Komparativna analiza antivirusnih programa

Nikolić, Krešimir

SVEUČILIŠTE U RIJECI
POMORSKI FAKULTET

KREŠIMIR NIKOLIĆ

KOMPARATIVNA ANALIZA ANTIVIRUSNIH PROGRAMA

ZAVRŠNI RAD

Rijeka, 2023

SVEUČILIŠTE U RIJECI
POMORSKI FAKULTET

KOMPARATIVNA ANALIZA ANTIVIRUSNIH PROGRAMA
COMPARATIVE ANALASYS OF ANTIVIRUS PROGRAMS

ZAVRŠNI RAD

Kolegij: Mikro i osobna računala
Mentor: izv. prof. dr. sc. Jasmin Ćelić
Student: Krešimir Nikolić
Studijski program: Elektroničke i informatičke tehnologije u pomorstvu
JMBAG: 0112077414

Rijeka, lipanj 2023

Student: Krešimir Nikolić
Studijski program: Elektroničke i informatičke tehnologije u pomorstvu
JMBAG: 0112077414

IZJAVA O SAMOSTALNOJ IZRADI ZAVRŠNOG RADA

Kojom izjavljujem da sam završni rad s naslovom **Komparativna analiza antivirusnih programa** izradio samostalno pod mentorstvom izv. prof. dr. sc. Jasmina Ćelića.

U radu sam primijenio/la metodologiju izrade stručnog/znanstvenog rada i koristio/la literaturu koja je navedena na kraju završnog rada. Tuđe spoznaje, stavove, zaključke, teorije i zakonitosti koje sam izravno ili parafrazirajući naveo/la u završnom radu na uobičajen, standardan način citirao/la sam i povezao/la s fusnotama i korištenim bibliografskim jedinicama, te nijedan dio rada ne krši bilo čija autorska prava. Rad je pisan u duhu hrvatskoga jezika.

Student

Krešimir Nikolić

Student: Krešimir Nikolić

Studijski program: Elektroničke i informatičke tehnologije u pomorstvu
JMBAG: 0112077414

IZJAVA STUDENTA – AUTORA
O JAVNOJ OBJAVI OBRANJENOG ZAVRŠNOG RADA

Izjavljujem da kao student – autor završnog rada dozvoljavam Pomorskom fakultetu Sveučilišta u Rijeci da ga trajno javno objavi i besplatno učini dostupnim javnosti u cjelovitom tekstu u mrežnom digitalnom repozitoriju Pomorskog fakulteta.

U svrhu podržavanja otvorenog pristupa završnim radovima trajno objavljenim u javno dostupnom digitalnom repozitoriju Pomorskog fakulteta, ovom izjavom dajem neisključivo imovinsko pravo iskorištavanja bez sadržajnog, vremenskog i prostornog ograničenja mog završnog rada kao autorskog djela pod uvjetima Creative Commons licencije CC BY Imenovanje, prema opisu dostupnom na http://creativecommons.org/licenses/

Student 

Krešimir Nikolić

Sažetak

Primarni cilj ovog istraživanja je provesti sveobuhvatnu procjenu antivirusnih softvera. Ovaj rad ima za cilj istaknuti stalnu prisutnost i stalno razvijajuću prirodu sigurnosnih prijetnji u računalnoj infrastrukturi, naglašavajući potrebu za povećanjem svijesti. Ispitivanjem metoda i tehnika napada, cilj je pokazati kako se prijetnje mogu identificirati, klasificirati i rangirati analizom rizika te omogućujući pravovremene i učinkovite obrambene strategije. Istraživanje je usmjereno na optimizaciju sustava zaštite analizom strukture, učinkovitosti i prikladnosti različitih antivirusnih programa unutar specifičnih računalnih okruženja. Prikazujući ilustrativne primjere, radom se ocjenjuje uspješnost ovih programa. Zaključno, uspoređuje se učinkovitost pojedinih antivirusnih programa za različite vrste zlonamjernih prijetnji te se istražuju i preporučuju optimalna rješenja.

KLJUČNE RIJEČI: antivirusni programi, sigurnosne prijetnje, komparativna analiza, analiza rizika, optimizacija sustava zaštite

Summary

The primary objective of this research is to conduct a comprehensive assessment of antivirus software. This study aims to highlight the ongoing presence and ever-evolving nature of security threats in computer infrastructure, emphasizing the need for increased awareness. By examining attack methods and techniques, the goal is to demonstrate how threats can be identified, classified, and ranked through risk analysis, enabling timely and efficient defense strategies. The research focuses on optimizing the protection system by analyzing the structure, effectiveness, and suitability of various antivirus programs within specific computer environments. By presenting illustrative examples, the study evaluates the performance of these programs. In conclusion, the effectiveness of individual antivirus programs is compared across different types of malicious threats, and optimal solutions are explored and recommended.

KEYWORDS: antivirus programs, security threats, comparative analysis, risk analysis, protection system optimization

SADRŽAJ

1. Uvod **1**

2. Sigurnosne prijetnje u računalnom svijetu **1**

2.1. Definicija sigurnosnih prijetnji 2

2.2. Vrste sigurnosnih prijetnji 2

2.2.1. Fizički zasnovane prijetnje 3

2.2.2. Web bazirane prijetnje 4

2.2.3. Mrežno zasnovane prijetnje 5

2.2.4. Društveni inžinjering 6

2.2.5. Krađa identiteta 7

2.2.6 Aplikacijski bazirane prijetnje 8

2.3 Računalni virusi 9

2.3.1 Tipovi računalnih virusa 9

2.3.2. Pet načina kako se računalni virusi sakrivaju 11

2.3.2.1. Samomodifikacija 11

2.3.2.2. Enkripcija 12

2.3.2.3. Polimorfni virusi 12

2.3.2.4. Metamorfni virusi 13

2.4. Računalni crvi 13

2.4.1. Princip rada računalnih crva 14

2.4.2 Razlike između crva i virusa 14

2.4.3. Struktura računalnog crva 15

2.4.3.1. Lokator cilja 15

2.4.3.2. Propagatori infekcije 16

2.4.3.3. Tehnike izvođenja koda 16

2.5. Trojanski konji 17

2.5.1. Tri najpoznatija oblika trojanaca 18

2.5.1.1. Zeus 18

2.5.1.2. Spyeye 18

2.5.1.3. Emotet 19

2.5.2. Zaštite od trojanaca 19

3. Antivirusni programi **21**

3.1. Detekcija računalnih prijetnji 21

3.1.1. Detekcija na temelju potpisa 21

3.1.2. Checksumming 22

3.1.3. Popis dopuštenih aplikacija 22

3.2. Uklanjanje prijetnji 22

3.3. Primjeri antivirusnih programa 23
3.3.1. Avast 23
3.3.2 AVG 25
3.3.3. Bitdefender 25
3.3.4. Avira 27
4. Usporedba rada antivirusnih programa 28
4.1. Testiranje Avast antivirusnog programa 29
4.2. Testiranje AVG antivirusnog programa 30
4.3. Testiranje Bitdefender antivirusnog programa 32
4.4. Testiranje Avira antivirusnog programa 35
Zaključak 38
Literatura 39

1. Uvod

U današnjem digitalnom dobu koji se brzo razvija, važnost snažnih mjera kibernetičke sigurnosti ne može se precijeniti. Sa sve većim brojem sigurnosnih prijetnji koje vrebaju u virtualnom svijetu, zaštita računalne infrastrukture postala je najveća briga. Kao rezultat toga, učinkovitost antivirusnih programa u borbi protiv ovih prijetnji privukla je značajnu pozornost. Ovaj rad zadire u područje antivirusnih programa, predstavljajući sveobuhvatnu komparativnu analizu koja ima za cilj rasvijetliti njihove različite mogućnosti i prikladnost u različitim računalnim okruženjima. Ispitivanjem dinamičke prirode sigurnosnih prijetnji i njihovih metoda napada koje se razvijaju, ovo istraživanje nastoji podići svijest o stalnoj prisutnosti rizika i potrebi za proaktivnom obranom.

Primarni cilj ovoga rada je pružiti pronicljivo istraživanje prepoznavanja, klasifikacije i rangiranja prijetnji kroz analizu rizika. Čineći to, mogu se identificirati učinkovite obrambene strategije i osigurati pravovremeno ublažavanje potencijalnih ranjivosti. Optimizacija zaštitnog sustava postaje ključni aspekt koji zahtijeva temeljito razumijevanje struktura antivirusnog programa i njihovih odgovarajućih funkcionalnosti. Kroz detaljan pregled različitih antivirusnih programa, ovaj rad koristi ilustrativne primjere za procjenu njihove učinkovitosti i prikladnosti unutar specifičnih računalnih okruženja. Oslanjajući se na scenarije iz stvarnog svijeta, cilj je ponuditi sveobuhvatnu procjenu koja razmatra višestruke aspekte zaštite od zlonamjernih prijetnji.

U konačnici, ova komparativna analiza pomno ispituje izvedbu pojedinačnih antivirusnih programa protiv različitih vrsta sigurnosnih prijetnji. Istražujući njihove jake i slabe strane, nastojimo identificirati najpouzdanija i najučinkovitija rješenja za borbu protiv rastućih rizika, čime se unapređuje sveukupna razina kibernetičke sigurnosti.

2. Sigurnosne prijetnje u računalnom svijetu

Uz rastuću prisutnost mobilnih telefona, prijenosnih i stolnih računala i sličnih uređaja, baza korisnika računala nastavlja se širiti velikom brzinom. Nažalost, ovaj skok u korištenju računala popraćen je paralelnim porastom broja neželjenih programa i kibernetičkih napada. Kada je u pitanju računalna sigurnost, primarni problem proizlazi iz rasprostranjenosti zlonamjernih programa koji predstavljaju značajnu prijetnju korisnicima.

2.1. Definicija sigurnosnih prijetnji

Zlonamjerni programi, poznati i kao zlonamjerni softver, odnose se na softver koji je namjerno dizajniran za nanošenje štete, ometanje operacija ili dobivanje neovlaštenog pristupa računalnim sustavima. Ovi programi obuhvaćaju različite oblike, kao što su virusi, crvi, trojanci, ransomware i spyware, te predstavljaju značajan rizik za integritet, povjerljivost i dostupnost digitalnih podataka.

Učinkovita zaštita od zlonamjernih programa od iznimne je važnosti u današnjem međusobno povezanom digitalnom krajoliku. Sa sve većim oslanjanjem na tehnologiju i eksponencijalnim rastom kibernetičkih prijetnji, zaštita računalnih sustava i mreža ključna je za sprječavanje neovlaštenog pristupa, povrede podataka, financijskih gubitaka, invazije na privatnost i štete po ugled. Snažne mjere zaštite, uključujući ažurirani antivirusni softver, vatrozid i svijest korisnika, bitne su za ublažavanje ovih rizika i osiguranje sigurnog računalnog okruženja.

Sigurnosna prijetnja odnosi se na svaki potencijalni događaj, aktivnost ili stanje koje može ugroziti povjerljivost, integritet ili dostupnost računalnih sustava, mreža ili podataka. Ove prijetnje mogu potjecati iz različitih izvora, uključujući zlonamjerne aktere, ranjivosti u softveru ili hardveru, taktike društvenog inženjerstva i vanjske čimbenike kao što su prirodne katastrofe. Sigurnosne prijetnje obuhvaćaju širok raspon rizika, uključujući neovlašteni pristup, povrede podataka, napade uskraćivanjem usluge, infekcije zlonamjernim softverom i curenje informacija, naglašavajući potrebu za proaktivnim mjerama za prepoznavanje, sprječavanje i ublažavanje ovih rizika.

2.2. Vrste sigurnosnih prijetnji

Vrste sigurnosnih računalnih prijetnji imaju različite izvore i oblike te ih prema tome možemo svrstati na [1][2]:

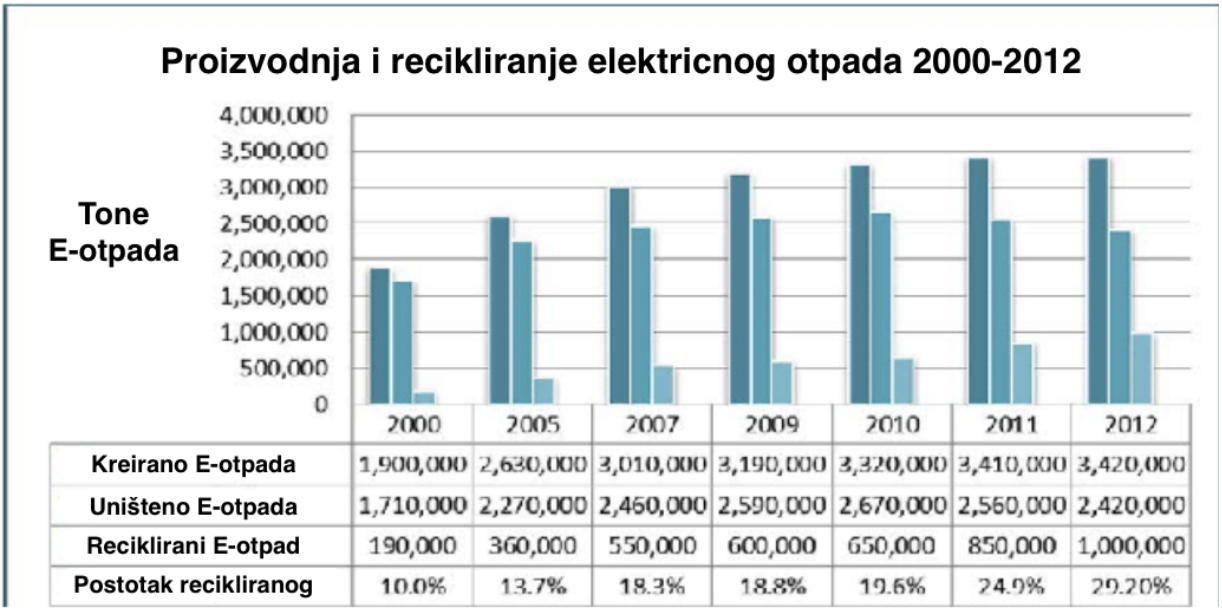
- Fizički zasnovane prijetnje
- Web bazirane prijetnje
- Mrežno zasnovane prijetnje
- Društveni inžinjering
- Krađa identiteta
- Aplikacijski bazirane prijetnje

2.2.1. Fizički zasnovane prijetnje

Fizičke prijetnje obuhvaćaju različite oblike otuđivanja, uključujući krađu ili neovlašteno posuđivanje osobnih uređaja. Krađa podrazumijeva protupravno stjecanje pokretne ili nepokretne imovine, što često rezultira materijalnom štetom. Međutim, posljedice se protežu izvan fizičkih gubitaka, budući da podaci, privatni dokumenti i pristup povjerljivim informacijama mogu pasti u ruke neovlaštenih osoba, ugrožavajući povjerljivost podataka - vitalni sigurnosni zahtjev za računalne sustave.

