CheckVir anti-virus testing and certification

Nikoletta Kárpáti, Veszprog Ltd., Hungary

Ph.D. Ferenc Leitold, Veszprem University - Veszprog Ltd., Hungary

About Authors

Nikoletta Kárpáti graduated from Veszprém University in 2002. Currently she is working for Veszprog Ltd. as project manager. She is dealing with anti-virus testing in the framework of CheckVir project. Her research interest is based on computer viruses: automatic methods for replicating, analysing computer viruses, and testing anti-virus software.

Mailing Address: Nikoletta Kárpáti, Kupa str. 14. H-8200 Veszprem, HUNGARY;

Phone: +36 88 407-285; Fax: +36 88 413-241; E-mail: niki@veszprog.hu; URL: www.checkvir.com

Continued on page 2…

Descriptors

computer virus, anti-virus, anti-virus testing, anti-virus certification, disinfection testing, quality assurance, quality engineering

Reference to, or **Citation** of this paper should be made as follows:
Kárpáti, N. & Leitold, F. (2004). CheckVir antivirus testing and certification. In U.E. Gattiker (Ed.), EICAR 2004 Conference CD-rom: Best Paper Proceedings (ISBN: 87-987271-6-8) 13 pages. Copenhagen: EICAR e.V.

Ferenc Leitold graduated from Technical University of Budapest in 1991. He received his Ph.D. at Technical University of Budapest too, in 1997 in the theme of computer viruses. Currently he teaches in the Department of Information Systems at Veszprem University. He teaches computer programming, computer security, and computer networks. His research interest is based on computer viruses: mathematical model of computer viruses, automatic methods for analysing computer viruses, and testing anti-virus software.

Mailing Address: Ph.D. Ferenc Leitold, Kupa str. 14. H-8200 Veszprem, HUNGARY;

Phone: +36 88 407-285; Fax: +36 88 413-241; E-mail: fleitold@veszprog.hu;

URL: www.checkvir.com, www.fleitold.com

ISBN: 87-987271-6-8

CheckVir anti-virus testing and certification

CheckVir is a project for anti-virus testing which was supported by the Hungarian Ministry of Education, Research and Development Division and by the Hungarian Ministry of Informatics. This antivirus testing project was started in 2001 and from April 2002 testing processes has been executed regularly in each month on different platforms using various sets of virus samples. During the CheckVir anti-virus testing project the anti-virus certification program is started from January 2004. In this paper the summary of this project will be shown as well as the results and experiences of the last two years.

Introduction

Software testers and quality engineers have to test their programs in as many various environments as possible with a lot of input combinations. In the case of anti-virus products, this task is more difficult because the product changes continuously, newer and newer procedures are being built in them. Anti-virus software usually include several thousands of detection and disinfecting algorithms, which should be tested on a great number of virus samples and of course on non-virus files as well.

Usually the following problems occur using anti-virus software:

- The anti-virus software can detect a virus but does not deal with special cases (e.g., too small or too big infected files where the virus usually makes mistake).
- The behaviour of at least two versions of an anti-virus software developed by the same company and working with the same engine are different(e.g., Win95 version of an anti-virus product can detect but the Win2K version of the same product is unable to detect the same virus in the same sample).
- The anti-virus software is able to detect a particular virus but only in some samples (e.g., usually in the case of polymorphic and macro viruses).

ISBN: 87-987271-6-8

- The anti-virus does not correctly wipe all virus-related macros from a document and after infecting this document with another one virus, a totally new macro virus may appear.
- The anti-virus program is unable to distinguish between similar but different viruses. In some of these cases, the program makes mistakes during the disinfecting procedure.
- The anti-virus program is able to correctly disinfect a particular virus but from some samples, however sometimes the result is bad and the disinfected file it cannot be executed.
- Other functional problems (e.g., the anti-virus software hangs up during the disinfection procedure for a particular virus).

In this year Veszprog Ltd. started to develop new automatic and semi-automatic methods solving this problem in the course of a new project. This short documentation highlights the first results of testing in the real environments executed during this project.

Testing algorithms

According to the CheckVir project, we are intended to provide a clear, accurate and reliable testing of anti-virus products. One of the most important expectations about our testing is that every test point has to be reproducible. We submit a problem or a bug if and only if there is a sequence of steps indicating the problem or the bug.

In our tests we distinguish *the problem* and *the bug*. *The problem* means whether a new feature should be developed into the tested product. E.g.: An anti-virus software can not detect a virus or disinfect it. *The bug* means that the behaviour of the tested anti-virus is not correct. E.g.: An anti-virus informs the user that a particular virus has been removed but the cleaned program file is unable to run. The main goal of our test procedures is to radically decrease the number of bugs as well as minimise the number of problems related to anti-virus products.

