海南省网络安全通报 2018 年第 3 期

一、我省本月网络安全总体情况

3 月，监测发现我省网络安全漏洞 46 起；被境外控制的木马僵尸受控主机数量为 6146 个，较上月 5876 个增加了 4.59%，列全国第 22 位；木马僵尸控制服务器数量为 11 个，较上月 10 个增加了 10%，列全国第 25 位。每日互联网流量最高值为 4096G，最低值 252G，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。

3 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

3 月，海南互联网应急中心共向各运营企业下发了 2206 条感染僵尸木马的 IP 数据，3 条僵尸木马病毒控制端 IP 数据，1234 条感染蠕虫病毒的 IP 数据；网站漏洞数据 46 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

3 月，海南互联网应急中心协调运营企业处置手机病毒 167 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 46 起，恶意代码事件 45 起，其它网络安全事件 1 起

三、本月安全要闻回顾

远程桌面协议 CredSSP 出现漏洞，影响所有版本的 Windows

HackerNews.cc3 月 14 日消息 RDP 和 WInRM 中使用的 CredSSP 协议（安全加密 Windows 用户远程登录过程）中出现严重漏洞，影响所有版本的 Windows。

远程攻击者额可以利用这个漏洞，使用 RDP 和 WinRM 窃取数据并运行恶意代码。这个漏洞由网络安全公司 Preempt Security 发现，

编号为 CVE-2018-0886，是一个逻辑加密漏洞，可被中间人攻击者利用，通过 WiFi 或物理接触网络来窃取 session 认证数据，发起远程进程调用攻击。如果用户和服务器通过 RDP 和 WinRM 连接协议进行认证，中间人攻击就能执行远程命令，入侵企业网络。而由于 RDP 是远程登录中最常用的应用，几乎所有企业用户都在使用，因此，这个漏洞可造成大范围影响。

目前，微软已经发布相关更新补丁，用户应尽快下载更新，同时可以禁用 RDP 等相关应用端口，尽可能少使用特权账户，多使用非特权账户。

附 1：网络安全信息报送情况

3 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 3620 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	3608
合计	**3620**

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	1234
木马事件	7
僵尸网络事件	2206
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	0
非授权访问事件	1
垃圾邮件事件	0
其他网络安全事件	167
合计	**3608**

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 3 月，CNCERT 监测发现我国大陆地区 424012 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 287449 个相比增加了 47.51%，其分布情况如图 1 所示。其中，海南省 6146 个（占全国 1.45%），全国排名第 22 位。

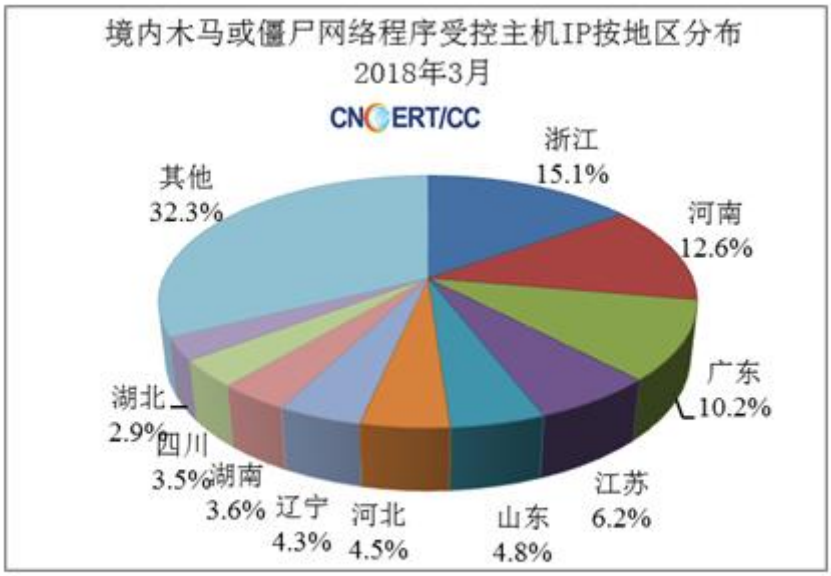

图 1：中国大陆木马或僵尸受控主机 IP 按地区分布

2、木马僵尸控制服务器的数量和分布

2018 年 3 月，CNCERT 监测发现我国大陆地区 2259 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 1660 个相比增加了 36.08%，其分布情况如图 2 所示。其中，海南省 11 个（占全国 0.49%），全国排名第 25 位。

