



# Independent AV testing

*Ph.D. Ferenc Leitold*

*fleitold@checkvir.com*

**[www.checkvir.com](http://www.checkvir.com)**

**VESZPROG Ltd.**

**&**

**University of Veszprém**

# Contents



- **CheckVir project**
- **Our viewpoint about testing**
- **Testing procedures**
- **Results**

# CheckVir project



- **Main goals of AV testing**
  - Inform AV users
  - Help AV developers in their work
- **Developing automatic AV testing methods**
  - started at the end of 2000
  - supported by the *Hungarian Ministry of Education, Research and Development Division*
- **Testing plan for 2002 was announced in March 2002**
- **Increasing computing capacity by July 2002**

# Our viewpoint



- We distinguish bugs and problems
- We do **not** count the correct behaviour
- We count only bugs and problems

# Testing procedures



- **Knowledge base tests**
  - Test of scanning and disinfection
  - On-access and on-demand tests
  - Comparing the results of “different usages”
  - False positive test
  - Testing in as real environment as possible
- **Checking the speed of execution**
- **Checking features, support, ...**

# Knowledge base tests



- **Preparing virus samples for test**
- **Installing and executing AV product**
- **Analysing results**

# Virus samples



- **Big number of samples should be replicated**
- **Test sets**
  - ItW test set including **old** and **new** viruses
  - test set for testing the engine capability
- **Which samples should be used ?**
  - only virus samples (can infect other goats) or
  - samples modified by viruses  
(workable infection, bad infection, corrupted)

# Virus samples



- **Big number of samples should be replicated**
- **Test sets**
  - ItW test set including **old** and **new** viruses
  - test set for testing the engine capability
- **Which samples should be used ?**
  - only virus samples (can infect other goats) or
  - samples modified by viruses  
(workable infection, bad infection, corrupted)



# Virus samples

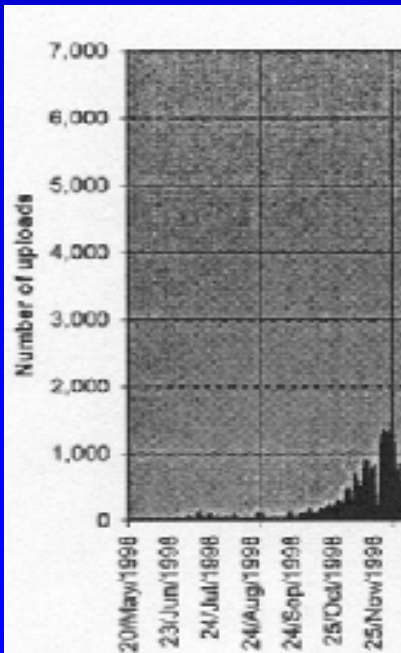
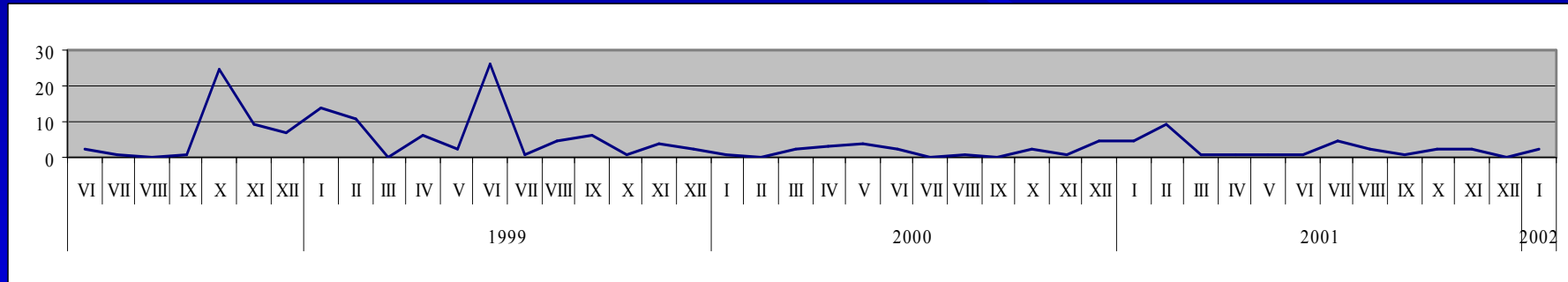
Why should we use old viruses ?