Prijenosna računala su zbog svoje prenosivosti posebno osjetljiva na krađu u usporedbi sa stolnim računalima. Inherentna mobilnost prijenosnih računala povećava njihovu izloženost fizičkim prijetnjama. Štoviše, fizički utemeljene prijetnje proširuju se i na napade na uređaje namijenjene recikliranju, pri čemu je recikliranje elektroničkog otpada posljednjih godina u stalnom porastu.

Imperativ je pozabaviti se ovim fizičkim ranjivostima i ojačati zaštitne mjere za zaštitu od potencijalnih kršenja, osiguravajući sigurnost i povjerljivost osjetljivih informacija u svijetu koji je sve više povezan.



Slika 1. Količina recikliranog otpada kroz godine [4]

2.2.2. Web bazirane prijetnje

Web bazirane prijetnje mogu se podjeliti u 3 kategorije [2]:

- *Phishing* napadi
- Iskoristavanje internetskog preglednika
- Automatsko preuzimanje aplikacija

Phishing uključuje online prijevarne aktivnosti u kojima se lažne poruke e-pošte, koje naizgled potječu od autentičnih entiteta kao što su banke, vladina tijela ili platforme za e-trgovinu, koriste kako bi se primatelji prevarili da otkriju osobne, financijske ili sigurnosne podatke. Kao posljedica toga, prevaranti mogu dobiti korisnička imena i lozinke ili podatke s kreditnih kartica. U takvim e-porukama od osoba se najčešće traži da preuzmu priloženi dokument ili da kliknu na poveznicu. *Phishing* napadi se mogu prepoznati po sljedećim obilježjima [5]:

- Sadržaj poruke je veoma primamljiv (npr. dobitak vrijedne nagrade)
- Napadač ističe hitnoću ili važnost u samom predmetu poruke

- U predmetu se nalazi poveznica sa kojom bi potencijalna žrtva trebala "potvrditi identitet" ili "ažurirati aplikaciju"
- Sa porukom najcesce dolazi i privitak koji je zapravo maliciozan program

Otmičar preglednika je neželjeni program koji se obično pojavljuje kao dodatak pregledniku ili "plug-in", što rezultira izmjenama postavki odabranog web preglednika. Ovi programi pokreću svoje radnje mijenjanjem početne stranice, zadane tražilice i postavki nove kartice. Nakon što se te promjene izvrše, otmičar preglednika ima mogućnost preusmjeravanja korisnika na određene web stranice u pokušaju povećanja njihove popularnosti. Promovirajući te web stranice i generirajući više internetskog prometa i posjetitelja, programeri otmičara preglednika zarađuju novac. Međutim, važno je napomenuti da se ne može jamčiti da su sva promovirana mjesta legitimna i sigurna.

Većina otmičara preglednika sposobna je prikupiti podatke o korisnikovim navikama pregledavanja. Ovi programi mogu pratiti pojmove za pretraživanje koje osoba koristi, često posjećene stranice, učitane datoteke, unesene informacije i slične podatke. Ove informacije klasificirane su kao osobni podaci koji ne otkrivaju identitet. [6]

Kada korisnik posjeti web stranicu, postoje slučajevi u kojima dolazi do automatskog preuzimanja aplikacije. U nekim slučajevima korisnik mora poduzeti određene radnje ili slijediti određene postupke kako bi otvorio preuzetu aplikaciju. S druge strane, u određenim situacijama zahtjev za preuzimanje aplikacije može se pokrenuti automatski bez intervencije korisnika. [2]

2.2.3. Mrežno zasnovane prijetnje

Mrežno zasnovane prijetnje se mogu podijeliti u dvije skupine [2]:

- Napade podvalom mreže
- Iskorištavanje mreže

Napad podvalom mreže ili "*spoofing*" je čin prikrivanja komunikacije ili identiteta tako da se čini da je povezan s pouzdanim, ovlaštenim izvorom. Napadi podvalom mogu imati mnoge oblike, od uobičajenih napada lažiranja e-pošte koji se koriste u kampanjama krađe

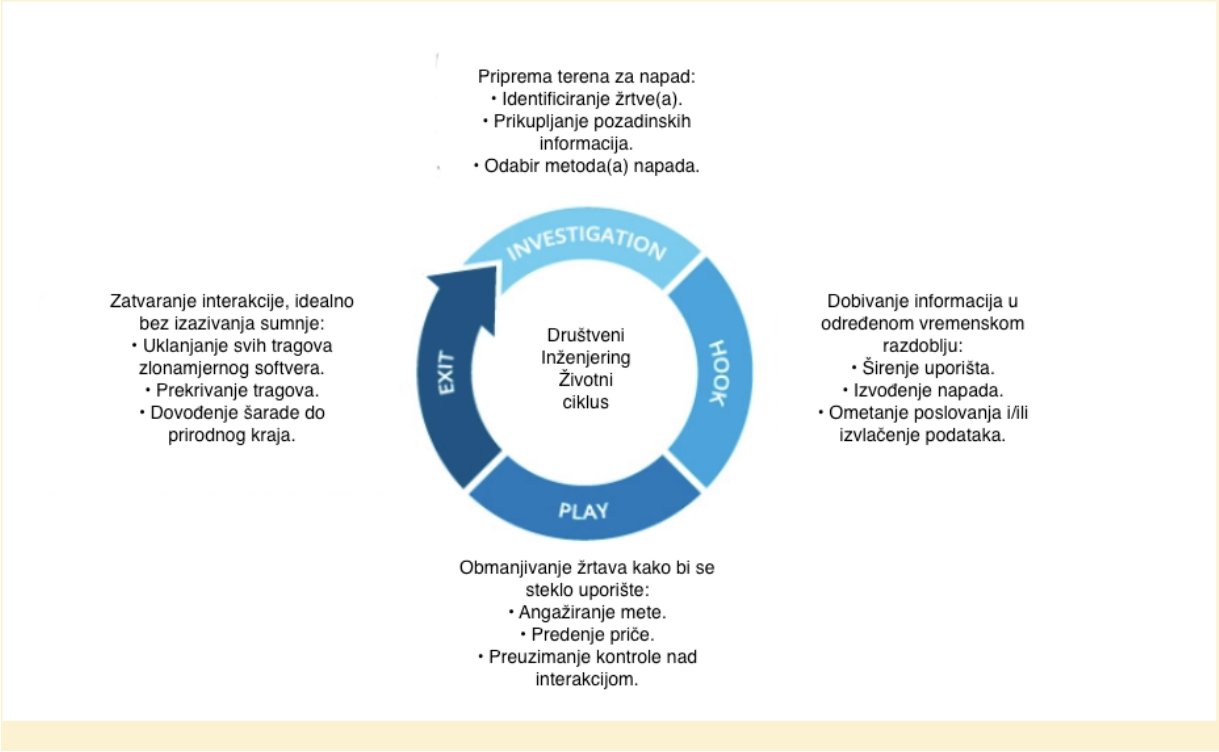
identiteta do napada lažiranja ID-a pozivatelja koji se često koriste za počinjenje prijevara. Napadi lažiranja obično iskorištavaju pouzdane odnose lažno predstavljajući osobu ili organizaciju koju žrtva poznaje. [7]

Mrežno iskorištavanje odnosi se na čin iskorištavanja ranjivosti mobilnih operativnih sustava ili drugog softvera koji se koristi unutar lokalnih i mobilnih mreža. Ova posebna prijetnja predstavlja značajan rizik jer se može izvršiti bez potrebe za sudjelovanjem korisnika. [2]

2.2.4. Društveni inžinjering

Društveni inženjering obuhvaća širok spektar zlonamjernih radnji koje se postižu kroz ljudske interakcije. Koristi psihološku manipulaciju kao sredstvo za prevaru korisnika. Kako bi napravili sigurnosne pogreške ili odaju osjetljive informacije.

Napadi društvenim inženjeringom događaju se u jednom ili više koraka. Počinitelj prvo istražuje željenu žrtvu kako bi prikupio potrebne pozadinske informacije, kao što su potencijalne točke ulaska i slabi sigurnosni protokoli, potrebni za nastavak napada. Zatim napadač pokušava steći povjerenje žrtve i pružiti poticaje za naknadne radnje koje krše sigurnosne prakse, poput otkrivanja osjetljivih informacija ili odobravanja pristupa kritičnim resursima.



Slika 2. životni ciklus društvenog inženjeringa [8]

2.2.5. Krađa identiteta

Lažni pojedinci koji se predstavljaju kao subjekti od povjerenja izvode napade krađe identiteta, koji im omogućuju dobivanje različitih vrsta povjerljivih informacija. Napredak tehnologije često je popraćen pojavom računalnih napada. Krađa identiteta je zapravo vrsta *phishinga* i postoje više taktika krađe [9]:

- Lukava komunikacija
- Osjećaj potrebe
- Lažno povjerenje
- Emocionalna manipulacija

U slučaju lukave komunikacije napadači posjeduju vještinu u manipuliranju pojedincima i stjecanju osjetljivih informacija skrivanjem zlonamjernih poruka i privitaka na mjestima gdje su ljudi manje oprezni, kao što su sandučići e-pošte. Često se pretpostavlja da su dolazne poruke u nečijem sandučiću benigne; međutim, treba biti oprezan jer se *phishing* e-pošte često čini pouzdanom i bezopasnom. Kako bi se spriječilo da ne tko postane žrtva

prijevare, ključno je odvojiti trenutak i pažljivo proučiti hiperveze i adrese e-pošte pošiljatelja prije nego što se klikne na njih.

Žrtve krađe identiteta često postanu žrtvom upravo stoga jer vjeruju da moraju odmah nešto poduzeti. One mogu nesvjesno preuzeti zlonamjerni softver prerušen u životopis ili otkriti bankovne vjerodajnice na sumnjivim web stranicama kako bi riješile navodne hitne potrebe. Iskorištavanje ovog osjećaja hitnosti uobičajen je i učinkovit trik. Kako bi se zaštitili podaci, treba biti na oprezu ili koristiti tehnologiju zaštite e-pošte za automatsku pomoć.

Oponašajući pouzdane izvore kao što su Google ili Wells Fargo, prijevarom napadači navode da korisnik nešto učini prije nego što shvati prijevaru. Neotkrivene prijetnje opstaju bez napredne sigurnosti. Vlastiti podaci se mogu zaštitit sigurnosnom tehnologijom e-pošte za filtriranje sumnjivog sadržaja.

Zlonamjerni pojedinci koriste psihološke taktike kako bi manipulirali metama sklonim impulzivnim radnjama. Oponašanjem pouzdanih izvora i poticanjem osjećaja hitnosti, napadači iskorištavaju emocije poput straha i tjeskobe. Ljudi često donose ishitrene odluke kada su suočeni s potencijalnim financijskim gubitkom, pravnim posljedicama ili nedostatkom resursa. Treba paziti na poruke koje zahtijevaju hitno djelovanje jer bi mogle biti dio prijevare.

2.2.6 Aplikacijski bazirane prijetnje

Aplikacije koje se mogu preuzeti predstavljaju razne sigurnosne rizike za mobilne i razne druge (mogu biti i obična računala) uređaje. Neke aplikacije označene kao "zlonamjerne" mogu izgledati legitimne na stranicama za preuzimanje, ali su zapravo dizajnirane za lažne aktivnosti. Čak se i naizgled pouzdan softver može iskoristiti u lažne svrhe. Ove prijetnje temeljene na aplikacijama obično spadaju u sljedeće kategorije:

- Zlonamjerni softver
- Špijunski softver
- Prijetnje privatnosti
- Ranjive aplikacije

Zlonamjerni softver izvršava zlonamjerne radnje nakon što se instalira na telefon. Može potajno generirati troškove na telefonskom računu, slati neželjene poruke vašim kontaktima ili dodijeliti kontrolu nad uređajem napadaču bez znanja korisnika.

Špijunski softver je osmišljen za prikupljanje ili iskorištavanje privatnih podataka bez pristanka korisnika. On cilja na informacije poput povijesti poziva, tekstualnih poruka, lokacije, povijesti preglednika, popisa kontakata, e-pošte i privatnih fotografija. Ukradeni podaci mogu se koristiti za krađu identiteta ili financijsku prijevaru.

Aplikacije koje prijete privatnosti, iako nisu nužno zlonamjerne, prikupljaju ili koriste osjetljive informacije (kao što su lokacija, popisi kontakata ili podaci koji otkrivaju osobnu identifikaciju) potrebne za njihovo funkcioniranje, ugrožavajući time privatnost.

Ranjive aplikacije sadrže nedostatke koji se mogu iskoristiti u zlonamjerne svrhe. Ove ranjivosti omogućuju napadačima pristup osjetljivim informacijama, izvođenje neovlaštenih radnji, ometanje usluga ili preuzimanje aplikacija na uređaje bez da o tome informiraju korisnika [10].

2.3 Računalni virusi

Računalni virus je vrsta zlonamjernog softvera koji se širi između računala i uzrokuje štetu podacima i softveru.

Računalni virusi imaju za cilj poremetiti sustave, uzrokovati značajne operativne probleme i dovesti do gubitka i curenja podataka. Jedan važan aspekt koji treba razumjeti o računalnim virusima je njihova sposobnost širenja kroz programe i sustave. Tipično, računalni virusi se pričvršćuju na izvršne host datoteke, dopuštajući njihovim virusnim kodovima da se izvrše kada se datoteka otvori. Odatle se kod širi mrežama, pogonima, programima za dijeljenje datoteka ili zaraženim privicima e-pošte, potječući iz dokumenta ili softvera kojemu je izvorno priložen [11].

