

杀毒软件评测



回溯测试

(全新/未知恶意软件静态检测)

语言：中文

2011年2月

最后修订：2011年5月21日

www.av-comparatives.org

目录



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

1. 简介

本测试报告是2011年2月测试¹的第二部分。由于本次测试需要深入的分析，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5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，但如果没有任何启发式/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。

这些产品使用了同2月22日测试时相同的升级包和病毒库，以及与2月份相同的检测设置（见本报告第6页）。本次测试，展示了这些产品在测试时主动的文件检测能力。我们使用了在2011年2月23日到3月3日之间出现的新恶意软件，作为本次测试的样本。下列产品参加了测试²：

- AVIRA AntiVir Premium 10.0
- BitDefender Anti-Virus Pro 2011
- eScan Anti-Virus 11.0
- ESET NOD32 Antivirus 4.2
- F-Secure Anti-Virus 2011
- G DATA AntiVirus 2011
- Kaspersky Anti-Virus 2011
- Microsoft Security Essentials 2.0
- Panda Antivirus Pro 2011
- Qihoo 360 Antivirus 1.1
- Sophos Anti-Virus 9.5
- Trustport Antivirus 2011

2. 说明

杀毒产品往往声称自己有很高的主动检测能力 - 但通过本次测试表明，这种说法言过其实。当然，这种说法并不仅仅是一种自我宣传，它有可能是产品达到的某种规定的百分比，但是这也取决于测试期限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的威胁时，其主动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，那么它就

¹ http://www.av-comparatives.org/images/stories/test/ondret/avc_od_feb2011.pdf

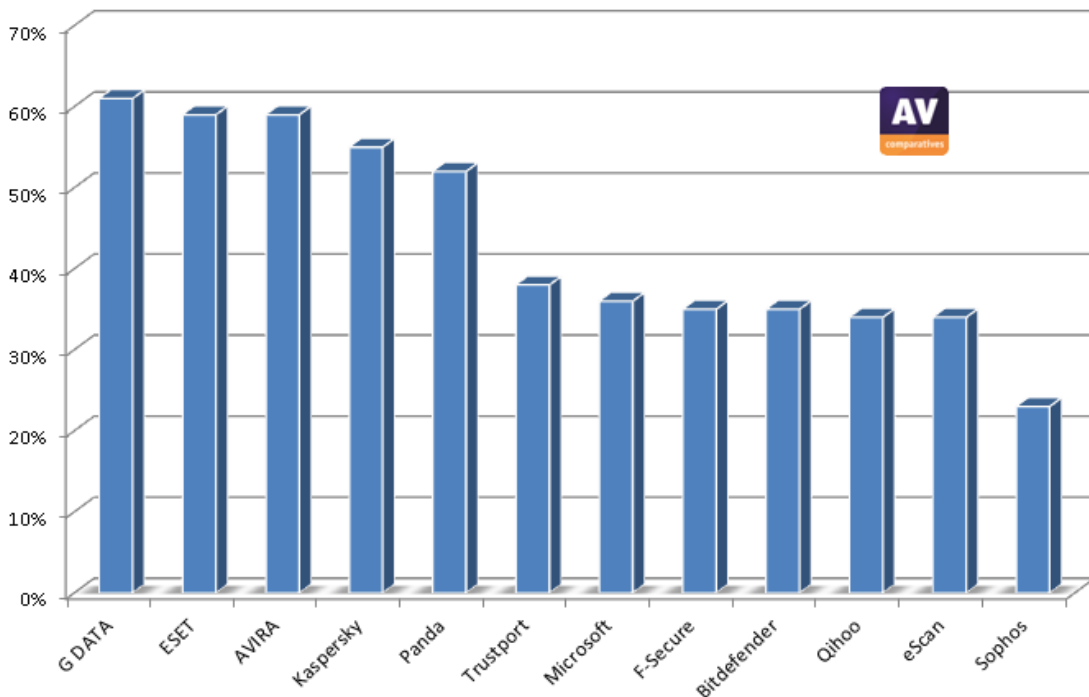
² Avast, AVG, K7, McAfee, PC Tools, Symantec, Trend Micro 和 Webroot 决定不公开测试报告，只公布获奖结果。

