安全产品“真实世界” 动态保护测试

2013 年 3 月-6 月

语言: 简体中文

2013 年 7 月

最后修订: 2013 年 7 月 25 日

www.av-comparatives.org

目录

简介

恶意软件带来的威胁正与日俱增。这不仅仅体现在恶意程序数量的增加上，它还包括这些恶意程序本身不断快速的演变。恶意程序对用户电脑的威胁方式也正在改变，不再是简单的基于文件的方式来传播恶意代码，而是演变成借助互联网来传播。总之，恶意软件不断的变换各种伎俩威胁用户的电脑，例如诱骗用户访问受感染的网页、安装流氓/恶意软件或打开带有恶意软件附件的电子邮件等等。

杀毒软件也在通过增加防御功能以扩大其为用户提供的保护范围，例如：网址拦截、内容过滤、反钓鱼措施和人性化的行为拦截。如果这些功能与安全产品提供的基于签名的检测和启发式检测完美融合，那么防病毒安全产品抵御威胁的能力将大大提高。

尽管有了这些新技术（提供防御功能），但继续对防病毒程序的基于签名和启发式检测的功能进行检测，仍然是非常重要的。也正是因为这些新的威胁，使基于签名/启发式检测的方法变得越来越重要。“零日”攻击变得日益频繁，这也意味着受恶意软件感染的危险程度在不断地增加。如果攻击不是被“传统”或“非传统”的方法截获，那么电脑就会被感染，而且恶意软件只能通过基于签名的按需扫描和启发式扫描，才可能被发现（并有希望被删除）。对于已感染的文件，由于额外的保护技术并不提供对现有存储数据的扫描，所以，在许多公司的文件服务器中仍然可以找到已被感染的文件。这些新的安全保护措施应被理解为防病毒软件良好检测率的补充，而不是代替。

在本次测试中，参与测试产品的所有功能都发挥了保护作用，而不只是一部分功能（如签名/启发式文件扫描）起作用。因此，提供的保护应该比仅使用部分功能检测病毒的能力要高。我们建议，一个产品的所有功能在检测病毒时都应有较高的查杀能力，不应只提供某种单一的功能（如网址拦截只有在浏览网页时才提供保护，但不能防御用其他方法引入的恶意软件或系统上已经存在的恶意程序）。

防病毒安全产品“真实世界”动态测试是 AV-Comparatives 和因斯布鲁克大学计算机科学与质量工程学院的一个合作项目。部分测试工作得到了奥地利政府的资助。

关于真实世界动态保护测试的方法已获得以下奖项及认证：

- 康斯坦丁奖 -由奥地利政府授予
- 2012 群集创意奖 -由蒂罗尔州地方招商局授予
- eAward 2012 -由 report.at（计算机杂志）和联邦总理办公室授予

测试程序

每天要使用上百个网址，测试数十家防病毒产品，而这些工作仅通过手动完成的话，工作量之大可以想象（因为对这成千上万的网站的访问是同时进行的），所以还是有必要通过一些自动化处理来完成。

实验室设置

每个待测试的安全程序都被安装在单独的测试电脑中。所有电脑都连接到互联网（详情如下）。在规定的日期，先更新系统，然后将已安装的安全程序和操作系统一起封存。整个测试都是在真正的工作环境中执行，我们不使用任何类型的虚拟环境。每个工作机都有自己的互联网连接和外部 IP 地址。我们与几个供应商达成了特殊的协议（故障转移群集和不阻止任何流量），以确保每台现场实时测试的电脑都有稳定的互联网连接。我们采取了必要的预防措施（使用特别配置的防火墙等），以防止对其他电脑的损害（即不引起病毒爆发）。

硬件和软件

本次测试，我们使用了相同的工作机、指令服务器和网络附加存储（NAS）。

	厂商	类型	中央处理器 CPU	内存	硬盘
工作机	Dell	Optiplex 755	Intel Core 2 Duo	4 GB	80 GB SSD
指令服务器	Supermicro	Microcloud	Intel Xeon E5	32 GB	4 x 500 GB SSD
NAS	Eurostor	ES8700-Open-E	Dual Xeon	32 GB	140 TB Raid 6

