Antivirusni programi

Šta su virusi?

- **Kompjuterski virusi** su programi napravljeni s namerom stvaranja smetnji u radu i različitih oštećenja datoteka i organizovanih podataka na računaru.
- Nazvani su tako jer imaju sposobnost razmnožavanja (sami sebe iskopiraju na više mesta na disku)
- Virus je program koji se razmnožava kopirajući samoga sebe u neki drugi deo izvršnoga koda.

Dejstvo virusa

- Kada se virus smesti unutar izvršnog koda, pokreće se svaki put kada se izvršava taj kod, a razmnožava se tražeći druge, 'čiste' domaćine svaki put kada se aktiviraju.
- Neki virusi se zapisuju preko originalnih datoteka, efektivno I efektivno ih uništavaju ali većina se jednostavno nastanjuje u programu-domaćinu tako da oboje preživljavaju.
- Virusi koji se šire putem e-maila su crvi.

PODELA VIRUSA

Virusi su podeljeni u osnovne klase:

- boot sektor virusi
- infektori datoteka (file infector)
- „trojanski konj“

Vrste virusa

- Boot sektor virusi
  - Aktiviraju se u boot-u sistema
- Parazitski virusi
  - Ubacuju svoj sadržaj u pokrenute datoteke
- Svestrani virusi
  - Napadaju i boot sektore i izvršne datoteke
- Virusi pratioci
  - Stvaraju .com datoteke u koje generišu svoj kod
- Link virusi
  - Napadaju datoteke operativnog sistema
- Makro virusi
  - Imaju mogućnost da sami sebe kopiraju, brišu i menjaju dokumente

ZARAŽENI RAČUNAR

- I uz najveće mere sigurnosti korisniku se može dogoditi da mu na računar dospie virus. To se obično događa korisnicima koji nisu primenili sve mere sigurnosti, odnosno koji su zanemarili upozorenja. Ako otkrijete da na vasem računaru postoji virus, posetite stranice vašeg antivirusnog programa jer se tamo nalaze i detaljne biblioteke s informacijama šta virus radi i kako se širi. Isto tako, tamo ćete pronaći i detaljnija uputstva o tome kako da se virus ukloni s računara.

ZAŠTITA RAČUNARA

- Osnovni oblik obrane od virusa je zaštita računara.
- Osnovna zaštita od virusa na samom računaru sprovodi se upotrebom programa za borbu protiv virusa. Zajedničkim imenom ovakvi programi se nazivaju **antivirusni programi**.

Šta su antivirusni programi

- Antivirusni softver, antivirusni program ili antivirus je računarski softver koji se koristi za zaštitu, identifikaciju i uklanjanje računarskih virusa, kao i drugih programa koji mogu uzrokovati probleme u korišćenju računara, oštetiti softver i/ili podatke, a jednim imenom ih nazivamo malware-i.
- Prvi antivirusni programi su počeli da se razvijaju 1983. godine.

ANTIVIRUSNI PROGRAMI

- Predstavljaju prvi nivo zaštite od virusa i trojanaca.
- To su softverski paketi sposobni da detektuju, izdvoje i (ili) eliminišu viruse.
- Svi antivirusni programi sastoje se iz više celina.
- Jedan deo je "Monitor" i rezidentan je u memoriji i osigurava neprestanu zaštitu od virusa, dok drugi deo "Scan" omogućava skeniranje celog sistema.
- Antivirusi su danas neophodan deo softvera koji svako treba da ima instaliran na svom računaru.

ANTIVIRUSNI PROGRAMI

- Pružaju različite načine nadgledanja i zaštite računara od malicioznog koda.
- Najčešće se radi o zaštiti u realnom vremenu i skeniranju na zahtev korisnika.
- Moderne verzije ovih programa nude razne druge vidove zaštite od virusa koji se šire putem Interneta.
- Najpoznatije kompanije koje nude I razvijaju ove programe su Symantec, Sophos, Panda, Kaspersky...

ANTIVIRUSNI PROGRAMI

- Broj danas poznatih virusa je oko 65.000, s tim da se opasnim smatra nekoliko stotina.
- Kvalitetna zaštita svodi se na:
  - Opreznost
  - upotrebu dobrih antivirusnih programa
  - redovno osvježavanje virusnih definicija.

ANTIVIRUSNE METODE

- **SKENERI**
  - Princip rada antivirus skenera bazira se na proveravanju datoteka, sektora i sistemske memorije u potrazi za poznatim i nepoznatim malicioznim kodom.
- Skeneri se dele u dvije kategorije:
  - opšti (general)
  - specijalni (special)

ANTIVIRUSNE METODE

- **BLOKERI DOGAĐAJA**
- Memorijski rezidentni programi koji "osluškuju" reakciju virusa i obaveštavaju o tome korisnika.

- Dobra osobina blokera je što zaustavljaju izvršavanje virusa u trenutku infekcije.
- Loša osobina je što vrlo često greše.

ANTIVIRUSNE METODE

- **IMUNIZATORI**
- dva tipa
  - one koji upozoravaju na infekciju.
  - one što blokiraju pokušaj virusa da uđe u sistem.

