Automatikus vírusvédelmi megoldások az Interneten

Dr. Leitold Ferenc, Erdélyi Gergely, Laczkó Gábor

Veszprog Kft.

fleitold@veszprog.veszprem.hu
dyce@veszprog.veszprem.hu
tiamat@veszprog.veszprem.hu

Antivirus problémák

Antivirus problémák

- Új operációs rendszerek (Windows'9X, Windows NT, ...)

Antivirus problémák

- Új operációs rendszerek (Windows'9X, Windows NT, ...)
- Makró vírusok
  - Word, Excel

Antivirus problémák

- Új operációs rendszerek (Windows'9X, Windows NT, ...)
- Makró vírusok
  - Word, Excel
  - Powerpoint, Access, ...

Windows'9X, NT
Boot vírus aktivizálódás

Windows'9X, NT
Boot vírus aktivizálódás

- PDR file törlése (Hare víruscsalád)

Windows'9X, NT
Boot vírus aktivizálódás

- PDR file törlése (Hare víruscsalád)
- F8 billentyű (MSDOS.SYS file)

Windows'9X, NT
Boot vírus aktivizálódás

- PDR file törlése (Hare víruscsalád)
- F8 billentyű (MSDOS.SYS file)
- Command mód
  MSDOS.SYS: WIN /D:F

Windows'9X, NT
Boot vírus aktivizálódás

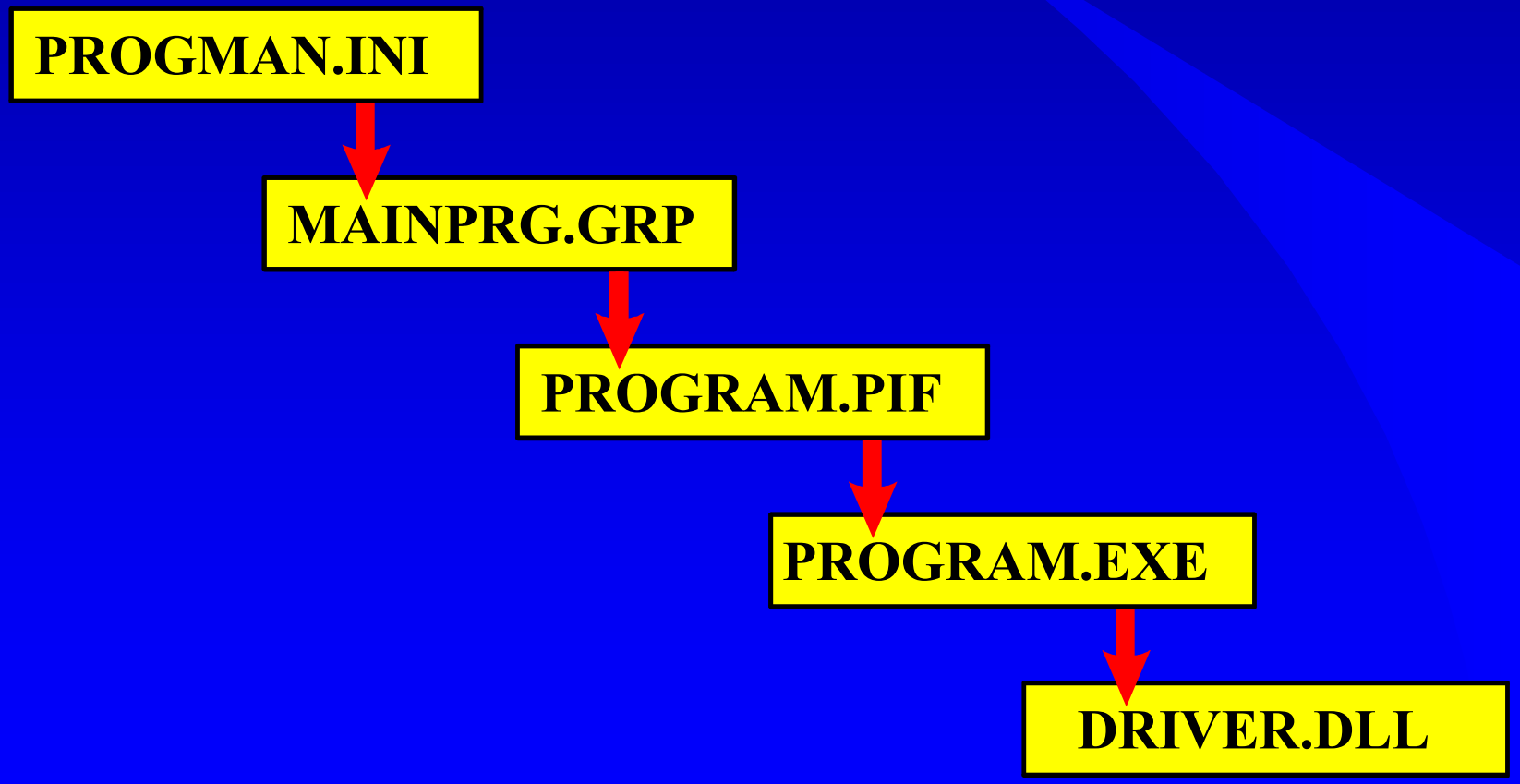
- PDR file törlése (Hare víruscsalád)
- F8 billentyű (MSDOS.SYS file)
- Command mód
  MSDOS.SYS: WIN /D:F
- 32BitDiskAccess=Off
  (SYSTEM.INI file)