2.3.1 Tipovi računalnih virusa

S obzirom na njihovo djelovanje računalni virusi mogu biti [12]:

- Rezidentni virusi
- Nerezidentni virusi

Rezidentni virusi se pokreću i učitavaju svoj kod u memoriju, gdje ostaje sve dok računalo radi. Ovi virusi koriste metode poput terminacija i ostati rezidentan (“Terminate and Stay Resident”, kraće TSR). i manipulacija memorijskim blokom (“Memory Block Manipulation”, kraće MBC) kako bi trajno ostali u memoriji računala. Zlonamjerni kod rezidentnog virusa koristi mehanizme operativnog sustava da se aktivira, kao što je pokretanje koda kad god se pokrene bilo koja aplikacija. Posljedično, novoinstalirane aplikacije također mogu biti zaražene kao rezultat ove aktivacije [12].

Nasuprot tome, nerezidentni računalni virus je vrsta virusa koji ne ostaje u RAM-u računala. Iako nerezidentni virusi mogu biti privremeno prisutni u RAM-u, oni nisu postojani. Kada se računalo isključi, RAM se obično čisti, sprječavajući pokretanje nerezidentnog računalnog virusa [13].

Neke od osnovnih vrsta virusa koje zahvaćaju računala su [12]:

- Boot sektor virusi
- Programski virusi

- Makro virusi

Virus sektora za pokretanje je vrsta računalnog virusa koji cilja na glavni zapis za pokretanje glavnog zapisa za podizanje sustava uređaja(“Master Boot Record”, kraće MBR). Za razliku od drugih virusa, ne zahtijeva da se žrtvino računalo uspješno pokrene kako bi ga zarazio. To znači da čak i mediji koji se ne mogu pokrenuti mogu pridonijeti širenju virusa sektora za pokretanje sustava. Ovi virusi kopiraju svoj zaraženi kod ili u boot sektor diskete ili particijsku tablicu tvrdog diska. Kada se računalo pokrene, virus se učitava u memoriju, dopuštajući mu da zarazi druge nezaražene diskove koje koristi sustav [14].

Programski virusi imaju sposobnost širenja različitim sredstvima, poput CD-a ili privitaka e-pošte. Oni se maskiraju unutar naizgled korisnih programa i aktiviraju se kada se program pokrene. Ti se virusi obično nazivaju virusima trojanskog konja, crpeći inspiraciju iz varljivog drvenog konja kojeg su Ulysses i Grci koristili tijekom Trojanskog rata. Slično kao što su vojnici izašli s konja kako bi otvorili vrata Troje, programski virusi mogu imati štetne učinke na računalne sustave. Razvojni programer softvera može namjerno ugraditi programske viruse ili ih tajno pričvrstiti tijekom njihovog putovanja s jednog računala na drugo. Oni također mogu poslužiti kao prijenosnici virusa i crva, pridonoseći daljnjoj infekciji [15].

Makro virus je vrsta računalnog virusa koji cilja makro naredbe, koje su odgovorne za automatizirano izvršavanje određenih radnji i naredbi unutar programa. Zamjenom ovih naredbi virus može nanijeti značajnu štetu računalnom sustavu. Sofisticirane aplikacije, poput programa za obradu teksta, često uključuju mogućnost automatskog pokretanja programa putem makronaredbi. To ih čini osjetljivima na makro viruse. Ovi virusi iskorištavaju jezik i funkcionalnost makronaredbi, otimajući važne naredbe, uključujući bitne zadatke poput otvaranja dokumenata. Posljedično, jednostavan čin otvaranja dokumenta može pokrenuti makro virus.

Makro virusi imaju sposobnost širenja različitim kanalima, uključujući privitke e-pošte, modeme, internet, mreže i pogone [16].

2.3.2. Pet načina kako se računalni virusi sakrivaju

Da bi računalni virus bio uspješan, mora ostati skriven. Učinkovitost virusa leži u njegovoj sposobnosti da neotkriveno djeluje unutar računalnog sustava. Prikrivanjem svoje

prisutnosti, virus može nastaviti svoje zlonamjerne aktivnosti, a da ga korisnik ili sigurnosne mjere ne primijete. Skriveni virus izbjegava izazivanje bilo kakve sumnje ili alarma, dopuštajući mu da ustraje i izvrši svoje namjeravane radnje. Može tiho oštetiti datoteke, ukrasti osjetljive podatke, poremetiti rad sustava ili se proširiti na druge uređaje. Izbjegavanjem otkrivanja virus se može nastaviti širiti i uzrokovati štetu tijekom duljeg razdoblja.

2.3.2.1. Samomodifikacija

Samomodifikacija je tehnika koju koriste virusi kako bi promijenili svoj izgled i izbjegli otkrivanje. Antivirusni programi obično traže virusne potpise uspoređujući uzorke koda s bazom podataka poznatih virusnih isječaka. Međutim, da bi se postigla 100% točnost, cijela baza koda virusa trebala bi se usporediti s bazom koda računala, što je nepraktično.

Umjesto toga, antivirusni softver koristi isječke virusa kao nizove za pretraživanje. Ovdje samomodifikacija stupa na scenu. Određeni virusi prate isječke koda koje koriste antivirusni programi i mijenjaju ih svaki put kada zaraze novi stroj. Promjenom svog potpisa, virus se pojavljuje jedinstven na svakom zaraženom sustavu. Ova pametna prijevara zavarava antivirusni program jer ne uspijeva pronaći nijedno pozitivno podudaranje i pretpostavlja da virus nije prisutan [17].

2.3.2.2. Enkripcija

Virusi koriste tehnike šifriranja kako bi izbjegli otkrivanje potpisa, obično koristeći tri metode.

Prva metoda uključuje korištenje šifre odnosno enkripcijskog algoritma zvanog XOR. XOR šifriranje koristi jednostavan ključ za kodiranje ulaza, stvarajući izlaz. Virus može primjeniti XOR operaciju između svakog pojedinog bajta i neke konstantne vrijednosti, omogućujući jednostavno dešifriranje. Ova enkripcija čuva virus skrivenim, ali omogućuje jednostavno raspakiranje i korištenje.

Druga metoda uključuje šifriranje cijelog virusa, ostavljajući samo šifrirani virus i ključ za dešifriranje. Budući da skeneri za otkrivanje virusa ne mogu identificirati šifrirani modul, izbjegava se pokretanje otkrivanja potpisa. Međutim, antivirusni programi mogu

prepoznati prisutnost ključa za šifriranje i staviti šifrirani kod u karantenu kao mjeru opreza. Ovaj pristup se danas rijetko koristi.

Treća metoda uključuje skrivanje šifriranog virusa unutar izvršne datoteke. Virus ostaje šifriran sve dok određeni skup radnji ne pokrene njegovu dešifraciju i izvršenje. Ova tehnika, poznata kao kripto virologija, često se oslanja na onemogućavanje antivirusnog softvera računala ručno ili tijekom ažuriranja. Dešifrirani virus tada inficira sustav i može trajno onemogućiti antivirusni softver kao dodatnu mjeru [17].

2.3.2.3. Polimorfni virusi

Polimorfni virusi predstavljaju značajan izazov za programere antivirusnog softvera, nadmašujući prethodne tehnike skrivanja virusa po složenosti.

Polimorfni virus uključuje mutirajući mehanizam koji djeluje kao jedinstveni agens za ponovno kodiranje, mijenjajući virus nakon svake infekcije ili specifičnih stanja. Taj mehanizam reprogramira kritične dijelove virusa koristeći različite kodne nizove kako bi postigao istu funkciju, što otežava otkrivanje i dešifriranje. U idealnom slučaju, savršeno izrađen polimorfni virus ne bi imao identične karakteristike istom virusu na drugom računalu, što ga čini gotovo neranjivim za antivirusne programe.

Brzina kojom se polimorfni virusi mijenjaju ovisi o različitim čimbenicima. U nekim slučajevima, haker može kontrolirati tempo promjene kako bi izbjegao davanje brojnih uzoraka virusa za obrnuti inženjering od strane antivirusnih istraživača. Ova strategija produljuje sposobnost virusa da izbjegne otkrivanje virusnih skenera, uzrokujući veću štetu tijekom duljih razdoblja [17].

2.3.2.4. Metamorfni virusi

Metamorfni virusi predstavljaju vrhunac otkrivanja virusa i izazova izbjegavanja. Mogu se smatrati pojačanom verzijom polimorfnih virusa. Za razliku od polimorfnih virusa koji modificiraju određene dijelove ili zadovoljavaju određene kriterije, metamorfni virusi se potpuno prepisuju sa svakom novom infekcijom.

Da bi to postigao, metamorfni virus se oslanja na metamorfni mehanizam. U usporedbi s polimorfnim virusima, metamorfni virusi općenito su veće veličine datoteke, što ih čini manje praktičnima za napade usmjerene na potrošače. Na primjer, metamorfni virus

W31/Simile sastojao se od preko 14 000 redaka koda, a većina je bila posvećena izvornom mehanizmu.

Napredak u brzini rada procesora i kapacitetu pohrane čini metamorfne viruse održivijima i primjenjivima u različitim scenarijima. Otkrivanje metamorfnih virusa predstavlja značajan izazov za antivirusni softver. Pristupi uključuju razvoj emulatora za oponašanje poznatih ponašanja metamorfnih virusa ili korištenje statističke analize uzoraka na šifriranom tijelu virusa. Međutim, nijedna tehnika ne nudi istu razinu pouzdanosti kao podudaranje potpisa, koje samo po sebi ima svoja ograničenja [17].

2.4. Računalni crvi

Računalni crv oblik je zlonamjernog softvera koji je dizajniran da se replicira i zarazi dodatna računala, a da pritom zadrži svoju prisutnost na zaraženim sustavima. Primarni cilj računalnog crva je širenje na nezaražena računala iskorištavanjem automatiziranih i skrivenih aspekata operativnog sustava. Obično korisnici postaju svjesni prisutnosti crva kada on počne trošiti resurse sustava i uzrokovati usporavanje ili prekide u drugim zadacima [18].

2.4.1. Princip rada računalnih crva

Računalni crvi često iskorištavaju ranjivosti u mrežnim protokolima, kao što je protokol za prijenos datoteka (“File Transfer Protocol”, kraće FTP), za širenje svoje infekcije. Nakon što se računalni crv uspješno infiltrira i aktivira na novozaraženom sustavu, njegov primarni cilj je ustrajati na tom sustavu i proširiti se na druge ranjive sustave.

Na primjer, ransomware crv *WannaCry* iskoristio je grešku u početnoj verziji protokola blok poruka windows poslužitelja (*Windows Server Message Block*, kraće SMBv1), koji se koristi za dijeljenje resursa. Nakon što se aktivira, *WannaCry* počinje skenirati mrežu u potrazi za potencijalnim metama, sustavima koji odgovaraju na SMBv1 zahtjeve koje šalje crv. Koristeći te klijente, crv se nastavlja širiti unutar mreže.

Zlonamjerni akteri mogu maskirati crva kao bezopasni sadržaj, kao što je radna datoteka ili naizgled bezopasna poveznica, navodeći korisnike da kliknu ili preuzmu crva. Ovi crvi mogu nositi zlonamjerne privitke ili sadržaje koji mogu brisati datoteke ili omogućiti neovlaštenu daljinsku kontrolu nad korisničkim računalima [18].

2.4.2 Razlike između crva i virusa

Glavna razlika između virusa i crva leži u njihovim zahtjevima za aktivaciju. Virusi se oslanjaju na aktivaciju svog domaćina, dok su crvi samostalni zlonamjerni programi sposobni za samoreplikaciju i neovisno širenje nakon proboja u sustav. Crvi rade bez potrebe za aktivacijom ili ljudskom intervencijom kako bi izvršili i proširili svoj kod.

Virusi se često skrivaju unutar dijeljenih ili preuzetih datoteka, uključujući izvršne i neizvršne datoteke poput *Word* dokumenata ili slikovnih datoteka. Ovi virusi ostaju neaktivni sve dok se zaražena host datoteka ne aktivira na ciljnom sustavu. Nakon što se aktivira, virus se može pokrenuti, izvršiti zlonamjerni kod i replicirati kako bi zarazio druge datoteke u sustavu.

Nasuprot tome, crvi ne ovise o aktivaciji svoje host datoteke. Jednom kada crv uđe u sustav, obično putem mrežne veze ili preuzete datoteke, može se odmah izvršiti, samoreplicirati i širiti bez pokretanja događaja. Crv stvara više kopija samog sebe, šireći se mrežama i internetskim vezama. Ove kopije inficiraju ranjiva računala i poslužitelje povezane s inicijalno zaraženim uređajem. Kroz ponavljajući proces samoumnožavanja, izvršavanja i širenja, infekcije temeljene na crvu brzo se šire računalnim mrežama i internetom [19].

2.4.3. Struktura računalnog crva

Svaki računalni crv sastoji se od nekoliko ključnih elemenata, uključujući module za identifikaciju cilja i širenje infekcije. Dodatno, postoje dodatne komponente kao što su daljinsko upravljanje, sučelje za ažuriranje, upravljanje životnim ciklusom i rutine korisnog opterećenja [20].

2.4.3.1. Lokator cilja

Učinkovit modul lokatora ciljeva izuzetno je važna komponenta računalnih crva. Najlakši mehanizam za napadača je prikupljanje e-mail adresa na sustavu na kojem je crv pokrenut i za slanje privitaka na takav sustav ciljeva, ali postoje mnogo sofisticiranije tehnike za brzo postizanje novih ciljeva, kao što je nasumična konstrukcija IP adresa u kombinaciji s

priključkom za skeniranje. Moderni računalni crvi napadaju mrežu koristeći više različitih protokola [20].

Prikupljanje adresa e-pošte je tehnika koju koriste računalni crvi za prikupljanje adresa e-pošte u zlonamjerne svrhe. Postoji više metoda za postizanje tog cilja. Napadač može koristiti standardne programska sučelja aplikacija (Application Programming Interface, kraće API), uključujući COM sučelja, za čitanje adresara. Primjer ovoga pokazuje računalni crv pod nazivom *W32/Serot*.

