COMODO antivírus telepítése és beállítása

COLLABORATORS

	TITLE : COMODO antivírus telepítése és beállítása	

ACTION	*NAME*	*DATE*	*SIGNATURE*
WRITTEN BY	Molnár, Tamás és Hazai, Géza	2014. február 12.	

REVISION HISTORY			
NUMBER	DATE	DESCRIPTION	NAME
1.0	2014.01.15	Az eredeti cikk	Tomi37
1.1	2014.02.12	Magyarázatok hozzáfűzése néhány ponthoz.	janu

Tartalomjegyzék

1. Bevezetés

Közismert tévhit az, hogy a **Linux** alatt nem terjednek a vírusok, ezért nincs is szükség vírus detektáló és -irtó programra. Pedig ugyanúgy terjednek a rosszindulatú programok, mint más operációs rendszer alatt: *rootkit*ek, *férgek* (worms), *trójai* programok, egyes *makró vírus*ok.

A vírus programok már a `DOS`-os világban megjelentek. Egyik markáns képviselőjük az `1701`, ismertebb nevén a potyogós volt. Még ma is inkább a Windows™-os világra jellemző. Amiért mégis foglalkozni kell a vírus detektálással:

- Windows™ rendszert használók számára továbbított fertőzött fájl a fogadónak komoly gondokat okozhat, és bár nekünk nem biztos, hogy problémánk támadt, a felelősség mégis a miénk.
- Minden olyan esetben, amikor a **Linux** felhasználó a `wine`-t használja, fennáll a veszélye, hogy Windows™-os állományok fertőződnek meg anélkül, hogy a felhasználó azt észrevenné...
- Ha **Linux**os gépünk levelező kiszolgáló, könnyen továbbíthatunk fertőzött levelet olyan felhasználónak, aki erre érzékeny rendszert használ.
- Nem mellesleg ma már léteznek kárt okozó különféle programok, amik **Linux** alatt is „hatásosak”, nem ritkák a betörést megkönnyítő különböző eljárások.

Természetesen megmaradnak azok az előnyök, amelyek a **Unix**™ alapú rendszerekre jellemzőek:

- A rendszer jellegéből adódóan a rosszindulatú programok károkozásának az esélye kisebb, mint más rendszereken.
- A **Linux** több felhasználós, több feladatos (multiusers, multitasking) jellegéből adódóan nagyobb terhelés nélkül lehet ellenőrzéseket futtatni, miközben a munkavégzés általában fennakadás nélkül folytatható.

A rosszindulatú programok **Linux** alatti terjedése lényegesen kisebb mértékű lesz, ha betartjuk azokat az alapvető szabályokat, amelyeket ma már minden disztribúció készítői, fejlesztői ajánlanak:

- Lehetőség szerint ne használjuk a *root* felhasználót, kizárólag csak rendszertechnikai feladatokra!
- A rendszer karbantartását, frissítését csak ellenőrzött, hivatalos tárolókból végezzük! Egyre több gyártó digitális aláírással látja el csomagjait, ezzel is védekezve a csomagok meghamisítása ellen.

A cikk szerkezete

Az eredeti írás egy rövid, képernyőképekkel illusztrált telepítési és konfigurálási leírást tartalmaz. A szerző súlyt fektetett arra, hogy a leírás lényegre törő és felesleges magyarázatoktól mentes legyen. Aki „csak” telepíteni és használni akarja a programot, ennek a fejezetnek az útmutatásai alapján ezt könnyen megteheti.

A közreadást követően felmerül néhány kérdés. Ezeket áttanulmányozva szükségesnek láttuk néhány kiegészítés, megjegyzés beépítését. Az eredeti célt nem szerettük volna megváltoztatni, ezért

Jelölések

Minden dokumentáció a jobb olvashatóság érdekében egységes jelölést alkalmaz. Ebben a dokumentációban igyekeztünk kerülni a bonyolult, a megértést nem mindig segítő különféle jelölés rendszereket. Néhány esetben azonban elkerülhetetlen volt a szövegből egyes típuselemeket kiemelni:

- Ha billentyű(ke)t kell lenyomni, ezt a következőképp jelöljük: pl. az Enter lenyomása: <ENTER>.
- Egy felhasználót *ezzel a betűtípussal* jelölünk pl.: *root*.
- Ha egy képernyőn egy adott gombot lehet/kell lenyomni, ennek a jelölése zárójelek közt a gomb felirata, pl.: (OK).

