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

1 ~ 2 月

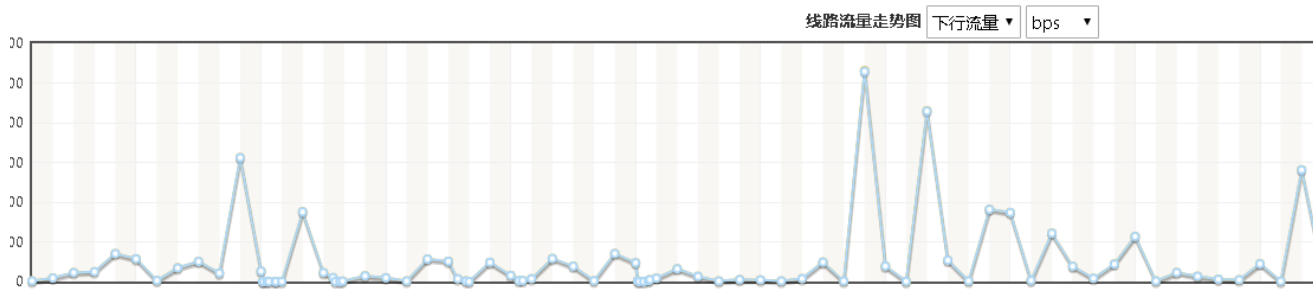
2020

校园网用户统计

2019年1月至2019年2月校园网在线用户分析

1~2月，校园网整体运行正常，日均在线用户4900人，其中无线用户日均在线1200人。

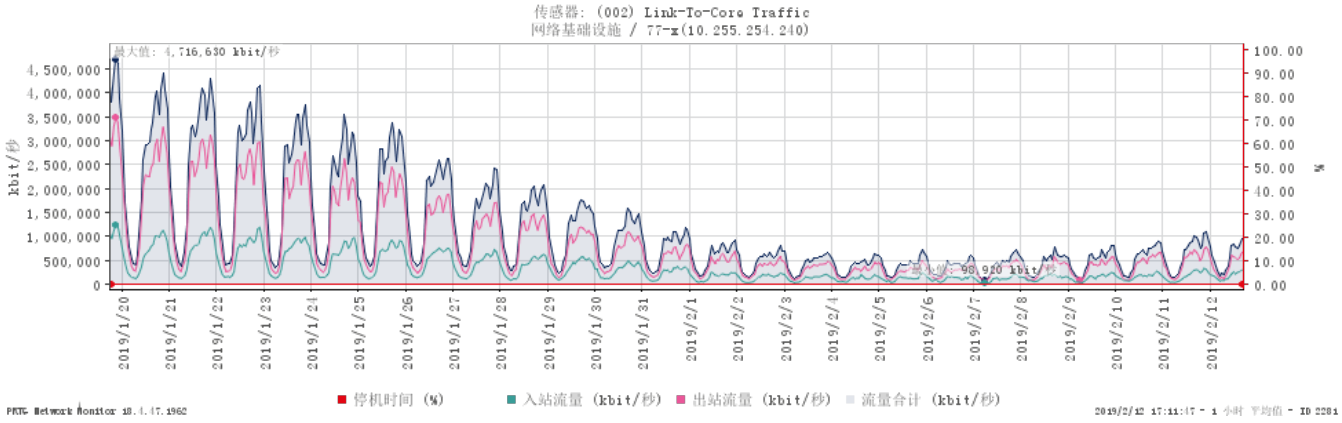
寒假期间校外VPN用户分析



整机下行总流量为17.26GB，上行总流量为56.09GB，峰值3.3Mbps，在线用户峰值最高达154个 ，累计有83540个用户使用过网络，本月最大并发会话数300 。

