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4月

目录

航空工业西安飞机工业（集团）有限责任公司来我校进行技术交流

4月3日下午，西安飞机工业（集团）有限责任公司科技与信息化部副部长周盛一行来我校调研综合运维管理平台的建设及应用情况，网络信息管理中心主任李军怀、副主任侯小军、相关科室负责人及承建方锐捷网络股份有限公司代表参加了会议，会议由李军怀教授主持。

李军怀主任指出，近年来学校对信息化建设越来越重视，数字化校园平台、移动校园平台以及校园一卡通平台建设已经具备一定规模，为学校3万多师生提供了丰富的应用的同时，也给运维管理工作带来了挑战。为保证各系统稳定、安全运行，提高管理和运维效率，实现线上、线下结合的综合运维管理平台建设势在必行。

周盛部长表示，作为工业企业信息化部门，各类系统管理与运维水平直接影响到企业的生产力。虽然属于不同行业，但是高校开放度较高，信息化建设、管理和运维思路存在一些共同的特点。

最后，周盛部长一行参观了数据中心机房和综合运维管理平台的实际演示。（杨超）

西安工业大学来校调研信息化建设

4月22日下午，西安工业大学信息技术中心马建军、刘璐一行人员，来我校调研“数字化校园平台”及“迎新系统”的建设及应用情况。网络信息管理中心主任李军怀出席会议。

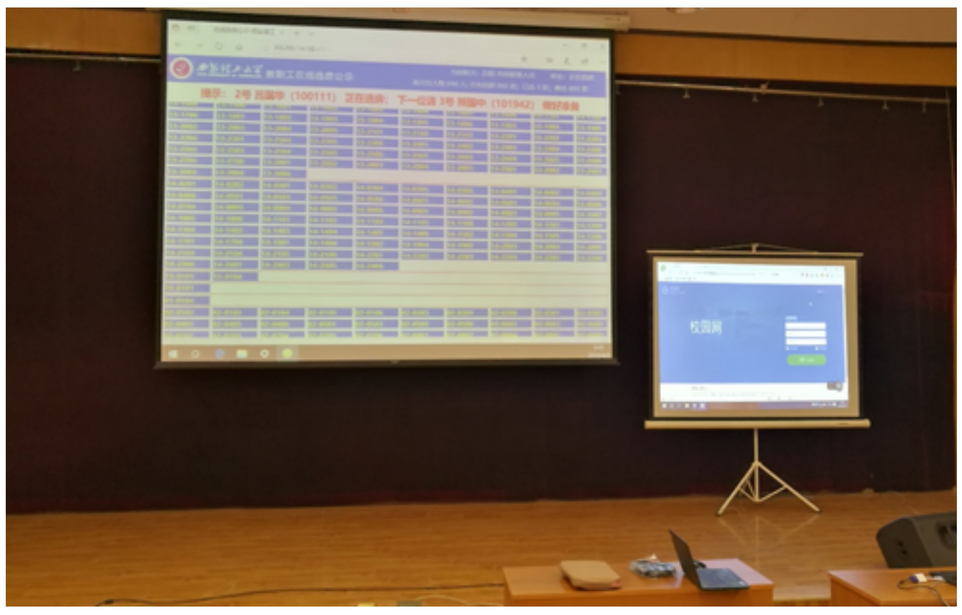
李军怀主任首先对到访客人表示热烈欢迎，就中心基本情况及我校近年来的信息化建设成果做了全面的介绍。然后，由信息管理部负责人详细介绍了“数字化校园平台”及“迎新系统”的建设与应用情况，现场演示了“基础平台”及“迎新系统”，并就数据交互与共享、迎新流程等贵方关心的问题做了重点研讨。

西安工业大学与会老师对我校的信息化建设成果给予了高度的评价。几位老师表示，此次交流学习对西安工业大学的信息化建设很有启发，希望今后可以进一步加强双方互动，增加交流机会。（李宏伟）

圆满完成教职工选房、“知行榜样”表彰大会网络保障工作

我校于4月进行启动了教职工选房工作，并顺利召开“知行榜样”表彰大会，为确保我校教职工选房及表彰大会直播的顺利进行，中心积极配合做好基础网络搭建和网络保障工作。

其中，此次选房工作自4月9日起至4月24日，共计12天。选房直播会场包括金花图书馆报告厅、教二楼100报告厅、教六楼510教室，选房期间三个会场同时使用大屏直播实时选房结果。我校“知行榜样”2019年优秀学生表彰大会暨颁奖典礼于4月12日晚7点在曲江校区大学生活动中心举行。学校1400名师生、家长在现场观看了颁奖典礼，活动同时面向全校、全社会开通了微信、微博、易班平台和校园网络高清直播通道，同时在线观看人数达4.3万人，直播流畅无异常。（李博鑫）



网络信息管理中心开展加强网站和信息系统账号安全管理行动

依据陕西省教育厅《关于加强信息系统账号安全管理的通知》要求，为保障我校网络与数据安全，防止师生个人信息泄露，进一步加强学校网站和信息系统的安全管理，切实保障学校网站和信息系统稳定运行和数据安全，网络信息管理中心开展加强网站和信息系统账号安全管理行动。

本次行动要求各单位对负责的网站和信息系统的所有账号及口令密码进行安全自查并定期检查，及时清理僵尸账号，规范口令设置，严禁使用弱口令密码。我中心对全校邮件系统3822个用户账号口令进行排查，共计处理187个弱口令账号。（王心成）

校园卡大事件

01 70周年校庆餐补发放工作

为庆祝学校推进“双一流”建设暨建校70周年纪念系列活动举行，校园卡管理部根据我校《关于为在校生发放餐费补助的通告》的相关精神，按照学校相关工作安排，为17000余名在校本科生及6000余名研究生发放餐费补助，并提供详细领款操作说明。（王力）

02 校园一卡通进一步完善充值渠道建设

网络信息管理中心与中国银行金花南路支行、新开普电子股份有限公司三方共同建设并上线中国银行APP校园卡充值项目。在已有自助现金机充值、圈存机充值、手机APP充值方法下，此项工作的完成进一步丰富了我校校园卡充值手段，为广大师生提供了更多的选择与便利。（王力）

信息档案支部组织召开2019年第三次全体党员大会

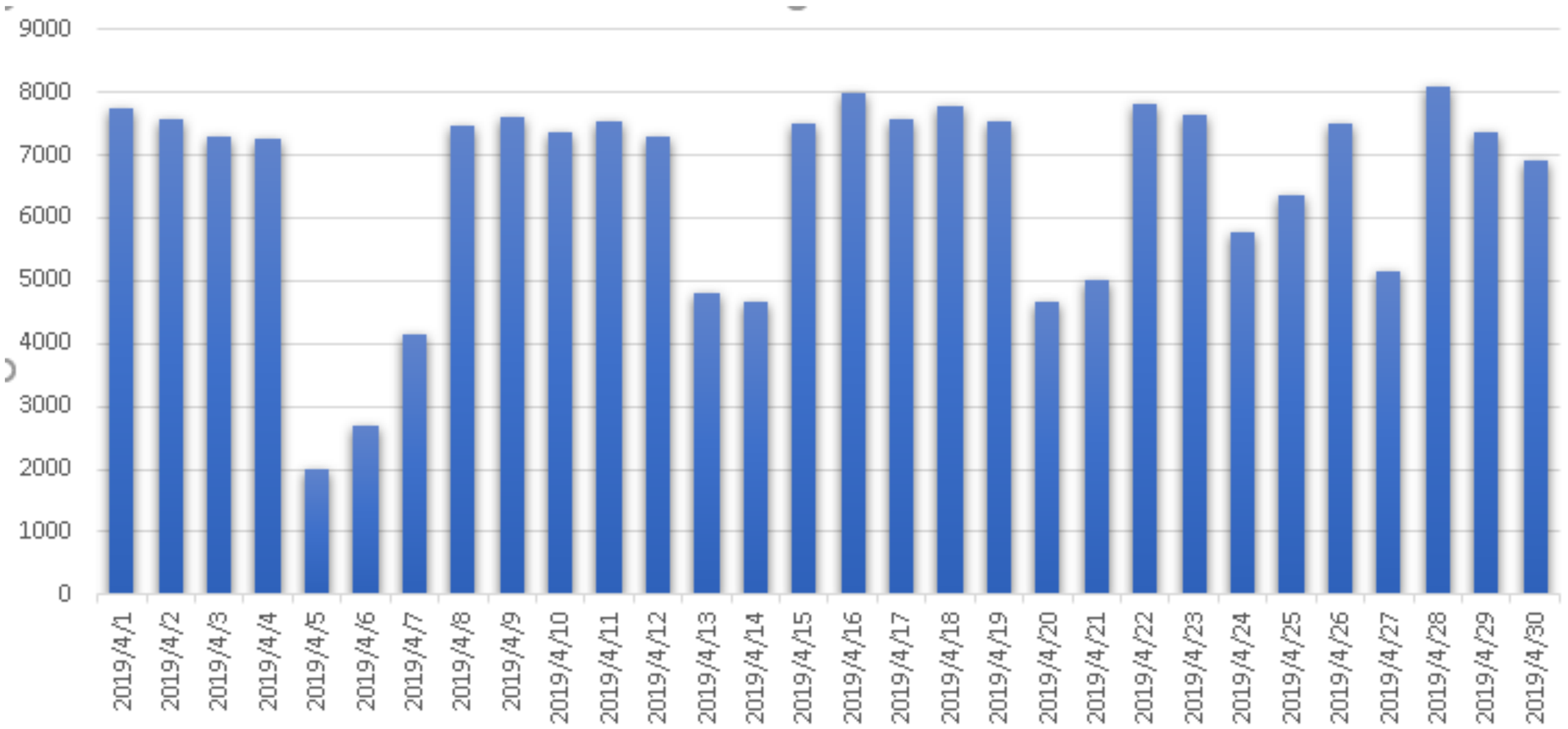
4月22日上午11:00，信息档案党支部书记侯小军在网络中心会议室主持召开2019年第三次全体党员大会。

会上，李志强副书记带领大家学习了《西安理工大学关于开展巡视整改专项工作的实施方案》、《中共西安理工大学委员会开展“支部建设年”活动实施方案》和《关于深入推进我校“讲政治、敢担当、改作风”专题教育常态化长效化的通知》，并传达了机关党委2019年工作要点。

