四川省公共互联网网络安全态势分析通报
(2020 年 9 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9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35.30Tbps。

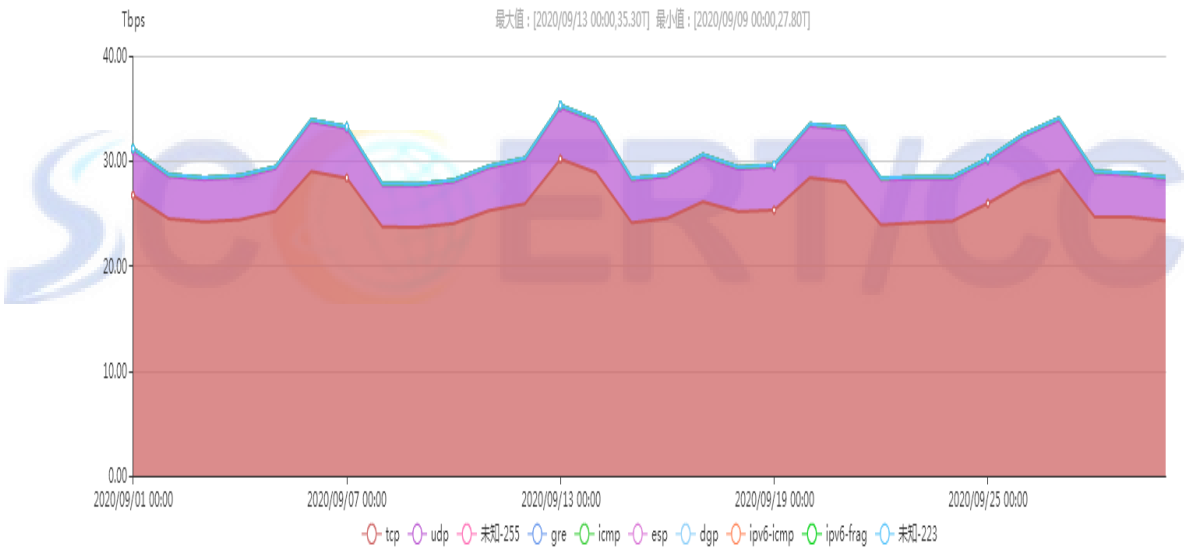

图 1.1 2020年9月四川省内流量监测情况

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。

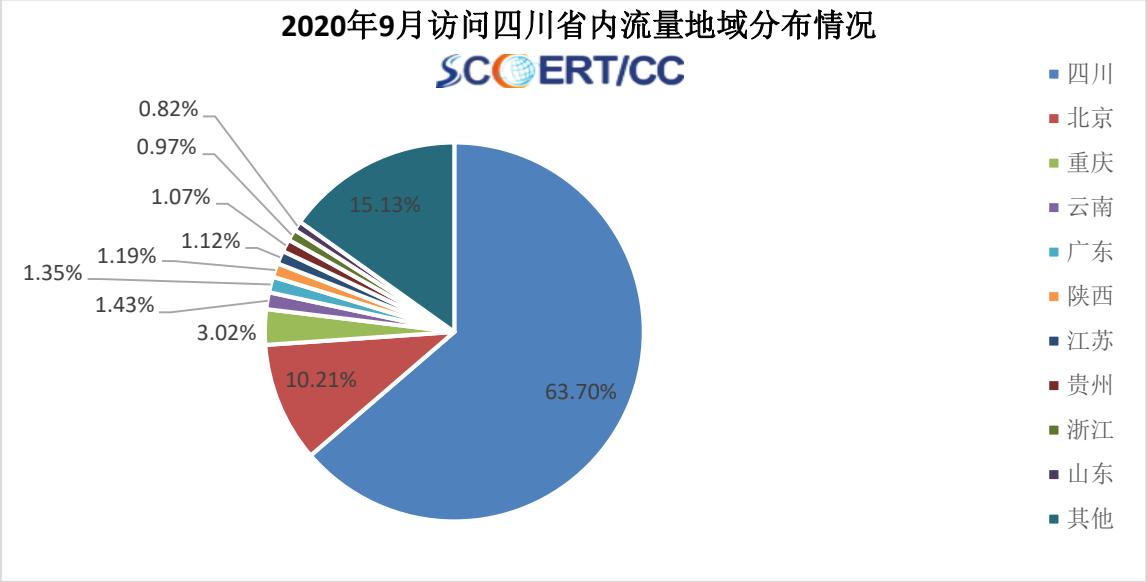

图 1.2 2020 年 9 月访问四川省内流量地域分布情况

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 9 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。

