西安理工大学
XI'AN UNIVERSITY OF TECHNOLOGY

网络信息管理中心

信息化工作简报

2019年5月

目录

我校推进“双一流”建设暨建校70周年庆典活动网络直播保障工作圆满完成

5月1日，西安理工大学推进“双一流”建设暨建校70周年纪念大会在金花校区田径运动举行。全体校领导、部分校友和在校师生6000余名到场观看校庆仪式及文艺晚会，为确保海内外校友和社会各界人士通过网络直播共享校庆喜悦，网络信息管理中心积极配合做好基础网络搭建和网络保障工作，直播期间，网络流畅无异常。（李博鑫）

西安建筑科技大学来校调研信息化建设

5月20日，西安建筑科技大学信息网络中心副主任窦浩一行3人，来我校调研了有关“网络安全制度”、“数字化校园平台”及“数据治理”的建设及应用情况，会议由网络信息管理中心副主任侯小军主持。双方表示通过此次交流，有利于实现校园信息化建设经验共享和优势互补，希望在今后能够继续加强交流合作，共同推进两所兄弟学校信息化发展。（李宏伟）

《教育网络助力高校教学与科研》技术报告

5月13日，赛尔网络有限公司陕西分公司总经理刘明辉一行7人，来校做了题为《教育网络助力高校教学与科研》的技术报告，网络信息管理中心主任李军怀对赛尔网络的到访表示热烈欢迎，并就学校信息化建设情况进行了简要介绍，会议由副主任侯小军主持。（李宏伟）

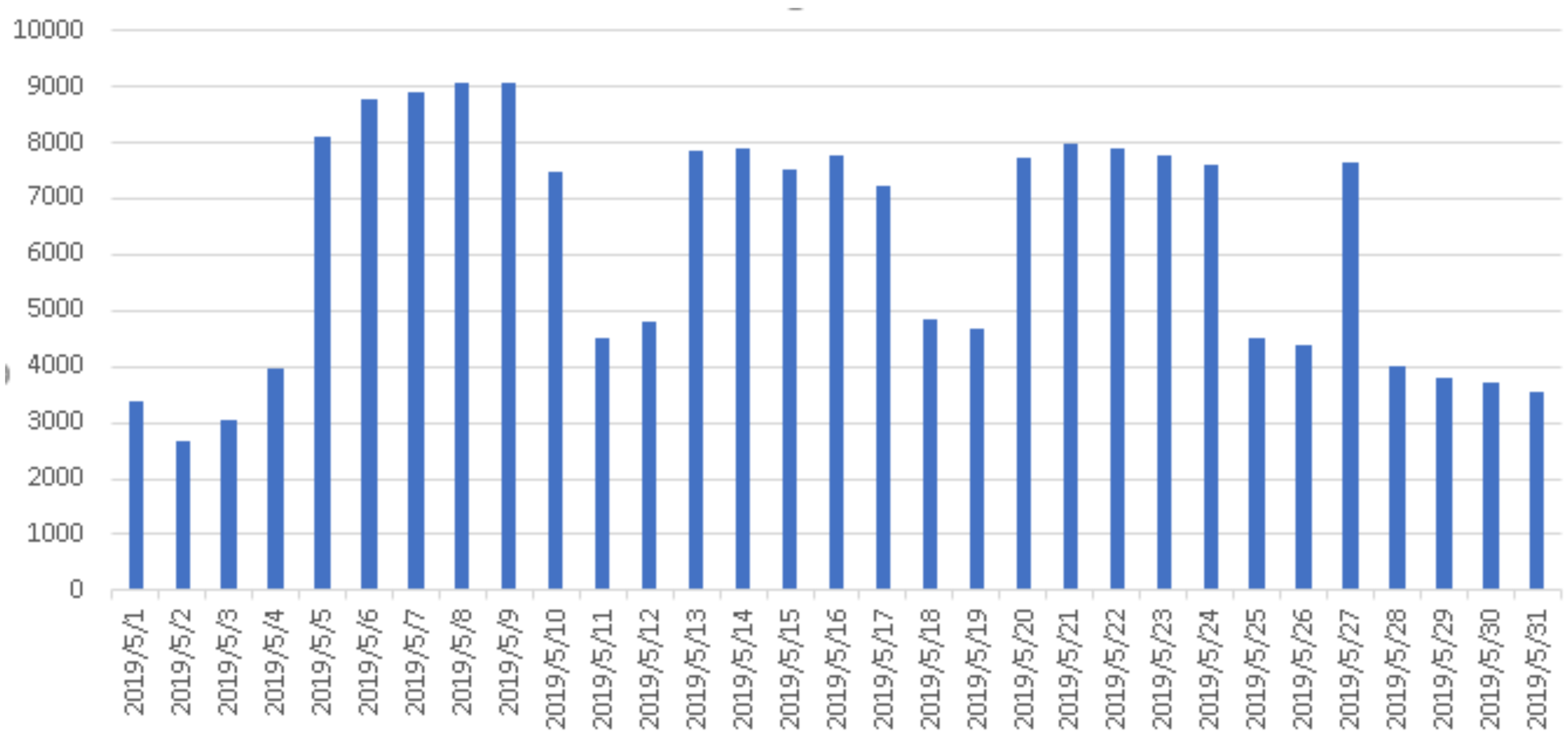
5月21日，甲骨文（中国）软件系统有限公司（西安）技术团队人员，来校做了《Oracle数据库应用与管理》的报告，网络信息管理中心相关技术负责人参加并学习。

5月22日，江苏金智教育信息股份有限公司（西安）技术团队人员，来校做了《主数据管理平台》的报告，网络信息管理中心相关技术负责人参加并学习。

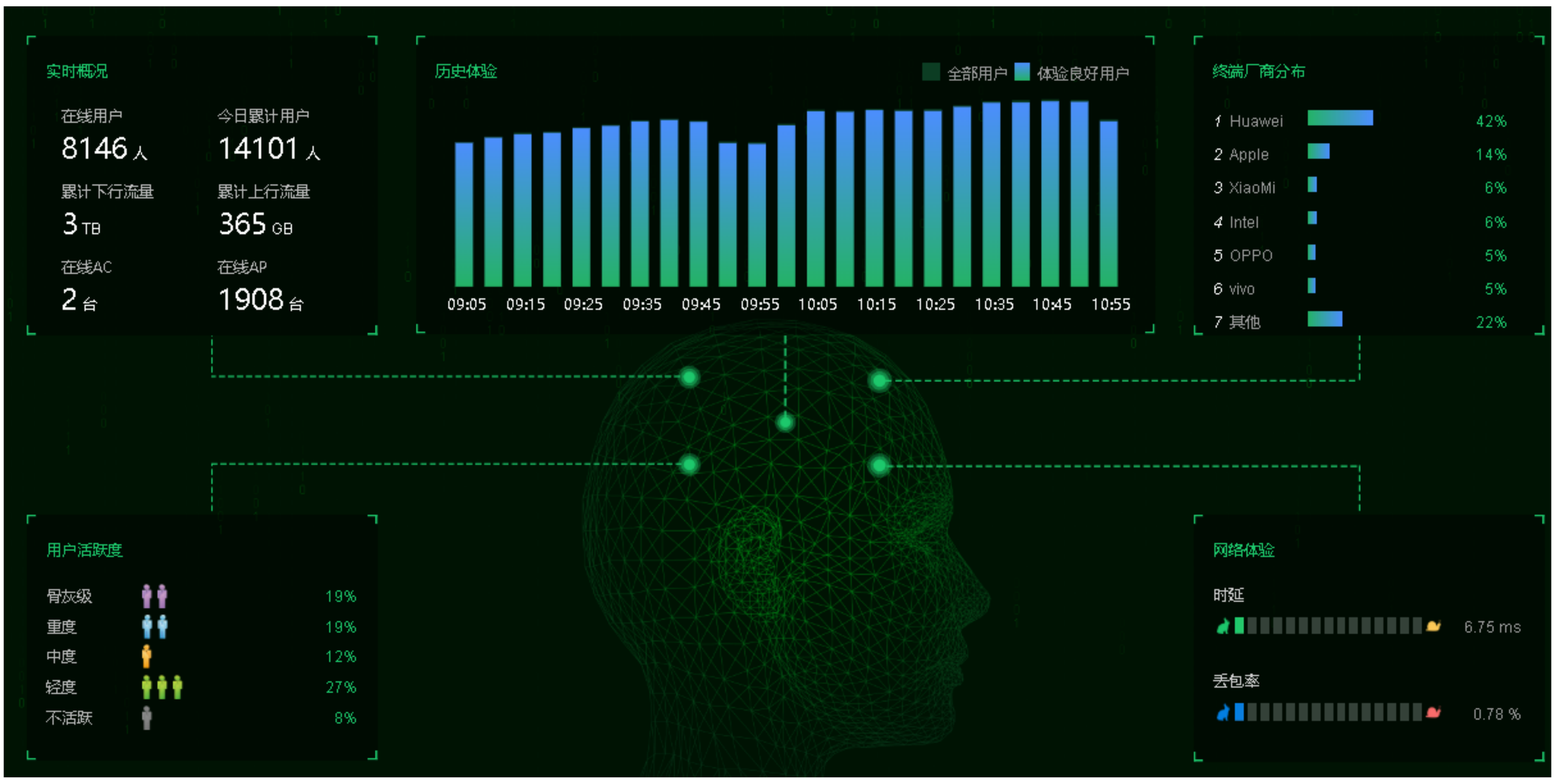
5月31日，西安尚易安华信息科技有限责任公司技术团队人员，来校做了《信息安全技术/网络安全等级保护基本要求（等保2.0）解读》的报告，网络信息管理中心相关技术负责人参加并学习。

