西安理工大学
XI'AN UNIVERSITY OF TECHNOLOGY

网络信息管理中心

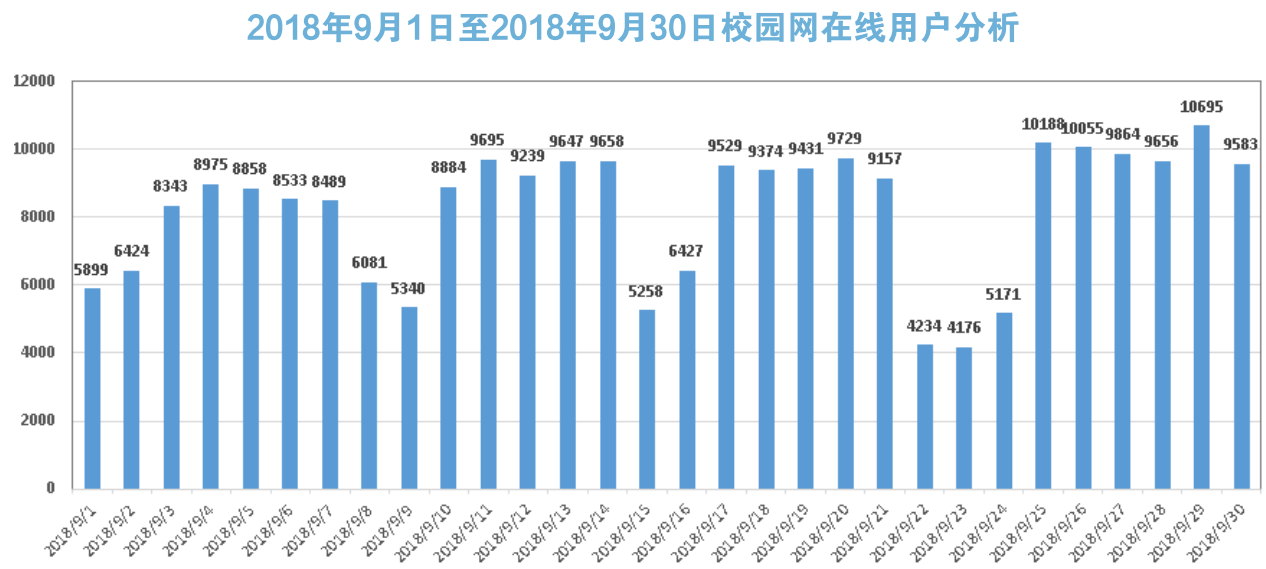
信息化工作简报

9 月

2018

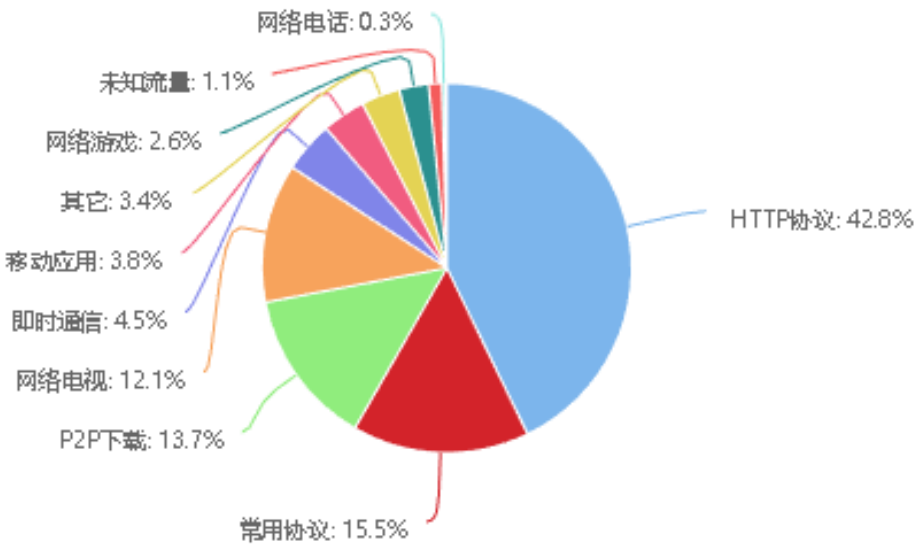
校园网用户统计、流量分布

9月，校园网整体运行正常，日均在线用户8200人，其中无线用户日均在线7000人。



