海南省网络安全通报 2017 年第 7 期

一、我省本月网络安全总体情况

2017 年 7 月，我省互联网网络安全状况整体评价为良，木马僵尸等反映网络安全状况的部分指数有所减少，其中我省被境外控制的木马僵尸受控主机数量为 10322 个，较上月 31417 个有大幅减少，列全国第 25 位；我省木马僵尸控制服务器数量为 6 个，比上月减少 57 个。从事件的地区分布来看，海口、三亚等地市感染僵尸木马的主机数量较多。本月共监测发现重要信息系统事件 6 起，重要信息系统漏洞事件 14 起，发生网页篡改安全事件 4 起。每日互联网流量最高值为 735G，最低值 100G，未发现流量异常情况。我省重要信息系统部门或网站被攻击数量未见明显改善，部分政府网站或系统存在被攻击痕迹，被植入后门的现象依然存在，需引起政府和重要信息系统部门高度重视。

二、本月网络安全工作动态

1. 互联网网络安全信息通报工作动态

国家计算机网络应急技术处理协调中心海南分中心（简称海南互联网应急中心），由海南省通信管理局授权，负责收集、汇总、分析和发布本省互联网网络安全信息工作。

7 月，海南互联网应急中心共接收各基础运营企业、增值运营企业、网络安全企业等信息通报工作成员单位提供的网络安全月度信息汇总表 7 份。各运营企业相关网络安全责任人应密切关注本单位运营网络的安全情况，积极做好网络安全事件信息报送工作。

2.开展木马僵尸感染主机清理工作

7 月，海南互联网应急中心共向各运营企业下发了 783 条感染僵尸木马的 IP 数据，44 条僵尸木马病毒控制端 IP 数据，431 条感染蠕虫病毒的 IP 数据，存在后门 IP 数据 3 条。各企业积极配合进行了处置。海南互联网应急中心针对各企业反馈涉事单位建立了重点单位监测表，进行每日监测，对监测发现的感染情况及时进行通报，并建立联系人机制，提高处置效率。

3.手机病毒处理工作

7 月，海南互联网应急中心协调运营企业处置手机病毒 180 条。运营企业通过短信提醒、免费客户服务热线、网上营业厅、门户网站公告等方式，及时向用户推送手机病毒感染信息和病毒查杀方法及工具，帮助用户了解手机病毒危害，引导用户清除手机病毒，并在手机病毒处置过程中特别注意保护用户隐私。同时，企业将手机病毒处置结果、用户投诉等情况通报我中心。

4.自主发现网络安全事件处置情况

海南互联网应急中心通过国家中心系统平台，自主监测发现并处理了一批被植入后门和网页篡改等网络安全事件，经过验证后向相关单位报送网络安全通报，并协助处理。其中包括：漏洞事件 14 起，网页篡改事件 3 起，后门事件 3 起，恶意代码事件 73 起。

附 1：网络安全信息报送情况

7 月，海南互联网应急中心处理及或向本地区各信息通报工作成员单位报送的网络安全事件共 1456 起。各类事件信息详细分类统计分别如表 1 和表 2 所示。（注：此统计全包括海南互联网应急中心通报数据，另包括企业自查数据）

网络安全事件信息报送类型统计（2017 年 7 月）	
事件类型	数量
IP 业务	0
基础 IP 网络	12
运营企业自有业务系统	0
域名系统	0
公共互联网环境	1444
合计	**1456**

表 1：网络安全事件信息报送类型统计

事件类型	数量
计算机病毒事件	0
蠕虫事件	431
木马事件	44
僵尸网络事件	783
域名劫持事件	0
网络仿冒事件	0
网页篡改事件	3
网页挂马事件	0
拒绝服务攻击事件	0
后门事件	3
非授权访问事件	0
垃圾邮件事件	0
其他网络安全事件	180
合计	**1444**

表 2：公共互联网环境事件信息报送类型统计

附 2：木马僵尸监测数据分析

1、木马僵尸受控主机的数量和分布

2017 年 6 月，监测发现我国大陆地区 1412538 个 IP 地址对应的主机被其他国家或地区通过木马程序秘密控制，与上月的 1409439 个相比增加了 0.22%，其分布情况如图 1 所示。其中，海南省 10322 个（占全国 0.73%），全国排名第 25 位。