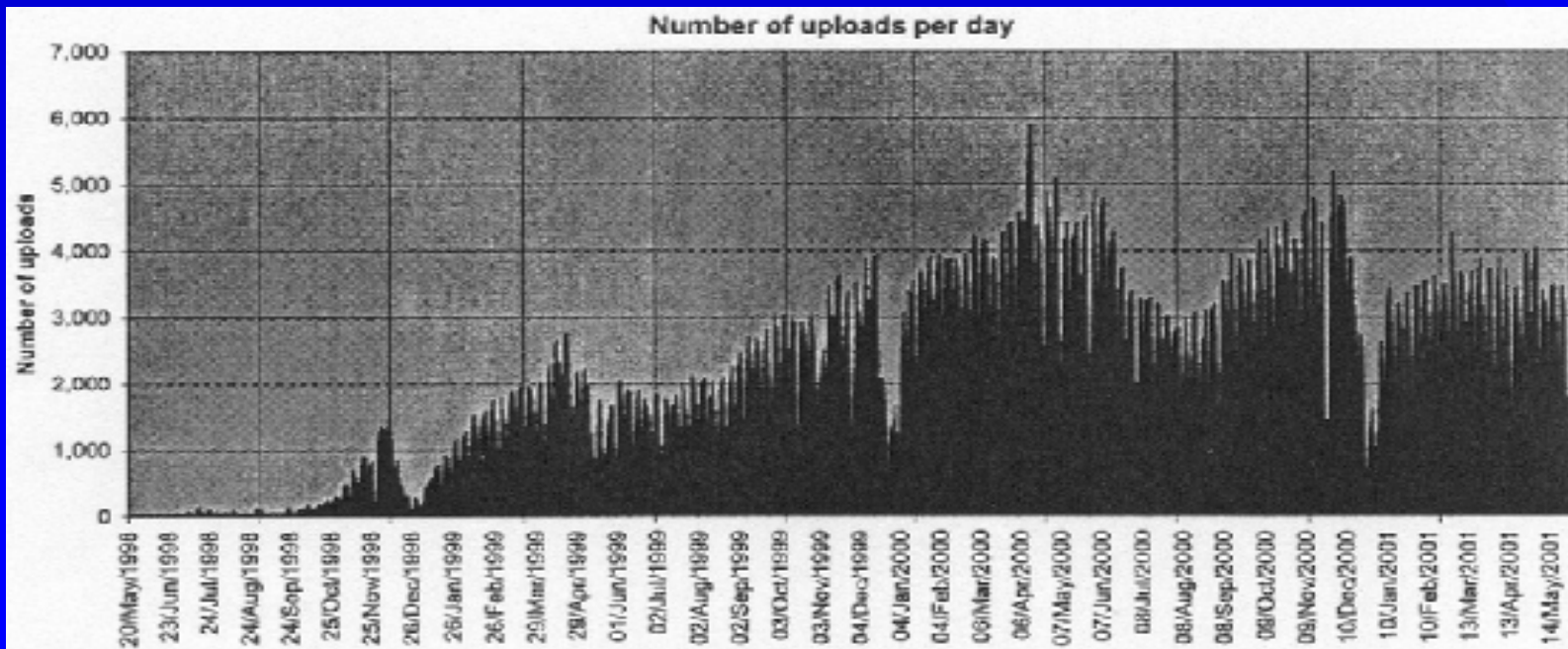
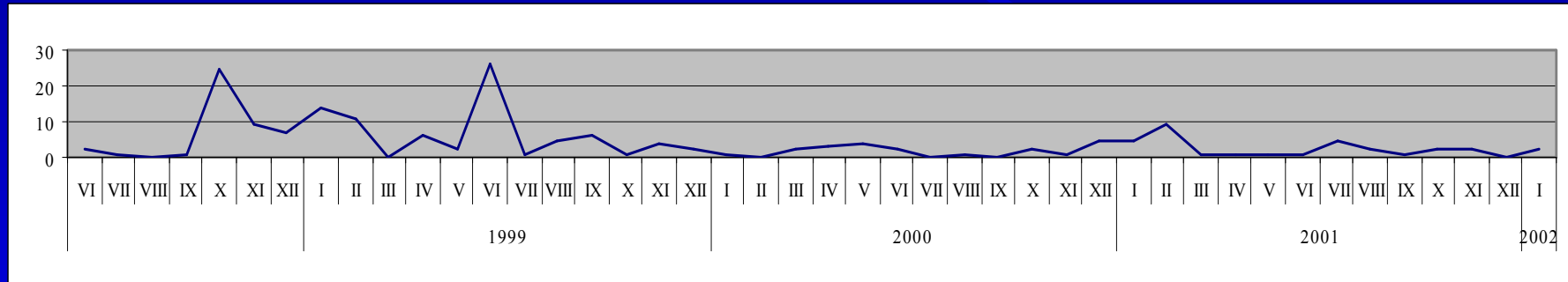
# Virus samples