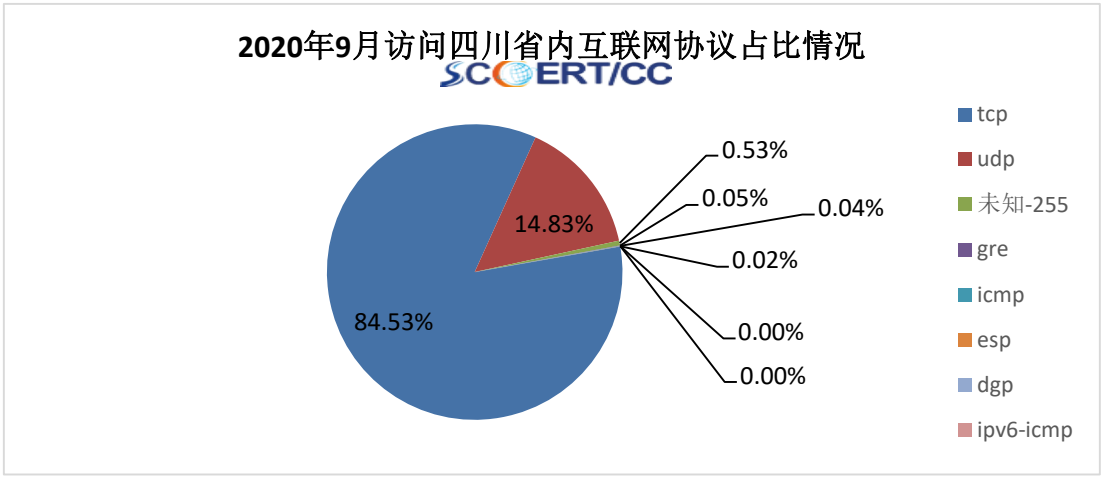

图 1.3 四川省内路由器协议占比情况

3. 省内互联网用户访问域名分布情况

2020 年 9 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综合服务、短视频、云服务类等，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、金山等大型互联网企业榜上有名。

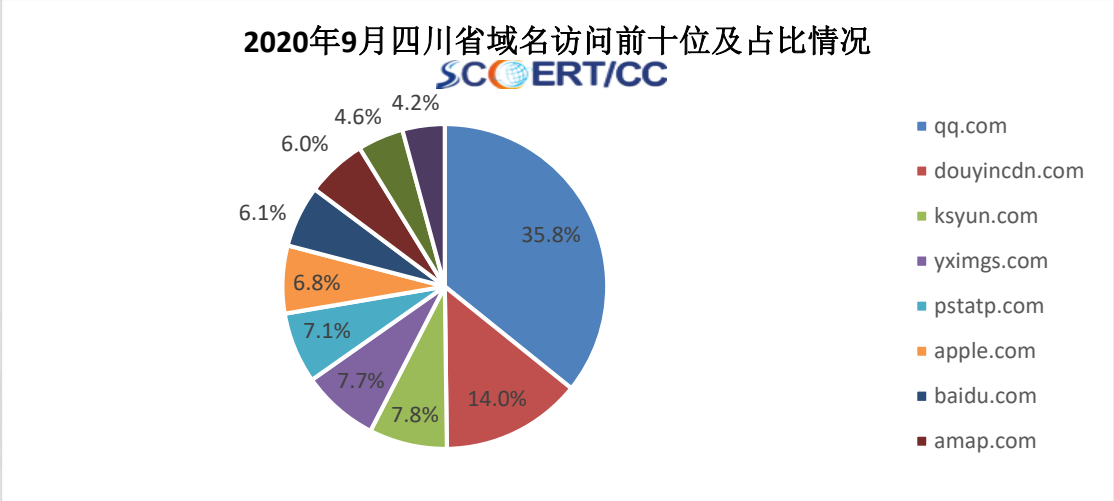

图 1.4 四川省内域名访问情况

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，未发生较大的网络安全事件。在公共互联网网络安全环境方面，除感染僵尸木马事件、飞客蠕虫、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 122371 个 IP 地址对应的主机被木马或僵尸程

序控制，环比上升 9.80%。2019 年 12 月-2020 年 9 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，整体呈上升趋势。

