山西省网络安全月度通报

2021 年第 5 期（总第 83 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 6 月

一、基本态势

2021 年 4 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 4 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 178 起。

2021 年 4 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）28566 条，检出疑似涉诈网页（URL）4.1 万条，疑似涉诈 APP 2696 个。

（一）基础网络运行安全

4 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

4 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）7643 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44.62%，列全国第26位；（2）11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31.25%，列全国第31位；（3）241个IP地址对应的主机感染“飞客”蠕虫病毒，较上月减少58.45%；（4）监测发现并处置一般网络安全事件178起。

（三）公共互联网信息安全

4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）28566条，较上月减少41.58%；（3）检出疑似涉诈网页（URL）4.1万条；（4）检出疑似涉诈APP 2696个，较上月增加173.43%。

二、重点工作与事件

（一）我局部署省内信息通信业建党一百周网络安全保障

按照部、省要求，结合我省网络安全现状，我局印发省内信息通信业庆祝建党一百周年网络安全保障方案，梳理重点保障对象清单，与省内基础电信企业、增值电信企业等建立专项保障机制，要求省内基础电信企业制定专项保障方案，与重点保障对象对接，同时指导开展对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。

三、行业管理

（一）互联网网络安全信息通报

4月，工业和信息化部向我局通报监测发现的事件9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146起，对23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

4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11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

4月，全行业共协调处置一般网络安全事件178起，其中：工信部通报我省网络安全事件9起，安全中心山西分中心协调处置169起。其中：僵木蠕恶意程序145起，移动互联网恶意程序1起，网页篡改10起，网站被植入后门9起，网站漏洞5起，主机受控7起，系统漏洞1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

4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

1571151 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浙江省（约占 11.4%）、江苏省（约占 9.8%）、安徽省（约占 9.6%）。具体分布情况如图 1 所示:

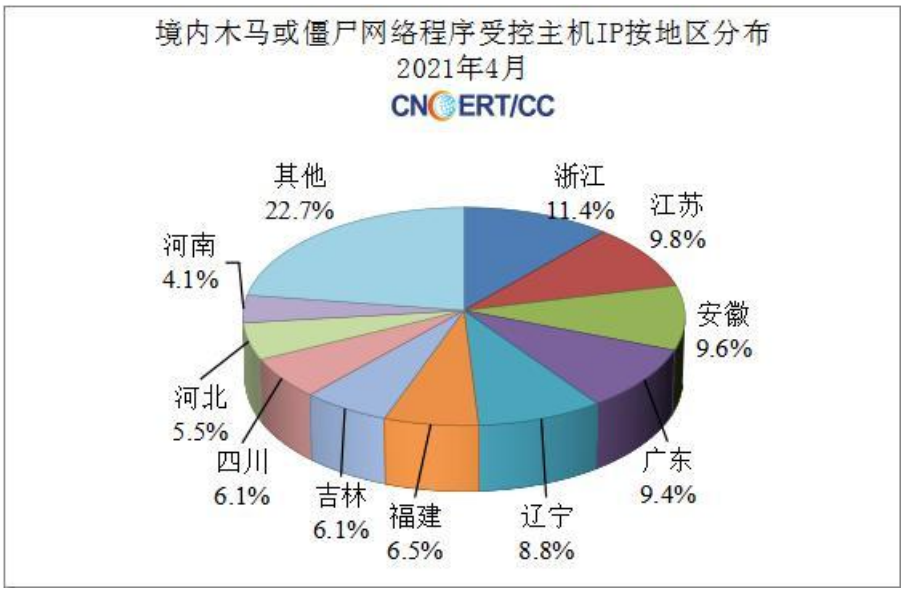

图 1 境内木马或僵尸网络程序受控主机按 IP 地区分布图

4 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，与上月持平，占全国受控主机总数的 0.48%。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:

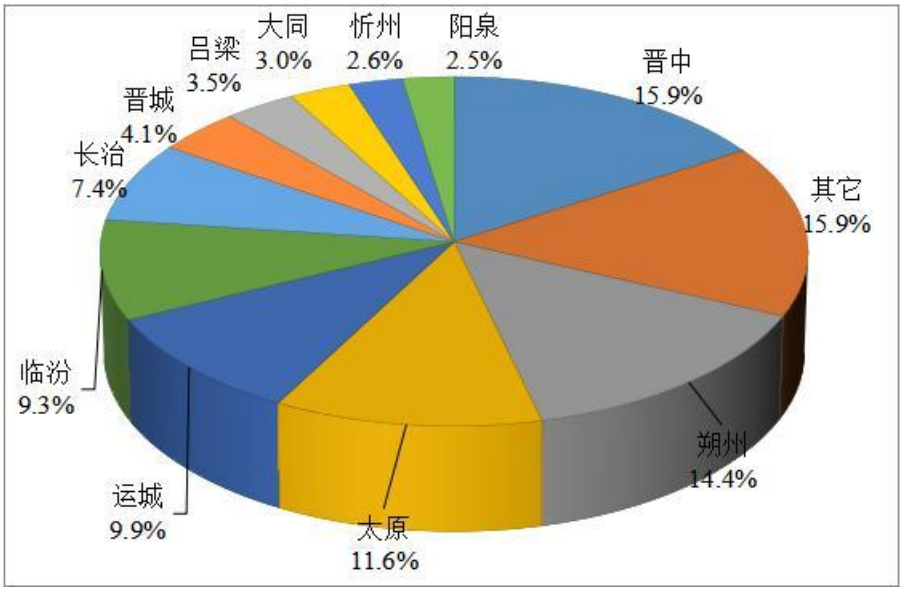

图 2 我省木马或僵尸程序受控主机分布图

2.木马或僵尸程序控制服务器分析

4 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 15581 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 33.6%）、福建省（约占 15.9%）、广东省（约占 6.0%）。具体分布情况如图 3 所示：

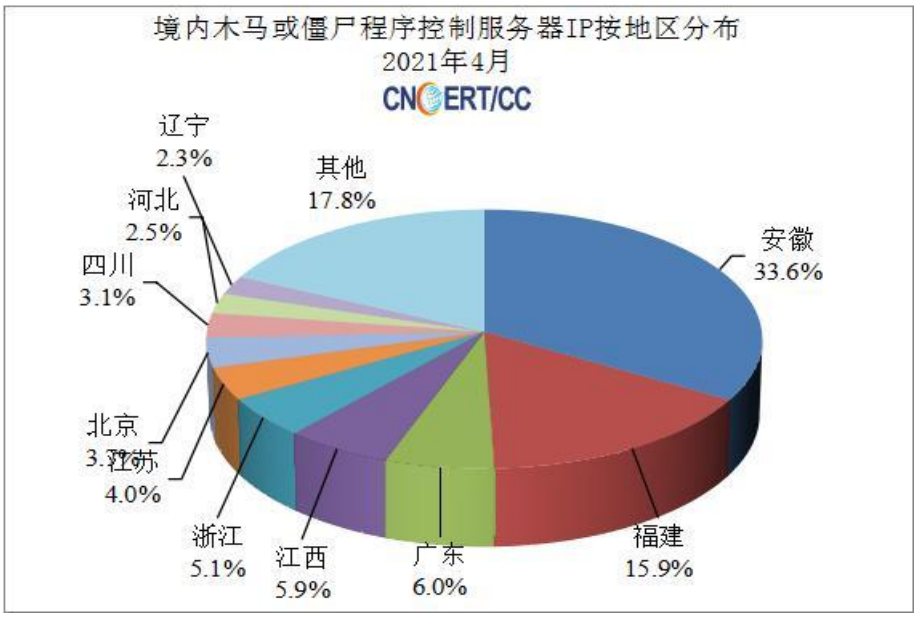

图 3 境内木马或僵尸程序控制服务器 IP 按地区分布图

4 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 0.07%，位列全国第 31 位，较上月下降 1 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：

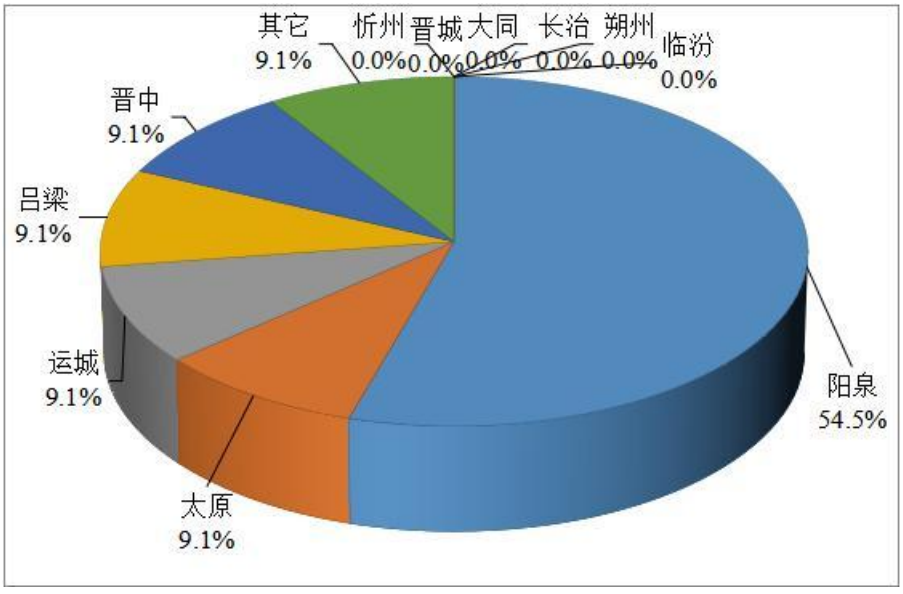

图 4 我省木马或僵尸程序控制服务器 IP 按地区分布图

3.木马或僵尸网络规模分布

4 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 2912 台，山西移动用户 567 台，山西电信用户 2887 台。

