# Računalni softver u funkciji zaštite od zlonamjernih prijetnji

**Ilić, Barbara**

**Undergraduate thesis / Završni rad**

**2018**

*Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj:* **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

*Permanent link / Trajna poveznica:* https://urn.nsk.hr/urn:nbn:hr:119:629631

*Rights / Prava:* In copyright / Zaštićeno autorskim pravom.

*Download date / Datum preuzimanja:* **2024-03-29**



*Repository / Repozitorij:*

Faculty of Transport and Traffic Sciences - Institutional Repository









**SVEUČILIŠTE U ZAGREBU**

**FAKULTET PROMETNIH ZNANOSTI**

**Barbara Ilić**

# RAČUNALNI SOFTVER U FUNKCIJI ZAŠTITE OD ZLONAMJERNIH PRIJETNJI

**ZAVRŠNI RAD**

**Zagreb, 2018.**

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

**ZAVRŠNI RAD**

# RAČUNALNI SOFTVER U FUNKCIJI ZAŠTITE OD ZLONAMJERNIH PRIJETNJI

# COMPUTER SOFTWARE IN THE FUNCTION OF PROTECTION AGAINST MALWARE THREATS

Mentor: dr. sc. Siniša Husnjak

Student: Barbara Ilić

JMBAG: 0135236822

Zagreb, srpanj 2018.

RAČUNALNI SOFTVER U FUNKCIJI ZAŠTITE OD ZLONAMJERNIH PRIJETNJI

SAŽETAK

Cilj ovog završnog rada jest prikazati klasifikaciju i karakteristike pojedine sigurnosne prijetnje usmjerene računalima, kao i prikazati načine zaštite računala od različitih oblika zlonamjernih prijetnji. Rad se temelji na prikazu specifikacija različitih računalnih softvera namijenjenih zaštiti od sigurnosnih prijetnji. Također, u svrhu rada obavljeno je testiranje softvera namijenjenih zaštiti od sigurnosnih prijetnji korištenih u radu. Testiranje je provedeno korištenjem Eicar testne datoteke, koja se može besplatno preuzeti u 4 različite inačice. Datoteka predstavlja standard razvijen u svrhu provođenja testiranja nad softverima namijenjenim zaštiti od sigurnosnih prijetnji bez da ostavlja trajne posljedice na sustav, a ispravan softver trebao bi datoteku detektirati kao pravi zlonamjerni softver. Na kraju rada napravljena je usporedba korištenih računalnih softvera prema podacima dobivenim testiranjem korištenjem Eicar testne datoteke, kao i prema mogućnostima koje pojedini softver pruža.

KLJUČNE RIJEČI: sigurnosne prijetnje; zaštita; sigurnost; računalni softver

SUMMARY

The purpose of this paper is to show the classification and characteristics of certain security problems for computers and to show the ways of protecting the computer from various forms of malware threats. This paper is based on the specification of various computer software designed to protect against security threats. Also, for the purpose of this paper the testing of software designed to protect against the security threats was done. Testing was done using Eicar test files, which can be downloaded for free in 4 different versions. The file represents a standard developed for testing software designed to protect against security threats without leaving any persistent consequences on the system. The right software should detect the file as real malicious software. At the end of this paper we made a comparison of used computer software according to data obtained by testing using Eicar test files as well as the capabilities provided by each software.

KEY WORDS: security threats; protection; security; computer software

# Sadržaj

1. Uvod ... 1
2. Sigurnosne prijetnje usmjerene računalima ... 2
2.1 Osnovna podjela izvora sigurnosnih prijetnji ... 2
2.1.1 Web bazirane prijetnje ... 2
2.1.2 Mrežno zasnovane prijetnje ... 3
2.1.3 Fizički zasnovane prijetnje ... 3
2.1.4 Socijalni inženjering ... 4
2.2 STRIDE klasifikacijska shema ... 5
2.2.1 Krađa identiteta (*Spoofing Identity*) ... 5
2.2.2 Napadi uskraćivanjem usluge – DoS ... 6
2.2.3 Ostali izvori sigurnosnih prijetnji ... 6
... 8
2.3 Udio pojedine vrste prijetnji ... 9
3. Klasifikacija i karakteristike zlonamjernog računalnog softvera ... 10
3.1 Računalni virus ... 10
3.1.1 Virusi prvog sektora tvrdog diska ... 11
3.1.2 Parazitski virusi ... 11
3.1.3 Svestrani virusi ... 11
3.1.4 Virusi pratioci ... 11
3.1.5 Makro virusi ... 12
3.1.6 *Link* virusi ... 13
3.2 Računalni crv ... 13
3.2.1 *Stuxnet* ... 13
3.2.2 *Duqu* ... 14
3.2.3 *Flame* ... 14
3.3 Trojanski konj ... 14
3.3.1 RAT trojanski konj ... 14
3.3.2 *Keylogger* ... 15
3.3.3 Špijunski softver ... 15
3.3.4 *Ransomware* ... 15
4. Računalni softver u funkciji zaštite od zlonamjernih prijetnji ... 16
4.1 Windows Defender ... 16

4.2 McAfee računalni softver u funkciji zaštite od zlonamjernih prijetnji ..... 19
4.3 Panda *Security* ..... 21
4.4 Avast računalni softver ..... 23
4.4.1 Avast *Internet Security* ..... 26
4.4.2 Avast *Premier* ..... 26
4.4.3 Avast *Ultimate* ..... 26
4.5 Kaspersky ..... 26
5. Usporedba softvera namijenjenih zaštiti od sigurnosnih prijetnji ..... 29
5.1 Testiranje računalnih softvera namijenjenih zaštiti od zlonamjernih prijetnji ..... 30
5.1.1 Testiranje Windows Defender računalnog softvera ..... 31
5.1.2 Testiranje McAfee računalnog softvera ..... 32
5.1.3 Testiranje Kaspersky računalnog softvera ..... 32
5.1.4 Testiranje Panda programa za računalnu sigurnost ..... 33
5.1.5 Testiranje Avast računalnog softvera ..... 34
5.2 Usporedba softvera temeljem dobivenih rezultata ..... 35
6. Zaključak ..... 36
Literatura ..... 37
Popis slika ..... 41
Popis grafikona ..... 41
Popis tablica ..... 41

# 1. Uvod

Internet predstavlja javno dostupnu paketnu mrežu, centraliziranu kao mrežu svih mreža, koju koriste milijuni korisnika diljem svijeta. Razvojem tehnologije, naglo raste broj korisnika Interneta čime raste važnost zaštite povjerljivih i osobnih podataka krajnjeg korisnika. Novijim tehnologijama raste mogućnost zaraze sustava nekim od oblika zlonamjernih prijetnji, čime krajnji korisnici postaju izloženi raznim oblicima napada, čega najčešće sami nisu svjesni. Stoga je vrlo važno informiranje krajnjeg korisnika o načinima zaštite, a sama zaštita može biti provedena na razne načine, pri čemu je najučinkovitiji način onaj u obliku korištenja računalnih softvera za zaštitu od zlonamjernih prijetnji.

U radu je obrađena tematika podjele zlonamjernih prijetnji koje svakodnevno prijete korisnicima terminalnih uređaja, te načini na koje se korisnici mogu zaštititi.

Naslov rada jest Računalni softver u funkciji zaštite od zlonamjernih prijetnji, a strukturiran je kroz 7 poglavlja, uključujući uvod i zaključak:

1. Uvod
2. Sigurnosne prijetnje usmjerene računalima
3. Klasifikacija i karakteristike zlonamjernog računalnog softvera
4. Računalni softver u funkciji zaštite od zlonamjernih prijetnji
5. Usporedba alata namijenjenih zaštiti od sigurnosnih prijetnji
6. Zaključak

U poglavlju *Sigurnosne prijetnje usmjerene računalima* obrađena je podjela prijetnji prema nekoliko različitih kriterija, pri čemu su detaljno razrađene i objašnjene sve pojedine vrste prijetnji te načini na koje se korisnici njima mogu zaraziti.

Treće poglavlje bavi se klasifikacijom zlonamjernog računalnog softvera te detaljnim karakteristikama pojedinih. Zlonamjerni softver klasificiran je prema šteti koju nanosi krajnjem korisniku terminalnog uređaja te se prema toj podjeli dijeli na 9 osnovnih skupina.

U poglavlju *Računalni softver u funkciji zaštite od zlonamjernih prijetnji* obrađeno je 5 različitih računalnih softvera koji se koriste u svrhu zaštite od zlonamjernih napada. U radu je korišteno i proučavano djelovanje sljedećih sigurnosnih softvera: Windows Defender, McAfee, Avast, Kaspersky te Panda. U svrhu rada korišteni su softveri koji su dostupni besplatno za preuzimanje koji su zatim uspoređeni s inačicama istih programa koji se mogu nabaviti po određenim cijenama.

U petom poglavlju napravljena je komparacija softvera namijenjenih zaštiti od sigurnosnih prijetnji, prema mogućnostima koje pojedini pružaju. Također je u ovom poglavlju iznesena kratka analiza pojedinog softvera na temelju svih dotadašnjih istraživanja. Računalni softveri korišteni u radu testirani su uz pomoć Eicar testne datoteke, namijenjene testiranju računalnih softvera za zaštitu od sigurnosnih prijetnji, čime se ispituje ispravnost i odziv pojedinog. Eicar testna datoteka lažna je „zlonamjerna prijetnja*“,* te se ispituje reakcija pojedinog softvera, pri čemu bi softver koji ispunjava svoju namjenu trebao detektirati datoteku kao pravu zlonamjernu prijetnju te je prema tome i tretirati.

Na kraju, u šestom poglavlju rada, donesen je jedinstven i subjektivan zaključak na temelju svega napisanog.

# 2. Sigurnosne prijetnje usmjerene računalima

Pojavom Interneta raste važnost zaštite osobnih podataka, koja se postiže na različite načine, a zaštita se provodi u skladu s osobnim potrebama krajnjeg korisnika. Prilikom zaštite i očuvanja sigurnosti krajnjeg korisnika najvažniju funkciju imaju sigurnosni mehanizmi poput brisanja povijesti pregledavanja, računalnih softvera za zaštitu od sigurnosnih prijetnji, fizičke zaštite, optimalnih lozinki te kriptiranja podataka. Sigurnosnim prijetnjama tako su najviše izloženi korisnici DSL veze, kabelskog interneta i stalnih veza, a razlog tome je stalna prisutnost korisnika na Internetu.

Zaštita podataka provodi se s ciljem sprečavanja krađe identiteta te nedopuštenog manipuliranja povjerljivim podacima krajnjeg korisnika. Fizička sigurnost također je bitan aspekt zaštite računalne infrastrukture i podataka. Fizička sigurnost obuhvaća skup metoda i sredstava korištenih u svrhu zaštite materijalne osnovice ili fizičkog dijela računala, odnosno hardvera, od neovlaštenog fizičkog pristupa sustavu te neovlaštenog korištenja njegovih resursa. U današnje vrijeme, razvojem tehnologije, razvijeni su sustavi koji omogućavaju visok stupanj fizičke zaštite. Primjer takvih sustava su nadzorne kamere, sigurnosni alarmi te posebni sustavi za zaključavanje.

Sigurnost predstavlja jedan od najbitnijih parametara važan za ostvarivanje odgovarajuće razine zaštite korisničkih podataka. U definiciji, sigurnost predstavlja sposobnost sustava da ne uzrokuje kritične ili katastrofalne posljedice, koje sa sobom nose trajna oštećenja sustava, [1]. Sukladno tome, šteta prouzrokovana djelovanjem prijetnje na sustav može se utvrditi prema vrijednosti imovine pogođene prijetnjom, ovisno o tome pogađa li prijetnja izravno povjerljive informacije krajnjeg korisnika, financijsku imovinu, osobni ugled, intelektualno vlasništvo tvrtke ili pojedinca.

## 2.1 Osnovna podjela izvora sigurnosnih prijetnji

Izvore sigurnosnih prijetnji usmjerenih računalima moguće je klasificirati u više različitih kategorija. Prema podjeli sigurnosne prijetnje dijele se u šest sljedećih skupina, prema [2]:

- *Web* bazirane prijetnje,
- Mrežno zasnovane prijetnje,
- Fizički zasnovane prijetnje,
- Aplikacijski bazirane prijetnje, koje obuhvaćaju različite vrste zlonamjernih softvera (*malware*), pri čemu zlonamjerni softver u definiciji predstavlja skup programa koji se pokreću na računalu nanoseći štetu sigurnosti sustava samog računala,
- Socijalni inženjering, te
- BYOD (*Bring Your Own Device*) [3], što predstavlja mogućnost korisnika da poslovne informacije prenese na vlastiti uređaj, noseći sa sobom rizik od krađe i otkrivanja privatnih podataka.

### 2.1.1 Web bazirane prijetnje

*Web* bazirane prijetnje mogu se podijeliti u 3 glavne kategorije, prema [2]:

1. Krađa identiteta (*phishing*),
2. Iskorištavanje internetskog preglednika, te
3. Automatsko preuzimanje aplikacija.

Prva kategorija mrežne krađe identiteta (*phishing*) odnosi se na prijevaru kojom se služe zlonamjerni korisnici, koristeći postojane Internet servise, s ciljem prikupljanja povjerljivih

podataka napadnutog korisnika, kako bi ostvarili određenu financijsku korist. Prema navodima nacionalnog središta za računalnu sigurnost (*Computer Emergency Response Team* – CERT), [4], *phishing* napad može se smatrati i vrstom socijalnog inženjeringa, a napadač koristi različite načine manipulacije kako bi od korisnika prikupio što više korisnih informacija, obuhvaćajući time lozinke, korisnička imena, pa čak i podatke s kreditnih kartica napadnutog. U pravilu, *phishing* napad se prenosi otvaranjem elektroničke pošte, koja dalje navodi napadnutog korisnika na određenu *web* stranicu zloćudnog *web* poslužitelja, obično maskiranog u lažnu stranicu banke ili slične ustanove, krivotvoreći njihov izgled, te prikupljajući tako povjerljive podatke korisnika.

Druga skupina *web* zasnovanih prijetnji, odnosno iskorištavanje *web* preglednika, odnosi se na iskorištavanje ranjivosti internetskog preglednika, koje može biti provedeno bez korisnikova znanja, a najčešće prijetnje uzrokovane ranjivošću predstavljaju prijetnje u obliku otimača preglednika (*browser hijacking*), [6]. Otimač preglednika, potencijalno je neželjeni program koji uzrokuje modifikacije u postavkama internetskog preglednika, čime se postiže mogućnost preusmjeravanja korisnika na unaprijed utvrđene stranice, za koje se ne može znati jesu li legitimne i bezopasne. Tako, napadač, odnosno kreator otimača internetskog preglednika podiže popularnost stranica na koje se korisnik preusmjerava te tako zarađuje novac.

Automatsko preuzimanje aplikacija nastupa prilikom posjeta određenoj internetskoj stranici, prilikom čega dolazi do preuzimanje aplikacija na računalo pri čemu se od korisnika mogu tražiti određena dopuštenja, međutim također je moguće preuzimanje bez poduzimanja ikakvih korisnikovih akcija i bez korisnikova znanja.

### 2.1.2 Mrežno zasnovane prijetnje

Mrežno zasnovane prijetnje, prema [2], moguće je podijeliti u dvije podskupine:

- Napade podvalom mreže, te
- Iskorištavanje mreže.

Napad podvalom mreže izveden je tako da se napadač predstavlja kao netko drugi s ciljem dobivanja pristupa ograničenim resursima uređaja ili u svrhu krađe povjerljivih podataka s istog. Takav napad može biti proveden, primjerice, postavljanjem mrežne pristupne točke na koju se korisnici zatim spajaju, a napadač tako dobiva pristup njihovim podacima.