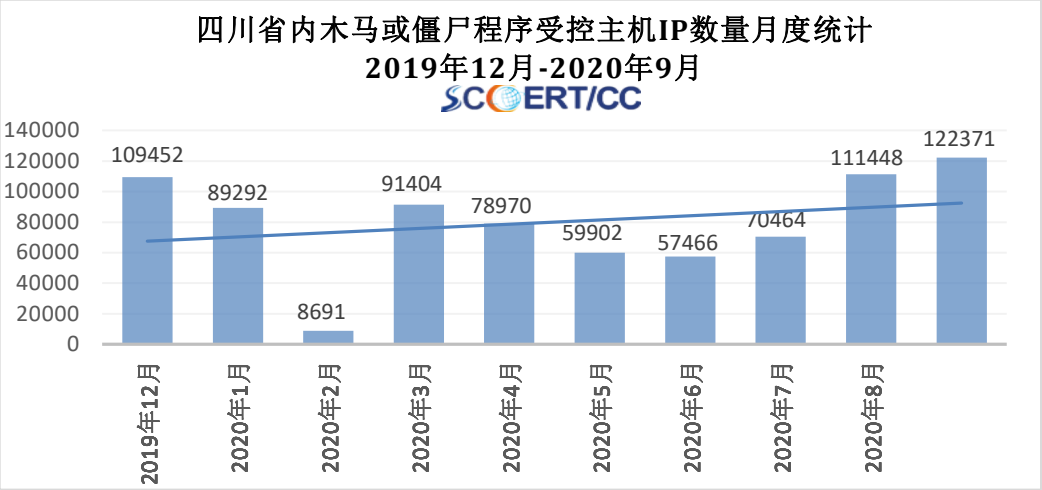

图 2.1 四川省木马或僵尸程序受控主机 IP 数量月度分布图

四川省本月有 8678 个 IP 地址存在木马或僵尸程序控制服务器，环比下降 10.05%。2019 年 12 月-2020 年 9 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，整体呈上升趋势。

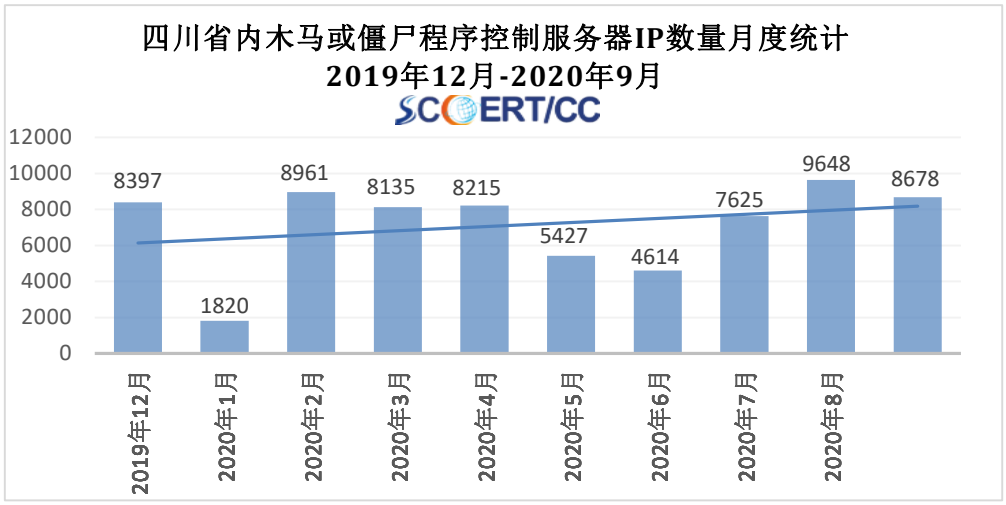

图 2.2 四川省木马或僵尸程序控制服务器 IP 数量月度分布图

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、广安、乐山，其中成都数量最多，有 63747 台主机感染僵尸木马。