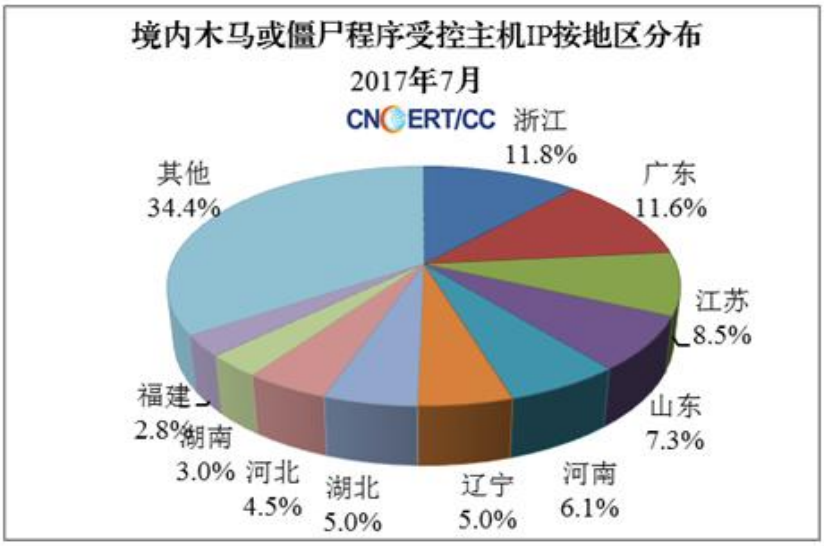

图 1：中国大陆木马或僵尸受控主机 IP 按地区分布

2、木马僵尸控制服务器的数量和分布

2017 年 7 月，监测发现我国大陆地区 2739 个 IP 地址对应的主机被利用作为木马控制服务器，与上月的 49018 个相比大幅减少，其分布情况如图 2 所示。其中，海南省 6 个（占全国 0.22%），全国排名第 27 位。

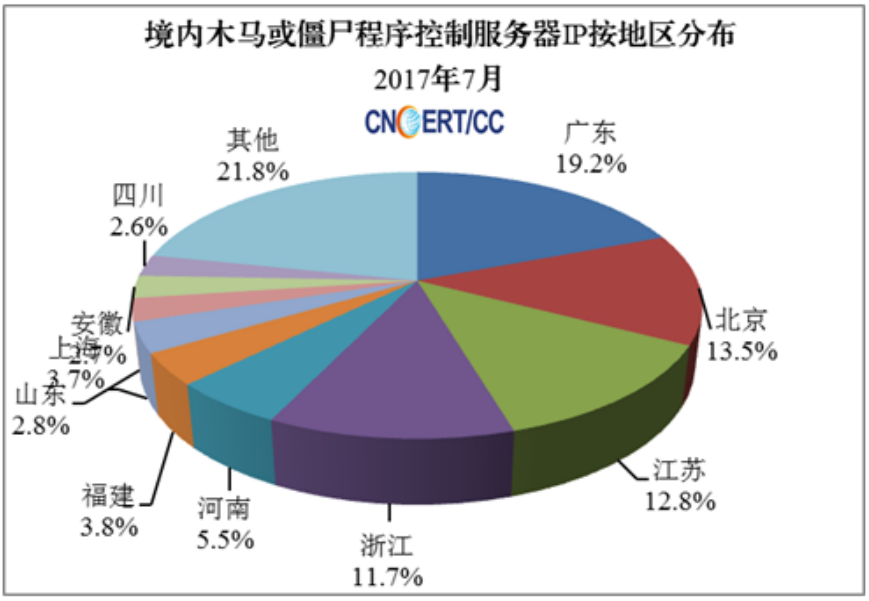

图 2：中国大陆木马或僵尸控制服务器 IP 按地区分布

3、境外木马控制服务器的数量和分布

2017 年 7 月，秘密控制我国大陆计算机的境外木马控制服务器 IP 有 5888 个，与上月的 20871 个相比减少了 71.79%，主要来自美国、俄罗斯等国家，具体分布如图 3 所示。

