HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Comodo antivirus

CCERT-PUBDOC-2007-05-191

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, **www.lss.hr -** laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Zbog velike količine zlonamjernih programa koji kruže Internetom, antivirusni programi postali su neophodni svakom korisniku kako Interneta, tako i računala općenito. S povećanom uporabom računalnih mreža raste i potreba za antivirusnom zaštitom, što dovodi do velike ponude antivirusnih programa. Velik dio njih zahtijeva plaćanje licenci, no postoje i neki proizvođači koji su voljni svoja rješenja ustupiti na korištenje bez ikakve naknade. Jedan od njih je i tvrtka Comodo koja između ostalih proizvoda nudi i antivirusni program.

Uvriježeno je mišljenje kako je razina zaštite koju nude besplatni antivirusni programi znatno niža od razine zaštite komercijalnih rješenja. Iako je to u većini slučajeva točno, ono što pružaju besplatni programi u određenim primjenama je sasvim dovoljno.

U ostatku dokumenta dan je kratak pregled mogućnosti i funkcionalnosti Comodo antivirusnog programa koji se s novom inačicom 2.0 pokušava nametnuti kao jedno od kvalitetnijih besplatnih antivirusnih rješenja za osobnu i poslovnu uporabu. Dokument nudi informacije vezane uz postupak instalacije, konfiguracije i korištenja programa, a cilj mu je uputiti potencijalnog korisnika i demonstrirati mu način rada ovog programa.

2. Općenito o antivirusnim alatima

Antivirusni alat sačinjen je od jednog ili više programa namijenjenih otkrivanju, onemogućavanju i eliminaciji računalnih virusa i drugih zlonamjerno napisanih programa. Djelovanje antivirusnih programa obično se temelji na dvije metode detekcije:

- ispitivanju i pregledavanju datoteka sa svrhom otkrivanja poznatih virusa prema definicijama koje se nalaze u rječniku virusnih definicija i
- identifikaciji sumnjivih aktivnosti svih aktivnih programa, pri čemu se promatraju aktivnosti na priključcima i sl.

Većina komercijalnih antivirusnih rješenja koristi obje navedene metode s naglaskom na postupak otkrivanja poznatih virusa prema rječniku virusnih definicija.

2.1. Metoda rječnika virusnih definicija

Kod ove metode antivirusni program prilikom pregleda datoteke uspoređuje njen sadržaj s unosima iz rječnika poznatih virusnih definicija. Ukoliko dio sadržaja datoteke odgovara nečem što je u rječniku definirano kao virus, antivirusni program poduzima jednu od sljedećih radnji:

- popravlja datoteku micanjem virusnog koda,
- stavlja datoteku u karantenu tako da ona postaje nedostupna ostalim programima na računalu i time sprječava daljnje širenje virusa ili
- briše zaraženu datoteku.

Kako bi ova metoda bila dugoročno uspješna, ona zahtijeva redovito obnavljanje rječnika virusnih definicija putem Interneta. Obnavljanje rječnika temelji se na detekciji novih virusa koju provodi proizvođač samostalno ili nad inficiranim datotekama dobivenim od korisnika.

Antivirusni programi temeljeni na ovoj metodi obično ispituju datoteke i programe u trenutku kad ih operativni sustav kreira, otvara/pokreće ili šalje/prima porukom elektroničke pošte. Na taj način antivirusni program može detektirati poznate viruse odmah nakon njihovog prijema ili aktivacije. Također administrator sustava može, prevencije radi, konfigurirati antivirusni program tako da radi periodička ispitivanja sustava i time osigurati još bolju razinu zaštite.

Iako se ovom metodom u određenim uvjetima može uspješno spriječiti širenje virusa, autori virusnih programa otišli su korak dalje pa su tako nastali takozvani „oligomorfni“, „ polimorfni“ i „metamorfni“ virusni programi. Oni enkriptiraju ili modificiraju dijelove vlastitog koda kako bi se maskirali i antivirusnim programima otežali detekciju pomoću virusnih definicija iz rječnika.

2.2. Metoda prepoznavanja sumnjivih aktivnosti

Kod ove metode ne pokušava se identificirati poznate viruse u datotekama već se prate aktivnosti svih programa na računalu. Ukoliko neki program pokušava upisivati podatke u neku izvršnu datoteku antivirusni program to može detektirati kao sumnjivu aktivnost, obavijestiti korisnika o tome i zahtijevati od njega odluku o daljnjim radnjama vezanim uz tu aktivnost.

U usporedbi s metodom rječnika virusnih definicija ova tehnika daje zaštitu i od novih, dosad nepoznatih virusa koji ne postoje u rječnicima virusnih definicija. Međutim, ona može dovesti i do velikog broja lažnih upozorenja koja će nakon nekog vremena umanjiti korisnikovu osjetljivost, tj. korisnik će na svako upozorenje reagirati odobrenjem čime antivirusni program gubi svoju svrhu. Problem je postao još izraženiji u novije vrijeme s povećanom pojavom legalnih programa koji u toku svog rada izmjenjuju izvršne datoteke.

2.3. Druge metode

Neki antivirusni programi koriste tzv. heurističke metode detekcije poput emuliranja izvršavanja koda svake izvršne datoteke prije njenog pokretanja. Ako antivirusni program u tijeku emulacije detektira pokušaj automodifikacije programskog koda ili na neki drugi raspozna virusno djelovanje (npr. aplikacija neposredno nakon pokretanja pokušava naći druge izvršne datoteke), može se pretpostaviti da je taj program zaražen virusom i indicirati to korisniku. Međutim, i ova metoda može rezultirati velikim brojem lažnih upozorenja.

Osim spomenutih, postoji i metoda temeljena na uporabi tzv. pješčanika (eng. *Sandbox*) koji imitira operativni sustav u kome se pokreću izvršne datoteke. Nakon što je datoteka izvršena antivirusni program analizira pješčanik u potrazi za bilo kakvim promjenama koje bi mogle indicirati virusnu prirodu izvršenog programa. Zbog znatnog utjecaja na performanse ova metoda se uglavnom koristi samo kod antivirusnih pretraga iniciranih na zahtjev korisnika. Ona može biti vrlo neuspješna u detekciji zbog nedeterminističkog ponašanja virusnih programa (različito djelovanje kod uzastopnih izvršavanja ili izostanak bilo kakvog djelovanja). Za pouzdanu detekciju potrebno je virus pokrenuti nekoliko puta.

Alternativa metodi rječnika je tzv. metoda bijelih lista (eng. *whitelisting*) gdje se umjesto detektiranja poznatih virusnih programa sprječava izvršavanje svih programa osim onih koji su prethodno označeni kao provjereni. Ovakvim pristupom riješen je problem potrebe za stalnim obnavljanjem rječnika virusnih definicija, a istovremeno se sprječava izvršavanje bilo kakvih nepoželjnih programa koje, budući da nisu na bijeloj listi, nije odobrio administrator. Budući da velike organizacije koriste velik broj službeno odobrenih programa, korisnost ove metode antivirusne zaštite uvelike ovisi o administratorovoj umješnosti vođenja i održavanja liste odobrenih programa. Shodno tome, uz implementacije ovog postupka zaštite, pojavili su se alati za održavanje i automatizaciju aplikacijskih inventara i bijelih lista.

3. Comodo antivirus (CAV)

U ovom poglavlju pregledno je opisan Comodo antivirus program inačice Beta 2.0.

