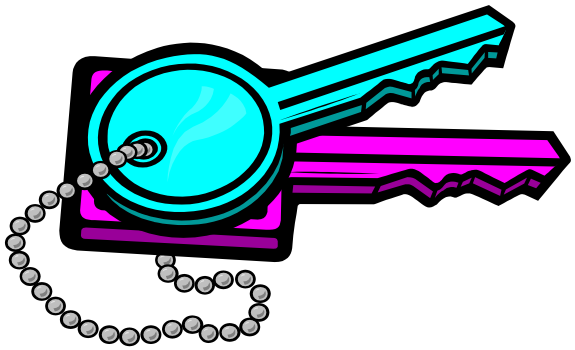
序论

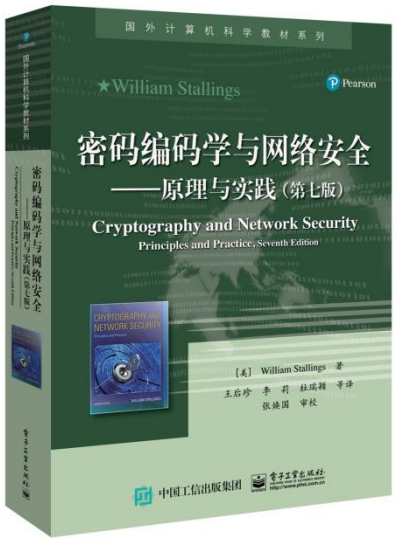


杨帆
2021春

信息安全概论

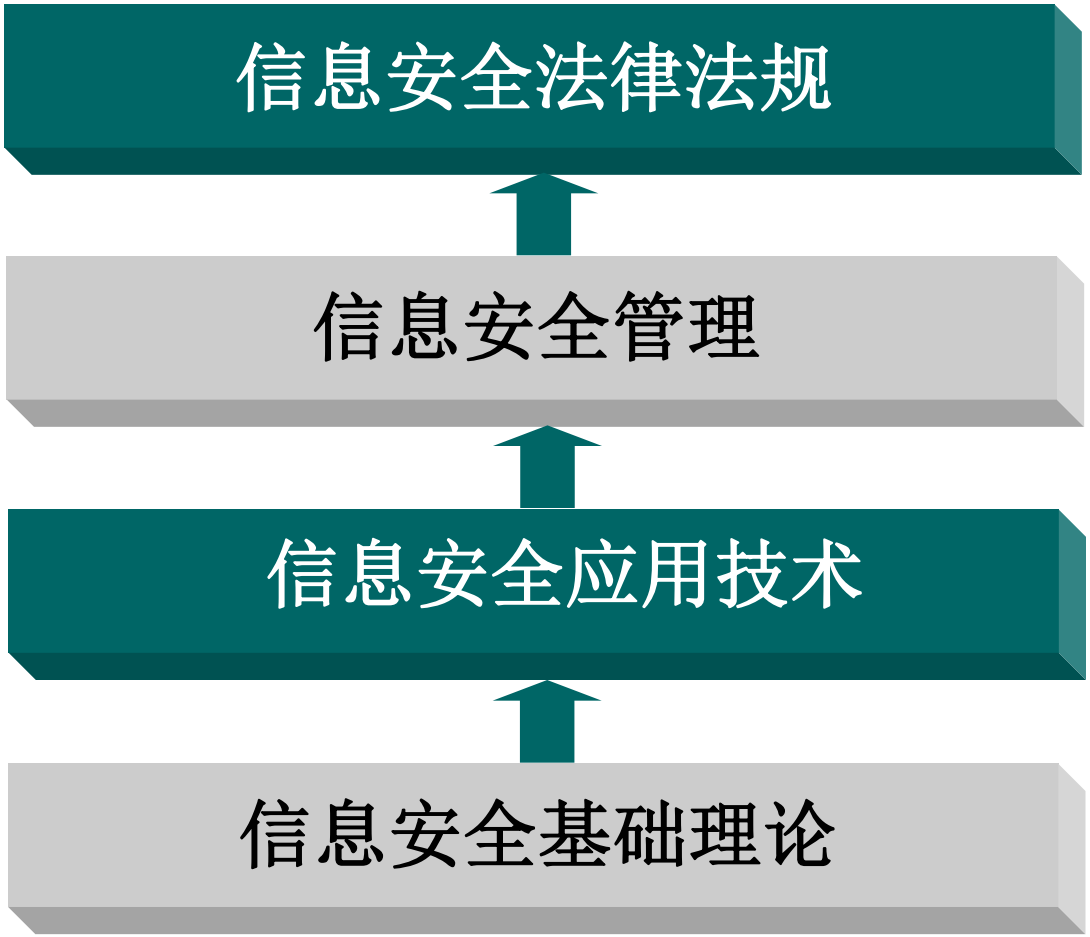
课程信息

- 课程目标
  - 入门课程，介绍基本原理和系统构架
- 课堂时间地点
  - Tues 5-6,未来城公教2-310
  - Wed 5-6,未来城公教2-310
- 教材
  - 《密码编码学与网络安全—原理与实践（第七版）》,电子工业出版社

