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

目录

学生大数据分析与服务平台顺利试运行

按照中心要求，秋季学期开学以来，信息管理部多次召开由中心主任、企业研发团队参加的学生大数据平台试运行准备会，先后召开了平台软件边界及主要存在问题研讨会、集成测试会、项目功能修订推进会、大数据平台技术培训会、数据正确性验证会等，多维度保障平台的数据准确、应用场景准确。

2019年9月26日上午，在学校第一会议室召开了学生大数据分析与服务平台试运行启动会，纪委书记李鹏出席会议并讲话，会议由网络信息管理中心主任李军怀主持，学生处、教务处、研究生院、团委及相关人员参加了会议。

会上，网络信息管理中心信息管理部主任李燕汇报了“大数据分析与服务平台”的建设情况及推广计划，并现场演示了平台的主要功能；各部门负责人就平台的建设目标及效果给予了良好评价，并提出了宝贵的意见和建议。

李鹏对平台建设工作成效给予了充分肯定。他指出，大数据是今后数据应用的发展方向，各部门思想上要重视，严把数据质量关；他要求，做好数据安全和隐私保护工作，团结协作建好平台，希望依托平台为学校的工作决策提供支持。

从2019年9月底开始，学生大数据分析与服务平台一期将上线试运行，该平台旨在为学校领导提供决策的数据支持，为各位工作人员提供数据参考，为广大师生提供个性化服务。目前完成的一期建设并不是大数据平台建设的终点，而是建设的第一步，网络信息管理中心将继续建好数据资产，优化平台功能，提高智能计算准确性，不断提升平台的服务质量。（李燕 张爱玲 李宏伟）

我校开展“校园网络安全主题日”活动

9月17日是国家网络安全宣传周的首个主题 “校园日”。为普及网络安全知识，提升网络安全意识，17日下午，网络信息管理中心携校团委、学生处，在西安理工大学数据中心机房与校园卡务中心，组织开展“校园网络安全主题日”活动。

活动期间，校园卡管理部在校园卡务中心大厅结合圈存机、自助现金充值机的现场演示，详细讲解了校园卡的使用须知等方面内容。网络安全管理部结合校园网基础设施和数据中心架构，实地展示讲解我校数据中心机房，并展示了我校的网络空间实时防御和追踪系统。信息管理部为学生作了《信息化之旅》的专题培训。

此次活动以“e言e行见素养，e点e滴筑安全”为主题，是我校2019年网络安全宣传周的系列活动之一，生动形象的为在校师生呈现出我校的网络安全体系和信息化发展变迁。（王心成）

我校代表队在陕西省第四届“网安启明星”大学生网络安全知识竞赛获得佳绩

2019年9月20日，陕西省第四届“网安启明星”大学生网络安全知识竞赛总决赛在西北工业大学落下帷幕。经过前期40余所高校代表队的激烈角逐，我校代表队在网络信息管理中心王心成老师的带领下，凭借出色发挥，在复赛中脱颖而出，成功晋级决赛。

在决赛中，我校机仪学院王昆鹏、理学院岳子林和计算机学院李若鹏三位同学经过“个人必答与团队必答”、“快速抢答”等四个环节的激烈比拼，最终获得团体优秀奖。机仪学院王昆鹏荣获“优秀选手”称号。（王心成）

信息档案支部组织召开“不忘初心、牢记使命”主题教育启动会

9月20日上午10:00，信息档案党支部组织召开“不忘初心、牢记使命”主题教育启动会。会议由信息档案党支部书记侯小军主持，支部全体党员参会学习。

侯小军书记传达了学校主题教育工作会议精神，解读了学校相关主题教育文件要求及工作实施方案的主要内容和安排，具体安排了主题教育工作实施方案、集中学习计划和学习要求。同时带领全体党员深入学习了习近平总书记在“不忘初心、牢记使命”主题教育工作会议重要讲话精神，领会“不忘初心、牢记使命”主题教育的重大意义（4个迫切需要）、1个根本任务、12字总要求、5个具体目标、4个重点措施和各级党组织的职责等。习近平总书记的重要讲话具有很强的政治性、思想性、针对性、指导性，是开展好本次主题教育的根本指针，是新时代加强党的建设的纲领性文献。

侯小军书记给全体党员上了一堂题为《扎实开展“不忘初心、牢记使命”主题教育，持续提升工作水平和服务质量》的党课，深入阐述了习近平新时代中国特色社会主义思想的理论体系主要核心要义产生、形成过程。侯书记强调，要把学习教育、调查研究、检视问题、整改落实四项重点措施贯通起来，有机融合、统筹推进；同时把理论学习和工作实际结合起来，持续提升工作水平和服务质量。

随后，李志强副书记带领大家学习了习近平总书记在内蒙古、甘肃考察并指导开展“不忘初心、牢记使命”主题教育时的讲话精神，研读了《习近平关于“不忘初心、牢记使命”重要论述选编》的部分文章。

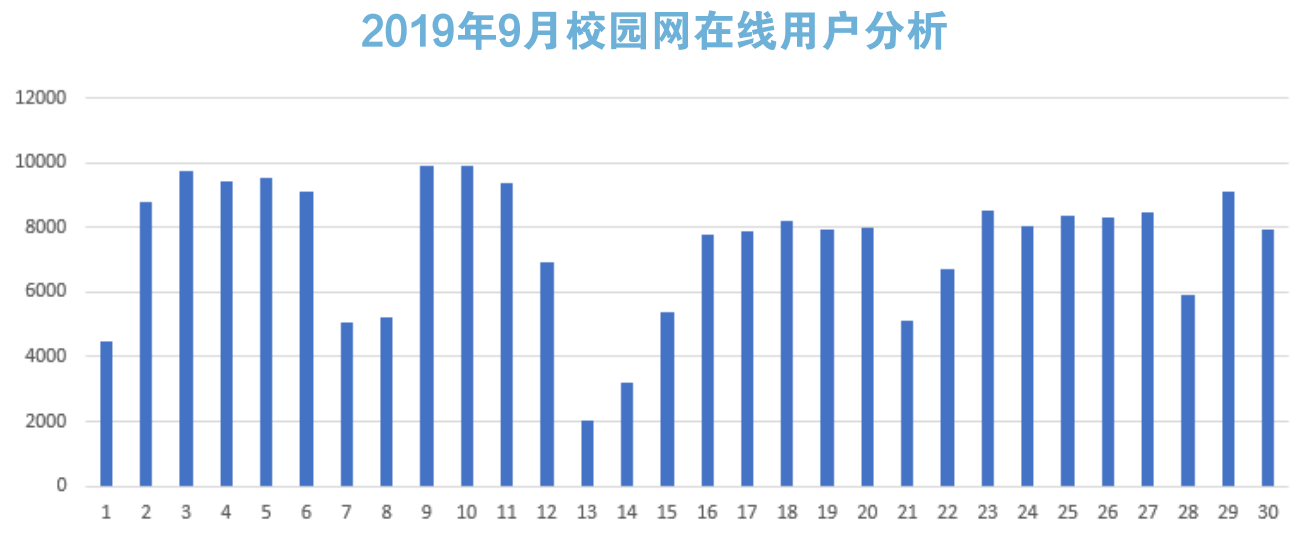
最后，信息档案支部全体党员集体观看了中午12:20的《一生只为一事来》。（杨超）

