四川省公共互联网网络安全态势分析通报（2021 年 4 月）

四川省通信管理局

2021 年 5 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 4 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 11.34Tbps。

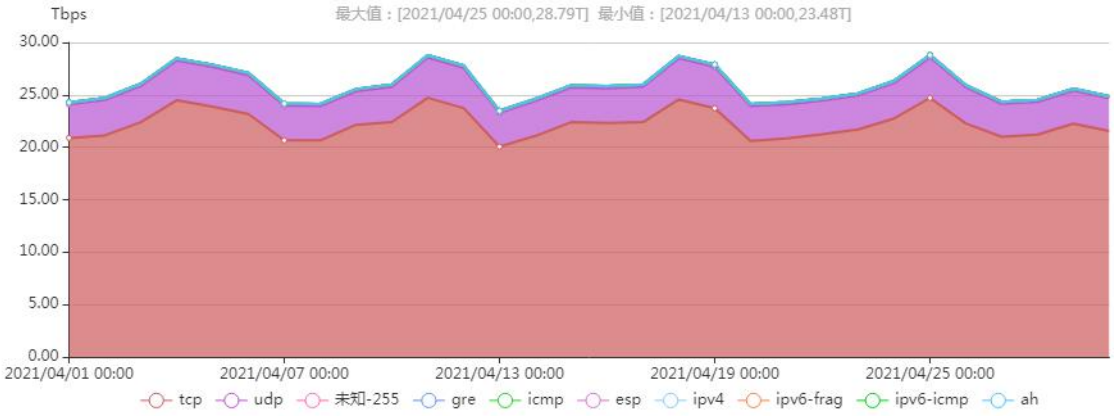

图 1.1 2021 年 4 月四川省内流量监测情况

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，可以发现访问省内网站流量最多。除本省外，排名前三位的地区依次为北京、重庆、云南。

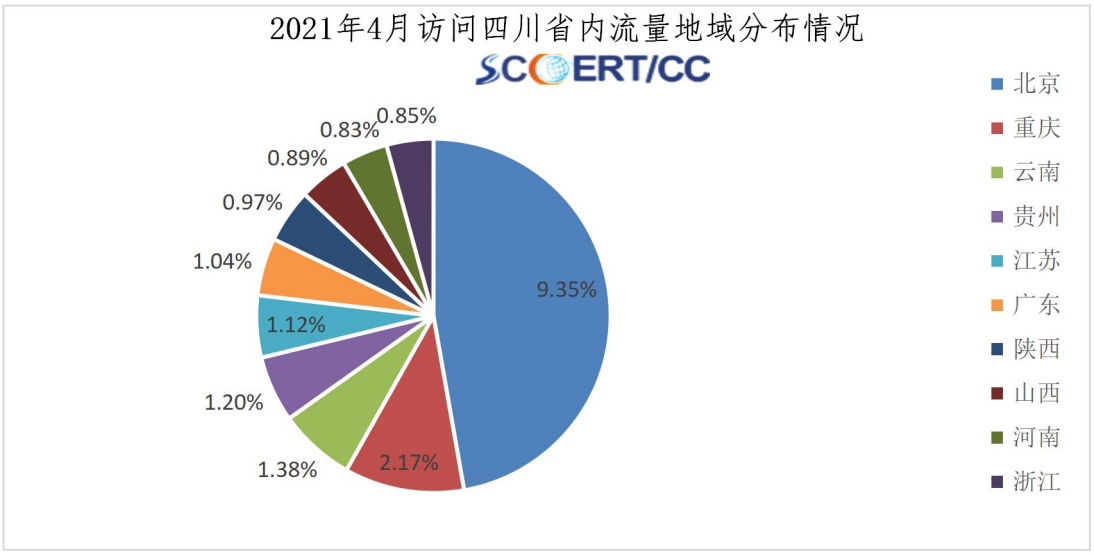

图 1.2 2021 年 4 月访问四川省内流量地域分布情况

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 4 月四川省内互联网用户访问网络的协议前七位占比情况如图 1.3 所示，排名前三的协议分别为 tcp、udp、gre。

