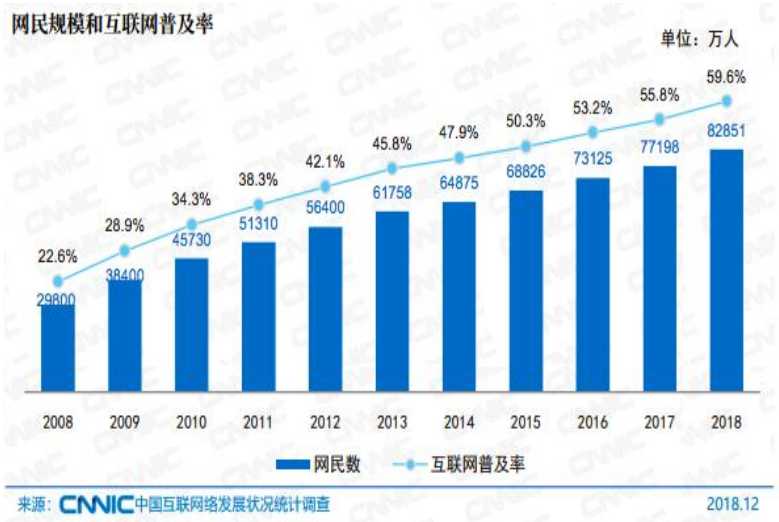
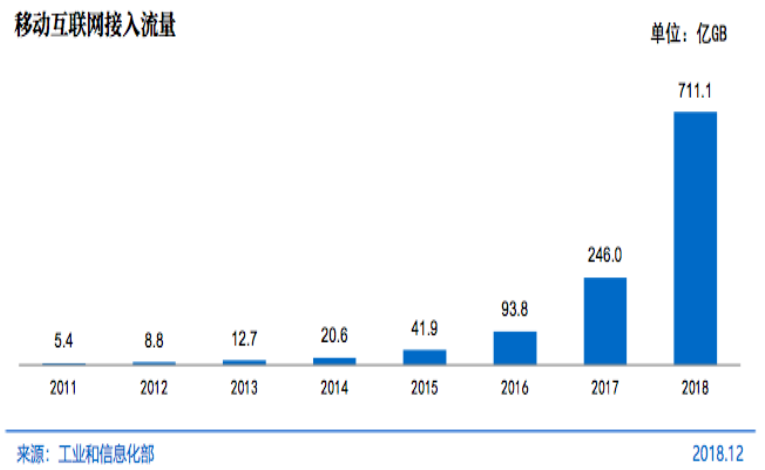
新型网络攻击手段分析与防御

中国人民公安大学（F馆F9展位）
信息技术与网络安全学院
芦天亮 副教授

中国网络发展现状

- 2019年2月，中国互联网络信息中心CNNIC发布了第43次《中国互联网络发展状况统计报告》，截至 2018年 12 月：
- 我国网民规模达8.29 亿,互联网普及率为59.6%；
- 我国国际出口带宽已将近9Tbps，较2017年增长22.2%；
- 移动互联网接入流量消费达711.1亿GB，较2017年增长189.1%。





网络安全现状

- 2018年CNCERT监测发现：
  - 我国境内感染病毒终端的数目累计616万个；
  - 我国境内被篡改网站数量累计23459个，其中政府网站689个；
  - 仿冒我国境内网站的页面约 5.3 万个，其中仿冒政务类网站明显上升占25.2%；
  - 国家信息安全漏洞共享平台收集整理的信息系统安全漏洞累计14216个。

网络攻击事件-教育网

- 勒索病毒（ransomware）

近两年，勒索病毒爆发并流行，给用户带来巨额损失。

2017年5月，勒索病毒“WannaCry”利用NSA泄漏出来的微软Windows系统漏洞大范围传播，波及150多个国家，受害者多达20万，并且还出现了变种。

大量企业甚至政府内网大规模感染，教育网受损严重，勒索病毒导致教学系统瘫痪，包括校园一卡通系统。

大量学生电脑感染病毒后，毕业论文被加密，为了毕业甚至支付赎金。

网络攻击事件-教育网

- 山东考生徐玉玉案
- 2016年8月19日，山东临沂市高三毕业生徐玉玉遭受以发放助学金为名义的电信诈骗，被骗走9900元学费。徐玉玉报警后在回家途中昏厥，后不治身亡。经审查：
  - 2016年4月，被告人杜天禹非法侵入山东省2016年普通高等学校招生考试信息平台网站，窃取考生个人信息64万余条，并对外出售牟利。
  - 2016年7月，被告人陈文辉从杜天禹手中购买五万余条考生信息，实施电信诈骗。
- 2017年7月，主犯陈文辉一审因诈骗罪、非法获取公民个人信息罪被判无期徒刑，没收个人全部财产。

