海南省网络安全通报 2018 年第 1 期

一、我省本月网络安全总体情况

1 月，监测发现我省网络安全漏洞 23 起；被境外控制的木马僵尸受控主机数量为 7284 个，较 2017 年 12 月份 11027 个减少了 33.94%，列全国第 24 位；木马僵尸控制服务器数量为 16 个，较 2017 年 12 月份 22 个减少了 27.27%。每日互联网流量最高值为 920G，最低值 95G，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。

1 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

1 月，海南互联网应急中心共向各运营企业下发了 1821 条感染僵尸木马的 IP 数据，16 条僵尸木马病毒控制端 IP 数据，344 条感染蠕虫病毒的 IP 数据；网站漏洞数据 23 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

1 月，海南互联网应急中心协调运营企业处置手机病毒 153 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:网页篡改及域名异常事件 3 起，网站后门事件 6 起，漏洞事件 23 起，恶意代码事件 33 起。

三、本月安全要闻回顾

1、全球网络安全中心正式成立

E 安全 1 月 26 日消息：各国政府及企业每年在网络攻击威胁应对领域的投入已增长至 4450 亿美元（约合人民币 2.85 万亿元），由第 48 届达沃斯世界经济论坛(WEF)牵头的全球网络安全中心于 2018

年 1 月 23 日正式成立。这一全新机构旨在提升网络弹性，同时建立起一套独立的最佳实践库，并将针对不同攻击场景提供指导性意见。

中心运营模式

根据世界经济论坛总裁阿洛伊斯·齐韦吉在新闻发布会上所言，该中心将常设于日内瓦，并计划于 2018 年 3 月正式开始运作。该中心还将帮助“网络发达”区域制定新的战略，用以保护各类关键基础设施。此外，物联网（IoT）与联网设备的兴起亦成为企业特别担心的一类挑战，人们普遍认为其会造成更严重的网络安全问题。

网络安全全球中心将自主管理。世界经济论坛发言人格奥尔·施密特 向公众介绍称，中心的运营将依赖成员资助，论坛本身将领投数百万瑞士法郎。目前，合作伙伴公司必须支付一定的费用才能加入，而政府、学术界和公民社会则可以免费加入。该中心计划 2018 年仅雇用 20-30 名员工。

目前还不知道有多少“政府合作伙伴”加入这个中心，不过在 2017 年 11 月份的筹备会议上，有近 20 个国家的政府代表参加了会议，其中包括几个 G7 和 G20 国家。

2、美众议院通过《网络漏洞公开报告法案》

HackerNews.cc1 月 15 日消息 据外媒报道，本周，美国众议院通过了《网络漏洞公开报告法案（Cyber Vulnerability Disclosure Reporting Act）》。虽然这一法案的适用范围非常有限，但电子前沿基金会（ EFF）对此还是表示支持并希望参议院也能为其亮绿灯。

据悉,H.R.3202 是一个简短且简单的法案,由议员 Jackson Lee 发起，其将要求国土安全局（ DHS ）向国会提交关于政府如何处理公开漏洞的相关报告。具体点来说，报告内容分为两个部分：DHS 为协调网络漏洞公开而制定的政策和程序描述；可能为机密属性的“附件 ”，包括一些特定实例的描述。

或许这一法案最好的地方就在于它能彰显政府确实如其长期以来所说的那样公开了大量漏洞。截止到目前，关于这方面的证据一直不多。所以假设政府有意公开报告和机密附件，那么公众对政府防御能力的信心极有可能会得到增强。

附 1：网络安全信息报送情况

1 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 2357 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（2018 年 1 月）	
事件类型	**数量**
IP 业务	0
基础 IP 网络	15
运营企业自有业务系统	0
域名系统	0
公共互联网环境	2342
合计	**2357**

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	344
木马事件	16
僵尸网络事件	1821
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	6
非授权访问事件	0
垃圾邮件事件	0
其他网络安全事件	153
合计	**2342**

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

2018 年 1 月，CNCERT 监测发现我国大陆地区 516798 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 2017 年 12 月的 436377 个相比增加了 18.43%，其分布情况如图 1 所示。其中，海南省 7284 个（占全国 1.41%），全国排名第 24 位。