校园网在线用户分析

2019年5月校园网在线用户分析

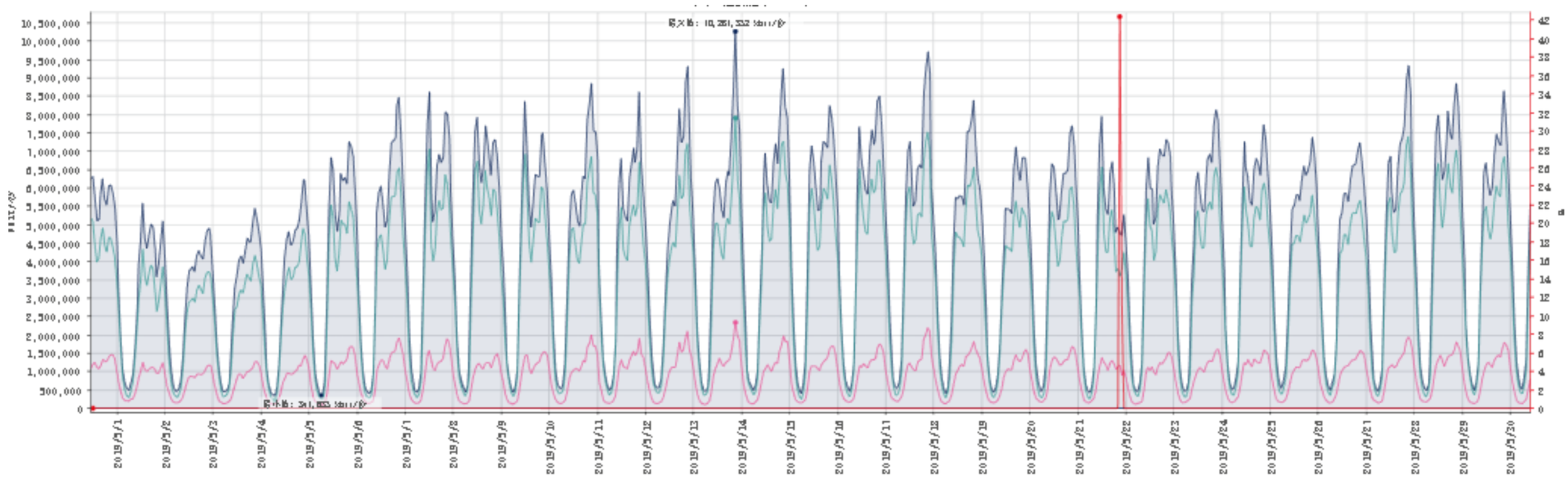


5月，校园网整体运行正常，日均在线用户6195人，其中无线用户日均在线4220人。



校园网出口流量分析

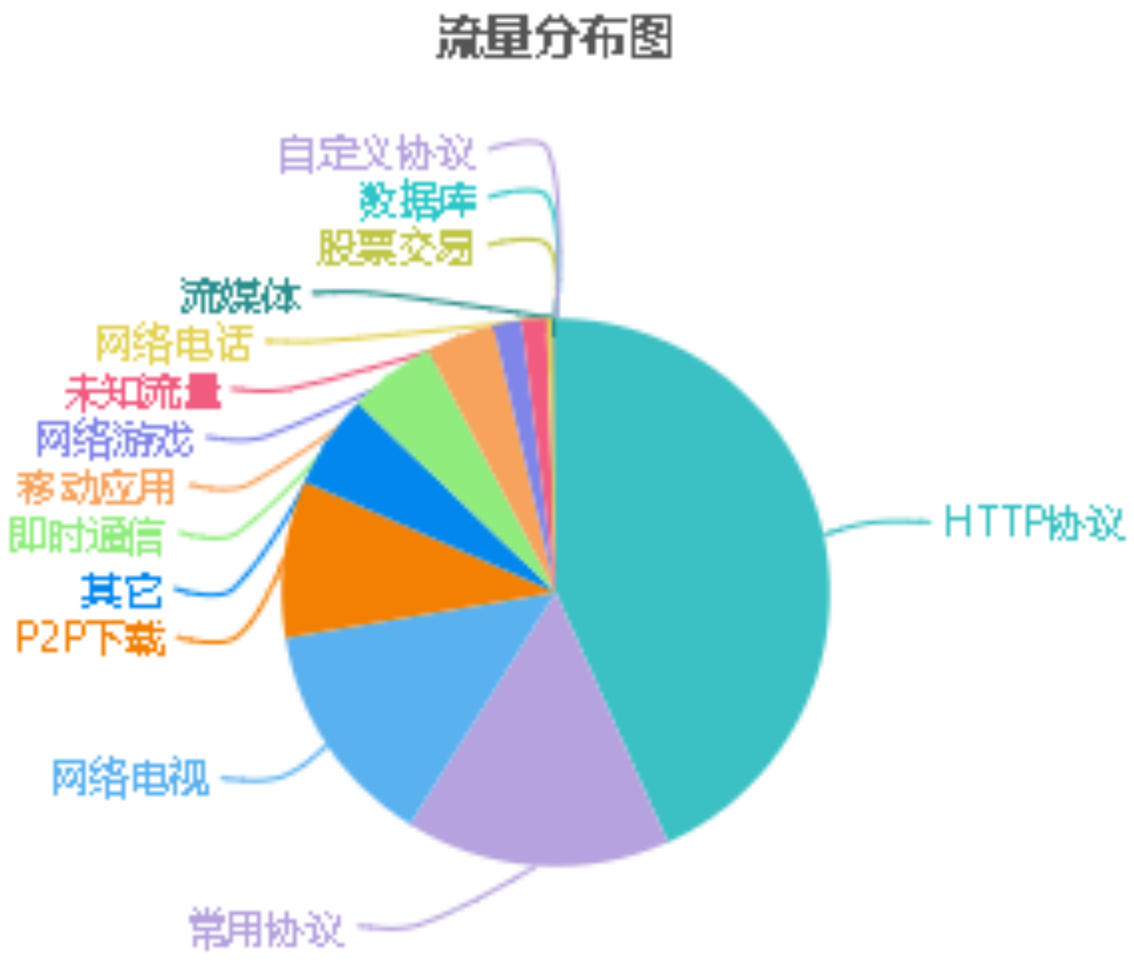
校园网出口流量趋势图



校园网出口峰值使用带宽近10G，2019年5月，校园网总下载流量达1.187PB，上传流量共计317T。

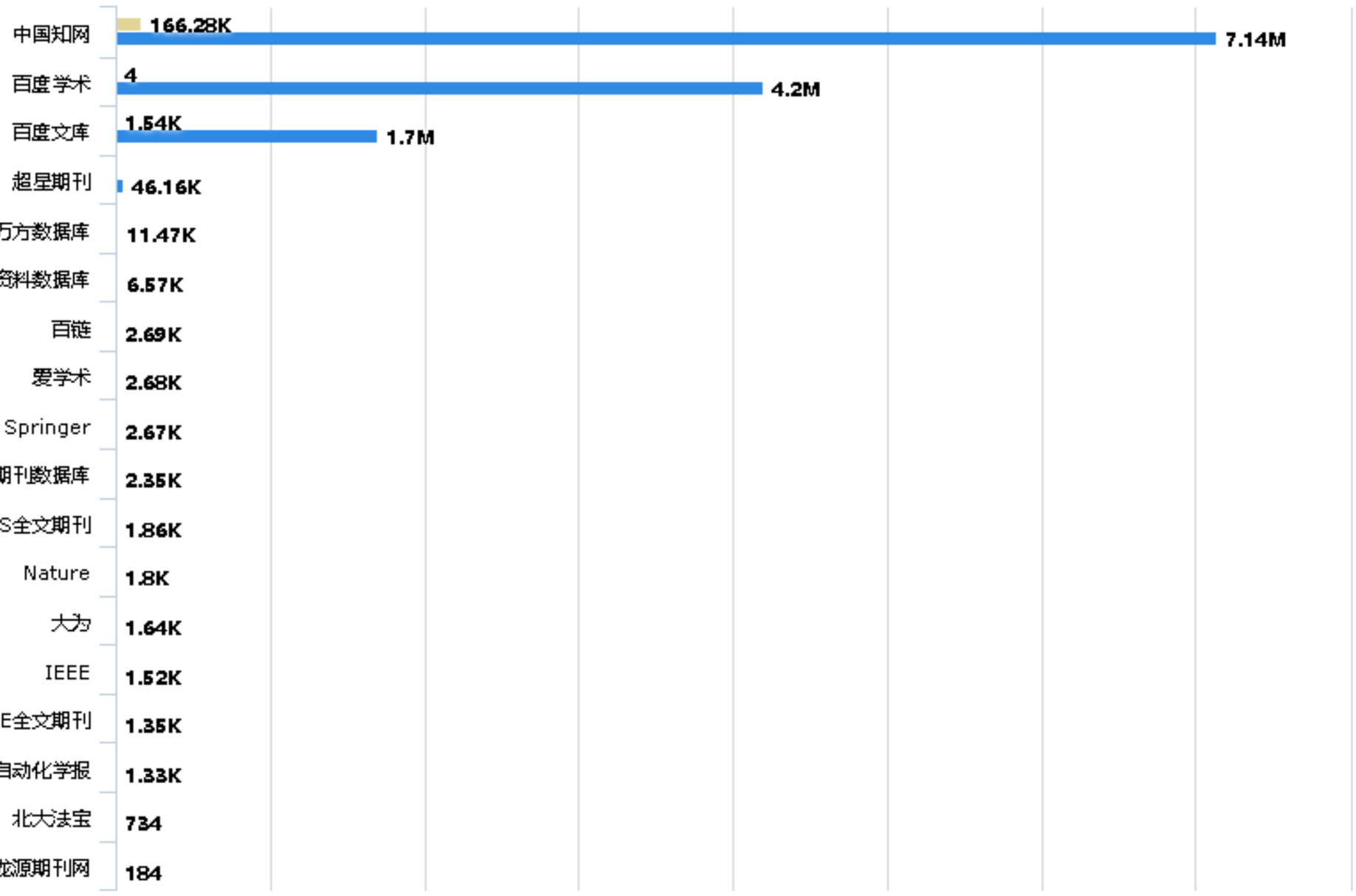
其中，HTTP日常访问产生流量达641.3T位居首位，常用协议流量及网络电视流量位居二三位，分别为231.65T和198.58T。