校园网流量分析

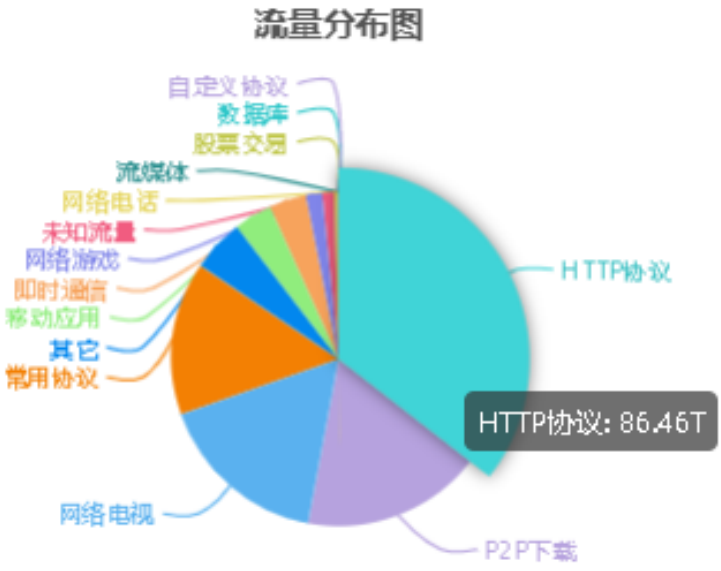
校园网出口流量趋势



校园网出口峰值使用带宽近5G，2019年1月-2月，校园网总下载流量达210T，上传流量共计70T。

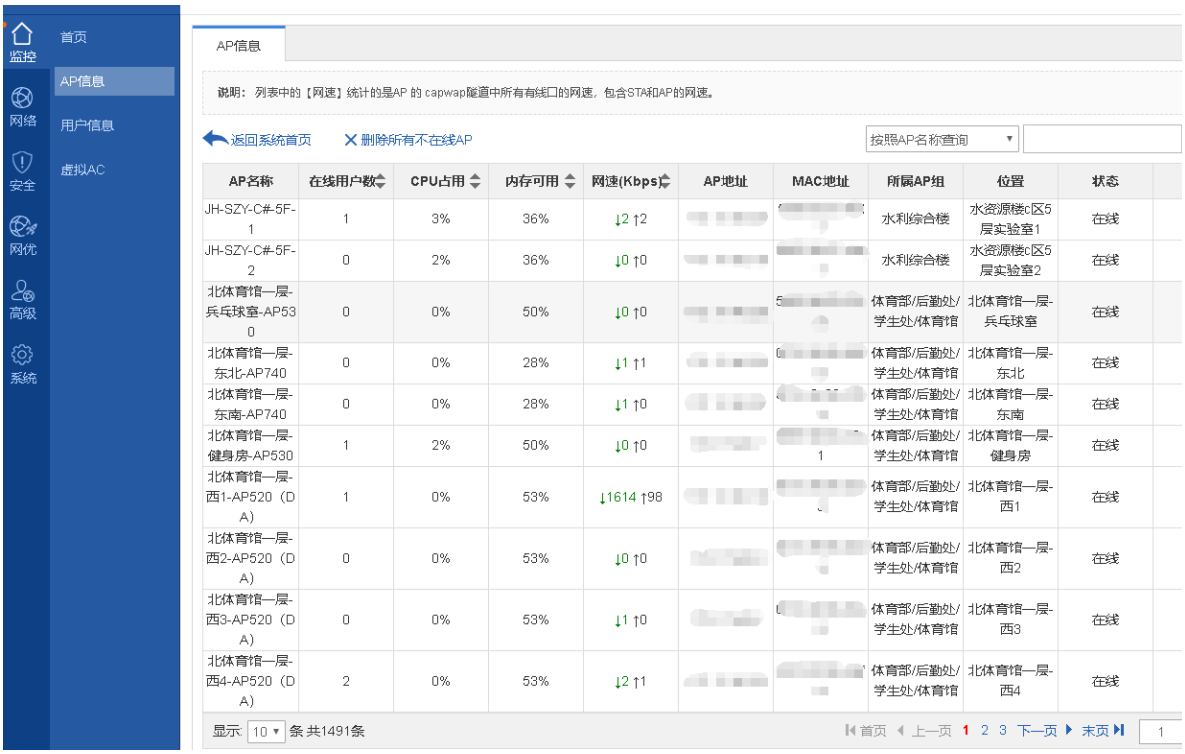
其中，HTTP日常访问产生流量占比37%位居首位，迅雷等P2P下载流量及网络电视流量分别占比约1 5%和16%。

