网络信息安全周报

【2018】第 5 期

党委宣传部
信息网络中心 编

2018 年 4 月 5 日

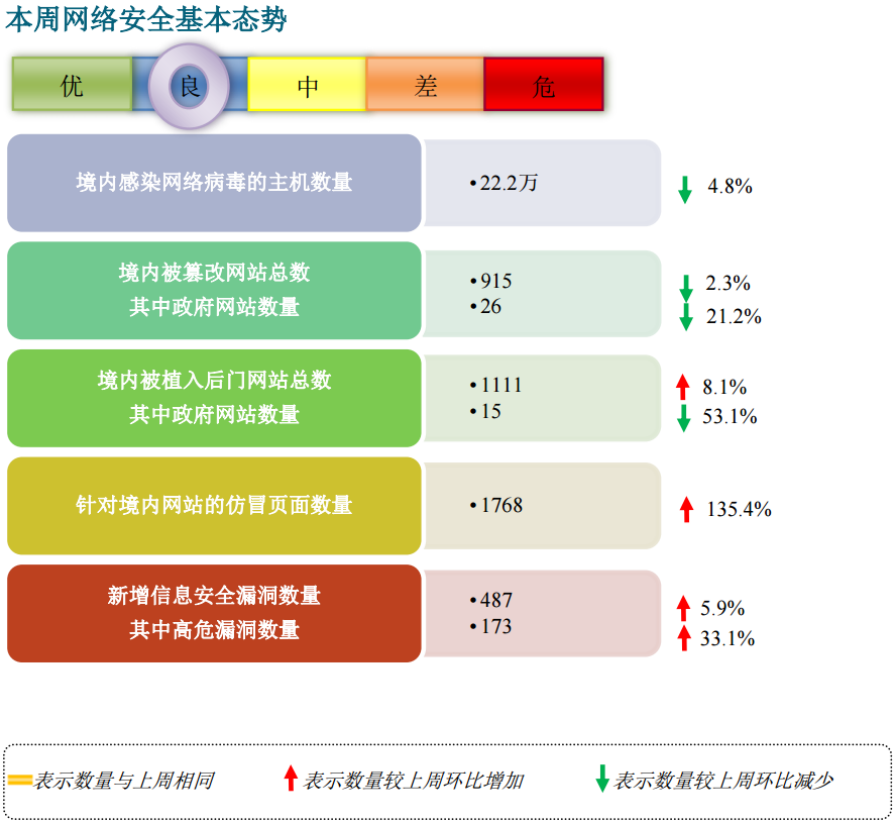
本期要目

- 【权威发布】全国网络安全信息与动态（2018 年 3 月 19 日—3 月 25 日）
- 【城院 IT】综合业务管理平台统计信息(2018 年 3 月 26 日—4 月 1 日)
- 【网络安全】2017 中国网络安全大事
- 【网络知识】网络安全周，盘点网络安全十大威胁！

全国网络安全信息与动态

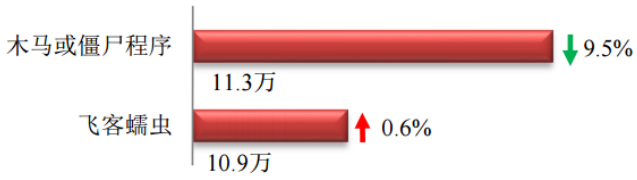
（2018 年 3 月 19 日—3 月 25 日）

根据国家互联网应急中心最新公告数据：



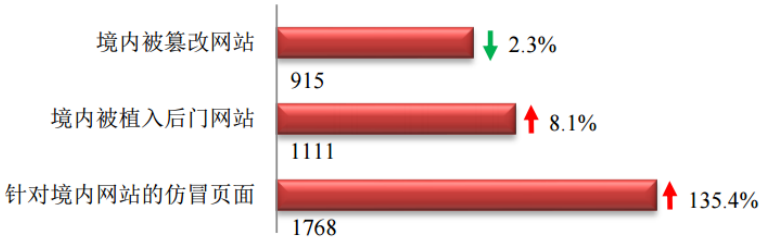
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 22.2 万个，其中包括境内被木马或被僵尸程序控制的主机约 11.3 万以及境内感染飞客（conficker）蠕虫的主机约 10.9 万。