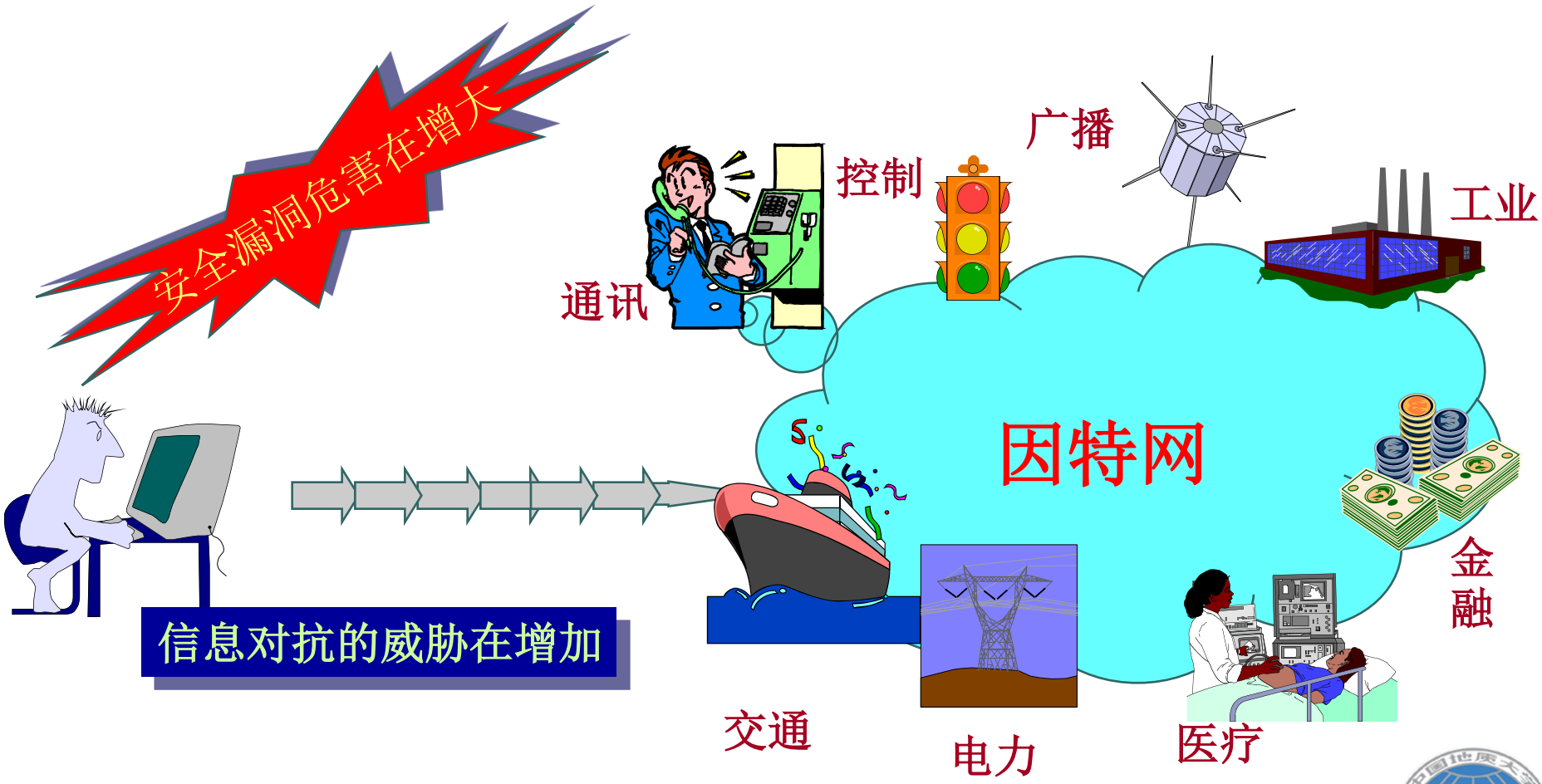


- 参考书
  - 《网络空间安全导论》,刘建伟著,清华大学出版社
  - 《信息安全技术概论》,冯登国著,电子工业出版社
- 评分
  - 考勤30%
  - 考试70%
- 联系方式
  - planesail@163.com

