Anti-Virus Comparative

恶意软件手动扫描测试

包括误报测试

语言：简体中文

2012年3月

最后修订：2012年4月10日

www.av-comparatives.org

目录

参加检测的产品

- AhnLab V3 Internet Security 8.0
- AvastFree Antivirus 7.0
- AVG Anti-Virus 2012
- AVIRA Antivirus Premium 2012
- BitDefender Antivirus Plus 2012
- BullGuard Antivirus 12
- eScan Anti-Virus 11.0
- ESET NOD32 Antivirus 5.0
- F-Secure Anti-Virus 2012
- G DATA AntiVirus 2012
- Kaspersky Anti-Virus 2012
- McAfee AntiVirus Plus 2012
- Microsoft Security Essentials 2.1
- Panda Cloud Free Antivirus 1.5.2
- PC Tools Spyware Doctor with AV 9.0
- 360 杀毒软件 3.0
- Sophos Anti-Virus 10.0
- QQ 电脑管家 5.3
- Trend Micro Titanium AntiVirus+ 2012

参与条件和测试方法

参与AVC测试的条件，已经在我们官网的测试方法文档中公布，读者在开始阅读本报告前，应先阅读下列链接中的测试方法文档。

http://www.av-comparatives.org/seiten/ergebnisse/methodology.pdf.

本报告仅包含已有中文版产品的的厂商。尚未提供中文版产品的厂商的检测结果，请通过我们官网：www.av-comparatives.org 所载的英文/国际防病毒产品报告中查阅。

参加检测产品的版本

恶意软件测试集于2012年2月16日封存，本次测试准备的样本数由291388个恶意程序样本参数组成。所有产品于2012年3月1日进行了更新。下列19款最新产品参与了本次公开测试：

- AhnLab V3 Internet Security 8.0.5.19
- AvastFree Antivirus 7.0.1407
- AVG Anti-Virus 2012.0.1913
- AVIRA Antivirus Premium 12.0.0.915
- Bitdefender Anti-Virus+ 15.0.36.1530
- BullGuard Antivirus 12.0.215
- eScan Anti-Virus 11.0.1139.1146
- ESET NOD32 Antivirus 5.0.95.0
- F-Secure Anti-Virus 12.49.104
- G DATA AntiVirus 22.1.0.2
- Kaspersky Anti-Virus 12.0.0.374
- McAfee AntiVirus Plus 11.0.654
- Microsoft Security Essentials 2.1.1116.0
- Panda Cloud Free Antivirus 1.5.2
- PC Tools Spyware Doctor with Antivirus 9.0.0.909
- 奇虎 360 杀毒软件 3.0.0.2121
- Sophos Anti-Virus 10.0
- 腾讯QQ电脑管家5.3.1620.711
- Trend Micro Titanium AntiVirus Plus 5.0.1280

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1。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、支持等）。尽管产品检测率的高低相当重要，但它只能用作考察整款杀毒软件的一方面。

---

[1] 关于产品中使用第三方杀毒引擎/病毒特征码的附加信息：**Bullguard、eScan 和 F-Secure** 使用的都是 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。**奇虎 360** 使用 AVIRA 和 Bitdefender 的引擎。 **腾讯** 使用 AVIRA 和 TrendMicro 的引擎。

AVC还提供整体产品“真实环境”下的动态测试，即覆盖产品其他方面特征的测试报告。请您关注我们网站上其他的测试和报告。

大部分产品运行时，使用默认的最高设置。还有某些产品，当发现恶意软件时，会自动切换到最高设置。这就无法实现使用真正“默认”的设置进行各种恶意软件的检测。为了使测试结果具有可比性，经过厂商的同意，我们将几个保留了默认设置的产品调成最高设置，或仍保留他们较低的设置。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由用户启动的扫描。通常情况下，这已经被用于访问时扫描和/或执行时扫描。我们允许保留较低设置的厂商（在手动扫描时不使用最高的设置）选择更高的设置进行测试，因为在访问时扫描/执行时扫描测试时可能使用较高的默认设置。因此，杀毒软件的检测率测试更接近于实际。我们也希望厂商能够去除用户界面中的偏执安全设定，如此高的设置对于普通用户而言弊大于利。下面是关于部分产品测试时所使用设置的一些说明（禁用扫描全部文件、压缩文件等）：

AVG、AVIRA:
要求不将压缩工具警报提示作为检测结果。因此，我们并未将其作为检测结果计入测试（既不包括在恶意样本库中，也不在白名单库）

Avast、AVIRA、Kaspersky:要求在测试中将启发式杀毒设定为高/增强。

F-Secure、Sophos、腾讯（QQ）：
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）
腾讯要求使用默认设置进行测试（未启用 Trend Micro 引擎）。

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。我们的测试是在有效的联网状态下完成的。我们不再提供没有云安全技术的检测率基准，只提供具有有效的云安全技术情况下的检测结果。用户应该清楚的是，处于离线状态下（或由于某些原因无法连接到云）进行的病毒检测，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（即对恶意程序的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[2]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可能已启动的扫描无效。

