

网络信息安全周报

【2018】第 13 期

党委宣传部
信息网络中心 编

2018 年 5 月 31 日

本期要目

- 【权威发布】全国网络安全信息与动态（2018 年 5 月 14 日—5 月 20 日）
- 【城院 IT】综合业务管理平台统计信息（2018 年 5 月 21 日—5 月 27 日）
- 【城院安全】网站群管理平台统计信息（2018 年 5 月 21 日—5 月 27 日）
- 【安全教育】微信新规即将执行，网友：真的封号？腾讯：零容忍！

全国网络安全信息与动态

（2018 年 5 月 7 日—5 月 13 日）

根据国家互联网应急中心最新公告数据：

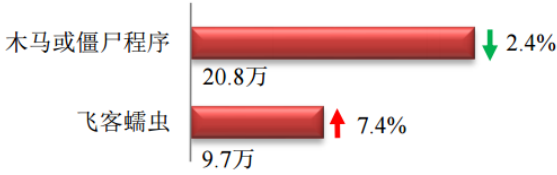
本周网络安全基本态势



— 表示数量与上周相同 ↑ 表示数量较上周环比增加 ↓ 表示数量较上周环比减少

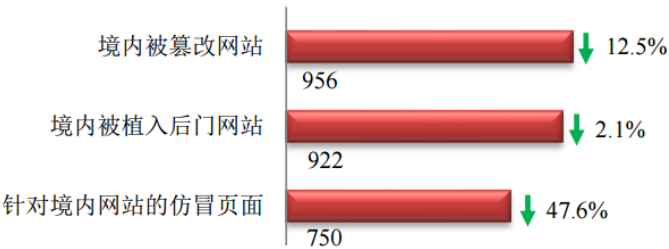
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 30.5 万个，其中包括境内被木马或被僵尸程序控制的主机约 20.8 万以及境内感染飞客（conficker）蠕虫的主机约 9.7 万。



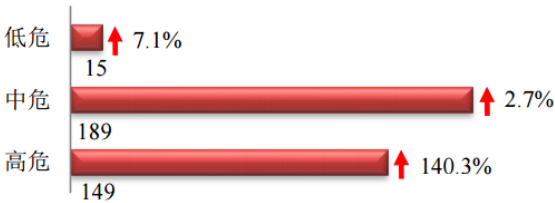
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 956 个；境内被植入后门的网站数量为 922 个；针对境内网站的仿冒页面数量为 750。



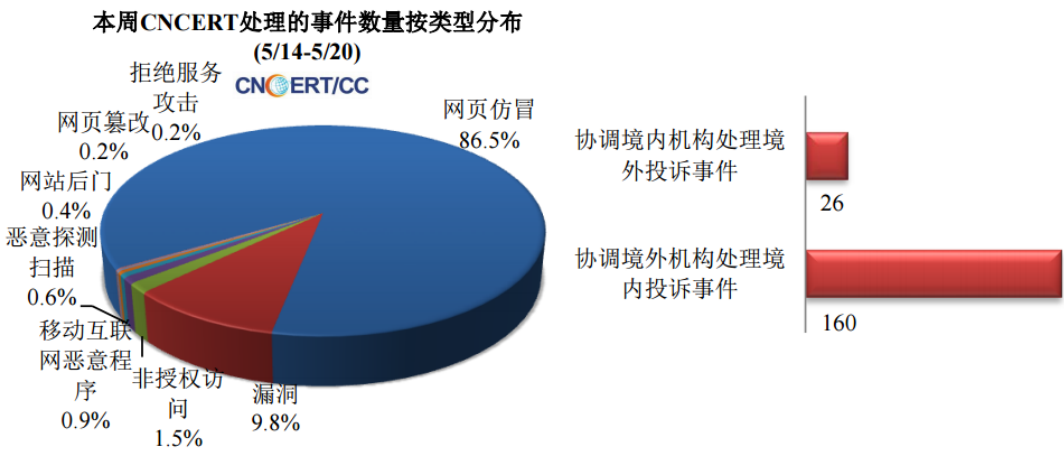
本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 353 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