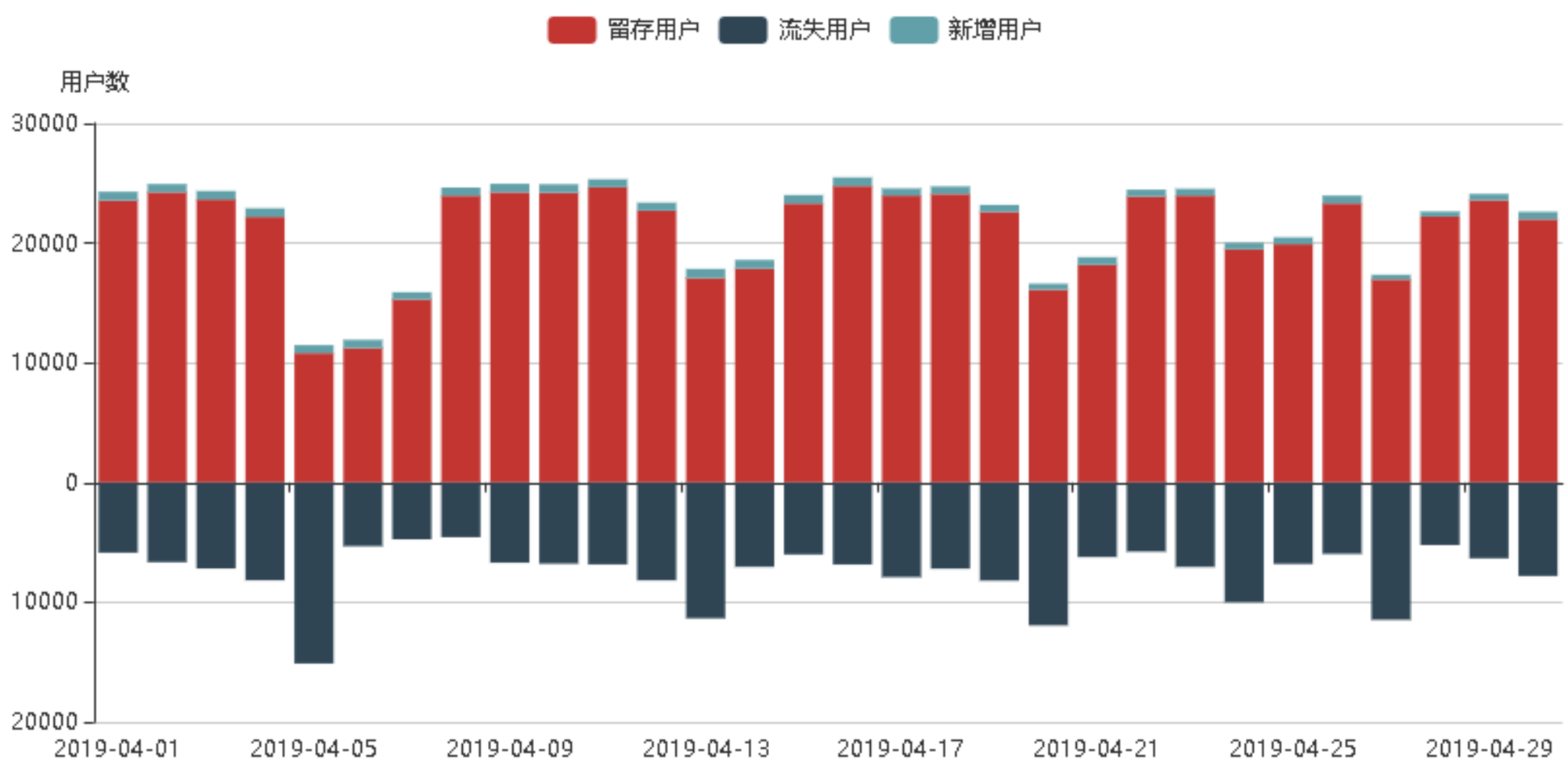
侯小军书记带领大家学习了学校《关于做好中国共产党西安理工大学第八次代表大会筹备工作的通知》、《关于中国共产党西安理工大学第八次代表大会代表选举工作的通知》和机关党委《关于做好机关党委代表选举有关工作的通知》，就此次代表选举工作的代表名额和构成原则、代表的资格条件、代表产生的程序、办法和完成的时间等做了详细的介绍。随后，信息档案党支部全体党员进行了投票，根据多数党员意见，经民主集中程序，提出代表候选人推荐名单上报机关党委。（杨超）

