

软件安全—恶意代码机理与防护

C10 恶意代码的检测技术

武汉大学国家网络安全学院 彭国军

guojpeng@whu.edu.cn

本讲提纲

- 10.1 恶意代码检测对象与策略
 - 10.2 特征值检测技术
 - 10.3 校验和检测技术
 - 10.4 启发式扫描技术
 - 10.5 虚拟机检测技术
 - 10.6 主动防御技术
 - 10.7 安全软件评测
-

10.1 恶意代码检测对象与策略

- 恶意代码的检测是将检测对象与恶意代码特征（检测标准）进行对比分析，定位病毒程序或代码，或检测恶意行为。
- 检测对象主要包括：
 - 引导扇区
 - 文件系统中可能带毒的文件
 - 内存空间
 - 主板BIOS等(网络流量、系统行为等)



检测对象1:引导扇区

□ 具有控制权的引导扇区:

- 硬盘主引导扇区、
- 硬盘操作系统引导扇区
- 可移动磁盘引导扇区

□ 检测目标:

- 引导区病毒、MBR木马等
-

检测对象2:可能带毒的文件

- 可执行程序
 - .exe;.dll;.com;.scr...
 - 数据文件
 - .doc;.xls;.ppt;.pdf; .mp3;.avi...
 - 脚本文件
 - .js;.vbs;.php;.pl...
 - 网页文件
 - .html;.htm;.asp...
 - ...
-

检测对象3:内存空间

- 恶意代码在传染或执行时，必然要占有一定的内存空间，部分功能代码驻留在内存中。
 - 部分恶意代码仅存在于内存之中
 - 无文件存在，或已自行删除
 - 或被外部动态按需注入
 - 部分恶意代码仅在内存中被还原
-

病毒的检测策略

- 专用检查技术：针对某个或某些特定已知恶意代码。
 - 反病毒软件必须随着新病毒的不断出现而频繁更新病毒库版本。
 - 如文件特征值检测技术；

 - 通用检测技术：针对已知和未知恶意代码。
 - 广义特性描述或一般行为特征作为判定依据。
 - 如启发式扫描技术、主动防御技术等
-

本讲提纲

- ❑ 10.1 恶意代码检测对象与策略
 - ❑ 10.2 特征值检测技术
 - ❑ 10.3 校验和检测技术
 - ❑ 10.4 启发式扫描技术
 - ❑ 10.5 虚拟机检测技术
 - ❑ 10.6 主动防御技术
 - ❑ 10.7 安全软件评测
-

10.2 特征值检测技术

❑ 病毒特征值是反病毒软件鉴别特定计算机病毒的一种标志。通常是从病毒样本中提取的一段或多段字符串或二进制串。

❑ 具体思路：

■ 获取样本-〉提取样本特征-〉更新病毒库-〉查杀病毒



特征值的提取选择

- **特定字符串：**从计算机病毒体内提取、为病毒所特有的特征串。如特定提示信息，特定签名信息等。
 - 例如大麻病毒的提示为：“Your PC is now stoned”等。
 - **感染标记：**病毒为避免重复感染而使用的**感染标记**。
 - 如黑色星期五的“suMs DOS”。
 - 从病毒代码的特定地方开始取出**连续的、不大于64且不含空格(ASCII值为32)的字节串**。
-

提取方法

□ 人工提取

- 反病毒工程师对病毒样本进行分析后，人工确定病毒特征

□ 自动提取

- 通过软件系统自动提取特定范围内特定长度具有一定特征的数据。
 - 处理不利则可能被别有用心者利用，形成误杀。
-

优缺点

- **优点：**检测速度快、误报率低等优点，为广大反病毒厂商所采用，技术也比较成熟。
 - **缺点：**只能检测已知恶意代码。容易被免杀绕过。
-

针对特征值检测技术，恶意软件如何对抗？

□ 手工修改自身特征

- 首先，利用反病毒软件定位
- 然后，进行针对性修改

□ 自动修改自身特征

- 加密、多态、变形等
-

本讲提纲

- 10.1 恶意代码检测对象与策略
 - 10.2 特征值检测技术
 - 10.3 校验和检测技术
 - 10.4 启发式扫描技术
 - 10.5 虚拟机检测技术
 - 10.6 主动防御技术
 - 10.7 安全软件评测
-

10.3 校验和检测技术—预期符合性

- **校验和检测技术**：在文件使用/系统启动过程中，检查检测对象的实际校验和**与预期是否一致**，因而可以发现文件/引导区是否感染。
- **预期**：正常文件内容和正常引导扇区数据

静态可信：可信计算机对主引导扇区和一些系统关键程序进行了校验，从而保障系统启动之后的初始安全。

使用方式

□ 运用校验和检测技术查病毒采用三种方式：

- **系统自动监测：**将校验和检查程序常驻内存，每当应用程序开始运行时，自动核验当前与预先保存的校验和是否一致。
 - **专用检测工具：**对被查的对象文件计算其正常状态的校验和，将校验和值写入被查文件中或检测工具中，而后进行比较。如**MD5Checker**。
 - **自我检测：**在应用程序中，放入校验和检测技术自我检查功能，将文件正常状态的校验和写入文件自身，应用程序启动比较现行校验和与原校验和值，实现应用程序的自检测。如**QQ**软件。
-

