



# 杀毒产品测评网站一览

——纵观各测评网站的权威性

日期: 二〇〇七年 四月

修订: 二〇〇七年 四月 二十日

作者: Andreas Clementi

网址: <http://www.av-comparatives.org>

## 目 录

1. 论独立测试的重要性 .....	2
2. 值得信赖的测试机构 .....	2
2.1 使用综合样本集的测试 .....	2
2.1.1 AV-Comparatives.org .....	3
2.1.2 AV-Test GmbH .....	3
2.2 以 WildList 样本集为主的测试 .....	3
2.2.1 VirusBulletin .....	4
2.2.2 CheckVir .....	4
2.3 认证机构 .....	4
2.3.1 ICSA Labs .....	5
2.3.2 西海岸实验室 .....	5
2.4 杂志测试 .....	6
2.5 学术测试 .....	6
2.5.1 汉堡大学反病毒测试中心 .....	6
2.5.2 坦佩雷大学病毒研究小组 <sup>[2]</sup> .....	6
2.5.3 莫斯科国力大学测试实验室 .....	7
2.5.4 马格德堡大学 .....	7
2.5.5 因斯布鲁克大学 .....	7
3. 缺乏可信度的测试或有漏洞的测试 .....	7
3.1 VXers 开展的测试 .....	7
3.1.1 Virus.gr .....	7
3.2 受商业利益和关系影响的测试 .....	8
3.2.1 TopTenReviews, 6starreviews & No1reviews .....	8
3.3 由用户/缺乏经验者开展的测试 .....	8
3.3.1 Malware-Test .....	8
3.3.2 Consumer Reports .....	8
3.3.3 基于多引擎扫描器和蜜罐样本的测试 .....	9
4. 结论 .....	9

## 1. 论独立测试的重要性

没有独立的反病毒产品测试网站,用户将很难了解哪些产品能为自己提供更好的保护,能更好的适应自己的需求。将独立测试的结果传达给公众,已被一些机构视为自己的目标,并为此花费了大量的精力、财力,同时,多年来的鉴定经验也使得他们在反病毒产品的测评领域更具权威。

## 2. 值得信赖的测试机构

完全独立的测试、认证机构并不多。目前就我个人所知,值得信赖的机构有如下几个:

- AV-Comparatives.org (AVC) ([www.av-comparatives.org](http://www.av-comparatives.org))
- AV-Test GmbH ([www.av-test.de](http://www.av-test.de))
- CheckVir ([www.checkvir.com](http://www.checkvir.com))
- ICSA 实验室 ([www.icsalabs.com](http://www.icsalabs.com))
- VirusBulletin (VB100) ([www.virusbtn.com](http://www.virusbtn.com))
- West Coast Labs (西海岸实验室) ([www.westcoastlabs.org](http://www.westcoastlabs.org))

这些机构在测试对象、测试方法、测试样本等方面各有不同,但他们的测试结果却经常趋于一致。通常你可以将以下测试结果作以比较:

基于多种样本的测试: AV-Comparatives.org ↔ AV-Test GmbH

基于 ItW 样本的测试: VirusBulletin ↔ CheckVir

认证机构: ICSA 实验室 ↔ 西海岸实验室

我们建议您不要只关注某一个测试,而是注意对比不同的测试,最后在比照中得出您的结论。

### 2.1 使用综合样本集的测试

AV-Test GmbH 与 AV-Comparatives.org 使用容量近 100 万的海量样本集。两家机构并不限制样本集的组成,并不断的加入功能完好的新样本。这些样本包括在实际生活中已经遇到或将可能遇到的各种有害程序。

“为了使测试更有效,识别率测试在测试方法上要有广泛性”,不能局限于使用 WildList (流行病毒) 样本。

另一方面,得知病毒何时才能被检测到同样十分重要,因此测试还须结合其他的手段,如前瞻性测试<sup>[1]</sup>。

## 2.1.1 AV-Comparatives.org

这里的测试由 Andreas Clementi 和他的团队完成。AV-Comparatives.org 多年从事反病毒产品的测试，自 2004 年起开始在网站上向公众公开测试结果。他们的测试有非常严格的测试规则和测试周期(每三个月)，测试对象为 16-18 款家庭版反病毒产品，这些产品运行于最常见的系统下，样本检测率均高于 85%。

