

13 恶意代码的检测技术

周威

`weizhou_sec@hust.edu.cn`

本讲提纲

- **13.1 恶意代码检测对象与策略**
- **13.2 特征值检测技术**
- **13.3 校验和检测技术**
- **13.4 启发式扫描技术**
- **13.5 虚拟机检测技术**
- **13.6 主动防御技术**
- **13.7 安全软件评测**

13.1 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：
 - 主板**BIOS**
 - 引导扇区
 - 文件系统中可能带毒的文件
 - 内存空间等
 - (网络流量**VDS**、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（**MBR**、**DPT**、**ID**）
 - 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;.avi...

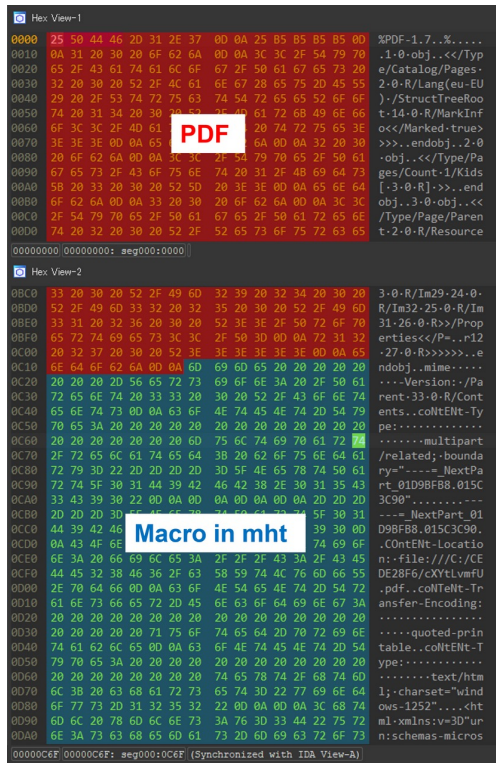
■ 脚本文件

- .js;.vbs;.php;.pl...

■ 网页文件

- .html;.htm;.asp...

■ 其他文件



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

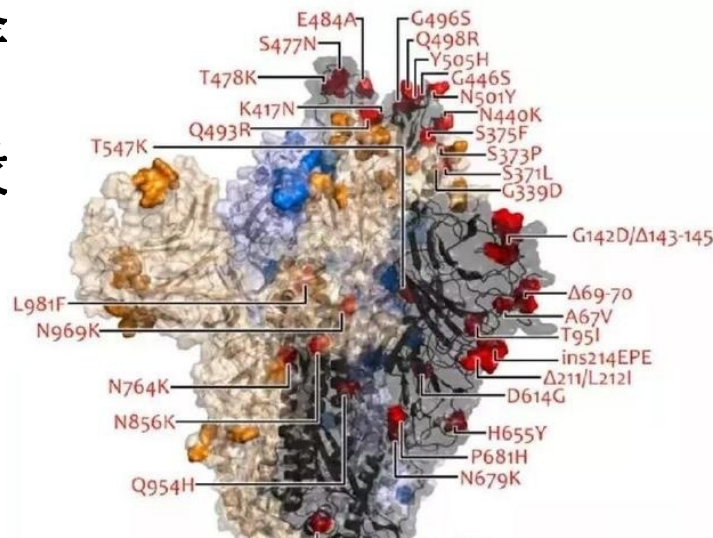
- 13.1 恶意代码检测对象与策略
- 13.2 特征值检测技术
- 13.3 校验和检测技术
- 13.4 启发式扫描技术
- 13.5 虚拟机检测技术
- 13.6 主动防御技术
- 13.7 安全软件评测

13.2 特征值检测技术

- **恶意代码特征值**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**N(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。

