山西省网络安全月度通报

2019 年第 6 期（总第 60 期）

主办：山西省通信管理局
国家计算机网络应急技术处理协调中心山西分中心　　2019 年 6 月

一、基本态势

2019 年 5 月，我省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。本月发现木马或僵尸程序受控主机 8869 台，木马或僵尸程序控制服务器 19 台，感染“飞客”蠕虫病毒主机 2594 台。太原、运城、大同排在全省受控木马或僵尸主机活动频繁地区前三位。

（一）基础网络运行安全

5 月，我省基础网络运行总体平稳，未出现造成较大影响的运行故障，未发生三级以上网络安全事件。

（二）公共互联网安全

5 月，根据监测数据显示，我省互联网网络安全环境主要情况如下：（1）8869 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，占全省 IP 总数 0.17%，较上月减少 8.32%；（2）19 个 IP 地址对应主机感染木马或僵尸程序成为控制服务器，占全省 IP 总数 0.0004%，较上月减少 36.7%；（3）2594 个 IP 地址对应的主机感染“飞客”蠕虫病毒，占全省 IP 总数 0.05%，较上月减少 21.8%；（4）23 个网站被篡改网页，较上月增长 156%；（5）36 个网站被植入后门，较上月增长 50%。

二、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

5 月，国家互联网应急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 396111 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广东省（约占 14.1%）、山东省（约占 9.0%）、河南省（约占 8.9%）。具体分布情况如图 1 所示：

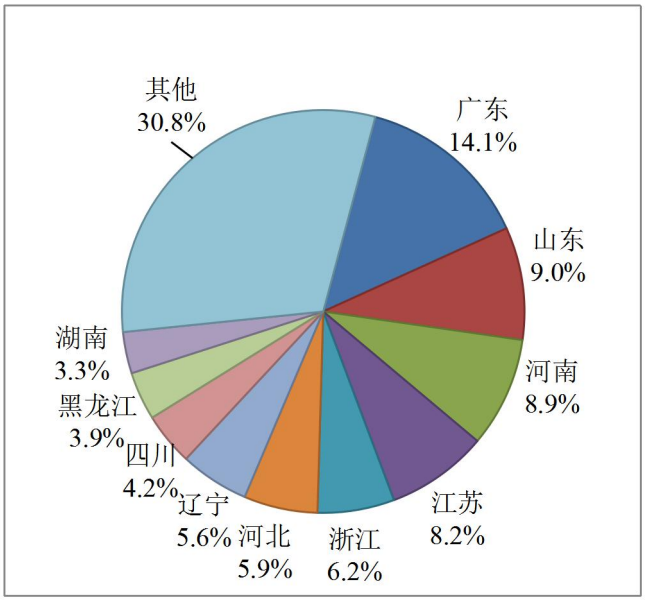

图 1 境内木马或僵尸网络程序受控主机按 IP 地区分布图

5 月，监测发现我省木马或僵尸程序受控主机 IP 地址数为 8869 个，占全国受控主机总数的 2.24%，位列全国第 16 位，较上月上升 2 位。其中，太原、运城、大同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：

