NSFOCUS

国内物联网资产的暴露情况分析

绿盟科技创新中心物联网安全实验室
绿盟威胁情报中心(NTI)

2017.3

关于绿盟科技

北京神州绿盟信息安全科技股份有限公司（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 30 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，绿盟科技在网络及终端安全、互联网基础安全、合规及安全管理等领域，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

目录

《国内物联网资产的暴露情况分析》
由如下部门联合撰写

- 绿盟科技创新中心物联网安全实验室
- 绿盟威胁情报中心（NTI）

绿盟科技持续关注物联网安全的相关信息，如需了解更多，请联系：

官方网站

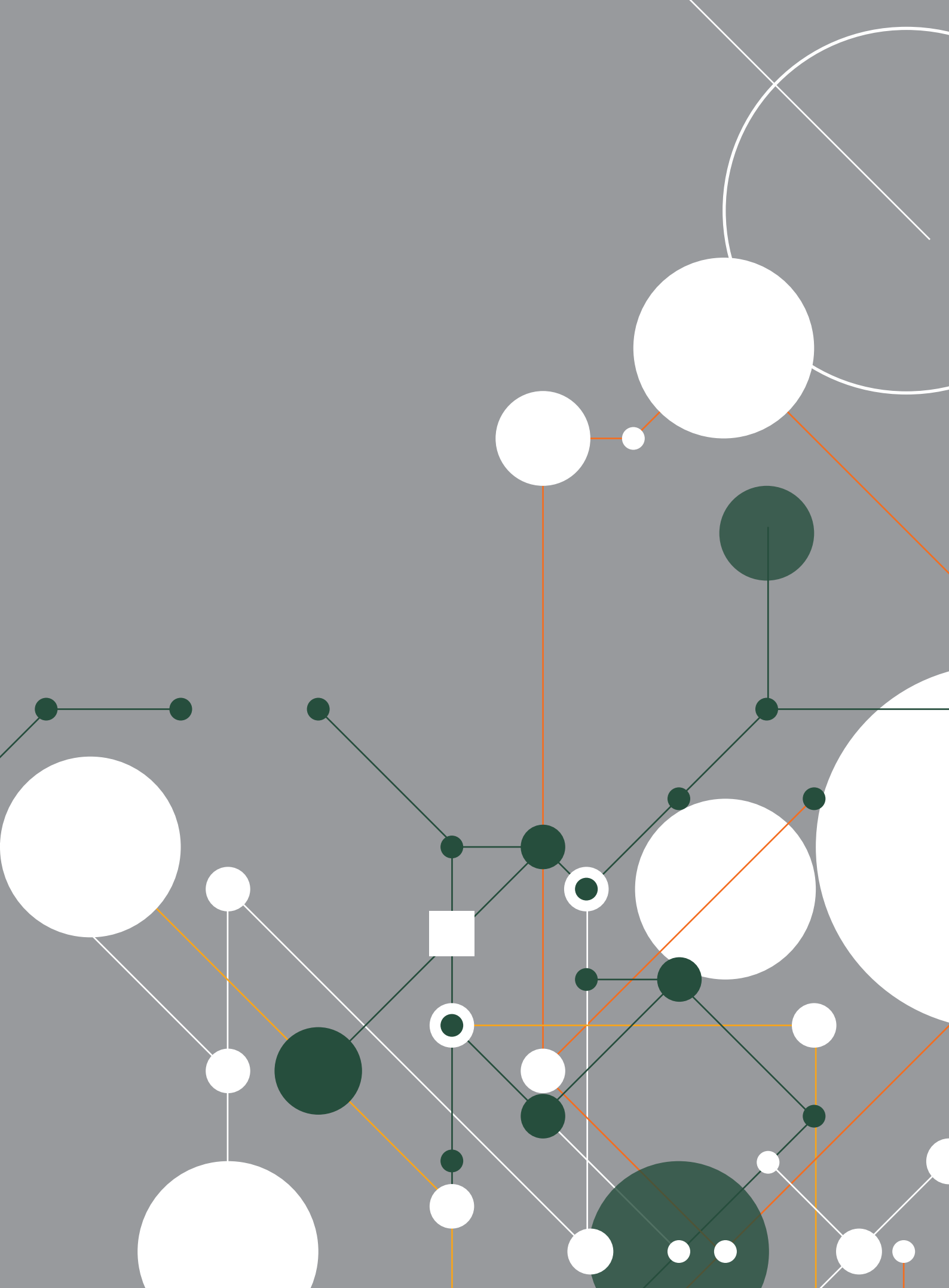
技术博客

微信公众号

特别声明

为避免客户数据泄露，所有数据在进行分析前都已经匿名化处理，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。

版权声明



一．简介

随着传感、计算、通信等技术的成熟，物联网在各行业将会出现越来越多的应用。市场研究机构 Gartner 预测 [12]，自 2015 年至 2020 年，物联网终端年均复合增长率为 33%，装机量高达 204 亿，其中三分之二为消费者应用。在联网的消费者和企业终端的投资的年均复合增长率为 20%，高达 2.9 万亿美元，将取代非联网设备的投资。2016 年，物联网被写进“十三五”规划，《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和应用。

与此同时，众多物联网设备和应用面临严峻的安全挑战。2016 年 9 月 20 日，著名的安全新闻工作者 Brian Krebs 的网站 KrebsOnSecurity.com 受到大规模的 DDoS 攻击，其攻击峰值达到 665Gbps，Brian Krebs 推测此次攻击由 Mirai 僵尸网络发动。2016 年 9 月 20 日，Mirai 僵尸网络针对法国网站主机 OVH 的攻击突破 DDoS 攻击记录，其攻击量达到 1.1Tpbs，最大达到 1.5Tpbs。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，美国东海岸地区遭受大面积网络瘫痪。2016 年 11 月 28 日，德国电信遭遇断网时间，攻击源来自 Mirai 僵尸网络的新变种。而 Mirai 僵尸网络的广泛传播，则是因为暴露在互联网的物联网设备存在安全问题，如弱口令等。

值得注意的是，很大一部分的受 Mirai 恶意代码感染的物联网设备是直接暴露在互联网上。因而，掌握物联网资产在全互联网中的暴露情况是一个非常值得关注的研究点，一种可行的研究方法是通过网络空间搜索引擎发现相关的物联网设备。

不同于互联网搜索引擎 Google、百度，网络空间搜索引擎（如 NTI [1]、Shodan [2]、ZoomEye [3]）关注于 IP 地址以及其所对应的设备、其上运行的服务，其中 NTI 是绿盟科技的威胁情报平台。对于安全研究人员，借助其所探测到的结果，在发现漏洞时，可快速了解其在全球的分布情况。

2016 年，趋势科技发布了一份基于 Shodan 的数据的研究报告 [9]，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）在互联网上的暴露情况。在 RSA2017 上，趋势科技的研究人员对研究报告的内容做了主题演讲 [10]。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、路由器等虽有提及，但并非关注的重点，只是作为某一行业探测到的产品出现。

在物联网相关的安全问题越来越引发人们的关注的背景下，对在互联网上暴露的广义物联网资产进行分析和梳理是有必要的，在获得相关数据后，可对物联网安全态势分析、政策和方案决策，以及技术上做进一步脆弱性和风险评估。

在技术路线方面，考虑到国内外的物联网系统和产品有较大的差异，本文中我们主要对位于中国的物联网资产进行了分析，通过展示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，目的是使公众提高物联网威胁的防范意识。

在第二章和第三章，我们分别从物联网设备维度和物联网操作系统维度进行了分析。第二章展示了都有哪些物联网设备暴露在互联网上以及其有怎样的分布情况。第三章我们对常见的物联网操作系统进行了搜索，以期使读者对暴露在互联网的操作系统的情况有一定的认识。

需要说明的是，一个物联网设备暴露在互联网并不一定意味着这个设备存在问题，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，则该设备便不存在弱口令的风险。但一旦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

心脏出血等）其暴露的相关服务被发现漏洞，就存在被攻破的风险。

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 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，我们对主流家用路由器的绝大多数型号进行了搜索；以海康威视为例，我们发现海康威视的摄像头的某些服务的 BANNER 信息中包含“Server: Hikvision-Webs”字符串，所以可以直接以该字符串请求搜索引擎就能搜索到海康威视的摄像头。

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。

1.2 关键性发现

我们对常见的物联网设备和操作系统进行了分析，关键性发现如下：

1. 海康威视和大华两大厂商的网络监控设备暴露数量最多，东南沿海为国内网络监控设备暴露最严重的区域。
2. 暴露在国内互联网上的路由器以国产品牌为主，暴露出来的端口所对应的协议以 UPnP 和 FTP 协议为主。互联网厂商的路由器销量增长迅猛但暴露较少。
3. 国内有上万台路由器感染恶意软件 Linux.Wifatch，路由器安全现状不容乐观。
4. 港台地区为网络打印机暴露的重灾区，暴露数量达总暴露量的 95% 以上。
5. 大部分搭载操作系统的设备未经更改默认配置就被部署到互联网上，这也是它们被探测到的主要原因。如：运行 DD-WRT 的设备开启的 7924 个 HTTP 服务中，有 22.6% 是由于 title 中具有“DD-WRT (build xxxxx="infopage">”信息而被暴露。98.6% 运行 uClinux 的设备都会带有“Server: uClinux/2.6.28.10 UPnP/1.0 MiniUPnPd/1.3”的 banner 信息。
6. 运行 DD-WRT 和 uClinux 的具有路由器功能的设备，在做了 NAT 的情况下，会使它本身的 IP 具有多个设备的融合属性。

二．常见物联网设备在国内的暴露情况

2.1 引言

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，可是便利之余，物联网设备中暗藏的安全问题也不容小觑。 通过数据收集与分析，了解到国内有十几种物联网设备存在数量较多的暴露情况，根据数量排序依次列出。由图 2.1 可以看出，用于接入互联网的设备暴露情况严重，国内的路由器和调制解码器（Modem）设备暴露数量较多，二者总数量达到 500 万以上。

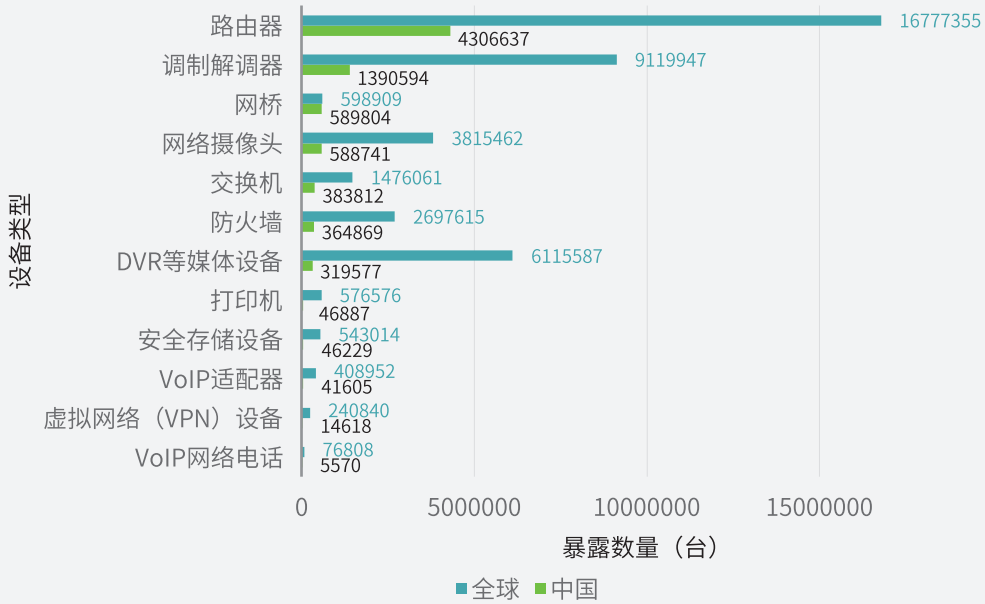


图 2.1 全球和国内物联网相关设备暴露情况

当然物联网设备不仅仅这些，还有一些比较小众（比如：门禁设备、温度监控系统和车辆调度系统等等）或者某些工业领域的设备并未列出，我们可能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 方式与物联网应用通信，隐藏在网关设备后面，这类设备不会暴露在互联网上。

