海南省网络安全通报 2017 年第 10 期

一、我省本月网络安全总体情况

10 月，海南省发生网页篡改安全事件 7 起；被境外控制的木马僵尸受控主机数量为 9700 个，较上月 10985 个有所减少，列全国第 23 位；木马僵尸控制服务器数量为 22 个，比上月增加 7 个。每日互联网流量最高值为 920G，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。

10 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

10 月，海南互联网应急中心共向各运营企业下发了 743 条感染僵尸木马的 IP 数据，56 条僵尸木马病毒控制端 IP 数据，480 条感染蠕虫病毒的 IP 数据；网站漏洞数据 17 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

10 月，海南互联网应急中心协调运营企业处置手机病毒 175 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 8 起，网页篡改事件 4 起，漏洞事件 17 起，恶意代码事件 80 起。

三、本月安全要闻回顾

1、第二届内地-香港网络安全论坛成功举办

中国网 10 月 18 日消息 2017 年 10 月 15 日，第二届内地-香港网络安全论坛在厦门市成功举办，中央网信办网络安全协调局局长赵泽良、香港特区政府资讯科技总监杨德斌出席，来自两地政府、高校和产业界的约 150 名专家代表参加了论坛。

论坛邀请了北京大学、四川大学、中国电子技术标准化研究院，以及香港个人资料私隐专员公署、智能城市联盟数据产业委员会的专家，围绕两地数据安全保护政策法律、个人信息保护标准与实践、网络安全人才培养等共同关心的话题，同两地代表进行了交流讨论，分享了经验做法。

2、WiFi 漏洞几乎影响所有无线设备

新浪网 10 月 17 日消息 北京时间 10 月 17 日早间消息，有计算机安全专家发现了 WiFi 设备的安全协议存在漏洞。这个漏洞影响许多设备，比如计算机、手机、路由器，几乎每一款无线设备都有可能被攻击。

漏洞名叫“KRACK”，也就是“KeyReinstallation Attack”（密钥重安装攻击）的缩写，它曝露了 WPA2 的一个基本漏洞，WPA2 是一个通用协议，大多现代无线网络都用到了该协议。计算机安全学者马蒂•凡赫尔夫（Mathy Vanhoef）发现了漏洞，他说漏洞存在于四路握手（four-wayhandshake）机制中，四路握手允许拥有预共享密码的新设备加入网络。

在最糟糕的情况下，攻击者可以利用漏洞从 WPA2 设备破译网络流量、劫持链接、将内容注入流量中。换言之，攻击者通过漏洞可以获得一个万能密钥，不需要密码就可以访问任何 WAP2 网络。一旦拿到密钥，他们就可以窃听你的网络信息。

漏洞的存在意味着 WAP2 协议完全崩溃，影响个人设备和企业设备，几乎每一台设备都受到威胁。

凡赫尔夫说：“如果你的设备支持 WiFi，极有可能会受到影响。”不过凡赫尔夫没有公布任何概念验证漏洞利用代码，暂时不会有太大的影响，攻击也不会大规模爆发。

周一时，美国国土安全局网络应急部门 US-CERT 确认了漏洞的存在，早在 2 个月前，US-CERT 已经秘密通知厂商和专家，告诉它们存在这样的漏洞。在 Black Hat 安全会议上，凡赫尔夫发表关于网络协议的演讲，他在讲话中谈到了新漏洞。

附 1：网络安全信息报送情况

10 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 1478 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	1466
合计	**1478**

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	480
木马事件	56
僵尸网络事件	743
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	8
非授权访问事件	0
垃圾邮件事件	0
其他网络安全事件	175
合计	**1466**

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 10 月，CNCERT 监测发现我国大陆地区 841752 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 1051278 个相比减少了 19.93%，其分布情况如图 1 所示。其中，海南省 9700 个（占全国 1.15%），全国排名第 23 位。