## Why should we use old viruses ?



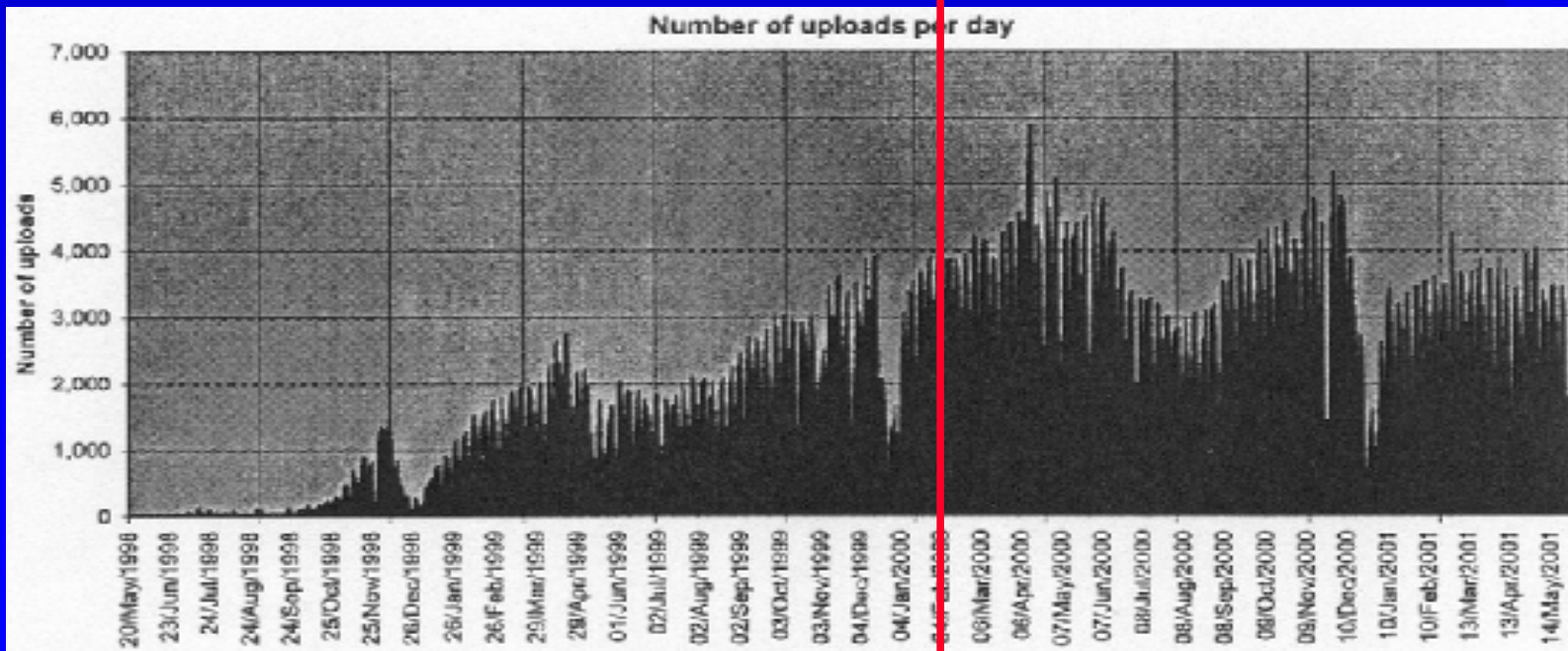
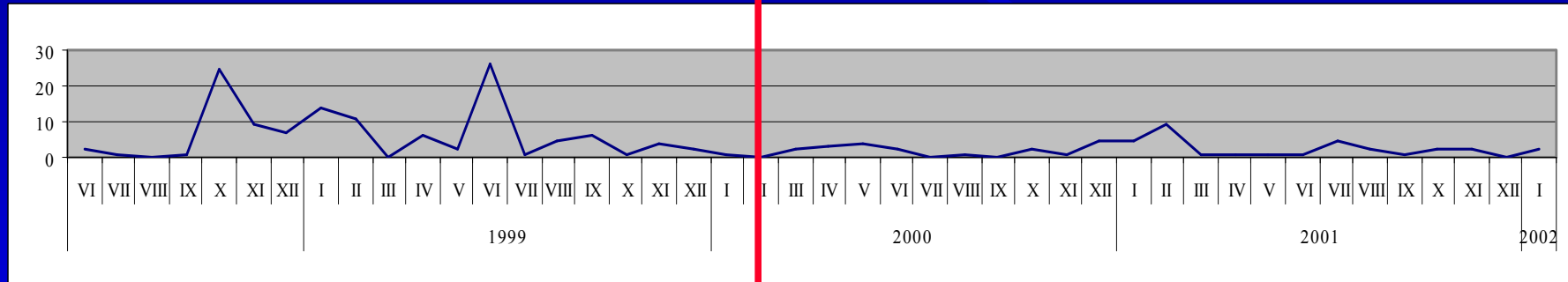
# Virus samples