2.2 视频监控设备

视频监控设备是一类非常重要的物联网设备，而且近年一些国际上的物联网安全事件很多与之有关，所以本节主要对国内的视频监控设备暴露情况进行统计及分析。

2.2.1 总体情况

权威研究机构 IHS 发布《2014 全球 CCTV 与视频监控设备市场研究报告》显示，全球视频监控市场份额前 15 位厂家分别为：海康、大华、安讯士、松下、三星泰科、博世安防、派尔高、霍尼韦尔、威智伦、泰科安防、索尼、宇视、Aventura、UTC、英飞拓。海康威视第一、大华股份第二，不过第一和第一之间差距较大[19]。图 2.2 为 HIS2013 年的中国监控设备市场份额的统计。

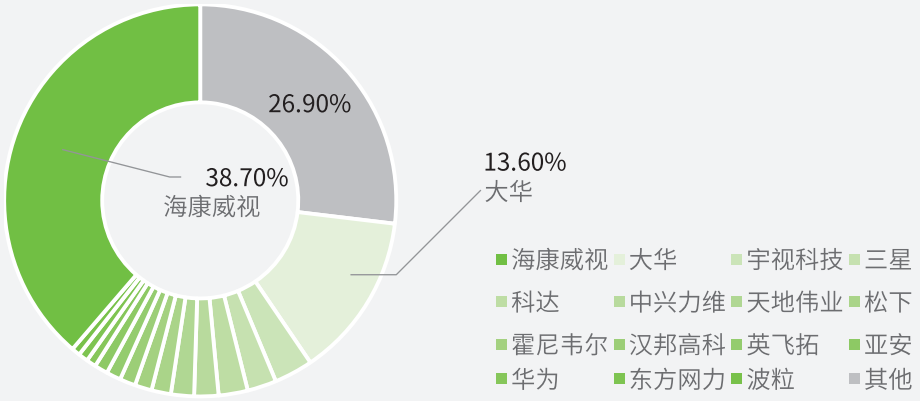


图 2.2 2013 年中国监控设备的市场份额大致情况

我们对以上及其他部分视频监控设备厂商暴露情况进行搜索，得出以下观点：

观点 1： 海康威视和大华两大厂商暴露数量较多

时至今日国内大概有 10 几家网络监控设备（网络硬盘摄像机、网络摄像头和视频服务器等）厂商的产品存在不同程度的暴露情况，其中海康威视和浙江大华两大厂商暴露数量较多。

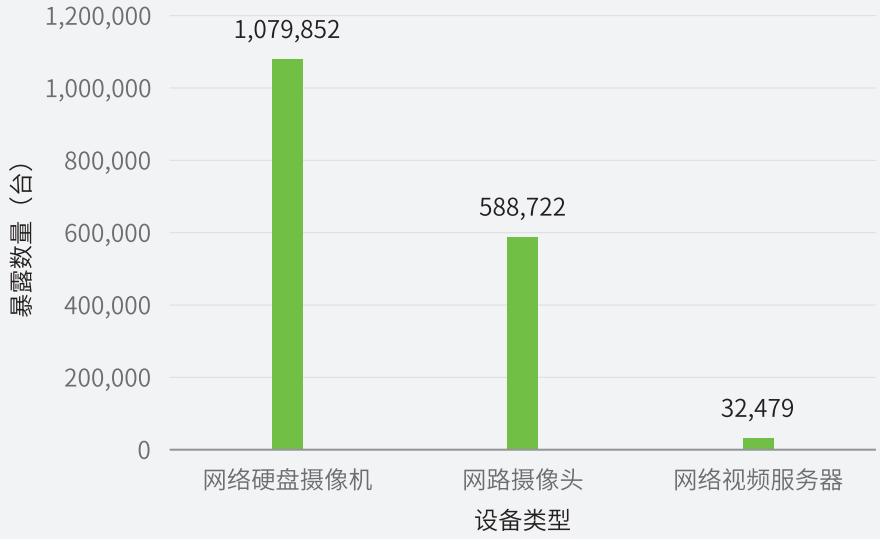


图 2.3 国内网络监控设备暴露概况

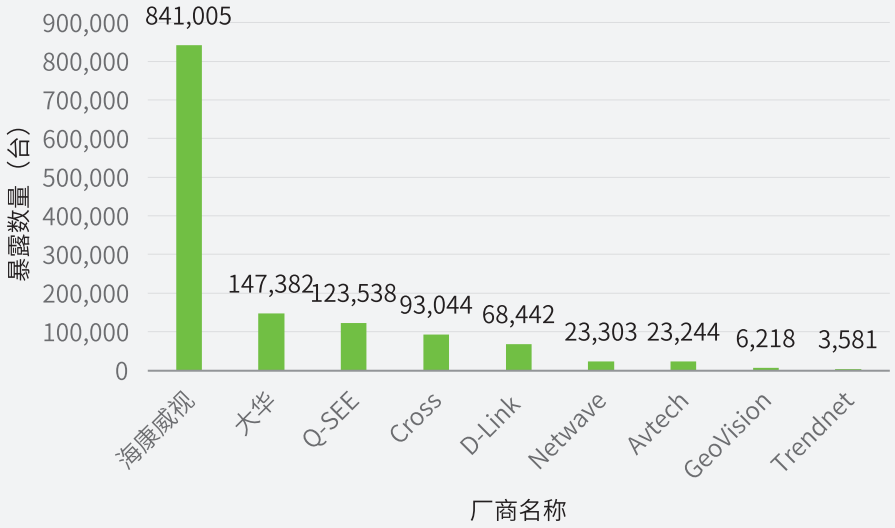


图 2.4 暴露的网络监控设备厂商分布

由以上两张图表可以看出，国内大概有一百多万台以上的监控设备存在暴露情况，其中网络硬盘摄像机设备暴露最为严重，而海康和大华两个厂商的产品占了约一百万台。

2.2.2 特定厂商

据图 2.4 可知，大华和海康两个厂商的网络监控设备暴露最多，所以接下来我们将这二者作为主要的分析对象，主要对其开放端口和地理位置进行了统计和分析。

2.2.2.1 开放端口分析

观点 2： 网络监控设备暴露的端口很多是默认端口

如图 2.5 所示，整理了暴露设备出现次数较多的端口和常用的端口及其对应的协议。根据查阅资料了解到不同的监控设备厂商会开放的默认端口有一定的差异性，比如：大华监控设备视频数据服务的默认端口是 37777，海康威视数据服务的默认端口是 8000。攻击者同样也可以根据上述资料找到相关设备的默认端口，从而通过扫描定位设备，故建议修改设备各项服务的默认端口，降低被攻击者通过广谱扫描而发现的风险。

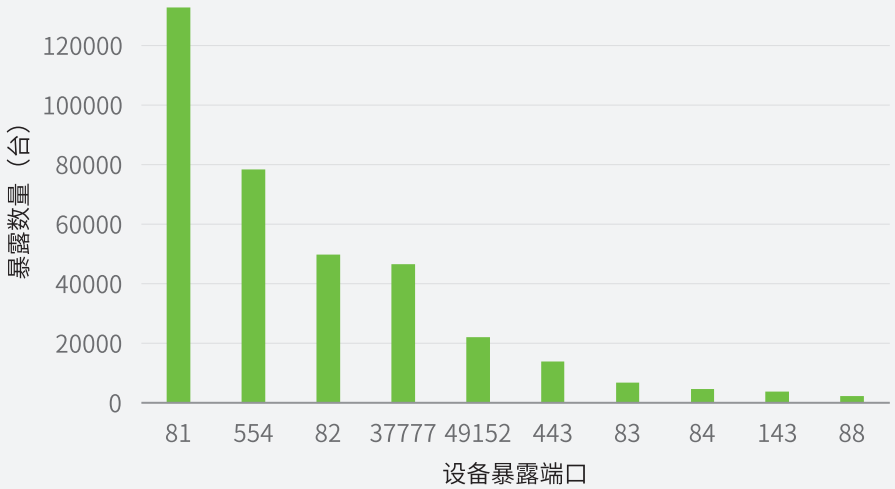


图 2.5 网络视频监控设备端口总暴露情况

表 2.1 视频监控设备端口和协议的对应关系

端口	80	554	443	49152	8080
协议	HTTP	RSTP	HTTPS	UPnP	HTTP

2.2.2.2 城市分布分析

观点 3： 网络监控设备东南沿海地区暴露现象较明显

由图 2.6 可知，网络监控设备主要分布在省会城市，大部分分布在广州、南京和福州东南沿海等商业较发达的地区，这跟网络视频监控设备的市场分布是相匹配的 [15]。但北京上海排名并不靠前，可能是因为东南沿海的制造业相对发达，作业线和仓库等对网络监控设备需求量较多，也有可能这两个城市虽然网络监控设备数量多，但安全意识较好，所以才会出现暴露设备不多的现象。当然这只是我们的根据初步结果所做的分析猜想，具体原因还需进一步的数据支撑和分析得出。

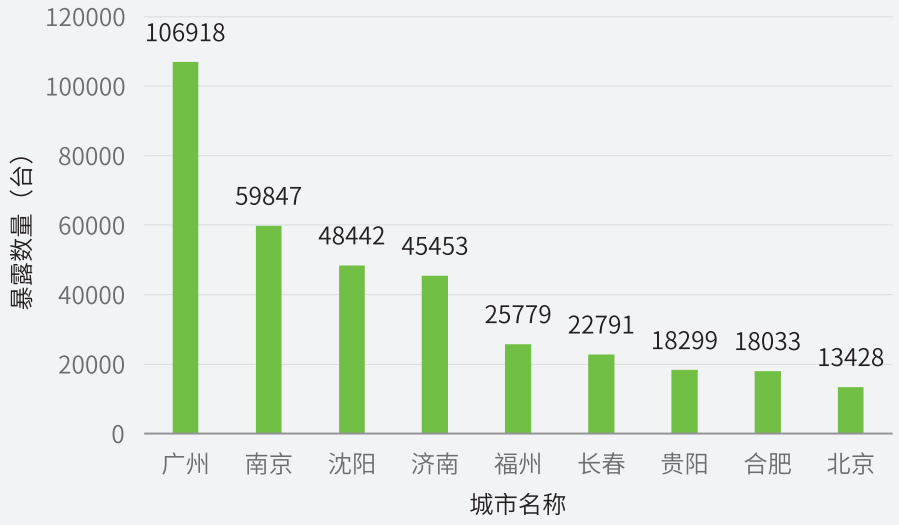


图 2.6 网络视频监控设备暴露城市分布情况

2.3 家用路由器

我们对主流的家用路由器进行了搜索，如迅捷、水星、TP-LINK、小米等。企业级路由器的使用场景、性能要求与家用路由器相差很大，因此我们在这一节主要关注家用路由器 [1]。

2.3.1 总体情况

观点 4： 暴露在国内互联网上的路由器以国产品牌为主

从图 2.7 可以看出，迅捷、水星的路由器基本都位于国内，友讯、腾达的大部分路由器也都位于国内。迅捷、水星、友讯（台湾）、TP-LINK、华硕（台湾）、腾达等均为国内厂商。

