网络信息安全周报

【2018】第 1 期

党委宣传部
信息网络中心 编

2018 年 3 月 8 日

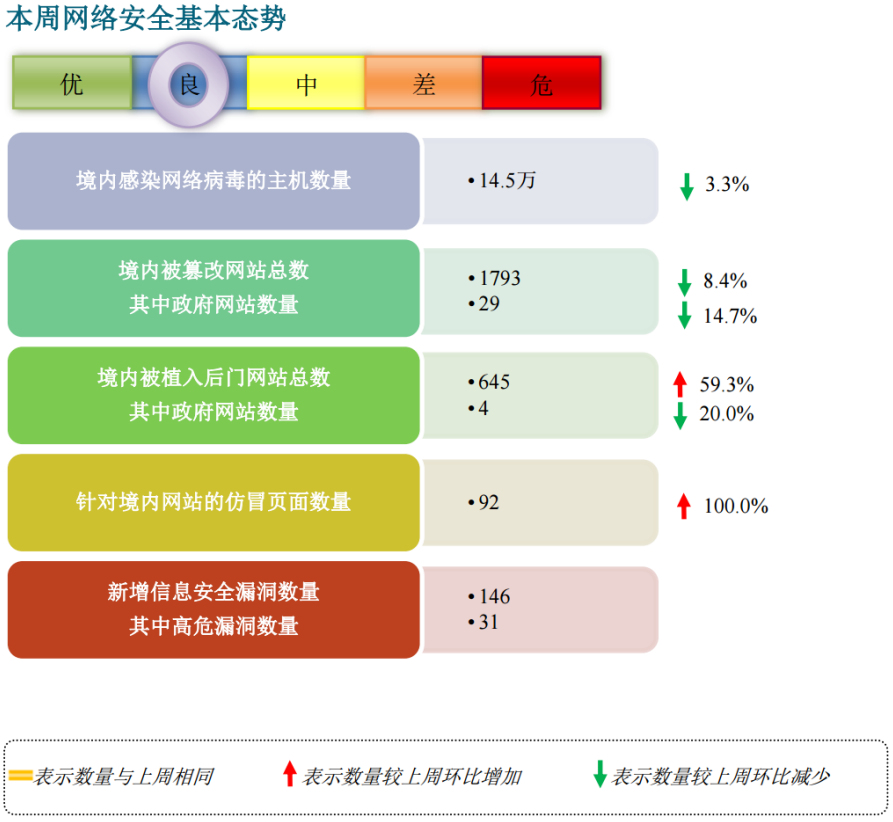
本期要目

- 【权威发布】全国网络安全信息与动态（2018 年 2 月 19 日—2 月 25 日）
- 【城院 IT】综合业务管理平台统计信息(2018 年 2 月 26 日—3 月 4 日)
- 【两会快评】防范网络风险 安全素养不可少
- 【安全分析】2018 年五大网络安全趋势

全国网络安全信息与动态

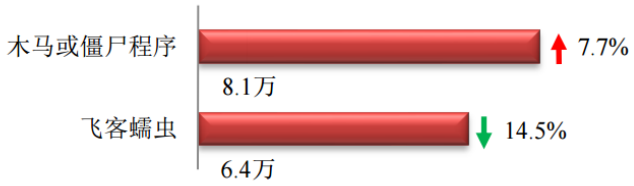
（2018 年 2 月 19 日—2 月 25 日）

根据国家互联网应急中心最新公告数据：



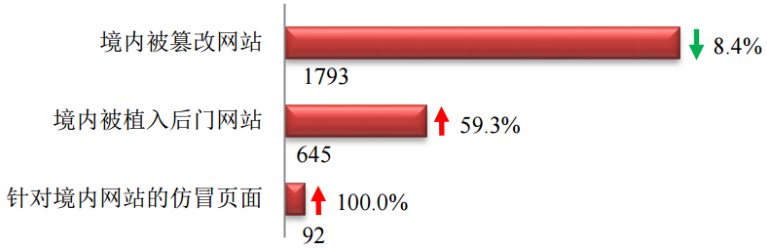
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 14.5 万个，其中包括境内被木马或被僵尸程序控制的主机约 8.1 万以及境内感染飞客（conficker）蠕虫的主机约 6.4 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 1793 个；境内被植入后门的网站数量为 645 个；针对境内网站的仿冒页面数量为 92。

