Centar Informacijske Sigurnosti

Online antivirusi

prosinac 2011.

CIS-DOC-2011-12-035

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

Prava korištenja

Sadržaj

1. Uvod

Antivirus ili antivirusni program koristi se za spriječavanje, prepoznavanje i uklanjanje zlonamjernih programa (eng. *malware*) kao što su računalni virusi (eng. *computer viruses*), računalni crvi (eng. *computer worm*), trojanski konji (eng. *trojan horses*), špijunski programi (eng. *spyware*) ili oglašivački programi (eng. *adware*).

Iako su antivirusni sustavi jako koristan alati za zaštitu računala, ponekad mogu imati i neke negativne posljedice. Antivirus može umanjiti performanse računala. Također, većina neiskusnih korisnika ne razumije zahtjeve, upite i odluke koje antivirus donosi, što može dovesti do proboja sigurnosti ako korisnik prihvati lošu odluku ili izabere krivu mogućnost za rješenje problema.

Uz sve to, valja napomenuti da antivirusni program uobičajeno radi na razini jezgre operacijskog sustava, što je jako osjetljivo i važno područje računala. Zahvaljujući tom položaju, antivirusni sustavi imaju pristup povjerljivim i zaštićenim podacima koji kontroliraju rad cijelog sustava. Samo jedna kriva odluka antivirusa dovodi u pitanje sigurnost podataka pohranjenih na računalu ili sam rad operacijskog sustava.

No, s druge strane, u današnje vrijeme, kada je Internet postao sastavni dio života većine ljudi, opasnost od zaraze računala zlonamjernim programima postala je veća nego ikad. Cijelo vrijeme dok je korisnik online, njegovo računalo je ranjivo i izloženo napadima raznih pažljivo zamaskiranih virusa, trojanaca i ostalih zlonamjenih programa koji se nalaze na brojnim Internet stranicama. Zbog zaštite korisnika od takvih prijetnji, uz tradicionalni desktop antivirus, nastaje i online antivirus. Prednosti takvog antivirusnog programa leže u činjenici da oni štite ne samo Internet stranice, već se mogu koristiti i za dodatnu zaštitu uz desktop antivirus. Slika 1. prikazuje popularne *online* antivirusne programe.

Usprkos brojnim prednostima ovakvog oblika zaštite, postoji još veliki broj korisnika koji nisu upoznati s njim, pa je cilj ovog dokumenta približiti i upoznati korisnike s pojmom *online* antivirusa.

U poglavlju 2 ukratko je opisana povijest razvoja računalnih virusa i antivirusnih sustavaNavedena je podijela zloćudnih programa, metode zaštite računala od njih te su opisani načini prepoznavanja zloćudnih programa.U poglavlju 3 opisan je način rada *online* antivirusa. Također je dan i pregled najpoznatijih proizvođača online antivirusa te su navedene prednosti i mane *online* antivirusnih sustava u odnosu na standardne antiviruse.

Slika 1. Popularni online antivirusni programi
Izvor: Google

2. Računalni virusi i antivirusni programi

2.1. Povijest razvoja virusa i antivirusa

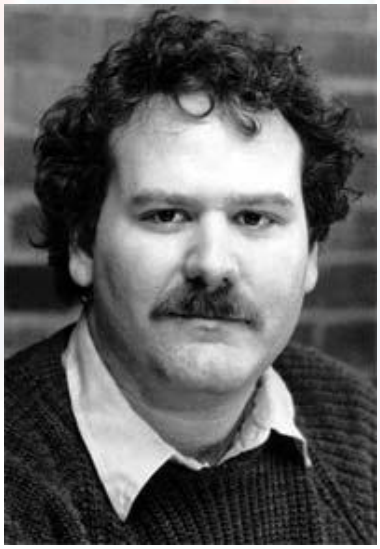
2.1.1. Pojava virusa i antivirusnih programa

Povijest programiranja virusa počinje 80-tih godina prošlog stoljeća. Većina računalnih virusa napisanih u razdoblju od 1980. godine do 1986. godine bila je usmjerena na samoreprodukciju i nije nanosila neku ozbiljnu štetu računalima. S vremenom se sve veći broj programera upoznao s programiranjem virusa. Tako nastaju virusi čiji cilj više nije samoreprodukcija, nego upravljanje i uništavanje podataka na zaraženom računalu.

S pojavom računalnih virusa javlja se i potreba za razvojem alata koji bi štitili računala od virusa - antivirusima. Nije poznato tko je napravio prvi antivirusni program, ali se smatra da su se pojavili početkom 1980.-tih godina. Prvo zabilježeno ukljanjenje računalnog virusa izveo je Bernd Fix[1] 1987. godine. Iste godine nastala su i dva antivirusna rješenja za platformu Atari ST[2] - G Data[3] i UVK 2000[4].

Od značajnijih osoba u ranim godinama razvoja antivirusnih programa valja istaknuti Freda Cohena (Slika 2.). On je izdao jedan od prvih akademskih članaka o računalnim virusima 1984. godine, a 1988. godine počeo je razvijati strategije kojima se koriste antivirusi za otkrivanje računalnih virusa. Njegove strategije koriste se i danas, ali u poboljšanom obliku.

U jednom od svojih poznatih radova o računalnim virusima "*Računalni virusi - Teorija i eksperimenti*" (eng. "*Computer Viruses - Theory and Experiments"*) iznio je čvrst teorijski dokaz kako ne postoji algoritam koji može savršeno otkriti sve moguće zloćudne programe.



Slika 2. Fred Cohen
Izvor: Google

[1] Bernd Fix (rođen 1962. god.), njemački stručnjak na području računalne sigurnosti.

[2] Atari ST - osobno računalo kompanije Atari Corporation proizvedeno 1985. godine.

[3] G data - skup antivirusnih rješenja kompanije G Data Software, Inc.

[4] UVK 2000 (eng. *Ultimate Virus Killer 2000*) - antivirusni program namijenjen za Atari ST

Godine 1988. započelo je i dopisivanje putem elektroničke pošte u BITNET/EARN[5] mrežama. Tema dopisivanja bio je razgovor o novim virusima i načinima za njihovo otkrivanje i uklanjanje. Na listi sudionika nalazili su se i John McAfee[6] i Eugene Kaspersky[7], danas poznati kao osnivači kompanija koje se bave razvojem i prodajom komercijalnih antivirusnih programa.

