四川省公共互联网网络安全态势分析通报

（2021 年 11 月）

四川省通信管理局

2021 年 12 月

目 录

一、 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 11 月四川省内流量总体正常，日均流量为 25.70Tbps,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 16.32Tbps。

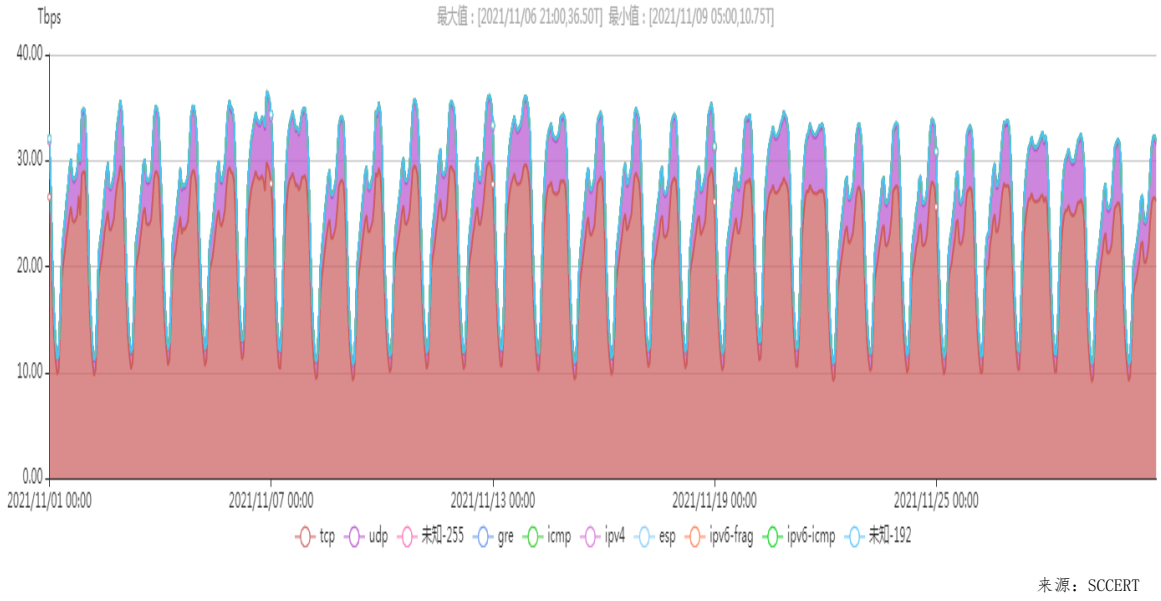

图 1.1 2021 年 11 月四川省内流量监测情况

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。

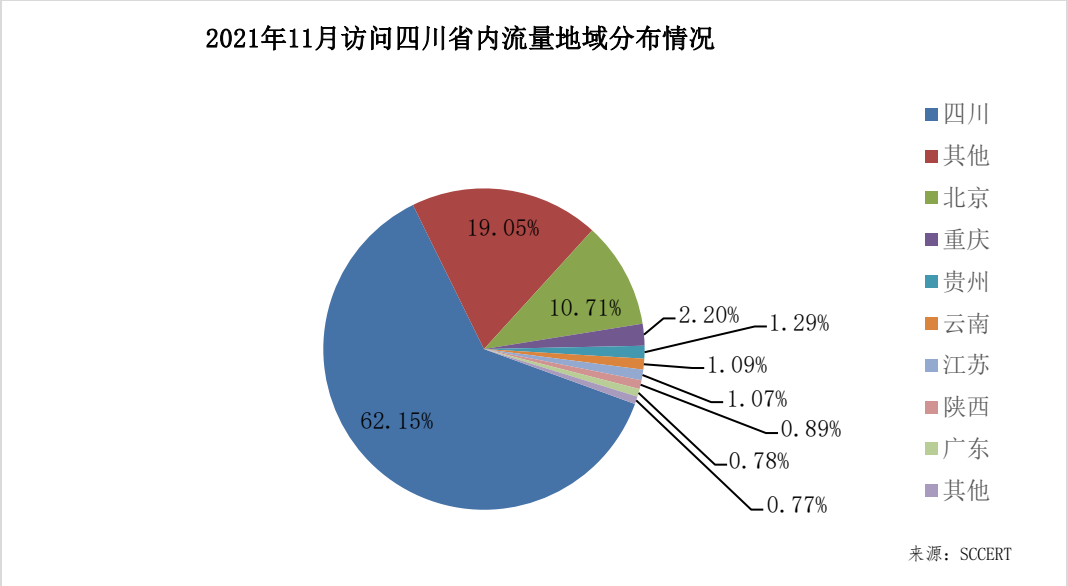

图 1.2 2021 年 11 月访问四川省内流量地域分布情况

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 11 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。

