海南省网络安全通报 2017 年第 6 期

一、我省本月网络安全总体情况

2017 年 6 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 31417 个，较上月 7697 个有大幅上涨，列全国第 28 位；我省木马僵尸控制服务器数量为 63 个，比上月增加 20 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。本月共监测发现重要信息系统事件 5 起，网页篡改安全事件 4 起，重要信息系统漏洞事件 11 起。每日互联网流量最高值为 652G，最低值 100G，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。

6 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

6月，海南互联网应急中心共向各运营企业下发了725条感染僵尸木马的IP数据，43条僵尸木马病毒控制端IP数据，466条感染蠕虫病毒的IP数据，存在后门IP数据5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

6月，海南互联网应急中心协调运营企业处置手机病毒169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，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，企业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：漏洞事件11起，后门事件5起，恶意代码事件74起。

附1：网络安全信息报送情况

6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1423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 6 月）	
事件类型	**数量**
IP 业务	0
基础 IP 网络	11
运营企业自有业务系统	0
域名系统	0
公共互联网环境	1412
合计	**1423**

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	466
木马事件	43
僵尸网络事件	725
域名劫持事件	0
网络仿冒事件	0
网页篡改事件	4
网页挂马事件	0
拒绝服务攻击事件	0
后门事件	5
非授权访问事件	0
垃圾邮件事件	0
其他网络安全事件	169
合计	**1412**

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 6 月，监测发现我国大陆地区 1409439 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 1257107 个相比增加了 12.12%，其分布情况如图 1 所示。其中，海南省 31417 个（占全国 2.23%），全国排名第 28 位。

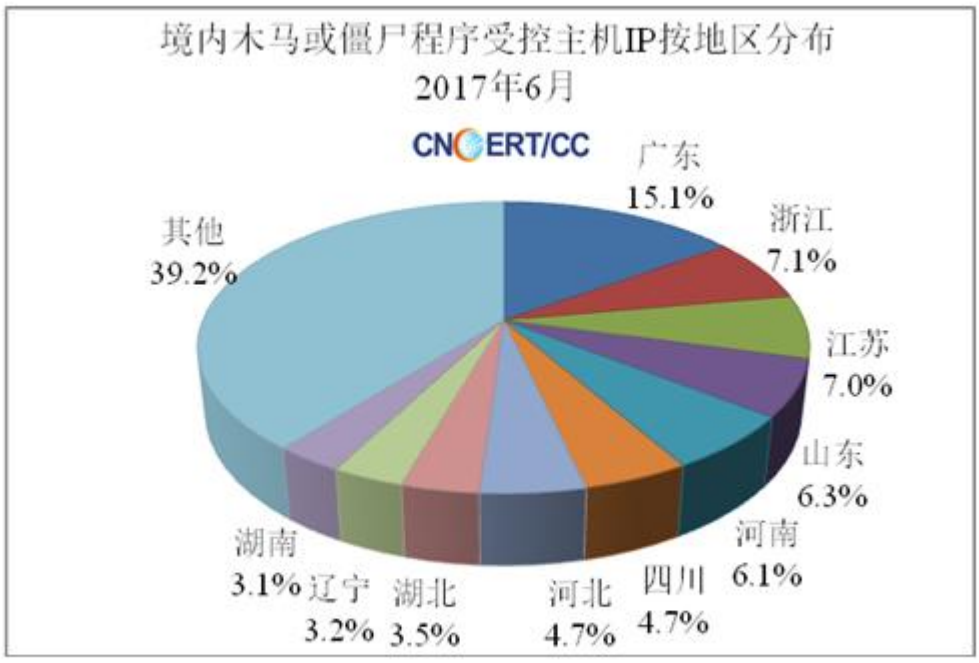

图 1：中国大陆木马或僵尸受控主机 IP 按地区分布

2、木马僵尸控制服务器的数量和分布

2017 年 6 月，监测发现我国大陆地区 49018 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 16206 个相比增加了 202.47%，其分布情况如图 2 所示。其中，海南省 63 个（占全国 0.27%），全国排名第 29 位。