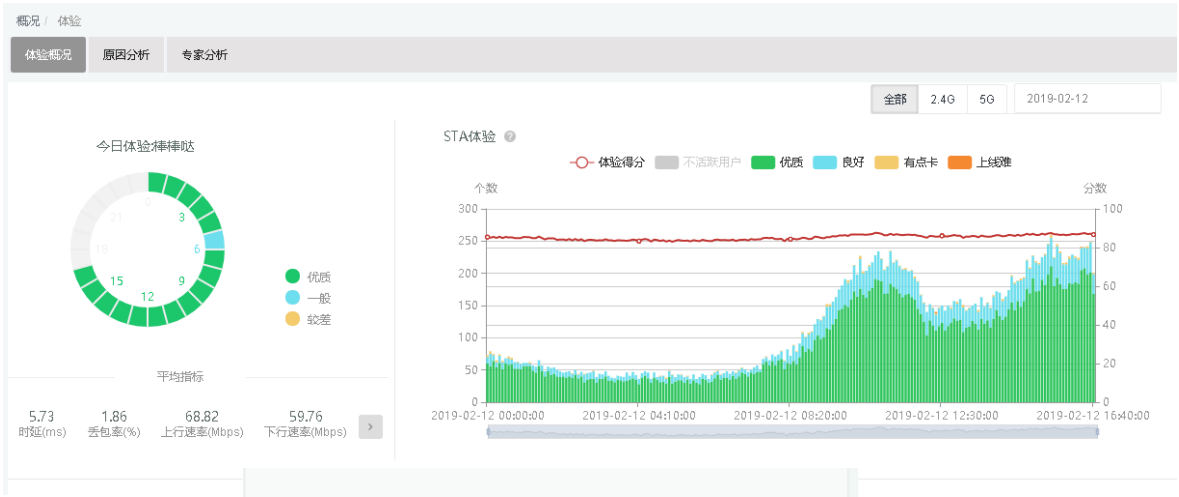
校园网出口流量分布

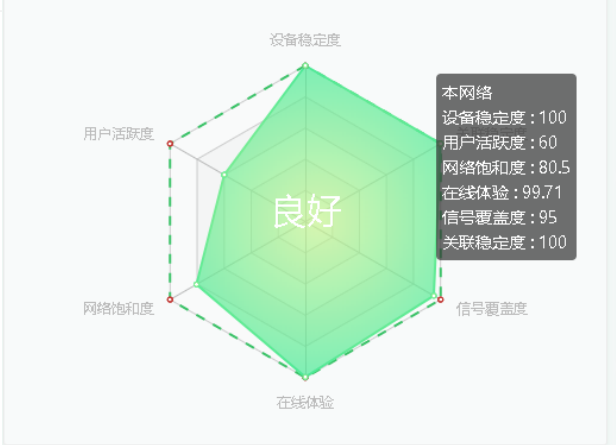


校园网升级与优化

寒假期间，对我校1491台无线网设备进行了软件升级，进一步增强网络稳定性，并根据具体区域进行无线网优化，提升师生用户体验。

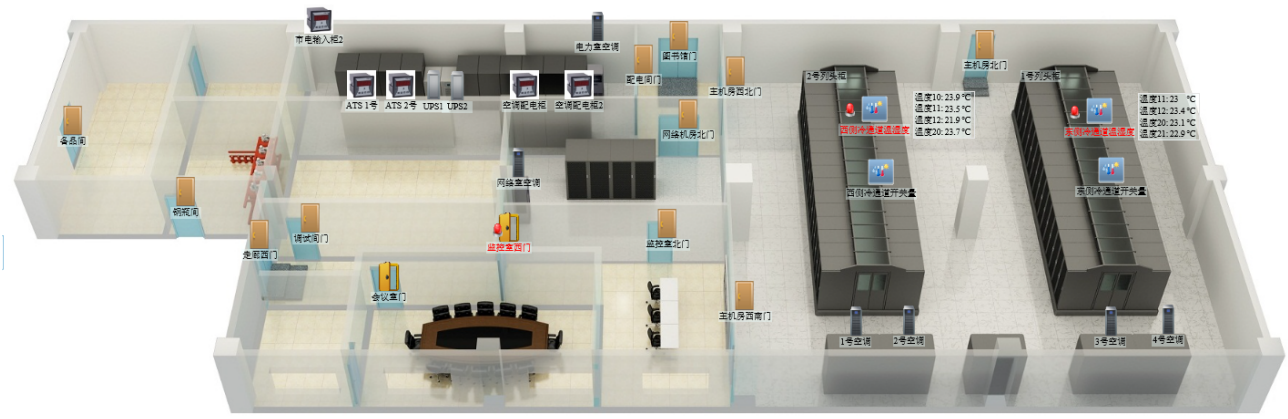






监控与安全巡检

寒假期间，对我校金花、曲江两校区数据中心机房、网络汇聚机房进行安全巡检11次，发现安全隐患 0 处，机房基础设施故障率 0 ，保障我校网络稳定及数据安全。

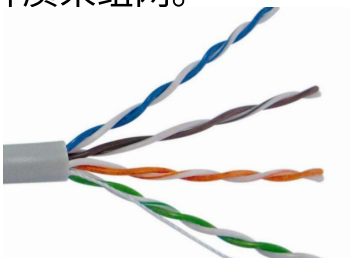


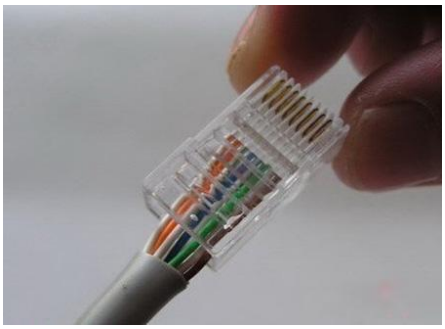
冷通道温度

站点	设备	信号	值
西安理工大学机房	东侧冷通道温湿度	温度10	22.9
西安理工大学机房	东侧冷通道温湿度	温度11	23.0
西安理工大学机房	东侧冷通道温湿度	温度12	23.4
西安理工大学机房	东侧冷通道温湿度	温度20	23.3
西安理工大学机房	东侧冷通道温湿度	温度21	22.9
西安理工大学机房	东侧冷通道温湿度	温度23	22.5
西安理工大学机房	东侧冷通道温湿度	网络通信	正常

校园网常用网线解读

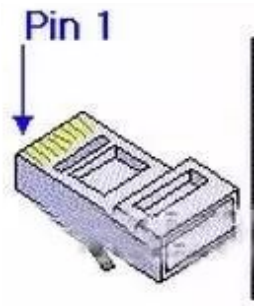
双绞线（俗称的“网线”）可按其是否外加金属网丝套的屏蔽层而区分为屏蔽双绞线（STP）和非屏蔽双绞线（UTP）。从性价比和可维护性出发，大多数局域网使用非屏蔽双绞线（UTP-Unshielded Twisted pair） 作为布线的传输介质来组网。

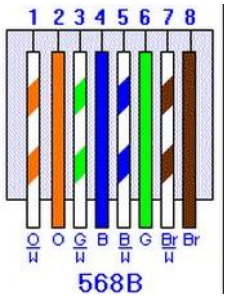




UTP网线由一定长度的双绞线和RJ45水晶头组成。双绞线单根的长度不应超过100M。

双绞线由8根不同颜色的线分成4对绞合在一起，成对扭绞的作用是为了尽可能减少电磁辐射与外部电磁干扰的影响。在EIA/TIA－568标准中，将双绞线按电气特性区分为：五类、六类线等。我校网络中最常用的是超五类线和六类线。





为了保持最佳的兼容性，线缆两端普遍采用EIA/TIA 568 B 标准来制作网线

事实上10M、100M以太网的网线只使用 1、2、3、6编号的芯线传递数据，即1、2用于发送，3、6用于接收，按颜色来说：橙白、橙两条用于发送；绿白、绿两条用于接收；4、5，7、8是双向线。

