西安理工大学
XI'AN UNIVERSITY OF TECHNOLOGY

网络信息管理中心

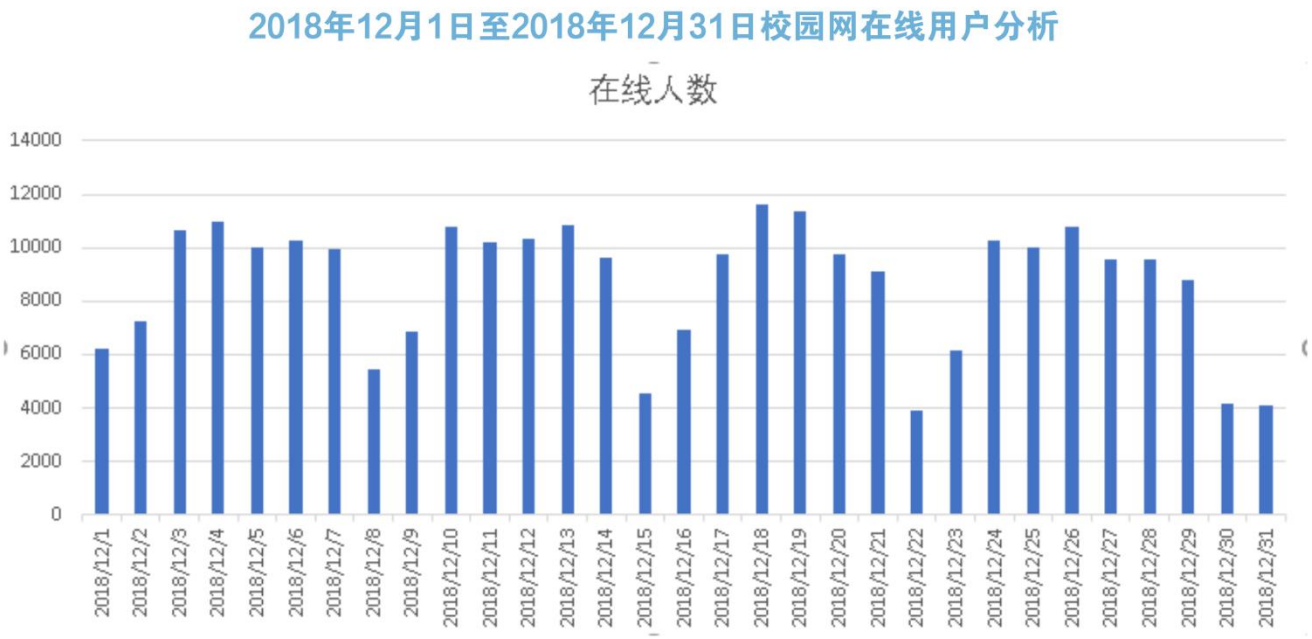
信息化工作简报

12月

2018

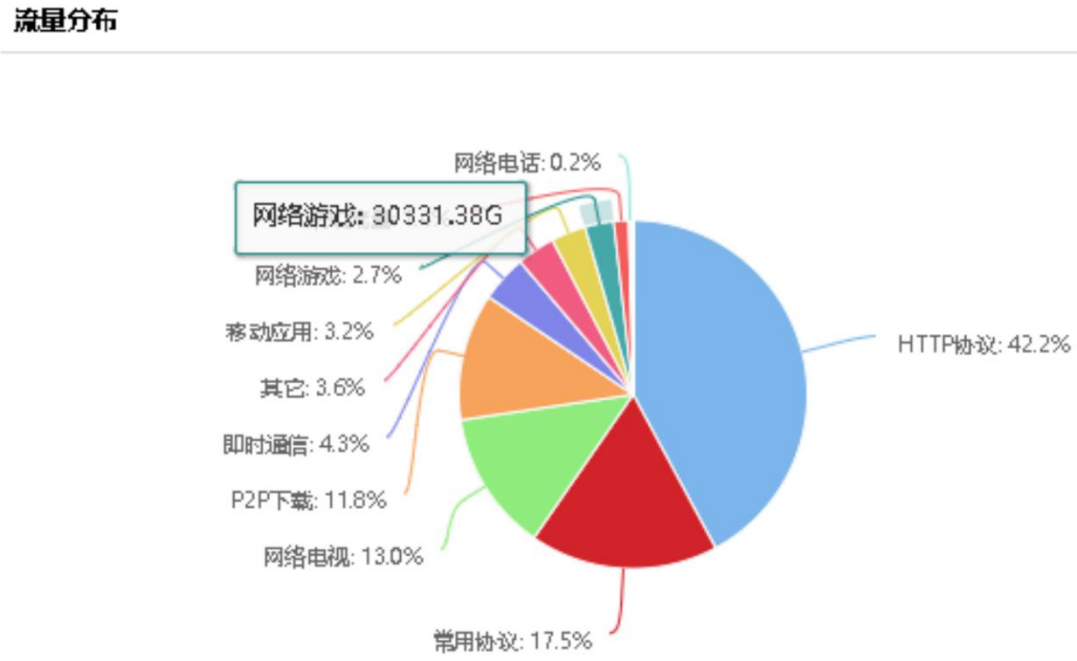
校园网用户统计、流量分布

12月，校园网整体运行正常，日均在线用户8705人，其中无线用户日均在线6270人。



校园网出口峰值使用带宽8.9G，2018年12月，校园网总下载流量达760T，上传流量共计200T。

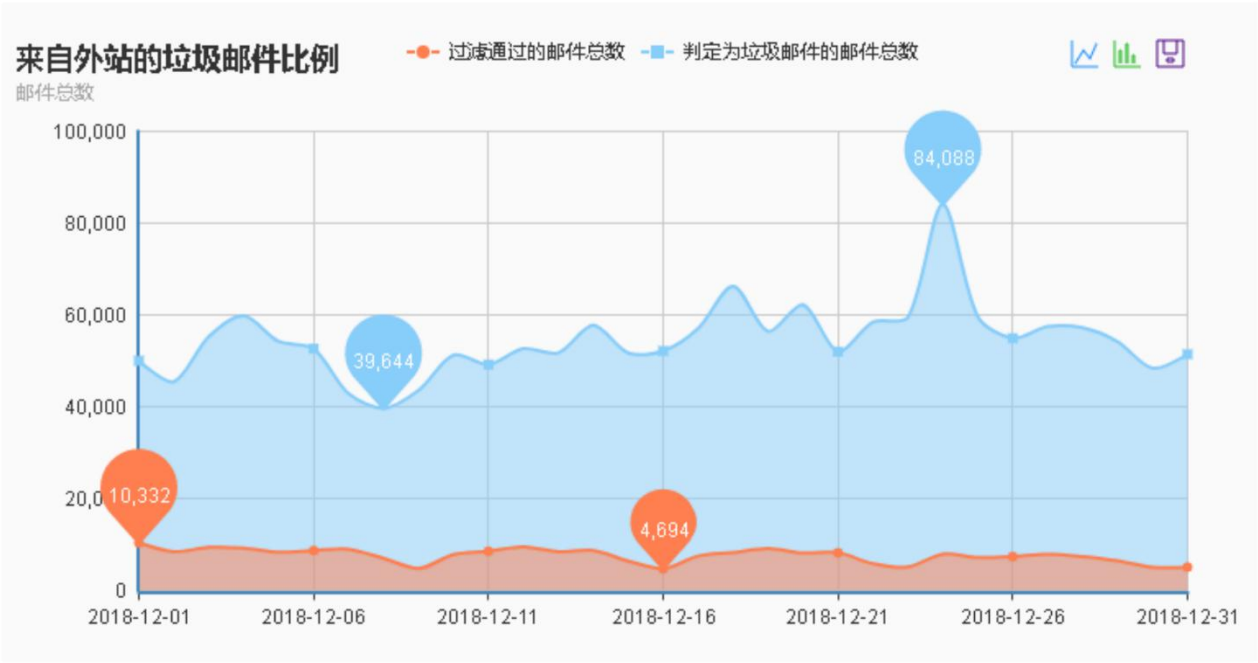
其中，HTTP日常访问产生流量占比42.2%位居首位，常用软件流量占比17.5%，迅雷等P2P下载流量及网络电视流量分别占比约11.8%和13%。



