国内物联网资产的暴露情况分析（2017.3）

绿盟科技 创新中心 物联网安全实验室

NSFOCUS

关于绿盟科技创新中心

云安全实验室

- 研究内容包括基于SDN/NFV的服务链设计、私有安全云服务设计、安全应用超市等
- 当前研究内容已应用于混合云服务提供商、电信运营商、能源、金融机构等众多领域客户

数据分析实验室

- 为绿盟科技产品线提供大数据分析和安全数据挖掘方面的支撑，旨在为安全产品和客户提供可落地的分析算法和可运维的分析能力

物联网安全实验室

- 对物联网安全事件进行分析，提出可落地的物联网安全防护措施及系统，为安全产品提供物联网攻击防护能力

CONTENTS 目 录

NSFOCUS

01

简介

NSFOCUS

背景

- 物联网发展前景广阔
  - Gartner预测，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
  - 2016年，物联网被写进“十三五”规划
- 众多物联网设备和应用面临严峻的安全挑战
  - 2016年下半年，物联网僵尸网络（Mirai）发动多起DDoS攻击事件
- 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，通过网络空间搜索引擎发现相关的物联网设备，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

网络空间搜索引擎

- 不同于互联网搜索引擎Google、百度，网络空间搜索引擎关注于IP地址以及其所对应的设备、其上运行的服务
  - NTI，绿盟科技的威胁情报平台
  - Shodan、ZoomEye
- 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

参考链接：https://nti.nsfocus.com/、https://www.shodan.io/、https://www.zoomeye.org/

研究内容和目的

研究内容

- 考虑到国内外的物联网系统和产品有较大的差异，我们主要对位于中国的物联网资产进行了分析
  - 物联网设备、物联网操作系统两个维度

目的

- 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

研究方法

- 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
- 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
  - 我们对主流家用路由器的绝大多数官网在售型号进行了搜索
  - 海康威视的视频监控设备的某些服务的 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视频监控设备
- 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

说明：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HTTP为例，收到的结果中包含了HTTP的header和body两部分。Server: Hikvision-Webs即位于HTTP的header部分

关键性发现

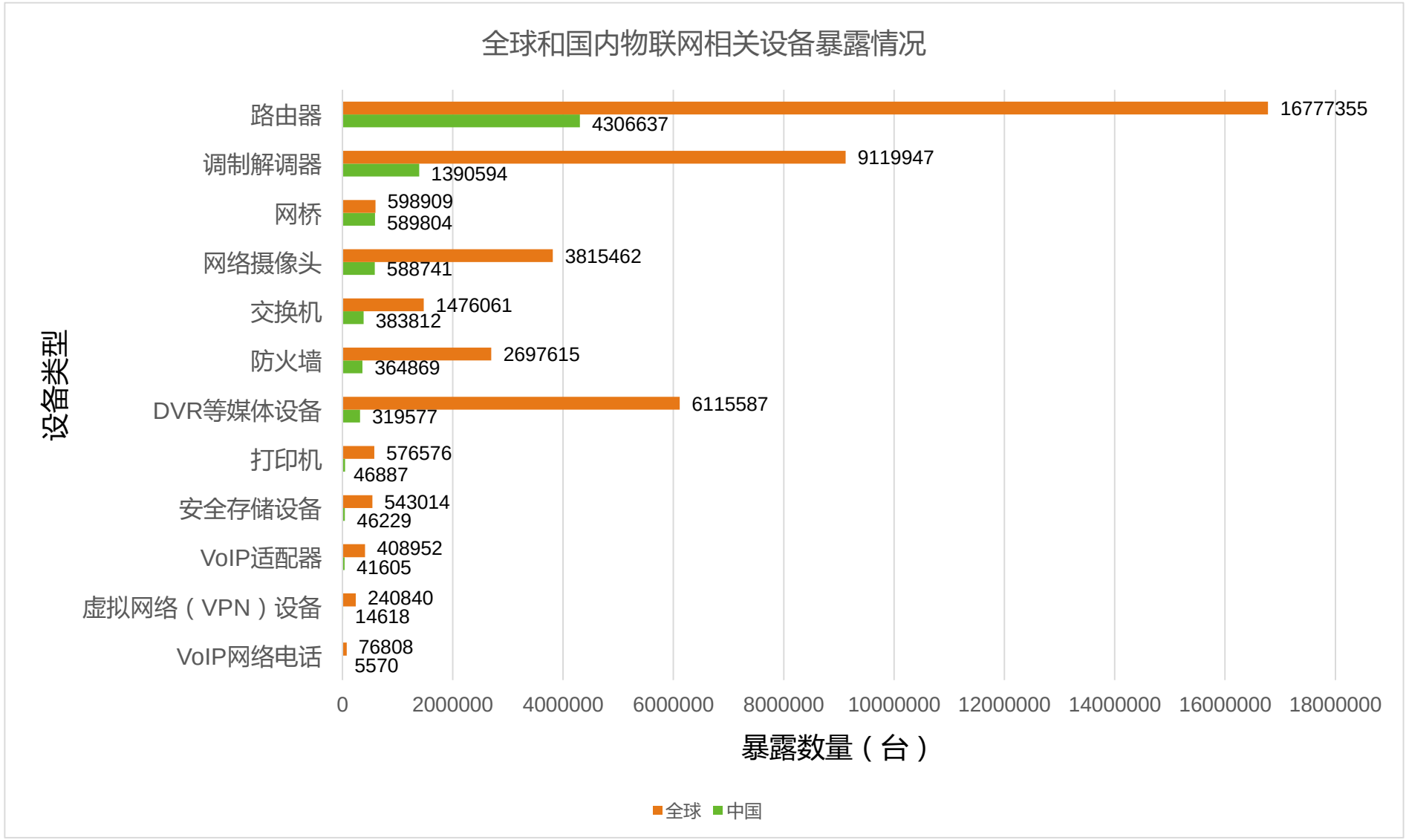
- 海康威视和浙江大华两大厂商的网络监控设备暴露数量最多，东南沿海为国内网络监控设备暴露最严重的区域
- 暴露在国内互联网上的路由器以国产品牌为主，暴露出来的端口所对应的协议以UPnP和FTP协议为主。互联网厂商的路由器销量增长迅猛但暴露较少
- 国内有上万台路由器感染恶意软件Linux.Wifatch，路由器安全现状不容乐观
- 港台地区为网络打印机暴露的重灾区，暴露数量达总暴露量的80%以上
- 大部分搭载操作系统的设备未经更改默认配置就被部署到互联网上，可通过操作系统特有的banner信息被网络空间搜索引擎探测到
- 运行DD-WRT和uClinux的具有路由器功能的设备，在做了NAT的情况下，会使它本身的IP具有多个设备的融合属性