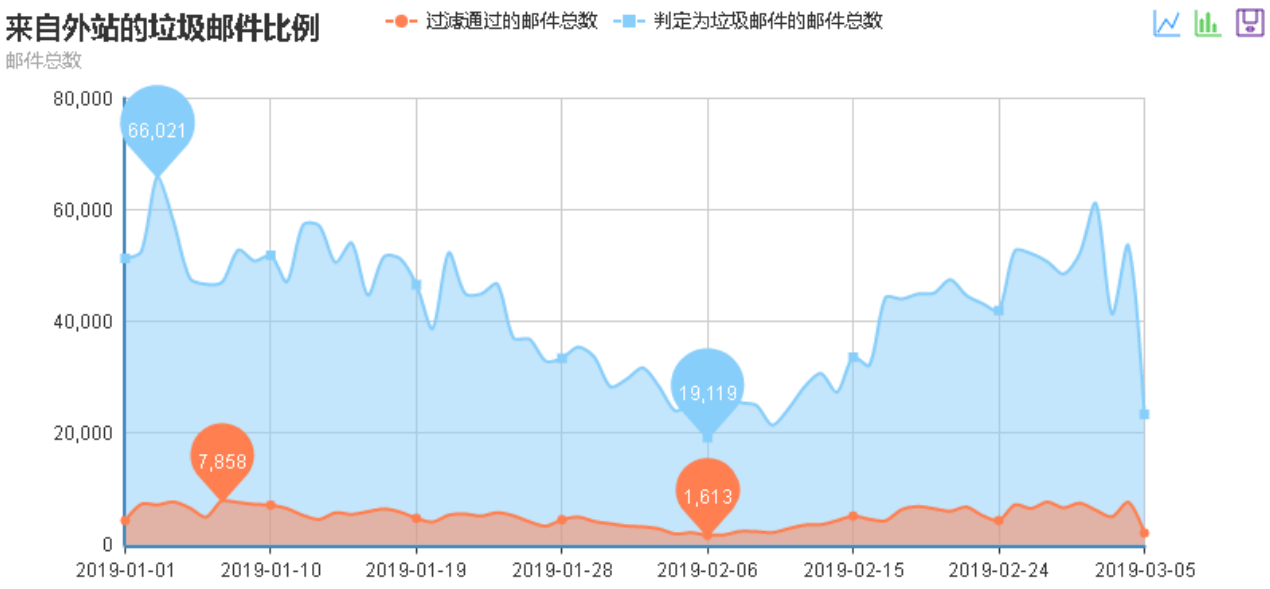
1000M网卡需要使用四对线，即8根芯线全部用于传递数据。

我校部分办公室使用网线作为电话线，导致网络带宽下降，电流干扰严重，大大降低了网络传输质量。个别用户使用了错误的线序制作水晶头，出现无法正常上网，或因干扰严重频繁出现网络错误报文，严重影响网络使用。建议广大师生避免类似情况出现，以保障稳定的网络办公环境。