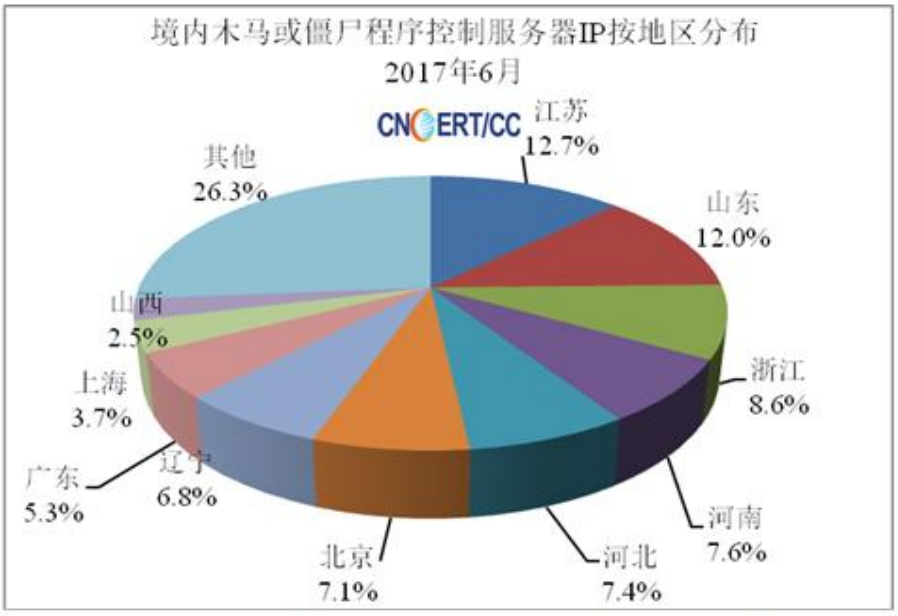

图 2：中国大陆木马或僵尸控制服务器 IP 按地区分布

3、境外木马控制服务器的数量和分布

2017 年 6 月，秘密控制我国大陆计算机的境外木马控制服务器 IP 有 20871 个，与上月的 11308 个相比增加了 84.57%，主要来自日本、美国等国家，具体分布如图 3 所示。

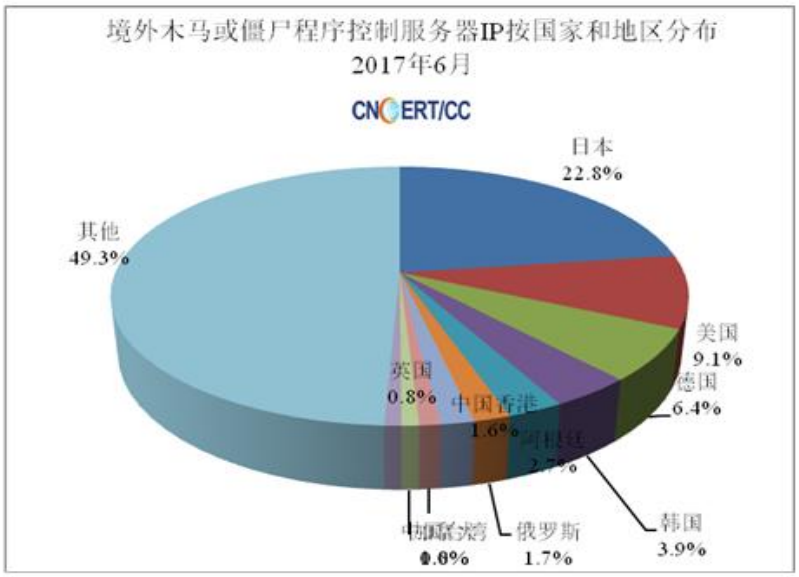

图 3：通过木马或僵尸程序控制中国大陆主机的境外 IP 按国家和地区分布

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 47 个，规模在 100－1000 的有 345 个，规模在 1000－5000 的有 85 个，分布情况如图 4 所示。