3.1. Opće informacije

Comodo antivirus jedan je u nizu proizvoda tvrtke Comodo. Detaljnije informacije o samoj tvrtci kao i o antivirusnom programu dostupne su na web stranicama:

- http://www.comodo.com/ i
- http://www.antivirus.comodo.com/ .

Ostali proizvodi Comodo tvrtke su vatrozidne aplikacije, digitalni certifikati za poruke elektroničke pošte, sigurnosni pregledi poslužitelja i upravitelji zaporkama. Važno je spomenuti da su svi navedeni proizvodi besplatni u svojim temeljnim inačicama, a vatrozid čak i u profesionalnoj inačici. Razlog naizgled opasnom tržišnom pothvatu leži u komercijalnoj politici koju koristi tvrtka. Ideja im je razviti potpuna sigurnosna rješenja za osobna računala i na taj način steći ugled na tržištu. To je zapravo radikalan način reklamiranja od kojeg krajnji korisnici imaju koristi. Tvrtka ostvaruje zaradu prodajom digitalnih sigurnosnih potvrda (eng. *digital certificate*) drugim tvrtkama.

3.2. Svojstva Comodo antivirusnog programa

Comodo antivirus inačica Beta 2.0 je, prema riječima proizvođača, besplatan antivirusni program koji osigurava sve funkcionalnosti konkurentnih komercijalnih proizvoda. Program podržava sljedeće funkcionalnosti:

- pregled svih datoteka prilikom pristupa u stvarnom vremenu,
- pregled datoteka na zahtjev korisnika,
- organizaciju periodičkih pregleda sustava,
- izoliranje zaraženih datoteka,
- sprječavanje instalacije i pokretanja *malware* i *spyware* programa,
- zaštitu od nepoznatih virusa heurističkim metodama detekcije,
- provjeru integriteta datoteka,
- kreiranje vlastite bijele liste,
- automatsko redovno osvježavanje baza poznatih virusnih definicija,
- inteligentne metode pregleda i pretraživanja za ubrzavanje detekcije virusa,
- automatski pregled svih poslanih i primljenih poruka te automatsko uklanjanje detektiranih virusa,
- pregled vanjskih perifernih uređaja kao što su vanjski diskovi, CD diskovi, DVD diskovi, USB uređaji, kamere, i sl.,

- pregled mrežnih resursa,
- pregled komprimiranih datoteka,
- automatski permanentni nadzor radne memorije,
- automatsku zaštitu od pokušaja masovnog slanja e-mail poruka,
- pohranjivanje svih zapisa o pregledima i aktivnostima ,
- slanje detektiranih virusa na analizu Comodo ekspertnom timu i
- lagan pristup svim funkcijama i postavkama programa.

Comodo antivirus inačica Beta 2.0 je aplikacija namijenjena sljedećim inačicama Windows operacijskih sustava:

- Windows XP Home,
- Windows XP Professional (Service Pack 1 ili kasniji) i
- Windows 2000 Professional (Service Pack 4 ili kasniji).

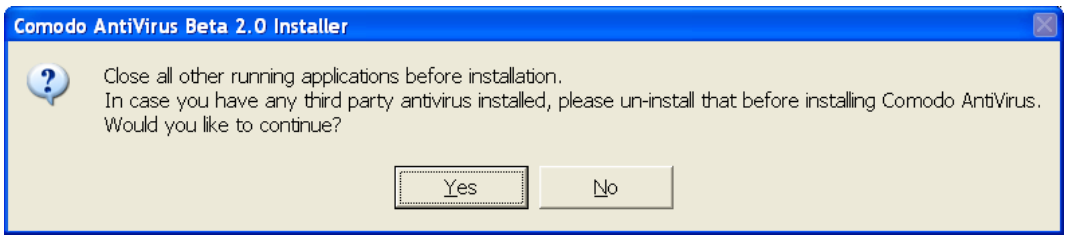
Ima slijedeće zahtjeve za resursima:

- 128MB radne memorije (eng. *RAM – Random Access Memory*),
- 50MB slobodnog mjesta na disku i
- Intel Pentium 300 MHz (ili ekvivalentan) procesor.

Svi korisnici čija računala zadovoljavaju navedene specifikacije mogu započeti instalaciju paketa.

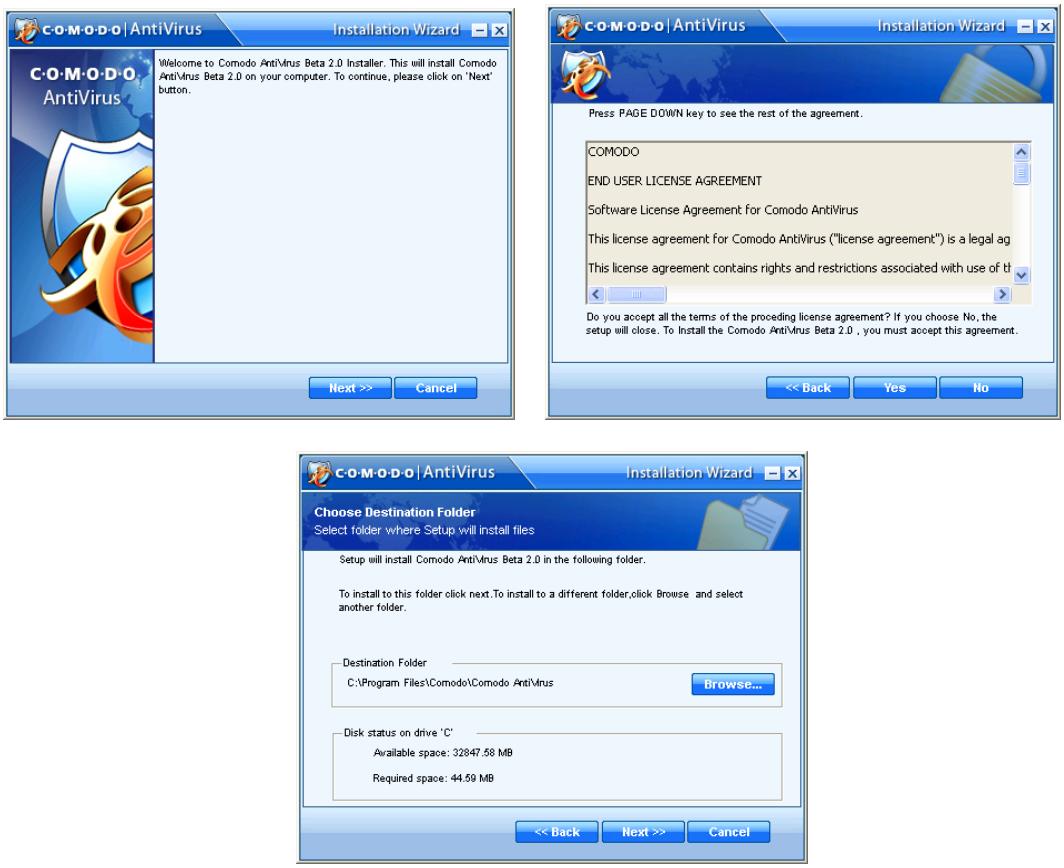
3.3. Preuzimanje i instalacija paketa

Odabirom poveznice *Download now* na web stranicama programa započinje postupak preuzimanja paketa. U trenutku pisanja ovog dokumenta najnovija inačica je Comodo AntiVirus Beta 2.0 veličine od oko 35MB. Paket se distribuira u obliku jedne izvršne instalacijske datoteke.
Instalacija započinje njenim pokretanjem. Na samom početku aplikacija korisnika obavještava o potrebi uklanjanja eventualno prisutnog drugog antivirusnog programa.
Upozorenje se nikako ne bi smjelo zanemariti jer su kolizije između različitih antivirusnih programa vrlo česte, a postoje i potvrđeni problemi nastali instalacijom Comodo antivirusa u takvim uvjetima.