Drugi pristup uključuje izravno čitanje datoteka kako bi se izdvojile adrese e-pošte ugrađene u njih. Štoviše, napredni crvi mogu iskoristiti protokol mrežnog prijenosa vijesti(Network News Transfer Protocol, kraće NNTP) za skeniranje novinskih grupa ili iskorištavanje tražilica poput *Googlea* za prikupljanje adresa e-pošte koristeći taktike slične onima koje koriste spameri [20].

2.4.3.2. Propagatori infekcije

Propagatori infekcije u računalnim crvima su moduli ili mehanizmi koji omogućuju crvu da se širi i zarazi druge sustave. Ovi propagatori koriste različite tehnike za olakšavanje replikacije i širenja koda crva. Uobičajene metode uključuju iskorištavanje ranjivosti u mrežnim protokolima, kao što je protokol za prijenos podataka (File Transfer Protocol, kraće FTP), ili korištenje zajedničkih mrežnih resursa i mehanizama za dijeljenje datoteka. Propagatori infekcije ključne su komponente crva jer omogućuju zlonamjernom softveru brzo širenje i zarazu velikog broja sustava unutar mreže ili preko interneta [20].

Peer-to-peer(P2P) napadi stekli su popularnost među računalnim crvima budući da ne zahtijevaju složene tehnike mrežnog skeniranja. Umjesto toga, ti se crvi jednostavno repliciraju u zajedničku mapu na peer-to-peer (P2P) mreži. Svaki sadržaj prisutan u ovoj mapi postaje pretraživ i dostupan drugim korisnicima na P2P mreži. Neki crvi čak stvaraju te zajedničke mape kako bi namamili korisnike koji traže sadržaj. Ovaj napad nalikuje instalaciji trojanaca, gdje korisnici dobrovoljno pokreću zlonamjerni kod na svojim sustavima kada naiđu na zajednički sadržaj na P2P mreži [20].

2.4.3.3. Tehnike izvođenja koda

Računalni crvi koriste različite metode za širenje svog koda s jednog sustava na drugi. Dok se većina crva oslanja na privitke e-pošte za širenje svog glavnog tijela, druge vrste crva koriste različite tehnike. To može uključivati umetnuti kod, tehnike *shellcodea* i eksploatacijski kod za ciljanje i napad na ranjive sustave [20].

Napredna metoda napada uključuje iskorištavanje cilja ubacivanjem koda izravno preko mreže. S tradicionalnim ranjivostima prelijevanja međuspremnika koje je sve teže iskoristiti, napadači se fokusiraju na ranjivosti na strani poslužitelja koje proizlaze iz neadekvatne provjere valjanosti unosa. Na primjer, crv *Perl/Santy* koristio je *Google* za identificiranje ranjivih web stranica i izvršio vlastitu *Perl* skriptu kroz ranjivost u softveru *phpBB* oglasne ploče. Ovaj crv uspješno je uništio brojne web stranice 21. prosinca 2004. Radnje koje crv poduzima ovise o modelu niti ranjivog poslužitelja [20]:

- Nova nit se stvara na početku poslužitelja
- Nova nit se stvara na svaki dolazni zahtjev

Nadalje, ovisno o kontekstu preuzete niti, crv;

- Radi u kontekstu SUSTAVA s visokim privilegijama.
- Pokreće se u kontekstu korisnika s visokim ili niskim privilegijama koje bi crv mogao eskalirati

U nekim slučajevima umetnuti kod stvara novi korisnički račun na meti koju napadač može koristiti za daljinsku prijavu u sustav.

Slika 3. Tipičan jednosmjerni napad ubacivanjem koda.

2.5. Trojanski konji

Trojanski konj vrsta je zlonamjernog softvera koji se pretvara u legitimni softver, varajući korisnike da ga izvrše ili instaliraju. Izraz, posuđen iz grčke mitologije, prikladno opisuje ovaj varljivi pristup. Jednom kada uđe u računalo, trojanski konj ima sposobnost manipulirati operativnim sustavom, što dovodi do prikazivanja oglasa koji generiraju prihod (pomoću skočnih prozora) za napadača. Međutim, situacija postaje daleko opasnija kada trojanski konj napadaču dodijeli neograničenu kontrolu nad kompromitiranim računalom.
Time napadač može [21]:

- uključiti zaraženo računalo u mrežu poznatu kao "*botnet*".
- ukrasti povjerljive informacije
- instalirati druge oblike zlonamjernog softvera
- prenositi, primati i izmjenjivati datoteke na zaraženom računalu.
- bilježiti pritisnute tipke (kao *keylogger*)
- pratiti (špijunirati) aktivnosti žrtve
- koristiti memoriju (prostor) tvrdog diska
- rušiti zaraženo računalo itd.

2.5.1. Tri najpoznatija oblika trojanaca

2.5.1.1. Zeus

Zeus Virus, također poznat kao Zeus Trojan zlonamjerni softver, vrsta je zlonamjernog softvera koji posebno cilja operativne sustave Microsoft Windows s ciljem krađe financijskih podataka. Prvobitno je otkriven 2007. godine i stekao je znatnu slavu kao jedan od najuspješnijih softverskih programa za botnet u svijetu. U nekim krugovima nazivan Zbot, Zeus je zarazio milijune strojeva i poslužio kao temelj za stvaranje brojnih sličnih vrsta malwarea izvedenih iz njegovog koda. Dok se činilo da je Zeusova prijetnja smanjena nakon navodnog umirovljenja njegovog tvorca 2010., javna dostupnost njegovog izvornog koda dovela je do pojave nekoliko varijanti, obnavljajući relevantnost i opasnost povezanu s ovim posebnim zlonamjernim softverom.

Nakon što se računalo zarazi virusom Zeus, ono pokazuje niz zlonamjernih ponašanja, ali njegove primarne funkcije su navede u nastavku.

Prvo, uspostavlja *botnet*, što je mreža kompromitiranih strojeva kojima potajno upravlja poslužitelj za naredbe i kontrolu kojim upravlja autor zlonamjernog softvera. *Botnet* omogućuje vlasniku prikupljanje velikih količina informacija ili izvođenje napada velikih razmjera. Osim toga, Zeus djeluje kao trojanac za financijske usluge posebno dizajniran za krađu bankovnih vjerodajnica sa zaraženih strojeva. To postiže upotrebom tehnika praćenja web stranica i *keylogginga*. Aktivnim praćenjem online aktivnosti korisnika zlonamjerni softver može prepoznati kada korisnik pristupa web stranici banke i diskretno zabilježiti pritiske tipki unesene tijekom pokušaja prijave. Ovaj podmukli pristup omogućuje trojancu da zaobiđe sigurnosne mjere primijenjene na tim web stranicama budući da snimljeni pritisci tipki točno odgovaraju korisnikovom unosu za prijavu [22].

2.5.1.2. Spyeye

SpyEye je zlonamjerni trojanac koji napada online bankovne račune s ciljem krađe novca od korisnika koji ništa ne sumnjaju. Varijante *SpyEyea* mogu se infiltrirati u korisničke sustave putem različitih vektora infekcije, uključujući blackhat optimizaciju za tražilice, spam e-pošte i druge vrste zlonamjernog softvera. Primarni cilj *SpyEyea* je olakšati krađu vrijednih informacija, osobnih identiteta i financijske imovine. Tijekom prvog izdanja, *SpyEye* se pojavio kao glavni konkurent poznatom trojancu poznatom kao Zeus.

SpyEye radi nevjerojatnom brzinom, što mu omogućuje automatsko i brzo pokretanje transakcija brzinom koja nadmašuje brzinu prosječnog pojedinca koji ručno komunicira s web-stranicom. Ova karakteristika služi kao crvena zastavica za banke, dopuštajući im da identificiraju prisutnost virusa *SpyEye* i blokiraju njegove lažne transakcije. Slijedom toga, tvorci *SpyEyea* trenutno nastoje oponašati autentično ponašanje korisnika tijekom navigacije web stranicama, s ciljem da bankama zakompliciraju otkrivanje njihovih napada [23].

2.5.1.3. Emotet

Emotet, napredni i modularni bankovni trojanac, prvenstveno radi kao *downloader* ili dropper za druge bankarske trojance. Njegov je utjecaj i dalje znatan, uzrokujući značajnu financijsku i operativnu štetu državnim, lokalnim, plemenskim i teritorijalnim vlastima, kao i privatnom i javnom sektoru.

Emotet posjeduje polimorfna svojstva koja mu omogućuju da izbjegne konvencionalne metode detekcije koje se oslanjaju na potpise. Ovaj trojanac koristi različite tehnike za

održavanje postojanosti, uključujući korištenje ključeva registra i usluga za automatsko pokretanje. Koristi modularne biblioteke dinamičkih poveznica za kontinuirani razvoj i poboljšanje svojih mogućnosti. Nadalje, *Emotet* pokazuje svijest o okruženjima virtualnih strojeva i može generirati lažne indikatore kada se izvršava u takvim okruženjima.

Distribucija *Emoteta* odvija se putem zlonamjerne pošte, što uključuje slanje e-poruka koje sadrže zlonamjerne privitke ili poveznice. Ove e-poruke često koriste poznate robne marke kako bi prevarile primatelje. Nedavne kampanje oponašale su *PayPal* potvrde o plaćanju. Do početne infekcije dolazi kada korisnik otvori ili klikne na zlonamjernu vezu za preuzimanje, PDF datoteku ili *Microsoft Wor*d dokument s omogućenom makronaredbom. Nakon preuzimanja, *Emotet* uspostavlja postojanost i pokušava se širiti preko lokalnih mreža pomoću ugrađenih modula za širenje [24].

2.5.2. Zaštite od trojanaca

Primarna i najučinkovitija obrana od trojanaca je oprez pri otvaranju privitaka e-pošte ili pokretanju programa, osiguravajući apsolutnu sigurnost o njihovom izvoru. Ovo se upozorenje odnosi na sve datoteke dobivene iz peer-to-peer programa ili web stranica. Međutim, potpuno izbjegavanje takvih aktivnosti rijetko je izvedivo u današnjem međusobno povezanom svijetu, što zahtijeva provedbu dodatnih specifičnih sigurnosnih mjera.

Uvijek treba dati prioritet održavanju softvera ažurnim, posebno bitnih programa poput operativnog sustava i preglednika. Hakeri iskorištavaju poznate sigurnosne propuste u tim programima, koji mogu pomoći zlonamjernim aktivnostima trojanaca. Čak i ako dobavljač softvera izda zakrpe za rješavanje tih ranjivosti, one su neučinkovite ako se ne provede nadogradnja i ostalog softvera. Kako bi se povećala sigurnost internetske veze, važno je održavati aktivan vatrozid. I softverski i hardverski vatrozidi učinkoviti su u upravljanju i filtriranju zlonamjernog internetskog prometa, često sprječavajući trojance da se infiltriraju u računalo [25].

Nakon stjecanja znanja o prirodi trojanskih konja, njihovim različitim vrstama i mogućim štetama koje mogu nanijeti, postaje imperativ razumjeti potrebne mjere samozaštite. Početni i temeljni korak uključuje instalaciju i aktivaciju antivirusnog i antimalware softvera.

Osim toga, ključno je osigurati da operativni sustav, preglednik i aplikacije na svim uređajima budu redovito ažurirani [26].

3. Antivirusni programi

Antivirusni programi su softver dizajniran sa specifičnom svrhom prepoznavanja, sprječavanja i iskorijenjivanja zlonamjernog softvera poput virusa, crva ili trojanaca. Nakon instalacije, većina antivirusnih programa radi u pozadini, aktivno skenirajući i štiteći računalo od potencijalnih virusnih prijetnji u stvarnom vremenu.

Ove sveobuhvatne aplikacije za zaštitu od virusa igraju ključnu ulogu u zaštiti datoteka i hardvera od raznih oblika zlonamjernog softvera, uključujući crve, trojanske konje i špijunski softver. Osim toga, mogu pružiti dodatne sigurnosne značajke kao što su prilagodljivi vatrozidi i mogućnost blokiranja određenih web stranica [27].

3.1. Detekcija računalnih prijetnji

Upotrebom naprednih algoritama i kontinuiranog skeniranja u stvarnom vremenu, antivirusni softver aktivno identificira i eliminira niz opasnosti, poput zlonamjernog softvera, virusa i zlonamjernog koda. Ovaj robusni pristup štiti vaše računalo, osigurava njegovu sigurnost i održava njegovo cjelokupno zdravlje.

Antivirusni programi koriste različite metode da bi pravovremeno detektirali i uklonili računalni virus [28]:

- Detekcija na temelju potpisa
- Checksumming
- Popis dopuštenih aplikacija

3.1.1. Detekcija na temelju potpisa

Detekcija na temelju potpisa oslanja se na različite digitalne karakteristike, koje se nazivaju potpisi, softverskih programa koji se izvode na zaštićenom sustavu. Antivirusni softver skenira programe, prepoznaje njihove potpise i uspoređuje ih s poznatim potpisima zlonamjernog softvera. Antivirusna rješenja iskorištavaju opsežnu bazu podataka utvrđenih potpisa zlonamjernog softvera, koju obično održava tim za sigurnosna istraživanja dobavljača antivirusnih programa. Ova baza se redovito ažurira i sinkronizira sa zaštićenim uređajima. Kada antivirusni program otkrije softver koji odgovara poznatom potpisu, zaustavlja proces i ili izolira ili uklanja identificiranu prijetnju. Iako ova metoda služi kao temeljno i učinkovito sredstvo za otkrivanje zlonamjernog softvera, ima ograničenja jer napadači razvijaju

sofisticiranije tehnike, čineći pristup temeljen na potpisima nedovoljnim u otkrivanju novih oblika prijetnji.

