西安理工大学
XI'AN UNIVERSITY OF TECHNOLOGY

# 网络信息管理中心

# 校园网运行与安全简报

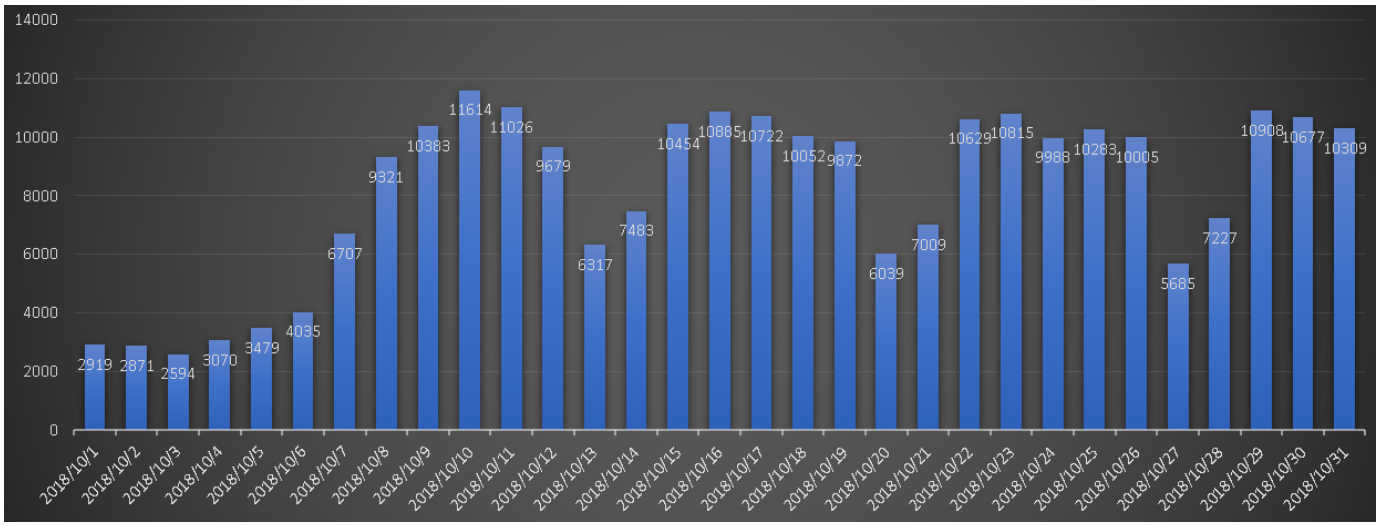
10月

2018

# 校园网用户统计、流量分布

10月，校园网整体运行正常，日均在线用户8160人，其中无线用户日均在线6000人。

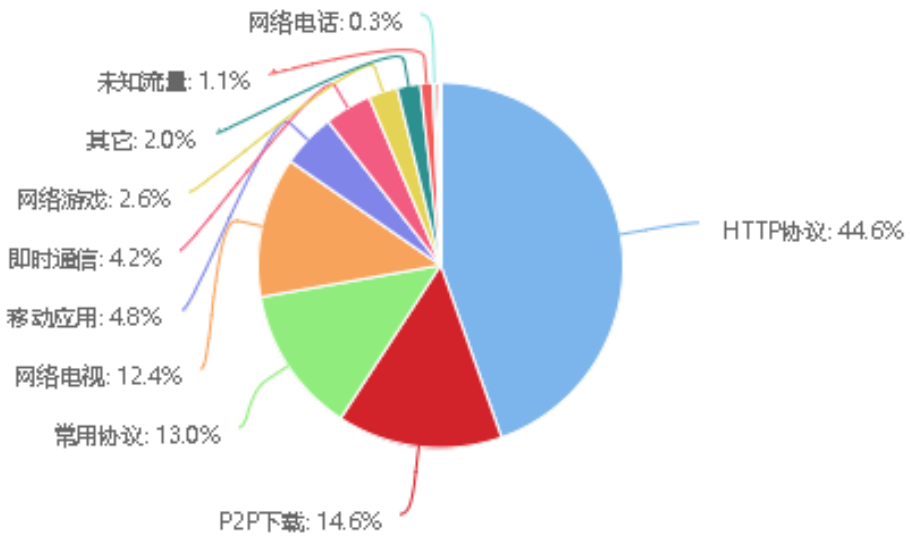