U tim početnim godinama Internet je još bio u svojim začetcima pa su se računalni virusi uobičajeno širili zaraženim disketama (eng. *floppy disks*). Antivirusni programi tog razdoblja bili su korisni, ali su se nadograđivali relativno rijetko. Također su bili i jednostavniji u usporedbi s današnjim antivirusnim programima, jer su trebali provjeriti samo izvršne datoteke i *boot* sektore prijenosnih diskova ili tvrdog diska.

2.1.2. Moderno doba

S razvojem Interneta opasnost od zaraze ne predstavljaju više samo prijenosni diskovi već se virusi počinju širiti i preko mreže (eng. *online*).

Uz to se javljaju i novi problemi za antivirusne programe:

- Makro naredbe korištene u programima za obradu teksta, kao što je na primjer Microsoft Word, predstavljaju rizik jer ih programeri virusa mogu iskoristiti za pisanje virusa ugniježdenih u dokumentu. To znači da se računalo može zaraziti samim otvaranjem dokumenta koji sadrži skrivenu makro naredbu u prilogu.
- Omogućeno je ugnježđivanje izvršnih objekata u inače neizvršnim formatima datoteka pa otvaranje takvih datoteka predstavlja rizik za sigurnost računala.
- Kasniji programi elektroničke pošte (Microsoft Outlook Express i Microsoft Outlook) bili su ranjivi na viruse ugniježdene u tijelu same elektroničke poruke. Korisnikovo računalo moglo se zaraziti samim otvaranjem takve poruke.

Navedeni problemi doveli su do potrebe da antivirusni sustavi počnu provjeravati razne oblike datoteka, a ne samo izvršne datoteke.

U današnje vrijeme, kada je stalan pristup Internetu uobičajen, a novi virusi se sve brže i češće pojavljuju, nužno je često nadograđivati antivirusne programe. Čak i tada je moguće da se novonastali virus uspije jako proširiti prije nego proizvođači antivirusnih programa uspiju izdati nadogradnju koja bi štitila računala od tog virusa.

[5] BITNET/EARN mreže - BITNET (eng. *Because It's There Network*) je nastala na području SAD-a, dok je EARN eng. (*European Academic Research Network*) koristila istu tehnologiju kao BITNET ali na području Europe.

[6] John McAfee (rođen 1945. god.) - programer i osnivač kompanije McAfee. Jedan od prvih osoba koje su dizajnirale antivirusni program i razvile virusni skener.

[7] Eugene Kaspersky (rođen 1965. god.) - stručnjak na području sigurnosti informacija. Suosnivač kompanije Kaspersky Lab koja se bavi proizvodnjom antivirusa i ostalih proizvoda namijenjenih sigurnosti računala.

2.2. Vrste zloćudnih programa

2.2.1. Računalni virus

Računalni virus je zloćudni program koji se širi računalnim sustavom ili mrežom koristeći se ovlastima korisnika koji su zaraženi. Zaraza se širi na način da virus unese kopiju samoga sebe u druge, inače korisne programe koji time i sami postaju virusi. [1]

Računalni virus se sastoji od sljedećih dijelova:

- dijela koji omogućava razmnožavanje virusa - obvezan dio virusa,
- dijela koji je nosiva komponenta (eng. *payload*) koja može biti bezopasna ili opasna - nije obvezna,
- dijela koji predstavlja funkciju za okidanje (eng. *trigger function*) - određuje vrijeme (a ponekad i događaj) kada će se aktivirati nosiva komponenta virusa - nije obvezna.

Ponekad virus zahtijeva interakciju čovjeka kako bi se kopirao (poput pokretanja programa koji sadrži virus ili otvaranja neke zaražene datoteke).

2.2.2. Računalni crv

Računalni crvi su zloćudni programi koji umnožavaju sami sebe, ali za razliku od računalnih virusa, svojim djelovanjem ne moraju zaraziti druge programe. Prenose se mrežama, često bez sudjelovanja čovjeka. Jedan od načina širenja je i prijenos putem elektroničke pošte. U tom slučaju računalni crv se nalazi u privitku.

Pristup računalu omogućuju im propusti u operacijskom sustavu ili programima, a posljedica je otežani rad mreže, oštećenje podataka i ugrožena sigurnost računala. [2]

2.2.3. Trojanski konj

Trojanski konj (ili trojanac) je zloćudni program koji se lažno predstavlja kao neki drugi program. Većinom se predstavlja kao neki uobičajeni korisnički program ili posebno primamljivi program. Za razliku od virusa i crva, trojanski konj se ne može sam umnožavati, ali ga korisnik može prekopirati na drugo računalo.

Trojanski konj može izvoditi razne aktivnosti, od krađe osjetljivih informacija (koje zatim šalje nekoj drugoj osobi) sve do nepotrebnog zauzimanja računalnih resursa i usporavanja rada računala. Teško ih je kontrolirati jer je metoda širenja korisnikovo povjerenje pa su mogući oblici u kojima se trojanac može pojaviti neograničene. [3]

2.2.4. Špijunski program

Spyware je široka kategorija zloćudnog programa s namjenom da preuzima djelomičnu kontrolu nad računalom bez znanja ili dozvole korisnika s ciljem stjecanja koristi za neku treću osobu (obično se radi o komercijalnoj dobiti). U pravilu se ne replicira, a zaraza se uglavnom događa prilikom posjeta ilegalnim Internet stranicama.

Tipične posljedice su prikazivanje *pop-up* reklama, preusmjeravanje HTTP (*eng. HyperText Transfer Protocol*) zahtjeva na stranice sa reklamnim sadržajem, krađa osobnih informacija, praćenje aktivnosti na Internetu u marketinške svrhe i dr. [4]

2.2.5. Oglašivački program

Oglašivački program je vrsta zloćudnog programa koji prikazuje ili preuzima oglase nakon što se instalira neki program ili nakon korištenja nekog programa.

Obično se nalaze u besplatnim programima (eng. *freeware*) kako bi njihovi autori pokrili troškove koji su bili potrebni za izradu tih programa. Neki oglašivački programi pripadaju i špijunskom programu te kao takvi narušavaju privatnost korisnika. [5]

2.3. Metode zaštite računala od zloćudnih programa

2.3.1. Desktop antivirus

Ovo je najčešći korišten oblik antivirusne zaštite. Riječ je o antivirusnom programu koji je instaliran na pojedinačno računalo i služi za njegovu zaštitu. Problem koji se javlja s ovom vrstom zaštite je u tom što je veliki broj ovakvih programa komercijalan, tj. naplaćuje se.

