西安理工大学
XI'AN UNIVERSITY OF TECHNOLOGY

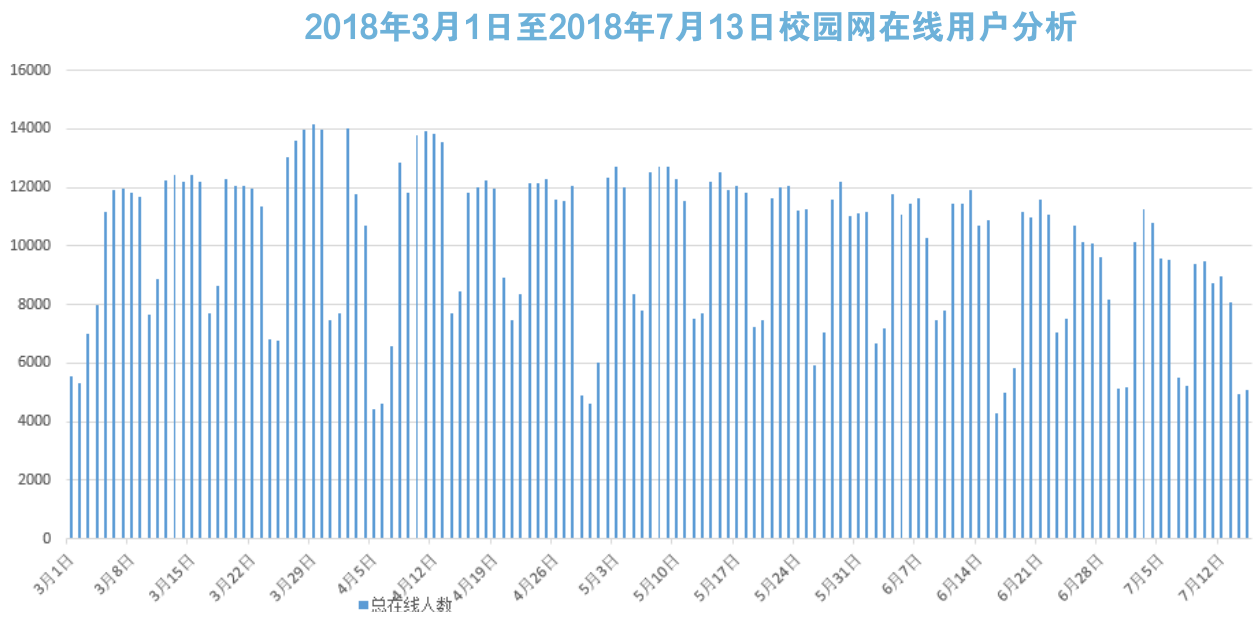
2018年度春季学期

校园网运行与安全简报

2018

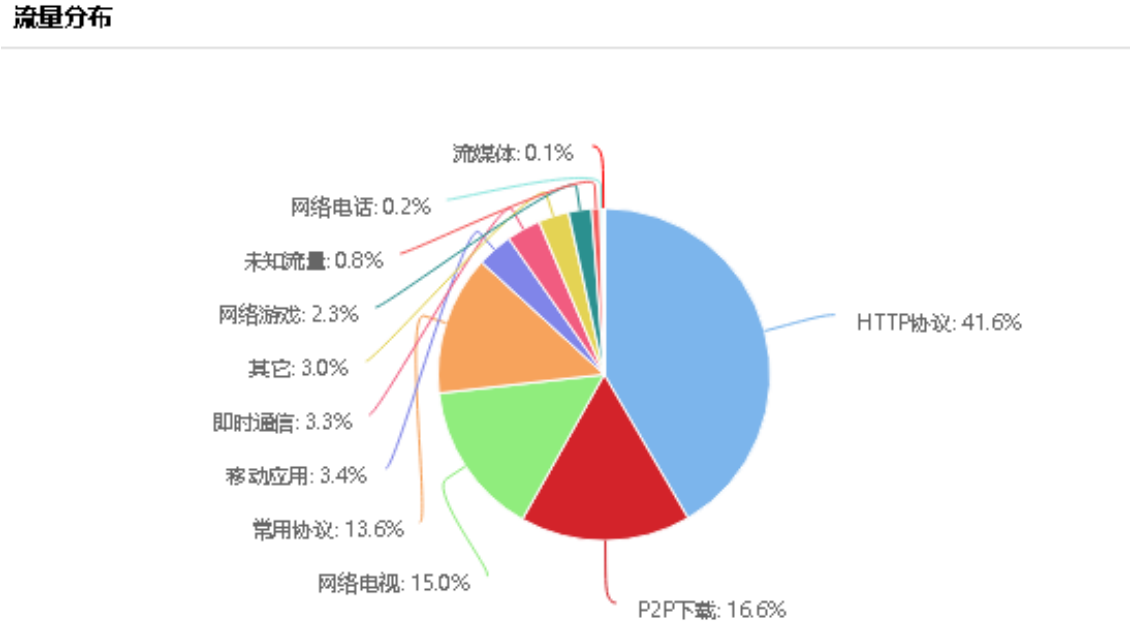
校园网用户统计、流量分布

本学期，校园网整体运行正常，日均在线用户1.2万人左右，其中无线用户日均在线7000人。



