四川省公共互联网网络安全态势分析通报
(2020 年 8 月)

目录

一、本月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

四川互联网应急中心通过对省内网络流量的持续监测，2020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15.58Tbps。

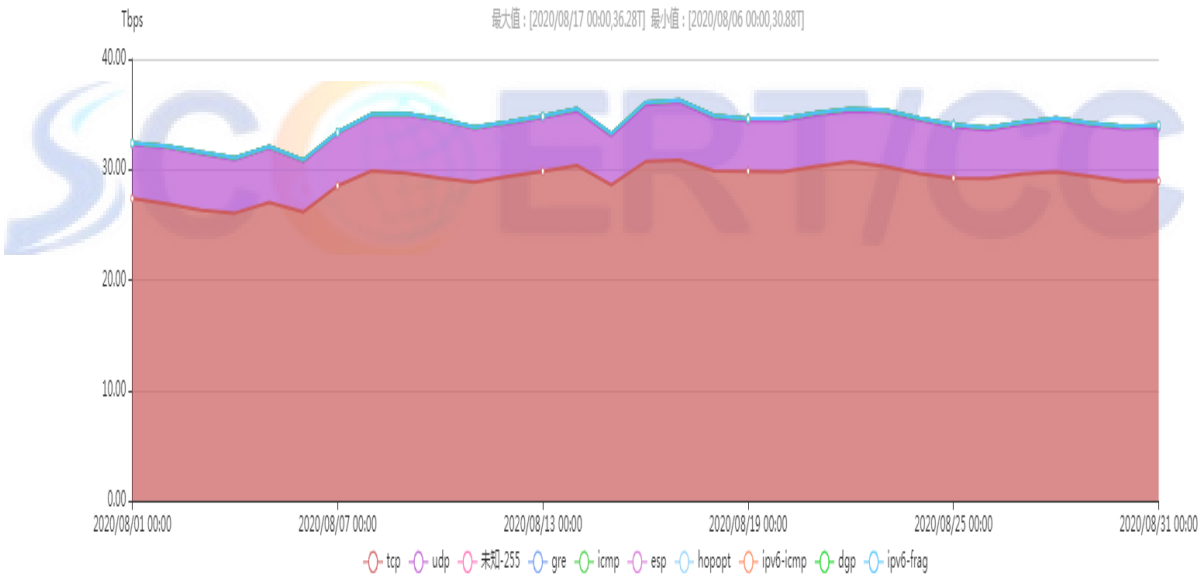

图1.1 2020年8月四川省内流量监测情况

1.2 访问省内网站流量地域分布情况

四川互联网应急中心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。

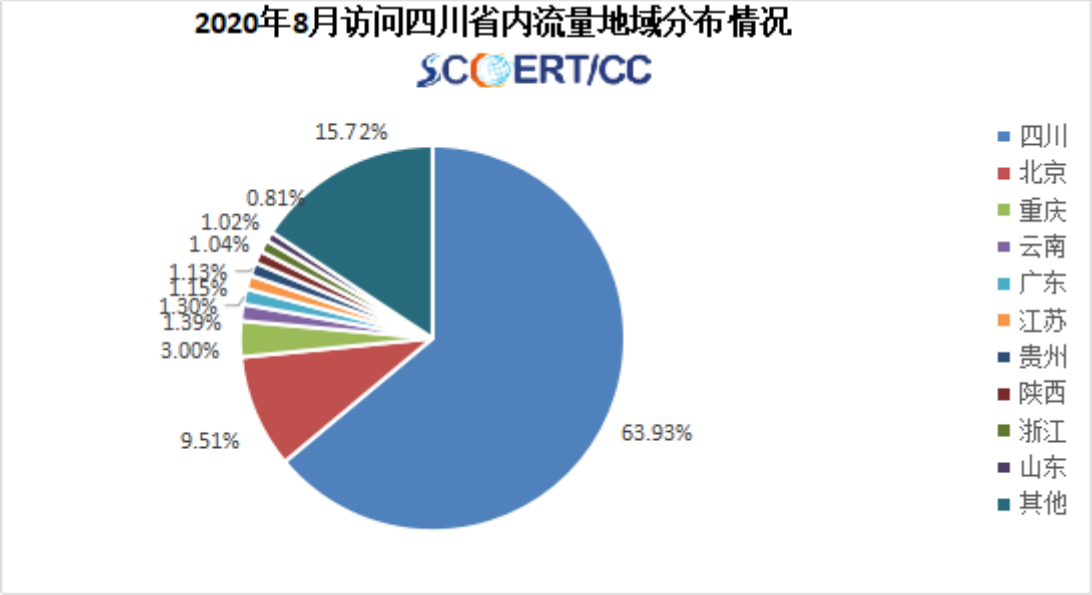

图 1.2 2020 年 8 月访问四川省内流量地域分布情况

2. 省内互联网用户访问协议情况

四川互联网应急中心通过对省内骨干网路由器传输协议的持续监测，2020 年 8 月四川省内互联网用户访问网络的协议前八位占比情况如图 1.3 所示，排名前三的协议分别为 tcp、udp、gre。