1 由于路由器厂商、型号众多，在数据中可能也会包含一些企业级的路由器。

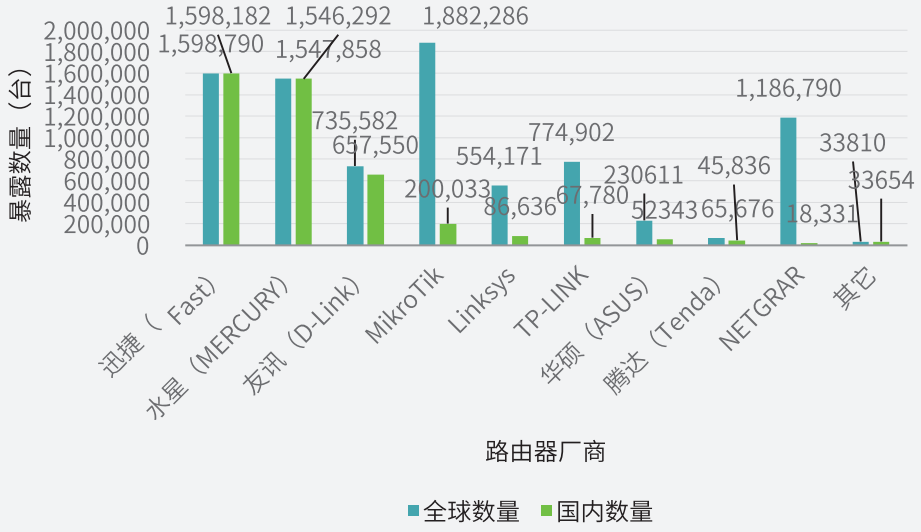


图 2.7 各路由器厂商的暴露情况

观点 5： 互联网厂商的路由器销量增长迅猛但暴露较少

互联网厂商的路由器销量增长迅猛，2017 年 1 月，小米路由器销量突破 1000 万台 [17]。根据艾媒咨询的数据显示 [18]，2016 年上半年，360 安全路由器以 51.5% 的占比位列智能路由器销量排行榜第一。从图 2.7 中我们还可以看出，暴露数量比较多的厂商均为传统路由器厂商，而小米 [2]、360[3]、极路由 [4] 等新兴路由器品牌暴露在互联网的路由器数量较少。

观点 6： 二线城市暴露出来的路由器数量最多

在城市分布上，我们选取了排名前 20 的城市。从图中可以看出，数量最多的几个城市均为二线城市。

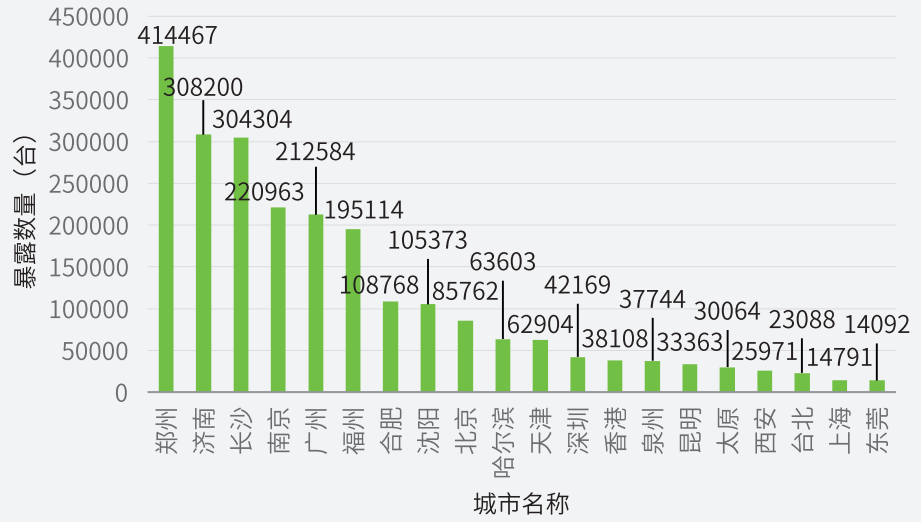


图 2.8 家用路由器按城市的分布情况

2 小米路由器搜索到的数量很少（可在 NTI 中搜索“Xiaomi Mini”、“MiWiFi”），与 360 安全路由器、极路由等均归于其它类别。
3 360 与磊科成立合资公司生产安全路由器，在 NTI 中搜索搜索“netcore”可搜到磊科路由器，从型号信息判断并非合资公司推出的安全路由器。
4 在 NTI 中搜索“hiwifi”可搜到极路由。

观点 7： 家用路由器端口分布广泛，但大多位于 1900、21、80、8080 端口

在端口分布上，我们发现一共有 39 个不同的端口出现，图 2.9 中选取了排名前 20 的端口，排名 20 之后的端口出现总数为 364 个。从图中可以看出，虽然端口号有很多，但其分布很集中。

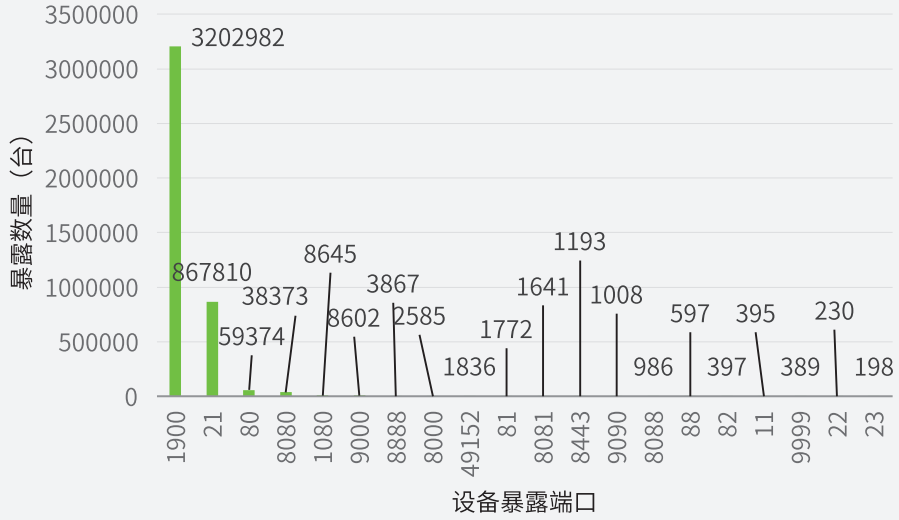


图 2.9 家用路由器按端口的分布情况

观点 8： 路由器暴露端口所对应的协议以 UPnP 和 FTP 协议为主

表 2.2 中显示了出现次数较多的端口和常用的端口（如 22、23）及其对应的协议。暴露在互联网中的路由器中使用最多的协议是 UPnP 协议，其次是 FTP 协议。

表 2.2 路由器端口和协议的对应关系

端口	1900	21	80、8080	22	23
协议	UPnP	FTP	HTTP	SSH	Telnet

UPnP（Universal Plug and Play，通用即插即用）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。

由于很多路由器默认开启 UPnP 功能，所以因该功能造成暴露的路由器数量是最多的。

暴露 21 端口的设备有 80 多万台。TP-LINK 的官网 [8] 中提到带 USB 接口的双频无线路由器系列产品接上移动存储设备后，可实现 FTP 服务器功能。用户可通过 FTP 服务向他人分享照片、电影、音乐等。

有些路由器（如水星）也会支持用户通过互联网远程管理路由器，所以，会有一些 HTTP 协议被检测到。不过，一般用户在配置好路由器之后不会轻易改变路由器的配置信息，而且也很少会有远程管理的需求，建议应关闭远程管理路由器的功能。

最后我们发现，运行在 80、8080 等端口的 HTTP 协议通信数据没有经过加密传输，存在被劫持的风险。

2.3.2 特定厂商

我们在分析的过程中发现有的厂商的设备分布展现出了其独特性，因此，我们选取了迅捷、水星和 TP-LINK

进行分析。

2.3.2.1 迅捷和水星

观点 9： 迅捷和水星两个厂商的路由器的端口分布和 banner 信息非常相似

在搜索的过程中，我们发现迅捷和水星两个厂商的路由器具有很强的相似性，其相似性主要体现在两个方面，一是端口以 1900 为主，二是 1900 端口对应的内容很相似。

图 2.10 和图 2.11 分别展示了迅捷路由器和水星路由器的端口分布，从中可以看出，暴露在互联网的端口均以 1900 为主。

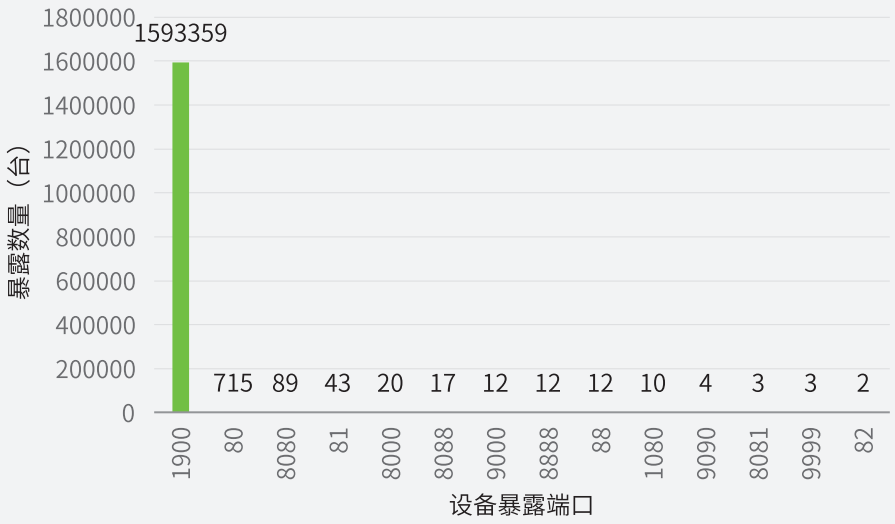


图 2.10 迅捷路由器的端口分布

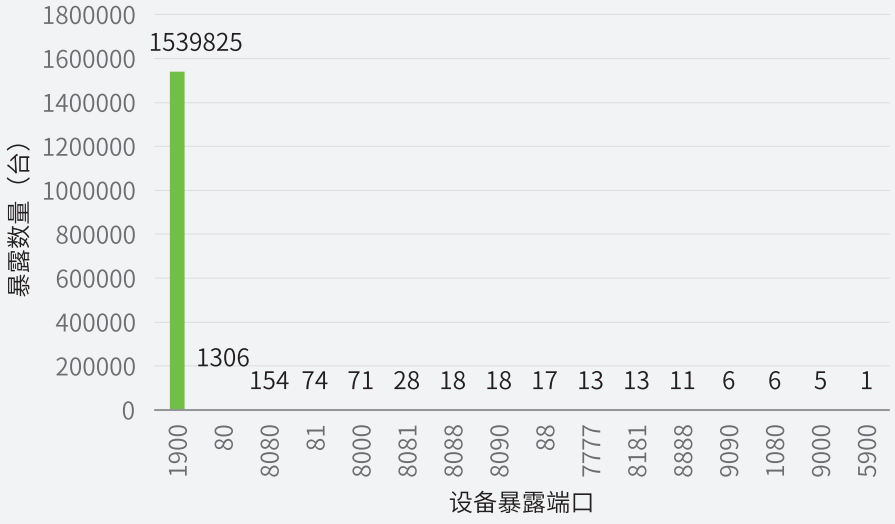


图 2.11 水星路由器的端口分布

图 2.12 和图 2.13 分别是迅捷路由器（FW313R）和水星路由器（MW313R）在 1900 端口的 banner 信息。可以看到两者除了型号不同外，其余均相同。

