Anti-Virus Comparative No.2

Proactive/retrospective test
(on-demand detection of virus/malware)

Date: May 2004 (2004-05)

Last revision of this report: 12. May 2004

Author: Andreas Clementi

Contact: contact@av-comparatives.org

Website: http://www.av-comparatives.org

1. Introduction

This test can be seen as the continuation of the last test (February 2004). The same products were used and the results show the purely proactive detection capabilities that the products had three months ago. Many new viruses and other types of malware appear every day, this is why it is important that Anti-Virus products not only provide new updates, as often and fast as possible, in order to identify those new threats, but also that they are able to detect such threats in advance with generic or heuristics techniques., Without this ability the user has to wait for an updated release of the Anti-Virus product. We used the same products with the same best possible settings that the scan engines had in the last comparative to make this test. For the test we used all the new samples that we received in the time period from the 5. February to the 5. May.

The following 13 products were tested in this comparative (last signature updates and versions are from 06. February 2004):
Avast! 4.1.342 Professional Edition
BitDefender Anti-Virus 7.2 Professional Edition
Dr.Web Anti-Virus for Windows 95-XP 4.30a
ESET NOD32 2.000.9
F-Prot Anti-Virus for Windows 3.14b
H+B EDV AntiVir Professional Edition 6.22.00.09
Kaspersky Anti-Virus Personal 4.5.0.95
McAfee VirusScan Professional 8.0.26
Panda Platinum Internet Security 8.02.00
Symantec Norton Anti-Virus 10.0.1.13
GeCAD Reliable Anti-Virus (RAV) 8.6.105
Sophos Anti-Virus 3.78
Trend Micro Internet Security 11.10

2. Description

In order to keep the test samples transparent for all participating AV companies, we used all received samples that were new for us, and we sorted they into 4 main categories:

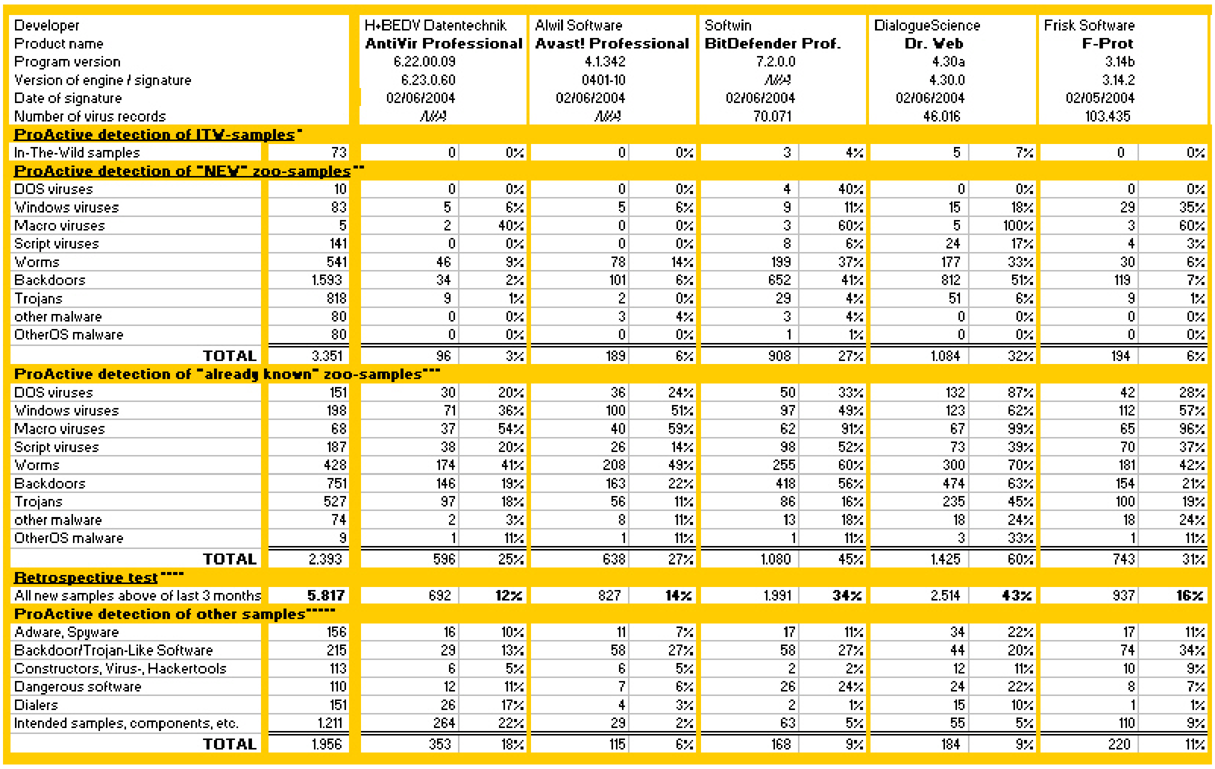
- ITW-samples: ITW-viruses that appeared during the last 3 months
- New zoo-samples: all new zoo-samples that were classified by us to be new / unknown to all tested Anti-Virus products. This category is split into subcategories by virus/malware type. Results of this category shows the pure proactive detection capability.
- “Already known” zoo-samples: all new zoo-samples that were already known by some Anti-Virus products. Sometimes an AV company receives a sample before the other companies and will already have released a signature in order to detect the sample. Such samples were moved into this category. This category is split into subcategories by virus/malware type.
- Other samples: all other samples were sorted as best we could into one of the following categories:
    - Adware, Spyware
    - Backdoor/Trojan-Like software
    - Constructors, Virus-, Hackertools
    - Dangerous software
    - Dialers
    - Intended samples (not full working samples) or components