Windows'9X, NT
Boot vírus aktivizálódás

- PDR file törlése (Hare víruscsalád)
- F8 billentyű (MSDOS.SYS file)
- Command mód
  MSDOS.SYS: WIN /D:F
- 32BitDiskAccess=Off
  (SYSTEM.INI file)
- Más interrupt módosítása

Windows'9X, NT
File vírusok

Windows'9X, NT
File vírusok



Makró vírusok aktivizálódása

Makró vírusok aktivizálódása

- Rendszer makrók módosítása

Makró vírusok aktivizálódása

- Rendszer makrók módosítása
- Menüpontok változtatása

Makró vírusok aktivizálódása

- Rendszer makrók módosítása
- Menüpontok változtatása
- Eszköztár hívások módosítása

Makró vírusok aktivizálódása

- Rendszer makrók módosítása
- Menüpontok változtatása
- Eszköztár hívások módosítása
- Billentyűk átdefiniálása

Makró vírusok lehetőségei

Makró vírusok lehetőségei

- Nyelvfüggetlen makrók

Makró vírusok lehetőségei

- Nyelvfüggetlen makrók
- NORMAL.DOT fertőzése

Makró vírusok lehetőségei

- Nyelvfüggetlen makrók
- NORMAL.DOT fertőzése
- Companion makró vírus

Makró vírusok lehetőségei

- Nyelvfüggetlen makrók
- NORMAL.DOT fertőzése
- Companion makró vírus
- Futás közben makró létrehozása

Makró vírusok lehetőségei

- Nyelvfüggetlen makrók
- NORMAL.DOT fertőzése
- Companion makró vírus
- Futás közben makró létrehozása
- Futás közben titkosítás

Makró vírusok lehetőségei

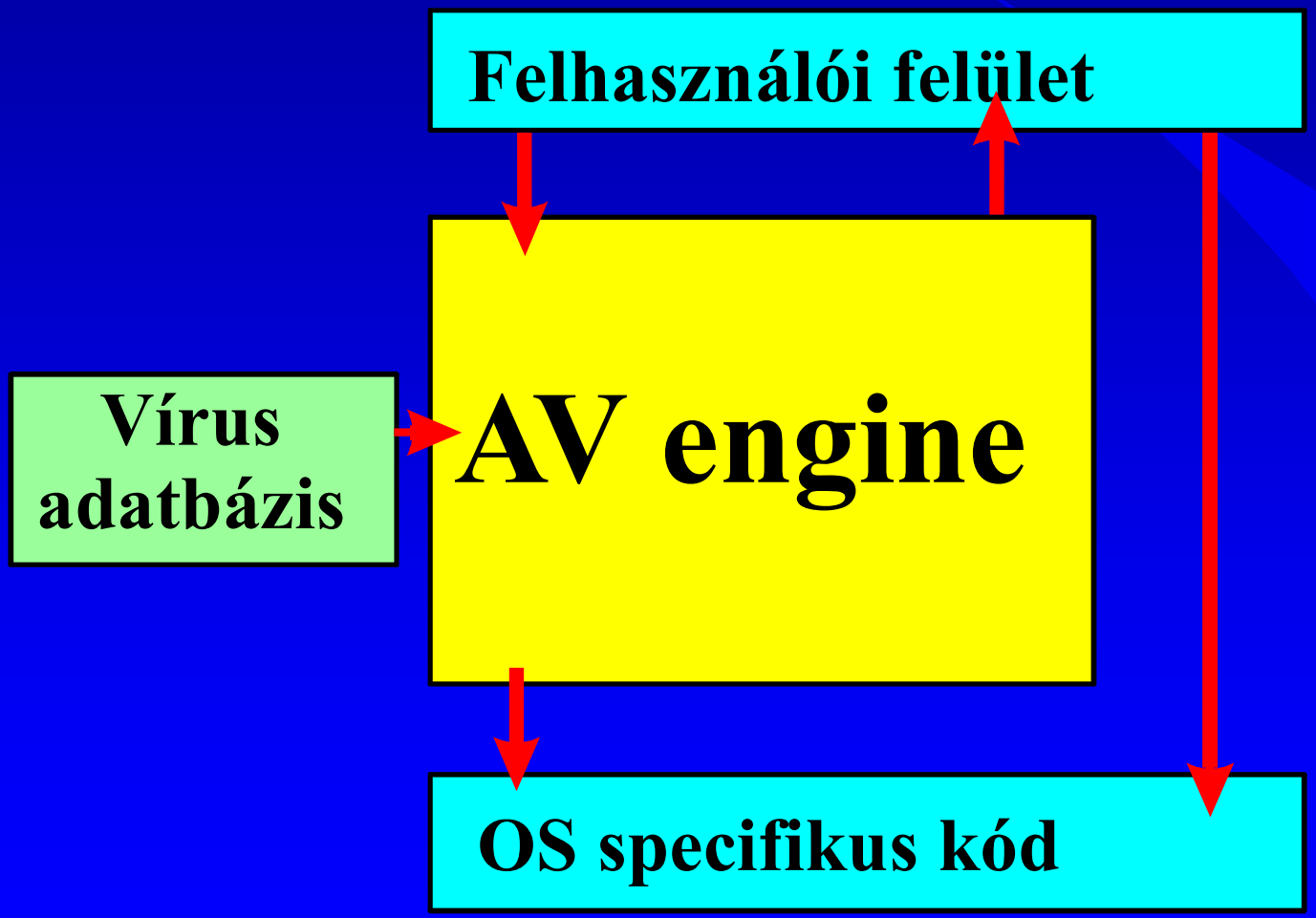
- Nyelvfüggetlen makrók
- NORMAL.DOT fertőzése
- Companion makró vírus
- Futás közben makró létrehozása
- Futás közben titkosítás
- Polimorf makró vírus