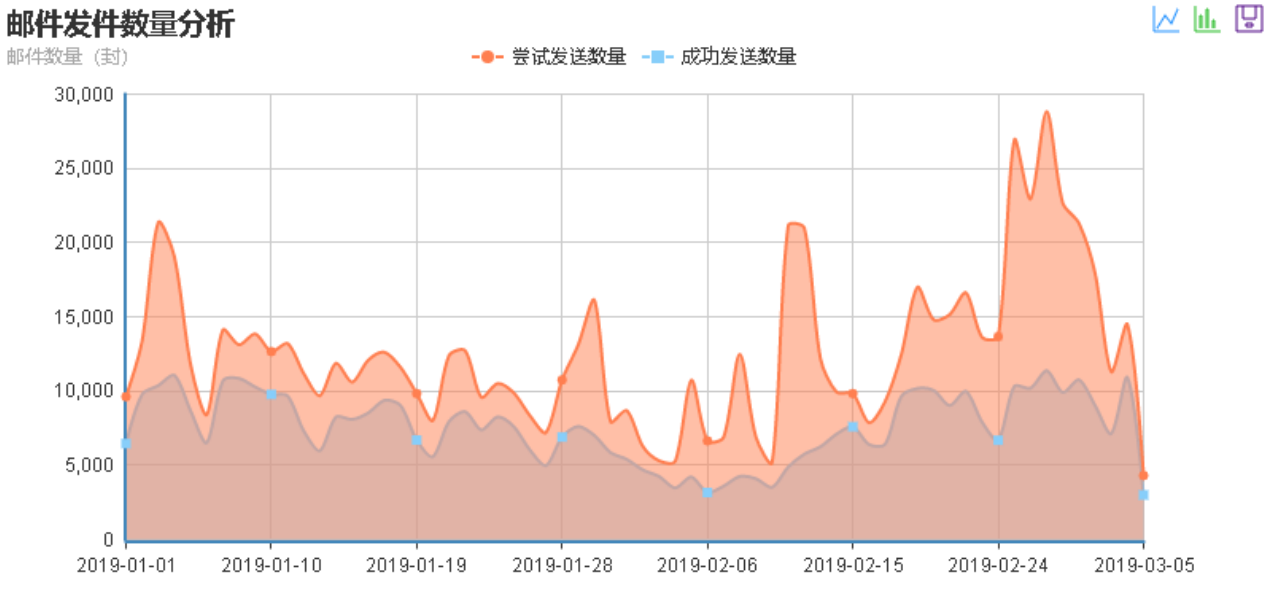
校园邮件系统运行数据

2019年1月~2月，我校邮件系统运行稳定，未出现服务终端故障，垃圾邮件拦截网关工作正常，日均拦截垃圾邮件近4.2万封，日均发送邮件8300封。

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



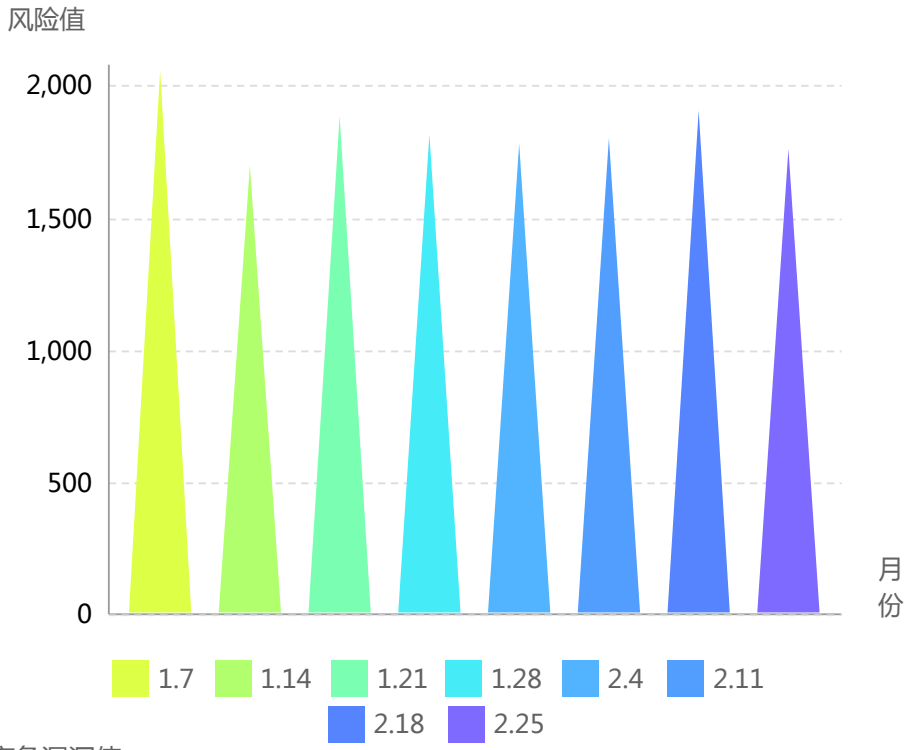
校园网络安全趋势

本周期统计以网络中心监测的数据作为主要依据，对我校195个信息系统（网站）面临的各类安全威胁进行总体态势分析。

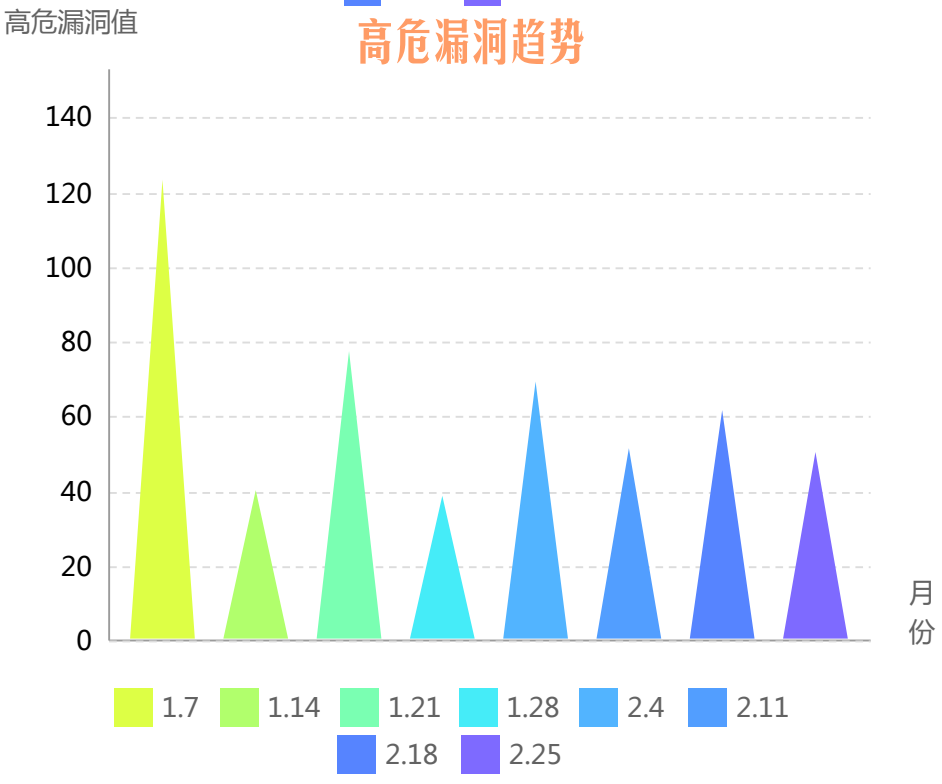
评估范围为：2019年1月1日-2月28日；通过常态化安全监测等一系列行动治理，我校本月网络安全状况整体评价为良，风险情况总体良好。

