

# A számítógépes vírusokról

The image features a central 3D puzzle structure. The puzzle pieces are light gray and white, with some pieces highlighted in a vibrant blue. The blue pieces form a shape that resembles a virus or a complex molecular structure. The background is a dark blue gradient with abstract, glowing light patterns that suggest a digital or scientific environment. The overall aesthetic is clean and modern, with a focus on the central puzzle and its glowing blue components.



# Mi a számítógépes vírus?

A számítógépes vírusok egyszerű, végrehajtható számítógépes programok.

Miután megfertőz egy fájlt vagy a rendszer más részeit, továbbterjed a szomszédos elemekre is.



# Mi a számítógépes vírus?

- Önmagát reprodukálja, azaz szaporodik
- Hagyományos eszközökkel nem látható
- Valamilyen állományhoz kapcsolódik
- Lappangási idejük van
- Többnyire kárt, vagy bosszúságot okoz



# A vírusok megfertőzhetik ...

- A **programfájlokat**, az **indítórekordokat** és a makróval rendelkező adatfájlokat
- Az **adatlemezeket** és a számítógépek közötti programátvitelhez használt lemezeket, de csak addig, míg azok nem lesznek írásvédettek
- Az elektronikus levélhez **csatolt fájlokat**, de csak a csatolás előtt



# A vírusok nem tudják megfertőzni ...

- A hardvert, a képfájlokat, a makró lehetőség nélküli adatfájlokat és a nem futtatható egyéb szoftverrészeket
- Az írásvédett lemezeket
- A szöveges elektronikus leveleket



# A vírusok fajtái

- **Közvetlen fertőző**
  - fertőzött fájl futtatásakor aktivizálódnak
  - átveszik a rendszer irányítását
  - „tiszta” fájlokat keres, amelyeket megfertőzhet
  - a fertőzött program bezárásakor a vírus abbahagyja a fertőzést



# A vírusok fajtái

- Tárrezidensen fertőző
  - aktivizálódása után átveszi a rendszer irányítását
  - magánál tartja a rendszer irányítását és közben folyamatosan terjed, mindaddig, míg a memória nem törlődik, még akkor is, ha a fertőzött programot bezárjuk



# Hogyan működik a vírus?

- **Időzítés**
  - számítógépre kerülése után még várakozik
  - lehet dátum, eltelt idő egy fertőzött program indítása óta, valahányadik elindított program a fertőzés óta





# Hogyan működik a vírus?

- Töltet
  - Az időzítő hozza működésbe
  - lehet szándékosan romboló hatású (pl.: OneHalf)
  - lehet jóindulatú (csak egy üzenetet jelenít meg, vagy egy dallamot játszik le (pl.: Boza))



# A vírusok típusai

- Programvírusok (állományvírusok)
  - futtatható fájlokat fertőz
- Indítóvírusok (boot-vírusok)
  - az indítórekordot fertőzi meg
- Makróvírusok
  - adatfájlokat fertőz



# A vírusok típusai

- Worm-ok, vagy férgek
  - Módosítják az operációs rendszert, gyakran a géppel együtt bootolnak, a hálózatot használva levelekhez csatolt állományként terjednek.
  - A csatolt állomány tartalmazza a vírust, melyet aktivizálva (megnézve), elküldi saját magát címjegyzékünk összes tagjának, vagy személyes adatainkat teszi közzé



# A vírusok típusai

- Trojan (trójai program)
  - Nem szaporodik és nem terjed



**NEM VÍRUS !!!**

- Olyan program, amely látszólag hasznos célt szolgál, de valójában a célja a fájlok károsítása, illetve vírusok elhelyezése a számítógépen.



# A vírusok típusai

- **Wabbit**
  - A gép erőforrásait emészti fel. Helyi gépen sokszorozódik.
- **Backdoor**
  - Lehetővé teszi a számítógéphez való hozzáférést.



# A vírusok típusai

- **Adware**
  - Nemkívánt hirdetések jelenít meg.
- **Spyware**
  - Adatokat gyűjt a gép működéséről és elküldi azokat a felhasználó hozzájárulása nélkül.



# A vírusok típusai

- Hoaxok
  - Átverések, kacsák
  - Elektronikus levélben „terjed”
  - Félrevezető információ küldése, majd továbbküldése minél több ismerősnek (pl.: téves vírusriasztás)



# Mi is az a Malware?

A **Malware** egy általános értelmű kifejezés, mely olyan programokra vonatkozik, amelyek pl. hirdetések megjelenítését, személyes adatok gyűjtését, vagy a számítógép konfigurációját állítják át úgy, hogy e tevékenységekbe rendszerint nincs beleszólásunk.



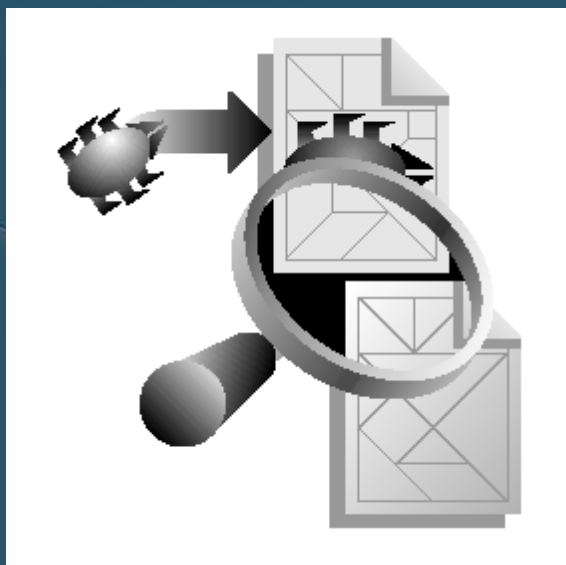


# Mi is az a Malware?

## Szimptómák:

- Nem kívánt pop-up reklám ablakok nyílnak meg, akkor is ha éppen nem a szörfölünk a weben
- A böngésző kezdő oldala, vagy a beállított kereső motor megváltozik a beleegyezésünk nélkül, ráadásul nem hagyja, hogy visszaállítsuk az eredeti állapotot
- Új és nem kívánt eszköztár jelenik meg a böngészőben, melyet nem lehet leszedni
- Ismeretlen email címekről visszaérkező levelek
- Hirtelen bekövetkező drámai teljesítmény csökkenés
- Az operációs rendszer, a web böngésző, vagy egyéb alkalmazások fagyogatni kezdenek

# Vírustechnológiák



- Lopakodó vírusok
  - megpróbálnak elrejtőzni
    - olvasásmegszakítók
    - méretmódosítók

