网络信息安全周报

【2018】第 14 期

党委宣传部
信息网络中心 编

2018 年 6 月 7 日

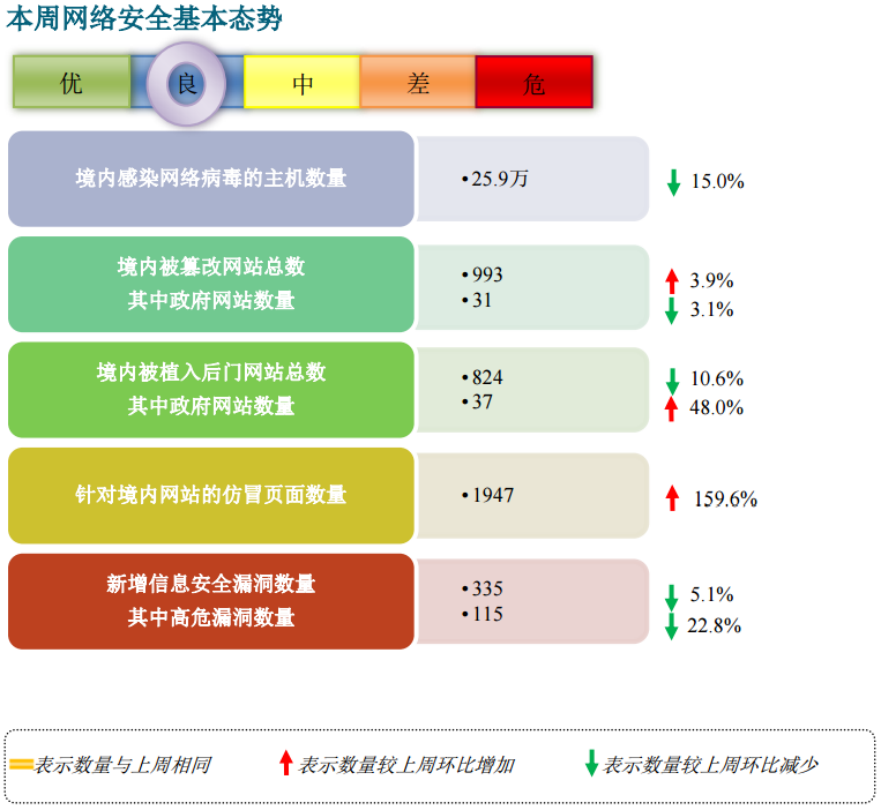
本期要目

- 【权威发布】全国网络安全信息与动态（2018 年 5 月 21 日—5 月 27 日）
- 【城院 IT】综合业务管理平台统计信息(2018 年 5 月 28 日—6 月 3 日)
- 【城院安全】网站群管理平台统计信息（2018 年 5 月 28 日—6 月 3 日）
- 【安全教育】人民日报整版讨论：奋力推进网络强国建设

全国网络安全信息与动态

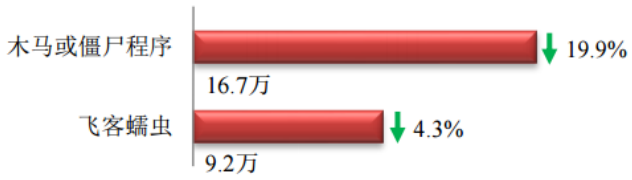
（2018 年 5 月 21 日—5 月 27 日）

根据国家互联网应急中心最新公告数据：



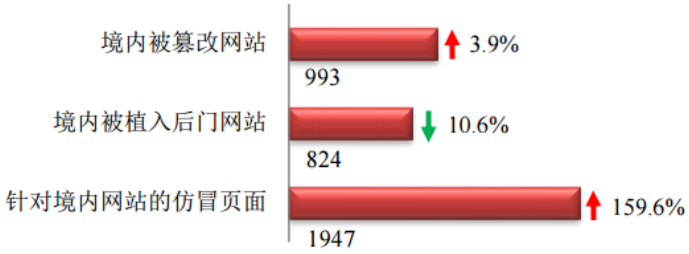
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 25.9 万个，其中包括境内被木马或被僵尸程序控制的主机约 16.7 万以及境内感染飞客（conficker）蠕虫的主机约 9.2 万。