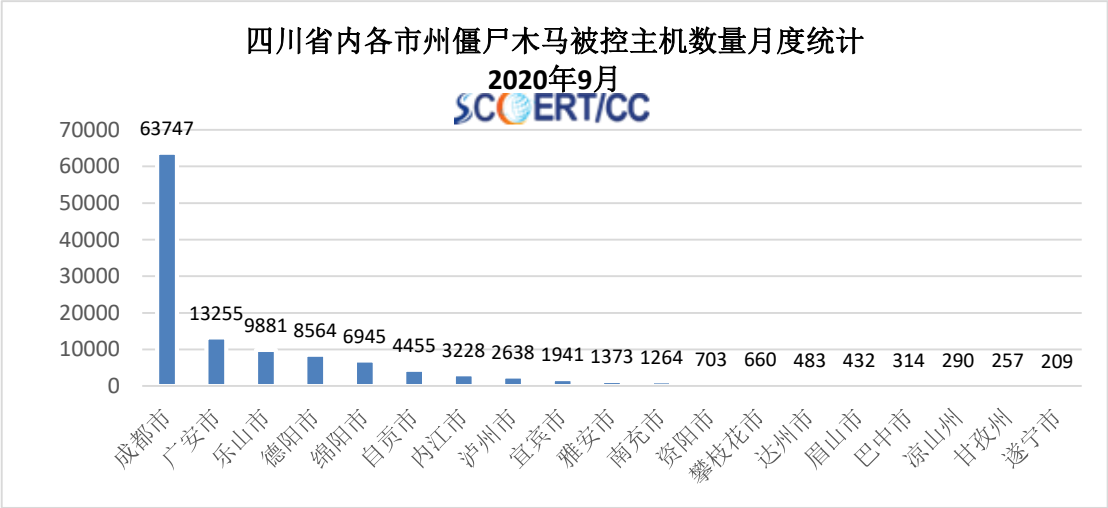

图 2.3 四川省内各市州主机感染僵尸木马主机数量分布

2. 飞客蠕虫

四川省本月有 8434 个 IP 地址对应的主机感染“飞客”蠕虫，环比上升 17.07%，数量大幅增加，2019 年 12 月-2020 年 9 月分布如图 2.4 所示，整体呈下降趋势。

