四川省公共互联网网络安全态势分析通报

（2021 年 6 月）

四川省通信管理局

2021 年 7 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 6 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 13.07Tbps。

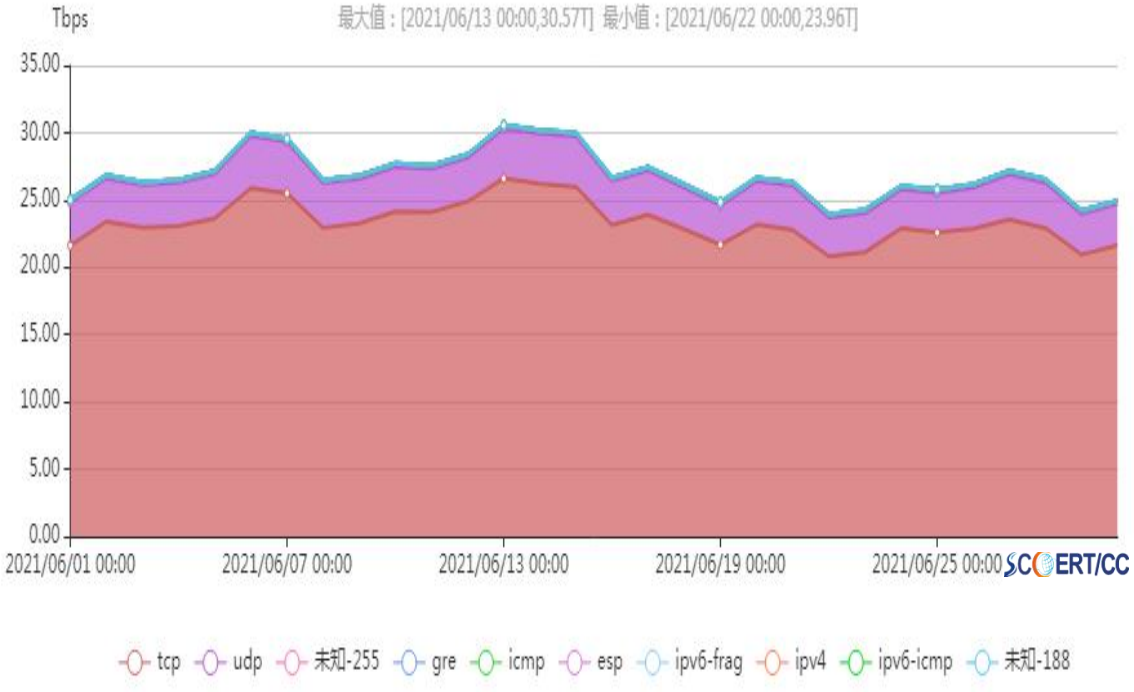

图 1.1 2021 年 6 月四川省内流量监测情况

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，可以发现四川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。

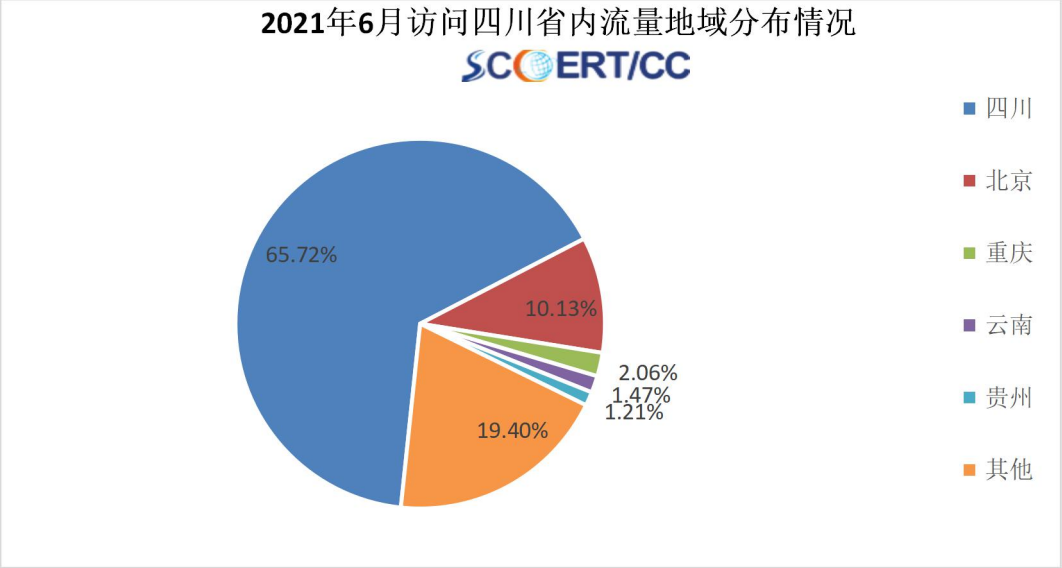

图 1.2 2021 年 6 月访问四川省内流量地域分布情况

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 6 月四川省内互联网用户访问网络的协议前二位占比情况如图 1.3 所示，分别为 tcp、udp。

