四川省网络安全态势分析通报
（2021 年 3 月）

四川省通信管理局

2021 年 4 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 3 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 11.63Tbps。

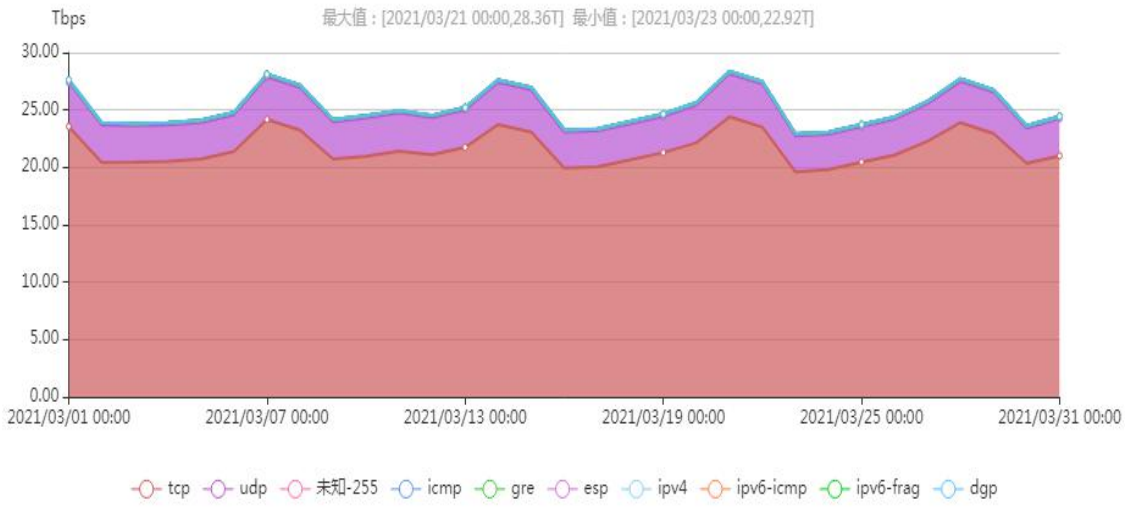


图 1.1 2021 年 3 月四川省内流量监测情况

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、贵州。

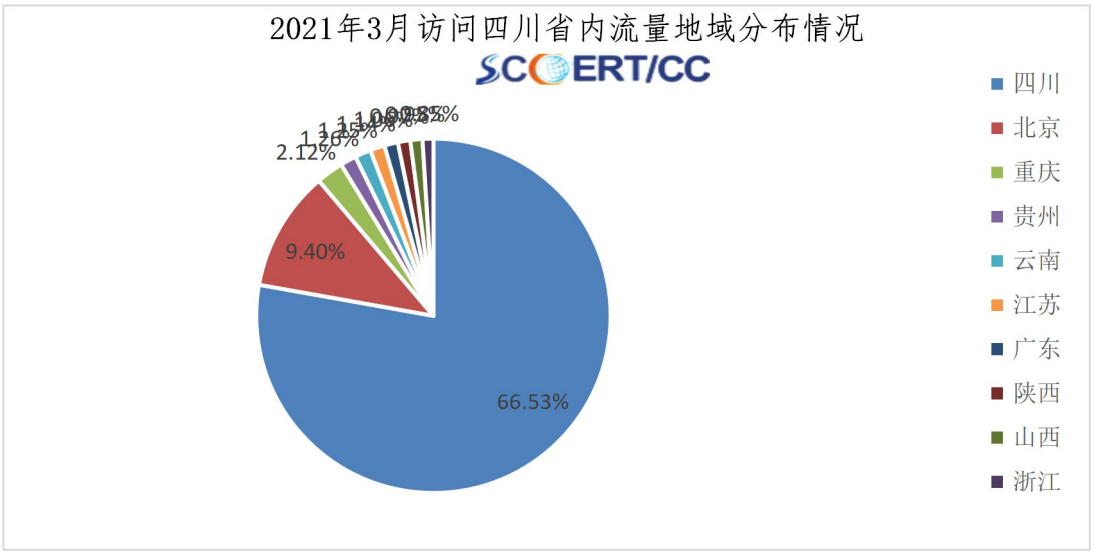


图 1.2 2021 年 3 月访问四川省内流量地域分布情况

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 3 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、icmp。

