清华大学出版社
TSINGHUA UNIVERSITY PRESS

重点大学信息安全专业规划系列教材

恶意代码与计算机病毒
——原理、技术和实践

第1章 恶意代码概述

刘功申
上海交通大学网络空间安全学院

本章学习目标

- 明确恶意代码的基本概念
- 了解恶意代码的发展历史
- 熟悉恶意代码的分类
- 熟悉恶意代码的命名规则
- 了解恶意代码的未来发展趋势

一、为什么提出恶意代码的概念？

- 计算机病毒的官方定义不能涵盖新型恶意代码
  - 《中华人民共和国计算机信息系统安全保护条例》
  - 《计算机病毒防治管理办法》
  - 传统计算机病毒定义：是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

传统计算机病毒定义的不足之处

- 传统定义强调：把破坏代码插入正常程序中，而忽略把代码直接复制到硬盘上的独立恶意程序（例如，木马），忽略恶意程序主动侵入设备（例如，蠕虫）等。
- 传统定义没有排除：具有恶意行为，但不是有意为之的行为，例如，不小心形成的恶意行为。
- 这些不足带来的法律问题
  - 使用这个定义可能逃脱应有的惩罚

二、恶意代码定义

- 恶意代码：在未被授权的情况下，以破坏软硬件设备、窃取用户信息、扰乱用户心理、干扰用户正常使用为目的而编制的软件或代码片段。
- 这个定义涵盖的范围非常广泛，它包含了所有敌意、插入、干扰、讨厌的程序和源代码。
- 一个软件被看作是恶意代码主要是依据创作者的意图，而不是恶意代码本身的特征。

恶意代码的特征

1. 目的性

- 目的性是恶意代码的基本特征，是判别一个程序或代码片段是否为恶意代码的最重要的特征，也是法律上判断恶意代码的标准。

2. 传播性

- 传播性是恶意代码体现其生命力的重要手段。

3. 破坏性

- 破坏性是恶意代码的表现手段。

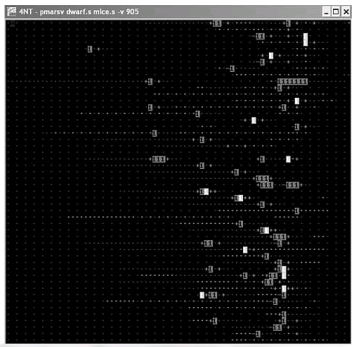
- 恶意代码产生的动机(原因)：
  - 计算机系统的脆弱性(IBM病毒防护计划)
  - 作为一种文化（hacker）
  - 病毒编制技术学习
  - 恶作剧\报复心理
  - 用于版权保护（xx公司）
  - 用于特殊目的（军事、某些计算机防病毒公司）
  - 赚钱、赚钱、赚钱……

三、恶意代码简史

- 萌芽
- Unix病毒
- DOS时代的病毒
- 网络时代的恶意代码
- 恶意代码新时代

1、萌芽阶段

- 在第一部商用电脑出现之前，冯·诺伊曼在他的论文《复杂自动装置的理论及组识的进行》里，就已经勾勒出了病毒程序的蓝图。
- 70年代美国作家雷恩出版的《P1的青春－The Adolescence of P1》一书中作者构思出了计算机病毒的概念。
- 美国电话电报公司(AT&T)的贝尔实验室中，三个年轻程序员道格拉斯.麦耀莱、维特.维索斯基和罗伯.莫里斯在工作之余想出一种电子游戏叫做“磁芯大战(core war)”。



```
;name          Dwarf
;author        A. K. Dewdney
;version       94.1
;date          April 29, 1993
;strategy      Bombs every fourth instruction.

ORG     1 ; Indicates execution begins with the second
          ; instruction (ORG is not actually loaded, and is
          ; therefore not counted as an instruction).

DAT.F   #0, #0     ; Pointer to target instruction.
ADD.AB  #4, $-1    ; Increments pointer by 4.
MOV.AB  #0, @-2    ; Bombs target instruction.
JMP.A   $-2, #0    ; Loops back two instructions.
```

2、第一个真病毒

- 博士论文的主题是计算机病毒
- 1983年11月3日，Fred Cohen博士研制出第一个计算机病毒（Unix）。

3、Dos时代的病毒

- 1986年初，巴基斯坦的拉合尔，巴锡特和阿姆杰德两兄弟编写了Pakistan病毒，即Brain，其目的是为了防范盗版软件。
  - Dos – PC – 引导区
- 1987年世界各地的计算机用户几乎同时发现了形形色色的计算机病毒，如大麻、IBM圣诞树、黑色星期五等等 。

视窗病毒

- 1988 年 3 月 2 日，一种苹果机的病毒发作，这天受感染的苹果机停止工作，只显示“向所有苹果电脑的使用者宣布和平的信息”。以庆祝苹果机生日。

莫里斯蠕虫（Morris Worm） 1988年

肇事者

- Robert T. Morris ，美国康奈尔大学学生，其父是美国国家安全局安全专家。

机理

- 利用sendmail, finger 等服务的漏洞，消耗CPU资源，并导致拒绝服务。

影响

- Internet上大约6000台计算机感染，占当时Internet 联网主机总数的10%，造成9600万美元的损失。

CERT/CC的诞生

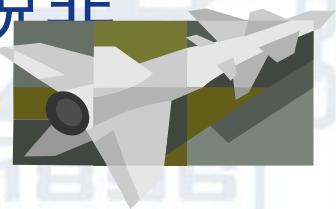
- DARPA成立CERT（Computer Emergency Response Team），以应付类似事件。

- 1989年，全世界计算机病毒攻击十分猖獗，其中“米开朗基罗”病毒给许多计算机用户（包括中国）造成了极大损失。

- 全球流行DOS病毒

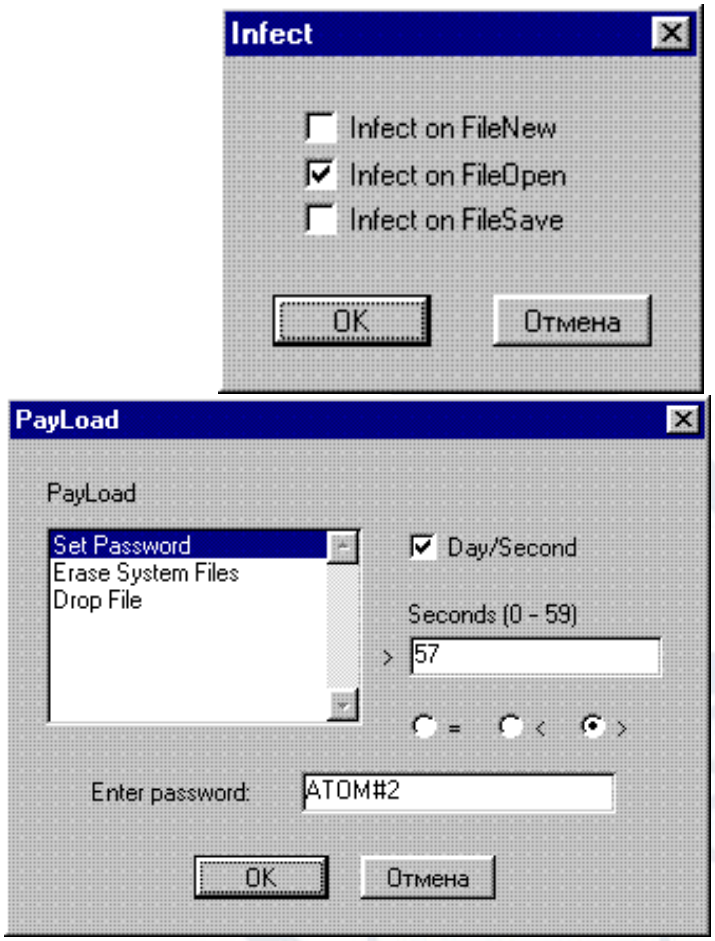
4、用于军事的恶意代码

- 在沙漠风暴行动的前几周，一块被植入病毒（AF/91（1991））的计算机芯片被安装进了伊拉克空军防卫系统中的一台点阵打印机中。
- 该打印机在法国组装，取道约旦、阿曼运到了伊拉克。
- 病毒瘫痪了伊拉克空军防卫系统中的一些Windows系统主机以及大型计算机，据说非常成功。



5、傻瓜式恶意代码——宏病毒

- 1996年，出现针对微软公司Office的“宏病毒”。
- 1997年公认为计算机反病毒界的“宏病毒年”。
- 特点：书写简单，甚至有很多自动制作工具



6、烧毁硬件的恶意代码CIH（1998-1999）

- 1998年，首例破坏计算机硬件的CIH病毒出现，引起人们的恐慌。
- 1999年4月26日，CIH病毒在我国大规模爆发，造成巨大损失。

7、网络恶意代码时代：蠕虫

- 1999年3月26日，出现一种通过因特网进行传播的美丽莎病毒。
- 2001年7月中旬，一种名为“红色代码”的病毒在美国大面积蔓延，这个专门攻击服务器的病毒攻击了白宫网站，造成了全世界恐慌。
- 2003年，“2003蠕虫王”病毒在亚洲、美洲、澳大利亚等地迅速传播，造成了全球性的网络灾害。
- 记忆犹新的3年（2003 - 2005）

- 2004年是蠕虫泛滥的一年，大流行病毒：
  - 网络天空(Worm.Netsky)
  - 高波(Worm.Agobot)
  - 爱情后门(Worm.Lovgate)
  - 震荡波(Worm.Sasser)
  - SCO炸弹(Worm.Novarg)
  - 冲击波(Worm.Blaster)
  - 恶鹰(Worm.Bbeagle)
  - 小邮差(Worm.Mimail)
  - 求职信(Worm.Klez)
  - 大无极(Worm.SoBig)

8、木马时代

- 2005年是木马流行的一年，新木马包括：
  - 8月9日，“闪盘窃密者（Trojan.UdiskThief）”病毒。该木马病毒会判定电脑上移动设备的类型，自动把U盘里所有的资料都复制到电脑C盘的“test”文件夹下，这样可能造成某些公用电脑用户的资料丢失。
  - 11月25日，“证券大盗”（Trojan/PSW.Soufan）。该木马病毒可盗取包括南方证券、国泰君安在内多家证券交易系统的交易账户和密码，被盗号的股民账户存在被人恶意操纵的可能。
  - 7月29日，“外挂陷阱”（troj.Lineage.hp）。此病毒可以盗取多个网络游戏的用户信息，如果用户通过登陆某个网站，下载安装所需外挂后，便会发现外挂实际上是经过伪装的病毒，这个时候病毒便会自动安装到用户电脑中。
  - 9月28日，" 我的照片" (Trojan.PSW.MyPhoto)病毒。该病毒试图窃取《热血江湖》、《传奇》、《天堂Ⅱ》、《工商银行》、《中国农业银行》等数十种网络游戏及网络银行的账号和密码。该病毒发作时，会显示一张照片使用户对其放松警惕。