Makró vírusok lehetőségei

- Nyelvfüggetlen makrók
- NORMAL.DOT fertőzése
- Companion makró vírus
- Futás közben makró létrehozása
- Futás közben titkosítás
- Polimorf makró vírus
- Lopakodó makró vírus

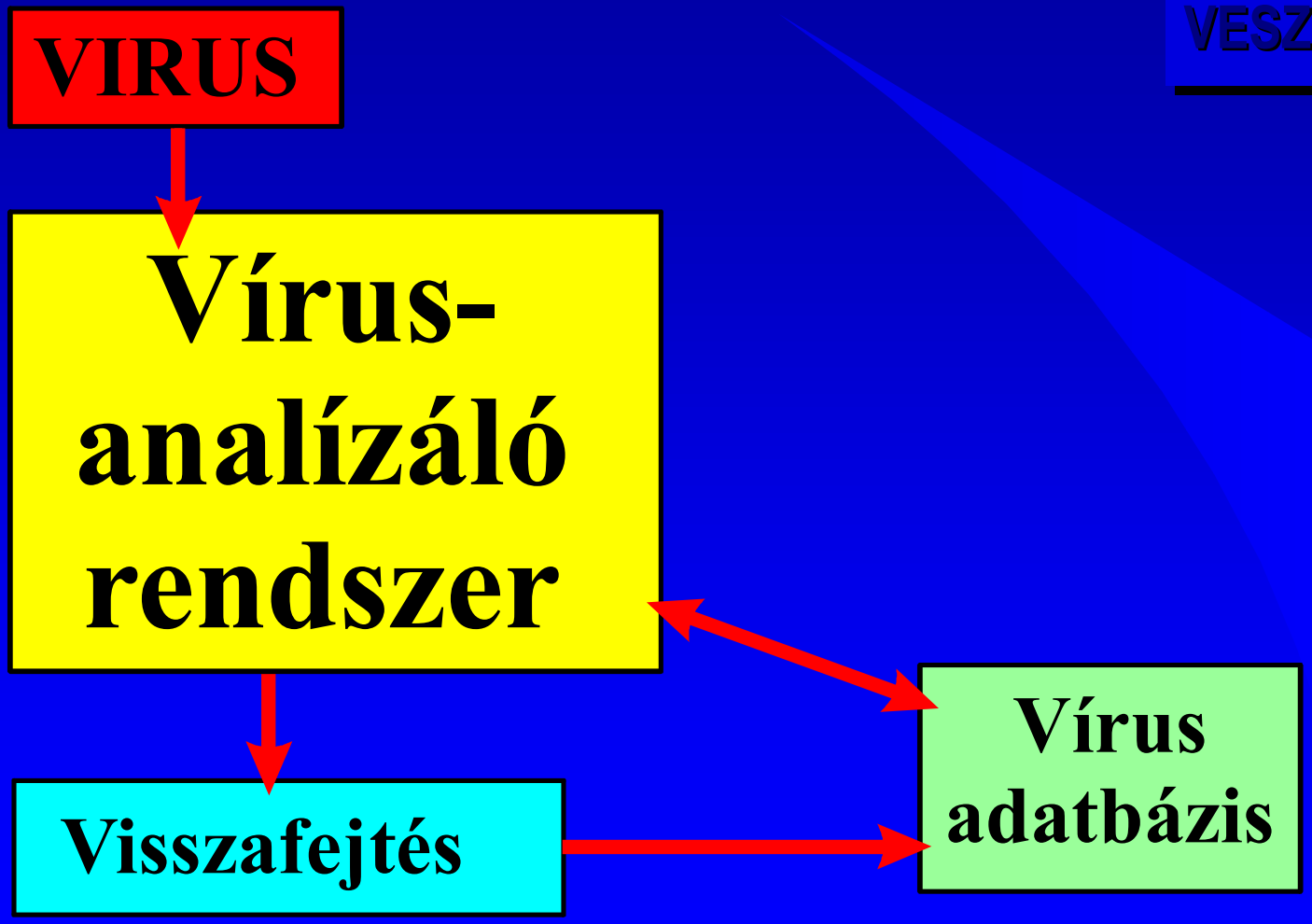
AV programok felépítése

AV programamok felépítése



Vírus adatbázis készítése

Vírus adatbázis készítése



Vírusanalízáló működése

Vírusanalízáló működése