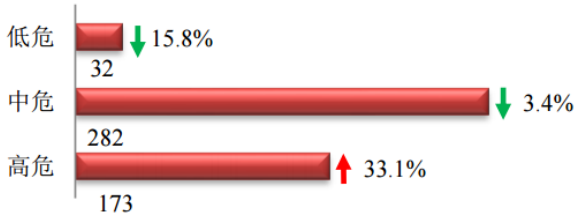
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 915 个；境内被植入后门的网站数量为 1111 个；针对境内网站的仿冒页面数量为 1768。



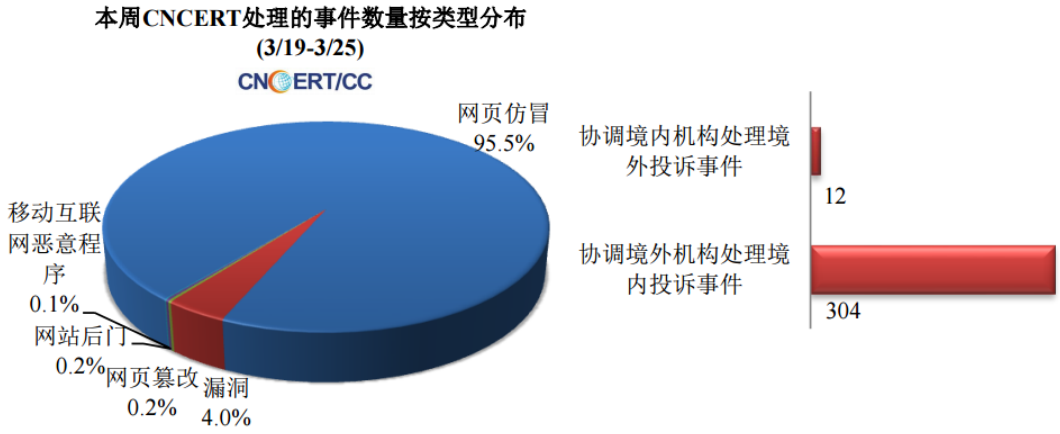
本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 487 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

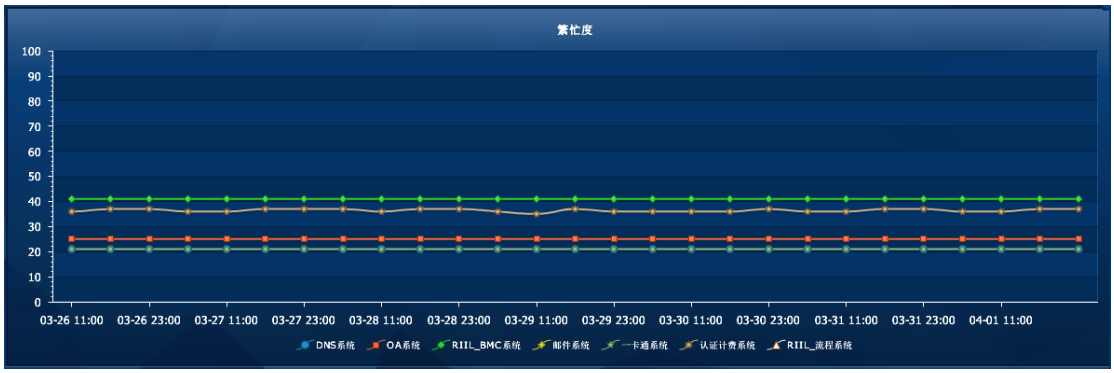
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 904 起，其中跨境网络安全事件 316 起。



城院 IT 综合业务管理平台统计信息

(2018 年 3 月 26 日—4 月 1 日)

