海南省网络安全通报 2017 年第 11 期

一、 我省本月网络安全总体情况

11 月，海南省发生网页篡改安全事件 2 起；被境外控制的木马僵尸受控主机数量为 8842 个，较上月 9700 个减少 8.85%，列全国第 23 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 800G，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。

11 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

11 月，海南互联网应急中心共向各运营企业下发了 690 条感染僵尸木马的 IP 数据，67 条僵尸木马病毒控制端 IP 数据，375 条感染蠕虫病毒的 IP 数据；网站漏洞数据 24 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

11 月,海南互联网应急中心协调运营企业处置手机病毒 193 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：网页篡改及信息泄露事件 3 起，漏洞事件 24 起，恶意代码事件 63 起。

三、本月安全要闻回顾

1、首届全球网络安全产业创新论坛在沪召开

11 月 7 日下午，在工业和信息化部、上海市政府指导下，由上海市经济和信息化委员会、上海社会科学院联合主办的首届“全球网络安全产业创新论坛”在上海新锦江大酒店召开。中国互联网发展基金会理事长马利、上海社会科学院党委书记于信汇、上海市经济信息化委总工程师张英、中国信息通信研究院副院长王志勤出席会议并致辞。

张英总工程师在致辞中指出，打造面向未来的智慧城市是上海建设卓越的全球城市，改善城市发展环境、促进城市功能提升、提高公共服务水平的重要举措。在智慧城市建设过程中，互联网已经成为驱动产业创新变革的先导力量，随着“互联网行动”的全面推进和两化深度融合，物理世界和网络空间相关交织，给城市运行和安全管理带来新威胁和新挑战。与此同时，金融服务移动普惠、智慧政务云数联动、工业制造智能物联等，为网络安全保障服务高端化和网络安全产业创新提供了难得的发展机遇。

网络安全产业已经成为保障国家网络安全的核心产业，《网络安全法》明确要求省、自治区、直辖市人民政府加大网络安全投入，扶持重点网络安全技术产业和项目。大力推进网络安全产业创新是经济和信息化部门落实网络安全国家战略的重要着力点。上海是我国信息产业的重要地区，在国产操作系统、中间件、数据库等基础产品，行业软件和国产密码应用方面具有比较优势，为大力发展网络安全产业提供了基础产业支撑。

作为 2017 全球城市信息化论坛的分论坛之一，本次论坛汇聚了国内外网络安全领域重量级学者、网络安全产业行业精英、国内外知名智库研究人员以及政府部门负责同志共 300 余人，共商网络安全产业创新发展科学路径，为促进国内外网络安全产业的创新合作和我国网信事业健康发展贡献智慧和力量。

会上，中国工程院院士沈昌祥、中国工程院院士倪光南和德国国家科学工程院院士克里斯托夫•梅内尔分别围绕可信计算的安全、安

全可控的信息技术体系和大数据安全作主旨演讲。卡巴斯基、中国网安集团、微软、阅安信息、观安信息等企业分享了各自在网络安全领域的创新实践。来自上海社会科学院、上海交通大学、上海市经济和信息化委员会以及相关网络安全企业的代表就智能时代的网络安全产业创新机遇与路径展开交流。

此外，由上海经济和信息化委员会指导，上海众人网络安全技术有限公司联合上海信息安全行业协会以及重要研究机构和企业发起成立的“上海赛博网络安全产业创新研究院”正式揭牌。提升政府治理能力大数据应用技术国家工程实验室发布了“大数据应用技术国家工程实验室开放基金”。《2017 全球网络安全企业竞争力》、《2018 全球十大 IT 发展趋势》、《2017 网络安全产业白皮书》等研究报告在会上同期发布。

2、微软警告两个特洛伊木马病毒出现更新，影响银行和企业用户

E 安全 11 月 8 日消息 微软已经确定了两个特洛伊木马，在过去几个月中已经显示出更新的活动。Qakbot 和 Emotet 是两个不同的恶意软件家族，但该公司指出，他们有相同的最终目标，即窃取可用于窃取金钱或进行身份盗窃的银行凭证。