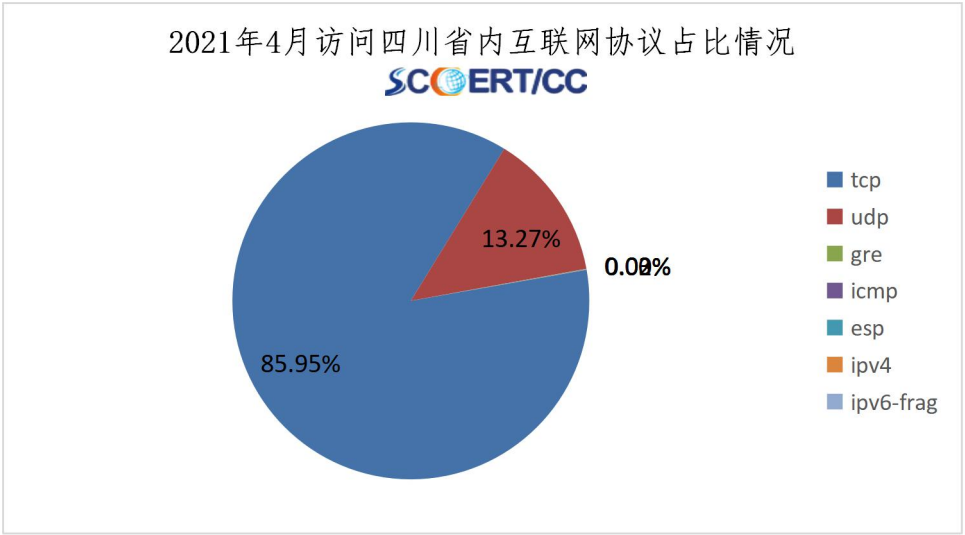

图 1.3 四川省内路由器协议占比情况

3. 省内互联网用户访问域名分布情况

2021 年 4 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。

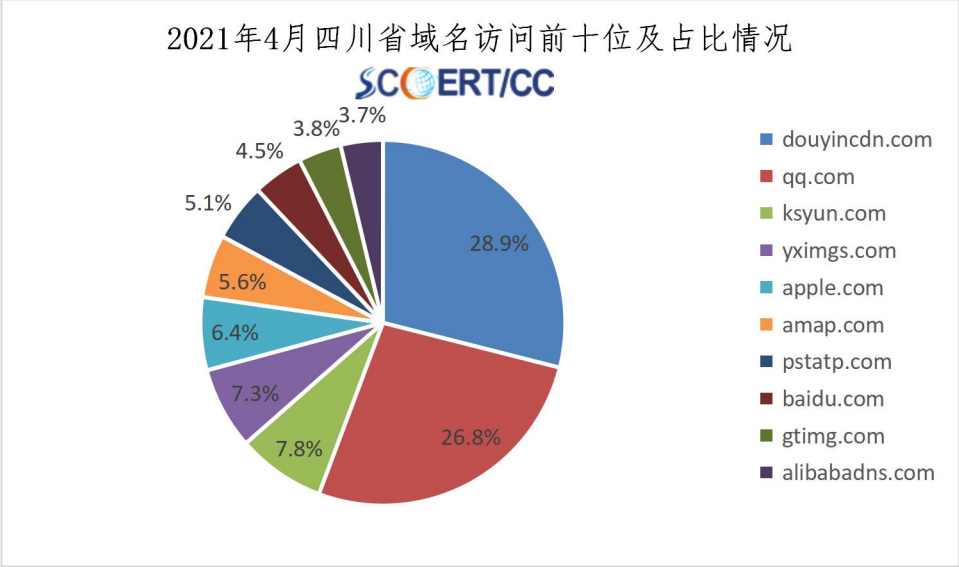

图 1.4 四川省内域名访问情况

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 198964 个 IP 地址对应的主机被木马或僵尸程序控制，环比上升 66.29%。2020 年 4 月-2021 年 4 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 8296 个 IP 地址存在木马或僵尸程序控制服务器，环比上升 29.16%。2020 年 4 月-2021 年 4 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，本月呈上升趋势。

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、广安，其中成都数量最多，有 97642 台主机感染僵尸木马。