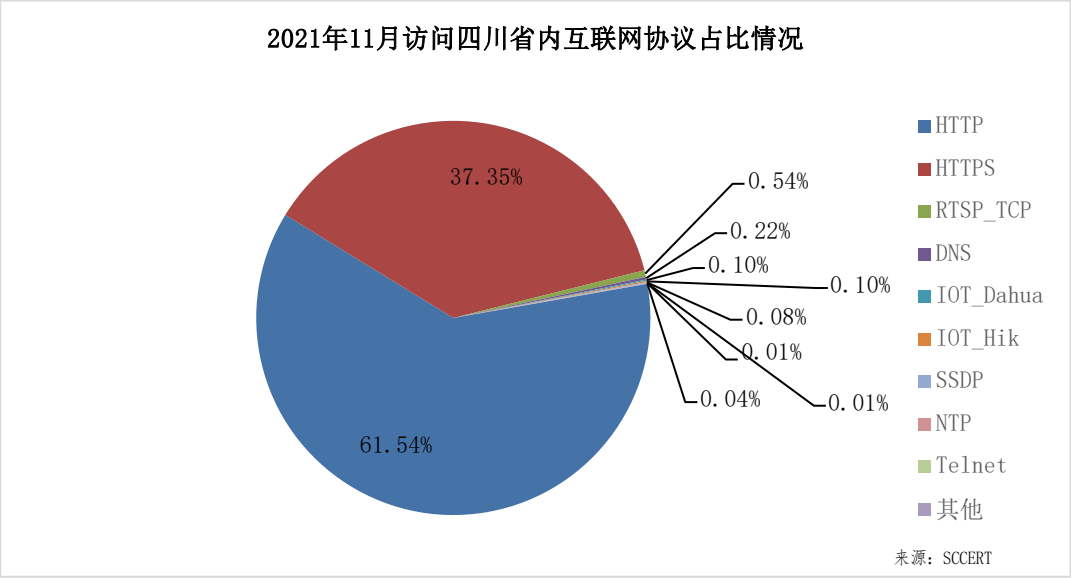

图 1.3 四川省内路由器协议占比情况

3.省内互联网用户访问域名分布情况

2021年11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、基础应用、搜索引擎类，通过域名访问数量也可以发现，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。省内ipv6普及率显著提升。

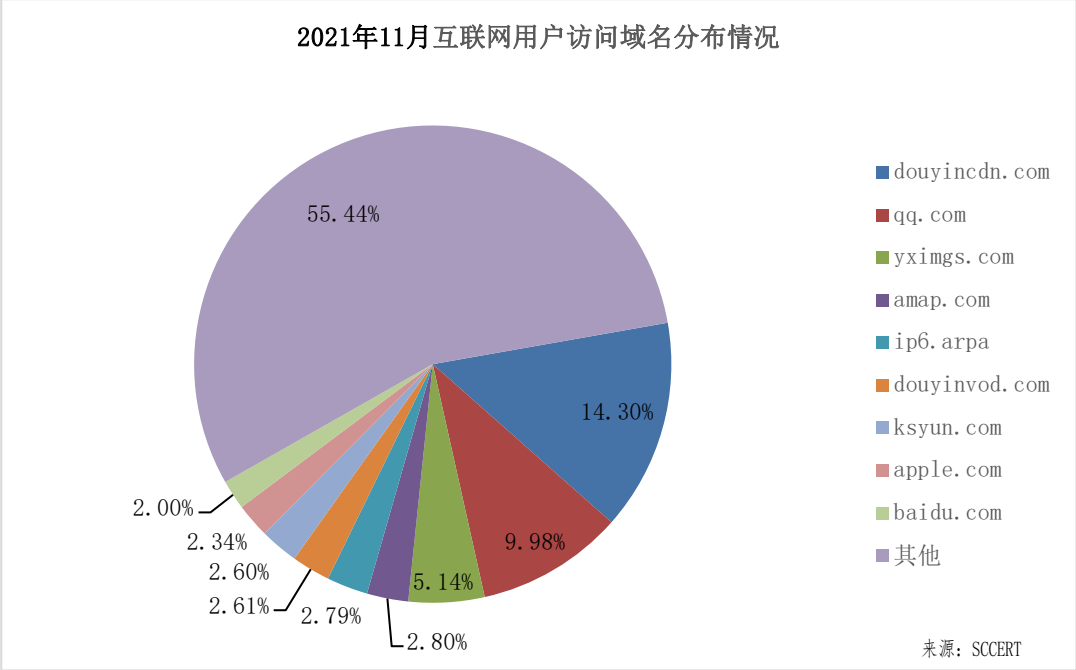

图1.4 四川省内域名访问情况

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，网络安全事件数量整体有所下降。

1. 木马、僵尸网络

四川省本月有 273,547 个 IP 地址对应的主机被木马或僵尸程序控制，环比下降 19.99%。2020 年 11 月-2021 年 11 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，本月较上月小幅下降。