02

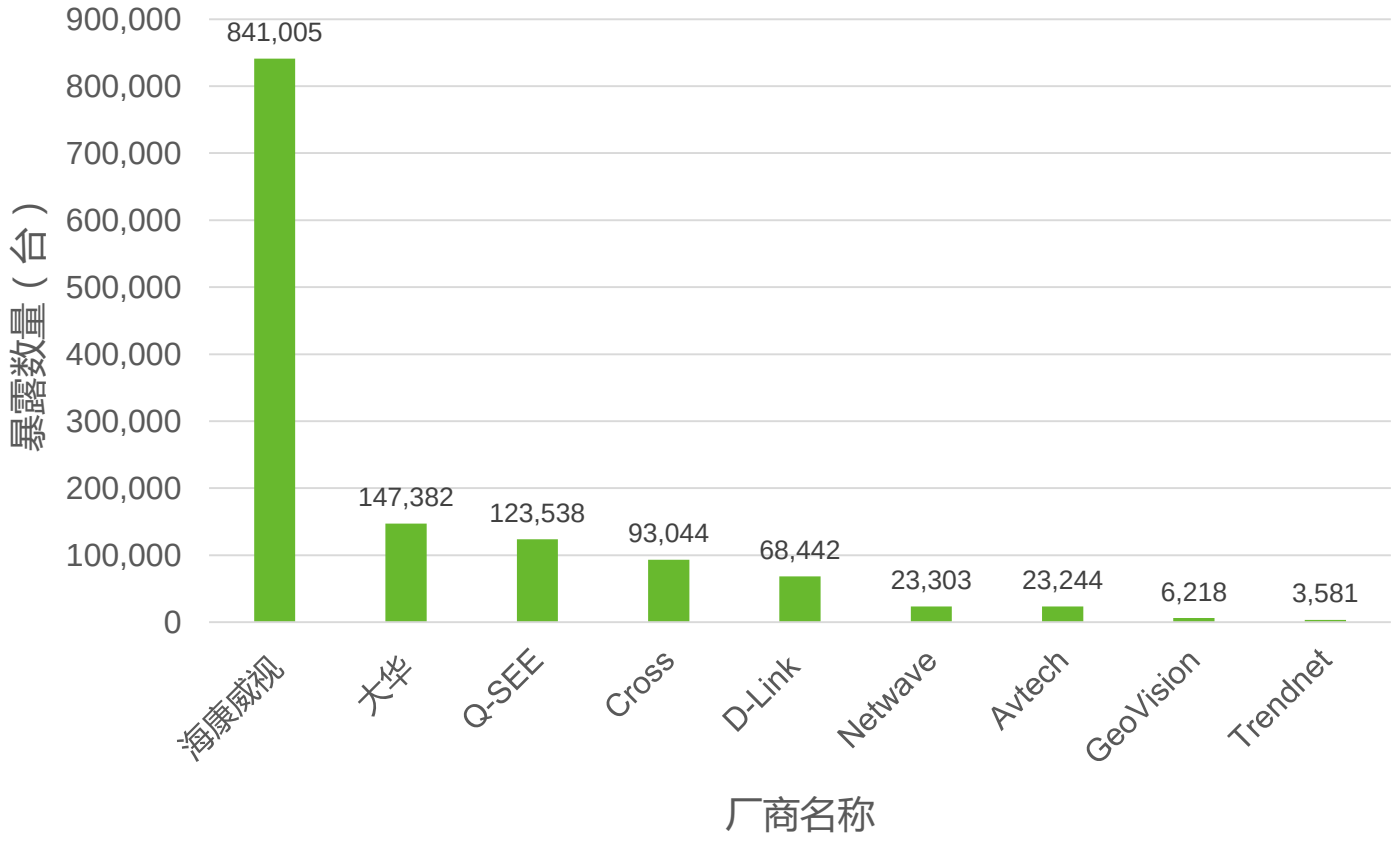
常见物联网设备在国内的暴露情况

NSFOCUS

全球和国内物联网相关设备暴露情况

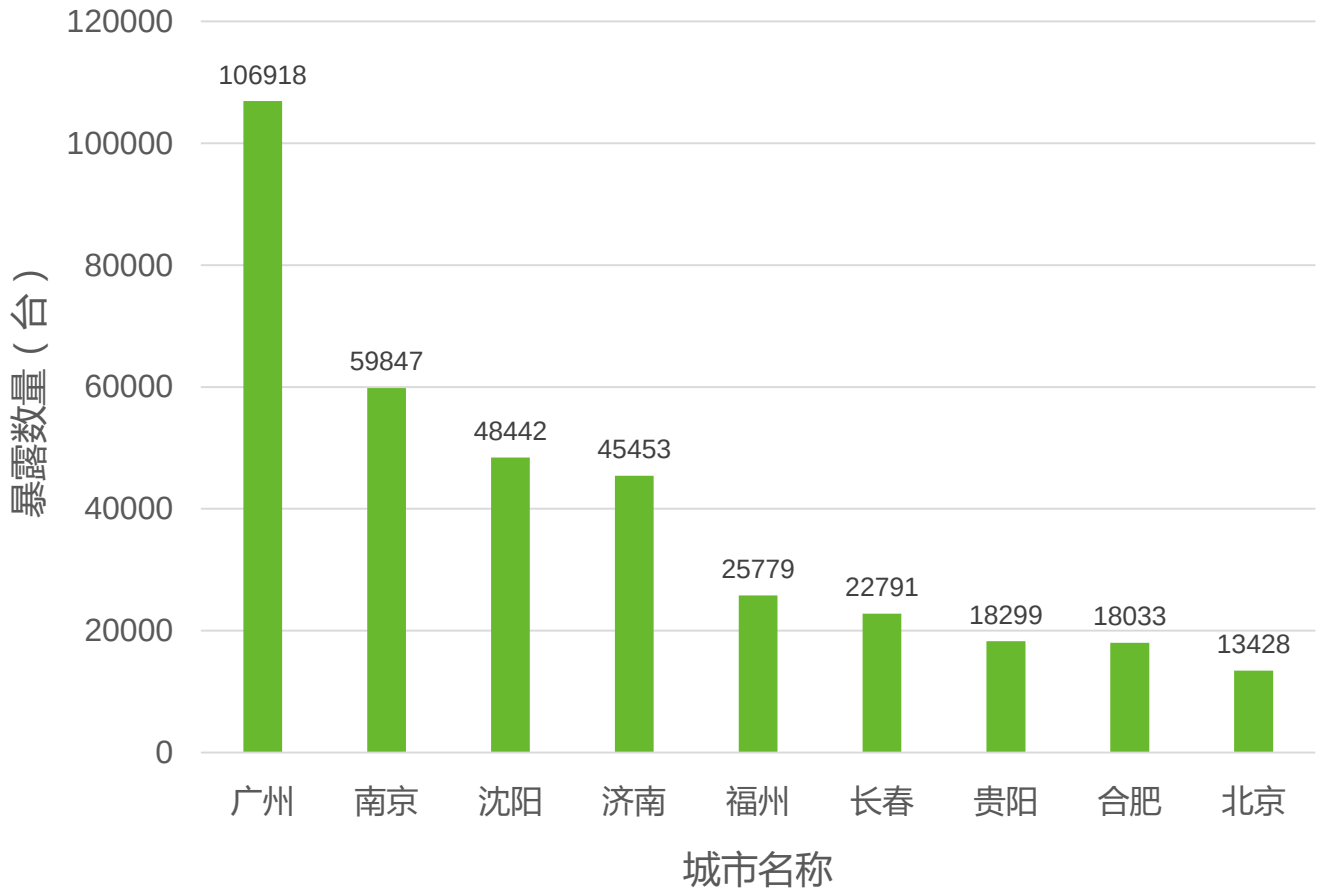


在视频监控设备中，海康威视和浙江大华两大厂商暴露数量较多



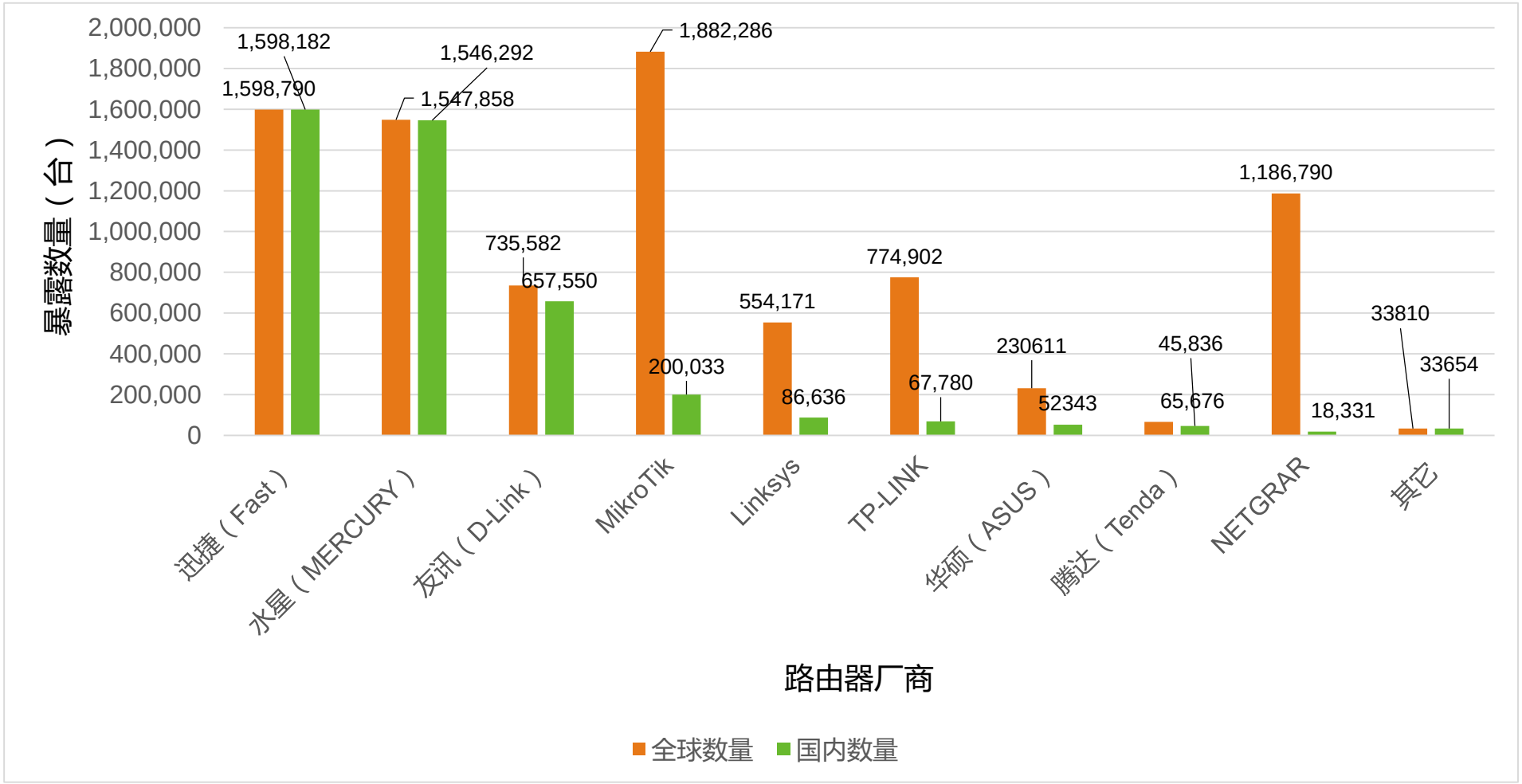
暴露的网络监控设备厂商分布

网络监控设备东南沿海地区暴露现象较明显



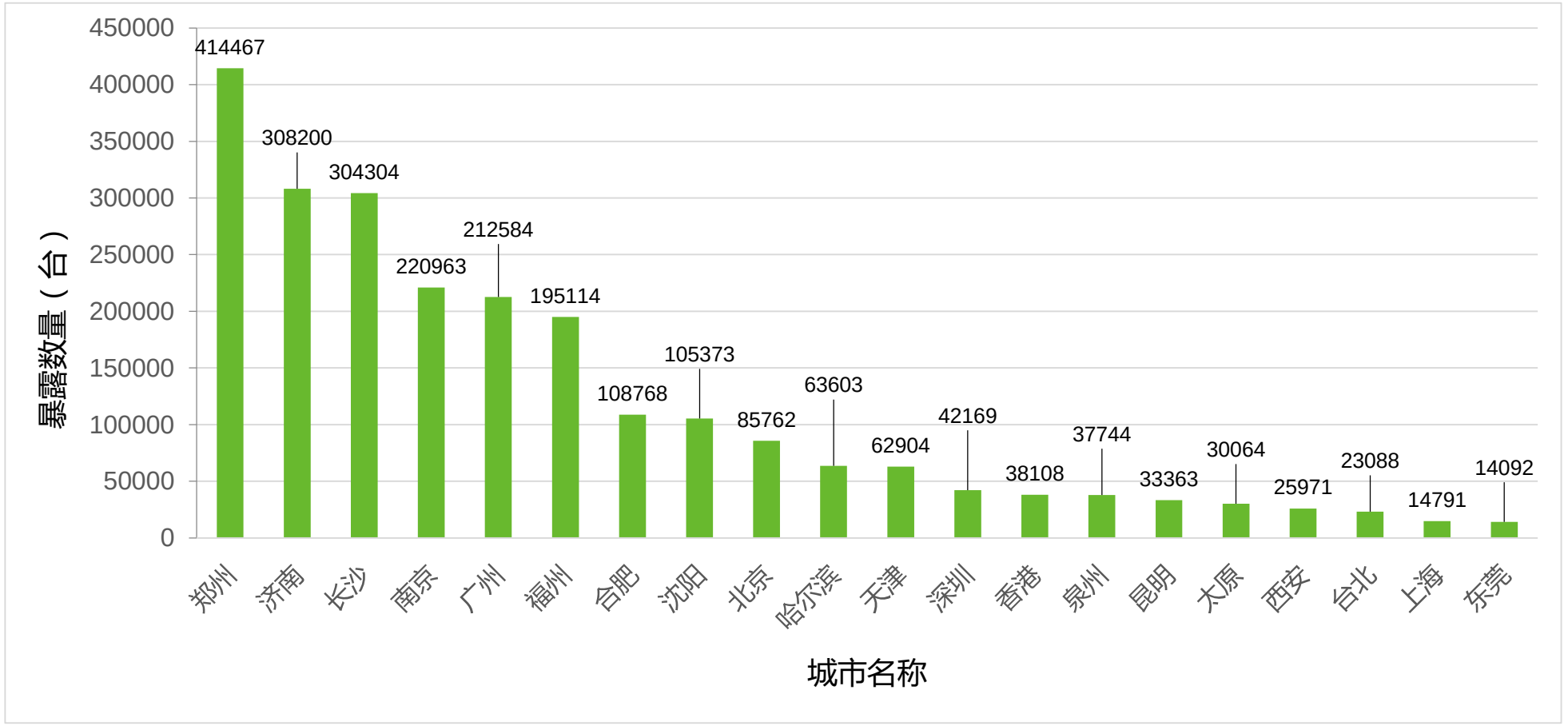
