ANTIVIRUS SCANNER ANALYSIS 1995

Marko Helenius

Virus Research Unit, University of Tampere, Department of Computer Science,
P.O.BOX 607, 33100 TAMPERE, FINLAND, Tel: +358 31 215 7139,
Fax: +358 31 215 6070, E-mail: cshema@uta.fi,
WWW: http://www.uta.fi/laitokset/virus, ftp: ftp.cs.uta.fi /pub/vru

This paper briefly introduces our methods of testing antivirus products and results of an antivirus scanner analysis carried out in the Virus Research Unit at Summer 1995. The analysis was performed with DOS-, Windows-, Netware-, OS/2 and memory resident versions of the scanners. I have also tried to think what a reader should be aware of when reading the results.

ACKNOWLEDGEMENTS

This analysis has required a lot of work efforts and carrying out the analysis took much more time than I ever expected. Therefore publication of the results has also been later than originally planned.
Also a lot of co-operation with antivirus researchers was required. I would like to thank the following people who have been of great help when carrying out the analysis.

Karsten Ahlbeck, Karahldata
Pavel Baudis, ALWIL Software
David Chess, IBM T.J.Watson Research Center
Shimon Gruper, Eliashim Microcomputers Ltd.
Dmitry Gryaznov, S&S International PLC.
Jan Hruska, Sophos Plc.
Peter Hubinsky, Slovak Antivirus Center
Mikko Hypponen, Data Fellows Ltd.
Trevor Iverach, Cybec Pty Ltd.
Eugene Kaspersky, KAMI Group
Jimmy Kuo, McAfee Association
Jeffrey Leeds, Symantec Peter Norton's Group
Cliff Livingstone, Look Software
Jim Lynch, McAfee Association
Roger Riordan, Cybec Pty Ltd.
Luca Sambucci, I.C.A.R.O.
Jonathan Stotter, Eliashim Microcomputers Ltd.
Frans Veldman, ESaSS Ltd.

1. INTRODUCTION

It is too often unclear how antivirus testers are working and what viruses they are using in their tests. This is not, however, how it should be. I believe it should be known to the public how antivirus testers are working and what viruses they are using in their tests. Also I believe, that a tester should admit the lacks of his/her tests to avoid misleading information. At least it should be known to the public what was actually tested. To give more exact view of our work I have briefly presented our methods of testing and some facts that readers should be aware of. This paper presents problems with collecting the "In the Wild" test set, how we are carrying out the tests, test results of the analysis and what a reader of the analysis should be aware of when reading the results.

This report presents results of an antivirus scanner analysis carried out by the Virus Research Unit in summer 1995. As a base for the analysis there were two test sets. One consisted of viruses found in the field according to antivirus researchers and the other consisted of viruses we had received before starting the analysis. The analysis includes tests of DOS and memory resident scanners against both the whole test set and the 'In the Wild' test set. Windows, NLM and OS/2 scanners were analyzed only against file viruses found in the field.

2. ANALYSING THE PRODUCTS

The following sections describe briefly how the analysis was carried out.

2.1 Excluding non-viruses

Trojan horses, joke programs, intended viruses, first generation viruses, innocent files and other non-viruses should be excluded from the test set. Otherwise products, which are good at detecting true viruses, but "bad" at detecting non-viruses would have lower score than they are worthy of and products, which are giving false alarms could perform well. After all we should be analysing how well products can detect viruses. In this analysis a lot of work efforts were used to exclude Trojan horses, joke programs, droppers, first generation viruses, innocent files, intended viruses and other non-viruses from the test set. The non-virus removal process was carried out with a help of an invention implemented at the Virus Research Unit. The invention is called as "Automatic and Controlled Virus Code Execution System" [Helenius 1995] and it executes automatically virus code in controlled area and saves infected areas into specific network directory. The system's power is that it is implemented so that it can be left to work on its own. It recovers automatically from hanging, damage and CMOS memory failures that execution of malicious software may cause.

2.2 Analyzing on-line DOS-scanners

Both the 'In the Wild' test set and whole test set were used for analysing on-line DOS-scanners. The analysis was carried out against both file and boot sector viruses. Detection of boot sector viruses was analyzed by writing one by one diskette boot images on diskettes and then skanning the diskettes. File virus detection capabilities were analysed by executing DOS-scanners from batch files by using the switches presented in table 1.