2018年10月1日至2018年10月30日校园网在线用户分析




校园网出口峰值使用带宽11G，2018年10月1日-2018年10月31日，校园网总下载流量达320T，上传流量共计210T。

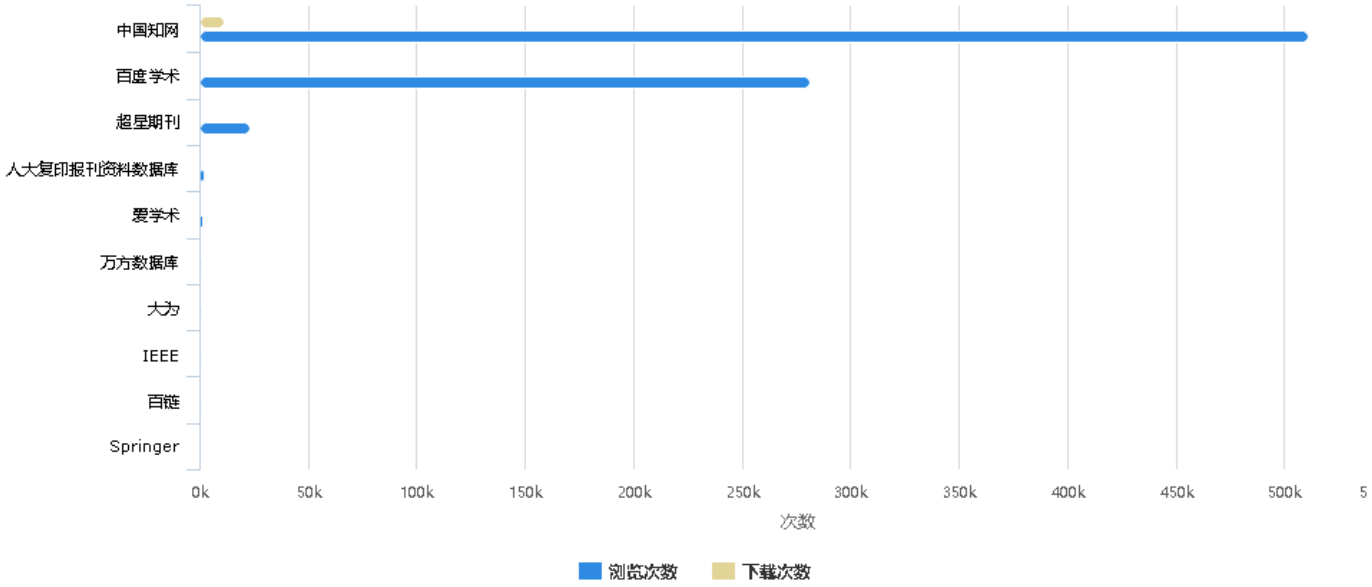
其中，浏览器日常访问产生流量占比44.6%位居首位，迅雷等P2P下载流量及web常规应用流量分别占比约14.6%和13%。