校园网出口峰值使用带宽7.45G，2018年9月1日-2018年9月30日，校园网下行总流量达到276TB，上行总流量170TB。

其中，浏览器日常访问产生流量占比42.8%位居首位，迅雷等P2P下载流量及网络电视相关应用分别占比约13.7%和12.1%。

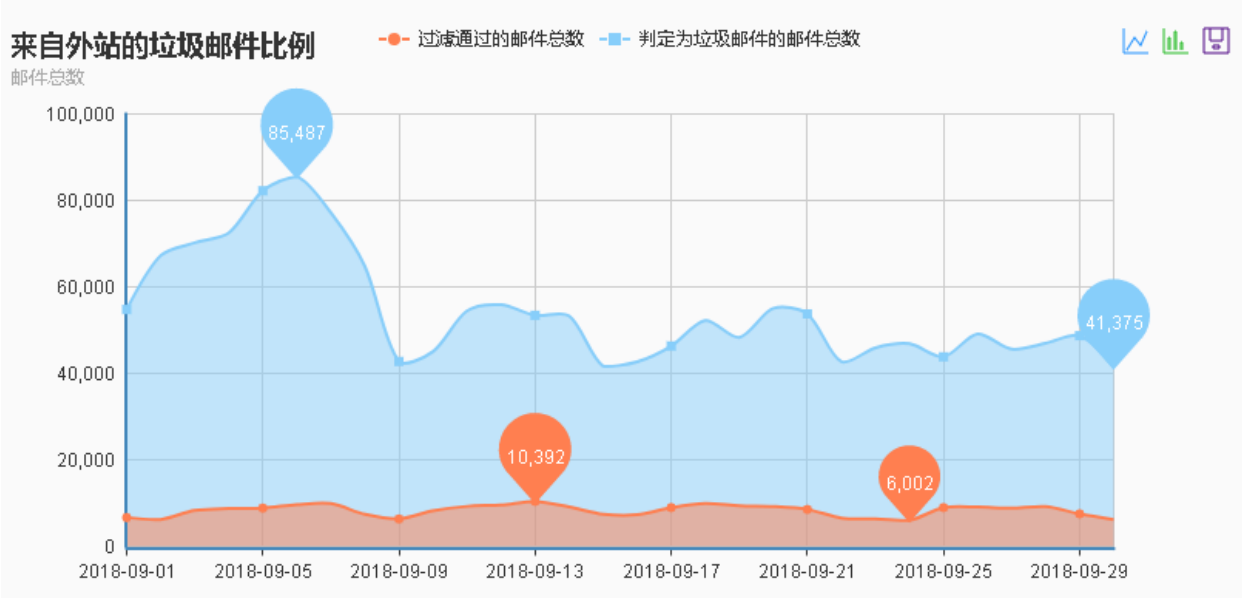


校园邮件系统运行数据

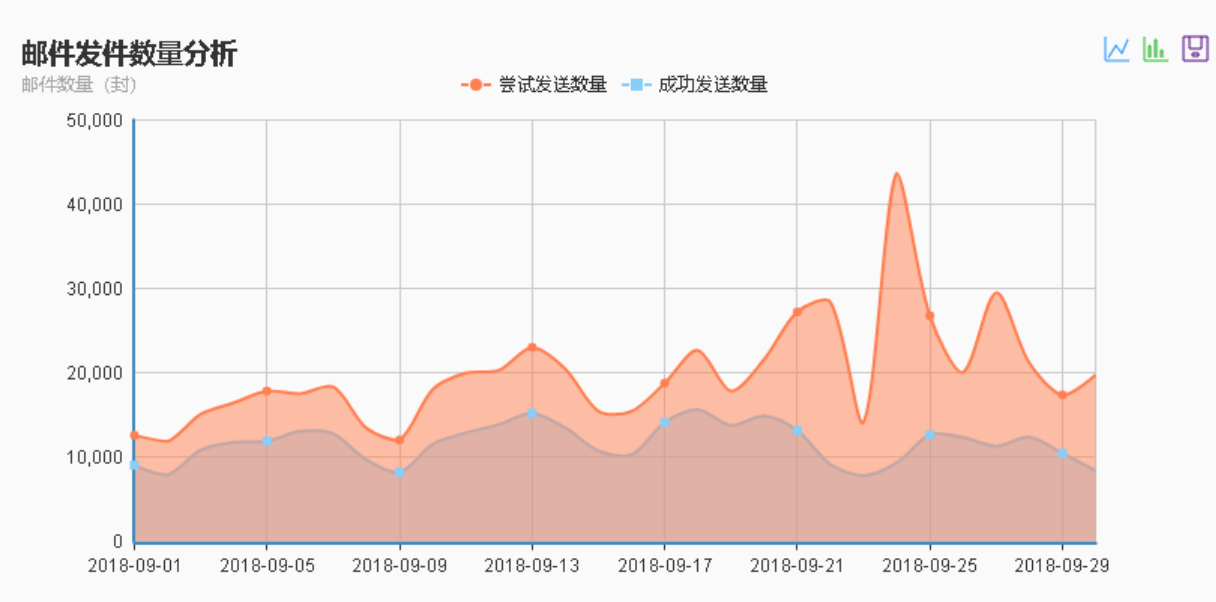