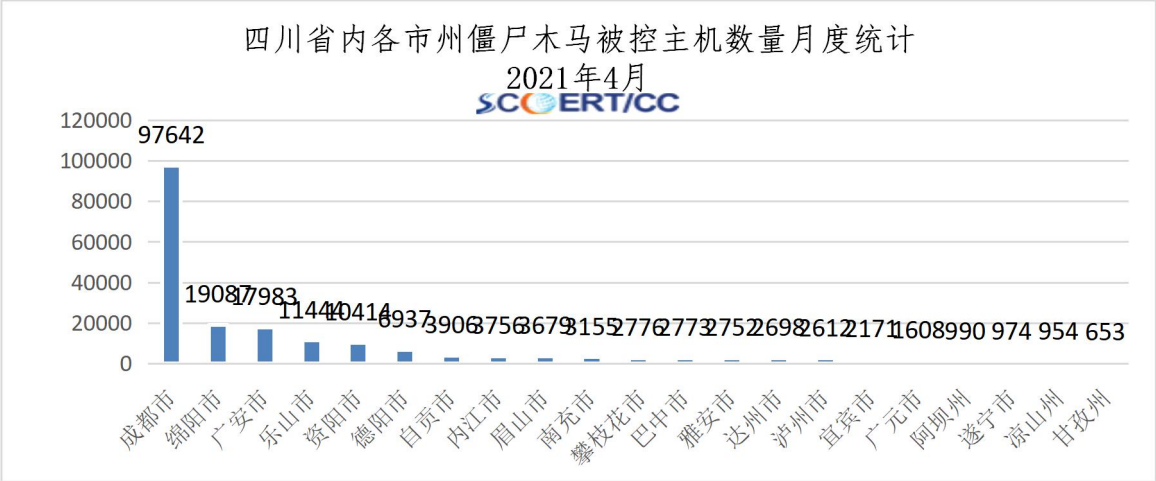

图 2.3 四川省内各市州主机感染僵尸木马主机数量分布

2. 网页篡改

本月，主机位于四川地区的被篡改网站数量为 225 个。2020 年 4 月-2021 年 4 月，四川省内被篡改网站数量月度分布如图 2.4 所示，整体呈下降趋势。

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 134 个。

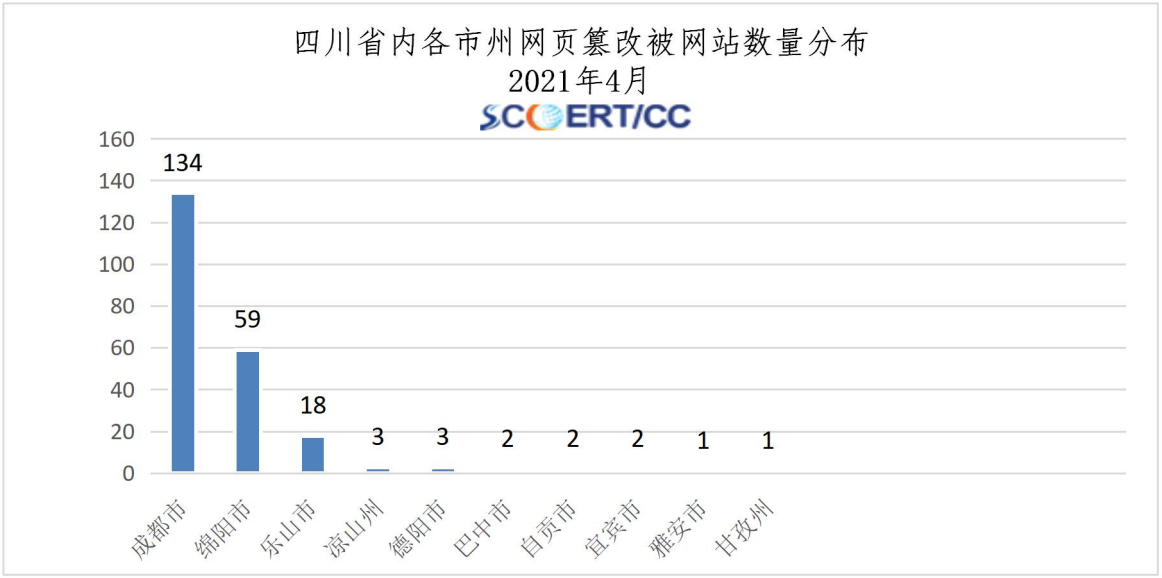

图 2.5 四川省内各市州网页篡改被网站数量分布

3. 网页后门

主机位于四川省被植入 176 个，环比上升 62.96%。2020 年 4 月-2021 年 4 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 136 个。

