HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza Windows Defender alata

CCERT-PUBDOC-2006-12-177

CARNet CERT u suradnji s LS&S

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

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

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

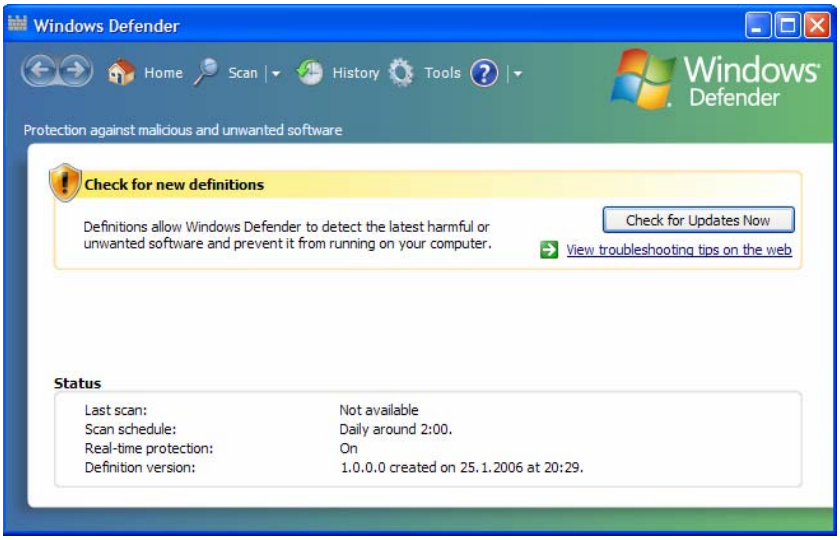
LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Windows Defender je Microsoft-ov alat za uklanjanje neželjenih programa (eng. *spyware, adware*) s korisničkog računala. Neželjeni su oni programi koji se bez znanja korisnika instaliraju na računalo i prikazuju iskočne reklame ili prate korisnikovo ponašanje i navike na Internetu. Windows Defender prepoznaje definirane nepoželjne programe, a liste novih definicija automatski skida s Microsoft-ovih web stranica.

Alat podržava Windows XP (sa Service Pack 2 skupom zakrpi), Windows Server 2003 (sa Service Pack 1 skupom zakrpi) te Windows Vista operacijske sustave, ali ne i ostale inačice operacijskih sustava tvrtke Microsoft. U svome radu ponaša se kao pozadinski proces što znači da pokrenut u pozadini filtrira sav promet koji korisnik učini putem Interneta. Ukoliko je potrebna korisnička intervencija, na alatnoj se traci prikazuje iskočni prozor s odgovarajućom obavijesti. Time se poboljšava proces filtriranja jer korisnik proširuje popis inicijalnih definicija. Definicije se obnavljaju automatski sa stranica proizvođača. Alat, osim što može spriječiti instaliranje neželjenog programskog koda, također može napraviti i cjeloviti pregled računala. Posebnost programa je besplatna instalacija, ali samo na legalnim inačicama Windows operacijskog sustava. Instalacija i obnavljanje definicija na piratskim inačicama nije moguća.



Slika 1: Izgled osnovnog sučelja alata

2. Windows Defender alat

2.1. Razvoj Windows Defender alata

Windows Defender je temeljen na uratku tvrtke Giant AntiSpyware koju je Microsoft kupio u listopadu 2004. godine s namjerom da korištenje Interneta učini sigurnijim za korisnike svojih Windows operacijskih sustava. Tada je Giant AntiSpyware slovio kao najbolje rješenje na tržištu. Od tada do izdavanja konačne inačice prošle su gotovo dvije godine. Nakon preuzimanja kompanije Microsoft je alat nazvao Windows Antispyware. Kroz proteklo vrijeme alat je više puta obnovljen novim definicijama potpisa, minornim promjenama funkcionalnosti, a i sam je programski kod morao biti nanovo napisan. Jedan od glavnih nedostataka izvornog programskog koda je njegova izvedba programskim jezikom Visual Basic koji se pokazao nedovoljno dobrim za širok spektar platformi na kojima je novoizrađeni programski paket trebao raditi.
Osim promjene jezika u kojem je pisan alat, bilo je potrebno izmijeniti i način njegovog izvršavanja. Alat se izvorno ponašao kao normalna Windows aplikacija, a ne kao servis, što je značilo da su ga mogli koristiti samo korisnici s administratorskim ovlastima. U konačnoj inačici alata nazvanoj Windows Defender, alat se ponaša poput servisa što znači da ga svi korisnici na računalu mogu koristiti i da su svi primjereno zaštićeni. Kroz cijelo vrijeme razvoja alat je ostao vodeći u svojoj kategoriji.