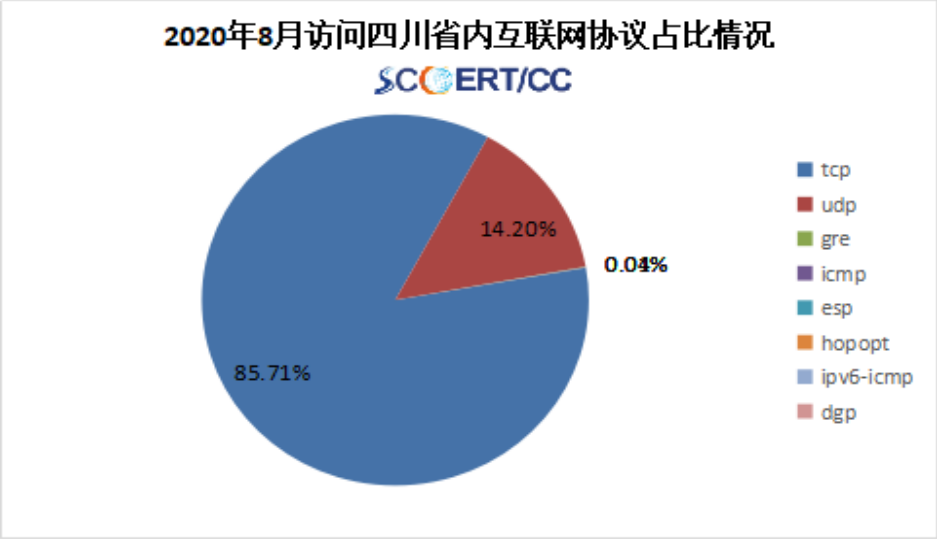

图 1.3 四川省内路由器协议占比情况

3. 省内互联网用户访问域名分布情况

2020 年 8 月，四川互联网应急中心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。

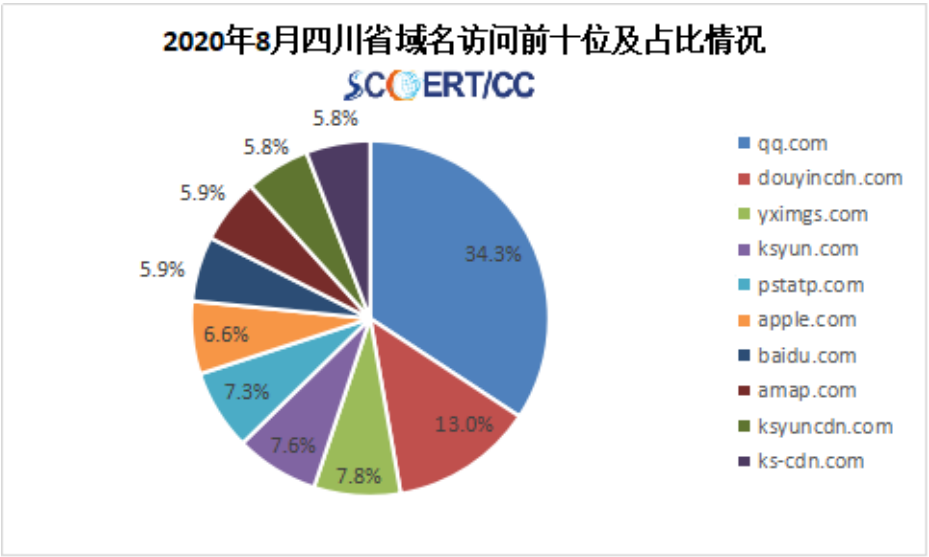

图 1.4 四川省内域名访问情况

二、本月网络安全基本态势

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，感染僵尸木马事件、网站后门事件数量有所上升，飞客蠕虫、网页篡改事件数量有所下降。