校园网出口流量分布图

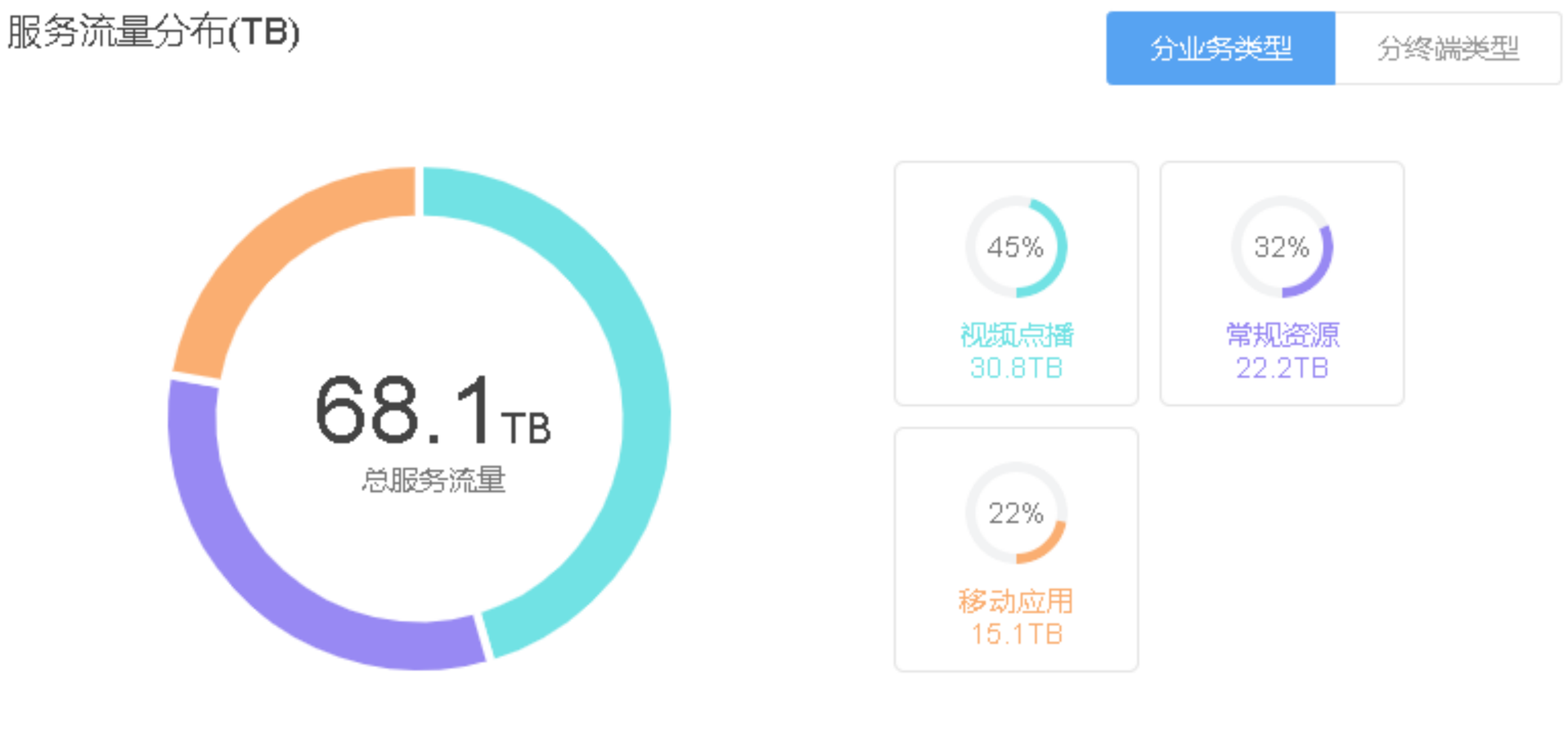


校园网资源使用分析

校园网图书资源访问统计



校园网出口内容加速用户流量分布排行

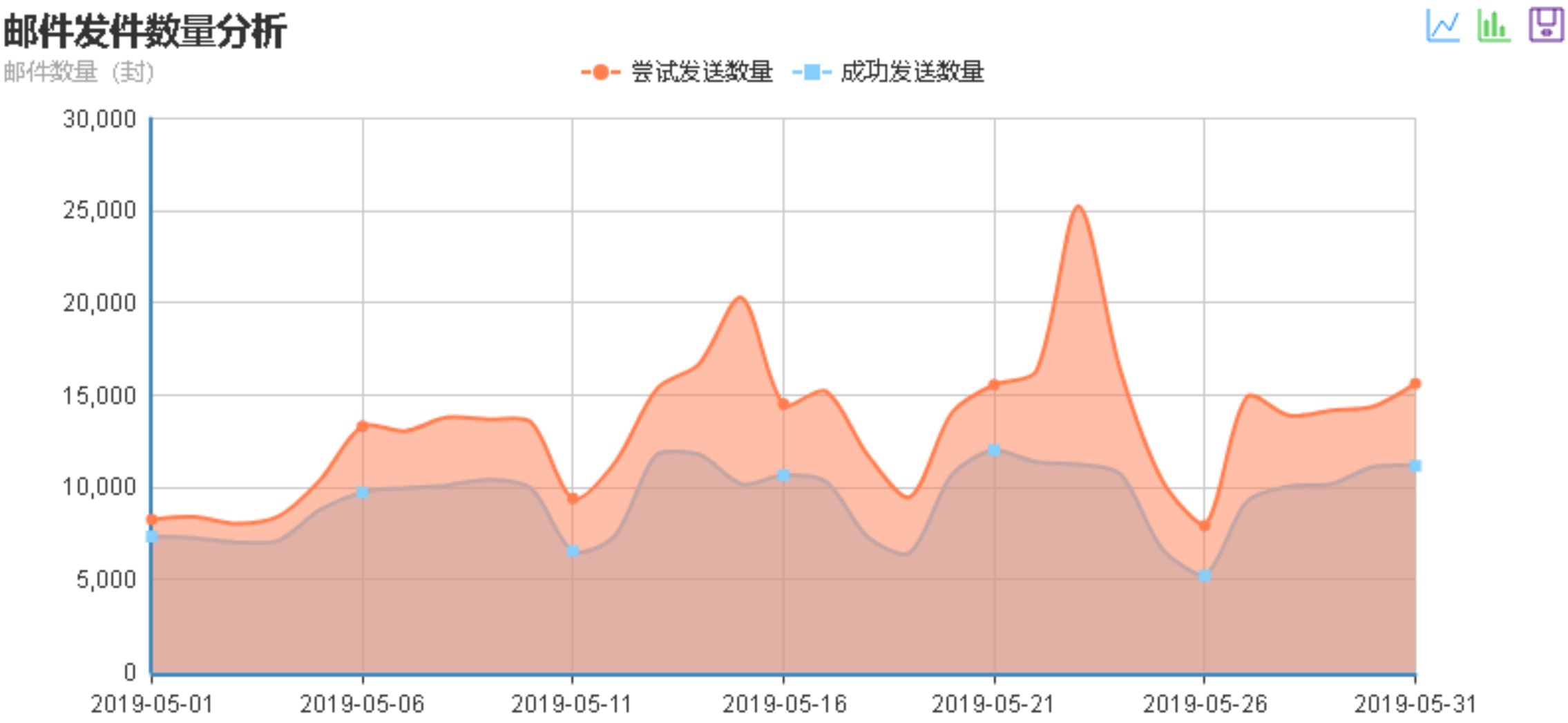


*注：以上数据由 Panabit® 飞享 ifeixiang.com 友情提供

校园电子邮件系统运行情况分析

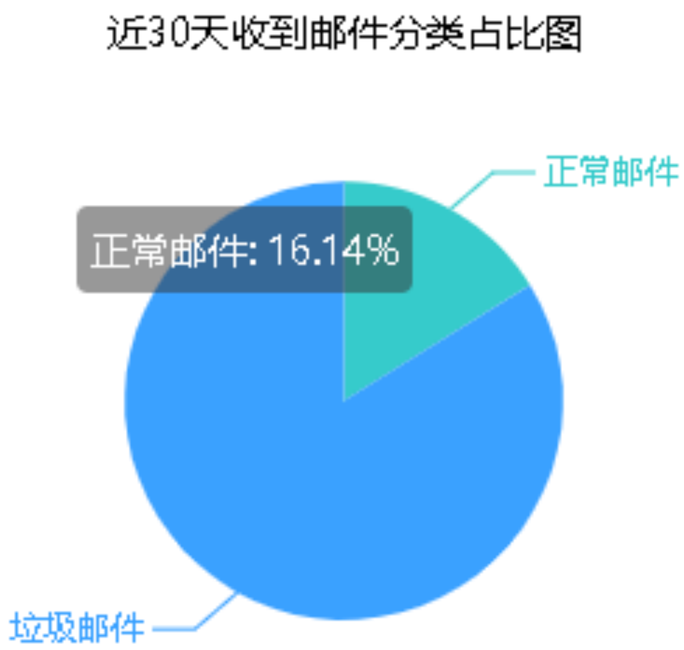
2019年5月，我校电子邮件系统运行稳定，反垃圾邮件网关工作正常，日均拦截垃圾邮件近6.3万封，日均发送邮件8765封。