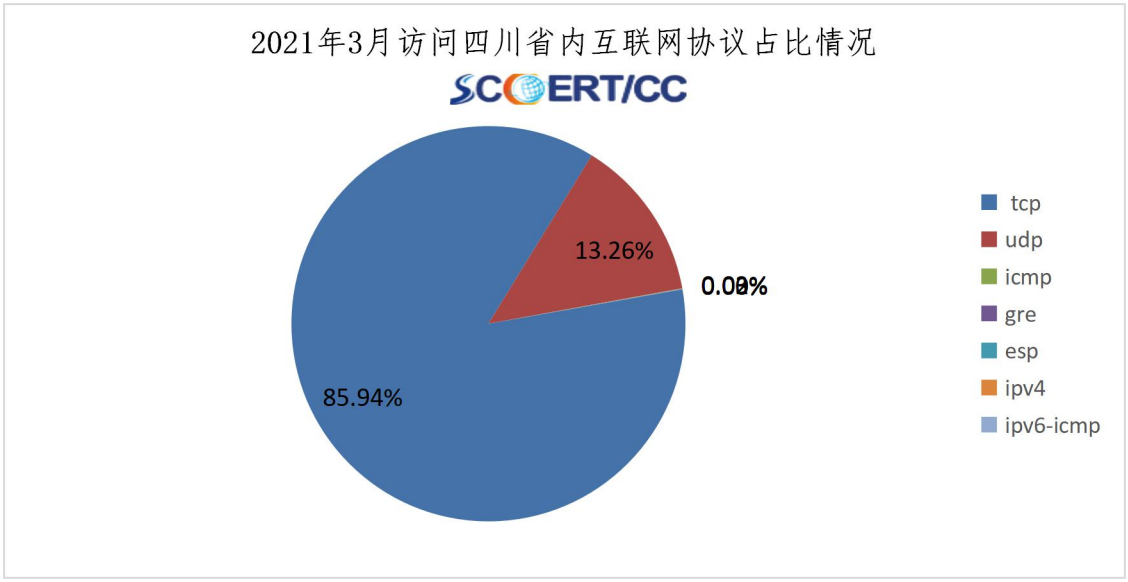


图 1.3 四川省内路由器协议占比情况

3. 省内互联网用户访问域名分布情况

2021 年 3 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。

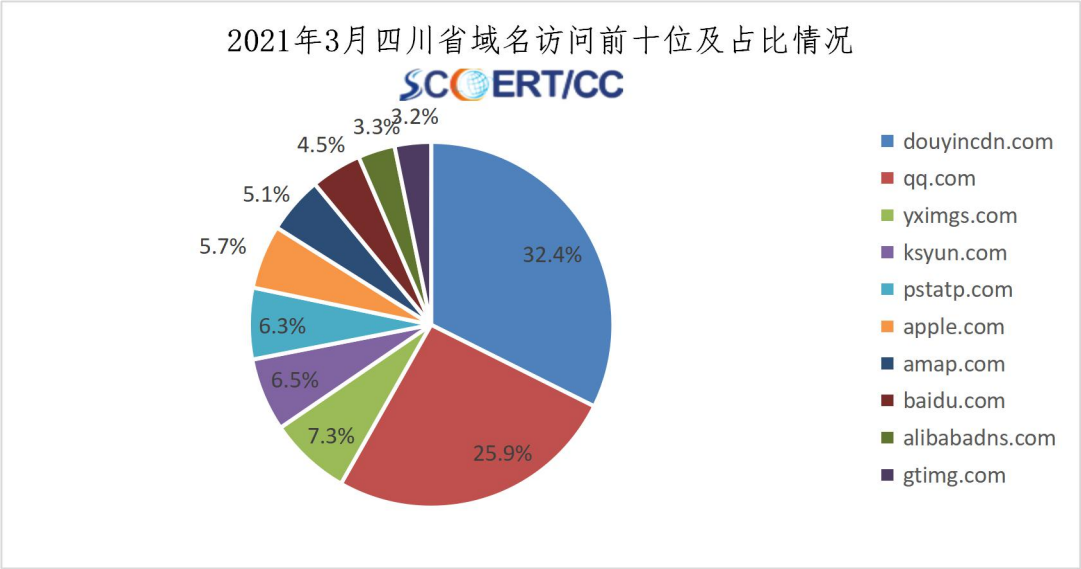


图 1.4 四川省内域名访问情况

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。在公共互联网网络安全环境方面，除感染僵尸木马事件、网页篡改事件数量有所上升，网站后门事件数量有所下降。

1.木马、僵尸网络

四川省本月有119651个IP地址对应的主机被木马或僵尸程序控制，环比上升42.70%。2020年3月-2021年3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。