校园网在线用户分析

2019年4月校园网在线用户分析

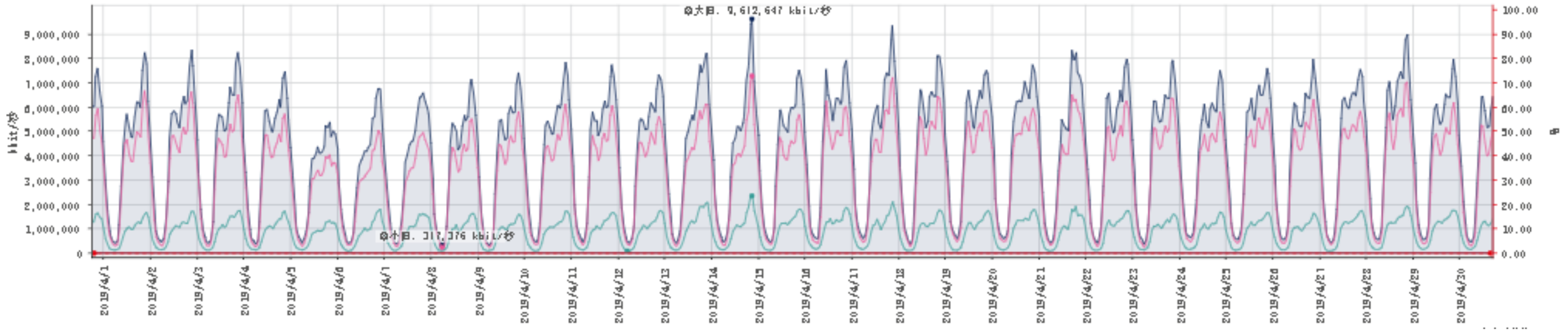


4月，校园网整体运行正常，日均在线用户6540人，其中无线用户日均在线5220人。（李博鑫）



校园网出口流量分析

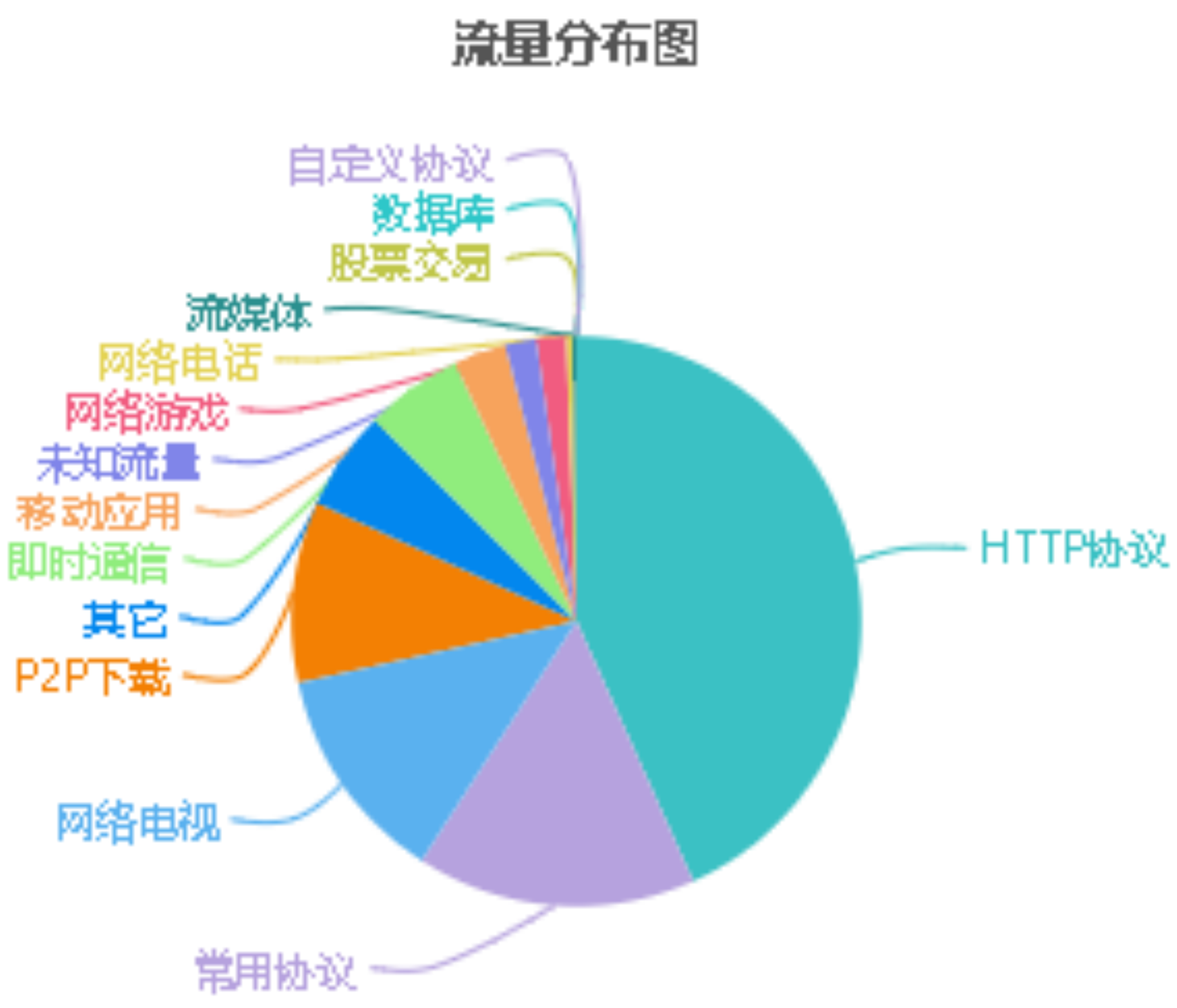
校园网出口流量趋势图



校园网出口峰值使用带宽近8G，2019年4月，校园网总下载流量达1.04PB，上传流量共计300T。

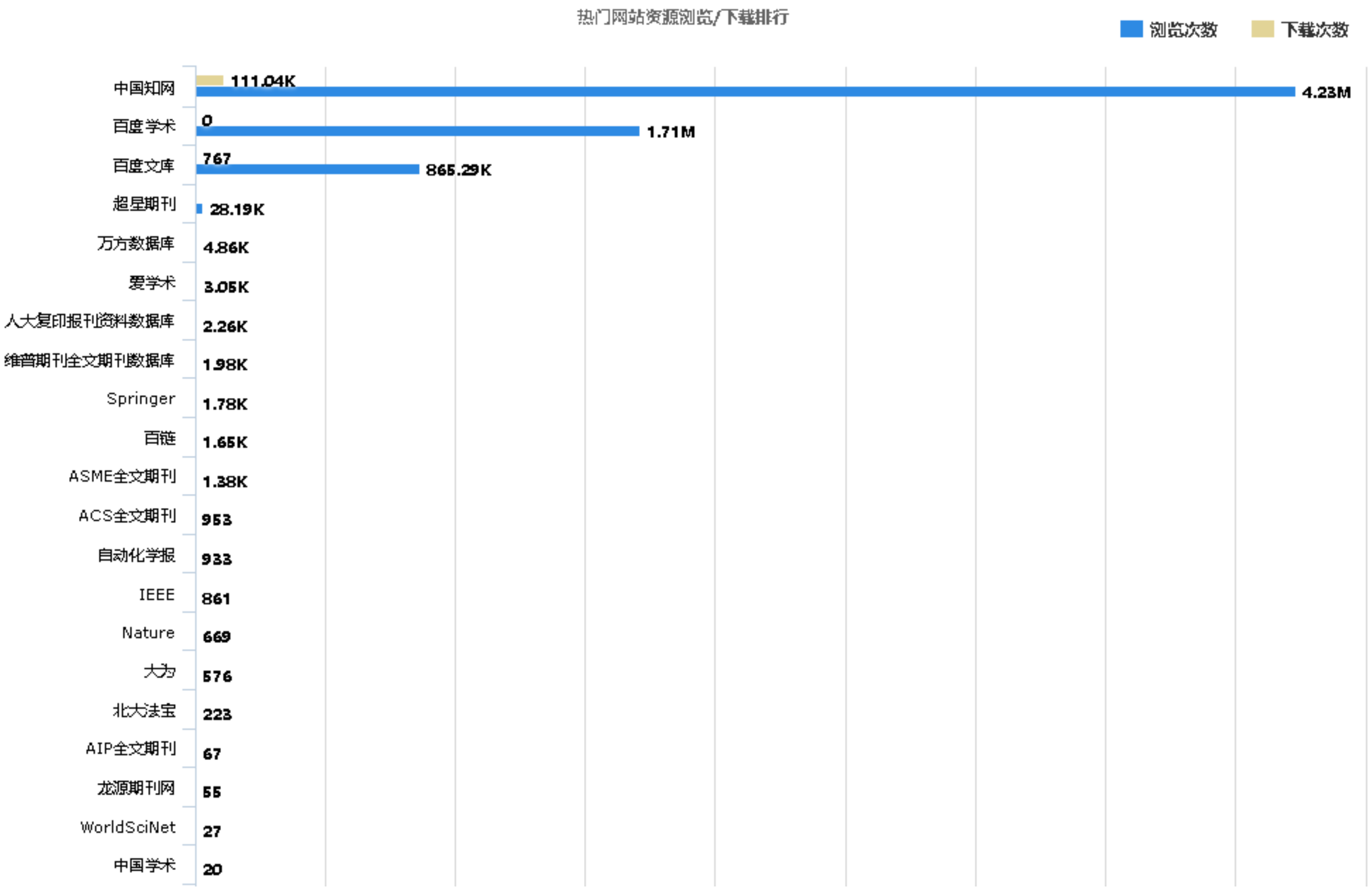
其中，HTTP日常访问产生流量达476T位居首位，迅雷等P2P下载流量及网络电视流量位居二三位，分别为140T和122T。（李博鑫）

