海南省网络安全通报 2017 年第 9 期

一、我省本月网络安全总体情况

9 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 10985 个，较上月 16171 个有所减少，列全国第 23 位；木马僵尸控制服务器数量为 15 个，比上月增加 13 个。每日互联网流量最高值为 770G，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。

9 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

9 月，海南互联网应急中心共向各运营企业下发了 767 条感染僵尸木马的 IP 数据，41 条僵尸木马病毒控制端 IP 数据，457 条感染蠕

虫病毒的 IP 数据；网站漏洞数据 8 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

9 月，海南互联网应急中心协调运营企业处置手机病毒 181 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。

三、本月安全要闻回顾

1、工信部发布《公共互联网网络安全威胁监测与处置办法》

中国网 9 月 15 日消息 记者 9 月 14 日从工信部获悉，工信部制定印发《公共互联网网络安全威胁监测与处置办法》，对公共互联网上存在或传播的、可能或已经对公众造成危害的网络资源、恶意程序、安全隐患或安全事件监测处置，并建立网络安全威胁信息共享平台，集成合力维护网络安全。

工信部提出，公共互联网网络安全威胁既包括被用于实施网络攻击的恶意ＩＰ地址、恶意域名、恶意电子信息、恶意程序等，也包括网络服务和产品中存在的安全隐患以及网络安全事件。这些一旦被发现认定，将采取停止服务、屏蔽、清除、通报等措施。

工信部提出建立网络安全威胁信息共享平台，统一汇集、存储、分析、通报、发布网络安全威胁信息，制定相关接口规范，与相关单位网络安全监测平台实现对接。

工信部网络安全管理局局长赵志国表示，工信部将完善危险监测处置、数据保护、新技术、新业务安全评估等政策，最大限度消除安全隐患，制止攻击行为，避免危害发生。《公共互联网网络安全威胁监测与处置办法》自 2018 年 1 月 1 日起实施。

2、土耳其计划出台国家网络安全新战略

新华网 9 月 1 3 日消息 土耳其交通、航运和信息部部长艾哈迈德•阿尔斯兰日前表示，政府正在计划出台新的国家网络安全战略和行动计划。

据当地媒体 1 2 日报道，阿尔斯兰说，此举旨在应对当今来自国内外的网络安全威胁、打击网络犯罪、防范黑客攻击。该计划包括 5 个战略目标、4 1 项行动主题和 1 6 7 个具体步骤。土耳其官方网络安全机构网络安全委员会已召开 4 次会议，为这项战略计划的起草酝酿做准备。

据介绍，土耳其成立了国家计算机紧急情况应对中心，以协调国有和私营企业在打击网络犯罪领域的合作，共同采取行动。未来政府

将公布新的有关法规，强制企业聘请全职的网络安全专家应对可能的网络威胁，未能采取相关网络防范措施的企业可能将面临政府罚款。土耳其还将成立一个封闭的虚拟网络，确保国家机构内部数据信息传输交换的安全。土耳其信息和通信技术委员会将在国家网络安全工作中发挥更加积极有效的作用。政府还将成立一个由 1000 名专业人士组成的专家团队来开展国家网络安全工作。

阿尔斯兰说，交通、航运和信息部计划在今年内举行一次网络安全演练，测试并评估土耳其应对国内网络安全威胁的防范能力，明年将开展针对国际网络威胁的演练和测试。

为提高公众对网络安全的意识，土耳其政府还准备建立一个公众互动平台，提供有关网络安全的在线模拟训练。

附 1：网络安全信息报送情况

9 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 1466 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	1454
合计	**1466**

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	457
木马事件	41
僵尸网络事件	767
域名劫持事件	0
网络仿冒事件	0
网页篡改事件	7
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	1
垃圾邮件事件	0
其他网络安全事件	181
合计	**1454**

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 9 月，监测发现我国大陆地区 1051278 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 1685365 个相比减少了 37.6%，其分布情况如图 1 所示。其中，海南省 10985 个（占全国 1.04%），全国排名第 23 位。