1

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 4 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 9053 家、工业设备 17.86 万台、工业互联网平台 10 个、工业 APP 5163 款。目前平台已完成与四川长虹、郎酒工业互联网标识解析二级节点对接，发现企业节点 31 个、标识数量 3.4 亿个。

2021 年 4 月，我省工业互联网安全态势整体平稳，无重大安全事件发生。发现的工业设备漏洞较上月减少 99.2%，安全威胁数量较上月增加 36.8%。针对工业企业的攻击主要分布在房地产业、研究和试验发展、汽车制造业，被攻击的地市主要集中在成都市、德阳市，攻击手段主要包括木马后门、Web 攻击、漏洞利用等。

1.网络安全威胁情况

2021 年 4 月，平台监测发现我省重点工业企业安全威胁 242280 起，其中高危安全威胁达到 101018 起，环比上月增长 31.17%；本月受到高危安全威胁的工业企业共计 107 家，环比上月增加 4.90%。随着护网行动的开展，近期安全威胁月累计数量总体呈现上升趋势。其中，4 月安全威胁事件上升尤为明显。2-4 月安全威胁数量如图 3.1 所示。

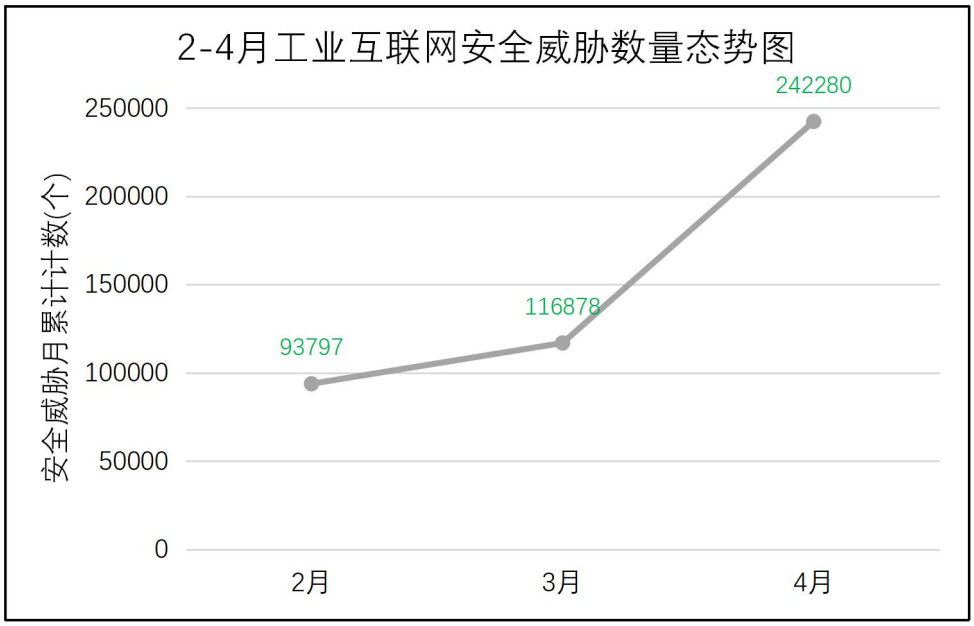

图 3.1　2-4 月工业互联网安全威胁数量态势图

本月主要安全威胁类型为木马后门、Web 攻击、漏洞利用、命令执行、非法外联，其中木马后门攻击次数达到 127728 次，占比为 53%，安全威胁类型分布情况如图 3.2 所示。

