网络信息安全周报

【2017】第 33 期

党委宣传部
信息网络中心 编

2017 年 12 月 14 日

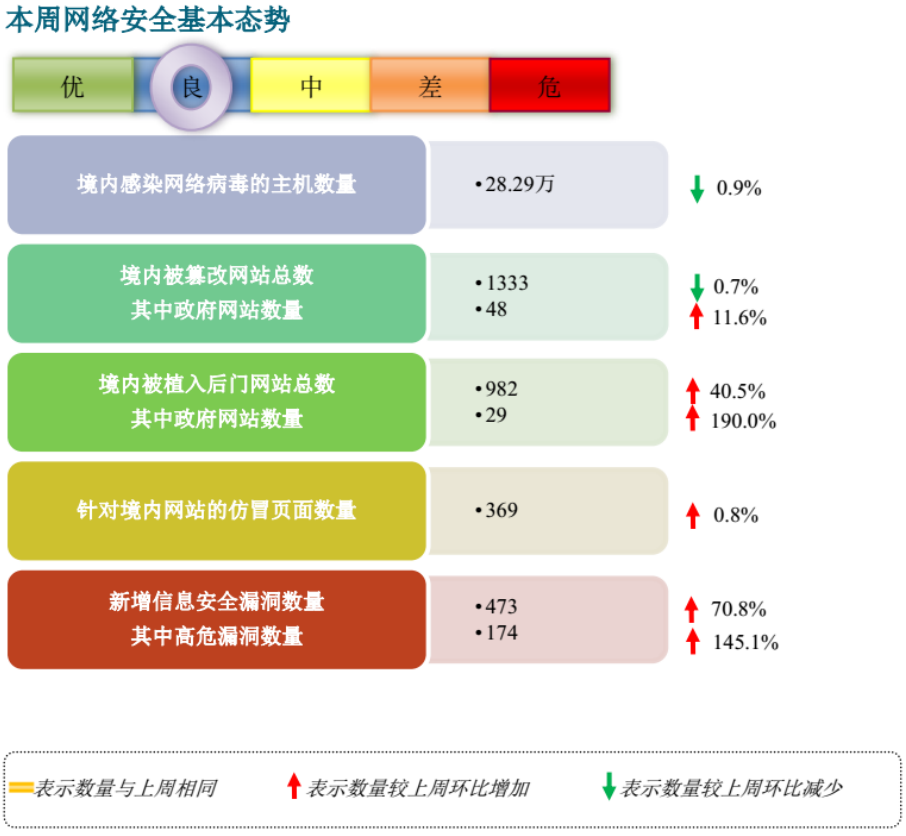
本期要目

- 【权威发布】全国网络安全信息与动态（2017 年 11 月 27 日-12 月 3 日）
- 【城院 IT】综合业务管理平台统计信息(2017 年 12 月 4 日—12 月 10 日)
- 【学习中国】习近平为构建网络空间命运共同体提供基本遵循
- 【经验介绍】WiFi 钥匙 APP 防蹭网，保障家庭网络安全！

全国网络安全信息与动态

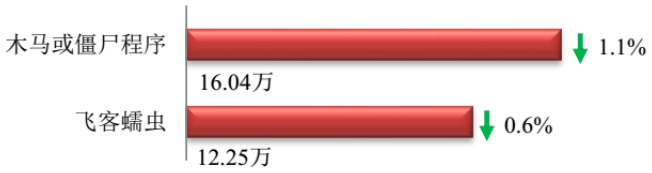
（2017 年 11 月 27 日-12 月 3 日）

根据国家互联网应急中心最新公告数据：



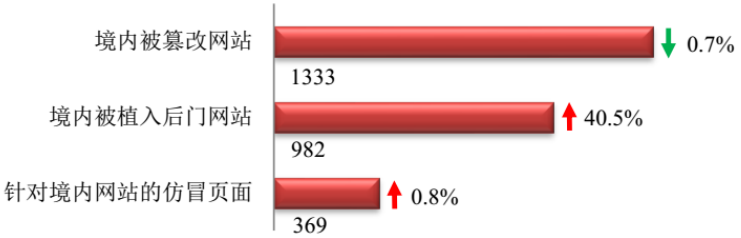
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 28.29 万个，其中包括境内被木马或被僵尸程序控制的主机约 16.04 万以及境内感染飞客（conficker）蠕虫的主机约 12.25 万。



