Anti-Virus Comparative

On-demand Detection of (Potentially) Unwanted Applications

like Adware, Spyware, Rogue Software

Language: English
November 2009
Last Revision: 2009-11-18

www.av-comparatives.org

Table of Contents

Tested Products

- avast! Free 5.0
- AVG Anti-Virus 9.0
- AVIRA AntiVir Premium 9.0
- BitDefender Anti-Virus 2010
- eScan Anti-Virus 10.0
- ESET NOD32 Antivirus 4.0
- F-Secure Anti-Virus 2010
- G DATA AntiVirus 2010

- Kaspersky Anti-Virus 2010
- Kingsoft AntiVirus 9 Plus
- McAfee VirusScan Plus 2010
- Microsoft Security Essentials 1.0
- Norman Antivirus & Anti-Spyware 7.30
- Sophos Anti-Virus 9.0.1
- Symantec Norton Anti-Virus 2010
- Trustport Antivirus 2010

Introduction

The issue with Adware, Spyware and other fraudulent software increased a lot over the past years. Such type of applications are not the typical malware and its classification is sometimes not an easy task – they are usually covered under the term "potentially unwanted applications" (PUA). Under some circumstances certain "potentially unwanted applications" are accepted/wanted applications in some countries, depending on cultural background or different judicature, due which sometimes legal disputes come up whether a software can be considered as malware or not. The term "potentially unwanted" covers this grey area. Usually our malware test-sets do not include this kind of threats, but as users may want to get an idea about the detection rate of potentially unwanted software of their Anti-Virus product. Anyway, it seems like the coverage of PUA's is similar to the coverage of malware.

The PUA Test-Set – containing around 1,1 million samples - used for this test includes only PE files and covers mainly Adware (e.g. mostly Virtumonde, Browser Hijackers, etc.), Spyware (e.g. Keyloggers, etc.), Rogue Software (e.g. mostly FakeAV's and other misleading applications, etc.). gathered from January 2009 to October 2009. We decided to do not include dialers, potentially dangerous tools and other grayware, not only because it would increase the test-set of several further millions of samples (and therefore take even longer to scan), but also because the inclusion and classification of such grayware applications is even more debatable.

The Adware/Spyware/Rogues (Potentially Unwanted Applications – PUA) sets were frozen the 10th October 2009. The system and the products were updated and frozen on the 4th November 2009.

We tested all products with highest settings (except F-Secure and Sophos – on their own request; see Report Nr. 23).

The results of our on-demand tests are usually applicable also for the on-access scanner (if configured the same way), but not for on-execution protection technologies (like HIPS, behaviour blockers, etc.).

A good detection rate is still one of the most important, deterministic and reliable features of an antivirus product. Additionally, most products provide at least some kind of HIPS, behaviour-based or other functionalities to block (or at least warn about the possibility of) malicious actions e.g. during the execution of malware, when all other on-access and on-demand detection/protection mechanism failed.

AV-Comparatives publishes also some other test reports which cover different aspects/features of the products. Please have a look on our website for further information. Even if we deliver various tests and show different aspects of Anti-Virus software, users are advised to evaluate the software by themselves and build their own opinion about them. Test data or reviews just provide guidance to some aspects that users cannot evaluate by themselves. We suggest and encourage readers to research also other independent test results provided by various well-known and established independent testing organizations, in order to get a better overview about the detection and protection capabilities of the various products over different test scenarios and various test-sets.

Please try the products on your own system before making a purchase decision based on these tests. There are also some other program features and important factors (e.g. price, ease of use/management, compatibility, graphical user interface, language, HIPS / behaviour blocker functions, etc.) to consider.