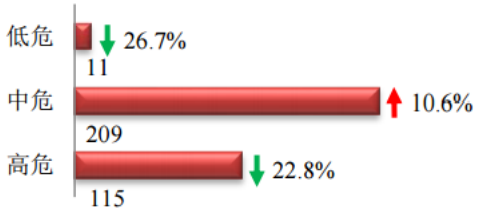
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 993 个；境内被植入后门的网站数量为 824 个；针对境内网站的仿冒页面数量为 1947。



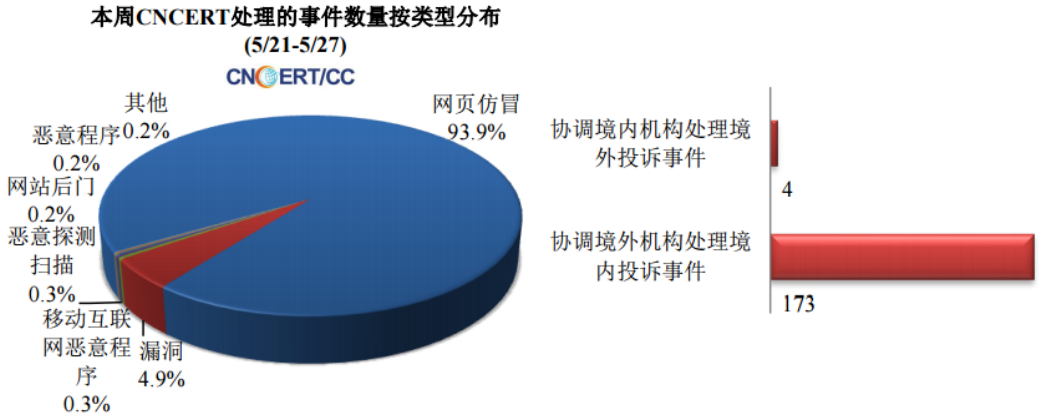
本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 335 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

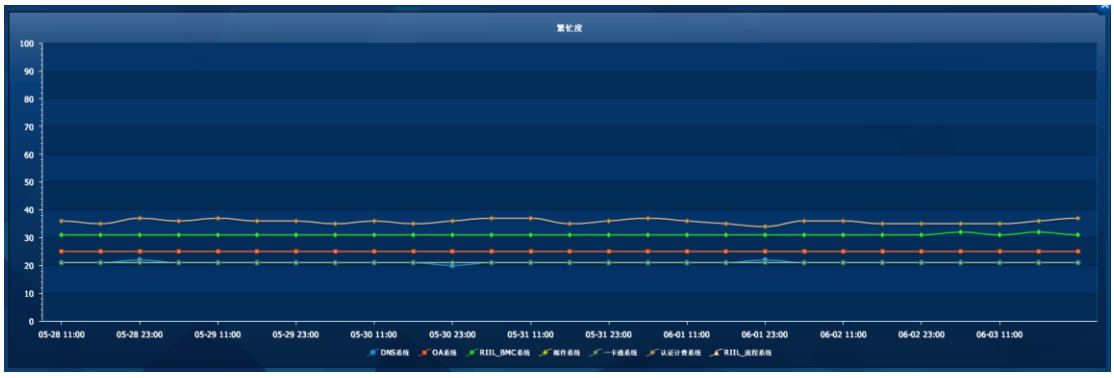
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 595 起，其中跨境网络安全事件 177 起。