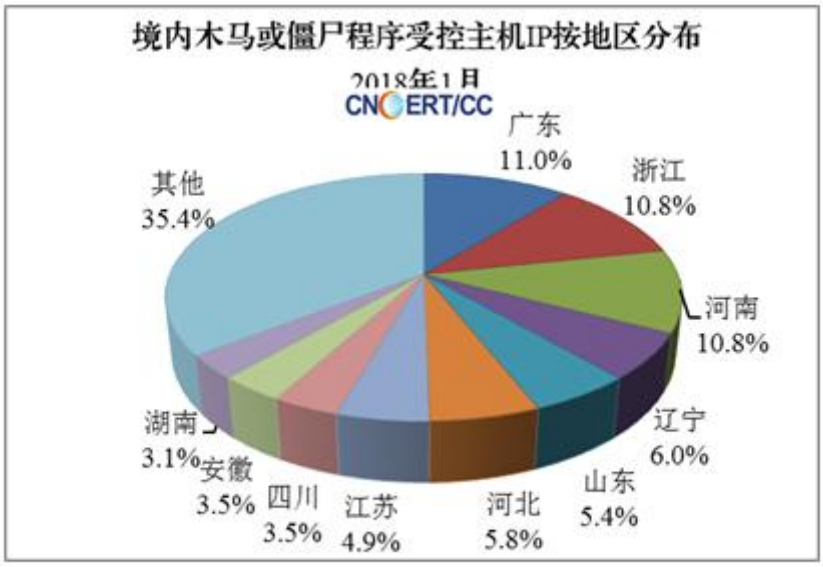

图 1：中国大陆木马或僵尸受控主机 IP 按地区分布

2、木马僵尸控制服务器的数量和分布

2018 年 1 月，CNCERT 监测发现我国大陆地区 2339 个 IP 地址对应的主机被利用作为木马控制服务器，与 2017 年 12 月的 2140 个相比增加了 9.3%，其分布情况如图 2 所示。其中，海南省 16 个（占全国 0.68%），全国排名第 26 位。

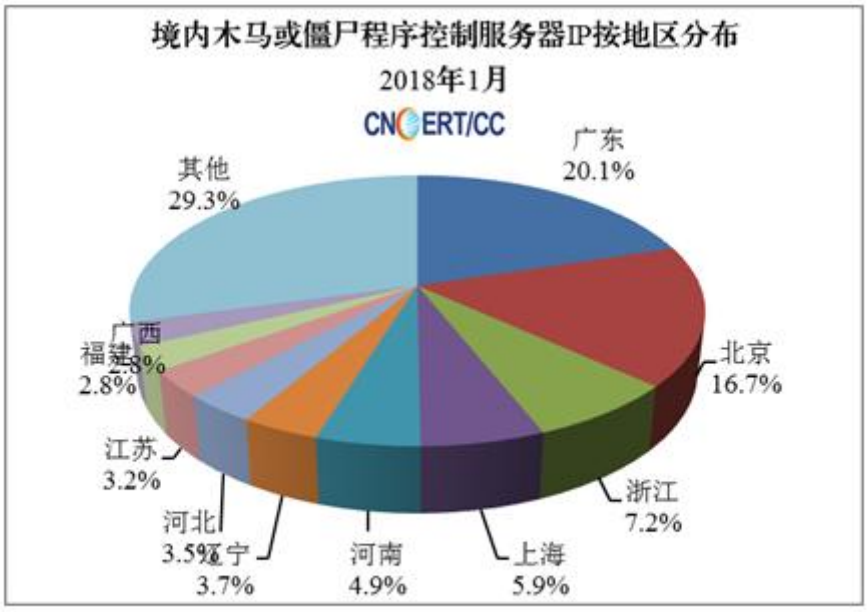

图 2：中国大陆木马或僵尸控制服务器 IP 按地区分布

3、境外木马控制服务器的数量和分布

2018 年 1 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 12606 个，与 2017 年 12 月的 11339 个相比增加了 11.17%，主要来自美国、日本等国家，具体分布如图 3 所示。

