

AVC 测试报告 第 22 号



主动/回溯测试

(新/未知恶意软件静态检测)

语言:中文

2010年8月

最后修订: 2010年12月6日

www.av-comparatives.org



目录

1. 简介.....	3
2. 说明.....	4
3. 测试结果.....	5
4. 检测结果概要.....	8
5. 误报测试.....	8
6. 本次检测产品所获奖项及评级.....	9
7. 版权及免责声明.....	10

1. 简介

本报告是 2010 年 8 月测试¹的第二部分。由于对本次测试工作的高要求、对测试结果的深入分析以及回溯测试集的准备等种种原因，使得本报告于十二月初才完成并交付。

由于每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且快速的更新，更重要的是还要能够用常规和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）。即使现在大多数防病毒产品提供每日、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 8 月 16 日测试时相同的升级包和病毒库，以及同 8 月份相同的检测设置（见本报告第 6 页）。本次测试显示了这些产品在测试时的主动检测能力。我们使用了在 2010 年 8 月 17 日和 24 日之间出现的新恶意软件作为本次测试的样本。以下 15 款安全产品参与了测试²：

- Avast! 免费³杀毒软件 5.0 (Free Antivirus)
- 小红伞杀毒软件 10.0 (AVIRA AntiVir Premium)
- 比特梵德杀毒软件 2011 (BitDefender Anti-Virus 2011)
- eScan 杀毒软件 10.0 (Anti - Virus)
- ESET NOD32 杀毒软件 4.2 (ESET NOD32 Antivirus 4.2)
- F - Secure 杀毒软件 2011 (F-Secure Anti-Virus 2011)
- 歌德塔杀毒软件 2011 (G DATA AntiVirus 2011)
- K7 全功能安全软件 10.0 (TotalSecurity 10.0)
- 卡巴斯基杀毒软件 2011 (Kaspersky Anti-Virus 2011)
- Microsoft 免费 MSE 1.0 (Microsoft Security Essentials 1.0)
- 熊猫卫士防病毒 2011 (Panda Antivirus Pro 2011)
- 比斯图反间谍和杀毒软件 8.0 (PC Tools Spyware Doctor with Antivirus 8.0)
- Sophos 杀毒软件 9.5 (Sophos Anti-Virus 9.5)
- 赛门铁克诺顿杀毒软件 2011 (Symantec Norton Anti-Virus 2011)
- Trustport 杀毒软件 2010 (Trustport Antivirus 2010)

¹ http://www.av-comparatives.org/images/stories/test/ondret/avc_od_aug2010.pdf

² AVG, Kingsoft, McAfee, Norman 和 Trend Micro 决定不要在本报告中披露并放弃奖项。

³ Avast Software 决定用其免费产品版本参与本次测试。

2. 说明

一些杀毒安全产品经常声称自己有很高的主动检测能力 - 但本次测试表明，这仍然是一种言过其实的说法。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规定百分比，但这也取决于测试期间及所使用的样本集的大小。这些数据显示，各杀毒引擎在检测新的威胁方面，其主动检测能力的良好程度。即使在一次回溯性测试中产品取得了较低的检测评分，用户也无需担心。如果杀毒安全软件总是保持最新，那么它能够检测出更多的样本。如果想了解具有最新病毒库和程序的杀毒产品的检测率，请看我们定期所出的按需检测报告。本次只对启发式/常规检测能力进行了（脱机）测试。有些产品或许还能检测出一些病毒样本例如应用程序运行控制等，或者通过其他的监控工具，如行为拦截器、网站信誉服务/云启发技术等（进行病毒检测），但 AV - Comparatives 对这些额外的保护技术只在例如整体产品动态测试中考虑，不包含在本次回溯测试的范围内。

3. 测试结果

请注意：

如果您要发布这些测试结果，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（如行为拦截等），以帮助防御全新/未知的恶意软件。正前面和以下几页介绍的同样，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。