ISBN: 87-987271-6-8

Testing of anti-virus software is a very delicate matter. Bearing this in mind at the beginning of the project a number of rules were accepted. Some of them are as follows:

- Infected files have to be made by breeding the virus. In this case, the "virus property" of infected files is proved.
- No other application will be installed on the test platform except the anti-virus software.
- Every test has to be repeatable.

Regular Checkvir tests

From April 2002 the Checkvir project provides regular anti-virus testing service. Tests are executed monthly on different platforms. Usually two or more different platforms are used for testing. Thus the results can be compared as well.

Table 1: Test platforms

Month	Platforms
April 2002	Windows 98 Windows 2000
May 2002	Windows Me, DOS Linux
June 2002	Windows NT4 Novell Netware 4.11
July 2002	Windows XP
August 2002	Windows Me
September 2002	Windows 98 Windows 2000

ISBN: 87-987271-6-8

October 2002	Windows ME Windows XP
November-December 2002	Windows 98 Windows XP Home Edition Debian Linux Windows 2000 Server
Janurary 2003	Windows 2000 server + Exchange 2000 Windows 98 + Outlook Express Windows 98 + The Bat!
February 2003	Windows Me Windows XP Home Edition Windows XP Proffessional Edition
March 2003	Windows 98 Debian Linux
April 2003	Windows 98 Windows 2000 Server Windows XP Home Edition
May 2003	Windows Me + MS Office 2000 Windows XP Professional Edition + MS Office XP
June 2003	Windows Me + Outlook Express Windows Me + Outlook Windows Me + The Bat!
July 2003	Windows 98 Windows XP Home Edition
August 2003	Windows Me Windows Server 2003
September 2003	Windows 98 Windows XP Professional Edition
October 2003	Windows 98 Windows XP Home Edition Windows 2000 Server
November 2003	Windows XP Home Edition
December 2003	Windows Me
January 2004	Windows XP Professional Edition

ISBN: 87-987271-6-8

February 2004	Windows 2000 Server
March 2004	Windows 2000 Server + MS Exchange
April 2004	Windows XP Home Edition, Linux
May 2004	Windows Me, Novell Netware 6
June 2004	Windows 2003 Server + MS Exchange

Regular tests are based on virus knowledge test now but other test points will be included in the test in the next 6 months.

During the preliminary test DOS file and boot viruses Windows file viruses, macro viruses and some scipt viruses were used. From April 2002 to August 2002 two virus sets were used for testing: file virus test set (including DOS and Windows file viruses) and macro virus test set (including mainly DOC and XLS viruses). From September 2002 tests are based on the actual Wildlist viruses of previous months as well. In the near future some other test sets will be used during the test (see Future plans).

Anti-virus Certification Program

During the CheckVir anti-virus testing project the anti-virus certification program has been started from **January 2004**. All of anti-virus products that are tested during the CheckVir anti-virus project are participating in the certification process too. There are two different level of certification:

Standard Level: Only the virus searching capability will be examined. The AV software products have to find all of tested virus samples.

Advanced Level: Virus searching and killing capability will be examined. Anti-virus products have to accomplish the conditions of Standard Level and the followings as well:

ISBN: 87-987271-6-8

- The code of virus has to be removed from the infected object in the case of all virus where it can be done theoretically.
- The repaired object is still usable.
- Loss of information during the removing process is allowed, but the user should be informed before it. For example during the remove of a macro virus from the document the AV can remove all of the macros from the document but the user should be informed before it.

During the certification the AV products that match the conditions receive the **"Certified by CheckVir - Standard Level"** or the **"Certified by CheckVir - Advanced Level"** certification.

During the certification process both of **on-demand** and **on-access** scanning are tested only infectious virus samples, – which are published on the Wildlist – are used. The set of virus samples is used for certification is based on the published Wildlist viruses one month prior the testing. At least 80% of the set includes viruses that are published on the last 3 issues of Wildlist. Maximum of 20% of the set may include any virus, which are published on any Wildlist. The list of used viruses are published at least on the 1st of the actual month on the www.checkvir.com website.

Results of the certification procedure including descriptions and summaries are published on www.checkvir.com website before 10th of the next month.