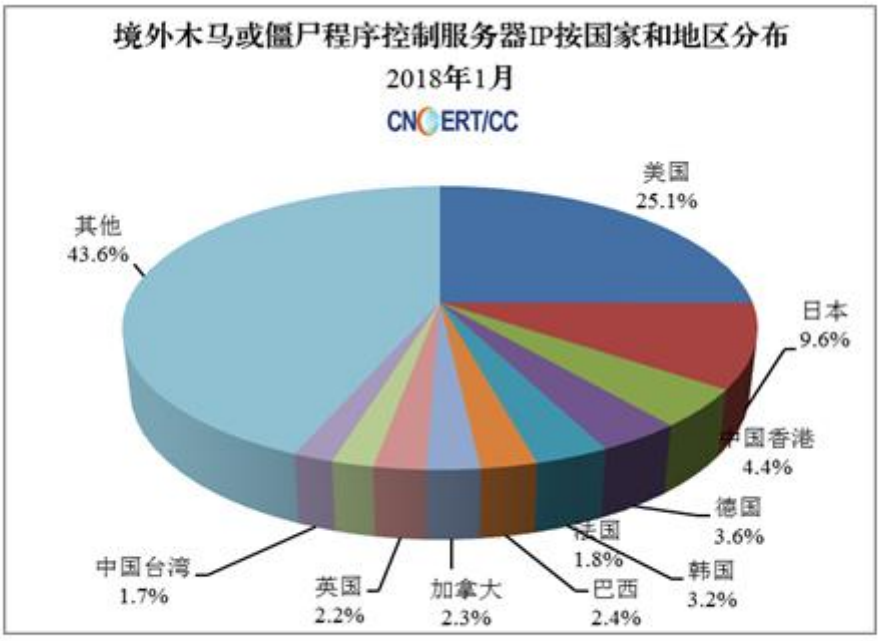

图 3：通过木马或僵尸程序控制中国大陆主机的境外 IP 按国家和地区分布

4、木马僵尸网络规模分布

2018 年 1 月，在 CNCERT 监测发现的僵尸网络中，规模大于 5000 的僵尸网络有 98 个，规模在 100－1000 的有 14592 个，规模在 1000－5000 的有 253 个，分布情况如图 4 所示。

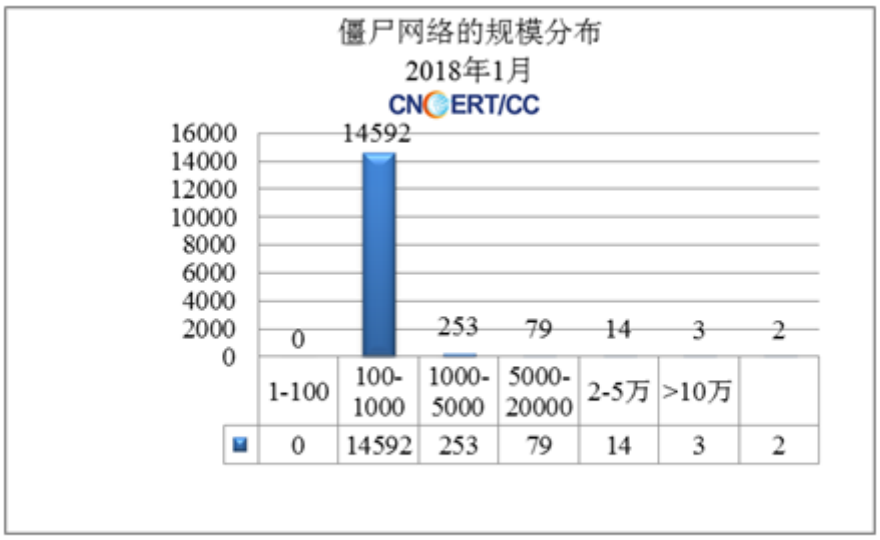

图 4：僵尸网络的规模分布

附 3、境内被植入后门的网站按地区分布

2018 年 1 月，CNCERT 监测发现我国大陆地区 2606 个网站被植入后门程序，比 2017 年 12 月的 3029 个减少了 13.97%，其分布情况如图 5 所示。其中，海南省 5 个（占全国 0.19%），排全国第 27 位。

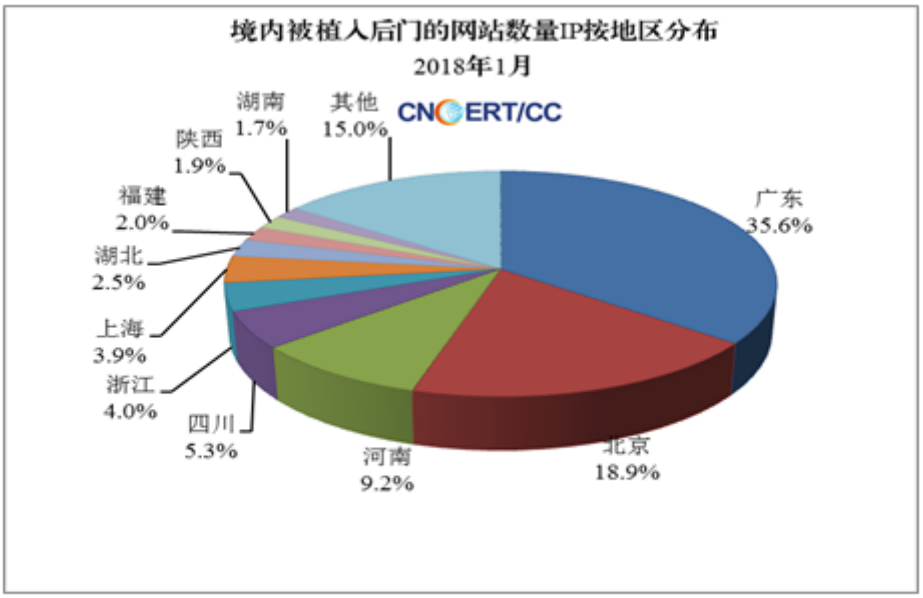

图 5：境内被植入后门的网站按地区分布

附 4、网页篡改监测数据分析

2018 年 1 月，CNCERT 监测发现我国大陆地区被篡改网站 4101 个，与 2017 年 12 月的 4130 个相比减少了 0.7%；其中，海南省 10 个（占全国 0.24%），排名第 19 位。具体分布如图 6 所示。