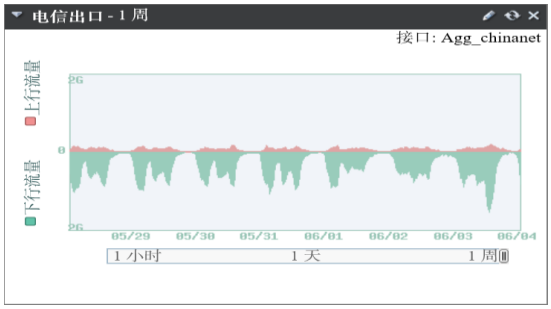
城院 IT 综合业务管理平台统计信息

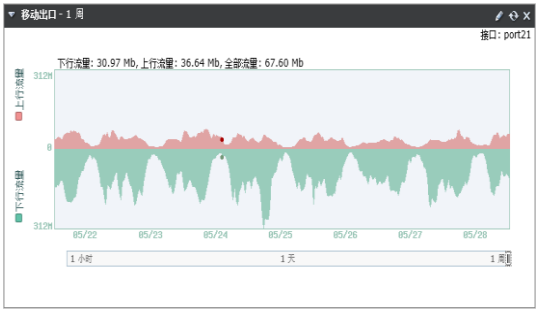
(2018 年 5 月 28 日—6 月 3 日)

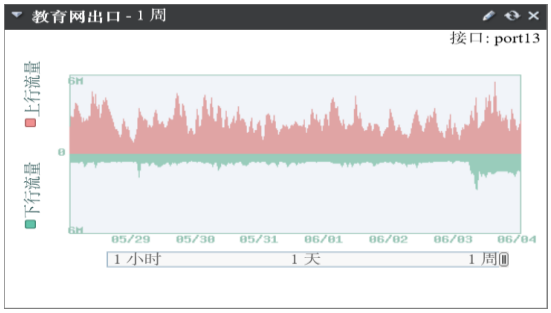
主要业务服务繁忙度

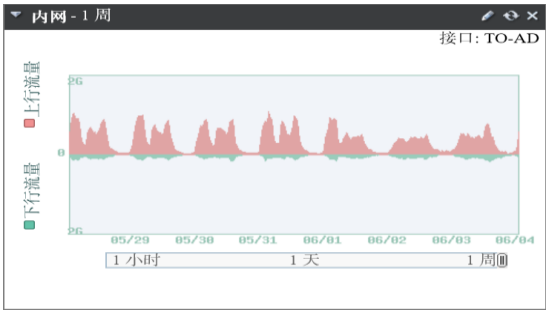


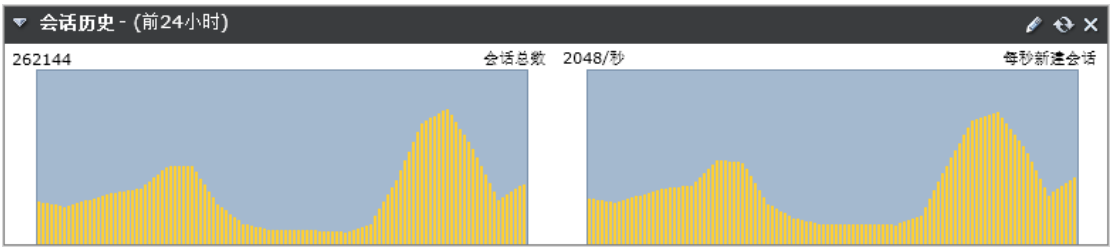
网络出口带宽情况统计









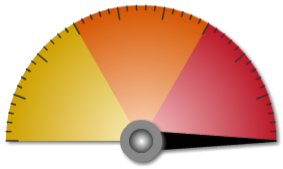


APT统计

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 5 月 28 日—6 月 3 日）

风险趋势

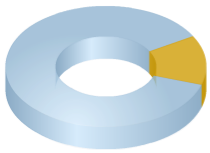


最近一周的全局风险等级为高，
在这段时间里共检测到 1275563 次攻击，其中低 44328 次，中 3194 次，高 1228041 次；在以上统计中由命令注入攻击、文件限制、爬虫产生的告警日志较多，请关注保护站点安全及防火墙配置，详情可查看此时间段的 [告警日志]。

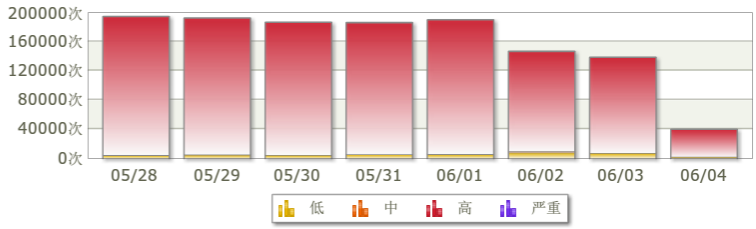
部署模式：透明代理 / 运行模式：正常模式 / 保护站点：3 个 / 规则库：2016082901

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...



