山西省网络安全月度通报

2021 年第 1 期（总第 79 期）

山西省通信管理局
国家计算机网络与信息安全管理中心山西分中心　　2021 年 2 月

一、基本态势

2020 年 12 月，我省公用通信网和公共互联网基础网络运行状况整体评价为良，未发生造成较大影响的网络运行故障，未发生三级以上网络安全事件。

2020 年 12 月，据监测数据显示，我省公共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，网络漏洞、网络攻击监测数据总体平稳。全行业共发现并处置一般网络安全事件 206 起。

2020 年 12 月，我省网络信息安全状况整体评价为良。本月发现并处置违法违规网页（URL）12084 条，检出疑似涉诈 URL 6 万条，疑似涉诈 APP 3921 个。

（一）基础网络运行安全

12 月，我省公用通信网和公共互联网基础网络运行总体平稳，未发生造成较大影响网络运行故障，未发生三级以上网络安全事件。

（二）公共互联网网络安全

12 月，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）21524 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 5.6%，列全国第 14 位；（2）20 个 IP 地址对应主机感染木马或僵尸程序成为控制服务器，较上月增加 300%，列全国第 16 位；（3）3230 个 IP 地址对应的主机感染“飞客”蠕虫病毒，较上月减少 15.9%；（4）监测发现并处置一般网络安全事件 206 起。

（三）公共互联网信息安全

12 月，据监测数据显示，我省公共互联网不良信息治理主要情况如下：（1）研判并推送涉黄涉赌类网站 55 个；（2）发现并处置违法违规 URL12084 条；（3）检出疑似涉诈 URL6 万条，较上月增加 10.4%；（4）检出疑似涉诈 APP3921 个，较上月增加 14.1%。

二、重点工作与事件

（一）我局完成 2020 年行业网络安全防护现场检查

12 月，按照工信部部署、我局全年工作计划及相关要求，我局组织开展对 36 家在省内开展业务的企业（6 家重点 IDC/ISP 企业、9 家重点互联网企业、8 家网约车企业、4 家工业互联网平台企业、2 家工业互联网二级标识解析节点企业、7 家在我省信息通信业开展网络安全服务的专业单位）开展了监督检查、现场技术检测，强化事中事后网络安全监管，对检查发现的问题要求企业限期整改。检查共发现系统漏洞 37 个，同比去年（19 个）增加 94.74%，其中部分系统存在弱口令漏洞、Microsoft 远程桌面服务远程代码执行、SQL 注入等可能导致系统被远程控制的安全防护漏洞。

三、行业管理

（一）互联网网络安全信息通报

12 月，工业和信息化部向我局通报监测发现的事件 30 起，我局委托安全中心山西分中心进行技术验证后，向涉事单位下发了网络安全威胁处置通知书。安全中心山西分中心同期向基础电信运营企业通报监测发现的事件 149 起，对 27 起网络安全事件及时协调处置、汇总，并以互联网网络安全事件的形式向各相关单位进行了通报。

（二）网络安全事件处置

1.僵尸木马专项治理行动

12 月，按照省通信管理局工作安排，安全中心山西分中心会同基础电信运营企业共同开展了僵尸木马控制端专项清理行动，对分布在我省的 5 台木马或僵尸程序控制服务器进行了集中清理，协调基础电信企业暂时停止对涉事专线用户的 IP 解析服务，直至该专线用户完成对自身主机恶意程序清理后予以恢复。

2.一般互联网网络安全事件处置

12 月，全行业共协调处置一般网络安全事件 206 起，其中：工信部通报我省网络安全事件 30 起，安全中心山西分中心协调处置 176 起。其中：僵木蠕恶意程序 147 起，移动恶意程序 2 起，网页篡改 20 起，网站被植入后门 1 起，网站漏洞 6 起，系统漏洞 6 起，恶意域名/URL 24 起，有效保障了我省重要信息系统和互联网专线用户的网络运行安全。

四、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，国家计算机网络与信息安全管理中心（以下简称“安全中心”）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1235726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安徽省（约占12.3%）、江苏省（约占10.4%）、辽宁省（约占9.2%）。具体分布情况如图1所示:

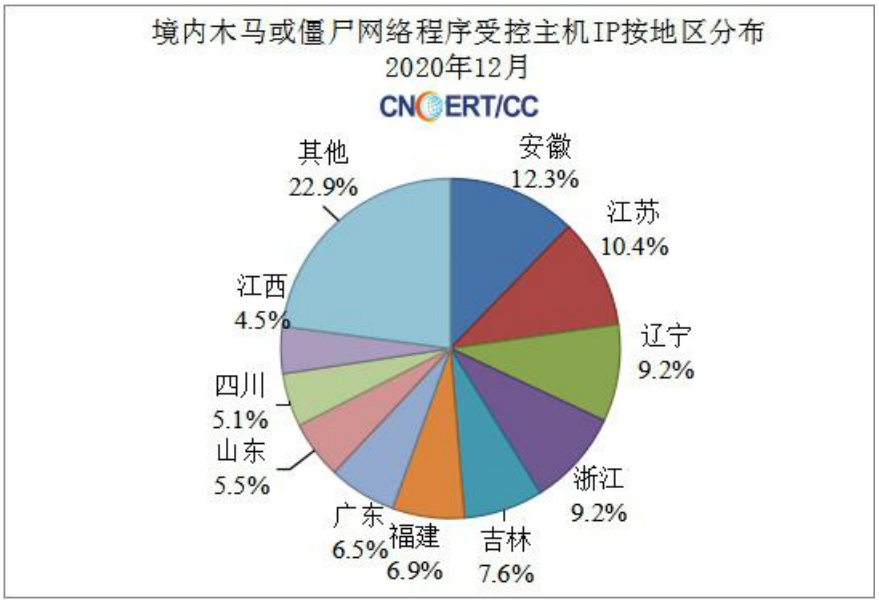

图1 境内木马或僵尸网络程序受控主机按IP地区分布图

12月，我省受感染木马或僵尸程序受控主机数量位列全国第14位，与上月持平，占全国受控主机总数的1.74%。其中，晋中、朔州、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:

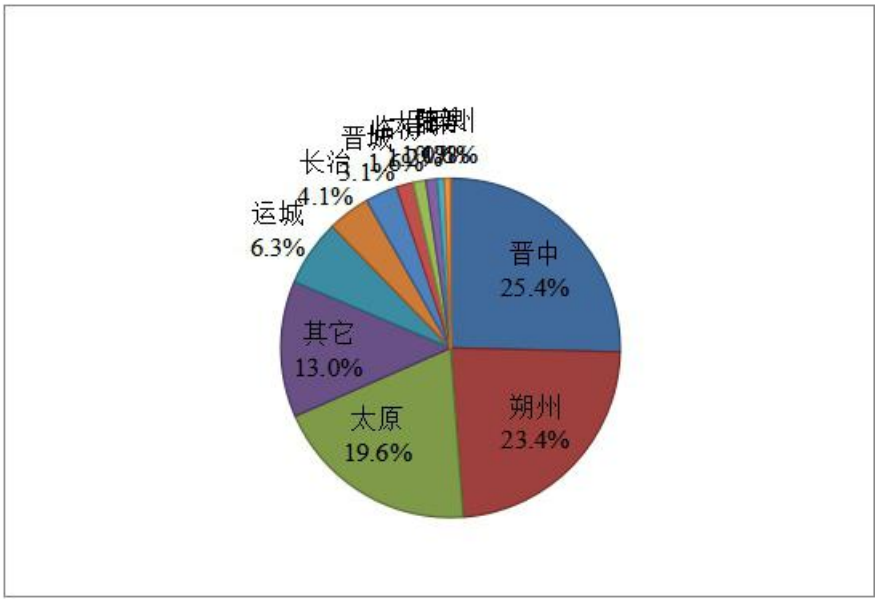

图 2 我省木马或僵尸程序受控主机分布图

2.木马或僵尸程序控制服务器分析

12 月，安全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 1027 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 14.9%）、江苏省（约占 11.1%）、浙江省（约占 9.4%）。具体分布情况如图 3 所示:

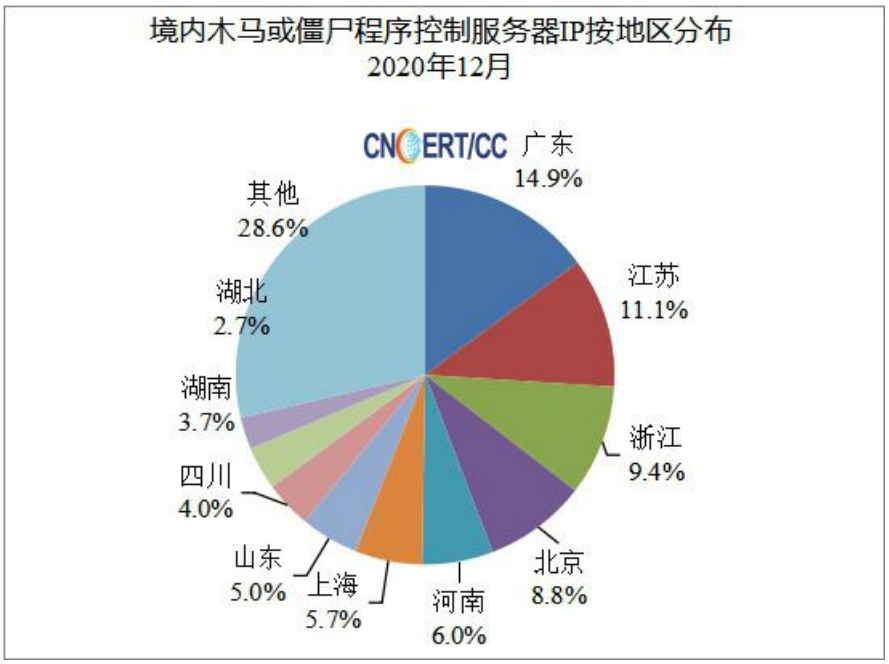

图 3 境内木马或僵尸程序控制服务器 IP 按地区分布图

12 月，我省受感染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 1.9%，位列全国第 13 位，较上月上升 9 位。其中，阳泉、太原、运城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：

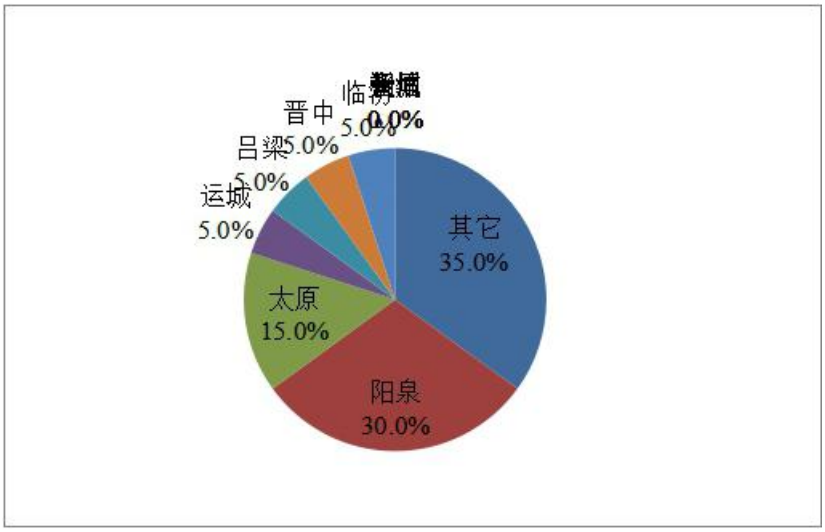

图 4 我省木马或僵尸程序控制服务器 IP 按地区分布图

3.木马或僵尸网络规模分布

12 月，安全中心山西分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：山西联通用户 11775 台，山西移动用户 990 台，山西电信用户 9869 台。

（二）网页篡改数据分析

12 月，安全中心监测发现中国大陆地区被篡改网站 14988 个，其中境内被篡改政府网站（.gov）数量为 81 个。被篡改网站最多的地区分别为北京市（约占 27.3%）、山东省（约占 13.9%）、浙江省（约占 10.5%）。具体分布情况如图 5 所示：

