Zaštita od virusa u Windows operacijskim sustavima

Kušer, Marina

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA

Stručni studij

ZAŠTITA OD VIRUSA U WINDOWS OPERACIJSKIM SUSTAVIMA

Završni rad

Marina Kušer

Osijek, 2016.

ETFOS
ELEKTROTEHNIČKI FAKULTET OSIJEK
Sveučilište Josipa Jurja Strossmayera u Osijeku

Obrazac Z1S: Obrazac za imenovanje Povjerenstva za obranu završnog rada na stručnom studiju

Osijek,

Odboru za završne i diplomske ispite

Imenovanje Povjerenstva za obranu završnog rada na stručnom studiju

Ime i prezime studenta:	**Marina Kušer**
Studij, smjer:	**Informatika**
Mat. br. studenta, godina upisa:	**0165060231, 2016.**
Mentor:	**Doc.dr.sc. Josip Balen**
Sumentor:	
Predsjednik Povjerenstva:	
Član Povjerenstva:	
Naslov završnog rada:	**Zaštita od virusa u Windows operacijskim sustavima**
Primarna znanstvena grana rada:	Programsko inženjerstvo
Sekundarna znanstvena grana (ili polje) rada:	
Zadatak završnog rada	U teorijskom dijelu rada potrebno je opisati vrste zlonamjernih programa u Windows operacijskim sustavima i metode zaštite od njih. U praktičnom dijelu rada potrebno je testirati različite programe za zaštitu te usporediti njihovu učinkovitost.
Prijedlog ocjene pismenog dijela ispita (završnog rada):	
Kratko obrazloženje ocjene prema Kriterijima za ocjenjivanje završnih i diplomskih radova:	**Primjena znanja stečenih na fakultetu:** **Postignuti rezultati u odnosu na složenost zadatka:** **Jasnoća pismenog izražavanja:** **Razina samostalnosti:**

Potpis sumentora:	**Potpis mentora:**

Dostaviti:

1. Studentska služba

U Osijeku, godine **Potpis predsjednika Odbora:**

Sveučilište Josipa Jurja Strossmayera u Osijeku

ELEKTROTEHNIČKI FAKULTET OSIJEK

IZJAVA O ORIGINALNOSTI RADA

Osijek,

Ime i prezime studenta:	Marina Kušer
Studij **:**	Informatika
Mat. br. studenta, godina upisa:	0165060231, 2013.

Ovom izjavom izjavljujem da je rad pod nazivom:
Zaštita od virusa u Windows operacijskim sustavima

izrađen pod vodstvom mentora

Doc.dr.sc. Josip Balen

i sumentora

moj vlastiti rad i prema mom najboljem znanju ne sadrži prethodno objavljene ili neobjavljene pisane materijale drugih osoba, osim onih koji su izričito priznati navođenjem literature i drugih izvora informacija.
Izjavljujem da je intelektualni sadržaj navedenog rada proizvod mog vlastitog rada, osim u onom dijelu za koji mi je bila potrebna pomoć mentora, sumentora i drugih osoba, a što je izričito navedeno u radu.

Potpis studenta:

Sadržaj

1. UVOD

U današnje vrijeme radni dan je nezamisliv bez korištenja računala. Korisnici su stručnjaci, pojedinci i tvrtke. Internetom se razmjenjuju velike količine podataka i u takvom okruženju rijetki su sustavi koji se ne susretnu sa nekim oblikom računalnog virusa.

Na isti način na koji virus naškodi ljudskom tijelu, tako i računalni virus može napraviti znatnu štetu na računalnim sustavima. Računalni virus je mali program koji se može širiti iz jednog računalnog sustava na drugi i uzrokovati smetnje s računalnim operacijama. On ima sposobnost da ošteti ili izbriše podatke na računalu. U najgorem slučaju može izbrisati sve podatke s tvrdog diska, no obično utječu na performanse i stabilnost računala. Potrebno je, primjerice otvoriti zaraženi privitak elektroničke pošte da bi virus zarazio računalo. Da bi spriječili pojavu virusa ili otkrili postoji li virus na računalu, potrebno je pokrenuti antivirusni program [1].

U ovom radu opisane su vrste računalnih virusa i njihove općenite karakteristike, te načini na koji se oni šire i kako djeluju. Iz poznavanja tih metoda razvijaju se tehnike obrane od virusa koje omogućavaju sigurni rad sustava. U praktičnom dijelu rada na računalo je namjerno postavljeno nekoliko virusa u različite mape i sa antivirusnim programima testirana je učinkovitost.

1.1. Zadatak završnog rada

Zadatak završnog rada je detaljno proučiti, opisati i usporediti računalne viruse. Potrebno je opisati kako se zaštiti od njih u Windows operacijskim sustavima (Windows 10). Nakon toga u praktičnom dijelu rada namjerno je postavljeno na računalo desetak virusa u različite mape. Zatim sa nekoliko antivirusnih programa pretraženo je računalo i testirana je učinkovitost testiranih programa te je to detaljno prodiskutirano.

2. OPIS RAČUNALNIH VIRUSA

Računalni virus je program koji može učiniti veliku štetu na računalu. On svojom reprodukcijom može zaraziti računalo jer ima sposobnost razmnožavanja, tj. bez znanja ili dopuštenja korisnika računala sami sebe kopiraju u disk [2]. Njihova uloga je da oštete računalo, uzrokuju nekontrolirane radnje na računalu te uništavanju i brišu podatke sa računala. Neki računalni virusi se odmah aktiviraju, dok drugi ostaju tajni nekoliko tjedana ili mjeseci ili se počnu polako aktivirati kako bi se izbjeglo aktiviranje.

U početku su se virusi širili preko disketa, no pojavom interneta on postaje idealan medij za prijenos virusa. Računalo se može zaraziti na dva načina: putem prijenosnih medija kao što su CD, DVD ili USB ili putem datoteka, koje su stigle uz elektroničku poštu i njihovom razmjenom putem interneta. Prvi potvrđeni računalni virus zvao se Elk Cloner iz 1982. godine. Nastao je kao šala te je bio vezan za računalo Apple II[1] i širio se na zaraženom disku. Na svoju pedesetu upotrebu, Elk Cloner virus bi se aktivirao, zarazio računalo te bi prikazivao kratku pjesmicu [2].

Fred Cohen je najpoznatiji kao osoba koja je definirala pojam „računalni virus“ i tehnike obrane od njih. Jedna od njegovih definicija glasi: „Računalni virus je program sposoban inficirati druge programe tako da ih modificira na način da sadrže eventualno evoluiranu kopiju tog virusa“ [3].

2.1. Osnovna podjela računalnih virusa

Internetom se razmjenjuju velike količine podataka i u takvom okruženju rijetki su sustavi koji se ne susretnu sa nekim oblikom zlonamjernog virusa. Kao što je i prije opisano, računalni virusi su programi koji se rekurzivno repliciraju i šire računalnim sustavima umetanjem vlastitih kopija koda u druge datoteke i ostale dijelove sustava. Neki od najpoznatijih računalnih virusa su: računalni crvi, trojanski konji, *spyware*, *adware*, pozivač, *rootkit* i lažna uzbuna [4].

2.1.1. Računalni crvi

Računalni crv (engl. *worms*) je program koji širi svoje funkcionalne kopije na druga računala putem mreže. Najčešći način širenja računalnog crva je putem elektroničke pošte. Postoje dvije vrste crva: crv na domaćinskom računalu i mrežni crv. Crv na domaćinskom računalu (engl. *host*

[1] Apple II – računalo koje je proizvodila američka tvrtka Apple između 1977. i 1993. godine te se njegovom pojavom kasnije stvara osobno računalo IBM PC ili PC koje je postalo standardno računalo

worm) za razmnožavanje na druga računala koristi mrežu te nakon što stvori kopiju, on uništava svoju prvobitnu verziju i postoji samo jedna kopija tog crva. Taj tip crva još se naziva i „zec“ jer stalno bježi mrežom. Mrežni crv (engl. *network worm*) se sastoji od više dijelova od kojih se svaki pokreće na različitom računalu u mreži i svaki dio obavlja različitu funkciju. On ima jedan glavni dio koji koordinira radom ostalih dijelova na mreži i zbog toga se naziva „hobotnicom“ [5].

2.1.2. Trojanski konji

Trojanski konj (engl. *Trojan horse*) je program koji se pretvara da izgleda bezopasno, ali najčešće ima neku skrivenu funkcionalnost. Ime mu dolazi iz grčke mitologije. Trojanski konj nije virus i za razliku od crva ne može sam sebe razmnožavati. Njega aktivira korisnik i na taj način izvršava naredbe korisnika, npr. brisanje podataka, širenje drugih virusa,krađa podataka itd.

Vrste trojanskih konja:

- Virus kapaljka (engl. *Dropper*) - program koji služi za instaliranje virusa na ciljani računalni sustav
- Stražnja vrata (engl. *Backdoor*) – program koji drugim osobama omogućava neovlašten pristup računalu bez znanja korisnika
- Preuzimač (engl. *Downloader*) – program koji kopira druge viruse s interneta i pokreće ih te time dolazi do zaraze računala virusom [6] [7].

2.1.3. Spyware/Adware

Spyware, odnosno špijunska programska podrška je program koji preuzima kontrolu rada na računalu bez znanja korisnika, šalju informacije o korisnikovom računalu na internet ili mijenja postavke internet preglednika. *Spyware*, kao i trojanski konj, ne može sam sebe razmnožavati. Dizajniran je da iskorištava zaražena računala za komercijalnu dobit. Zaraza sa takvim virusom se u većini slučaja događa pri posjeti ilegalnih stranica.

