**四川省公共互联网网络安全态势分析通报（2021年7月）**

**四川省通信管理局**

**2021年8月**

目录

[一、 本月公共互联网基本情况分析 2](#_Toc81231519)

[1.省内互联网用户访问流量情况 2](#_Toc81231520)

[2.省内互联网用户访问协议情况 3](#_Toc81231521)

[3.省内互联网用户访问域名分布情况 4](#_Toc81231522)

[二、 本月公共互联网网络安全态势 4](#_Toc81231523)

[1.木马、僵尸网络 4](#_Toc81231524)

[2.网页篡改 6](#_Toc81231525)

[3.网页后门 7](#_Toc81231526)

[三、 本月工业互联网网络安全态势 8](#_Toc81231527)

[1.网络安全威胁情况 9](#_Toc81231528)

[2.工业设备安全漏洞情况 10](#_Toc81231529)

[3.行业安全态势分析 12](#_Toc81231530)

[4.地域安全态势分析 12](#_Toc81231531)

[四、 重要网络安全威胁预警 14](#_Toc81231532)

[1.国家网信办关于下架“滴滴企业版”等25款App的通报 14](#_Toc81231533)

[2.中央网信办、国家发展改革委、工业和信息化部印发《关于加快推进互联网协议第六版（IPv6）规模部署和应用工作的通知》 14](#_Toc81231534)

[3.工信部通报145款侵害用户权益行为APP 15](#_Toc81231535)

[4.工信部关于下架侵害用户权益APP名单的通报 15](#_Toc81231536)

[5.工信部、国家网信办、公安部联合印发《网络产品安全漏洞管理规定》 16](#_Toc81231537)

[6.工信部大力推进APP开屏弹窗信息骚扰用户问题整治 16](#_Toc81231538)

## **本月公共互联网基本情况分析**

## **1.省内互联网用户访问流量情况**

**1.1省内流量访问整体情况**

通过对省内网络流量的持续监测，2021年7月四川省内流量总体正常，未发生较大规模流量攻击安全事件，主要传输协议以TCP协议为主、端口以80端口流量为主。在基础电信企业日均流量方面，以中国移动流量占比最高，为13.98Tbps。



**图1.1 2021年7月四川省内流量监测情况**

**1.2访问省内网站流量地域分布情况**

通过对省内网络流量的持续监测，访问我省网站流量按地区分布总体情况如图1.2所示，可以发现除四川外北京访问四川省内网站流量最多。除本省外，排名前三位的地区依次为北京、重庆、云南。

**图1.2 2021年7月访问四川省内流量地域分布情况**

## **2.省内互联网用户访问协议情况**

通过对省内骨干网路由器传输协议的持续监测，2021年7月四川省内互联网用户访问网络的协议前两位占比情况如图1.3所示，分别为tcp、udp。

**图1.3 四川省内路由器协议占比情况**

## **3.省内互联网用户访问域名分布情况**

2021年7月，通过对省内互联网用户访问数据的持续监测，域名访问前十整体情况如图1.4所示，通过分析可以发现，省内公众上网类型主要为小视频、云服务、生活服务类等，通过域名访问数量也可以发现，在国内主流互联网公司中，腾讯、字节跳动等大型互联网公司榜上有名。

**图1.4 四川省内域名访问情况**

## **本月公共互联网网络安全态势**

本月，四川省公共互联网网络安全状况整体评价为“良”。省内基础网络运行总体平稳，互联网骨干网各项监测指标正常，未发生较大以上网络安全事件。

## **木马、僵尸网络**

四川省本月有56589个IP地址对应的主机被木马或僵尸程序控制，环比下降181.73%。2020年7月-2021年7月四川省木马和僵尸程序受控主机IP数量月度分布如图2.1所示，本月较上月大幅度下降。

**图2.1四川省木马或僵尸程序受控主机IP数量月度分布图**

四川省本月有6456个IP地址存在木马或僵尸程序控制服务器，环比下降22.17%。2020年7月-2021年7月四川省木马和僵尸程序控制服务器IP数量月度分布如图2.2所示，本月呈下降趋势。

**图2.2四川省木马或僵尸程序控制服务器IP数量月度分布图**

四川省本月各市州主机感染僵尸木马数量如图2.3所示，前三位依次为成都、绵阳、达州，其中成都数量最多，有33463台主机感染僵尸木马。

**图2.3四川省内各市州主机感染僵尸木马主机数量分布**

## **网页篡改**

本月，主机位于四川地区的被篡改网站数量为382个，环比下降20.91%。2020年7月-2021年7月，四川省内被篡改网站数量月度分布如图2.4所示，本月较上月小幅下降。