校园卡部工作动态

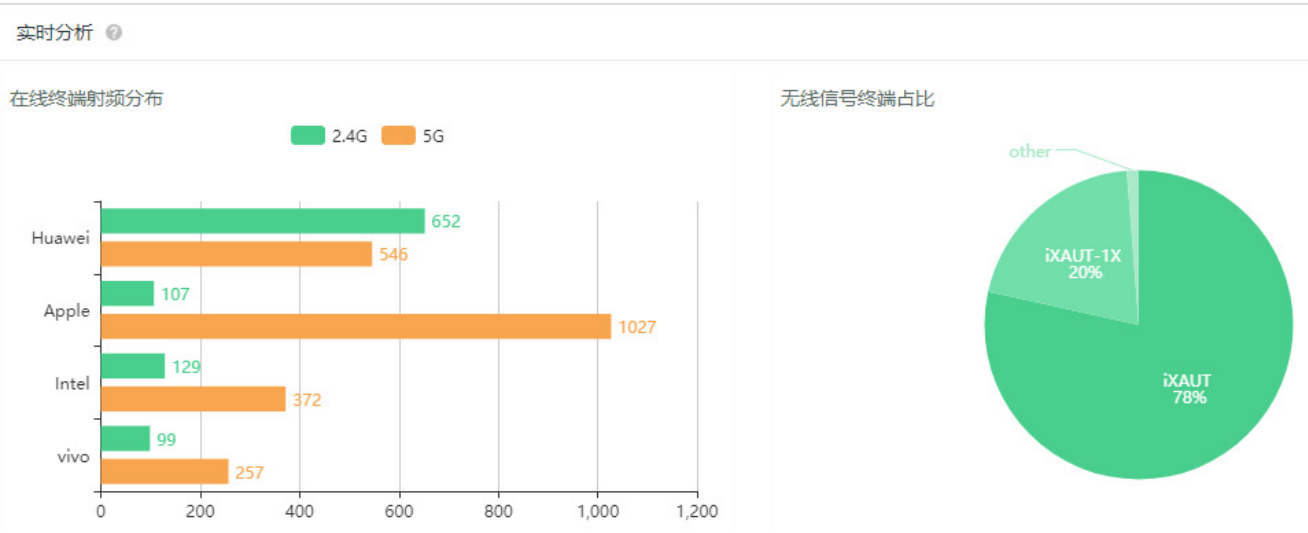
积极参与“校园网络安全主题日”活动，在曲江校区校园卡务中心向同学们详细讲解了校园卡的功能、校园卡使用须知、校园卡使用过程中的注意事项和使用安全等事项，并在曲江校园卡务中心大厅对圈存机、自助现金充值机等设备的功能进行了现场演示。通过此次活动，让学生们进一步了解了我校校园卡的运行机制，运行状态，运行安全。

9月23日至26日，完成了阳光体育考勤系统的改造维修相关工作。其中，对金花校区篮球场的网络线路进行了重新铺设，对乒羽场的网络线路、电源线路进行了重新铺设，并对所有线路进行了PVC管嵌套，保证其使用质量与使用安全。对北门体育馆的的电源问题进行了修复。此项工作的完成，修复了之前数据不能实时上传的问题，保证了学生们的打卡记录安全性与数据上传的时效性，取得了良好的效果。(王力)

校园网在线用户分析

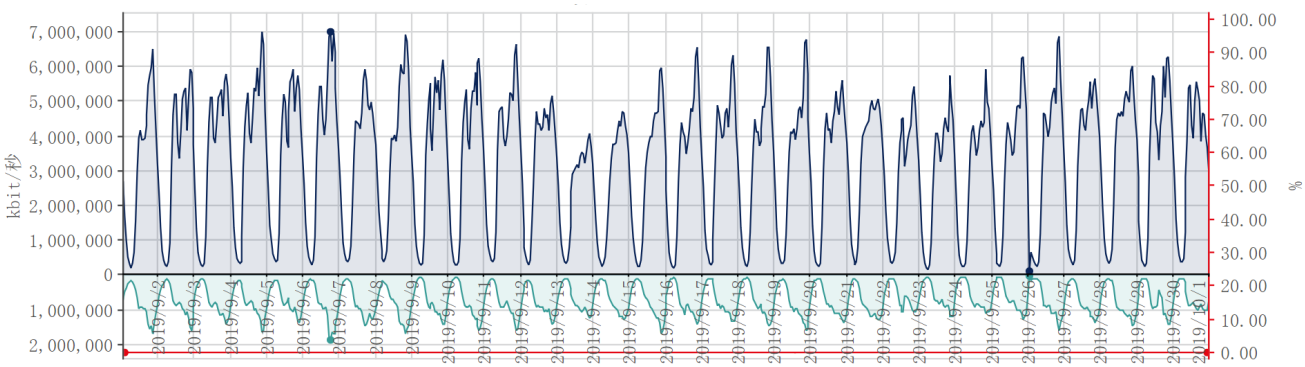


9月，校园网整体运行正常，日均在线用户7476人，其中无线用户日均在线5820人。其中iXAUT网络使用人数占比80%，iXAUT-1X网络使用人数占比20%，各厂商终端5G频段使用用户持续上升。



校园网出口流量分析

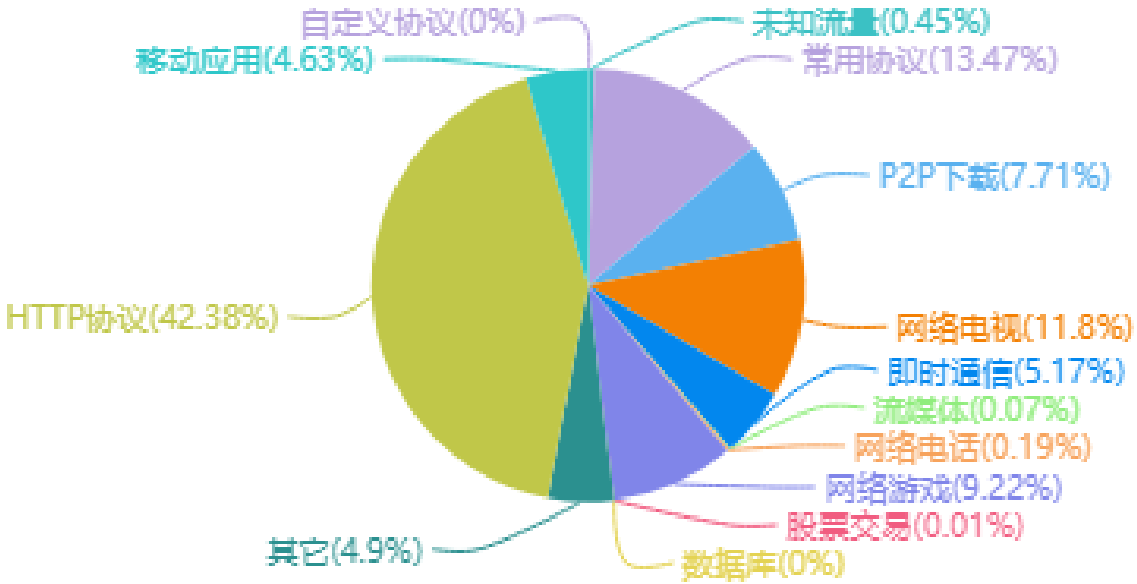
校园网出口流量趋势图



校园网出口峰值使用带宽近7G，2019年9月，校园网总下载流量达1.1PT，上传流量共计261T。

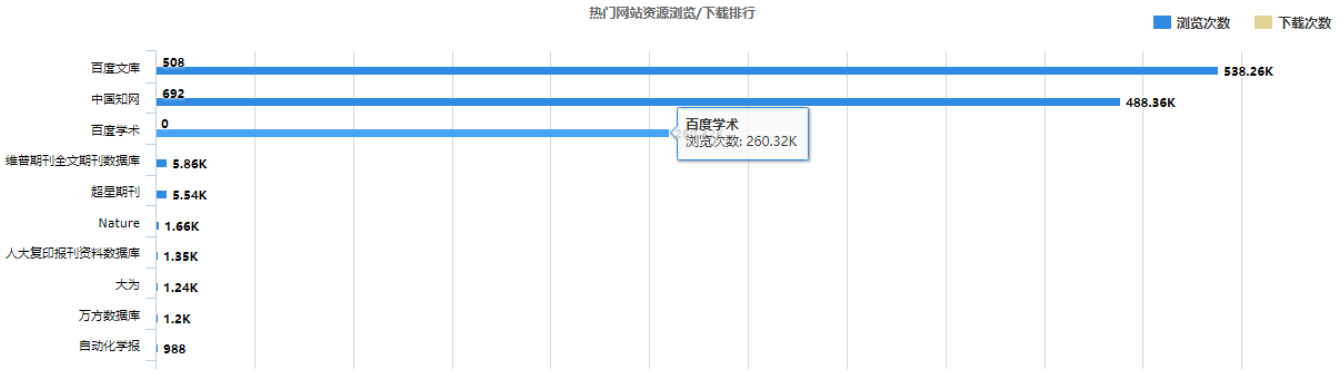
其中，HTTP日常访问产生流量达562.5T位居首位，常用协议流量及网络电视流量位居二三位，分别为179和156T。