It is not always possible to determine which categories samples should fall in, though we have attempted to do so. For this reason the results have been rounded to whole numbers. Anti-Virus products often claim to have high proactive detection capabilities – far higher than those in our test. This is not always just a self-promotional statement; it is possible that products can reach the stated percentages, but this is dependent on the duration of the test-period and the size of the sample set. For example: if you keep always your scanner updated and 10 new viruses appear in the time period between the next update, it is possible that the scanner detects (depending on the nature of samples they are) none, most or all (if you are lucky) of the samples (our experience with some products shows that on retrospective tests of 1 week periods some scanners have a detection rate of around 70%). We used samples that appeared the last 3 months in order to measure the underlying proactive detection ability of the scan engines. There are other kinds of testing procedures we could have employed to make a proactive/retrospective test, however these would not have delivered valid results for all the 13 products in an efficient and timely manner. Anyway this is our very first test of this kind and we will improve the procedures in order to make future tests of this kind better. In the last 3 months many new samples appeared In-The-Wild, the Bagle, NetSky, Mydoom and Sober variants; for this kind of worm generic detections, heuristic improvements and other technologies had to be implemented with updates in the Anti-Virus products, in order that some of the new ITW-samples were detected by some products before a signature for those samples was released. This test cannot show these measures as it just shows the proactive detection capability that the scanners had on the 5th February over the samples that appeared during the following 3 month period. The results should show that it is always necessary to keep your Anti-Virus software always up-to-date to have the highest available security level that your product can provide you. At this moment (1st June 2004) most of the used samples are already detected by most of the tested scanners, so if you constantly update your scanner, you are protected against all (or most of the) viruses and malware that were used for this test. Please also note that we tested only the on-demand detection capability. Some products could was able to detect new samples e.g. on-access or by other monitoring tools.