Adware, odnosno oglašivačka programska podrška je program koji automatski prikazuje ili preuzima oglase na računalo sa ili bez dozvole korisnika. Na internetu je postavljeno puno reklama i oglasa što navodi korisnika da kupi lažni program koji zapravo ne uklanja *spyware*, nego ga instalira na računalo. Oglašivačka programska podrška može biti klasificirana kao ostali oblici zlonamjernih programa. Može se predstavljati kao trojanski konj i kao neka korisna aplikacija te pritom prikazivati različite oglase [8].

2.1.4. Pozivač

Pozivač (engl. *dialer*) je program koji se instalira na računalo bez znanja korisnika i spada u spyware računalne viruse. Njegov cilj je da prekida postojeću korisnikovu vezu s internetom i da uz pomoć modema računala biranje telefonskog broja preusmjeri na broj koji je postavio pozivač sa skupim tarifama. Preuzimanjem ovih virusa najčešće je moguće posjećivanjem lažnih stranica [9].

2.1.5. Rootkit

Rootkit je općeniti naziv za skup programa koji omogućava pristup sa najvišim ovlastima. On prikriva svoje prisustvo na računalu šireći virus. Takvu vrstu programske podrške je teško pronaći i ukloniti sa računala te je najbolje rješenje reinstalacija Windowsa. Uspješan *rootkit* potencijalno može ostati na računalu godinama, ako je neotkriven. Sve to vrijeme će ukrasti informacije i resurse iz računala. *Rootkit* često sadrži i tzv. „stražnja vrata“, odnosno program koji drugim osobama omogućava ulaz u sustav bez njihova znanja [10].

2.1.6. Lažna uzbuna

Lažna uzbuna (engl. *hoax*) je elektronička pošta čiji je cilj lažno predstavljanje i dezinformacija primatelja. Najčešće predstavlja poruke koje navode korisnika da oda svoje povjerljive podatke ili da poduzme neku radnju bez opravdanog razloga [11]. Primjer lažne uzbune:

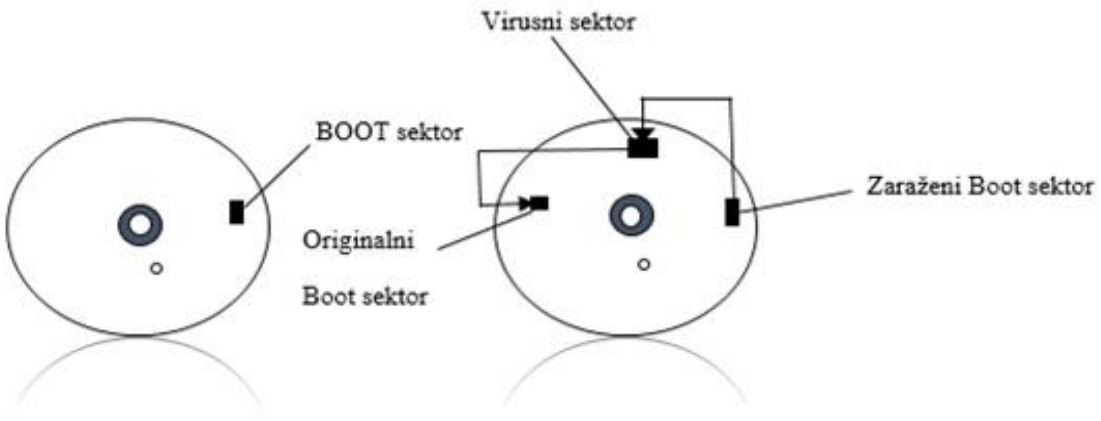
„Ovu poruku Vam šalje osnivač Microsofta želeći vas upozoriti: svijetom vreba novi virus (zove se Miaxao) koji briše 99% datoteka s diska te onesposobljuje antivirusne programe. Miaxao je podrijetlom iz Kine, autor mu je nepoznat, kao ni datum nastanka. Do sada je, prema novijim podacima, napao 38 milijuna računala u cijelom svijetu, i to uglavnom u Europi, SAD-u i Kanadi. Molimo Vas, proslijedite poruku svojim prijateljima i poznanicima koji vjerojatno ne znaju za virus“ [12].

2.2. Podjela virusa prema načinu funkcioniranja

Virusi se mogu podijeliti i prema načinu funkcioniranja na: viruse prvog sektora tvrdog diska, parazitske viruse, svestrane viruse, viruse pratioce, link viruse i makro viruse. Svaka vrsta ima određenu funkciju i služi određenoj svrsi.

2.2.1. Virusi prvog sektora tvrdog diska

Prvi sektor tvrdog diska (engl. *Boot sektor*) je područje na tvrdom disku, disketi ili na drugom uređaju za pohranu podataka koje je idealno za infekciju. Virus se širi tako da umetne svoj kod u prvi sektor tvrdog diska računala, obriše sadržaj tog sektora i umjesto programa za podizanje sustava snimi sebe. Zatim se virus aktivira, ako se podigne sustav sa zaraženog diska te učita u RAM memoriju. Od tog trenutka će zaraziti svaku disketu koja se bude koristila (Sl. 2.1). Jedan od prvih virusa, Elk Cloner, je bio takav virus [13].



Slika 2.1. *Virus prvog sektora tvrdog diska*

2.2.2. Parazitski virusi

Najčešća vrsta virusa su parazitski virusi. Parazitski virusi unose svoj kod u samu strukturu programa i tako se razmnožava. Oni općenito ne diraju cijelu datoteku nego se postavljaju na početku ili kraju virusa. Nakon što su programi i datoteke zaražene kodom parazitskih virusa, oni ostaju djelomično ili potpuno funkcionalni i tako se korisniku čini da je sve u redu. Datoteke koje mogu zaraziti su: *.com, .exe, .sys, .ovl* i druge [14].

2.2.3. Svestrani virusi

Svestrani virusi imaju mnogo funkcija kao što su krađa podataka ili napadanje prvog sektora tvrdog diska i izvršnih datoteka. Tako povećavaju mogućnost širenja. Ovi virusi su iznimno efikasni u širenju, poput virusa prvog sektora tvrdog diska [15].

2.2.4. Link virusi

Link virusi su jedni od najinfektivnijih vrsta virusa jer kad se jednom pokrenu, u trenu inficiraju napadnuti računalni sustav i mogu napraviti veliku štetu na disku. Kao i virusi pratioci, link virusi ne mijenjaju „napadnute“ programe nego pokazivač u strukturi direktorija. Ova izrazito infektivna vrsta virusa, na sreću, ima samo dva predstavnika i ukupno četiri varijante [15].

2.2.5. Makro virusi

Makro virusi su programi napisani u programskom jeziku nekog aplikacijskog programa i unutar njega se razmnožavaju. Najčešće su ugrađeni u dokumentima u programima za obradu teksta kao što su Word ili Excel. Imaju mogućnost da sami sebe kopiraju, brišu i mijenjaju dokumente. Makro virusi se mogu širiti kroz privitke elektroničke pošte, prijenosnih medija, mreža i interneta [15].

2.2.6. Virusi pratioci

Virusi pratioci su najjednostavniji oblici računalnih virusa. U istom direktoriju s istim imenom koriste prioritet tako da se *.com* datoteke uvijek izvršavaju prve. Virus pratilac pomoću *.exe* programa stvori *.com* datoteku i u nju ugradi svoj kod te će se umjesto originala izvršiti *.com* program sa virusnim kodom. Kada se to izvrši, kontrola se vraća na program s *.exe* ekstenzijom [16].

3. ZAŠTITA OD RAČUNALNIH VIRUSA

„Za zaštitu od računalnih virusa, potrebno je:

- Instalirati antivirusni program. Ako se instalira i redovito ažurira antivirusni program, zaštitit će računalo od virusa. Antivirusni programi pregledavaju računalo i traže viruse koji pokušavaju zaraziti poruke elektroničke pošte, operacijski sustav ili datoteke. Svakog se dana pojavljuju novi virusi, stoga je potrebno redovito provjeravanje ima li novih ažuriranja.
- Ne otvarati poruke elektroničke pošte od nepoznatih pošiljatelja. Mnogi se virusi nalaze u privitku poruka elektroničke pošte i počet će se širiti čim se otvori privitak poruke elektroničke pošte.
- Koristiti blokator skočnih prozora na pregledniku. Skočni prozori mali su prozori preglednika koji se pojavljuju na vrhu internetske stranice. Iako većinu tih prozora stvaraju oglašivači, oni mogu sadržavati zlonamjerni ili nesigurni kod. Blokator skočnih prozora može spriječiti pojavu nekih ili svih takvih prozora.
- Održavati Windows ažurnim. Microsoft povremeno izdaje posebna sigurnosna ažuriranja koja olakšavaju zaštitu računala. Ta ažuriranja pomažu spriječiti viruse i ostale napade na računalo zatvaranjem mogućih sigurnosnih rupa. Sustav Windows mora imati uključeno automatsko ažuriranje sustava Windows da bi primao ta ažuriranja.
- Koristiti vatrozid. Vatrozid za Windows ili bilo koji drugi vatrozid obavijestit će korisnika ako na računalu dođe do sumnjivih aktivnosti ili ako se virus pokuša povezati s računalom. Vatrozid također može spriječiti viruse i hakere da na računalo preuzmu potencijalno štetne programe.
- Koristiti postavke privatnosti u pregledniku. Internetska mjesta mogu koristiti privatne podatke korisnika jer ćete time lakše spriječiti ciljano oglašavanje, prijevaru i krađu identiteta.
- Očistiti internetsku predmemoriju i povijest pregledavanja. Većina preglednika pohranjuje podatke o internetskim mjestima koja se posjeti te podatke koje ta internetska mjesta mogu zatražiti. Pohrana tih detalja na računalu može biti korisna, no ponekad će biti potrebno izbrisati neke ili sve podatke“ [17].