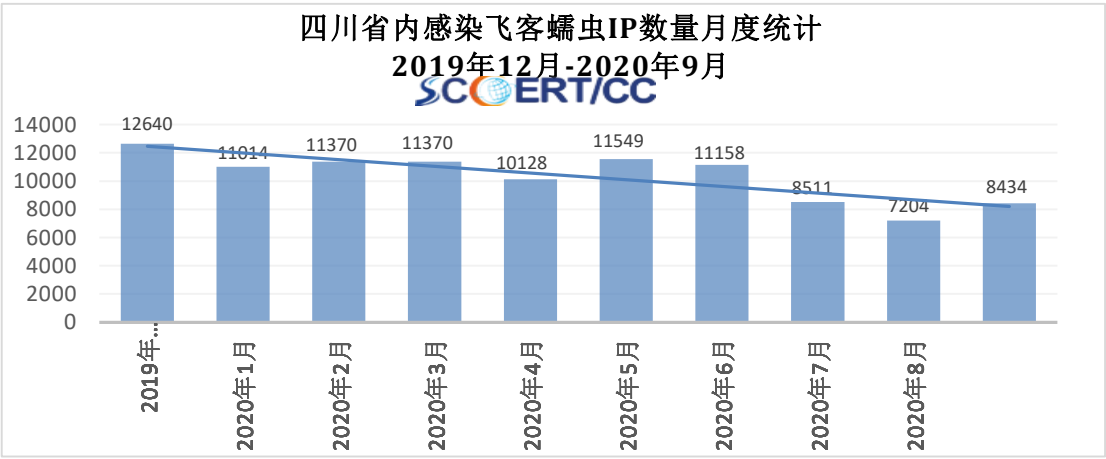

图 2.4 四川省感染“飞客”蠕虫的主机对应 IP 数量月度分布图

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 5136 台主机感染飞客蠕虫。

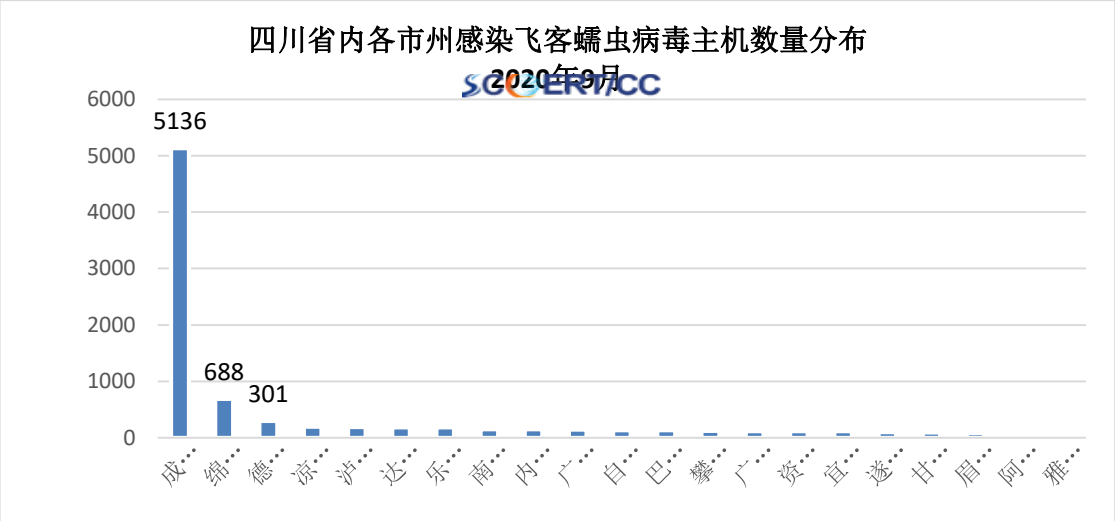

图 2.5 四川省内各市州主机感染飞客蠕虫病毒主机数量分布

3. 网页篡改

本月，主机位于四川地区的被篡改网站数量为 625 个，环比上升 6.11%。2019 年 12 月-2020 年 9 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。