据报道，这两个银行木马原本针对网上银行用户，现在，企业，中小企业和其他组织也被感染。更糟糕的是，一些变种能够在系统和网络上传播，可能会恶化感染率。通常，作为附件提供的特洛伊木马将启动攻击过程。当下载执行并安装时，它会欺骗合法的 Windows 服务以降低怀疑。然后，它将与命令与控制（C&C）通信，该服务器将负

责提供有关如何执行恶意软件说明。

据说 Qakbot 和 Emotet 可以感染网络共享文件夹和驱动器，包括可移动的 U 盘等。它们还可以使用服务器消息块（SMB）在其他机器上复制自己的副本。如果用户系统受到感染，微软建议断开与互联网连接以防止与（C&C）服务器通信。该公司还建议停止恶意软件的自动执行，并监控网络中断后可能的再次感染。

附 1：网络安全信息报送情况

11 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	1327
合计	**1339**

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	375
木马事件	67
僵尸网络事件	690
域名劫持事件	0
网络仿冒事件	0
网页篡改事件	2
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	193
合计	**1327**

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 11 月，CNCERT 监测发现我国大陆地区 637604 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 841752 个相比减少了 24.25%，其分布情况如图 1 所示。其中，海南省 8842 个（占全国 1.05％），全国排名第 23 位。

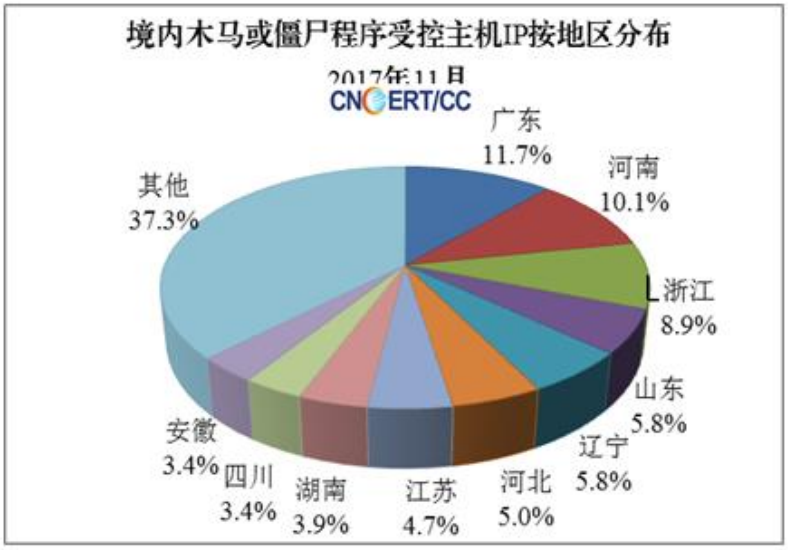

图 1：中国大陆木马或僵尸受控主机 IP 按地区分布

2、木马僵尸控制服务器的数量和分布

2017 年 11 月，CNCERT 监测发现我国大陆地区 2484 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 2680 个相比减少了 7.31%，其分布情况如图 2 所示。其中，海南省 22 个（占全国 0.89％），全国排名第 21 位。

2017 年 11 月，CNCERT 监测发现我国大陆地区 637604 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 841752 个相比减少了 24.25%，其分布情况如图 1 所示。其中，海南