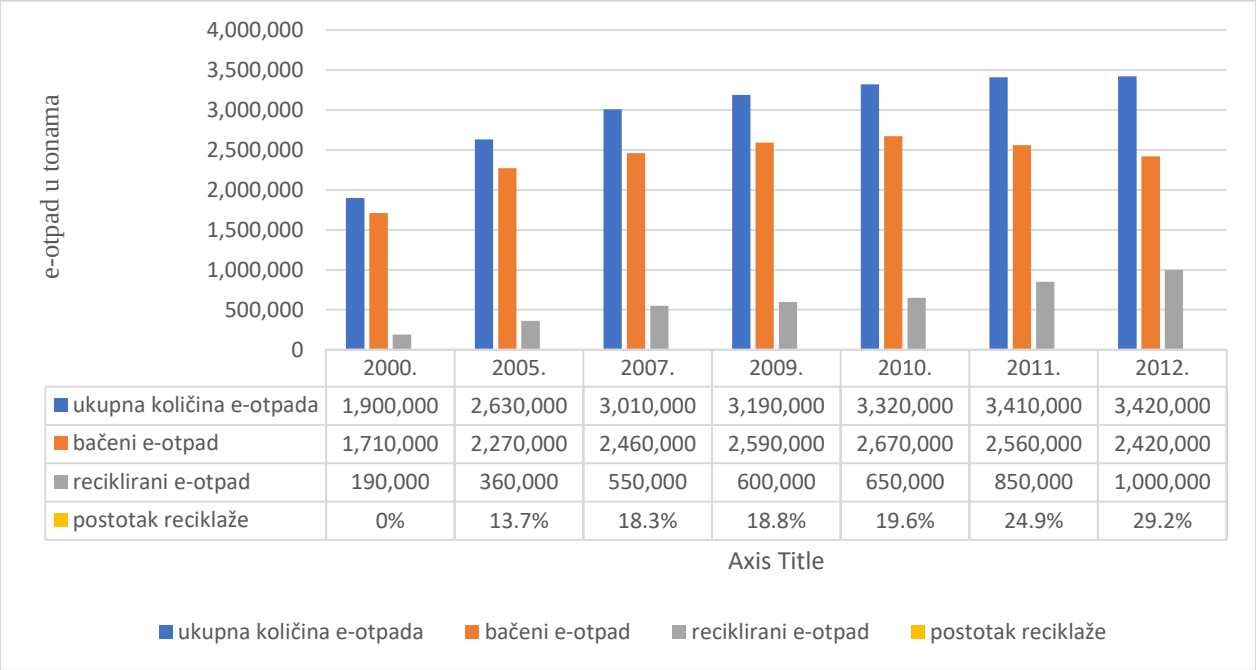
Iskorištavanje mreže vrsta je napada koja koristi programske sigurnosne propuste operativnih sustava, a često ne zahtijevaju nikakvu intervenciju korisnika, što ih čini posebno opasnima, [2].

### 2.1.3 Fizički zasnovane prijetnje

Fizički zasnovane prijetnje odnose se na prijetnje u obliku krađe, posudbe ili gubitka samog uređaja. Krađa predstavlja kazneno djelo otuđivanja pokretne ili nepokretne imovine, s ciljem protupravnog prisvajanja iste. Osim materijalne štete, veći problem predstavlja gubitak podataka, privatnih te poslovnih dokumenata, te samim time pristup povjerljivim informacijama pojedinca postaje dostupan neovlaštenoj trećoj strani, narušavajući tako povjerljivost podataka koja sama po sebi predstavlja jedan od temeljnih sigurnosnih zahtjeva koja računala trebaju ispunjavati. Prijenosna računala podložnija su krađi u odnosu na stolna, a razlog tome njihova je mobilnost.

Također, u skupinu fizički zasnovanih prijetnji mogu se svrstati napadi na uređaje namijenjene recikliranju, pri čemu je reciklaža elektroničkog otpada u zadnjih nekoliko godina u stalnom porastu.

Na grafikonu 1 prikazan je postotak reciklaže elektroničkog opada u razdoblju od 2000. do 2012. godine. U promatranom razdoblju, postotak reciklaže elektroničkog otpada je u stalnom porastu.




| | 2000. | 2005. | 2007. | 2009. | 2010. | 2011. | 2012. |
|---|---|---|---|---|---|---|---|
| ukupna količina e-otpada | 1,900,000 | 2,630,000 | 3,010,000 | 3,190,000 | 3,320,000 | 3,410,000 | 3,420,000 |
| bačeni e-otpad | 1,710,000 | 2,270,000 | 2,460,000 | 2,590,000 | 2,670,000 | 2,560,000 | 2,420,000 |
| reciklirani e-otpad | 190,000 | 360,000 | 550,000 | 600,000 | 650,000 | 850,000 | 1,000,000 |
| postotak reciklaže | 0% | 13.7% | 18.3% | 18.8% | 19.6% | 24.9% | 29.2% |

**Grafikon 1.** Postotak reciklaže elektroničkog otpada u razdoblju 2000.-2012. godine

Izvor: [7]

Ukupna količina elektroničkog otpada u promatranom razdoblju od 2000. do 2012. godine porasla je za 3230000 tona. Kao što je vidljivo na grafikonu 1 količina e-otpada raste s godinama, pri čemu također raste i postotak reciklaže bačenog otpada. S grafikona 1 je vidljivo kako je postotak reciklaže od 2000. godine do 2012. porastao za 19,20%.

### 2.1.4 Socijalni inženjering

Socijalni inženjering predstavlja skup tehnika kojima se pojedinca navodi na niz postupaka na štetu krajnjeg korisnika, u svrhu otkrivanja povjerljivih informacija, odnosno dobivanja pristupa određenim resursima koje inače napadaču nisu dostupni. Većina napada povezana sa socijalnim inženjeringom podijeljena je u četiri temeljna segmenta, prema [8]: sakupljanje informacija o žrtvi, uspostava veze sa žrtvom, pristupanje žrtvi te realizacija napada.

Socijalni inženjering, kao vrsta napada, može se klasificirati u tri osnovne podskupine, prema [8]: *phishing*, *vishing* te *impersonation*. *Phishing* napadi odnose se na napade koji se šire slanjem poruka s izvora koji djeluje povjerljivo, u svrhu prikupljanja povjerljivih informacija korisnika, primjerice broja kreditnih kartica te pinova. S druge strane, *vishing* napad vrlo je sličan *phishing* napadu, pri čemu se do povjerljivih podataka želi doći telefonskim putem, lažiranjem telefonskog broja pozivatelja. Naposljetku, *impersonation* predstavlja vrstu napada kojim se do povjerljivih informacija krajnjeg korisnika pokušava doći lažnim predstavljanjem, odnosno krađom identiteta, [8].

## 2.2 STRIDE klasifikacijska shema

Model rizika (*Threat Model*) predstavlja proces koji procjenjuje sigurnost bilo kojeg sustava temeljenog na *webu*, identificirajući područja s problemima i određujući rizik povezan sa svakim područjem. Ovaj proces, prema [9], obuhvaća pet koraka:

1. Identifikacija ciljeva sigurnosti, obuhvaćajući određivanje sveobuhvatnih ciljeva koje organizacija ima u pogledu sigurnosti i zaštite,
2. Pregled sustava, čime se određuju komponente samog sustava, putovi kroz koje informacije putuju te granice povjerenja,
3. Razvrstavanje sustava, određujući komponente sustava koje se odnose na sigurnost sustava,
4. Identifikacija prijetnje, što obuhvaća navođenje svih potencijalnih vanjskih prijetnji, fokusirajući se na one poznate, te
5. Prepoznavanje ranjivosti, razmatrajući identificirane prijetnje i određujući slabost sustava u pojedinim područjima.

STRIDE klasifikacijska shema namijenjena kategorizaciji poznatih prijetnji usmjerenih računalima, predstavlja akronim sastavljen od početnih slova svakog od šest izvora prijetnji redom, [9]:

1. Krađa identiteta (***S**poofing identity*),
2. Uplitanje (***T**ampering with data*) obuhvaća niz akcija kao što su modificiranje, dodavanje, brisanje ili mijenjanje podataka,
3. Odstupanje (***R**apudiation*) predstavlja odbijanje izvršavanja radnji, tako da se prijetnja odnosi na sposobnost sustava da se suprotstavi prijetnji odbacivanja,
4. Otktivanje informacija (***I**nformation dislosure*), obuhvaća otkrivanje podataka uključujući izlaganje informacija pojedincima koji ne bi trebali imati pristup tim podacima,
5. Napadi uskraćivanjem usluge (***D**enial of Service* – DoS) koji predstavljaju pokušaj stvaranja resursa računala nedostupnim legalnim korisnicima, te
6. Podizanje prava (***E**levation of privillege*) što predstavlja vrstu prijetnje kojom neovlašteni korisnik dobiva pristup povjerljivim podacima te je stoga u mogućnosti narušiti čitav sustav računala.

### 2.2.1 Krađa identiteta (*Spoofing Identity*)

Krađa identiteta predstavlja pokušaj krađe identiteta, tako da se napadač predstavlja kao autorizirani korisnik sustava. Krađa identiteta jedan je od najbrže rastućih napada, a obuhvaća krađu povjerljivih informacija kao što su podaci s kreditnih kartica, vozačkih dozvola, osobnih iskaznica te sličnih isprava, s ciljem lažnog predstavljanja te nanošenja manjih ili većih šteta žrtvi koja je napadnuta. Zaštitu od krađe identiteta, prema [10], moguće je provesti kroz sljedeće korake,

- Suzdržavanje od dijeljenja povjerljivih informacija putem Interneta ili telefona, u bilo kojem slučaju u kojem krajnji korisnik nije siguran u povjerljivost druge strane,
- Posebnu opreznost pridati ostavljanju svojih podataka na javno dostupnim Internetskim stranicama.

### 2.2.2 Napadi uskraćivanjem usluge – DoS

DoS napadi, [11], predstavljaju napade uskraćivanjem usluge, koje karakterizira namjerno generiranje velike količine mrežnog prometa s ciljem preopterećenja mrežnih resursa kao i samih poslužitelja. DoS napadom računalo postaje nedostupno krajnjem korisniku, kojemu su namijenjene njegove usluge.

DoS napad moguće je provesti na različite načine, pri čemu su pet osnovnih tipova napada, prema [11]:

1. Potrošnja računalnih resursa,
2. Poremećaj konfiguracijskih podataka,
3. Poremećaj informacija o stanju mreže,
4. Poremećaj fizičke komponente mreže, te
5. Prekid komunikacije među legitimnim korisnicima.

### 2.2.3 Ostali izvori sigurnosnih prijetnji

Također se u izvore sigurnosnih prijetnji, prema [48], mogu ubrojiti napadi kao što su podvala mreže (*spoofing*), napadi skeniranjem (*scanning),* napadi njuškanjem (*sniffing*), napadi čišćenjem (*scavenging*), napadi tuneliranjem (*tunneling*), *hakerski* napadi, *hoax* te *spam*.

Podvala predstavlja vrstu napada kojim napadač stvara lažni sadržaj, kako bi zavarao cjelokupan sustav ili dio mreže s ciljem krađe identiteta ili ostvarivanja protupravne imovinske koristi. Sadržaj je napisan tako da kod korisnika ne izaziva nikakvu sumnju, te tako napadač lažnim predstavljanjem pokušava doći do korisnih i povjerljivih informacija žrtve, [12].

Napadi skeniranjem, prema [48], dijele se na:

- sekvencijalno skeniranje (*sequential scanning)*, pri čemu se napadač pokušava prijaviti u sustav pokušajem različitih kombinacija lozinki, te
- *dictionary scanning*, pri čemu se napadač pokušava prijaviti u sustav korištenjem lozinki koje mogu biti rječničke riječi, kao što je lozinka.

Napad njuškanjem jedna je od najčešće metoda krađe podataka, a predstavlja presretanje, praćenje te hvatanje mrežnih aktivnosti korisnika, [13]. Napad njuškanjem može se podijeliti u dvije skupine: lokalni napad, koji obuhvaća presretanje podataka namijenjenih računalu krajnjeg korisnika te s druge strane daljinski napad, kojim se presreću podaci namijenjeni nekom drugom računalu s kojim krajnji korisnik razmjenjuje podatke.

Napadi čišćenjem, prema [48], dijele se na dvije podskupine:

- pregledavanje (*browsing*), koje obuhvaća skeniranje velikih količina nezaštićenih podataka s ciljem dobivanja pristupa povjerljivim informacijama, te
- pretraživanje smeća (*dumpster diving*), čime napadač pokušava dobiti informacije pretraživanjem otpada s ciljem dobivanja pristupa povjerljivim podacima.

Napad tuneliranjem predstavlja oblik napada koji koristi funkcije sustava niske razine, kao što su jezgra operativnog sustava ili upravljački program za uređaj, kako bi osigurali pristup sigurnosnim podacima.

*Hakeri*, odnosno osobe koje provode hakerske napade, koriste se različitim metodama kako bi pristupili računalnom sustavu bez znanja i dozvole krajnjega korisnika. Postoje različite vrste hakerskih napada, koji se generalno mogu podijeliti u četiri kategorije, prema [14]:

- Presijecanje, odnosno prekidanje, čime se prekida tok informacija, odnosno onemogućava se pružanje neke usluge ili funkcioniranje samoga sustava, te s obzirom na to napad presijecanjem može se okarakterizirati kao napad na raspoloživost sustava, zatim
- Presretanje (*interception),* može biti provedeno na više različitih načina, a najčešće je to prisluškivanje prometa na mreži te nadziranje njegovog intenziteta, pri čemu se napad presretanjem može ubrojiti u napad na povjerljivost sustava,
- Izmjena (*modification*), obuhvaća izmjenu korisničkih podataka, izmjenu pristupnih prava te načina funkcioniranja programa ili sustava, a najčešće ostaje neprimjetan određeno vrijeme, pri čemu napad izmjenom predstavlja napad na integritet, te
- Proizvodnja (*fabrication*), koja obuhvaća napade generiranjem lažnog prometa, lažnih podataka ili izdavanja neovlaštenih podataka, te samim time ova vrsta napada spada u napade usmjerene autentičnosti sustava.

*Hoax* predstavlja poruku elektroničke pošte, neistinitog sadržaja, poslana s ciljem zastrašivanja korisnika. Cilj stvaratelja *hoax*-a jest prosljeđivanje poruke na što veći broj adresa, pri čemu primatelji prosljeđuju ovakav oblik poruke misleći kako time pomažu drugima. Važno je napomenuti kako ovakav oblik napada ne može prouzrokovati nikakva znatna oštećenja sustava, osim opterećenja sustava korisnika, [47].

*Spam,* [15], predstavlja neželjenu elektroničku poruku poslanu s ciljem oglašavanja raznog reklamnog sadržaja, u svrhu *phishing* napada ili s ciljem distribucije zlonamjernih poveznica. Osim širenjem putem elektroničke pošte, *spam* se također može širiti elektroničkim forumima, blogovima, društvenim mrežama, servisima za izravnu komunikaciju te drugim sustavima za razmjenu poruka ili drugih podataka. Kako bi se spam mogao širiti, širitelji moraju prikupiti što više adresa elektroničkih pošta, a to čine preko raznih *chat*-ova, Internetskih stranica ili pak zlonamjernih prijetnji zaraženih računala. Jedan od načina zaštite od *spam*-a jest kodiranje elektroničkih adresa kako bi ona bila neprepoznatljiva.

Na stranicama neovisnog instituta za informacijsku sigurnost, [36], prikazani su statistički podaci koji prikazuju udio *spam* poruka u pojedinoj državi u posljednjih 60 dana, što je prikazano na slici 1. Statistika je napravljena na temelju registriranja, kategoriziranja te mapiranja poruka klasificiranih kao *spam*.



