山西省网络安全月度通报

2019 年第 5 期（总第 59 期）

山西省通信管理局　　2019 年 5 月

一、基本态势

2019 年 4 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 9674 台，木马或僵尸程序控制服务器 30 台，感染“飞客”蠕虫病毒主机 3317 台。太原、运城、晋中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

4 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

4 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）9674 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 0.18%，较上月减少 12.2%;（2）30 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 0.0006%，较上月增长 42.9%;（3）3317 个 IP 地址对应的主机感染“飞客”蠕虫病毒，占全省 IP 总数 0.06%，较上月增长 17.1%;（4）9 个网站被篡改网页，较上月增长 125%;（5）24 个网站被植入后门，较上月减少 35.1%。

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

4 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 510163 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河南省（约占 11.8%）、广东省（约占 11.2%）、江苏省（约占 10.3%）。具体分布情况如图 1 所示：

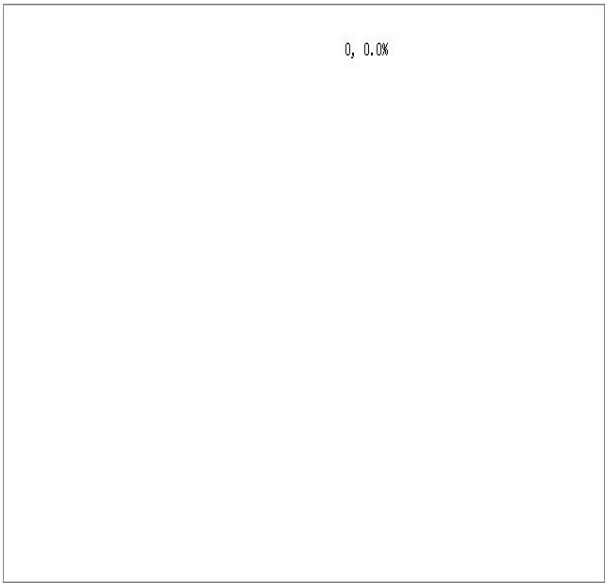

图 1 境内木马或僵尸网络程序受控主机按 IP 地区分布图

4 月，监测发现我省木马或僵尸程序受控主机 IP 地址数为 9674 个，占全国受控主机总数的 1.90%，位列全国第 18 位，较上月下降 3 位。其中，太原、运城、晋中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，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 1827 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 22.4%）、江苏省（约占 15.3%）、北京市（约占 13.6%）。具体分布情况如图 3 所示：

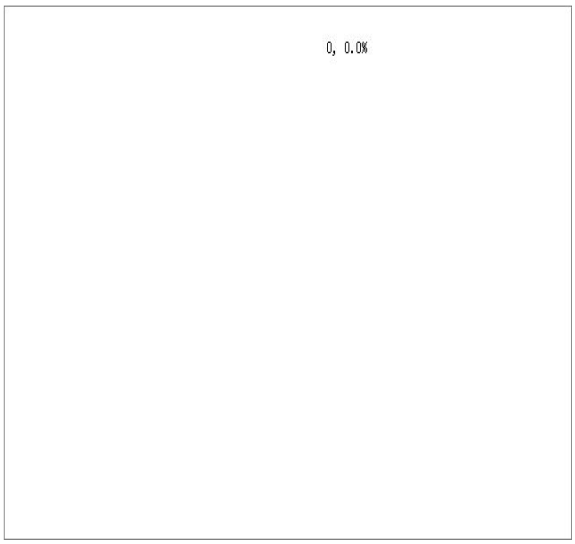

图 3 境内木马或僵尸程序控制服务器 IP 按地区分布图

4 月，我省木马或僵尸程序控制服务器 IP 地址数为 30 个，占全国控制服务器总数的 1.64%，位列全国第 17 位，较上月下降 4 位。其中，太原、阳泉、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：

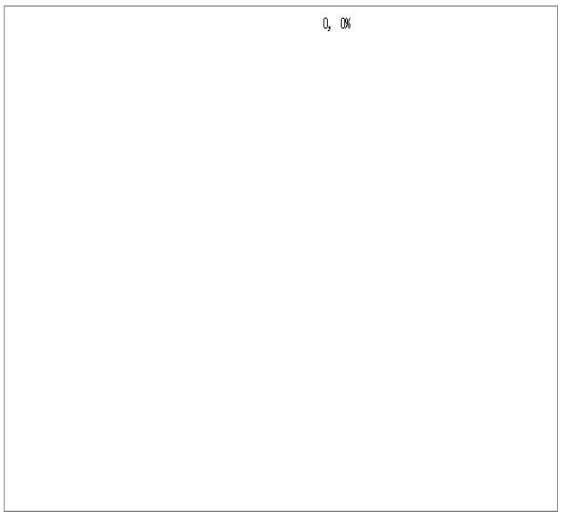

图 4 我省木马或僵尸程序控制服务器分布图

3. 木马或僵尸网络规模分布

4 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 4578 台，山西移动 986 台，山西电信 142 台。我省存在的较大规模僵尸网络有 5175 台受控主机。