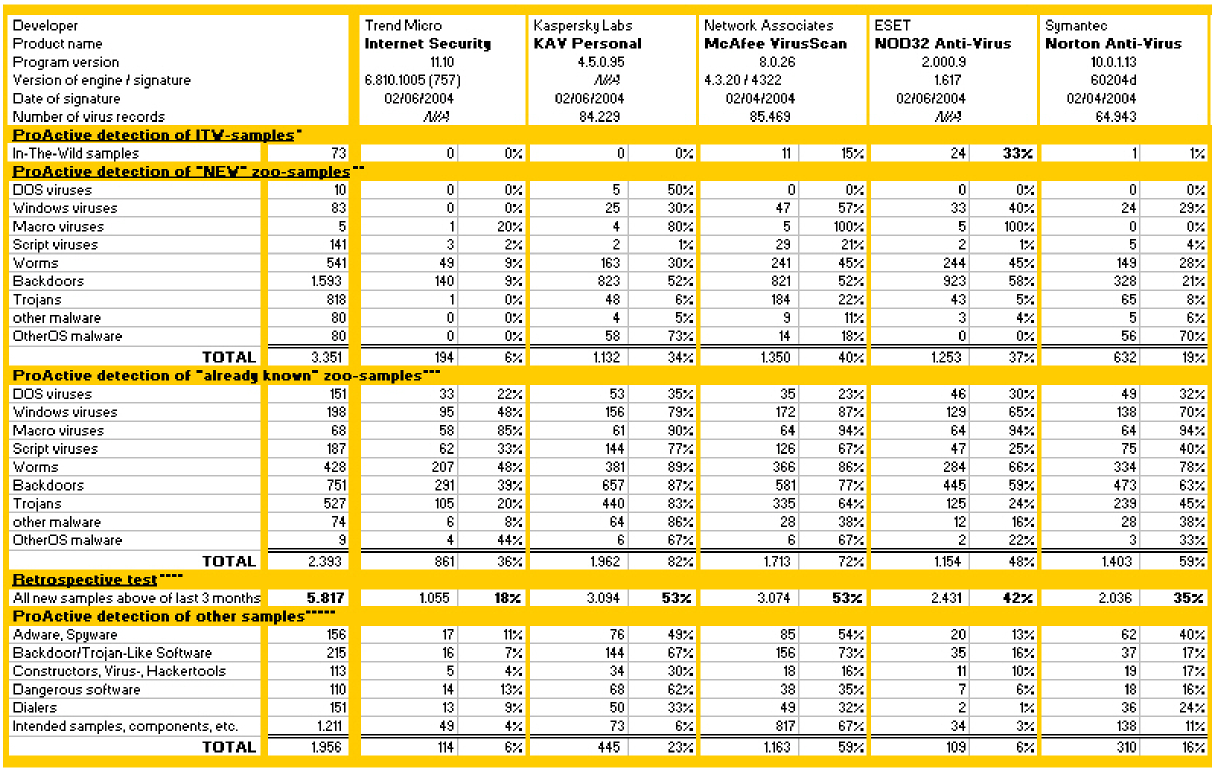
From all samples we received during the 5. February and the 5. May, 7.773 samples were totally new for us. From those 7.773 samples, 73 were ITW-samples (according to the Wildlist or also samples that appeared In-The-Wild in some country regions), 3.351 were determined to be totally new to ANY tested Anti-Virus product, 2.393 were determined to be already known by some Anti-Virus products and 1.956 samples were determined to be other samples, like Adware, Dialers, Tools, intended samples, etc.

A quick analysis of these numbers we can see that 44% were totally new samples, 31% were already known by some scanners and 25% were other samples. If we take a look into the subcategories we see that nowadays there are mostly Backdoors (40%), Trojans (23%) and Worms (17%) around and that all the other categories are just 20% in total. While the ITW-samples consist always nearly only of worms, there are no statistics of how many backdoors and Trojans are "ITW", but this does not mean that they do not pose a real threat – if malware authors create backdoors in order to make use of them.