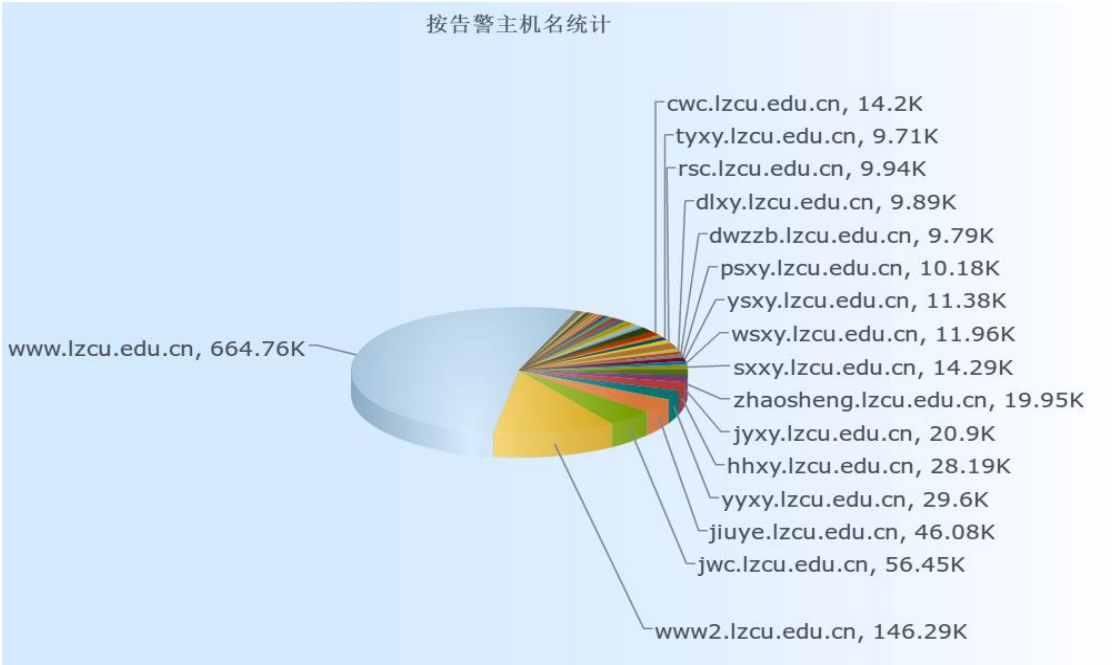
风险...



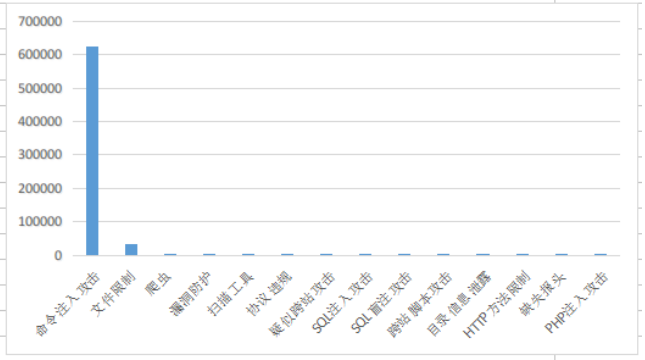
攻击类型统计(T...