需要说明的是，banner 信息中虽然有型号，但是并没有厂商信息，我们在搜索引擎中对这两个型号进行搜索，

找到了其对应的厂商，从而建立了型号与厂商的关联。

端口	服务	Banner 信息
1900	SSDP UDP	HTTP/1.1 200 OK CACHE-CONTROL: max-age=600 DATE: Mon, 11 Jan 2016 23:21:11 G MT EXT: LOCATION: http://192.168.1.1:1900/igd.xml SERVER: 300M Wireless N Router F W313R, UPnP/1.0 ST: upnp:rootdevice

图 2.12 迅捷路由器（FW313R）的 banner

端口	服务	Banner 信息
9010	TCP	No Data
1900	SSDP UDP	HTTP/1.1 200 OK CACHE-CONTROL: max-age=600 DATE: Tue, 12 Jan 2016 00:43:11 G MT EXT: LOCATION: http://192.168.1.1:1900/igd.xml SERVER: 300M Wireless N Router MW313R, UPnP/1.0 ST: upnp:rootdevice

图 2.13 水星路由器（MW313R）的 banner

观点 10： 三款迅捷路由器和四款水星路由器占暴露在互联网上的各自厂商的路由器总数的 99% 以上

虽然迅捷和水星路由器的型号众多，但是暴露在互联网的设备中大部分数量集中在很少的型号上。迅捷路由器中的 FWR310、FW300R 和 FW313R 占据了所有被发现的迅捷路由器 [5] 的 99.76%，水星路由器中的 MW310R、MW300R、MW305R 和 MW313R 占据了所有被发现的水星路由器的 99.69%。

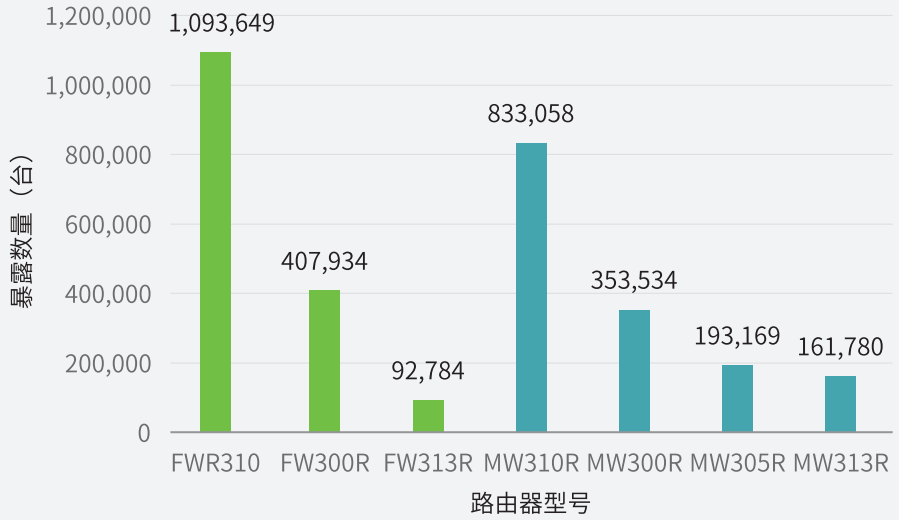


图 2.14 迅捷和水星路由器主要型号的数量

2.3.2.2 TP-LINK

观点 11： 8.7% 的 TP-LINK 路由器位于国内，八个型号的路由器占了国内 TP-LINK 路由器总数的 82%

TP-LINK 路由器同样也是型号众多，但是暴露在互联网的设备中大部分数量集中在很少的型号上。与迅捷和水星路由器主要位于国内的现象不同，只有 8.7% 的 TP-LINK 路由器位于国内。

5 我们对迅捷和水星官网的所有在售路由器的型号进行了搜索。

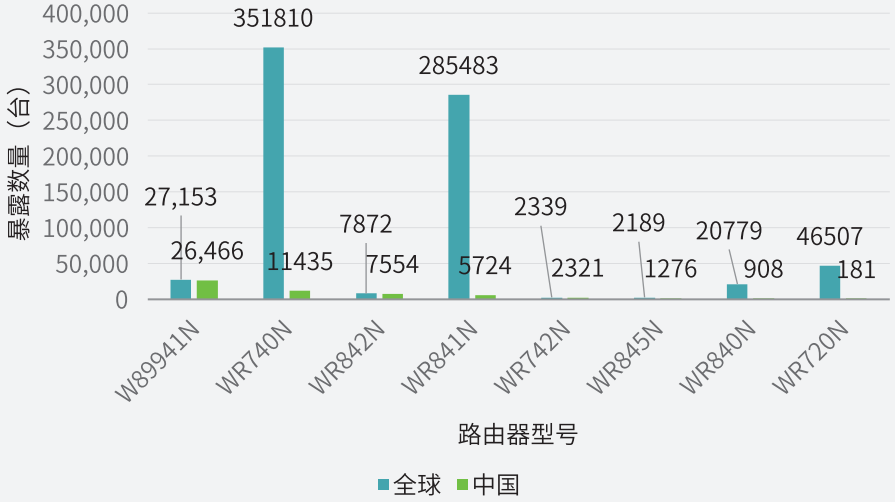


图 2.15 TP-LINK 路由器主要型号的数量

观点 12： 暴露出来的 TP-LINK 路由器有 26% 位于一线城市，18% 位于香港和台湾

TP-LINK 路由器的城市分布如下图所示，可以看出，除香港外，排名前几的城市均为一线城市。不过在上海我们只找到了 45 台设备。台湾的多个城市（台北、台中、桃园、台南、高松）均有一定数量的 TP-LINK 路由器暴露出来。

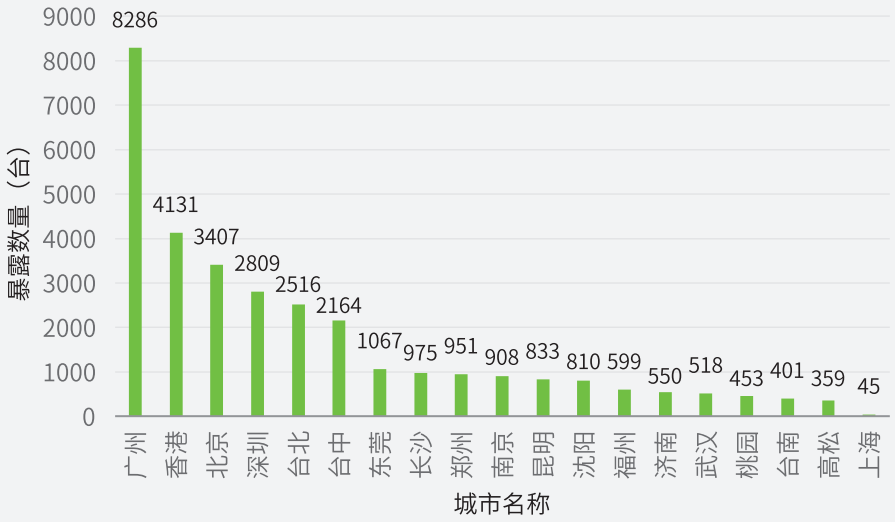


图 2.16 TP-LINK 路由器的城市分布

观点 13： TP-LINK 路由器暴露出来的端口所对应的协议以 UPnP 和 HTTP 为主

TP-LINK 路由器所使用的端口主要有 1900、80、1080、8080、8888 等端口，在这 5 个端口中，除 1900 端口对应 UPnP 协议外，其余端口均对应 HTTP 协议。

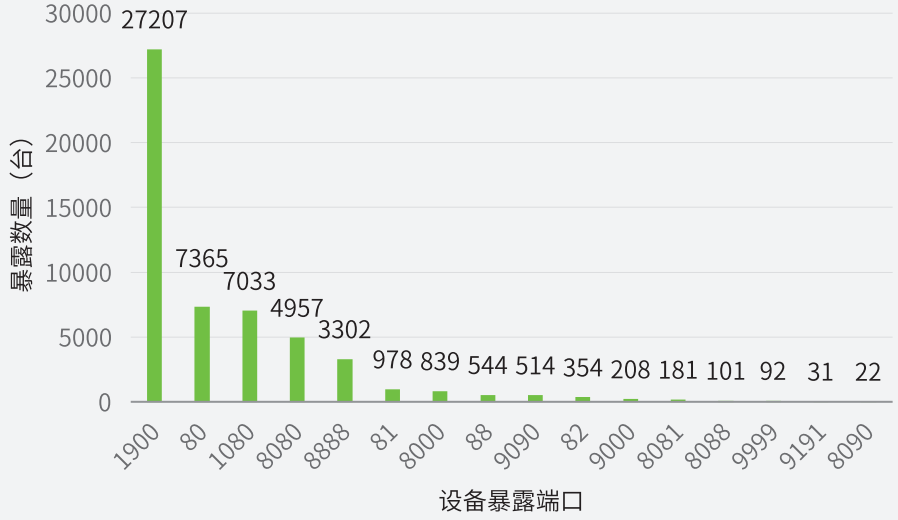


图 2.17 TP-LINK 路由器的端口分布

观点 14： TP-LINK 路由器不同型号暴露出来的协议分布有所不同

表 2.3 TP-LINK 路由器型号和主要协议的对应关系

型号	W89941N	WR740N	WR842N	WR841N	WR742N
协议	均为 UPnP 协议	主要为 HTTP 协议	主要为 HTTP 协议	主要为 HTTP 协议	以 HTTP 协议为主，但是也有 UPnP 协议出现

不同型号的端口暴露情况也有明显的差异，我们对分布数量在前 5 的 TP-LINK 路由器进行分析，为了更容易体现差异性，这里用协议取代端口号来进行分析。

2.3.3 其它发现

观点 15： 国内有上万台设备感染 Linux.Wifatch

在对路由器的信息进行分析的过程中，我们无意中发现有些路由器的 23 端口返回以下信息：

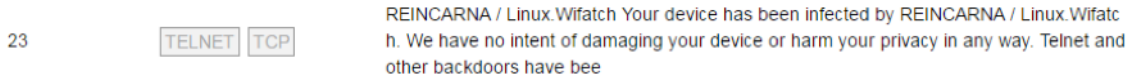


图 2.18 Linux.Wifatch 的 banner

Linux.Wifatch 是一款恶意软件，出现于 2014 年 11 月，它利用远程登录（Telnet）和其他协议感染使用弱密码或默认密码的设备。一旦得手，Wifatch 就禁用 Telnet，并给出图 2.18 所示的 banner 信息。

2015 年 10 月，赛门铁克研究员马里奥 • 巴拉诺 [13] 详细说明了这款恶意软件，该恶意软件感染了成千上万台路由器、网络监控摄像头和其他设备。国内的安全媒体如 FreeBuf [4]、安全牛 [5] 在当时也都有相关的文章对其进行介绍。

有意思的是，Wifatch 虽然感染了物联网设备，但并不执行恶意行为，相反会扫描其他已知恶意软件并将其他恶意软件隔绝在外，似乎在“保护”该设备。Linux.Wifatch 代码开源，可参见（https://gitlab.com/rav7teif/linux.wifatch）。