网络视频监控设备暴露城市分布情况

暴露在国内互联网上的家用路由器以国产品牌为主



各路由器厂商的暴露情况

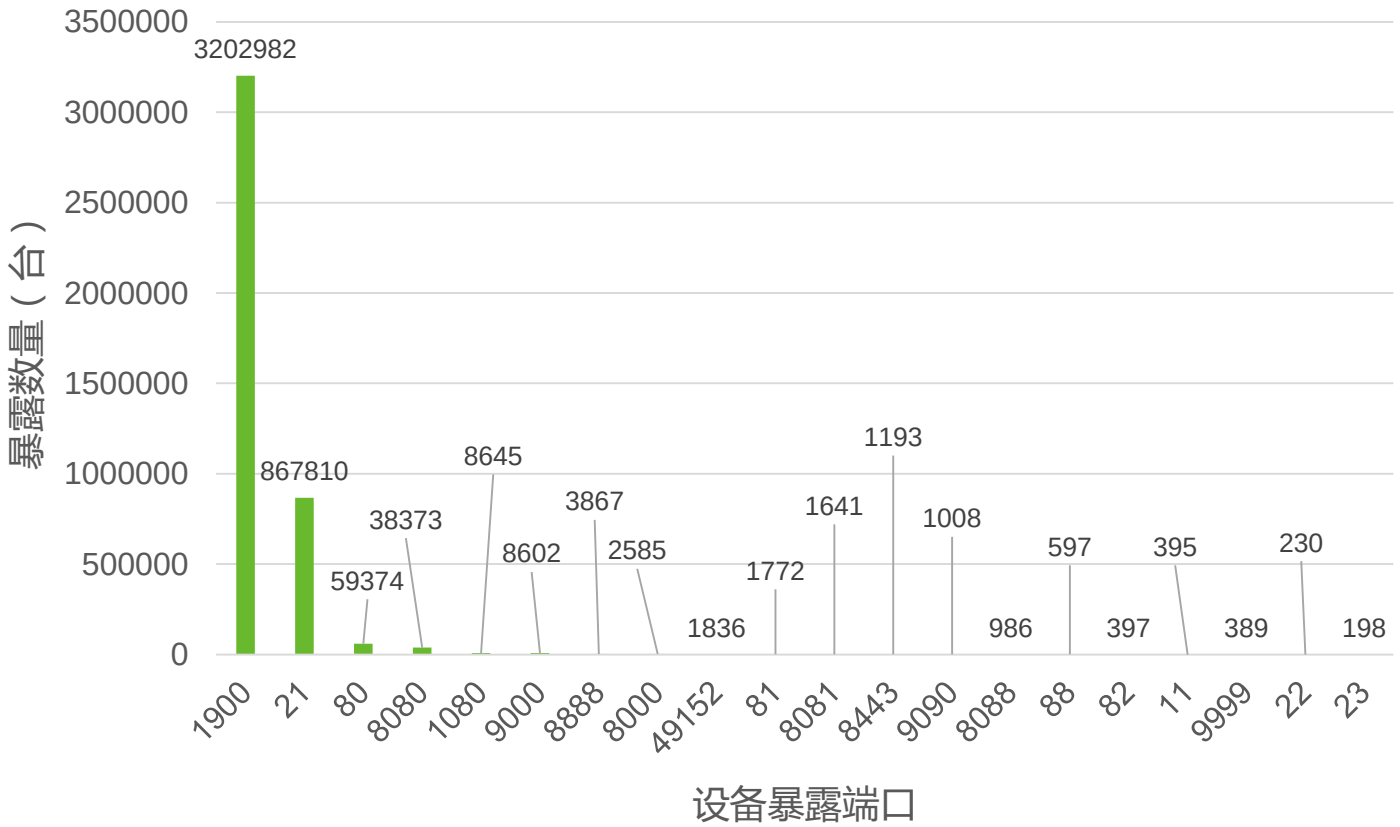
二线城市暴露出来的路由器数量最多



家用路由器按城市的分布情况

NSFOCUS

家用路由器端口分布广泛，但大多位于1900、21、80、8080端口
端口所对应的协议以UPnP和FTP协议为主



家用路由器按端口的分布情况

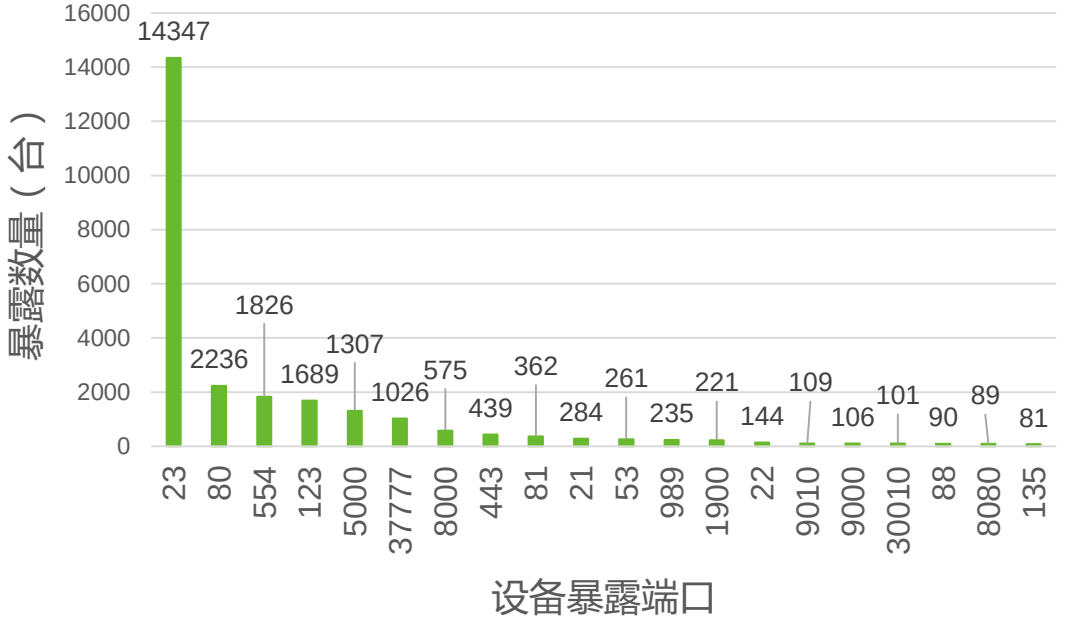