个人数据的地下交易

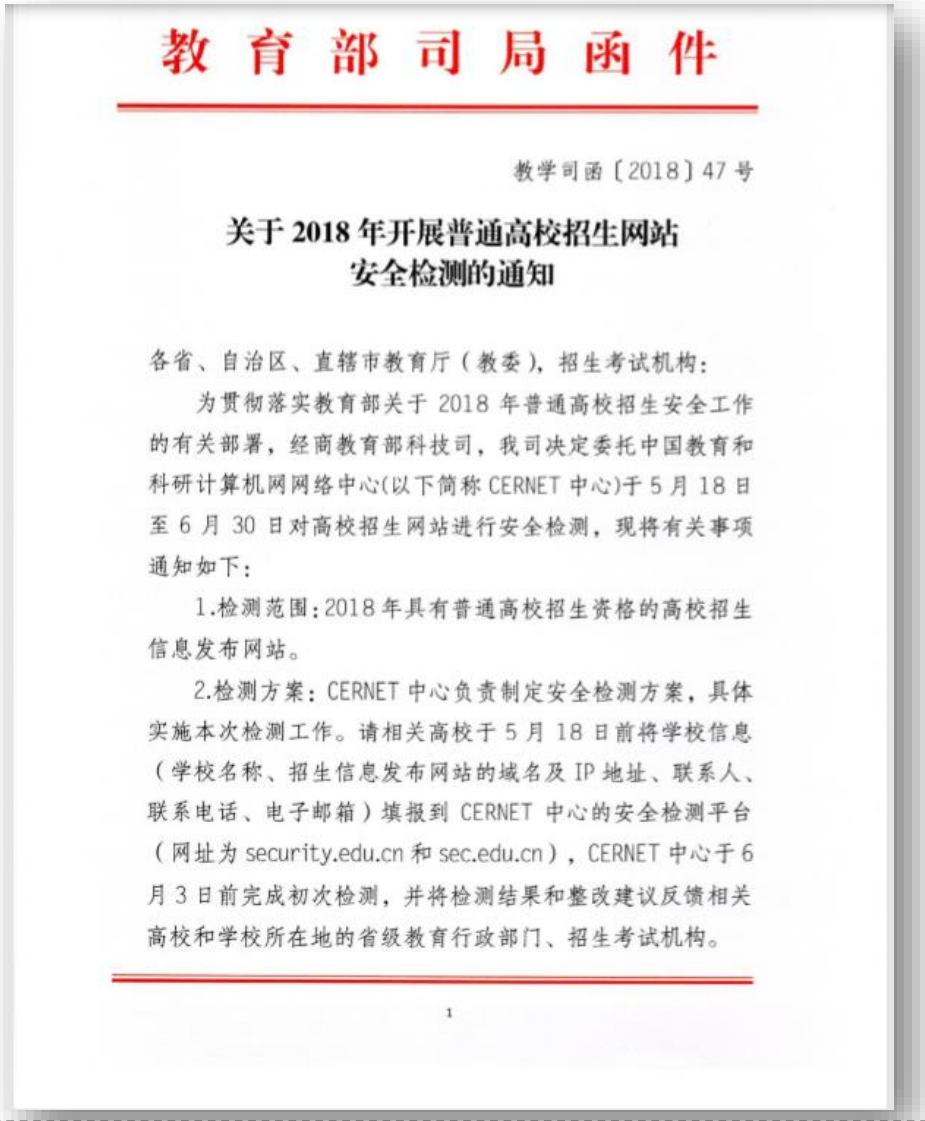
- 除了考生报名信息之外，如网购消费记录、医疗信息、新生儿信息、信用卡等多种重要个人信息也被明目张胆地放在网上公开销售。根据信息质量高低要价0.1元至5元不等。

高校招生网站安全检测

背景

为贯彻落实教育部关于2018年普通高校招生安全工作的有关部署， 在教育部学生司的指导下，CERNET国家网络中心于2018年开展了“教育部高考信息服务网站安全检查工作”。

这是继2017年后，第二次开展“教育部高考信息服务网站安全检查工作” 本次对全国1976所高校招生信息发布网站进行安全检查。



教 育 部 司 局 函 件

教学司函〔2018〕47号

关于2018年开展普通高校招生网站安全检测的通知

各省、自治区、直辖市教育厅（教委），招生考试机构：

为贯彻落实教育部关于2018年普通高校招生安全工作的有关部署，经商教育部科技司，我司决定委托中国教育和科研计算机网网络中心(以下简称CERNET中心)于5月18日至6月30日对高校招生网站进行安全检测，现将有关事项通知如下：

