**四川省公共互联网网络安全态势分析通报（2021年9月）**

**四川省通信管理局**

**2021年10月**

**目 录**

[一、本月公共互联网基本情况分析 2](#_Toc86217441)

[1.省内互联网用户访问流量情况 2](#_Toc86217442)

[2.省内互联网用户访问协议情况 3](#_Toc86217443)

[3.省内互联网用户访问域名分布情况 4](#_Toc86217444)

[二、本月公共互联网网络安全态势 4](#_Toc86217445)

[1.木马、僵尸网络 4](#_Toc86217446)

[2.网页篡改 6](#_Toc86217447)

[3.网页后门 7](#_Toc86217448)

[三、本月工业互联网网络安全态势 8](#_Toc86217449)

[1.网络安全威胁情况 9](#_Toc86217450)

[2.工业设备安全漏洞情况 10](#_Toc86217451)

[3.行业安全态势分析 12](#_Toc86217452)

[4.地域安全态势分析 12](#_Toc86217453)

[四、重要网络安全威胁预警 14](#_Toc86217454)

[1.中共中央办公厅 国务院办公厅印发《关于加强网络文明建设的意见》 14](#_Toc86217455)

[2.工业和信息化部关于加强车联网网络安全和数据安全工作的通知 14](#_Toc86217456)

[3.工信部通报334款侵害用户权益APP 15](#_Toc86217457)

## **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9月四川省内流量总体正常，日均流量为27.62Tbps,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17.38Tbps。



来源：SCCERT

 **图1.1 2021年9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9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9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HTTP、HTTPS。

**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9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，通过分析发现，省内公众上网类型主要为短视频、云服务、生活服务类，通过域名访问数量也可发现，在国内主流互联网公司中，字节跳动、腾讯、百度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**

## **二、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，但网络安全事件数量整体有所上升。

## **1.木马、僵尸网络**

四川省本月有299,615个IP地址对应的主机被木马或僵尸程序控制，环比上升75.2%。2020年9月-2021年9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，本月较上月大幅上升。

**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4,501个IP地址存在木马或僵尸程序控制服务器，环比上升5.8%。2020年9月-2021年9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，整体呈下降趋势。

**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168,953台主机感染僵尸木马，较上月大幅上升。

**图2.3四川省内各市州主机感染僵尸木马主机数量分布**

## **2.网页篡改**

本月，主机位于四川地区的被篡改网站数量为283个，环比下降17.25%。2020年9月-2021年9月，四川省内被篡改网站数量月度分布如图2.4所示，连续四个月小幅下降。

**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224个，较上月继续小幅下降。

**图2.5四川省内各市州网页篡改被网站数量分布**

## **3.网页后门**

主机位于四川省的被植入后门180个，环比上升52.54%。2020年9月-2021年9月，四川省内被植入后门网站月度分布情况如图2.6所示，下半年开始逐步上升。

**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120个。

**图2.7四川省被植入后门的网站主机数量月度分布图**

## **三、本月工业互联网网络安全态势**

截至 2021年9月30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 11,415家、工业设备 17.96 万台、工业 APP 18,760 款。累计共发现66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9月我省总体安全威胁数量较上月大幅增加，其中木马后门威胁事件达388,334次，占总体威胁数量的71.32%；攻击类型主要包括木马后门、挖矿事件、Web攻击等；从被攻击的行业来看，攻击事件主要分布在计算机、通信和其他电子设备制造业业、非金属矿物制品业和汽车制造业等；从被攻击的地域来看，被攻击的地市主要包括成都市、绵阳市和德阳市，威胁事件数量占据全省总数的99.82%；从境外攻击视角来看，境外恶意网络攻击行为主要来自于德国、新加坡、美国、俄罗斯和英国等国家，成都市、绵阳市和德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9月，平台监测发现我省重点工业企业安全威胁544,472起，涉及企业460家。其中高危安全威胁488,949起，占威胁总量的89.80%，安全威胁数量环比上个月增加149.70%；本月受到高危安全威胁的工业企业共计385家，环比增加71.86%。6-9月安全威胁事件数量呈大幅上升趋势，其中木马后门和挖矿事件增加幅度最大。今年4-9月安全威胁数量如图3.1所示。