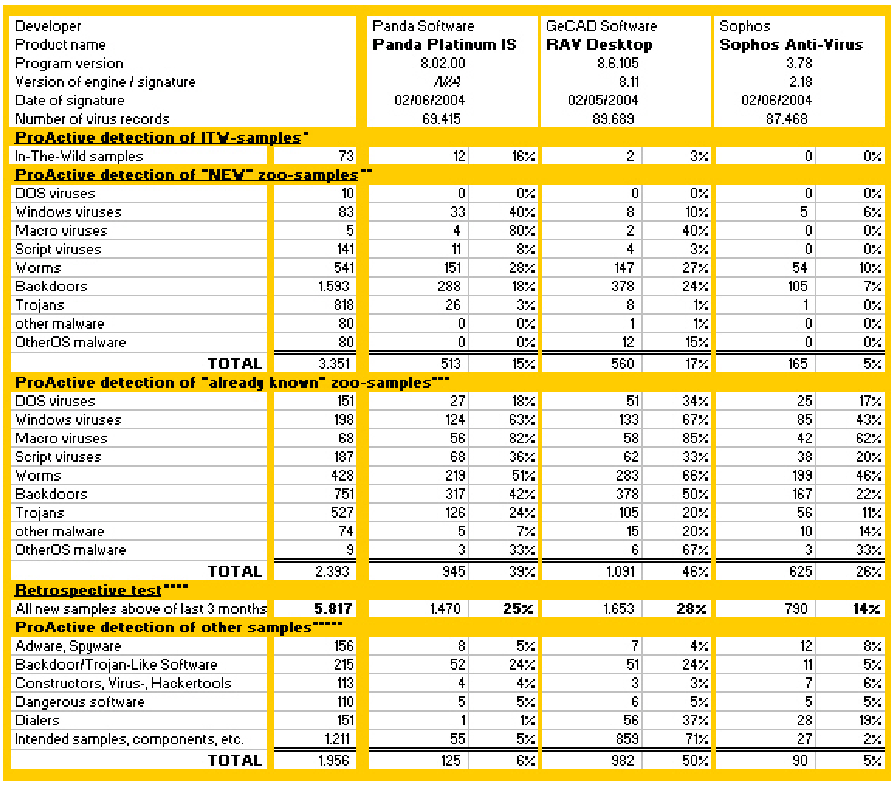
3. Test results



Developer		H+BEDV Datentechnik		Alwil Software		Softwin		DialogueScience		Frisk Software	
Product name		**AntiVir Professional**		**Avast! Professional**		**BitDefender Prof.**		**Dr. Web**		**F-Prot**	
Program version		6.22.00.09		4.1.342		7.2.0.0		4.30a		3.14b	
Version of engine / signature		6.23.0.60		0401-10		N/A		4.30.0		3.14.2	
Date of signature		02/06/2004		02/06/2004		02/06/2004		02/06/2004		02/05/2004	
Number of virus records		N/A		N/A		70.071		46.016		103.435	
ProActive detection of ITW-samples*											
In-The-Wild samples	73	0	0%	0	0%	3	4%	5	7%	0	0%
ProActive detection of "NEW" zoo-samples**											
DOS viruses	10	0	0%	0	0%	4	40%	0	0%	0	0%
Windows viruses	83	5	6%	5	6%	9	11%	15	18%	29	35%
Macro viruses	5	2	40%	0	0%	3	60%	5	100%	3	60%
Script viruses	141	0	0%	0	0%	8	6%	24	17%	4	3%
Worms	541	46	9%	78	14%	199	37%	177	33%	30	6%
Backdoors	1.593	34	2%	101	6%	652	41%	812	51%	119	7%
Trojans	818	9	1%	2	0%	29	4%	51	6%	9	1%
other malware	80	0	0%	3	4%	3	4%	0	0%	0	0%
OtherOS malware	80	0	0%	0	0%	1	1%	0	0%	0	0%
TOTAL	3.351	96	3%	189	6%	908	27%	1.084	32%	194	6%
ProActive detection of "already known" zoo-samples***											
DOS viruses	151	30	20%	36	24%	50	33%	132	87%	42	28%
Windows viruses	198	71	36%	100	51%	97	49%	123	62%	112	57%
Macro viruses	68	37	54%	40	59%	62	91%	67	99%	65	96%
Script viruses	187	38	20%	26	14%	98	52%	73	39%	70	37%
Worms	428	174	41%	208	49%	255	60%	300	70%	181	42%
Backdoors	751	146	19%	163	22%	418	56%	474	63%	154	21%
Trojans	527	97	18%	56	11%	86	16%	235	45%	100	19%
other malware	74	2	3%	8	11%	13	18%	18	24%	18	24%
OtherOS malware	9	1	11%	1	11%	1	11%	3	33%	1	11%
TOTAL	2.393	596	25%	638	27%	1.080	45%	1.425	60%	743	31%
Retrospective test****											
All new samples above of last 3 months	**5.817**	692	**12%**	827	**14%**	1.991	**34%**	2.514	**43%**	937	**16%**
ProActive detection of other samples*****											
Adware, Spyware	156	16	10%	11	7%	17	11%	34	22%	17	11%
Backdoor/Trojan-Like Software	215	29	13%	58	27%	58	27%	44	20%	74	34%
Constructors, Virus-, Hackertools	113	6	5%	6	5%	2	2%	12	11%	10	9%
Dangerous software	110	12	11%	7	6%	26	24%	24	22%	8	7%
Dialers	151	26	17%	4	3%	2	1%	15	10%	1	1%
Intended samples, components, etc.	1.211	264	22%	29	2%	63	5%	55	5%	110	9%
TOTAL	1.956	353	18%	115	6%	168	9%	184	9%	220	11%