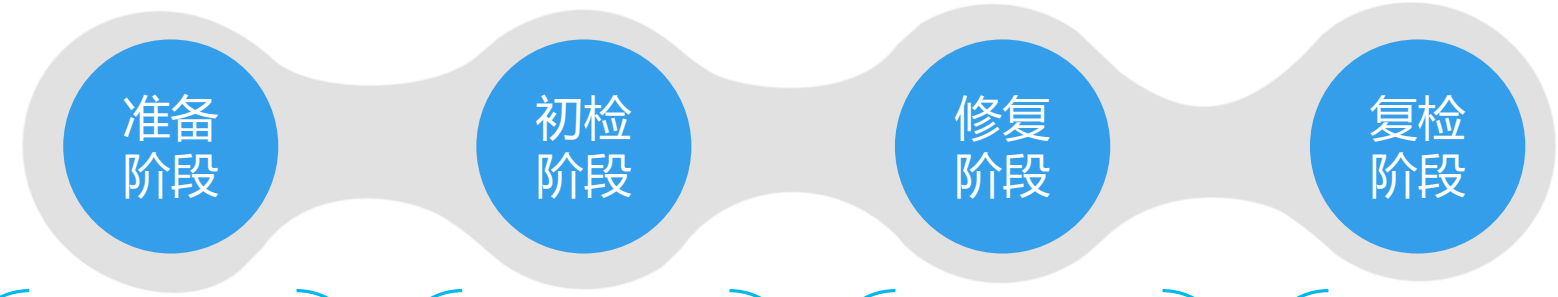
1.检测范围：2018年具有普通高校招生资格的高校招生信息发布网站。

2.检测方案：CERNET中心负责制定安全检测方案，具体实施本次检测工作。请相关高校于5月18日前将学校信息（学校名称、招生信息发布网站的域名及IP地址、联系人、联系电话、电子邮箱）填报到CERNET中心的安全检测平台（网址为security.edu.cn和sec.edu.cn），CERNET中心于6月3日前完成初次检测，并将检测结果和整改建议反馈相关高校和学校所在地的省级教育行政部门、招生考试机构。