3.1.2. Checksumming

Checksumming je oblik analize potpisa koji koristi kontrolne zbrojeve ciklusne provjere redundantnosti kako bi se osigurao integritet datoteke. Kontrolni zbroj igra ulogu u provjeri integriteta datoteke, što pomaže u rješavanju primarnog ograničenja otkrivanja temeljenog na potpisu—generiranja lažnih pozitivnih rezultata. Kako bi izbjegli metode identifikacije temeljene na potpisu, hakeri često koriste polimorfne zlonamjerne reklame. Polimorfni virusi posjeduju sposobnost mijenjanja svog koda tijekom replikacije, što otežava prepoznavanje dosljednih obrazaca pretraživanja. Tipično, hakeri šifriraju nasumične naredbe za dešifriranje unutar koda virusa pomoću ključeva koji nisu konstantni.

3.1.3. Popis dopuštenih aplikacija

Popis dopuštenih aplikacija, također poznat kao "*whitelisting*", djeluje na način koji je suprotan pristupu napada. Umjesto da specificira koji bi softver antivirusni program trebao blokirati, on održava popis odobrenih aplikacija i ograničava sve izvan ovog popisa.

Iako nije besprijekorno, ovo rješenje može biti nevjerojatno učinkovito, osobito u postavkama visoke sigurnosti. Legitimne aplikacije često sadrže sigurnosne ranjivosti ili nepotrebne značajke koje povećavaju potencijalnu površinu napada. U određenim slučajevima sama aplikacija može biti bezopasna, ali njezino korištenje može izložiti uređaj prijetnjama. Na primjer, u određenim okruženjima može postojati potreba za zabranom pregledavanja weba i upotrebe e-pošte.

3.2. Uklanjanje prijetnji

Nakon što antivirusni program pomoću gore navedenih metoda utvrdi da program predstavlja prijetnju, nastavlja sa stavljanjem datoteke ili programa u karantenu. Ova izolacija osigurava da identificirani sigurnosni rizik ostane odvojen od ostatka računala, čineći ga bezopasnim za krajnjeg korisnika. Obično, kada se to dogodi, antivirusni program obavještava korisnika računala o otkrivenoj prijetnji i traži od njega da poduzme potrebne radnje kako bi antivirusni program dovršio proces. Korisniku se nude opcije kao što su brisanje otkrivene

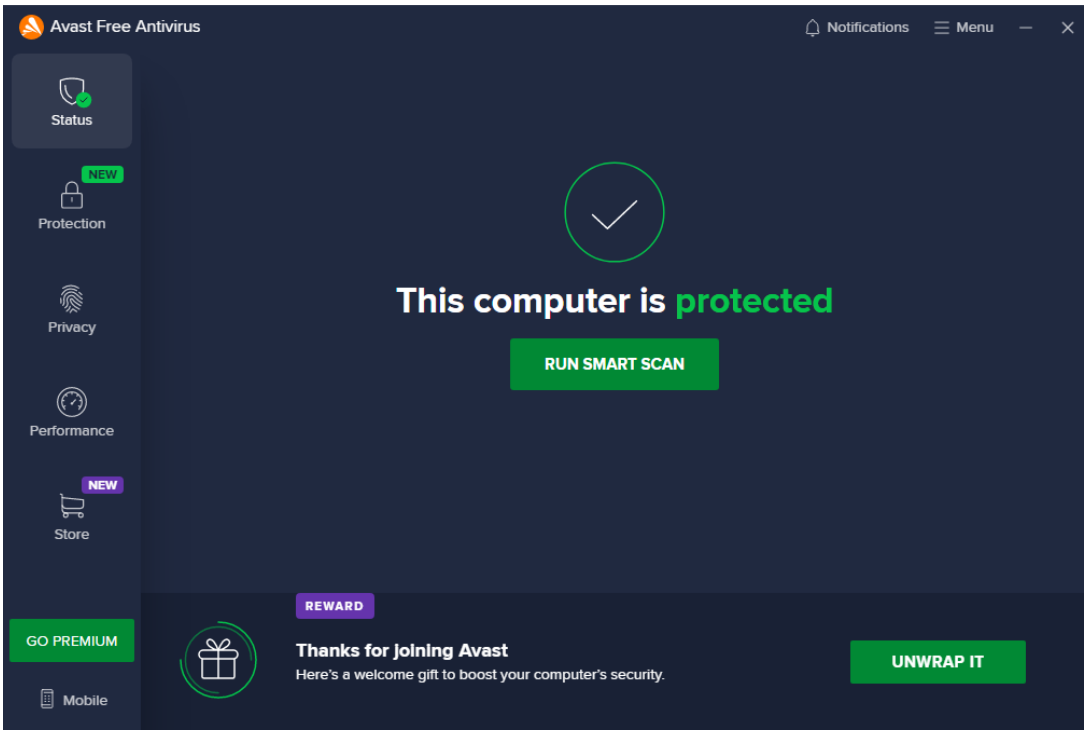
datoteke/programa, nastavak držanja u karanteni ili proglašavanje programa legitimnim i njegovo zadržavanje. Opcija zadržavanja programa često se nalazi na manje vidljivom području unutar sučelja antivirusnog programa. Međutim, ovisno o ozbiljnosti prijetnje i specifičnom antivirusnom softveru koji se koristi, mogućnost zadržavanja datoteke možda neće biti dostupna.

3.3. Primjeri antivirusnih programa

Kao primjere vrhunskih antivirusnih softvera odabrani su vodeći antivirusni programi iz 2023. U sljedećem odjeljku procijenit će se učinkovitost sljedećih programa: Avast, AVG, Bitdefender i Avira.

3.3.1. Avast

Avast je popularan izbor koji koristi više od 435 milijuna aktivnih korisnika širom svijeta kako bi zaštitili svoje pametne telefone i računala od zlonamjernog softvera i drugih prijetnji na mreži. Sa svojim skupom izvrsnih sigurnosnih značajki, softver blokira više od 1,5 milijardi prijetnji svaki mjesec. Ove značajke uključuju mehanizam za skeniranje zlonamjernog softvera koji može otkriti prijetnje u stvarnom vremenu i antivirusnu bazu podataka koja se često ažurira novim identificiranim prijetnjama i slabostima. Avast nudi napredne sigurnosne mjere protiv internetskih prijetnji. Ovo korisnicima omogućuje izbjegavanje lažnih web stranica, sigurnu kupovinu i blokiranje web špijuna [30].



Slika 4. Sučelje antivirusnog programa Avast

Avast nudi razne dodatne značajke za zaštitu sustava [31]:

- Sigurnost Wi-Fi mreže
- Sigurno pregledavanje i slanje e-pošte
- Zaštita od "*ransomwarea*"
- Upozorenja o curenju podataka

Avast također nudi dodatak za browser koji omogucuje osnovnu zaštitu od zlonamjernih web-mjesta i krađe identiteta. Mogu se osigurati vlastiti podaci o pregledavanju i dobit upute za privatnost korak po korak.

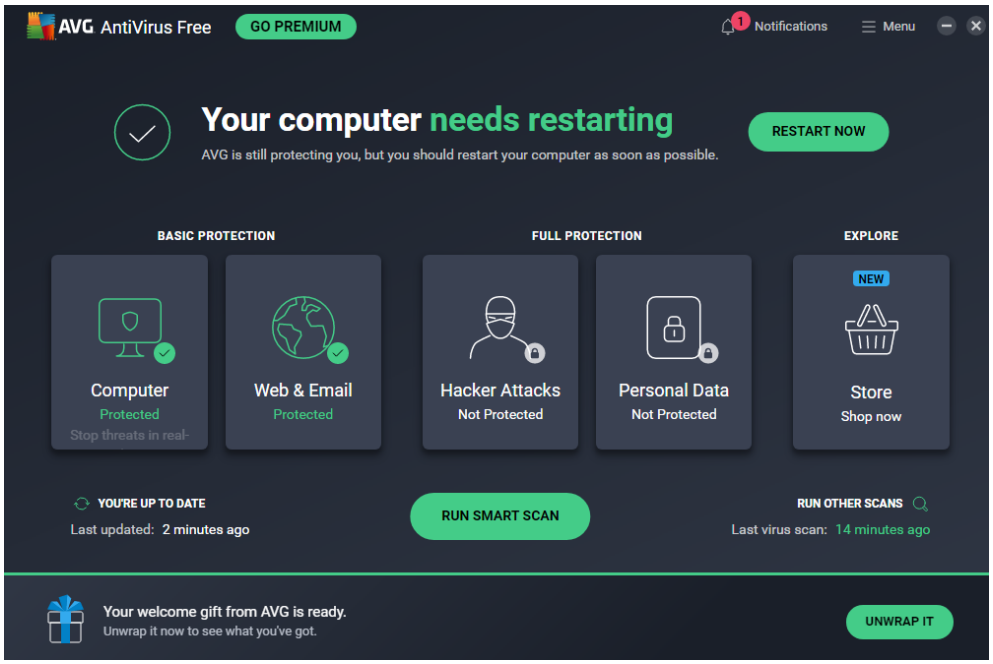
Dodatak nudi:

- Jednostavno izbjegavanje zlonamjernih web stranica i krađe identiteta
- Blokiranje mreže tragača
- Optimizaciju postavki privatnosti
- Uklanjanje "gnjavaže" sa web kolačićima

Neki su korisnici prijavili povremene skočne oglase i obavijesti koje promoviraju dodatne proizvode Avast.

3.3.2 AVG

AVG Antivirus pouzdan je i naširoko korišten antivirusni program koji pruža bitnu zaštitu od virusa, zlonamjernog softvera i drugih prijetnji na mreži. Nudi skeniranje u stvarnom vremenu za otkrivanje i uklanjanje zlonamjernog softvera prije nego što naškodi računalu. Sa značajkama kao što su zaštita od pregledavanja weba i automatska ažuriranja, AVG Antivirus pomaže osigurati sigurnost i sigurnost digitalnog okruženja.



Slika 5. Sučelje AVG antivirusnog programa

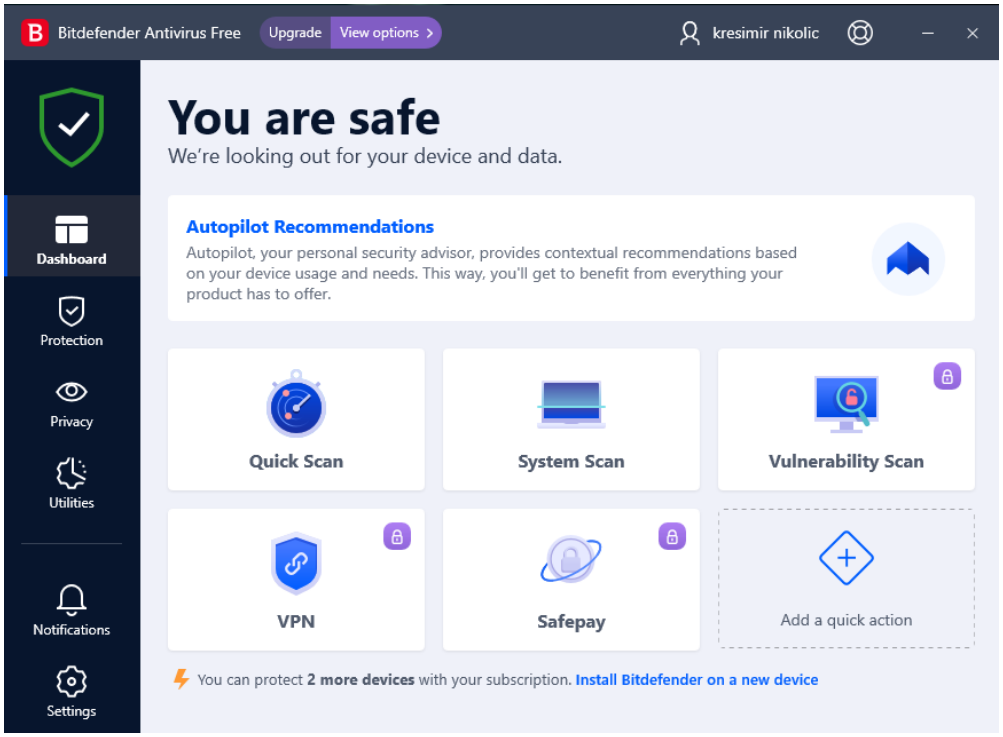
AVG takodjer posjeduje značajke za zaštitu od krađe identiteta i internet prijevara kao i skeniranje računala od virusa te web zaštitu.

Besplatna verzija uključuje ograničene značajke u usporedbi s plaćenom verzijom, poput napredne zaštite od *ransomwarea* i vatrozida.

3.3.3. Bitdefender

Bitdefender Antivirus visoko je hvaljeni antivirusni program poznat po svojim snažnim sigurnosnim značajkama i naprednim mogućnostima otkrivanja prijetnji. Nudi sveobuhvatnu zaštitu od raznih oblika zlonamjernog softvera, uključujući viruse, ransomware i phishing

napade. Sa svojim intuitivnim korisničkim sučeljem i minimalnim utjecajem na sustav, Bitdefender Antivirus pruža besprijekorno i učinkovito antivirusno rješenje za korisnike koji traže vrhunsku sigurnost. Osim za osobnu uporabu Bitdefender je popularan među većim firmama kao solucija za zaštitu.



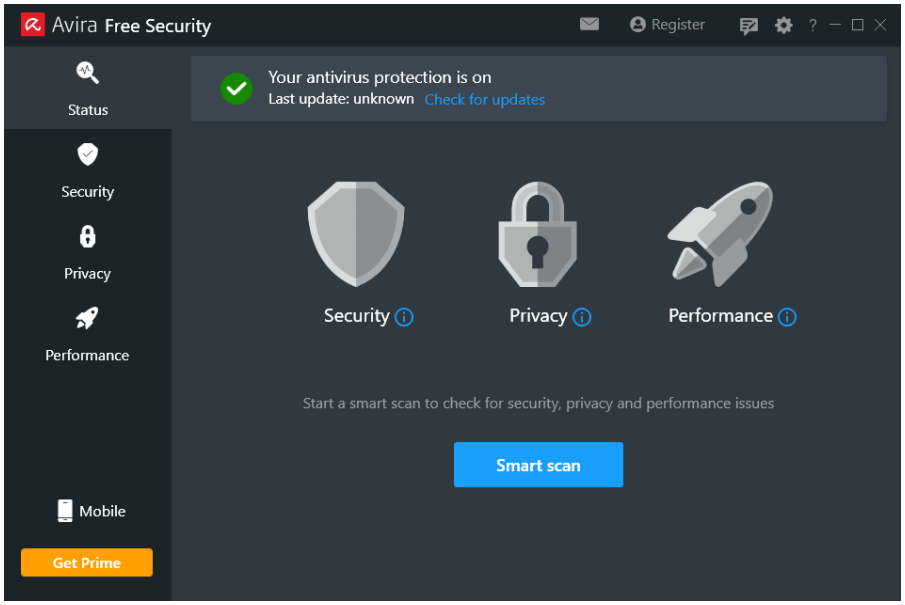
Slika 6. Sučelje Bitdefender antivirusnog programa

Bitdefender Antivirus nudi osnovne funkcije za zaštitu računala. Sadrži skeniranje u stvarnom vremenu, aktivno praćenje sustava u potrazi za prijetnjama zlonamjernim softverom i automatska ažuriranja kako bi antivirusni softver bio ažuran s najnovijim definicijama virusa i sigurnosnim zakrpama, pružajući zaštitu od novih prijetnji.

