

Anti-Virus Comparative



回溯测试

(全新/未知恶意软件静态检测)

语言：简体中文

2011 年 8 月

最后修订：2011 年 11 月 14 日

www.av-comparatives.org

目录



1. 简介	3
2. 说明	3
3. 测试结果	4
4. 误报测试	7
5. 本次检测产品所获奖项及评级	8
6. 版权及免责声明	9

1. 简介

本测试报告是 2011 年 8 月份检测率测试¹的第二部分。由于需要对本次测试进行深入的分析，以及对回溯性测试集的准备等诸多高标准的要求，故本报告于 11 月末得以完成。

由于每一天都有许多新病毒和其它各类恶意软件产生，所以杀毒产品不仅需要提供尽可能频繁并且快速的更新，更重要的是还要能够用常规/或启发式技术提前发现这些威胁（或在离线时也不执行这些威胁）。即使现在大多数杀毒产品提供每天、每小时或以云为基础的更新，但如果没有启发式/常规技术方法，那么就意味着总会有一个时间段用户是无法得到可靠的保护的。

参与测试的产品使用的升级包、病毒库以及检测设置，同 2011 年 8 月 12 日测试时相同（见本报告第 6 页）。本次测试展示了这些产品在测试时的主动检测能力。我们本次测试使用的全新恶意软件样本，出现在 2011 年 8 月 13 日到 20 日之间。下列产品参加了测试²：

- avast!Free Antivirus 6.0
- AVIRA AntiVir Personal 10.2
- BitDefender Anti-Virus Plus 2012
- eScan Anti-Virus 11.0
- ESET NOD32 Antivirus 5.0
- F-Secure Anti-Virus 2011
- G DATA AntiVirus 2012
- Kaspersky Anti-Virus 2012
- Microsoft Security Essentials 2.1
- Panda Cloud Antivirus 1.5
- Qihoo 360 Antivirus 2.0
- Trustport Antivirus 2012

2. 说明

杀毒厂商往往声称自己的产品有很高的主动检测能力-但本次测试表明，这种说法仍然是传说。当然，传说并不仅仅是为了自我宣传，它有可能是指产品达到的某些所述的功能水平，但是这也取决于测试期间及所使用的样本集的大小。这些数据还显示了，各个杀毒引擎在检测本次测试使用的新威胁（有时也被称为零日威胁）时，其主动（访问时或按需）检测能力的良好程度。即便在回溯测试中如果产品的得分比较低，用户也无需担心。如果杀毒软件总是保持最新，那么也许就可以检测出更多的样本。如果想要了解带有最新病毒库和程序的杀毒产品的检测率，请看我们定期的按需检测报告。根据对本次测试的设计和样本范围，仅对启发式/常规检测能力（在脱机的情况下）做了测试。有些杀毒产品可能针对部分样本还有其他的检测手段，如：应用程序运行控制或其他监控工具，诸如行为拦截、网页声誉/云启发式等。但 AV-

¹ http://www.av-comparatives.org/images/stories/test/ondret/avc_od_aug2011.pdf

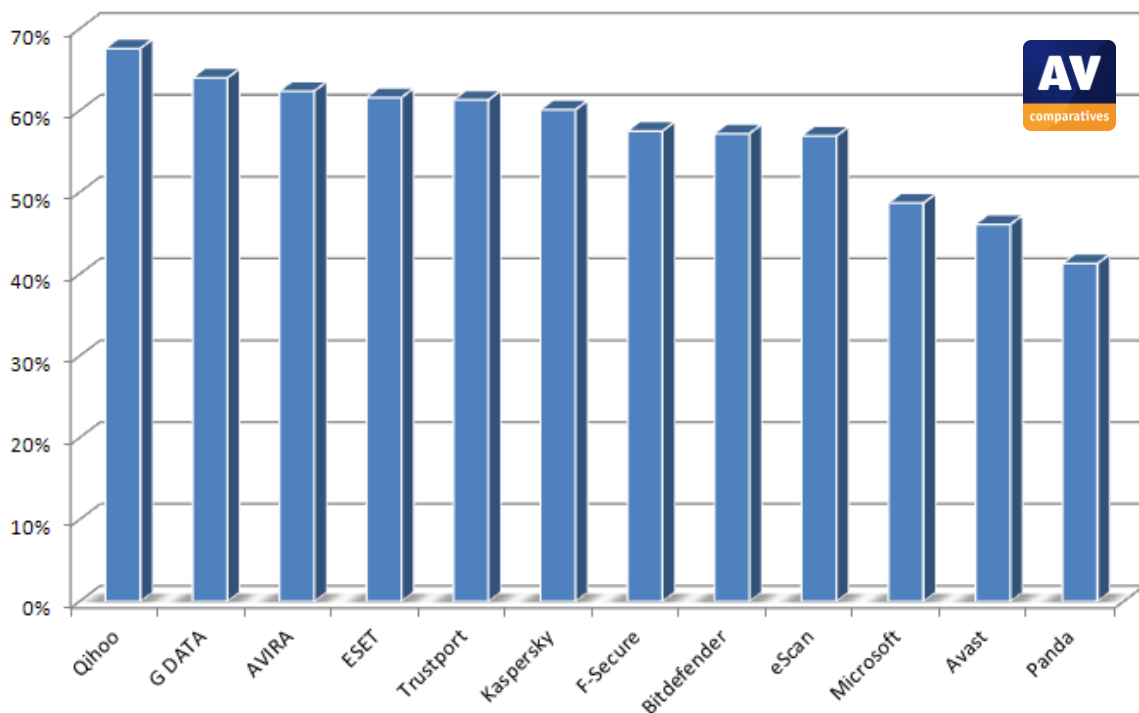
² AVG、K7、McAfee、PC Tools、Sophos、Symantec、Trend Micro和 Webroot 决定不参与本次测试，并声明放弃评测结果。