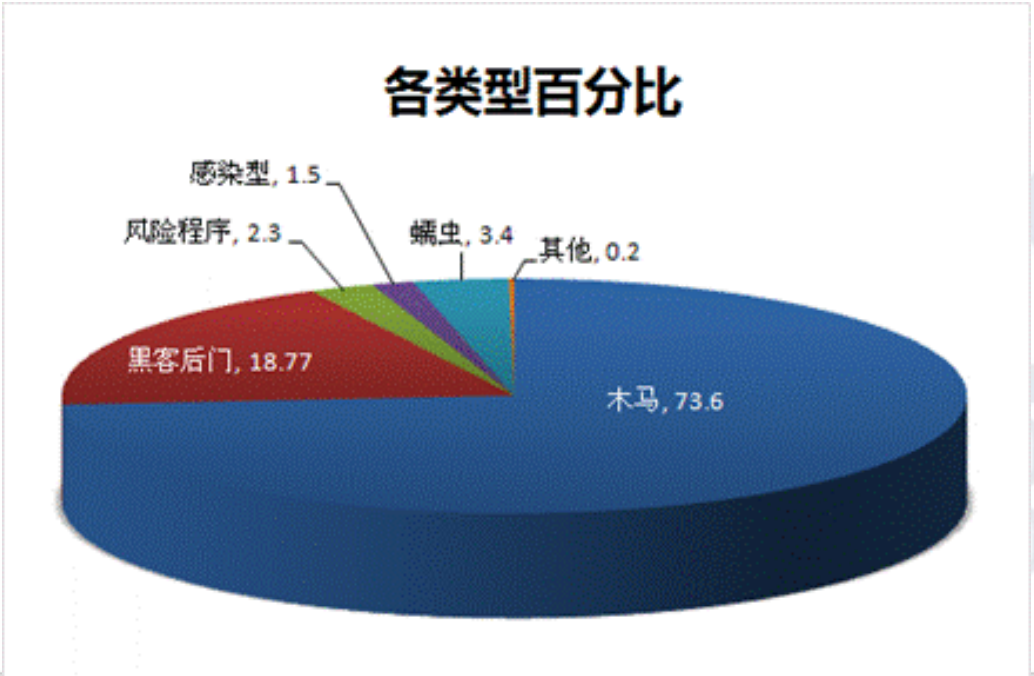
2006年木马仍然是病毒主流，变种层出不穷

- 2006年上半年，江民反病毒中心共截获新病毒33358种，另据江民病毒预警中心监测的数据显示，1至6月全国共有7322453台计算机感染了病毒，其中感染木马病毒电脑2384868台，占病毒感染电脑总数的32.56%，感染广告软件电脑1253918台，占病毒感染电脑总数的17.12%，感染后门程序电脑 664589台，占病毒感染电脑总数的9.03%，蠕虫病毒216228台，占病毒感染电脑总数的2.95%，监测发现漏洞攻击代码感染181769台，占病毒感染电脑总数的2.48%，脚本病毒感染15152台，占病毒感染电脑总数的2.06%。

最前沿病毒

- 2007年：
  - 流氓软件——反流氓软件技术对抗的阶段。
    - Cnnic
    - 3721 – yahoo
    - 熊猫烧香
- 2008年：
  - 木马
  - ARP
  - Phishing（网络钓鱼）

- 2009年
  - 恶意代码产业化
  - 木马是主流
  - 其他：浏览器劫持、下载捆绑、钓鱼



- 2010年
  - 新增恶意代码750万（瑞星）；
  - 流行恶意代码：快捷方式真假难分、木马依旧猖獗，但更注重经济利益和特殊应用。

2011年

- 随着SNS等新型社交网络的迅速崛起，恶意代码制造者又有了新的病毒载体平台。
  - 例如，新浪微波的
- 移动互联网平台恶意代码。例如，手机病毒。

2012年中国计算机病毒统计

- 根据金山毒霸安全中心统计2012年共捕获病毒样本总量超过4200万个，比上一年增长41.4%，月捕获病毒样本数在300万至450万个之间，日均超过11万个。
- 鬼影病毒、AV终结者末日版、网购木马、456游戏木马、连环木马(后门)、QQ粘虫木马、新淘宝客病毒、浏览器劫持病毒、传奇私-Fu劫持者、QQ群蠕虫病毒等病毒类型对用户危害最大。

9、手机恶意代码登场

TOP 10 mobile threats detected in

	Name*	% of all attacks
1	DangerousObject.Multi.Generic	40.42%
2	Trojan-SMS.AndroidOS.OpFake.bo	21.77%
3	AdWare.AndroidOS.Ganlet.a	12.40%
4	Trojan-SMS.AndroidOS.FakeInst.a	10.37%
5	RiskTool.AndroidOS.SMSreg.cw	8.80%
6	Trojan-SMS.AndroidOS.Agent.u	8.03%
7	Trojan-SMS.AndroidOS.OpFake.a	5.49%
8	Trojan.AndroidOS.Plangton.a	5.37%
9	Trojan.AndroidOS.MTK.a	4.25%
10	AdWare.AndroidOS.Hamob.a	3.39%

来源：http://securelist.com/analysis/kaspersky-security-bulletin/58335/mobile-malware-evolution-2013/

2014 年终最猖狂的手机木马 TOP10

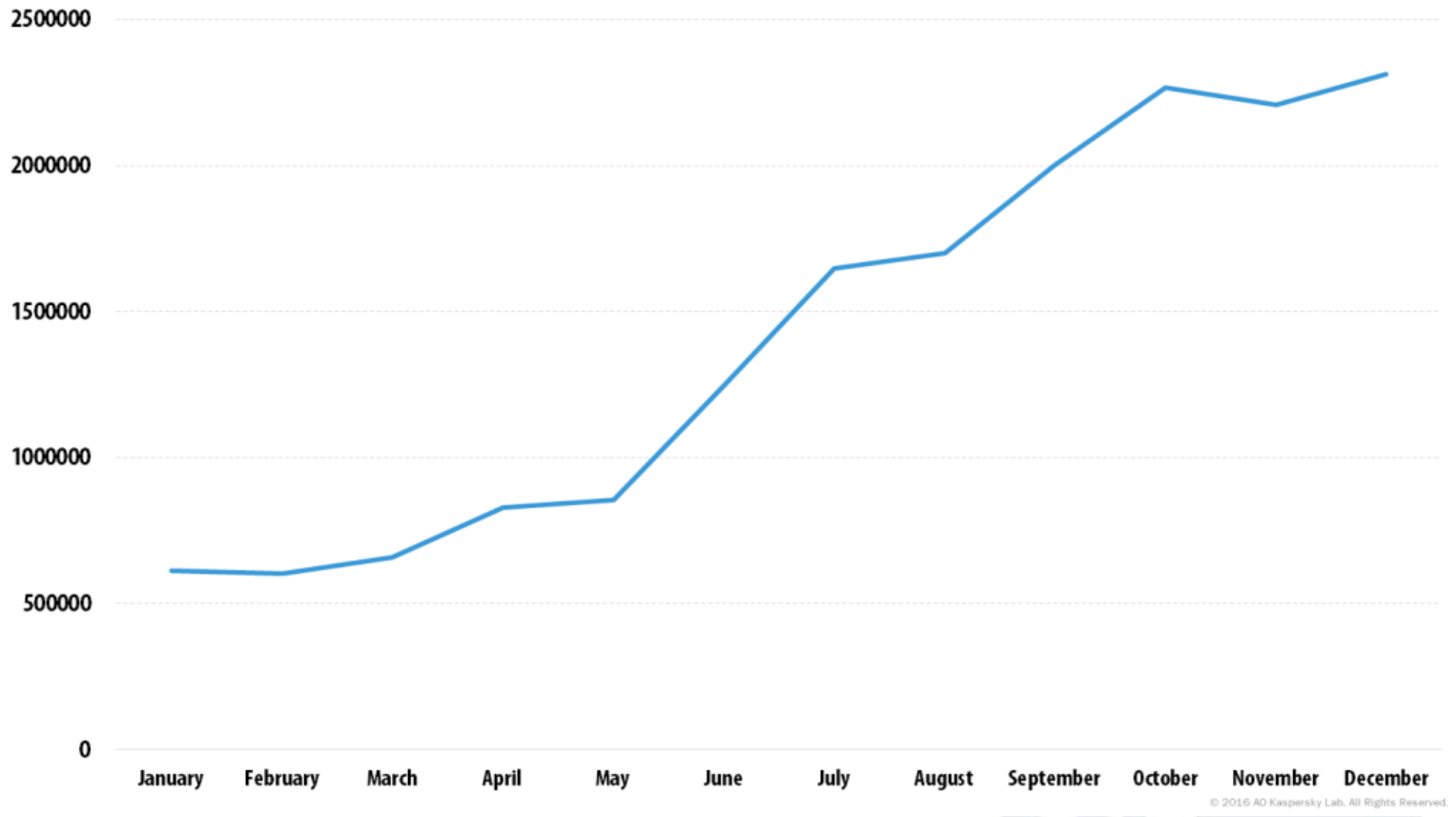
名称	恶意行为	感染量
无码高清	恶意广告弹窗，耗费流量	140.65 万
咪咪影院	私下软件，泄露隐私，耗费流量和话费	92.66 万
色啦影音	私下软件，泄露隐私，耗费流量和话费	53.55 万
冲浪快讯	接收短信指令控制向外发送指定短信，泄露隐私信息，伪造卸载界面，防止正常卸载	48.08 万
全民切水果（山寨版）	私下软件，泄露隐私，耗费流量和话费	30.07 万
快播魅影	私下软件，泄露隐私，耗费流量和话费	24.97 万
雷电战机	私下软件，泄露隐私，耗费流量和话费	19.66 万
狂浪视觉	私下软件，泄露隐私，耗费流量和话费	12.65 万
真人美女	私下软件，泄露隐私，耗费流量和话费	9.53 万
极欲视频	诱导用户注册设备管理器，释放恶意子包，强制在第三方应用上弹出广告，诱骗用户点击后造成话费损失。	8.09 万