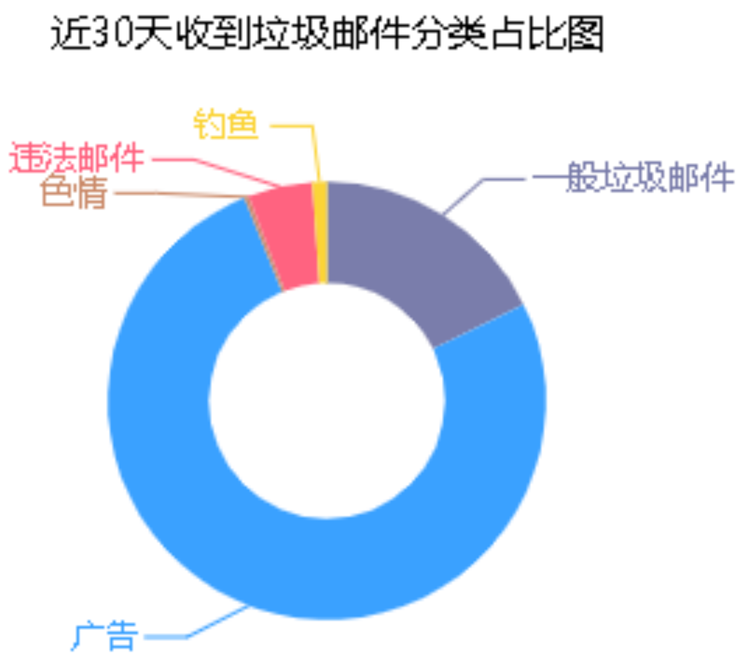
校园邮件系统发送数据统计



校园邮件系统接收邮件分类统计

邮件类型

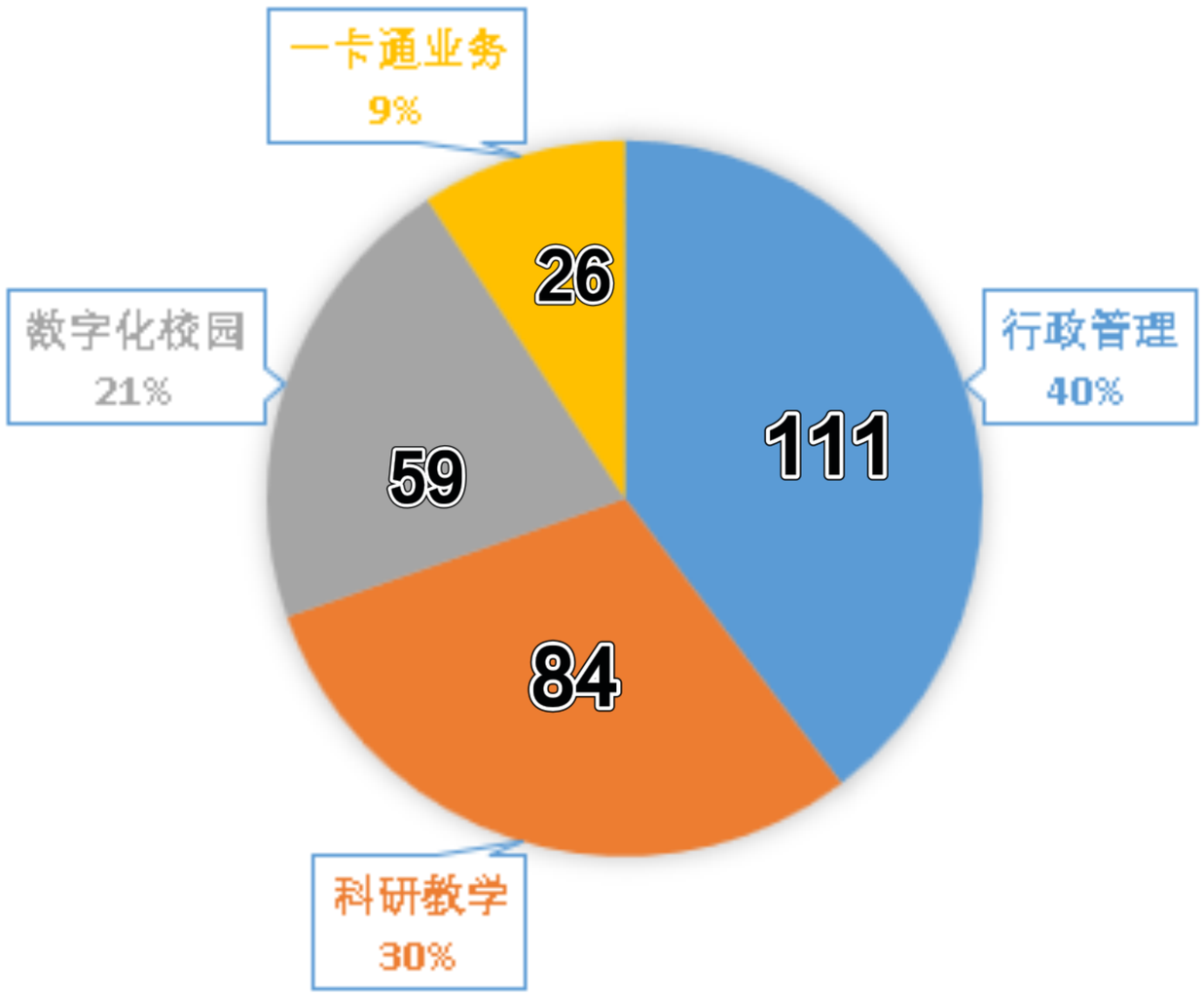




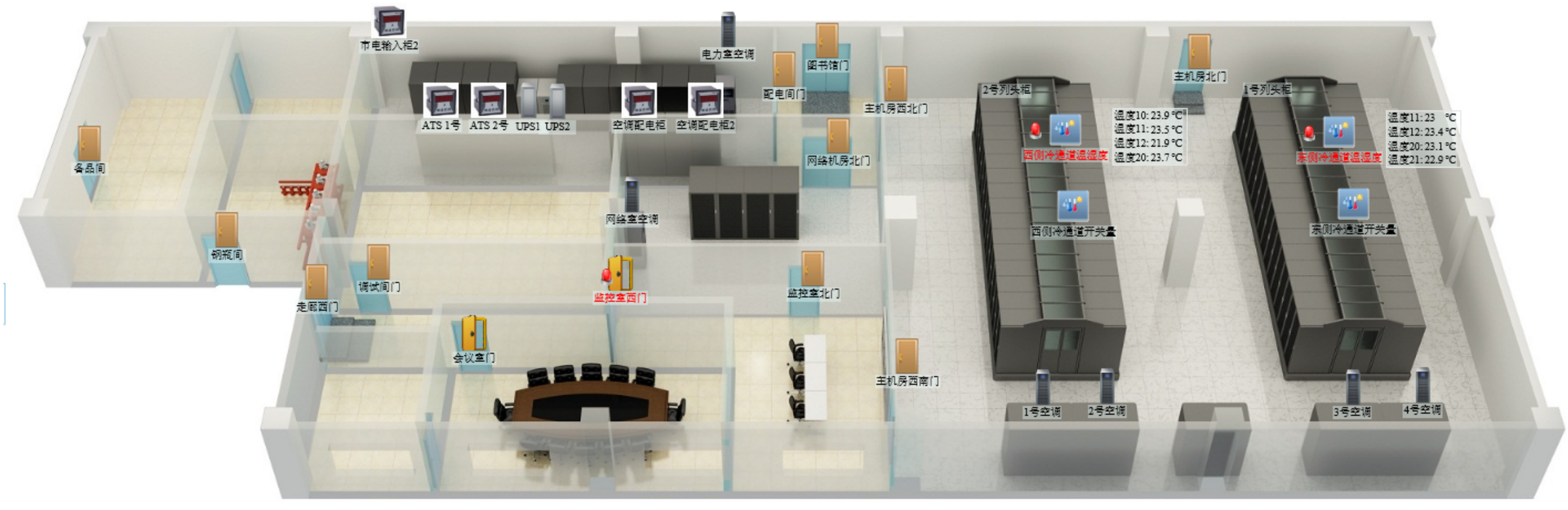
数据中心运行情

网络信息管理中心采用服务器虚拟化技术使得传统独立硬件服务器的硬件资源得到了充分利用，不仅为学校的校办、人事处、财务处、教务处、研究生院、科技处等十几个业务处室的30多项应用提供服务，更为学校老师的科研项目和实验教学提供了良好的基础。（李蒙）