2018年9月，我校邮件系统运行稳定，垃圾邮件拦截网关工作正常。

用户日均对外发送邮件1.1万余封，邮件系统日均拦截垃圾邮件近5万封。

校园邮件系统垃圾邮件拦截数据统计

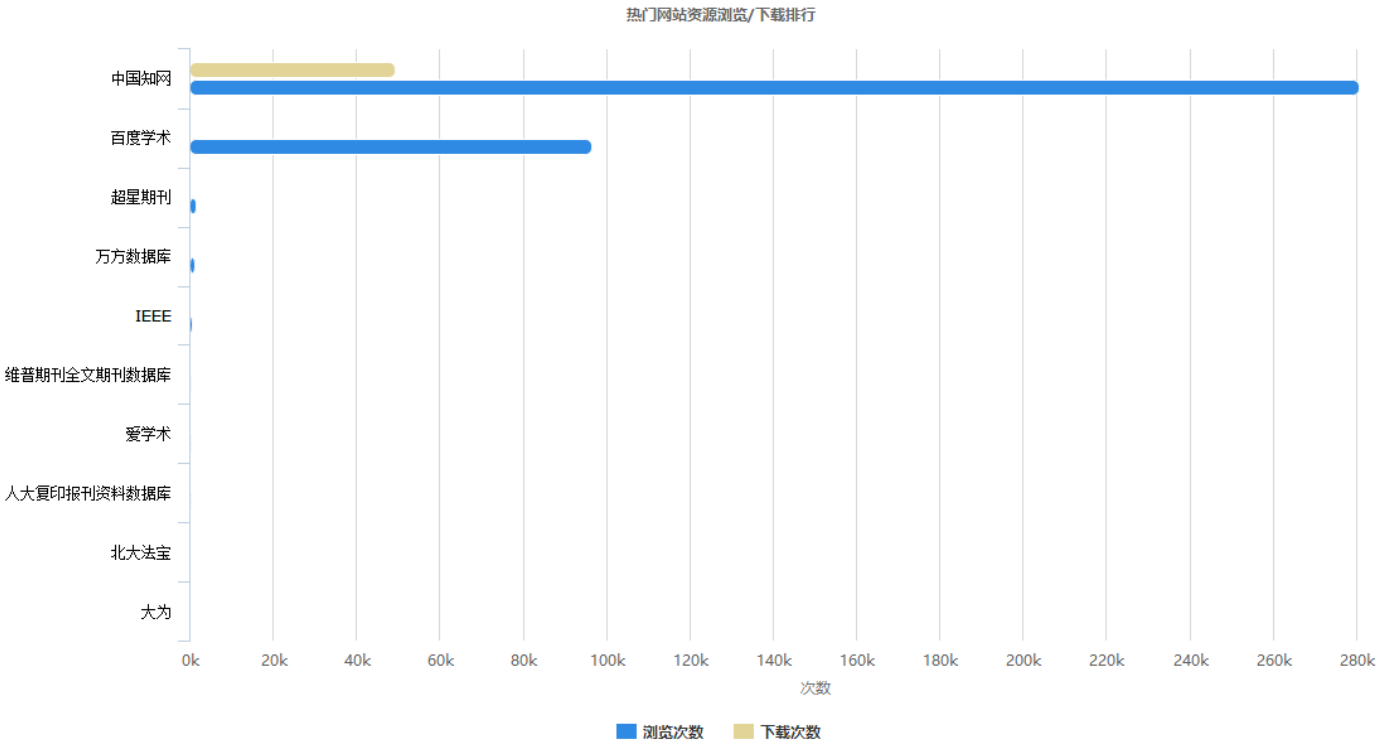


校园邮件系统发件数据统计

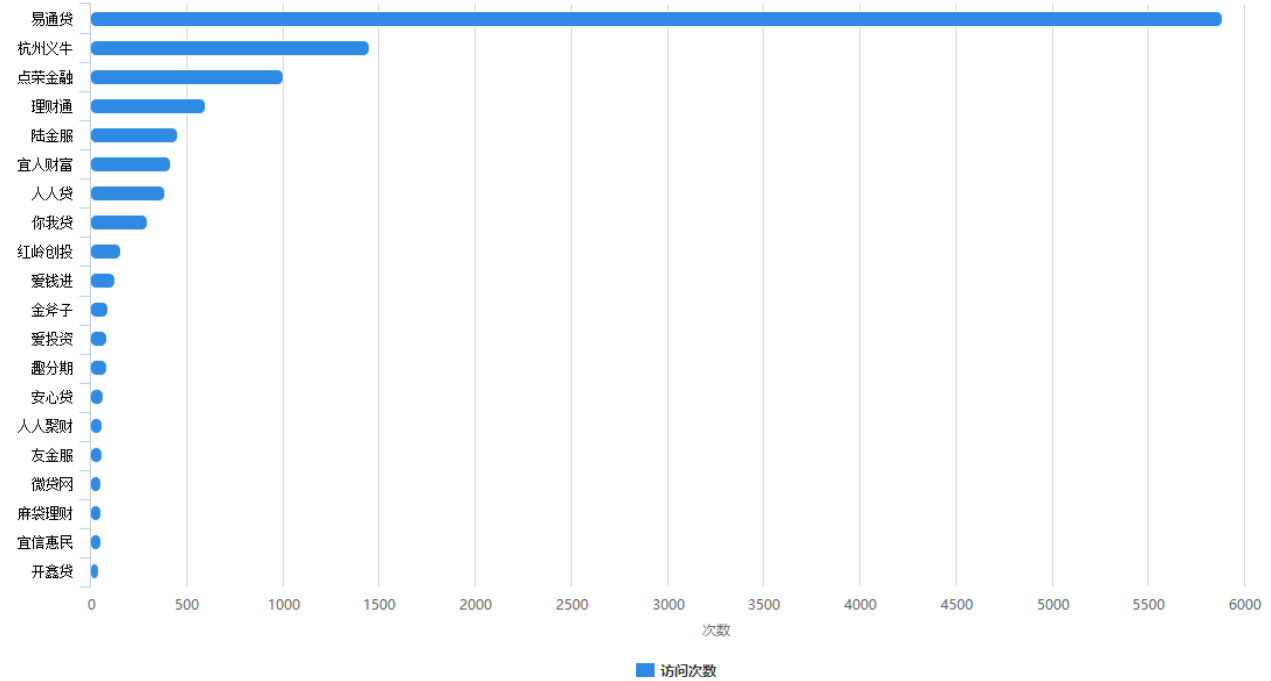


校园网大数据

图书资源访问情况



金融APP访问情况



校园网应用小贴士

关于校园邮件系统，你应该知道的几件事

校园邮箱分类

分类	教师邮箱	学生邮箱	部门邮箱
域名	@xaut.edu.cn	@stu.xaut.edu.cn	@xaut.edu.cn
收发限制	日发送上限300 收件无限制	日发送上限300 收件无限制	日发送上限2000 收件无限制
个人网盘	500M	500M	无
邮箱别名	4个	4个	2个

