Experiences of CheckVir Anti-Virus Testing

Ph.D. Ferenc Leitold

fleitold@checkvir.com

www.checkvir.com

VESZPROG Ltd.
&
University of Veszprém

Contents

- CheckVir project
- Resources
- Publicity
- Tested products
- Some results

CheckVir project

VESZPROG

- **Developing automatic AV testing methods**
  - started at the end of 2000
  - supported by the *Hungarian Ministry of Education, Research and Development Division*
- **Building infrastructure – increasing computing capacity**
  - supported by the *Hungarian Ministry of Informatics*

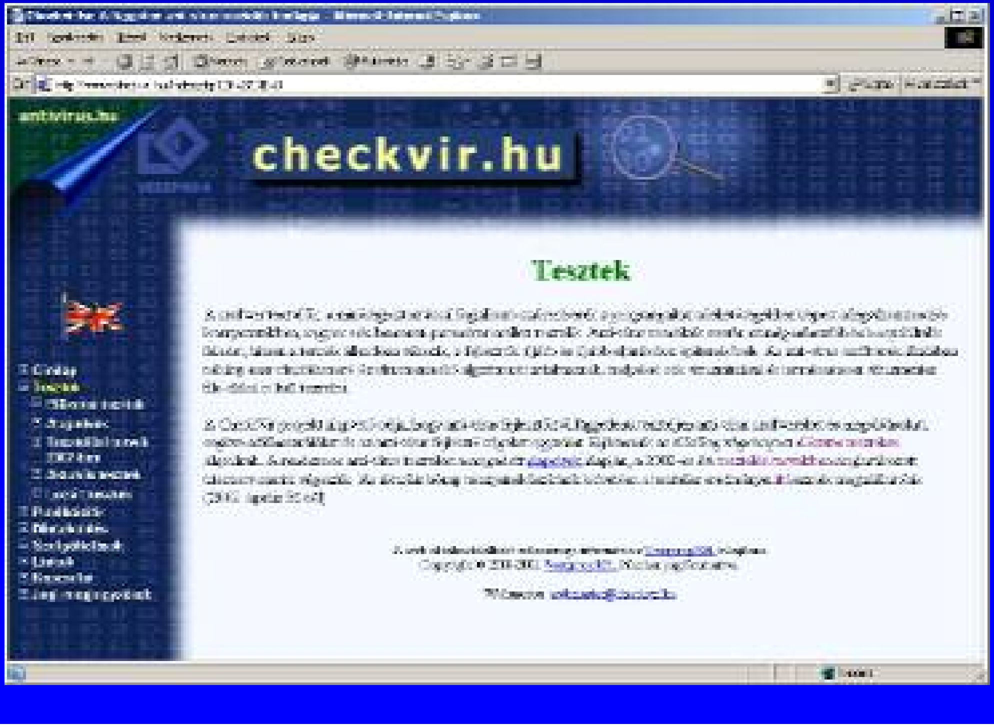
Resources

- Hardware
  - 25 P IV computer
  - 100 Mbit/s network
  - archiving systems (DVD RW, 24 GB tape)

- Software
  - MSDN Universal
  - Novell Developer Kit
  - Debian Linux
  - Virtual machine software (VMWare, Win4Lin)
  - Macro tools (Macro Express, Wintask)

Publicity

- Testing plan was announced in March 2002
  - Results published on www.checkvir.hu & www.checkvir.com
  - Summary of results published in October 2002 issue of the hungarian CHIP



Tesztek

[illegible]

[illegible]

Publicity

- Testing from November 2002 to October 2003
  - Results published on www.checkvir.hu & www.checkvir.com
  - Results are published monthly in the hungarian PCWORLD from January to December 2003

Tested products

VESZPROG

Developer	Product(s)
Computer Associates	eTrust InoculateIT
F-Secure	F-Secure Anti-Virus 5
GeCAD Software	RAV for Windows, Linux, MS Exchange
ID Anti-Virus Lab.	Dr. Web for Windows 95-XP, Unix
Kaspersky Lab.	Kaspersky Anti-Virus
Network Associates	McAfee VirusScan
Norman	Norman Virus Control, Norman for MS Exchange
Panda Software	Panda Antivirus Titanium, Platinum 7
Softwin	BitDefender Prof., BitDefender for Linux, MS Exchange
Sophos	Sophos Anti-Virus
Symantec Corporation	Norton AntiVirus 2003, Norton AntiVirus Corporate
VirusBuster Ltd.	VirusBuster for Windows, Linux, MS Office