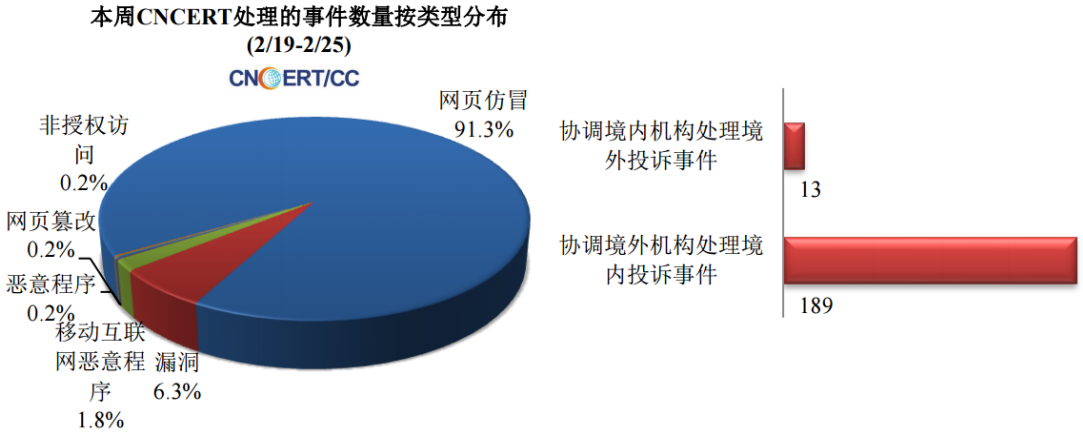


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 146 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

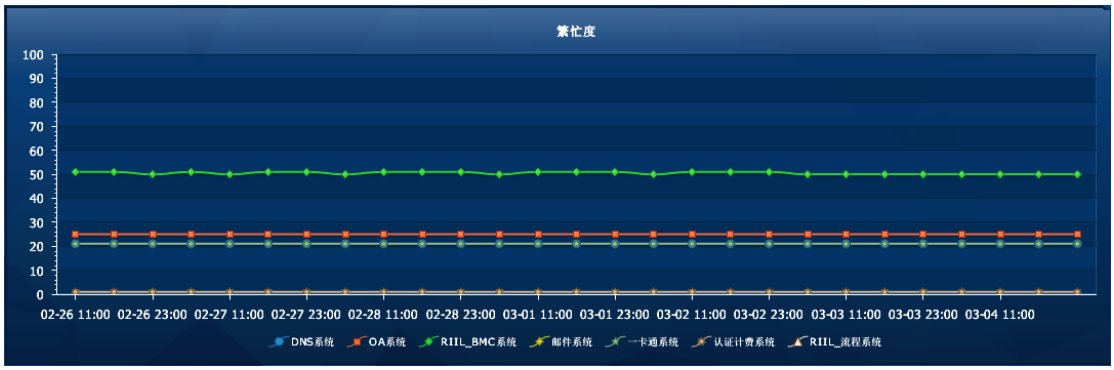
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 494 起，其中跨境网络安全事件 202 起。