1.木马、僵尸网络

四川省本月有 111,448 个 IP 地址对应的主机被木马或僵尸程序控制，环比上升 36.77%。2019 年 12 月-2020 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。

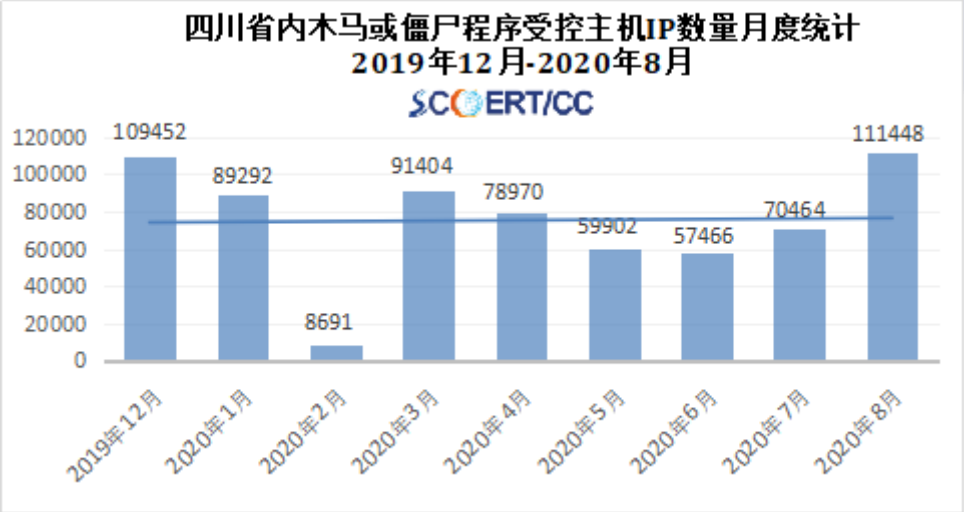

图 2.1 四川省木马或僵尸程序受控主机 IP 数量月度分布图

四川省本月有 9,648 个 IP 地址存在木马或僵尸程序控制服务器，环比上升 20.97%。2019 年 12 月-2020 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。