# Vírustechnológiák

- Önmódosító vírusok

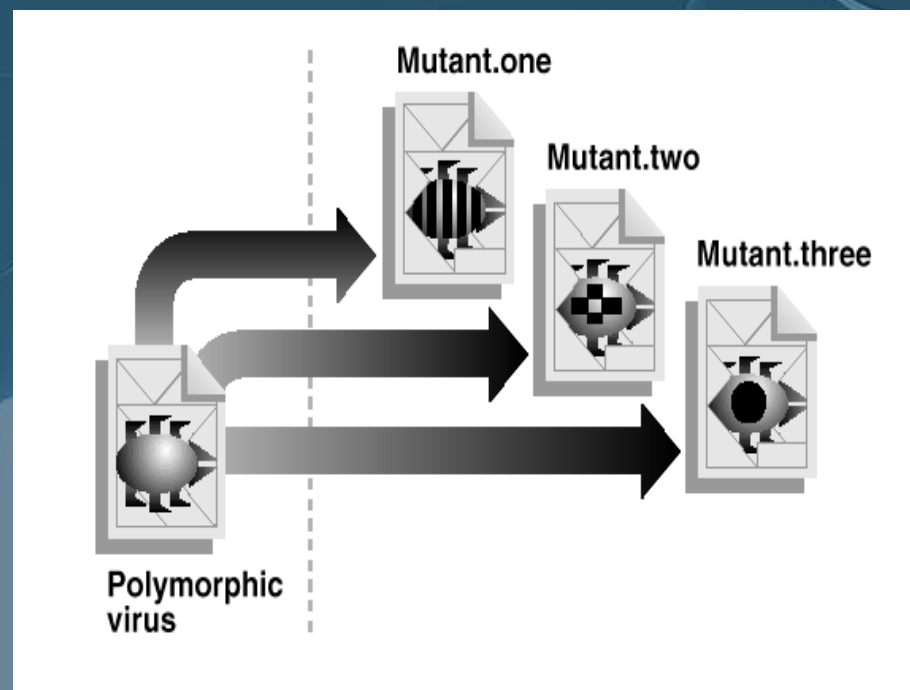
- mindig módosítja a saját kódját a programtörzsben



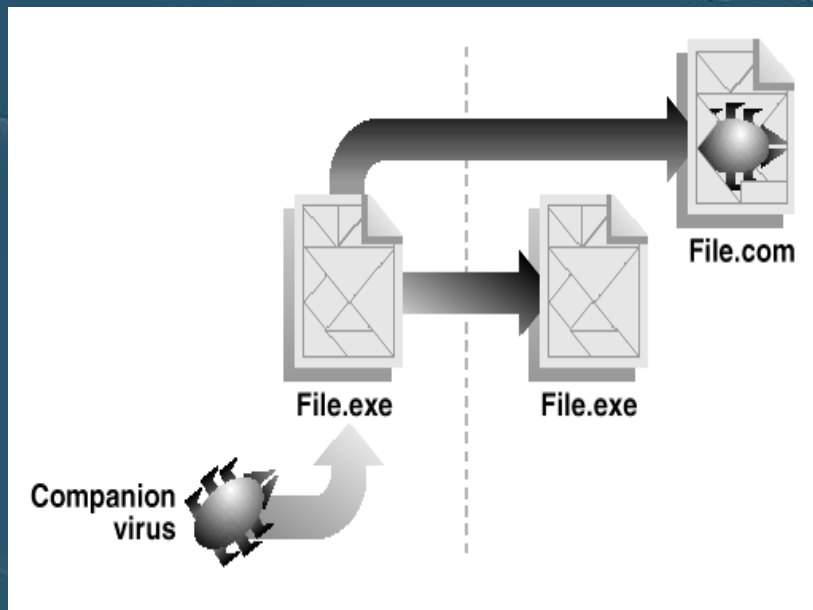
Nincs két egyforma víruskód.



Nehezíti az észlelést.



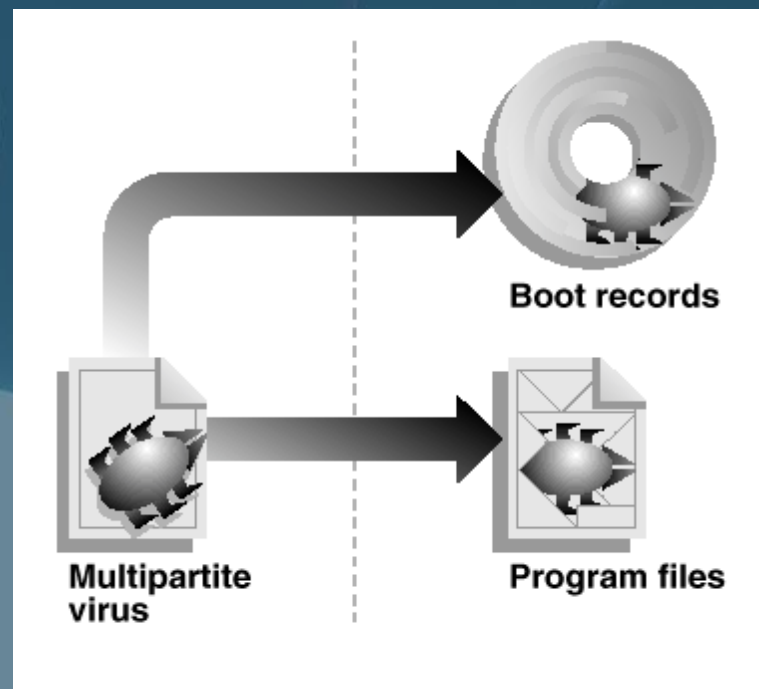
# Vírustechnológiák



- Társvírusok
  - új fájlt hoz létre
  - az OS-t „utasítja”, hogy a kiválasztott fájl helyett az új hajtódjék végre (pl.: .EXE fájllal azonos .COM fájlt hoz létre, az OS a .COM-ot futtatja előbb)