Prednost ove vrste zaštite je u činjenici što na tržištu postoji veliki broj desktop antivirusa pa korisnik može odabrati onaj antivirus koji najbolje odgovara njegovim potrebama. Naime, neki proizvodi postižu bolje rezultate kod jednog tipa zlonamjernih programa (npr. oglašivački program), dok im je uspješnost po pitanju drugog tipa slabija (i obratno). Problem koji se javlja kod desktop antivirusa jest da nije moguće istodobno imati instalirano više različitih desktop antivirusa na jednom računalu (u najboljem slučaju moguće je instalirati 2).

Najpoznatiji proizvođači desktop antivirusa su kompanije McAfee, Bitdefender, Kaspersky Lab, Avast, AVG itd.

2.3.2. Antivirusni sustav na oblaku

Antivirusni sustav baziran na oblaku (eng. *cloud antivirus*) kao vrsta antivirusne zaštite je osobito popularna kod računala koja nemaju dovoljnu snagu da sama izvode redovita skeniranja i potragu za zarazama.

Jedan način primjene antivirusnih sustava na oblaku uključuje skeniranje sumnjivih datoteka pomoću većeg broja antivirusnih programa. Taj način zaštite predložen je već u prvoj implementaciji antivirusnog sustava na oblakuzvanoj CloudAV. CloudAV je bio dizajniran s ciljem da šalje programe ili datoteke na oblak na mreži gdje bi oni zatim bili skenirani s većim brojem antivirusnih programa kako bi se poboljšala stopa prepoznavanja. Taj koncept je još uvijek u upotrebi.

2.3.3. Mrežni vatrozid

Mrežni vatrozid (eng. *network firewall*) spriječava nepoznate programe i procese u pristupu sustavu. Ipak, oni nisu antivirusi i ne pokušavaju ništa identificirati ili ukloniti.

Ipak, štite od zaraza koje dolaze izvana u zaštićenu mrežu ili računalo i ograničavaju aktivnost zlonamjernih programa kojima je računalo eventualno zaraženo tako da blokiraju dolazeći ili odlazeći promet na određenim TCP/IP (eng. *Transmission Control Protocol/Internet Protocol)* priključnicama. Zbog navedenog se mogu koristiti kao dodatak antivirusnom sustavu, ali nikako kao njegova zamjena. Neki često korišteni mrežni vatrozidi na raznim verzijama Unix sustava su na primjer IPF (eng. *IPFilter*), IPFW (eng. *IPFirewall*) i PF (eng. *Packet Filter*).

2.3.4. Specijalizirani alati

Specijalizirani alati koriste se za uklanjanje zaraza koje standardni antivirusi ne uspijevaju ukloniti ili za uklanjanje određenih drugih tipova infekcija. Među takve alate ubrajaju se tzv. *rescue* diskovi (bootable CD or USB) koji se koriste za pokretanje antivirusnog programa izvan instaliranog operacijskog sustava. Ovakav pristup je iznimno koristan kada se zbog virusa operacijski ustav ne može podignuti ili kada je računalo zaraženo zloćudnim programom kojeg instalirani antivirusni sustav ne može ukloniti.

2.3.5. *Online* antivirusi

Oblik detekcije zloćudnog programa koji je osobito popularan u posljednje vrijeme. O njemu će više riječi biti u poglavlju 3.

2.4. Načini prepoznavanja računalnih virusa

Postoji nekoliko metoda kojima antivirusni programi mogu identificirati zlonamjerne programe. Najpoznatije su [6]:

1. prepoznavanje na temelju uzorka (eng. *signature based detection*),
2. prepoznavanje korištenjem heuristike (eng. *heuristic-based detection*),
3. pokretanje u sigurnom okruženju ili emulacija datoteka (eng. *file emulation*) te
4. prepoznavanje *rootkit* programa (eng. *rootkit detection*).

U nastavku je dan kratak pregled navedenih metoda.

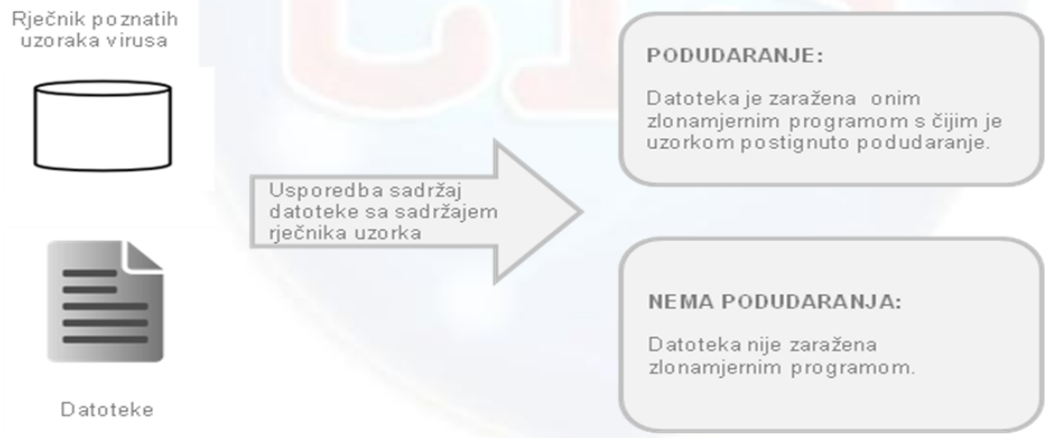
2.4.1. Prepoznavanje na temelju uzorka

Prepoznavanje na temelju uzorka je najčešće korištena metoda.

Antivirusni sustav posjeduje riječnik poznatih uzoraka virusa (eng. *dictionary of virus signatures*). Prilikom procesa prepoznavanja virusa i drugih zlonamjernih programa, antivirusni program uspoređuje sadržaj datoteke sa sadržajima rječnika. Pri tom se cijela datoteka pretražuje i kao cjelina i dio po dio (jer virus može biti ugniježđen u samu datoteku) (Slika 3.).

