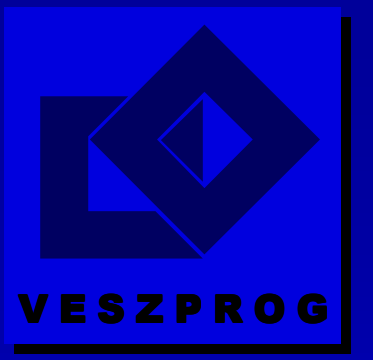
CheckVir Antivirus Testing and Certification



Ph.D. Ferenc Leitold

fleitold@checkvir.com

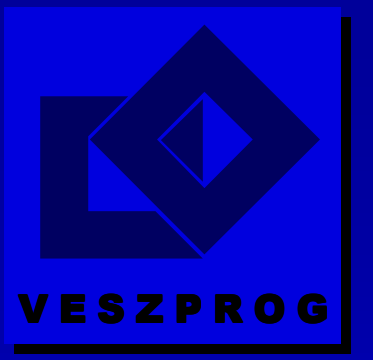
www.checkvir.com

VESZPROG Ltd.

&

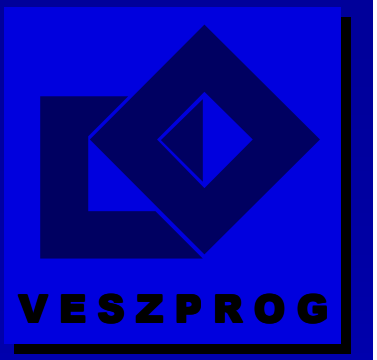
University of Veszprém

Contents



- CheckVir project
- Testing procedures
- Anti-Virus Certification Program
- Certification results
- Future plans

CheckVir project



- **Developing automatic anti-virus testing methods**
  (from the end of 2000)
  - *automatic replicating algorithms for different type of viruses*
  - *automatic procedures for testing AV software*
- **Anti-virus testing monthly**
  (from April 2002)
  - *testing on-access and on-demand scanner on 1 or 2 platforms*
- **CheckVir Anti-Virus Certification Program**
  (from January 2004)
  - *standard and advanced level*

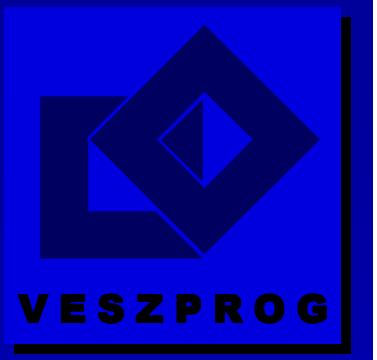
Testing procedures

- Replicating samples
- Classification of samples
- Executing antivirus software
- Result analysis

