网络信息安全周报

【2018】第 11 期

党委宣传部
信息网络中心 编

2018 年 5 月 17 日

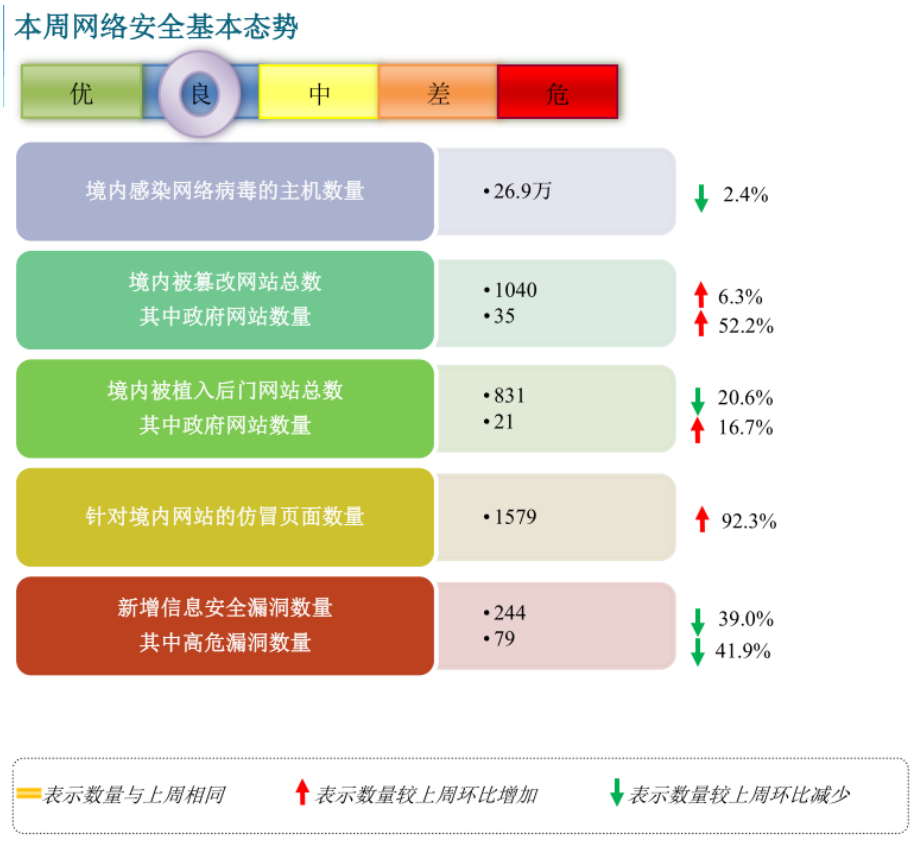
本期要目

- 【权威发布】全国网络安全信息与动态（2018 年 4 月 30 日—5 月 6 日）
- 【城院 IT】综合业务管理平台统计信息(2018 年 5 月 7 日—5 月 13 日)
- 【城院安全】网站群管理平台统计信息（2018 年 5 月 7 日—5 月 13 日）
- 【安全教育】网络安全宣传周丨习总书记的网络安全观

全国网络安全信息与动态

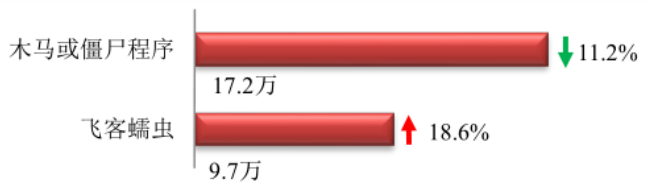
（2018 年 4 月 30 日—5 月 6 日）

根据国家互联网应急中心最新公告数据：



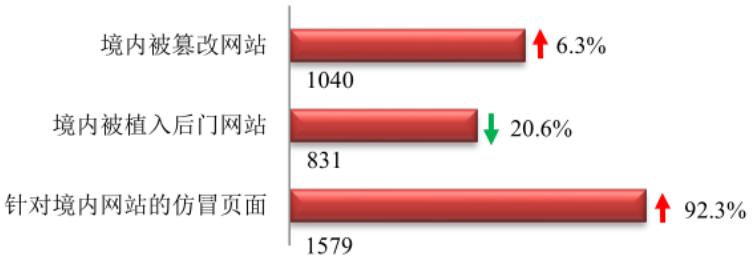
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 26.9 万个，其中包括境内被木马或被僵尸程序控制的主机约 17.2 万以及境内感染飞客（conficker）蠕虫的主机约 9.7 万。