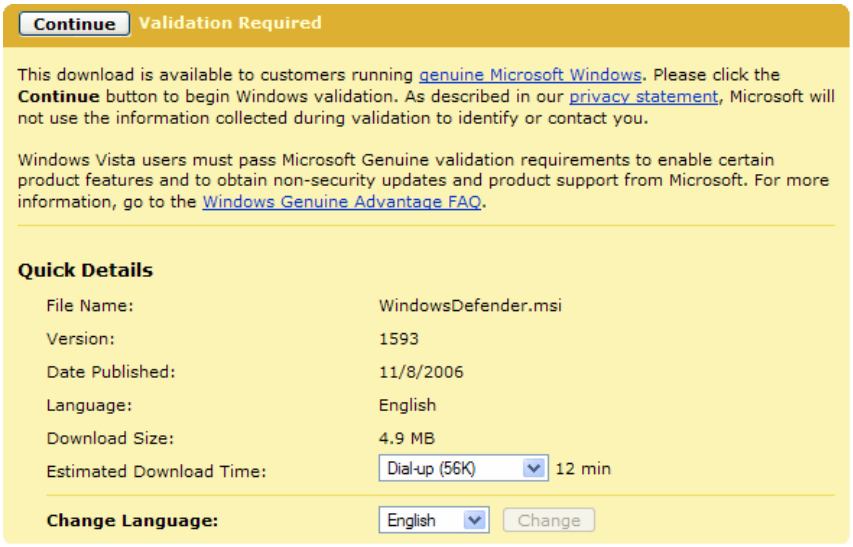
2.2. Preduvjeti sustava za instalaciju Windows Defender alata

Za instalaciju Windows Defender alata potrebno je imati operacijski sustav Windows XP s nadogradnjom Service Pack 2, Windows Server 2003 s nadogradnjom Service Pack 1 ili Windows Vista. Osim navedenih sustava prethodno je potrebno postaviti program Windows Installer 3.1, te instalirati Microsoft Internet Explorer inačice 6.0 ili više.
Ukoliko se prilikom instalacije ne koristi brza i stalna Internetska veza, proces instalacije može biti dugotrajan. Alat zahtijeva provjeru autentičnosti Windows operacijskog sustava. Ukoliko se ne koristi legalna inačica sustava, postupak instalacije se prekida.
Zahtjevi na sklopovlje uključuju slijedeće stavke:

- PC računalo minimalne radne frekvencije 233 MHz, iako je za ugodno korištenje preporučeno računalo s procesorom Pentium III ili boljim,
- najmanje 64 Mb radne memorije, pri čemu je preporučljivo imati 128 Mb ili više i
- najmanje 20 Mb diskovnog prostora.

2.3. Instalacija

Prilikom instalacije alat nudi mogućnost pristupa Microsoft SpyNet zajednici. Radi se o zajednici programera tvrtke Microsoft koji se bave brzim rješavanjem problema vezanih uz neželjene programe. Ovaj korak moguće je i preskočiti te naknadno definirati. Nakon završetka instalacije alat preporuča pristup stranicama proizvođača kako bi osvježio popis definicija i eventualno se nadogradio na posljednju inačicu. U posljednjem koraku instalacije odabire se i učestalost cjelokupnog pregleda korisničkog računala u potrazi za neželjenim programima. Nakon ovog koraka alat neprimjetno nastavlja svoj rad u pozadini.



Slika 2: Provjera licenciranog operacijskog sustava

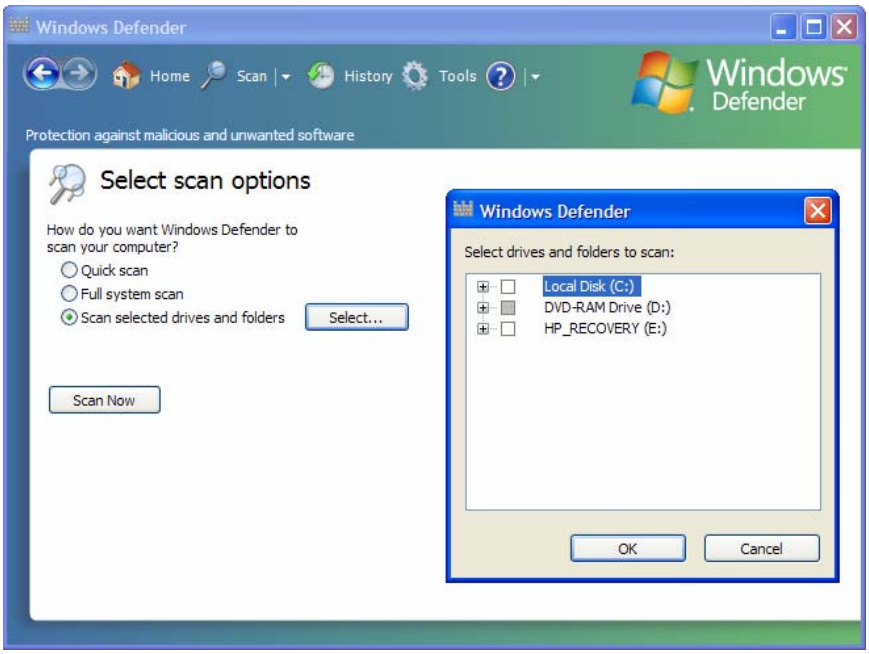
3. Funkcionalnosti alata

Nakon što se uspješno provede instalacija Windows Defender alata, moguće je koristiti se opcijama koje on nudi. Grafički prikaz vidljiv na zaslonu je sučelje prema servisu Windows Defender koji se postojano izvodi u pozadini. Servis se izvodi čak i kada na računalo nije prijavljen niti jedan korisnik. Korisničko sučelje se prikazuje samo za vrijeme osvježavanja popisa definicija i u slučaju pojave nekog problema u radu.

