海南省网络安全通报 2017 年第 5 期

一、我省本月网络安全总体情况

2017 年 5 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 7697 个，较上月 6956 个有小幅上涨，列全国第 26 位;我省木马僵尸控制服务器数量为 43 个,比上月增加 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。本月共监测发现网页篡改事件 5 起，重要信息系统漏洞事件 10 起。每日互联网流量最高值为 708G，最低值 99G，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。

5 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

5 月，海南互联网应急中心共向各运营企业下发了 789 条感染僵尸木马的 IP 数据，542 条僵尸木马病毒控制端 IP 数据，247 条感染蠕虫病毒的 IP 数据；后门 IP 数据 53 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

5 月，海南互联网应急中心协调运营企业处置手机病毒 362 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：恶意程序 74 起，漏洞事件 10 起，网页篡改 2 起，后门事件 10 起。

附 1：网络安全信息报送情况

5 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 1179 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 5）	
事件类型	**数量**
IP 业务	0
基础 IP 网络	13
运营企业自有业务系统	0
域名系统	0
公共互联网环境	1166
合计	**1179**

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	247
木马事件	76
僵尸网络事件	466
域名劫持事件	0
网络仿冒事件	0
网页篡改事件	5
网页挂马事件	0
拒绝服务攻击事件	0
后门事件	10
非授权访问事件	0
垃圾邮件事件	0
其他网络安全事件	362
合计	**1166**

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 5 月，监测发现我国大陆地区 1257107 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 1016871 个相比增加了 23.63%，其分布情况如图 1 所示。其中，海南省 7697 个（占全国 0.61%），全国排名第 26 位。

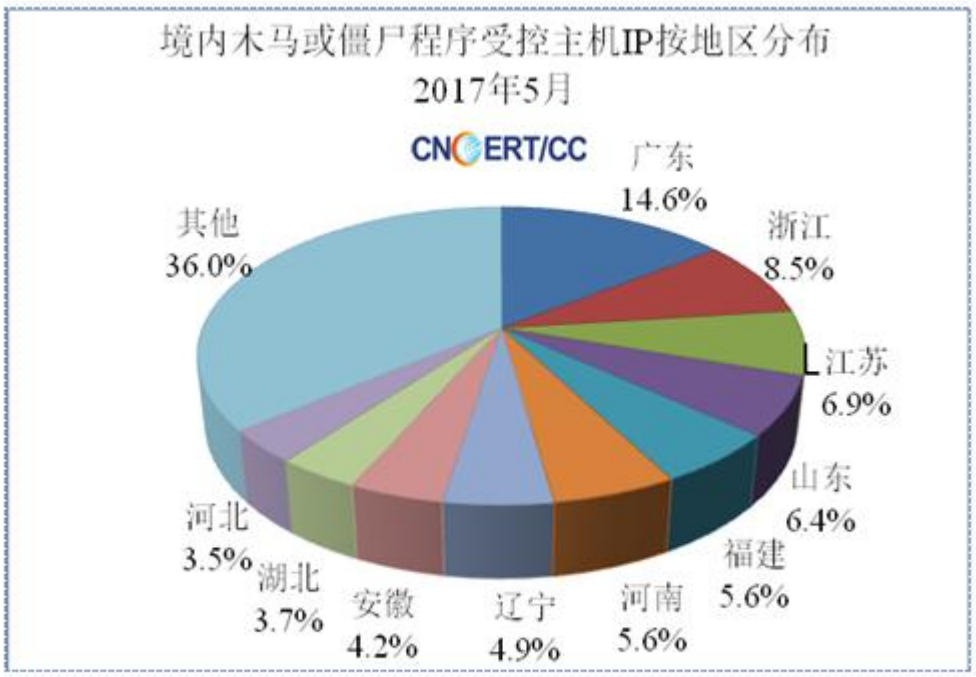

图 1：中国大陆木马或僵尸受控主机 IP 按地区分布

2、木马僵尸控制服务器的数量和分布

2017 年 5 月，监测发现我国大陆地区 16206 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 6800 个相比增加了 138.30%，其分布情况如图 2 所示。其中，海南省 43 个（占全国 0.27%），全国排名第 26 位。