该机构的网站免费提供关于测试方法与测试细节的报告。

AV-Comparatives.org 会进行非常广泛的测试，包括(但不限于)如下几种：对大量有害程序的按需扫描测试、对新型或未知的有害程序的前瞻性测试<sup>[1]</sup>或前瞻性测试、多态病毒测试、误报测试、扫描速度测试，等等。

AV-Comparatives.org 有时还会在测试结束后不久，发布其他专项测试的结果。AV-Comparatives 颁发的奖项分三级：Standard，Advanced 和 Advanced+。

官方网站：<http://www.av-comparatives.org>

## 2.1.2 AV-Test GmbH

这里的测试由 Andreas Marx 的团队负责。AV-Test GmbH 从事反病毒产品(及防火墙等相关安全产品)的测试已有多年。AV-Test GmbH 的测试有固定的测试周期，测试结果由 AV-Test 代表反病毒厂商或杂志，公布于包括网站、杂志等诸多媒体。

AV-Test GmbH 是全球最大的反病毒产品测试中心。在多个不同的平台上对产品进行全面地测试，测试包括(但不限于)病毒爆发测试、压缩/档案测试、对海量病毒样本的按需扫描与常驻防护测试、ItW 病毒测试、扫描速度测试、系统性能影响测试等。其测试方法公开，但需付费获取。测试结果在流行的电脑杂志上都可找到，但其网站目前不提供下载。

官方网站：<http://www.av-test.de>

AV-Comparatives.org 与 AV-Test GmbH 均使用被广泛接受的测试方法，均公开测试结果，并允许反病毒厂商核对测试结果，例如向他们提供产品漏检的样本等。

## 2.2 以 WildList 样本集为主的测试

The WildList (流行病毒清单) (<http://www.wildlist.org>) 包含了世界范围内广泛传播的病毒。WildList 每周发布一次，但通常会延误几个月，这就意味着反病毒厂商在病毒上榜之前有几个月的时间来发现这些病毒。

WildList 主要包含病毒和蠕虫, 而没有覆盖现在经常发现而且危害严重的木马和类似有害程序。WildCore (核心) 样本的获取只限于某些厂商, 其它厂商或机构 (包括 AV-Comparatives 在内) 是无法得到的, 这使得使用复制样本的测试难免会受到些偏见。但是, 任何优秀的反病毒产品都应该有能力通过 ITW (流行病毒) 测试。

## 2.2.1 VirusBulletin

VB100 测试由 John Hawes 组织, 隔月在不同的平台上开展。

所有参加测试的反病毒产品都会接受 VB 病毒样本的测试, 其中主要样本会出现在 Wildlist (流行病毒列表) 中。其他如多态病毒等测试用样本, 仅用于测试, 而不会影响产品是否通过测试或是否可以获得有名的 VB100 奖项。VB100 仅仅要求受测产品的按需扫描与常驻防护在不误报 VirusBulletin 无毒样本的情况下检测到全部 ItW 病毒样本。

包括速度测量在内的详细报告被公布在每月的 Virus Bulletin 的杂志上, 该杂志年定价 175 美元。杂志同时刊登其他的新闻、分析和一些反病毒领域的有趣文章。VB100 测试的初步结果可以在网站上免费获得 (需要进行简单的免费注册), 过去的测试结果连同其相关的完整评论也可以在网站上找到。

官方网站: <http://www.virusbulletin.com>

## 2.2.2 CheckVir

该测试由 Ferenc Leitold 的团队完成。CheckVir 进行针对 WildList (流行病毒列表) 样本的按需扫描和常驻扫描测试 (其中大约 80%来自于最新的三个 WildList, 最多 20%的病毒选自任意的 WildList)。

要获得标准资格受测产品需检测到测试使用的所有样本, 而要得到高级资格, 产品还必须能修复被感染的文件。

官方网站: <http://www.checkvir.com>

## 2.3 认证机构

认证可以为各种产品在既定领域的使用设定标准, 因此认证的重要性不言而喻。认证的存在对反病毒厂商来说是很重要的, 但对家庭用户来说却意义不大。某家反病毒厂商在其论坛就认证机构如何认证这样解释道:

*此处内容 (在发布前) 应某些测试机构要求已删除 (我们不便透露具体的机构), 因为据该机构称此部分信息有失准确。*

为了避免引起问题我们同意删除此部分, 所以您在本文中看不到相关内容。

对于想了解自己的杀毒软件能否抵御来自 WildList 样本的侵害的家庭用户，我认为您应该查看一下 VirusBulletin 和 CheckVir 的测试结果，因为他们的测试是一次性完成的，发布的结果包括失败产品。

下面要提到的两个认证机构：ICSA 实验室与西海岸实验室，颁发了很多专门的认证奖项（例如：间谍软件、木马清除者、防火墙等），但我们这里仅关注其中的反病毒认证。他们同时也提供各种 WildList 测试。

### 2.3.1 ICSA Labs

“ICSA 实验室的反病毒产品认证项目与其分项测试标准，对待测产品是否包含相关组件或产品来清除非自我复制型有害程序没有特殊要求，因此反病毒认证标准不要求处理有害或无害的监控软件、广告软件、后门、木马和其他的一些非自我复制程序。”

受测产品（按需扫描和常驻扫描）必须检测到来自 WildList 的全部病毒样本，和 “Zoo” Sample（实验室样本）中 90% 以上的样本。不过没人知道测试中使用的 “Zoo” 样本数量到底有多少。ICSA 实验室测试结果只列出成功通过测试的产品名单，网站没有提供未通过测试产品和通过测试所需次数的相关信息。

官方网站：<http://www.icsalabs.com>

### 2.3.2 西海岸实验室

该认证由 Chris Thomas 团队负责。西海岸实验室（West Coast Labs）与 ICSA 实验室一样，是一个独立的反病毒产品测试组织。

“一个产品要通过一级反病毒认证，就必须能检测到所有 WildList 内的病毒。” “所有已申请一级反病毒测试的产品都会接受 ‘In the Wild’ 列表内病毒的测试，测试用病毒均至少先于产品发布前两个月被记录在 WildList 中。”

“对首次送检的产品，西海岸实验室将为其免费进行一次初检，之后的所有测试将按约定好的费率收费。对于未通过测试产品的复检同样按约定费率收费。”

“通过二级认证的产品必须在符合一级认证的条件下，能够对所有已被流行病毒感染但尚可修复的文件进行修复。” “在流行的病毒中大约只有 12 种病毒感染后的档案是可修复的。”

西海岸实验室只会透露谁通过了测试，网站没有列出测试失败的产品，以及过关产品通过认证前重复送检的次数。

官方网站：<http://www.westcoastlabs.org>

## 2.4 杂志测试

我不知道将杂志测评列入可信测试是否合适, 因为在我看来, 测试的可信性在于测试结果, 这取决于测试得到的数据是由独立测试机构 (通常是 AV-Test GmbH 或 AV-Comparatives.org) 发布的还是来自杂志自家测试的。杂志通常还会评价其他的产品特性如: 产品价格、程序界面颜色、易用度、对系统的明显影响等, 最后将检测结果与以上主观考量综合后打分。这就是为什么引用同样的测试结果, 一些杂志却会选出不同的赢家。

总而言之, 这一切都是情理之中的, 因为杂志总是要标新立异来推销自己。杂志测评的一点不足在于文章到印刷发行时, 已经是距离测评近三个月之后了。

杂志测评中最坏的情况莫过于杂志在测试中使用 DIY 的测试样本。通常这样的测试样本不但数量太少没有代表性, 而且在选择和维护上也都有问题 (通常其中存在很多垃圾文件)。

## 2.5 学术测试

现在的学术测试日渐稀少, 尽管目前已经没有仍活跃在这一领域的机构, 但下面还是列出其中最为人所知的几个机构。

### 2.5.1 汉堡大学反病毒测试中心

该测试由 Klaus Brunnstein 和他的学生们完成 (Vasiline Bontchev 也曾在此工作)。该项目曾连续活跃了十年 (从 1994 年至 2004 年), 但到了 2004 年, 由于 Klaus Brunnstein 博士有其他繁忙的工作在身, 就停止了该项目。

