安全软件评测

「恶意软件手动检测」报告

包含误报和手动扫描速度测试

语言: 中文

2011 年 8 月

最后修订：

2011 年 9 月 27 日

www.av-comparatives.org

目录

参加检测的产品	3
参与条件和测试方法	4
参加检测产品的版本	4
总评	5
检测结果	6
遗漏样本	8
测试结果概要	10
误报测试	11
按需扫描速度测试	12
本次检测产品所获奖项及评级	13
版权及免责声明	14

参加检测的产品

- avast! Free Antivirus 6.0
- AVG Anti-Virus Free Edition 10.0
- AVIRA AntiVir Personal 10.2
- BitDefender Antivirus Plus 2012
- eScan Anti-Virus 11.0
- ESET NOD32 Antivirus 5.0
- F-Secure Anti-Virus 2011
- G DATA AntiVirus 2012
- K7 TotalSecurity 11.1
- Kaspersky Anti-Virus 2012
- McAfee AntiVirus Plus 2011
- Microsoft Security Essentials 2.1
- Panda Cloud Antivirus 1.5
- PC Tools Spyware Doctor with AV 8.0
- Qihoo 360 Antivirus 2.0
- Sophos Anti-Virus 9.7
- Symantec Norton Anti-Virus 2012
- Trend Micro Titanium AntiVirus+ 2012
- Trustport Antivirus 2012
- Webroot AntiVirus with Spy Sweeper 7.0

参与条件和测试方法

参与 AV-Comparatives 测试的条件已经在我们官网的测试方法文档中公布 http://www.av-comparatives.org/seiten/ergebnisse/methodology.pdf. 读者在开始阅读本报告前，应先阅读上面提到的测试方法文档。

参与本次测试的厂商数量限定在 20 个，他们均有较高的知名度，这些厂商同意接受本次测试并参与 2011 年的一系列公开测试活动。

参与测试产品的版本

病毒样本已于 2011 年 8 月 1 日被封存。测试系统环境和产品最后更新并封存的时间是 2011 年 8 月 12 日。下列 20 款最新产品[1]参与了本次公开测试：

- avast! Free Antivirus 6.0.1203
- AVG Anti-Virus Free Edition 10.0.1392
- AVIRA AntiVir Personal 10.2.0.700
- BitDefender Anti-Virus+ 15.0.27.319
- eScan Anti-Virus 11.0.1139.998
- ESET NOD32 Antivirus 5.0.90.0
- F-Secure Anti-Virus 10.51.106
- G DATA AntiVirus 22.0.2.32
- K7 TotalSecurity 11.1.0050
- Kaspersky Anti-Virus 12.0.0.374 (abc)
- McAfee AntiVirus Plus 15.0.291
- Microsoft Security Essentials 2.1.1116.0
- Panda Cloud Antivirus Free 1.5.1
- PC Tools Spyware Doctor with Antivirus 8.0.0.655
- Qihoo 360 Antivirus 2.0.1.1332
- Sophos Anti-Virus 9.7.4
- Symantec Norton Anti-Virus 19.1.0.21
- Trend Micro Titanium AntiVirus Plus 2012
- Trustport Antivirus 10.0.0.4796
- Webroot AntiVirus with Spy Sweeper 7.0.11.25

在您参照本测试结果做出购买决定前，请先在自己的系统上试用这些产品[2]。因为您还需要考虑这些安全产品的其他众多功能，以及一些重要因素（如：价格、易用性、兼容性、用户图形界面、语言、基于主机的入侵防御（HIPS）、行为拦截功能、网页过滤器、客户服务等）。某些产品会向您提供一些附加功能，如：在恶意软件运行期间，提供额外的病毒防护（如果在事先的实时监测和手动检测中未检测到）。

[1] Avast, AVG, AVIRA 和 Panda 决定用其各自的免费版本参与本次测试。

[2] 关于产品中使用第三方杀毒引擎/病毒特征码的附加信息：eScan、F-Secure 和 奇虎 360 都是使用 BitDefender 的杀毒引擎。G DATA 使用 Avast 和 BitDefender 的杀毒引擎。PC Tools 使用赛门铁克的病毒特征码。Trustport 使用 AVG 和 BitDefender 的杀毒引擎。Webroot 使用 Sophos 的杀毒引擎。