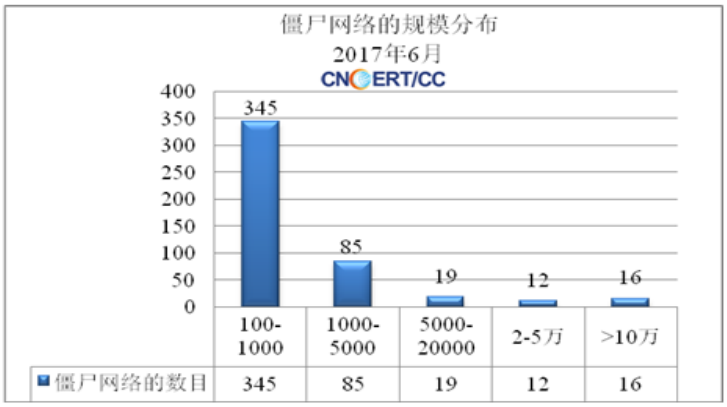

图 4：僵尸网络的规模分布

附 3、境内被植入后门的网站按地区分布

2017 年 6 月，监测发现我国大陆地区 4226 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 10 个（占全国 0.39%），排全国第 28 位。

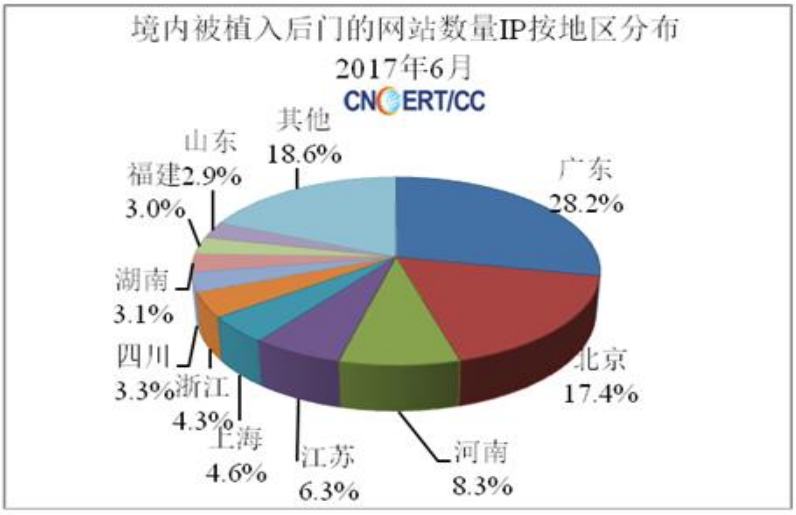

图 5：境内被植入后门的网站按地区分布

附 4、网页篡改监测数据分析

2017 年 6 月，我国大陆地区被篡改网站 3669 个，与上月的 6245 个相比有大幅减少；其中，海南省 4 个（占全国 0.11%），排名第 26 位。具体分布如图 6 所示。

