网络信息安全周报

【2018】第 16 期

党委宣传部
信息网络中心 编

2018 年 6 月 21 日

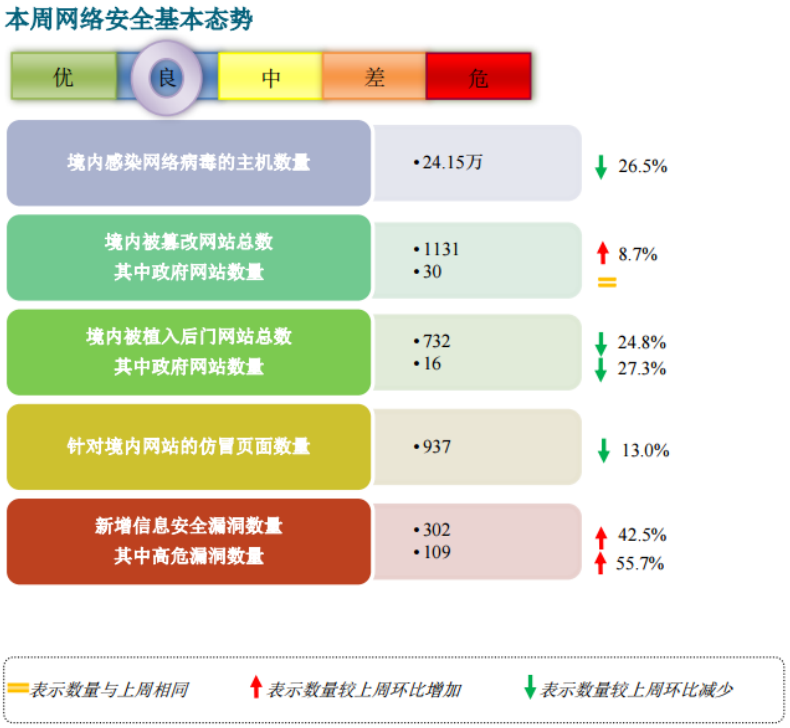
本期要目

- 【权威发布】全国网络安全信息与动态（2018 年 6 月 11 日—6 月 17 日）
- 【城院 IT】综合业务管理平台统计信息(2018 年 6 月 11 日—6 月 17 日)
- 【城院安全】网站群管理平台统计信息（2018 年 6 月 11 日—6 月 17 日）
- 【网络知识】手机 WiFi 总是断开连接又重连之间重复是怎么回事?如何解决?

全国网络安全信息与动态

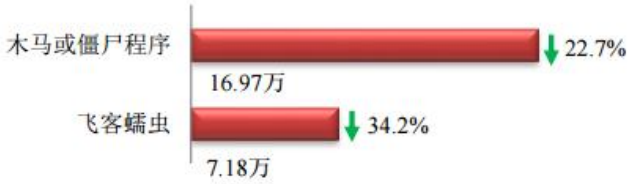
（2018 年 6 月 11 日—6 月 17 日）

根据国家互联网应急中心最新公告数据：



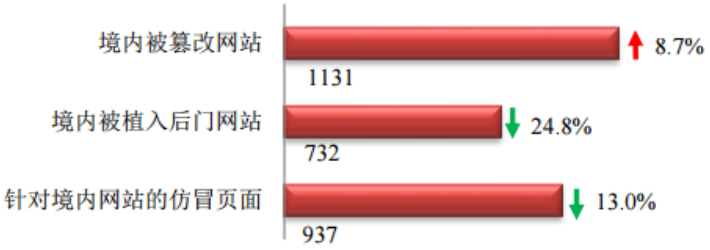
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 24.15 万个，其中包括境内被木马或被僵尸程序控制的主机约 16.97 万以及境内感染飞客（conficker）蠕虫的主机约 7.18 万。



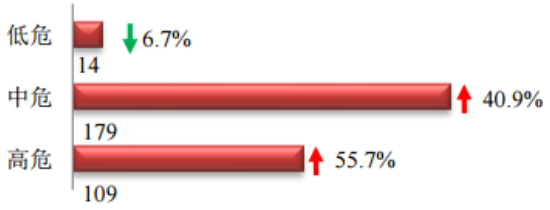
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1131 个；境内被植入后门的网站数量为 732 个；针对境内网站的仿冒页面数量为 937。