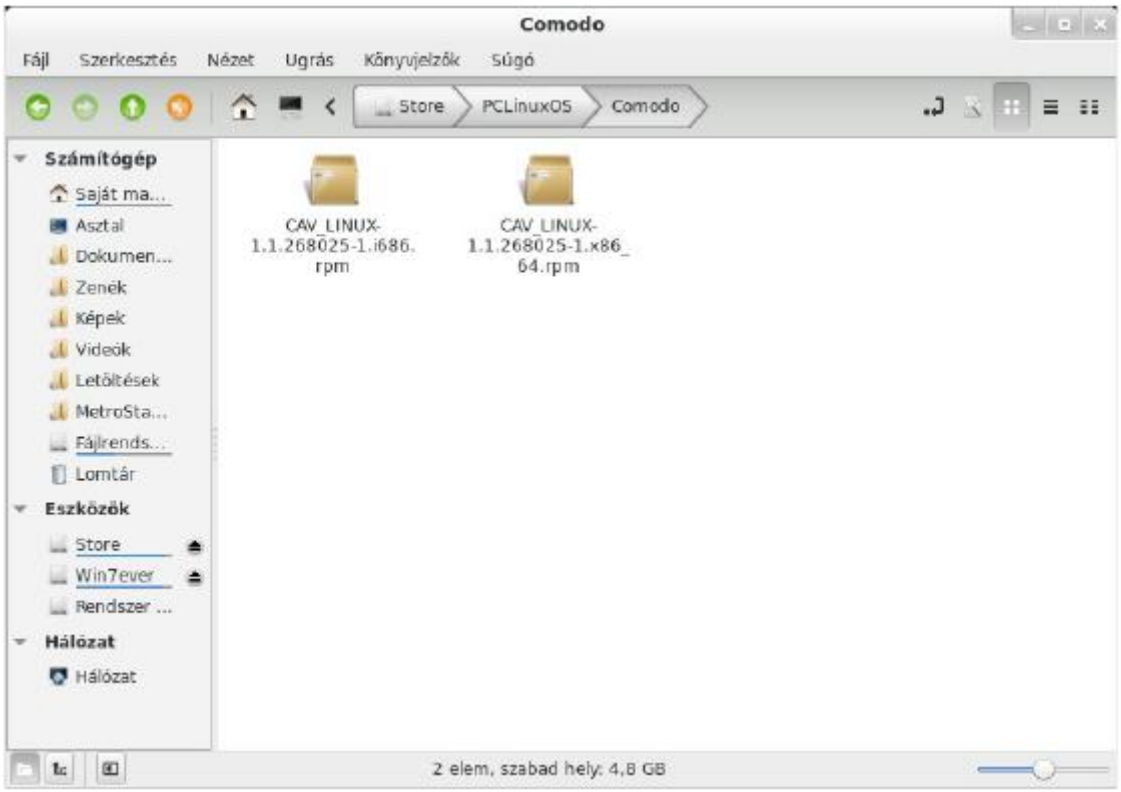
2. Telepítés és konfigurálás

Kivonat

> Ebben a részben az eredeti leírást közöljük változatlan tartalommal. Ahol elengedhetetlenül szükséges volt, ott a jobb érthetőség kedvéért igazítottunk a szövegen.