**图2.4四川省被篡改网站数量月度分布图**

四川省本月各市州网站网页篡改数量比例如图2.5所示，前三位依次为成都、绵阳、乐山，其中成都最多，被篡改网站数量为287个。

**图2.5四川省内各市州网页篡改被网站数量分布**

## **网页后门**

主机位于四川省被植入87个，环比下降56.06%。2020年7月-2021年7月，四川省内被植入后门网站月度分布情况如图2.6所示，整体呈下降趋势。

**图2.6四川省被植入后门的网站主机数量月度分布图**

四川省本月各市州网站后门数量比例如图2.7所示，前三位依次为成都、绵阳、乐山，其中成都数量最多，达55个。

**图2.7四川省被植入后门的网站主机数量月度分布图**

## **本月工业互联网网络安全态势**

截至 2021年7月31日，四川省工业互联网安全态势感知平台（以下简称平台）监测发现我省联网工业企业 11,346家、工业设备 17.85 万台、工业 APP 15,203 款。累计共发现63家工业互联网平台，其中10家平台归属于四川省。

近期，我省工业互联网安全态势整体平稳，无重大安全事件发生。2021年7月我省总体安全威胁数量较上月有所增加，其中木马后门威胁事件达63,129次，占总体威胁数量的62.39%；攻击类型主要包括木马后门、Web攻击、非法外联等；从被攻击的行业来看，攻击事件主要分布在橡胶和塑料制品业、汽车制造业和房地产业等；从被攻击的地域来看，被攻击的地市主要包括成都市、德阳市和泸州市，威胁事件数量占据全省总数的99.90%；从境外攻击视角来看，境外恶意网络攻击行为主要来自于美国、俄罗斯、加拿大、法国和荷兰等国家，成都市、德阳市和绵阳市是境外恶意网络行为重点攻击的区域。

## **1.网络安全威胁情况**

2021年7月，平台监测发现我省重点工业企业安全威胁133,196起，涉及企业210家。其中高危安全威胁97,688起，占威胁总量的73.34%，安全威胁数量环比上个月增加103.33%；本月受到高危安全威胁的工业企业共计163家，环比减少23.83%。4-6月安全威胁事件数量呈下降趋势，其中木马后门和Web攻击下降幅度最大，7月份安全事件有所增加。今年2-7月安全威胁数量如图3.1所示。

**图3.1 2-7月工业互联网安全威胁数量态势图**

本月平台监测到针对四川省恶意网络攻击行为101,187起，威胁类型主要包括木马后门、Web攻击、非法外联、挖矿事件和异常流量，其中木马后门攻击次数达63,129次，占比62.39%。7月份安全威胁类型分布情况如图3.2所示。

**图3.2 安全威胁类型分布图**

从安全威胁类型角度进行分析，与上月相比，各类威胁事件均有所增加；其中木马后门和非法外联增加幅度最大，达到186.90%和284.43%。7月份安全威胁类型top5及环比变化情况如图3.3所示。

**图3.3 6-7月安全威胁类型top5及环比变化情况**

## **2.工业设备安全漏洞情况**

截至2021年7月31日，平台监测我省工业企业安全漏洞189,734个，其中高危漏洞34,811个，占总设备漏洞的18.35%。归属于成都市的企业涉及漏洞较多，占全省工业设备新增漏洞数量的74.49%。工业互联网设备应用程序漏洞类型数量排名如表1所示。

表1 漏洞类型编号排名（top10）

|  |  |  |  |
| --- | --- | --- | --- |
| 漏洞编号 | 数量 | 漏洞类型 | 漏洞等级 |
| CNVD-2016-00961 | 29112 | 拒绝服务 | 中危 |
| CNVD-2016-00982 | 29112 | 拒绝服务 | 中危 |
| CNVD-2016-00962 | 29112 | 拒绝服务 | 中危 |
| CNVD-2018-06530 | 14220 | 未授权的信息泄露 | 中危 |
| CNVD-2018-05440 | 5394 | 管理员访问权限获取 | 高危 |
| CNVD-2016-01325 | 1495 | 未授权的信息泄露 | 中危 |
| CNVD-2016-00276 | 1415 | 拒绝服务 | 中危 |
| CNVD-2016-00274 | 1414 | 未授权的信息泄露 | 中危 |
| CNVD-2016-01769 | 1414 | 管理员访问权限获取 | 高危 |
| CNVD-2016-00392 | 1414 | 拒绝服务 | 中危 |

监测到的设备漏洞类型中，排名前三的是拒绝服务、未授权的信息泄露、管理员访问权限获取。主要漏洞类型分布如图3.4所示：

**图3.4 应用程序漏洞类型分布图**

## **3.行业安全态势分析**

2021年7月我省各行业受攻击次数有所增加，主要集中在橡胶和塑料制品业、汽车制造业和房地产业。汽车制造业和非金属矿物制品业增长幅度最大。7月我省重点行业受攻击次数环比变化情况如图3.5所示。

**图3.5 重点行业受攻击次数环比变化情况**

## **4.地域安全态势分析**

2021年7月，通过对我省被攻击地市进行监测分析，成都市受攻击的次数相对较多，达到77,275次，占全省被攻击次数的76.37%。各地市受网络攻击次数排名情况如图3.6所示。

**图3.6 网络攻击数量地市排名**

7月份，全省被攻击主机356个，主要集中在成都、德阳、绵阳，占全省被攻击主机的95.51%。泸州、南充和攀枝花本月被攻击主机较上月有所减少。重点地市受攻击主机数量环比变化情况如图3.7所示。