校园网出口流量分布图

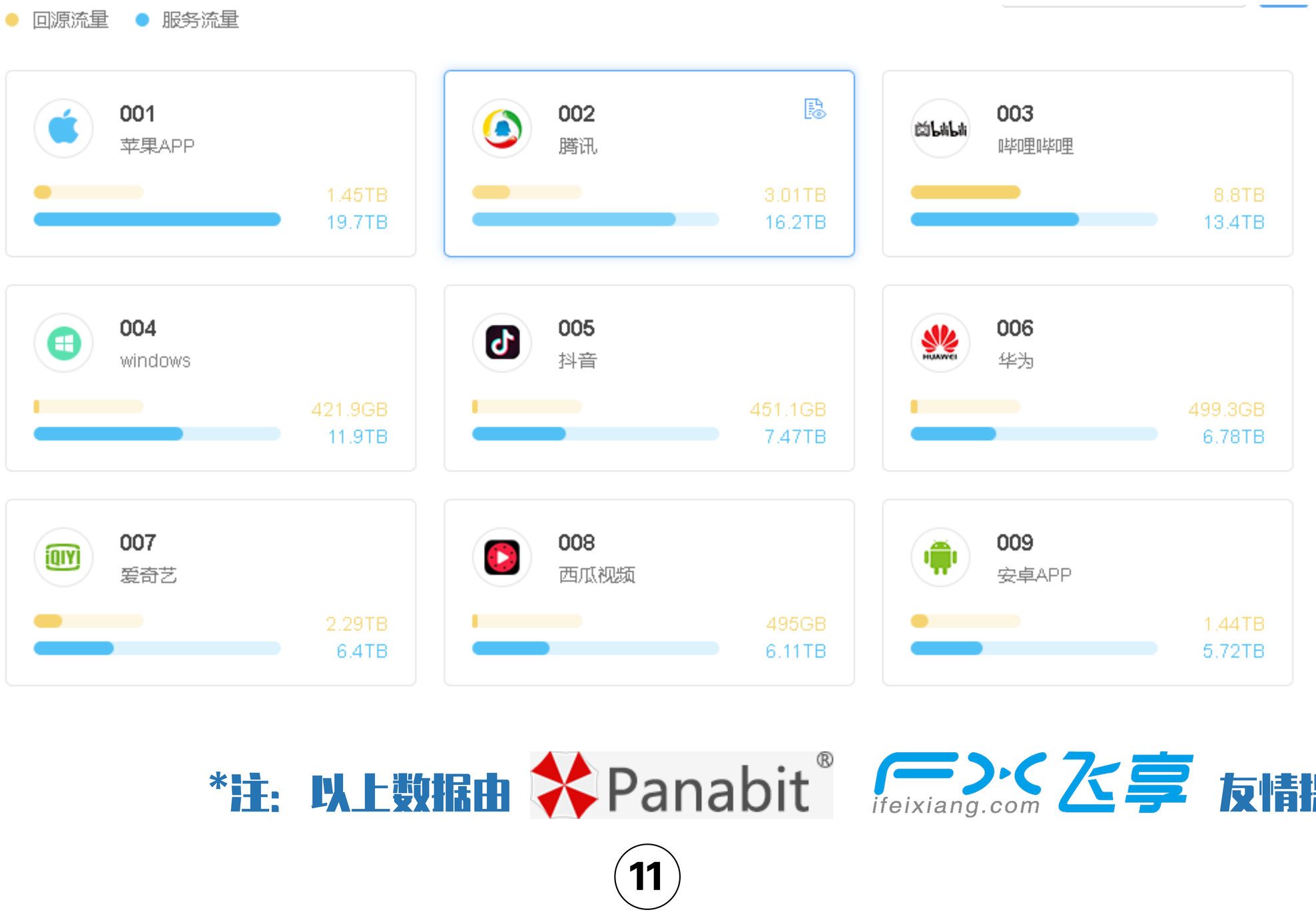


校园网资源使用分析

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

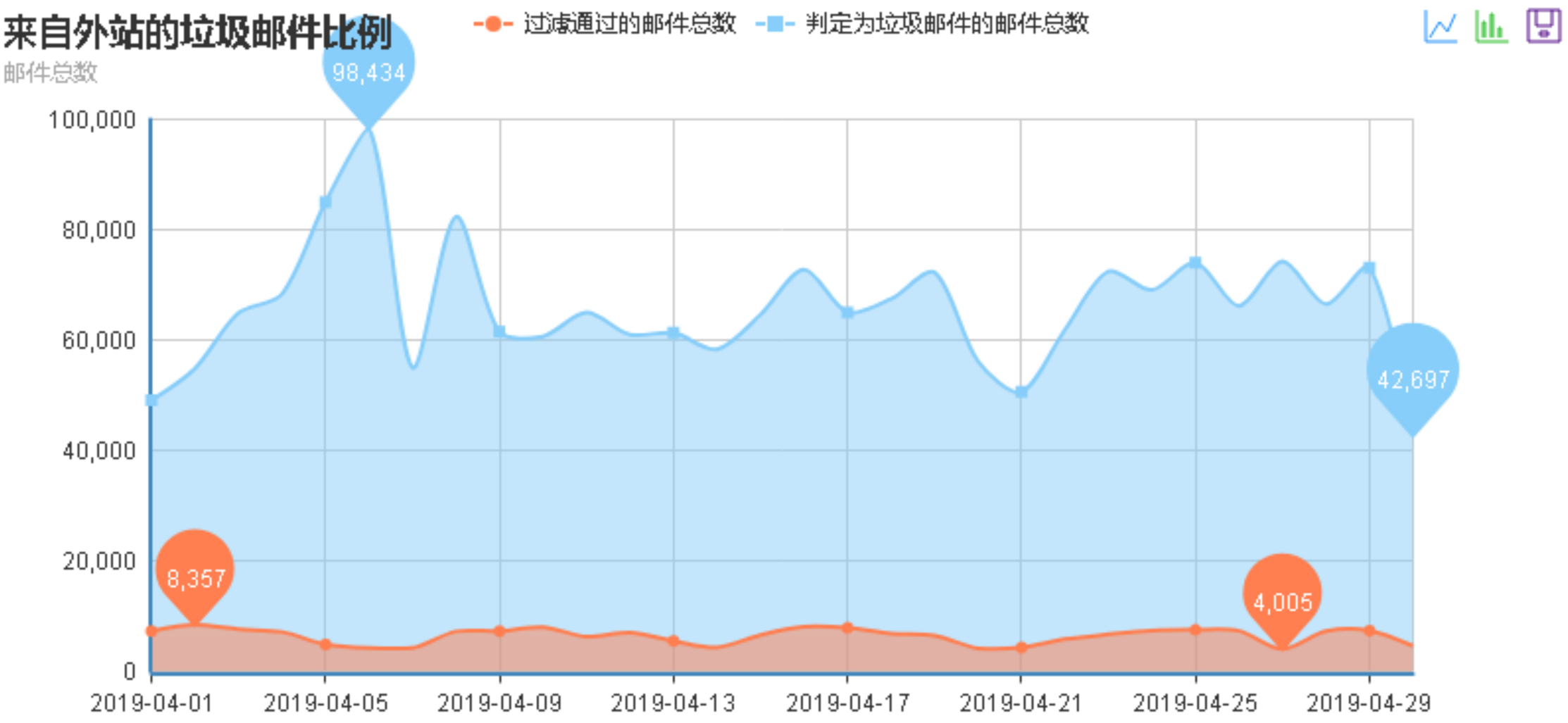


*注：以上数据由 Panabit® 飞享 ifeixiang.com 友情提供

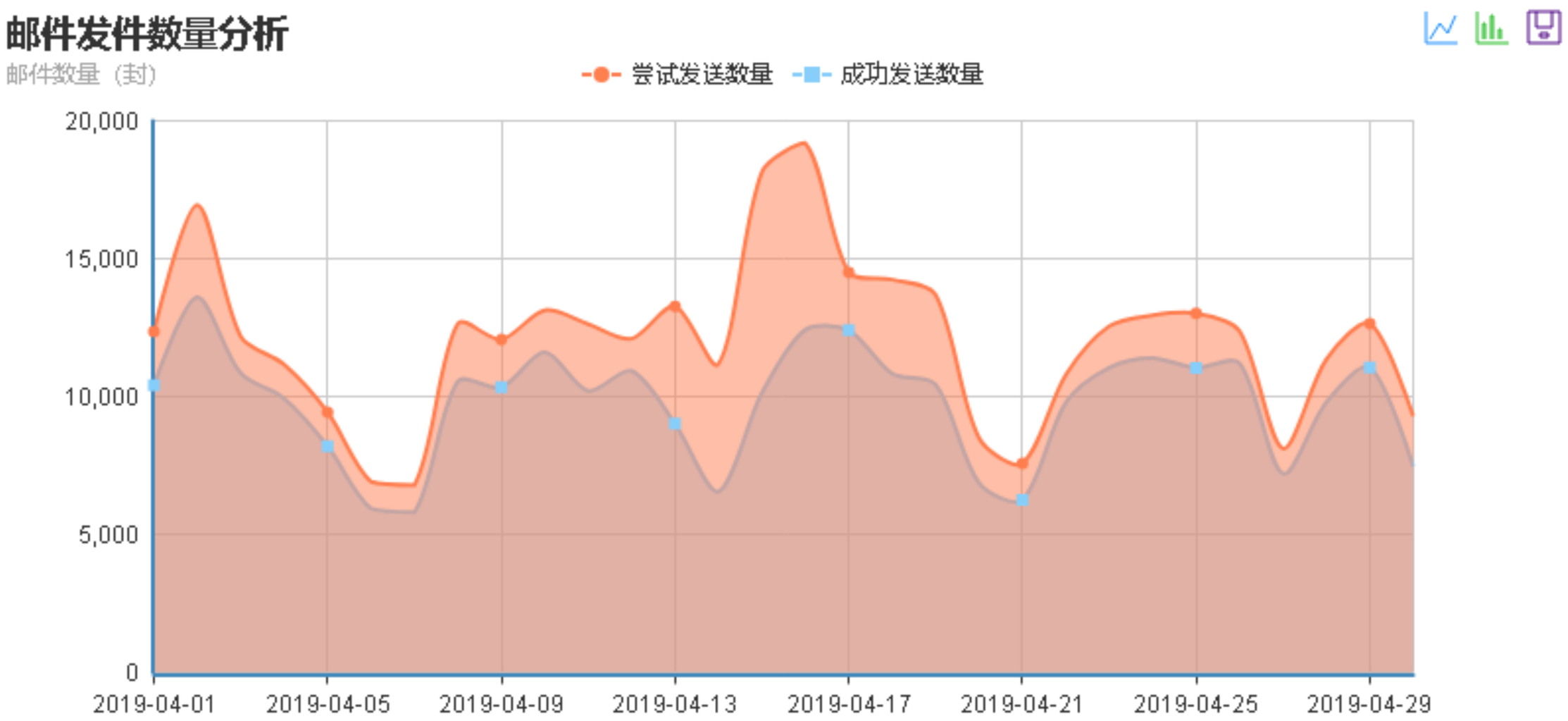
校园电子邮件系统运行情况分析

2019年4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6.6万封，日均发送邮件9774封。（李博鑫）

