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

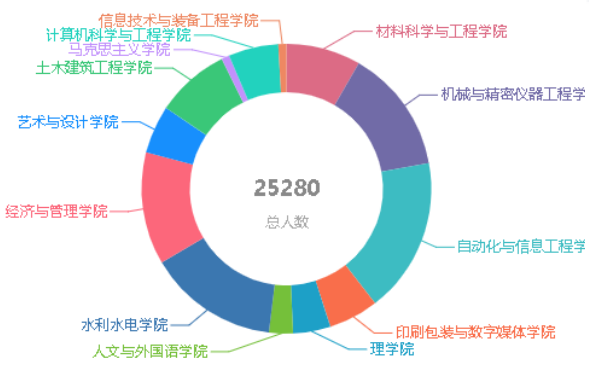
2019年3月

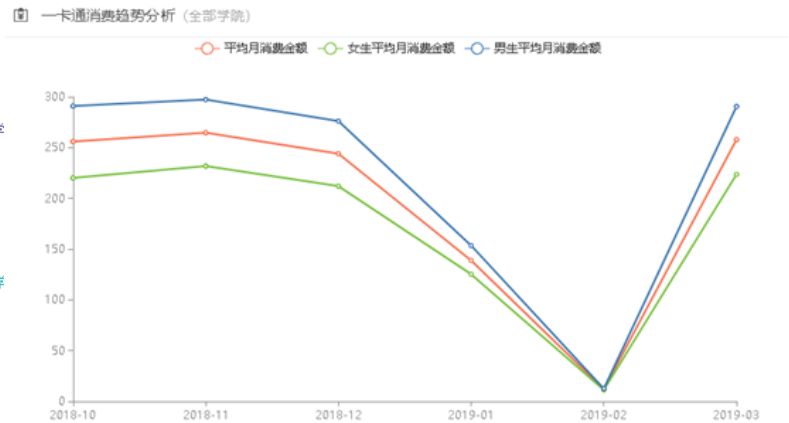
目录

我校召开学生大数据工作会议

3月28日上午，网络信息管理中心会同教务处、学生处和研究生院召开学生大数据工作会议，校党委副书记崔亦国出席会议并讲话。会上，大数据分析与服务平台建设方相关负责人就学生大数据分析与服务平台的建设进度、推进计划和亟待解决的问题进行了详细汇报，并就后期如何顺利开展建设计划与各部门相关负责人进行了热烈讨论。

学生大数据平台通过整合学校数据资源，进行跨域关联、分析，为学校教育教学提供辅助。建设可扩展的全方位大数据管理平台，为充实我校整体数据信息化建设和数据的积累打下坚实的基础，充分发挥我校数据的价值，为学生服务和管理提供数据支持。（雷龙涛）

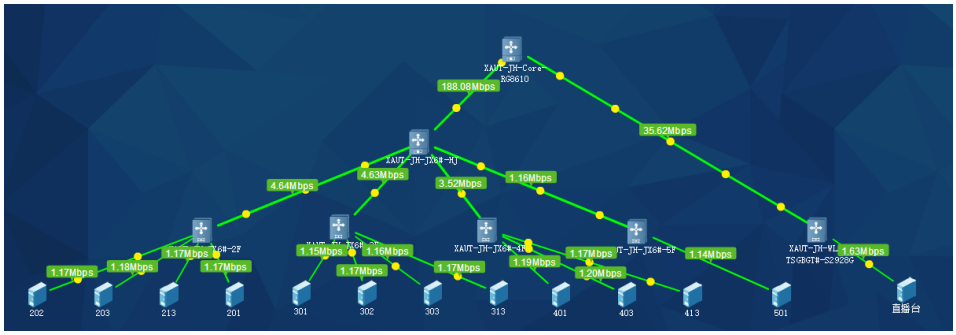




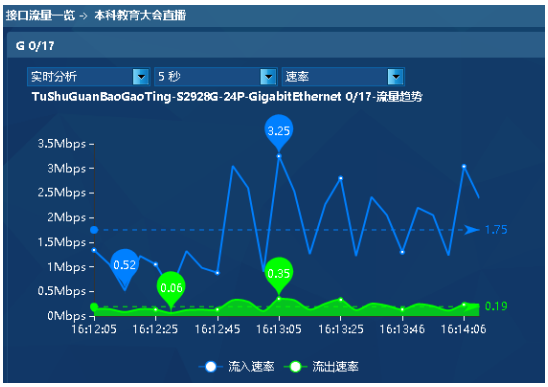
本科教育工作会议网络保障工作圆满完成

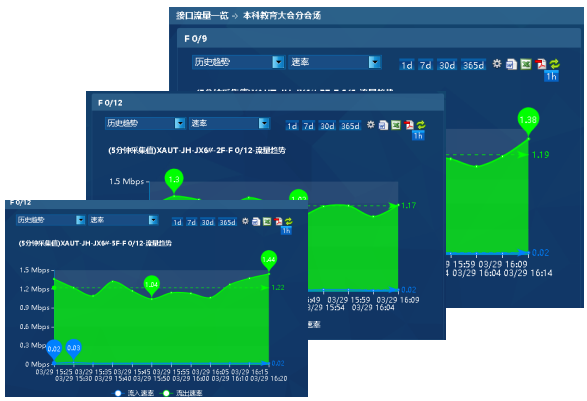
3月29日-31日，本科教育工作会议在我校举行。为确保本科教育工作会议网络视频直播的正常进行，网络信息管理中心充分做好保障工作，对图书馆报告厅主会场及教六楼12个分会场网络接入环境进行了全面检查和测试，并在会议直播期间对网络运行情况进行全方位的网络质量监控。监控数据显示，会议期间未发生网络故障，各会场网络视频直播清晰流畅，圆满完成网络保障任务。（李博鑫）