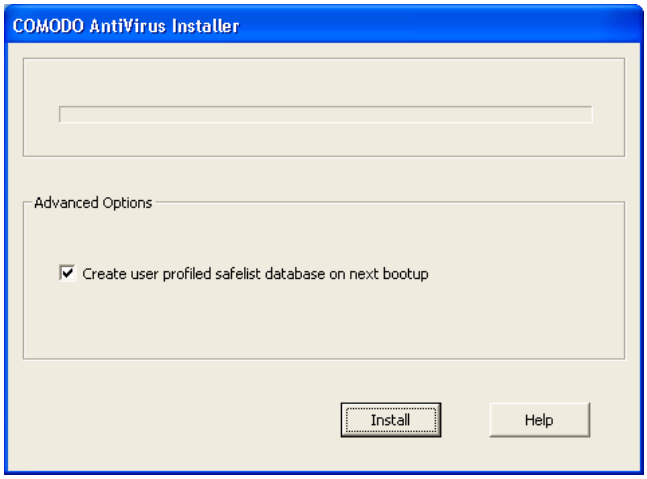
Tablica 1. Upozorenje prije instalacije Comodo antivirusa

Ostatak instalacijske procedure je jednak kod većine programskih paketa pa se ovdje neće posebno opisivati nego samo prikazati na slijedećoj slici.



Tablica 2. Postupak instalacije

Dodatak uobičajenom postupku instalacije je opcija za kreiranje liste sigurnih aplikacija kod prvog pokretanja antivirusa prikazana na slici 3.



Tablica 3. Opcija za kreiranje liste sigurnih aplikacija

Lista sigurnih aplikacija vezana je uz HIPS (eng. *Host Intrusion Prevention System*) funkcionalnost Comodo antivirusa koja omogućava detekciju neovlaštenog pokretanja izvršnih datoteka. Više informacija o toj funkcionalnosti i primjeni liste sigurnih aplikacija može se pronaći u poglavlju 3.5.4.
Slijedi izvedba postupka vezanog uz registraciju antivirusa. Od korisnika se traži opcionalno upisivanje ispravne adrese elektroničke pošte te uključivanje ili isključivanje mogućnosti primanja obavijesti vezanih uz paket.
Kako bi instalacija bila potpuna potrebno je ponovno pokrenuti sustav, nakon čega se, zbog odabrane opcije za vrijeme instalacije, pokreće postupak kreiranja liste sigurnih aplikacija.

Time je završena instalacija Comodo antivirus programa koji se nakon instalacije automatski pokreće sa uobičajenim postavkama. Korisničko sučelje kao i konfiguracija standardnih i naprednih postavki opisani su u sljedećim poglavljima.
Potrebno je naglasiti da će Comodo antivirus odmah po pokretanju u pozadini pokrenuti proceduru za osvježavanje rječnika virusnih definicija. Ukoliko je računalo povezano na Internet, rječnik će biti uspješno ažuriran.

3.4. Korisničko sučelje Comodo antivirusa

Nakon instalacije Comodo dodaje indikator u tzv. sustavsku ladicu (eng. *system tray*). Isto tako, dodaje se i kratica (eng. *shortcut*) na radnu površinu (eng. *desktop*) kao i zapis u *All Programs* izborniku. Korisničko sučelje prikazano je na slijedećoj slici, a može se pokrenuti odabirom jedne od pobrojenih pristupnih točaka.

Tablica 4. Korisničko sučelje Comodo antivirusa

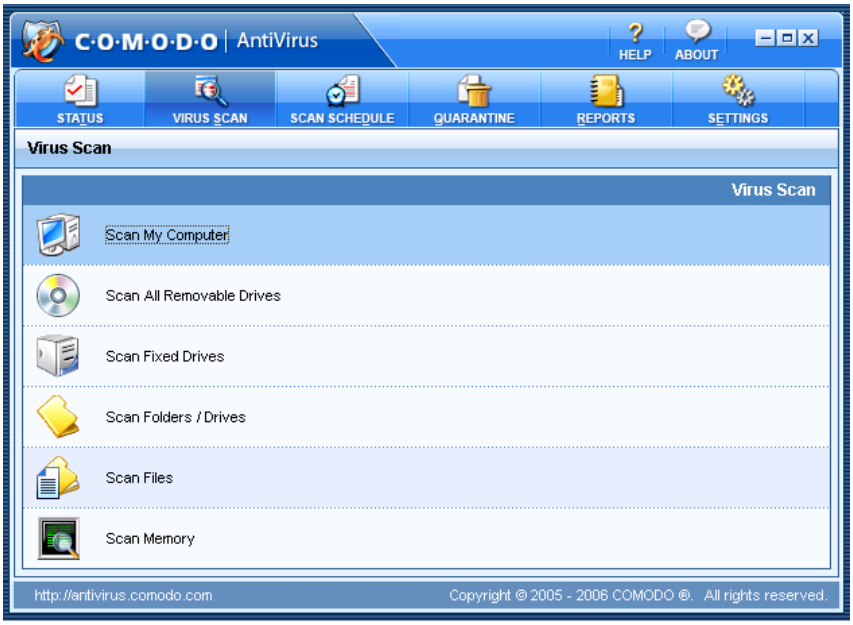
Ono, osim što omogućava pristup svim funkcionalnostima Comodo antivirusa, prilikom otvaranja nudi i cjelovit pregled statusa programa i njegovih sigurnosnih postavki. Dostupne su slijedeće informacije:

- Status pojedinih sigurnosnih komponenti programa s mogućnošću njihovog uključivanja i isključivanja:
  - *On Access Scanner* – komponenta koja osigurava zaštitu u stvarnom vremenu provjerom datoteka prilikom njihovog kreiranja, otvaranja ili kopiranja.
  - *Email Scanner* – komponenta koja osigurava zaštitu od virusa primljenih putem poruka elektroničke pošte. Komponenta također provjerava odlazne poruke elektroničke pošte te sprječava njihovu masovnu distribuciju iniciranu aplikacijom crvom (eng. *worm*).
  - *HIPS Application Control* – komponenta koja osigurava zaštitu od neovlaštenog pokretanja aplikacija.
  - *Automatic Updater* – komponenta koja osigurava automatsko osvježavanje rječnika virusnih definicija.
- Informacija o zadnjem obavljenom pregledu sustava. Ovdje je moguće pokrenuti novi pregled sustava.
- Informacija o trenutnoj inačici rječnika virusnih definicija. Eksplicitnim zahtjevom korisnika riječnik se može osvježiti u proizvoljnom trenutku.
- Informacija o statusu licence za korištenje.

Korisničko sučelje dodatno omogućava pristup i izbornicima opisanim u sljedećim poglavljima.

3.4.1. Izbornik *Virus Scan*

Izbornik omogućava pokretanje pregleda cijelog sustava ili nekog njegovog eksternog ili internog dijela. Prikazan je na sljedećoj slici.

