网络信息安全周报

【2018】第 4 期

党委宣传部
信息网络中心 编

2018 年 3 月 29 日

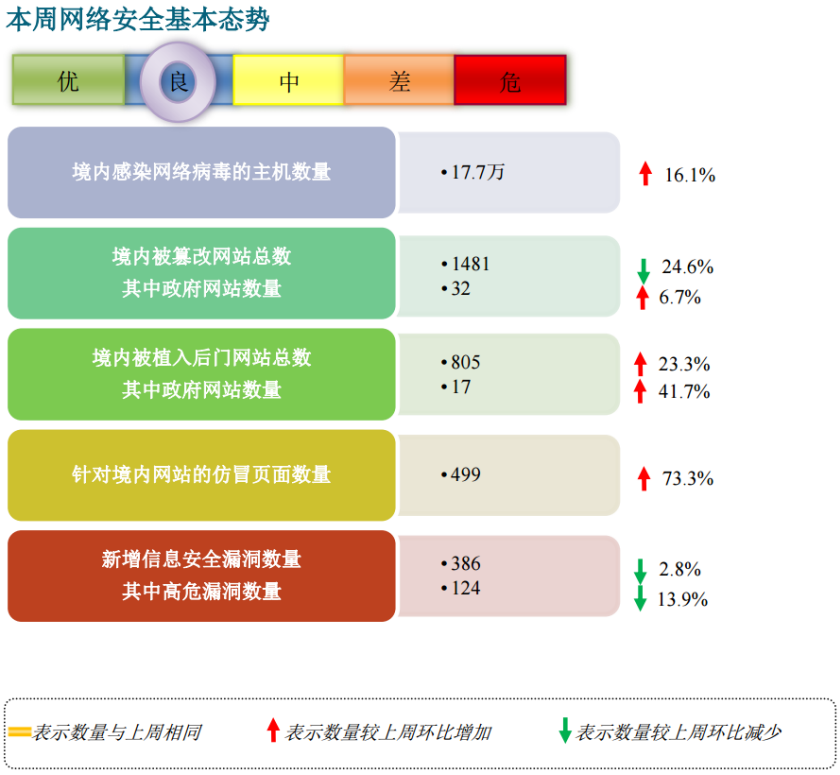
本期要目

- 【权威发布】全国网络安全信息与动态（2018 年 3 月 5 日—3 月 11 日）
- 【权威发布】甘肃省网络安全工作情况通报(2018 年第 3 期)-摘要
- 【城院 IT】综合业务管理平台统计信息(2018 年 3 月 19 日—3 月 25 日)
- 【网警普法】 发生危害网络安全事件后的报告义务
  网络安全法，一定要知道！

全国网络安全信息与动态

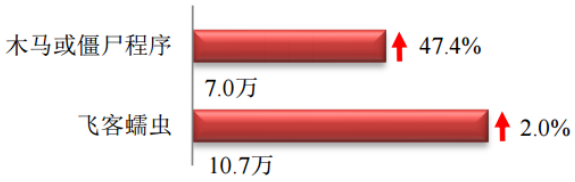
（2018 年 3 月 5 日—3 月 11 日）

根据国家互联网应急中心最新公告数据：



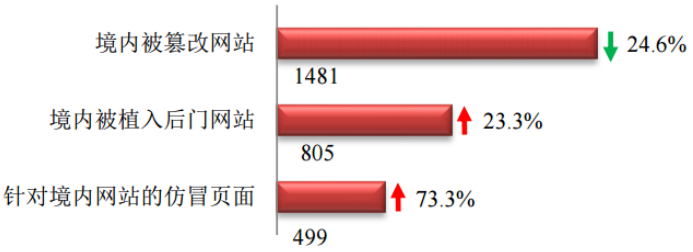
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 17.7 万个，其中包括境内被木马或被僵尸程序控制的主机约 7.0 万以及境内感染飞客（conficker）蠕虫的主机约 10.7 万。



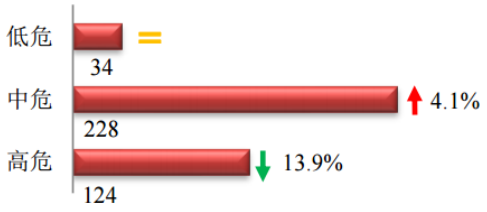
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1481 个；境内被植入后门的网站数量为 805 个；针对境内网站的仿冒页面数量为 499。