**流量分布**

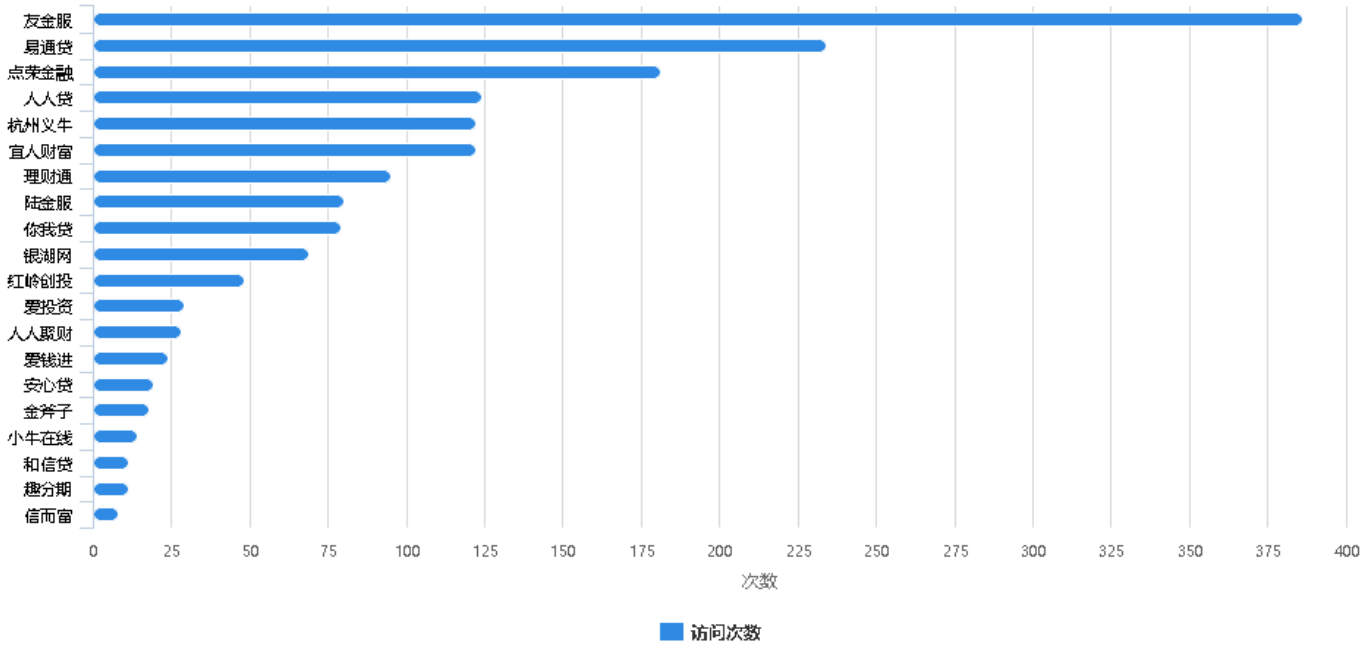


# 校园网大数据

## 图书资源访问情况




## 金融APP访问情况



# 关于校园网路由器、交换机的使用说明

## 交换机与路由器的区别

| 分类 | 交换机 | 路由器 |
| --- | --- | --- |
| 代理功能 | 有 | 无 |
| 端口 | 所有端口功能相同 使用无需区分， 端口一般有4口、8口、16口、24口 | 有WAN口与LAN区分，一般只有4个端口或更少 |
| 管理 | 使用无需配置 ，大部分无法管理 | 有后台管理系统，使用时需配置 |
| IPv6 | 自动转发 | 部分不支持 |

## 我校网设备配置方案

我校校园网实行统一DHCP地址分配IP的方式，用户终端网卡需配置为IP自动获取的方式，获取学校统一分发的IP地址方可认证上网。

交换机用户无需任何配置，将主线与用户线同时接在交换机上的任意端口即可。

路由器（包括有线路由器和无线路由器）的用户需要关闭内置DHCP功能，且将主线与用户线全部接在路由器LAN端口，以保证下挂终端可以正确的获取学校分发IP地址，正常认证上网。

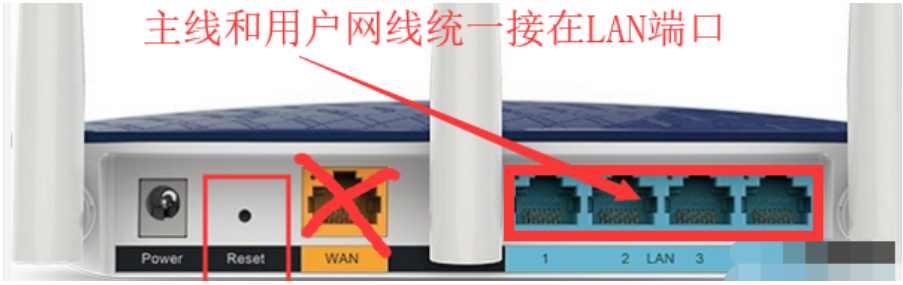
# 路由器具体配置说明

## 1.关闭路由器DHCP功能

将电脑用网线接在路由器后方LAN端口，在电脑浏览器URL地址栏中输入路由器的管理地址，一般在路由器机身背面标牌处有提示，多为192.168.0.1或192.168.1.1。