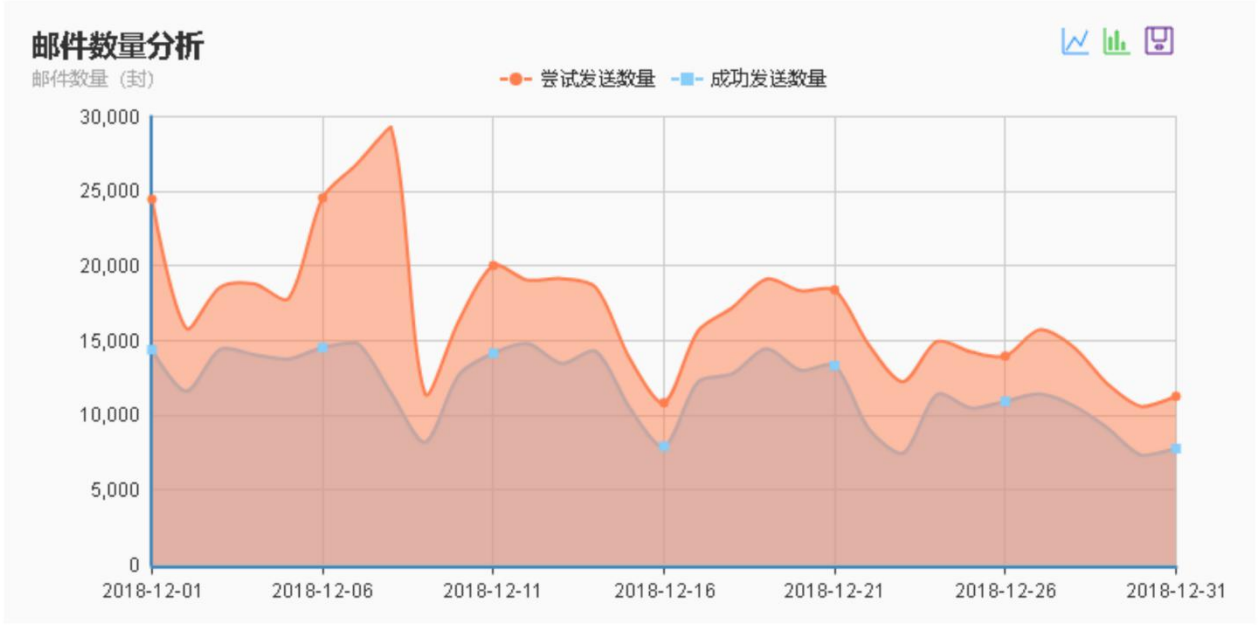
校园邮件系统运行数据

2018年12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

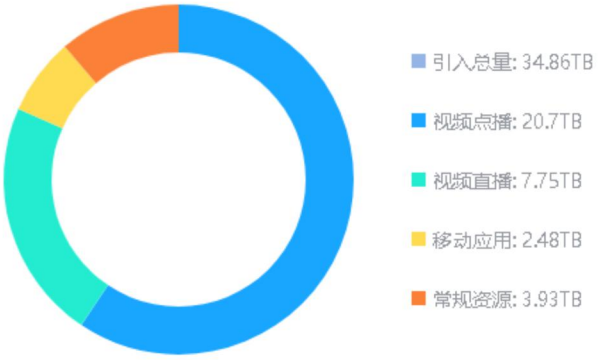


校园邮件系统发件数据统计



校园网应用大数据

校园网出口内容加速资源引入情况



CDS引入了240个内容方，共计 34.86TB 的内容资源。
引入视频点播资源 20.7TB，相当于18277小时的1080P高清视频。
引入视频直播资源 7.75TB，相当于7343小时的超清直播。
引入移动应用资源 2.48TB，相当于991个iOS 10.3升级包。
引入常规资源 3.93TB，相当于10544937张高清图片。