省 8842 个（占全国 1.05%），全国排名第 23 位。

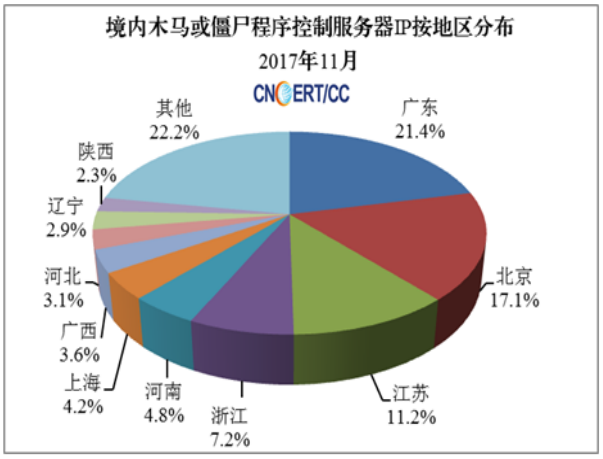

图 2：中国大陆木马或僵尸控制服务器 IP 按地区分布

3、境外木马控制服务器的数量和分布

2017 年 11 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 6911 个，与上月的 6466 个相比增加了 6.88%，主要来自美国、日本等国家，具体分布如图 3 所示。

2017 年 11 月，CNCERT 监测发现我国大陆地区 637604 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 841752 个相比减少了 24.25%，其分布情况如图 1 所示。其中，海南省 8842 个（占全国 1.05%），全国排名第 23 位。

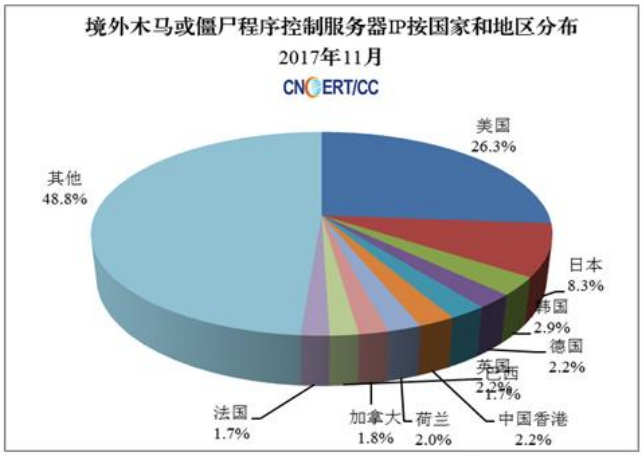

图 3：通过木马或僵尸程序控制中国大陆主机的境外 IP 按国家和地区分布

4、木马僵尸网络规模分布

2017 年 11 月，在 CNCERT 监测发现的僵尸网络中，规模大于 5000 的僵尸网络有 27 个，规模在 100－1000 的有 246 个，规模在 1000－5000 的有 73 个，分布情况如图 4 所示。

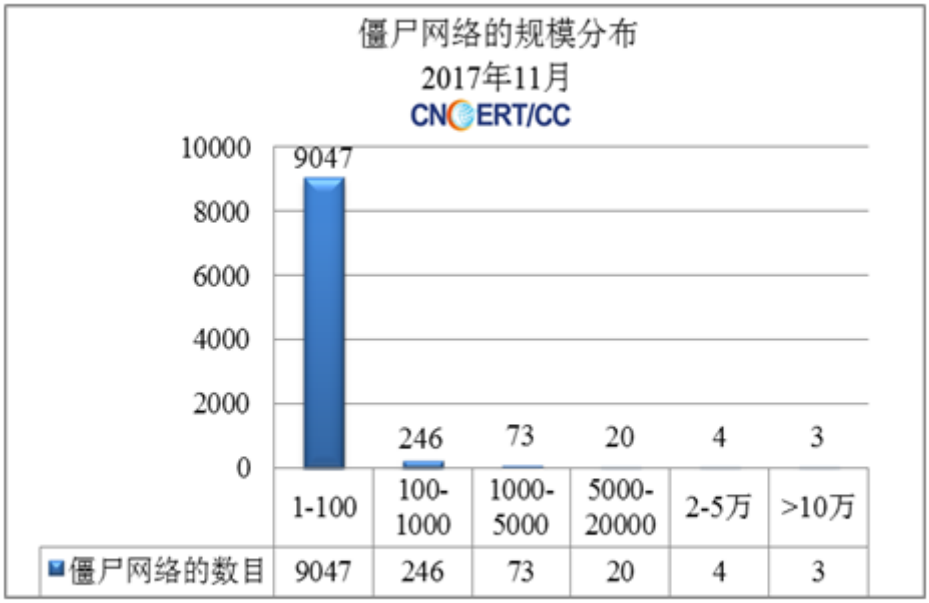

图 4：僵尸网络的规模分布

附 3、境内被植入后门的网站按地区分布

2017 年 11 月，CNCERT 监测发现我国大陆地区 2504 个网站被植入后门程序，比上月的 2180 个增加了 14.86%，其分布情况如图 5 所示。其中，海南省 6 个（占全国 0.24%），排全国第 25 位。