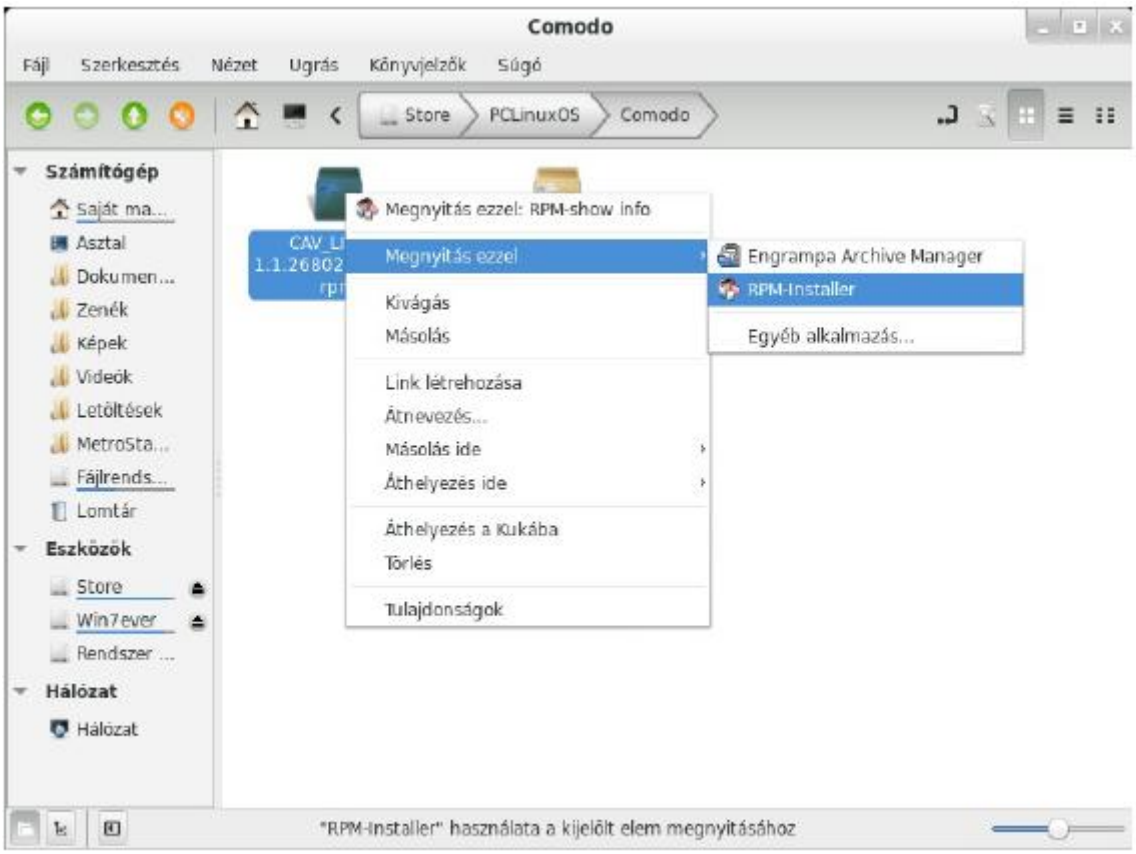
Az eredeti szöveghez képest annyi változtatás is látható, hogy néhány pont végén szerepel a „(Kiegészítés)” megjegyzés. Erre kattintva a megfelelő magyarázathoz jutunk, ahonnan az ott szereplő linkre kattintva visszajutunk a kiinduló ponthoz.

1. Telepítsük Synapticból az RPM-Installer csomagot.
2. A fájkezelőben keressük meg a letöltött telepítőt:



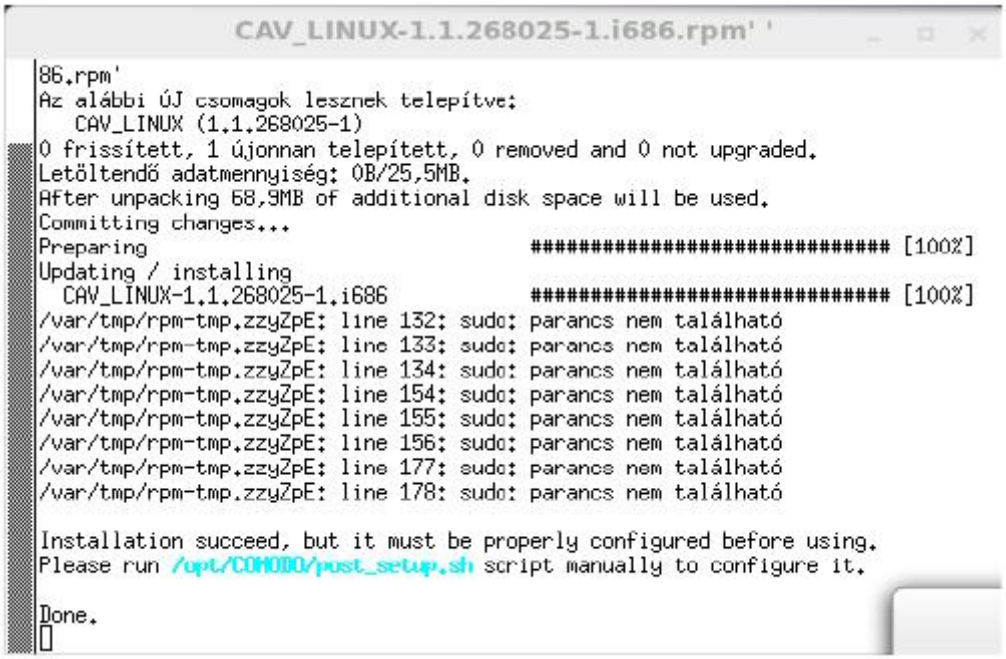
(Kiegészítés)