3.1. Izbornik za skeniranje sustava

Osnovna funkcionalnost alata je zaštita od neželjenih programskih paketa. Pritom je potrebno izdvojiti nekoliko važnijih mogućnosti:

- *Quick scan* (hrv. brzo skeniranje) – ovom opcijom se omogućava brz pregled sustava. Radnju je moguće rasporediti za automatsko pokretanje u određeno doba dana, čime se osiguravaju vitalni, a ujedno i najranjiviji dijelovi operacijskog sustava. Obnavljanje popisa definicija obavlja se u pozadini i obično se automatski izvrši prije pokretanja *Quick scan* opcije.
- *Full scan* (hrv. detaljno skeniranje) – ova opcija omogućava skeniranje cijelog računala u potrazi za neželjenim programima, ali se rjeđe pokreće jer traje bitno dulje od *Quick Scan* opcije. Sam proces traje oko 45 minuta na prosječnom računalu te ga se preporuča provoditi jednom tjedno.
- *Custom scan* (hrv. korisnički definirano skeniranje) – ova opcija omogućava preciznije postavljanje odrednica pregleda. Tu se, prije svega, misli na odabir korištene metode (*Quick Scan* ili *Full Scan*), vremena u kome će biti pokrenuta, diskovnih pogona koji će biti pregledani i sl.



Slika 3: Odabir pogona kod *Custom Scan* opcije

Zavisno o rezultatima provjere datoteka, Windows Defender prijavljuje sljedeće razine upozorenja za detektirane programe:

- *Severe* (hrv. ozbiljan) – ova oznaka označava da je program klasificiran kao vjerojatno zlonamjeran program (npr. računalni virusi ili crvi) te da ga je potrebno ukloniti.
- *High* (hrv. visok) – označava programe koji mogu skupljati osobne informacije korisnika te negativno utjecati na privatnost ili sigurnost računala (npr. kroz promjene u postavkama bez upozorenje ili odobrenja) pa ih se stoga preporuča ukloniti.
- *Medium* (hrv. srednji) – kao i prethodna razina označava programe koji mogu skupljati osobne informacije i kroz različite promjene postavki utjecati na sigurnost računala.
- *Low* (hrv. nizak) – označava potencijalno neželjene programe koji mogu skupljati osobne informacije o korisniku ili promijeniti način izvođenja računala, ali ti programi uglavnom rade u skladu s licenčnim uvjetima. Ti programi uglavnom nisu opasni, osim ako su instalirani bez znanja korisnika.
- *Not yet classified* (hrv. neklasificiran) – označava programe koji mogu biti opasni ako su instalirani bez znanja korisnika. U slučaju nepoznavanja programa preporuča se detaljnija analiza te eventualno uključenje u SpyNet zajednicu.

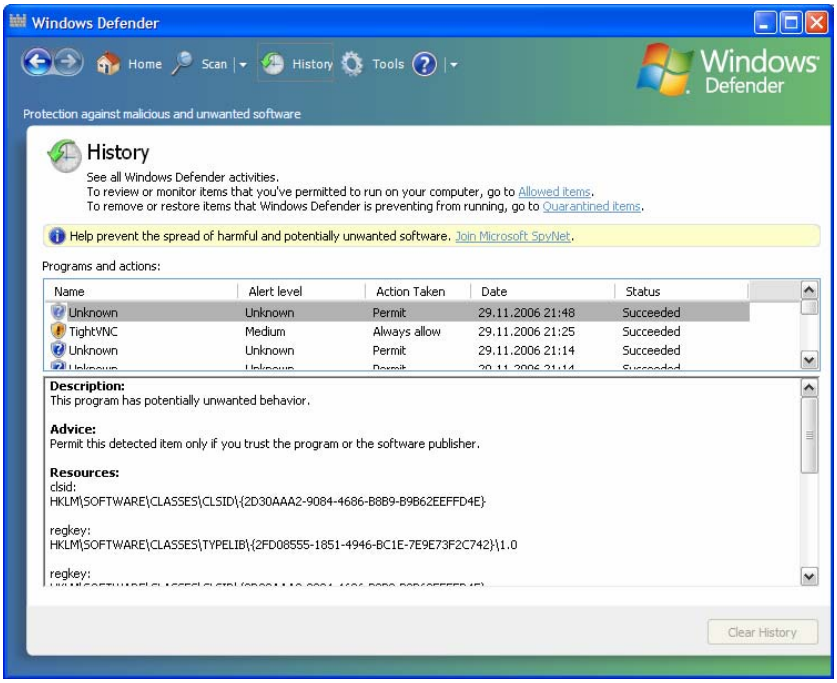
3.2. Izbornik za pregled starih aktivnosti (eng. *History*)