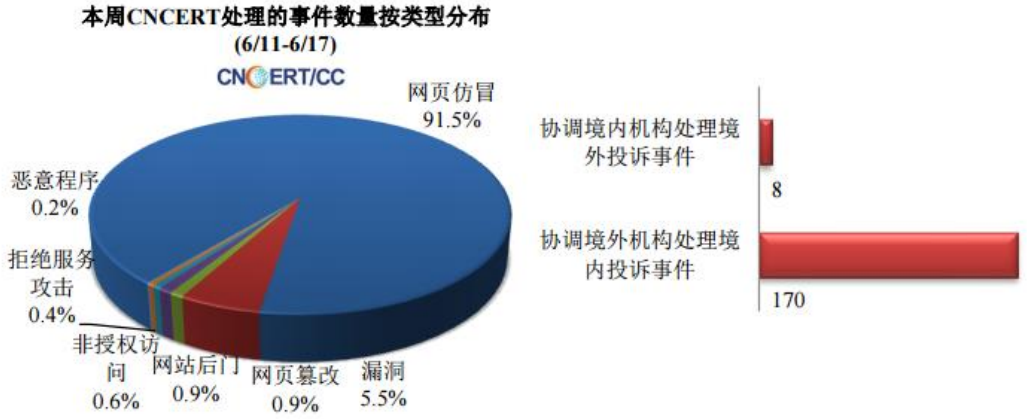
本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 302 个，信息安全漏洞威胁整体评价级别为中。



本周事件处理情况

本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 532 起，其中跨境网络安全事件 178 起。

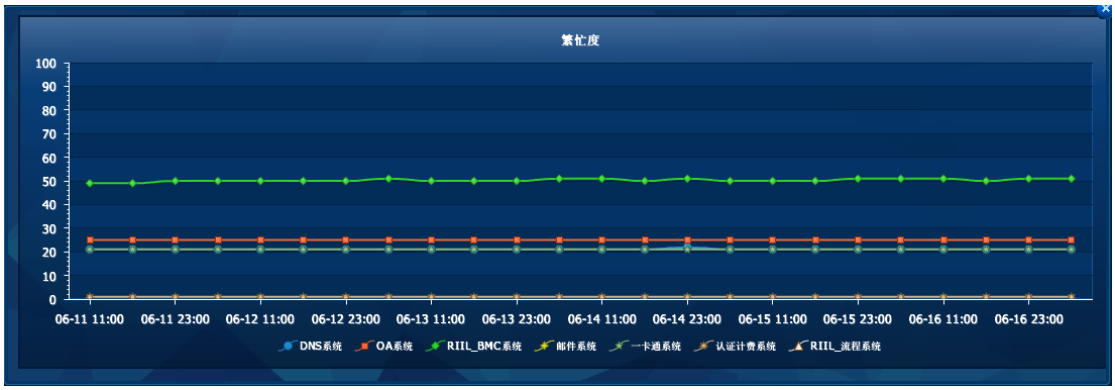


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 486 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 477 起和政府公益仿冒事件 7 起。

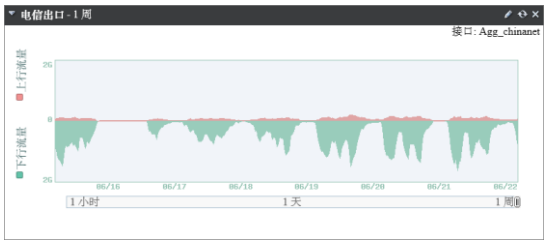
城院 IT 综合业务管理平台统计信息

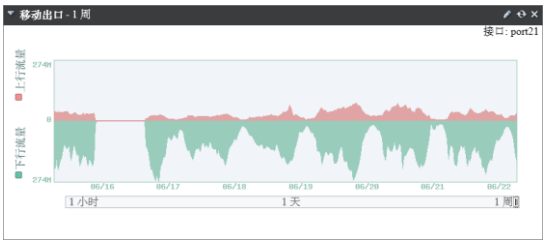
(2018 年 6 月 11 日—6 月 17 日)

