**四川省公共互联网网络安全态势分析通报（2021年8月）**

**四川省通信管理局**

**2021年9月**

**目 录**

[一、本月公共互联网基本情况分析 2](#_Toc83287209)

[1.省内互联网用户访问流量情况 2](#_Toc83287210)

[2.省内互联网用户访问协议情况 3](#_Toc83287211)

[3.省内互联网用户访问域名分布情况 4](#_Toc83287212)

[二、本月公共互联网网络安全态势 4](#_Toc83287213)

[1.木马、僵尸网络 4](#_Toc83287214)

[2.网页篡改 6](#_Toc83287215)

[3.网页后门 7](#_Toc83287216)

[三、本月工业互联网网络安全态势 8](#_Toc83287217)

[1.网络安全威胁情况 9](#_Toc83287218)

[2.工业设备安全漏洞情况 10](#_Toc83287219)

[3.行业安全态势分析 12](#_Toc83287220)

[4.地域安全态势分析 12](#_Toc83287221)

[四、重要网络安全威胁预警 13](#_Toc83287222)

[1.国家网信办会同有关部门深入推进摄像头偷窥等黑产集中治理工作 13](#_Toc83287223)

[2.全国人大法工委：个人信息保护法草案（三次审议稿）拟作六方面修改 14](#_Toc83287224)

[3.《中华人民共和国个人信息保护法》发布 15](#_Toc83287225)

[4.五部委联合发布《汽车数据安全管理若干规定（试行）》 16](#_Toc83287226)

[5.《关键信息基础设施安全保护条例》发布 16](#_Toc83287227)

[6.国家网信办就《互联网信息服务算法推荐管理规定（征求意见稿）》公开征求意见 17](#_Toc83287228)

## **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8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13.94Tbps。



来源：SCCERT

 **图1.1 2021年8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，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8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8月四川省内互联网用户访问网络的协议占比情况如图1.3所示，占比前两位的分别为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8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，通过域名访问数量分析，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**

## **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。

## **1.木马、僵尸网络**

四川省本月有74,317个IP地址对应的主机被木马或僵尸程序控制，环比上升31.33%。2020年8月-2021年8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，本月较上月较大幅度上升。

**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4,240个IP地址存在木马或僵尸程序控制服务器，环比下降34.33%。2020年8月-2021年8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，连续三月呈下降趋势。

**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、南充，其中成都数量最多，有43,719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**

## **2.网页篡改**

本月，主机位于四川地区的被篡改网站数量为342个，环比下降10.47%。2020年8月-2021年8月，四川省内被篡改网站数量月度分布如图2.4所示，本月继续小幅下降。

**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分布如图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252个，较上月小幅下降。

**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118个，环比上升35.63%。2020年8月-2021年8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分布如图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79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8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 11,376家、工业设备 17.94 万台、工业 APP 18,510 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8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145,958次，占总体威胁数量的66.94%；攻击类型主要包括木马后门、Web攻击、挖矿事件等；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、房地产业和汽车制造业等；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99.91%；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、加拿大、法国、荷兰和俄罗斯等国家，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8月，平台监测发现我省重点工业企业安全威胁218,048起，涉及企业312家。其中高危安全威胁158,946起，占威胁总量的72.89%，安全威胁数量环比上个月增加63.71%；本月受到高危安全威胁的工业企业共计224家，环比增加37.42%。6-8月安全威胁事件数量呈上升趋势，其中木马后门和挖矿事件增加幅度最大。今年3-8月安全威胁数量如图1所示。

**图3.1 3-8月工业互联网安全威胁数量态势图**

2021年8月平台监测到针对四川省恶意网络攻击行为218,048起，威胁类型主要包括木马后门、Web攻击、挖矿事件、非法外联和异常流量，其中木马后门攻击次数达145,958次，占比66.94%。8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；其中木马后门和挖矿事件加幅度最大，达到131.21%和310.55%。8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 7-8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8月31日，平台监测我省工业企业安全漏洞189,827个，其中高危漏洞34,903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8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。其中计算机和电子制造业、房地产业增长幅度最大。8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8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155,653次，占全省被攻击次数的71.38%。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**

8月份，全省被攻击主机537个，主要集中在成都、德阳、绵阳，占全省被攻击主机的97.21%。泸州和眉山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.**国家网信办会同有关部门深入推进摄像头偷窥等黑产集中治理工作