数据来源：360 手机安全中心

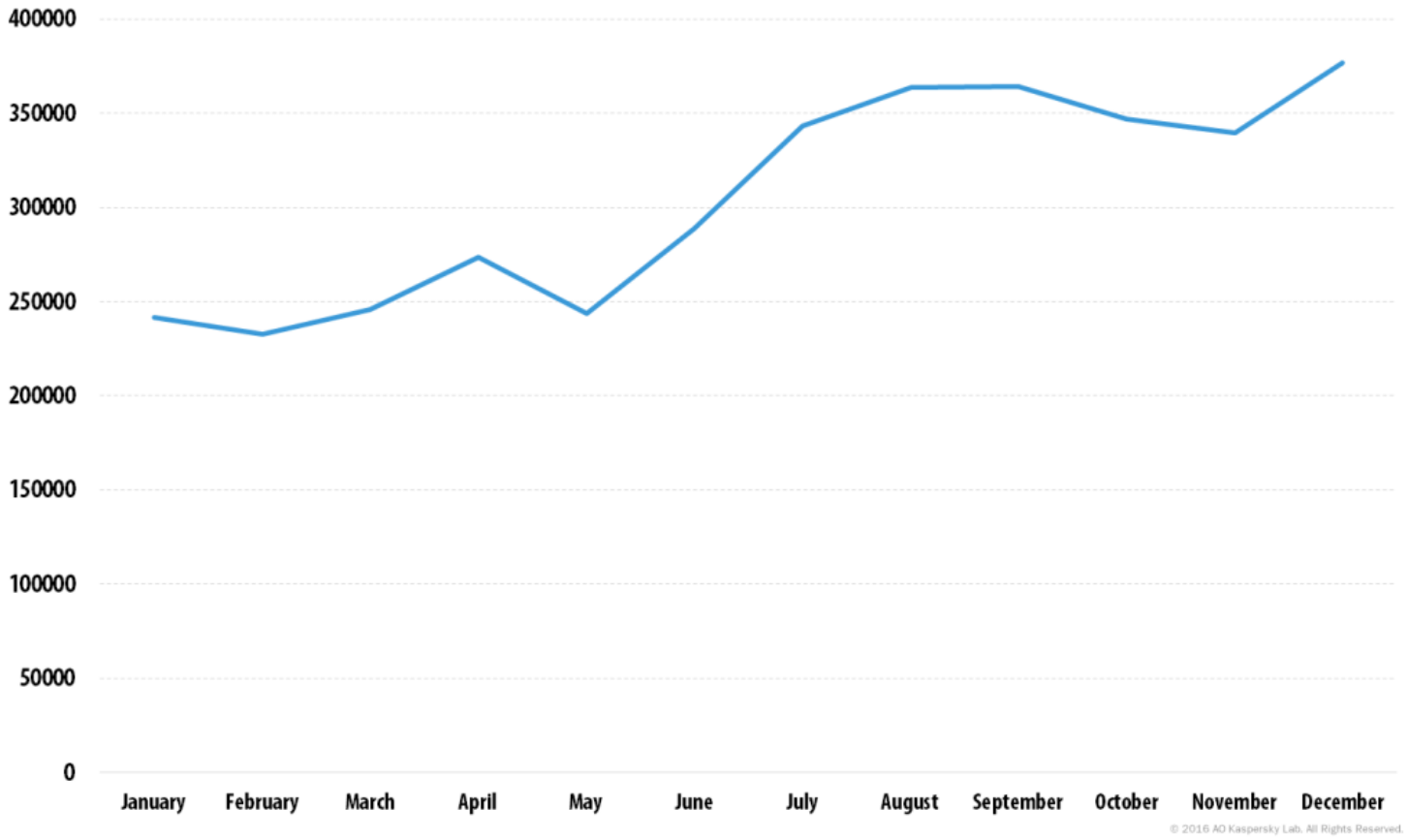
2015年移动恶意代码行为（Kaspasky）

- 2015年,卡巴斯基实验室检测到的内容如下:
  - •2,961,727个恶意安装包
  - •884,774个新的恶意移动项目——数量较前一年增长了三倍.
  - •7,030个移动银行木马

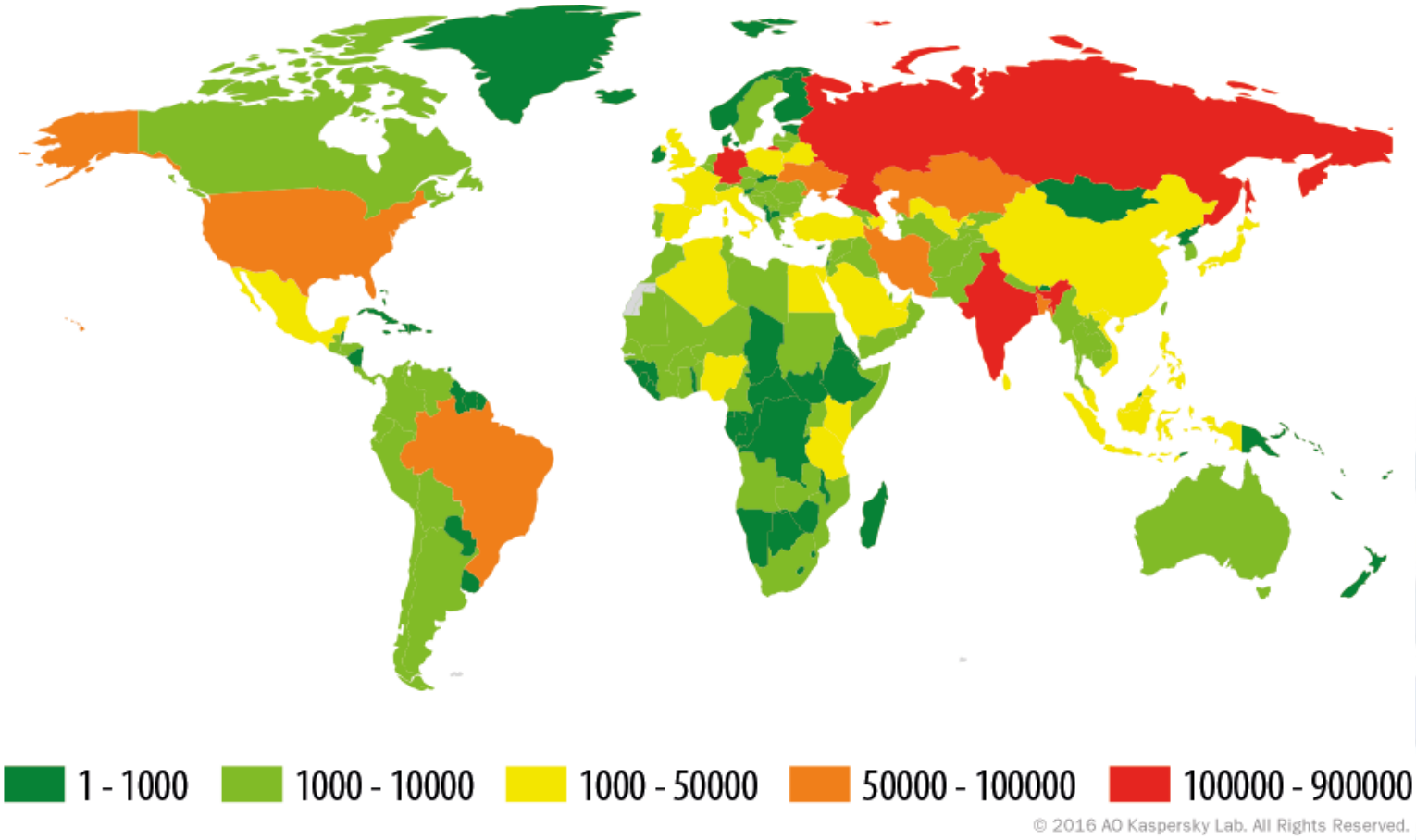
The number of attacks blocked by Kaspersky Lab solutions, 2015



The number of users protected by Kaspersky Lab solutions, 2015



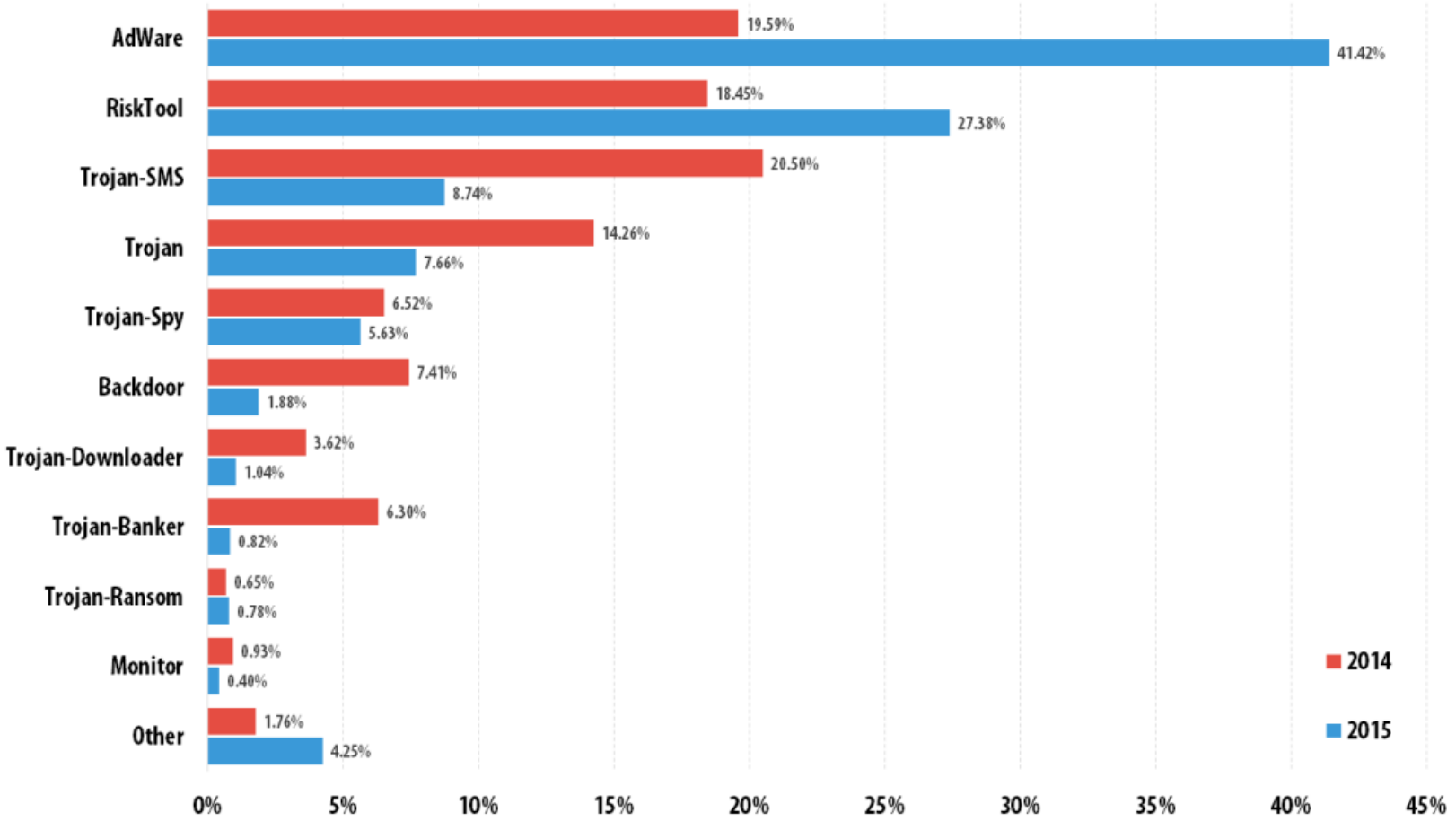
The geography of mobile threats by number of attacked users, 2015



TOP 10 countries by the percentage of attacked users

	Country	% of attacked users*
1	China	37
2	Nigeria	37
3	Syria	26
4	Malaysia	24
5	Ivory Coast	23
6	Vietnam	22
7	Iran	21
8	Russia	21
9	Indonesia	19
10	Ukraine	19

Distribution of new mobile malware by type in 2014 and 2015



10、恶意代码新时代——勒索、APT、工控、物联网

1.Conficker

- Conficker是一种针对微软的Windows操作系统的计算机蠕虫病毒，最早的版本出现在2008年秋季。

2.Sality

- 通过僵尸网络控制

3.Locky

- Locky是勒索软件家族新成员，出现于2016年年初，通过RSA-2048和AES-128算法对100多种文件类型进行加密。Locky通过漏洞工具包或包含JS、WSF、HTA或LNK文件的电子邮件传播。