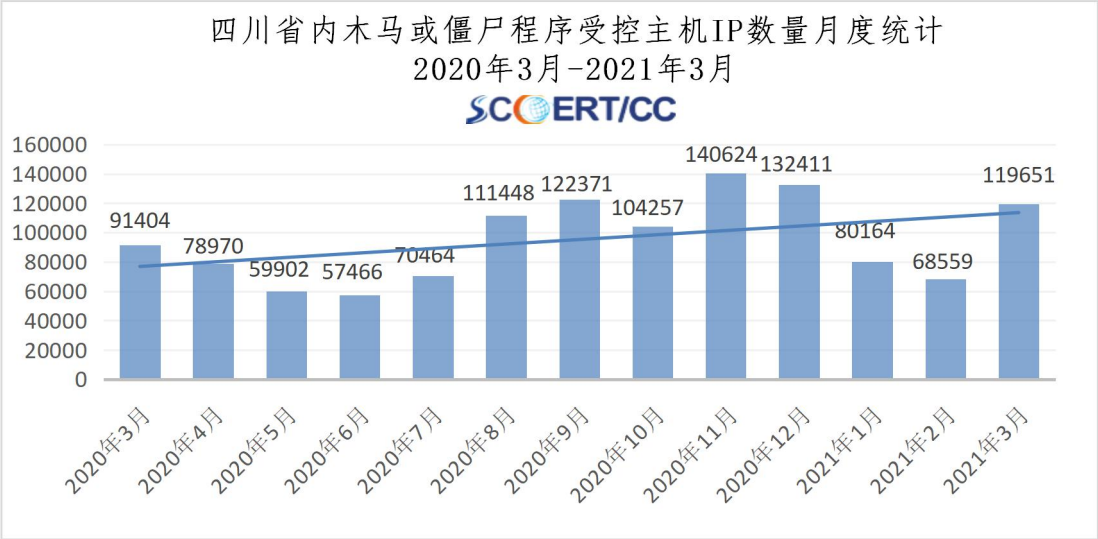


图2.1 四川省木马或僵尸程序受控主机IP数量月度分布图

四川省本月有6423个IP地址存在木马或僵尸程序控制服务器，环比上升51.12%。2020年3月-2021年3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、资阳，其中成都数量最多，有 60178 台主机感染僵尸木马。

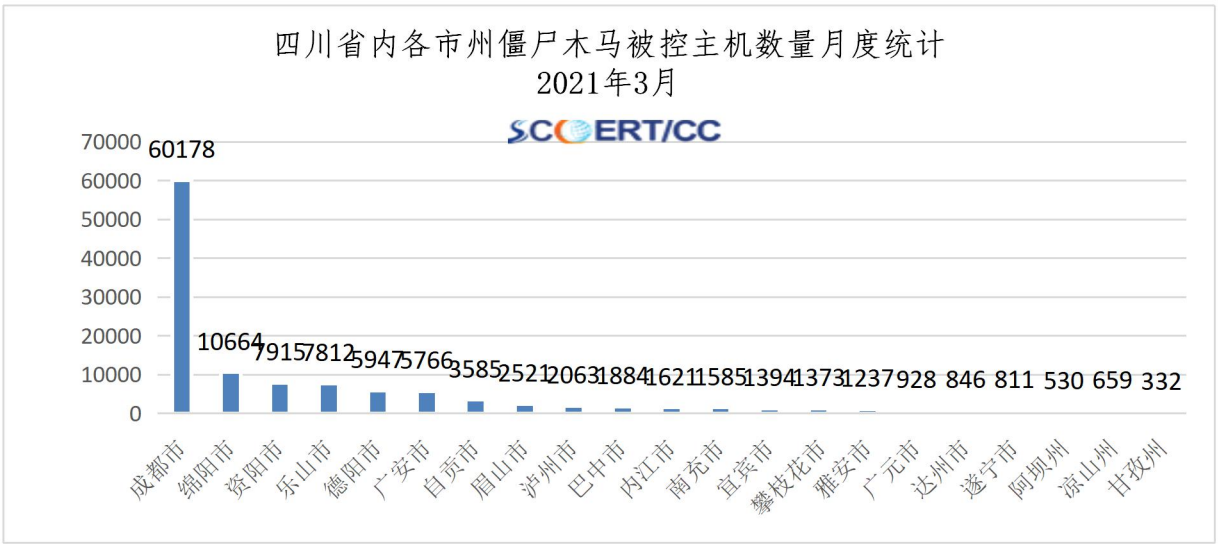


图 2.3 四川省内各市州主机感染僵尸木马主机数量分布

2. 网页篡改

本月，主机位于四川地区的被篡改网站数量为 534 个。2020 年 3 月-2021 年 3 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 421 个。