[2] 下列链接为您提供一些关于云安全的支持和反对意见：
http://www.av-test.org/fileadmin/pdf/publications/vb_2009_avtest_paper_why_in-the-cloud_scanning_is_not_a_solution.pdf

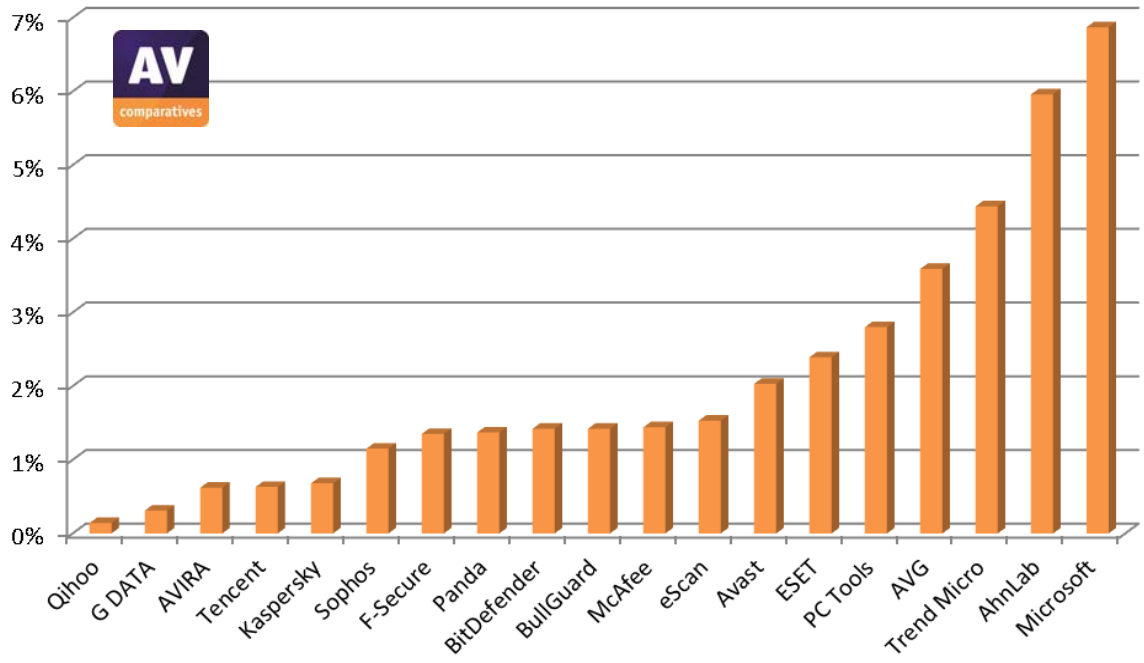
今年，报告将不再另行提供对各类恶意程序的检测情况。就像去年我们公布的，也不再提供按需扫描速度测试。我们也提请用户们关注一下我们另外的测试，而不要仅关心此类测试。这也是为了能够让用户了解我们多年以来一直提供的其他类型的测试，例如整体产品“真实环境”下的保护能力测试（WPDT）。

通过查阅遥感数据，我们创建了试图能涵盖日常生活中，对用户真正产生威胁的流行样本测试集。由于多态恶意软件的数量越来越多，我们采用聚类法，将类似的文件进行归类。这使我们能够评估流行多态恶意程序样本，并在不引起偏差的情况下减少样本集的大小。因此，每个遗漏的样本都代表一个遗漏的文件组或恶意程序参数。我们决定使用此方法，因为它有助于减少，比如样本集中同一家族恶意程序中出现不恰当的样本的影响。我们通过使用和不使用聚类文件，对结果或排序进行了比较。使用的样本越少（每种使用一个）越能减少接下来的测试工作量，因为样本集越小，越可以进行更好的分析。

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。通过使用集群，没有要达到的固定阈值，因为阈值会因各种结果而不同。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。

	检测率集群/组 （经测试者查阅统计方法后得出）			
	4	**3**	**2**	**1**
很少 （0-2 个误报） *少 （3-15 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 （500 个误报）	**已测试**	**已测试**	**已测试**	**已测试**

遗漏样本图 （越低越好）



文件已被分成集群。每个遗漏的样本代表一个漏查的变量。所有产品的检测结果都相当不错，且遗漏样本数不到测试集的10%，所以我们决定将检测率分成三组。

这个测试结果并不适用于执行防御技术（如:基于主机的入侵防御（HIPS）。对于在基于此种技术情况下的检测率情况，将在我们今年新推出的启发式/行为监测测试中进行评测。请不要错过报告的第二部分（将在几个月后发布），这部分将包含新的启发式检测或行为监测测试。它将评估各产品对全新或未知病毒的检测和拦截能力（通过手动扫描或执行扫描的拦截程序，使用本地启发式检测和常规特征码检测，而不用云安全技术，即当文件被执行时，来阻止恶意行为）。