Replicating samples

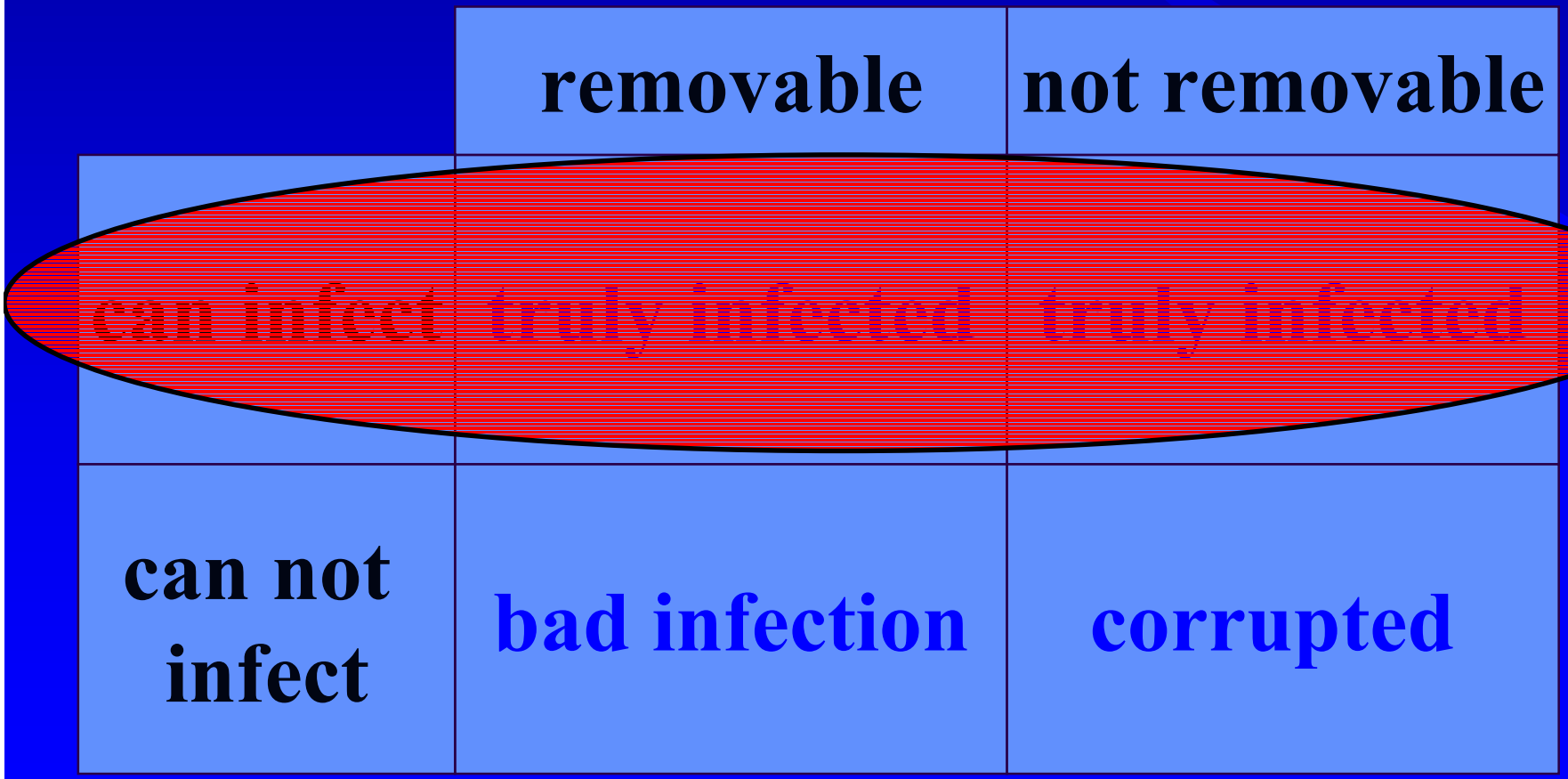
- Using emulator (VMWare, Win4Lin, DOSemu, …)
  - not real environment in some cases
  - easy to control
  - easy to provide the security
- Using native environment
  - real environment
  - difficult to control
  - difficult to provide the security