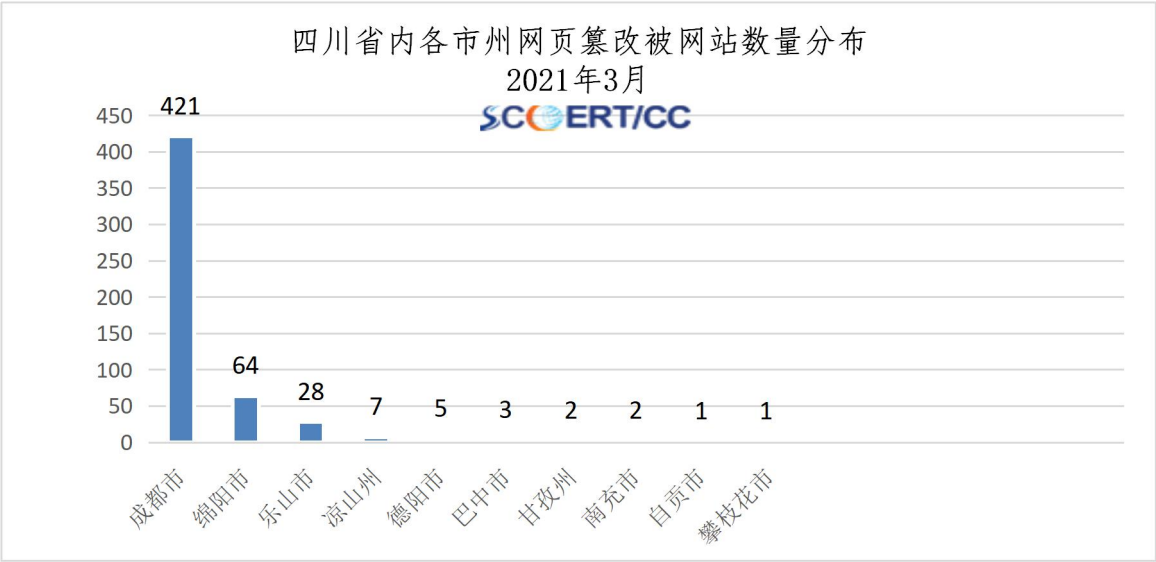


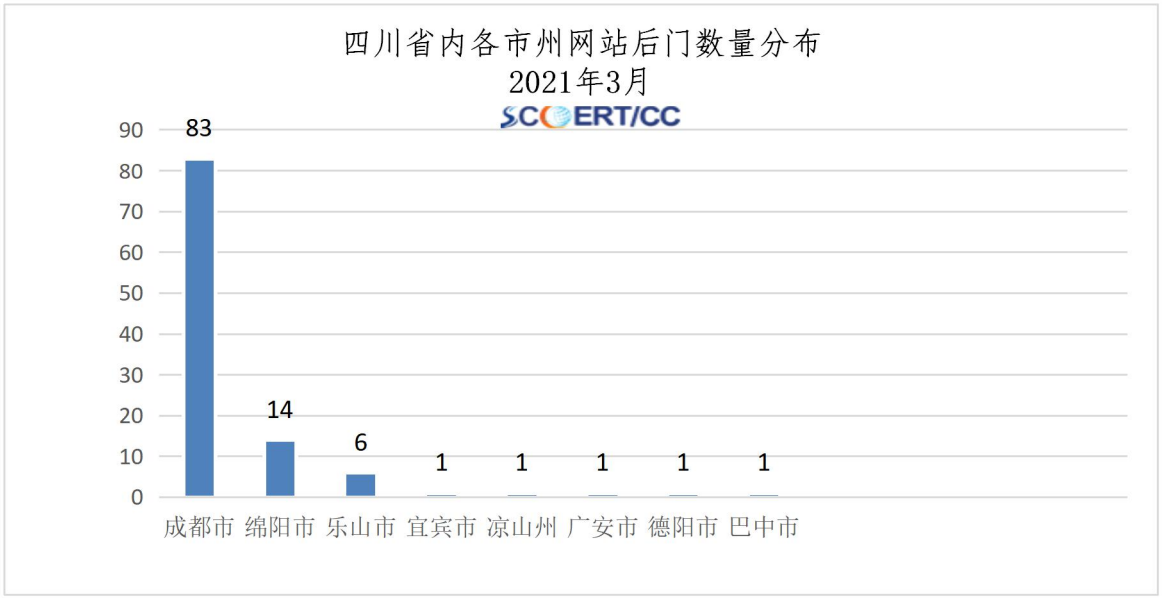
图 2.5 四川省内各市州网页篡改被网站数量分布

3. 网页后门

主机位于四川省被植入 108 个，环比下降 60.73%。2020 年 3 月-2021 年 3 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 83 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 3 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 1.12 万家、工业设备 17.86 万台、工业互联网平台 10 个、工业 APP 5098 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 3 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。平台专线接入规模持续扩大，发现的工业设备漏洞较上个月增加 932.27%，安全威胁数量较上月环比增加 24.6%。针对工业企业的攻击主要分布在汽车制造业、化学原料和化学制

品制造业、酒饮料和精制茶制造业，被攻击的地市主要集中在成都市、南充市，而攻击手段主要包括 Web 攻击、木马后门、非法外联等。

1.网络安全威胁情况

2021 年 3 月，平台监测发现我省重点工业企业安全威胁 116878 起，其中高危安全威胁 44068 起，环比上月增长 60.97%；本月受到高危安全威胁的工业企业 102 家，环比上月增加 64.52%。近期安全威胁月累计数量总体呈上升趋势，如图 3.1 所示。