NTI 的数据显示，目前全国有 14347 台设备被该恶意软件所感染，全球有 93480 台设备被感染。

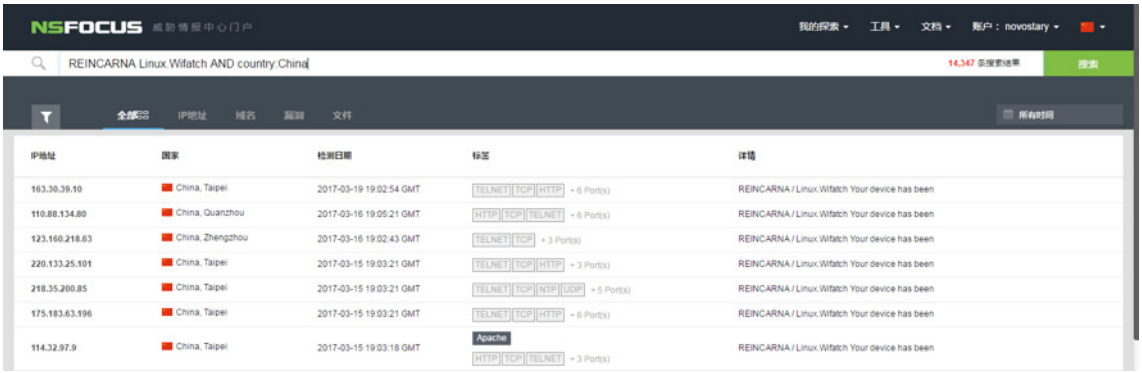


图 2.19 Linux.Wifatch 在 NTI 中的搜索结果

我们对相关 IP 所暴露出的端口进行了分析，如图 2.20 所示。很多设备在感染 Linux.Wifatch 后仅暴露 23 端口，或只暴露除 23 端口外的少数其他端口。因此很难确定出被感染的设备是什么，可能有很大一部分是路由器，此外暴露端口 554 和 37777 一般是视频监控设备。

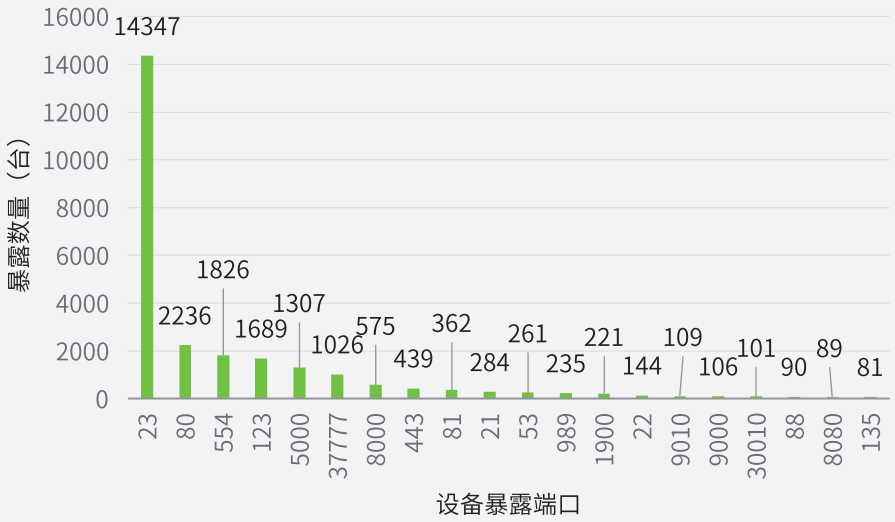


图 2.20 Linux.Wifatch 相关的设备端口暴露情况

对路由器恢复出厂设置及重新启动可以移除该恶意软件，但若不对其固件进行升级或者修改弱口令，设备很可能被重新感染。

2.4 打印机

众所周知，打印机在商务场景中扮演着非常重要的作用，在互联网 + 时代，企业对移动打印的需求越来越大，这也催生了越来越多所谓的“智能”打印机，从功能上看，这些打印机和普通打印机有个显著的区别是大多支持 WiFi 直连、NFC 打印、云打印等移动打印功能 [16]。虽然智能化的打印机能给我们提供一定的便利性，但是否存在安全问题，同样也不容忽视。接下来本节主要对国内的打印机设备的暴露情况进行统计及分析。

2.4.1 总体情况

2017 年 3 月，发生在台湾的安全事件值得一提 [7]，台湾多所学校的打印机被黑客攻击，扬言如果学校不按照

其求付款就发动攻击来瘫痪学校网络。事实上，大部分联机打印机使用外网 IP，其中部分学校打印机和物联网设备使用默认密码，这些设备直接暴露给攻击者，前述的安全事件可能会越来越多。

观点 16： 惠普和爱普生暴露数量较多，占暴露总量的 50% 以上

作为联网终端设备的打印机，其安全问题应该受到用户、厂商的重视。根据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》[14] 可知，2015 年打印机的市场占有率如图 2.21 所示，我们依照占有率的排名对不同品牌的打印机暴露情况进行搜索。如图 2.22 所示，目前有许多品牌打印机存在不同程度的暴露情况，惠普、爱普生和富士施乐暴露数量较多，占暴露总量的 75% 以上。

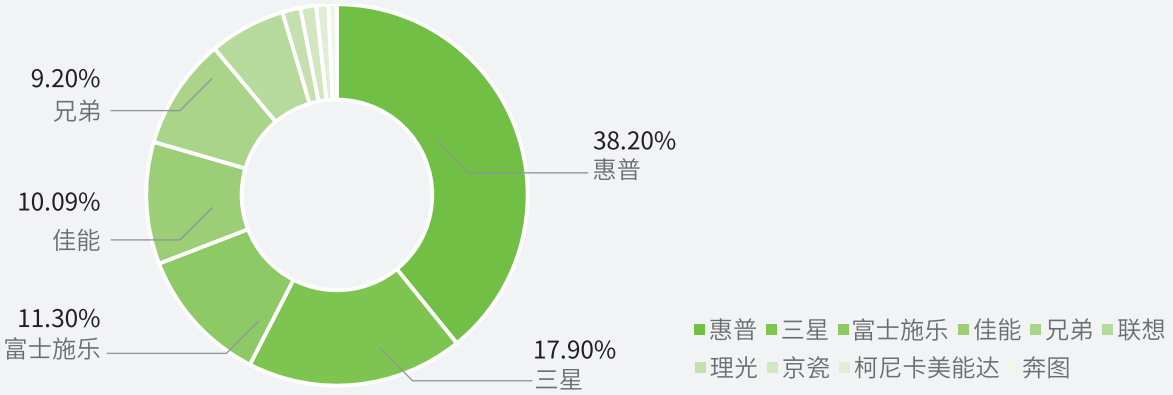


图 2.21 2015 年打印机市场占有率

图 2.22 网络打印机暴露的品牌分布情况

观点 17： 暴露的打印机主要分布在港台地区，占总暴露量的 95% 以上。

由图 2.23 可以看出，网络打印机暴露的城市中，除了北京以外，其他均为台湾和香港地区。由图 2.24 端口的暴露情况可知，港台地区的打印设备半数以上开放了 WEB 服务（80 端口为 WEB 服务的默认端口）。出现这种情况可能会跟港台的打印机的配置习惯有关。当然这只是我们的根据初步结果所做的分析猜想，具体原因还需进一步的数据支撑和分析得出。

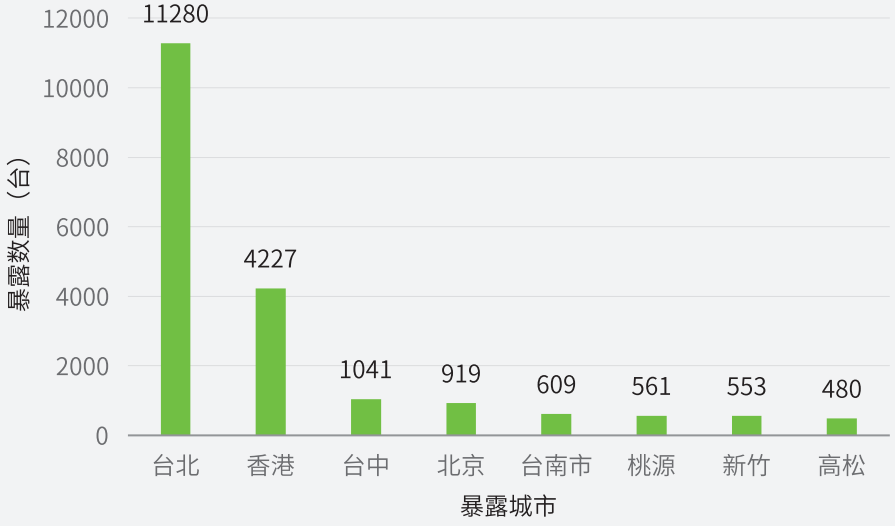


图 2.23 网络打印机暴露的城市分布情况

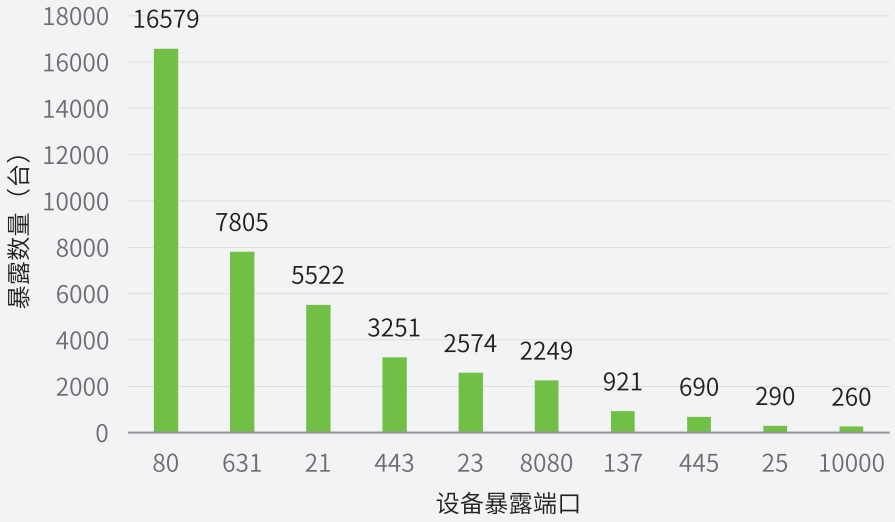


图 2.24 网络打印机暴露的端口数量分布情况

2.4.2 特定厂商

2.4.2.1 开放端口分析

下面主要对 HP 打印机进行研究分析，得到以下数据结果：

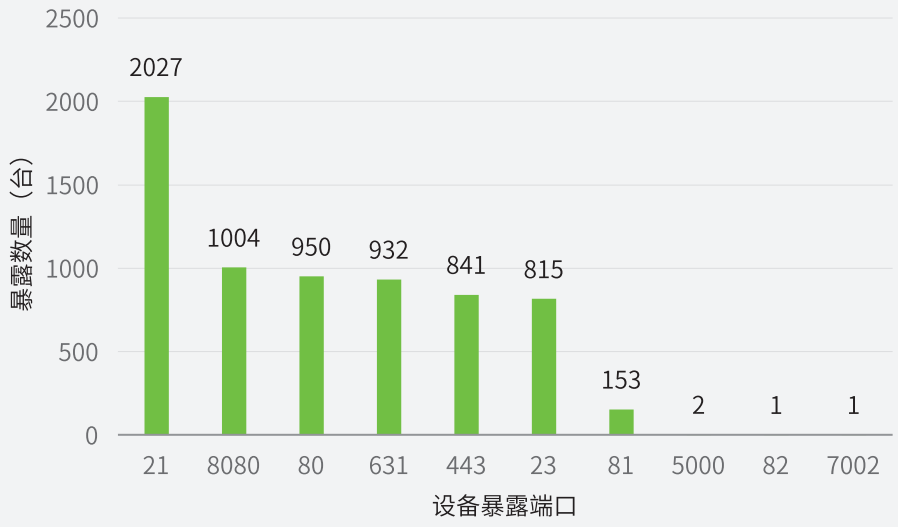


图 2.25 HP 打印机端口暴露情况

表 2.4 打印机设备端口和协议的对应关系

端口	21	80、8080	443	631	23
协议	FTP	HTTP	HTTPS	CUPS	Telnet

观点 18： HP 打印设备提供 WEB 服务远程访问打印机功能

如表 2.4 所示，我们整理了暴露设备出现次数较多的端口和常用的端口及其对应的协议。其中 631 为 CUPS（Common UNIX Printing System）的默认端口，CUPS 是为解决 Unix/Linux 打印限制的打印机软件。由图 2.25 可以看出，暴露的打印机 30% 左右都开放了 80 和 8080 端口用来提供 WEB 服务。建议如果没必要 WEB 访问进行打印，应关闭相关端口，局域网访问即可。