城院 IT 综合业务管理平台统计信息

(2018 年 2 月 26 日—3 月 4 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
档案馆	34		党委宣传部	
教学质量监测与评估中心	16		电子信息科学与技术研究所	
信息技术教育与应用研究所	13		电子与信息工程学院	
党委组织部	7		发展规划处	
马克思主义学院	7		甘肃省高等学校外语教学指导委员会	
兰州城市学院	5		甘肃文化翻译中心	
廉政网	5		甘肃张芝书法院	
党委学生工作部	3		国有资产管理处	
教务处	3		后勤管理处	
就业服务网	3		机关党委	
路易艾黎研究中心	3		机械工程学院	
地理与城乡规划学院	2		基本建设处	
外国语学院	2		教师发展中心	
化学与环境工程学院	1		卡务中心	
教育学院	1		兰州城市学院校医院	
科学研究处	1		旅游学院	
人事处	1		美术与设计学院	
膳食处	1		商学院	
石油工程学院	1		审计	
数学学院	1		实训中心	
体育学院	1		团委	
音乐学院	1		文史学院	
保卫处			心理咨询中心	
城市社会心理研究中心			信息网络中心	
城市信息与系统科学研究所			学位办公室	
传媒学院			幼儿师范学院	
创新创业学院			招生网	
党委（校长）办公室			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
191541	站点名称：甘肃文化翻译中心	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-03-02 17:14:23
191540	站点名称：甘肃文化翻译中心	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-03-02 17:14:22
191539	站点名称：甘肃文化翻译中心	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-03-02 17:14:22
191537	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	2018-03-02 15:18:56
191536	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	2018-03-02 15:18:54
191535	站点名称：卡务中心	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	2018-03-02 15:18:00
191530	站点名称：发展规划处	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-03-02 08:07:44
191529	站点名称：发展规划处	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-03-02 08:07:44
191528	站点名称：发展规划处	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-03-02 08:07:43
191527	站点名称：发展规划处	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	2018-02-28 20:15:45
191526	站点名称：发展规划处	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	2018-02-28 20:15:45
191525	站点名称：发展规划处	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	2018-02-28 20:15:44
191516	站点名称：发展规划处	185.153.198.252	欧洲和中东地区	含有非法请求参数	SQL注入	2018-02-26 14:11:12
191515	站点名称：发展规划处	185.153.198.252	欧洲和中东地区	含有非法请求参数	SQL注入	2018-02-26 14:11:11
191514	站点名称：发展规划处	185.153.198.252	欧洲和中东地区	含有非法请求参数	SQL注入	2018-02-26 14:11:10
191511	管理平台	42.91.2.43	甘肃省兰州市 电信	含有非法请求参数	错误帐号或密码	2018-02-25 22:48:55
191510	管理平台	42.91.2.43	甘肃省兰州市 电信	含有非法请求参数	错误帐号或密码	2018-02-25 22:48:29
191509	管理平台	125.71.43.205	四川省成都市 电信	含有非法请求参数	错误帐号或密码	2018-02-25 22:27:22
191508	管理平台	125.71.43.205	四川省成都市 电信	含有非法请求参数	错误帐号或密码	2018-02-25 20:48:09
191505	站点名称：城市社会心理研究中心（新）	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	2018-02-24 17:33:18
191504	站点名称：城市社会心理研究中心（新）	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	2018-02-24 17:33:18
191503	站点名称：城市社会心理研究中心（新）	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	2018-02-24 17:33:17
191502	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	2018-02-23 11:39:38
191501	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	2018-02-23 11:39:38
191500	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	2018-02-23 11:39:37
191499	站点名称：发展规划处	185.92.73.108	欧洲和中东地区	含有非法请求参数	SQL注入	2018-02-17 23:15:29
191498	站点名称：发展规划处	185.92.73.108	欧洲和中东地区	含有非法请求参数	SQL注入	2018-02-17 23:15:29
191497	站点名称：发展规划处	185.92.73.108	欧洲和中东地区	含有非法请求参数	SQL注入	2018-02-17 23:15:27
191496	站点名称：机关党委	91.247.38.61	乌克兰	含有非法请求参数	SQL注入	2018-02-17 08:10:29
191495	站点名称：机关党委	91.247.38.61	乌克兰	含有非法请求参数	SQL注入	2018-02-17 08:10:28
191494	站点名称：机关党委	91.247.38.61	乌克兰	含有非法请求参数	SQL注入	2018-02-17 08:10:27
191493	站点名称：党委组织部	185.92.73.109	欧洲和中东地区	含有非法请求参数	SQL注入	2018-02-15 23:52:08
191492	站点名称：党委组织部	185.92.73.109	欧洲和中东地区	含有非法请求参数	SQL注入	2018-02-15 23:52:08
191491	站点名称：党委组织部	185.92.73.109	欧洲和中东地区	含有非法请求参数	SQL注入	2018-02-15 23:52:06
191490	站点名称：党委宣传部	185.92.73.106	欧洲和中东地区	含有非法请求参数	SQL注入	2018-02-15 00:57:22
191489	站点名称：党委宣传部	185.92.73.106	欧洲和中东地区	含有非法请求参数	SQL注入	2018-02-15 00:57:22
191488	站点名称：党委宣传部	185.92.73.106	欧洲和中东地区	含有非法请求参数	SQL注入	2018-02-15 00:57:20
191487	站点名称：信息网络中心	61.178.98.67	甘肃省兰州市 电信	含有非法请求参数	SQL注入	2018-02-12 16:21:26
191486	站点名称：信息网络中心	61.178.98.67	甘肃省兰州市 电信	含有非法请求参数	SQL注入	2018-02-12 16:21:26