知识构架



信息安全的重要性



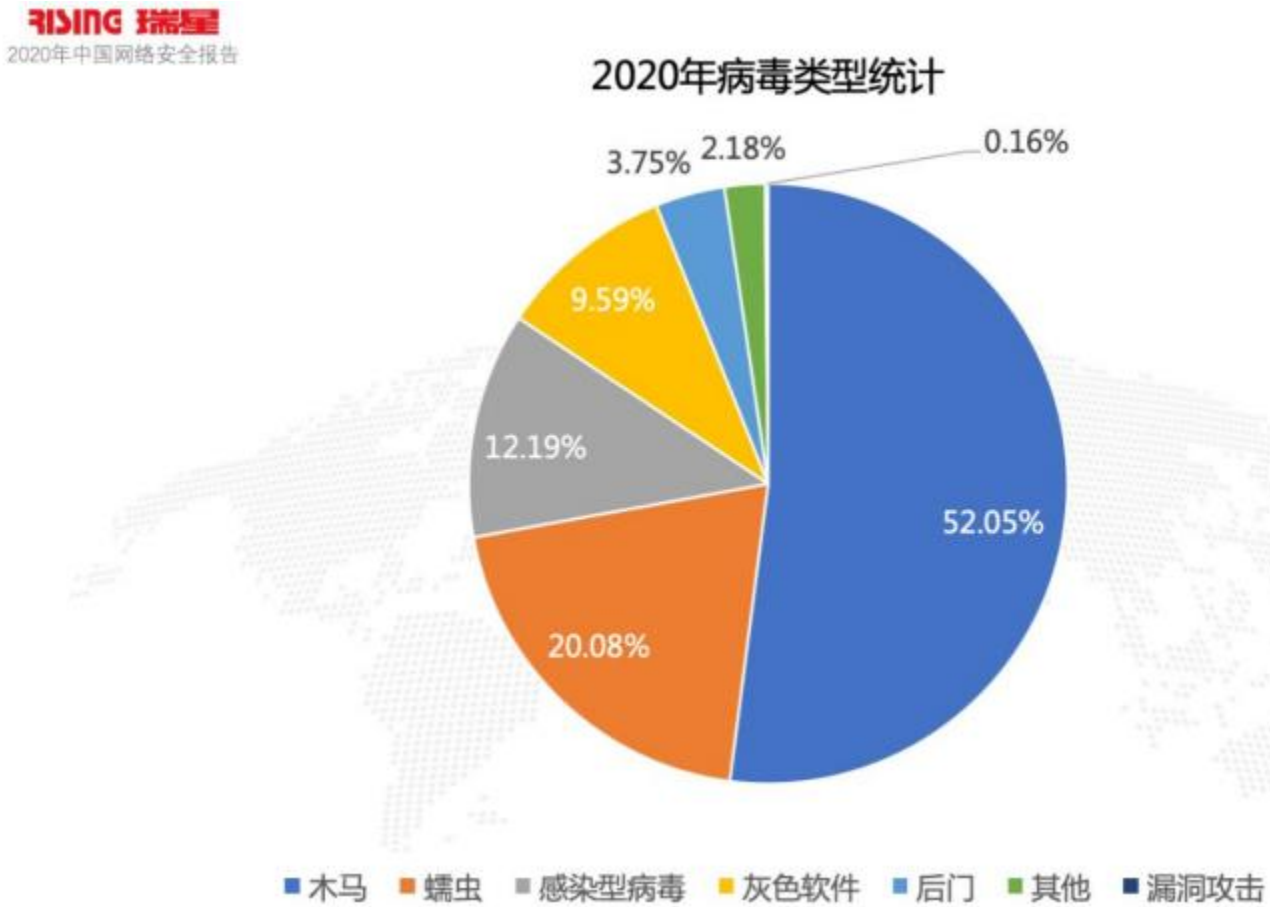
National Strategy国家战略

- 2004年，十六大把信息安全列为国家安全的重要组成部分
- 2009年，胡锦涛在第64届联大强调信息安全的重要性
- 2012年，十八大明确“高度关注海洋、太空、网络空间安全”
- 2014年，习近平任中央网络安全和信息化小组组长，提出“没有网络安全就没有国家安全，没有信息化就没有现代化”
- 2015年，国务院学位委员会决定在“工学”门类下增设“网络空间安全”一级学科
- 2016年12月27日，《国家网络空间安全战略》发布
- 2017年6月1日，施行《网络安全法》，采用网络实名制
- 2019年中美贸易战，国家制定“自主可控”的战略思想，推广国产操作系统、数据库和办公软件等基础软件
- 2020年1月1日，《中华人民共和国密码法》正式实施
- 2020年，《数据安全法》和《个人信息保护法》进入立法程序

2020年中国网络安全报告

1. 恶意软件

共截获病毒样本总量1.48亿个，病毒总体数量比2019年同期上涨43.71%。



2020年中国网络安全报告(续)

RISING 瑞星
2020年中国网络安全报告

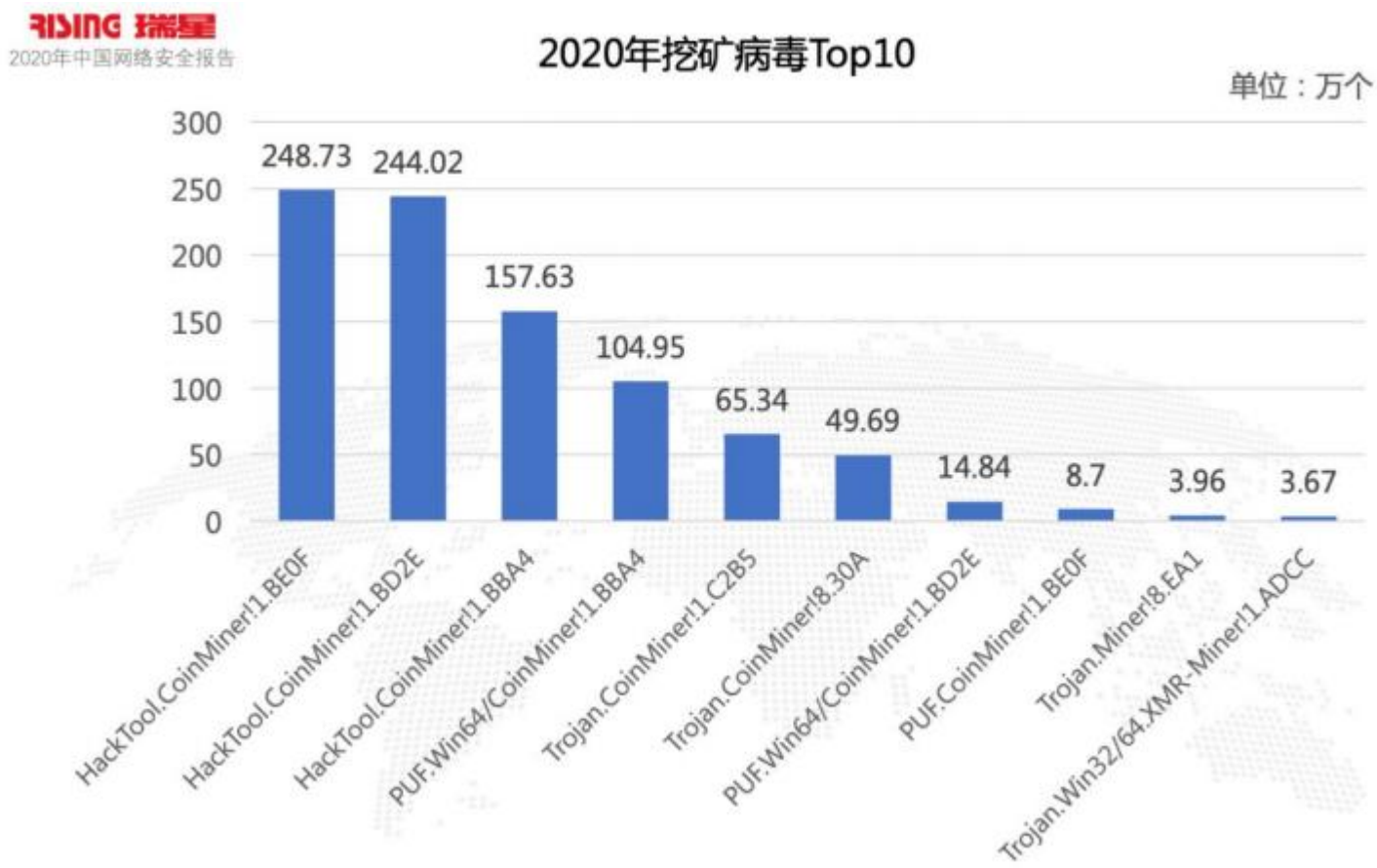
2020年病毒Top10

排名	病毒家族	描述
1	Adware.AdPop	流氓软件使用的弹窗模块
2	Trojan.ShadowBrokers	ShadowBrokers入侵了NSA的方程式小组，窃取了黑客工具包并免费发布，被病毒广泛使用以进行蠕虫传播
3	Trojan.Vools	利用永恒之蓝漏洞传播，攻击局域网中的计算机，传播挖矿木马
4	Adware.Downloader	各种高速下载器，后台恶意推广流氓软件
5	Trojan.Inject	恶意Crypter打包程序，常用来保护后门、木马、间谍软件，达到逃避安全软件检测目的
6	Trojan.Win32/64.XMR-Miner	挖矿木马，利用用户机器计算资源挖取数字货币
7	Worm.Ramnit	Ramnit感染型，感染用户PE文件和网页文件
8	Worm.VobfusEx	利用U盘传播的蠕虫病毒
9	Ransom.FileCryptor	勒索软件，加密用户的文件数据，勒索赎金
10	Backdoor.Agent	后门程序，使受害机器沦为肉鸡，窃取用户隐私数据