4.Cutwail

- 一款僵尸网络，用于DDoS攻击并发送垃圾邮件。

- **5.Zeus**
  - Zeus是几年前出现的一款银行木马。
- **6.Chanitor**
  - 被称为Hancitor或H1N1,使用垃圾邮件来传播木马。
- **7.Tinba – 木马**
- **8.Cryptowall**
  - Cryptowall是CryptoLocker勒索软件的变种。
- **9.Blackhole - 一种恶意程序工具包,**
- **10.Nivdort - 模块化木马。**

2018十大恶意软件

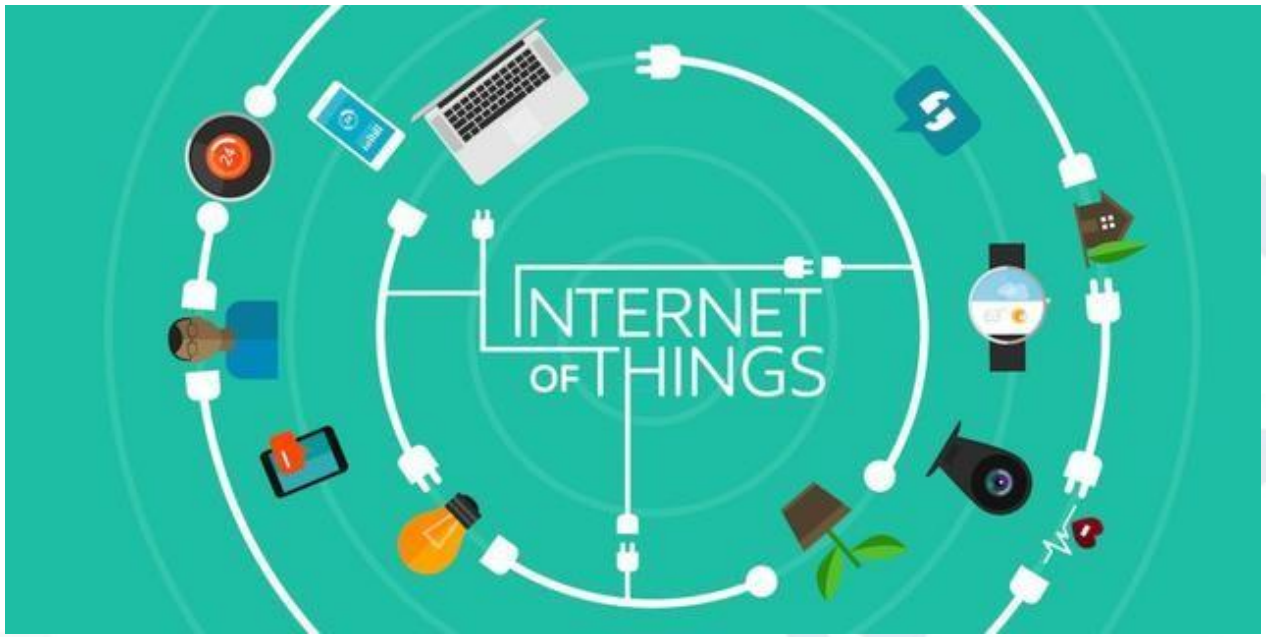
- APT武器：**持续升级的APT28工具系列**
  - **白俄罗斯**
- 工控系统：继Stuxnet之后最大威胁的Industroyer
  - 能够直接控制变电中的电路开关和继电器
- **物联网：持续“扩张”的Mirai家族**
  - 2017年与Mirai相关的知名恶意软件包括：Rowdy、IoTroops、Satori等。这些恶意软件以mirai的源代码为本体，经过不断的变异改进，已经从传统的Linux平台演变到了Windows平台，利用的端口也在不断变化，从传统的弱口令攻击转变到了弱口令和漏洞利用的综合攻击方式，同时感染设备范围由网络摄像机、家庭路由，正向有线电视机顶盒等领域“扩张”。

- **银行/金融：在线销售的CutletMaker**
  - CutletMaker的软件于2017年5月开始在AlphaBay暗网市场上销售，因为美国有关机构在7月中旬关闭了AlphaBay，软件经营方现新建了一个独立网站专门销售该软件。
- **犯罪勒索：占领半壁江山的WannaCry**
- **移动终端：安卓终端排名第一的Rootnik**
- **劫持与广告：造成史上最大规模感染的FireBall**
  - FireBall可以控制互联网浏览器, 监视受害者的 web 使用, 并可能窃取个人文件。FireBall 与拥有3亿客户声称提供数字营销和游戏应用程序的中国公司Rafotech（卿烨科技http://www.rafotech.com/）相关。

- **Windows & office：被滥用的NSA工具DoublePulsar**
- **恶意邮件：造成30亿美元损失的尼日利亚钓鱼**
- **无文件/脚本恶意软件：被用于挖矿的NSA 漏洞利用工具Zealot**
  - 利用 NSA 漏洞大量入侵 Linux 和Windows 服务器同时植入恶意软件“ Zealot ”来挖掘 Monero 加密货币的攻击

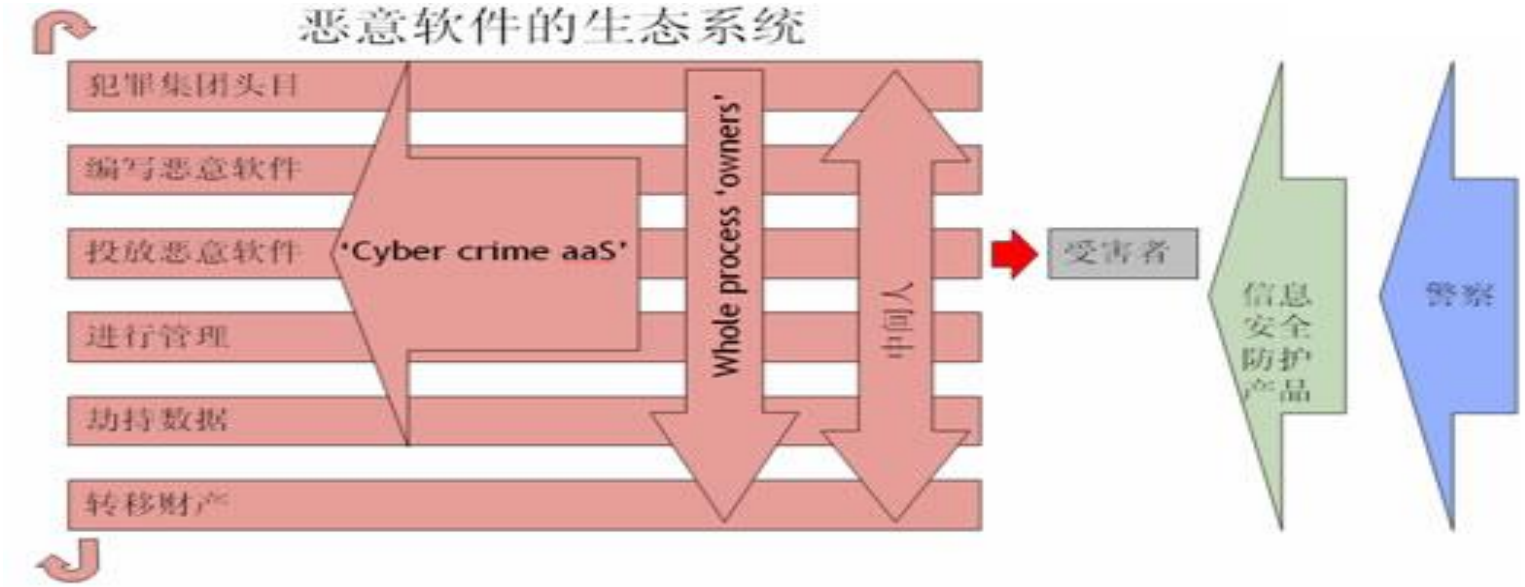
2019年的新趋势

- 勒索软件的规模正在增长。
- 基于物联网平台的僵尸网络-〉DDOS攻击



总体趋势总结

- 网络化发展　专业化发展　简单化发展
- 多样化发展　自动化发展　犯罪化发展



四、病毒人生（法律）

- 1983 年 11 月 3 日，弗雷德·科恩 (Fred Cohen) 博士研制出一种在运行过程中可以复制自身的破坏性程序，伦·艾德勒曼 (Len Adleman) 将它命名为计算机病毒(computer viruses)，并在每周一次的计算机安全讨论会上正式提出。

- 1988年冬天，正在康乃尔大学攻读的莫里斯，把一个被称为“蠕虫”的电脑病毒送进了美国最大的电脑网络——互联网。1988年11月2日下午5点，互联网的管理人员首次发现网络有不明入侵者。当晚，从美国东海岸到西海岸，互联网用户陷入一片恐慌。

- CIH病毒，又名“切尔诺贝利”，是一种可怕的电脑病毒。它是由台湾大学生陈盈豪编制的，九八年五月间，陈盈豪还在大同工学院就读时，完成以他的英文名字缩写“CIH”名的电脑病毒起初据称只是为了“想纪念一下1986的灾难”或“使反病毒软件公司难堪”。

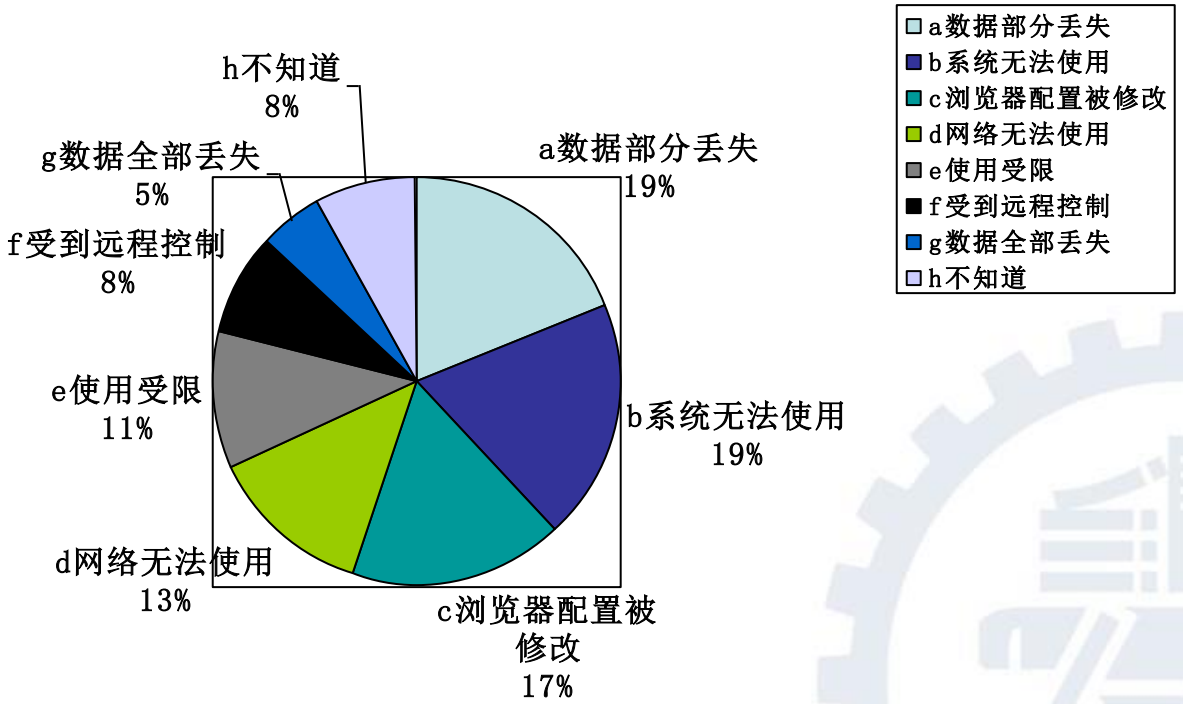
- 年仅18岁的高中生杰弗里·李·帕森因为涉嫌是“冲击波”电脑病毒的制造者于2003年8月29日被捕。对此，他的邻居们表示不敢相信。在他们的眼里，杰弗里·李·帕森是一个电脑天才，而决不是什么黑客，更不会去犯罪。