# Vírustechnológiák

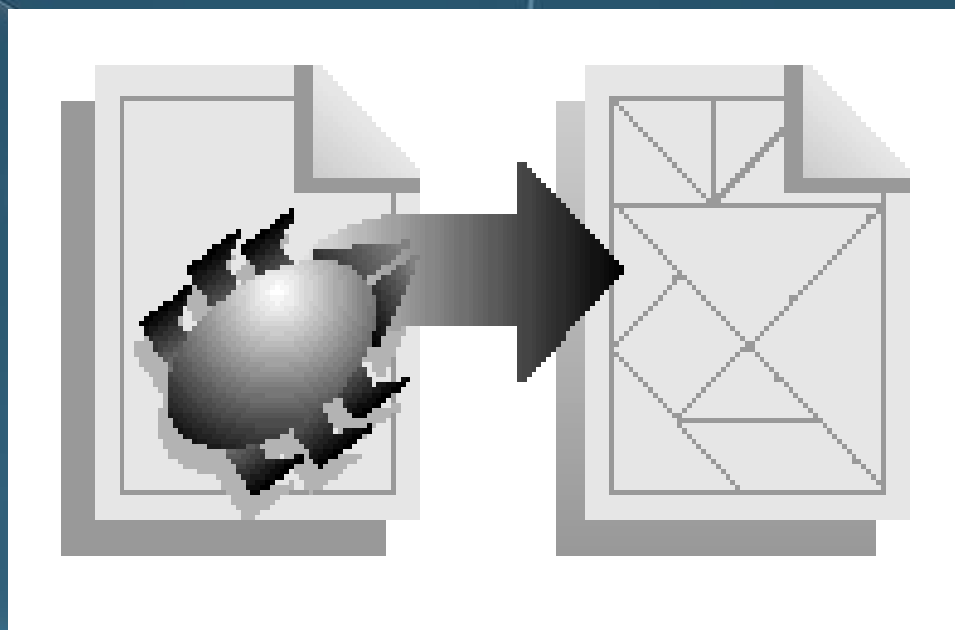
- Több módon fertőző vírusok
  - egyszerre program- és indítóvírusok (pl.: Tequila  
↓  
szövegszerkesztés  
↓  
indítórekord)





# Vírusfertőzési ciklus 1.

Fertőzés





# Fertőzés forrása lehet...

- Ismeretlen eredetű floppy használata
- Otthoni vagy iskolai lemez
- Barátoktól kölcsönként lemez
- Nem megbízható kereskedőtől származó szoftver



# Fertőzés forrása lehet...

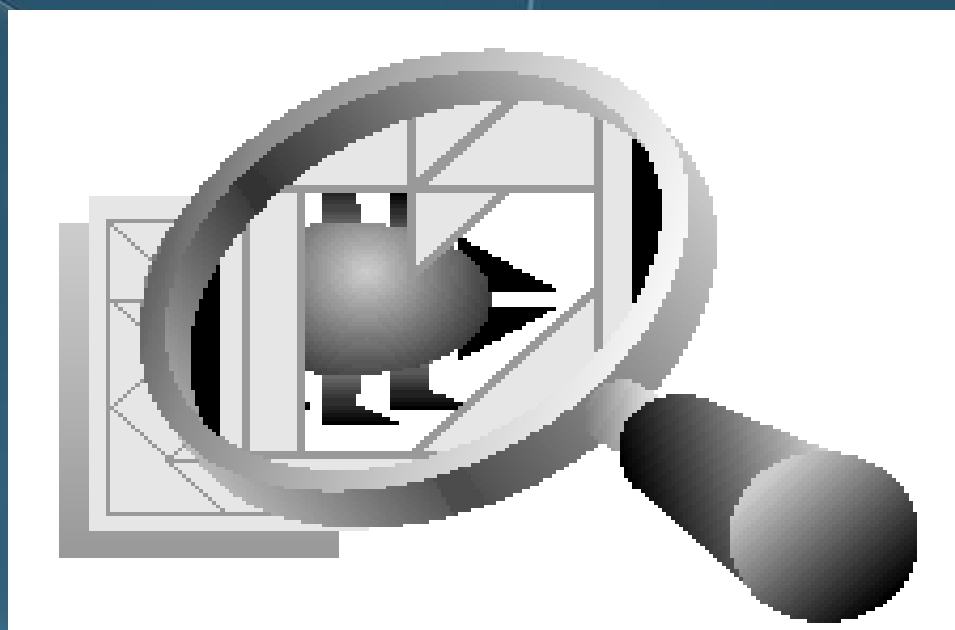
- Kalóz szoftver
- Tömörített vagy megnyitott szoftver
- Internet szolgáltatótól letöltött program
- E-mail melléletek





# Vírusfertőzési ciklus 2.

## Észlelés





# Észlelés - megfigyelés

- Furcsa rendszerviselkedés
- Hiányzó fájlok
- Programok működésképtelensége



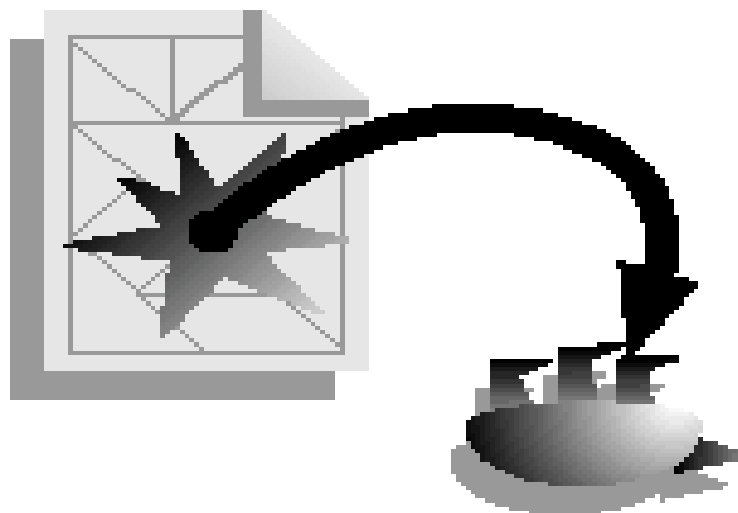
# Észlelés


- **Segédprogrammal**
  - **Víruselhárító szoftverrel észlelt vírus**



# Vírusfertőzési ciklus 3.

## Helyreállítás





# Helyreállítás - „Takarítás”

- Programok újratelepítése a mesterlemezről
- Fájlok kijavítása víruselhárító szoftverrel
- Visszaállítás fertőzésmentes biztonsági másolatról