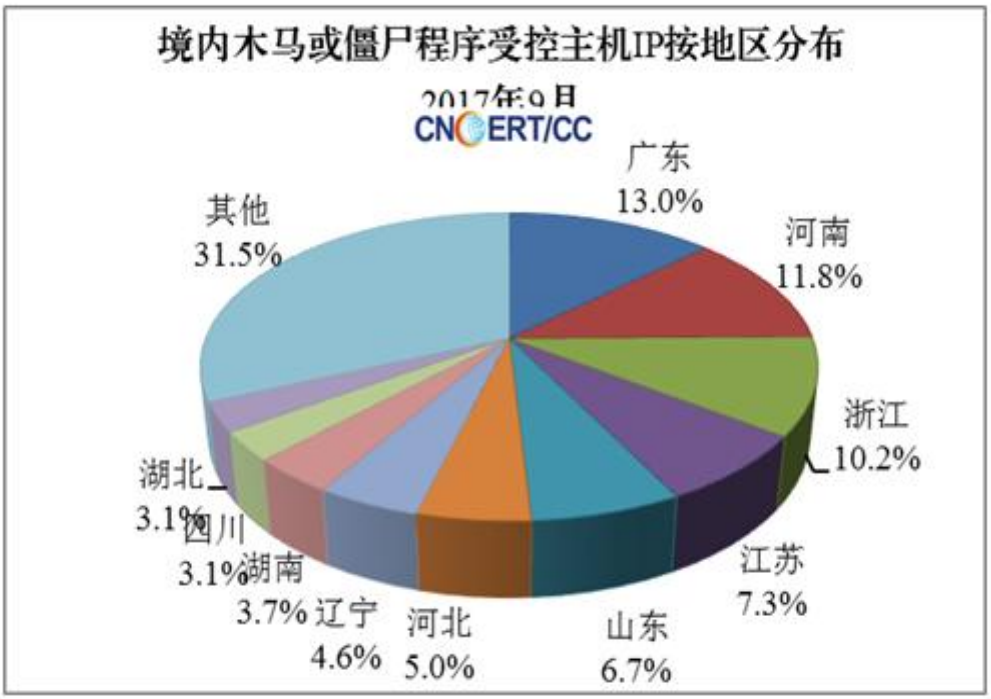

图 1：中国大陆木马或僵尸受控主机 IP 按地区分布

2、木马僵尸控制服务器的数量和分布

2017 年 9 月，监测发现我国大陆地区 2416 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 2901 个相比减少了 16.7%，其分布情况如图 2 所示。其中，海南省 15 个（占全国 0.62%），全国排名第 24 位。