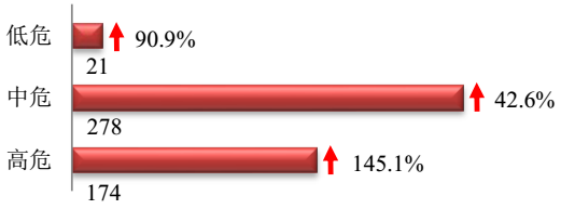
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1333 个；境内被植入后门的网站数量为 982 个；针对境内网站的仿冒页面数量为 369。



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 473 个，信息安全漏洞威胁整体评价级别为中。



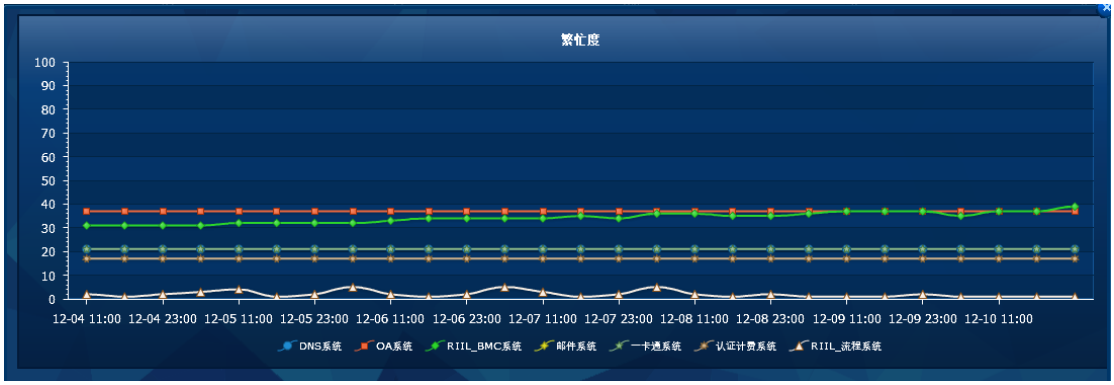
本周事件处理情况

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 463 起，其中跨境网络安全事件 210 起。

城院 IT 综合业务管理平台统计信息

(2017 年 12 月 4 日—12 月 10 日)

主要业务服务繁忙度



网站集群网页更新情况统计

站点名称	发布数量	站点名称	发布数量
兰州城市学院	30	档案馆	
外国语学院	30	党委（校长）办公室	
党委组织部	19	党委宣传部	
就业服务网	10	电子信息科学与技术研究所	
教学质量监测与评估中心	7	甘肃省高等学校外语教学指导委员会	
传媒学院	6	甘肃文化翻译中心	
地理与城乡规划学院	6	甘肃张芝书法院	
商学院	4	国有资产管理处	
文史学院	4	后勤管理处	
路易艾黎研究中心	3	机关党委	
音乐学院	3	基本建设处	
发展规划处	2	教师发展中心	
化学与环境工程学院	2	卡务中心	
教育学院	2	科学研究处	
兰州城市学院校医院	2	旅游学院	
廉政网	2	美术与设计学院	
马克思主义学院	2	人事处	
党委学生工作部	1	膳食处	
电子与信息工程学院	1	审计	
机械工程学院	1	实训中心	
教务处	1	数学学院	
石油工程学院	1	体育学院	
信息网络中心	1	团委	
幼儿师范学院	1	心理咨询中心	
保卫处		信息技术教育与应用研究所	
城市社会心理研究中心		学位办公室	
城市信息与系统科学研究所		招生网	
创新创业学院		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
191296	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	2017-12-08 00:49:36
191295	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	2017-12-08 00:49:35
191294	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	2017-12-08 00:49:35
191293	站点名称：廉政网	110.87.188.33	福建省福州市 电信	含有非法请求参数	跨站脚本注入	2017-12-07 06:13:33
191292	站点名称：廉政网	110.87.188.33	福建省福州市 电信	含有非法请求参数	跨站脚本注入	2017-12-07 06:13:23
191291	站点名称：廉政网	110.87.188.33	福建省福州市 电信	含有非法请求参数	跨站脚本注入	2017-12-07 06:12:53
191290	站点名称：就业服务网	198.204.225.114	美国	含有非法请求参数	SQL注入	2017-12-06 22:43:57
191289	站点名称：就业服务网	198.204.225.114	美国	含有非法请求参数	SQL注入	2017-12-06 22:43:56
191288	站点名称：就业服务网	198.204.225.114	美国	含有非法请求参数	SQL注入	2017-12-06 22:43:55
191285	站点名称：卡务中心	185.92.73.108	欧洲和中东地区	含有非法请求参数	SQL注入	2017-12-05 17:33:47
191284	站点名称：卡务中心	185.92.73.108	欧洲和中东地区	含有非法请求参数	SQL注入	2017-12-05 17:33:46
191283	站点名称：卡务中心	185.92.73.108	欧洲和中东地区	含有非法请求参数	SQL注入	2017-12-05 17:33:15