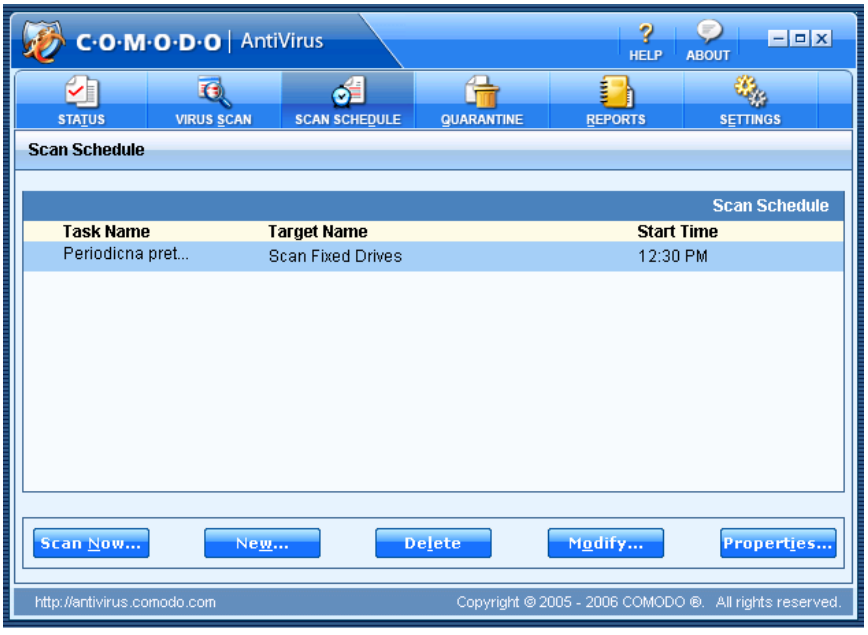


Tablica 5. Izbornik *Virus Scan*

Nakon odabira jedne od opcija pokreće se pregled odabranog dijela sustava.

3.4.2. Izbornik *Scan Schedule*

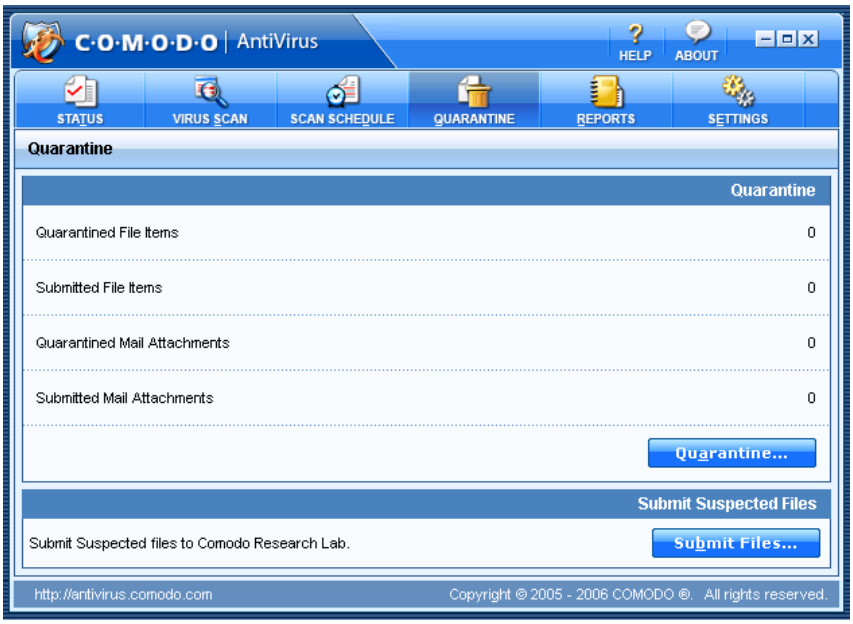
Izbornik *Scan Schedule* omogućava konfiguraciju periodičkih ili pojedinačnih pregleda sustava u određeno vrijeme. Prikazan je na slici 6.



Tablica 6. Izbornik *Scan Schedule*

3.4.3. Izbornik *Quarantine*

Izbornik *Quarantine* daje pregled datoteka stavljenih u izolaciju tijekom prijašnjih pregleda sustava. Prikazan je na slijedećoj slici , na kojoj je uočljiv kratak izvještaj o broju i vrstama datoteka u izolaciji, dok se detaljan pregled sadržaja karantene može dobiti odabirom opcije *Quarantine...* .



Tablica 7. Izbornik *Quarantine*

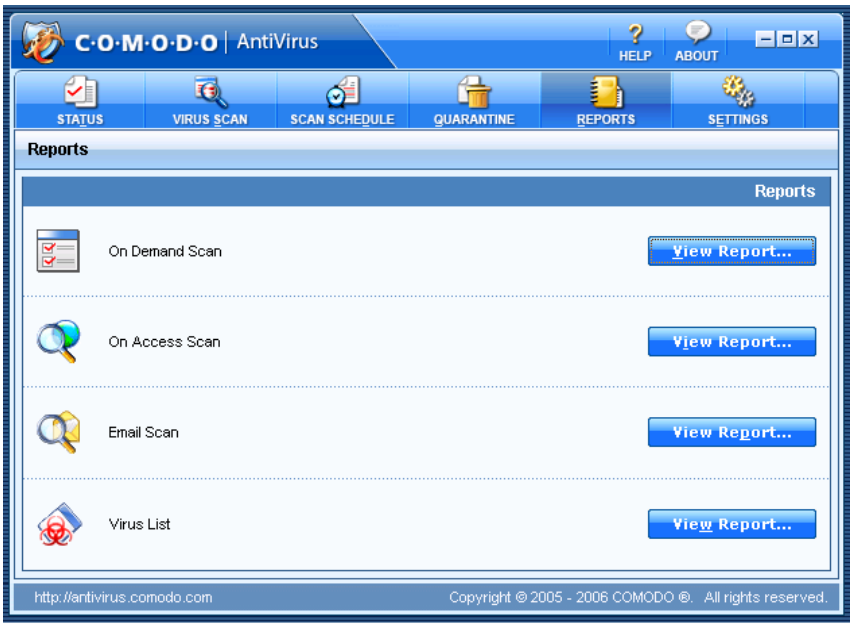
Potrebno je spomenuti i dodatnu funkcionalnost izbornika koja korisniku omogućava slanje sumljive datoteke na analizu ekspertima u tvrtki Comodo. Slanje je vrlo jednostavno, a Comodo se obvezuje poslati rezultat provedene analize na adresu elektroničke pošte unesenu prilikom slanja datoteke.

3.4.4. Izbornik *Reports*

Izbornik *Reports* (Tablica 8) daje korisniku uvid u izvještaje svih dosad učinjenih pregleda sustava koji su radi lakšeg snalaženja podijeljeni u 3 kategorije:

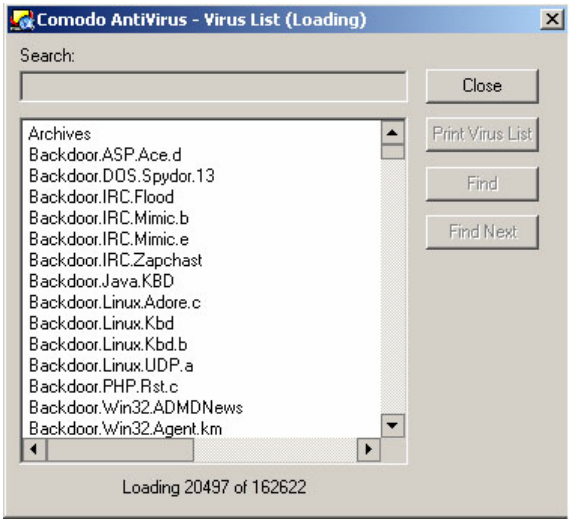
- *On Demand Scan* - pregledi na zahtjev korisnika,
- *On Access Scan* – pregledi prilikom pristupa datoteci te
- *Email Scan* – pregled e-mail poruka.