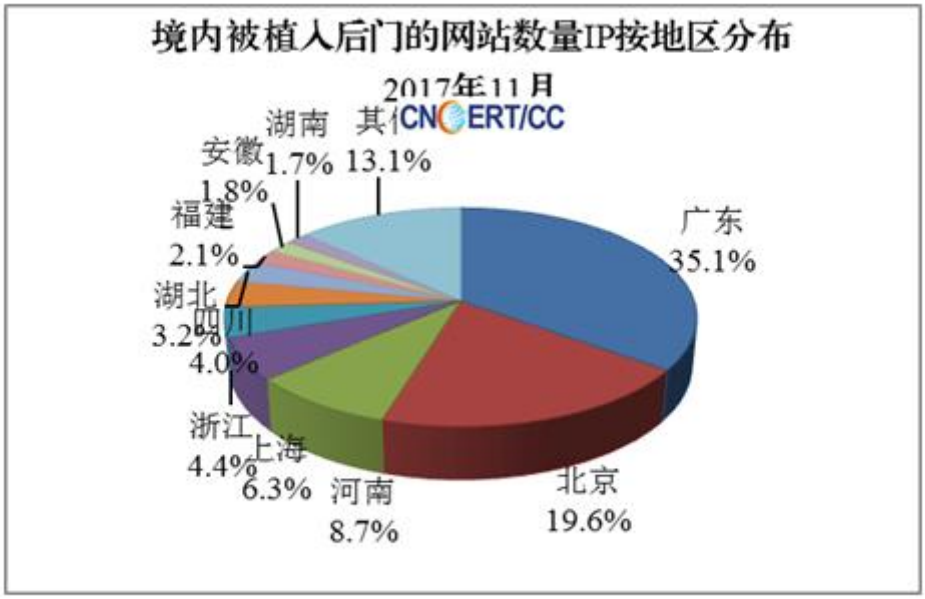

图 5：境内被植入后门的网站按地区分布

附 4、网页篡改监测数据分析

2017 年 11 月，CNCERT 监测发现我国大陆地区被篡改网站 2368 个，与上月的 5163 个相比减少了 54.14%；其中，海南省 2 个（占全国 0.14%），排名第 28 位。具体分布如图 6 所示。