Developer		Trend Micro		Kaspersky Labs		Network Associates		ESET		Symantec	
Product name		**Internet Security**		**KAV Personal**		**McAfee VirusScan**		**NOD32 Anti-Virus**		**Norton Anti-Virus**	
Program version		11.10		4.5.0.95		8.0.26		2.000.9		10.0.1.13	
Version of engine / signature		6.810.1005 (757)		N/A		4.3.20 / 4322		1.617		60204d	
Date of signature		02/06/2004		02/06/2004		02/04/2004		02/06/2004		02/04/2004	
Number of virus records		N/A		84.229		85.469		N/A		64.943	
ProActive detection of ITW-samples*											
In-The-Wild samples	73	0	0%	0	0%	11	15%	24	**33%**	1	1%
ProActive detection of "NEW" zoo-samples**											
DOS viruses	10	0	0%	5	50%	0	0%	0	0%	0	0%
Windows viruses	83	0	0%	25	30%	47	57%	33	40%	24	29%
Macro viruses	5	1	20%	4	80%	5	100%	5	100%	0	0%
Script viruses	141	3	2%	2	1%	29	21%	2	1%	5	4%
Worms	541	49	9%	163	30%	241	45%	244	45%	149	28%
Backdoors	1.593	140	9%	823	52%	821	52%	923	58%	328	21%
Trojans	818	1	0%	48	6%	184	22%	43	5%	65	8%
other malware	80	0	0%	4	5%	9	11%	3	4%	5	6%
OtherOS malware	80	0	0%	58	73%	14	18%	0	0%	56	70%
TOTAL	3.351	194	6%	1.132	34%	1.350	40%	1.253	37%	632	19%
ProActive detection of "already known" zoo-samples***											
DOS viruses	151	33	22%	53	35%	35	23%	46	30%	49	32%
Windows viruses	198	95	48%	156	79%	172	87%	129	65%	138	70%
Macro viruses	68	58	85%	61	90%	64	94%	64	94%	64	94%
Script viruses	187	62	33%	144	77%	126	67%	47	25%	75	40%
Worms	428	207	48%	381	89%	366	86%	284	66%	334	78%
Backdoors	751	291	39%	657	87%	581	77%	445	59%	473	63%
Trojans	527	105	20%	440	83%	335	64%	125	24%	239	45%
other malware	74	6	8%	64	86%	28	38%	12	16%	28	38%
OtherOS malware	9	4	44%	6	67%	6	67%	2	22%	3	33%
TOTAL	2.393	861	36%	1.962	82%	1.713	72%	1.154	48%	1.403	59%
Retrospective test****											
All new samples above of last 3 months	**5.817**	1.055	**18%**	3.094	**53%**	3.074	**53%**	2.431	**42%**	2.036	**35%**
ProActive detection of other samples*****											
Adware, Spyware	156	17	11%	76	49%	85	54%	20	13%	62	40%
Backdoor/Trojan-Like Software	215	16	7%	144	67%	156	73%	35	16%	37	17%
Constructors, Virus-, Hackertools	113	5	4%	34	30%	18	16%	11	10%	19	17%
Dangerous software	110	14	13%	68	62%	38	35%	7	6%	18	16%
Dialers	151	13	9%	50	33%	49	32%	2	1%	36	24%
Intended samples, components, etc.	1.211	49	4%	73	6%	817	67%	34	3%	138	11%
TOTAL	1.956	114	6%	445	23%	1.163	59%	109	6%	310	16%



