海南省网络安全通报 2017 年第 12 期

一、我省本月网络安全总体情况

12 月，监测发现我省网络安全漏洞 18 起；被境外控制的木马僵尸受控主机数量为 11027 个，较上月 8842 个增加 24.7%，列全国第 16 位；木马僵尸控制服务器数量为 22 个，与上月持平。每日互联网流量最高值为 890G，最低值 100G，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。

12 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

12 月，海南互联网应急中心共向各运营企业下发了 559 条感染僵尸木马的 IP 数据，93 条僵尸木马病毒控制端 IP 数据，379 条感染蠕虫病毒的 IP 数据；网站漏洞数据 18 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

12 月，海南互联网应急中心协调运营企业处置手机病毒 157 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：网站后门事件 2 起，漏洞事件 18 起，恶意代码事件 49 起。

三、本月安全要闻回顾

特朗普发布首份《国家安全战略》要做三件事保护网络安全

美国当地时间 2017 年 12 月 18 日下午，特朗普公布了其任职期内的首份国家安全战略报告，长达 68 页，其中强调本届政府在全球及外交政策层面将始终坚持 “美国至上”的方针，囊括了用于改善美国国家网络安全方法的行动纲要清单。这份长达 68 页的报告文件中涉及多项美国国家安全问题，包括与中国之间的经济关系、美国核

武器库存的致命威胁，以及旨在改善国家网络安全方法的行动纲要清单。

白宫方面表示：美国将“投入资源以支持并提升实现网络攻击归因的能力，确保有能力作出快速反应。

网络安全战略报告总结建议指出，特朗普政府的计划将使得美国能够更轻松地“根据需求”对敌对方实施网络行动。美国政府将与美国国会合作，应对继续阻碍即时情报与信息共享、有碍网络工具规划运营以及开发的种种挑战。一旦拥有针对网络空间内恶意行为者采取行动的机会，美国将及时获悉相关风险，但在考虑应对选项时不会故意犯险。

美国将努力改善美国政府已经严重老化的 IT 基础设施。

这份国家安全战略报告提到美国将“在冲突范围内改善我们的网络工具，旨在保护美国政府资产及美国的关键信息基础设施，保障数据与信息的完整性。

美国政府还将推动一轮‘吸引、培养及挽留’各政府机构与部门网络安全专业人员队伍的努力。

2017 年初，特朗普签署了拖延很久的《增强联邦政府网络与关键性基础设施网络安全》总统行政令，要求在联邦政府之内建立多项网络安全评估指标——但此举尚未对美国政策作出任何重大改变。该项行政令要求各机构与部门负责人使用来自私营部门的网络安全最佳实践，从而进一步确保所在部门系统的安全性，同时以更大力度全面推进政府网络安全的现代化转型。

2017 年 12 月 12 日，特朗普签署了美国 《2018 财年国防授权法案》。该法案为美国 2018 财年制定了政策和预算指导方针，其中也包括各种网络安全举措。

附 1：网络安全信息报送情况

12 月，海南互联网应急中心处理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 1200 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）	
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	1188
合计	**1200**

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	379
木马事件	93
僵尸网络事件	559
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	0
垃圾邮件事件	0
其他网络安全事件	157
合计	**1188**

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 12 月，CNCERT 监测发现我国大陆地区 436377 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 637604 个相比减少了 31.56%，其分布情况如图 1 所示。其中，海南省 11027 个（占全国 2.53％），全国排名第 16 位。