3. Válasszuk ki a rendszerünknek megfelelő verziót: 32 bites i686, 64 bites x86_64.
4. Az RPM csomagot futtassuk az RPM installer segítségével:



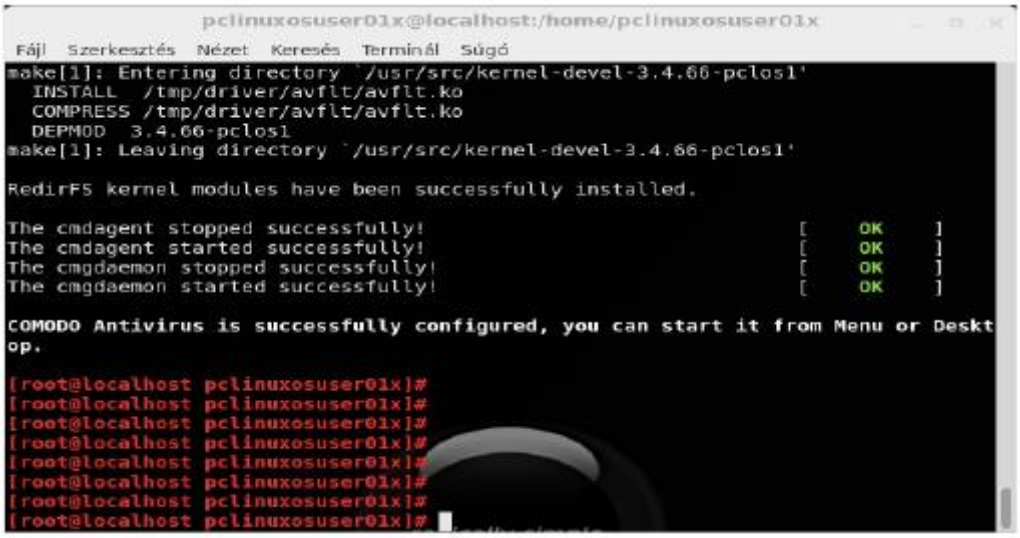
(Kiegészítés)

5. A felugró terminálban a password-höz írjuk be *root* jelszavunkat.
6. Ha lefutott a telepítés, a következő kép fogad minket:



(Kiegészítés)

7. Zárjuk be a terminált.
8. Nyissunk új terminált *root* jogosultsággal(`su` majd <ENTER> és jelszó), majd a képen látható `/opt/COMODO/post_setup.sh` parancsot írjuk be majd <ENTER>.
9. Megjelenik a licenc-szerződés, melyen az <ENTER> gomb lenyomásával tudunk lapozni és a végén elfogadni.
10. Ha a végére értünk, <ENTER>-rel tudjuk elfogadni.
11. Ezután tetszőlegesen megadhatjuk e-mail címünket is (nem kötelező), hogy a COMODO újdonságairól e-mailben értesülhessünk. Ezt <ENTER>-rel ugorhatjuk át.
12. Most rákérdez a grafikus felület nyelvére. A magyar nyelv a *13*-as, ezt írjuk be, majd <ENTER>. Ha később szeretnénk ezt beállítani, <ENTER>-rel ugorhatjuk át. A 16. pontban leírjuk, hogyan lehet a grafikus felületen a nyelvet beállítani.
13. Ha ezt látjuk a Terminálban, a telepítés sikeresen befejeződött. Zárjuk be a terminált (`exit` parancs, majd bezárás).