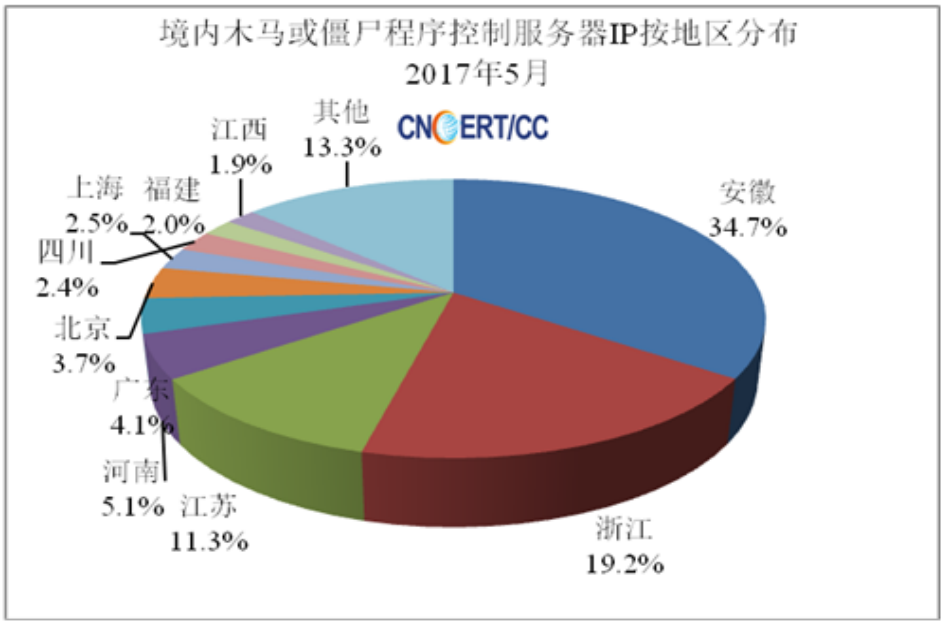

图 2：中国大陆木马或僵尸控制服务器 IP 按地区分布

3、境外木马控制服务器的数量和分布

2017 年 5 月，秘密控制我国大陆计算机的境外木马控制服务器 IP 有 11308 个，与上月的 6890 个相比增加了 64.1%，主要来自美国、韩国等国家，具体分布如图 3 所示。

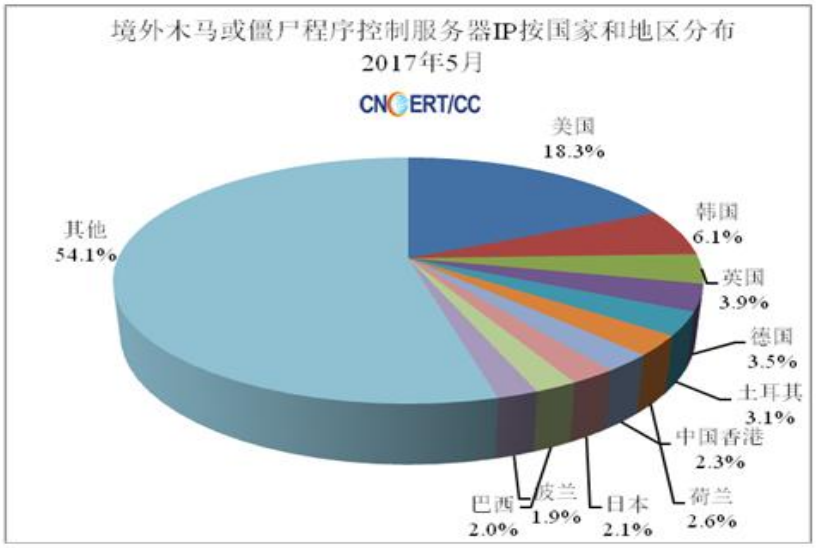

图 3：通过木马或僵尸程序控制中国大陆主机的境外 IP 按国家和地区分布

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 38 个，规模在 100－1000 的有 358 个，规模在 1000－5000 的有 113 个，分布情况如图 4 所示。