- “Sok” fertőzött példány létrehozása

Vírusanalízáló működése

- “Sok” fertőzött példány létrehozása
- Következtetések levonása

Vírusanalízáló működése

- “Sok” fertőzött példány létrehozása
- Következtetések levonása
- Tesztelés, ellenőrzés

Vírus adatbázis készítése

(automatikusan)

Vírus adatbázis készítése

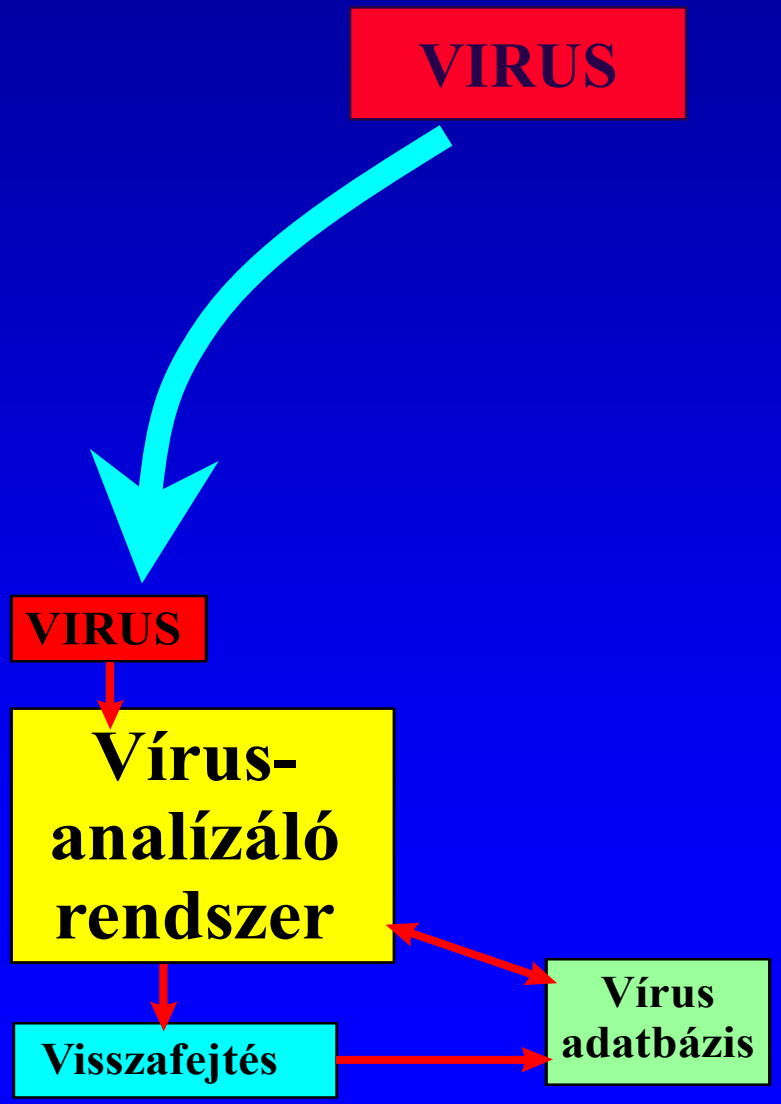
VIRUS

(automatikusan)