（二）网页篡改数据分析

4 月，安全中心监测发现中国大陆地区被篡改网站 3188 个，其中境内被篡改政府网站（.gov）数量为 8 个。被篡改网站最多的地区分别为北京市（约占 23.9%）、山东省（约占 12.1%）、浙江省（约占 10.5%）。具体分布情况如图 5 所示：

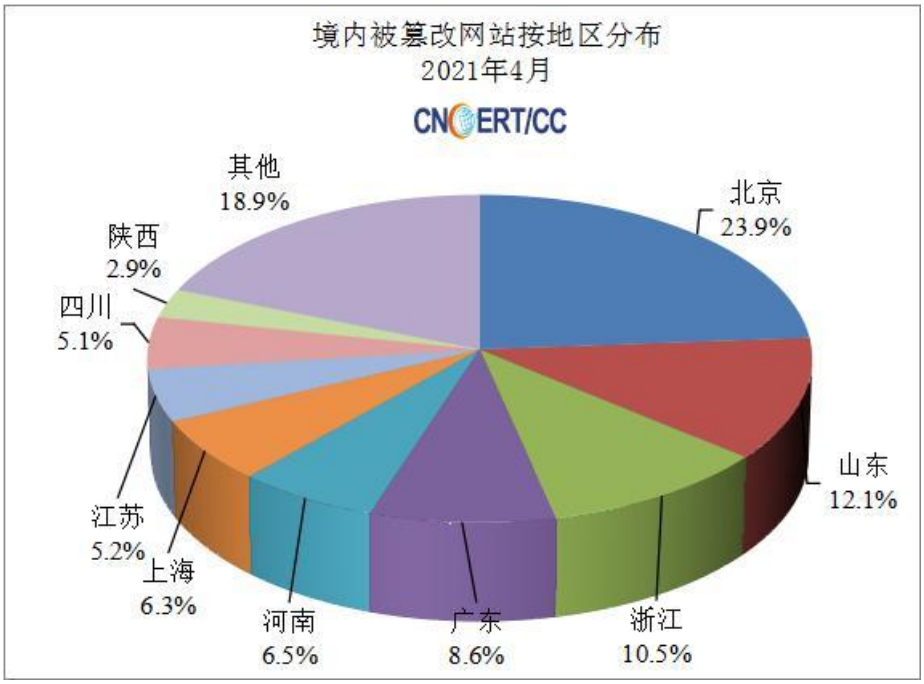

图 5 境内被篡改网站按地区分布图

4 月，安全中心山西分中心监测发现我省有 9 个网站被篡改网页，占全国被篡改网站总数的 0.28%，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

4月，安全中心山西分中心监测发现我省有9个网站被植入后门，占全国被植入后门网站总数的0.34%，位列全国第22位。

（四）“飞客”蠕虫数据分析

4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241台。其中，太原、晋中、长治排在全省感染“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：

