杀毒软件评测

「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 2 月

最后修订：2011 年 4 月 9 日

www.av-comparatives.org

目录

参加检测的产品

- avast! Free Antivirus 5.1
- AVG Anti-Virus Free Edition 10.0
- AVIRA AntiVir Personal 10.0
- BitDefender Antivirus Pro 2011
- eScan Anti-Virus 11.0
- ESET NOD32 Antivirus 4.2
- F-Secure Anti-Virus 2011
- G DATA AntiVirus 2011
- K7 TotalSecurity 10.0
- Kaspersky Anti-Virus 2011
- McAfee AntiVirus Plus 2011
- Microsoft Security Essentials 2.0
- Panda Antivirus Pro 2011
- PC Tools Spyware Doctor with AV 8.0
- Qihoo 360 Antivirus 1.1
- Sophos Anti-Virus 9.5
- Symantec Norton Anti-Virus 2011
- Trend Micro Titanium AntiVirus+ 2011
- Trustport Antivirus 2011
- Webroot AntiVirus with Spy Sweeper 7.0

参与条件和测试方法

参与 AV-C 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以及参与 2011 年的一系列公开测试活动。

参加检测的产品版本

病毒样本已于 2011 年 2 月 10 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 2 月 22 日。下列 20 款最新产品[1]参与了本次公开测试：

- avast! Free Antivirus 5.1.889[2]
- AVG Anti-Virus Free Edition 10.0.1204
- AVIRA AntiVir Personal 10.0.0.611
- BitDefender Anti-Virus Pro 14.0.24.337
- eScan Anti-Virus 11.0.1139.855
- ESET NOD32 Antivirus 4.2.71.2
- F-Secure Anti-Virus 10.51.106
- G DATA AntiVirus 21.1.2.2
- K7 TotalSecurity 10.0.0051
- Kaspersky Anti-Virus 11.0.2.556
- McAfee AntiVirus Plus 14.5.130
- Microsoft Security Essentials 2.0.657.0
- Panda Antivirus Pro 10.00.00
- PC Tools Spyware Doctor with Antivirus 8.0.0.624
- Qihoo 360 Antivirus 1.1.0.1310
- Sophos Anti-Virus 9.5.5
- Symantec Norton Anti-Virus 18.5.0.125
- Trend Micro Titanium AntiVirus+ 2011
- Trustport Antivirus 11.0.0.4606
- Webroot AntiVirus with Spy Sweeper 7.0.6.38

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[3]。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 和 AVIRA 决定用其各自的免费版本参与本次测试。

[2] Avast 用于本次测试所提交的是版本 5.1。Avast6.0 版本的检测率也应是相同的（这一点已得到 Avast 的确认）。

[3] 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设置（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 更乐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（虽然他们清楚，测试中会应用这样的设置，并且也将对后续的误报测试、性能测试等产生影响），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。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 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（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。

检测结果

由于当今的 Windows 病毒、宏病毒和恶意脚本病毒比起盛行的木马、后门、蠕虫等恶意程序，不过是小巫见大巫而已，所以这一部分不再单独列出。而是将它们同 Rootkits、漏洞等一并归到“其他恶意软件/病毒”组中。

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。

Company *Product* *Program version*		Qihoo **360 Antivirus** 1.1.0.1310		AVIRA **AntiVir Personal** 10.0.0.611		Avast Software **avast! Free Antivirus** 5.1.889		AVG Technologies **AVG Free Anti-Virus** 10.0.1204	
Award reached in this test		STANDARD		ADVANCED+		ADVANCED		STANDARD	
Number of false positives On-demand scanning speed		**very many** average		**few** average		**many** fast		**few** average	
Worms	23.273	23.215	99,8%	23.094	99,2%	23.068	99,1%	22.581	97,0%
Backdoors/Bots	42.988	42.513	98,9%	42.539	99,0%	42.336	98,5%	39.786	92,6%
Trojans	319.560	313.190	98,0%	312.225	97,7%	314.355	98,4%	292.207	91,4%
other malware/viruses	17.722	16.179	91,3%	15.539	87,7%	17.135	96,7%	14.300	80,7%
TOTAL	**403.543**	395.097	**97,9%**	393.397	**97,5%**	396.894	**98,4%**	368.874	**91,4%**