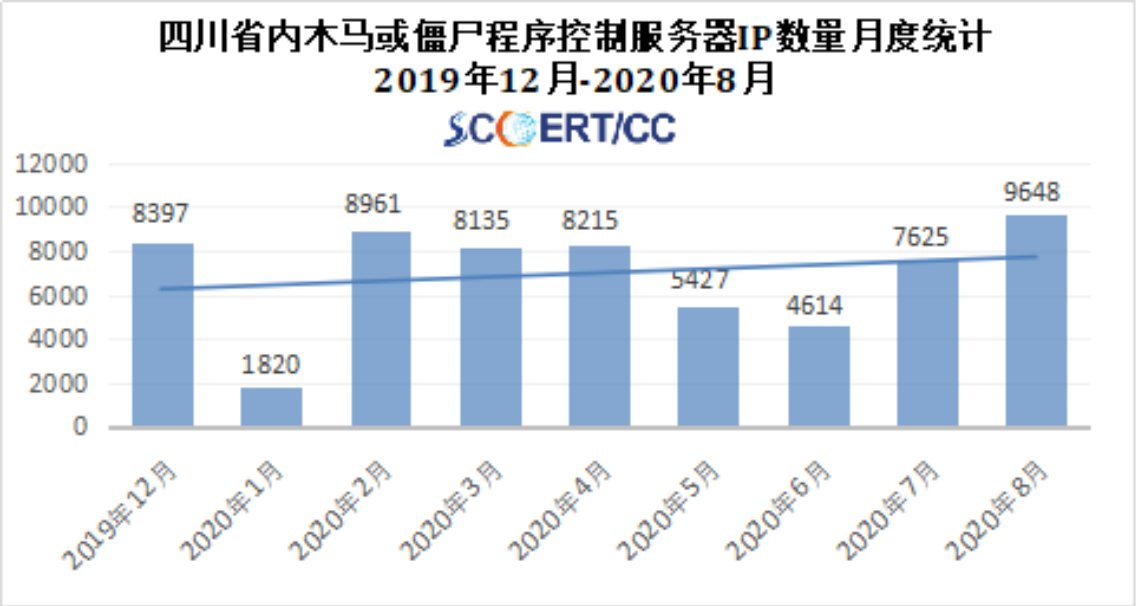

图 2.2 四川省木马或僵尸程序控制服务器 IP 数量月度分布图

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、乐山、广安，其中成都数量最多，有 59,772 台主机感染僵尸木马。

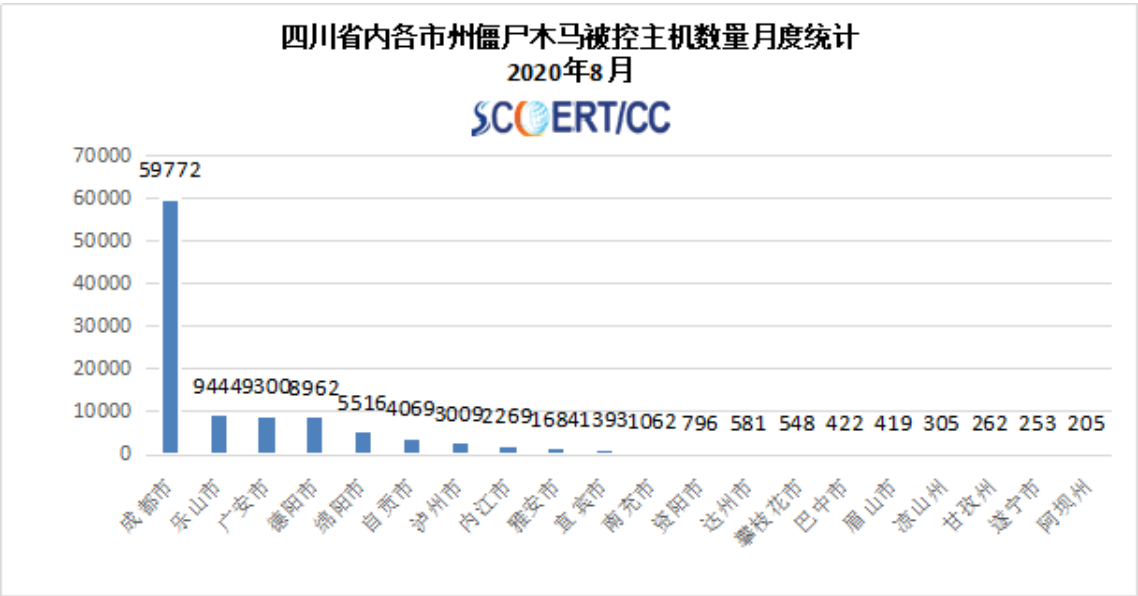

图 2.3 四川省内各市州主机感染僵尸木马主机数量分布

2.飞客蠕虫

四川省本月有 7,204 个 IP 地址对应的主机感染“飞客”蠕虫，环比下降 18.14%，数量略有减少，2019 年 12 月-2020 年 8 月分布如图 2.4 所示，本月大幅下降。