14. Futtassuk a COMODO-t (menü → COMODO menü → COMODO antivírus).
15. Megjelenik a COMODO grafikus felülete:

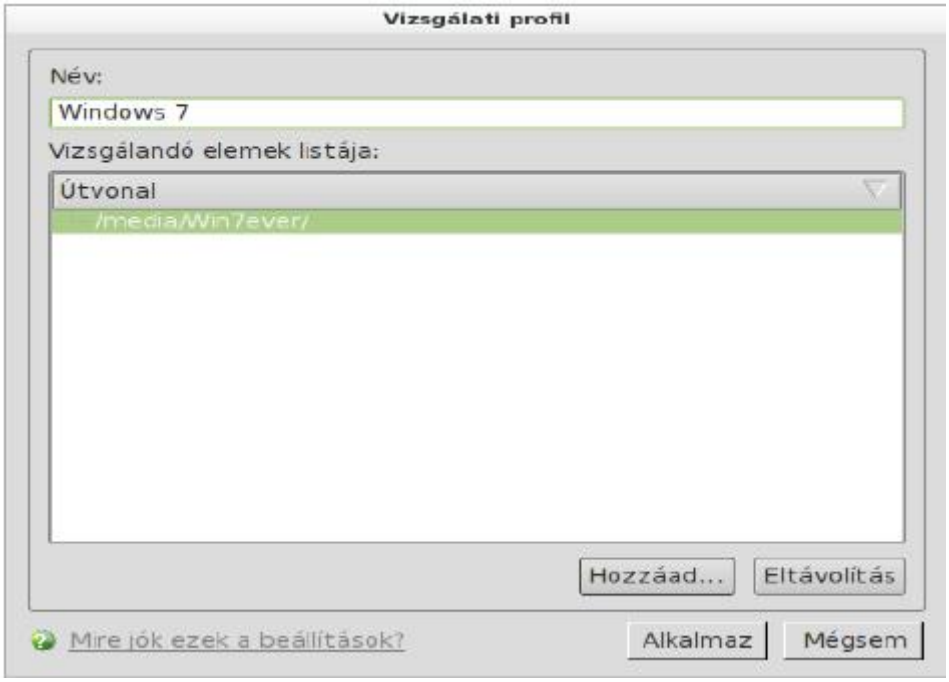
16. Válasszuk a *More* fület majd itt a *Preferences*-t és a `Language` pontban állítsuk be a legördülő menüben a magyar nyelvet majd (OK) és (YES):

17. És a grafikus felület ezután magyar nyelven fogad minket:

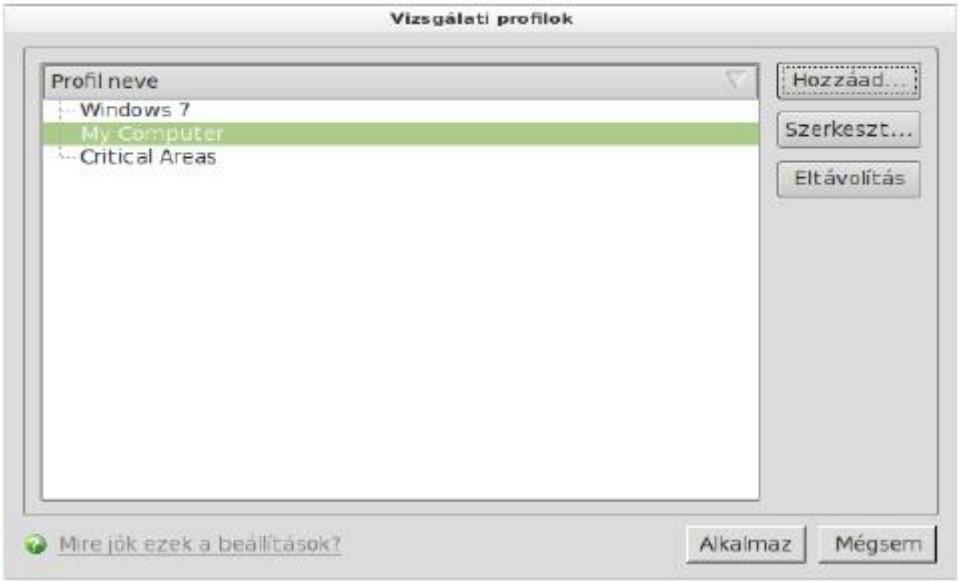
18. Frissítsük a vírus adatbázist: Antivírus → Vírusadatbázis frissítése:

19. Ha ez befejeződött, még egy teendőnk van, ha **Windows**™ operációs rendszer is van gépünkön. Válasszuk ki ugyanitt a `Vizsgálati profilok` menüpontot, majd a megjelenő ablakban a (Hozzáad...) gomb lenyomása után válasszuk ki a (Partíció)-t: (Hozzáad...) itt válasszuk ki a **Windows**™ partíciónkat majd kattintsunk a jobbra mutató nyílra. Ennek hatására hozzáadódik a listához:

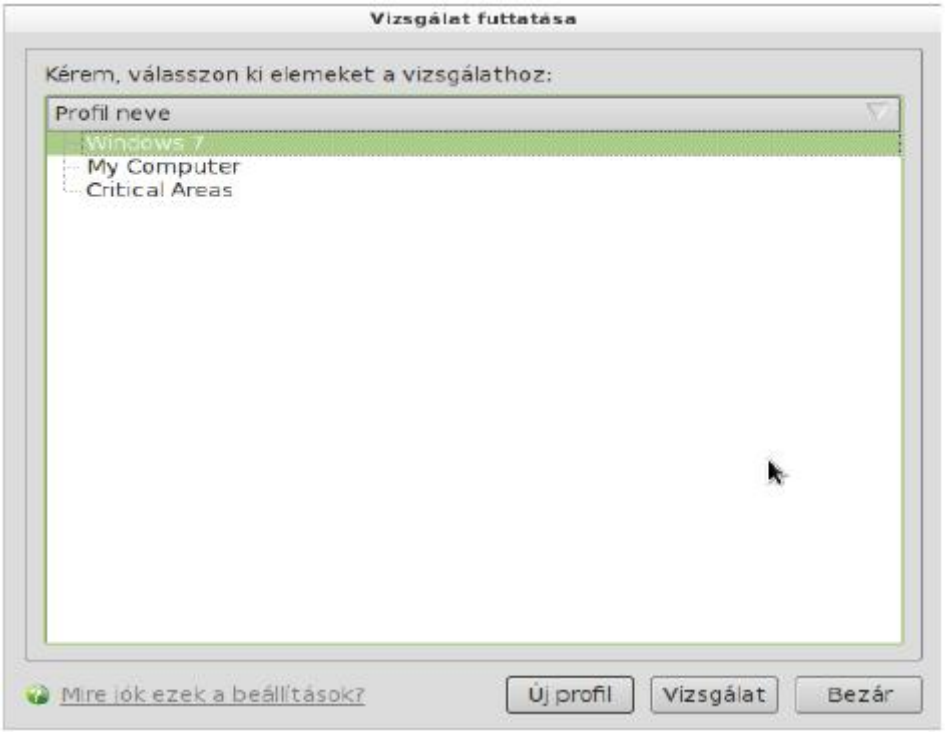
20. Kattintsunk az (Alkalmaz)-ra majd a megjelenő ablakban adjuk meg a vizsgálati profil nevét. Ez bármi lehet, én, mivel ez a Windows 7 operációs rendszerem partíciója, értelemszerűen ezt a nevet adtam neki. Majd ha ezzel megvagyunk, kattintsunk az (Alkalmaz)-ra:



21. Ezzel hozzá is adtuk a vizsgálandó területek listájához. Kattintsunk az (Alkalmaz)-ra:



22. A Windows rendszer partíciónk átvizsgálásához nyissuk meg a `Vizsgálat futtatása` menüpontot, majd itt válasszuk ki a listából a Windows-t és kattintsunk a Vizsgálat gombra:



Ezután már csak egyetlen teendőnk maradt, hogy maximális hatékonysággal védjen minket a COMODO. A rendszertálcán kattintsunk az ikonjára jobb egérgombbal. Az `Antivírus biztonsági szint`et állítsunk *Valósidejű*re.

Ha meg szeretnénk nyitni a kezelő felületet, ugyanígy kattintsunk a rendszertálcán az ikonra, majd a `Megnyit...`-ra.

3. Magyarázat az egyes lépésekhez

Kivonat

> Ebben a részben az előző rész néhány lépéséhez fűzünk megjegyzéseket. Célunk az, hogy a felmerült kérdésekre választ adjunk, így a vírus detektálásban és -írtásban kevésbé járatos felhasználó is tájékozottabbá válhat.

Az előző részben a telepítés és konfigurálás egyes lépéseit mutattuk be. Aki ez alapján telepíti és konfigurálja a COMODO antivírus programot, teljes értékű munkát végzett.