可以检测到更多的样本。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。此次仅对启发式/常规检测能力进行了测试（离线）。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、行为拦截、网页声誉/云启发式等。但 AV-C 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，大部分被测的产品都能主动检测到大量的全新/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，“云”功能不被列入考评，给用户提供的更新频率和升级速度、恶意软件是如何进入到系统的，也不列入考评，因为这些功能都不是本次测试的目的。

某些厂商的产品也不包括在本次测试中。因为他们认为，由于在回溯测试过程中缺少 Internet 连接或阻止的网址（URL）未被考虑，这样，自己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，我们也不考虑网址（URL）拦截。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。剩下的几个测试的产品中，也有基于云技术的（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。

一些厂商对于不参加此项测试而给出的更进一步（非正式的）的解释，大多是源于营销方面的原因，例如，在这种类型的测试中，他们的得分通常比主要竞争对手低。另一个原因可能是因为在2月的测试中，误报太多，因而担心在回溯测试中也可能获得更低的分数，或者还因为他们只是不想让用户看到测试的结果没有接近100%。一些未参与本次测试的厂商表示，明年很可能重新回到主动回溯测试中来。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，为了使检测结果具有可比性，我们在厂商没有明确要求的前提下，测试了全部使用最高设置的产品（在整个测试过程中，我们将使用相同的设置，其原因是这些最高的设置通常要么会导致过多的误报，要么对系统性能有过高的影响，或在不久的将来厂商计划更改或取消这些设置）。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, Sophos: 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: 要求不启用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。为了取得可比性的检查结果，我们依据各自厂商的要求对剩下的几个产品进行了最高设置（或保留较低设置）。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恶意软件，这些恶意软件都已被查到过，并且2月份的最后一周左右很盛行。我们认为¼的测试样本是“非常普遍”的。作为已流行的恶意软件，可能是被反映措施发现的较快，当有许多用户受到感染时，说明最初的主动检测率可能较低（因为如果他们被主动检测到，他们就不会泛滥，因为这些恶意程序会被事先阻止）。

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

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

些杀毒产品更新病毒库的执行情况，请您浏览我们在2月和8月所做的手动（按需）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。所有参与测试的产品都是精挑细选的优秀安全产品，如果正确使用其中任意一款产品并保持持续更新便能够保证客户安全。

以下您将看到的是，参与测试的产品对于我们整理的，大约在二月的最后一周内出现的，全新和流行恶意软件（9177个恶意软件样本）的主动按需检测结果：

新恶意软件的主动检测结果：

1. G DATA	61%
2. ESET, AVIRA	59%
3. Kaspersky	55%
4. Panda	52%
5. Trustport	38%
6. Microsoft	36%
7. F-Secure, Bitdefender	35%
8. Qihoo, eScan	34%
9. Sophos	23%

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2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/avc_report25_fp.pdf

很少误报 (0-3):	Microsoft [1], Bitdefender [3], eScan [3], F-Secure [3]
少误报 (4-15):	Sophos [4], AVIRA [9], Kaspersky [12], Trustport [12]
多误报 (超过15):	G DATA [18], Panda [18], ESET [20]
很多误报 (超过100):	Qihoo [104]

⁴ 所有列示的误报已经在2月份上报并发送给杀软厂商核实，目前可能已得到处理。

6. 本次检测产品所获奖项及评级

AVC对于测试结果采用3级制【标准(STANDARD), 优秀(ADVANCED)和最佳(ADVANCED+)】。

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
	AVIRA Kaspersky
	G DATA* ESET* Panda* TrustPort Microsoft F-Secure BitDefender eScan
	Sophos
	Qihoo*
不包含 ⁵	Avast, AVG, K7, McAfee, PC Tools, Symantec, Trend Micro, Webroot

*:有“多”次误报的产品按照以下评比标准归类：

	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

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。

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5月)

**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