Test Results

Graph of missed samples (lower is better)
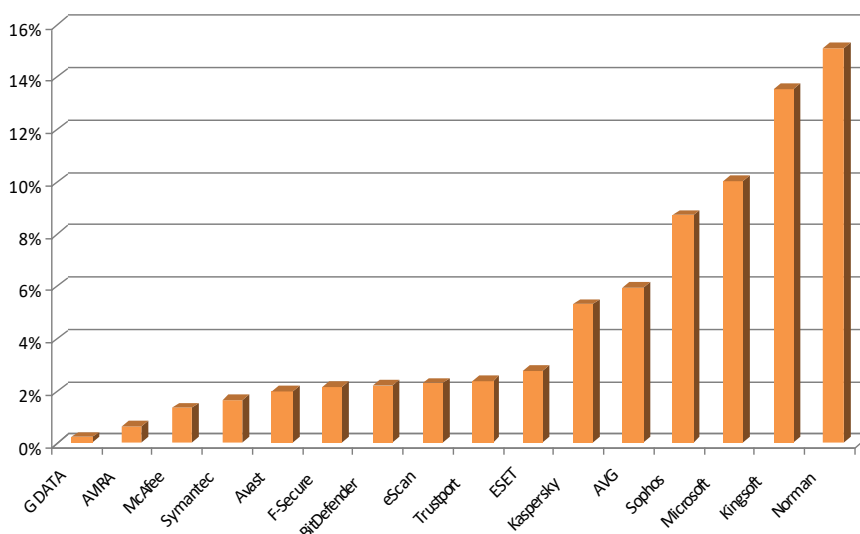
Summary results

Detection rates of Adware/Spyware/Rogues:

1.	G DATA	99%	2517
2.	McAfee[1]	98%	8841 (50794)
3.	AVIRA	99%	9985
4.	Symantec	98%	11515
5.	Bitdefender	97%	12106
6.	F-Secure	97%	12571
7.	eScan	97%	13212
8.	Trustport	97%	32251
9.	Avast	98%	32453
10.	Kaspersky	94%	32765
11.	ESET	97%	36470
12.	Sophos	91%	38805
13.	Microsoft	90%	47652
14.	AVG	94%	49662
15.	Norman	84%	91151

---

[1] McAfee VirusScan Plus 2009 and above comes with the "in-the-cloud" Artemis technology turned on by default. For corporate users or home users using older McAfee products without "Active Protection" - as well as all other users - it may be important to know what the baseline minimum detection rate of McAfee would be, should the Internet connection be not available. **The McAfee detection rate without Internet connection was 92.6%.**

| 16. | Kingsoft | 86% | 111743 |

Award levels reached in this test

AV-Comparatives provides a 3-level-ranking-system (STANDARD, ADVANCED and ADVANCED+).

AWARDS (based on detection of unwanted programs)	**PRODUCTS** (in no specific order)[2]
ADVANCED+ ★★★ ADWARE / SPYWARE DETECTION NOV 09	✓ G DATA ✓ McAfee[3] ✓ Symantec ✓ AVIRA ✓ F-Secure ✓ BitDefender ✓ eScan
ADVANCED ★★ ADWARE / SPYWARE DETECTION NOV 09	✓ Kaspersky ✓ TrustPort ✓ ESET ✓ Avast ✓ Sophos ✓ Microsoft ✓ AVG
STANDARD ★ ADWARE / SPYWARE DETECTION NOV 09	✓ Norman ✓ Kingsoft

The above Awards are based only on detection rates of unwanted programs like Adware, Spyware and Rogue AVs. For detection rates of malware like Trojans, backdoors, viruses, etc., as well as for false alarm rates of the products, please refer to the other test reports available on our website.

The awards are given according to the table below:

Detection Rates			
<87%	**87 - 93%**	**93 - 97%**	**97 - 100%**
tested	STANDARD	ADVANCED	ADVANCED+

---

[2] We suggest to consider products with same the award to be as good as the other products with same award.
3 McAfee without „in-the-cloud" would have scored ADVANCED.

Copyright and Disclaimer

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives e.V. (November 2009)