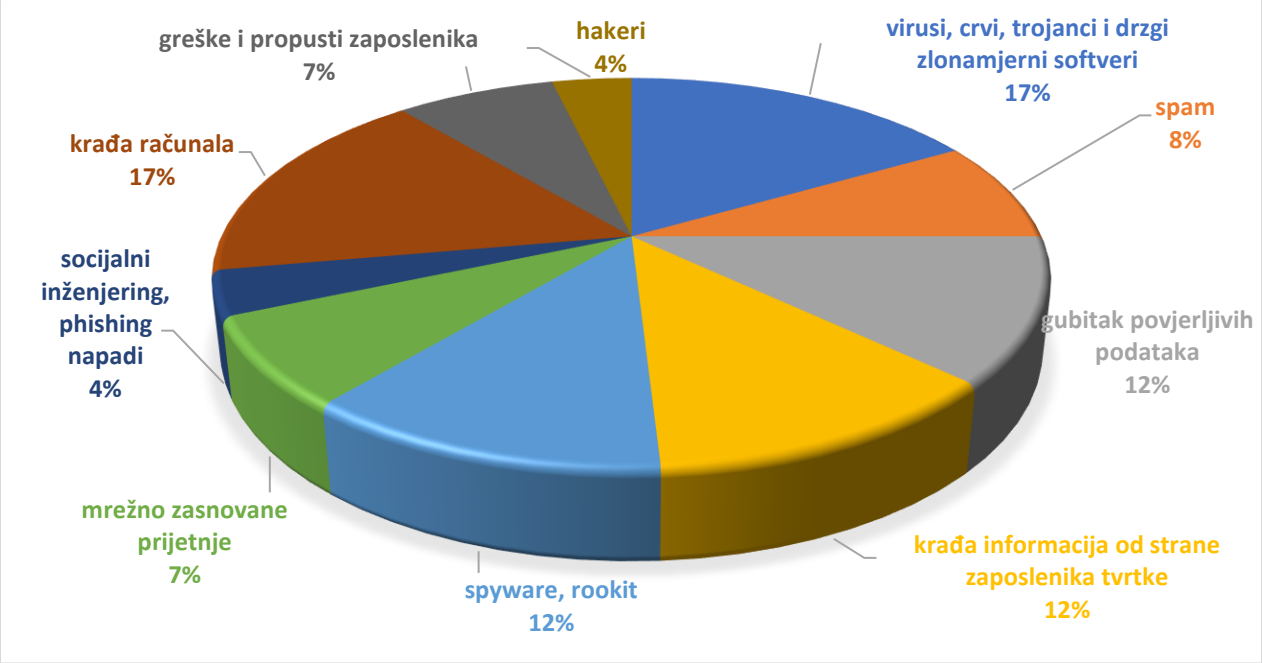

**Slika 1.** Udio *spam* poruka

Izvor: [36]

U posljednjih 60 dana, najviše *spam* poruka bilo je na području Ujedinjenog kraljevstva, na koje otpada 30,9% *spam* poruka, dok je na drugom mjestu Kina koja zauzima upola manji udio u odnosu na Ujedinjeno Kraljevstvo, s postotkom od 15,6%. Na posljednjem mjestu s najmanjim udjelom od 1,6% nalazi se Indija. Svi navedeni podaci prikazani su na slici 1.Važno je napomenuti kako podaci nisu stalni već se mijenjanju iz tjedna u tjedan.

## 2.3 Udio pojedine vrste prijetnji

Sigurnosne prijetnje namijenjene računalima mogu se klasificirati prema više različitih kriterija. Na grafikonu 2 prikazan je udio koji se odnosi na količinu pojedine vrste zlonamjernih prijetnji na sustav, dobivena istraživanjem provedenom 2013. godine, prema [4]. Shodno tome, najveći broj napada na sustav uzrokovan je nekom vrstom zlonamjernog softvera, primjerice virusa, crva i sl. te prema statistici ovaj oblik napada zauzima 18% ukupnog udjela, a jednaki udio zauzimaju i fizički napadi u obliku krađe računala. Odmah zatim slijede napadi uzrokovani krađom povjerljivih informacija od strane zaposlenika same tvrtke, na koje otpada 13% ukupnog udjela, dok gubitak povjerljivih podataka također zauzima 13% ukupnog udjela. Napadi u obliku *spam-a* zauzimaju 9% ukupnog udjela, slijede greške i propusti zaposlenika tvrtke s 8%, jednako kao i mrežno zasnovane prijetnje uključujući i napade uskraćivanjem usluge. Najmanji udio otpada na *hakere* te socijalni inženjering, koji zauzimaju 4% ukupnog udjela. Važno je napomenuti kako se ovi udjeli mijenjaju iz godine u godinu.




**Grafikon 2.** Udio pojedine vrste prijetnji na sustav

Izvor: *[4]*

Virusi, crvi, trojanski konji i drugi zlonamjerni softveri očekivano zauzimaju prvo mjesto u ukupnom udjelu, budući da korisnici terminalnih uređaja najčešće nisu ni svjesni izloženosti napadima, pa tako zanemaruju korištenje računalnih softvera za zaštitu od prijetnji čime postaju laka meta *hakerima* i ostalim napadačima.

# 3. Klasifikacija i karakteristike zlonamjernog računalnog softvera

Zlonamjerni softver (*malicious software*) predstavlja softver dizajniran tako da je u mogućnosti pokrenuti se na računalu samostalno, bez korisnikovog pristanka, s ciljem nanošenja štete napadnutom računalu. Zlonamjerni softver klasificira se prema šteti koju nanosi zaraženom računalu te se prema tome može podijeliti u devet skupina, prema [49]:

- Virus,
- Crv,
- Trojanski konj,
- Špijunski softver (*spyware*),
- Zlonamjerni *adware*, naziv je za program koji napada računalo preusmjeravanjem zahtjeva za pretraživanje na oglašivačke *web* stranice, prikupljajući tako podatke o vrsti *web* stranica koje se posjećuju, [16],
- *Crimeware*, koji predstavlja svaki oblik zlonamjernog koda koji potiče i pomaže u kriminalnim radnjama putem računala, uključujući krađu identiteta, ucjene te krađu osobnih podataka, [17], čiji je krajnji cilj ostvarivanje određene imovinske koristi,
- *Scareware*, predstavlja oblik zlonamjernog softvera koji se širi prijevarom korisnika, [18],
- *Ransomware*, te
- *Rootkit*, odnosno tajni računalni program, koji se koristi kako bi osigurao pristup računalu, skrivajući svoje postojanje i nedozvoljene radnje od korisnika i samog sustava, [19]. *Rootkit* predstavlja računalni program osmišljen kako bi prikrio postojanje malicioznih programa unutar računala te kako ih antivirusni program ne bi mogao detektirati. Upravo zbog mogućnosti prikrivanja, smatra se jednim od najopasnijih zlonamjernih kodova.

## 3.1 Računalni virus

Računalni virus vrsta je zlonamjernog softvera konstruiran tako da svojom reprodukcijom može zaraziti računala tako da se bez korisnikovog znanja i pristanka replicira u datotečni sustav ili memoriju ciljanog računala. Tehnički gledano, računalni virus vrsta je zlonamjernog koda ili programa, napisan da bi mijenjao način rada računala, a dizajniran kako bi se prenosio s jednog računala na drugo. Najčešće se širi u obliku izvršnog zlonamjernog koda putem Interneta, privitaka u e-mailovima ili putem zaraženih medija poput vanjskog hard diska ili pak USB kablova. Prema svojoj strukturi, računalni virus kao program ne razlikuje se od drugih programa koje krajnji korisnici svjesno koriste na računalu, stoga računalo samo po sebi ne može razlikovati virus od ostalih programa te je iz tog razloga vrlo važno korištenje te redovno ažuriranje i održavanje antivirusnih programa, u svrhu zaštite računala od raznih oblika napada i virusa, [20].

Prema načinu funkcioniranja, računalne viruse moguće je podijeliti u šest osnovnih skupina, prema [22]:

- Virusi prvog sektora tvrdog diska (*boot viruses*),
- Parazitski virusi,
- Svestrani virusi,
- Virusi pratioci,
- Link virusi, te
- Makro virusi.

### 3.1.1 Virusi prvog sektora tvrdog diska

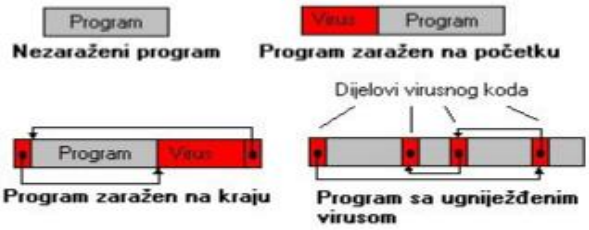
Računalni virusi također se mogu klasificirati prema okruženju koje napadaju. Pod pojam okruženje podrazumijeva se aplikacija ili operativni sustav čije je prisustvo potrebno kako bi virus inficirao datoteke. Virusi prvog sektora tvrdog diska (*boot virusi*) funkcioniraju na bazi algoritma koji pokreće operativni sustav, a širi se tako što napada boot sektor, briše podatke iz njega, a to mjesto replicira kopijom samog sebe.

Dvije su osnovne vrste mehanizma zaraze virusom, direktna te indirektna zaraza. Virusi prvog sektora tvrdog diska najčešće se ponašaju kao indirektni virusi pri zarazi koja se prenosi putem zaražene diskete te kao direktni virusi pri napadu na tvrdi disk računala, [21].

### 3.1.2 Parazitski virusi

Parazitski virusi mijenjaju kod zaražene datoteke te zaražena datoteka pri tome ostaje djelomično ili potpuno funkcionalna. Parazitski virusi je jedan od najraširenijih oblika virusa, a kako bi prikrio svoju prisutnost aktivira se u početni program koji se otvara, mijenjajući tok inficiranog programa tako da se virusni kod izvrši prvi.

Na slici 2 prikazan je način funkcioniranja parazitskog virusa. Prvi dio predstavlja nezaraženi program, zatim program koji je zaražen virusom na početku, program koji je zaražen virusom na kraju, te program s ugniježđenim virusima unutar njega.




**Slika 2.** Prikaz načina rada parazitskih virusa

Izvor: [22]

Parazitski računalni virusi sposobni su zaraziti .COM, .EXE, .SYS, .OVL i druge datoteke, [22].

### 3.1.3 Svestrani virusi

Svestrani virusi (*multipartite viruses*) koji se još nazivaju i hibridnim virusima, vrsta su zlonamjernog programa koji se širi velikom brzinom, sposobni zaraziti i *boot* sektore i izvršne programe, povećavajući tako mogućnost širenja. Svestrani virusi u mogućnosti su inficirati jedno računalo više puta i u različitom vremenskom periodu, [22].

### 3.1.4 Virusi pratioci

Virusi pratioci predstavljaju najjednostavniji oblik računalnog virusa, koristeći prioritete kojima se izvršavaju programi s istim imenom pod DOS-om, [23]. Datoteke s ekstenzijom .com izvršavaju se prije datoteka s ekstenzijom .exe. Virus pratioc najprije stvara datoteku s ekstenzijom .com koristeći ime već postojeće datoteke s ekstenzijom .exe te unutar nje ugrađuje svoj kod.

Način na koji rade virusi pratioci je jednostavan; nakon pozivanja programa, umjesto originala sa .exe sufiksom, najprije se izvršava podmetnuti .com program koji sadrži virusni kod, što je prikazano na slici 3. Nakon što je virusni kod izvršen, on vraća kontrolu programu s ekstenzijom .com.




**Slika 3.** Način rada virusa pratioca

Izvor: [22]

Važno je napomenuti da ova vrsta virusa ne ostavlja značajnu štetu na računalu i samom sustavu.

### 3.1.5 Makro virusi

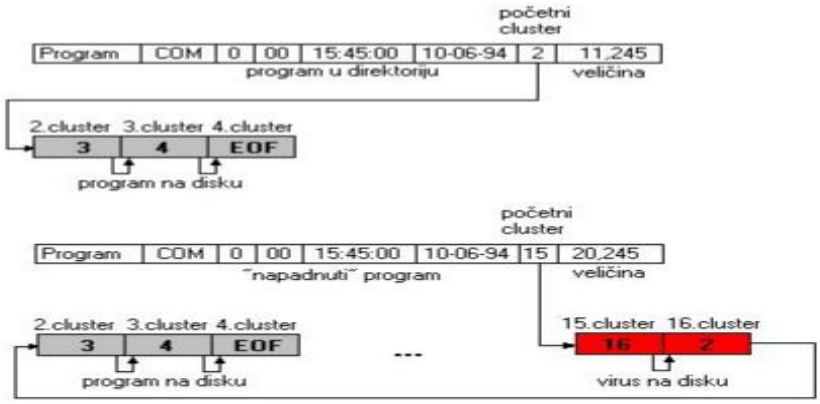
Makro virus, [23], predstavlja oblik virusa napisan na istom makro jeziku koji se koristi za softverske aplikacije, kao što su obrađivači teksta, primjerice Microsoft Word ili Microsoft Excel. Makro virusi prenose se ugrađivanjem zlonamjernog koda u makro naredbe koje su povezane s dokumentima, tablicama i drugim podatkovnim datotekama, čime se zlonamjerni program pokreće prilikom samog otvaranja zaraženih dokumenata. Tipično se makro virusi šire sumnjivim privicima elektroničke pošte namijenjenim krađi identiteta napadnutog korisnika. Tako se širenje odvija vrlo brzo, prosljeđivanjem zaraženih privitaka među korisnicima. Neki makro virusi mogu uzrokovati nepravilnosti u tekstualnim datotekama, kao što su nedozvoljeno mijenjanje ili brisanje sadržaja unutar datoteke. S druge strane, ova vrsta zlonamjernog programa ima mogućnost pristupanja računima elektroničke pošte, što omogućuje nedozvoljeno prosljeđivanje kopija zaraženih datoteka svim kontaktima korisnika, koji zatim otvaraju te datoteke, jer dolaze iz pouzdanih izvora, te se tako makro virus širi.

Budući da se makro virusi obično šire u aplikacijskim datotekama dijeljenim putem elektroničke pošte, obrana od ove vrste virusa uključuje metode skeniranja ulaznih privitaka elektroničke pošte, sprječavajući tako otvaranje sumnjivih datoteka te prenošenje virusa. Bitan način zaštite od makro virusa jest i korištenje i redovito održavanje programa namijenjenih zaštiti od zlonamjernih prijetnji, kao i korištenje filtara za neželjenu poštu, čime se umanjuje vjerojatnost da će računalo biti zaraženo zlonamjernim softverom. Također je bitno ne otvarati privitke elektroničke pošte sumnjivog sadržaja, čak i kada se čini da su od pouzdanih izvora te onemogućiti korištenje makronaredbi u potpunosti.

Ako je računalo već zaraženo makro virusom, vrlo je bitno isti ukloniti iz sustava računala. Prvi korak pri uklanjanju ovog oblika virusa jest ponovno pokretanje sustava računala u sigurnom načinu rada (*Safe Mode*). Od pomoći također može biti i brisanje privremenih datoteka na računalu. Naposljetku je potrebno napraviti skeniranje računala pomoću nekog od programa za zaštitu od zlonamjernih prijetnji koji će detektirati virus i sigurno ga ukloniti iz sustava.

### 3.1.6 *Link* virusi

*Link* virusi predstavljaju najinfektivniji oblik virusa, koji se vrlo brzo šire kroz sustav, nakon što su jednom pokrenuti. Princip rada link virusa prikazan je na slici 4.




**Slika 4.** Način rada link virusa

Izvor: [22]

Djeluju po principu mijenjanja pokazivača u strukturi direktorija te ih tako preusmjeravaju na *cluster* u disku gdje je prethodno sakriven virusni kod, [22]. Na slici 4 prikazan je način rada *link* virusa.

## 3.2 Računalni crv

Računalni crv predstavlja oblik zlonamjernog softvera dizajniran kako bi se širio kroz računalnu mrežu, neprestano se umnožavajući, zagušujući tako promet podataka na mreži li zatrpavajući podacima memoriju hard diska, sve dok ona ne postane posve puna. Crvi, identično kao i virusi, repliciraju funkcionalnu kopiju sebe, te mogu prouzročiti jednaku štetu kao i računalni virus. Računalni crvi troše veliku količinu memorije, pa *web* i mrežni poslužitelji, te sama računala, u jednom trenutku prestaju reagirati. Tipično se crv širi preko računalnih mreža, iskorištavanjem ranjivosti operativnog sustava. otvaranjem privitaka elektroničke pošte sumnjivog sadržaja, a nakon što uđu u računalo, crvi spontano stvaraju dodatne poruke elektroničke pošte koje sadrže kopije crva te se tako šire dalje, [20].

Računalni crv, [24] predstavlja jednu od najčešćih vrsta zlonamjernih prijetnji. Temeljna razlika između računalnog crva i virusa je u načinu prenošenja, pri čemu je za inficiranje računala virusom potreban neki oblik ljudske aktivnosti, dok crv, s druge strane, može inficirati sustav bez ikakve inicijacije od strane krajnjeg korisnika.

