山西省网络安全月度通报

2021 年第 2 期（总第 80 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 3 月

一、基本态势

2021 年 1 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。

2021 年 1 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 181 起。

2021 年 1 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）8568 条，检出疑似涉诈 URL 155 万条。

（一）基础网络运行安全

1 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

1 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）14719 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 31.6%，列全国第 19 位；（2）16 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 20%，列全国第 26 位；（3）898 个 IP 地址对应的主机感染“飞客”蠕虫病毒，较上月减少 72.2%；（4）监测发现并处置一般网络安全事件 181 起。

（三）公共互联网信息安全

1 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）发现并处置违法违规 URL8568 条；（3）检出疑似涉诈 URL 155 万条，较上月增加 2487.4%。

二、重点工作与事件

（一）我省信息通信业圆满完成 2021 年省“两会”网络安全保障任务

按照省“两会”安全保卫工作领导组部署要求，1 月 19 日至 24 日，我局成立领导小组，按照“统一领导、分工负责、全面保障、协同联动”的工作原则和“精干实效”的工作要求，制定专项保障方案，建立专项保障机制，梳理保障清单，对省内重要网站开展安全风险评估，委托国家计算机网络应急技术处理协调中心山西分中心对省内基础电信运营企业和主要增值电信业务经营单位开展了网络安全专项检查，指导信息通信业开展了省级重点网站实时监测、互联网恶意代码清理专项行动，坚决防范网络安全重大风险，坚决遏制网络安全重大事故，实现了确保网络基础设施平稳运营、确保不发生大规模数据泄漏事件、确保专项通信保障工作高效稳妥开展、确保突发事件应急处置快速有效的“四个确保”工作目标。

省“两会”重要通信保障期间，我省公用通信网和公共互联网网络

运行稳定，省际出入口峰值流量正常，未发生重大通信事故，未发生重大网络安全事件。

三、行业管理

（一）互联网网络安全信息通报

1 月，工业和信息化部向我局通报监测发现的事件 8 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 144 起，对 29 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

1 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 16 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

1 月，全行业共协调处置一般网络安全事件 181 起，其中：工信部通报我省网络安全事件 8 起，安全中心山西分中心协调处置 173 起。其中：僵木蠕恶意程序 144 起，信息泄露 1 起，恶意 IP 地址 1 起，网页篡改 19 起，网站被植入后门 3 起，网站漏洞 6 起，恶意域名/URL 7 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

1 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 1191688 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 12.5%）、浙江省（约占 11.0%）、江苏省（约占 10.3%）。具体分布情况如图 1 所示:

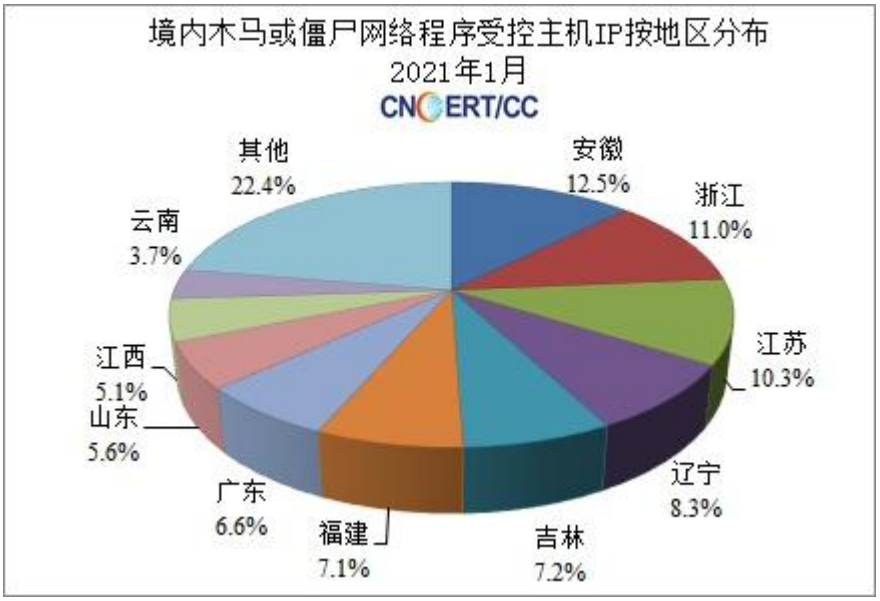

图 1 境内木马或僵尸网络程序受控主机按 IP 地区分布图

1 月，我省受感染木马或僵尸程序受控主机数量位列全国第 19 位，较上月下降 5 位，占全国受控主机总数的 1.24%。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:

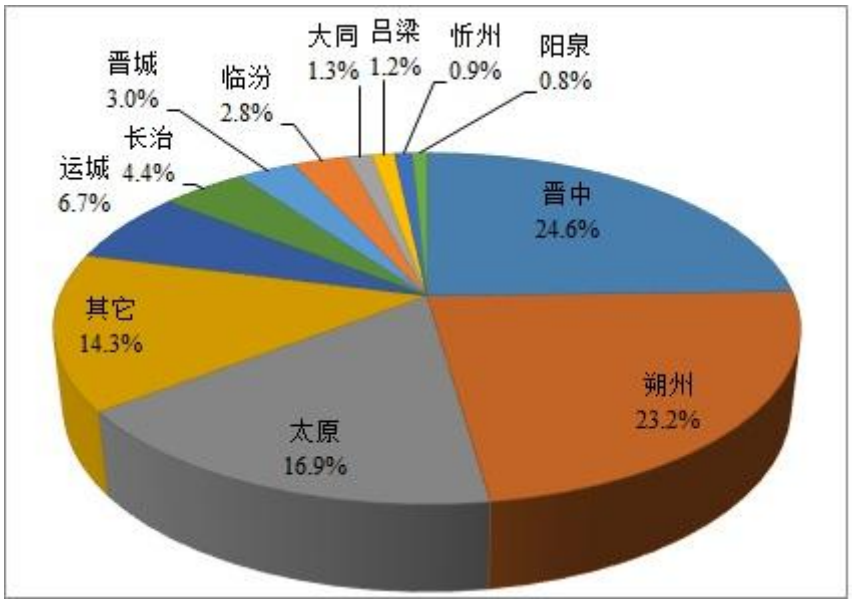

图 2 我省木马或僵尸程序受控主机分布图

2.木马或僵尸程序控制服务器分析

1 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 2406 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 14.0%）、江苏省（约占 11.7%）、浙江省（约占 8.4%）。具体分布情况如图 3 所示:

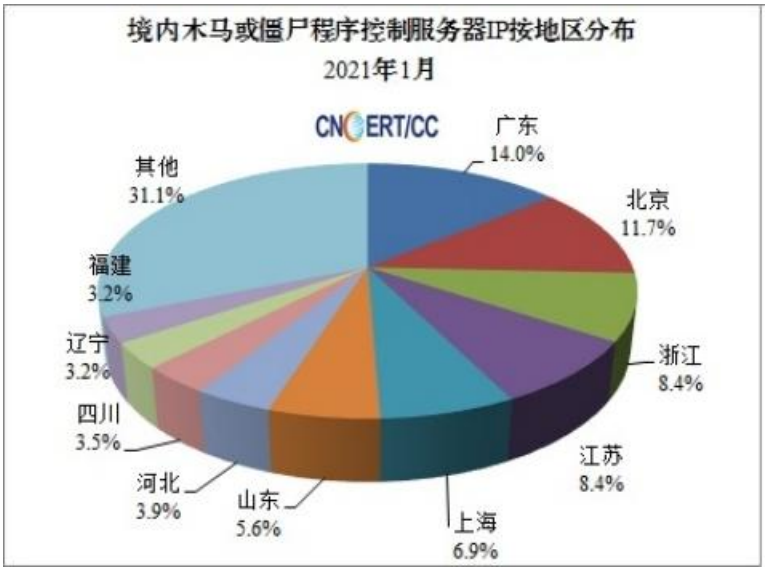

图 3 境内木马或僵尸程序控制服务器 IP 按地区分布图

1 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 0.7%，位列全国第 26 位，较上月下降 13 位。其中，阳泉、太原、吕梁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：