A telepítéshez: Az egyes csomagok letölthetőek: Download Comodo Antivirus for Linux.

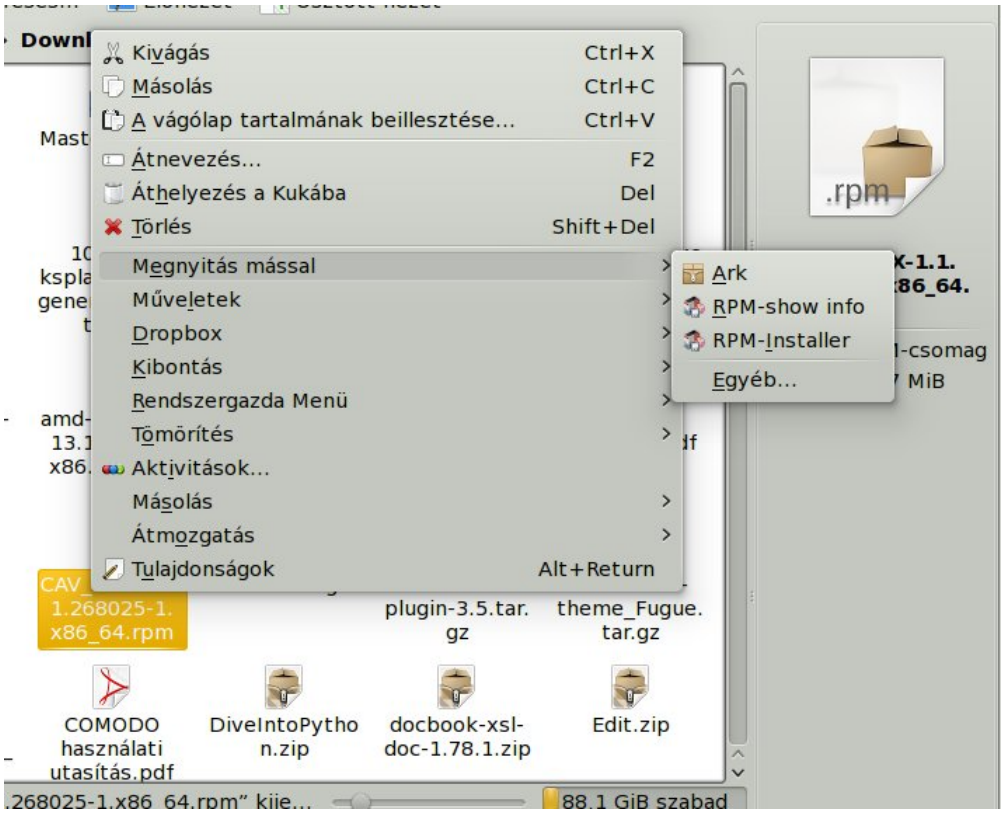
A megjelenő lapon be kell állítani:

1. az operációs rendszert („Choose your operating system” – ez pontatlan, ténylegesen a disztribúcióról van szó),

   Ha a lenyíló ablakban a használt disztribúció nem jelenik meg, a jellegében legközelebb állót lehet kiválasztani, pl.: **PCLinuxOS** használók a *Fedora*-t választhatják;
2. az architektúrát („32 bit or 64 bit?”).

A lapon szerepel a támogatott rendszerek listája („Supported Operating Systems”), a rendszer követelmények („Minimum Hardware Requirements”) és mindkét jellemző beállítása után megjelenik a letöltendő méret („File Details”).

Az rmp-install használatához: Az alkalmazott asztali felülethez tartozó fájlkezelő a bemutatottól esetleg eltérő menüelemeket mutathat. KDE alatt pl. így néz ki a *Dolphin*:



A lényeg az, hogy legyen a helyi menüben `rpm installer` menüpont.

Az installálást követően látható terminál ablakban: Több sor mutatja, hogy az adott rendszeren nincs telepítve a *sudo* (erre írja ki a „. . . sudo: parancs nem található” üzenetet). Annak ellenére, hogy rpm csomagot telepítettek, mégis a szkript az Ubuntu által követett megoldás jelenlétét feltételezi. Ez nem probléma, a telepítés ettől még hibátlanul lefut, de a konfigurálást külön indítani kell.