山西省网络安全月度通报

2020 年第 11 期（总第 77 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 11 月

一、基本态势

2020 年 10 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 10 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 195 起。

2020 年 10 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）1736 个，检出疑似涉诈 URL6.2 万条，疑似涉诈 APP4625 个。

（一）基础网络运行安全

10 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

10 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）5071 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 9.8%，列全国第 21 位；（2）3 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 40%，列全国第 24 位；（3）3391 个 IP 地址对应的主机感染“飞客”蠕虫病毒，较上月增加 37.1%，列全国第 19 位；（4）监测发现并处置一般网络安全事件 144 起。

（三）公共互联网信息安全

10 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 93 个；（2）发现并处置违法违规 URL1736 个；（3）检出疑似涉诈 URL6.2 万条，较上月增加 5.3%；（4）检出疑似涉诈 APP4625 个，较上月减少 33.23%。

二、重点工作与事件

（一）我局与省工信厅联合印发《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》

10 月，依据工信部有关文件要求及会议精神，我局与省工信厅联合制定印发了《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），对省内 12 家工业企业、6 家平台企业、2 家二级标识解析节点企业、3 家基础电信企业进行了调研，了解当前我省工业互联网发展、应用现状、企业面临的问题，为下一步与省级工业互联网安全态势感知平台的对接奠定基础。

三、行业管理

（一）互联网网络安全信息通报

10 月，工业和信息化部向我局通报监测发现的事件 16 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 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

10 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

10 月，全行业共协调处置一般网络安全事件 195 起，其中：工信部通报我省网络安全事件 16 起，安全中心山西分中心协调处置 179 起。其中：僵木蠕恶意程序 119 起，恶意程序 22 起，非授权访问 1 起，信息泄露 1 起，网页篡改 24 起，网站被植入后门 7 起，网站漏洞 5 起，主机受控 1 起，系统漏洞 3 起，恶意域名/URL 12 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

10 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 1003880 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 16.5%）、江苏省（约占 14.1%）、浙江省（约占 11.4%）。具体分布情况如图 1 所示:

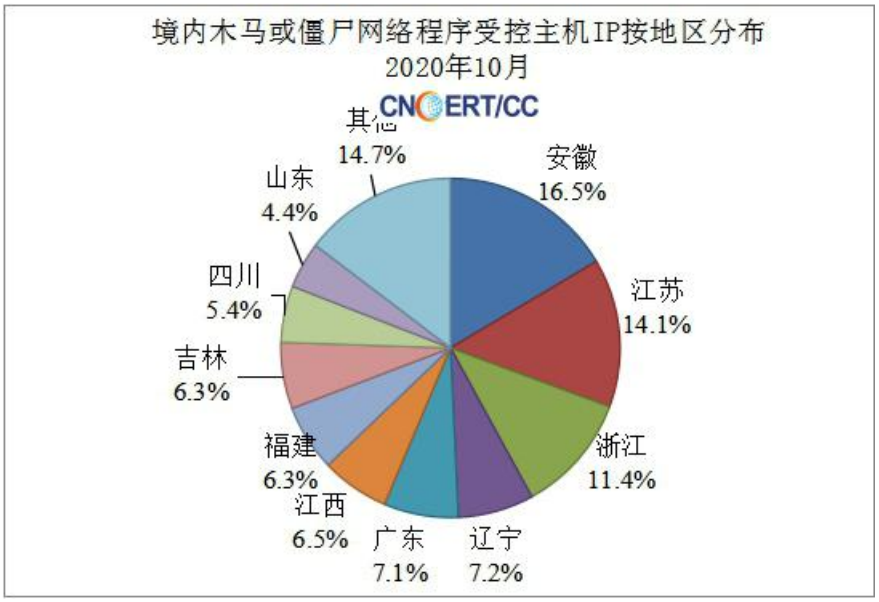

图 1 境内木马或僵尸网络程序受控主机按 IP 地区分布图

10 月，我省受感染木马或僵尸程序受控主机数量位列全国第 21 位，较上月上升 1 位，占全国受控主机总数的 0.51%。其中，太原、朔州、运城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:

