海南省网络安全通报 2017 年第 8 期

一、我省本月网络安全总体情况

2017 年 8 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 16171 个，较上月 10322 个有所增加，列全国第 25 位；我省木马僵尸控制服务器数量为 2 个，比上月减少 4 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。每日互联网流量最高值为 770G，最低值 100G，未发现流量异常情况。本月共监测发现重要信息系统事件 6 起。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所属部门高度重视。

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。

8 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

8 月，海南互联网应急中心共向各运营企业下发：763 条感染僵尸木马的 IP 数据、37 条僵尸木马病毒控制端 IP 数据、415 条感染蠕虫病毒的 IP 数据、存在后门的 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的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

8 月，海南互联网应急中心协调运营企业处置手机病毒 165 条。运营企业通过短信提醒、免费客户服务热线、网上营业厅和门户网站公告等方式，及时向用户推送手机感染病毒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，运营企业及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批网站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，并协助相关单位对网络安全时间进行处理。其中包括：拒绝服务攻击事件 1 起，网页篡改事件 3 起，网站被植入后门事件 3 起，恶意代码事件 72 起。

附 1：网络安全信息报送情况

8 月，海南互联网应急中心处理及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 1398 起。各类事件信息详细分类统计分别如表 1 和表 2 所示。（注：此统计数据包括海南互联网应急中心通报数据、企业自查数据）

网络安全事件信息报送类型统计（2017 年 8）	
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	1386
合计	**1398**

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	415
木马事件	37
僵尸网络事件	763
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	165
合计	**1386**

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 8 月，监测发现我国大陆地区 1685365 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 1412538 个相比增加了 19.3%，其分布情况如图 1 所示。其中，海南省 16171 个（占全国 0.96%），全国排名第 25 位。

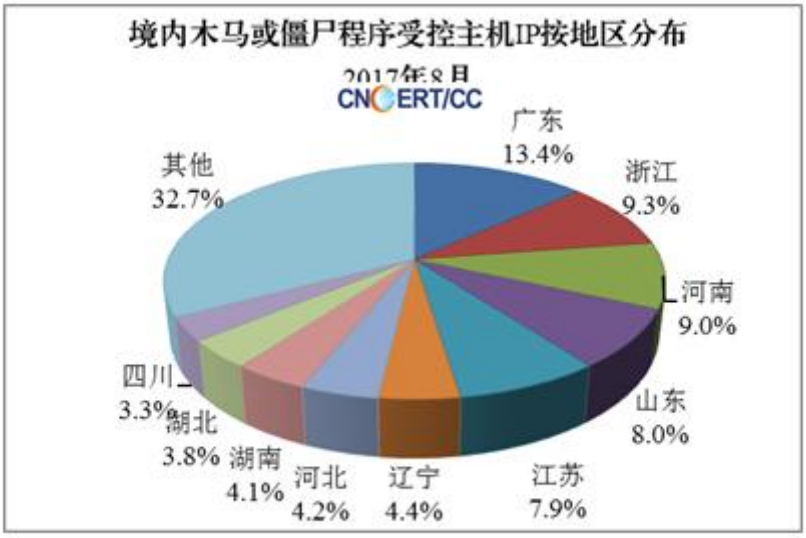

图 1：中国大陆木马或僵尸受控主机 IP 按地区分布

2.木马僵尸控制服务器的数量和分布

2017 年 8 月，监测发现我国大陆地区 2901 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 2739 个相比稍有增加，其分布情况如图 2 所示。其中，海南省 2 个（占全国 0.07%），全国排名第 30 位。