Osim pregleda izvještaja izbornik omogućava i pregled liste svih virusa sadržanih u trenutnoj inačici rječnika virusnih definicija.



Tablica 8. Izbornik *Reports*

On Demand Scan kategorija sadrži potpune izvještaje svih dosad provedenih pregleda na zahtjev korisnika.
On Access Scan kategorija sadrži podatke o svim zaraženim datotekama koje su otkrivene prilikom pokušaja ostvarivanja pristupa.
Email Scan kategorija sadrži listu svih otkrivenih zaraženih e-mail poruka.
Primjer pregleda liste virusnih definicija prikazan je na slici 9.



Tablica 9. Pregled liste virusnih definicija

3.5. Konfiguracija Comodo antivirusa

Comodo antivirusa može se konfigurirati uporabom korisničkog sučelja putem izbornika *Settings* prikazanog na slijedećoj slici.

Tablica 10. Izbornik *Settings*

Konfiguracija Comodo antivirusa podijeljena je prema funkcionalnostima objašnjenim u sljedećim poglavljima.

3.5.1. *On Demand Scan*

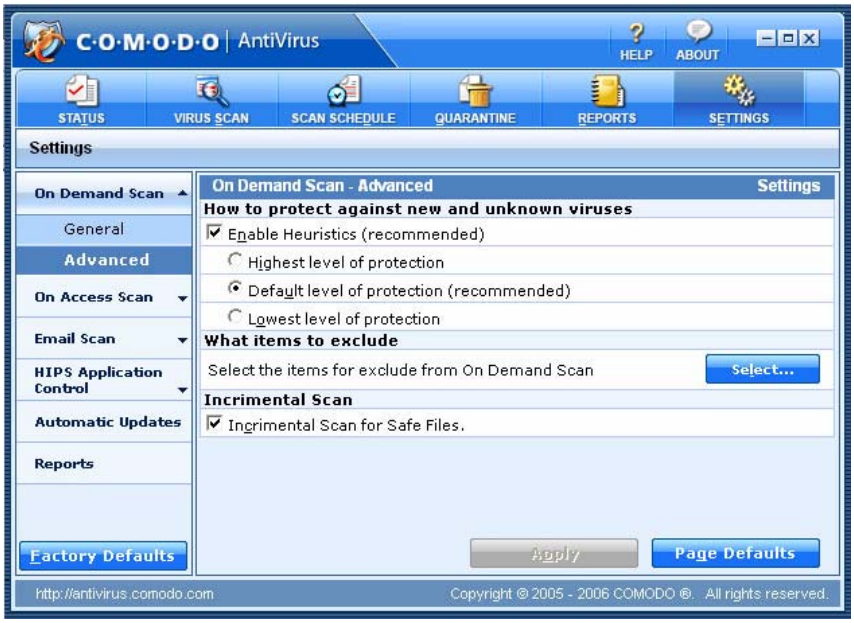
Konfiguracija pregleda na zahtjev korisnika dijeli se u dvije kategorije: opću (eng. *General*) i naprednu. (eng. *Advanced*).
Opća konfiguracija (Tablica 11) sadrži sljedeće postavke:

- Pregled datoteka učitanih u radnu memoriju (uz pregled datoteka na disku) – ako je učitana datoteka zaražena Comodo antivirus će prekinuti proces vezan uz tu datoteku i ukloniti virus.
- Aktivnosti nakon otkrivanja virusa – korisnik može odabrati:
  - Automatsku dezinfekciju zaražene datoteke. Ukoliko dezinfekcija nije moguća program će automatski staviti zaraženu datoteku u karantenu.
  - Ručnu kontrolu aktivnosti nakon otkrivanja. Nakon otkrivanja virusa Comodo antivirus od korisnika zahtijeva donošenje odluke o daljnjim aktivnostima. Moguće je datoteku ručno dezinficirati, obrisati ili staviti u karantenu.
- Odabir datoteka koje će se pregledavati:
  - *All files* – pregled svih datoteka.
  - *Selective Extension* – pregled datoteka odabranih ekstenzija. Korisnik može ručno odabrati vrste datoteka koje želi pregledavati.
- Napredne opcije pregleda, gdje korisnik može uključiti:
  - Pregled komprimiranih datoteka i/ili
  - Pregled upakiranih datoteka (dinamičke biblioteke koje se raspakiravaju prilikom izvršavanja).

Tablica 11. Opća konfiguracija pregleda na zahtjev korisnika

Napredna konfiguracija pregleda na zahtjev korisnika (Tablica 12) sadrži sljedeće postavke:

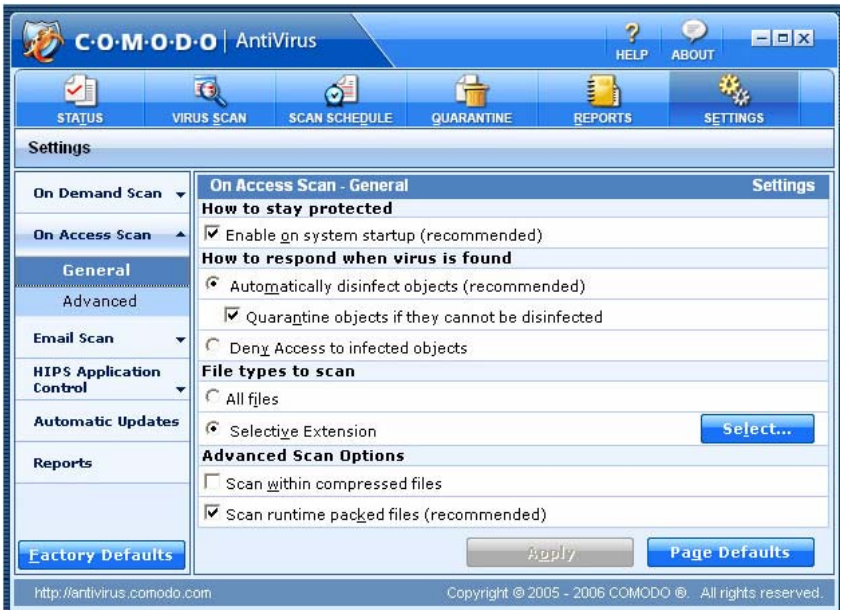
- Heuristička zaštita od novih i nepoznatih virusa – moguće odabrati jednu od tri razine zaštite:
  - visoku,
  - uobičajenu ili
  - nisku.
- Odabir datoteka koje nije potrebno pregledavati heurističkom metodom – korisnik može specificirati listu datoteka ili direktorija koje nije potrebno uključiti u ove preglede.
- Inkrementalni pregled datoteka sa liste sigurnih datoteka.



***Tablica* 12.** Napredne postavke pregleda na zahtjev korisnika

3.5.2. *On Access Scan*

Konfiguracija pregleda datoteka prilikom pristupa dijeli se također na dvije kategorije: opću (eng. *General*) i naprednu. (eng. *Advanced*).
Opća konfiguracija (Tablica 13) sadrži identične postavke kao i *On Demand scan* s razlikom u postavci pregleda radne memorije, koja je ovdje zamijenjena s postavkom automatske aktivacije pregleda kod podizanja sustava. Za razliku od opće, napredna konfiguracije se ni u čemu ne razlikuje od one kod pregleda na zahtjev korisnika.