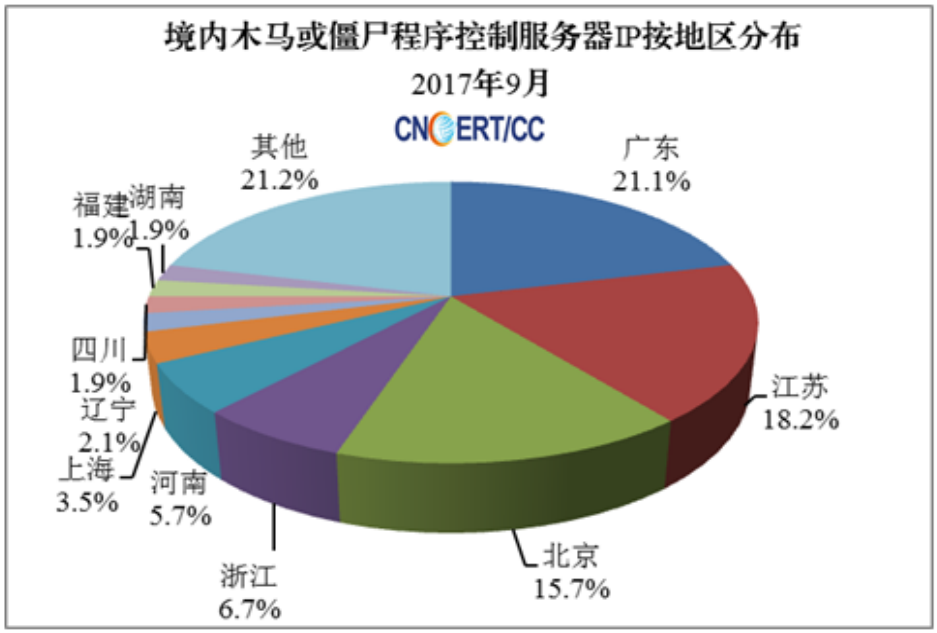

图 2：中国大陆木马或僵尸控制服务器 IP 按地区分布

3、境外木马控制服务器的数量和分布

2017 年 9 月，秘密控制我国大陆计算机的境外木马控制服务器 IP 有 5560 个，与上月的 7042 个相比减少了 21%，主要来自美国、俄罗斯等国家，具体分布如图 3 所示。

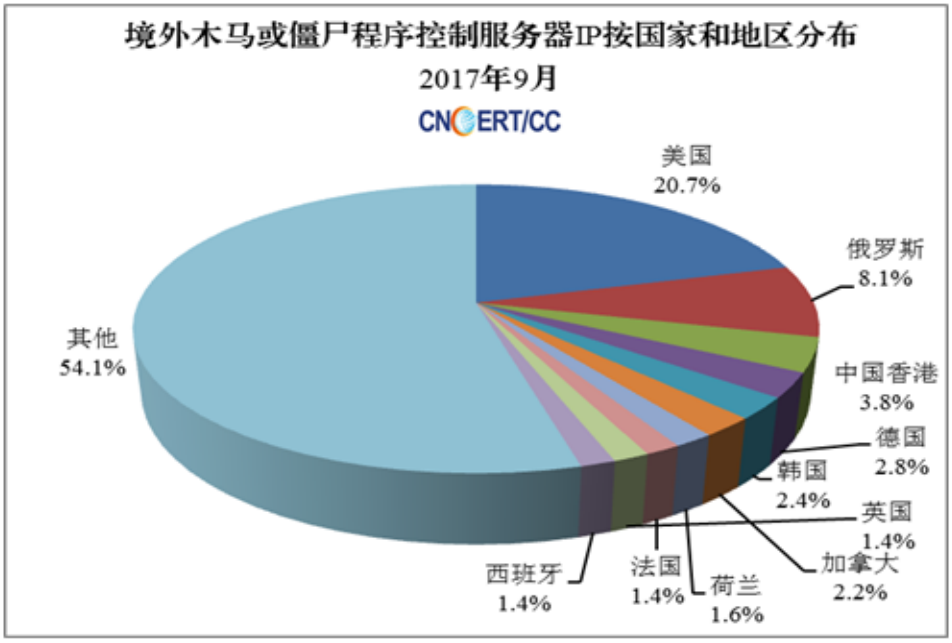

图 3：通过木马或僵尸程序控制中国大陆主机的境外 IP 按国家和地区分布

4、木马僵尸网络规模分布

在发现的僵尸网络中，规模大于 5000 的僵尸网络有 33 个，规模在 100－1000 的有 330 个，规模在 1000－5000 的有 85 个，分布情况如图 4 所示。