Metode detekcije

- Detekcija bazirana na uzorcima
  - Najčešća metoda
  - Uporedjuje sadržaj datoteke sa uzorcima iz baze podataka koja sadrži poznate kodove virusa
  - Najmanje validan metod iako se redovno ažurira sadržaj baze
  - Ne opterećuje previše RAM memoriju
  - Lako ga je predvideti
  - Iako ovaj pristup sprečava masovno širenje virusa u normalnim uslovima, autori virusa pokušavaju biti korak ispred pišući viruse koje kodiraju ili na neki način sakrivaju deo svog koda kako ga antivirus program ne bi mogao otkriti

Metode detekcije

- Heuristička metode

To je metoda traženja neuobičajene aktivnosti.

Obuhvata proces traganja za sumnjivim komandama u datotekama.

Može se raditi:

- Analiza datoteka
- Emulacija datoteka

Metode detekcije

- Analiza datoteka
  - Proverava kod datoteke/programa
  - Prijavljuje svaku sumnjivu liniju koda
  - Opterećuje RAM memoriju
  - Može prijaviti bezopasan program kao virus
- Emulacija datoteka
  - Pokreće program u virtuelnom okruženju
  - Belezi sve njegove aktivnosti
  - Oduzima svu RAM memoriju

ŠEST KORAKA U ANTIVIRUSNOJ ZAŠTITI

- **Korak 1:**
  - Obavezno instalirati neki od antivirusnih alata!
- **Korak 2:**
  - Redovno ažuriranje antivirusa.
- **Korak 3:**
  - Podesiti antivirusni softver da automatski skenira sve datoteke.
- **Korak 4:**
  - Skenirati sve datoteke koje dolaze sa Interneta.
- **Korak 5:**
  - Povremeno skenirati celi disk.
- **Korak 6:**
  - Skenirati hard disk nakon instalacije softvera.

Gde sve Antivirus može da pomogne?

- Maliciozni programi koji se skidaju bez našeg predhodnog odobrenja
- Phishing
- Clickbait reklame
- Lažni antivirusi
- Piratski sajtovi
- Zaražene fleš memorije
- Nebezbedne wifi mreže

VRSTE ANTIVIRUSNIH PROGRAMA

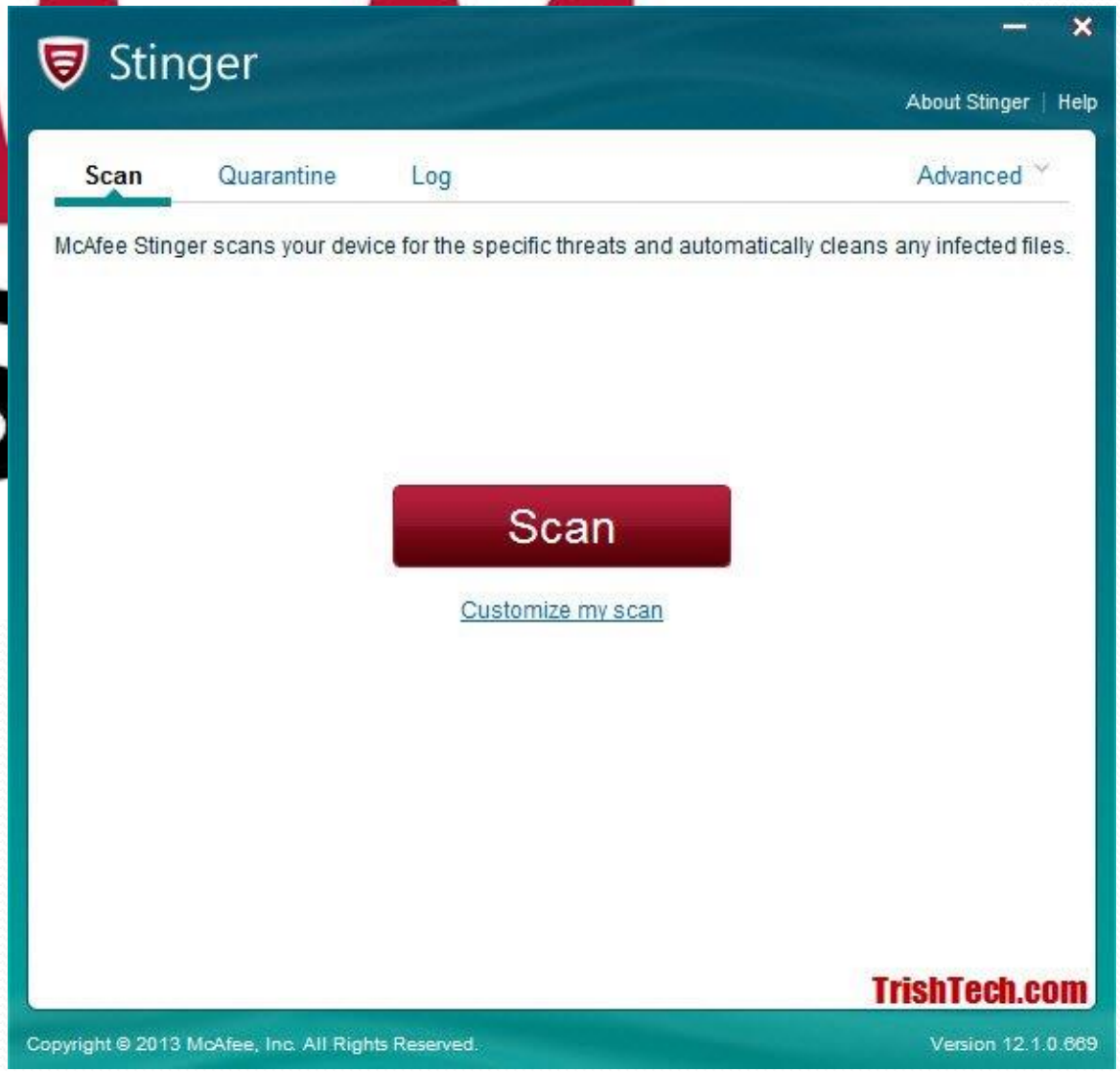
- Najpoznatiji i najčešće korišteni antivirusni programi su:
  - **NORTON ANTIVIRUS**
  - **SOPHOS ANTI-VIRUS**
  - **MCAFFEE**
  - **PCCLLIN**
  - **NOD32**