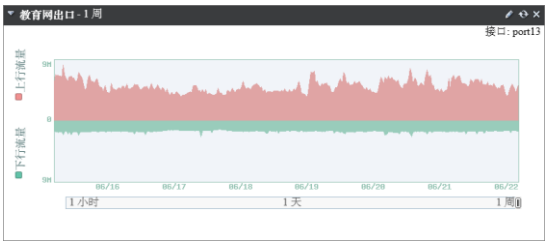
主要业务服务繁忙度

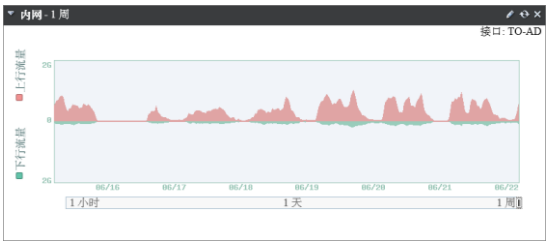


网络出口带宽情况统计







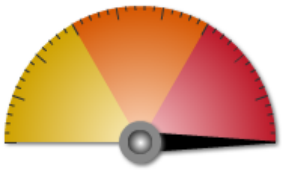


APT统计

防火墙统计	
恶意	2401
检测到0-day恶意软件变种	0
可疑文件	0
安全文件	157111631

【城院安全】网站群管理平台统计信息（2018 年 6 月 11 日—6 月 17 日）

风险趋势

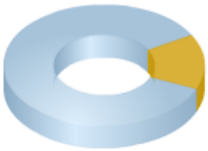


最近一周的全局风险等级为高，
在这段时间里共检测到 1237916 次攻击，其中低 57916 次，中 7340 次，高 1172660 次；在以上统计中由**命令注入攻击、爬虫、文件限制**产生的告警日志较多，请关注保护站点安全及防火墙配置，详情可查看此时间段的 [告警日志]。

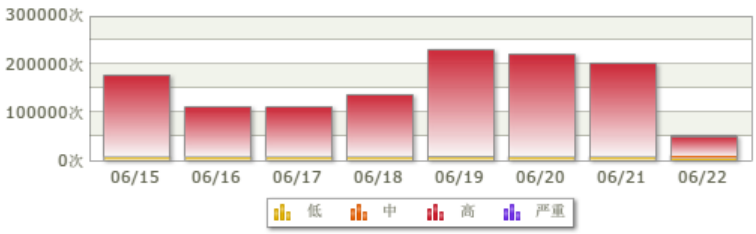
部署模式：透明代理 / 运行模式：正常模式 / 保护站点：3 个 / 规则库：2016082901