Računalni crvi uzrokovali su milijarde dolara štete u proteklih nekoliko desetljeća. Neki od poznatijih crva su svakako *Stuxnet, the Duqu* i *the Flame.*

### 3.2.1 *Stuxnet*

*Stuxnet,* [25], zlonamjerni je računalni crv, najprije detektiran od strane *Kaspersky* laboratorija za računalnu zaštitu, u lipnju 2010. godine, koji se širi iskorištavanjem ranjivosti operativnog sustava Windows. *Stuxnet* crv odgovoran je za uništavanje iranskog nuklearnog programa.

### 3.2.2 *Duqu*

*Duqu* predstavlja zbirku računalnih zlonamjernih programa, otkrivenih u rujnu 2011. godine, pri čemu se prvotno mislilo da je *Duqu* zapravo *Stuxnet* crv. Laboratorij za kriptografsku i sistemsku sigurnost sa sjedištem u Mađarskoj, detektira prijetnju koju imenuje *Duqu*, prema prefiksu 'DQ' koji daje naziv datotekama koje stvara, [26] .

### 3.2.3 *Flame*

*Flame* predstavlja zlonamjerni program koji se aktivno koristi kao cyber oružje za ciljne entitete u nekoliko zemalja. Otkriven je od strane *Kaspersky* laboratorija za računalnu sigurnost u suradnji s Međunarodnim telekomunikacijskim savezom (ITU). Osnovni cilj mu je krađa povjerljivih informacija, [27].

## 3.3 Trojanski konj

Trojanski konj vrsta je zlonamjernog programa čiji je primarni cilj inficiranje ciljanog računalnog sustava, pri čemu se takvi programi najčešće koriste u svrhu krađe osobnih podataka, širenje drugih virusa ili smanjenje performansi cjelokupnog računala. Trojanski konj najčešće dolazi u obliku nekog legitimnog programa, s ciljem prikrivanja svoga postojanja te kako bi tako od krajnjeg korisnika dobio dozvolu za instalaciju. Za razliku od virusa, trojanski konj nema mogućnost repliciranja i prenošenja na druge legitimne datoteke, a budući da je skriven unutar sustava, krajnji korisnik ne može ga sam detektirati, te stoga on ostavlja znatne posljedice na sustav narušavajući sigurnost samog korisnika, [28].

Trojanski konj može se klasificirati prema počinjenoj šteti na zaraženom računalu u četiri sljedeće kategorije, prema [29]:

1. Alat za daljinsko administriranje (*Remote Administration Tools* - RAT),
2. *Keylogger*-e,
3. *Password retreivers*, koji predstavlja oblik trojanskog konja koji traži lozinke na računalu i registru te ih kao takve šalje napadaču putem elektroničke pošte, te
4. FTP trojanske konje, koji napadaču omogućuju pristup žrtvinom računalu, korištenjem protokola za prijenos datoteka (*File Transfer Protocol* – FTP), s ciljem pristupanja povjerljivim informacijama korisnika.

### 3.3.1 RAT trojanski konj

RAT trojanski konj vrsta je trojanskog konja čiji je princip rada taj da pokreće server na računalu žrtve te tako omogućuje napadaču pristup žrtvinom računalu, pri čemu je velika vjerojatnost da će u sustavu neko vrijeme ostati neopažen. RAT kao vrsta zlonamjernog softvera sastavljen je od dva dijela: glavnog programa koji se nalazi na računalu napadača, te servera koji se šalje žrtvi kojega je moguće ga poslati na dva načina; samostalno ili unutar nekog, već postojećeg programa.

Budući da RAT omogućuje administrativnu kontrolu nad računalom žrtve, napadaču je moguće mijenjanje i upravljanje svim stavkama na ciljanom računalu, uključujući, [30]:

1. Praćenje ponašanja korisnika putem *keylogger-a* ili drugih špijunskih softvera,
2. Pristup povjerljivim informacijama krajnjeg korisnika, kao što su korisnička imena, lozinke, brojevi kreditnih kartica te podataka s osobnih iskaznica i sličnih isprava,
3. Aktivacija web kamere računala te snimanje videozapisa,
4. Distribuiranje raznih drugih virusa i zlonamjernih programa,

5. Oblikovanje pogona, te
6. Brisanje, preuzimanje te mijenjanje datoteka i datotečnih sustava.

### 3.3.2 *Keylogger*

*Keylogger* vrsta je zlonamjernog softvera koji spada u skupinu trojanskih konja, a kao što mu i sam naziv govori, primarni cilj mu je praćenje slova unesenih uz pomoć tipkovnice, što predstavlja opasnost od otkrivanja povjerljivih podataka, uključujući sva korisnička imena i lozinke. Keylogger prati i pamti svaki otisak koji može identificirati, vraćajući informacije nazad samom dizajneru zlonamjernog softvera. Što se tiče zaštite od ovog oblika trojanskog konja, računalni softveri namijenjeni zaštiti od zlonamjernih prijetnji nemaju mogućnost detekcije *keylogger-a*, a najbolji način zaštite jest zaštita od nenamjernog odavanja lozinki, [31].

### 3.3.3 Špijunski softver

Špijunski softver (*spyware)* predstavlja vrstu zlonamjernog softvera čija je svrha preuzimanje kontrole na računalu na koji se proširi bez znanja i dozvole krajnjeg korisnika. Za razliku od virusa i crva, obično se ne replicira, a najčešći način zaraze špijunskim softverom je posjetom zaraženih internetskih stranica. Predstavlja ozbiljnu prijetnju sigurnosti i pouzdanosti sustava, te kao posljedicu za sobom ostavlja bitnu degradaciju performansi računala, koje se očituju u opterećenju procesora, zauzimanjem prostora na disku, a i povećanjem mrežnih aktivnosti, [32]. Radi zaštite od špijunskog softvera koriste se posebni programi namijenjeni uklanjanju ovog oblika zlonamjerne prijetnje (*anti-spyware* program), koji služe detekciji i otklanjanju špijunskog softvera iz sustava računala.

### 3.3.4 *Ransomware*

*Ransomware*, [33], jest naziv za skup zlonamjernih programa, koji krajnjem korisniku onemogućuju korištenje vlastitog računala. Od korisnika čije je računalo zaraženo traži se određena otkupnina u zamjenu za daljnje korištenje računala. *Ransomware* zlonamjerni softver u mogućnosti je šifrirati povjerljive podatke korisnika, uključujući poslovne dokumente, tražeći pri tom otkupninu za dešifriranje. Također, takvi programi imaju sposobnost brisanja unaprijed određenih dokumenata i datotečnih sustava, te se ujedno mogu koristiti u svrhu krađe.

# 4. Računalni softver u funkciji zaštite od zlonamjernih prijetnji

Računalni softver u funkciji zaštite od zlonamjernih prijetnji predstavlja softver namijenjen zaštiti, detekciji i otklanjaju zlonamjernih prijetnji usmjerenih računalima koje mogu prouzročiti probleme i oštećenja sustava. Predstavlja prvi korak zaštiti računala i osobnih podataka. Vrlo često je zlonamjerne prijetnje moguće povezati s velikim financijskim gubicima, naročito kada je riječ o infekcijama većih poduzeća ili tvrtki, [34]. Shodno tome, korištenje sigurnosnog softvera, odnosno softvera za zaštitu od zlonamjernih prijetnji, vrlo je bitan korak pri zaštiti sigurnosti krajnjeg korisnika, kao i zaštiti povjerljivih podataka pojedinca ili tvrtke. U svrhu rada korišteno je i testirano djelovanje pet različitih računalnih softvera namijenjenih zaštiti od zlonamjernih prijetnji: Windows Defender, McAfee, Panda, Avast te Kaspersky.

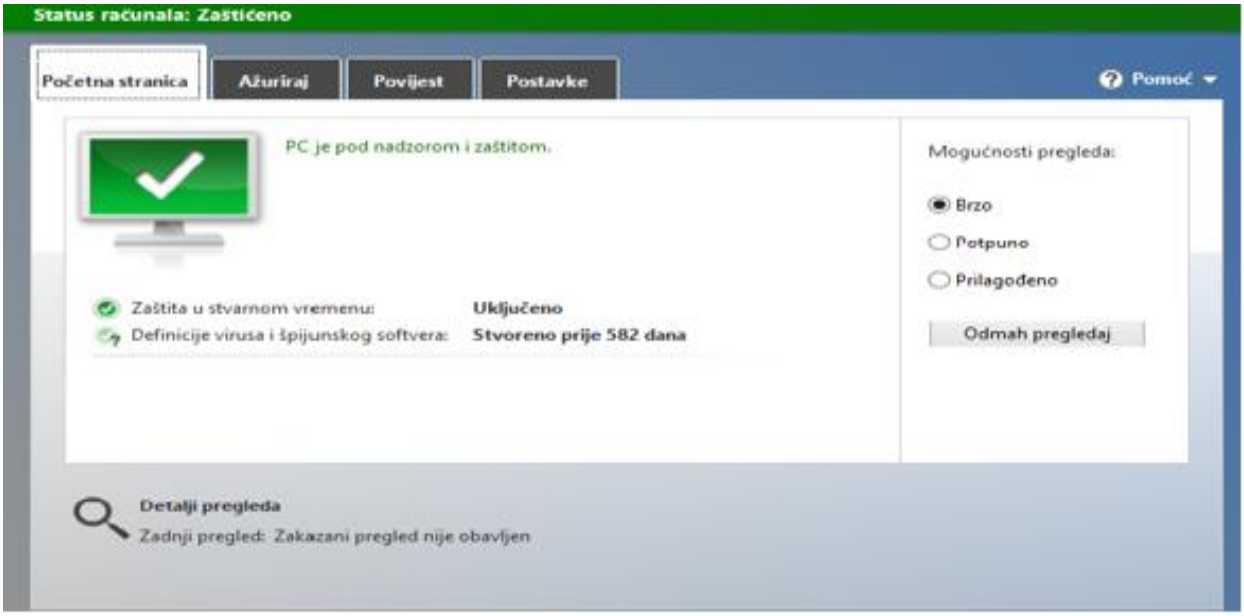
## 4.1 Windows Defender

Windows Defender računalni je softver namijenjen zaštiti od zlonamjernih prijetnji, a kod novijih operativnih sustava (OS), odnosno OS Windows 8 te 10, dolazi instaliran u kompletu sa samim OS. Windows Defender, [35], koristi zaštitu u realnom vremenu za pregled preuzimanja te programa koji se koriste na računalu. Zaštitu u stvarnom vremenu također je moguće isključiti u bilo kojem trenutku, no ona će se sama ponovno automatski uključiti nakon nekog vremena kako bi zaštitila sustav od mogućih i potencijalnih napada. Dok je zaštita isključena, Windows Defender neće vršiti pregled preuzimanja te programa koji se koriste na računalu, čime se potencijalno ugrožava sigurnost samog sustava.

Zaštita pomoću Windows Defender softvera provedena je u sedam segmenata, prema [35]:

- Zaštita od zlonamjernih prijetnji, što obuhvaća pregled sustava računala radi otkrivanja potencijalno opasnih programa,
- Zaštita računa,
- Vatrozid i zaštita mreže, čime se postiže filtriranje mrežnog prometa radi stvaranja sigurnosne zone,
- Kontrola aplikacija i preglednika, što omogućuje zaštitu uređaja od preuzimanja i korištenja potencijalno opasnih aplikacija, datoteka te web mjesta,
- Sigurnost uređaja, što obuhvaća zaštitu od napada zlonamjernog softvera,
- Performanse i stanje uređaja, omogućavajući održavanje uređaja ažurnim, te
- Mogućnost obiteljskih značajki, što omogućuje praćenje aktivnosti djece na internetu.

Windows Defender radi u pozadini sustava te izbacuje obavijest kada detektira potencijalu prijetnju na računalu. Bez obzira na to, moguće je napraviti pregled sustava računala u bilo kojem trenutku. Na slici 5 prikazano je samo sučelje Windows Defender računalnog softvera. Sa slike je vidljivo kako je uz pomoć programa Windows Defender moguće provesti tri načina pregleda sustava: brzo, potpuno i prilagođeno. Potpunim pregledom program vrši skeniranje cjelokupnog sustava računala, ispitujući postojanje potencijalnih prijetnji na sustav te ih uklanjajući, ako takve postoje, dok se prilagođenim pregledom vrši pregled odabrane datoteke, programa ili mjesta na računalu, također radi ispitivanja postojanja bilo kakvog neželjenog ili sumnjivog sadržaja unutar sustava.




**Slika 5.** Sučelje Windows Defender računalnog softvera

Neovisni institut za informacijsku sigurnost (*The independent IT- Security Institute)* vodeći je međunarodni i neovisni pružatelj usluga na području informatičke sigurnosti te testiranja programa namijenjenih zaštiti od sigurnosnih prijetnji. Cilj istraživanja koje ovaj institut provodi je u vidu izravnog otkrivanja najnovijih zlonamjernih programa, kao i testiranja pojedinog računalnog softvera namijenjenog zaštiti od zlonamjernih prijetnji, provođenjem raznih analiza pomoću najsuvremenijih metoda. Na stranicama instituta za informacijsku sigurnost, provođenjem testiranja pojedinog računalnog softvera za zaštitu od sigurnosnih prijetnji, testirani programi se rangiraju prema tri faktora, zaštita, performanse te iskoristivost, te ih se prema tome ocjenjuje brojevima na skali od 0 do 6, [36].

U tablici 1 prikazani su rezultati toga testa provedenog na softveru Windows Defender na OS Windows 8.0/8.1 te na OS Windows 10. Iz tablice 1, prema ocjenama u vidu zaštite sustava, vidljivo je kako je u razdoblju od 2014. do prosinca 2015. Windows Defender računalni softver, testiran na OS Windows 8.0/8.1 pružao vrlo nisku razinu zaštite. Aritmetičkom sredinom vrijednosti iz tablice 1, prosječna ocjena ovog softvera, testiranog na OS Windows 8.0/8.1, na području zaštite jest niskih 1.9/6.0, dok su u ostala dva područja ocjene više: 4.7/6.0 za performanse te 5.9/6.0 za iskoristivost.

U tablici 1 također su prikazani rezultati testiranja Windows Defender računalnog softvera provedenog na OS Windows 10, u razdoblju od travnja 2016. do prosinca 2017. Na OS Windows 10, Windows Defender računalni softver ostvario je bolje rezultate u vidu zaštite sustava u odnosu na OS Windows 8.0/8.1, pri čemu je ostvarena prosječna ocjena za zaštitu 4.7/6.0, dobivena aritmetičkom sredinom vrijednosti navedenih u tablici 2. Na preostala dva polja, softver je dobio lošije ocjene u odnosu na testiranje provedeno na OS Windows 8.0/8.1, pri čemu je prosječna ocjena na polju performansi 4.4/6.0, dok je prosječna ocjena za iskoristivost 4.5/6.0.

**Tablica 1.** Rezultati testiranja Windows Defender-a

| **OS Windows 8.0/8.1** | | | |
|---|---|---|---|
| | **Zaštita** | **Performanse** | **Iskoristivost** |
| **Prosinac 2016.** | 4,5/6,0 | 5,5/6,0 | 6,0/6,0 |
| **Lipanj 2016.** | 4,0/6,0 | 5,5/6,0 | 5,5/6,0 |
| **Prosinac 2015.** | 4,5/6,0 | 5,0/6,0 | 6,0/6,0 |
| **Lipanj 2015.** | 0,5/6,0 | 3,0/6,0 | 6,0/6,0 |
| **Veljača 2015.** | 0,0/6,0 | 3,5/6,0 | 6,0/6,0 |
| **Listopad 2014.** | 0,0/6,0 | 5,5/6,0 | 6,0/6,0 |
| **Travanj 2014.** | 0,0/6,0 | 5,0/6,0 | 6,0/6,0 |
| **OS Windows 10** | | | |
| **Prosinac 2017.** | 6,0/6,0 | 5,5/6,0 | 4,0/6,0 |
| **Listopad 2017.** | 6,0/6,0 | 5,5/6,0 | 4,0/6,0 |
| **Lipanj 2017.** | 5,5/6,0 | 6,0/6,0 | 6,0/6,0 |
| **Travanj 2017.** | 4,5/6,0 | 4,5/6,0 | 6,0/6,0 |
| **Listopad 2016.** | 3,0/6,0 | 4,5/6,0 | 5,5/6,0 |
| **Travanj 2016.** | 3,0/6,0 | 5,0/6,0 | 6,0/6,0 |

Izvor: *[36]*

Što se tiče prednosti ovog računalnog softvera, Windows Defender će se u slučaju preuzimanja bilo kojeg drugog softvera za zaštitu od zlonamjernih prijetnji automatski isključiti, kako bi drugi softver mogao nesmetano raditi i time štititi sustav od potencijalnih opasnosti. Prednost Windows Defender-a također je i ta što je ovaj softver, korišten na OS Windows 8 te

Windows 10, u potpunosti besplatan. Ipak, ovaj softver predstavlja neku vrstu osnovne zaštite računala, te je moguće pronaći puno kvalitetnije softvere na internetu, također besplatne za preuzimanje.