内容方排行TOP15

1.哔哩哔哩 9.64TB	2.网宿 4.49TB	3.腾讯 2.65TB	4.爱奇艺 2.52TB	5.斗鱼 1.91TB
6.新浪 1.40TB	7.未归类 1.33TB	8.安卓APP 1.13TB	9.苹果APP 1015.03GB	10.虎牙 958.22GB
11.百度 820.85GB	12.优酷 786.53GB	13.网易 774.27GB	14.压缩文件 689.61GB	15.8686 512.98GB

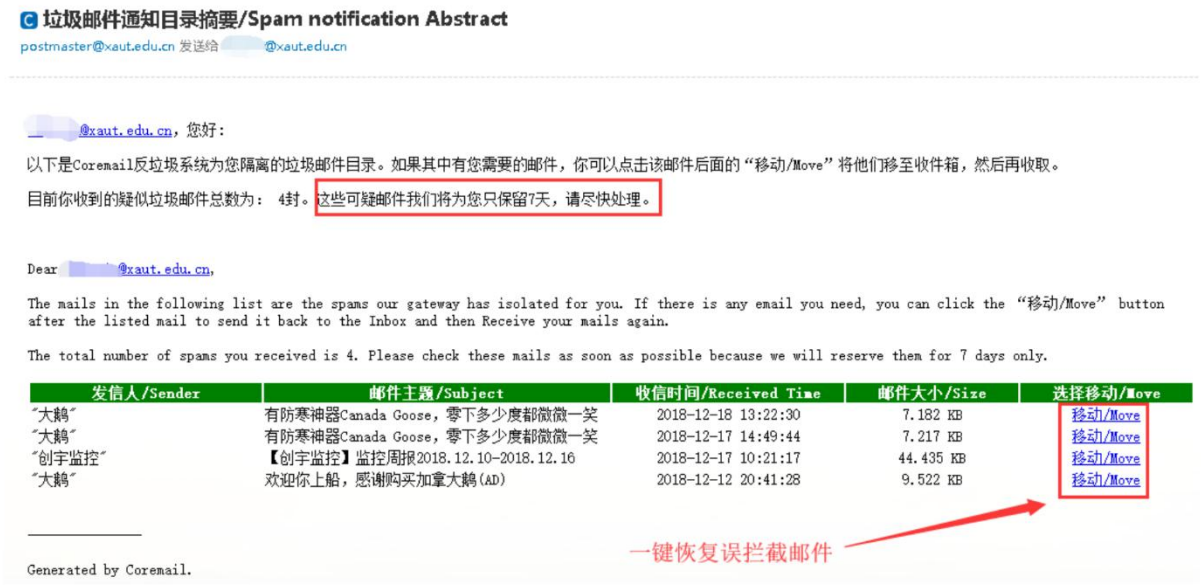
最受欢迎榜单

关于校园邮件系统小窍门

反垃圾邮件通知信

我校邮件系统支持垃圾邮件拦截提醒功能，为了防止少数邮件被邮件网关误拦截，造成重要信件未正常收到，影响日常工作，建议用户手动开启该功能。

启动功能后，用户可以根据需求设置提醒邮件的发送频率，配置完毕后即可定期接收提醒邮件。在提醒邮件中，用户可以一键恢复误拦截邮件至收件箱。



关于校园邮件系统小窍门

日常钓鱼邮件防范

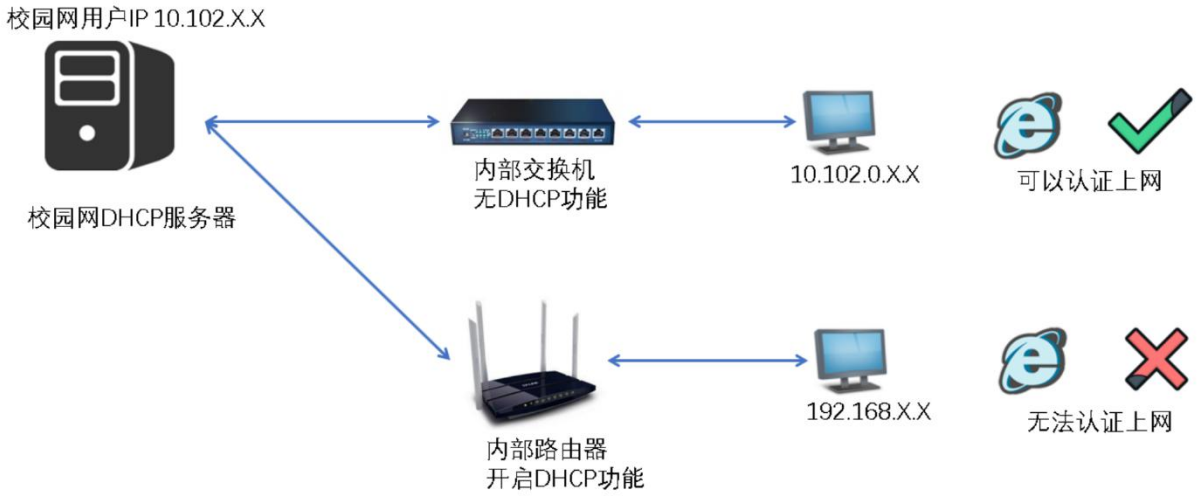
钓鱼邮件指利用伪装的电邮，欺骗收件人将账号、口令等信息回复给指定的接收者；或引导收件人连接到特制的网页，这些网页通常会伪装成和真实网站一样，如银行或理财的网页，令登录者信以为真，输入信用卡或银行卡号码、账户名称及密码等而被盗取。