Tablica 13. Opće postavke pregleda prilikom pristupa datoteci

3.5.3. *Email Scan*

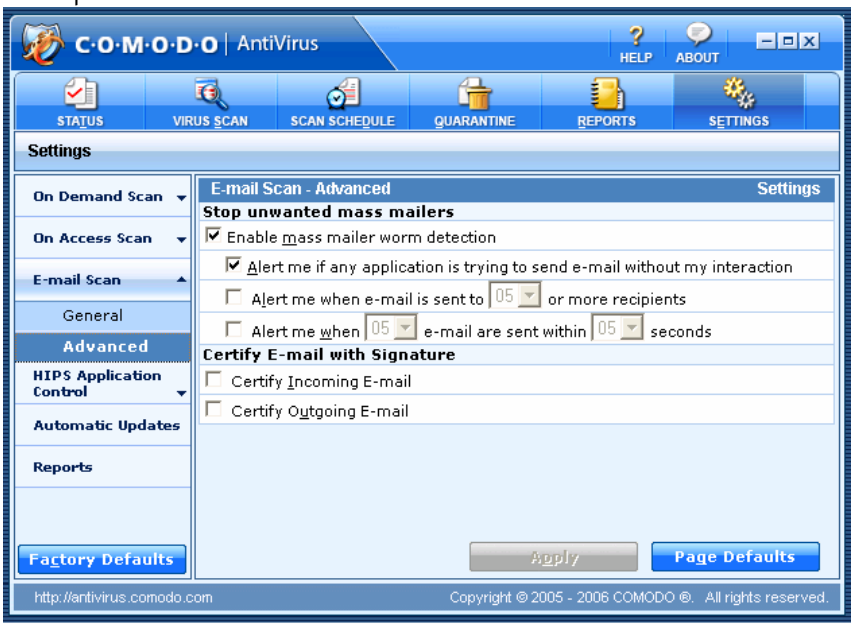
Konfiguracija pregleda poruka elektroničke pošte dijeli se također na dvije kategorije: opću (eng. *General*) i naprednu. (eng. *Advanced*).
Opća konfiguracija (Tablica 14) sadrži slijedeće postavke:

- Pregled dolaznih poruka.
- Pregled odlaznih poruka.
- Aktivnosti nakon otkrivanja virusa. Ovdje korisnik može odabrati:
  - automatsku dezinfekciju zaražene datoteke u prilogu e-mail poruke ili
  - ručnu kontrolu aktivnosti nakon otkrivanja, pri čemu Comodo nakon otkrivanja virusa od korisnika zahtijeva donošenje odluke o daljnjim aktivnostima.
- Postavke prikaza prilikom pregleda poruka. Grupa sadrži slijedeće opcije:
  - prikaz animacije prilikom pregleda dolaznih poruka i
  - prikaz indikatora napretka prilikom pregleda odlaznih poruka.

Tablica 14. Opće postavke pregleda e-mail poruka

Napredna konfiguracija pregleda e-mail poruka (Tablica 15) sadrži sljedeće postavke:

- Detekcija masovnog slanja e-mail poruka uzrokovanog crv (eng. *worm*) programima . Ovdje se može definirati što će se i u kojoj mjeri provjeravati, a nude se slijedeće stavke:
  - prikaz upozorenja ukoliko neka aplikacija pokušava poslati poruku elektroničke pošte bez znanja korisnika,
  - prikaz upozorenja ako se poruka elektroničke pošte pokušava poslati prema većem broju korisnika te
  - prikaz upozorenje ako se uzastopno pokušava slati poruke elektroničke pošte.
- Certificiranje poruka elektroničke pošte koje može uključivati certificiranje dolaznih i/ili odlaznih poruka.



Tablica 15. Napredne postavke pregleda e-mail poruka

3.5.4. HIPS konfiguracija

HIPS (eng. *Host Intrusion Prevention System*) je funkcionalnost Comodo antivirusa koja provodi kontrolu neovlaštenog pokretanja aplikacija s ciljem sprečavanja pokretanja zlonamjerno oblikovanih programa. HIPS kontrola temelji se na listi sigurnih aplikacija, tj. listi sigurnih izvršnih datoteka koja je kreirana prilikom instalacije Comodo antivirusa u sklopu procesa profiliranja računala. Ukoliko lista nije kreirana prilikom instalacije Comodo antivirus će za HIPS provjeru koristiti svoju standardnu listu. Budući da je ta lista znatno veća od one koja nastaje profiliranjem korisničkog računala, bitno je primijetiti kako će u tom slučaju HIPS provjere će biti nešto sporije. Ako lista nije kreirana prilikom instalacije programa, bit će kreirana naknadno prilikom pokretanja pregleda računala, na zahtjev korisnika ili prilikom pokretanja pregleda za vrijeme pristupa datoteci.
Kreirana lista sadrži popis svih aplikacija i izvršnih datoteka koje se smatraju sigurnima i o čijem pokretanju korisnik neće biti obavještavan. Za sve ostale izvršne datoteke Comodo antivirus će prilikom pokretanja prikazati upozorenje korisniku i od njega tražiti odluku o daljnjim akcijama.
Konfiguracija HIPS kontrole također je dostupna unutar izbornika za izmjenu postavki Comodo antivirusa i podijeljena je u dvije skupine: opću (eng. *General*) i naprednu. (eng. *Advanced*).
Opća konfiguracija (Tablica 16) sadrži slijedeće postavke:

- uključivanje HIPS kontrole,
- odabir razine zaštite,
- administraciju liste dozvoljenih/nedozvoljenih aplikacija,
- odabir datoteka/aplikacija koje HIPS neće kontrolirati (moguće odabrati i direktorij u kojem se nalazi više aplikacija) i
- postavku automatskog slanje datoteka na analizu ekspertima tvrtke Comodo.

Tablica 16. Opće postavke HIPS kontrole

Tablica 17. Napredne postavke HIPS kontrole

Napredna HIPS konfiguracija (Tablica 17) sadrži sljedeće postavke:

- postavku prikaza upozorenja kod blokiranja aplikacije,
- postavku prikaza upozorenja kod propuštanja aplikacije i
- postavku automatske provjere u listi na Comodo poslužitelju ukoliko aplikacija nije navedena u lokalnoj listi.

3.5.5. Ostale postavke

Osim opisanih postoje i postavke za automatsko osvježavanje rječnika virusnih definicija i administraciju izvještaja, ali one zbog intuitivnosti i jednostavnosti neće biti detaljnije opisane.