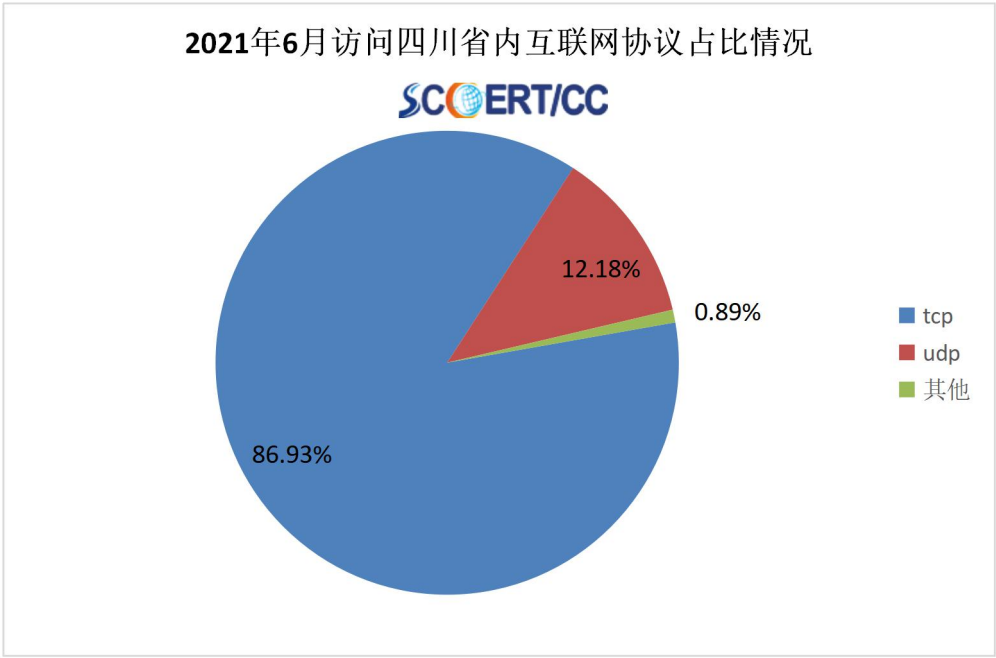

图 1.3 四川省内路由器协议占比情况

3. 省内互联网用户访问域名分布情况

2021 年 6 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。

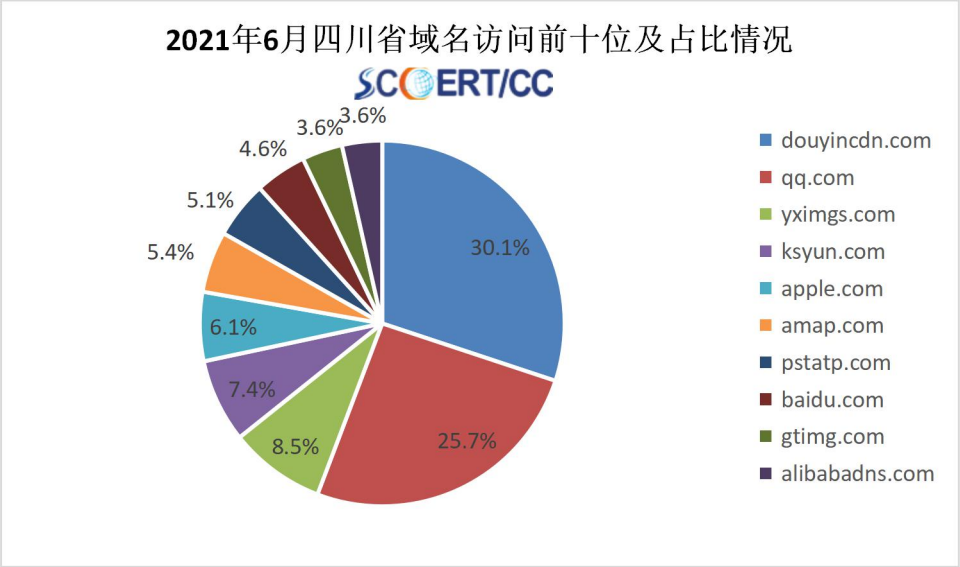

图 1.4 四川省内域名访问情况

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 159430 个 IP 地址对应的主机被木马或僵尸程序控制，环比下降 29.95%。2020 年 6 月-2021 年 6 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 7887 个 IP 地址存在木马或僵尸程序控制服务器，环比下降 64.27%。2020 年 6 月-2021 年 6 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、资阳，其中成都数量最多，有 81568 台主机感染僵尸木马。