主要业务服务繁忙度



网站集群网页更新情况统计

网站	更新		网站	更新
就业服务网	17		电子与信息工程学院	
兰州城市学院	13		发展规划处	
旅游学院	8		甘肃省高等学校外语教学指导委员会	
教学质量监测与评估中心	6		甘肃文化翻译中心	
教育学院	4		甘肃张芝书法院	
石油工程学院	4		后勤管理处	
机械工程学院	3		化学与环境工程学院	
马克思主义学院	3		机关党委	
外国语学院	3		基本建设处	
文史学院	3		教师发展中心	
城市社会心理研究中心	2		教务处	
创新创业学院	2		卡务中心	
国有资产管理处	2		科学研究处	
商学院	2		兰州城市学院校医院	
党委学生工作部	1		路易艾黎研究中心	
廉政网	1		人事处	
美术与设计学院	1		膳食处	
数学学院	1		审计	
信息网络中心	1		实训中心	
保卫处			体育学院	
城市信息与系统科学研究所			团委	
传媒学院			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	
党委宣传部			音乐学院	
党委组织部			幼儿师范学院	
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	

站群系统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
191679	站点名称：人事处	222.247.181.194	湖南省长沙市 电信	含有非法请求参数	SQL注入	2018-04-01 22:51:26
191678	站点名称：心理咨询中心	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	2018-04-01 21:12:21
191677	站点名称：心理咨询中心	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	2018-04-01 21:12:20
191676	站点名称：心理咨询中心	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	2018-04-01 21:12:19
191675	站点名称：美术与设计学院	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-04-01 17:51:50
191674	站点名称：美术与设计学院	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-04-01 17:51:50
191673	站点名称：美术与设计学院	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-04-01 17:51:49
191672	站点名称：教育学院	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	2018-03-31 23:38:30
191671	站点名称：教育学院	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	2018-03-31 23:38:29
191670	站点名称：教育学院	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	2018-03-31 23:38:28
191669	站点名称：兰州城市学院	124.152.203.251	甘肃省兰州市 联通	含有非法请求参数	SQL注入	2018-03-30 20:49:01
191668	站点名称：兰州城市学院	124.152.203.251	甘肃省兰州市 联通	含有非法请求参数	SQL注入	2018-03-30 20:49:00
191667	站点名称：兰州城市学院	124.152.203.251	甘肃省兰州市 联通	含有非法请求参数	SQL注入	2018-03-30 20:49:00
191666	管理平台	10.0.92.151	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： gzc	错误帐号或密码	2018-03-30 09:47:41
191665	站点名称：兰州城市学院	118.180.5.174	甘肃省兰州市 网宿科技电信CDN节点	含有非法请求参数	SQL注入	2018-03-30 06:17:12
191664	站点名称：电子与信息工程学院	118.180.5.174	甘肃省兰州市 网宿科技电信CDN节点	含有非法请求参数	SQL注入	2018-03-30 06:12:33
191663	站点名称：信息网络中心	118.180.5.174	甘肃省兰州市 网宿科技电信CDN节点	含有非法请求参数	SQL注入	2018-03-30 06:11:10
191661	管理平台	223.104.27.120	甘肃省兰州市 移动	登录位置：网站管理； 登录账号： mssj	错误帐号或密码	2018-03-29 15:49:30
191660	站点名称：旅游学院	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-03-29 11:17:50
191659	站点名称：旅游学院	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-03-29 11:17:49
191658	站点名称：旅游学院	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-03-29 11:17:49
191657	管理平台	10.0.23.208	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	2018-03-29 09:08:57
191656	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	2018-03-27 15:35:14
191655	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	2018-03-27 10:16:41
191654	管理平台	10.0.70.44	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	2018-03-27 09:16:04
191653	管理平台	10.0.70.44	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	2018-03-27 09:15:38
191652	管理平台	10.0.70.44	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	2018-03-27 09:15:16
191651	站点名称：科学研究处	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-03-25 09:03:58
191650	站点名称：科学研究处	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-03-25 09:03:58
191649	站点名称：科学研究处	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-03-25 09:03:58