U ovoj opciji moguće je pregledavati aktivnosti koje su u prošlosti izvođene na računalu. Zapisi su klasificirani u više kategorija:

- *Allowed items* – pod ovom opcijom mogu se vidjeti sve stavke kojima je odobreno izvršavanje nakon upita Windows Defender alata.
- *Quarantined items* – pod ovom opcijom nabrojene su sve stavke koje alat ne prepoznaje ili nisu prošle korisničku intervenciju (da im se odobri ili zabrani izvršavanje).
- *Join Microsoft SpyNet* – pod ovom opcijom moguće je stavke koje alat ili korisnik ne prepoznaju proslijediti zajednici Microsoft SpyNet koja će odrediti pripadaju li u skupinu neželjene programske potpore.

Za svaku od stavki opisana je skupina kojoj pripada. Program tada prikazuje opis stavke: što je ona, kako se izvodi, i čemu služi (ukoliko se radi o programu). Time se kod korisnika smanjuje mogućnost pogrešne kategorizaciji stavke (npr. zabrane pokretanja Internet preglednika). Ukoliko je potrebno, prikazan je i savjet koji uključuje i kratku informaciju o tome što će se dogoditi ukoliko se dozvoli ili onemogući dotična stavka.

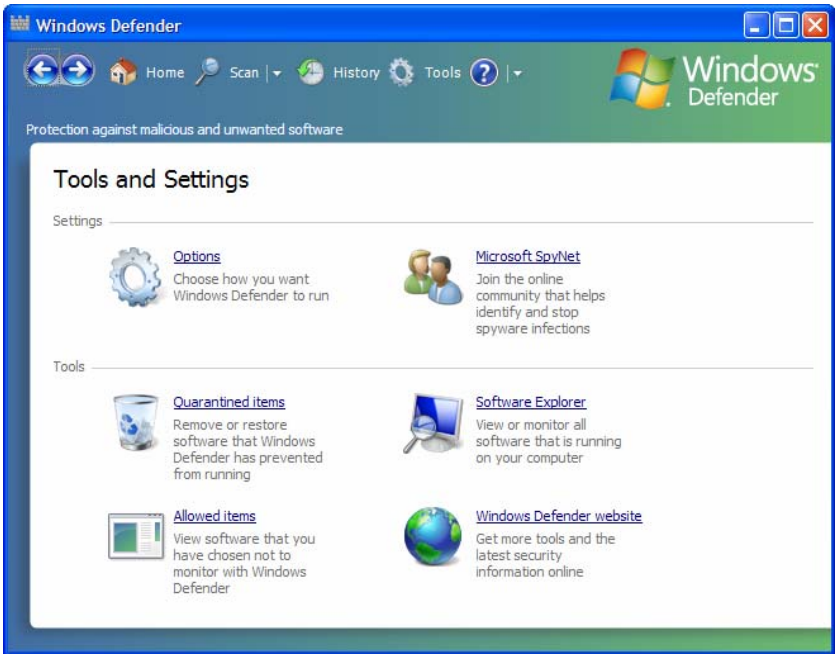
Osim toga, za svaku stavku prikazan je i odgovarajući ključ u Windows Registry-u, što upućenijim korisnicima omogućuje kontroliranje izvršavanja stavke tj. uključivanje i isključivanje njenih parametara. Sve stavke iz pregleda *History* moguće je izbrisati opcijom *„Clear history".*