时间范围：最近一周 ▼ 保护站点：全局 ▼ 危险等级：全部 ▼ 动作：全部 ▼ 详细

保护站点攻击次数对比



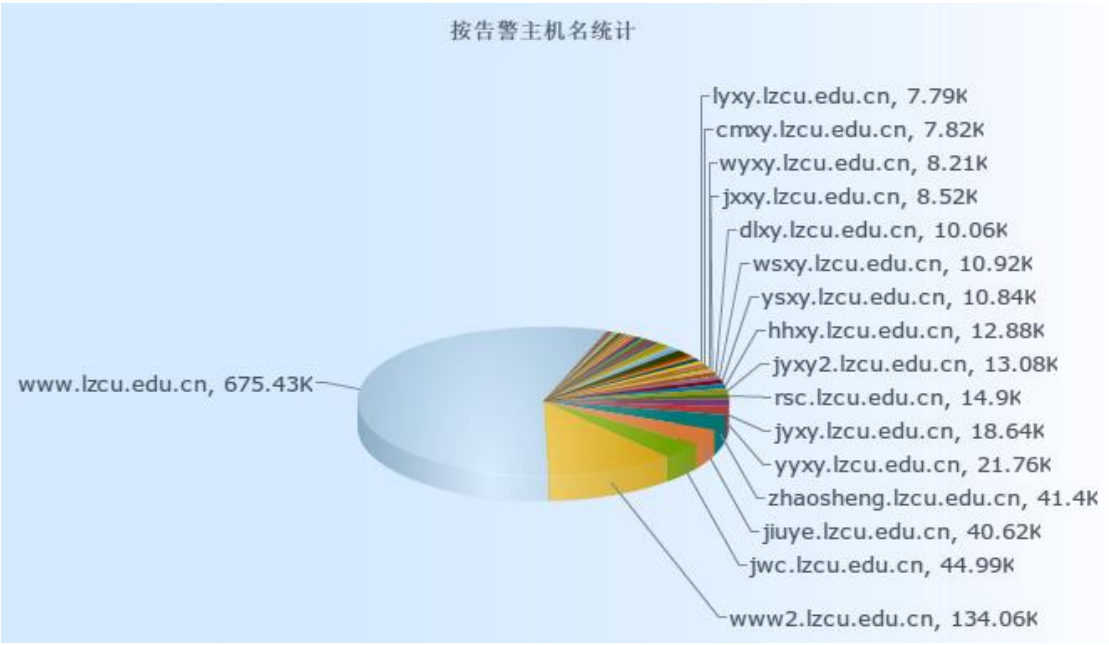
风险趋势图



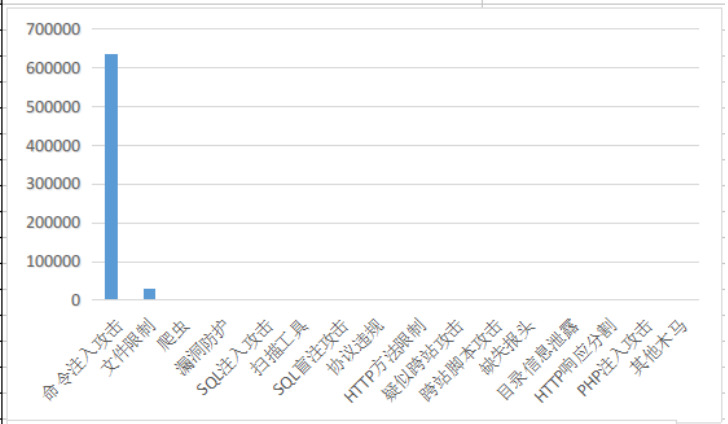
攻击类型统计(TOP)

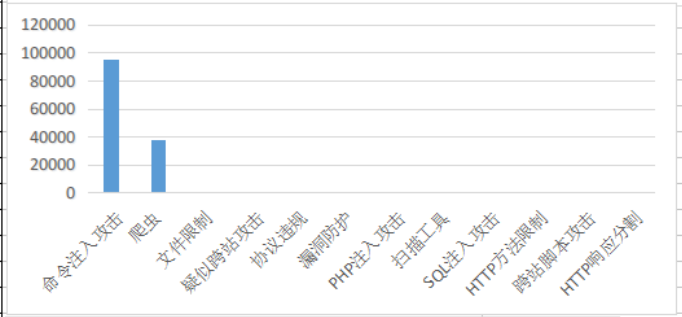
	全部 ↓	告警	阻断	重定向	放行
命令注入攻击	**1121144**	1121026	118	0	0
爬虫	**55921**	55706	215	0	0
文件限制	**45989**	44407	1582	0	0
其它	14862	4226	10636	0	0

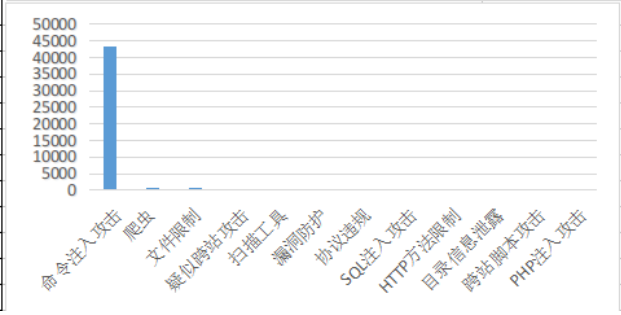
按告警主机名统计



主机名	事件	统计
www.lzcu.edu.cn	命令注入攻击	636756
	文件限制	29729
	爬虫	4632
	漏洞防护	743
	SQL注入攻击	728
	扫描工具	644
	SQL盲注攻击	568
	协议违规	555
	HTTP方法限制	547
	疑似跨站攻击	423
	跨站脚本攻击	44
	缺失报头	26
	目录信息泄露	12
	HTTP响应分割	9
	PHP注入攻击	7
	其他木马	3
www2.lzcu.edu.cn	命令注入攻击	95428
	爬虫	38297
	文件限制	96
	疑似跨站攻击	81
	协议违规	77
	漏洞防护	24
	PHP注入攻击	18
	扫描工具	17
	SQL注入攻击	7
	HTTP方法限制	5
	跨站脚本攻击	3
	HTTP响应分割	2
jwc.lzcu.edu.cn	命令注入攻击	43156
	爬虫	902
	文件限制	863
	疑似跨站攻击	16
	扫描工具	14
	漏洞防护	13
	协议违规	11
	SQL注入攻击	5
	HTTP方法限制	3
	目录信息泄露	3
	跨站脚本攻击	3
	PHP注入攻击	1