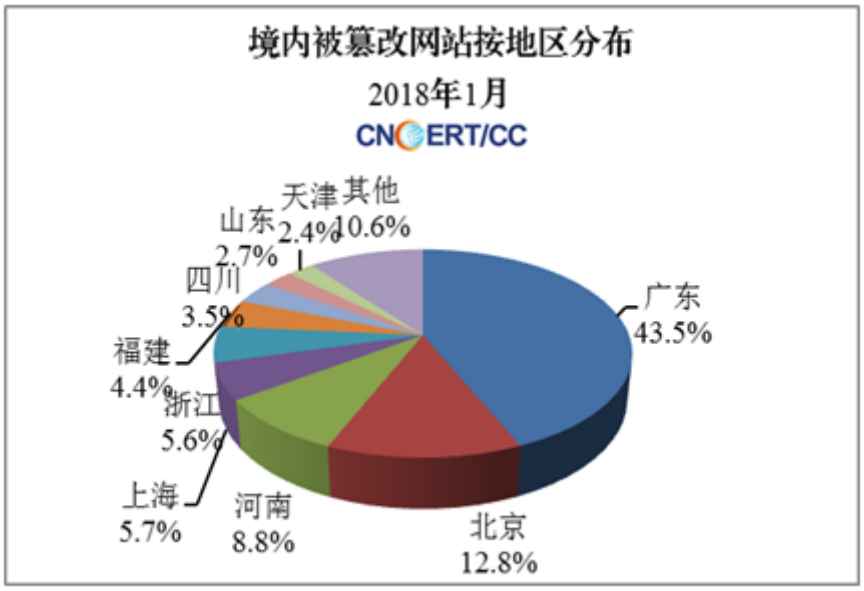

图 6：境内被篡改网站按地区分布

附 5：恶意代码数据分析

2018 年 1 月，恶意代码捕获与分析系统监测得到的放马站点统计。

1. 2018 年 1 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. 2018 年 1 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	120.26.127.170
2	cl.urndf.com	43.242.181.16
3	www.go890.com	125.76.247.169
4	dl.urndf.com	117.23.6.63
5	dxdown.nonglirili.net	121.12.98.72
6	dl.apxlx.com	220.181.105.173
7	cl.qpzqxz.com	218.95.139.53
8	dl.qpzqxz.com	117.23.6.65
9	cl.apxlx.com	117.23.6.64
10	cl.gxjsxq.com	122.72.35.190

附 6：重要漏洞与重要事件处置公告

2018 年 1 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 PHP GD Graphics Library 存在拒绝服务漏洞的安全公告

2018 年 1 月 18 日，国家信息安全漏洞共享平台（CNVD）收录了 PHP GD Graphics Library 存在拒绝服务漏洞（CNVD-2018-02505，对应 CVE-2018-5711）。综合利用上述漏洞，攻击者可以构造恶意 GIF 文件，远程利用 PHP 函数形成无限循环的方式发起拒绝服务攻击。目前，漏洞利用代码已公开，且厂商已发布漏洞修复版本。

一、漏洞情况分析

PHP（超文本预处理器）是一种通用开源脚本语言。GD Graphics Library（又名 libgd 或 libgd2）是一个开源的用于动态创建图像的库，它支持创建图表、图形和缩略图等，广泛应用于 PHP 语言的开发。

该漏洞触发的前提条件为受影响版本的 PHP，并且使用了 libgd 库，漏洞文件存在于 ext/gd/libgd/gd_gif_in.c。在“LWZReadByte_”函数存在一个循环（while-loop），该循环里“GetCode_”函数会调用 GetDataBlock 来读取 GIF 图片中的数据，但由于“GetCode_”函数未能正确处理 int 到 unsigned char 的类型转换，导致 PHP 在解析特定 GIF 文件调用 PHP 函数 imagecreatefromgif 或 imagecreatefromstring 时出现死循环，从而导致服务器计算资源大量消耗，直至崩溃宕机。该漏洞允许远程攻击者利用该漏洞导致拒绝服务攻击。

CNVD 对上述漏洞的综合评级为“高危”。

二、漏洞影响范围

PHP 5 < 5.6.33 版本

PHP 7.0 < 7.0.27 版本

PHP 7.1 < 7.1.13 版本

PHP 7.2 < 7.2.1 版本

三、漏洞修复建议

目前，厂商已发布升级新版本以修复该漏洞，最新版本下载链接 http://php.net/downloads.php。

附：参考链接：

http://php.net/ChangeLog-7.php

https://bugs.php.net/bug.php?id=75571

http://www.cnvd.org.cn/flaw/show/CNVD-2018-02505