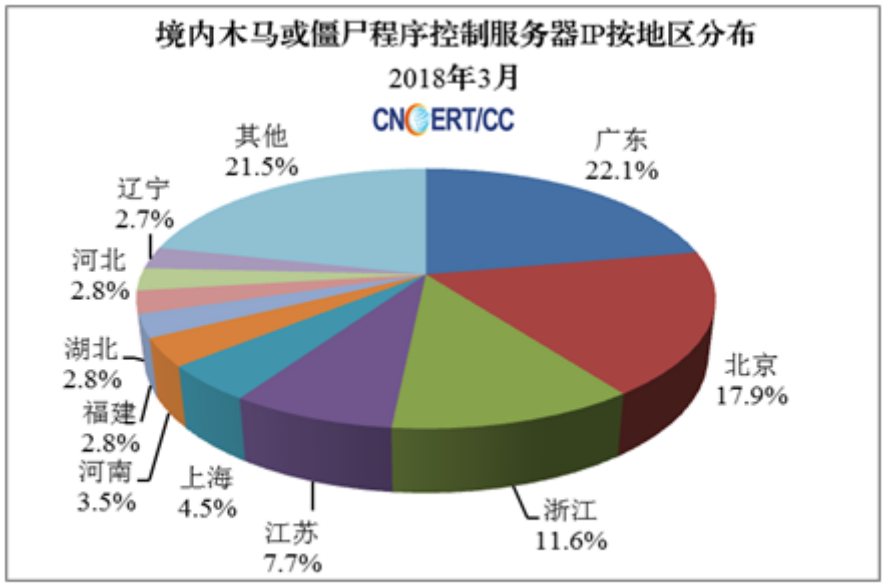

图 2：中国大陆木马或僵尸控制服务器 IP 按地区分布

3、境外木马控制服务器的数量和分布

2018 年 3 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 15304 个，与上月的 7341 个相比增加了 108.47%，主要来自美国、越南、日本等国家，具体分布如图 3 所示。

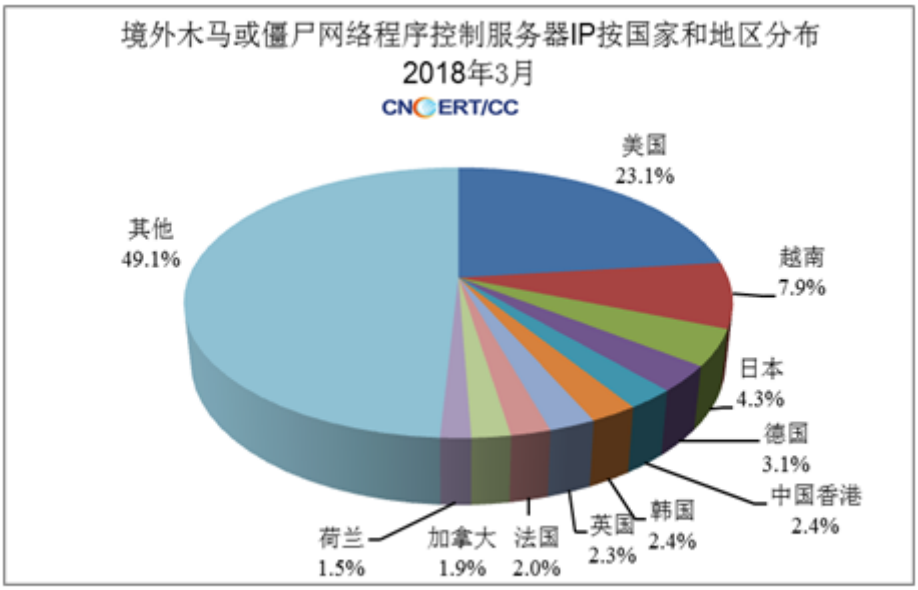

图 3：通过木马或僵尸程序控制中国大陆主机的境外 IP 按国家和地区分布

4、木马僵尸网络规模分布

2018 年 3 月，在 CNCERT 监测发现的僵尸网络中，规模大于 5000 的僵尸网络有 31 个，规模在 100－1000 的有 335 个，规模在 1000－5000 的有 81 个，分布情况如图 4 所示。

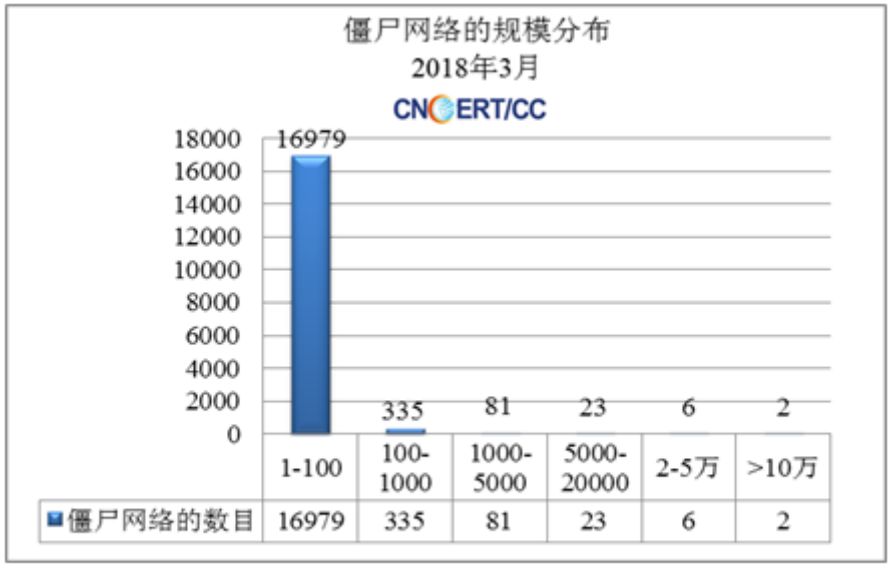

图 4：僵尸网络的规模分布

附 3、境内被植入后门的网站按地区分布

2018 年 3 月，CNCERT 监测发现我国大陆地区 2858 个网站被植入后门程序，比上月的 1718 个增加了 66.36%，其分布情况如图 5 所示。其中，海南省 2 个（占全国 0.07％），全国排名第 28 位。