## 4.2 McAfee računalni softver u funkciji zaštite od zlonamjernih prijetnji

McAfee računalni je softver namijenjen zaštiti od zlonamjernih prijetnji, s ciljem zaštite sigurnosti potrošača, malih ili velikih tvrtki kao i različitih poduzeća. McAfee računalni softver za zaštitu od prijetnji dostupan je u četiri verzije, a u svrhu rada testirano je djelovanje besplatne verzije.

U tablici 2 prikazani su rezultati testiranja McAfee softvera za zaštitu od zlonamjernih prijetnji na OS Windows 8.0/8.1 te na OS Windows 10, provedenog od strane neovisnog instituta za informacijsku sigurnost. Testiranje je provedeno prema tri kriterija: zaštita, performanse te iskoristivost, prema čemu je računalni softver ocijenjen ocjenama na skali od 0 do 6 za svako pojedino područje. Iz tablice 2 vidljivo je kako su ovi podaci relativni, te se mijenjaju iz godine u godinu. Prema aritmetičkoj sredini vrijednosti iz tablice 3, prosječna ocjena koju je McAfee računalni softver ostvario testiranjem na OS Windows 8.0/8.1 u području zaštite jest 5.4, u području performansi 5.5 te u području iskoristivosti 5.9.

U tablici 2 također su prikazani su rezultati testiranja istog softvera, od strane neovisnog instituta za informacijsku sigurnost, provedenih na OS Windows 10, u razdoblju od 2016. do 2017. godine. Aritmetičkom sredinom vrijednosti iz tablice 2, softver je ostvario prosječni rezultat od 5.0 u području zaštite, 5.6 na području performansi te 6.0 u području iskoristivosti.

**Tablica 2.** Rezultati testiranja McAfee softvera za zaštitu od prijetnji

| **OS Windows 8.0/8.1** | | | |
|---|---|---|---|
| | **Zaštita** | **Performanse** | **Iskoristivost** |
| **Prosinac 2017.** | 5,5/6,0 | 5,5/6,0 | 6,0/6,0 |
| **Listopad 2017.** | 5,0/6,0 | 5,5/6,0 | 6,0/6,0 |
| **Lipanj 2017.** | 5,5/6,0 | 6,0/6,0 | 6,0/6,0 |
| **Travanj 2017.** | 6,0/6,0 | 5,5/6,0 | 6,0/6,0 |
| **Listopad 2016.** | 5,5/6,0 | 5,5/6,0 | 5,5/6,0 |
| **Travanj 2016.** | 5,5/6,0 | 5,0/6,0 | 6,0/6,0 |
| **Travanj 2014.** | 6,0/6,0 | 5,5/6,0 | 6,0/6,0 |
| **OS Windows 10** | | | |
| **Prosinac 2017.** | 6,0/6,0 | 6,0/6,0 | 6,0/6,0 |
| **Lipanj 2017.** | 5,5/6,0 | 6,0/6,0 | 6,0/6,0 |
| **Travanj 2017.** | 4,5/6,0 | 5,5/6,0 | 6,0/6,0 |
| **Listopad 2016.** | 5,5/6,0 | 5,5/6,0 | 6,0/6,0 |
| **Travanj 2016.** | 3,5/6,0 | 5,0/6,0 | 6,0/6,0 |

Izvor: *[36]*

Osim besplatne inačice McAfee softvera za zaštitu od prijetnji, na internetu ga je moguće nabaviti u još tri različite verzije, [37]: McAfee *Antivirus Plus,* McAfee *Internet Security* te McAfee *Total Protection*.

McAfee *Antivirus Plus* s jednom godinom zaštite, prema [39], omogućuje:

- Zaštitu računala od zlonamjernih prijetnji,
- Zaštitu kućne mreže,
- Alate za optimizaciju PC računala,
- Zaštitu Apple i Mac računala,
- Zaštitu iOS mobitela i tableta,
- Zaštitu Android mobitela i tableta, te
- Sigurnost društvenih mreža.

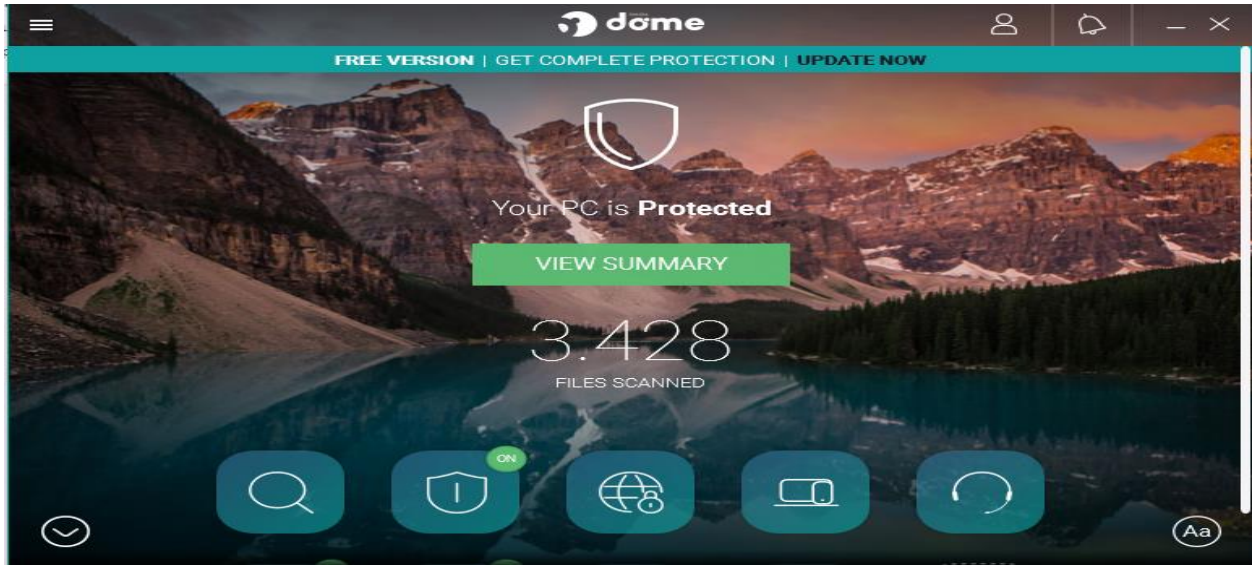
Druga inačica ovog programa trenutno ponuđenog na tržištu, McAfee *Internet Security* u odnosu na McAfee *Antivirus Plus*, obuhvaća zaštitu u vidu anti-spam-a, te također roditeljsku zaštitu, čime je omogućeno praćenje ponašanja djece na internetu. Posljednja inačica, McAfee *Total Protection* također uz sve navedene mogućnosti uključuje zaštitu u vidu zaključavanja datoteka.

## 4.3 Panda *Security*

Panda *Security* tvrtka je za računalnu sigurnost koja pruža rješenja vezana za informacijsku sigurnost krajnjeg korisnika. Osnovana je 1990. godine, sa sjedištem u Španjolskom gradu Bilbau, a njene podružnice nalaze se širom SAD-a, Španjolske, Francuske, Njemačke, Japana, Nizozemske te Belgije, [38]. U njihovoj ponudi informacijskih rješenja i zaštite sigurnosti nalazi se Panda računalni program namijenjen zaštiti od sigurnosnih prijetnji.

Sučelje besplatne verzije softvera za zaštitu od zlonamjernih prijetnji Panda prikazano je na slici 6. Osnovna mogućnost koju besplatna verzija programa Panda nudi jest skeniranje sustava koje je moguće provesti na tri načina:

- skeniranjem kritičnih zona, čime se vrši pregled programa koji se trenutno koriste u svrhu otkrivanja potencijalnih opasnosti, zatim
- skeniranje cjelokupnog sustava, čime se vrši pregled cjelokupnog računala, što može potrajati i do nekoliko sati, te naposljetku
- birani pregled, pri čemu krajnji korisnik sam određuje koja će mjesta i datoteke program pregledati.




**Slika 6.** Sučelje softvera za zaštitu od zlonamjernih prijetnji Panda

Računalni softver za zaštitu informacijske sigurnosti, Panda, u svojoj besplatnoj verziji nudi mogućnost otkrivanja zlonamjernih prijetnji poput virusa, špijunskih softvera i sličnih sumnjivih datoteka.

U tablici 3 prikazani su rezultati testiranja softvera Panda, provedenih od strane neovisnog instituta za informacijsku sigurnost, na OS Windows 8.0/8.1 te OS Windows 10. Prosječna ocjena, dobivena aritmetičkom sredinom vrijednosti iz tablice 3, koju je Panda računalni softver ostvario testiranjem na OS Windows 8.0/8.1, u području zaštite jest 5.7/6.0, u području performansa 3.9/6.0, dok je u području iskoristivosti ostvario prosječnu ocijenu 5.5/6.0.

U tablici 3 prikazani su također rezultati dobiveni istim testiranjem na istom programu, provedenim na OS Windows 10, u razdoblju od listopada 2015. do prosinca 2017. Prosječna ocjena, dobivena aritmetičkom sredinom vrijednosti iz tablice 3, koju je softver ostvario u području zaštite jest 6.0/6.0, u području performansi 3.6/6.0 te u području iskoristivosti 5.6/6.0. Uspoređujući rezultate koje je softver ostvario testiranjem provedenim na OS Windows 8.0/8.1 te na OS Windows 10, može se zaključiti kako isti softver pruža veću razinu zaštite na OS Windows 10 u odnosu na OS Windows 8.0/8.1.

**Tablica 3**. Rezultati testiranja softvera Panda

| **OS Windows 8.0/8.1** | | | |
|---|---|---|---|
| | **Zaštita** | **Performanse** | **Iskoristivost** |
| **Prosinac 2016.** | 5,5/6,0 | 2,5/6,0 | 5,5/6,0 |
| **Lipanj 2016.** | 5,5/6,0 | 4,5/6,0 | 6,0/6,0 |
| **Prosinac 2015.** | 6,0/6,0 | 3,5/6,0 | 5,0/6,0 |
| **Lipanj 2015.** | 6,0/6,0 | 5,0/6,0 | 6,0/6,0 |
| **Veljača 2015.** | 5,5/6,0 | 4,0/6,0 | 5,0/6,0 |
| **Listopad 2014.** | 6,0/6,0 | 4,5/6,0 | 5,0/6,0 |
| **Travanj 2014.** | 5,5,/6,0 | 3,0/6,0 | 6,0/6,0 |
| **OS Windows 10** | | | |
| | **Zaštita** | **Performanse** | **Iskoristivost** |
| **Prosinac 2017.** | 6,0/6,0 | 3,5/6,0 | 6,0/6,0 |
| **Listopad 2016.** | 6,0/6,0 | 3,5/6,0 | 5,0/6,0 |
| **Travanj 2016.** | 6,0/6,0 | 4,0/6,0 | 5,5/6,0 |
| **Listopad 2015.** | 6,0/6,0 | 3,5/6,0 | 6,0/6,0 |

Izvor: *[36]*

Također uz besplatnu inačicu, ovaj program za zaštitu od zlonamjernih prijetnji moguće je nabaviti u još četiri verzije, [39]: Panda *Essential*, Panda *Advanced*, Panda *Complete* i Panda *Premium*. Pandu *Essential* pruža učinkovitu zaštitu od zlonamjernih prijetnji, uključujući korištenje funkcija vatrozida, također omogućuje zaštitu Mac i Android uređaja u realnom vremenu, skeniranje USB kablova i prevenciju od prenošenja nekog oblika zlonamjernog softvera tim putem.

Dodatne mogućnosti koje nudi Panda *Advanced,* u odnosu na Pandu *Essential* uključuju roditeljsku zaštitu, zatim zaštitu identiteta prilikom elektroničkog poslovanja i sličnih akcija te zaštitu od *ransomware*-a.

Kod verzije Panda *Complete,* dodatne mogućnosti u odnosu na prethodne verzije uključuju zaštitu lozinki te alat za čišćenje sustava, čime je moguće povećati performanse i ubrzati samo računalo.

Posljednja verzija, Panda *Premium*, u odnosu na ostale verzije pruža dodatne mogućnosti u vidu 20GB prostora na računalnom oblaku (*cloud*), čime dolazi do štednje memorije računala, a također uključuje tehničku podršku 24/7.

## 4.4 Avast računalni softver

Avast program za zaštitu od zlonamjernih prijetnji razvijen je od strane tvrtke Avast *Software* a.s. sa sjedištem u Pragu. Softver Avast prema istraživanjima 2017. godine proglašen je najboljim sigurnosnim softverom, a na Internetu ga se može preuzeti u besplatnoj verziji. Softver dolazi s konzolom koja pruža potpunu zaštitu nad ciljanim računalom, [40].

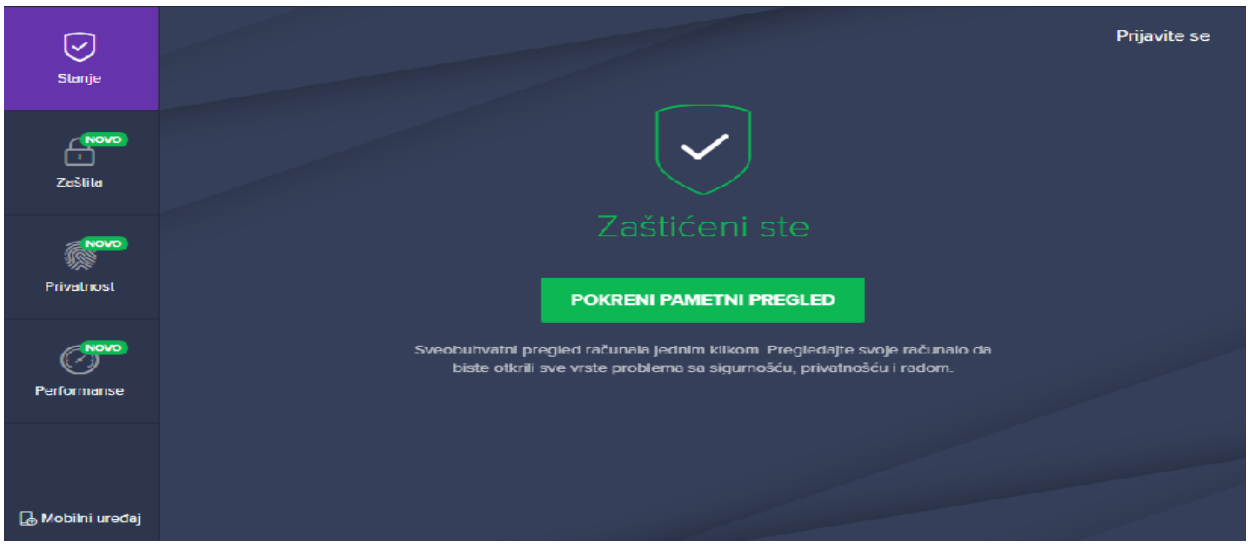
Softver obuhvaća 4 osnovne mogućnosti: rubriku stanje, zaštita, privatnost te performanse. Odabirom opcije „Stanje“, sigurnosni softver omogućuje sveobuhvatan pregled računala, čime je moguće otkriti sve potencijalne opasnosti vezane uz sigurnosti i privatnost. Aktivacijom „pametnog pregleda“ ovaj sigurnosni softver vrši pretraživanje cjelokupnog računala, kako bi se otkrili i otklonili sve eventualne zlonamjerne prijetnje koji se nalaze na njemu. To može potrajati nekoliko minuta, no pregled se u svakom trenutku može prekinuti, iz bilo kojeg razloga.