校园网出口峰值带宽约10G，2018年3月1日-2018年7月1日，校园网总下载流量达3000T，上传流量共计1000T。

其中，浏览器日常访问产生流量占比41%左右，迅雷等P2P下载流量及网络电视相关应用分别占比约17%和15%。

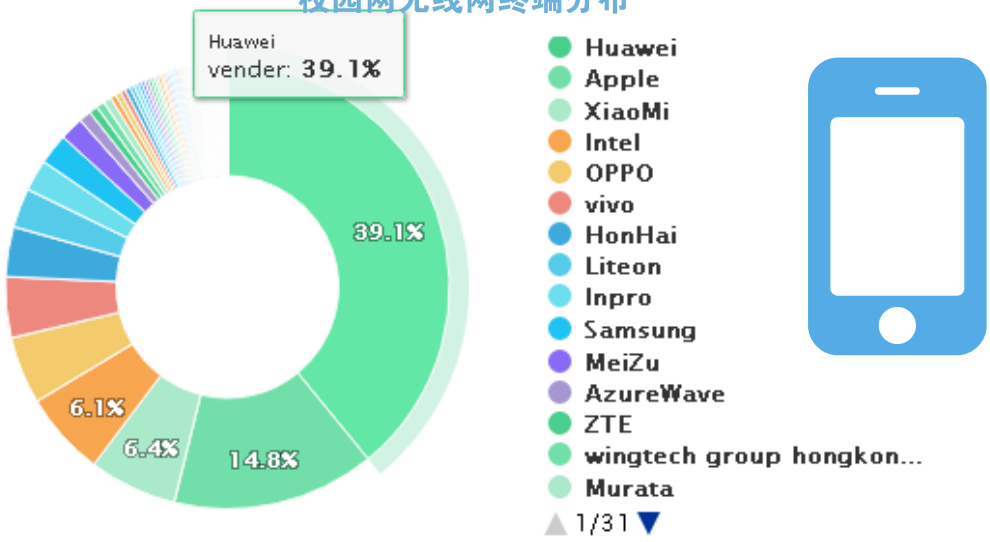


校园网大数据

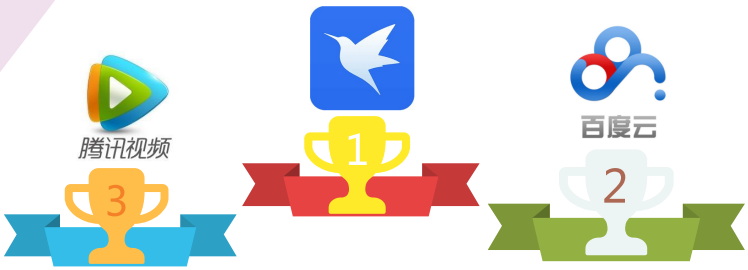
从校园无线网终端数量统计数据可以看出，我校用户在网终端主要以华为手机或平板为主，苹果和小米位列二、三位。