1

高校招生网站安全检测

检查流程



- 部署漏洞扫描服务器。
- 开发高校招生网站安全服务平台，便于各高校网络安全负责人注册并上传信息。

- 高校网络安全负责人上报招生信息发布网站。
- CERNET NOC安全小组对招生网站进行漏洞扫描和检测。

- 将检测结果通知各高校，并提供漏洞的修复解决方案。
- 高校修复网站漏洞后，将整改方案上传至电子自服务平台。

- 由CERNET NOC安全小组对网站重新扫描，并验证网站修复。

高校招生网站安全检测

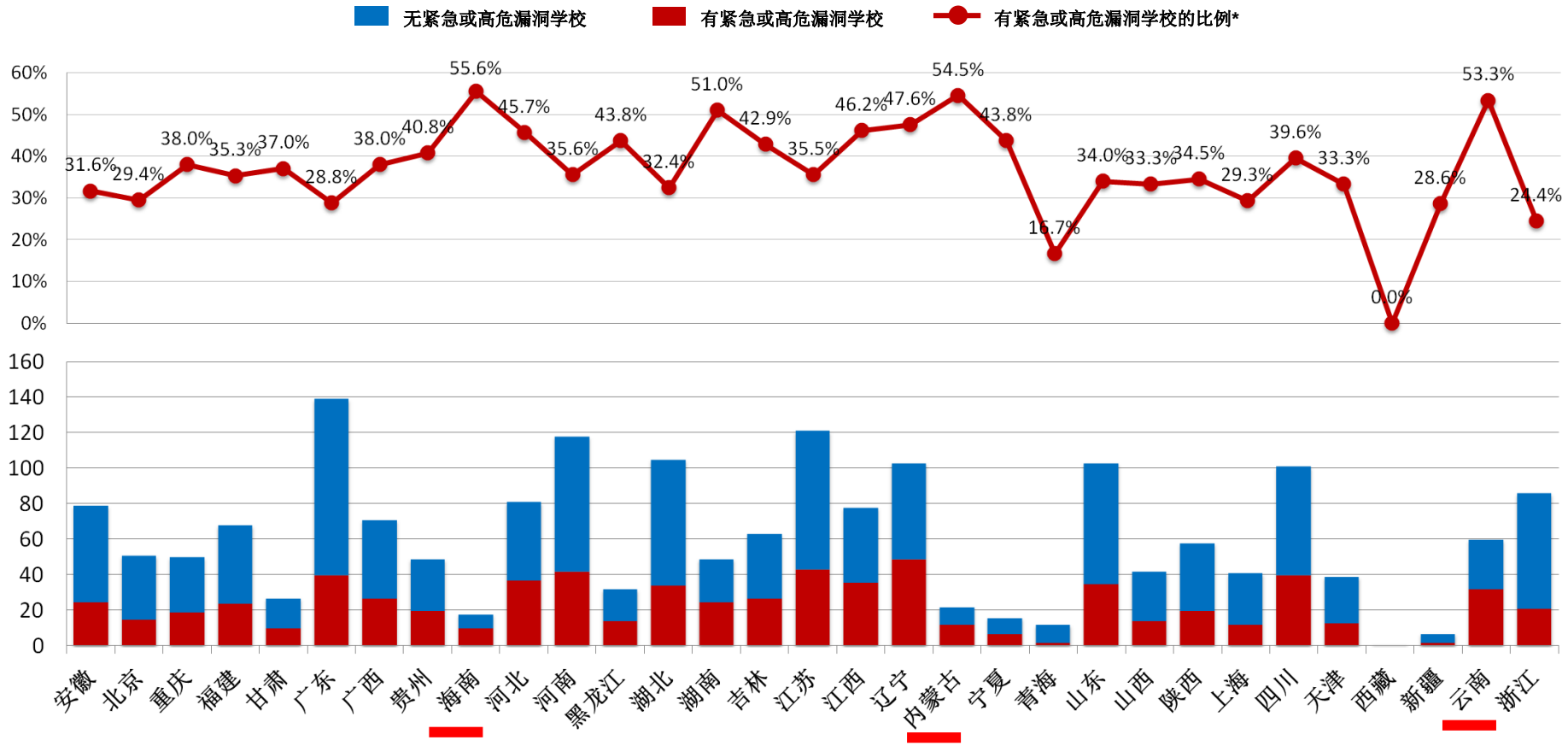
初检时间：2018年5月17日至6月20日

初检完成：1890 所高校， 2100 个网站

	漏洞数量（个）		学校数量（所）	
	2018	2017	**2018**	2017
紧急漏洞	171	-	135	-
高危漏洞	5,678	37,641	662	693
中危漏洞	27,479	10,889	1,615	689
低危漏洞	45,638	1,203,130	1,530	1,592

高校招生网站安全检测

初检各省有紧急和高危漏洞的学校数量



* 仅统计初检完成扫描的学校

新型网络攻击手段分析

- 物联网设备攻击（摄像头、智能家居、汽车等）
- 移动互联网攻击（手机病毒、钓鱼WiFi等）
- 关键信息基础设施攻击（电网、水利及交通等）

著名黑客：巴纳比·杰克攻击ATM机和心脏起搏器

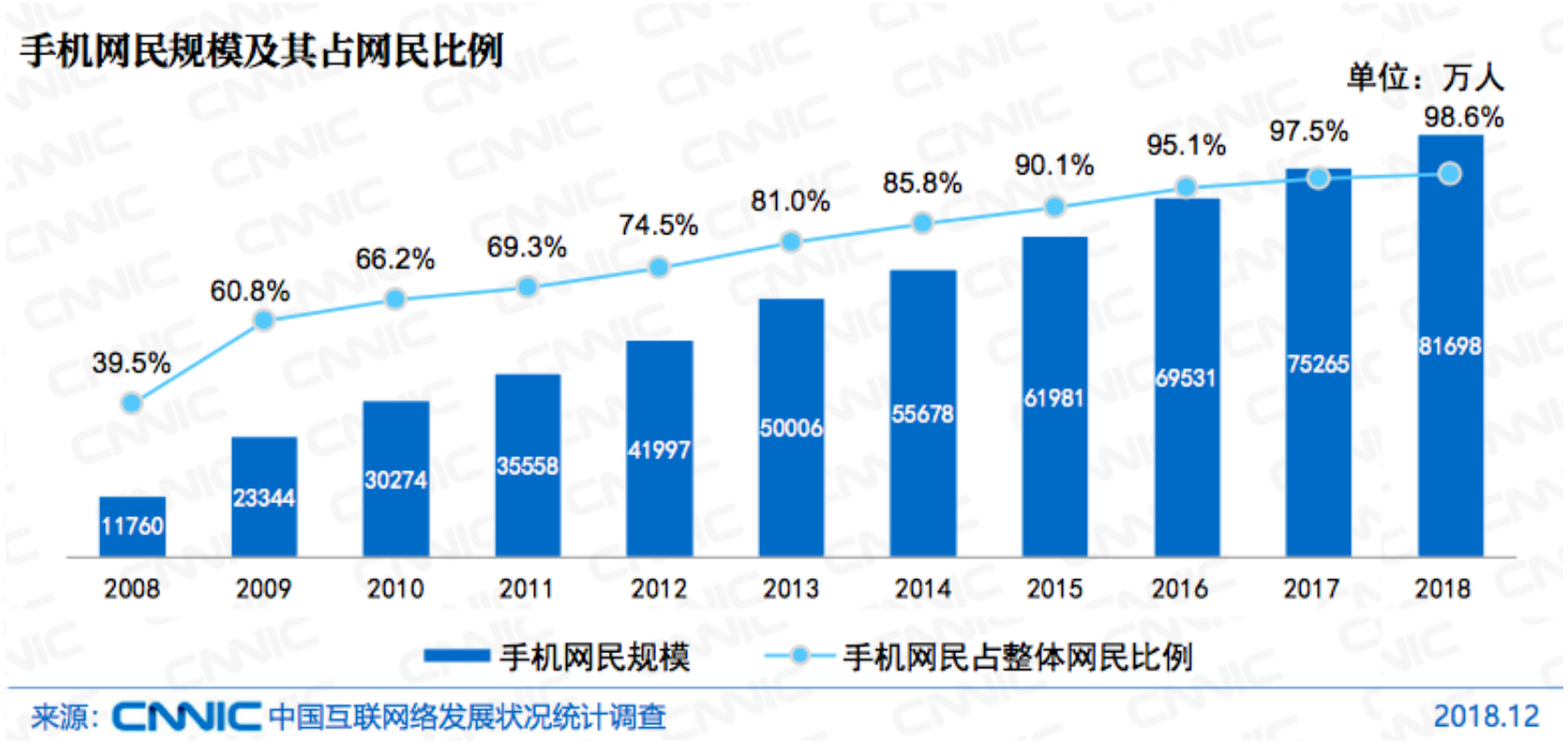
- 巴纳比·杰克(Barnaby Jack），(1977年12月 - 2013年7月)是一位新西兰的黑客、程序员和计算机安全专家。他因在2010年黑帽子大会上演示了入侵ATM取款机并当场让ATM取款机吐出钱而引起广泛关注。
- 黑帽大会自1997年创立以来,每年在美国拉斯维加斯召开。2010年有大约7000名黑客和网络安全专家出席了本次“黑帽大会”开幕式。
- 2013年，他还计划在8月份举行的黑帽子大会上演示如何入侵心脏除颤器和心脏起搏器。可以在距离目标50英尺（约15米）的范围内侵入心脏起搏器，并让起搏器释放出足以致人死亡的830V电压。
- 但是他在7月25日被发现死于旧金山的公寓中。

