山西省网络安全月度通报

2020 年第 1 期（总第 67 期）

山西互联网应急中心　　2020 年 1 月

一、基本态势

2019 年 12 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 14470 台，木马或僵尸程序控制服务器 13 台，感染“飞客”蠕虫病毒主机 2928 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

12 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

12 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）14470 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，较上月减少 6.52%；（2）13 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 66.7%；（3）2928 个 IP 地址对应的主机感染“飞客”蠕虫病毒，较上月减少 8.84%；（4）18 个网站被篡改网页，较上月减少 5.3%；（5）3 个网站被植入后门，较上月减少 75%。

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

12 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 1299438 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 16.2%）、浙江省（约占 13.5%）、广东省（约占 11.7%）。具体分布情况如图 1 所示：

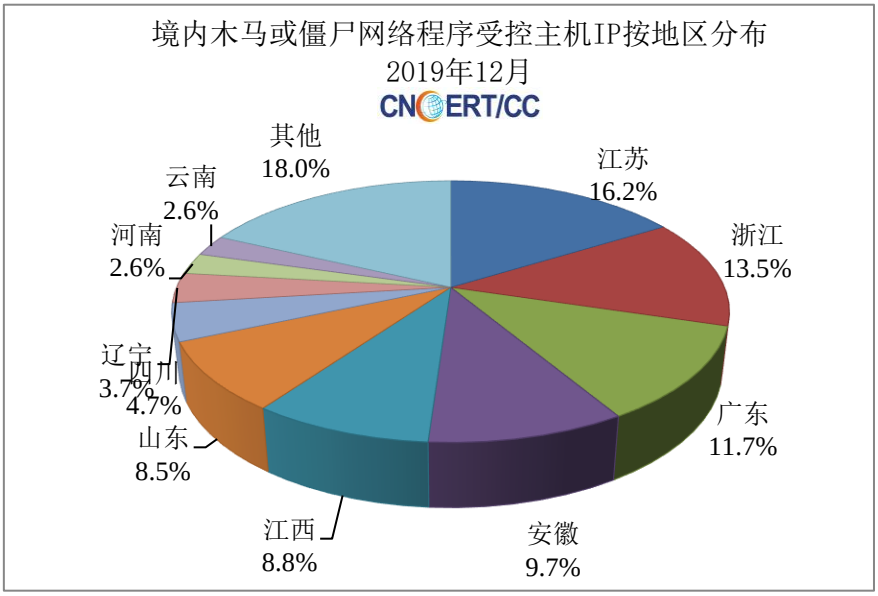

图 1 境内木马或僵尸网络程序受控主机按 IP 地区分布图

12 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 16 位，较上月下降 1 位，占全国受控主机总数的 1.11%。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：

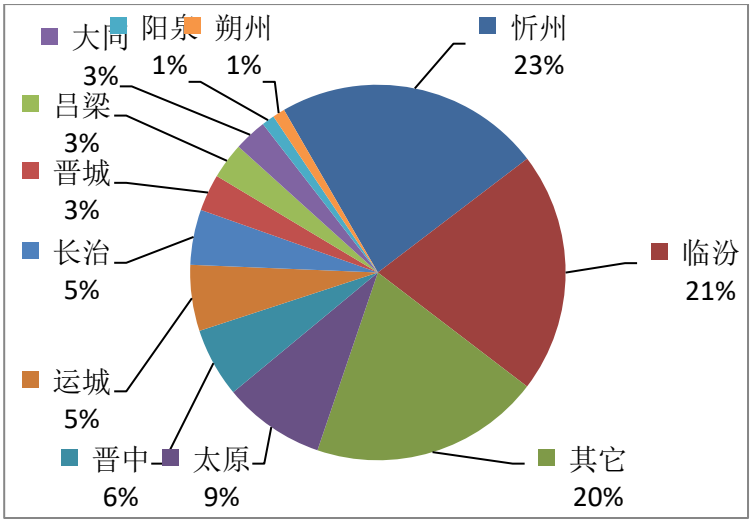

图 2 我省木马或僵尸程序受控主机分布图

2. 木马或僵尸程序控制服务器分析

12 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广东省（约占 16.6%）、江苏省（约占 15.5%）、北京（约占 11.1%）。具体分布情况如图 3 所示：