2020年中国网络安全报告(续)

2020年中国网络安全报告(续)

共截获勒索软件样本共156万个；挖矿病毒样本总体数量为922万个，同比上涨332.32%。



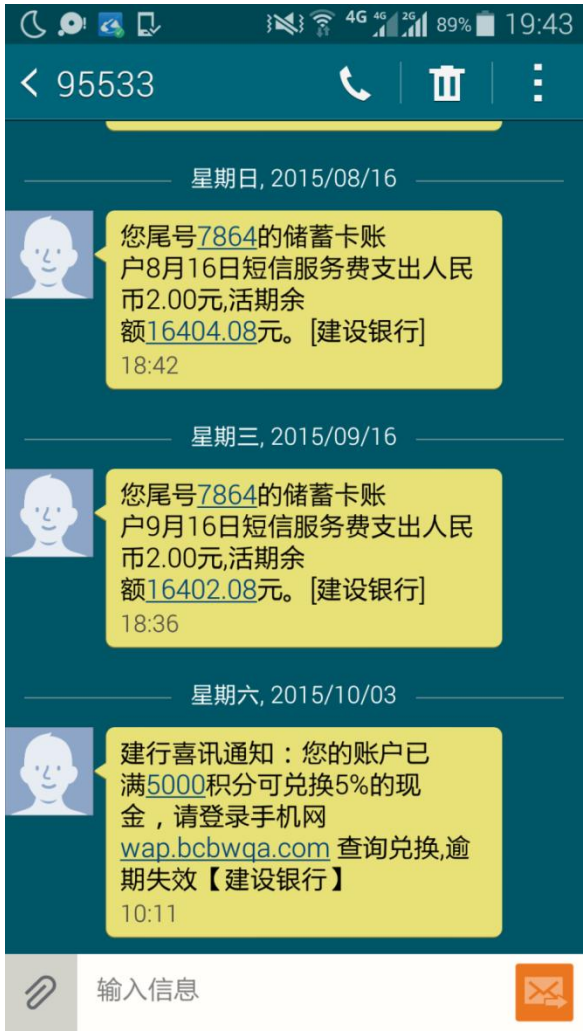
2020年中国网络安全报告(续)

2. 恶意网址

全球共截获恶意网址（URL）总量6693万个，其中挂马类网站4305万个，钓鱼类网站2388万个。

2020年中国网络安全报告(续)

2020年中国网络安全报告(续)



伪基站攻击

手机钓鱼网站

2020年中国网络安全报告(续)

3. 手机安全

共截获手机病毒样本581万个，病毒总体数量比2019年同期上升69.02%。

2020年中国网络安全报告(续)

RISING 瑞星
2020年中国网络安全报告

2020年手机病毒Top5

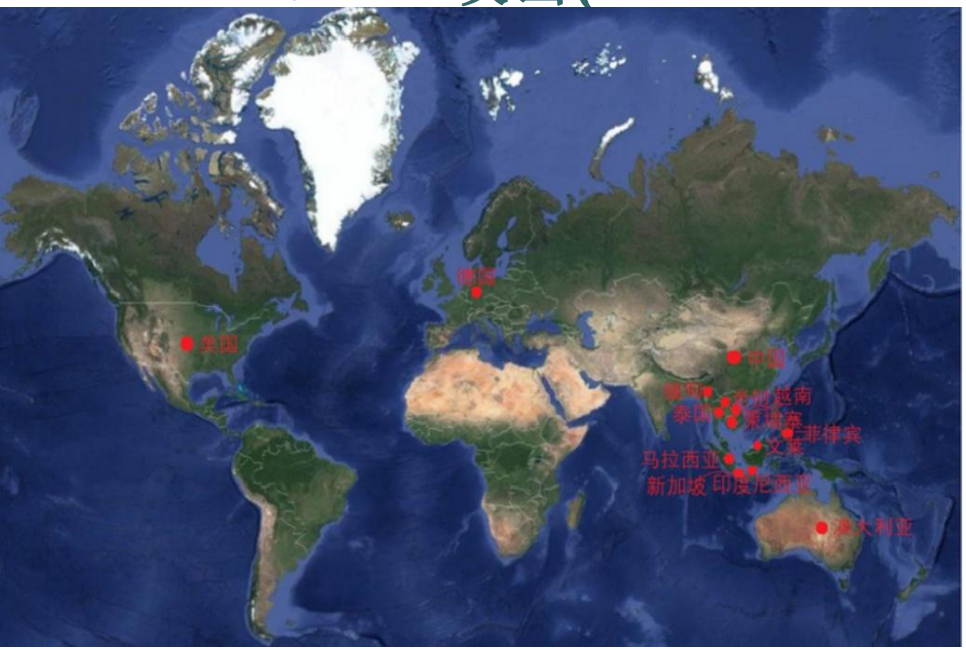
排名	病毒名	描述
1	Adware.Mobby/Android!8.A0FC	不断显示广告，包括全屏显示广告、阻止其他应用窗口的显示、弹出各种通知、创建快捷方式和加载网站等
2	Dropper.Agent/Android!8.37E	通过伪造、篡改、劫持短信、彩信、邮件、通讯录、通话记录、收藏夹、桌面等方式诱导用户触发点击等行为
3	Trojan.SMSreg!8.2DFC	运行后无明显扣费提示，用户若不慎点击会发送扣费短信，造成用户资费损失
4	Trojan.Android.Zdtad!1.A21F	会弹出窗口、下载推广软件，并且无法正常卸载、删除和退出进程
5	Trojan.Hiddad/Android!8.4E1	对合法的应用进行重新打包，并发布到第三方商店，会显示广告，访问操作系统内置安全细节，允许攻击者获取用户敏感数据

2020年中国网络安全报告(续)

4. CVE漏洞(Common Vulnerabilities & Exposures)

2020年中国网络安全报告(续)

5. APT攻击(Advanced Persistent Threat)



来源于越南的“海莲花”
全球攻击目标

2020年中国网络安全报告(续)

中华人民共和国国防部国际军事合作办公室

Office for international Military Cooperation

Ministry of National Defense, People's Republic of China

News Letter: June

40 female officers trained for peacekeeping mission

A total of 40 female officers from 26 countries received certificates on 19 June for completing a peacekeeping training program jointly sponsored by China's Ministry of National Defense and UN Women.