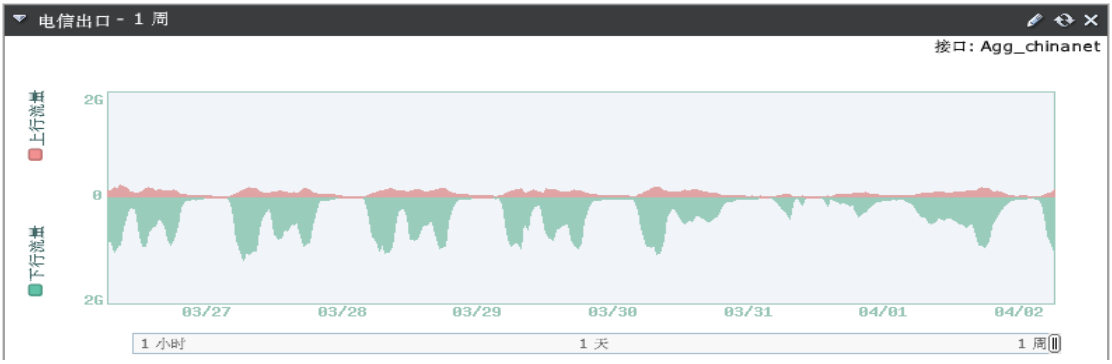
站群系统应用防火墙网站访问 IP 封禁记录

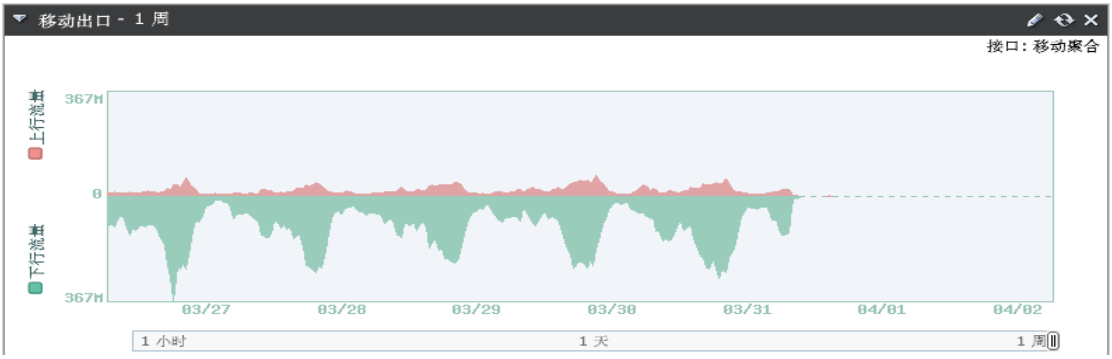
封禁IP	封禁IP归属地	封禁开始时间 ▼	封禁结束时间
27.255.77.11	韩国 Ehost互联网数据中心	2018-04-01 21:12:21	2018-04-02 07:12:21
110.87.188.33	福建省福州市 电信	2018-04-01 17:51:50	2018-04-02 03:51:50
27.255.77.11	韩国 Ehost互联网数据中心	2018-03-31 23:38:30	2018-04-01 09:38:30
124.152.203.251	甘肃省兰州市 联通	2018-03-30 20:49:01	2018-03-31 06:49:01
118.180.5.174	甘肃省兰州市 网宿科技电信CDN节点	2018-03-30 06:17:12	2018-03-30 16:17:12
110.87.188.33	福建省福州市 电信	2018-03-29 11:17:50	2018-03-29 21:17:50
110.87.188.33	福建省福州市 电信	2018-03-25 09:03:58	2018-03-25 19:03:58
27.255.77.11	韩国 Ehost互联网数据中心	2018-03-24 18:56:13	2018-03-25 04:56:13