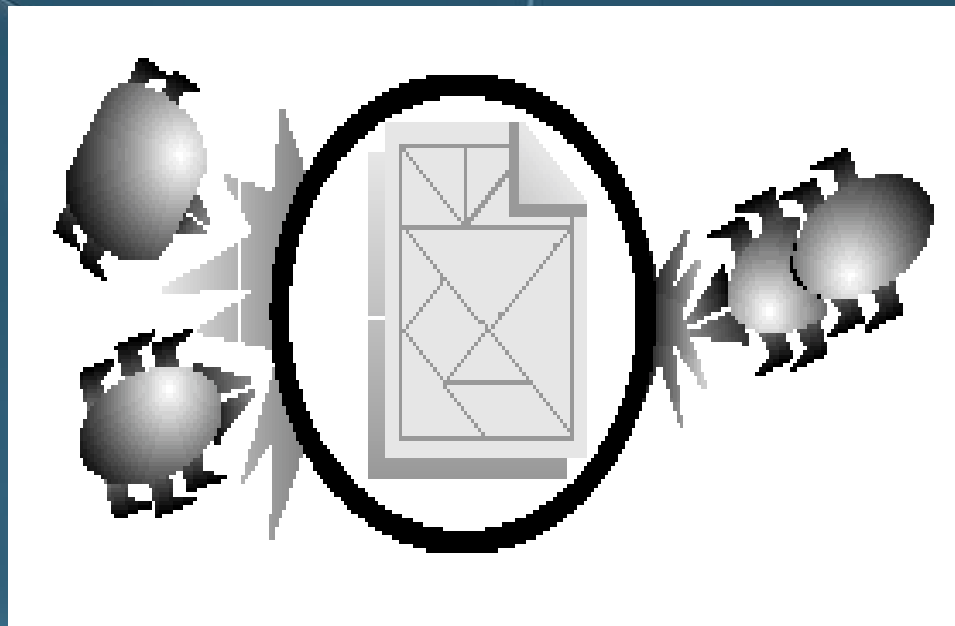
# Helyreállítást követően ...

- Az összes fájl újbóli vizsgálata a fertőzés forrásának megkereséséhez
- Az összes floppy újbóli vizsgálata a fertőzés forrásának megkereséséhez
- Az esetlegesen fertőzött biztonsági másolatok selejtezése
- Fokozott víruselhárítás egy ideig



# Vírusfertőzési ciklus 4.

## Megelőzés





# Megelőzés

- **Vírusfigyelő programokkal:**
  - Norton AntiVirus
  - NOD32
  - F-Secure (volt F-Prot)
  - VirusScan
  - VirusBuster ...

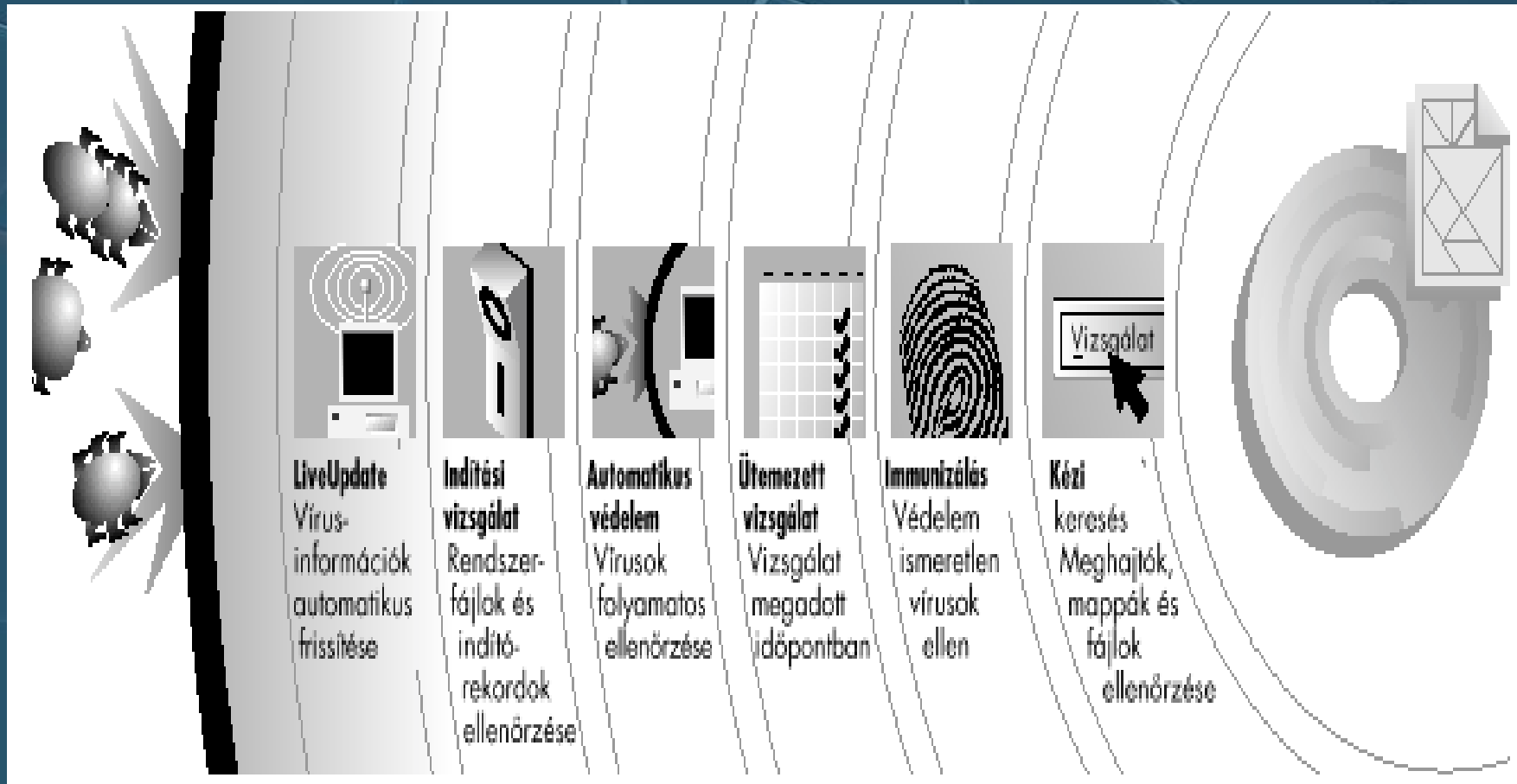




# Alkalmazott keresési módok

- **Aláírásos keresés**
  - Már ismert vírusok kódjaival (aláírásával) dolgozik
  - 100%-os biztonságot nyújt
- **Heuresztikus keresés**
  - Valószínűsíti a vírustevékenységet
  - Kb. 80%-os biztonsággal ismeri fel

# Norton AntiVirus védelme



# Norton AntiVirus védelme

The screenshot shows the Norton AntiVirus 2003 application window. The title bar reads "Norton AntiVirus". The interface includes a yellow header bar with "LiveUpdate" and "Beállítások" (Settings) buttons, and a "Súgó" (Help) button. A left sidebar contains "Norton AntiVirus", "Állapot" (Status), "Víruskeresés" (Scan), and "Jelentések" (Reports). The main area displays "Rendszer: OK" (System: OK) with a green checkmark. Below this are two sections: "Rendszervédelmi vizsgálatok" (System Protection Checks) and "Vírusleírás-szolgáltatás" (Virus Definition Service). The first section lists "Auto-Protect", "E-mail üzenetek", "Szkriptellenőrzés", and "Teljes rendszervizsgálat" (2004.06.15), all with green checkmarks and "Bekapcsolva" (On) status. The second section lists "Vírusleírások" (2004.06.19), "Előfizetés" (2005.05.21), and "Automatikus LiveUpdate" (Bekapcsolva), all with green checkmarks. A right-hand box titled "Az elem leírása" (Item Description) explains that red items need attention and that clicking items provides details and actions. The bottom of the window features the Symantec logo and the text "Norton AntiVirus™ 2003".