01 会议直播业务网络拓扑



02 各会场网络流量实时监控

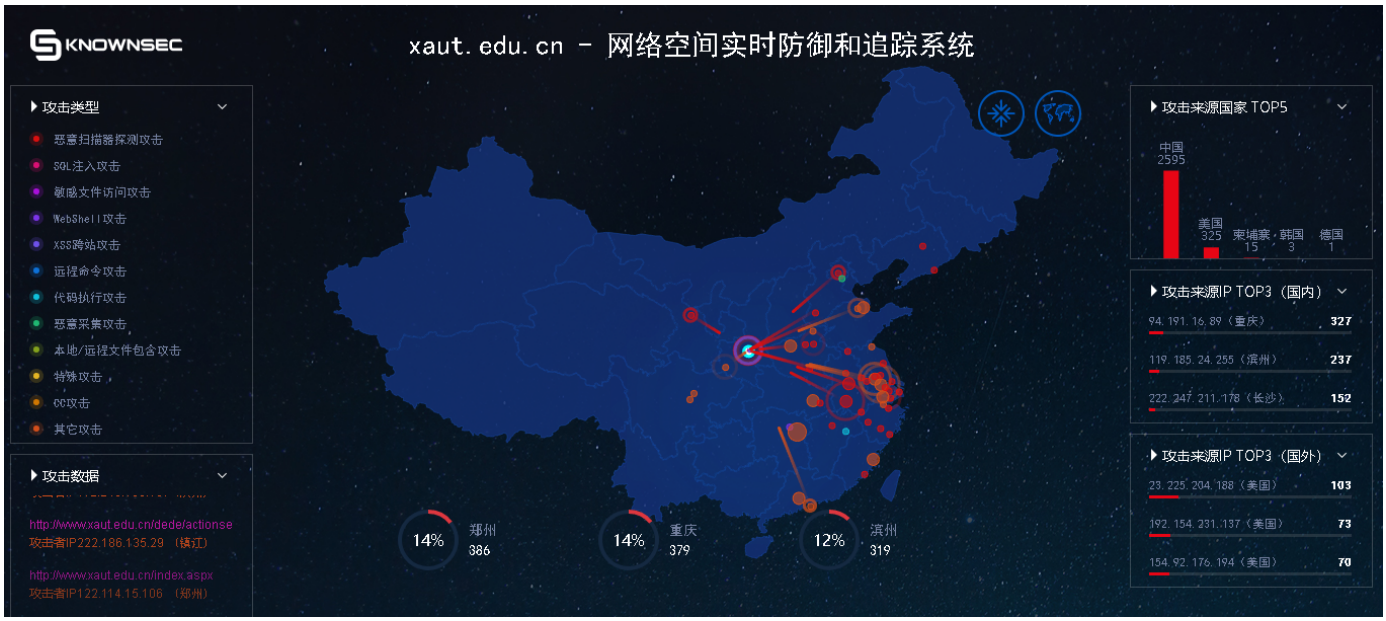




网络信息管理中心开展2019年春季学期网络安全综合治理行动

为全面贯彻中省关于网络安全工作的统筹部署，落实《中华人民共和国网络安全法》和陕西省教育厅《关于进一步加强我省教育信息系统安全应急处置工作的通知》等文件精神要求，有效防范和抵御安全风险隐患，切实保障信息系统（网站）稳定运行和数据安全，网络信息管理中心自3月27日起开展以“堵塞安全漏洞、规范安全管理”为目标的网络安全综合治理行动，全面查找发现各类安全漏洞和突出问题。

本次治理工作共计处理问题网站14个高危信息系统（网站）；通过对学校信息系统（网站）的排查，存在7个“双非”信息系统；需要整改或补充登记信息的虚拟服务器18台。（王心成）



校园信息系统（网站）安全状态总览

校园一卡通工本费缴纳支持财务处统一支付平台

按照学校相关工作计划和工作安排，进一步方便广大师生缴纳校园一卡通工本费（补卡、换卡），网络信息管理中心从本学期开始新增移动支付手段收取校园一卡通工本费。我校各类临时办卡人员或因遗失等原因需补办新卡的师生均可通过微信、支付宝扫描二维码的方式或者登录西安理工大学微信企业号方式缴纳补卡费。

此项工作的顺利开展，丰富了校园一卡通工本费的缴纳方式，师生可自行选择喜欢的方式缴纳补卡费。我中心会一如既往地开拓校园一卡通新应用，扩展新场景，为广大师生提供优质的服务。

01 使用西安理工大学企业微信缴费

校内师生可通过“西安理工大学微信企业号”—“财务缴费”—“生活缴费”—“网络中心一卡通补卡费”进行缴费，备注信息内输入班级信息，如“会计151”，并完成支付，点击主界面左上角“≡”，可查询交费订单并作为交费凭据。

02 校园统一支付平台

第一步 微信或支付宝扫描支付平台二维码；

第二步 扫码后登录（用户名：学号，密码：六个零）；

第三步 点击“生活缴费”选择“网络中心一卡通补卡费”；

第四步 备注信息内输入班级信息如“会计151”并完成支付；

第五步 点击主界面左上角“≡”，可查询交费订单并作为交费凭据。

（王力）

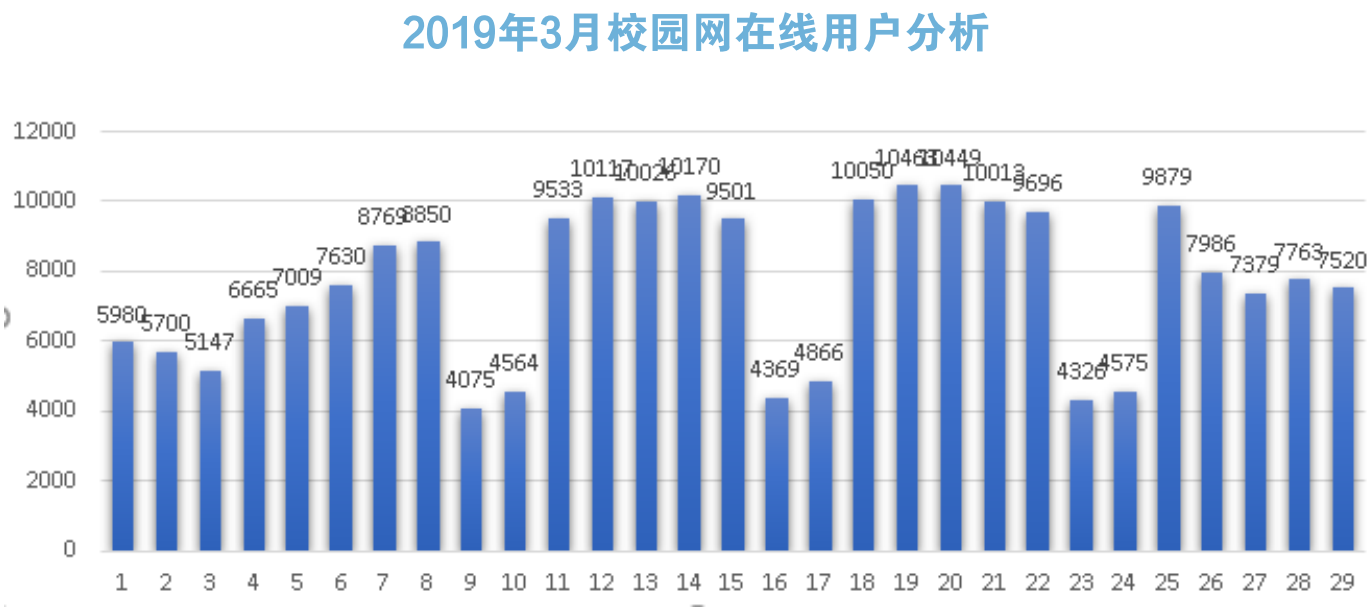
信息档案支部集中学习宣讲全省教育大会精神

遵照学校党委办公室《关于深入学习贯彻全国全省教育大会及相关文件精神的通知》和机关党委《关于传达学习全国、全省教育大会及学校工作会精神的通知》文件精神，信息档案支部以党小组讨论形式，分别在网络信息管理中心会议室和档案馆会议室组织召开了党小组会议。