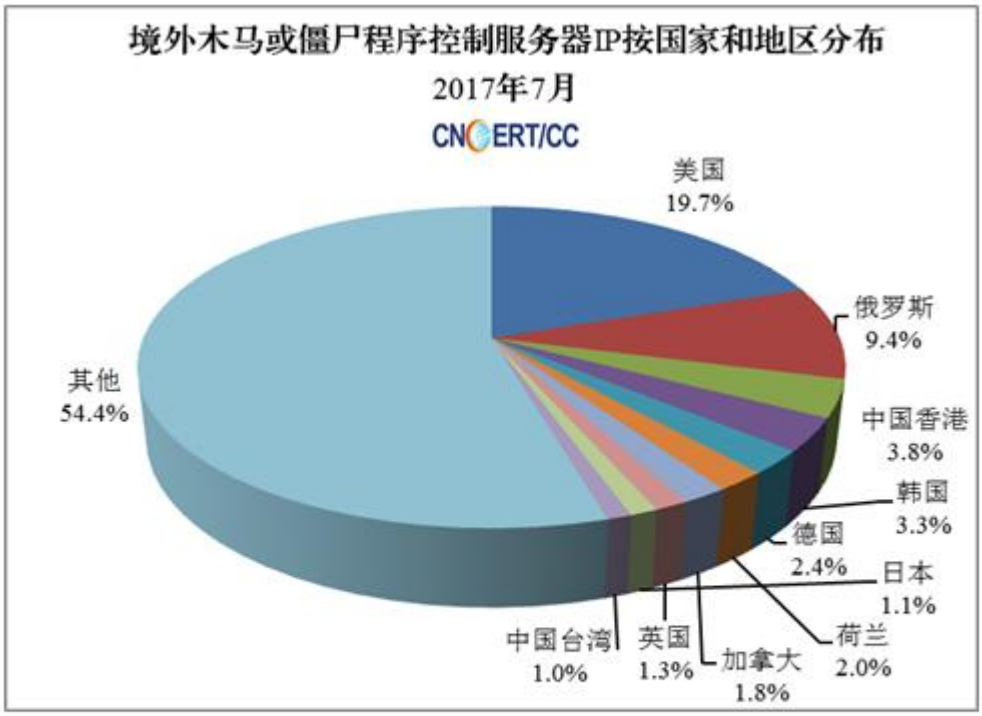

图 3：通过木马或僵尸程序控制中国大陆主机的境外 IP 按国家和地区分布

4、木马僵尸网络规模分布

在发现的僵尸网络中，规模大于 5000 的僵尸网络有 57 个，规模在 100－1000 的有 369 个，规模在 1000－5000 的有 160 个，分布情况如图 4 所示。

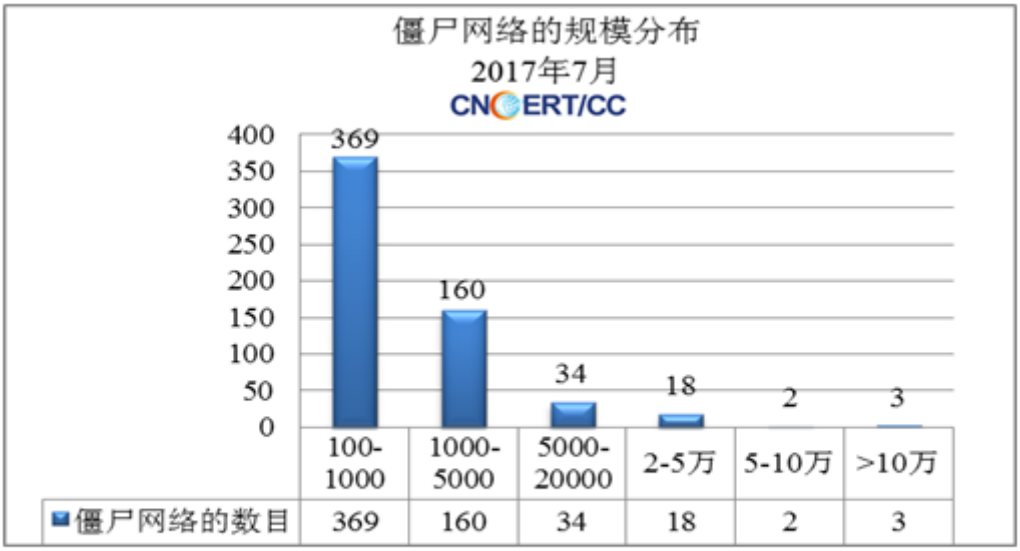

图 4：僵尸网络的规模分布

附 3：境内被植入后门的网站按地区分布

2017 年 7 月，监测发现我国大陆地区 4146 个网站被植入后门程序，其分布情况如图 5 所示。其中，海南省 7 个（占全国 0.17%），排全国第 28 位。