3.1. Opis antivirusnih programa

Općenito, da bi se zaštitilo od računalnih virusa, na računalo se treba instalirati antivirusni program. Antivirusni program je računalna programska podrška koji se koristi kao zaštita i uklanjanje računalnih virusa. Korištenjem antivirusnog programa podrazumijeva se da će se dobivati upozorenja i obavijesti o novim virusima koji prijete računalu. Ako antivirusni program pronađe virus, on ga šalje u „izolaciju“ ili ga potpuno izbriše prije nego što učini štetu računalu ili datotekama. Zaštita od virusa bi trebala biti aktivna i iznimno je važna redovita nadogradnja. Kada bi danas svako računalo imalo neki antivirusni program, računalni svijet i internet bi bili mnogo sigurnije mjesto [18].

Danas na tržištu postoji mnogo antivirusnih programa i teško je odabrati najbolje rješenje. Neki od najboljih antivirusnih programa za 2016. godinu su: Bitdefender Antivirus Plus, Avast Antivirus, AVG Antivirus, Avira Antivirus Pro, Panda Antivirus Pro (Tab. 3.1).

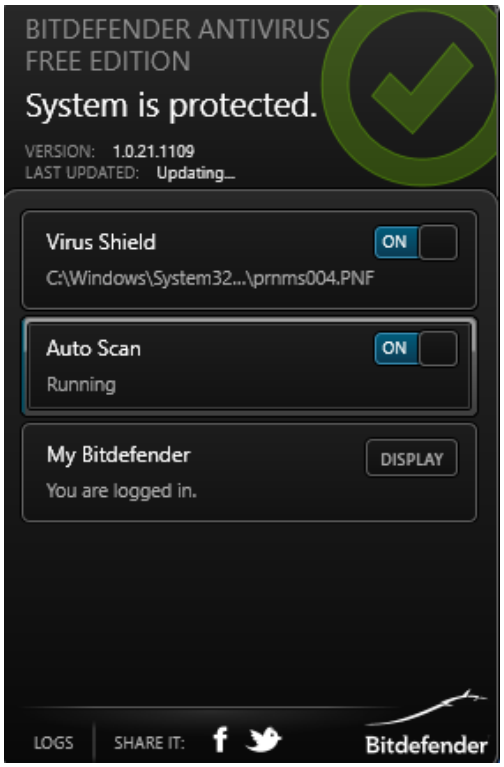
Tablica 3.1. *Usporedba najboljih antivirusnih programa za 2016. godinu [19] [20]*

	Ocjena	Windows 10	Skeniranje za el. poštu	USB skeniranje	Lako korištenje	Zaštita
Bitdefender Antivirus Plus	99,8%	DA	DA	DA	DA	100%
Kaspersky Anti-Virus	93,2%	DA	DA	NE	DA	92%
McAfee AntiVirus Plus	92,8%	DA	DA	DA	DA	100%
Norton Security	90,5%	DA	DA	DA	NE	100%
Avast Antivirus	90,0%	DA	DA	DA	DA	100%
Avira Antivirus Pro	88,2%	DA	DA	NE	NE	100%
AVG Antivirus	87,7%	DA	DA	NE	DA	100%
ESET Antivirus	85,5%	DA	DA	DA	DA	100%
Panda Antivirus Pro	84,5%	DA	NE	NE	NE	95%
F-Secure Anti-Virus	83,2%	DA	DA	NE	DA	98%

3.1.1. Bitdefender Antivirus Free Edition

Bitdefender pruža najbolje performanse i brzinu računala. Funkcionalan je kao programska podrška za otkrivanje i uklanjanje zlonamjernih programa. Ima funkciju koja automatski ažurira antivirusnu bazu podataka kako bi osigurao stabilan i učinkovit rad. Njegove glavne značajke su:

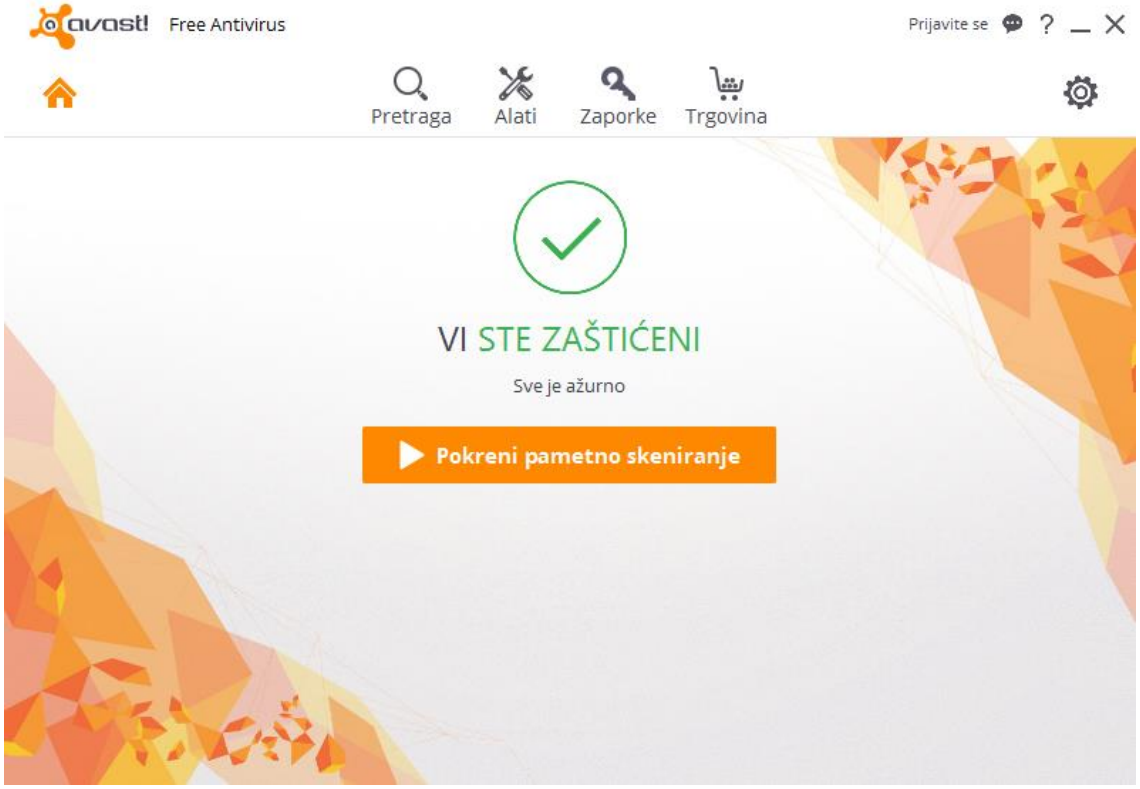
- Otkrivanje spyware modula
- Zaštita od neželjene pošte i blokiranje neželjenih sadržaja
- Daljinski upravljač [21].



Slika 3.1. *Prikaz ekrana Bitdefender Antivirusa*

3.1.2. Avast Free Antivirus

Avast Free Antivirus jedan je od najpouzdanijih i najčešće korištenog besplatnog antivirusnog programa u svijetu koji nudi visok nivo zaštite od virusa već u besplatnoj inačici. Jako je učinkovit jer se stalno ažurira i zaustavlja prijetnje u realnom vremenu te se lako koristi. On nudi zaštitu datoteke, internetsku zaštitu i zaštitu elektroničke pošte. Pruža brzu zaštitu u odnosu na ostale antivirusne programe te nudi zaštitu i za internetske preglednike. Instalacija programa je jednostavna i brza. Na slici 3.2. je početni ekran koji pokazuje da li je računalo zaštićeno [21].



Slika 3.2. *Prikaz ekrana Avast Free Antivirusa*

3.1.3. AVG Free Antivirus

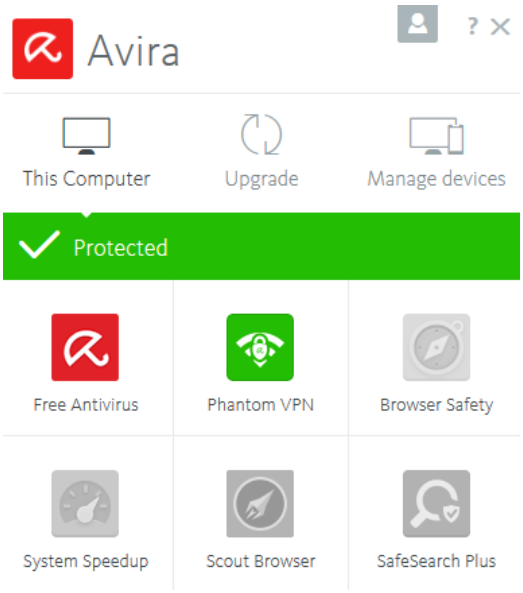
AVG Free Antivirus je jedan od najpopularnijih antivirusnih programa. Ovaj osnovni paket će zaštititi računalo od virusa, računalnih crva, trojanaca i ostalih zlonamjernih programa prilikom pregledavanja interneta ili provjere elektroničke pošte. Sadrži komponente koje omogućuju korisniku siguran boravak na internetu. AVG posjeduje sigurnosni sustav koji provjerava stranice koje se posjećuju te ako pronađe stranicu koja je označena kao opasna i zlonamjerna, na to upozorava korisnika. Jednostavan je za korištenje i njegov rad ne usporava računalo. Njegove glavne značajke su:

- Zaštita sustava od različitih vrsta virusa
- Provjera prometa za prijetnje
- Poboljšanje performansi sustava
- Filtriranje neželjene pošte [21].