**Norton AntiVirus**

LiveUpdate Beállítások Súgó

**Norton AntiVirus**

Állapot

Víruskeresés

Jelentések

**Rendszer: OK**

**Rendszervédelmi vizsgálatok**

✓ Auto-Protect	Bekapcsolva
✓ E-mail üzenetek	Bekapcsolva
✓ Szkriptellenőrzés	Bekapcsolva
✓ Teljes rendszervizsgálat	2004.06.15.

**Vírusleírás-szolgáltatás**

✓ Vírusleírások	2004.06.19.
✓ Előfizetés	2005.05.21.
✓ Automatikus LiveUpdate	Bekapcsolva

**Az elem leírása**

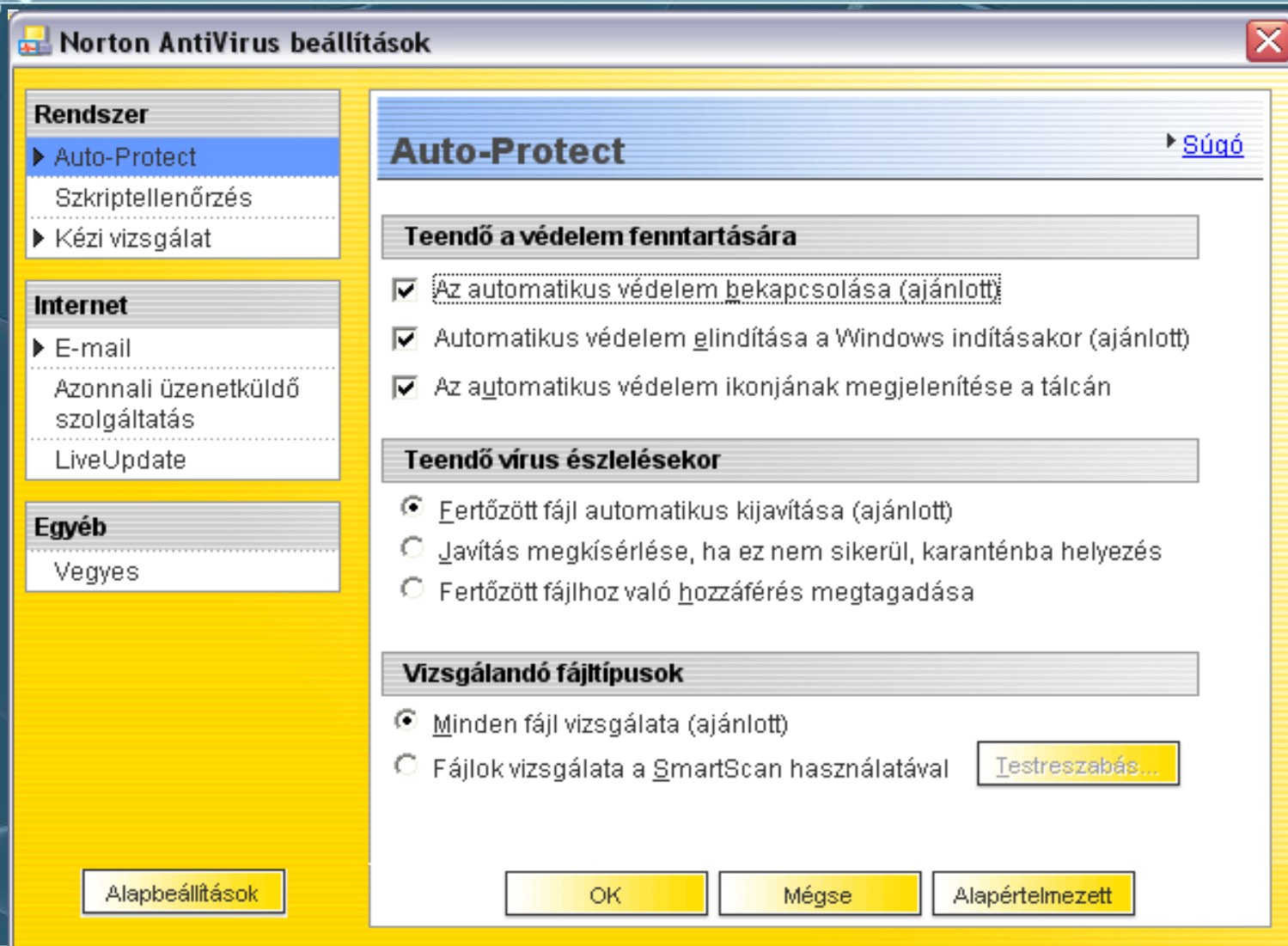
A pirossal jelölt elemek azonnali figyelmet igényelnek.

A balra látható elemeket kattintással jelölheti ki, ekkor elolvashatja az adott elem részletes leírását és végrehajthatja a szükséges lépéseket.

**symantec.**

**Norton AntiVirus™ 2003**

# Norton AntiVirus védelme



# Norton AntiVirus védelme

The screenshot displays the Norton AntiVirus 2003 application window. The title bar reads "Norton AntiVirus". The interface includes a yellow header bar with "LiveUpdate" and "Beállítások" (Settings) buttons, and a "Súgó" (Help) button. A left sidebar contains "Norton AntiVirus", "Állapot" (Status), "Víruskeresés" (Virus Search), and "Jelentések" (Reports). The main area is titled "Víruskeresés" and contains a table of tasks and their settings.