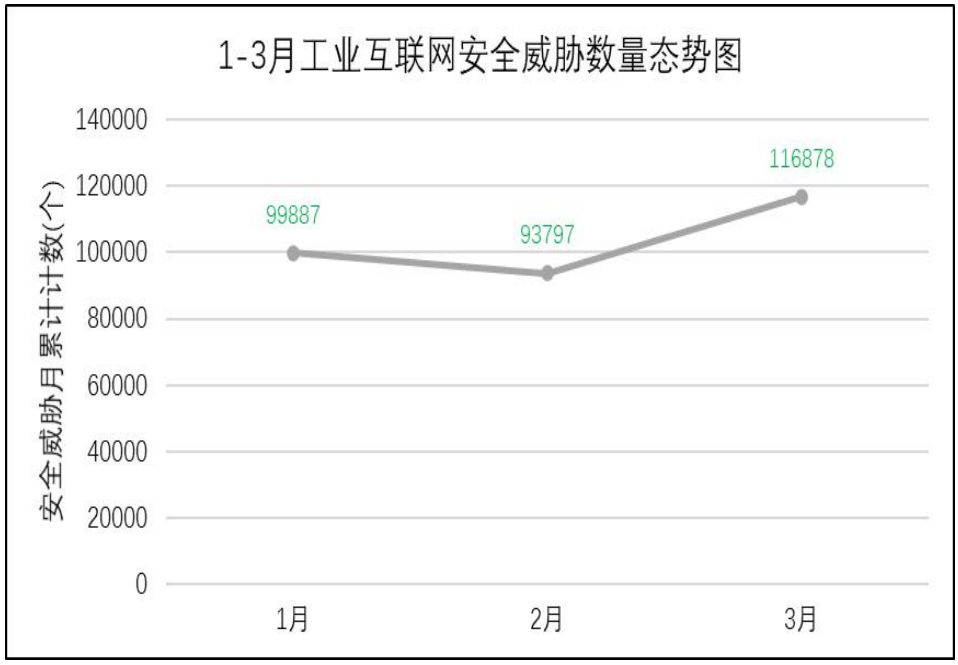


图 3.1　1-3 月工业互联网安全威胁数量态势图

本月主要安全威胁类型为 Web 攻击、木马后门、命令执行、异常流量、漏洞利用，其中 Web 攻击次数达到 67851 次，占比为 58%，安全威胁类型分布情况如图 3.2 所示。

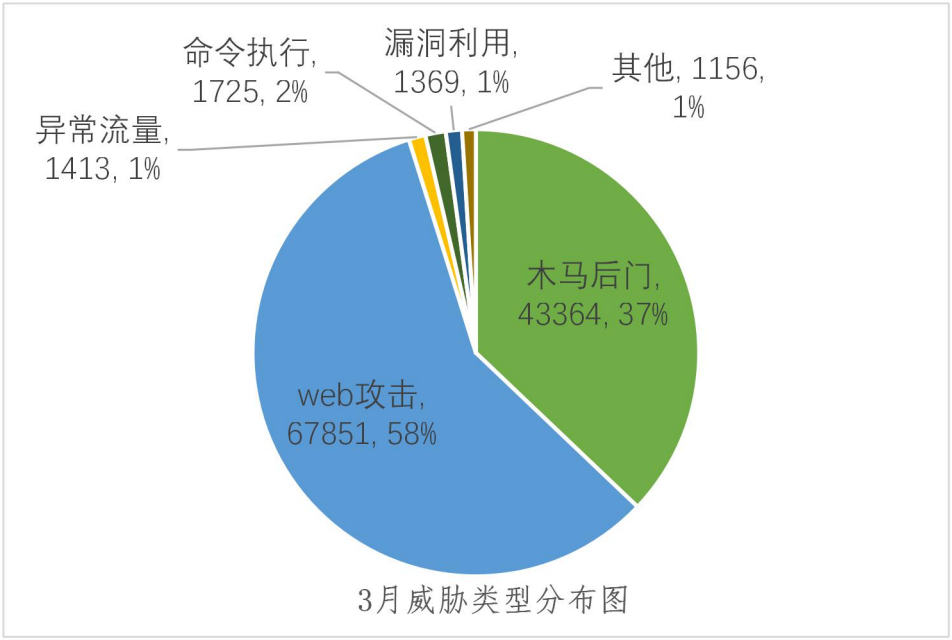


图 3.2 安全威胁类型分布图

从安全威胁类型角度进行分析，2-3 月各类威胁数量均呈现上升趋势。其中 Web 攻击数量最大，达到 67851 起；增长幅度最大的为异常流量，增长幅度达到 83.75%。本月安全威胁类型 top5 及环比变化情况如图 3.3 所示。