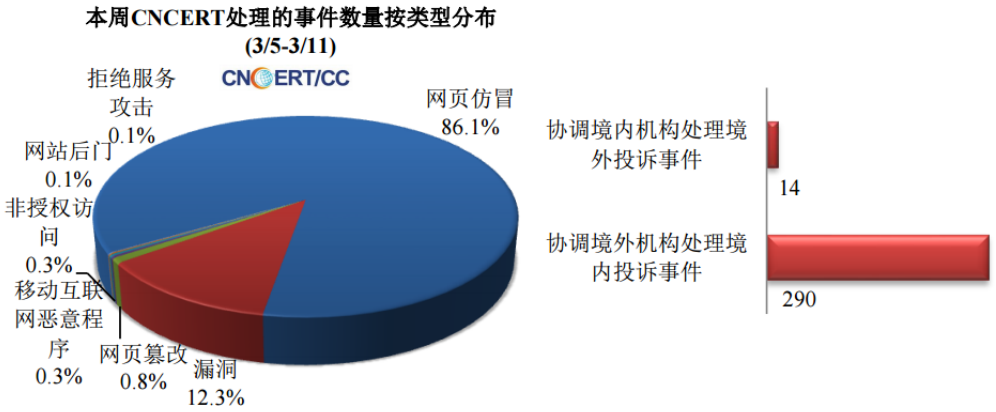
本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 386 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 726 起，其中跨境网络安全事件 304 起。

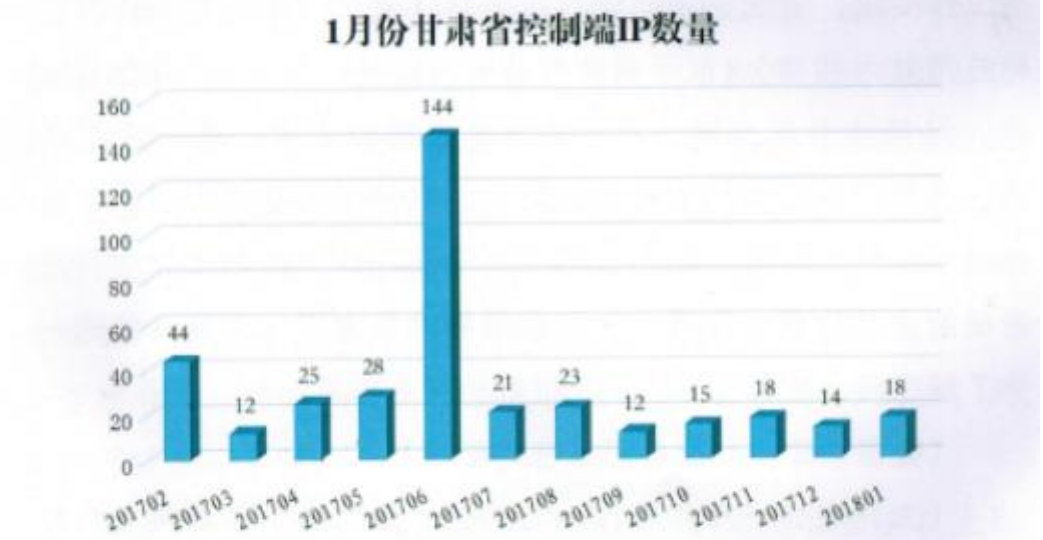


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 625 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 549 起和政府公益仿冒事件 60 起。

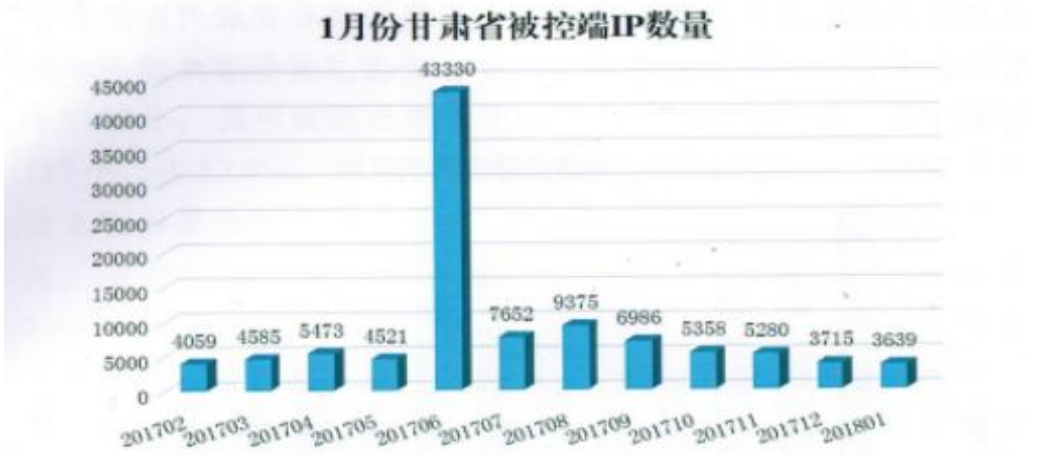
【权威发布】甘肃省网络安全工作情况通报(2018 年第 3 期)摘要

二、全省互联网网络安全监测情况

（一）木马僵尸网络控制端事件。2018年1月，甘肃省发现18个IP被利用作为木马僵尸控制服务器，较上月监测数量增加4个IP。从监测情况看，于2017年6月出现该事件峰值，为144个IP，2017年7月-2018年1月整体情况较为平稳。如下图所示：