在路由器后台管理系统中寻找“DHCP”相关选项，选择不启用或关闭，然后点击保存，最后在系统功能中手动重启路由器，即可完成配置。

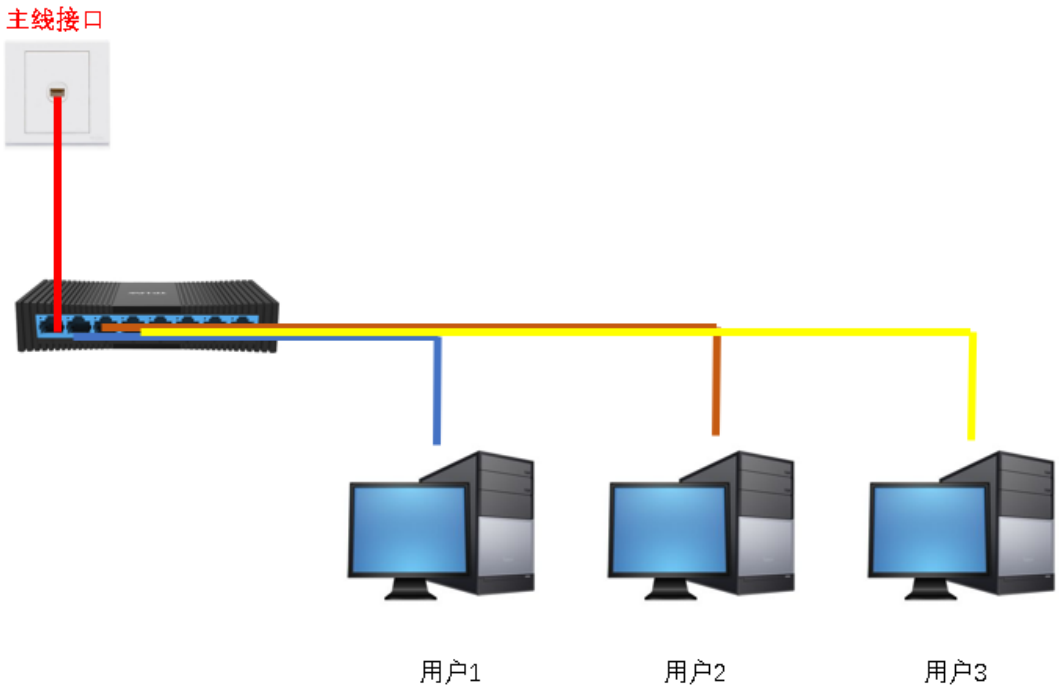

## 2.将主线和用户线统一接在LAN端口




完成配置后，用户通过无线或者有线网连接路由器，都可以正常获取IP认证上网。

# 推荐设备及使用建议

目前我校部分楼宇办公室因接入人数众多，室内网络设备众多，经常出现主线无法识别、内网环路、arp病毒攻击等问题。
建议校内各单位根据各办公室、教研室具体师生数量合理规划网络设备采购方案，且采用清晰简洁的内部网络线路结构。