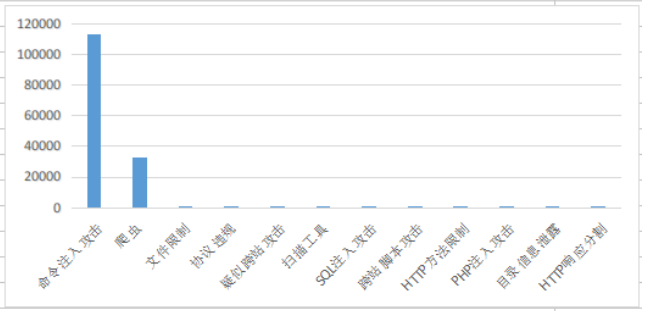
	全部 ↓	告警	阻断	重定向	放行
命令注入攻击	**1140130**	1140090	40	0	0
文件限制	**48892**	48431	461	0	0
爬虫	**39642**	39412	230	0	0
其它	13978	3829	10149	0	0

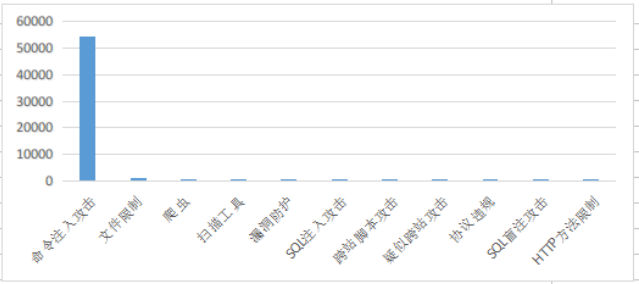
按告警主机名统计



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	625795
	文件限制	31536
	爬虫	3997
	漏洞防护	822
	扫描工具	806
	协议违规	709
	疑似跨站攻击	383
	SQL注入攻击	371
	SQL盲注攻击	283
	跨站脚本攻击	30
	目录信息泄露	15
	HTTP方法限制	9
	缺失报头	5
	PHP注入攻击	2
www2.lzcu.edu.cn 兰州城市学院备份网站	命令注入攻击	113122
	爬虫	33005
	文件限制	48
	协议违规	48
	疑似跨站攻击	29
	扫描工具	25
	SQL注入攻击	3
	跨站脚本攻击	3
	HTTP方法限制	2
	PHP注入攻击	2
	目录信息泄露	2
	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	54246
	文件限制	1179
	爬虫	826
	扫描工具	69
	漏洞防护	50
	SQL注入攻击	33
	跨站脚本攻击	13
	疑似跨站攻击	11
	协议违规	10
	SQL盲注攻击	7
	HTTP方法限制	4







威胁	事件	统计
高危险等级	命令注入攻击	1147532 次
	文件限制	49024 次
	SQL注入攻击	2235 次
	漏洞防护	2021 次
	SQL盲注攻击	1173 次
	疑似跨站攻击	790 次
	跨站脚本攻击	357 次
	HTTP方法限制	82 次
	HTTP响应分割	29 次
	目录信息泄露	24 次
	缺失报头	7 次
	PHP注入攻击	4 次
	系统命令访问攻	1 次
中危险等级	协议违规	3154 次
低危险等级	爬虫	41022 次
	扫描工具	2292 次
	协议违规	1943 次
	缺失报头	108 次
	漏洞防护	7 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	25	甘肃文化翻译中心	
教学质量监测与评估中心	18	甘肃张芝书法院	
就业服务网	13	国际交流处	
音乐学院	11	国际文化翻译学院	
党委宣传部	10	国有资产管理处	
外国语学院	6	后勤管理处	
教育学院	4	机关党委	
教务处	3	机械工程学院	
科学研究处	3	基本建设处	
饮食服务中心	3	教师发展中心	
甘肃省民族音乐研究中心	2	卡务中心	
化学与环境工程学院	2	兰州城市学院校医院	
创新创业学院	1	廉政网	
发展规划处	1	路易艾黎研究中心	
旅游学院	1	美术与设计学院	
马克思主义学院	1	人事处	
数学学院	1	商学院	
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		体育学院	
城市信息与系统科学研究所		团委	
传媒学院		文史学院	
档案馆		心理咨询中心	
党委（校长）办公室		信息技术教育与应用研究所	
党委学生工作部		学报编辑部	
党委组织部		学位办公室	
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	
电子与信息工程学院		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