攻击摄像头

- 近年来，随着智能手机、可穿戴设备、智能摄像头等终端设备的迅速发展和普及应用，给人们生活带了便利。但由于安全意识薄弱，使用初始密码等弱口令进行登录，致使智能设备存在被黑客攻击的安全风险隐患。
- 2017年6月，媒体报道，有人在QQ群中兜售远程控制家庭摄像头的破解软件，并有大量人员非法购买后利用摄像头进行偷窥，公民个人隐私被严重侵犯。
- 北京警方耗时19天破获该案，成功打掉了全国首例网上传播家庭摄像头破解软件的犯罪链条，抓获涉案人员24名。**涉案QQ群组及账号达5000余个**。
- 出售破解软件人员党某因涉嫌《刑法》第285条非法获取计算机信息系统数据罪被刑事拘留。

移动互联网攻击-手机网民统计

- 截止2018年12月，我国手机网民规模达8.17亿,网民中使用手机上网的比例由 2017 年底的97.5%提升至98.6%,手机网民规模继续保持稳定增长。



移动互联网攻击-手机恶意程序

2018 年，捕获的手机恶意程序数量283万余个，较 2017年增长 11.7%，主要 针对安卓平台。

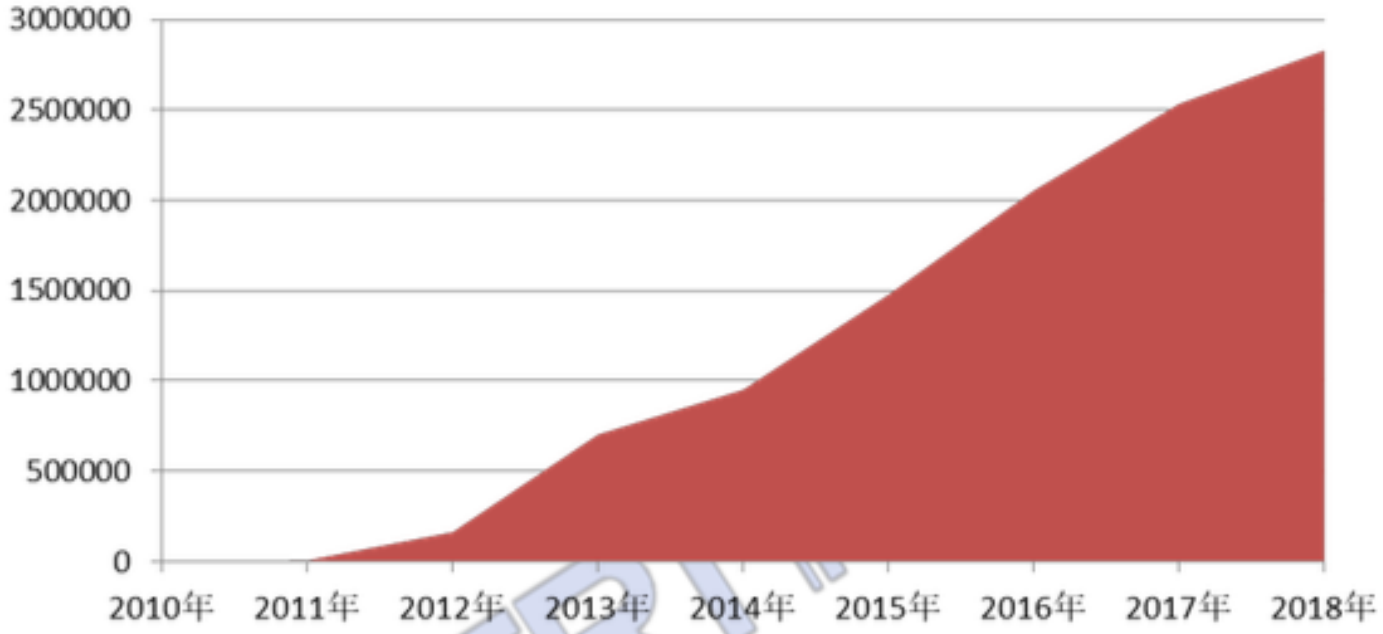


图 6 2010 年至 2018 年移动互联网恶意程序捕获数量走势

移动互联网攻击-钓鱼WiFi

黑客搭建诱骗WiFi，伪装成餐厅、单位等正常无线网络，并且通常不设置密码。当用户贪图便宜接入时，黑客偷偷的监听网络数据，窃听未经过加密处理的账号、密码和网银等个人信息。