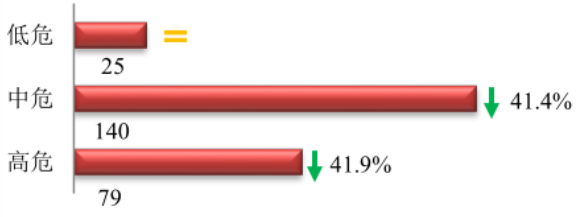
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1040 个；境内被植入后门的网站数量为 831 个；针对境内网站的仿冒页面数量为 1579。



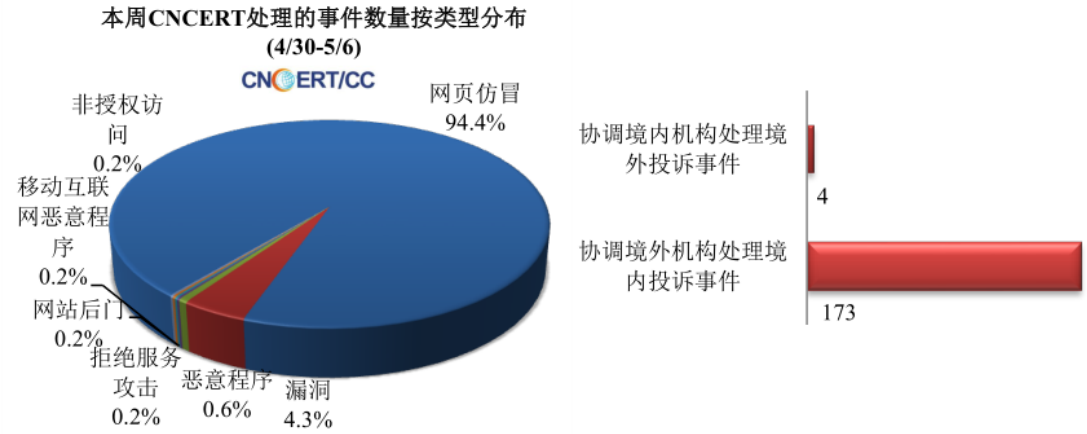
本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 244 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

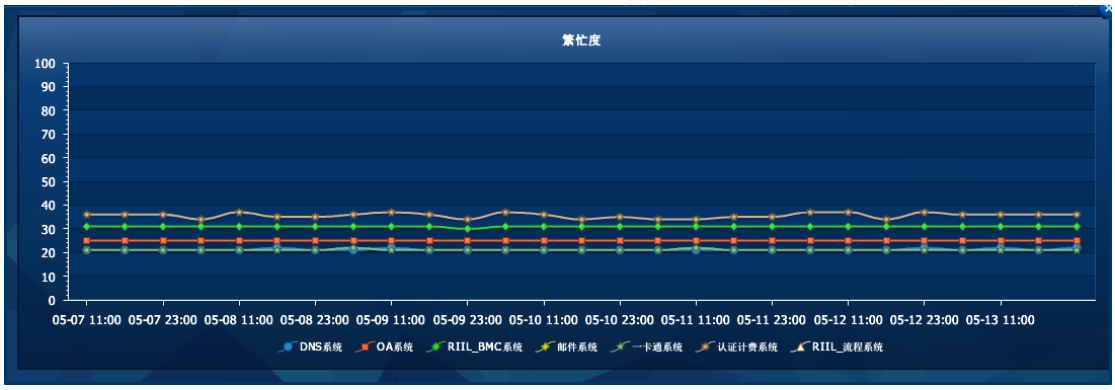
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 514 起，其中跨境网络安全事件 177 起。



城院 IT 综合业务管理平台统计信息

(2018 年 5 月 7 日—5 月 13 日)

主要业务服务繁忙度



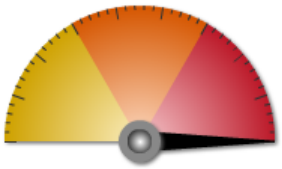
网络出口带宽情况统计

APT统计

防火墙统计	
恶意	837
检测到0-day恶意软件变种	0
可疑文件	0
安全文件	62547931

【城院安全】网站群管理平台统计信息（2018 年 5 月 7 日—5 月 13 日）

风险趋势

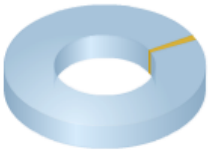


最近一周的全局风险等级为高，
在这段时间里共检测到 1010524 次攻击，其中低 25452 次，中 3755 次，高 981317 次；在以上统计中由**命令注入攻击、文件限制、爬虫**产生的告警日志较多，请关注保护站点安全及防火墙配置，详情可查看此时间段的 [**告警日志**]。