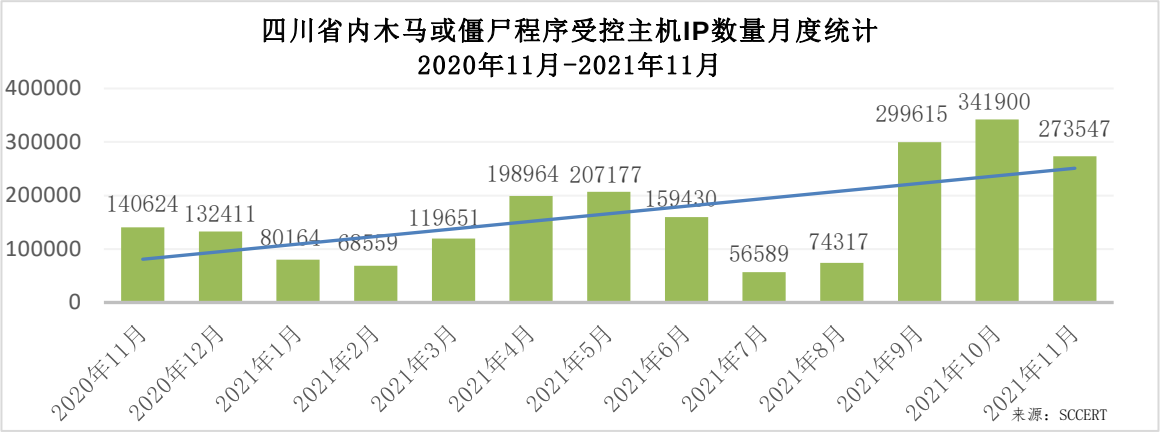

图 2.1 四川省木马或僵尸程序受控主机 IP 数量月度分布图

四川省本月有 5,100 个 IP 地址存在木马或僵尸程序控制服务器，环比上升 5.61%。2020 年 11 月-2021 年 11 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，近三个月小幅上升。

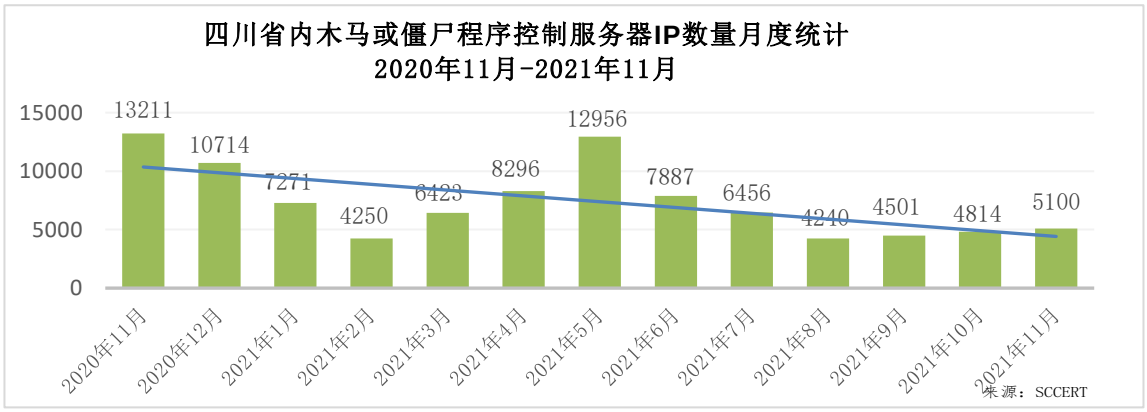

图 2.2 四川省木马或僵尸程序控制服务器 IP 数量月度分布图

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 149,750 台主机感染僵尸木马，较上月降低 21.46%。

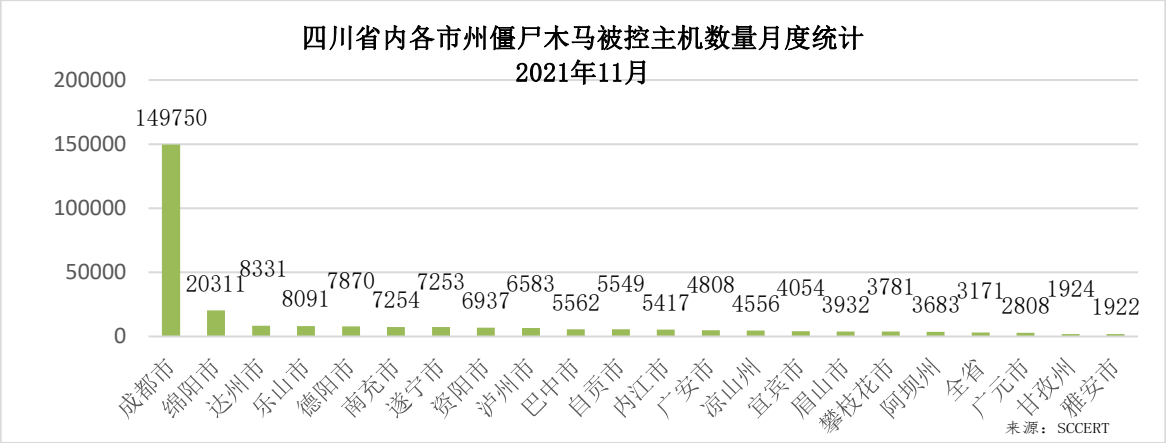

图 2.3 四川省内各市州主机感染僵尸木马主机数量分布

2. 网页篡改

本月，主机位于四川地区的被篡改网站数量为 205 个，环比下降 57.2%。2020 年 11 月-2021 年 11 月，四川省内被篡改网站数量月度分布如图 2.4 所示，较上月大幅下降，降幅超过上月总数一半以上。