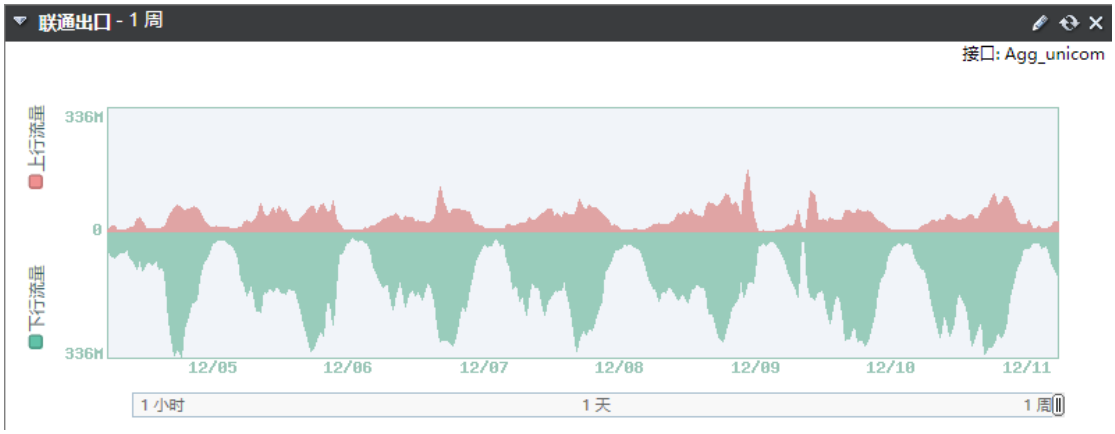
站群系统应用防火墙网站访问 IP 封禁记录

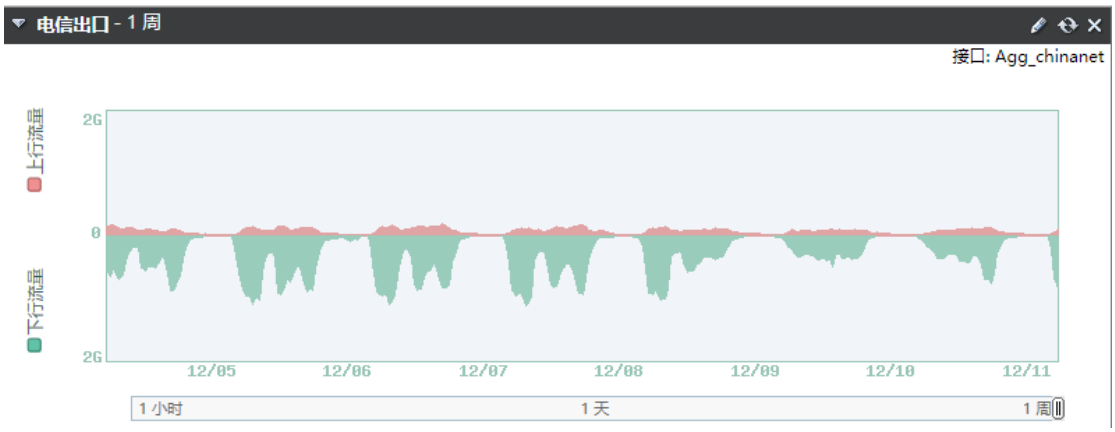
封禁IP	封禁IP归属地	封禁开始时间 ▼
118.180.5.174	甘肃省兰州市 网宿科技电信CDN节点	2017-12-08 00:49:36
110.87.188.33	福建省福州市 电信	2017-12-07 06:13:33
198.204.225.114	美国	2017-12-06 22:43:57
185.92.73.108	欧洲和中东地区	2017-12-05 17:33:47