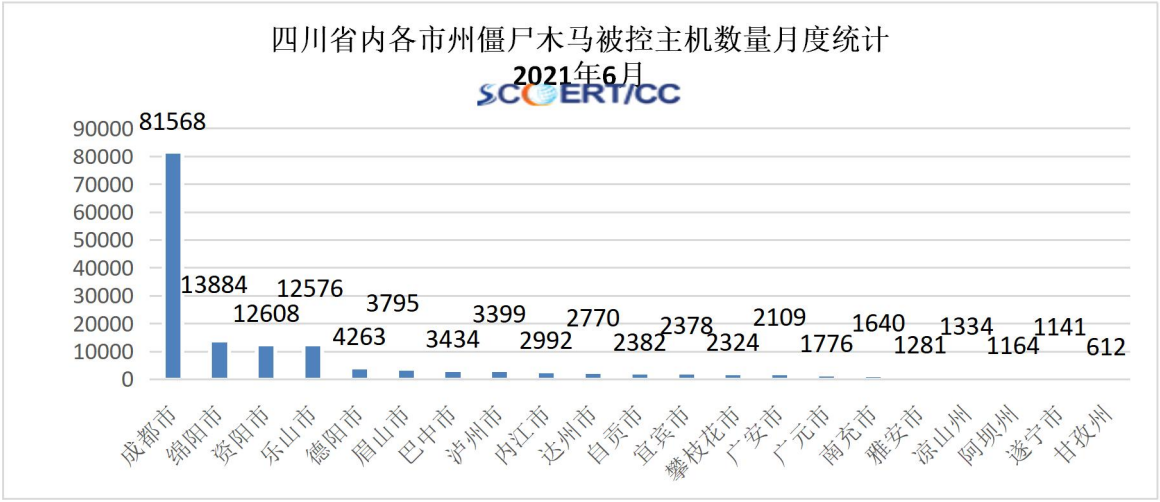

图 2.3 四川省内各市州主机感染僵尸木马主机数量分布

2. 网页篡改

本月，主机位于四川地区的被篡改网站数量为 483 个，环比上升 263%。2020 年 6 月-2021 年 6 月，四川省内被篡改网站数量月度分布如图 2.4 所示，本月较上月大幅上升。