测试使用的是 2013 年 3 月 4 日更新的 Microsoft Windows 7 Professional SP1 64 位操作系统。此外安装的一些易受攻击的软件包括：

厂商	产品	版本	厂商	产品	版本
Adobe	Flash Player ActiveX	11.5	Microsoft	Office Home Premium	2010
Adobe	Flash Player Plug-In	11.5	Microsoft	.NET Framework	4.0
Adobe	Acrobat Reader	11.0	Mozilla	Firefox	18.0.1
Apple	QuickTime	7.7	Oracle	Java	1.7.0.11
Microsoft	Internet Explorer	9.0	VideoLAN	VLC Media Player	2.0.5

在测试现场，由于使用较多最新的第三方软件和更新的 Windows 7 64 位操作系统，加大了发现漏洞的难度。这至少也能提醒用户，应该让自己的操作系统和应用程序始终保持最新，以尽量减少因使用未打补丁的软件而受感染的风险。

设置

我们使用每款安全套装产品的默认设置[1]。我们的整体产品动态测试旨在模拟真实世界中，用户每天使用电脑时经历、遇到的种种情况。如果（软件程序）需要用户干预，我们总是选择“允许”或类似的操作口令。无论结果怎样，如果产品能保护系统，即便是当我们允许程序运行时，安全程序仍要求用户作出决定，那这个结果仍然算作是已拦截（保护成功）。如果系统被感染，我们将它算作依靠用户干预。我们认为，“保护”就应该是系统不会受到感染。也就是说没有恶意软件在运行（或已被删除或终止），而且没有明显的或恶意软件引起的系统变化。关于对正在运行病毒，出站防火墙询问是否阻止用户工作机和网络之间流量而发出的警报，因发出的警报太少或太晚，所以我们不将它看做是保护。

每个测试日的准备

每天早晨，更新所有的杀毒软件，制作当天新的基本镜像文件。执行每个测试实例前，各安全产品都有一定的时间，来下载和安装刚刚发布的新的更新，以及加载其各自的保护模块（在某些情况下，需要一些时间）。如果当天产品有新的重要数字签名更新，但在每个测试实例开始前又无法下载/安装的，那么至少说明该产品在当天的开始有可用的签名。这与现实世界中，一个普通用户遇到的情况是相同的。

每个恶意网址的测试周期

在浏览每一个新的恶意网址前，我们都要更新程序或病毒库（如上所述）。产品的主要新版本每月初安装一次（即内置编号的第一位数字不同），这也是我们在每月报告中，只给出产品的主要版本号的原因。我们的测试软件可以实时监控测试机，所以被恶意软件所作的任何修改都会被记录下来。此外，检测识别算法能够检查杀毒程序是否检测到恶意软件。每个测试事项结束后，机器恢复到其原来的准备状态。

保护

安全产品应该能够保护用户的电脑。但保护机制从哪个阶段开始并不重要。既可以在用户浏览网站时（例如通过网址拦截提供保护），也可以在恶意软件试图运行或当下载文件/创建文件时或当恶意软件被执行时（提供保护）（要么由用户执行要么由恶意软件执行）。恶意软件被执行后（如果之前未被阻止），我们让恶意程序运行几分钟，这也是为了给恶意行为拦截程序做出反应留出时间，并对恶意软件的破坏结果执行解救操作。如果没有检测到恶意软件，但系统确实是受到感染/损害，那么测试进程进入“系统受损”环节。但是，如果必需要求用户进行干预的，并且如果需要由用户决定某个程序是否是恶意软件，或者在最不好的情况下需要由用户确定系统受损，我们将此归为“依靠用户”。