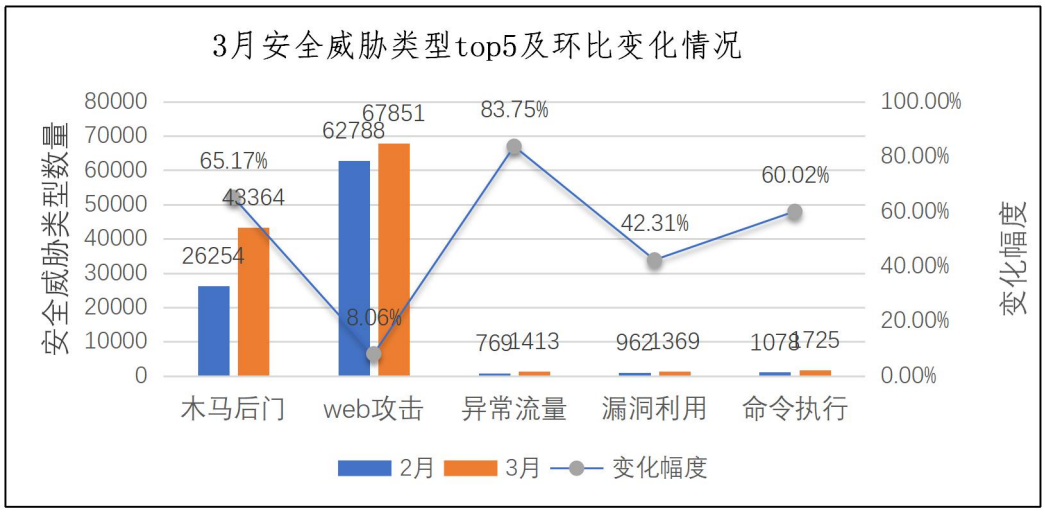


图 3.3 3 月安全威胁类型 top5 及环比变化情况

2. 工业设备安全漏洞情况

截止 2021 年 3 月，平台累计监测发现我省工业互联网安全

漏洞 189649 个，其中高危漏洞 34576 个，占比 18.23%，中危漏洞 151261 个，占比 79.76%，低危漏洞 3812 个，占比 2.01%。

漏洞设备类型主要分布在数据传输模块（DTU）、MySQL、电子设备等，占总漏洞设备的 80%左右。漏洞设备类型分布如图 3.4 所示。

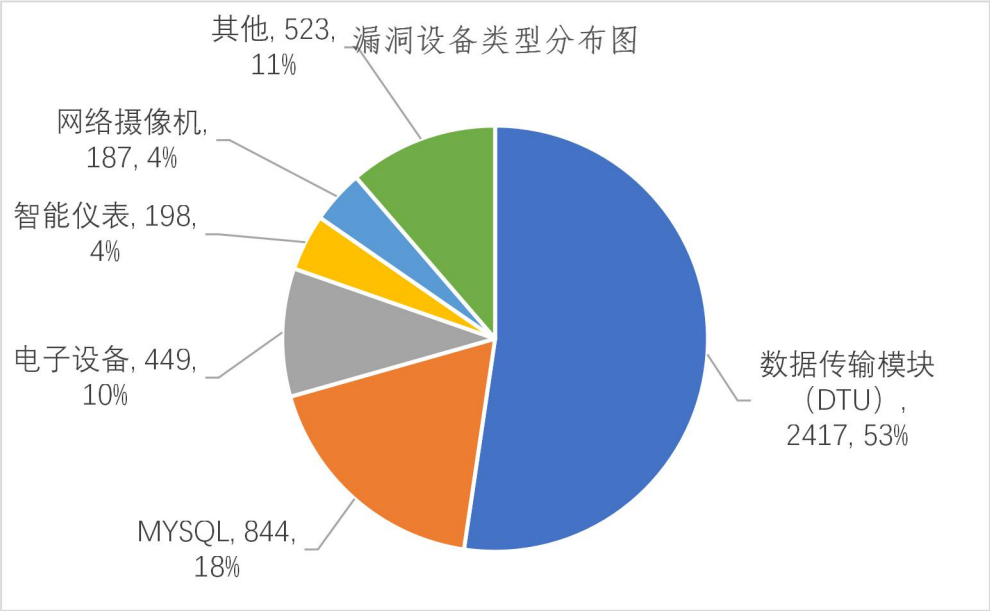


图 3.4 漏洞设备类型分布图

截至 2021 年 3 月，监测到我省企业设备高危漏洞 34576 个，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 69.58%。涉及的漏洞类型分布如图 3.5 所示：

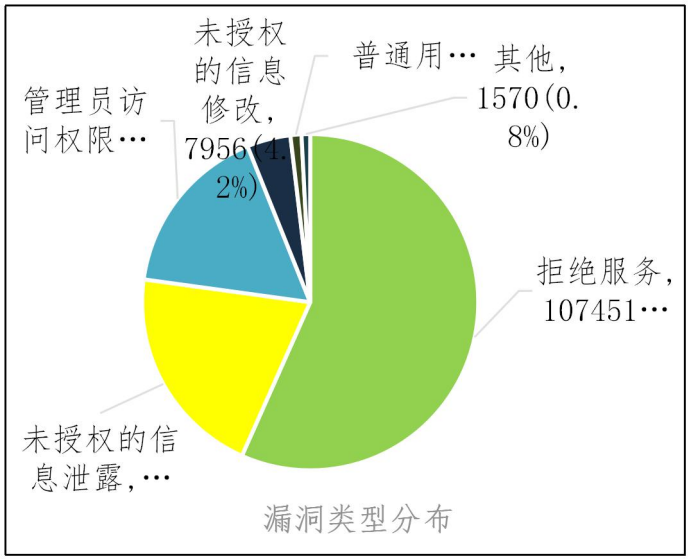


图 3.5 应用程序漏洞类型分布图

3. 行业安全态势分析

2021 年 3 月监测发现针对我省汽车制造业的网络攻击行为 9398 次，较 2 月环比增加 81.29%，为本月被攻击次数最多的行业。与上月相比，化学原料和化学制品制造业，酒、饮料和精制茶制造业，计算机、通信和其他电子制造业，非金属矿物制品业受攻击次数明显下降，2 月、3 月我省重点行业受攻击次数环比变化情况如图 3.6 所示。

