山西省网络安全月度通报

2019 年第 12 期（总第 66 期）

山西省通信管理局　　2019 年 12 月

一、基本态势

2019 年 11 月，我省互联网网络安全状况整体评价为良，互联网骨干网各项监测指标正常。本月发现木马或僵尸程序受控主机 15480 台，木马或僵尸程序控制服务器 39 台，感染“飞客”蠕虫病毒主机 3212 台。忻州、临汾、太原排在全省受控木马或僵尸主机活动频繁地区前三位。

（一）基础网络运行安全

11 月，我省基础网络运行总体平稳，未出现造成较大影响的运行故障，未发生三级以上网络安全事件。

（二）公共互联网安全

11 月，根据监测数据显示，我省互联网网络安全环境主要情况如下：（1）15480 个 IP 地址对应的主机被境内外黑客通过木马或僵尸程序控制，较上月增加 8.8%；（2）39 个 IP 地址对应主机感染木马或僵尸程序成为控制服务器，较上月减少 9.3%；（3）3212 个 IP 地址对应的主机感染“飞客”蠕虫病毒，较上月增长 4.42%；（4）19 个网站被篡改网页，较上月减少 53.7%；（5）12 个网站被植入后门，较上月减少 7.7%。

二、数据导读

（一）木马僵尸监测数据分析

1.木马或僵尸程序受控主机分析

11 月，国家计算机网络应急技术处理协调中心（以下简称“国家互联网应急中心”）对木马僵尸的活动状况进行了抽样监测，发现中国大陆地区 1280608 个 IP 地址对应的主机被木马或僵尸程序控制。事件高发的三个省份分别为江苏省（约占 17.0%）、浙江省（约占 15.0%）、广东省（约占 10.6%）。具体分布情况如图 1 所示：

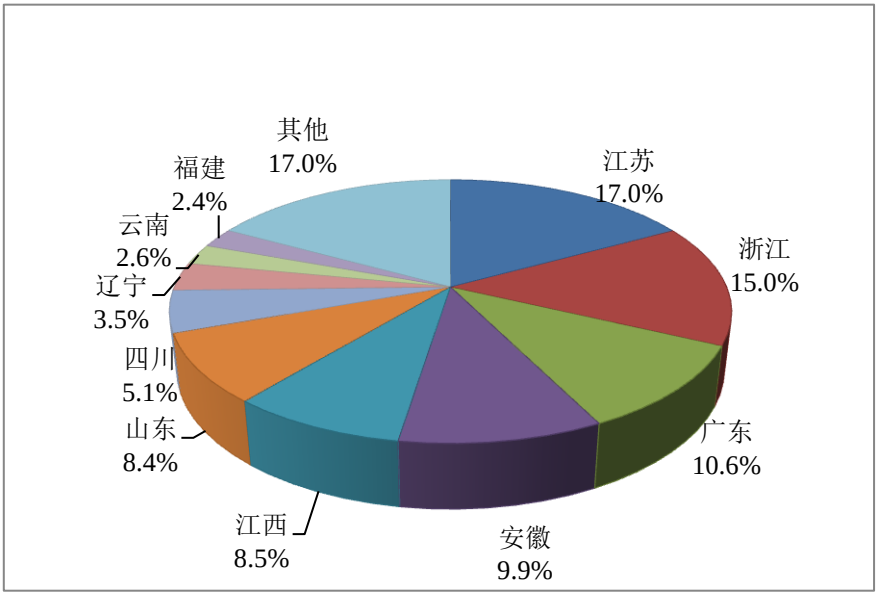

图 1 境内木马或僵尸网络程序受控主机按 IP 地区分布图

11 月，监测发现我省木马或僵尸程序受控主机数量位列全国第 15 位，较上月上升 1 位，占全国受控主机总数的 1.2%，位列全国第 16 位，较上月上升 1 位。其中，忻州、临汾、太原排在全省受控木马或僵尸主机活动频繁地区前三位。具体分布情况如图 2 所示：