2019年1月-2月网络安全态势分布图

风险值趋势



高危漏洞趋势



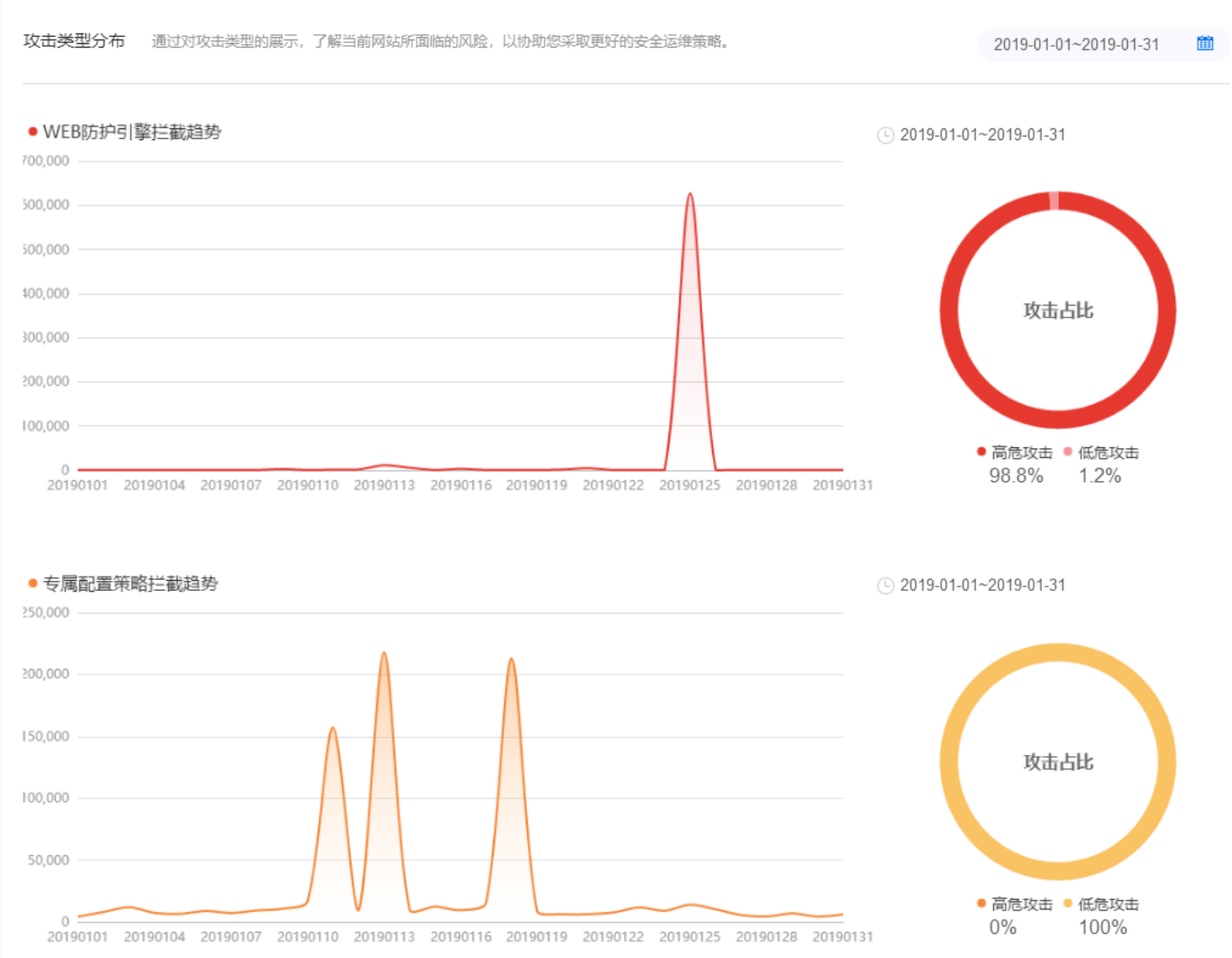
校园网络安全趋势

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1月1日-2月28日。

重要信息系统（网站）基本情况

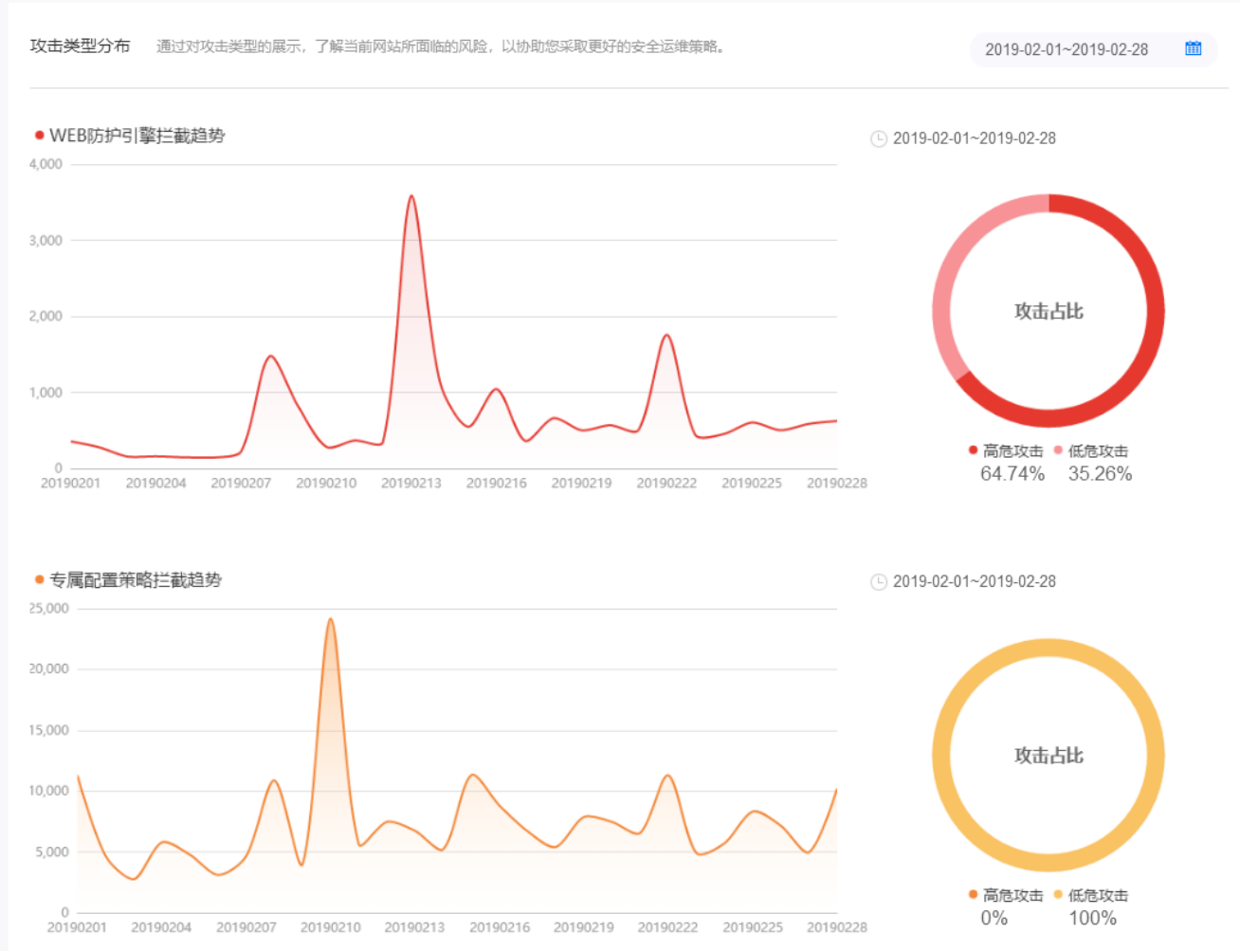
总请求数	总流量	搜索引擎	Alexa 全球排名
37600392次	2590.04GB	535890次	93793