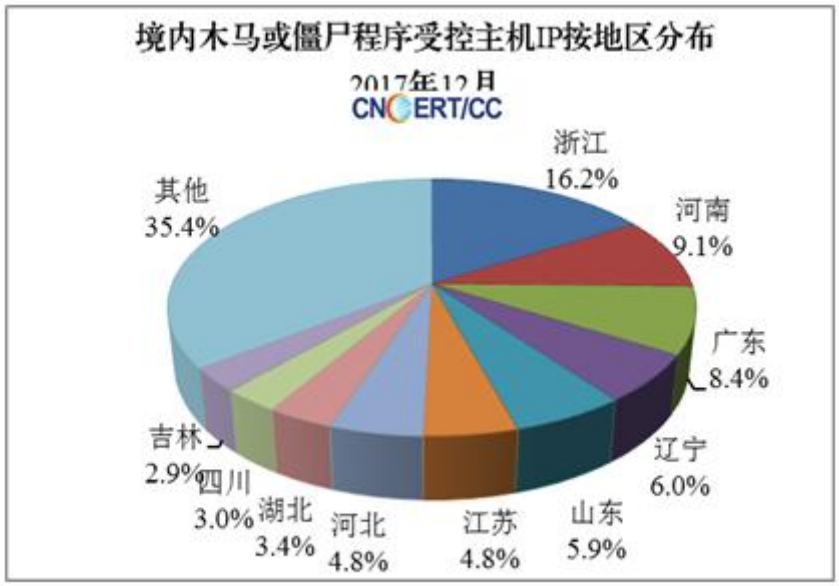

图 1：中国大陆木马或僵尸受控主机 IP 按地区分布

2、木马僵尸控制服务器的数量和分布

2017 年 12 月，CNCERT 监测发现我国大陆地区 2140 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 2484 个相比减少了 13.85%，其分布情况如图 2 所示。其中，海南省 22 个（占全国 1.03％），全国排名第 24 位。

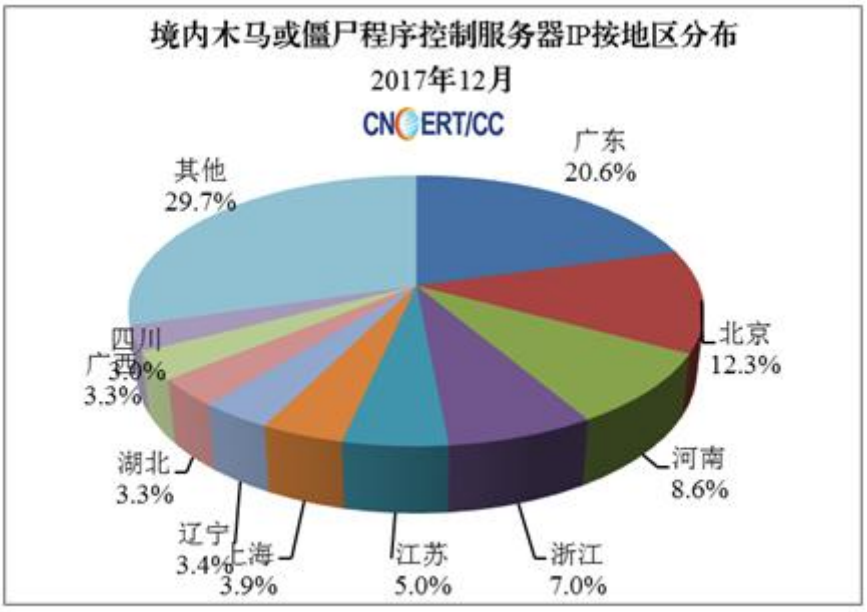

图 2：中国大陆木马或僵尸控制服务器 IP 按地区分布

3、境外木马控制服务器的数量和分布

2017 年 12 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 11339 个，与上月的 6911 个相比增加了 64.07%，主要来自美国、日本等国家，具体分布如图 3 所示。