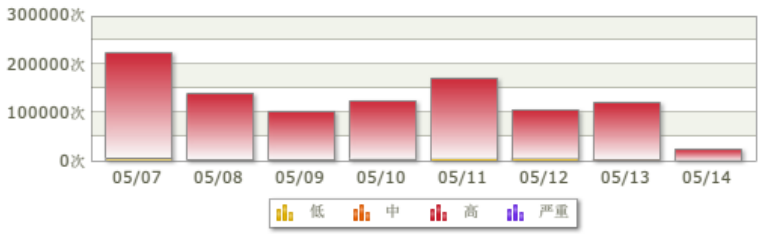
部署模式：透明代理 / 运行模式：正常模式 / 保护站点：3 个 / 规则库：2016082901

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



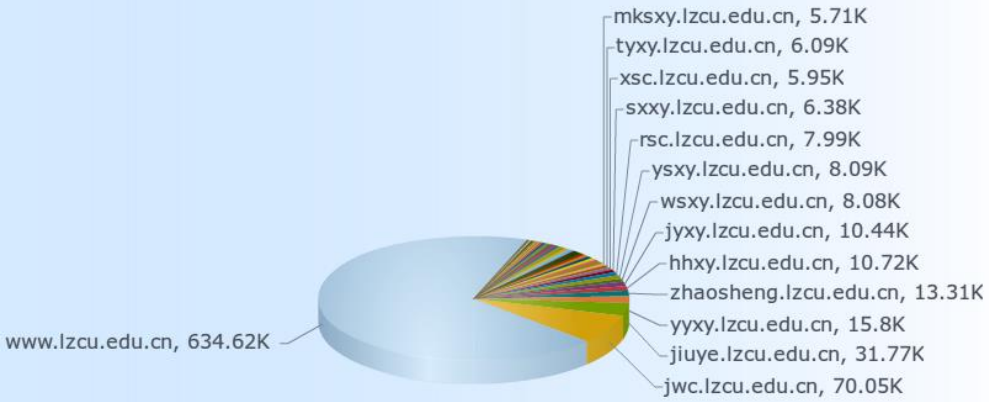
风险趋势图



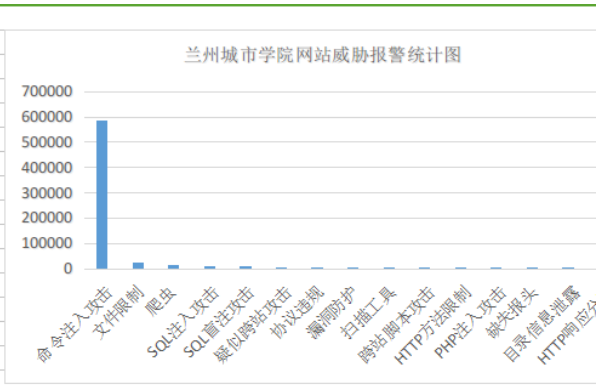
攻击类型统计(TOP)

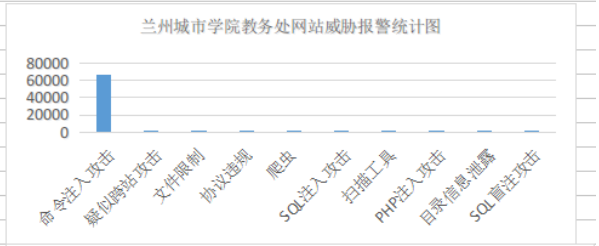
	全部 ↓	告警	阻断	重定向	放行
命令注入攻击	**924005**	923316	689	0	0
文件限制	**36691**	35320	1371	0	0
爬虫	**20350**	20143	207	0	0
其它	29572	13382	16190	0	0