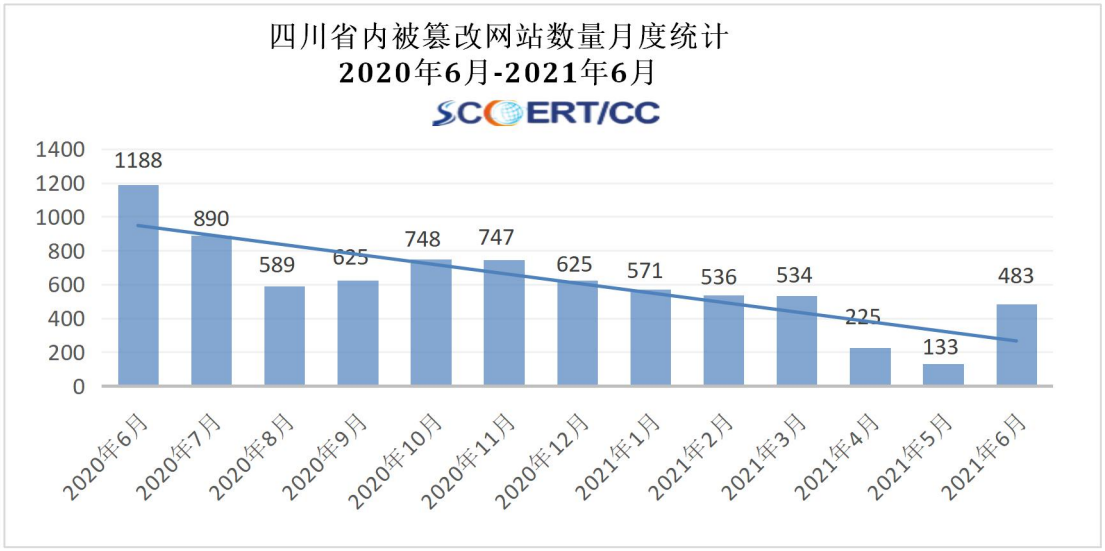

图 2.4 四川省被篡改网站数量月度分布图

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 362 个。

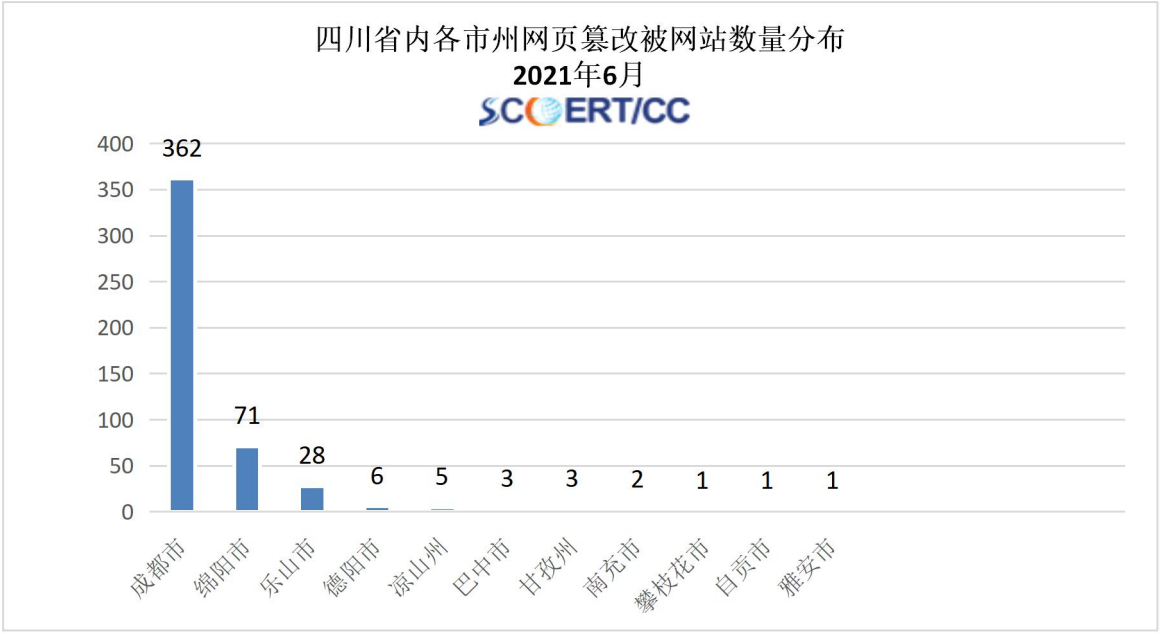

图 2.5 四川省内各市州网页篡改被网站数量分布

3. 网页后门

主机位于四川省被植入 198 个，环比下降 32.88%。2020 年 6 月-2021 年 6 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。

