山西省网络安全月度通报

2019 年第 9 期（总第 63 期）

山西省通信管理局　　2019 年 9 月

一、基本态势

2019 年 8 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 15062 台，木马或僵尸程序控制服务器 11 台，感染“飞客”蠕虫病毒主机 3417 台。吕梁、忻州、太原排在全省受控木马或僵尸主机活动频繁地区前三位。

（一）基础网络运行安全

8 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

8 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）15062 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 0.3%，较上月增长 83.9%;（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，占全省 IP 总数 0.0002%，较上月减少 26.7%;（3）3417 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 1.2%;（4）102 个网站被篡改网页，较上月增长 36%;（5）18 个网站被植入后门，较上月减少 5.3%。

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

8 月，国家计算机网络应急技术处理协调中心（以下简称“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 1027700 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江苏省（约占 14.9%）、浙江省（约占 13.3%）、广东省（约占 9.0%）。具体分布情况如图 1 所示：

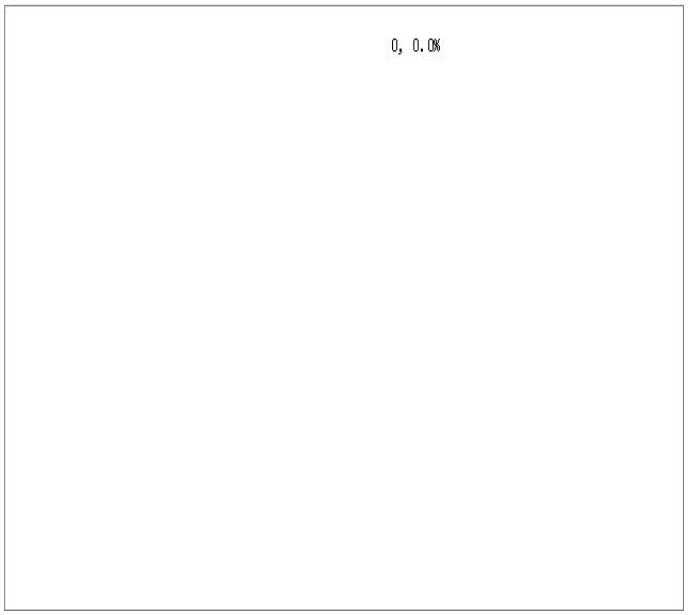

图 1 境内木马或僵尸网络程序受控主机按 IP 地区分布图

8 月，监测发现我省木马或僵尸程序受控主机 IP 地址数为 15062 个，占全国受控主机总数的 1.47%，位列全国第 16 位，与上月持平。其中，吕梁、忻州、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

8 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 2004 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 23.1%）、北京市（约占 21.7%）、江苏省（约占 13.9%）。具体分布情况如图 3 所示:

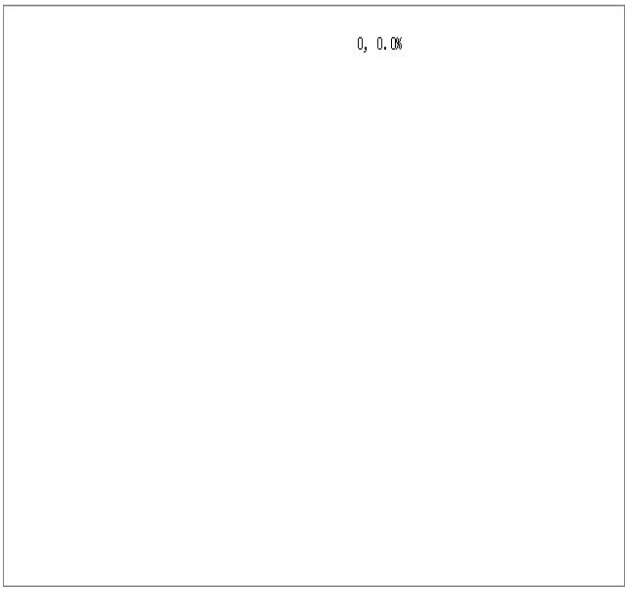

图 3 境内木马或僵尸程序控制服务器 IP 按地区分布图

8 月，我省木马或僵尸程序控制服务器 IP 地址数为 11 个，占全国控制服务器总数的 0.55%，位列全国第 16 位，较上月上升 4 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：