Slika 4: Pregled dozvola nad pronađenim stavkama

3.3. Izbornik s raznim alatima i opcijama (eng. *Tools and Settings*)

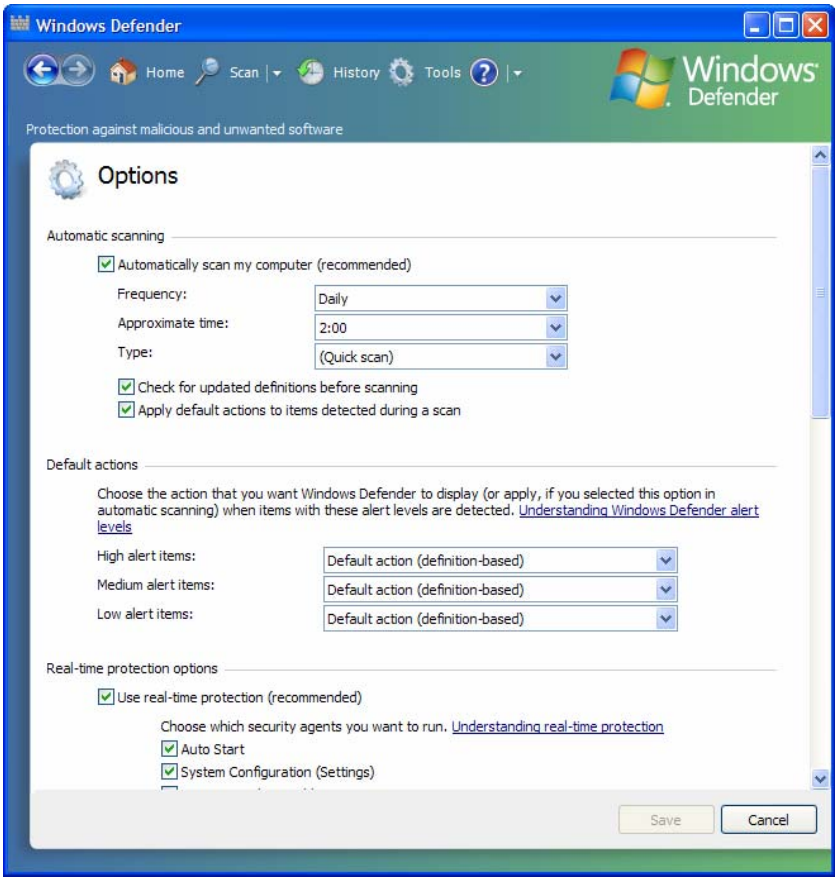
Pod ovim izbornikom prikazane su stavke koje omogućuju izmjenu postavki vezanih uz rad alata Windows Defender, ali i pokretanje dodatnih alata. Na sljedećoj slici prikazan je izgled osnovnog sučelja ovog izbornika.



Slika 5: *Tools and Settings* izbornik

3.3.1. Podizbornik *Options*

Otvaranjem podizbornika *Options* dolazi se do dijaloga koji omogućuje izmjenu postavki rada alata. Njime se može definirati učestalost pregleda pri čemu je moguće odabrati automatsko dnevno pokretanje ili pokretanje u određeni dan u tjednu, vrstu pregleda (*Quick scan* ili *Full system scan*) i vrijeme pokretanja, te da li će alat prije pokretanja pregleda ažurirati popis definicija. Ukoliko alat pronađe neželjeni program moguće je zadati i način na koji će se s njime postupati: želi li se staviti u karantenu ili odmah obrisati.



Slika 6: Sučelje *Options* podizbornika

Unutar izbornika *Options* moguće je definirati i zaštitu sustava u stvarnom vremenu (eng. *real time protection*). Taj oblik zaštite omogućava upozoravanje korisnika kad se određeni *spyware* program ili neki drugi neželjeni program pokuša instalirati ili pokrenuti na korisnikovom računalu. Korisnik za tako detektirane programe može odabrati neku od sljedećih akcija:

- *Ignore* (hrv. ignoriraj) – omogućava instalaciju programa, a ako program bude bio pokrenut tijekom narednog skeniranja ili ukoliko program pokuša promijeniti neke sigurnosne postavke na računalu, Windows Defender će generirati upozorenje vezano uz taj program.
- *Quarantine* (hrv. stavi u karantenu) – Windows Defender odabirom ove opcije stavlja program u karantenu, te onemogućava pokretanje detektiranog programa dok se programu to eksplicitno ne omogući ili dok se ne ukloni s računala.
- *Remove* (hrv. ukloni) – trajno uklanjanje programa s računala.
- *Always Allow* (hrv. uvijek dozvoli) – ovu opciju potrebno je odabrati samo u slučajevima kad je program provjereno nezlonamjeran, a ona omogućava da se program više ne detektira od strane Windows Defender alata.

Real time protection oblik zaštite upozorava i kad određeni programi pokušaju promijeniti važnije Windows sistemske postavke. S obzirom da u je u tom trenutku program već pokrenut na računalu, korisnik može odabrati jednu od sljedeće dvije opcije:

- *Permit* (hrv. dozvoli) – omogućava programu mijenjanje sigurnosno zavisnih sistemskih postavki na računalu.
- *Deny* (hrv. zabrani) – onemogućava programu mijenjanje sigurnosno zavisnih sistemskih postavki na računalu.

Iako je korisnicima omogućeno odabiranje pojedinih programa i postavki za nadziranje, preporučeno je odabiranje svih. U tu svrhu koriste se tzv. agenti koji obavljaju nadziranje u različitim uvjetima. Sljedeća tablica opisuje raspoložive agente.