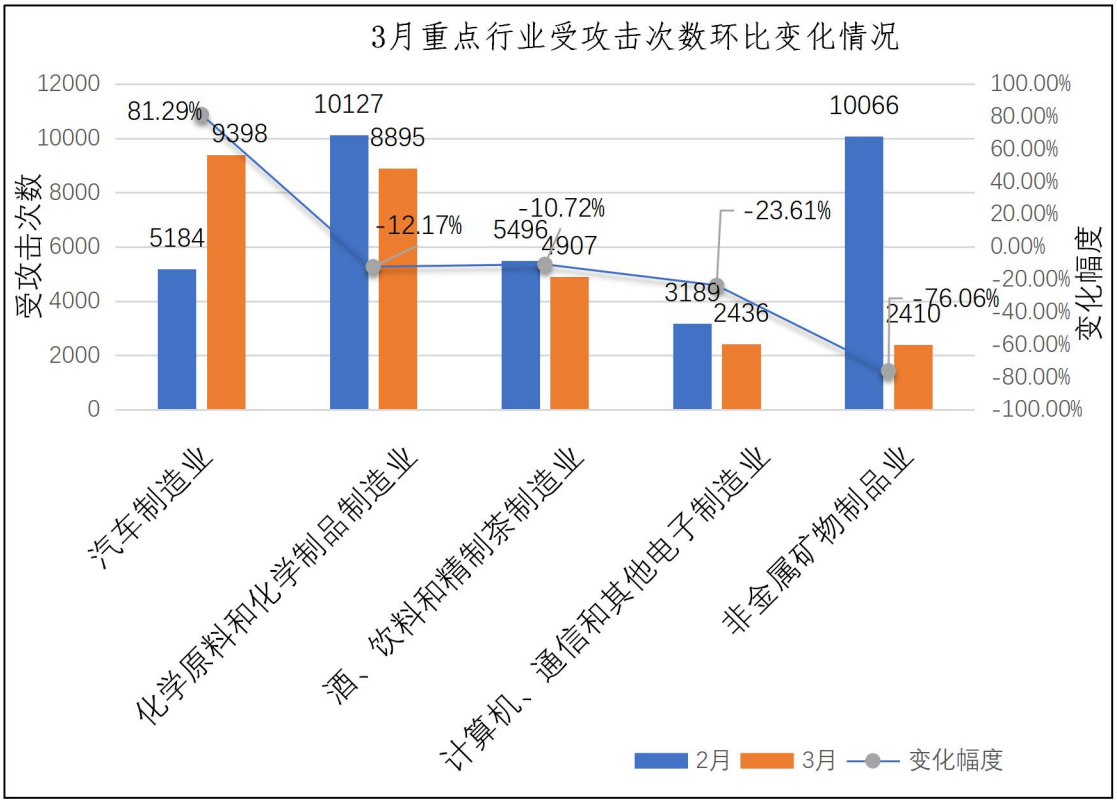


图 3.6 重点行业受攻击次数环比变化情况

4. 地域安全态势分析

2021 年 3 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 108676 次，各地市受网络攻击次数排名情况如图 3.7 所示。

图 3.7 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 334 个，主要集中在成都、德阳、绵阳，占全省被攻击主机的 95.80%，重点地市受攻击主机数量环比变化情况如图 3.8 所示。