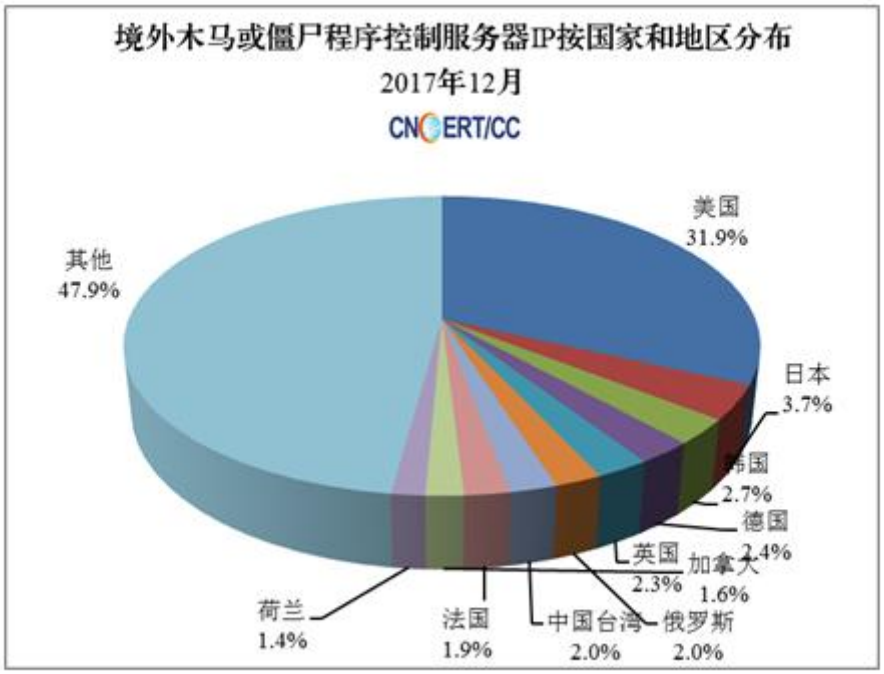

图 3：通过木马或僵尸程序控制中国大陆主机的境外 IP 按国家和地区分布

4、木马僵尸网络规模分布

2017 年 12 月，在 CNCERT 监测发现的僵尸网络中，规模大于 5000 的僵尸网络有 96 个，规模在 100－1000 的有 13127 个，规模在 1000－5000 的有 256 个，分布情况如图 4 所示。

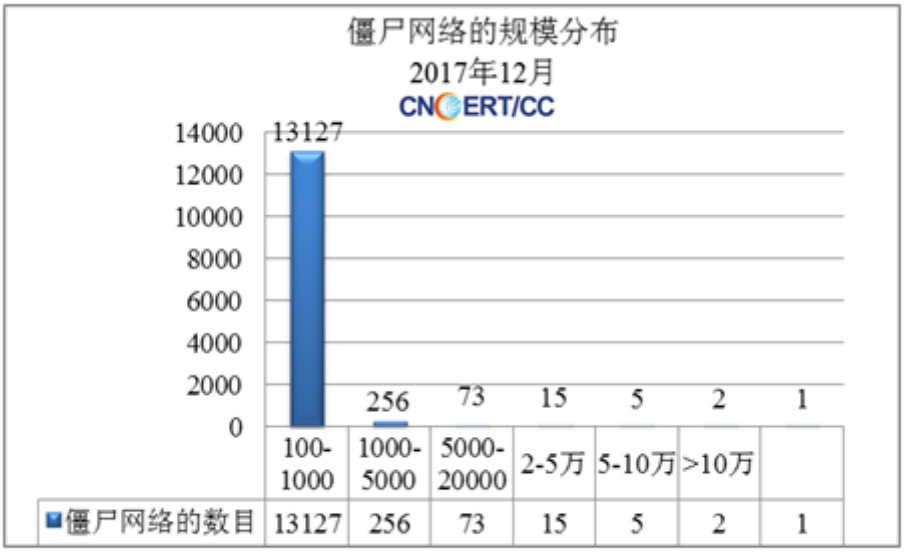

图 4：僵尸网络的规模分布

附 3、境内被植入后门的网站按地区分布

2017 年 12 月，CNCERT 监测发现我国大陆地区 3029 个网站被植入后门程序，比上月的 2504 个增加了 20.97%，其分布情况如图 5 示。其中，海南省 8 个（占全国 0.26%），排全国第 28 位。