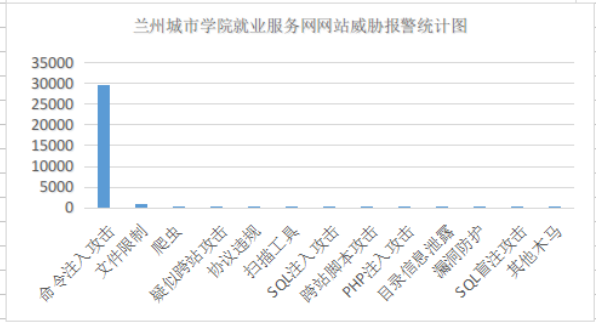
按告警主机名统计



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	584677
	文件限制	23123
	爬虫	14461
	SQL注入攻击	3297
	SQL盲注攻击	3033
	疑似跨站攻击	2023
	协议违规	1901
	漏洞防护	1373
	扫描工具	422
	跨站脚本攻击	188
	HTTP方法限制	55
	PHP注入攻击	51
	缺失报头	10
	目录信息泄露	1
	HTTP响应分割	1
jwc.lzcu.edu.cn 兰州城市学院教务处网站	命令注入攻击	67123
	疑似跨站攻击	745
	文件限制	730
	协议违规	699
	爬虫	537
	SQL注入攻击	146
	扫描工具	47
	PHP注入攻击	15
	目录信息泄露	2
	SQL盲注攻击	2
jiuye.lzcu.edu.cn 兰州城市学院就业服务网	命令注入攻击	29719
	文件限制	851
	爬虫	461
	疑似跨站攻击	354
	协议违规	309
	扫描工具	38
	SQL注入攻击	12
	跨站脚本攻击	7
	PHP注入攻击	7
	目录信息泄露	4
	漏洞防护	3
	SQL盲注攻击	2
	其他木马	1







威胁	事件	统计
高危险等级统计	命令注入攻击	852922 次
	文件限制	35143 次
	疑似跨站攻击	3989 次
	SQL注入攻击	3912 次
	SQL盲注攻击	3236 次
	漏洞防护	1666 次
	跨站脚本攻击	227 次
	HTTP方法限制	141 次
	系统命令访问攻击	95 次
	PHP注入攻击	88 次
	目录信息泄露	15 次
	HTTP响应分割	12 次
	缺失报头	8 次
	其他木马	3 次
中危险等级统计	协议违规	3602 次
低危险等级统计	爬虫	19156 次
	扫描工具	783 次
	协议违规	558 次
	缺失报头	57 次

网站群管理平台网页更新情况统计

站点名称	合计	站点名称	合计
教学质量监测与评估中心	21	发展规划处	
兰州城市学院	17	甘肃省高等学校外语教学指导委员会	
就业服务网	14	甘肃省民族音乐研究中心	
教务处	10	甘肃文化翻译中心	
党委宣传部	8	甘肃张芝书法院	
马克思主义学院	7	国际交流处	
音乐学院	7	国际文化翻译学院	
幼儿师范学院	4	国有资产管理处	
党委（校长）办公室	3	后勤管理处	
廉政网	3	机关党委	
财务处	2	基本建设处	
教育学院	2	教师发展中心	
数学学院	2	教育学院	
团委	2	卡务中心	
文史学院	2	科学研究处	
传媒学院	1	兰州城市学院校医院	
党委学生工作部	1	美术与设计学院	
电子与信息工程学院	1	人事处	
化学与环境工程学院	1	商学院	
机械工程学院	1	审计处	
路易艾黎研究中心	1	石油工程学院	
旅游学院	1	实训中心	
信息网络中心	1	体育学院	
饮食服务中心	1	外国语学院	
保卫处		网络报修	
城市社会心理研究中心		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	
创新创业学院		学报编辑部	
档案馆		学位办公室	
党委组织部		音乐研究中心	
地理与城乡规划学院		招生网	
电子信息科学与技术研究所		职业技能鉴定所	