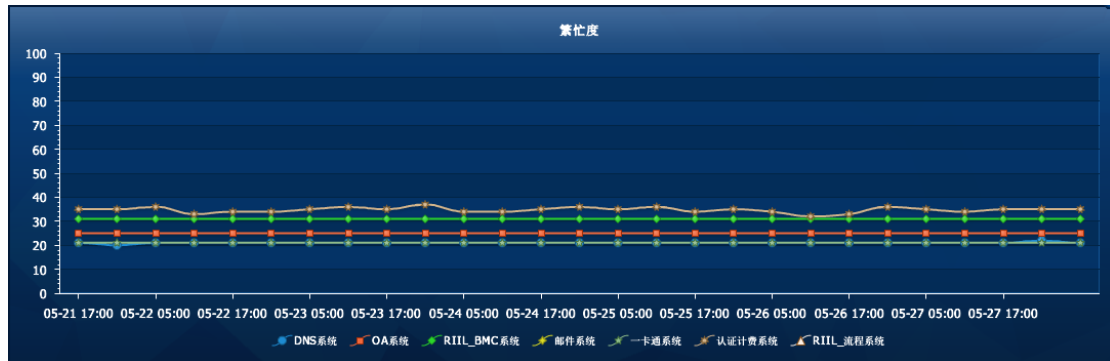
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 533 起，其中跨境网络安全事件 186 起。



城院 IT 综合业务管理平台统计信息

(2018 年 5 月 14 日—5 月 20 日)

主要业务服务繁忙度



网络出口带宽情况统计



【城院安全】网站群管理平台统计信息（2018 年 5 月 14 日—5 月 20 日）

风险趋势



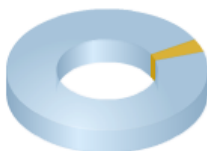
最近一周的全局风险等级为高，

在这段时间里共检测到 1103263 次攻击，其中低 24200 次，中 2218 次，高 1076845 次；在以上统计中由命令注入攻击、文件限制、爬虫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]。

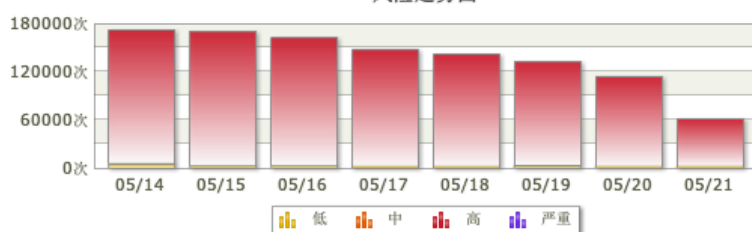
部署模式：透明代理 / 运行模式：正常模式 / 保护站点：3 个 / 规则库：2016082901