5月数据中心虚机情况统计

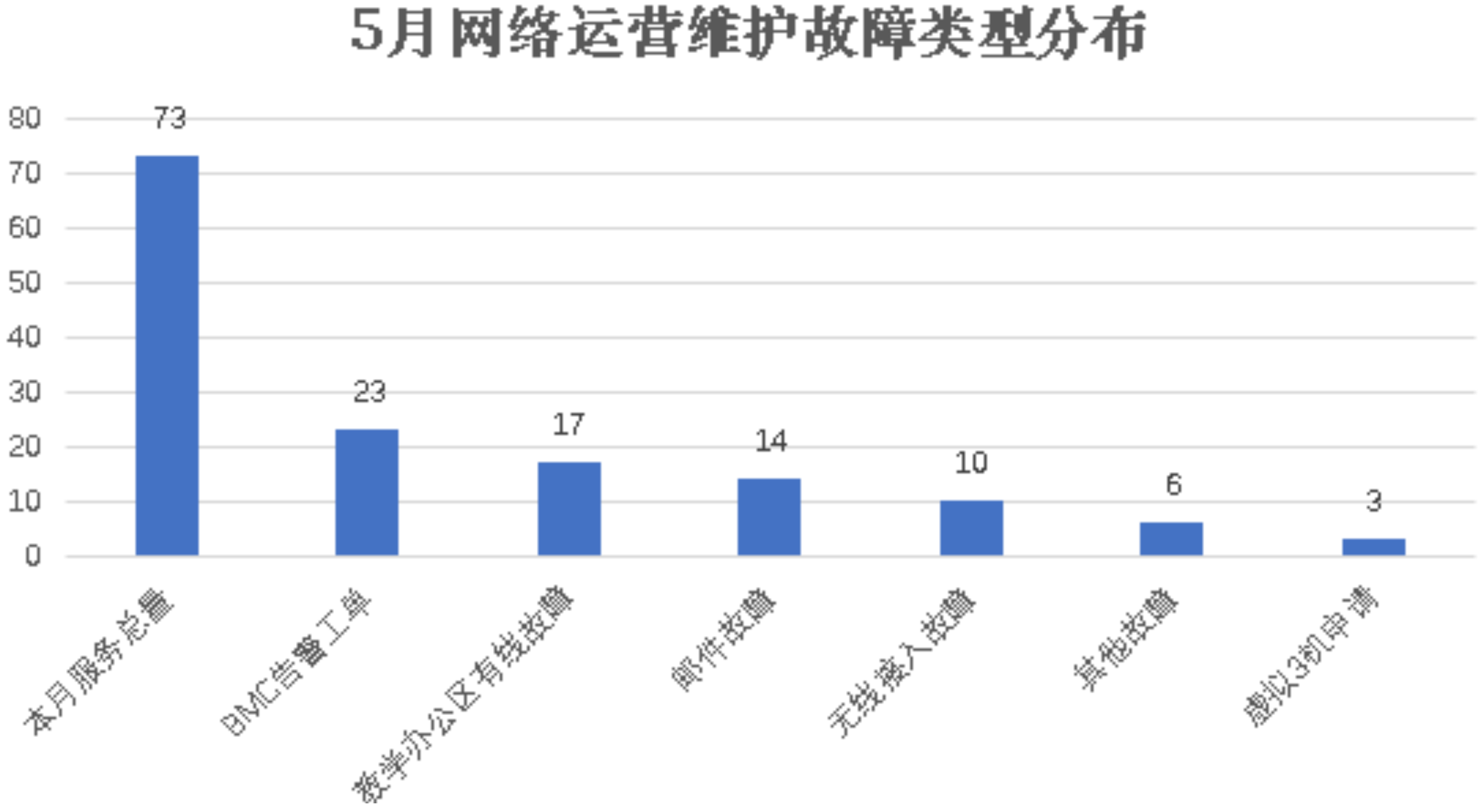


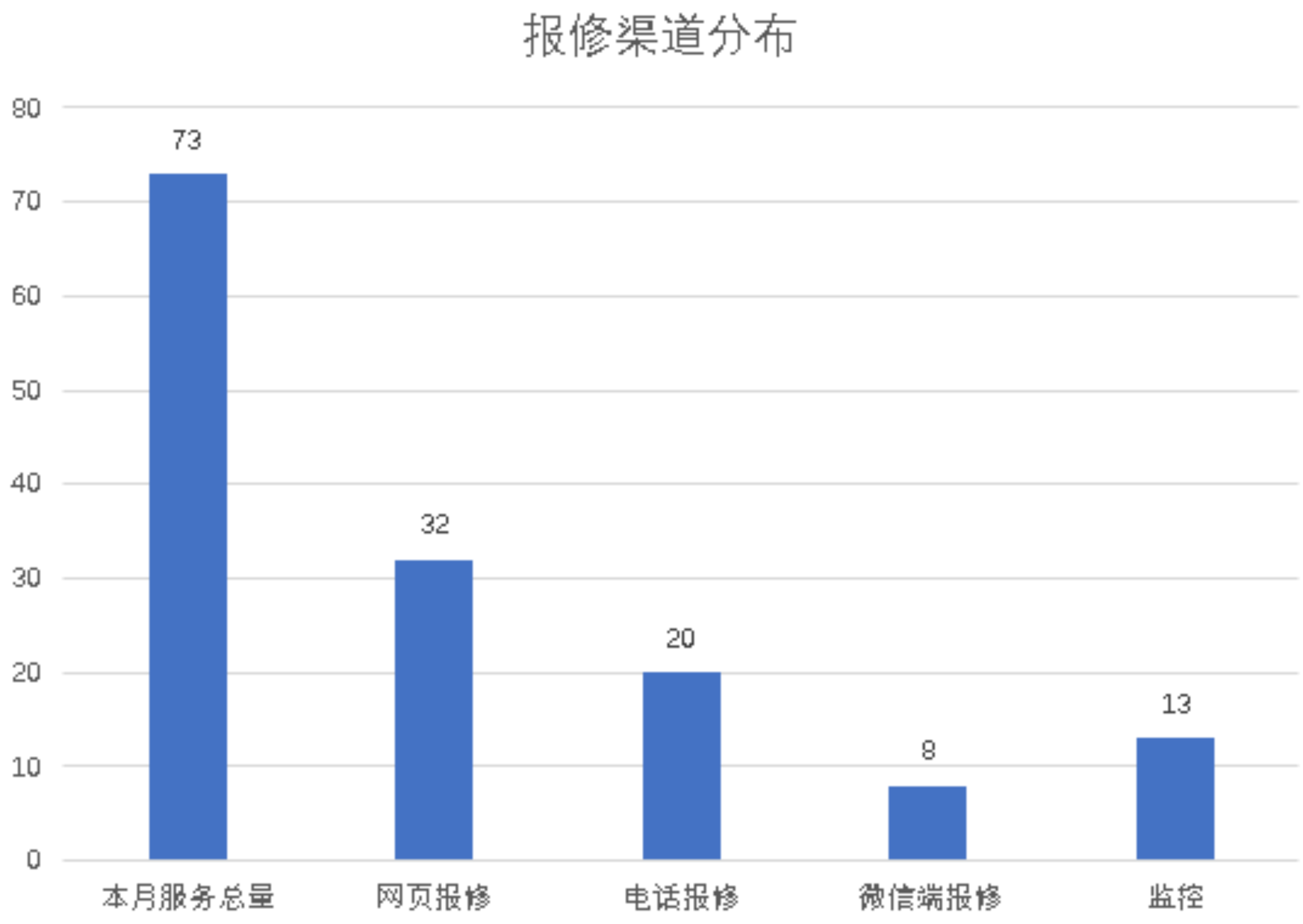
数据中心机房整体运行稳定，其中5月17日及5月23日停电2次，UPS电池供电正常，服务器及网络设备未出现停机。中心机房空调故障34次，已及时处理，未影响机房整体制冷环境。（赵阳）



校园网工作数据情况分析

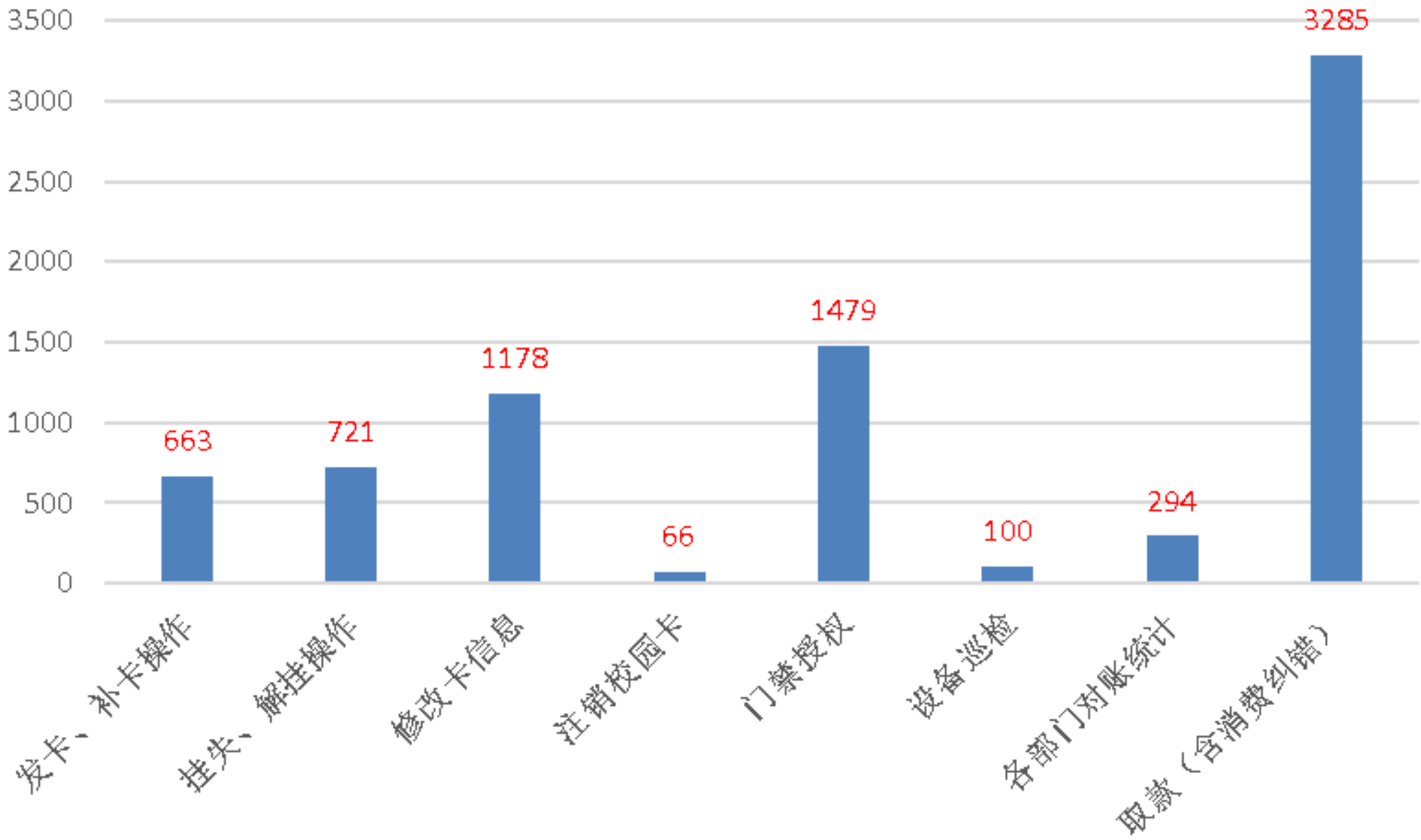
2019年5月，网络与安全管理部共受理各类故障、告警73件，接到报修、业务申请后均能第一时间响应并及时解决问题，保证校园网正常运行。(殷仕刚)