据统计，我校目前大部分收到钓鱼邮件主要以冒充管理员发系统通知信为主，主要为了骗取我校师生邮箱账户密码，经常以邮箱空间已满或邮件账户出现异常为由，要求用户及时登录某个激活页面。黑客骗取用户名密码后便使用其对外发送大量广告邮件，致使我校域名被互联网邮件监测组织拉黑，严重影响正常对外交流办公。

我校师生请以知行网通知为准，请勿轻信可以邮件，如有疑问请直接电话咨询网络信息管理中心。

校园网常见故障--路由器错误配置

目前我校70%以上办公室、教研室使用无线路由实现局域网分线功能，多数用户未对路由器进行正常的配置便会造成网络故障。主要原因在于路由器默认开启代理模式，用户电脑无法正常获取到校园网的用户段IP，导致认证服务器拒绝用户认证信息，从而无法上网。



校园网接入路由器（包括无线及有线路由器）的正确配置方法：

1.用户登录路由器管理后台，关闭路由器自身DHCP功能，确认保存配置后手动重启路由器。

2.将房间内主线及用户电脑接入线缆同时接到路由器后方具有LAN标识的端口。

3.用户手动禁用网卡，再次启用后重新获取网络IP地址，确认网卡获取到非169开头或192开头地址，便可尝试认证上网。

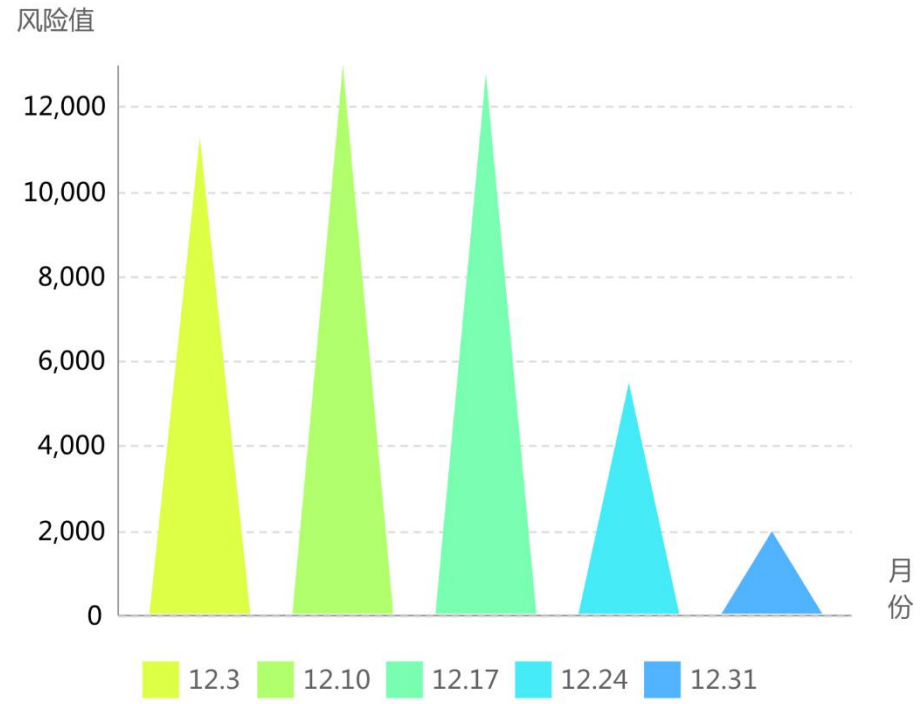
校园网络安全趋势

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。

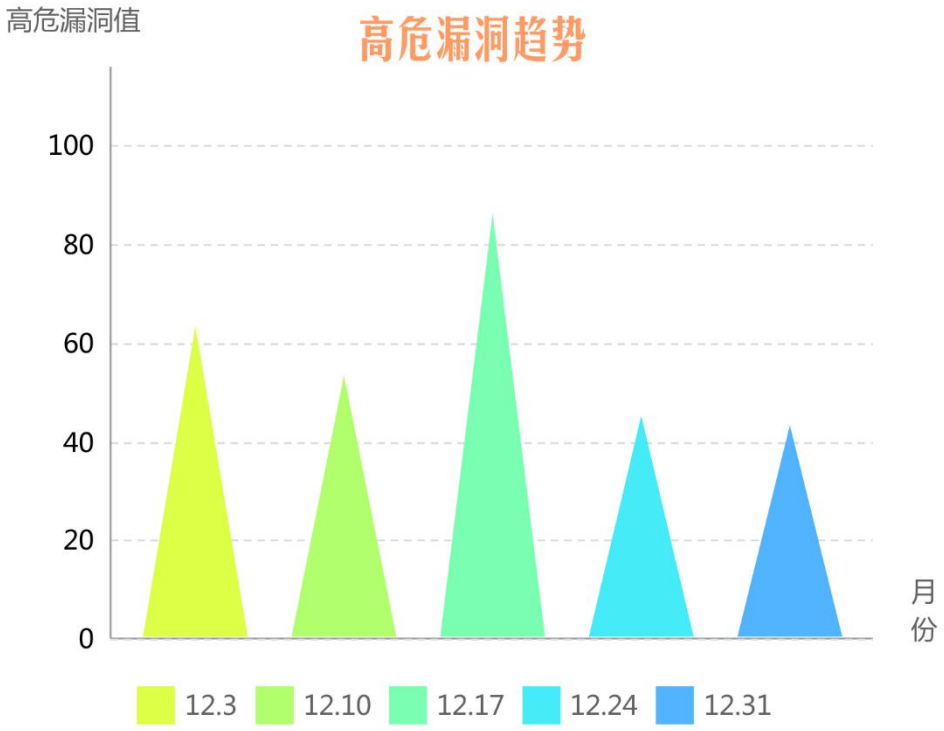
评估范围为：2018年12月1日-12月31日；通过常态化安全监测等一系列行动治理，我校本月网络安全状况整体评价为良，风险情况总体呈明显下降趋势。