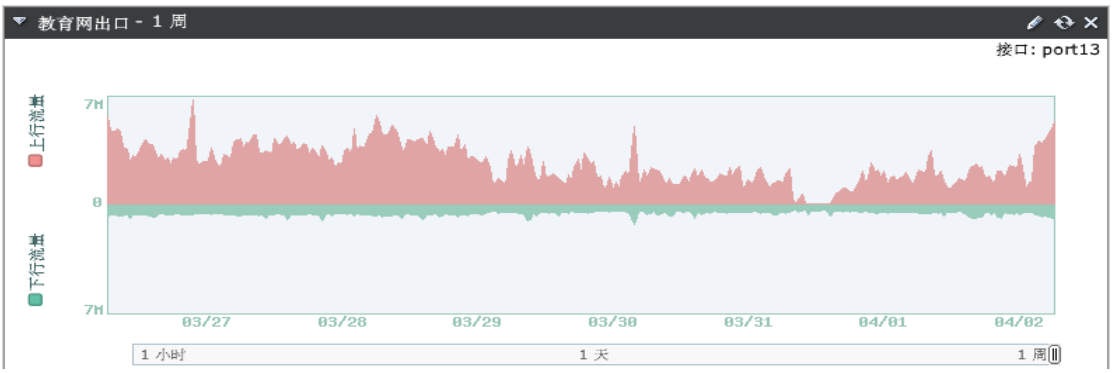
站群系统应用防火墙网站危险文件扫描记录

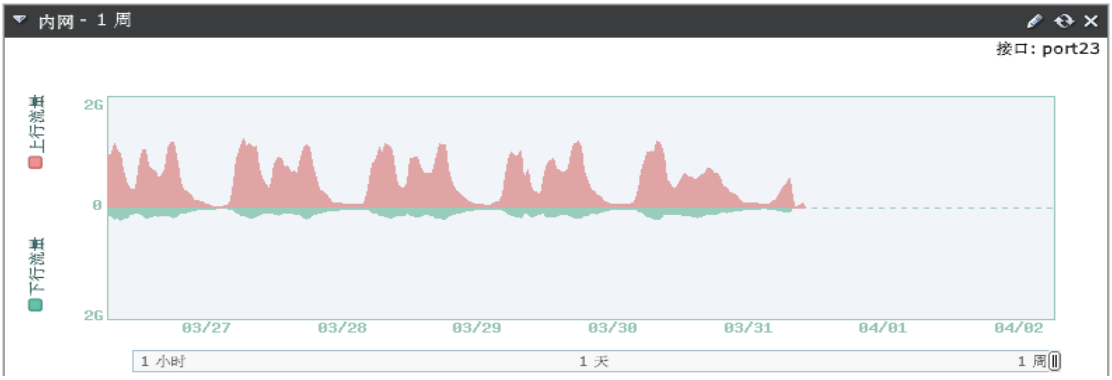
序号	路径	类型	操作
1	E:\VSB9\manager\system_owners\lyxy_webprj\content.jsp	恶意js引用	查看
2	E:\VSB9\manager\system_owners\lzcsxy_webprj\cheng_2.jsp	恶意js引用	查看
3	E:\VSB9\manager\system_owners\lzcsxy_webprj\content.jsp	恶意js引用	查看
4	E:\VSB9\manager\system_owners\lzcsxy_webprj\dh_jianjie.jsp	恶意js引用	查看
5	E:\VSB9\manager\system_owners\lzcsxy_webprj\index.jsp	恶意js引用	查看
6	E:\VSB9\manager\system_owners\lzcsxy_webprj\list.jsp	恶意js引用	查看
7	E:\VSB9\manager\system_owners\lzcsxy_webprj\list_1.jsp	恶意js引用	查看
8	E:\VSB9\manager\system_owners\lzcsxy_webprj\list_2.jsp	恶意js引用	查看
9	E:\VSB9\manager\system_owners\lzcsxy_webprj\new_list_1.jsp	恶意js引用	查看
10	E:\VSB9\manager\system_owners\lzcsxy_webprj\xiaobao.jsp	恶意js引用	查看
11	E:\VSB9\manager\system_owners\lzcsxy_webprj\xinxiang.jsp	恶意js引用	查看
12	E:\VSB9\manager\system_owners\lzcsxy_webprj\xr_lingdao.jsp	恶意js引用	查看
13	E:\VSB9\manager\system_owners\sxy_webprj\index.jsp	恶意js引用	查看
14	E:\VSB9\manager\system_owners\sygcxy_webprj\index.jsp	恶意js引用	查看
15	E:\VSB9\manager\system_owners\zsw_webprj\index.jsp	恶意js引用	查看