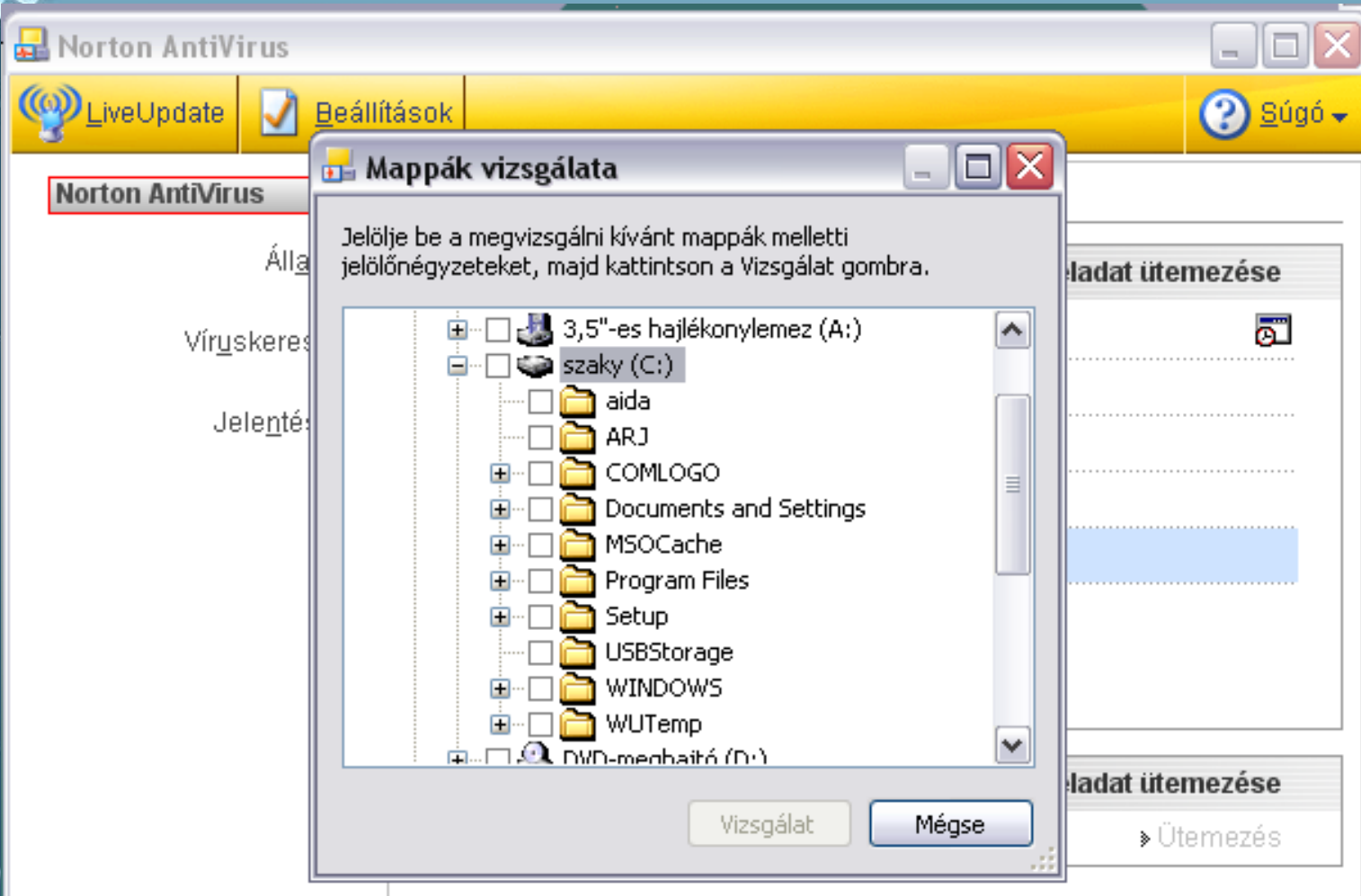
Feladat	Feladat ütemezése
A számítógép vizsgálata	
Minden cserélhető meghajtó vizsgálata	
Minden hajlékonylemez-meghajtó vizsgálata	
Meghajtók vizsgálata	
Mappák vizsgálata	
Fájlok vizsgálata	

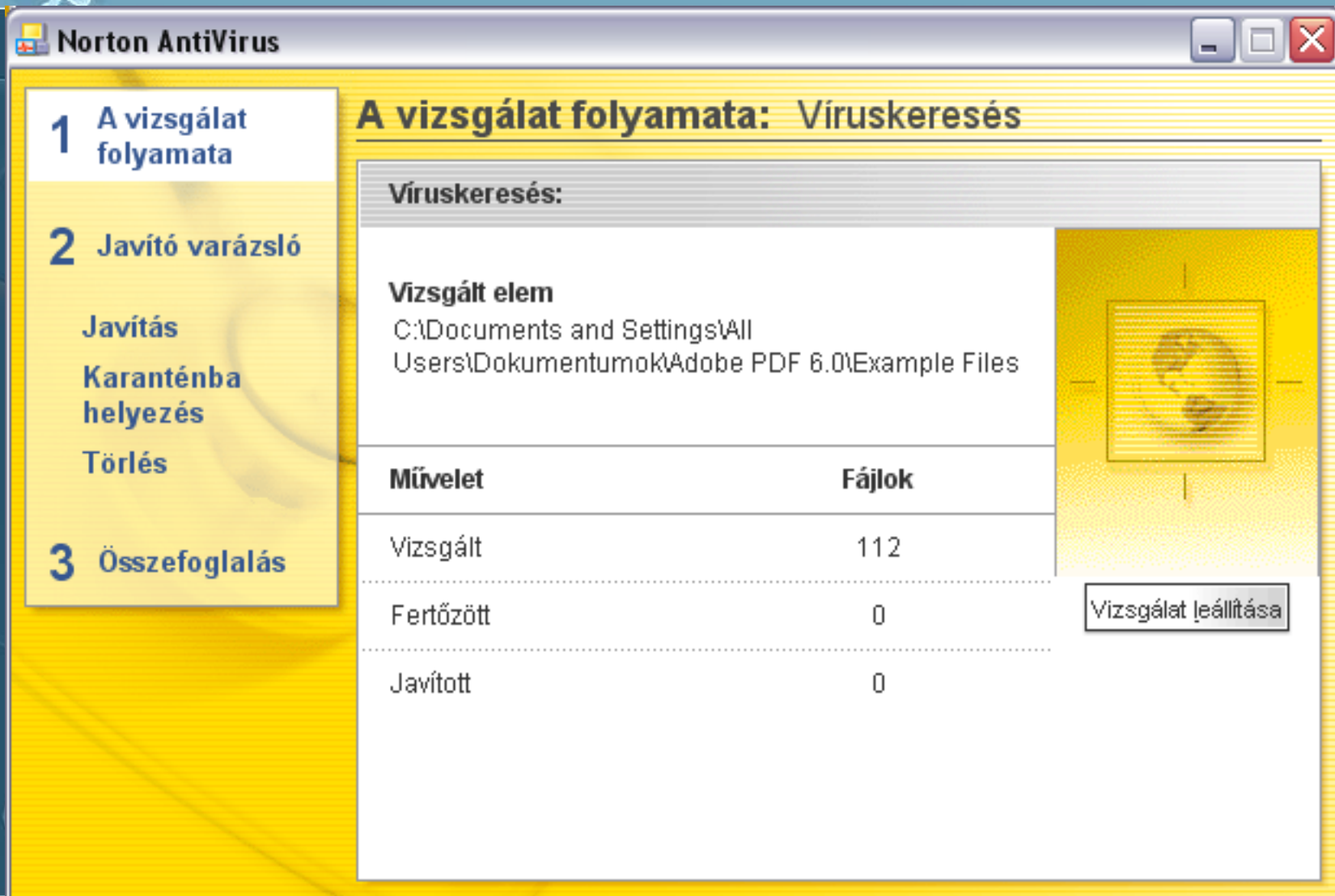
Műveletek	Feladat ütemezése
» <a href="#">Vizsgálat</a> » <a href="#">Új</a> » Szerkesztés » Törlés	» <a href="#">Ütemezés</a>