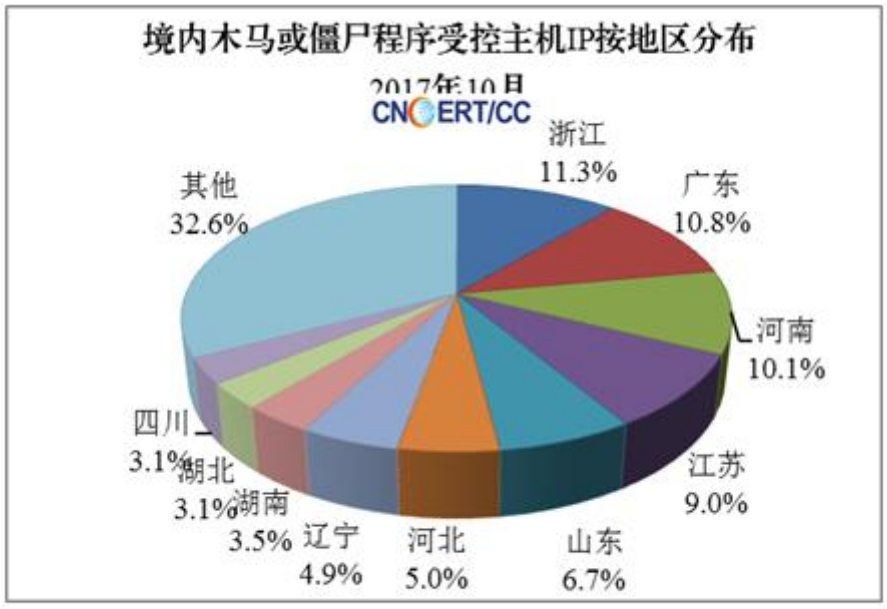

图 1：中国大陆木马或僵尸受控主机 IP 按地区分布

2、木马僵尸控制服务器的数量和分布

2017 年 10 月，CNCERT 监测发现我国大陆地区 2680 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 2416 个相比增加了 10.93%，其分布情况如图 2 所示。其中，海南省 22 个（占全国 0.82%），全国排名第 20 位。

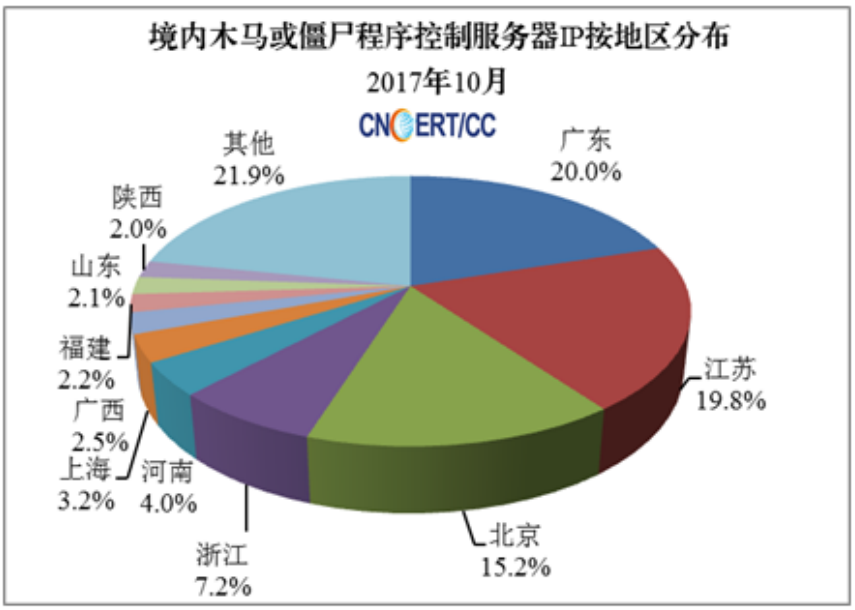

图 2：中国大陆木马或僵尸控制服务器 IP 按地区分布

3、境外木马控制服务器的数量和分布

2017 年 10 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 6466 个，与上月的 5560 个相比增加了 16.29%，主要来自美国、俄罗斯等国家，具体分布如图 3 所示。