网络出口带宽情况统计





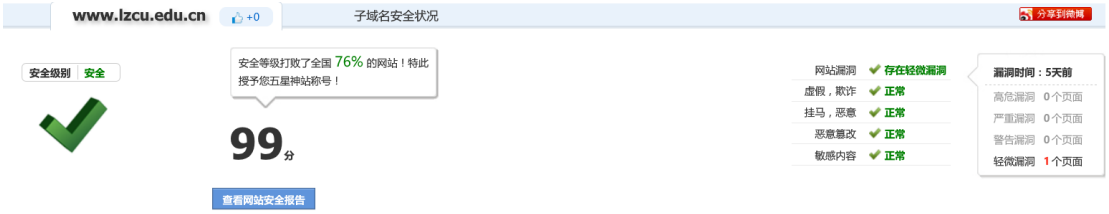




APT统计

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

网站安全检测一（360 网站安全检测）



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

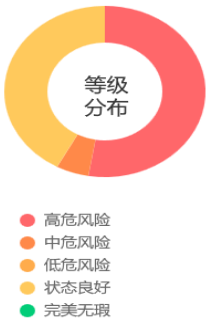
正常

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	583.23 ms	100 %
OA办公主页【http://oa.lzcu.edu.cn】	源站监控	2	580.44 ms	100 %
WEB【http://www.lzcu.edu.cn】	源站监控	2	432.23 ms	100 %
WEB【http://www.lzcu.edu.cn】	源站监控	2	399.76 ms	100 %

网站安全检测二（百度云观测）

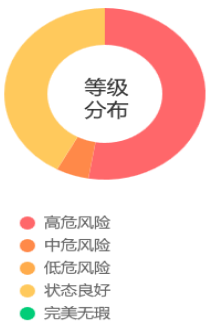
昨日百度中国互联网安全指数上限为100点，距离完美还差50.34点。全行业的网站安全等级偏低。（每日指数上限随观测站点变化而变化）
所有观测站点中，43786个为完美等级站点，626230个为良好等级站点，2183950个为低危等级站点，1183258个为中危等级站点，2387717个为高危等级站点。

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

【网络安全】2017 中国网络安全大事

经济参考报 2018-02-06 10:00:04

2 月 5 日，由中国计算机学会计算机安全专业委员会和新华社《经济参考报》互联网+周刊共同主办的 2017 年中国网络安全大事发布会在京举行。本次会议发布了结合专家组评选和线上投票遴选出的 2017 年网络安全大事。

本次活动通过对 2017 年互联网安全行业发生的众多大事件及相关重要新闻的梳理，综合专家组评选意见和线上投票，甄选出 13 条在 2017 年产生重大影响的网络安全大事。中科院信息工程研究所，中科院大学，公安部一所，国家计算机网络与信息安全管理中心，全国信息安全标准化技术委员会，中国计算机学会计算机安全专业委员会等单位的众多专家参与了本次评选活动。

参会专家和业界人士普遍认为，这些入选事件显示出互联网安全目前在国民经济、社会发展和人民生活中的重要影响，同时还预示了经济和行业发展的下一步趋势，对企业和个人未来决策具有重大意义。

一、中央网信办印发《国家网络安全事件应急预案》

1 月 10 日，中央网络安全和信息化领导小组办公室下发关于印发《国家网络安全事件应急预案》的通知。通知指出编制目的是为了建立健全国家网络安全事件应急工作机制，提高应对网络安全事件能力，预防和减少网络安全事件造成的损失和危害，保护公众利益，维护国家安全、公共安全和社会秩序。

二、外交部等部门发布《网络空间国际合作战略》

3 月 1 日，经中央网络安全和信息化领导小组批准，外交部和国家互联网信息办公室共同发布《网络空间国际合作战略》，此战略以和平发展、合作共赢为主题，以构建网络空间命运共同体为目标，就推动网络空间国际交流合作首次全面系统提出中国主张，为破解全球网络空间治理难题贡献中国方案，是指导中国参与网络空间国际交流与合作的战略性文件。

