Experiences of CheckVir AV Testing

Ph.D. Ferenc Leitold

Veszprem University - Veszprog Ltd., Hungary

About the Author

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 30 9599-486; Fax: +36 88 413-241; E-mail: fleitold@veszprog.hu;

URL: www.checkvir.com

Descriptors

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

Reference to this paper should be made as follows

Leitold, F. (2003). Experiences of CheckVir AV Testing. In U.E. Gattiker (Ed.), EICAR Conference Best Paper Proceedings (ISBN: 87-987271-2-5) 10 pages. Copenhagen: EICAR.

Experiences of CheckVir AV Testing

Abstract

CheckVir is a project for anti-virus testing. ***Starting of this project was supported by the Hungarian Ministry of Education, Research and Development Division (IKTA-00033/2000).*** *The purpose of these tests is not the ranking of anti-virus softwares. The results of these tests do not claim that an anti-virus product is better than another. Of course we cannot claim that any anti-virus product works totally correctly or it has not got any mistake. The test results indicate only that there are a number of cases or there are no cases where the tested anti-virus software fails on the tested environment against the used virus samples. The main goal of these tests is that the results of the tests published on this web site help users in the fight against viruses, help anti-virus developers in their work and the anti-virus products become better and free from bugs.*

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).
- 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.

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.

Testing phases

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:

The testing procedures include the following steps:

- Anti-virus products have to be sent to Veszprog Ltd. CheckVir team by post or e-mail. Alternatively, by arrangement, products can be downloaded from the developer's FTP or HTTP site.
- The products will be tested according to the principles and the published test specification.

- Statistical results will be published and sent back to the developer. Also, by arrangement, the developers receive the whole test results including all information to reproduce the problems and bugs.

Test specification

Anti-virus testing includes the following steps:

1. After the list of used viruses for the test has been published, the viruses are replicated.
2. On-access and on-demand scanning of anti-virus products are tested for scanning only. Report files are generated and they have to include the same information. The results have to chime in with the following criterions:
    - The anti-virus product has to detect viruses in all of the infected samples.
    - The anti-virus product has to give the same virus name to the viruses that are replicated from the same infected source file.
    - If the anti-virus product detects none of the replicated samples from the same infected source file, then it is a **problem**, but **NOT a bug!**
    - If some of the replicated samples from the same infected source file is detected by the anti-virus product, but some of them are not then, it is a **bug**, and **NOT a problem!**
    - The anti-virus products of the same developer with the same scanning engine and using the same database and the same settings have to detect the same virus in the same virus sample.
    - Different methods of an anti-virus product (e.g.: on-access and on-demand) have to detect the same virus in the same virus sample (using the same settings).
3. On-access and on-demand scanning of anti-virus products are tested for disinfection. Report files are generated and they have to include the same information. Results have to chime in with the following criterions:
    - If an infected item is disinfected according to the report file then it has to be disinfected. If it is not then this is a bug.
    - If an infected item is NOT disinfected according to the report file then it has to be unchanged. If it is not then this is a bug.
    - If an infected item has to be disinfected then it can not infect other items any more.
    - If an infected item has to be disinfected then it can not be suspected by other anti-virus products. If this is not true then it is a bug of one or other product.

- If an infected item has to be disinfected then it has to be fully workable, it has to be used without hanging or crashing the machine or any subsystem of it. If this is not true then it is a bug.

- If a file infected with a macro virus has to be disinfected then it has NOT to leave all macros which were previously in the original file. An anti-virus product may clear all of macros of the document file but the user has to be informed about it. If the user is not informed then it is a problem.

- Disinfecting by anti-virus products of the same developer with the same scanning engine, using the same database and using the same settings has to produce the same disinfected items.

- Different methods of an anti-virus product (e.g.: on-access and on-demand) have to produce the same disinfected items (using the same settings).

4. Anti-virus products are tested using non-infected items. With the aid of this test the false positives are checked.

5. At the end of the testing the features of the product are tested and summarised. According to the installation the following features are checked:

    - Is there any possibility to select the directory where the product will be installed?

    - Can the product detect whether a previous version of the product has been installed?

    - Can the product detect whether another anti-virus product has been installed?

    - Can the product create *Emergency disk*?

    - Does the user have to restart the system after the installation?

According to the on-access and on-demand scanning the following features are checked:

- Is there any possibility to set the extensions for checking?

- What are the known compressed file formats?

- Can the product check files compressed by multiple times?

- Can the product check e-mails?

- What are the supported mailing softwares?

- What are the possibilities if a virus found?

- Which languages are supported?

According to the support of the product the followings are checked:

- What are the possibilities for upgrading the database and/or the engine?
- Is there any possibility for central management?
- Is there any possibility for schedule test(s)?
- Is there any newsletter about the product?
- What kind of information can be received by the newsletter?

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.