Kako antivirusi rade?

- Bitno je da nikada na kompjuteru nema instalirana dva antivirusna programa, koji će biti automatski aktivirani. To može dovesti do usporavanja ili čak blokade računara.
- Takođe, bitno je da se antivirusni programi osvežavaju, odnosno apdejtuju novim definicijama virusa.

Virus removal tools

- Postoje i alati specijalizovani za uklanjanje virusa. Radi se o softverima dizajniranim specifično za određene tipove virusa. Ne radi se o kompletnim antivirusnim programima, ali ovi alati imaju mnogo veću efikasnost. Većinom su besplatni.

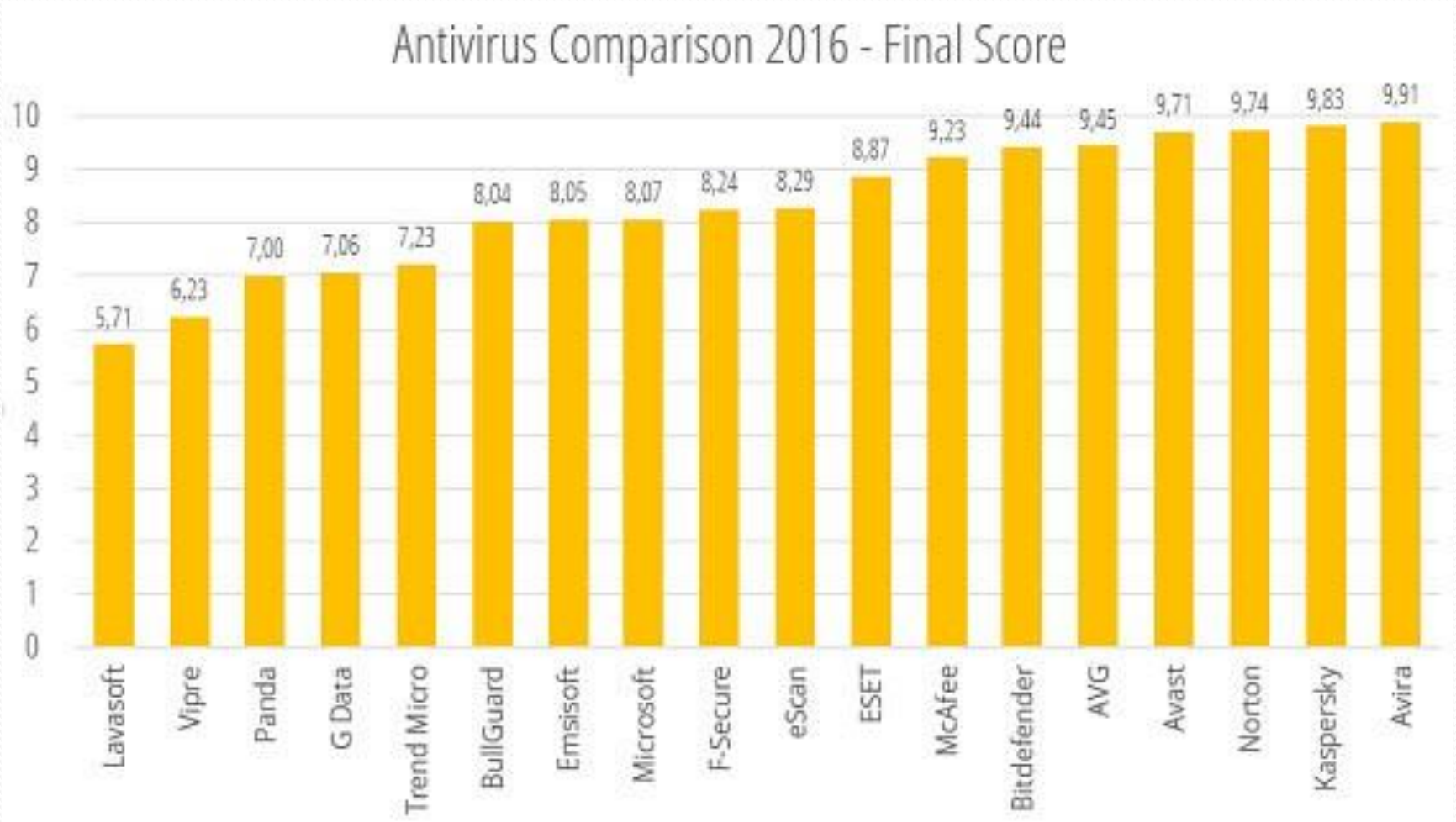

Stinger