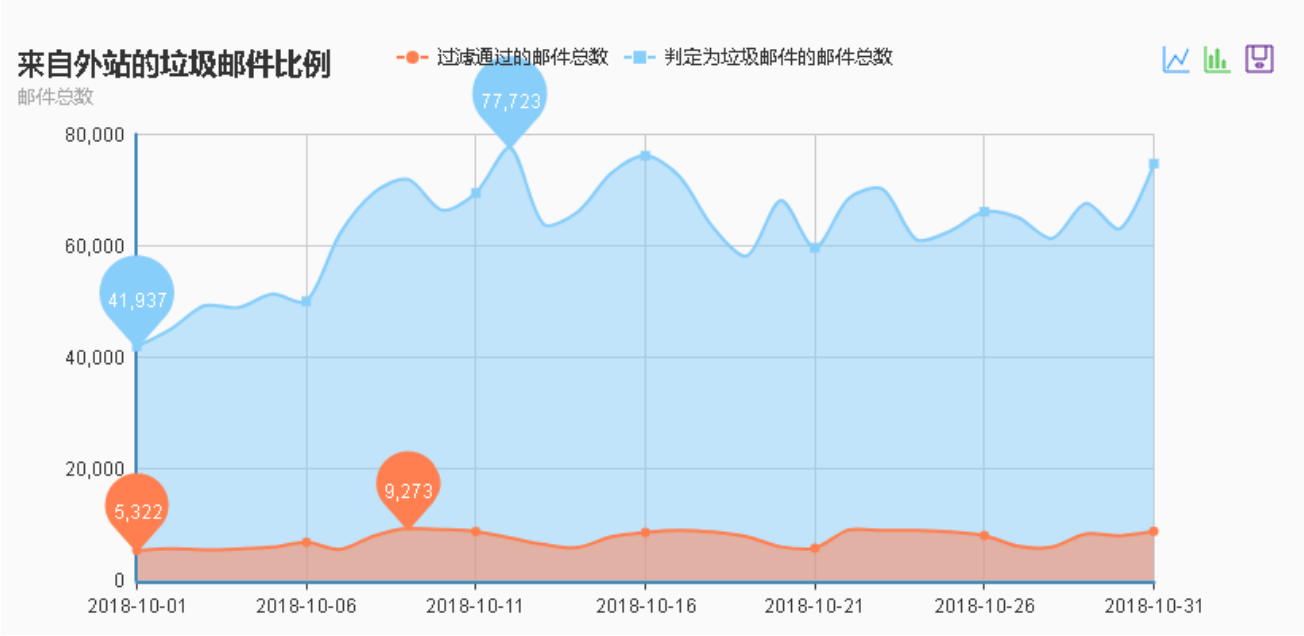

一般8人以下建议采购千兆8口交换机，24人以下建议采购24口全千兆交换机，24人以上的建议采用两台24口全千兆交换机

建议在内部网络布线初期将主线及用户网线两段按序号做好标注，以便日常维护。

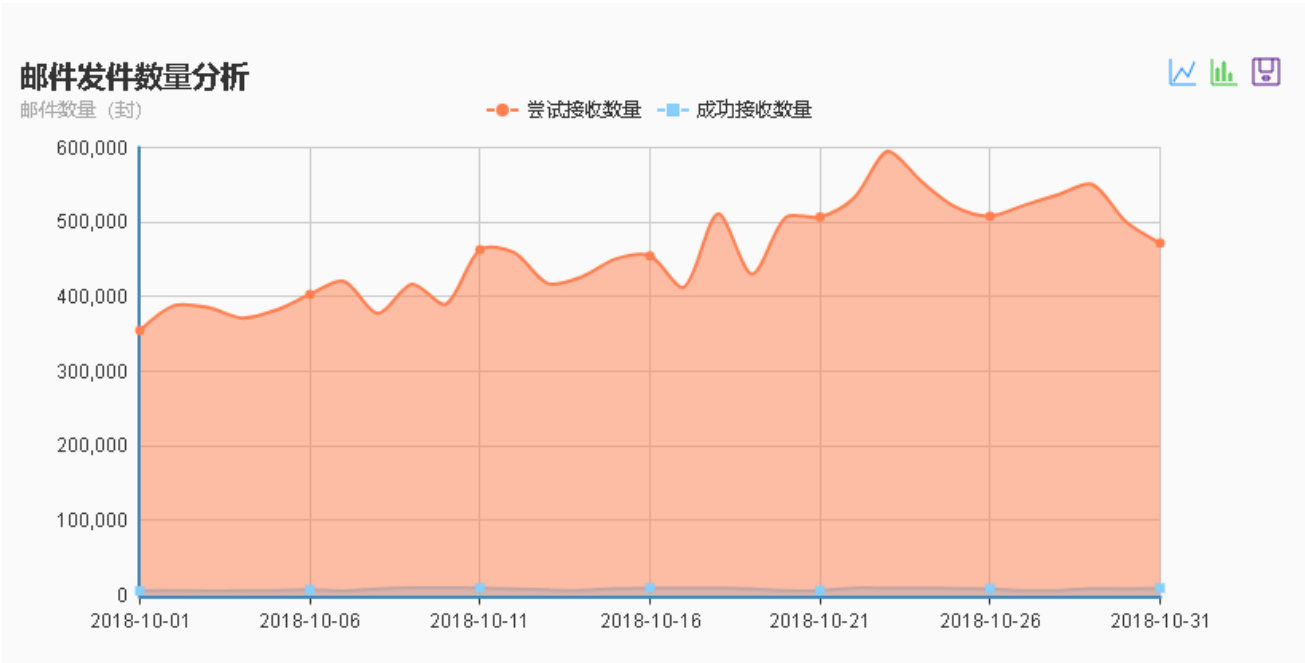
# 校园邮件系统运行数据

2018年10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6.2万封。