**图3.7 地域受攻击主机数量变化情况**

## **重要网络安全威胁预警**

## **1.**国家网信办关于下架“滴滴企业版”等25款App的通报

2021年7月9日，据中国网信网消息，根据举报，经检测核实，“滴滴企业版”等25款App存在严重违法违规收集使用个人信息问题。国家互联网信息办公室依据《中华人民共和国网络安全法》相关规定，通知应用商店下架上述25款App，要求相关运营者严格按照法律要求，参照国家有关标准，认真整改存在的问题，切实保障广大用户个人信息安全。各网站、平台不得为“滴滴出行”和“滴滴企业版”等上述25款已在应用商店下架的App提供访问和下载服务。

## **2.中央网信办、国家发展改革委、工业和信息化部印发《关于加快推进互联网协议第六版（IPv6）规模部署和应用工作的通知》**

2021年7月23日，据中国网信网消息，近日，中央网信办、国家发展改革委、工业和信息化部印发《关于加快推进互联网协议第六版（IPv6）规模部署和应用工作的通知》（以下简称《通知》）。《通知》落实《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》有关要求，明确了“十四五”时期深入推进IPv6规模部署和应用的主要目标、重点任务和时间表，是各地区、各部门推进IPv6部署应用工作的指导性文件。《通知》指出，互联网协议第六版（IPv6是互联网升级演进的必然趋势、网络技术创新的重要方向、网络强国建设的基础支撑。“十四五”时期是加快数字化发展、建设网络强国和数字中国的重要战略机遇期，我国IPv6发展处于攻坚克难、跨越拐点的关键阶段，要立足新发展阶段，贯彻新发展理念，构建新发展格局，落实高质量发展要求，坚定不移推进IPv6规模部署和应用。

## **3.工信部通报145款侵害用户权益行为APP**

2021年7月19日，据工业和信息化部网站消息，依据《网络安全法》《电信条例》《电信和互联网用户个人信息保护规定》等法律法规，按照《关于开展纵深推进APP侵害用户权益专项整治行动的通知》（工信部信管函〔2020〕164号）工作部署，工业和信息化部近期组织第三方检测机构针对用户反映问题较多的医疗健康、电子商务、实用工具等类型手机应用软件进行了专项检查，已通知相关企业进行了整改。截至目前，尚有71款APP未完成整改。各通信管理局按工信部APP整治行动部署，积极开展手机应用软件监督检查，辽宁省、浙江省、广东省、四川省、宁夏回族自治区通信管理局检查发现仍有74款APP未完成整改。上述145款APP应在7月26日前完成整改落实工作，逾期不整改的，工信部将依法依规组织开展相关处置工作。

## **4.工信部关于下架侵害用户权益APP名单的通报**

2021年7月12日，据工信部网站消息，工信部公开通报第5批（总第14批）APP，经第三方检测机构核查复检，截至目前尚有18款APP未按照工信部要求完成整改。上海、安徽、广东、四川省（市）通信管理局检查发现共有30款APP仍未完成整改依据《网络安全法》《电信和互联网用户个人信息保护规定》《移动智能终端应用软件预置和分发管理暂行规定》等法律和规范性文件要求，工信部组织对上述48款APP进行下架。相关应用商店应在本通报发布后，立即组织对名单中应用软件进行下架处理。

## **5.工信部、国家网信办、公安部联合印发《网络产品安全漏洞管理规定》**

2021年7月13日，据中国网信网消息，工信部、国家网信办和公安部联合发布《网络产品安全漏洞管理规定》。该规定自2021年9月1日起施行。中华人民共和国境内的网络产品（含硬件、软件）提供者和网络运营者，以及从事网络产品安全漏洞发现、收集、发布等活动的组织或者个人，均应遵守本规定。此外规定细化了相关政府职能部门分工：国家互联网信息办公室负责统筹协调网络产品安全漏洞管理工作。工业和信息化部负责网络产品安全漏洞综合管理，承担电信和互联网行业网络产品安全漏洞监督管理。公安部负责网络产品安全漏洞监督管理，依法打击利用网络产品安全漏洞实施的违法犯罪活动。有关主管部门加强跨部门协同配合，实现网络产品安全漏洞信息实时共享，对重大网络产品安全漏洞风险开展联合评估和处置。

## **6.工信部大力推进APP开屏弹窗信息骚扰用户问题整治**

2021年7月8日，据工信部网站消息，工业和信息化部近期对用户反映强烈投诉较多的“弹窗信息标识近于无形、关闭按钮小如蝼蚁、页面伪装瞒天过海、诱导点击暗度陈仓”等违规行为进行了集中整治，督促企业重视用户诉求，解决好在开屏信息页面中存在利用文字、图片、视频等方式欺骗误导用户跳转等问题。截至目前，百度、阿里、腾讯、字节跳动、新浪微博、爱奇艺等68家7头部互联网企业已按要求完成整改。2021年第二季度，开屏弹窗信息用户投诉举报数量环比下降50%，误导用户点击跳转第三方页面问题同比下降80%。