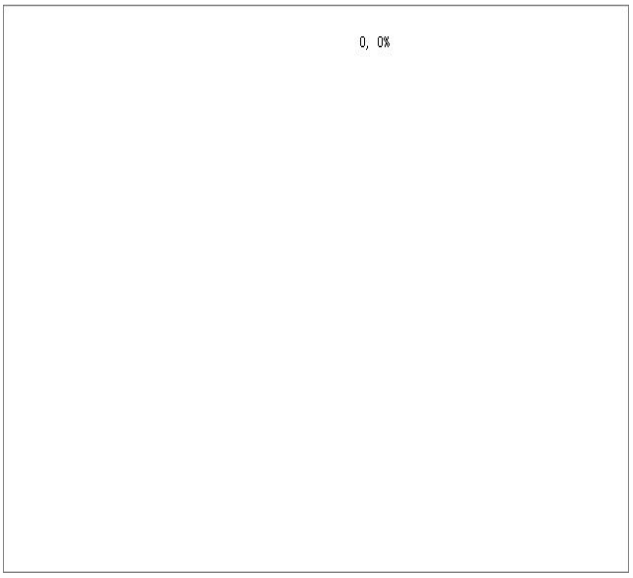

图 4 我省木马或僵尸程序控制服务器分布图

3. 木马或僵尸网络规模分布

8 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 11940 台，山西移动 1486 台，山西电信 1636 台。我省存在的较大规模僵尸网络有 3803 台受控主机。

（二）网页篡改数据分析

8 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 99283 个，其中境内被篡改政府网站（.gov）数量为 721 个。被篡改网站最多的地区分别为北京市（约占 21.4%）、广东省（约占 12.2%）、山东省（约占 11.2%），具体分布情况如图 5 所示：

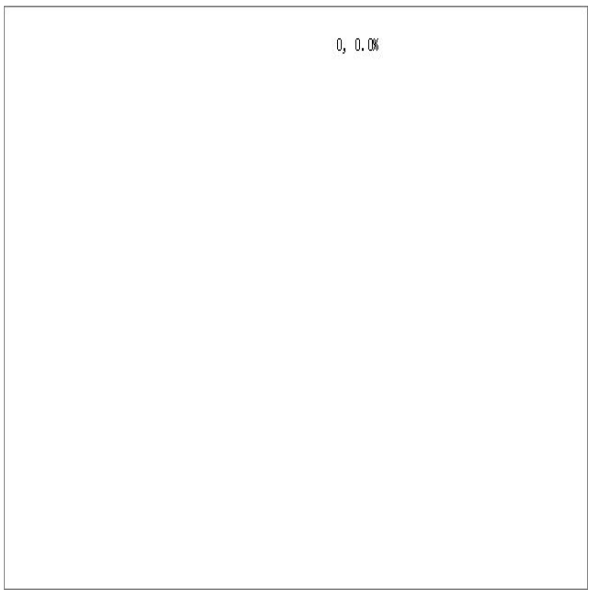

图 5 境内被篡改网站按地区分布图

8 月，我省有 102 个网站被篡改网页，占全国被篡改网站总数的 0.1%，位列全国第 24 位，与上月持平，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

8 月，我省有 18 个网站被植入后门，占全国被植入后门网站总数的 0.15%，位列全国第 25 位，与上月持平。其中政府和事业单位网站占全部被植入后门网站数量的 5.56%，同期全国的平均数为 11.3%。具体分布情况如图 6 所示：

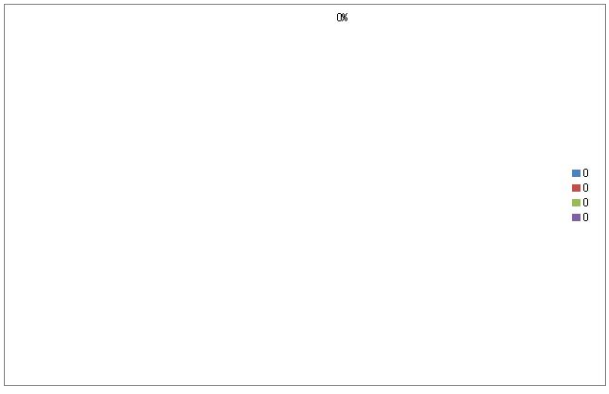

图 6 我省被植入后门网站数量按类型分布图

（四）“飞客”蠕虫数据分析

8 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 270094 个。事件高发的三个省份分别为广东省（约占 30.1%）、浙江省（约占 7.4%）和江苏省（约占 6.5%），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