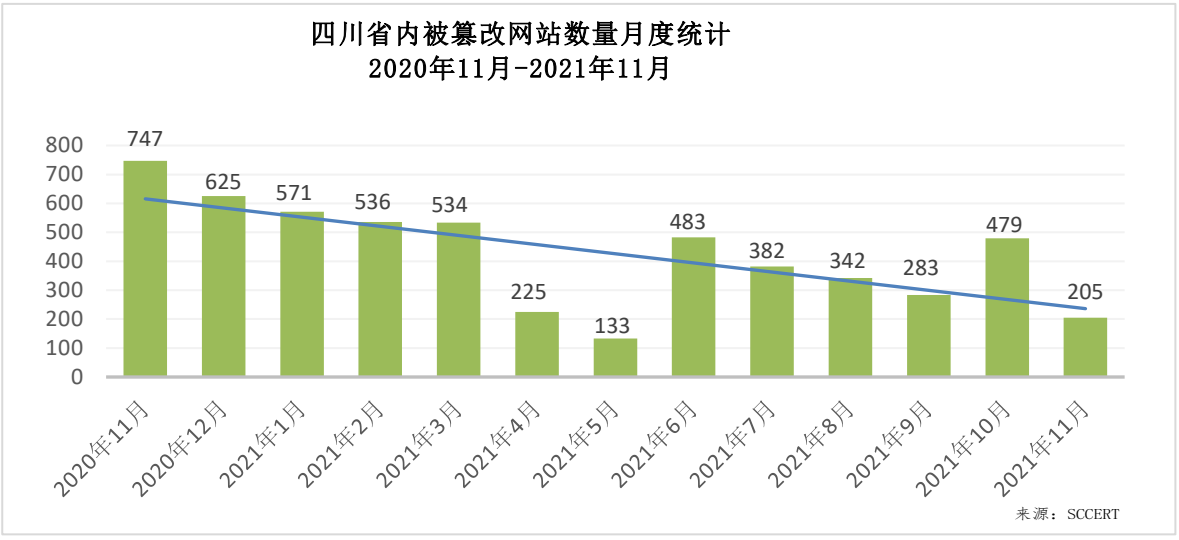

图 2.4 四川省被篡改网站数量月度分布图

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 154 个，较上月继续下降 31.25%。

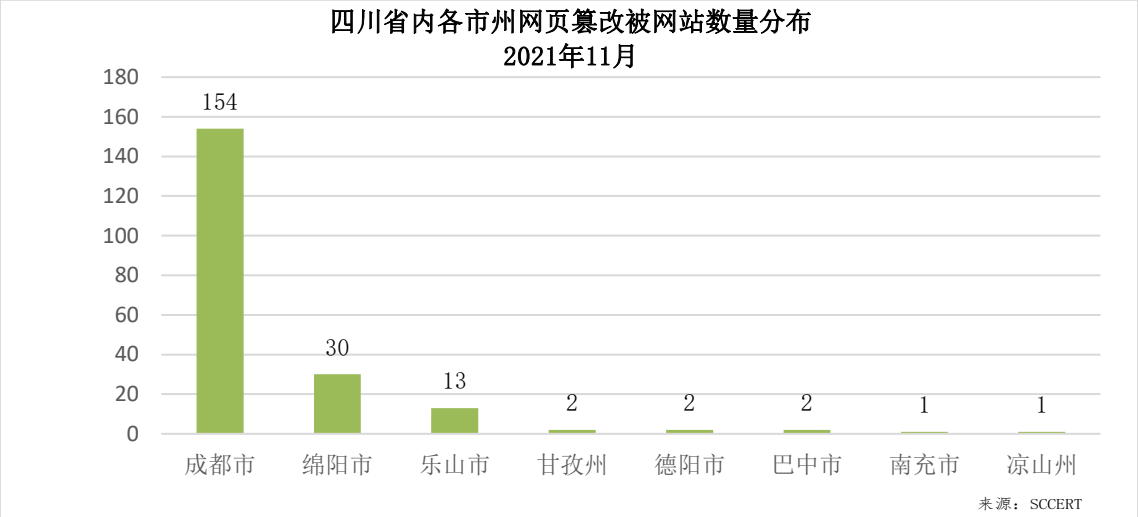

图 2.5 四川省内各市州网页篡改被网站数量分布

3. 网页后门

主机位于四川省的被植入后门 137 个，环比下降 5.52%。2020 年 11 月-2021 年 11 月，四川省内被植入后门网站月度分布情况如图 2.6 所示，连续三个月下降。