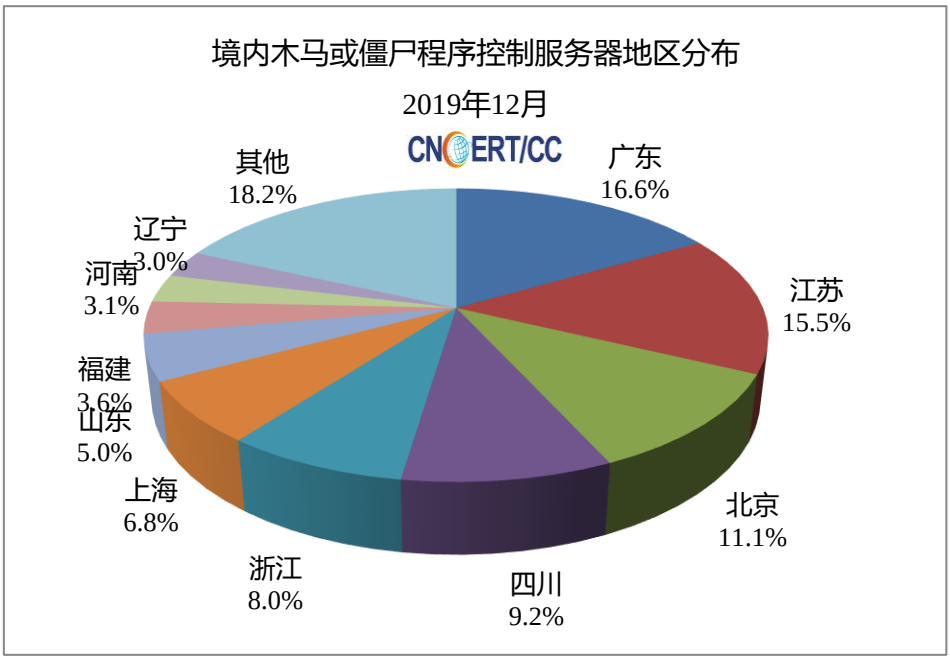

图 3 境内木马或僵尸程序控制服务器 IP 按地区分布图

12 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 0.84%，位列全国第 20 位，较上月下降 6 位。其中，木马或僵尸控制服务器均位于阳泉、太原，具体情况如图 4 所示：

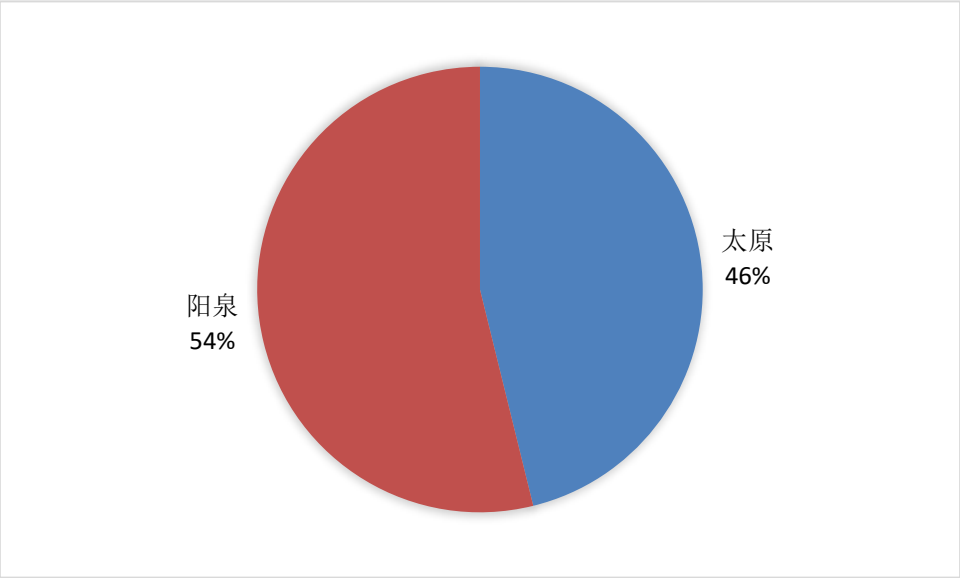

图 4 我省木马或僵尸程序控制服务器分布图

3. 木马或僵尸网络规模分布

12 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 9600 台，山西移动 1468 台，山西电信 2458 台。

（二）网页篡改数据分析

12 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 17286 个，其中境内被篡改政府网站（.gov）数量为 63 个。被篡改网站最多的地区分别为北京市（约占 26.2%）、广东省（约占 12.2%）、山东省（约占 11.6%），具体分布情况如图 5 所示：