- 李俊，大学本科毕业
  - 大于1000万用户染毒
  - 损失数亿元人民币
  - 处罚：最高无期？

五、恶意代码的主要危害

- 直接危害：
- 1.病毒激发对计算机数据信息的直接破坏作用
- 2.占用磁盘空间和对信息的破坏
- 3.抢占系统资源
- 4.影响计算机运行速度
- 5.计算机病毒错误与不可预见的危害
- 6.计算机病毒的兼容性对系统运行的影响

病毒的危害情况


h不知道
8%
a数据部分丢失
19%
g数据全部丢失
5%
f受到远程控制
8%
e使用受限
11%
b系统无法使用
19%
d网络无法使用
13%
c浏览器配置被修改
17%
a数据部分丢失
b系统无法使用
c浏览器配置被修改
d网络无法使用
e使用受限
f受到远程控制
g数据全部丢失
h不知道

- 间接危害：
  - 1.计算机病毒给用户造成严重的心理压力
  - 2.造成业务上的损失
  - 3.法律上的问题

近几年来的重大损失

年　份	攻击行为发起者	受害PC数目	损失金额 (美元)
2006	木马和恶意软件	——	——
2005	木马	——	——
2004	Worm_Sasser (震荡波)	——	——
2003	Worm_MSBLAST (冲击波)	超过140万台	——
2003	SQL Slammer	超过20万台	9.5亿至12亿
2002	Klez	超过6百万台	90亿
2001	RedCode	超过1百万台	26亿
2001	NIMDA	超过8百万台	60亿
2000	Love Letter	——	88亿
1999	CIH	超过6千万台	近100亿

清华大学出版社
TSINGHUA UNIVERSITY PRESS

重点大学信息安全专业规划系列教材

恶意代码与计算机病毒
——原理、技术和实践

六、恶意代码的分类

总体上分两大类

- 第一大类：传统的计算机病毒
  - 感染操作系统引导程序
  - 感染可执行文件（感染exe、com、elf文件）
  - 感染数据文件（宏病毒、Shell脚本恶意代码）
- 第二大类：传统计算机病毒之外的恶意代码
  - 木马、蠕虫、流氓软件……
  - 后门、僵尸、移动端恶意代码……

清华大学出版社
TSINGHUA UNIVERSITY PRESS

重点大学信息安全专业规划系列教材

恶意代码与计算机病毒
——原理、技术和实践

七、计算机病毒的传播途径

1、软盘

- 软盘作为最常用的交换媒介，在计算机应用的早期对病毒的传播发挥了巨大的作用，因那时计算机应用比较简单，可执行文件和数据文件系统都较小，许多执行文件均通过软盘相互拷贝、安装，这样病毒就能通过软盘传播文件型病毒；另外，在软盘列目录或引导机器时，引导区病毒会在软盘与硬盘引导区内互相感染。因此软盘也成了计算机病毒的主要的寄生“温床”。

2、光盘

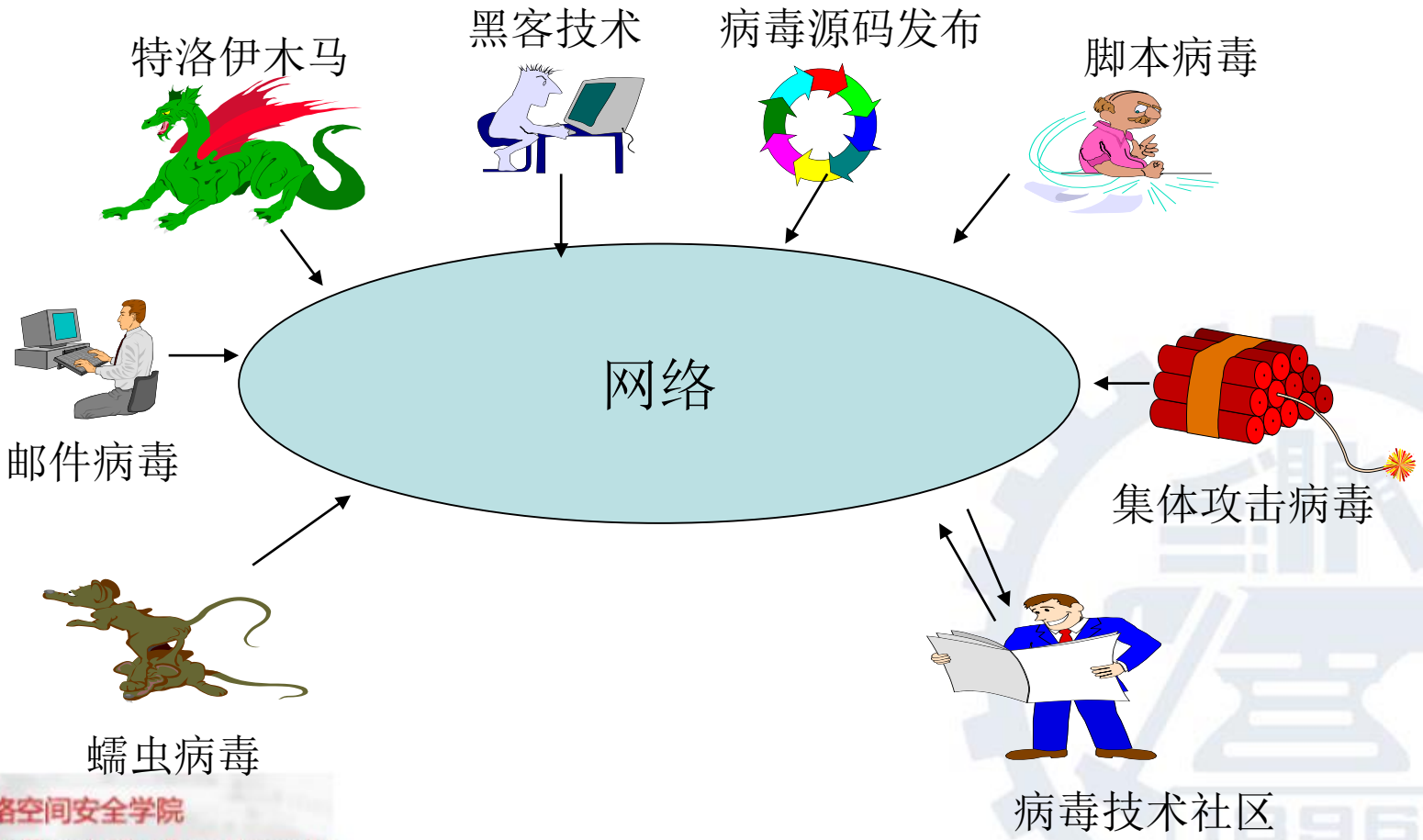
- 光盘因为容量大，存储了大量的可执行文件，大量的病毒就有可能藏身于光盘，对只读式光盘，不能进行写操作，因此光盘上的病毒不能清除。以谋利为目的非法盗版软件的制作过程中，不可能为病毒防护担负专门责任，也决不会有真正可靠的技术保障避免病毒的传入、传染、流行和扩散。当前，盗版光盘的泛滥给病毒的传播带来了极大的便利。甚至有些光盘上杀病毒软件本身就带有病毒，这就给本来“干净”的计算机带来了灾难。

3、硬盘（含移动硬盘、USB）

- 有时，带病毒的硬盘在本地或移到其他地方使用甚至维修等，就会将干净的软盘传染或者感染其他硬盘并扩散。

4、有线网络

网络——〉病毒的加速器



触目惊心的计算——卿斯汉

- 如果：
- 20分钟产生一种新病毒，通过因特网传播（30万公里/秒）。联网电脑每20分钟感染一次，每天开机联网2小时。
- 结论：
- 一年以内一台联网的电脑可能会被最新 病毒感染2190次。
- 另一个数字：
- 75%的电脑被感染。

网络服务——〉传播媒介

- 网络的快速发展促进了以网络为媒介的各种服务（FTP, WWW, BBS, EMAIL等）的快速普及。同时，这些服务也成为了新的病毒传播方式。
- **电子布告栏（BBS）：**
- **电子邮件（Email）：**
- **即时消息服务（QQ, ICQ, MSN等）：**
- **WEB服务：**
- **FTP服务：**
- **新闻组：**

5、无线通讯系统

- 病毒对手机的攻击有3个层次：攻击WAP服务器，使手机无法访问服务器；攻击网关，向手机用户发送大量垃圾信息；直接对手机本身进行攻击，有针对性地对其操作系统和运行程序进行攻击，使手机无法提供服务。

八、染毒计算机的症状

病毒表现现象：

计算机病毒发作前的表现现象

病毒发作时的表现现象

病毒发作后的表现现象

与病毒现象相似的硬件故障

与病毒现象相似的软件故障

1、发作前的现象

- 平时运行正常的计算机突然经常性无缘无故地死机
- 操作系统无法正常启动
- 运行速度明显变慢
- 以前能正常运行的软件经常发生内存不足的错误
- 打印和通讯发生异常
- 以前能正常运行的应用程序经常发生死机或者非法错误
- 系统文件的时间、日期、大小发生变化
- 运行Word，打开Word文档后，该文件另存时只能以模板方式保存
- 磁盘空间迅速减少
- 网络驱动器卷或共享目录无法调用
- 基本内存发生变化
- 陌生人发来的电子邮件

2、发作时的现象

- 提示一些不相干的话
- 发出一段的音乐
- 产生特定的图像
- 硬盘灯不断闪烁
- 进行游戏算法
- Windows桌面图标发生变化
- 计算机突然死机或重启
- 自动发送电子邮件
- 鼠标自己在动

3、发作后的现象

- 硬盘无法启动，数据丢失
- 系统文件丢失或被破坏
- 文件目录发生混乱
- 部分文档丢失或被破坏
- 部分文档自动加密
- 修改系统文件
- 使部分可软件升级主板的BIOS程序混乱，主板被破坏
- 网络瘫痪，无法提供正常的服务

4、与病毒现象类似的软件故障

- 出现“Invalid drive specification”(非法驱动器号)
- 软件程序已被破坏(非病毒)
- 软件与操作系统的兼容性
- 引导过程故障
- 用不同的编辑软件程序