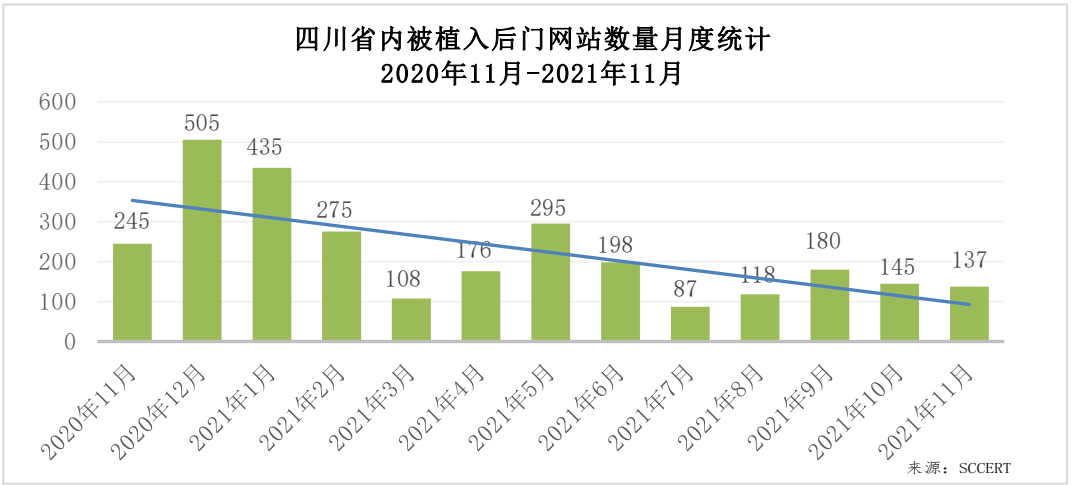

图 2.6 四川省被植入后门的网站主机数量月度分布图

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 95 个。

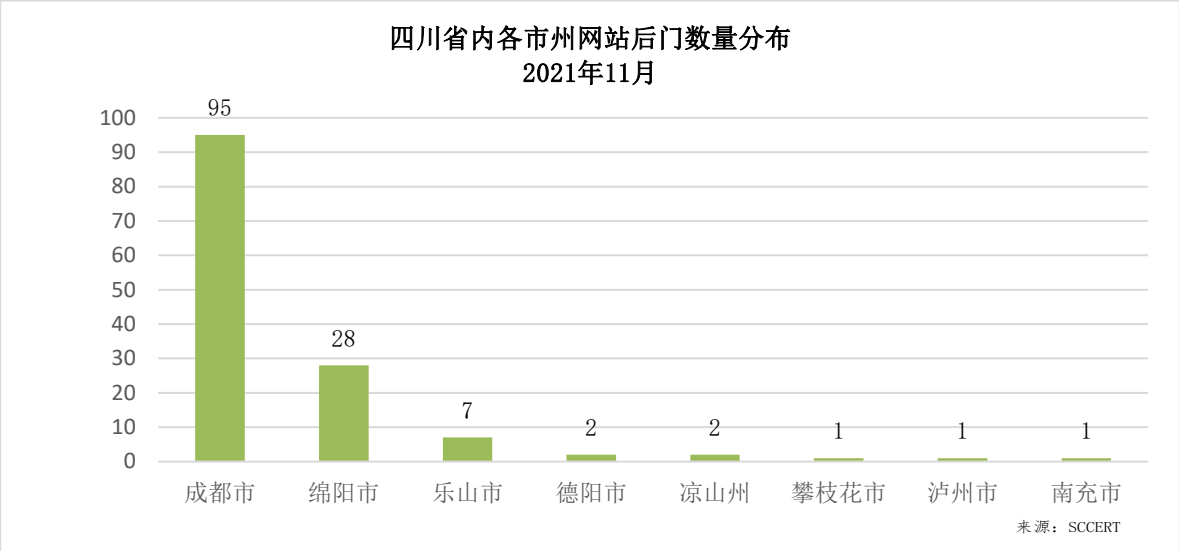

图 2.7 四川省被植入后门的网站主机数量月度分布图

三、本月工业互联网网络安全态势

截至 2021 年 11 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 11,794 家、工业设备 18.01 万台、工业 APP 19,509 款。累计共发现 67 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 11 月我省总体安全威胁数量较上月大幅上升，其中木马后门威胁事件 101,640 次，占总体威胁数量的 48.14%；攻击类型主要包括木马后门、挖矿事件、漏洞利用等；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、汽车制造业和电气机械和器材制造业等；从被攻击的地域来看，被攻击的地市主要包括绵阳市、成都市和德阳市，威胁

事件数量占据全省总数的 96.15%；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、德国、新加坡、荷兰和俄罗斯等国家，绵阳市、成都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 11 月，平台监测发现我省重点工业企业安全威胁 211,119 起，涉及企业 604 家。其中高危安全威胁 149,699 起，占威胁总量的 70.91%，安全威胁数量环比上月上升 57.42%；本月受到高危安全威胁的工业企业共计 478 家，比上月增加 91 家。11 月安全威胁事件数量大幅上升，与 8 月安全威胁事件数量基本相当，其中挖矿事件和 web 攻击上升幅度最大。今年 6-11 月安全威胁数量如图 3.1 所示。