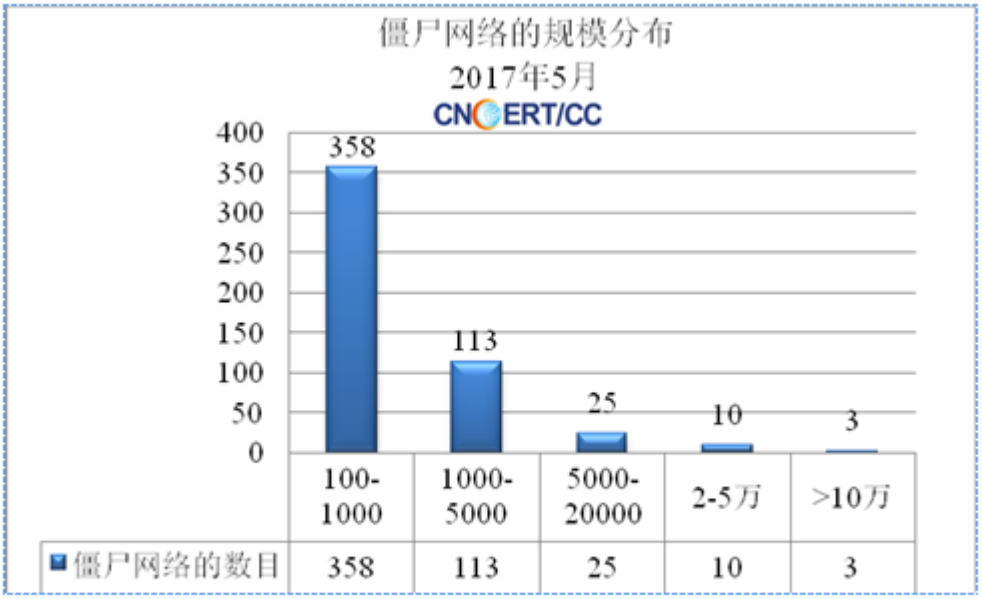

图 4：僵尸网络的规模分布

附 3:境内被植入后门的网站按地区分布

2017 年 5 月，监测发现我国大陆地区 4916 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 19 个（占全国 0.39%），排全国第 25 位。

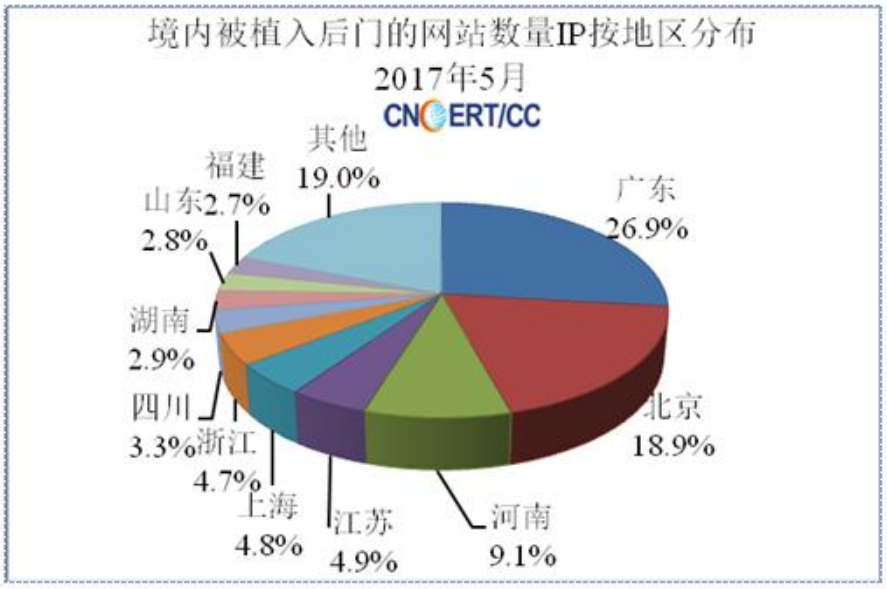

图 5：境内被植入后门的网站按地区分布

附 4:网页篡改监测数据分析

2017 年 5 月，我国大陆地区被篡改网站 6245 个，与上月的 6312 个相比有所减少；其中，海南省 5 个（占全国 0.06%），排名第 25 位。具体分布如图 6 所示。