熊猫烧香特征码提取

setup.exe X

Address	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
0000c040	2a	2a	2a	ce	e4	2a	ba	ba	2a	c4	d0	2a	c9	fa	2a	b8
0000c050	d0	2a	c8	be	2a	cf	c2	2a	d4	d8	2a	d5	df	2a	2a	2a
0000c060	00	00	00	00	ff	ff	ff	ff	1f	00	00	00	b8	d0	d0	bb
0000c070	b0	ac	c2	ea	2c	6d	6f	70	65	72	79	b6	d4	b4	cb	c4
0000c080	be	c2	ed	b5	c4	b9	d8	d7	a2	21	7e	00	ff	ff	ff	ff
0000c090	04	00	00	00	78	62	6f	79	00	00	00	00	ff	ff	ff	ff
0000c0a0	20	00	00	00	22	2b	2b	ce	ec	2b	2b	2b	2b	2b	2b	2b
0000c0b0	c1	fb	2b	b8	d8	2b	c9	be	22	ce	c1	fb	2b	b8	d8	2b
0000c0c0	d7	2b	2b	2a	00	00	00	00	ff	ff	d7	2b	2b	2a	00	00
0000c0d0	77	68	62	6f	79	00	00	00	ff	ff	77	68	62	6f	79	00
0000c0e0	64	7d	74	71	3b	2a	26	74	79	6c	64	7d	74	71	3b	2a
0000c0f0	62	6f	79	27	62	6c	74	2e	76	6a	62	6f	79	27	62	6c

***武*汉*男*生*感
*染*下*载*者***
.... 感谢
艾玛,mopery对此木
马的关注!~.

Section Viewer					
Name	V. Offset	V. Size	R. Offset	R. Size	Flags
CODE	00001000	0000BD30	00000400	0000BE00	60000020
DATA	0000D000	000002C0	0000C200	00000400	C0000040
BSS	0000E000	000007DD	0000C600	00000000	C0000000
.idata	0000F000	00000C68	0000C600	00000E00	C0000040
.tls	00010000	00000008	0000D400	00000000	C0000000
.rdata	00011000	00000018	0000D400	00000200	50000040
.reloc	00012000	00000AA8	0000D600	00000C00	50000040
.rsrc	00013000	00000A00	0000E200	00000A00	50000040

Close

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

- 13.1 恶意代码检测对象与策略
- 13.2 特征值检测技术
- 13.3 校验和检测技术
- 13.4 启发式扫描技术
- 13.5 虚拟机检测技术
- 13.6 主动防御技术
- 13.7 安全软件评测

13.3 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、
- 不能识别病毒特征
- 效率低。

本讲提纲

- 13.1 恶意代码检测对象与策略
- 13.2 特征值检测技术
- 13.3 校验和检测技术
- 13.4 启发式扫描技术
- 13.5 虚拟机检测技术
- 13.6 主动防御技术
- 13.7 安全软件评测