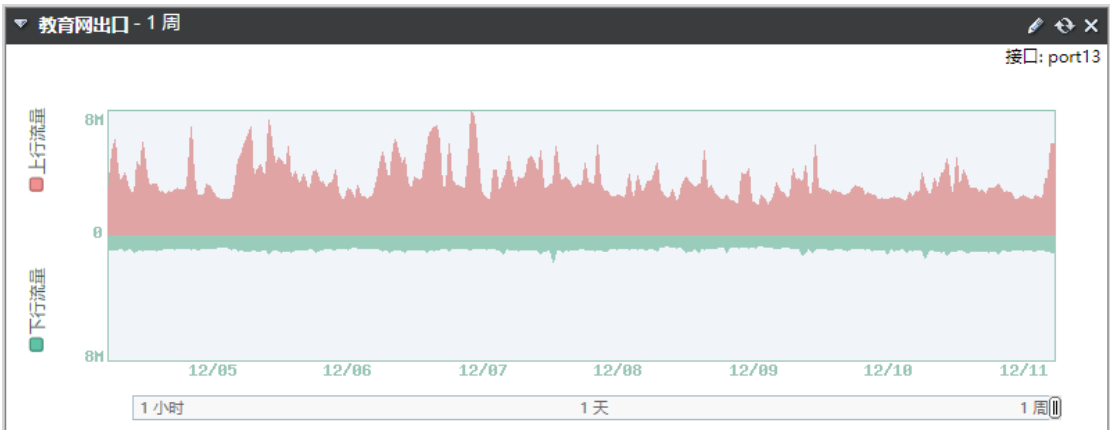
站群系统应用防火墙网站危险文件扫描记录

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



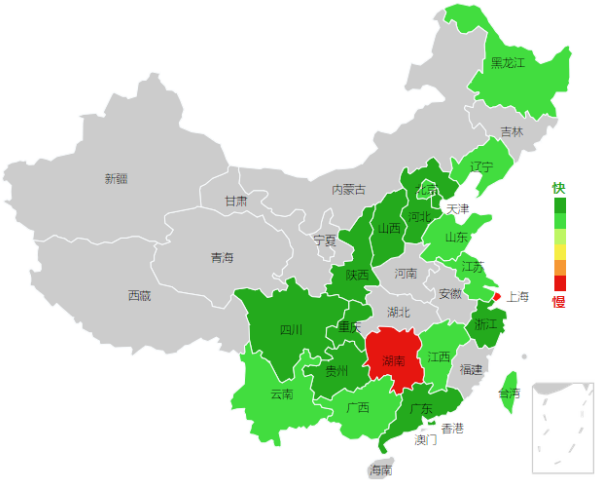




APT统计

防火墙统计	
恶意	2401
检测到0-day恶意软件变种	0
可疑文件	0
安全文件	81447468

360 网站测速（http://www.lzcu.edu.cn）



平均速度排行		
名次	省份	平均速度(KB/s)
1	陕西	1,131.89
2	山西	504.33
3	天津	477.57

北京					
监测点	运营商	总耗时/ms	解析时间/ms	连接时间/ms	下载时间/ms
北京市	电信	1443.12	1254.01	30.79	158.33

360 网站评分（http://www.lzcu.edu.cn）

360 网站 DNS 检测（http://www.lzcu.edu.cn）

输入源IP	归属地
219.246.21.192	甘肃兰州教育网

解析结果IP	所用DNS	所属运营商
219.246.21.192	101.226.4.6(上海电信) 114.114.114.114(114DNS.COM114DNS.COM) 8.8.8.8(GOOGLE.COMGOOGLE.COMlevel3.com) 121.28.148.33(河北石家庄联通) 168.95.1.1(台湾cht.com.tw) 125.71.5.51(四川成都电信)	电信 其他 其他 联通 其他 电信

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	356.67 ms	75 %
学校OA系统【http://oa.lzcu.edu.cn】	源站监控	3 1	324.19 ms	75 %
学校主页【http://www.lzcu.edu.cn】	源站监控	3 1	266.88 ms	75 %
学校主页【http://www.lzcu.edu.cn】	源站监控	3 1	357.77 ms	75 %