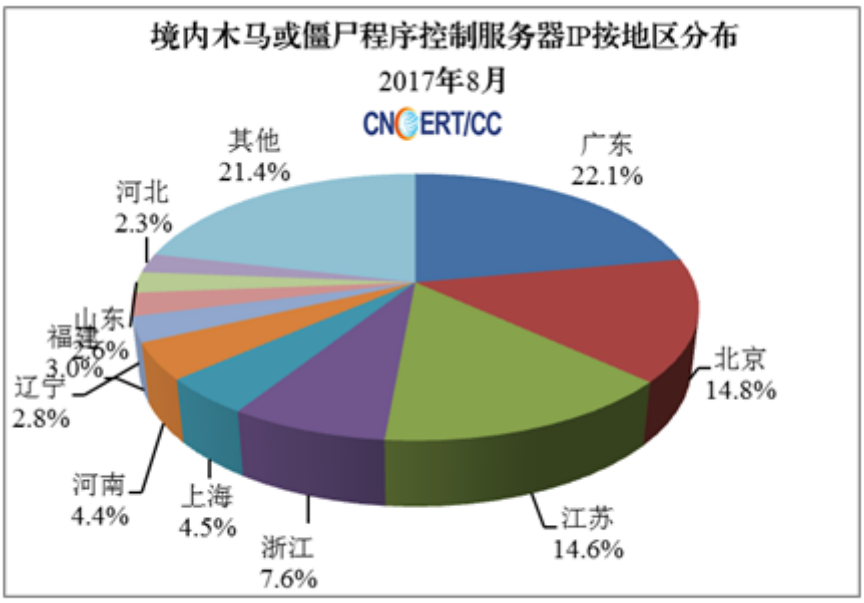

图 2：中国大陆木马或僵尸控制服务器 IP 按地区分布

3.境外木马控制服务器的数量和分布

2017 年 8 月，秘密控制我国大陆计算机的境外被木马控制的服务器 IP 有 7042 个，与上月的 5888 个相比增加了 19.6%，主要来自美国、俄罗斯等国家，具体分布如图 3 所示。

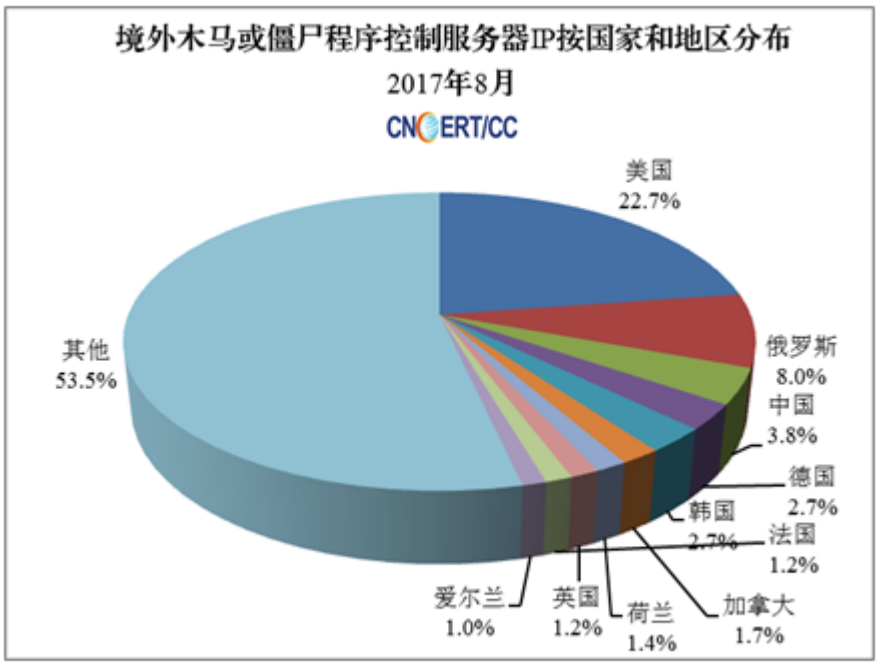

图 3：通过木马或僵尸程序控制中国大陆主机的境外 IP 按国家和地区分布

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 478 个，规模在 1000－5000 的有 170 个，分布情况如图 4 所示。