这里的测试非常详细, 有很好的研究方法, 不过其测试目的在于向学生演示如何在测试中使用有效的测试方法, 而不在于使用实时的测试结果来比较各个反病毒方案。

测试用扫描器的病毒库并没有更新至同一天, 测试集中仍含有一些不必要的文件 (这在大型的测试集合中也是正常的), 因此试验的结果自然不应被用来衡量各个反病毒产品。不过由于其优秀的测试方法, aVTC 仍将是反病毒综合测试领域的首选参照范本。

官方网站: <http://agn-www.informatik.uni-hamburg.de/vtc>

### 2.5.2 坦佩雷大学病毒研究小组<sup>[2]</sup>

该测试由 Marko Helenius 领导。该小组目前没有进行任何反病毒产品的评估项目, 但小组表示只要条件允许, 他们愿意在未来继续开展他们的分析研究。

官方网站: <http://www.uta.fi/laitokset/virus>

### 2.5.3 莫斯科国力大学测试实验室

让产品在大量的实际生活环境中接受检验,是莫斯科国力大学测试实验室的试验目标。他们的测试结果从不在主页上公布,更不幸的是,整个项目目前似乎被终止了。

### 2.5.4 马格德堡大学[3]

此项目已于几年前由 AV-Test.de GmbH 公司接手。

官方网站: <http://www.av-test.de>

### 2.5.5 因斯布鲁克大学[4]

该项目已在数年前由 AV-Comparatives.org 项目接管。

官方网站: <http://www.av-comparatives.org>

## 3. 缺乏可信度的测试或有漏洞的测试

不幸的是,网络上流传着很多有问题的测试,有些有意制造问题,有些则是由于疏忽。下面就举几个最为人熟知的例子:

### 3.1 VXers 开展的测试

VXer 通常是指那些通过与他人交换的途径来收集病毒样本的人,大多数的 VXers 仅仅是样本收集者,他们没有病毒分析经验。

#### 3.1.1 Virus.gr

Virus.gr 由一名为 VirusP (Antony Petrakis) 的病毒收集者所维护。

VirusP 每半年发布一次测试结果。在这些测试中,样本的功能性没有得到检验,测试的产品也没有升级至同一天,厂商们更没有机会验证测试结果的正确性。样本的选择由所使用的反病毒扫描软件来完成。

此外,用于检测交换样本的防病毒软件,或是病毒库内使用唯一命名方式的防病毒软件会更具有优势,因此测试结果也会受到影响。该测试目前已销声匿迹几年了,看来 VirusP 在为他的测试改进作努力。

## 3.2 受商业利益和关系影响的测试

### 3.2.1 TopTenReviews, 6starreviews & No1reviews

某家反病毒厂商清楚地解释了此类“评测”是如何进行的。

“……就是某些人的生财之道。如果你仔细观察前五名的‘立刻购买’链接，你会发现其中都包含一个成员 ID。这就意味着作者在每一笔经由此链接进行的交易中会获得 20% 的收益……作者给 15 家反病毒厂商去函要求他们加入伙伴关系。一些厂商做出了回应，一些没有。接着他就会在网站上捏造些垃圾消息……比较市场上不同的产品，但他早就悉心于将成员厂商的杀毒产品置于榜首。所以你看到的测评，年年相同。其背后的作者只要按时更新日期，并把自己最赚钱的防病毒软件置于榜首就可以了。另外，其测试表格内的产品数据都是错误和过时的。大家不要轻信甚至没必要访问这些网站……”

## 3.3 由用户/缺乏经验者开展的测试

在很多网站、论坛上你可以看到由不同用户完成的反病毒软件测试。不幸的是，这些测试由于其使用的样本容量小、样本未经分析（其中包含垃圾文件），加之你对测试者了解甚少（有可能是某些防病毒软件公司的枪手），整个测试是不可靠的。同样的原因也适用于那些由杂志编辑们偶尔组织的零星测试。