钓　　新华社发 蒋跃新 作

智能家居攻击

- **对物联网(IoT)的攻击将聚焦智能家居自动化**
- 在Defcon 2015黑客大会上就发布了25个物联网设备以前未知的漏洞，涉及设备包括智能体重秤、智能冰箱、监控摄像头、智能微波炉、婴儿监视器等智能设备等，均存在被入侵的安全隐患。

视频监控设备攻击

- 2015年，主营安防产品的海康威视生产的视频监控设备被曝严重的安全漏洞，被黑客组织入侵和控制。遍布于金融、智能交通、公安、能源、司法等领域。视频监控设备被不法分子控制，必然会导致敏感图像信息被情报机构获得，例如政府部门内部监控图像、银行内部监控图像、交通监控图像、宾馆监控图像等。

智能汽车攻击

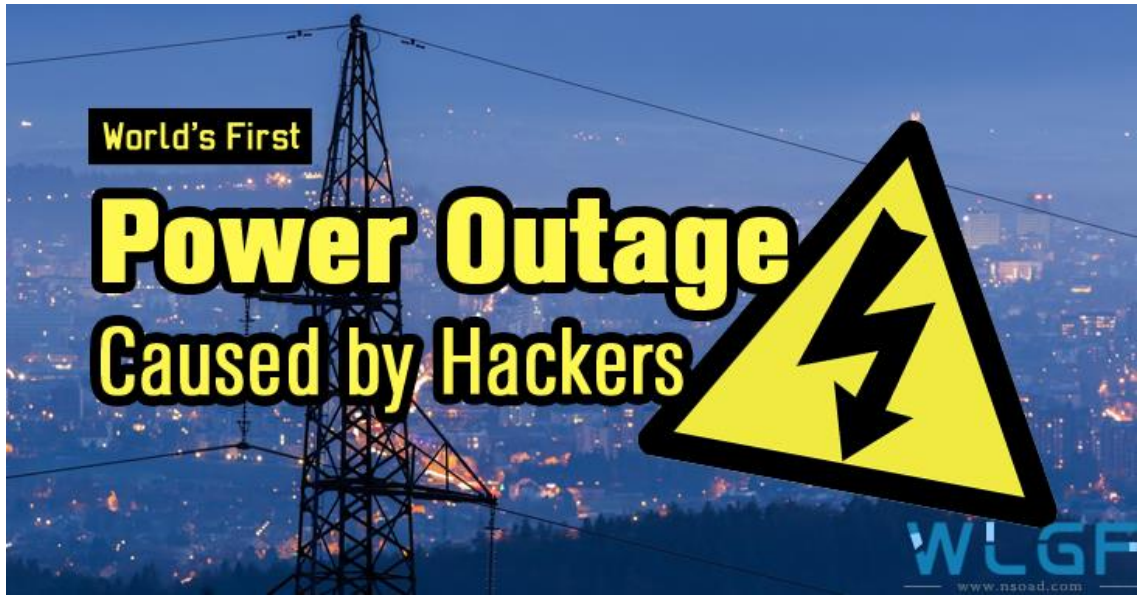
- 一些智能汽车可以很容易地被入侵，不仅获得信息，甚至可远程操控汽车的某些功能。
- 在BLACKHAT2015会议上远程破解了一辆未经改装的汽车，此举震惊了整个汽车行业。同年2月，宝马的ConnectedDrive 服务被曝出漏洞，通信没有使用HTTPS进行加密传输，泄露了包括VIN、控制指令等信息，黑客可以随意打开车门，启动汽车，为此宝马召回220 万辆汽车。

关键信息基础设施攻击

- 随着工业信息化进程的推进，计算机及网络通信等技术在智能电网、交通、石油化工、核工业、水利、采矿等国家重要的生产行业中运用。
- 这使得工业控制系统也必将面临病毒、黑客入侵、拒绝服务等安全威胁，其安全事故造成的社会影响和经济损失会更为严重。

乌克兰电力攻击

- 2015年12月23日，乌克兰电力供应商通报了持续三个小时的大面积停电事故。后经调查发现，停电事故为网络攻击导致。攻击者使用附带有恶意代码的Excel邮件附件渗透了某电网工作站人员系统，向电网网络植入了BlackEnergy恶意软件，获得对发电系统的远程接入和控制能力。



南美五国大停电，政府称不排除网络攻击

- 2019年6月16日，南美洲的阿根廷和乌拉圭两国发生了全国范围的大规模停电，有超过4800万人受影响。大停电还波及了巴拉圭、巴西南部以及部分智利城市，当地居民原本平静的周末变得混乱不堪。
- 交通几乎全部瘫痪
- 居民用水和网络通信都受到影响
- 餐厅及店铺提供蜡烛或关门
- 阿根廷民众地方选举投票被推迟