Usprkos činjenici da je ovaj način prepoznavanja zlonamjernih programa najrasprostranjeniji, može se dogoditi da se računalo zarazi novim zlonamjernim programom čiji uzorak još nije poznat antivirusnom sustavu i ne nalazi se u njegovu rječniku (eng. *zero-days threats*). U takvim slučajevima prepoznavanje na temelju uzorka je neučinkovito.

Najpoznatiji antivirusni sustav koji koristi prepoznavanje na temelju uzorka je antivirusni sustav kompanije Kaspersky.



Slika 3. Koraci pri prepoznavanju zlonamjernih programa korištenjem prepoznavanja na temelju uzorka

Izvor: CIS

2.4.2. Prepoznavanje korištenjem heuristike

Sofisticiraniji antivirusni programi koriste heuristiku pri prepoznavanju zlonamjernih programa. Ovaj pristup je u prednosti pred prepoznavanjem na temelju uzorka jer se može

koristiti i za prepoznavanje varijacija postojećih ili za prepoznavanje *zero-day*[8] zlonamjernih programa.

Većina virusa je u početku samo manja zaraza sustava. Međutim, kroz mutacije ili zbog izmjena koje napravi zlonamjerni korisnik, mogu prerasti u mnogobrojne inačice koje se međusobno blago razlikuju. Ipak, ta razlika je dovoljna da prepoznavanje na temelju uzorka doživi neuspjeh. U takvim slučajevima koristi se heuristički pristup poznat kao generičko prepoznavanje (eng. *generic detection*). Takav oblik prepoznavanja u datoteci traži poznati zlonamjerni kod ili njegove varijacije na temelju znanja o početnoj definiciji dotičnog virusa.

Iako je ponekad poželjno moći prepoznati o kojoj se inačici dotičnog zlonamjernog programa radi, najčešće nas to ne zanima, nego nam je samo bitno da je riječ o takvom programu. Tada je puno brži i učinkovitiji pristup prepoznavanju temeljen na generičkom uzorku. Takav uzorak sadrži kod koji je zajednički svim inačicama dotičnog zlonamjernog programa ispresijecan sa zamjenskim znakovima (eng. *wildcard characters*) na mjestima gdje se kodovi inačica zlonamjernih programa razlikuju. Zamjenski znakovi omogućuju antivirusnom sustavu prepoznavanje virusa čak i ako se pokušaju zamaskrati ubacivanjem dodatnog beznačajnog koda.

Antivirusni sustav kompanije Bitdefender poznat je po učinkovitom korištenju heuristike pri detekciji zlonamjernih programa.

2.4.3. Pokretanje u sigurnom okruženju

Antivirusni programi koji koriste ovaj način zaštite računala od zaraze virusima zapravo predviđaju što će datoteka učiniti nakon pokretanja. To čine na način da pokrenu datoteku u sigurnom okruženju (tzv. *sandbox*) i analiziraju posljedice pokretanja kako bi se uvjerili da datoteka ne sadrži skrivenu zarazu.

Sigurno okruženje pruža strogo kontrolirani skup resursa kojima se koriste programi koji se pokreću u njemu. Pri tom su pristup mreži, čitanje s ulaznih uređaja i pristup glavnom sustavu računala onemogućeni ili jako ograničeni.

Pokretanje u sigurnom okruženju najčešće se koristi za pokretanje neprovjerenog programskog koda ili sumljivih programa dobivenih od nepouzdanih izvora.

Među antivirusnim sustavima koji omogućuju pokretanje u sigurnom okruženju najpoznatiji je Avast! Pro Antivirus.

2.4.4. Prepoznavanje *rootkit* programa

Rootkit je tip zlonamjernog programa posebno dizajniran za postizanje administratorskih prava nad sustavom. Pri tome je naglasak na zahtjevu da preuzimanje prođe neprimijećeno, tj. *rootkit* ima potpuni pristup sustavu, a pri tom je nevidljiv korisniku i ne prikazuje se na listi pokrenutih procesa u task manageru.

Rootkit programi mogu promijeniti funkcioniranje operacijskog sustava i u nekim slučajevima čak utjecati na rad antivirusnog sustava. Ovaj tip zlonamjernog programa je teško ukloniti iz sustava i najčešće je potrebna potpuna ponovna instalacija operacijskog sustava. Primjer alata za uklanjanje *rootkit* programa je alat GMER, ali i antivirusni programi poznatih kompanija kao što su Panda, AVG itd. također nude zaštitu od *rootkit* programa.

[8] Zero-day zlonamjerni program - novi, prethodno nepoznati zlonamjerni program čiji uzorak još nije poznat

3. *Online* antivirusi

U današnje doba *online* antivirusi predstavaljaju jako popularan način prepoznavanja zlonamjernih programa među korisnicima računala. Mnogi razlozi za to su: u svakom trenutku *online* antivirusi su nadograđeni na posljednje inačice programa, jednostavni su za korištenje zahvaljujući preglednom sučelju i većina ih je besplatna.

Skoro svi vodeći proizvođači antivirusnih programa danas nude neku vrstu *online* skeniranja za sadašnje i buduće korisnike. Naime, kompanije se vode sljedećom logikom - ako besplatno *online* skeniranje pronađe i ukloni neku zarazu, onda je velika vjerojatnost da će korisnik poželjeti imati i plaćenu instalaciju dotičnog programa koja će mu učinkovito štititi podatke i računalo od budućih zaraza.

Ipak, *online* antivirusi imaju dosta prednosti pred desktop antivirusima, ali i neke nedostatke koji su navedeni u nastavku dokumenta [7].

3.1. Način rada online antivirusa

Online antivirusi imaju mnogo sličnosti s tradicionalnim desktop antivirusima. Ipak, njihov glavni nedostatak je što oni ne pružaju dugotrajnu zaštitu. Naime, *online* antivirusi koriste se za detekciju i uklanjanje samo onih zlonamjernih programa koji se nalaze na računalu u trenu pokretanja *online* antivirusnog programa.

Svi online antivirusni programi imaju 3 faze rada:

1. instalacija potrebnih datoteka,
2. skeniranje računala te
3. prikaz rezultata skeniranja.

Tijekom procesa instalacije na računalo se instaliraju datoteke potrebne za rad *online* antivirusa među kojima je i riječnik uzoraka virusa poznatih u trenu pokretanja alata. Datoteke se instaliraju u mapu privremenih datoteka, što olakšava njihovo uklanjanje i spriječava mogući utjecaj na registre operacijskog sustava.

