



提高信息安全意识

信息安全认知实习

授课老师：颀夏青

xiexiaqing@bupt.edu.cn

网络安全学院实验中心

2018年9月14日



提纲

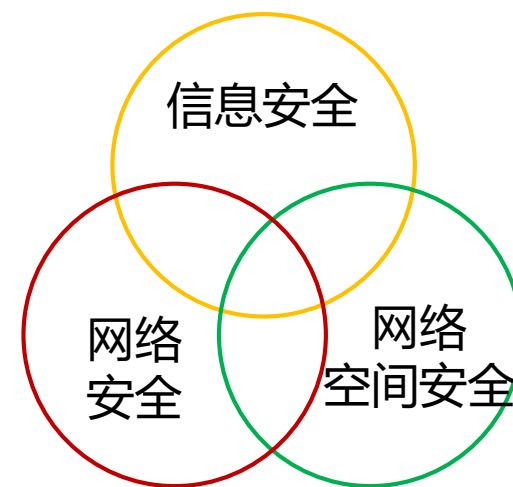
- 国际国内网络空间安全形势严峻
- 信息安全与个人安全息息相关
- 如何提高个人网络空间安全意识

三个概念：信息安全、网络安全与网络空间安全

- 信息安全可泛称各类信息安全问题
- 网络安全指称网络所带来的各类安全问题
- 网络空间安全则特指与陆域、海域、空域、太空并列的全球五大空间中的网络空间安全问题。
- 三者均类属于非传统安全领域，都聚焦于信息安全，可以相互使用，但各有侧重

信息安全 >> 网络安全 >> 网络空间安全

互联网技术发展普及推动下的进化



学科视角（培养方案）

参考文献：

[1] 方滨兴, 邹鹏, 朱诗兵. 网络空间主权研究[J]. 中国工程科学, 2016, 18(6): 1-7.

信息主权

- 信息安全作为一个大的概念，也引申出一系列相关的概念，如信息主权、信息疆域、信息战等。所谓信息主权，是指一个国家对本国的信息传播系统和传播数据进行自主管理的权利，是信息时代国家主权的重要组成部分。
- 由此也形成了信息疆域的概念，即同国家安全有关的信息空间及物理载体。

技术无国界，但是技术工作者是有国界的

捍卫国家的信息主权，乃至网络空间主权是每一个公民义不容辞的责任

网络空间主权

- **网络空间**可以简单定义为：网络空间是一种人造的电磁空间，其以终端、计算机、网络设备等为**载体**，**人类**通过在其上对**数据**进行计算、通信来实现特定的**活动**。在这个空间中，人、机、物可以被有机地连接在一起进行互动，可以产生影响人们生活的各类信息，包括内容、商务、控制信息等。
- **网络空间主权**是国家主权在位于其领土之中的信息通信基础设施所承载的网络空间中的自然延伸，即对出现在该空间的信息通信技术活动（针对网络虚拟角色而言）及信息通信技术系统本身（针对平台）及其数据（虚拟资产）具有主权（对数据操作的干预权利）。

参考文献：

[1] 方滨兴, 邹鹏, 朱诗兵. 网络空间主权研究[J]. 中国工程科学, 2016, 18(6): 1-7.