伊朗攻击美国大坝

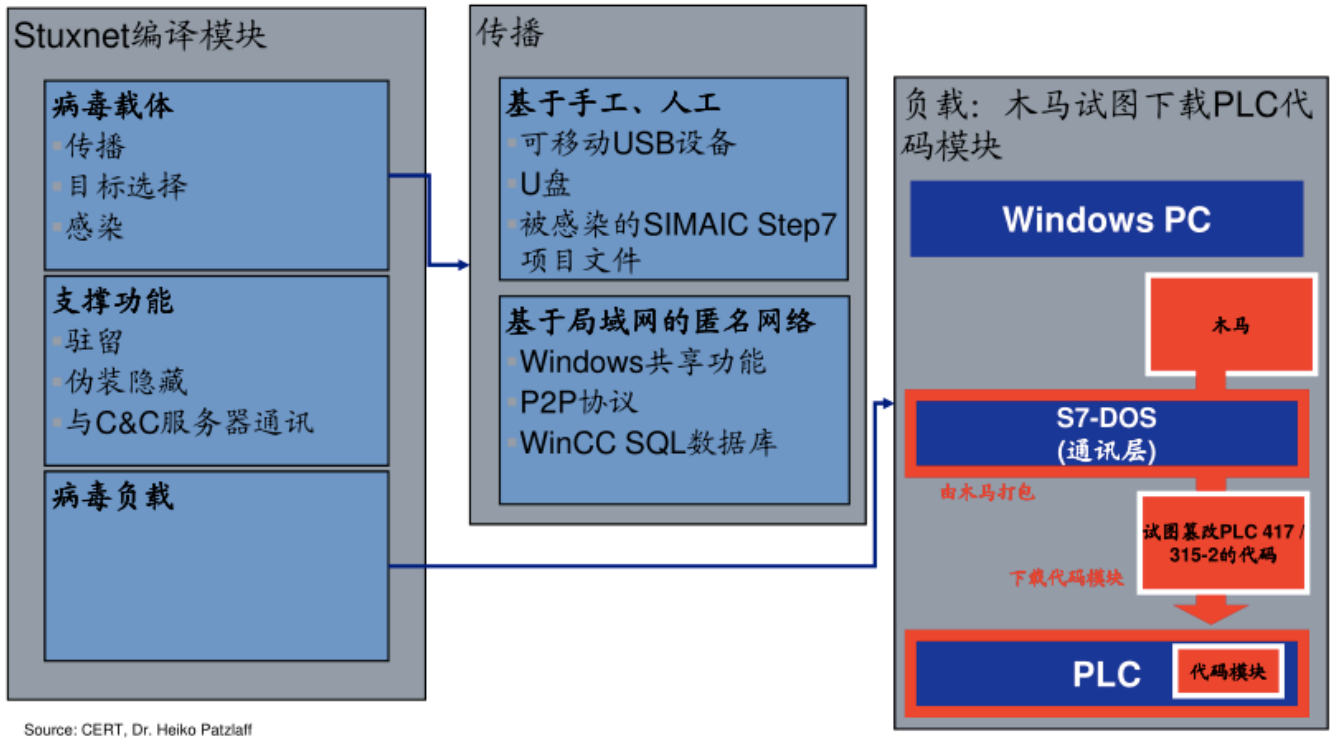
- 2016年3月，美国司法部公开指责7名伊朗黑客入侵了纽约鲍曼水坝（Bowman Avenue Dam）的一个小型防洪控制系统。幸运的是，黑客还没有完全获得整个大坝计算机系统的控制权，仅只是进行了一些信息获取和攻击尝试。这些伊朗黑客可能为伊朗伊斯兰革命卫队服务，他们还涉嫌攻击了包括摩根大通、美国银行、纽约证券交易所在内的46家金融机构。

工业信息安全-核电站(震网病毒)

- 2006年，伊朗重启核计划，在核工厂安装大批离心机，生产浓缩铀，为进一步制造核武器准备原料。
- 经军事威胁和经济制裁无效，美国和以色列开始秘密研发针对核工厂破坏的病毒。美国人甚造了一座模拟核工厂，招募了一批顶级黑客和核工程专家。

工业信息安全-核电站(震网病毒)

“震网”代码非常精密，主要有两个功能，一是使伊朗的离心机运行失控，二是掩盖发生故障的情况，以“正常运转”记录回传给管理部门，造成决策的误判。在攻击中，伊朗纳坦兹铀浓缩基地至少有1/5的离心机因感染该病毒而被迫关闭。



Source: CERT, Dr. Heiko Patzlaff

工业信息安全-核电站(震网病毒)

- 2008年，伊朗内贾德总统视察核工厂，他沉重的心情反映到脸上。
- 不过这并不重要，真正关键的是该图片不经意地泄露了核工厂的问题：左下方的屏幕显示的点，每一个都代表一台离心机，绿色代表运行正常，夹杂的两个灰色小点，则说明有两台离心机出了故障。