路由器端口和协议的对应关系

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

国内有上万台设备感染Linux.Wifatch

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，并给出下图所示的banner信息

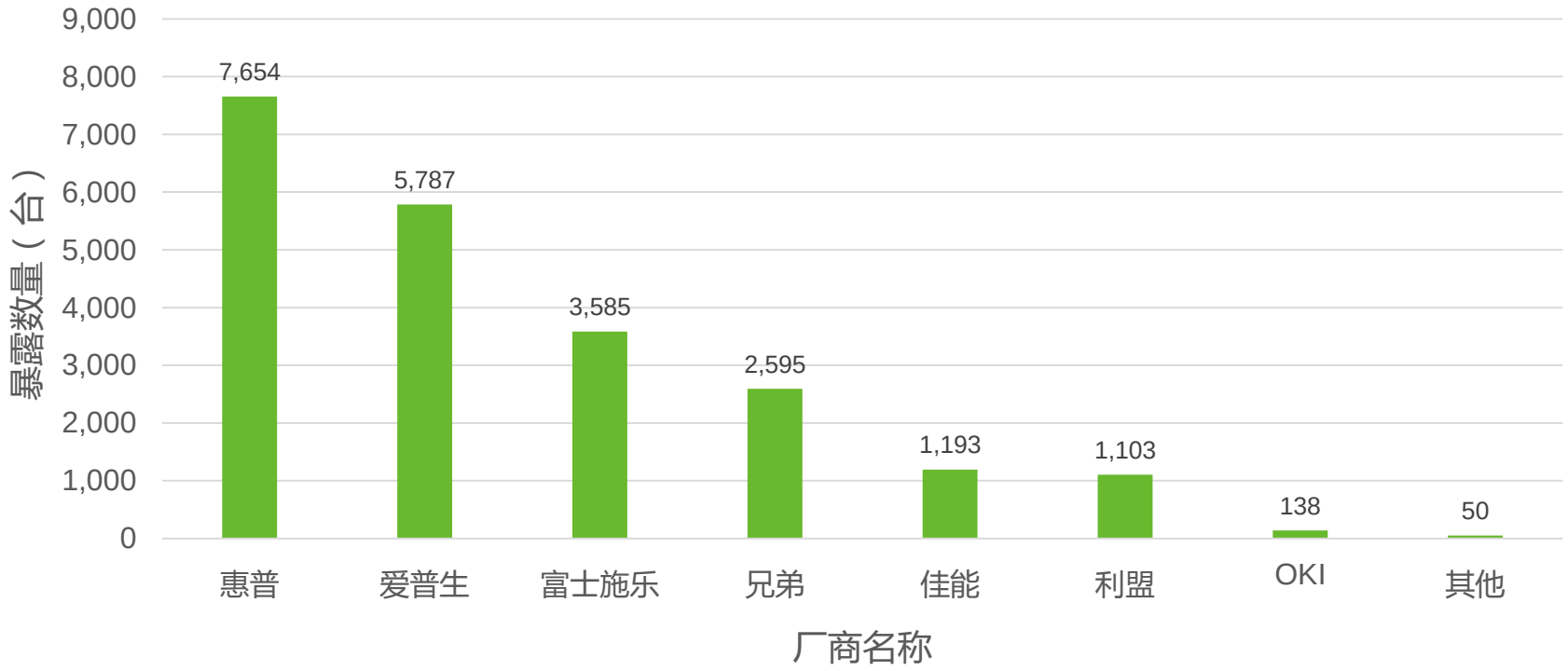
23	TELNET TCP	REINCARNA / Linux.Wifatch Your device has been infected