校园网出口流量分布图

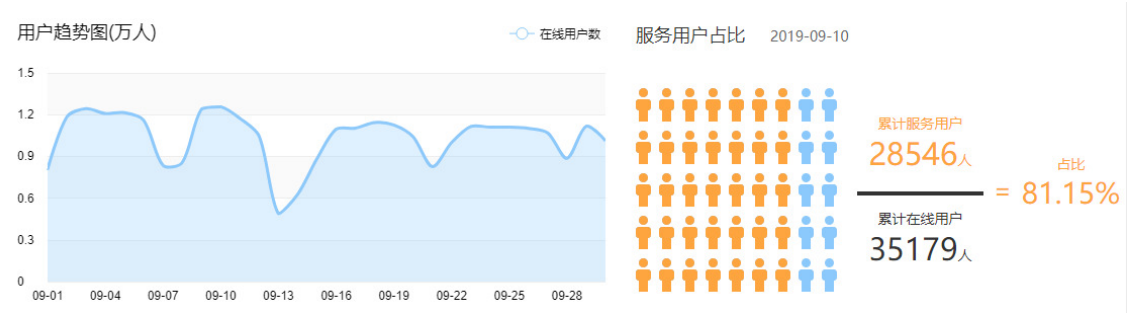


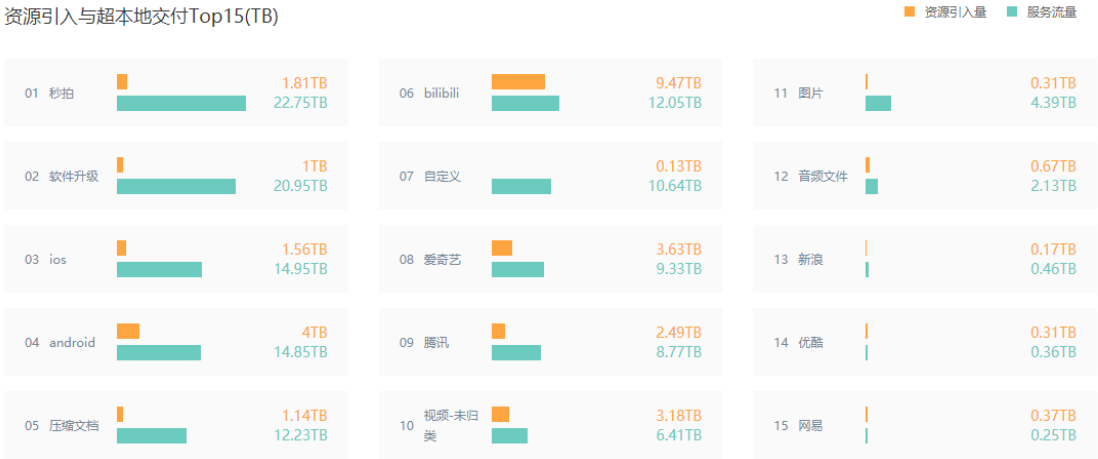
校园网资源使用分析

校园网图书资源访问统计



校园网出口内容加速数据



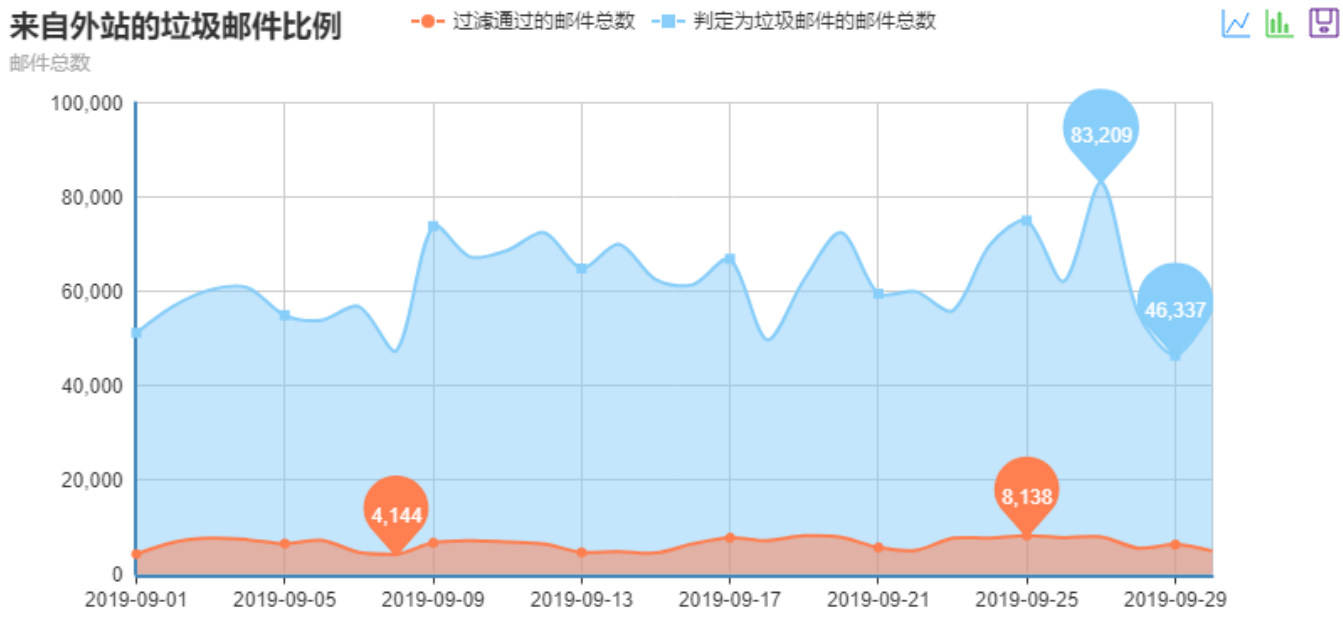


*注：以上数据由 Panabit® 飞享 ifeixiang.com 友情提供

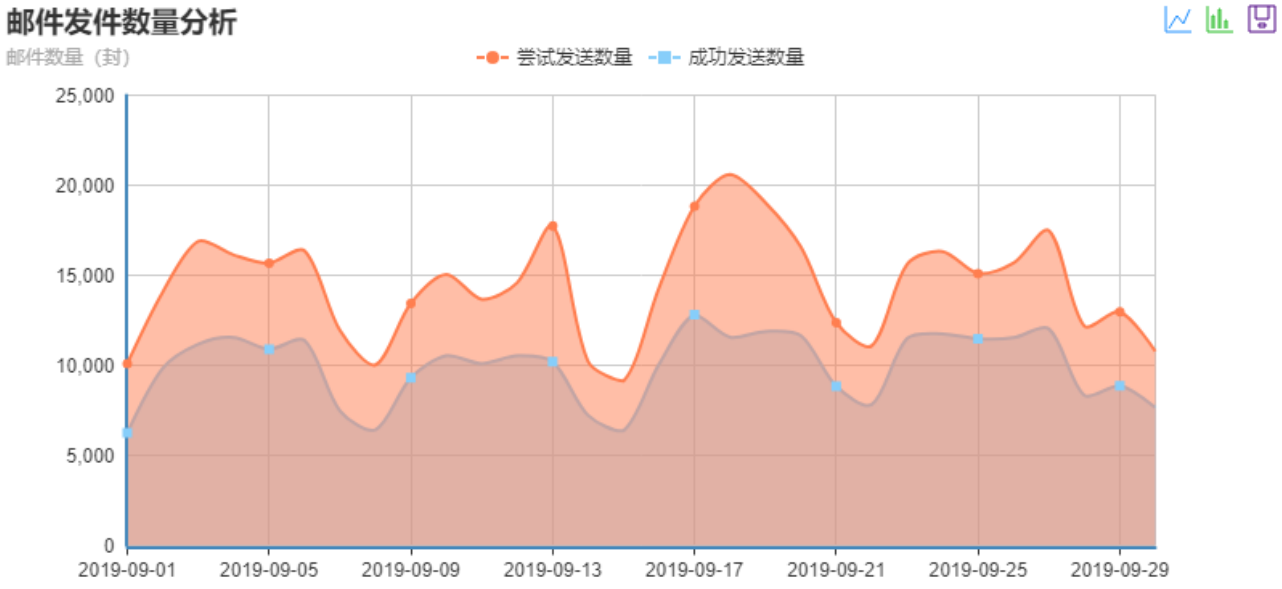
校园电子邮件系统运行情况分析

2019年9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61919封，日均发送邮件9025封。

校园邮件系统垃圾邮件防御数据统计

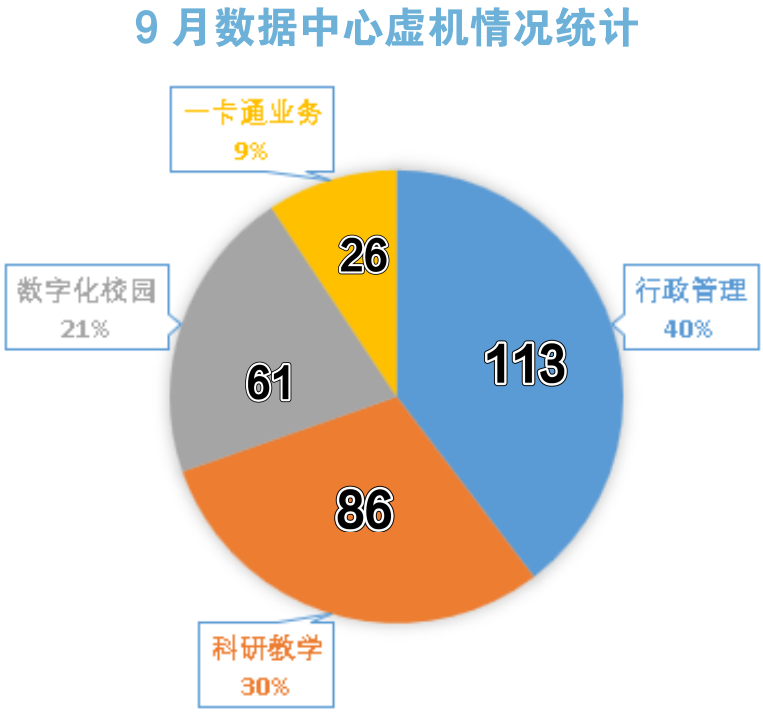