对一款杀毒软件进行评价，最重要的、可靠而具有决定性的因素之一，就是其是否具备良好的检测能力。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。

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。

结果

当您对比下列产品的检测率时，也请考虑每款产品的误报率[3] 。

总检测率：

1.	奇虎360	99.9%
2.	G DATA	99.7%
3.	AVIRA、腾讯	99.4%
4.	卡巴斯基	99.3%
5.	Sophos	98.9%
6.	F-Secure、熊猫、比特梵德 BullGuard、迈克菲	98.6%
7.	eScan	98.5%
8.	Avast	98.0%
9.	NOD 32	97.6%
10.	PC Tools	97.2%
11.	AVG	96.4%
12.	趋势科技	95.6%
13.	安博士	94.0%
14.	微软 MSE	93.1%

所使用的测试集中包含近30万个过去几个月以来，到近期一直流行的恶意样本。

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分别报告给各自的安全厂商，到目前为止误报或许已被解决。

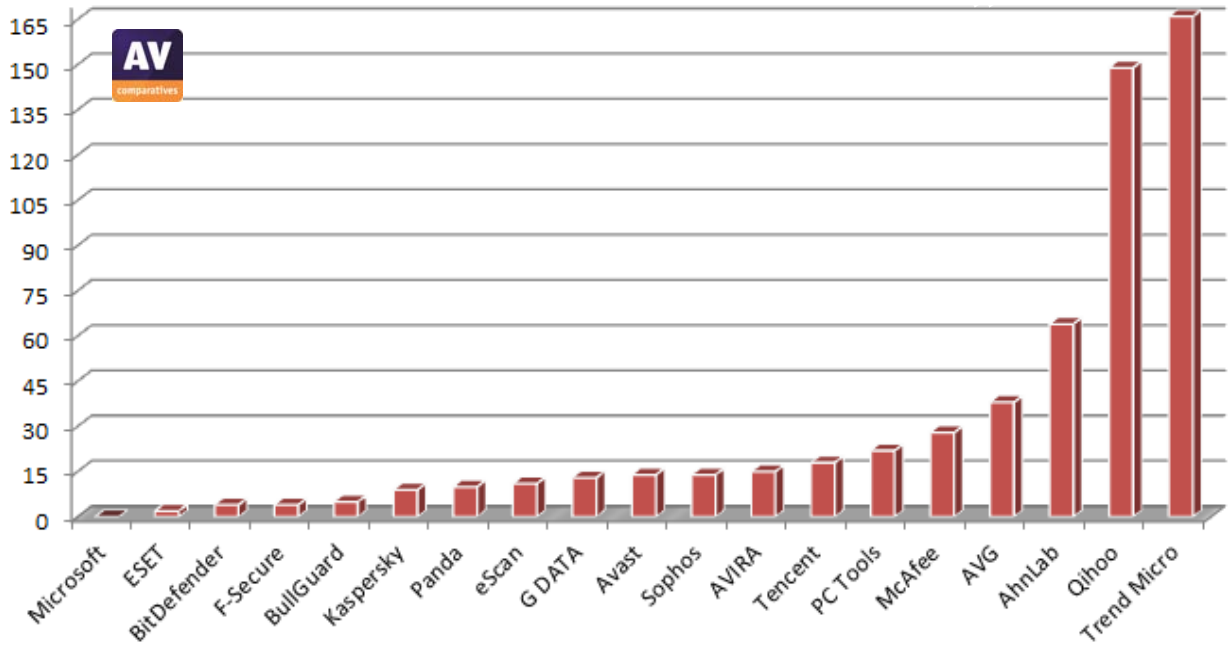
[3] 我们估计最后一组（在应用聚类法后）的误差应低于 0.2%

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.	微软 MSE	0	
2.	NOD 32	2	很少误报
3.	比特梵德、eScan、 F-Secure	4	
4.	BullGuard	5	
5.	卡巴斯基	9	
6.	熊猫	10	少误报
7.	eScan	11	
8.	G DATA	13	
9.	Avast、Sophos	14	
10.	AVIRA	15	
11.	腾讯	18	
12.	比斯图	22	
13.	迈克菲	28	
14.	AVG	38	多误报
15.	安博士	64	
16.	奇虎	149	
17.	趋势科技	166	很多误报

已发现的误报（包括假设的流行数据）的详细情况，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_mar2012.pdf



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基础上)	产品
	✓ G DATA ✓ AVIRA ✓ 卡巴斯基 ✓ Sophos ✓ F-Secure ✓ 熊猫 ✓ 比特梵德 ✓ BullGuard ✓ eScan ✓ Avast ✓ NOD 32
	✓ 腾讯 * ✓ 迈克菲
	✓ 奇虎* ✓ 比斯图* ✓ AVG* ✓ 微软 MSE ✓ 趋势科技*
	✓ 安博士 *

***：带星号的产品因误报被降级**

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10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. (2012 年 4 月)