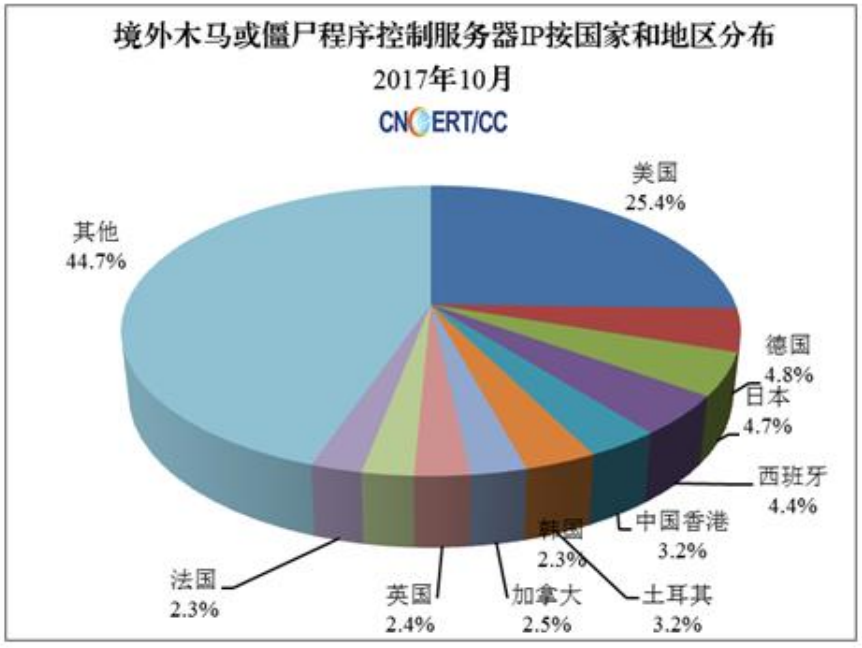

图 3：通过木马或僵尸程序控制中国大陆主机的境外 IP 按国家和地区分布

4、木马僵尸网络规模分布

在 CNCERT 监测发现的僵尸网络中，规模大于 5000 的僵尸网络有 36 个，规模在 100－1000 的有 260 个，规模在 1000－5000 的有 74 个，分布情况如图 4 所示。

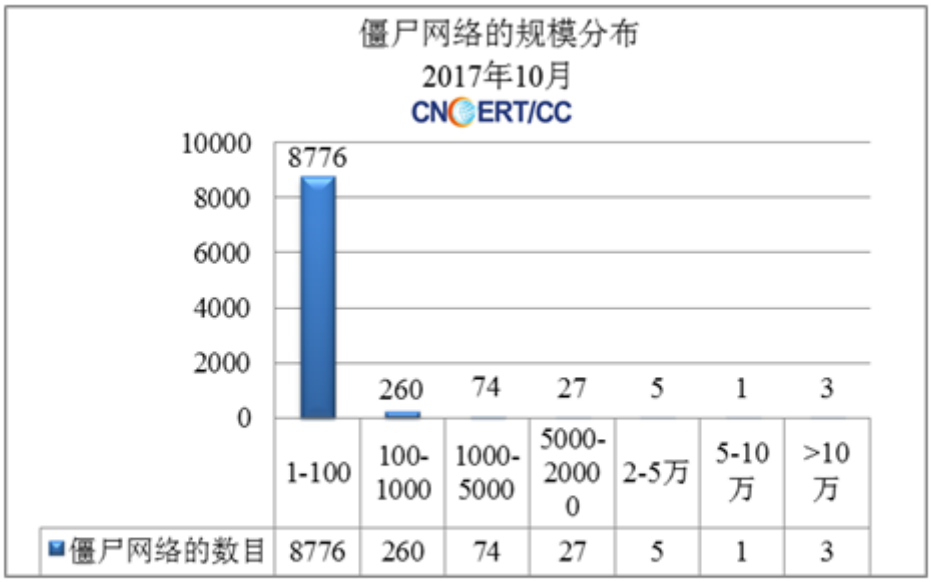

图 4：僵尸网络的规模分布

附 3、境内被植入后门的网站按地区分布

2017 年 10 月，CNCERT 监测发现我国大陆地区 2180 个网站被植入后门程序，比上月的 2825 个减少了 22.83%，其分布情况如图 5 所示。其中，海南省 3 个（占全国 0.14%），排全国第 28 位。