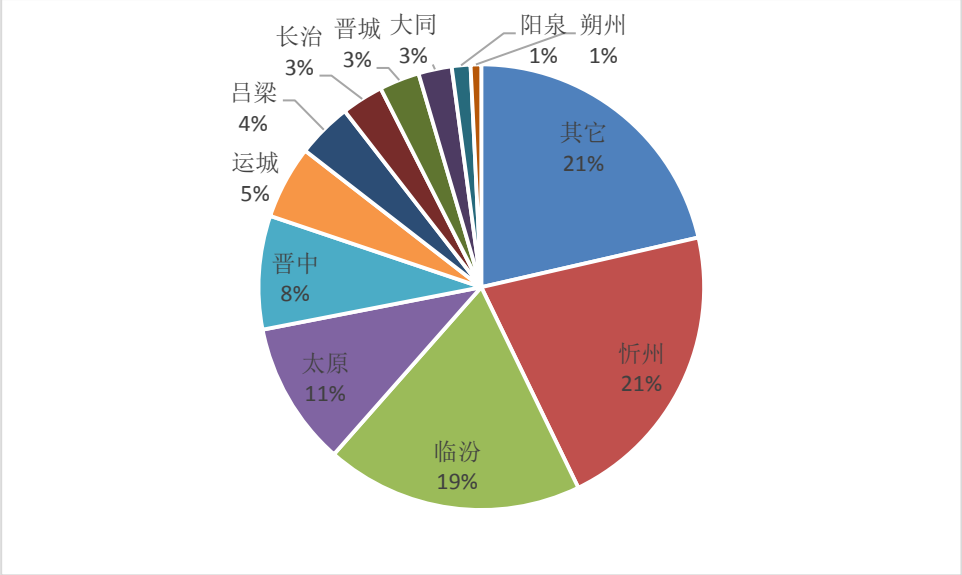

图 2 我省木马或僵尸程序受控主机分布图

2.木马或僵尸程序控制服务器分析

11 月，国家互联网应急中心对木马僵尸的活动状况进行了抽样监测，发现中国大陆地区 2253 个 IP 地址对应的主机成为木马或僵尸程序控制服务器。事件高发的三个省份分别为江苏省（约占 18.6%）、广东省（约占 11.6%）、浙江省（约占 9.9%）。具体分布情况如图 3 所示：

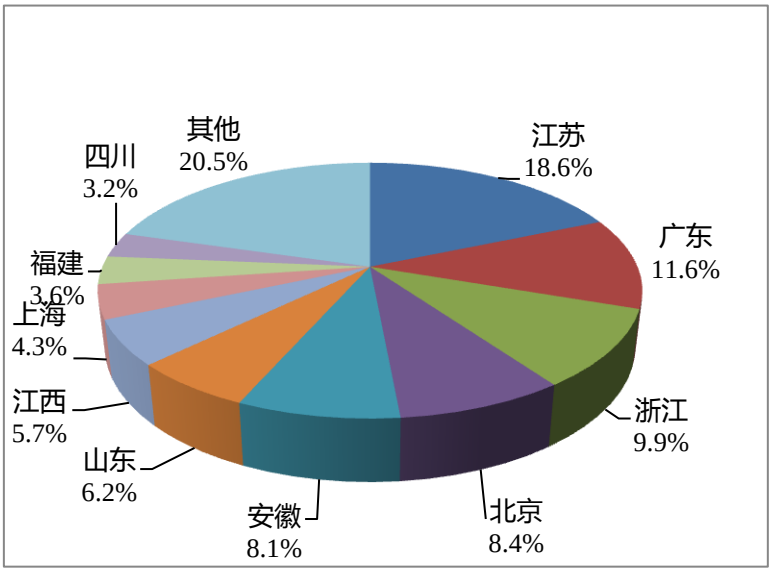

图 3 境内木马或僵尸程序控制服务器 IP 按地区分布图

11 月，我省木马或僵尸程序控制服务器数量占全国控制服务器总数的 1.73%，位列全国第 14 位，较上月下降 1 位。其中，阳泉、太原、忻州排在全省控制木马或僵尸主机活动频繁地区前三位。具体分布情况如图 4 所示：