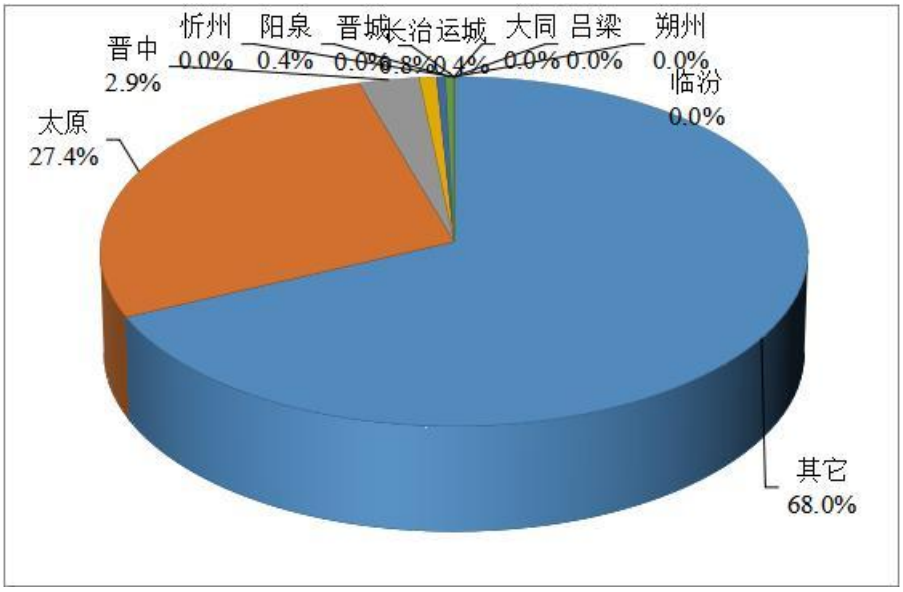

图6 我省感染“飞客”蠕虫的主机IP按地区分布图

（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

4月，安全中心国家信息安全漏洞共享平台（CNVD）收录各类漏洞2679个，包含高危漏洞695个、中危漏洞1622个、低危漏洞

362 个，其中可远程攻击 2071 个，0day 漏洞 1409 个。

五、重要安全漏洞提示

（一）关于致远OA旧版本用户存在安全隐患应及时进行修复的风险提示

2021年4月10日，国家信息安全漏洞共享平台（CNVD）发现致远OA旧版本的用户由于未及时更新厂商补丁，存在安全隐患。由于致远OA软件旧版本（V8.0以下，V8.0于2020年6月11日发布）集成的Fastjson组件存在反序列化漏洞，攻击者利用该漏洞，可在未授权的情况下获取目标服务器权限，实现服务器的远程代码执行。目前厂商已发布升级固件以修复漏洞，请用户及时下载补丁更新，避免漏洞引发相关的网络安全事件。

参考链接：https://www.cnvd.org.cn/webinfo/show/6296

（二）关于Google Chrome存在远程代码执行漏洞的安全公告

2021年4月14日，国家信息安全漏洞共享平台（CNVD）收录了Google Chrome远程代码执行漏洞（CNVD-2021-27989）。攻击者利用该漏洞，可在未授权的情况下远程执行代码。目前厂商已发布升级固件以修复漏洞，请用户及时下载补丁更新，避免漏洞引发相关的网络安全事件。

参考链接：https://www.cnvd.org.cn/webinfo/show/6326

六、要闻回顾

（一）国内部分

1. 国家七部门联合发布《网络直播营销管理办法（试行）》

近日，国家互联网信息办公室、公安部、商务部、文化和旅游部、国家税务总局、国家市场监督管理总局、国家广播电视总局等七部门联合发布《网络直播营销管理办法（试行）》（以下简称《办法》），自2021年5月25日起施行。国家互联网信息办公室有关负责人表示，《办法》旨在规范网络市场秩序，维护人民群众合法权益，促进新业态健康有序发展，营造清朗网络空间。

2. 国家互联网信息办公室发布《数字中国发展报告（2020年）》

4月25日上午，国家互联网信息办公室副主任盛荣华在第四届数字中国建设峰会主论坛上发布《数字中国发展报告（2020年）》。

报告指出，“十三五”时期，各地区、各部门坚持以习近平新时代中国特色社会主义思想特别是习近平总书记关于网络强国的重要思想为指导，认真落实国家信息化战略规划部署，《“十三五”国家信息化规划》主要目标任务顺利完成，数字中国建设取得重要成就。信息基础设施建设规模全球领先，截至2020年底，网民规模增长到9.89亿，已建成5G基站71.8万个。信息技术创新能力持续提升，我国全球创新指数排名跃升至第14位。数字经济发展活力不断增强，我国数字经济核心产业增加值占GDP比重达到7.8%。数字政府服务效能显著提升，我国电子政务发展指数全球排名上升到第45位。信息便民惠民加速普及，网络空间国际合作深化拓展，信息化发展环境不断优化。

（二）国际部分

1. 法国宣布网络安全建设方针

法国总统马克龙近日宣布，法国将斥资 10 亿欧元加强网络安全建设、应对网络攻击行为。这项计划主要致力于加强网络安全人员的教育培训、探索技术解决方案，以更好地保护企业和社区。根据计划，法国政府将斥资 1.4 亿欧元用于相关人员的教育和培训，并建设占地 2 万平方米的“网络校园”。据介绍，这个校园不仅提供培训，还汇集了网络安全领域 60 多个公私机构，是一个更有效率、更安全的网络建设“孵化器”。

2. 南非加快数字产业发展

南非通信与数字技术部日前向国会提交了一份加快数字与云技术发展的议案，旨在增强国家数字服务能力，提高政府数据分析研判水平，保障南非数据主权与安全。

根据规划，南非将整合两家国有数字技术企业，成立国家数字基础公司。该公司有权兼容南非电力公司、南非公路局、南非运输公司等国有企业的数据库，实现大数据统一管理。此外，南非还将新建一个高性能计算与数据处理中心，整合现有公共数字资源，为国家各部门、各级机构、企业、大学、民间社会组织等提供数字云服务。为确保该中心数据服务的连续性，政府还将建设两个数据备份中心和独立的配套供电系统，确保系统不间断运行。

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