[1]参加测试的安全产品使用的默认设置都是由厂商提供的，应与自己官网上产品使用的默认设置相同。

正因为如此，测试结果图中的黄色部分既可以理解为受到保护，也可以理解为未受到保护（这取决于每个用户在那种情况下可能作出的决定）。由于该动态测试是以模拟真实世界的条件和几种不同的技术方式（例如云扫描技术，信誉评估服务等）来进行的，因此必须面对的事实是，这种测试不能重复或复制，例如静态检测率测试。无论如何，我们记录更多合理的可能性，来证明我们的发现和结论。我们请参加检测的厂商提供各自产品中有用的日志功能，如果产生异议，通过此记录可以为他们提供更多想要的证据和数据。每次测试后，厂商都有时间对我们结论中反映的受到威胁的情况提出异议，以便我们重新检查自动化测试系统或我们的分析结果中可能存在的问题。

如果是云产品，我们将只考虑该产品在测试时的结果;有时安全厂商提供的云服务，由于故障或厂商的维护而停机，但对此厂商往往不披露或通知给用户。这也是如果产品过多依赖云服务（而不使用本地启发式、行为拦截等）可能会产生风险的原因，在这种情况下，产品所提供的安全性会明显下降。安全产品中使用的云特征码/信誉服务，应该用来配合其他的保护功能（如本地实时扫描和启发式、行为拦截等），而不应完全取代这些功能，如离线云服务可能意味着用户的电脑被置于较高的风险当中。

测试集

我们测试的重点主要包括当前可见的以及，对普通用户而言会产生问题的有关恶意网站/恶意软件。通常会让直接指向可执行恶意软件的网址（URL）尽可能的占 50%的比例，然后会下载恶意软件，这样可以模拟用户被社会工程引诱到垃圾邮件或恶意网站中，或安装一下木马或其他恶意软件。剩下的是偷渡式下载漏洞-通常情况下，这些恶意程序会被所有主流安全产品检测出来，这可能也是得分看起来较高的原因所在。

我们用自己的爬网系统不断地搜索恶意网站并选取恶意网址（包括垃圾邮件的恶意链接）。我们还手动搜索恶意网址。如果一天之中，我们的内部抓网工具无法找到足够的有效恶意网址，我们的一些外部签约分析员会为 AV - Comparatives 专门提供额外的恶意网址（首先由 AV-Comparatives 独家使用）和其他资源。

在这种测试中，使用足够的测试案例是非常重要的。如果在对比测试中使用的样本数量不足，那么，在保护作用方面，不同的测试结果可能并不能代表测试的产品[2]之间的实际差异。我们认为，即使在我们的测试中（使用几千个网址作为测试案例），只要他们对合法文件或网站的错误拦截率不超过行业平均水平，那么，处于相同保护集群的产品，实际上基本是一样的。

测试中，共使用了 3,163 个恶意测试实例，其中 1191 个由于补丁级别的原因而无效-因此，这些测试实例未计入。

[2] 更多内容请点击下列链接：
http://www.av-comparatives.org/images/stories/test/statistics/somestats.pdf

评论

微软的 MSE 产品提供了基本的恶意软件防护，可以轻松地从 Windows Update 安装，可作为恶意软件保护比较的基础使用。Windows 7 包括防火墙和自动更新，当执行网上下载的文件时，会向用户发出警告。此外，大多数时髦的浏览器都包括弹窗拦截、反钓鱼/URL 过滤器，当用户从网上下载文件时，会发出警告。但是，这些仅仅是一些内置的保护功能，尽管这些功能存在，系统仍然逃脱不了被感染的可能。因为对于这种情况，大多数发生在普通用户身上，他们可能会被社会工程黑客诱骗而访问这些恶意网站或安装这些恶意软件。用户对安全产品真正期望的是，对于是否真的要执行某个文件，（安全产品能够独立判断）不需要征求用户的意见等，但又期望安全产品能在任何情况下都能保护他们的系统，不管他们做什么（例如，执行未知的文档）都无需去考虑风险之类的问题。

测试的产品

许多厂商生产一种简单的反恶意软件程序（通常称为“杀毒软件”）和一种套装产品（通常称为“互联网安全套装”），其实就是后者多包括一些与安全有关的其他功能，如厂商自己的防火墙。此外，一些厂商还生产第三种类型的产品，带有附加功能，如备份，这与安全不产生直接的关系。在这项测试中，我们通常使用的是互联网安全套装，因为任何使系统免受损害的保护功能都可以被用上。然而，如果厂商愿意，也可以选择提交自己的杀毒软件产品进行测试。