校园有线及无线网流量统计数据显示，迅雷下载高居我校流量榜首位，百度云作为大众常用的云数据网盘排名第二，腾讯视频成为校园最受欢迎视频应用。

校园网无线网终端分布



校园网TOP10应用



4 链克 迅雷链克

5 爱奇艺 爱奇艺视频

6 PPStream

7 bilibili B站

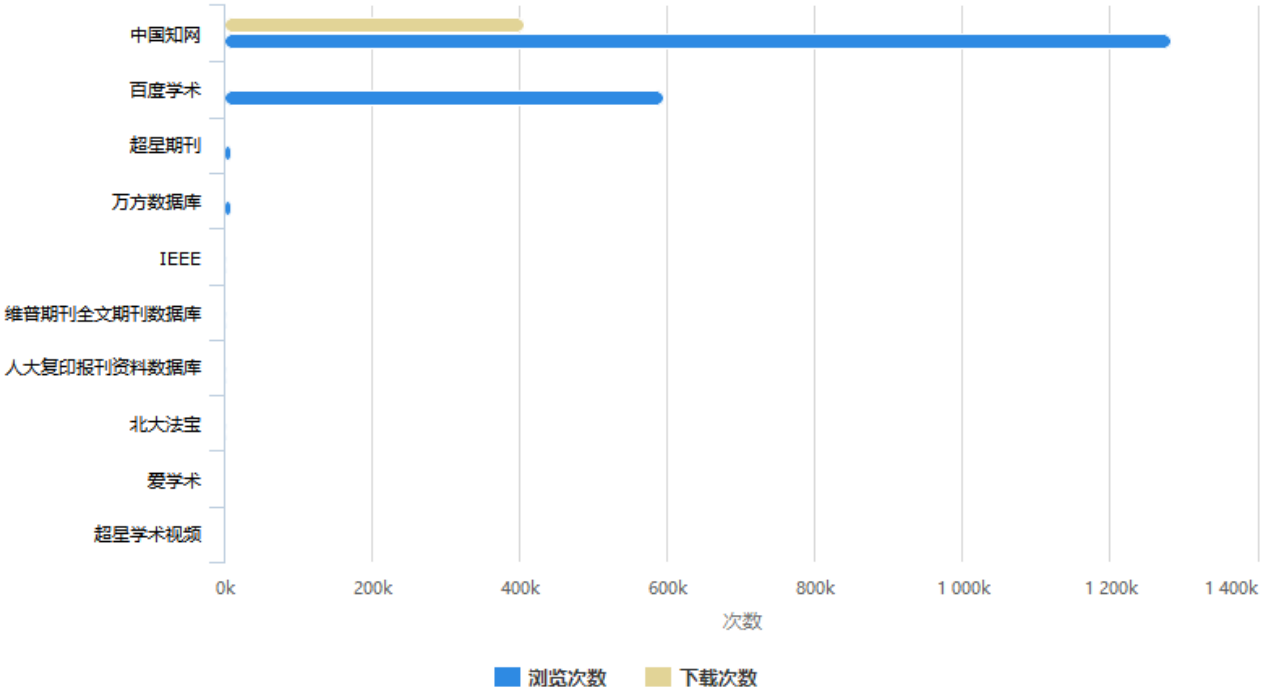
8 斗鱼直播

9 抖音APP

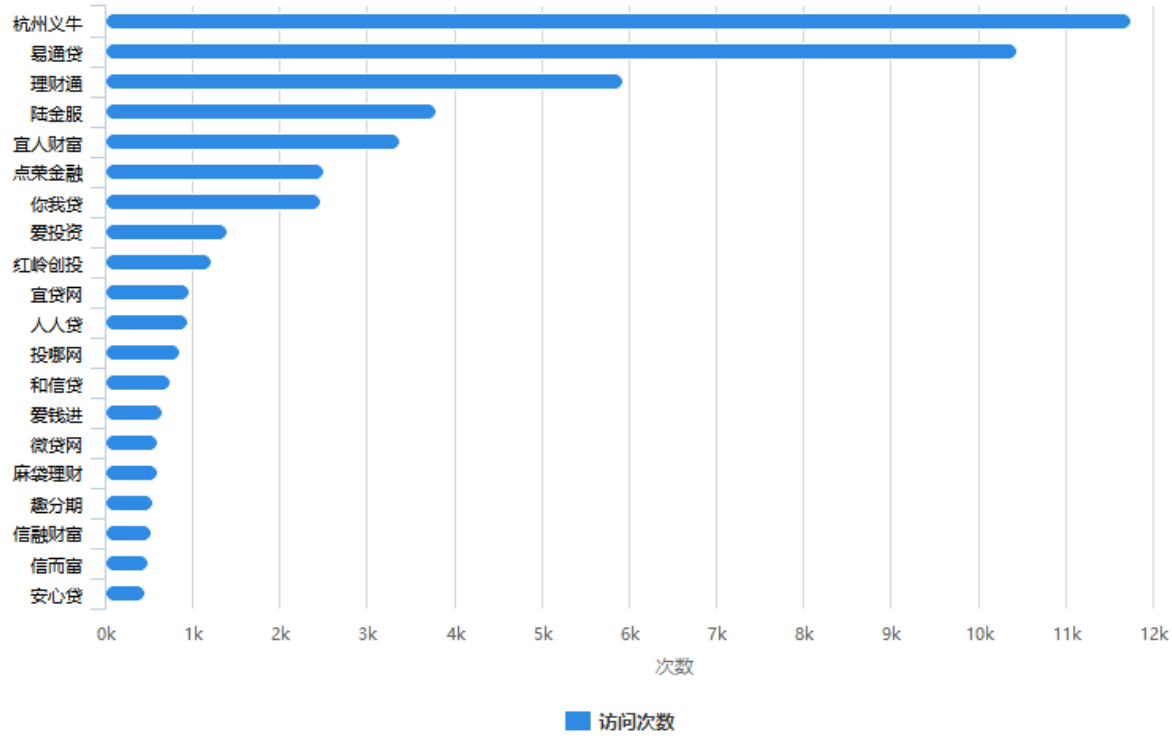
10 快手APP

校园网大数据

图书资源访问情况



金融APP访问情况



关于无线校园，你应该知道的几件事

无线WIFI的2.4G和5G代表的意义和区别

2.4G和5G分别代表了两种不通的技术标准， 两者各有优缺点：

频段	2.4G	5G
优点	2.4G信号工作频率低，传播时衰减小，传播距离更远。	5G信号频段宽，无线环境干净，干扰少，网速稳定，且5G可以支持更高的无线传输速率。
缺点	2.4G信号频宽较窄，信道量少，家电、无线设备大多使用此频段，无线环境拥挤，干扰较大。	5G工作频率较高，传播时衰减较大，覆盖能力不如2.4G。

我校无线校园网运行现状

我校无线校园网建设均采用业界主流无线双频设备，智能化5G优先接入技术，实时动态的终端连接优化技术。我校两期无线网建设共计安装1479台无线设备（主设备），覆盖金花、曲江共计36座楼宇以及餐厅、足球场、活动中心等各类公共场所，日均累计服务用户2万余人次。

无线网“无感知认证”是什么？

“无感知”认证技术，具体是指对于终端用户来说，无线网络的准入过程没有感知，即无需繁琐的账号密码输入、校验过程，即可实现无线的安全接入。

如何查看和设置无线网“无感知认证”？

我校“无感知认证功能”暂时只对教师开放测试权限，每个账户默认只能绑定一台“无感知认证”设备，默认绑定首次登录无线网的设备，用户可以登录SAM用户自助服务系统（http://sam.xaut.edu.cn/selfservice/）查看或解绑。