重点大学信息安全专业规划系列教材
恶意代码与计算机病毒
——原理、技术和实践

5、与病毒现象类似的硬件故障

- 系统的硬件配置
- 电源电压不稳定
- 插件接触不良
- 软驱故障
- 关于CMOS的问题

九、计算机病毒的命名规则

CARO命名规则，每一种病毒的命名包括五个部分：

- 病毒家族名
- 病毒组名
- 大变种
- 小变种
- 修改者

CARO规则的一些附加规则包括：

- 不用地点命名
- 不用公司或商标命名
- 如果已经有了名字就不再另起别名
- 变种病毒是原病毒的子类

精灵（Cunning）病毒是瀑布（Cascade）病毒的变种，它在发作时能奏乐，因此被命名为Cascade.1701.A。Cascade是家族名，1701是组名。因为Cascade病毒的变种的大小不一（1701, 1704, 1621等），所以用大小来表示组名。A 表示该病毒是某个组中的第一个变种。

业界补充：

反病毒软件商们通常在CARO命名的前面加一个前缀来标明病毒类型。比如，WM表示MS Word宏病毒；Win32指32位Windows病毒；VBS指VB脚本病毒。这样，梅丽莎病毒的一个变种的命名就成了W97M.Melissa.AA，Happy 99蠕虫就被称为Win32.Happy99.Worm。

- VGrep是反病毒厂商的一种尝试，这种方法将已知的病毒名称通过某种方法关联起来，其目的是不管什么样的扫描软件都能按照可被识别的名称链进行扫描。VGrep将病毒文件读入并用不同的扫描器进行扫描，扫描的结果和被识别出的信息放入数据库中。每一个扫描器的扫描结果与别的扫描结果相比较并将结果用作病毒名交叉引用表。VGrep的参与者赞同为每一种病毒起一个最通用的名字最为代表名字。拥有成千上万扫描器的大型企业集团要求杀毒软件供应商使用VGrep命名，这对于在世界范围内跟踪多个病毒的一致性很有帮助。

清华大学出版社
TSINGHUA UNIVERSITY PRESS

重点大学信息安全专业规划系列教材

恶意代码与计算机病毒
——原理、技术和实践

十、计算机病毒防治

病毒防治的公理

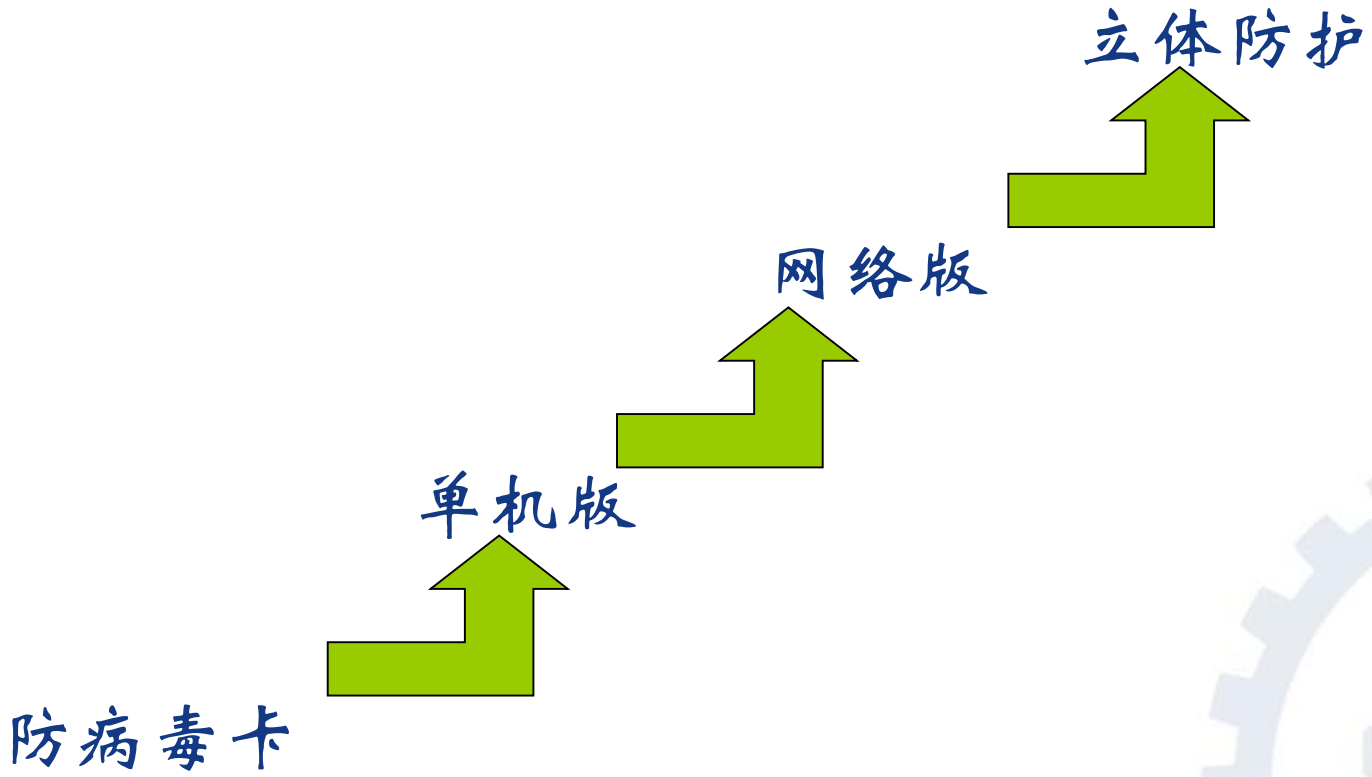
1、不存在这样一种反病毒软硬件，能够防治未来产生的所有病毒。

2、不存在这样一种病毒程序，能够让未来的所有反病毒软硬件都无法检测。

3、目前的反病毒软件和硬件以及安全产品是都易耗品，必须经常进行更新、升级。

4、病毒产生在前，反病毒手段滞后的现状，将是一个长期的过程。

人类为防治病毒所做出的努力



对计算机病毒应持有的态度

1.客观承认计算机病毒的存在，但不要惧怕病毒。

3.树立计算机病毒意识，积极采取预防（备份等）措施。

4.掌握必要的计算机病毒知识和病毒防治技术，对用户至关重要。

5.发现病毒，冷静处理。

目前广泛应用的几种防治技术：

➢特征码扫描法

特征码扫描法是分析出病毒的特征病毒码并集中存放于病毒代码库文件中，在扫描时将扫描对象与特征代码库比较，如有吻合则判断为染上病毒。该技术实现简单有效，安全彻底；但查杀病毒滞后，并且庞大的特征码库会造成查毒速度下降；

➢虚拟执行技术

该技术通过虚拟执行方法查杀病毒，可以对付加密、变形、异型及病毒生产机生产的病毒，具有如下特点：

- 在查杀病毒时在机器虚拟内存中模拟出一个“指令执行虚拟机器”
- 在虚拟机环境中虚拟执行（不会被实际执行）可疑带毒文件
- 在执行过程中，从虚拟机环境内截获文件数据，如果含有可疑病毒代码，则杀毒后将其还原到原文件中，从而实现对各类可执行文件内病毒的查杀

➢智能引擎技术

智能引擎技术发展了特征码扫描法的优点，改进了其弊端，使得病毒扫描速度不随病毒库的增大而减慢。刚刚面世的瑞星杀毒软件2003版即采用了此项技术，使病毒扫描速度比2002版提高了一倍之多；

➢计算机监控技术

- 文件实时监控
- 内存实时监控
- 脚本实时监控
- 邮件实时监控
- 注册表实时监控
- 参考：www.sysinternals.com

➢未知病毒查杀技术

未知病毒技术是继虚拟执行技术后的又一大技术突破，它结合了虚拟技术和人工智能技术，实现了对未知病毒的准确查杀。

➢压缩智能还原技术

世界上的压缩工具、打包工具、加“壳”工具多不胜数，病毒如果被这样的工具处理后被层层包裹起来，对于防病毒软件来说，就是一个噩梦。为了使用统一的方法来解决这个问题，反病毒专家们发明了未知解压技术，它可以对所有的这类文件在内存中还原，从而使得病毒完全暴露出来。

➢多层防御，集中管理技术

反病毒要以网为本，从网络系统的角度设计反病毒解决方案，只有这样才能有效地查杀网络上的计算机病毒。

在网络上，软件的安装和管理方式是十分关键的，它不仅关系到网络维护和管理的效率和质量，而且涉及到网络的安全性。好的杀毒软件需要能在几分钟之内便可轻松地安装到组织里的每一个NT服务器上，并可下载和散布到所有的目的机器上，由网络管理员集中设置和管理，它会与操作系统及其它安全措施紧密地结合在一起，成为网络安全管理的一部分，并且自动提供最佳的网络病毒防御措施。

➢病毒免疫技术

病毒免疫技术一直是反病毒专家研究的热点，它通过加强自主访问控制和设置磁盘禁写保护区来实现病毒免疫的基本构想。实际上，最近出现的软件安全认证技术也应属于此技术的范畴，由于用户应用软件的多样性和环境的复杂性，病毒免疫技术到广泛使用还有一段距离。

病毒防治技术的趋势前瞻

➢ 加强对未知病毒的查杀能力

加强对未知病毒的查杀能力是反病毒行业的持久课题，目前国内外多家公司都宣布自己的产品可以对未知病毒进行查杀，但据我们研究，国内外的产品只有少数可以对同一家族的新病毒进行预警，不能清除。

目前有些公司已经在这一领域取得了突破性的进展，可以对未知DOS病毒、未知PE病毒、未知宏病毒进行防范。其中对未知DOS病毒能查到90%以上，并能准确清除其中的80%，未知PE病毒能查到70%以上、未知宏病毒能实现查杀90%.