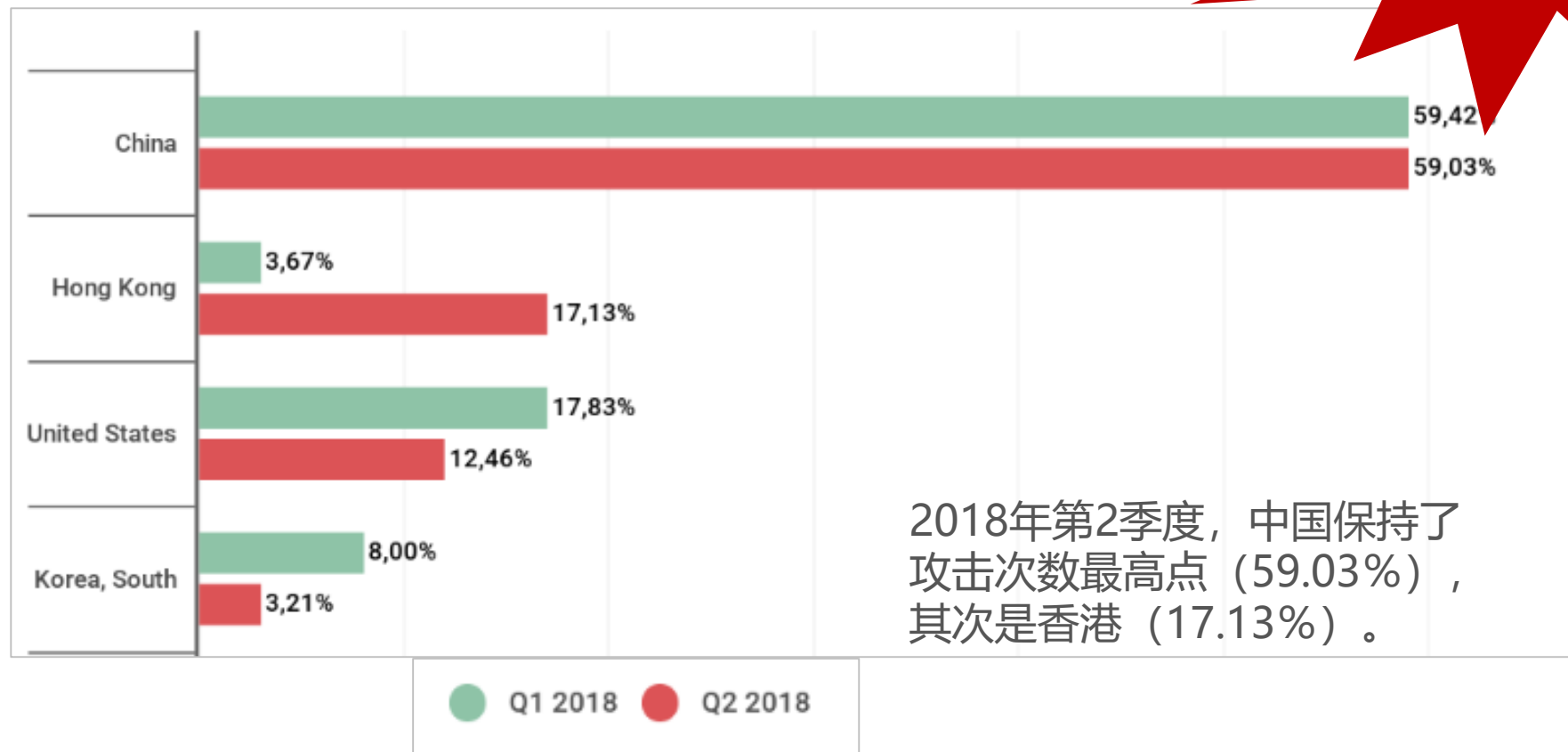
目录

- 国际国内网络安全形势严峻
- 信息安全与个人安全息息相关
- 如何提高个人网络安全意识

国际国内网络空间安全形势严峻

■ 中国是受DDOS攻击最多的国家