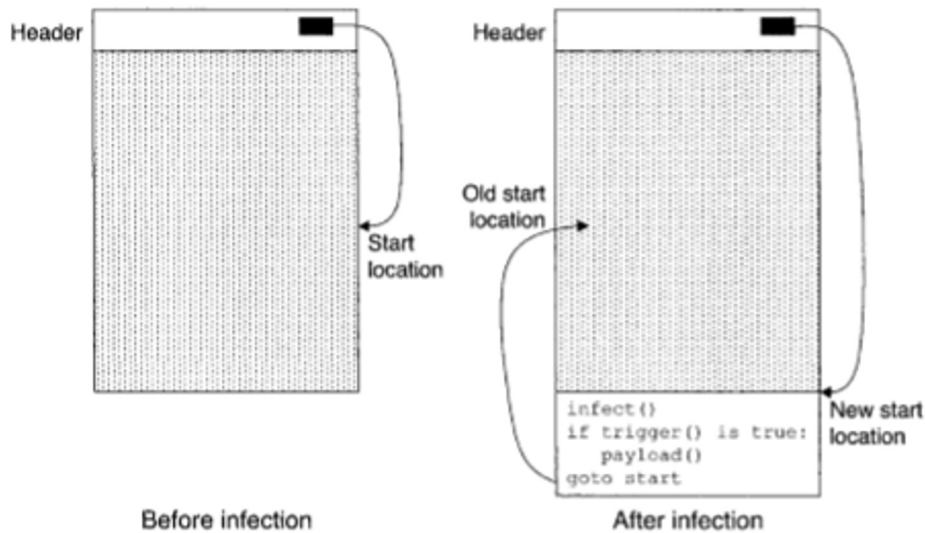
13.4 启发式扫描技术

- **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。

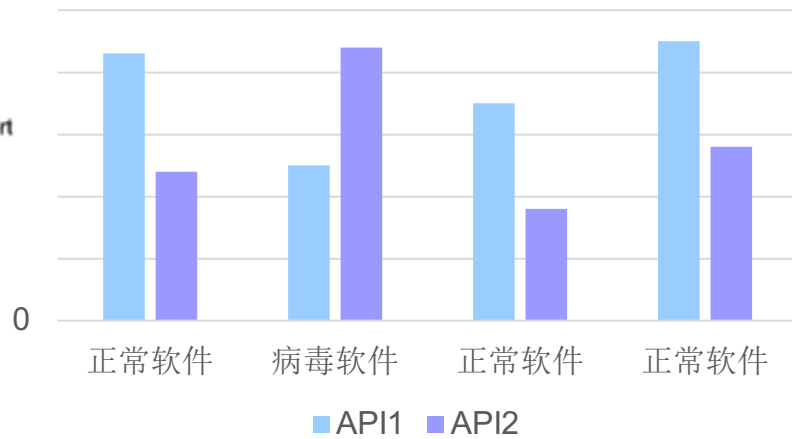
可疑的程序代码指令序列

- 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、远距离跳转指令(超过文件长度的三分之二) 等
- 敏感系统行为
- 敏感API函数（序列）调用功能。。。

长跳转、敏感API统计



不同API 调用次数统计
示意图



系统调用DLL

Kernel32.dll 常见的DLL，核心系统功能：访问和操作内存、文件和硬件等等

Advapi32.dll 服务管理器和注册表组件

User32.dll 用户界面

Gdi32.dll 图形显示和操作

Ntdll.dll Windows内核的接口

Wsock32.dll 联网DLL

Ws2_32.dll

Wininet.dll 更高层次的网络函数，实现了如FTP、HTTP

PackedProgram

■ Kernel32.dll:

- GetModuleHandleA
- LoadLibraryA
- GetProcAddress
- ExitProcess
- VirtualAlloc
- VirtualFree

□ User32.dll:

- MessageBoxA

启发式扫描步骤



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。



Report



Export

Consumer Test Charts

Consumer

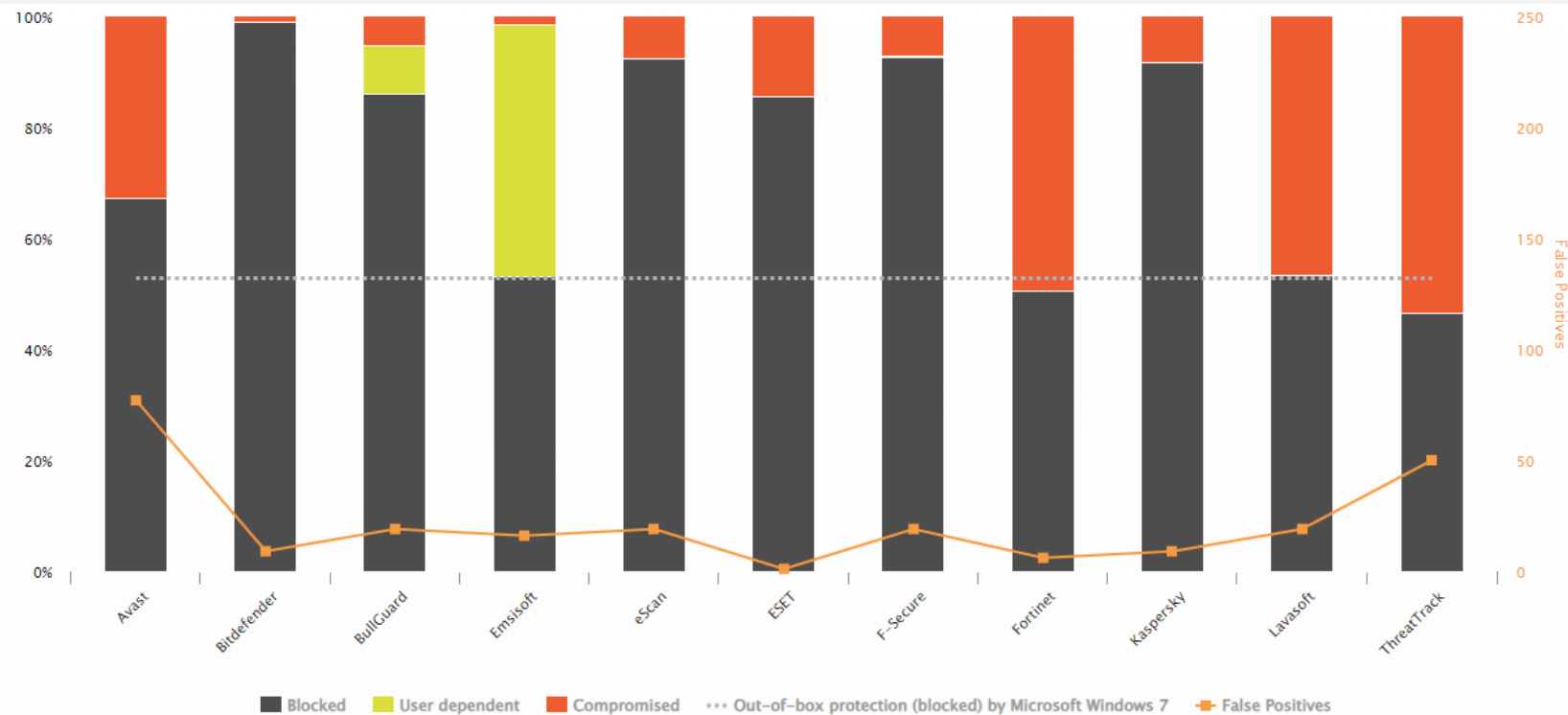
Heuristic Behavioural Test

2015

Mar

by vendor

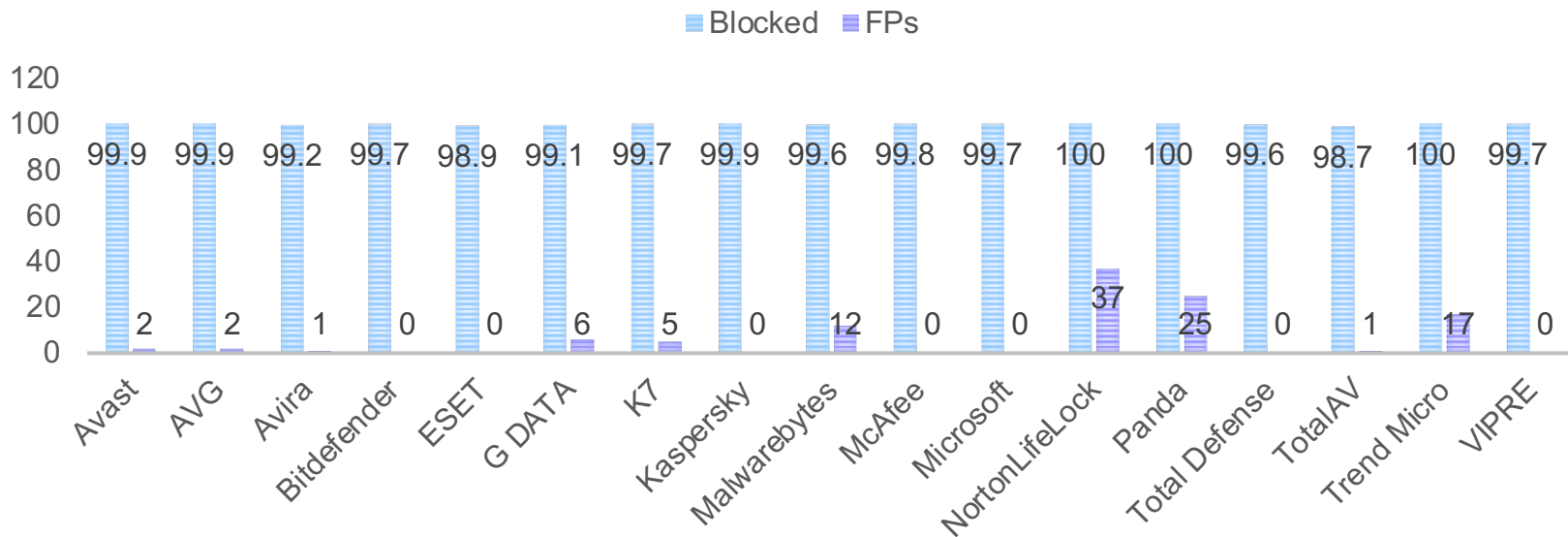
0 - 100%



2021 AVC测试结果-拦截率、误报率

误报：干净样例被错误归入恶意代码

图表标题



针对启发式扫描技术，病毒如何博弈？

■ 直接对抗

- 关闭启发式机制
- 关闭反病毒软件

■ 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？

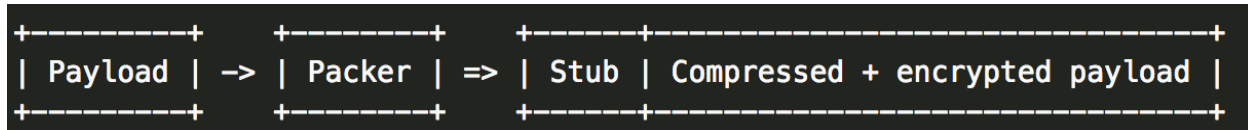
本讲提纲

- 13.1 恶意代码检测对象与策略
- 13.2 特征值检测技术
- 13.3 校验和检测技术
- 13.4 启发式扫描技术
- 13.5 虚拟机检测技术
- 13.6 主动防御技术
- 13.7 安全软件评测

13.5 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。

■ 不足

- 病毒可以检测自身是否处于虚拟化环境中进而改变行为特征

本讲提纲

- 13.1 恶意代码检测对象与策略
- 13.2 特征值检测技术
- 13.3 校验和检测技术
- 13.4 启发式扫描技术
- 13.5 虚拟机检测技术
- 13.6 主动防御技术
- 13.7 安全软件评测

13.6 主动防御技术

- 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。

13.7 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？




























13.7.1 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