Classification samples

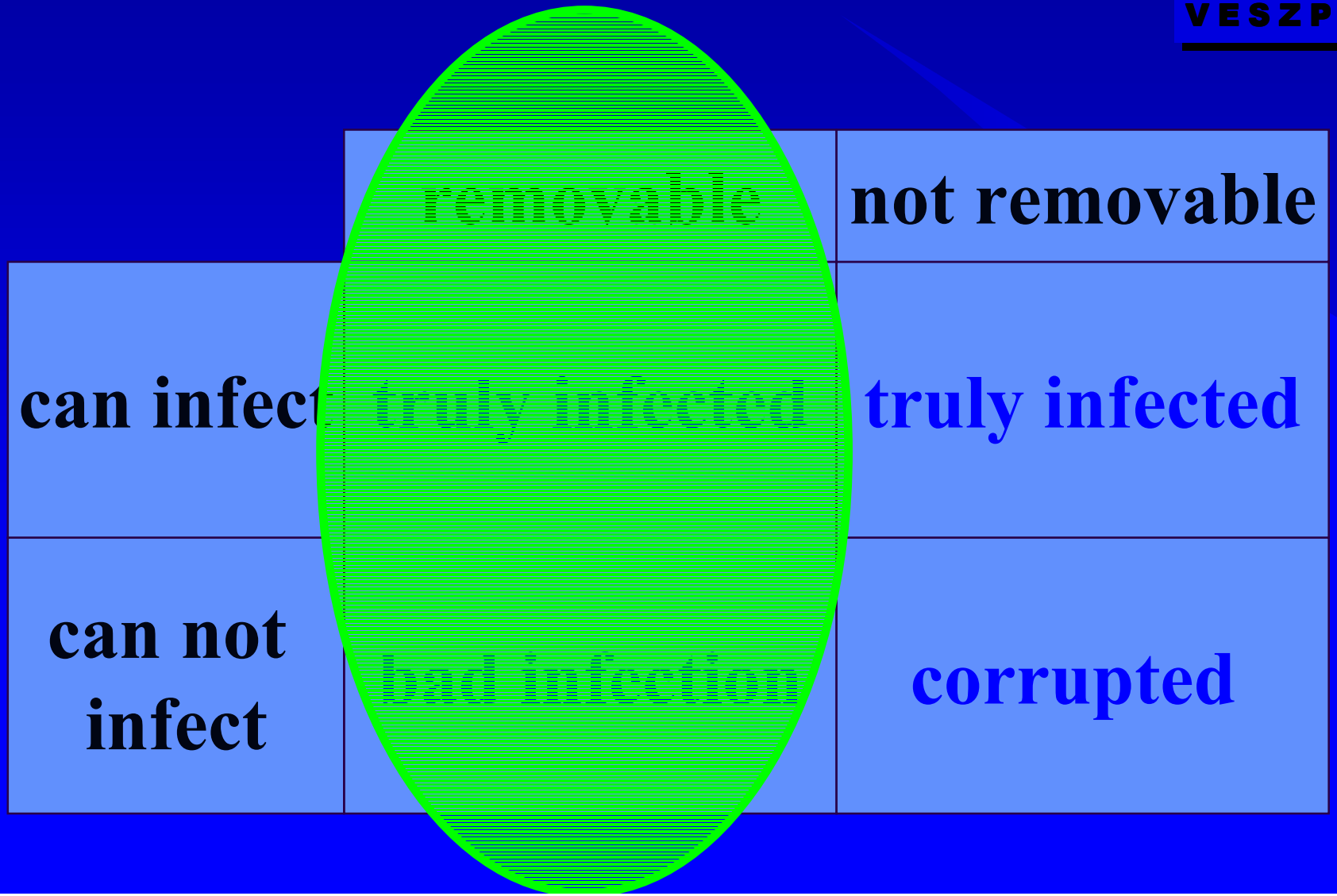


	removable	not removable
can infect	truly infected	truly infected
can not infect	bad infection	corrupted