校园邮件系统垃圾邮件拦截数据统计



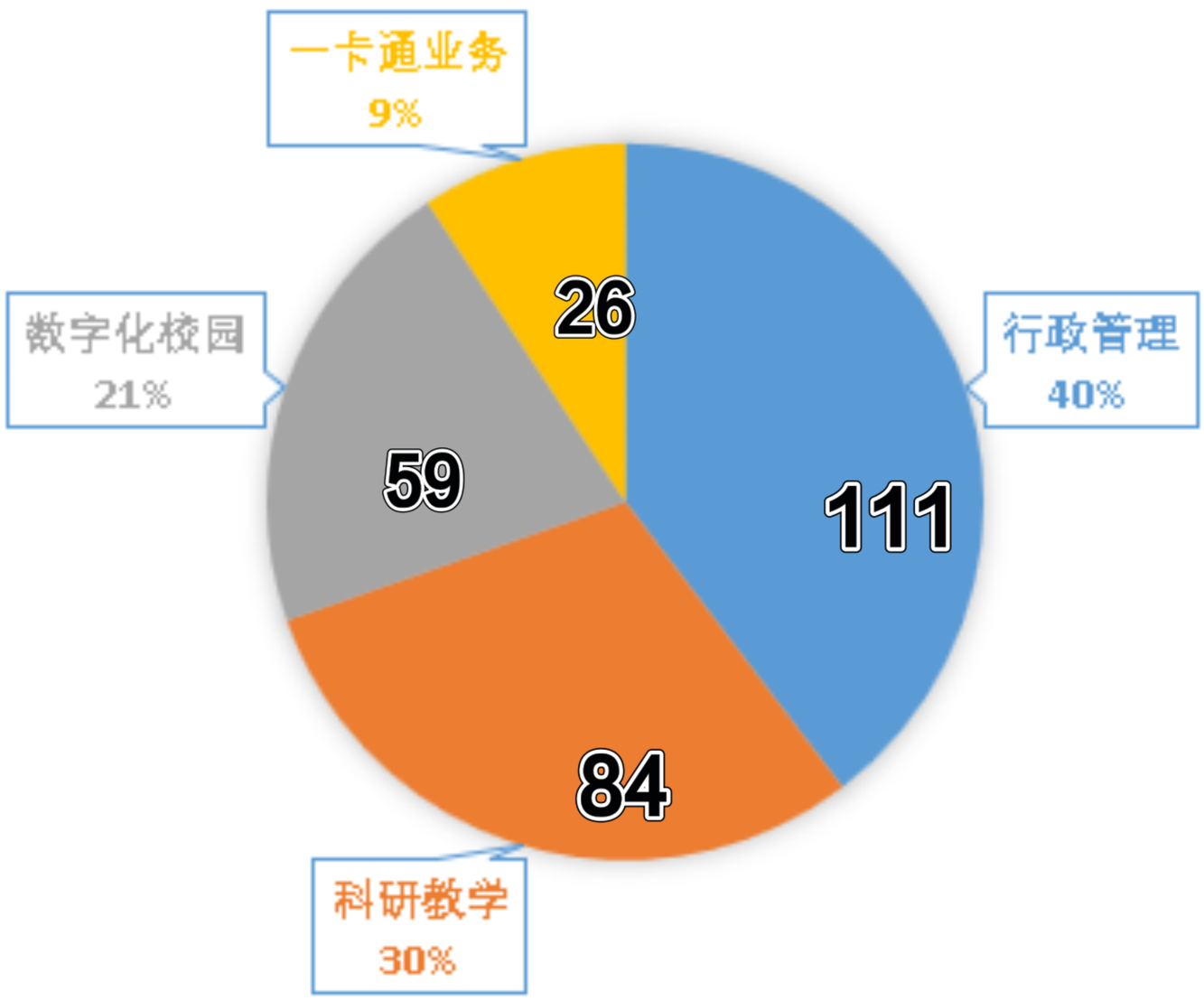
校园邮件系统邮件发送数据统计



数据中心运行报告

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）

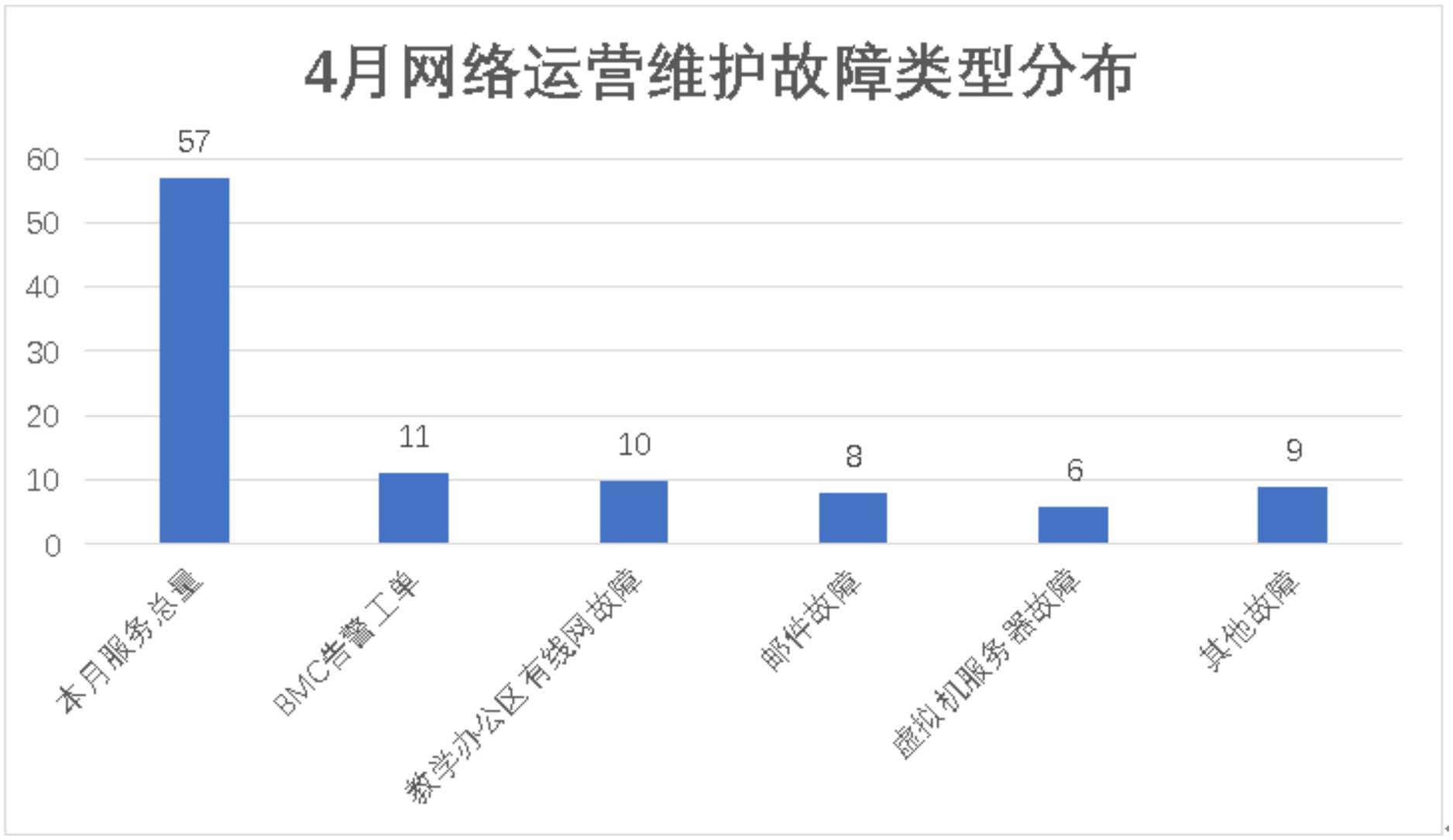
4月数据中心虚机情况统计

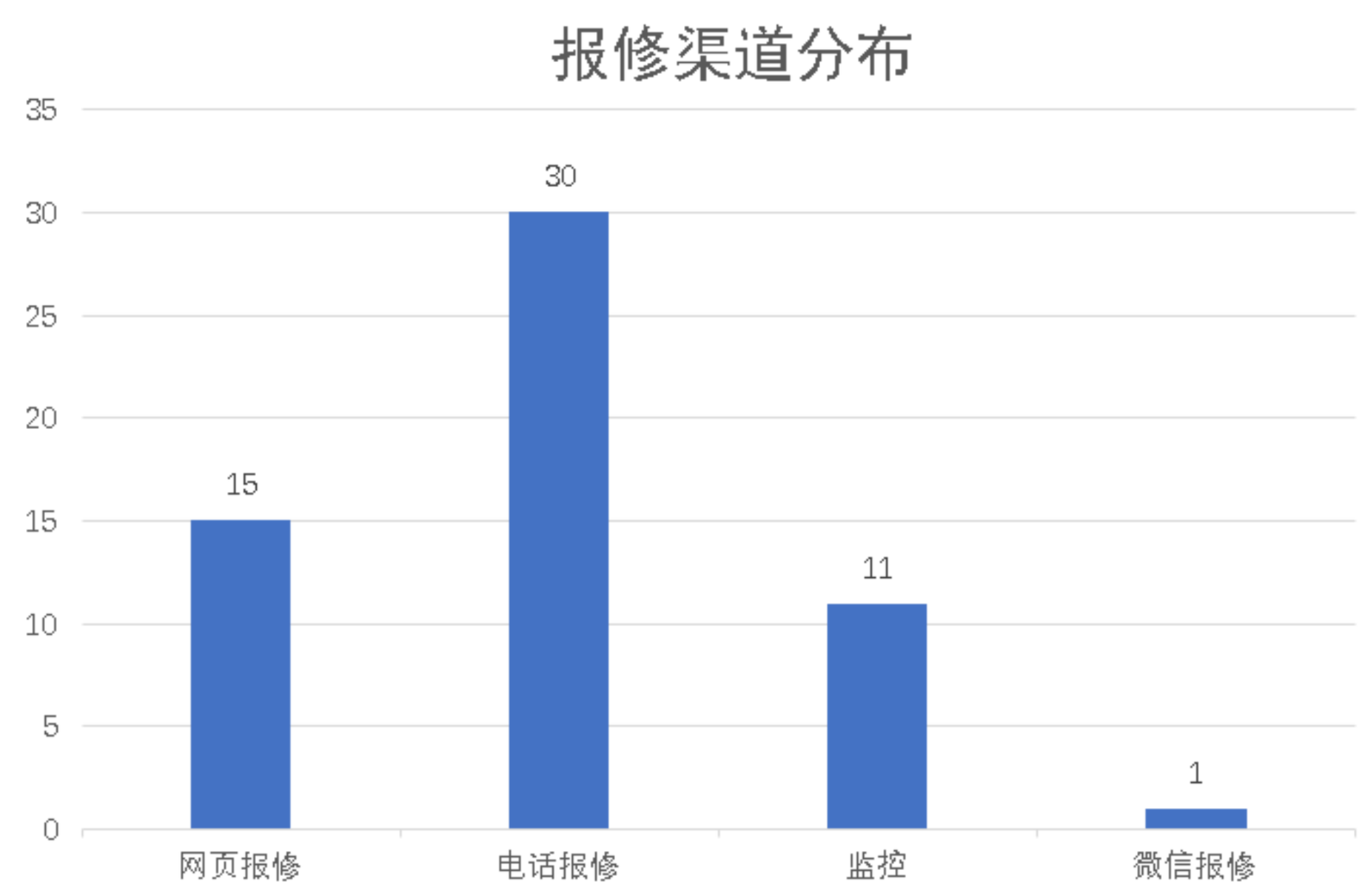


数据中心机房整体运行稳定，其中4月8日及4月27日停电2次，UPS电池供电正常，服务器及网络设备未出现停机。中心机房空调故障6次，已及时处理，未影响机房整体制冷环境。（赵阳）

校园网运维数据分析

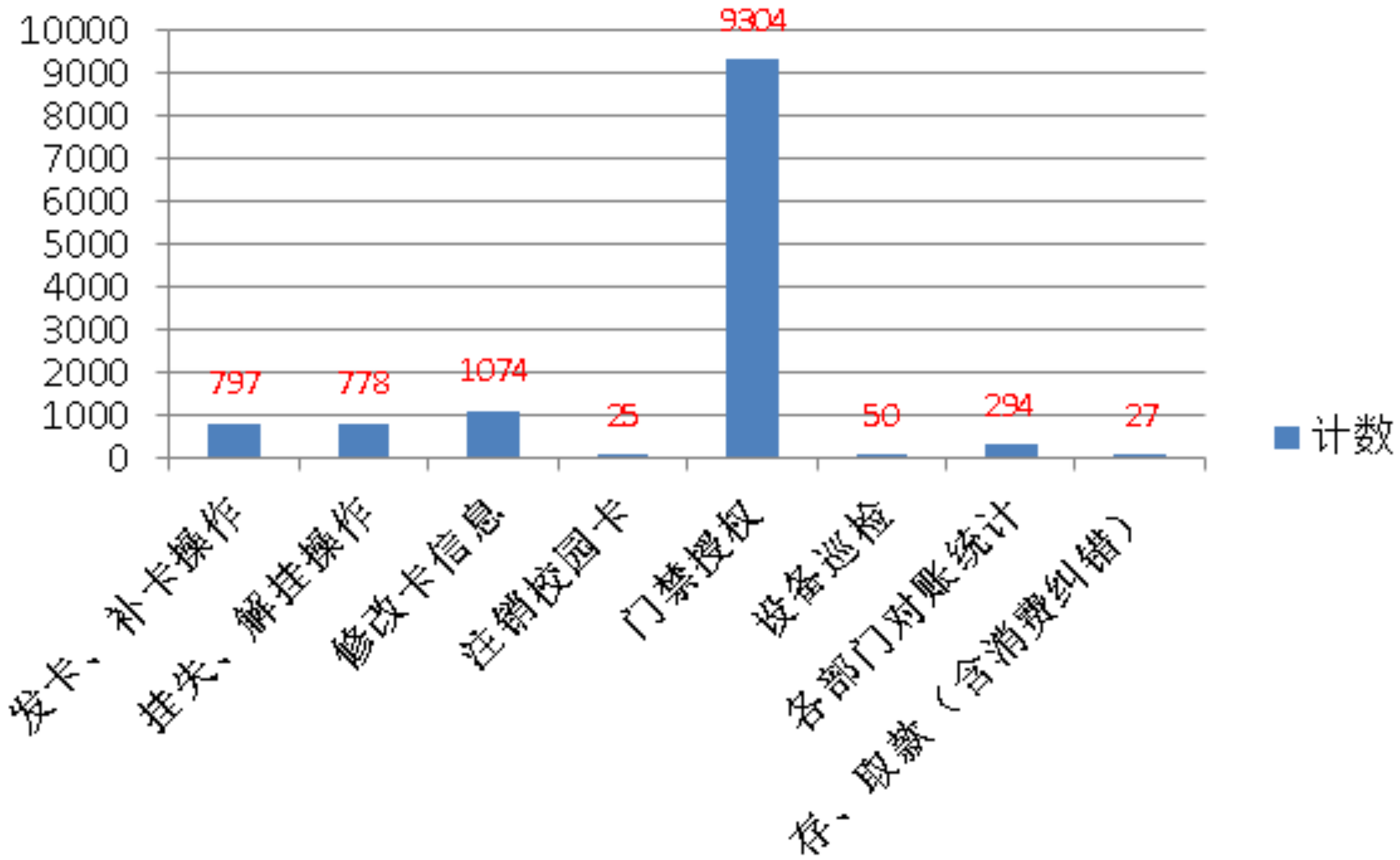
2019年4月，网络信息管理中心共受理各类故障、告警57件，接到报修、业务申请后均能第一时间响应并及时解决问题，保证了校园网正常运行。（殷仕刚）



