Zaštita od računalnih virusa

Dangubić, Ivana

Sveučilište Jurja Dobrile u Puli
Fakultet informatike

Ivana Dangubić

Zaštita od računalnih virusa

Završni rad

Pula, 2019.

Sveučilište Jurja Dobrile u Puli
Fakultet informatike

Ivana Dangubić

Zaštita od računalnih virusa

Završni rad

JMBAG: 0303068807,redovita studentica

Studijski smjer: Informatika

Predmet: Računalne mreže

Znanstveno područje: Društvene znanosti
Znanstveno polje: Informacijske i komunikacijske znanosti
Znanstvena grana: Informacijski sustavi i informatologija

Mentor: prof. dr. sc. Mario Radovan

Pula, rujan 2019.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisana Ivana Dangubić, kandidatkinja za prvostupnicu informatike, ovime izjavljujem da je ovaj Završni rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Završnog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student

_____

U Puli, _____, _____ godine

IZJAVA

o korištenju autorskog djela

Ja, Ivana Dangubić dajem odobrenje Sveučilištu Jurja Dobrile u Puli, kao nositelju prava iskorištavanja, da moj završni rad pod nazivom Zaštita od računalnih virusa koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu s Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.

Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

U Puli, _____ (datum)

Potpis

_____

Sadržaj

1. Uvod ... 1

2. Računalni virusi ... 3

2.1. Širenje računalnih virusa ... 5

2.2. Podjela računalnih virusa ... 6

2.2.1. Datotečni virus (eng. File infector virus) ... 6

2.2.2. Virusi prvog sektora (eng. Boot sector Virus/ boot virus) ... 7

2.2.3. Makro virusi (eng. Macro viruses) ... 8

2.2.4. Svestrani virusi (eng. Multipartite Viruses) ... 9

2.2.5. Virusi web skripte (eng. Web scripting virus) ... 9

2.2.6. Računalni crvi (eng. Worms) ... 10

2.2.7. Trojanski konj (eng. Trojan horse) ... 12

2.2.8. Spyware/Adware ... 13

3. Zaštita od računalnih virusa ... 14

3.1. Antivirusni programi ... 15

3.1.1. Bitdefender Antivirus Free Edition ... 17

3.1.2. Avast Free Antivirus ... 19

3.1.3. Avira Free Antivirus ... 20

3.1.4. AVG Free Antivirus ... 22

3.1.5. Panda Free Antivirus ... 23

4. Testiranje antivirusnih programa ... 25

4.1. Testiranje Bitdefender Antivirus Free Edition računalnog programa ... 26

4.2. Testiranje Avast Free Antivirus računalnog programa ... 28

4.3. Testiranje Avira Free Antivirus računalnog programa ... 30

4.4. Testiranje AVG Free Antivirus računalnog programa ... 32

4.5. Testiranje Panda Free Antivirus računalnog programa ... 34

5. Zaključak ... 36

Literatura ... 37

Popis slika ... 39

Summary ... 42

1. Uvod

Uporabom računalnih mreža korisnici se svakodnevno suočavaju s rizikom „zaraze“ od računalnih virusa. U ovome radu pisati ću kako se zaštiti od računalnih virusa, a isto tako i što su to virusi, kako se šire, podjela virusa i opis nekih od ostalih zlonamjernih programa koji se smatraju virusima (eng. Malware).

Razvojem tehnologije postoji veća mogućnost „zaraze“ zlonamjernim softverima. Dakle, svako računalo koje je spojeno na internet izloženo je brojnim elektroničkim prijetnjama. Računalni virus je zlonamjerni program koji se prenosi na korisničko računalo bez korisnikova znanja i obavlja zlonamjerne radnje. Nakon što zlonamjerni softver „zarazi“ naš uređaj, on može uzrokovati štetu na različite načine kao što je brisanje naših datoteka/podataka, mijenjanje raznih postavki sustava, usporavanje rada računala, prikazivanje lažnih poruka i instaliranje špijunskog softvera (eng. Spyware) koji prikuplja naše privatne podatke, lozinke isl. Računalni virusi mogu se prenositi/širiti sa računala na računalo skrivajući se unutar nekog dokumenta ili aplikacije bez znanja korisnika računala. Prilikom prvog pokretanja „zaražene“ datoteke virus se aktivira.

Izraz virusi upotrebljen je po prvi put od strane autora znanstvene fantastike Davida Gerrolda te je označavao neželjeni računalni kod. David Gerrold 1970-ih napisao je niz kratkih priča o izmišljenom G.O.D stroju (super računalo) koje su kasnije 1972. godine spojene u roman „Kada je Harlie bio jedan“ (eng. When Harlie Was One). Opis virusa u tom romanu ne odgovara tj. ne uklapa se u trenutno prihvaćenu, popularnu definiciju računalnog virusa. Fred Cohen 1983. godine definirao je pojam računalnog virusa.

Većina virusa „napada“ osobna računala te je do sada ustanovljeno više od 10.000 virusa, a otprilike oko 85 posto svih poznatih virusa „inficira“ programske datoteke kao što su proračunske tablice i računalne igre.

Postoje razne tehnike kako se zaštiti od računalnih virusa, no najpoznatija i najučinkovitija je uporaba antivirusnog programa. Instalacijom antivirusnog programa ili antivirusa možemo zaštiti svoje računalo od virusa i raznih zlonamjernih prijetnji. Antivirusni program će skenirati viruse i ukloniti ih ukoliko je računalo već zaraženo te će isto tako služiti kao prevencija od „zaraze“ zlonamjernim programima. Kako bi

zaštita bila osigurana potrebno je redovito nadograđivati antivirusni program zbog kontinuirane pojave novih zlonamjernih prijetnji.

U ovome radu detaljno ću opisati najpoznatije vrste računalnih virusa i zlonamjernih softvera.

2. Računalni virusi

„Računalni virus je računalni program koji može „inficirati“ druge programe modificirajući ih na taj način da to podrazumijeva stvaranje vlastite kopije“ (Cohen, 1990.). Virusi imaju slične karakteristike kao i biološki virusi koji inficiraju ljude. Računalni virus prelazi s računala na računalo kao što na primjer virus prehlade prelazi s djeteta na jednog roditelja, a zatim s roditelja na drugog roditelja itd. U početku virusi su se širili putem disketa ili CD-a, no kako je popularnost interneta rasla tako je on postao glavni medij prijenosa virusa. Struktura računalnih virusa može se podijeliti na tri dijela gdje se obaveznim smatra samo prvi dio računalnog virusa. Prva komponenta omogućuje „infekciju“ odnosno razmnožavanje. Drugi dio/komponenta predstavlja nosivu komponentu (eng. payload) koja nije obavezna, a može ili ne mora biti opasna. „Ovaj dio definira sve aktivnosti virusa koje će biti izvedene uz njegovo širenje. Treći dio, koji također nije obvezan, predstavlja funkcija za okidanje (engl. trigger) koja definira vrijeme ili događaj prilikom kojeg će biti izvršena nosiva komponenta virusa.“(Ždrnja, 2003.)

Rich Skrenta, tadašnji srednjoškolac 1982. godine stvorio je prvi potvrđeni računalni virus. Virus se zvao Elk Cloner te je bio vezan za operacijski sustav Apple DOS 3.3. Virus se širio preko diskete, a prvotno je bio dizajniran iz šale. Godine 1983. informatičar Frederick B. Cohen/Fred Cohen definirao je pojam „Virus“ u svom istraživačkom radu „Eksperimenti sa računalnim virusima“ (eng. "Computer virus experiments") i kako se obraniti od njih.

Virus se obično veže za neki program, datoteku ili sektor za pokretanje tvrdog diska. Kada se zaražena aplikacija ili datoteka pokrene na računalu, virus se aktivira i izvršava u sustavu. Nakon toga virus se nastavlja replicirati i širiti pridružujući svoje kopije drugim datotekama i aplikacijama u sustavu. Kao što je već spomenuto nakon što virus „zarazi“ računalo, može doći do brisanja podataka, sporijeg rada računala, krađe podataka/nedostatak podataka, pojava raznih reklama, rušenja sustava, promjene lozinka, slanje raznih poruka preko elektroničke pošte sa korisnikova računala, instalacija špijunskog softvera koji prikuplja naše privatne podatke, lozinke itd.

Računalnim virusima se nazivaju i neki drugi zlonamjerni programi kao što su računalni crvi (eng. Worms) kojima nije potrebna interakcija s korisnikom kako bi pristupili određenom računalu. Na primjer korisnik može pristupiti mrežnoj aplikaciji koja je ranjiva, a kojoj je ujedno napadač poslao zlonamjerni softver. Aplikacija zatim može prihvatiti zlonamjerni softver s interneta i pokrenuti ga bez ikakve interakcije s korisnikom.

2.1. Širenje računalnih virusa

Kako popularnost interneta raste, „zaraza“ računalnim virusima sve je češća te je moguća na više različitih načina. Kako bi se virus uspješno širio mora se klonirati, prenijeti na druga računala, te opet ponoviti ciklus replikacije samoga sebe. Naravno kako bi to uspjelo virus se veže za razne programe/datoteke na računalu, prenosi se na elektroničku poštu (eng. E-mail) kao privitak datoteke ili poruke te se čak može preuzeti preko web stranice. Način širenja virusa sa računala na računalo možemo podijeliti u dvije kategorije: Vanjski mediji i računalne mreže. Bilo koji uređaj za pohranu nazivamo vanjskim medijem, a on može sadržavati datoteku računala i biti povezan sa računalom. Primjeri vanjskog medija su: disketa, tvrdi disk (eng. Hard Disk), CD, DVD, USB isl. Mreža je skupina povezanih računala koja mogu razmjenjivati neke resurse. Virusi se putem internet mreže mogu kretati putem elektroničke pošte, raznih razgovora (eng. Chat), Web stranica, poveznicama na društvenim mrežama itd.

Kada je virus preuzet na računalo on se aktivira pokretanjem „zaražene“ datoteke. Nakon pokretanja, virus se instalira u memoriji računala kako bi se mogao replicirati u ostale datoteke/aplikacije koje korisnik pokreće odnosno koristi. Na kraju virus će se proširiti na druga računala disketom, mrežom i drugim načinima koje sam prethodno opisala.

2.2. Podjela računalnih virusa

Virusima ne definiramo programe koji čine štetu ili kradu podatke na našim računalima, već programe koji se mogu sami replicirati. Programi koji uzrokuju štetu, a koji nemaju mogućnosti replikacije samog sebe nazivamo Trojanski konji.

Neki od najpoznatijih računalnih virusa su datotečni virusi, makro virusi, virusi prvog sektora, svestrani virusi, virusi web skripte itd.

Uz tipične viruse postoje i zlonamjerni programi koje također svrstavamo u kategorije virusa, a to su računalni crvi, trojanski konji, špijunski softveri, reklamni softveri isl.

2.2.1. Datotečni virus (eng. File infector virus)

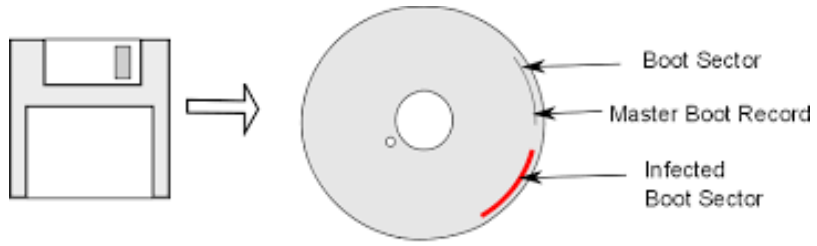
Datotečni virusi su najpoznatija vrsta virusa, a koriste izvršne datoteke kao svoje domaćine. Datotečni virus unosi svoj kod u strukturu programa s namjerom da ih učini neupotrebljivim ili da im nanese traju štetu. Ova vrsta virusa može „zaraziti“ razne operacijske sustave kao što su Macintosh, Windows i Unix. Datotečni virus može se širiti po sustavu i preko mreža kako bi zarazio druge sustave. Postoje također i tipovi datotečnog virusa koje se prepisuju preko datoteke domaćina. Datoteke koje se mogu „zaraziti“ ovom vrstom virusa imaju ekstenziju .exe i .com kao što su računalne ili video igre, aplikacije za proračunske tablice, programi za obradu teksta itd.

Najpoznatiji primjer datotečnog virusa je virus Cleevix koji je otkriven 2006.godine. Cleevix funkcionira na način kada se izvrši, traži trenutni direktorij ili sistemski direktorij te tada „inficira“ sve izvršne datoteke unutar tog direktorija. Ovaj virus lako je primjetiti pošto izbacuje poruku nakon izvršenja „infekcije“.