校园邮件系统发送邮件统计



数据中心运行情况

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）



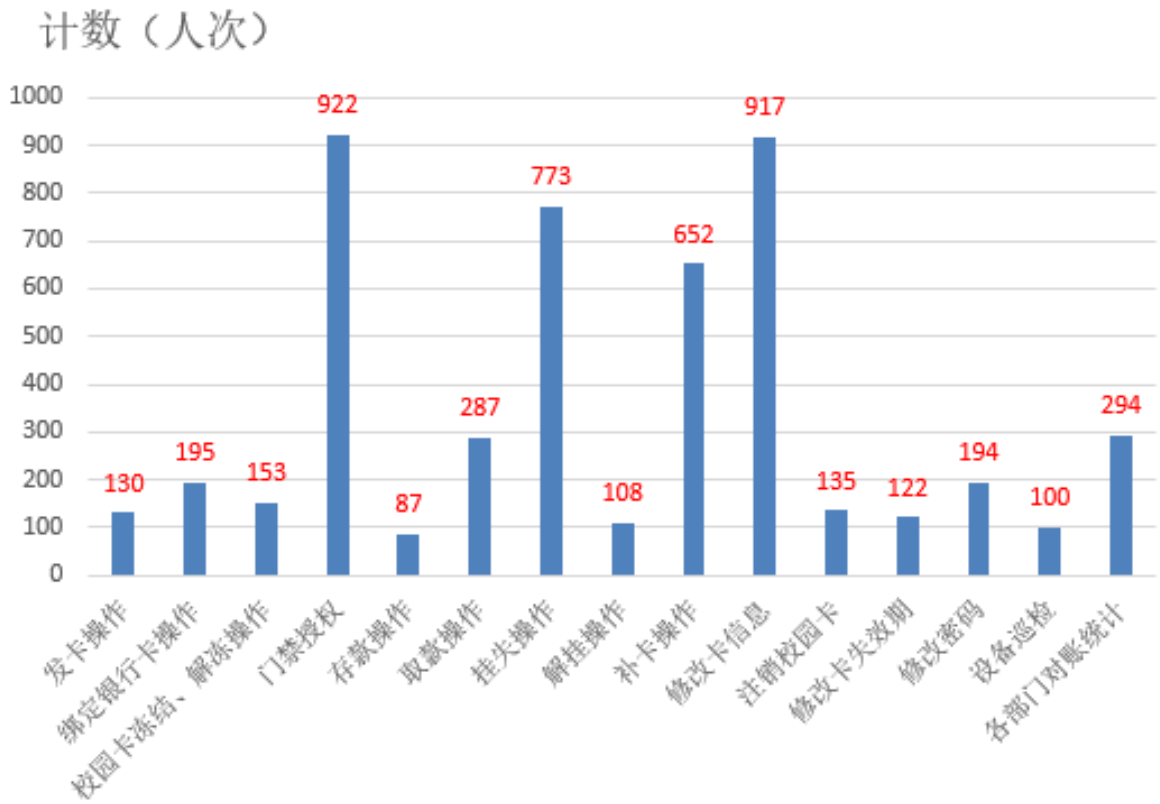
数据中心机房整体运行稳定，9月发生2次停电，UPS电池供电正常，服务器及网络设备未出现停机。中心机房空调故障0次，均及时处理，未影响机房整体制冷环境。（赵阳）

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	22.1
西安理工大学机房	东侧冷通道温湿度	温度11	22.4
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	21.0
西安理工大学机房	东侧冷通道温湿度	温度21	22.6
西安理工大学机房	东侧冷通道温湿度	温度23	25.0
西安理工大学机房	东侧冷通道温湿度	网络通信	正常