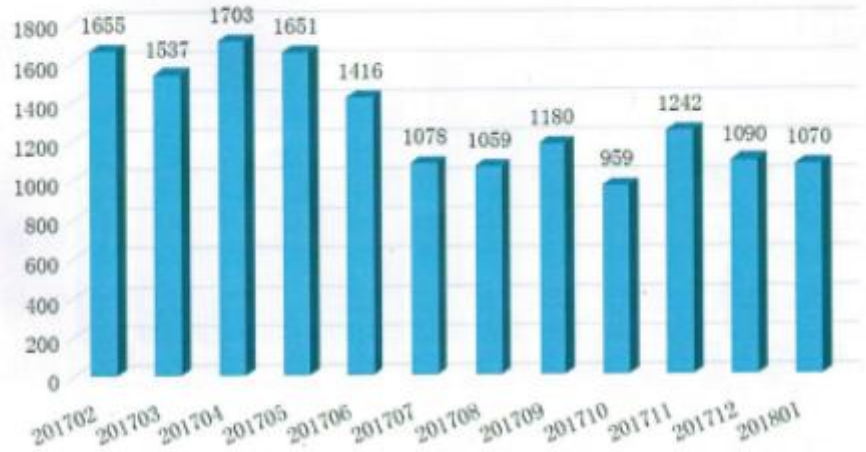


（二）木马僵尸网络被控端事件。2018年1月，甘肃省有3639个IP被外省市或其它国家通过木马僵尸程序秘密控制，较上月减少76个，达到一年来的最低值。从监测情况看，于2017年6月出现峰值，为43330个IP，2017年8月-2018年1月整体呈下降趋势。如下图所示：



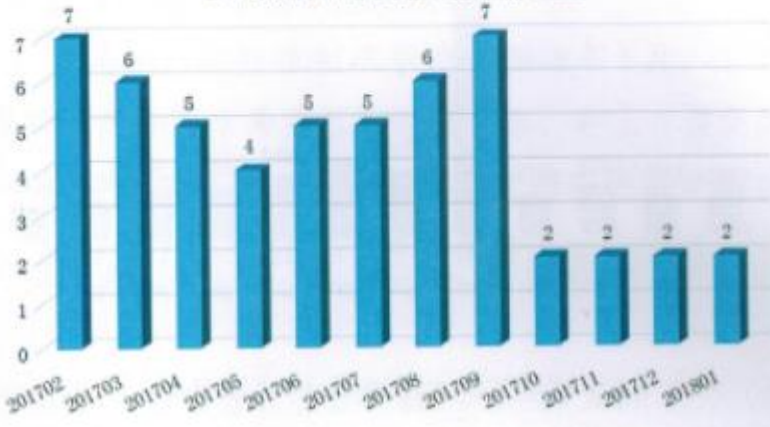
（三）飞客蠕虫事件。2018年1月，甘肃省有1070个IP主机感染飞客蠕虫病毒，较上月减少20个。从监测情况看，于2017年4月出现峰值，为1703个IP主机，2017年6月-2018年1月整体情况较平稳。如下图所示：

1月份甘肃省感染蠕虫病毒主机数量

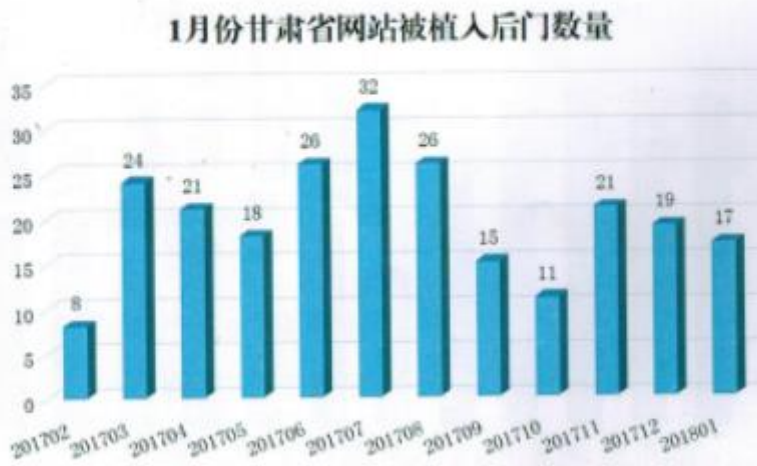


（四）网页篡改事件。2018年1月，甘肃省监测有2个网站被篡改，分别是定西市工商行政管理局网站和天水天脉源食品有限公司网站，监测数量较上月没有变化，继续维持近一年来的最低值。如下图所示：

