



# 可能有害的应用程序 手动检测报告

（包括广告软件、间谍软件和流氓软件）

语言:中文

2010年12月

最后修订: 2010年12月22日

[www.av-comparatives.org](http://www.av-comparatives.org)

# 目录



测试的产品	3
简介	4
测试结果	5
测试结果汇总	5
本次测试的获奖级别	6
版权及免责声明	7



## 测试的产品

- Aavast! Free 5.0
- AVG Anti-Virus 2011
- AVIRA AntiVir Premium 10.0
- BitDefender Antivirus 2011
- eScan AntiVirus 11.0
- ESET NOD32 Antivirus 4.2
- F-Secure Anti-Virus 2011
- G DATA AntiVirus 2011
- K7 TotalSecurity 10
- Kaspersky Anti-Virus 2011
- Kingsoft AntiVirus 2011
- McAfee Antivirus Plus 2011
- Microsoft Security Essentials 1.0
- Norman Antivirus & Anti-Spyware 8.0
- Panda Antivirus Pro 2011
- PC Tools Spyware Doctor with AV 8.0
- Sophos Anti-Virus 9.5
- Symantec Norton AntiVirus 2011
- Trend Micro Titanium Antivirus 2011
- Trustport Antivirus 2011

## 简介

在过去的几年里，通过互联网流传的广告软件、间谍软件以及特别是欺诈软件，增长速度迅猛。这种恶意程序并不是典型的病毒程序。有时，对于它们的分类也不是一项轻易就能完成的事情；所以，通常使用术语“Potentially Unwanted Application 可能有害的应用程序”（PUA）来统称此类恶意程序。在有些情况下，由于各国的文化背景或者法律制度不同，某些“可能有害的应用程序”在一些国家被接受或允许。对于那些法律纠纷，有时也正是由于对一个程序是否被认定为恶意程序或相反而产生的。所以，用术语“可能有害的”正好能够涵盖这一灰色区域。通常我们的病毒测试集不包括这种威胁程序，但用户可能想知道他们（使用或关注的）防病毒产品对于“可能有害的应用程序”的反应程度。

为本次测试准备的 PUA（可能有害的应用程序）测试集，含有 82036 个此类程序测试样本。它仅包括从 2010 年 7 月至 2010 年 11 月间已收集或再现的可执行文件程序，并且主要包括流氓软件（如假防病毒和其他误导或恶意的/不安全的应用程序）、广告软件（如 Virtumonde，浏览器劫持）和间谍软件（如键盘记录器）。有些测试的产品可能将测试样本集中的一些样本（PUAs）归类为木马程序，而另外的产品可能由于某些法律原因，不一定要添加检测“可能有害的应用程序”作为公司策略。测试集之所以如此小和有限的原因，是因为我们试图提前移除了某些可能引起争议或不该属于本测试集的程序类型（如 CasinoClients、游戏、工具栏、工具等）。那些在本次测试中得分高的产品厂商，如果（感觉）法律后果会很严重时，可能仅排除检测；否则如果单从技术层面上来讲，它有足够的检测理由的话，这些产品继续检测。特别是，如果产品有特殊复选框的，即必须用户手动选择才能获悉“可能”有害的或不安全的程序的，这些程序应该被检测，否则其属于正常检测或根本没有报告过。如果有些厂商对于那些“可能有害的程序文件”非常不情愿的通知用户的，这也能从测试结果观察到。如果一些厂商只简单地添加每一样检测（包括在灰色地带的这些程序文件），那么您在我们的网站上可能会看到它的误报测试<sup>1</sup> 结果。

PUA 测试集于 2010 年 11 月 6 日被冻结。参与测试的防病毒安全产品于 2010 年 12 月 1 最后更新。我们使用最高的设置测试了所有产品（除 F - Secure 和 Sophos 有自己的要求外）。

AV - Comparatives 还发布了一些其它的测试报告，这些报告包括了防病毒产品的各个方面和特点。更多信息请您查看我们的网站。尽管我们进行各种测试，并展示防病毒软件的各个不同方面，但用户应自行评价软件，来形成自己的观点。测试数据或评论仅提供指导，因为毕竟用户在某些方面无法自行评估。我们鼓励读者也参考其他著名的独立测试机构提供的独立测试结果。这将会使用户对各种产品，通过不同的测试场景及各种测试集（的测试）取得的检测率和保护能力，有更好的了解。