尽管产品检测率相当的重要，但它只是整款杀毒软件的一方面特性。所以 AV-C 还提供整体产品的动态测试，即覆盖产品其他方面特征的测试报告。

总评

现在，几乎所有的杀软产品在默认情况下，都采用最高的安全设置（至少在电脑进行全盘手动扫描或计划任务扫描时），或者一旦发现病毒感染，就会自动切换到最高安全设置。因此，为了获得具有可比性的测试结果，如果厂商没有明确的要求，我们将所有测试产品都设定成最高安全设置。由于这种最高安全设置常常导致太多的误报、系统资源占用量大或者这些设置即将在不久以后被厂商更改或移除等原因，厂商可能不希望在测试过程中使用这种高安全设置。下面列出部分产品测试时所使用的（总是禁用扫描全部文件等），例如：默认情况下未设定为最高设置的地方：

Avast, AVIRA, Kaspersky, Symantec: 要求在测试中将启发式杀毒设定为高/增强。因此，我们建议用户也考虑将启发式设定为高/ /增强。

F-Secure, Sophos: 要求在测试和评级中使用各自的默认设置（即不使用他们的高级启发式杀毒/可疑检测设置）

AVG, AVIRA:要求不将压缩工具警报提示作为检测结果计入测试。因此，我们并未将这些作为检测结果计入测试（包括恶意样本库及白名单库）

AV-C 更愿意使用产品默认设置进行测试。由于大部分产品在默认情况下，都采用最高安全设置运行（或者一旦检测到恶意软件就会自动切换到的最高安全设置），为了获得具有可比性的结果并依照各个相关厂商的要求，我们仅对少数产品保留了最高安全设置（或保留较低的设置）。我们希望安全厂商在默认情况下，提供较强的安全设置，即将默认设置设到最高检测级别，尤其是用于计划扫描或已由用户启动的扫描，这样可能会更合理。我们也希望所有厂商能够去除用户界面中的偏执安全设定，如此高的设定对于普通用户而言弊大于利。由于一些厂商决定使用较强的设置参加我们的测试，这种设置显示，在默认情况下，较好的选项也适合较强的设置，这也是我们之所以建议用户也考虑使用这些设置的原因。

有几款产品使用云技术，这种技术需要保证有效的互联网连接。我们联网进行了此项测试。虽然我们不再显示无云技术的检测率底线，而只显示有效的云安全技术的检测结果，但用户应该清楚的是，处于离线状态下（通过云）进行病毒检测时，在某些少数情况下检测率可能会降低（或者因缺乏云经验，无法连接到云安全中心）。云技术应被视为一种能额外提高检测率的辅助功能（即反应次数和误报抑制），而不应被完全看做是用于本地脱机检测的替代。万一与云的连接中断时，安全厂商应确保用户能被警示，例如病毒扫描期间，这种中断可能对所提供的保护产生极大的影响并使例如已启动的扫描无效。我们已经看到，一些过多依赖云的产

品在 PE 格式的恶意软件的检测率上要略胜一筹，而在非 PE 格式的恶意软件，如目前的“其他恶意软件/病毒”类别的检测率上则较低。

已查阅的遥感测试数据也包括在近六个月以来光顾过用户的流行恶意软件样本中。由于此次关注的病毒样本都是近期流行的或广泛传播过的（多数是过去三个月内），所以为本次测试准备的样本集比以前年度的小。

测试结果

下表是各类产品使用测试集后，得出的包含详细检测率信息的测试结果。在本次测试过程中，Sophos 和 Webroot（使用 Sophos 技术）由于云技术问题，使得检测率较低。测试显示的结果也包括估计的云检测率（但仅列入测试结果展示范围之内）。

Company		Qihoo		AVIRA		Avast Software		AVG Technologies	
Product		**360 Antivirus**		**AntiVir Personal**		**avast! Free Antivirus**		**AVG Free Anti-Virus**	
Program version		2.0.1.1332		10.2.0.700		6.0.1203		10.0.1392	
Award reached in this test		ADVANCED		ADVANCED+		ADVANCED+		ADVANCED	
Number of false positives		**many**		**few**		**few**		**many**	
On-demand scanning speed		slow		fast		fast		average	
Worms	9.707	9.674	99,7%	9.680	99,7%	9.464	97,5%	9.143	94,2%
Backdoors/Bots	20.502	20.458	99,8%	20.469	99,8%	19.846	96,8%	19.924	97,2%
Trojans	170.352	169.811	99,7%	169.767	99,7%	166.083	97,5%	163.595	96,0%
other malware/viruses	5.482	4.983	90,9%	5.091	92,9%	4.981	90,9%	4.589	83,7%
TOTAL	**206.043**	204.926	**99,5%**	205.007	**99,5%**	200.374	**97,2%**	197.251	**95,7%**