191485	站点名称：信息网络中心	61.178.98.67	甘肃省兰州市 电信	含有非法请求参数	SQL注入	2018-02-12 16:21:26
191484	站点名称：信息网络中心	61.178.98.67	甘肃省兰州市 电信	含有非法请求参数	SQL注入	2018-02-12 16:21:26
191483	站点名称：信息网络中心	61.178.98.67	甘肃省兰州市 电信	含有非法请求参数	SQL注入	2018-02-12 09:46:28
191482	站点名称：信息网络中心	61.178.98.67	甘肃省兰州市 电信	含有非法请求参数	SQL注入	2018-02-12 09:46:28
191481	站点名称：信息网络中心	61.178.98.67	甘肃省兰州市 电信	含有非法请求参数	SQL注入	2018-02-12 09:46:28
191475	站点名称：教务处	194.28.115.112	摩尔多瓦	含有非法请求参数	SQL注入	2018-02-01 08:06:19
191474	站点名称：教务处	194.28.115.112	摩尔多瓦	含有非法请求参数	SQL注入	2018-02-01 08:06:19
191473	站点名称：教务处	194.28.115.112	摩尔多瓦	含有非法请求参数	SQL注入	2018-02-01 08:06:18
191472	站点名称：兰州城市学院	106.120.101.58	北京市 电信	含有非法请求参数	SQL注入	2018-01-28 17:41:56
191471	站点名称：兰州城市学院	106.120.101.58	北京市 电信	含有非法请求参数	SQL注入	2018-01-28 17:41:56
191470	站点名称：兰州城市学院	106.120.101.58	北京市 电信	含有非法请求参数	SQL注入	2018-01-28 17:41:56
191469	管理平台	42.91.7.200	甘肃省兰州市 电信	含有非法请求参数	错误帐号或密码	2018-01-27 11:29:12
191468	站点名称：党委组织部	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-01-24 09:10:54
191467	站点名称：党委组织部	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-01-24 09:10:54
191466	站点名称：党委组织部	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-01-24 09:10:53
191465	站点名称：数学学院	94.130.237.171	乌克兰	含有非法请求参数	SQL注入	2018-01-23 21:07:40
191464	站点名称：数学学院	94.130.237.171	乌克兰	含有非法请求参数	SQL注入	2018-01-23 21:07:22
191463	站点名称：数学学院	94.130.237.171	乌克兰	含有非法请求参数	SQL注入	2018-01-23 21:04:06
191462	站点名称：卡务中心	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-01-23 17:18:43
191461	站点名称：卡务中心	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-01-23 17:18:42
191460	站点名称：卡务中心	110.87.188.33	福建省福州市 电信	含有非法请求参数	SQL注入	2018-01-23 17:18:42
191459	站点名称：电子与信息工程学院	120.32.41.124	福建省福州市 电信	含有非法请求参数	SQL注入	2018-01-23 10:17:15
191458	站点名称：电子与信息工程学院	120.32.41.124	福建省福州市 电信	含有非法请求参数	SQL注入	2018-01-23 10:17:15
191457	站点名称：电子与信息工程学院	120.32.41.124	福建省福州市 电信	含有非法请求参数	SQL注入	2018-01-23 10:17:15
191456	站点名称：兰州城市学院	113.0.90.88	黑龙江省哈尔滨市 联通	含有非法请求参数	SQL注入	2018-01-23 10:00:42
191455	站点名称：兰州城市学院	113.0.90.88	黑龙江省哈尔滨市 联通	含有非法请求参数	跨站脚本注入	2018-01-23 09:56:43
191454	站点名称：数学学院	94.130.237.171	乌克兰	含有非法请求参数	SQL注入	2018-01-22 00:02:14
191453	站点名称：数学学院	94.130.237.171	乌克兰	含有非法请求参数	SQL注入	2018-01-22 00:02:03
191452	站点名称：数学学院	94.130.237.171	乌克兰	含有非法请求参数	SQL注入	2018-01-22 00:01:44
191451	站点名称：数学学院	94.130.237.171	乌克兰	含有非法请求参数	SQL注入	2018-01-21 23:32:04
191450	站点名称：兰州城市学院	185.153.198.252	欧洲和中东地区	含有非法请求参数	SQL注入	2018-01-20 21:20:01
191449	站点名称：兰州城市学院	185.153.198.252	欧洲和中东地区	含有非法请求参数	SQL注入	2018-01-20 21:20:01
191448	站点名称：兰州城市学院	185.153.198.252	欧洲和中东地区	含有非法请求参数	SQL注入	2018-01-20 21:19:59
191447	站点名称：创新创业学院	59.56.149.78	福建省福州市 电信	含有非法请求参数	SQL注入	2018-01-20 16:53:07
191446	站点名称：创新创业学院	59.56.149.78	福建省福州市 电信	含有非法请求参数	SQL注入	2018-01-20 16:53:07
191445	站点名称：创新创业学院	59.56.149.78	福建省福州市 电信	含有非法请求参数	SQL注入	2018-01-20 16:53:06
191442	站点名称：传媒学院	59.56.149.78	福建省福州市 电信	含有非法请求参数	SQL注入	2018-01-18 15:42:13
191441	站点名称：传媒学院	59.56.149.78	福建省福州市 电信	含有非法请求参数	SQL注入	2018-01-18 15:42:13
191440	站点名称：传媒学院	59.56.149.78	福建省福州市 电信	含有非法请求参数	SQL注入	2018-01-18 15:42:13
191439	管理平台	27.224.147.48	甘肃省平凉市 电信	含有非法请求参数	错误帐号或密码	2018-01-17 20:16:46
191438	管理平台	123.151.77.72	天津市 电信IDC机房	含有非法请求参数	错误帐号或密码	2018-01-17 18:57:53
191435	站点名称：保卫处	117.28.207.144	福建省厦门市 电信	含有非法请求参数	SQL注入	2018-01-12 05:11:44
191434	站点名称：保卫处	117.28.207.144	福建省厦门市 电信	含有非法请求参数	SQL注入	2018-01-12 05:11:44
191433	站点名称：保卫处	117.28.207.144	福建省厦门市 电信	含有非法请求参数	SQL注入	2018-01-12 05:11:44
191429	站点名称：人事处	198.204.225.114	美国	含有非法请求参数	SQL注入	2018-01-09 15:49:15
191428	站点名称：人事处	198.204.225.114	美国	含有非法请求参数	SQL注入	2018-01-09 15:49:15
191427	站点名称：人事处	198.204.225.114	美国	含有非法请求参数	SQL注入	2018-01-09 15:49:14
191426	管理平台	42.92.184.69	甘肃省 电信	含有非法请求参数	错误帐号或密码	2018-01-09 15:36:12
191423	站点名称：兰州城市学院	10.0.125.142	局域网 对方和您在同一内部网	含有非法请求参数	跨站脚本注入	2018-01-08 23:50:13
191422	站点名称：兰州城市学院	10.0.125.142	局域网 对方和您在同一内部网	含有非法请求参数	跨站脚本注入	2018-01-08 23:48:04