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

13.7.2 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**

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.

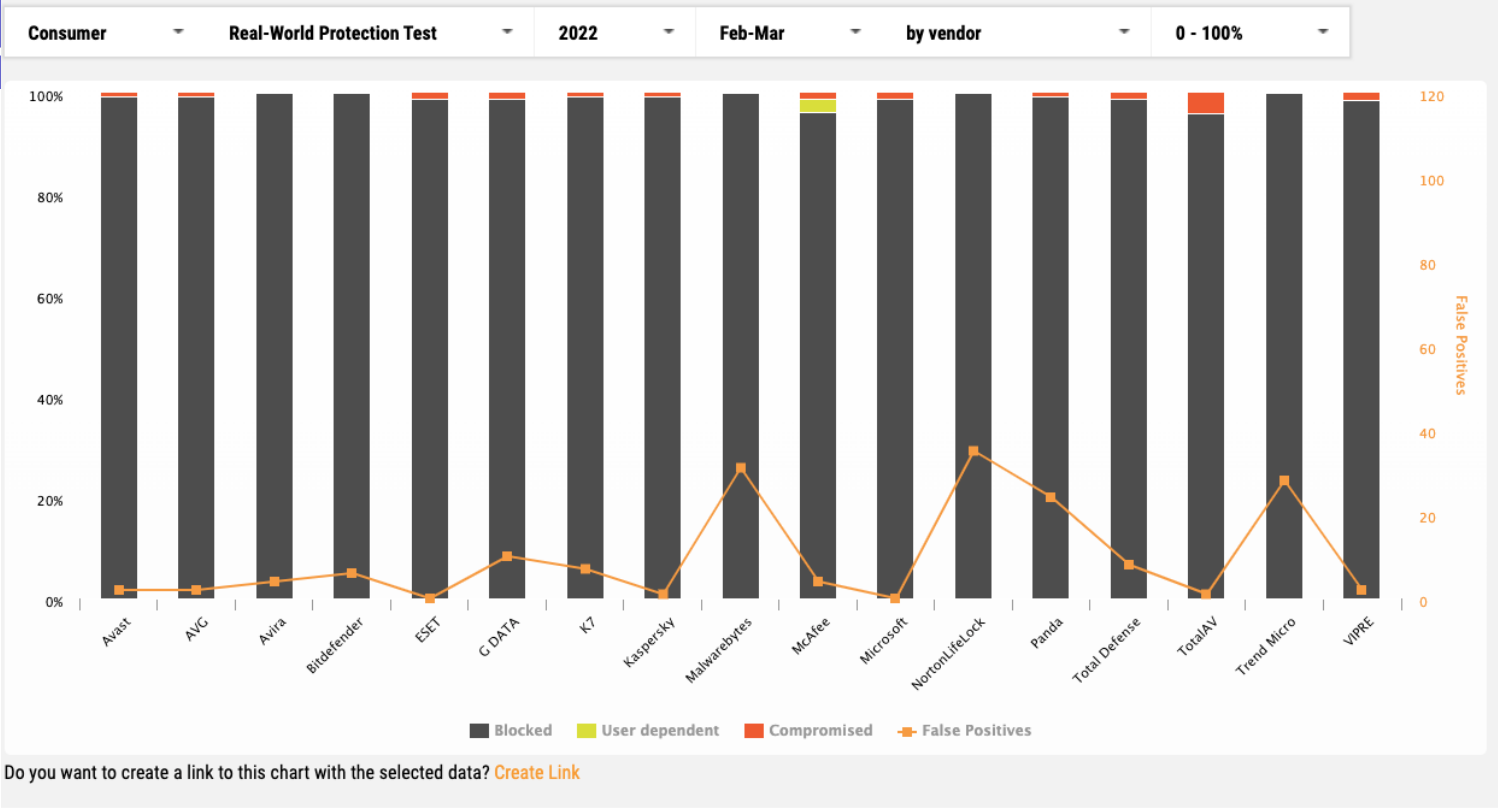
The story of AV-Comparatives began the way it does with so many computer users, namely with a virus infection. In 1993, **Andreas Clementi** was hit by a computer virus: the "November 17 virus – NOV_17.855". This awakened his interest. Andreas was not satisfied with the sometimes very contradictory tests of antivirus programs in computer magazines, and so began the intensive investigation of malware and antivirus software, which continues to this day. In 1999, he and **Peter Stelzhammer** founded AV-Comparatives as a student project at the University of Innsbruck. This was done purely out of technical interest, to see how good the products of different manufacturers actually are. The response was enormous, as the manufacturers of antivirus software became aware of the duo in Innsbruck and wanted to take part in the tests.