Odabirom druge po redu rubrike, odnosno opcije „Zaštita“, Avast sigurnosni softver pruža više različitih mogućnosti, od kojih su neke iskoristive korištenjem besplatnog softvera, dok je za neke opcije potrebna nadogradnja. Sama nadogradnja nije besplatna, te prema tome te mogućnosti nije moguće koristiti na besplatnoj inačici sigurnosnog softvera. Bez obzira na to, opcijom „Zaštita“ moguće je aktivirati više korisnih funkcija, kao što je odabir vrste pregleda, čime program nudi 4 kategorije pregleda: potpuni pregled radi zlonamjernih prijetnji, čime se vrši pretraživanje cijelog sustava računala, radi otkrivanja potencijalnih zlonamjernih prijetnji, zatim ciljni pregled, kojim omogućuje pregledavanje ciljane datoteke ili programa, pregled prilikom pokretanja, koji se vrši prilikom pokretanja samog operativnog sustava, te naposljetku prilagođeni pregled, čime je moguće stvoriti vlastiti način pregleda računala, na kojeg može utjecati sam krajnji korisnik.

Odabirom rubrike „Privatnost“, softver nudi mogućnost automatskog pohranjivanja lozinki, međutim da bi ta opcija funkcionirala, potrebno ju je najprije preuzeti i instalirati na računalo. Također, odabirom ove rubrike nudi se mogućnost zaštite povjerljivih podataka, no ta opcija također nije besplatna već ju je moguće preuzeti nadogradnjom.

Rubrika „Performanse“ služi radi poboljšanja performansi sustava, te se aktivacijom te opcije pokreće također jedan oblik skeniranja računala, kako bi se otkrile slabosti samoga sustava te kako bi softver mogao preventivno djelovati na njih.

Sve opisane mogućnosti softvera Avast prikazane su na slici 7.




**Slika 7.** Sučelje sigurnosnog softvera Avast

Na kraju „pametnog pregleda“ i samog otklanjanja pronađenih poteškoća, Avast će ponuditi nadogradnju koja omogućava još bolju zaštitu sustava, međutim kao što je ranije navedeno, nadogradnja nije besplatna, te se ovom verzijom softvera mogu koristiti samo opcije koje su ponuđene na korištenje kao besplatne.

U tablici 4 prikazani su rezultati testiranja računalnog softvera Avast, od strane neovisnog instituta za računalnu sigurnost, provedenog na OS Windows 8.01/8.1 te OS Windows 10. Prosječna ocjena koju je ovaj softver ostvario testiranjem na OS Windows 8.0/8.1 u vidu zaštite sustava jest 5.4/6.0, na području performansi 4.3/6.0 te je u vidu iskoristivosti ostvario prosječnu ocjenu od 5.9/6.0. Prosječna ocjena dobivena je aritmetičkom sredinom vrijednosti navedenih u tablici 4.

Istim testiranjem, provedenim u razdoblju od listopada 2015. do prosinca 2017., na OS Windows 10, Avast je ostvario rezultate prikazane u tablici 4. Prosječna ocjena ovog softvera u vidu zaštite jest 5.8/6.0, na području performansi 4.5/6.0, dok je prosječna ocjena u vidu iskoristivosti 5.8/6.0. Prosječne vrijednosti dobivene su aritmetičkom sredinom vrijednosti navedenih u tablici 8. Uspoređujući rezultate dobivene testiranjem softvera na OS Windows 8.0/8.1 te na OS Windows 10 moguće je zaključiti kako Avast računalni softver pruža veću razinu zaštite na OS Windows 10 u odnosu na OS Windows 8.

**Tablica 4**. Rezultati testiranja softvera Avast

| **OS Windows 8.0/8.01** | | | |
|---|---|---|---|
| | **Zaštita** | **Performanse** | **Iskoristivost** |
| **Prosinac 2016.** | 6,0/6,0 | 3,5/6,0 | 6,0/6,0 |
| **Lipanj 2016.** | 5,5/6,0 | 4,5/6,0 | 6,0/6,0 |
| **Prosinac 2015.** | 6,0/6,0 | 5,0/6,0 | 6,0/6,0 |
| **Lipanj 2015.** | 5,5/6,0 | 4,0/6,0 | 6,0/6,0 |
| **Veljača 2015.** | 6,0/6,0 | 4,0/6,0 | 5,5/6,0 |
| **Listopad 2014.** | 5,0/6,0 | 4,0/6,0 | 5,5/6,0 |
| **Travanj 2014.** | 3,5,/6,0 | 5,0/6,0 | 6,0/6,0 |
| **OS Windows 10** | | | |
| | **Zaštita** | **Performanse** | **Iskoristivost** |
| **Prosinac 2017.** | 6,0/6,0 | 5,5/6,0 | 5,5/6,0 |
| **Lipanj 2017.** | 6,0/6,0 | 5,0/6,0 | 6,0/6,0 |
| **Travanj 2017.** | 6,0/6,0 | 4,5/6,0 | 5,5/6,0 |
| **Listopad 2016.** | 6,0/6,0 | 3,5/6,0 | 6,0/6,0 |
| **Travanj 2016.** | 6,0/6,0 | 4,5/6,0 | 6,0/6,0 |
| **Listopad 2015.** | 5,0/6,0 | 5,0/6,0 | 6,0/6,0 |

Izvor: *[36]*

Osim besplatne inačice, Avast softver za zaštitu od zlonamjernih prijetnji trenutno se na tržištu nudi u tri različite verzije: Avast *Internet Security*, Avast *Premier* te Avast *Ultimate*¸ koje je moguće nabaviti po određenim cijenama za određeni period korištenja

### 4.4.1 Avast *Internet Security*

Avast *Internet Security*, inačica je računalnog softvera Avast, a mogućnosti koje ova verzija softvera pruža, prema [41], su sljedeće:

- Zaštita od *hakera*, štiteći pri tome privatne datoteke te fotografije kako ih ne bi bilo moguće šifrirati,
- Izbjegavanje lažnih internetskih stranica, šifrirajući privatne podatke kako bi sve povjerljive informacije ostale zaštićene,
- Zaštita od phishing napada,
- Vatrozid,
- Zaštita od *spam*-a,
- Zaštita Wi-Fi mreže,
- Detekcija bilo kojeg oblika zlonamjernog softvera,
- Kiber (*cyber*) zaštita, što omogućava automatsko slanje sumnjivih datoteka na pregled,
- Prepoznavanje i blokiranje uzoraka sumnjivog ponašanja, za zaštitu od nepoznatih prijetnji i otkupnine,
- Pametno pretraživanje,
- Zaštita od *ransomware*-a, te
- Zaštita lozinki.

Prema statistici Avast *Internet Security* program štiti računalo od 2 bilijuna vrsta zlonamjernih napada mjesečno, skenirajući 200 bilijuna usklađenih lokatora sadržaja (*Uniform Resource* Locator – URL) svaki mjesec te 300 milijuna ovih datoteka svaki novi mjesec, [41].

### 4.4.2 Avast *Premier*

Druga verzija Avast softvera za zaštitu, Avast *Premier*, štiti računalo, kućnu mrežu te lozinke od svih oblika zlonamjernih prijetnji uz pomoć pametne detekcije temeljene na računalnom oblaku.

Novost u odnosu na Avast *Internet Security* jest u vidu učinkovite zaštite web kamere, tražeći dopuštenje krajnjeg korisnika prije svakog korištenja kamera, [42]. Moguće je također onemogućiti korištenje kamere te je naknadno ponovno omogućiti. Također, još jedna dodatna opcija jest trajno uklanjanje osjetljivih datoteka, čime je moguće na siguran način izbrisati datoteke iz sustava s garancijom da neće moći biti oporavljane od treće strane. Avast *Premier* također omogućuje automatsko ažuriranje aplikacija, čime se postiže smanjenje sigurnosnih rizika.

### 4.4.3 Avast *Ultimate*

Uključujući usluge Avast *Premier*-a, dodatne usluge koje Avast *Ultimate* pruža su uklanjanje sakrivenog smeća, čime se oslobađa prostor na disku te ubrzava samo računalo, zatim zaštita virtualne privatne mreže (*Virtual Private Network* – VPN), odnosno šifriranje internetske veze radi sigurnijeg te anonimnog pregledavanja te zaštita lozinki upozorenjem na propuštene lozinke te prijavom na poznate web stranice sa samo jednim klikom, [43].

## 4.5 Kaspersky

Kaspersky softver za zaštitu od zlonamjernih prijetnji razvijen je od strane tvrtke Kaspersky Lab, koja je osnovana 1997. godine u Moskvi s regionalnim uredima širom svijeta, [44]. Softver Kaspersky odlikuje velika brzina rada, pouzdanost te fleksibilnost, a u usporednim analizama s drugim sličnim programima, Kaspersky redovito zauzima prvo mjesto na ljestvici.

U tablici 5 prikazani su rezultati testiranja softvera Kaspersky na OS Windows 8.0/8.1. te na OS Windows 10, provedenog od strane neovisnog instituta za računalnu sigurnost. Iz tablice 5 može se zaključiti kako je softver testiran na OS Windows 8.0/8.1 ostvario odlične rezultate u sva tri polja na kojima je provedeno testiranje, ostvarivši prosječnu ocjenu 6.0/6.0 na sva tri polja. Kaspersky softver vrši zaštitu računala bez da usporava sustav računala na kojem radi te točno razlikuje sigurnosne i zlonamjerne datoteke.

Istim testiranjem, provedenim u razdoblju od listopada 2015. do prosinca 2017. godine, na OS Windows 10, Kaspersky softver za zaštitu od zlonamjernih prijetnji ostvario je sljedeće prosječne rezultate: 6.0/6.0 za zaštitu, 6.0/6.0 za performanse te 5,9/6.0 za iskoristivost, što je također prikazano u tablici 5.

**Tablica 5.** Rezultati testiranja softvera Kaspersky

| **OS Windows 8.0/8.1** | | | |
|---|---|---|---|
| | **Zaštita** | **Performanse** | **Iskoristivost** |
| **Prosinac 2016.** | 6,0/6,0 | 6,0/6,0 | 6,0/6,0 |
| **Lipanj 2016.** | 6,0/6,0 | 6,0/6,0 | 6,0/6,0 |
| **Prosinac 2015.** | 6,0/6,0 | 6,0/6,0 | 6,0/6,0 |
| **Lipanj 2015.** | 6,0/6,0 | 6,0/6,0 | 6,0/6,0 |
| **Veljača 2015.** | 6,0/6,0 | 6,0/6,0 | 6,0/6,0 |
| **Listopad 2014.** | 6,0/6,0 | 6,0/6,0 | 6,0/6,0 |
| **Travanj 2014.** | 6,0,/6,0 | 6,0/6,0 | 6,0/6,0 |
| **OS Windows 10** | | | |
| | **Zaštita** | **Performanse** | **Iskoristivost** |
| **Prosinac 2017.** | 6,0/6,0 | 6,0/6,0 | 6,0/6,0 |
| **Lipanj 2017.** | 6,0/6,0 | 6,0/6,0 | 6,0/6,0 |
| **Travanj 2017.** | 6,0/6,0 | 6,0/6,0 | 6,0/6,0 |
| **Listopad 2016.** | 6,0/6,0 | 6,0/6,0 | 6,0/6,0 |
| **Travanj 2016.** | 6,0/6,0 | 5,5/6,0 | 6,0/6,0 |
| **Listopad 2015.** | 6,0/6,0 | 6,0/6,0 | 6,0/6,0 |

Izvor: *[36]*

Osim besplatne verzije ovog softvera, Kaspersky je moguće nabaviti u tri korisnički orijentirana paketa: Kaspersky *Anti-Virus*, Kaspersky *Internet Security* te Kaspersky *Total Security*. U tablici 6 prikazana je usporedba paketa programa Kaspersky prema mogućnostima koje pojedini paket nudi.

**Tablica 6.** Usporedba paketa Kaspersky prema uslugama koje omogućavaju

| Mogućnosti | Kaspersky Anti-Virus | Kaspersky Internet Security | Kaspersky Total Security |
|---|---|---|---|
| **Zaštita od zlonamjernog softvera** | DA | DA | DA |
| **Sigurnost i učinkovitost** | DA | DA | DA |
| **Jednostavnost korištenja** | DA | DA | DA |
| **Roditeljska zaštita** | NE | DA | DA |
| **Sigurnost računala** | NE | DA | DA |
| **Zaštita djece** | NE | NE | DA |
| **Sigurnost lozinki** | NE | NE | DA |
| **Enkripcija, šifriranje** | NE | NE | DA |

Izvor: *[44]*

Kaspersky *Anti-Virus*, osim osnovne zaštite od zlonamjernih programa kao što su virusi, špijunski softveri i krađa identiteta, Kaspersky *Anti-Virus* osigurava kombinaciju sigurnosti i učinkovitosti.

Drugi paket, Kaspersky *Internet Security*, nadovezujući se na Kaspersky *Anti-Virus*, omogućava i zaštitu privatnosti, dodatnu sigurnosti prilikom online bankarstva i trgovina kao i roditeljsku zaštitu.

Posljednji paket, Kaspersky *Total Security*, pruža najveću razinu zaštite, te nadovezujući na prethodnike omogućava uz osnovnu roditeljsku zaštitu također visoku razinu zaštite za djecu na internetu, zaštitu lozinki te enkripciju, odnosno šifriranje podataka.

# 5. Usporedba softvera namijenjenih zaštiti od sigurnosnih prijetnji

Računalna sigurnost predstavlja složenu disciplinu koja obuhvaća brigu o svim mogućim i potencijalnim segmentima napada na računala te ostalu informatičku imovinu, [52]. Kako bi se postigao što veći stupanj zaštite podataka, svako računalo trebalo bi ispunjavati 3 temeljna sigurnosna zahtjeva, prema [2]:

1. Povjerljivost, kojim sustav treba osigurati da poslani, odnosno primljeni podaci ne budu čitljivi trećoj strani,
2. Integritet, koji predstavlja mogućnost otkrivanja bilo kakve namjerne ili nenamjerne izmijene poslanih, odnosno primljenih podataka, te
3. Raspoloživost, što predstavlja sposobnost sustava biti dostupan u trenutku kada je to potrebno.

Utjecaj prijetnje na sustav može se utvrditi prema vrijednosti imovine pogođene prijetnjom, pri čemu prijetnja može djelovati izravno na osobne podatke te povjerljive informacije krajnjeg korisnika, intelektualno vlasništvo tvrtke ili pojedinca, financijsku imovinu kao i na osobni te politički ugled pojedinca, [2]. Zaštita od sigurnosnih prijetnji može biti provedena na razne načine, od kojih je najučinkovitiji način zaštite korištenje računalnih softvera namijenjenih zaštiti od sigurnosnih prijetnji.

U radu je promatrano djelovanje te su proučavane mogućnosti 5 različitih računalnih softvera namijenjenih zaštiti od zlonamjernih prijetnji: Windows Defender, McAfee, Avast, Panda Dome te Kaspersky.

U tablici 7 prikazana je usporedba računalnih softvera namijenjenih zaštiti od zlonamjernih prijetnji prema mogućnostima. Iz tablice je moguće zaključiti kako je od besplatnih softvera , uspoređujući 5 navedenih, najbolji Avast, koji u svojoj besplatnoj inačici sadrži vatrozid, mogućnost zaštite e-maila te web zaštitu, što ostali besplatni softveri navedeni u tablici 2 većinom ne sadržavaju. Windows Defender, kao što je i ranije navedeno, pruža samo osnovne mogućnosti zaštite od zlonamjernih prijetnji. Budući da je ovaj softver instaliran samom instalacijom novijih OS, moguće je zaključiti kako on sam po sebi ne pruža dovoljnu razinu zaštite te kako bi krajnji korisnik bio u potpunosti siguran i zaštićen od bilo kojeg oblika zlonamjernih prijetnji, trebao bi na svom računalu posjedovati i neki drugi računalni softver, koji nudi veću razinu zaštite u odnosu na Windows Defender. Panda softver za zaštitu od zlonamjernih prijetnji u svojoj besplatnoj izvedbi nudi nešto više mogućnosti od samog pametnog pregleda, uključujući web zaštitu.