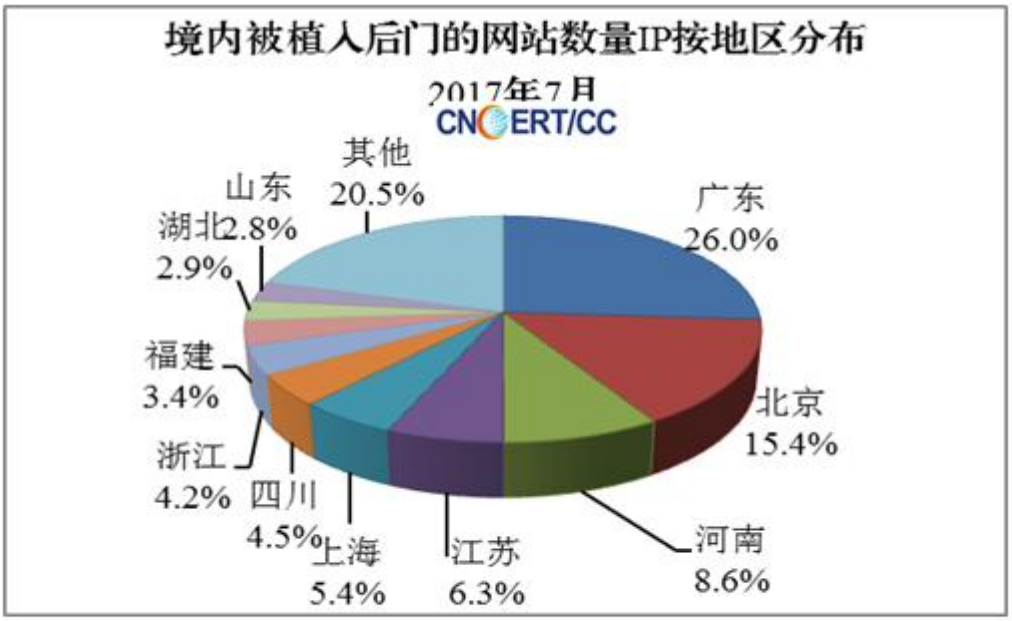

图 5：境内被植入后门的网站按地区分布

附 4：网页篡改监测数据分析

2017 年 7 月，我国大陆地区被篡改网站 6468 个，与上月的 3669 个相比有大幅增加；其中，海南省 4 个（占全国 0.06%），排名第 27 位。具体分布如图 6 所示。