校验和检测对象

- 文件头部
 - 文件属性
 - 文件内容
 - 系统数据等
-

（一）文件头部

- 一般比较整个文件效率较低，有的检测仅比较文件的头部。
 - 现有大多数寄生病毒需要改变宿主程序的头部。
-

（二）文件基本属性

- 文件的基本属性包括文件长度、文件创建日期和时间、文件属性(一般属性、只读属性、隐含属性、系统属性)、文件的首簇号等。
-

（三）文件内容-校验和

- 对文件内容（可含文件的属性）的全部字节进行某种函数运算，这种运算所产生的适当字节长度的结果就叫做校验和。
 - 这种校验和在很大程度上代表了原文件的特征，一般文件的任何变化都可以反映在校验和中。
 - 可以采用一些散列函数，如MD5...
 - CRC校验...
-

（四）系统数据

- 病毒可能修改、且相对固定的重要系统数据。
 - 如硬盘主引导扇区、分区引导扇区，内存中断向量表、SSDT、设备驱动程序处理例程等。
-

校验和检测技术优缺点

□ 优点：

- 方法简单、
- 能发现未知病毒、
- 目标文件的细微变化也能发现。

□ 缺点：

- 必须预先记录正常文件的校验和 [预期]、
 - 误报率高、
 - 不能识别病毒名称、
 - 效率低。
-

本讲提纲

- 10.1 恶意代码检测对象与策略
 - 10.2 特征值检测技术
 - 10.3 校验和检测技术
 - 10.4 启发式扫描技术
 - 10.5 虚拟机检测技术
 - 10.6 主动防御技术
 - 10.7 安全软件评测
-

10.4 启发式扫描技术

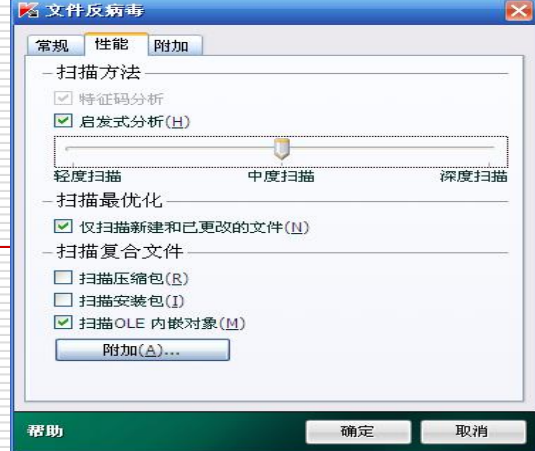
- **经验和知识**：专业反病毒技术人员使用反汇编、调试或沙箱工具稍加分析，就可能判定出某程序是否染毒，为什么？
 - 启发式代码扫描技术(Heuristic Scanning)实际上就是**恶意代码检测经验和知识的软件实现**。
-

可疑的程序代码指令序列

- ❑ 格式化磁盘类操作
 - ❑ 搜索和定位各种可执行程序的操作
 - ❑ 实现驻留内存的操作
 - ❑ 发现非常用的或未公开的系统功能调用的操作、子程序调用中只执行入栈操作、远距离(超过文件长度的三分之二)跳转指令等
 - ❑ 敏感系统行为,
 - ❑ 敏感**API**函数(序列)调用功能。。。
-

启发式扫描步骤

1. 定义通用可疑特征（指令序列或行为）



2. 对上述功能操作将被按照安全和可疑的等级进行**排序**，授以不同的**权值**。

3. 鉴别特征，如果程序的权值总和超过一个事先定义的**阈值**，则认为“发现病毒”