2021年8月9日，据中国网信网消息，今年5月以来，国家网信办会同工业和信息化部等相关政府部门深入推进摄像头偷窥等黑产集中治理工作，对人民群众反应强烈的非法利用摄像头偷窥个人隐私画面、交易隐私视频、传授偷窥偷拍技术等侵害公民个人隐私行为进行集中治理。国家网信办指导各地网信办督促各类平台清理相关违规有害信息2.2万余条，处置平台账号4000余个、群组132个，下架违规产品1600余件。其中，百度、腾讯、UC等重点网站平台，清理有害信息8000余条、处置违规账号134个；京东、淘宝、闲鱼等电商平台，下架违规宣传或违规售卖摄像设备1600余件、处置违规账号3700余个、清理违规信息1.2万余条。对存在隐私视频信息泄露隐患的14家视频监控APP厂商进行了约谈，并督促其完成整改。工业和信息化部组织各省、自治区、直辖市通信管理局、专业机构、基础电信企业，以及18个重点视频监控云平台、摄像头生产企业代表，召开全国电视电话会议，部署摄像头网络安全集中整治工作；组织开展智能音视频采集设备应用安全、网络安全、数据安全等有关标准宣传普及，督促摄像头生产企业对照安全标准开展自查自纠，组织检测机构进入5家摄像头生产企业开展现场巡查和产品抽检；组织对18家具有行业代表性的视频监控云平台开展检查，发现处置SQL注入、越权操作等一批高危漏洞；全面排查联网摄像头存在的安全隐患，发现4万多个弱口令、未授权访问、远程命令执行等摄像头漏洞，取证并处置500余个。

## **2.全国人大法工委：个人信息保护法草案（三次审议稿）拟作六方面修改**

2021年8月13日，据中国人大网消息，13日上午，全国人大常委会法制工作委员会举行记者会，发言人臧铁伟介绍立法工作有关情况并回答记者提问。据介绍，十三届全国人大常委会第三十次会议将于8月17日至20日在北京举行。根据各方面意见，提请本次常委会会议审议的个人信息保护法草案（三次审议稿）拟作如下主要修改：一是，我国宪法规定，国家尊重和保障人权，公民的人格尊严不受侵犯，公民的通信自由和通信秘密受法律保护。制定实施本法对于保障公民的人格尊严和其他权益具有重要意义。据此，拟在草案第一条中增加规定根据宪法制定本法。二是，进一步完善个人信息处理规则，特别是对应用程序（APP）过度收集个人信息、大数据杀熟等作出有针对性规范。三是，将不满十四周岁未成年人的个人信息作为敏感个人信息，并要求个人信息处理者对此制定专门的个人信息处理规则。四是，完善个人信息跨境提供的规则，对按照我国缔结或者参加的国际条约、协定向境外提供个人信息、对转移到境外的个人信息的保护不应低于我国的保护标准等作出规定。五是，增加个人信息可携带权的规定，完善死者个人信息保护的规定。六是，对完善个人信息保护投诉、举报工作机制及违法处理个人信息涉嫌犯罪案件的移送提出明确要求。

## **3.《中华人民共和国个人信息保护法》发布**

2021年8月20日，据中国人大网消息，《中华人民共和国个人信息保护法》已由中华人民共和国第十三届全国人民代表大会常务委员会第三十次会议于2021年8月20日通过，现予公布，自2021年11月1日起施行。本法规定任何组织、个人不得侵害自然人的个人信息权益。在中华人民共和国境内处理自然人个人信息的活动，适用本法。在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动，有下列情形之一的，也适用本法：（一）以向境内自然人提供产品或者服务为目的；（二）分析、评估境内自然人的行为；（三）法律、行政法规规定的其他情形。

## **4.五部委联合发布《汽车数据安全管理若干规定（试行）》**

2021年8月20日，据中国网信网消息，国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、交通运输部联合发布《汽车数据安全管理若干规定（试行）》（以下简称《规定》），自2021年10月1日起施行。国家互联网信息办公室有关负责人表示，出台《规定》旨在规范汽车数据处理活动，保护个人、组织的合法权益，维护国家安全和社会公共利益，促进汽车数据合理开发利用。《规定》明确，汽车数据处理者应当履行个人信息保护责任，充分保护个人信息安全和合法权益。开展个人信息处理活动，汽车数据处理者应当通过显著方式告知个人相关信息，取得个人同意或者符合法律、行政法规规定的其他情形。处理敏感个人信息，汽车数据处理者还应当取得个人单独同意，满足限定处理目的、提示收集状态、终止收集等具体要求或者符合法律、行政法规和强制性国家标准等其他要求。汽车数据处理者具有增强行车安全的目的和充分的必要性，方可收集指纹、声纹、人脸、心律等生物识别特征信息。

## **5.《关键信息基础设施安全保护条例》发布**

2021年8月18日，据中国政府网消息，《关键信息基础设施安全保护条例》已经2021年4月27日国务院第133次常务会议通过，现予公布，自2021年9月1日起施行。本条例所称关键信息基础设施，是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。在国家网信部门统筹协调下，国务院公安部门负责指导监督关键信息基础设施安全保护工作。国务院电信主管部门和其他有关部门依照本条例和有关法律、行政法规的规定，在各自职责范围内负责关键信息基础设施安全保护和监督管理工作。省级人民政府有关部门依据各自职责对关键信息基础设施实施安全保护和监督管理。

## **6.国家网信办就《互联网信息服务算法推荐管理规定（征求意见稿）》公开征求意见**

2021年8月27日，据中国网信网消息，为了规范互联网信息服务算法推荐活动，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益，促进互联网信息服务健康发展，国家互联网信息办公室起草了《互联网信息服务算法推荐管理规定（征求意见稿）》（内容详见中国网信网）），向社会公开征求意见。