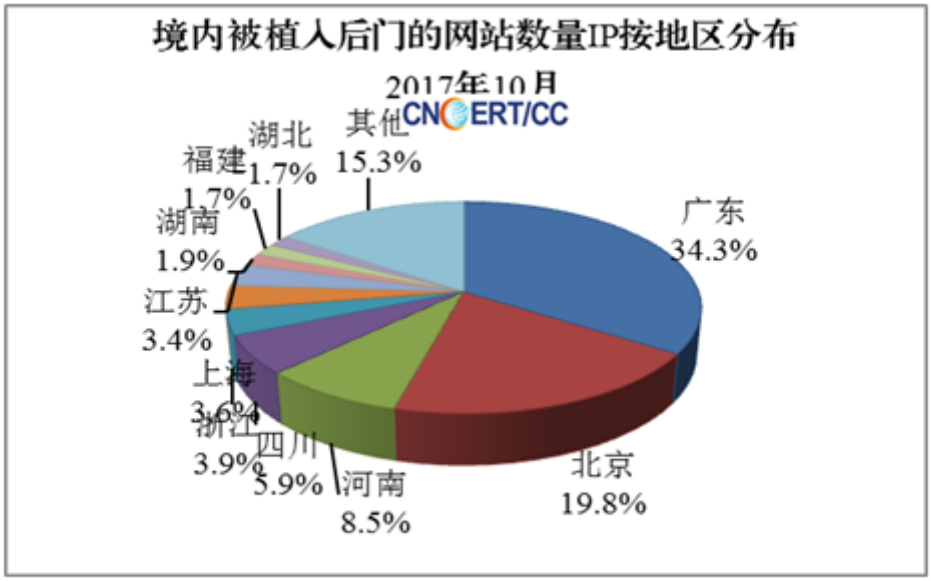

图 5：境内被植入后门的网站按地区分布

附 4、网页篡改监测数据分析

2017 年 10 月，CNCERT 监测发现我国大陆地区被篡改网站 5163 个，与上月的 5494 个相比稍有回落；其中，海南省 7 个（占全国 0.14%），排名第 24 位。具体分布如图 6 所示。

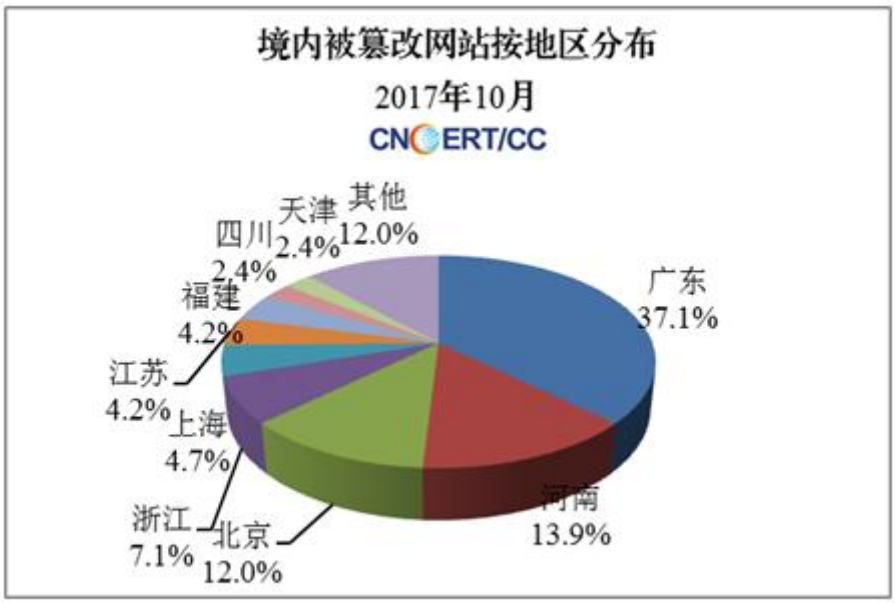

图 6：境内被篡改网站按地区分布

附 5：恶意代码数据分析

2017 年 10 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 10 月 CNCERT 捕获的恶意代码数量