Company		BitDefender		MicroWorld		F-Secure		G DATA Security	
Product		**BitDefender AV Plus**		**eScan Anti-Virus**		**F-Secure Anti-Virus**		**G DATA AntiVirus**	
Program version		15.0.27.319		11.0.1139.998		10.51.106		22.0.2.32	
Award reached in this test		ADVANCED+		ADVANCED		ADVANCED+		ADVANCED+	
Number of false positives		**few**		**many**		**few**		**few**	
On-demand scanning speed		average		average		average		average	
Worms	9.707	9.534	98,2%	9.534	98,2%	9.536	98,2%	9.689	99,8%
Backdoors/Bots	20.502	20.193	98,5%	20.213	98,6%	20.223	98,6%	20.454	99,8%
Trojans	170.352	168.150	98,7%	168.228	98,8%	168.302	98,8%	169.932	99,8%
other malware/viruses	5.482	4.955	90,4%	4.971	90,7%	4.970	90,7%	5.372	98,0%
TOTAL	**206.043**	202.832	**98,4%**	202.946	**98,5%**	203.031	**98,5%**	205.447	**99,7%**

Company		K7 Computing		Kaspersky Labs		McAfee		ESET	
Product		**K7 TotalSecurity**		**Kaspersky AV**		**McAfee AntiVirus +**		**NOD32 Antivirus**	
Program version		11.1.0050		12.0.0.374 (abc)		15.0.291		5.0.90.0	
Award reached in this test		TESTED		ADVANCED+		ADVANCED+		ADVANCED+	
Number of false positives		**many**		**very few**		**none**		**very few**	
On-demand scanning speed		fast		average		fast		average	
Worms	9.707	8.128	83,7%	9.546	98,3%	9.102	93,8%	9.461	97,5%
Backdoors/Bots	20.502	18.331	89,4%	20.313	99,1%	20.133	98,2%	19.979	97,4%
Trojans	170.352	145.650	85,5%	167.341	98,2%	165.785	97,3%	166.301	97,6%
other malware/viruses	5.482	4.323	78,9%	5.321	97,1%	4.480	81,7%	4.807	87,7%
TOTAL	**206.043**	176.432	**85,6%**	202.521	**98,3%**	199.500	**96,8%**	200.548	**97,3%**

Company *Product* *Program version*		Symantec **Norton Anti-Virus** 19.1.0.21		Panda Security **Panda Cloud AV** 1.5.1		Microsoft **Security Essentials** 2.1.1116.0		Sophos **Sophos Anti-Virus** 9.7.4	
Award reached in this test		ADVANCED		ADVANCED+		ADVANCED		N/A	
Number of false positives On-demand scanning speed		**many** average		**very few** average		**very few** slow		**many** average	
Worms	9.707	9.311	95,9%	9.675	99,7%	9.318	96,0%	8.841	91,1%
Backdoors/Bots	20.502	20.031	97,7%	20.490	99,9%	18.319	89,4%	18.953	92,4%
Trojans	170.352	162.771	95,5%	169.917	99,7%	157.361	92,4%	161.601	94,9%
other malware/viruses	5.482	3.737	68,2%	4.418	80,6%	4.668	85,2%	4.788	87,3%
TOTAL	**206.043**	195.850	**95,1%**	204.500	**99,3%**	189.666	**92,1%**	194.183	**94,2%**

Company *Product* *Program version*		PC Tools **SpywareDoctor+AV** 8.0.0.655		Trend Micro **Trend Micro TiAV+** 2012		Trustport **Trustport Antivirus** 10.0.0.4796		Webroot **Webroot AV+SS** 7.0.11.25	
Award reached in this test		TESTED		ADVANCED+		ADVANCED		N/A	
Number of false positives On-demand scanning speed		**many** slow		**few** fast		**many** slow		**many** average	
Worms	9.707	8.379	86,3%	9.386	96,7%	9.683	99,8%	8.825	90,9%
Backdoors/Bots	20.502	18.548	90,5%	19.819	96,7%	20.467	99,8%	18.928	92,3%
Trojans	170.352	152.836	89,7%	165.244	97,0%	169.961	99,8%	161.499	94,8%
other malware/viruses	5.482	2.331	42,5%	4.579	83,5%	5.102	93,1%	4.787	87,3%
TOTAL	**206.043**	182.094	**88,4%**	199.028	**96,6%**	205.213	**99,6%**	194.039	**94,2%**