每月测试的产品主要版本如下：

厂商	产品	3 月份版本	4 月版本	5 月版本	6 月版本
AhnLab	V3 Internet Security	8.0	8.0	8.0	8.0
Avast	Free Antivirus	8.0	8.0	8.0	8.0
AVG	Internet Security	2013	2013	2013	2013
Avira	Internet Security	2013	2013	2013	2013
Bitdefender	Internet Security	2013	2013	2013	2013
BullGuard	Internet Security	2013	2013	2013	2013
Emsisoft	Anti-Malware	7.0	7.0	7.0	7.0
eScan	Internet Security	14.0	14.0	14.0	14.0
ESET	Smart Security	6.0	6.0	6.0	6.0
F-Secure	Internet Security	2013	2013	2013	2013
Fortinet	FortiClient	5.0	5.0	5.0	5.0
G DATA	Internet Security	2013	2014	2014	2014
Kaspersky	Internet Security	2013	2013	2013	2013
金山	新毒霸	2013	2013	2013	2013
McAfee	Internet Security	2013	2013	2013	2013
Microsoft	Security Essentials	4.2	4.2	4.2	4.2
Panda	Cloud Free Antivirus	2.1.1	2.1.1	2.1.1	2.1.1
奇虎	360 杀毒	4.0	4.0	4.0	4.0
Sophos	Endpoint Security	10.2	10.2	10.2	10.2
腾讯	电脑管家	7.4	7.4	7.4	7.4
ThreatTrack	Vipre Internet Security	2013	2013	2013	2013
Trend Micro	Titanium Internet Security	2013	2013	2013	2013

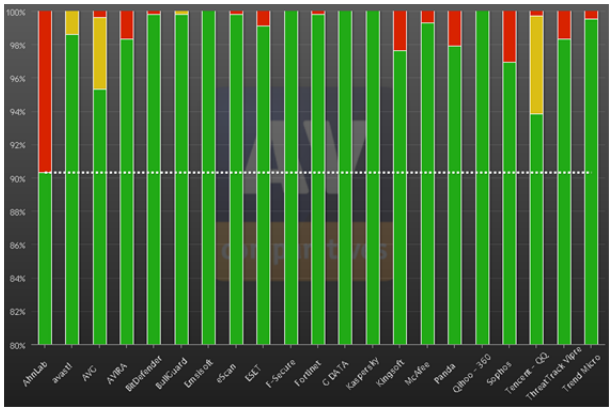
测试实例

测试时间	测试实例
2013 年 3 月 11 日至 25 日	422
2013 年 4 月 3 日至 23 日	545
2013 年 5 月 3 日至 28 日	431
2013 年 6 月 5 日至 21 日	574
合计	1972

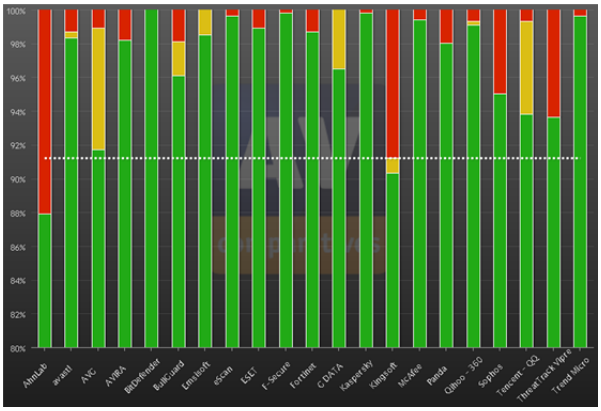
测试结果

以下是过去几个月[3]测试结果的总览。.