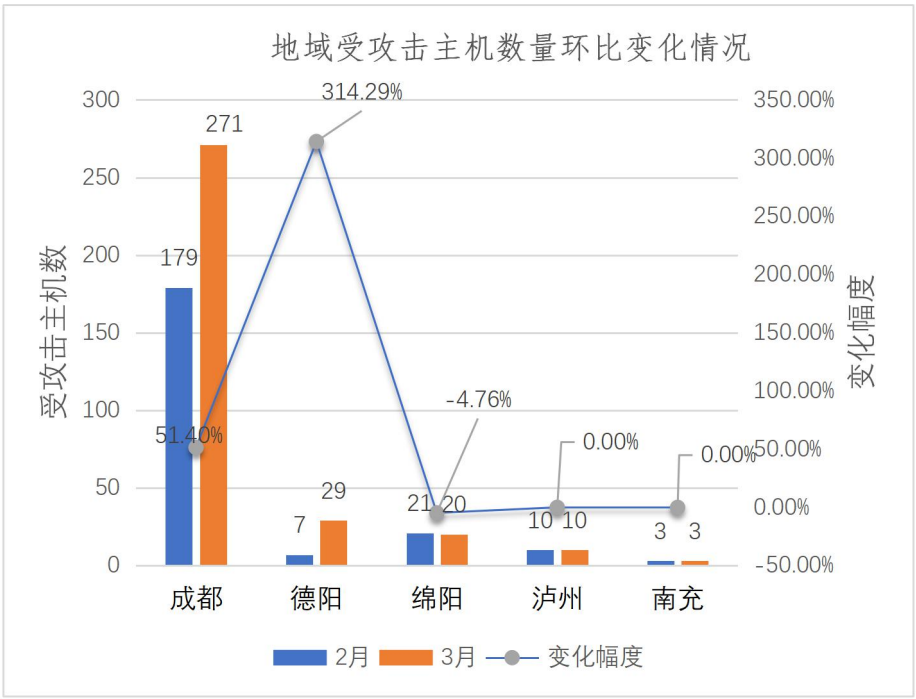


图 3.8 地域受攻击主机数量变化情况

四、 重要网络安全威胁预警

1．CNVD 发布 VMware 多款产品存在远程代码执行漏洞的安全公告

2 月 24 日，国家信息安全漏洞共享平台（CNVD）收录了 VMwarevCenterServer 远程代码执行漏洞（CNVD-2021-12322，对应 CVE-2021-21972）、VMwareESXiOpenSLP 堆溢出漏洞（CNVD-2021-12321，对应 CVE-2021-21974）。攻击者利用上述漏洞，可在未授权的情况下远程执行代码。目前，部分漏洞细节和利用代码已公开。根据 VMware 公司发布的漏洞安全公告，VMware 多个组件存在远程代码执行、堆溢出漏洞和信息泄露漏洞的高危漏洞。1）VMwarevCenterServer 远程代码执行漏洞。未经身份验证的攻击者利用该漏洞，通过向目标主机的 443 端口发送恶意构造请求，写入后门文件，进而在 vCenterServer 的操作系统上实现远程代码执行。2）VMwareESXiOpenSLP 堆溢出漏洞。与 ESXi 宿主机处于同一网段、未经身份验证的攻击者利用该漏洞，通过向目标主机的 427 端口发送恶意构造请求，触发 OpenSLP 服务基于堆的缓冲区溢出，导致远程代码执行。经综合技术研判，上述漏洞的威胁程度高，范围广，CNVD 对上述漏洞的综合评级为“高危”。目前，VMware 公司已发布新版本修复上述漏洞，CNVD 建议用户立即升级至最新版本。

2.CNVD 发布关于 MicrosoftExchangeServer 存在多个高危漏洞的安全公告

2021 年 3 月 4 日，国家信息安全漏洞共享平台（CNVD）收

录了 MicrosoftExchangeServer 远程代码执行漏洞（CNVD-2021-14768、CNVD-2021-14769、CNVD-2021-14770，对应 CVE-2021-26854、CVE-2021-26412、CVE-2021-27078）、MicrosoftExchangeServer任意文件写入漏洞(CNVD-2021-14810、CNVD-2021-14811，对应 CVE-2021-27065、CVE-2021-26858）、MicrosoftExchangeServer 反序列化漏洞（CNVD-2021-14812，对应 CVE-2021-26857）、MicrosoftExchangeServer 请求伪造漏洞（CNVD2021-14813，对应 CVE-2021-26855）。攻击者综合利用上述漏洞，可在未授权的情况远程执行代码。目前，部分漏洞细节已公开。微软公司已发布了关于 Exchange 服务的紧急安全更新，修复了 7 个相关漏洞：1）Exchange 服务端请求伪造漏洞（CVE-2021-26855）：未经授权的攻击者利用该漏洞，可发送任意 HTTP 请求并通过 Exchange 服务身份验证。2）Exchange 反序列化漏洞（CVE-2021-26857）：具有管理员（administrator）权限的攻击者利用该漏洞通过发送恶意请求，实现在 Exchange 服务器上以 SYSTEM 身份的任意代码执行。该漏洞单独利用须具备较高的前提条件。3）Exchange 任意文件写入漏洞（CVE2021-26858/CVE-2021-27065）：经过 Exchange 服务身份验证的攻击者，利用该漏洞，可实现对服务器的任意目录文件写入。4）Exchange 远程代码执行漏洞（CVE-2021-26412/CVE-2021-26854/CVE2021-27078）：攻击者利用此漏洞，可获得目标服务器的权限，最终在服务器上的任意代码执行。经综合技术研判，上述漏洞的威胁程度高，范围广，

CNVD 对上述漏洞的综合评级为“高危”。目前，微软公司已发布新版本修复上述漏洞，CNVD 建议用户立即升级至最新版本，避免印发漏洞相关的网络安全事件。