Comparatives 对这些额外的保护技术仅在例如整体产品动态测试中加以考证、评测，而不在此项测试的考评范围之内。

3. 测试结果

请注意：如果您要发布这些检测结果，那么您也有义务对产品的使用加入注释，来说明产品也使用额外的保护功能（如行为拦截器等）以帮助防御全新/未知的恶意软件。正如先前和以下几页所描述的那样，本次测试仅评估产品在离线情况下，通过启发式/常规检测技术对未知/新恶意软件的防御能力，而无需执行或在线提交。

按照检测率排序，下表显示了各种产品的主动按需检测能力。获奖结果（见本报告第 8 页）不仅仅以“新”的恶意软件检测率为基础，而且还考虑到误报率。



通过上表可以看出，被测的产品都能主动检测到大部分的全新/未知恶意程序，而且没有执行（这些恶意程序）。这些产品在采用被动的启发式的同时，还提供其他的保护机制，例如 HIPS（基于主机的入侵防御系统）、行为分析和行为拦截器、网页信誉服务和云启发式技术等，又增加了一层额外的保护。回溯测试是通过在测试过程中，通过使用被动的扫描来展示产品主动发现新的恶意软件（但不执行它）的能力。在回溯测试中，未将“云”特征考虑在内，因为这不属于本次测试要考证的范围。

某些厂商的产品也不包括在本次测试中。因为他们认为，由于在回溯测试现场缺少 Internet 连接或阻止的网页地址（URL）未被考虑等情况下，他们产品的实际检测能力不能够得到充分的展示，因此决定在此次“主动/回溯”测试中不要包括在内。我们的“主动/回溯”测试方法，确实不允许基于云技术的产品，远程连接到他们的云技术基地，我们也不考虑拦截

网页地址（URL）。因为对于此类型的测试，这都不是我们想要评测和比较的重点。其他几个测试的产品中，也有基于云的技术（有些没有），但这些产品仍然能提供良好的离线常规/启发式检测，而不必依靠或发送数据到自己的云基地，也没有发生很多误报且不依赖恶意软件的载体（即不依靠 URL 黑名单过滤）。云技术只应被看做是一种能额外提供增强保护的功能，而永远不应该用它来替代安全产品的基本保护功能。

一些厂商对于不参与回溯测试给出的进一步的理由（非正式）包括，他们知道在此类测试中，自己的得分会较低，不想让用户看到，与其他厂商相比自己的测试结果，并且离达到 100% 还有些距离。如果说，由于技术和市场营销的原因，或许这是可以理解的。但是，用户应该有权知道产品在各个方面的评分和各种测试情况；只要告知或引导用户了解产品的现状，他们自己会明白到底哪个程序最适合自己的，如果与用户的利益无关，用户会查阅由 AV - Comparatives 提供的其他类型的测试结果，如整体产品动态测试，它旨在模拟现实世界的需要，并将产品的各种保护功能也考虑在内。

如今，几乎没有任何杀毒产品单纯依赖于“简单”的特征码了。为捕获新的恶意软件，它们都使用复杂的常规特征码、启发式等，无需下载病毒库或对新威胁进行初始人工分析。此外，杀毒厂商继续提供病毒库和程序更新，以填补因主动检测机制最初无法检测某些威胁而产生的空白。杀毒软件使用各种技术来保护电脑。这种多层次的保护组合通常能提供良好的保障。

现在几乎所有的产品，在默认情况下都运行最高的保护设置（至少无论是在入口点，还是在整个电脑的按需扫描和计划扫描过程中）或当发现感染时，会自动切换到最高设置。因此，为使测试结果具有可比性，除非厂商事先明确，否则我们全部使用最高设置测试所有产品。为了避免一些常见的问题，以下是关于部分产品使用的设置提示（总是启用扫描所有文件等）：