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
191882	站点名称：兰州城市学院	101.226.68.215	上海市 电信	含有非法请求参数	SQL注入	2018-06-03 03:36:55
191881	站点名称：财务处	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-06-01 21:38:18
191880	站点名称：财务处	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-06-01 21:38:18
191879	站点名称：财务处	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-06-01 21:38:18
191878	站点名称：路易艾黎研究中心	36.7.154.41	安徽省合肥市 电信	含有非法请求参数	跨站脚本注入	2018-06-01 10:45:42
191877	站点名称：卡务中心	36.5.154.111	安徽省合肥市 电信	含有非法请求参数	跨站脚本注入	2018-06-01 10:39:55
191876	站点名称：兰州城市学院	36.5.154.111	安徽省合肥市 电信	含有非法请求参数	跨站脚本注入	2018-06-01 10:39:54
191875	站点名称：财务处	36.5.154.111	安徽省合肥市 电信	含有非法请求参数	跨站脚本注入	2018-06-01 10:39:53
191874	管理平台	10.0.25.164	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	2018-05-31 09:52:53
191873	管理平台	10.0.77.10	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： fzghc	错误帐号或密码	2018-05-30 08:44:20
191866	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	2018-05-28 16:09:18
191865	管理平台	10.0.65.60	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	2018-05-28 16:05:54

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
110.87.188.33	福建省福州市 电信	2018-06-01 21:38:18	2018-06-02 07:38:18
36.5.154.111	安徽省合肥市 电信	2018-06-01 10:39:55	2018-06-01 20:39:55

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	9831		团委	44
教务处	1214		国有资产管理处	43
化学与环境工程学院	661		后勤管理处	40
就业服务网	583		国际交流处	38
教育学院	452		基本建设处	37
音乐学院	414		饮食服务中心	37
石油工程学院	389		发展规划处	36
体育学院	379		创新创业学院	34
地理与城乡规划学院	374		党委宣传部	33
财务处	366		甘肃省民族音乐研究中心	28
文史学院	357		学位办公室	27
教育学院	353		廉政网	27
机械工程学院	307		城市信息与系统科学研究所	24
旅游学院	291		心理咨询中心	17
数学学院	274		路易艾黎研究中心	16
电子与信息工程学院	258		信息技术教育与应用研究所	14
人事处	216		审计	13
幼儿师范学院	208		城市社会心理研究中心	9
美术与设计学院	202		甘肃张芝书法院	7
传媒学院	151		信息网络中心	3
马克思主义学院	147		甘肃文化翻译中心	2
教学质量监测与评估中心	143		电子信息科学与技术研究所	2
外国语学院	127		兰州城市学院校医院	2
商学院	101		职业技能鉴定所	2
党委组织部	93		保卫处	2
党委学生工作部	71		机关党委	2
学校办公室	60		甘肃省高等学校外语教学指导委员会	1
科学研究处	55		卡务中心	1
教师发展中心	51			

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：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

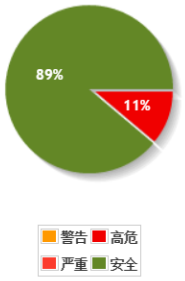
黑客篡改网站监控

正常

网站敏感内容监控

正常

www.lzcu.edu.cn　子域名安全状况



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	515.27 ms	100 %	详情
OA办公主页【http://oa.lzcu.edu.cn】	源站监控	2	525.91 ms	100 %	详情
WEB【http://www.lzcu.edu.cn】	源站监控	2	358.12 ms	100 %	详情
WEB【http://www.lzcu.edu.cn】	源站监控	2	451.9 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
2018-05-25 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）

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	4 高危	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】人民日报整版讨论：奋力推进网络强国建设

甘州在线 2018-06-04 08:31:59

信息化为中华民族带来了千载难逢的机遇，决不能同这样的历史机遇失之交臂。在全国网络安全和信息化工作会议上，习近平同志发表重要讲话，站在人类历史发展与党和国家全局高度，科学分析了信息化变革给我们带来的机遇和挑战，深入阐述了网络强国战略思想，明确了网络强国建设的战略目标、原则要求以及互联网发展治理的中国主张。如何深入贯彻习近平网络强国战略思想，推动信息领域核心技术突破？如何发挥数字经济的引领作用？如何主动参与网络空间国际治理进程？本期观察版围绕这些问题展开讨论。