**Tablica 7.** Usporedba softvera za zaštitu od zlonamjernih prijetnji

| **Računalni softver** | **Mogućnosti** | | | | |
|---|---|---|---|---|---|
| | **Pretraga na zahtjev** | **Vatrozid** | **Anti-Spam** | **Zaštita e-maila** | **Web zaštita** |
| **Avast Free Antivirus** | DA | DA | NE | DA | DA |
| **Avast Internet Security** | DA | DA | DA | DA | DA |
| **Avast Premier** | DA | DA | DA | DA | DA |
| **Kaspersky Antivirus** | DA | NE | NE | DA | DA |
| **Kaspersky Total Security** | DA | DA | DA | DA | DA |
| **Kaspersky Internet Security** | DA | DA | DA | DA | DA |
| **Windows Defender** | DA | NE | NE | NE | NE |
| **McAfee Antivirus** | DA | NE | NE | DA | NE |
| **McAfee Internet Security** | DA | DA | DA | DA | DA |
| **Panda Antivirus** | DA | NE | NE | NE | DA |

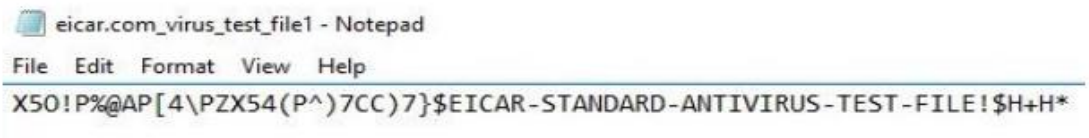
Izvor: *[53]*

## 5.1 Testiranje računalnih softvera namijenjenih zaštiti od zlonamjernih prijetnji

U svrhu rada provedeno je testiranje odziva pojedinog računalnog softvera. Testiranje odziva provedeno je korištenjem *Eicar* (*European Institute for Computer Antivirus Research* - EICAR) testne datoteke. Testiranje je izvršeno tako da je prvotno instaliran jedan od softvera za zaštitu od zlonamjernih prijetnji, a nakon testiranja, taj je program uklonjen kako ne bi ometao rad drugog računalnog softvera.

*Eicar* testna datoteka, [46], jest datoteka razvijena od strane Europskog instituta za računalna antivirusna istraživanja s ciljem testiranja programa namijenjenih zaštiti od sigurnosnih prijetnji. Eicar institut za računalna antivirusna istraživanja osnovan je 1991. godine te predstavlja nezavisnu platformu za informacijske sigurnosne stručnjake na područjima znanosti, istraživanja, razvoja, implementacije i upravljanja.

Na slici 8 prikazan je 68 *byte*-ni kod koji predstavlja *Eicar* testnu datoteku.




**Slika 8.** Eicar testna datoteka

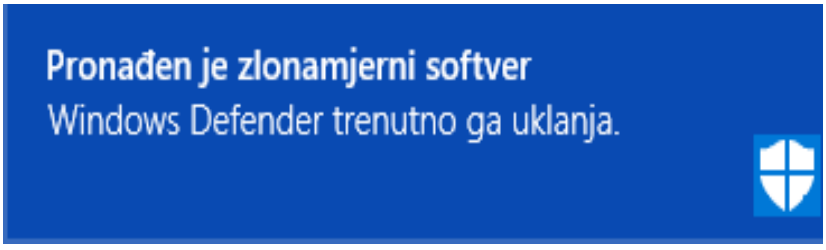
Izvor: [46]

Svrha korištenja *Eicar* testne datoteke jest utvrđivanje ispravnosti instaliranog zaštitnog programa te provjera unutarnjih postupaka zaštitnog programa kada se pronađe potencijalna zlonamjerna prijetnja. Eicar testna datoteka ponaša se kao prava zlonamjerna prijetnja, te omogućava krajnjim korisnicima testiranje sigurnosnih softvera na siguran način, bez uporabe pravih zlonamjernih prijetnji. Ispravan program za zaštitu trebao bi detektirati Eicar datoteku kao pravu zlonamjernu prijetnju. *Eicar* datoteka legitimni je program sastavljen isključivo od ASCII znakova tako da ju je lako moguće stvoriti korištenjem nekog od alata za uređivanje teksta.

### 5.1.1 Testiranje Windows Defender računalnog softvera

*Eicar* testna datoteka dolazi u 4 inačice: prva inačica eicar.com sadrži ASCII osmobitni niz, druga inačica eicar.com.txt zapravo predstavlja kopiju prve inačice s drugim nazivom stvorena iz razloga što su neki korisnici imali problema s preuzimanjem eicar.com verzije, zatim treća verzija sadrži testnu datoteku unutar zip arhive te je zadnja verzija zip arhiva koja unutar sebe sadrži treću datoteku.

Prilikom preuzimanja eicar.com datoteke, Windows Defender automatski ga prepoznaje kao prijetnju te izbacuje obavijest prikazanu na slici 9. Windows Defender datoteku je detektirao kao zlonamjerni softver te ju je automatski uklonio iz sustava.

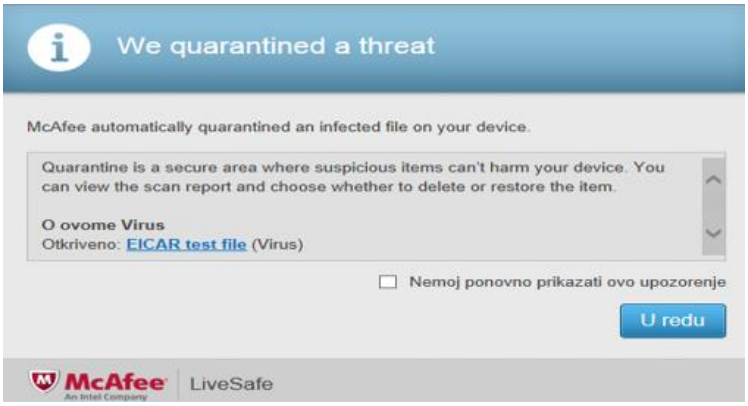



**Slika 9.** Detekcija Eicar.com datoteke

Prilikom preuzimanja ostalih triju verzija, Windows Defender računalni softver namijenjen zaštiti od zlonamjernih prijetnji prikazuje istu obavijest koja je prikazana na slici 19, prilikom čega se može zaključiti kako je Windows Defender ispravno instaliran te prepoznaje sve moguće vrste prijetnji, uključujući i prijetnje unutar zip datoteka.

### 5.1.2 Testiranje McAfee računalnog softvera

Preuzimanjem prve datoteke eicar.com, McAfee sigurnosni softver nakon vrlo kratkog vremena od preuzimanja detektirao je sumnjivu datoteku i prepoznao ju kao zlonamjernu prijetnju, što je prikazano na slici 10. McAfee detektirao je eicar.com datoteku kao potencijalu prijetnju.

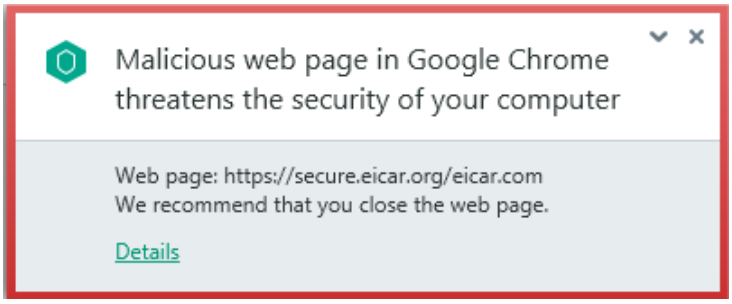



**Slika 10.** Detekcija Eicar testne datoteke korištenjem McAfee računalnog softvera

Preuzimanjem ostalih triju verzija Eicar testne datoteke, McAfee također reagira isto kao i na prvotnu eicar.com datoteku, detektirajući datoteku kao zlonamjernu prijetnju te izbacujući istu obavijest prikazanu na slici 20.

### 5.1.3 Testiranje Kaspersky računalnog softvera

Kaspersky softver namijenjen zaštiti od zlonamjernih prijetnji blokirao je sam pokušaj preuzimanja eicar.com testne datoteke, što je prikazano na slici 11. Kaspersky testnu datoteku automatski prepoznaje kao prijetnju, ne dozvoljavajući instalaciju u sustav.




**Slika 11.** Detekcija Eicar.com testne datoteke korištenjem Kaspersky računalnog softvera

Kaspersky softver također je blokirao pokušaj preuzimanja ostalih inačica Eicar testne datoteke, prikazujući istu obavijest koja je prikazana na slici 21. Shodno tome, dokazano je kako je softver ispravno konfiguriran te da ispravno obavlja funkciju za koju je namijenjen.

### 5.1.4 Testiranje Panda programa za računalnu sigurnost

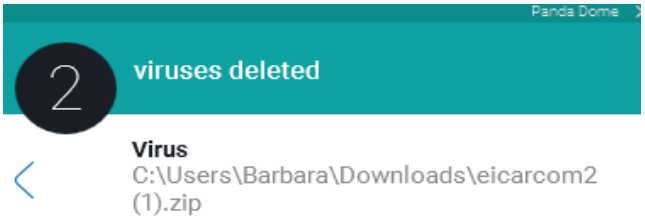
Preuzimanjem eicar.com testne datoteke, namijenjene testiranju odziva pojedinog softvera za zaštitu, Panda softver automatski prepoznaje datoteku kao potencijalnu opasnost, odnosno potencijalni virus, te izbacuje obavijest prikazanu na slici 12.




**Slika 12.** Detekcija Eicar.com testne datoteke korištenjem Panda softvera za računalnu sigurnost

Prilikom preuzimanja arhivirane eicar.zip datoteke, Panda blokira njeno preuzimanje, te prepoznaje datoteku kao zlonamjernu prijetnju te izbacuje istu obavijest koja je prikazana na slici 12.

Prilikom preuzimanja sva 4 oblika Eicar testne datoteke, Panda softver za zaštitu od zlonamjernih prijetnji prepoznaje sumnjivu datoteku, blokira njeno preuzimanje, tretirajući datoteku kao zlonamjernu prijetnju, te je automatski uklanjajući iz sustava, što je prikazano na slici 13.

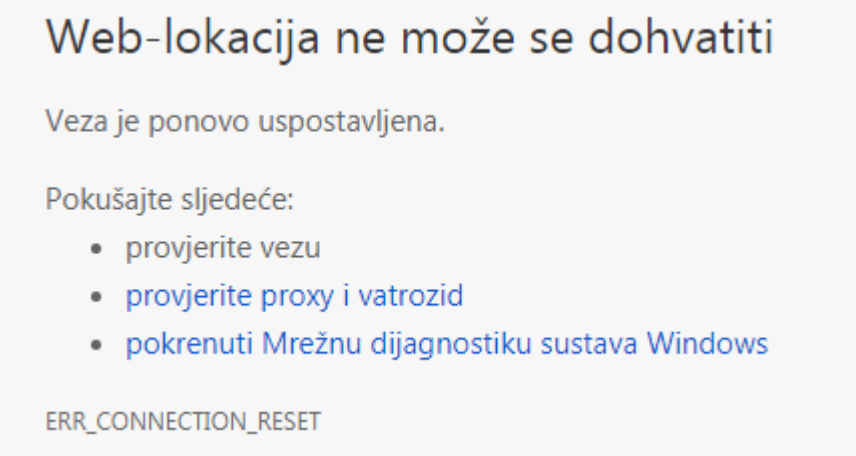



**Slika 13.** Uklanjanje Eicar.zip datoteke

Panda program tako postupa sa svakom od skinutih inačica, pri čemu se može zaključiti kako je ovaj program namijenjen zaštiti od zlonamjernih prijetnji ispravno konfiguriran te ispravno detektira sve tipove zlonamjernih prijetnji.

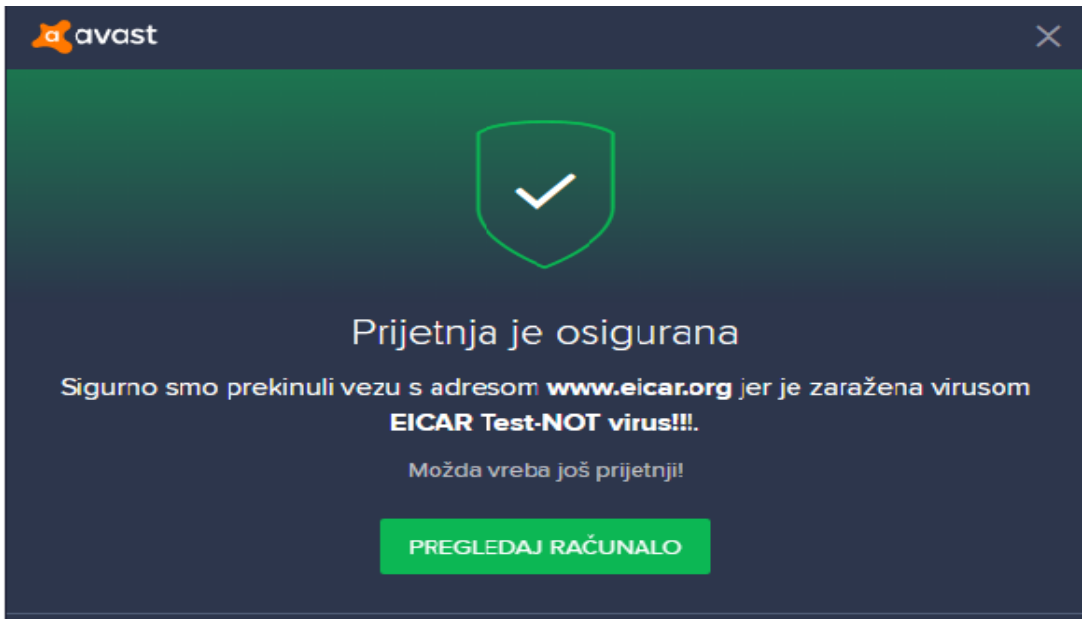
### 5.1.5 Testiranje Avast računalnog softvera

Avast računalni softver namijenjen zaštiti od zlonamjernih prijetnji također je testiran korištenjem Eicar testne datoteke. Pokušajem preuzimanja prve inačice datoteke eicar.com, Avast računalni softver blokira sam pokušaj, preusmjeravajući web stranicu na stranicu prikazanu slikom 14.




**Slika 14**. Preusmjeravanje web stranice prilikom preuzimanja Eicar.com testne datoteke

Avast program za računalnu sigurnost odbio je sam pokušaj preuzimanja Eicar testne datoteke, detektirajući datoteku kao potencijalnu prijetnju, što je prikazano na slici 15.




**Slika 15.** Detekcija Eicar.com datoteke korištenjem računalnog softvera Avast

Avast računalni softver tako postupa sa svakom od sljedećih verzija Eicar testne datoteke, detektirajući je kao zlonamjernu prijetnju te ne dozvoljavajući instaliranje datoteke u sustav.

## 5.2 Usporedba softvera temeljem dobivenih rezultata

Računalni softveri namijenjeni zaštiti od sigurnosnih prijetnji korišteni u ovome radu testirani su uz pomoć Eicar testne datoteke. Svaki od računalnih softvera detektirao je sve inačice Eicar datoteke kao pravu zlonamjernu prijetnju.

Razlika u testiranim softverima prikazana je u tablici 8. Iz tablice 8 vidljivo je kako Panda, McAfee te Windows Defender računalni softver dozvoljavaju preuzimanje testne datoteke u sustav računala, detektiraju je kao zlonamjernu prijetnju te je potom uklanjaju iz sustava, dok s druge strane, Kaspersky te Avast računalni softveri ne dozvoljavaju instaliranje Eicar datoteke u sustav računala. Kaspersky računalni softver blokirao je svaki pokušaj preuzimanja Eicar datoteke, detektirajući je kao potencijalnu zlonamjernu prijetnju. Avast računalni softver ne dozvoljava pristup stranici namijenjenoj preuzimanju Eicar testne datoteke, preusmjerava preglednik na drugu web stranicu te javlja obavijest o potencijalnoj opasnosti.