AVIRA, Kaspersky: 要求在测试中将启发式杀毒设为高/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: 要求在测试和评级中使用默认设置（即不使用高级启发式杀毒/可疑检测设置）

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-Comparatives 更倾向于使用默认设置进行测试。由于多数产品在默认情况下，都是按照最高设置运行（或当发现恶意程序时，会自动切换到最高设置，所以，不太可能通过“默认”设置来测试产品抵御各种恶意软件的能力），为了取得可比性的检测结果，我们依据相应厂商的要求对剩下的几个产品进行了最高设置（或保留默认设置）我们希望，所有厂商能够在检测率/误报/系统影响之间找到适当的平衡，并在默认情况下，提供已经最高的安全性保护，删除用户界面的偏执设置，太高的设置对于普通用户来说弊大于利。

这一次，我们尽力让回溯测试集仅包括全新的恶意软件，这些恶意软件都已被查到过，并且在 8 月份最后一次更新产品后的几天内很盛行。此外，我们仔细的将恶意软件样本分列到属于不同的群组中（即样本彼此之间有哪些差别，以便不包括太多实际上相同的样本）。恶意软件之所以盛行，可能是因各种感染措施反应较快，当有许多用户受到感染时，说明安全产品最初的主动检测率可能下降（因为如果这些恶意软件被事先阻止或主动检测到，他们就不会泛滥）。

4. 检测结果概要

结果表明，扫描引擎的主动（常规/启发式）文件检测³能力对新的恶意软件具有抵御作用。分数以百分比计算至最接近的整数。请不要以此结果作为一种绝对的质量评估-此结果只是想让您知道，在这个特定的测试中，哪一种产品能检测到更多病毒，哪一种检测到的病毒少一些。要想知道这些杀毒产品随着更新病毒库的表现，请您阅读我们在 2 月和 8 月所做的检测率测试报告。要了解各种产品所提供的保护程度，请关注我们正在进行的整体产品动态测试。

读者应先看测试结果，然后根据需要形成自己的意见。

以下您将看到的是，参与测试的产品对于我们整理的，大约在八月中下旬的几天内出现的，全新和流行恶意软件（9003 个不同的恶意软件样本）的主动按需检测结果：

全新恶意软件的主动检测结果：

1.	Qihoo	67.6%
2.	G DATA	64.0%
3.	AVIRA	62.4%
4.	ESET	61.6%
5.	Trustport	61.3%
6.	Kaspersky	60.1%
7.	F-Secure	57.5%
8.	Bitdefender	57.2%
9.	eScan	56.9%
10.	Microsoft	48.7%
11.	Avast	46.1%
12.	Panda	41.4%

³ 本次测试在离线状态下执行的按需测试-不是执行或行为或云测试

5. 误报测试

为了更好地评价产品检测能力的质量，误报率也必须考虑进去。误报⁴就是杀毒产品将无辜的文件判断成被感染，但实际上它并没有被感染。有时，误报引起的麻烦不亚于真正感染了病毒。





误报测试结果已经包含在 8 月份的测试报告中。有关详情，请随时阅读该报告，报告位置 http://www.av-comparatives.org/images/stories/test/fp/AV-Comparatives_fp_aug2011.pdf

很少误报 (0-3):	Kaspersky, Microsoft, Panda, ESET
少误报 (4-15):	F-Secure, Bitdefender, Avast, AVIRA, G DATA
多误报 (超过 15):	Qihoo, eScan, Trustport

⁴ 所有列示的误报已经在 8 月份上报并发送给厂商核实，目前已得到处理。

6. 本次检测产品所获奖项及评级

下面是参与本次回溯测试的产品达到的获奖等级：

获奖等级	产品
	G DATA AVIRA ESET Kaspersky F-Secure Bitdefender
	Qihoo* TrustPort* eScan* Microsoft Avast Panda
	-
	-
不包含 ⁵	AVG、K7、McAfee、PC Tools、 Sophos、 Symantec、Trend Micro、 Webroot

*:有“多”次误报的产品按照以下评比标准归类⁶：

	主动检测率			
	0-10%	10-25%	25-50%	50-100%
无 - 少误报	已测试	标准	优秀	最佳
许多误报	已测试	已测试	标准	优秀
很多误报	已测试	已测试	已测试	标准
极多误报	已测试	已测试	已测试	已测试

⁵ 由于这些产品已经参与了我们的年度公开系列测试，但是因厂商决定不要参与此次测试，所以只在列表中公布产品名称（详情请见本报告的第4页和第5页）。

⁶ 考虑到某些厂商未参加测试，我们认为在此情况下，用固定阈值法代替聚类法更合理（因为由于未将低分产品包含进来，可能会产生“不公平”的群组分类）。

7. 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。

AV-Comparatives e.V. (2011 年 11 月)