校园卡务月度数据统计

校园卡务中心 9月工作数据统计



2019年 9月餐厅消费数据排名

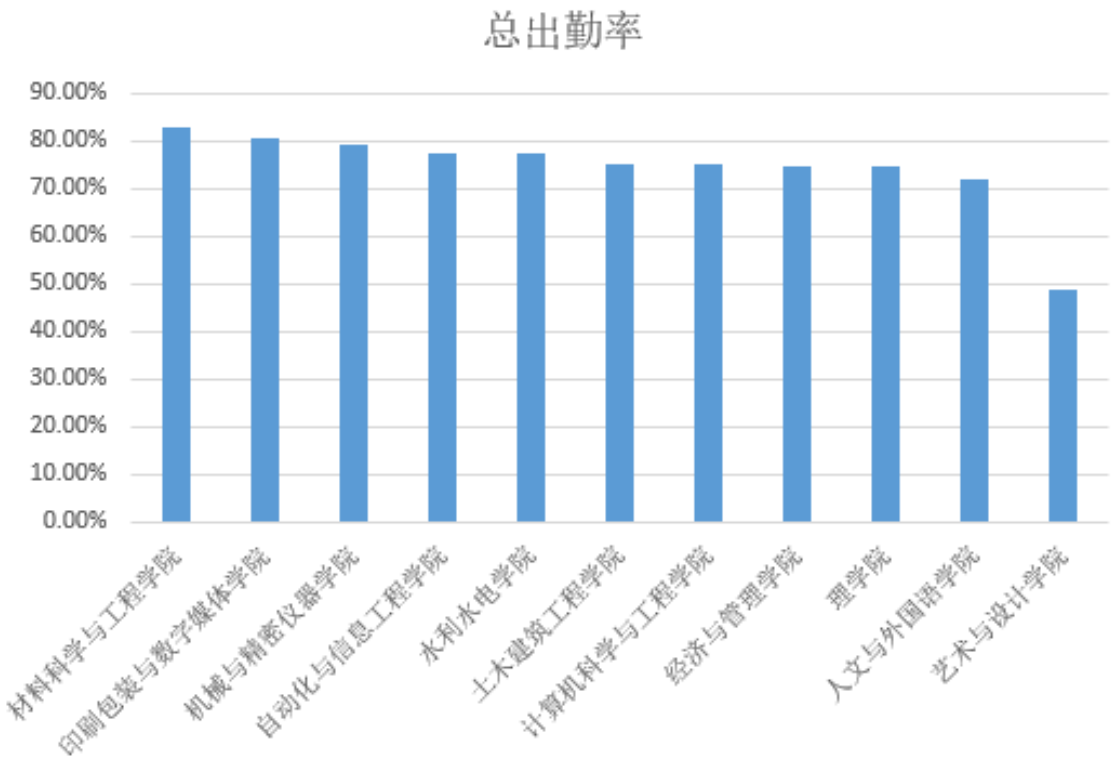
金花校区餐厅各窗口销量情况

餐厅名	名次		
	1	2	3
金花一餐厅	小卖部	山西饼	香再来
金花二餐厅	锅巴饭	快餐	新吧台
民族餐厅	豆浆	快餐	拉面

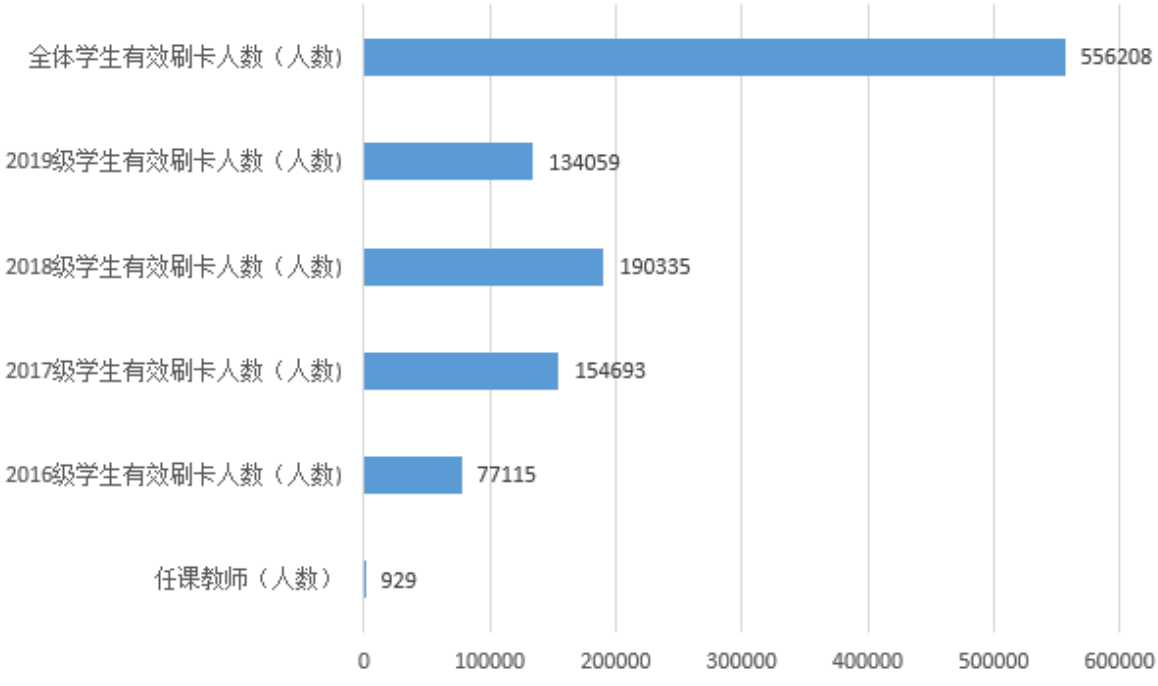
曲江校区餐厅各窗口销量情况

餐厅名	名次		
	1	2	3
曲江一餐厅	自选餐	小卖部	香锅
曲江二餐厅	川菜	麻辣烫	柠檬鱼
曲江三餐厅	自助餐	蒸鸡饭	盖浇饭
曲江四餐厅	麻辣拌	锡纸包饭	自助餐
民族餐厅	饼、炒饼	拌面、泡馍	快餐
教工餐厅	麦香饼	快餐	米线

2019年 9 月教务考勤系统运行情况统计图



2019年 9月教务考勤系统运行情况统计图



校园无线网与手机4G

我们国家也会在对国际电信联盟划给我们的各个无线电频段再进行细分给各个运营商

1、电信

4G的FDD频段：上行1765-1780MHz，下行1860-1875MHz

4G的TDD频段是不分上下行的，频段为：2370-2390MHz

2、联通

4G的FDD频段和3G一样： 上行1940-1965MHz，下行2130-2155MHz

4G的TDD频段：2300-2320MHz

3、移动

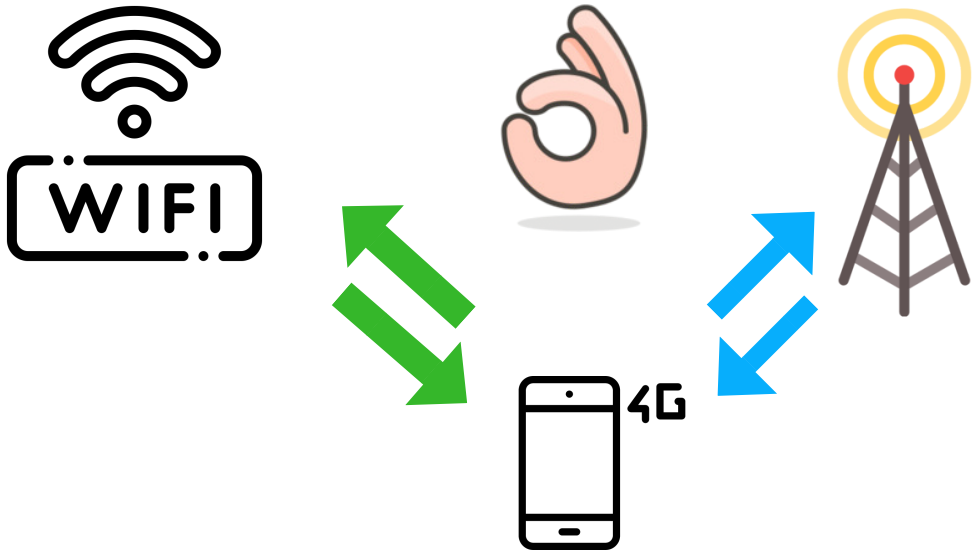
4G的TDD频段：上行2575-2635MHz

校园无线网（WIFI）

2.4G的频段：2400-2483.5MHz

5G的频段：5725-5850MHz

从上面可以看出，WIFI和手机信号不在同一频段，故是不会干扰手机信号的。



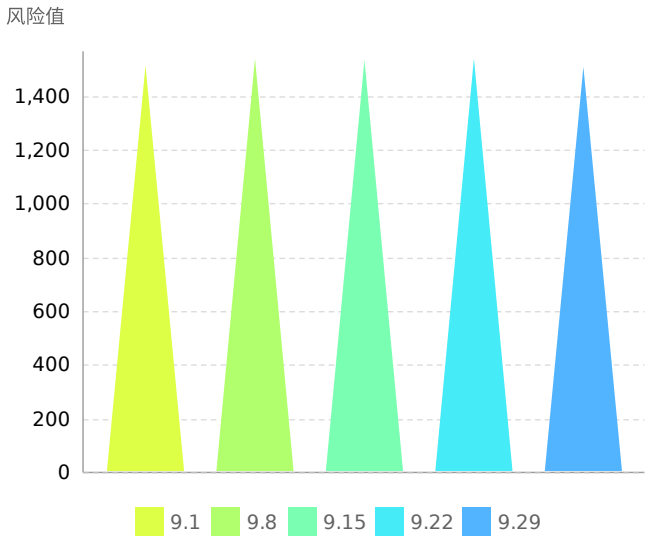
校园网络安全趋势

本网络安全态势分布图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9月1日-30日。

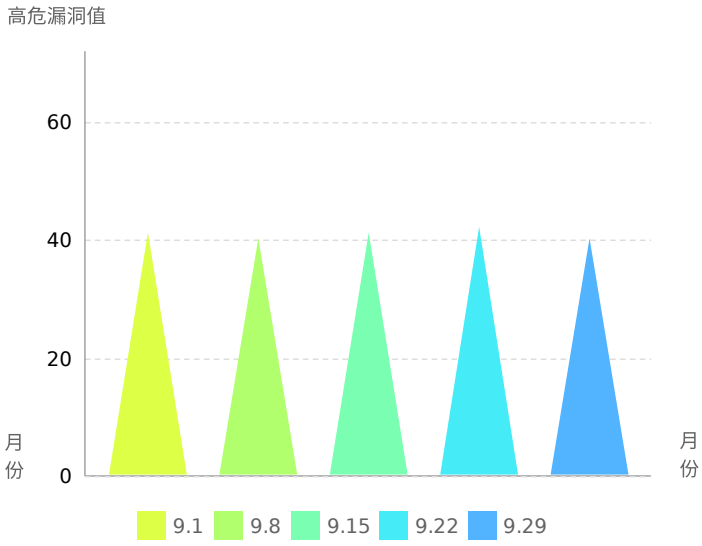
通过常态化安全监测等治理手段，我校9月网络安全状况整体评价为良，风险值较上月有所下降。