总检测率由测试人员分析集群后，依据层次聚类法分组而成。同往常一样，检测结果中也考虑了误报情况。但我们也在考虑，在未来的测试和评级中是否也要对误报的评估进行改变。

通过使用集群，不再需要达到固定的阈值，因为阈值会因各种结果而有所变动。测试人员合理地定义集群，而不是单靠集群，以避免发生如果未来所有的产品成绩都不好，那么无论怎样都不能取得较高的排名。同时，我们也在为明年的测试准备不同的规则，以避免由于占据在较低集群中的外围厂商的出现，而使太多的安全厂商出现在第一集群。喜欢老的奖评制度的用户，可以自己运用固定百分比评级制度来推算。

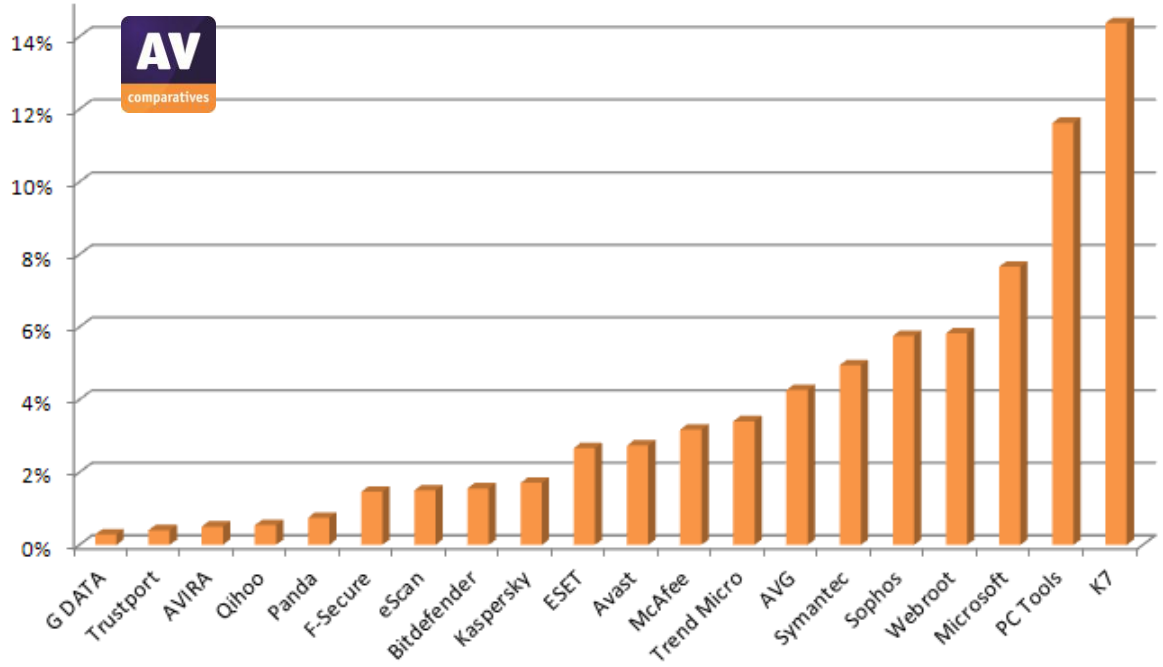
	检测率集群/组 (经测试者查阅统计方法后得出)			
	4	**3**	**2**	**1**
少误报 (0-15 个误报)		标准	优秀	最佳+
多误报 (16-100 个 误报)	已测试	已测试	标准	优秀
很多误报 (101-500 个误报)	已测试	已测试	标准	标准
极多误报 (超过 500 个误报)	已测试	已测试	已测试	已测试