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
191828	管理平台	10.0.76.54	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： mzyy	错误帐号或密码	2018-05-11 15:54:24
191827	站点名称：教务处	10.0.111.99	局域网 对方和您在同一内部网	含有非法请求参数	SQL注入	2018-05-11 10:27:12
191826	站点名称：教务处	10.0.111.99	局域网 对方和您在同一内部网	含有非法请求参数	SQL注入	2018-05-11 10:27:12
191825	站点名称：教务处	10.0.111.99	局域网 对方和您在同一内部网	含有非法请求参数	SQL注入	2018-05-11 10:27:12
191824	站点名称：兰州城市学院	106.117.15.84	河北省石家庄市 电信	含有非法请求参数	SQL注入	2018-05-11 07:53:45
191823	站点名称：兰州城市学院	106.117.15.84	河北省石家庄市 电信	含有非法请求参数	SQL注入	2018-05-11 07:53:45
191822	站点名称：兰州城市学院	106.117.15.84	河北省石家庄市 电信	含有非法请求参数	SQL注入	2018-05-11 07:53:45
191821	站点名称：兰州城市学院	106.117.15.84	河北省石家庄市 电信	含有非法请求参数	SQL注入	2018-05-11 07:34:13
191820	管理平台	10.0.122.101	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： dwbgs	错误帐号或密码	2018-05-10 15:42:53
191819	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： nic	错误帐号或密码	2018-05-08 15:21:37
191818	管理平台	206.189.35.123	美国	登录位置：站群管理； 登录账号： admin	错误帐号或密码	2018-05-07 19:25:09
191817	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	2018-05-07 16:11:13
191816	站点名称：职业技能鉴定所	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-05-07 03:11:23
191815	站点名称：职业技能鉴定所	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-05-07 03:11:22
191814	站点名称：职业技能鉴定所	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-05-07 03:09:11

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
10.0.111.99	局域网 对方和您在同一内部网	2018-05-11 10:27:12	2018-05-11 20:27:12
106.117.15.84	河北省石家庄市 电信	2018-05-11 07:53:45	2018-05-11 17:53:45
110.87.188.33	福建省福州市 电信	2018-05-07 03:11:23	2018-05-07 13:11:23

网站群管理平台 5 月份网站累计访问次数

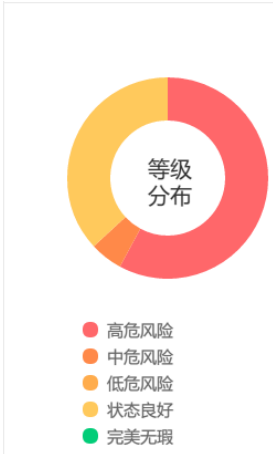
站点名称	访问次数	站点名称	访问次数
兰州城市学院	36723	饮食服务中心	103
教务处	6913	后勤管理处	103
就业服务网	1193	教师发展中心	92
教育学院	1189	党委组织部	87
化学与环境工程学院	983	信息网络中心	83
文史学院	968	学报编辑部	76
幼儿师范学院	929	城市社会心理研究中心（新）	76
音乐学院	809	甘肃文化翻译中心	70
人事处	722	团委	68
外国语学院	722	廉政网	66
马克思主义学院	657	保卫处	65
数学学院	625	学位办公室	63
机械工程学院	585	职业技能鉴定所	55
电子与信息工程学院	517	审计	51
旅游学院	514	心理咨询中心	46
财务处	482	党委宣传部	36
石油工程学院	454	基本建设处	36
体育学院	452	实训中心	35
美术与设计学院	431	卡务中心	33
传媒学院	429	发展规划处	29
商学院	419	兰州城市学院校医院	26
党委学生工作部	309	甘肃张芝书法院	21
国有资产管理处	260	电子信息科学与技术研究所	13
地理与城乡规划学院	257	机关党委	9
科学研究处	250	信息技术教育与应用研究所	4
教学质量监测与评估中心（新）	216	城市信息与系统科学研究所	2
创新创业学院	200	国际文化翻译学院	1
路易艾黎研究中心	187	甘肃省民族音乐研究中心	1
党委（校长）办公室	154	国际交流处	1

网站安全检测一（360 网站安全检测）

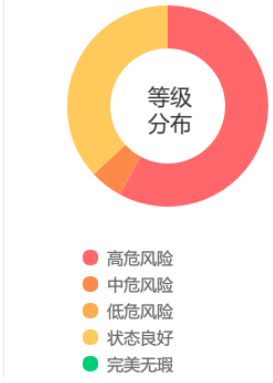
监控对象	类型	监测点	响应时间	访问成功率	
OA办公主页【http://oa.lzcu.edu.cn】	源站监控	2	502.69 ms	100 %	详情
OA办公主页【http://oa.lzcu.edu.cn】	源站监控	2	465.02 ms	100 %	详情
WEB【http://www.lzcu.edu.cn】	源站监控	2	310.21 ms	100 %	详情
WEB【http://www.lzcu.edu.cn】	源站监控	2	496.03 ms	100 %	详情