2019年9月网络安全态势分布图

风险值趋势



高危漏洞趋势



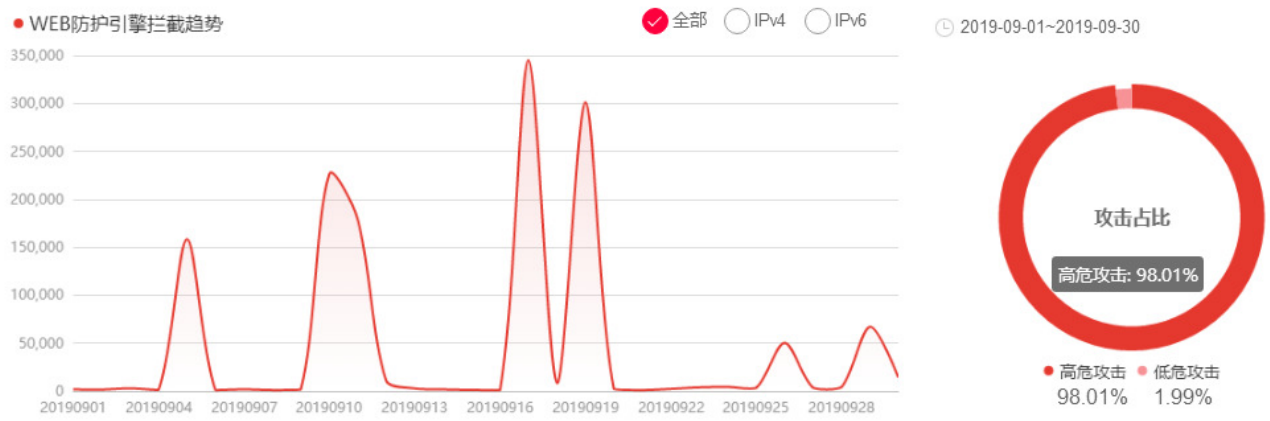
9月份重要信息系统（网站）基本情况

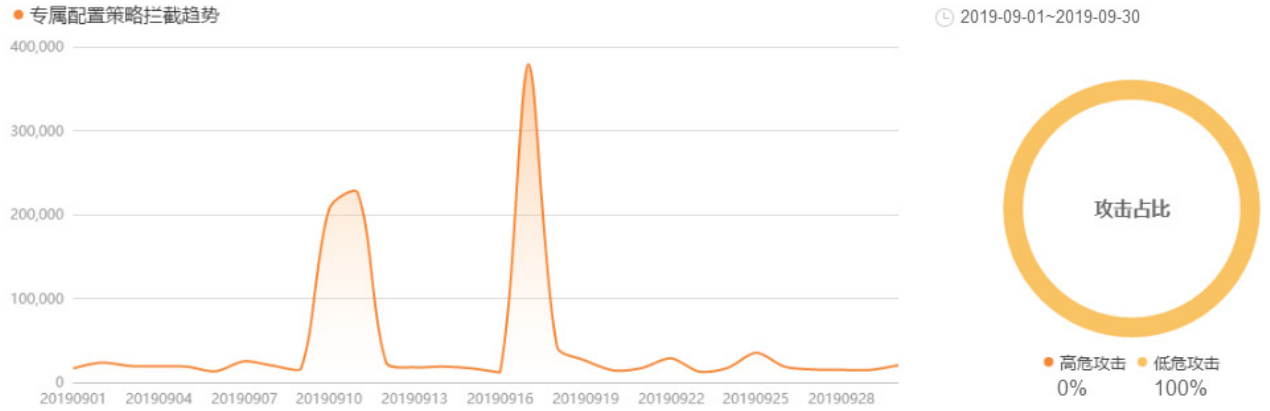
总请求数	总流量	搜索引擎	Alexa 全球排名
32,558,540次	3.40 TB	792,840次	264210

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9月1日-30日。

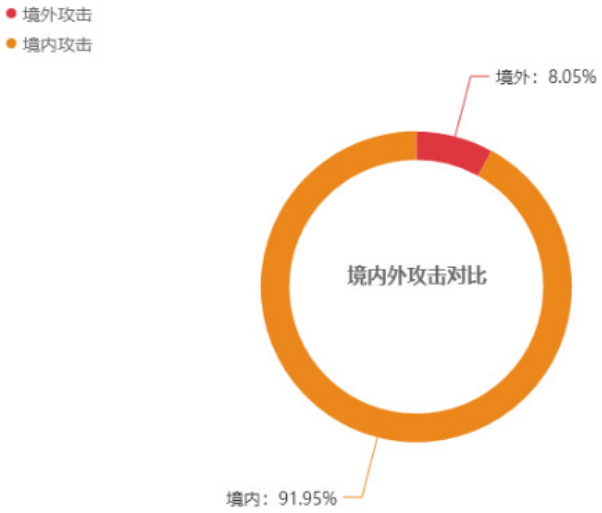
2019年9月1日-9月30日攻击拦截态势和网络攻击态势分布





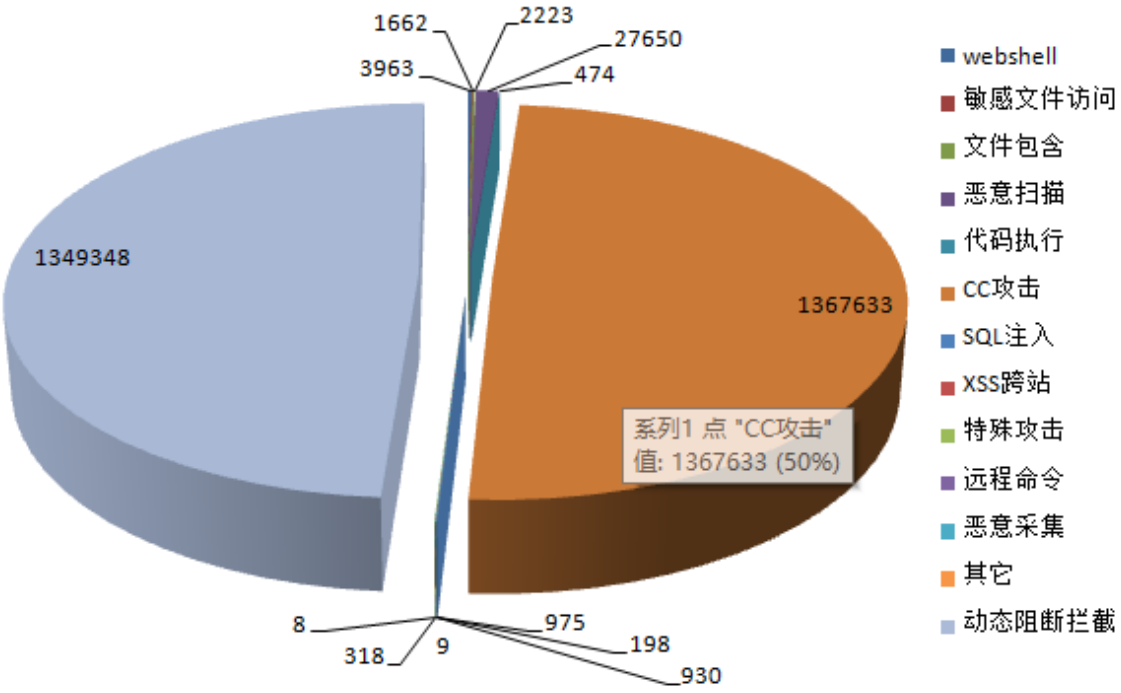
攻击趋势对比：通过本时段和上月时段的攻击趋势对比，攻击峰值（WEB应用攻击次数）共42381次，出现时间2019-08-10；对比峰值（WEB应用攻击次数）380374次，出现时间2019-09-17。

2019年9月1日-9月30日网站遭受黑客攻击分布图



境外攻击分布来源Top10

国家名称	攻击次数
美国	10907
德国	3532
保加利亚	2560
新加坡	1842
罗马尼亚	1579
南非	1546
韩国	1179
日本	1008
欧洲地区	641
菲律宾	485



本月共发生各类安全攻击2755391次，黑客攻击占总请求数的比率为8.12%，其中敏感文件访问1,662次、Webshell攻击3,963次、文件包含攻击2,223次、恶意扫描27,650次、代码执行474次、CC攻击1367,633次、SQL注入975次、XSS跨站攻击198次、特殊攻击930次、远程命令9次，恶意信息采集318次，其它8次，动态阻断拦截134,9438次。

美国中央情报局网络武器库分析与披露

2017年3月7日，维基解密首次在其网站对外曝光了美国中央情报局（CIA）相关资料，代号为Vault7，并且从当月直至9月7日每周都会对外披露其中一个项目的相关资料内容。

(奇安信威胁情报中心)

经奇安信对历史曝光的CIA网络武器及相关资料进行研究，发现这些网络武器曾用于攻击中国的目标人员和机构，其主要发生在2012年到2017年，目标可能涉及国内的航空行业。

网络武器

Athena（雅典娜）项目

Athena（雅典娜）项目是维基解密于2017年5月19日披露的，其用于在Windows系统上提供远程信标和程序加载的木马程序，从其功能介绍也可以推断出其更可能用于获取到攻击立足时，向目标主机植入的攻击模块，并用于加载和执行下阶段载荷。