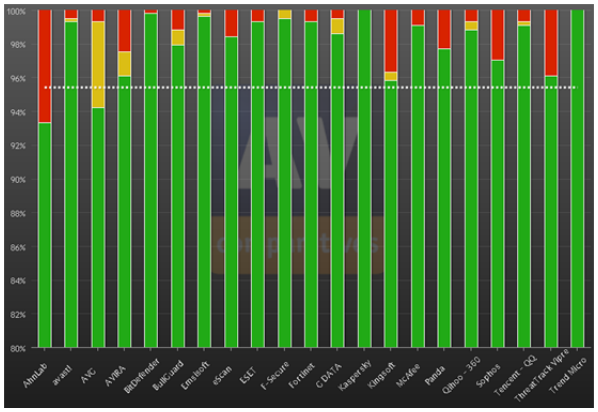
2013 年 3 月 – 422 个测试实例



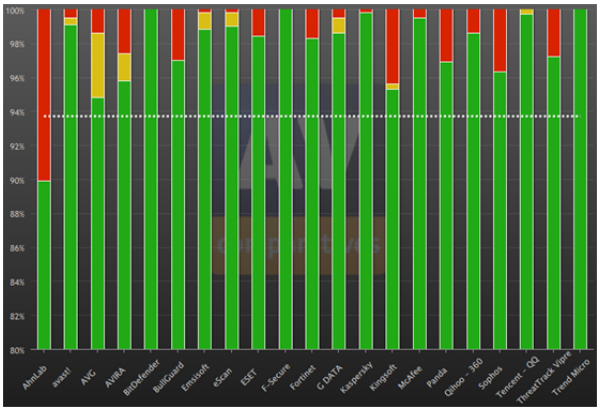
2013 年 4 月 – 545 个测试实例



2013 年 5 月 – 431 个测试实例



2013 年 6 月 – 574 个测试实例



[3] 有兴趣的用户，如果想查看各个安全产品所达到的确切的拦截率（不包括误报率），可以通过我们的官网来阅读每月更新的互动图表： http://chart.av-comparatives.org/chart1.php

我们无意在这份报告中提供每个单独月份测试使用的确切数字，以避免某些厂商滥用测试月份和测试集的大小只因 1-2 例的微小差别，来声称自己的产品好于其他产品。我们在汇总报告中标明使用的测试数量，它包含的测试案例更多，也可以让您观察到更明显的差别。