About Stinger | Help
Scan
Quarantine
Log
Advanced
McAfee Stinger scans your device for the specific threats and automatically cleans any infected files.
Scan
Customize my scan
TrishTech.com
Copyright © 2013 McAfee, Inc. All Rights Reserved.
Version 12.1.0.669

False positives/False negatives

- U slučaju lažno pozitivnih rezultata, antivirusi ispravne datoteke prepoznaju kao loše, pa ih stoga i uklanjaju.

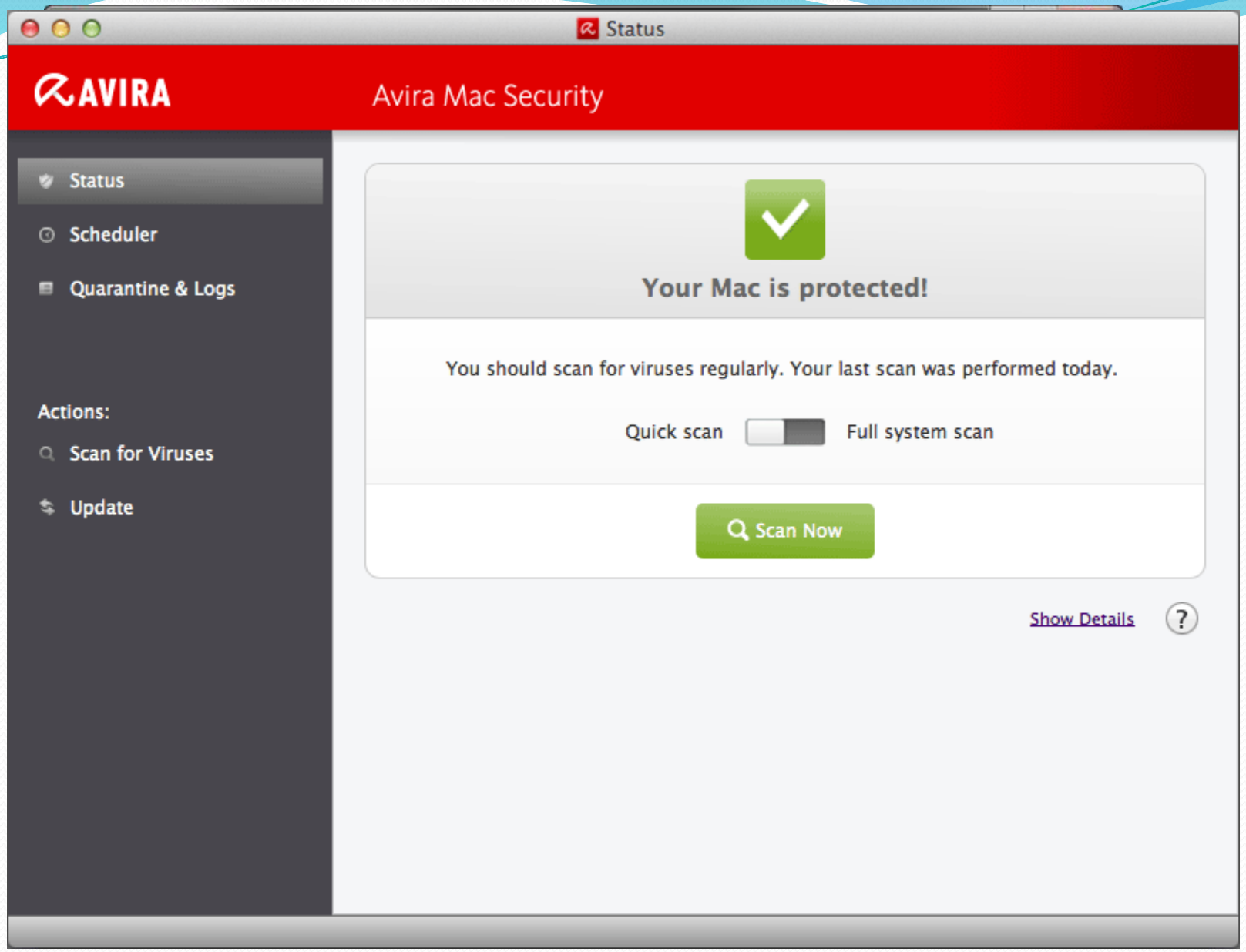
- Sa druge strane, moguće je da antivirus ne prepozna virusom zaražene fajlove, u tom slučaju dobijaju se lažno negativni rezultati.

Koii antivirus odabrati?