Na početku faze skeniranja korisnik može odabrati način skeniranja i prostor koji je potrebno skenirati. Nakon izvršenog odabira, *online* antivirus počinje s radom, tj. pretražuje zadani prostor u potrazi za zlonamjernim programima.

Nakon što proces skeniranja završi, korisnik će biti obaviješten o rezultatima skeniranja. Pojedini *online* antivirusi samo prikazuju rezultate skeniranja, dok drugi nude i opciju uklanjanja pronađenih zlonamjernih programa.

3.2. Prednosti online antivirusa

Neke od osnovnih prednosti *online* antivirusnih programa su:

- **Većina ih je besplatna**

  Nema potrebe za probnom inačicom ili registracijom kao kod većine desktop antivirusa.

- **Točnije prepoznavanje**

  Prvi korak većeg broja zlonamjernih programa jest onemogućiti rad instaliranog antivirusnog programa. To se ne može dogoditi s *online* antivirusima pa oni nude točnije prepoznavanje jer zlonamjerni program kojim je zaraženo korisnikovo računalo ne utječe na njihov rad.

- **Izbor usluge**

  Korisnik može svaki put koristiti različitu vrstu zaštite, ovisno o potrebama u tom trenutku.

  Poznato je da danas većina desktop antivirusa može otkriti i ukloniti različite oblike zlonamjernih programa, ali neki proizvodi postižu bolje rezultate kod jednog tipa zlonamjernih programa (npr. oglašivački program), dok im je uspješnost po pitanju

drugog tipa slabija (i obratno). Problem koji se javlja uz ovo jest da nije moguće istodobno imati instalirano više različitih desktop antivirusa na jednom računalu (u najboljem slučaju moguće je instalirati 2).

Online antivirusi se ne susreću s ovim problemom, pa korisnik može računalo skenirati s onim proizvodom koji nudi najbolju uspješnost pri prepoznavanju i uklanjanju tipa zlonamjernog programa na koji korisnik sumnja.

- **Uklanjanje težih oblika zaraze**

  Ponekad nije ni moguće instalirati desktop antivirus ako je računalo već zaraženo jer neki zlonamjerni programi ne dozvoljavaju instalaciju antivirusa. U tom slučaju potencijalno rješenje, uz specijalizirane alate koji su u većini slučajeva skupi, predstavlja *online* antivirus.

- **Nije potrebna deinstalacija**

  Ako u nekom trenutku korisnik više ne želi koristiti odabrani *online* antivirus, sve što treba učiniti je ukloniti skinuti riječnik uzoraka virusa (riječnik se preuzima kao privremena datoteka i nema utjecaja na najosjetljiviji dio operacijskog sustava - registre).

3.3. Nedostaci online antivirusa

Osnovni nedostaci online antivirusa su:

- **Nepostojanje stabilne Interenet veze**

  Za pokretanje *online* antivirusa potrebna je stabila Internet veza. Neki zlonamjerni programi mogu utjecati na TCP/IP postavke i na taj način onemogućiti pokretanje *online* antivirusa.

- **Korisnički računi s ograničenim pravima**

  Internet preglednik zahtijeva određene privilegije kako bi se *online* skeniranje moglo provesti. Ako su privilegije ograničene, to znači da korisnik nema potrebna prava vezana uz njegov korisnički račun koja bi dozvolila preuzimanje riječnika uzoraka virusa i ne može pokrenuti *online* antivirus.

- "Pametni virusi" mogu spriječiti pokretanje online antivirusa.
- *Online* antivirus, za razliku od desktop antivirusa, ne može spriječiti buduće zaraze, samo može otkriti i ukloniti postojeće.
- Neki *online* antivirusi nemaju mogućnost uklanjanja pronađenih zlonamjernih programa.
- Ponekad je potrebno ponoviti skeniranje nakon ponovnog pokretanja računala. Većina *online* antivirusa ovisi o programima Internet Explorer i ActiveX, a zlonamjerni program često zna utjecati na njihove postavke, pa *online* antivirus ponekad ne može ukloniti zarazu odjednom.

3.4. Besplatni online antivirusi

U nastavku dokumenta slijedi pregled najpopularnijih online antivirusa.

3.4.1. Trend Micro HouseCall

Online antivirus kompanije Trend Micro, Trend Micro HouseCall, nudi prepoznavanje i uklanjanje virusa i špijunskih programa. Trenutno je najpopularniji *online* antivirus. Osim zbog odličnog uspjeha prepoznavanja i uklanjanja, prednosti su mu da ga se može koristiti na operacijskim sustavima Windows i Mac, preko web preglednika IE ili Mozilla te uz pomoć ActiveX ili Java engine. Nedostatak je da ipak zahtijeva preuzimanje i instalaciju na računalo, iako se sve prepoznavanje odvija *online*.

Prikaz rada programa dan je na slici 4.

Slika 4. Izgled prozora Trend Micro online antivirusa
Izvor : Google

3.4.2. BitDefender Online Scan

Online antivirus kompanije Bitdefender, BitDefender Online Scan, nudi mogućnost slanja izvješća BitDefender laboratoriju sigurnosti nakon što je skeniranje računala završeno, čime korisnik može pomoći razvoju proizvoda. Korisnik može izabrati particije koje želi skenirati, čime se reducira vrijeme potrebno za skeniranje. Podržava samo web preglednik IE.

Prikaz sučelja programa dan je na slici 5.

Slika 5. BitDefender Online Scan
Izvor : Google

3.4.3. McAfee FreeScan

McAfee FreeScan je *online* antivirus najpopularnije kompanije na području sigurnosti računala u SAD-u - McAfee kompanije. Nedostatak je što zahtijeva preglednik IE inačice 5.0+ i radi samo s ActiveX kontrolom koja mora biti omogućena. Omogućuje samo prepoznavanje zaraza, ne i njihovo uklanjanje.