图 2.4 四川省感染“飞客”蠕虫的主机对应 IP 数量月度分布图

四川省本月各市州主机感染“飞客”蠕虫比例如图 2.5 所示，前三位依次为成都、绵阳、德阳，其中成都数量最多，有 4,325 台主机感染飞客蠕虫。

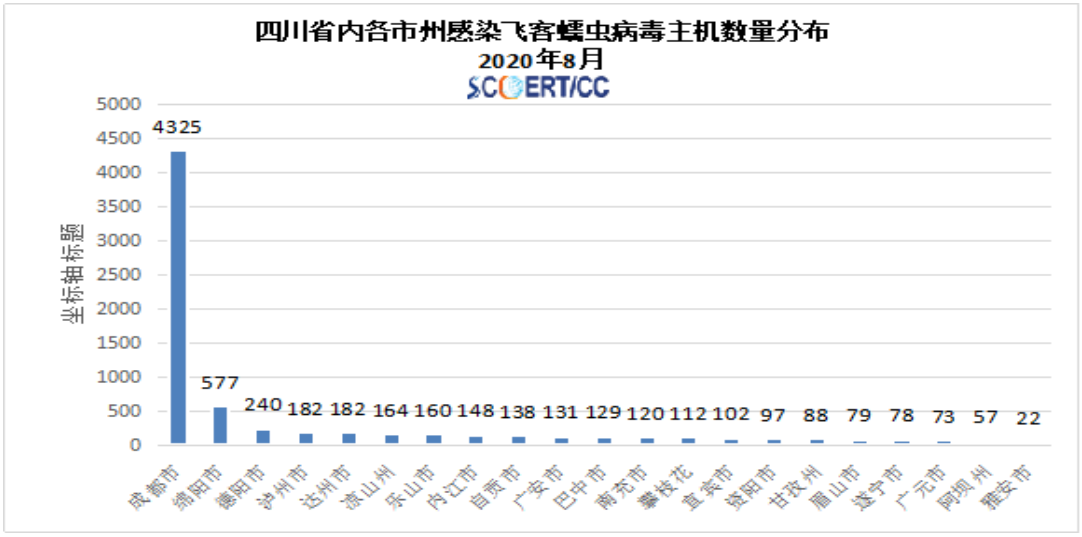

图 2.5 四川省内各市州主机感染飞客蠕虫病毒主机数量分布

3.网页篡改

本月，主机位于四川地区的被篡改网站月均数量为 589 个，环比下降 33.82%。2019 年 12 月-2020 年 8 月，四川省内被篡改网站数量月度分布如图 2.6 所示，整体呈下降趋势。