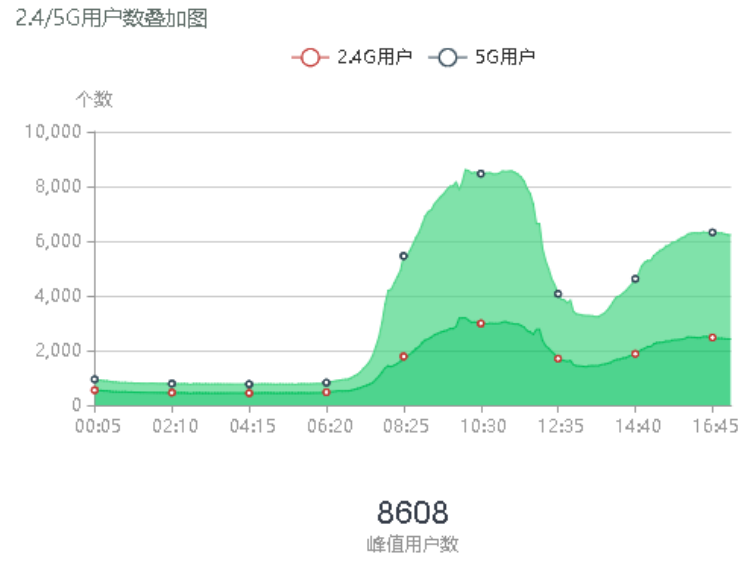
2019年1月9日，陕西省委、省政府在西安召开全省教育大会。这次大会在习近平新时代中国特色社会主义思想和党的十九大精神指引下，深入学习贯彻习近平总书记关于教育的重要论述和全国教育大会精神，全面贯彻落实党的教育方针，分析面临形势，安排部署新时代全省教育改革发展的各项工作。省委书记胡和平出席会议并讲话，省长刘国中主持并做总结讲话，教育部副部长郑富芝出席会议并讲话，省委副书记贺荣就会议贯彻落实提出了明确要求。

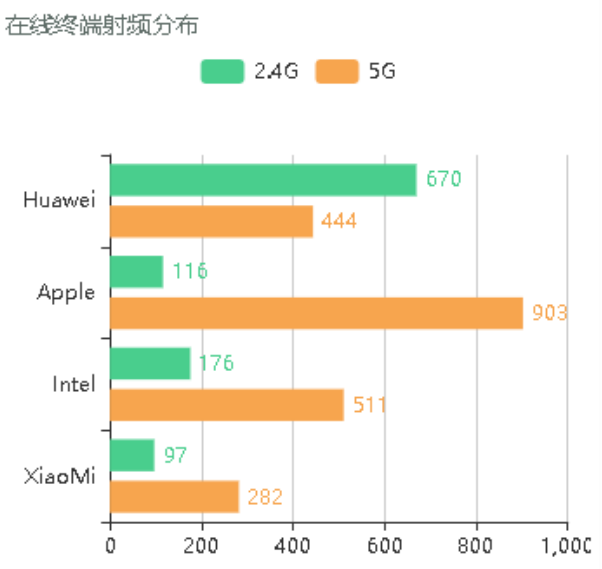
通过学习，大家纷纷表示，要认真学习贯彻全省教育大会精神，以饱满的工作热情迎接即将到来的学校本科教育大会。立足本职工作，为学校本科教学建言献策，做好服务。（杨超）

