网络信息安全周报

【2018】第 9 期

党委宣传部
信息网络中心 编

2018 年 5 月 3 日

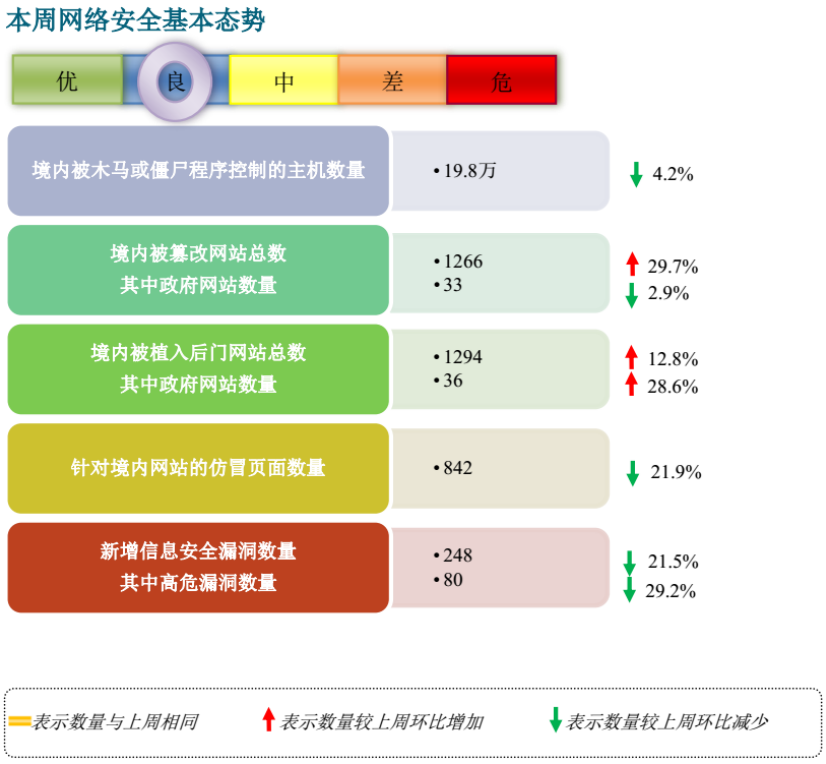
本期要目

- 【权威发布】全国网络安全信息与动态（2018 年 4 月 16 日—4 月 22 日）
- 【城院 IT】综合业务管理平台统计信息(2018 年 4 月 23 日—4 月 29 日)
- 【城院安全】网站群管理平台统计信息（2018 年 4 月 23 日—4 月 29 日）
- 【安全教育】习近平在全国网络安全和信息化工作会议上强调了这些

全国网络安全信息与动态

（2018 年 4 月 16 日—4 月 22 日）

根据国家互联网应急中心最新公告数据：

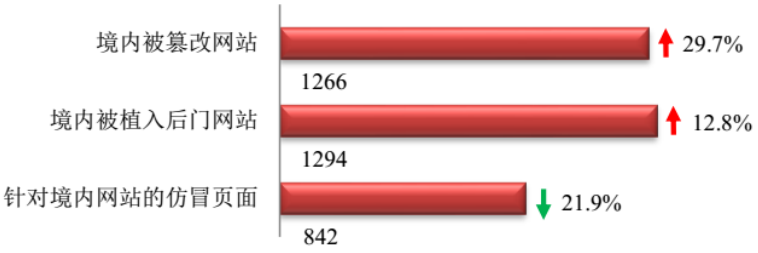


本周网络病毒活动情况

本周，境内被木马或僵尸程序控制的主机数量约为 19.8 万。

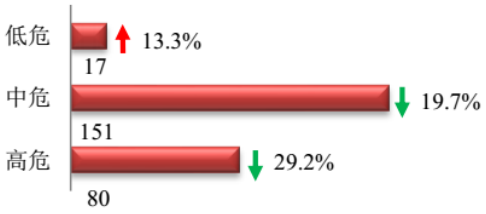
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1266 个；境内被植入后门的网站数量为 1294 个；针对境内网站的仿冒页面数量为 842。



