山西省网络安全月度通报

2020 年第 12 期（总第 78 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　　2020 年 12 月

一、基本态势

2020 年 11 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 11 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 198 起。

2020 年 11 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）3782 条，检出疑似涉诈 URL5.4 万条，疑似涉诈 APP3437 个。

（一）基础网络运行安全

11 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

11 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）22806 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349.7%，列全国第14位；（2）5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66.7%，列全国第22位；（3）3839个IP地址对应的主机感染“飞客”蠕虫病毒，较上月增加13.2%，列全国第15位；（4）监测发现并处置一般网络安全事件198起。

（三）公共互联网信息安全

11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173个；（2）发现并处置违法违规URL3782条；（3）检出疑似涉诈URL5.4万条，较上月减少12.5%；（4）检出疑似涉诈APP3437个，较上月减少25.7%。

二、重点工作与事件

（一）我局圆满完成工业互联网安全联合调研工作

11月，依据前期我局与省工信厅联合印发的《山西省工业和信息化厅 山西省通信管理局关于开展工业互联网安全调研的通知》（工信厅软件字〔2020〕204号）文件要求，完成了对太原、大同、运城、临汾、长治、晋城、吕梁等七个地市共23家企业的调研工作，调研了解各类企业现有工业互联网发展现状，宣贯工信部相关文件精神及要求，并对二级标识解析节点、工业互联网平台企业的相关系统进行技术检测，协助企业发现问题、整改漏洞、消除安全隐患，为下一步制定属地工业互联网安全试行工作方案奠定基础。

三、行业管理

（一）互联网网络安全信息通报

11 月，工业和信息化部向我局通报监测发现的事件 13 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 150 起，对 35 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

11 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 3 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

11 月，全行业共协调处置一般网络安全事件 198 起，其中：工信部通报我省网络安全事件 13 起，安全中心山西分中心协调处置 185 起。其中：僵木蠕恶意程序 150 起，移动恶意程序 2 起，信息泄露 6 起，网页篡改 21 起，网站被植入后门 4 起，网站漏洞 4 起，主机受控 8 起，恶意域名/URL 3 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

11 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 1204615 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 12.2%）、江苏省（约占 11.7%）、辽宁省（约占 9.1%）。具体分布情况如图 1 所示:

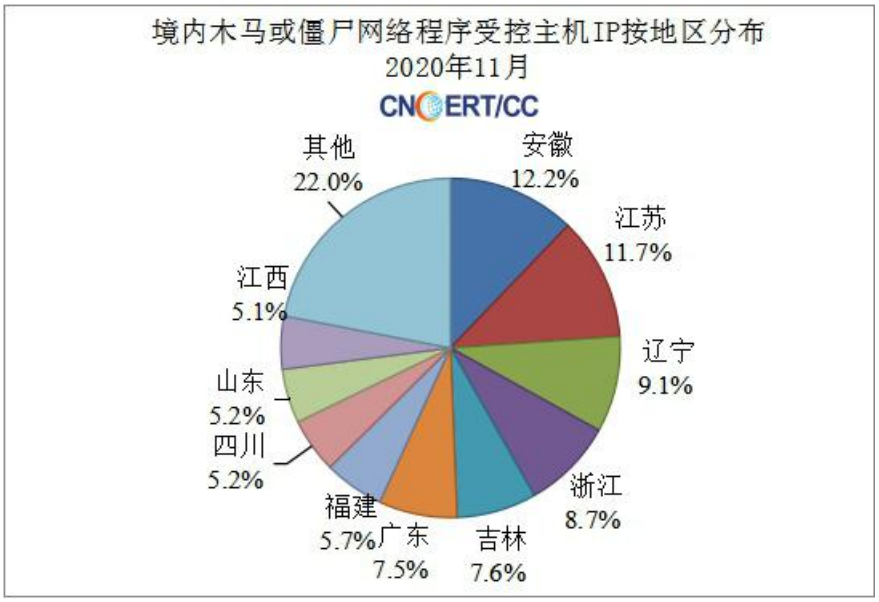

图 1 境内木马或僵尸网络程序受控主机按 IP 地区分布图

11 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，较上月上升 7 位，占全国受控主机总数的 1.89%。其中，朔州、晋中、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:

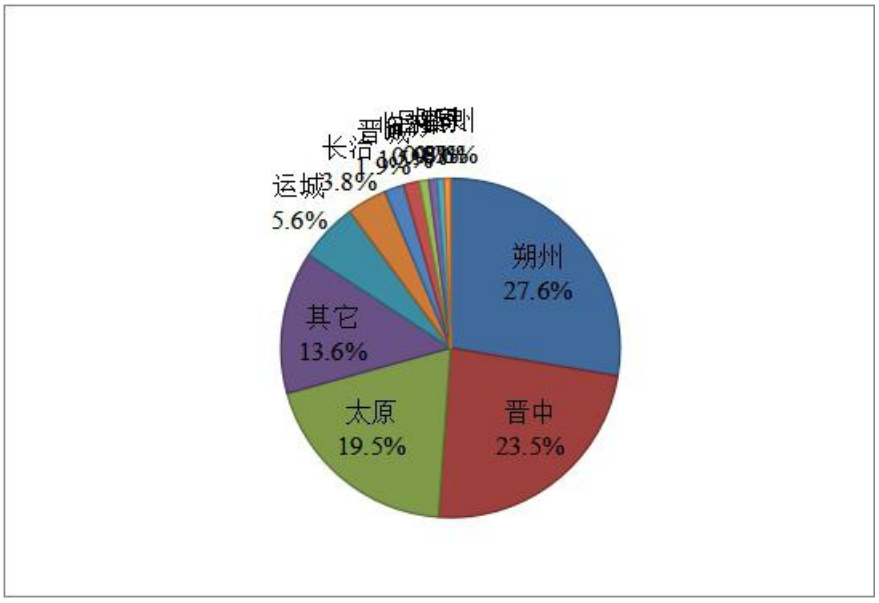

图 2 我省木马或僵尸程序受控主机分布图

2.木马或僵尸程序控制服务器分析

11 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 1299 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北京市（约占 15.6%）、上海市（约占 13.3%）、云南省（约占 11.8%）。具体分布情况如图 3 所示：

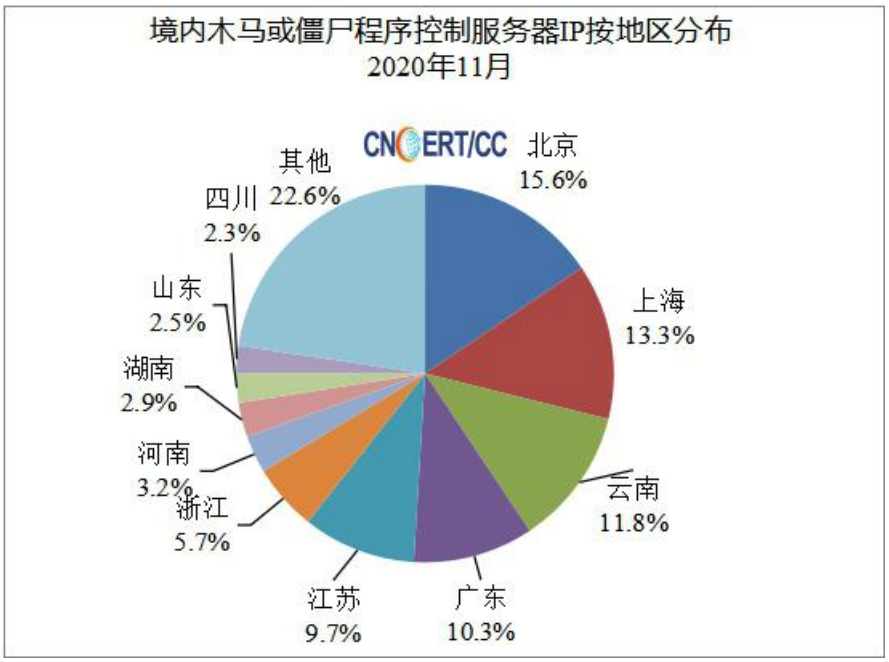

图 3 境内木马或僵尸程序控制服务器 IP 按地区分布图

11 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 0.38%，位列全国第 22 位，较上月上升 2 位。本月木马或僵尸程序控制服务器均在太原。