by REINCARNA / Linux.Wifatch. We have no intent of damaging your device or harm your privacy in any way. Telnet and other backdoors have bee



Linux.Wifatch相关的设备端口暴露情况

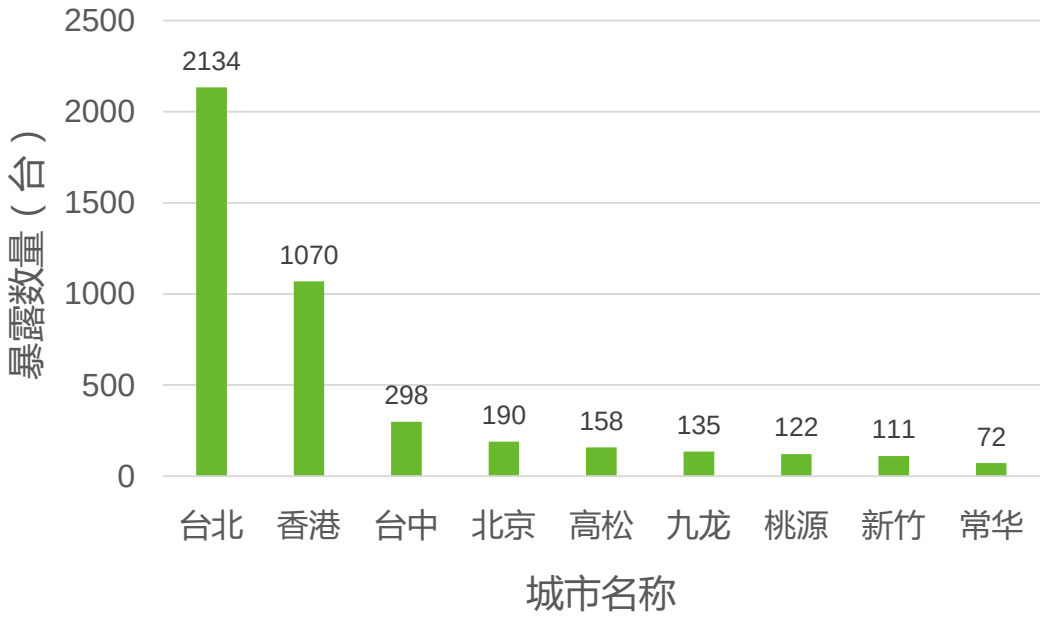
可在NTI中搜索REINCARNA AND country:China，国内数量为14347（2017/4/11）