2.4.2.2 城市分布分析

观点 19： 暴露的 HP 打印机主要分布在港台地区

根据上述统计可以发现，暴露的打印机主要分布在港台地区，占总暴露数量的 90% 以上，这一现象可能跟港台地区打印设备配置习惯有关。由图 2.26 端口的暴露情况可知，港台地区的打印设备半数以上开放了 WEB 服务，这样的配置习惯会大大增加打印设备在互联网上暴露的概率。当然这只是我们的根据初步结果所做的分析猜想，具体原因还需进一步的数据支撑和分析得出。

图 2.26 HP 打印机暴露城市分布情况

打印机在过去是长期被忽视的领域，合规性更是无从谈起，所以使用时更应提高警惕，不给蓄意不轨的人有可乘之机。建议一方面关闭不必要的端口，减少在互联网暴露现象；另一方面如果有相关的设置，可以对打印机的访问做一些限制，比如限制列表以外的 IP 访问打印机。

2.5 小结

网络监控设备、路由器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[6] 事件就是黑客利用网络摄像设备的弱口令等安全漏洞，主要对网络监控设备实施入侵，并植入恶意软件构建僵尸网络，致使网络瘫痪等现象。如果有大量的物联网设备暴露在互联网上，像此类的安全事件随时都有可能发生，不仅会让我们无法正常使用这些设备，更重要的是某些重要信息也会被他人窃取。

三．物联网操作系统在国内的暴露情况

3.1 引言

中国信通院发布的物联网白皮书（2016）[11] 指出：物联网操作系统面向可伸缩、互通性实现创新发展。书中把市场上现有的物联网操作系统分为两种，一种是由智能手机、PC 系统剪裁而来，用在嵌入式设备上，具备较强的应用能力，但是底层的优化能力差；另一种是由传统的嵌入式操作系统演化而来，其基于传统操作系统的任务调度等优势，加入了联网等功能，有些还甚至集成了市场上常用的无线模组驱动程序，以满足物联网设备稳定工作和联网的基本需求。

本章搜集了常见的物联网操作系统，并针对其中应用较广的操作系统进行分析，希望可以对读者有所帮助。

3.2 操作系统列表

本节列出了几个比较常见的操作系统和固件，包括：uClinux、VxWorks、DD-Wrt、OpenWrt、Fuchsia、Raspbian、Nucleus、Tizen、Raspberry Pi、MICO、LEDE、Contiki、Zephyr、Brillo。我们对每个操作系统在 NTI 中的暴露情况做了数量统计，其分布如图 3.1 所示：

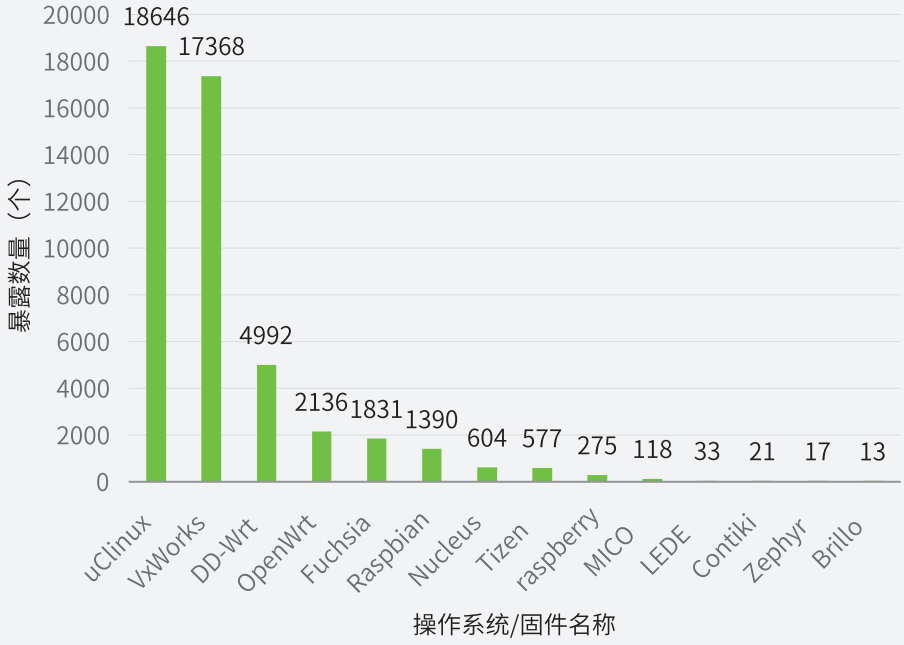


图 3.1 各操作系统数量对比

在 NTI 中找到的数量差别比较大。数量较多的系统是 uClinux、VxWorks、DD-WRT、OpenWrt、Fuchsia、Raspbian/Raspberry Pi、Nucleus 和 Tizen。其中，搜索“Tizen”获得的信息虽然数量多，但是大多数由于存在于设备的 banner 中的系统列表中而被搜索到（如 banner 中出现这样的信息：",mac:"MacOS",win:"Windows",tizen:"Tizen",linux chrome"），与 Tizen 操作系统本身和应用并无关系，所以暂时不对 Tizen 进行分析。由于 OpenWrt、DD-WRT 和 LEDE 均源于 Linksys 的一款路由器的源码，本次把这三款操作系统或固件集中在一个小节中分析。因此，接下来分别对 uClinux、VxWorks、OpenWrt 系列（DD-WRT、OpenWrt、LEDE）、

Raspbian/Raspberry Pi、Nucleus 分析。由于其余操作系统数量较少，所以暂不做分析。另外，对各个操作系统信息分析的过程中，会忽略一些数量较少的服务或端口，例如：只对数量在 50 以上的端口或者服务做数量对比，分析某些设备或操作系统的特征。

3.3 物联网操作系统设备信息暴露情况与分析

3.3.1 Nucleus

基于 Nucleus OS 的开发包名为 MTK，所以很多人容易联想到国产的手机。在 2008 年，以 MTK 为平台的山寨手机依靠奥运直播风靡一时，当时山寨手机上用的就是 Nucleus 操作系统。现在 Nucleus 也被 Mentor Graphics 用于硬件系统的功耗控制（Power Limit），平常对硬件和底层关心较多的朋友可以关注一下。

观点 20： 运行“Nucleus”的设备通常会开启 HTTP 服务和 FTP 服务。平均每个主机开启了 1.59 个端口提供 HTTP 服务，开启 21 端口的主机占到所有主机总数的 75.6%。

在 NTI 找到了 604 条主机 IP，对端口和上层协议统计信息如下：

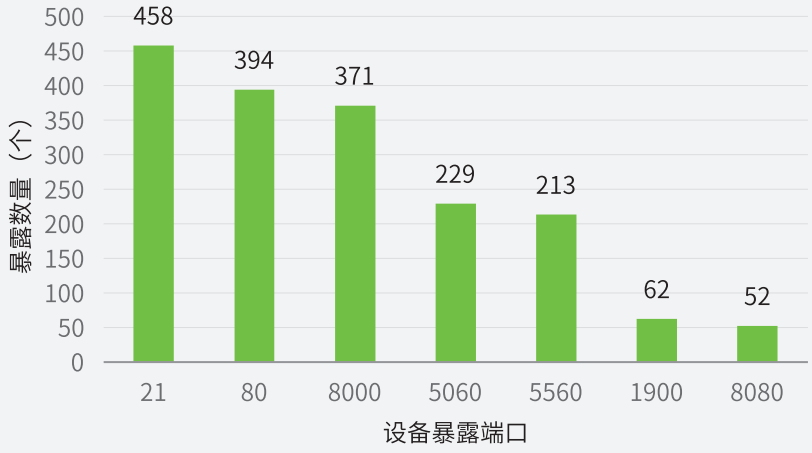


图 3.2 Nucleus 端口统计

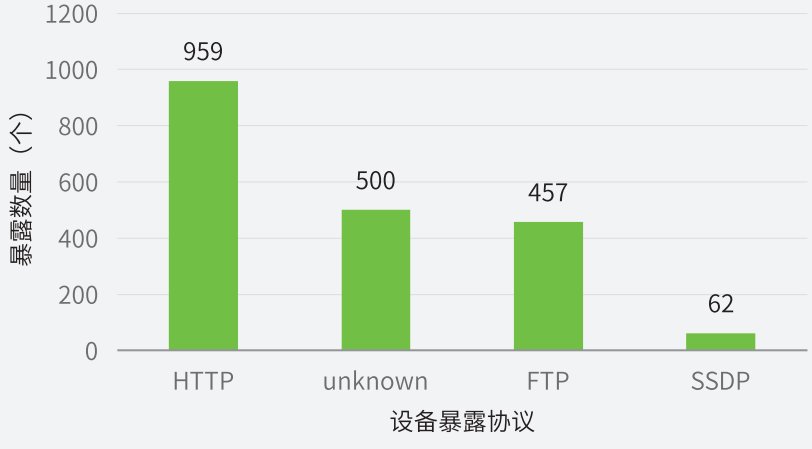


图 3.3 Nucleus 协议统计

从图 3.2 和图 3.3 中可以分析得出：HTTP 服务数量是主机数量（604）的 1.587 倍。FTP 服务的数量占到主机数量的 75.6%。同时，针对此类设备，统计了 HTTP 协议中的 title 信息。如图 3.4 所示：

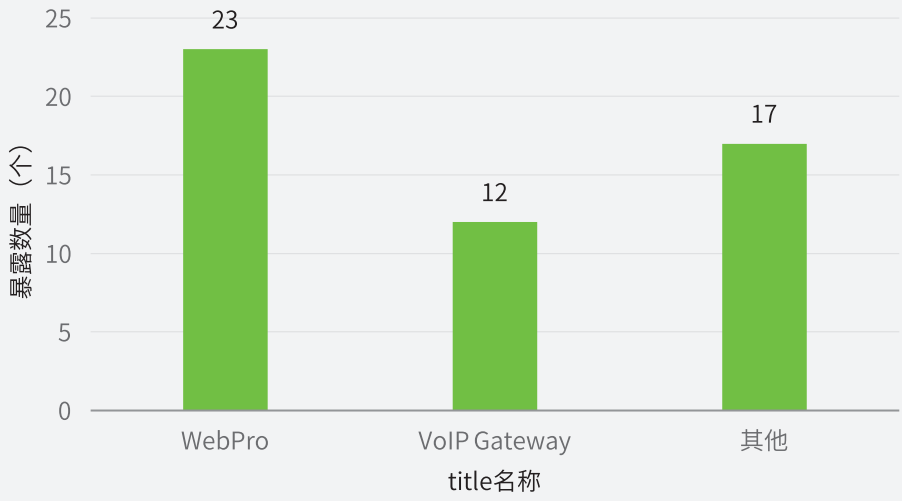


图 3.4 Nucleus 中 HTTP 页面非空白 title 统计

在开放 HTTP 协议的主机中，具有 title 信息的总共有 513 个。这些设备不多，仅供参考，因为空白 title 就有 460 个，除去空白项之外，WebPro 占到了 43.4%，VoIP GateWay 占到了 22.6%。根据这些的信息，可以猜测，在 460 个空白项中，有一部分是网关类产品，如果 IP 被设置了访问限制，知道开启了端口却无法访问相应服务就很正常，获取的 title 字段自然为空。