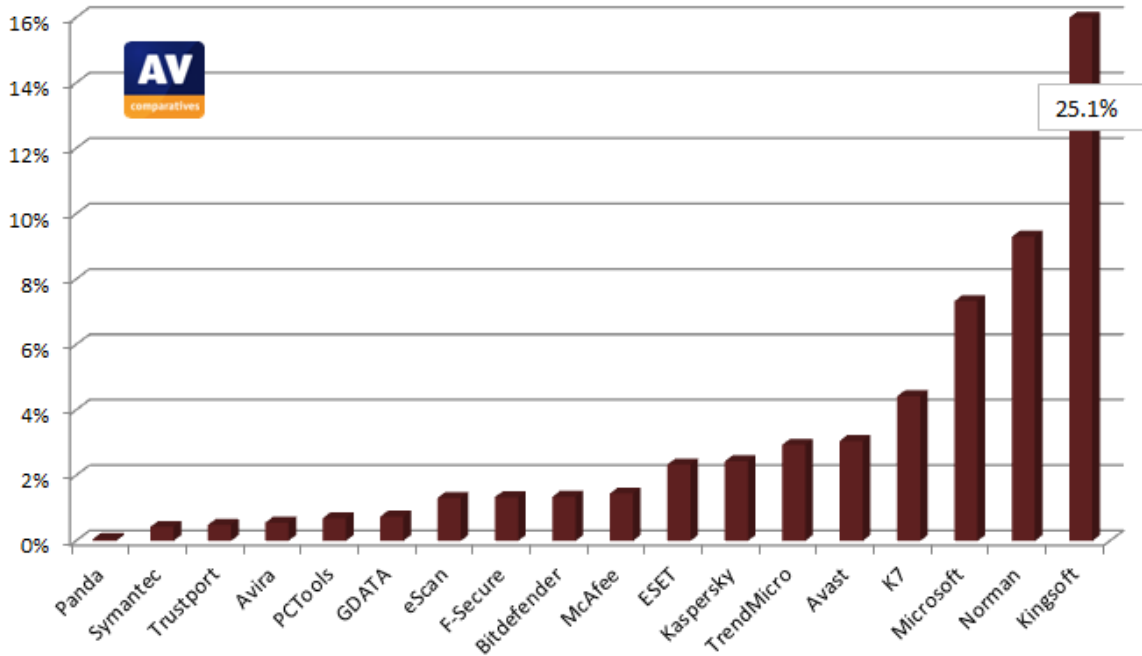
由于每个防病毒安全产品厂商都经过自己的标准来定义 PUA 工具栏，这增加了 PUA 公平测试的难度，所以，明年我们不打算进行单独的 PUA 测试。

---

<sup>1</sup> <http://www.av-comparatives.org/comparativesreviews/false-alarm-tests>

## 测试结果

### 遗漏样本图表



### 测试结果汇总

“可能有害的应用程序”检测率<sup>2</sup>：

1. Panda (熊猫) 99.9%
2. Symantec (赛门铁克) 99.6%
3. Trustport 99.5%
4. AVIRA (小红伞) 99.4%
5. PC Tools (比斯图), G DATA(歌德塔) 99.3%
6. eScan, F-Secure, Bitdefender (比特梵德), McAfee (迈克菲) 98.7%
7. ESET (NOD32) 97.7%
8. Kaspersky(卡巴斯基) 97.6%
9. Trend Micro (趋势科技) 97.1%
10. Avast 96.9%
11. K7 95.6%
12. Microsoft(微软) 92.7%
13. Norman 90.7%
14. Kingsoft (金山) 74.9%

<sup>2</sup> 其中，那些可能关心让自己的电脑无需他们的经验就拥有此功能，对“可能有害的应用程序”希望被告知的用户，可能更喜欢得分高的产品，同时，那些对于此类信息不希望防病毒安全产品通知他们的用户，可能更倾向于那些警报较保守的产品。

## 本次测试达到奖励标准

AV - Comparatives 设立的奖项为 4 级制：已测试 (TESTED)、标准 (STANDARD)、优秀 (ADVANCED) 和最佳 (ADVANCED+) 各个获奖组的定义是通过咨询/使用层次聚类法。

奖项 (以可能有害的程序检测为基础)	产品 (排名不分先后) <sup>3</sup>
	<ul style="list-style-type: none"> <li>✓ Panda (熊猫)</li> <li>✓ Symantec (赛门铁克)</li> <li>✓ Trustport</li> <li>✓ AVIRA (小红伞)</li> <li>✓ PC Tools (比斯图)</li> <li>✓ G Data (歌德塔)</li> <li>✓ eScan</li> <li>✓ F-Secure</li> <li>✓ BitDefender (比特梵德)</li> <li>✓ McAfee (迈克菲)</li> </ul>
	<ul style="list-style-type: none"> <li>✓ ESET (NOD32)</li> <li>✓ Kaspersky (卡巴斯基)</li> <li>✓ Trend Micro (趋势科技)</li> <li>✓ Avast</li> <li>✓ K7</li> </ul>
	<ul style="list-style-type: none"> <li>✓ Microsoft (微软)</li> <li>✓ Norman (诺曼)</li> </ul>
	<ul style="list-style-type: none"> <li>✓ Kingsoft (金山)</li> </ul>
不包含 <sup>4</sup>	<ul style="list-style-type: none"> <li>✓ Sophos*</li> <li>✓ AVG*</li> </ul>

以上产品取得的奖项仅以可能有害的应用程序检测率为基础。要想知道像特洛伊木马、后门、和其他各种病毒等的检测率、以及产品的误报率情况，请参阅我们网站上的其他专项测试报告。

<sup>3</sup> 我们建议对所有获得相同奖项的产品给予同等考虑。

<sup>4</sup> AVG 和 Sophos 决定不参与本次测试，并放弃获奖评选。由于这些产品参与我们每年的公开测试系列，既然这些厂商决定不参加本次测试，所以我们仅将它们列在名单上。

## 版权及免责声明

本报告的版权©归 AV-Comparatives®所有。任何出版物对本测试结果的使用，无论是全部或部分，都必须先得到 AV-Comparatives 管理部门明确的书面同意并允许。对使用本报告提供的信息，可能会产生或导致的损害或损失，AV-Comparatives 和参与测试的人员，不承担责任。我们竭尽全力可能，确保基本数据的正确性，但并不代表 AV-Comparatives 对测试结果的正确性需要承担义务。对报告的正确性，完整性，或者在任何特定的时间，对报告提供的内容是否适合特殊目的的需求，我们不做任何保证。对于在创建，生成或发表测试结果过程中，所涉及到的任何人，对任何间接的，特殊的损害或利益损失，使用或不能使用该网站提供的服务，测试文件或任何相关的数据引起的或与之相关的事宜，均不承担任何责任。AV-Comparatives 是在奥地利注册的非盈利性组织。

更多关于 AV-Comparatives 及测试方法，请访问我们的网站。

AV-Comparatives e.V. (2010 年 12 月)