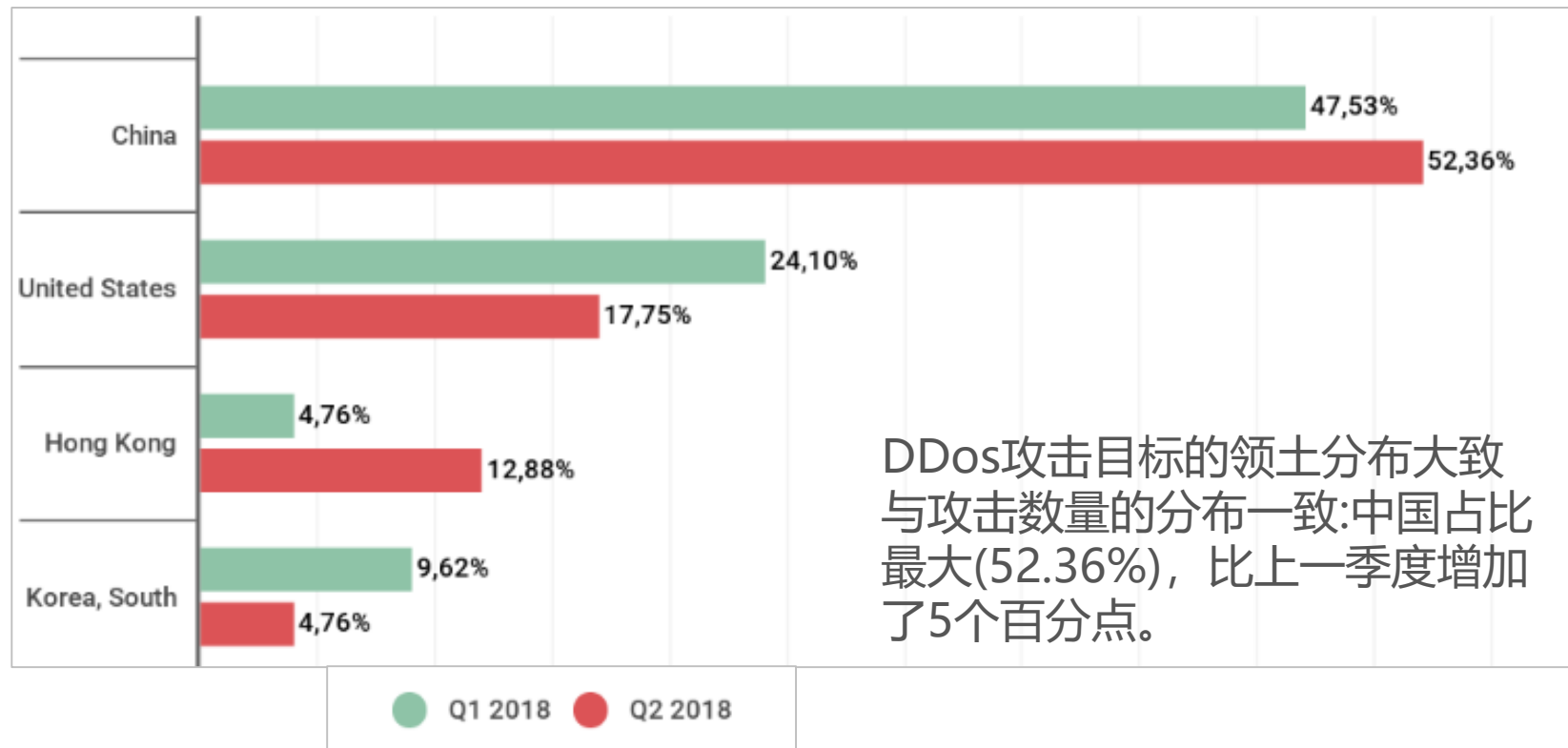
脆弱



数据来源：<https://securelist.com/ddos-report-in-q2-2018/86537/>

国际国内网络空间安全形势严峻

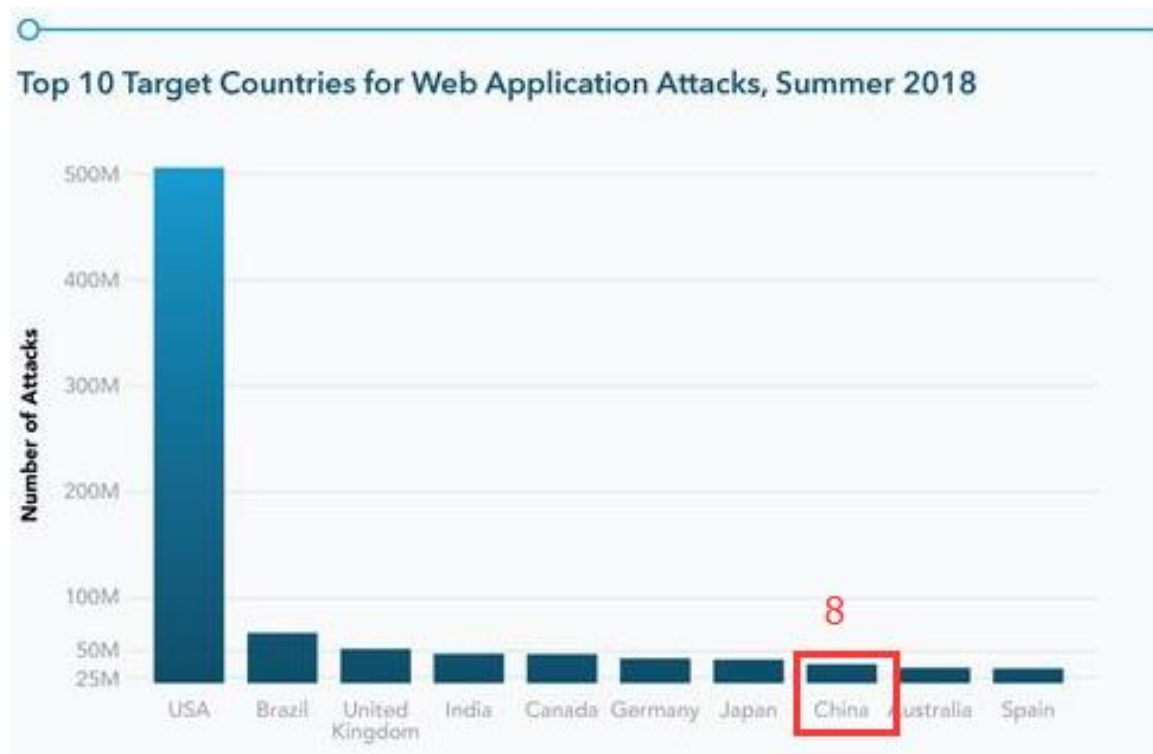