Results

The following systems were used for testing: Intel P4 processor 2 GHz , 512Mb of DDR RAM

The used platform was installed clearly before the testing procedure was executed. After the installation of the operating system only the anti-virus software was installed. The following anti-virus software were tested in the CheckVir project:

ISBN: 87-987271-6-8

Table 2: Tested anti-virus software

Product	Developer
AntiVirusKit	G DATA Software AG
Avast32	ALWIL Trade
BitDefender Professional	Softwin SRL
Dr. Web Anti-Virus	ID Anti-Virus Lab.
eScan	Micro World Technologies Inc.
eTrust Antivirus	Computer Associates
F-Secure Anti-Virus	F-Secure Ltd.
F-Secure Anti-Virus Client Security	F-Secure Ltd.
Kaspersky Anti-Virus	Kaspersky Lab.
McAfee VirusScan	Network Associates
NOD32 Antivirus	ESET Software
Norman Virus Control	Norman ASA
Norton AntiVirus 2002, 2003, 2004	Symantec Corp.
Norton AntiVirus Corporate	Symantec Corp.
OfficeScan	Trend Micro Inc.
Panda Antivirus Titanium	Panda Software
Panda Antivirus Platinum 7	Panda Software
Panda Antivirus Platinum Internet Security	Panda Software
PC Cillin	Trend Micro Inc.
RAV	GeCAD Software
Sophos Anti-Virus	Sophos Plc.
VirusBuster	VirusBuster Ltd.
VirusScan	NAI

ISBN: 87-987271-6-8

EICAR 2004 Conference CD-rom Editor: Urs E. Gattiker

ISBN: 87-987271-6-8

The following table shows some results of our tests:

Table 3: Some results of the testing of August 2003

	Wild list viruses (total 179)	Script viruses (total 3210)	Macro viruses (total 370)	Polymorfic viruses (total 50)
Dr. Web for Windows				
Windows ME	179	2778	364	41
Windows Server 2003	179	2778	364	41
eTrust Antivirus v7				
Windows ME	179	3196	370	49
Windows Server 2003	179	3196	370	49
F-Secure Anti-Virus				
Windows ME	179	3205	369	50
Windows Server 2003	179	3205	369	50
Kaspersky Anti-Virus				
Windows ME	179	3207	368	50
Windows Server 2003	179	3207	368	50
Norman Virus Control				
Windows ME	177	2457	345	46
Windows Server 2003	177	2457	345	46
Norton AntiVirus 2003				
Windows ME	179	3169	368	50
Windows Server 2003	179	3169	368	50
Norton Corporate Edition				
Windows ME	179	3169	368	50
Windows Server 2003	179	3169	368	50
OfficeScan				
Windows ME	179	3175	368	50
Windows Server 2003	179	3175	368	50
Panda Anti-Virus Platinum 7				
Windows ME	179	3176	369	49
Windows Server 2003	179	3176	369	49
Sophos Anti-Virus				
Windows ME	178	3064	365	49
Windows Server 2003	178	3064	365	49
VirusBuster for Windows				
Windows ME	179	3182	369	49
Windows Server 2003	179	3182	369	49

ISBN: 87-987271-6-8

Conclusions

During the execution of our tests the antivirus products were run ont he whole virus se tat the same time. According to this the followings were supposed:

- Antivirus products are able to handle so many (about 100000 – 200000) files.
- Antivirus products can scan such amount of files automatically and they can finish the scan within reasonable time.
- Antivirus products can make a report file about each action executed.

In some cases antivirus products did not meet with these conditions. Some characteristic problems were the followings:

- After scanning some ten thousands of files the speed of execution process decreased radically (about 100 file/hour).
- After finding 65535 virus the antivirus product finished its work.
- Report file did not include all of actions.

The purpose of these tests was not the testing of stability but the testing of virus knowledge. In the mentioned cases testers tried to find a workaround for the purpose of executing the whole tests on each antivirus product.

Using very large number of samples almost all antivirus product missed some of known viruses. It means that testing with a few samples can not give real results. And tests focused on InTheWild viruses only and these are that viruses that antivirus developers process as soon as possible.

According to the test results it can be seen that the numbers of missed samples are higher than the numbers in the case of detecting. However there are viruses that can not disinfect correctly.

ISBN: 87-987271-6-8

References

Gordon, S.; Howard F. (2000). Antivirus Software Testing for the New Millenium. Proceedings of the 23rd National Information Security Conference, Baltimore USA, 2000.

Leitold, F. (1995). Automatic Virus Analyser System. Proceedings of the 5th International Virus Bulletin Conference, Boston USA, 1995, pp. 99-107.

Leitold, F. (2002). Independent AV testing. Proceedings of the 11th International EICAR Conference, Berlin Germany, 2002.

Marx, A. (2000). A Guideline to Anti-Malware-Software testing. Proceedings of the 9th International EICAR Conference Brussels Belgium, 2000.

ISBN: 87-987271-6-8