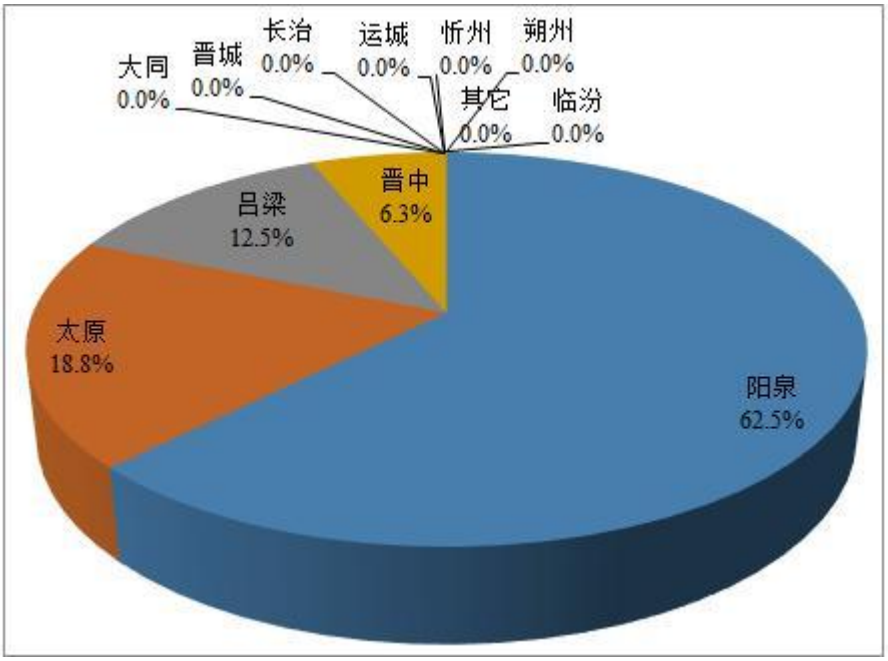

图 4 我省木马或僵尸程序控制服务器 IP 按地区分布图

3.木马或僵尸网络规模分布

1 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 6969 台，山西移动用户 379 台，山西电信用户 5932 台。

（二）网页篡改数据分析

1 月，安全中心监测发现中国大陆地区被篡改网站 12718，其中境内被篡改政府网站（.gov）数量为 77 个。被篡改网站最多的地区分别为北京市（约占 26.8%）、山东省（约占 12.3%）、广东省（约占 11.2%）。具体分布情况如图 5 所示：