Slika 3.3. *Prikaz ekrana AVG Free Antivirusa*

3.1.4. Avira Free Antivirus

Avira Free Antivirus je antivirusni program koji štiti računalo od virusa i ostalih zlonamjernih programa. Sustav omogućuje pronalaženje i uklanjanje virusa ili blokiranje oglasa. Njegova instalacija je vrlo jednostavna i lagana te za razliku od konkurencije ne zahtjeva da se uklone konkurentske antivirusne aplikacije. Osim računalnih crva i trojanskih konja, ovaj besplatni program štiti računalo i od *spyware* i *adware* virusa [21].

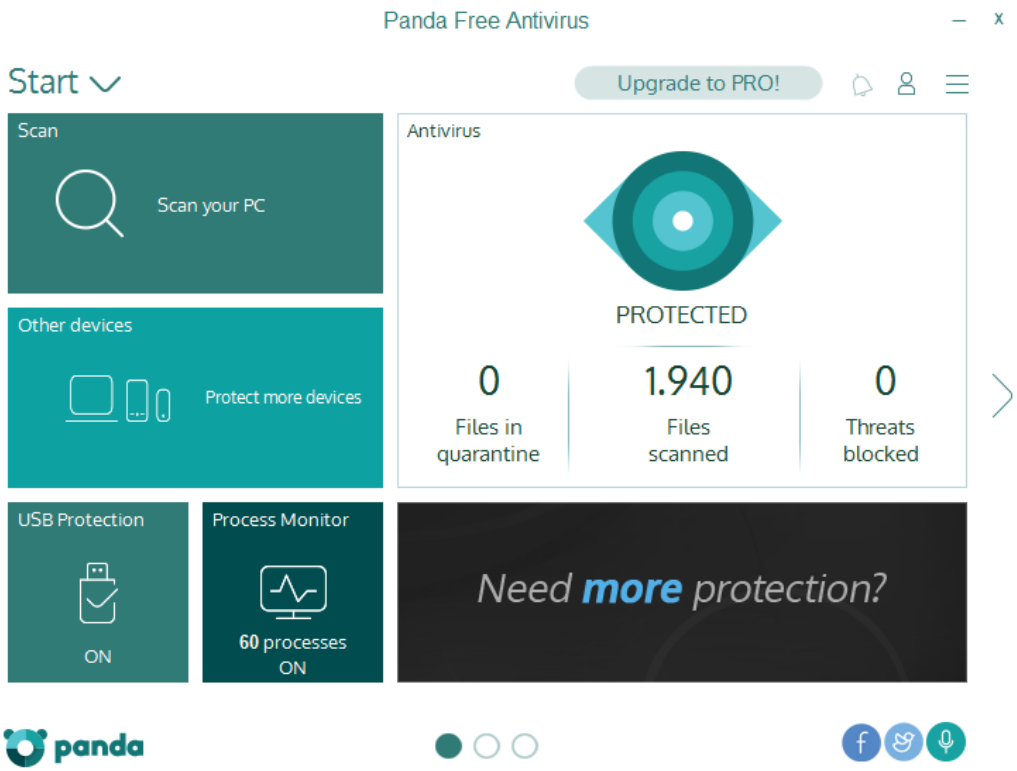


Slika 3.4. *Prikaz ekrana Avira Free Antivirusa*

3.1.5. Panda Free Antivirus

Panda Free Antivirus je lagan za korištenje te pruža brzu i efikasnu zaštitu od zlonamjernih programa. Njegove glavne značajke su:

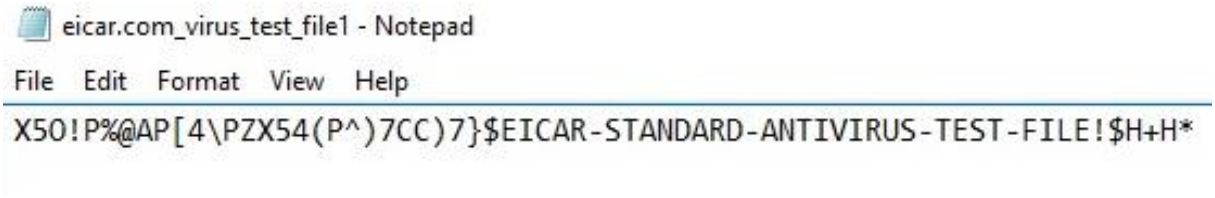
- Zaštita od različitih prijetnji
- Sposobnost da se ograniči pristup djeci na različite internetske stranice
- Skeniranje podataka
- Mogućnost udaljenog pristupa [21].



Slika 3.5. *Prikaz ekrana Panda Free Antivirusa*

4. EKSPERIMENTLNO TESTIRANJE ANTIVIRUSNE ZAŠTITE

Za eksperimentalno testiranje antivirusne zaštite preuzeta je „zlonamjerna“ EICAR datoteka [22]. EICAR datoteka je razvijena od strane organizacije koja se bavi računalnim antivirusnim istraživanjima i zaštitom informatičkih tehnologija (Sl. 4.1). Ona omogućuje testiranje antivirusne zaštite bez potrebe korištenja pravog računalnog virusa koji bi mogao napraviti veliku štetu na računalu. Antivirusni program pri skeniranju odgovoriti će na isti način kao da je pronašao štetni virus [23].



Slika 4.1. *EICAR test datoteka*

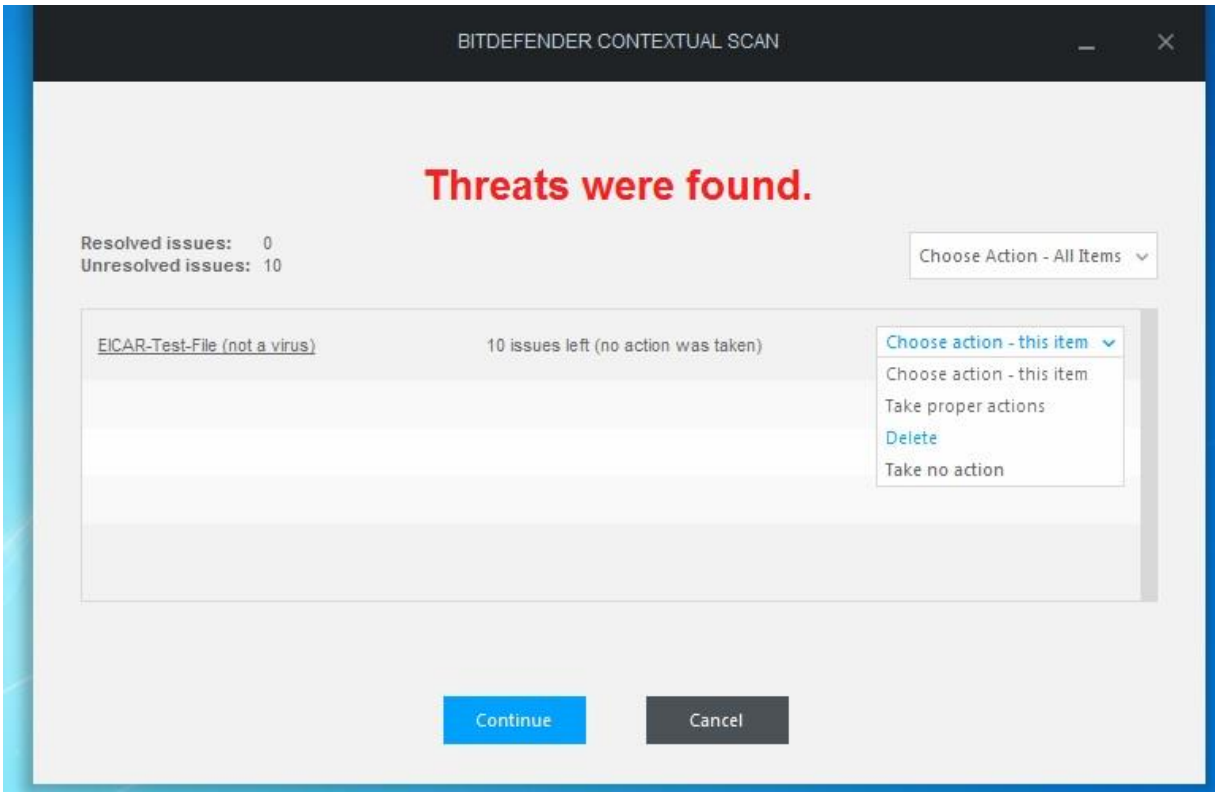
4.1. Eksperimentalne postavke

U sklopu završnog rada korišteno je računalo s operacijskim sustavom Windows 10 koji uključuje dvojezgreni procesor Intel Core i3 frekvencije 1.90 GHz te 64-bitnu arhitekturu sa ugrađenih 4 GB fizičke radne memorije. Tvrdi disk je kapaciteta 500 GB. Testiranje je izvršeno tako da je instaliran antivirusni pogram. Zatim je kreirano virtualno okruženje sa mapama i podmapama u koje su se umnožile i rasporedile testne zlonamjerne datoteke. U svaku od pet podmapa stavljene su dvije testne zlonamjerne datoteke. Nakon toga je pokrenuto skeniranje kreiranih mapa i podmapa sa svakom od pet navedenih antivirusnih programa.

4.2. Bitdefender Antivirus Free Edition

Bitdefender je antivirusna zaštita sa mnogim opcijama koje su instalirane u sam program, a to su mogućnost čišćenja privremene memorije računala, internetskih preglednika i njegove povijesti te uređivanje registra operacijskog sustava. Također u svojim alatima nudi puno opcija podrške za korisnikovo računalo, ali jednako opterećuje sustav kao i ostale manje antivirusne zaštite sa manje alata i mogućnosti. Program ima vrlo pregledno sučelje kroz koje se može nadzirati računalo.