191421	站点名称：信息网络中心	151.80.238.152	意大利	含有非法请求参数	SQL注入	2018-01-08 22:23:19
191420	管理平台	115.155.88.96	甘肃省兰州市 兰州大学	含有非法请求参数	错误帐号或密码	2018-01-08 11:35:40
191419	管理平台	115.155.88.96	甘肃省兰州市 兰州大学	含有非法请求参数	错误帐号或密码	2018-01-08 11:34:25
191418	管理平台	115.155.88.96	甘肃省兰州市 兰州大学	含有非法请求参数	错误帐号或密码	2018-01-08 11:29:00
191417	站点名称：信息网络中心	199.249.223.63	美国	含有非法请求参数	SQL注入	2018-01-06 22:18:52
191412	站点名称：膳食处	212.90.148.126	德国	含有非法请求参数	SQL注入	2018-01-04 23:36:23
191411	站点名称：膳食处	212.90.148.126	德国	含有非法请求参数	SQL注入	2018-01-04 23:36:19
191410	站点名称：膳食处	212.90.148.126	德国	含有非法请求参数	SQL注入	2018-01-04 23:36:16
191409	站点名称：膳食处	94.73.146.42	土耳其	含有非法请求参数	SQL注入	2018-01-04 22:47:01
191408	站点名称：信息网络中心	62.210.129.246	法国	含有非法请求参数	SQL注入	2018-01-04 19:02:51
191395	站点名称：兰州城市学院	117.28.207.190	福建省厦门市 电信	含有非法请求参数	SQL注入	2018-01-02 02:40:06
191394	站点名称：兰州城市学院	117.28.207.190	福建省厦门市 电信	含有非法请求参数	SQL注入	2018-01-02 02:40:06
191393	站点名称：兰州城市学院	117.28.207.190	福建省厦门市 电信	含有非法请求参数	SQL注入	2018-01-02 02:40:06
191392	站点名称：兰州城市学院	60.12.225.166	浙江省嘉兴市 联通	含有非法请求参数	跨站脚本注入	2018-01-01 14:27:40
191391	站点名称：兰州城市学院	60.12.225.166	浙江省嘉兴市 联通	含有非法请求参数	跨站脚本注入	2018-01-01 14:27:40
191390	站点名称：兰州城市学院	60.12.225.166	浙江省嘉兴市 联通	含有非法请求参数	跨站脚本注入	2018-01-01 14:27:40
191389	站点名称：兰州城市学院	60.12.225.166	浙江省嘉兴市 联通	含有非法请求参数	跨站脚本注入	2018-01-01 14:27:40
191388	站点名称：兰州城市学院	60.12.225.166	浙江省嘉兴市 联通	含有非法请求参数	SQL注入	2018-01-01 14:10:01