校园网在线用户分析



3月，校园网整体运行正常，日均在线用户7692人，其中无线用户日均在线5621人。近期校园无线网已成为主干网络。

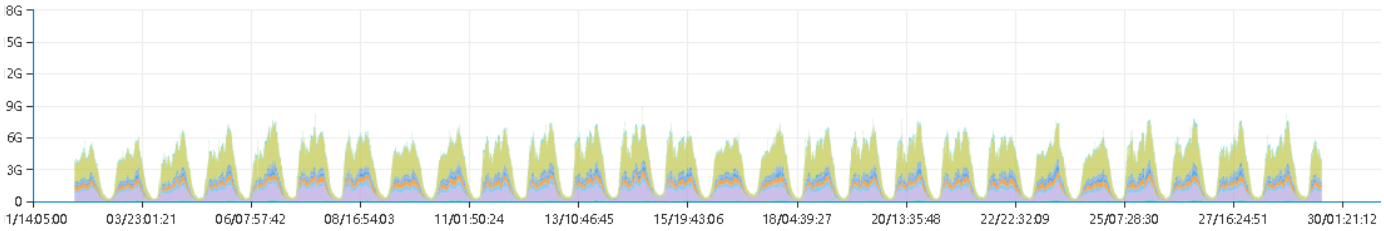




校园网用户终端主力已经从2.4G转为5G，随着用户终端的不断更新换代，我校无线终端的平均接入速度有明显提升。

校园网出口流量分析

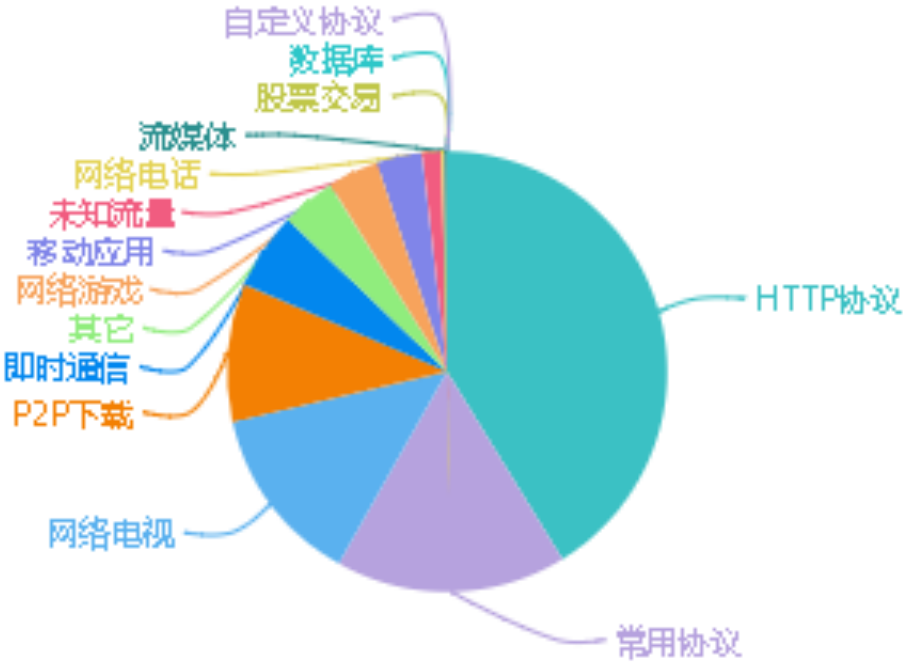
校园网出口流量趋势图



校园网出口峰值使用带宽近6G，2019年3月，校园网总下载流量达1.1PB，上传流量共计400T。

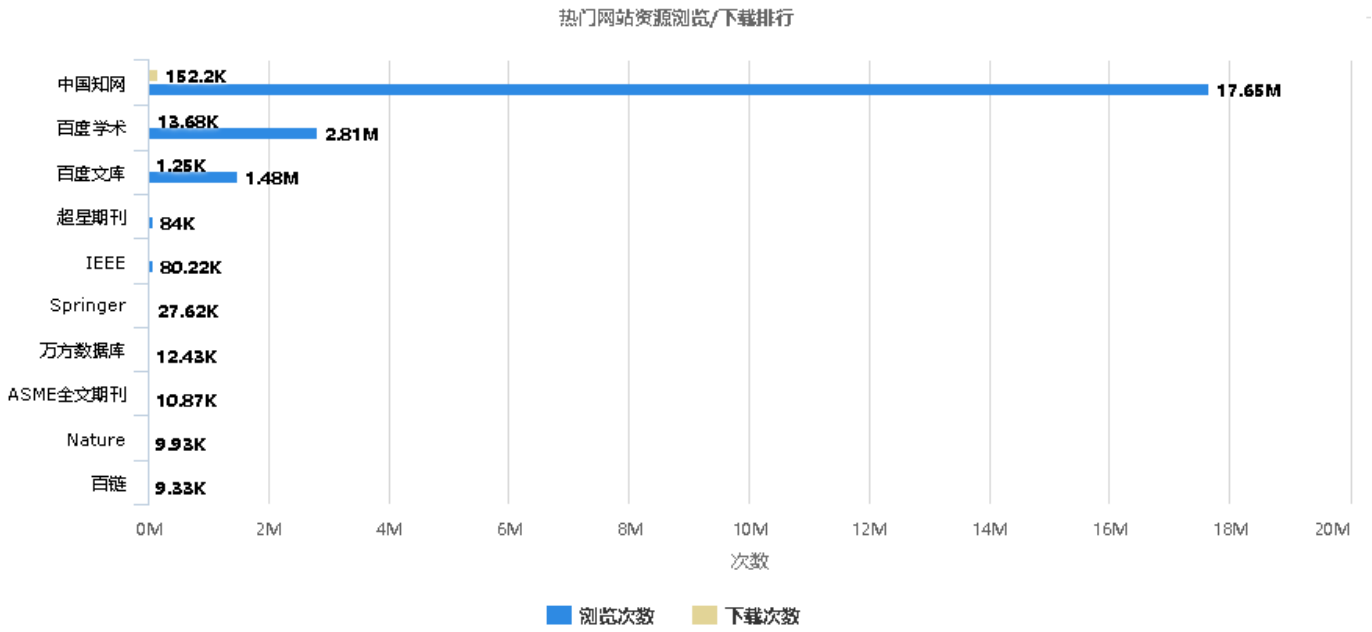
其中，HTTP日常访问产生流量达571T位居首位，迅雷等P2P下载流量及网络电视流量位居二三位，分别为140T和182T。