Početno skeniranje i proces instalacije mogu biti dugotrajni i zahtijevni za resurse, privremeno usporavajući rad sustava.

3.3.4. Avira

Avira Antivirus je renomirani antivirusni program poznat po svojim moćnim sigurnosnim značajkama i pouzdanim mogućnostima otkrivanja prijetnji. Pruža sveobuhvatnu zaštitu od zlonamjernog softvera, virusa i drugih internetskih prijetnji, pomažući u zaštiti računala i osobnih podataka. Uz značajke kao što su skeniranje u stvarnom vremenu, web zaštita i VPN za sigurno pregledavanje, Avira Antivirus nudi robusnu obranu od zlonamjernih aktivnosti na internetu.



Slika 7. Sučelje Avira antivirusnog programa

Besplatna verzija prikazuje povremene skočne oglase koji potiču korisnike na nadogradnju na verziju koja se plaća za dodatne značajke.

4. Usporedba rada antivirusnih programa

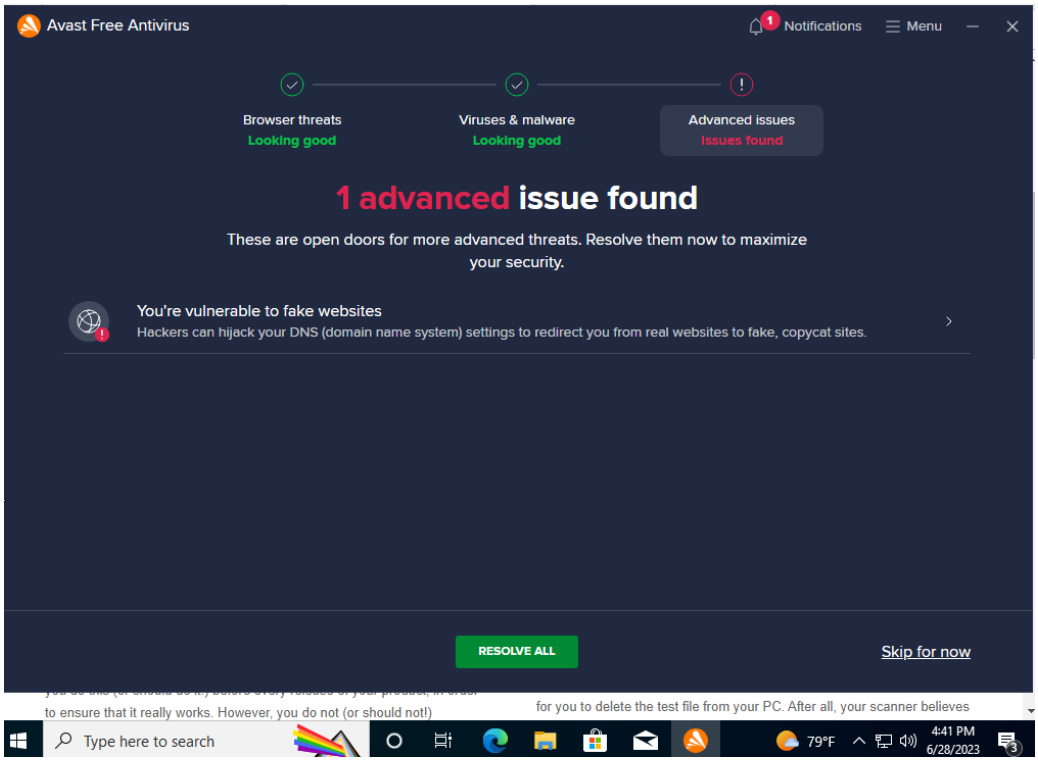
U ovom poglavlju će se provesti testiranje svih gore navedenih antivirusnih programa na sljedeći način. Instalacija operativnog sustava Windows 10 u zaštićenom okruženju izrađena je pomoću softvera VirtualBox. VirtualBox pruža sigurno okruženje za testiranje antivirusnih programa bez rizika od izazivanja bilo kakve neželjene štete na stvarnom računalu. Sve naredne radnje izvode se unutar okruženja VirtualBox.

Za optimalnu učinkovitost antivirusnog programa potrebno je onemogućiti Windows Defender unutar operativnog sustava. Nakon što je operativni sustav postavljen, instalira se antivirusni program koji se testira. Proces testiranja uključuje korištenje datoteke “Eicar” (Europski institut za istraživanje računalnih antivirusnih programa - EICAR). Eicar test datoteka se može dobiti preuzimanjem s [32]. Ovu je datoteku posebno razvio Europski institut za istraživanje računalnih antivirusnih programa za procjenu mogućnosti programa za zaštitu od sigurnosnih prijetnji. Institut Eicar služi kao neovisna platforma za stručnjake za informacijsku sigurnost koji se bave znanstvenim istraživanjem, razvojem, implementacijom i upravljanjem.

Nakon instalacije antivirusnog programa preuzima se Eicar datoteka, a rezultati testiranja bit će prikazani u sljedećim odjeljcima ovog rada.

4.1. Testiranje Avast antivirusnog programa

Kad je Avast antivirusni program instaliran na Windows 10 na VirtualBoxu program javlja uspješnost instalacije te pokreće prvo sigurnosno skeniranje. Nakon skeniranja program odmah javlja da je sustav izložen opasnosti.



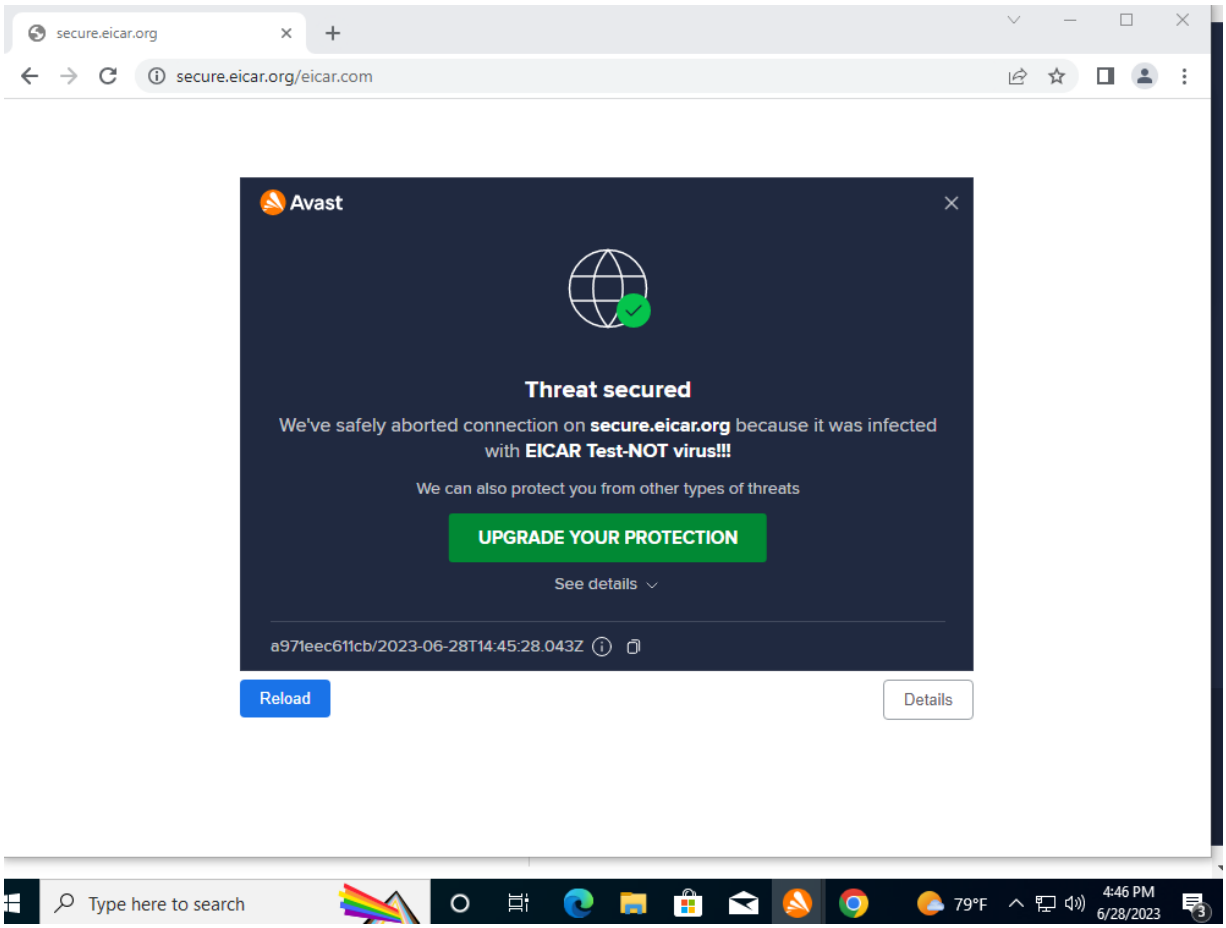
Slika 8. Avast antivirusni program daje upozorenje o opasnosti

U sljedećem koraku se preuzima Eicar datoteka. Eicar datoteka je raspoloživa u 4 oblika:

- Eicar.com
- Eicar.com.txt
- Eicar_com.zip
- Eicarcom2.zip

Za svrhe testiranja antivirusnog programa provjerit će se sve četiri datoteke.

Odmah prilikom preuzimanja prve datoteke “eicar.com” Avast antivirusni program je primjetio prijetnju te prekinuo konekciju.



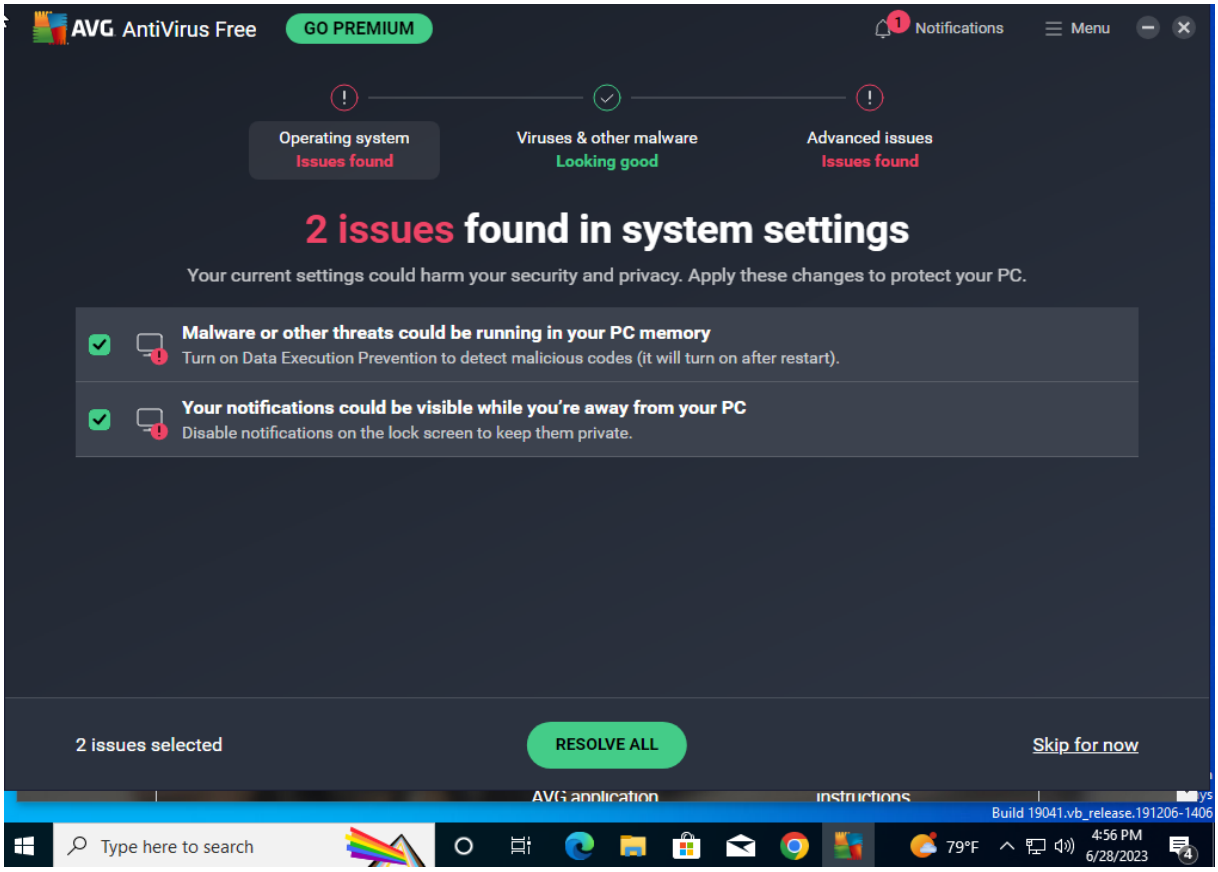
Slika 9. Avast prekida konekciju prilikom preuzimanja datoteke

Prilikom skidanja druge datoteke eicar.com.txt Avast je još jednom prekinuo konekciju sa istom porukom kao prilikom prvog preuzimanja. Ista poruka se pojavila i kod preuzimanja preostale dvije datoteke.