Developer		Panda Software		GeCAD Software		Sophos	
Product name		**Panda Platinum IS**		**RAV Desktop**		**Sophos Anti-Virus**	
Program version		8.02.00		8.6.105		3.78	
Version of engine / signature		N/A		8.11		2.18	
Date of signature		02/06/2004		02/05/2004		02/06/2004	
Number of virus records		69.415		89.689		87.468	
ProActive detection of ITW-samples*							
In-The-Wild samples	73	12	16%	2	3%	0	0%
ProActive detection of "NEW" zoo-samples**							
DOS viruses	10	0	0%	0	0%	0	0%
Windows viruses	83	33	40%	8	10%	5	6%
Macro viruses	5	4	80%	2	40%	0	0%
Script viruses	141	11	8%	4	3%	0	0%
Worms	541	151	28%	147	27%	54	10%
Backdoors	1.593	288	18%	378	24%	105	7%
Trojans	818	26	3%	8	1%	1	0%
other malware	80	0	0%	1	1%	0	0%
OtherOS malware	80	0	0%	12	15%	0	0%
TOTAL	3.351	513	15%	560	17%	165	5%
ProActive detection of "already known" zoo-samples***							
DOS viruses	151	27	18%	51	34%	25	17%
Windows viruses	198	124	63%	133	67%	85	43%
Macro viruses	68	56	82%	58	85%	42	62%
Script viruses	187	68	36%	62	33%	38	20%
Worms	428	219	51%	283	66%	199	46%
Backdoors	751	317	42%	378	50%	167	22%
Trojans	527	126	24%	105	20%	56	11%
other malware	74	5	7%	15	20%	10	14%
OtherOS malware	9	3	33%	6	67%	3	33%
TOTAL	2.393	945	39%	1.091	46%	625	26%
Retrospective test****							
All new samples above of last 3 months	**5.817**	1.470	**25%**	1.653	**28%**	790	**14%**
ProActive detection of other samples*****							
Adware, Spyware	156	8	5%	7	4%	12	8%
Backdoor/Trojan-Like Software	215	52	24%	51	24%	11	5%
Constructors, Virus-, Hackertools	113	4	4%	3	3%	7	6%
Dangerous software	110	5	5%	6	5%	5	5%
Dialers	151	1	1%	56	37%	28	19%
Intended samples, components, etc.	1.211	55	5%	859	71%	27	2%
TOTAL	1.956	125	6%	982	50%	90	5%

Used ITW-samples:

Samples are listed using KAV names and McAfee names (note that other vendors could use other variant names). All samples appeared ITW at least in german-speaking regions. We used just the worms, not the dropped components. The list does NOT rely only on the main list of the International Wildlist[1] but also on other reported ItW-cases.

ITW-samples (KAV-names): I-Worm.Bagle.b, I-Worm.Bagle.c, I-Worm.Bagle.e, I-Worm.Bagle.f, I-Worm.Bagle.g, I-Worm.Bagle.h, I-Worm.Bagle.i, I-Worm.Bagle.j, I-Worm.Bagle.k, I-Worm.Bagle.n, I-Worm.Bagle.o, I-Worm.Bagle.p, I-Worm.Bagle.s, I-Worm.Bagle.t, I-Worm.Bagle.y, I-Worm.Bagle.z, I-Worm.Mydoom.e, I-Worm.Mydoom.f, I-Worm.Mydoom.g, I-Worm.NetSky.aa, I-Worm.NetSky.ab, I-Worm.NetSky.b, I-Worm.NetSky.c, I-Worm.NetSky.d, I-Worm.NetSky.e, I-Worm.NetSky.g, I-Worm.NetSky.h, I-Worm.NetSky.j, I-Worm.NetSky.p, I-Worm.NetSky.q, I-Worm.NetSky.r, I-Worm.NetSky.x, I-Worm.NetSky.y, I-Worm.Sober.d, I-Worm.Sober.e, I-Worm.Sober.f, Worm.Win32.Doomjuice.a, Worm.Win32.Doomjuice.b, Worm.Win32.Sasser.a, Worm.Win32.Sasser.c, Worm.Win32.Welchia.b.