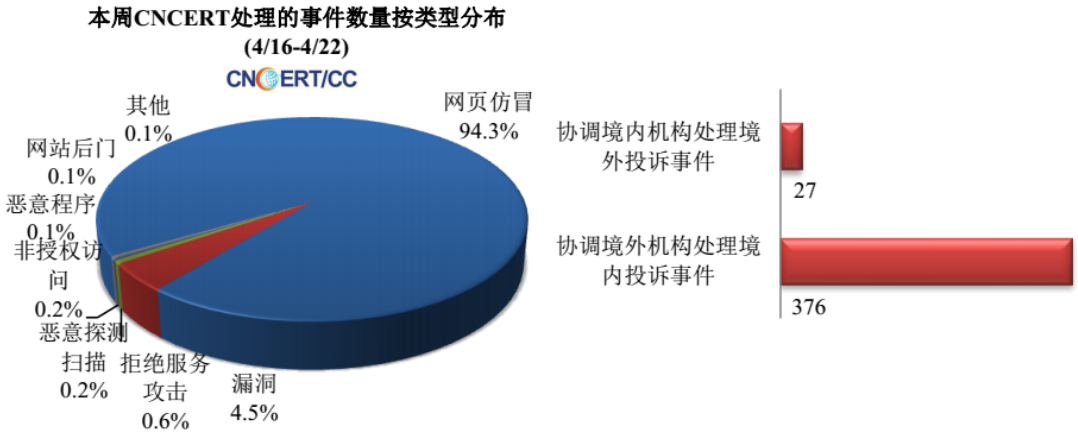
本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 248 个，信息安全漏洞威胁整体评价级别为高。



本周事件处理情况

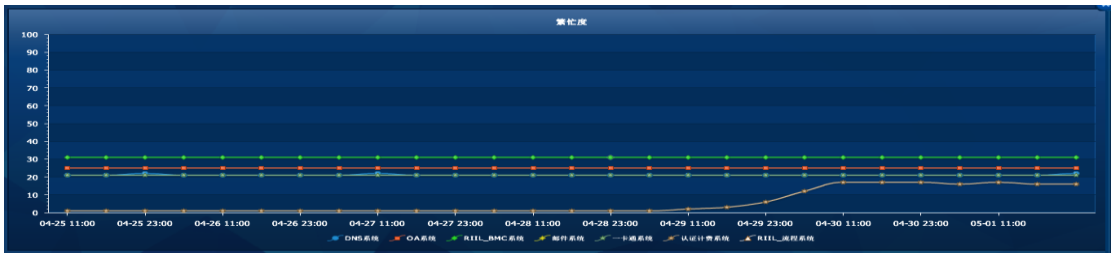
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 1070 起，其中跨境网络安全事件 403 起。