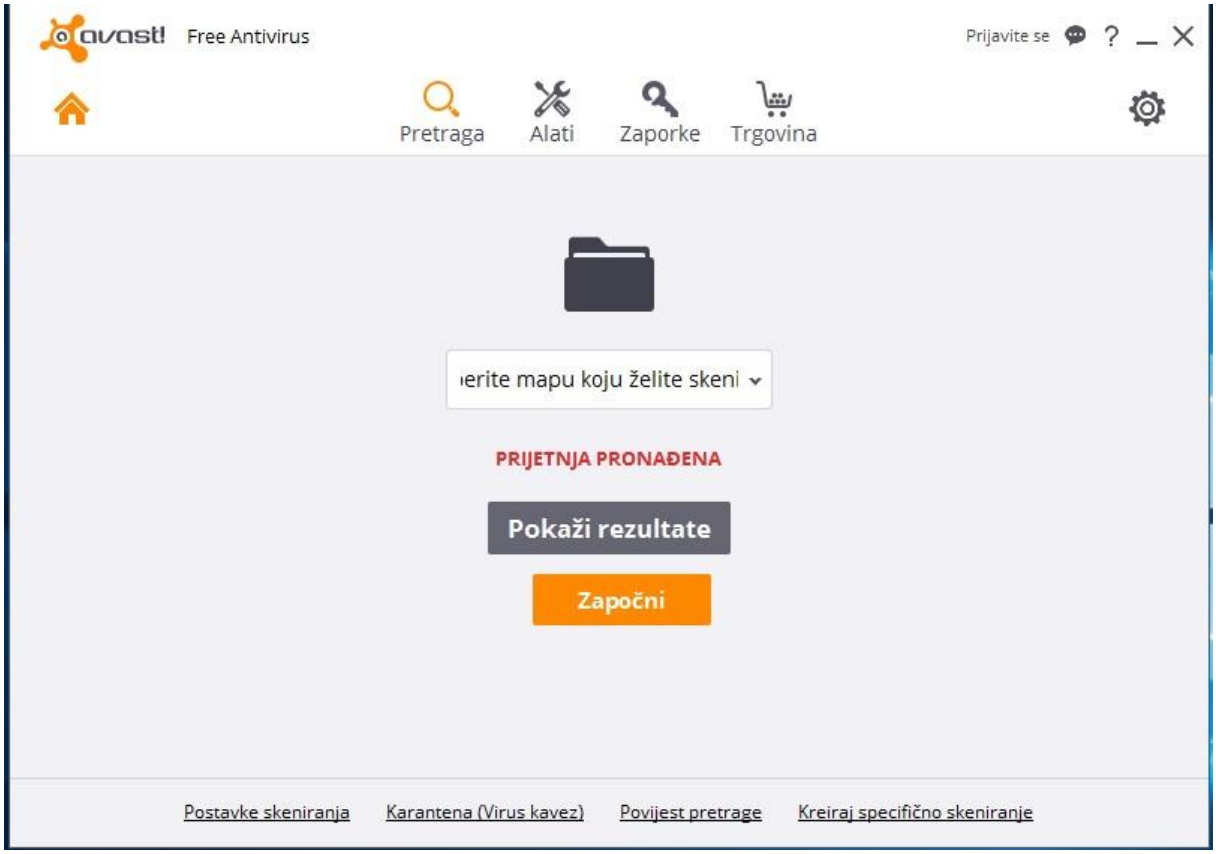
Nakon selektiranja zlonamjenih datoteka, Bitdefender je odmah našao sve zaražene datoteke. Ponudio je par opcija, koje su: brisanje datoteka, ne radi ništa i prepusti Bitdefenderu da napravi potrebne korake. Nakon toga su virusi svi obrisani sa računala (Sl. 4.2).



Slika 4.2. *Bitdefender je pronašao prijetnju*

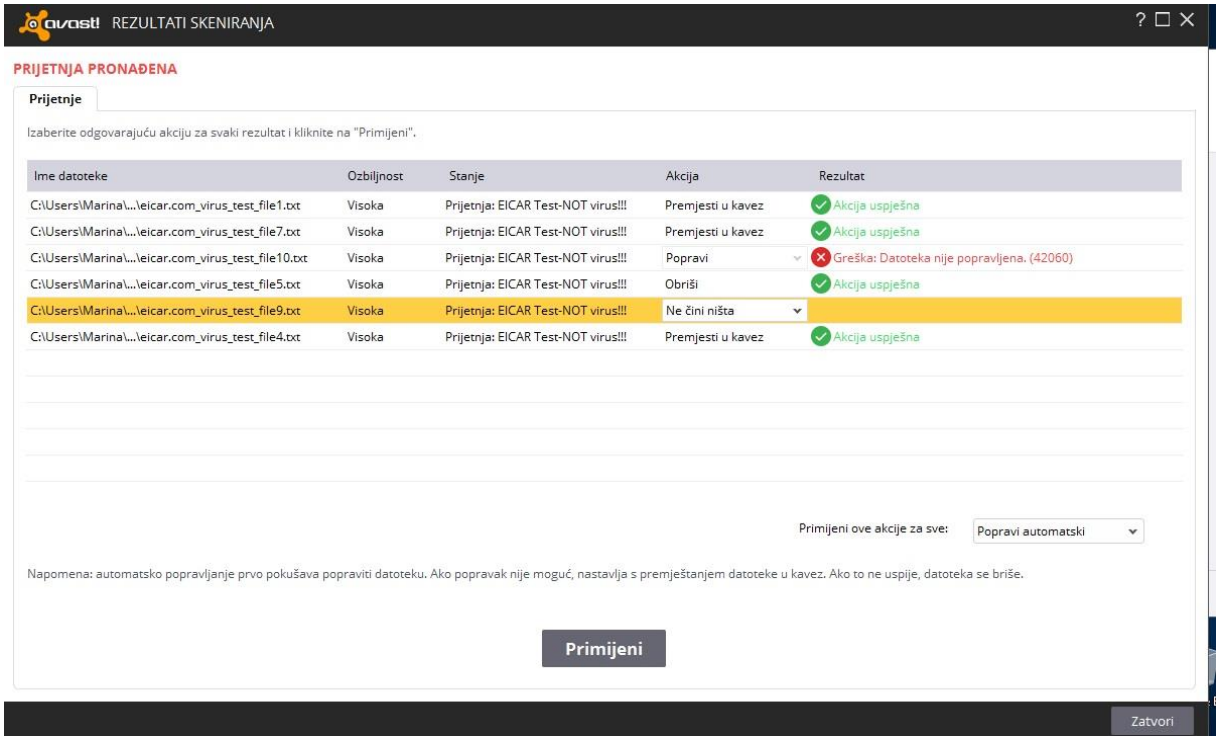
4.3. Avast Free Antivirus

Njegova instalacija je vrlo jednostavna, kao i kod AVG Free Antivirusa. Avast u svom izoliranom virtualnom okruženju pokreće sumnjivu datoteka i gleda njezino ponašanje i onda zaključuje da li je ta datoteka sigurna ili nije. AVG ima i inteligentni skener koji omogućuje proces skeniranja u kratkom roku, a pritom ne utječe na razinu zaštite i sigurnosti. Ako su datoteke sigurne, one ostaju zapamćene i ne skeniraju se ponovno te to znatno doprinosi brzini rada Avast antivirusnog programa. Besplatna verzija Avast antivirusa je slična verziji koja se naplaćuje. Nakon pokretanja antivirusne zaštite i ručne pretrage, potrebno je skenirati samo direktorije u kojima se nalaze testne zlonamjerne datoteke. Avast antivirusna zaštita je odmah pronašla prijetnju (Sl. 4.3).