网站安全检测二（百度云观测）

http://www.lzcu.edu.cn　　更新时间：2017-12-10 20:13:30

指数评价

所属行业：教育培训

22.01% ↓

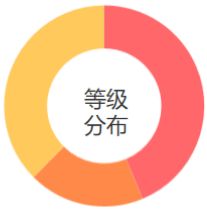
战胜了全国 **0.00%** 的网站

关联网站安全

关联网站数	最低指数评价
16	4.0 高危

查看更多>>

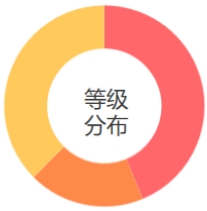
该网站安全指数评价 高危 但是仍存在改进空间。建议 开启云观测服务>> ，查看评价详情，获取最新网站安全报警，及时修复以免被搜索引擎风险标识或降权。



- 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	49 中危	查看详情>>
ecard.lzcu.edu.cn	41.2 中危	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	34 高危	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



- 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
old.lzcu.edu.cn	44 中危	查看详情>>
pop.lzcu.edu.cn	5.8 高危	查看详情>>
smtp.lzcu.edu.cn	4 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

【学习中国】习近平为构建网络空间命运共同体提供基本遵循

学习中国 2017-12-10 20:34:18

“天下兼相爱则治，交相恶则乱。”网络空间是人类共同的活动空间，网络空间前途命运应由世界各国共同掌握。12 月 3 日，习近平在致第四届世界互联网大会的贺信中强调，“大家的事由大家商量着办，做到发展共同推进、安全共同维护、治理共同参与、成果共同分享”。这又一次丰富和发展了互联网治理的中国方案，为携手共建网络空间命运共同体提供了基本遵循。请随“学习中国”小编一起学习。

2015 年 12 月 16 日，第二届世界互联网大会在浙江省乌镇开幕。国家主席习近平出席开幕式并发表主旨演讲。

发展共同推进。互联网是社会发展的新引擎。中国从 1994 年全功能接入国际互联网至今，短短 23 年间，中国互联网发展取得了举世瞩目的成就。截止 2017 年 6 月，我国网民规模已达 7.51 亿，互联网普及率达到 54.3%；电子商务交易额约占全球电子商务零售市场的 39.2%；移动支付交易规模超过 81 万亿元。中国网民数量全球第一，电子商务总量全球第一，电子支付总额全球第一……中国互联网飞速发展不仅成为拉动中国经济增长的“引擎”，并且也为世界经济注入了强大动力。同时，中国积极主动地向世界分享自己的经验和机遇。中国连续四年举办世界互联网大会，希望搭建全球互联网共享共治平台，共同推动互联网健康发展。中国积极推进“一带一路”建设信息化发展，以信息化建设带动与沿线国家的经济合作伙伴关系，打造互联互通生态链，构建网络空间命运共同体。习近平指出：“中国数字经济发展将进入快车道。中国希望通过自己的努力，推动世界各国共同搭乘互联网和数字经济发展的快车。”

安全共同维护。当前，世界主要国家都已进入网络空间战略集中部署期，同时网络安全问题也越来越严重。网络犯罪，网络恐怖以及网络攻击等网络公害越发严重；木马僵尸网络、钓鱼网站等非传统网络安全威胁有增无减；物联网、云计算、大数据等新技术新应用、数据和用户信息泄露等的网络安全问题日益突出；不少网络犯罪分子还将触角伸向了跟人们生活息息相关的网络终端，网络安全形势与挑战日益严峻复杂。网络安全是全球性挑战，没有哪个国家能够置身事外、独善其身。网络空间，不应成为各国角力的战场，更不能成为违法犯罪的温床。习近平指出：“各国应该共同努力，防范和反对利用网络空间进行的恐怖、淫秽、贩毒、洗钱、赌博等犯罪活动。不论是商业窃密，还是对政府网络发起黑客攻击，都应该根据相关法律和国际公约予以坚决打击。”

治理共同参与。随着世界多极化、经济全球化、文化多样化、社会信息化深入发展，网络空间的竞争也愈演愈烈。网络领域发展不平衡、规则不健全、秩序不合理等问题日益凸显；不同国家和地区信息鸿沟不断拉大，现有网络空间治理规则难以反映大多数国家意愿和利益。只有推动互联网全球治理体系变革，建立新的全球互联网治理体系，才能满足各国网络发展要求，