校园网出口流量分布图

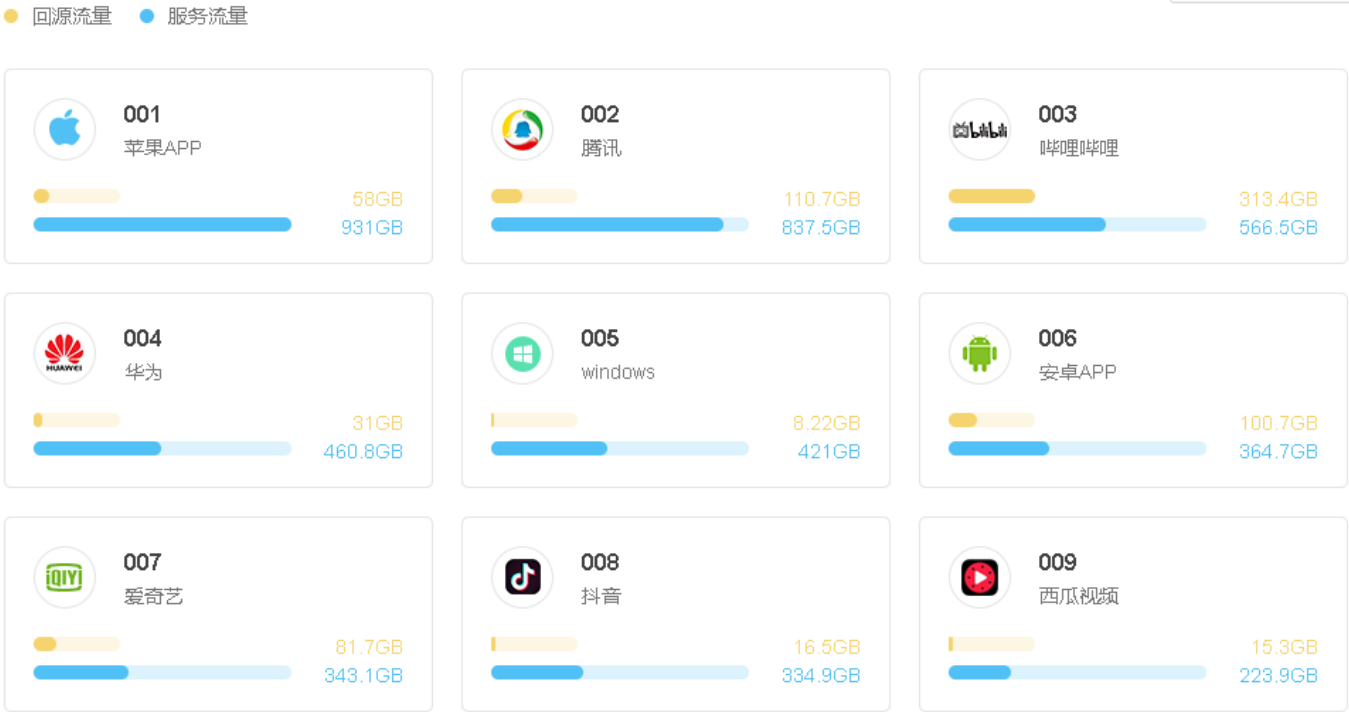


校园网资源使用分析

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

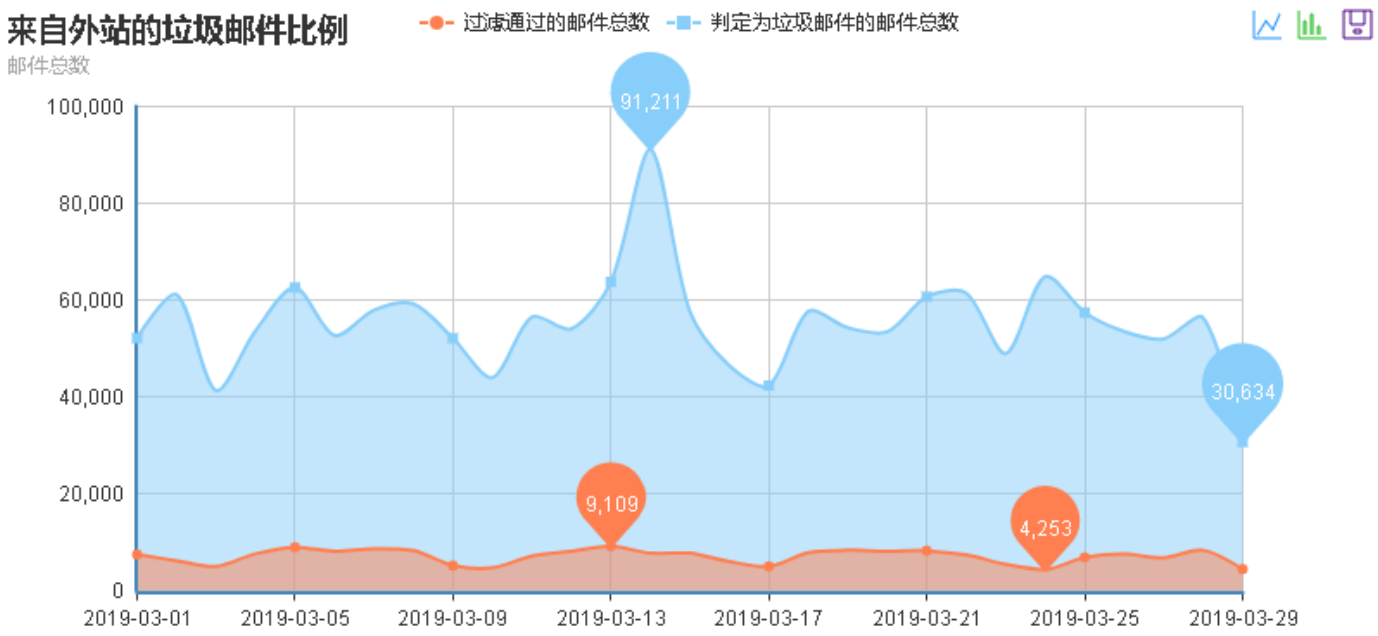


*注：以上数据由 Panabit® 友情提供

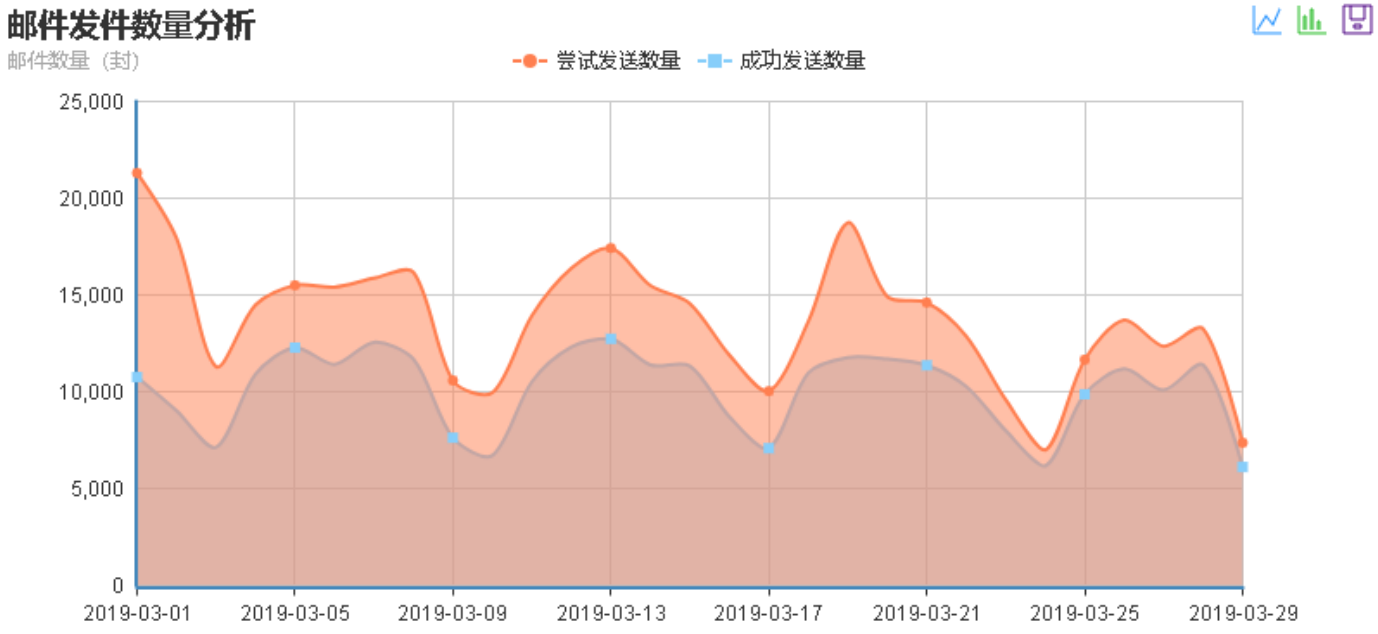
校园电子邮件系统运行情况分析

2019年3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6万封，日均发送邮件9600封。

校园邮件系统垃圾邮件拦截数据统计

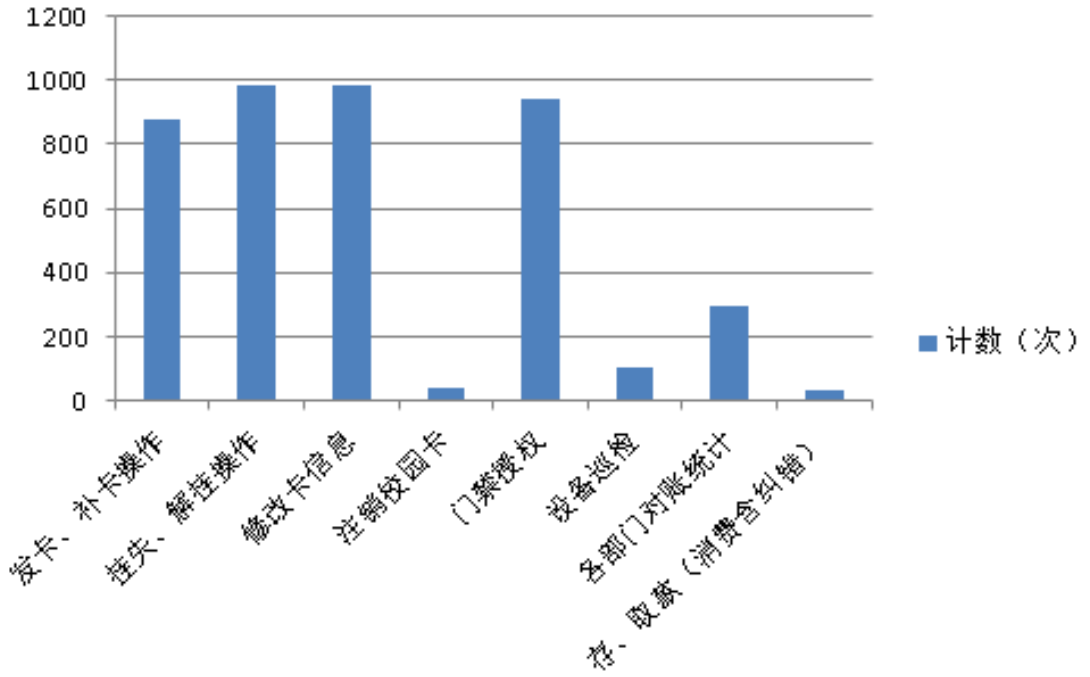