8 月，监测发现山西省感染“飞客”蠕虫病毒主机 3417 台，占全国受感染总数的 1.27%，位列全国第 22 位，与上月持平。具体分布情况如图 8 所示：

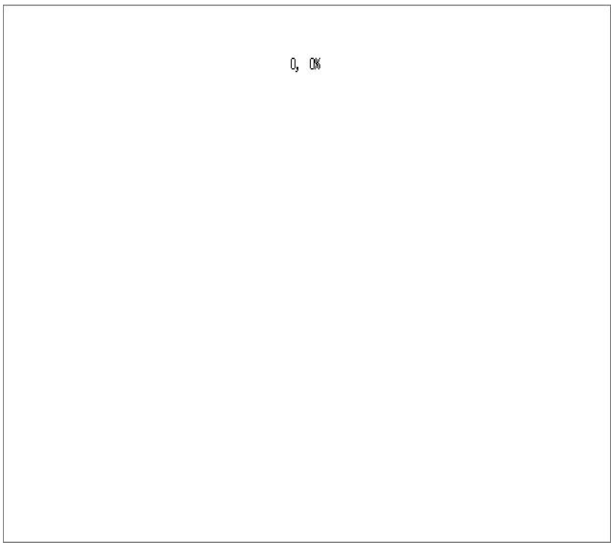

图 8 我省感染“飞客”蠕虫的主机 IP 按地区分布图

（五）移动互联网恶意程序传播服务器数据分析

8 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

8 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.Privacy.emial.uc	信息窃取	2019/8/1
A.Privacy.emial.ri	信息窃取	2019/81
A.Privacy.emial.jp	信息窃取	2019/8/1
A.Privacy.emial.no	信息窃取	2019/8/5
A.Privacy.emial.pi	信息窃取	2019/8/6
A.Privacy.emial.li	信息窃取	2019/8/9
A.Privacy.emial.yp	信息窃取	2019/8/13
A.Privacy.emial.ki	信息窃取	2019/8/13
A.Privacy.emial.vi	信息窃取	2019/8/21
A.Privacy.emial.fz	信息窃取	2019/8/21

（七）安全漏洞数据分析

8 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 1821 个，其中高危漏洞 445 个、中危漏洞 1165 个、低危漏洞 211 个，其中 0day 漏洞 336 个，可远程攻击漏洞 1552 个。

2018 年 9 月至 2019 年 8 月 CNVD 收录漏洞按月统计情况分布如图 9 所示:

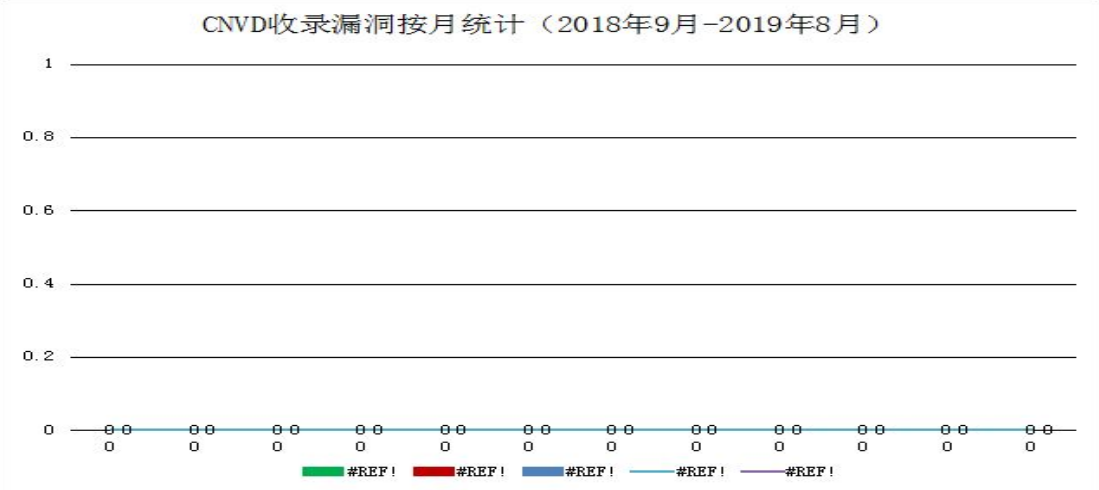

图 9 CNVD 收录漏洞按月统计情况

三、重要安全漏洞提示

（一）Qualcomm WLAN 芯片远程代码执行漏洞

Qualcomm WLAN芯片是高通平台处理WLAN/WIFI协议的专用芯片，属于高通Baseband子系统，用于提高WLAN/WIFI处理速度和性能，降低能耗。Qualcomm WLAN芯片存在远程代码执行漏洞。攻击者可以通过控制WLAN固件，最终导致在服务器上执行任意代码。Redis是一个广泛使用的开源数据库，支持网络传输，并提供了多种语言的API。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-2019-28290

（二）深信服 SSL VPN 设备命令执行漏洞

深信服科技股份有限公司是一家专注于企业级安全、云计算

及基础架构的产品、服务和解决方案供应商。深信服VPN-2050存在溢出漏洞，攻击者可利用该漏洞执行命令、获取服务器权限。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：https://www.cnvd.org.cn/flaw/show/CNVD-2019-29574