启发式扫描优缺点

□ 优点

- 能够发现未知病毒

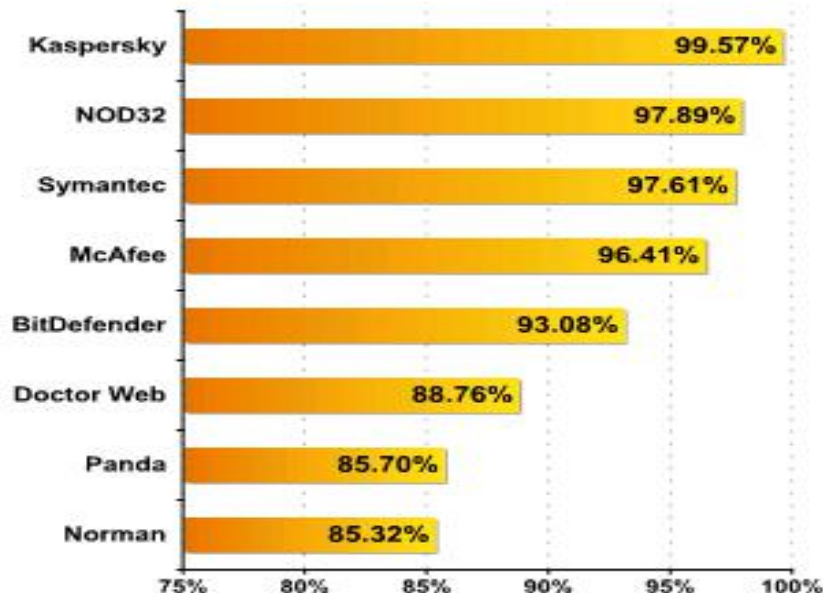
□ 缺点

- 误报率高

□ 解决方案：

- 启发式扫描技术+传统扫描技术
 - 可提高病毒检测软件的检测率，同时有效降低了总的误报率。
-

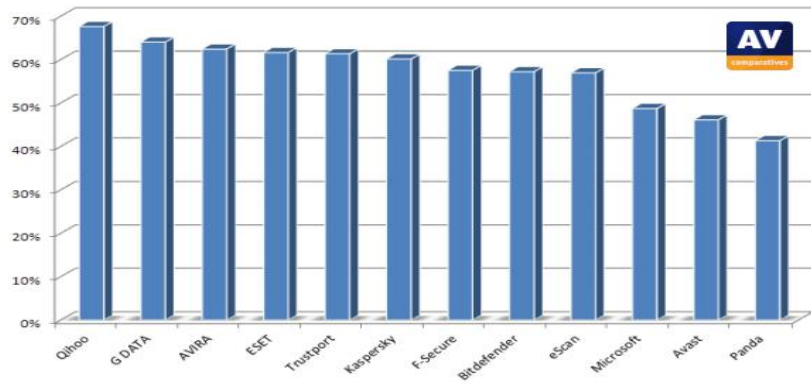
“启发式扫描+特征值扫描”的检测率



Overall detection rates
(Source: AV-comparatives.org)

2011年11月测试结果—未知病毒静态检测能力

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。



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'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

2014年AVC测试结果—启发式 / 行为检测能力

Heuristic/Behavioural Test - 2014 Mar

Vendor	Award	
		Advanced+
		Advanced+
		Advanced+
		Advanced+
		Advanced+
		Advanced+
		Advanced+
		Advanced

		Advanced
		Advanced
		Standard
		Tested

针对启发式扫描技术，病毒如何博弈？

□ 直接对抗

- Disable启发式机制
- Disable反病毒软件

□ 绕行

- 哪些是启发式检测的特征项？
 - 是否有其他替代实现方式？
-

本讲提纲

- ❑ 10.1 恶意代码检测对象与策略
 - ❑ 10.2 特征值检测技术
 - ❑ 10.3 校验和检测技术
 - ❑ 10.4 启发式扫描技术
 - ❑ 10.5 虚拟机检测技术
 - ❑ 10.6 主动防御技术
 - ❑ 10.7 安全软件评测
-

10.5 虚拟机检测技术

□ 为什么需要虚拟机检测技术？

- 加密、多态、变形病毒的出现
- 加壳技术

□ 加密病毒：

- 真实代码被压缩或加密，但最终需要在内存中还原
-

虚拟机检测技术

- 在反病毒系统中设置的一种程序机制，它能在内存中模拟一个小的封闭程序执行环境，所有待查文件都以解释方式在其中被虚拟执行。
 - 通常虚拟执行一小部分代码即可
-

□ 虚拟机检测技术具有如下优点：

- 有效处理加密类病毒
- 虚拟机技术+特征值扫描，准确率更高。
- 虚拟机技术+启发式扫描，有利于检测未知变形病毒。

本讲提纲

- 10.1 恶意代码检测对象与策略
 - 10.2 特征值检测技术
 - 10.3 校验和检测技术
 - 10.4 启发式扫描技术
 - 10.5 虚拟机检测技术
 - 10.6 主动防御技术
 - 10.7 安全软件评测
-

10.6 主动防御技术

东方微点

- 主动防御检测技术有时也被称为行为监控等技术。
- 动态监视所运行程序调用各种应用编程接口（API）的动作，自动分析程序动作之间的逻辑关系，自动判定程序行为的合法性。
- 监控应用程序的敏感行为，并向用户发出提示，供用户选择。



常见可疑行为

- ❑ 对可执行文件进行写操作
- ❑ 写磁盘引导区
- ❑ 病毒程序与宿主程序的切换
- ❑ 写注册表启动键值
- ❑ 远程线程插入
- ❑ 安装、加载驱动
- ❑ 键盘钩子
- ❑ 自我隐藏
- ❑ 下载并执行等
- ❑ ...



优缺点

- 优点：可发现未知恶意软件、可准确地发现未知恶意软件的恶意行为。
 - 缺点：可能误报警、不能识别恶意软件名称，以及在实现时有一定难度。
-

本讲提纲

- 10.1 恶意代码检测对象与策略
 - 10.2 特征值检测技术
 - 10.3 校验和检测技术
 - 10.4 启发式扫描技术
 - 10.5 虚拟机检测技术
 - 10.6 主动防御技术
 - 10.7 安全软件评测
-

10.7 安全软件评测

- 如此多的反病毒软件，哪款更适合你？
 - 各个反病毒软件采用了哪些关键技术？
 - 各自有什么特色？

Compare manufacturer results

Select an area of application, compare the results for the relevant manufacturer, and forward your view as a link.