控制指令

指令	功能
cmd_at	该指令用于计划任务相关的设置。
cmd_idlewatch	该指令主要通过GetLastInputInfo监控机器设备的活动情况
cmd_wincontrol	通过postMessage向指定gui发送消息，结合SendInput鼠标左键的操作，再配合一开始设置的隐藏桌面，以实现对用户机器上任意GUI应用的控制。
cmd_catInstall	该指令主要通过DCOM loader设置IPC$,ADMIN$共享的方式以实现在局域网的传播。

Fluxwire Node

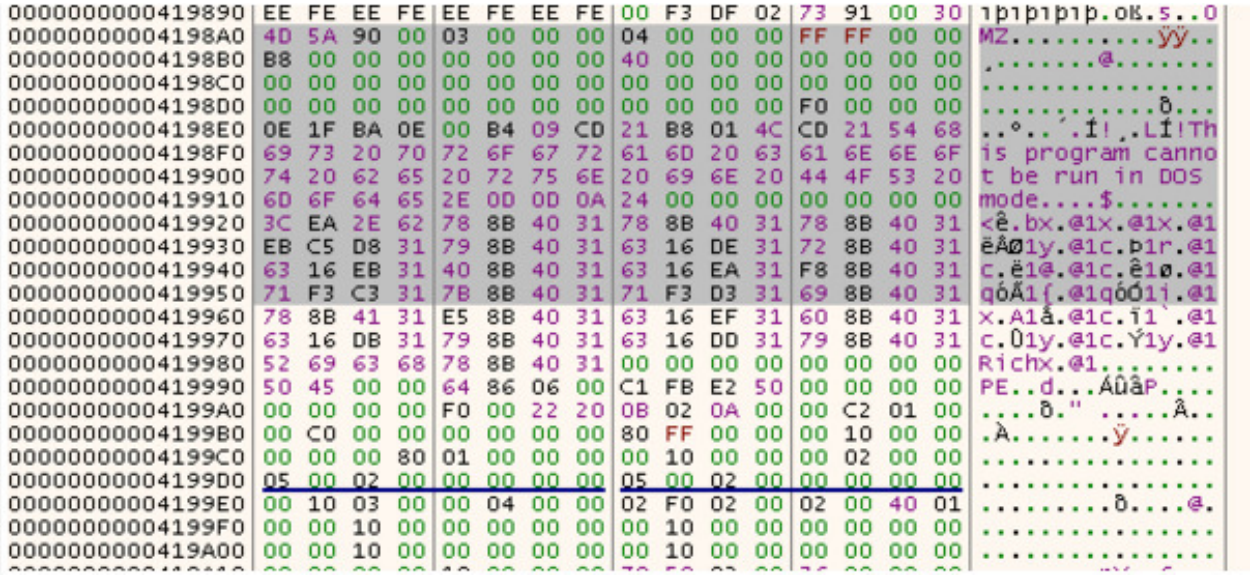
Fluxwire是CIA为了实现mesh networking而创建的项目，在泄露的文档中包括了一份关于Fluxwire的Linux版本控制端的介绍和使用手册，其确实是支持在内网下做更多模块下发，并且有的还支持命名管道的通信方式。

1.3 Supported Platforms and Architectures

Platform	x86	x64	PPC	MIPS	ARM	Sparc
Microsoft Windows	✔	✔			✔	
Linux	✔	✔	✔	✔	✔	✔
Mac OS X	✔	✔				
FreeBSD	✔					
OpenBSD						
NetBSD						
Solaris	✔					✔
AIX			✔			
SCO						

Gray Lambert

它是一个“NOBUS”后门程序，其复杂性在于能够通过广播、多播和单播命令在一个网络中嗅探多个受害者，从而允许操作者在多个受感染机器的网络中精确的发起攻击活动。



White Lambert

该样本为一个dll，其主要功能在DllMain中，该样本最终加载一个驱动，以确保其能正确加载起来，再加载之后的恶意驱动。加载之后首先同样是通过和之前一致的算法在配合RtlDecompressBufferat解压出最终的驱动，并寻址到入口并调用。

指令	含义
Copy	拷贝文件
Move	移动文件
Rename	修改文件名
Info	获取系统信息
Exit	设置退出标记
Close	同上
Quit	同上
Uninstall	卸载该驱动
Ndisls	列举自有协议信息
Dir	列目录
Ls	同上
Pwd	获取当前目录
Cd	切换目录
touch	创建文件

Backdoor.Trojan.LH1;

其主体逻辑是通过创建线程执行。通过命令导出宿主机的证书和私钥信息，然后获取主机信息，包括Mac地址，计算机名，以及当前用户。并生成用户UUID，该UUID会作为标识并用于后续HTTPS通信头部的X-MV-Host字段。

控制命令	功能描述
	初始行为，获取指令
get-scanner	获取扫描模块
run-scanner	运行扫描模块，并回传扫描结果
回传扫描结果	
exfil-file	压缩并回传文件
上传文件	
destroy-agent	销毁

Green Lambert;

Green Lambert为可执行文件，并且与LP（Listening Post）通信。其主要功能用于和远端的LP进行连接设置，同时具备浏览器相关凭据窃取及模块加载的功能。

函数名	功能
InitFunc_0	获取版本信息
InitFunc_1	通过/etc/init.d和/etc/rc.d写入ConfigInitdFile维持持久化
InitFunc_2	通过写入多种shell的配置文件维持持久化
InitFunc_3	通过写入XSession相关配置文件维持持久化
InitFunc_4	从代理URL中解析网络代理
InitFunc_5	URL相关解析
InitFunc_6	常量赋值
InitFunc_7	生成UUID
InitFunc_8	从系统环境变量获取代理配置

Stolen Goods;

Stolen Goods是CIA用来实现持久性的一个项目，其用于持久化Grasshopper安装器和Shellterm的shellcode注入程序。

```
// 动态获取API
signed int sub_100040D0()
{
  HMODULE v0; // eax

  v0 = LoadLibraryW(L"ntdll.dll");
  hLibModule = v0;
  if ( !v0 )
    return -1;
  ZwClose = (int (__stdcall *)(_DWORD))GetProcAddress(v0, "ZwClose");
  if ( !ZwClose )
  {
LABEL_8:
    FreeLibrary(hLibModule);
    return -1;
  }
  ZwOpenFile = (int (__stdcall *)(_DWORD, _DWORD, _DWORD, _DWORD, _DWORD, _DWORD))GetProcAddress(
                                                                                    hLibModule,
                                                                                    "ZwOpenFile");
  if ( !ZwOpenFile )
    goto LABEL_14;
  ZwWriteFile = (int)GetProcAddress(hLibModule, "ZwWriteFile");
  if ( !ZwWriteFile )
  {
    FreeLibrary(hLibModule);
    return -1;
  }
  ZwReadFile = (int (__stdcall *)(_DWORD, _DWORD, _DWORD, _DWORD, _DWORD, _DWORD, _DWORD, _DWORD, _DWORD))Get
  if ( !ZwReadFile )
    goto LABEL_8;
  RtlInitUnicodeString = (int (__stdcall *)(_DWORD, _DWORD))GetProcAddress(hLibModule, "RtlInitUnicodeString"
  if ( RtlInitUnicodeString )
    return 0;
LABEL_14:
  FreeLibrary(hLibModule);
  return -1;
}
```