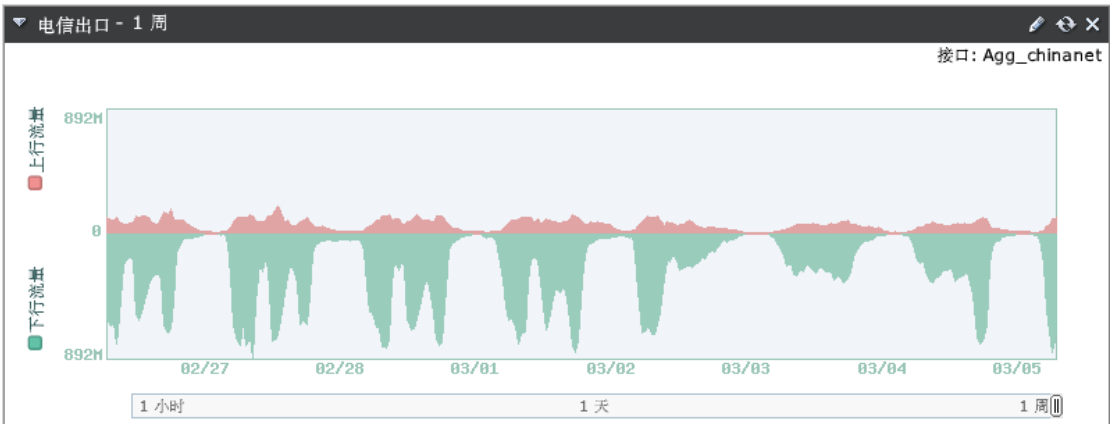
站群系统应用防火墙网站访问 IP 封禁记录

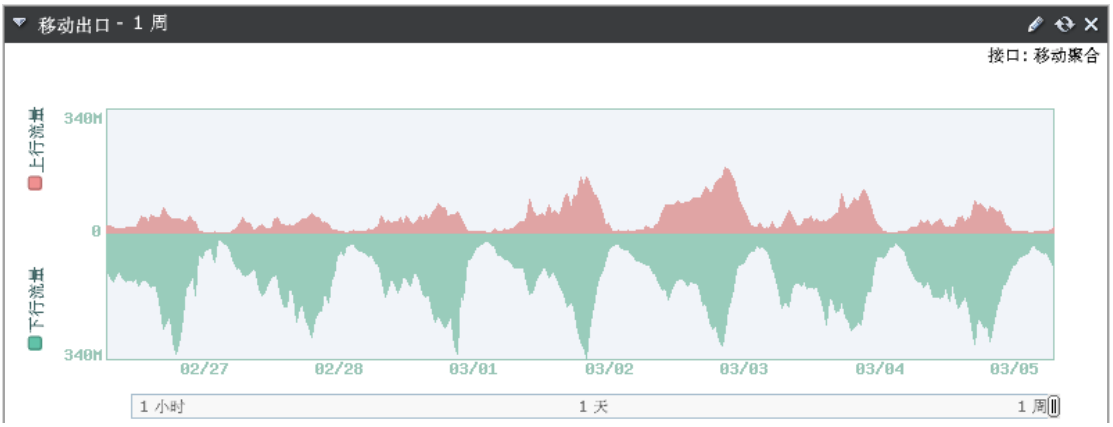
封禁IP	封禁IP归属地	封禁开始时间 ▼	封禁结束时间
110.87.188.33	福建省福州市 电信	2018-03-02 17:14:23	2018-03-02 18:54:23
118.180.5.174	甘肃省兰州市 网宿科技电信CDN节点	2018-03-02 15:18:56	2018-03-02 16:58:56
110.87.188.33	福建省福州市 电信	2018-03-02 08:07:44	2018-03-02 09:47:44
27.255.77.11	韩国 Ehost互联网数据中心	2018-02-28 20:15:45	2018-02-28 21:55:45
185.153.198.252	欧洲和中东地区	2018-02-26 14:11:12	2018-02-26 15:51:12
27.255.77.11	韩国 Ehost互联网数据中心	2018-02-24 17:33:18	2018-02-24 19:13:18
118.180.5.174	甘肃省兰州市 网宿科技电信CDN节点	2018-02-23 11:39:38	2018-02-23 13:19:38
185.92.73.108	欧洲和中东地区	2018-02-17 23:15:29	2018-02-18 00:55:29
91.247.38.61	乌克兰	2018-02-17 08:10:29	2018-02-17 09:50:29
185.92.73.109	欧洲和中东地区	2018-02-15 23:52:08	2018-02-16 01:32:08
185.92.73.106	欧洲和中东地区	2018-02-15 00:57:22	2018-02-15 02:37:22
61.178.98.67	甘肃省兰州市 电信	2018-02-12 16:21:26	2018-02-12 18:01:26
61.178.98.67	甘肃省兰州市 电信	2018-02-12 16:21:26	2018-02-12 18:01:26
61.178.98.67	甘肃省兰州市 电信	2018-02-12 09:46:28	2018-02-12 11:26:28
194.28.115.112	摩尔多瓦	2018-02-01 08:06:19	2018-02-01 09:46:19
106.120.101.58	北京市 电信	2018-01-28 17:41:56	2018-01-28 19:21:56
110.87.188.33	福建省福州市 电信	2018-01-24 09:10:54	2018-01-24 10:50:54
94.130.237.171	乌克兰	2018-01-23 21:07:40	2018-01-23 22:47:40
110.87.188.33	福建省福州市 电信	2018-01-23 17:18:43	2018-01-23 18:58:43
120.32.41.124	福建省福州市 电信	2018-01-23 10:17:15	2018-01-23 11:57:15
94.130.237.171	乌克兰	2018-01-22 00:02:14	2018-01-22 01:42:14
185.153.198.252	欧洲和中东地区	2018-01-20 21:20:01	2018-01-20 23:00:01
59.56.149.78	福建省福州市 电信	2018-01-20 16:53:07	2018-01-20 18:33:07
59.56.149.78	福建省福州市 电信	2018-01-18 15:42:13	2018-01-18 17:22:13
117.28.207.144	福建省厦门市 电信	2018-01-12 05:11:44	2018-01-12 06:51:44
198.204.225.114	美国	2018-01-09 15:49:15	2018-01-09 17:29:15
212.90.148.126	德国	2018-01-04 23:36:23	2018-01-05 01:16:23
117.28.207.190	福建省厦门市 电信	2018-01-02 02:40:06	2018-01-02 04:20:06
60.12.225.166	浙江省嘉兴市 联通	2018-01-01 14:27:40	2018-01-01 16:07:40