Agent	Svrha
Auto Start	Nadzire listu programa kojima je dozvoljeno automatsko podizanje prilikom podizanja Windows operacijskog sustava. Korisniku je time omogućeno detektiranje i uklanjanje svih nepoželjnih programa koji se pokreću zajedno s podizanjem operacijskog sustava.
System Configuration (Settings)	Nadzire sigurnosno vezane postavke operacijskog sustava. Korištenjem ovog agenta omogućeno je detektiranje nepoželjnih programa koji mijenjaju programske ili sistemske postavke.
Internet Explorer Add-ons	Nadzire sve programe koji se pokreću zajedno s pokretanjem Internet Explorer preglednika, a koji mogu biti različiti *spyware* programi.
Internet Explorer Configurations (Settings)	Nadzire sigurnosne postavke Internet Explorer preglednika što predstavlja prvu crtu obrane od različitih neželjenih programa s Interneta koji mogu pokušati promijeniti te postavke bez odobrenja korisnika.
Internet Explorer Downloads	Nadzire datoteke i programe koji su namijenjeni radu s Internet Explorer preglednikom (npr. ActiveX) koje preglednik sam instalira i pokreće kako se ne bi u tim datotekama ugnijezdili i neželjeni programi.
Services and Drivers	Nadzire servise i upravljačke programe prilikom njihovih interakcija s Windows operacijskim sustavom i korisnikovim programima. U suprotnom, neželjeni programi mogu iskoristiti te servise i upravljačke programe, koji imaju pristup važnim programima, kako bi mogli pristupiti računalu te se skriveni izvršavati.
Application Execution	Nadzire sumnjive aktivnosti koje se događaju kod pokretanja programa. Naime, neželjeni programi mogu iskoristiti različite propuste u dozvoljenim programima te se npr. izvršavati paralelno s njima i sl.
Application Registration	Nadzire alate i datoteke na operacijskom sustavu kad su programi označeni da se mogu pokretati u bilo koje vrijeme, a ne samo prilikom pokretanja Windows sustava ili drugih programa. Ovaj oblik nadziranja je potreban iz razloga što neželjeni programi mogu podesiti svoje pokretanje bez obavijesti, npr. u točno određeno vrijeme.
Windows Add-ons	Nadzire pomoćne programe koji imaju svrhu da povećaju ili sigurnost, ili performanse, ili mogućnosti pregledavanja web stranica, itd. Nadziranje je potrebno jer takvi programi mogu samostalno instalirati druge nepoželjne programe.

Tablica 1: Pregled agenata i njihovih uloga u otkrivanja nepoželjnih programa

Uz navedene opcije unutar *Options* podizbornika, raspoložive se i opcije koje korisniku omogućavaju definiranje skeniranja nad arhiviranim datotekama i direktorijima u potrazi za skrivenim prijetnjama. Također, korisniku je omogućeno i definiranje korištenja heurističkih metoda u svrhu detektiranja potencijalno zlonamjernog programskog koda. Ukoliko je korisnik administrator tada on može

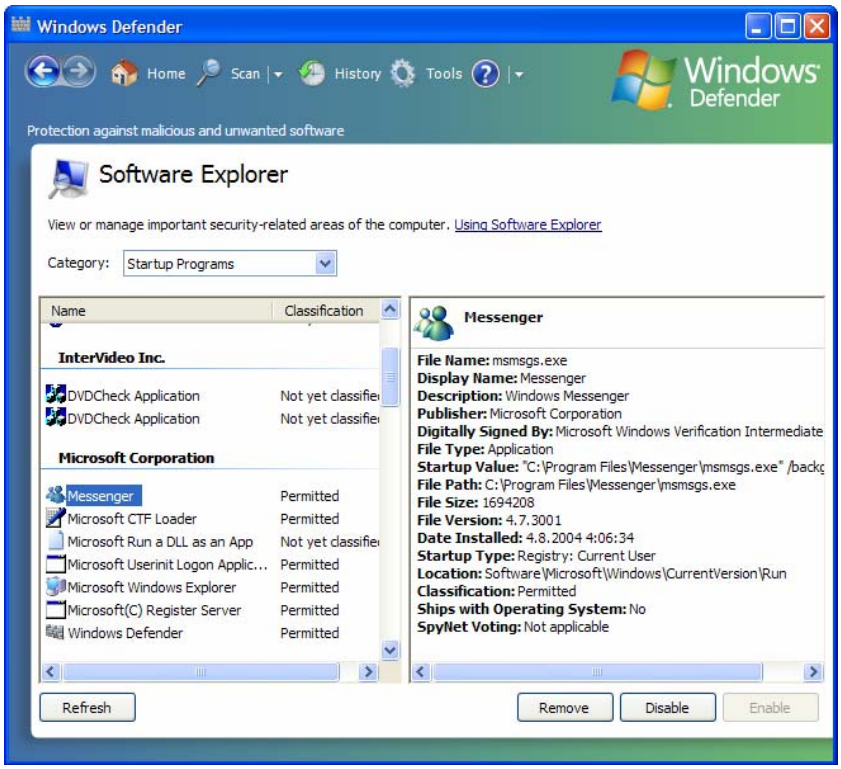
definirati da li i ostali korisnici, koji nemaju administratorske ovlasti, imaju pravo koristiti Windows Defender alat.