2.2.2. Virusi prvog sektora (eng. Boot sector Virus/ boot virus)

Virusi prvog sektora su jedni od najopasnijih virusa. To je virus koji utječe na sektor za pokretanje sustava(eng. Boot Sector). Na sektoru za podizanje sustava koji se nalazi na disku (čvrsti disk ili SSD), postoji program (eng. Master Boot Record) koji pokreće računalo prilikom njegovog uključivanja. Virus prvog sektora zamjenjuje se s tim programom odnosno unosi svoj kod, a zatim se dalje širi na ostale diskove. Ako se virus nalazi na disketi on će se jednako tako i proširiti na tvrdi disk. Kada se virus aktivira, učitati će se u RAM memoriju te tako zaraziti svaku disketu koju korisnik poželi koristiti. Ovi virusi se najčešće šire putem zaražene diskete ili USB uređaja. Posljedica virusa prvog sektora je nemogućnost podizanja sustava, drugim riječima ako uključite računalo, ono se neće pokrenuti. Prvi „boot sektor virus“ zvao se „Brain“ kojeg je bilo vrlo teško detektirati, a funkcionirao je na prethodno opisani način.

Slika 1. Virus prvog sektora



Boot Sector Virus Infection

Izvor: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1981886 (04.07.2019)

2.2.3. Makro virusi (eng. Macro viruses)

Makro je programski jezik kojim je napisan makro virus kao što i samo ime govori. Makro jezikom napisane su aplikacije kao što su programi za obradu teksta, proračunske tablice itd. Makro virusi su najčešće prisutni kod Microsoft Office programskih paketa, a može „zaraziti“ bilo koje računalo te bilo koji operacijski sustav. Razlog tome je što se ovaj virus bazira na aplikaciji, a ne na operacijskom sustavu. Makro virusi se šire na način da tvorac virusa kreira makro naredbu (niz naredbi koje pomažu u automatizaciji nekih zadataka) koja sadrži virus te ju zatim pridružuje Word dokumentu. Nakon toga taj dokument može biti poslan preko elektroničke pošte, interneta, nekih drugih mreža itd. Ukoliko korisnik otvori taj privitak elektroničke pošte, dokument/virus se otvara na računalu korisnika. Kada je dokument otvoren makro naredba se pokreće te se virus izvršava i kopira u glavnu datoteku. Iz tog razloga kada korisnik otvori ili kreira novu datoteku glavna datoteka će biti kopirana u novu.

Također virus može ponovo poslati privitak elektroničke pošte dalje. Najpoznatiji makro virus zove se Melissa koji je bio poznat po brzini širenja. U 3 dana Melissa virus zarazio je 100,000 računala, a širio se putem elektroničke pošte.

2.2.4. Svestrani virusi (eng. Multipartite Viruses)

Kao što je do sada opisano neki virusi mogu zaraziti/utjecati ili na sektor za pokretanje (eng. Boot sector) ili izvršne datoteke. Svestrani virus može zaraziti oboje te na taj način može uzrokovati veću štetu od ostalih virusa. Ovi virusi aktiviraju se prilikom pokretanja računala zbog „napada“ na sektor za podizanje sustava, ali istovremeno „napadaju“ i izvršne datoteke. Svestrani virusi mogu se brže širiti od datotečnih virusa ili virusa prvog sektora zbog svojih višestrukih mogućnosti. Svestrani virusi mogu uzrokovati veliku štetu uključujući nemogućnost pokretanja računala i neupotrebljivosti datoteka kao što je već navedeno kod prethodnih primjera. Uz sve to ovu vrstu virusa vrlo je teško ukloniti jer čak i ako se očiste datoteke zaražene virusom, a u sektoru za podizanje sustava se i dalje nalazi virus on će se ponovno kopirati i proširiti kada se računalo ponovno pokrene/uključi.

2.2.5. Virusi web skripte (eng. Web scripting virus)

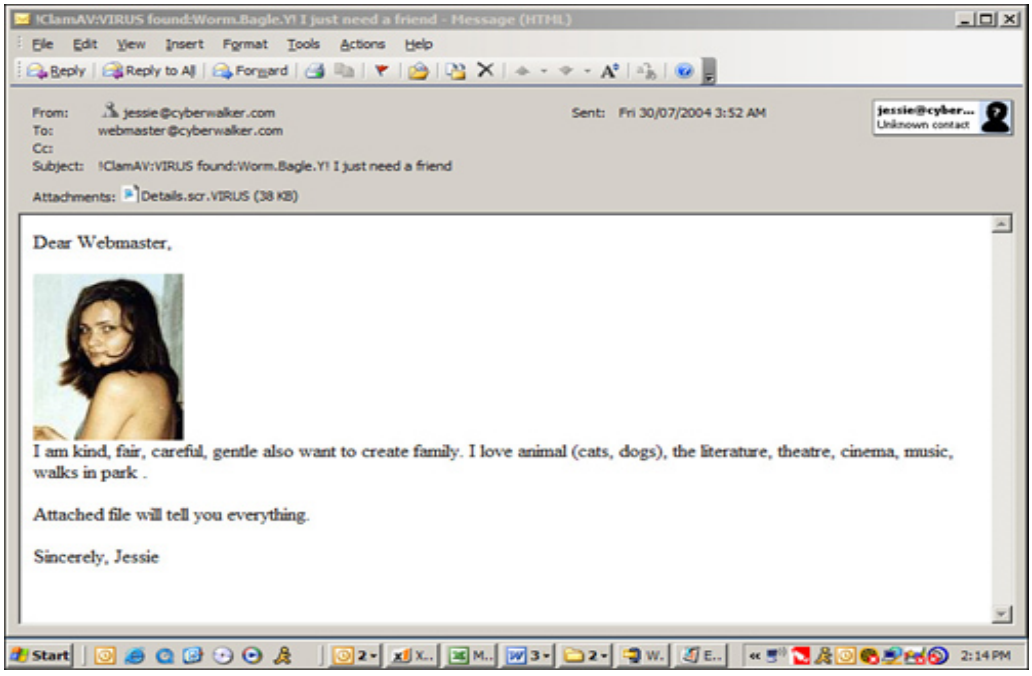
Virusi web skripte „borave“ u određenim poveznicama (eng. Link) , oglasima, slikama, videozapisima i aplikacijskim okvirima web stranica (eng. Web layout). Ako korisnik odabere sliku, videozapis ili link koji sadrži zlonamjerne kodove, virus će se automatski preuzeti ili će korisnika preusmjeriti na zlonamjernu web stranicu. U većini slučajeva virus postoji kada je njegov kod umetnut unutar web stranice bez znanja tvorca te iste stranice. Na taj način proizvođač virusa može imati uvid u podatke korisničkog imena i lozinke raznih korisnika. Virusi web skripte obično „napadaju“ web mjesta sa velikom populacijom, kao što su društvene mreže i elektronička pošta, a imaju sposobnost vrlo brzog širenja. Posljedica virusa web skripte je usporen rad računala, neočekivano i učestalo gašenje računala, promjena početne stranice preglednika ili radne površine itd.

2.2.6. Računalni crvi (eng. Worms)

Računalni crvi su mrežni virusi koji se prenose i reproduciraju preko računalne mreže. Za razliku od virusa, računalni crvi ne trebaju datoteku ili program na računalu kako bi se proširili, već je dovoljno otvoriti privitak elektroničke pošte i crv će imati pristup računalu. Kada korisnik otvori privitak na elektroničkoj pošti koja sadrži virus crva, on tada inficira sustav te se kopira i šalje kopije na ostale adrese elektroničke pošte koje je pronašao na inficiranom računalu ili koristeći ugrađeni poslužitelj elektroničke pošte (eng. Mailer). Najpoznatiji računalni crv koji funkcionira na taj način je računalni crv elektroničke pošte (eng. Mass-mailing worm). Računalni crvi mogu biti dizajnirani na način da im ne treba interakcija s korisnikom da bi se izvršili. Koriste razne tehnike kao što su ranjive web aplikacije koje sam ranije opisala. Privitak isto tako može i pružiti vezu na neku zlonamjernu web stranicu. „Virusi“ kao što su računalni crvi se ne vežu za neki program ali mogu inficirati operacijski sustav, mrežu ili aplikaciju elektroničke pošte. Ponekad svrha računalnog virusa je samo stvaranje kopija što rezultira preopterećenju mreže. Računalni crvi također mogu sadržati dijelove koda (eng. payloads) koji su napisani kako bi izvodili određene zlonamjerne akcije na zaraženom računalu, a ne samo za širenje crva. Oni su uglavnom dizajnirani u svrhu krađe podataka ili brisanja datoteka. Osim preko elektroničke pošte, crvi koriste i razne druge mrežne komunikacijske protokole kako bi se što brže proširili internetom.

Na slici 2. možemo vidjeti primjer u kojemu je računalni crv poslan preko elektroničke pošte kao privitak. Naime u primjeru virus se predstavlja nepoznatom djevojkom.

Slika 2. Primjer računalnog crva poslanog preko elektroničke pošte



Izvor: Walker, Andy (2005, Studeni). Absolute Beginner's Guide to Security, Spam, Spyware and Viruses. Preuzeto s https://learning.oreilly.com/library/view/absolute-beginners-guide/0789734591/ch01.html (04.07.2019)

2.2.7. Trojanski konj (eng. Trojan horse)

Trojanski konj je zlonamjerni softver koji se pretvara da izgleda bezopasno i legitimno, no može uzrokovati štetu. Trojanski konj se može pretvarati da je nešto korisno ili zabavno, a zapravo uzrokuje štetu. Naziv je dobio po priči o osvajanju grada Troje, gdje se protivnici skrivaju unutar drvenog konja kako bi prikriveno ušli u Troju. Ovaj zlonamjerni softver nije virus te se ne može sam razmnožavati. Pošto se trojanski konj pretvara kao nešto korisno ili zabavno korisnik ga može instalirati na svoje računalo ne znajući da je to zlonamjerni softver. Kada trojanski konj „zarazi“ računalo on može obrisati datoteke, krasti podatke, instalirati dodatni špijunski softver isl. Može se širiti putem „zaraženog“ privitka elektroničke pošte, besplatne igre (koju treba instalirati na računalo), raznih aplikacija, filmova itd.

Neke od najpoznatijih vrsta trojanskih konja su :

- Preuzimač (eng. Downloader) – program koji preko interneta preuzima i instalira druge zlonamjerne programe na računalo korisnika. Na taj način može doći do „zaraze“ virusom.
- Kapaljka (eng. Dropper) – program koji sadrži virus kako bi „zarazio“ namijenjeno računalo. Pomoću njega virus može izbjeći razotkrivanje od antivirusnog programa
- Stražnja vrata (eng. Backdoor) – program koji omogućuje tvorcima zlonamjernih softvera neovlašteni pristup.

2.2.8. Spyware/Adware

Spyware je zlonamjerni računalni program koji je instaliran na računalu korisnika bez njegova znanja. Glavna namjena ovog programa je prikupljanje raznih informacija „zaraženog“ računala kao što su: informacije o aktivnostima pregledavanja na internetu (koje web stranice korisnik posjećuje), povijest pregledavanja, elektronička pošta, mrežni promet, osobne informacije korisnika (informacije kreditne kartice), pregledavanje pritisnutih tipki na tipkovnici (eng. Keylogger) itd. Također, namjena spyware-a može biti prosljeđivanje odnosno slanje navedenih informacije nekoj drugoj osobi putem interneta. Za razliku od virusa i računalnih crva Spyware nema mogućnost repliciranja na računalu. Ovakvim programom moguće se „zaraziti“ posjećivanjem ilegalnih i nepoznatih stranica te preuzimanjem programa nepoznatih autora. Posljedice zaraze spyware programom su nemogućnost pokretanja računala, preusmjeravanje na web stranice reklamnih proizvoda, zauzeće prostora na tvrdom disku, prekinuti rad programa i računala itd.

Adware ili reklamni softver je zlonamjerni program koji prikazuje nepoželjne oglase. Ovaj softver prati navike korisnika te u skladu s njima prikazuje razne oglase i reklame. Adware može biti vrsta besplatnog softvera podržanog oglasima koji se prikazuje u obliku skočnih prozora, na pregledniku ili alatnoj traci računala. Većina ovakvih programa je neugodna, ali sigurna te se uglavnom koristi u marketinške svrhe . Dok postoje i druge vrste koje mogu prikupljati razne privatne informacije, pratiti aktivnosti na internetu ili snimati pritisnute tipke na tipkovnici. Računalo je „zaraženo“ adware programom ukoliko se oglasi počnu prikazivati u aplikacijama ili na radnoj površini čak i ako korisnik ne pregledava internetom

I spyware i adware mogu biti ugrađeni u neki besplatni softver te ih na taj način korisnik može vrlo lako „pokupiti“.