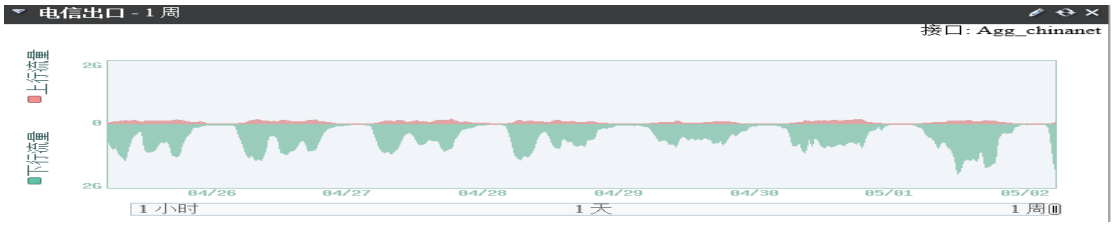
城院 IT 综合业务管理平台统计信息

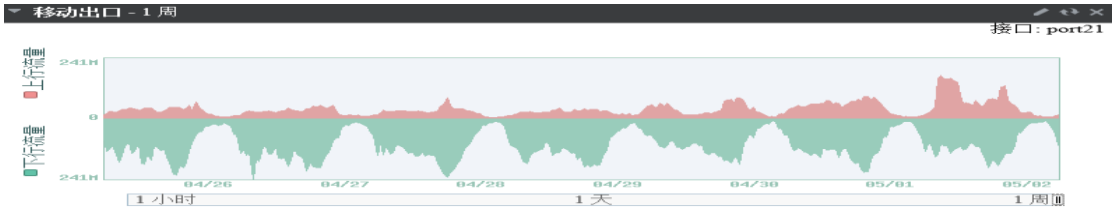
(2018 年 4 月 23 日—4 月 29 日)

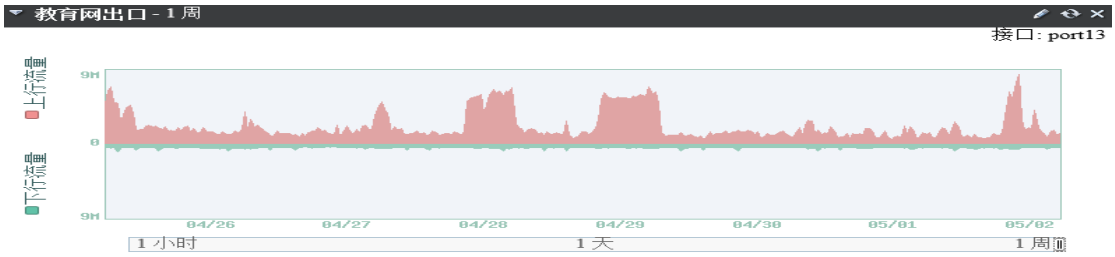
主要业务服务繁忙度

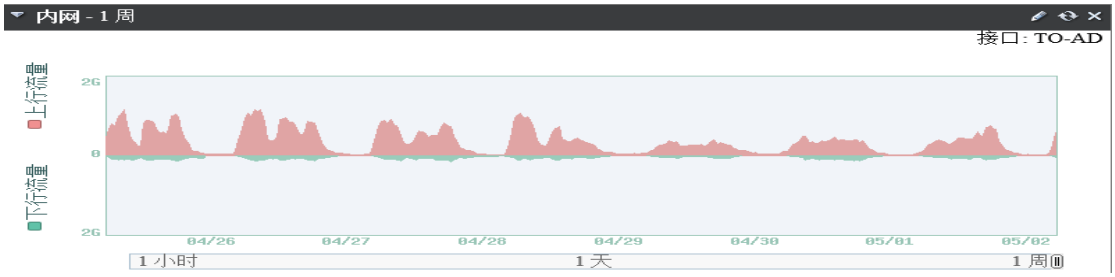


网络出口带宽情况统计







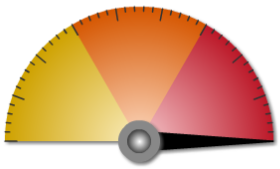


APT统计

防火墙统计	
恶意	424
检测到0-day恶意软件变种	0
可疑文件	0
安全文件	70470216

【城院安全】网站群管理平台统计信息（2018 年 4 月 23 日—4 月 29 日）

风险趋势

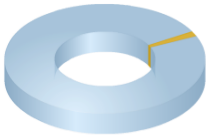


最近一周的全局风险等级为高，
在这段时间里共检测到 213382 次攻击，其中低 12468 次，中 3443 次，高 197471 次；在以上统计中由**命令注入攻击**、**文件限制**、**SQL注入攻击**产生的告警日志较多，请关注保护站点安全及防火墙配置，详情可查看此时间段的 [**告警日志**] 。