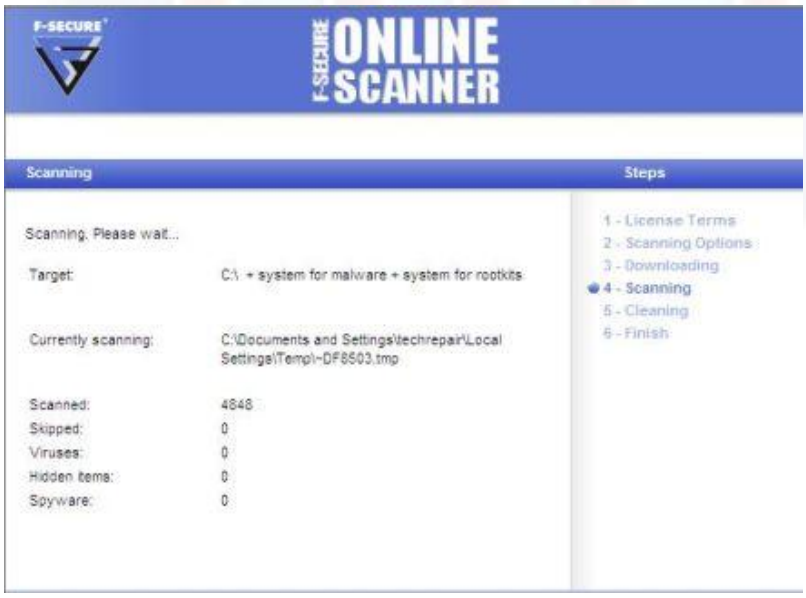
Prikaz rada programa dan je na slici 6.

Slika 6. Izgled prozora FreeScan online antivirusa
Izvor: Google

3.4.4. F-Secure Free Online Scanner

F-Secure Free Online Scanner je besplatni *online* antivirus koji omogućava prepoznavanje i uklanjanje virusa i *rootkit* programa. Zahtijeva uporabu web preglednika IE.

Prikaz skeniranja programa dan je na slici 7.



Slika 7. Izgled prozora F-Secure online antivirusa
Izvor: Google

3.4.5. ESET NOD32 Online Antivirus Scanner

ESET NOD32 Online Antivirus Scanner je besplatni *online* antivirus. Koristi patentiranu tehnologiju ThreatSense firme ESET. ThreatSense tehnologija uz prepoznavanje na temelju uzorka koristi i prepoznavanje korištenjem heuristike, čime se postiže bolja zaštita od novih virusa. Uz to, istraživačima u laboratorijimaautomatski se (ili manualno) dostavljaju primjeri novih kodova za koje se sumnja da su zlonamjerni, što vodi smanjenju razdoblja ranjivosti na nove prijetnje.

Ovaj antivirus nudi prepoznavanje i uklanjanje velikog broja zlonamjernih programa uključujući i špijunski program. Zahtijeva korištenje ActiveX kontrole i preglednika IE.

Prikaz rada programa dan je na slici 8.

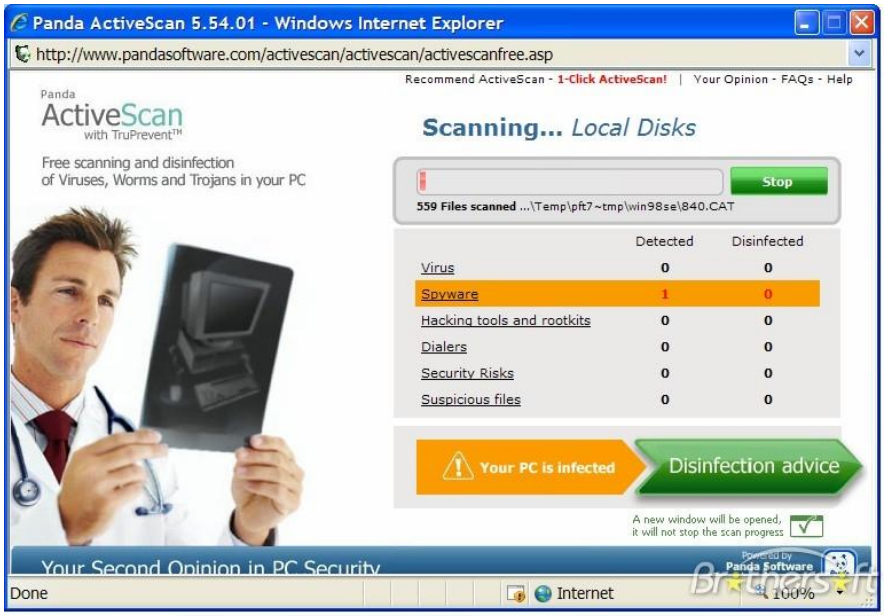
Slika 8. Izgled prozora Eset NOD32 online antivirusa
Izvor: Google

3.4.6. Panda ActiveScan

Panda ActiveScan je antivirusni sustav tvrtke Panda Security. Koristi njihovu TruPrevent tehnologiju koja omogućuje da antivirus instaliran na korisnikovu računalu automatski šalje izvješće kompanijinom laboratoriju kada primjeti sumljivi dio koda za koji nije pronašao uzorak u riječniku. Time se ubrzava proces otkrivanja novih virusa i njihovih uzoraka.

Može otkriti ogroman broj zaraza, uključivo razne zlonamjernih programa. Besplatna inačica ne nudi mogućnost uklanjanje otkrivenih zaraza. Prednost je mogućnost rada i s preglednikom IE i Mozilla.

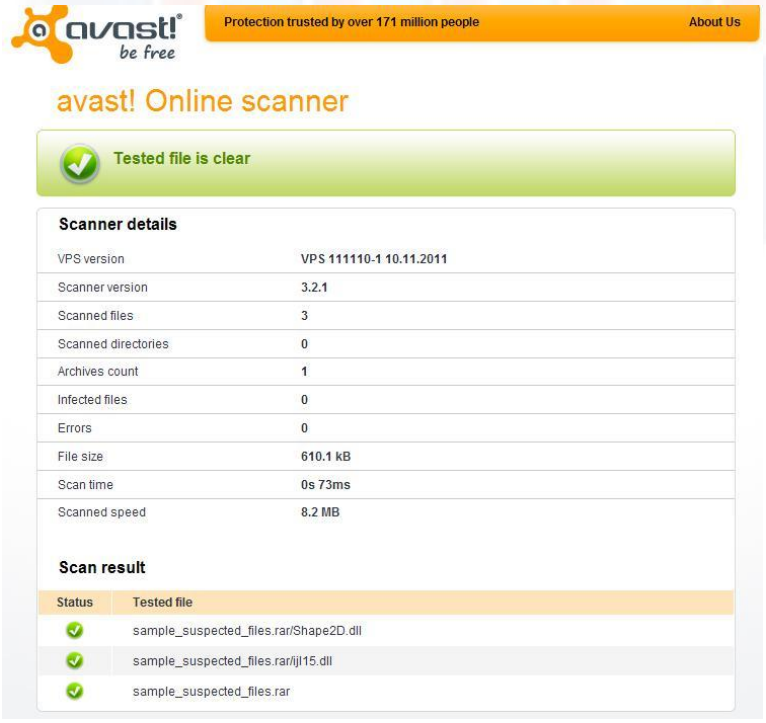
Prikaz rada programa dan je na slici 9.