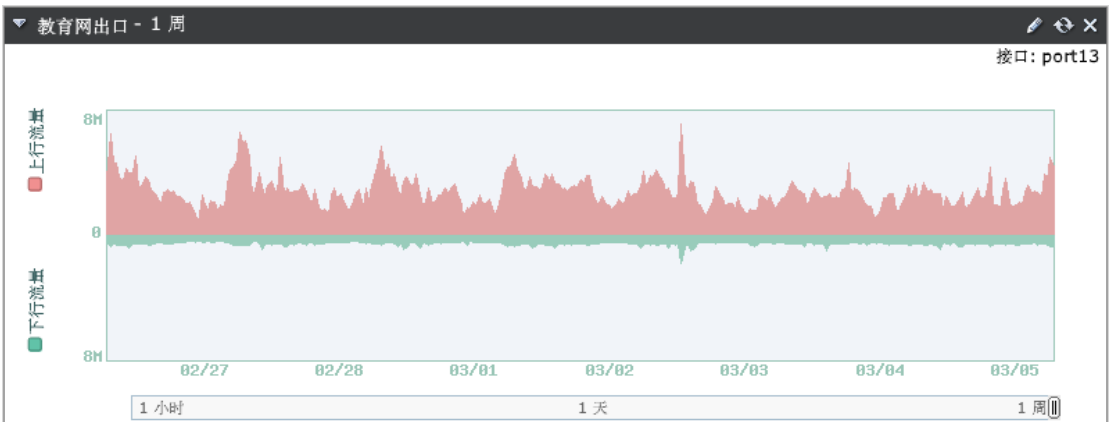
站群系统应用防火墙网站危险文件扫描记录

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

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）

注：存在“服务器配置信息泄露”风险，“发现 robots.txt 文件”。

监控对象	类型	监测点	响应时间	访问成功率	
学校OA系统【http://oa.lzcu.edu.cn】	源站监控	3 1	341.1 ms	75 %	详情
学校OA系统【http://oa.lzcu.edu.cn】	源站监控	3 1	319.74 ms	75 %	详情
学校主页【http://www.lzcu.edu.cn】	源站监控	3 1	229.41 ms	75 %	详情
学校主页【http://www.lzcu.edu.cn】	源站监控	3 1	358.4 ms	75 %	详情

网站安全检测二（百度云观测）

http://www.lzcu.edu.cn　　更新时间：2018-03-04 19:12:37

指数评价

所属行业：教育培训

30.10% ↓

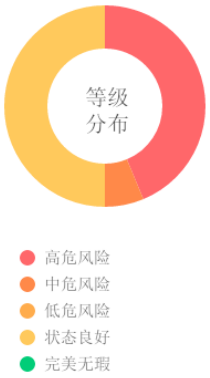
战胜了全国 0.00% 的网站

关联网站安全

关联网站数　　最低指数评价

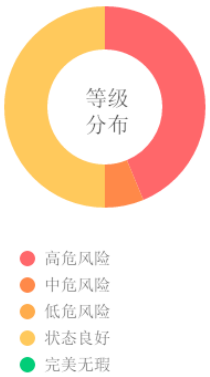
查看更多>>

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。



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>>
ecard.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>>
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>>

当前 1 / 2 页　首页　上一页　下一页　尾页



域名	指数评价	操作
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

【两会快评】防范网络风险 安全素养不可少

人民网科普 2018-03-05 08:22:00

智能摄像头上“捣捣鬼”，APP 上打“马虎眼”，“扫一扫”中藏危险……两会期间，不少代表委员对网络安全问题深有感触，构建更全面的网络安全体系已成为共识。

全国政协委员、中国电子信息产业发展研究院院长卢山说，去年工信部下架改号 APP 超过 2000 个，其中利用新手段破坏网络安全事件占比相当大。全国政协委员、360 集团董事长周鸿祎则认为，网民应具备一定的防身技能，相关部门也要在预警防御上有新突破。

其实，一些网络安全事件的受害者，不一定是被技术水平强大的黑客专门盯上了，而是在使用互联网产品时麻痹大意，“明知山有虎，偏向虎山行”。作为网络素养的重要组成部分，每个人都应当具备一定的网络安全意识与能力。

以最近时有媒体曝光的网络摄像头泄露隐私事件为例。一些用户购买不正规的小厂商生产的摄像头，其本身的安全水准就不达标，所以很容易被人窃取监控画面；很多用户在使用远程监控功能时，没有意识到自己的隐私被“直播”到了网上。发生这些问题，既有厂商没有履行提醒和告知义务的原因，也有用户对产品属性和功能了解不够全面的原因。

互联网安全不仅是一门技术，还是一种素养。就像在现实中，你家安装多高级的防盗门，是技术问题；而出门时有没有把防盗门关严实，会不会在关上防盗门的同时留下了一扇敞开的窗户，则是安全素养问题。

相比之下，机构用户更应该把网络安全素养放在网络安全工作的中心位置。

跟个人用户不同，机构用户维护系统的成本较高，一些机构的软件系统长期不更新，埋下了安全隐患。这两年常有新闻曝光，机场、高校等公共机构成为勒索病毒的受害者。这些受害机构，平时使用较为传统的网络安全防护手段，在网络安全方面的投入较少，一旦中招，就导致大规模的设备瘫痪。