	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
+	2018-05-10 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
+	2018-05-10 13:33:54	WEB【http://www.lzcu.edu.cn】	HTTP	已恢复	[异常] 响应连接被重置	2小时6分钟
+	2018-05-10 12:57:12	OA办公主页【http://oa.lzcu.edu.cn】	HTTP	已恢复	[异常] 响应连接被重置	20分钟
+	2018-05-10 12:52:31	OA办公主页【http://oa.lzcu.edu.cn】	HTTP	已恢复	[异常] 响应连接被重置	24分钟
+	2018-05-10 12:43:56	WEB【http://www.lzcu.edu.cn】	HTTP	已恢复	[异常] 响应连接被重置	38分钟
+	2018-05-10 12:17:26	OA办公主页【http://oa.lzcu.edu.cn】	HTTP	已恢复	[异常] 响应连接被重置	10分钟
+	2018-05-10 12:17:25	OA办公主页【http://oa.lzcu.edu.cn】	HTTP	已恢复	[异常] 响应连接被重置	10分钟
+	2018-05-10 12:13:55	WEB【http://www.lzcu.edu.cn】	HTTP	已恢复	[异常] 响应连接被重置	20分钟
+	2018-05-10 12:12:14	WEB【http://www.lzcu.edu.cn】	HTTP	已恢复	[异常] 响应连接被重置	3小时21分钟

网站安全检测二（百度云观测）



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	34 高危	查看详情>>
kyc.lzcu.edu.cn	34 高危	查看详情>>

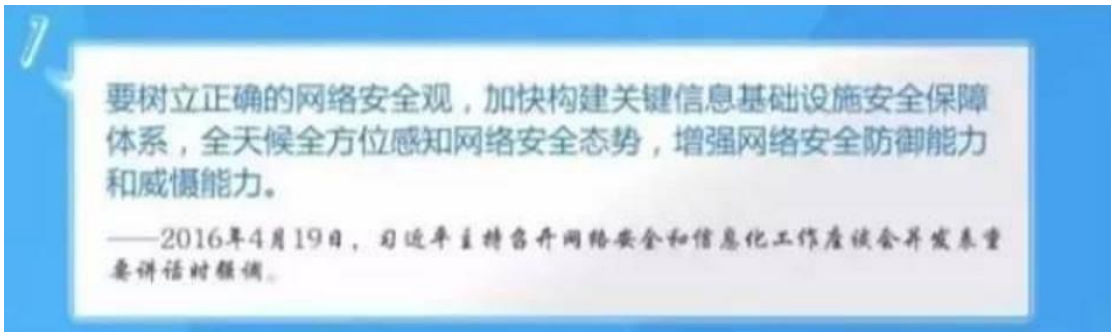


域名	指数评价	操作
lzcu.edu.cn	80 良好	查看详情>>
nic.lzcu.edu.cn	90 良好	查看详情>>
oa.lzcu.edu.cn	84 良好	查看详情>>
old.lzcu.edu.cn	44 中危	查看详情>>
pop.lzcu.edu.cn	0 高危	查看详情>>
smtp.lzcu.edu.cn	0 高危	查看详情>>
syzz.lzcu.edu.cn	4 高危	查看详情>>
test.lzcu.edu.cn	84 良好	查看详情>>
www2.lzcu.edu.cn	4 高危	查看详情>>

【安全教育】网络安全宣传周丨习总书记的网络安全观

版纳网警巡查执法 2017-06-01 16:31:29

2017 年 2 月 17 日，习近平总书记主持召开国家安全工作座谈会时进一步强调：“要突出抓好政治安全、经济安全、国土安全、社会安全、网络安全等各方面安全工作”“要筑牢网络安全防线，提高网络安全保障水平，强化关键信息基础设施防护，加大核心技术研发力度和市场化引导，加强网络安全预警监测，确保大数据安全，实现全天候全方位感知和有效防护”“要加大对维护国家安全所需的物质、技术、装备、人才、法律、机制等保障方面的能力建设，更好适应国家安全工作需要。



2

大国网络安全博弈，不单是技术博弈，还是理念博弈、话语权博弈。我们提出了全球互联网发展治理的“四项原则”、“五点主张”，特别是我们倡导尊重网络主权、构建网络空间命运共同体，赢得了世界绝大多数国家赞同。