3.木马或僵尸网络规模分布

11 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 8392 台，山西移动用户 354 台，山西电信用户 7654 台。

（二）网页篡改数据分析

11 月，安全中心监测发现中国大陆地区被篡改网站 16114 个，其中境内被篡改政府网站（.gov）数量为 96 个。被篡改网站最多的地区分别为北京市（约占 27.0%）、山东省（约占 13.2%）、广东省（约占 10.5%）。具体分布情况如图 4 所示:

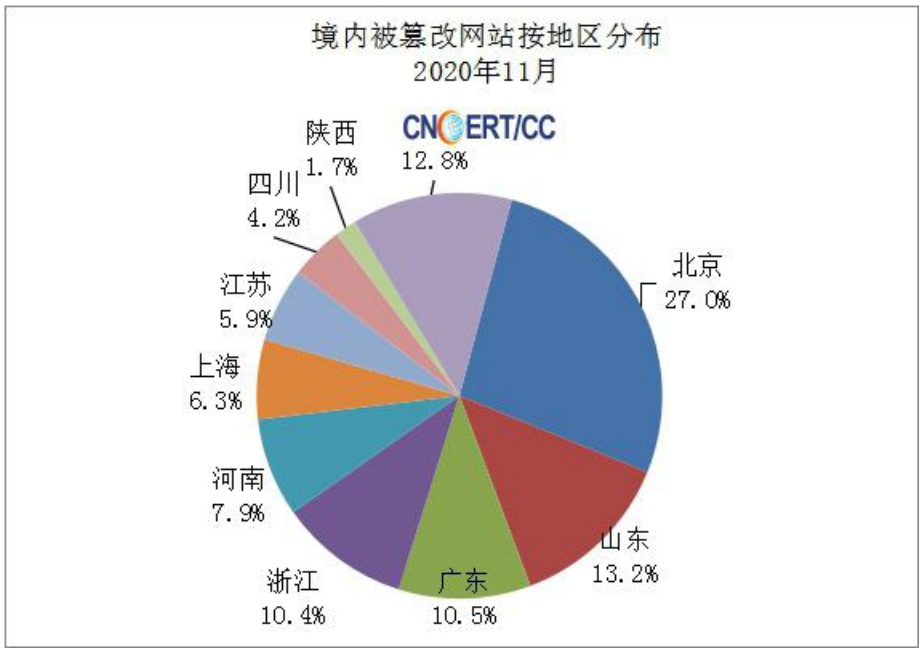

图 4 境内被篡改网站按地区分布图

11 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 0.12%，位列全国第 25 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

11 月，安全中心山西分中心监测发现我省有 4 个网站被植入后门，占全国被植入后门网站总数的 0.14%，位列全国第 24 位。

（四）“飞客”蠕虫数据分析

11 月，安全中心对“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 192816 个。事件高发的三个省份分别为广东省（约占 26.7%）、浙江省（约占 6.2%）和江苏省（约占 5.9%），具体分布情况如图 5 所示:

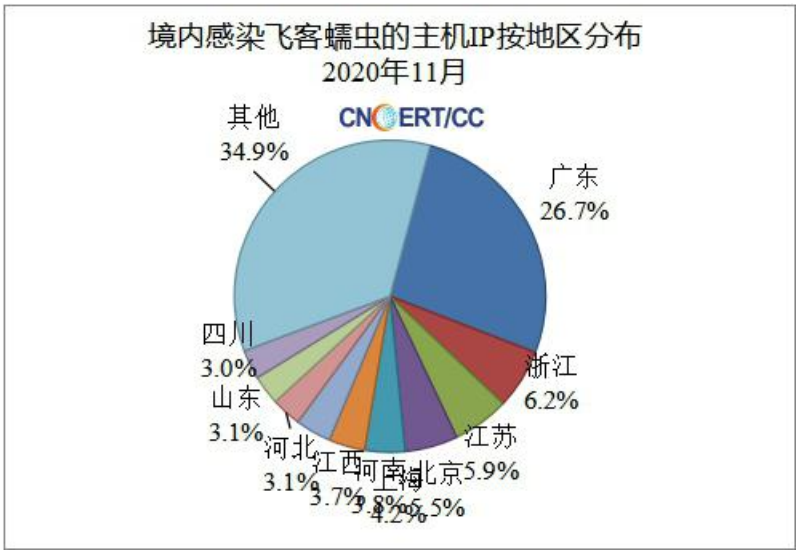

图 5 境内感染飞客蠕虫的主机 IP 按地区分布图

11 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 3839 台，占全国受感染总数的 1.99%，位列全国第 15 位，较上月上升 4 位。具体分布情况如图 6 所示:

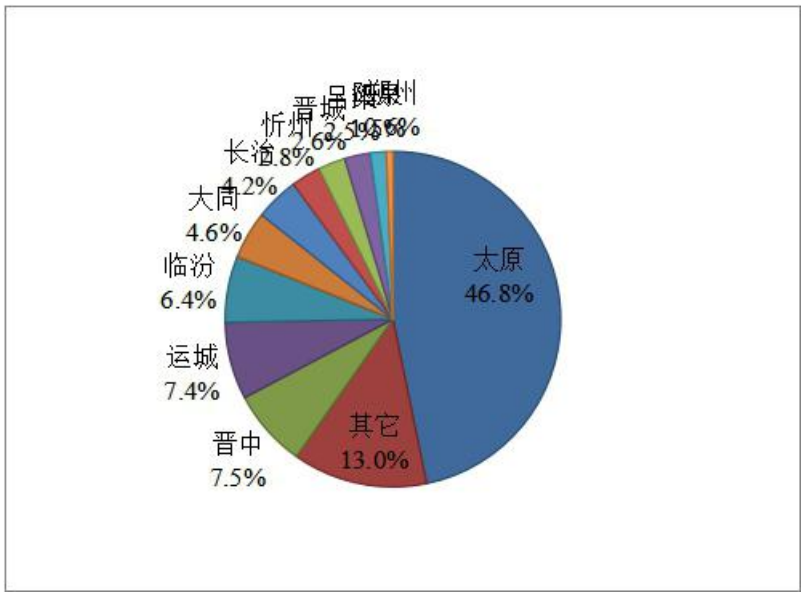

图 6 我省感染“飞客”蠕虫的主机 IP 按地区分布图

（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

11 月，安全中心国家信息安全漏洞共享平台（CNVD）收录各类漏洞 1976 个，包含高危漏洞 590 个、中危漏洞 1037 个、低危漏洞 349 个，其中可远程攻击 1474 个。

五、重要安全漏洞提示

（一）Paradox IP150缓冲区溢出漏洞

Paradox IP150是一个提供通过网络来监控管理Paradox设备的通信模块。本周，Paradox IP150被披露存在缓冲区溢出漏洞。远程攻击者可利用该漏洞提交特殊的请求，可以应用程序上下文执行任意代码或使应用程序崩溃。目前，厂商尚未发布上述漏洞的修补程序。CNVD提醒广大用户随时关注厂商主页，以获取最新版本。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-66574