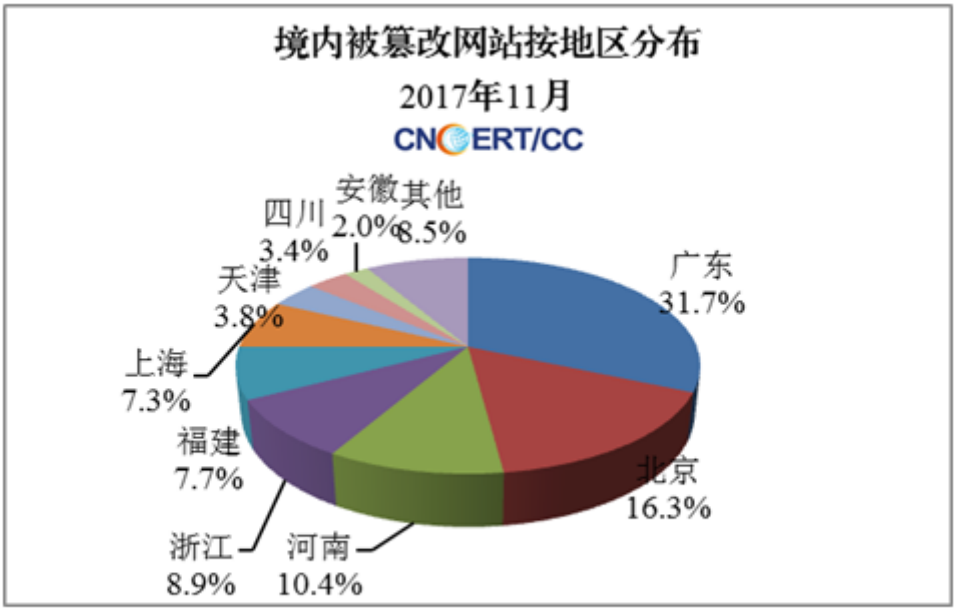

图 6：境内被篡改网站按地区分布

附 5：恶意代码数据分析

2017 年 11 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 11 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 11 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	211.138.60.141
4	dl.gxjsxq.com	117.23.6.63
5	cl.qpzqxz.com	117.23.6.67
6	cl.wokxn.com	117.23.6.68
7	wdx.go890.com	218.95.139.53
8	cl.urndf.com	218.203.111.22
9	dl.apxlx.com	223.111.16.246
10	cl2.cjsdxz.com	218.203.111.25

附 6：重要漏洞与重要事件处置公告

2017 年 11 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Microsoft office组件EQNEDT32.EXE存在内存破坏漏洞的安全公告

近日，国家信息安全漏洞共享平台（CNVD）收录了 Microsoft office 组件 EQNEDT32.EXE 内存破坏漏洞（CNVD-2017-34031，对应 CVE-2017-11882），该漏洞允许未经身份验证的远程攻击者在目标系统上执行恶意代码。微软office在过去17年中，包括office365在内的所有版本均存在该漏洞，漏洞影响范围极为广泛。

一、漏洞情况分析

2017年11月14日，微软发布了安全补丁修复了office组件中的一个内存破坏漏洞，该漏洞位于负责在文档中插入和编辑公式(OLE 对象) 的 MS 办公室组件EQNEDT32.EXE中。由于内存操作不正确， 组件无法正确处理内存中的对象， 从而使攻击者可以在登录用户的上下文中执行恶意代码。2000年，微软厂商在office 2000中引入了EQNEDT32EXE，并保存在 office 2007之后发布的所有版本中，以确保软件与旧版本的文档的兼容性。利用此漏洞需要使用受影响的微软office 或 Microsoft 写字板程序打开恶意文件，使未经身份验证的远程攻击者可以在目标系统上执行恶意代码，远程安装恶意软件，进而可能控制整个操作系统。CNVD 对该漏洞的综合评级为“高危”。

二、漏洞影响范围

Microsoft Office 2007及其以后，包括office365在内的所有Microsoft office版本。

三、防护建议

微软公司已经发布该漏洞的补丁，鉴于该漏洞广泛存在，且易于被用于发起网络攻击，CNVD 强烈建议 office 用户尽快更新 11 月的安全补丁，以防止黑客和网络控制他们的计算机。

临时解决方案：不能及时更新安全补丁的用户，用户可以在命令提示符下运行以下命令，在 Windows 注册表中禁用该组件:

regadd"HKLM\SOFTWARE\Microsoft\Office\Common\COMCompatibility\{0002CE02-0000-0000-C000-000000000046}"/v"CompatibilityFlags" /t REG_DWORD /d 0x400

对于 x64 OS 中的 32 位 Microsoft Office 软件包，运行以下命令:

regadd"HKLM\SOFTWARE\Wow6432Node\Microsoft\Office\Common\COMCompatibility\{0002CE02-0000-0000-C000-000000000046}"/v"CompatibilityFlags" /t REG_DWORD /d 0x400

此外，用户还应启用 MicrosoftOffice 沙箱等以防止活动内容执行(OLE/ActiveX/Macro)。

附：参考链接：

https://thehackernews.com/2017/11/microsoft-office-rce-exploit.html

http://www.cnvd.org.cn/flaw/show/CNVD-2017-34031

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882(微软官方安全建议)