The training, which ran from June 08 to 19, aimed to increase the abilities of female peacekeepers in protecting the interests of women and children, and aiding victims of regional violence.

The officers, including five from China, were selected by UN Women.

The training included courses on peacekeeping action overviews, humanitarian action principles, protecting civilians in conflicts and community development, as well as exercises on cooperation, early warning and researching information.

This is the fourth time since 2016 that China has hosted training programs aimed at female peacekeepers.

According to an official with the Defense Ministry, the training showed China's efforts in fulfilling its international obligations, undertaking peace missions, and promoting gender equality in peacekeeping.

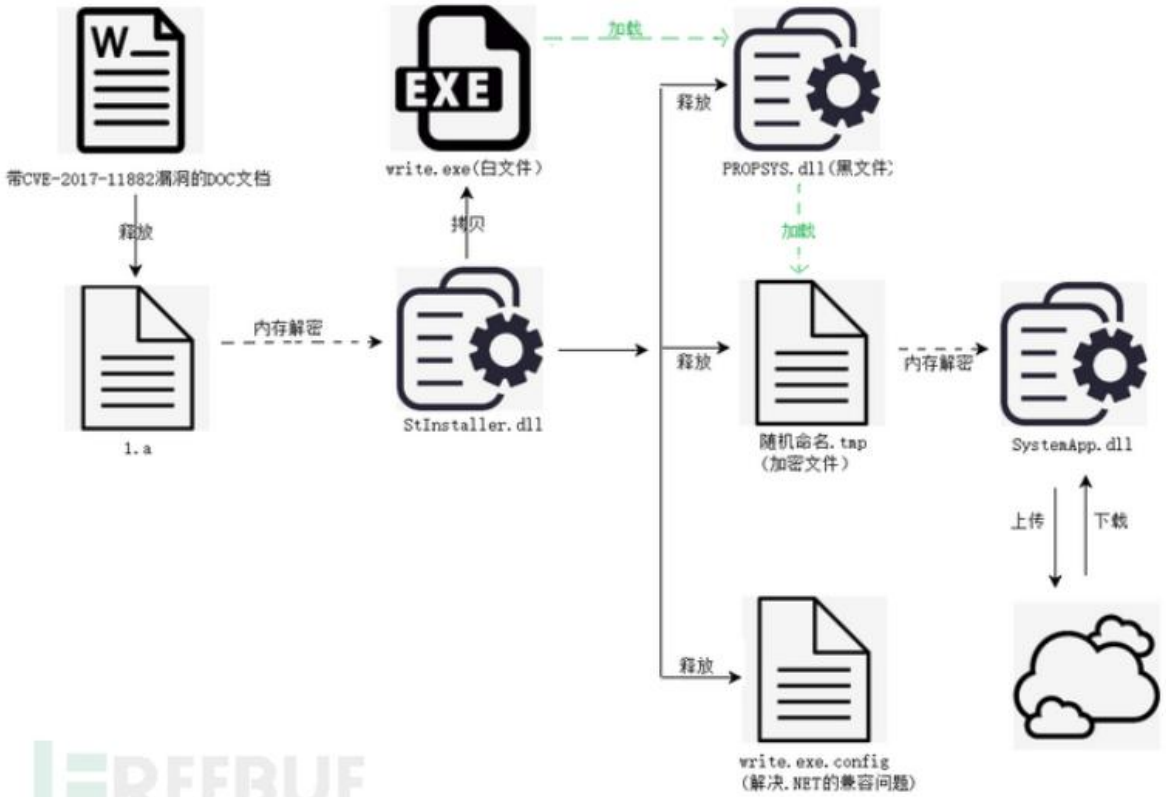
UN Under-Secretary-General for Peacekeeping Operations, Jean-Pierre Lacroix, attended the ceremony and spoke highly of China's efforts in peacekeeping actions.

He expressed hopes that female peacekeepers will account for around 15 percent of all peacekeepers in the near future.

图：OIMC News Letter.pdf.lnk

来源于印度APT组织“响尾蛇”对中国的攻击

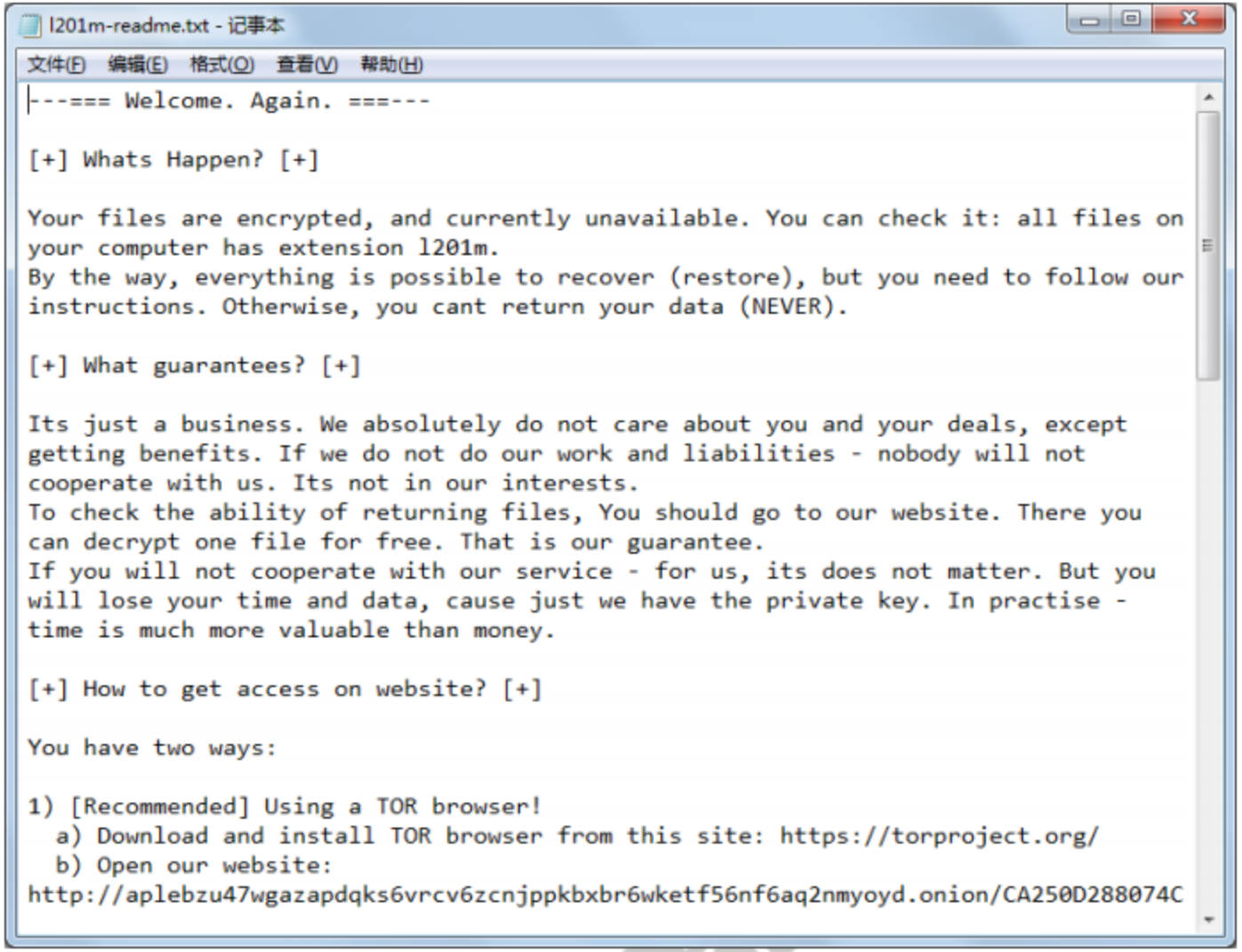
2020年中国网络安全报告(续)