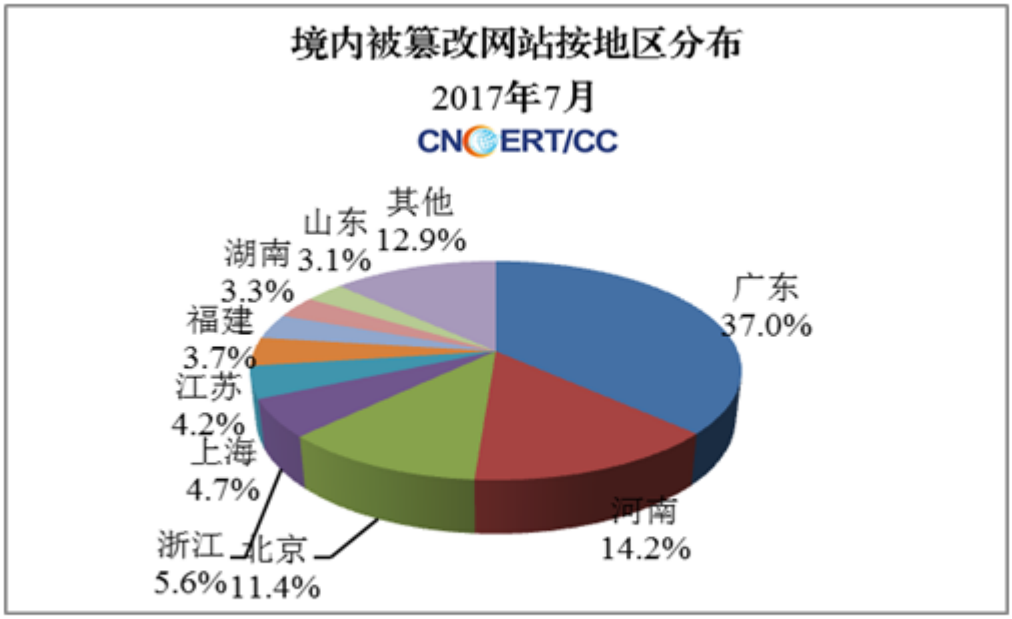

图 6：境内被篡改网站按地区分布

附 5：恶意代码数据分析

2017 年 7 月，恶意代码捕获与分析系统监测得到的放马站点统计。

1.2017 年 7 月 CNCERT 捕获的恶意代码数量

名称	数量
新增恶意代码名称数	1
新增恶意代码家族数	1

2. 2017 年 7 月活跃放马站点域名和 IP

排序	活跃放马站点域名	活跃放马站点 IP
1	dl.wandoujia.com	106.37.238.1
2	dl.cdn.wandoujia.com	111.206.15.2
3	nc-dl.wdjcdn.com	120.26.127.170
4	i.kpzip.com	61.136.163.78
5	cl.xzqxzs.com	183.60.106.54
6	cl.gxjsxq.com	122.70.142.167
7	www.go890.com	61.133.192.170
8	down.nxwb.net	222.28.152.177
9	cl2.cjsdxz.com	61.233.139.70
10	cl2.dhfszh.com	110.40.4.3

附 6：重要漏洞与重要事件处置公告

2017 年 7 月，CNVD 整理和发布以下重要安全漏洞信息。同时提醒用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。（更多漏洞信息，请关注 CNVD 官方网站：www.cnvd.org.cn）

关于 Apache Strusts2 存在远程命令执行漏洞威胁的情况通报

7 月 7 日，Apache Struts 发布最新的安全公告，Struts2 存在远程命令执行漏洞（命名编号为 S2-048）。国家信息安全漏洞共享平台（CNVD）已将该漏洞收录为高危漏洞（编号：CNVD-2017-13259），攻击者可以利用该漏洞获取服务器主机系统权限。目前，漏洞利用代码已在互联网上公开。从 8 日凌晨起，互联网上已经出现了大量的攻击尝试且存在若干实现漏洞利用的案例报告。具体情况如下：

一、S2-048 漏洞情况分析

Struts2 是第二代基于 Model-View-Controller (MVC)模型的 Java 企业级 web 应用框架，是较为流行的容器软件中间件。2017 年 7 月 7 日，Apache Struts 发布最新的安全公告 S2-048,漏洞成因是 Showcase 应用演示 Struts2 整合 Struts 1 的插件中存在一处任意代码执行缺陷，当应用使用了 Struts2Struts1 的插件时，用户可以构造特定输入（一般为 Header 字段的 OGNL 表达式）发送到 ActionMessage 类中可导致命令执行，进而获得服务器主机系统权限。

二、漏洞影响范围

S2-048 漏洞主要影响使用 Struts 1 插件的 Struts 2.3.x 版本，并存在一定的漏洞利用前提限定。在漏洞公开后，国内安全厂商在用户侧也开展了积极的应急防护。CNCERT 抽样监测发现 S2-48 漏洞未产生严重安全问题。

根据 CNCERT 抽样测试结果（>1000 个网站案例,以在 S2-045 漏洞中受到影响的案例为主），受 S2-048 漏洞影响的 Apache Struts2

网站比例约为0.6%，暂未发现党政机关和重要信息系统用户单位案例。

三、漏洞修复建议

官方已在Struts 2.5.10.1版本中修复了该漏洞，请参考官网及时升级：http://struts.apache.org/download.cgi#struts25101。同时，未能及时升级的系统可以参照官方给出的临时解决方案，或启用已生成有针对性防护策略的国内厂商网络侧防护产品（如：防火墙、云WAF等）。

临时解决方案：应使用资源键（resource keys），而不是将原始消息直接传递给ActionMessage类。正确和错误的方式如下所示：

（正确的方式）messages.add("msg",new ActionMessage("struts1.gangsterAdded",gform.getName()));

（错误的方式）messages.add("msg",new ActionMessage("Gangster " + gform.getName() + " wasadded"))。