面对花样百出的网络安全问题，政府部门同样也要不断提高互联网安全意识，用符合互联网规律的治理手段，对危害互联网安全的违法犯罪分子实施精准打击。

“徐玉玉被诈骗案”曝光以后，电信网络诈骗案件成了公众关心的痛点。据报道，2017 年全国公安机关共破获电信网络诈骗案件 7.8 万起，查处违法犯罪人员 4.7 万名，同比分别上升 55.2%、50.77%。尽管公安机关的打击力度不断加强，但电信网络诈骗作案人员依然存在侥幸心理。

被动的、事后的打击，显然不足以建立起完善的网络安全体系。政府部门应针对网络安全问题制定新规则，从源头上掐断违法犯罪者的命门。比如，平台如何管理用户数据，如何定义网络隐私，就需要新的规则界定。

正如很多人所说的，网络技术本身无所谓好坏，它既可以服务于大众，也可能成为公共安全的毒瘤。显然，只有确立了正确的意识，具备了必要的安全素养，才能确保技术始终走在正道上。

【安全分析】2018 年五大网络安全趋势（摘录）

行长叠报 2018-01-27 09:20:11

鉴于去年网络攻击事件数量急剧上升，普华永道印度网络安全负责人 Sivarama Krishnan 列出了五大趋势，以此界定 2018 年印度的网络安全形势。

趋势一：个人隐私和数据保护。

个人隐私和数据保护将成为 2018 年的重点。Aadhaar 泄密事件[1]已经引发了所有人对个人隐私和数据保护的担忧。

因此，信息数据安全将在 2018 年处于核心地位。首先，欧盟的“一般数据保护条例”（GDPR）将对跨国公司产生很大的影响。

其次，印度最高法院支持“隐私权”的裁决也会影响安全形势。各个机构将更加关注对先进的加密和密钥管理技术的更新，以保护客户数据。

纵观全世界也是如此，客户数据安全在互联网行业竞争中将变得更加激烈，网络安全关系到拥有大数据的企业的生死存亡。

趋势二：机器学习日趋成熟。

网络安全中的机器学习（machine learning）将在经历一个短暂的低谷后，进一步成熟完善。

由于大家都希望拥有实时预测网络安全事件的技术，市场将会出现更多的相关产品，研发者也会进一步付诸行动，并将重点放在机器学习的实际效果上。

趋势三：私人订制安全解决方案。

随着黑客对不同组织和用户发起的针对性的攻击，网络威胁情况变得越来越复杂，安全部门正逐渐认识到需要为不同的组织设计特有的安全层。

因此，安全部门将探索非标准解决方案，包括构建内部功能以满足网络安全要求。由于每个企业的性质不同，他们也会更多地投资于本地化的解决方案或者产品。

趋势四：安全创业公司黄金期。

随着对定制解决方案的需求不断增长，以及对已经公开的解决方案的担忧，网络安全创业公司将获得更多活力，并可能在 2018 年达到一个临界点。

许多大型银行、通讯公司、保险公司、政府机构和电子商务公司等等，则会发现之前的安全产品和解决方案在市场上不再具有竞争力，从而迫使研发者重新构建和实施更加创新的安全解决方案。

趋势五：回归本源。

安全部门会关注基础性的东西。虽然恶意软件和勒索软件的攻击将持续增长，但安全部门将会重新关注和保护真正重要的内容，如个人定位、数据储存等。

重点将从保护端点到保护组织数据，无论它是在物理数据中心还是在云端。

加密、访问权限、云安全和安全 DevOps 将成为 2018 年的一些关键举措。

总结

2018 年，由于复杂和有针对性的网络攻击的频率不断增加，迫使安全部门加强他们的网络防御，同时也会受到更多攻击者的威胁。

注释：Aadhaar 泄密事件

自 2009 年起，印度开始推行生物身份识别项目 Aadhaar，至今已经收集了 11.3 亿印度居民和公民的生物识别数据（照片、十指指纹和虹膜扫描），这些数据能为每个人提供一个唯一的 12 位身份证明编号。但是越来越多的证据表明，政府对这个数据库的保护做得并不到位，这些信息正面临着严重的泄露危机。

2018 年 1 月 4 日，印度《论坛报》称，有人正在以低得惊人的价格出售 Aadhaar 数据库。

该消息由一位名叫 Bharat Bhushan Gupta 的乡村企业家爆出。Gupta 表示，此前有人在移动社交工具 WhatsApp 上向他退推销 Aadhaar 数据库。购买之后他发现，Aadhaar 数据库为他提供了大量意想不到的用户信息。

考虑到这可能会涉及到大规模的隐私泄露，于是 Gupta 主动向印度特立识别委员会（UIDAI）反映了该问题。之后，Gupta 又联系了印度《论坛报》的记者 Rachna Khaira。随后，Rachna Khaira 对这一事件展开了一些调查并发文报道。

抄送：校领导