April 2002	In April anti-virus products for **Windows 98** and **Windows 2000** are invited.
May 2002	In May anti-virus products for **Windows Me**, **DOS** and **Linux** are invited.
June 2002	In June anti-virus products for **Windows NT4** and **Novell Netware 4.11** are invited.
July 2002	In July anti-virus products for **Windows XP** are invited.
August 2002	In August anti-virus products for **Windows Me** are invited.
September 2002	In September anti-virus products for **Windows 98** and **Windows 2000** are invited.
October 2002	In October anti-virus products for **Windows ME** and **Windows XP** are invited.

Table 1: Test platforms.

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

Virus test sets

During the preliminary test DOS file and boot viruses Windows file viruses, macro viruses and some script 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 of the previous month. In the near future some other test sets will be used during the test (see Future plans).

Results

Tests were run from April to October 2001. 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:

Product	Developer
AntiVirusKit	G DATA Software AG
Avast32	ALWIL Trade
Dr. Web Anti-Virus	ID Anti-Virus Lab.
eScan	Micro World Technologies Inc.
eTrust	Computer Associates
F-Secure Anti-Virus	F-Secure Ltd.
Kaspersky Anti-Virus	Kaspersky Lab.
McAfee VirusScan	Network Associates
Norton AntiVirus 2002, 2003	Symantec Corp.
Norton AntiVirus Corporate	Symantec Corp.
Panda Antivirus Titanium	Panda Software
RAV	GeCAD Software
Sophos Anti-Virus	Sophos Plc.
VirusBuster	VirusBuster Ltd.

Table 2: Tested anti-virus software

The following table shows the results of the test of October in case of detection and disinfection as well:

	Unknown viruses	*Detected correctly*	*Some samples found, some not*	*Disinfected all*	*Some samples disinfected, some not*	*Unable to disinfect*
AntiVirus Kit						
Windows ME	0	171	1	89	13	70
Windows XP	0	171	1	89	13	70
Avast32						
Windows ME	0	171	1	77	3	92
Windows XP	0	170	2	74	6	92
Dr. Web						
Windows ME	0	170	2	89	13	70
Windows XP	0	170	2	89	13	70
eScan						
Windows ME	0	170	2	88	14	70
Windows XP	0	170	2	88	14	70
F-Secure Anti-Virus						
Windows ME	0	169	3	92	17	63
Windows XP	0	169	3	92	17	63
Kaspersky Anti-Virus						
Windows ME	0	169	3	88	14	70
Windows XP	0	169	3	88	14	70
McAfee VirusScan						
Windows ME	0	171	1	90	68	14
Windows XP	0	171	1	90	68	14
Norton AntiVirus 2002						
Windows ME	0	172	0	87	13	72
Windows XP	0	172	0	87	13	72
Norton AntiVirus Corporate						
Windows ME	0	172	0	n/a	n/a	n/a
Windows XP	0	172	0	n/a	n/a	n/a
Panda Antivirus Titanium						
Windows ME	1	168	3	161	8	2
Windows XP	1	168	3	161	8	2
RAV						
Windows ME	0	166	6	85	5	82
Windows XP	0	166	6	85	5	82
Sophos Anti-Virus						
Windows ME	0	169	3	87	9	76
Windows XP	0	169	3	87	9	76
VirusBuster						
Windows ME	0	169	3	97	42	33
Windows XP	0	169	3	97	42	33

Table 3: Test results of the testing October 2002

Conclusions

During the execution of our tests the antivirus products were run on the whole virus set at 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.

Future plans

In the future we would like to extend this test as follows:

- Execute tests on other virus test sets.
- Increase the number of different viruses as well as the number of virus samples per a virus.
- After at least one year testing the trends of results will be published.

The following table shows the plan of Checkvir project in the next 8 month:

Month	Platforms	Virus test sets	Speciality
November 2002	Win2000+Exchange2000, Win98+Outlook	Wildlist	E-mail viruses
December 2002	WinXP, DOS	Wildlist	Possible actions after detection
January 2003	Win2000 Server, Debian Linux+Samba	Wildlist	Update / upgrade: method, procedure, licence, cost
February 2003	Win Me, Novell Netware	Wildlist, Polymorphic	.Polymorphic and metamorphic viruses
March 2003	Win 98, Win 2000	Wildlist, Polymorphic	Speed vs. liability
April 2003	Win Me + Outlook Exp., Win Me +The Bat!	Wildlist, Polymorphic, Macro	Managing,
May 2003	Win XP, Win Me	Wildlist, Polymorphic, Macro	On-demand and on-access
June 2003	Win 98, Win 2000 server	Wildlist, Polymorphic, Macro, Wildlist 200211-200306	Testing heuristics: Old AV (from November 2002) against new viruses

Table 4: Checkvir tests from November 2002 to June 2003

References

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.