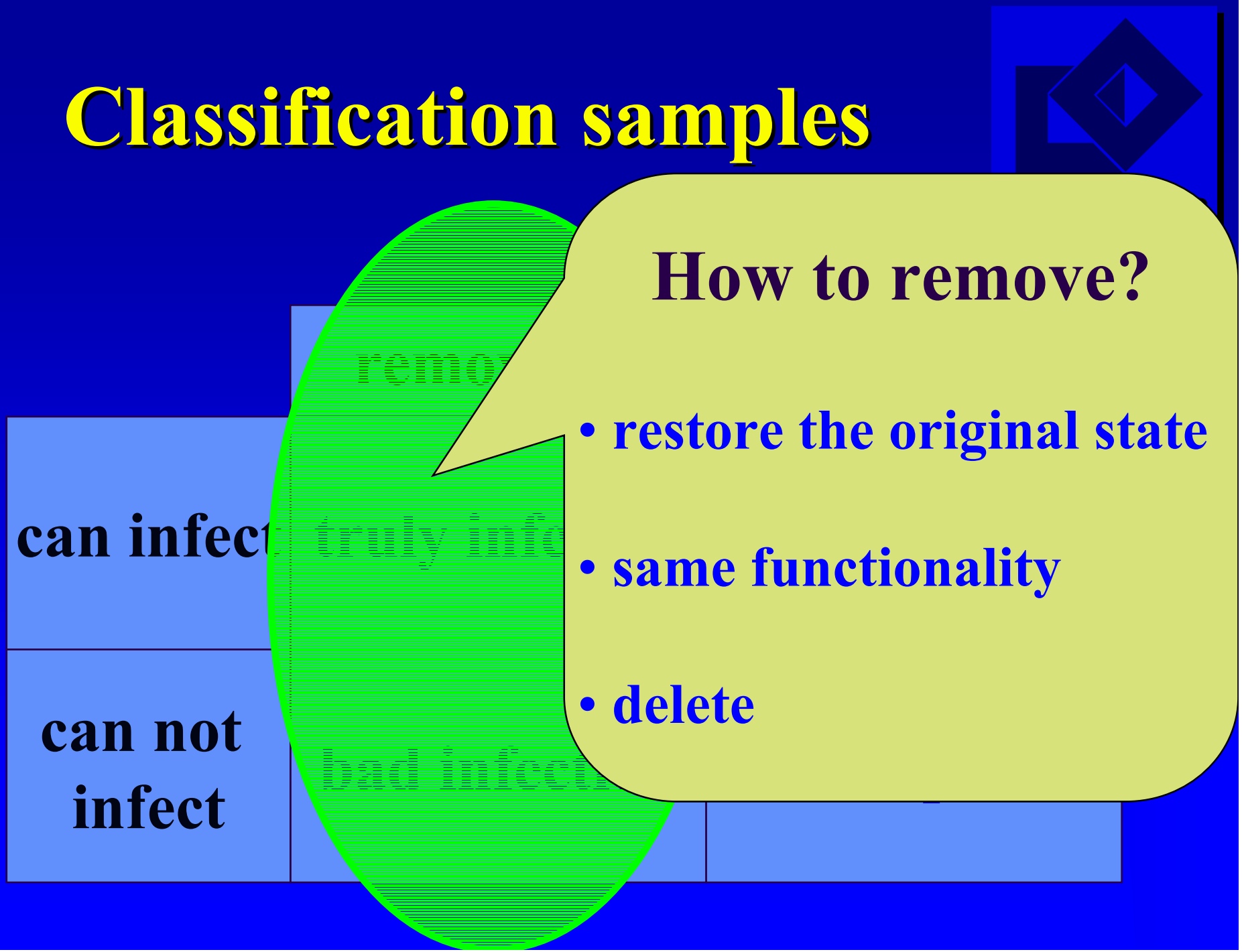
Classification samples



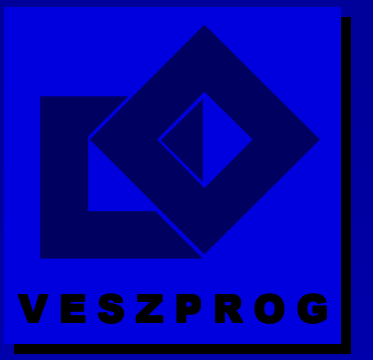
Classification samples



Classification samples

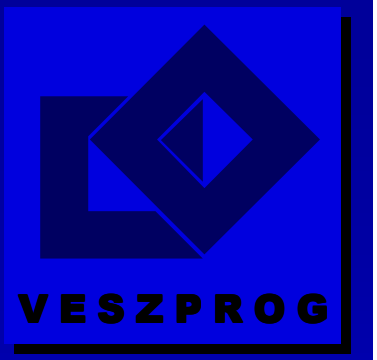


Executing antivirus software



- Different settings:
  - on-access or on-demand scan
  - scan only or scan & kill
  - different options
- Execute in one step or separate the test collection
- Execute in real or in emulated environment

Result analysis



- **Analysis of report files**

  Problems:

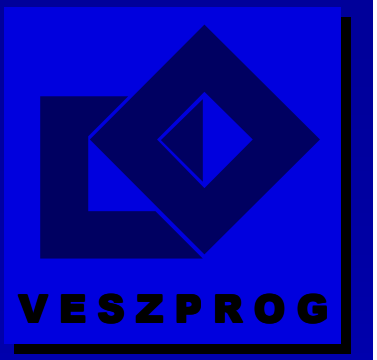
  - **AV has to create and store report file of all events**
  - **difficult to distinguish between delete and kill by delete actions**

- **Analysis of selected action's results**

  Problems:

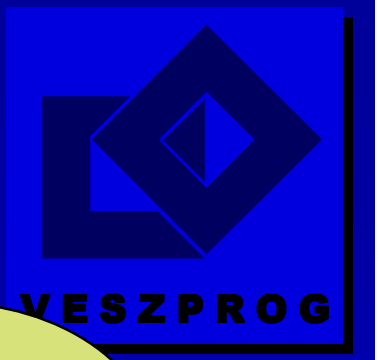
  - **antivirus products have to be executed more times**
  - **different antivirus software – different actions**

Anti-Virus Certification Program



- Certification procedures
  - on-demand scanning
  - e-mail and on-access scanning

Anti-Virus Certification Program

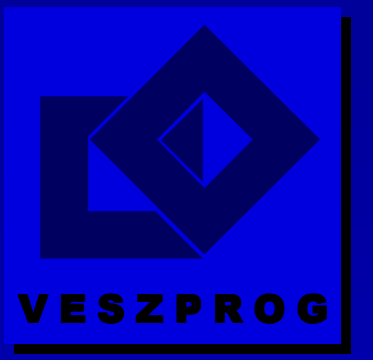


- Certification
  - on-deman
  - e-ma

A product or a set of products may be submitted into the certification program.

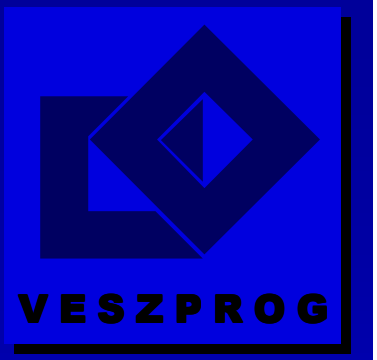
If the case of a set of products then they may receive the certification TOGETHER!

Anti-Virus Certification Program



- Certification procedures
  - on-demand scanning
  - e-mail and on-access scanning
- Virus set -> mix of new and old Wildlist viruses
  - at least 80% from the last 3 months
  - maximum 20% from previous lists
- Deadlines
  - List of used viruses is published on 1st of each month
  - AV products should be submitted by 10th of each month
  - AV products are installed and updated by 15th of each month
  - results are published about 10th of the next month