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

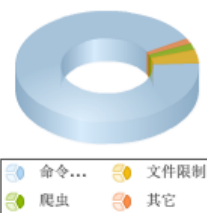
保护站点攻击次数对比



风险趋势图

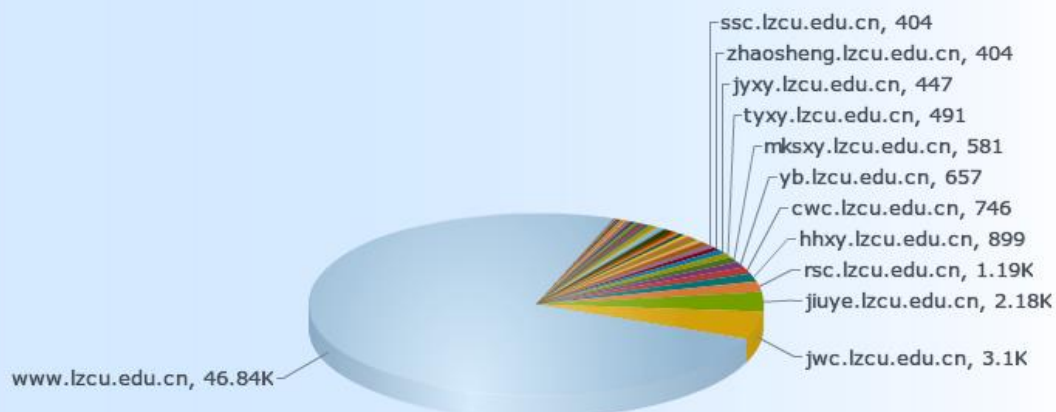


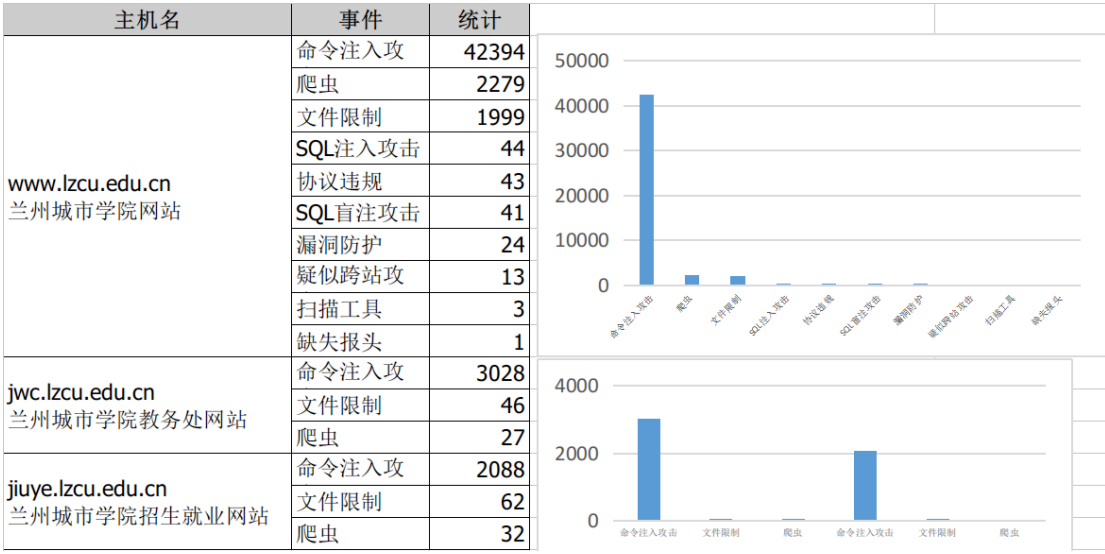
攻击类型统计(TOP)



	全部↓	告警	阻断	重定向	放行
命令注入攻击	1019776	1018800	976	0	0
文件限制	45702	43670	2032	0	0
爬虫	20088	19872	216	0	0
其它	17697	6534	11163	0	0

按告警主机名统计





威胁	事件	统计
高	命令注入攻击	1029931 次
	文件限制	46963 次
	漏洞防护	11461 次
	SQL注入攻击	7008 次
	疑似跨站攻击	1990 次
	跨站脚本攻击	1900 次
	SQL盲注攻击	640 次
	HTTP方法限制	321 次
	目录信息泄露	303 次
	HTTP响应分割	248 次
	系统命令访问攻击	22 次
	PHP注入攻击	20 次
	缺失报头	9 次
	其他木马	1 次
中	协议违规	1871 次
	漏洞防护	3 次
低	爬虫	31982 次
	协议违规	3645 次
	扫描工具	2427 次
	缺失报头	195 次
	漏洞防护	12 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	31	国有资产管理处	
就业服务网	19	后勤管理处	
党委宣传部	6	机关党委	
化学与环境工程学院	4	机械工程学院	
文史学院	4	基本建设处	
传媒学院	2	教师发展中心	
教育学院	2	教务处	
党委学生工作部	1	教学质量监测与评估中心	
马克思主义学院	1	卡务中心	
商学院	1	科学研究处	
数学学院	1	兰州城市学院校医院	
团委	1	廉政网	
信息网络中心	1	路易艾黎研究中心	
保卫处		旅游学院	
财务处		美术与设计学院	
城市社会心理研究中心		人事处	
城市信息与系统科学研究所		审计	
创新创业学院		石油工程学院	
档案馆		实训中心	
党委（校长）办公室		体育学院	
党委组织部		外国语学院	
地理与城乡规划学院		心理咨询中心	
电子信息科学与技术研究所		信息技术教育与应用研究所	
电子与信息工程学院		学报编辑部	
发展规划处		学位办公室	
甘肃省高等学校外语教学指导委员会		音乐学院	
甘肃省民族音乐研究中心		饮食服务中心	
甘肃文化翻译中心		幼儿师范学院	
甘肃张芝书法院		招生网	
国际交流处		职业技能鉴定所	
国际文化翻译学院			