三、公安部加大整治黑客攻击破坏和打击侵犯公民个人信息犯罪行动力度

3 月 10 日，公安部召开电视电话会议，就进一步推进打击整治黑客攻击破坏和网络侵犯公民个人信息犯罪专项行动进行部署。同期，公安部还公布破获一起盗卖 50 亿条公民信息的特大案件，犯罪团伙涉嫌入侵社交、游戏、视频直播、医疗等各类公司的服务器，非法获取用户账号、密码、身份证、电话号码、物流地址等重要信息 50 亿条。

四、勒索病毒席卷全球

5 月 12 日，英国、意大利、俄罗斯等全球多个国家爆发 WannaCry 勒索病毒攻击。WannaCry 勒索软件席卷全球，至少 150 个国家、30 万名用户中招，造成损失达 80 亿美元，已经影响到金融、能源、医疗等众多行业，造成严重的危机管理问题。中国部分 Windows 操作系统用户遭受感染，校园网用户首当其冲，大量实验室数据和毕业设计被锁定加密。部分大型企业的应用系统和数据库文件被加密后，无法正常工作，影响巨大。

五、《中华人民共和国网络安全法》正式实施

6 月 1 日，《中华人民共和国网络安全法》正式实施，作为网络领域的基础性法律，此法的公布和实施不仅从法律上保障了广大人民群众在网络空间的利益，有效维护了国家网络空间主权和安全，同时将严惩破坏我国网络空间安全的组织和个人。

六、央视曝光大量家庭摄像头遭入侵 质检总局发警示

6 月 18 日，中央电视台报道称，大量家庭摄像头遭入侵，有人借此非法牟利。同日，国家质检总局官网发布关于智能摄像头的质量安全的风险警示称，已检测的 40 批次中，32 批次样品存在质量安全隐患，可能导致用户监控视频被泄露，或智能摄像头被恶意控制等危害。

七、《一流网络安全学院建设示范项目管理办法》出台

8 月 8 日，中央网络安全和信息化领导小组办公室秘书局和教育部办公厅发布关于印发《一流网络安全学院建设示范项目管理办法》的通知。通知要求加强和创新网络安全人才培养，争创一流网络安全学院。

八、世界首条量子保密通信干线——“京沪干线”开通

9 月 29 日，世界首条量子保密通信干线——“京沪干线”正式开通。结合“京沪干线”与“墨子号”量子卫星的天地链路，我国科学家成功实现了首次洲际量子保密通信。这标志着我国已构建出天地一体化广域量子通信网络雏形，为未来实现覆盖全球的量子保密通信网络迈出了坚实的一步。

九、十九大报告深入阐述网络安全问题

10 月 18 日，中国共产党第十九次全国代表大会在北京人民大会堂开幕。十九大制定了新时代中国特色社会主义的行动纲领和发展蓝图，提出要建设网络强国、数字中国、智慧社会，推动互联网、大数据、人工智能和实体经济深度融合，建立网络综合治理体系，营造清朗的网络空间，提高基于网络信息体系的联合作战能力等，发展数字经济、共享经济，培育新增长点、形成新动能，中国数字经济发展将进入快车道。

十、我国物联网安全关键技术 TRAIS-X 成国际标准

10 月 23 日，中国自主研发的物联网安全协议关键技术 TRAIS-X，被国际标准组织正式发布，成为国际标准技术规范。TRAIS-X 是物联网基础性创新技术，属于射频识别（RFID）空中接口安全 TRAIS 技术体系，是具有完全自主知识产权的空中接口安全协议。本次获国际标准技术规范采纳并发布，是我国在全球物联网关键核心技术领域的又一重大突破。

十一、我国两数字签名算法被收入国际标准

11 月 3 日，在第 55 次 ISO/IEC 联合技术委员会信息安全技术分委员会（SC27）德国柏林会议上，含有我国 SM2 与 SM9 数字签名算法的 ISO/IEC14888-3/AMD1《带附录的数字签名第 3 部分：基于离散对数的机制-补篇 1》获得一致通过，成为 ISO/IEC 国际标准，进入标准发布阶段。SM2 与 SM9 数字签名算法被收入 ISO/IEC 国际标准，标志着我国向国际标准化组织（ISO）和国际电工委员会（IEC）贡献中国智慧和中国标准取得重要突破，将进一步促进我国在密码技术和网络空间安全领域的国际合作和交流。两数字签名算法收入 ISO/IEC。