另外，有 441 条 FTP 的 banner 中出现这样的信息：“220 Nucleus FTP Server (Version 1.7) ready”，这就意味着这些设备存在一定的共性，这种共性或者因为厂商而存在，或者因为系统本身的特性而存在。60 个主机出现这样的 banner：“Nucleus/4.3 UPnP/1.0”，而且在图 3.3 中找到的 SSDP 服务的数量为 62，可以证明一部分主机还开启了和 UPnP、SSDP 等相关的服务。

3.3.2 OpenWrt/DD-WRT/LEDE

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，OpenWrt 和 DD-WRT 就是其中的两个，而 LEDE 是基于 OpenWrt 的一款嵌入式 Linux 发行版。它们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、机器人等）上面。

观点 21：运行“OpenWrt/DD-WRT/LEDE”的设备中，至少有 13.0% 没有修改默认配置，做端口映射的现象也比较常见。

图 3.5 和图 3.6 对 OpenWrt 系列的端口和上层协议数据进行了简单的统计：

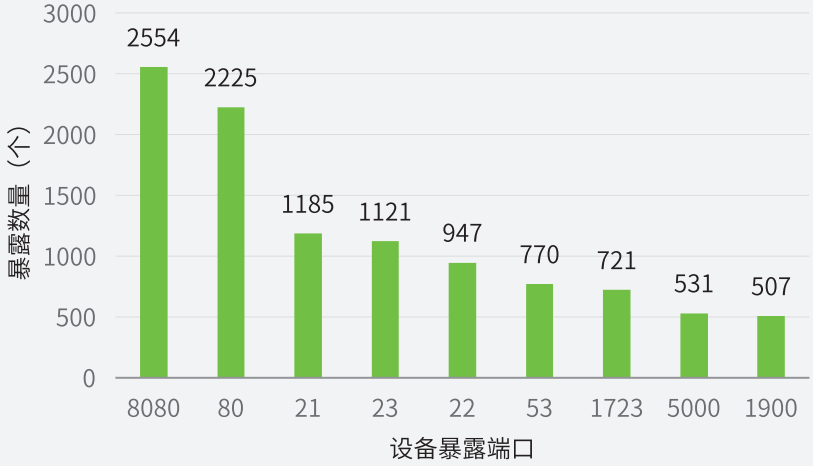


图 3.5 OpenWrt 系列端口统计

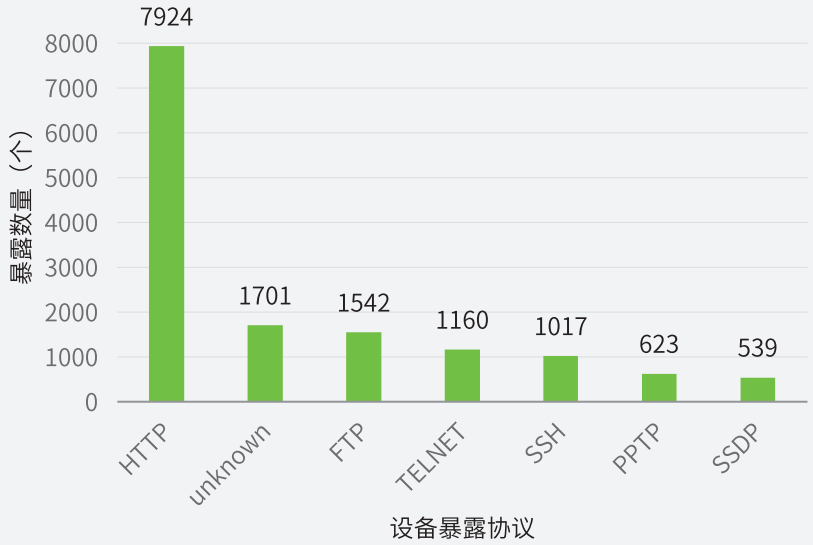


图 3.6 OpenWrt 系列协议统计

在 7150 台主机中，HTTP、SSH、FTP 和 Telnet 服务开启的数量较多。HTTP 协议的数量达到了 7924 个，是主机数量的 1.108 倍，SSH、FTP 数据也都超过了 1000。如果以端口数据统计，开启 21 端口的主机占到了 16.5%，开启 22 端口的主机占到了 13.2%，开启 23 端口的主机占到了 15.6%。

另外，一个 IP 开启了多个相同服务的现象在这类设备上很常见：

DD-Wrt	[redacted]	cathayQ1100-1 (build 13491M) - 資訊	HTTP	81	2016-06-02T15:31:13
DD-Wrt	[redacted]	VoIP Gateway	HTTP	8080	2016-06-02T15:31:13
DD-Wrt	[redacted]	VoIP Gateway	HTTP	8081	2016-06-02T15:31:13
DD-Wrt	[redacted]	Q1100-5F (build 19154) - 資訊	HTTP	82	2016-06-02T15:31:13
DD-Wrt	[redacted]	cathayipad5f (build 19154) - 資訊	HTTP	83	2016-06-02T15:31:13
DD-Wrt	[redacted]		HTTP	84	2016-06-02T15:31:13

图 3.7 OpenWrt 系列部分 HTTP 服务信息统计

图 3.7 中，某个主机开启了 6 个 HTTP 服务，这 6 个服务的 title 信息出现了 4 种设备，由此可见，这一个 IP 背后至少有 5 台设备，其中有两台 VoIP Gateway。由此可知，简单扫描是无法确定设备类型的，因为 NAT 映射

会使得一个 IP 具有多个设备的融合属性。

同时，发现它们的 banner 信息中有这样的字符出现：DD-WRT (build xxxxx="infopage">（xxxxx 表示 5 位数字，通常是 DD-WRT 固件编译版本），也有这样的字符出现：R6300 DD-WRT (build 。所以，以 build 为关键字进行字符匹配检索时，发现在 16583 个服务中，build 字段出现了 2148 次，约为 13.0%。Basic realm="DD-WRT" 字符出现了 817 次，约为 4.9%。这说明了一部分人基于 DD-WRT 类固件或者操作系统开发时，并没有改变路由器的默认配置。

3.3.3 Raspbian/Raspberry Pi

Raspbian 是一个基于 Debian，为 Raspberry Pi（中文翻译为“树莓派”，下同）硬件优化的免费操作系统，它提供超过 35,000 个软件包。广大智能硬件爱好者对这个系统再熟悉不过了。与传统的嵌入式操作系统相比，Raspbian 只需要由爱好者通过诸如 Win32DiskImager 这样的软件，把官方提供的 img 系统包直接烧入到 SD 卡，即可运行在树莓派硬件之上。许多创客（Maker）都在基于树莓派、Arduino 等开源硬件做一些有意义的事情。

观点 22： 运行“Raspbian”的设备有一个很重要的特征：67.9% 的设备上，SSH 服务是对外开放的。

NTI 的数据中总共有 1390 个国内主机。图 3.8 和图 3.9 统计了主机开启的服务和端口：

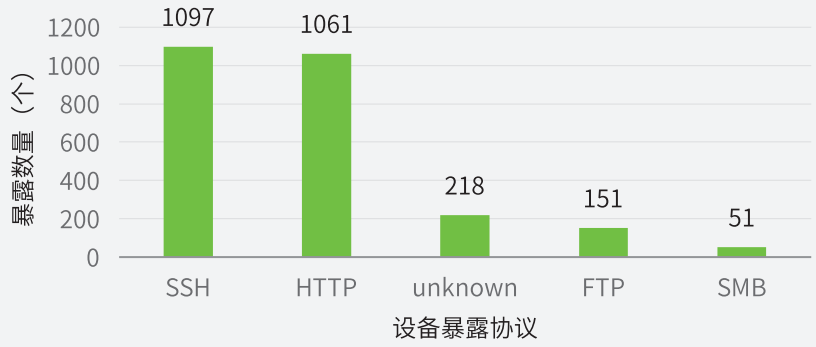


图 3.8 Raspbian 协议统计

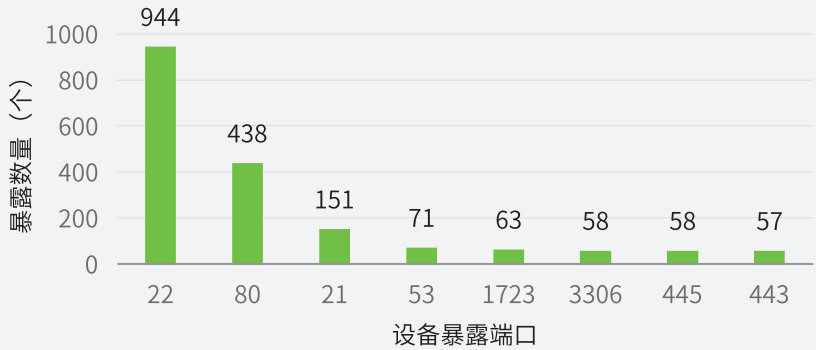


图 3.9 Raspbian 端口统计

根据统计情况看，在 1390 个主机中，有 944 台主机开放了 22 端口，占有率高达 67.9%。由于树莓派是一个开源智能硬件，它的出现主要是方便开发者、智能硬件发烧友快速制作产品原型，所以大多数人并没有修改 Raspbian 默认配置，保留了 SSH 服务。可以说绝大部分这类设备（智能硬件——树莓派）SSH 服务是对外开放的。

当对端口分析时，发现暴露数量在 10-50 的端口大多数为 HTTP 服务，正好解答了图 3.8 和图 3.9 中 HTTP 协议和 80、443 端口数量差距较大的问题。图 3.10 中，8080、8000、81、8888、88、8081、82、8088、

10000、8443、5000、83、10089、8090 这些经常开启 HTTP 服务的端口的个数为 307。加上 443 端口和 80 端口，总数超过 800。

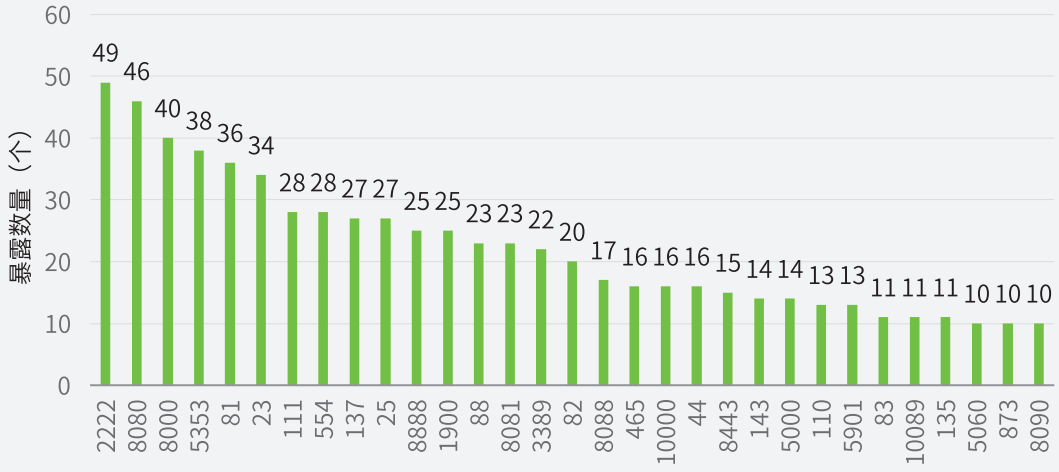


图 3.10 暴露数量介于 10-50 的端口统计

3.3.4 uClinux

一开始的 uClinux 是 Linux 2.0 内核的衍生物，用于没有内存管理单元（MMU）的微控制器，而且 Linux 微控制器项目在处理器架构的品牌识别和覆盖方面都有所增长。今天的 uClinux 作为操作系统包括了 2.0、2.4 和 2.6 的 Linux 内核版本，以及用户应用程序，库和工具链的集合。uClinux 是嵌入式 Linux 领域非常重要的分支，已应用于路由器、机顶盒、PDA 等领域。