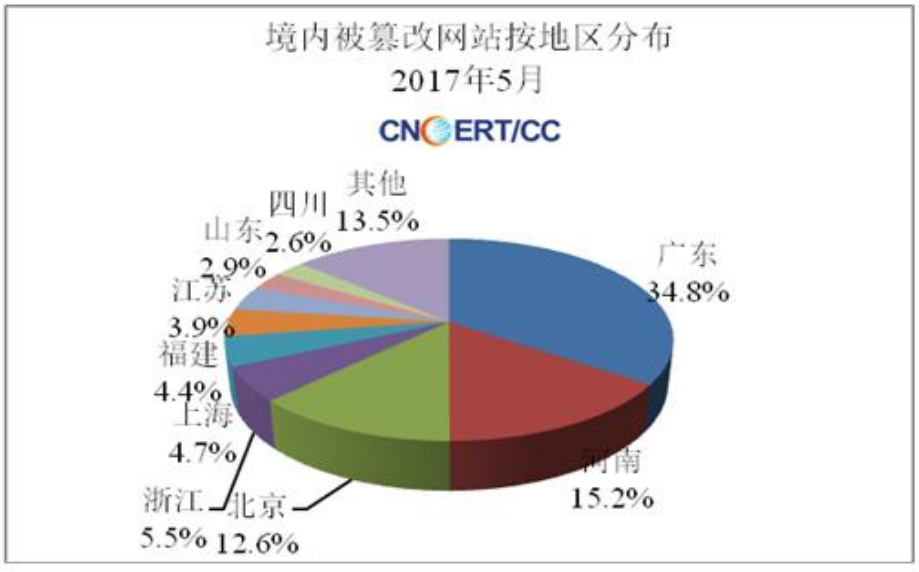

图 6：境内被篡改网站按地区分布

附 5：恶意代码数据分析

2017 年 5 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 5 月 CNCERT 捕获的恶意代码数量

名称	数量
新增恶意代码名称数	4
新增恶意代码家族数	1

2. 2017 年 5 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	183.60.106.54
2	cl.xzqxzs.com	120.26.127.170
3	down.nxwb.net	61.133.192.170
4	nc-dl.wdjcdn.com	106.37.238.1
5	i.kpzip.com	36.42.32.220
6	cl.gxjsxq.com	117.23.6.67
7	dl.wandoujia.com	117.23.6.64
8	dl.cdn.wandoujia.com	222.28.152.177
9	idq.liukejun.com	221.230.141.238
10	icq.liukejun.com	117.23.6.63

附 6：重要漏洞与重要事件处置公告

2017 年 5 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）

关于重点防范 Windows 操作系统勒索软件

攻击的情况公告

安全公告编号:CNTA-2017-0029

安全公告编号:CNTA-2017-0039

北京时间 5 月 13 日，互联网上出现针对 Windows 操作系统的勒索软件的攻击案例，勒索软件利用此前披露的 Windows SMB 服务漏洞（对应微软漏洞公告：MS17-010）攻击手段，向终端用户进行渗透传播，并向用户勒索比特币或其他价值物，涉及到国内用户（已收到多起高校案例报告），已经构成较为严重的攻击威胁。

一、勒索软件情况

4 月 16 日，CNCERT 主办的 CNVD 发布《关于加强防范 Windows 操作系统和相关软件漏洞攻击风险的情况公告》，对影子纪经人“ShadowBrokers”披露的多款涉及 Windows 操作系统 SMB 服务的漏洞攻击工具情况进行了通报（相关工具列表如下），并对有可能产生的大规模攻击进行了预警:

表 有可能通过 445 端口发起攻击的漏洞攻击工具

工具名称	主要用途
ETERNALROMANCE	SMB 和 NBT 漏洞，对应 MS17-010 漏洞，针对 139 和 445 端口发起攻击，影响范围:Windows XP, 2003, Vista, 7, Windows 8, 2008, 2008 R2
EMERALDTHREAD	SMB 和 NETBIOS 漏洞，对应 MS10-061 漏洞，针对 139 和 445 端口，影响范围：Windows XP、Windows 2003
EDUCATEDSCHOLAR	SMB 服务漏洞，对应 MS09-050 漏洞，针对 445 端口
ERRATICGOPHER	SMBv1 服务漏洞，针对 445 端口，影响范围：Windows XP、 Windows server 2003，不影响 windows Vista 及之后的操作系统
ETERNALBLUE	SMBv1、SMBv2 漏洞，对应 MS17-010，针对 445 端口,影响范围：较广，从 WindowsXP 到 Windows 2012
ETERNALSYNERGY	SMBv3 漏洞，对应 MS17-010，针对 445 端口，影响范围：Windows8、Server2012
ETERNALCHAMPION	SMB v2 漏洞，针对 445 端口

综合 CNVD 技术组成员单位奇虎 360 公司、安天公司等单位已获知的样本情况和分析结果，该勒索软件在传播时基于 445 端口并利用

SMB 服务漏洞(MS17-010),总体可以判断是由于此前“Shadow Brokers”披露漏洞攻击工具而导致的后续黑产攻击威胁。当用户主机系统被该勒索软件入侵后，弹出如下勒索对话框，提示勒索目的并向用户索要比特币。而用户主机上的重要数据文件，如：照片、图片、文档、压缩包、音频、视频、可执行程序等多种类型的文件，都被恶意加密且后缀名统一修改为“.WNCRY”。目前，安全业界暂未能有效破除该勒索软的恶意加密行为，用户主机一旦被勒索软件渗透，只能通过重装操作系统的方式来解除勒索行为，但用户重要数据文件不能直接恢复。

图 勒索软件界面图（来源：安天公司）

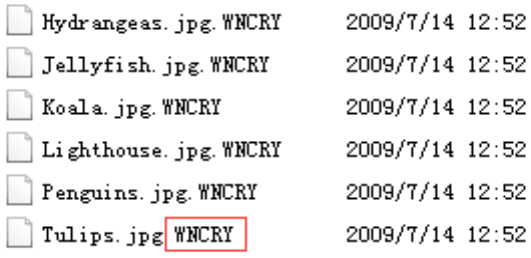

图 用户文件被加密（来源：安天公司）

二、应急处置措施

根据CNVD秘书处普查的结果，互联网上共有900余万台主机IP暴露445端口（端口开放），而中国大陆地区主机IP有300余万台。CNCERT已经着手对勒索软件及相关网络攻击活动进行监测，目前共发现有向全球70多万个目标直接发起的针对MS17-010漏洞的攻击尝试。建议广大用户及时更新Windows已发布的安全补丁，同时在网络边界、内部网络区域、主机资产、数据备份方面做好如下工作：

（一）关闭445等端口(其他关联端口如：135、137、139)的外部网络访问权限，在服务器上关闭不必要的上述服务端口；

（二）加强对445等端口（其他关联端口如：135、137、139)的内部网络区域访问审计，及时发现非授权行为或潜在的攻击行为；

（三)由于微软对部分操作系统停止安全更新，建议对WindowXP和Windows server 2003主机进行排查（MS17-010更新已不支持），使用替代操作系统。

（四）做好信息系统业务和个人数据的备份。CNCERT后续将密切监测和关注该勒索软件对境内党政机关和重要行业单位以及高等院校的攻击情况，同时联合安全业界对有可能出现的新的攻击传播手段、恶意样本变种进行跟踪防范。

附：参考链接

https://blogs.technet.microsoft.com/msrc/2017/04/14/protecting-customers-and-evaluating-risk/?from=timeline&isappinstalled=0（微软发布的官方安全公告）

https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/（微软发布已停服务的 XP 和部分服务器版特别补丁）

http://www.cnvd.org.cn/webinfo/show/4110（CNVD 安全公告）