**图3.1 4-9月工业互联网安全威胁数量态势图**

2021年9月平台监测到针对四川省恶意网络攻击行为544,472起，威胁类型主要包括木马后门、挖矿事件、Web攻击、勒索病毒和漏洞利用，其中木马后门攻击次数达388,334次，占比71.32%。9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；其中挖矿事件和勒索病毒增加幅度最大，达到716.75%和423.35%。9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 8-9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9月30日，平台监测我省工业企业安全漏洞189,842个，其中高危漏洞34,913个，占总设备漏洞的18.39%。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74.47%。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-2016-00982 | 29115 | 拒绝服务 | 中危 |
| CNVD-2016-00961 | 29112 | 拒绝服务 | 中危 |
| CNVD-2016-00962 | 29109 | 拒绝服务 | 中危 |
| CNVD-2018-06530 | 14221 | 未授权的信息泄露 | 中危 |
| CNVD-2018-05440 | 5393 | 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-2016-00274 | 1416 | 拒绝服务 | 中危 |
| CNVD-2016-00276 | 1415 | 未授权的信息泄露 | 中危 |
| CNVD-2016-00392 | 1414 | 拒绝服务 | 中危 |
| CNVD-2016-01769 | 1414 | 管理员访问权限获取 | 高危 |

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9月我省各行业受攻击次数有所增加，主要集中在计算机和电子制造业、汽车制造业和房地产业。计算机和电子制造业、房地产业增长幅度最大。9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9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237,020次，占全省被攻击次数的43.53%。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**

9月份，全省被攻击主机682个，主要集中在成都、德阳、宜宾和绵阳，占全省被攻击主机的97.95%。本月宜宾受到攻击的主机数为54个，排全省第三。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.** 中共中央办公厅 国务院办公厅印发《关于加强网络文明建设的意见》

2021年9月14日，中共中央办公厅、国务院办公厅印发了《关于加强网络文明建设的意见》（以下简称《意见》）。《意见》指出，要强化网络平台责任，加强网站平台社区规则、用户协议建设，引导网络平台增强国家安全意识。深入推进“清朗”、“净网”系列专项行动，深化打击网络违法犯罪，深化公众账号、直播带货、知识问答等领域不文明问题治理，开展互联网领域虚假信息治理。坚持依法治理网络空间，把弘扬社会主义核心价值观贯穿网络立法执法司法普法各环节，发挥法律法规对维护良好网络秩序、树立文明网络风尚的保障作用。加强个人信息保护法、 数据安全法贯彻实施，加快制定修订并实施文化产业促进法、广播电视法、网络犯罪防治法、未成年人网络保护条例、互联网信息服务管理办法等法律法规。

## **2. 工业和信息化部关于加强车联网网络安全和数据安全工作的通知**

2021年9月16日，工业和信息化部发布关于加强车联网网络安全和数据安全工作的通知。通知要求为各相关企业要建立网络安全和数据安全管理制度，明确负责人和管理机构，落实网络安全和数据安全保护责任。强化企业内部监督管理，加大资源保障力度，及时发现并解决安全隐患。加强网络安全和数据安全宣传、教育和培训。全面加强安全保护。各相关企业要采取管理和技术措施，按照车联网网络安全和数据安全相关标准要求，加强汽车、网络、平台、数据等安全保护，监测、防范、及时处置网络安全风险和威胁，确保数据处于有效保护和合法利用状态，保障车联网安全稳定运行。

## **3.** **工信部通报334款侵害用户权益APP**

2021年9月23日，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，工业和信息化部组织第三方检测机构对手机应用软件进行检查，重点对假日出行、民生服务类APP进行抽测，尚有52款APP未完成整改。各通信管理局按照工业和信息化部统筹部署，积极开展APP技术检测，尚有282款APP未按时限要求完成整改。上述334款APP应在2021年9月29日前完成整改落实工作。逾期不整改的，工业和信息化部将依法依规组织开展相关处置工作。