——2016年4月19日，习近平主持召开网络安全和信息化工作座谈会并发表重要讲话时强调。

3

今年是“十三五”开局之年，网络安全和信息化工作是“十三五”时期的重头戏。希望同志们积极投身网络强国建设，更好发挥网信领域企业家、专家学者、技术人员作用，支持他们为实现全面建成小康社会、实现中华民族伟大复兴的中国梦作出更大的贡献！

——2016年4月19日，习近平主持召开网络安全和信息化工作座谈会并发表重要讲话时强调。

4

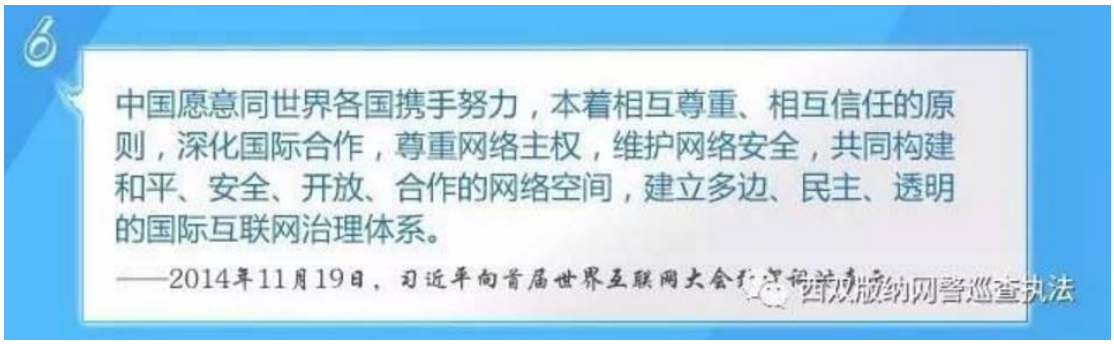
当今时代，社会信息化迅速发展，一个安全、稳定、繁荣的网络空间，对一国乃至世界和平与发展越来越具有重大意义。中国倡导建设和平、安全、开放、合作的网络空间，主张各国制定符合自身国情的互联网公共政策。