1月份甘肃省被篡改网站数量



（五）网站后门事件。2018年1月，甘肃省内发现17起网站被植入后门事件，监测数量较上月减少2起。从监测情况看，于2017年7月出现峰值，为32起。如下图所示：



（数据来源：甘肃省通信管理局）

六、一月份全省网络安全漏洞事件整改处置情况

2018年1月，全省共通报网络安全漏洞及事件32起，其中转发中央网信办通报5起，占总数15.6%；我省自行监测通报27起，占总数84.4%。已整改30起，占总数93.75%；未整改2起（兰州市商业学校网站2起），占总数6.25%。

按地区划分，省直单位10起，兰州市8起，庆阳市6起，定西市2起，白银市2起，金昌市1起，陇南市1起，张掖市1起，兰州新区1起。按照通报类型分，网络安全事件20起，占总数的62.5%；各类漏洞12起，占总数的37.5%。网络安全事件中，植入黑页、跳转代码3起，网页非法篡改17起；各类漏洞中，弱口令漏洞3起，SQL注入漏洞2起，跨站脚本漏洞2起，WebLogic反序列化漏洞1起，网站配置文件泄露漏洞1起，IIS短文件名泄露漏洞1起，Web列目录漏洞1起，未授权访问漏洞1起。具体如下表所示：

序号	网站名称	域名	漏洞名称	整改情况
1	甘肃省对外经贸服务网	www.gfta.org.cn	植入恶意黑页	已整改
2	金昌市人民政府网站	www.jc.gansu.gov.cn	SQL注入漏洞	已整改
3	宁县青年网	www.nxqn.org.cn	植入恶意黑页	已整改
4	甘肃省草原监督管理局公文管理系统	61.178.74.31:81	SQL注入漏洞	已整改
5	甘肃省12349居家养老服务平台	118.180.24.34:8088/	弱口令	已整改
6	信用中国(甘肃)网站	www.gscredit.gov.cn	WebLogic反序列化漏洞	已整改
7	靖远县卫计委网站	www.jyxwsjsj.com	网站非法篡改	已整改
8	通渭县农村信用社网站	gstwrcu.com	网站非法篡改	已整改
9	中国·漳县网	www.zhangxian.gov.cn	网站非法篡改	已整改
10	网站非法篡改	www.gsdx.gov.cn	网站配置文件泄露	已整改
11	机械研究与应用网站	www.jxyj1978.com	IIS短文件名泄露漏洞	已整改
12	榆中县人民检察院网站	www.yzxrmjcy.gov.cn	网站非法篡改	已整改
13	康县档案局网站	www.kxda.net	网站非法篡改	已整改
14	兰州工业研究院网站	www.lziri.com.cn	网站非法篡改	已整改
15	甘肃省商务厅网站	www.gsdofcom.gov.cn	网站非法篡改	已整改
16	庆阳市工信委网站	www.qysiit.gov.cn	网站非法篡改	已整改
17	兰州新区综合保税区网站	www.lzxqftz.gov.cn	植入跳转代码	已整改
18	兰州城市建设学校网站	www.lzcj.edu.cn	网站非法篡改	已整改
19	甘肃省小陇山林业科学研究所网站	www.gsxlslks.com	网站非法篡改	已整改
20	庆阳市公共资源交易中心网站	www.qyggzyjy.gov.cn	Web列目录漏洞	已整改
21	兰州市七里河区教育局网站	www.lzqlh.com	网站非法篡改	已整改
22	庆阳人民防空办公室网站	www.qyrf.gov.cn	跨站脚本漏洞	已整改

23	高台县人民代表大会网站	rd.gaotai.gov.cn	弱口令	已整改
24	兰州市军队离退休干部第二休养所网站	www.lzjxes.com	网站非法篡改	已整改
25	兰州市商业学校网站	www.lzcoms.cn	网站非法篡改	未整改
26	靖远党建网	jydj.baiyin.cn	网站非法篡改	已整改
27	环县人民法院网站	www.hxfy.gov.cn	跨站脚本漏洞	已整改
28	兰州市道路运输从业人员管理信息系统	202.100.78.226	弱口令	已整改
29	甘肃科聚网	www.gskeju.cn	未授权访问漏洞	已整改
30	庆阳市道路运输管理局网站	www.qyyz.org.cn	网站非法篡改	已整改
31	永登党建网	www.ydjcdj.gov.cn	网站非法篡改	已整改
32	兰州市商业学校网站	lzssyxx.qy.xb-cloud.com	网站非法篡改	未整改