Antivirus Comparison 2016 - Final Score
10
9
8
7
6
5
4
3
2
1
0
5,71
6,23
7,00
7,06
7,23
8,04
8,05
8,07
8,24
8,29
8,87
9,23
9,44
9,45
9,71
9,74
9,83
9,91
Lavasoft
Vipre
Panda
G Data
Trend Micro
BullGuard
Emsisoft
Microsoft
F-Secure
eScan
ESET
McAfee
Bitdefender
AVG
Avast
Norton
Kaspersky
Avira

Avira

- Jedan od trenutno najboljih antivirusa.Nastao u nemackoj,spada medju najzastupljenije antiviruse, kako tvrde iz te kompanije sa preko 500 miliona korisnika.Postoje 3 vrste paketa koji se mogu kupiti,a cene variraju izmedju 35 I 65 dolara.


Status
AVIRA
Avira Mac Security
Status
Scheduler
Quarantine & Logs
Actions:
Scan for Viruses
Update
Your Mac is protected!
You should scan for viruses regularly. Your last scan was performed today.
Quick scan
Full system scan
Scan Now
Show Details

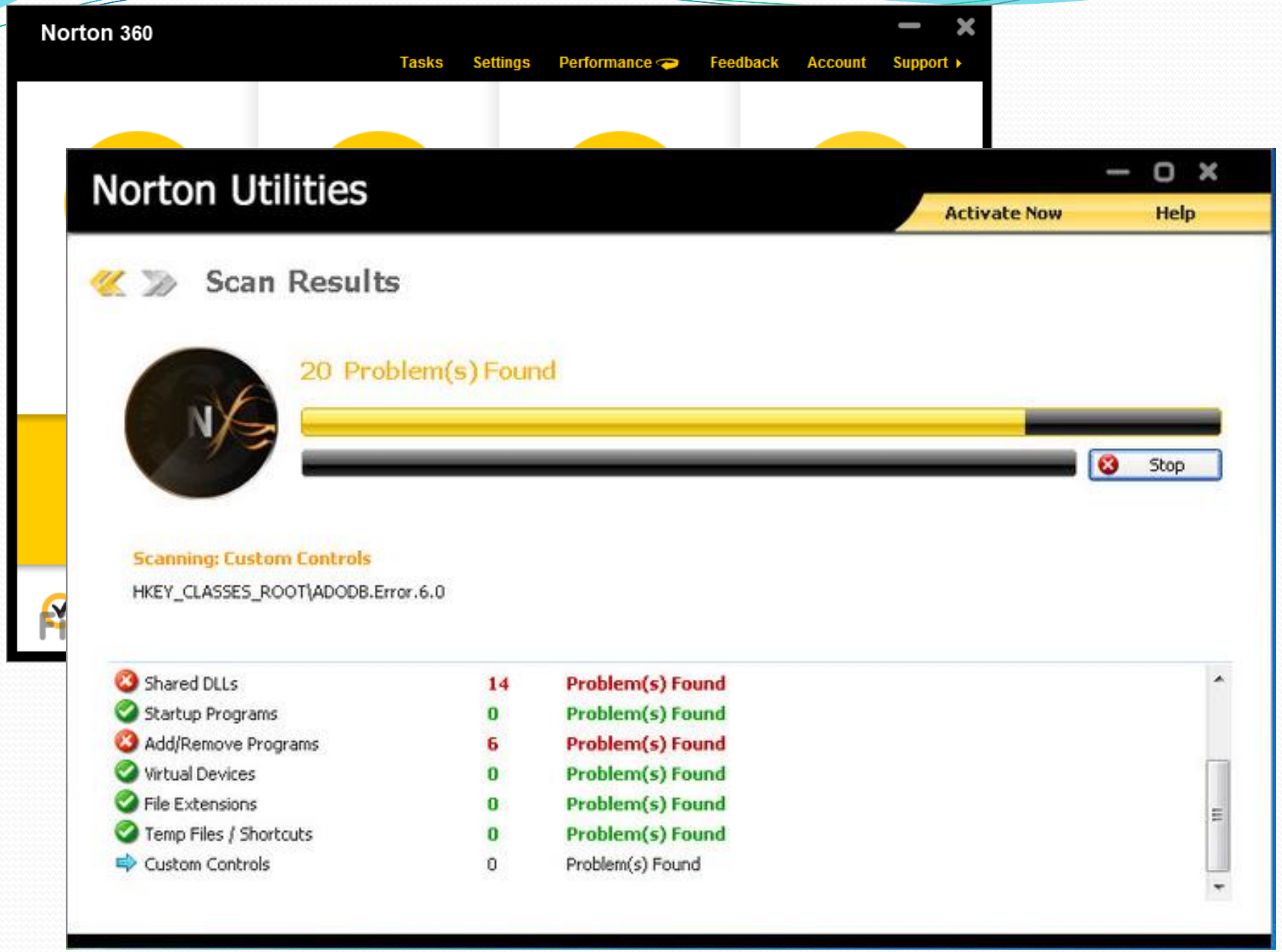
Kasperski

- Jedan je od lidera na polju zaštite računara. Otkriva prilično veliki broj štetočina a kompanija može da se pohvali da najbrže osvežava nove definicije virusa (oko 2 sata od trenutka pojavljivanja virusa). Ima odlično radno okruženje koje će svima omogućiti da se lako prilagode. Program je najskuplji od ovde predstavljenih i košta 50 dolara.