■ 中国是受DDOS攻击最多的国家



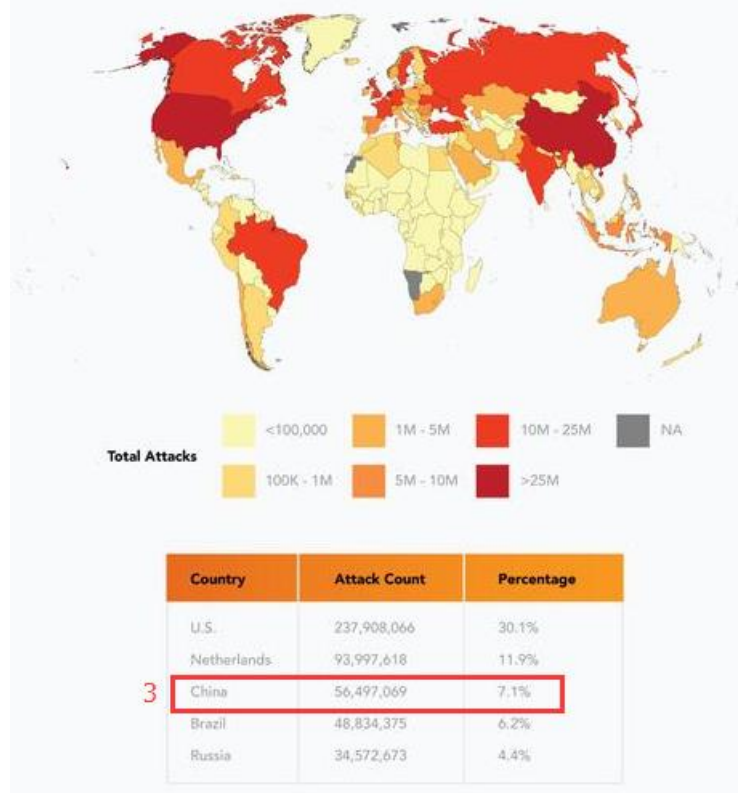
数据来源: <https://securelist.com/ddos-report-in-q2-2018/86537/>