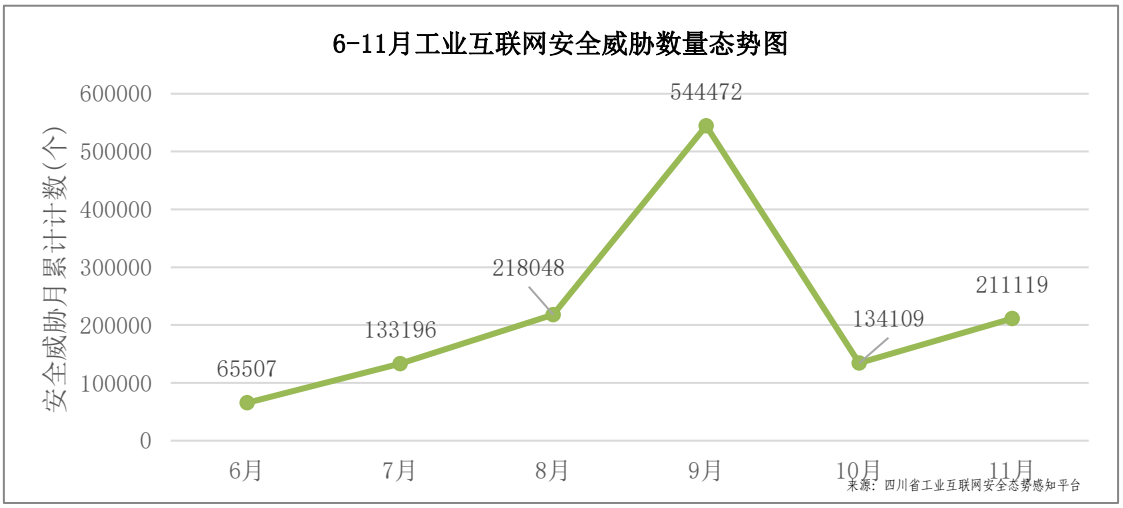

图 3.1 6-11 月工业互联网安全威胁数量态势图

2021 年 11 月平台监测到针对四川省恶意网络攻击行为 211,119 起，威胁类型主要包括木马后门、挖矿事件、漏洞利用、命令执行和 Web 攻击，其中木马后门攻击次数达 101,640 次，占

比 48.14%。11 月份安全威胁类型分布情况如图 3.2 所示。

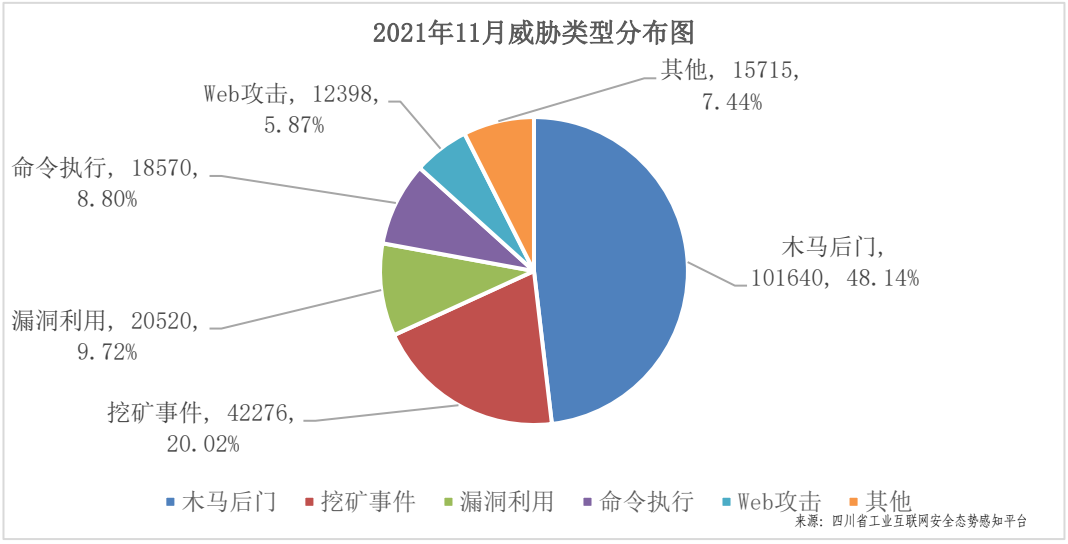

图 3.2　安全威胁类型分布图

从安全威胁类型角度进行分析，与上月相比，大部分威胁事件大幅上升；其中挖矿事件和 Web 攻击上升幅度最大，达到 407.03%和 179.93%。11 月份安全威胁类型 top5 及环比变化情况如图如图 3.3 所示。