KASPERSKY
Kaspersky
Virus Removal Tool
Kaspersky Internet Security
KASPERSKY
Details
Computer is protected
Threats: none
Protection components: main components enabled
Databases: not updated recently
License: 342 days remaining
Scan
Update
Safe Money
Reports
My profile
Settings
Support
Licensing

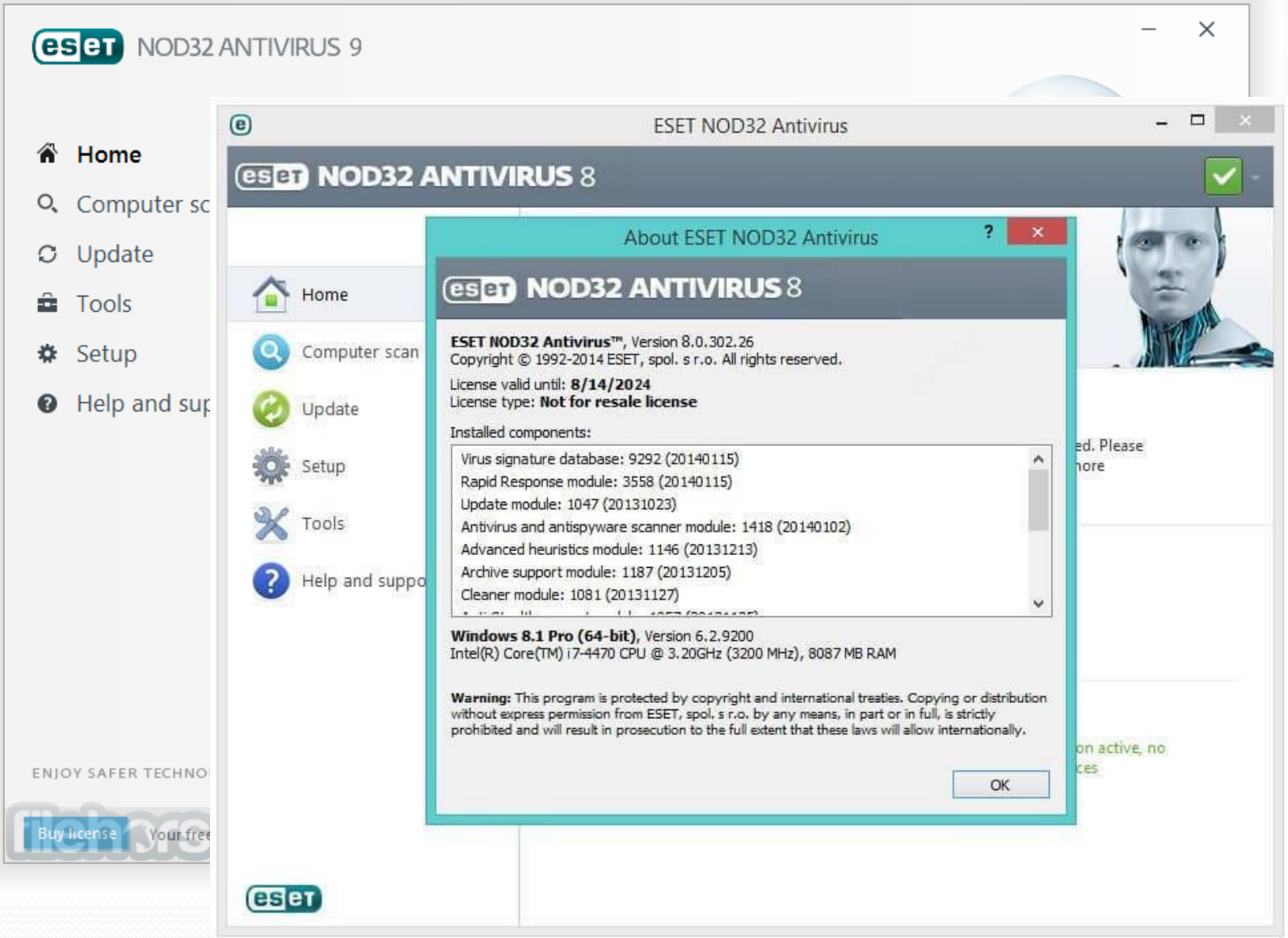
Norton

- Jedan od najstarijih i idalje jedan od najboljih antivirusa, sa velikim procentom otkrivenih pretnji. Ranije verzije su imale manu jer su primetno usporavale sistem, ali to je sada prošlost. Cena ovog programa je oko 40 dolara.