Slika 9. Izgled prozora Panda ActivScan online antivirusa
Izvor : Google

3.4.7. Avast! Online Virus Scanner

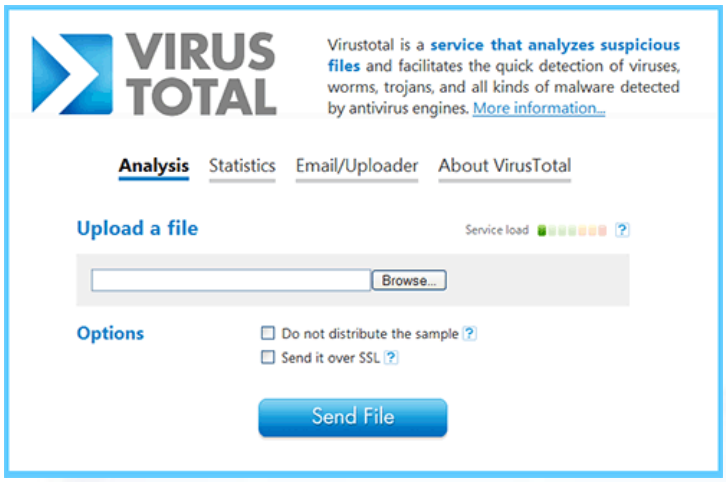
Za razliku od prethodno spomenutih *online* antivirusa, Avast! Online Virus Scanner nudi mogućnost skeniranje samo jedne datoteke. To je osobito korisno ako korisnika zanima je li određena datoteka zaražena ili ne. Naime, umjesto skeniranja cijelog računala (za što je potrebno neko određeno vrijeme), Avast! Online Virus Scanner omogućuje korisniku provjeru samo jedne datoteke za koju postoji sumnja da je zaražena. Prikaz rezultata skeniranja jedne datoteke dan je na slici 10.



Slika 10. Izgled prozora Avast! Online Scannera
Izvor: Google

3.4.8. Virus Total

Virus Total je besplatni *online* antivirus. Kao i Avast! omogućuje korisniku skeniranje i uklanjanje zlonamjernih programa iz jedne datoteke. Jako je popularan alat među brojnim korisnicima. Prikaz sučelja programa dan je na slici 11.



Slika 11. Izgled prozora Virus Total online antivirusa
Izvor: Google

3.5. Komercijalni online antivirusi

3.5.1. Pivot Online Anti-Virus

Pivot Online Anti-Virus namijenjen je korisnicima koji posjeduju vlastite Internet stranice. Radi se o jednom od prvih *online* antivirusa ovog tipa, proizvedenom u kompaniji Entacore.

Princip rada je sljedeći:

- korisnik se registrira na stranicama proizvoda i upiše detalje o svojoj Internet stranici.
- Nakon toga Pivot Online Anti-Virus skenira stranicu i uspoređuje datoteke s poznatim uzorcima zlonamjernih programa.
- Ako se otkrije zaražena datoteka, pronađeni zlonamjerni program se uklanja iz nje.

Ovaj tip *online* antivirusa nije besplatan, a cijena ovisi o količini stranica koje korisnik štiti ovim antivirusom. U tablici u nastavku dan je pregled cijena i usluga koje nudi Pivot Online Anti-Virus.

Jednokratno korištenje	19 $ (USD)
Godišnja zaštita jedne internet stranice	69 $ (USD)
Godišnja zaštita 5 internet stranica	169 $ (USD)
Godišnja zaštita 10 internet stranica	269 $ (USD)
Godišnja zaštita 20 internet stranica	469 $ (USD)
Godišnja zaštita 30 internet stranica	699 $ (USD)
Godišnja zaštita 40 internet stranica	930 $ (USD)

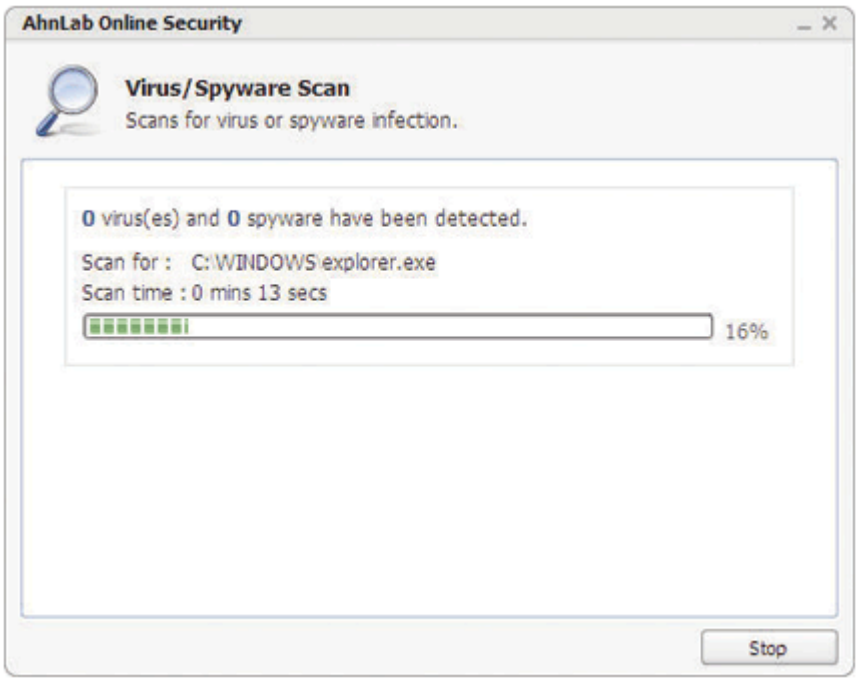
Tablica 1. Pregled cijena i usluga koje nudi Pivot Online Anti-Virus
Izvor : Entacore [8]

3.5.2. AhnLab Online Security

AhnLab Online Security je komercijalni *online* antivirus kompanije AhnLab. Odlikuje se jednostavnim korisničkim sučeljem i brojnim opcijama za skeniranje i uklanjanje zlonamjernih programa. Namjenjen je uklanjanju računalnih virusa i špijunskih programa.