Slika 4.3. *Avast antivirusna zaštita je pronašla prijetnju*

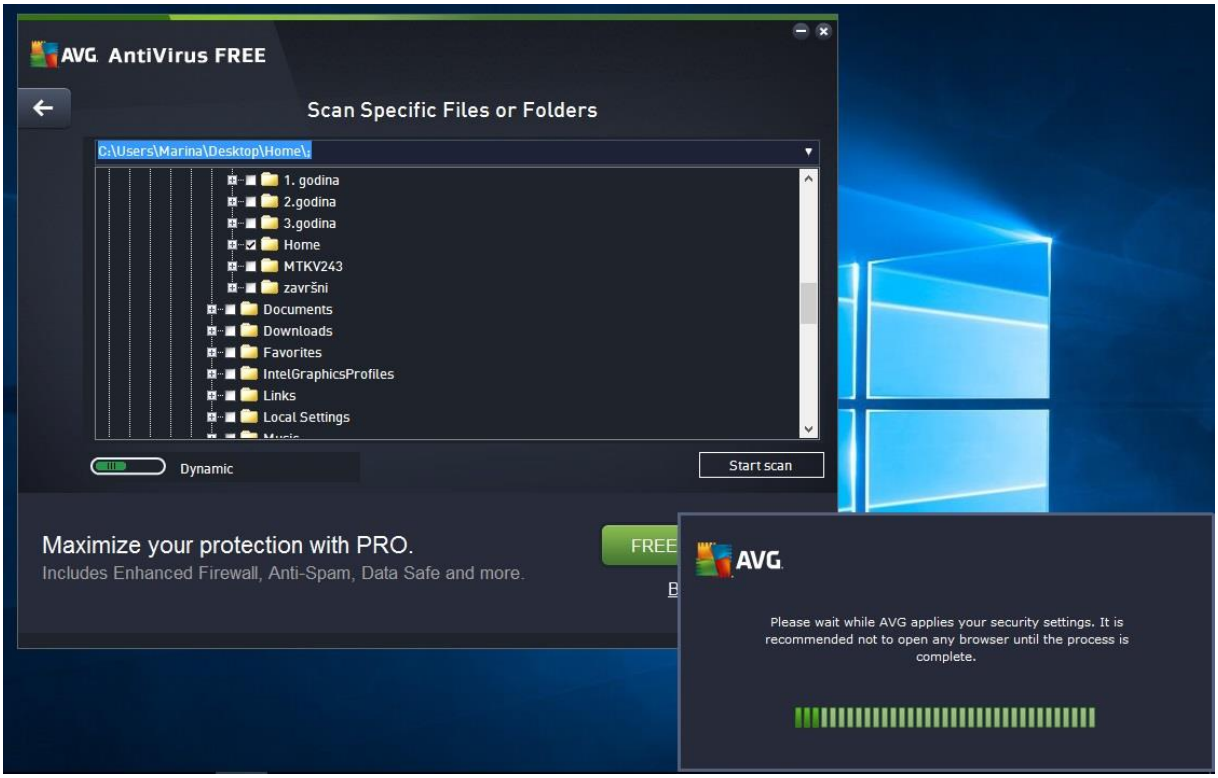
Našao je svih 10 kreiranih prijetnji te su ponuđene sljedeće opcije: popraviti automatski (program će sam pokušati pronaći rješenje problema), premjesti u kavez (program će spremiti zaražene datoteke u kavez i onemogućit će njihovo daljnje djelovanje i širenje), popravi te opcija obriši i ne čini ništa. Avast antivirusna zaštita daje mogućnost selektiranja jednog ili više virusnih testnih datoteka i dozvoljava da se za svakoga zasebno primjenjuje jedna od navedenih opcija sankcioniranja testne datoteke. Na slici 4.4. se vidi primjer otklanjanja zaraženih datoteka sa navedenim opcijama. Opcija popravi automatski i ne čini ništa jedino nisu primijenjene. Popravi automatski potrebno je dva puta pokrenuti da bi se izbrisala zaražena datoteka.



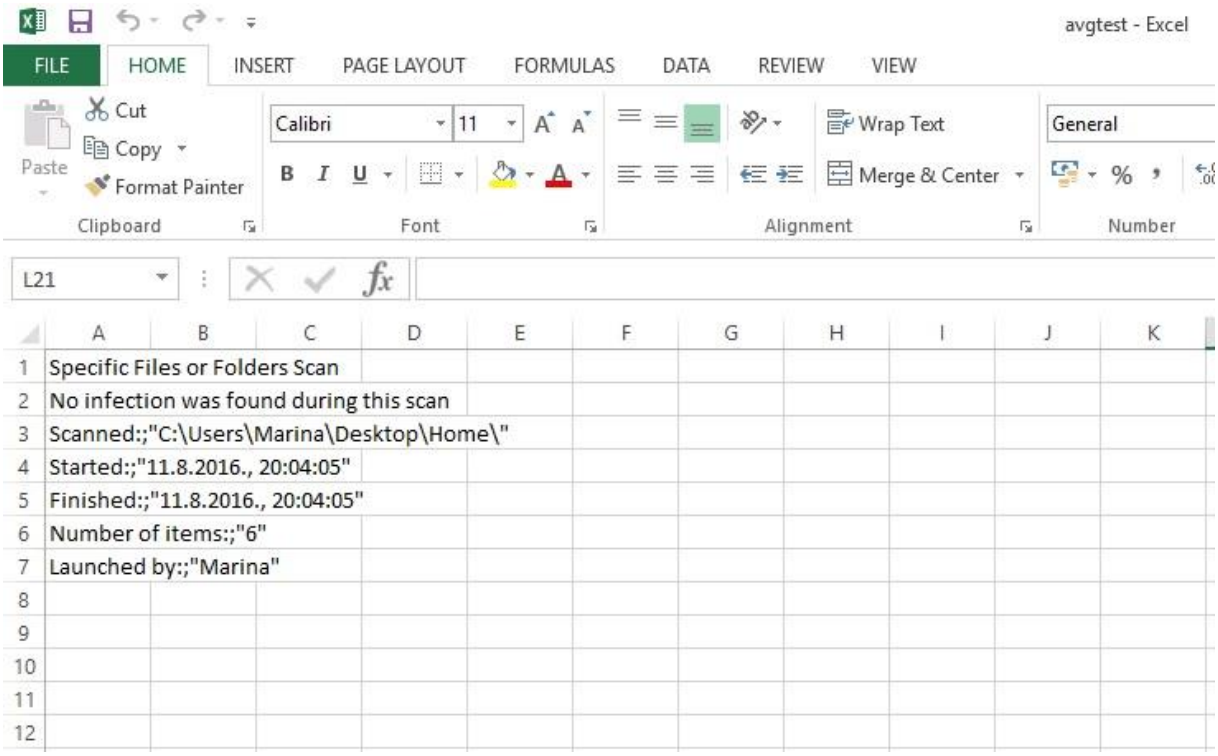
Slika 4.4. *Primjer otklanjanja zaraženih datoteka u Avast antivirusnom programu*

4.4. AVG Free Antivirus

Prilikom instalacije AVG antivirusne zaštite izabrana je besplatna zaštita koja je skromnija sa opcijama od verzije koja se naplaćuje, no za ovo testiranje besplatna verzija ispunjava uvjete koji su potrebni. Nakon završetka instalacije AVG je automatski počeo nadogradnju te se sam nadogradio na najnoviju verziju, tj. inačicu. Zatim su skenirani samo kreirani direktoriji sa zlonamjernim datotekama (Sl. 4.5). AVG je prilikom odabira direktorija za skeniranje ponudio dinamičnu, standardnu, srednju i brzu opciju skeniranja. Razlike u tim opcijama su u omjeru kvaliteta i brzine skeniranja računala. Brže je površno, a detaljnije je kvalitetnije i sporije skeniranje. Za ovo testiranje je odabrana srednja opcija. Antivirusna zaštita nije pronašla zarazu te je ponudila ispisivanje rezultata u *.csv* formatu gdje su dobiveni detaljniji rezultati skeniranja. U ovom slučaju nije pronašlo ništa kao što se može iščitati iz izlaznog podatka (Sl. 4.6).



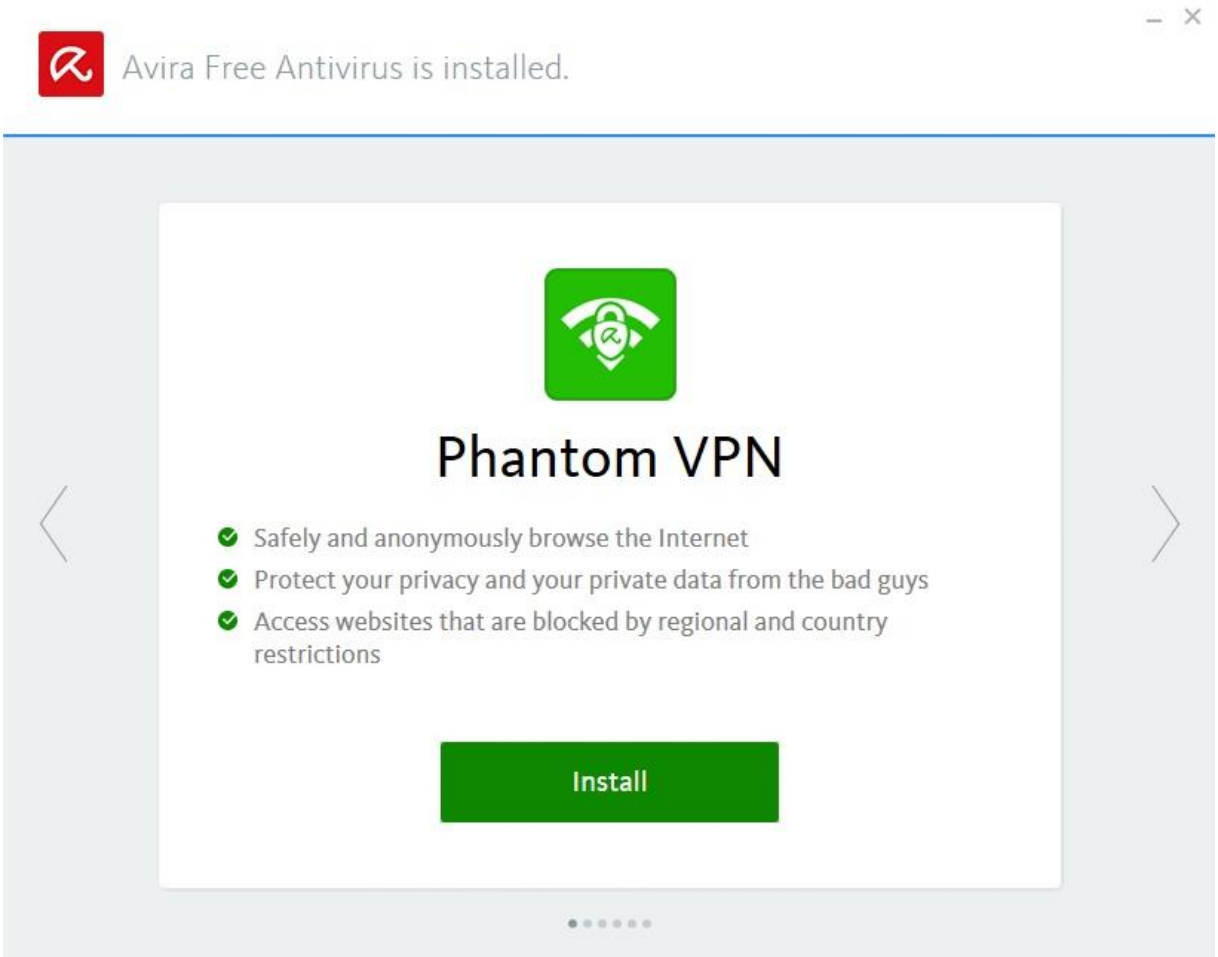
Slika 4.5. *Odabir direktorija prije skeniranja u AVG antivirusnom programu*