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
191842	站点名称: 党委宣传部	94.103.9.30	摩尔多瓦	含有非法请求参数	SQL注入	2018-05-17 10:58:00
191841	站点名称: 党委宣传部	94.103.9.30	摩尔多瓦	含有非法请求参数	SQL注入	2018-05-17 10:57:58
191840	站点名称: 党委宣传部	94.103.9.30	摩尔多瓦	含有非法请求参数	SQL注入	2018-05-17 10:57:57
191839	管理平台	10.0.108.22	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: hjgc	错误帐号或密码	2018-05-17 08:23:56
191838	管理平台	10.0.38.27	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: kyc	错误帐号或密码	2018-05-16 14:40:07
191837	管理平台	10.0.39.192	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	2018-05-15 10:38:05
191836	管理平台	10.0.133.50	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: xlyjzx	错误帐号或密码	2018-05-14 22:44:17
191835	站点名称: 兰州城市学院	182.118.33.6	河南省郑州市 奇虎360科技联节点	含有非法请求参数	SQL注入	2018-05-14 17:35:42
191834	站点名称: 兰州城市学院	182.118.33.6	河南省郑州市 奇虎360科技联节点	含有非法请求参数	SQL注入	2018-05-14 16:45:12
191833	站点名称: 兰州城市学院	182.118.33.6	河南省郑州市 奇虎360科技联节点	含有非法请求参数	SQL注入	2018-05-14 11:53:56

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
94.130.237.171	乌克兰	2018-05-22 18:46:05	2018-05-23 04:46:05
121.48.158.4	四川省成都市 电子科技大学清水河校区	2018-05-21 11:47:24	2018-05-21 21:47:24
121.48.158.9	四川省成都市 电子科技大学清水河校区	2018-05-21 11:35:41	2018-05-21 21:35:41
94.103.9.30	摩尔多瓦	2018-05-17 10:58:00	2018-05-17 20:58:00

网站群管理平台 5 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	99381	国际交流处	420
教务处	14044	教师发展中心	270
就业服务网	3867	后勤管理处	261
教育学院	3569	饮食服务中心	246
文史学院	2908	团委	216
化学与环境工程学院	2855	信息网络中心	201
外国语学院	2617	廉政网	186
音乐学院	2615	学位办公室	184
人事处	2215	城市社会心理研究中心	175
马克思主义学院	1963	甘肃文化翻译中心	171
旅游学院	1928	发展规划处	137
地理与城乡规划学院	1879	党委宣传部	131
石油工程学院	1834	国际文化翻译学院	126
幼儿师范学院	1818	基本建设处	104
电子与信息工程学院	1761	心理咨询中心	101
机械工程学院	1639	保卫处	101
商学院	1517	兰州城市学院校医院	90
数学学院	1506	卡务中心	88
财务处	1413	职业技能鉴定所	85
美术与设计学院	1395	审计	77
传媒学院	1263	学报编辑部	76
体育学院	1237	实训中心	55
科学研究处	908	甘肃省民族音乐研究中心	54
党委学生工作部	681	甘肃张芝书法院	52
学校办公室	616	机关党委	46
教学质量监测与评估中心	491	信息技术教育与应用研究所	27
党委组织部	487	电子信息科学与技术研究所	22
创新创业学院	462	甘肃省高等学校外语教学指导委员会	18
国有资产管理处	452	城市信息与系统科学研究所	3
路易艾黎研究中心	435		