Company *Product* *Program version*		BitDefender **BitDefender AV Pro** 14.0.24.337		MicroWorld **eScan Anti-Virus** 11.0.1139.855		F-Secure **F-Secure Anti-Virus** 10.51.106		G DATA Security **G DATA AntiVirus** 21.1.2.2	
Award reached in this test		ADVANCED+		ADVANCED+		ADVANCED+		ADVANCED	
Number of false positives On-demand scanning speed		**few** average		**few** average		**few** average		**many** average	
Worms	23.273	23.072	99,1%	23.072	99,1%	23.089	99,2%	23.261	99,9%
Backdoors/Bots	42.988	42.132	98,0%	42.132	98,0%	42.416	98,7%	42.896	99,8%
Trojans	319.560	312.359	97,7%	311.795	97,6%	313.915	98,2%	318.845	99,8%
other malware/viruses	17.722	16.153	91,1%	16.153	91,1%	16.279	91,9%	17.602	99,3%
TOTAL	**403.543**	393.716	**97,6%**	393.152	**97,4%**	395.699	**98,1%**	402.604	**99,8%**

Company *Product* *Program version*		K7 Computing **K7 TotalSecurity** 10.0.0051		Kaspersky Labs **Kaspersky AV** 11.0.2.556		McAfee **McAfee AntiVirus +** 14.5.130		ESET **NOD32 Antivirus** 4.2.71.2	
Award reached in this test		TESTED		ADVANCED+		ADVANCED+		ADVANCED	
Number of false positives On-demand scanning speed		**few** fast		**few** average		**none** average		**many** average	
Worms	23.273	21.711	93,3%	23.105	99,3%	23.013	98,9%	23.069	99,1%
Backdoors/Bots	42.988	36.733	85,4%	42.028	97,8%	42.441	98,7%	42.006	97,7%
Trojans	319.560	272.123	85,2%	308.880	96,7%	309.287	96,8%	312.111	97,7%
other malware/viruses	17.722	9.836	55,5%	17.250	97,3%	16.032	90,5%	16.082	90,7%
TOTAL	**403.543**	340.403	**84,4%**	391.263	**97,0%**	390.773	**96,8%**	393.268	**97,5%**

Company *Product* *Program version*		Symantec **Norton Anti-Virus** 18.5.0.125		Panda Security **Panda Antivirus Pro** 10.00.00		Microsoft **Security Essentials** 2.0.657.0		Sophos **Sophos Anti-Virus** 9.5.5	
Award reached in this test		ADVANCED		ADVANCED		ADVANCED		ADVANCED	
Number of false positives On-demand scanning speed		**few** average		**many** fast		**very few** slow		**few** average	
Worms	23.273	21.755	93,5%	23.122	99,4%	23.005	98,8%	22.328	95,9%
Backdoors/Bots	42.988	41.638	96,9%	42.966	99,9%	41.211	95,9%	37.822	88,0%
Trojans	319.560	307.215	96,1%	318.934	99,8%	308.242	96,5%	304.553	95,3%
other malware/viruses	17.722	14.748	83,2%	11.024	62,2%	14.115	79,6%	15.008	84,7%
TOTAL	**403.543**	385.356	**95,5%**	396.046	**98,1%**	386.573	**95,8%**	379.711	**94,1%**

Company *Product* *Program version*		PC Tools **SpywareDoctor+AV** 8.0.0.624		Trend Micro **Trend Micro TiAV+** 2011		Trustport **Trustport Antivirus** 11.0.0.4606		Webroot **Webroot AV+SS** 7.0.6.38	
Award reached in this test		STANDARD		TESTED		ADVANCED+		TESTED	
Number of false positives On-demand scanning speed		**few** slow		**very many** average		**few** average		**many** fast	
Worms	23.273	21.599	92,8%	23.131	99,4%	23.233	99,8%	21.732	93,4%
Backdoors/Bots	42.988	40.545	94,3%	41.762	97,1%	42.675	99,3%	35.928	83,6%
Trojans	319.560	297.403	93,1%	300.564	94,1%	317.376	99,3%	272.565	85,3%
other malware/viruses	17.722	14.749	83,2%	15.601	88,0%	17.071	96,3%	14.802	83,5%
TOTAL	**403.543**	374.296	**92,8%**	381.058	**94,4%**	400.355	**99,2%**	345.027	**85,5%**