ITW-samples (McAfee-names): W32/Bagle.b@MM, W32/Bagle.d@MM, W32/Bagle.c@MM, W32/Bagle.e@MM, W32/Bagle.f@MM, W32/Bagle.h@MM, W32/Bagle.i@MM, W32/Bagle.j@MM, W32/Bagle.k@MM, W32/Bagle.g@MM, W32/Bagle.n@MM, W32/Bagle.p@MM, W32/Bagle.q@MM, W32/Bagle.t@MM, W32/Bagle.u@MM, W32/Bagle.z@MM, W32/Bagle.aa@MM, W32/Mydoom.f@MM, W32/Mydoom.g@MM, W32/Mydoom.h@MM, W32/Netsky.z@MM, W32/Netsky.aa@MM, W32/Netsky.b@MM, W32/Netsky.c@MM, W32/Netsky.d@MM, W32/Netsky.e@MM, W32/Netsky.g@MM, W32/Netsky.h@MM, W32/Netsky.j@MM, W32/Netsky.o@MM, W32/Netsky.p@MM, W32/Netsky.q@MM, W32/Netsky.w@MM, W32/Netsky.x@MM, W32/Sober.d@MM, W32/Sober.e@MM, W32/Sober.f@MM, W32/Doomjuice.worm.a, W32/Doomjuice.worm.b, W32/Sasser.worm.c, W32/Sasser.worm.a, W32/Sasser.worm.b, W32/Sasser.worm.d, W32/Nachi.worm.b.

[1] The WildList Organisation International www.wildlist.org

4. Summary results

Here are the results reached by each scanner on various categories, sorted by detection rate over the samples appeared in a 3-month time period:

(a) ProActive detection of new ITW-samples:

1.	NOD32	33%
2.	Panda	16%
3.	McAfee	15%
4.	Dr.Web	7%
5.	BitDefender	4%
6.	RAV	3%
7.	Symantec	1%
8.	all the others	0%

(b) ProActive detection of new Backdoors, Trojans and other malware:

1.	McAfee	41%
2.	NOD32	39%
3.	Kaspersky	35%
3.	Dr.Web	35%
4.	BitDefender	27%
5.	Symantec	16%
5.	RAV	16%
6.	Panda	13%
7.	TrendMicro	6%
8.	F-Prot	5%
9.	Sophos	4%
9.	Avast	4%
10.	H+BEDV	2%

(c) ProActive detection of new DOS, Windows and OtherOS viruses/malware, Worms, Macro and Script viruses/malware:

1.	McAfee	39%
2.	NOD32	33%
3.	Kaspersky	30%
4.	Symantec	27%
5.	BitDefender	26%
5.	Dr.Web	26%
6.	Panda	23%
7.	RAV	20%
8.	Avast	10%
9.	F-Prot	8%
10.	Sophos	7%
11.	H+BEDV	6%
11.	TrendMicro	6%

The categories (a), (b) and (c) shows the detection rates over samples that were unknown to ANY tested product. The results shows the pure proactive detection capabilities of the scan engines.

(d) ProActive detection of "already known" samples:

1.	Kaspersky	82%
2.	McAfee	72%
3.	Dr.Web	60%
4.	Symantec	59%
5.	NOD32	48%
6.	RAV	46%
7.	BitDefender	45%
8.	Panda	39%
9.	TrendMicro	36%
10.	F-Prot	31%
11.	Avast	27%
12.	Sophos	26%
13.	H+BEDV	25%

The category (d) shows the detection rates over samples that were already know to some anti-virus companies. The results could be interpreted as which anti-virus was the first in having most of those samples or was faster to detect them.

(e) ProActive detection of Adware, Dialer, Tools and all other kind of potentially malicious software:

1.	McAfee	59%
2.	RAV	50%
3.	Kaspersky	23%
4.	H+BEDV	18%
5.	Symantec	16%
6.	F-Prot	11%
7.	Dr.Web	9%
7.	BitDefender	9%
8.	Panda	6%
8.	Avast	6%
8.	TrendMicro	6%
8.	NOD32	6%
9.	Sophos	5%

(f) Retrospective Test (proactive detection results over all samples received during the 3-month period):

1.	Kaspersky	53%
1.	McAfee	53%
2.	Dr.Web	43%
3.	NOD32	42%
4.	Symantec	35%
5.	BitDefender	34%
6.	RAV	28%
7.	Panda	25%
8.	TrendMicro	18%
9.	F-Prot	15%
10.	Avast	14%
10.	Sophos	14%
11.	H+BEDV	12%

5. Credits & ranks

Based on the results above, the products will now be scored as follow (I made this just for my own curiosity):

Importance given to the categories:
The importance is weighted as follow based on the sources where they reached us (= from where/who) and in order to try to deliver fair results to all participating companies. But by doing so, the rankings are very subjective - this is how I would rank the scanners based on this test. As you see, I give much more importance to ItW-samples than to other samples.