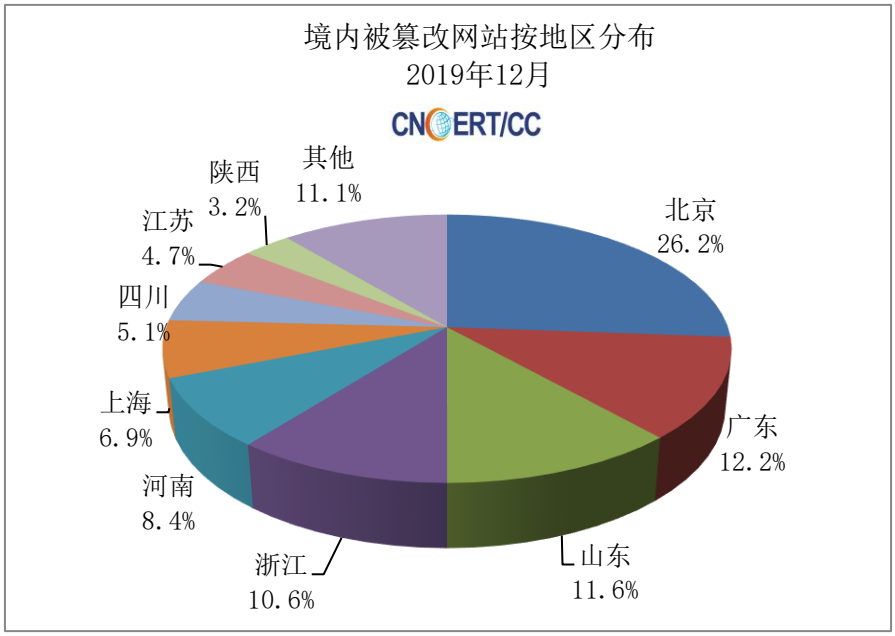

图 5 境内被篡改网站按地区分布图

12 月，我省有 18 个网站被篡改网页，占全国被篡改网站总数的 0.1%，位列全国第 26 位，较上月上升 1 位，主要的篡改攻击方式为“aaa”和“暗链测试”。

（三）网站后门数据分析

12 月，我省有 3 个网站被植入后门，占全国被植入后门网站总数的 0.027%，位列全国第 30 位，较上月下降 2 位。具体分布情况如图 6 所示：

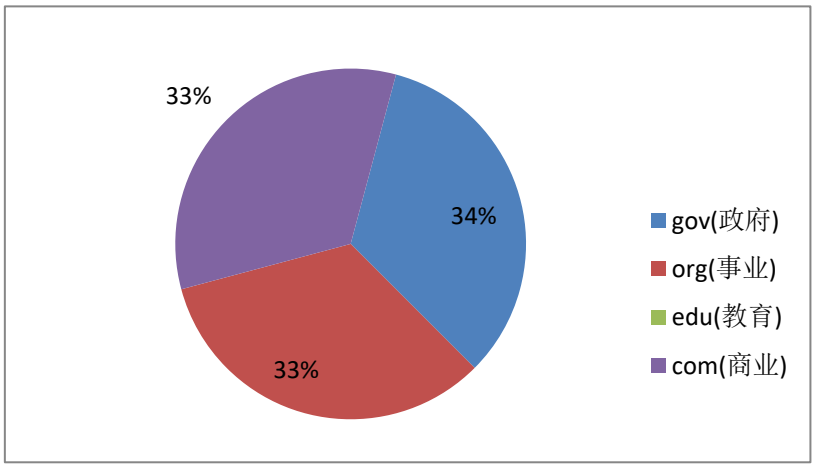

图 6 我省被植入后门网站数量按类型分布图

（四）“飞客”蠕虫数据分析

12 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 222202 个。事件高发的三个省份分别为广东省（约占 30.2%）、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：