2018年11月1日-11月30日网络安全态势分布图

风险值趋势



高危漏洞趋势



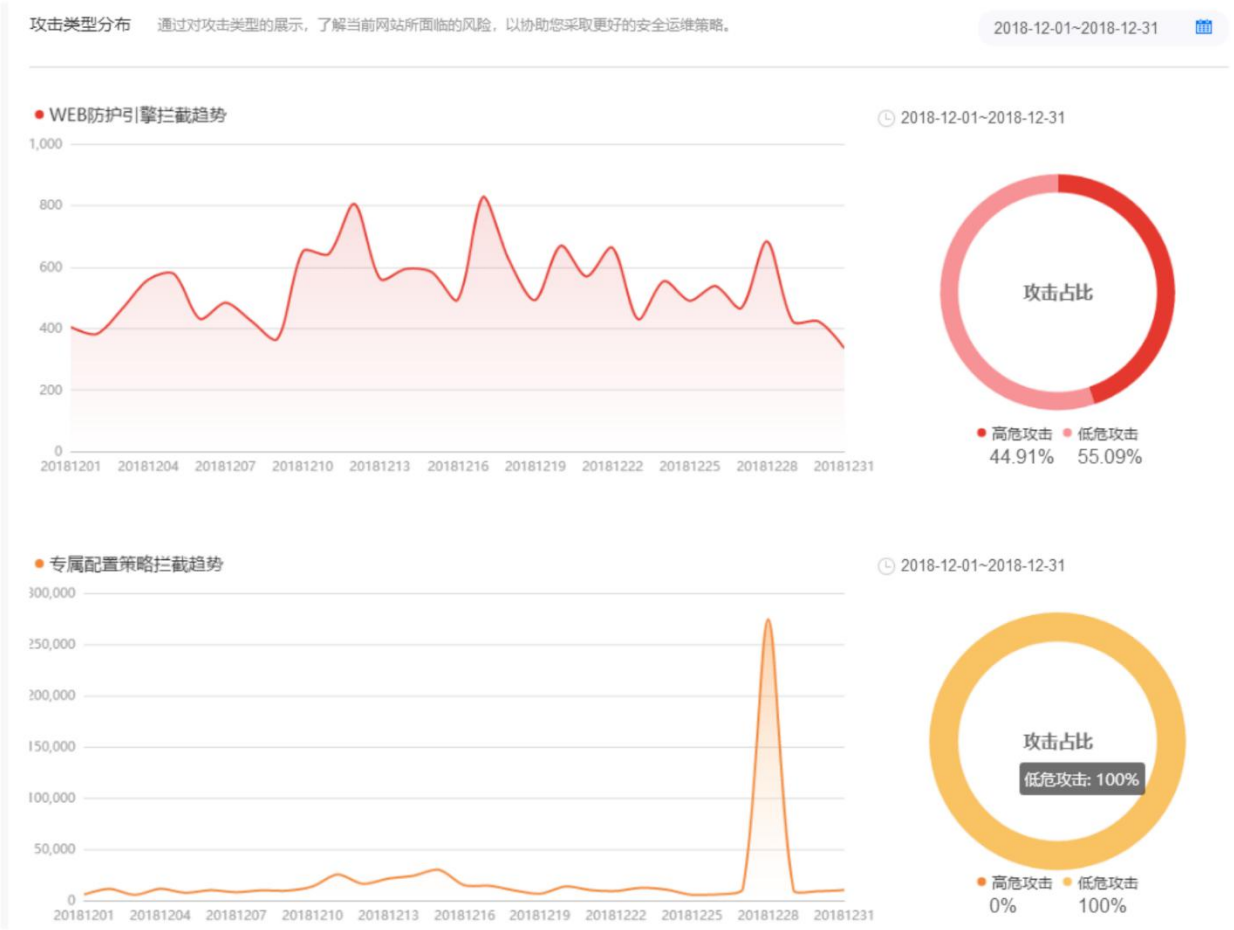
校园网络安全趋势

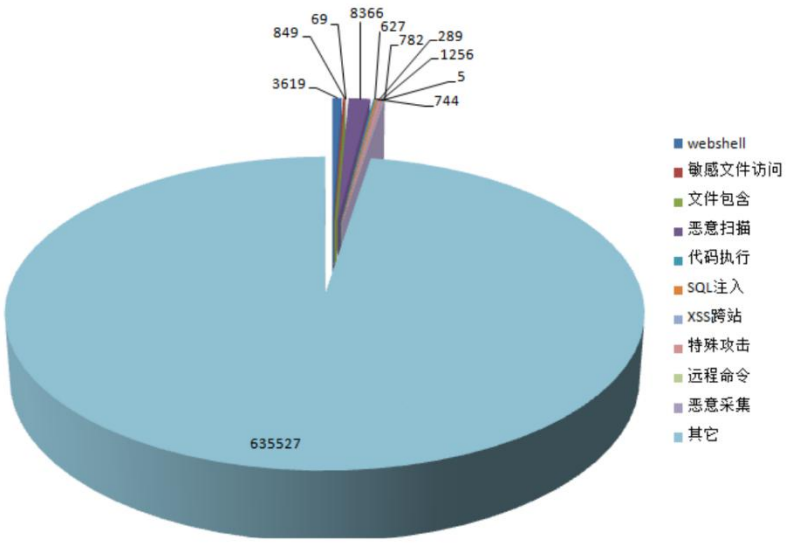
本周期统计以网络中心监测的数据作为主要依据，对我校重要信息系统（网站）面临的各类安全威胁及基本情况进行总体态势分析；评估范围为：2018年12月1日-12月31日。

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
21177362次	1606.64GB	320,633次	75195

2018年11月1日-11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652133次，黑客攻击占总请求数的比率为3.08%，其中Webshell