- 防杀针对掌上型移动通讯工具和PDA的病毒

随着掌上型移动通讯工具和PDA的广泛使用，针对这类系统的病毒已经开始出现，并且威胁将会越来越大，反病毒公司将投入更多的力量来加强此类病毒的防范。

➢兼容性病毒的防杀

目前已经发现可以同时在微软WINDOWS和日益普及的LINUX两种不同操作系统内运作的病毒，此类病毒将会给人们带来更多的麻烦，促使反病毒公司加强防杀此类病毒。

➢蠕虫病毒和脚本病毒的防杀不容忽视

蠕虫病毒是一种能自我复制的程序，驻留内存并通过计算机网络复制自己，它通过大量消耗系统资源，最后导致系统瘫痪。给人们带来了巨大的危害，脚本病毒因为其编写相对容易正成为另一种趋势，这两类病毒的危害性使人们丝毫不能忽视对其的防杀。

清华大学出版社
TSINGHUA UNIVERSITY PRESS

重点大学信息安全专业规划系列教材

恶意代码与计算机病毒
——原理、技术和实践

十一、杀毒软件及评价

上海交通大学 网络空间安全学院
School Of Cyber Security,ShanghaiJiao Tong University

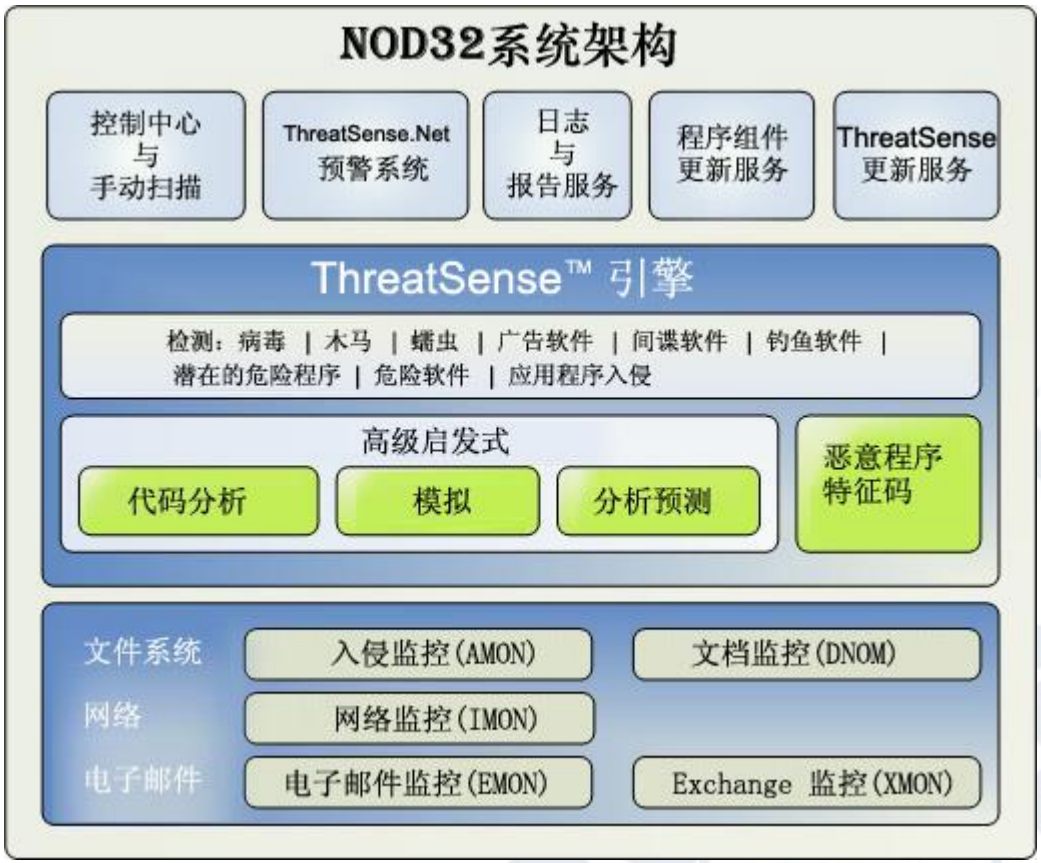
（一）杀毒软件必备功能

- 病毒查杀能力
- 对新病毒的反应能力
- 对文件的备份和恢复能力
- 实时监控功能
- 及时有效的升级功能
- 智能安装、远程识别功能
- 界面友好、易于操作
- 对现有资源的占用情况

- 系统兼容性
- 软件的价格
- 软件商的实力

（二）国内外杀毒软件及市场

- 金山毒霸、瑞星杀毒、KV3000、PC-Cillin VirusBuster、Norton AntiVirus、Mcafee Virus Scan、Kaspersky Antivirus、F-Secure Antivirus,Nod32等。



《电脑报》2008评测结果

软件名称	查杀能力	主动防御能力	自身强壮度	查杀速度	全盘扫描时间	病毒样本包查杀病毒数（个）	查杀未知病毒数量（个）	被病毒攻破	闲时占用系统资源
瑞星	B	B	A	C	18分	3532	8	否	8M
江民	A	A	A	A	4分54秒	3590	10	否	13M
金山	B	C	B	A	8分26秒	3497	3	是	30M
熊猫	B	A	A	A	5分40秒	3512	10	否	75M
趋势	B	A	A	B	12分12秒	3516	10	否	16M
卡巴斯基	A	B	B	C	16分59秒	3516	8	是	15M
NOD32	B	A	A	C	18分06秒	3461	10	否	3M
驱逐舰	C	C	B	A	8分38秒	163	3	是	20M

2014年

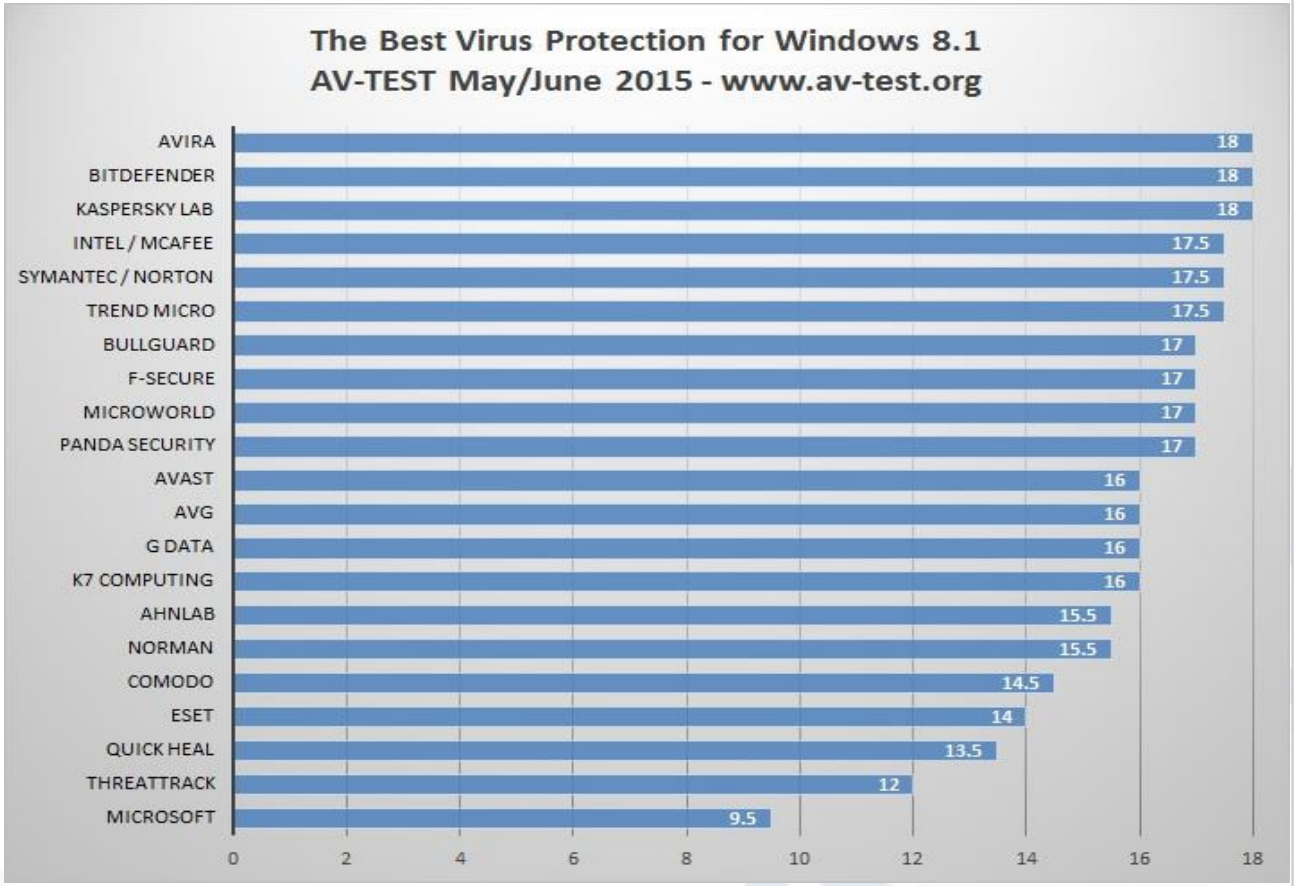

AV-C杀毒软件年终评测排行榜
Trend Micro 7.5
360杀毒 1.5
Bitdefender 0
Kaspersky Lab 0
Avira 4
F-Secure 69.5
Emsisoft 15
ESET 3
Fortinet 13
Panda 46
eScan 31
AVG 0
Avast 5
McAfee 81
腾讯电脑管家 32.5
BullGuard 6
Sophos 4
金山杀毒 19
百度杀毒 5
Lavasoft 0
ThreatTrack Vipre 20
AhnLab 0
杀毒软件 拦截率（越高越好）
误报数（越低越好）
奖项水平

清华大学出版社
TSINGHUA UNIVERSITY PRESS

重点大学信息安全专业规划系列教材

恶意代码与计算机病毒
——原理、技术和实践

2015年



清华大学出版社
TSINGHUA UNIVERSITY PRESS

杀毒软件免费下载 2016排行榜前十名

1 金山新毒霸（悟空）

新毒霸2016悟空拥有全球最先进的云查杀引擎和超强的病毒分析和查杀能力，已实现全新病毒快速鉴别。还拥有30核云查杀引擎，不占用内存，不影响电脑速度。全球首创网购敢赔险，若因病毒木马、欺诈导致网上购物财产损失可获得赔偿。

立即下载

2 360安全卫士

360安全卫士是一款由奇虎公司推出的功能强、效果好、受用户欢迎的上网安全软件。360安全卫士拥有查杀木马、清理恶评插件、保护隐私、修复漏洞、电脑体检、电脑救援、保护隐私等多种功能。

立即下载

3 腾讯电脑管家

腾讯电脑管家（原名QQ电脑管家）是腾讯公司推出的一款免费安全软件，能有效预防和解决计算机上常见的安全风险。拥有云查杀木马，系统加速，漏洞修复，实时防护，网速保护，电脑诊所，QQ账号密码防盗保护及QQ等级加速等功能。

立即下载

4 360杀毒软件

360杀毒软件是360安全中心出品的一款免费的云安全杀毒软件。它创新性地整合了五大领先查杀引擎，包括国际知名的BitDefender病毒查杀引擎、小红伞病毒查杀引擎、360云查杀引擎、360主动防御引擎以及360第二代QVM人工智能引擎，为您带来安全、专业、有效、新颖的查杀防护体验。

立即下载

5 2345安全卫士

2345安全卫士是集电脑体检、木马查杀、垃圾清理、修复系统漏洞、系统加速、软件管理等功能为一体的电脑安全管理的软件，2345安全卫士采用最新的云计算技术以及全新的第三代查杀引擎，5星环绕式系统防护有效查杀各类新型流行木马，占用电脑磁盘空间小，闪电查杀更快更安全。

立即下载

6 百度杀毒软件

最好的免费杀毒软件【百度杀毒软件】是百度公司与计算机反病毒专家卡巴斯基合作出品的全新杀毒软件，集合了百度强大的云端计算反病毒引擎专业能力，一改杀毒软件卡机臃肿的形象，竭力为用户提供轻巧不卡机的产品体验。

立即下载

7 瑞星杀毒软件

瑞星杀毒软件V16是一款以用户体验为产品构架思路，以用户操作和视觉效果为标准的全新安全产品。瑞星V16，分别从用户操作体验提升、查杀与监控功能优化和“自我保护”功能强化等角度，做了37项重大更新。