## Why should we use old viruses ?



# Virus samples

## Why should we use old viruses ?



# Virus samples



- **Big number of samples should be replicated**
- **Test sets**
  - ItW test set including **old** and **new** viruses
  - test set for testing the engine capability
- **Which samples should be used ?**
  - only virus samples (can infect other goats) or
  - samples modified by viruses  
(workable infection, bad infection, corrupted)

# Virus samples

Which samples should be used ?



# Virus samples

Which samples should be used ?



Virulent?	YES	NO



# Virus samples

Which samples should be used ?



Virulent? Repairable?	YES	NO
YES		
NO		

# Virus samples

Which samples should be used ?



Virulent? Repairable?	YES	NO
YES	<b>(non-overwrite viruses) should be detected should be repaired</b>	
NO		

# Virus samples

## Which samples should be used ?



Virulent?	YES	NO
Repairable?	<b>(non-overwrite viruses)</b> <b>should be detected</b> <b>should be repaired</b>	
	<b>(overwrite viruses)</b> <b>should be detected</b>	

# Virus samples

## Which samples should be used ?



Virulent?	YES	NO
Repairable?	<b>(non-overwrite viruses)</b> <b>should be detected</b> <b>should be repaired</b>	<b>(wrong infections)</b> <b>should be detected</b> <b>should be repaired</b>
	<b>(overwrite viruses)</b> <b>should be detected</b>	

# Virus samples

## Which samples should be used ?



Virulent? Repairable?	YES	NO
YES	(non-overwrite viruses) should be detected should be repaired	(wrong infections) should be detected should be repaired
NO	(overwrite viruses) should be detected	(corrupted items) should be detected

# Executing AV product



- **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**

# Analysing results (scanning test)



- **AV should detect all of virus samples (if not -> PROBLEM)**
- **AV should identify the same virus in all of virus samples replicated from the same virus (if not -> BUG)**
- **Results of “different usages” of an AV product should be the same (if not -> BUG)**