3.3.2. Podizbornik *Software Explorer*

Alat *Software Explorer* omogućava pregledavanje detaljnih informacija o programima koji se izvršavaju na računalu i koji mogu utjecati na privatnost i sigurnost računala. Programi koji se mogu nadzirati su sljedeći:

- programi koji se pokreću automatski prilikom podizanja Windows operacijskog sustava (eng. *Startup programs*),
- programi koji se u trenutku pregledavanja izvršavaju na računalu, bilo na grafičkom zaslonu ili kao pozadinski procesi (eng. *Currently running programs*),
- mrežno orijentirani programi koji se mogu spojiti na Internet ili neku drugu mrežu (eng. *Network-connected programs*), te
- *Winsock* davatelji usluga koji pružaju mrežne i komunikacijske usluge niže razine za Windows operacijski sustav te ostale programe koji se izvode na Windows sustavu, a uobičajeno imaju pristup važnim dijelovima operacijskog sustava (eng. *Winsock service providers*).

Nadziranim programima je moguće zabraniti pokretanje ili ih samo onemogućiti u pokretanju pri podizanju sustava. Programe koji su aktivni moguće je prekinuti u izvođenju, čime se smanjuje opterećenje računala.



Slika 7: Pregledavanje programa korištenjem *Software Explorer* izbornika

Informacije koje su vidljive za pojedini program, variraju od programa do programa. Programima se navode imena, nazivi proizvođača, opisi, lokacija s koje se pokreće, oznaka da li se program pokreće automatski, oznaka da li je program digitalno potpisan i sl.

3.3.3. Ostali podizbornici

Osim prethodno navedena dva podizbornika (*Options* i *Software Explorer*), u *Tools and Setting* izborniku postoje i drugi podizbornici:

- *Microsoft SpyNet* – nudi se mogućnost pristupa *on-line* zajednici koja rješava probleme neklasificiranih stavki,

- *Quarantined items* – prikaz programa koji se nalaze u karanteni,
- *Allowed items* – prikaz programa kojima je dozvoljeno izvođenje,
- *Windows Defender website* – link na web stranice Windows Defender alata.

3.4. Načini prepoznavanja zlonamjernih programa

U velikoj količini programa teško je zaključiti koji od njih uklanja ili modificira podatke bez korisnikovog znanja. Kako bi tome doskočio, Microsoft u suradnji s ostalim proizvođačima programske potpore dijeli svoja saznanja u otkrivanju i analizi zlonamjernih programa. U radu ta saznanja primjenjuje tako što korisnicima objašnjava što programski kod čini, a njima prepušta odluku o tome da li će mu omogućiti ili onemogućiti izvođenje.
Kako bi se neki program ocijenio potencijalno opasnim, potrebno ga je promotriti s više stajališta. Najvažnije je cilj s kojim se program pokreće. Ukoliko se to događa istovremeno s pokretanjem operativnog sustava, potrebno ga je razlikovati od npr. antivirusnog alata koji se također pokreće automatski sa sustavom. Jedina razlika među njima je mogućnost isključivanja automatskog pokretanja koja kod antivirusnog programa postoji, ali kod zlonamjernog programa nije dostupna. Vrlo je važno program procijeniti i prema osobi ili organizaciji koja ga je kreirala, ali je ipak najvažniji kriterij u ocjeni samo ponašanje programa. Ono može biti vrlo štetno ukoliko se, primjerice, radi o tzv. programskom crvu, ili manje opasno ukoliko se radi o iskočnom prozoru.
Postoji pet kriterija po kojima se procjenjuje stupanj nepoželjnosti programa:

- Varljivo ponašanje – program se izvršava na računalu bez korisnikovog znanja. Korisnika se sprečava u prekidu izvršavanja aktivnosti i nije mu dopušteno ukloniti program.
- Privatnost – prikupljaju se, koriste i dalje prosljeđuju određene informacije vezane uz korisnikovo ponašanje (npr. posjećena web odredišta) bez njegovog znanja.
- Sigurnost – pokušava se zaobići ili onemogućiti sve sigurnosne postavke na računalu sa ciljem ugrožavanja sigurnosti računala.
- Radna svojstva – umanjuju se radna svojstva računala usporavanjem izvršavanja ostalih programa.
- Primjena novih svojstava – prate se izvještaji korisnika i ostalih proizvođača programske potpore te se predviđaju novi oblici ponašanja zlonamjernih programa. Predviđeni oblici se primjenjuju u izgradnji zaštite.

4. Ostale značajke alata

Osnovni cilj pri razvoju alata Windows Defender bio je napraviti robustan sustav koji će, gledano sa strane korisnika, biti čim jednostavniji. Osim promjena u korisničkom sučelju i načina na koji se program izvodi, mnogo izmjena je učinjeno i u programskom kodu. Usporedi li se završna inačicu s početnom vidljiva su poboljšanja u vremenu pregleda što je posljedica primjene heurističke analitičke metode koju početna inačica nije podržavala. Alat također podržava razne vrste komprimiranih datoteka (npr. ZIP, RAR). Ovo je vrlo korisno jer se putem njih uobičajeno distribuiraju mnogi neželjeni programi. Windows Defender također radi u sprezi s Microsoftovim Internet preglednikom Internet Explorer (inačice 6 i 7). Pri tome pregledava preuzete datoteke i blokira web odredišta koja sadrže neželjen programski kod.