我们发现，为获取好的测试结果，少数厂商试图使用游戏规则。如坚持认为某些恶意文件为“干净的文件”或“可能有害的软件”等。还有的厂商坚持，每一个未被自己的产品检测到的恶意文件都是“不重要或非流行的”恶意文件，即使别的遥测数据已显示，但仍坚持自己的观点。有时，一些厂商还声称，他们的云安全检测技术曾经检测到所有在我们测试中未检测出的样本。通常情况下，我们能够用这些实实在在的云安全技术或产品证明，他们确实不能检测或根本就没检测到我们的恶意软件样本。我们认为，当用户与云安全中心的连接中断时，依赖云安全技

术的厂商应确保他们的产品总是能够满足需求，并且能够警示用户。如果厂商的云安全中心在测试时关闭或无法访问，只要已启用了 Internet 连接，那么，这只能是产品或厂商的错误，而不能归咎于用户或测试机构。

测试结果反映了测试时的检测率。如果某些厂商的云安全需要一个完美的、稳定的、超高速的互联网连接，则应该对系统做出明确的要求。否则，应该象那些已经对企业用户使用严格的隐私策略的厂商那样，他们应为家庭用户提供本地的云安全。此外，一些厂商由于营销的原因，当得知自己的测试得分低于常规预期时，想要自己的测试结果不被公布。但我们不允许撤销测试，因为我们希望将结果提供给我们的读者。我们将来可能会找个办法来解决类似的问题。

遗漏样本图示 (越低越好)



在本次测试过程中，Sophos 和 Webroot（使用 Sophos 技术）由于云技术问题，使得检测率较低。测试显示的结果也包括估计的云检测率（但仅列入测试结果展示范围之内）。

百分比仅指测试使用的病毒样本比例。即使它只是子病毒样本，但对于查看遗漏病毒样本的数量仍然是重要的。

我们手动测试的结果通常也适用于实时扫描器（如果设置方式相同），但是并不适用于执行防御技术（如: 基于主机的入侵防御（HIPS）、行为拦截功能等）。

良好的检测率始终是评定一款杀毒软件的具有决定性并且广泛适用的最重要的因素之一。除此之外，大多数产品还会提供一些象基于主机的入侵防御（HIPS）、行为拦截、信誉评级或其他拦截功能来阻止恶意行为（或者至少是报警功能），如：在恶意软件运行期间，如果所有

的实时监测和手动检测都未能检测到它的运行，那么安全产品的这些额外病毒防护功能会发挥作用。

请不要错过包含回溯测试的报告的第二部分（它将会在几个月后发布），它对于产品对全新的/未知恶意软件的检测能力进行了评估（使用本地启发式和常规签名技术的按需或访问时扫描，而不是云安全）。

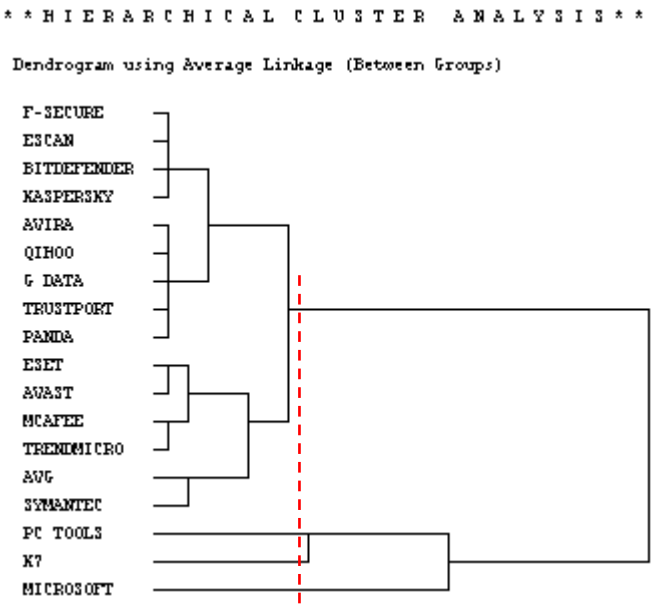
虽然我们对杀毒软件的各个方面进行了多种测试和演示，但仍然建议用户自己对软件进行评估并形成自己的意见。测试数据或报告仅提供一些指导，毕竟有些方面用户自己无法评价。我们建议并鼓励读者去研究其他各种知名的独立测试机构提供的独立测试结果，以便更好判断各种产品在不同的测试条件和测试环境下，对病毒的查杀能力。