Product	***Command line***
Avast 7.07	LGUARD %1%2 /P /S /RAV%2.REP
AVP 2.1 (3.6.1995)	AVP /W=AP%2.REP /S /Y /Q %1%2
Central Point (1.6.1995)	CPAV %1%2 /P /R
Dr. Solomon 7.13	FINDVIRU %1%2 /REPORT=FV%2.REP /LOUD /VID
F-PROT 2.18	F-PROT %1%2 /NOWRAP /LIST /NOMEM /REPORT=FP%2.REP
IBM Antivirus 2.2	BMAVSP -LOGIBMAVSP.LOG -PROGRAMS -VLOG -NB -NREP -NWIPE -NFSCAN %1%2
Inoculan 3.0	NOCULAN %1%2 /LIS IN%2.REP
Integrity Master 2.51	IM /NOB /NE /VL /REPA /1 /RF=E:\IM_NEW\IM%3.REP
Microsoft Antivirus (6.2.1995)	MSAV %1%2 /P /R
Norman Virus Control 3.57	NVC %1%2 /LFNO%2.REP /LA /S /U /Y
Norton Antivirus (1.6.1995)	Scan executed from graphic interface
McAfee Scan 2.2.2	SCAN /REPORT S2%2.REP /RPTALL /NOMEM /SUB %1%2
Sweep 2.74	SWEEP %1%2*.EXE %1%2*.COM %1%2*.SYS %1%2*.BAT -REC -NK -NAS -NB -P=SW%2.REP

Thunderbyte 6.35	TBSCAN %1%2 LARGEDIR EXPERTLOG NOAUTOHR BATCH LOG LOGNAME=TB%2.REP
VET 8.212	VET %1%2 /E /F /N /X /R
Virusafe 6.5	VREMOVE %1%2 /R /C /D

Table 1: Command line switches

2.3 Analysing memory resident scanners

Memory resident scanners were analysed against file viruses by copying files when the memory resident part of a product was activated. A drawback of this method is that some products may detect more viruses when actual virus code is executed and some products may not even detect viruses at all when files are copied. The reason for using the file copy method is that when preparing the analysis we did not have automatic system for the file execution method. However when the automatic and controlled virus code execution system is now implemented, even the file execution method is possible. Boot sector virus tests of memory resident scanners were carried out by attaching infected diskettes with the "DIR"-command.

2.4 Analyzing Windows, NLM and OS/2 scanners

Windows, NLM and OS/2 scanners were analyzed only against file viruses found on the field. The whole test set was not included because of restricted disk space, or because in case of Windows scanners some products could not create large enough log files. Boot sector viruses were not included, because so far we do not have methods for the automatic analysis in these environments.

2.5 Report file creation

I believe, that it should be known to the public, what was actually tested and how did we conclude the results in a test. So this is why we have always prepared cross-references, which clearly show which sample files were found by which product. To implement the report file generation we are first using awk-scripts to organize the report files into analogous format. After this we are using a specific tool, which unites the report files.

2.6 Analysing scanning speed

Speed performance tests were carried out in two clean computers and scanning time includes memory tests, checking scanner's own integrity and all what is needed to do after the scanning is started from the command line. Reason for the method is that this is the real time needed for scanning a hard disk. Memory resident scanners were analysed by executing 40 files when a memory resident scanner was loaded.

3. PROBLEMS WITH THE 'IN THE WILD' TEST SET

For a virus to be included "In the Wild" test set, it must have been found in the "field" at least once. This is not, however, as obvious as it sounds. How do we know, that a virus has been found in the field at least once. Someone must have reported to some antivirus researcher, that the virus has been found in the field but how do we know that someone has reported the virus to some anti-virus researcher. One solution is to use Joe Well's list [Joe Wells], which includes viruses, which have been reported as found in the field according to main anti-virus researchers. It does not, however, contain all the viruses found from the field, because all the cases are not reported to Joe Wells. For example, we in Finland have viruses found in the field, which have been reported to antivirus researchers and/or to Central Criminal Police, but some of them still are not in the Joe Well's list. I have also reports from other anti-virus researchers of viruses found in the field, which are not in the Joe Well's list. However, those viruses mentioned in the Joe Well's list should at least be included in the test set. My solution was to use the viruses mentioned in our old test report [Helenius 1994] as a base for the test bed and to ask comments and additions from antivirus researchers and to combine the results with the Joe Well's list.