Some results

- Virus knowledge tests
- Speed tests
- Testing heuristic

Virus knowledge tests

VESZPROG

	BitDef.	Dr.Web	eTrust	FSAV	KAV	McAfee	NAV2003	Nort.Corp.	NVC	Panda	RAV	Sophos	Vbuster
ItW test set (170 viruses)													
ON DEMAND TEST													
all samples unknown	0	1	0	0	0	0	0	0	0	0	0	0	0
all samples known	169	168	170	170	170	170	170	170	168	169	168	170	170
some samples unknown	1	1	0	0	0	0	0	0	2	1	2	0	0
ON ACCESS TEST													
all samples unknown	0	1	0	0	0	0	0	0	0	0	0	0	0
all samples known	169	167	170	170	170	170	170	170	167	169	167	170	170
some samples unknown	1	2	0	0	0	0	0	0	3	1	3	0	0
Polymorphic test set (45 viruses)													
ON DEMAND TEST													
all samples unknown	0	0	0	0	0	0	0	0	0	0	0	0	0
all samples known	40	40	45	45	44	44	43	43	43	40	42	44	45
some samples unknown	5	5	0	0	1	1	2	2	1	5	3	1	0
ON ACCESS TEST													
all samples unknown	0	0	0	0	0	0	0	0	0	0	0	0	0
all samples known	40	40	45	45	44	44	43	43	43	40	42	44	45
some samples unknown	5	5	0	0	1	1	2	2	1	5	3	1	0

Virus knowledge tests

VESZPROG

	BitDef.	Dr.Web	eTrust	FSAV	KAV	McAfee	NAV2003	Nort.Corp.	NVC	Panda	RAV	Sophos	Vbuster
ItW test set (170 viruses)													
ON DEMAND TEST													
all samples unknown	0	1	0	0	0	0	0	0	0	0	0	0	0
all samples known	169	168	170	170	170	170	170	170	168	169	168	170	170
some samples unknown	1	1	0	0	0	0	0	0	2	1	2	0	0
ON ACCESS TEST													
all samples unknown	0	1	0	0	0	0	0	0	0	0	0	0	0
all samples known	169	167	170	170	170	170	170	170	167	169	167	170	170
some samples unknown	1	2	0	0	0	0	0	0	3	1	3	0	0
Polymorphic test set (45 viruses)													
ON DEMAND TEST													
all samples unknown	0	0	0	0	0	0	0	0	0	0	0	0	0
all samples known	40	40	45	45	44	44	43	43	43	40	42	44	45
some samples unknown	5	5	0	0	1	1	2	2	1	5	3	1	0
ON ACCESS TEST													
all samples unknown	0	0	0	0	0	0	0	0	0	0	0	0	0
all samples known	40	40	45	45	44	44	43	43	43	40	42	44	45
some samples unknown	5	5	0	0	1	1	2	2	1	5	3	1	0