# Analysing results (disinfection test)



Disinfected samples



# Analysing results (disinfection test)



**Infected samples**

**Disinfected samples**

**Really disinfected samples**

# Analysing results (disinfection test)



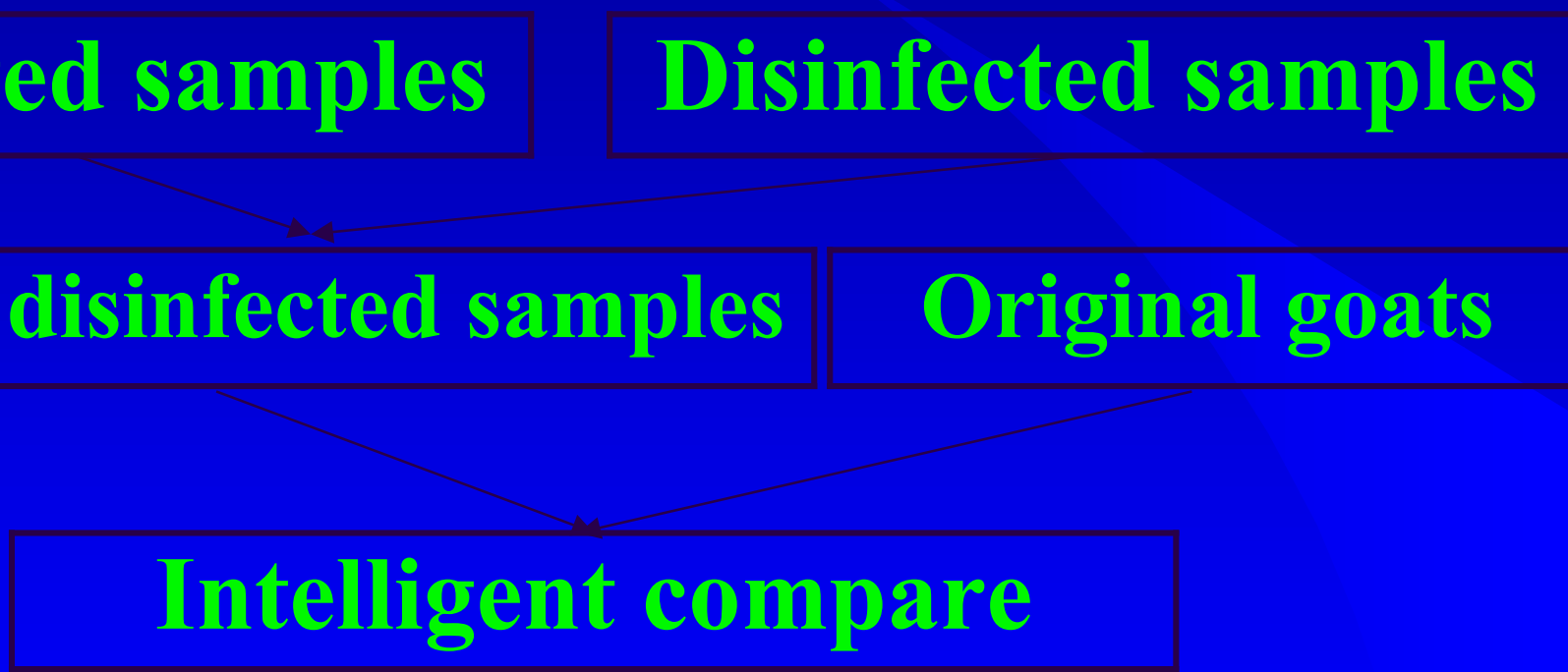
**Infected samples**

**Disinfected samples**

**Really disinfected samples**

**Original goats**

**Intelligent compare**



# Analysing results (disinfection test)



**Infected samples**

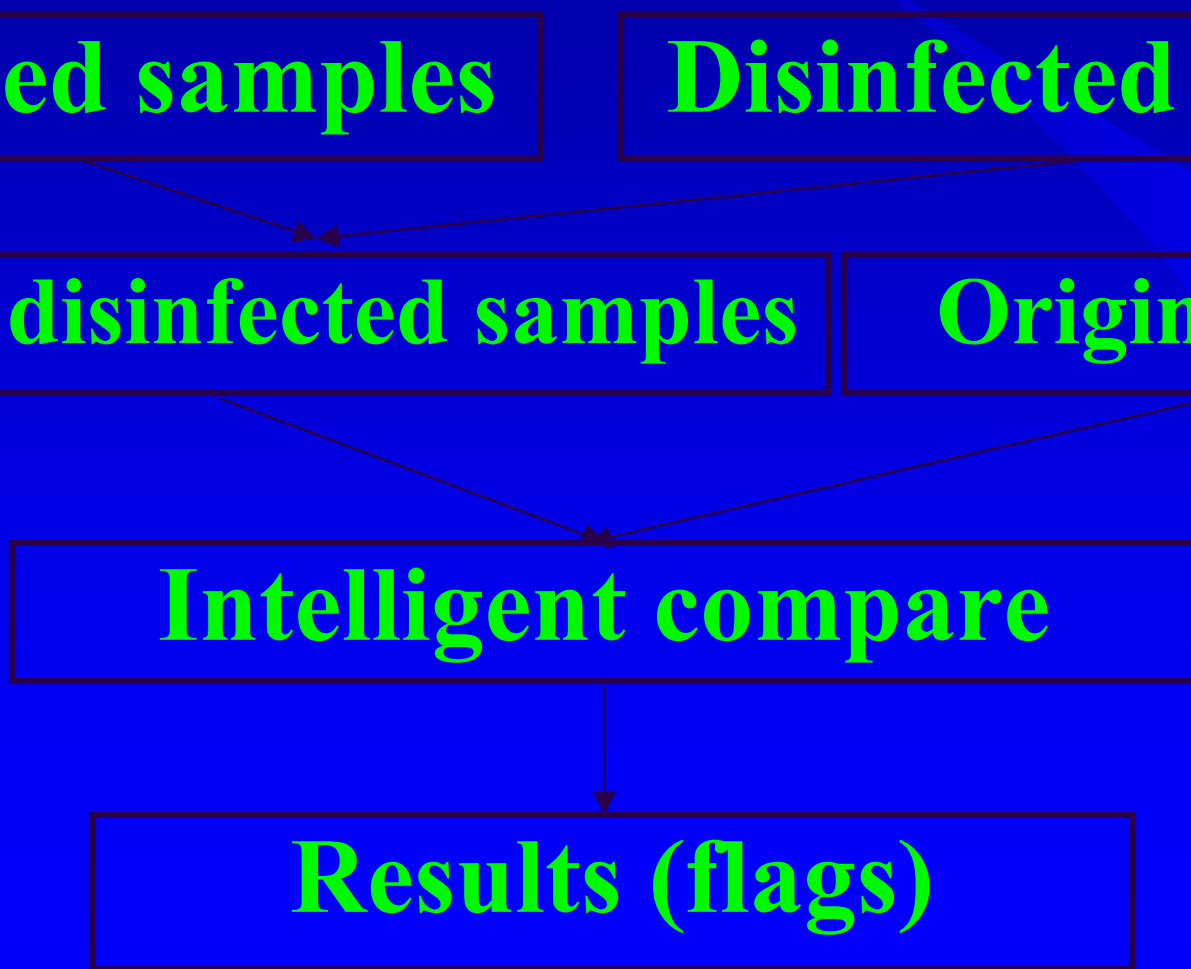
**Disinfected samples**

**Really disinfected samples**

**Original goats**

**Intelligent compare**

**Results (flags)**



# Some interesting results



The screenshot shows the Trend PC-cillin 7.5 interface. A dialog box in the foreground reports "Suche abgeschlossen. Keinen Virus gefunden." (Search completed. No virus found). Below it, a progress bar is at 0%. In the background, another window shows search results for "Infizierte Datei" (Infected file) with a progress bar at 100%. A yellow warning icon is visible next to the text "Suche abgeschlossen. Virus gefunden." (Search completed. Virus found.).

Infizierte Datei	Status
E:\macro\passnhs\00-fj-02\passnhs_.xl	XM_TOTALERA Übergehen
E:\macro\passnhs\00-fj-02\passnhs_.xls	XM_TOTALERA Übergehen
E:\macro\mntjoro\1x-00-02\vk.nwyr~1.xls	XM_TJORO.1 Übergehen
E:\macro\mntjoro\1x-00-02\voksau~1.xls	XM_TJORO.1 Übergehen
E:\macro\mntjoro\1x-00-02\kguenv~1.xls	XM_TJORO.1 Übergehen
E:\macro\mntjoro\00-eg-02\mntjoro_.xls	XM_TJORO.1 Übergehen
E:\macro\abe\00-h-02\tabej_.xl	XM_TABEJ Übergehen