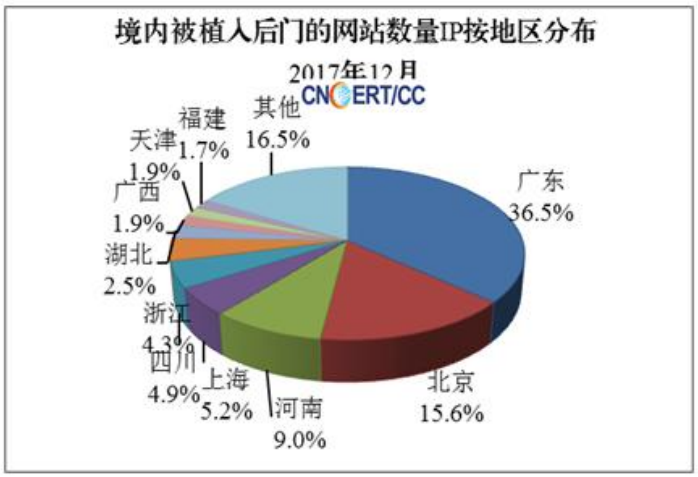

图 5：被植入后门的网站按地区分布

附 4、网页篡改监测数据分析

2017 年 12 月，CNCERT 监测发现我国大陆地区被篡改网站 4130 个，与上月的 2368 个相比增加了 74.41%；其中，海南省 9 个（占全国 0.22%），排名第 22 位。具体分布如图 6 所示。

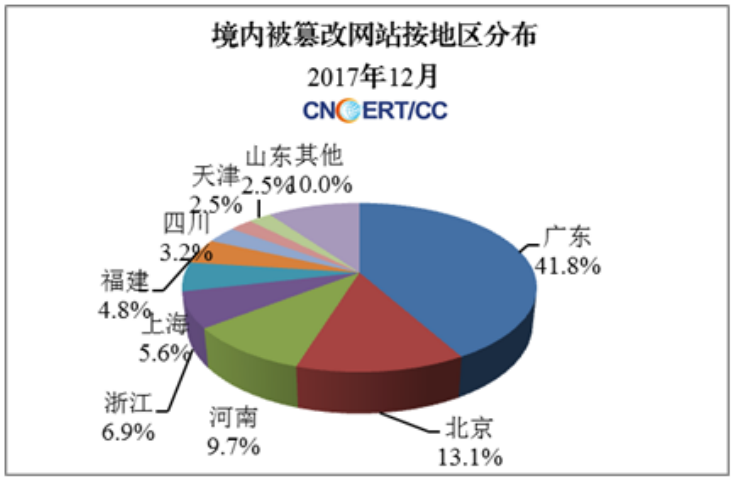

图 6：境内被篡改网站按地区分布

附 5：恶意代码数据分析

2017 年 12 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 12 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	0

2. 2017 年 12 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	43.242.181.16
2	www.go890.com	120.26.127.170
3	cl.urndf.com	117.23.6.63
4	cl2.cjsdxz.com	117.23.6.64
5	dl.urndf.com	117.23.6.65
6	dl.apxlx.com	125.76.247.169
7	cl.qpzqxz.com	218.95.139.53
8	cl.wokxn.com	61.133.192.170
9	wdx.go890.com	61.132.238.81
10	down.nxwb.net	118.180.26.36

附 6：重要漏洞与重要事件处置公告

2017 年 12 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 Synapse 存在远程代码执行漏洞的安全公告

2017 年 12 月 11 日，国家信息安全漏洞共享平台（CNVD）收录了 Apache Synapse 远程代码执行漏洞 CNVD-2017-36700，对应 CVE-2017-15708）。攻击者可利用上述漏洞通过注入特制的序列化对象远程执行代码。

一、漏洞情况分析

Apache Synapse 是一个简单的、高质量开放源代码的替代方法，为实现 SOA 提供了一种途径，它可以公开现有的应用程序，而无需重新编写任何代码。

近日，Apache Synapse 发布了新版本修复的一个远程代码执行漏洞（CVE-2017-15708）。该漏洞源于 Apache Commons Collections 库包含“functor”包中的各个类可被序列化所致。攻击者可以通过注入特制的序列化对象，并在其类路径中包含 Apache Commons Collections 库，且不执行任何类型的输入验证，导致可远程执行代码。CNVD 对该漏洞的综合评级为“高危”。

二、漏洞影响范围

漏洞影响 Apache Synapse 3.0.1 之前的所有版本。

三、防护建议

Apache Synapse 官方已经发布了最新的 3.0.1 版本修复该漏洞，请受影响的用户尽快升级到最新版本：

http://synapse.apache.org/download/3.0.1/download.cgi。

附：参考链接：

http://www.openwall.com/lists/oss-security/2017/12/10/4

http://synapse.apache.org/index.html

http://www.cnvd.org.cn/flaw/show/CNVD-2017-36700