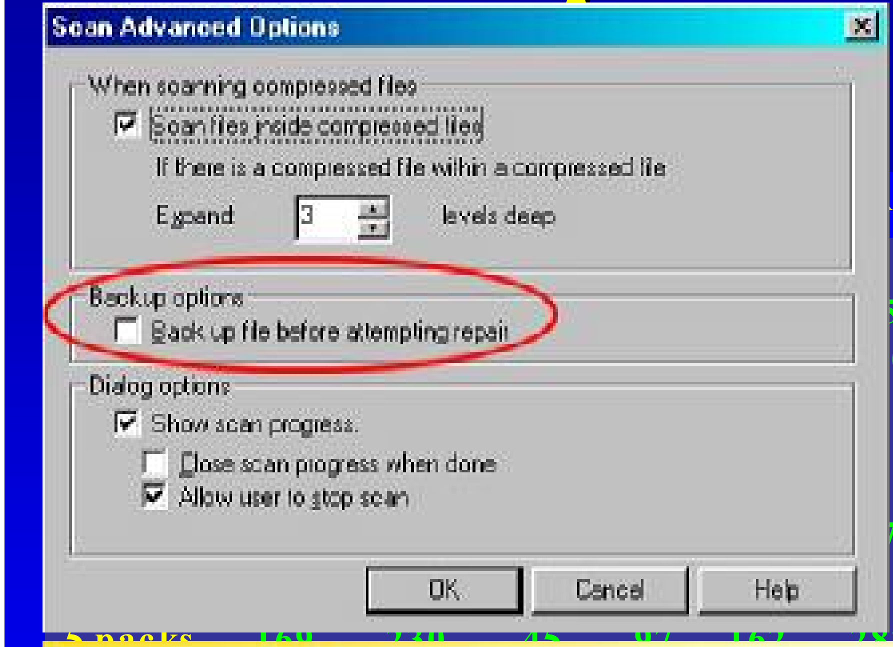
Speed tests

VESZPROG

	BitDef.	Dr.Web	eTrust	FSAV	KAV	McAfee	NAV2003	Nort.Corp.	NVC	Panda	RAV	Sophos	Vbuster
Time of scanning virus free files (sec)													ON DEMAND TESTS
1 pack	597	79	53	286	138	85	76	77	150	48	189	32	99
5 packs	3358	392	279	1251	695	410	341	354	736	227	955	216	493
10 packs	6726	798	581	2517	1408	821	665	723	1487	342	1921	483	975
Time of scanning infected files (sec)													
1 pack	34	43	10	23	33	57	137* 648**	64* 713**	22	15	39	44	72
5 packs	169	230	45	97	162	282	670* 6875**	290* 95575**	122	81	170	233	352
10 packs	344	422	89	190	334	564	1348*	833*	427	159	332	463	698
Time of copiing virus free files (sec)					Time of copiing without AV: 327 sec.								ON ACCESS TEST
5 packs	3207	647	645	2764	3280	1328	647	672	599	637	1983	1145	1445

Speed tests

VESZPROG



Scan Advanced Options

When scanning compressed files

☑ Scan files inside compressed files

If there is a compressed file within a compressed file

Expand 3 levels deep

Backup options

□ Back up file before attempting repair

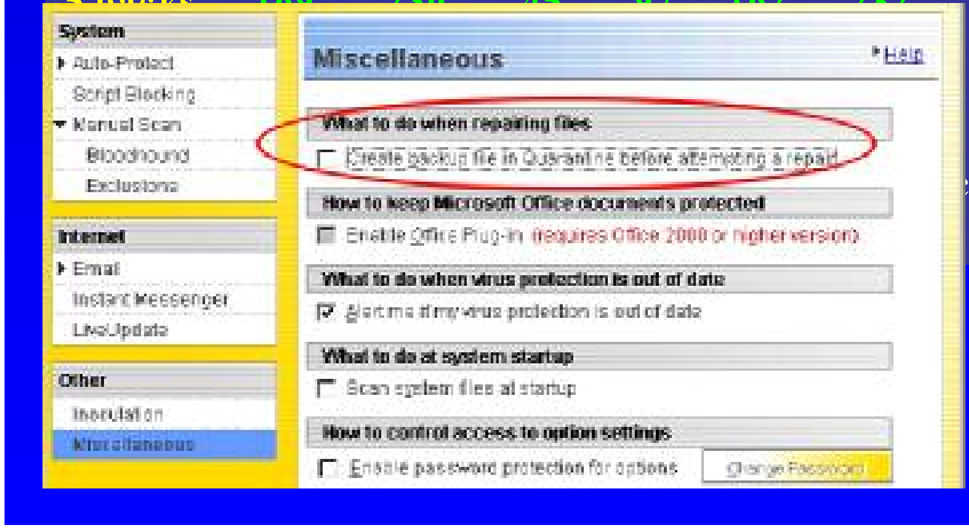
Dialog options

☑ Show scan progress.

□ Close scan progress when done

☑ Allow user to stop scan

	…fee	NAV2003	Nort.Corp.	NVC	Panda	RAV	Sophos	Vbuster
								ON DEMAND TESTS
	5	76	77	150	48	189	32	99
	0	341	354	736	227	955	216	493
	1	665	723	1487	342	1921	483	975
	7	137* 648**	64* 713**	22	15	39	44	72
5 packs 169 230 45 97 163	282	670* 6875**	290* 95575**	122	81	170	233	352
		1348*	833*	427	159	332	463	698
…opiing without AV: 327 sec.								ON ACCESS TEST
		647	672	599	637	1983	1145	1445



Miscellaneous

What to do when repairing files

□ Create backup file in Quarantine before attempting a repair

How to keep Microsoft Office documents protected

□ Enable Office Plug-in (requires Office 2000 or higher version)