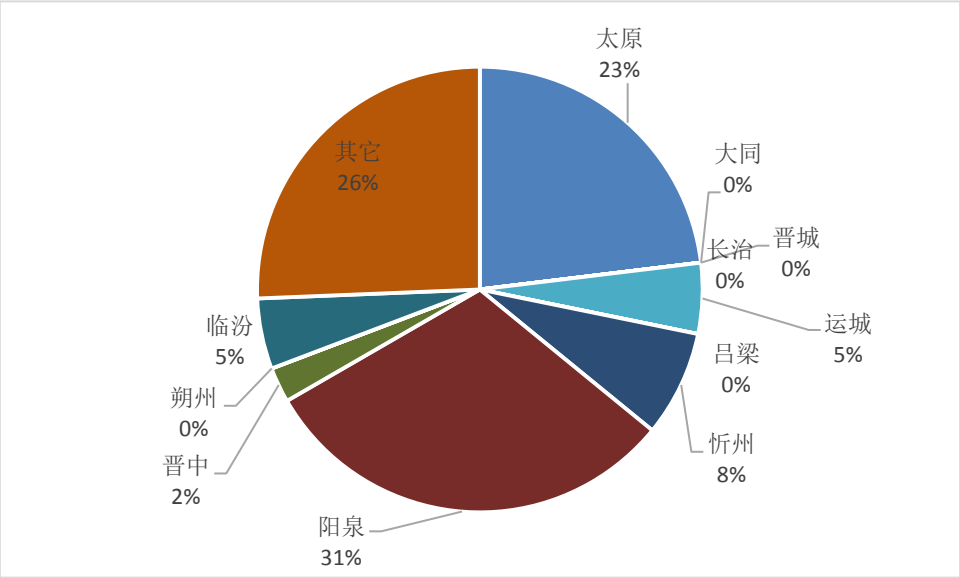

图 4 我省木马或僵尸程序控制服务器分布图

3.木马或僵尸网络规模分布

11 月，山西互联网应急中心监测发现省内三家基础电信运营企业受木马或僵尸感染用户主机数目分别为：山西联通 10249 台，山西移动 1099 台，山西电信 3175 台。

（二）网页篡改数据分析

11 月，国家互联网应急中心监测发现中国大陆地区被篡改网站 20135 个，其中境内被篡改政府网站（.gov）数量为 57 个。被篡改网站最多的地区分别为北京市（约占 26.5%）、山东省（约占 12.0%）、广东省（约占 11.7%），具体分布情况如图 5 所示：

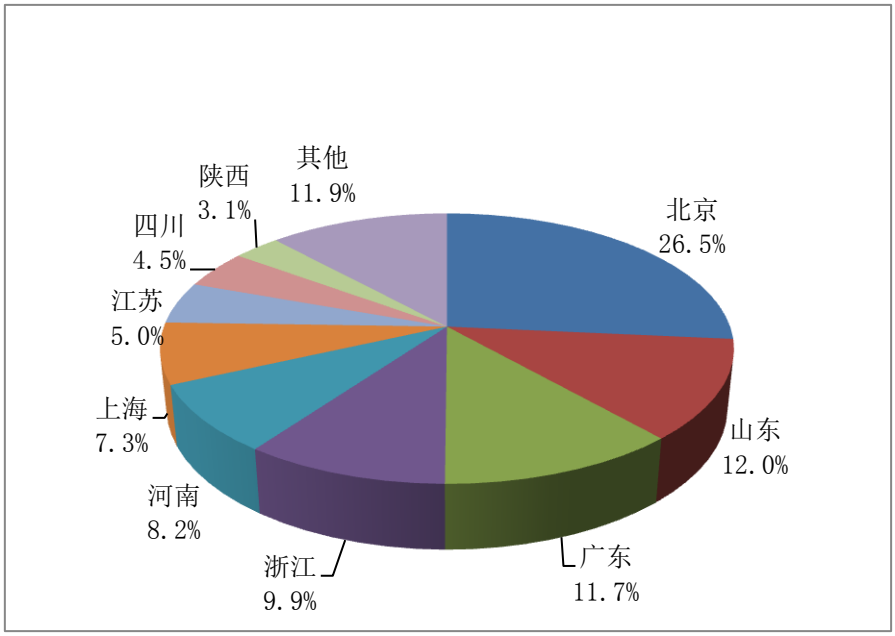

图 5 境内被篡改网站按地区分布图

11 月，我省有 19 个网站被篡改网页，占全国被篡改网站总数的 0.13%，位列全国第 27 位，较上月下降 2 位，主要的篡改攻击方式为“页面攻击”和“暗链攻击”。