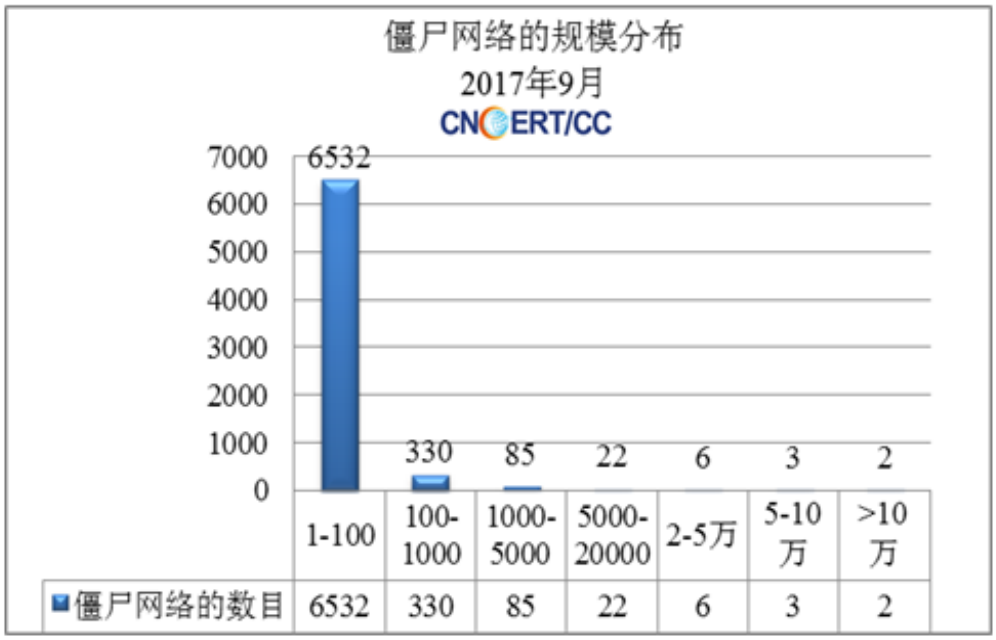

图 4：僵尸网络的规模分布

附 3、境内被植入后门的网站按地区分布

2017 年 9 月，监测发现我国大陆地区 2825 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 8 个（占全国 0.28%），排全国第 27 位。

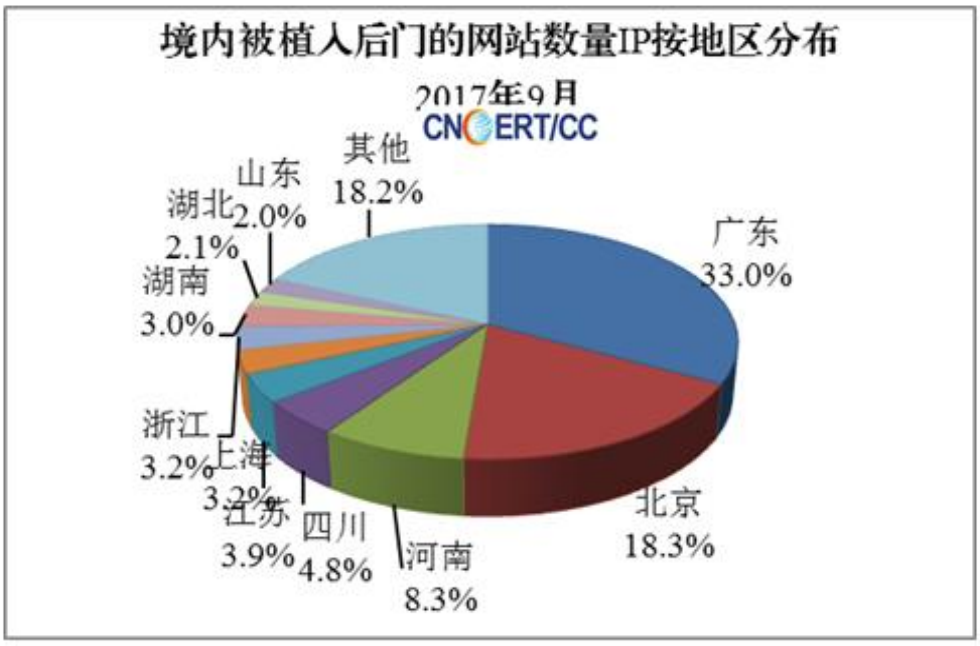

图 5：境内被植入后门的网站按地区分布

附 4、网页篡改监测数据分析

2017 年 9 月，我国大陆地区被篡改网站 5494 个，与上月的 6109 个相比稍有回落；其中，海南省 7 个（占全国 0.13%），排名第 25 位。具体分布如图 6 所示。