Most of the "In the Wild" listings do not have exact information, which variants of viruses are found in the field. Sometimes the exact variant can be identified directly, but in most cases further examination is needed. This causes problems when constructing the test set. Sometimes I could receive the original virus from antivirus researchers but this is not always possible. I had to compare several sources of information between each other to determine, which variant of the virus was "In the Wild". In most cases this comparing process was producing results and I could almost certainly identify the correct variant, but still I cannot be absolutely certain, that all variants were chosen correctly.

A yet new problem appeared when the analysis was already ready. I noticed that it is possible to affect the test results by single incidents or simply by lying. Thus unclear cases were first sent for commenting and then removed unless there was no other evidence. Exact description of the 'In the Wild' test set construction is described in the separate file WILD_VIR.TXT.

4. THE RESULTS OF THE ANALYSIS

The following sections present results of the analysis. The detection percentages were calculated so that for each virus an average of detection was counted. So if a scanner could detect only part of the sample files of a virus, an average detection was calculated. A drawback of this method is that it does not perfectly take into account that a partly detected virus may cause trouble for a user, because undetected files may cause reinfection of the virus. On the other hand, even unreliably detected virus does get caught. This slows down the spread of the virus and thus unreliable detection should be taken into account. Anyway, because estimating reliable detection would be too unsure, I decided to count the averages.

4.1 DOS scanner analysis with the whole test set

The whole test set included 250 boot sector viruses and 3586 file viruses. Some memory resident scanners may detect more viruses than presented in the tables, because some scanners may detect virus on execution of a virus. McAfee Association's Vshield should detect polymorphic viruses when the scanner is activated with the /POLY switch. Also Dr. Solomon's Virus Guard should detect polymorphic viruses by detecting the viruses from the memory. There is a plus mark after these scanners. There are also Windows versions of F-PROT's, Dr. Solomon's and Norton's memory resident scanners. Because there are more resources available in Windows, it is possible that these scanners may detect even more viruses than DOS-versions of the memory resident scanners. However because of the lack of time Windows versions could not be analysed. Memory resident parts of Avast and VET could not be analyzed, because these scanners do not check files when they are copied. The first parts of table 2 present results of on-line DOS-scanners and the latter part presents results of memory resident scanners.

Scanner	***Boot sector***	***File***	***Combination***	***Boot sector***	***File***	***Combination***
Avast 7.07	97.8	98.59	**98.5**	RGuard	RGuard	**RGuard**
AVP 2.1 (3.6.1995)	97.37	99.72	**99.6**	--------	--------	**--------**
Central Point (1.6.1995)	90.07	72.11	**73.3**	49.8	41.59	**42.12**
Dr. Solomon 7.13	100	99.42	**99.5**	100	94.22+	**94.6+**
F-PROT 2.18	98.00	98.76	**98.7**	85.2	78.79	**79.2**
IBM Antivirus 2.2	98.8	96.22	**96.4**	44.8	9.8	**12.1**
Inoculan 3.0	85.00	77.84	**78.3**	85.0	77.18	**77.7**
Integrity Master 2.51	85.87	88.47	**88.3**	--------	--------	**--------**

Microsoft Antivirus (6.2.1995)	52.16	52.17	**52.2**	53.81	38.9	**39.8**
Norman Virus Control 3.57	98.4	97.77	**97.8**	NVC.SYS	NVC.SYS	**NVC.SYS**
Norton Antivirus (1.6.1995)	85.2	83.17	**83.3**	84.8	83.44	**83.5**
McAfee Scan 2.2.2	89.2	89.05	**89.1**	82.4	79.43+	**79.6+**
Sweep 2.74	100	98.23	**98.3**	InterCheck	InterCheck	**InterCheck**
Thunderbyte 6.35	98.4	98.14	**98.2**	63.6	79.38	**78.4**
VET 8.212	91.6	83.43	**84.0**	VET_RES	VET_RES	**VET_RES**
Virusafe 6.5	90.7	71.12	**72.4**	90.9	68.76	**70.2**

Table 2: Results of DOS scanners, when the whole test set was used

Most scanners seem to perform well. A clear exception is Microsoft Antivirus, which could detect only about half of the viruses in the test bed. Also memory resident scanners of IBM Antivirus, Central Point Antivirus and Microsoft Antivirus could detect less than half of the viruses in the test bed. In most cases memory resident scanners cannot detect as many viruses as on-line scanners.