The taskbar at the bottom shows the Start button, several icons, and two instances of "Trend PC-cillin 7.5" running. The system clock shows 6:27 PM.

# Some interesting results



The screenshot shows a Windows 95 desktop with several overlapping windows. In the foreground, a "Hard Disk is Full" dialog box is displayed, with the text: "You have run out of disk space on drive C. To free space on this drive by deleting old or unnecessary files, click Disk Cleanup." Below the text are "Disk Cleanup..." and "Cancel" buttons. Overlapping this is a "Microsoft Visual C++ Runtime Library" error dialog box with a red 'X' icon, containing the text: "Runtime Error", "Program: C:\PROGRAM FILES\DRWEB\DRWEB32W.EXE", and "abnormal program termination". Below the error dialog is a Dr.Web interface window showing a list of files and their actions. The table below is a representation of the data shown in the screenshot.

File Name	Path	Size	Action
crunch-21.com	D:\standard\crunch-21\0...	Cruncher: 4000	Cured
crunch-21.com	D:\standard\crunch-21\0...	Cruncher: 4000	Cured
crunch-21.com	D:\standard\crunch-21\0...	Cruncher: 4000	Cured
crunch-21.com	D:\standard\crunch-21\0...	Cruncher: 4000	Cured

At the bottom of the Dr.Web window, there is a progress bar and a status bar showing "D:\standard\crunch-21\00-ao-03\crunch-21.com" with values "69553" and "28697". The taskbar at the bottom shows the Start button, several icons, and the text "Dr.Web for Windows 95-X...", "Microsoft Visual C++ Ru...", and the time "15:57".

# An interesting result