十二、多部门联手合力打击治理电信网络诈骗

据公安部网站消息，建立 23 个部门和单位参加的部际联席会议制度高规格打击电信诈骗，健全涉电信诈骗犯罪侦查工作机制，深化跨境跨区域警务合作，建立诈骗电话通报阻断、被骗资金快速止付机制……一系列打击治理电信诈骗犯罪机制的创新，其目的就是实现侦查打击、重点整治、防范治理三位一体，坚决把犯罪分子的嚣张气焰打下去，切实守护好老百姓的钱袋子。

十三、网络安全技术大赛空前活跃

2017 年，国内网络安全技术各类大赛空前活跃，比赛范围和影响力明显提升。CTF 夺旗赛、AWD 攻防赛、Pwn 漏洞赛等传统赛事规模日益扩大；数据分析赛、靶场赛、人工智能机器人比赛、运维技术赛等等新颖赛事不断涌现；赛事发起及运作日趋专业化、行业化、规模化、细分化，一些顶级赛事还推出反作弊系统来保证赛事健康发展。各项赛事也和高校教育教学、行业技术练兵、优秀人才选拔等实际工作紧密结合。

【网络知识】网络安全周，盘点网络安全十大威胁！

聊城网警 2017-09-14 17:21:09

1、计算机病毒——程序或可执行码，通过复制自身来进行传播，会影响电脑的正常运作。

2017 年 5 月 12 日，全球 99 个国家和地区发生超过 7.5 万起电脑病毒攻击事件，罪魁祸首是一个名为“想哭”(WannaCry)的勒索软件。

2、蠕虫——可通过 USB 设备或电子邮件附件等进行传播，会影响邮件收发。

2017 年 5 月 12 日，在英国伦敦，一名由于医院电子系统遭到病毒攻击而无法进行心脏手术的男子在医院外接受媒体采访。

3、木马——不会自我繁殖，也并不刻意“感染”其他文件，但会使电脑失去防护，易于被黑客控制。

2017 年 5 月 12 日，在西班牙马德里一家电信公司外拍摄的监控摄像头。

4、间谍软件——未经你同意而偷偷安装在电脑上，不断地将您的信息反馈给控制该软件的人。

德国法兰克福火车站拍摄的无法正常工作的电子时刻表。

5、广告程序——通常以弹窗形式出现，不会对电脑造成直接伤害，但可能会成为间谍软件的载体。

2017 年 5 月 13 日，德国莱比锡火车站一个无法正常工作的电子时刻表。

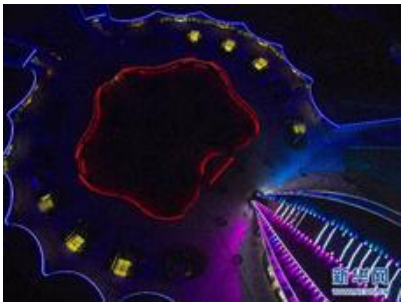
6、垃圾邮件——可以被用来发送不同类型的恶意软件，也可能对邮件服务器造成不良影响。

2017 年 5 月 12 日，在英国伦敦，一名女子观看遭到病毒攻击的网页。

7、网络钓鱼——通过假冒的电子邮件和伪造的 Web 站点来进行诈骗活动，受骗者往往会泄露重要私人资料。

2017 年 5 月 12 日，在德国开姆尼茨，一处电子时刻表遭到病毒攻击而无法工作。

8、网址嫁接——形式更复杂的网络钓鱼。利用 DNS 系统，建立以假乱真的假网站，套取受骗者的信息。



图为 2016 年“网络安全博览会”主展馆夜景。

9、键盘记录器——可以记录用户在键盘上的操作，黑客可以搜寻特定信息，比如账号密码等。

四川省暨成都市 2016 年国家网络安全宣传周活动现场，工作人员讲解网络安全知识。

10、假的安全软件——伪装成安全软件，提出虚假报警，诱使用户卸载有用的安防软件，以便于盗取网络支付等信息。

2017 年海南电力系统网络安全攻防演练在海口举行，图为演练现场。

抄送：校领导