海南省网络安全通报 2018 年第 2 期

一、我省本月网络安全总体情况

2 月，监测发现我省网络安全漏洞 77 起；被境外控制的木马僵尸受控主机数量为 5876 个，较上月 7284 个减少了 19.33%，列全国第 19 位;木马僵尸控制服务器数量为 10 个,较上月 16 个减少了 37.5%，列全国第 25 位。每日互联网流量最高值为 1894G，最低值 240G，未发现流量明显异常情况。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或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。

2 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 10 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

2 月，海南互联网应急中心共向各运营企业下发了 5203 条感染僵尸木马的 IP 数据，13 条僵尸木马病毒控制端 IP 数据，1020 条感染蠕虫病毒的 IP 数据；网站漏洞数据 77 条。各企业积极配合并进行

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

2 月，海南互联网应急中心协调运营企业处置手机病毒 300 条。运营企业通过短信提醒、免费客户服务热线、网上营业厅或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及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，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些被植入后门和被篡改网页的网络安全事件，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:漏洞事件 77 起，恶意代码事件 21 起，其它网络安全事件 2 起。

三、本月安全要闻回顾

北约合作网络防御卓越中心（CCDCOE）将负责协调北约所有机构网络防御行动训练

2 月 1 日消息据外媒报道，北约合作网络防御卓越中心（CCDCOE）被选定来协调联盟内所有网络防御行动领域的教育和培训解决方案。

CCDCOE 是一家总部位于爱沙尼亚，由 20 个不同国家组成的知识中心。从技术上讲，这是一个军事组织，它的任务是为盟友提供

360 度的网络防御，并且输送技术、战略、行动和法律方面的专业知识。

除上述功能之外，CCDCOE 还扮演了一个新的角色——作为网络防御作战教育和训练纪律的负责人，这一新角色由北约两个战略指挥部门之一的最高盟军指挥部（SACT）授予，主要职责是与位于美国弗吉尼亚州诺福克的盟军司令部密切合作。

CCDOE 的负责人 Merle Maigre 表示：“我们很荣幸在这个新的挑战中发挥作用，投资于培训和教育可能是我们可以做出的最好的承诺。虽然回报是丰厚的，但不能总是以美元或欧元来衡量价值。因为投资培训和教育在技术浪潮的背景下给我们带来了新的机遇，不过需要注意的是技能过时得也更快。”

另外，CCDCOE 也是 “塔林手册 2.0 ”的发源地（该手册是关于国际法如何适用于网络运营的综合指南）、组织了世界上最大最复杂的国际技术性现场网络防御演习。

附 1：网络安全信息报送情况

2 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 6573 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（2018 年 2）	
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	6561
合计	**6573**

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	1020
木马事件	13
僵尸网络事件	5203
域名劫持事件	0
网络仿冒事件	0
网页篡改事件	0
网页挂马事件	0
拒绝服务攻击事件	0
后门事件	25
非授权访问事件	0
垃圾邮件事件	0
其他网络安全事件	300
合计	**6561**

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

2018 年 2 月，CNCERT 监测发现我国大陆地区 287449 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，与上上月的 516798 个相比减少了 44.38%，其分布情况如图 1 所示。其中，海南省 5876 个（占全国 2.04%），全国排名第 19 位。