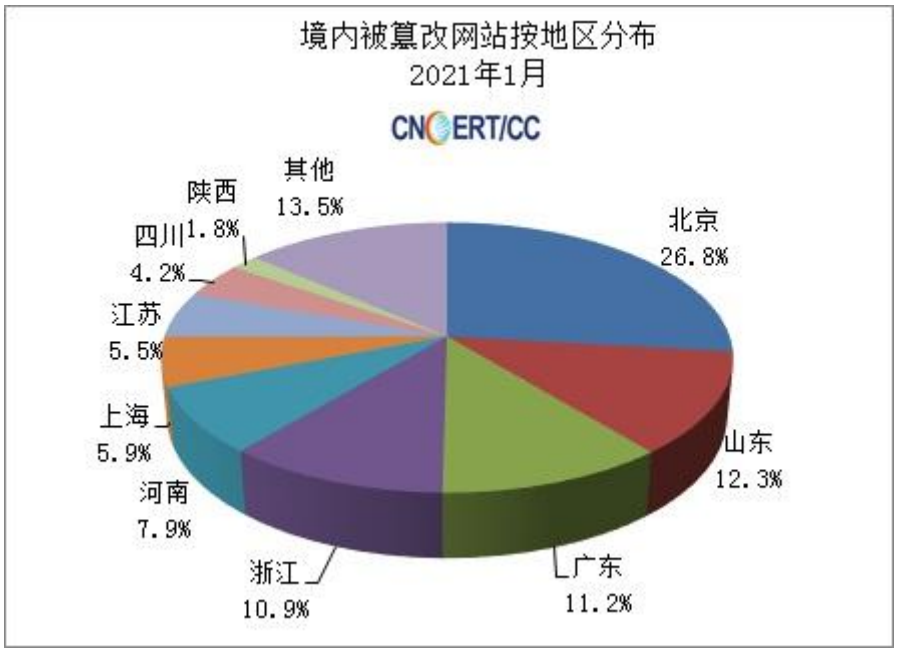

图 5 境内被篡改网站按地区分布图

1 月，安全中心山西分中心监测发现我省有 19 个网站被篡改网页，占全国被篡改网站总数的 0.15%，位列全国第 26 位，较上月下降 2 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

1月，安全中心山西分中心监测发现我省有3个网站被植入后门，占全国被植入后门网站总数的0.09%，位列全国第26位。

（四）“飞客”蠕虫数据分析

1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898台。其中，太原、运城、晋中排在全省感染“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：

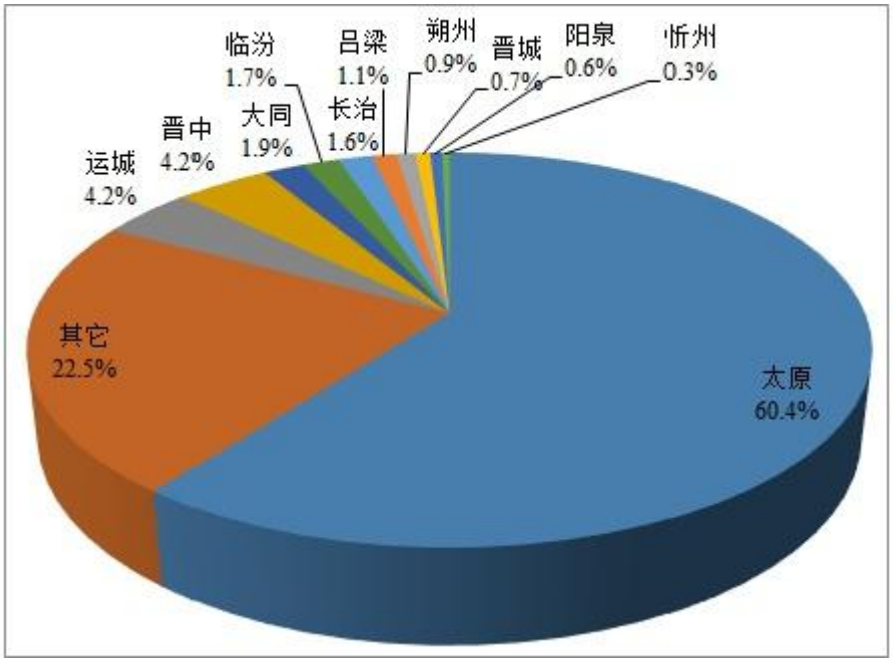

图6 我省感染“飞客”蠕虫的主机IP按地区分布图

（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

1月，安全中心国家信息安全漏洞共享平台（CNVD）收录各类漏洞1660个，包含高危漏洞570个、中危漏洞914个、低危漏洞176个，其中可远程攻击1148个，0day漏洞844个。

五、重要安全漏洞提示

（一）关于致远OA系统存在文件上传漏洞的安全公告

致远OA是由北京致远互联软件股份有限公司（以下简称致远公司）开发的一款协同办公产品，构建了面向中大型、集团组织的数字化协同运营平台。

近日，有安全人员披露了致远OA系统高危漏洞。未经身份验证的攻击者利用该漏洞，可通过精心构造恶意脚本文件，使用POST方法向目标服务器上传文件，继而通过远程代码执行植入网站后门，控制目标服务器。目前，漏洞细节已公开，厂商已发布版本补丁修复。