附录：网络安全名词解释——SQL 注入攻击

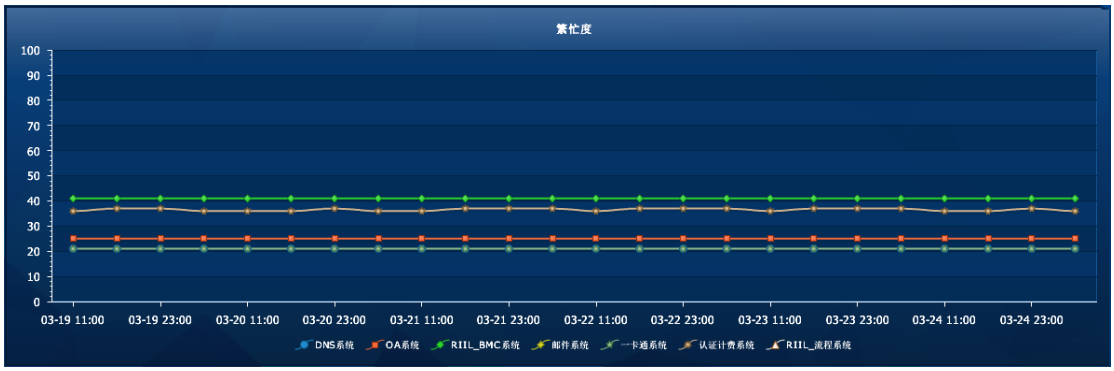
随着 B/S 模式应用开发的发展，使用这种模式编写应用程序的程序员也越来越多。但是由于程序员的水平及经验也参差不齐，相当大一部分程序员在编写代码的时候，没有对用户输入数据的合法性进行判断，使应用程序存在安全隐患。

SQL 注入即是指 web 应用程序对用户输入数据的合法性没有设定判断，网络攻击者可以通过在 web 应用程序中事先定义好的查询语句的结尾上添加额外的 SQL 语句的方式，以此来实现欺骗数据库服务器执行非授权的任意查询，从而进一步得到相应的数据信息，攻击者根据程序返回的结果，获得某些他想得知的数据，这就是 SQL 注入攻击。

城院 IT 综合业务管理平台统计信息

(2018 年 3 月 19 日—3 月 25 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
兰州城市学院	17		招生网	
教学质量监测与评估中心	9		城市信息与系统科学研究所	
创新创业学院	8		审计	
就业服务网	7		文史学院	
廉政网	6		甘肃张芝书法院	
传媒学院	5		科学研究处	
化学与环境工程学院	3		美术与设计学院	
商学院	3		保卫处	
音乐学院	3		城市社会心理研究中心	
电子与信息工程学院	3		数学学院	
外国语学院	3		党委宣传部	
信息技术教育与应用研究所	2		体育学院	
幼儿师范学院	2		人事处	
马克思主义学院	2		电子信息科学与技术研究所	
兰州城市学院校医院	2		膳食处	
发展规划处	2		基本建设处	
教育学院	2		国有资产管理处	
石油工程学院	2		党委（校长）办公室	
地理与城乡规划学院	1		卡务中心	
机关党委	1		党委学生工作部	
信息网络中心	1		甘肃文化翻译中心	
路易艾黎研究中心	1		后勤管理处	
教务处	1		档案馆	
机械工程学院			党委组织部	
职业技能鉴定所			旅游学院	
心理咨询中心			教师发展中心	
甘肃省高等学校外语教学指导委员会			团委	
学位办公室			实训中心	

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
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
191648	站点名称：就业服务网	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	2018-03-24 18:56:13
191647	站点名称：就业服务网	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	2018-03-24 18:56:11
191646	站点名称：就业服务网	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	2018-03-24 18:56:11
191645	站点名称：教育学院	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-03-22 16:19:51
191644	站点名称：教育学院	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-03-22 16:19:51
191643	站点名称：教育学院	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-03-22 16:19:51
191642	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	2018-03-22 08:55:43
191641	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	2018-03-22 08:36:07
191640	管理平台	10.0.4.235	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： sxy	错误帐号或密码	2018-03-21 16:20:06
191639	站点名称：机械工程学院	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-03-21 14:43:31
191638	站点名称：机械工程学院	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-03-21 14:43:30
191637	站点名称：机械工程学院	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-03-21 14:43:30
191636	管理平台	10.4.22.111	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	2018-03-21 09:28:49
191635	管理平台	10.4.22.111	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	2018-03-21 09:28:34
191634	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	2018-03-21 03:57:43
191633	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	2018-03-21 03:57:43
191632	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	跨站脚本注入	2018-03-21 03:57:08
191631	站点名称：就业服务网	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	2018-03-21 03:49:44
191630	管理平台	10.0.24.23	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	2018-03-20 15:58:37
191629	管理平台	59.76.112.138	甘肃省 教育网	登录位置：站群管理； 登录账号： admin	错误帐号或密码	2018-03-20 08:30:01
191628	管理平台	59.76.112.138	甘肃省 教育网	登录位置：站群管理； 登录账号： admin	错误帐号或密码	2018-03-20 08:19:21
191627	站点名称：教务处	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-03-19 20:50:29
191626	站点名称：教务处	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-03-19 20:50:29
191625	站点名称：教务处	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-03-19 20:50:29
191624	管理平台	59.76.112.138	甘肃省 教育网	登录位置：站群管理； 登录账号： admin	错误帐号或密码	2018-03-19 17:28:10
191623	管理平台	10.0.127.72	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： ADMIN	错误帐号或密码	2018-03-19 15:16:18
191622	管理平台	10.0.127.72	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： ADMIN	错误帐号或密码	2018-03-19 15:15:35
191621	管理平台	10.0.127.72	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： ADMIN	错误帐号或密码	2018-03-19 15:14:52
191620	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	2018-03-19 08:09:42
191619	站点名称：教师发展中心	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-03-19 02:22:21
191618	站点名称：教师发展中心	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-03-19 02:22:21
191617	站点名称：教师发展中心	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-03-19 02:22:21