各公司的测评结果

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

Vendor	Test	Award	Platform
 Avast	Avast Free Antivirus	Real-World Protection Test July-October 2023	★ ★ ★
Microsoft Windows			
 AVG	AVG Free AntiVirus	Real-World Protection Test July-October 2023	★ ★ ★
Microsoft Windows			
 Avira	Avira Prime	Real-World Protection Test July-October 2023	★ ★ ★
Microsoft Windows			
 Bitdefender	Bitdefender Internet Security	Real-World Protection Test July-October 2023	★ ★ ★
Microsoft Windows			
 G Data	G Data Total Security	Real-World Protection Test July-October 2023	★ ★ ★
Microsoft Windows			
 Kaspersky	Kaspersky Standard	Real-World Protection Test July-October 2023	★ ★ ★
Microsoft Windows			
 McAfee	McAfee Total Protection	Real-World Protection Test July-October 2023	★ ★ ★
Microsoft Windows			
 F-Secure	F-Secure Internet Security	Real-World Protection Test July-October 2023	★ ★ ☆
Microsoft Windows			
 K7 COMPUTING	K7 Total Security	Real-World Protection Test July-October 2023	★ ★ ☆
Microsoft Windows			
 Microsoft	Microsoft Defender	Real-World Protection Test July-October 2023	★ ★ ☆
Microsoft Windows			
 norton	Norton Antivirus Plus	Real-World Protection Test July-October 2023	★ ★ ☆
Microsoft Windows			
 TOTAL AV	TotalAV Antivirus Pro	Real-World Protection Test July-October 2023	★ ★ ☆
Microsoft Windows			
 Avast	Avast Free Antivirus	Real-World Protection Test July-October 2023	★ ★ ★
Microsoft Windows			