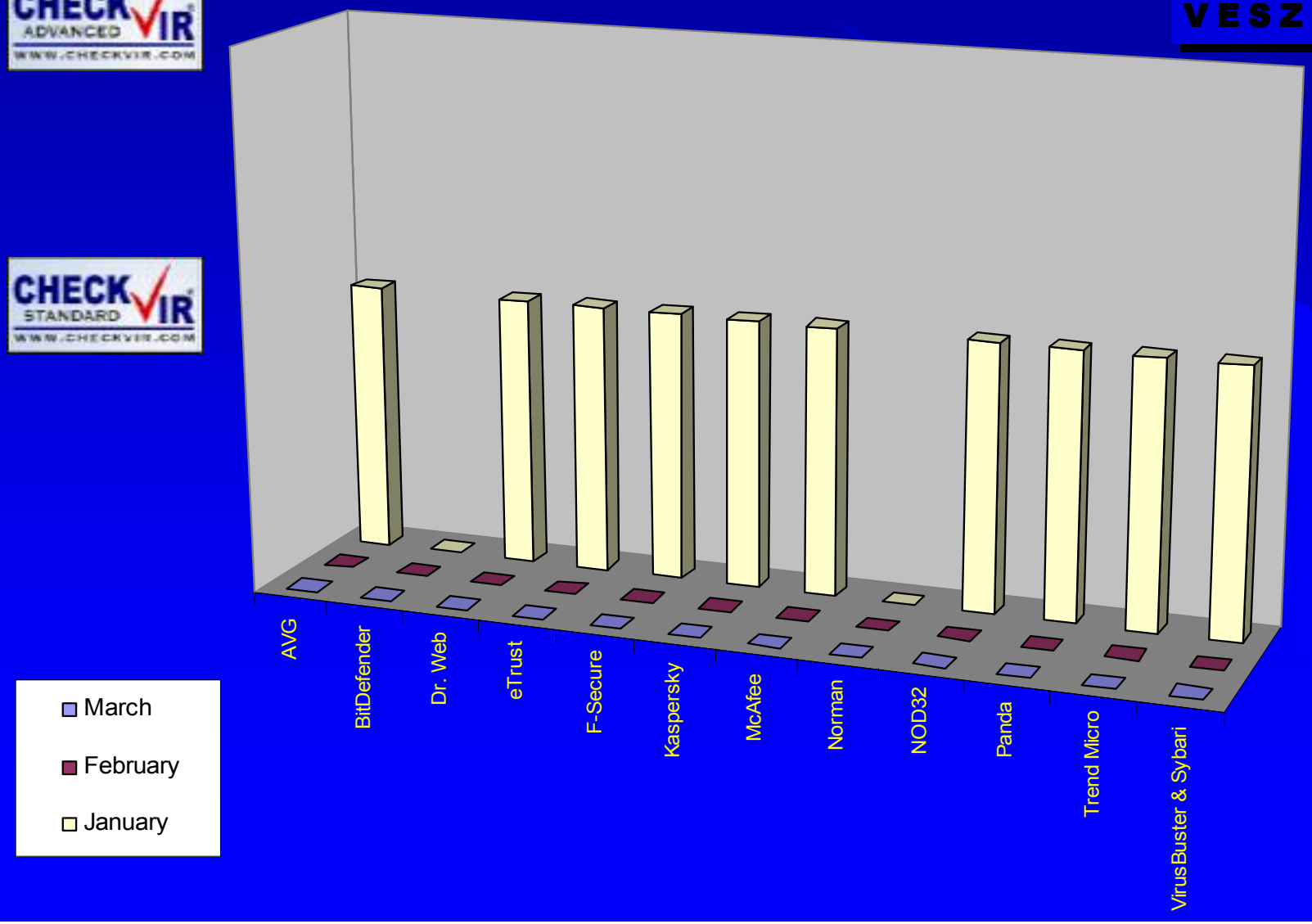
Certification Levels



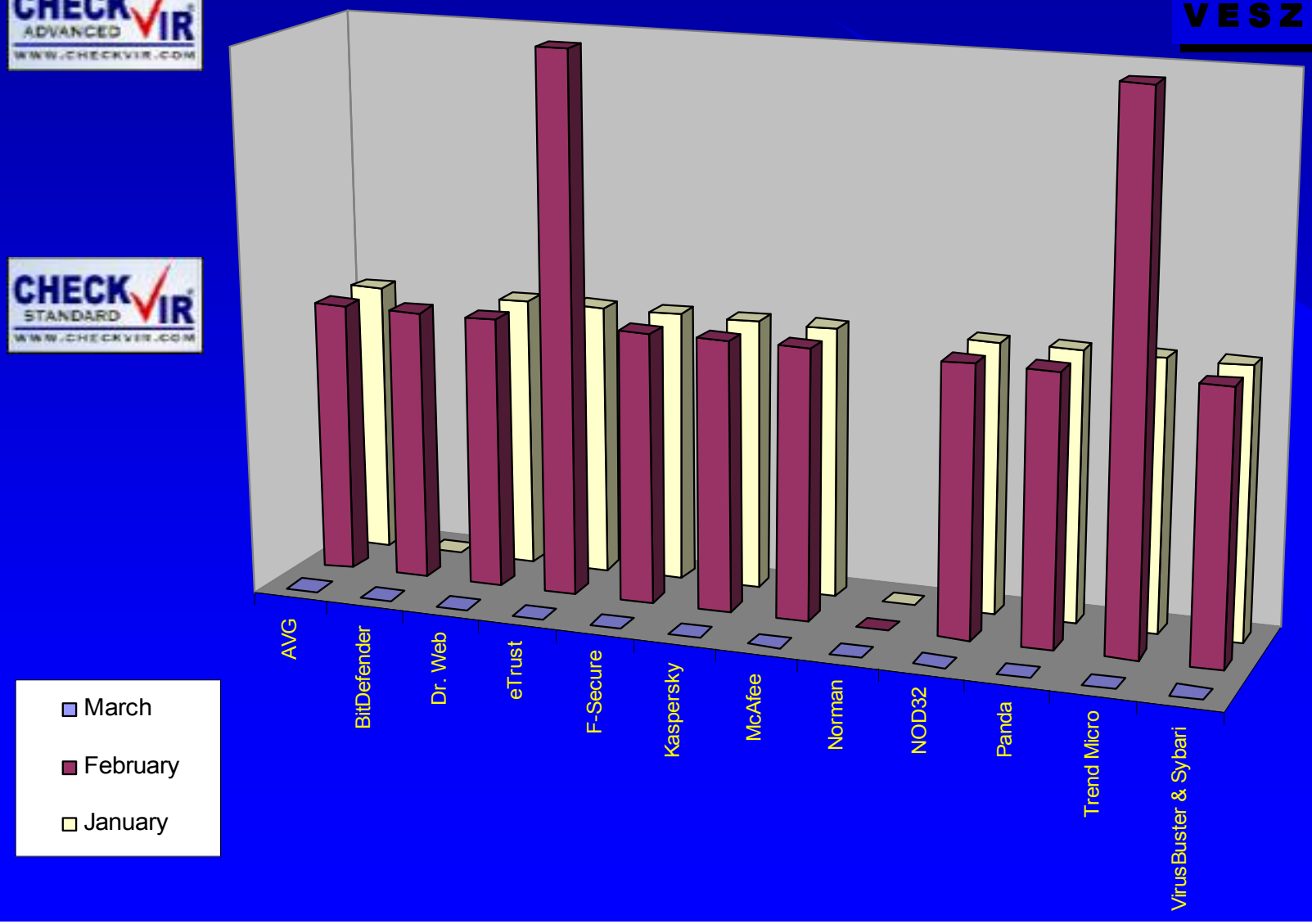
- **Standard Level**
  - Searching capability only
  - Every sample has to be detected