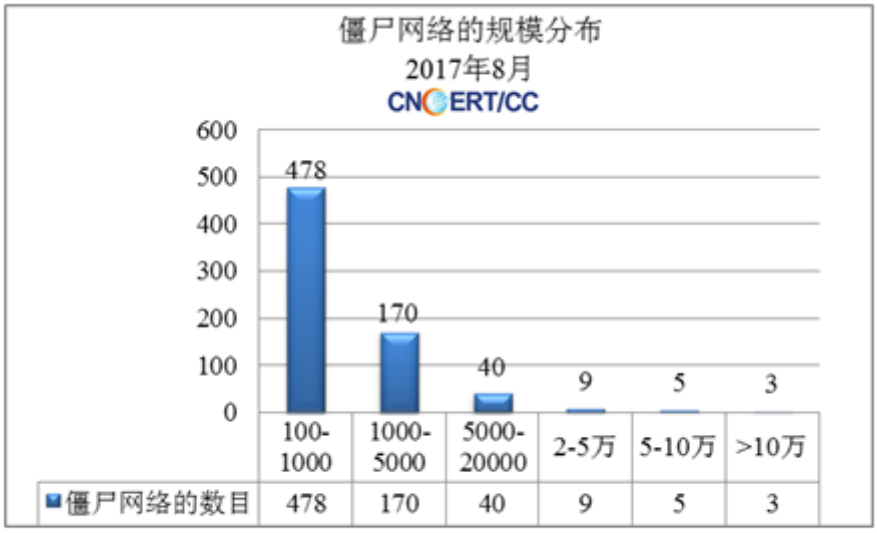

图 4：僵尸网络的规模分布

附 3：境内被植入后门的网站按地区分布

2017 年 8 月，监测发现我国大陆地区 4247 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 12 个（占全国 0.28%），排全国第 28 位。

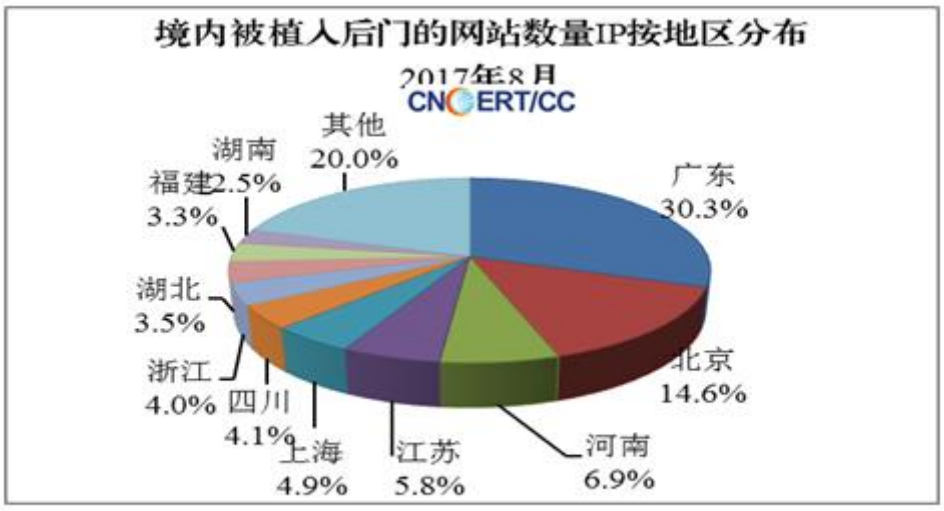

图 5：境内被植入后门的网站按地区分布

附 4：网页篡改监测数据分析

2017 年 8 月，我国大陆地区被篡改网站 6109 个，与上月的 6468 个相比稍有回落；其中，海南省 9 个（占全国 0.15%），排名第 25 位。具体分布如图 6 所示。