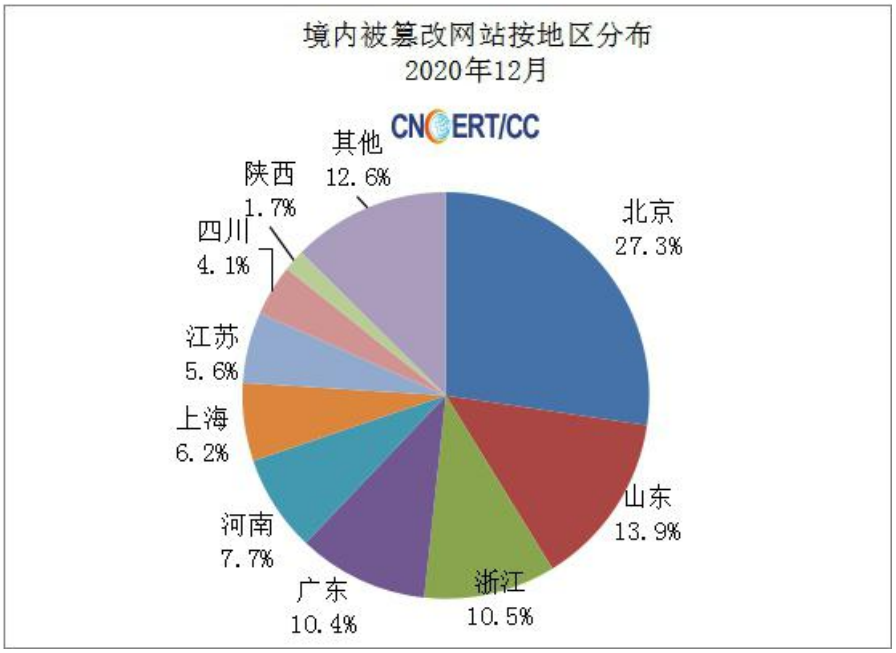

图 5 境内被篡改网站按地区分布图

12 月，安全中心山西分中心监测发现我省有 20 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 24 位，较上月下降 1 位，主要的篡改内容为游戏类和博彩类敏感词汇。

（三）网站后门数据分析

12 月，安全中心山西分中心监测发现我省有 1 个网站被植入后门，占全国被植入后门网站总数的 0.05%，位列全国第 27 位。

（四）“飞客”蠕虫数据分析

12 月，安全中心山西分中心监测发现我省受感染“飞客”蠕虫病毒主机 3230 台。其中，太原、临汾、运城排在全省感染“飞客”蠕虫主机活动频繁地区前三位。具体分布情况如图 6 所示:

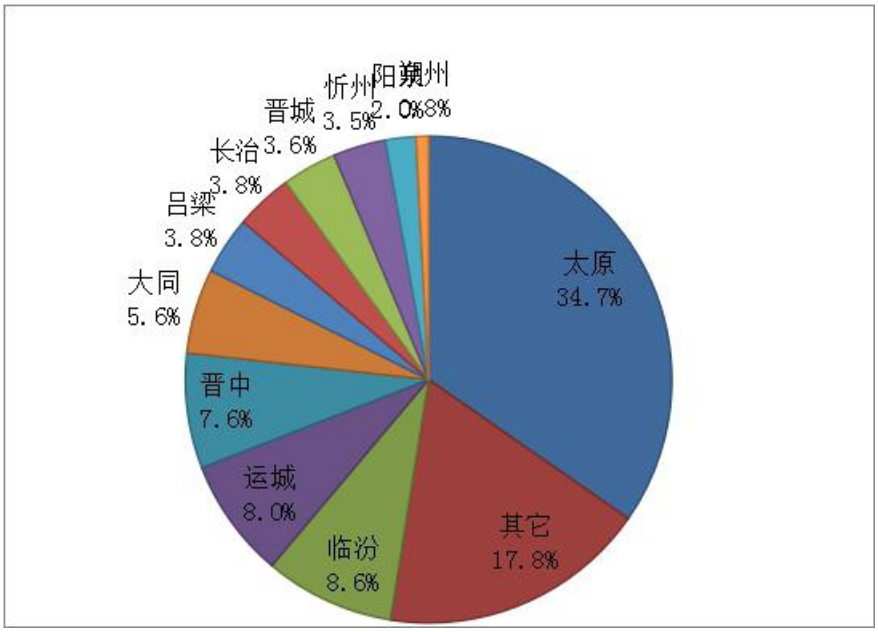

图 6 我省感染“飞客”蠕虫的主机 IP 按地区分布图

（五）安全漏洞数据分析

1.安全中心国家信息安全漏洞共享平台（CNVD）安全漏洞分析

12 月，安全中心国家信息安全漏洞共享平台（CNVD）收录各类漏洞 1221 个，包含高危漏洞 469 个、中危漏洞 637 个、低危漏洞 115 个，其中可远程攻击 872 个，0day 漏洞 766 个。

五、重要安全漏洞提示

（一）Apache Struts2存在远程代码执行漏洞（S2-061）

Struts2是第二代基于Model-View-Controller（MVC）模型的java企业级web应用框架，成为国内外较为流行的容器软件中间件。

2020年12月8日，Apache Strust2发布最新安全公告，Apache Struts2存在远程代码执行的高危漏洞（CVE-2020-17530）。由于Struts2会对一些标签属性的属性值进行二次解析，当这些标签属性使用了`%{x}`且`x`的值用户可控时，攻击者利用该漏洞，可通过构造特定参数，获得目标服务器的权限，实现远程代码执行攻击。