Norton 360
Tasks
Settings
Performance
Feedback
Account
Support
Norton Utilities
Activate Now
Help
Scan Results
20 Problem(s) Found
Stop
Scanning: Custom Controls
HKEY_CLASSES_ROOT\ADODB.Error.6.0
Shared DLLs 14 Problem(s) Found
Startup Programs 0 Problem(s) Found
Add/Remove Programs 6 Problem(s) Found
Virtual Devices 0 Problem(s) Found
File Extensions 0 Problem(s) Found
Temp Files / Shortcuts 0 Problem(s) Found
Custom Controls 0 Problem(s) Found

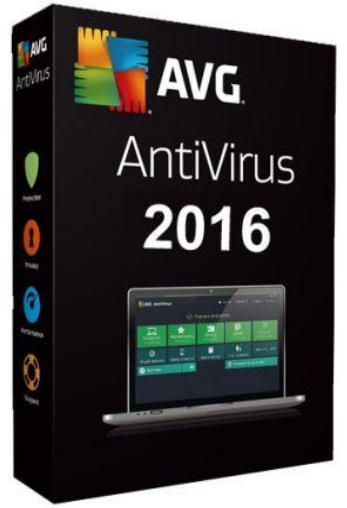
NOD32

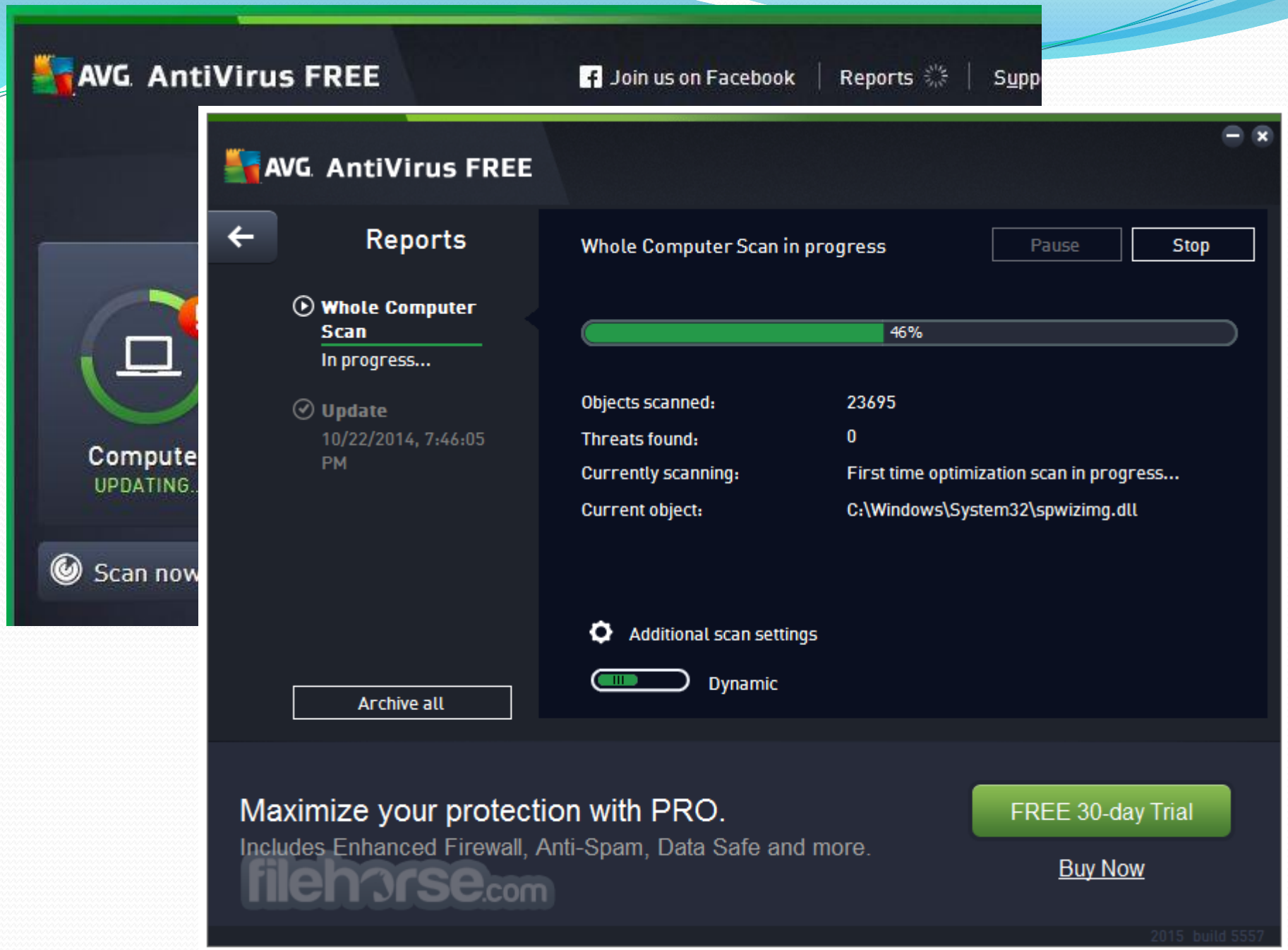
- Nod 32 je program čiji se tvorci ponose malim zauzećem memorije i neprimetnim uticajem na brzinu računara. Ima najbolju proaktivnu zaštitu, instalira se brzo i bez problema, a standardna podešavanja su mu prilagođena prosečnom korisniku, međutim podrazumevani pregled celog računara nije obuhvaćen automatski tako da ga sami morate izvršiti. Program je prilično brz, jer u jednom pregledu traži sve štetočine, i viruse i špijune, za razliku od drugih koji to rade u dva koraka.
- Cena mu je 40 dolara.