4.1. Podrška za Windows operativne sustave

Jedna od većih prednosti Windows Defender alata je podrška za nadolazeće 64-bitne operacijske sustave. Prva inačica alata je dostupna samo na engleskom jeziku, ali se tijekom 2007. predviđa i objava lokaliziranih inačica. Korisnici Windows Vista operacijskog sustava Windows Defender dobivaju kao njegov sastavni dio.

4.2. SpyNet zajednica

SpyNet zajednica je operativna podrška alatu Windows Defender. Ukoliko alat pronađe neklasificirani program tad njegov opis može proslijediti SpyNet zajednici koja ga klasificira kao neželjen, potencijalno opasan ili dozvoljen program. Sama klasifikacija određena je kao postotni iznos što znači

da je prikazan postotak korisnika koji su dozvolili pokretanje programa i korisnika koji to nisu učinili. Na temelju te informacije, korisnik određuje hoće li dozvoliti pokretanje programa na svom računalu.

4.3. Povratak na početno stanje (eng. *Rollback*)

Ovo je vrlo korisna mogućnost koja korisniku dozvoljava vraćanje računala u prethodno stanje, ukoliko je greškom zabranio pokretanje nekog programa. Tipičan primjer za to je program Real Player koji služi za pregled multimedijskih sadržaja. Alat Windows Defender blokira ga u izvođenju jer se koristi pristupom Internetu. Budući da pregled multimedijskih sadržaja poput zvuka i slike doista zahtijeva pristup Internetu, kako bi se osigurao pravilan rad programa, potrebno je poništiti postavljenu zabranu.

4.4. Efikasnost

Osnovna namjena alata je sprečavanje pokretanja neželjenih programa. Windows Defender može raditi u dva načina. Prvi način uključuje kontrolu cjelokupnog prometa prema Internetu. Ukoliko program sadrži opis neke stavke i prepozna ju kao potencijalno opasnu, tada se ona blokira. Osim programskog koda, alat može prepoznati i izmjenu *registry* ključeva. Sam proces je transparentan i ne ometa korisnika u radu. U ovom načinu rada, promjene su trenutne.

Drugi način rada je skeniranje sustava automatski ili na zahtjev. Ovdje je potrebno odgovarajuće vrijeme da računalo pregleda sustav (ovisno o vrsti skeniranja i broju odabranih mapa) što u praksi može biti između 15-tak minuta do više o sat vremena ukoliko se radi o potpunom skeniranju sustava.

Iz navedenih parametara vidi se da je Windows Defender efikasniji u blokiranju zlonamjernog koda nego u njegovom skeniranju što je uvjetovano načinom rada te se po tome ne razlikuje od konkurentskih proizvoda.

Ono što Windows Defender razlikuje od konkurencije je ugrađena podrška za SpyNet zajednicu. Budući da Windows Defender aktivno razmjenjuje podatke sa SpyNet zajednicom, očekuje se smanjenje broja pogrešno detektiranih neželjenih programa.

5. Zaključak

Sigurnost korištenja računala u mrežnom okruženju primarna je zadaća analiziranog alata. On pri tome mnogo pomaže jer od korisnika ne zahtijeva česte intervencije već se izvršava u pozadini i, samo ako je potrebno, korisnika obavijesti o utvrđenim nepravilnostima. Sam postupak je moguće potpuno automatizirati ukoliko se alat češće koristi i ukoliko se tokom tog korištenja stvori veća heuristička baza podataka.

Prednosti alata su besplatnost i dodatne funkcionalnosti, poput pregleda i nadzora nad stavkama koje se pokreću zajedno s računalom, stavkama koje se trenutno izvode, ali i stavkama koje zahtijevaju pristup Internetu. Jednostavno korisničko sučelje omogućava korisniku brzo upoznavanje s alatom i njegovim funkcionalnostima.

Iako alat ne posjeduje velik broj funkcionalnosti poput nekih kompleksnijih postojećih rješenja, za manje zahtjevne korisnike, Windows Defender može biti idealno rješenje.

6. Reference

[1] Microsoft Antispyware review, http://www.adwarereport.com/mt/archives/000091.html, prosinac 2006.

[2] Microsoft Windows Defender, http://reviews.cnet.com/Microsoft_Windows_Defender_beta_2/4505-3688-7-312566, prosinac 2006.

[3] Windows Defender Beta 2 vs. Spyware, http://blogs.zdnet.com/Spyware/?p=787, prosinac 2006.

[4] Paul Thurrot's Supersite for Windows: Windows Defender, http://winsupersite.com/reviews/windefender_beta2.asp, prosinac 2006.

[5] Methods used by Windows Defender to identify spyware http://www.microsoft.com/athome/security/spyware/software/msft/analysis.mspx, prosinac 2006.

[6] System requirements: Windows Defender http://www.microsoft.com/athome/security/spyware/software/about/sysreq.mspx, prosinac 2006.