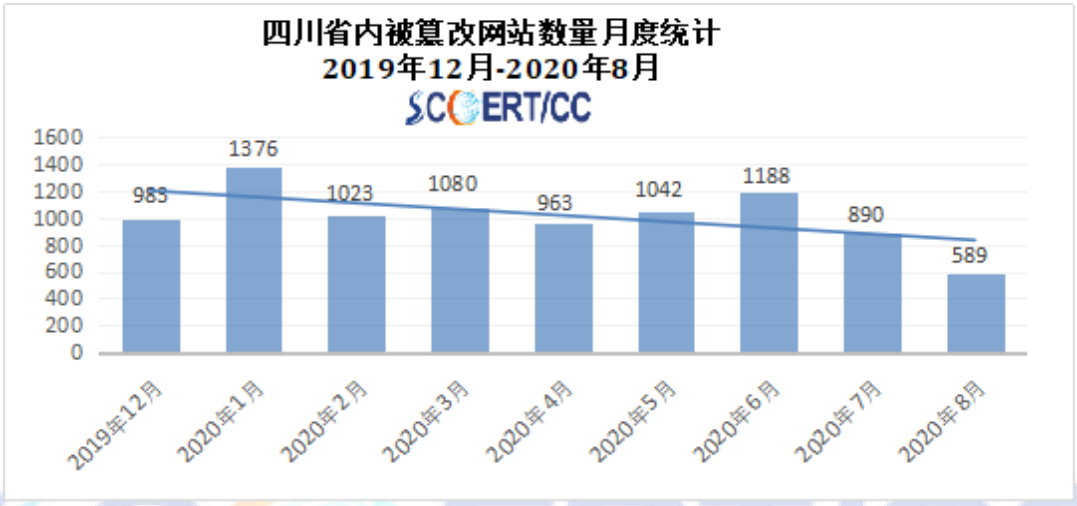

图 2.6 四川省被篡改网站数量月度分布图

四川省本月各市州网站网页篡改数量比例如图 2.7 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 455 个。

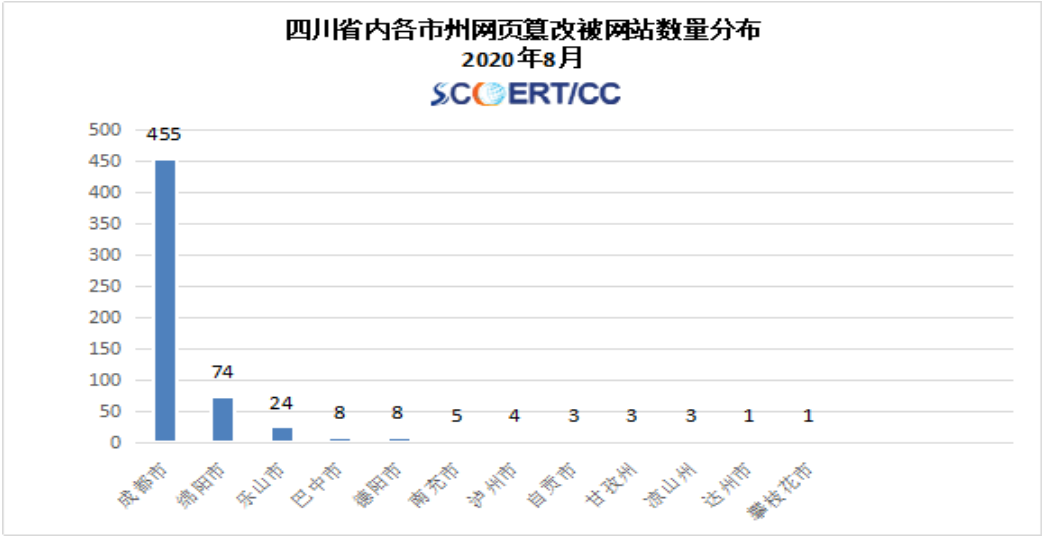

图 2.7 四川省内各市州网页篡改被网站数量分布

4.网页后门

主机位于四川省被植入 517 个，环比上升 0.1%。2019 年 12 月-2020 年 8 月，四川省内被植入后门网站月度分布情况如图 2.8 所示，整体呈下降趋势。

图 2.8 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 2.9 所示，前三位依次为成都、绵阳、乐山，其中成都数量最多，达 313 个。