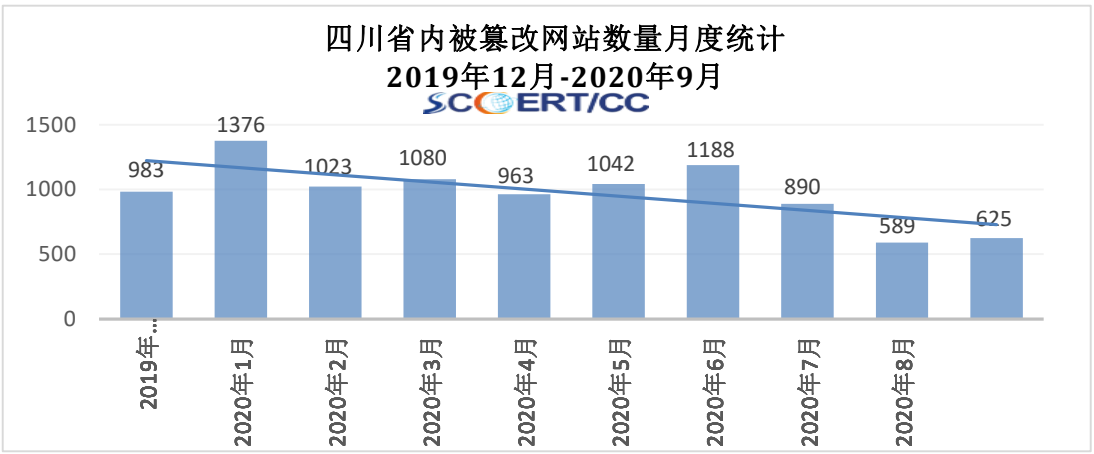

图 2.6 四川省被篡改网站数量月度分布图

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 473 个。

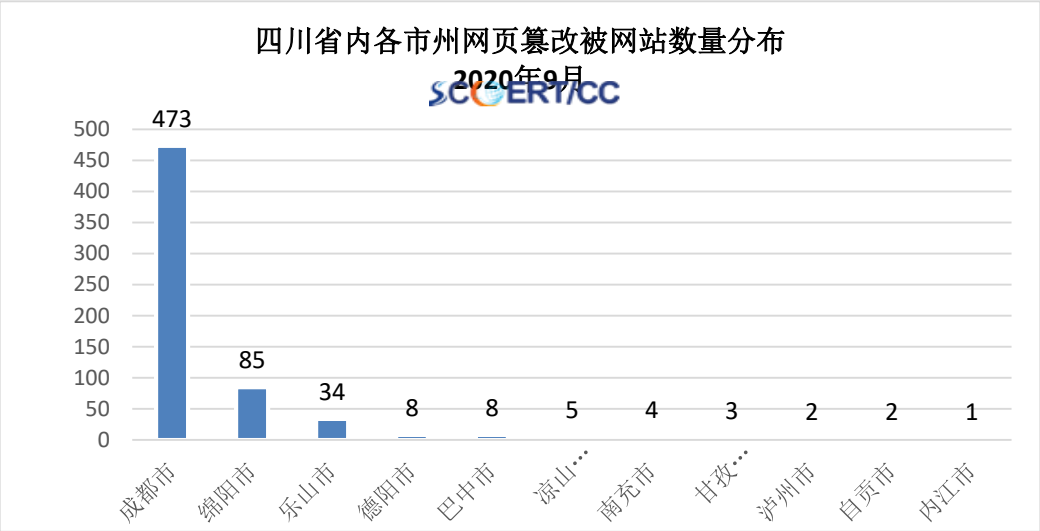

图 2.7 四川省内各市州网页篡改被网站数量分布

4. 网页后门

主机位于四川省内被植入后门网站数为 396 个，环比下降 23.40%。2019 年 12 月-2020 年 9 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。