响尾蛇攻击过程

2019年中国网络安全报告(续)

6. 勒索



图：Sodinokibi 勒索信

2020年中国网络安全报告(续)

7. 数据泄露

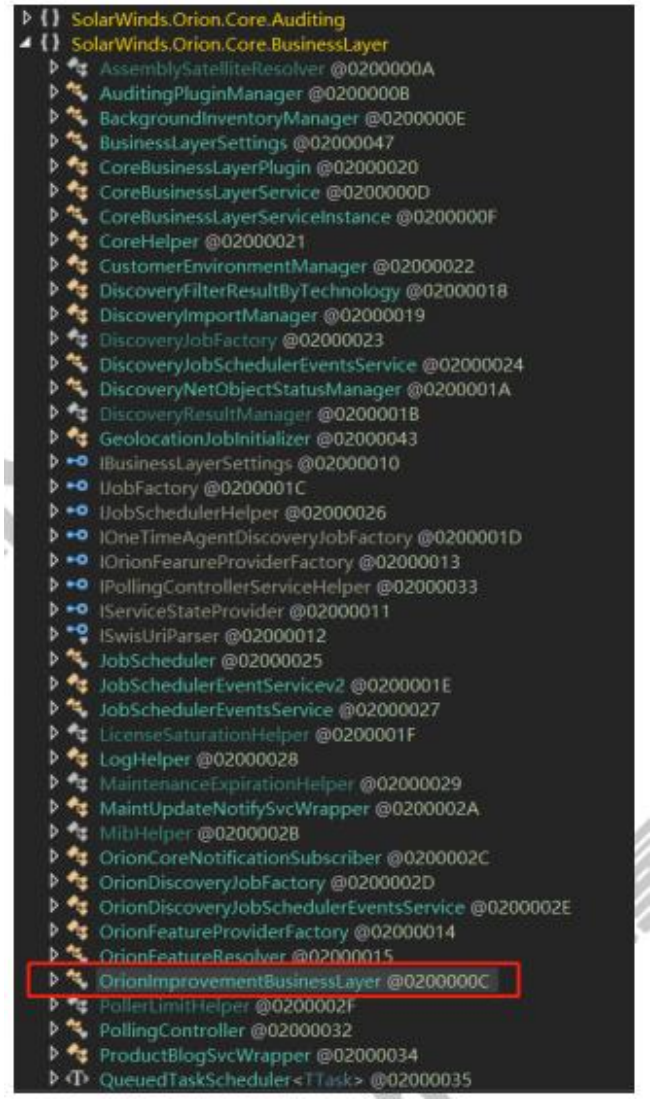
RISING 瑞星
2020年中国网络安全报告

2020年数据泄露事件

月份	数据泄露事件简述
一月	中国电信超2亿条用户信息被卖；7000多名武汉返乡人员信息遭泄露
二月	美高梅酒店1060万个客人数据泄露；万豪酒店520万客人信息被泄露
三月	微博5.38亿用户数据在暗网出售；秘密共享应用Whisper数据泄露，数百万用户的敏感信息可被在线查看
四月	青岛胶州中心医院6千余人就诊名单泄露；任天堂的30万个账户被非法登陆 用户信息或泄露
五月	曝泰国最大移动运营商泄露83亿条用户数据记录；英国易捷航空遭网络攻击信息泄露 约900万乘客信息被盗
六月	台湾2000万人个人信息在暗网泄露；甲骨文公司泄露数十亿条网络数据记录
七月	英国约克大学,教职工和学生记录数据泄露 ；能源供应商EDP被Ragnar Locker勒索软件攻击，超10TB的业务记录被泄露
八月	圆通"内鬼"泄露40万条客户信息；Freepik出现安全漏洞，830万用户数据遭泄露
九月	广西一医护人员倒卖8万条婴儿信息被追责；约1000名白俄罗斯高级警察的详细信息被泄露了
十月	泰州警方破获一起侵犯公民个人信息案，涉及800余万条数据；迈阿密的科技公司遭受了1TB的客户和业务数据泄露
十一月	330万台老年机被植入木马，数百万条公民个人信息遭贩卖；日本游戏商Capcom内部网络遭黑客攻击1T数据泄露
十二月	央视曝光简历信息被贩卖，招聘平台成简历信息泄露源头；英国能源供应商People's Energy数据遭泄露，影响了整个客户数据库

2020年中国网络安全报告(续)