攻击3619次、敏感文件访问849次、文件包含攻击69次、恶意扫描8366次、代码执行627次、SQL注入744次、XSS跨站攻击 289次、特殊攻击1256次、远程命令5次、恶意信息采集782次，其它635527次。

潜伏在身边的黑客

2018年全球高级持续性威胁盘点

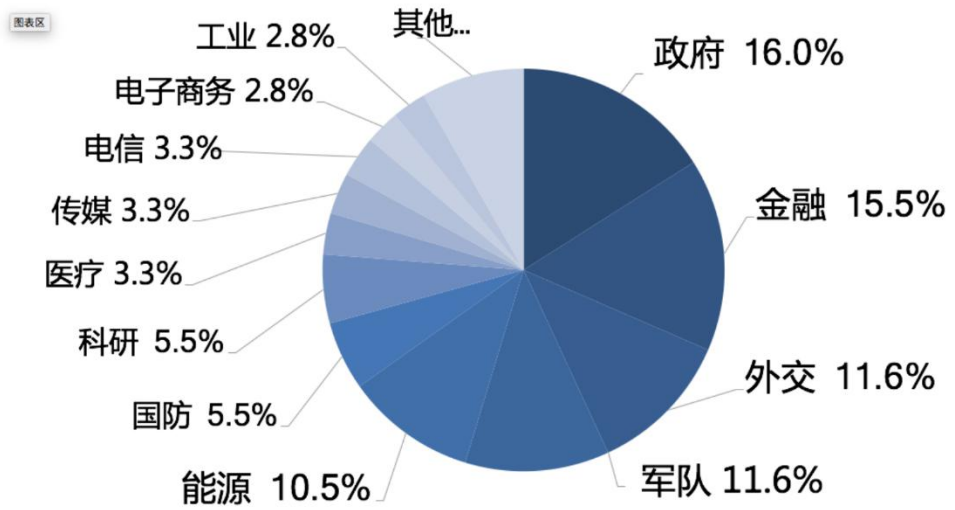
(360威胁情报中心)

APT组织，通常具有国家或情报机构背景，或者专门实施网络间谍活动，其攻击动机主要是长久性的情报刺探、收集和监控，也会实施如牟利和破坏为意图的攻击威胁。APT组织主要攻击的目标包括政府、军队、外交、国防外，也覆盖科研、能源以及国家基础设施性质的行业和产业。

近年来，数个活跃的网络犯罪组织也呈现出明确的组织化特点，并且使用其自身特色的攻击工具和战术技术。网络犯罪组织对于如金融、银行、电子商务、餐饮零售等行业带来了巨大的资金损失和业务安全风险。