### 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



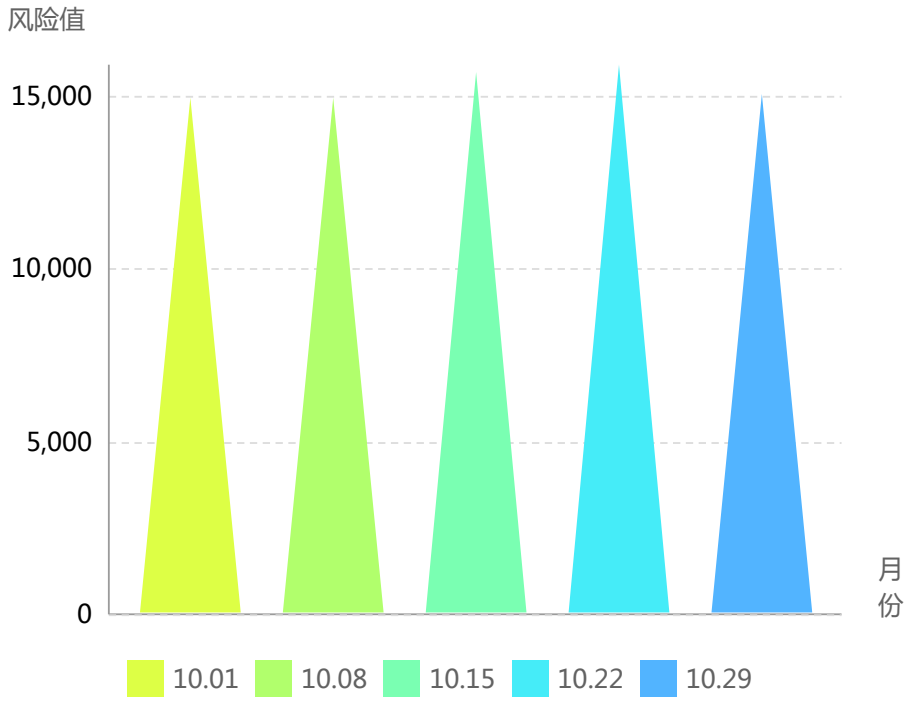
# 校园网络安全趋势

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。

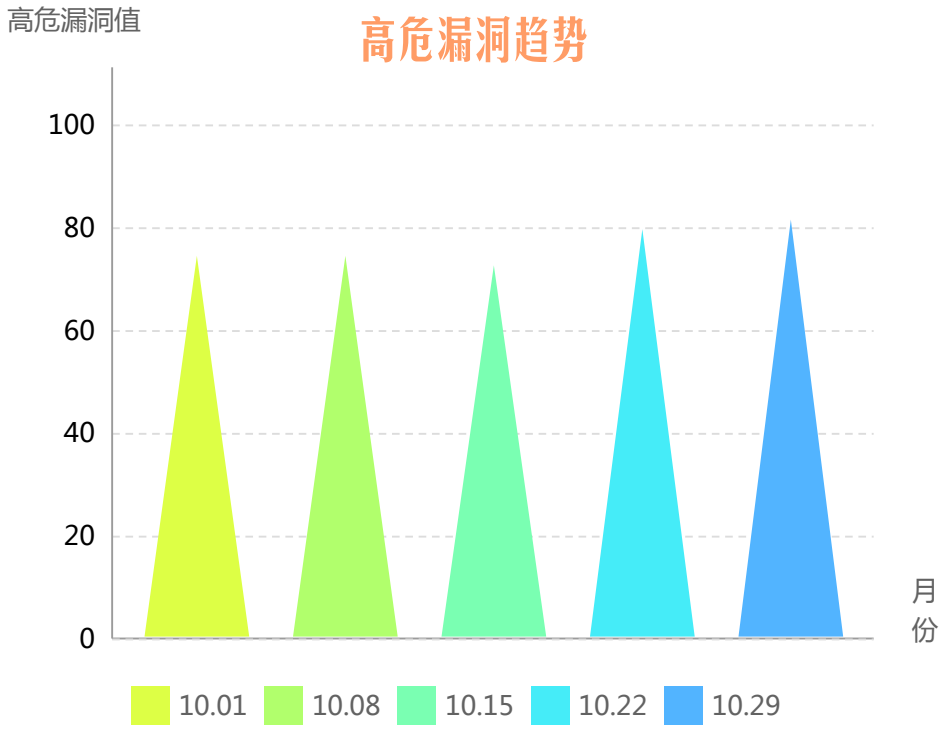
评估范围为：2018年10月1日-10月31日；自开学以来网络中心通过常态化安全监测等一系列行动治理，我校网络安全状况整体评价为良。