3. Zaštita od računalnih virusa

Kako bi obranili računalo od stalnih prijetnji zlonamjernih programa potrebno ga je zaštiti. Postoje razne tehnike zaštite računala od virusa, kako bi to učinili potrebno je:

- Instalirati antivirusni program – antivirusni programi su najbolja obrana od zlonamjernih programa. Da bi zaštita bila učinkovita potrebno je obraćati pozornost na ispravnost rada antivirusa odnosno njegovu ažurnost zbog dolaska novih virusa. Antivirusni programi traže viruse i druge zlonamjerne programe te ih uklanjaju.
- Ne otvarati poruke elektroničke pošte od nepoznatih pošiljatelja – kao što je već prije spomenuto, većina virusa širi se putem privitka elektroničke pošte. Ukoliko je pošiljatelj nepoznat te ne očekujete poruku s privitkom ili je čak poruka poslana s vlastite email adrese treba ju izbjegavati i ne otvarati.
- Redovito ažurirati operacijski sustav – ažuriranje operacijskih sustava sprječava „zarazu“ virusima ispravljanjem nekih mogućih sigurnosnih propusta.
- Upotrebljavati vatrozid (eng. Firewall) – „vatrozid je sustav koji kontrolira pristup između dvije mreže - kao što je privatni LAN i nesiguran, javni Internet.“ (3Com Corporation, 2000.)

Ove tehnike primjenjujemo ukoliko je računalo zaraženo nekim zlonamjernih programom ili se jednostavno želimo preventivno zaštiti.

3.1. Antivirusni programi

Antivirusni program ili antivirus je program koji služi za detektiranje i uklanjanje virusa sa „zaraženog“ računala. Antivirusni programi pojavili su se ubrzo nakon pojave i prvih virusa. Namjena antivirusnih programa je zaštiti računalo od virusa te ukloniti sve pronađene viruse. Program će slati upozorenja ukoliko pronađe viruse ili razne zlonamjerne prijetnje računalu. Kada je virus detektiran na računalu antivirusni program može upitati korisnika, hoće li virus biti smješten u izolaciju (eng. Quarantine) ili potpuno izbrisan. Ako je virus u izolaciji, tada je spriječen od poduzimanja bilo kakve štete te ga se može poslati na analizu proizvođačima antivirusa. Većina antivirusa može se koristiti za zaštitu i od ostalih zlonamjernih programa kao što su računalni crvi, trojanski konji, spyware isl.

Različiti antivirusni programi imaju različite značajke te svaki ima svoje prednosti i mane, a neki od najboljih antivirusnih programa za 2019. godinu su: Bitdefender Antivirus Plus 2020 (Bitdefender), Bitdefender Internet Security 23.0 (Bitdefender), Norton AntiVirus Plus (Norton Antivirus), Norton Security (Norton Antivirus), ESET Internet Security (ESET), Kaspersky Anti-Virus (Kaspersky lab), Panda Antivirus Pro (Panda Security), AVG Ultimate 2019 (AVG Technologies), Avast Premier 2019 (Avast Software), Avast Free AntiVirus (Avast Software), Avira Antivirus Pro 2019 (AVIRA Antivirus), McAfee Total Protection 2019 (McAfee) itd.

U ovome radu opisati ću neke od najboljih besplatnih verzija antivirusnih programa koje ću također i testirati.

Tablica 1. opisuje rezultate testiranja Bitdefender antivirusnog programa za Windows i macOS operacijske sustave. Uz pojedini datum moguće je vidjeti ocjenu zaštite, performanse, iskoristivost i verziju antivirusnog programa. Kao što i samo ime govori zaštita predstavlja obranu/zaštitu od zlonamjernih programa kao što su virusi, računalni crvi, trojanski konji isl. Performanse predstavljaju utjecaj proizvoda odnosno antivirusnog programa na brzinu računala, a iskoristivost označava kako sigurnost softvera utječe na upotrebljivost cijelog računala (npr. Lažne uzbune ili blokade prilikom korištenja raznih web stranica).

Sljedeće tablice opisuje ostale antivirusne programe te su opisane jednako kao i tablica 1.

Tablica 1. Rezultati testiranja Bitdenfender antivirusnog programa

Datum	Operacijski sustav	Zaštita	Performanse	Iskoristivost	Verzija
Lipanj 2019.	Windows 10	5	6	6	Internet Security 23.0
Travanj 2019.	Windows 10	6	6	6	Internet Security 23.0
Veljača 2019.	Windows 10	5.5	5.5	5.5	Internet Security 23.0
Prosinac 2018.	Windows 10	6	6	6	Internet Security 23.0
Lipanj 2019.	macOS	6	6	6	Antivirus for Mac 7.2
Prosinac 2018.	macOS	6	6	6	Antivirus for Mac 7.1
Lipanj 2018.	macOS	6	6	6	Antivirus for Mac 6.1

Izvor: https://www.av-test.org/en/ (01.08.2019.)

Tablica 2. Rezultati testiranja Avast antivirusnog programa

Datum	Operacijski sustav	Zaštita	Performanse	Iskoristivost	Verzija
Lipanj 2019.	Windows 10	5.5	6	6	Free AntiVirus 19.5
Travanj 2019.	Windows 10	5.5	6	6	Free AntiVirus 19.2/19.4
Veljača 2019.	Windows 10	6	5.5	6	Free AntiVirus 19.1
Prosinac 2018.	Windows 10	6	5.5	6	Free AntiVirus 18.7/18.8
Lipanj 2019.	macOS	6	5.5	6	Security 13.12
Prosinac 2018.	macOS	4.5	6	6	Security 13.11
Lipanj 2018.	macOS	6	4	6	Security 13.5

Izvor: https://www.av-test.org/en/ (01.08.2019.)

Tablica 3. Rezultati testiranja Avira antivirusnog programa

Datum	Operacijski sustav	Zaštita	Performanse	Iskoristivost	Verzija
Lipanj 2019.	Windows 10	5.5	5.5	6	Antivirus Pro 15.0
Travanj 2019.	Windows 10	6	5.5	6	Antivirus Pro 15.0
Veljača 2019.	Windows 10	6	5.5	6	Antivirus Pro 15.0
Prosinac 2018.	Windows 10	6	6	6	Antivirus Pro 15.0
Lipanj 2019.	macOS	6	5	6	Antivirus Pro 3.10
Prosinac 2018.	macOS	6	5	6	Antivirus Pro 3.10
Lipanj 2018.	macOS	5.5	5	6	Antivirus Pro 3.9

Izvor: https://www.av-test.org/en/ (01.08.2019.)

3.1.1. Bitdefender Antivirus Free Edition

Bitdefender Antivirus Free Edition besplatna je verzija antivirusnog programa, a dostupna je za Windows, Mac OS i Android operacijske sustave. Ovaj antivirusni program, kao i ostali nudi zaštitu od virusa i ostalih zlonamjernih prijetnji, a ima mogućnost automatskog skeniranja. Besplatna verzija uključuje i zaštitu od prevara kao što je pokušaj krađe identiteta sa kreditne kartice. Uz sve to ova verzija antivirusnog programa skenira sve veze kojima korisnik pristupa putem preglednika i automatski ih blokira ukoliko su nesigurne ili sumnjive.

Prednosti:

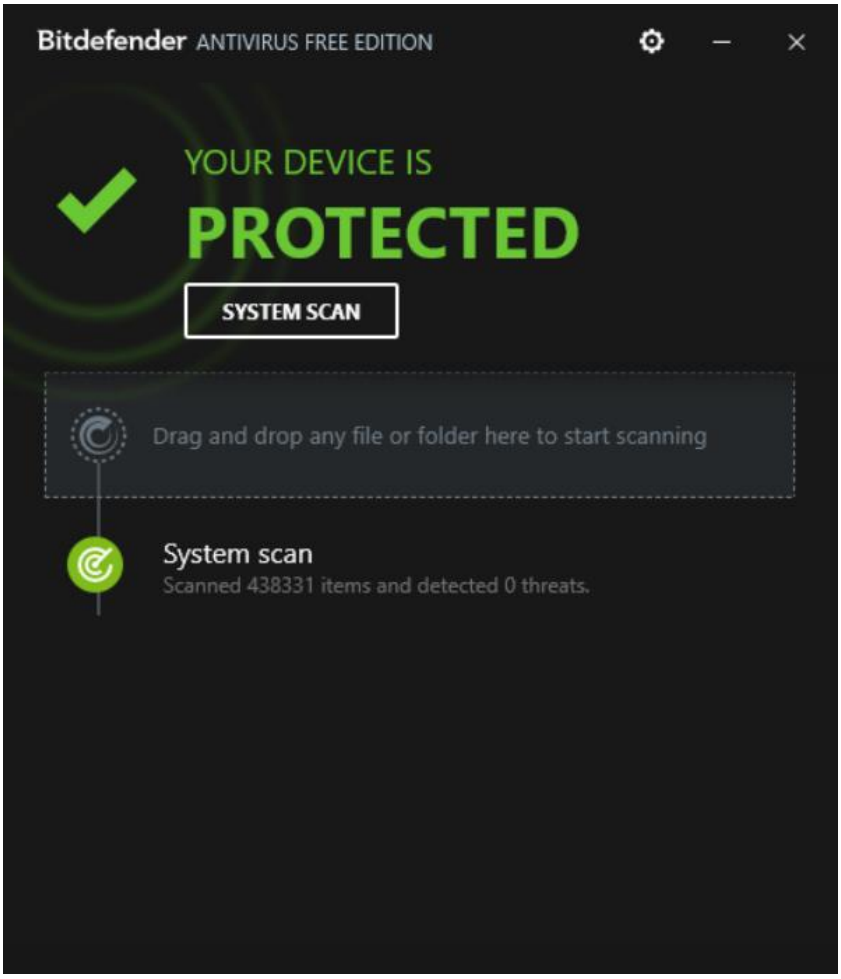
- Vrlo jednostavan i brz prilikom instalacije i korištenja
- Izvrsna detekcija virusa
- Definicije virusa redovito se ažuriraju
- Automatsko skeniranje
- Brzo skeniranje

Mane:

- Napredni korisnici možda žele veću kontrolu

- Moguće ga je koristiti samo kod kuće – bez poslovne upotrebe
- Nije moguće brzo skeniranje (eng. Quick Scan)

Slika 3. Prikaz sučelja Bitdefender Antivirus Free Edition antivirusnog programa



3.1.2. Avast Free Antivirus

Avast programi su jedni od najpopularnijih i najpouzdanijih antivirusnih softvera. „Avast Free Antivirus može pronaći i zaustaviti nepoznate datoteke tehnologijom „CyberCapture“, a uz to i poboljšati Wi-Fi inspektorom koji može pronaći slabe točke u usmjerivaču.“(Tom McNamara, Listopad 2017). Instalacijom avast antivirusnog programa uključuje i sigurni preglednik „Avast Secure Browser“ koji će pružati dodatnu zaštitu. Ova besplatna verzija dostupna je za Windows, macOS i Android operacijske sustave. Osim zaštite od virusa Avast Free Antivirusima ima razne pogodnosti kao što su: ažuriranja softvera na računalu kako bi se povećala sigurnost, udaljena pomoć koja pomaže korisniku na internetu (eng. Remote Assistance), mogućnost prebacivanja na „Ne uznemiravaj“ karakteristiku koja će onemogućiti ažuriranja ili neke skočne obavijesti (eng. popups) prilikom gledanja filmova ili korištenja računalnih igara.

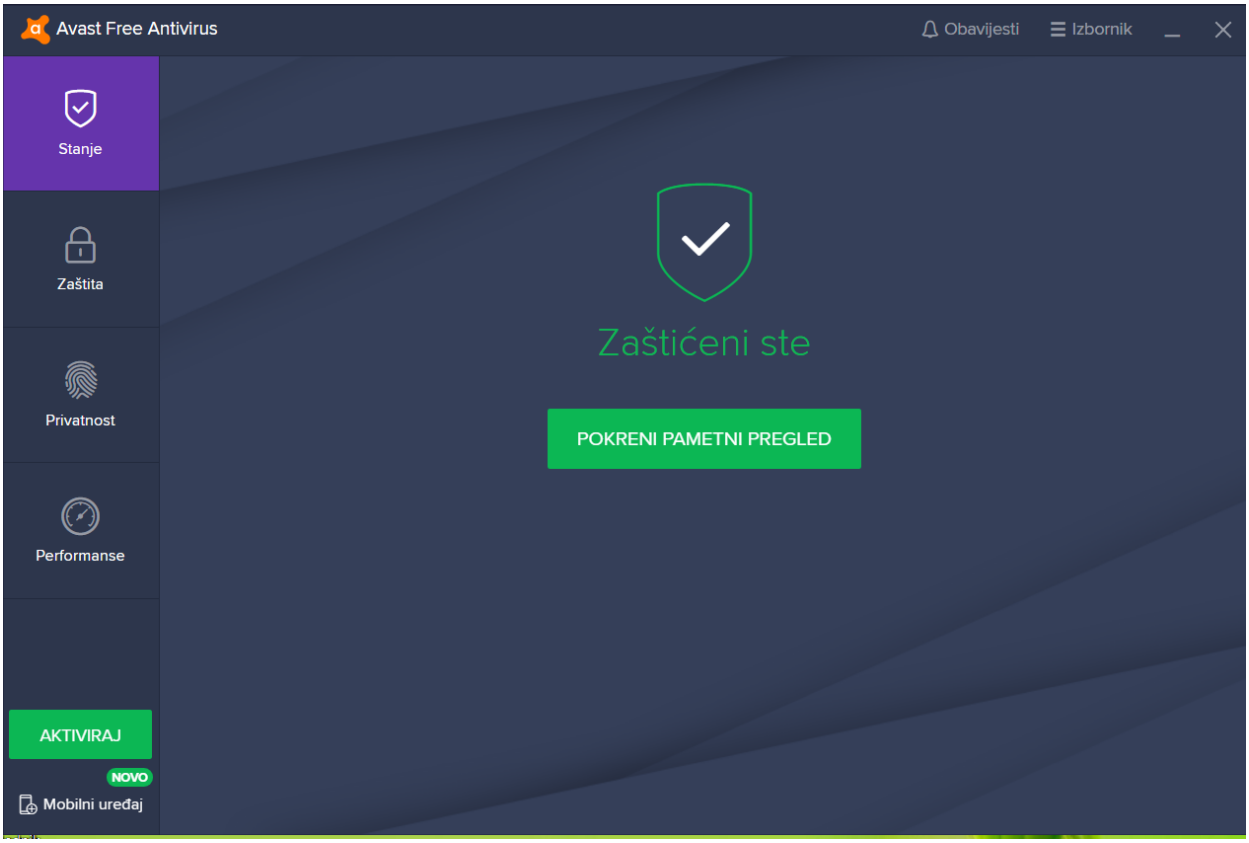
Prednosti:

- Jednostavnost korištenja
- Dobra zaštita od zlonamjernih softvera
- Niska cijena - ukoliko se odluči uzeti Avast Pro
- Snažne performanse
- Besplatna verzija

Mane:

- Ograničene značajke kao što je upravitelj lozinkom

Slika 4. Prikaz sučelja Avast Free Antivirus računalnog programa



3.1.3. Avira Free Antivirus

Avira antivirus koristi razne tehnike zaštite od najnovijih prijetnji. Ova verzija antivirusnog programa je uvijek besplatna i nudi vatrozid (eng. Firewall). Kao i ostali antivirusni programi Avira sprječava „napade“ zlonamjernih softvera, otkriva internetsku prijetnju prije nego što „inficira“ računalo te nudi niz drugih sigurnosnih značajki kao na primjer otkrivanje ranjivosti sustava. Uz sve to ima mogućnost identifikacije problema datoteke koja se preuzima na računalo. Avira ima sličnu značajku (eng. Gamer Mode) kao i antivirusni program Avast koja omogućuje blokiranje raznih ažuriranja, skeniranja i zaostajanja sustava prilikom korištenja

računalnih igara ili gledanja videozapisa i filmova. Ova značajka aktivira se automatski kada korisnik igra računalne igre ili gleda videozapise.

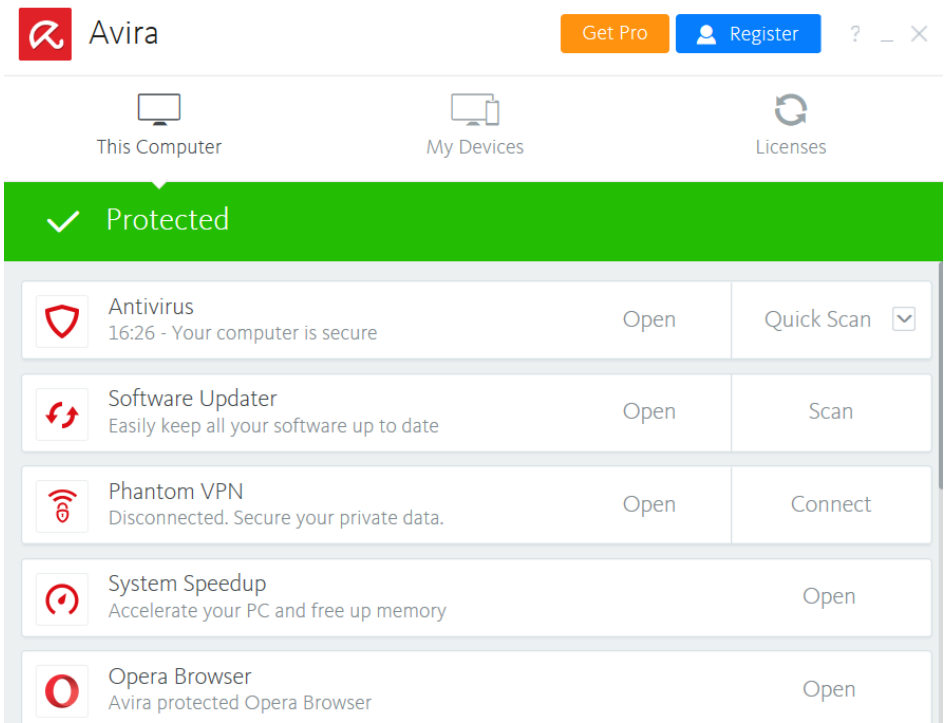
Prednosti:

- Prilagodljivost
- Jednostavnost korištenja
- Dobra zaštita od zlonamjernih softvera
- Brzina rada softvera

Mane:

- Besplatna verzija ne uključuje automatsko skeniranje poruka elektroničke pošte, preuzimanja i USB uređaja.

Slika 5. Prikaz sučelja Avira Free Antivirus računalnog programa



3.1.4. AVG Free Antivirus

AVG Free Antivirus je besplatna verzija antivirusnog programa koja ima sve očekivane značajke koje bi antivirusni program trebao sadržavati. Kao na primjer zaštita od virusa i drugih zlonamjernih programa, skeniranje elektroničke pošte, filtriranje Web stranica radi blokiranja zlonamjernih veza itd. Besplatna verzija nema raznih oglasa ili ograničenja koja bi natjerala korisnika da nadogradi odnosno kupi antivirusni program. Ovaj antivirusni program ima mogućnost brzog skeniranja (eng. Quick Scan) ili potpuno skeniranje sustava (eng. Deep Scan). Opcija rasporeda skeniranja (eng. Schedule Scan) može se koristiti za više prilagođenih skeniranja koja čini gotovo sve što korisnik poželi. Dakle, Mogu se pregledati određene datoteke ili mape tj. može se definirati koje datoteke i arhive treba pregledati, optimizacije performansi koje treba primijeniti itd. AVG isto kao i Avast nudi dodatni sigurni preglednik „AVG Secure Browser“ koji će omogućiti dodatnu zaštitu prilikom pretraživanja internetom.

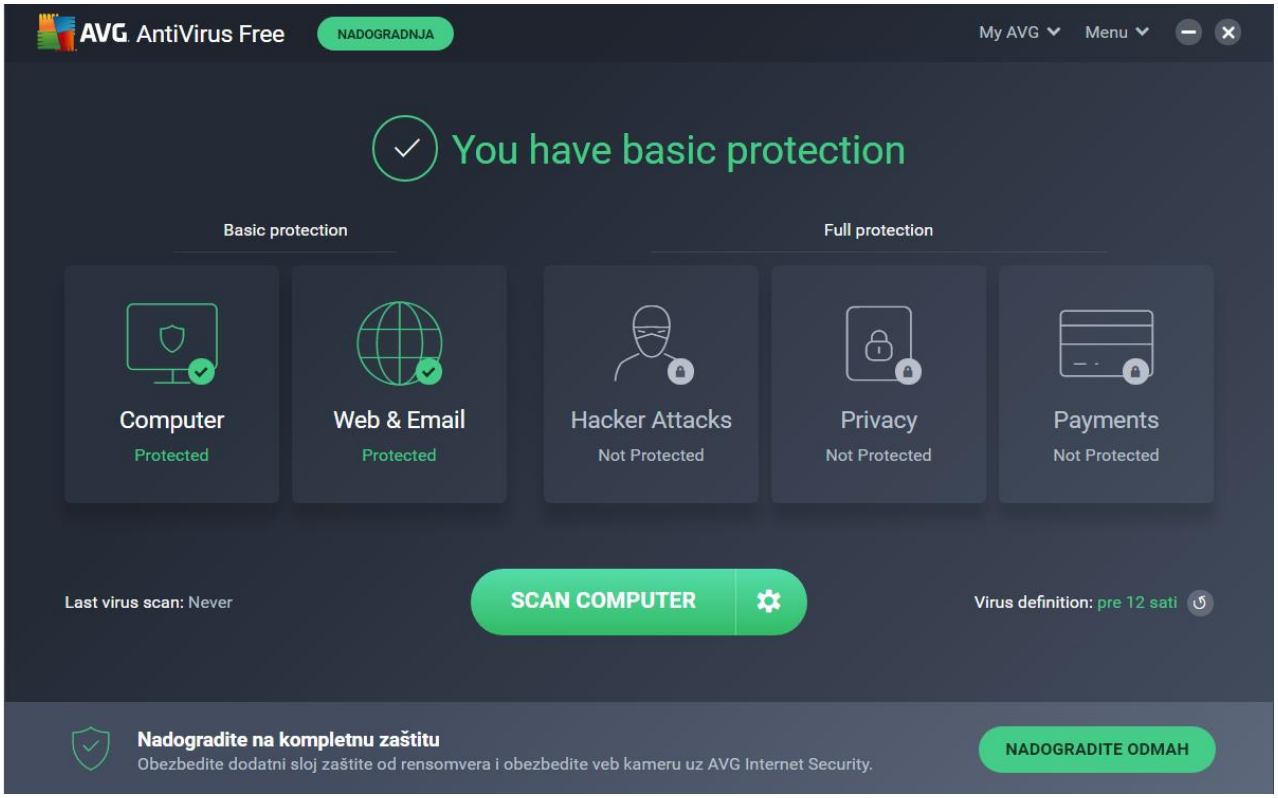
Prednosti:

- Vrlo dobra zaštita od zlonamjernih softvera
- Besplatne verzije za Windows, macOS i Android operacijske sustave
- Brzina rada i jednostavnost

Mane:

- Malo dodataka u usporedbi s ostalim antivirusnim programima
- Besplatna verzija nema vatrozid

Slika 6. Prikaz sučelja AVG Free Antivirus računalnog programa



3.1.5. Panda Free Antivirus

Panda Free Antivirus je besplatna verzija koja se uglavnom bazira na svoj osnovni antivirusni sustav bez posebnih dodataka. Moguće je skenirati prilagođeno, kritično i skeniranje cijelog sustava. Prilagođeno skeniranje omogućuje odabir samo ciljane mape, a skeniranja su vrlo brza i jednostavna. Kao i većina antivirusnih programa Panda ima značajke zaštite USB diska i zaštitu privatne mreže (VPN). Panda Free Antivirus ima dodatnu značajku (eng. Process Monitor) koja prikazuje procese koji su pokrenuti na računalu, ispisuje gdje su preuzeti, prikazuje njihov sigurnosni status, kada su se pojavili na računalu itd. Ovaj antivirusni program pruža dobru zaštitu, vrlo je jednostavan i pregledan za korištenje, no ne ističe se u odnosu na ostale konkurentne antivirusne programe.

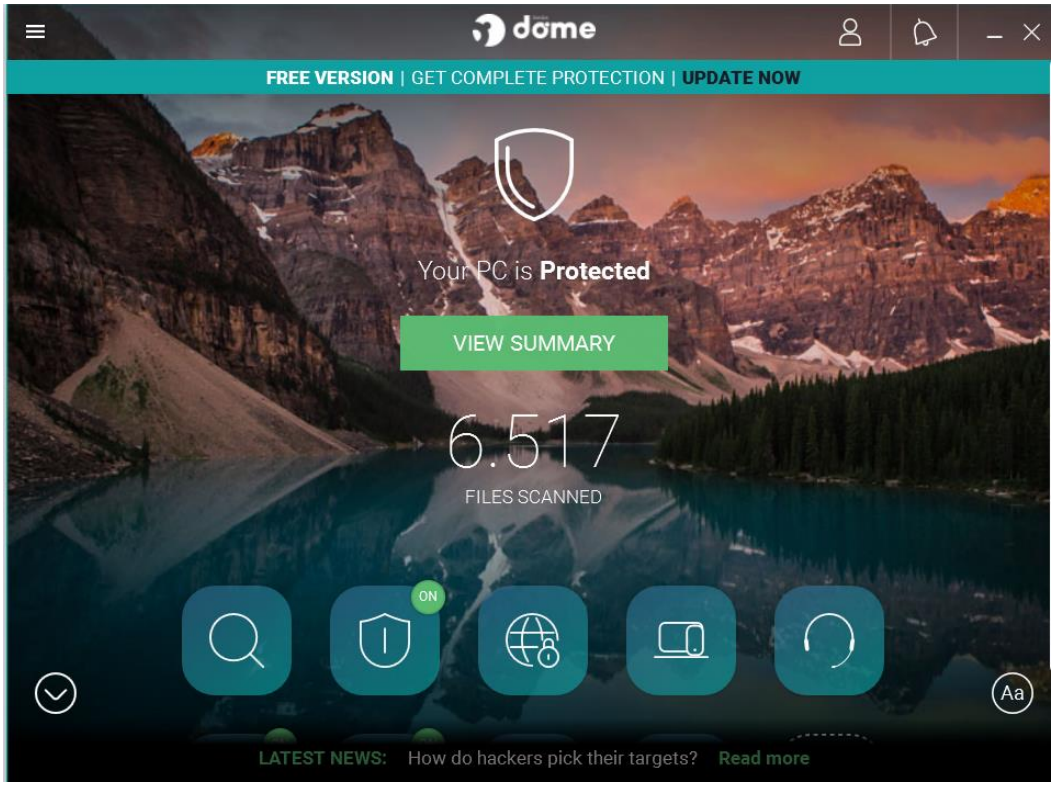
Prednosti:

- Dobra zaštita od zlonamjernih prijetnji
- Jednostavnost i brzina rada
- Dobro dizajnirano korisničko sučelje

Mane:

- Minimalni dodaci
- Prosječnost

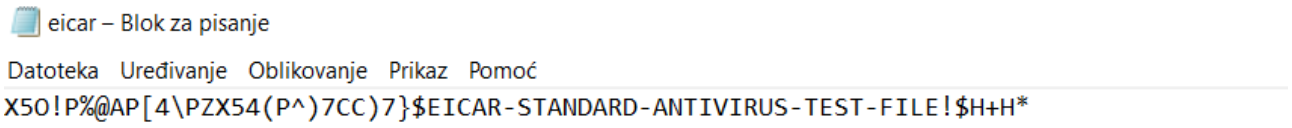
Slika 7. Prikaz sučelja Panda Free Antivirus računalnog programa



4. Testiranje antivirusnih programa

U ovom poglavlju opisati ću rezultate testiranja prethodno opisani besplatnih antivirusnih programa. Kako bi uspješno testirala antivirusne programe koristila sam testnu datoteku EICAR koja predstavlja zlonamjernu prijetnju. EICAR datoteku razvio je Europski institut koji se bavi istraživanjem računalnih virusa. Testna datoteka napravljena je kako bi se testirala reakcija antivirusnog programa na zlonamjernu prijetnju bez ugrožavanja računala stvarnim prijetnjama. EICAR testna datoteka nije virusi, niti sadrži ikakve dijelove virusnog koda.

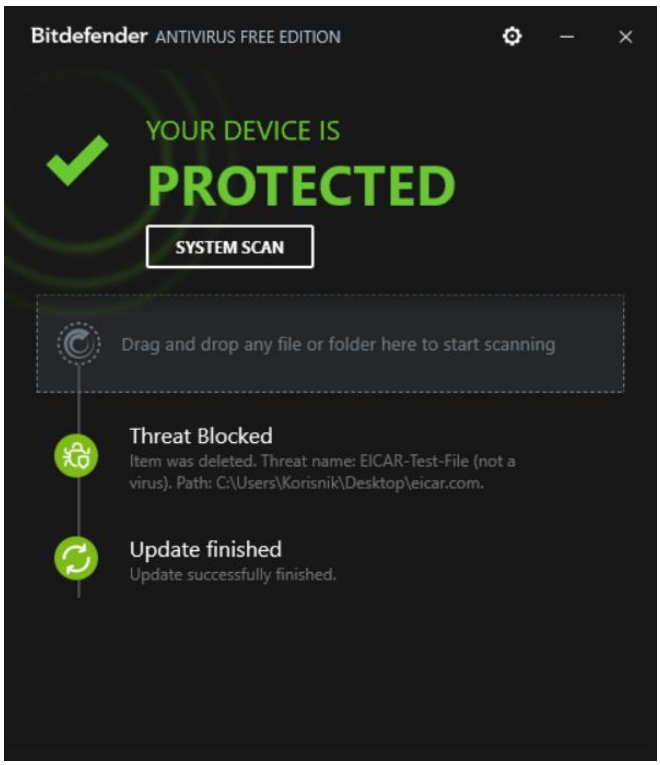
Slika 8. Eicar testna datoteka



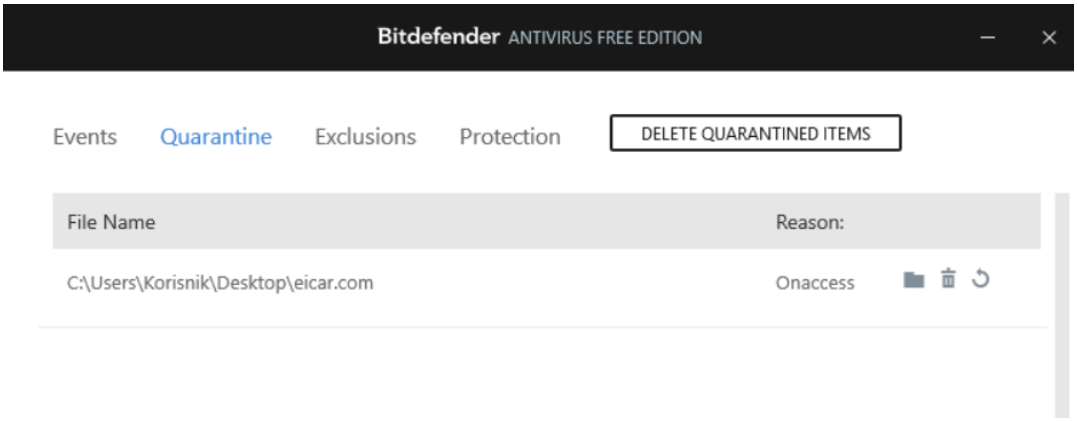
4.1. Testiranje Bitdefender Antivirus Free Edition računalnog programa

Kod testne datoteke EICAR napisala sam u programu „Blok za pisanje“ te sam ju spremila pod nazivom „eicar.com“. Kada sam to učinila antivirusni program Bitdefender odmah ju je prepoznao kao prijetnju. Automatski ju je izbrisao sa računala i stavio u izolaciju. Nakon toga sami odabiremo hoćemo li izbrisati datoteku iz izolacije ili ju tamo ostaviti. Kao što sam ranije opisala ukoliko se zlonamjernih softveri nalaze u izolaciji ne mogu naštetiti računalu. Isto tako ukoliko se ova testna datoteka preuzme sa Internet-a Bitdefender automatski će blokirati preuzimanje sa te stranice (sl.11.) ako ju ipak uspijemo preuzeti ponoviti će se postupak brisanja „prijetnje“. Bitdefender program odmah blokira zlonamjernu prijetnju prije nego što ona uspije inficirati računalo.

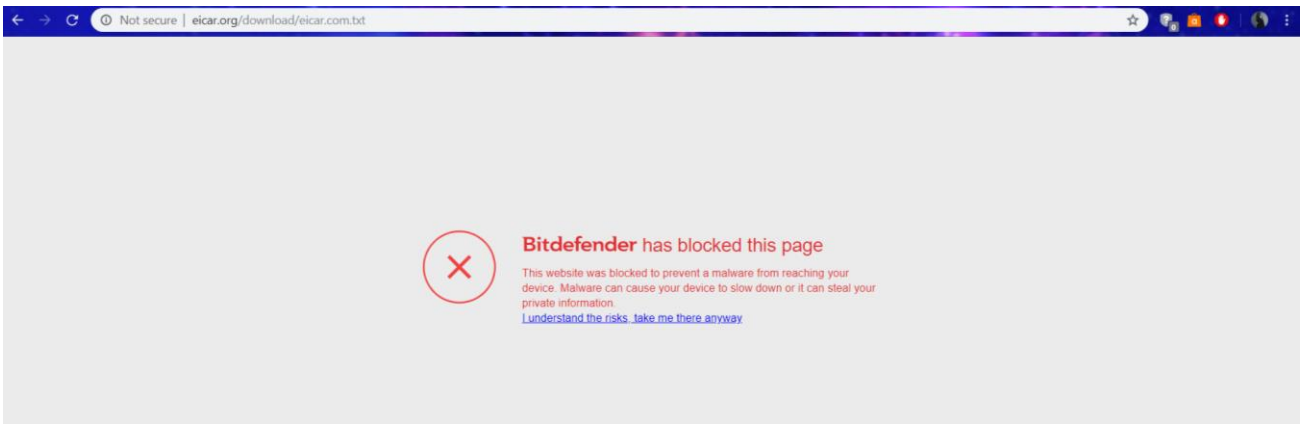
Slika 9. Detekcija i automatsko brisanje Eicar testne datoteke korištenjem Bitdefender Antivirus Free Edition antivirusnog programa



Slika 10. Prikaz testne datoteke EICAR u izolaciji



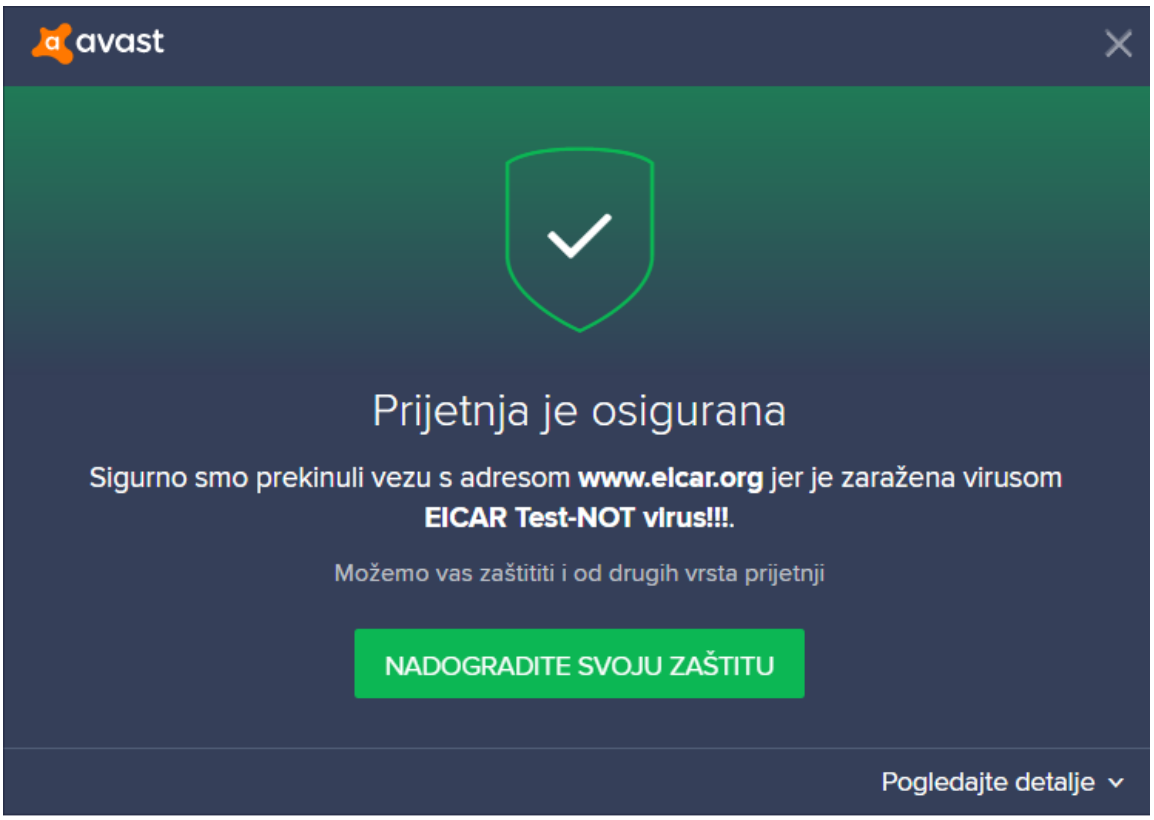
Slika 11. Prikaz blokirane stranice Bitdefender antivirusnim programom



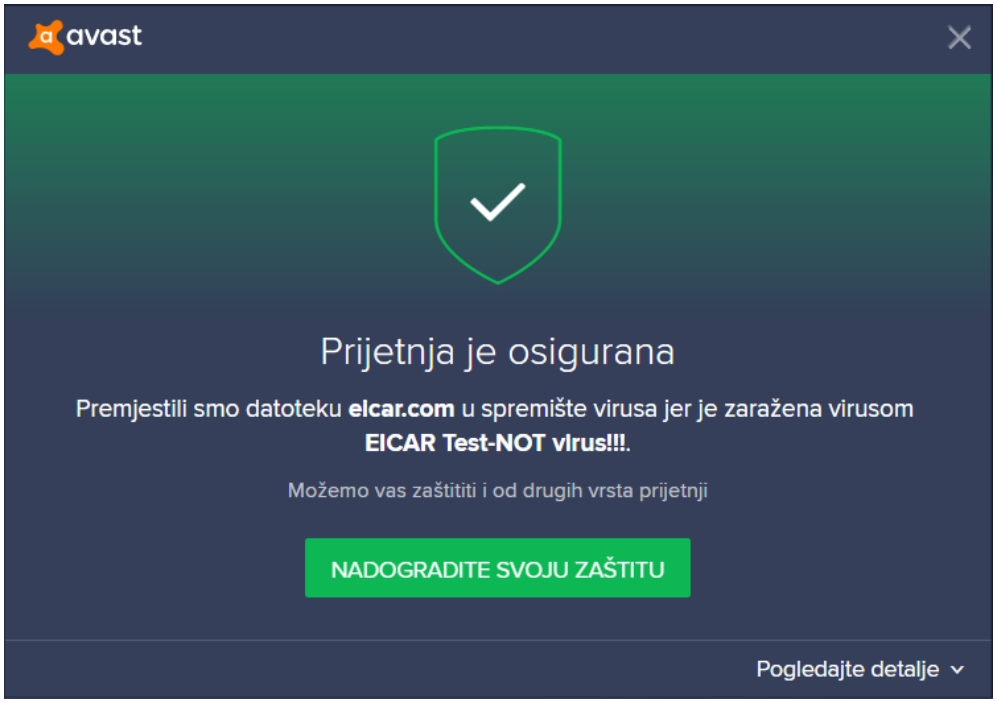
4.2. Testiranje Avast Free Antivirus računalnog programa

Kao i obično pokušala sam preuzeti Eicar testnu datoteku, no Avast antivirusni program automatski je blokirao radnju odnosno prekinuo preuzimanje i pokazao upozoravajuću poruku o sumnjivoj datoteci (sl. 12.). Kada sam se ipak odlučila sama kreirati testnu datoteku odnosno ubaciti kod testne datoteke u program „Blok za pisanje“, antivirusni program detektirao je prijetnju, obrisao ju te nakon toga premjestio u izolaciju gdje ju možemo sami obrisati (sl. 13. i 14.).