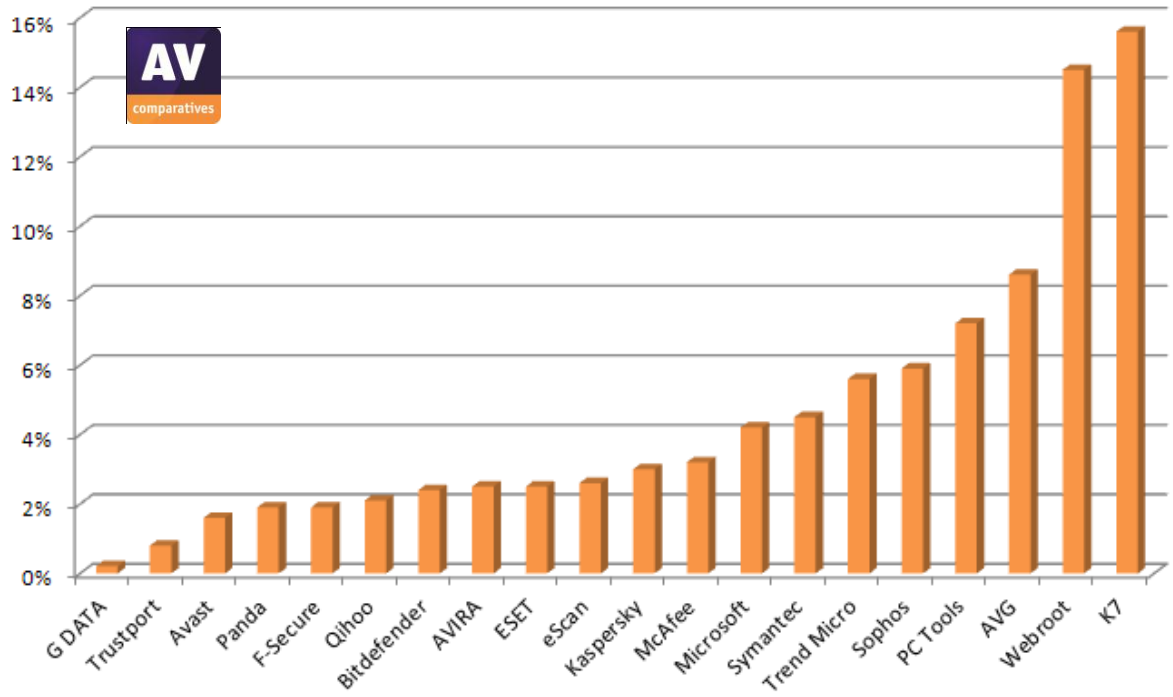
如同以前报告中公布的那样（并且已在 2010 年的整体产品动态测试中应用），今年此项测试的获奖情况如下：总检测率（保留两位小数）由测试人员分析集群后，依据层次聚类法分组而成。与以往一样误报也被考虑进去（未来可能更严格的使用“很多”和“极多”来表述误报结果），但我们正在对改变误报率（的方法）进行评估。

通过使用集群，不再需要达到固定的阈值，因为阈值会因结果不同而有所变动。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。

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，但应记住，测试集只是一个子集，而不是一个绝对的样本集，所以在不同的测试中单一检测率的波动不应该被高估。用户可以参考这些数字，在一个特定的测试中应用恶意软件集来比较这些产品的不同检测率。

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

遗漏样本图示 (越低越好)



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。

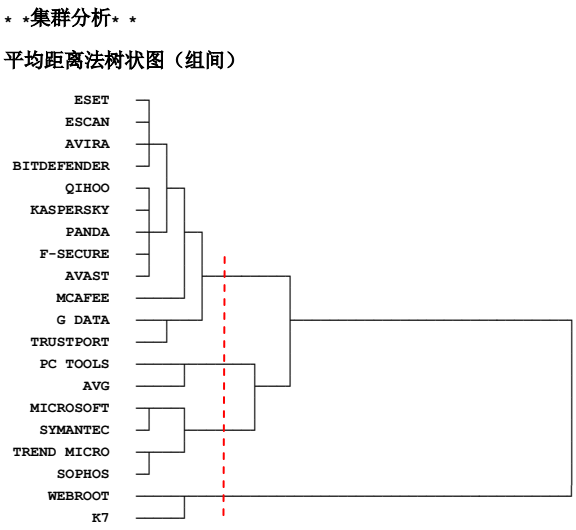
我们手动测试的结果通常也适用于实时扫描器（如果设置方式相同），但是并不适用于执行防御技术（如：基于主机的入侵防御（HIPS）、行为拦截功能等）。
良好的检测率始终是评定一款杀毒软件的具有决定性并且广泛适用的最重要的因素之一。除此之外，大多数产品还会提供一些象基于主机的入侵防御（HIPS）、行为拦截、信誉评级或其他拦截功能来阻止恶意行为（或者至少是报警功能），如：在恶意软件运行期间，如果所有的实时监测和手动检测都未能检测到它的运行，那么安全产品的这些额外病毒防护功能会发挥作用。
请不要错过包含回溯测试的报告的第二部分（它将会在几个月后发布），它对于产品对新的/未知恶意软件的检测能力进行了评估。
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。