Norman Virus Control has instead of a memory resident scanner an active monitoring program. Sweep does not have a memory resident scanner, but Sweep's Intercheck can be used like a memory resident scanner in a computer that is connected to a network server. All unauthorized files and boot sectors are copied to the network server and then netware version of Sweep scans the files. Therefore detection capabilities are same as for the network version. A drawback of the method is the extra traffic that Intercheck causes for the network server when copying files and boot sectors.

4.2 Dos scanner analysis with the 'In the Wild' test set

The 'In the Wild' test included viruses found in the field according to antivirus researchers. A previous analysis carried out by the Virus Research Unit was used as a base for the 'In the Wild' test set. The base was sent to antivirus researchers for commenting and a new list was prepared by using received comments and Joe Well's 'In the Wild' list [Wells]. Joe Well's list includes viruses, which have been reported as found in the field according to main antivirus researchers. The test set included 86 boot sector viruses and 239 file viruses found in the field according to antivirus researchers.

Scanner	***Boot sector***	***File***	***Combination***	***Boot sector***	***File***	***Combination***
Dr. Solomon 7.13	100.00	99.23	**99.5**	100.00	92.78+	**94.7+**
AVP 2.1 (3.6.1995)	97.47	100	**99.3**	--------	--------	**--------**
Sweep 2.74	100.00	98.97	**99.2**	InterCheck	InterCheck	**InterCheck**
Avast 7.07	96.84	100	**99.1**	RGuard	RGuard	**RGuard**
F-PROT 2.18	95.57	98.97	**98.0**	89.24	84.54	**85.9**
Thunderbyte 6.35	96.2	98.3	**97.7**	76.33	83.0	**81.06**
IBM Antivirus 2.2	96.2	97.63	**97.2**	66.46	28.97	**39.8**
Norman Virus Control 3.57	97.47	93.75	**94.8**	NVC.SYS	NVC.SYS	**NVC.SYS**
McAfee Scan 2.2.2	94.3	92.87	**93.3**	88.99	79.36+	**82.1+**
Integrity Master 2.51	89.24	92.01	**91.2**	--------	--------	**--------**

VET 8.212	94.94	88.5	**90.4**	VET_RES	VET_RES	**VET_RES**
Norton Antivirus (1.6.1995)	91.77	86.49	**88.0**	90.25	86.51	**87.6**
Virusafe 6.5	87.66	81.78	**83.5**	87.66	77.76	**80.6**
Inoculan 3.0	81.01	82.06	**81.8**	81.01	81.46	**81.3**
Central Point (1.6.1995)	82.91	78.52	**79.8**	42.15	50.53	**48.1**
Microsoft Antivirus (6.2.1995)	44.57	61.4	**56.5**	46.29	44.83	**45.25**

Table 3: Results of DOS scanners, when 'In the Wild' test set was used

When viruses found in the field were used as a test bed most scanners could improve their score and most scanners seem to perform well. Again a clear exception is on-line version of Microsoft Antivirus and memory resident portions of IBM Antivirus, Central Point Antivirus and Microsoft Antivirus. Detecting viruses found in the field is more critical than detecting all viruses and therefore those producers who cannot detect near 100% should pay attention on detecting viruses found in the field.

4.3 Windows scanner analysis

Windows scanners were analysed only with file viruses found in the field. The whole test set was not included, because some scanners had problems with creating a large report file. Report file creation caused problems for some scanners even with the "In the Wild" test set and therefore these scanners could not be analysed. Boot sector viruses were not included in the test set, because so far we do not have methods for automating the analysis task in Windows.

