山西省网络安全月度通报

2021 年第 4 期（总第 82 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 4 月

一、基本态势

2021 年 3 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 3 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 187 起。

2021 年 3 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）48894 条，检出疑似涉诈网页（URL）67.3 万条，疑似涉诈 APP 986 个。

（一）基础网络运行安全

3 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

3 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）5285 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 74.14%，列全国第 26 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，较上月增加 45.45%，列全国第 30 位；（3）580 个 IP 地址对应的主机感染“飞客”蠕虫病毒，较上月增加 231.43%；（4）监测发现并处置一般网络安全事件 187 起。

（三）公共互联网信息安全

3 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网页（URL）48894 条；（3）检出疑似涉诈网页（URL）67.3 万条，较上月减少 23.26%；（4）检出疑似涉诈 APP 986 个。

二、重点工作与事件

（一）试行开展山西省工业互联网企业网络安全分类分级管理工作

为深入贯彻落实《国务院关于深化“互联网+先进制造业”发展工业互联网的指导意见》（国发〔2017〕50 号）、工业和信息化部等十部门《加强工业互联网安全工作的指导意见》（工信部联网安〔2019〕168 号）等部署要求，加强我省工业互联网网络安全管理，提升工业互联网企业网络安全防护水平。我局与省工业和信息化厅联合印发《山西省通信管理局山西省工业和信息化厅关于试行开展山西省工业互联网企业网络安全分类分级管理工作的通知》（晋通管联〔2021〕7 号），决定在省内试行开展工业互联网企业网络安全分类分级管理工作。旨在通过试行开展工业互联网企业网络安全分类分级管理工作，进一步完善分类分级规则标准、定级流程，提升

工业互联网安全系列防护规范的科学性、有效性和可操作性，加快构建我省分类分级管理制度；进一步落实企业网络安全主体责任，形成可复制可推广的分类分级管理模式；总结一批工业互联网网络安全典型解决方案，选拔一批优秀示范企业、培育一批专业服务机构。

三、行业管理

（一）互联网网络安全信息通报

3 月，工业和信息化部向我局通报监测发现的事件 17 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 145 起，对 25 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

3 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

3 月，全行业共协调处置一般网络安全事件 187 起，其中：工信部通报我省网络安全事件 17 起，安全中心山西分中心协调处置 170

起。其中：僵木蠕恶意程序 142 起，网页篡改 19 起，网站被植入后门 3 起，网站漏洞 7 起，主机受控 10 起，系统漏洞 6 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

3 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 1146575 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 11.4%）、江苏省（约占 10.3%）、辽宁省（约占 8.8%）。具体分布情况如图 1 所示：