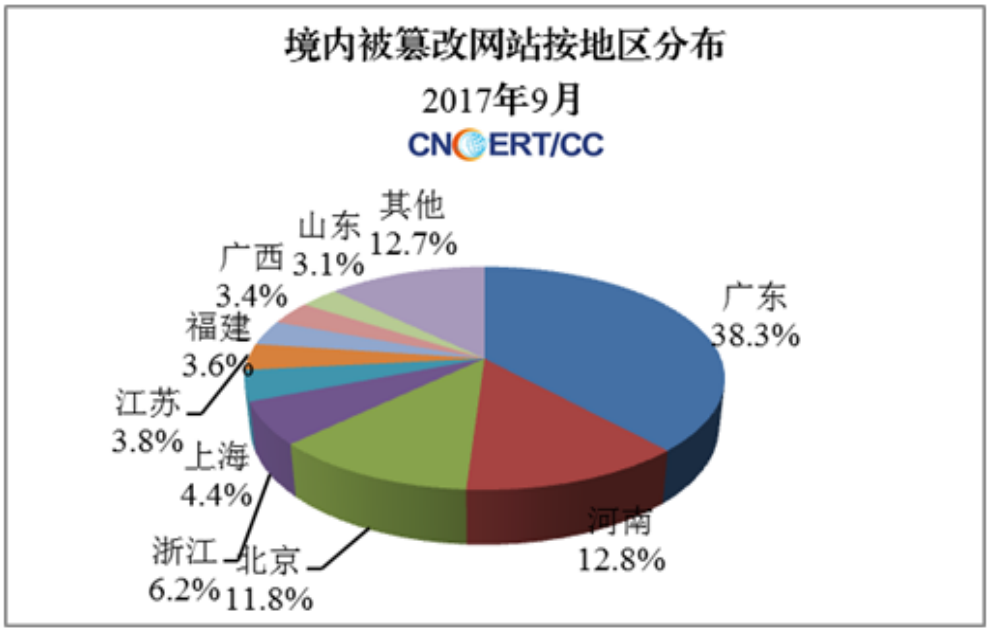

图 6：境内被篡改网站按地区分布

附 5：恶意代码数据分析

2017 年 9 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 9 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	1

2. 2017 年 9 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	123.138.23.10
2	down.downcdn.net	120.26.127.170
3	down.downxiazai.net	61.133.192.170
4	www.go890.com	211.138.60.141
5	cl.gxjsxq.com	117.23.6.67
6	down.nxwb.net	117.23.6.63
7	nc-dl.wdjcdn.com	117.23.6.68
8	dl.gxjsxq.com	106.37.238.1
9	cl.xzqxzs.com	218.203.111.22
10	dl.xzqxzs.com	218.203.111.25

附 6：重要漏洞与重要事件处置公告

2017 年 9 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）

关于蓝牙(Bluetooth)协议存在多个漏洞的安全公告

近日，国家信息安全漏洞共享平台（CNVD）收录了蓝牙(Bluetooth)协议存在的8个安全漏洞。由于漏洞涉及到基础协议，影响到Android、iOS、Windows以及Linux系统设备甚至使用短距离无线通信技术的物联网设备，相关设备范围十分广泛。综合利用上述漏洞，攻击者还可以控制设备，突破访问企业数据和网络，向横向相邻的设备传播恶意软件，极有可能导致大规模蠕虫的跨网攻击。

一、漏洞情况分析

物联网安全研究公司Armis Labs披露了一个新的攻击方法，搭载主流移动、桌面、IoT操作系统包括Android、iOS、Windows、Linux系统的设备均受其影响。攻击者是通过蓝牙(Bluetooth)协议远程不经过任何传统网络介质发起攻击，因此被命名为“BlueBorne”。Armis Labs还披露与BlueBorne相关的8个漏洞，其中的4个高危漏洞详情如下：