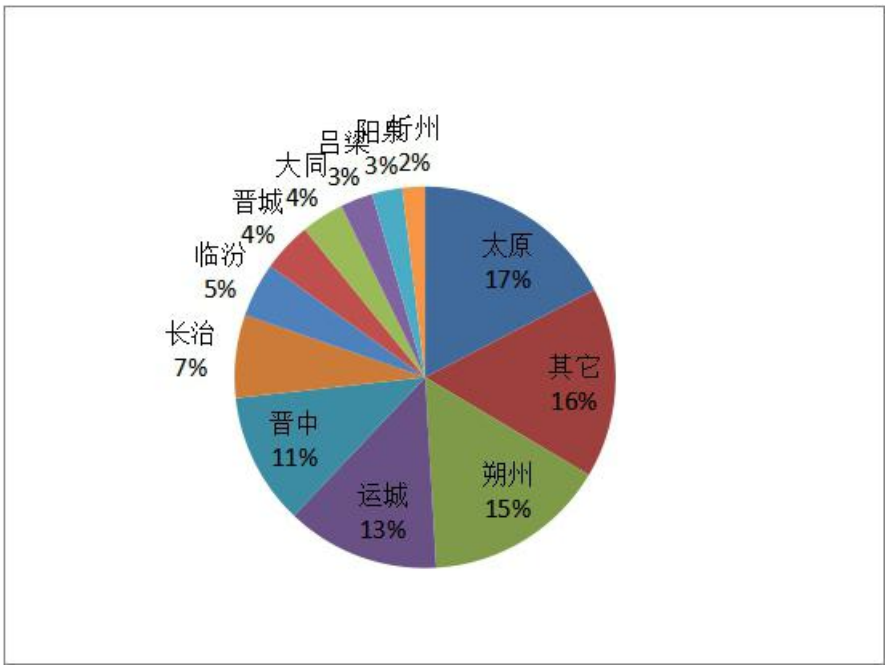

图 2 我省木马或僵尸程序受控主机分布图

2.木马或僵尸程序控制服务器分析

10 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 692 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江苏省（约占 16.5%）、北京市（约占 15.0%）、广东省（约占 14%）。具体分布情况如图 3 所示:

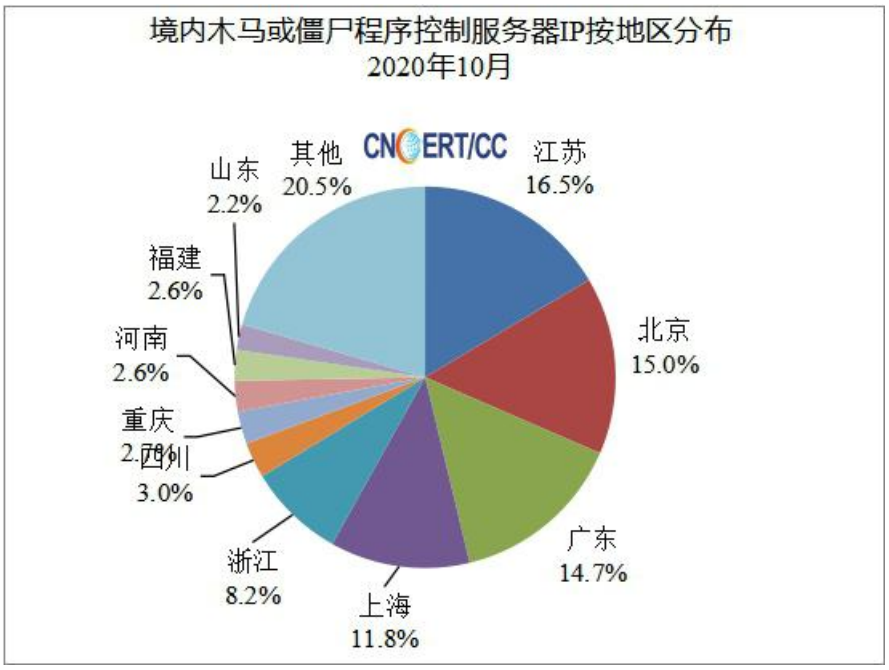

图 3 境内木马或僵尸程序控制服务器 IP 按地区分布图

10 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 0.43%，位列全国第 24 位，较上月下降 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