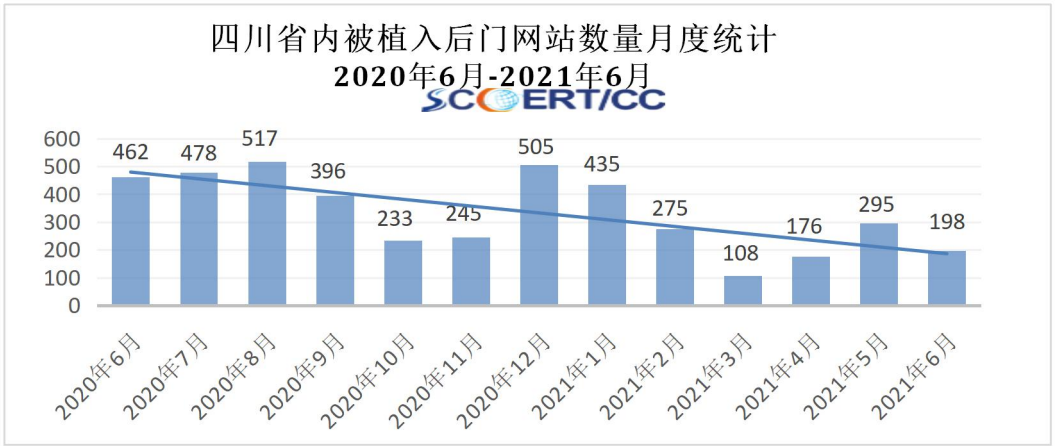

图 2.6 四川省被植入后门的网站主机数量月度分布图

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 142 个。

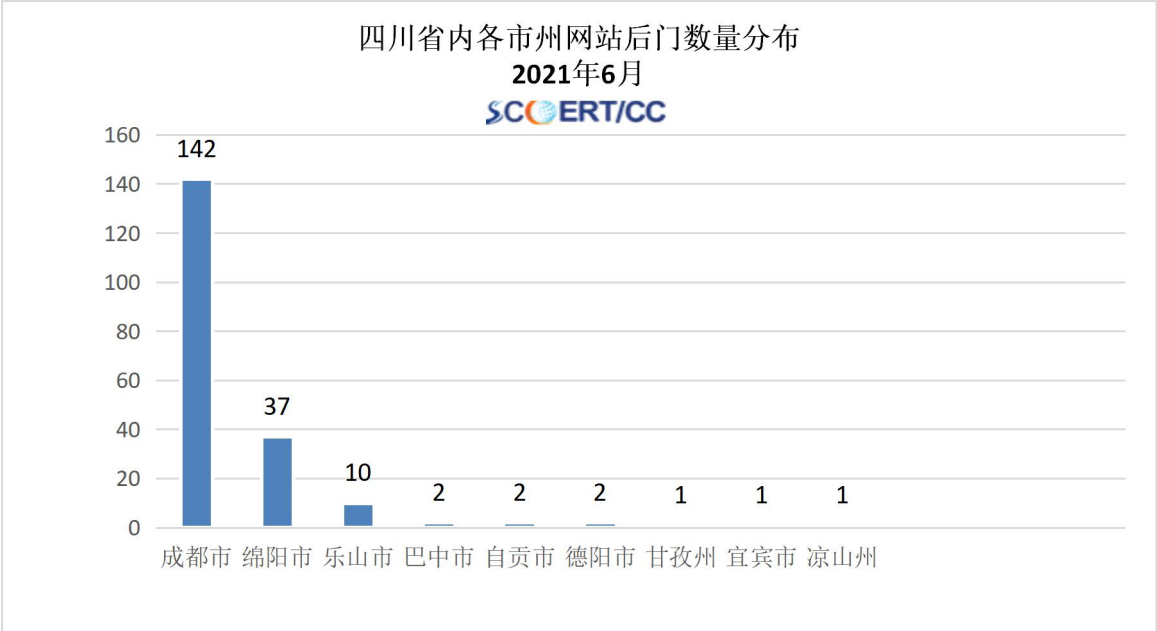

图 2.7 四川省被植入后门的网站主机数量月度分布图

三、 本月工业互联网网络安全态势

截至 2021 年 6 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 11073 家、工业设备 17.88 万台、工业 APP 7223 款。截至 2021 年 6 月 30 日态势感知平台共发现 50 家工业互联网平台，其中有 10 家平台归属于四川省。

2021 年 6 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。发现的安全威胁数量较上月减少 60%。从攻击行为来看，本月各主要安全威胁均有所下降，其中 web 攻击下降幅度最大。木马后门攻击占比达 64.93%，位居本月威胁事件榜首；从被攻击的行业来看，针对工业企业的攻击主要分布在橡胶和塑

料制品业、房地产业、汽车制造业、软件和信息技术服务业，其中橡胶和塑料制品业取代研究和试验发展成为本月的重点安全威胁行业；从被攻击的地域来看，被攻击的地市主要集中在成都市、德阳市和泸州市，占据全省被攻击主机的 94.03%；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 6 月，平台监测发现我省重点工业企业安全威胁 65507 起，涉及企业 125 家。其中高危安全威胁 43707 起，占据总体威胁数量中的 66.72%，安全威胁数量环比上月减少 60%；本月受到高危安全威胁的工业企业共计 117 家，与上月相比减少 19.66%。近期安全威胁事件数量均呈下降趋势，其中木马后门和 web 攻击下降幅度最大。3-6 月安全威胁数量如图 3.1 所示。