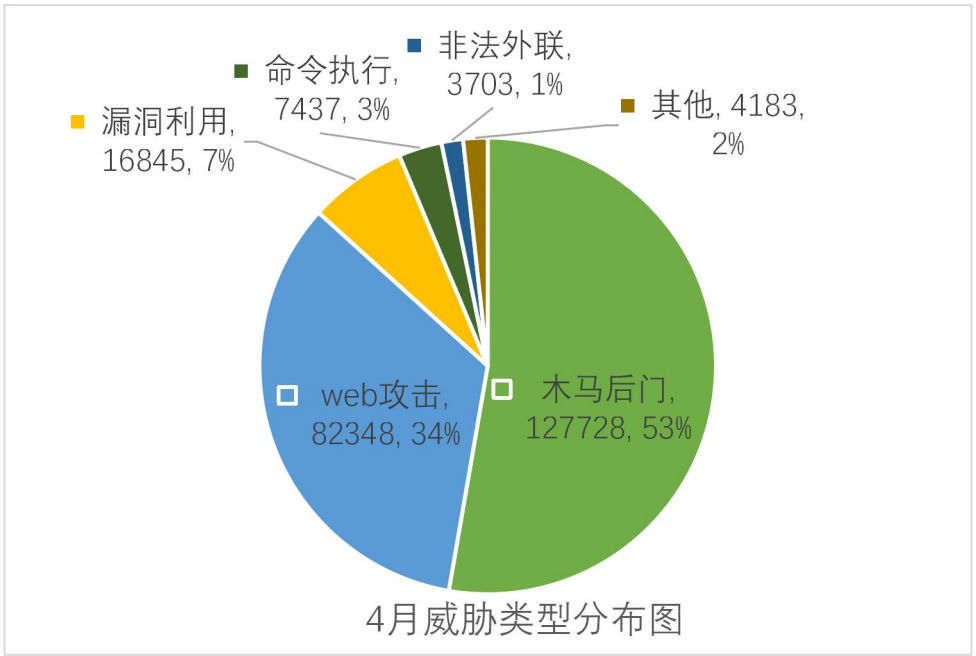

图 3.2 安全威胁类型分布图

从安全威胁类型角度进行分析，近期各类威胁数量均呈现上

升趋势。其中木马后门攻击次数最多，达到 127728 次；增长幅度最大的为漏洞利用，增长幅度达到 784.25%。本月安全威胁类型 top5 及环比变化情况如图 3.3 所示。

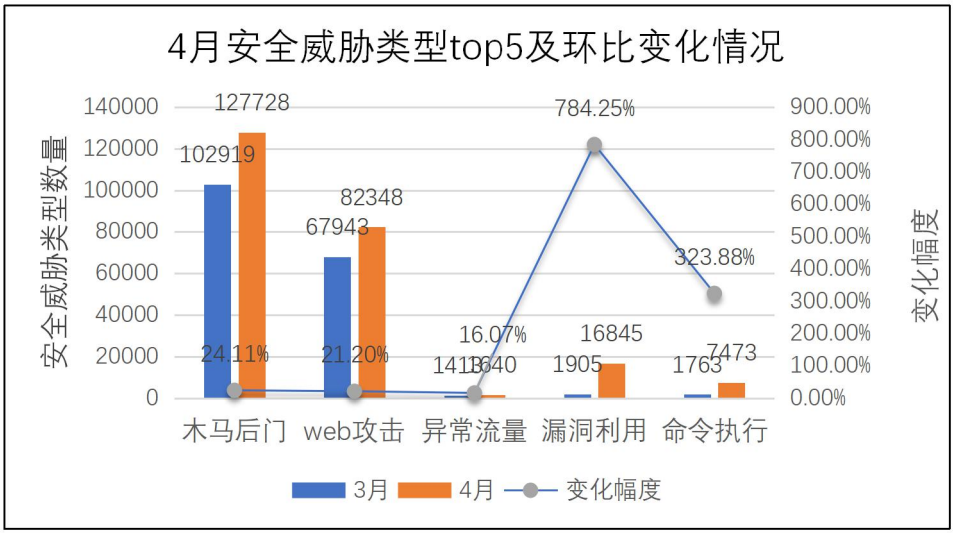

图 3.3　4 月安全威胁类型 top5 及环比变化情况

2. 工业设备安全漏洞情况

截至 2021 年 4 月，监测到我省企业设备漏洞 189660 个，其中高危漏洞 34740 个，占总设备漏洞的 18.32%。漏洞主要集中在成都市的企业，占全省工业设备新增漏洞数量的 74.51%。涉及的漏洞类型分布如图 3.4 所示：