测试结果汇总（3月-6月）

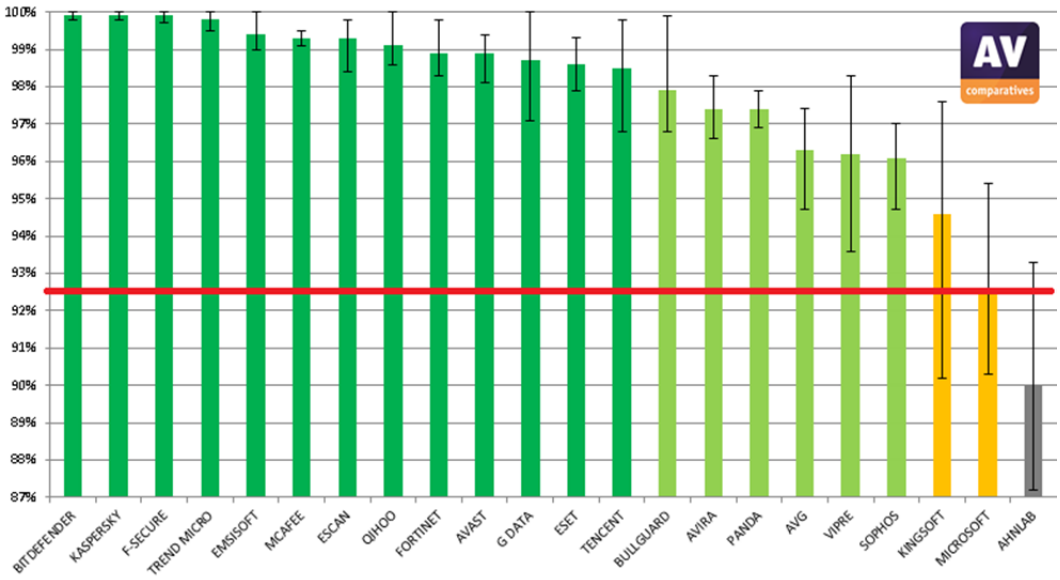
测试时间：2013年3月 – 6月 （1972 个测试实例）

	自动拦截	依靠用户	未拦截	拦截率 [自动拦截 % + (依靠用户 %)/2][4]	所属集群[5]
Bitdefender, Kaspersky	1970	-	2	99,9%	1
F-Secure	1968	3	1	99,9%	1
Trend Micro	1968	-	4	99,8%	1
Emsisoft	1954	14	4	99,4%	1
McAfee	1959	-	13	99,3%	1
eScan	1956	5	11	99,3%	1
奇虎	1953	3	16	99,1%	1
Fortinet	1951	-	21	98,9%	1
Avast	1946	12	14	98,9%	1
G DATA	1937	19	16	98,7%	1
ESET	1944	1	27	98,6%	1
腾讯	1920	43	9	98,5%	1
BullGuard	1922	16	34	97,9%	2
AVIRA	1914	15	43	97,4%	2
Panda	1920	-	52	97,4%	2
AVG	1848	102	22	96,3%	2
Vipre	1897	-	75	96,2%	2
Sophos	1896	-	76	96,1%	2
金山	1861	9	102	94,6%	3
Microsoft	1825	-	147	92,5%	3
AhnLab	1774	-	198	90,0%	4

[4] 需要用户参与的情况下，只被赋予一半的拦截率。例如，如果一个程序自动拦截 80%，另有 20%是在用户参与的情况下完成，那么，它的拦截率是 20%的一半，即 10%，因此它总的拦截率是 90%。

[5] 系统聚类法：使用群体之间（欧氏距离）的平均拦截率连接定义四个群组（参见第 12 页的树状图）。

下面的图表显示以上安全产品的总拦截率（对所有样本），包括个别月份的最低和最高拦截率。



安全产品“误报”测试（错误拦截的域/文件）

安全产品“真实世界”动态测试的误报测试由两部分组成：（浏览时）被错误拦截的域和（下载/安装时）被错误地阻止的文件。两种情况都进行测试是非常有必要的，因为如果仅测试上述两种情况之一，可能会使主要功能只侧重于一种防御方法，如侧重于 URL 或信誉服务过滤，或侧重于如访问时/基于行为的保护的产品处于不利的地位。

A） (浏览时)被错误拦截的域

我们使用了大约 1000 个随机选择的热门域名。如果拦截了非恶意的域名或网址，则被看成是误报。被错误拦截的域已上报给各厂商审查，目前应该已得到解决。

如果拦截整个域，安全产品所造成的风险，可不仅仅是只会产生让人不信任的警告那么简单，最终会给域的所有者造成潜在的经济损失（除了损害网站声誉外），还可能导致如广告收入的损失。因此，我们强烈建议厂商，只有在域的唯一目的是执行或提供恶意代码的情况下，阻止整个域，否则仅阻止恶意网页（只要确实是恶意的）。侧重于拦截基于网页信誉的网址的安全产品，可能在这方面的测试中会得到较高的分，因为他们可能会拦截许多不受欢迎的或新的站点。

B）（下载/安装时）被错误地阻止的文件

我们使用了 100 多个不同的应用程序，这些应用程序被 16 个不同的流行下载网站列为热门下载或被推荐下载。从原始开发者网站下载应用程序后（而不是从门户网站下载），保存到磁盘中并安装，从而观察应用程序在此安装过程中是否在任何阶段被拦截。此外，我们还将几个在过去月份的动态测试中，作为恶意软件而备受争议的合法文件也包括在测试集中。