如何让无线网更快？

1.采用支持5G频段网络的设备。

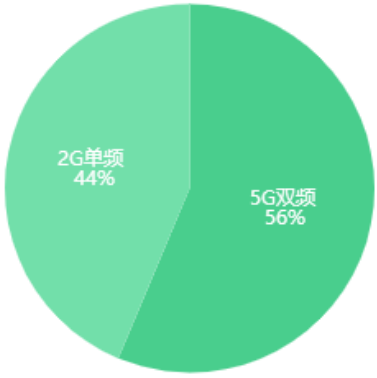
5G频段支持更多无线信道，用户分布均匀，信号干扰较少，网络数据传输速度快。

2.保障收发终端设备功率。

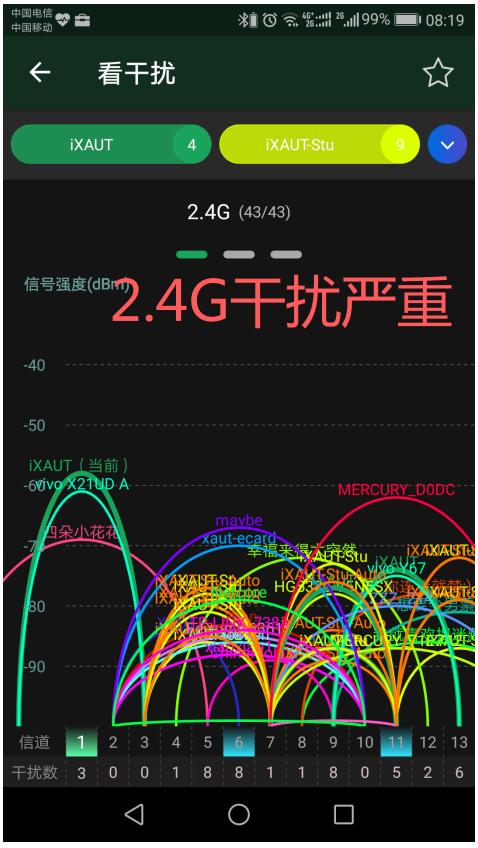
部分计算机使用的便携式网卡，因功率不足导致数据传输不稳定，总体网速缓慢。

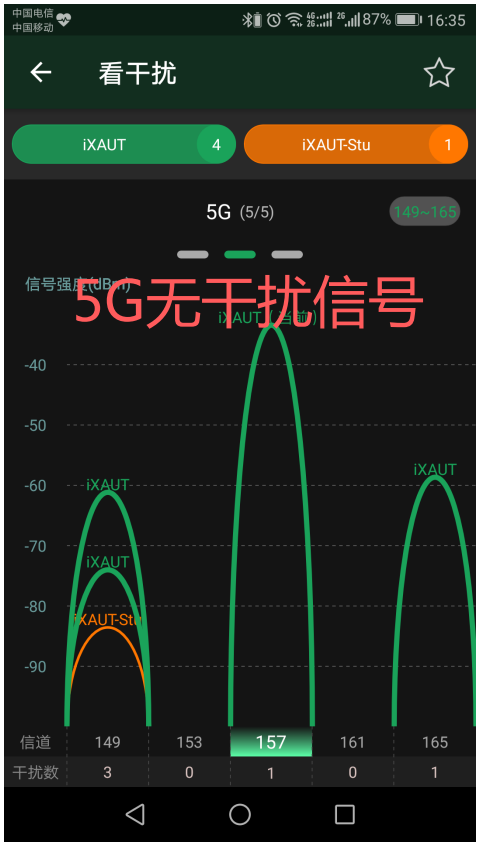
3.减少周围无线信号干扰。

我校办公区域因私设路由器过多，导致用户上网信道饱和，尤其2.4G频段干扰元数量庞大，校园网5G用户只占总用户数55%。



主动关闭教研室内的路由器无线功能或直接用有线交换机替代，可以更好的保障校园无线信号的稳定性。另外，部分无线设备被金属柜体完全遮挡也是导致网络信号差的原因。





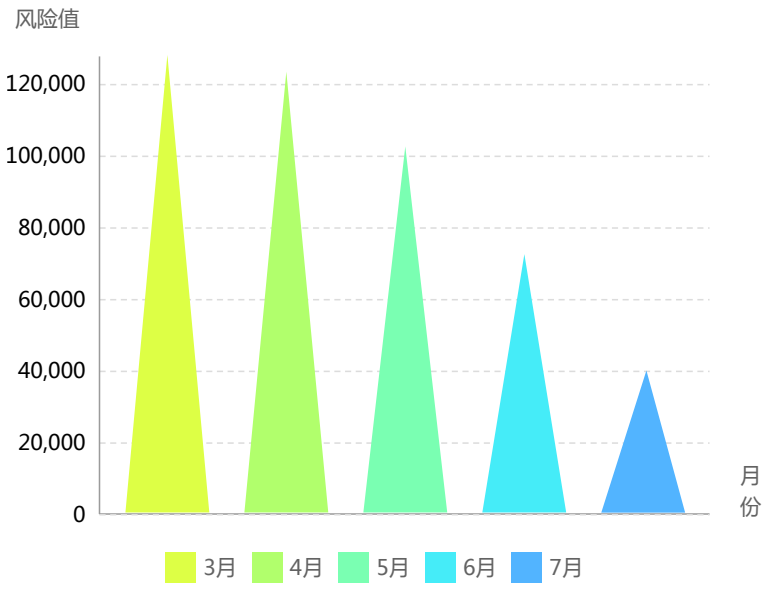
校园网络安全趋势

本周期统计以网络中心监测的数据作为主要依据，对我校192个信息系统（网站）面临的各类安全威胁进行总体态势分析。

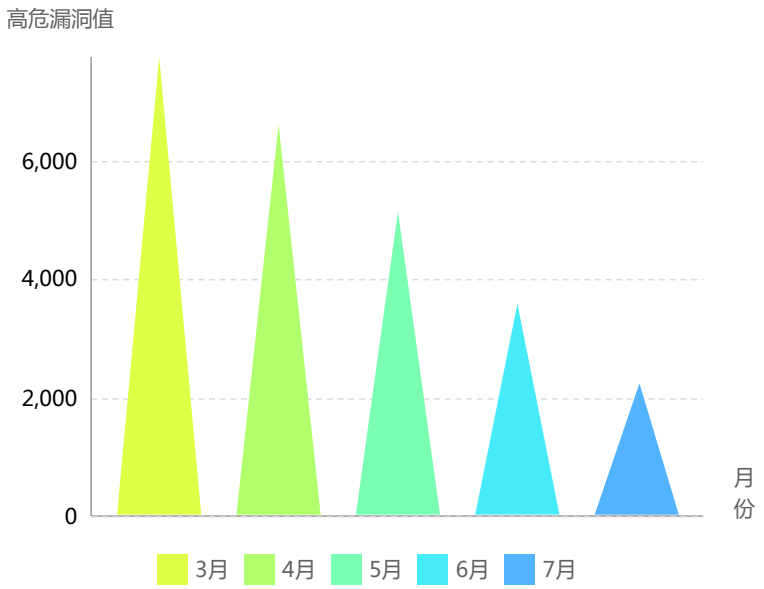
评估范围为：2018年3月1日-7月15日；自开学以来网络中心通过常态化安全监测、春季学期网络安全大检查及网络安全综合治理等一系列行动治理，我校网络安全状况整体评价为良。