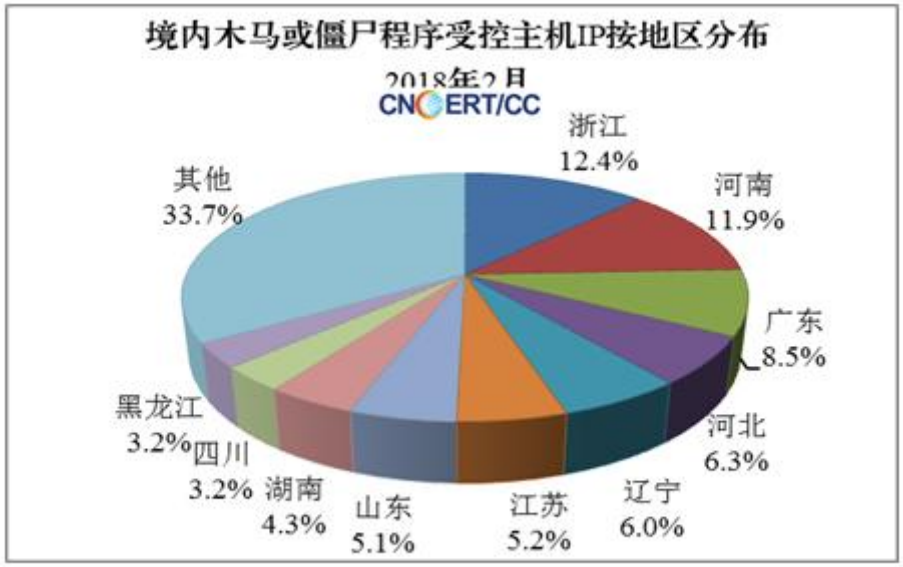

图 1：中国大陆木马或僵尸受控主机 IP 按地区分布

2、木马僵尸控制服务器的数量和分布

2018 年 2 月，CNCERT 监测发现我国大陆地区 1660 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 2339 个相比减少了 29.03%，其分布情况如图 2 所示。其中，海南省 10 个（占全国 0.60%），全国排名第 25 位。

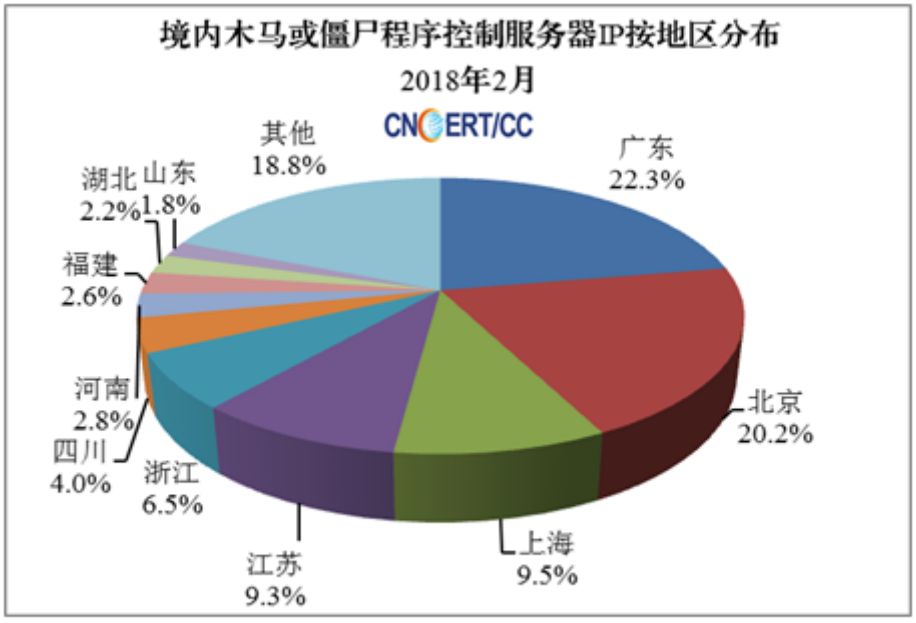

图 2：中国大陆木马或僵尸控制服务器 IP 按地区分布

3、境外木马控制服务器的数量和分布

2018 年 2 月，CNCERT 监测发现秘密控制我国大陆计算机的境外木马控制服务器 IP 有 7341 个，与上月的 12606 个相比减少了 41.77%，主要来自美国、巴西、日本等国家，具体分布如图 3 所示。