威胁	事件	统计
高危险等级统计	命令注入攻击	1100716 次
	文件限制	44739 次
	SQL注入攻击	3066 次
	疑似跨站攻击	1519 次
	漏洞防护	1359 次
	SQL盲注攻击	996 次
	HTTP方法限制	703 次
	跨站脚本攻击	242 次
	HTTP响应分割	137 次
	目录信息泄露	82 次
	PHP注入攻击	52 次
	缺失报头	22 次
	其他木马	3 次
	系统命令访问攻击	1 次
中危险等级统计	协议违规	1600 次
低危险等级统计	爬虫	47710 次
	协议违规	2507 次
	扫描工具	987 次
	缺失报头	10 次
	漏洞防护	6 次

网站群管理平台网页更新情况统计

网站	更新	网站	更新
兰州城市学院	26	甘肃省民族音乐研究中心	
学报编辑部	14	甘肃文化翻译中心	
就业服务网	10	甘肃张芝书法院	
党委宣传部	8	国际交流处	
国际文化翻译学院	7	国有资产管理处	
教师发展中心	7	后勤管理处	
科学研究处	4	化学与环境工程学院	
城市社会心理研究中心	3	机关党委	
教学质量监测与评估中心	3	机械工程学院	
马克思主义学院	3	基本建设处	
文史学院	3	教务处	
音乐学院	3	教育学院	
传媒学院	2	卡务中心	
创新创业学院	2	兰州城市学院校医院	
廉政网	2	路易艾黎研究中心	
旅游学院	2	美术与设计学院	
党委学生工作部	1	审计	
电子与信息工程学院	1	石油工程学院	
人事处	1	实训中心	
商学院	1	体育学院	
数学学院	1	团委	
保卫处		外国语学院	
财务处		心理咨询中心	
城市信息与系统科学研究所		信息技术教育与应用研究所	
档案馆		信息网络中心	
党委（校长）办公室		学位办公室	
党委组织部		饮食服务中心	
地理与城乡规划学院		幼儿师范学院	
电子信息科学与技术研究所		招生网	
发展规划处		职业技能鉴定所	
甘肃省高等学校外语教学指导委员会			

网站群管理平台应用防火墙入侵防护记录

A	B	C	D	E	F	G
序号	入侵位置	入侵者IP	归属地	详细信息	入侵方式	入侵时间
191932	管理平台	42.245.209.223	江苏省南京市 教育网	登录位置：网站管理； 登录账号： gswhfy	错误帐号或密码	2018-06-17 22:14:08
191931	管理平台	117.157.64.239	中国 移动	登录位置：网站管理； 登录账号： jyxy4	错误帐号或密码	2018-06-17 11:40:39
191930	管理平台	10.0.108.93	局域网 对方和您在同一内部网	登录位置：网站管理； 登录账号： cmxy	错误帐号或密码	2018-06-15 12:21:18
191929	管理平台	42.91.165.185	甘肃省兰州市 电信	登录位置：网站管理； 登录账号： xlyjzx	错误帐号或密码	2018-06-14 23:08:51
191928	管理平台	10.0.190.233	局域网 对方和您在同一内部网	登录位置：站群管理； 登录账号： admin	错误帐号或密码	2018-06-14 10:50:32
191927	管理平台	10.0.29.210	局域网 对方和您在同一内部网	登录位置：网站管理； 登录账号： lzw	错误帐号或密码	2018-06-13 16:30:59
191926	管理平台	10.0.28.87	局域网 对方和您在同一内部网	登录位置：网站管理； 登录账号： sxy	错误帐号或密码	2018-06-12 11:39:35
191925	管理平台	10.4.52.156	局域网 对方和您在同一内部网	登录位置：网站管理； 登录账号： jyxy2	错误帐号或密码	2018-06-11 20:04:09
191924	管理平台	10.0.120.150	局域网 对方和您在同一内部网	登录位置：网站管理； 登录账号： rsc	错误帐号或密码	2018-06-11 14:52:16
191923	管理平台	10.4.35.19	局域网 对方和您在同一内部网	登录位置：网站管理； 登录账号： jyxy4	错误帐号或密码	2018-06-11 11:39:16
191921	管理平台	10.0.93.71	局域网 对方和您在同一内部网	登录位置：站群管理； 登录账号： admin	错误帐号或密码	2018-06-11 09:29:45
191920	管理平台	118.120.173.169	四川省泸州市 电信	登录位置：站群管理； 登录账号： yxy1	错误帐号或密码	2018-06-11 08:31:45