ESET NOD32 ANTIVIRUS 9
Home
Computer sc
Update
Tools
Setup
Help and sup
ENJOY SAFER TECHNO
Buy license
ESET NOD32 Antivirus
ESET NOD32 ANTIVIRUS 8
Home
Computer scan
Update
Setup
Tools
Help and suppo
About ESET NOD32 Antivirus
ESET NOD32 ANTIVIRUS 8
ESET NOD32 Antivirus™, Version 8.0.302.26
Copyright © 1992-2014 ESET, spol. s r.o. All rights reserved.
License valid until: 8/14/2024
License type: Not for resale license
Installed components:
Virus signature database: 9292 (20140115)
Rapid Response module: 3558 (20140115)
Update module: 1047 (20131023)
Antivirus and antispyware scanner module: 1418 (20140102)
Advanced heuristics module: 1146 (20131213)
Archive support module: 1187 (20131205)
Cleaner module: 1081 (20131127)
Windows 8.1 Pro (64-bit), Version 6.2.9200
Intel(R) Core(TM) i7-4470 CPU @ 3.20GHz (3200 MHz), 8087 MB RAM
Warning: This program is protected by copyright and international treaties. Copying or distribution without express permission from ESET, spol. s r.o. by any means, in part or in full, is strictly prohibited and will result in prosecution to the full extent that these laws will allow internationally.
OK

AVG

- Ovo je program čija je besplatna varijanta često vidljiva na računarima kod nas. Što se tiče plaćene verzije ona zauzima neku da kažemo sredinu među programima ovog tipa. Dobar je u odstranjivanju pretnji ali mu je proaktivna zaštita jako slaba, a ima i lošije radno okruženje. Cena paketa je 30 dolara.




AVG AntiVirus FREE
Join us on Facebook
Reports
Supp
Compute
UPDATING..
Scan now
AVG AntiVirus FREE
Reports
Whole Computer Scan
In progress...
Update
10/22/2014, 7:46:05 PM
Archive all
Whole Computer Scan in progress
Pause
Stop
46%
Objects scanned: 23695
Threats found: 0
Currently scanning: First time optimization scan in progress...
Current object: C:\Windows\System32\spwizimg.dll
Additional scan settings
Dynamic
Maximize your protection with PRO.
Includes Enhanced Firewall, Anti-Spam, Data Safe and more.
FREE 30-day Trial
Buy Now
filehorse.com
2015 build 5557

renosni uredjaji

- Paralelno sa razvojem razlicitih vrsta prenosnih uredjaja,razvili su se I virusi koji ih napadaju.Kao posledica ove pojave proizvodjaci antivirusnih softvera razvili su I softver prilagodjen ovim uredjajima.Kod ovih uredjaja cesce se pojavljuju hardverski bazirana resenja u vidu neke vrste ROM memorije,koja proverava sadrzaj na prenosnom uredjaju.

Najpouzdaniji antivirusi za mobilne telefone

- 1. **CM Mobile Security**
- 2. **AVG Mobile Security**
- 3. **Bitdefender Antivirus**
- 4. **Lookout Security and Antivirus**
- **5. Malwarebytes Anti-malware**

CM Mobile Security

- Konstantno se nalazi na vrhu liste najpopularnijih antivirus programa, besplatni antivirus kompanije *CM Security*. Njihova aplikacija **CM Mobile Security** je antivrius program koji koristi najmanje radne memorije i čija se baza definicija najčešće ažurira, što omogućava konstantnu zaštitu. Pored ovoga njihova aplikacija omogućava blokiranje neželjenih poziva i poruka, kao i uklanjanje nepotrebnih podataka u memoriji i sigurno pretraživanje


CM Security
11:59
AV-TEST's most frequent #1 app
Scan
Apps & System
Safe
System is protected
#1 Mobile Security
Light Fast Secure
#1 Antivirus engine inside
Completely Secure App Lock
Small, fast, and totally FREE

AVG Mobile Security

- AVG je kompanija poznata po besplatnim i pouzdanim antivrius programima zaWindows. Međutim, veoma brzo su postali i jedna od vodećih kompanija na Android platformi jer je njihov Android antivirus jedan od najpopularnijih i najkorištenijih anti vriusa za Android.
- AVG Mobile Security uživa veliko poverenje korisnika i do sada je preuzet više od 200 miliona puta!


3:51 PM
AVG AntiVirus PRO
Protection
Performance
Anti-Theft
Privacy
Last scan: Oct 14, 2012
Scan Now
5:29 PM
Performance
Task Killer
Close unused apps
Running apps: 44
Free memory: 244MB
Battery Consumption
Optimize your battery usage
Status: Discharging
Level: 51%
Data Usage
Monitor your mobile data usage
Set data plan
Storage Usage
Manage your device storage usage
Free system space: 0.90GB
Free USB space: 10.18GB

ZAKLJUČAK

- U današnje vreme je gotovo nezamisliv rad na računaru bez zaštite od virusa koje možemo dobiti otvaranjem bilo koje stranice na internetu.
- Potrebno je imati dobre antivirusne programe!
- Potrebno je redovno obnavljati antivirusne programe jer svakog dana nastaju milijoni novih virusa!

Kraj!