（三）网站后门数据分析

11 月，我省有 12 个网站被植入后门，占全国被植入后门网站总数的 0.12%，位列全国第 28 位，较上月持平。其中政府和事业单位网站占全部被植入后门网站数量的 15.4%，同期全国的平均数为 2.8%。具体分布情况如图 6 所示：

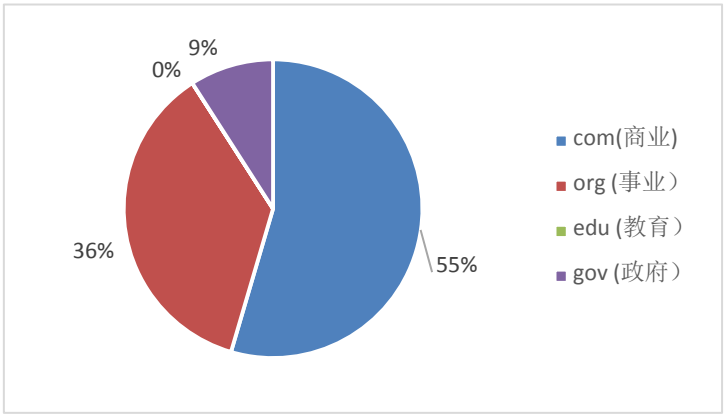

图 6 我省被植入后门网站数量按类型分布图

（四）“飞客”蠕虫数据分析

11 月，国家互联网应急中心对“飞客”蠕虫的活动状况进行了抽样监测，发现境内感染“飞客”蠕虫的主机 IP 地址共 241166 个。事件高发的三个省份分别为广东省（约占 30.1%）、江苏省（约占 7.4%）和浙江省（约占 6.7%），其分布情况如图 7 所示：