我校邮件系统运行现状

我校邮件系统采用学生云端部署+教师本地私有云的部署方式，大大提高了邮件的管理效率和系统可用性。截至2018年9月30日，系统师生账户共计32445个。

邮件系统的登录方式

我校邮件系统目前支持3种登录方式：

1. 电脑Web页面登录
2. 手机Web页面登录
3. 第三方客户端登录（Foxmail、QQmail、论客等）

如何设置客户端收发信件

1.配置邮件服务器域名地址

	教师邮箱	学生邮箱	端口号
POP3服务器	pop3.xaut.edu.cn	edu.icoremail.net	110
IMAP服务器	imap.xaut.edu.cn	edu.icoremail.net	143
SMTP服务器	smtp.xaut.edu.cn	edu.icoremail.net	25

2.客户端设置IMAP与POP3的区别

POP3协议允许电子邮件客户端下载服务器上的邮件，但是在客户端的操作（如移动邮件、标记已读等），不会反馈到服务器上。比如通过客户端收取了邮箱中的2封邮件并移动到其他文件夹，邮箱服务器上的这些邮件是没有同时被移动的 。

IMAP提供webmail 与电子邮件客户端之间的双向通信，客户端的操作都会反馈到服务器上，对邮件进行的操作，服务器上的邮件也会做相应的动作。

这意味着当您使用网络浏览器登录到邮箱时，您在电子邮件客户端和移动设备上执行的操作（例如，将邮件移至“分享”文件夹）将立即自动反映在邮箱中（例如，在您下次登录时，这封电子邮件已具有一个“分享”标签）。

垃圾邮件提醒功能

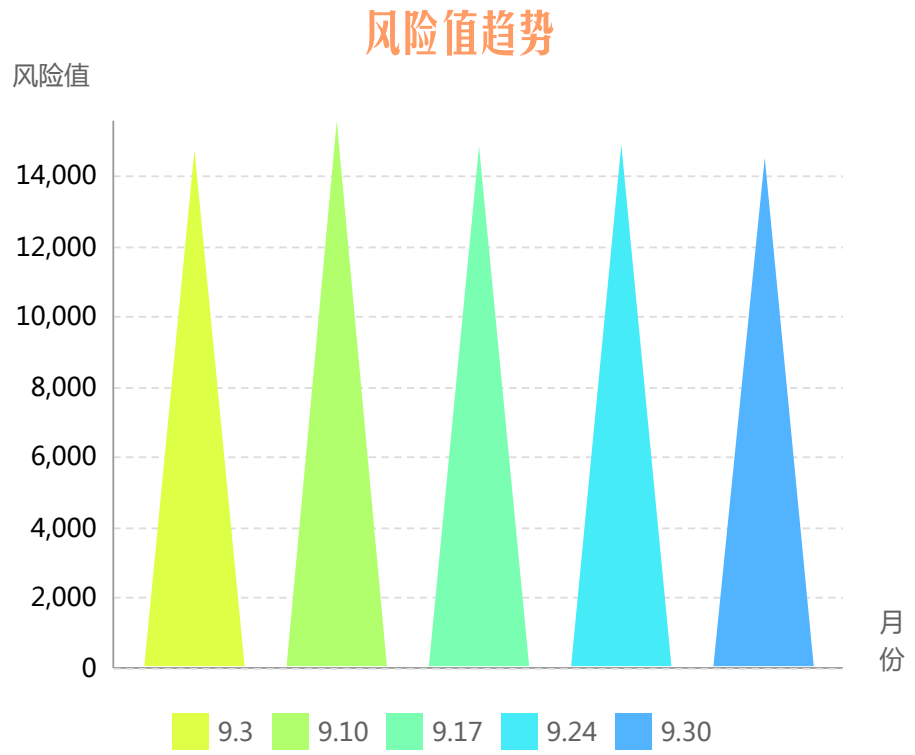
校园邮件系统提供“垃圾邮件通知”功能，用户可以自行根据需要调整通知频率，避免少数邮件被系统误拦截，出现收不到邮件的情况。