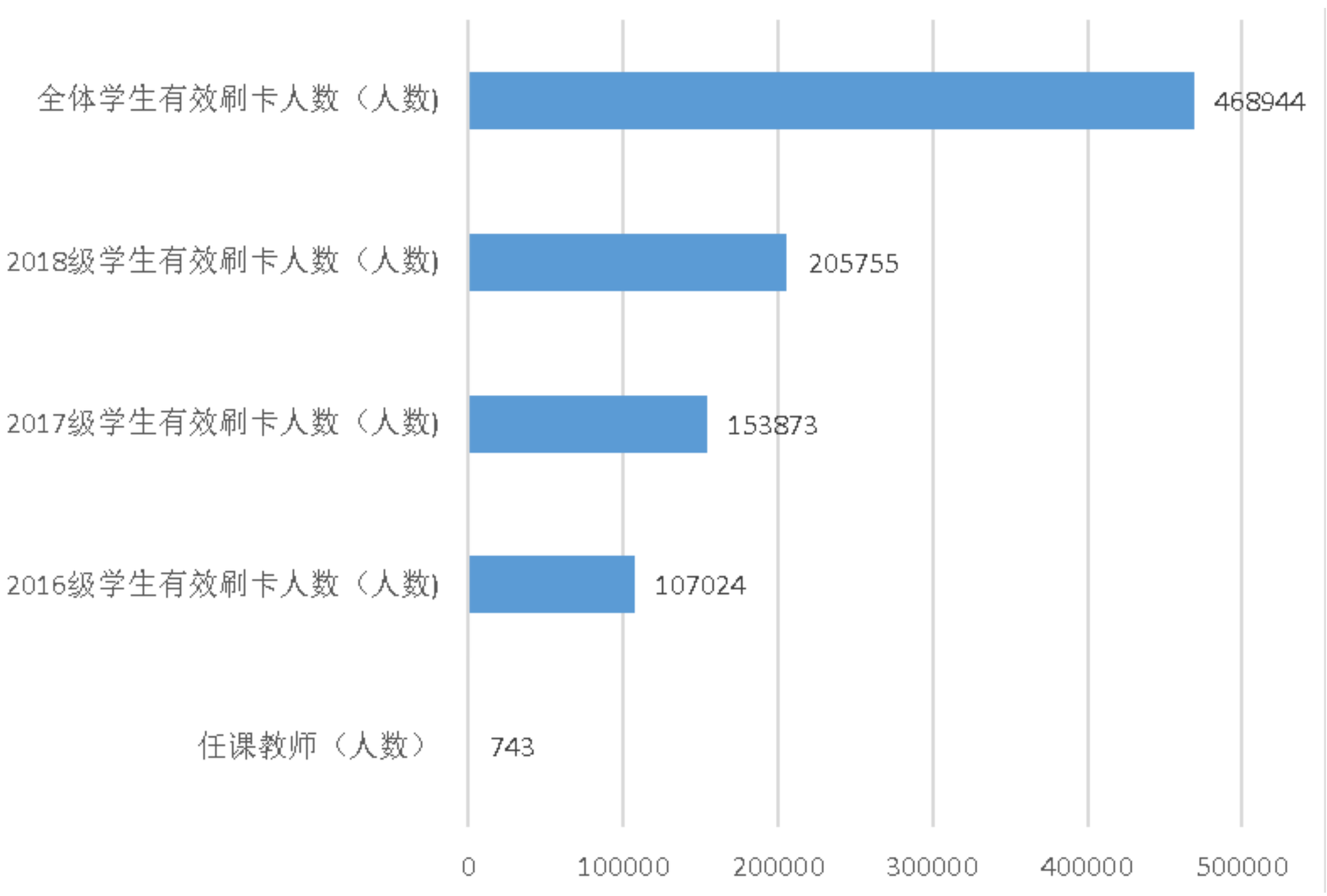


校园卡务中心月度数据统计

校园卡务中心5月工作数据统计



2019年5月教务考勤系统运行情况统计图



2019年5月餐厅消费数据排名

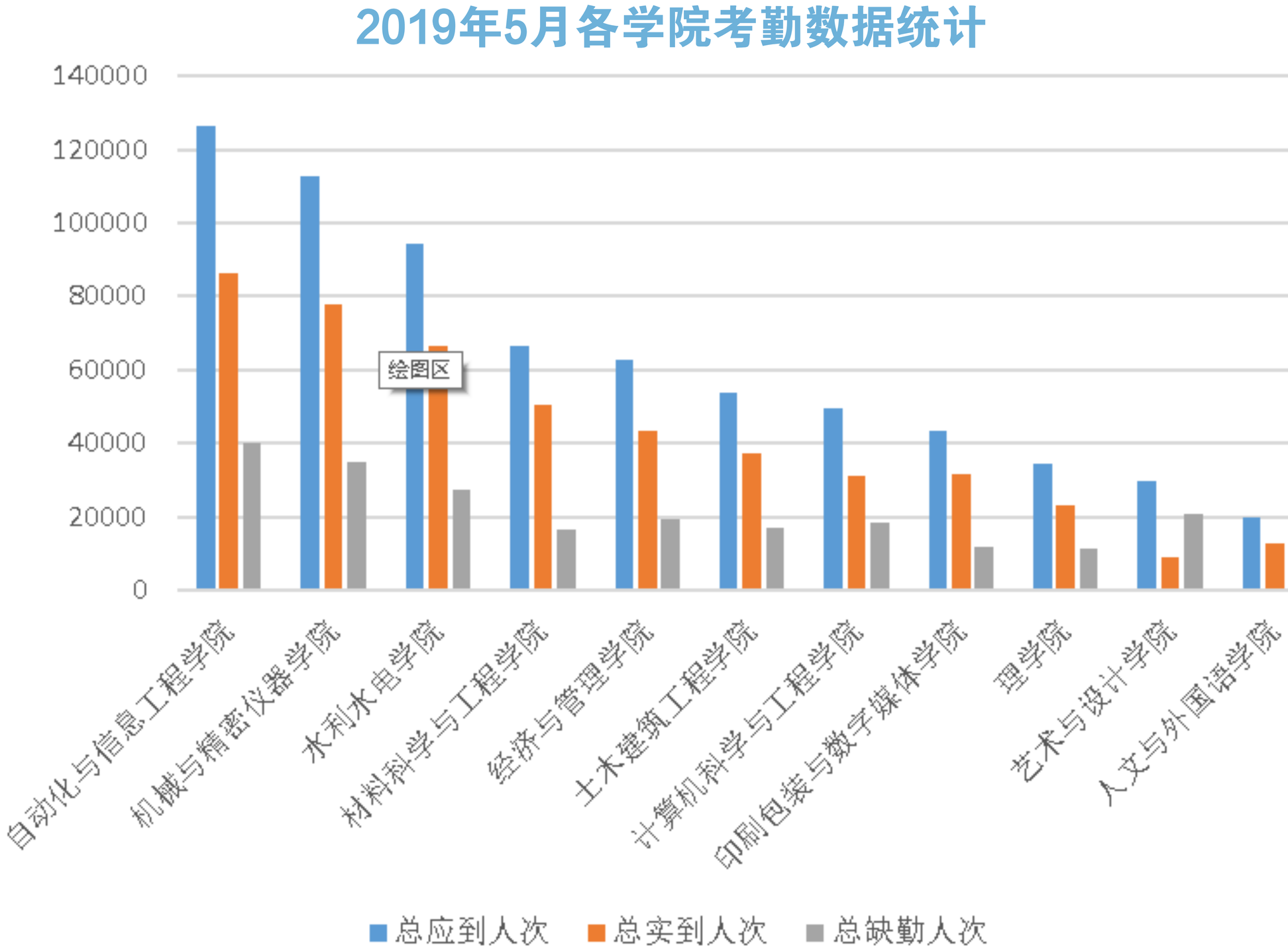
金花校区餐厅各窗口销量情况

餐厅名	名次		
	1	2	3
金花一餐厅	小卖部	山西饼	干锅
金花二餐厅	快餐	乐华士	面夫子
民族餐厅	豆浆	土豆片夹馍	快餐

曲江校区餐厅各窗口销量情况

餐厅名	名次		
	1	2	3
曲江一餐厅	香锅	自选餐	小卖部
曲江二餐厅	川菜	麻辣烫	柠檬鱼
曲江三餐厅	自助餐	蒸鸡饭	包子
曲江四餐厅	地锅鸡	二十四道疯味	麻辣香锅
民族餐厅	饼、凉皮	快餐	拌面、泡馍
教工餐厅	麦香饼	快餐	煮馍

2019年5月各学院考勤数据统计



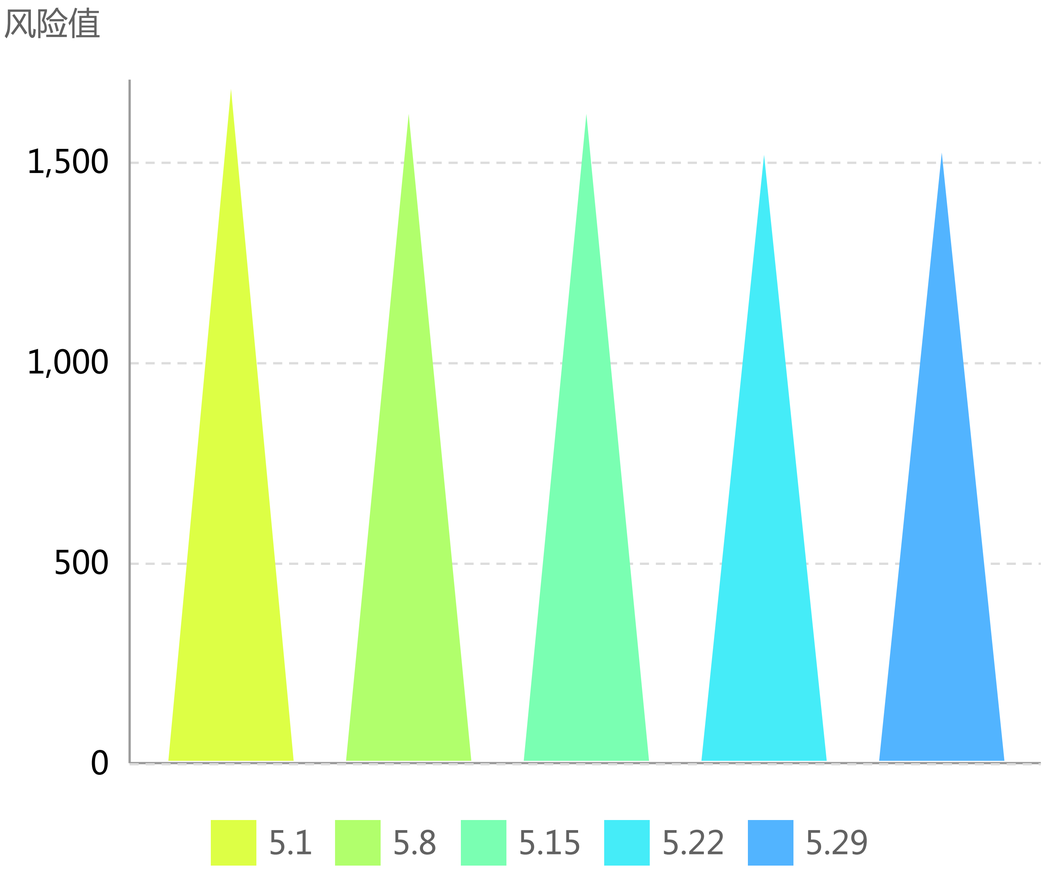
校园网络安全趋势

本网络安全态势分布图以网络信息管理中心监测的数据作为主要依据，对我校重要信息系统（网站）面临的各类安全威胁及基本情况进行总体态势分析，评估范围为2019年5月1日-31日。