国际国内网络空间安全形势严峻

■ 2018全球Web攻击十大目标国家：中国排第八



Source Countries for Web Application Attacks - Worldwide, Summer, 2018

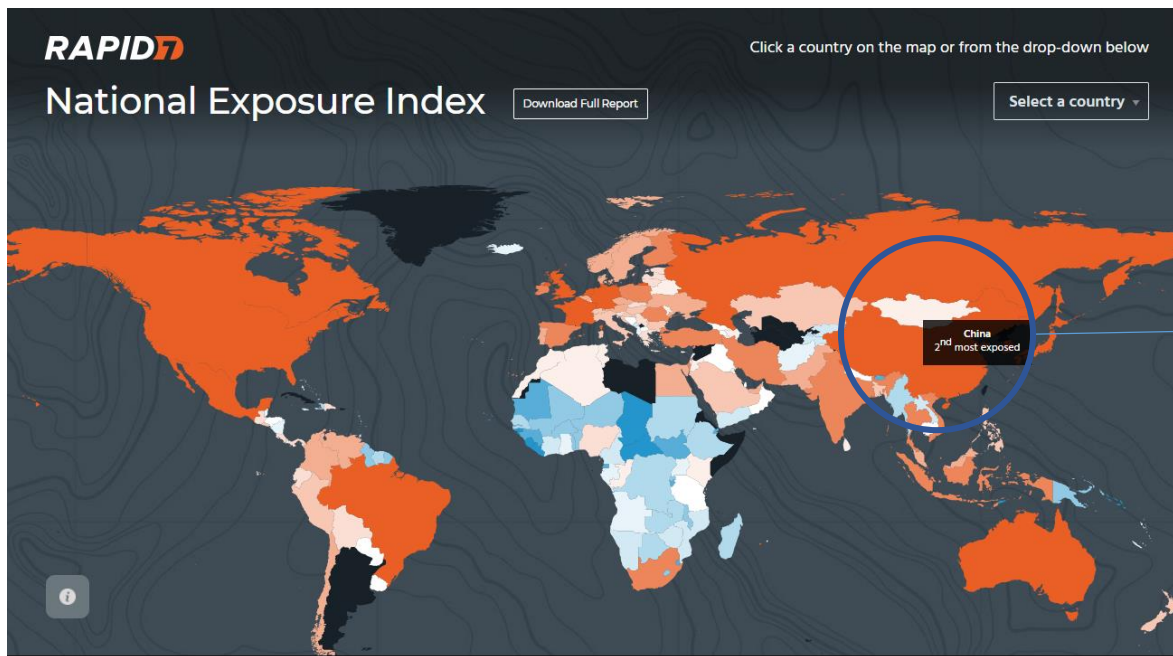


数据来源：《夏季互联网安全Web 攻击报告》

<https://blogs.akamai.com/2018/06/summer-soti---web-attacks.html>

国际国内网络空间安全形势严峻

■ 2018全球端口暴露指数：中国第二



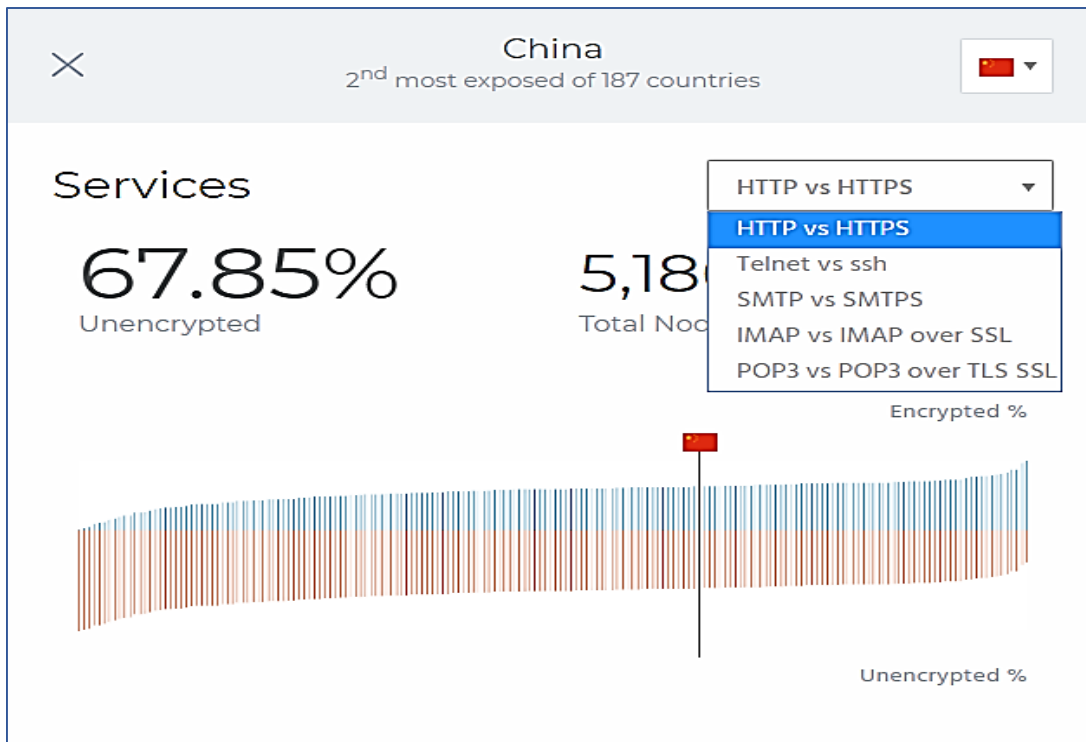
Rapid7 近日发布的《2018国家暴露指数报告》显示，全球端口暴露最严重的十个国家为美国、中国、加拿大、韩国、英国、法国、荷兰、日本、德国和墨西哥，其中美国暴露的情况最严重，其次为中国。

数据来源：《全球暴露指数2018》

<https://www.rapid7.com/data/national-exposure/2018.html#CN>

国际国内网络空间安全形势严峻

■ 2018全球端口暴露指数：中国第二



- 中国的数据库暴露程度惊人，有180万个响应的数据库服务端口。
- 中国有超过**3.4亿**个 IPv4 地址，Rapid7 的研究人员发现中国有约1400万台服务器对扫描有响应。