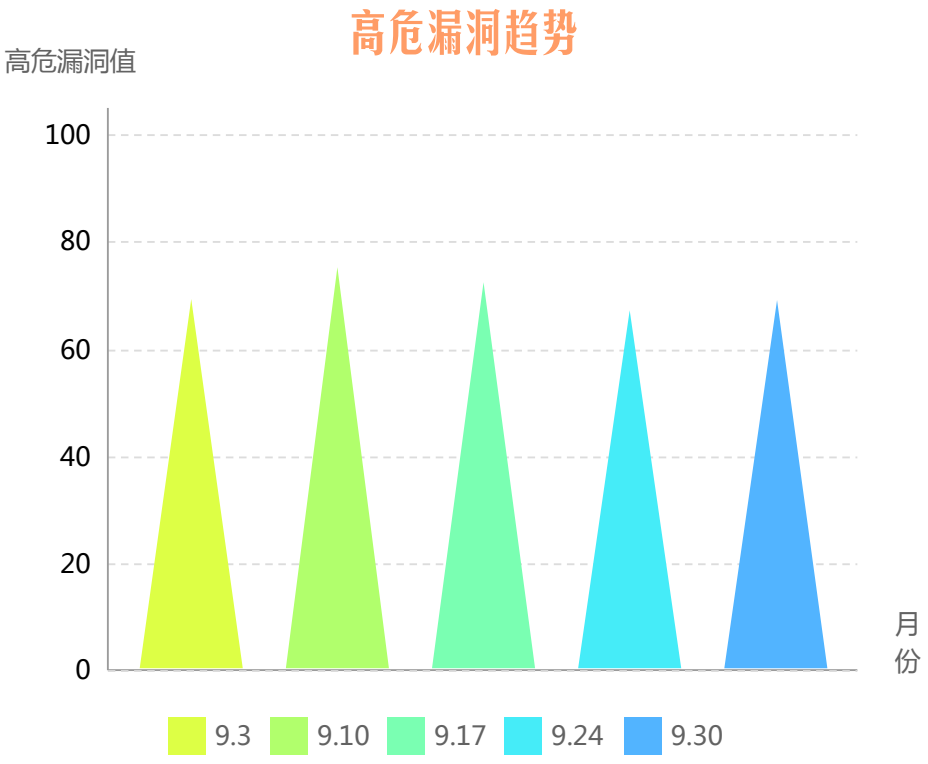
网络与信息安全趋势

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9月1日-9月30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9月1日-9月30日网络安全态势分布图