整体实际防护能力测试结果<https://www.av-comparatives.org/comparison>



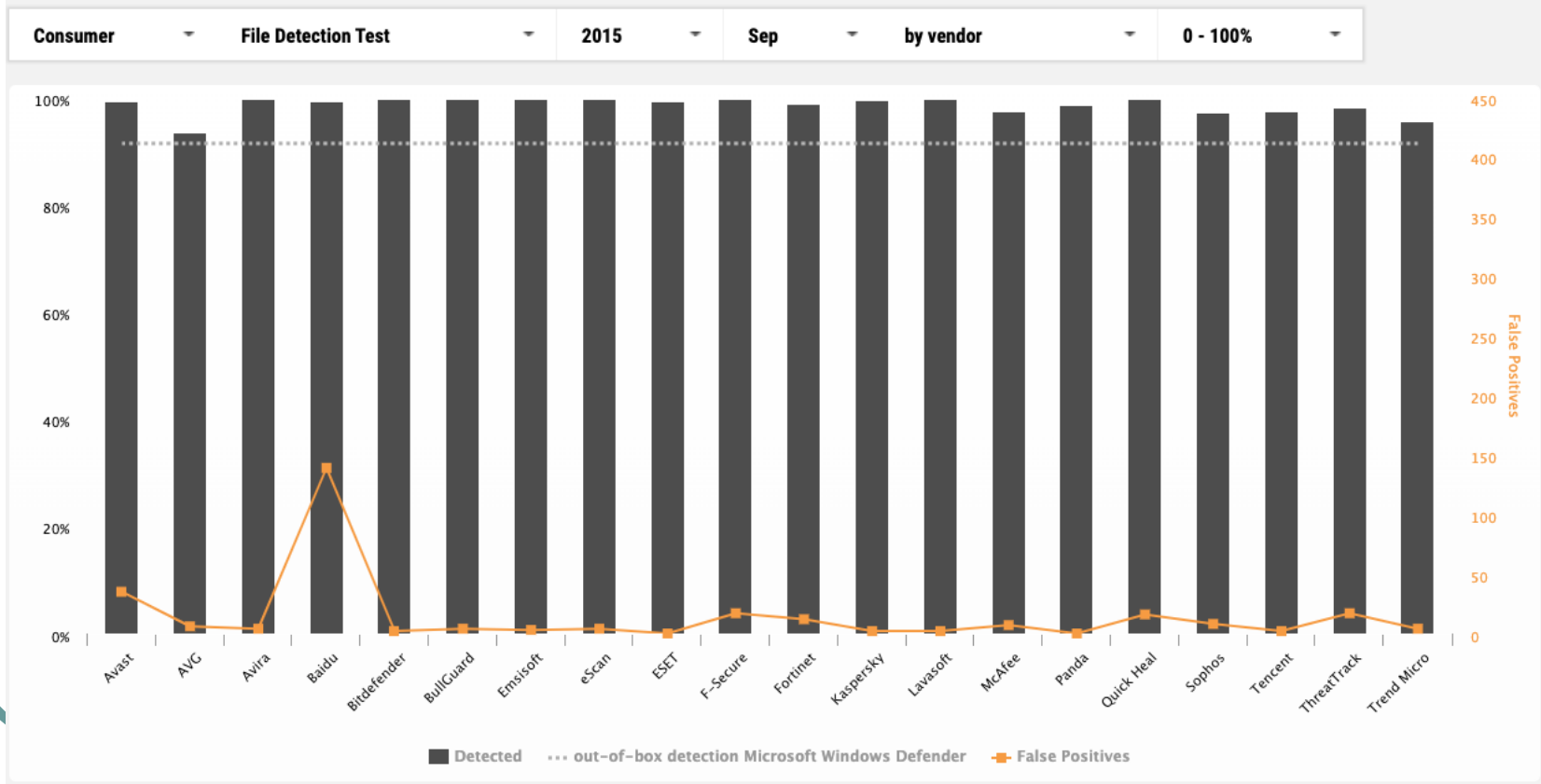
Terminology:

- Blocked ... Malware was successfully blocked by AV
- User Dependent ... The user had the option to allow the execution of the malware
- Compromised ... Malware compromised the system
- False Positive ... A clean sample was wrongly detected as malicious