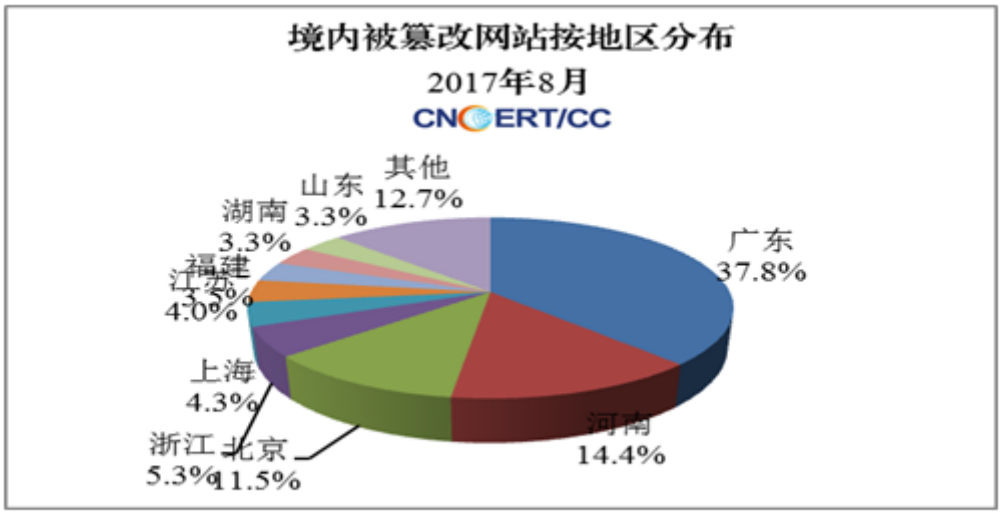

图 6：境内被篡改网站按地区分布

附 5：恶意代码数据分析

2017 年 8 月，恶意代码捕获与分析系统监测得到的放马站点统计如下所示：

1. 2017 年 8 月 CNCERT 捕获的恶意代码数量

名称	数量
新增恶意代码名称数	2
新增恶意代码家族数	0

2. 2017 年 8 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	www.go890.com	123.138.23.10
2	down.downcdn.net	120.26.127.170
3	cl.gxjsxq.com	61.133.192.170
4	down.downxiazai.net	117.23.6.63
5	down.nxwb.net	211.138.60.141
6	nc-dl.wdjcdn.com	117.23.6.68
7	dl.gxjsxq.com	117.23.6.67
8	cl.xzqxzs.com	223.111.16.246
9	dl.cdn.wandoujia.com	106.37.238.1
10	dl.wandoujia.com	113.142.84.79

附 6：重要漏洞与重要事件处置公告

2017 年 8 月，CNVD 整理和发布了以下重要安全漏洞信息，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）

关于重点防范 WindowsSearch 服务远程代码

执行漏洞威胁的安全公告

8 月，在微软公司发布的月度例行安全更新中，国家信息安全漏洞共享平台（CNVD）收录了 Windows Search 服务存在的一处远程代码执行漏洞（CNVD-2017-20509，对应 CVE-2017-8620）。根据分析，该漏洞潜在的利用方法有可能与此前 Wanancry 勒索病毒攻击原理类似，一旦披露利用代码，极有可能诱发大规模的攻击。

一、漏洞情况分析

Windows 搜索服务（WSS）是 windows 的一项默认启用的基本服务。允许用户在多个 Windows 服务和客户端之间进行搜索。

Windows 搜索处理内存中的对象时，存在远程执行代码漏洞，成功利用此漏洞的攻击者可以控制受影响的系统。虽然漏洞与 SMB 协议本身无关，但攻击者可 SMB 目标作为攻击媒介，因此该漏洞面临着与 Wannacry 类似的大规模利用风险。

CNVD 对该漏洞的技术评级为“高危”。

二、漏洞影响范围

漏洞影响微软公司多款 Windows 产品，包括个人桌面和服务器操作系统，列表如下 ：

Microsoft Windows 10 Version 1607 for 32-bit Systems

Microsoft Windows 10 Version 1607 for x64-based Systems

Microsoft Windows 10 for 32-bit Systems

Microsoft Windows 10 for x64-based Systems

Microsoft Windows 10 version 1511 for 32-bit Systems

Microsoft Windows 10 version 1511 for x64-based Systems

Microsoft Windows 10 version 1703 for 32-bit Systems

Microsoft Windows 10 version 1703 for x64-based Systems

Microsoft Windows 7 for 32-bit Systems SP1

Microsoft Windows 7 for x64-based Systems SP1

Microsoft Windows 8.1 for 32-bit Systems

Microsoft Windows 8.1 for x64-based Systems

Microsoft Windows RT 8.1

Microsoft Windows Server 2008 R2 for Itanium-based Systems SP1

Microsoft Windows Server 2008 R2 for x64-based Systems SP1

Microsoft Windows Server 2008 for 32-bit Systems SP2

Microsoft Windows Server 2008 for Itanium-based Systems SP2

Microsoft Windows Server 2008 for x64-based Systems SP2

Microsoft Windows Server 2012

Microsoft Windows Server 2012 R2

Microsoft Windows Server 2016

三、漏洞修复建议

建议Windows用户安装补丁更新,如果未能及时部署补丁更新,建议在禁用Windows Search服务。