名称	数量
新增恶意代码名称数	3
新增恶意代码家族数	0

2. 2017 年 10 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.gxjsxq.com	117.23.6.67
4	dl.gxjsxq.com	117.23.6.63
5	cl.wokxn.com	117.23.6.68
6	cl.xzqxzs.com	218.203.111.22
7	cl.urndf.com	218.203.111.25
8	cl2.cjsdxz.com	211.138.60.141
9	cl.qpzqxz.com	219.144.69.103
10	down1.7654.com	113.142.84.79

附 6：重要漏洞与重要事件处置公告

2017 年 10 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 WPA2 无线网络密钥重装漏洞的安全公告

近日，国家信息安全漏洞共享平台（CNVD）收录了 WPA2 无线网络组密钥重装漏洞（CNVD-2017-，对应 CVE-2017-13077、CVE-2017-13078、CVE-2017-13079、CVE-2017-13080、CVE-2017-13081、CVE-2017-13082、CVE-2017-13084、CVE-2017-13086、CVE-2017-13087、CVE-2017-13088）。远程攻击者利用该漏洞可实现包括数据包解密和注入、TCP 连接劫持、HTTP 内容注入或单播和组寻址帧的重放攻击。

一、漏洞情况分析

WPA 全名为 Wi-FiProtected Access，中文译名 Wi-Fi 网络安全接入，包括:WPA 和 WPA2 两个标准，是一种保护无线电脑网络(Wi-Fi)安全的系统。WPA2 (WPA 第二版)是基于 WPA 的一种新的加密方式，具备完整的 IEEE 802.11i 标准体系。

WPA2 无线网络加密协议漏洞，入侵方式被称作“密钥重装攻击”。Wi-Fi 保护访问 II(WPA2)的密钥协商握手协议存在设计缺陷，可通过部分报文重放，重置随机数和会话密钥，导致无线接入点(AP)或客户端重新安装密钥。攻击者利用这些漏洞，可在 AP 和客户端的连接范围内，实现包括数据包解密和注入、TCP 连接劫持、HTTP 内容注入或单播和组寻址帧的重放攻击，破坏数据传输的机密性。

CNVD 对该漏洞的综合评级为“中危”。

二、漏洞影响范围

受影响的厂商如下：

ArubaNetworks、Cisco、Espressif Systems、Fortinet, Inc.、FreeBSD Project、Google、HostAP、IntelCorporation、Juniper Networks、MicrochipTechnology、Microsoft Corporation、OpenBSD、Peplink、RedHat, Inc.、Samsung Mobile。

三、处置措施

目前，已修复该漏洞的厂商如下，CNVD 建议用户及时下载补丁进行更新：

Cisco:https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171016-wpa

IntelCorporation:https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00101&languageid=en-fr

Juniper:http://kb.juniper.net/JSA10827

Microsoft:https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-13080

Aruba:http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2017-007.txt

Broadcom: Advisory will be distributeddirectlyto customers

Marvell: Advisory to be distributeddirectly tocustomers

MojoNetworks:http://www.mojonetworks.com/wpa2-vulnerability

Peplink:https://forum.peplink.com/t/security-advisory-wpa2-vulnerability-vu-228519/12715

SierraWireless:https://source.sierrawireless.com/resources/airlink/software_reference_docs/technical-bulletin/sierra-wireless-technical-bulletin—wpa-and-wpa2-vulnerabilities/

WatchGuard:https://www.watchguard.com/wgrd-blog/wpa-and-wpa2-vulnerabilities-update

Wi-FiAlliance:https://www.wi-fi.org/securityupdate2017

附：参考链接：

https://www.kb.cert.org/vuls/id/228519/

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-13080