CNVD对该漏洞的综合评级为“高危”。

参考链接：https://www.cnvd.org.cn/webinfo/show/5899

（二）Microsoft Azure Sphere20.07存在代码执行漏洞

Microsoft Azure Sphere是美国微软（Microsoft）公司的一个应用于云环境提供安全防护的设备。

Microsoft Azure Sphere 20.07版本存在代码执行漏洞，该漏洞源于常规签名代码执行功能允许任意代码执行。攻击者可利用该漏洞执行使用PACKET_MMAP触发此漏洞的shellcode。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-73758

六、要闻回顾

（一）国内部分

1. 让老年人更好融入数字生活

党的十九届五中全会审议通过的《中共中央关于制定国民经济

和社会发展第十四个五年规划和二〇三五年远景目标的建议》提出，积极开发老龄人力资源，发展银发经济。数字技术快速发展，移动化、智能化、个性化的消费走进千家万户，也同样影响着老年群体。当“数字化”遇到“老龄化”，一方面老年人的生活因“数字化”而更便利，另一方面，跟不上“数字化”发展步伐的老年人也不在少数。

工信部于12月25日宣布，开展专项行动，解决老年人上网用网难题。专项行动首批将完成115个公共服务类网站和43个手机APP的适老化及无障碍改造，覆盖国家相关部委及省级政府、新闻资讯、生活购物、医疗健康等领域。

2. 全国一体化大数据中心协同创新体系将加速构建

12月28日国家发改委、中央网信办、工业和信息化部、国家能源局四部门联合印发《关于加快构建全国一体化大数据中心协同创新体系的指导意见》。《意见》指出，加快构建全国一体化大数据中心协同创新体系，是贯彻落实党中央、国务院决策部署的具体举措。

《意见》提到，要加强全国一体化大数据中心顶层设计。其中包括，优化数据中心基础设施建设布局，加快实现数据中心集约化、规模化、绿色化发展，形成“数网”体系；加强跨部门、跨区域、跨层级的数据流通与治理，打造数字供应链，形成“数链”体系；加快提升大数据安全水平，强化对算力和数据资源的安全防护，形成“数盾”体系等。

（二）国际部分

1. 2020 中俄网络媒体云论坛召开 聚焦“疫情时期网络媒体的作用”

12 月 18 日，2020 中俄网络媒体云论坛在北京和莫斯科通过视频会议方式举行。中央网络安全和信息化委员会办公室副主任牛一兵，俄罗斯联邦数字发展、通讯与大众传媒部副部长切尔科索娃·贝拉·穆哈比耶夫娜出席论坛并在开幕式上致辞。

中俄网络媒体论坛自 2016 年以来已举办三届，成为中俄两国网络媒体管理部门开展对话、加强协作的重要平台。今年，论坛围绕“疫情时期网络媒体的作用”的主题，进一步推动两国网络媒体深化交流合作，提升国际话语权。

2. 弥合数字鸿沟 共享发展红利

国际电信联盟近日发布的《衡量数字化发展：2020 年事实与数字》报告显示，全球有超过一半的人口在使用互联网。从 2015 年到 2020 年，4G 网络覆盖范围在全球范围内扩大了一倍，到 2020 年底将覆盖全球近 85%的人口。报告显示，疫情防控期间，数字鸿沟问题进一步凸显。发达国家与发展中国家、城市与农村、不同群体之间的数字基础设施建设及互联网接入的差距持续扩大，如何确保数字化成果惠及所有人，成为各方关注的焦点。

国际电信联盟建议，各国政府需要采取协调监管、吸引投资和商业激励等措施，为数字化普惠发展和打造数字化社会营造有利环境。

主送：省委办公厅、省政府办公厅、省委政法委、省委网信办、省“扫黄打非”办、省公安厅、省安全厅。

抄送：工业和信息化部网络安全管理局、中国信息通信研究院、国家计算机网络与信息安全管理中心，中国联通山西省分公司、中国移动通信集团山西有限公司、中国电信山西分公司。

局内：局领导，各处室。

信息编辑：山西省通信管理局 网络安全管理处

技术支撑：国家计算机网络与信息安全管理中心山西分中心 中国信息通信研究院安全所

地址：太原市南内环街 2 号

电话/传真：0351-8788159