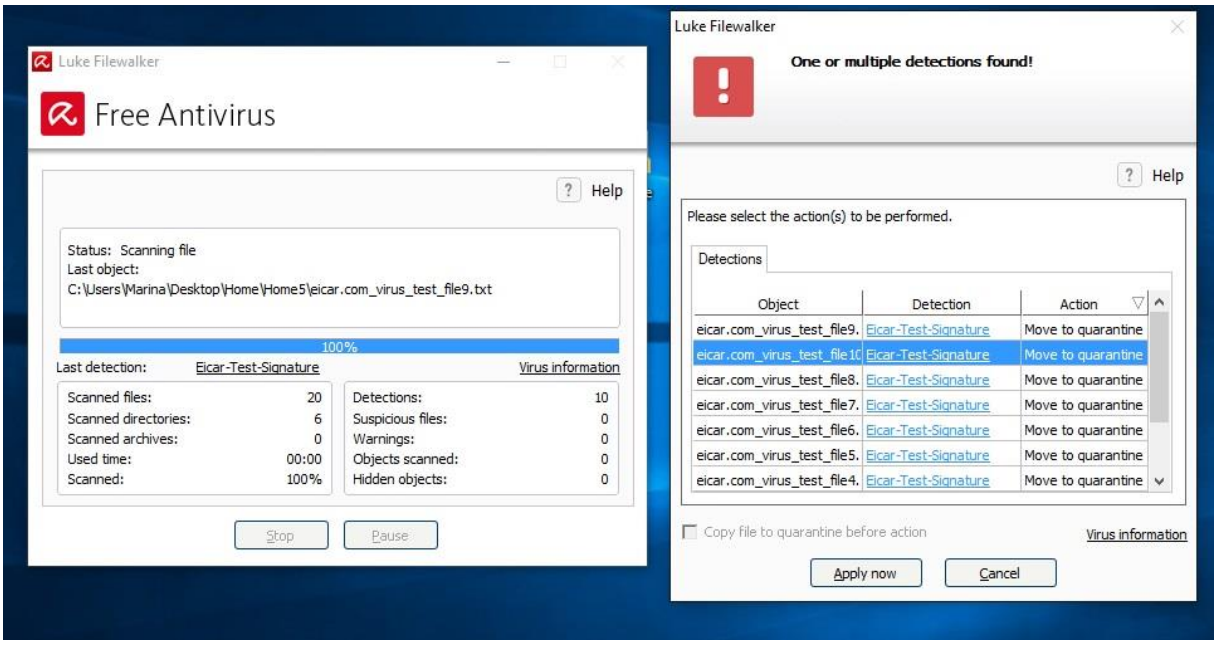
Slika 4.6. *Rezultat testiranja AVG antivirusne zaštite*

4.5. Avira Free Antivirus

Avira antivirusna zaštita prilikom instalacije ponudila je još dodatke poput Phantom VPN koji omogućava anonimno pretraživanje internetom te može zaštititi računalo u određenim situacijama (Sl. 4.7). Drugi dodatak je Avira System Speedup koji poboljšava brzinu računala i njegove performanse te oslobađava prostor i popravlja disk. Nakon pokretanja antivirusne zaštite desnim klikom na direktorij u kojem se nalaze zaražene datoteke pokrenuto je skeniranje tog direktorija. Avira je prepoznala sve zaražene datoteke i standardno ponudila opciju prebacivanja zaraženih datoteka u kavez, kao što je ponudio i Avast (Sl. 4.8). Ostavila je opcije poput ignoriraj, pobriši i preimenuj zaražene datoteke. Opcije pobriši i prebaci u kavez su najdjelotvornije opcije u otklanjanju zaraženih datoteka.



Slika 4.7. *Dodatak Phantom VPN u Avira antivirusnom programu*

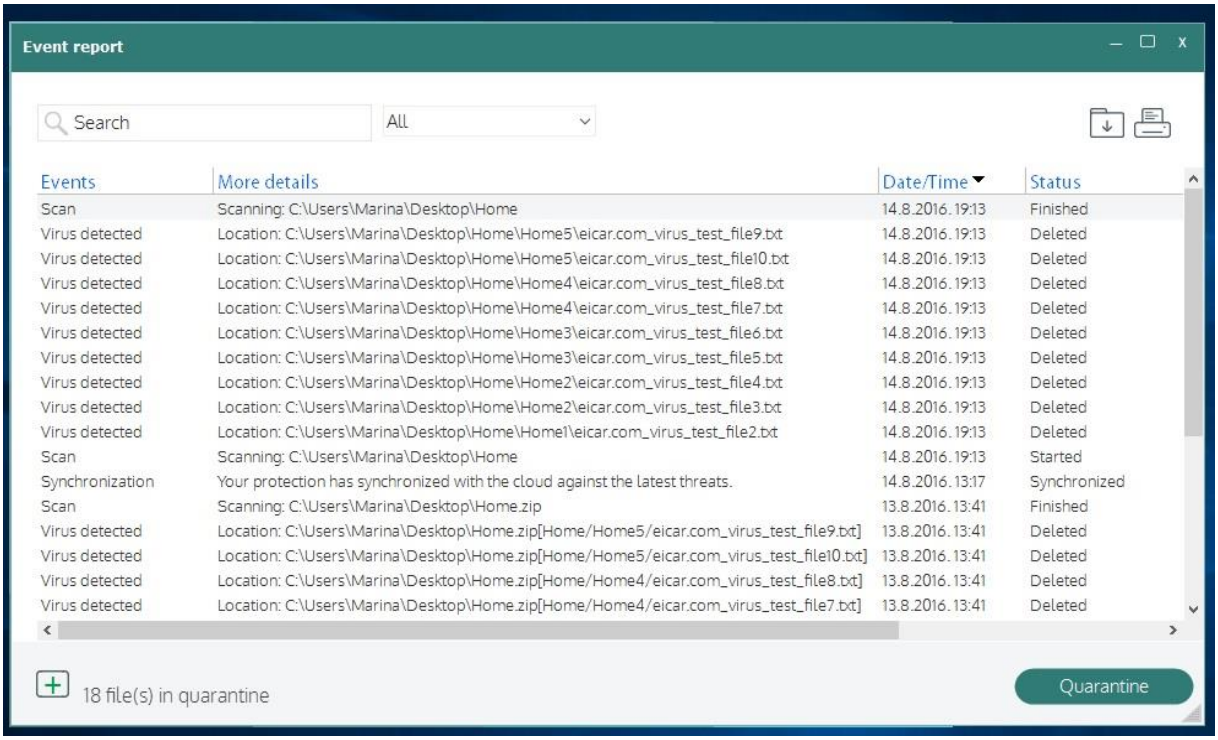


Slika 4.8. *Avira je prepoznala sve zaražene datoteke*

4.6. Panda Free Antivirus

Panda je ujedno i jedna od najlaganijih antivirusnih zaštita što joj daje i prednost jer manje opterećuje računalni sustav svojim radom. Ona vrši automatsko ažuiranje baze podataka o najnovijim virusima tako da omogućava stalnu zaštitu. Panda ima opciju za oporavak sustava oštećenog virusima i to efikasno obavlja kada su u pitanju teško zaražena računala. Za ovo testiranje je instalirana besplatna verzija koja ima manje, ali dovoljno mogućnosti (Sl. 4.9). Dolazi sa malom instalacijom koja ne zahtjeva veliko zauzeće memorije. Panda koristi najviše memorije kada je pokrenuto skeniranje sustava. Također je veoma brz i ne opterećuje sustav u bilo kojem slučaju. Sučelje je vrlo ugodno i pregledno i sve funkcije su pri ruci. Jednostavno se može započeti skeniranje, pogledati izvješća prijašnjih skeniranja i prilagoditi postavke. Sve je dostupno jednim klikom na glavnom prozoru. Nakon klika na opciju skeniraj odmah i odabira prilagođenog skeniranja te odabira direktorija Panda antivirusna zaštita je pronašla 9/10 antivirusa (Sl. 4.10).