### 3.3.1 Malware-Test

Malware-test<sup>[5]</sup> 使用的样本收集自“蜜罐”，样本的功能性并未得到检验，受检产品没有经过统一的更新和设置，样本检测数目的计算也有问题。最后，原本在正确的测试条件下应该相同的测试结果变得参差不齐（差异最高可达 12%）。总体来说，整个测试充满了错误。

### 3.3.2 Consumer Reports

2006 年，Consumer Reports<sup>[6]</sup> 发布过一份完全错误的测试报告，该报告使用了自创自改的 5500 份病毒样本，还将自己的方法标榜为测试杀毒能力的唯一正确方法来向大众兜售。AV-Test GmbH 和 AV-Comparatives.org 等机构所使用的方法（前瞻性测试）就是用来精确测试这种能力的，而这份报告却忽视了这些明确的、已被详细记录了的方法。

提起这件事的目的在于提醒大家：即使测试来自于知名的杂志，大家也不要轻信。杂志的评论员们往往没有必需的技能和设备来组织公平的测试。他们应该守住自己的老本行，更多的关注价格的比较，而将测试的工作留给更加经验丰富，

有资质的独力测试机构来完成。

### 3.3.3 基于多引擎扫描器和蜜罐样本的测试

此类测试存在如下问题：

- 来自蜜罐或上报至此类网站的样本通常是已损坏的且样本的功能性没有得到校验。
- 样本主体是间谍软件和其他工具。
- 样本容量太小，选择上没有做到真正的随机选择。
- 多引擎在线扫描器的设置有别于家用产品的设置。

## 4. 结论

最好的方式是不要听信一家之言，在一段时期内，多访问几家独立测试站点，从而确定产品的样本检测率。然后结合个人在使用试用产品时的感受，从资源消耗、界面设计、兼容性等方面综合考虑，最后做出判断。

另外，在阅读测评时，您应问问自己如下问题：

- 1.该测试的样本容量如何？样本的分组代表了什么？
- 2.谁组织的测试？他有没有足够的测试经验、相关知识和资源来进行这样的测试？
- 3.测试的样本中是否包含无用的文件，或其他成分如安全工具等？测试者是否以某些方式检验过他们的样本？
- 4.测试的结果是否可重现？测试是否可能被验证？反病毒厂商是否在测试后得到了漏检的样本以便验证？
- 5.测试使用的设置是怎样的？所有送检产品是否使用相同的设置？
- 6.该测试是何时的？是否已经过期？
- 7.所有参测产品是否在同样环境下接受测试？升级日期是否一致？
- 8.测试是如何进行的？测试的方法是否公开？能否得到广大反病毒厂商和研究人员的广泛的认同？
- 9.测试者有否从测试结果中得到过好处？
- 10.测试的目的是什么？测试的内容是什么？测试的结果说明了什么？

## 版权及免责声明

本出版物的版权归属于 AV-Comparatives。

任何公开出版物以全文，部分等任何形式使用本文中的提到的测试结果等部分，必须在出版前得到 AV-Comparatives 的书面授权。对于由文中涉及的消息所造成的损失或相关的连带损失，AV-Comparatives 与其测试者不负任何责任。

尽管我们尽最大可能保证基本数据的正确性，但 AV-Comparatives 方面的任何代表，均不对测试结果的正确性负责。对曾经发布过的任何消息或内容，我们能担保其正确性，完整性和对特定用途的适用性。

任何参与创建、制作或发布测试结果的其他人员，对由于使用或未能使用我网站提供的服务、检测文书及相关数据等而造成间接的额外损害或损失，以及由此产生的后果和风险，不承担任何责任。

Andreas Clementi, AV-Comparatives

2007 年 四月

### 附注：

[1] 前瞻性测试 (retrospective test)：一种故意使用旧病毒库，来检测防病毒软件对新病毒检测能力的测试方法。

[2] University of Tampere 位于芬兰。

[3] University of Magdeburg 位于德国。

[4] University of Innsbruck 位于奥地利。

[5] 这里指 malware-test.com，一个专门从事有害软件测试的网站。

[6] 这里指 ConsumerPeport.Org 美国最大、最权威的消费者维权网站。