受害目标的行业与地域

2018年公开高级威胁事件报告涉及行业分布情况

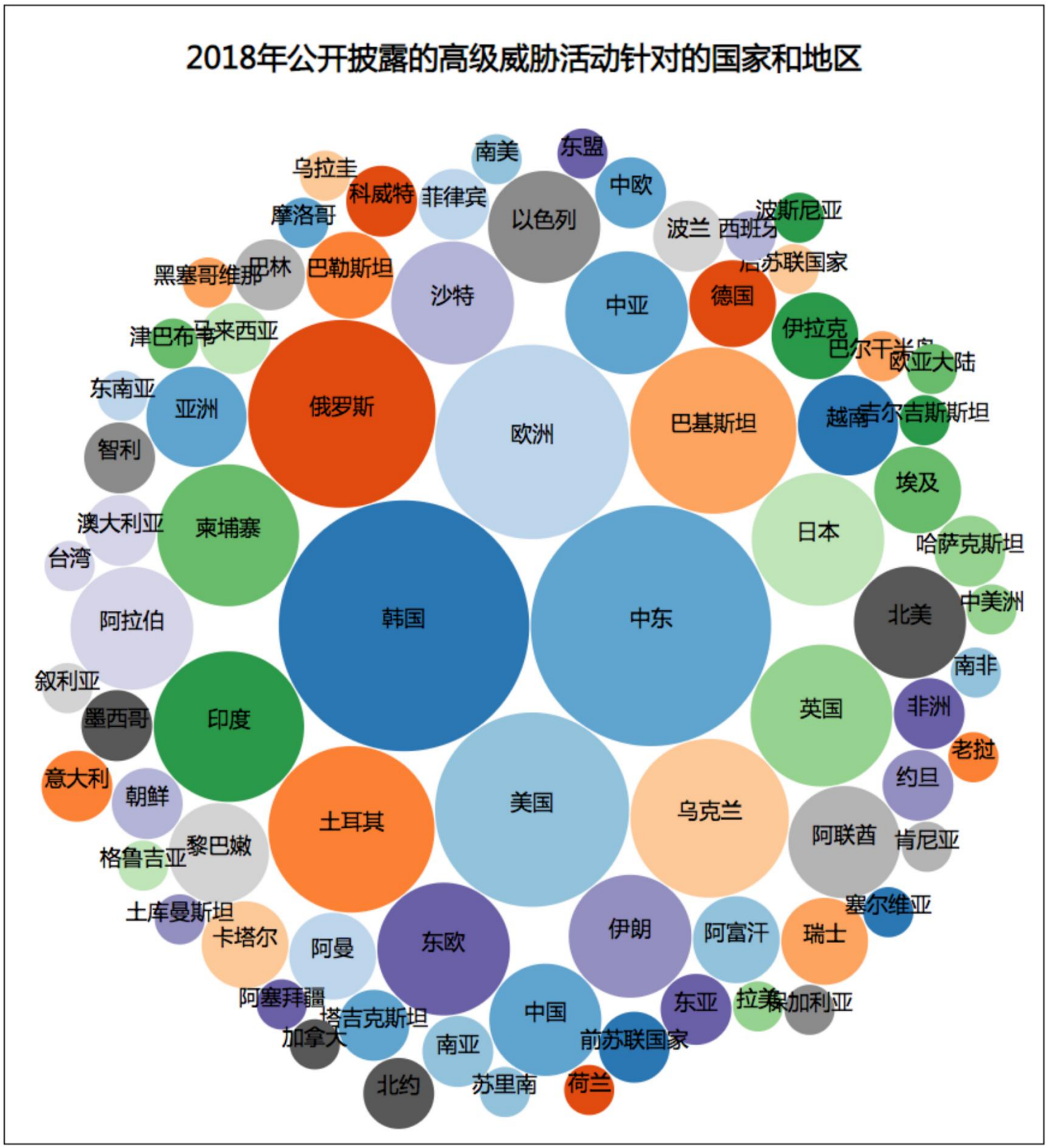


从公开披露的高级威胁活动中涉及目标行业情况来看，政府、外交、军队、国防依然是 APT 攻击者的主要目标，这也与 APT 攻击的主要意图和目的有关，值得注意的是国家的基础性行业也正面临着攻击风险，如能源、电力、工业、医疗等。

而金融行业主要面临一些成熟的网络犯罪团伙的攻击威胁，如MageCart、Cobalt Group等等，其组织化的成员结构和成熟的攻击工具实现对目标行业的规模化攻击，这与过去的普通黑客攻击是完全不同的。除了针对金融、银行外，电子商务、在线零售等也是其攻击目标。

而从下图中高级威胁活动涉及目标的国家和地域分布情况（摘录自公开报告中提到的受害目标所属国家或地域），可以看到高级威胁攻击活动几乎覆盖了全球绝大部分国家和区域。经对公开报告中命名的攻击行动名称、攻击者名称，及同一背景来源进行归类处理后，总共涉及109个命名的威胁来源命名。

潜伏在身边的黑客


2018年公开披露的高级威胁活动针对的国家和地区
南美
东盟
乌拉圭
中欧
科威特
菲律宾
以色列
摩洛哥
波兰
西班牙
波斯尼亚
巴林
巴勒斯坦
黑塞哥维那
沙特
中亚
德国
苏联国家
伊拉克
津巴布韦
马来西亚
巴尔干半岛
欧亚大陆
东南亚
亚洲
俄罗斯
欧洲
巴基斯坦
越南
吉尔吉斯斯坦
智利
埃及
澳大利亚
柬埔寨
日本
哈萨克斯坦
台湾
韩国
中东
北美
中美洲
阿拉伯
南非
叙利亚
印度
英国
非洲
墨西哥
老挝
意大利
朝鲜
美国
乌克兰
约旦
土耳其
阿联酋
肯尼亚
黎巴嫩
格鲁吉亚
塞尔维亚
土库曼斯坦
卡塔尔
阿曼
东欧
伊朗
阿富汗
瑞士
阿塞拜疆
塔吉克斯坦
中国
东亚
拉美
保加利亚
加拿大
南亚
前苏联国家
北约
苏里南
荷兰

潜伏在身边的黑客

针对中国境内的APT组织和威胁

一、海莲花（APT-C-00）

“海莲花”APT 组织是一个长期针对我国政府、科研院所、海事机构、海域建设、航运企业等领域的 APT 攻击组织，该组织在过去不仅频繁对我国境内实施 APT 攻击，也针对东南亚周边国家实施攻击，包括柬埔寨，越南等。

二、毒云藤（APT-C-01）

毒云藤（APT-C-01），也被国内其他安全厂商称为穷奇、绿斑。该组织从2007年开始至今，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。

该组织主要使用鱼叉攻击投放漏洞文档或二进制可执行文件；使用的恶意木马包括Poison Ivy，ZxShell，XRAT等，并使用动态域名，云盘，第三方博客作为其控制回传的基础设施。

三、蓝宝菇（APT-C-12）

蓝宝菇（APT-C-12）组织最早从2011年开始持续至今，对我国政府、军工、科研、金融等重点单位和部门进行了持续的网络间谍活动。该组织主要关注核工业和科研等相关信息。被攻击目标主要集中在中国大陆境内。

蓝宝菇组织也主要使用鱼叉邮件实施攻击，其投放的文件主要是RLO伪装成文档的可执行文件或LNK格式文件。

潜伏在身边的黑客

2018年全球十大APT攻击事件

1. 韩国平昌冬奥会APT攻击事件

危害程度 ★★★攻击频度 ★★ 攻击技术 ★★★
事件时间：平昌奥运会期间，首次活动于2017年12月22日
攻击组织：Hades
受害目标：韩国平昌奥运会举办方
相关攻击武器：Olympic Destroyer
相关漏洞：无
攻击入口：鱼叉邮件攻击