——编 者

在核心技术领域实现突破（人民观察）

田 丽

建设网络强国，是以习近平同志为核心的党中央准确把握信息时代特征提出的战略目标。近年来，我国网信事业发展取得重大成就，但信息领域所掌握的核心技术同世界先进水平相比仍有不小差距，这成为我国网信事业发展的重要制约。突破并掌握核心技术既是建设网络强国的重要内容，也是建成网络强国的必由之路。习近平同志指出，核心技术是国之重器。要下定决心、保持恒心、找准重心，加速推动信息领域核心技术突破。我们必须下大力气把核心技术的命门掌握在自己手里，努力实现核心技术突破，并打造出可持续发展和良性循环的产业链、生态链、价值链，为网络强国建设打下扎实根基。

核心技术是国之重器

信息革命给人类社会带来了生产力质的飞跃和生产关系的深刻调整，与农业革命、工业革命相比较，其覆盖范围更广泛、影响更深远。如今，互联网广泛渗透到经济、政治、文化、社会、生态、军事等各领域。一个国家在网络空间的掌控力、竞争力如何，已成为判断其综合国力和国际竞争力的重要标准。

党的十八大以来，以习近平同志为核心的党中央把信息化作为我国抢占新一轮发展制高点、构筑国际竞争新优势的契机，对信息化相关的重大理论和实践问题作出科学回答，形成了网络强国战略思想，指引我国网信事业取得历史性成就。但应清醒看到，我国虽已是网络大国，但同网络强国相比还有一定差距。近年来，我国高度重视核心技术发展，在高性能计算、量子通信、5G 等一些领域取得了突破，但核心技术受制于人的状况尚未得到根本改变。

信息化为中华民族带来了千载难逢的机遇。抓住这一历史机遇，必须掌握信息领域核心技术这一国之重器，实现核心技术突破。这不仅是提升国家竞争力的需要，更是维护国家战略安全的根基。对核心技术的掌握能力，决定着一个国家的网络安全能力、建设水平和综合治理能力。有效运用互联网促进社会治理，让人民群众共享网信事业发展成果，必须紧紧抓住核心技术自主创新这个“牛鼻子”，构建高水平的、安全可控的信息技术体系。

认识和把握技术发展规律

技术创新和发展有其自身规律，认识和把握这些规律是实现信息领域核心技术突破的首要之举。

维护安全和追求效益是信息技术发展的驱动力。维护安全是技术变革的一大动力。人类历史上很多颠覆性技术都是在维护国家安全、军事安全的需要下产生的。互联网的前身——阿帕网就是为解决通信安全问题而设计出来的。而推动互联网真正普及的，则是大量商业网站的接入和网络服务商的出现。维护安全和追求效益两种力量交互作用、交替推进，持续刺激信息技术推陈出新。

信息技术发展以系统生态更新迭代为特征。以往，技术发展呈现线性连锁特征。某一方面的技术突破会依次传导创新动力，引起其他相关领域的技术发展。信息领域核心技术发展则是以系统生态更新迭代为特征。生态更新的技术创新模式，意味着信息领域核心技术突破未必需要沿袭传统的追赶超越战略，有可能通过系统生态的迭代实现弯道超车。

公共政策对信息技术创新具有明显的催化作用。政府的政策引导、资源投入以及服务监管对技术创新具有深远影响。纵观发达国家的科技创新实践，政府通常都起到了强大的行政推动和政策引导作用。比如，在不同时期制定不同的科技发展规划，确定不同的创新重点，为创新提供税收政策、金融政策等支持。

领军企业是信息技术发展的主力军。从发达国家的经验来看，最新的核心技术通常诞生在领军企业中。企业追求经济效益，由企业作为技术引进和转化开发的主体，可以保证技术创新的主动性和高效性，并在成功提升经济效益的基础上，形成增加技术创新投入的良性循环。领军企业将知识发现进行技术化开发、市场化扩散、资本化运作，成为推动信息技术突破的重要力量。