检测结果概要

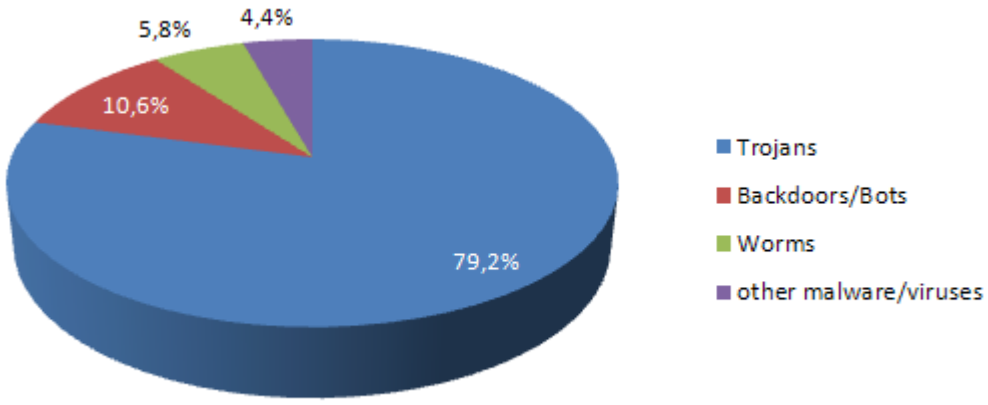
当您对比下列产品的检测率[4]时，也请考虑每款产品的误报率。

总检测率（分为四个群组）：

1.	G DATA	99.8%
2.	Trustport	99.2%
3.	Avast	98.4%
4.	Panda, F-Secure	98.1%
5.	Qihoo	97.9%
6.	Bitdefender	97.6%
7.	AVIRA, ESET	97.5%
8.	eScan	97.4%
9.	Kaspersky	97.0%
10.	McAfee	96.8%
11.	Microsoft	95.8%
12.	Symantec	95.5%
13.	Trend Micro	94.4%
14.	Sophos	94.1%
15.	PC Tools	92.8%
16.	AVG	91.4%
17.	Webroot	85.5%
18.	K7	84.4%