Vírus adatbázis készítése

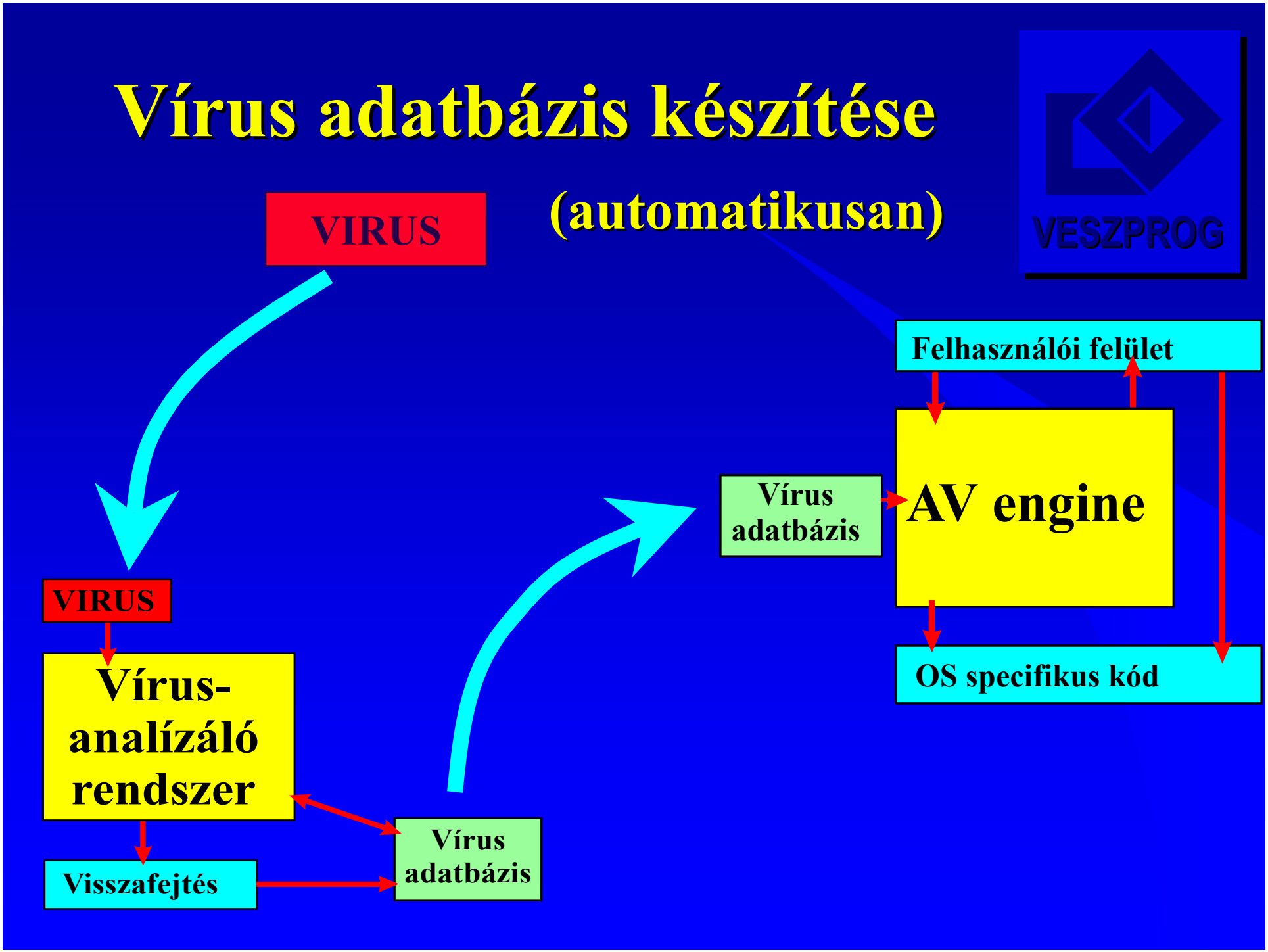
(automatikusan)