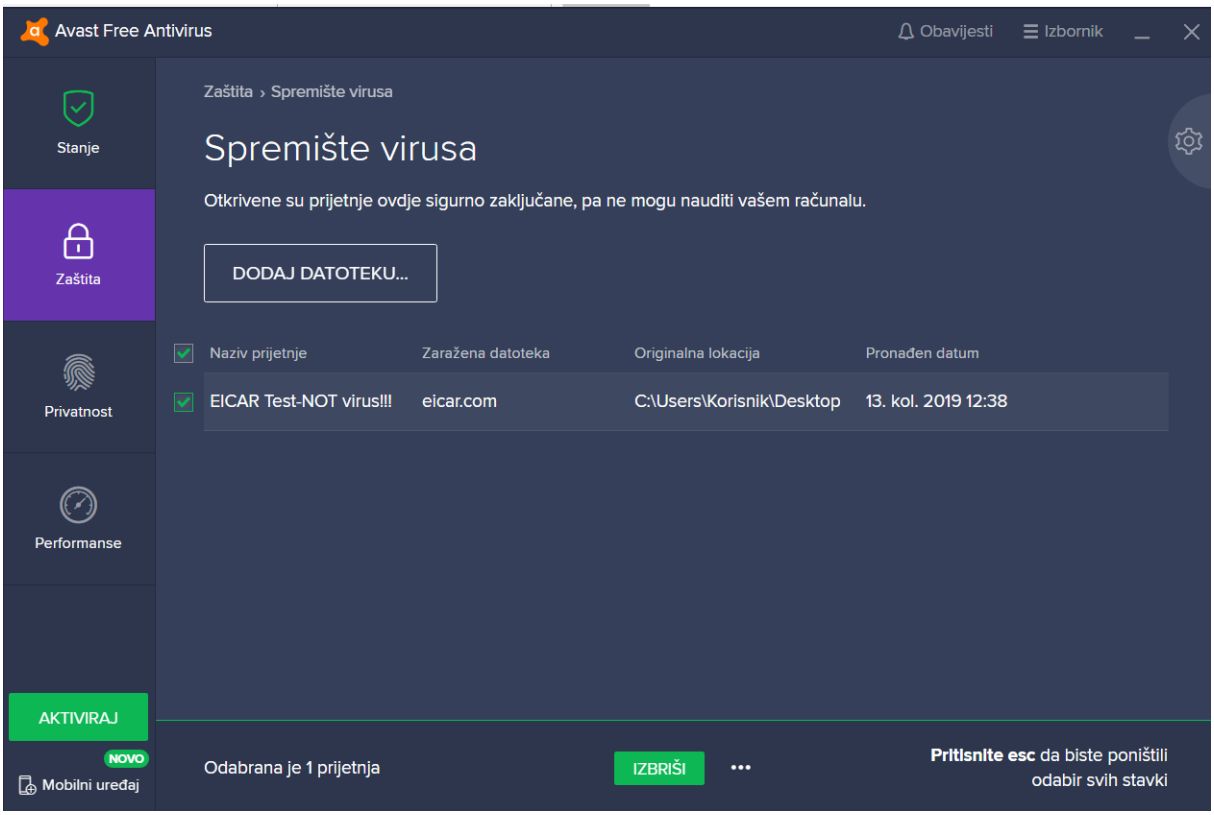
Slika 12. Detekcija EICAR datoteke Avast Free Antivirus računalnog programa



Slika 13. Detekcija i automatsko brisanje EICAR testne datoteke



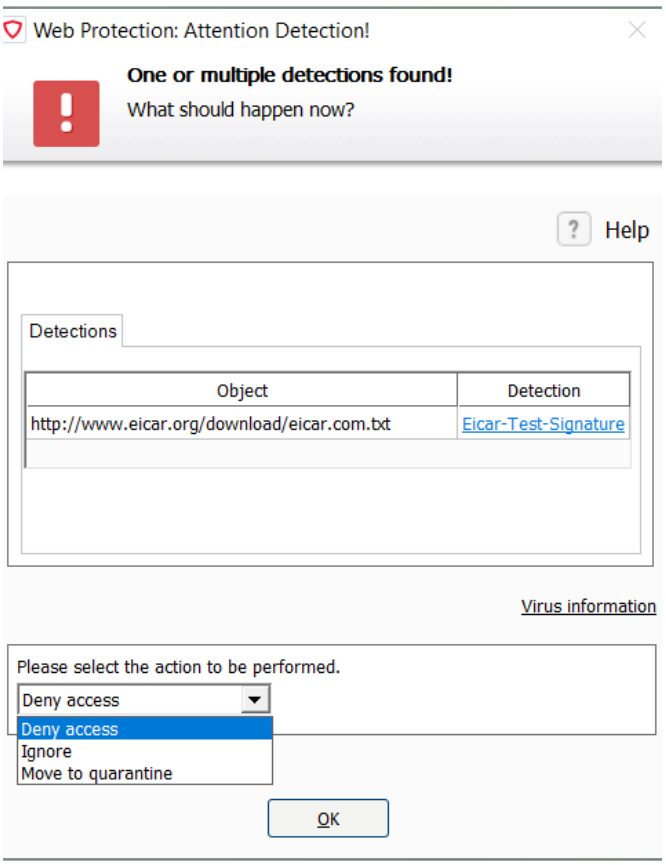
Slika 14. Prikaz testne datoteke EICAR u izolaciji



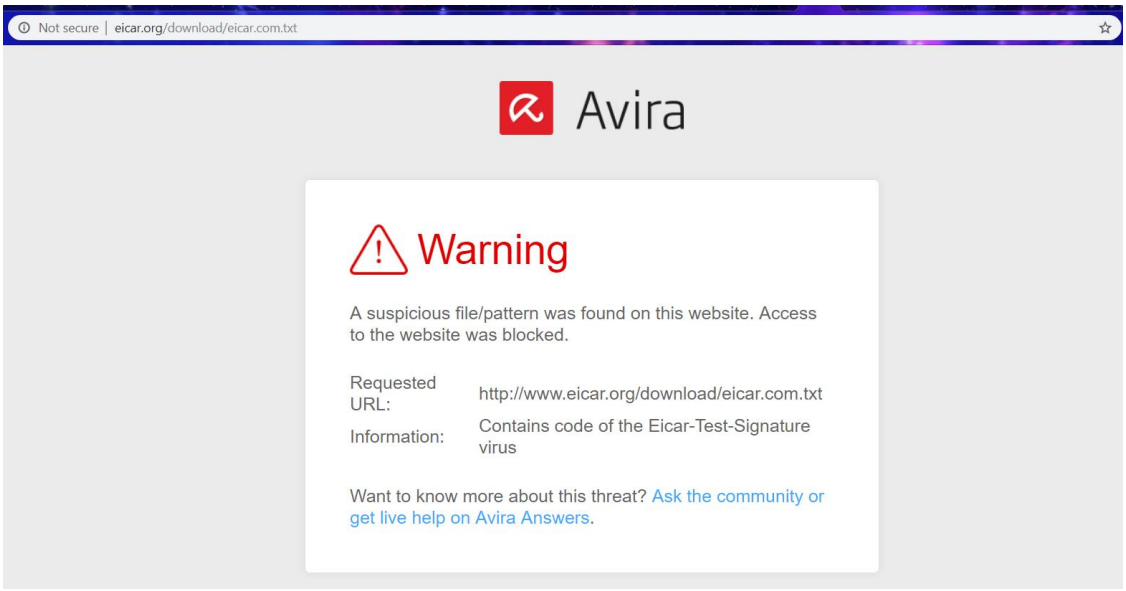
4.3. Testiranje Avira Free Antivirus računalnog programa

Prilikom preuzimanja testne datoteke pokazuje se upozoravajuća poruka sa detekcijom zlonamjerne prijetnje. Nakon toga imamo mogućnost odabrati hoćemo li „prijetnju“ ignorirati, premjestiti u izolaciju ili joj odbiti pristup.(sl.15.). Ako se odlučimo za odbijanje pristupa antivirus će izbaciti poruku na pregledniku stranice sa koje smo preuzeli testnu datoteku.(sl.16.). Ukoliko se ipak odlučimo premjestiti datoteku u izolaciju moći ćemo ju tamo izbrisati kao i kod Bitdefender i Avast antivirusnih programa. Ako se ipak odlučimo za ignoriranje prijetnje tada će nam se datoteka preuzeti na računalo što je opasno kada se radi o pravoj zlonamjernoj prijetnji što u ovom slučaju nije.

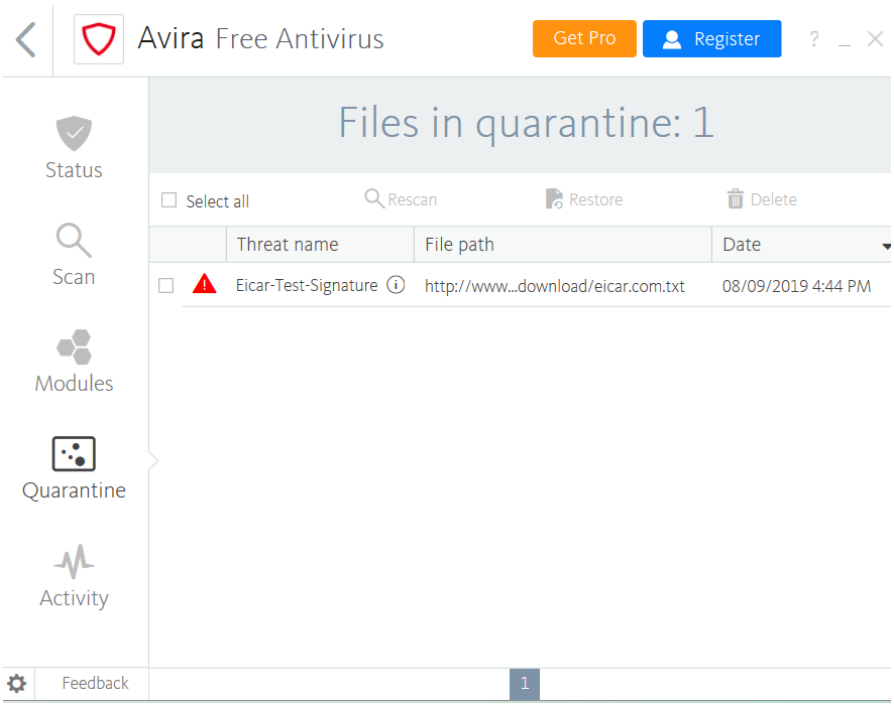
Slika 15. Detekcija Eicar testne datoteke korištenjem Avira Free antivirus računalnog programa