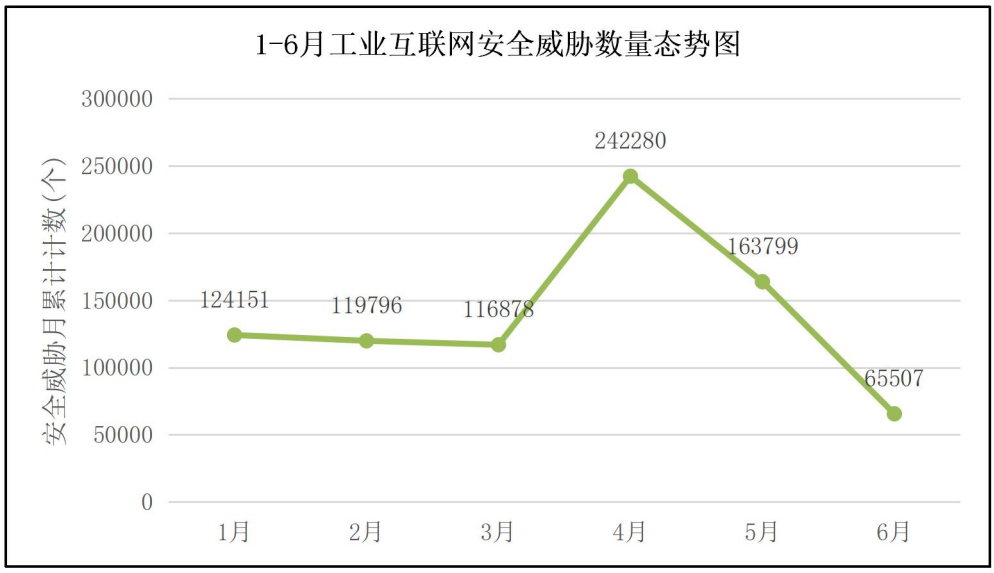

图 3.1　1-6 月工业互联网安全威胁数量态势图

本月平台监测恶意网络行为 65507 起，木马后门、Web 攻击、漏洞利用、异常流量和非法外联为本月主要安全威胁类型，其中

木马后门攻击次数达到 42535 次，占比为 64.93%，6 月安全威胁类型分布情况如图 3.2 所示。

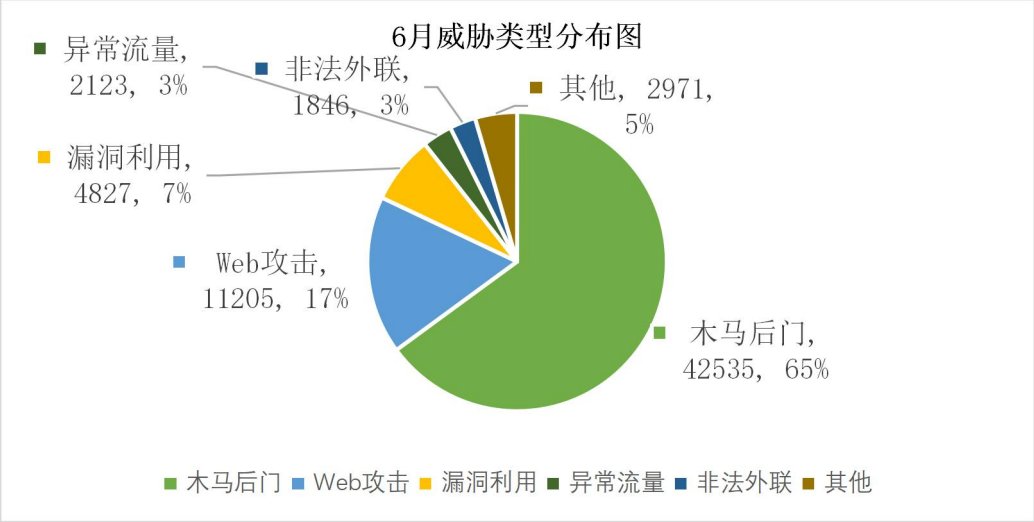

图 3.2　安全威胁类型分布图

从安全威胁类型角度进行分析，6 月各主要安全威胁类型均呈下降趋势。其中下降幅度最大的为 web 攻击和木马后门，下降幅度分别为 79.45%和 54.05%。本月安全威胁类型 top5 及环比变化情况如图 3.3 所示。