Prema tome, može se zaključiti da je Avast antivirusni program svoj posao vrlo dobro izvršio te nije ni dopustio da zaražena datoteka dođe na memoriju računala.

4.2. Testiranje AVG antivirusnog programa

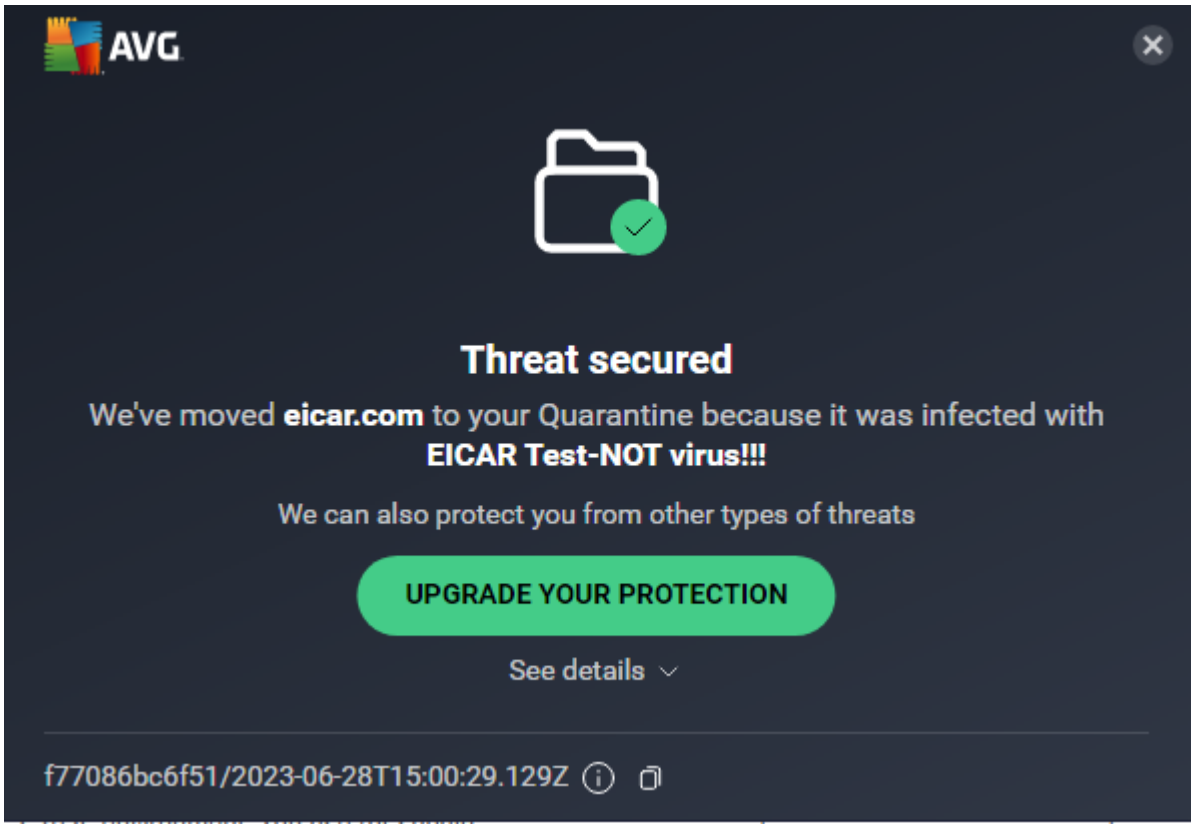
Kad je AVG antivirusni program instaliran na Windows 10 na VirtualBoxu, program javlja uspješnost instalacije te pokreće prvo sigurnosno skeniranje. Nakon skeniranja program takodjer javlja da je sustav izložen opasnost, ovog puta AVG program je u odnosu na Avast uočio dvije opasnosti.



Slika 10. AVG antivirusni program daje upozorenje o dvije opasnosti

Kod preuzimanja dvije datoteke eicar.com i eicar.com.txt nailazimo na sličnu situaciju kao i kod Avast antivirusnog programa gdje AVG antivirusni program odmah blokira konekciju te ne postoji ni mogućnost preuzimanja datoteke.

Prilikom preuzimanja eicar_com.zip datoteke AVG antivirusni program ne javlja niti primjećuje ikakvu opasnost. Prilikom pokretanja programa unutar datoteke AVG prepoznaje virus te javlja da se računalo mora restartati da bi se program stavio u karantenu. Prilikom preuzimanja datoteke eicarcom2-zip program također ne prepoznaje opasnost. Ipak, pokretanje programa izaziva aktivnost AVG-a koji javlja da je prijetnja prepoznata te odmah stavljena u karantenu.

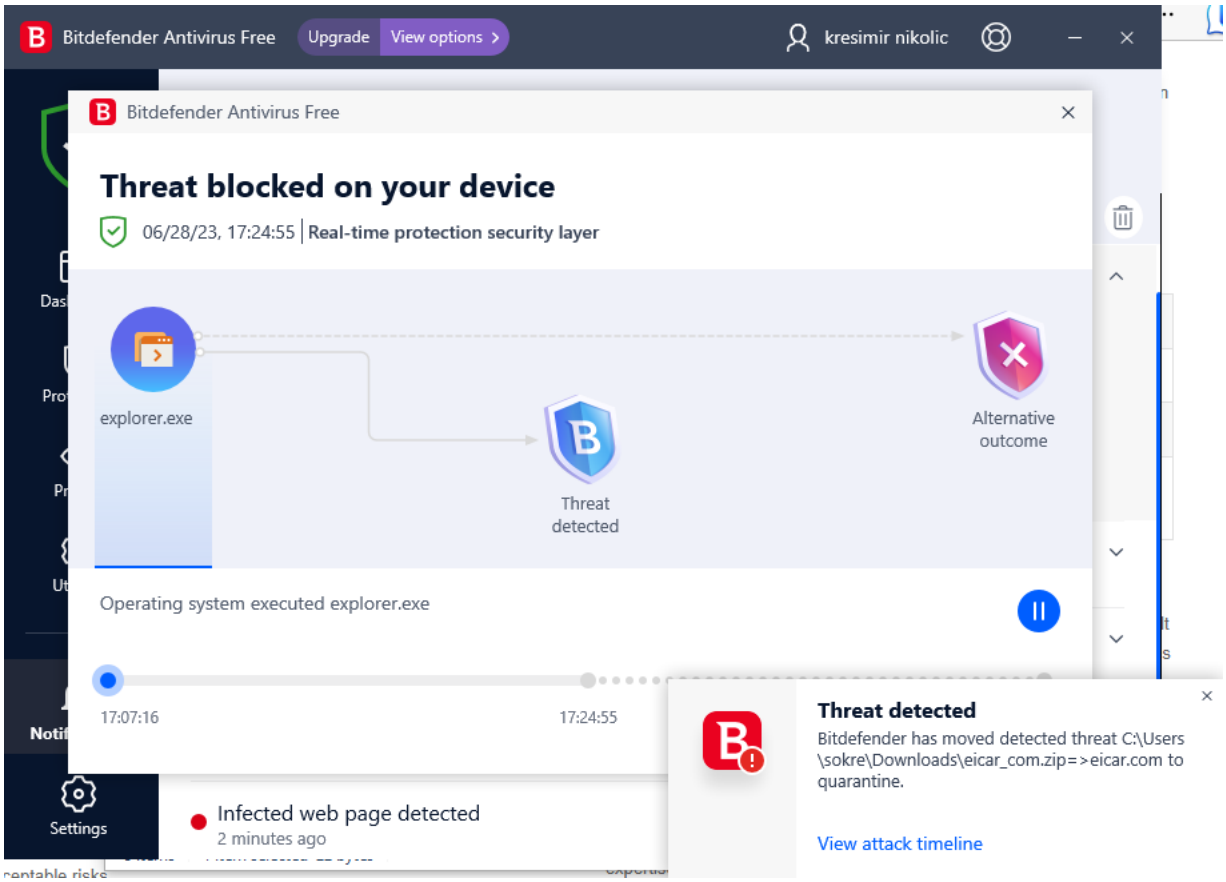


Slika 11. AVG antivirusni program stavlja zaraženu datoteku u karantenu

4.3. Testiranje Bitdefender antivirusnog programa

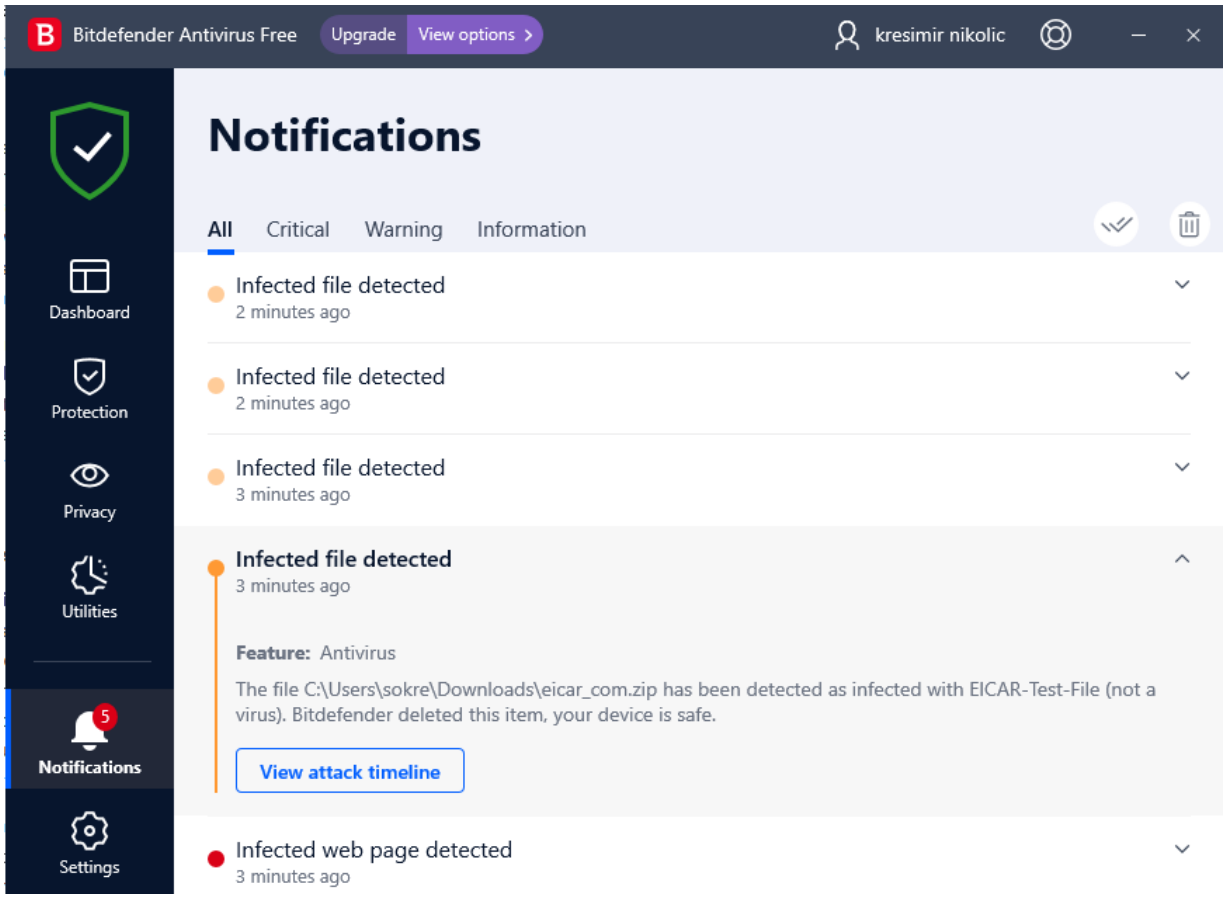
Kad je Bitdefener antivirusni program instaliran, što je potrajalo znatno duže od prijašnjih programa na Windows 10 na VirtualBoxu, program javlja uspješnost instalacije te pokreće prvo sigurnosno skeniranje. Kao i ostali programi Bitdefender obavlja sigurnosno skeniranje. Zanimljivo je da ne prepoznaje nikakve sigurnosne opasnosti u odnosu na Avast i AVG.

Prilikom preuzimanja prve dvije datoteke, kao i kod prijašnjih antivirusnih programa Bitdefender blokira stranicu te ne dopušta preuzimanje datoteke. Isti je slučaj i kod preostale dvije datoteke ali s obzirom da su skinute provjerit će se ponašanje Bitdefendera prilikom pokretanja programa.



Slika 12. Bitdefender blokira virus te ga stavlja u karantenu

Bitdefender je prilikom pokretanja eicar_com.zip i eicarcom2.zip prepoznao oba virusa te ih odmah stavio u karantenu. U odnosu na druge antivirusne programe Bitdefender nudi notifikacije o prepoznatoj prijetnji i akciji koja je izvedena.