Search/display test

ALL MOBILE HOME USER CORPORATE USER

Select a manufacturer select all deselect all

AegisLab	AhnLab	阿里钱盾	360	ANTY	ARMOR for ANDROID	avast! be free	AVG	Avira	Baidu
Bitdefender	Bornaria	BullGuard	ZONE ALARM	cheetahmobile	COMODO	Dr.WEB	duapps	EMSI SOFT	eset
F-Secure	FORTINET	GDATA	G-Protector	GFI	IKARUS	Jarviz	Juniper	K7	KASPERSKY
金山 KINGSOFT	KSmobile	LAVASOFT	lookout	Intel Security	Microsoft	eScan	NORMAN	Norton	NQmobile
NSHC	PANDA	pctools	PCKeeper	PSafe	360	Quick Heal	SecurityCoverage	SOPHOS	SPAMfighter
SUVsoft	Symantec	腾讯手机管家	腾讯安全管家	ThreatTrack	TOTAL DEFENSE	TREND MICRO	TrustGo	Trustlook	VisualThreat
WEBROOT	White Gate	Zoner AntiVirus							

10.7.1 部分典型的反病毒软件评测机构


























- VB100%
 - www.virusbtn.com
- AV-Comparative
 - www.av-comparatives.org
- AV-Test
 - www.av-test.org
- anti-malware-test
 - www.anti-malware-test.com
- WestCoastLabs
 - www.westcoastlabs.com
- ICSA实验室
 - www.icsalabs.com
- Secure Computing
 - www.securecomputing.com.cn
- PCSL
 - <http://www.pcsecuritylabs.net>

主要评测机构:

<http://www.av-comparatives.org/list-of-av-testing-labs/>

部分安全评测机构评测方法

（AV—Comparative 2014年6月对比数据）

Comparative Testing Labs	Real-World Protection Test	Number of test cases per month	File Detection Test	Number of test cases	Behavioral Test	Performance Test	Malware Removal Test	Included vendors
AV-Comparatives		~800 (~3000 per report)		~125000				~25
AV-Test		~100 (~200 per report)		~12500				~25
Dennis Technology Labs		~50 (100 per report)		N/A				~10
PC Security Labs		N/A		~20000				~25
VirusBulletin		N/A		~20000				~50

Data as of June 2014

10.7.2 AV-Comparative测试方法与结果

Real-World Protection Tests

Full product long-term dynamic test reports. We thoroughly evaluate the suites' "real-world" protection capabilities with default settings. Monthly results and two 4-month overview reports. The framework is recognized as an innovation in computer science.

» [VIEW](#)

File Detection Tests

The File Detection Test is one of the most deterministic factors to evaluate the effectiveness of an anti-virus engine. These test reports are released twice a year and include false alarm test. See how the products perform in this basic component test.

» [VIEW](#)

Performance Tests

Programs running in background such as real time protection antivirus software use some percentage of system resources. These tests help users evaluate their anti-virus protection in terms of system speed (system performance).

» [VIEW](#)

Mobile Security Reviews

Integration of new technologies into smartphones also brings risks of malware, phishing and concentrated attacks on sensitive data. This section contains tests and reviews of Mobile Security products.

» [VIEW](#)

Mac Security Reviews

These reviews evaluate the protection provided to Mac OS users. Macs are being attacked more and more by cybercriminals, who start to take advantage of the complacency towards malware threats amongst Mac users.

» [VIEW](#)

Business Reviews

These tests put special emphasis on business product features which are important to sys admins. The resulting reviews are time-saving resources for sys admins when they need to decide on an antivirus solution.

» [VIEW](#)

Heuristic / Behaviour Tests

These Heuristic/Behaviour tests evaluate the products against new and unknown malware to measure the proactive protection capabilities (heuristics, generic signatures, behaviour blocker, aso).

The Heuristic / Behaviour Tests also take into consideration the false positive rate.

» [VIEW](#)

False Alarm Tests

False alarms can sometimes cause as much troubles as a real infection.

With AV testing it is important to measure not only detection capabilities but also reliability – one of reliability aspects is certainly product's tendency to flag clean files as infected.

» [VIEW](#)

Malware Removal Tests

These tests (aimed mainly for home users) evaluate the anti-virus products' capability of removing malware and its leftovers from an already compromised system.

For this test we use mainly prevalent "in-the-field" samples from infected PCs of customers.

» [VIEW](#)

Anti-Phishing Tests

These tests evaluate the protection provided against phishing websites. These malicious websites can pose a real threat to any user who is connected to the Internet, as they attempt to steal sensitive information such as usernames, passwords, and credit card details.

» [VIEW](#)

Single Product Tests

Often, antivirus vendors rely on AV-Comparatives to give them an unbiased and competent feedback regarding their new product features and feature updates. These commissioned reviews of a single product help vendors improve their software and offer valuable data regarding the product's overall performance.

» [VIEW](#)

Archive

Looking for something in the archive? The archive stores data from previous years, quickly accessible if needed, like e.g. older or discontinued tests, etc.

» [VIEW](#)

AV-Comparative

- AV-Comparatives是一个由奥地利反病毒实验室主持的杀软独立测试项目。
- 参与测评的产品的成绩：
 - Advanced+、Advanced、Standard、Tested

About us

AV-Comparatives is an independent organization offering systematic testing that checks whether security software, such as PC/Mac-based antivirus products and mobile security solutions, lives up to its promises. Using one of the largest sample collections worldwide, it creates a real-world environment for truly accurate testing. AV-Comparatives offers freely accessible results to individuals, news organizations and scientific institutions. Certification by AV-Comparatives provides an official seal of approval for software performance which is globally recognized.

Currently, AV-Comparatives' Real-World Protection Test is the most comprehensive and complex test available when it comes to evaluating the real-life protection capabilities of antivirus software. Put simply, the test framework replicates the scenario of an everyday user in an everyday online environment – the typical situation that most of us experience when using a computer with an Internet connection.

AV-Comparatives works closely with several academic institutions, especially the University of Innsbruck's Department of Computer Science, to provide scientific testing methods.