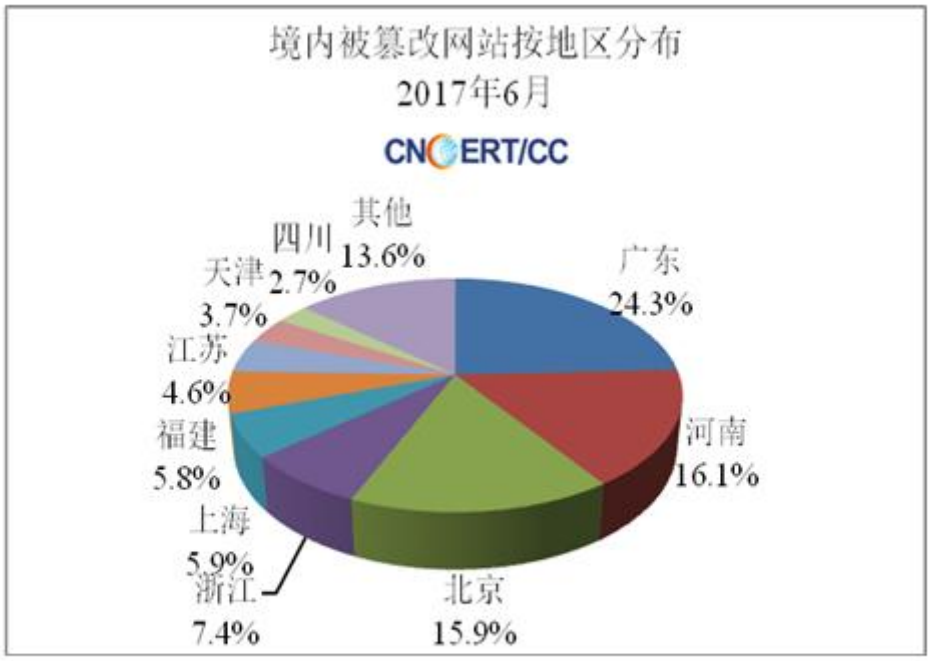

图 6：境内被篡改网站按地区分布

附 5：恶意代码数据分析

2017 年 6 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 6 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. 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	dl.wandoujia.com	106.37.238.1
2	dl.cdn.wandoujia.com	111.206.15.2
3	nc-dl.wdjcdn.com	120.26.127.170
4	i.kpzip.com	61.136.163.78
5	cl.xzqxzs.com	183.60.106.54
6	cl.gxjsxq.com	122.70.142.167
7	www.go890.com	61.133.192.170
8	down.nxwb.net	222.28.152.177
9	cl2.cjsdxz.com	61.233.139.70
10	cl2.dhfszh.com	110.40.4.3

附 6：重要漏洞与重要事件处置公告

2017 年 6 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）

关于海康威视与大华股份多款网络摄像机产品
存在身份认证绕过与配置文件密码泄露等高危漏洞的安全公告

近期，国家信息安全漏洞共享平台（CNVD）收录了海康威视与大华股份网络摄像机存在身份认证绕过漏洞、配置文件密码泄露等漏洞（CNVD-2017-06977、CNVD-2017-08191、CNVD-2017-08192、CNVD-2017-06997）。综合利用上述漏洞，远程攻击者可利用漏洞提升权限或加密其他用户身份获取敏感信息，并控制网络设备。由于漏洞利用较为简单,有可能被黑客组织利用于传播网络病毒(如:蠕虫)。

一、漏洞情况分析

Hikvision Cameras、Hikvision DS-2CD2xx2F-I 等系列为海康威视（Hikvision）公司（股票代码：SZ.002415）的网络摄像机产品；大华 DH-IPC-HDBW23A0RN-ZS 等系列设备为大华（DaHua）公司（股票代码：SZ.002236）的网络摄像机产品。多款网络摄像机产品存在类似身份认证不当漏洞与配置文件密码泄露漏洞，远程攻击者可利用漏洞提升权限或加密其他用户身份获取敏感信息，并控制网络设备。

详情如下：

漏洞编号	漏洞描述	主要影响产品
CNVD-2017-06977、CVE-2017-7921	海康威视多个网络摄像机产品存在身份认证不当漏洞，应用程序没有充分或正确地验证用户，则会出现不正确的身份验证漏洞。可能会允许攻击者在系统上升级其权限，并获取敏感信息。	Hikvision Digital Technology DS-2DFx Series 5.4.5 Build 160928
		Hikvision Digital Technology DS-2DFx Series 5.2 build 140805
		Hikvision Digital Technology DS-2CD63xx Series 5.3.5 Build 160106
		Hikvision Digital Technology DS-2CD63xx Series 5.0.9 build 140305
		Hikvision Digital Technology DS-2CD4xx5 Series 5.4 Build 160421
		Hikvision Digital Technology DS-2CD4xx5 Series 5.2 build 140721
		Hikvision Digital Technology DS-2CD4x2xFWD Series 5.4 Build 160414
		Hikvision Digital Technology DS-2CD4x2xFWD Series 5.2 build 140721
		Hikvision Digital Technology DS-2CD2xx2FWD Series 5.4.4 Build 161125
		Hikvision Digital Technology DS-2CD2xx2FWD Series 5.3.1 build 150410