8. 供应链攻击



2010年重大安全事件

2011年重大安全事件

网站或社区	信息泄露涉及用户数	是否证实
开发者技术社区 CSDN	600 余万	已确认并报案
天涯社区	4000 万	已确认，但泄露规模未确认
新浪微博	网传 476 万	未证实
多玩游戏	网传 800 万	未证实
7K7K 小游戏	网传 2000 万	否认
178 游戏	网传 1000 万	否认
人人网	网传 476 万	否认
网传开心网、猫扑、世纪佳缘、珍爱网、美空网、百合网等网站也涉及用户信息泄露，泄露规模不详，但均未证实		
图表制作：财新网（http://www.caixin.cn/）		

2012年重大安全事件

2013年重大安全事件

2014年重大安全事件

2015年重大安全事件

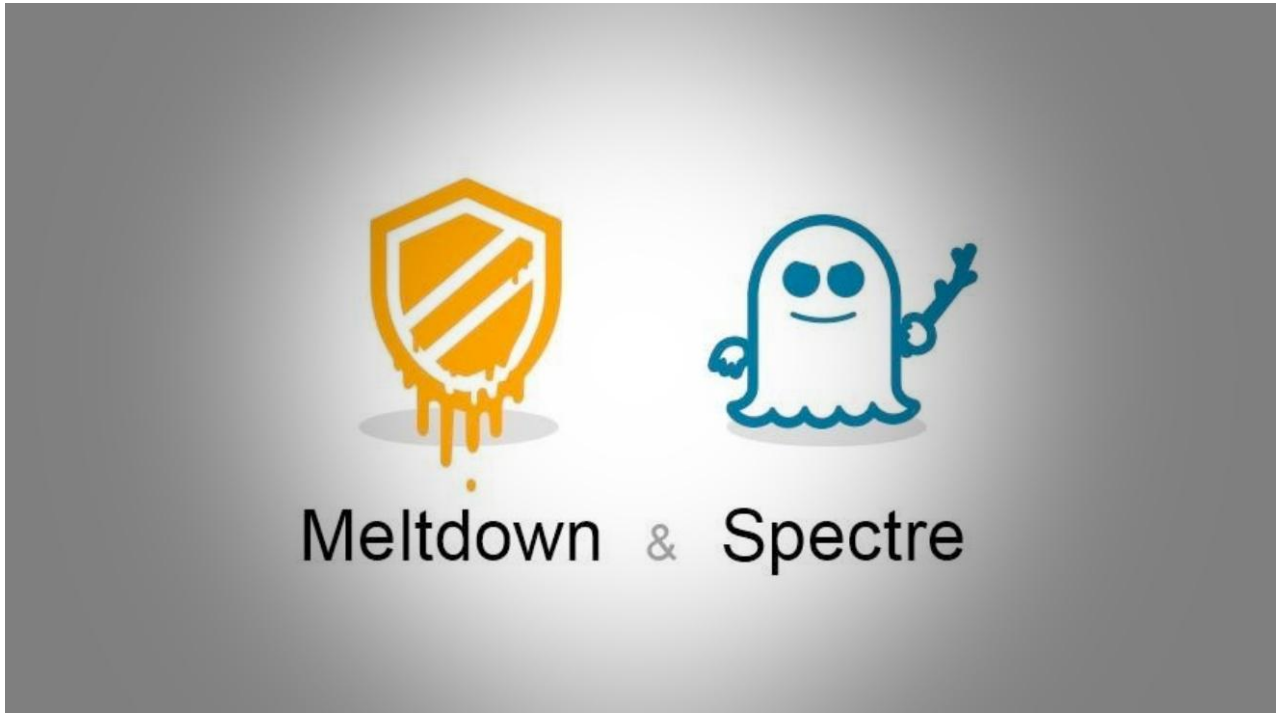
漏洞作者：路人甲	相关厂商：网易
事件编号：WooYun-2015-147763	

今日（10月19日）乌云漏洞报告平台接到了一起惊人的数据泄密报告！有白帽子报告称网易的用户数据库疑似泄露，影响数量总共近5亿条，泄露信息包括用户名、密码（MD5）、密码提示问题/答案（MD5）、注册IP、生日等。

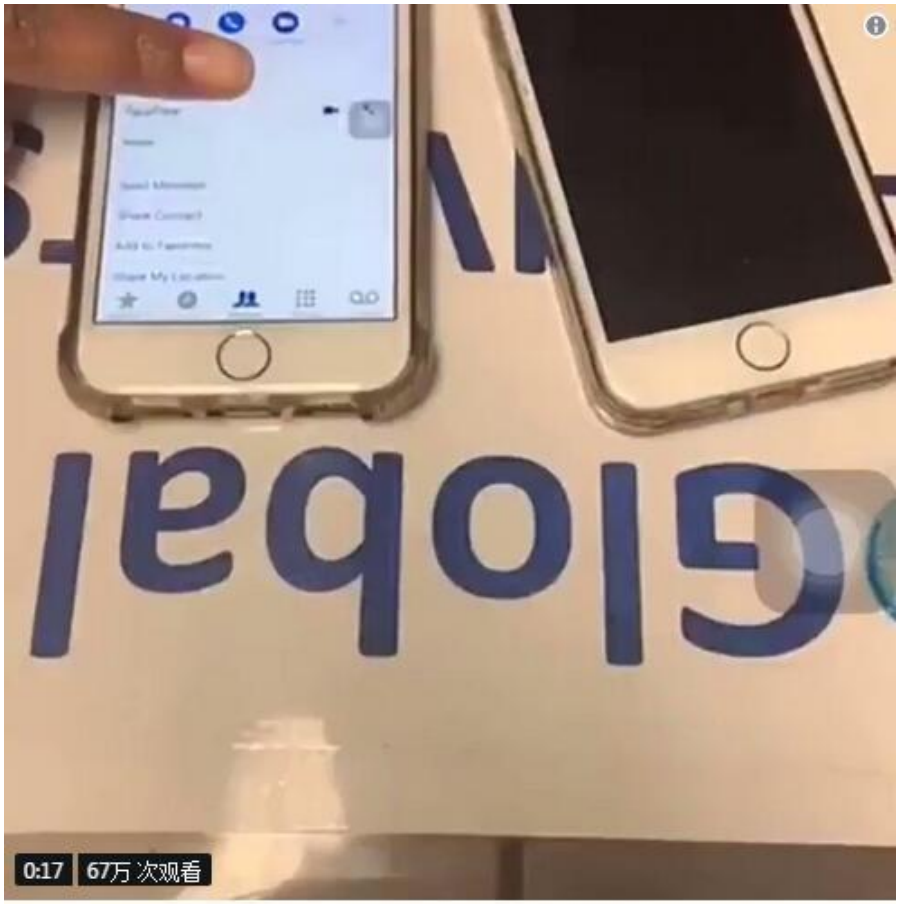
2016年重大安全事件

2017年重大安全事件

2018年重大安全事件



2019年重大安全事件



Benji Mobb™
@BmManski

Now you can answer for yourself on FaceTime even if they don't answer🤨#Apple explain this..