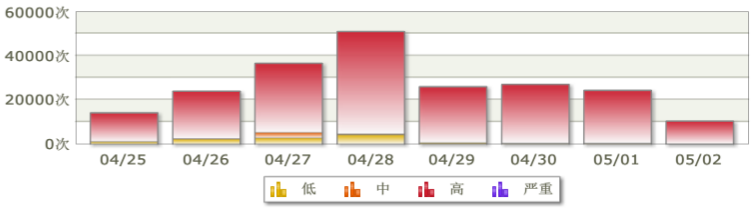
部署模式：透明代理 / 运行模式：正常模式 / 保护站点：2 个 / 规则库：2016082901

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...



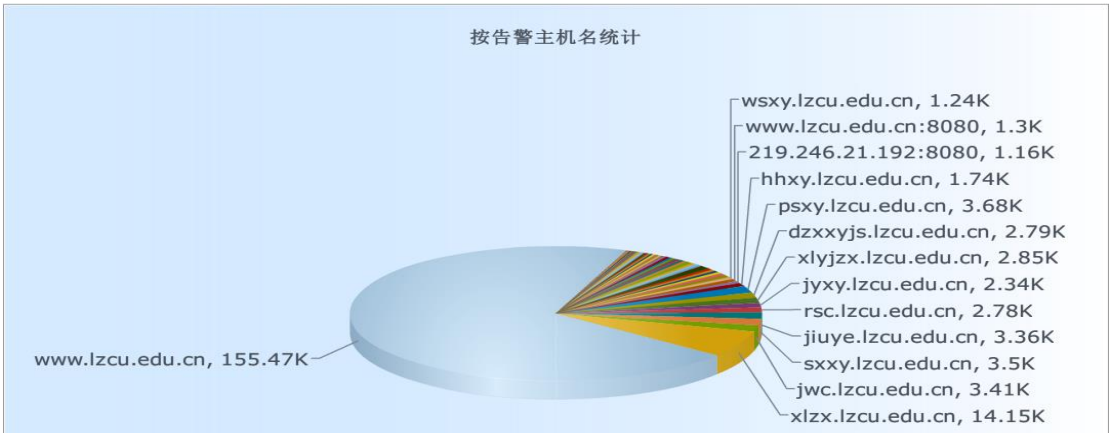
风险...



攻击类型统计(T...

	全部 ↓	告警	阻断	重定向	放行
命令注入攻击	**97198**	0	97198	0	0
文件限制	**40051**	39668	383	0	0
SQL注入攻击	**26450**	22912	3538	0	0
其它	49703	16389	33314	0	0

按告警主机名统计 - 报表摘要	
威胁	高于等于 低
发生时间	大于等于 2018-04-25 08:53:11
发生时间	小于等于 2018-05-02 08:53:11
报表生成时间	2018-05-02 08:50:41