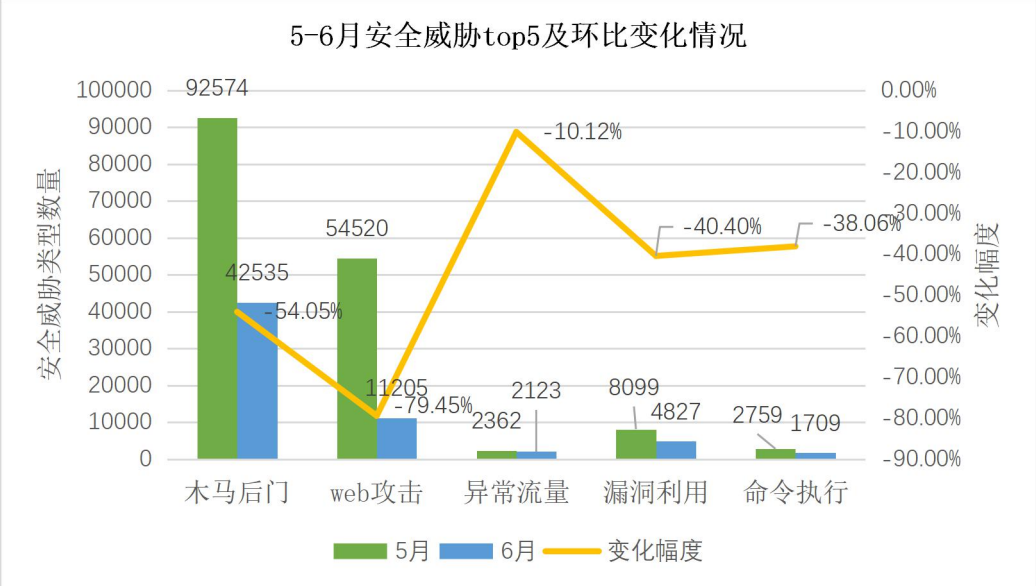

图 3.3　5-6 月安全威胁类型 top5 及环比变化情况

2. 工业设备安全漏洞情况

截至 2021 年 6 月，监测到我省企业安全漏洞 189745 个，其中高危漏洞 34822 个，占总设备漏洞的 18.35%。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 74.49%。通过对工业互联网中暴露的工业资产的持续安全漏洞监测，需要重点关注的高中危安全漏洞如表 1 所示。

表 1 漏洞类型编号排名（top10）

漏洞编号	数量	漏洞类型
CNVD-2016-00962	29116	拒绝服务
CNVD-2016-00982	29112	拒绝服务
CNVD-2016-00961	29108	拒绝服务
CNVD-2018-06530	14221	未授权的信息泄露
CNVD-2018-05440	5393	管理员访问权限获取
CNVD-2016-01325	1495	未授权的信息泄露
CNVD-2016-01769	1415	管理员访问权限获取
CNVD-2016-00274	1415	未授权的信息泄露
CNVD-2016-00276	1415	拒绝服务
CNVD-2016-00392	1414	拒绝服务

监测到的设备漏洞中，排名前三的为拒绝服务、未授权信息泄露、管理员访问权限获取。涉及的漏洞类型分布如图 3.4 所示：

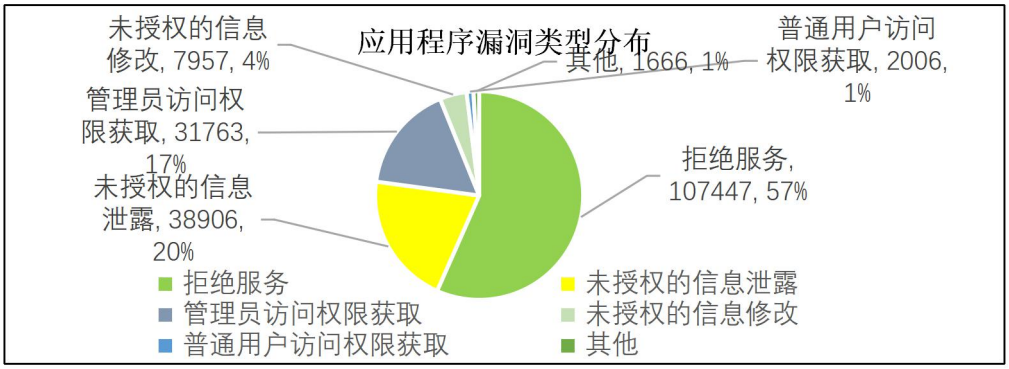

图 3.4 应用程序漏洞类型分布图

3. 行业安全态势分析

从行业类型角度分析，2021 年 6 月，针对我省各行业的攻击次数总体有所减少，但针对我省橡胶和塑料制品业的攻击次数有所增加。本月橡胶和塑料制品业攻击次数达 8606 次，取代研究和试验发展成为本月被攻击次数最多的行业。5 月、6 月我省重点行业受攻击次数环比变化情况如图 3.5 所示。