- **Advanced Level**
  - Searching and disinfection capability
  - Virus code has to be erased
  - Disinfected object has to be the same functionality as before infection
  - Loss of information is accepted if the user has been previously informed

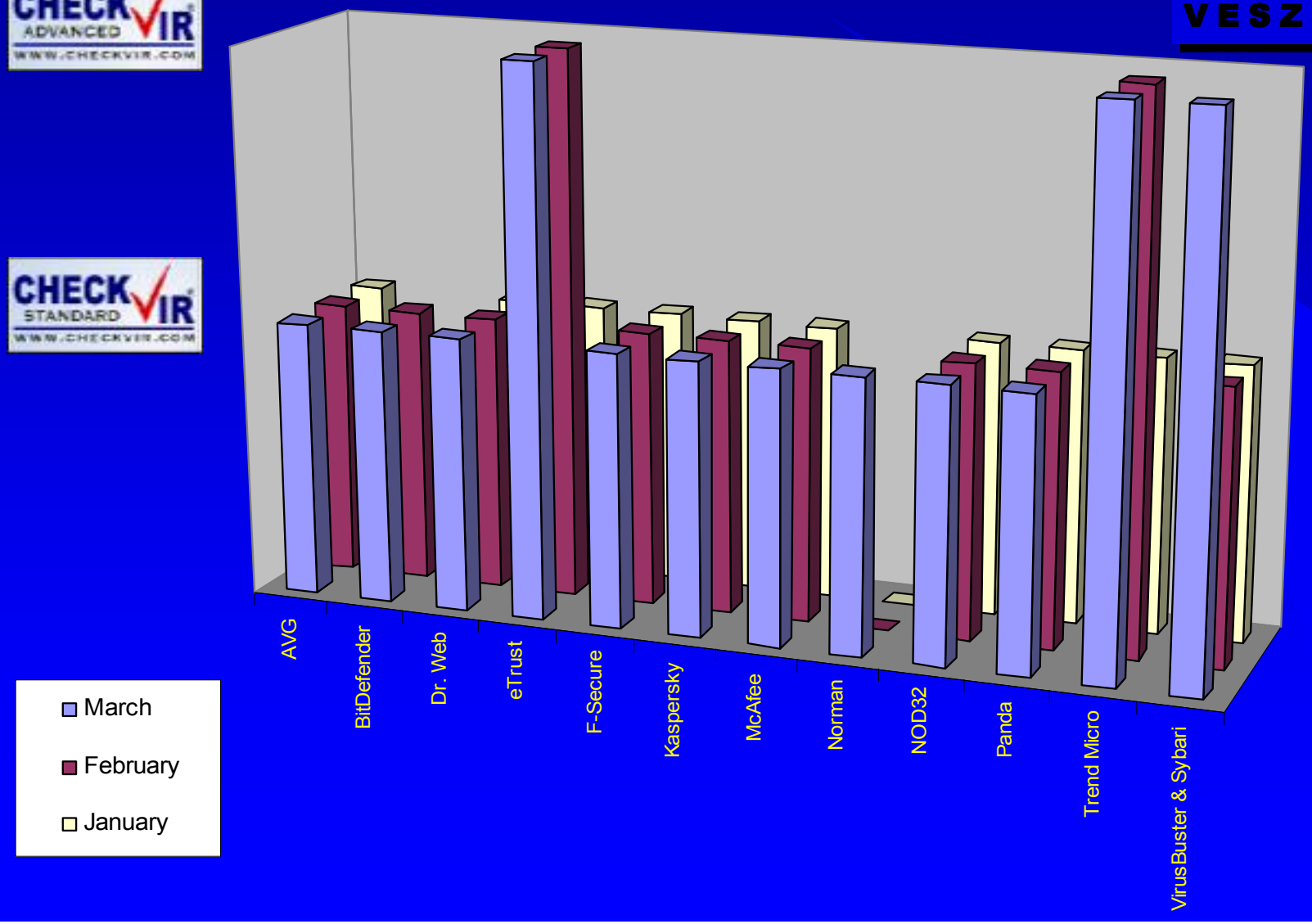
Certification results



Certification results



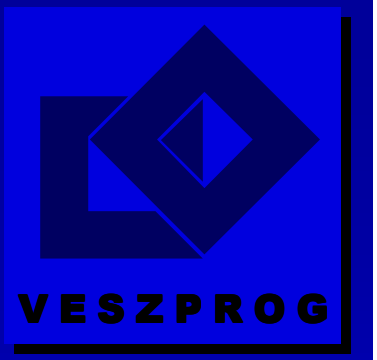
Certification results



Future plans

- **Advanced+ Level (from July 2004)**
  - Restoring capability of the whole system
  - Virus code has to be erased from every infected object
  - System has to be the same functionality as before the infection
  - Modified objects (e.g. registry database) has to be restored

Future plans



- **Real-time AV Testing**
  - Automatic tests
    - if new AV database exists
    - if there is a new widespread virus
  - Automatic analysis of results
  - Automatic publication on

www.checkvir.com


antivirus.hu
checkvir.com
Welcome to the checkvir.com web site,
the home of independent anti-virus testing!
[Actual test - April 2004] [Last closed test - March 2004]
Home
Certification
Tests
Papers
Sending samples
Services
Links
Contact
Legal notice
Anti-Virus Certification Program
During the CheckVir anti-virus testing project the anti-virus certification program has been started at January 2004. On-demand and on-access scanning methods of anti-virus products are tested monthly on various platforms against in-the-wild viruses. More...
During the certification process we use the following viruses:
[April 2004] [May 2004]
About CheckVir project
The main purpose of CheckVir project is testing anti-virus products and solutions independently from developers, helping users and anti-virus companies as well.
Results - March 2004
In March 2004 antivirus products was tested under Windows XP Professional + Outlook Express (client) and under Windows 2000 Server + Exchange 2000 (server) platforms.
The following products received CheckVir STANDARD certification:
CHECKVIR STANDARD WWW.CHECKVIR.COM
Client
-AVG Anti-virus Professional
-BitDefender Professional Edition
-Dr. Web Scanner for Windows
-F-Secure Anti-Virus Client Security
-Kaspersky Anti-Virus Workstation
-McAfee VirusScan Enterprise
-NOD32 Antivirus System
-Norman Virus Control
-Panda Titanium Antivirus 2004
Server
-AVG Anti-Virus 7.0 Email Server Edition
-BitDefender for MS Exchange 2000
-F-Secure Anti-Virus for MS Exchange
-Kaspersky Anti-Virus for MS Exchange Server 2000
-McAfee GroupShield 6.0 for MS Exchange
-NOD32 Antivirus System
-Norman Virus Control v5 for MS

VESZPROG

?