Slika 4.9. *Instalacija Panda antivirusne zaštite*



Slika 4.10. *Panda nije pronašla 1 antivirus*

4.7.Diskusija za testiranje antivirusne zaštite

Za testiranje antivirusne zaštite preuzeta je EICAR testna datoteka koja omogućuje testiranje antivirusne zaštite te je kreirano virtualno okruženje sa mapama i podmapama u koje su se umnožile i rasporedile testne datoteke. U mapu od pet podmapa stavljene su dvije testne datoteke. Zatim su instalirani antivirusni programi po redu (Bitdefender, Avast, AVG, Avira i Panda). Na računalo se ne smije instalirati više od jednog antivirusnog programa istovremeno jer to usporava računalo. Pokrenuto je skeniranje kreirane mape sa svakom od pet navedenih antivirusnih programa i testirana je njihova učinkovitost. Bitdefender, Avast i Avira su pronašli svih 10 virusa, Panda je pronašla 9, a AVG nije pronašao niti jedan. Svaki antivirusni program radi drugačije. Bitdefender pruža najbolje performanse i brzinu. Jedina mana je ta što je kompliciranija za instalaciju. Avast je antivirusni program s vrlo malim ažuriranjima koja nadopunjuju informacije o virusima i načinima njihova uklanjanja. Jedan je od boljih besplatnih antivirusnih programa sa sustavom zaštite i brojem otkrivanja virusa te je bolji od nekih antivirusnih programa koji se plaćaju. Ima jednostavno sučelje i ne troši mnogo resursa te ima puno opcija i dodataka. AVG po broju otkrivenih virusa zaostaje za Avastom. Ne može se mjeriti sa konkurencijom jer osim mjesta na disku zauzima velike resurse računala i spor je prilikom skeniranja računala. Avira je dobar program i otkriva vrlo visok postotak virusa. Vrlo je malen i ne troši mnogo resursa, a otklanja viruse na visokoj razini. Ponekad i neke datoteke koje nisu virus označi kao virus i stavlja ih u kavez. U ovom testiranju je pronašao svih 10 testnih datoteka. Panda je također dobar antivirusni program, ali u ovom testiranju nije pronašao jednu testnu datoteku što je mali nedostatak u odnosu na ostale antivirusne programe.

5. ZAKLJUČAK

Računalni virusi su programi koji mogu na računalu napraviti veliku štetu. Mogu se prenositi zaraženim disketama ili internetom. Danas postoji mnogo alata i načina za sprječavanje širenja virusa, ali niti jedan alat nije stopostotna zaštita. U ovom radu su opisani temeljni principi na kojima rade računalni virusi i tehnike obrane od njih u Windows operacijskim sustavima koje omogućavaju siguran rad. U praktičnom dijelu rada je postavljeno nekoliko virusa u različite mape. Preuzeta je EICAR datoteka koja omogućuje testiranje antivirusne zaštite bez korištenja pravog računalnog virusa. Sa pet odabranih antivirusnih programa (Bitdefender, Avast, AVG, Avira i Panda) pretraženo je računalo i testirana je njihova učinkovitost. Bitdefender, Avast i Avira su pronašli svih 10 virusa, Panda je pronašla 9, a AVG nije pronašao niti jedan. Na temelju ostvarenih rezultata, dolazi se do zaključka da svaki antivirusni program radi drugačije i ima druge učinke. Bitdefender se temelji na tehnologiji koja pruža najbolje performanse i brzinu računala te je nagrađivana kao najbolja zaštita. Jedina mana je ta što je kompliciranija za instalirati i instalacija traje malo duže. Avast, Avira, AVG i Panda su zato jednostavne za instalaciju i korištenje, ali ne pronalaze virus tako brzo i dobro kao Bitdefender. Stoga je bolje imati Bitdefender koji je kompliciraniji i brži, nego jednostavne i spore antivirusne programe za korištenje.

LITERATURA

[1] Microsoft Corporation, *Viruses*,
http://windows.microsoft.com/hr-hr/windows/viruses-faq#1TC=windows-7, lipanj 2016.

[2] Wikipedia, *Computer Virus*,
https://en.wikipedia.org/wiki/Computer_virus#Boot_sector_viruses, lipanj 2016.

[3] F. Cohen, Computer Viruses: Theory and Experiments, Computers and Security 6, Elsevier Advanced Technology Publications, pp. 22-35, USA, 1987.

[4] T. Erjavec, Programski virusi u operacijskom sustavu PC-DOS/MS-DOS, Zagreb, 1990.

[5] Zloćudni softver,
https://hr.wikipedia.org/wiki/Zlo%C4%87udni_softver#Ra.C4.8Dunalni_virus, lipanj 2016.

[6] *What are Trojans?*,
https://blog.malwarebytes.org/cybercrime/2013/06/what-are-trojans/, lipanj 2016.

[7] Wikipedia, Trojanski konj (softver),
https://hr.wikipedia.org/wiki/Trojanski_konj_(softver), lipanj 2016.

[8] *Spyware*,
http://www.spychecker.com/spyware.html, lipanj 2016.

[9] Dialer,
https://www.hakom.hr/default.aspx?id=489, lipanj 2016.

[10] Microsoft Corporation, *Malware Protection Center, Rootkits*,
https://www.microsoft.com/en-us/security/portal/mmpc/threat/rootkits.aspx, lipanj 2016.

[11] CARNet, Što je hoax?,
https://www.carnet.hr/hoax_recognizer/hoax, lipanj 2016.

[12] Wikipedia, Hoax,
https://hr.wikipedia.org/wiki/Hoax, lipanj 2016.

[13] What is a Boot Sector Virus?,
https://usa.kaspersky.com/internet-security-center/definitions/boot-sector-virus#.V18FrvmLTIU, lipanj 2016.

[14] Computer Virus Definitions,
http://jdstiles.com/tips/computer/vparas.html, lipanj 2016.

[15] Računalni virus,
https://hr.wikipedia.org/wiki/Ra%C4%8Dunalni_virus, lipanj 2016.

[16] *Companion Virus*,
http://www.virusradar.com/en/glosary/companion-virus, lipanj 2016.

[17] Microsoft Corporation, *How to protect computer from viruses*, http://windows.microsoft.com/hr-hr/windows/how-protect-computer-from-viruses#how-protect-computer-from-viruses=windows-7, lipanj 2016.
[18] K. Dulčić, Oblici štete od računalnih virusa i odgovornost za štetu, Zb. Prav. fak. Sveuč. Rij. (1991), v. 28, br. 1, Rijeka, 2007.
[19] *Antivirus Software Reviews*, http://anti-virus-software-review.toptenreviews.com/, lipanj 2016.
[20] Wikipedia, *Comparison of antivirus software*, https://en.wikipedia.org/wiki/Comparison_of_antivirus_software#Legend, lipanj 2016.
[21] *Antiviruses*, http://hr.vessoft.com/software/windows/category/antiviruses, srpanj 2016.
[22] *EICAR datoteka*, www.eicar.org, kolovoz 2016.
[23] *EICAR General Info*, http://www.eicar.org/6-0-General-Info.html, kolovoz 2016.

SAŽETAK

Računalni virus je računalni program koji svojom reprodukcijom može zaraziti računala. On bez znanja ili dopuštenja korisnika računala sam sebe kopira u datotečni sustav. Virusi se najčešće šire s jednog računala na drugo u obliku zlonamjenog koda putem interneta, privitaka elektroničke pošte, diskete, CD, DVD ili USB diska. Neki od najpoznatijih računalnih virusa su računalni crvi i trojanski konji. Računalni crv je program koji širi svoje kopije na druga računala putem mreže te koristi ranjivost sustava kako bi se proširio. Trojanski konj je program koji se pretvara da izgleda bezopasno i predstavlja se kao neka igra ili sadržaj elektroničke pošte, ali najčešće ima skrivenu štetnu funkcionalnost. Da bi se zaštitili od računalnih virusa, na računalo se treba instalirati antivirusna zaštita. Koristi se kao zaštita i uklanja viruse. Kada ga antivirusna zaštita pronađe, šalje ga u „izolaciju“ ili ga potpuno izbriše sa računala. Neki od antivirusnih programa su: Bitdefender, Avast, AVG, Avira i Panda. Testirajući njihovu učinkovitost, postavljeno je na računalo desetak virusa u različite mape. Za testiranje je korištena EICAR datoteka koja omogućuje testiranje bez potrebe korištenja pravog virusa. Bitdefender, Avast i Avira pronašli su svih 10 virusa, Panda je pronašla 9, a AVG nije pronašao niti jedan.

Ključne riječi: računalni virus, antivirusna zaštita, računalni crv, trojanski konj

ABSTRACT

A computer virus is a computer program that can infect other computers with reproduction. Without the knowledge or permission of computer users it can copy itself in the file system. The viruses are usually spread from one computer to another in the form of malicious code over the Internet, e-mail attachments, floppy disks, CD, DVD or USB drive. Some of the best known computer viruses are computer worms and Trojan horses. A computer worm is a program that spreads its own copies to other computers over a network and uses system vulnerability to spread. A Trojan horse is a program that pretends to look harmless and presents itself as a game or the content of an e-mail but usually has a hidden harmful functionality. To protect against computer viruses it is necessary to install antivirus protection on a computer system. It is used as a protection and removes viruses. When the antivirus protection finds virus, it sends it in the "quarantine" or completely delete it from the computer. Some antivirus programs are: Bitdefender, Avast, AVG, Avira and Panda. To test their efficiency a dozen computer viruses were places in different folders. For the testing purposes EICAR file that allows testing without using real viruses was used. Bitdefender, Avast and Avira found all 10 viruses, Panda found a 9 and AVG didn't find any.

Keywords: computer virus, antivirus protection, computer worm, Trojan horse

ŽIVOTOPIS

Marina Kušer rođena je 10. svibnja 1994. godine u Zagrebu. Živi u Kutini. Osnovnu školu upisala je i završila u OŠ „Zvonimira Franka“ u Kutini. Nakon osnovne škole završava prirodoslovno-matematičku gimnaziju u Kutini 2013. godine. Iste 2013. godine upisuje preddiplomski stručni studij Elektrotehnike, smjer Informatika na Elektrotehničkom fakultetu u Osijeku. Raspolaže prilično dobrim znanjem engleskog jezika kojeg aktivno koristi. Također, razumije dosta njemački i španjolski jezik. Uz stečena znanja na fakultetu izuzetno je zainteresirana za programiranje i internetski dizajn. Upoznata je s gotovo svim alatima programa Office koje svakodnevno koristi.

Marina Kušer