Pri prepoznavanju koristi heuristiku što omogućuje veću zaštitu i sigurnost.

Prikaz sučelja programa dan je na slici 12.



Slika 12 Izgled sučelja AhnLab Online Security antivirusa
Izvor: AhnLab Online Security [9]

4. Zaključak

U posljednje vrijeme sve veći broj stručnjaka tvrdi kako je prošlo vrijeme tradicionalnih antivirusnih metoda za prepoznavanje i uklanjanje virusa, trojanaca i ostalih zlonamjernih programa, a koje se zasnivaju na uspoređivanju koda s virusnim uzorkom. Oni smatraju kako se takve metode ne mogu nositi s poplavom raznih inačica zlonamjernih programa. Dodatan argument kojim se koriste jest da većina autora zlonamjernih programa ispituju svoje "proizvode" na postojećim antivirusnim programima kako bi se uvjerili da ih dotični antivirusi neće otkriti. Ipak, računalu je potreban neki oblik zaštite, a antivirusi su za sada još uvijek dovoljno učinkovita rješenja. Uz to valja istaknuti kako postoji veliki broj proizvođača antivirusnih programa što omogućuje da svaki korisnik pronađe odgovarajuću zaštitu za sebe.

Uz tradicionalne desktop antiviruse, većina tih proizvođača nudi i *online* inačicu svojih proizvoda, koja ne zahtijeva instalaciju na računalo te ima brojne prednosti pred desktop inačicama. Iako *online* antivirusi ne nude zaštitu u vidu neprestanog nadzora računala kao desktop antivirusi, još uvijek predstavljaju odličan dodatak zaštiti korisničkih računala s kojim bi svaki korisnik trebao biti upoznat. Periodička provjera računala *online* antivirusom može pomoći u boljoj zaštiti korisničkih podataka i sigurnijoj upotrebi računala.

5. Leksikon pojmova

Antivirus ili antivirusni program

Koristi se za spriječavanje, prepoznavanje i uklanjanje malicioznih programa (eng. malware) kao što su računalni virusi (eng. computer viruses), računalni crvi (eng. computer worm), trojanski konji (eng. trojan horses), špijunski program (eng. spyware) ili oglašivački program (eng. adware).

http://en.wikipedia.org/wiki/Antivirus_software

Računalni virus

Računalni virus (eng. *computer virus*), je program koji može "zaraziti" druge programe tako da u njih unese kopiju samog sebe (koja može biti modificirana). Virus se može proširiti računalnim sustavom ili mrežom koristeći se ovlastima korisnika koji su zaraženi. Svaki program koji je zaražen postaje virus i tako zaraza raste.

http://hr.wikipedia.org/wiki/Računalni_virus

Računalni crv

Računalni crvi (eng. *computer worm*) su računalni programi koji umnožavaju sami sebe. Pri tome koriste računalne mreže da bi se kopirali na druga računala, često bez sudjelovanja čovjeka. Za razliku od virusa, sa svojim djelovanjem ne moraju inficirati druge programe. Mogu stići i kao privitak u elektroničkoj pošti te im pristup računalu omogućuju propusti u operacijskim sustavima i programima. Crvi otežavaju rad mreže, a mogu oštetiti podatke i kompromitirati sigurnost računala.

http://hr.wikipedia.org/wiki/Računalni_crv

Trojanski konj

Trojanski konj ili kraće trojanac (eng. *trojan horse*) je maliciozni računalni program koji se lažno predstavlja kao neki drugi program s korisnim ili poželjnim funkcijama.

http://hr.wikipedia.org/wiki/Trojanski_konj_%28softver%29

Špijunski program

Špijunski program (eng. *spyware*) je široka kategorija malicioznog softwarea sa namjenom da presreće ili preuzima djelomično kontrolu rada na računalu bez znanja ili dozvole korisnika.

http://hr.wikipedia.org/wiki/Spyware

Oglašivački program

Oglašivački program (eng. *adware*) je program koji automatski prikazuje ili preuzima oglase na računalu nakon što je instaliran neki program ili nakon korištenja nekog programa.

http://hr.wikipedia.org/wiki/Adware

Rootkit

Rootkit-ovi su zlonamjerni programi koji su napravljeni da bi preuzeli kontrolu nad operacijskim sustavom tako da nadomjeste sustavske procese i podatke bez dopuštenja korisnika.

http://os2.zemris.fer.hr/ns/2008_Mackovic/rootkit.htm

Vatrozid sustav

Uređaj čija je uloga zaštititi mrežu od neovlaštenog pristupa blokiranjem i zabranom prometa prema pravilima koje korisnik sam određuje.

http://en.wikipedia.org/wiki/Firewall(computing)

6. Reference

[1] Wikipedia, Računalni virus
http://hr.wikipedia.org/wiki/Računalni_virus, prosinac 2011.

[2] Wikipedia, Računalni crv
http://hr.wikipedia.org/wiki/Računalni_crv, prosinac 2011.

[3] Wikipedia, Trojanski konj
http://hr.wikipedia.org/wiki/Trojanski_konj_%28softver%29, prosinac 2011.

[4] Wikipedia, Spyware
http://hr.wikipedia.org/wiki/Spyware, prosinac 2011.

[5] Wikipedia, Adware
http://hr.wikipedia.org/wiki/Adware, prosinac 2011.

[6] Wikipedia, Antivirus software
http://en.wikipedia.org/wiki/Antivirus_software, prosinac 2011.

[7] Top Free Online Virus Scan Services
http://charlemont.hubpages.com/hub/Top-Free-Online-Virus-Scan, prosinac 2011.

[8] Pivot Online Anti-Virus
http://entacore.com/online/pivotoav, prosinac 2011.

[9] AhnLab Online Security
http://global.ahnlab.com/en/site/product/productSubDetail.do?prod_type=P1&prod_class=P&prod_seq=9011 , prosinac 2011.