VESZPROG



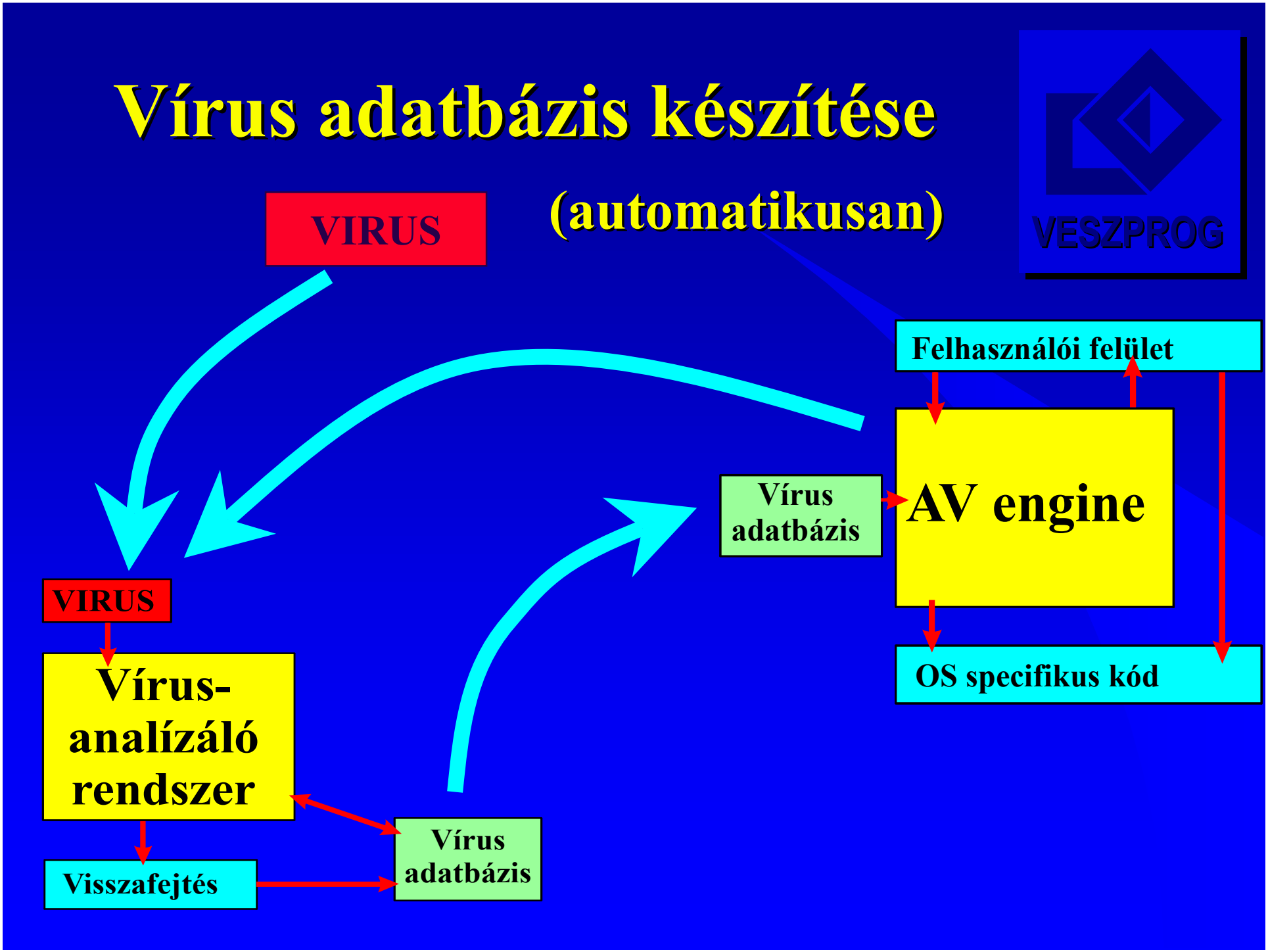
Vírus adatbázis készítése

(automatikusan)



Vírus adatbázis készítése

(automatikusan)