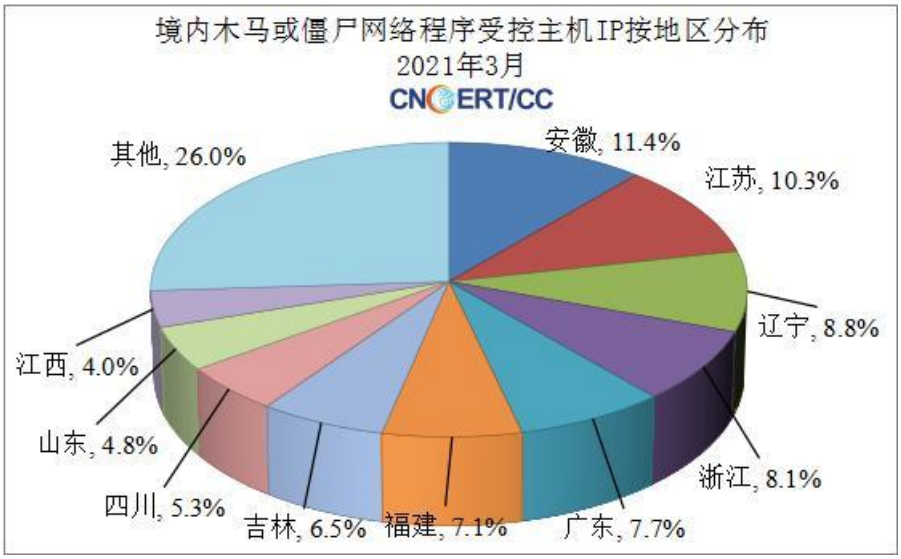

图 1 境内木马或僵尸网络程序受控主机按 IP 地区分布图

3 月，我省受感染木马或僵尸程序受控主机数量位列全国第 26 位，较上月上升 1 位，占全国受控主机总数的 0.46%。其中，晋中、

太原、临汾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:

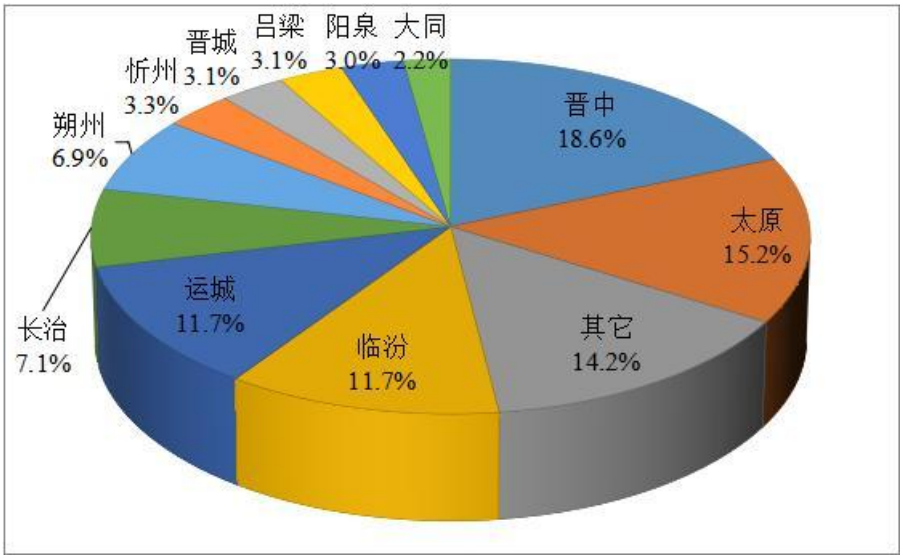

图 2 我省木马或僵尸程序受控主机分布图

2.木马或僵尸程序控制服务器分析

3 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 5662 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安徽省（约占 29.1%）、广东省（约占 8.9%）、浙江省（约占 7.3%）。具体分布情况如图 3 所示:

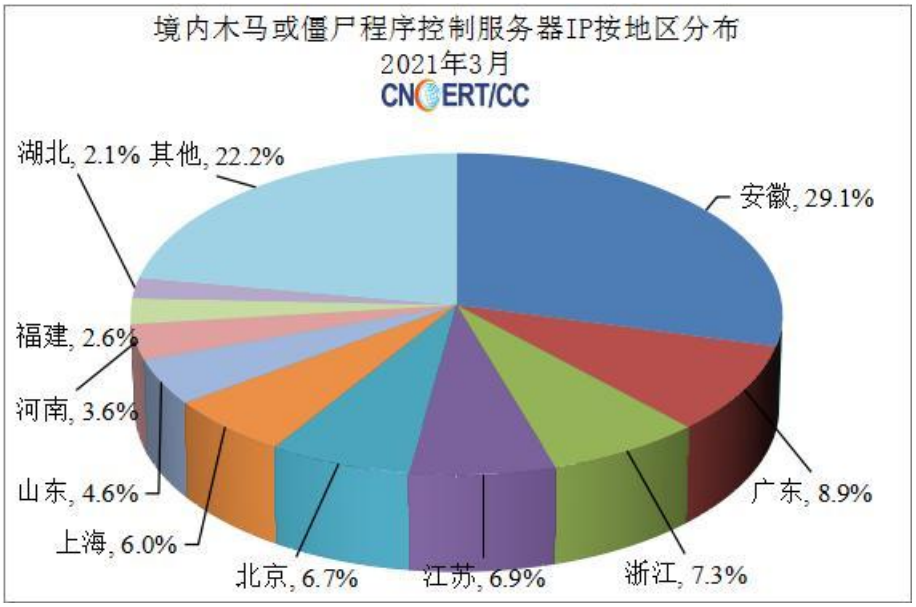

图 3 境内木马或僵尸程序控制服务器 IP 按地区分布图

3 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 0.3%，位列全国第 30 位，较上月下降 2 位。其中，阳泉、太原、晋中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：

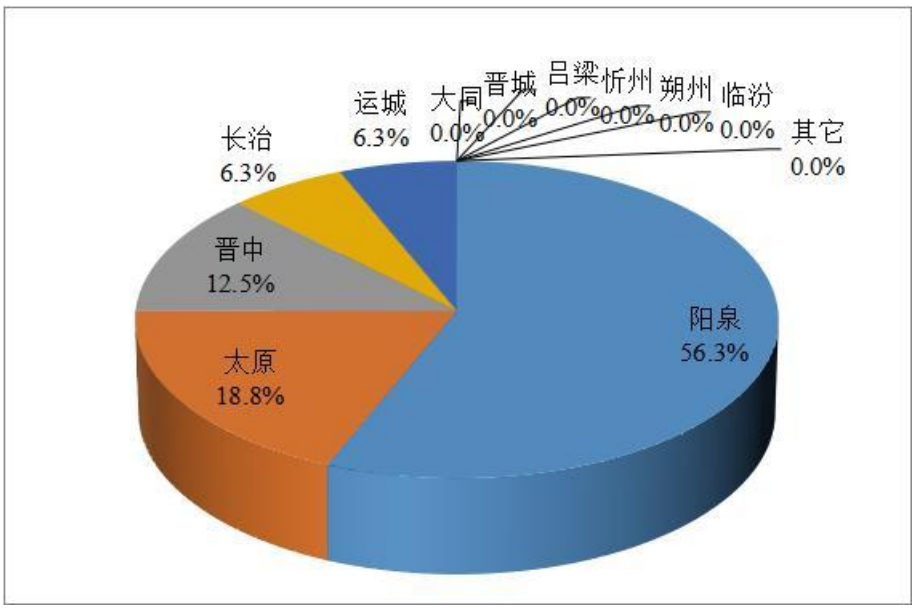

图 4 我省木马或僵尸程序控制服务器 IP 按地区分布图

3.木马或僵尸网络规模分布

3 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 2013 台，山西移动用户 275 台，山西电信用户 1510 台。

（二）网页篡改数据分析

3 月，安全中心监测发现中国大陆地区被篡改网站 12947 个，其中境内被篡改政府网站（.gov）数量为 61 个。被篡改网站最多的地区分别为北京市（约占 27.1%）、山东省（约占 12.5%）、广东省（约占 11.2%）。具体分布情况如图 5 所示：