10 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 1400 台，山西移动用户 249 台，山西电信用户 1436 台。

（二）网页篡改数据分析

10 月，安全中心监测发现中国大陆地区被篡改网站 17955 个，其中境内被篡改政府网站（.gov）数量为 83 个。被篡改网站最多的地区分别为北京市（约占 26.2%）、山东省（约占 12.9%）、浙江省（约占 11.1%）。具体分布情况如图 4 所示:

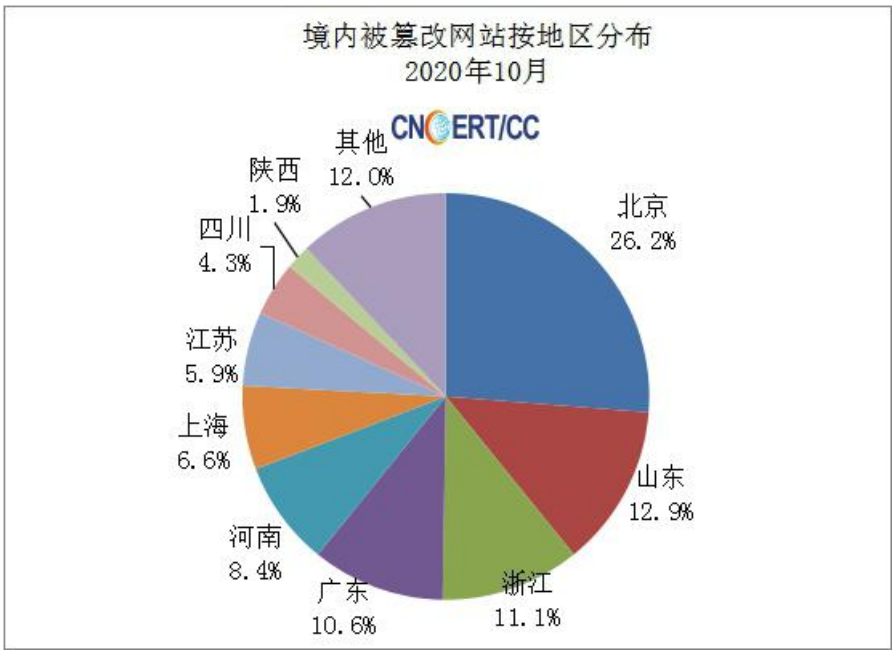

图 4 境内被篡改网站按地区分布图

10 月，安全中心山西分中心监测发现我省有 23 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 23 位，较上月上升 4 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

10 月，安全中心山西分中心监测发现我省有 7 个网站被植入后门，占全国被植入后门网站总数的 0.3%，位列全国第 21 位。

（四）“飞客”蠕虫数据分析

10 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 182699 个。事件高发的三个省份分别为广东省（约占 28.0%）、江苏省（约占 6.4%）和浙江省（约占 6.4%），具体分布情况如图 5 所示:

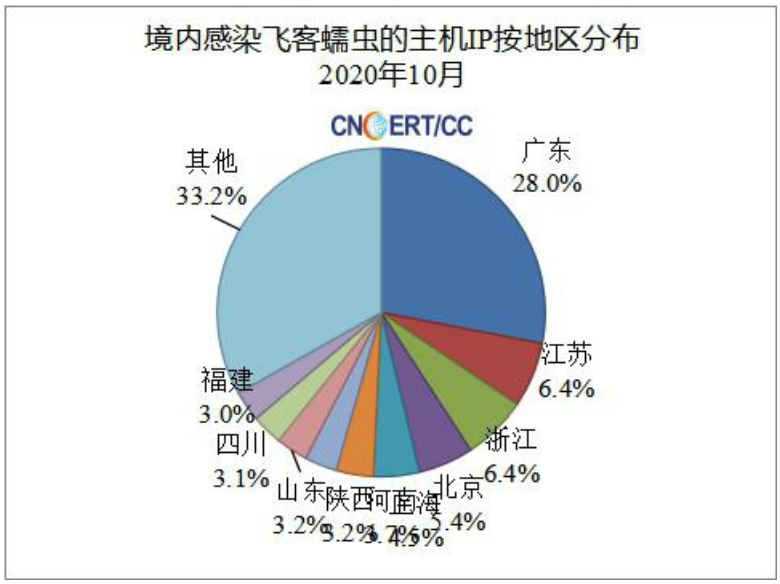

图 5 境内感染飞客蠕虫的主机 IP 按地区分布图

10 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 3391 台，占全国受感染总数的 1.86%，位列全国第 19 位，较上月持平。具体分布情况如图 6 所示:

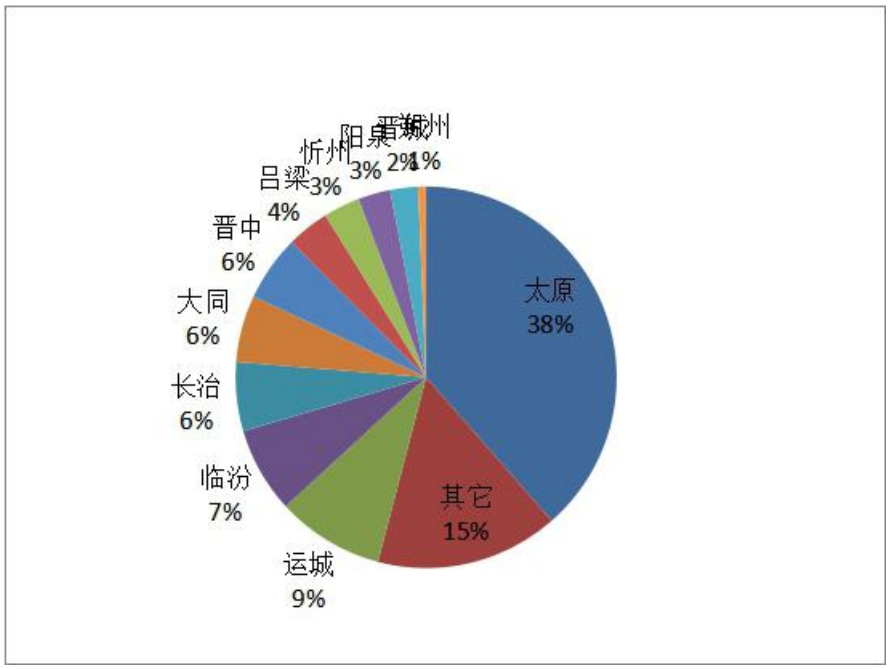

图 6 我省感染“飞客”蠕虫的主机 IP 按地区分布图

（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

10 月，安全中心国家信息安全漏洞共享平台（CNVD）收录各类漏洞 1373 个，包含高危漏洞 478 个、中危漏洞 707 个、低危漏洞 188 个，其中可远程攻击 1026 个。

五、重要安全漏洞提示

（一）Linux内核曝严重蓝牙漏洞，影响多个版本

谷歌安全研究人员在LinuxKernel中发现了一组蓝牙漏洞（BleedingTooth），该漏洞可能允许攻击者进行零点击攻击，运行任意代码或访问敏感信息。

BleedingTooth 漏洞分别被命名为 CVE-2020-12351，CVE-2020-12352和CVE-2020-24490。其中最严重的漏洞是基于堆的类型混淆漏洞（CVE-2020-12351），被评为高危漏洞 ，CVSS评分达到8.3。据悉，漏洞存在于BlueZ中，软件栈默认情况下为Linux实现了所有蓝牙核心协议和层。除Linux笔记本电脑外，它还用于许多消费或工业物联网设备。受害者蓝牙覆盖范围内的远程攻击者都可以通过目标设备的bd地址来利用此漏洞 。攻击者能够通过发送恶意的l2cap数据包来触发漏洞，导致拒绝服务，甚至执行具有内核特权的任意代码。

