Anti-Virus Comparative

On-demand Detection of Potentially Unwanted Applications

(Adware, Spyware, Rogue Software)

Language: English
November 2009
Last Revision: 30th November 2009

www.av-comparatives.org

Table of Contents

Tested Products

- avast! Free 5.0
- AVG Anti-Virus 9.0
- AVIRA AntiVir Premium 9.0
- BitDefender Antivirus 2010
- eScan AntiVirus 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 (5400 engine)
- Microsoft Security Essentials 1.0
- Norman Antivirus & Anti-Spyware 7.30
- Sophos Anti-Virus 9.0.1
- Symantec Norton AntiVirus 2010
- Trustport Antivirus 2010

Introduction

The amount of adware, spyware and other fraudulent software circulating on the Internet has increased a great deal over the past few years. Such applications are not typical malware and their classification is sometimes not an easy task; they are usually described using the term "potentially unwanted application" (PUA). Under some circumstances, certain "potentially unwanted applications" are accepted/wanted in some countries, depending on cultural background or legal system, due to which legal disputes sometimes come up as to whether a program can be considered to be malware or not. The term "potentially unwanted" covers this grey area. Usually our malware test sets do not include this kind of threat, but users may want to know how well their Anti-Virus program detects potentially unwanted software. Anyway, it seems that the detection rates of PUAs is similar to the detection rate of malware.

The PUA test set used for this test contains 750297 samples. It includes only program executable files and covers mainly adware (e.g. Virtumonde, browser hijackers), spyware (e.g. keyloggers), and rogue software (e.g. fake antivirus and other misleading applications), gathered between January 2009 and October 2009. We decided not to include dialers, potentially dangerous tools and other greyware, also because the inclusion and classification of such greyware applications is even more debatable. Some products may classify some PUAs as Trojans, while some other products may not want to add detection for some potentially unwanted applications as their company policy.

The adware/spyware/rogue (Potentially Unwanted Applications – PUA) sets were frozen on the 29th October 2009. The system and the products were updated on the 6th November 2009. We tested all the products with highest settings (except F-Secure and Sophos on their own request; see Report No. 23).

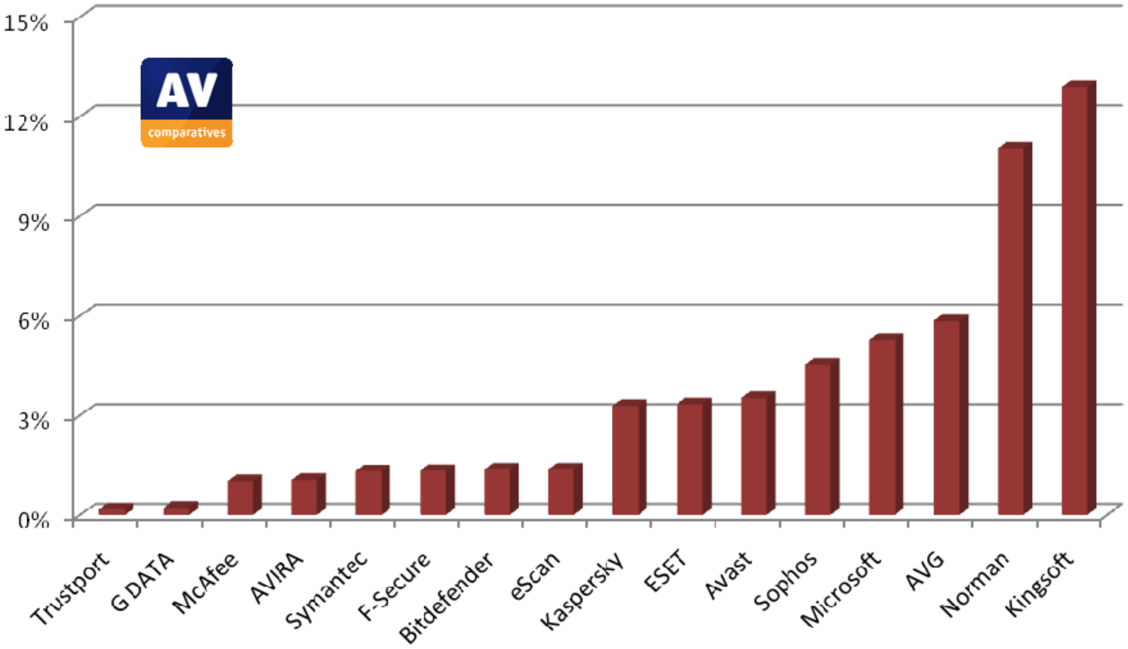
The results of our on-demand tests are usually also applicable to the on-access scanner (if configured the same way), but not for on-execution protection technologies such as host-based intrusion protection systems (HIPS) and behaviour blockers. A good detection rate is still one of the most important, deterministic and reliable features of an antivirus product. Additionally, most products provide at least some kind of HIPS, behaviour-based protection or other functionality to block (or at least warn of) malicious actions, e.g. during the execution of malware, when all other on-access and on-demand detection/protection mechanisms have failed.

AV-Comparatives also publishes some other test reports which cover different aspects/features of the antivirus products. Please have a look at our website for further information. Even if we produce various tests and show different aspects of Anti-Virus software, users are advised to evaluate the software by themselves and form their own opinion of it. Test data or reviews just provide guidance on some aspects that users cannot evaluate by themselves. We encourage readers to consider other independent test results provided by various well-known and established independent testing organizations. This will enable them to get a better overview of 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, support) to consider.

Test Results

Graph of missed samples (lower is better)



Summary results

Detection rates for adware/spyware/rogues:

1.	Trustport, G DATA	99.8%
2.	McAfee[1], AVIRA	98.9%
3.	Symantec, F-Secure, Bitdefender, eScan	98.6%
4.	Kaspersky	96.7%
5.	ESET	96.5%
6.	Avast	96.3%
7.	Sophos	95.4%
8.	Microsoft	94.6%
9.	AVG	93.9%
10.	Norman	88.5%
11.	Kingsoft	87.1%

[1] McAfee comes with "in-the-cloud" Artemis technology turned on by default. The McAfee detection rate without an Internet connection would be 94.4%.

Award levels reached in this test

AV-Comparatives provides a 4-level ranking system: TESTED, STANDARD, ADVANCED and ADVANCED+.

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

The above Awards are based only on detection rates for unwanted programs like adware, spyware and rogue AVs. To see detection rates for malware like Trojans, backdoors, viruses, etc., as well as for false alarm rates of the products, please refer to the other Main Test reports available on our website.

This was our first PUA detection test - the thresholds for the awards may change / be adapted in the next PUA detection test. Anyway, looking at the number of missed samples, three clearly distinguished detection groups can be observed – and awards given accordingly.

[2] We suggest considering all products with same the award to be as good as each other.

Copyright and Disclaimer

AV-Comparatives e.V. and its testers cannot be held 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 take every possible care to ensure the correctness of the basic data, but liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives e.V. We do not give any guarantee of the correctness, completeness, or suitability for a specific 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 website, test documents or any related data. AV-Comparatives e.V. is a registered Austrian Non-Profit-Organization.

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

AV-Comparatives e.V. (November 2009)