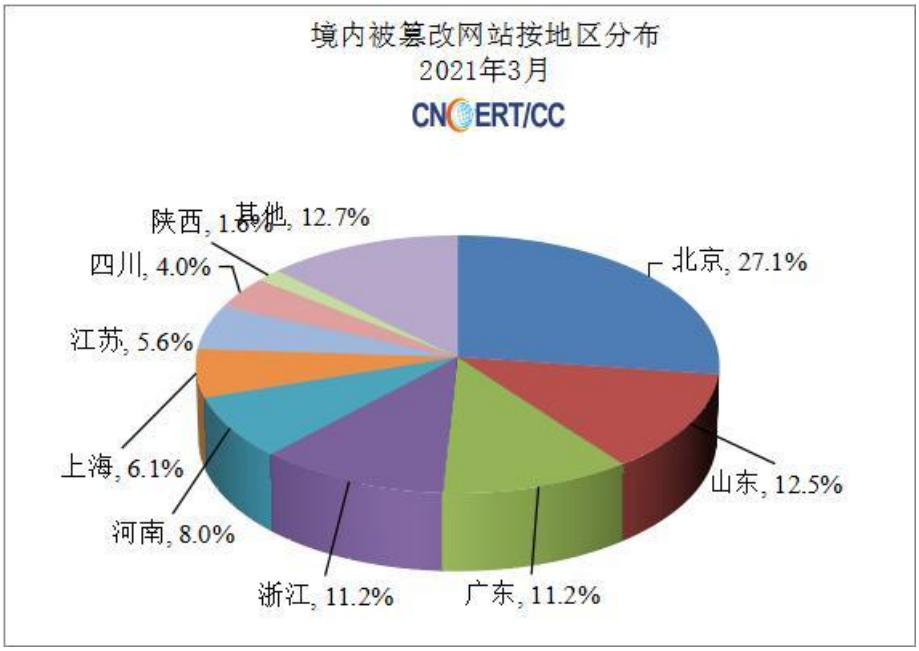

图 5 境内被篡改网站按地区分布图

3 月，安全中心山西分中心监测发现我省有 18 个网站被篡改网页，占全国被篡改网站总数的 0.14%，位列全国第 26 位，与上月持平，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

3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0.16%，位列全国第25位。

（四）“飞客”蠕虫数据分析

3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580台。其中，太原、忻州、朔州排在全省感染“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：

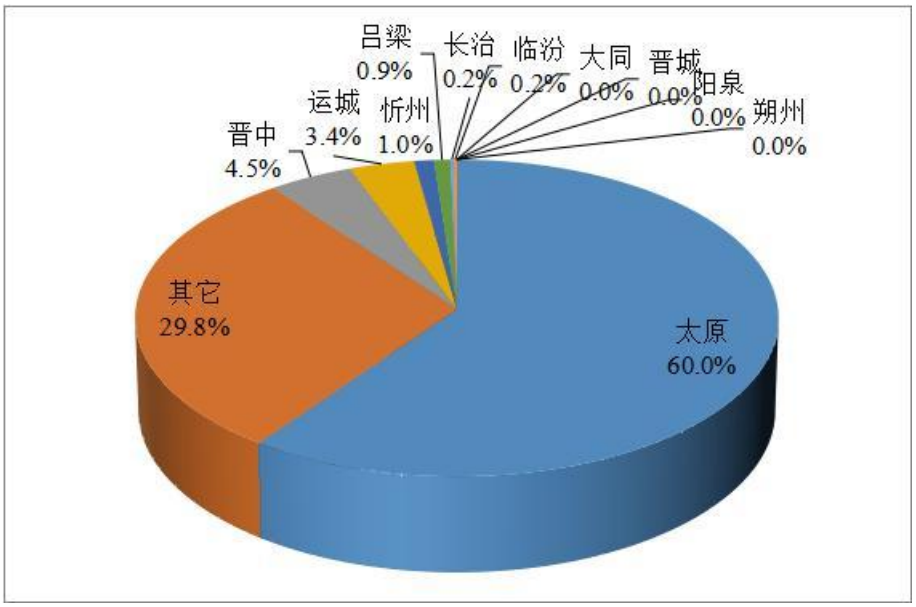

图6 我省感染“飞客”蠕虫的主机IP按地区分布图

（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

3月，安全中心国家信息安全漏洞共享平台（CNVD）收录各类漏洞2822个，包含高危漏洞692个、中危漏洞1246个、低危漏洞884个，其中可远程攻击1771个，0day漏洞1766个。