网站安全检测一（360 网站安全检测）

www.lzcu.edu.cn

子域名安全状况

分享到微信

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：2分钟前

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

89%

11%

警告 高危 严重 安全

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	841.85 ms	100 %
OA办公主页【http://oa.lzcu.edu.cn】	源站监控	2	1090.76 ms	100 %
WEB【http://www.lzcu.edu.cn】	源站监控	2	404.07 ms	100 %
WEB【http://www.lzcu.edu.cn】	源站监控	2	516.28 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
2018-05-25 00:29:35	OA办公主页【http://oa.lzcu.edu.cn】	HTTP	已恢复	[异常] 连接超时	1小时3分钟
2018-05-25 00:29:34	OA办公主页【http://oa.lzcu.edu.cn】	HTTP	已恢复	[异常] 连接超时	1小时1分钟
2018-05-25 00:25:35	WEB【http://www.lzcu.edu.cn】	HTTP	已恢复	[异常] 连接超时	1小时4分钟
2018-05-25 00:17:00	WEB【http://www.lzcu.edu.cn】	HTTP	已恢复	[异常] 连接超时	1小时19分钟
2018-05-23 11:59:25	OA办公主页【http://oa.lzcu.edu.cn】	HTTP	已恢复	[异常] 连接超时	1小时36分钟
2018-05-23 11:59:25	OA办公主页【http://oa.lzcu.edu.cn】	HTTP	已恢复	[异常] 连接超时	1小时31分钟
2018-05-23 11:49:10	WEB【http://www.lzcu.edu.cn】	HTTP	已恢复	[异常] 连接超时	1小时48分钟
2018-05-23 11:49:10	WEB【http://www.lzcu.edu.cn】	HTTP	已恢复	[异常] 连接超时	1小时48分钟
2018-05-10 13:55:48	OA办公主页【http://oa.lzcu.edu.cn】	HTTP	已恢复	[异常] 响应连接被重置	7分钟
2018-05-10 13:52:13	OA办公主页【http://oa.lzcu.edu.cn】	HTTP	已恢复	[异常] 响应连接被重置	11分钟

网站安全检测二（百度云观测）



【安全教育】微信新规即将执行，网友：真的封号？腾讯：零容忍！

祥懿科技 2018-05-28 19:37:55

随着移动互联网的发展，微信已经渗透到国民生活的方方面面，据不完全统计，微信国内的用户已经超过 10 亿之多。这么多的用户，如何合理规范管理微信，已经成为了当下的重要话题。想必大家都应该碰到过网络诈骗、恶意营销、网络赌博等情况，这些行为严重影响了整个社会的和谐发展，所以必须要加以整治。



最近，腾讯将会对微信做出重大调整，将在本月 29 号正式执行生效，违规者将可能会永久封号。其实大家有目共睹，如今的微信已经成了广告、诈骗人员的天下了，伪造聊天记录、恶意营销、诱导分享等等，这些已经让不少人开始逃离了朋友圈。



本次新规的主要内容如下图所示：

1. 规范特殊识别码、口令类信息传播

为避免过度营销造成对用户的骚扰，朋友圈内不允许发布及传播具有识别、标记功能的特殊识别码、口令类信息。

2. 禁止更改用户返回路径

外部链接禁止更改用户返回路径，包括但不限于用户点击“返回”时强制跳转到非上一级页面等。

3. 禁止使用含有用户隐私数据的浮层

鉴于外部链接中使用浮层可能导致用户头像昵称等信息泄露，外链分享将禁止使用含有用户数据隐私的浮层，否则视为违规处理。

其中最重要的整治对象是微信的外部链接，想必大家最近也有注意到，很多分享在朋友圈的视频链接都无法直接打开。这是因为腾讯规定了，如果在没有获得允许的情况下，是禁止传播有试听节目的视频。对于这点，很多网友都表示不太友好，毕竟微信是每天玩最多的软件了，如果都看不到别人分享的视频链接，只能是手动下载看了。

腾讯发布最严外链公告
用户将不能在微信中分享的视频APP名单



不管怎么样吧，腾讯此次的新规，也是为了给大家营造一个良好的网络气氛。不少网友怀孕，那些经常分享低俗内容、恶意营销、诈骗钱财的人是不是真的会被封号吗？对此腾讯也表态：“零容忍”！

抄送：校领导