数据来源：《全球暴露指数2018》

<https://www.rapid7.com/data/national-exposure/2018.html#CN>

国际国内网络空间安全形势严峻

■ 2017僵尸网络盛行国家：中国第三

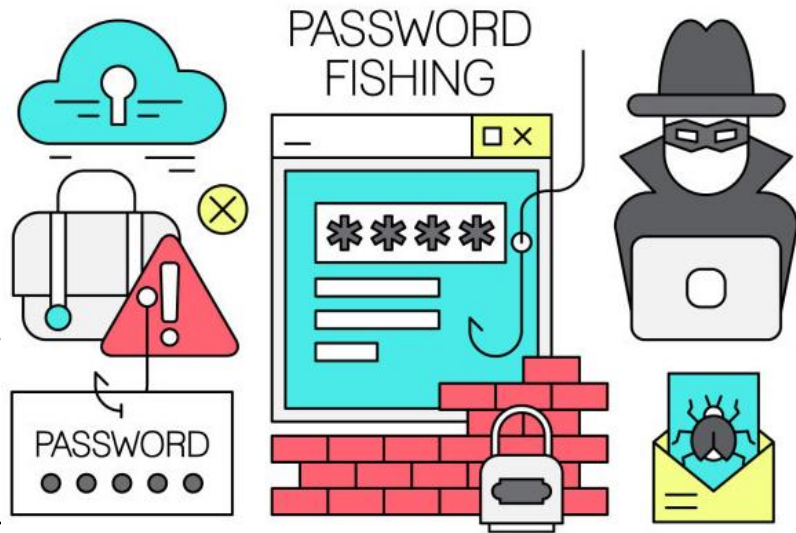
- 根据 CenturyLink 研究研究实验室公布的数据，中国、日本、韩国以及澳大利亚在2017年年内出现大量僵尸网络流量，年内日均威胁活动高达**19.5万次**。各僵尸网络共影响到1.04亿个独立目标，例如包括服务器、手持设备以及其它互联网接入设备。
- 在2017年的僵尸流量榜上位列前五的国家分别为美国、中国、德国、俄罗斯以及英国，美国、中国、俄罗斯位列恶意流量三甲。

国际国内网络空间安全形势严峻

■ 2018年2月，韩国平昌冬季奥运会遭遇黑客攻击

当全球目光聚焦平昌冬奥会时，奥组委却不得不临时关闭服务器和平昌冬奥会网站，官网宕机12小时、比赛场馆附近网络瘫痪、门票无法打印导致观众无法正常入场，媒体中心系统故障导致无法正常观看直播.....引发各种猜测。几天后的新闻发布会上，平昌冬奥筹委会发言人宋百裕（Sung Baik-you）对外证实，平昌冬奥官网宕机是网络攻击所致。而据国际知名安全公司McAfee报告，称针对韩国平昌奥运会，黑客组织开展了鱼叉式网络钓鱼攻击。

- 一次典型的**鱼叉式钓鱼邮件攻击**
- 攻击目标是：@pyeongchang2018.com账号的相关用户
- **身份伪装**：假装来自**韩国国家反恐中心（NCTC）** info@nctc.go.kr，实际上邮件从Postfix邮件服务器发送，来自位于新加坡的攻击者。
- **内容伪装**：韩文编写，附件为含恶意宏的Word文档，原文件名“ 농식품부, 평창 동계올림픽 대비 축산악취 방지대책 관련기관 회의 개최.doc（由农林业部和平昌冬奥会组织）。当时NCTC正在为奥运会进行**反恐演习**，邮件中特地提到了反恐演习，以骗取收件人信任，增加打开附件的概率。



国际国内网络空间安全形势严峻

■ 加密货币采矿软件攻击致欧洲废水处理设施瘫痪

挖矿机致欧洲废水处理服务器瘫痪

文章来源：企鹅号 - E安全

E安全2月15日讯 工业网络安全企业Radiflow公司近日表示，四台接入欧洲废水处理设施运营技术网络的服务器遭遇加密货币采矿恶意软件的入侵。该恶意软件直接拖垮了废水处理设备中的 HMI 服务器 CPU。Radiflow公司称，此次事故亦是加密货币恶意软件首次对关键基础设施运营商的运营技术网络展开攻击。

- 基础设施安全涉及到电力、水力、网络等，关系国计民生。

国际国内网络空间安全形势严峻

■ Facebook用户数据泄露

Facebook史上最大规模数据泄露牵出惊天丑闻

2018年3月16日，Facebook 被曝在2014年有超过5000万名用户（接近Facebook美国活跃用户总数的三分之一，美国选民人数的四分之一）资料遭“剑桥分析”公司非法用来发送政治广告，部分媒体将其视为 Facebook 有史以来遭遇的最大型数据泄露事件，但 Facebook 方面否认这是一起数据泄露事件。