Slika 16. Prikaz blokirane stranice Avira antivirusnim programom



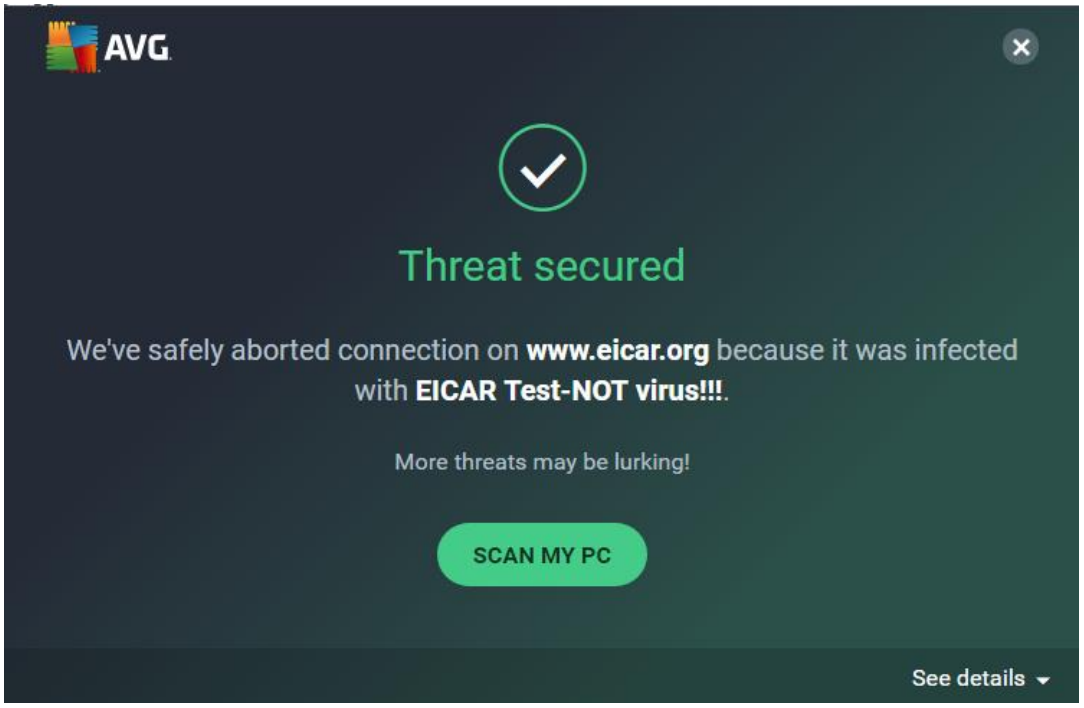
Slika 17. Prikaz testne datoteke EICAR u izolaciji



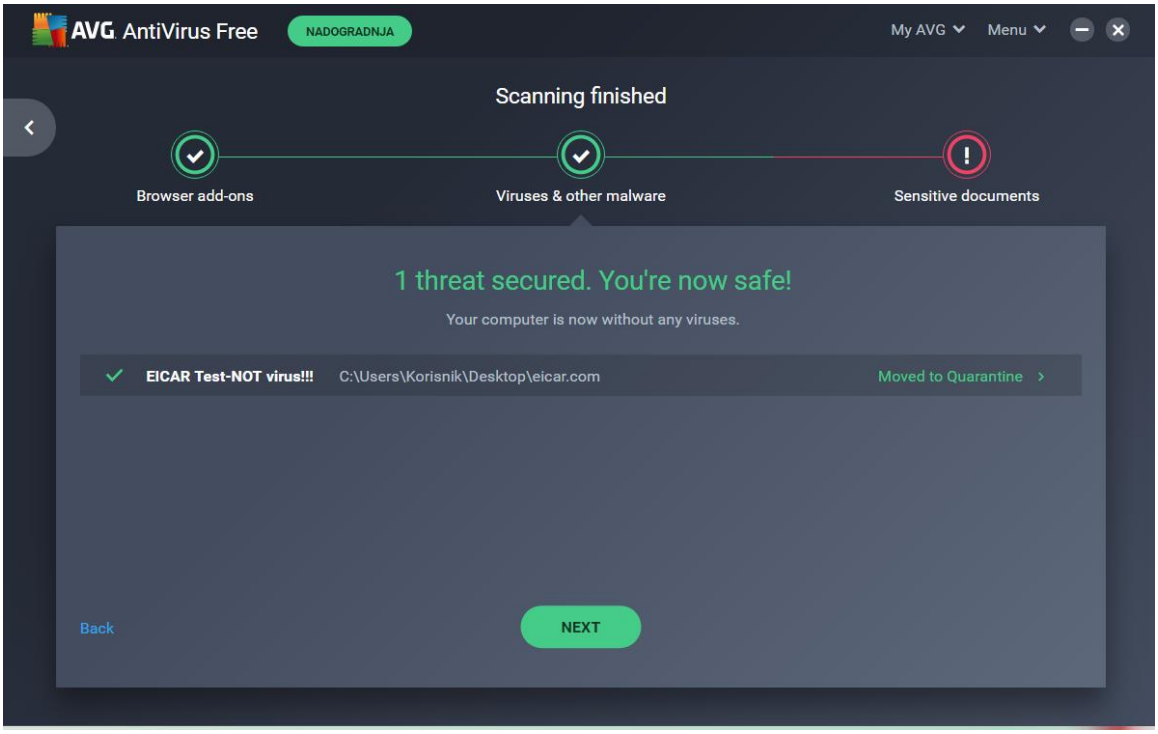
4.4. Testiranje AVG Free Antivirus računalnog programa

AVG Free Antivirus funkcionira na sličan način kao i Avast. Dakle, pokušala sam preuzeti Eicar testnu datoteku, no AVG antivirusni program automatski je blokirao radnju i pokazao upozoravajuću poruku, isto kao i Avast (sl. 18.). Također, upisala sam kod EICAR datoteke u „Blok za pisanje“ te je AVG detektirao prijetnju, obrisao ju i premjestio u izolaciju (sl.19. i 20.). Ovaj antivirusni program radi na sličan način kao prethodno testirani, no za razliku od Avira antivirusnog programa, AVG nije upitao što želim raditi sa datotekom, već ju je odmah blokirao.

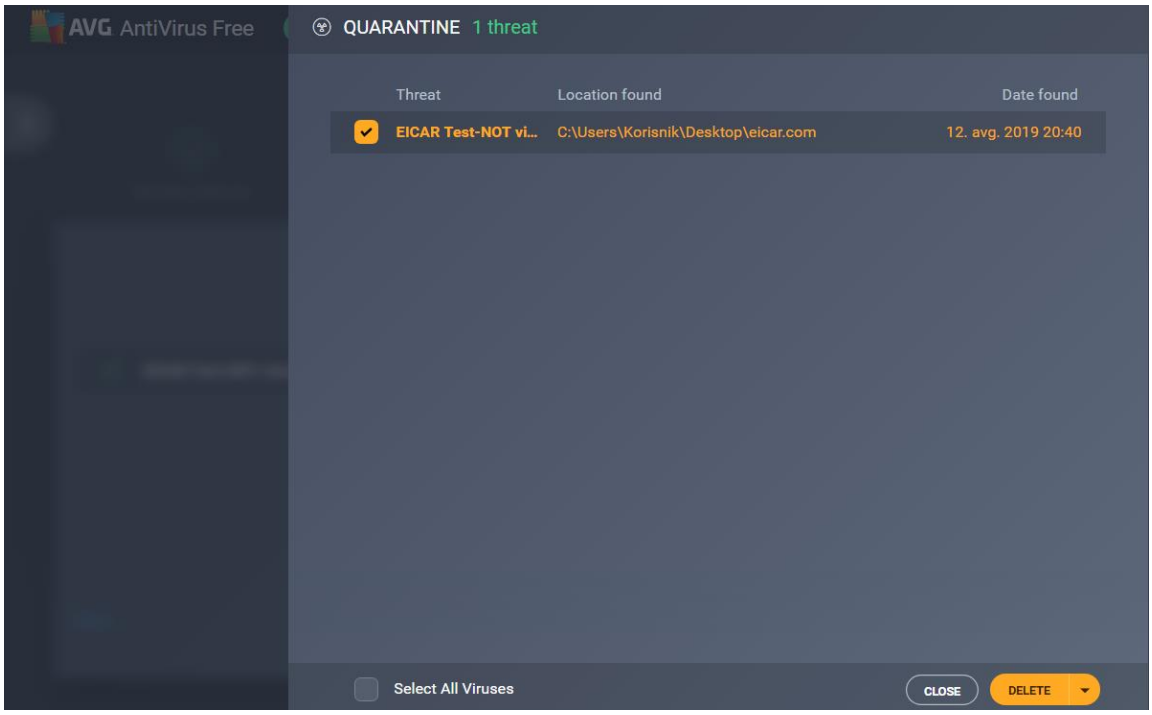
Slika 18. Detekcija i blokiranje preuzimanja testne datoteke korištenjem AVG Free Antivirus računalnog programa



Slika 19. Detekcija i brisanje testne datoteke



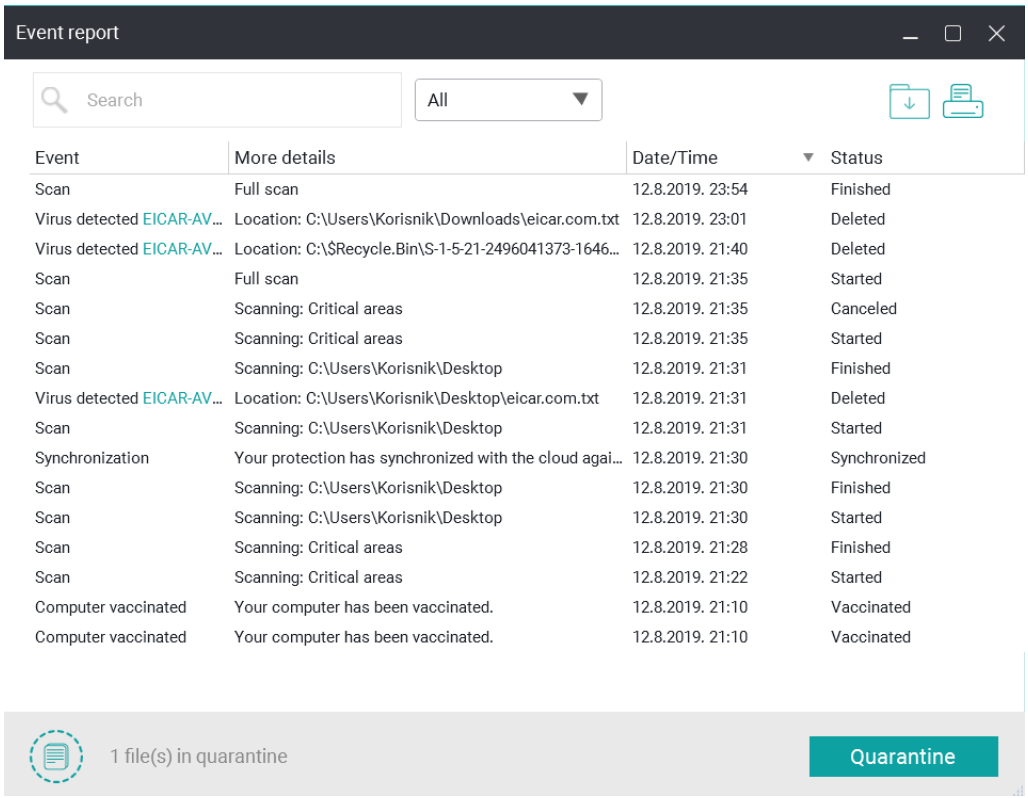
Slika 20. Prikaz testne datoteke EICAR u izolaciji



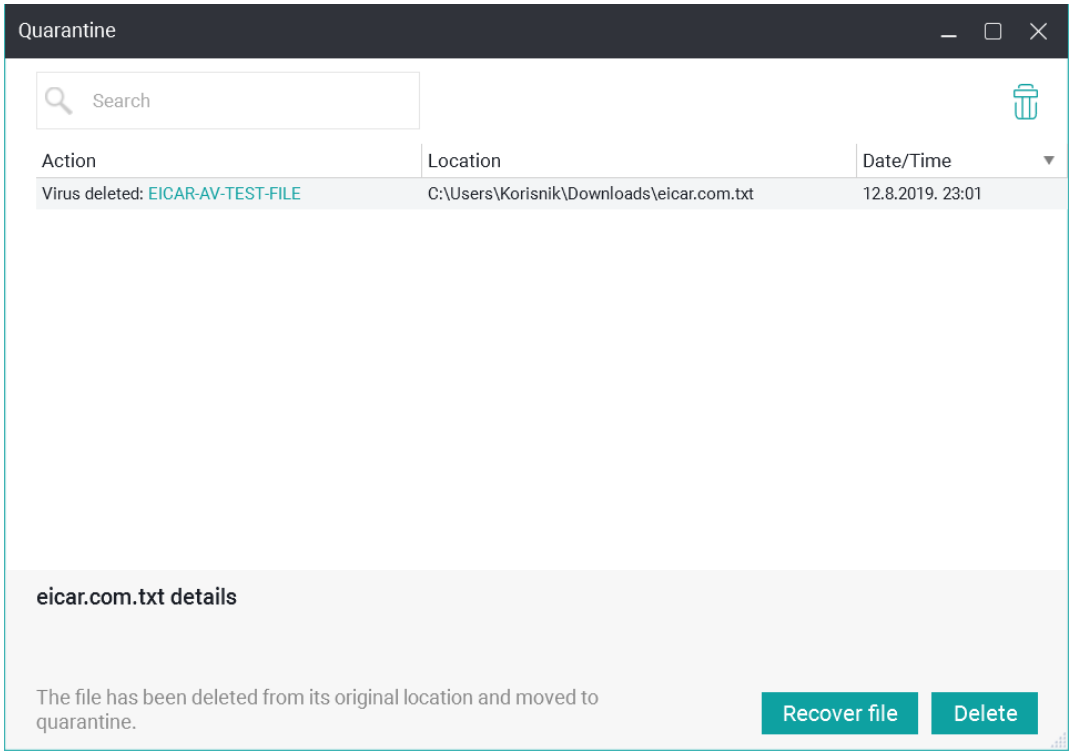
4.5. Testiranje Panda Free Antivirus računalnog programa

Prilikom preuzimanja EICAR testne datoteke Panda Free Antivirus nije blokirao preuzimanje ili pokazao upozoravajuću poruku kao kod prijašnjih primjera antivirusnih programa. Uspješno sam preuzela „zlonamjernu“ datoteku što nije bilo moguće prilikom testiranja prethodnih antivirusnih programa. Nakon preuzimanja testne datoteke pokrenula sam skeniranje cijelog sustava te je zatim Panda antivirusni program detektirao prijetnju. Nakon što ju je detektirao, automatski je izbrisao prijetnju i premjestio ju u izolaciju.