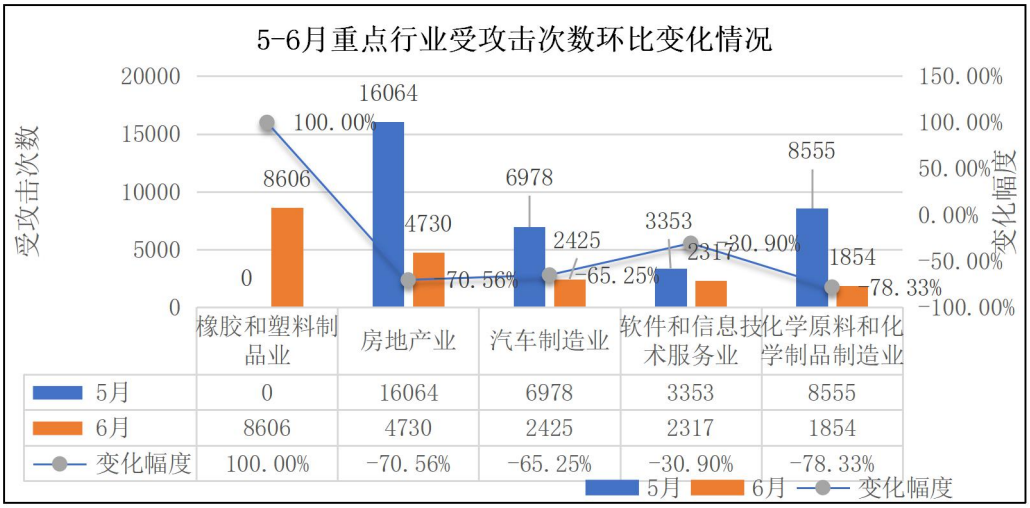

图 3.5 重点行业受攻击次数环比变化情况

4. 地域安全态势分析

2021 年 6 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 24099 次，占全省被攻击次数的 66.96%。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 268 个，主要集中在成都、德阳、绵阳，占全省被攻击主机的 94.03%。成都、绵阳和南充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。

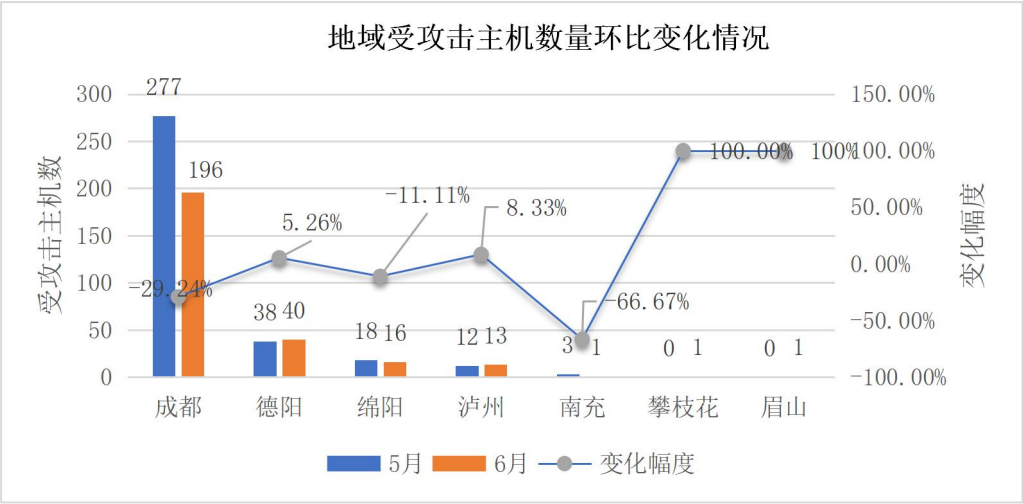

图 3.7 地域受攻击主机数量变化情况

四、 重要网络安全威胁预警

1.关于用友 NCBeanShell 存在远程代码执行漏洞的安全公告

2021 年 6 月 3 日，据国家信息安全漏洞共享平台（CNVD）消息，4 月 12 日，CNVD 收录了用友 NCBeanShell 远程代码执行漏洞（CNVD-2021-30167）。该漏洞的综合评级为“高危”。攻击者利用该漏洞，可在未授权的情况下远程执行代码，该漏洞对部署于公共互联网上的用友 NC6.5 系统构成一定的安全风险。目前，漏洞利用细节已公开，用友公司已发布版本补丁完成修复，并通过服务渠道推送解决方案，授权用户可以通过访问链接进行下载。CNVD 建议该产品用户立即通过官方网站安装最新补丁，及时消除漏洞隐患。