立即下载

8 卡巴斯基

卡巴斯基反病毒软件获得了独特的知识和技术，使得卡巴斯基成为了病毒防卫的技术领导者和专家。该公司的旗舰产品-著名的卡巴斯基安全软件，主要针对家庭及个人用户，能够彻底保护用户计算机不受各类互联网威胁的侵害。

立即下载

9 诺顿杀毒软件

诺顿杀毒软件是Symantec公司个人信息安全产品之一，亦是一个广泛被应用的反病毒程序。该项产品发展至今，除了原有的防毒外，还有防间谍等网络安全风险的功能，还提供了Norton Rescue Tools来协助使用者清除难以修复的中毒文件。

立即下载

10 小红伞Avira AntiVir

Avira AntiVir是一款由德国的Avira公司所开发的杀毒软件。针对病毒、蠕虫、特洛伊木马、Rootdkit、钓鱼、广告软件和间谍软件等威胁提供保护，并且经受全球超过1亿次的测试和考验。而且Avira AntiVir Personal免费提供。

立即下载

http://www.dnhys.com/

清华大学出版社
TSINGHUA UNIVERSITY PRESS

重点大学信息安全专业规划系列教材

恶意代码与计算机病毒
——原理、技术和实践

BUSINESS WINDOWS CLIENT

The Best Virus Protection for Windows 8.1

AV-TEST
The Independent IT-Security Institute

Manufacturer	Product	AV-TEST-Certificate	Protection (max. 6 pts.)	Performance (max. 6 pts.)	Usability (max. 6 pts.)	Overall Points Total (max. 18 pts.)
AVG	Antivirus Business		6.0	5.5	6.0	17.5
Bitdefender	Endpoint Security		5.5	6.0	5.5	17.0
F-Secure	Client Security		6.0	5.5	4.0	15.5
G Data	Antivirus Business		5.5	5.0	5.0	15.5
Invincea	Enterprise		4.5	6.0	4.0	14.5
Kaspersky Lab	Endpoint Security		6.0	5.5	6.0	17.5
Kaspersky Lab	Small Office Security		6.0	6.0	6.0	18.0
Intel Security	McAfee Endpoint Security		4.5	5.5	6.0	16.0
Microsoft	System Center Endpoint Protection		4.5	5.5	5.5	15.5
Seqrite	Endpoint Security		4.0	5.0	5.0	14.0
Sophos	Endpoint Security and Control		5.0	4.5	6.0	15.5
Symantec	Endpoint Protection		6.0	5.5	6.0	17.5
Trend Micro	Office Scan		5.5	5.5	5.5	16.5

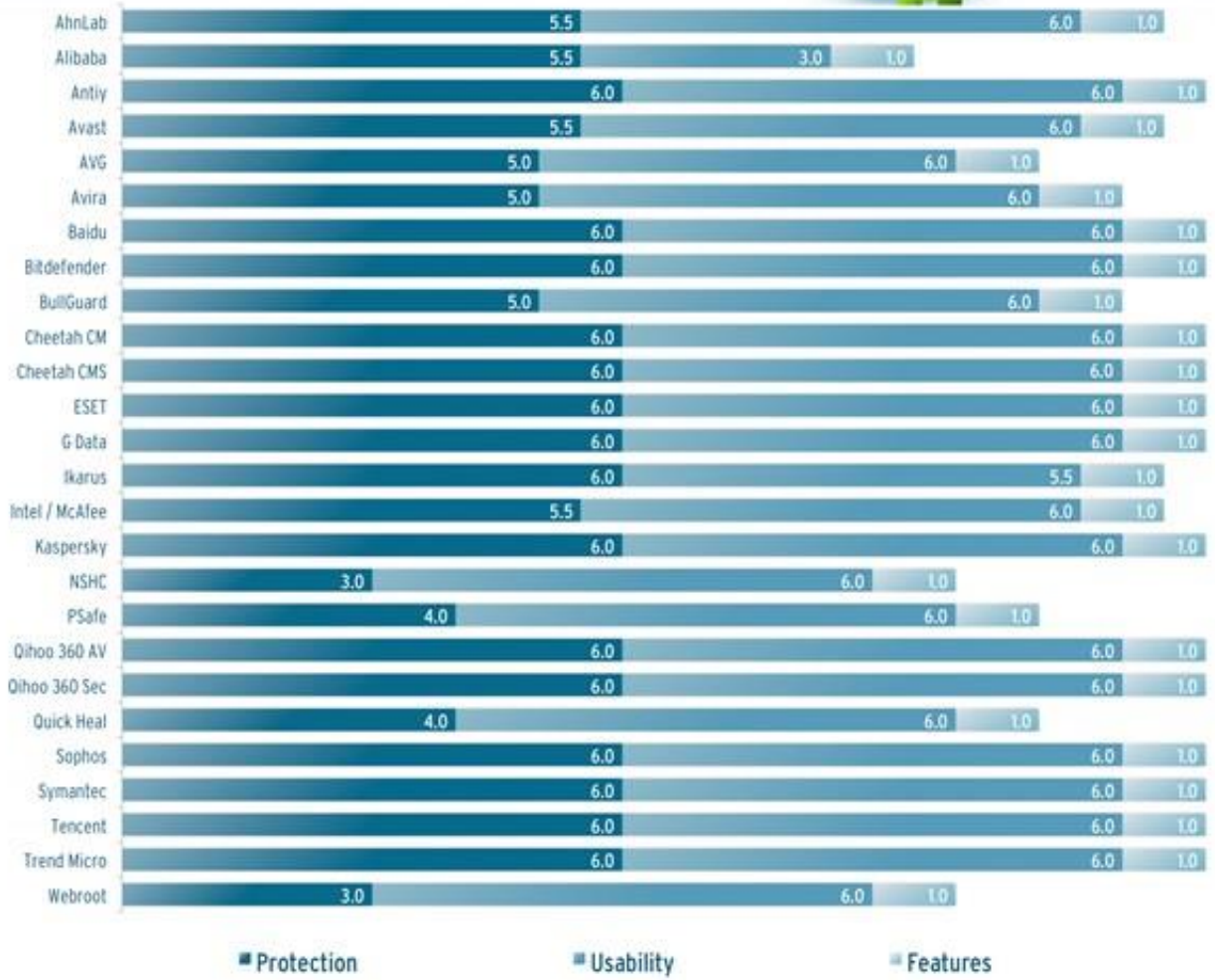
June 2016

Source: https://www.av-test.org

MOBILE DEVICES ANDROID

The Best Virus Protection for Android Mobile Devices

AV-TEST
The Independent IT-Security Institute



June 2016

Source: https://www.av-test.org

清华大学出版社
TSINGHUA UNIVERSITY PRESS

重点大学信息安全专业规划系列教材

恶意代码与计算机病毒
——原理、技术和实践

十二、解决方案和策略

防病毒策略

1、建立病毒防治的规章制度，严格管理；

2、建立病毒防治和应急体系；

3、进行计算机安全教育，提高安全防范意识；

4、对系统进行风险评估；

5、选择经过公安部认证的病毒防治产品；

6、正确配置，使用病毒防治产品；

7、正确配置系统，减少病毒分侵害事件；

8、定期检查敏感文件；

9、适时进行安全评估，调整各种病毒防治策略；

10、建立病毒事故分析制度；

11、确保恢复，减少损失；

清华大学出版社
TSINGHUA UNIVERSITY PRESS

重点大学信息安全专业规划系列教材

十三、国内外病毒产品的技术发展态势

- 国内外反病毒公司在反病毒领域各有所长
- 国内外产品竞争激烈

随着中国信息化进程的深入开展，多家国际反病毒公司基本撤出了在中国的杀毒业务；

- 国内反病毒企业发展势头强劲

国内以360为代表，进入了免费时代

➢反病毒服务是竞争关键

要推动企业信息安全建设、并从根本上改变国内信息安全现状，建立健全的服务体系是关键。

相信人类受到恶意代码侵害及由此带来的损失将逐步减少，国内反病毒行业在政府的规范和用户的支持下将取得更好的成绩！

相关资源

- 1. Wildlist国际组织
  - http://www.wildlist.org
  - 该网站维护世界各地发现的病毒列表。网站负责维护这个列表，并且按月打包供用户下载。此外，网站上还有一些计算机病毒方面的学术论文。
- 2. 病毒公告牌
  - http://www.virusbtn.com
  - 对于任何关心恶意代码和垃圾信息防护、检测和清除的人来说，病毒公告在线杂志是一个必不可少的参考。逐日逐月地，病毒公告牌提供如下信息：
  - 1)来自于反恶意代码业界的发人深省的新闻和观点
  - 2)最新恶意代码威胁的详细分析
  - 3)探索反恶意代码技术开发的长篇文档
  - 4)反恶意代码专家的会见
  - 5)对当前反病毒产品的独立评测
  - 6)覆盖垃圾邮件和反垃圾邮件技术的月报

3. 卡饭论坛

http://bbs.kafan.cn

- 卡饭的意思是卡巴斯基的FANS（爱好者），取其谐音，即为卡饭。卡饭论坛最初是一个以卡巴斯基爱好者为主体，以计算机安全软件为主要内容的论坛。随着国产计算机安全软件的兴起，卡饭论坛对主流的计算机安全软件均有不同程度的涉猎，迄今为止已发展成为最大的计算机安全论坛之一。论坛的开放时间是2006年6月1日。

4. 亚洲反病毒研究者协会(AVAR)

- http://www.aavar.org
- AVAR(亚洲反病毒研究者协会)成立于1998年6月。协会的宗旨是预防计算机病毒的传播和破坏，促进亚洲的反病毒研究者间建立良好的合作关系。

- 5. 国家计算机病毒应急处理中心
- http://www.antivirus-china.org.cn
- 网站主要内容是病毒流行列表、病毒SOS求救、数据恢复等。
- 6. 病毒观察
- http://www.virusview.net
- 网站主要内容包括病毒预报、新闻、评论、相关法规、反病毒资料、安全漏洞、密码知识、病毒百科在线检索等。

7. HACK80

- www.hack80.com
- HACK80是集黑客技术交流、黑客工具分享的黑客论坛。与传统黑客联盟不同，该论坛在守法的前提下提倡自由的技术交流，力求成为一个气氛优秀的技术圈子。

8. 安全焦点

- http://www.xfocus.net
- 安全焦点是中国目前顶级的网络安全站点，那里集聚的一大批知名的黑客。网站内容包括安全论文、安全工具、安全漏洞以及逆向技术等。

9. 看雪论坛

- https://bbs.pediy.com/
- 看雪论坛是致力于PC、移动、物联网安全研究及逆向工程相关的开发者舍却。网站主要内容包括黑客频道、防毒技巧、网络安全新闻和病毒新闻等。

10. 国际计算机安全联合会(ICSA-InterNational Computer Secwrity Association)

- http://www.icsa.com/
- 如要对Internet的安全问题感兴趣,你可以访问国家计算机安全联合会(NCSA)的站点。这里会看到很多关于国家计算机安全联合会各种活动的信息,包括会议,培训、产品认证和安全警告等。在这里你可以了解到国际知名的病毒防治软件登记请况。

Any Questions?

Thank You!