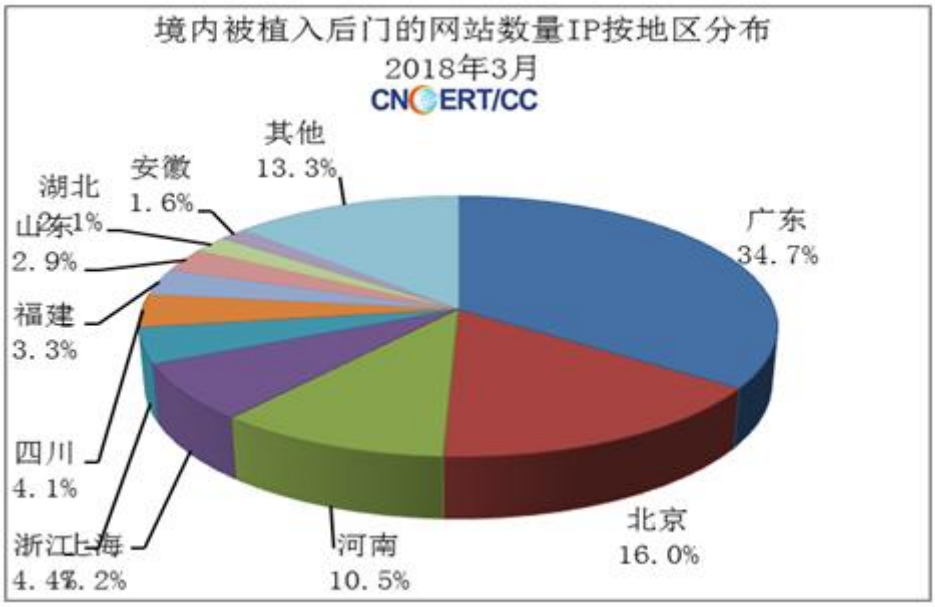

图 5：境内被植入后门的网站按地区分布

附 4、网页篡改监测数据分析

2018 年 3 月，CNCERT 监测发现我国大陆地区被篡改网站 2559 个，与上月的 3678 个相比减少了 30.42%；其中，海南省 5 个（占全国 0.20%），排名第 21 位。具体分布如图 6 所示。

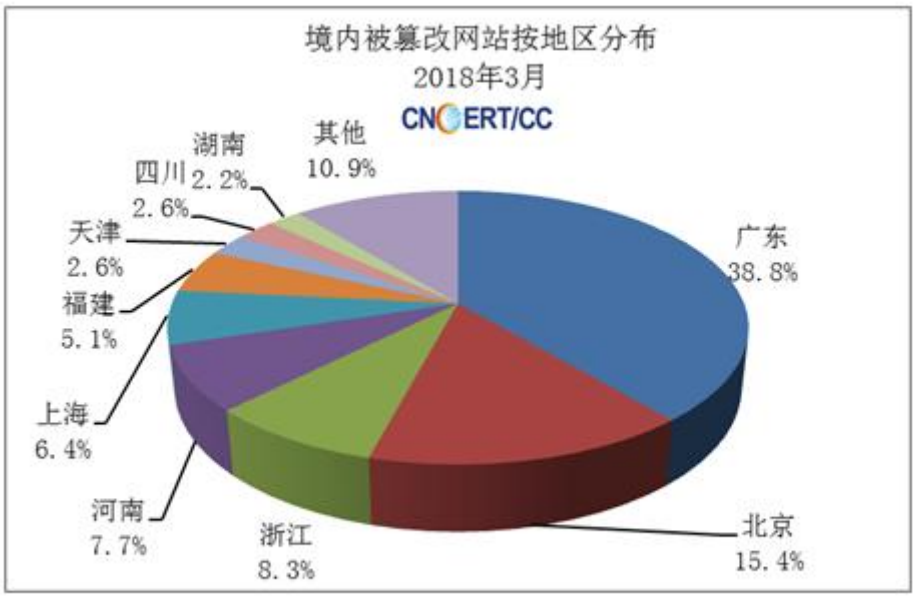

图 6：境内被篡改网站按地区分布

附 5：恶意代码数据分析

2018 年 3 月，恶意代码捕获与分析系统监测得到的放马站点统计。

1. 2018 年 3 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 3 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	www.go890.com	117.23.6.63
2	cl.urndf.com	120.26.127.170
3	dl.urndf.com	220.181.105.173
4	down.nxwb.net	122.72.35.190
5	dxdown.nonglirili.net	61.133.194.190
6	cl.qpzqxz.com	117.23.6.64
7	url.222bz.com	117.23.6.65
8	rkverify.securestudies.com	111.161.3.176
9	dl.apxlx.com	171.111.154.225
10	cl.apxlx.com	117.131.204.56