观点 23： 98.4% 运行“uClinux”的设备都会开启 SSDP 服务。

在 NTI 中搜索到 18646 个主机。由于数量较大，直接统计了协议和端口信息。

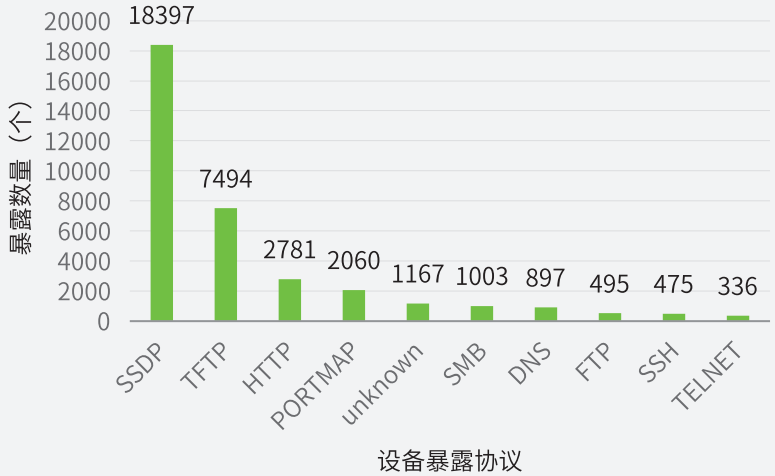


图 3.11 uClinux 协议统计

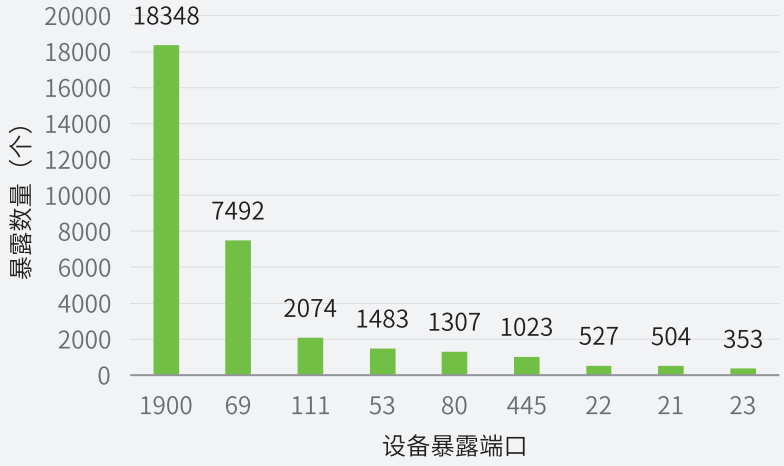


图 3.12 uClinux 端口统计

由于端口和协议种类较多，图 3.11 和图 3.12 中只显示了数量大于或等于 300 的主机，纵向看，协议和对应端口号从数量关系上基本对应，如 SSDP 协议的 1900 端口号上传输数据，两者数量差别不大。横向看，特征就凸显出来了，18646 个主机中有 18348 个主机开启了 1900 端口，约占主机总数的 98.4%，几乎全部的 SSDP 服务都在 1900 端口上，而且在 banner 信息中，Server: uClinux/2.6.28.10 UPnP/1.0 MiniUPnPd/1.3 出现了 18001 次。因此，可以猜测，这类设备往往会是路由器类设备，通过 UPnP 技术实现局域网内多台设备和服务的远程访问。

3.3.5 VxWorks/ WindRiver

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 24： 运行“VxWorks”的设备对 HTTP、SSH 和 Telnet 开放较多，平均每个主机开启了 1.08 个端口提供 HTTP 服务，21 端口和 22 端口占所有主机数量的 67.5% 和 66.9%。

由于 VxWorks 专用性较强，所以其指纹特征较为可信。NTI 中有 17368 个主机，其端口和上层协议分布如图 3.13 和图 3.14 所示：

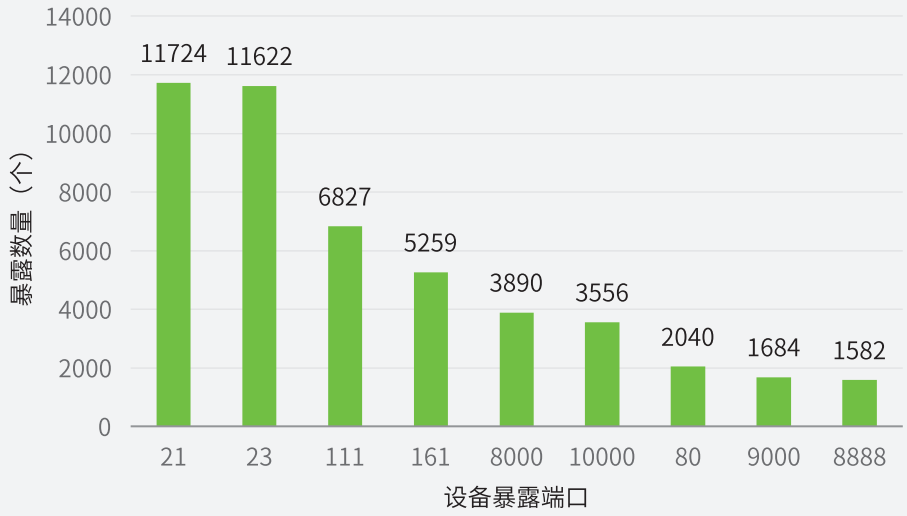


图 3.13 VxWorks 端口统计

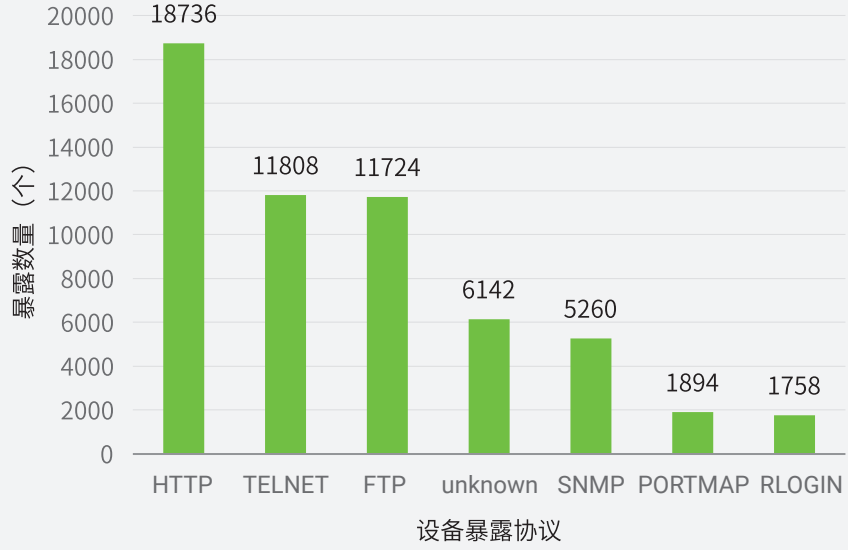


图 3.14 VxWorks 协议统计

从端口分布上看，23 端口和 21 端口数量非常接近，占到了约全部主机的 67%。其他的端口中，HTTP 协议占了大部分。从协议统计的信息中可以看出，HTTP 服务的数量达到了 18736 个，是全部主机数量的 1.079 倍。所以，在 VxWorks 这类设备上，平均至少会开启一个 HTTP 服务。FTP 和 Telnet 服务的数量和对应的端口号（21、22 端口）信息差距不大，从结果上看，FTP 和 21 端口的数量是一样的，Telnet 服务有一部分被映射到了其他的端口。

另外，在 VxWorks 的 17368 主机中，有 9716 个主机的 banner 信息含有 220 VxWorks (VxWorks5.5.1) FTP server ready。在 4758 个主机中出现了 VxWorks SNMPv1/v2c AgentVxWorks SNMPv1/v2c Agent 或 VxWorks SNMPv1/v2c Agent 的 banner 信息。

3.4 物联网操作系统分析小结

到此为止，我们分析了 Nucleus、OpenWrt、Raspbian、uClinux、VxWorks 这几种比较常见的操作系统。主要针对设备暴露的端口、应用层协议。可以说明：

1. 运行以上 5 个操作系统的设备会暴露一些特性，这些特性会出现在服务的 banner 信息中。例如 VxWorks 的“220 VxWorks (VxWorks5.5.1) FTP server ready”、uClinux 的“Server: uClinux/2.6.28.10 UPnP/1.0 MiniUPnPd/1.3”等。
2. 有些设备未经更改默认配置，直接部署到了互联网上。例如：DD-WRT 固件中 HTTP 协议的 title 字段中包含“DD-WRT (build xxxxx="infopage">”。
3. 某些 IP（设备）背后隐藏着很多内网 IP（设备）。往往有多个设备通过 UPnP 挂接到路由器上，表现为一个 IP 的不同服务中会有多个设备的标识出现，因为 NAT 映射会使得一个 IP 具有多个设备的融合属性。

其他的操作系统（如 Brillo、TinyOS、LiteOS、Linino OS、Ostro、FreeRTOS、Contiki、MICO、Zephyr 等）因为在网络空间搜索引擎中暴露数目较少，本文不在对其进行深入分析。

四．总结

借助于 NTI、Shodan 和 ZoomEye 的扫描数据，我们对位于中国的物联网资产进行了分析。分析维度分为两类，一类着眼于设备，关注于不同种类的设备在互联网的分布情况；一类着眼于物联网操作系统，关注于都有哪些操作系统暴露在互联网上。

由于精力有限，很难保证涵盖到所有种类，对于所包含的类别，也很难保证数据百分之百的准确性。但在分析过程中，我们通过对于三大搜索引擎的数据对比以及分析，尽可能确保了数据的全面性和准确性。另外，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。从这个角度来讲，少量遗漏或噪声数据并不影响文章的观点。

本次我们主要对物联网设备中的视频监控设备、路由器和打印机进行分析，未来我们将会分析更多设备的暴露情况，并对本文中的数据做必要更新。

结合我们的分析，下面分别从用户角度和厂商角度给出一些防护建议。

用户角度：

（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）及时升级设备固件。

厂商角度：

（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。

参考资料

[1] NTI，绿盟科技威胁情报中心，https://nti.nsfocus.com/

[2] Shodan，https://www.shodan.io/

[3] ZoomEye，https://www.zoomeye.org/

[4] 路由器“保护”天使：“恶意软件”Linux.Wifatch，http://www.freebuf.com/news/80510.html

[5] 神秘恶意软件 Wifatch 开发者浮出水面，http://www.aqniu.com/industry/10656.html

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

[7] 13.7 亿数据泄露大案如约而至，http://mt.sohu.com/20170307/n482644552.shtml

[8] 如何访问双频无线路由器 FTP 服务器，http://service.tp-link.com.cn/detail_article_511.html

[9] 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

[10] 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

[11] 物联网白皮书（2016），中国信通院

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

[13] Is there an Internet-of-Things vigilante out there?, https://www.symantec.com/connect/blogs/there-internet-things-vigilante-out-there

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

[15] 全球 60 余万台 IOT 设备遭 Mirai 感染，http://www.kejixun.com/article/161020/237548.shtml

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

[17] 小米路由器销量破千万 连接设备破 1.2 亿，http://tech.ifeng.com/a/20170119/44533970_0.shtml

[18] 360 路由器 2016 上半年销量增长 143% 排名第一，http://network.pconline.com.cn/821/8217402.html

[19] 宇视 2013 年居中国市场第三：构建最全产品序列，http://news.c-ps.net/article/201409/212461.html

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