What to do when virus protection is out of date

☑ Alert me if my virus protection is out of date

What to do at system startup

□ Scan system files at startup

How to control access to option settings

□ Enable password protection for options

Speed tests

VESZPROG

	BitDef.	Dr.Web	eTrust	FSAV	KAV	McAfee	NAV2003	Nort.Corp.	NVC	Panda	RAV	Sophos	Vbuster
Time of scanning virus free files (sec)													ON DEMAND TESTS
1 pack	597	79	53	286	138	85	76	77	150	48	189	32	99
5 packs	3358	392	279	1251	695	410	341	354	736	227	955	216	493
10 packs	6726	798	581	2517	1408	821	665	723	1487	342	1921	483	975
Time of scanning infected files (sec)													
1 pack	34	43	10	23	33	57	137* 648**	64* 713**	22	15	39	44	72
5 packs	169	230	45	97	162	282	670* 6875**	290* 95575**	122	81	170	233	352
10 packs	344	422	89	190	334	564	1348*	833*	427	159	332	463	698
Time of copiing virus free files (sec)						Time of copiing without AV: 327 sec.							ON ACCESS TEST
5 packs	3207	647	645	2764	3280	1328	647	672	599	637	1983	1145	1445

Testing heuristic

	BitDef.	Dr.Web	eTrust	FSAV	KAV	McAfee	NVC	NAV2003	Nort.Corp.		Panda		RAV	Sophos		Vbuster	
Heuristic level										1	2	3			1	2	3
all suspicious	16	27	4	13	4	19	1	7	7	7	14	19	8	0	2	16	18
some suspicious	20	25	5	11	4	22	6	6	6	11	17	17	4	0	4	17	18
all suspicious or infected	3	0	3	5	2	3	2	1	1	0	0	1	3	0	0	0	0
some suspicious or infected	3	2	3	4	3	0	4	0	0	2	2	2	1	0	0	0	0
all reported multiply	1	1	0	0	3	0	0	0	0	0	0	0	1	0	0	0	0
some reported multiply	1	1	0	0	6	0	0	0	1	0	0	0	1	0	0	0	0
all reported, else	1	4	3	4	9	2	1	1	1	0	2	2	3	0	0	0	0
some reported, else	2	1	0	0	2	0	1	1	2	1	1	1	0	3	0	0	0
All samples reported	21	32	10	22	18	24	4	9	9	7	16	22	15	0	2	16	18
Some samples reported	26	29	8	15	15	22	11	7	9	14	20	20	6	3	4	17	18
At least one sample reported	47	61	18	37	33	46	15	16	18	21	36	42	21	3	6	33	36
NOT reported	252	238	281	262	266	253	284	283	281	278	263	257	278	296	293	266	263

Testing heuristic

VESZPROG

	BitDef.	Dr.Web	eTrust	FSAV	KAV	McAfee	NVC	NAV2003	Nort.Corp.	Panda			RAV	Sophos	Vbuster		
Heuristic level										1	2	3			1	2	3
all suspicious	16	27	4	13	4	19	1	7	7	7	14	19	8	0	2	16	18
some suspicious	20	25	5	11	4	22	6	6	6	11	17	17	4	0	4	17	18
all suspicious or infected	3	0	3	5	2	3	2	1	1	0	0	1	3	0	0	0	0
some suspicious or infected	3	2	3	4	3	0	4	0	0	2	2	2	1	0	0	0	0
all reported multiply	1	1	0	0	3	0	0	0	0	0	0	0	1	0	0	0	0
some reported multiply	1	1	0	0	6	0	0	0	1	0	0	0	1	0	0	0	0
all reported, else	1	4	3	4	9	2	1	1	1	0	2	2	3	0	0	0	0
some reported, else	2	1	0	0	2	0	1	1	2	1	1	1	0	3	0	0	0
All samples reported	21	32	10	22	18	24	4	9	9	7	16	22	15	0	2	16	18
Some samples reported	26	29	8	15	15	22	11	7	9	14	20	20	6	3	4	17	18
At least one sample reported	47	61	18	37	33	46	15	16	18	21	36	42	21	3	6	33	36
NOT reported	252	238	281	262	266	253	284	283	281	278	263	257	278	296	293	266	263

-> maximum ~20% of new viruses found

Future plans

Test is going on …

- test on bigger sets
- test disinfection

VESZPROG

?

www.checkvir.com