（二）Oracle WebLogic Server远程代码执行漏洞

Oracle Fusion Middleware（Oracle融合中间件）是美国甲骨文（Oracle）公司的一套面向企业和云环境的业务创新平台。该平台提供了中间件、软件集合等功能。Oracle WebLogic ServerOracle Fusion Middleware Console 多版本存在安全漏洞，未经身份验证的攻击者可以利用该漏洞通过HTTP访问网络，从而破坏Oracle WebLogic Server。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-61040

六、要闻回顾

（一）国内部分

1. 中国网络空间安全协会等联合发起成立智能网安研究中心

为贯彻落实党的十九届五中全会精神，加快建设科技强国，坚定不移建设网络强国，近日，在中国网络空间安全协会主办、南开大学承办的“网安中国行”智能网络安全论坛上，由天津市委网信办、中国网络空间安全协会、中国新一代人工智能发展战略研究院联合发起的智能网络安全研究中心正式设立。南开大学原校长、世界工程师协会主席、中国新一代人工智能发展战略研究院执行院长龚克主持论坛，南开大学常务副校长许京军、中国网络空间安全协会秘书长李欲晓以及天津市委网信办副主任徐滨彦出席致辞，并共同为智能网络安全研究中心揭牌。近三年来，我国工业互联网基础设施建设稳步推进、应用创新生态持续壮大、经济社会贡献不断增强。特别是今年以来，以工业互联网为代表的新基建成为对冲疫情影响和经济下行压力的有力抓手。

2. 5G 为数字化转型插上翅膀

正式商用一年来，我国 5G 发展驶入快车道。截至 9 月底，全国已开通 5G 基站 69 万个，提前完成 2020 年 5G 基站建设目标。目前，我国已经基本实现了地市级 5G 网络覆盖。在电信运营商、设备厂商、行业企业的共同努力下，5G 在各行业应用加速落地，以其代表的信息通信基础设施也逐渐产生强大的推动作用，为数字化、智能化转型注入新动力。

不容忽视的是，目前国内 5G 发展仍面临建网运营成本较高、计费机制不完善等问题，应用场景不够多、安全问题等也是亟待克服

的短板。比如，在5G规模部署过程中，就面临着基站站址获取难，进入成本高等问题。为此，一些地方注重资源利用的集约化，实行5G站点资源开放，大力发展智慧灯杆。

（二）国际部分

1. 共享共治互联互通，打造更紧密的网络空间命运共同体

11月18日，世界互联网大会组委会发布的《携手构建网络空间命运共同体行动倡议》指出，国际社会应采取更加积极、包容、协调、普惠的政策，加快全球信息基础设施建设，促进互联互通，推动数字经济创新发展。

互联网是人类共同的家园，全人类从未像今天这样在网络空间休戚与共、命运相连。维护一个和平、安全、开放、合作、有序的网络空间，就是在维护我们自己美好的家园。当今世界正经历百年未有之大变局，新冠肺炎疫情持续蔓延，给世界各国带来严重冲击。在当前疫情背景下，构建网络空间命运共同体的重要性和紧迫性更加凸显。面对新的风险和挑战，国际社会在网络空间领域应加强团结协作、维护公平正义、共享数字红利，携手构建更加紧密的网络空间命运共同体，共同开创人类更加美好的未来。

2. 沙特发布国家数据和人工智能战略

近日，沙特阿拉伯发布了一项国家数据和人工智能战略。根据该战略，到2030年，沙特将在人工智能领域吸引约200亿美元的国内外投资、培训超过2万名数据和人工智能专家、创建300多家初创企业等。沙特数据与人工智能局主席加姆迪表示，该战略旨在进

一步发展数据和人工智能产业，促进沙特经济转型。

日前在沙特召开的全球人工智能峰会上，沙特数据与人工智能局与阿里巴巴和华为等公司签署了合作协议，内容涉及智慧城市建设、阿拉伯语人工智能技术开发等。沙特表示将与中方企业携手制定人工智能人才培养计划，为沙特高校学生和研发人员提供专业培训，加强人工智能人才库建设。

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