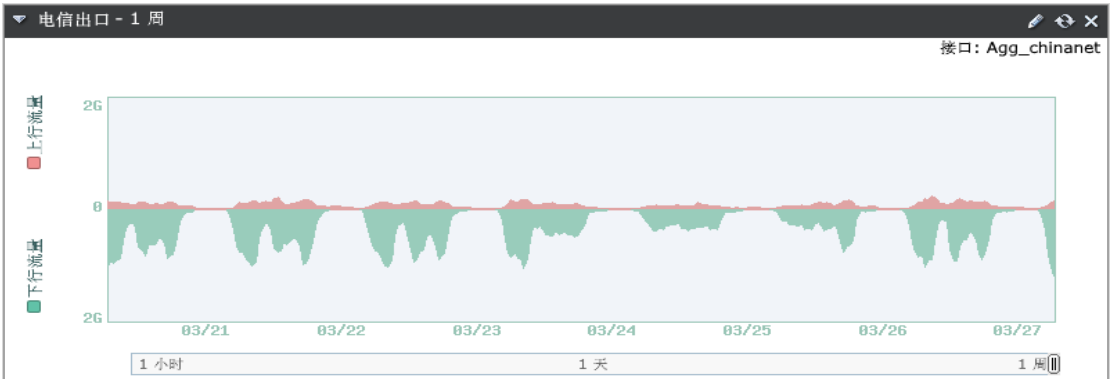
站群系统应用防火墙网站访问 IP 封禁记录

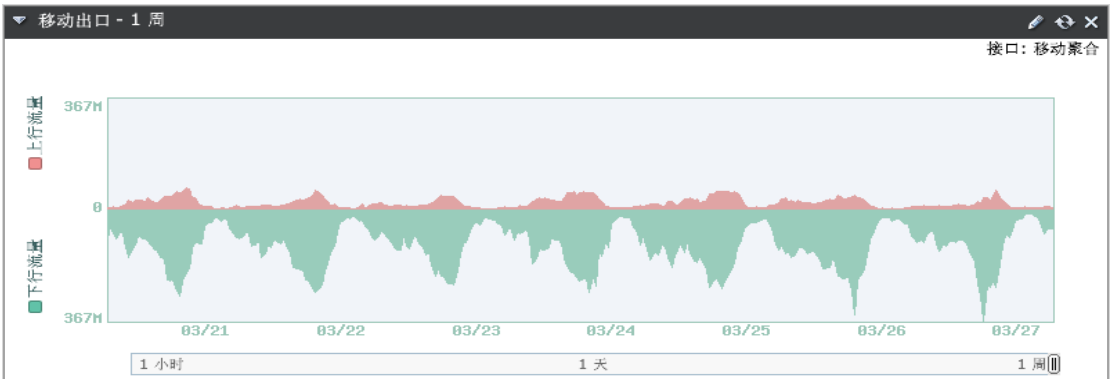
封禁IP	封禁IP归属地	封禁开始时间 ▼	封禁结束时间
110.87.188.33	福建省福州市 电信	2018-03-25 09:03:58	2018-03-25 19:03:58
27.255.77.11	韩国 Ehost互联网数据中心	2018-03-24 18:56:13	2018-03-25 04:56:13
110.87.188.33	福建省福州市 电信	2018-03-22 16:19:51	2018-03-23 02:19:51
110.87.188.33	福建省福州市 电信	2018-03-21 14:43:31	2018-03-22 00:43:31
118.180.5.174	甘肃省兰州市 网宿科技电信CDN节点	2018-03-21 03:57:43	2018-03-21 13:57:43
110.87.188.33	福建省福州市 电信	2018-03-19 20:50:29	2018-03-20 06:50:29
110.87.188.33	福建省福州市 电信	2018-03-19 02:22:21	2018-03-19 04:02:21