关键基础设施的安全问题

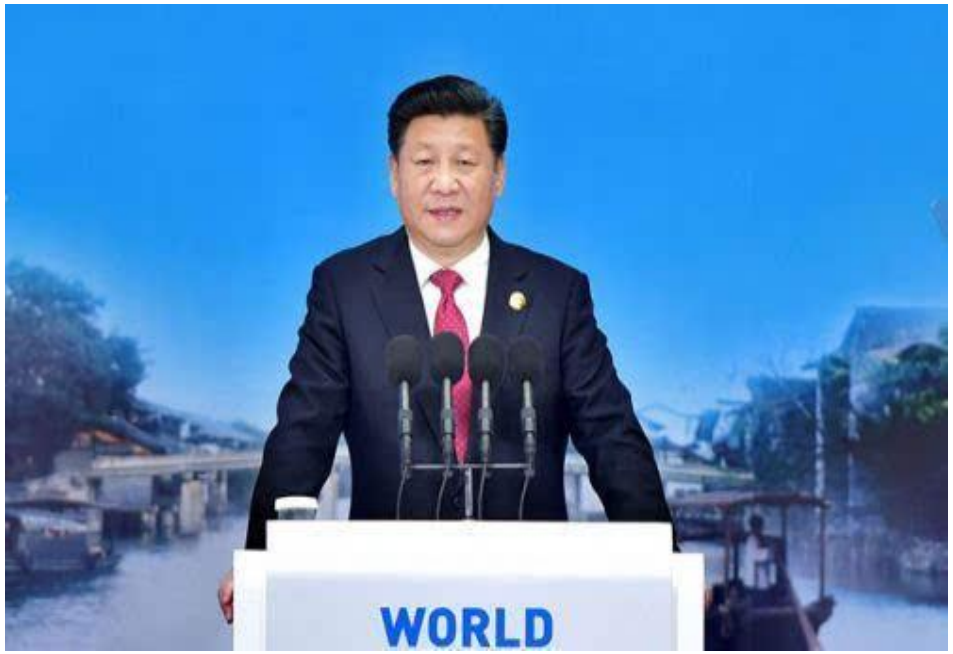
关键基础设施关系到国家的安全、社会稳定，交通、能源、电力、教育、医疗、水利等重要信息系统一旦受到攻击，将造成巨大的损失。

出于政治、军事、经济等目的，黑客组织以及恐怖分子都可能把民航、铁路、电力等重要信息系统作为攻击目标。必须要提前做好安全防护和应急预案。

网络安全上升为国家战略

- 2014年2月，中央网络安全和信息化建设领导小组成立，“没有信息化就没有现代化，没有网络安全就没有国家安全”。网络空间成为继海陆空天之后的“第五空间”（领网）。

- 2015年12月，第二届世界互联网大会在乌镇举行，习主席在发言中指出：世界范围内侵害个人隐私、侵犯知识产权、网络犯罪等时有发生，网络监听、网络攻击、网络恐怖主义活动等成为全球公害。



《国家网络空间安全战略》发布

- 由国家互联网信息办公室于2016年12月27日发布并实施。
- 《战略》明确，当前和今后一个时期国家网络空间安全工作的战略任务是**坚定捍卫网络空间主权、坚决维护国家安全、保护关键信息基础设施、加强网络文化建设、打击网络恐怖和违法犯罪、完善网络治理体系、夯实网络安全基础、提升网络空间防护能力、强化网络空间国际合作**等9个方面。
- 《战略》是为了贯彻落实习近平关于推进全球互联网治理体系变革的“四项原则”和构建网络空间命运共同体的“五点主张”。

《网络安全法》实施

《网络安全法》于2017年6月1日起正式施行，意味着我国向建设网络强国的制度保障迈出坚实的一步。主要有以下重点内容

- 确立了网络空间主权原则，将网络安全顶层设计法制化；
- 对关键信息基础设施实行重点保护；
- 加强个人信息保护，加大对网络诈骗等犯罪的打击力度；
- 实名认证制度。；
- 重要数据强制本地存储制度和境外数据传输审查评估制度；
- 网络通信管制制度。

《网络安全等级保护制度2.0》国家标准发布

- 等保2.0相关国家标准于5月13日正式发布，2019年12月1日开始实施。
- 网络安全等级保护制度对国家网络安全保障有着不可替代的作用。
- 等保2.0标准在1.0标准的基础上，注重全方位主动防御、安全可信、动态感知和全面审计，实现了对传统信息系统、基础信息网络、云计算、大数据、物联网、移动互联和工业 控制信息系统等保护对象的全覆盖。

《公安机关互联网安全监督检查规定》施行

- 公安部发布的《公安机关互联网安全监督检查规定》自2018年11月1日起施行。《规定》适用于公安机关依法对互联网服务提供者和联网使用单位履行法律、行政法规规定的网络安全义务情况进行的安全监督检查。
- 公安机关开展监督检查，可以采取进入营业场所、机房、工作场所，要求监督检查对象的负责人或者网络安全管理人员对监督检查事项作出说明，查阅、复制与互联网安全监督检查事项相关的信息、查看网络与信息安全保护技术措施运行情况等措施。

谢谢！