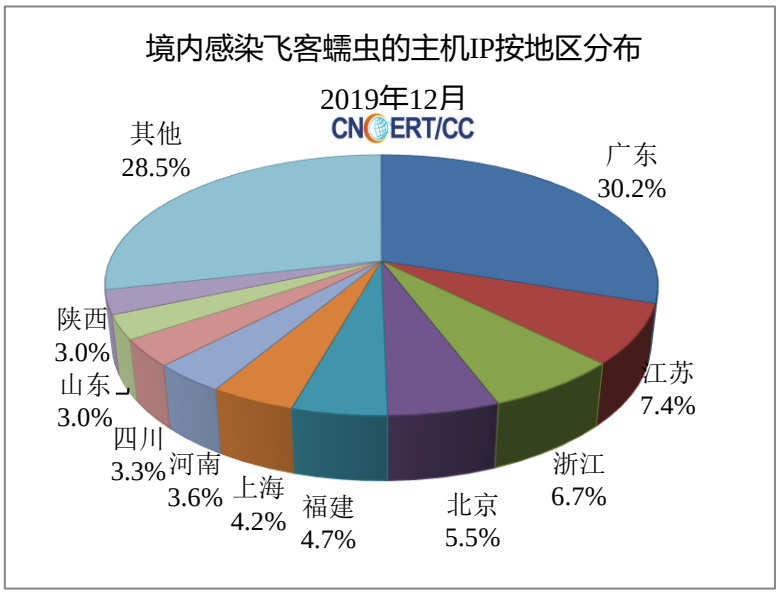

图 7 境内感染飞客蠕虫的主机 IP 按地区分布图

12 月，监测发现山西省感染“飞客”蠕虫病毒主机 2928 台，占全国受感染总数的 1.31%，位列全国第 22 位，与上月持平。具体分布情况如图 8 所示：

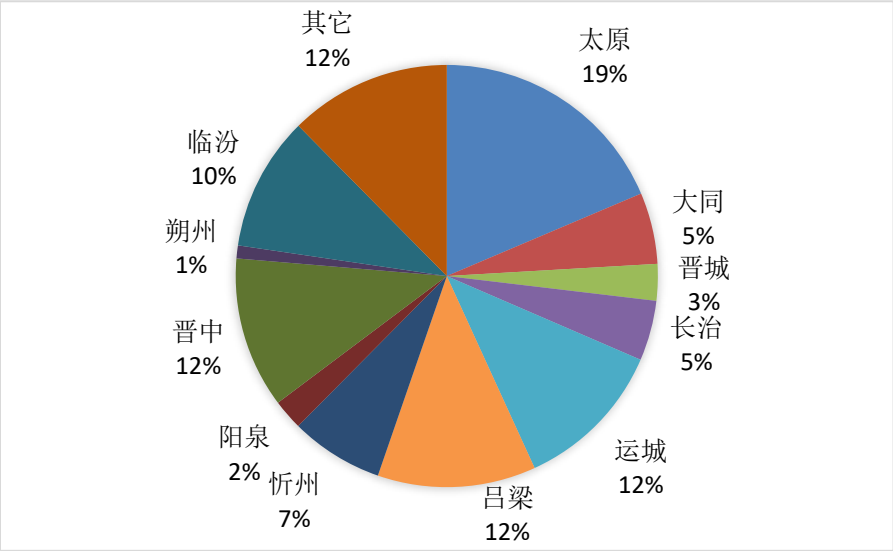

图 8 我省感染“飞客”蠕虫的主机 IP 按地区分布图

（五）移动互联网恶意程序传播服务器数据分析

12 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

12 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 1279 个，其中高危漏洞 517 个、中危漏洞 666 个、低危漏洞 96 个，其中 0day 漏洞 604 个，可远程攻击漏洞 1096 个。

2019 年 1 月至 2019 年 12 月 CNVD 收录漏洞按月统计情况分布如图 9 所示：

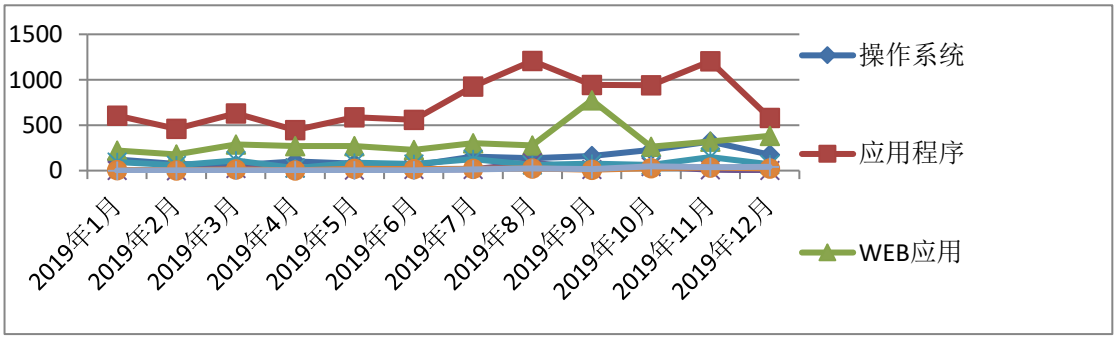

图 9 CNVD 收录漏洞按月统计情况

三、重要安全漏洞提示

（一）GoAhead Web 服务器存在高危漏洞

近日，网络安全研究人员披露了GoAheadWeb服务器软件中两个新漏洞的详细信息。其中一个漏洞（CVE-2019-5096）可以被攻击者利用远程执行命令，上传恶意代码，并控制物联网设备。GoAhead Web服务器软件是一个广泛用于物联网智能设备的微型应用程序，使用设备超过数十亿台。

参考链接：https://www.cnvd.org.cn/webinfo/show/5321

（二）Chrome 浏览器组件存在任意代码执行漏洞

近日，腾讯的安全研究人员通报其发现的位于Chrome浏览器WebSQL和SQLite组件上的远程代码执行漏洞。攻击者利用该漏洞，通过社工手段诱使用户访问恶意网页，实现对用户浏览器网页进程的权限控制和代码执行。

参考链接：https://www.cnvd.org.cn/webinfo/show/5333