各公司的历次测评结果

<http://chart.av-comparatives.org/awardslist.php>



Vendors - AV-Comparatives

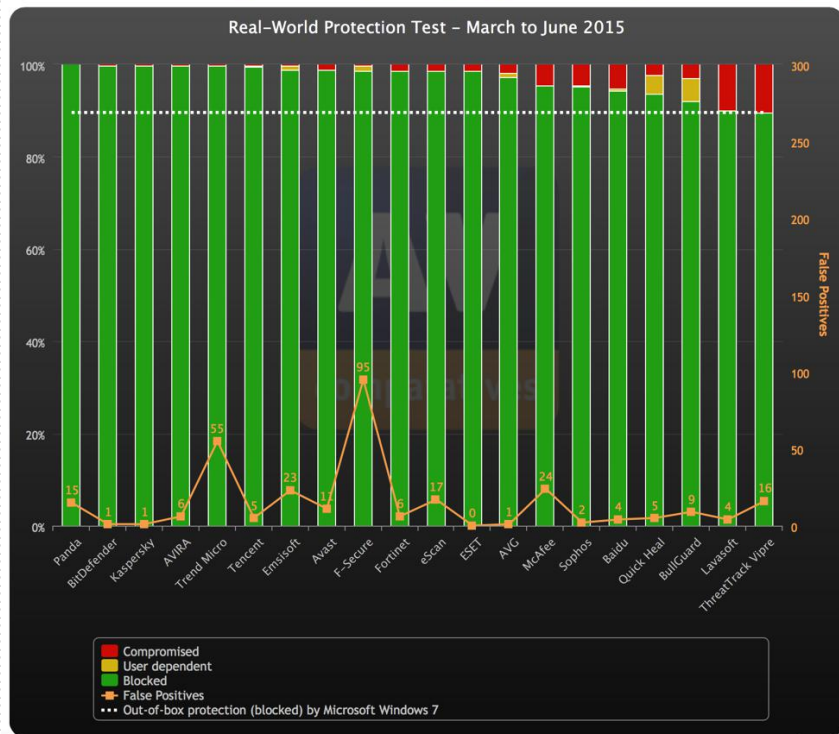
Please select a vendor to show his awards.



2014、2015年Real World Protection Test 整体实际防护能力测试结果

<http://chart.av-comparatives.org/chart1.php>

Test: Real-World Protection Test Year: 2015 Month: Jul Sort: by value Zoom: 0 - 100%



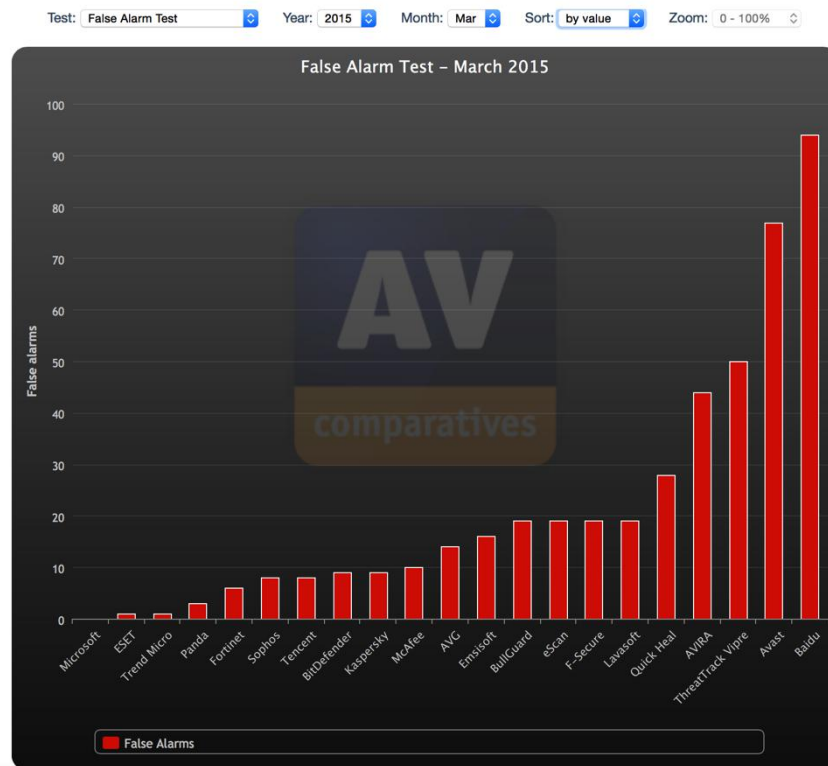
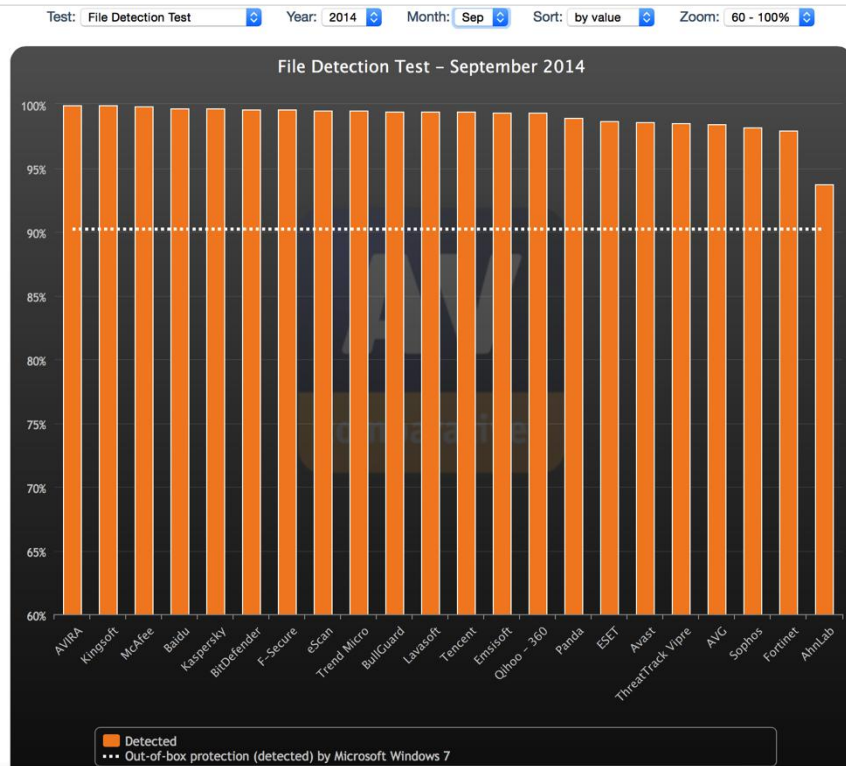
Test: Real-World Protection Test Year: 2014 Month: Dec Sort: by value Zoom: 0 - 100%