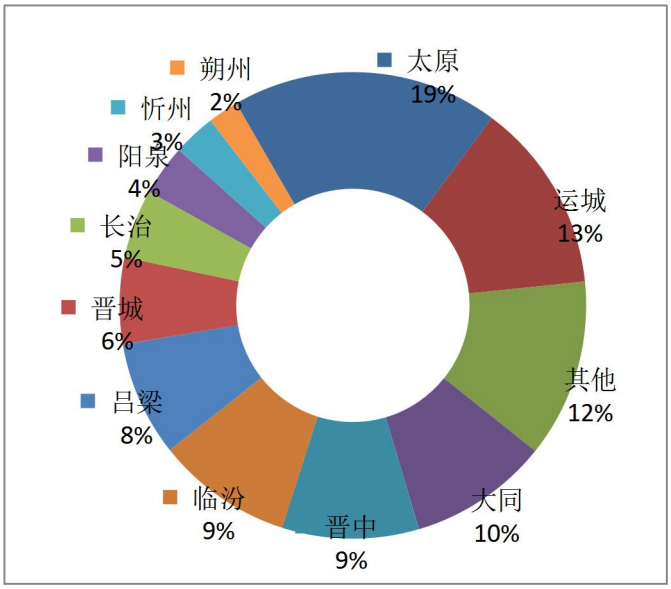

图 2 我省木马或僵尸程序受控主机分布图

2. 木马或僵尸程序控制服务器分析

5 月，国家互联网应急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 2804 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 22.1%）、北京市（约占 21.6%）、江苏省（约占 13.7%）。具体分布情况如图 3 所示：

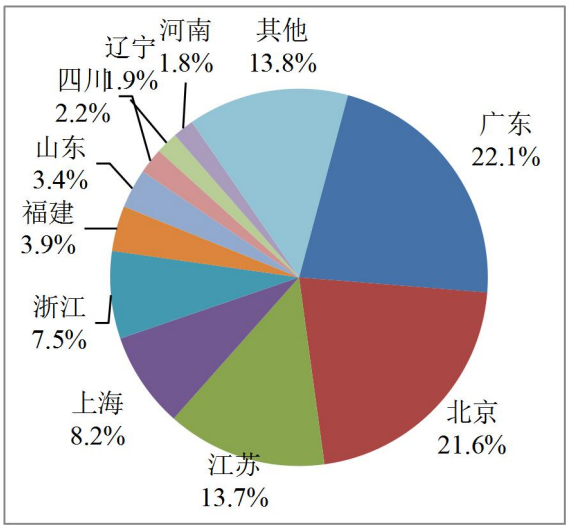

图 3 境内木马或僵尸程序控制服务器 IP 按地区分布图

5 月，我省木马或僵尸程序控制服务器 IP 地址数为 19 个，占全国控制服务器总数的 0.68%，位列全国第 17 位，与上月持平。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：

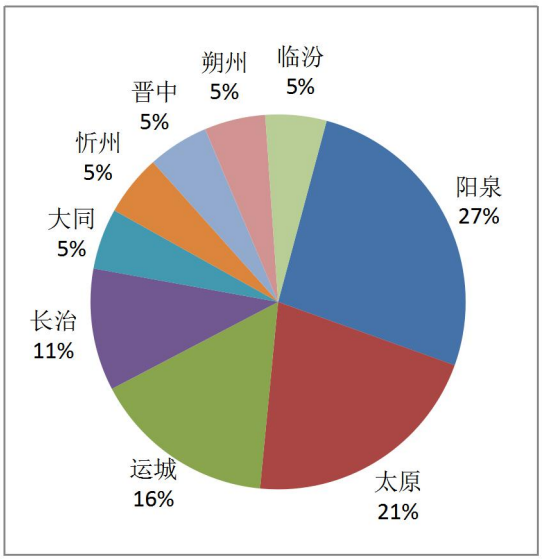

图 4 我省木马或僵尸程序控制服务器分布图

3. 木马或僵尸网络规模分布

5 月，山西互联网应急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 6074 台，山西移动 173 台，山西电信 1613 台。我省存在的较大规模僵尸网络有 4777 台受控主机。

（二）网页篡改数据分析

5 月，国家互联网应急中心监测发现中国大陆地区被篡改网站 19718 个，其中境内被篡改政府网站（.gov）数量为 55 个。被篡改网站最多的地区分别为北京市（约占 25.0%）、广东省（约占 11.5%）、山东省（约占 9.8%），具体分布情况如图 5 所示：