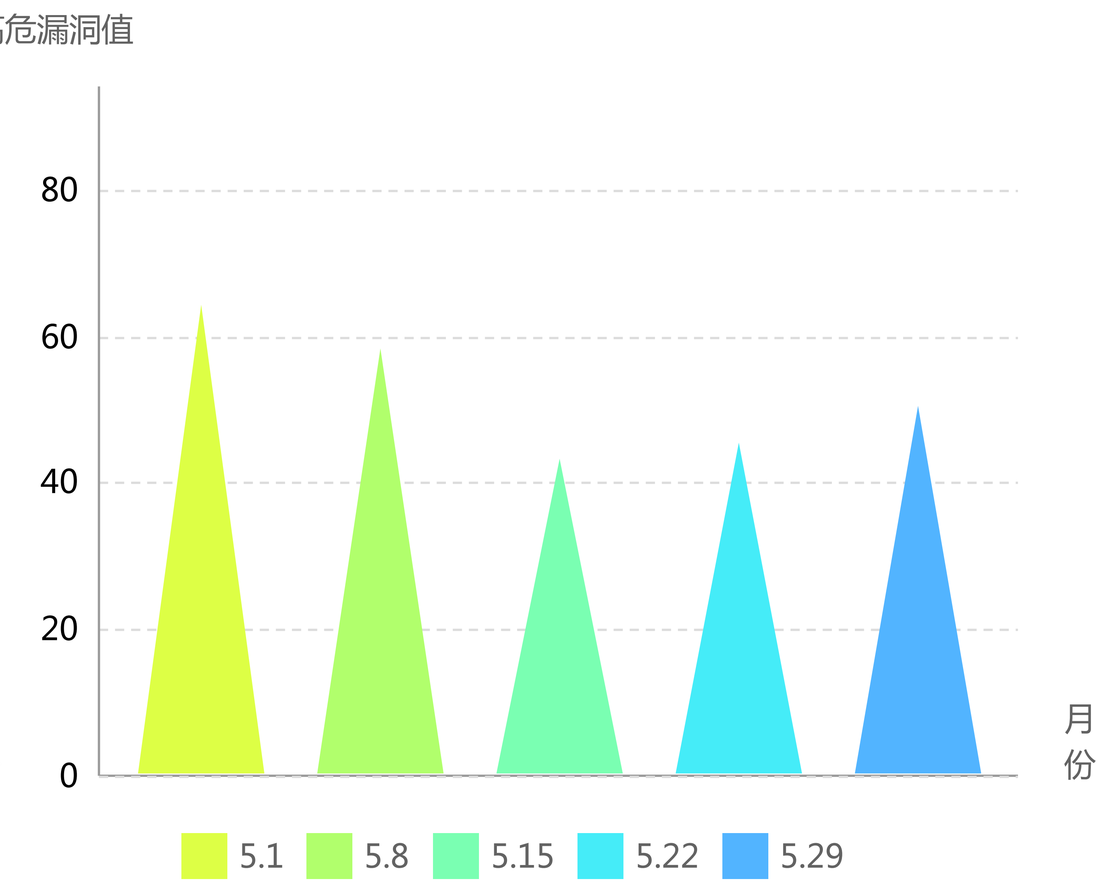
通过常态化安全监测等治理手段，我校本月网络安全状况整体评价为良，风险值环比下降。

2019年5月网络安全态势分布图

风险值趋势



高危漏洞趋势

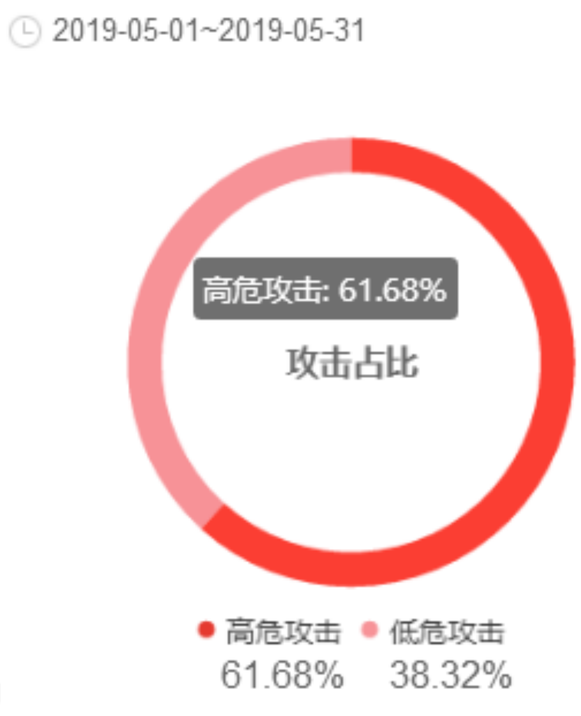


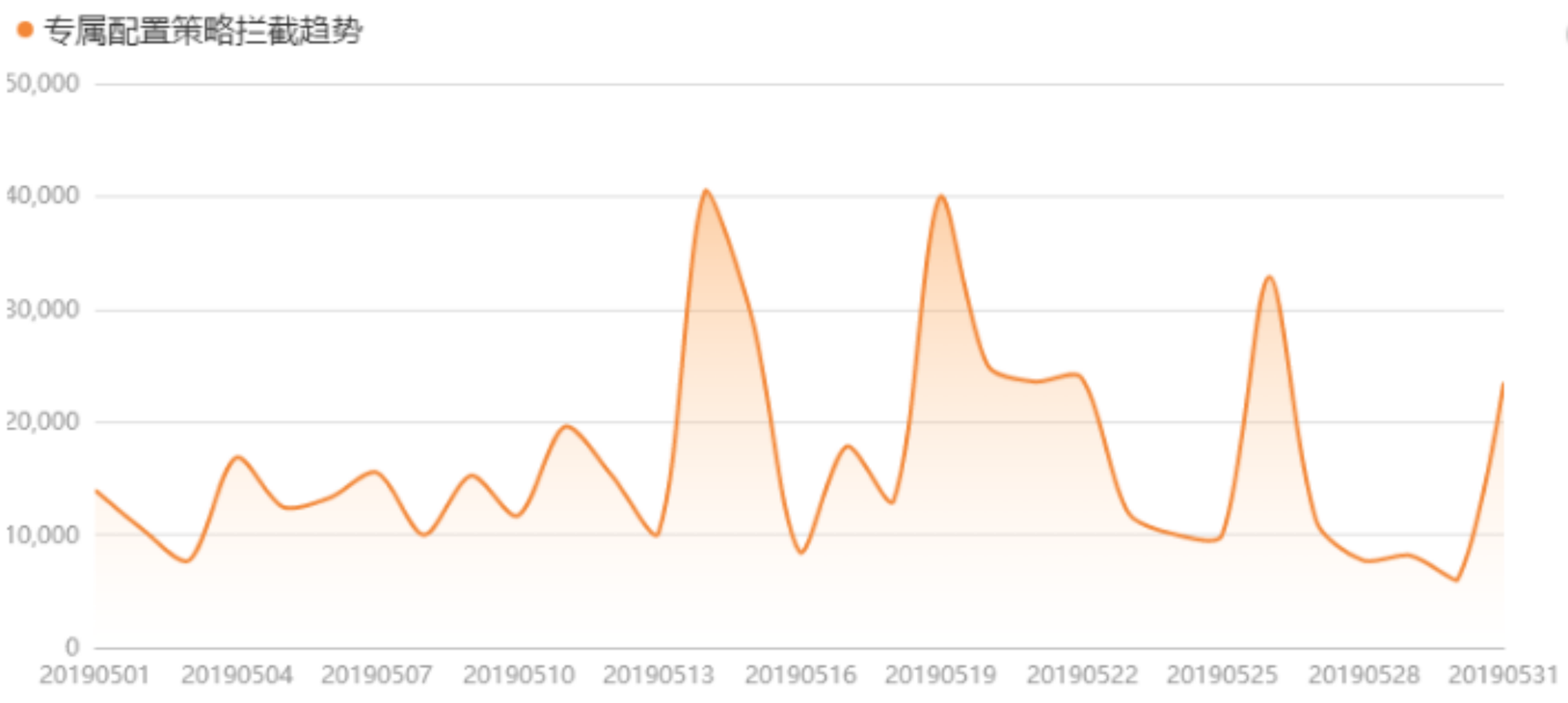
重要信息系统（网站）基本情况

总请求数	总流量	搜索引擎	Alexa 全球排名
25067684次	1980.42GB	462,257次	88412

本攻击拦截态势和网络攻击态势分布图以网络信息管理中心监测的数据作为主要依据，对我校重要信息系统（网站）面临的各类安全威胁及基本情况进行总体态势分析，评估范围为2019年5月1日-31日。