漏洞编号	漏洞描述	攻击条件	漏洞评级
信息泄露漏洞 (CVE-2017-0785、CNVD-2017-26761)	Android操作系统中的第一个漏洞揭露了非常有价值的信息，漏洞发生在SDP服务器上，攻击者可通过向SDP服务器发出构造的请求，然后服务器会在返回攻击者的响应中泄露它内存中的信息，可帮助攻击者识别周围的蓝牙服务，以及利用下面提到的远程代码执行漏洞。	需要蓝牙开启，但不需要配对。	高危
远程代码执行漏洞#1 (CVE-2017-0781、CNVD-2017-26762)	该漏洞发生在蓝牙网络封装协议（Bluetooth Network Encapsulation Protocol，BNEP）服务中，该服务用于通过蓝牙连接共享互联网（tethering）。由于BNEP服务中存在缺陷，攻击者可构造非常容易利用的surgical memory corruption，然后攻击者就可完全接管设备然后执行任意代码了。由于缺乏适当的授权认证，触发此漏洞根本不需要任何用户交互，身份验证或者配对，因此目标用户完全无法察觉正在进行的攻击。	需要蓝牙开启，但不需要配对。	高危
远程代码执行漏洞#2 (CVE-2017-0782、CNVD-2017-26763)	这个漏洞跟上一个相似，但是存在于BNEP服务的高层——PAN（Personal Area Networking）profile中，这个文件用于在两个设备之间建立IP网络连接。在这个漏洞的情景下，memory corruption更大，但还是可以被攻击者利用以在获取受影响的设备的完全控制权。跟上一个漏洞类似，这个漏洞无需用户交互，认证或配对即可触发。	需要蓝牙开启，但不需要配对。	高危
The Bluetooth Pineapple –中间人攻击 (CVE-2017-0783、CNVD-2017-26765)	中间人攻击使得攻击者能够拦截并干扰出入目标设备的流量。在WiFi环境下，要发起MITM，攻击者不仅需要特殊的设备，还需要有从目标设备发往它已经建立连接的“开放”WiFi网络（没有加密秘钥的）的连接请求。攻击者必须嗅探到“连接”在“开放”网络上的目标设备发往“开放”网络的802.11的探测请求包，之后再伪装成这个“开放”网络，向目标设备返回探测响应。而在蓝牙(Bluetooth)中，攻击者可以主动地使用支持Bluetooth的设备玩弄目标设备。这个漏洞位于蓝牙协议栈的PAN profile中，可使得攻击者在受害者的设备上创建一个恶意的网络接口，重新配置网络路由，然后使设备上的所有通信流量都走这个恶意网络接口。这种攻击不需要用户交互，认证或者配对，这就使得实际的攻击发生于无形之中。	需要蓝牙开启，但不需要配对。	高危

二、漏洞影响范围

1、Android 设备：

Android 手机，平板终端以及相关可穿戴设备

2、IOS 设备：

iPhone, iPad, iPod 在 iOS 9.3.5 及以下版本，AppleTV 7.2.2 及以下版本均受 RCE(远程代码执行漏洞)影响。iOS 10 未受到漏洞影响。

3、Windows 设备：

Windows Vista 以来的所有 Windows 版本

4、基于 Linux 操作系统的相关设备：

所有运行 BlueZ 的 Linux 设备都受到信息泄漏漏洞的影响（CVE-2017-1000250）。所有内核版本从 3.3-rc1(2011 年 10 月发布)开始的 Linux 系统设备都受到远程代码执行漏洞的影响(CVE-2017-1000251)。

三、防护建议

1、Google 和 Apple 厂商已经修复了相关漏洞：

①升级 iOS 版本至 9.3.5 以上

②升级 Android 版本至 6.0 以上

2、微软已在今年 7 月 11 日发布安全更新，并在 9 月 12 日发布了相应的通知，建议 Windows 用户查看更新信息：

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8628

临时防护建议：

不能及时升级设备的建议暂时关闭蓝牙开关。