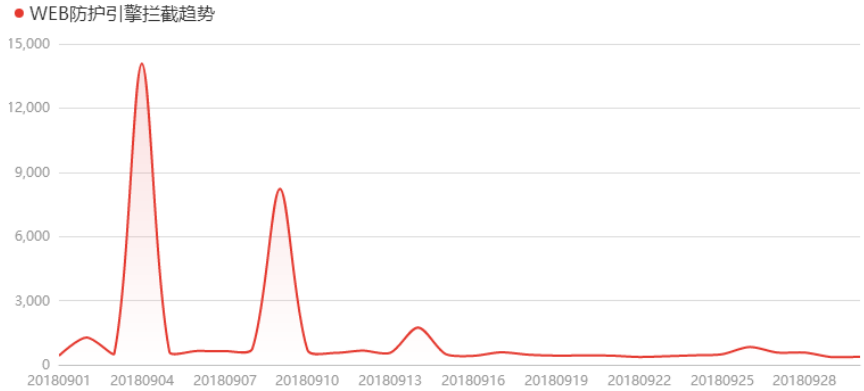
网络与信息安全趋势

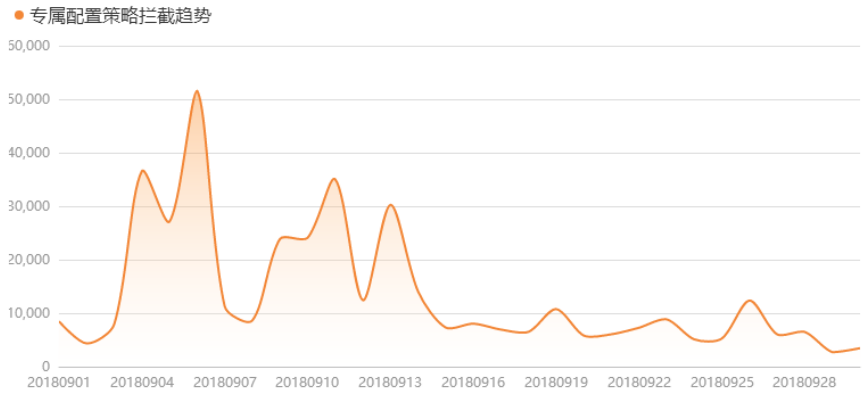
本周期统计以网络中心监测的数据作为主要依据，对我校重要信息系统（网站）面临的各类安全威胁及基本情况进行总体态势分析；评估范围为：2018年9月1日-9月30日。

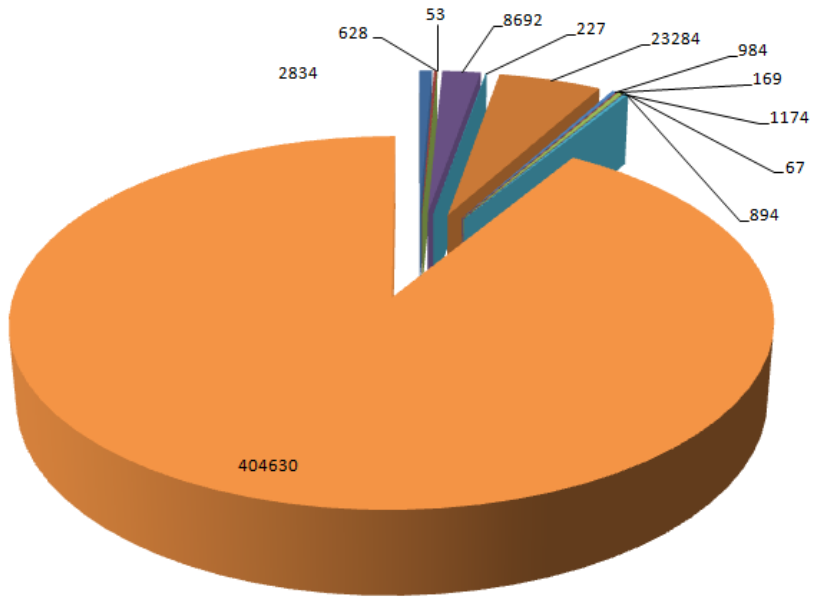
重要信息系统（网站）基本情况

总请求数	总流量	搜索引擎	Alexa 全球排名
27928674次	2488.46GB	423,623次	123648

2018年9月1日-9月30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443636次，黑客攻击占总请求数的比率为1.59%，其中Webshell攻击2834次、敏感文件访问628次、文件包含 攻击53次、恶意扫描8692次、代码执行227次、CC攻击23284次、SQL注入984次、XSS跨站攻击 169次、特殊攻击1174次、远程命令执行67次、恶意信息采集894次，其它404630次。

潜伏在身边的黑客

“毒云藤”

该组织在多次攻击行动中，都使用了 Poison Ivy（毒藤）木马，并在中转信息时，曾使用云盘作为跳板传输资料，这跟爬藤类植物，颇有相似之处。根据360威胁情报中心对APT组织的命名规则，同时结合关联地区常见的蔓藤植物，将该组织命名为“毒云藤”。

军政情报刺探者揭露（360威胁情报中心）

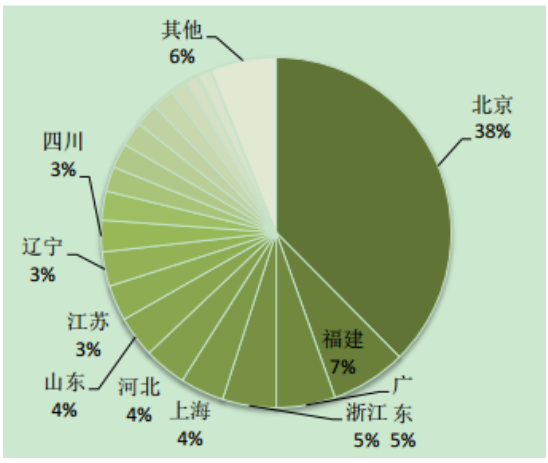
“毒云藤”组织（APT-C-01）是一个针对政府、军工、海事等领域敏感信息持续发起攻击的 APT 组织。另，国内安天实验室于 2018 年 9 月 19 日发布 APT 攻击组织“绿斑”（Green Spot），根据对比约定，二者是同一组织。