安全产品的责任是抵御恶意站点或不良的程序文件，而不能是删减或限制用户仅访问著名的受欢迎的应用程序和网站。如果用户非要选择那些提示用户可能阻止一些合法站点或文件的高安全设置，这种情况下，或许可以考虑接受。然而，作为默认设置，用户未得到警示的，我们认为这并不可取。由于测试是在某个时点上准时完成的，且关于非常流行的软件或网站的误报测试通常会被察觉，并在几个小时内修复，所以，要碰上非常流行的应用程序误报是非常令人感到意外的。因此，如果在已完成的误报测试中，例如只针对很受欢迎的应用程序，或只使用已列入白名单的下载网站的前 50 个文件的话（都是被安全厂商监控的），那么，可能会是一种时间和资源的浪费。即使少数的用户，当自己的电脑被某些恶意软件感染时，会感觉郁闷(因为，使用同样的安全软件，凭什么只有自己被感染，而不是大部分用户），同样，当唯独只有他们的电脑受到某些误报的影响时，也会不舒服。当然，误报最好不要对太多的用户造成影响，也不管多少用户被感染或成为病毒感染或攻击的目标，能有效地避免任何误报并抵御任何恶意程序文件，才应该是安全软件的目标所在。安全厂商内部的品质保证测试所关注的是，基于用户数据的误报的广泛程度，但是对普通用户最重要的是，要知道安全产品对于识别正常和恶意文件的精确程度。

下表显示的是，被错误拦截的域名或文件数量：

	错误拦截的正常域/文件(自动拦截 / 用户参与[6])	**错误拦截得分[7]**
AhnLab, AVG, ESET, Microsoft	- / - (-)	0
Kaspersky, Sophos	1 / - (1)	1
G DATA	1 / 1 (2)	1.5
AVIRA, 金山	3 / - (3)	3
奇虎, 腾讯	4 / - (4)	4
Avast	- / 10 (10)	5
Emsisoft	5 / - (5)	5
BullGuard, eScan, Panda, Trend Micro	6 / - (6)	6
	平均 (7)	*平均 (7)*
Vipre	17 / - (17)	17
Bitdefender	24 / - (24)	24
F-Secure	22 / 13 (35)	28.5
Fortinet, McAfee	31 / - (31)	31

由于测试的安全产品错误地拦截网站/文件，所以，我们需要确定在认证计划中必须降级的产品。我们使用了聚类分析法，同时也参考了平均分，最后经过研究并作出艰难的决定。以下产品因误报超过平均值不得不被降级：

Bitdefender, Fortinet, F-Secure, McAfee 和 Vipre。

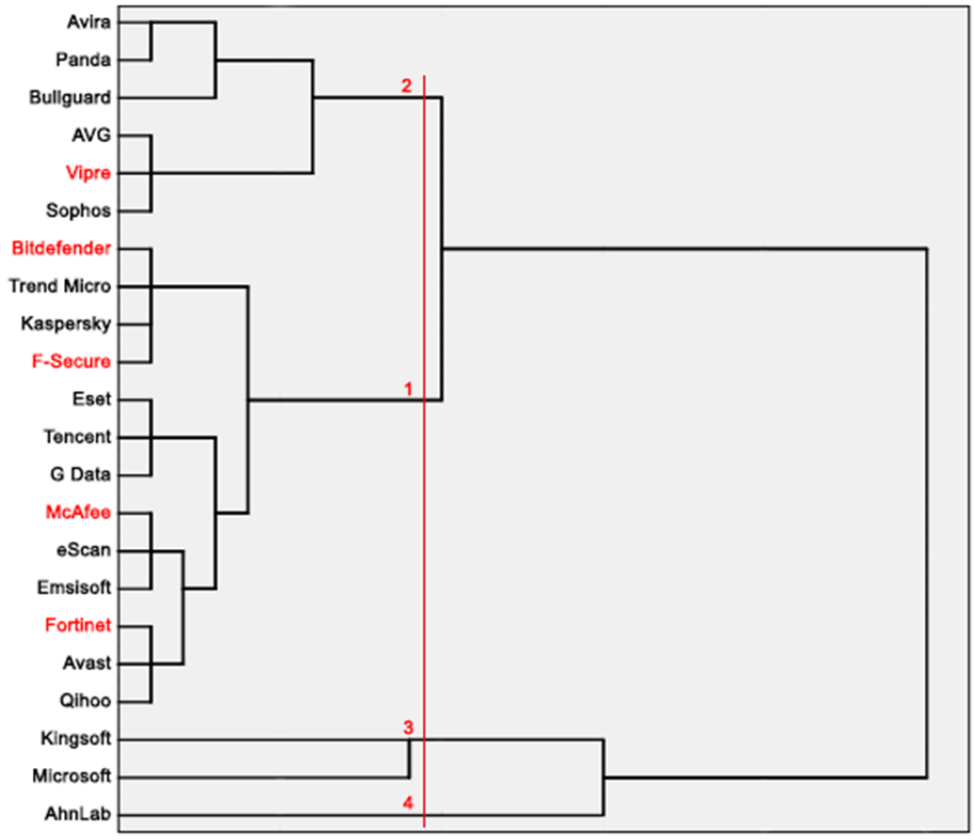
作为一种试验，我们看到，那些错误地拦截 URL 或阻止文件下载/执行的产品，仅仅是因为这些网址或文件是未知的（即完全阻止了无辜的文件）和/或没有相关的信誉信息。当我们从自己的一个网站下载一个新的自写无辜/清洁程序时，Avast 发出的警告消息是：文件未知（依靠用户）。F-Secure, McAfee 和 Trend Micro 则完全错误地阻止了文件下载或打开 URL，并将它当作恶意文件或