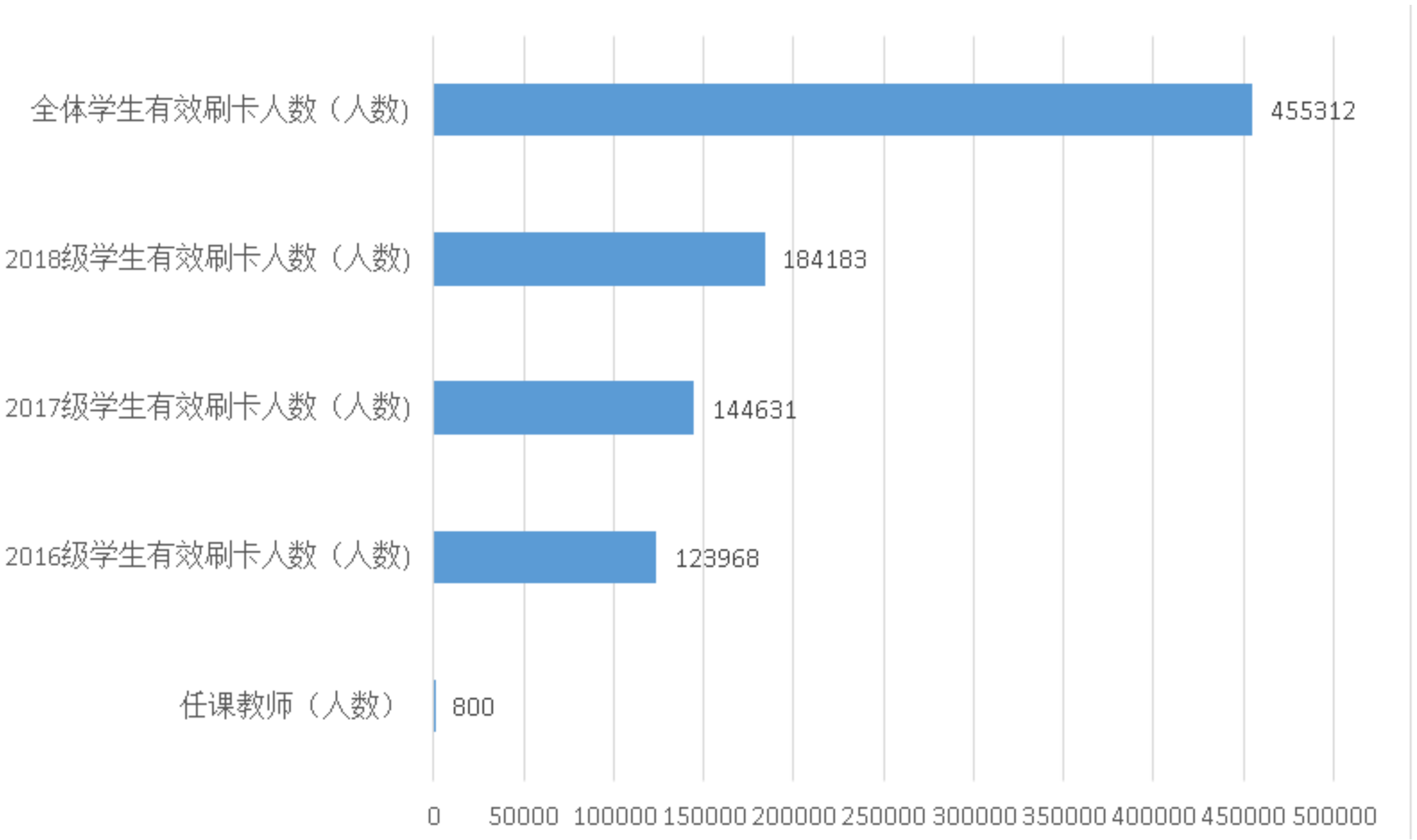


校园卡务中心月度数据统计

校园卡务中心工作数据统计

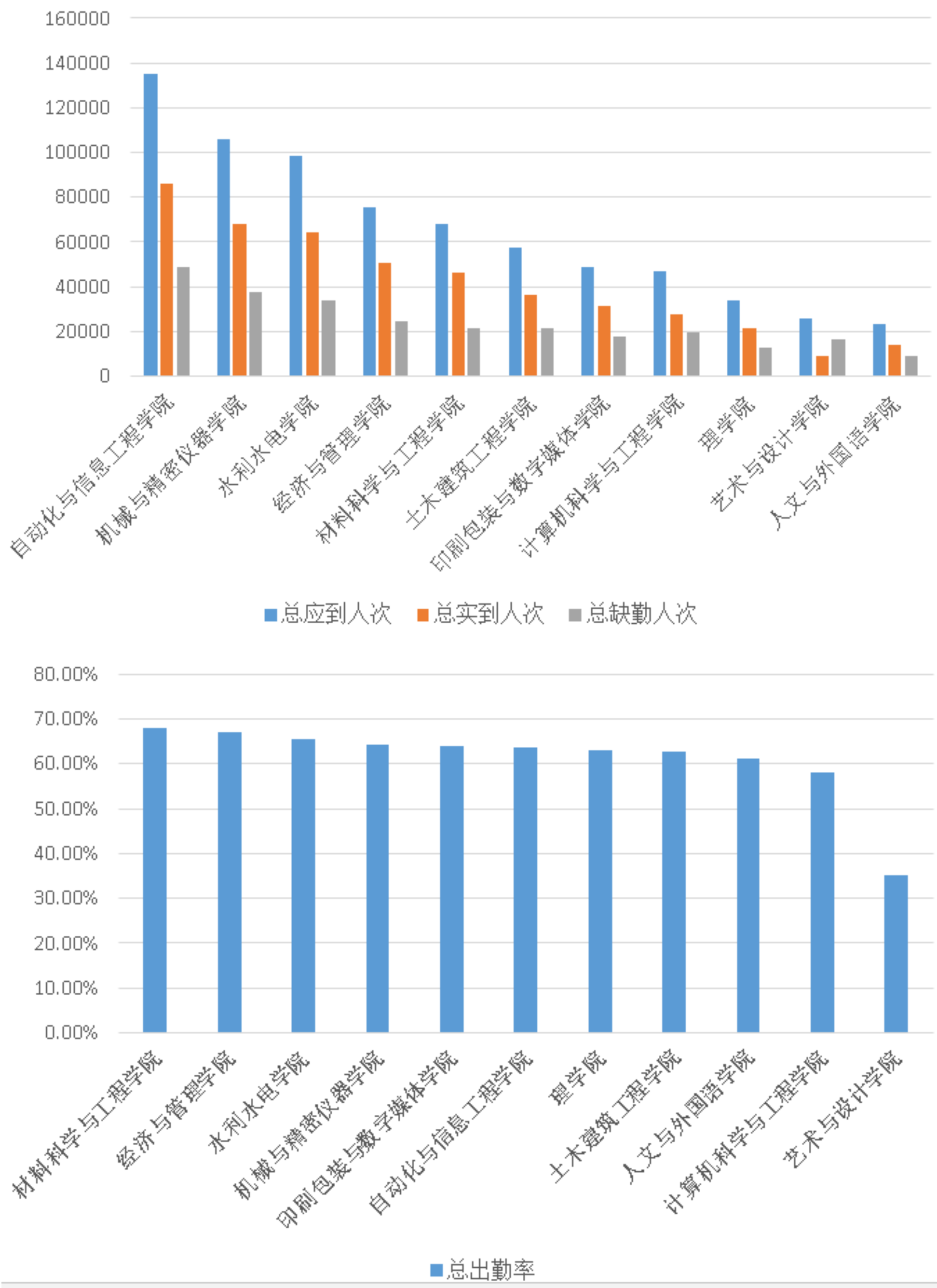


2019年4月教务考勤系统运行情况统计图



校园卡务中心月度数据统计

2019年4月教务考勤数据统计图



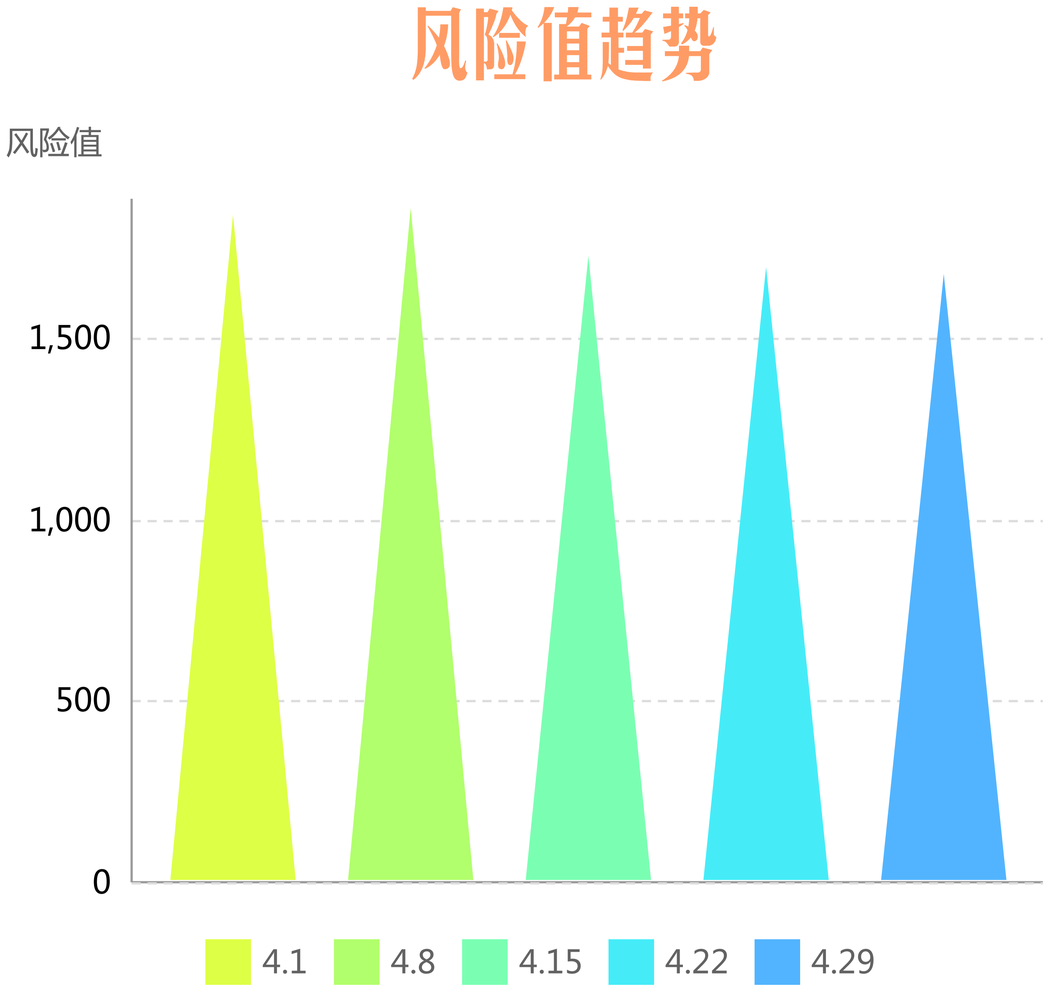
校园网络安全趋势

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4月1日-30日。

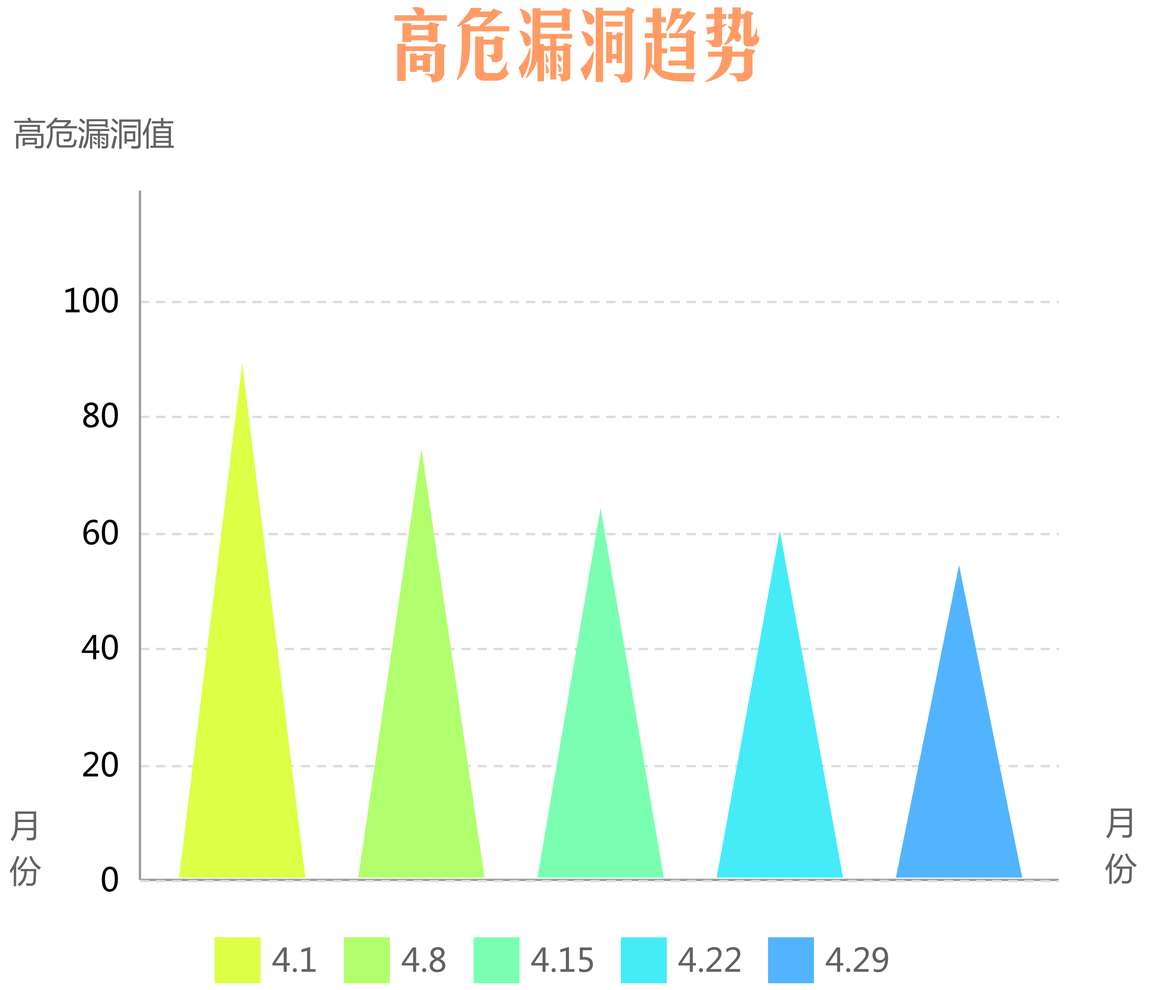
通过常态化安全监测等一系列行动治理，我校本月网络安全状况整体评价为良，风险情况总体良好。（王心成）