攻击目的和受害分析

从 2007 年开始至今，360 追日团队发现毒云藤组织对中国国防、政府、科技、教育以及海事机构等重点单位和部门进行了长达 11 年的网络间谍活动。该组织主要关注军工、中美关系、两岸关系和海洋相关领域（南海、东海、测绘）。

360 追日团队捕获毒云藤的首个木马出现在 2007 年 12 月。在之后的 11 年中先后捕获到了 13 个版本的恶意代码，涉及样本数量 73 个。该组织在初始攻击环节主要采用鱼叉式钓鱼邮件攻击，攻击之前对目标进行了深入调研和精心挑选，选用与目标所属行业或领域密切相关的内容构造诱饵文件和邮件，主要采用相应具体领域相关会议材料、研究成果或通知公告等主题。这些木马的感染者遍布国内 31 个省级行政区。

攻击地域分布



中国被感染地区比例及分布图
（2014 年 7 月-2015 年 6 月）

网络间谍活动相关时间节点

2007 年 12 月，首次发现与该组织相关的木马（疑似对某大型船务公司进行相关攻击）

2008 年 3 月，对国内某高校重点实验室（某科研机构）

2009 年 2 月，开始对军工行业展开攻击（某知名军工类期刊杂志社）

2012 年 2 月，首次发现基于 zxshell 代码的修改版后门 1，其关键功能是窃取如.doc\.ppt\类文档文件

2013 年 3 月，对中科院，以及若干科技、海事等领域国家部委、局等进行了集中攻击

2013 年 10 月，对中国某政府网站进行水坑攻击

2014 年 5 月，发现 zxshell 修改版后门 2，增加了如“军”，“航”，“报告”关键字的搜索

2015 年 2 月 25 日，对某军工领域协会组织（国防科技相关）、中国工程院等攻击，发现酷盘版样本

2017 年 10 月，对某大型媒体机构网站和泉州某机关相关人员实施鱼叉攻击

2018 年 5 月，针对数家船舶重工企业、港口运营公司等海事行业机构发动攻击

重大漏洞预警

1 Android系统广播机制存在漏洞，恶意软件可绕过安全机制跟踪用户

Android系统的内部广播机制会暴露敏感的用户和设备信息，手机上安装的应用可在用户不知情或未经许可的情况下访问获取这些信息。Android系统的内部广播机制泄露的数据包括：Wi-Fi网络名称、Wi-Fi网络BSSID，本地IP地址、DNS服务器信息和设备的MAC地址等详细信息。

解决方案:

因为这是一个重大的API变更，谷歌仅在Android P/9中修复了这个问题，旧版的Android系统不会得到更新，建议用户升级到Android P/9或更高版本。

2 通过Safari浏览器漏洞进行的URL欺骗攻击

允许攻击者在Windows的Edge浏览器和iOS的Safari中进行URL欺骗攻击。利用这个漏洞,攻击者可以模仿任何web页面,包括Gmail、Facebook、Twitter、甚至银行网站,并创建假的登录屏幕或其他形式盗窃用户的凭证和其他数据。

解决方案：

微软8月份的安全更新已经修复了Edge地址栏欺骗漏洞，但Safari尚未修复，可能使Apple用户受到网络钓鱼攻击。

3 Windows任务计划程序被曝存在0 day漏洞

该漏洞存在于Windows 10和Windows Server 2016 64位操作系统任务计划程序的高级本地程序调用（ALPC）接口之中，这两个版本的操作系统中ALPC的API函数未对请求权限进行正确的验证，因此任何本地攻击者都将可以对请求数据进行修改，实现提权。

解决方案:

目前，微信官方目前尚未发布补丁修复该漏洞，针对此中危漏洞，请广大用户及时关注微软官方补丁更新升级，并提前部署好信息安全防御工作。