2018年3月1日-7月15日网络安全态势分布图

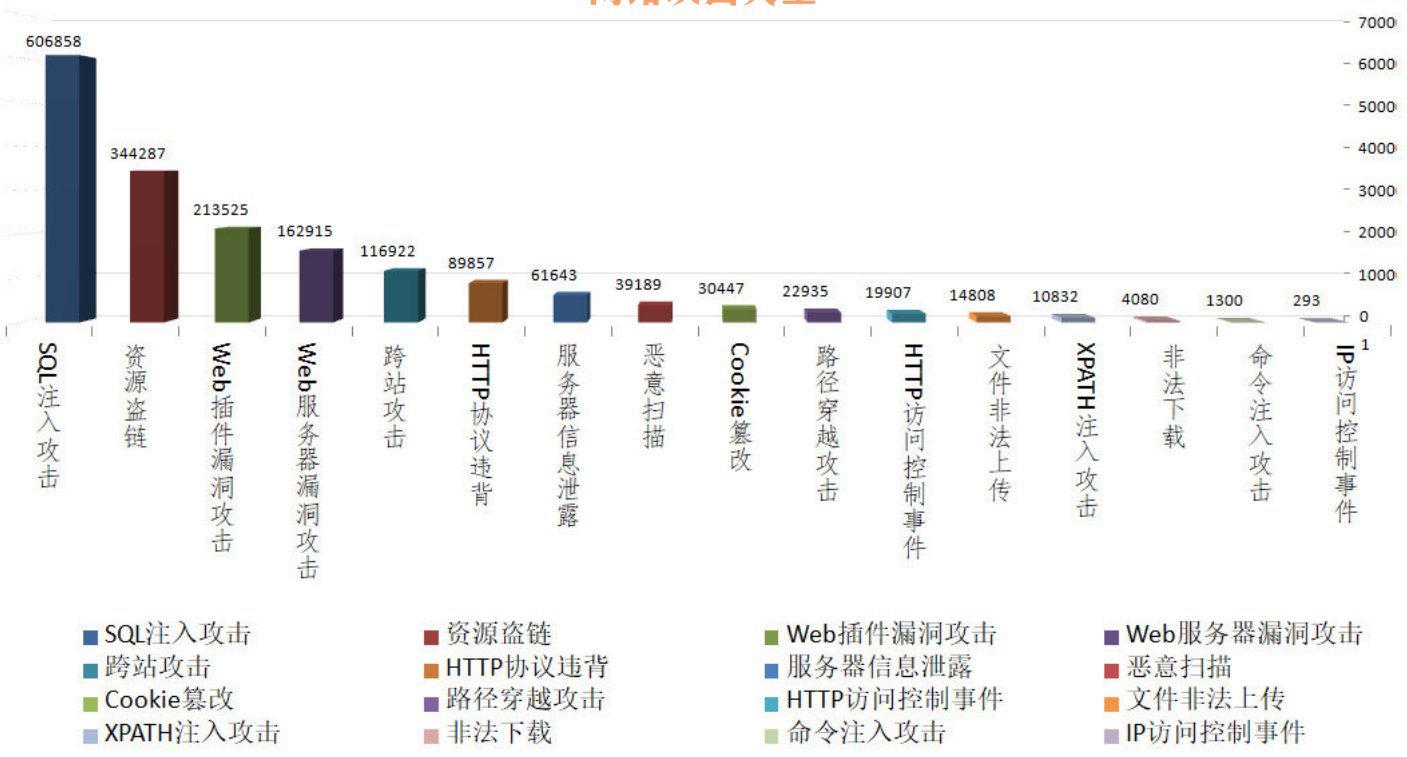
风险值趋势



高危漏洞趋势



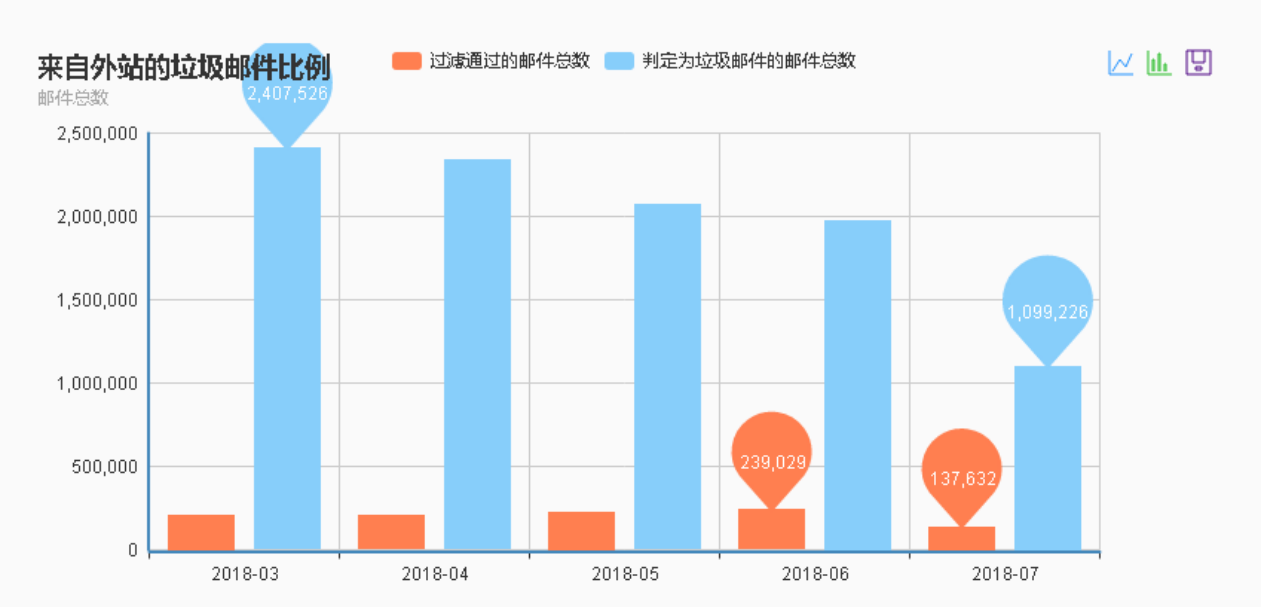
网络攻击类型