Windows scanner	***'In the Wild' file virus***
Avast 7.07	98.97
AVP 2.1 (3.6.1995)	--------
Central Point (1.6.1995)	Not tested
Dr. Solomon 7.13	99.23
F-PROT 2.18	97.94
IBM Antivirus 2.2	98.43
Inoculan 3.0	Not tested
Integrity Master 2.51	--------
Microsoft Antivirus (6.2.1995)	Not tested
Norman Virus Control 3.57	93.75
Norton Antivirus (1.6.1995)	68.72
McAfee Scan 2.2.2	93.90
Sweep 2.74	--------
Thunderbyte 6.35	93.91

VET 8.212	--------
Virusafe 6.5	Not tested

Table 4: Results of Windows scanners

Almost every analysed Windows version can detect almost as many viruses as the DOS version of the product. An exception is the Windows version of Norton antivirus, which can detect fewer viruses than DOS-version of the product. Inoculan, Microsoft antivirus and Virusafe were not included because these products could not create a large enough log file of infected files.

4.4 NLM scanner analysis

Also NLM scanners were executed only with the file viruses found in the field. Reason for this was limited disk space on the network server. Table 5 presents results of the netware scanner analysis.

Netware scanner	***'In the Wild' file virus***
Avast 7.07	--------
AVP 2.1 (3.6.1995)	Forthcoming
Central Point (1.6.1995)	Not tested
Dr. Solomon 7.13	99.23
F-PROT 2.18	89.64
IBM Antivirus 2.2	97.38
Inoculan 3.0	82.06
Integrity Master 2.51	--------
Microsoft Antivirus (6.2.1995)	--------
Norman Virus Control 3.57	93.75
Norton Antivirus (1.6.1995)	Not tested
McAfee Scan 2.2.2	Not tested
Sweep 2.74	98.97
Thunderbyte 6.35	---------
VET 8.212	Forthcoming

Virusafe 6.5	Not tested

Table 5: Results of Netware scanners

The NLM version of most scanners' could detect the same number of viruses as the DOS version. F-PROT's netware version uses quick scanning engine and cannot therefore detect as many viruses than the DOS-version of the scanner.

4.5 OS/2 scanner analysis

OS/2 scanners were executed only with the file viruses found in the field. Reason for excluding the whole test set was limited disk space. Boot sector viruses were not included in the test set, because so far we do not have methods for automating the analysis task. OS/2 scannners were analyzed with one month newer versions of the scanners. Reason for this was that F-PROT's OS/2 scanner was received a month later than other products and therefore a newer versions of the other analysed products were included.

OS/2 scanner	***'In the Wild' file virus***
Dr. Solomon 7.50	99.48
F-PROT 2.18c	98.97
IBM Antivirus 2.2	98.4.
McAfee Scan 2.2.2	----------
Sweep 2.75	98.97

Table 6: Results of OS/2scanners

All analyzed OS/2 scanners seemed to work as well as DOS-versions. McAfee Association has also OS/2 scanner, but it could not be analyzed since it works only with OS/2 versions 2.0 or later.

4.6 Speed performance analysis

Speed performance tests were carried out in two clean computers and scanning time includes memory tests, checking scanner's own integrity and all what a product need to do after scanning is started from the command line. Only the DOS versions were analysed. Test computer 1 was a 486 DX computer with 40 MHz CPU clock with 220 Megabytes of used diskspace and test computer II was 386 SL computer with 25 MHz CPU clock and 55 megs of disk space was used. Exact configuration of the test computers is included in the appendix 1.

Memory resident scanners were analysed by executing 40 files in the same computers when a memory resident scanner was loaded. The files returned control back to DOS after execution of the file. List of these files is included in the file RESFILES.DIR. Table 7 presents scanning speed of on-line DOS-scanners in the 80486 computer and table 8 presents scanning speed and memory usage of memory resident scanners in the 80486 computer. Tables 9 and 10 present corresponding scanning speed performance tests when 80386 computer is used. For speed performance tests it should be noted that although fast scanning speed is does spur users to perform the scanning more often, more important is that scanning is reliable e.g. the product is able to find viruses also.