更好地造福各国人民。中国是全球互联网治理体系的捍卫者，也是身体力行的践行者。在 G20、金砖国家、亚太经济合作组织、上海合作组织等国际框架和多边机制内，中国大力推动建立信息化领域国际互信对话机制；在移动通信、“互联网+”、云计算、物联网等关键技术和重要领域，中国积极参与国际标准制定。习近平指出：“国际网络空间治理，应该坚持多边参与，由大家商量着办，发挥政府、国际组织、互联网企业、技术社群、民间机构、公民个人等各个主体作用，不搞单边主义，不搞一方主导或由几方凑在一起说了算。”

成果共同分享。今日中国，互联网成果正在全面渗透实体经济的方方面面，造福各行各业。互联网教育、互联网医疗、互联网养老促进了城乡协调和共享发展；电子商务交易额从 2012 年的 7.89 万亿元增长到 2016 年年底的 22.97 万亿元；微信支付、支付宝支付等移动支付模式加速推进我国迈向无现金社会时代，在中国，无论是扫码支付、共享单车还是网上购物，一部手机就可以全部搞定。电子商务、移动支付和社交通信等应用正成为很多国家人民向往和羡慕的新生活方式。中国人民愿意让我们的互联网发展成果惠及世界各国。

“一枝独放不是春，百花齐放春满园”，互联网是人类的共同家园，习近平提出的“四个共同”，为全球互联网治理于发展贡献了新的中国智慧。

【经验介绍】WiFi 钥匙 APP 防蹭网，保障家庭网络安全！

2017-12-10 10:05:15 人民网

小编经常会接到小伙伴的反馈：家里是 50M 的光纤宽带，但有时下载速度却只有 125KB/s，尝试过修改密码后网速变正常，但不久网速又变慢了，是不是我家路由器有问题？

在此，路由君表示：

那么出现这种情况究竟是什么原因导致的呢？

其实很大可能是因为你家的 WiFi 被蹭了

我家 WiFi 为啥被蹭了？

1.WiFi 没有设置密码，或使用简单密码，如 12345678，陌生人很容易就能蹭网。

2.WiFi 密码被泄露。在这个无 WiFi 不生活的年代，为省流量很多人都会安装 WIFI 破解 APP，其实它不是密码破解工具，而是密码分享工具，在你“破解”他人 WiFi 的同时也将自己的 WiFi 分享出去了.手机安装 WiFi 破解 APP 后，它会将你家的无线网络信息共享到了蹭网服务器上，陌生人搜到该无线信号就能获得 WiFi 密码。

被蹭网有什么危害？

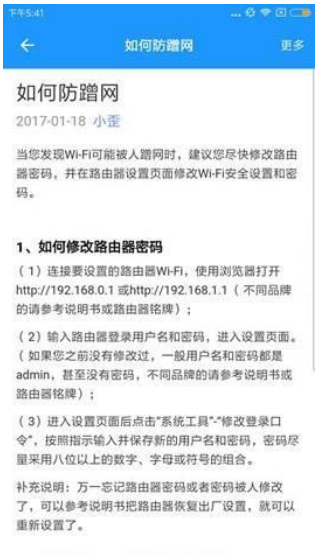
1.影响网络稳定，占用带宽，造成网速慢、网络掉线、卡顿等；

2.威胁网络安全与个人隐私，蹭网后路由器容易被入侵，蹭网者将有机会利用 DNS 欺骗、劫持等方法，把用户引入搭设好的钓鱼网站，伺机盗取用户隐私、个人信息、支付密码，并最终窃取财产。

如何查看家里的 WiFi 被蹭网了？

这个很简单，手机通过 WiFi 钥匙 APP 就能够检测当前当前连接 WiFi 的连接人数，并且能够直观地看到连接的具体设备是什么。如果这些设备中有你不认识的设备，那就是蹭网的人。点击【安检测速】-【防蹭网扫描】就能查看。

而如何防蹭网？上图中最下面的几个字瞧见了吗？点击【如何防蹭网】进去，就有小编为各位歪粉准备的防蹭网攻略。包括如何修改路由器密码、如何修改 WiFi 密码，精准的攻略都在这里哦~下载 WiFi 钥匙就可以获取最全的防蹭网攻略！



抄送：校领导