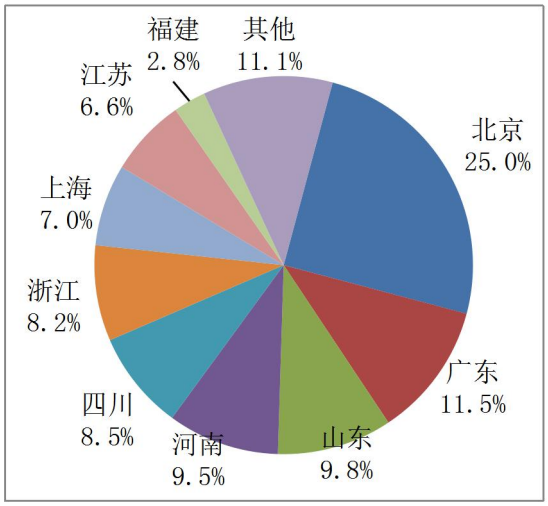

图 5 境内被篡改网站按地区分布图

5 月，我省有 23 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，较上月上升 2 位，主要的篡改攻击方式为“页面攻击”和“暗链攻击”。

（三）网站后门数据分析

5 月，我省有 36 个网站被植入后门，占全国被植入后门网站总数的 0.57%，位列全国第 24 位，较上月下降 1 位。其中政府和事业单位网站占全部被植入后门网站数量的 2.78%，同期全国的平均数为 3.59%。具体分布情况如图 6 所示：

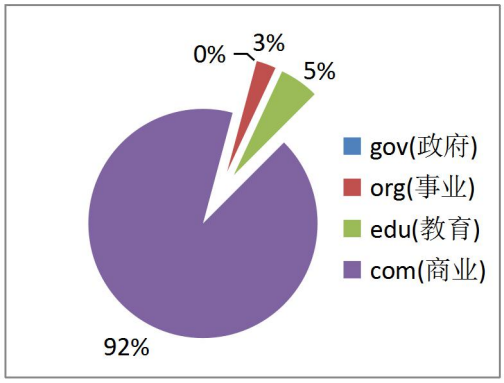

图 6 我省被植入后门网站数量按类型分布图

（四）“飞客”蠕虫数据分析

5 月，国家互联网应急中心对“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 209263 个。事件高发的三个省份分别为广东省（约占 28.2%）、江苏省（约占 7.6%）和浙江省（约占 7.4%），其分布情况如图 7 所示：