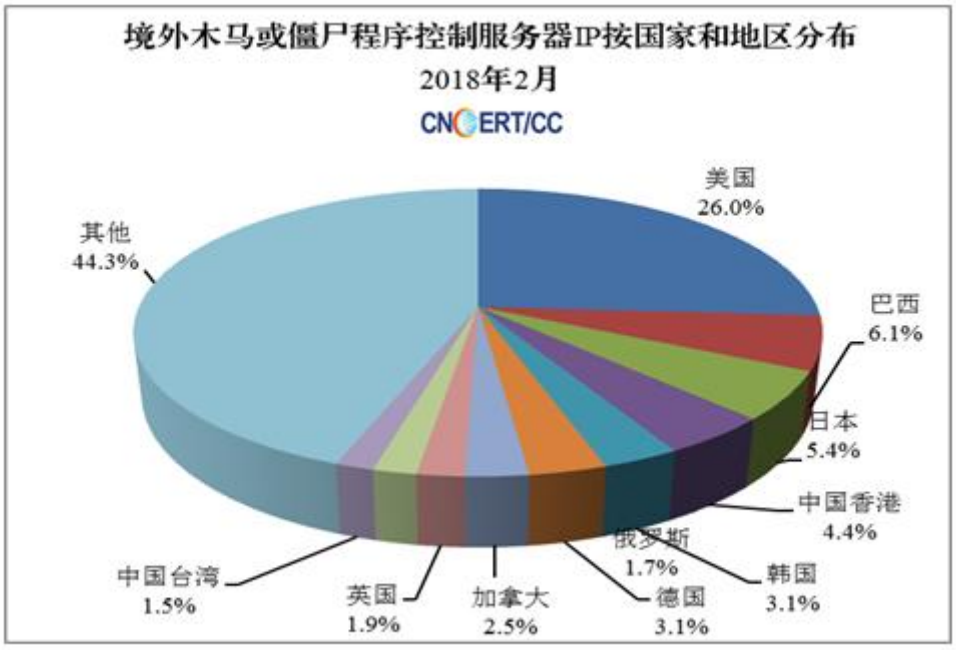

图 3：通过木马或僵尸程序控制中国大陆主机的境外 IP 按国家和地区分布

4、木马僵尸网络规模分布

2018 年 2 月，在 CNCERT 监测发现的僵尸网络中，规模大于 5000 的僵尸网络有 57 个，规模在 100－1000 的有 8747 个，规模在 1000－5000 的有 180 个，分布情况如图 4 所示。

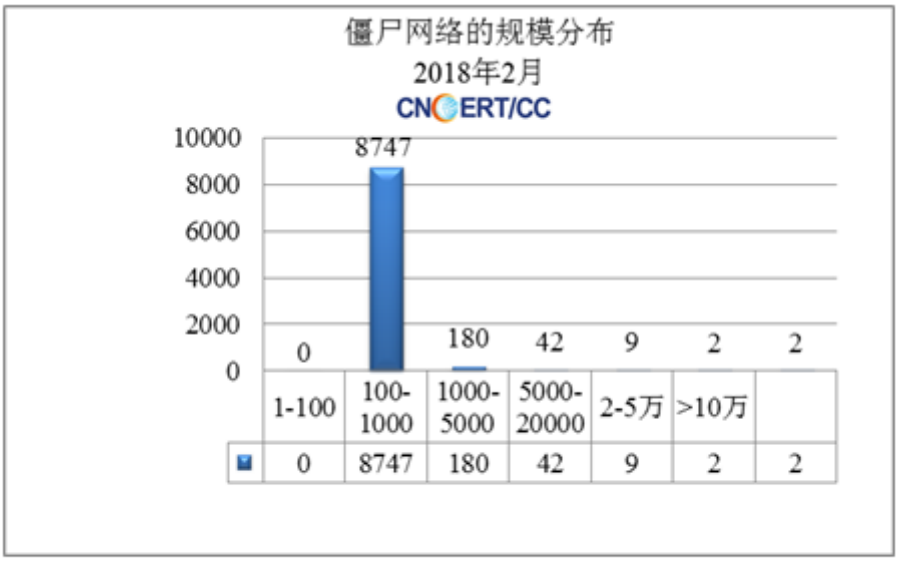

图 4：僵尸网络的规模分布

附 3、境内被植入后门的网站按地区分布

2018 年 2 月，CNCERT 监测发现我国大陆地区 1718 个网站被植入后门程序，比上月的 2606 个减少了 34.08%，其分布情况如图 5 所示。本月未监测到海南被植入后门的网站。