A = % *3.0
B = % *1.2
C = % *1.5
D = % *1.0
E = % *0.1

The numbers are adapted for the use with the previous credits and are calculated as follow:
10 - {11 – [(∑ %CAT)/ 7]} = CREDIT

	a	b	c	d	e	**CREDIT FOR THIS TEST**
Avast	8	9	8	11	8	7.4
BitDefender	5	4	5	7	7	4.0
Dr.Web	4	3	5	3	7	2.8
F-Prot	8	8	9	10	6	7.2
H+BEDV	8	10	11	13	4	8.4
Kaspersky	8	3	3	1	3	3.8
McAfee	3	1	1	2	1	1.0
NOD32	1	2	2	5	8	1.0
Panda	2	6	6	8	8	3.4
RAV	6	5	7	6	2	4.8
Sophos	8	9	10	12	9	8.0
Symantec	7	5	4	4	5	4.4
TrendMicro	8	7	11	9	8	7.4

Based on those results, I would rank the products as follow:

1st place:	McAfee	(1.0)
1st place:	NOD32	(1.0)
2nd place:	Dr.Web	(2.8)
3rd place:	Panda	(3.4)
4th place:	Kaspersky	(3.8)
5th place:	BitDefender	(4.0)
6th place:	Symantec	(4.4)
7th place:	RAV	(4.8)
8th place:	F-Prot	(7.2)
9th place:	TrendMicro	(7.4)
9th place:	Avast	(7.4)
11th place:	Sophos	(8.0)
12th place:	H+BEDV	(8.4)

The test results we provide are done mainly on zoo-samples and all tested scanners detect now most of them, even though it is highly unlikely that you will ever encounter one of them on your PC. We provide theoretical statistics. For other test based only on ItW-samples, look on the results provided by some other testing organizations.

If you now put the credits of the comparative Nr.1 together with the credits of the comparative Nr.2, you will see how I personally would rank how the scan engines were in February 2004. Anyway I remember you that ALL the tested products are really very good scanners and if you use any of them, you can feel safe against real threats.

CREDITS OF THE COMPARATIVE NR.1 WERE:

1st place: Kaspersky	(1.4)
2nd place: McAfee	(2.2)
3rd place: Panda	(4.0)
3rd place: RAV	(4.0)
4th place: F-Prot	(5.6)
5th place: Symantec	(6.6)
6th place: Dr.Web	(7.8)
6th place: Sophos	(7.8)
7th place: BitDefender	(8.8)
8th place: NOD32	(9.0)
9th place: Avast	(9.8)
10th place: TrendMicro	(11.0)
10th place: H+BEDV	(11.0)

TOTAL CREDITS FOR TEST Nr.1 + Nr.2:

1st place: McAfee	(3.2)
2nd place: Kaspersky	(5.2)
3rd place: Panda	(7.4)
4th place: RAV	(8.8)
5th place: NOD32	(10.0)
6th place: Dr.Web	(10.6)
7th place: Symantec	(11.1)
8th place: BitDefender	(12.8)
8th place: F-Prot	(12.8)
9th place: Sophos	(15.8)
10th place: Avast	(17.2)
11th place: TrendMicro	(18.4)
12th place: H+BEDV	(19.4)

6. Copyright and Disclaimer

We can not be made liable for any damage or loss which might occur as a result of, or in connection with the use of the information provided in this paper. We takes every care to ensure the correctness of the basic data, but a liability for the correctness of the test results can not be taken by Andreas Clementi. We do not give any guaranty for the correctness, completeness, etc. for a certain purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage or loss of profits arising out of or related to the use or inability to use the services provided by the site and correlate data.

Andreas Clementi, Austria (May 2004)