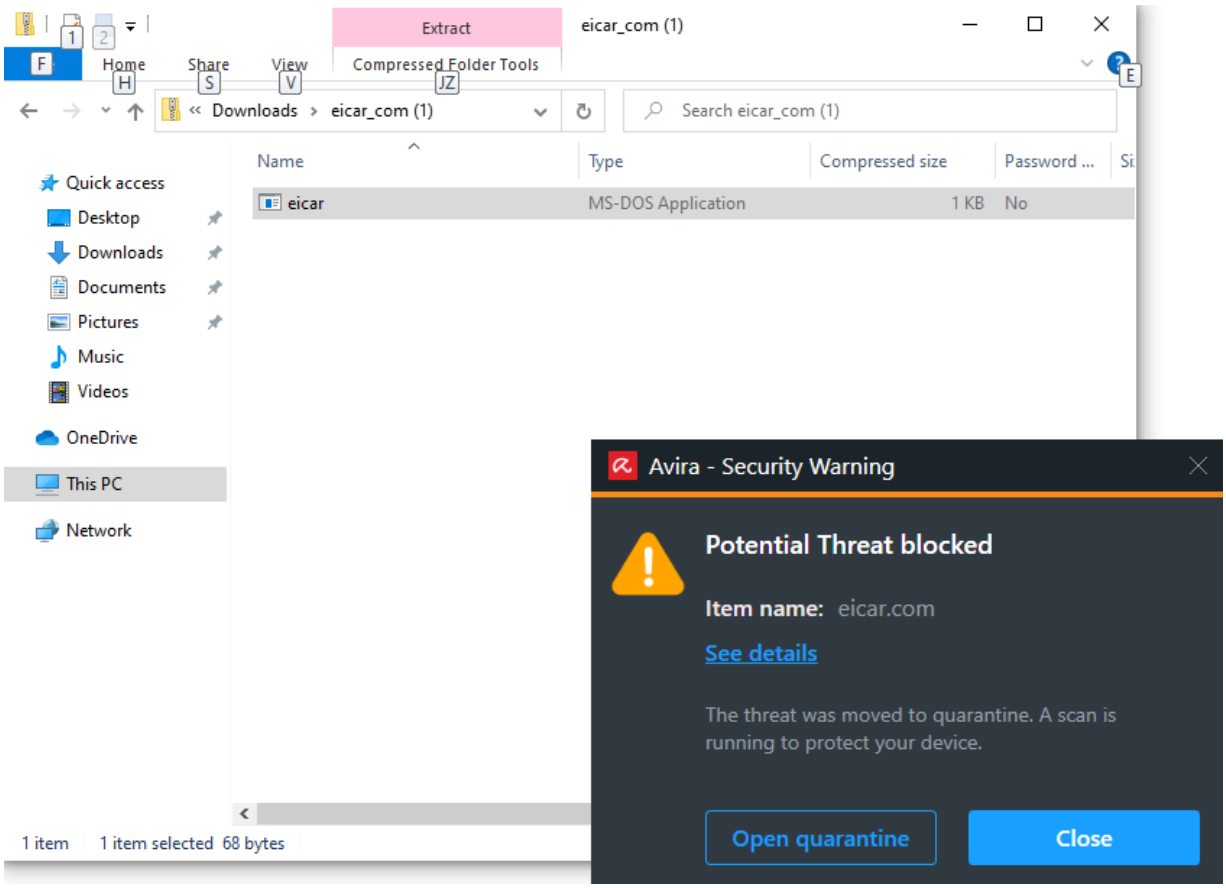
Slika 13. Bitdefender povijest zaštite te poduzete akcije

4.4. Testiranje Avira antivirusnog programa

Kad je Avira antivirusni program instaliran na Windows 10 na VirtualBoxu, program javlja uspješnost instalacije te pokreće prvo sigurnosno skeniranje. Kao i ostali programi Avira obavlja sigurnosno skeniranje te javlja čak 6 sigurnosnih opasnosti.

Slika 14. Avira antivirusni program javlja sigurnosne opasnosti

Prilikom skidanja prve dvije datoteke situacija je ista kao i kod drugih programa odnosno Avira ne dopušta skidanje te automatski blokira web stranicu. Kod druge dvije datoteke program dopušta skidanje na računalo ali prilikom pokretanja programa se virus stavlja u karantenu.



Slika 15. Avira antivirusni program stavlja program u karantenu te pokreće sigurnosno skeniranje

	eicar.com	Eicar.com.txt	eicar_com.zip	eicarcom2.zip
Avast	Pokušaj preuzimanja blokiran	Pokušaj preuzimanja blokiran	Detekcija prilikom pokretanja programa	Detekcija prilikom pokretanja programa
AVG	Pokušaj preuzimanja blokiran	Pokušaj preuzimanja blokiran	Detekcija prilikom pokretanja - potreban restart računala	Detekcija prilikom pokretanja programa
Bitdefender	Pokušaj preuzimanja blokiran	Pokušaj preuzimanja blokiran	Pokušaj preuzimanja blokiran	Pokušaj preuzimanja blokiran
Avira	Pokušaj preuzimanja blokiran	Pokušaj preuzimanja blokiran	Detekcija prilikom pokretanja programa	Detekcija prilikom pokretanja programa

Tablica 1. Rezultati testiranja antivirusnih programa

Zaključak

Uz sve veću zastupljenost interneta i računala u našem svakodnevnom životu, proširio se i raspon prijetnji usmjerenih na računalne sustave, podatke i krajnje korisnike. Ovo naglašava veliku važnost informacijske sigurnosti u zaštiti podataka i šireg područja računalstva. Kontinuirana evolucija tehnologije uvodi nove oblike zlonamjernih prijetnji, predstavljajući značajne rizike za sve korisnike računala. Primarni kanal za zarazu zlonamjernim softverom ostaje internet, uglavnom putem preuzimanja neprovjerenih datoteka i izlaganja osobnih podataka. Stoga postaje imperativ zaštititi svoje podatke i računalo legitimnim sredstvima. Jednostavan pristup zaštiti korisnika je upotreba računalnog softvera koji je eksplicitno dizajniran za suzbijanje zlonamjernih i sigurnosnih prijetnji. Unatoč tome, razumijevanje temeljne dinamike i prepoznavanje potencijalnih prijetnji i dalje je ključno za smanjenje rizika od infekcije.

Važno je naglasiti da se izbor među ovim testiranim programima u velikoj mjeri se svodi na osobne preferencije i specifične potrebe, budući da su svi pokazali skoro identice performanse. Korisnici mogu s pouzdanjem odabrati bilo koju od ovih opcija, znajući da će njihove potrebe za digitalnom sigurnošću biti i više nego dovoljne.

Međutim, dok su antivirusni programi ključna komponenta naše internetske obrane, ne bi se trebali isključivo oslanjati na njih. Najvažnije je bit oprezan u mrežnim aktivnostima. Čak ni najnapredniji antivirusni softver ne može zamijeniti našu vlastiti nemar kada je u pitanju preuzimanje i korištenje sadržaja s interneta. Prakticiranje navika sigurnog pregledavanja, oprez sa sumnjivim poveznicama ili preuzimanjima i ažuriranje sustava ključni su koraci u održavanju sigurnog digitalnog okruženja. Stoga, dok su antivirusni programi doista impresivni u svojim mogućnostima, vlastita pozornost mora ostati sastavni dio naših digitalnih života.

Može se zaključiti da su besplatne verzije antivirusnih programa solidne opcije, pod uvjetom da korisnik posjeduje sveobuhvatno razumijevanje njihove funkcionalnosti, razine zaštite koju nude i načina na koji štite korisnika. Procjena besplatnih antivirusnih programa koji koriste Eicar datoteke identificirala je Bitdefender kao najbolji izbor, koji dosljedno

sprječava zlonamjerna preuzimanja i brzo neutralizira sve druge Eicar datoteke, učinkovito i djelotvorno.

Literatura

[1] *Nepoznat autor, Što je računalna sigurnost*: https://www.microsoft.com/hr-hr/security/business/security-101/what-is-cybersecurity (15.6.2023)

[2] *Nepoznat autor, Terminalni uređaji, sigurnost primjene terminalnih uređaja:* http://e-student.fpz.hr/Predmeti/T/Terminalni_uredaji/Materijali/10_-_Sigurnost_primjene_terminalnih_uredjaja_-_09122013.pdf (15.6.2023)

[3] *Cuklin, S. 2022 Recikličnost električnog i elektroničkog: otpada*https://repozitorij.gfv.unizg.hr/islandora/object/gfv%3A666/datastream/PDF/view (15.6.2023)

[4] *Islam, R. 2016 E-Waste Generation and recycling:* https://www.researchgate.net/figure/EPA-data-from-Municipal-Solid-Waste-Generation-Recycling-and-Disposal-in-the-United_fig4_290973754 (16.6.2023)

[5] *Nepoznat autor, Phishing napadi – kako ih prepoznati i zaštititi se:* https://azop.hr/phishing-napadi-kako-ih-prepoznati-i-zastititi-se/ (16.6.2023)

[6] *E. Hall, G. 2016 Što je to otimač preglednika i kako ukloniti takav program:* https://virusi.hr/otimac-preglednika/ (16.6.2023)

[7] *Nepoznat autor, What is a Spoofing Attack:* https://www.rapid7.com/fundamentals/spoofing-attacks/ (16.6.2023)

[8] *Nepoznat autor, What is Social Engineering:* https://www.imperva.com/learn/application-security/social-engineering-attack/ (16.6.2023)

[9] *Nepoznat autor, Što je krađa identiteta:* https://www.microsoft.com/hr-hr/security/business/security-101/what-is-phishing (16.6.2023)

[10] *Nepoznat autor, Nepoznat autor, What is a Mobile Threat:* https://www.lookout.com/glossary/what-is-a-mobile-threat (16.6.2023)

[11] *Nepoznat autor, What are Computer Viruses:* https://www.fortinet.com/resources/cyberglossary/computer-virus (25.6.2023)

[12] *Nepoznat autor, O virusima:* https://www.cert.hr/virusi/ (25.6.2023)

[13] *Nepoznat autor, Resident vs Non-Resident Computer Viruses: What's the Difference?, 2020:*

https://logixconsulting.com/2020/05/25/resident-vs-non-resident-computer-viruses-whats-the-difference/ (25.6.2023)

[14] *Nepoznat autor, Što je virus sektora boot?, 2023:* https://hr.theastrologypage.com/boot-sector-virus (25.6.2023)

[15] *Nepoznat autor, Boot & Program Viruses:* https://www.livinginternet.com/i/is_vir_prog.htm (25.6.2023)

[16] *Nepoznat autor, Što je makro virus?, 2023:* https://hr.theastrologypage.com/macro-virus

[17] *Nepoznat autor, Viruses: 5 Ways They Hide from Anti-Virus Software, 2015:* https://www.bankvault.com/viruses-how-they-hide-from-antivirus-programs/ (26.6.2023)

[18] *Bedell, C. 2022 What is a Computer Worm:* https://www.techtarget.com/searchsecurity/definition/worm (26.6.2023)

[19] *Nepoznat autor, What's the Difference between a Virus and a Worm?:* https://www.kaspersky.com/resource-center/threats/computer-viruses-vs-worms (26.6.2023)

[20] *Nepoznat autor, Strategies of Computer Worms, Concise Oxford English Dictionary, Revised Tenth Edition, p. 9.1-9.6:* https://ptgmedia.pearsoncmg.com/images/0321304543/samplechapter/szor_ch09.pdf (26.6.2023)

[21] *Nepoznat autor, O TROJANSKIM KONJIMA:* https://www.cert.hr/trojanski_konji/ (27.6.2023)

[22] *Nepoznat autor, Zeus Virus:* https://www.kaspersky.com/resource-center/threats/zeus-virus (27.6.2023)

[23] *Nepoznat autor, What is SpyEye:* https://zemana.com/us/removal-guide/avoid-spyeye-virus-in-mobile-banking.html (27.6.2023)

[24] *Nepoznat autor, Emotet Malware CISA, 2020:* https://www.cisa.gov/news-events/alerts/2018/07/20/emotet-malware (27.6.2023)

[25] *Nepoznat autor, Avoiding a Trojan Virus: Keeping the Gates Closed:* https://www.kaspersky.co.uk/resource-center/preemptive-safety/avoiding-a-trojan-virus (27.6.2023)

[26] *Nepoznat autor, What is a Trojan and how can you protect yourself?:* https://www.bbvapivot.com/en/cybersecurity/what-is-a-trojan-and-how-can-you-protect-yourself/ (27.6.2023)

[27] *What is Antivirus - Definition, Meaning & Explanation:* https://www.verizon.com/articles/internet-essentials/antivirus-definition/ (28.6.2023)

[28] *4 Malware Detection Techniques and Their Use in EPP and EDR:* https://www.cynet.com/malware/4-malware-detection-techniques-and-their-use-in-epp-and-edr/ (28.6.2023)

[29] *The Best Free Antivirus Software for 2023:* https://www.pcmag.com/picks/the-best-free-antivirus-protection (28.6.2023)

[30] *Iwuozor. J, Main. K, Avast Antivirus Review 2023: Pricing, Pros And Cons, 2023:* https://www.forbes.com/advisor/in/business/software/avast-antivirus-review/ (28.6.2023)

[31] *Download Avast:* https://www.avast.com/free-antivirus-download#pc (28.6.2023)

[32] *Avast Online Security Plugin:* https://www.avast.com/avast-online-security#pc (28.6.2023)

[32] *ANTI MALWARE TESTFILE:* https://www.eicar.org/download-anti-malware-testfile/ (28.6.2023)

Popis kratica

Kratica	Puni naziv na stranom jeziku	Tumačenje na hrvatskom jeziku
TSR	Terminate and Stay Resident	Terminacija i ostati rezidentan
MBC	Memory Block Manipulation	Manipulacija memorijskim blokom
MBR	Master Boot Record	Zapis za pokretanje glavnog zapisa za podizanje sustava uređaja
FTP	File Transfer Protocol	Protokol za prijenos datoteka
SMBv1	Windows Server Message Block	Blok poruka windows poslužitelja
API	Application Programming Interface	Standardne programska sučelja aplikacija
NNTP	Network News Transfer Protocol	Protokol mrežnog prijenosa vijesti
P2P	Peer to Peer	Peer to Peer

Popis slika

Slika 1. Količina recikliranog otpada kroz godine 4
Slika 2. životni ciklus društvenog inženjeringa 7
Slika 3. Tipičan jednosmjerni napad ubacivanjem koda. 18
Slika 4. Sučelje antivirusnog programa Avast 25
Slika 5. Sučelje AVG antivirusnog programa 26
Slika 6. Sučelje Bitdefender antivirusnog programa 27
Slika 7. Sučelje Avira antivirusnog programa 28
Slika 8. Avast antivirusni program daje upozorenje o opasnosti 30
Slika 9. Avast prekida konekciju prilikom preuzimanja datoteke 31
Slika 10. AVG antivirusni program daje upozorenje o dvije opasnosti 32
Slika 11. AVG antivirusni program stavlja zaraženu datoteku u karantenu 33
Slika 12. Bitdefender blokira virus te ga stavlja u karantenu 34
Slika 13. Bitdefender povijest zaštite te poduzete akcije 35
Slika 14. Avira antivirusni program javlja sigurnosne opasnosti 36
Slika 15. Avira antivirusni program stavlja program u karantenu te pokreće sigurnosno skeniranje 37

Popis tablica

Tablica 1. Rezultati testiranja antivirusnih programa 38