Anti-Virus Comparative

On-demand detection of Spyware, Adware, dangerous tools and other potentially unwanted software

Date: October 2006 (2006-10)

Last revision: 31th October 2006

Author: Andreas Clementi

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

1. Introduction

This is the first test of this kind done by AV-Comparatives. Due that, it may not be optimal and improvements may follow in future tests.

This is an on-demand file content detection test of Spyware, Adware, dangerous tools and other potentially unwanted software. As the test-set contains also other potential threats, it should be avoided to call it "Spyware-Test". By file content means that the files have to be detected regardless of their location and their names, which is an essential ability for the detection of the files used for this test, as potential threats can be located anywhere and with any name. This test will not tell anything about removal capabilities. The goal of this test is of informational purpose only: it will show you which products warn you about the presence of those potentially unwanted files and how much they detect from the AV-Comparatives set of unwanted programs, as nowadays pratically all Anti-Virus products include additional settings to detect also such files/programs.

2. Tested products

We test only Anti-Virus products. All products were updated the 19th October 2006 and used with the best possible detection settings/databases. The following 15 products were tested:

- Avast! 4.7 Professional Edition
- AVG Anti-Malware 7.5
- AVIRA AntiVir Premium 7
- BitDefender Anti-Virus 10
- Dr.Web Anti-Virus for Windows 95-XP 4.33
- ESET NOD32 Anti-Virus 2.5
- F-Prot Anti-Virus 4 (BETA)
- F-Secure Anti-Virus 2007
- Gdata AntiVirusKit (AVK) 2007
- Kaspersky Anti-Virus 6.0
- McAfee VirusScan Plus 2007
- Norman Virus Control 5.82
- Symantec Norton Anti-Virus 2007
- TrustPort Antivirus Workstation 2.0
- VBA32 Workstation 3.11.1

3. Test-Set

For this test, only Win32 PE executables (*.EXE and *.DLL files) were included in the test-set, which means that registry entries, cookies, traces, etc. are not included. This Test-Set contains about 77000 files, which are NOT included in our regular test-sets used for our usual quadrimestral on-demand tests. They are not included in our regular test-sets because those files for various reasons do not fit in the given malware categories.

Some programs/files can be considered as "clean" (depending e.g. on what their purpose is and if their presence is acknowledged) or as "Greyware", so their detection is not a must and only facultative/optional. They can and should not be called false positives. For false positive rates of Anti-Virus products, please have a look on the false alarm test results included in the latest test report of May and November.

In any case, those files are generally files that users usually would not like to have on their PC without their consent.

The 'unwanted files' test-set contains:
a) harmful Adware, Spyware, Ad-Spy-related downloaders, Hijackers, Keyloggers, Trojans, RAT's, Rootkits, etc. (62%)
b) Backdoor tools, constructors/kits, various potentially dangerous or potentially unwanted (virus/hacker) tools and applications (24%)
c) Dialers, etc. (14%)

Most home users are hitted by the first category a), which is with 62% also the most represented category in this test-set. Some tools may be for legitimate use and pose a marginal risk: they may get detected by various AV programs with enabled riskware detection options due various reasons, e.g. because a large corporate asked the AV vendor to add detection for this kind of tool or because many home users bothered the AV vendor to detect this 'unusual' tool or because also product Z detects it and users want also their product to detect it.

4. Test results

Those results are of informational use only – they tell you which product detects on-demand more or fewer of the files included in the specific test-set, but nothing more. So it can not be stated product X is "better" than product Y, as the detection of such kind of files are not a must for an Anti-Virus product. The results are:

1. Gdata AVK	~97%
2. F-Secure, Kaspersky, AVIRA	~96%
3. TrustPort, BitDefender, McAfee	~92%
4. ESET (NOD32), Symantec, AVG, Dr.Web, Norman	~89%
5. Avast, VBA32	~82%
6. F-Prot (Beta)	~72%

5. Final notes

The on-demand detection/information given by the tested Anti-Virus products[1] about the presence of Spyware[2] and other potentially unwanted software is in general very high.
In this kind of test, some dedicated Anti-Spyware products would for various reasons score very low compared to the results of those Anti-Virus products. If readers anyway feel safer by using also another additional dedicated Anti-Spyware[3] product, it should be considered that every additional program running in the background takes additional system resources (for maybe not that much additional benefit). Testing Anti-Spyware products correctly is a complicated and time-consuming task. Due that, we will not attempt to test dedicated Anti-Spyware products and redirect users to other independent testing organizations like e.g. WCL Checkmark - www.westcoastlabs.org.
This test does not just determine the level of protection - as it contains also Greyware, user preference has to be taken into account: If an user does not think such applications are an issue, some products may annoy him with the alerts. If an user thinks those applications are an issue, then some products may be more comforting.

[1] Some other product we could not include or name scored lower than the ones you see here tested.
[2] http://www.antispywarecoalition.org/documents/DefinitionsJune292006.htm
[3] Suggested freeware Anti-Spyware products: Windows Defender, Spybot Search & Destroy.
Suggested commercial Anti-Spyware products: PC-Tools Spyware Doctor, Webroot SpySweeper.

Five suggestions[4] to lower the risk of spyware and other threats:

- Do not use your PC with administration rights
- Use legal software and install only applications you really need
- Keep your system, browser, mail client and other applications up-to-date and configure the security/privacy settings properly
- If you do not use a Security Suite, use at least an Anti-Virus and a Firewall – and keep them updated
- Do not trust every website or other sources: Be aware that even programs contained on CD/DVD of some computer magazines contain potentially dangerous tools, harmful adware or spyware which will affect your system.

6. Copyright and Disclaimer

Andreas Clementi, AV-Comparatives (October 2006)

[4] More detailed tips can be found for example on www.antispywarecoalition.org/documents/safetytips.htm