symantec. Norton **AntiVirus**™ 2003

# Norton AntiVirus védelme



# Norton AntiVirus védelme



The screenshot shows the Norton AntiVirus application window. The title bar reads "Norton AntiVirus". The interface is in Hungarian. On the left, there is a sidebar with three main sections:

- 1 A vizsgálat folyamata** (The scan process), which includes sub-options: "Javítás" (Repair), "Karanténba helyezés" (Move to quarantine), and "Törlés" (Delete).
- 2 Javító varázsló** (Repair wizard)
- 3 Összefoglalás** (Summary)

The main area is titled "A vizsgálat folyamata: Víruskeresés" (The scan process: Virus search). It displays the following information:

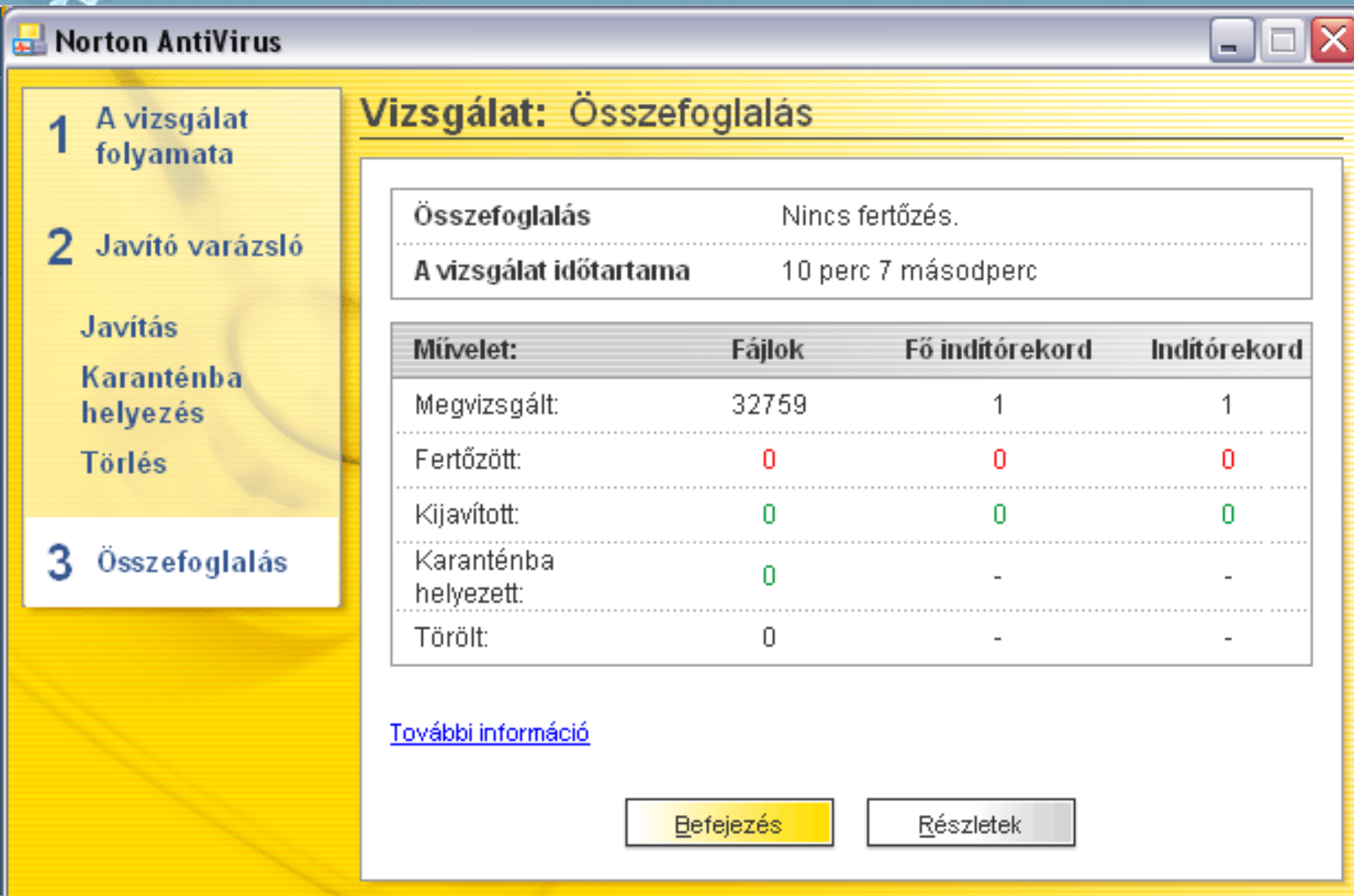
**Víruskeresés:**

**Vizsgált elem**  
C:\Documents and Settings\All Users\Dokumentumok\Adobe PDF 6.0\Example Files

Művelet	Fájlok
Vizsgált	112
Fertőzött	0
Javított	0

On the right side of the main area, there is a yellow box containing a globe icon and a button labeled "Vizsgálat leállítása" (Stop scan).

# Norton AntiVirus védelme



The image shows the Norton AntiVirus application window. The title bar reads "Norton AntiVirus". On the left, there is a vertical navigation pane with three main sections: "1 A vizsgálat folyamata", "2 Javító varázsló", and "3 Összefoglalás". The "3 Összefoglalás" section is currently selected and highlighted. Below the navigation pane, there are several options: "Javítás", "Karanténba helyezés", and "Törlés".