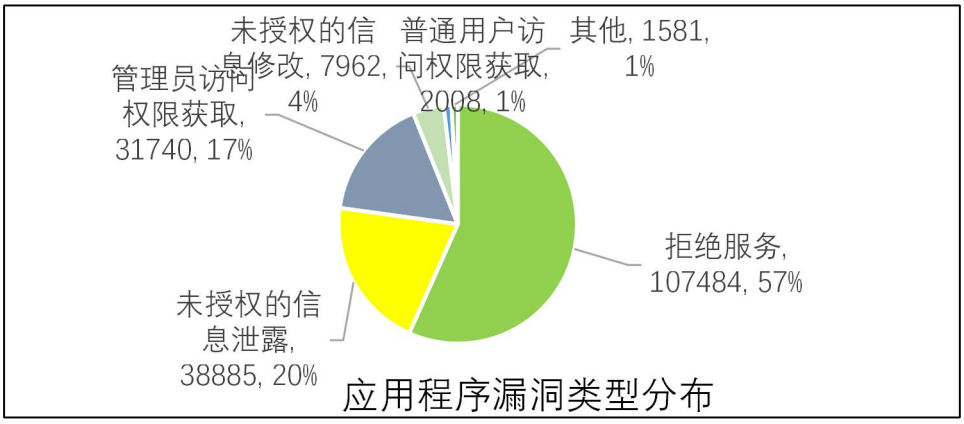

图 3.4 应用程序漏洞类型分布图

3. 行业安全态势分析

由于护网行动的开展，2021 年 4 月监测发现，针对我省各行业的攻击次数呈现指数式上升，其中针对我省房地产业的网络攻击行为 43627 次，较 3 月环比增加 218035.00%，为本月被攻击次数最多的行业。3 月、4 月我省重点行业受攻击次数环比变化情况如图 3.5 所示。

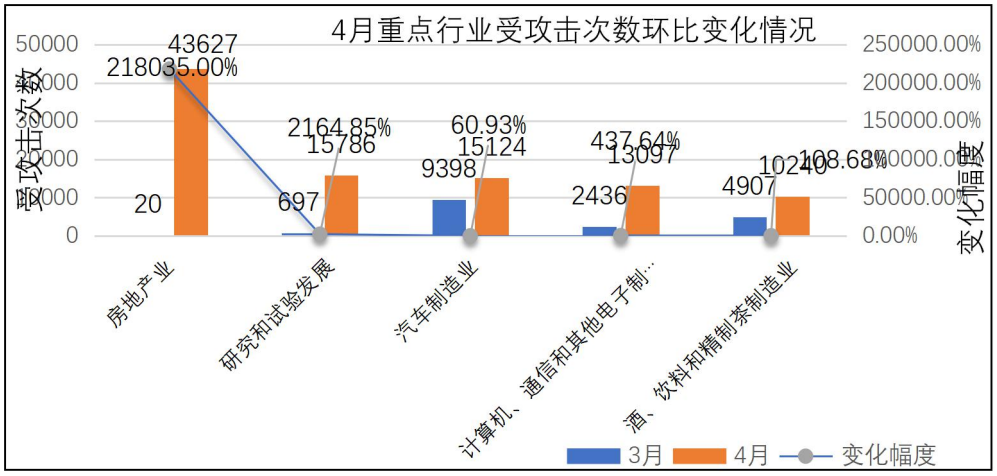

图 3.5 重点行业受攻击次数环比变化情况

4. 地域安全态势分析

2021 年 4 月对我省重点工业企业所在地域进行监测分析，成都受攻击的次数相对较多，为 142193 次，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

从被攻击者视角分析，全省被攻击主机 322 个，主要集中在成都、德阳、绵阳，占全省被攻击主机的 94.72%，重点地市受攻击主机数量环比变化情况如图 3.7 所示。