2019年4月网络安全态势分布图

风险值趋势



高危漏洞趋势



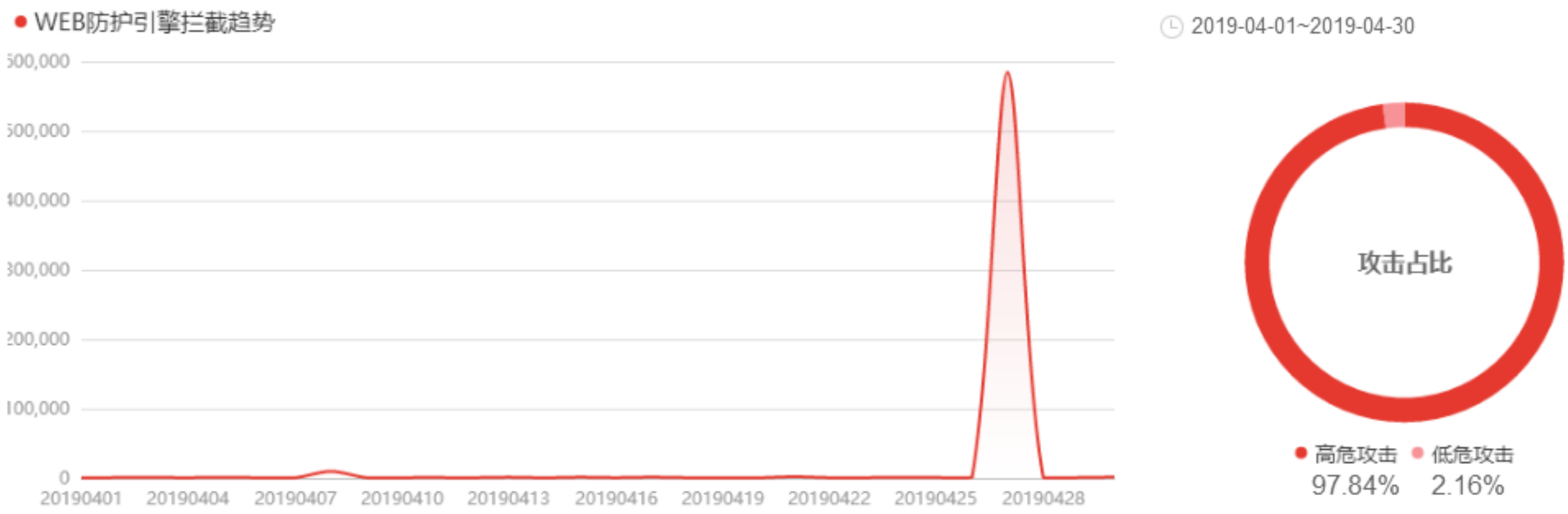
重要信息系统（网站）基本情况

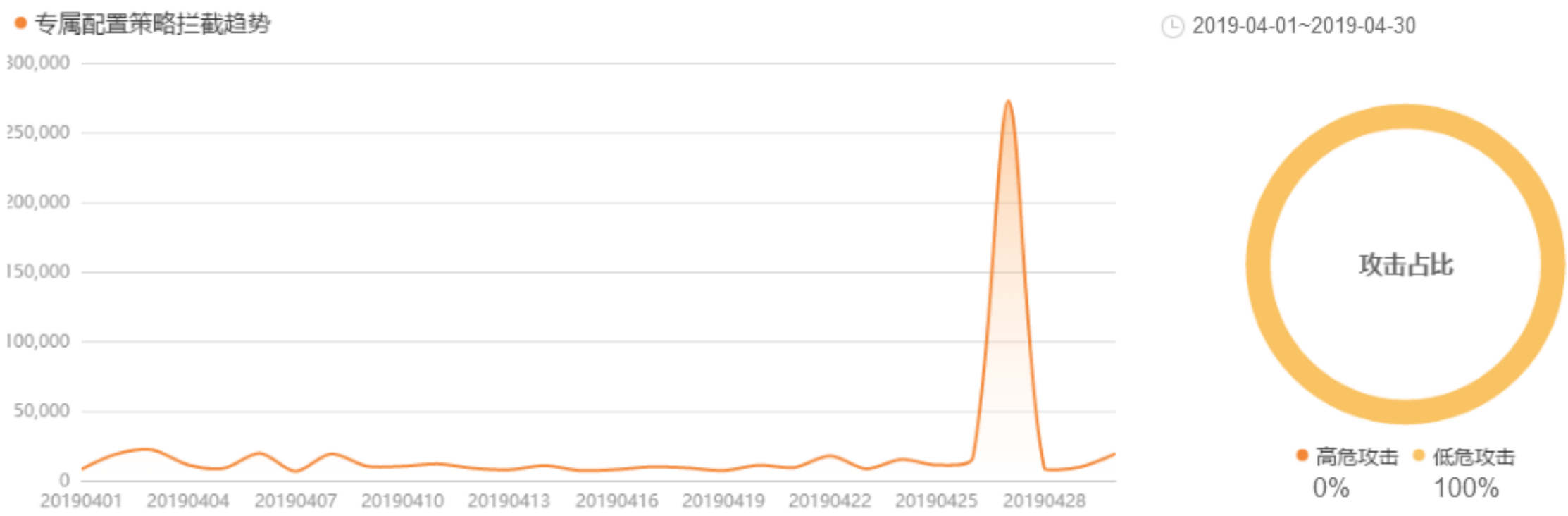
总请求数	总流量	搜索引擎	Alexa 全球排名
27254029次	2071.68GB	337,434次	98116

校园网络安全趋势

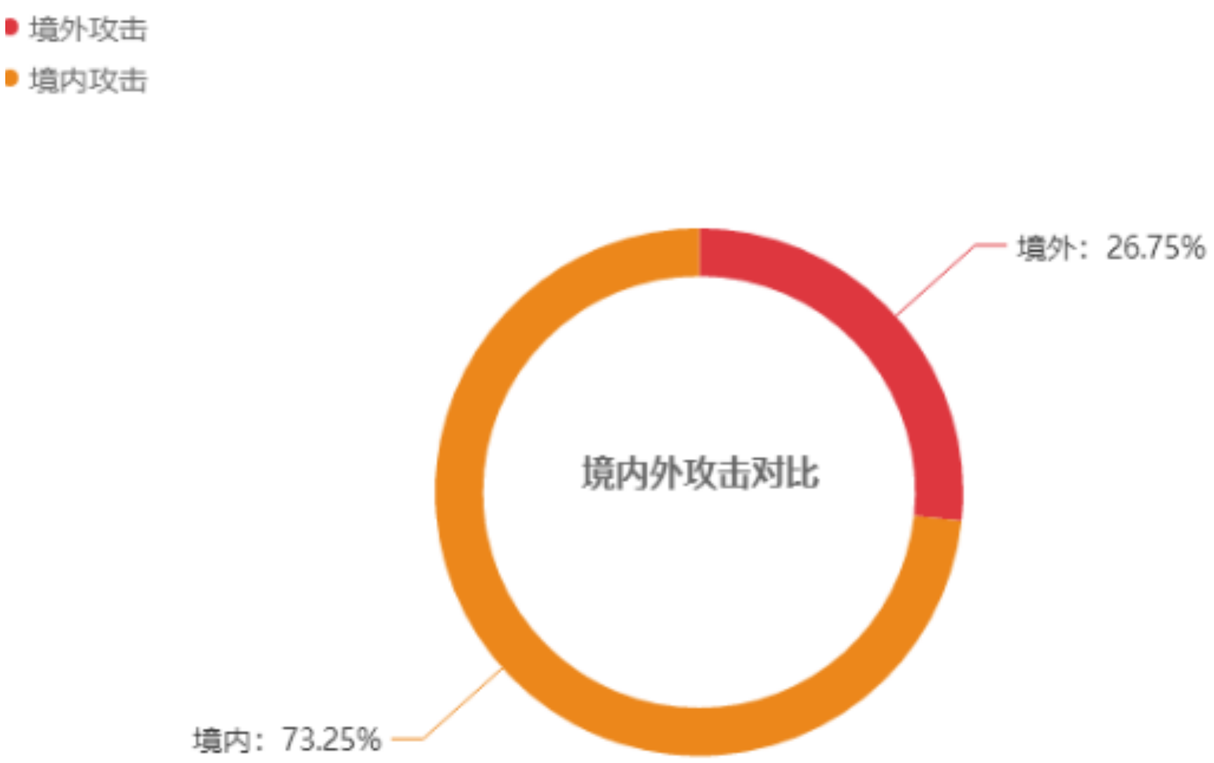
本攻击拦截态势和网络攻击态势分布图以网络信息管理中心监测的数据作为主要依据，对我校重要信息系统（网站）面临的各类安全威胁及基本情况进行态势分析，评估范围为2019年4月1日-30日。（王心成）