2019年1月1日-1月31日攻击拦截态势和网络攻击态势分布

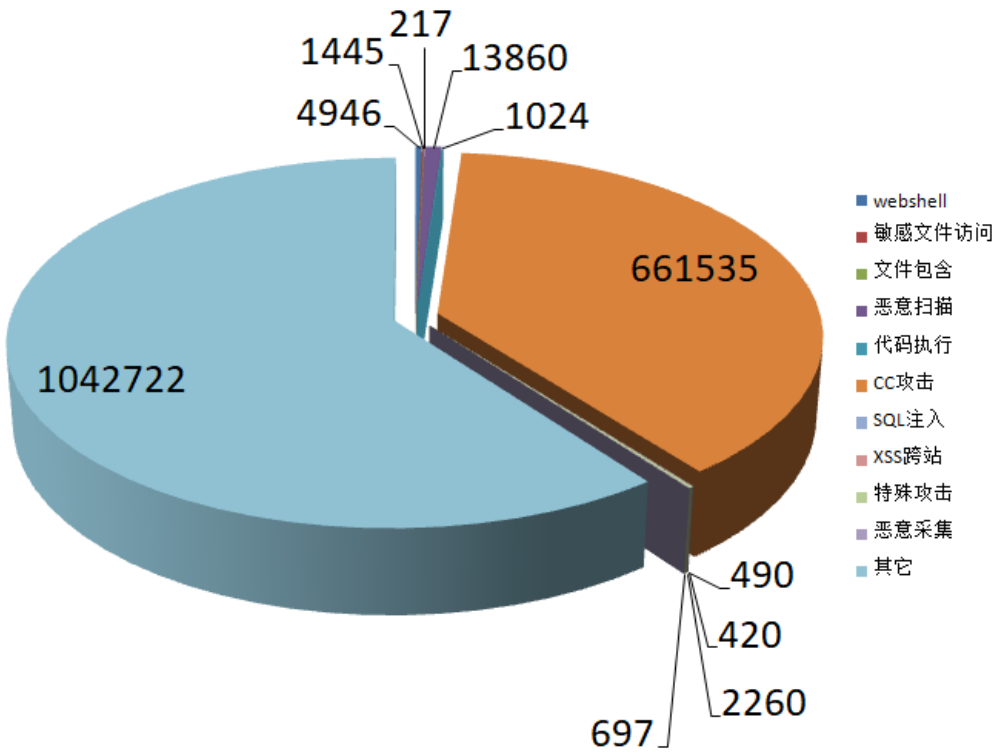


校园网络安全趋势

2019年2月1日-2月28日攻击拦截态势和网络攻击态势分布



2019年1月1日-2月28日网站遭受黑客攻击分布图



本周期内共发生各类安全攻击1729616次，黑客攻击占总请求数的比率为4.6%，其中敏感文件访问1445次、Webshell攻击4946次、文件包含攻击217次、恶意扫描13860次、代码执行1024次、CC攻击663515次、SQL注入490次、XSS跨站攻击420次、特殊攻击2260次、恶意信息采集697次，其它1042722次。

《网络安全法》解读

网络安全为人民，
网络安全靠人民，
维护网络安全环境人人有责

谷安天下出品

制定网络安全法的背景

- 网络安全是国家安全的重要组成部分
- 网络入侵攻击频繁
- 个人信息泄露严重
- 危害国家和社会的信息的泛滥

2.关于保障网络产品和服务安全

目标

维护网络安全，首先要保障网络产品和服务的安全。

解读内容

- 明确网络产品和服务提供者的安全义务(相关条文：第二十二条)；
- 网络关键设备和网络安全专用产品的安全认证和安全检测制度上升为法律并作了必要的规范（相关条文：第二十三条）；
- 建立关键信息基础设施运营者采购网络产品、服务的安全审查制度（相关条文：第三十五条）。

—《网络安全法》7大焦点内容—

1.关于维护网络主权和战略规划

目标

维护网络空间主权和国家安全

解读内容

- 在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理。(相关条文：第二条)；
- 对国家网络安全战略和重要领域网络安全规划、促进网络安全的支持措施作了规定(相关条文：第二章)。

3.关于保障网络运行安全

目标

保障网络安全可靠运行。

解读内容

- 保障网络运行安全，必须落实网络运营者第一责任人的责任。据此，将现行的网络安全等级保护制度上升为法律（相关条文：第二十一条）；
- 保障关键信息基础设施安全，维护国家安全、经济安全和保障民生（相关条文：第三章第二节）。

图片来源
(www.aqniu.com)

《网络安全法》解读

4.关于保障网络数据安全

目标

保护网络数据，维护国家安全、经济安全，保护公民合法权益，促进数据利用。

解读内容

- 要求网络运营者采取数据分类、重要数据备份和加密等措施，防止网络数据被窃取或者篡改（相关条文：第二十一条）；
- 加强对公民个人信息的保护，防止公民个人信息数据被非法获取、泄露或者非法使用（相关条文：第四十一条至第四十四条）；
- 要求关键信息基础设施的运营者在境内存储公民个人信息等重要数据；确需在境外存储或者向境外提供的，应当按照规定进行安全评估（相关条文：第三十七条）。

5.关于保障网络信息安全

目标

加强网络信息保护，规范网络信息传播活动。

解读内容

- 明确网络运营者处置违法信息的义务，规定：网络运营者发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告（相关条文：第四十七条）；
- 发送电子信息、提供应用软件不得含有法律、行政法规禁止发布或者传输的信息（相关条文：第四十八条）；
- 为维护国家安全和侦查犯罪的需要，侦查机关依照法律规定，可以要求网络运营者提供必要的支持与协助（相关条文：第二十八条）；
- 赋予有关主管部门处置违法信息、阻断违法信息传播的权力（相关条文：第四十八条）。