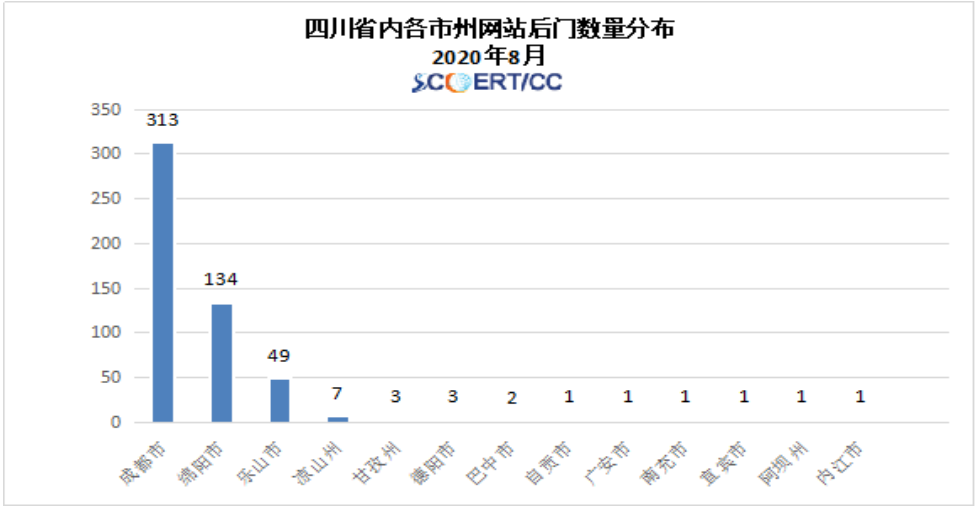

图 2.9 四川省被植入后门的网站主机数量月度分布图

三、重要网络安全威胁预警

1. 工信部通报下架 8 款侵害用户权益 APP

8 月 19 日，工信部网站发布关于下架侵害用户权益 App 名单的通报.通报显示，7 月 24 日，工信部通报了 58 家存在侵害用户权益行为 APP 企业的名单。截至目前，尚有 8 款 APP 未按要求限时完成整改，依相关法规，工信部组织对上述 APP 进行下架处理。工信部表示，相关应用商店应在本通报发布后，立即组织对名单中应用软件进行下架处理。

2. 全球最大邮轮运营商嘉年华公司遭遇勒索软件攻击

8 月 17 日，据“ZDNet”网站消息，当日，全球最大的游轮运营商嘉年华公司披露了一个系统安全漏洞，并承认 8 月 15 日遭遇勒索软件攻击。攻击者“访问并加密了公司某品牌部分信息技术系统”，并下载了相关文件。目前，该公司已就此事通知了执法部门，并与法律顾问和事故应对专业人员进行了接触。尽管可能面对潜在的诉讼，但预计事件不会对公司“业务、运营或财务业绩”产生实质性影响。嘉年华并未透露事件具体细节，比如加密其网络的勒索软件名称，或者受影响的内部网络或品牌。

3. FritzFrog 僵尸网络正通过 SSH 感染 Linux 服务

8 月 20 日，据 Freebuf 网站消息，研究人员发现了一个名为 FritzFrog 的先进的 P2P 僵尸网络，该僵尸网络自 2020 年 1 月以来一直积极地瞄准全球的 SSH 服务器，其中，北美、中国、

韩国是重灾区。据悉，该僵尸网络用 Golang 语言编写，具有可蠕虫功能，主要瞄准政府、教育和金融部门的实体。作为一种模块化、多线程、无文件的 SSHInternet 蠕虫，FritzFrog 通过破坏公共 IP 地址来发展 P2P 僵尸网络。此外，为了避免被检测，FritzFro 的进程是以 ifconfig 和 nginx 名称运行，然后侦听端口 1234 以等待命令。攻击者通过 SSH 连接到受感染的计算机，然后在计算机上运行一个 netcat 客户端，再将其连接到恶意软件的服务器。最后，通过 SSH 发送的 ant 命令将用作 netcat 的输入，并重定向到恶意软件。根据专家的说法，该僵尸网络自 1 月 9 日以来一直处于活跃状态，已累计使用 20 种不同版本的恶意软件二进制文件进行了 13000 次攻击。

4. 2020 中国网络安全年会在网上成功召开

8 月 12 日，以“并肩应对威胁挑战”为主题的 2020 中国网络安全年会在网上成功召开。本届中国网络安全年会由国家互联网信息办公室指导，国家计算机网络应急技术处理协调中心（CNCERT/CC）主办，天融信、启明星辰、长安通信、恒安嘉新、安天、阿里云、奇安信、深信服、安恒、亚信安全联合主办，中国通信学会通信安全技术委员会协办。中央网络安全和信息化委员会办公室副总工程师、国家计算机网络应急技术处理协调中心主任李湘宁致欢迎辞。中国工程院院士邬贺铨、邬江兴、张平作主旨报告，工业和信息化部网络安全管理局副局长张新，公安部