The main content area is titled "Vizsgálat: Összefoglalás". It displays the following information:

- Összefoglalás**: Nincs fertőzés.
- A vizsgálat időtartama**: 10 perc 7 másodperc

Below this, there is a table with the following data:

Művelet:	Fájlok	Fő indítórekord	Indítórekord
Megvizsgált:	32759	1	1
Fertőzött:	0	0	0
Kijavított:	0	0	0
Karanténba helyezett:	0	-	-
Törölt:	0	-	-

At the bottom of the main content area, there is a link for "További információ" and two buttons: "Befejezés" and "Részletek".



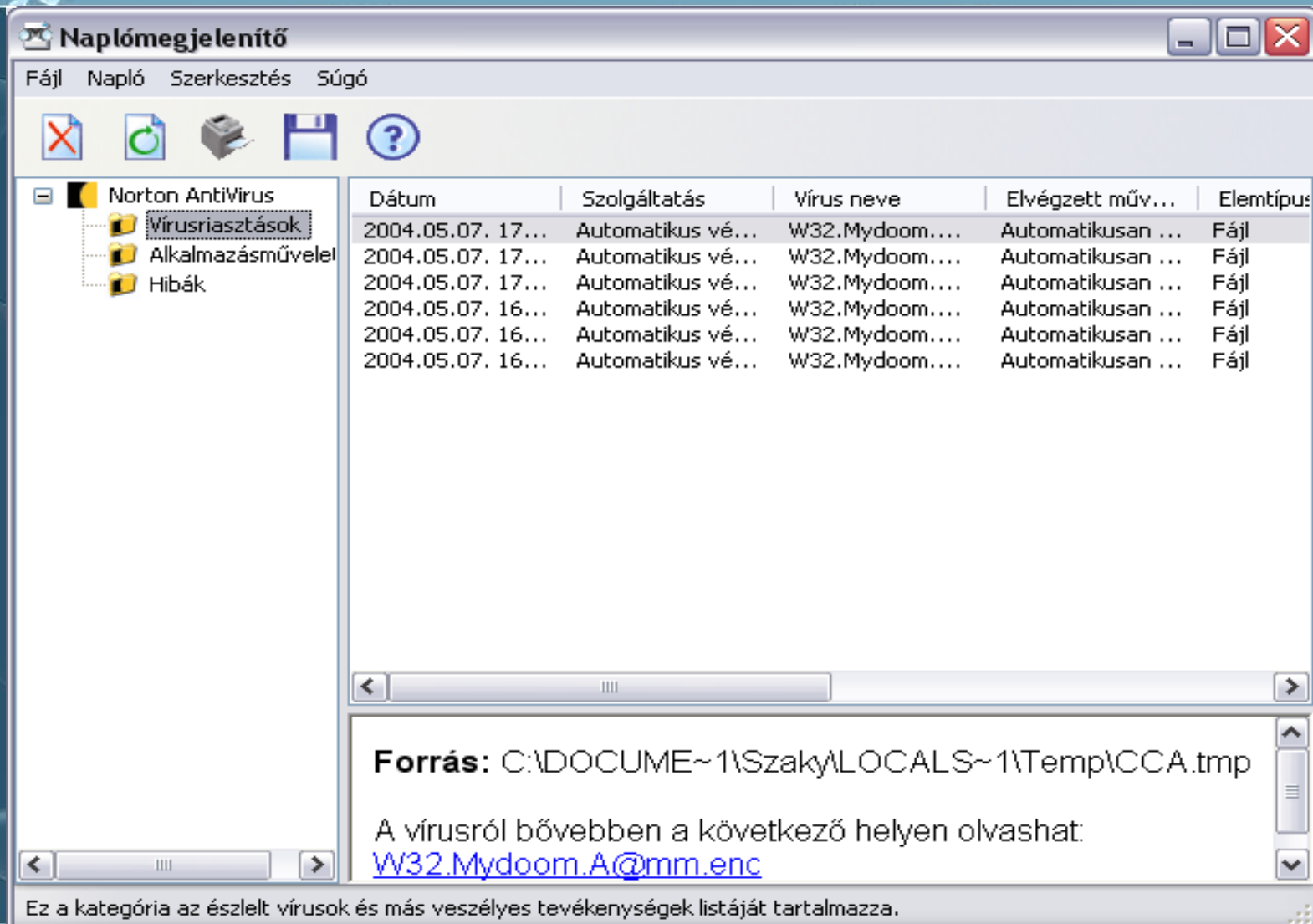
# Norton AntiVirus védelme

The screenshot displays the Norton AntiVirus 2003 application window. The title bar reads "Norton AntiVirus". The interface includes a yellow header bar with "LiveUpdate" and "Beállítások" (Settings) buttons, and a "Súgó" (Help) button. A left sidebar contains navigation options: "Norton AntiVirus", "Állapot" (Status), "Víruskeresés" (Virus Search), and "Jelentések" (Reports), which is currently selected. The main area, titled "Jelentések", lists four report categories, each with an icon and a "Megtekintés" (View) button:

- Karanténba tett elemek** (Quarantined items) - icon of a red pill bottle
- Online vírushatározó** (Online virus scanner) (használatához internetelérés szükséges) (requires internet access for use) - icon of a magnifying glass over a biohazard symbol
- Eseménynapló** (Event log) - icon of a calendar
- Víruslista** (Virus list) - icon of a document with a virus symbol

At the bottom of the window, the Symantec logo and "Norton AntiVirus™ 2003" are displayed.

# Norton AntiVirus védelme



**Naplómegjelenítő**

Fájl Napló Szerkesztés Súgó

Norton AntiVirus

- Vírusriasztások
- Alkalmazásművelet
- Hibák

Dátum	Szolgáltatás	Vírus neve	Elvégzett műv...	Elemtípus
2004.05.07. 17...	Automatikus vé...	W32.Mydoom...	Automatikusan ...	Fájl
2004.05.07. 17...	Automatikus vé...	W32.Mydoom...	Automatikusan ...	Fájl
2004.05.07. 17...	Automatikus vé...	W32.Mydoom...	Automatikusan ...	Fájl
2004.05.07. 16...	Automatikus vé...	W32.Mydoom...	Automatikusan ...	Fájl
2004.05.07. 16...	Automatikus vé...	W32.Mydoom...	Automatikusan ...	Fájl
2004.05.07. 16...	Automatikus vé...	W32.Mydoom...	Automatikusan ...	Fájl

**Forrás:** C:\DOCUME~1\Szaky\LOCALS~1\Temp\CCA.tmp

A vírusról bővebben a következő helyen olvashat:  
[W32.Mydoom.A@mm.enc](#)

Ez a kategória az észlelt vírusok és más veszélyes tevékenységek listáját tartalmazza.