主机名	事件	统计
www.lzcu.edu.cn 兰州城市学院网站	命令注入攻击	76806 次
	文件限制	26310 次
	SQL注入攻击	23120 次
	SQL盲注攻击	22871 次
	爬虫	3834 次
	协议违规	888 次
	疑似跨站攻击	586 次
	扫描工具	470 次
	针对IE8的跨站攻击	314 次
	漏洞防护	217 次
	HTTP方法限制	22 次
	目录信息泄露	14 次
	缺失报头	11 次
	跨站脚本攻击	4 次
	文件注入攻击	3 次
	PHP注入攻击	2 次
xlzx.lzcu.edu.cn 心理咨询中心网站	命令注入攻击	7304 次
	协议违规	2920 次
	SQL注入攻击	1335 次
	扫描工具	916 次
	文件限制	794 次
	SQL盲注攻击	251 次
	疑似跨站攻击	212 次
	爬虫	204 次
	漏洞防护	122 次
	针对IE8的跨站攻击	64 次
	LDAP注入攻击	12 次
	跨站脚本攻击	8 次
	HTTP方法限制	3 次
	文件注入攻击	3 次
	缺失报头	1 次
jwc.lzcu.edu.cn 教务处网站	命令注入攻击	2330 次
	文件限制	572 次
	爬虫	213 次
	SQL注入攻击	95 次
	扫描工具	85 次
	SQL盲注攻击	38 次
	针对IE8的跨站攻击	30 次
	HTTP方法限制	28 次
	漏洞防护	9 次
	协议违规	4 次
	疑似跨站攻击	1 次
	跨站脚本攻击	1 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	29	电子信息科学与技术研究所	
教学质量监测与评估中心	24	发展规划处	
就业服务网	13	甘肃省高等学校外语教学指导委员会	
党委宣传部	10	甘肃文化翻译中心	
音乐学院	8	甘肃张芝书法院	
马克思主义学院	6	国有资产管理处	
科学研究处	3	后勤管理处	
路易艾黎研究中心	3	化学与环境工程学院	
数学学院	3	机关党委	
教育学院	2	机械工程学院	
廉政网	2	基本建设处	
体育学院	2	教师发展中心	
外国语学院	2	教务处	
幼儿师范学院	2	卡务中心	
传媒学院	1	旅游学院	
电子与信息工程学院	1	美术与设计学院	
兰州城市学院校医院	1	人事处	
商学院	1	膳食处	
信息网络中心	1	审计	
保卫处		石油工程学院	
财务处		实训中心	
城市社会心理研究中心		团委	
城市信息与系统科学研究所		文史学院	
创新创业学院		心理咨询中心	
档案馆		信息技术教育与应用研究所	
党委（校长）办公室		学位办公室	
党委学生工作部		招生网	
党委组织部		职业技能鉴定所	
地理与城乡规划学院			

网站群管理平台应用防火墙入侵防护记录

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
191770	管理平台	10.0.191.52	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： pjb	错误帐号或密码	2018-04-28 17:30:55
191769	管理平台	10.0.69.177	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： jwc	错误帐号或密码	2018-04-28 16:08:43
191768	站点名称：心理咨询中心	218.66.59.84	福建省福州市 电信	含有非法请求参数： "()&%<acx><ScRiPt >kghe(9284)</ScRiPt>	跨站脚本注入	2018-04-28 16:04:29
191767	站点名称：心理咨询中心	110.87.188.33	福建省福州市 电信	含有非法请求参数	跨站脚本注入	2018-04-28 16:03:49
191766	站点名称：心理咨询中心	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-04-28 16:03:49
191765	管理平台	10.0.114.19	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： jwc_zhk	错误帐号或密码	2018-04-28 15:35:51
191764	管理平台	10.0.114.19	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： jwc_zhk	错误帐号或密码	2018-04-28 15:35:32
191763	管理平台	10.0.120.35	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： jwc	错误帐号或密码	2018-04-28 15:33:14
191762	管理平台	10.0.8.212	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： yhb	错误帐号或密码	2018-04-28 11:21:33
191761	管理平台	10.0.127.240	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： jyfw	错误帐号或密码	2018-04-27 11:14:38
191760	管理平台	10.0.116.40	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： cxcy	错误帐号或密码	2018-04-27 10:50:51
191759	管理平台	10.0.116.40	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： cxcy	错误帐号或密码	2018-04-27 10:50:16
191758	管理平台	10.0.108.30	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： yyxy	错误帐号或密码	2018-04-27 08:26:18
191757	站点名称：电子信息科学与技术研究所	27.255.77.11	韩国 Ehost互联网数据中心	含有非法请求参数	SQL注入	2018-04-27 04:42:52
191756	站点名称：电子信息科学与技术研究所	27.255.77.11	韩国 Ehost互联网数据中心	含有非法请求参数	SQL注入	2018-04-27 04:42:52
191755	站点名称：电子信息科学与技术研究所	27.255.77.11	韩国 Ehost互联网数据中心	含有非法请求参数	SQL注入	2018-04-27 04:42:52
191754	管理平台	10.0.4.183	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： yesf	错误帐号或密码	2018-04-24 17:03:36
191753	管理平台	10.0.108.187	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： wgyxy	错误帐号或密码	2018-04-24 15:28:20
191752	管理平台	10.0.108.19	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： lzw	错误帐号或密码	2018-04-24 11:23:49
191751	管理平台	10.0.116.40	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： xcbsf	错误帐号或密码	2018-04-24 10:13:08
191750	站点名称：外国语学院	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-04-24 00:18:04
191749	站点名称：外国语学院	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-04-24 00:18:04
191748	站点名称：外国语学院	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-04-24 00:18:04
191747	站点名称：就业服务网	185.92.73.105	欧洲和中东地区	含有非法请求参数	SQL注入	2018-04-23 18:54:52
191746	站点名称：就业服务网	185.92.73.105	欧洲和中东地区	含有非法请求参数	SQL注入	2018-04-23 18:54:51
191745	站点名称：就业服务网	185.92.73.105	欧洲和中东地区	含有非法请求参数	SQL注入	2018-04-23 18:54:50
191744	管理平台	10.0.116.40	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： xcbsf	错误帐号或密码	2018-04-23 18:27:13
191743	管理平台	10.0.116.40	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： xcbsf	错误帐号或密码	2018-04-23 18:26:55