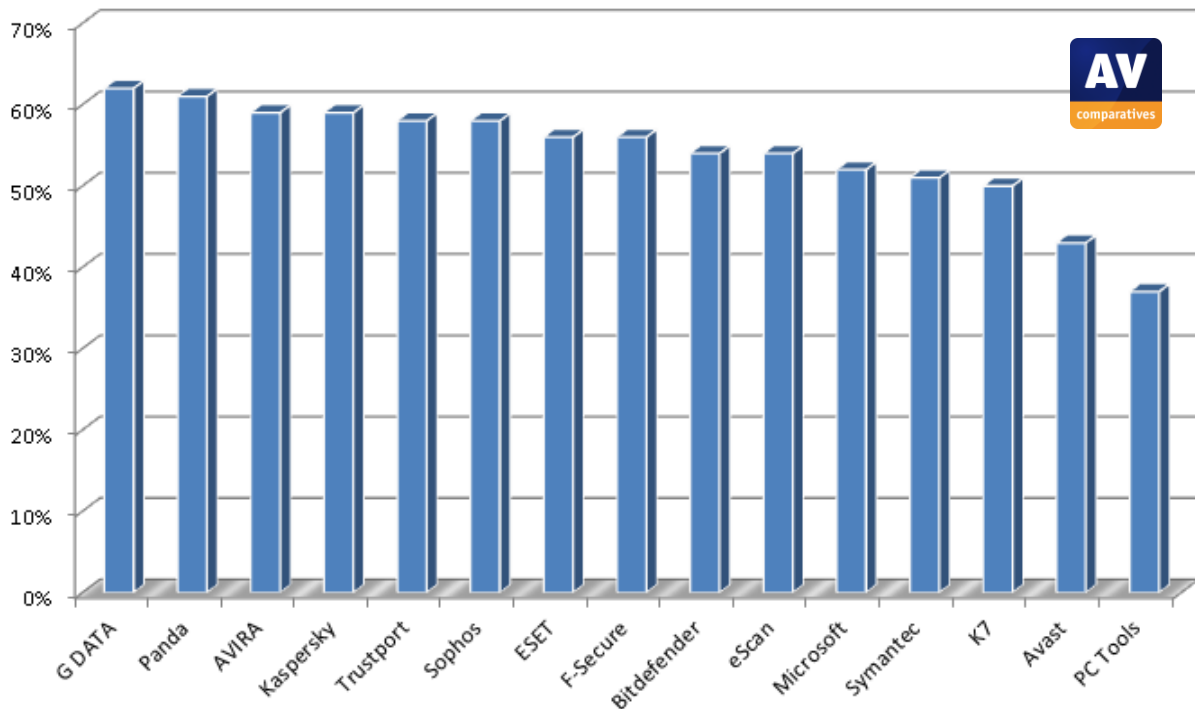
Company	AVIRA		Avast Software		BitDefender		MicroWorld		
Product	AntiVir Premium		avast! Free Antivirus		BitDefender AV		eScan Anti-Virus		
Program version	10.0.0.603		5.0.594		14.0.23.312		10.0.1058.677		
Certification level reached	ADVANCED+		ADVANCED		ADVANCED+		ADVANCED+		
Number of false positives	few		few		few		few		
ProActive detection of "NEW" samples									
Worms	1.607	856	53%	639	40%	804	50%	802	50%
Backdoors	3.114	2.282	73%	1.604	52%	1.713	55%	1.704	55%
Trojans	17.440	9.965	57%	7.242	42%	9.382	54%	9.243	53%
other malware/viruses	1.076	708	66%	606	56%	764	71%	747	69%
TOTAL	23.237	13.811	59%	10.091	43%	12.863	54%	12.496	54%

Company	F-Secure		G DATA Security		K7 Computing		Kaspersky Labs		
Product	F-Secure Anti-Virus		G DATA AntiVirus		K7 TotalSecurity		Kaspersky AV		
Program version	10.50.197		21.0.3.1		10.0.0040		11.0.1.400 (a)		
Certification level reached	ADVANCED+		ADVANCED+		ADVANCED		ADVANCED		
Number of false positives	very few		few		many		many		
ProActive detection of "NEW" samples									
Worms	1.607	802	50%	832	52%	681	42%	961	60%
Backdoors	3.114	1.760	57%	2.316	74%	1.962	63%	1.825	59%
Trojans	17.440	9.615	55%	10.382	60%	8.519	49%	10.079	58%
other malware/viruses	1.076	764	71%	822	76%	503	47%	730	68%
TOTAL	23.237	12.941	56%	14.352	62%	11.665	50%	13.595	59%

Company	ESET		Symantec		Panda Security		Microsoft		
Product	NOD32 Antivirus		Horton Anti-Virus		Panda Antivirus Pro		Security Essentials		
Program version	4.2.58.3		18.1.0.30		10.00.00		1.0.1963.0		
Certification level reached	ADVANCED+		ADVANCED+		ADVANCED		ADVANCED+		
Number of false positives	few		few		many		very few		
ProActive detection of "NEW" samples									
Worms	1.607	782	49%	759	47%	788	49%	712	44%
Backdoors	3.114	1.909	61%	1.895	61%	1.942	62%	2.099	67%
Trojans	17.440	9.586	55%	8.753	50%	10.901	63%	8.653	50%
other malware/viruses	1.076	753	70%	537	50%	515	48%	523	49%
TOTAL	23.237	13.030	56%	11.944	51%	14.146	61%	11.987	52%

Company	Sophos		PC Tools		Trustport		
Product	Sophos Anti-Virus		SpywareDoctor+AV		TrustPort AV		
Program version	9.5.1		8.0.0.594		5.0.0.4134		
Certification level reached	ADVANCED+		ADVANCED		ADVANCED		
Number of false positives	few		few		many		
ProActive detection of "NEW" samples							
Worms	1.607	844	53%	651	41%	815	51%
Backdoors	3.114	1.632	52%	1.139	37%	1.724	55%
Trojans	17.440	10.360	59%	6.165	35%	10.231	59%
other malware/viruses	1.076	630	59%	533	50%	773	72%
TOTAL	23.237	13.466	58%	8.488	37%	13.543	58%