网站群管理平台应用防火墙网站访问 IP 封禁记录

（无）

网站群管理平台 6 月份网站累计访问次数

站点名称	访问次数	站点名称	访问次数
兰州城市学院	95414	国际文化翻译学院	492
教务处	11508	学位办公室	411
就业服务网	4515	教师发展中心	395
教育学院	4419	国有资产管理处	393
教育学院	3912	学校办公室	371
文史学院	3002	党委组织部	336
化学与环境工程学院	2865	党委宣传部	333
音乐学院	2700	后勤管理处	317
人事处	2436	团委	295
地理与城乡规划学院	2160	保卫处	285
外国语学院	2144	兰州城市学院校医院	275
电子与信息工程学院	2135	基本建设处	246
石油工程学院	2135	饮食服务中心	210
机械工程学院	2013	心理咨询中心	192
幼儿师范学院	1942	信息网络中心	180
旅游学院	1940	甘肃文化翻译中心	179
马克思主义学院	1743	发展规划处	149
传媒学院	1719	卡务中心	134
数学学院	1643	城市社会心理研究中心（新）	127
财务处	1598	审计	120
体育学院	1401	学报编辑部	86
美术与设计学院	1390	甘肃省民族音乐研究中心	85
商学院	1255	电子信息科学与技术研究所	69
党委学生工作部	785	信息技术教育与应用研究所	46
国际交流处	784	甘肃张芝书法院	36
科学研究处	767	城市信息与系统科学研究所	29
教学质量监测与评估中心（新）	607	机关党委	20
创新创业学院	561	职业技能鉴定所	19
路易艾黎研究中心	555	甘肃省高等学校外语教学指导委员会	8
廉政网	519	实训中心	5

网站安全检测一（360 网站安全检测）

www.lzcu.edu.cn +0 子域名安全状况 分享到微博

安全级别 安全

安全等级打败了全国 76% 的网站！特此授予您五星神站称号！

99分

查看网站安全报告

网站漏洞 存在轻微漏洞
虚假，欺诈 正常
挂马，恶意 正常
恶意篡改 正常
敏感内容 正常

漏洞时间：1周前
高危漏洞 0个页面
严重漏洞 0个页面
警告漏洞 0个页面
轻微漏洞 1个页面

网站安全漏洞

存在"服务器配置信息泄露"风险，安全性降低5% 漏洞信息已隐藏，只对网站管理员开放 请先验证权限

虚假或欺诈网站监控

正常

挂马或恶意网站监控

正常

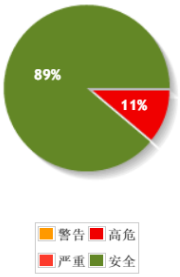
黑客篡改网站监控

正常

网站敏感内容监控

正常

www.lzcu.edu.cn 子域名安全状况



安全	syzz.lzcu.edu.cn
安全	nic.lzcu.edu.cn
安全	mail.lzcu.edu.cn
安全	oa.lzcu.edu.cn
安全	jwc.lzcu.edu.cn
高危	jpkc.lzcu.edu.cn
安全	ftp.lzcu.edu.cn
安全	www2.lzcu.edu.cn
安全	cj.lzcu.edu.cn

监控对象	类型	监测点	响应时间	访问成功率
OA办公主页【http://oa.lzcu.edu.cn】	源站监控	2	577.72 ms	100 %
OA办公主页【http://oa.lzcu.edu.cn】	源站监控	2	491.42 ms	100 %
WEB【http://www.lzcu.edu.cn】	源站监控	2	289.91 ms	100 %
WEB【http://www.lzcu.edu.cn】	源站监控	2	393.96 ms	100 %