2019年4月1日-4月30日攻击拦截态势和网络攻击态势分布





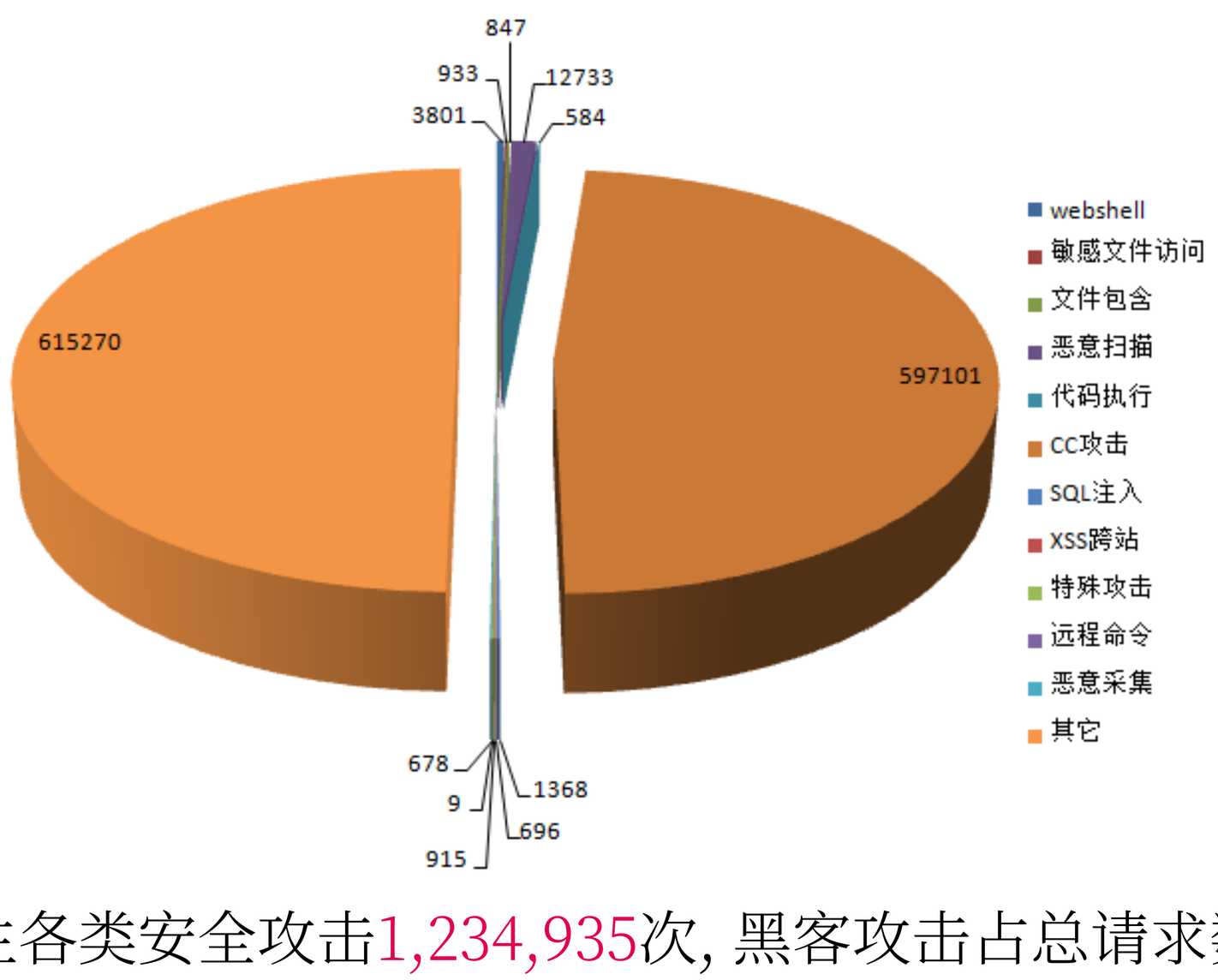
2019年4月1日-4月30日攻击拦截态势和网络攻击态势分布



境外攻击分布来源Top10

国家名称	攻击次数
美国	40205
南非	3637
亚太地区	1156
菲律宾	1069
柬埔寨	814
印度	723
新加坡	466
马来西亚	447
法国	216
日本	203

2019年4月1日-4月30日网站遭受黑客攻击分布图



本月共发生各类安全攻击1,234,935次，黑客攻击占总请求数的比率为4.63%，其中敏感文件访问933次、Webshell攻击3,801次、文件包含攻击847次、恶意扫描12,733次、代码执行584次、CC攻击597,101次、SQL注入1,368次、XSS跨站攻击696次、特殊攻击915次、恶意信息采集678次，其它类型攻击615,270次。（王心成）

Anubis Android 银行木马技术分析及新近活动总结

Anubis是一种Android银行恶意软件，自2017年以来已经为全球100多个国家，300多家金融机构带来了相当大的麻烦。截止目前，爆发地主要为欧洲国家，国内暂未发现该木马。

(奇安信威胁情报中心)

Anubis主要通过伪装成金融应用、手机游戏、购物应用、软件更新、邮件应用、浏览器应用甚至物流应用等，从而渗透进谷歌应用商店，诱骗用户下载安装。

背景介绍

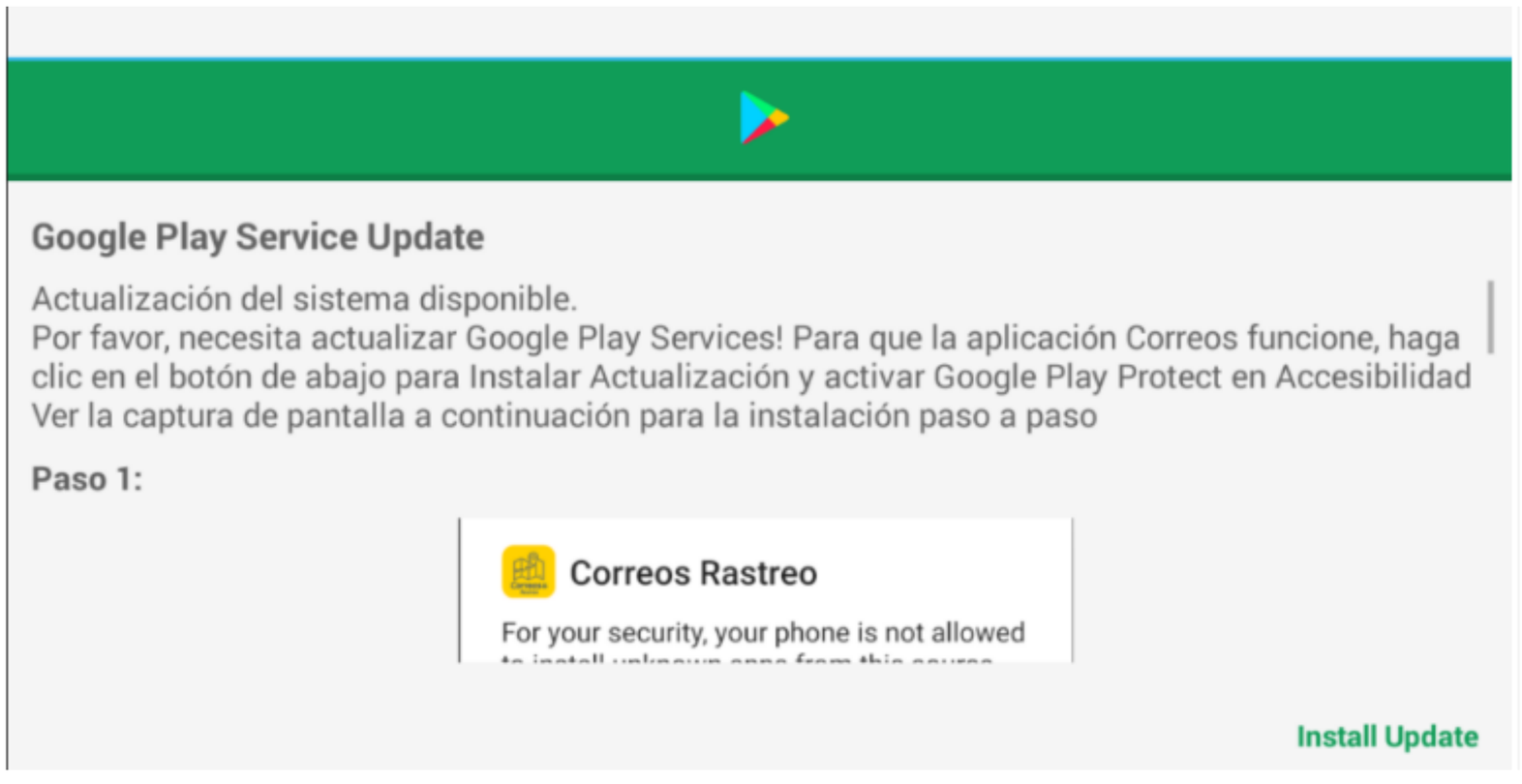
Anubis通过仿冒各种应用诱骗用户安装使用，当软件被激活后，会展现给用户一个仿冒的钓鱼页面，从而获取用户敏感信息，如银行账号密码等。其具备一般银行木马的功能，包括屏蔽用户短信，获取转发用户短信等功能。Anubis同时可以从服务端获取远控指令，对用户手机进行进一步控制。Anubis还是第一个集成勒索软件功能的Android银行木马。Anubis功能之多、之强大，甚至可以作为间谍软件进行使用。

样本执行流程（邮政运营商为例）

仿冒西班牙邮政运营商Correos的恶意软件，运行后会释放仿冒为Google Play Service Updater V2.1的木马程序，诱骗用户安装更新。

样本执行流程

仿冒为Correos的程序运行后，会诱骗用户安装更新Google Play，而该更新软件即为Anubis木马程序



当Anubis木马运行后，先隐藏自身，达到保护自身的目的；通过服务器可以下发30多种指令，获取对用户手机的全面控制权，其中主要功能有，获取键盘记录、加密用户手机文件、开启VNC远程、打开指定web界面等。

主要远控指令	指令对应的功能
Send_GO_SMS	向指定电话号码发送指定内容
nymBePsG0	获取用户手机通讯录
GetSWSGO	获取用户手机短信
	telbookgotext=
getapps	获取用户手机已安装应用
getpermissions	获取已有的权限信息
startaccessibility	权限请求
startpermission	权限请求
=ALERT|	提示消息
=PUSH|	推送通知
startAutoPush	根据不同国家，推送不同的消息
RequestPermissionGPS	请求获取地理位置权限
|ussd=	呼叫转移
|recordsound=	录音

新近活动

安全厂商对2019年后的Anubis样本进行了数据统计，统计Anubis仿冒的主要图标，可以发现，Anubis木马主要通过仿冒一些主流的应用或者浏览器插件，诱骗用户进行更新，从而可以最大限度的迷惑用户，使木马本身可以顺利安装到用户手机中。此外Anubis自爆发以来仿冒过全球378个金融机构应用程序信息。

Anubis自爆发以来，其主要活动区域在欧美等地，虽然目前国内暂时没有发现此类银行木马，但其代码字符串混淆中，含有中文混淆方案，所以依然值得我们警惕。Anubis主要以渗透进入谷歌商店为主要传播平台，木马本身以仿冒金融机构、主流应用程序、浏览器插件为主要伪装手段。虽然谷歌商店一直在清理相关恶意木马，但仍然有残留的软件在活跃。（王心成）

1 IE 11浏览器被爆安全漏洞：可远程窃取本地PC文件

在处理.MHT已保存页面的时候能够让黑客窃取PC上的文件。而.MHT文件格式的默认处理应用程序是IE 11浏览器，因此即使将Chrome作为默认网页浏览器这个尚未修复的漏洞依然有效。该漏洞是钓鱼网络攻击的理想选择。

解决方案:

该漏洞适用于Windows 7/8.1/10系统。在微软正式修复IE 11浏览器上的漏洞之前，推荐用户尤其是企业用户尽量减少通过IE 11浏览器下载和点击不明文件。

2 McAfee Network Security Manager权限提升漏洞（CNVD-2019-12787）

McAfee Network Security Manager中存在安全漏洞。攻击者可利用该漏洞绕过限制，提升权限。

影响产品： McAfee Network Security Manager（NSM）

解决方案:

用户可参考如下厂商提供的安全补丁以修复该漏洞：https://kc.mcafee.com/corporate/index?page=content&id=SB10275

3 Oracle MySQL Server拒绝服务漏洞（CNVD-2019-12459）

Oracle MySQL中的MySQL Server组件5.7.25及之前版本和8.0.15及之前版本的Server: PS子组件存在安全漏洞。攻击者可利用该漏洞造成拒绝服务（挂起或频繁崩溃），影响数据的可用性。

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://www.oracle.com/technetwork/security-advisory/cpuapr2019verbose-5072824.html

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