4. Testiranje

Budući da je Comodo antivirus još uvijek u probnoj fazi (beta inačica) nad njim nisu provedeni referentni testovi koji bi dali detaljan uvid u kvalitetu detekcije virusa. Međutim provedeni su testovi nad prethodnom inačicom programa koji su dali rezultate prikazane slijedećom tablicom:

Comodo 1.0.0.4						
Vrsta virusa	**Ukupno**	**Detektirano**	**Detektirano bez heuristike**	**Nije detektirano**	**Vrijeme (min)**	**Detekcija (%)**
File	**256**	24	24	232	1	**9,38%**
MS-DOS	**38851**	12987	12987	25864	3	**33,43%**
Windows	**1978**	1377	1377	601	1	**69,62%**
Macro	**7638**	1459	1459	6179	1	**19,10%**
Malware	**7769**	3529	3529	4240	4	**45,42%**
Script	**10003**	4370	4370	5633	3	**43,69%**
Trojan - Backdoor	**80689**	36633	36633	44056	43	**45,40%**
Ukupno	**147184**	60379	60379	86805	56	**41,02%**

Tablica 18. Rezultati referentnog testiranja Comodo antivirusa inačice 1.0.0.4

Rezultati pokazuju relativno slabu efikasnost mehanizmima detekcije virusa kako metodom rječnika virusnih definicija tako i heurističkim metodama. Prema inicijalnim komentarima beta test korisnika

inačica 2.0 sadrži značajna poboljšanja u odnosu na testiranu inačicu, ali nepostojanje referentnih usporednih testova ovim komentarima odriče objektivan značaj.
Što se tiče ostalih parametara kvalitete antivirusnog programa za inačicu Comodo antivirusa Beta 2.0 mogu se ocijeniti:

- funkcionalnost,
- kvaliteta korisničkog sučelja,
- jednostavnost korištenja i
- zauzeće resursa.

4.1. Funkcionalnost

Kao što je već spomenuto u poglavlju 3.1 Comodo antivirus sadrži sve standardne funkcionalnosti antivirusnih programa. Od dodatnih funkcionalnosti tu je zaštita od *Malware* i *Spyware* programa. Ona se ostvaruje indirektno pomoću HIPS kontrole koja sprečava instaliranje i pokretanje *Malware* i *Spyware* aplikacija .
Iako se može reći da HIPS kontrola sprječava pokretanje i instalaciju takvih programa, ne može se potvrditi da će Comodo antivirus otkriti *Spyware* programe koji su pasivni, tj. one koji se nalaze u tzv. inventarnim (eng. *Registry*) zapisima računala. S druge strane HIPS kontrola je funkcionalnost koju većina ostalih antivirusnih programa ne posjeduje pa će se tek nakon nekog vremena njenog korištenja moći reći da li i u kojoj mjeri ona predstavlja komparativnu prednost, a koliko reklamnu funkcionalnost bez stvarne svrhe.
Druga, dijelom nestandardna, funkcionalnost je slanje zaraženih ili sumnjivih datoteka na analizu ekspertima u tvrtko Comodo. Može se reći da je funkcionalnost sveprisutna i dostupna korisniku na svakom koraku što će vjerojatno doprinijeti broju korisnika koji će je stvarno koristiti. Stvarna kvaliteta ove funkcionalnosti moći će ipak biti ocijenjena tek kad se utvrdi kvaliteta ekspertnog tima tvrtke Comodo, tj. kvaliteta i brzina odgovora na poslane korisničke dojave i upite.

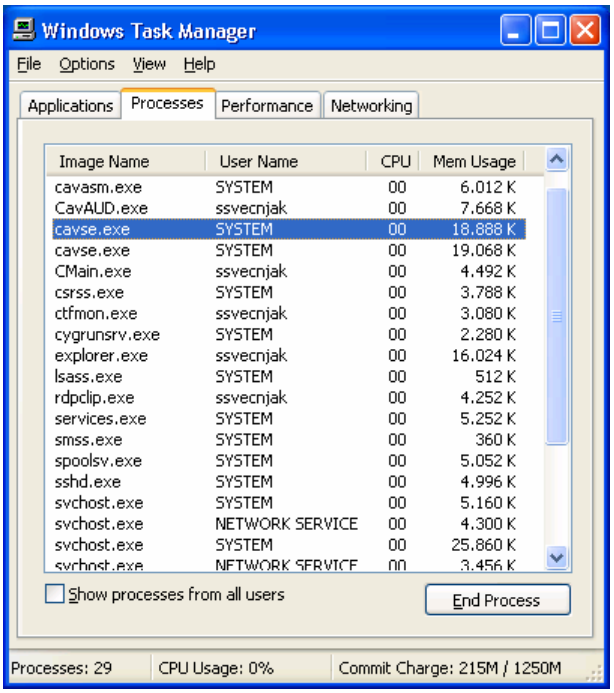
4.2. Kvaliteta korisničkog sučelja

Nakon pregleda sučelja i njegovog korištenja može se zaključiti da se ono svojim kvalitetama ne razlikuje bitno od konkurencije te da zadovoljava sve potrebe korisnika. Ono je intuitivno i dobro organizirano, upozorenja koja se pojavljuju osiguravaju dovoljnu količinu informacija i ne predstavljaju smetnju u radu niti zbunjuju korisnika, dok su izvještaji pregledni i koncizni.

4.3. Zauzeće resursa

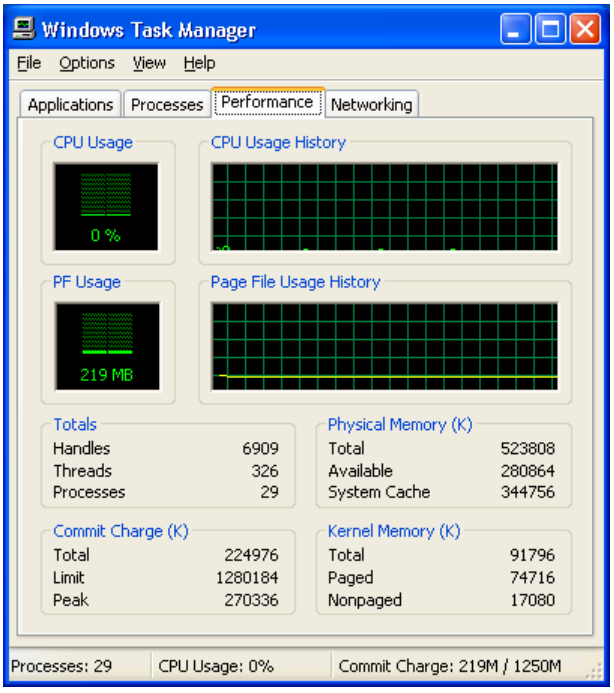
Comodo antivirus nije zahtjevan što se tiče sustavskih resursa. Za vrijeme pasivnog korištenja aktivirano je pet procesa (Tablica 19):

- cavasm.exe,
- CavAUD.exe,
- Cavse.exe (2 instance) i
- CMain.exe.



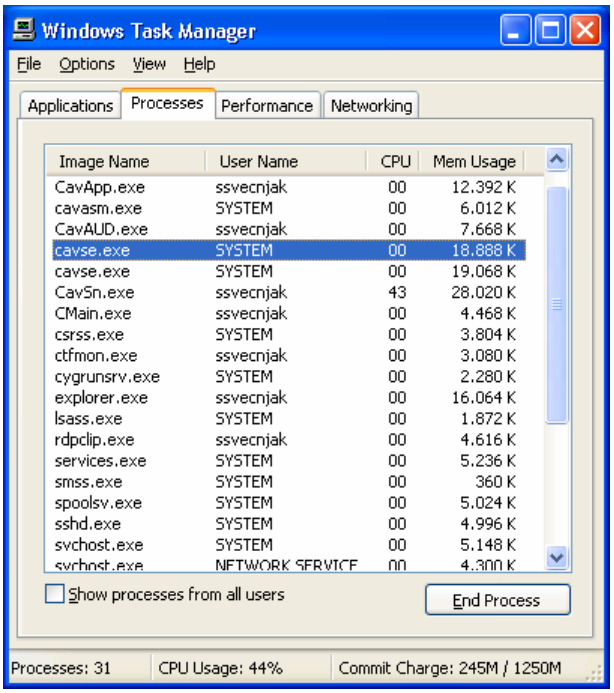
Tablica 19. Procesi Comodo antivirusa u pasivnom načinu rada

Svih pet procesa zajedno zauzimaju otprilike deklariranu količinu radne memorije (oko 50 MB) što ne predstavlja značajno opterećenje za današnju uobičajenu računalnu konfiguraciju. Osim toga, ni procesi ne predstavljaju znatno opterećenje za procesor pa se može reći da u pasivnom načinu rada Comodo ne utječe na opće performanse sustava (Tablica 20).