十一局巡视员、副局长、总工程师郭启全致辞。此外，奇安信集团董事长齐向东，安天科技集团股份有限公司董事长、首席架构师肖新光，杭州安恒信息技术股份有限公司董事长、总裁范渊，天融信科技集团首席执行官李雪莹，亚信安全总裁陆光明，长安通信科技有限责任公司常务副总裁陈训逊，恒安嘉新（北京）科技股份公司首席执行官陈晓光，阿里巴巴副总裁刘松，启明星辰集团合伙人、高级副总裁、网御星云公司总裁胡晓峰，深信服科技股份有限公司副总裁、核心战略负责人马程也围绕网络安全热点问题分享了精彩观点。今年，2020 中国网络安全年会首次以网上方式举办，大会还设置了“5G 时代的万物互联与安全挑战”“新基建—工业互联网安全”“网络安全态势感知”“5G 的数字能力与安全”“新基建新安全”“5G 安全论坛”等共 6 个主题分论坛。经过 16 年的发展，一年一度的“中国网络安全年会”已成为国内网络安全领域的重要会议，得到政府有关部门、互联网企业、重要信息系统单位和广大互联网用户的广泛关注，是国内网络安全“产、学、研、用”各界进行技术业务交流的重要桥梁和纽带，对于推动我国网络安全工作、提高社会网络安全意识起到了积极作用。

5.《2019 年中国互联网网络安全报告》发布

8 月 11 日，CNCERT 编写的《2019 年中国互联网网络安全报告》正式发布。自 2008 年起，CNCERT 持续编写发布中国互联网

网络安全年度报告，依托 CNCERT 多年来从事网络安全监测、预警和应急处置等工作的实际情况，对我国互联网网络安全状况进行总体判断和趋势分析，具有重要的参考价值。该系列报告为政府部门提供监管支撑，为互联网企业提供运行管理技术支持，向社会公众普及互联网网络安全知识，对提高全社会、全民的网络安全意识发挥积极作用。《2019 年中国互联网网络安全报告》汇总分析了 CNCERT 自有网络安全监测数据和 CNCERT 网络安全应急服务支撑单位报送的数据，具有重要的参考价值，内容涵盖我国互联网网络安全态势分析、网络安全监测数据分析、网络安全事件案例详解、网络安全政策和技术动态等多个方面。其中，报告对计算机恶意程序传播和活动、移动互联网恶意程序传播和活动、网站安全监测、DDoS 攻击监测、安全漏洞预警与处置、网络安全事件接收与处理等情况进行深入细致的分析，并对 2019 年的典型网络安全事件进行专题介绍。此外，报告对国内网络安全组织发展情况和 CNCERT 举办的国内外重要活动等进行了总结。最后，报告对 2020 年网络安全热点问题进行预测。

6. 关于防范黑客通过仿冒“ETC 在线认证”网站实施网络诈骗的风险提示

近期，CNCERT 监测发现互联网上出现大量仿冒“ETC 在线认证”网站的钓鱼页面。诈骗分子通过此类钓鱼网站，诱骗获取用户的真实姓名、银行卡账号、身份证号、银行预留手机号、取款

密码等个人隐私信息，从而盗取资金。请广大网民强化风险意识，加强安全防范，避免不必要的经济损失，主要建议包括：（1）要仔细核对网址，如北京市 ETC 的官方网站为 https://www.bjetc.cn/；（2）不要轻易打开来历不明的网址链接；（3）据悉 ETC 官方近期没有在线验证要求，如有业务办理方面的疑惑，可及时联系当地 ETC 网点进行咨询；（4）不轻易提供自己的银行卡号、取款密码、身份证号等重要隐私信息。