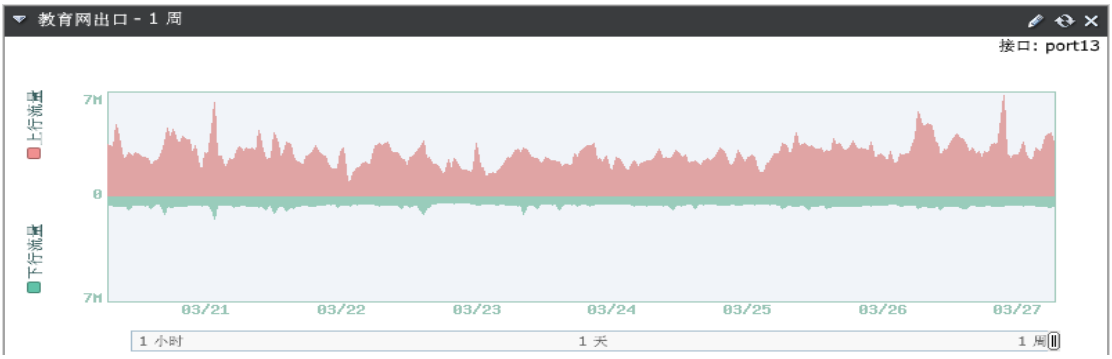
站群系统应用防火墙网站危险文件扫描记录

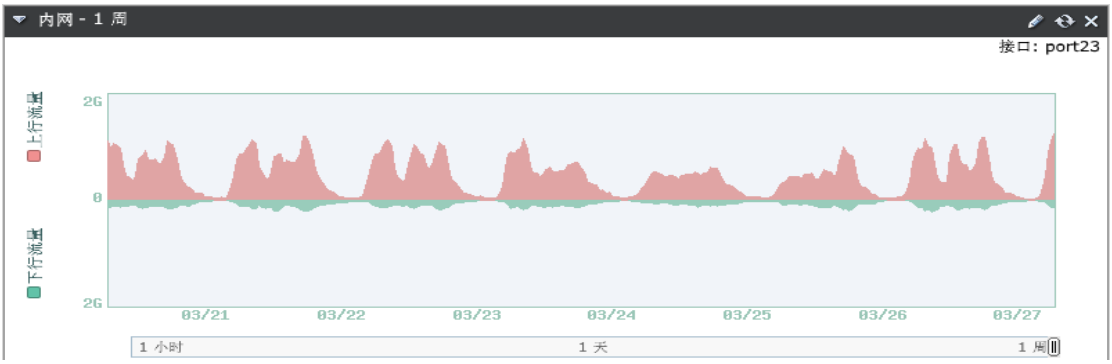
序号	路径	类型	操作
1	E:\VSB9\manager\system_owners\lyxy_webprj\content.jsp	恶意js引用	查看
2	E:\VSB9\manager\system_owners\lzcsxy_webprj\cheng_2.jsp	恶意js引用	查看
3	E:\VSB9\manager\system_owners\lzcsxy_webprj\content.jsp	恶意js引用	查看
4	E:\VSB9\manager\system_owners\lzcsxy_webprj\dh_jianjie.jsp	恶意js引用	查看
5	E:\VSB9\manager\system_owners\lzcsxy_webprj\index.jsp	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





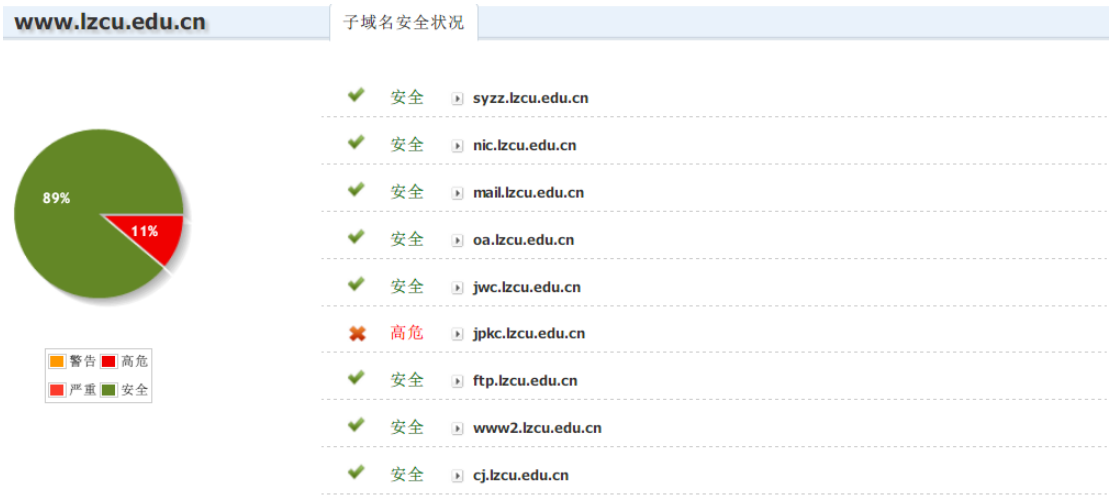




APT统计

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）



网站监控 【当前共添加了 0 个网站监控】 继续创建

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 2	285.16 ms	50 %	详情
OA办公主页【http://oa.lzcu.edu.cn】	源站监控	2 2	269.88 ms	50 %	详情
WEB【http://www.lzcu.edu.cn】	源站监控	2 1	317.1 ms	66.67 %	详情
WEB【http://www.lzcu.edu.cn】	源站监控	2 1	285.63 ms	66.67 %	详情