CNVD对该漏洞的综合评级为“高危”。

参考链接：https://www.cnvd.org.cn/webinfo/show/5959

（二）Microsoft Visual Studio远程代码执行漏洞（CNVD-2021-01041）

Microsoft Visual Studio是一个集成的开发环境，用于开发计算机程序、网站、Web应用程序、Web服务和移动应用程序。

Microsoft Visual Studio存在远程代码执行漏洞。攻击者可利用该漏洞在当前用户的上下文中执行任意代码。

CNVD对该漏洞的综合评级为“高危”。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-01041

六、要闻回顾

（一）国内部分

1. 2020 年电信业务量增长超两成 农村宽带用户增长较快

工业和信息化部近日对外发布 2020 年通信业统计公报。公报显示，2020 年我国通信业保持平稳运行，电信业务收入增速回升，电信业务总量较快增长。经初步核算，2020 年电信业务收入累计完成 1.36 万亿元，比上年增长 3.6%，增速同比提高 2.9 个百分点。按照上年价格计算的电信业务总量 1.5 万亿元，同比增长 20.6%。

从网络速率和普遍服务水平来看，2020 年，我国 4G 用户总数达到 12.89 亿户，全年净增 679 万户，占移动电话用户数的 80.8%。全国行政村通光纤和 4G 比例均超过 98%，电信普遍服务试点地区平均下载速率超过 70M，农村和城市实现“同网同速”。

2. 国家网信办修订《互联网用户公众账号信息服务管理规定》发布施行

国家互联网信息办公室 1 月 22 日发布新修订的《互联网用户公众账号信息服务管理规定》（以下简称《规定》）。《规定》自 2021 年 2 月 22 日起施行。《规定》共 23 条，包括公众账号信息服务平台信息内容和公众账号管理主体责任、公众账号生产运营者信息内容生产和公众账号运营管理主体责任、真实身份信息认证、分级分类管理、行业自律、社会监督及行政管理等条款。

国家互联网信息办公室有关负责人表示，发布《规定》旨在进一步加强互联网用户公众账号的依法监管，促进公众账号信息服务健康有序发展。

（二）国际部分

1. 中东地区数字经济加速发展

近年来，中东国家不断寻求经济多样化转型。疫情防控期间，地区多国加大政策支持力度，不断扩大互联网基础设施建设，努力创造数字经济产业良好营商环境，助推数字化转型进程。

目前，中东国家与中国的数字合作成果显著。华为已与科威特、阿联酋、沙特、巴林等国 10 余个中东电信运营商签署技术协议，建设 5G 网络；沙特数据与人工智能局不久前与中国相关企业和机构签署合作协议，内容涉及智慧城市建设、阿拉伯语人工智能技术开发等；埃及教育部与福建网龙网络公司合作，推出在线教育产品，覆盖全埃 2200 多万学生和 100 多万教师，在因疫情停课期间提供远程学习支持，并为疫情后的教学提供长期服务；中国—阿联酋经济贸易数字展览会、中国—中东及北非（摩洛哥）国际贸易数字展览会等在线展会相继举办，运用互联网、云技术创新展会服务模式和外贸洽谈方式，深化中国与中东地区的数字经济合作。

2. 欧盟加大力度规范数字服务市场

欧盟轮值主席国葡萄牙外长席尔瓦日前表示，葡萄牙在 2021 年上半年担任欧盟轮值主席国期间，将全力推动《数字市场法》和《数字服务法》立法进程，加大力度规范网络空间。

2020 年底，欧盟公布《数字市场法》和《数字服务法》草案。欧盟认为，少数数字平台事实上成为数字市场的“守门人”，拥有规则制定权，负有特殊责任：一方面，数字平台推动创新，为消费者、客户、产业创造价值，帮助市场提升运营效率，提供发展机会；另

一方面，数字平台亟待规范，平台安全运行面临巨大挑战。因此，欧盟将构建现代法律体系，保障用户安全和基本权利，维护公平开放的在线平台环境。

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