## 2018年10月1日-10月31日网络安全态势分布图

### 风险值趋势




### 高危漏洞趋势



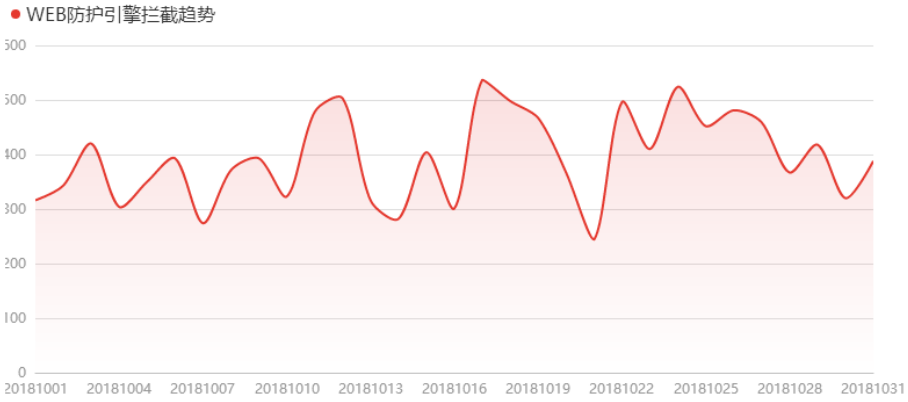
# 校园网络安全趋势

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：2018年10月1日-10月31日。

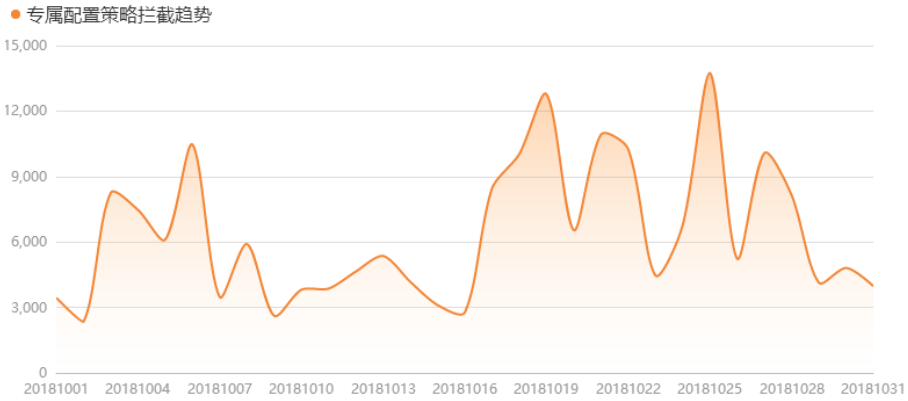
## 重要信息系统（网站）基本情况

| 总请求数 | 总流量 | 搜索引擎 | Alexa 全球排名 |
|---|---|---|---|
| 18459168次 | 1862.45GB | 264892次 | 93863 |

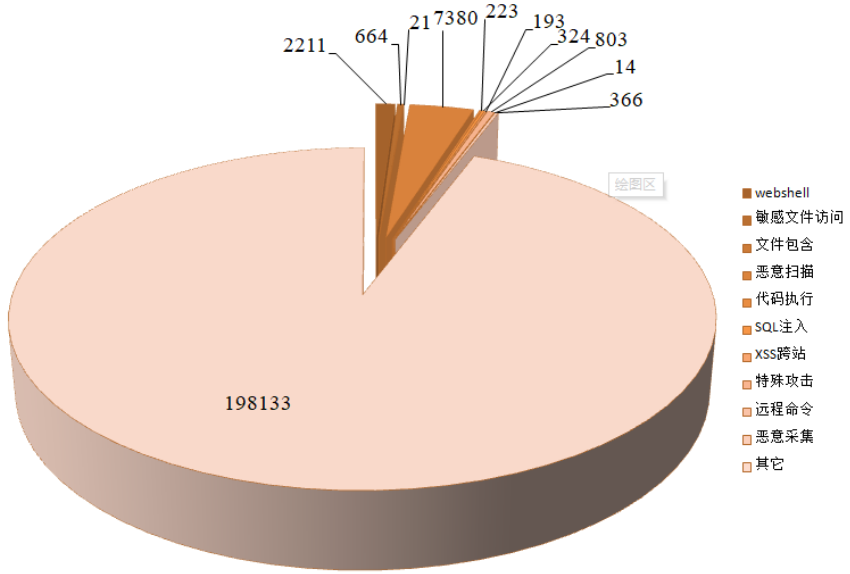
## 2018年10月1日-10月31日攻击拦截态势和网络攻击态势分布












本周期内共发生各类安全攻击210332次，黑客攻击占总请求数的比率为1.14%，其中Webshell攻击2211次、敏感文件访问664次、文件包含攻击21次、恶意扫描7380次、代码执行223次、SQL注入324次、XSS跨站攻击 193次、特殊攻击803次、远程命令执行14次、恶意信息采集366次，其它198133次。