测试结果概要

当您对比下列产品的检测率[3]时，也请考虑每款产品的误报率

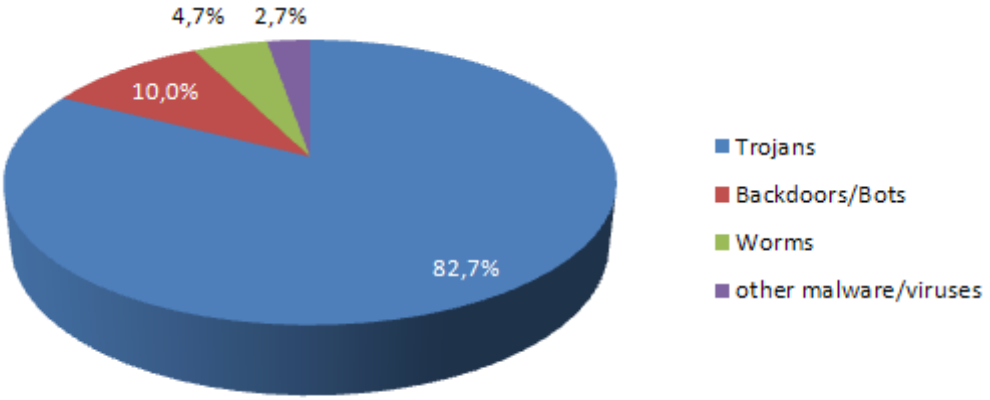
总检测率 (分为四个群组):

1.	G DATA	99.7%
2.	Trustport	99.6%
3.	AVIRA, Qihoo	99.5%
4.	Panda	99.3%
5.	F-Secure, eScan	98.5%
6.	Bitdefender	98.4%
7.	Kaspersky	98.3%
8.	ESET, Avast	97.3%
9.	McAfee	96.8%
10.	Trend Micro	96.6%
11.	AVG	95.7%
12.	Symantec	95.1%
13.	Microsoft	92.3%
14.	PC Tools	88.4%
15.	K7	85.6%



在本次测试过程中，Sophos 和 Webroot（使用 Sophos 技术）由于云技术问题，使得检测率较低。与厂商进一步接触调查后，仍无法确定问题的根本和结果中显示的包括云的检测率。由于我们无法完全独立地进行验证（因为云不能恢复），所以，显示的 Webroot 和 Sophos 的测试结果“只作为展示”。目前，Sophos 和 Webroot 的测试结果只是一个粗略的估计。Sophos 和 Webroot 的检测率在 94.2％[4]左右 。

所使用的测试集包含大约 20 万个到上个月为止出现或流行的恶意软件样本，主要包括：



[3] 我们估计误差在 0.2%左右

[4] 虽然受影响的厂商也是非常优秀的，但我们不得不采取这样的方式来处理云安全有关的问题，也是为了在未来的测试中，避免其他厂商误用或做手脚。

误报测试

为了较好的评估杀软产品的检测能力（从恶意文件中区分正常文件），我们还提供误报测试。有时，误报引起的麻烦不亚于真正感染了病毒。当您比照检测率指标时，也请考虑误报率的问题，容易造成误报的产品也更容易取得较高的分数。所有发现的误报都已被分别报告给各自的杀软厂商，或许到现在为止已经被解决。