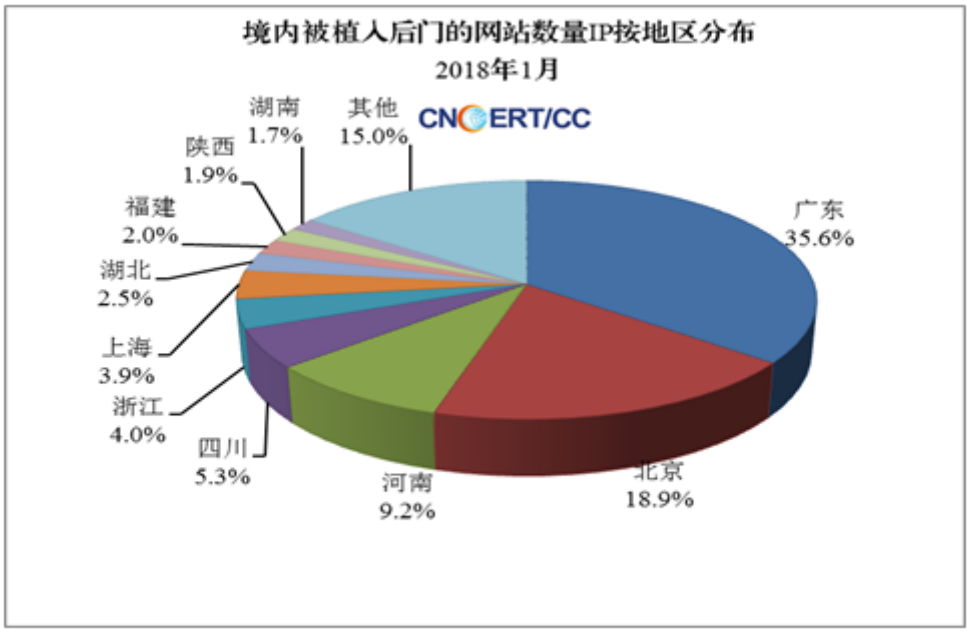

图 5：境内被植入后门的网站按地区分布

附 4、网页篡改监测数据分析

2018 年 2 月，CNCERT 监测发现我国大陆地区被篡改网站 3678 个，与上月的 4101 个相比减少了 10.31%；其中，海南省 28 个（占全国 0.76%），排名第 14 位。具体分布如图 6 所示。

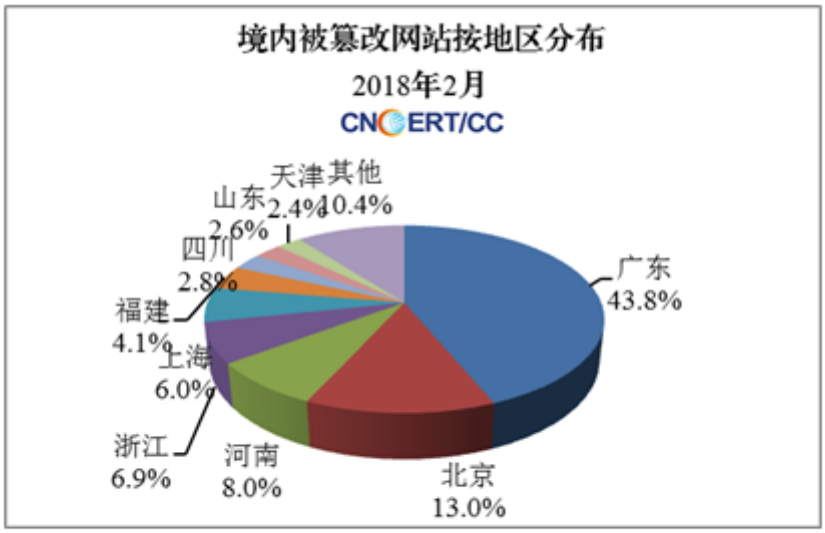

图 6：境内被篡改网站按地区分布

附 5：恶意代码数据分析

2018 年 2 月，恶意代码捕获与分析系统监测得到的放马站点统计。

r:black'>3678 个，与上月的 4101 个相比减少了 10.31%；其中，海南省 28 个（占全国 0.76%），排名第 14 位。具体分布如图 6 所示。

1. 2018 年 2 月 CNCERT 捕获的恶意代码数量

名称	数量
新增恶意代码名称数	0
新增恶意代码家族数	0

2. 2018 年 2 月活跃放马站点域名和 IP

序号	活跃放马站点域名	活跃放马站点 IP
1	i.kpzip.com	120.26.127.170
2	cl.urndf.com	43.242.181.16
3	www.go890.com	125.76.247.169
4	dl.urndf.com	117.23.6.63
5	dxdown.nonglirili.net	121.12.98.72
6	dl.apxlx.com	220.181.105.173
7	cl.qpzqxz.com	218.95.139.53
8	dl.qpzqxz.com	117.23.6.65
9	cl.apxlx.com	117.23.6.64
10	cl.gxjsxq.com	122.72.35.190