2019年5月1日-5月31日攻击拦截态势和网络攻击态势分布

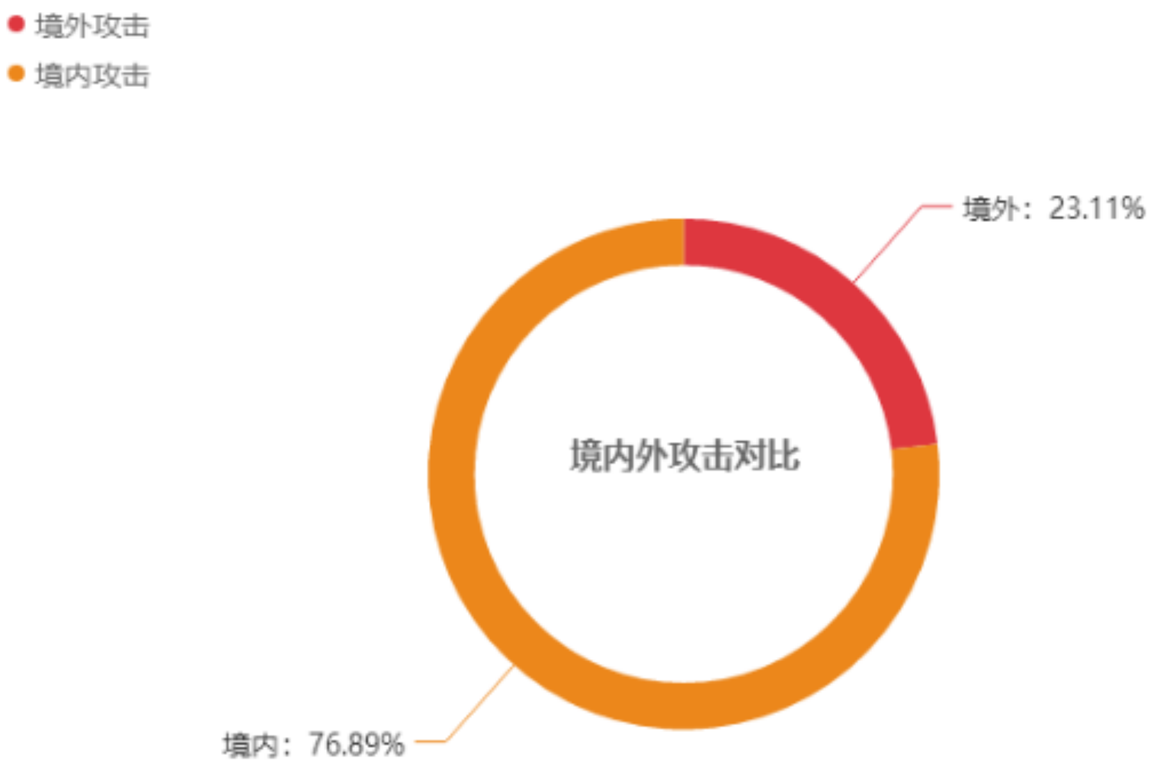




攻击趋势对比：通过本时段和上月时段的攻击趋势对比，攻击峰值（WEB应用攻击次数）共43355次，出现时间2019-05-14；对比峰值（WEB应用攻击次数）273249次，出现时间2019-04-27。

校园网络安全趋势

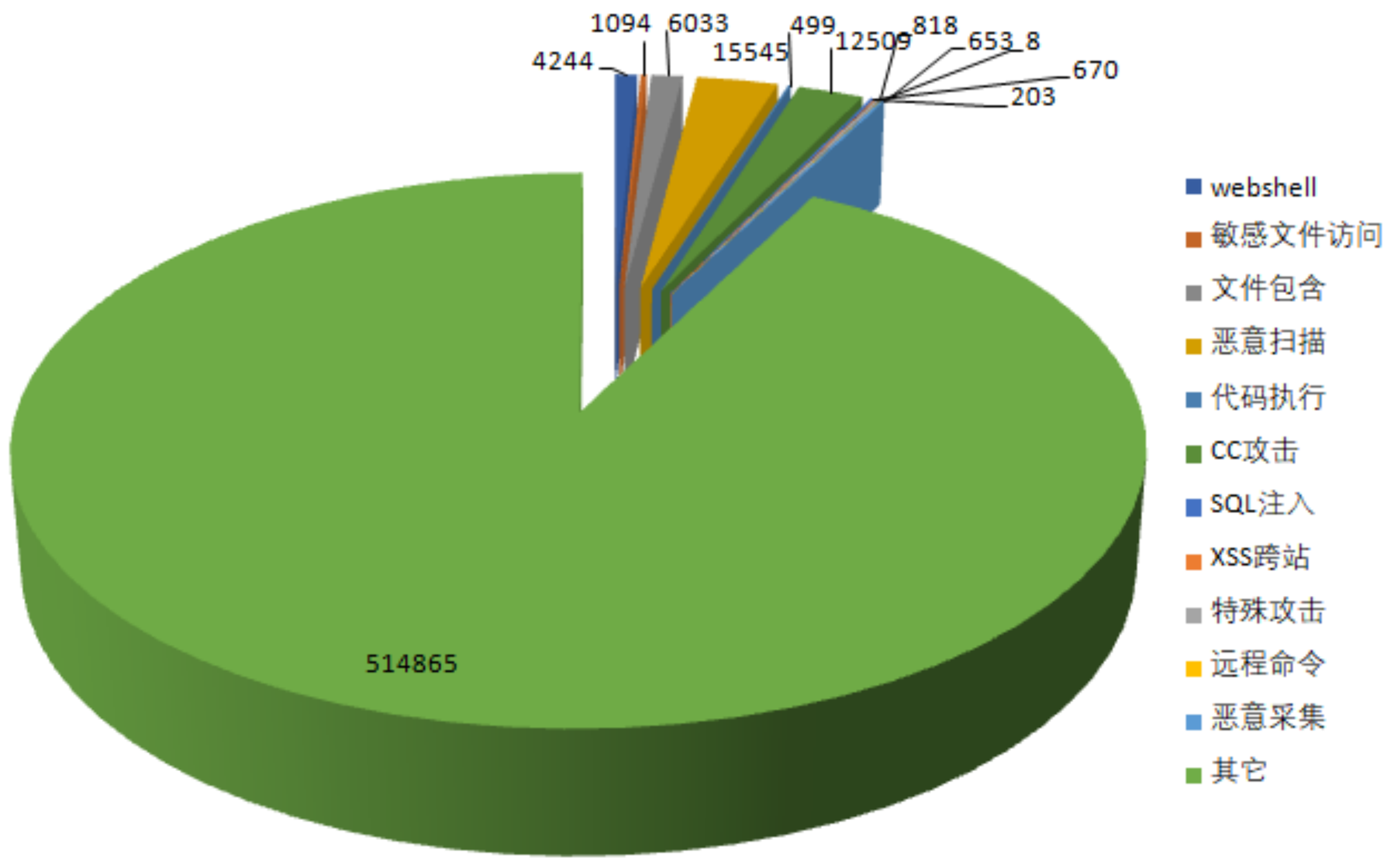
2019年5月1日-5月31日攻击拦截态势和网络攻击态势分布



境外攻击分布来源Top10

国家名称	攻击次数
美国	33862
南非	6345
印度	2361
亚太地区	1363
奥地利	911
欧盟	901
菲律宾	899
马来西亚	653
老挝	320
新加坡	310

2019年5月1日-5月31日网站遭受黑客攻击分布图



本月共发生各类安全攻击557141次，黑客攻击占总请求数的比率为2.22%，其中敏感文件访问1,094次、Webshell攻击4,244次、文件包含攻击6,033次、恶意扫描15,545次、代码执行499次、CC攻击12,509次、SQL注入670次、XSS跨站攻击203次、特殊攻击818次、远程命令8次，恶意信息采集653次，其它类型攻击514,865次。

潜伏在身边的黑客

银钩：针对国内网银用户的钓鱼的攻击活动

(奇安信威胁情报中心)

由于攻击背后的团伙最终目的为针对电信和经商用户的银行账号进行财产窃取，因此将该团伙命名为：银钩，意指利用银行木马作为诱饵，等待猎物上钩之意。

钓鱼邮件攻击手段历史已久，这类攻击背后，往往是一个黑产团伙在进行运营活动，而投放钓鱼邮件进行攻击仅仅是团伙在这条黑色产业链上的一部分。

背景介绍

银钩团队利用钓鱼邮件的攻击手法有所不同，其使用了附件为漏洞利用文档的手法进行攻击，试图通过漏洞触发后的木马感染用户电脑，从而窃取个人资产。从邮件内容可见，攻击者为了引诱受害者打开附件文档，故意将邮件中的兑奖方式标红，使得受害者有打开电子发票查看信息的欲望，同时对于经商人员来说，发票是一个重要报销手段，因此同样有理由打开附件文档。

捕获样本

以顺丰电子发票为主题的钓鱼邮件，该类钓鱼邮件的附件和链接打开后其实为一个钓鱼网站，用于进行用户账号密码盗取。

信息安全漏洞公告

1 Microsoft Windows Search 远程执行代码漏洞

Microsoft Windows Search存在远程代码执行漏洞。攻击者可以利用此漏洞在当前用户的上下文中执行任意代码。失败的漏洞利用尝试可能会导致拒绝服务的情况。

解决方案:

目前厂商已发布升级补丁以修复漏洞，补丁获取链接:
https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-8450

2 Microsoft Internet Explorer缓冲区溢出漏洞

Microsoft Internet Explorer 9、10和11中脚本引擎处理内存对象的方法存在缓冲区溢出漏洞。该漏洞源于网络系统或产品在内存上执行操作时，未正确验证数据边界，导致向关联的其他内存位置上执行了错误的读写操作。攻击者可利用该漏洞导致缓冲区溢出或堆溢出等。

解决方案:

目前厂商已发布升级补丁以修复漏洞，补丁获取链接:
https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0918

3 Microsoft远程桌面服务远程代码执行漏洞

未经身份验证的攻击者利用该漏洞，向目标Windows主机发送恶意构造请求，可以在目标系统上执行任意代码。由于该漏洞存在于RDP协议的预身份验证阶段，因此漏洞利用无需进行用户交互操作，存在被不法分子利用进行蠕虫攻击的可能。

解决方案:

目前，微软官方已发布补丁修复此漏洞，补丁获取链接:
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

西安理工大学
XI'AN UNIVERSITY OF TECHNOLOGY

网络信息管理中心

信息化工作简报

主　　编：李军怀 侯小军

副主编：杨超 胡先智 雷龙涛

编　　辑：李博鑫 王心成 李宏伟
王力　李蒙　赵阳
殷仕刚　张晋 安洋

审　　核：张晓宇

扫码关注

西安理工大学微信企业号