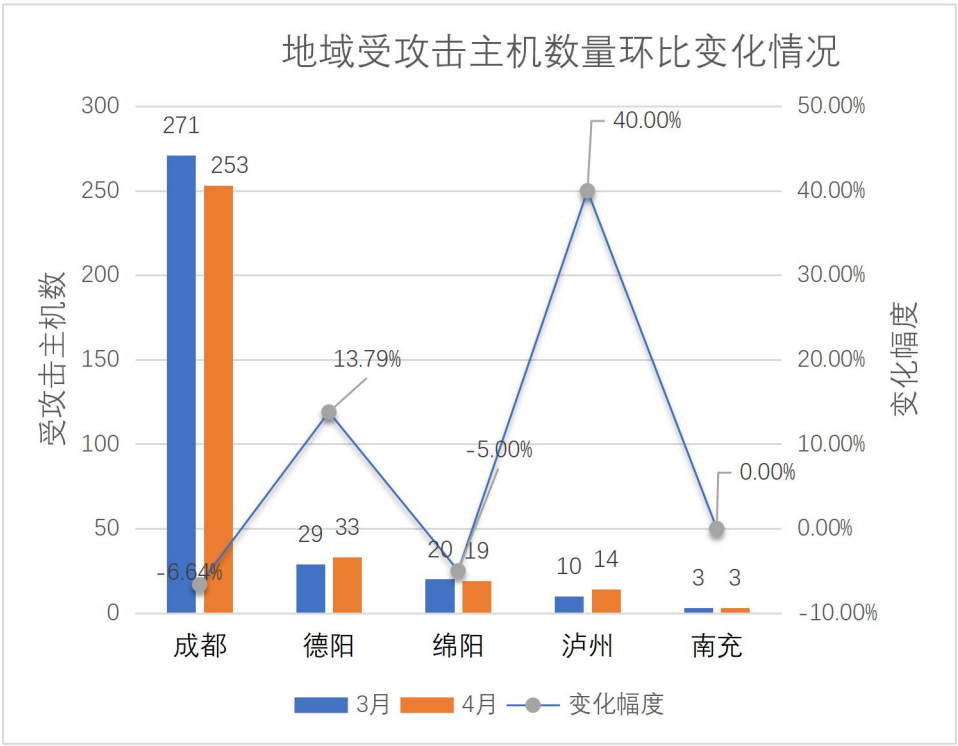

图 3.7 地域受攻击主机数量变化情况

四、 重要网络安全威胁预警

1.Microsoft 发布 2021 年 4 月安全更新

2021年4月13日，据国家信息安全漏洞共享平台（CNVD）官网消息，微软发布了2021年4月份的月度例行安全公告，修复了其多款产品存在的104个安全漏洞。受影响的产品包括：Windows1020H2&WindowsServerv20H2（79个）、Windows102004&WindowsServerv2004（79个）、Windows101909&WindowsServerv1909（77个）、Windows8.1&Server2012R2（55个）、WindowsServer2012（54个）、WindowsRT8.1（54个）和MicrosoftOffice-relatedsoftware（7个）。利用上述漏洞，攻击者可以绕过安全功能限制，获取敏感信息，提升权限，执行远程代码，或发起拒绝服务攻击等。CNVD提醒广大Microsoft用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

2.关于 GoogleChrome 存在远程代码执行漏洞的安全公告

2021 年 4 月 14 日，据国家信息安全漏洞共享平台（CNVD）官网消息，CNVD 收录了 GoogleChrome 远程代码执行漏洞（CNVD-2021-27989）。攻击者利用该漏洞，可在未授权的情况下远程执行代码。目前，漏洞细节已公开，厂商已发布新版本修复该漏洞。未经身份验证的攻击者利用该漏洞，可通过精心构造

恶意页面,诱导受害者访问,实现对浏览器的远程代码执行攻击,但攻击者单独利用该漏洞无法实现沙盒（SandBox）逃逸。CNVD提醒广大用户使用 GoogleChrome 浏览器时不要关闭默认沙盒模式，谨慎访问来源不明的网页链接或文件，并更新至最新版本。