♡ 15.7K 3:24 AM - Jan 29, 2019

7,059 people are talking about this

2020年重大安全事件

2021年重大安全事件

网络安全新特征

- 网站拖库成为黑客盗号的主要手段
- 国产操作系统发展迎来春天，病毒威胁不可回避
- 勒索软件和APT攻击目标全面转向企事业用户，攻击手法专业化，攻击对象定向化

历史原因

- 在计算机设计之初，安全被极大的被忽视
  - 计算机产业长期处于“幸存模式”，一直致力于克服技术和经济成本的障碍
  - 很多安全技术措施被删减，被迫做出大量让步

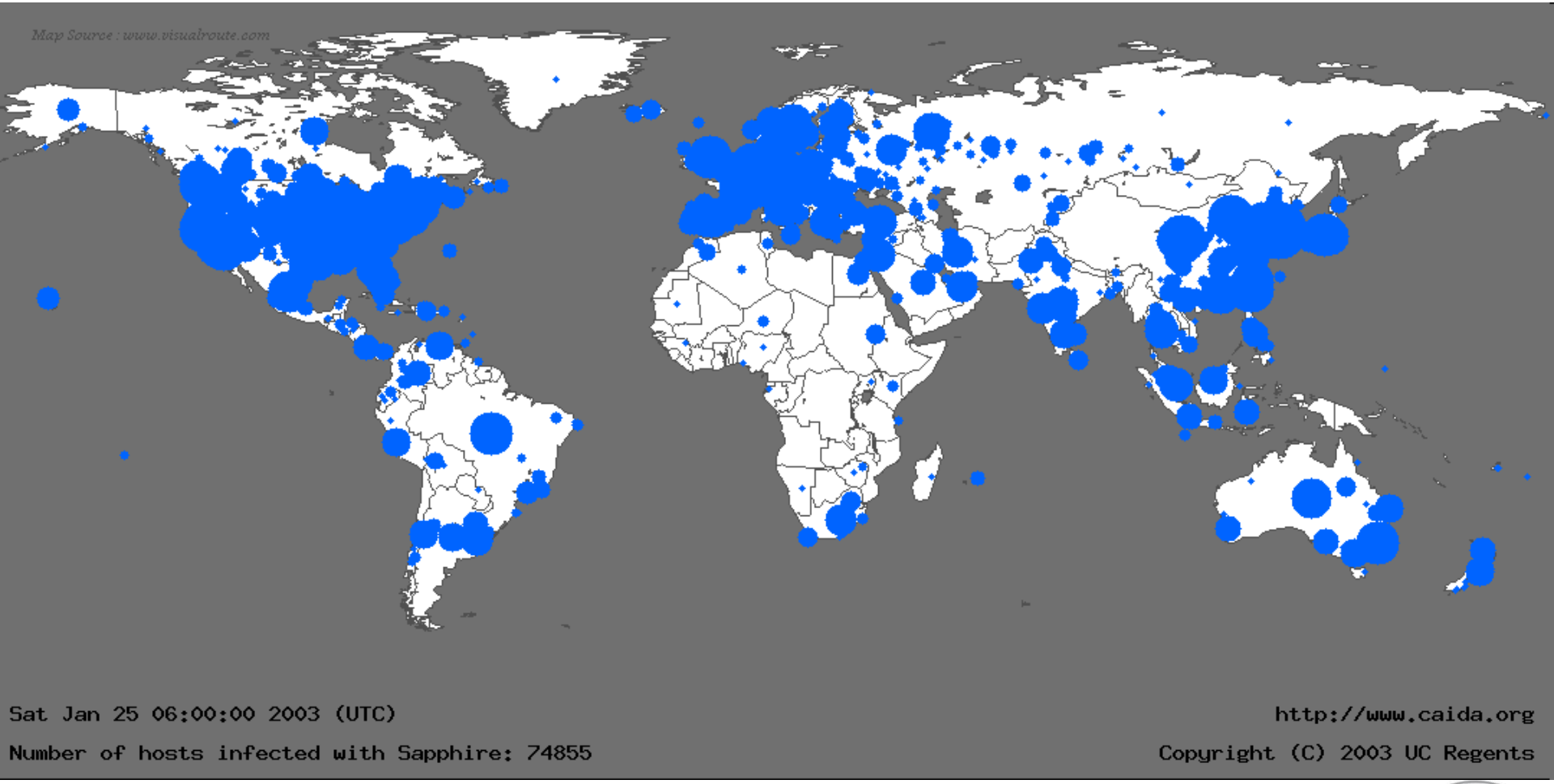
IT产业今非昔比

- 计算机产业早已脱离“幸存模式”
  - 性能卓越，成本低廉
  - 计算机在社会的各方面得到普及
- Internet打造地球村
  - 全球计算机相互连通，相互依存
  - Internet放大了任何安全危害的后果

生物学类比

- 计算机生态与生物种群相似
  - 单一体系架构（冯诺依曼架构）和几种有限的OS(Windows，Linux，IoS，Android)占统治地位
- 生物学中，单一种群很危险
  - 一种疾病或病毒可以在一夜之间将这个种群灭绝，因为单一种群共享同一缺陷
  - 该疾病只需要一个在宿主间传播的载体
- 计算终端就像生物种群，Internet提供传播载体
  - 全世界只有一种牛，并且它们在同一个池塘中饮水！

蓝宝石蠕虫Slammer的全球感染范围



中国信息安全严峻形势

- 全社会没有意识到信息安全的重要性
- 关键技术受制于外国
- 管理不能适应信息化发展的需求
- 信息安全专家短缺

课程内容

密码学

网络安全

信息内容安全

系统安全

2021

Thank you…