4.6.1 Test computer I, dos-scanners

Product	**Command line**	**Scanning time**
Thunderbyte	TBSCAN C:\	0:21
Thunderbyte	TBSCAN co C:\	0:21
Sweep	SWEEP C:	0:44
Virusafe	VREMOVE /SL /C /G	0:55
Dr. Solomon	FINDVIRU C:	0:58
Norton Antivirus	NAV C:	1:01
F-PROT	F-PROT C:	1:03
Avast	LGUARD C:\ /P	1:05
Norman	NVC C:	1:08
McAfee Scan	SCAN C:	1:51

VET	VET C:\ /X /R /F	1:51
Central Point	CPAV /P C:	1:56
Inoculan	INOCULAN C:\	2:05
Integrity Master	IM /VO /ND	2:23
Microsoft Antivirus	MSAV /P C:	2:24
IBM Antivirus	IBMAVSP -NLOG -PROGRAMS C:	2:49
AVP	AVP /Y /Q	5:04

Table 7: Scanning speed of the on-line DOS-scanners

4.6.2 Test computer I, memory resident scanners:

Product	**Command line**	**Time**	**Conventional**	**Upper memory**
No scanner loaded		0:06		
F-PROT	VIRSTOP /COPY	0:06	37,728	0
IBM Antivirus	IBMAVDR C:\IBMAV\	0:06	5,984+4,642	0
Thunderbyte	TBSCANX	0:06	42,464+3,360	0
Norton Antivirus	NAVTSR	0:08	56,480	0
Dr. Solomon	GUARD	0:14	9,248	0
Inoculan	IMMUNE	0:16	7,552	0
McAfee Scan	VSHIELD /ANYACCESS	0:16	0	31,216

F-PROT	VIRSTOP /COPY /DISK	0:18	3,984	0
Central Point	VSAFE	0:40	24,352	0
Microsoft Antivirus	VSAFE	0:43	22,912	0
Virusafe	VS /CH	0:44	0	10,480

Table 8: Scanning speed and memory usage of the memory resident scanners

4.6.3 Test computer II, DOS-scanners

Product	**Command line**	**Scanning time**
Thunderbyte	TBSCAN C:\	0:18
Thunderbyte	TBSCAN co C:\	0:23
Norton Antivirus	NAV C:	1:00
Virusafe	VREMOVE /SL /C /G	1:00
Avast	LGUARD C:\ /P	1:27
Sweep	SWEEP C:	1:31
Dr. Solomon	FINDVIRU C:	1:43
Norman	NVC C:	1:53
VET	VET C:\ /X /R /F	1:53
McAfee Scan	Scan c:	2:05
Inoculan	INOCULAN C:\	2:26
F-PROT	F-PROT C:	2:40
Integrity Master	IM /VO /ND	2:45
Microsoft Antivirus	MSAV /P C:	3:38
IBM Antivirus	IBMAVSP -NLOG -PROGRAMS C:	4:35
Central Point	CPAV /P C:	6: 22

AVP	AVP /Y /Q	9:37

Table 9: Scanning speed of the on-line DOS-scanners

4.6.4 Test computer II, memory resident scanners

Product	**Command line**	**Time**	**Conventional**
No scanner loaded		0:10	
F-PROT	VIRSTOP /COPY	0:11	37,728
IBM Antivirus	IBMAVDR C:\IBMAV\	0:11	5,984+4642
Thunderbyte	TBSCANX	0:11	42,464+3,360
Norton Antivirus	NAVTSR	0:13	3,248
F-PROT	VIRSTOP /COPY /DISK	0:27	3,984
McAfee Scan	VSHIELD /ANYACCESS	0:29	9,104
Dr. Solomon	GUARD	0:32	9,280
Inoculan	IMMUNE	0:37	7,552
Central Point	VSAFE	1:20	7,280
Microsoft Antivirus	VSAFE	1:21	6,848
Virusafe	VS /CH	1:41	10,480

Table 10: Scanning speed and memory usage of memory resident scanners

The fastest on-line scanner seems to be Thunderbyte antivirus and slowest seems to be AVP.

IBMAVDR, TBSCANX and Virstop without /DISK option seems to be the fastest memory resident scanners, but these scanners are also consuming much conventional memory (Virstop, TBSCANX) or detection capabilities (IBMAVDR). In most cases memory resident scannners are keeping parts of them on the fixed disk and thus slowing down scanning speed but saving valuable conventional memory.