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”恶意软件检测率为基础，而且还考虑到误报率。



以上可以看出，大部分参与测试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）。这些产品在使用被动的启发式的同时，还提供其他的保护机制，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被执行（它）的能力。在回溯测试中，“云”功能不被列入考评，以及为用户提供的更新频率或更新速度都不在测试的范围之内。

一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 连接的情况下，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技术基地，因为对于此类型的测试，这不并不是我们想要评测和比较的重点。另外几个测试的产品中有的也有基于云的技术（有些没有），但他们同时仍然提供良好的离线常规/启发式检测，而不必依靠/发送数据到了自己的云基地，并且也没有太多的误报。云技术只应被看作是（对用户）提供的一种额外的增强保护功能，而不应用它来替代安全产品的基本保护功能。

如今，几乎没有任何防病毒安全产品单纯的依靠“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，而无需下载病毒库或对新的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，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要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（卡巴斯基）、Symantec（赛门铁克）、TrustPort:要求在测试中将启发式杀毒设定为高/增强。因此，我们建议用户考虑也将启发式设定为高/增强。

F - Secure, Sophos: 要求使用默认设置进行测试和评级（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测试。由于大部分产品默认情况下运行最高设置（或当发现恶意软件时自动切换到最高设置，这样就不可能通过“默认”的设置进行防御各种恶意软件的测试），为了取得可比性的检测结果，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（或保留较低的设置）。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。

4. 检测结果概要

结果表明：杀毒引擎的主动（常规/启发式）扫描检测⁴能够防御新的恶意软件。按百分比计算的分数接近整数。请不要以此结果作为一种绝对的质量评估结果 - 此结果只是想让您知道，在这次特定的测试中，那一种产品能检测到更多病毒，那一种检测到的病毒少一些。要想知道这些杀毒产品执行更新病毒库的情况，请您阅读我们在二月和八月所做的手动（按需）测试报告。读者应先看测试结果，然后根据自身需要酌情选购。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最新便能够保证用户安全。以下您将看到的是，参与测试的杀毒产品对于我们整理的，在大约一周内出现的新恶意软件的主动按需检测结果：

新恶意软件主动检测结果：

1. **G DATA (歌德塔) 62%**
2. **Panda(熊猫) 61%**
3. **AVIRA(小红伞), Kaspersky(卡巴斯基) 59%**
4. **Trustport, Sophos 58%**
5. **ESET NOD32, F-Secure 56%**
6. **BitDefender(比特梵德), eScan 54%**
7. **Microsoft(微软) 52%**
8. **Symantec(赛门铁克) 51%**
9. **K7 50%**
10. **Avast 43%**
11. **PC Tools (比斯图)**

5. 误报测试

为了更好地评估检测能力，误报率是必须要考虑的。错误报警（或误报）⁵就是杀毒产品将无辜的文件判断成被染毒文件，但实际上它并未被感染。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八月的测试报告中。有关详情，请阅读下列报告链接 http://www.av-comparatives.org/images/stories/test/fp/avc_fp_aug2010.pdf

很少误报 (0-3) :	F-Secure, Microsoft (微软)
少误报 (4-15) :	Bitdefender (比特梵德), eScan, ESET, PC Tools (比斯图), Avast, Symantec (赛门铁克) AVIRA (小红伞), Sophos, G DATA (歌德塔)
很多误报 (超过 15) :	Trustport, Kaspersky (卡巴斯基), K7, Panda (熊猫)





⁴本次测试执行的是脱机和按需病毒扫描测试-不是执行/行为方面/云有关的测试

⁵所有发现的误报在 8 月份已经报给厂商，现在已经解决。

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【标准 (STANDARD)，优秀 (ADVANCED) 和最佳 (ADVANCED+)】。在以前的主要测试中所达到的评级总览，可以在我们的网站⁶上找到。

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 (歌德塔) AVIRA Sophos ESET F-Secure BitDefender (比特梵德) eScan 微软 Symantec (赛门铁克)
	Panda* (熊猫) Kaspersky* (卡巴斯基) TrustPort* K7* Avast PC Tools (比斯图)
	-
	-
不包含 ⁷	AVG* Kingsoft* (金山) McAfee* (迈克菲) Norman* (诺曼) Trend Micro* (趋势科技)

*: 有“多”误报的产品是按照以下评分标准归类的：

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

⁶ <http://www.av-comparatives.org/comparativesreviews/main-tests/summary-reports>

⁷ 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，所以产品名称只被加列在列表中（本报告的第五页已详细说明）。

7. 版权及免责声明

本报告的版权©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 对测试结果的准确性需要承担义务。对于报告的正确性、完整性，或者在任何特定时间，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营利性组织。

AV-Comparatives e.V. (2010年11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