原本作为世界财富排行榜第四名的扎克伯格近日财富缩水严重，此次事件曝光后，Facebook 仅一天之内市值蒸发**60亿美元**（约合人民币380亿元）。

扎克伯格在英美9家报纸登报道歉，正式为泄密说了Sorry

澎湃新闻记者 承天蒙

2018-03-26 09:33 来源：澎湃新闻

字号

Facebook创始人马克·扎克伯格（Mark Zuckerberg）在9家周日报纸上为“信任的违背”登报道歉。

- 算法和数据库最终造就了一款强大的**政治工具**，可识别摇摆不定的选民，并推送不可能会产生共鸣的消息。

信息安全与个人安全息息相关

■ 观看视频《真实的较量》2' 25''

- 在中央网信办网络安全协调局、上海市网信办的指导下，上海广播电视台融媒体中心制作的大型新闻专题片《第五空间》，是国内第一部聚焦网络安全的电视新闻专题片，三集分别为《透明的时代》、《隐秘的威胁》和《真实的较量》。对应个人、社会、国家三个维度，呈现一份震撼的网络安全调查报告。
- 推荐：
- 第一集：《透明的时代》
- http://www.cac.gov.cn/2017-09/16/c_1121673974.htm
- 第二集：《隐秘的威胁》
- http://www.cac.gov.cn/2017-09/17/c_1121676845.htm
- **第三集：《真实的较量》**
- **http://www.cac.gov.cn/2017-09/18/c_1121679259.htm**



目录

- 国际国内网络空间安全形势严峻
- 信息安全与个人安全息息相关
- 如何提高个人网络空间安全意识

信息安全与个人安全息息相关

■ 信息安全关系学生生命财产安全，影响学生前途命运

- 航班信息泄露事件

点击可查看付款码数字



信息安全与个人安全息息相关

■ 2017年5月勒索病毒事件高校成重灾区

360针对校园网勒索病毒事件的监测数据显示，国内首先出现的是ONION病毒，平均每小时攻击约200次，夜间高峰期达到每小时1000多次；WNCRY勒索病毒则是5月12日下午新出现的全球性攻击，并在中国的校园网迅速扩散，夜间高峰期每小时攻击约4000次。

由于国内曾多次出现利用445端口传播的蠕虫病毒，部分运营商对个人用户封掉了445端口。但是教育网并无此限制，存在大量暴露着445端口的机器，因此成为不法分子使用NSA黑客武器攻击的重灾区。正值高校毕业季，勒索病毒已造成一些应届毕业生的论文被加密篡改，直接影响到毕业答辩。

- 信息安全关系国家命运，也关系每一个人的生命、财产安全。

信息安全与个人安全息息相关

■ 2018年8月28日，酒店5亿条数据泄露

华住旗下酒店开房数据（汉庭，桔子，全季等）

主题帖交易信息一览					
交易类型	出售数量	单价[BTC]	约合[美元]	商家最后在线	
出售	10	8	55200	08-28 13:14	
交易状态	已成交	剩余数量	投诉期限	发布时间	
出售中	0	10	付款后3天	08-28 06:00	

购买操作: 请仔细查阅交易信息, 商品单价, 投诉期限以及对方最后在线时间, 如需购买, 请输入数量, 点击提交

购买数量:

确认提交:

回复

第一个未读帖子 • 1 帖子 • 分页: 1 / 1

helen250

帖子: 4

注册时间: 2018年-8月-21日 00:34

联系: 

华住旗下酒店开房数据（汉庭，桔子，全季等）

由 helen250 » 2018年-8月-28日 06:00

出售华住旗下所有酒店数据（汉庭/美爵/禧玥/漫心/诺富特/美居/CitiGO/桔子/全季/星程/宜必思尚品/宜必思/怡莱/海友）


附件当中为测试数据，各提供10000条数据供大佬测试。

crm.txt为华住官网注册资料，包括姓名，手机号，邮箱，身份证号，登陆密码等信息。全部资料共53G，大约1.23亿条记录

cusinfo为酒店入住时登记的身份信息，主要包括姓名，身份证号，家庭住址，生日，内部id号。全部资料共22.3G，大约1.3亿人身份证信息

history 为酒店开房记录，包括内部id号（可与cusinfo做关联查询），同房间关联号，姓名，卡号，手机号，邮箱，入住时间，离开时间，酒店id号，房间号，消费金额等信息。共66.2G，大约2.4亿条记录。