惠普和爱普生的打印机暴露数量较多，占暴露总量的50%以上

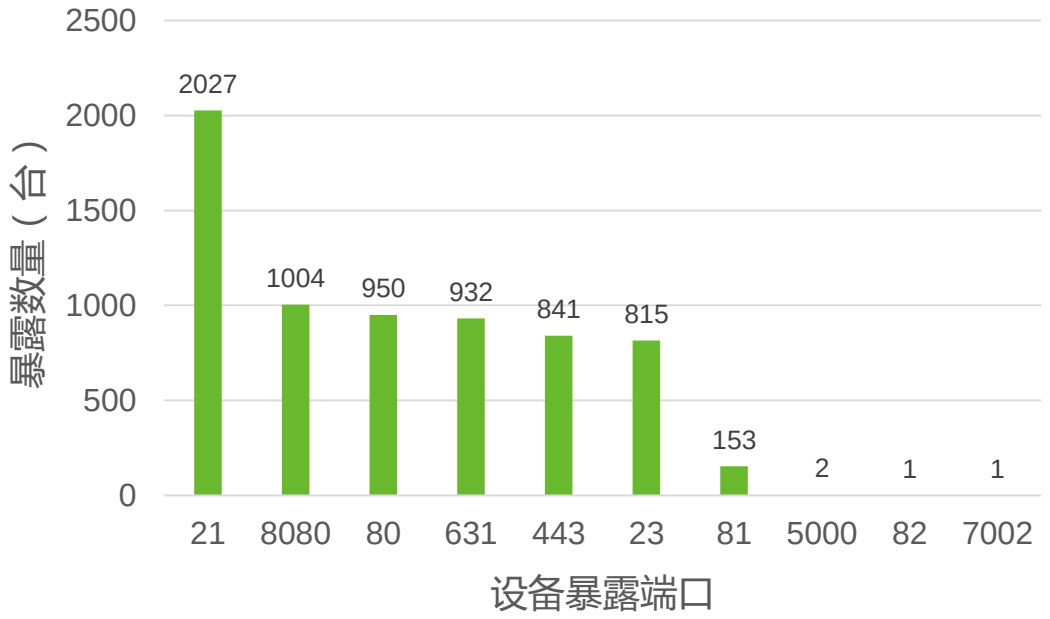


网络打印机暴露的品牌分布情况

暴露的HP打印机主要分布在港台地区
暴露端口以21、80、8080、631、443、23为主



HP打印机暴露城市分布情况



HP打印机端口暴露情况

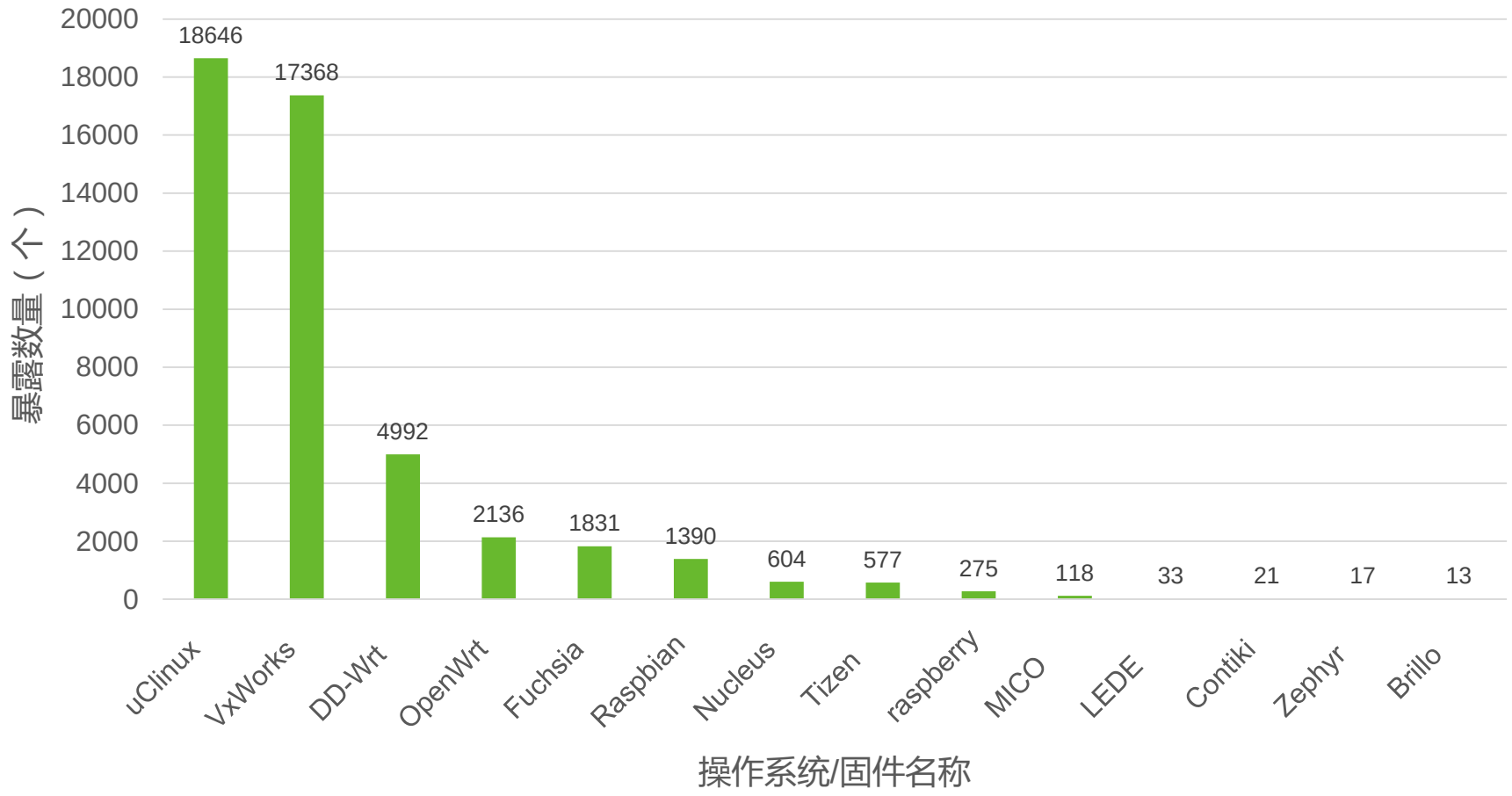
说明：631端口为CUPS（Common UNIX Printing System）的默认端口，CUPS是为解决Unix/Linux 打印限制的打印机软件