校园邮件系统邮件发送数据统计

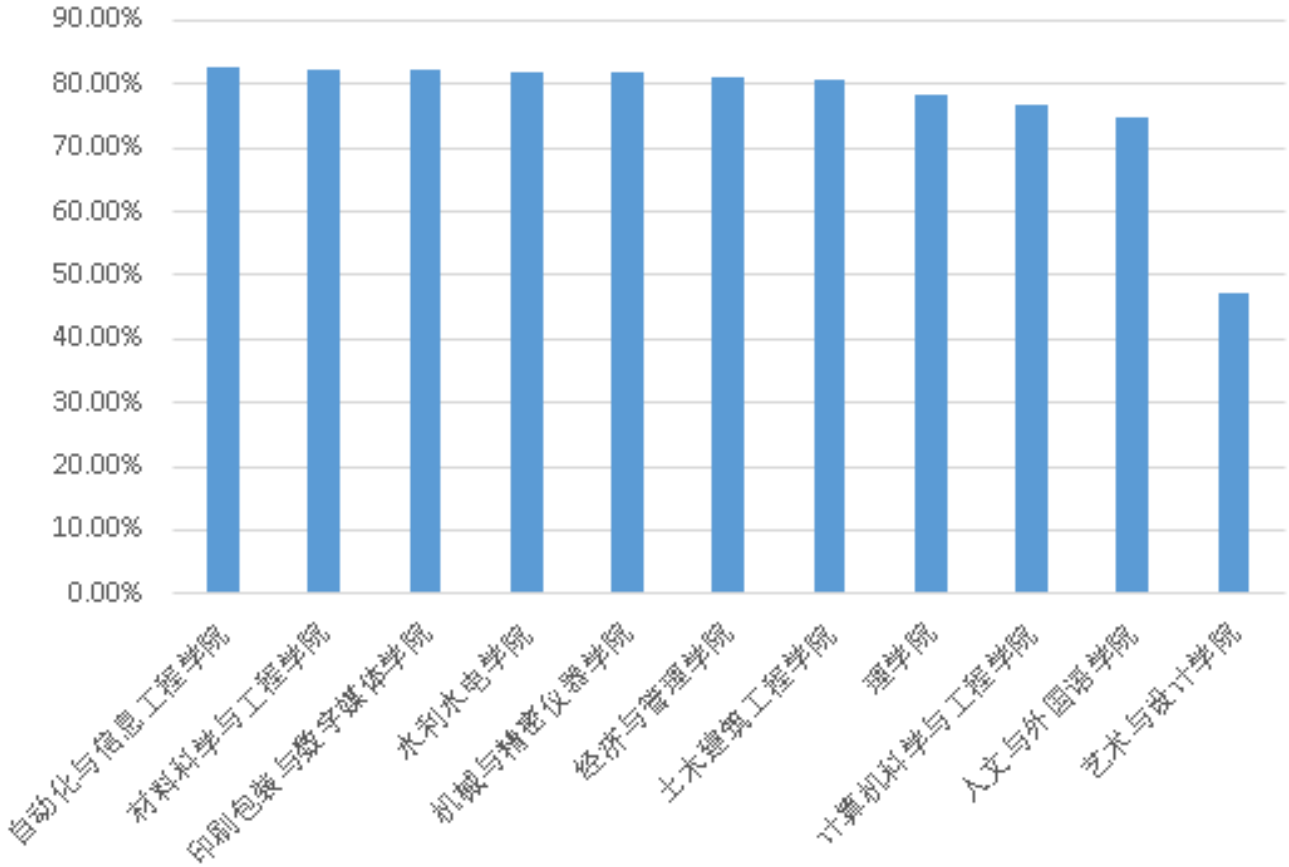


校园卡务中心月度数据统计报告

校园卡务中心工作数据统计

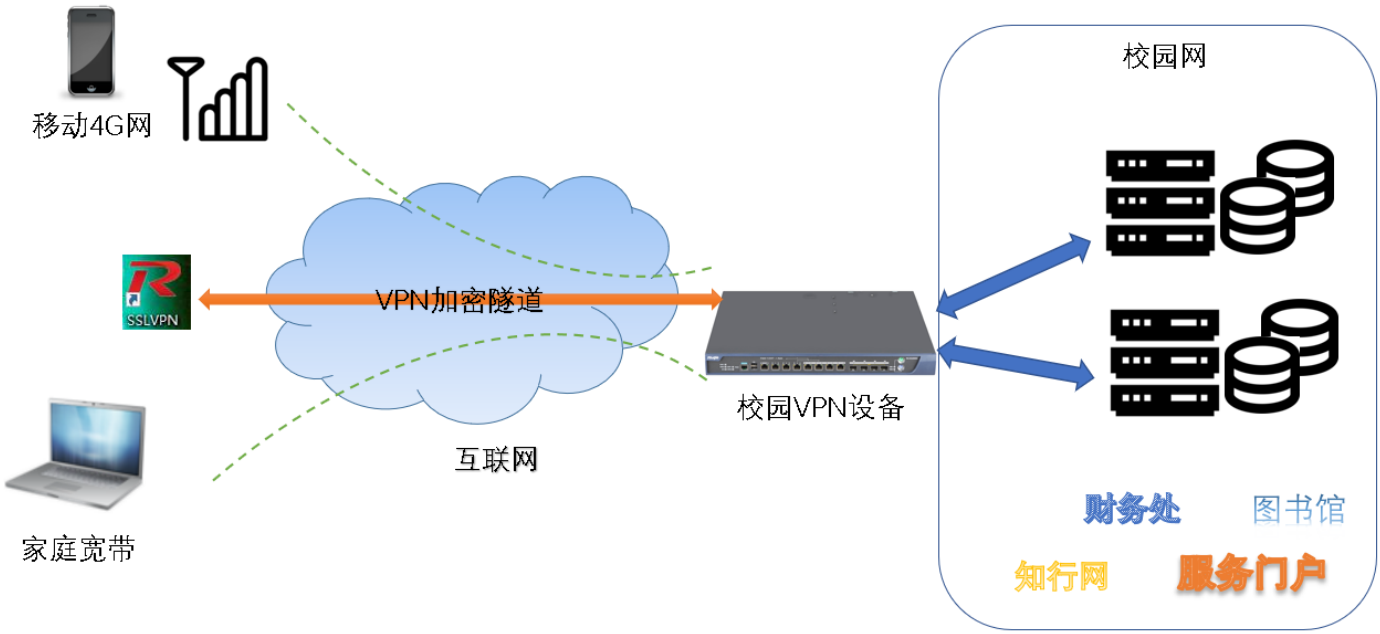


各学院总出勤率统计柱状图



解读校园网VPN

虚拟专用网络(VPN)的功能是：在公用网络上建立专用网络，进行加密通讯。在企业网络中有广泛应用。VPN网关通过对数据包的加密和数据包目标地址的转换实现远程访问。VPN有多种分类方式，主要是按协议进行分类。VPN可通过服务器、硬件、软件等多种方式实现。



我校主要提供两种VPN登录方式，网页版VPN及PC客户端版VPN，在外师生可以通过登录VPN，安全的访问校园内网资源，任何可以接入互联网的地区都可以登录VPN正常的学习办公。