以上数据脱裤时间为2018年8月14号。

欢迎各位有需要的大佬购买，以上全部信息打包价为8比特币，或者520门罗币。 购买的大佬请联系我邮箱或者暗网私信我，我把数据的下载地址和解压密码发给你，如果权限不丢失，后续数据还可以免费发给已购买的大佬。

信息安全与个人安全息息相关

- 坚守底线：《网络安全法》

- 视频：4分钟



目录

- 国际国内网络安全形势严峻
- 信息安全与个人安全息息相关
- 如何提高个人信息安全意识

如何提高个人信息安全意识

- 认识“信息不安全”的现状，树立危机意识
- 认真学习专业知识，掌握防范方法，做安全的驾驭者
- 勇担重任，以建设网络安全强国为己任
- 忠告：作为一名搞安全的，必须懂法守法，严守法律红线

如何提高个人信息安全意识

- 反其道而观之，让我们看看知乎上那些安全大拿们怎么说

有哪些属于做安全的人才有的习惯？

- 0.看到美女头像，先当成男的
- 1.熟练使用右键 -通过Google搜索功能和审查元素
- 2.看到链接，先加单引号
- 3.看到网站，先收集whois信息，再进行安全测试
- 4.看到用户名，收集个人信息
- 5.看到公司名，使用天眼查查询
- 6.看到输入框，测试最大长度和不可见字符
- 7.看到后台，进行权限校验

有哪些属于做安全的人才有的习惯？

- 8.看到搜索结果，分析如何SEO
- 9.用各种方法尝试获得别人的账号
- 10.多写代码，少用工具
- 11.玩游戏先找外挂，看看最高多少分
- 12.经常钓鱼，测试自己的想法
- 13.学会伪装，不要暴露自己
- 14.多思考为什么，理解安全的本质

来源：<https://www.zhihu.com/question/266139470/answer/305688135>

如何提高个人信息安全意识

有哪些属于做安全的人才有的习惯？

432 人赞同了该回答

- 1.接/拨陌生号码前先在支付宝、微信里查一下
- 2.加QQ前先在支付宝和微信、空间、腾讯微博里查一下
- 3.QQ、微信、手机号、邮箱都会习惯性的在各大搜索引擎里查一下
- 4.看网站的时候会在参数里加入"<>\等字符
- 5.看到熟悉的框架、CMS会根据经验测测漏洞或进入管理后台简单试一下弱口令
- 6.填写手机号都是13333333333，身份证全是网上搜的
- 7.不顺眼的程序都放虚拟机运行
- 8.用开源程序都去官网下
- 9.有人问比较敏感的问题会比较警惕
- 10.发来的链接不乱点，先看一下源代码
- 11.看到终端机就上戳戳下戳戳
- 12.不连公共WiFi
- 13.PC登陆账号时密码倒着输
- 14.日常膜拜同行大黑哥们

有哪些属于做安全的人才有的习惯？

- 【千万不要把摄像头放在卧室！】
- 【千万不要把摄像头放在卧室！】
- 【千万不要把摄像头放在卧室！】

我手边在做的智能安防项目。在做平台，也在整和绝大部分安防硬件的SDK。

我说个恐怖的事实，迄今为止【所有厂家的终端摄像头，都能监视客户；如果服务者想的话】不仅仅是360.....想要安全，找服务好，口碑好的安防服务商。

如何提高个人信息安全意识

有哪些属于做安全的人才有的习惯？

597 人赞同了该回答

- 1.不安装任何杀毒软件
- 2.不信任的软件全部在虚拟机里运行
- 3.开机必先挂vpn，不挂没安全感
- 4.看到low一点的网站就忍不住在地址栏加个admin
- 5.在vps中使用攻击脚本，扫描工具
- 6.在电脑上习惯用命令行创建用户，习惯性在用户名后加上\$
- 7.本地搭建漏洞复现环境习惯修改host指向一个短域名
- 8.看到可控输出点就忍不住试试XSS
- 9.浏览网页后还要浏览一遍源代码
- 10.看到傻逼的人就忍不住想社工一波

作业

- 观看下列视频之一：
- (1) 美国最新 “网络战揭秘” 史诗纪录片
- 视频链接：<https://www.easyaq.com/course/41.shtml>
- (2) 真实的较量（上网搜索《第五空间》）
- 完成一份报告，标题自拟，谈谈你对网络空间安全以及网络空间安全战的认识，字数不少于1000字。



感谢聆听！

信息安全认知实习

授课老师：颀夏青

xiexiaqing@bupt.edu.cn

网络空间安全学院实验中心

2018年9月14日