参考链接：https://www.cnvd.org.cn/webinfo/show/5782

（二）Foxit Reader和PhantomPDF缓冲区存在溢出漏洞

Reader是一套PDF文档阅读软件。Foxit Reader是一款PDF文档阅

读器。V8是其中的一个开源JavaScript引擎。mPDF是一款使用PHP编写的用于将HTML转换成PDF文件的库。Foxit Reader 和PhantomPDF 10.1版本存在缓冲区溢出漏洞。该漏洞源于网络系统或产品在内存上执行操作时，未正确验证数据边界，导致向关联的其他内存位置上执行了错误的读写操作。攻击者可利用该漏洞导致缓冲区溢出或堆溢出等。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-57568

六、要闻回顾

（一）国内部分

1. 工业互联网发展全面开启数字经济新时代

工业互联网作为新一代信息通信技术与制造业深度融合的关键基础设施，2017 年以来加速发展，从概念普及到行业深耕，通过全要素、全产业链、全价值链全面连接，为数字化、网络化、智能化提供实现途径，加速产业数字化进程。

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。

工业互联网通过结合新一代信息技术，正在推动数字经济与实体经济深度融合，赋能千行百业数字化转型，已经成为全面开启数字经济新时代的“金钥匙”，更是“十三五”期间助推经济社会高质量发展的重要引擎。

2. 我国立法加强个人信息保护 收集用户数据要事前告知取得同意

根据个人信息保护法草案说明，截至2020年3月，中国互联网用户已达9亿，互联网网站超过400万个，应用程序数量超过300万个，个人信息保护已成为广大人民群众最关心最直接最现实的利益问题之一。

近年来，随着大数据等技术的发展，一些网络平台擅自收集用户数据等行为，让群众反映强烈。13日首次提请全国人大常委会会议审议的个人信息保护法草案，确立以“告知——同意”为核心的个人信息处理一系列规则，有望为破解这些问题提供法律依据。

草案规定，处理个人信息应当在事先充分告知的前提下取得个人同意，并且个人有权撤回同意；重要事项发生变更的应当重新取得个人同意；不得以个人不同意为由拒绝提供产品或者服务。

个人信息处理者在处理个人信息前，应当以显著方式、清晰易懂的语言将个人信息处理者的身份、联系方式，个人信息的处理目的、处理方式，处理的个人信息种类、保存期限，个人行使本法规定权利的方式和程序等事项向个人告知。

（二）国际部分

1. 美英签署新协议在AI领域展开合作 进一步对抗中国

据外媒报道，近日特朗普政府将宣布，美国和英国已经签署了一项新协议，在人工智能的研发方面进行合作。

这项合作的主要原因是，美国及其盟友担心中国将在人工智能

领域超越他们。这种合作关系表明，美国和英国认为，通过联合，他们有更好的机会击败中国。

美国首席技术官 Michael Kratsios 说，“美国和我们的盟友必须引领世界发展尖端的人工智能技术，保护人类免受威权主义和压迫，我们自豪地与我们的特殊伙伴和盟友联合王国一道，按照共同的民主价值观，为我们公民的福祉推进人工智能创新”。

2. 2020 全球技术转移大会 欧洲多家科技项目和机构亮相

2020 全球技术转移大会（INNO-MATCH EXPO）组织了大量国内外相关团队在展会中开展对接活动，展会旨在通过“需求侧引领、供给侧发力，服务侧助力”，建立汇聚全球创新资源、助力中国创新的桥梁。

大会线下展区面积近万平方米并配套云展示，共有 32 家服务机构、40 家中小型企业以及 7 个城市国家馆参展，主要内容包括四大板块（国家重大成果 Tech-top、企业创新需求对接 Tech-need、世界桥梁 Tech-world、中小企业创新产品首发 Tech-new）和特设展区，集中展示全国一万余项技术创新需求，500 余项国际国内待转化成果，200 余项中小企业创新产品、100 项共性需求解决方案，50 余家科技服务机构。

据全球技术转移大会英国馆的承办单位 CENTI GROUP(中欧科技创新网络）创始人、董事长宰承峰表示，CENTI 作为中欧之间的互通平台，始终致力于中欧之间的技术、产业、经济和金融的发展，为实现中欧市场的双边资源互补和夯实中欧合作继续作出努力，并

相信国际性的沟通交流将带来更多中欧之间互惠互利的合作。

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