2015年File Detection&False Alarm Test

<http://chart.av-comparatives.org/chart1.php>

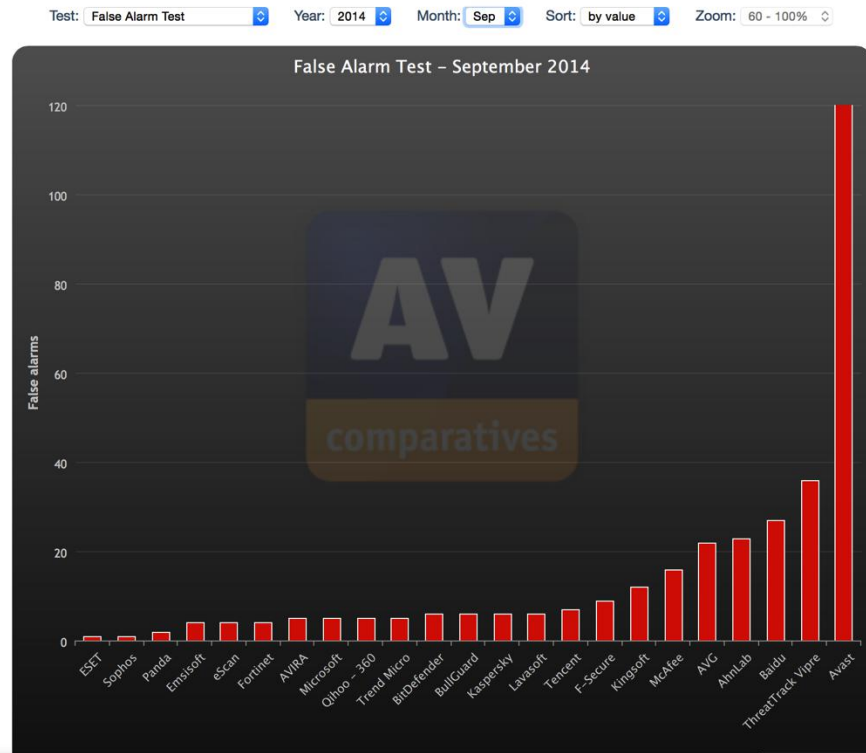
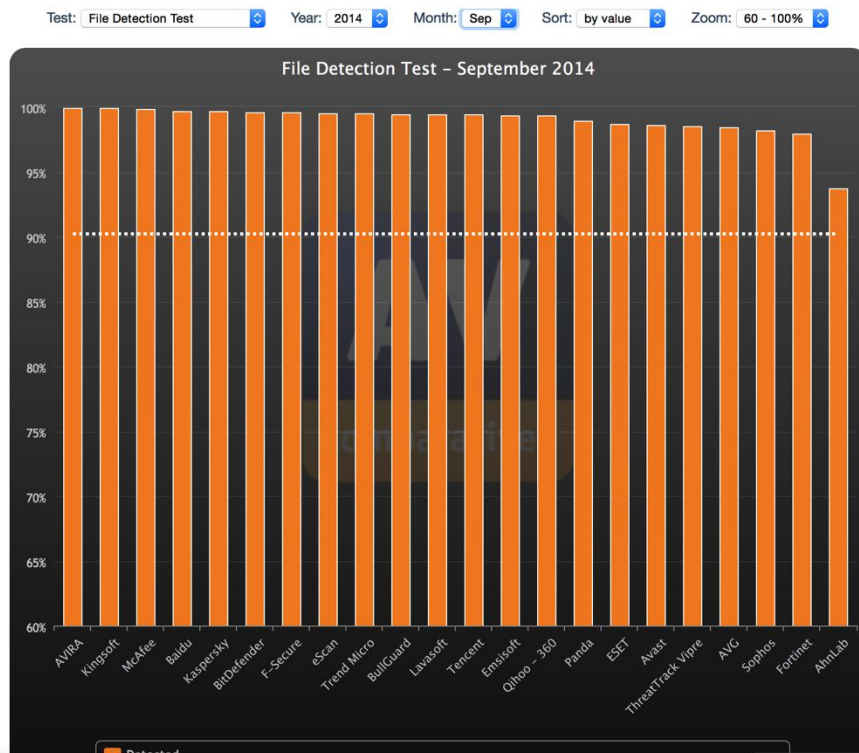
中文报告: http://www.av-comparatives.org/wp-content/uploads/2015/04/avc_fdt_201503_cn.pdf



