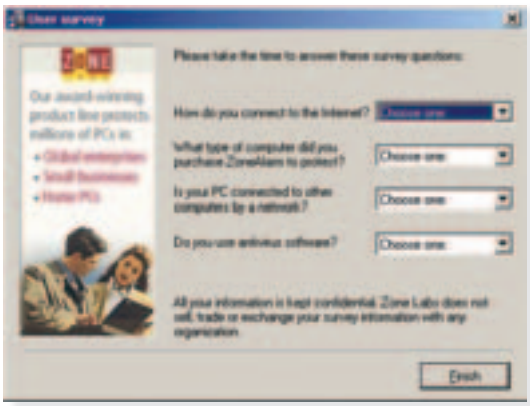
2. Upišite svoje registracijske podatke. Ukoliko donje dvije kućice s pitanjima želite li primati obavijesti od ZoneLabsa ostavite uključenima, svakako pročitajte dokument do kojeg pristupate klikom na *See our Privacy Policy*.

3. Pročitajte tekst licence i upoznajte se s pravilima korištenja aplikacije. Kliknite na kućicu pored *I accept the terms of the preceding License Agreement*, a zatim na *Install*.

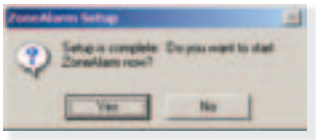
4. Instalacija započinje.



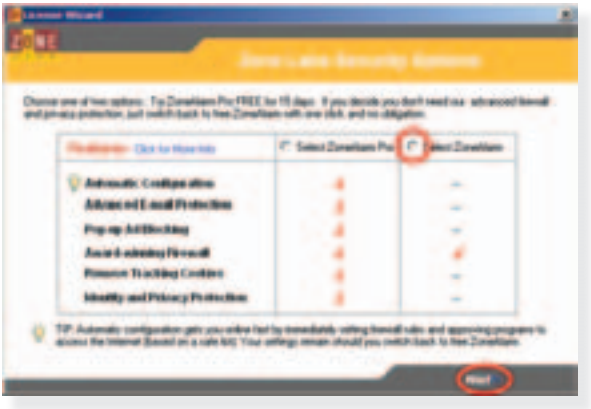
5. Po želji ispunite anketu ili jednostavno kliknite *Finish*.



6. Kliknite *Yes* da bi pokrenuli ZoneAlarm.



7. Odaberite *Select ZoneAlarm* i kliknite *Next*.

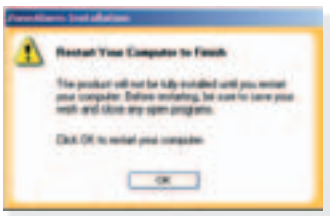


8. Kliknite *Finish*.

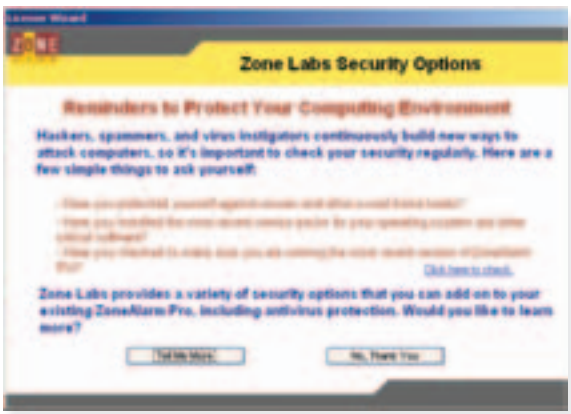
9. Kliknite *Next*.

10. Kliknite *Done*.

11. Nakon što kliknete *OK*, vaše računalo će se ponovno pokrenuti.

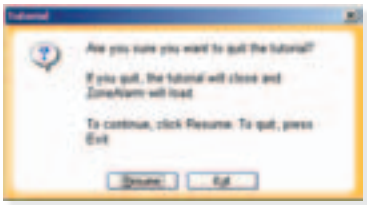


12. Odmah nakon pokretanja pojavit će se sljedeći prozor. ZoneAlarm vam nudi da se informirate o komercijalnoj verziji Pro koja ima više mogućnosti zaštite. Ako ne namjeravate kupiti ZoneAlarm Pro, kliknite *No, Thank You*.



13. Pojavit će se vodič (*tutorial*) kroz upotrebu vatrozida ZoneAlarm. Preporučujemo da ovaj vodič pročitate jer sadrži mnogo korisnih informacija o radu s vašim vatrozidom. Kroz korake vodiča krećite se tipkama *Next* i *Back*. Ako ipak želite preskočiti vodič kliknite *Finish*, nakon čega se pojavljuje upit da potvrdite zatvaranje.

14. Kliknite *Exit*.



15. Pojavit će se kontrolni prozor vatrozida ZoneAlarm. Zatvorite ZoneAlarmov kontrolni prozor. Pojavljuje se poruka koja objašnjava da ovim postupkom niste ugasili vatrozid, već samo njegov kontrolni prozor.

16. Na slici je prikazan izbornik iz kojeg je moguće ugasiti vatrozid ako to želite. Kliknite na opciju *Don't show this message again*, a zatim na *OK*. ZoneAlarm je aktivan i spreman za rad.

+CERT.hr

CARNet

Helpdesk za krajnje korisnike:
Telefon: 0800 CARNet (0800 227638)
E-mail: *helpdesk@CARNet.hr*

Ured za odnose s javnošću:
E-mail: *press@CARNet.hr*

Adresa za kontakt:
CARNet CERT
Ulica Josipa Marohnića bb, 10000 Zagreb
Telefon: 01-6165-770, Telefax: 01-6165-615
E-mail: *ccert@cert.hr*
Web: *http://www.cert.hr*

NACIONALNO SREDIŠTE ZA SIGURNOST RAČUNALNIH SUSTAVA