## 潜伏在身边的黑客

**“海莲花”**

（360威胁情报中心）

2012年4月起，有境外黑客组织对中国政府、科研院所、海事机构、海域建设、航运企业等相关重要领域展开了有组织、有计划、有针对性的长时间不间断攻击。根据360威胁情报中心对APT组织的命名规则，同时结合其某些攻击特点，将该组织命名为“海莲花”（OceanLotus）。

“海莲花”组织（APT-C-00）组织的攻击周期之长、攻击目标之明确、攻击技术之复杂、社工手段之精准，都说明该组织绝非一般的民间黑客组织，而很有可能是具有国外政府支持背景的、高度组织化的、专业化的境外国家级黑客组织。

## 攻击目的和受害分析

该组织主要通过"鱼叉攻击"和"水坑攻击"等方法，配合多种社会工程学手段进行渗透，向境内特定目标人群传播特种木马程序，秘密控制部分政府人员、外包商和行业专家的电脑系统，窃取系统中相关领域的机密资料。

360 天眼实验室捕获海莲花的首个特种木马出现在2012年4月。在此后的3年中，又先后捕获了与该组织相关的4种不同形态的特种木马程序样本100余个，这些木马的感染者遍布国内29个省级行政区和境外的36个国家。此外，2018年，360威胁情报中心发现了“海莲花”组织使用的新的CVE-2017-11882漏洞文档，通过对该漏洞文档及相关攻击活动的分析，关联到其针对南亚国家的攻击活动。360威胁情报中心认为该组织利用“永恒之蓝”漏洞对我国高校实施新一轮重点攻击活动，并随后进行横向渗透。

## 针对国内高校攻击活动相关事件时间线

- 2017.4.4 “影子经纪人”泄露的NSA攻击武器中包含了“永恒之蓝”漏洞利用相关
- 2017.4.27-28 “海莲花”组织注册相关域名
- 2017.5.9 疑似“海莲花”组织利用“永恒之蓝”针对国内高校的攻击行动
- 2017.5.12 WannaCry事件全面爆发
- 2017.5.13 微软发布紧急修补补丁
- 2017.5.15 疑似“海莲花”组织攻击行动呈下降趋势

# 重大漏洞预警

## 1 Mozilla Firefox拒绝服务漏洞（CNVD-2018-21847）

Mozilla Firefox是美国Mozilla基金会开发的一款开源Web浏览器。 Mozilla Firefox 63之前版本中存在安全漏洞。远程攻击者可利用该漏洞造成拒绝服务

解决方案:

厂商已发布漏洞修复程序，请及时关注更新：https://www.mozilla.org/en-US/security/advisories/mfsa2018-26/；https://www.mozilla.org/en-US/security/advisories/mfsa2018-27/

## 2 多款Apple产品Kernel内存破坏漏洞（CNVD-2018-20992）

多款Apple产品中的Kernel组件存在安全漏洞。攻击者可利用该漏洞以内核权限执行任意代码（内存破坏）

解决方案：

厂商已发布漏洞修复程序，请及时关注更新：https://support.apple.com/zh-cn/HT209139

## 3 D-Link路由器密码明文存储漏洞

DWR-116、DIR-140、DIR-640等均是D-Link公司路由器产品。 D-Link路由器多个系列存在密码明文存储漏洞，该漏洞源于管理密码以明文形式存储在/tmp/XXX /0文件中。具有目录遍历（或LFI）的攻击者可以轻松获得完整的路由器访问权限。

解决方案:

用户可联系供应商获得补丁信息：http://www.dlink.com/

西安理工大学
XI'AN UNIVERSITY OF TECHNOLOGY

# 网络信息管理中心

# 校园网运行与安全简报

扫码关注

西安理工大学微信企业号

2018