		Hikvision Digital Technology DS-2CD2xx2F-I Series 5.4 build 160530
		Hikvision Digital Technology DS-2CD2xx2F-I Series 5.2 build 140721
		Hikvision Digital Technology DS-2CD2xx0F-I Series 5.4 Build 160401
		Hikvision Digital Technology DS-2CD2xx0F-I Series 5.2 build 140721
CNVD-2017-08191、CVE-2017-7923	海康威视多款摄像机被发现密码直接保存在配置文件中，攻击者可以利用该漏洞导致用户可提升权限或假冒另一用户的身份，从而访问敏感信息。	DS-2CD2xx2F-I Series V5.2.0 build 140721 to V5.4.0 Build 160530
		DS-2CD2xx0F-I Series V5.2.0 build 140721 to V5.4.0 Build 160401
		DS-2CD2xx2FWD Series V5.3.1 build 150410 to V5.4.4 Build 161125
		DS-2CD4x2xFWD Series V5.2.0 build 140721 to V5.4.0 Build 160414
		DS-2CD4xx5 Series V5.2.0 build 140721 to V5.4.0 Build 160421
		DS-2DFx Series V5.2.0 build 140805 to V5.4.5 Build 160928
		DS-2CD63xx Series V5.0.9 build 140305 to V5.3.5 Build 160106

CNVD-2017-08192、CVE-2017-7925	大华(Dahua)多款数字录像机和IP摄像机被发现密码直接保存在配置文件中，攻击者可利用该漏洞假冒特权用户的身份并获得对敏感信息的访问权。	DH-IPC-HDBW23A0RN-ZS, DH-IPC-HDBW13A0SN, DH-IPC-HDW1XXX, DH-IPC-HDW2XXX, DH-IPC-HDW4XXX, DH-IPC-HFW1XXX, DH-IPC-HFW2XXX, DH-IPC-HFW4XXX, DH-SD6CXX, DH-NVR1XXX, DH-HCVR4XXX, DH-HCVR5XXX, DHI-HCVR51A04HE-S3, DHI-HCVR51A08HE-S3, and DHI-HCVR58A32S-S2
CNVD-2017-06997、CVE-2017-7927	大华(Dahua)的多款网络摄像机存在身份验证漏洞。设备使用用户密码hash值替代密码本身来验证身份，这可能允许攻击者不获得实际密码的情况下绕过身份验证，获得设备权限。	Dahuasecurity DHI-HCVR58A32S-S2 0
		Dahuasecurity DHI-HCVR51A08HE-S3 0
		Dahuasecurity DHI-HCVR51A04HE-S3 0
		Dahuasecurity DH-SD6CXX 0
		Dahuasecurity DH-NVR1XXX 0
		Dahuasecurity DH-IPC-HFW4XXX 0
		Dahuasecurity DH-IPC-HFW2XXX 0
		Dahuasecurity DH-IPC-HFW1XXX 0
		Dahuasecurity DH-IPC-HDW4XXX 0
		Dahuasecurity DH-IPC-HDW2XXX 0
		Dahuasecurity DH-IPC-HDW1XXX 0
		Dahuasecurity DH-IPC-HDBW23A0RN-ZS 0
		Dahuasecurity DH-IPC-HDBW13A0SN 0
		Dahuasecurity DH-HCVR5XXX 0
		Dahuasecurity DH-HCVR4XXX 0

CNVD对上述漏洞综合评级为“高危”。

二、防护建议

目前，海康威视公司和大华公司已及时给出了上述漏洞的安全解决方案，请访问厂商主页及时修复漏洞：

http://www.hikvision.com/us/about_10805.html

http://www.hikvision.com/us/about_10807.html

http://us.dahuasecurity.com/en/us/Security-Bulletin_030617.php

http://us.dahuasecurity.com/en/us/Security-Bulletin_04032017.php

若未能及时升级，建议可以通过临时关闭网络摄像机产品的远程管理界面或认证端口来防范网络攻击。

附：参考链接：

http://www.securityfocus.com/bid/98312

http://www.securityfocus.com/bid/98313

https://nvd.nist.gov/vuln/detail/CVE-2017-7921

https://nvd.nist.gov/vuln/detail/CVE-2017-7923

https://nvd.nist.gov/vuln/detail/CVE-2017-7925

https://nvd.nist.gov/vuln/detail/CVE-2017-7927

http://www.cnvd.org.cn/flaw/show/CNVD-2017-06977

http://www.cnvd.org.cn/flaw/show/CNVD-2017-08191

http://www.cnvd.org.cn/flaw/show/CNVD-2017-08192

http://www.cnvd.org.cn/flaw/show/CNVD-2017-08191