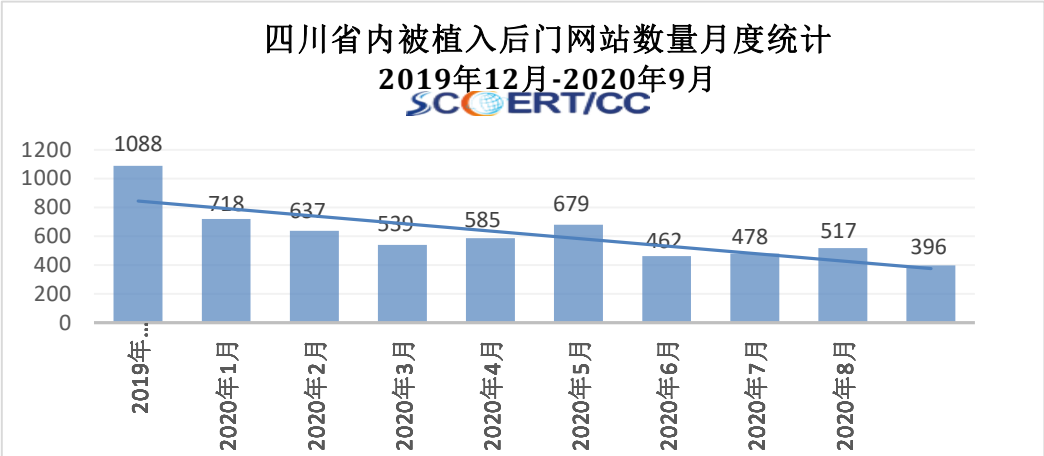

图 2.8 四川省被植入后门的网站主机数量月度分布图

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 255 个。

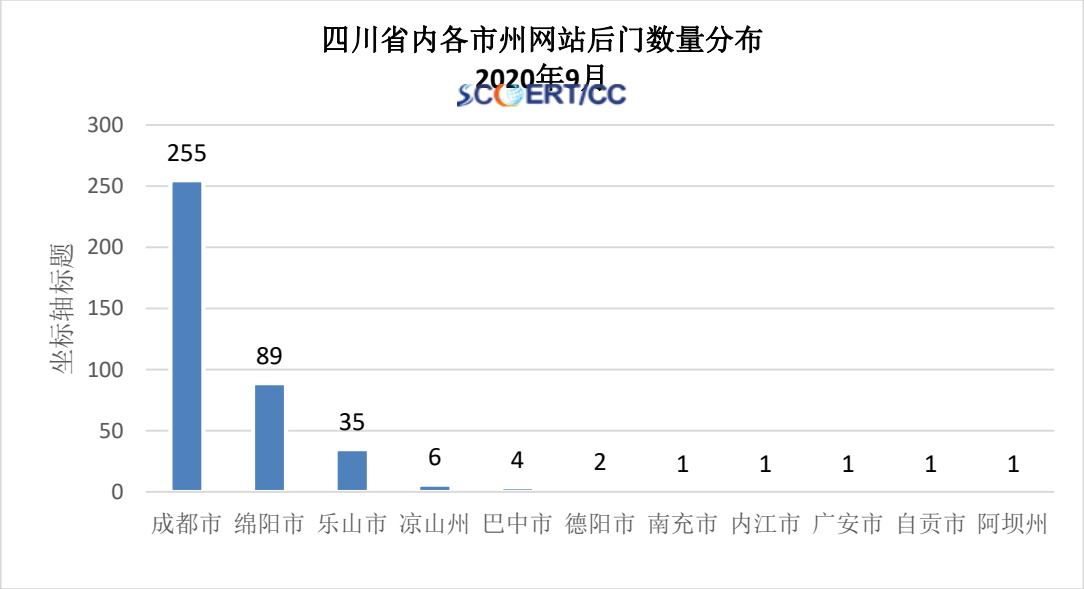

图 2.9 四川省被植入后门的网站主机数量月度分布图

三、重要网络安全威胁预警

1.Visa 发现一款新型信用卡窃取器 能够规避检测并窃取用户卡内数据

9 月 8 日，据外媒报道，Visa 发布了一项关于新的信用卡 JavaScript 窃取器的警告，它被称为 Baka，这种电子窃取器会在窃取银行卡信息后自动从内存中删除，实现了规避检测的新功能。专家在全球多个使用 Visa eTD 功能的商家网站上发现了 Baka 窃取器。Baka 窃取器的工作原理是动态地向远程 JavaScript 文件加载当前页面，添加脚本标记。JavaScript 网址以加密格式硬编码在加载器脚本中，攻击者可以更改每个受害者的网址。据了解，Baka 是第一个使用 XOR 密码对硬编码进行

加密的 JavaScript 窃取恶意软件。

2.Mykings 僵尸网络新变种通过 PcShare 远程控制，已感染超 5 万台电脑挖矿

9 月 11 日，腾讯安全威胁情报中心检测到 Mykings 挖矿僵尸网络变种木马，更新后的 Mykings 会在被感染系统安装开源远程控制木马 PcShare，对受害电脑进行远程控制，可进行操作文件、服务、注册表、进程、窗口等多种资源，并且可以下载和执行指定的程序。Mykings 僵尸网络木马还会关闭 Windows Defender、检测卸载常见杀毒软件；卸载竞品挖矿木马和旧版挖矿木马；下载“暗云”木马感染硬盘主引导记录（MBR)实现长期驻留；通过计划任务、添加启动项等实现开机自动运行等行为。由于 MyKings 僵尸网络主动扩散的能力较强，影响范围较广，对企业用户危害严重。根据推测，Mykings 僵尸网络目前已控制超过 5 万台电脑进行挖矿作业。

3.工信部下架 23 款侵害用户权益 APP

9 月 14 日，工信部在官方网站上发布，23 款 APP 因侵害用户权益且未按要求完成整改被下架，蛋壳公寓、小咖秀、会说话的汤姆猫 2 都在被下架名单中。8 月 31 日，工信部向社会通报了 101 家存在侵害用户权益行为的 APP 企业的名单。截至目前，尚有 23 款 APP 未按要求完成整改，工信部组织对上述 APP 进行下架。相关应用商店应在通报发布后，立即组织对名单中应用软件进行下架处理。

23 款 APP 涉及到购物、租房、游戏、视频等，蛋壳公寓、小咖秀、会说话的汤姆猫 2、安卓读书都在被下架名单范围内。工信部近期加大了对侵害用户权益行为的监管。今年 8 月，VISTA 看天下、蓝舞者、39 互联网医院、乐游、松果文档、大角虫漫画、宜搜 漫画、一米工作等 8 款 APP 也被工信部点名下架，原因同样是未按期完成整改。

4.微软 Bing 应用数据库遭泄露多达 1 亿条搜索记录被截取

9 月 27 日，据外媒报道，WizCase 专家在互联网上搜索敞开的数据库或服务器时发现了一个不受保护的 Elasticsearch 服务器，其中包含了与微软旗下 Bing 移动应用程序用户相关的 TB 级数据。该数据库中的身份验证被移除，其内容暴露给互联网上的所有人。暴露的 6.5 TB 服务器每天接收多达 200G 的数据。WizCase 指出，Bing 移动应用软件仅在谷歌 Play 上就有超过 1000 万的下载量，每天记录数百万次搜索。微软称目前已解决了配置不当问题。

5.CNCERT 发布《2020 年上半年我国互联网网络安全监测数据分析报告》

为全面反映 2020 年上半年我国互联网网络安全状况，CNCERT 对上半年监测数据进行了梳理，9 月 27 日发布了《2020 年上半年我国互联网网络安全监测数据分析报告》。报 告从恶意程序、安全漏洞、拒绝服务攻击、网站安全、云平台安全、工业控制系统安全 六个方面对我国 2020 年上半年网络安全监测

数据情况，对攻击来源、攻击对象、攻击规模等进行了详细梳理，以及时反映我国网络安全整体情况。