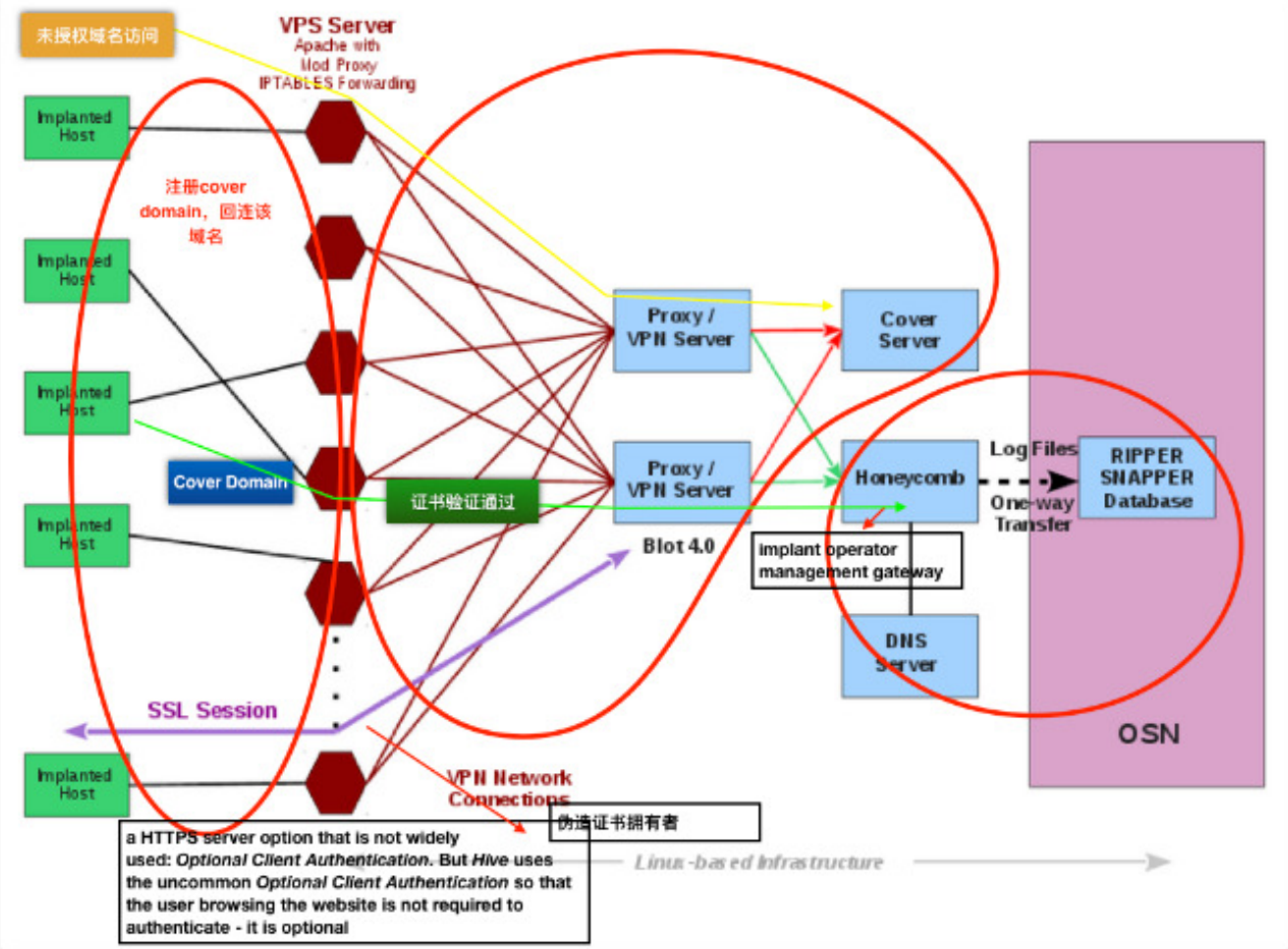
控制基础设施

从维基解密披露文档我们得知CIA用于控制基础设施部署的项目名为HIVE，其由EDB部门所开发。HIVE分为3个部分，implant，LP和CC。其中Blot为隐藏的服务器。Honeycomb是植入物的行动管理网关。其通信逻辑为：

1.选择一个看似正常的域名（cover domain）和商用VPS服务，其上安装组件。VPS服务器连接Blot；

2. 正常用户访问时，由于开启了可选验证标记（其利用了一个特殊的HTTPS服务选项“Optional Client Authentication”），则不验证并定向到Cover Server；

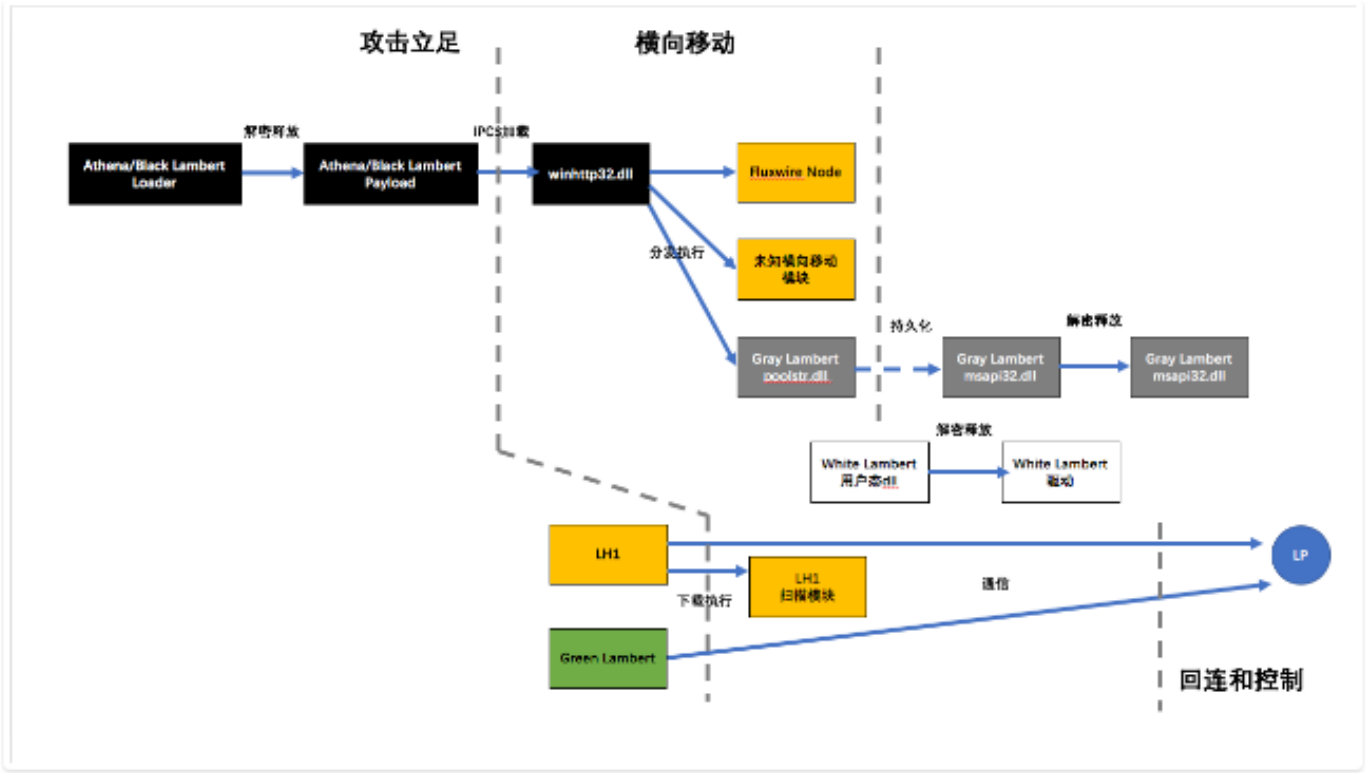
3. 植入物访问时，会访问Honeycomb。



攻击链

奇安信结合上述分析按照攻击链绘制了相关网络武器的利用过程和关系，并对其TTP进行横向对比。

Execution	Credential Access	Lateral Movement	Persistence	Exfiltrate/Monitor	Command and Control	Evasion
Athena						
(Black Lambert)	Y		Y	Y		
Fluxwire Node	Y					Y
Gray Lambert	Y			Y	Y	
White Lambert	Y				Y	
LH1	Y				Y	Y
Green Lambert	Y	Y		Y	Y	Y
Stolen Goods	Y			Y		



1 Microsoft Windows和Windows Server远程执行代码漏洞

Microsoft Windows中存在远程代码执行漏洞，该漏洞源于主机系统上Hyper-V网络交换机未能正确验证虚拟机操作系统上认证用户的输入，攻击者可利用该漏洞在主机操作系统上执行任意代码。

解决方案：
厂商已发布了漏洞修复程序，请及时关注更新：
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0720

2 Linux kernel内存泄露漏洞（CNVD-2019-32349）

Linux kernel 5.1.13之前版本中的drivers/scsi/libsas/sas_expander.c文件存在内存泄露漏洞。攻击者可利用该漏洞造成拒绝服务。

解决方案：
厂商已发布了漏洞修复程序，请及时关注更新：
https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=3b0541791453fbe7f42867e310e0c9eb6295364d

3 Coremail论客客户端存在远程命令执行漏洞

Coremail论客客户端存在远程命令执行漏洞。攻击者可利用漏洞执行命令，获得服务器权限。

解决方案：
厂商已提供漏洞修补方案，请关注厂商主页及时更新：
https://lunkr.cn/dl?p=mail

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 李燕
编　辑：李博鑫 王心成 李宏伟
王力 李蒙 赵阳
殷仕刚 张晋 安洋
张爱玲 赵红毅
审　核：张晓宇

扫码关注

西安理工大学微信企业号