异常发生时间	监控对象	监控类型	当前状态	事件信息	持续时间
2018-06-13 13:48:14	WEB【http://www.lzcu.edu.cn】	HTTP	已恢复	[异常] 下载数据超时	10分钟

网站安全检测二（百度云观测）

昨日百度中国互联网安全指数上限为100点，距离完美还差49.88点。全行业的网站安全等级偏低。（每日指数上限随观测站点变化而变化）
所有观测站点中，0个为完美等级站点，408561个为良好等级站点，2533107个为低危等级站点，1099796个为中危等级站点，2182015个为高危等级站点。

等级分布

域名	指数评价	操作
alumni.lzcu.edu.cn	80 良好	查看详情>>
bf.lzcu.edu.cn	4 高危	查看详情>>
cj.lzcu.edu.cn	90 良好	查看详情>>
dwxcb.lzcu.edu.cn	34 高危	查看详情>>
ecard.lzcu.edu.cn	34 高危	查看详情>>
jiuye.lzcu.edu.cn	34 高危	查看详情>>
jpkc.lzcu.edu.cn	14 高危	查看详情>>
jpkc2.lzcu.edu.cn	49 中危	查看详情>>
jwc.lzcu.edu.cn	34 高危	查看详情>>
kyc.lzcu.edu.cn	34 高危	查看详情>>

当前 1 / 2 页 首页 上一页 下一页 尾页

等级分布

域名	指数评价	操作
lzcu.edu.cn	80 良好	查看详情>>
nic.lzcu.edu.cn	90 良好	查看详情>>
oa.lzcu.edu.cn	84 良好	查看详情>>
old.lzcu.edu.cn	44 中危	查看详情>>
pop.lzcu.edu.cn	0 高危	查看详情>>
smtp.lzcu.edu.cn	0 高危	查看详情>>
syzz.lzcu.edu.cn	4 高危	查看详情>>
test.lzcu.edu.cn	84 良好	查看详情>>
www2.lzcu.edu.cn	4 高危	查看详情>>

【网络知识】手机 WiFi 总是断开连接又重连之间重复是怎么回事?如何解决?

信息网络中心 2018.6.21

手机 WiFi 总是断开连接又重连之间重复是怎么回事?如何解决?大家是不是也遇到这样的情况，导致自己无法上网。其实只要我们找对了原因，然后对症下药，就能解决处理。好了，下面小编就为大家介绍原因以及三种解决方案，一起来看看吧！

答案 1:WIFI、无线网络自动关闭

当手机锁屏以后，为了节省电量，系统会自动关闭 wifi 连接，开启屏幕后又会自动连接。如果不想要自动关闭 wifi 的功能，可以在手机的设置，通用里，点击自动锁定，选择永不，这样手机就不会锁屏，也不会断开网络连接，但缺点是耗电量也会相对提高。您也可以进入“手机设置->无线和网络->WLAN 设置”，点击手机下方的”菜单“按钮，在弹出的菜单中选择“高级”，然后在“WLAN 休眠策略”的下拉菜单中选择”从不“，从而实现 WLAN 始终开启，永不休眠。选择合适 WIFI 休眠策略可以帮助您获得更好的手机体验。

答案 2:如何用 WIFI 上网

首先需要您附近有可用的无线网络，然后进入手机设置的“无线和网络”菜单，勾选“打开 WLAN”，然后进入“WLAN 设置”，搜索可用的无线网络。搜索到以后，点击连接即可(有些无线网络有密码保护，需要您输入密码才能连接)。

答案 3:WIFI 连接不上无线局域网(WLAN)

一、如果网络有密钥的话 首先要确保获得密钥。

二、另外有的网络有过滤机制(例如，MAC 地址过滤) 请确保过滤机制没有将您的手机过滤掉。

三、更换网络制式 现在的家用无线路由器一般是支持 802.11b 和 802.11g 制式。电脑的网卡一般都是支持的。 但是很多手机只是支持其中一种，请更换网络制式后重启路由器试试。另外建议不要选择混合模式。

答案 4：手机 WiFi 总是断开连接又重连之间重复

联系信息网络中心将手机 MAC 地址绑定即可解决此类问题。

以上就是手机 WiFi 总是断开连接又重连之间重复的几种解决方案，希望能帮到大家！

抄送：校领导