立足国情实现技术突破

改革开放 40 年来，我国科学技术水平显著提升。基础研究和前沿技术实现多点突破、群体跃升，在众多领域取得一批具有世界影响的重大成果，科技支撑引领能力显著增强。同时也应看到，我们在信息领域还有一些核心技术尚未掌握。在遵循技术创新发展规律的基础上，要立足我国国情，下大力气突破信息领域核心技术，建设数字中国，让信息化成为经济社会发展的引擎。

以习近平网络强国战略思想为引领。习近平网络强国战略思想是我们党不断推进理论创新和实践创新的科学成果，科学回答了事关网信事业长远发展的一系列重大理论和实践问题，为把握信息革命历史机遇、加强网络安全和信息化工作、加快推进网络强国建设明确了前进方向、提供了根本遵循。核心技术上要取得更大进步，实践中就要贯彻落实习近平网络强国战略思想，抢抓信息化发展的历史机遇，正确处理开放与自主、安全与发展的关系，坚定不移走出一条中国特色网络发展之道。

加大基础科学研究投入。信息技术在我国的发展，最初源于强大的市场驱动力。因此，基础性、关键性信息技术研发不够充分。随着网络应用普及和影响力提升，信息技术领域基础科学研究薄弱会对我国网信事业发展产生制约。今后，要在基础科学研究领域加大人力和物力投入，强化基础科学研究的支撑作用，打通基础研究和技术创新衔接的绿色通道，力争以基础研究带动应用技术群体突破。

提升企业技术创新能力。如今，一大批颇具竞争力的中国网信企业异军突起，取得了骄人成绩。中国庞大的网民基数所产生的技术人口红利以及比较优越的政策环境在其中起到主要作用。应当看到，我国网信企业的原始技术创新能力还不强，缺乏技术创新规划。一些网信企业过分关注市场布局，而不是核心技术积累。如果仅仅依靠庞大市场而不是靠掌握核心技术来赚钱，形成这种发展惯性就可能导致技术创新动力不足，不利于企业核心竞争力的增强。因此，要继续完善金融、

财税、国际贸易、人才、知识产权保护等制度，优化市场环境，更好释放各类创新主体的活力。

营造激发技术创新的政策环境。实现核心技术突破，政府可以发挥更为积极的政策引导作用，实现管理方式由粗放型向精准型、节约型转变。推动建立和完善适应企业技术创新和协同发展的治理方式，形成有利于技术交流和深化研发的产业平台与市场机制，引导企业通过资本、人才、项目合作的方式加入全球创新体系。同时，继续改革高校及科研单位技术创新管理方式，激活技术思维，营造创新文化，对基础性、颠覆性技术突破给予更多宽容和支持，让不同创新主体的能量最大程度地发挥出来。

立足全球产业链和价值链谋划核心技术的突破口与着力点。信息技术产业内部是一套完整的、紧密关联的生态系统。例如，集成电路产业链包括原材料、设备、设计、制造和封测等许多部分。每一部分又包括诸多细分领域。通过加强对全球产业链和价值链的分析，寻找其中的关键环节，重点研究未来技术和未来产业，汇聚战略资源集中攻关，我们就有可能实现后来居上，以基础技术突破占领下一代技术生态系统的起点和基线，从根本上提升对产业链的控制力和对价值链的作用力，推进技术系统生态的更新迭代，完成核心技术的跨越式发展。

实现核心技术突破不会在历史等待中自动完成，不会在市场交易中自发实现，需要我们增强紧迫感和使命感，马不停蹄继续追赶下去。在党中央坚强领导下，坚持以习近平网络强国战略思想为指导，奋力推进网络强国建设，我们就一定能够把握信息时代主动权，赢得中华民族的光辉未来。

（作者为北京大学互联网发展研究中心主任）

《 人民日报 》（ 2018 年 06 月 04 日 16 版）

抄送：校领导