Problémák

Problémák

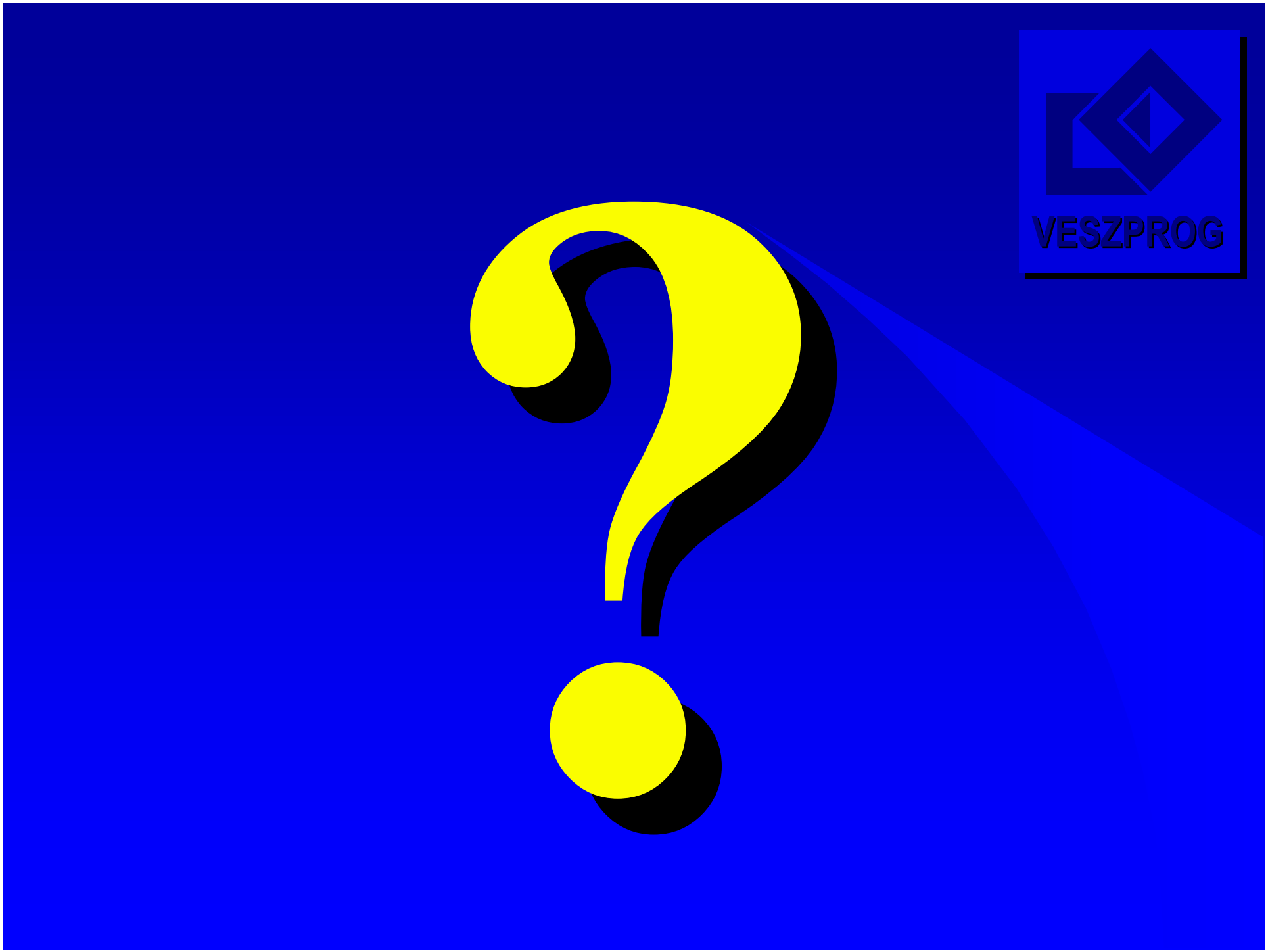
- Új, ismeretlen típusú vírusok

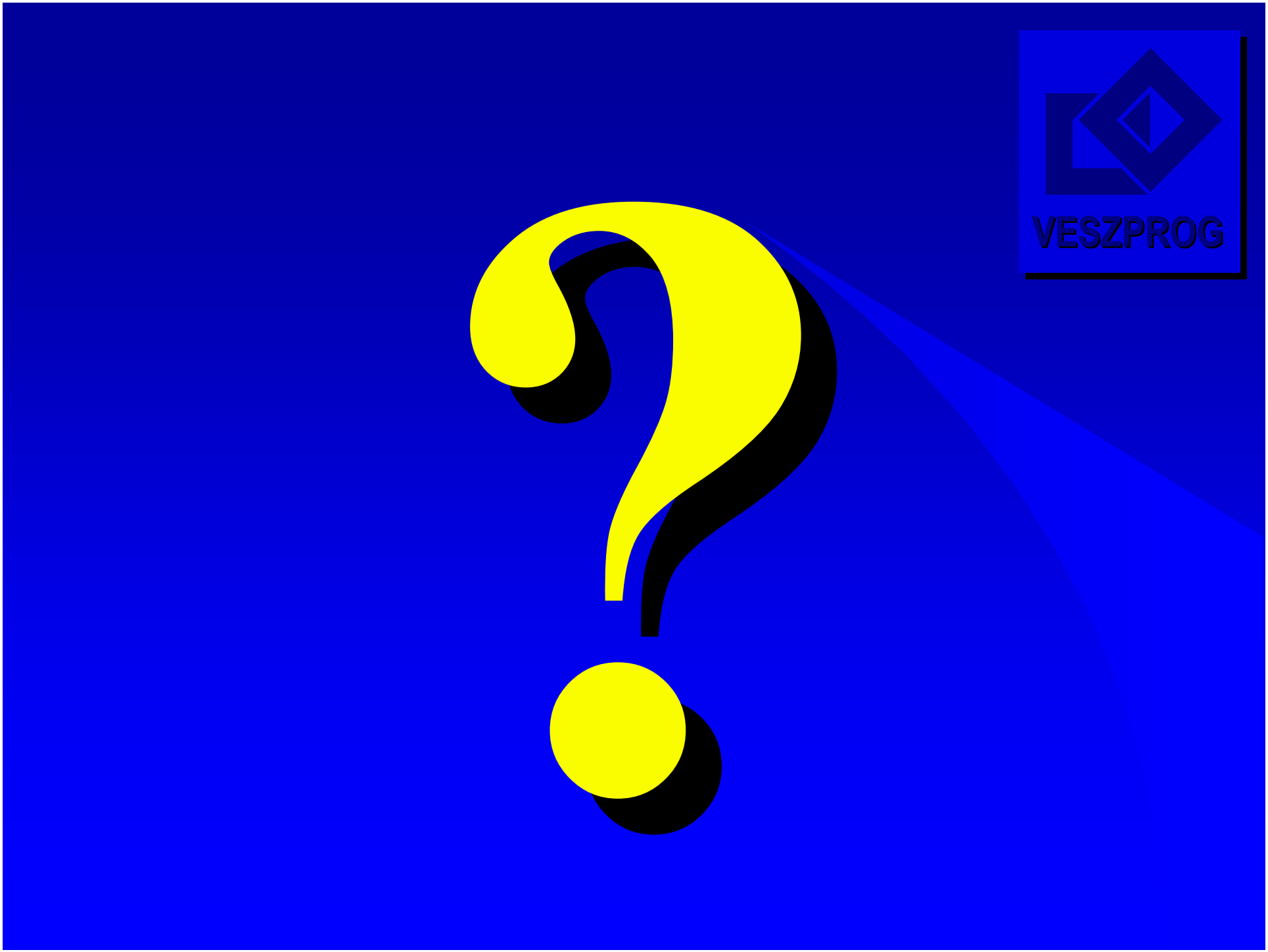
Problémák

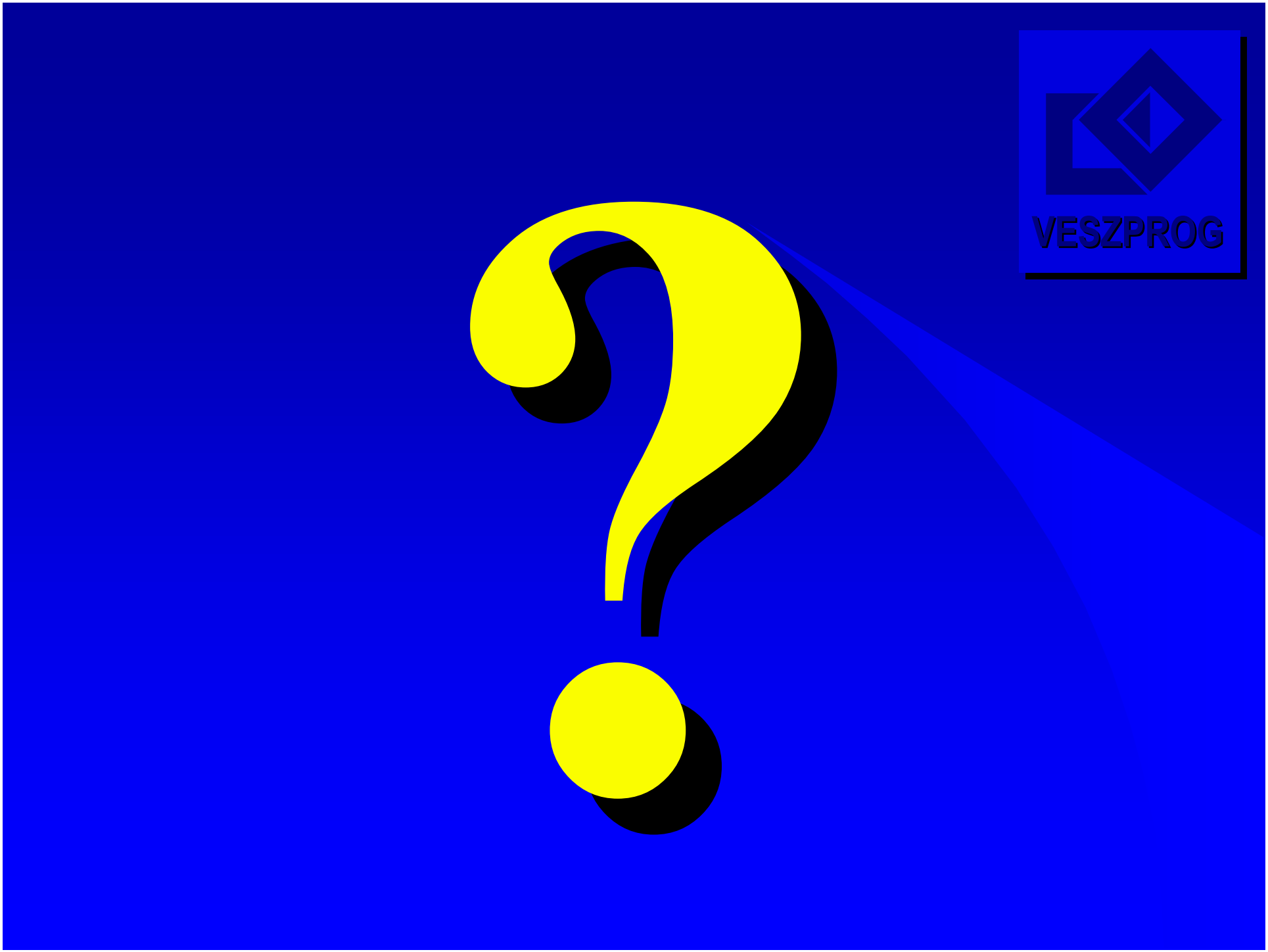
- Új, ismeretlen típusú vírusok
- Vírusanalízáló rendszer hatékonysága

Problémák

- Új, ismeretlen típusú vírusok
- Vírusanalízáló rendszer hatékonysága
- Egyszerre jelentkező “sok” kérés


VESZPROG


VESZPROG


VESZPROG