误报测试结果

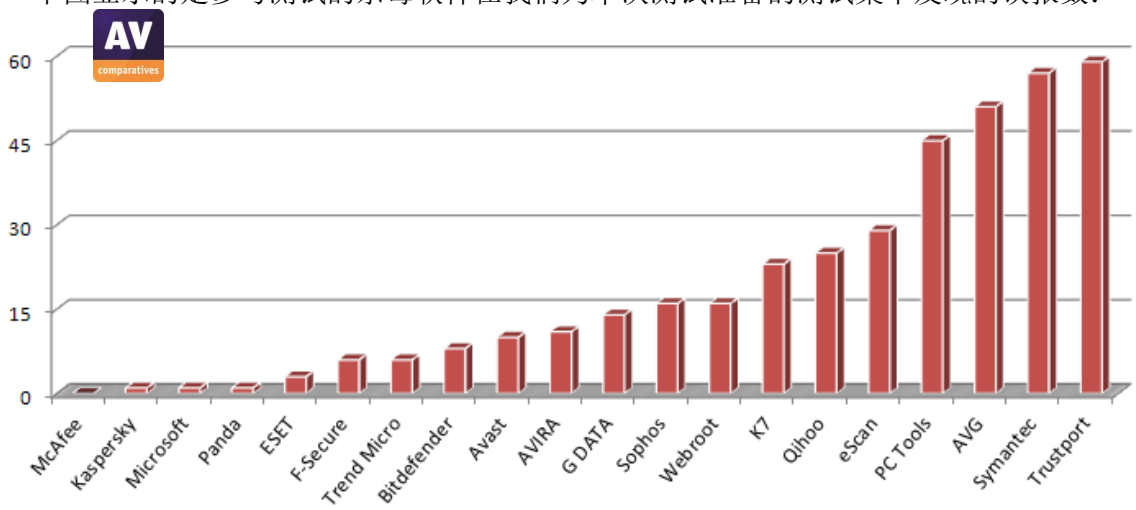
在我们准备的测试集中发现的误报数量（越少越好）：

1.	McAfee	0	
2.	Kaspersky, Microsoft, Panda	1	很少误报
3.	ESET	3	
4.	F-Secure, Trend Micro	6	
5.	Bitdefender	8	
6.	Avast	10	多误报
7.	AVIRA	11	
8.	G DATA	14	
9.	Sophos, Webroot	16*	
10.	K7	23	
11.	Qihoo	25	
12.	eScan	29	
13.	PC Tools	45	很多误报
14.	AVG	51	
15.	Symantec	57	
16.	TrustPort	59	

*由于 Sophos / Webroot 云技术的问题，我们无法确定，如果与云安全中心的连接正常发挥作用，是不是就不会有更多的误报。他们的测试结果只做列示。

有关已发现误报（包括假设的流行数据）的细节，可以参见为此准备的一份独立报告：
http://www.av-comparatives.org/images/stories/test/fp/avc_fp_aug2011.pdf