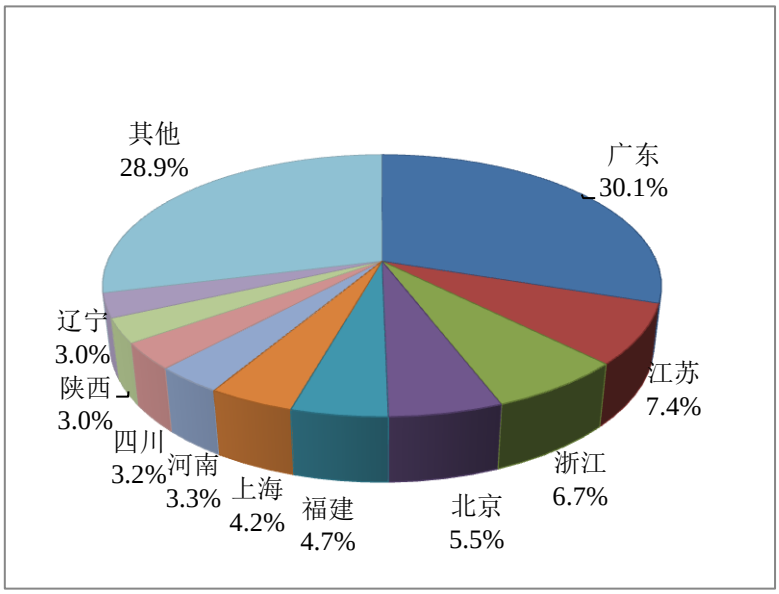

图 7 境内感染飞客蠕虫的主机 IP 按地区分布图

11 月，监测发现山西省感染“飞客”蠕虫病毒主机 3212 台，占全国受感染总数的 1.3%，位列全国第 22 位，与上月持平。具体分布情况如图 8 所示：

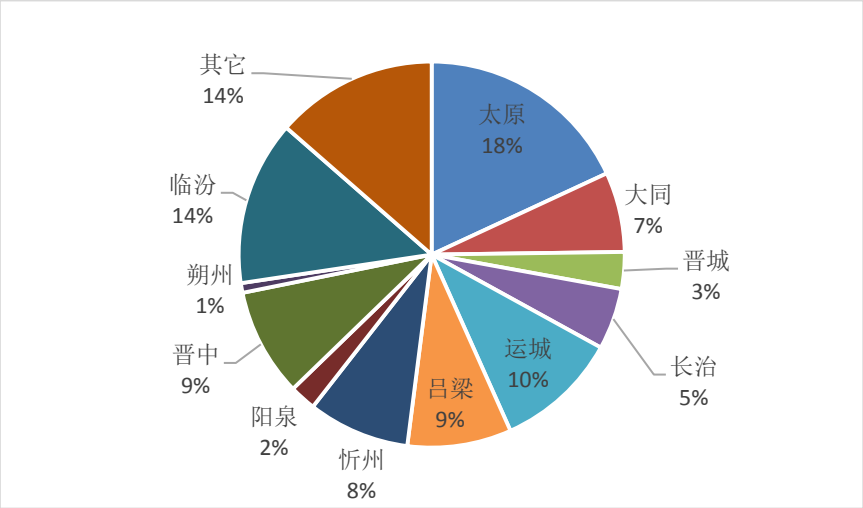

图 8 我省感染“飞客”蠕虫的主机 IP 按地区分布图

（五）移动互联网恶意程序传播服务器数据分析

11 月，未监测发现我省移动互联网恶意程序传播服务器。

（六）安全漏洞数据分析

11 月，国家互联网应急中心收到来自国家信息安全漏洞共享平台（CNVD）报告的漏洞数量 2078 个，其中高危漏洞 510 个、中危漏洞 1323 个、低危漏洞 245 个，其中 0day 漏洞 1740 个，可远程攻击漏洞 591 个。

2019 年 1 月至 2019 年 11 月 CNVD 收录漏洞按月统计情况分布如图 9 所示：

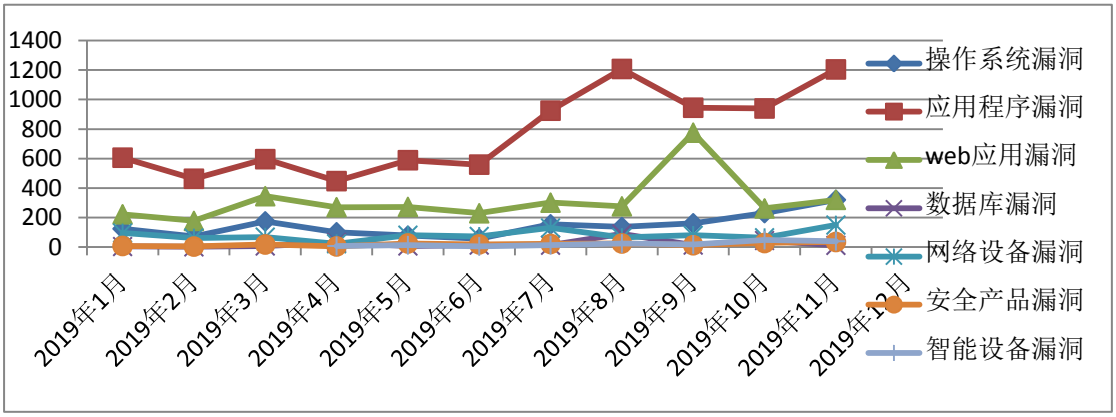

图 9 CNVD 收录漏洞按月统计情况

三、重要安全漏洞提示

（一）云存储应用存在越权访问和文件上传漏洞

2019年11月18日，国家信息安全漏洞共享平台（CNVD）收录了由腾讯安全玄武实验室发现并报送的云存储应用越权访问和文件上传漏洞（CNVD-2019-37364）。攻击者利用该漏洞，可在越权的情况下，远程读取、修改云存储中的内容。目前，漏洞相关细节未公开，漏洞影响范围和危害较大。

参考链接：https://www.cnvd.org.cn/webinfo/show/5291

（二）安卓摄像头应用含高危漏洞 影响数亿设备

11月，安全研究团队的研究人员表示，任何应用程序在不具备具体权限的情况下均可控制安卓摄像头 app 并强制其拍照或录视频，即使手机锁定且屏幕关闭的情况也不例外。该团队将研究结果告知谷歌，后者通知了其它安卓厂商，其中三星已确认其智能手机中也存在这些漏洞。谷歌指出其它原始设备制造厂商也确认了这些漏洞的存在，影响全球数亿台设备。该团队在报告中说明的是从 Pixel 2和 Pixel 3 设备上找到的漏洞，不过谷歌所有的手机模型均存在这些被统称为 CVE-2019-2234 的漏洞问题。

参考链接：https://www.cnvd.org.cn/webinfo/show/5303