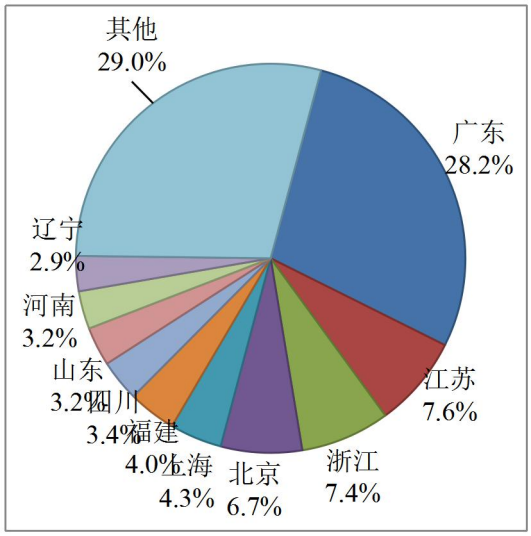

图 7 境内感染飞客蠕虫的主机 IP 按地区分布图

5 月，监测发现山西省感染“飞客”蠕虫病毒主机 2594 台，占全国受感染总数的 1.24%，位列全国第 22 位，与上月持平。具体分布情况如图 8 所示：

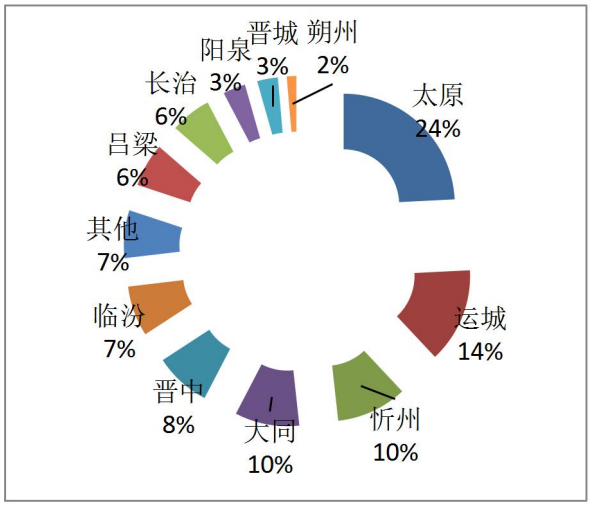

图 8 我省感染“飞客”蠕虫的主机 IP 按地区分布图

（五）移动互联网恶意程序传播服务器数据分析

5 月，未监测发现我省移动互联网恶意程序传播服务器。

（六）移动互联网新增恶意 APP 情况通报

5 月，新增移动互联网恶意 APP 应用有:

APP 名称/恶意代码名称	恶意行为	首次发现时间
a.rogue.Supe.b	远程控制	2019/5/3
a.rogue.GSexplayer.r	远程控制	2019/5/3
a.privacy.cocoam.a	远程控制	2019/5/3
a.expense.zhxapp.a	远程控制	2019/5/3
a.rogue.MalCrypt.h	远程控制	2019/5/15
a.payment.FakeInst.h	远程控制	2019/5/17
a.rogue.GSexplayer.r	远程控制	2019/5/21
a.expense.SmsSend.ft	远程控制	2019/5/21
a.rogue.sexplayer.u	远程控制	2019/5/26
a.rogue.StealMoneyGame.a	远程控制	2019/5/26

（七）安全漏洞数据分析

5 月，国家互联网应急中心收到来自国家信息安全漏洞共享平台（CNVD）报告的漏洞数量 1061 个，其中高危漏洞 306 个、中危漏洞 661 个、低危漏洞 94 个，其中 0day 漏洞 488 个，可远程攻击漏洞 936 个。

2018 年 6 月至 2019 年 5 月 CNVD 收录漏洞按月统计情况分布如图 9 所示:

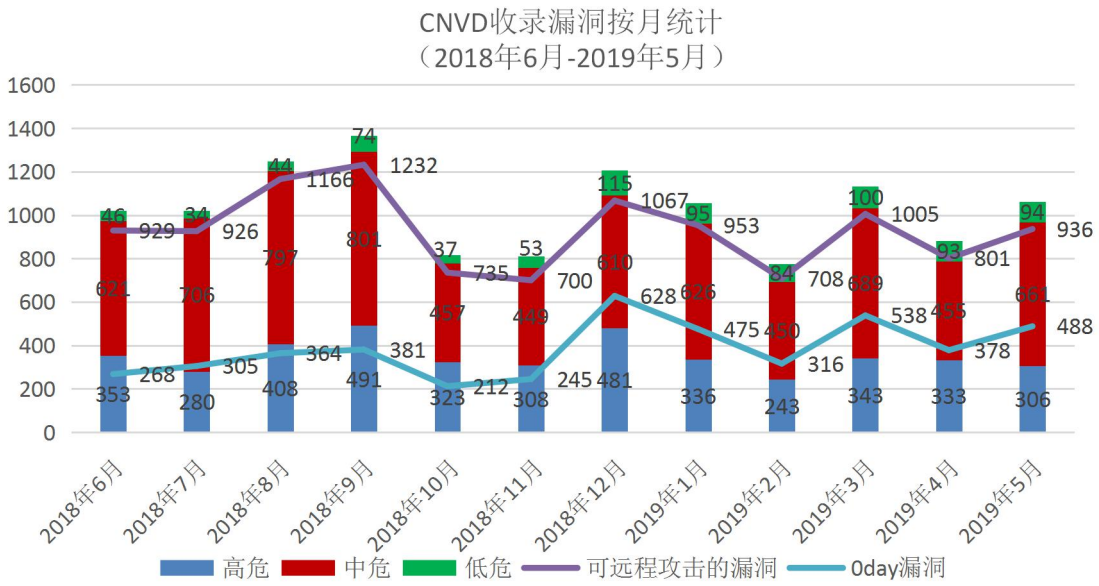

图 9 CNVD 收录漏洞按月统计情况

三、重要安全漏洞提示

（一）Microsoft Exchange Server 远程代码执行漏洞

Microsoft Exchange Server是美国微软公司（Microsoft）的一套电子邮件服务程序，它提供邮件存取、储存、转发，语音邮件，邮件过滤筛选等功能。Microsoft Exchange Server中存在远程代码执行漏洞，该漏洞源于软件未能正确处理内存中的对象，远程攻击者可利用该漏洞在系统用户的上下文中运行任意代码。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/flaw/show/CNVD-2019-14453

（二）超级 CMS 内容管理系统存在文件上传漏洞

超级 CMS 内容管理系统由 SEO 研究中心（moonseo.cn）为了解决网站优化问题而研发的一套产品，本产品采用面向

对象方式自主研发的 MVC 框架开发，它是一款开源的内容管理系统。超级 CMS 内容管理系统存在文件上传漏洞。攻击者可以利用漏洞上传 webshell，获得服务器权限。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：http://www.cnvd.org.cn/flaw/show/CNVD-2019-14578

信息编辑：国家计算机网络应急技术处理协调中心山西分中心
地　　址：太原市南内环街 2 号
电　　话：0351-8788226　　13103510088
传　　真：0351-8788113
电子邮箱：sxcert@cert.org.cn
微 信 号：shxcert(山西互联网应急中心)
二 维 码：

附录：

国家计算机网络应急技术处理协调中心山西分中心介绍

国家计算机网络应急技术处理协调中心山西分中心（以下称山西互联网应急中心）成立于2002年9月，原是工业和信息化部所属的国家计算机网络应急技术处理协调中心（以下称国家互联网应急中心）在山西省的分支机构。根据中央文件精神和整体部署，现国家互联网应急中心及各地分中心整体划转为中央网信办管理。山西互联网应急中心致力于建设山西的互联网网络安全监测中心、预警中心、应急中心，有力支撑省委网信办、山西省通信管理局履行关键信息基础设施网络安全、互联网网络安全相关监管职能；保障我省基础信息网络的安全防护和安全运行，为我省重要信息系统及关键部门提供必要的网络安全监测、预警、应急、处置、防范等安全服务和技术支持。拥有山西省范围内最为先进的互联网网络安全监测平台和功能最为强大、最为齐全的网络安全监测技术能力，能够在省际出入口、省级骨干网节点有效地监测发现网络钓鱼、网页篡改、拒绝服务攻击、恶意代码感染等网络安全事件，并协调组织实施应急处置。

山西互联网应急中心依托于国家级的网络安全监测平台、国家权威的知识库（漏洞库、病毒库、特征库）、高效的国家公共互联网网络安全应急体系、成熟的网络安全业务能力（监测发现、

通报预警、应急处置），现开展的常态化互联网网络安全工作有：

- ✧ 网络钓鱼监测与处置工作
- ✧ 木马样本分析与处置工作
- ✧ 手机应用 APP 风险评估和安全检测工作
- ✧ 假冒用户单位恶意 APP 监测与处置工作
- ✧ 互联网网络安全关口监测工作
- ✧ 域名安全事件监测与应急处置工作
- ✧ 拒绝服务攻击等流量异常事件监测与应急处置工作
- ✧ 网站安全监测与通报工作
- ✧ 安全漏洞发现与通报工作
- ✧ 联网终端安全监测与通报工作
- ✧ 案件调查与取证配合工作
- ✧ 国家网络安全态势信息通报工作
- ✧ 网络安全技术交流与培训工作