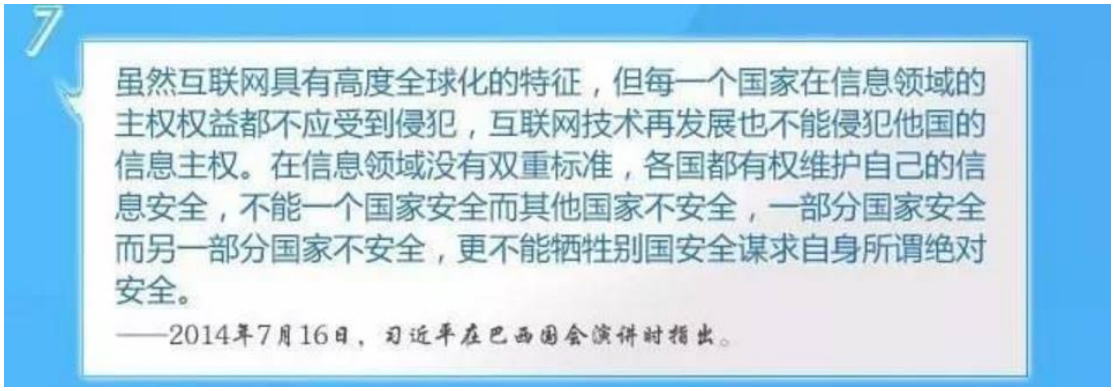
——2015年9月23日，习近平会见参加第八届中美互联网论坛的双方代表时强调。

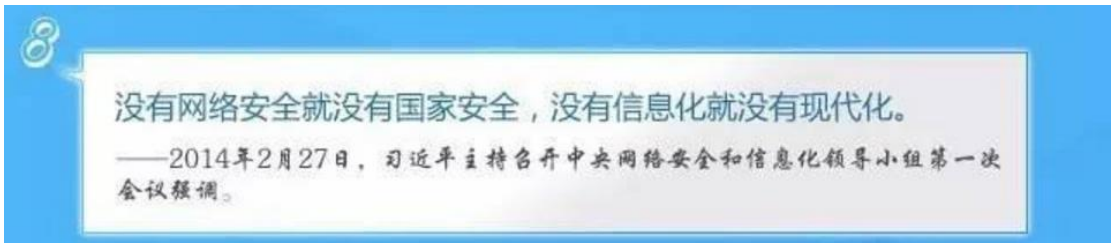
5

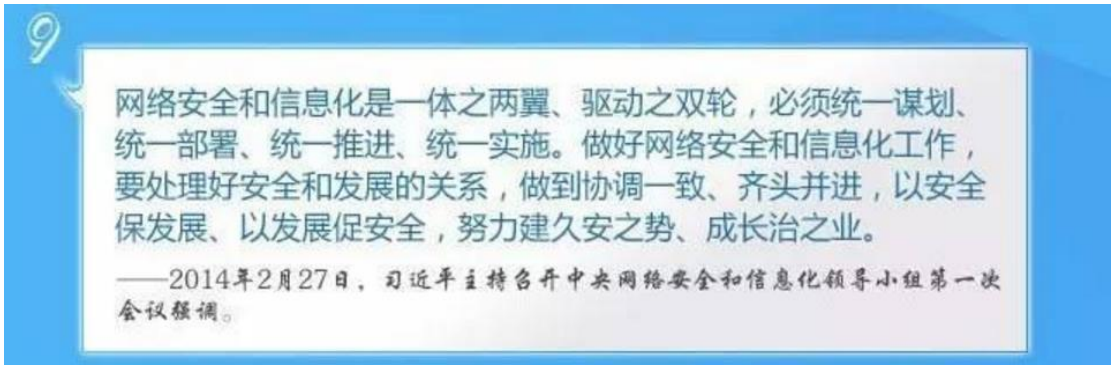
互联网作为20世纪最伟大的发明之一，把世界变成了“地球村”，深刻改变着人们的生产生活，有力推动着社会发展，具有高度全球化的特性。但是，这块“新疆域”不是“法外之地”，同样要讲法治，同样要维护国家主权、安全、发展利益。

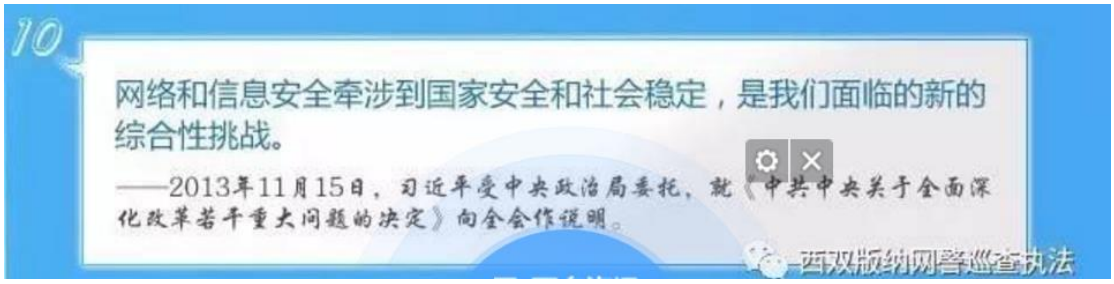
——2015年9月22日，习近平接受《华尔街日报》书面采访时指出。


6
中国愿意同世界各国携手努力，本着相互尊重、相互信任的原则，深化国际合作，尊重网络主权，维护网络安全，共同构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的国际互联网治理体系。
——2014年11月19日，习近平向首届世界互联网大会
西双版纳网警巡查执法


7
虽然互联网具有高度全球化的特征，但每一个国家在信息领域的主权权益都不应受到侵犯，互联网技术再发展也不能侵犯他国的信息主权。在信息领域没有双重标准，各国都有权维护自己的信息安全，不能一个国家安全而其他国家不安全，一部分国家安全而另一部分国家不安全，更不能牺牲别国安全谋求自身所谓绝对安全。
——2014年7月16日，习近平在巴西国会演讲时指出。


8
没有网络安全就没有国家安全，没有信息化就没有现代化。
——2014年2月27日，习近平主持召开中央网络安全和信息化领导小组第一次会议强调。


9
网络安全和信息化是一体之两翼、驱动之双轮，必须统一谋划、统一部署、统一推进、统一实施。做好网络安全和信息化工作，要处理好安全和发展的关系，做到协调一致、齐头并进，以安全保发展、以发展促安全，努力建久安之势、成长治之业。
——2014年2月27日，习近平主持召开中央网络安全和信息化领导小组第一次会议强调。


10
网络和信息安全牵涉到国家安全和社会稳定，是我们面临的新的综合性挑战。
——2013年11月15日，习近平受中央政治局委托，就《中共中央关于全面深化改革若干重大问题的决定》向全会作说明。
西双版纳网警巡查执法

抄送：校领导