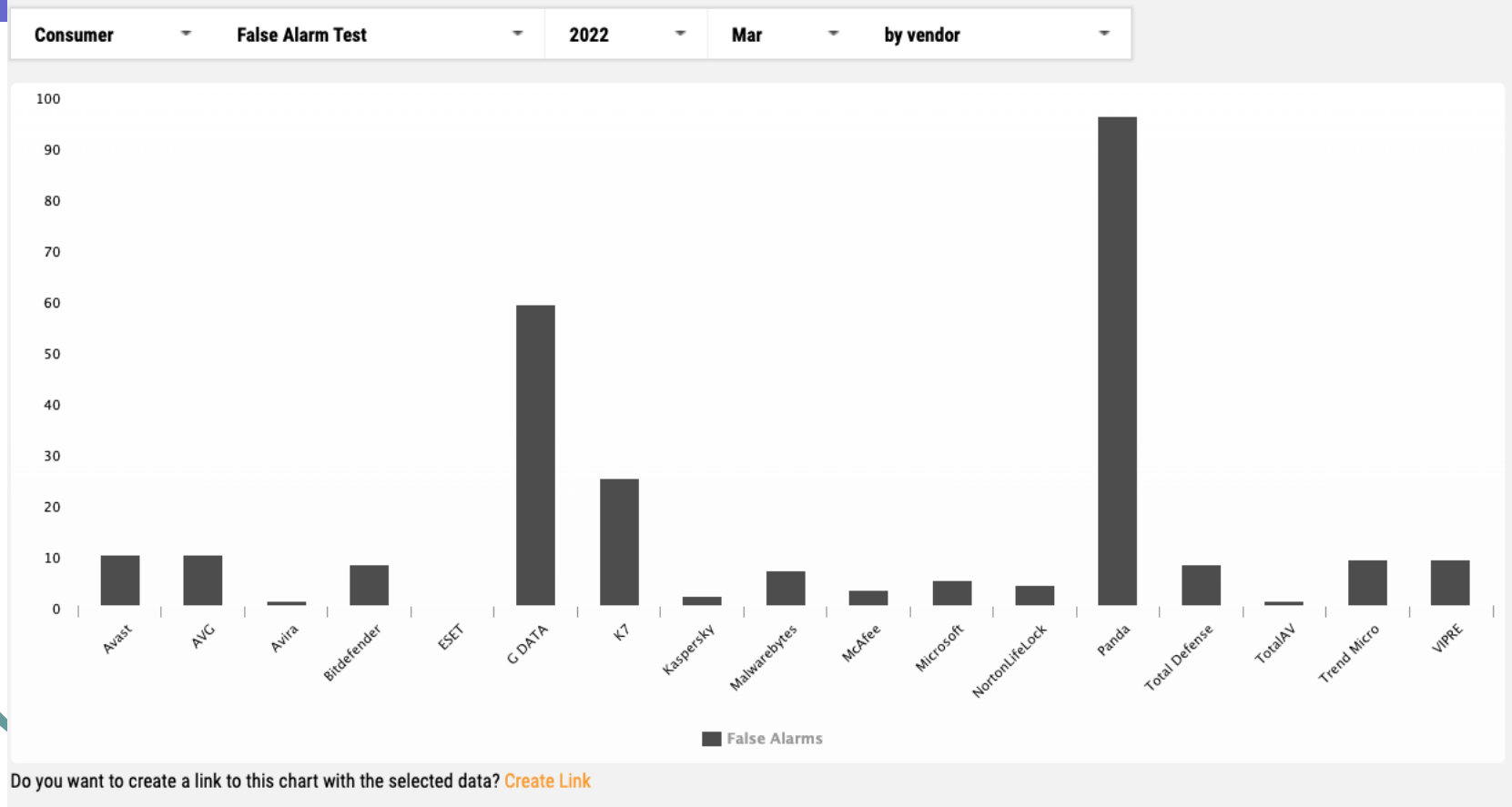
2015年File Detection

Consumer Test Charts

Report Export



2015年False Alarm Test



2015年移动安全防护软件检测率测试结果

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

思考题

- “提高安全意识，是否安装安全软件都是无所谓的”。这种观点是否正确，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？

思考题

- 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和传统杀毒软件的优缺点？
- 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？

软件课程结束

预祝大家考出好成绩！
谢谢