温馨提示：

VPN隧道对接入网络质量有一定要求，建议优先使用有线网络登录VPN。并且，因部分终端浏览器存在兼容性问题，推荐使用PC客户端登陆VPN。

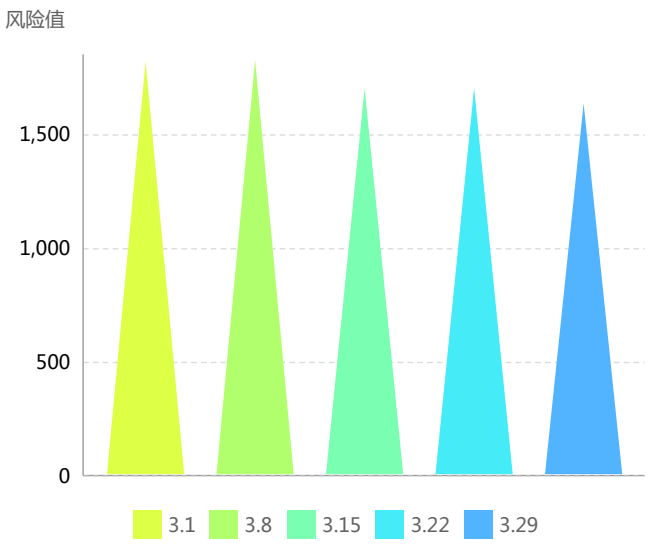
校园网络安全趋势

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3月1日-31日。

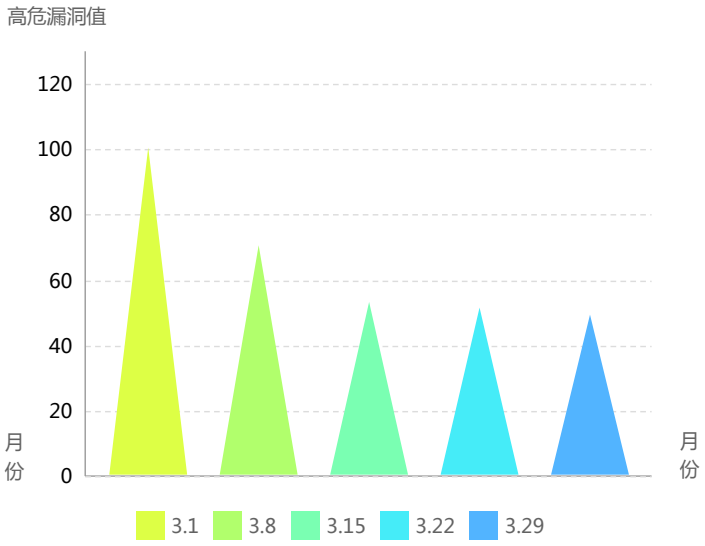
通过常态化安全监测等一系列行动治理，我校本月网络安全状况整体评价为良，风险情况总体良好。

2019年3月网络安全态势分布图

风险值趋势



高危漏洞趋势



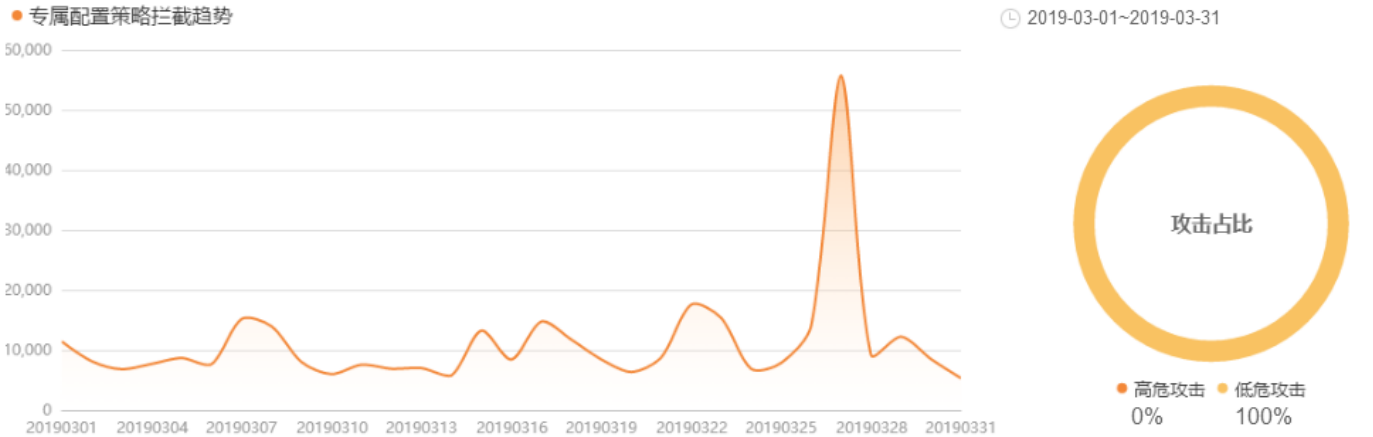
重要信息系统（网站）基本情况

总请求数	总流量	搜索引擎	Alexa 全球排名
41355285次	2677.22GB	404,926次	103485

校园网络安全趋势

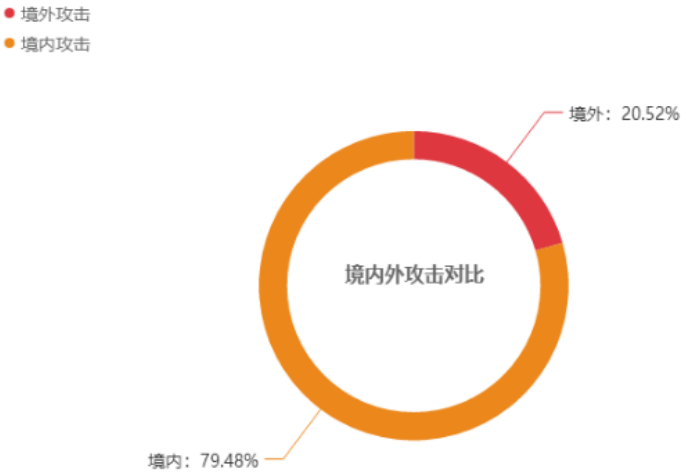
本攻击拦截态势和网络攻击态势分布图以网络信息管理中心监测的数据作为主要依据，对我校重要信息系统（网站）面临的各类安全威胁及基本情况进行总体态势分析，评估范围为2019年3月1日-31日。

2019年3月1日-3月31日攻击拦截态势和网络攻击态势分布



2019年3月1日-3月31日攻击拦截态势和网络攻击态势分布

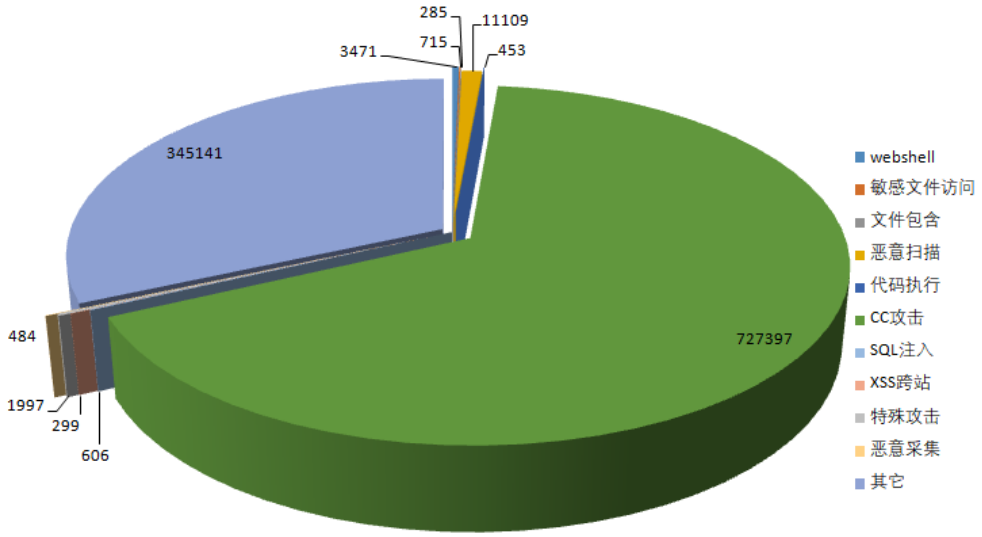
境外攻击概览　通过境内外攻击对比及境外攻击top数据了解境外攻击概况。　2019-03-01~2019-03-31