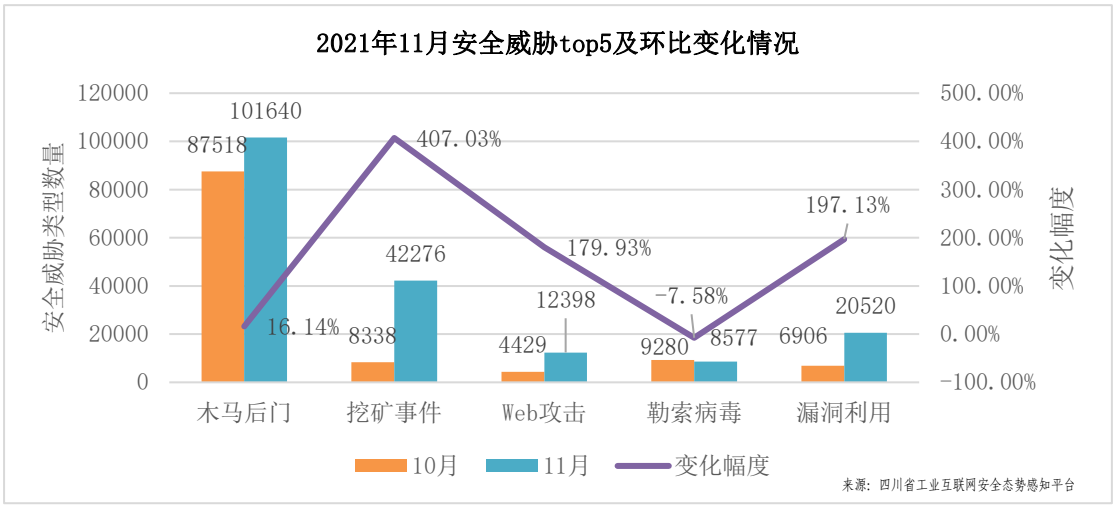

图 3.3　10-11 月安全威胁类型 top5 及环比变化情况

2. 工业设备安全漏洞情况

截至 2021 年 11 月 30 日，平台监测我省工业企业安全漏洞

190,069 个，其中高危漏洞 35,130 个，占总设备漏洞的 18.48%。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：

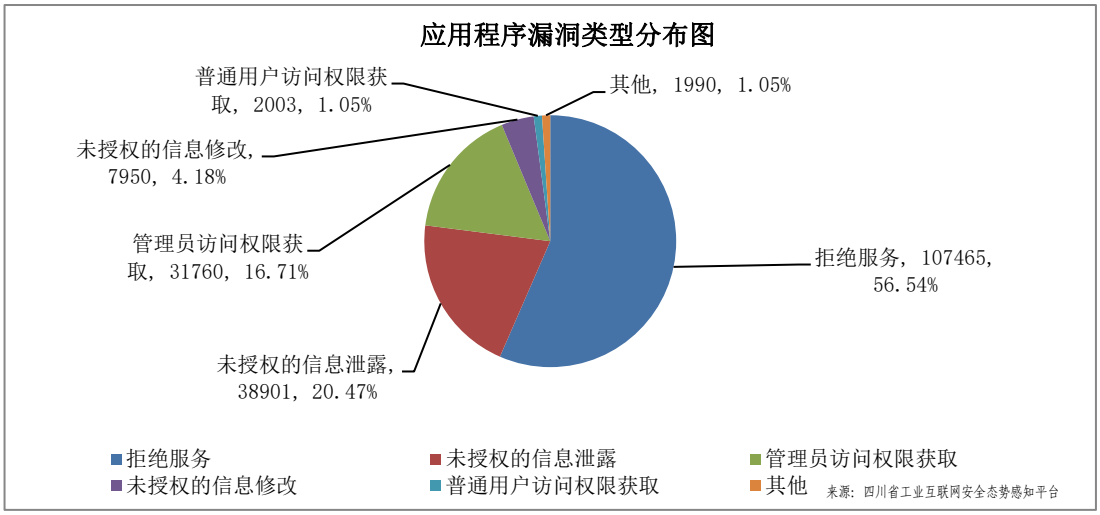

图 3.4 应用程序漏洞类型分布图

3. 行业安全态势分析

2021 年 11 月我省各行业受攻击次数大幅上升，主要集中在计算机、通信和其他电子设备制造业、批发业和汽车制造业。批发业、电气机械和器材制造业上升幅度最大。11 月我省重点行业受攻击次数环比变化情况如图 3.5 所示。

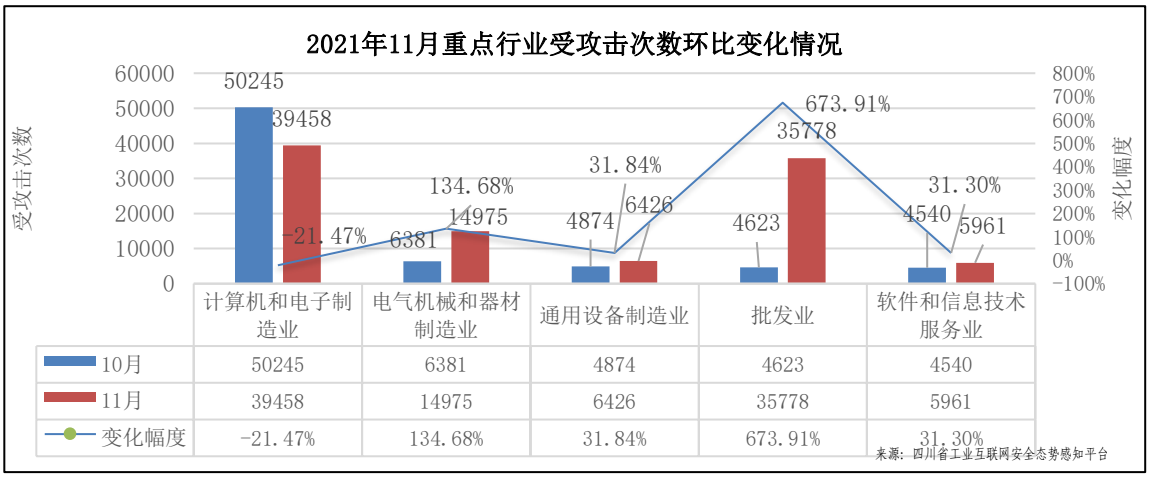

图 3.5 重点行业受攻击次数环比变化情况

4. 地域安全态势分析

2021 年 11 月，通过对我省被攻击地市进行监测分析，绵阳市受攻击的次数相对较多，达到 82,188 次，占全省被攻击次数的 38.93%。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