所使用的测试集包含大约40万个恶意软件样本（最近6个月的），主要包括：



[4] 我们估计误差在 0.2%左右。

误报测试

为了较好的评估杀软产品的检测能力，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。

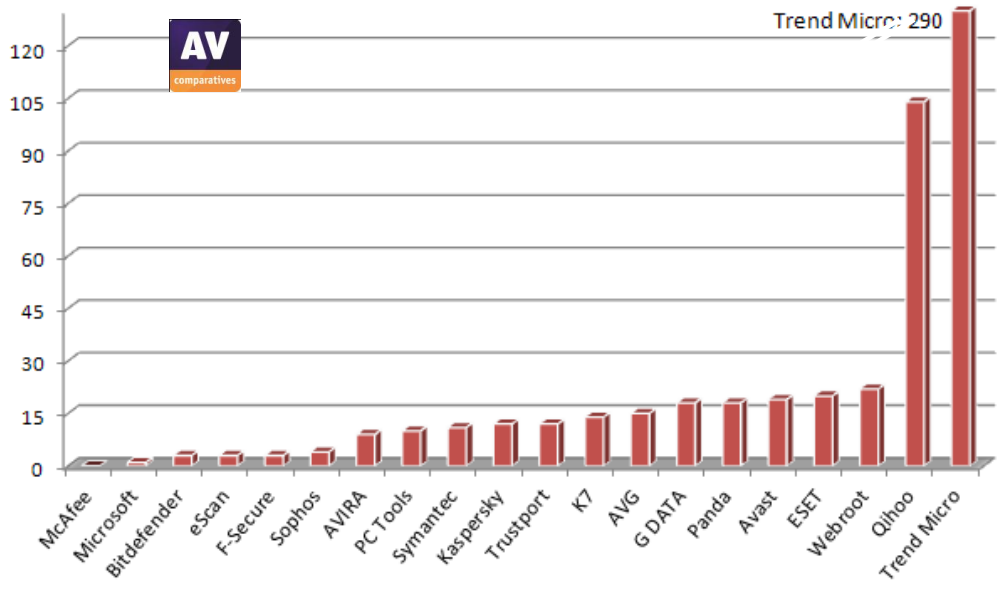
误报结果

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.	Microsoft	1	很少误报
3.	Bitdefender, eScan, F-Secure	3	
4.	Sophos	4	
5.	AVIRA	9	
6.	PC Tools	10	少误报
7.	Symantec	11	
8.	Kaspersky, Trustport	12	
9.	K7	14	
10.	AVG	15	
11.	G DATA, Panda	18	
12.	Avast	19	多误报
13.	ESET	20	
14.	Webroot	22	
15.	Qihoo	104	很多误报
16.	Trend Micro	290	

有关已发现的误报（包括他们的流行数据）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_feb2011.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

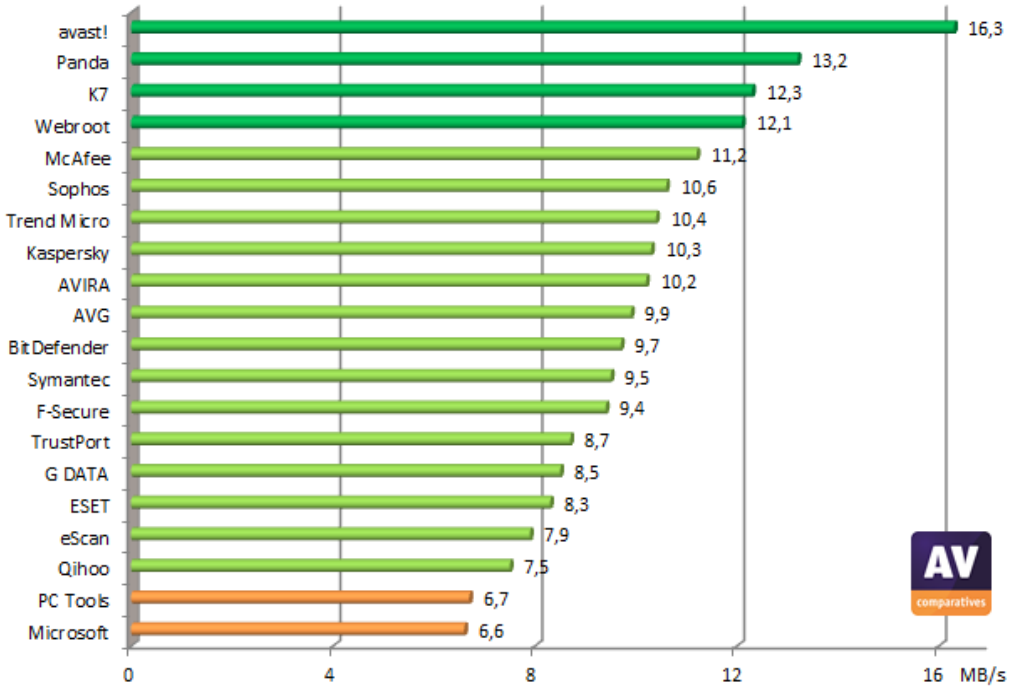


扫描速度测试

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。

大多数产品都有通过跳过先前扫描过的文件来减少扫描时间的技术。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 Duo E8300/2.83GHz、 2GB 内存、SATA II 硬盘。2012 年，我们可能在手动恶意软件检测报告中，将不再提供手动扫描速度测试。

[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。

本次检测产品所获奖项及评级

AV-C对于测试结果采用3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基础上)	产品
	✓ Trustport ✓ F-Secure ✓ Bitdefender ✓ AVIRA ✓ eScan ✓ Kaspersky ✓ McAfee
	✓ G DATA* ✓ Avast* ✓ Panda* ✓ ESET* ✓ Microsoft ✓ Symantec ✓ Sophos
	✓ Qihoo* ✓ PC Tools ✓ AVG
	✓ Webroot* ✓ Trend Micro* ✓ K7

*：带星号的产品因误报获得了较低的奖项

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。

版权及免责声明

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 4 月)