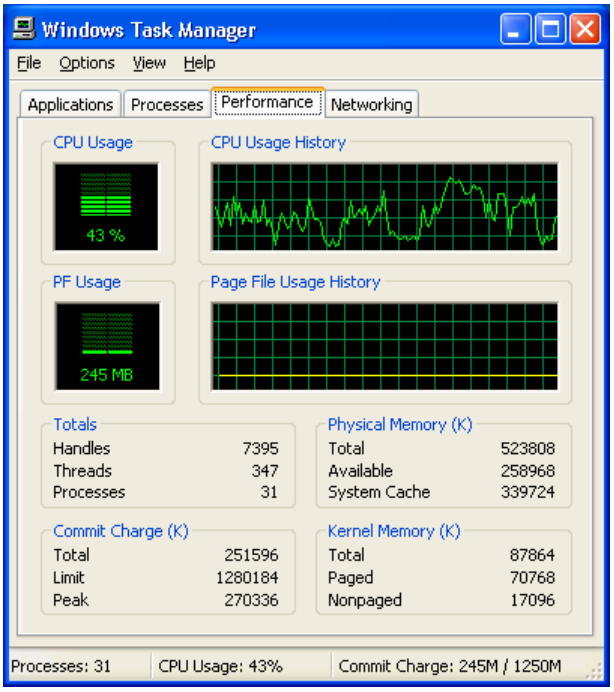
Tablica 20. Opterećenje resursa Comodo antivirusa u pasivnom načinu rada

Kod pregleda sustava pokreću se dva dodatna procesa CavApp.exe i CavSn.exe pa ukupno zauzeće memorije raste na cca 100 MB (Tablica 21).



Tablica 21. Procesi Comodo antivirusa u aktivnom načinu rada (pregled u tijeku)

Osim većeg zauzeća memorije, raste i opterećenje procesora koje varira između 20% i 60% (Tablica 22), što je u usporedbi s ostalim antivirusnim programima također uobičajena vrijednost. Krajnja ocjena zauzeća resursa je zadovoljavajuća jer je u pasivnom načinu rada Comodo antivirus gotovo neprimjetan, dok u aktivnom načinu rada ne predstavlja ništa veću smetnju od većine ostalih antivirusnih alata.



Tablica 22. Opterećenje računala u aktivnom načinu rada Comodo antivirusa (pregled u tijeku)

5. Konkurentske aplikacije

U odnosu na konkurenciju Comodo antivirus se može promatrati s dva gledišta – u konkurenciji svih antivirusnih programa i u konkurenciji besplatnih programa. Usporedbu na osnovu referentnih testova nije moguće donijeti jer objektivni testovi za trenutnu inačicu Comodo antivirusa (2.0) ne postoje. Ako se zaključak donosi na temelju rezultata testova prethodne inačice (Comodo antivirus 1.0.0.4) nova inačica antivirusa zahtijeva dosta poboljšanja kako bi održala korak s konkurencijom. Prema rezultatima slijedeće liste Comodo antivirus inačica 1.0.0.4 stoji vrlo loše s ukupnim postotkom detekcije virusa od 41,02 %.

1. Kaspersky version 6.0.0.303 - 99.62%
2. Active Virus Shield by AOL version 6.0.0.299 - 99.62%
3. F-Secure 2006 version 6.12.90 - 96.86%
4. BitDefender Professional version 9 - 96.63%
5. CyberScrub version 1.0 - 95.98%
6. eScan version 8.0.671.1 - 95.82%
7. BitDefender freeware version 8.0.202 - 95.57%
8. BullGuard version 6.1 - 95.57%
9. AntiVir Premium version 7.01.01.02 - 95.45%
10. Nod32 version 2.51.30 - 95.14%

...

46. Comodo version 1.0.0.4 - 41.02%

...

58. Abacre version 1.4 - 0.00%

Tablica 23. Usporedni test antivirusnih programa prema postotku detekcije virusa – ukupan poredak prema rezultatima testiranja iz svibnja 2006. (izvor - Antivirus programs and guides - [4])

Ako se iz rezultata uzmu u obzir samo besplatni antivirusni programi situacija je još lošija jer je Comodo antivirus inačice 1.0.0.4 (koja u vrijeme testiranja nije bila besplatna) na posljednjem mjestu.

1. Active Virus Shield by AOL version 6.0.0.299 - 99.62%

...

9. **Comodo version 1.0.0.4 - 41.02%**

Tablica 24. Usporedni test antivirusnih programa prema postotku detekcije virusa – poredak besplatnih programa

Iz ovog bi se dalo zaključiti da je Comodo krenuo u osvajanje antivirusnog tržišta prilično skromno te da će tek ova inačica pokazati koliko su eksperti tvrtke Comodo uspjeli uhvatiti korak s konkurencijom.

6. Zaključak

Comodo antivirus inačica 2.0 na prvi pogled izgleda kao velik napredak za tvrtku – velik izbor funkcionalnosti, uljepšano korisničko sučelje i prelazak na besplatnu distribuciju očito pokazuju da je tvrtka Comodo odlučila uložiti više truda u svoj antivirusni proizvod. Budući da je tvrtka već stekla zavidnu reputaciju na tržištu svojim vatrozidnim proizvodom (koji je također besplatan) pretpostavlja se da će s prelaskom na besplatnu distribuciju i antivirusni program dobiti na kvaliteti jer bi u suprotnom predstavljao vrlo negativnu reklamu za tvrtku i mogao negativno utjecati na reputaciju ostalih proizvoda tvrtke Comodo.

Ako je suditi samo prema sučelju i funkcionalnostima Comodo antivirus stoji uz bok ostalim besplatnim antivirusnim alatima, a na nekim poljima je čak i u prednosti (HIPS kontrola, slanje datoteka na analizu). Ako će do izdavanja službene inačice Comodo stručnjaci raditi na algoritmima za detekciju virusa i značajno ih poboljšati službena inačica mogla bi postati jedan od kvalitetnijih proizvoda besplatne distribucije. Budući da Comodo licenca dozvoljava korištenje antivirusnog programa i u poslovne svrhe također bez naknade i manji poslovni korisnici bi mogli biti zainteresirani. Ipak, krajnja ocjena ovog programa moći će se dati tek kad postanu dostupni prvi rezultati referentnog testiranja službene inačice.

7. Reference

[1] Službena stranica Comodo antivirus aplikacije http://www.anitivirus.comodo.com, svibanj 2007.

[2] Comodo forum http://forums.comodo.com, svibanj 2007.

[3] Comodo AntiVirus Review http://mbalat.blogspot.com/2006/07/comodo-antivirus-review.html, svibanj 2007.

[4] Antivirus programs and guides http://www.virus.gr/english/fullxml/default.asp?id=82&mnu=82,, svibanj 2007.

[5] Comodo User Manual – upute za korisnike distribuirane zajedno s inačicom 2.0

[6] Antivirus software http://en.wikipedia.org/wiki/Anti-virus_software , svibanj 2007.