03

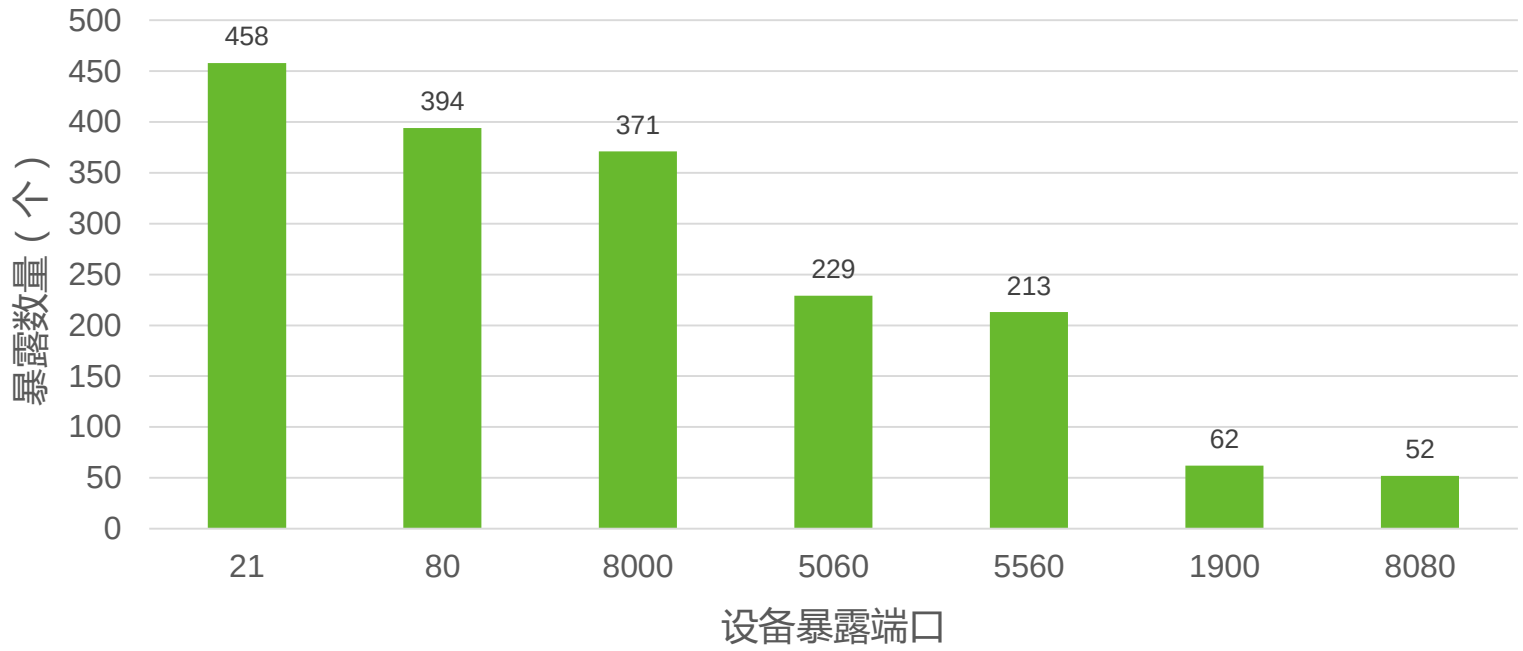
物联网操作系统在国内的暴露情况

NSFOCUS

物联网操作系统在国内的暴露情况

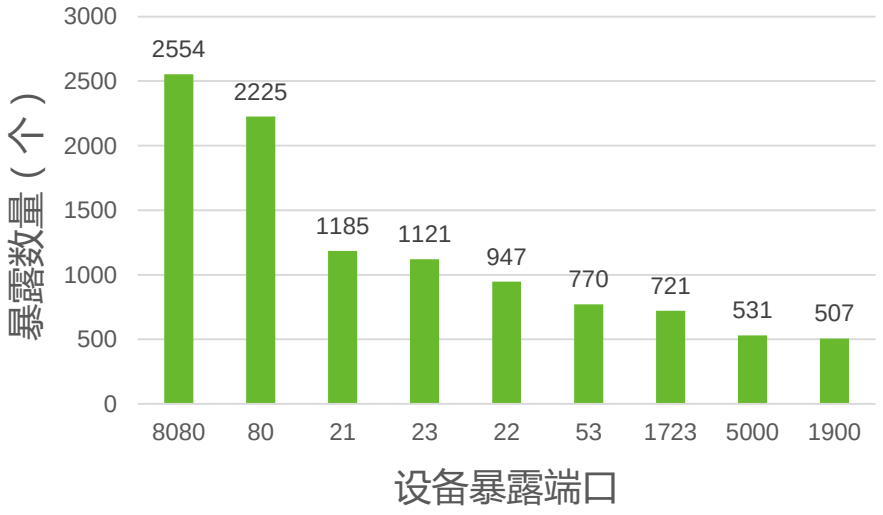


运行“Nucleus”的设备通常会开启HTTP服务和FTP服务，开启FTP服务的主机占到所有主机总数的75.6%

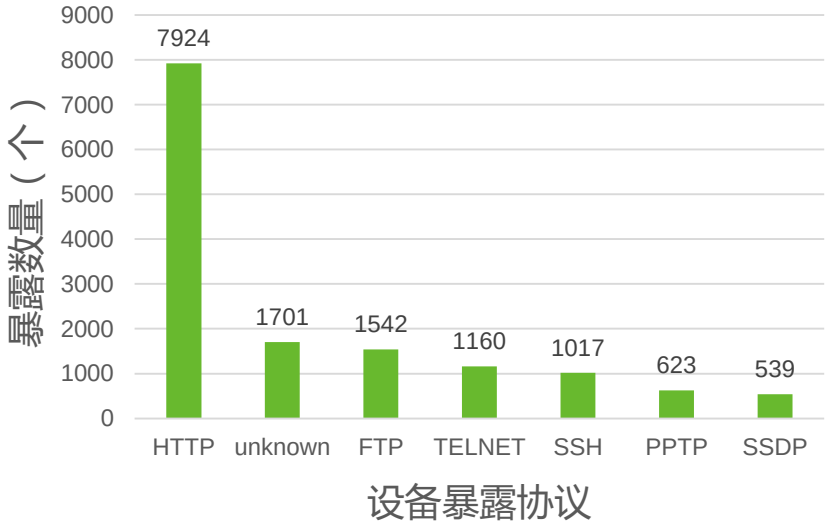


Nucleus暴露端口统计

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



OpenWrt系列端口统计

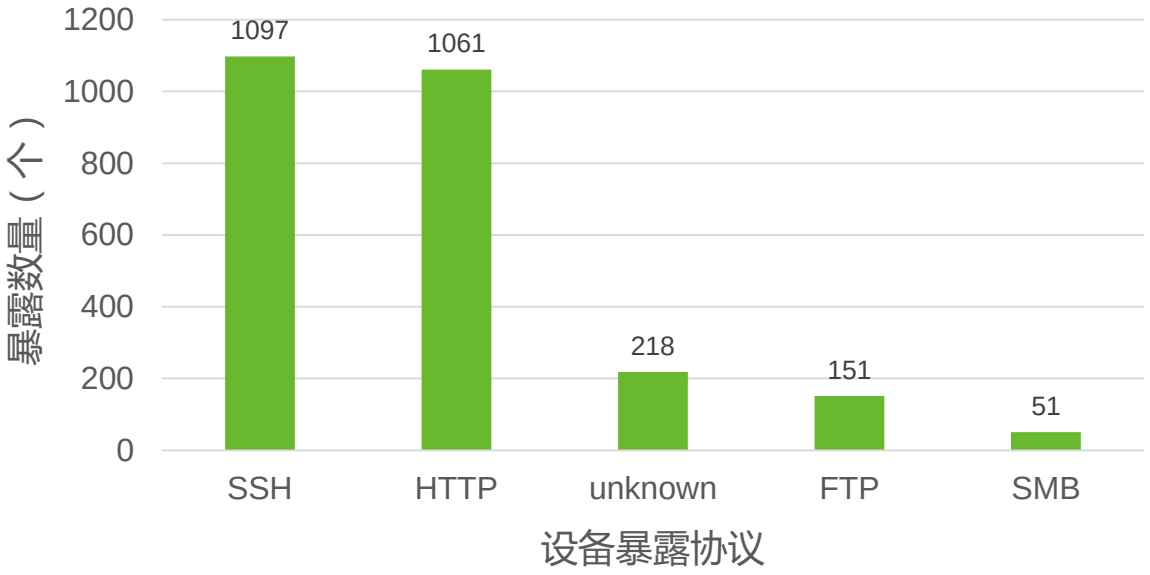


OpenWrt系列协议统计

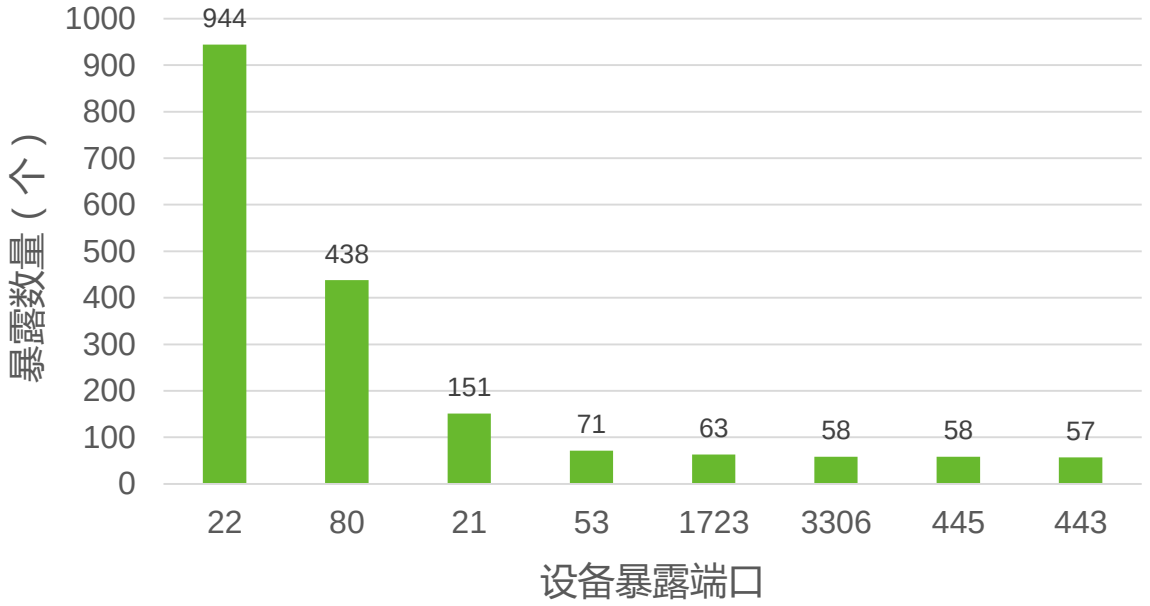
cathayQ1100-1 (build 13491M) - 資訊	HTTP	81
VoIP Gateway	HTTP	8080
VoIP Gateway	HTTP	8081
Q1100-5F (build 19154) - 資訊	HTTP	82
cathayipad5f (build 19154) - 資訊	HTTP	83
	HTTP	84