五、重要安全漏洞提示

（一）关于Microsoft Exchange Server存在多个高危漏洞的安全公告

2021年3月2日，微软公司发布了关于Exchange 服务的紧急安全更新，修复了7个相关漏洞：1）Exchange 服务端请求伪造漏洞（CVE-2021-26855）：未经授权的攻击者利用该漏洞，可发送任意HTTP请求并通过Exchange服务身份验证。2）Exchange反序列化漏洞（CVE-2021-26857）：具有管理员（administrator）权限的攻击者利用该漏洞通过发送恶意请求，实现在Exchange服务器上以SYSTEM身份的任意代码执行。该漏洞单独利用须具备较高的前提条件。3）Exchange任意文件写入漏洞（CVE-2021-26858/CVE-2021-27065）：经过Exchange服务身份验证的攻击者，利用该漏洞，可实现对服务器的任意目录文件写入。4）Exchange远程代码执行漏洞（CVE-2021-26412/CVE-2021-26854/CVE-2021-27078）：攻击者利用此漏洞，可获得目标服务器的权限，最终在服务器上的任意代码执行。

CNVD对上述漏洞的综合评级为“高危”。

参考链接：https://www.cnvd.org.cn/webinfo/show/6136

（二）Google Android Framework权限提升漏洞

Android是美国Google公司和开放手持设备联盟（简称OHA）共同开发的一套以Linux为基础的开源操作系统。Google Android 8.1、9、10、11中的Framework组件存在权限提升漏洞。攻击者可利用该漏洞

会导致本地特权升级。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-19755

六、要闻回顾

（一）国内部分

1. 国家四部门联合发布《常见类型移动互联网应用程序必要个人信息范围规定》

近日，国家互联网信息办公室、工业和信息化部、公安部、国家市场监督管理总局四部门联合发布《常见类型移动互联网应用程序必要个人信息范围规定》（以下简称《规定》），旨在落实《中华人民共和国网络安全法》关于个人信息收集合法、正当、必要的原则，规范移动互联网应用程序（App）个人信息收集行为，保障公民个人信息安全。

2. 工信部严查“诱导老年人下载 APP”等违规行为

近日，针对“3.15”晚会曝光的“诱导老年人下载 APP”、“APP 违规收集老年人个人信息”等情况，工信部针对存在欺骗误导用户下载问题的 APP，责令整改 300 款、公开通报 37 款、下架 3 款；针对存在违规处理个人信息问题的手机管家、内存优化、垃圾清理类 APP，责令整改 75 款、公开通报 20 款、下架 1 款。

（二）国际部分

1. 美国发布国家安全战略指导方针，将网络安全作为优先事项

3 月 3 日消息，美国白宫国家安全委员会公布了拜登政府的《国家安全战略中期指导方针》，其中提到，美国将提升网络安全性作

为整个政府的当务之急，增强其网络空间中的能力、准备度和应变能力，鼓励私营部门和各级政府进行合作，扩大对基础设施和人员的投资，以有效保护国家免受恶意网络活动的侵害。美国将重申其参与网络问题的国际承诺，与盟友和合作伙伴一道努力维护现有的网络空间国际规则并塑造新的全球规范。美国将要求攻击主体对破坏性的的恶意网络活动负责，通过网络和非网络手段对网络攻击迅速做出相应响应。

2. 中国同阿盟发布《数据安全合作倡议》

3 月 29 日，外交部副部长马朝旭同阿拉伯国家联盟首席助理秘书长扎齐举行中阿数据安全视频会议，双方签署并发表《中阿数据安全合作倡议》。

双方高度评价中阿双边关系发展，并一致认为，在当前数字经济迅猛发展、数据和网络安全风险突出背景下，达成《中阿数据安全合作倡议》具有重要特殊意义，标志着双方数字领域战略互信和务实合作进入新阶段。双方愿以此为契机不断深化合作，共同推动全球数字治理和国际规则制定。

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