Slika 21. Detekcija testne datoteke Panda Free Antivirus računalnim programom



Slika 22. Prikaz testne datoteke EICAR u izolaciji



5. Zaključak

Računalni virusi su zlonamjerni programi koji mogu uzrokovati mnogo štete. Pod pojam „računalni virus“ smatraju se razni zlonamjerni programi koji jednako tako predstavljaju prijetnju i mogu naštetiti računalu. Tijekom godina broj virusa se drastično povećao, te je sve potrebnija adekvatna zaštita od njih. Kako bi se osigurala kvalitetna zaštita od virusa potrebno je instalirati antivirusni program koji osim zaštite od virusa pruža zaštitu i od drugih zlonamjernih prijetnji. Antivirusni program možemo koristiti i kao prevenciju te ga je potrebno redovno nadograđivati zbog nadolazećih novih prijetnji.

Testiranjem pet najpoznatijih besplatnih verzija antivirusnih programa uočila sam razne prednosti i mane. Iako svaki od njih pruža dobru zaštitu bitno se razlikuju. Kako bi ih uspješno testirala koristila sam testnu datoteku koja „oponaša“ virus bez ugrožavanja vlastitog računala. Svaki testirani antivirusni program spriječio je preuzimanje datoteke osim Panda Free Antivirus-a. Panda antivirus, za razliku od ostalih dopustio je preuzimanje, a testnu datoteku uočio je tek kada sam pokrenula skeniranje cijelog sustava. Ostali antivirusni programi automatski su blokirali, izbrisali ili premjestili testnu datoteku u izolaciju. Može se zaključiti da i besplatne verzije antivirusnih programa mogu pružati dovoljno dobru zaštitu i sigurnost na internetu uz jednostavnost korištenja.

Iako antivirusni programi mogu usporiti rad računala i dalje smatram da su neophodni te da ih treba koristiti svatko tko se svakodnevno služi internetom. Kao što sam ranije opisala virusi se najčešće šire internetom, a ponekad je dovoljno samo pristupiti nesigurnoj odnosno zlonamjernoj web stranici kako bismo „zarazili“ svoje računalo. Treba napomenuti da niti jedan sustav ne pruža stopostotnu zaštitu te treba izbjegavati sumnjive web stranice, poruke elektroničke pošte nepoznatih pošiljatelje, razne reklame, oglase i slične sadržaje.

Literatura

Knjige:

1. Ždrnja, B. (2003.) *Što su i kako rade virusi: (kako zaštititi i očistiti računalo od virusa, crva, trojanskih konja),* Zagreb: Bug [etc.]
2. Pavičić, T. (2005.) *Kako se boriti protiv neželjene pošte, virusa i špijunskih programa*, Zagreb: Mikro knjiga.

E- Knjige:

1. Walker, A. (2005.) *Absolute Beginner's Guide to Security, Spam, Spyware & Viruses, Indianapolis,* QUE Corporation, Dostupno na: O'Reilly, (pristupljeno 03. srpnja 2019.)
2. Szor, P. (2005.) *The Art of Computer Virus Research and Defense,* Addison-Wesley Professional, Dostupno na: O'Reilly, (pristupljeno 10. srpnja 2019.)
3. Gregory, P. (2004.)*Computer Viruses for dummies,* Indianapolis, Indiana: Wiley Publishing, Inc, Dostupno na: https://hxz.es/Computer%20Viruses%20for%20Dummies.pdf, (pristupljeno 10. srpnja 2019.)
4. Harley, D., Slade,R., Gattiker, U., (2001.) *Viruses Revealed*, Osborne, The McGraw-Hill Companies, Dostupno na: https://doc.lagout.org/network/1_Security/Virus%20Revealed.pdf, (pristupljeno 20. srpanj 2019.)
5. Ludwig, M. (1995.) *The GIANT Black Book of Computer Viruses,* Arizona: American Eagle Publications,Inc., Dostupno na: https://doc.lagout.org/security/Malware%20%26%20Forensics/The%20Giant%20Black%20Book%20of%20Computer%20Viruses.pdf, (pristupljeno 01. kolovoz 2019.)
6. Cohen, F. (1990.) *A Short Course on Computer Viruses*, Pittsburgh, Dostupno na: http://all.net/books/virus/SCVirusBook.pdf, (pristupljeno 28. lipanj 2019.)

Internetske stranice:

1. Information tehnology services, An Introduction to Computer Viruses, 2000, https://nnt.es/An%20Introduction%20to%20Computer%20Viruses.pdf, (pristupljeno 04. srpnja 2019.)
2. CERT.hr, O virusima, https://www.cert.hr/virusi, (pristupljeno 07. srpnja 2019.)
3. Avast, What is a computer worm, https://www.avast.com/c-computer-worm, (pristupljeno 04. srpnja 2019.)
4. Norton, Malware, What is a computer virus?, https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html, (pristupljeno 12. srpnja 2019.)
5. Tech-faq, The History of Computer Viruses, http://www.tech-faq.com/history-of-computer-viruses.html, (pristupljeno 15. srpnja 2019.)
6. MakeUseOf, Dan Price, The 10 best free antivirus software, 2019, https://www.makeuseof.com/tag/ten-best-antivirus-programs, (pristupljeno 03. kolovoz 2019.)
7. Tom's Guide Staff, Paul Wagenseil, Best Free Antivirus Software 2019, https://www.tomsguide.com/us/best-free-antivirus,review-6003.html , (pristupljeno 04. kolovoz 2019.)
8. VoIP Shield , Utmost Defense Against CyberAttack, Erika Hernandez, 20 Common Types of Viruses Affecting Your Computer, 2018, https://www.voipshield.com/20-common-types-of-viruses-affecting-your-computer, (pristupljeno 07. kolovoz 2019.)
9. Avast Free Antivirus, Tom Mcnamara, 2017, https://download.cnet.com/Avast-Free-Antivirus/3000-2239_4-10019223.html, (pristupljeno 05. kolovoz 2019.)
10. 3Com Corporation, “Network Security: A Simple Guide to Firewalls“, 2000, http://www.uky.edu/~dsianita/390/firewall1.pdf (pristupljeno 03. kolovoz 2019.)
11. AV-TEST-The Independent IT-Security Institute, „The best Windows antiviurs software for home users“, https://www.av-test.org/en/antivirus/home-windows (pristupljeno 01. kolovoz 2019.)
12. AV-TEST-The Independent IT-Security Institute, „The best Windows antiviurs software for MacOs users“, https://www.av-test.org/en/antivirus/home-macos/ (pristupljeno 01. kolovoz 2019.)

Popis slika

Slika 1. Virus prvog sektora 7
Slika 2. Primjer računalnog crva poslanog preko elektroničke pošte 11
Slika 3. Prikaz sučelja Bitdefender Antivirus Free Edition antivirusnog programa 18
Slika 4. Prikaz sučelja Avast Free Antivirus računalnog programa 20
Slika 5. Prikaz sučelja Avira Free Antivirus računalnog programa 21
Slika 6. Prikaz sučelja AVG Free Antivirus računalnog programa 23
Slika 7. Prikaz sučelja Panda Free Antivirus računalnog programa 24
Slika 8. Eicar testna datoteka 25
Slika 9. Detekcija i automatsko brisanje Eicar testne datoteke korištenjem Bitdefender Antivirus Free Edition antivirusnog programa 26
Slika 10. Prikaz testne datoteke EICAR u izolaciji 27
Slika 11. Prikaz blokirane stranice Bitdefender antivirusnim programom 27
Slika 12. Detekcija EICAR datoteke Avast Free Antivirus računalnog programa 28
Slika 13. Detekcija i automatsko brisanje EICAR testne datoteke 29
Slika 14. Prikaz testne datoteke EICAR u izolaciji 29
Slika 15. Detekcija Eicar testne datoteke korištenjem Avira Free antivirus računalnog programa 30
Slika 16. Prikaz blokirane stranice Avira antivirusnim programom 31
Slika 17. Prikaz testne datoteke EICAR u izolaciji 31
Slika 18. Detekcija i blokiranje preuzimanja testne datoteke korištenjem AVG Free Antivirus računalnog programa 32
Slika 19. Detekcija i brisanje testne datoteke 33
Slika 20. Prikaz testne datoteke EICAR u izolaciji 33
Slika 21. Detekcija testne datoteke Panda Free Antivirus računalnim programom 34
Slika 22. Prikaz testne datoteke EICAR u izolaciji 35

Popis tablica

Tablica 1. Rezultati testiranja Bitdenfender antivirusnog programa 16
Tablica 2. Rezultati testiranja Avast antivirusnog programa.....16
Tablica 3. Rezultati testiranja Avira antivirusnog programa 17

Izvori slika:

Slika 1. Virus prvog sektora
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1981886

Slika 2. Primjer računalnog crva poslanog preko elektroničke pošte
https://learning.oreilly.com/library/view/absolute-beginners-guide/0789734591/ch01.html

Izvori tablica:

Tablica 1. Rezultati testiranja Bitdenfender antivirusnog programa
https://www.av-test.org/en/antivirus/home-windows/
https://www.av-test.org/en/antivirus/home-macos/

Tablica 2. Rezultati testiranja Avast antivirusnog programa
https://www.av-test.org/en/antivirus/home-windows/
https://www.av-test.org/en/antivirus/home-macos/

Tablica 3. Rezultati testiranja Avira antivirusnog programa
https://www.av-test.org/en/antivirus/home-windows/
https://www.av-test.org/en/antivirus/home-macos/

Sažetak

Mnogi korisnici računala susreli su se u svom radu s nekom vrstom zlonamjernog softvera. Računalni virus ima sposobnost repliciranja u datotečni sustav i prenošenja sa računala na računalo uzrokujući veliku štetu. Virus se može širiti na razne načine kao što je privitak elektroničke pošte, web stranice, poveznice na društvenim mrežama, disketa, CD, DVD, USB uređaja isl. Pojavom prvih virusa pojavljuje se ubrzo i pojam antivirusni program. Antivirusni program može brzo detektira i ukloniti sve pronađene viruse sa računala. Većina antivirusnih programa prilagođena je različitim operacijski sustavima kao što su Windows, macOS, Android te svaki ima svoje prednosti i mane. Neki od najboljih antivirusnih programa za 2019. godinu su Bitdefender Antivirus Plus 2020, Norton AntiVirus Plus, ESET Internet Security, Kaspersky Anti-Virus, McAfee AntiVirus Plus itd. Iako antivirusni programi pružaju dobru zaštitu ipak poželjno je izbjegavati nesigurne web stranice i nepoznate i neočekivane poruke elektroničke pošte jer niti jedan alat ne pruža stopostotnu zaštitu. U okviru ovog završnog rada izvršeno je testiranje pet antivirusnih sustava kako bi se provjerila njihova zaštita; rezultati testiranja iznijeti su i komentirani u radu.

Ključne riječi: računalni virus , računalni crv , trojanski konj, zlonamjerni programi, širenje računalnih virusa, antivirusna zaštita, Avast, Avira, Bitdefender, AVG, Panda.

Summary

Many computer users have encountered some sort of malware in their work. The computer virus can replicate itself to the file system and transmit from computer to computer causing damage. The virus can spread in a variety of ways, such as email attachments, web pages, social media links, floppy disks, CDs, DVDs, USB devices, etc. With the advent of the first viruses, the term antivirus program soon emerges. An antivirus program can quickly detect and remove any viruses from your computer. Most antivirus programs are tailored to different operating systems such as Windows, macOS, Android, and each has its own advantages and disadvantages. Some of the best antivirus programs for 2019 are Bitdefender Antivirus Plus 2020, Norton AntiVirus Plus, ESET Internet Security, Kaspersky Anti-Virus, McAfee AntiVirus Plus, etc. Although anti-virus programs provide good protection, it is advisable to avoid unsafe websites and unknown and unexpected emails because neither tool provides one hundred percent protection. As part of this final paper, five antivirus systems were tested to verify their protection; test results are presented and commented on the paper.

Key words: computer virus, computer worm, trojan horse, malware, spreading, antivirus protection, Avast, Avira, Bitdefender, AVG, Panda.