一个IP开启了多个HTTP服务的现象在这类设备上很常见

67.9%的运行“Raspbian”的设备开启了SSH服务

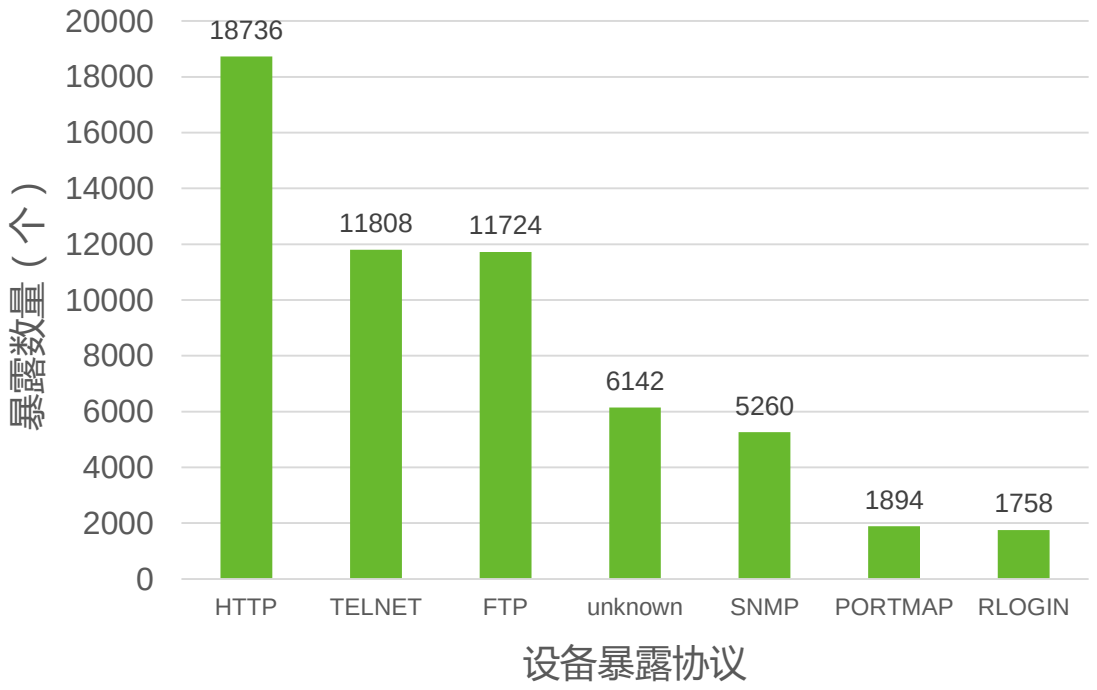


Raspbian协议统计

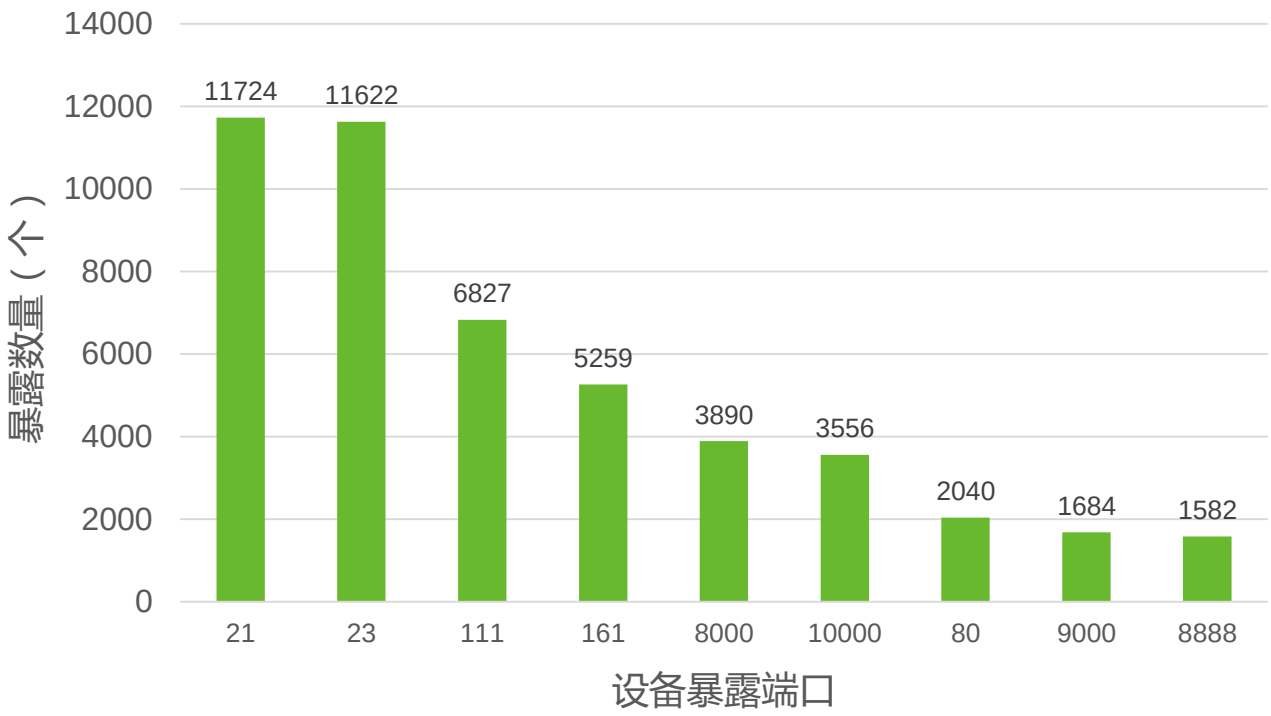


Raspbian暴露端口统计

运行“VxWorks”的设备对HTTP、SSH和Telnet开放较多



VxWorks协议统计



VxWorks暴露端口统计

NSFOCUS

04

总结

总结

- 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，我们通过对于三个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

防护建议—用户角度

- 修改初始口令以及弱口令，加固用户名和密码的安全性
- 关闭不用的端口，如FTP（21端口）、SSH（22端口）、Telnet（23端口）等
- 及时升级设备固件

防护建议—厂商角度

- 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
- 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
- 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
- 设置访问控制规则，严格控制从互联网发起的访问

谢谢！

NSFOCUS