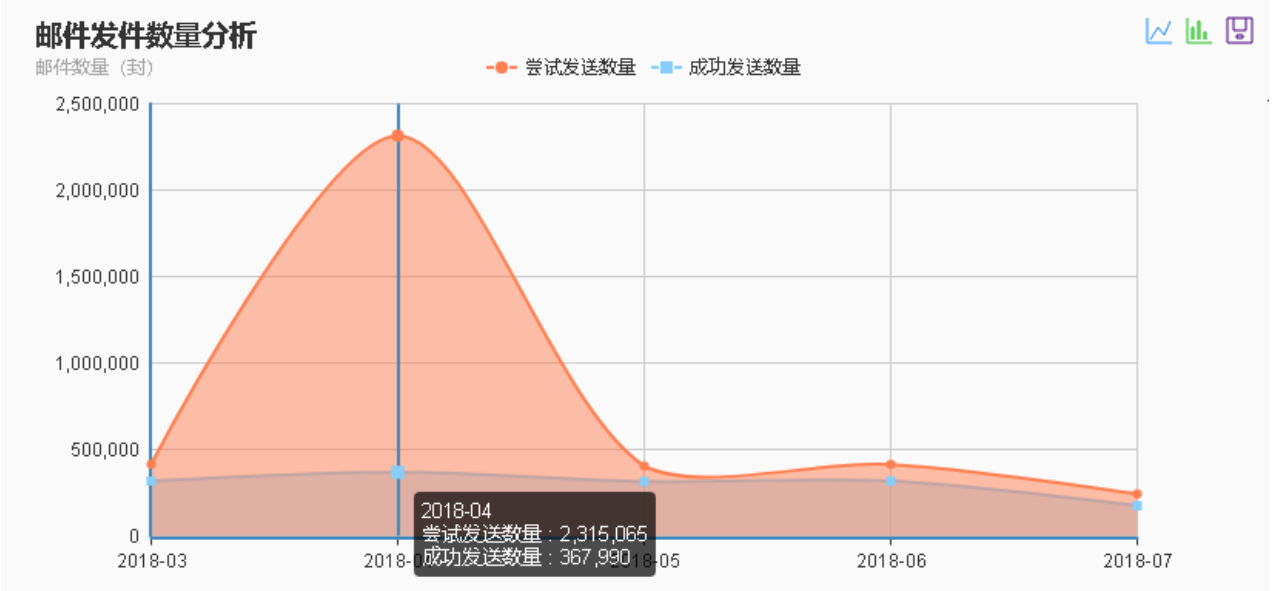
校园邮件系统运行数据

自2017年6月校园邮件系统正式运行至今，系统运行稳定，未出现服务终端故障，垃圾邮件拦截网关工作表现出色，月均拦截垃圾邮件近200万封。用户月均对外发送50万余封邮件。