（二）网页篡改数据分析

4 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 7083 个，其中境内被篡改政府网站（.gov）数量为 85 个。被篡改网站最多的地区分别为北京市（约占 24.8%）、广东省（约占 11.4%）、山东省（约占 9.3%），具体分布情况如图 5 所示：

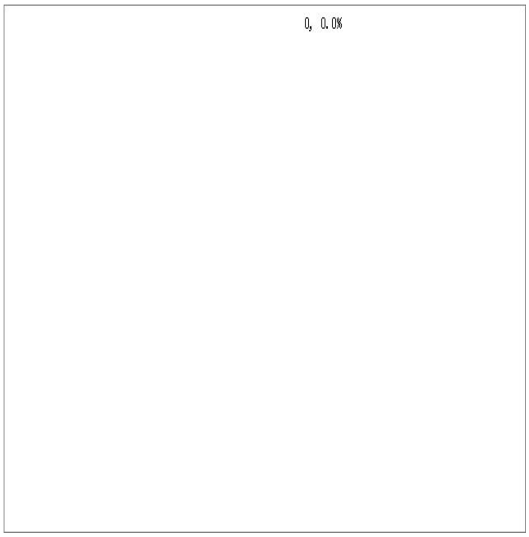

图 5 境内被篡改网站按地区分布图

4 月，我省有 9 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 27 位，较上月下降 6 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

4 月，我省有 24 个网站被植入后门，占全国被植入后门网站总数的 0.54%，位列全国第 23 位，较上月上升 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 12.5%，同期全国的平均数为 3.7%。具体分布情况如图 6 所示：

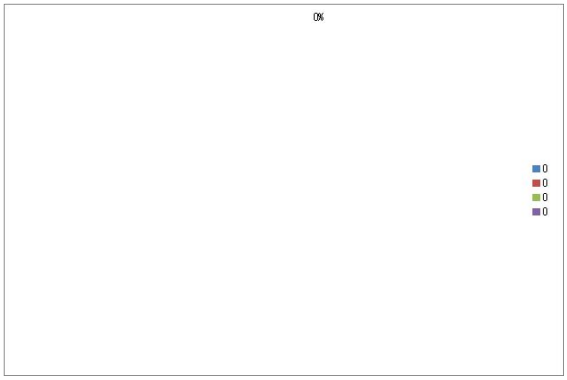

图 6 我省被植入后门网站数量按类型分布图

（四）“飞客”蠕虫数据分析

4 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281381个。事件高发的三个省份分别为广东省（约占28.5%）、江苏省（约占7.8%）和浙江省（约占7.2%），其分布情况如图7所示:

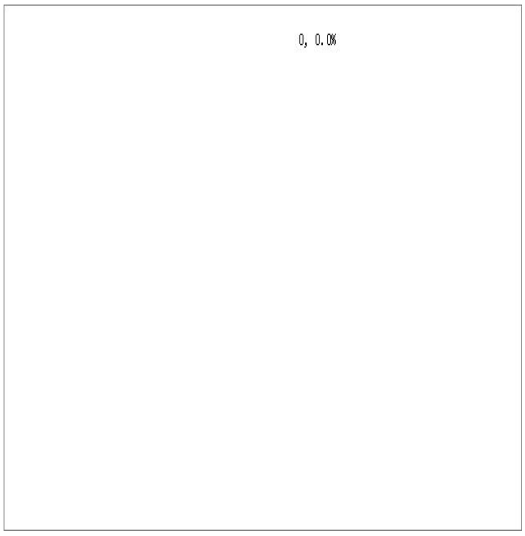

图7 境内感染飞客蠕虫的主机IP按地区分布图

4月，监测发现山西省感染“飞客”蠕虫病毒主机3317台，占全国受感染总数的1.18%，位列全国第22位，较上月下降1位。具体分布情况如图8所示:

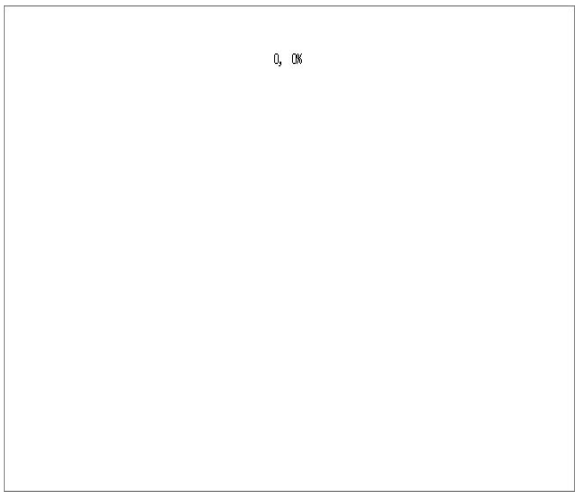

图8 我省感染“飞客”蠕虫的主机IP按地区分布图

（五）移动互联网恶意程序传播服务器数据分析

4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

4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
Trojan.Win32.Bayrob.gen	远程控制	2019/4/2
Trojan.Win32.Bayrob.gen	远程控制	2019/4/4
Email-Worm.Win32.Mydoom.l	远程控制	2019/4/4
Trojan.Win32.Generic	远程控制	2019/4/8
Email-Worm.Win32.Mydoom.l	远程控制	2019/4/11
Trojan-PSW.Win32.Tepfer.gen	远程控制	2019/4/22
Email-Worm.Win32.Mydoom.l	远程控制	2019/4/23
Email-Worm.Win32.Mydoom.l	远程控制	2019/4/28
Trojan.Win32.Generic	远程控制	2019/4/30
Email-Worm.Win32.Mydoom.l	远程控制	2019/4/30

（七）安全漏洞数据分析

4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881个，其中高危漏洞333个、中危漏洞455个、低危漏洞93个，其中0day漏洞378个，可远程攻击漏洞801个。

2018年5月至2019年4月CNVD收录漏洞按月统计情况分布如图9所示：

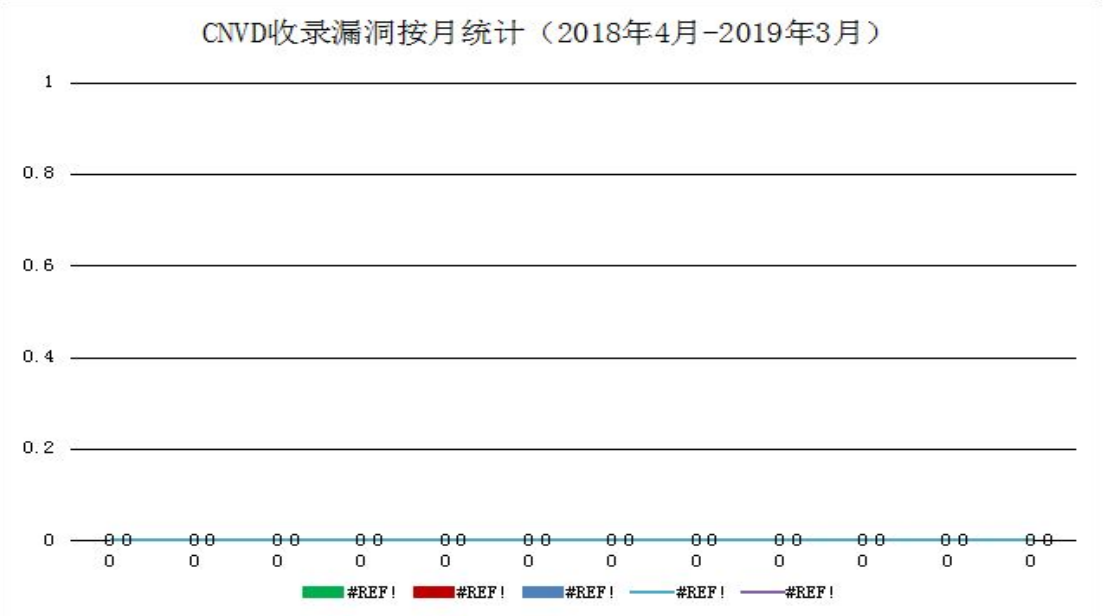

图 9 CNVD 收录漏洞按月统计情况

三、重要安全漏洞提示

（一）Oracle MySQL Server 拒绝服务漏洞

Oracle MySQL是美国甲骨文（Oracle）公司的一套开源的关系数据库管理系统。Oracle MySQL多个版本中的Server组件存在安全漏洞。攻击者可利用该漏洞造成拒绝服务（挂起或频繁崩溃），影响数据的可用性。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-2019-12459

（二）VMware Fusion 虚拟机端远程代码执行漏洞

VMware Fusion 是 VMware 公司出品的一款适用于 Mac 操作系统的虚拟机软件。VMware Fusion 虚拟机端存在远程代码执行漏洞，攻击者可通过 VMware Fusion 在本地启动的

WebSocket API 接口在所有已安装 VMware Tools 的虚拟机上利用该漏洞执行任意代码。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：http://www.cnvd.org.cn/flaw/show/CNVD-2019-08856