网站群管理平台应用防火墙网站访问 IP 封禁记录

封禁IP	封禁IP归属地	封禁开始时间 ▼	封禁结束时间
27.255.77.11	韩国 Ehost互联网数据中心	2018-04-27 04:42:52	2018-04-27 14:42:52
110.87.188.33	福建省福州市 电信	2018-04-24 00:18:04	2018-04-24 10:18:04
185.92.73.105	欧洲和中东地区	2018-04-23 18:54:52	2018-04-24 04:54:52

网站群管理平台 4 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	82140		党委（校长）办公室	319
教务处	7372		团委	295
就业服务网	7107		后勤管理处	217
化学与环境工程学院	3260		甘肃文化翻译中心	199
教育学院	3053		保卫处	194
电子与信息工程学院	2327		膳食处	162
外国语学院	2283		党委组织部	162
文史学院	2217		教师发展中心	133
人事处	2105		发展规划处	131
机械工程学院	2070		廉政网	129
地理与城乡规划学院	1977		学位办公室	122
音乐学院	1933		信息网络中心	120
数学学院	1771		卡务中心	115
旅游学院	1682		甘肃张芝书法院	114
马克思主义学院	1583		心理咨询中心	113
石油工程学院	1464		审计	111
美术与设计学院	1382		兰州城市学院校医院	90
幼儿师范学院	1316		信息技术教育与应用研究所	80
体育学院	1194		基本建设处	77
商学院	1095		机关党委	77
传媒学院	925		甘肃省民族音乐研究中心	74
科学研究处	772		实训中心	53
财务处	580		电子信息科学与技术研究所	53
教学质量监测与评估中心（新）	578		城市社会心理研究中心（新）	36
国有资产管理处	563		城市信息与系统科学研究所	24
创新创业学院	413		职业技能鉴定所	23
党委宣传部	410		国际交流处	8
路易艾黎研究中心	384		甘肃省高等学校外语教学指导委员会	1
党委学生工作部	370			

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

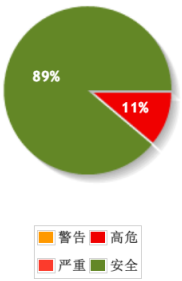
黑客篡改网站监控

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	535.58 ms	100 %	详情
OA办公主页【http://oa.lzcu.edu.cn】	源站监控	2	535.29 ms	100 %	详情
WEB【http://www.lzcu.edu.cn】	源站监控	2	544.79 ms	100 %	详情
WEB【http://www.lzcu.edu.cn】	源站监控	2	1825.32 ms	100 %	详情