11 月份，全省被攻击主机 637 个，主要集中在成都、德阳、绵阳，占全省被攻击主机的 93.72%。本月被攻击主机较上月有所减少，乐山、攀枝花和遂宁本月没有主机被攻击。重点地市受攻击主机数量环比变化情况如图 3.7 所示。

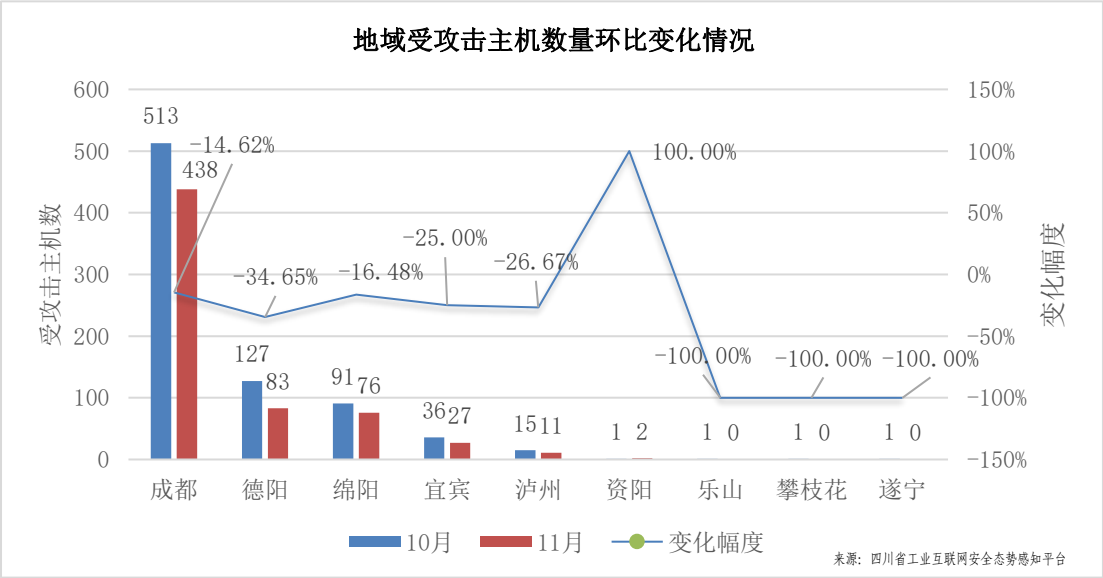

图 3.7 地域受攻击主机数量变化情况

四、 重要网络安全威胁预警

1. 中央网络安全和信息化委员会印发《提升全民数字素养与技能行动纲要》

2021 年 11 月 5 日，中央网络安全和信息化委员会印发《提升全民数字素养与技能行动纲要》（以下简称《行动纲要》），对提升全民数字素养与技能做出安排部署。纲要强调要提高全民网络安全防护能力。引导全民积极参与国家网络安全宣传周、“网络安全进社区”等活动，普及网络安全知识，提升网络安全防范意识。通过举办网络安全专题讲座和培训班、制作印发宣传册、

线上视频宣讲等方式，增强全民对网络谣言、电信诈骗、信息窃取等不法行为的辨别能力和安全防护技能。强化个人信息和隐私保护。要加大个人信息和隐私保护相关法律法规的普及宣传力度，提高全民个人信息和隐私保护意识。制定完善个人信息和隐私保护标准，健全个人信息和隐私保护监管机制，优化社会群众监督举报机制，压实行业组织、企业机构等保护个人信息安全主体责任，加大对侵犯个人信息和隐私等违法犯罪行为的打击力度。

2. 国家互联网信息办公室对《网络数据安全管理条例（征求意见稿）》公开征求意见

2021 年 11 月 14 日，为落实《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律关于数据安全管理的规定，规范网络数据处理活动，保护个人、组织在网络空间的合法权益，维护国家安全和公共利益，根据国务院 2021 年立法计划，国家互联网信息办公室会同相关部门研究起草《网络数据安全管理条例（征求意见稿）》，向社会公开征求意见。

3. 工信部通报 38 款违规 APP 涉及超范围索取权限、过度收集用户个人信息等问题

2021 年 11 月 3 日，工信部针对用户反映强烈的 APP 超范围、高频次索取权限，非服务场景所必需收集用户个人信息，欺骗误导用户下载等违规行为进行了检查，共发现 38 款 APP 存在问题。各通信管理局按照工信部统筹部署，积极开展 APP 技术检测，截

至目前尚有 17 款 APP 未按时限要求完成整改，要求限期整改，逾期不整改或整改不到位的，工信部将依法依规进行处置并予以行政处罚。