校园邮件系统垃圾邮件拦截数据统计



校园邮件系统发件数据统计



潜伏在身边的黑客

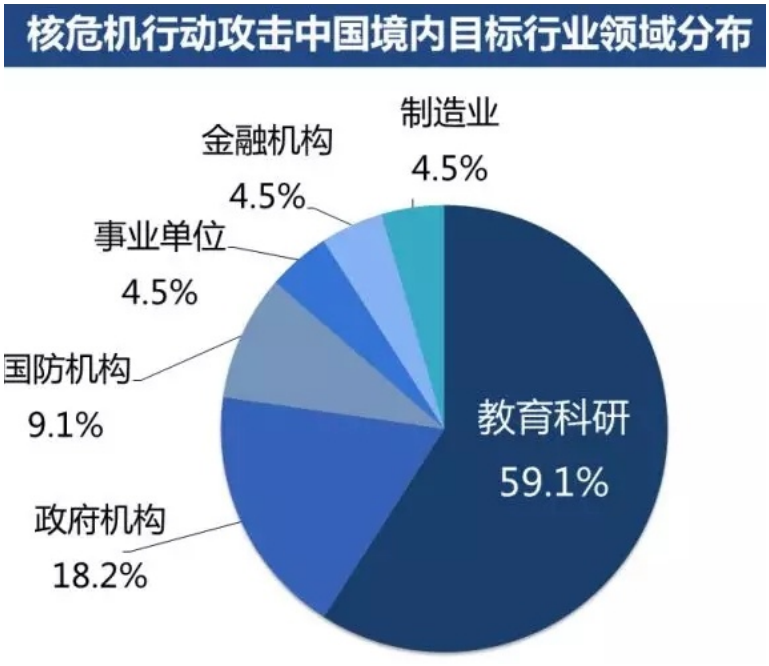
“蓝宝菇”	考虑到核武器爆炸时会产生蘑菇云，并结合该组织的一些其他特点及360威胁情报中心对APT组织的命名规则，将该组织命名为蓝宝菇。
核危机行动揭露（360威胁情报中心）	该组织相关恶意代码中出现特有的字符串（Poison Ivy密码是：NuclearCrisis），结合该组织的攻击目标特点，将该组织的一系列攻击行动命名为核危机行动（Operation NuclearCrisis）

攻击目的和受害分析

从2011年开始持续至今，高级攻击组织蓝宝菇（APT-C-12）对我国政府、军工、科研、金融等重点单位和部门进行了持续的网络间谍活动。该组织主要关注核工业和科研等相关信息。被攻击目标主要集中在中国大陆境内。

截止2018年5月，360追日团队已经监测到核危机行动攻击的境内目标近30个。其中，教育科研机构占比最高，达59.1%，其次是政府机构，占比为18.2%，国防机构排第三，占9.1%。其他还有事业单位、金融机构制造业等占比为4.5%。中国北京地区是核危机行动攻击的重点区域，其次是上海、海南等地区。

行业分布



核危机行动相关时间节点

- 2011年3月，首次发现与该组织相关的木马，针对政府相关机构进行攻击。
- 2011年11月，对某核工业研究机构进行攻击。
- 2012年1月，对某大型科研机构进行攻击。
- 2012年3月，对某军事机构进行攻击。
- 2012年6月，对国内多所顶尖大学进行攻击。
- 2013年6月，对某中央直属机构进行攻击，同时开始使用新类型的RAT。
- 2014年8月，发现该组织对重点目标机构进行大量横向移动攻击。
- 2014年12月，发现新的RAT，该后门具备窃取指定扩展名文档等重要功能。
- 2015年9月，针对多个国家的华侨办事机构进行攻击。
- 2018年4月，针对国内某重要敏感金融机构发动鱼叉邮件攻击。

重大漏洞预警

1 Windows与Microsoft Excel远程代码执行漏洞

成功利用Windows远程代码执行漏洞的攻击者，可以在目标系统上执行任意代码。

成功利用Microsoft Excel远程代码执行漏洞的攻击者，能在当前用户环境下执行任意代码，如果当前用户使用管理员权限登录，攻击者甚至可以完全控制该用户的系统。

解决方案:

目前，微软官方已经发布补丁修复了上述漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

2 手机程序第三方解压缩库输入验证安全漏洞

成功利用该漏洞的攻击者，可以远程读取应用数据、甚至执行任意代码，具体危害与受影响应用的功能和权限相关。iOS平台内置第三方解压缩库（经验证，包括但不限于SSZipArchive和ZipArchive两种库）的应用均可能受漏洞影响，安卓平台中使用第三方解压缩库进行解压缩的应用，如果没有对解压缩路径进行检查的可能也会受到漏洞影响。

解决方案：

目前，相关厂商暂未发布解决方案,但可通过临时解决方案缓解漏洞造成的危害，具体措施如下：

1.在解压缩时对最终路径做“../”文件名和符号链接的过滤。 2.使用 https 下载资源，或者对下载的文件进行校验防止被恶意修改。

3 微信支付官方SDK XXE漏洞

成功利用该漏洞的攻击者可以远程读取服务器文件，获取商户服务器上的隐私数据，甚至可以支付任意金额购买商品。使用有漏洞的Java版本微信支付SDK进行支付交易的商家网站可能受此漏洞影响。

解决方案:

目前，微信官方已经发布补丁修复该漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。