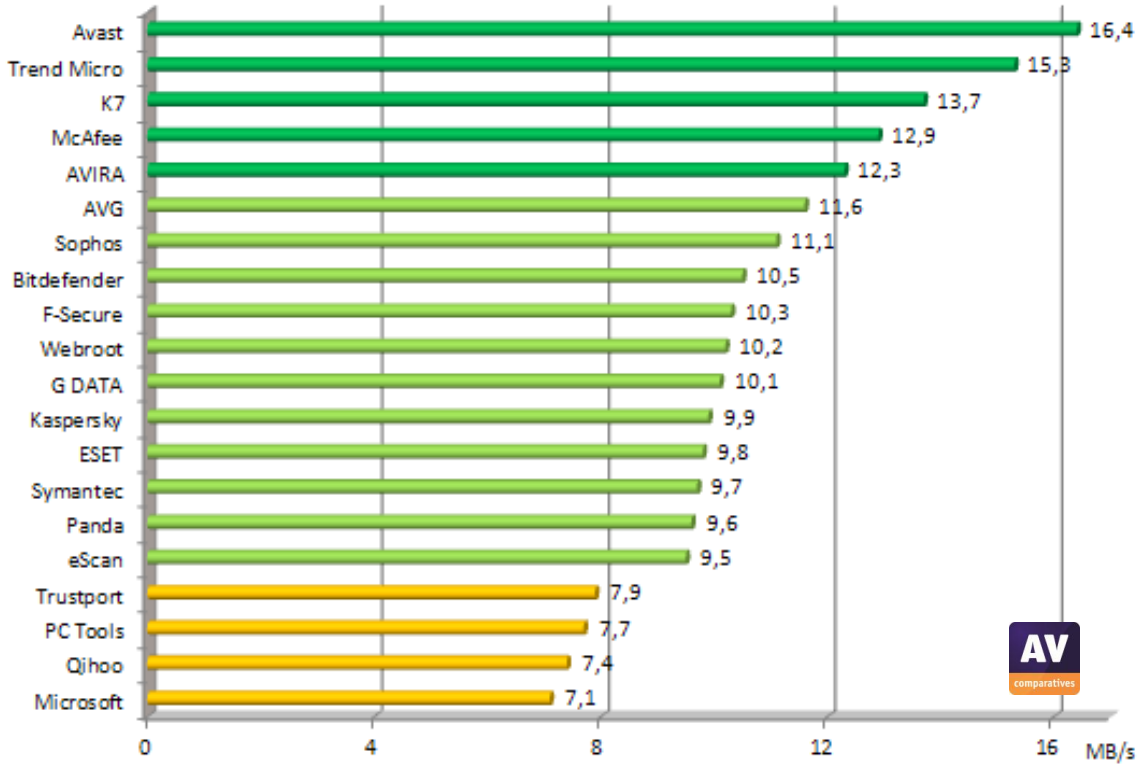
下图显示的是参与测试的杀毒软件在我们为本次测试准备的测试集中发现的误报数：



按需扫描速度测试

杀毒软件由于各种原因导致其扫描速度各不相同。这其中必须要将每款杀毒软件的检测率即可靠性的好坏考虑进去，比如：杀毒软件是否使用仿真编码，是否能够检测到多态变种病毒，是否能做深度启发式扫描分析和活跃 ROOTKIT 扫描，深入和彻底的还原压缩文件和解压支持程度，额外的安全扫描，是否真能扫描所有文件类型（或使用“云”白名单）等。大部分产品都能跳过先前扫描过的文件，以减少后续的扫描时间。由于我们想知道扫描速度（当真正的对文件进行病毒扫描时）和不跳过文件时的速度，所以指纹技术在此次测试中被禁用并不被列入考虑范畴。我们认为，部分产品应将什么是性能优化扫描更明确的告知用户，然后让用户自己决定是否选择时间较短的性能优化扫描（不重新扫描全部文件，有忽略受感染文件的潜在风险！）或一次全面安全扫描。

下图以 MB/sec（兆/秒）为单位，显示了多款杀毒软件在最高安全设置下，对我们整个白名单库用于误报测试的扫描速度（越快越好）。扫描速度会根据白名单库[5]、设置和硬件的不同而不同。



平均扫描速度的计算方法是用白名单库的大小（MB）除以完成扫描所需时间（sec）。由于文件库、所用硬件等有所不同，所以本次测试的扫描速度，不能与将来的测试或其他的测试相比较。扫描速度测试是在 Windows XP SP3 环境下进行，所采用硬件是相同的 Intel Core 2

[5] 要想知道各款产品在您的个人电脑的扫描速度，建议您自己试用这些产品。

Duo E8300/2.83GHz、 2GB 内存、SATA II 硬盘。 2012 年，我们将不再提供手动扫描速度测试[6]。

本次检测产品所获奖项及评级

AV-Comparatives 对于测试结果采用分级制【标准(STANDARD)， 优秀 ADVANCED）和最佳（ADVANCED+）】由于本报告不仅包括奖项评级，还包括检测率等数据，所以，高级用户可以根据个人意愿来判断，如：只考虑单项得分而不考虑误报。

获奖等级 (基于检测率和误报率的基础上)	产品
AV comparatives ADVANCED+ ★★★ ON DEMAND DETECTION TEST AUG 2011	✓ G DATA ✓ AVIRA ✓ Panda ✓ F-Secure ✓ Bitdefender ✓ Kaspersky ✓ ESET ✓ Avast ✓ McAfee ✓ Trend Micro
AV comparatives ADVANCED ★★ ON DEMAND DETECTION TEST AUG 2011	✓ Trustport* ✓ Qihoo* ✓ eScan* ✓ AVG* ✓ Symantec* ✓ Microsoft
AV comparatives STANDARD ★ ON DEMAND DETECTION TEST AUG 2011	-
AV comparatives TESTED ON DEMAND DETECTION TEST AUG 2011	✓ PC Tools* ✓ K7

*：带星号的产品因误报获得了较低的奖项

由于测试中 Sophos 和 Webroot 出现的云安全技术问题，本次测试（见第 9 页的评论）结果仅供展示。获奖产品不光是归功于它的病毒检测率，也考虑了它们对我们建立的白名单库产生的误报率。在本报告第 7 页，您可以看到测试产品的获奖情况。一款高检测率但同时也有很高误报的产品，可能还不如一款检测率稍差但误报较少的产品。

[6]各种性能测试可以通过下列链接查阅： http://www.av-comparatives.org/comparativesreviews/performance-tests

版权及免责声明

本 2011 年报告©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。我们竭尽一切可能，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. (2011 年 9 月)

Advertisement

Every second counts.
Who is attacking you? And how?

Even the best AV solution leaves you exposed to zero-day and custom malware attacks.

Get real-time analysis.
No waiting for signature updates.

validEDGE
www.validedge.com

ValidEdge Malware Analysis Appliances
Free 30-day evaluation.

DETECT

ANALYZE

HEAL