2014年File Detection&False Alarm Test

<http://chart.av-comparatives.org/chart1.php>

中文报告: http://www.av-comparatives.org/wp-content/uploads/2014/10/avc_fdt_201409_cn.pdf



2014、2015年Heuristic Behavioural Test

<http://chart.av-comparatives.org/chart1.php>

2015年报告: http://www.av-comparatives.org/wp-content/uploads/2015/07/avc_beh_201503_en.pdf



2015年移动安全防护软件检测率测试结果

http://www.av-comparatives.org/wp-content/uploads/2015/03/avc_mob_201502_cn.pdf

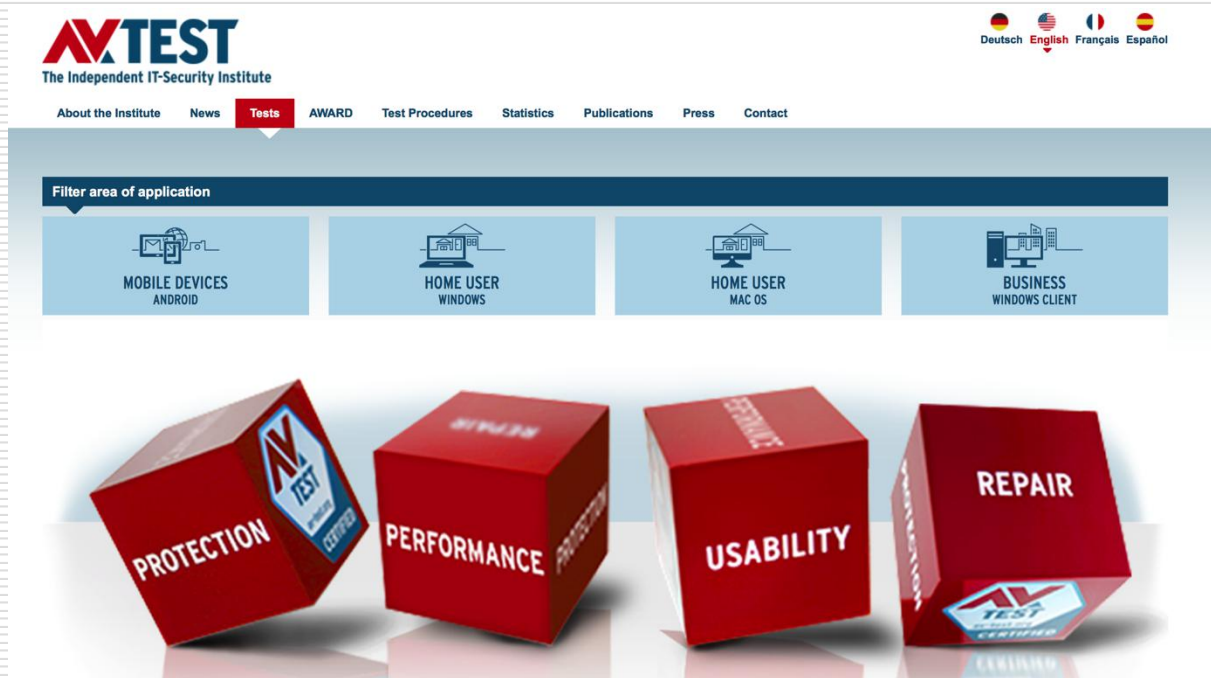
2015 年 2 月 23 日对所有测试的安全产品进行了更新和测试。测试是在有有效互联网连接的真实的安卓智能手机（没有使用虚拟机）上进行的。测试集由专门的 APK 文件组成。首先进行的是按需扫描（on-demand）。之后，手工重新安装未检测到的应用。之所以这样做，是为了允许各安全软件使用实时保护功能来检测恶意应用。

检测率结果

	厂商名称	检测率 ⁶	产品
1.	Antiy Qihoo 360	100.0%	Antiy AVL for Android 2.3 Qihoo 360 AntiVirus 1.3
2.	AVIRA ESET	99.9%	Avira Antivirus Security 3.9 ESET Mobile Security 3.0
3.	Avast	99.8%	Avast Mobile Security 4.0
4.	AhnLab	99.7%	AhnLab V3 Mobile 2.1
5.	Bitdefender Kaspersky Lab	99.6%	Bitdefender Mobile Security 2.36 Kaspersky Internet Security 11.7
6.	Trend Micro	99.3%	Trend Micro Mobile Security 6.0
7.	Quick Heal	98.6%	Quick Heal Total Security 2.0
8.	G Data	96.1%	G Data Internet Security 25.7
9.	安管家	94.7%	安管家 安全管家 5.0

10.7.3 AVTest测试对象和方法

<https://www.av-test.org/en/antivirus/>



AVTest测试方法

测试纬度	Protection (保护能力)	Performance (性能影响)	Usability (可用性)	Repair (修复能力)
测试方法	<p>在纯净可联网电脑环境中安装防护软件，检测其实时保护能力：</p> <ul style="list-style-type: none">• Web恶意网站• Email恶意附件• 来自外部存储设备的恶意文件（两个样本集合，均经AVTest发现和分析）	<ul style="list-style-type: none">• 文件下载• 本地及网络文件拷贝• 程序安装• 程序运行（如Word、Excel等）	<ul style="list-style-type: none">• 提示信息对用户的干扰（distraction）• 误报率	<p>对活动病毒体（以及对系统的恶意或非恶意修改）的清除与恢复能力</p>