网站安全检测二（百度云观测）

百度安全指数　更新时间:2018-03-27 02:41　查看详情>>

百度安全指数

50.05↑0.36

中国互联网当前处于 中危 状态

观测站点 6331318 （↓142588）

恶意站点 950 （↑794）

漏洞 6993166 （↓118117）

http://www.lzcu.edu.cn　更新时间：2018-03-26 20:36:57

指数评价

34.0

所属行业：教育培训

27.89% ↓

战胜了全国 0.00% 的网站

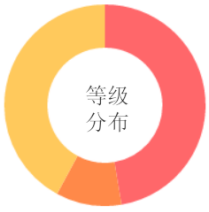
关联网站安全

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。



高危风险
中危风险
低危风险
状态良好
完美无瑕

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	39.79 高危	查看详情>>
ecard.lzcu.edu.cn	34 高危	查看详情>>
jiuye.lzcu.edu.cn	39.79 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	41.2 中危	查看详情>>

当前 1 / 2 页　首页　上一页　下一页　尾页

高危风险
中危风险
低危风险
状态良好
完美无瑕

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

【网警普法】发生危害网络安全事件后的报告义务

湖南网警巡查执法 2018-01-11 17:31:37

《中华人民共和国网络安全法》第二十五条规定：网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

该法条中的“按照规定向有关主管部门报告”具体有哪些规定呢？

1、《中华人民共和国计算机信息系统安全保护条例》（1994 年国务院令第 147 号，2011 年修订）第十四条：对计算机信息系统中发生的案件，有关使用单位应当**在 24 小时内向当地县级以上人民政府公安机关报告**。

2、《计算机信息网络国际联网安全保护管理办法》（1997 年公安部第 33 号令）第十条：互联单位、接入单位及使用计算机信息网络国际联网的法人和其他组织应当履行下列安全保护职责，其中第六项规定：发现有本办法第四条、第五条、第六条、第七条所列情形之一的，应当**保留有关原始记录，并在二十四小时内向当地公安机关报告**。

3、**《中华人民共和国电信条例》（2000 年国务院第 291 号令，2014 年修订）第六十一条**：在公共信息服务中，电信业务经营者发现电信网络中传输的信息明显属于本条例第五十七条所列内容的，应当立即停止传输，保存有关记录，并**向国家有关机关报告**。

网络运营者如果不履行按照规定报告的义务，有什么后果呢？

《中华人民共和国网络安全法》第五十九条第一款规定：网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

（注：法律中所说的“网络运营者”，是指网络的所有者、管理者和网络服务提供者。）

【网警普法】网络安全法，一定要知道！

石嘴山普法 2017-02-21 17:30:39

当今时代，网络的普及为人们的生活带来了极大的便利，与此同时，在看不见、摸不着的网络空间里，安全问题正成为牵动公众神经的焦点。公众网络生活面临哪些新陷阱、新诈骗手段？网络安全的守护者们又有哪些新的“撒手锏”？

1.网上那些行为会被认为《刑法》第二百四十六条第一款规定的“捏造事实诽谤他人”

1) 将信息网络上涉及他人的原始信息内容篡改为损害他人名誉的事实，在信息网络上散布，或者组织、指使人员在信息网上散布的；

2) 明知是捏造的损害他人名誉的事实，在信息网络上散布，情节恶劣的，以“捏造事实诽谤他人”论。

2.利用信息网络诽谤他人，在什么情形下，应当认定为《刑法》第二百四十六条第一款规定的“情节严重”

1) 同一诽谤信息实际被点击、浏览次数达到五千次以上，或者被转发次数达到五百次以上的；

2) 造成被害人或则其近亲属精神失常、自残、自杀等严重后果的；

3) 两年内曾因诽谤受过行政处罚，又诽谤他人的；

4) 其他情节严重的情形。

3.利用信息网络诽谤他人，在什么情形下，应当认定为《刑法》第二百四十六条第二款规定的“严重危害社会秩序和国家利益”

1) 引发群体性事件的；

2) 引发公共秩序混乱的；

3) 引发民族、宗教冲突的；

4) 诽谤多人，造成恶劣社会影响的；

5) 损害国家形象，严重危害国家利益的；

6) 造成恶劣国际影响的；

7) 其他严重危害社会秩序和国家利益的情形；

抄送：校领导