[6] 对于用户来说，虽然需要用户参与这种设置相当恼人（尤其是关于正常的文件），但这些安全产品的“错误拦截率”仅被计为 0.5（如同拦截率）。
[7] 越低越好

网站来处理。虽然这种保护技术是以元数据为基础，包括如信誉服务和白名单，有利于在检测率测试中取得高分。但必须清楚的是，这也可能导致无辜/干净的文件和 URL 被检测/拦截，且仅仅只是因为云和/或因为承载的文件太新而无法识别出。

成绩树状图

树状图（根据群体之间的平均联动）显示的是聚类分析的结果。它将相似的集群在同一水平连接起来。红色的虚线表示定义的水平相似。每个交叉表示一个组（在这种情况下，共分成 4 组）。误报数（错误拦截得分）超过平均值的产品以红色标记（根据排序方法被降级）。



排序方法	**拦截得分 集群[8] 4**	**拦截得分 集群 3**	**拦截得分 集群 2**	**拦截得分 集群 1**
< ∅ FPs	已测试	标准	优秀	最佳
> ∅ FPs	已测试	已测试	标准	优秀

第 9 页图中显示的是，默认设置情况下，与对 Microsoft Windows（红线）的恶意软件平均防护率对比后的测试结果。在 Windows 8 中，这种防护由 Windows Defender 提供。在默认情况下，Windows Defender 已预装在操作系统中。在 Windows 7 相当于微软的 MSE，MSE 不是预装的，但可以作为一个选项，通过 Windows Update 服务轻松地免费添加。

[8] 请参阅第 9 页的拦截得分集群。

本次测试产品取得的成绩

评测奖励是测试人员在对测试结果（经过研究统计模型后）的对比研究基础上做出的决定。以下是各安全产品在本次安全产品“真实世界”动态测试中取得的成绩[9]：

成绩	产品
	Kaspersky Trend Micro Emsisoft eScan 奇虎 Avast G DATA ESET 腾讯
	Bitdefender* F-Secure* McAfee* Fortinet* BullGuard AVIRA Panda AVG Sophos
	Vipre* 金山
	AhnLab

** 由于错误地拦截网站或文件（误报）被降一级。见第 12 页*

那些不关心错误阻止文件或网站（误报）的专家级用户，可以自由的参考第 9 页的拦截率，而不需考虑我们因评测排名而考虑的误报。

[9] 成绩中不包括微软安全产品，由于其默认的保护程序（可选）已包含在操作系统中，因此不计成绩。

版权及免责声明

AV-Comparatives 是在奥地利注册的非盈利性组织。更多关于 AV-Comparatives 及测试方法，请访问我们的网站。

AV-Comparatives e.V. (2013 年 7 月)