**Tablica 8.** Usporedba softvera temeljem rezultata dobivenih testiranjem uz pomoć Eicar testne datoteke

| | Detekcija potencijalne prijetnje | Preuzimanje datoteke u sustav | Postupak s preuzetom datotekom |
|---|---|---|---|
| **Windows Defender** | DA | DA | nakon preuzimanja datoteke javlja obavijest o potencijalnoj opasnosti te uklanja datoteku iz sustava |
| **McAfee** | DA | DA | nakon preuzimanja datoteke javlja obavijest o potencijalnoj opasnosti te uklanja datoteku iz sustava |
| **Avast** | DA | NE | blokira sam pokušaj preuzimanja datoteke preusmjeravajući preglednik na drugu web stranicu |
| **Panda** | DA | DA | nakon preuzimanja datoteke javlja obavijest o potencijalnoj opasnosti te uklanja datoteku iz sustava |
| **Kaspersky** | DA | NE | blokira sam pokušaj preuzimanja datoteke |

Ovim radom dokazano je kako besplatne inačice sigurnosnih softvera osiguravaju dostatnu razinu zaštite za krajnje korisnike računala.

# 6. Zaključak

Informacijska sigurnost predstavlja vrlo bitan aspekt zaštite povjerljivih podataka krajnjih korisnika. Razvojem tehnologije te porastom korisnika terminalnih uređaja raste važnost zaštite osobnih podataka. S razvojem tehnologija dolazi do pojave različitih oblika zlonamjernih prijetnji koje predstavljaju veliku opasnost za sve korisnike terminalnih uređaja, koji najčešće korištenjem Interneta postaju izloženi raznim oblicima prijetnji. Shodno tome, vrlo je važno preventivno djelovati te se preventivno zaštititi od eventualnih napada usmjerenih računalima i krajnjim korisnicima. Jedan od najučinkovitijih oblika zaštite od zlonamjernih prijetnji jest korištenje računalnih softvera namijenjenih zaštiti od zlonamjernih prijetnji. Takve softvere vrlo je lako preuzeti u besplatnim inačicama, međutim moguće ih je nabaviti i po određenim cijenama.

Ovim radom dokazano je kako besplatne inačice sigurnosnih softvera osiguravaju dostatnu razinu zaštite za krajnje korisnike računala. Računalni softveri namijenjeni zaštiti od sigurnosnih prijetnji korišteni u ovome radu testirani su uz pomoć Eicar testne datoteke. Svaki od računalnih softvera detektirao je sve inačice Eicar datoteke kao pravu zlonamjernu prijetnju. Temeljem rezultata dobivenih testiranjem uz pomoć korištenja Eicar testne datoteke može se zaključiti kako je najbolji računalni softver Kaspersky koji ne dozvoljava preuzimanje datoteke u sustav blokirajući sam pokušaj preuzimanja datoteke.

Po ocjenama AV testa dostupnim na stranicama Neovisnog instituta za informacijsku sigurnost, prema čemu se računalni softveri testiraju prema trima kriterija: zaštita, performanse te iskoristivost, najboljim softverom se pokazao Kaspersky računalni softver. Kaspersky je na svim područjima te na oba OS na kojima je testiran, OS Windows 8.0/8.1 te OS Windows 10, ostvario najbolje prosječne ocjene. Prosječne ocijene dobivene su računanjem aritmetičke sredine ocjena dobivenih za pojedino razdoblje.

Prema svemu navedenom, moguće je zaključiti kako i besplatni softveri namijenjeni zaštiti od zlonamjernih prijetnji ispravno obavljaju svoju funkciju te štite krajnjeg korisnika od različitih oblika prijetnji. Moguće je zaključiti, prema testiranju provedenom uz pomoć Eicar testne datoteke te prema ocjenama AV testa, da je od korištenih softvera u ovome radu najbolji Kaspersky računalni softver, koji je ostvario najbolje ocijene te je blokirao bilo koji pokušaj preuzimanja Eicar testne datoteke, te tako zaštitio računalo od samog unošenja prijetnji u sustav.

# Literatura


[1] „Sigurnost osobnih računala s Windows operacijskim sustavom“, Dostupno: http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2005-07-129.pdf (Zadnje pristupano: 18.04.2018.)

[2] S. Husnjak, „Sigurnost primjene terminalnih uređaja“, Fakultet prometnih znanosti, 09.12.2013., Dostupno: http://e-student.fpz.hr/Predmeti/T/Terminalni_uredaji/Materijali/10_-_Sigurnost_primjene_terminalnih_uredjaja_-_09122013.pdf (Zadnje pristupano: 08.05.2018.)

[3] „BYOD- Korištenje privatnih uređaja u poslovne svrhe“, Dostupno: https://sysportal.carnet.hr/node/1235 (Zadnje pristupano: 11.04.2018.)

[4] „Phishing“, Dostupno: http://www.cert.hr/19795-2/phishing/ (Zadnje pristupano: 11.04.2018.)

[5] Gabey G., „Policy framework a must for Security today: IDC“, 04.10.2013., Dostupno: https://www.digitalnewsasia.com/security/policy-framework-a-must-for-security-today-idc (Zadnje pristupano: 05.04.2018.)

[6] „Što je to otimač preglednika i kako ukloniti takav program“, Dostupno: http://virusi.hr/otimac-preglednika/ (Zadnje pristupano: 11.04.2018.)

[7] „Facts and Figures on E-Waste and Recycling“, Dostupno: http://www.electronicstakeback.com/wp-content/uploads/Facts_and_Figures_on_EWaste_and_Recycling.pdf (Zadnje pristupano: 11.04.2018.)

[8] „CERT.hr: O socijalnom inženjeringu“, Dostupno: http://www.cert.hr/socijalni_inzenjering/ (Zadnje pristupano: 11.03.2018.)

[9] „STRIDE Threat Model: Example & Owerview“, Study.com, Dostupno: https://study.com/academy/lesson/stride-threat-model-example-overview.html (Zadnje pristupano 08.05.2018.)

[10] „Krađa identiteta- Što je i kako se zaštititti?“, Dostupno: http://plaviured.hr/vodici/krada-identiteta-sto-je-i-kako-se-od-nje-zastititi/ (Zadnje pristupano: 05.04.2018.)

[11] „DDoS napad“, Dostupno: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2008-09-240.pdf (Zadnje pristupano: 05.04.2018.)

[12] „Spoofing napadi“, Dostupno: http://security.foi.hr/wiki/index.php/Spoofing_napadi (Zadnje pristupano: 19.03.2018.)

[13] „Sigurnost“, Dostupno: http://www.znanje.org/knjige/computer/net/03/sigurnost.htm (Zadnje pristupano:13.04.2018.)

[14] „Hakerski napadi“, Dostupno: http://web.studenti.math.pmf.unizg.hr/~ksekuli/napadi.htm (Zadnje pristupano:13.04.2018.)

[15] „Spam“, Dostupno: https://www.cert.hr/19795-2/spam/ (Zadnje pristupano 08.05.2018.)

[16] „What is adware?“, Dostupno: https://www.kaspersky.com/resource-center/threats/adware (Zadnje pristupano:14.04.2018.)

[17] „O crimeware softveru“, Dostupno: https://www.cert.hr/crimeware/ (Zadnje pristupano: 14.04.2018.)

[18] „O scareware softveru“, Dostupno: https://www.cert.hr/scareware/ (Zadnje pristupano:14.04.2018.)

[19] „Rootkit: What is a Rootkit and How to Detect It | Veracode“, Dostupno: https://www.veracode.com/security/rootkit (Zadnje pristupano: 25.12.2017.)

[20] mr.sc. Katerina Dulčić, Pravni fakultet Sveučilišta u Rijeci, „Oblici štete od računalnih virusa i odgovornost za štetu“, Dostupno: http://hrcak.srce.hr/index.php?show=clanak&id_clanak_jezik=40013

[21] „Virusi (Računalni): E-enciklopedija“, Dostupno: https://lupiga.com/enciklopedija/virusi-racunalni (Zadnje pristupano 09.05.2018.)

[22] D. Androić, „Računalni virusi“, Prirodoslovno-matematički fakultet, Dostupno: http://www.phy.pmf.unizg.hr/~dandroic/nastava/rm/racunalni_virusi.pdf (Zadnje pristupano: 21.04.2018.)

[23] „What is macro virus?“, Dostupno: https://searchsecurity.techtarget.com/definition/macro-virus (Zadnje pristupano: 26.04.2018.)

[24] „Computet Warms Malware, What is a computer warm?“, Dostupno: https://www.veracode.com/security/computer-worm (Zadnje pristupano: 26.04.2018.)

[25] „The Real Story of Stuxnet“, Dostupno: https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet/ (Zadnje pristupano: 26.04.2018.)

[26] „Duqu- tajanstveni računalni virus kojega se ne može zaustaviti“, Dostupno: http://www.poslovni.hr/vijesti/duqu-tajanstveni-racunalni-virus-kojega-se-ne-moze-zaustaviti-188897 (Zadnje pristupno: 26.04.2018.)

[27] „What is Flame Malware“, Dostupno: https://www.kaspersky.com/flame (Zadnje pristupano: 26.04.2018.)

[28] „Trojan Horse Malware“, Dostupno: https://www.lifewire.com/whats-a-trojan-horse-virus-3972285 (Zadnje pristupano: 09.05.2018.)

[29] „Trojanski konji: E-enciklopedija“, Dostupno: https://www.lupiga.com/enciklopedija/trojanski-konji (Zadnje pristupano: 10.04.2018.)

[30] „What is RAT (remote access Trojan)“, Dostupno: https://searchsecurity.techtarget.com/definition/RAT-remote-access-Trojan (Zadnje pristupano: 14.04.2018.)

[31] „What is a keylogger trojan“, Dostupno: https://www.lifewire.com/what-is-a-keylogger-trojan-153623 (Zadnje pristupano:14.04.2018.)

[32] „O adware / spywareu | Nacionalni CERT“, Dostupno: http://www.cert.hr/malver/adware (Zadnje pristupano: 21.04.2018.)

[33] „Ransomware- CERT.hr“, Dostupno: https://www.cert.hr/19795-2/ransomware/ (Zadnje pristupano:14.04.2018.)

[34] „Antivirus (anti- virus)- zašto je nužan i koji izabrati?“, Dostupno: http://www.ide3.hr/hr/reference/novosti-blog/tehno-kutak/antivirus-(anti-virus)zasto-je-nuzan-i-koji-izabrati (Zadnje pristupano: 09.05.2018.)

[35] „Zaštita uređaja pomoću centra Windows Defender Security Center“, Dostupno: https://support.microsoft.com/hr-hr/help/4013263/windows-10-protect-my-device-with-windows-defender-antivirus (Zadnje pristupano: 04.05.2018.)

[36] „AV test, The Independent IT-Security Institute“, Dostupno: https://www.av-test.org/en/antivirus/home-windows/windows-8/december-2016/ (Zadnje pristupano: 14.04.2018.)

[37] „McAfee“, Dostupno: http://www.mcafee-store.com/mcafee/wm/lp1/index.html?curr=hr&lang=hr&gclid=Cj0KCQjwibDXBRCyARIsAFHp4fp40iAFatEhuvxBRmHnGn8TiHxpjkKCnM1VvnFIG2KRuQ4ODvVNiREaArqDEALw_wcB (Zadnje pristupano: 04.05.2018.)

[38] „Panda Security“, Dostupno: https://www.crunchbase.com/organization/panda-security#section-overview (Zadnje pristupano: 18.04.2018.)

[39] „The nex-gen antivirus program“, Dostupno: https://www.pandasecurity.com/security-promotion/?reg=HR&lang=en&track=99838&campaign=dome1802&option=mix&x-hideselection=true&gclid=Cj0KCQjwibDXBRCyARIsAFHp4frdMRNmVkXafKNeuqGsHkglGJIFy7InrKxxHw2wG53ysEA2F9kw1n0aAmDFEALw_wcB (Zadnje pristupano: 04.05.2018.)

[40] „Najbolji besplantni antivirusni programi“, Dostupno: http://www.racunalo.com/najbolji-besplatni-antivirus-programi-veljaca-2017/ (Zadnje pristupano: 22.02.2018.)

[41] „Avast Internet Security“, Dostupno: https://www.avast.com/internet-security (Zadnje pristupano: 04.05.2018.)

[42] „Avast Premier“, Dostupno: https://www.avast.com/premier (Zadnje pritupano: 04.05.2018.)

[43] „Avast Store“, Dostupno: https://www.avast.com/store#! (Zadnje pristupano: 04.05.2018.)

[44] „Kompletna paleta Kaspersky rješenja – najbolje antivirusne zaštite za kućne i poslovne korisnike“, Dostupno: http://www.getim.info/sites/getim/o-nama/mogucnosti-placanja/109-kompletna-paleta-kaspersky-rjeenja-najbolje-antivirusne-zatite-za-kune-i-poslovne-korisnike (Zadnje pristupano: 06.05.2018.)

[45] „Computer Security Products for Home Users, Kaspersky Lab“, Dostupno: https://www.kaspersky.com/home-security (Zadnje pristupano: 05.05.2018.)

[46] „European Expert Group for IT-Security“, Dostupno: http://www.eicar.org/85-0-Download.html (Zadnje pristupano:14.04.2018.)

[47] „Hoax – Cert.hr“, Dostupno: https://www.cert.hr/19795-2/hoax/ (Zadnje pristupano: 14.05.2018.)

[48] „Computer Security Threat Sources“, Dostupno: http://www.comptechdoc.org/man/Business_guide/risk-assessment/securitythreats.html (Zadnje pristupano: 15.05.2018.)

[49] „Zlonamjerni softver – CERT“, Dostupno: https://www.cert.hr/19795-2/malver/ (Zadnje pristupano 21.04.2018.)

[50] „Fizička zaštita informacijskih sustava“, Dostupno: https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-06-304.pdf (Zadnje pristupano 14.05.2018.)

[51] „Savjeti kako se zaštititi od zlonamjernog softvera“, Dostupno: https://www.pmf.unizg.hr/_download/repository/kakosezatitiodzlonamjernogsoftvera.pdf (Zadnje pristupano: 03.06.2018.)

[52] „Doctor Web: statement on Virus Bulletin comparative reviews“, Dostupno: https://news.drweb.com/show/?i=83&c=5&p=5&lng=en (Zadnje pristupano: 18.06.2018.)

# Popis slika

**Slika 1.** Udio spam poruka ..... 8
**Slika 2.** Prikaz načina rada parazitskih virusa ..... 11
**Slika 3.** Način rada virusa pratioca ..... 12
**Slika 4.** Način rada link virusa ..... 13
**Slika 5.** Sučelje Windows Defender računalnog softvera ..... 17
**Slika 6.** Sučelje softvera za zaštitu od zlonamjernih prijetnji Panda ..... 21
**Slika 7.** Sučelje sigurnosnog softvera Avast ..... 24
**Slika 8.** Eicar testna datoteka ..... 31
**Slika 9.** Detekcija Eicar.com datoteke ..... 31
**Slika 10.** Detekcija Eicar testne datoteke korištenjem McAfee računalnog softvera ..... 32
**Slika 11.** Detekcija Eicar.com testne datoteke korištenjem Kaspersky računalnog softvera ..... 32
**Slika 12.** Detekcija Eicar.com testne datoteke korištenjem Panda softvera za računalnu sigurnost ..... 33
**Slika 13.** Uklanjanje Eicar.zip datoteke ..... 33
**Slika 14**. Preusmjeravanje web stranice prilikom preuzimanja Eicar.com testne datoteke ..... 34
**Slika 15.** Detekcija Eicar.com datoteke korištenjem računalnog softvera Avast ..... 34

# Popis grafikona

**Grafikon 1.** Postotak reciklaže elektroničkog otpada u razdoblju 2000.-2012. godine ..... 4
**Grafikon 2.** Udio pojedine vrste prijetnji na sustav ..... 9

# Popis tablica

**Tablica 1.** Rezultati testiranja Windows Defender-a ..... 18
**Tablica 2.** Rezultati testiranja McAfee softvera za zaštitu od prijetnji ..... 19
**Tablica 3**. Rezultati testiranja softvera Panda ..... 22
**Tablica 4**. Rezultati testiranja softvera Avast ..... 25
**Tablica 5.** Rezultati testiranja softvera Kaspersky ..... 27
**Tablica 6.** Usporedba paketa Kaspersky prema uslugama koje omogućavaju ..... 28
**Tablica 7.** Usporedba softvera za zaštitu od zlonamjernih prijetnji ..... 30
**Tablica 8.** Usporedba softvera temeljem rezultata dobivenih testiranjem uz pomoć Eicar testne datoteke ..... 35