境外攻击分布来源Top10

国家名称	攻击次数
美国	21419
南非	4590
柬埔寨	3225
菲律宾	612
罗马尼亚	538
法国	341
韩国	275
瑞典	208
日本	179
老挝	137

2019年3月1日-3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1,091,957次, 黑客攻击占总请求数的比率为2.69%， 其中敏感文件访问715次、Webshell攻击3,471次、文件包含攻击285次、恶意扫描11,109次、代码执行453次、CC攻击727,397次、SQL注入606次、XSS跨站攻击299次、特殊攻击1,997次、恶意信息采集484次， 其它类型攻击354,141次。

KBuster：以伪造韩国银行APP的韩国黑产活动披露

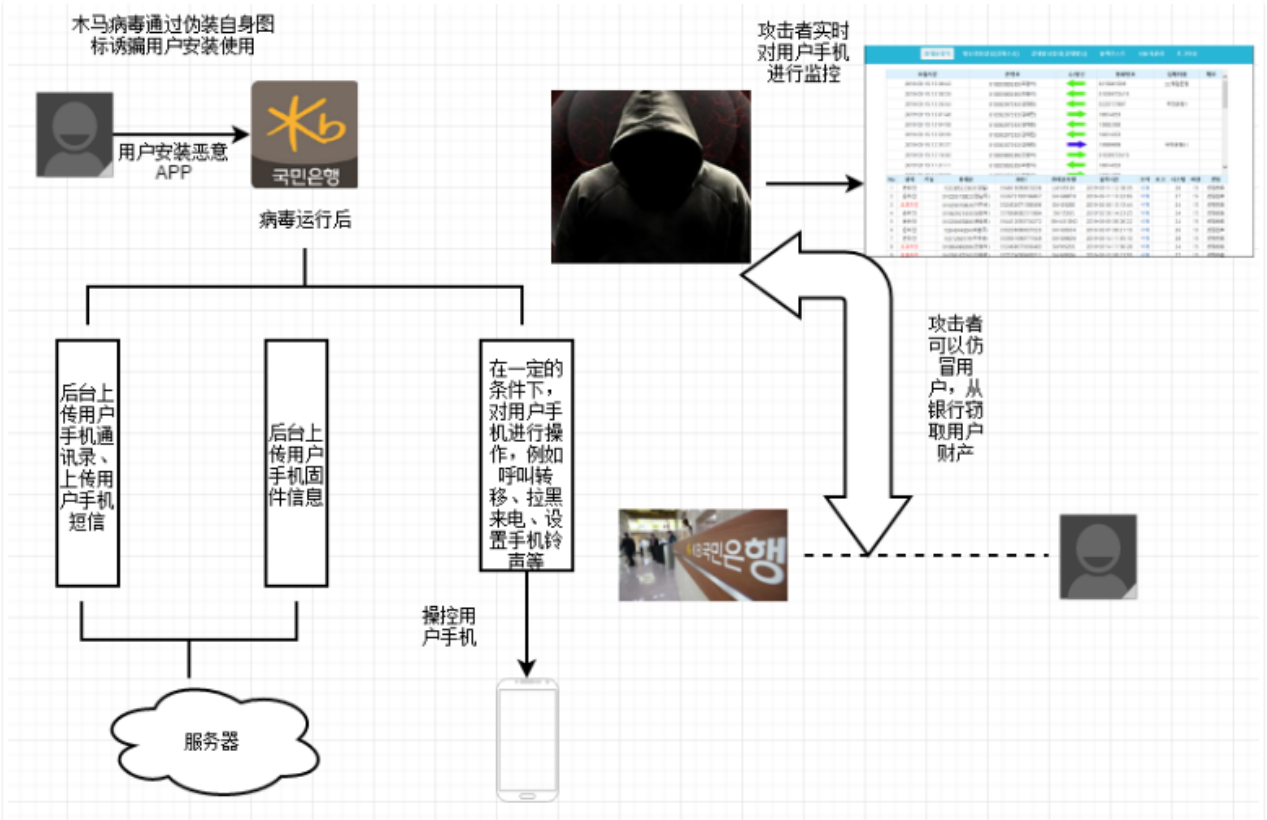
(360威胁情报中心)

针对韩国手机银行用户的黑产活动，其最早活动可能从2018年12月22日起持续至今。结合木马程序和控制后台均为韩语显示，认为其是由韩国的黑产团伙实施。

攻击平台主要为Android，攻击目标为韩国银行APP使用者，攻击手段为通过仿冒韩国银行APP，窃取用户个人信息，并远程控制用户手机，以便跳过用户直接与银行连线验证，从而窃取用户个人财产。

受害银行

样本执行流程（国民银行为例）



样本执行流程

该木马运行以后会弹出仿冒为“国民银行”的钓鱼页面，并诱骗用户填写个人信息；

而此时，木马会在后台获取用户通讯录、短信内容并上传至固定服务器，并会在服务器对用户手机进行监控，每隔5秒对用户手机当前状态进行刷新，从而达到实时监控；除此之外，该木马会对用户手机进行远控操作，并可对韩国相关银行等金融行业的369个电话号码进行呼叫转移操作从而绕过银行双因素认证，还可以监听手机通话、修改来电铃声、私自挂断用户来电并拉黑来电号码等操作。

1 多款Apple产品WebKit内存错误引用漏洞（CNVD-2019-08714）

多款Apple产品中的WebKit组件存在内存错误引用漏洞。攻击者可借助恶意制作的Web内容利用该漏洞执行任意代码。影响产品：Apple Apple iOS <12.2；Apple tvOS <12.2；Apple Safari <12.1；Apple iTunes for Windows <12.9.4；Apple AirDrop <7.11

解决方案：
厂商已发布升级补丁以修复漏洞，补丁获取链接：https://support.apple.com/zh-cn/HT209599

2 Google Android Kernel组件权限提升漏洞（CNVD-2019-07371）

Google Android Kernel组件Binder driver存在权限提升漏洞。攻击者可利用该漏洞获取权限。
影响产品：Android Android 0

解决方案：
厂商已发布漏洞修复程序，请及时关注更新：https://source.android.com/security/bulletin/2019-02-01

3 Mozilla Firefox中间人攻击漏洞（CNVD-2019-08537）

Mozilla Firefox 66之前版本中存在安全漏洞，该漏洞源于程序未能正确地对同源导航执行Upgrade-Insecure-Requests。攻击者可利用该漏洞实施中间人攻击。

解决方案：
厂商已发布了漏洞修复程序，请及时关注更新：https://www.mozilla.org/en-US/security/advisories/mfsa2019-07/

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 李蒙
李宏伟 张晋 王力
安洋
校　对：赵阳 殷仕刚
审　核：张晓宇

扫码关注

西安理工大学微信企业号