5. DISCUSSION AND CONCLUSIONS

A lot of work was assigned to carry out everything as well as possible. Carrying out an anti-virus scanner analysis requires a lot of work and still there is always something to improve. Also this analysis has drawbacks, which a reader of the results should be aware of while examining them. Firsts of all performance of checksum calculation and active monitoring programs were not analyzed. Also products' disinfection capabilities were not examined. A thorough analysis should also include a false alarm rate test. Because of restricted time there was no false alarm rate test in this analysis. In addition the tests were not carried out while viruses were memory resident although this is often the case, when a computer is infected with a virus. In addition all possible viruses were not included. Only viruses that Virus Research Unit had received before starting the analysis were included. Also it should be noted, that all viruses found in the field were not included, because only viruses we assume as being found on the field were included. In addition we might have done a mistake while checking correct variants of the viruses in the "In the Wild" test set. It is also always possible, that someone has given us misleading information although we have tried to do our best to verify the information given us whenever possible. Also it should be noted, that we did not try to measure how common each virus is and so the percentages do not directly measure the actual risk level of infection. Instead the percentage just presents, how many per cents of viruses used in this analysis the products could detect. A lot of work was used to exclude non-viruses, droppers and first generation viruses from the test set. However, we might have done mistakes and therefore it is possible to have non-viruses included although I believe that there are only few such mistakes. Also it should be noted that we did not try to check whether a product can reliably detect a virus e.g. we did not count cases, where a product did not detect all replicates of a same virus. Because of the mentioned drawbacks the results give only an overall impression of the performance of the tested products.

Regardless of the drawbacks I believe, that there are some advantages in this analysis. We succeeded to include most memory resident, Windows, Netware and OS/2 scanners in the analysis. In addition the test set includes large set of files and two test sets were included. In addition, this analysis has advanced cross-references, which clearly show, which viruses were detected by which product and by which name.

REFERENCES

[Helenius] Marko Helenius, 'Automatic and Controlled Virus Code Execution System ',
An article from the proceedings of the eicar 1995 conference held in Zuerich, Switzerland 27.-29.11 1995. Available electronically via anonymous ftp as ftp.cs.uta.fi: /pub/vru/documents/automat.zip

[Helenius] Marko Helenius, "Antivirus scanner analysis by using the "In the Wild" test set", 18.11.1994, Available electronically via anonymous ftp as ftp.cs.uta.fi: /pub/vru/documents/wildtest.zip

[Wells] Joe Wells, "PC Viruses in the Wild", Available electronically via anonymous ftp as ftp.informatik.uni-hamburg.de: /pub/virus/texts/viruses/wild????.zip

APPENDIX 1, TEST COMPUTERS FOR THE SPEED PERFORMANCE ANALYSIS

TEST COMPUTER I:

486 DX Samsung, 128k cache memory, 40 MHz CPU clock, 340M Scsi fixed disk, 16M operating memory, 621k free conventional memory, 155k free upper memory, 120M free disk space

Software installed on hard disk: MS-DOS 6.2, Windows 3.1, Excel 5.0, Windows Word 2.0, Power Point 4.0, Canon BJC-4000 electronic printer manual, Microsoft entertainment pack 2.0, shareware games, test files for analyzing memory resident scanners.

Installed TSR programs and device drivers: HIMEM.SYS, EMM386.EXE, SMARTDRV.EXE, SETVER.EXE, DISPLAY.SYS, KEYB.EXE, DOSKEY.COM

TEST COMPUTER II:

386 SL Olivetti portable, 64k cache memory, 25 MHz CPU clock, 60M fixed disk drive, 4M operating memory, 592k free conventional memory, 2k free upper memory, 5M free disk space.

Installed TSR programs and device drivers: HIMEM.SYS, EMM386.EXE, SMARTDRV.EXE, SETVER.EXE, DISPLAY.SYS, KEYB.EXE, DOSKEY.COM, POWER.EXE, ANSI.SYS

Software installed on hard disk: MS-DOS 6.2, Microsoft Windows 3.1, Microsoft Works 3.0, Lotus Organizer, Microsoft entertainment pack 2.0, shareware games, test files for analyzing memory resident scanners.