6.关于监测预警与应急处置

目标

加强国家的网络安全监测预警和应急制度建设，提高网络安全保障能力

解读内容

- 要求国务院有关部门建立健全网络安全监测预警和信息通报制度，加强网络安全信息收集、分析和情况通报工作（相关条文：第五十一条、第五十二条）；
- 建立网络安全应急工作机制，制定应急预案（相关条文：第五十三条）；
- 规定预警信息的发布及网络安全事件应急处置措施（相关条文：第五十四条）；
- 为维护国家安全和社会公共秩序，处置重大突发社会安全事件，对网络管制作了规定（相关条文：第五十八条）。

7.关于网络安全监督管理体制

目标

明确网络安全监督与管理主体，落实网络安全管理职责。

解读内容

- 国家网信部门负责统筹协调网络安全工作和相关监督管理工作，并在一些条款中明确规定了其协调和管理职能；
- 国务院工业和信息化、公安等部门按照各自职责负责网络安全保护和监督管理相关工作（相关条文：第八条）。

《网络安全法》解读

根据《网络安全法》二十一条规定，网络运营者应当按照网络安全等级保护制度的要求，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

法律责任

如果出了网络安全事故，后果有三个：

不履行等保制度：责令改正+警告

不改正/危害网络安全：1-10万元罚款

主体负责人：5千元-5万元罚款

根据《网络安全法》二十二条规定，网络产品、服务的提供者不得设置恶意程序，并应当为其产品、服务持续提供安全维护；网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规。

法律责任

如果提供网络产品时违反以上规定，后果有四个：

危害网络安全：5-50万元罚款

主体负责人：1-10万元罚款

非法收集信息：违法所得1-10倍罚款

情节严重者：停业整顿或吊销营业执照

《网络安全法》解读

根据《网络安全法》二十五条规定，网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险;在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

法律责任

没有应急预案的，没有及时处置高危漏洞、网络攻击的;在发生网络安全事件时处置不恰当的，后果有两个：

不改正/危害网络安全:1-10万元罚款

危害网络安全：5千元-5万元罚款

根据《网络安全法》四十七条规定，网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

法律责任

如果置之不管，后果有三个：

不履行义务：责令整改+警告

不改正/情节严重：10-50万元罚款，停业整顿或吊销营业执照

主体负责人：1-10万元罚款

违法案例

1. 四川一网站因高危漏洞遭入侵被罚

事件：宾市翠屏区“教师发展平台”网站因网络安全防护工作落实不到位，导致网站存在高危漏洞，造成网站发生被黑客攻击入侵的网络安全事件。

处罚行为：未落实网络安全等级保护制度，未履行网络安全保护义务

处罚措施：对直接负责的主管人员罚款5千，机构罚款1万元

法律依据：《网络安全法》第21条、第59条

2. 河南一网站被黑因未履行网络安全保护获罚

事件：新乡市封丘县图书馆网站遭到黑客攻击，因未采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施，致使网页被篡改。

处罚行为：未履行网络安全保护义务

处罚措施：对直接负责的主管人员罚款5千，机构罚款1万元，给予负责网络安全工作的直接责任人行政警告处分

法律依据：《网络安全法》第21条、第59条

3. 山西一网站不履行网络安全保护义务被处罚

事件：山西忻州市某省直事业单位网站存在SQL注入漏洞，严重威胁网站信息安全，连续被国家网络与信息安全信息通报中心通报。

处罚行为：未按照网络安全等级保护制度的要求，采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施

处罚措施：警告并责令其改正

法律依据：《网络安全法》第21条、第59条

4. 哈尔滨一网站不维护遭黑客攻击被罚

事件：方正县农业技术推广中心设立的“方正农业社会化服务平台”遭受黑客攻击入侵，在社会上造成恶劣影响。

处罚行为：未按照网络安全等级保护制度的要求落实网络安全主体责任，存在高危安全漏洞并被黑客攻击入侵

处罚措施：对机构罚款2万元

法律依据：《网络安全法》第21条、第59条

重大漏洞预警

1 WinRAR存在系列远程代码执行漏洞

发布时间早于5.70 Beta 1版本的WinRAR软件及使用unacev2.dll动态共享库的解压、文件管理类工具软件存在此漏洞；漏洞攻击者利用该漏洞，通过诱使用户使用WinRAR打开恶意构造的压缩包文件，将恶意代码写入系统启动目录或者写入恶意dll劫持其他软件进行执行，实现对用户主机的任意代码执行攻击。

解决方案:

1、使用WinRAR软件的用户：WinRAR厂商已发布新版本修复此漏洞，CNVD建议立即升级至最新版本：https://www.win-rar.com/download.html。

2、其他解压、文件管理类软件是否受影响的判断方法：用户可通过检查软件安装目录下是否存在unacev2.dll文件进行判断。

2 Windows Sever容易受到DoS攻击

所有运行IIS（互联网信息服务）的Windows Server 2016、Windows Server Version 170、WindowsServer Version 1803以及Windows 10 (1607、1703、1709和1803版本)都会受遭遇该DoS攻击

解决方案:

目前尚未有针对该漏洞的缓解措施或变通措施。建议用户参考二月份的非安全更新建议，及时更新以确保安全。

3 多款Apple产品WebKit类型混淆漏洞（CNVD-2019-03314）

多款Apple（Apple IOS <12.1.3，Apple tvOS <12.1.2，Apple iCloud for Windows <7.10）产品中的WebKit组件存在类型混淆漏洞。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。

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://support.apple.com/zh-cn/HT209451

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

扫码关注

西安理工大学微信企业号