在测试中使用了行为监控系统：Sunshine

AVTest测试结果:

<https://www.av-test.org/en/press/test-results/>

Test Results

2015

2014

2013

2012

2011

2010

Mobile Devices Android

January 2014

Products: 30

Android

PNG
RGB

XLSX
Excel 2010+

Screenshots
RGB

March 2014

Products: 31

Android

PNG
RGB

XLSX
Excel 2010+

Screenshots
RGB

May 2014

Products: 30

Android

PNG
RGB

XLSX
Excel 2010+

Screenshots
RGB

July 2014

Products: 29

Android

PNG
RGB

XLSX
Excel 2010+

Screenshots
RGB

September 2014

Products: 32

Android

PNG
RGB

XLSX
Excel 2010+

Screenshots
RGB

November 2014

Products: 31

Android

PNG
RGB

XLSX
Excel 2010+

Screenshots
RGB

Home User Windows

February 2014

Products: 25

Windows 7

PNG
RGB

XLSX
Excel 2010+

Screenshots
RGB

April 2014

Products: 25

Windows 8/8.1

PNG
RGB

XLSX
Excel 2010+

Screenshots
RGB

June 2014

Products: 23

Windows 8¹

PNG
RGB

XLSX
Excel 2010+

Screenshots
RGB

August 2014

Products: 18

Mac OS X

PNG
RGB

XLSX
Excel 2010+

Screenshots
RGB

August 2014

Products: 24

Windows 7

PNG
RGB

XLSX
Excel 2010+

Screenshots
RGB

[illegible]

2013年：安天实验室—AVL反病毒引擎获得AVTest“移动最佳保护奖”



The **AV-TEST AWARD FOR BEST PROTECTION 2013** will be presented to the best product of the year in terms of its protective effect on the Windows und Android operating systems. This category evaluates products according to the protection that they provide against current threats such as malware infections caused by zero-day attacks such as those found in malicious websites and e-mails.

Home Users (Windows):

Bitdefender Internet Security

Corporate Users (Windows):

F-Secure Client Security

Mobile Devices (Android):

Antiy AVL



The **AV-TEST AWARD FOR BEST PERFORMANCE 2013** will be presented to the security software that has the least influence upon a system once installed. The tests that are carried out involve typical activities such as loading websites, downloading software, installing and starting up programs and copying files.

Home Users (Windows):

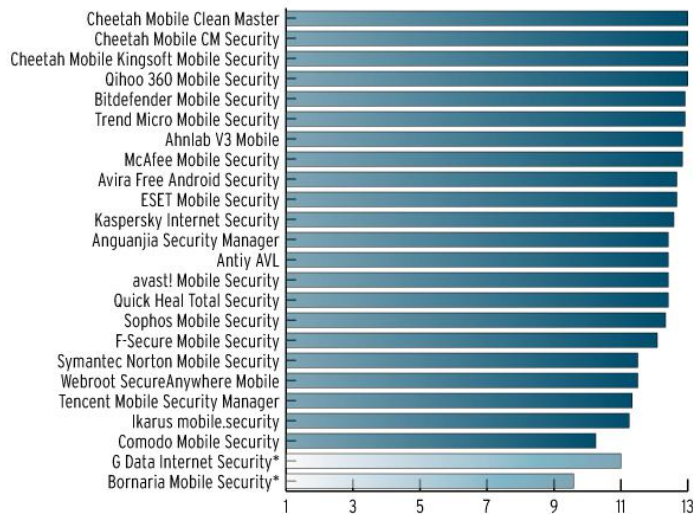
Bitdefender Internet Security

Corporate Users (Windows):

Symantec Endpoint Protection



2014年：猎豹及360获得最佳Android安全产品奖



AV-TEST BEST ANDROID SECURITY PRODUCT 2014 AWARD

The AV-TEST BEST ANDROID SECURITY PRODUCT 2014 AWARD recognizes the safest product for mobile devices.

The 2014 award went to two apps due to a tie vote: Qihoo 360 MobileSecurity and Cheetah Mobile Clean Master.



Android security app



360 AntiVirus ▶



Android security app



Clean Master ▶



课后思考

- ❑ “有人说自己安全意识好，是否安装安全软件都是无所谓的”。请问这一观点是否正确，为什么？
 - ❑ 目前部分安全软件对未知恶意代码检出率高，但误报率也高，有的安全软件检出率相对较低，但误报率也低。对于普通用户来说，你更偏向于向其推荐哪一类安全软件？为什么？
 - ❑ 除了反病毒软件之外，目前市面上还有一部分恶意软件在线检测平台（如 **virustotal**）或沙箱平台（如金山火眼），与终端反病毒软件相比，这类平台各有哪些优缺点？
 - ❑ 当前不少反病毒厂商均推出了云查杀功能，请问云查杀的机理是什么？
 - ❑ 目前部分安全软件测评机构对反病毒软件的未知恶意软件查杀能力进行测试，请问什么是未知恶意软件？其如何构建“未知恶意软件”测试样本集合？
-