2. 针对乌克兰IOT设备的恶意代码攻击事件

危害程度 ★★★★★攻击频度 ★★★★ 攻击技术 ★★★★
事件时间：最早从2016年开始，2018年5月首次披露
攻击组织：疑似APT28
受害目标：主要为乌克兰
相关攻击武器：VPNFilter
相关漏洞：针对IOT设备的多种漏洞
攻击入口：利用IOT设备漏洞远程获得初始控制权

3. APT28针对欧洲、北美地区的一系列定向攻击事件

危害程度 ★★★★攻击频度 ★★★★ 攻击技术 ★★★★★
事件时间：贯穿整个2018年
攻击组织：APT28
受害目标：北美、欧洲、前苏联国家的政府组织
相关攻击武器：Cannon、Zebrocy等
相关漏洞：Office文档模板注入、疑似Lojack软件缺陷或0day漏洞
攻击入口：鱼叉邮件、Office模板注入

4. 蓝宝菇APT组织针对中国的一系列定向攻击事件

危害程度 ★★★★攻击频度 ★★★ 攻击技术 ★★★
事件时间：2018年4月（首次攻击时间为2011年）
攻击组织： 蓝宝菇（BlueMushroom）
受害目标：中国政府、军工、科研、金融等重点单位和部门
相关攻击武器：PowerShell后门
相关漏洞：无
攻击入口：鱼叉邮件和水坑攻击

5. 海莲花APT组织针对我国和东南亚地区的定向攻击事件

危害程度 ★★★★攻击频度 ★★★★★ 攻击技术 ★★★
事件时间：2018年全年（首次攻击时间为2012年）
攻击组织：海莲花（OceanLotus）
受害目标：东南亚国家、中国及其相关科研院所、海事机构、航运企业等
相关攻击武器：Denis家族木马、Cobalt Strike、CACTUSTORCH框架木马
相关漏洞：微软Office漏洞、MikroTik路由器漏洞、永恒之蓝漏洞
攻击入口：鱼叉邮件和水坑攻击

潜伏在身边的黑客

2018年全球十大APT攻击事件

6. 蔓灵花组织针对中国、巴基斯坦的一系列定向攻击事件

危害程度 ★★★攻击频度 ★★★★ 攻击技术 ★★★
事件时间：2018年初
攻击组织： 蔓灵花（BITTER）
受害目标：中国、巴基斯坦
相关攻击武器：“蔓灵花”特有的后门程序
相关漏洞：InPage文字处理软件漏洞CVE-2017-12824、微软公式编辑器漏洞等
攻击入口：鱼叉邮件攻击

7. APT38针对全球范围金融机构的攻击事件

危害程度 ★★★★★攻击频度 ★★★★ 攻击技术 ★★★★
事件时间：最早于2014年，持续活跃至今
攻击组织：APT38
受害目标：金融机构，银行，ATM，SWIFT
相关攻击武器：多种自制恶意程序
相关漏洞：多种漏洞
攻击入口：鱼叉攻击，水坑攻击

8. 疑似DarkHotel APT组织利用多个IE 0day“双杀”漏洞的定向攻击事件

危害程度 ★★★攻击频度 ★★ 攻击技术 ★★★★
事件时间：首次发现于2018年5月
攻击组织：DarkHotel
受害目标：中国
相关攻击武器：劫持操作系统DLL文件（msfte.dll、NTWDBLIB.DLL）的插件式木马后门
相关漏洞：CVE-2018-8174、CVE-2018-8373等
攻击入口：鱼叉邮件攻击

9. 疑似APT33使用Shamoon V3针对中东地区能源企业的定向攻击事件

危害程度 ★★★★攻击频度 ★★ 攻击技术 ★★★
事件时间：2018年12月发现
攻击组织：疑似APT33
受害目标：中东和欧洲的石油和天然气公司
相关攻击武器：Shamoon V3
相关漏洞：无
攻击入口：鱼叉邮件攻击

10. Slingshot：一个复杂的网络间谍活动

危害程度 ★★★★攻击频度 ★★ 攻击技术 ★★★★★
事件时间：2012至2018年2月
攻击组织：疑似针对伊斯兰国和基地组织成员
受害目标：非洲和中东各国的路由器设备
相关攻击武器：自制的攻击武器
相关漏洞：CVE-2007-5633、CVE-2010-1592、CVE-2009-0824
攻击入口：可能通过Windows漏洞利用或已感染的Mikrotik路由器

重大漏洞预警

1 Microsoft Internet Explorer远程代码执行漏洞（CNVD-2018-26979）

Microsoft IE 9、10和11版本中存在远程代码执行漏洞，该漏洞源于程序未能正确的访问内存中的对象。远程攻击者可利用该漏洞在当前用户的上下文中执行任意代码，损坏内存。

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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8447

2 Google Android权限提升漏洞（CNVD-2018-26777）

Android8.1版本和9版本中的v4l2_slice_video_decode_accelerator.cc文件的V4L2SliceVideoDecodeAccelerator::Dequeue存在权限提升漏洞，该漏洞源于程序执行了错误的边界检测，攻击者可利用该漏洞提升权限（越界读取）。

解决方案：

厂商已发布了漏洞修复程序，请及时关注更新：
https://source.android.com/security/bulletin/2018-12-01

3 Microsoft ChakraCore和Edge远程代码执行漏洞（CNVD-2018-26972）

Microsoft ChakraCore和Edge中存在远程代码执行漏洞。远程攻击者可利用该漏洞在当前用户的上下文中执行任意代码，损坏内存。

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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8467

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

2018