当前告警事件【当前共有 2 个告警事件】

监控对象	类型	异常信息	发生时间	已持续	
WEB【http://www.lzcu.edu.cn】	源站监控	[故障] HTTP状态码503	2018-04-19 16:16:36	4天17小时	详情
WEB【http://www.lzcu.edu.cn】	源站监控	[故障] HTTP状态码503	2018-04-19 16:26:12	4天17小时	详情

网站安全检测二（百度云观测）

百度安全指数 更新时间:2018-05-02 02:48 查看详情>>

百度安全指数

52.44↑0.35

中国互联网当前处于 中危 状态

观测站点 6313713（↑492）

恶意站点 784（↑69）

漏洞 6723122（↓2957）

http://www.lzcu.edu.cn 更新时间：2018-05-01 20:04:31

指数评价

34.0

所属行业：教育培训

30.70% ↓

战胜了全国 0.00% 的网站

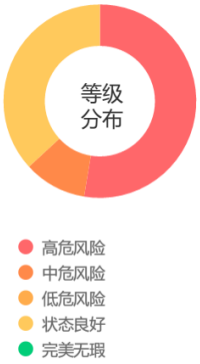
关联网站安全

关联网站数 19

最低指数评价 0 高危

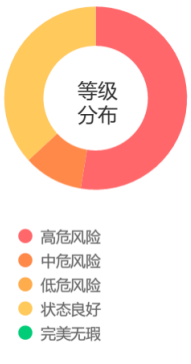
查看更多>>

该网站安全指数评价 高危 但是仍存在改进空间。建议 开启云观测服务>> ，查看评价详情，获取最新网站安全报警，及时修复以免被搜索引擎风险标识或降权。



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>>
jpkc2.lzcu.edu.cn	90 良好	查看详情>>
jpkc.lzcu.edu.cn	14 高危	查看详情>>
jwc.lzcu.edu.cn	41.2 中危	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



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>>

当前 2 / 2 页 首页 上一页 下一页 尾页

【安全教育】习近平在全国网络安全和信息化工作会议上强调了这些

浙江新闻 2018-04-22 14:58:00　2018-04-22 14:58 | 新华视点

全国网络安全和信息化工作会议20日至21日在北京召开。习近平出席会议并发表重要讲话。他强调，信息化为中华民族带来了千载难逢的机遇。还有哪些金句？快来了解！


@新华视点
新华社法人微博
我们不断推进理论创新和实践创新，不仅走出一条中国特色治网之道，而且提出一系列新思想新观点新论断，形成了网络强国战略思想。
新华视点


@新华视点
新华社法人微博
要压实互联网企业的主体责任，决不能让互联网成为传播有害信息、造谣生事的平台。
新华视点


@新华视点
新华社法人微博
没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。
新华视点
@新华视点
新华社法人微博
要依法严厉打击网络黑客、电信网络诈骗、侵犯公民个人隐私等违法犯罪行为，切断网络犯罪利益链条，持续形成高压态势，维护人民群众合法权益。
新华视点


@新华视点
新华社法人微博
要推动产业数字化，利用互联网新技术新应用对传统产业进行全方位、全角度、全链条的改造，提高全要素生产率，释放数字对经济发展的放大、叠加、倍增作用。
新华视点


@新华视点
新华社法人微博
要抓住当前信息技术变革和新军事变革的历史机遇，深刻理解生产力和战斗力、市场和战场的内在关系，把握网信军民融合的工作机理和规律，推动形成全要素、多领域、高效益的军民深度融合发展的格局。
新华视点

（原标题《金句来了！习近平在全国网络安全和信息化工作会议上强调了这些重要内容》。编辑陆斯超）

抄送：校领导